シトリックス バーチャル アプリケーションズ および デスクトップ 7 2511

> **重要:**
>
> Current Release (CR) および Long Term Service Release (LTSR) の製品ライフサイクル戦略については、「ライフサイクルマイルストーン」を参照してください。

> Citrix Virtual Apps and Desktops は、あらゆるネットワークを介して、あらゆるデバイスにアプリケーションとデスクトップを配信する仮想化ソリューションを提供し、データセキュリティを強化し、コストを削減し、生産性を向上させます。

Citrix Virtual Apps and Desktops向け長期サービスリリース (LTSR) プログラムは、Citrix Virtual Apps and Desktopsリリースに安定性と長期サポートを提供します。

- ユースケース情報については、`<https://www.citrix.com/products/citrix-virtual-apps-and-desktops/>` を参照してください。
- Citrix Virtual Apps and Desktops の展開におけるコンポーネントとテクノロジーについては、「技術概要」を参照してください。

以前のリリース

現在利用可能なその他のリリースのドキュメントは、「Citrix Virtual Apps and Desktops」にあります。

さらに以前のリリースについては、ドキュメントは「レガシードキュメント」にアーカイブされています。

Citrix Cloud™ における Citrix Virtual Apps および Desktops

Citrix Cloud Virtual Apps and Desktops の提供は Citrix DaaS です。詳しくは、「Citrix DaaS」を参照してください。

役立つリンク

- Citrix サポート可能性パック
- LTSR FAQ
- Citrix Virtual Apps and Desktops サービスオプション
- 製品ライフサイクル日付
- Citrix Workspace app 向け LTSR プログラム

シトリックス バーチャルアプリおよびデスクトップ™ 7 2511

リリースについて

この Citrix Virtual Apps and Desktops リリースには、Windows Virtual Delivery Agent (VDA) の新しいバージョンと、いくつかのコアコンポーネントの新しいバージョンが含まれています。次のことができます。

- **サイトのインストールまたはアップグレード**: このリリースの ISO を使用して、コアコンポーネントと VDA をインストールまたはアップグレードします。最新バージョンをインストールまたはアップグレードすると、最新の機能を使用できます。
- **既存のサイトでの VDA のインストールまたはアップグレード**: 展開が既にあり、コアコンポーネントをアップグレードする準備ができていない場合でも、新しい VDA をインストール (またはアップグレード) することで、最新の HDX™ 機能のいくつかを活用できます。VDA のみをアップグレードすることは、非本番環境で機能強化をテストする場合に役立ちます。

  VDA をこのバージョンにアップグレードした後、マシンカタログの機能レベルを更新する必要はありません。詳しくは、「VDA のバージョンと機能レベル」を参照してください。

インストールとアップグレードの手順:

- 新しいサイトを構築する場合は、「インストールと構成」の順序に従ってください。
- サイトをアップグレードする場合は、「展開のアップグレード」を参照してください。

デリバリーコントローラー

Delivery Controller アップグレード用の LocalDB 自動インストール

Delivery Controller をアップグレードすると、メタインストーラーはサポートされている最新の SQL Server Express LocalDB バージョンを自動的にインストールします。この機能強化により、アップグレードプロセスが効率化されます。これにより、手動で LocalDB をインストールすることなく、ローカルホストキャッシュデータベースの互換性が確保されます。詳しくは、「自動更新」を参照してください。

HDX

デバイス

WIA リダイレクトの機能強化

管理者は、WIA リダイレクトを使用するために VDA でレジストリを変更する必要がなくなりました。Studio で WIA リダイレクトポリシー設定を有効にするだけで済みます。

USB 診断ツールの機能強化

USB 診断ツールは、管理者とドメインユーザーの両方をサポートするようになり、構成の問題を指摘し、最適化を提案する新しい「推奨事項」セクションが追加されました。

マルチホップセッションでのキーボードおよびバーコード入力の信頼性の向上

この機能は、**スキャンコード入力モード**で動作する非 Windows クライアントの入力信頼性を向上させ、キーイベントが Windows VDA によって順次処理されることを保証し、**RDP ダブルホップセッション**中の文字エラーを排除し、バーコードスキャナーが特殊文字ではなく数字を正しくレンダリングするようにします。

マルチメディア

パフォーマンスとユーザーエクスペリエンスを向上させるためのオーバーレイクリッピングの最適化

HDX Microsoft Teams最適化やUCSDK最適化などのマルチメディア最適化機能のオーバーレイクリッピングメカニズムは、パフォーマンスと視覚的な正確性を向上させるために再設計されました。

この機能強化により、メニューや通知などのアプリケーション要素がビデオコンテンツの背後に誤って表示される視覚的な不具合が解決され、よりシームレスなユーザーエクスペリエンスが提供されます。

この新しいアプローチは、リソースを大量に消費するメソッドも置き換え、VDAでのCPU使用率を大幅に削減します。詳細については、MTOPの機能リファレンスまたはUCSDKの機能リファレンスを参照してください。

ブラウザコンテンツリダイレクトのシングルサインオンサポート

ブラウザコンテンツリダイレクトは、シングルサインオンサポートにより合理化されたユーザーエクスペリエンスを提供するようになり、VDA側の認証とCookie共有を可能にします。この機能強化により、冗長なログインが排除され、BCRウィンドウが閉じられた後でもBCRセッション全

体で認証とCookieの永続性が維持されるため、生産性が向上します。このシームレスなエクスペリエンスは、認証がクライアントではなくVDAから行われることを保証することで、セキュリティをさらに強化します。

詳細については、ブラウザコンテンツリダイレクトのドキュメントを参照してください。

ブラウザコンテンツリダイレクトのサーバー側証明書検証

ブラウザコンテンツリダイレクトは、証明書検証サポートによりさらに強化されました。クライアントからリダイレクトされたWebサイトにアクセスする場合、クライアントオーバーレイブラウザは、サーバーまたはMitMプロキシからの証明書を信頼しない場合があります。このような場合、BCRはVDAの証明書ストアに対してホストまたはプロキシの証明書を検証できるようになりました。

詳細については、サーバー側証明書検証のドキュメントを参照してください。

グラフィック

一般的なHDXグラフィックの改善

このリリースでは、HDX Graphics に大幅な改善が加えられ、VDA の CPU、メモリ、帯域幅の消費量を著しく削減できます。パフォーマンスの向上に加えて、お客様は LAN ネットワークでより高い初期設定の画質も実感できます。

Director 用 HDX 画面共有

HDX画面共有は、Citrix Virtual Apps and Desktopsオンプレミスインストール向けのCitrix Directorと、Citrix Cloud展開向けのCitrix Monitorを使用したシャドウイングで利用できます。HDX画面共有は、シャドウイングの新しい方法であり、現在のシャドウイングに代わるネイティブで低遅延の代替手段を提供します。Director向けHDX画面共有は、ドメインに参加していないVDAやEntra IDに参加しているVDAを含むすべてのVDAで利用できます。

HDX 画面共有の改善

HDX画面共有の改善点には、HDX画面共有ポートとタイムアウトを制御するための構成ポリシーが含まれます。

AMD V710 GPUのサポート

AMD v710 GPUsのサポートが追加されました。

シームレスアプリケーション

シームレスアプリケーションの改善

シームレスアプリケーションが、透過ウィンドウと動的ウィンドウプレビュー（Windows Peek）をサポートするようになりました。

シームレスアプリケーションのWindowsアクセシビリティ設定

シームレスアプリケーションのWindowsアクセシビリティ設定は、すべてのシームレスセッションでデフォルトでオンになりました。

HDX 接続

HDX ダイレクト

外部ユーザー向けの追加のHDX Directステータス詳細をログに記録するための新しいイベントが追加されました。詳細については、「HDX Directのトラブルシューティング」を参照してください。

仮想配信エージェント (VDA)

コマンドライン経由でVDAをインストールまたはアップグレードするためのカスタムスクリプトを生成する

コマンドラインでVDAをインストールまたはアップグレードするためのカスタムスクリプトを生成する新機能が導入されました。VDAインストーラーUI内で、ユーザーは無人インストールまたはアップグレード用のカスタムスクリプトを作成できるようになりました。この機能強化により、インストーラーパスやWebSocketトークンなどのパラメーターを使用してこれらのスクリプトを構成、保存、実行するためのステップバイステップのガイダンスが提供されます。この機能は、展開プロセスにおける自動化と精度を大幅に向上させます。

VDA メタインストーラーヘルパーツール

VDAのインストールとトラブルシューティングを簡素化および合理化するための新しいVDAメタインストーラーヘルパーツールが利用可能になりました。これは、SCCMタスクシーケンスの検証と生成を支援し、VDAインストール要件との互換性を確保します。このツールには、インストールログをレビューし、エラーや警告を強調表示し、解決策の推奨事項を提供するログアナライザーも含まれています。シンプルなMSIインストールと使いやすいインターフェイスにより、IT管理者はVDAをより効率的に、より少ない問題で展開できます。

VDAメタインストーラーの変更点

Citrix Virtual Apps and Desktops 7 2511では、Citrix Device Trust、uberAgent、およびWorkspace Environment ManagementエージェントのVDA内への統合インストールが導入されています。/componentsや/excludeなどの柔軟なコマンドラインオプションを使用して、Citrix Workspaceアプリ、Secure Access Client、User Personalization Layerなどのコンポーネントのインストール、アップグレード、またはアンインストールをカスタマイズできます。ただし、デフォルトの動作とコンポーネントの選択は、シングルセッションOS VDAとマルチセッションOS VDAで異なります。詳細については、「VDAのインストール」および「コマンドラインを使用したインストール」を参照してください。

シングルセッションコアサービス Virtual Delivery Agent 用の新しいメタインストーラー

Windows 365 Cloud PCおよびRemote PCの展開向けに、新しい軽量のシングルセッションVDAメタインストーラーが利用可能になりました。このインストーラーは既存のRemote PCインストーラーに基づいて構築されており、完全なシングルセッションVDAの合理化されたバージョンとして機能し、Profile Management、deviceTRUST、uberAgent、WEM、Backup and Restore、およびVDA Upgrade Agentとともに、不可欠なVDAコンポーネントを提供します。これにより、パッケージサイズが大幅に削減され、クラウドベースのワークロードのインストール信頼性が向上します。最新のRemote PCシナリオ向けに設計されたこのインストーラーは、Windows 365およびRemote PCにCitrixワークロードを展開するための簡素化された高性能なオプションを提供します。

Citrix 常時オン トレース

すべてのCVADコンポーネント向けのCitrix AOT

最新のアップデートでは、Always-On Tracing (AOT) が大幅に拡張され、Citrix環境全体でログを収集、一元化、分析することが容易になりました。Web Studioの新しい構成エクスペリエンスにより、管理者はログサーバーの定義、ログ記録範囲の制御、Directorへのアクセスを1か所から有効にでき、すべての設定はサイトデータベースを通じて自動的に伝播されます。Directorには専用のログビューが追加され、検索、時間フィルター、カテゴリ、重大度フィルター、マシンレベルフィルターを使用して、AOTイベントをリアルタイムで可視化できます。AOTの適用範囲は、Mac VDA、Linux VDA、FAS、Session Recording Serverなど、すべてのコアコンポーネントを含むより多くのCitrixコンポーネントに拡張され、制御プレーンとデータプレーンのワークフロー全体で真のエンドツーエンドトレースが可能になりました。

AOTログサーバーは、取り込みパフォーマンスの向上、ノードあたり最大10,000コンポーネントのサポート、およびLZ4を使用した圧縮の改善によるストレージ効率の向上によって強化されまし

た。新しいサイジングガイダンスとパフォーマンスベースラインは、管理者が環境の容量を計画し、ストレージとIOPSを調整するのに役立ちます。スタンドアロンコンポーネントは、シンプルなPowerShellコマンドを通じてログをログサーバーにプッシュできるようになり、集中ログモデルに準拠します。詳細を確認し、ここから展開を開始してください。

ウェブスタジオ

AWSローカルゾーンでのワークロードのプロビジョニング

Amazon Workspaces Core Managed InstancesとEC2ワークロードをAWSローカルゾーンに直接プロビジョニングできるようになりました。この新機能は、次のことに役立ちます。

- Citrixワークロードをエンドユーザーの近くに展開することで、低遅延アクセスを提供します。
- 完全なAWSリージョンが提供されていない地域で、Citrixインフラストラクチャの地域カバレッジを向上させます。

目的のローカルゾーンのホスティングユニットでホスト接続を作成し、そのローカルゾーンにVMをプロビジョニングできます。

詳細については、以下を参照してください。

- Amazon WorkSpaces Core マネージドインスタンス:
  - Web Studioを使用して接続を作成する
  - マシンカタログノードからマシンカタログを作成する
- AWS EC2:
  - Web Studioを使用して接続を作成する
  - Web Studioを使用してカタログを作成する

Web Studio を使用した AWS EC2 でのクロスアカウントプロビジョニング

Cloud Connector を別の AWS アカウント (共有サービスアカウントまたはサイトコンポーネントアカウント) に配置し、クロスアカウントアクセス (クロスアカウント IAM ロール) を持つ IAM ロールを使用し、追加の Cloud Connector を別の AWS アカウントに配置することなく、MCS プロビジョニングされたマシンカタログを別のセカンダリ AWS アカウント (ワークロードアカウント) に配置したいというユースケースがあります。このような展開モデルは、PowerShell SDK を使用してすでにサポートされており、Web Studio UI を使用してもサポートされるようになりました。

AWS EC2 でのバックアップ VM 構成

Web Studio では、キャパシティ関連の問題が発生した場合に Machine Creation Services (MCS) がフォールバックできる AWS 環境のバックアップ EC2 インスタンスタイプ (オンデマンドまたはスポットインスタンスにできる「バックアップ SKU」) のリストを定義できるようになりました。MCS は、リストで指定された順序でバックアップ EC2 インスタンスタイプにフォールバックしようとします。詳細については、「Studio を使用したカタログの作成」を参照してください。

AWS EC2 セキュリティグループ構成

Web Studio でカタログの作成または編集にマシンプロファイルを使用する場合、セキュリティグループの構成プロセスが合理化されました。セキュリティグループを手動で構成する必要がなくなり、専用の構成ページがスキップされるため、マシンプロファイルの設定との一貫性が確保されます。マシンプロファイルに基づかないカタログの既存のワークフローは変更されません。さらに、テナンシータイプ選択メニューは、カタログ作成ウィザードの**セキュリティ**タブから**仮想マシン**タブに移動されました。詳細については、「Web Studio を使用したカタログの作成」を参照してください。

Azure で暗号化された準備済みイメージをリージョン間で共有する

Azure Compute Gallery (ACG) イメージは、ディスク暗号化セット (DES) で暗号化できます。この機能を使用すると、DES を使用して、同じサブスクリプションおよびテナント内の複数のリージョン間で暗号化された準備済み ACG イメージを共有できます。その後、暗号化された準備済みイメージが共有されているリージョンにマシンカタログを作成できます。詳細については、「暗号化された準備済みイメージをリージョン、サブスクリプション、テナント間で共有する」を参照してください。

Azure の MCS マシンカタログで ZRS を有効にする

Azure MCS マシンカタログのディスク構成でゾーン冗長ストレージ (ZRS) を構成できるようになりました。この機能強化は、次のことに役立ちます。

- ゾーンレベルの停止に対する VM の回復性を向上させます。
- Azureが利用可能な任意のゾーンでVMを起動できるようにし、VM配置の柔軟性を高めます。
- ディスクの元のゾーンが利用できない場合でもVMの可用性を確保することで、ローカル冗長ストレージ (LRS) の制限を克服します。

既存のAzure MCSマシンカタログを作成および編集する際に、ZRSを構成できます。

詳細については、以下を参照してください。

- Web Studio で Azure Resource Manager イメージを使用してマシンカタログを作成する
- カタログの編集

エフェメラルOSディスク使用のためのNVMe v6 SKUを表示

Web Studioを使用して、エフェメラルOSディスクをNVMeディスクに保存するオプションが利用可能になりました。詳細については、「Azure エフェメラルディスク」を参照してください。

Web Studioを使用したAzure機密VMでのイメージ管理のサポート

イメージノードを使用して、Azure Confidential VMと互換性のあるイメージを準備および管理できるようになりました。この目的を達成するためにPowerShellコマンドを使用することもできます。詳細については、「Azure Confidential VM」を参照してください。

Azureでローカル冗長ストレージタイプ (LRS) またはゾーン冗長ストレージタイプを選択するオプション

Web Studioでは、マシンカタログ作成時のデータ回復オプションとして、ローカル冗長ストレージ（LRS）タイプとゾーン冗長ストレージ（ZRS）タイプを選択できるようになりました。これらの冗長ストレージタイプが提供する利点を検討し、要件に基づいて選択できます。

AHV 上の Nutanix Prism Central との統合

新しいホスト接続であるNutanix AHV Prism Centralを使用して、Citrix Virtual Apps and Desktops環境をNutanix Prism Central経由でNutanix AHVクラスターに接続できるようになりました。

Nutanix AHV Prism Centralホスト接続を使用する利点は次のとおりです。

- 電源管理のみのVDAとMCSプロビジョニングされたVDAの両方を含むマシンカタログをサポートします。
- テンプレートバージョンを使用して、AHVクラスター間でMCSマスターVMの共有を可能にします。
- ホスト接続での証明書信頼を簡素化します。
- Delivery Controllersにプラグインを個別にインストールする必要がなくなります。

詳細については、以下を参照してください。

- Nutanix仮想化環境
- Nutanixクラウドおよびパートナーソリューション
- Nutanixへの接続

- Nutanixクラウドおよびパートナーソリューションへの接続
- Nutanixカタログの作成
- Nutanixカタログの管理

Azure LocalでWindowsおよびLinux仮想マシンをプロビジョニングする

Azure Local上のWindowsおよびLinux VM向けに、MCSを使用してMCSマシンカタログとCitrix Provisioningカタログをプロビジョニングおよび管理できるようになりました。

Windows VMの場合、ホスティング接続とユニットを作成および管理し、Windows 10/11シングルセッションおよびWindows Serverマルチセッション VM（永続的および非永続的の両方）をプロビジョニングできます。作成後に新しいVMのネットワーク、ライトバックキャッシュ（WBC）、またはADサービスアカウント設定を更新することもできます。これは、オンプレミスAD、ドメイン非参加、およびEntraハイブリッド参加デバイスをサポートします。

Linux VMの場合、この機能はUbuntu、CentOS、Red Hat Enterprise、SUSEをサポートします。これらのOSタイプでカタログをプロビジョニングし、永続的および非永続的なLinux VMを展開し、認証のためにオンプレミスADまたはドメイン非参加VMと統合し、ホストユニット（ストレージおよびネットワーク設定を含む）を管理し、カタログ内の新しくプロビジョニングされたVMで構成変更を実行できます。

詳細については、以下を参照してください。

- Azure Localへの接続
- Azure Localカタログの作成
- Citrix Provisioningドキュメント: Citrix StudioでCitrix Provisioning™カタログを作成する

XenServer での準備済みイメージバージョンの管理

XenServer 仮想化環境でイメージ管理機能が一般提供されるようになりました。**イメージ**ノードを使用して、複数のイメージバージョンを作成し、複数のマシンカタログに適用または更新できます。この実装により、ストレージと時間のコストが大幅に削減され、VM の展開とイメージの更新プロセスが簡素化されます。この目的を達成するために PowerShell コマンドを使用することもできます。詳細については、「XenServer で準備済みイメージマシンカタログを作成する」を参照してください。

準備済みイメージの割り当て中にメモを追加する

この機能を使用すると、準備済みイメージを使用してMCSカタログを作成または更新する際に、Web StudioとPowerShellを使用してカスタムメモを追加できるようになりました。MCSは、すべての準備済みイメージの割り当ての記録を保持します。これにより、次のことが可能になります。

- カタログに割り当てられたすべての準備済みイメージのイメージ割り当て履歴を取得する。
- **クイックロールバックのために以前のイメージ割り当てを使用する**アクションを使用して、マシンカタログを以前に割り当てられた準備済みイメージにすばやくロールバックします。履歴リストからバージョンを選択するだけで、迅速かつ情報に基づいたロールバックが可能です。ロールバックの詳細については、「異なる準備済みイメージでマシンカタログを更新する」を参照してください。

この機能は、Azure 環境と VMware 環境の両方に適用できます。

準備済みイメージを含むカタログの作成については、以下を参照してください。

- Azureで準備済みイメージマシンカタログを作成する
- VMwareで準備済みイメージマシンカタログを作成する

準備済みイメージでカタログを更新する方法については、「」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/manage-prepared-image-machine-catalogs).

プロビジョニングコストインサイトの視覚化

マシンカタログの詳細なコスト情報を表示できるようになりました。この視覚化により、過去 30 日間のプロビジョニングコストと傾向の概要がわかります。

レポートは、個々のカタログに基づいてプロビジョニングコストを分類し、各カテゴリが総コストにどのように貢献しているかを明確に理解できるようにします。レポートは次のとおりです。

- 過去30日間に発生した総コストを表示します。
- 現在の30日間の総コストを、前の30日間と比較します。
- のコスト詳細を表示します:
    - コンピューティングコスト
    - ストレージコスト
    - ネットワークコスト
    - その他のコスト

詳細については、「カタログの詳細を表示」を参照してください。

信頼されていないホスト接続証明書の再信頼オプション

信頼されていない証明書が原因でホスト接続の停止が発生した場合、Web Studio でそのホスト接続の証明書を再信頼できます。詳細については、「TLS 証明書の信頼をテストする」を参照してください。

休日のカスタムスケジュール

Autoscale を使用すると、祝日などの特定の日にデリバリーグループ内の未使用の VM をオフにするカスタムスケジュールを作成して、不要なリソース消費を削減できるようになりました。

カスタムスケジュールを作成するには:

1. Web Studio で、**Delivery Groups** に移動します。デリバリーグループを右クリックし、**Manage Autoscale** を選択します。
2. **Schedule** ページで、**Create schedule** をクリックします。

詳細については、「Studio を使用してカスタム祝日スケジュールを作成する」を参照してください。

検索ノードでのマシンハードウェアビュー

Machine Creation Services (MCS) を使用してプロビジョニングされたマシンについて、検索ノードで専用のハードウェアビューにアクセスできるようになりました。このビューにより、マシンのハードウェア詳細がより明確になり、MCSでプロビジョニングされたマシンの管理が容易になります。 主な利点は次のとおりです。

- マシンサイズ、オペレーティングシステム、ライセンスタイプ、セキュリティ設定、ネットワーク、イメージとテンプレート、ディスク設定など、詳細なハードウェア構成を表示します。
- ハードウェアフィルターと検索オプションを使用して、マシンを簡単に見つけます。

現在、ハードウェアビューは、VMware、XenServer、SCVMM/Hyper-V、Nutanix PC、Azure、Azure Arc、Azure Local、AWS EC2、およびGCPのMCSプロビジョニングマシンで利用できます。OpenShiftおよびAmazon WorkSpaces Core Managed Instancesでは、現在、基本的なハードウェア情報のみが列として表示されます。詳細については、「検索 > ハードウェアビューでMCSプロビジョニングマシンを監視する」を参照してください。

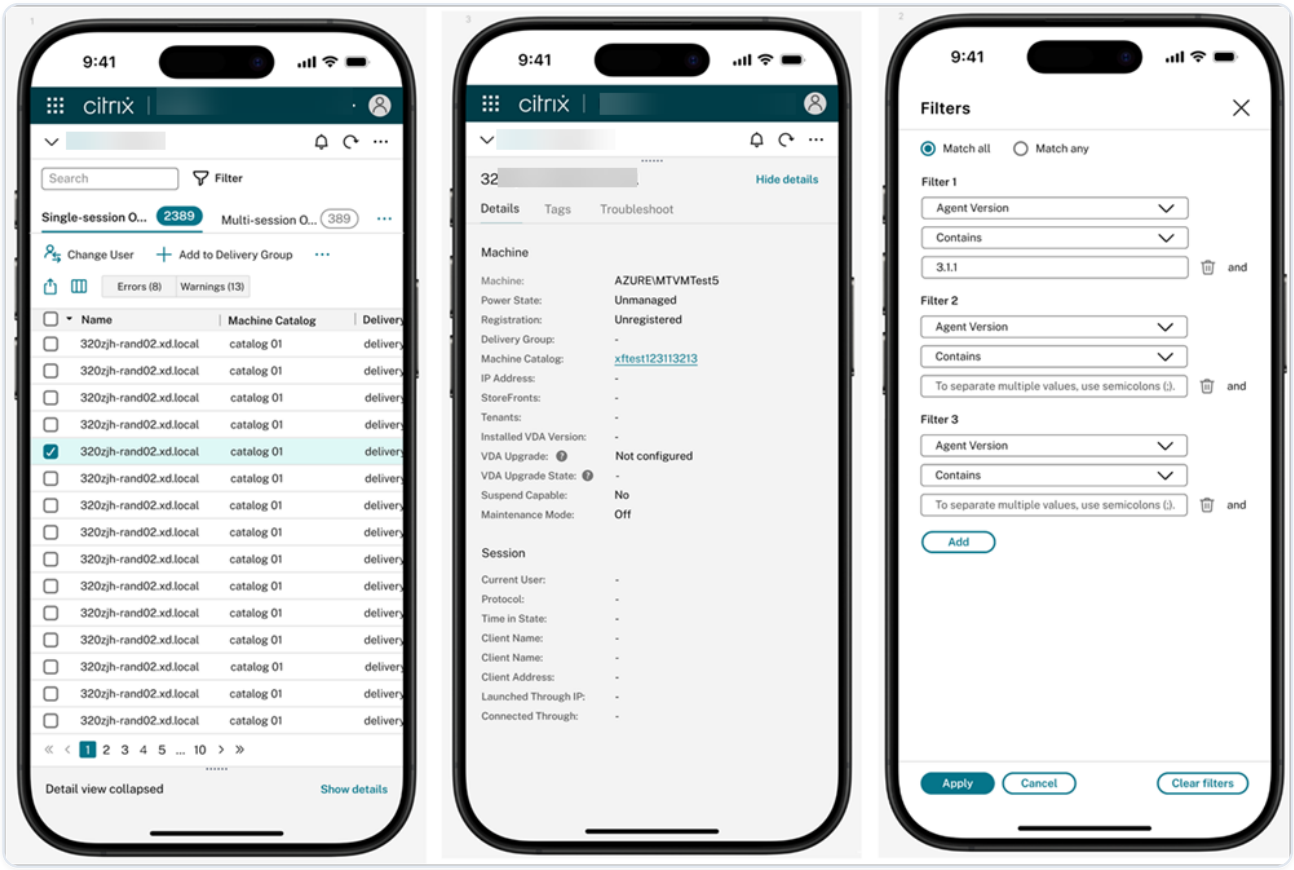
重要な外出先でのタスク向けに強化されたモバイルエクスペリエンス

モバイルデバイスからCitrix Virtual Apps and Desktopsの展開をより簡単に管理できるようになりました。更新されたエクスペリエンスは、小さな画面向けに最適化されており、デスクトップが利用できない場合でもモバイルデバイスからStudioにアクセスしやすくなっています。アラートに対応する場合でも、構成ミスをすばやく確認する場合でも、すぐにアクションを起こすことができ、デスクに戻るまで待つ必要はありません。

モバイルインターフェイスはアクセシビリティが向上し、タッチフレンドリーな操作のために設計されています。レイアウトと機能は、モバイルワークフローにより適するように、デスクトップエクスペリエンスとは若干異なる場合があります。

レスポンシブなレイアウトと合理化されたナビゲーションにより、次のことが可能になります。

- 展開の健全性を一目で監視
- マシンカタログとデリバリーグループの詳細を表示
- マシンの再起動やデリバリーグループの無効化など、主要なアクションを実行



カタログ作成時のAzure VMコストの見積もり

マシンカタログを作成する際に、VMサイズとディスクコストを含むAzure仮想マシンの月額コストを見積もることができるようになりました。また、1日の稼働時間、稼働日数、節約プラン、予

約インスタンス、シャットダウンストレージなどの設定を調整して、見積もりをさらに細かくすることもできます。この機能は、展開をより効率的に計画し、早期にコストを最適化するのに役立ちます。

詳細については、「概要ページで月額見積もりの詳細を表示する」を参照してください。

構成の健全性チェック用のサイト診断テスト

ホームのサイト詳細ウィジェットからサイト診断テストを実行できるようになりました。この機能は、Citrix Virtual Apps and Desktops環境の健全性を迅速に評価し、一般的な構成の問題を特定するのに役立ちます。パフォーマンスの問題のトラブルシューティングを行う場合でも、アップグレードの準備をする場合でも、これらのテストは迅速で実用的な洞察を提供します。検出される一般的な問題には、次のものがあります。

- Delivery Controller の通信障害
- データベースの接続または構成エラー

この機能は、アップグレード中に特に役立ち、展開の前後でサイトが安定して準備ができていることを確認するのに役立ちます。詳細については、「サイトの詳細」を参照してください。

より明確な制御とカスタマイズのための再起動UIの改善

再起動スケジュールのUIを強化し、再起動モードをより明確でカスタマイズしやすくしました。グレースフル再起動と強制再起動を簡単に区別し、ニーズに合わせてカスタム再起動期間を設定できるようになりました。 情報に基づいた選択ができるように、強制再起動がセッションが応答しない場合でもマシンを強制的に再起動できる方法など、主要なオプションを説明するツールチップも追加しました。

詳細については、「再起動スケジュールの作成」を参照してください。

新しいログインページ設定

Web Studioの**設定**ノードに、Web Studioのログインエクスペリエンスを向上させるための2つのオプションが追加されました。

- **ログインページ通知**: 重要な情報を管理者に共有するためのカスタムメッセージを表示します。
- **接続されているDelivery Controllerを表示**: 接続されているDelivery ControllerのFQDNを表示し、可視性と透明性を高めます。

詳細については、「設定」を参照してください。

マイプリファレンス設定でStudioビューをカスタマイズする

設定ノードの下に新しい**マイプリファレンス**タブが追加されました。このタブの設定により、Studioインターフェイスを好みに合わせて調整できます。これらの設定はあなたのアカウントにのみ適用され、他の管理者には影響しません。 以下のオプションを設定できます。

- **日付と時刻**: 既定のタイムゾーン、日付形式、時刻形式を設定します。これらの設定は、スケジュールされた再起動や自動スケーリングなど、時刻に関連する表示のためにStudio全体で使用されます。
- **フォルダービュー**: **マシンカタログ**、**デリバリーグループ**、**アプリケーション**ノードでフォルダービューを表示するか非表示にするかを選択します。
- **検索でのタブオーダー**: **検索**ノード内のタブオーダーをカスタマイズします。

詳しくは、「設定」を参照してください。

SQL Server接続設定の強化

SQL Server接続に3つのセキュリティ設定（**暗号化**、**サーバー証明書を信頼する**、**証明書のホスト名**）を構成できるようになりました。これらの設定により、柔軟性が向上し、本番環境の要件に基づいてデータベース接続のセキュリティを強化できます。 この機能強化をサポートするために、以下のUIを更新しました。

- **Citrix Site Manager**: サイトの作成時またはデータベース設定の変更時にこれらのオプションを構成できます。
- **Web StudioのSettingsページ**: データベース設定の変更時にこれらのオプションを構成できます。

詳しくは、「データベースのセットアップ」および「データベースの場所の変更」を参照してください。

Web Studioのインストールにおける柔軟性

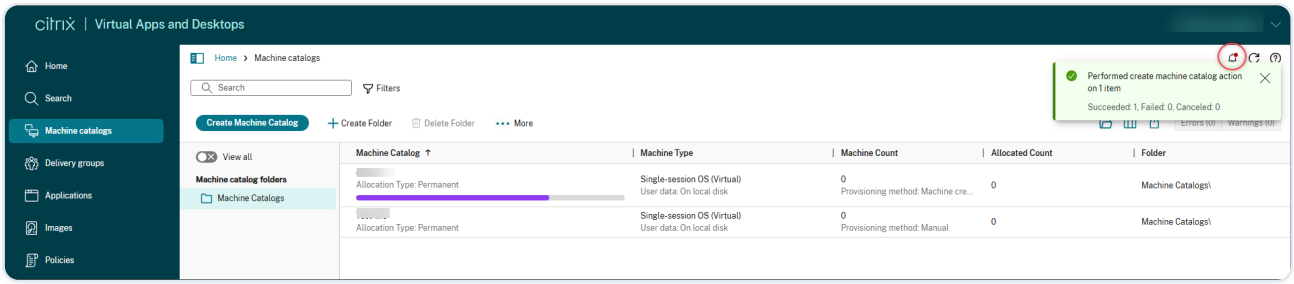
Web Studioを、サイト名に関係なく**サイトID = 1**の任意のIIS Webサイトにインストールできるようになりました。この機能強化により、Web Studioを**Default Web Site**に限定されることなく、カスタムIISサイトでホストできます。

インストーラーの実行時にIISがインストールされていない場合、IISは自動的にセットアップされ、Web Studioは**Default Web Site**に展開されます。IISがすでにインストールされている場合は、**サイトID**が**1**である限り、任意の名前とパスでサイトを事前に作成できます。

詳しくは、「Web Studioのインストール」を参照してください。

セッション内通知とバックグラウンド操作

Web Studioに通知センターが追加され、バックグラウンド操作のリアルタイムな可視性と操作結果のレポートが提供されるようになりました。時間のかかる操作を開始すると、進行中であることを知らせる通知が右上に表示されます。以前はUIをブロックしていた操作がバックグラウンドで実行されるようになり、中断することなく作業を続行できます。操作が完了すると、リアルタイムのステータス通知が表示され、結果も通知センターに保存されます。通知センターは48時間の履歴を保持するため、最近のアクティビティを簡単に追跡できます。



Studioキャッシュモード

Studioは管理データをキャッシュするようになり、コンソールがより高速で応答性が向上しました。ノードを再訪すると、以前に読み込まれたビューが瞬時に表示され、ナビゲーション時の待機時間が短縮されます。

Microsoft Entra IDユーザーへのCitrixグループポリシーの割り当てのサポート

StudioでIDPからMicrosoft Entra IDユーザーにCitrixグループポリシーを割り当てることができるようになりました。この機能強化により、特定のユーザーグループにポリシーを適用する際の柔軟性が高まり、Citrix Virtual Apps and DesktopsとWindows 365を使用した展開が簡素化されます。

プラットフォームをまたがるデスクトップアイコンのカスタマイズ

Web Studioでは、任意のデスクトップのデスクトップアイコンをカスタマイズできるようになりました。以前は、すべてのデスクトップでデフォルトのアイコンが使用されており、Studioで変更することはできませんでした。これで、次のことが可能になります。

- アイコンをアップロードし、デスクトップまたはアプリに使用する
- 個々のデスクトップのアイコンを変更する
- 選択したデスクトップの組み込みアイコンから選択する

詳しくは、「デリバリーグループの作成」および「デリバリーグループの管理」を参照してください。

デリバリーグループにおけるアクセスポリシーのよりきめ細かな制御のサポート

以前は、PowerShellまたはREST APIを使用してのみ、特定のユーザーにアクセスポリシーを適用できました。現在、この目標はStudioで直接達成できます。この機能強化により、さまざまなユーザーまたはユーザーグループに対して異なるアクセス条件を定義する際の柔軟性が高まり、より詳細なアクセス制御が可能になります。詳しくは、「アクセスポリシーのユーザー範囲を構成する」を参照してください。

さらに、StudioとPowerShellまたはREST APIアプローチとの互換性が向上しました。以前は、PowerShellまたはREST APIを使用してユーザー範囲を持つアクセスポリシーを構成した場合、Studioのユーザーおよびアクセスポリシーページはブロックされていました。Studioはこれらのシナリオを完全にサポートするようになり、必要に応じて明確な情報またはUIガイダンスを提供します。

デリバリーグループレベルでのアプリに対するアクセス制御のサポート

Studioでは、以前は個々のアプリレベルでのみアプリのアクセス制御を行え、デリバリーグループレベルでは行えませんでした。現在では、デリバリーグループレベルでアプリのアクセス制御を実行できます。この機能は現在、デリバリーグループ内のすべてのアプリへのアクセス制御に限定されています。

詳細については、「特定のユーザーへのアプリケーションアクセスを制限する」を参照してください。

セキュリティ強化のためのユーザー割り当てのデフォルトの強化

デリバリーグループ内でユーザーを割り当てる際のデフォルトの動作を更新しました。制限された制御がデフォルトとなり、セキュリティの向上とより詳細なアクセス制御が保証されます。代替オプションである **認証済みユーザーがリソースを使用することを許可する** は、現在 **非推奨** と明確にマークされており、広範なアクセスを目的とした共有またはプールされたデスクトップ、キオスク環境、テスト目的などの特定のシナリオでのみ使用する必要があります。この変更は、必要なときに柔軟性を提供しつつ、リスクを軽減するのに役立ちます。

詳細については、「アクセスポリシーのユーザー範囲を構成する」を参照してください。

Always-on Tracing (AOT) ログをログサーバーに転送する

Web Studioを使用すると、CitrixコンポーネントからのAOTログを、指定されたログサーバーに転送できるようになりました。この機能により、Citrix環境の集中トラブルシューティングと高度な監視が可能になります。詳細については、「設定」を参照してください。

アプリケーションパッケージ管理の改善

Web Studioでは、更新を確認する際に、ソースの場所に存在しなくなったパッケージを自動的に削除するオプションを選択できるようになりました。**基本設定** フィールドにあるこの新しい **不在パッケージを削除** オプションは、**パッケージ** タブから古いエントリを削除することで、アプリケーションパッケージUIを簡単にクリーンアップするのに役立ちます。 さらに、App packages ノード内のいくつかのタブとセクションの名前が変更され、Studioで現在サポートされている幅広いパッケージタイプとの整合性が向上しました。

- **ソースの追加** は 検出プロファイルの作成 になりました
- **パッケージの更新を確認** は **更新を確認** になりました
- **ソースの削除はプロファイルの削除になりました**

詳細については、「アプリパッケージの管理」を参照してください。

Elastic App レイヤーの検出と割り当てのサポート

Web Studioの **App packages** ノードを使用して、Elastic Appレイヤーを検出および公開できるようになりました。この機能により、次のことが可能になります。

- Citrix App Layeringを使用して作成されたElastic Appレイヤーのライブラリを検出して列挙します。
- 非永続的なマシンカタログ上のユーザーにアプリを柔軟に配信するための割り当てポリシーを作成します。
- イメージがApp Layeringアプライアンスから公開されたかどうかに関係なく、ポータブルなElastic Appレイヤーを任意の非永続的なWindowsマシンに配信します。

詳細については、「Elastic Appアプリケーション」を参照してください。

Numecent Cloudpaging アプリの検出と割り当てのサポート

Web Studio の**App packages**ノードを使用して、Numecent Cloudpaging アプリを検出して公開できるようになりました。

詳細については、「Cloudpagingアプリケーション」を参照してください。

パッケージ化されたアプリケーションの可視性を制御するサポート

Web Studioを使用すると、デスクトップ、**Citrix Workspace > Apps**、またはその両方で、パッケージ化されたアプリケーションの可視性を制御できるようになりました。特定のパッケージ化されたアプリの可視性を変更するには、**Applications**ノードに移動し、アプリケーションを選択

して、**Properties > Delivery**を選択します。 デフォルトでは、パッケージ化されたアプリケーションは**Citrix Workspace > Apps**でのみ配信されます。

詳細については、「アプリケーションプロパティの変更」を参照してください。

ライトバックキャッシュディスクにAzure一時ディスクを自動的に使用するサポート

StudioでMCSプロビジョニングされたカタログを編集すると、必要な条件が満たされている場合、カタログはライトバックキャッシュ（WBC）ディスクにAzure一時ディスクを自動的に使用するようになりました。その結果、カタログに追加される新しいVMは、WBCディスクにAzure一時ディスクを使用します。 以前は、カタログ作成時に条件を満たしていなかった場合、後でカタログが更新されて条件を満たしたとしても、WBCディスクにAzure一時ディスクは使用されませんでした。 利点：

- コストを削減します。VMの電源がオフの場合、一時ディスクにはストレージコストが発生しません。
- 柔軟性を向上させます。カタログを再作成することなく、WBCに一時ディスクを使用します。MCSプロビジョニングされたカタログは、次のすべての条件を満たす場合に、WBCディスクにAzure一時ディスクを自動的に使用します。
- MCSIOが有効になっている。
- WBCディスクは非永続的です。
- VMサイズには、WBCディスクに十分な大きさの一時ディスクが含まれています。
- WBCディスクにはドライブ文字が指定されていません。

詳細については、「Microsoft Azureカタログの作成」を参照してください。

Citrix ディレクター

マシン診断インサイト

Citrix Directorに新しいマシン診断インサイトパネルが追加され、セッション障害やパフォーマンスの問題をプロアクティブに特定してトラブルシューティングするのに役立ちます。この機能は、15分ごとに更新されるリアルタイムのインサイトを導入し、サイト全体の問題のあるマシンを強調表示します。

DirectorとCitrix Virtual Apps and Desktops集中ログサーバーのAOT統合

Directorは、基盤となる診断機能としてAlways On Tracing (AOT) と統合されています。これにより、重要なVDAおよびセッションイベントの継続的かつ低オーバーヘッドなキャプチャと分析が可能になります。

主な機能は次のとおりです。

- AOTログの表示: DDC、VDA、StoreFrontなど、さまざまなCitrix Virtual Apps and Desktopsコンポーネントのログにアクセスします。
- AOTログのフィルターと検索: 特定の期間のAOTログを取得し、カテゴリ、ログクラス、ホスト名による検索とフィルターをサポートします。
- Director/Monitorとのシームレスな統合: Director/Monitorの「マシンフィルター」、「セッション起動失敗診断」、「アクティビティマネージャー」から、特定のVDAまたはセッションのきめ細かいAOTログデータに簡単に移行できます。

「IN」演算子を使用した主要エンティティの複数選択サポート

この機能強化により、「IN」演算子を使用して、ユーザー、マシン、デリバリーグループなどの主要なフィルターフィールドに複数の値を選択できるようになります。

デリバリーグループの複数選択のサポート

トレンドタブのセッションおよびログオンパフォーマンスページにあるデリバリーグループのドロップダウンが、次の機能で強化されました。

- テキスト入力を使用してデリバリーグループ名を検索
- 包括的な分析のために、最大15個のデリバリーグループを複数選択

この機能強化により、使いやすさが向上し、複数のデリバリーグループ間で同時に、より効率的な監視と比較が可能になります。

強化されたワークロードの適正化

強化されたワークロードの適正化ページは、デリバリーグループの使用状況とサイジングの側面を分析するのに役立ちます。これにより、デリバリーグループはマシンまたはユーザーのアクティビティに基づいて分析できます。 マシンベースの分析により、次のことが可能になります。 使用状況に基づいて仮想デスクトップを分類し、アクティビティがない、または低いマシンを特定し、未使用のリソースへの支出を削減します。 仮想デスクトップのリソース使用率を分析し、適正化する必要があるマシンを特定して、コストを削減したり、ユーザーエクスペリエンスを向上させたりします。

ユーザーベースの分析では、次のことが可能です。

- ユーザーをアクティビティに基づいて分類します。IT衛生上の理由から、アクティビティのないユーザーのアクセス権を削除することを検討してください。使用率の低いユーザーは、リソースをより効率的に使用するために共有リソースに移動できます。
- ユーザーのリソース消費量を分析し、平均よりも高いまたは低いリソース消費量を持つコホートを特定して、ユーザーをより効果的に分散させます。

この分析は、Windows 365 EnterpriseやFrontline dedicatedのように、仮想デスクトップがユーザーに静的に割り当てられているシナリオに最適です。ランダムに割り当てられた仮想デスクトップまたはマルチセッションマシンを持つデリバリーグループも分析できますが、ユーザーがこれらのマシン間を移動するため、分析は平均値を示します。

> **注:**
>
> ページ上部の「すべてのワークロード」ボタンからアクセスできる従来の適正化分析は、今後のリリースで非推奨になります。

垂直および水平ロードバランシングアラートの処理が改善されました

以前は、`UseVerticalScalingForRdsLaunches` を true に設定し、Studio で「最大セッション数」ポリシーを構成すると、マシンは「最大容量」状態に移行しました。Director は、制限が垂直または水平ロードバランシングのいずれかによって到達したかどうかにかかわらず、「最大容量」のアラートをトリガーしました。「最大負荷に達しました」などの特定のエラーが発生した場合、垂直ロードバランシングと水平ロードバランシングを区別する方法はありませんでした。これにより、垂直スケーリングシナリオにおける予期される動作に対して不要なアラートが発生し、時間の無駄と混乱を招いていました。

垂直負荷分散がアクティブで、マシンがセッション制限に達すると、「垂直スケーリングの最大容量」という新しい状態に移行します。Director はこの新しい状態に対してアラートを生成しなくなります。アラートは、水平スケーリングシナリオでの「最大容量」に対してのみトリガーされます。新しい状態は、フィルターおよびカスタムレポートページで確認でき、予期される状態と例外的な状態を区別しやすくなります。この機能強化により、不要なアラートを回避し、実際の問題に集中できるようになり、監視とトラブルシューティングが効率化されます。これは、Set-BrokerSite を使用して `UseVerticalScalingForRdsLaunches` を構成し、Studio で「最大セッション数」ポリシーを設定した場合に適用されます。

成功したセッション起動のマップビュー

Citrix Director のマップビューは、管理者に Citrix 環境全体での成功したセッション起動の包括的な地理的視覚化を提供します。この機能は、ユーザー接続をグローバル規模で視覚的にマッピングし、IT チームが地域ごとのパフォーマンスパターンを迅速に特定し、地理的な接続の問題をトラブルシューティングし、位置情報データに基づいてエンドユーザーエクスペリエンスを最適化するのに役立ちます。マップには、さまざまな地理的場所でのログオンパフォーマンスを示す色分けされた接続ポイントが表示されます。

Microsoft Teams 最適化 (Slimcore) の詳細を Mac 用 Citrix Workspace アプリに拡張

Microsoft Teams Slimcore 最適化の可視性を、Citrix Workspace アプリ (CWA) バージョン 2508 以降を実行している Mac エンドポイントに拡張しています。以前は Windows エンドポイントに限定されていましたが、Director を使用する管理者は、Mac ユーザー向けにこの最適化を表示および活用できるようになり、環境全体で一貫したパフォーマンスインサイトを確保できます。

> **注:**
>
> ページ上部の「すべてのワークロード」ボタンからアクセスできる従来の適正化分析は、今後のリリースで非推奨になります。

垂直および水平ロードバランシングアラートの処理の改善

以前は、`UseVerticalScalingForRdsLaunches` を true に設定し、Studio で「最大セッション数」ポリシーを構成すると、マシンは「最大容量」状態に移行しました。Director は、垂直または水平ロードバランシングのいずれによって制限に達したかに関わらず、「最大容量」のアラートをトリガーしていました。「最大負荷に達しました」などの特定のエラーが発生した場合、垂直ロードバランシングと水平ロードバランシングを区別する方法はありませんでした。これにより、垂直スケーリングシナリオにおける予期される動作に対して不要なアラートが発生し、時間の無駄と混乱を招いていました。

現在、垂直ロードバランシングがアクティブで、マシンがセッション制限に達すると、新しい状態である「垂直スケーリングの最大容量」に移行します。Director はこの新しい状態に対してアラートを生成しなくなりました。アラートは、水平スケーリングシナリオにおける「最大容量」に対してのみトリガーされます。新しい状態は「フィルター」および「カスタムレポート」ページで確認でき、予期される状態と例外的な状態を区別しやすくなります。この機能強化により、不要なアラートを回避し、実際の問題に集中できるようになり、監視とトラブルシューティングが効率化

されます。これは、Set-BrokerSite を使用して `UseVerticalScalingForRdsLaunches` を構成し、Studio で「最大セッション数」ポリシーを設定した場合に適用されます。

セッション起動成功のマップビュー

Citrix Directorのマップビューは、管理者にCitrix環境全体でのセッション起動の成功に関する包括的な地理的視覚化を提供します。この機能は、ユーザー接続をグローバル規模で視覚的にマッピングし、ITチームが地域のパフォーマンスパターンを迅速に特定し、地理的な接続の問題をトラブルシューティングし、位置データに基づいてエンドユーザーエクスペリエンスを最適化するのに役立ちます。マップには、さまざまな地理的場所でのログオンパフォーマンスを示す色分けされた接続ポイントが表示されます。

Microsoft Teams最適化（Slimcore）の詳細をCitrix Workspace App for Macに拡張

Microsoft Teams Slimcore最適化の可視性を、Citrix Workspace app (CWA) バージョン2508以降を実行しているMacエンドポイントに拡張しています。以前はWindowsエンドポイントに限定されていましたが、Directorを使用する管理者は、Macユーザー向けにこの最適化を表示および活用できるようになり、環境全体で一貫したパフォーマンスインサイトを確保できます。

> **注:**
>
> CWA Macのバージョンは2508以降である必要があります。

セッション障害のインサイト

以前は、セッション障害の原因を理解するのに課題がありました。ユーザーセッションが失敗した理由に関する詳細な診断インサイトが不足していました。この機能により、包括的なセッション障害診断インサイトが得られます。エラーパターンを検出し、主要な障害原因を迅速に特定できます。システムは、特定のデリバリーグループまたはマシンに影響を与える障害を強調表示します。また、ブロックされたユーザー接続の可視性も得られます。これにより、セッションの問題をより迅速にトラブルシューティングして解決する能力が向上します。この機能強化は、Monitor および Director サービスに適用されます。

切断されたセッションおよび終了したセッションでセッショントポロジが利用可能に

Citrix Director のセッショントポロジビューは、切断されたセッションおよび終了したセッションをサポートするようになり、包括的なセッション後分析のために最後に認識された状態のトポロジを表示します。

コスト削減に期間延長とカスタム日付範囲が追加されました

パワーマネージドマシンのコスト削減データを、以前の 45 日間の制限から 90 日間表示できるようになりました。また、カスタム日付ピッカーも追加され、管理者は特定の拡張された期間にわたる削減をスキャンおよび分析するためのより多くの制御と柔軟性を得られます。

セッション起動の失敗によってブロックされたユーザーを表示

管理者は、**セッション起動の失敗によってブロックされたユーザーを可視化**できるようになりました。この新しい概要は、**Connections**ビューの**Filters**内にあり、障害の優先順位付けと分析の改善を可能にします。

ユーザー全体のセッション再接続時間の可視化

セッション再接続時間機能は、Citrix Directorの既存のセッションログオン時間機能を拡張し、セッション再接続に関連するメトリックを含めます。この機能強化により、管理者は再接続パフォーマンスの傾向を可視化できるようになり、ユーザーエクスペリエンスのトラブルシューティングと最適化が向上します。

ユーザーセッション全体のユニファイドコミュニケーションアプリのメトリックを表示する機能

セッションビューに、ユーザーセッションのユニファイドコミュニケーション (UC) アプリケーションの使用状況に関する詳細な洞察を提供する新しい表示列がいくつか追加されました。これらの列は次のとおりです。**すべての UC アプリ名、UC アプリ名、UC アプリ最適化状態、UC アプリプラグインマネージャー名、UC アプリプラグインマネージャーバージョン、UC アプリプラグインインストール済み、UC アプリプラグインバージョン、UC アプリバージョン、UC アプリプラグインマネージャー、UC アプリ仮想チャネル状態、UC アプリ仮想チャネル許可リスト**。これらの属性は、「列の選択」オプションを使用して、メインのセッションテーブルビューに表示するように選択できます。詳細については、「ユニファイドコミュニケーションアプリのメトリック」を参照してください。

トレンドにおけるデリバリーグループ選択の強化

トレンドタブのセッションおよびログオンパフォーマンスページで、デリバリーグループのドロップダウンが強化されました。これにより、次のことが可能になります。

- テキスト入力を使用してデリバリーグループ名を検索
- 包括的な分析のために最大15個のデリバリーグループを複数選択

この機能強化により、使いやすさが向上し、複数のデリバリーグループ間でより効率的な同時監視と比較が可能になります。

シングルセッションOS向けHDX画面共有によるリモートアシスタンス

Director は、ネイティブの HDX 画面共有テクノロジーを活用したリモートアシスタンスをサポートするようになりました。この機能は、IT 管理者やヘルプデスクチームがシングルセッション環境のエンドユーザーにリモートサポートを提供するための、安全で高性能な方法を提供し、既存のリモートアシスタンス方法を補完または置き換えるものです。

マシン作成サービス™ (MCS)

Amazon Workspaces Core Managed InstancesでのMCSマシンカタログ作成のサポート

MCSは、Amazon Workspaces Core Managed Instancesと統合され、顧客のAWSアカウントで永続的および非永続的なMCSマシンカタログをプロビジョニングできるようになりました。

この機能により、次のことが可能になります。

- Amazon WorkSpaces Core Managed Instancesへの(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/connections/connection-amazon-wsc.html)ホスト接続を作成できます。
- (/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/create-prepared-image-amazon-wsc.html)準備済みイメージを作成し、(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/create-catalog-amazon-wsc.html)その準備済みイメージとマシンプロファイルを使用して、永続または非永続MCSマシンカタログを作成します。
- (/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/create-prepared-image-amazon-wsc.html#share-prepared-images-across-availability-zones)同じまたは異なるAWSリージョン内の異なるアベイラビリティゾーン間で単一の準備済みイメージを共有します。現在、PowerShellコマンドのみを使用して、異なるAWSリージョン間で準備済みイメージを共有できます。

MCSでのVMware vVolsのサポート

vSphere環境でMCSとVMware vVolsを使用できるようになりました。以前は、vVols上にMCSカタログを作成するとPBMエラーが発生していました。この更新により、その問題が解決されます。この統合により、MCS仮想マシンのストレージをきめ細かく制御できます。詳細については、(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/connections/connection-vmware-virtualization-environments#storage-profile-vsan)「ストレージプロファイル（vSAN）」を参照してください。

AWS EC2 Spotインスタンスの使用のサポート

この機能を使用すると、マシンプロファイルワークフローを使用して、AWS仮想化環境でSpotインスタンス（永続的なリクエストのみ）のMCSマシンカタログを作成できます。

オンデマンドインスタンスと比較して、Spotインスタンスは最大90%のコスト削減を提供します。ただし、容量が利用できなくなった場合、SpotインスタンスはAmazon EC2によって中断される可能性があり、そのため、重要でないアプリケーションやデスクトップにのみ適しています。

さらに、この機能を使用すると、SpotインスタンスをバックアップSKUとして使用できます。

詳細については、(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create/create-machine-catalog-aws#create-a-catalog-using-aws-spot-instance)「AWS Spotインスタンスを使用してカタログを作成する」を参照してください。

すべてのオンプレミスハイパーバイザーでのAzure Arcオンボーディングのサポート

Azure Arcを使用すると、組織はどこにホストされているVMなどのリソースを、Azureで実行されているかのように管理できます。Azure Arcを使用すると、Azure MonitorなどのAzureサービスを利用して、リソースの包括的な可視性とプロアクティブな管理を実現できます。

この機能を使用すると、PowerShellコマンドを使用してMCSマシンカタログのAzure Arcオンボーディングを有効にできます。オンボーディング後、VMはAzureポータルから管理でき、電源管理、拡張機能の追加または削除、ポリシーの割り当て、組み込みのAzureポリシーによるArc対応VMでのAzure Monitorの有効化などの操作を実行できます。

現在、この機能は、Citrixのすべてのオンプレミスハイパーバイザー（VMware、Nutanix、SCVMM）に適用されます。

詳しくは、(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create#onboard-vms-to-azure-arc)を参照してください。

Azureでのデータディスクプロビジョニングのサポート

AzureのMCSマシンカタログで、MCSによって作成された永続的または非永続的なVMに、永続的なデータディスクを作成して割り当てることができるようになりました。データディスクは、イベントログ、セキュリティトレース、アプリケーションデータなどの永続的なデータを保存するために使用されます。

データディスクはマスターイメージからプロビジョニングする必要があります。ストレージタイプ、暗号化設定、ゾーンなどのプロパティは、カスタムプロパティで指定されていない場合、カスタムプロパティまたはOSディスクテンプレートから派生します。データディスクを使用してMCSマシンカタログを作成する方法については、データディスクのプロビジョニングを参照してください。

MCSは一意のマシンGUIDを維持します

VDAバージョン2511以降のMCSプロビジョニング済みWindows VMは、再起動やイメージ更新後も一意の`MachineGuid`を維持するようになりました。この機能強化により、複数のVMが同じ`MachineGuid`を共有し、ライセンスやアプリケーション登録に影響を与える問題が解決されます。

ホスティング接続にWinHttp (netsh) プロキシサーバー設定を使用する

この機能により、ホスティング接続でDDCに構成されたWinHttp (netsh) プロキシサーバー設定を使用できるようになります。詳細については、ホスティング接続にWinHttp (netsh) プロキシサーバー設定を使用するを参照してください。

Azure: 休止状態のVMに対するクロスファミリーバックアップVMサイズのサポート

Azure上のMCSは、休止状態が有効なマシンカタログのバックアップ構成でクロスファミリーVMサイズを使用できるようになり、回復性が向上しました。この機能により、再開時のブルースクリーンエラーを防ぐためにクロスファミリーフォールバックをブロックしていた以前の制限がなくなります。休止状態のVMを再開中に割り当てエラーが発生した場合、MCSは自動的にサイズ変更を処理し、引き続き動作するVMを確保します。VMサイズを切り替えるには、休止状態をクリアする必要があり、その結果、VMのメモリ状態（RAMデータ）が失われることに注意してください。この機能は、永続的および非永続的なMCSカタログの両方で利用可能です。詳細については、バックアップVMサイズの構成を参照してください。

Azure: MCSカタログのクローン作成

Azure仮想化環境で、既存の永続的および非永続的なMCSマシンカタログをクローンするために、`Copy-ProvScheme` PowerShellコマンドを使用できるようになりました。この機能は、関連する構成、ネットワークマッピング、セキュリティグループなど、既存のスキームの詳細をコピーして新しいプロビジョニングスキームを作成します。これにより、次のことが可能になります。

- 既存の単一カタログを複数のカタログに分割し、異なるカタログレベルのポリシーと構成を適用する。
- 大規模なカタログ内の特定の仮想マシンを分離して、迅速なテストを行ったり、機能ロールに基づいて個別に扱ったりする。

詳細については、MCSカタログのクローン作成を参照してください。

オートスケール™

インテリジェント Autoscale

インテリジェント Autoscale は、最小限の管理設定で Delivery Group のパフォーマンスターゲットを設定できるデータ駆動型の Autoscale 機能です。パフォーマンスターゲット値は 1 から 99 の範囲で、その値はユーザーエクスペリエンスとコストの間の目標バランスを指定します。

- 低い値はコスト削減を優先します。
- 高い値はユーザーエクスペリエンスを優先します。

パフォーマンスターゲットは、過去の使用状況データと組み合わされて、1 日の 30 分ごとのブロックに対して最適なバッファ容量 (電源をオンにする VM の数) を計算します。したがって、毎日開始時に 48 の最適なバッファ容量が計算されます。

最適なバッファ容量は、利用可能なマシンを管理するために、ピーク時/オフピーク時のバッファ容量とプールサイズを置き換えます。

詳細については、「Intelligent Autoscale スケジュールプラグイン」(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/autoscale/autoscale-plugin#intelligent-autoscale-schedules-plug-in)を参照してください。

Autoscale ホリデープラグイン

この機能を使用すると、VMの電源管理に関連する標準のAutoscale設定から逸脱し、指定された祝日にVMの電源をオフにすることができます。たとえば、平日にはほとんどのVMの電源をオンにしたい場合でも、デフォルトでは祝日には平日のスケジュールが適用されます。このようなシナ

リオを管理するには、Autoscale ホリデープラグインを使用して、指定された祝日にVMの電源をオフにします。詳細については、「Autoscale ホリデープラグイン」(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/autoscale/autoscale-plugin#autoscale-holiday-plug-in)を参照してください。

マシンのドレイン状態と理由を特定する

`Get-BrokerMachineV2` PowerShell コマンドレットは、2つの新しいプロパティを提供するようになりました。`IsDraining`はマシンがドレイン中であるかどうかを確認し、`DrainingReason`は正確な原因を指定します。これにより、マシンの可用性を効果的にトラブルシューティングおよび管理できます。ゲストOSのドレイン理由は、マルチセッションマシンにのみ適用されます。

例: マルチセッションマシン VDA-01 が新しいユーザーセッションを受け入れていないことに気づきました。ドレイン状態にあると疑っています。`Get-BrokerMachineV2 -MachineName "VDA-01" | Select-Object Name, IsDraining, DrainingReason` を実行します。出力には、`IsDraining` が `True`、`DrainingReason` が `AutoscaleScaleDown` と表示されます。これにより、Autoscale がシャットダウンのためにドレイン状態を開始したことが確認されます。マシンの状態をすぐに理解できます。

詳細については、「ドレイン状態」(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/autoscale/get-started#drain-state)を参照してください。

ドレイン中のマシンをAutoscaleの計算から除外する

再起動スケジュールによるドレイン中のマシンをAutoscaleの容量計算から除外できるようになりました。これにより、過剰なプロビジョニングが防止され、リソース使用率の最適化に役立ちます。この動作を有効にするには、マルチセッションデリバリーグループで `ExcludeNaturalRebootDrainingFromAutoscale` プロパティを `True` に設定します。

この機能は以下にのみ適用されます。

- マルチセッションOSデリバリーグループ。
- クラウド向けの**Graceful restart**またはオンプレミス展開向けの**Re-start all machines after draining session**で構成された再起動スケジュール。

例えば、10個のアクティブセッションを持つデリバリーグループを考えます。2台のマシンがスケジュールされた再起動のためにドレイン中です。以前は、Autoscaleはこれら2台のドレイン中のマシンを利用可能と見なし、新しいマシンの過剰なプロビジョニングにつながる可能性がありました。この機能により、Autoscaleはドレイン中のマシンを認識して無視します。真に利用可能な容

量のみをカウントします。これにより、Autoscaleポリシーがリソースを正確にプロビジョニングし、不要なインフラストラクチャコストを防ぐことができます。

詳細については、「Autoscale計算からドレイン中のマシンを除外する」を参照してください。

Citrix Virtual Desktop Assistantアプリケーション

Citrix Virtual Desktop Assistantアプリケーションの機能強化

Citrix Virtual Desktop Assistantアプリケーションは、以下の新機能を持つように強化されました。

- ワークステーションVDA: アプリはデフォルトでインストールされるようになりました。リソース使用量を最小限に抑えるため、明示的に起動されない限り、CPUとメモリの使用状況を監視します。
- サーバーVDA: Citrix Virtual Apps and Desktops ISOでアプリが利用可能になり、簡単にインストールできます。
- 最適化タイル: メモリ解放の詳細を明確に表示するように再設計され、より良いリソースインサイトを提供します。
- キーボードページ: キーボード設定と同期ステータスを表示および管理します。
- USBページ: リアルタイムのUSBデバイスリダイレクトステータスを監視します。

詳細については、「Citrix Virtual Desktop Assistantアプリケーション」を参照してください。

アプリ保護

ポリシー改ざん検出のApp Protectionサポート

Citrix Virtual Apps and Desktopsバージョン2511以降、ポリシー改ざん検出機能はデフォルトで有効になっています。詳細については、ポリシー改ざん検出を参照してください。

> **注:**
>
> Citrix Virtual Apps and Desktopsバージョン2511以降、`Default.ica`ファイルを使用してApp Protectionを有効にすると、セッション起動は失敗します。代わりに、Web StudioまたはPowerShellを使用して、Delivery Controllerからデリバリーグループでポリシーを有効にしてください。キーロギング対策とスクリーンショット対策の構成を参照してください。

プレビュー機能

NVIDIAクライアントGPU向けHDXグラフィック超解像度

HDXグラフィックススーパーレゾリューションは、NVIDIA製の互換性のあるクライアントGPUもサポートするようになりました。

マージグループを使用したカナリアデプロイの有効化

アプリケーションおよびデスクトップリソースのカナリアデプロイモデルを実装するために、マージグループを使用できるようになりました。この機能により、同じリソースの複数のバージョンを公開しながら、エンドユーザーには単一のアイコンとして表示できます。

マージグループを使用すると、特定のユーザーグループを同じリソースの異なる実装バージョンに誘導できます。ユーザーの一部（例えば5%）を新しいバージョンのテストに割り当て、残りのユーザーは安定版を使用させることができます。新しいバージョンで問題が発生した場合でも、ユーザーエクスペリエンスを中断することなく、安定版に簡単にフェイルオーバーできます。この機能は、再列挙や構成変更を必要とせずに、高可用性と災害復旧の両方のシナリオをサポートします。

詳しくは、マージグループを使用したカナリアデプロイの有効化を参照してください。

プロファイル管理

新機能については、独自のドキュメントにある新機能の記事を参照してください。

リナックス ブイディーエー

新機能については、独自のドキュメントにある新機能の記事を参照してください。

セッション録画

新機能については、独自のドキュメントにある「新機能」(/ja-jp/session-recording/current-release/whats-new)の記事を参照してください。

シトリックス プロビジョニング™

新機能については、独自のドキュメントにある「新機能」(/ja-jp/provisioning/current-release/whats-new.html)の記事を参照してください。

macOS 用 シトリックス バーチャル デリバリー エージェント

新機能については、独自のドキュメントにある「新機能」(/ja-jp/mac-vda/whats-new.html)の記事を参照してください。

ワークスペース環境管理™

新機能については、独自のドキュメントにある「新機能」(/ja-jp/workspace-environment-management/current-release/whats-new)の記事を参照してください。

フェデレーション認証サービス

新機能については、独自のドキュメントにある「新機能」(/ja-jp/federated-authentication-service/current-release/whats-new.html)の記事を参照してください。

修正された問題

Citrix Virtual Apps and Desktops™ 7 2511 には、以下の修正された問題が含まれています。

> **注：**
>
> Citrix Virtual Apps™ and Desktops の以前のバージョンにおける問題の修正は、本リリースおよび以降のリリースに含まれています。

全般

- uberAgent® サービスが VDA とは独立して (VDA MetaInstaller を介さずに) インストールされている場合、VDA のアンインストール時に uberAgent サービスをアンインストールしてはなりません。
- App-Vでパッケージ化されたアプリケーションを公開すると、ユーザーがアプリケーションを移動またはサイズ変更できない場合があります。回避策として、次のレジストリ値を設定します: `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI\SeamlessSwclFlags(DWORD) = 2`。このキーは、この特定の問題を回避するためにのみ使用する必要があり、ウィンドウのサイズ変更や移動に関するユーザーエクスペリエンスを低下させる可能性があります。

- NAPS2バージョン8.xで新しいプロファイルが作成され、フィーダーベースのスキャンがすぐに開始されると、アプリケーションがクラッシュする可能性があります。この問題は、NAPS2バージョン8.1.4で特に観察されています。
- Unicode 入力モードが有効な状態で Citrix Workspace アプリを使用して VDA にアクセスし、「Unicode キーボードレイアウトマッピング」または「自動キーボード表示」のグループポリシーがオンになっている場合、大きなページをスクロールする際に Microsoft Excel のパフォーマンスが低下する可能性があります。この問題は、UIAutomation API が Excel と互換性がないために発生します。

HDX

マルチメディア

- ブラウザコンテンツリダイレクトのオーバーレイがアクティブな場合、それが誤って最上位ウィンドウのままになり、Windows タスクバーで他のアプリケーションのプレビューにカーソルを合わせても、それらが前面に表示されないことがあります。
- Webサイトが VDA 上でレンダリングされる (フォールバックモード) クライアントから、ブラウザコンテンツリダイレクトを完全にサポートするクライアントにアクティブなセッションをローミングすると、そのWebサイトの既存のブラウザタブがコンテンツを表示できなくなる場合があります。
- HTML5ビデオのリダイレクトにおいて、ユーザーが音量スライダーを調整して音声再生が再開された後でも、プレーヤーの音量アイコンがミュート状態から更新されない視覚的なバグを解決しました。
- セッション中にユーザーが画面ペインから画面またはプログラムを選択したときに、ctxoverlay.exe がクラッシュする問題を解決しました。

プロファイル管理

- Profile Management 2511 documentationは、このリリースでの更新に関する具体的な情報を提供します。

リナックス ブイディーエー

- Linux VDA 2511 documentationは、このリリースでの更新に関する具体的な情報を提供します。

セッションレコーディング

- Session Recording 2511 documentationは、このリリースでの更新に関する具体的な情報を提供します。

ワークスペース環境管理™

- Workspace Environment Management 2511 documentationは、このリリースでの更新に関する具体的な情報を提供します。

Citrix プロビジョニング™

- Citrix Provisioning 2511 documentationは、このリリースでの更新に関する具体的な情報を提供します。

フェデレーション認証サービス

- Federated Authentication Service 2511 documentationは、このリリースでの更新に関する具体的な情報を提供します。

既知の問題

Citrix Virtual Apps and Desktops™ 7 2511 には、以下の既知の問題が含まれています。

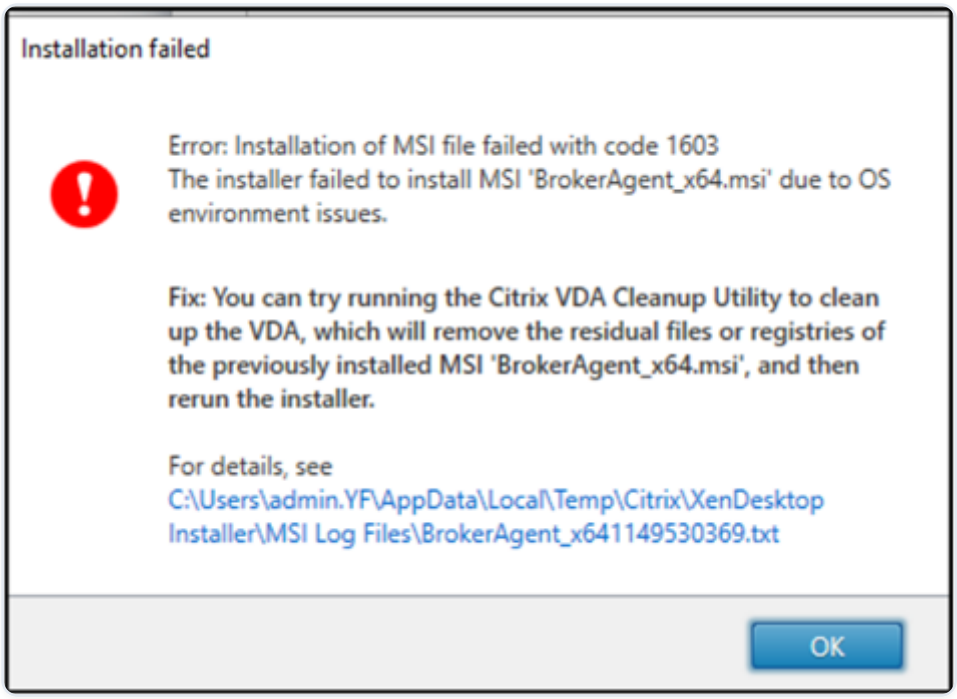
注

- 既知の問題に回避策がある場合は、問題の説明の後に記載されています。
- レジストリエントリの変更を推奨する回避策には、以下の警告が適用されます。

> **警告:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix® は、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターの使用は、お客様ご自身の責任において行ってください。編集する前に、必ずレジストリをバックアップしてください。

全般

- Windows 10 (22H2) および Windows Server 2022 プラットフォームでの Citrix VDA インストール中に、以下のエラーが発生する場合があります。



また、ブローカーエージェントの msi ログに、次のエラーメッセージが表示される場合があります。

```
MSI (s) (04:D8) [09:46:08:426]: Note: 1: 1722 2: CA_RunInstallAgent 3:
C:\Program Files\Citrix\Virtual Desktop Agent\BrokerAgent.exe 4:
-install

CustomAction CA_RunInstallAgent returned actual error code 1701 (note
this may not be 100% accurate if translation happened inside sandbox)

MSI (s) (04:D8) [09:46:08:427]: Product: Citrix Virtual Desktop Agent -
x64 -- Error 1722. There is a problem with this Windows Installer
package. A program run as part of the setup did not finish as expected.
Contact your support personnel or package vendor. Action
CA_RunInstallAgent, location: C:\Program Files\Citrix\Virtual Desktop
Agent\BrokerAgent.exe, command: -install
```

この問題を解決するには、インストーラーを閉じ、Windows パフォーマンスカウンターを再構築し、マシンを再起動してから、再度インストールを実行してください。詳細については、Microsoft ドキュメント Manually rebuild performance counters for Windows Server 2008 64 bit or Windows Server 2008 R2 systems を参照してください。

- アプリバーを起動してから、Windows 用 Citrix Workspace™ アプリで接続センターメニューを開くと、アプリバーがホストサーバーの下に表示されません。

- Windows Server 2022、Windows 10 Enterprise マルチセッション、および Windows 11 Enterprise マルチセッションを実行しているセッションホストでは、マルチセッション VDA の **セッション制限** 設定が拒否されます。
- Microsoft は、モダン印刷ダイアログを使用する際に印刷ジョブ間で印刷設定が保持されない問題があることを確認しており、現在対応中です。現在の見込みでは、2025年前半に解決される予定です。モダン印刷ダイアログは、Windows 11 や Windows Server 2025 などの新しい OS バージョンでデフォルトで有効になっています。OS をレガシー印刷ダイアログを使用するように構成するには、次の操作を行います。

  a. レジストリエディターを開きます。
  b. `HKEY_CURRENT_USER\Software\Microsoft\Print\UnifiedPrintDialog` に移動します。
  c. 右クリックして、**新規 > DWORD (32 ビット) 値** を選択します。
  d. 値の名前を **PreferLegacyPrintDialog** に変更します。
  e. **PreferLegacyPrintDialog** を右クリックして、**修正** を選択します。
  f. 値のデータを `1` に設定し、**OK** をクリックします。

- Citrix Virtual Apps and Desktopsセッション中に、オーディオ再生をサポートするクライアントモニターの電源を入れ直すと（オフにしてからオンにする）、VDAのサウンドコントロールパネル（mmsys.cpl）内のモニターのオーディオ再生デバイスの名前が、正しい特定の名前から「Citrix HDX Audio」に変わります。これは断続的な問題です。回避策として、VDAのサウンドコントロールパネル（mmsys.cpl）ウィンドウを閉じてから再起動します。
- Windows Server 2019 Virtual Delivery Agent (VDA)で公開されている特定のアプリケーション内から新しいプリンターを追加しようとすると、プリンターが一覧表示または追加されないエラーが発生します。具体的には、`rundll32.exe`にアクセスできないことを示すエラーメッセージが表示されます。

  回避策として、アプリケーションにすでに表示されているプリンターを使用するか、現在のセッションで利用できるようにプリンターを追加します。
- セッションがアクティブなときにクライアントマシンでデバイス名が変更されても、新しい名前はセッション設定にすぐに反映されません。この動作は、再生デバイスと録音デバイスの両方に影響します。

  回避策として、更新されたデバイス名を表示するには、セッションから切断してから再接続する必要があります。または、セッションからログアウトして再度ログインすることでも、この問題は解決されます。

- Browser Content Redirection (BCR) 用に構成されたタブを含む複数のChromeブラウザタブが、あるChromeウィンドウから別のChromeウィンドウに同時にドラッグアンドドロップされると、リダイレクトされたコンテンツが予期しない動作を示す可能性があります。
- ビデオコンテンツを含むタブを新しいウィンドウに移動すると、再生が停止したり、ビデオが表示されなくなったりする場合があります。
- Browser Profile SharingでBrowser Content redirectionを使用する場合、複数のプロファイルでのSSO永続性はサポートされていません。
- Windows 11には、デスクトップ上でウィンドウをスナップする新しいUI機能があります。ユーザーがウィンドウをドラッグしている間、デスクトップ上部に特別なツールバーが表示されます。そのため、マルチメディアオーバーレイのクリッピングロジックが、この機能のために導入された新しい見えない/透明なウィンドウが原因で、上部または中央の領域を切り取ってしまいます。

  回避策については、以下を参照してください。

  - ウィンドウをスナップするセクション。
  - 「ウィンドウをスナップする」機能を無効にする方法

- **Citrix VDAが既にインストールされているマシンでインプレースWindowsアップグレード後に印刷が失敗する可能性がある** インプレースWindowsアップグレード後、Citrix印刷プロバイダーが呼び出されなくなり、印刷エラーが発生する可能性があります。この問題は、Windowsアップグレードプロセスが印刷プロバイダーの実行順序をリセットし、Citrixに登録されたプロバイダーを保持しないために発生します。Microsoftは、これがWindowsの動作であり、アップグレード中に実行順序のプロバイダー登録を現在保持しないことを確認しています。

回避策は、適切なレジストリの場所にプリントプロバイダーを再度追加することです。

```
1.  Open the Registry Editor.

1.  Go to `HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Print\Providers`

1.  Right-click **order** and select **Modify**.

1.  Add the values `Universal Printer` and `Client Printer` above any
other providers.

1.  Reboot the VDA.
```

オーディオ

- ヘッドセットなどのオーディオデバイスが、USBリダイレクトを使用してWindows Server Virtual Delivery Agent (VDA) (例: Windows Server 2019または2022) に汎用的にリダイレクトされ、同じVDA上で複数のユーザーセッションが同時にアクティブになっている場合、タスクバーの右下隅にある音量アイコンをクリックして設定を調整すると、Windows `ShellExperienceHost.exe` プロセスが予期せずクラッシュする可能性があります。この問題は主に、オーディオデバイスがアクティブにリダイレクトされていないセッションで発生しますが、同じVDA上の別のセッションが汎用USBオーディオリダイレクトを使用している場合に発生します。

  回避策として、タスクマネージャーを介して、影響を受けるセッションで Windows Explorer プロセス (explorer.exe) を再起動します。これにより、ボリュームアイコンがクラッシュせずに機能するようになる可能性があります。

マシン クリエーション サービス™

- Accelerated Networkingが有効になっている複数のネットワークインターフェイス (NIC) を持つマシンプロファイルを使用する場合、選択したVMサイズがすべてのNICでAccelerated Networkingをサポートしていることを確認してください。一部のAzure VMサイズ (例: Standard_D2ads_v5) は、Accelerated Networkingを単一のNICに制限します。マシンプロファイルがVMサイズで許可されているよりも多くのNICでAccelerated Networkingを有効にしている場合、マシンはエラー `VmSizeRestrictedToSingleNicWithAcceleratedNetworkingEnable` で起動に失敗します。これを解決するには、複数のNICでAccelerated Networkingをサポートするサイズを選択するか、マシンプロファイルを更新して1つのNICでのみAccelerated Networkingを有効にします。
- Azure Connected Machineエージェントバージョン1.61以降がインストールされ、オンボードされたAzureローカルVMを使用してマスターイメージを準備する場合、エージェント構成ファイルの削除時にアクセス拒否のため、MCSでのカタログ作成がイメージ準備プロセスで失敗します。回避策として、マスターイメージの作成中に次の手順を実行します。`C:\ProgramData\AzureConnectedMachineAgent\Config\agentconfig.json` に移動し、ファイルを右クリックして を選択し、 属性のチェックボックスをオフにします。
- Nutanix AHV Prism Centralホスト接続を使用してMCSカタログに大量のVMを追加すると、`OutOfMemory` エラーで失敗する可能性があります。これを回避するには、単一バッチで作成するVMの数を減らしてください。一度に追加するVMは最大10台にすることをお勧めします。

- 既存のVDAをバージョン2511にアップグレードした後、`MachineGuid` はマシン固有のユニークな値に変更されます。ライセンスのために `MachineGuid` に依存するソフトウェアは、再登録が必要になる場合があります。
- VDAバージョン2511のTLS暗号化は、環境がマスターイメージから継承されたワイルドカード証明書に依存している場合、機能しなくなります。

  シングルセッションマシンに対する回避策として、代わりにマシンごとの証明書を使用できます。詳細については、VDAでのTLS/DTLSの有効化 を参照してください。
- `InstanceType` を使用して作成された VM は、Red Hat OpenShift 環境ではマスターイメージとしてサポートされていません。
- Red Hat OpenShift 仮想化環境で MCS マシンカタログを作成する場合、異なるオペレーティングシステムタイプを持つマスターイメージとマシンプロファイルを使用することはできません。これは、Red Hat OpenShift が各 OS タイプを管理する方法によるものです。したがって、Windows VM をマスターイメージとして使用し、非 Windows (例: Linux) VM をマシンプロファイルとして使用すること、またはその逆はサポートされていません。
- Red Hat OpenShift環境で、マスターイメージがドメインに参加している場合、カタログ作成に使用された後にドメイン信頼を失う可能性があります。この問題は、OpenShift環境の制限により、Citrix Virtual Apps™ and Desktops 2503以降のバージョンに影響します。回避策は、マスターイメージでドメインに参加しないことです。CitrixはRed Hatと協力して、ネットワーク分離機能を強化しています。
- AWSでホストされているVMware環境では、マスターイメージでvTPMが有効になっている場合、MCSマシンカタログの作成が失敗します。この問題は、すべてのCitrix Virtual Apps and Desktopsバージョンに影響し、VMware環境の問題が原因です。サポートについては、VMwareサポートにお問い合わせください。

ウェブスタジオ

- Web Studioを2511より*前の*バージョンから2511にアップグレードした後、以前のバージョンがデフォルトの `C:\Program Files\Citrix` ではなく*非デフォルト*のディレクトリにインストールされていた場合、Web Studioが開かなくなります。

  回避策として、`StudioConfig.exe` を使用してWeb Studioマニフェストファイル内のDelivery Controllerアドレスを手動で構成します。
- Web StudioからVDAのヘルスチェックを実行すると、ログオン期間チェックのレポートに次の警告が表示されます。



プロファイル管理

- Profile Management 2511 documentation には、このリリースでの更新に関する具体的な情報が記載されています。

macOS 用 シトリックス Virtual Delivery Agent

- Citrix Virtual Delivery Agent for macOS 2511 ドキュメント

リナックス ブイディーエー

- Linux VDA 2511 documentation には、このリリースでの更新に関する具体的な情報が記載されています。

セッションレコーディング

- Session Recording 2511 documentation には、このリリースでの更新に関する具体的な情報が記載されています。

ワークスペース環境管理™

- Workspace Environment Management 2511 documentation には、このリリースでの更新に関する具体的な情報が記載されています。

シトリックス プロビジョニング™

- Citrix Provisioning 2511 documentation には、このリリースでの更新に関する具体的な情報が記載されています。

フェデレーション認証サービス

- Federated Authentication Service 2511 documentation には、このリリースでの更新に関する具体的な情報が記載されています。

廃止予定

この記事のお知らせは、段階的に廃止されるプラットフォーム、Citrix製品、および機能について事前にお知らせし、お客様がタイムリーなビジネス上の意思決定を行えるようにすることを目的としています。Citrixは、お客様の使用状況とフィードバックを監視し、それらがいつ廃止されるかを決定します。お知らせは、その後のリリースで変更される可能性があり、すべての非推奨の機能や機能が含まれているとは限りません。製品ライフサイクルサポートの詳細については、製品ライフサイクルサポートポリシーの記事を参照してください。Long Term Service Release (LTSR) サービスオプションについては、`<https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX205549>` を参照してください。

非推奨と削除

次の表は、非推奨または削除されたプラットフォーム、Citrix®製品、および機能を示しています。**太字**の日付は、このリリースでの変更を示します。

非推奨

非推奨とは、将来のリリースからその機能または機能を削除する予定であることを意味します。その機能または機能は、正式に削除されるまで引き続き動作し、完全にサポートされます。この非推奨通知は、数ヶ月から数年にわたる場合があります。削除後、その機能または機能は動作しなくなります。この通知は、機能または機能が削除される前に、お客様がコードを計画し更新するための十分な時間を与えるためのものです。非推奨の項目については、可能な限り代替案が提案されます。

項目	非推奨が発表されたバージョン	代替
UDP経由のオーディオのサポート (UDP経由のオーディオリアルタイムトランスポートおよびオーディオUDPポート範囲)	2511	アダプティブオーディオをオーディオ用EDT損失許容モードとともに使用します。以下の最小バージョンが必要です。

項目	非推奨が発表されたバージョン	代替	
		仮想デリバリーエージェント • ウィンドウズ 2308 • リナックス 2411 • Mac 2411 Citrix Workspace アプリ	
		該当なし - Windows 2309 • リナックス 2402 • Mac 2402	
オーディオ品質設定(およびレガシーオーディオコーデックのサポート)	2511	適応型オーディオを使用します。以下の最小バージョンが必要です。 バーチャル デリバリー エージェント • ウィンドウズ 2109 • リナックス 2112 • Mac 2411	

項目	非推奨が発表されたバージョン	代替
		Citrix Workspace アプリ • ウィンドウズ 2109 • リナックス 2109 • Mac 2109
ローカルアプリアクセス (LAA)	2511	LAAに直接の代替手段はありません。お客様は、代わりにエンドポイントからVDAにローカルにインストールされたアプリケーションをインストールすることをお勧めします。LAAは、2402 LTSRまたは2507 LTSRで、そのメンテナンスが終了するまでサポートされます。この非推奨化に伴い、Microsoft Internet ExplorerおよびFirefox用のLocal App Access拡張機能も非推奨となります。
HTML5マルチメディアリダイレクト	2511	ブラウザコンテンツリダイレクト
ファイルベースのライセンス	2507	ライセンスアクティベーションサービス (LAS) は、Citrix製品スイート全体の製品アクティベーション

項目	非推奨が発表されたバージョン	代替
		のための次世代テクノロジーです。ファイルベースのライセンスを使用しているお客様は、互換性のあるリリースにアップグレードし、このテクノロジー移行を April 15, 2026 までに行う必要があります。April 15, 2026 以降、LASはCitrixオンプレミスコンポーネントをアクティベートおよびライセンス供与する唯一の方法となります。
`Get-BrokerMachine` のサポート	2507	`Get-BrokerMachineV2` を使用
「**ユニバーサル印刷最適化のデフォルト**」ポリシー設定の「画像圧縮」セクションにある「**ヘビーウェイト圧縮を有効にする**」オプションのサポート	2507	
「`Repair-AcctADAccount` PowerShellコマンド」のサポート	2503	次のコマンドを使用します • `Repair-AcctIdentity`: IDアカウントの現在の状態を変更せずに修復す

項目	非推奨が発表されたバージョン	代替
		るため。これにより、既存のプロビジョニング済みVMの既存の使用中IDアカウントを修復できます。たとえば、Microsoft Entraハイブリッド参加済みIDアカウントの `repair userCertificate` 属性。AD参加済みIDアカウントの `Repair identity info`（マシンパスワード/信頼キーペアを含む）。 • `Reset-AcctIdentity`: IDアカウントを初期状態にリセットするため（たとえば、汚染された状態から利用可能な状態へ）。これにより、汚染されたIDアカウントを利用可能なIDアカウントとしてプールに戻す

項目	非推奨が発表されたバージョン	代替
		ことができます。
3D HDXグラフィックポリシーの最適化	2411	圧縮にビデオコーデックを使用し、[画面全体]に設定します。`<https://docs.citrix.com/ja-jp/citrix-virtual-apps-desktops/2511/policies/reference/ica-policy-settings/graphics-policy-settings.html#use-video-codec-for-compression>`を参照してください
NVIDIA GPUハードウェアエンコーディング（NVENC）の要件：vGPU 15以前、およびドライバーバージョン529.19以前。	2411	現在サポートされているNVIDIAドライバー（vGPU 16以降、およびドライバーバージョン536.22以降）を使用してください。詳細については、NVIDIAがサポートするvGPUおよびドライバーのバージョンに関する`<https://docs.nvidia.com/vgpu/index.html#driver-versions>`を参照してください。

項目	非推奨が発表されたバージョン	代替	
以下の `-AcctADAccount` PowerShellコマンドのサポート • New-AcctADAccount • Add-AcctADAccount	2411	-AcctIdentity PowerShellコマンドを使用してください • New-AcctIdentity • Add-AcctIdentity	
該当なし - Update-AcctADAccount		廃止された項目 - Update-AcctIdentity	
• リムーブ-アカウントADアカウント		• リムーブ-アカウントアイデンティティ	
項目: Unlock-AcctADAccount • Get-AcctADAccount		項目: Unlock-AcctIdentity • Get-AcctIdentity	
`-ResetIdentityInfo` PowerShellコマンドのサポート	2411	`-Recreate` を使用してIDディスクを再作成します。詳細については、アクティブなコンピューターアカウントのID情報を修復するを参照してください。	
MMCベースのStudio	2411	MMCベースのStudioは2511で削除されました。代わりにWeb	

項目	非推奨が発表されたバージョン	代替
		Studioを使用してください。
複数モニターフック	2407	-
ドメインパススルー認証	2407	シングルサインオン用の拡張ドメインパススルーを使用してください。
ランデブー V1	2402	Rendezvous V2を使用してください。
セキュア ICA®	2402	(/ja-jp/citrix-virtual-apps-desktops/2511/hdx-transport/secure-hdx)を使用してください。
Windows Server 2016でのVDAサポート	2402	最新のWindows Serverバージョンにアップグレードしてください。
Windows Server 2016でのDelivery Controller™、Web Studio、Citrix Director、Citrix License Server、Citrix StoreFront、シングルセッションOS用Server VDI、マルチセッションOS用VDA、Active Directoryフォレストおよびドメイン、Universal Print Serverのサポート	2402	Windows Server の最新バージョンにアップグレードしてください。

項目	非推奨が発表されたバージョン	代替
サイト構成、構成ログ、および監視データベースに対する Microsoft SQL Server バージョン 2016 および 2017 のサポート	2402	Microsoft SQL Server の最新バージョンにアップグレードしてください。
オンデマンドプロビジョニング機能より前に作成された Azureカタログ（「レガシー」カタログ）のサポート	2402	Azure レガシーカタログVMを再作成します。カタログはオンデマンドでプロビジョニングされるため、ストレージコストを節約できます。
ターゲット最小フレームレートポリシー	2311	**グラフィックステータスインジケーター**を使用して、ターゲット最小フレームレートを変更します。
カタログが作成されたリージョンとは異なるリージョンでマスターイメージを使用するためのサポート	2311	Azure Compute Gallery を使用して、マスターイメージを目的のリージョンにレプリケートします。
HDX™ グラフィック表示メモリ制限設定	2311	クライアントの表示レイアウトが完全に収まるように、必要な最小限のメモリが割り当てられます。
HDX Graphicsにおけるプログレッシブモードのサポート	2311	Thinwireを使用します。「プログレッシブモード」を参照してください。(/ja-jp/

項目	非推奨が発表されたバージョン	代替
		citrix-virtual-apps-desktops/2511/policies/reference/hdx-registry-settings#progressive-mode).
Internet Explorer 11におけるブラウザコンテンツリダイレクトのサポート	2311	Google Chromeベースのブラウザコンテンツリダイレクトを使用します。
BrokerにおけるSQL Server 2016のサポート	2308	最新バージョンを使用します。詳しくは、「システム要件」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2511/system-requirements.html).
Directorにおける XenApp 5.xのサポート	2308	---
Directorにおける XenApp 6.xのサポート	2308	---
Director のアラート用 SCOM パック	2308	---
Director のプラグインのサポート	2308	---
WebRTC SDP 形式 (プラン B) のサポート	2308	Citrix Workspace™ アプリをサポートされているバージョン

項目	非推奨が発表されたバージョン	代替
		にアップグレードしてください。
Microsoft Teams Optimization のシングルウィンドウモードのサポート	2308	Citrix Workspace アプリをマルチウィンドウモードをサポートするバージョンにアップグレードしてください。詳細については、「機能マトリックスとバージョンサポート」を参照してください。
AWS 環境で使用される `AwsCaptureInstanceProperties` のサポート	2308	マシンプロファイルを使用します。「マシンプロファイルを使用してカタログを作成する」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create/create-machine-catalog-aws#create-a-catalog-using-a-machine-profile).
`Schedule-ProvVMUpdate` PowerShellコマンド	2305	`Set-ProvVMUpdateTimeWindow` を使用します。
`Request-ProvVMUpdate` PowerShellコマンド	2305	`-StartsNow` および `-DurationInMinutes -1` パラメーターを指定して `Set-`

項目	非推奨が発表されたバージョン	代替
		`ProvVMUpdateTimeWindow`を使用します。
`Cancel-ProvVMUpdate` PowerShellコマンド	2305	`Clear-ProvVMUpdateTimeWindow`を使用します。
`New-ProvScheme`コマンドで使用される`DedicatedTenancy`パラメーター	2303	`TenancyType`パラメーターを使用します。
ライセンスサーバーVPX	2206	---
Azure環境でVMをプロビジョニングするためのアンマネージドディスク。	2206	マネージドディスクを使用。
ホストからクライアントへの (URL) リダイレクト	2203	双方向コンテンツリダイレクト。
クラウドおよびオンプレミス環境で使用される4つのAWS固有のコマンド（`Revoke-HypSecurityGroupIngress`、`Revoke-HypSecurityGroupEgress`、`Grant-HypSecuritygroupegress`、`Grant-HypSecurityGroupI	2203	---

項目	非推奨が発表されたバージョン	代替
`ngress`）のサポート。		
VDAメタインストーラーからのCitrix Files for WindowsおよびCitrix Files for Outlook。	2203	スタンドアロンインストーラーを使用します。
VDAメタインストーラーからのWEM Agentコンポーネント。	2203	---
XenAppおよびXenDesktop、Provisioning Services、StoreFront用のCitrix SCOM Management Pack。監視可能な製品バージョンについては、Citrix SCOM Management Packs documentationを参照してください。	1912	展開の監視と管理にはDirectorを使用してください。SCOMのEOLと代替策の詳細については、https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX266943を参照してください。
モビリティSDK / モバイルSDK（旧Citrix Labsより）	7.16	モバイルエクスペリエンスポリシー設定、およびホスト型デスクトップ/アプリのネイティブエクスペリエンスに置き換えられました。

削除された機能

Citrix Virtual Apps and Desktopsでは、削除された項目は削除されるか、サポートされなくなります。

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
Remote PC Access用のSCCM統合型Wake on LANオプション。	2012	2511	スタンドアロンのWake on LAN機能(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/remote-pc-access.html#wake-on-lan)を使用します。
システムセンター コンフィギュレーションマネージャー用のシトリックスコネクタ 3.1 のサポート	2311	2507	イメージまたはアプリケーションの更新を手動で実行します。
AWSボリュームワーカーのサポートを削除しました	2311	2503	直接ディスクのアップロードとダウンロードを使用します。直接ディスクのアップロードとダウンロードを参照してください。
SQL Server 2016および2017のサポート	2402および2308	2411	SQL Server 2019および2022を使用します。
MCS I/Oライトバックキャッシュを、ディスクキャッシュのみを含み、メモ	2402	2411	ライトバックキャッシュを有効にしてマシンを作成する場合、**Memory**

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
リキャッシュを含まないように構成するサポート			**cache size (MB)** オプションを選択し、ゼロ以外のサイズを指定します。
Citrix StudioでのPVSインポートウィザードのサポート	1912 LTSR	2311	以下のいずれかの方法でCitrix Provisioning™マシンをプロビジョニングします • Citrix Provisioning Consoleを使用してマシンをプロビジョニングし、Citrix Provisioning Devices Export Wizardを使用してCitrix Virtual Apps and Desktopsにエクスポートします。Export Devices Wizardで詳

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
			細を確認してください。 • Web Studioを使用してCitrix Provisioningカタログを作成します。詳細については、Citrix StudioでCitrix Provisioningカタログを作成するを参照してください。
Windows向けCitrix Workspaceアプリ 1912	---	2402	最新バージョンを使用してください。
HDX Graphics FullScreen + テキスト最適化	2311	2311	
HDX 3D ProでのNVIDIA Frame Buffer Capture (NVFBC) のサポート	2308	2311	Desktop Duplication API (DDAPI) を使用してください。

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
ポリシー設定「インボックスプリンタードライバーの自動インストール」に対するVDAサポート。	7.16	2311	なし。ポリシー設定は、以前のOS (Windows 7、Windows Server 2012 R2以前) のVDAでのみサポートされています。
NVIDIA GPUハードウェアエンコーディング (NVENC) は以下で利用可能：vGPU 11以前、およびドライバーバージョン466.77以前。	2305	2305	現在サポートされているNVIDIAドライバーを使用してください：vGPU 13以降、バージョン471.41以降。
Citrixサポートツール (SupportabilityTool_x64 .msi) はVDAメタインストーラーから。	---	2212	---
Citrixライセンス管理コンソール (Windows License Server 11.16.3ビルド30000に最後に含まれ、Windows License Server v11.16.6ビルド31000で削除されました)。	2003	2006	Citrix Licensing Managerを使用してください。

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
Citrix Indirect Display Driver (IDD) グラフィックアダプターのサポートはWindows 10 バージョン 1709以前で。	2003	2003	Citrix Virtual Apps™ and Desktops 7 1912 LTSR VDAを使用します。
GRID 9以前のディスプレイドライバーを使用するNVIDIA GPU (NVENC) によるハードウェアエンコード。	2003	2003	Citrix Virtual Apps and Desktops 7 2003以降のVDAでGRID 10ディスプレイドライバーを使用するか、Citrix Virtual Apps and Desktops 7 1912 LTSR VDAを使用します。
セルフサービスパスワードリセット (SSPR) 機能。	2003	2006	---
VDAおよびコアサーバーコンポーネントにおけるMicrosoft .NET Frameworkバージョン4.8より前のバージョンのサポート。Delivery Controller、Studio、	1912	2003	.NET Frameworkバージョン4.8にアップグレードします。

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
Directorが含まれます。			
Windows Server 2012 R2環境で動作するVDA。	1912	2003	サポートされているオペレーティングシステムにVDAをインストールします。
Citrix Virtual Apps and Desktops Premiumエディションの AppDNA®アプリケーション移行コンポーネント。	1909	2003	---
32ビット (x86) マシンへのStudioのインストール。	1909	2003	サポートされているx64オペレーティングシステムにインストールします。
シームレスアプリケーションにおけるExcelフックのサポート。これは、各Microsoft Excel 2010ワークブックに対して個別のタスクバーアイコンを作成するために使用されていました。	1909	1909	---

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
Windows Server 2012 R2 (サービスパックを含む) 上のコアサーバーコンポーネント。含まれるもの: Delivery Controller、Studio、Director。	1906	2003	より新しいサポート対象のオペレーティングシステムにインストールしてください。
Microsoft SQL Serverバージョン2008 R2、2012、2014 (すべてのサービスパックとエディションを含む) 上のサイト構成、構成ログ、および監視データベースのサポート。	1906	2003	サポートされているMicrosoft SQL Server バージョンにデータベースをインストールしてください。
x86プラットフォーム上のWindows 10におけるVDAのサポート。	1906	1909*	サポートされているx64オペレーティングシステムにVDAをインストールします。*この機能は、Citrix Virtual Apps and Desktops 7 1912 LTSRで引き続きサポートされています。
Citrix Virtual Apps and	1903	1906	---

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
Desktopsインストールメディアからの Citrix Smart Tools Agentの削除。			
Red Hat Enterprise Linux/CentOS 7.5 上での Linux VDA のサポート。	1903	1903	Red Hat Enterprise Linux の新しいバージョンに Linux VDA をインストールします。
Citrix Virtual Apps and Desktops (旧 XenApp and XenDesktop) と Citrix Receiver、および Workspace Hub 間の TLS 1.0 および TLS 1.1 プロトコルに対する StoreFront のサポート。	7.17	2203	Citrix Receiver を、TLS 1.2 プロトコルをサポートする Citrix Workspace アプリにアップグレードします。Citrix Workspace アプリの詳細については、https://docs.citrix.com/ja-jp/citrix-workspace-app を参照してください。
ポリシー設定「インボックスプリンタードライバーの自動インストール」に対する VDA のサポート。	7.16	2311	なし。このポリシー設定は、以前の OS (Windows 7、Windows Server 2012 R2 およびそれ以前) の VDA で

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
			のみサポートされます。
Framehawk ディスプレイリモートテクノロジーのサポート	1811	1903	adaptive transport を有効にした Thinwire を使用します。
すべてのCitrix Virtual Apps and Desktops (およびXenApp and XenDesktop) バージョンにおけるCitrix Smart Scaleのサポート。この機能は31 May 2019にサポート終了となります。	1808	1906	電力管理機能の向上のため、Citrix Cloud上のVirtual Apps and Desktops Service の使用を検討してください。
Citrix StoreFront、Citrix VDA、Citrix Studio、Citrix Director、およびCitrix Delivery Controllerによる Microsoft .NET Frameworkバージョン4.5.1、4.5.2、4.6、4.6.1、4.6.2、および4.7のサポート。	7.18	1808	.NET Frameworkバージョン4.7.1以降にアップグレードしてください。(インストーラーは、まだインストールされていない場合、.NET Framework 4.7.1を自動的にインストールします。)

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
Red Hat Enterprise Linux 7.3におけるLinux VDAのサポート。	7.18	1808	Red Hat Enterprise Linuxのより新しいバージョンにLinux VDAをインストールしてください。
SUSE Linux Enterprise Server 11 Service Pack 4におけるLinux VDAのサポート。	7.16	7.16	サポートされているSUSEバージョンにLinux VDAをインストールします。
VDAsでのCitrix WDDMドライバーのサポート	7.16	7.16	Citrix WDDMドライバーは、VDAsとともにインストールされなくなりました。
Windows 10バージョン1511（Threshold 2）およびそれ以前のWindowsシングルセッションOSリリース（Windows 8.xおよびWindows 7を含む）（`<https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-`	7.15 LTSR（および7.12）	7.16	Windows 10最小バージョン1607（Redstone 1）以降の半期チャネルにシングルセッションOS VDAをインストールします。1607 LTSBを使用している場合は、7.15 VDAをお勧めします。CTX224843を参照してください。

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
`windows-7-virtual-desktop-users/>`を参照）。			
Windows Server 2008 R2およびWindows Server 2012（Service Packを含む）上のVDA	7.15 LTSR（および7.12）	7.16	サポートされているオペレーティングシステムにVDAをインストールします。
デスクトップコンポジションリダイレクト（以前はDirectX Command Remotingとして知られていた） (DCR)	7.15 LTSR	7.16	Thinwireを使用してください。
Windows Server 2012およびWindows Server 2008 R2（Service Packを含む）上のコアコンポーネント。含まれるもの：Delivery Controller、Studio、Director、StoreFront、License Server、Universal Print Server。	7.15 LTSR	7.18	サポートされているオペレーティングシステムにコンポーネントをインストールしてください。

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
Windows Server 2012およびWindows Server 2008 R2（Service Packを含む）でのセルフサービスパスワードリセット（SSPR）機能	7.15 LTSR	7.18	より新しいサポートされているオペレーティングシステムにインストールしてください。
Windows 7、Windows 8、およびWindows 8.1（Service Packを含む）でのStudio	7.15 LTSR	7.18	サポートされているオペレーティングシステムにStudioをインストールします。
Flashリダイレクト	7.15 LTSR	1912	ビデオコンテンツをHTML5ビデオとして作成します。管理対象コンテンツにはHTML5ビデオのリダイレクトを、公開Webサイトにはブラウザコンテンツのリダイレクトを使用します。詳細については、Flashリダイレクトのサポート終了の注記を参照してください。
StoreFrontとのCitrix Online統	7.14 (およびStoreFront 3.11)	StoreFront 3.12	---

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
合（Goto製品）			
VDAのインストール中に作成され、VDAマシンのローカル管理者グループに追加されていたユーザーアカウントCtxAppVCOMAdminは、作成されなくなりました。基盤となる「COM」メカニズムも削除されました。	7.14	7.14	Windowsサービス CtxAppVServiceは同じ機能を実行します。これは自動的にインストールおよび構成され、ユーザーによる操作は不要です。
Windows Server 2008 32ビットでのUniversal Print Server UpsServerコンポーネントのサポート	7.14	7.14	より新しいサポート対象のオペレーティングシステムにインストールする。
Internet Explorer 8 上のストアフロントおよびReceiver for Web	7.13	7.13	---
Citrix App-Vコンポーネントのインストールを防止するためのVDAコマンドラインインストー	7.13	7.13	コマンドラインインストールオプション/exclude "Citrix Personalization for App-V –

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
ルオプション / no_appv			VDA"を使用する。
フル製品インストーラーは、新規インストール時にCitrix.Common.Commandsスナップインをインストールしなくなり、既存のインストールをアップグレードする際に自動的に削除します。	7.13	7.13	Citrix.Common.Commandsスナップインによって提供されていた一部のPowerShellコマンドは、XenApp 6.5 SDKで引き続き利用可能です。
*-CtxIconコマンドレットによって提供されていたアイコンデータを操作する部分的な機能。	7.13	7.13	Broker Serviceの*-BrokerIcon cmdletsによって提供されるようになりました。
レガシーThinwireモード	7.12	7.16	Thinwireを使用してください。Windows Server 2008 R2でレガシーThinwireモードを使用している場合は、Windows Server 2012 R2またはWindows Server 2016に移行し、Thinwireを使用してください。

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
StoreFront 2.0、2.1、2.5、および2.5.2からのインプレースアップグレード	7.13	7.16	これらのバージョンのいずれかから、より新しいサポート対象バージョンにアップグレードし、その後XenApp and XenDesktop 7.16にアップグレードしてください。
XenDesktop 5.6または5.6 FP1からのインプレースアップグレード	7.12	7.16	XenDesktop 5.6または5.6 FP1の展開を現在のXenDesktopバージョンに移行してください。これを行うには、まずXenDesktop 7.6 LTSR（最新のCUを含む）にアップグレードし、次に最新のCitrix Virtual Desktops（旧XenDesktop）リリースまたはLTSRバージョンにアップグレードしてください。
32ビット (x86) マシンへのDelivery Controller、Director、	7.12	7.16	サポートされているx64オペレーティングシ

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
StoreFront、またはLicense Serverのインストール。			ステムにインストールします。
接続リース	7.12	7.16	ローカルホストキャッシュを使用します。
Windows XPで使用されるXenDesktop 5.6。Windows XPへのVDAインストールはサポートされていません。	7.12	7.16	サポートされているオペレーティングシステムにVDAをインストールします。
CloudPlatform接続のサポート	7.12	2003	別のサポートされているハイパーバイザーまたはクラウドサービスを使用してください。
Azure Classic (Azure Service Management とも呼ばれる) 接続のサポート	7.12	2003	Citrix Cloud の Virtual Apps and Desktops Service の使用を検討してください。
AppDisks 機能 (およびそれをサポートする Studio への AppDNA 統合)	7.13	2003	Citrix App Layering を使用してください。
Personal vDisk 機能	7.15	2006†	Citrix App Layering ユーザーレイヤー

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
			または ユーザーパーソナライゼーションレイヤー テクノロジーを使用してください。

† Citrix Virtual Apps and Desktops 7 2003 では、Personal vDisk ドライバーが VDA インストーラーから削除されました。Citrix Virtual Apps and Desktops 7 2006 では、Personal vDisk ドライバーのワークフローが Studio から削除されました。

システム要件

はじめに

このドキュメントのシステム要件は、この製品バージョンがリリースされた時点のものでした。更新は定期的に行われます。ここに記載されていないコンポーネント（ホストシステム、Citrix Workspace™ app、Citrix Provisioning™など）のシステム要件は、それぞれのドキュメントに記載されています。

インストールを開始する前に、インストールの準備を確認してください。

特に記載がない限り、コンポーネントインストーラーは、必要なバージョンがマシンで検出されない場合、ソフトウェアの前提条件（.NETおよびC++パッケージなど）を自動的に展開します。Citrix®インストールメディアには、これらの前提ソフトウェアの一部も含まれています。

インストールメディアにはいくつかのサードパーティコンポーネントが含まれています。Citrixソフトウェアを使用する前に、サードパーティからのセキュリティ更新プログラムを確認し、インストールしてください。

グローバリゼーションについては、Knowledge Centerの記事CTX119253を参照してください。

Windows Serverにインストールできるコンポーネントおよび機能の場合、特に記載がない限り、Nano Serverのインストールはサポートされていません。Server Coreは、Delivery ControllerおよびDirectorのみでサポートされています。

ハードウェア要件

RAMとディスク容量の値は、製品イメージ、オペレーティングシステム、およびマシン上のその他のソフトウェアの要件に追加されるものです。パフォーマンスは、構成によって異なります。構成には、使用する機能、ユーザー数、その他の要因が含まれます。最小要件のみを使用すると、パフォーマンスが低下する可能性があります。

次の表に、コアコンポーネントの最小要件を示します。

コンポーネント	最小
すべてのコアコンポーネントとStoreFront™を1台のサーバーにインストール（評価目的のみ、本番環境展開ではない）	5 GB RAM
すべてのコアコンポーネントとStoreFrontを1台のサーバーに、テスト展開または小規模な本番環境向けに	12 GB RAM
Delivery Controller™ (ローカルホストキャッシュにはより多くのディスク容量が必要です)	5 GB RAM、800 MB ハードディスク
スタジオ	1 GB RAM、100 MB ハードディスク
ディレクター	2 GB RAM、200 MB ハードディスク
StoreFront	2 GB RAM、ディスクの推奨事項については、StoreFrontのドキュメントを参照してください
ライセンスサーバー	8 GB RAM。ディスクの推奨事項については、ライセンスドキュメントを参照してください

デスクトップとアプリケーションを提供するVMのサイジング

ハードウェア製品の複雑で動的な性質、および各展開に固有のニーズがあるため、具体的な推奨事項は提供できません。一般的に、Citrix Virtual Apps™ VMのサイジングは、ユーザーのワークロードではなくハードウェアに基づいています。例外はRAMです。より多くのRAMを消費するアプリケーションには、より多くのRAMが必要です。

詳細については、以下を参照してください:

- Citrix Tech Zone にサイジングに関するガイダンスが含まれています。
- Citrix Virtual Apps and Desktops Single Server Scalability では、単一の物理ホストでサポートできるユーザー数またはVM数について説明しています。

マイクロソフト ビジュアル C++

Delivery Controller、Virtual Delivery Agent (VDA)、またはUniversal Print Serverをインストールすると、Citrixインストーラーは Microsoft Visual C++ 2015–2022 Redistributableを自動的にインストールします。

- マシンにそのランタイムの以前のバージョン（2015-2019など）が含まれている場合、Citrixインストーラーがそれをアップグレードします。
- マシンに2015年より前のバージョンが含まれている場合、Citrixは新しいバージョンを並行してインストールします。

デリバリーコントローラー

> **注:**

> **ライセンスサーバーのバージョン互換性:** ライセンスサーバーがバージョン11.17.2ビルド53100以降で実行されていることを確認してください。この前提条件を満たさない場合、Citrix Virtual Apps and Desktops (CVAD) サイトのアップグレードおよびサイト作成がブロックされます。

> サポートされているオペレーティングシステム:

- ウィンドウズサーバー 2025
- Windows Server Core 2022 (ウィンドウズ サーバー コア 2022)
- Windows Server 2022 (ウィンドウズ サーバー 2022)
- Windows Server 2019、StandardおよびDatacenter Edition、およびServer Coreオプション付き

要件:

- Microsoft .NET Framework 4.8（またはそれ以降のバージョン）がまだインストールされていない場合、自動的にインストールされます。
- Windows PowerShell 3.0、4.0、または5.0。
- Microsoft Visual C++ 2015–2022 再頒布可能パッケージ。
- Citrix Virtual Apps and Desktopsバージョン2407から2411以降にアップグレードする場合、またはバージョン2411以降を新規インストールする場合は、最初のステップとしてライセンスサーバーを最新バージョン（バージョン11.2.17ビルド53100以降）に更新してください。その後、Delivery Controllerをアップグレードします。これを怠ると、UIに警告メッセージが表示され、コマンドラインインストールが失敗します。

> **注:**

> Citrix Virtual Apps and Desktops™ Delivery Controllerは、読み取り専用ドメインコントローラー (RODC) をサポートしていません。

データベース

> **注:**

> バージョン2411以降、データベースにAzure SQL Managed Instanceを使用できます。

> サイト構成、構成ログ、および監視データベースでサポートされているMicrosoft SQL Serverのバージョン：

- SQL Server 2022、Express、Standard、およびEnterprise エディション。
  - 新規インストールの場合：既存のサポートされているSQL Serverインストールが検出されない場合、Controllerのインストール時に、累積更新プログラム14が適用されたSQL Server Express 2022がデフォルトでインストールされます。
- SQL Server 2019、Express、Standard、およびEnterprise エディション。

以下のデータベース高可用性ソリューションがサポートされています（SQL Server Expressはスタンドアロンモードのみをサポートします）：

- SQL Server AlwaysOn フェールオーバー クラスター インスタンス
- SQL Server AlwaysOn 可用性グループ (基本可用性グループを含む)
- SQL Server データベース ミラーリング

コントローラーとSQL Serverサイトデータベース間の接続には、Windows認証が必要です。

ローカルホストキャッシュに関する考慮事項: Microsoft SQL Server Express LocalDB は、ローカルホストキャッシュがスタンドアロンで使用する SQL Server Express の機能です。ローカルホストキャッシュは、SQL Server Express LocalDB 以外の SQL Server Express のコンポーネントを必要としません。

- コントローラーをインストールする際、ローカルホストキャッシュ機能で使用するために、累積更新プログラム15適用済みのMicrosoft SQL Server Express LocalDB 2022がインストールされます。(このインストールは、サイトデータベース用のデフォルトのSQL Server Expressインストールとは別です。)

- コントローラーをアップグレードする際、既存のMicrosoft SQL Server Express LocalDBのバージョンは自動的にアップグレードされません。交換要件と手順については、「SQL Server Express LocalDBの交換」を参照してください。

その他のデータベース情報:

- データベース
- CTX114501 には、現在サポートされているデータベースが一覧表示されています
- データベースのサイジングに関するガイダンス
- ローカルホストキャッシュ

ウェブスタジオ

> **注:**
>
> - Web Studioは、オンプレミスのCitrix Virtual Apps and Desktops展開を構成および管理できるWebベースの管理コンソールです。ユーザーエクスペリエンスの向上を目的として設計されており、Citrix Studioよりも一般的に応答が高速です。インストール手順については、「Web Studioのインストール」を参照してください。
> - バージョン2511以降、Web Studio（Webベース）はCitrix Virtual Apps and Desktopsの唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。

> Web Studioのインストールと使用に関するサポート対象のオペレーティングシステム、ブラウザ、表示設定、およびハードウェア要件については、Web Studioの記事のシステム要件を参照してください。

シトリックス ディレクター

サポートされているオペレーティングシステム:

- ウィンドウズ サーバー 2025
- ウィンドウズ サーバー コア 2022
- ウィンドウズ サーバー 2022

- Windows Server 2019、StandardおよびDatacenterエディション、およびServer Coreオプション

要件:

- Microsoft .NET Framework 4.8がインストールされていない場合（またはそれ以降のバージョンがインストールされていない場合）、自動的にインストールされます。
- Microsoft Internet Information Services (IIS) 7.0およびASP.NET 2.0。IISサーバーの役割に静的コンテンツの役割サービスがインストールされていることを確認してください。このソフトウェアがまだインストールされていない場合は、Windows Serverのインストールメディアを求められ、そのソフトウェアがインストールされます。
- Citrix Directorがインストールされているマシンでイベントログを表示するには、Microsoft .NET Framework 2.0をインストールする必要があります。

Citrix プロファイル管理:

- VDAにCitrix Profile ManagementおよびCitrix Profile Management WMI Plug-inがインストールされており（インストールウィザードの**追加コンポーネント**ページ）、Directorでユーザープロファイルの詳細を表示するためにCitrix Profile Management Serviceが実行されていることを確認してください。

システム センター オペレーションズ マネージャー (SCOM) 統合の要件:

- システムセンター 2012 R2 オペレーションズマネージャー

Directorの表示でサポートされているブラウザー:

- マイクロソフト エッジ。
- Firefox ESR (延長サポートリリース)。
- クローム。

Directorを表示するための推奨される最適な画面解像度は1440 x 1024です。

シングルセッションOS用Virtual Delivery Agent (VDA)

サポートされているオペレーティングシステム:

- ウィンドウズ 11
- Windows 10 (x64のみ)、現在メインストリームサポート中のすべてのバージョン。

- エディションのサポートについては、Knowledge Centerの記事CTX224843を参照してください。

要件:

- Microsoft .NET Framework 4.8がまだインストールされていない場合（またはそれ以降のバージョンがインストールされていない場合）、自動的にインストールされます。
- Microsoft Visual C++ 2015–2022 再頒布可能パッケージ。

Remote PC Accessは、物理的なオフィスPCにインストールするこのVDAを使用します。このVDAは、Windows 11およびWindows 10上のCitrix Virtual Desktops™ Remote PC Accessのセキュアブートをサポートします。

複数のマルチメディアアクセラレーション機能（HDX MediaStream Windows Media Redirectionなど）を使用するには、VDAをインストールするマシンにMicrosoft Media Foundationがインストールされている必要があります。マシンにMedia Foundationがインストールされていない場合、マルチメディアアクセラレーション機能はインストールされず、動作しません。Citrixソフトウェアのインストール後にマシンからMedia Foundationを削除しないでください。削除すると、ユーザーはマシンにログオンできなくなります。ほとんどのサポートされているWindowsシングルセッションOSエディションでは、Media Foundationのサポートはすでにインストールされており、削除できません。ただし、Nエディションには特定のメディア関連テクノロジーが含まれていません。そのソフトウェアはMicrosoftまたはサードパーティから入手できます。詳細については、インストール準備を参照してください。

Linux VDA の詳細については、Linux Virtual Delivery Agent の記事を参照してください。

Server VDI 機能を使用するには、コマンドラインインターフェイスを使用して、サポートされている Windows Server マシンに Windows シングルセッション OS 用の VDA をインストールできます。Server VDI を参照してください。

Windows 7 マシンに VDA をインストールする方法については、以前のオペレーティングシステムを参照してください。

マルチセッションOS用Virtual Delivery Agent (VDA)

サポートされているオペレーティングシステム:

- ウィンドウズ サーバー 2025
- Windows 11 (Citrix DaaS™でのみサポート)

- Windows 10 (x64のみ、Citrix DaaSでのみサポート)、現在メインストリームサポート中のすべてのバージョン。
- ウィンドウズ サーバー 2022
- ウィンドウズ サーバー 2019、スタンダード および データセンター エディション

インストーラーは以下の要件を自動的に展開します。これらはCitrixインストールメディアの**Support**フォルダーにもあります。

- Microsoft .NET Framework 4.8 は、まだインストールされていない場合 (またはそれ以降のバージョンがインストールされていない場合) は自動的にインストールされます。
- Microsoft Visual C++ 2015–2022 再頒布可能パッケージ。

リモートデスクトップサービス役割サービスがまだインストールおよび有効化されていない場合、インストーラーは自動的にそれらをインストールして有効化します。

いくつかのマルチメディアアクセラレーション機能 (HDX MediaStream Windows Media Redirection など) では、VDA をインストールするマシンに Microsoft Media Foundation がインストールされている必要があります。マシンに Media Foundation がインストールされていない場合、マルチメディアアクセラレーション機能はインストールされず、動作しません。Citrix ソフトウェアのインストール後にマシンから Media Foundation を削除しないでください。削除すると、ユーザーはマシンにログオンできなくなります。ほとんどの Windows Server バージョンでは、Media Foundation 機能はサーバーマネージャーを通じてインストールされます。詳細については、インストール準備 を参照してください。

VDAにMedia Foundationが存在しない場合、以下のマルチメディア機能は動作しません。

- Windows Mediaリダイレクト
- HTML5ビデオのリダイレクト
- HDX™ RealTimeウェブカメラのリダイレクト

Linux VDAについては、Linux Virtual Delivery Agentの記事を参照してください。

Windows Server 2008 R2マシンにVDAをインストールする方法については、以前のオペレーティングシステムを参照してください。

Amazon WorkSpaces Coreマネージドインスタンスの VDA

サポートされているオペレーティングシステム:

- Windows 11シングルセッション

- Windows 10シングルセッション
- Windows サーバー 2025
- Windows サーバー 2022
- Windows サーバー 2019
- Windows サーバー 2016
- Ubuntu サーバー 24.04 LTS
- デビアン 12

ホスト / 仮想化リソース

以下のホスト/仮想化リソース（アルファベット順）がサポートされています。該当する場合、メジャー. マイナーバージョンとその更新がサポートされます。Knowledge Centerの記事CTX131239には、現在のバージョン情報と既知の問題へのリンクが含まれています。

一部の機能は、すべてのホストプラットフォームまたはすべてのプラットフォームバージョンでサポートされていない場合があります。詳細については、機能のドキュメントを参照してください。

Remote PC AccessのWake on LAN機能には、Microsoft System Center Configuration Manager 2012以降が必要です。

サポートされているハイパーバイザー:

- **Azure ローカル**

  詳細については、Azure Local環境を参照してください。

- **ゼンサーバー (旧称 Citrix ハイパーバイザー™)**

  CTX131239には、現在のバージョン情報と既知の問題へのリンクが含まれています。

  詳細については、「XenServer仮想化環境」(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/install-prepare/xenserver.html)を参照してください。

- **マイクロソフト システム センター バーチャル マシン マネージャー**

  サポートされているSystem Center Virtual Machine Managerのバージョンに登録できるHyper-Vのすべてのバージョンが含まれます。

  CTX131239には、現在のバージョン情報と既知の問題へのリンクが含まれています。

  詳細については、「Microsoft System Center Virtual Machine Manager仮想化環境」を参照してください。

- **Nutanix アクロポリス**

  CTX131239 には、現在のバージョン情報と既知の問題へのリンクが含まれています。

  詳細については、Nutanix仮想化環境 を参照してください。

- **ヴイエムウェア ヴイスフィア (ヴイセンター + イーエスエックスアイ)**

  vSphere vCenter Linked Mode操作はサポートされていません。

  CTX131239 には、現在のバージョン情報と既知の問題へのリンクが含まれています。

  詳細については、VMware仮想化環境 を参照してください。

サポートされているパブリッククラウドホスト:

- **アマゾン ウェブ サービス (AWS)**

  AWSを使用して仮想マシンをプロビジョニングする方法については、Amazon Web Services 仮想化環境 を参照してください。

- **Google Cloud Platform** 詳細については、Google Cloud Platform仮想化環境 および Google CloudでのCitrix DaaSの開始 を参照してください。

- **マイクロソフト Azure Resource Manager**

  Microsoft Azure Resource Managerを使用して仮想マシンをプロビジョニングする方法については、Microsoft Azure Resource Manager仮想化環境 を参照してください。

- **レッドハット OpenShift**

  Red Hat OpenShiftを使用して仮想マシンをプロビジョニングする方法については、Red Hat OpenShift仮想化環境 を参照してください。

- **Nutanix クラウドおよびパートナーソリューション**

  Nutanix クラウドおよびパートナーソリューションの使用については、「Nutanix cloud and partner solutions」を参照してください。

- **VMware クラウドおよびパートナーソリューション**

  VMware クラウドおよびパートナーソリューションの使用については、「VMware cloud and partner solutions」を参照してください。

展開にパブリッククラウドホスト接続を追加する場合は、次の点を考慮してください。

- ハイブリッド権限ライセンスが必要です。ハイブリッド権限ライセンスについては、「Transition and Trade-Up (TTU) with Hybrid Rights」を参照してください。ライセンスの追加については、「Create a site」を参照してください。
- 情報源は Citrix DaaS のドキュメントを参照しています。Citrix DaaS 製品のパブリッククラウドホストに精通している場合でも、オンプレミスバージョンとはいくつかの違いがあります。
    - Citrix DaaS への更新は、約4週間ごとに展開されます。そのため、Citrix DaaS で利用できる特定の機能がオンプレミスバージョンでは利用できない場合があります。

Active Directory の機能レベル

Active Directory フォレストおよびドメインでサポートされている機能レベルは次のとおりです。

- ウィンドウズ サーバー 2025
- ウィンドウズ サーバー 2016
- ウィンドウズ サーバー 2012 R2
- Windows サーバー 2012
- Windows サーバー 2008 R2
- ウィンドウズ サーバー 2008

> **注:**
>
> Citrix Virtual Apps and Desktopsサイトをアップグレードする前に、個々の機能の要件を確認してください。新しい機能やVDAでは、特定の最小Active Directory機能レベルが必要になる場合があります。

HDX

オーディオ

Multi-Stream ICA®のUDPオーディオは、Windows向けCitrix WorkspaceアプリおよびLinux 13向けCitrix Workspaceアプリでサポートされています。

エコーキャンセルは、Windows向けCitrix Workspaceアプリでサポートされています。

特定のHDX機能のサポートと要件を参照してください。HDX機能とCitrix Workspaceアプリの詳細については、機能マトリックスを参照してください。

HDX Windows Media の配信

Windows Mediaクライアント側コンテンツフェッチ、Windows Mediaリダイレクト、およびリアルタイムWindows Mediaマルチメディアトランスコーディングでは、次のクライアントがサポートされています：Windows向けCitrix Workspaceアプリ、iOS向けCitrix Workspaceアプリ、Linux向けCitrix Workspaceアプリ。

Windows 8デバイスでWindows Mediaクライアント側コンテンツフェッチを使用するには、Citrix Multimedia Redirectorをデフォルトプログラムとして設定します。**コントロールパネル > プログラム > 既定のプログラム > 既定のプログラムの設定**で、**Citrix Multimedia Redirector**を選択し、**このプログラムを既定として設定**または**このプログラムの既定を選択**をクリックします。GPUトランスコーディングには、Compute Capability 1.1以降のNVIDIA CUDA対応GPUが必要です。`<https://developer.nvidia.com/cuda/cuda-gpus>`を参照してください。

HDX 3D Pro 機能

WindowsシングルセッションOS用VDAは、実行時にGPUハードウェアの存在を検出します。

アプリケーションをホストする物理マシンまたは仮想マシンは、GPUパススルーまたは仮想GPU (vGPU) を使用できます。

- GPUパススルーは以下で利用可能です。
  - XenServer®
  - ニュータニックス AHV
  - VMware vSphereおよびVMware ESX（ここでは仮想Direct Graphics Acceleration (vDGA) と呼ばれます）
- vGPU は以下で利用できます:
  - XenServer
  - ニュータニックス AHV
  - ヴイエムウェア ブイスフィア

`<https://docs.citrix.com/ja-jp/citrix-virtual-apps-desktops/2511/graphics/hdx-3d-pro>`を参照してください。

Citrix は、ホストコンピューターに少なくとも 4 GB の RAM と、2.3 GHz 以上のクロック速度を持つ 4 つの仮想 CPU を搭載することを推奨します。

グラフィック処理ユニット (GPU):

- NVIDIA GRID API を使用した仮想化グラフィックスアクセラレーションの場合、NVIDIA Virtual GPU (vGPU) ソフトウェアバージョン 13 以降でサポートされているすべての NVIDIA GRID GPU とともに HDX 3D Pro を使用できます。`<https://docs.nvidia.com/grid/index.html>` を参照してください。 サポートされているハイパーバイザーとハードウェアの詳細なリストについては、NVIDIA vGPU ソフトウェア のドキュメントを参照してください。
- 仮想化グラフィックスアクセラレーションは、Intel Xeon Processor E3 Family のデータセンターグラフィックスプラットフォームおよび Intel データセンター GPU Flex シリーズでサポートされています。詳細については、GPU Flex シリーズ を参照してください。
- AMD GPU は、AMD の mxGPU 仮想化でサポートされています。サポートされているハードウェアの詳細については、AMD ドキュメント を参照してください。

ユーザーデバイス:

- Citrix は、ハードウェアリソースに応じて最大 8 台の 4K モニターをサポートしています。使用される GPU によっては、この最大値に他のハードウェア制限がある場合があります。
- Citrixは、ユーザーデバイスに4GB以上のRAMと1.6GHz以上のクロック速度を持つCPUを搭載することを推奨しています。最適なパフォーマンスを得るには、ユーザーデバイスに8GB以上のRAMと3GHz以上のクロック速度を持つデュアルコアCPUを搭載することを推奨します。
- マルチモニターアクセスには、Citrixはクアッドコアcpuを搭載したユーザーデバイスを推奨しています。
- Citrix Workspaceアプリがインストールされている必要があります。

詳細については、HDX 3D Proの記事 および www.citrix.com/xenapp/3d を参照してください。

ユニバーサル プリント サーバー

ユニバーサルプリントサーバーは、クライアントコンポーネントとサーバーコンポーネントで構成されています。UpsClientコンポーネントはVDAインストールに含まれています。UpsServerコンポーネントは、ユーザーセッションでCitrix Universal™ Print Driverを使用してプロビジョニングしたい共有プリンターが存在する各プリントサーバーにインストールします。

UpsServerコンポーネントは以下をサポートしています。

- ウィンドウズ サーバー 2025
- ウィンドウズ サーバー 2022
- Windows サーバー 2019

要件:

- Microsoft Visual C++ 2015–2022 再頒布可能パッケージ
- マイクロソフト .NET フレームワーク 4.8 (最小)

マルチセッションOS用VDAの場合、印刷操作中のユーザー認証には、ユニバーサルプリントサーバーがVDAと同じドメインに参加している必要があります。

スタンドアロンのクライアントおよびサーバーコンポーネントパッケージもダウンロードできます。

詳細については、プリンターのプロビジョニングを参照してください。

その他

Citrix License Server 11.17.2以降のみがサポートされています。詳細については、ライセンスを参照してください。

バージョンの互換性に関する詳細については、製品マトリックスを参照してください。

サポートされているStoreFrontのバージョンについては、StoreFrontのシステム要件を参照してください。

Citrixポリシー情報をサイト構成データベースではなくActive Directoryに保存する場合、Microsoft Group Policy Management Console (GPMC)が必要です。`CitrixGroupPolicyManagement_x64.msi`を個別にインストールする場合（たとえば、Citrix Virtual Apps and Desktopsのコアコンポーネントがインストールされていないマシンにインストールする場合）、そのマシンにはVisual Studio 2015ランタイムがインストールされている必要があります。詳細については、Microsoftのドキュメントを参照してください。

GPMCを使用してドメインGPOを編集する場合は、Delivery Controllerを含むすべてのマシンで（Windows Server Managerの）グループポリシー管理機能を有効にしてください。

複数のNICがサポートされています。

デフォルトでは、現在のVDAをインストールしても、Windows用Citrix Workspaceアプリはインストールされません。詳細については、Windows用Citrix Workspaceアプリのドキュメントを参照してください。

その機能でサポートされているブラウザー情報については、ローカルアプリアクセスを参照してください。

このバージョンのCitrix Virtual Apps and Desktopsには、HDX RealTime Connector 2.9 LTSR以降が必要です。詳細については、HDX RealTime Optimization Packのドキュメントを参照してください。

この製品はPowerShellバージョン3から5をサポートしています。

技術概要

Citrix Virtual Apps and Desktops™ は、IT部門が仮想マシン、アプリケーション、ライセンス、セキュリティを制御できるようにし、あらゆるデバイスからどこからでもアクセスを提供できる仮想化ソリューションです。

Citrix Virtual Apps™ and Desktops は以下を可能にします:

- エンドユーザーが、デバイスのオペレーティングシステムやインターフェースに依存せずにアプリケーションやデスクトップを実行すること。
- 管理者が、ネットワークを管理し、選択したデバイスまたはすべてのデバイスからのアクセスを制御すること。
- 管理者が、単一のデータセンターからネットワーク全体を管理すること。

Citrix Virtual Apps and Desktops は、FlexCast Management Architecture (FMA) と呼ばれる統合アーキテクチャを共有しています。FMAの主な機能は、単一のサイトから複数のバージョンのCitrix Virtual AppsまたはCitrix Virtual Desktops™を実行できることと、統合されたプロビジョニングです。

主要コンポーネント

Citrix Virtual Apps and Desktops を初めて使用する場合、この記事が最も役立ちます。

この図は、一般的な展開（サイトと呼ばれます）における主要コンポーネントを示しています。

一般的な展開における主要コンポーネント(/en-us/citrix-virtual-apps-desktops/2511/media/components-new-op.png)

デリバリーコントローラー™

Delivery Controller は、サイトの中心的な管理コンポーネントです。各サイトには1つ以上のDelivery Controllerがあります。データセンター内の少なくとも1台のサーバーにインストールされます。サイトの信頼性と可用性を高めるために、複数のサーバーにControllerをインストールしてください。展開にハイパーバイザーまたはその他のサービスが含まれている場合、Controllerサービスはそれと通信して以下を行います:

- アプリケーションとデスクトップを配信する

- ユーザーアクセスを認証および管理する
- ユーザーと、そのデスクトップおよびアプリケーションとの間の接続を仲介する
- ユーザー接続を最適化する
- 接続を負荷分散する

ControllerのBroker Serviceは、どのユーザーがどこにログオンしているか、ユーザーがどのようなセッションリソースを持っているか、およびユーザーが既存のアプリケーションに再接続する必要があるかどうかを追跡します。Broker ServiceはPowerShellコマンドレットを実行し、TCPポート80を介してVDA上のブローカーエージェントと通信します。TCPポート443を使用するオプションはありません。

Monitor Serviceは履歴データを収集し、監視データベースに配置します。このサービスはTCPポート80または443を使用します。

Controllerサービスからのデータはサイトデータベースに保存されます。

Controllerは、デスクトップの状態を管理し、需要と管理構成に基づいてデスクトップを起動および停止します。

データベース

各サイトには、構成情報とセッション情報を保存するために、少なくとも1つのMicrosoft SQL Serverデータベースが必要です。このデータベースは、Controllerを構成するサービスによって収集および管理されるデータを保存します。データベースをデータセンター内にインストールし、Controllerへの永続的な接続があることを確認してください。

サイトは、構成ログデータベースと監視データベースも使用します。デフォルトでは、これらのデータベースはサイトデータベースと同じ場所にインストールされますが、これは変更できます。

仮想配信エージェント (VDA)

VDAは、ユーザーに提供するサイト内の各物理または仮想マシンにインストールされます。これらのマシンはアプリケーションまたはデスクトップを提供します。VDAはマシンがControllerに登録できるようにし、それにより、マシンとそれがホストするリソースがユーザーに利用可能になります。VDAはマシンとユーザーデバイス間の接続を確立および管理します。VDAは、ユーザーまたはセッションにCitrix®ライセンスが利用可能であることを確認し、セッション用に構成されたポリシーを適用します。

VDAは、VDA内のブローカーエージェントを介して、Controller内のBroker Serviceにセッション情報を通信します。ブローカーエージェントは複数のプラグインをホストし、リアルタイムデータを収集します。それはTCPポート80を介してControllerと通信します。

「VDA」という言葉は、エージェントとそれがインストールされているマシンを指すためによく使われます。

VDAは、シングルセッションおよびマルチセッションのWindowsオペレーティングシステムで利用できます。マルチセッションWindowsオペレーティングシステム用のVDAは、複数のユーザーが同時にサーバーに接続できるようにします。シングルセッションWindowsオペレーティングシステム用のVDAは、一度に1人のユーザーのみがデスクトップに接続できるようにします。Linux VDAも利用可能です。

シトリックス StoreFront™

StoreFront は、ユーザーを認証し、ユーザーがアクセスするデスクトップとアプリケーションのストアを管理します。これは、ユーザーが利用できるようにするデスクトップとアプリケーションへのセルフサービスアクセスを提供するエンタープライズアプリケーションストアをホストできます。また、ユーザーのアプリケーションサブスクリプション、ショートカット名、その他のデータも追跡します。これにより、ユーザーは複数のデバイスで一貫したエクスペリエンスを享受できます。

シトリックス ワークスペース™ アプリ

ユーザーデバイスやその他のエンドポイント（仮想デスクトップなど）にインストールされた Citrix Workspace アプリは、ドキュメント、アプリケーション、デスクトップへの迅速で安全なセルフサービスアクセスをユーザーに提供します。Citrix Workspace アプリは、Windows、Web、およびサービスとしてのソフトウェア（SaaS）アプリケーションへのオンデマンドアクセスを提供します。デバイス固有の Citrix Workspace アプリソフトウェアをインストールできないデバイスの場合、Citrix Workspace アプリ for HTML5 は、HTML5互換のWebブラウザを介した接続を提供します。

スタジオ

Web Studio は、オンプレミスの Citrix Virtual Apps and Desktops 展開を構成および管理できる Web ベースの管理コンソールです。ユーザーエクスペリエンスの向上を目的として設計されており、Windows ベースの管理コンソールである Citrix Studio よりも一般的に応答が高速です。

詳細については、「Web Studio のインストール」を参照してください。

セキュアプライベートアクセス

Citrix Secure Private Access オンプレミスソリューションは、StoreFront を Web および SaaS アプリへの統合アクセス ポータルとして使用し、仮想アプリおよびデスクトップを Citrix Workspace の統合された一部として、ブラウザベースのアプリ（内部 Web アプリおよび SaaS ア

プリ）へのゼロトラストネットワークアクセスを簡単に提供する機能により、組織全体のセキュリティとコンプライアンス体制を強化します。このソリューションは、既存の NetScaler および StoreFront のリリースと互換性があり、バージョンに変更は必要ありません。詳細については、「オンプレミス向け Secure Private Access」を参照してください。

シトリックス Director

Director は、IT サポートおよびヘルプデスクチームが環境を監視し、システムに重大な問題が発生する前にトラブルシューティングを行い、エンドユーザーのサポートタスクを実行できるようにする Web ベースのツールです。1つの Director 展開を使用して、複数の Citrix Virtual Apps または Citrix Virtual Desktops サイトに接続して監視できます。

Director には以下が表示されます。

- Controller 内の Broker Service からのリアルタイムセッションデータ。これには、Broker Service が VDA 内のブローカーエージェントから取得するデータが含まれます。
- Controller 内の Monitor Service からの履歴サイトデータ。

Director は、Citrix Gateway デバイスによってキャプチャされた ICA® パフォーマンスおよびヒューリスティックデータを使用して、データから分析を構築し、それを管理者に提示します。

Director を使用して、Windows リモートアシスタンス経由でユーザーのセッションを表示および操作することもできます。

Citrix ライセンスサーバー

License Server は、Citrix 製品のライセンスを管理します。Controller と通信して各ユーザーのセッションのライセンスを管理し、Studio と通信してライセンスファイルを割り当てます。サイトには、ライセンスファイルを保存および管理するために、少なくとも1つのライセンスサーバーが必要です。

ハイパーバイザーまたはその他のサービス

ハイパーバイザーまたはその他のサービスは、サイト内の仮想マシンをホストします。これらは、アプリケーションとデスクトップをホストするために使用するVM、およびCitrix Virtual Apps and Desktopsコンポーネントをホストするために使用するVMです。ハイパーバイザーは、ハイパーバイザーの実行と仮想マシンのホストに完全に特化したホストコンピューターにインストールされます。

Citrix Virtual Apps and Desktops は、さまざまなハイパーバイザーおよびその他のサービスをサポートしています。

多くの展開ではハイパーバイザーが必要ですが、Remote PC Access を提供するためにハイパーバイザーは必要ありません。また、Provisioning Services (PVS) を使用してVMをプロビジョニングする場合も、ハイパーバイザーは必要ありません。

追加コンポーネント

以下のコンポーネントも、Citrix Virtual Apps and Desktops の展開に含めることができます。詳細については、それぞれのドキュメントを参照してください。

Citrix Provisioning™ (シトリックス プロビジョニング™)

Citrix Provisioning (旧 Provisioning Services) は、一部のエディションで利用可能なオプションコンポーネントです。仮想マシンをプロビジョニングするための MCS の代替手段を提供します。MCS がマスターイメージのコピーを作成するのに対し、PVS はマスターイメージをユーザーデバイスにストリーミングします。PVS はこれを行うためにハイパーバイザーを必要としないため、物理マシンをホストするために使用できます。PVS は Controller と通信して、ユーザーにリソースを提供します。

Citrix Gateway (シトリックス ゲートウェイ)

ユーザーが企業ファイアウォールの外部から接続する場合、Citrix Virtual Apps and Desktops は Citrix Gateway (旧 Access Gateway および NetScaler® Gateway) テクノロジーを使用して、TLS でこれらの接続を保護できます。Citrix Gateway または VPX 仮想アプライアンスは、非武装地帯 (DMZ) に展開される SSL VPN アプライアンスです。これは、企業ファイアウォールを介した単一の安全なアクセスポイントを提供します。

シトリックス SD-WAN™

支社などのリモートロケーションのユーザーに仮想デスクトップが提供される展開では、Citrix SD-WAN テクノロジーを使用してパフォーマンスを最適化できます。リピーターは WAN 全体のパフォーマンスを高速化します。ネットワークにリピーターがある場合、支社のユーザーは WAN 経由で LAN のようなパフォーマンスを体験できます。Citrix SD-WAN は、ユーザーエクスペリエンスのさまざまな部分に優先順位を付けることができるため、たとえば、大きなファイルや印刷ジョブがネットワーク経由で送信されたときに、支社のユーザーエクスペリエンスが低下することはありません。HDX™ WAN 最適化は、トークン化された圧縮とデータ重複排除を提供し、帯域幅要件を劇的に削減し、パフォーマンスを向上させます。

一般的な展開の仕組み

サイトは、スケーラビリティ、高可用性、フェールオーバーを可能にし、設計上セキュアなソリューションを提供する専用の役割を持つマシンで構成されています。サイトは、VDAがインストールされたサーバーとデスクトップマシン、およびアクセスを管理するDelivery Controllerで構成されます。

展開におけるコンポーネント間の通信 (/en-us/citrix-virtual-apps-desktops/2511/media/deployment-overview.png)

VDAを使用すると、ユーザーはデスクトップやアプリケーションに接続できます。ほとんどの配信方法ではデータセンターの仮想マシンにインストールされますが、リモートPCアクセス用に物理PCにインストールすることもできます。

Controllerは、リソース、アプリケーション、デスクトップを管理し、ユーザー接続を最適化およびバランス調整する独立したWindowsサービスで構成されています。各サイトには1つ以上のControllerがあります。セッションは遅延、帯域幅、ネットワークの信頼性の影響を受けるため、可能であればすべてのControllerを同じLAN上に配置してください。

ユーザーがControllerに直接アクセスすることはありません。VDAはユーザーとController間の仲介役として機能します。ユーザーがStoreFrontを使用してログオンすると、資格情報はController上のBroker Serviceに渡されます。その後、Broker Serviceは、ユーザーに設定されたポリシーに基づいてプロファイルと利用可能なリソースを取得します。

ユーザー接続の処理方法

セッションを開始するには、ユーザーは自分のデバイスにインストールされているCitrix Workspaceアプリ、またはStoreFront Webサイトのいずれかを介して接続します。

ユーザーは、必要な物理または仮想デスクトップ、あるいは仮想アプリケーションを選択します。

ユーザーの資格情報は、この経路を介してControllerにアクセスします。Controllerは、Broker Serviceと通信して、どのリソースが必要かを判断します。Citrixは、Citrix Workspaceアプリから送信される資格情報を暗号化するために、管理者がStoreFrontにSSL証明書を配置することを推奨しています。

ユーザー接続フロー (/en-us/citrix-virtual-apps-desktops/2511/media/user-connections.png)

Broker Serviceは、ユーザーがアクセスを許可されているデスクトップとアプリケーションを決定します。

資格情報が検証されると、利用可能なアプリケーションまたはデスクトップに関する情報が、StoreFront-Citrix Workspaceアプリの経路を通じてユーザーに返送されます。ユーザーがこのリストからアプリケーションまたはデスクトップを選択すると、その情報は経路を介してControllerに戻されます。その後、Controllerは特定のアプリケーションまたはデスクトップをホストする適切なVDAを決定します。

Controllerはユーザーの資格情報を含むメッセージをVDAに送信し、その後、ユーザーと接続に関するすべてのデータをVDAに送信します。VDAは接続を受け入れ、同じ経路を介してCitrix Workspaceアプリに情報を返送します。StoreFrontで一連の必須パラメーターが収集されます。これらのパラメーターは、Citrix WorkspaceアプリとStoreFront間のプロトコル会話の一部として、またはICA（Independent Computing Architecture）ファイルに変換されてダウンロードされる形で、Citrix Workspaceアプリに送信されます。サイトが適切に設定されていれば、このプロセス全体を通じて資格情報は暗号化されたままになります。

ICAファイルはユーザーのデバイスにコピーされ、デバイスとVDA上で実行されているICAスタックとの間に直接接続を確立します。この接続は、管理インフラストラクチャ（Citrix Workspaceアプリ、StoreFront、およびController）をバイパスします。

Citrix WorkspaceアプリとVDA間の接続には、Citrix Gatewayプロトコル（CGP）が使用されます。接続が失われた場合、セッションの信頼性機能により、ユーザーは管理インフラストラクチャを介して再起動することなく、VDAに再接続できます。セッションの信頼性は、Citrixポリシーで有効または無効にできます。

クライアントがVDAに接続すると、VDAはユーザーがログオンしたことをControllerに通知します。その後、Controllerはこの情報をサイトデータベースに送信し、監視データベースにデータのログ記録を開始します。

データアクセスが機能する仕組み

すべてのCitrix Virtual Apps and Desktopsセッションは、IT部門がStudioまたはDirectorを介してアクセスできるデータを生成します。Studioを使用すると、管理者はBroker Agentからリアルタイムデータにアクセスしてサイトを管理できます。Directorは、同じデータに加えて、監視データベースに保存されている履歴データにもアクセスします。また、ヘルプデスクサポートとトラブルシューティングのために、NetScaler GatewayからHDXデータにもアクセスします。

展開におけるデータアクセス(/en-us/citrix-virtual-apps-desktops/2511/media/data-access.png)

Controller内では、Broker Serviceがリアルタイムデータを提供するマシンのすべてのセッションのセッションデータを報告します。Monitor Serviceもリアルタイムデータを追跡し、監視データベースに履歴データとして保存します。

StudioはBroker Serviceとのみ通信します。リアルタイムデータのみにアクセスします。Directorは、Broker Service（Broker Agent内のプラグインを介して）と通信して、サイトデータベースにアクセスします。

Directorは、HDXデータに関する情報を取得するためにCitrix Gatewayにもアクセスできます。

デスクトップとアプリケーションの配信

マシンカタログを使用して、アプリケーションとデスクトップを配信するマシンを設定します。次に、利用可能なアプリケーションとデスクトップ（カタログ内のマシンを使用）と、それらにアクセスできるユーザーを指定するデリバリーグループを作成します。オプションで、アプリケーションのコレクションを管理するためにアプリケーショングループを作成することもできます。

マシンカタログ

マシンカタログは、単一のエンティティとして管理する仮想マシンまたは物理マシンのコレクションです。これらのマシン、およびそれらに含まれるアプリケーションまたは仮想デスクトップは、ユーザーに提供するリソースです。カタログ内のすべてのマシンには、同じオペレーティングシステムとVDAがインストールされています。また、同じアプリケーションまたは仮想デスクトップも含まれています。

通常、マスターイメージを作成し、それを使用してカタログ内に同一のVMを作成します。VMの場合、そのカタログ内のマシンのプロビジョニング方法として、Citrixツール（Citrix ProvisioningまたはMCS）またはその他のツールを指定できます。あるいは、既存の独自のイメージを使用することもできます。その場合、ターゲットデバイスを個別に、またはサードパーティの電子ソフトウェア配布（ESD）ツールを使用して一括で管理する必要があります。

有効なマシンタイプは次のとおりです。

- **マルチセッションOS:** マルチセッションオペレーティングシステムを搭載した仮想マシンまたは物理マシン。Citrix Virtual Apps公開アプリ（サーバーベースのホスト型アプリケーションとも呼ばれる）およびCitrix Virtual Apps公開デスクトップ（サーバーホスト型デスクトップとも呼ばれる）の配信に使用されます。これらのマシンには、複数のユーザーが同時に接続できます。
- **シングルセッションOS:** シングルセッションオペレーティングシステムを搭載した仮想マシンまたは物理マシン。VDIデスクトップ（オプションでパーソナライズ可能なシングルセッションOSを実行するデスクトップ）、VMホスト型アプリ（シングルセッションOSからのアプリケーション）、およびホスト型物理デスクトップの提供に使用されます。これらのデスクトップには、一度に1人のユーザーのみが接続できます。

- **Remote PC Access:** リモートユーザーがCitrix Workspaceアプリを実行している任意のデバイスから物理的なオフィスPCにアクセスできるようにします。オフィスPCはCitrix Virtual Desktops展開を通じて管理され、ユーザーデバイスは許可リストで指定する必要があります。

詳細については、「Citrix Virtual Apps and Desktops Image Management」および「マシンカタログの作成」を参照してください。

デリバリーグループ

デリバリーグループは、どのユーザーがどのアプリケーション、デスクトップ、またはその両方にどのマシンでアクセスできるかを指定します。デリバリーグループには、マシンカタログからのマシンと、サイトにアクセスできるActive Directoryユーザーが含まれます。Active Directoryグループとデリバリーグループは、同様の要件を持つユーザーをグループ化する方法であるため、Active Directoryグループによってユーザーをデリバリーグループに割り当てることができます。

各デリバリーグループは複数のカタログからのマシンを含めることができ、各カタログは複数のデリバリーグループにマシンを提供できます。ただし、個々のマシンは一度に1つのデリバリーグループにのみ属することができます。

デリバリーグループのユーザーがアクセスできるリソースを定義します。たとえば、異なるアプリケーションを異なるユーザーに配信するには、1つのカタログのマスターイメージにすべてのアプリケーションをインストールし、そのカタログに十分な数のマシンを作成して、複数のデリバリーグループに分散させます。その後、各デリバリーグループを構成して、マシンにインストールされているアプリケーションの異なるサブセットを配信できます。

詳細については、「デリバリーグループの作成」を参照してください。

アプリケーショングループ

アプリケーショングループは、より多くのデリバリーグループを使用するよりも、アプリケーション管理とリソース制御の利点を提供します。タグ制限機能を使用すると、既存のマシンを複数の公開タスクに使用できるため、展開と追加のマシンの管理に関連するコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）するものと考えることができます。アプリケーショングループは、デリバリーグループ内のマシンのサブセットを分離してトラブルシューティングする場合にも役立ちます。

詳細については、「アプリケーショングループの作成」を参照してください。

詳細情報

- シトリックス バーチャルアプリおよびデスクトップの図

- ネットワークポート
- データベース
- サポートされているハイパーバイザーおよびその他のサービス

データベース

> **注:**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> Citrix Virtual AppsまたはCitrix Virtual Desktops™サイトでは、次の3つのSQL Serverデータベースを使用します。

- **Site:**（サイト構成とも呼ばれます）には、実行中のサイト構成、現在のセッション状態、および接続情報が保存されます。
- **Logging:**（構成ログとも呼ばれます）には、サイト構成の変更と管理アクティビティに関する情報が保存されます。このデータベースは、構成ログ機能が有効になっている場合（デフォルト = 有効）に使用されます。
- **Monitoring:**には、Directorが使用するセッションや接続情報などのデータが保存されます。

各Delivery Controllerはサイトデータベースと通信します。Controllerとデータベース間ではWindows認証が必要です。Controllerは、サイト内の他のControllerに影響を与えることなく、接続を解除したり電源を切ったりできます。ただし、これはサイトデータベースが単一障害点となることを意味します。データベースサーバーが故障した場合、既存の接続はユーザーがログオフまたは切断するまで機能し続けます。サイトデータベースが利用できなくなった場合の接続動作については、Local Host Cacheを参照してください。

Citrixは、データベースに関して以下を推奨します。

- **定期的にバックアップする。** データベースサーバーが故障した場合にバックアップから復元できるように、データベースを定期的にバックアップしてください。各データベースのバックアップ戦略は異なる場合があります。詳細については、CTX135207を参照してください。ただし、これはCitrixXenDesktopDBを参照していますが、これは現在サポートされておらず、お客様は利用できません。

- **Site、Monitoring、およびLoggingのSQL Serverデータベースを定期的にバックアップおよび復元する。** SQL Serverデータベースに関する具体的な情報については、Creating Full and Differential Backups of a SQL Server Databaseを参照してください。

サイトに複数のゾーンが含まれている場合は、プライマリゾーンに常にサイトデータベースが含まれていることを確認してください。すべてのゾーンのControllerがそのデータベースと通信します。

高可用性

自動フェールオーバーを確実にするために考慮すべき高可用性ソリューションがいくつかあります。

- **AlwaysOn Availability Groups（Basic Availability Groupsを含む）：** SQL Server 2012で導入されたこのエンタープライズレベルの高可用性および災害復旧ソリューションは、1つ以上のデータベースの可用性を最大化できます。AlwaysOn Availability Groupsでは、SQL ServerインスタンスがWindows Server Failover Clustering（WSFC）ノード上に存在する必要があります。詳細については、Windows Server Failover Clustering with SQL Serverを参照してください。
- **SQL Serverデータベースミラーリング:** データベースをミラーリングすることで、アクティブなデータベースサーバーが失われた場合でも、自動フェイルオーバープロセスが数秒で発生し、ユーザーは通常影響を受けません。この方法は、各データベースサーバーに完全なSQL Serverライセンスが必要となるため、他のソリューションよりも高価です。ミラーリング環境ではSQL Server Express Editionを使用できません。
- **SQLクラスタリング:** Microsoft SQLクラスタリングテクノロジーを使用すると、障害が発生した別のサーバーのタスクと責任を1つのサーバーが自動的に引き継ぐことができます。ただし、このソリューションのセットアップはより複雑であり、自動フェイルオーバープロセスはSQLミラーリングなどの代替手段よりも通常遅くなります。
- **ハイパーバイザーの高可用性機能の使用:** この方法では、データベースを仮想マシンとして展開し、ハイパーバイザーの高可用性機能を使用します。このソリューションは、既存のハイパーバイザーソフトウェアを使用し、SQL Server Express Editionも使用できるため、ミラーリングよりも安価です。ただし、自動フェイルオーバープロセスは遅く、データベース用に新しいマシンが起動するのに時間がかかり、ユーザーへのサービスが中断される可能性があります。

ローカルホストキャッシュ機能は、SQL Serverの高可用性のベストプラクティスを補完します。ローカルホストキャッシュにより、サイトデータベースが利用できない場合でも、ユーザーはア

プリケーションやデスクトップに接続および再接続できます。詳細については、「ローカルホストキャッシュ」を参照してください。

サイト内のすべてのControllerが失敗した場合、VDAを高可用性モードで動作するように構成できます。これにより、ユーザーは引き続きデスクトップとアプリケーションにアクセスできます。高可用性モードでは、VDAはControllerによって仲介される接続ではなく、ユーザーからの直接ICA接続を受け入れます。この機能は、すべてのControllerとの通信が失敗するまれなケースでのみ使用してください。この機能は、他の高可用性ソリューションの代替ではありません。詳細については、「CTX 127564」を参照してください。

SQLクラスタリングまたはSQLミラーリングのインストールで、ノードにControllerをインストールすることはサポートされていません。

データベースソフトウェアのインストール

> **注：**
>
> バージョン2411以降、データベースにAzure SQL Managed Instanceを使用できます。

> デフォルトでは、最初のDelivery Controller™をインストールするときに、そのサーバーで別のSQL Serverインスタンスが検出されない場合、SQL Server Express Editionがインストールされます。このデフォルトのアクションは、概念実証またはパイロット展開には通常十分です。ただし、SQL Server ExpressはMicrosoftの高可用性機能をサポートしていません。

デフォルトのインストールでは、デフォルトのWindowsサービスアカウントと権限が使用されます。これらのデフォルトの詳細（Windowsサービスアカウントのsysadminロールへの追加を含む）については、Microsoftのドキュメントを参照してください。この構成では、ControllerはNetwork Serviceアカウントを使用します。Controllerには、追加のSQL Serverロールや権限は必要ありません。

必要に応じて、データベースインスタンスの**インスタンスを非表示**を選択できます。Web Studioでデータベースのアドレスを構成するときは、インスタンス名ではなく、インスタンスの静的ポート番号を入力します。SQL Serverデータベースエンジンのインスタンスを非表示にする方法の詳細については、Microsoftのドキュメントを参照してください。

ほとんどの運用環境の展開、およびMicrosoftの高可用性機能を使用するすべての展開では、サポートされている非ExpressエディションのSQL Serverのみを使用することをお勧めします。最初のControllerがインストールされているサーバー以外のマシンにSQL Serverをインストールしま

す。システム要件には、サポートされているSQL Serverのバージョンが一覧表示されています。データベースは1台以上のマシンに配置できます。

サイトを作成する前にSQL Serverソフトウェアがインストールされていることを確認してください。データベースを作成する必要はありませんが、作成する場合は空である必要があります。Microsoftの高可用性テクノロジーの構成も推奨されます。

Windows Updateを使用してSQL Serverを最新の状態に保ちます。

サイト作成ウィザードからデータベースをセットアップする

サイト作成ウィザードの**データベース**ページで、データベース名とアドレス（場所）を指定します。（データベースアドレス形式を参照してください。）DirectorがMonitor Serviceを照会する際の潜在的なエラーを避けるため、監視データベースの名前に空白を使用しないでください。

データベースページでは、データベースをセットアップするための2つのオプション（自動とスクリプトの使用）が提供されます。一般的に、必要なデータベース権限がある場合（Web Studioユーザーおよびcitrix管理者）、自動オプションを使用できます。（データベースのセットアップに必要な権限を参照してください。）

サイトを作成した後で、構成ログおよび監視データベースの場所を後で変更できます。「データベースの場所を変更する」を参照してください。

ミラーデータベースを使用するようにサイトを構成するには、以下を完了してから、自動またはスクリプトによるセットアップ手順に進みます。

1. 2台のサーバー（AとB）にSQL Serverソフトウェアをインストールします。
2. サーバーAで、プライマリとして使用するデータベースを作成します。サーバーAでデータベースをバックアップし、サーバーBにコピーします。
3. サーバーBで、バックアップファイルを復元します。
4. サーバーAでミラーリングを開始します。

サイト作成後にミラーリングを確認するには、PowerShell コマンドレット `get-configdbconnection` を実行して、接続文字列にミラーへのフェールオーバーパートナーが設定されていることを確認します。

ミラーリングされたデータベース環境で後からDelivery Controllerを追加、移動、または削除する場合は、「Delivery Controllers」を参照してください。

自動セットアップ

必要なデータベース権限がある場合は、次の手順でデータベースをセットアップします。

1. サイト作成ウィザードの**データベース**ページで、**Studioからデータベースを作成およびセットアップ**を選択します。
2. プライマリデータベースの名前とアドレスを指定します。
3. データベース接続設定のセキュリティと柔軟性を向上させるために、以下のSQL Server接続オプションを構成します。

   - **暗号化**: 接続の暗号化レベルを指定します。
   - **サーバー証明書を信頼する**: サーバー証明書の検証をバイパスするには、これを選択します。
   - **証明書のホスト名**: サーバーの証明書が一致する必要があるホスト名を入力します。この設定により、より厳格な証明書検証が保証されます。

   詳細については、このMicrosoft記事を参照してください。

指定したアドレスにデータベースが存在する場合、そのデータベースは空である必要があります。指定したアドレスにデータベースが存在しない場合、データベースが見つからないことが通知され、データベースを作成するかどうかを尋ねられます。その操作を確定すると、Web Studioは自動的にデータベースを作成し、プライマリデータベースとレプリカデータベースの初期化スクリプトを適用します。

スクリプトによるセットアップ

必要なデータベース権限がない場合は、データベース管理者など、権限を持つ人に支援を依頼してください。手順は次のとおりです。

1. サイト作成ウィザードの ページで、 を選択します。この操作により、サイト、監視、ログの各データベースについて、プライマリデータベースとレプリカデータベースごとに次の3種類のスクリプトが生成されます。

   - *名前に「SysAdmin」を含むスクリプト*。データベースとDelivery Controllerのログインを作成するスクリプトです。これらのタスクにはsecurityadmin権限が必要です。
   - *名前に「DbOwner」を含むスクリプト*。データベースにユーザーロールを作成し、ログインを追加し、データベーススキーマを作成するスクリプトです。これらのタスクには `db_owner` 権限が必要です。
   - *名前に「Mixed」を含むスクリプト*。必要な権限に関係なく、すべてのタスクを1つのスクリプトにまとめたものです。

   スクリプトの保存場所を指定できます。

> **注:**
>
> エンタープライズ環境では、データベースのセットアップには、異なる役割（権限）を持つ異なるチームによって処理される可能性のあるスクリプトが含まれます。`securityadmin`または`db_owner`。該当する場合、まず`securityadmin`ロールを持つ管理者によって「SysAdmin」スクリプトを実行し、次に`db_owner`権限を持つ管理者によって「DbOwner」スクリプトを実行します。これらのスクリプトを生成するには、PowerShellを使用することもできます。詳細については、推奨されるデータベース権限スクリプトを参照してください。

2. これらのスクリプトをデータベース管理者に渡します。サイト作成ウィザードは、この時点で自動的に停止します。後で戻ってサイト作成を続行するときに、プロンプトが表示されます。

データベース管理者は、データベースを作成します。各データベースには、次の特性が必要です。

- `_CI_AS_KS`で終わる照合順序を使用します。`_100_CI_AS_KS`で終わる照合順序を使用することをお勧めします。
- 最高のパフォーマンスを得るには、SQL ServerのRead-Committed Snapshotを有効にします。詳細については、「CTX 137161」を参照してください。
- 該当する場合は、高可用性機能が構成されていること。
- ミラーリングを構成するには、まずデータベースを完全復旧モデルを使用するように設定します（シンプルモデルがデフォルトです）。プライマリデータベースをファイルにバックアップし、ミラーサーバーにコピーします。次に、ミラーサーバーでバックアップファイルを復元します。最後に、プライマリサーバーでミラーリングを開始します。

データベース管理者は、SQLCMD コマンドラインユーティリティまたは SQLCMD モードの SQL Server Management Studio を使用して、次の操作を実行します。

- 高可用性 SQL Server データベースインスタンスで `xxx_Replica.sql` スクリプトをそれぞれ実行します (高可用性が構成されている場合)。
- プリンシパル SQL Server データベースインスタンスで `xxx\_Principal.sql` スクリプトをそれぞれ実行します。

SQLCMD の詳細については、Microsoft のドキュメントを参照してください。

すべてのスクリプトが正常に完了したら、データベース管理者はCitrix管理者に3つのプライマリデータベースアドレスを渡します。

Web Studio はサイト作成を続行するように求めます。**データベース**ページに戻り、次の手順を完了します。

1. アドレスを入力します。
2. データベース接続設定のセキュリティと柔軟性を向上させるために、次の SQL Server 接続オプションを構成します。

   - **暗号化**: 接続の暗号化レベルを指定します。
   - **サーバー証明書を信頼する**: サーバー証明書の検証をバイパスするには、これを選択します。
   - **証明書のホスト名**: サーバーの証明書が一致する必要があるホスト名を入力します。この設定により、より厳格な証明書検証が保証されます。

   詳細については、このMicrosoft記事を参照してください。

データベースをホストしているサーバーのいずれかに接続できない場合、エラーメッセージが表示されます。

データベースのセットアップに必要な権限

データベースを作成および初期化する（またはデータベースの場所を変更する）には、ローカル管理者およびドメインユーザーである必要があります。また、特定のSQL Server権限も必要です。以下の権限は、Active Directoryグループメンバーシップによって明示的に構成または取得できます。Web Studioのユーザー資格情報にこれらの権限が含まれていない場合、SQL Serverのユーザー資格情報の入力を求められます。

操作	目的	サーバーロール	データベースロール
データベースの作成	適切な空のデータベースを作成する	`dbcreator`	
スキーマの作成	すべてのサービス固有のスキーマを作成し、最初のControllerをサイトに追加する	`securityadmin` *	`db_owner`
コントローラーを追加	サイトにコントローラー（最初のコントローラー以外）を追加	`securityadmin` *	`db_owner`

操作	目的	サーバーロール	データベースロール
コントローラー（ミラーサーバー）を追加	ミラーデータベースのミラーロールにあるデータベースサーバーにコントローラーログインを追加	`securityadmin` *	
コントローラーを削除	サイトからコントローラーを削除	**	`db_owner`
スキーマを更新	スキーマの更新またはホットフィックスを適用		`db_owner`

* 技術的にはより制限的ですが、実際には、`securityadmin` サーバーロールを `sysadmin` サーバーロールと同等として扱うことができます。

** コントローラーがサイトから削除されても、データベースサーバーへのコントローラーのログオンは削除されません。これは、同じマシン上のこのCitrix製品以外のサービスで使用されているログオンが誤って削除されるのを防ぐためです。ログオンが不要になった場合は、手動で削除する必要があります。この操作には、`securityadmin` サーバーロールのメンバーシップが必要です。

Web Studio を使用してこれらの操作を実行する場合、Web Studio ユーザーは、適切なサーバーロールのメンバーであるデータベースサーバーアカウントを持っているか、またはそのアカウントの資格情報を提供できる必要があります。

優先データベース権限スクリプト

エンタープライズ環境では、データベースのセットアップには、異なる役割（権限）を持つ異なるチームが処理する必要があるスクリプトが含まれます。`securityadmin` または `db_owner`。

PowerShell を使用して、推奨されるデータベース権限を指定できます。デフォルト以外の値を指定すると、個別のスクリプトが作成されます。一方のスクリプトには `securityadmin` ロールが必要なタスクが含まれます。もう一方のスクリプトは `db_owner` 権限のみを必要とし、データベース管理者に連絡することなく Citrix 管理者が実行できます。

`get-*DBSchema` コマンドレットでは、`-DatabaseRights` オプションには次の有効な値があります。

- `SA`: データベースと Delivery Controller のログインを作成するスクリプトを生成します。これらのタスクには `securityadmin` 権限が必要です。
- `DBO`: データベースにユーザーロールを作成し、ログインを追加し、データベーススキーマを作成するスクリプトを生成します。これらのタスクには `db_owner` 権限が必要です。
- `Mixed`: (デフォルト) 必要な権限に関係なく、すべてのタスクを1つのスクリプトにまとめます。

詳細については、コマンドレットのヘルプを参照してください。

データベースアドレスの形式

データベースアドレスは、次のいずれかの形式で指定できます。

- `ServerName`
- `ServerName\InstanceName`
- `ServerName,PortNumber`

AlwaysOn可用性グループの場合は、場所フィールドにグループのリスナーを指定します。

データベースの場所を変更する

サイトを作成した後、*構成ログ*データベースと*監視*データベースの場所を変更できます。ただし、*サイト*データベースの場所は変更できません。データベースの場所を変更する際は、次の点に注意してください。

- 以前のデータベースのデータは、新しいデータベースにはインポートされません。
- ログを取得する際、両方のデータベースからログを集約することはできません。
- 新しいデータベースの最初のログエントリは、データベースの変更が発生したことを示しますが、以前のデータベースを特定するものではありません。
- 強制ログが有効になっている場合、構成ログデータベースの場所を変更することはできません。
- SQL ServerとAzure SQLの間でデータベースの場所を変更することはサポートされていません。

データベースの場所を変更するには：

1. Microsoft SQL Serverを使用している場合は、データベースを配置するサーバーにサポートされているバージョンがインストールされていることを確認してください。必要に応じて、高可用性機能をセットアップします。

2. Web Studioにサインインし、左側のペインで を選択します。
3. タイルを見つけて を選択します。
4. ページで、新しい場所を指定するデータベースを選択し、アクションバーで を選択します。
5. 新しい場所とデータベース名を指定します。データベースがAzure SQLでホストされている場合は、データベースを管理する権限を持つサービスプリンシパルの資格情報を入力します。
6. Web Studioにデータベースを作成させたい場合で、適切な権限がある場合は、**完了**をクリックします。プロンプトが表示されたら、**完了**をクリックすると、Web Studioが自動的にデータベースを作成します。Web Studioは、ユーザーの資格情報を使用してデータベースへのアクセスを試みます。それが失敗した場合は、データベースユーザーの資格情報の入力を求められます。その後、Web Studioはデータベーススキーマをデータベースにアップロードします。資格情報は、データベース作成期間中のみ保持されます。
7. Web Studioにデータベースを作成させたくない場合、または十分な権限がない場合は、**データベーススクリプトの生成**をクリックします。生成されたスクリプトには、必要に応じてデータベースとミラーデータベースを手動で作成するための手順が含まれています。スキーマをアップロードする前に、データベースが空であり、少なくとも1人のユーザーがデータベースにアクセスして変更する権限を持っていることを確認してください。

詳細情報

- データベースサイジングツール。
- SQL Serverの高可用性ソリューションを使用する場合のサイトデータベースのサイジングと接続文字列の構成。

配信方法

Citrix Virtual Apps and Desktops™は、さまざまな配信方法を提供します。単一の配信方法では、すべての要件を満たせない可能性があります。

はじめに

適切なアプリケーション配信方法を選択することで、スケーラビリティ、管理性、ユーザーエクスペリエンスの向上に役立ちます。

- **インストール済みアプリ:** アプリケーションはベースデスクトップイメージの一部です。インストールプロセスには、レジストリの変更に加えて、dll、exe、およびその他のファイルがイメージドライブにコピーされます。詳しくは、「マシンカタログの作成」を参照してください。

- **ストリーミングアプリ（Microsoft App-V）：** アプリケーションはプロファイルされ、オンデマンドでネットワーク経由でデスクトップに配信されます。アプリケーションファイルとレジストリ設定は、仮想デスクトップ上のコンテナに配置され、ベースオペレーティングシステムおよび相互から分離されます。この分離により、互換性の問題に対処できます。詳しくは、「App-Vアプリケーションの展開と配信」を参照してください。
- **レイヤー化されたアプリ（Citrix App Layering）：** 各レイヤーには、単一のアプリケーション、エージェント、またはオペレーティングシステムが含まれています。1つのOSレイヤー、1つのプラットフォームレイヤー（VDA、Citrix Provisioningエージェント）、および多数のアプリケーションレイヤーを統合することで、管理者は新しい展開可能なイメージを簡単に作成できます。レイヤー化により、OS、エージェント、およびアプリケーションが単一のレイヤーに存在するため、継続的なメンテナンスが簡素化されます。レイヤーを更新すると、そのレイヤーを含むすべての展開済みイメージが更新されます。詳しくは、「Citrix App Layering」を参照してください。
- **ホスト型Windowsアプリ：** マルチユーザーのCitrix Virtual Appsホストにインストールされ、デスクトップではなくアプリケーションとして展開されるアプリケーションです。ユーザーは、VDIデスクトップまたはエンドポイントデバイスからホスト型Windowsアプリにシームレスにアクセスでき、アプリがリモートで実行されているという事実を意識することはありません。詳しくは、「デリバリーグループの作成」を参照してください。
- **ローカルアプリ：** エンドポイントデバイスに展開されるアプリケーションです。アプリケーションはエンドポイントで実行されますが、そのインターフェイスはユーザーのホスト型VDIセッション内に表示されます。詳しくは、「ローカルアプリアクセスとURLリダイレクト」を参照してください。

デスクトップについては、公開デスクトップまたはVDIデスクトップを検討してください。

Citrix Virtual Apps™の公開アプリとデスクトップ

マルチセッションOSマシンを使用して、Citrix Virtual Apps and Desktops公開アプリと公開デスクトップを配信します。

ユースケース：

- 多くのユーザーにアプリケーションを配信するコストを最小限に抑えながら、安全で高精細なユーザーエクスペリエンスを提供するために、安価なサーバーベースの配信を希望する場合。
- ユーザーが明確に定義されたタスクを実行し、パーソナライズやアプリケーションへのオフラインアクセスを必要としない場合。ユーザーには、コールセンターオペレーターや小売店員などのタスクワーカー、またはワークステーションを共有するユーザーが含まれます。
- アプリケーションの種類: 任意のアプリケーション。

利点と考慮事項:

- データセンター内で管理可能でスケーラブルなソリューション。
- 最も費用対効果の高いアプリケーション配信ソリューション。
- ホストされたアプリケーションは一元的に管理され、ユーザーはアプリケーションを変更できません。これにより、一貫性があり、安全で、信頼性の高いユーザーエクスペリエンスが提供されます。
- ユーザーはアプリケーションにアクセスするためにオンラインである必要があります。

ユーザーエクスペリエンス:

- ユーザーは、StoreFront™、**スタート**メニュー、または提供されたURLから1つ以上のアプリケーションを要求します。
- アプリケーションは仮想的に配信され、ユーザーデバイス上で高解像度でシームレスに表示されます。
- プロファイル設定に応じて、ユーザーのアプリケーションセッションが終了するとユーザーの変更が保存されます。それ以外の場合、変更は削除されます。

アプリケーションの処理、ホスト、および配信:

- アプリケーション処理は、ユーザーデバイス上ではなく、ホスティングマシンで行われます。ホスティングマシンは、物理マシンまたは仮想マシンにすることができます。
- アプリケーションとデスクトップはマルチセッションOSマシンに存在します。
- マシンはマシンカタログを通じて利用可能になります。
- マシンカタログからのマシンは、同じアプリケーションセットをユーザーグループに配信するデリバリーグループに編成されます。
- マルチセッションOSマシンは、デスクトップまたはアプリケーション、あるいはその両方をホストするデリバリーグループをサポートします。

セッション管理と割り当て:

- マルチセッションOSマシンは、1台のマシンから複数のセッションを実行し、複数の同時接続ユーザーに複数のアプリケーションとデスクトップを配信します。各ユーザーは、すべてのホスト型アプリケーションを実行できる単一のセッションを必要とします。

  たとえば、ユーザーがログオンしてアプリケーションを要求すると、そのマシン上の1つのセッションは他のユーザーには利用できなくなります。2人目のユーザーがログオンし、そのマシンがホストするアプリケーションを要求すると、同じマシン上の2つ目のセッションも利用できなくなります。両方のユーザーがさらにアプリケーションを要求しても、ユーザーは同

じセッションを使用して複数のアプリケーションを実行できるため、追加のセッションは必要ありません。さらに2人のユーザーがログオンしてデスクトップを要求し、同じマシンで2つのセッションが利用可能な場合、その単一のマシンは4つのセッションを使用して4人の異なるユーザーをホストしていることになります。

- ユーザーが割り当てられているデリバリーグループ内で、最も負荷の低いサーバー上のマシンが選択されます。セッションが利用可能なマシンは、ユーザーがログオンしたときに、そのユーザーにアプリケーションを配信するためにランダムに割り当てられます。

VMホスト型アプリ

シングルセッションOSマシンを使用してVMホスト型アプリケーションを配信します

ユースケース:

- 安全で、一元管理を提供し、ホストサーバーあたり多数のユーザーをサポートするクライアントベースのアプリケーション配信ソリューションを求めているとします。これらのユーザーに、高解像度でシームレスに表示されるアプリケーションを提供したいと考えています。
- ユーザーは、社内ユーザー、外部請負業者、サードパーティの共同作業者、およびその他の暫定的なチームメンバーです。ユーザーは、ホストされているアプリケーションへのオフラインアクセスを必要としません。
- アプリケーションの種類: 他のアプリケーションとうまく連携しない可能性のあるアプリケーションや、Microsoft .NET Frameworkのようにオペレーティングシステムと相互作用する可能性のあるアプリケーション。これらの種類のアプリケーションは、仮想マシンでのホスティングに最適です。

利点と考慮事項:

- マスターイメージ上のアプリケーションとデスクトップは、データセンター内のマシンで安全に管理、ホスト、実行され、より費用対効果の高いアプリケーション配信ソリューションを提供します。
- ログオン時に、ユーザーは同じアプリケーションをホストするように構成されたデリバリーグループ内のマシンにランダムに割り当てることができます。また、ユーザーがログオンするたびに、単一のマシンを単一のユーザーにアプリケーションを配信するように静的に割り当てることもできます。静的に割り当てられたマシンでは、ユーザーは仮想マシンに独自のアプリケーションをインストールして管理できます。
- シングルセッションOSマシンでは、複数のセッションの実行はサポートされていません。したがって、各ユーザーはログオン時にデリバリーグループ内の単一のマシンを消費し、ユーザーはアプリケーションにアクセスするためにオンラインである必要があります。

- この方法により、アプリケーション処理用のサーバーリソースの量と、ユーザーデータ用のストレージの量を増やすことができます。

ユーザーエクスペリエンス：

- マルチセッションOSマシンで共有アプリケーションをホストする場合と同様の、シームレスなアプリケーションエクスペリエンス。

アプリケーションの処理、ホスト、および配信：

- 仮想シングルセッションOSマシンである点を除けば、マルチセッションOSマシンと同じです。

セッション管理と割り当て：

- シングルセッションOSマシンは、単一のマシンから単一のデスクトップセッションを実行します。アプリケーションのみにアクセスする場合、オペレーティングシステムは各アプリケーションを新しいセッションと見なすため、単一ユーザーは複数のアプリケーションを使用できます（単一のアプリケーションに限定されません）。
- デリバリーグループ内で、ユーザーがログオンすると、静的に割り当てられたマシン（ユーザーがログオンするたびに同じマシン）またはセッションの可用性に基づいて選択されるランダムに割り当てられたマシンのいずれかにアクセスできます。

VDIデスクトップ

シングルセッションOSマシンを使用して、Citrix Virtual Apps and Desktops VDIデスクトップを配信します。

VDIデスクトップは仮想マシンでホストされ、各ユーザーにデスクトップオペレーティングシステムを提供します。

VDIデスクトップは、公開デスクトップよりも多くのリソースを必要としますが、インストールされているアプリケーションがサーバーベースのオペレーティングシステムをサポートする必要はありません。また、選択するVDIデスクトップの種類に応じて、これらのデスクトップを個々のユーザーに割り当てることができます。これにより、ユーザーは高度なパーソナライズが可能になります。

VDIデスクトップ用のマシンカタログを作成するときは、次のいずれかの種類のデスクトップを作成します。

- **ランダム非永続デスクトップ（プールされたVDIデスクトップとも呼ばれる）：** ユーザーがこれらのデスクトップのいずれかにログオンするたびに、そのユーザーはデスクトップのプール

から選択されたデスクトップに接続します。このプールは単一のマスターイメージに基づいています。マシンの再起動時に、デスクトップへのすべての変更は失われます。

- **静的非永続デスクトップ：** 最初のログオン時に、ユーザーはデスクトップのプールからデスクトップを割り当てられます。（プール内の各マシンは単一のマスターイメージに基づいています。）最初の使用後、ユーザーがデスクトップを使用するためにログオンするたびに、そのユーザーは最初の使用時に割り当てられた同じデスクトップに接続します。マシンの再起動時に、デスクトップへのすべての変更は失われます。
- **静的永続デスクトップ:** 他の種類のVDIデスクトップとは異なり、ユーザーはこれらのデスクトップを完全にパーソナライズできます。最初のログオン時に、ユーザーはデスクトッププールからデスクトップを割り当てられます。そのユーザーによるその後のログオンは、初回使用時に割り当てられたのと同じデスクトップに接続します。デスクトップへの変更は、マシンが再起動しても保持されます。

リモートPCアクセス

Remote PC Accessは、Citrix Virtual Apps and Desktopsの機能であり、組織が従業員に企業リソースへのリモートアクセスを安全な方法で簡単に許可できるようにします。Citrixプラットフォームは、ユーザーが物理的なオフィスPCにアクセスできるようにすることで、この安全なアクセスを可能にします。ユーザーがオフィスPCにアクセスできれば、仕事に必要なすべてのアプリケーション、データ、リソースにアクセスできます。Remote PC Accessは、テレワークに対応するための他のツールの導入と提供の必要性を排除します。たとえば、仮想デスクトップやアプリケーション、およびそれらに関連するインフラストラクチャなどです。

Remote PC Accessは、仮想デスクトップとアプリケーションを提供するCitrix Virtual Apps and Desktopsと同じコンポーネントを使用します。その結果、Remote PC Accessの展開と構成の要件およびプロセスは、仮想リソースを提供するためのCitrix Virtual Apps and Desktopsの展開に必要なものと同じです。この統一性により、一貫性のある統合された管理エクスペリエンスが提供されます。ユーザーは、Citrix HDX™を使用してオフィスPCセッションを配信することで、最高のユーザーエクスペリエンスを得られます。

詳細については、リモートPCアクセス。

ネットワークポート

完全なネットワークポート情報は、Citrix Technologies で使用される通信ポートに記載されています。

Citrix®コンポーネントがインストールされると、オペレーティングシステムのホストファイアウォールも、デフォルトで、デフォルトのネットワークポートに一致するように更新されます。

ポート情報が必要になる場合があります。

- 規制遵守のため。
- Citrix Virtual Apps and Desktops™コンポーネントと他のCitrix製品またはコンポーネントの間にネットワークファイアウォールがある場合、そのファイアウォールを適切に構成できるようにするため。
- オペレーティングシステムのホストファイアウォールではなく、アンチマルウェアパッケージに付属しているものなど、サードパーティのホストファイアウォールを使用する場合。
- これらのコンポーネント（通常はWindowsファイアウォールサービス）のホストファイアウォールの構成を変更する場合。
- コンポーネント機能を再構成して別のポートまたはポート範囲を使用し、その構成で使用されていないポートを無効にするかブロックする場合。

一部のポートは、Internet Assigned Numbers Authority (IANA) に登録されています。これらの割り当てに関する詳細は`<http://www.iana.org/assignments/port-numbers>`で入手できます。ただし、IANAが保持する記述情報は、必ずしも今日の使用状況を反映しているわけではありません。

また、VDA および Delivery Controller™ 上のオペレーティングシステムは、独自の用途のために受信ポートを必要とします。詳細については、Microsoft Windows のドキュメントを参照してください。

HDX™

> **警告:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になる深刻な問題が発生する可能性があります。Citrix® は、レジストリエディターの誤った使用によって生じた問題が解決されることを保証できません。レジストリエディターは、お客様ご自身の責任においてご使用ください。編集する前に、必ずレジストリをバックアップしてください。

> Citrix HDX は、あらゆるデバイスおよびネットワーク上で、集中管理されたアプリケーションとデスクトップのユーザーに高精細なエクスペリエンスを提供する幅広いテクノロジーのセットです。

仮想チャネル(/en-us/citrix-virtual-apps-desktops/2511/media/hdx-vir-channels.png)

HDXは、次の3つの技術原則に基づいて設計されています。

- インテリジェントなリダイレクト
- 適応型圧縮
- データ重複排除

これらをさまざまな組み合わせで適用することで、ITおよびユーザーエクスペリエンスを最適化し、帯域幅の消費を削減し、ホスティングサーバーあたりのユーザー密度を向上させます。

- **インテリジェントなリダイレクト** - インテリジェントなリダイレクトは、画面アクティビティ、アプリケーションコマンド、エンドポイントデバイス、ネットワークおよびサーバーの機能を検査し、アプリケーションまたはデスクトップのアクティビティをいつ、どこでレンダリングするかを即座に判断します。レンダリングは、エンドポイントデバイスまたはホスティングサーバーのいずれかで実行できます。
- **適応型圧縮** - 適応型圧縮により、リッチなマルチメディアディスプレイを低帯域幅のネットワーク接続で配信できます。HDX はまず、入力、デバイス、ディスプレイの種類（テキスト、ビデオ、音声、マルチメディア）など、いくつかの変数を評価します。最適な圧縮コーデックと、CPU および GPU の最適な使用比率を選択します。その後、各固有のユーザーと状況に基づいてインテリジェントに適応します。このインテリジェントな適応は、ユーザーごと、またはセッションごとに行われます。

  適応型圧縮(/en-us/citrix-virtual-apps-desktops/2511/media/hdx-adaptive-compression.png)
- **データ重複排除** - ネットワークトラフィックの重複排除は、クライアントとサーバー間で送信される集約データを削減します。これは、ビットマップグラフィック、ドキュメント、印刷ジョブ、ストリーミングメディアなど、一般的にアクセスされるデータ内の繰り返されるパターンを利用することで実現されます。これらのパターンをキャッシュすることで、変更のみがネットワーク経由で送信され、重複するトラフィックが排除されます。HDX は、マルチメディアストリームのマルチキャストもサポートしています。これは、各ユーザーとの 1 対 1 の接続ではなく、ソースからの単一の送信が 1 つの場所で複数のサブスクライバーによって表示されるものです。

詳細については、「高精細なユーザーワークスペースで生産性を向上」を参照してください。

デバイス上

HDXは、ユーザーエクスペリエンスを向上および最適化するために、ユーザーデバイスのコンピューティング能力を使用します。HDXテクノロジーにより、ユーザーは仮想デスクトップまたはアプリケーションでマルチメディアコンテンツをスムーズかつシームレスに利用できます。ワーク

スペースコントロールを使用すると、ユーザーは仮想デスクトップとアプリケーションを一時停止し、中断した時点から別のデバイスで作業を再開できます。

ネットワーク上

HDXは、低帯域幅および高遅延のWAN接続を含むあらゆるネットワーク上で最高のパフォーマンスを提供するために、高度な最適化および高速化機能を組み込んでいます。

HDXの機能は、環境の変化に適応します。これらの機能は、パフォーマンスと帯域幅のバランスを取ります。デスクトップまたはアプリケーションが社内ネットワークでローカルにアクセスされるか、企業ファイアウォールの外部からリモートでアクセスされるかにかかわらず、各ユーザーシナリオに最適なテクノロジーを適用します。

データセンター内

HDXは、クライアントデバイスの機能に関係なく、サーバーの処理能力とスケーラビリティを使用して、高度なグラフィックパフォーマンスを提供します。

Citrix Directorによって提供されるHDXチャネル監視は、ユーザーデバイス上の接続されたHDXチャネルのステータスを表示します。

HDX インサイト

HDX Insightは、NetScaler® Network InspectorとPerformance ManagerをDirectorと統合したものです。ICAトラフィックに関するデータを取得し、リアルタイムおよび履歴の詳細のダッシュボードビューを提供します。このデータには、クライアント側およびサーバー側のICAセッション遅延、ICAチャネルの帯域幅使用量、および各セッションのICAラウンドトリップタイム値が含まれます。

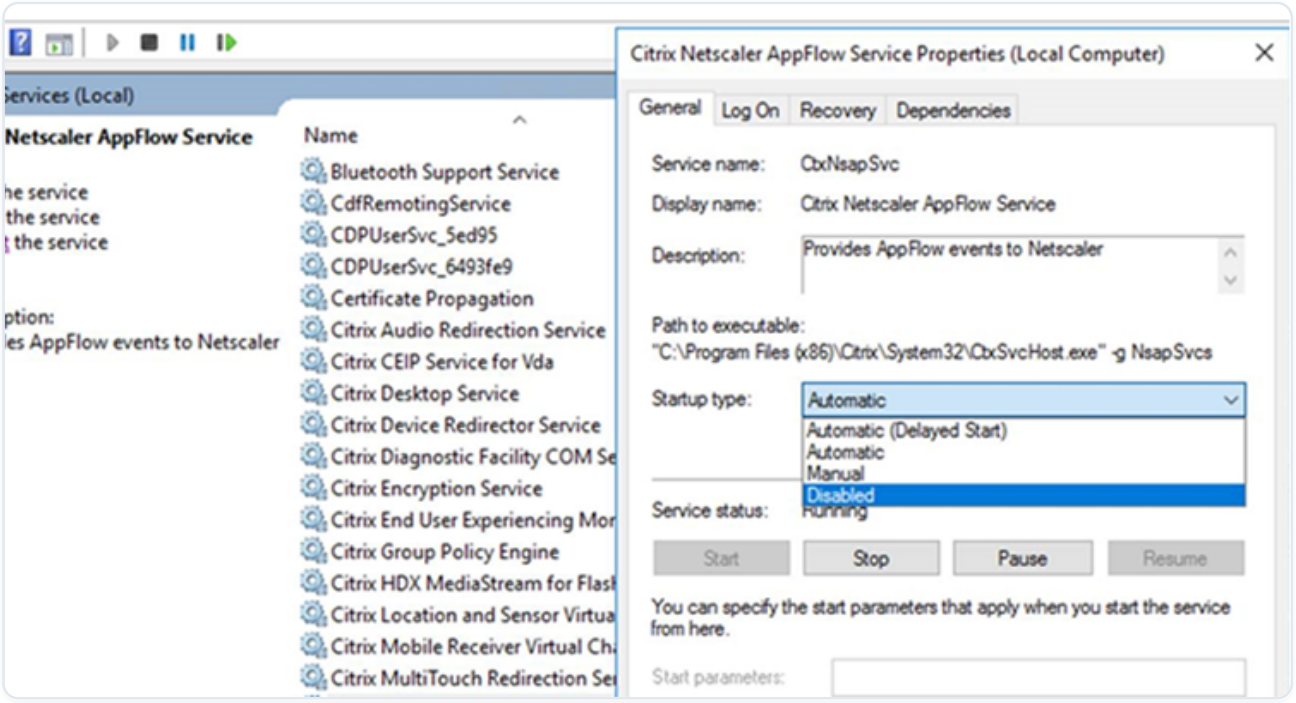
NetScalerでHDX Insight仮想チャネルを使用して、必要なすべてのデータポイントを非圧縮形式で移動させることができます。この機能を無効にすると、NetScalerデバイスは、さまざまな仮想チャネルに分散されたICA®トラフィックを復号化および解凍します。単一の仮想チャネルを使用することで、複雑さが軽減され、スケーラビリティが向上し、費用対効果が高まります。

最小要件:

- NetScalerバージョン 12.0 ビルド 57.x
- Citrix Workspace™ アプリ (Windows版) 1808
- シトリックス レシーバー Windows版 4.10
- Mac用Citrix Workspaceアプリ 1808
- Mac用 シトリックス レシーバー 12.8

HDX Insight仮想チャネルの有効化または無効化

この機能を無効にするには、Citrix NetScaler Application Flowサービスのプロパティを「Disabled」に設定します。有効にするには、サービスを「Automatic」に設定します。いずれの場合も、これらのプロパティを変更した後は、サーバーマシンを再起動することをお勧めします。デフォルトでは、このサービスは有効（Automatic）になっています。



仮想デスクトップからHDX機能を利用する

- ブラウザコンテンツリダイレクト（4つのHDXマルチメディアリダイレクトテクノロジーの1つ）が、HTML5およびWebRTCマルチメディアコンテンツの配信をどのように高速化するかを確認するには：

  a. Chromeブラウザ拡張機能をダウンロードし、仮想デスクトップにインストールします。

  b. ブラウザコンテンツリダイレクトが仮想デスクトップへのマルチメディアコンテンツの配信をどのように高速化するかを体験するには、YouTubeなどのHTML5ビデオを含むウェブサイトから、デスクトップでビデオを視聴します。ユーザーは、ブラウザコンテンツリダイレクトが実行されていることを知りません。ブラウザコンテンツリダイレクトが使用されているかどうかを確認するには、ブラウザウィンドウを素早くドラッグします。ビューポートとユーザーインターフェイスの間に遅延またはフレーム外の表示が見られます。ウェブページを右クリックして、メニューから**About HDX Browser Redirection**を探すこともできます。

- HDXが高品位オーディオをどのように配信するかを確認するには：

a. Citrixクライアントを最高のオーディオ品質に設定します。詳細については、Citrix Workspaceアプリのドキュメントを参照してください。

b. デスクトップでデジタルオーディオプレーヤー（iTunesなど）を使用して音楽ファイルを再生します。

HDXは、デフォルトでほとんどのユーザーに優れたグラフィックとビデオ体験を提供し、設定は不要です。ほとんどのユースケースで最高の体験を提供するCitrixポリシー設定は、デフォルトで有効になっています。

- HDXは、クライアント、プラットフォーム、アプリケーション、ネットワーク帯域幅に基づいて最適な配信方法を自動的に選択し、変化する条件に基づいて自己調整します。
- HDXは、2Dおよび3Dグラフィックとビデオのパフォーマンスを最適化します。
- HDXを使用すると、ユーザーデバイスは、ホストサーバーを介さずに、インターネットまたはイントラネット上のソースプロバイダーからマルチメディアファイルを直接ストリーミングできます。このクライアント側コンテンツフェッチの要件が満たされない場合、メディア配信はサーバー側コンテンツフェッチとマルチメディアリダイレクトにフォールバックします。通常、マルチメディアリダイレクト機能ポリシーの調整は必要ありません。
- マルチメディアリダイレクトが利用できない場合、HDXはリッチなサーバーレンダリングビデオコンテンツを仮想デスクトップに配信します。たとえば、`<http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/>`のような高解像度ビデオを含むWebサイトでビデオを視聴できます。

知っておくと良いこと：

- HDX機能のサポートと要件については、システム要件の記事を参照してください。特に明記されていない限り、HDX機能はサポートされているWindowsマルチセッションOSおよびWindowsシングルセッションOSマシン、およびRemote PC Accessデスクトップで利用できます。
- このコンテンツでは、ユーザーエクスペリエンスを最適化し、サーバーのスケーラビリティを向上させ、帯域幅要件を削減する方法について説明します。Citrixポリシーとポリシー設定の使用方法については、このリリースのCitrixポリシードキュメントを参照してください。
- レジストリの編集を含む手順については、注意して使用してください。レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

自動クライアント再接続とセッションの信頼性

ホストされたアプリケーションまたはデスクトップにアクセスしているときに、ネットワークの中断が発生する場合があります。よりスムーズな再接続を体験するために、自動クライアント再接続とセッションの信頼性を提供しています。デフォルトの構成では、セッションの信頼性が開始され、その後、自動クライアント再接続が続きます。

自動クライアント再接続：

自動クライアント再接続は、切断されたセッションに再接続するためにクライアントエンジンを再起動します。自動クライアント再接続は、設定で指定された時間の経過後にユーザーセッションを閉じ（または切断し）ます。自動クライアント再接続が進行中の場合、システムは次のようにアプリケーションおよびデスクトップのネットワーク中断通知をユーザーに送信します。

- **デスクトップ。** セッションウィンドウがグレー表示され、再接続までの時間を表示するカウントダウンタイマーが表示されます。
- **アプリケーション。** セッションウィンドウが閉じ、再接続が試行されるまでの時間を表示するカウントダウンタイマーを含むダイアログがユーザーに表示されます。

自動クライアント再接続中、セッションはネットワーク接続を期待して再起動します。自動クライアント再接続が進行中の間、ユーザーはセッションを操作できません。

再接続時、切断されたセッションは保存された接続情報を使用して再接続します。ユーザーは通常どおりアプリケーションとデスクトップを操作できます。

デフォルトの自動クライアント再接続設定：

- 自動クライアント再接続タイムアウト: 120秒
- 自動クライアント再接続: 有効
- 自動クライアント再接続認証: 無効
- 自動クライアント再接続ログ記録: 無効

詳細については、(/ja-jp/citrix-virtual-apps-desktops/2511/policies/reference/ica-policy-settings/auto-client-reconnect-policy-settings.html)のを参照してください。

セッションの信頼性:

セッションの信頼性により、ネットワークの中断があってもICAセッションがシームレスに再接続されます。セッションの信頼性は、設定で指定された時間の経過後にユーザーセッションを閉じ（または切断し）ます。セッションの信頼性タイムアウト後、自動クライアント再接続設定が有効になり、切断されたセッションへのユーザーの再接続が試行されます。セッションの信頼性が

進行中の場合、アプリケーションとデスクトップのネットワーク中断通知は次のようにユーザーに送信されます。

- **デスクトップ。** セッションウィンドウが半透明になり、再接続までの時間がカウントダウンタイマーで表示されます。
- **アプリケーション。** ウィンドウが半透明になり、通知領域から接続中断のポップアップが表示されます。

セッションの信頼性がアクティブな間、ユーザーはICAセッションを操作できません。ただし、ネットワーク中断直後の数秒間は、キーストロークなどのユーザーアクションがバッファリングされ、ネットワークが利用可能になったときに再送信されます。

再接続すると、クライアントとサーバーはプロトコル交換の同じ時点から再開します。セッションウィンドウの半透明性がなくなり、アプリケーションには適切な通知領域のポップアップが表示されます。

デフォルトのセッションの信頼性設定

- セッションの信頼性タイムアウト: 180秒
- 再接続UIの不透明度レベル: 80%
- セッションの信頼性接続: 有効
- セッションの信頼性ポート番号: 2598

詳細については、セッションの信頼性ポリシー設定を参照してください。

自動クライアント再接続とセッションの信頼性を備えたNetScaler:

サーバーでマルチストリームおよびマルチポートポリシーが有効になっており、かつ以下の条件のいずれかまたはすべてが真である場合、自動クライアント再接続は機能しません。

- NetScaler Gatewayでセッションの信頼性が無効になっている。
- NetScalerアプライアンスでフェールオーバーが発生する。
- NetScaler SD-WANがNetScaler Gatewayとともに使用されている。

HDX アダプティブスループット

HDXアダプティブスループットは、出力バッファーを調整することで、ICAセッションのピークスループットをインテリジェントに微調整します。出力バッファーの数は、初期値として高い値に設定されます。この高い値により、特に高遅延ネットワークにおいて、データがより迅速かつ効率的にクライアントに送信されます。インタラクティブ性の向上、ファイル転送の高速化、ビデオ再生

のスムーズ化、フレームレートと解像度の向上により、ユーザーエクスペリエンスが強化されます。

ICAセッション内のデータストリームがインタラクティブ性に悪影響を与えているかどうかを判断するために、セッションのインタラクティブ性は常に測定されます。そのような場合、セッションへの大量データストリームの影響を軽減し、インタラクティブ性を回復させるためにスループットが低下します。

> **重要:**
>
> HDXアダプティブスループットは、出力バッファーの設定方法を変更し、このメカニズムをクライアントからVDAに移行するため、手動での構成は不要です。

この機能には、以下の要件があります。

- VDA バージョン 1811 以降
- Windows 用 Workspace アプリ 1811 以降

ユーザーデバイスに送信される画質の向上

以下の視覚表示ポリシー設定は、仮想デスクトップからユーザーデバイスに送信される画像の品質を制御します。

- 視覚品質。ユーザーデバイスに表示される画像の視覚品質を制御します: medium、high、always lossless、build to lossless (デフォルト = medium)。medium のデフォルト設定を使用した場合の実際のビデオ品質は、利用可能な帯域幅によって異なります。
- ターゲットフレームレート。仮想デスクトップからユーザーデバイスに送信される1秒あたりの最大フレーム数を指定します (デフォルト = 30)。CPU が遅いデバイスの場合、より低い値を指定することでユーザーエクスペリエンスを向上させることができます。1秒あたりの最大サポートフレームレートは 60 です。
- 表示メモリ制限。セッションの最大ビデオバッファーサイズをキロバイト単位で指定します (デフォルト = 65536 KB)。より多くの色深度と高い解像度を必要とする接続の場合、制限を増やしてください。必要な最大メモリを計算できます。

> **注:**

> 「**ディスプレイメモリ制限**」設定は廃止されました。この変更により、Citrixはディスプレイメモリを制限しなくなりました。代わりに、クライアントのディスプレイレイアウトが完全に収まるように、必要な最小限のメモリが割り当てられます。

ビデオ会議のパフォーマンスを向上させる

いくつかの一般的なビデオ会議アプリケーションは、マルチメディアリダイレクトを介したCitrix Virtual Apps and Desktopsからの配信に最適化されています (例: HDX RealTime Optimization Pack を参照)。最適化されていないアプリケーションの場合、HDXウェブカメラビデオ圧縮は、セッション中のビデオ会議におけるウェブカメラの帯域幅効率と遅延耐性を向上させます。このテクノロジーは、専用のマルチメディア仮想チャネルを介してウェブカメラトラフィックをストリーミングします。このテクノロジーは、アイソクロナスHDX Plug-n-Play USBリダイレクトサポートと比較して帯域幅の使用量が少なく、WAN接続でもうまく機能します。

Citrix Workspaceアプリのユーザーは、Desktop Viewerの「マイクとウェブカメラ」設定で**「マイクまたはウェブカメラを使用しない」**を選択することで、デフォルトの動作を上書きできます。ユーザーがHDXウェブカメラビデオ圧縮から切り替えるのを防ぐには、ICAポリシー設定 > USBデバイスポリシー設定の下にあるポリシー設定を使用して、USBデバイスリダイレクトを無効にします。

HDXウェブカメラビデオ圧縮には、以下のポリシー設定が有効になっている必要があります (すべてデフォルトで有効になっています)。

- クライアントオーディオリダイレクト
- クライアントマイクのリダイレクト
- マルチメディア会議

ウェブカメラがハードウェアエンコーディングをサポートしている場合、HDXビデオ圧縮はデフォルトでハードウェアエンコーディングを使用します。ハードウェアエンコーディングは、ソフトウェアエンコーディングよりも多くの帯域幅を消費する可能性があります。ソフトウェア圧縮を強制するには、レジストリキー HKCU\Software\Citrix\HdxRealTime に次のDWORDキー値 DeepCompress_ForceSWEncode=1 を追加します。

ネットワークトラフィックの優先順位

Quality of Serviceをサポートするルーターを使用して、セッションの複数の接続にわたるネットワークトラフィックに優先順位が割り当てられます。ユーザーデバイスとサーバー間でICAトラフィックを伝送するために、4つのTCPストリームと2つのユーザーデータグラムプロトコル（UDP）ストリームが利用可能です。

- TCPストリーム - リアルタイム、インタラクティブ、バックグラウンド、バルク
- UDPストリーム - 音声およびFramehawkディスプレイリモート処理

各仮想チャネルは特定の優先順位に関連付けられ、対応する接続で転送されます。接続に使用されるTCPポート番号に基づいて、チャネルを個別に設定できます。

Windows 10、Windows 8、およびWindows 7マシンにインストールされたVirtual Delivery Agent（VDA）では、複数チャネルストリーミング接続がサポートされています。ネットワーク管理者と協力して、**Multi-Port Policy**設定で構成されているCommon Gateway Protocol（CGP）ポートがネットワークルーターに正しく割り当てられていることを確認してください。

Quality of Serviceは、複数のセッション信頼性ポートまたはCGPポートが構成されている場合にのみサポートされます。

警告:

この機能を使用する場合は、トランスポートセキュリティを使用してください。Citrixは、Internet Protocol Security（IPsec）またはTransport Layer Security（TLS）の使用を推奨しています。TLS接続は、接続がマルチストリームICAをサポートするNetScaler Gatewayを通過する場合にのみサポートされます。社内ネットワークでは、TLSを使用したマルチストリーム接続はサポートされていません。

複数のストリーミング接続に対してQuality of Serviceを設定するには、以下のCitrixポリシー設定をポリシーに追加します（詳細については、マルチストリーム接続ポリシー設定を参照してください）。

- マルチポートポリシー - この設定は、複数の接続にわたるICAトラフィックのポートを指定し、ネットワークの優先順位を確立します。
  - CGPデフォルトポート優先順位リストから優先順位を選択します。デフォルトでは、プライマリポート（2598）は高優先順位です。
  - 必要に応じて、CGP port1、CGP port2、CGP port3にさらにCGPポートを入力し、それぞれの優先順位を特定します。各ポートには一意の優先順位が必要です。

  追加のTCPトラフィックを許可するように、VDA上のファイアウォールを明示的に構成します。
- マルチストリームコンピューター設定 - この設定はデフォルトで無効になっています。環境でマルチストリームサポート付きのCitrix NetScaler SD-WANを使用している場合、この設定を構

成する必要はありません。サードパーティ製ルーターまたはレガシーNetScaler SD-WANを使用して目的のQuality of Serviceを実現する場合は、このポリシー設定を構成してください。

- Multi-Stream ユーザー設定 - この設定はデフォルトで無効になっています。

これらの設定を含むポリシーを有効にするには、ユーザーはログオフしてからネットワークにログオンする必要があります。

リモート言語バーの表示/非表示

言語バーには、アプリケーションセッションで優先される入力言語が表示されます。この機能が有効になっている場合（デフォルト）、Windows 向け Citrix Workspace アプリの **［高度な設定］>［言語バー］** UI から言語バーを表示または非表示にできます。VDA 側のレジストリ設定を使用すると、言語バー機能のクライアント制御を無効にできます。この機能が無効になっている場合、クライアント UI 設定は有効にならず、ユーザーごとの現在の設定によって言語バーの状態が決まります。詳しくは、「ユーザーエクスペリエンスの向上」を参照してください。

VDA から言語バー機能のクライアント制御を無効にするには：

1. レジストリエディターで、HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI に移動します。
2. DWORD 値キー SeamlessFlags を作成し、0x40000 に設定します。

Unicode キーボードマッピング

Windows 以外の Citrix Receiver は、ローカルキーボードレイアウト（Unicode）を使用します。ユーザーがローカルキーボードレイアウトとサーバーキーボードレイアウト（スキャンコード）を変更すると、同期が取れなくなり、出力が正しくない場合があります。たとえば、User1 がローカルキーボードレイアウトを英語からドイツ語に変更します。その後、User1 がサーバー側のキーボードをドイツ語に変更します。両方のキーボードレイアウトがドイツ語であっても、同期が取れていないために文字出力が正しくない場合があります。

Unicode キーボードレイアウトマッピングの有効化または無効化

デフォルトでは、この機能は VDA 側で無効になっています。この機能を有効にするには、VDA 上のレジストリエディター regedit を使用して機能をオンに切り替えます。次のレジストリキーを追加します。

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名前: EnableKlMap

種類: DWORD

値: 1

この機能を無効にするには、**EnableKlMap** を 0 に設定するか、**CtxKlMap** キーを削除します。

Unicode キーボードレイアウトマッピング互換モードを有効にする

デフォルトでは、Unicode キーボードレイアウトマッピングは、サーバー側でキーボードレイアウトを変更すると、一部の Windows API を自動的にフックして新しい Unicode キーボードレイアウトマップを再ロードします。一部のアプリケーションはフックできません。互換性を維持するために、この機能を互換モードに変更して、これらのフックされていないアプリケーションをサポートできます。次のレジストリキーを追加します。

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名前: DisableWindowHook

種類: DWORD

値: 1

通常のUnicodeキーボードレイアウトマッピングを使用するには、**DisableWindowHook** を 0 に設定します。

Citrix ICA® 仮想チャネル

> **警告:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような重大な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。レジストリエディターの使用は、お客様ご自身の責任において行ってください。編集する前に、必ずレジストリをバックアップしてください。

ICA仮想チャネルとは何ですか?

Citrix Workspace™アプリとCitrix Virtual Apps and Desktops™サーバー間の機能と通信の大部分は、仮想チャネルを介して行われます。仮想チャネルは、Citrix Virtual Apps and Desktopsサー

バーを使用する際のリモートコンピューティングエクスペリエンスに不可欠な部分です。仮想チャネルは次の目的で使用されます。

- オーディオ
- COMポート
- ディスク
- グラフィック
- LPTポート
- プリンタ
- スマートカード
- サードパーティ製のカスタム仮想チャネル
- ビデオ

より多くの機能を提供するために、Citrix Virtual Apps™ and DesktopsサーバーおよびCitrix Workspaceアプリ製品の新しいバージョンとともに、新しい仮想チャネルがリリースされることがあります。

「仮想チャネル」(/en-us/citrix-virtual-apps-desktops/2511/media/ica-virtual-channels-1.png)

仮想チャネルは、サーバー側アプリケーションと通信するクライアント側仮想ドライバーで構成されています。Citrix Virtual Apps and Desktopsには、さまざまな仮想チャネルが付属しています。これらは、提供されているソフトウェア開発キット (SDK) のいずれかを使用して、顧客やサードパーティベンダーが独自の仮想チャネルを作成できるように設計されています。

仮想チャネルは、さまざまなタスクを安全に実行する方法を提供します。たとえば、Citrix Virtual Appsサーバーで実行されているアプリケーションがクライアント側のデバイスと通信する場合や、クライアント側の環境と通信するアプリケーションなどです。

クライアント側では、仮想チャネルは仮想ドライバーに対応します。各仮想ドライバーは特定の機能を提供します。一部は通常の操作に必要であり、その他はオプションです。仮想ドライバーはプレゼンテーション層プロトコルレベルで動作します。Windows Station（WinStation）プロトコル層によって提供されるチャネルを多重化することにより、いつでも複数のプロトコルをアクティブにできます。

以下の機能は、このレジストリパスの下にあるVirtualDriverレジストリ値に含まれています。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0`

または

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0` (64ビットの場合)

- Thinwire3.0（必須）
- ClientDrive
- ClentPrinterQueue
- ClentPrinterPort
- クリップボード
- ClientComm
- ClientAudio
- LicenseHandler (必須)
- TWI (必須)
- SmartCard
- ICACTL (必須)
- SSPI
- TwainRdr
- ユーザーエクスペリエンス
- Vd3d

> **注:**
>
> 特定のクライアント機能を無効にするには、レジストリキーからこれらの値の1つ以上を削除します。たとえば、クライアントクリップボードを削除したい場合は、**Clipboard**という単語を削除します。

> このリストには、クライアント仮想ドライバーファイルとそれぞれの機能が含まれています。Citrix Virtual AppsおよびWindows向けCitrix Workspaceアプリはこれらのファイルを使用します。これらは、汎用USB仮想チャネルで説明されている汎用USBを除き、ダイナミックリンクライブラリ（ユーザーモード）の形式であり、Windowsドライバー（カーネルモード）ではありません。

- vd3dn.dll – デスクトップコンポジションリダイレクトに使用されるDirect3D仮想チャネル

- vdcamN.dll – 双方向オーディオ
- vdcdm30n.dll – クライアントドライブマッピング
- vdcom30N.dll - クライアントCOMポートマッピング
- vdcpm30N.dll – クライアントプリンターマッピング
- vdctln.dll – ICAコントロールチャネル
- vddvc0n.dll – 動的仮想チャネル
- vdeuemn.dll - エンドユーザーエクスペリエンス監視
- vdgusbn.dll – 汎用USB仮想チャネル
- vdkbhook.dll – 透明キーパススルー
- vdlfpn.dll – UDPライクなトランスポートを介したFramehawkディスプレイチャネル
- vdmmn.dll – マルチメディアサポート
- vdmrvc.dll – Mobile Receiver仮想チャネル
- vdmtchn.dll - マルチタッチサポート
- vdscardn.dll – スマートカードサポート
- vdsens.dll – センサー仮想チャネル
- vdspl30n.dll – クライアントUPD
- vdsspin.dll – ケルベロス
- vdtuin.dll – 透明UI
- vdtw30n.dll – クライアント Thinwire
- vdtwin.dll – シームレス
- vdtwn.dll – ツイン

一部の仮想チャネルは、他のファイルにコンパイルされています。たとえば、クリップボードマッピングはwfica32.exeで利用できます。

64ビット互換性

Windows向けCitrix Workspaceアプリは64ビット互換です。32ビット用にコンパイルされたほとんどのバイナリと同様に、これらのクライアントファイルには64ビットコンパイルされた同等のものがあります。

- brapi64.dll
- confmgr.dll
- ctxlogging.dll

- ctxmui.dll
- icaconf.exe
- icaconfs.dll
- icafile.dll
- pnipcn64.dll
- pnsson.dll
- ssoncom.exe
- ssonstub.dll
- vdkbhook64.dll

汎用USB仮想チャネル

汎用USB仮想チャネルの実装では、仮想チャネルドライバーvdgusbn.dllに加えて、2つのカーネルモードドライバーを使用します。

- ctxusbm.sys
- ctxusbr.sys

ICA仮想チャネルの仕組み

仮想チャネルは複数の方法でロードされます。シェル（サーバーの場合はWfShell、ワークステーションの場合はPicaShell）が一部の仮想チャネルをロードします。一部の仮想チャネルはWindowsサービスとしてホストされます。

シェルによってロードされる仮想チャネルモジュール（例）：

- EUEM
- ツイン
- クリップボード
- マルチメディア
- シームレスセッション共有
- タイムゾーン

一部はカーネルモードとしてロードされます。例:

- CtxDvcs.sys – 動的仮想チャネル
- Icausbb.sys – 汎用USBリダイレクト

- Picadm.sys – クライアントドライブマッピング
- Picaser.sys – COMポートリダイレクト
- Picapar.sys – LPTポートリダイレクト

サーバー側のグラフィック仮想チャネル

`ctxgfx.exe` は、ワークステーションとターミナルサーバーベースのセッションの両方でグラフィック仮想チャネルをホストします。`Ctxgfx` は、対応するドライバー (RDSH 用の `Icardd.dll`、ワークステーション用の `vdod.dll` および `vidd.dll`) と対話するプラットフォーム固有のモジュールをホストします。

XenDesktop® 3D Pro展開の場合、VDA上の対応するGPUにOEMグラフィックドライバーがインストールされます。`Ctxgfx` は、OEMグラフィックドライバーと対話するために特殊なアダプターモジュールをロードします。

Windowsサービスでの特殊チャネルのホスティング

Citrix Virtual Apps and Desktopsサーバーでは、さまざまなチャネルがWindowsサービスとしてホストされます。このようなホスティングは、セッション内の複数のアプリケーションとサーバー上の複数のセッションに対して、1対多のセマンティクスを提供します。このようなサービスの例を次に示します。

- Citrixデバイスリダイレクターサービス
- Citrix動的仮想チャネルサービス
- Citrixエンドユーザーエクスペリエンス監視サービス
- Citrix 位置情報およびセンサー仮想チャネルサービス
- Citrix マルチタッチリダイレクトサービス
- Citrix 印刷マネージャーサービス
- Citrix スマートカードサービス
- Citrix オーディオリダイレクトサービス (Citrix Virtual Desktops™ のみ)
- Citrix ICA ステータスチャネルサービス

Citrix Virtual Apps のオーディオ仮想チャネルは、Windows Audio サービスを使用してホストされます。

サーバー側では、すべてのクライアント仮想チャネルは WinStation ドライバー (Wdica.sys) を介してルーティングされます。クライアント側では、wfica32.exe に組み込まれている対応する

WinStation ドライバーがクライアント仮想チャネルをポーリングします。この画像は、仮想チャネルのクライアントとサーバーの接続を示しています。

仮想チャネル接続の図(/en-us/citrix-virtual-apps-desktops/2511/media/virtual-channel-connection.png)

この概要には、仮想チャネルを使用したクライアントとサーバー間のデータ交換が含まれています。

1. クライアントは Citrix Virtual Apps and Desktops サーバーに接続します。クライアントは、サポートする仮想チャネルに関する情報をサーバーに渡します。
2. サーバー側のアプリケーションが起動し、仮想チャネルへのハンドルを取得し、必要に応じてチャネルに関する追加情報を照会します。
3. クライアント仮想ドライバーとサーバー側アプリケーションは、次の2つの方法を使用してデータを渡します。
    - サーバーアプリケーションがクライアントに送信するデータを持っている場合、データは直ちにクライアントに送信されます。クライアントがデータを受信すると、WinStation ドライバーは ICA ストリームから仮想チャネルデータを逆多重化し、直ちにクライアント仮想ドライバーに渡します。
    - クライアント仮想ドライバーがサーバーに送信するデータを持っている場合、データは WinStation ドライバーが次にポーリングしたときに送信されます。サーバーがデータを受信すると、仮想チャネルアプリケーションが読み取るまでキューに入れられます。サーバー仮想チャネルアプリケーションにデータが受信されたことを通知する方法はありません。
4. サーバー仮想チャネルアプリケーションが完了すると、仮想チャネルを閉じ、割り当てられたリソースを解放します。

Virtual Channel SDK を使用して独自の仮想チャネルを作成する

> **注:**
>
> Citrix SDK は、Citrix Developer ポータル (https://developer.cloud.com) で入手できます。

> Virtual Channel SDK を使用して仮想チャネルを作成するには、中程度のプログラミング知識が必要です。この方法を使用して、クライアントとサーバー間の主要な通信パスを提供し

ます。たとえば、セッション内のプロセスで使用するために、スキャナーなどのデバイスをクライアント側で実装する場合などです。

注:

- Virtual Channel SDK は、仮想チャネルのサーバー側を記述するために WFAPI SDK を必要とします。
- Citrix Virtual Apps and Desktops のセキュリティが強化されたため、ICA セッションで開くことを許可する仮想チャネルを指定する必要があります。詳細については、「仮想チャネル許可リストポリシー設定」を参照してください。

ICA Client Object SDK を使用して独自の仮想チャネルを作成する

ICA Client Object (ICO) を使用して仮想チャネルを作成する方が、Virtual Channel SDK を使用するよりも簡単です。**CreateChannels** メソッドを使用してプログラムで名前付きオブジェクトを作成することにより、ICO を使用します。

重要:

Citrix Receiver for Windows バージョン 10.00 以降 (および Citrix Workspace apps for Windows) でセキュリティが強化されたため、ICO 仮想チャネルを作成する際には追加の手順を実行する必要があります。

仮想チャネルのパススルー機能

Citrix が提供するほとんどの仮想チャネルは、ICA セッション内 (パススルーセッションとも呼ばれます) で Citrix Workspace app for Windows を使用する場合、変更なしで動作します。クライアントを複数のホップで使用する場合には考慮事項があります。

次の機能は、シングルホップまたはマルチホップで同じように動作します。

- クライアント COM ポートマッピング
- クライアントドライブマッピング
- クライアントプリンターマッピング
- クライアント UPD

- エンドユーザーエクスペリエンス監視
- 汎用 USB
- ケルベロス
- マルチメディアサポート
- スマートカードサポート
- 透明キーパススルー
- トウェイン

待ち時間の固有の性質、および各ホップで実行される圧縮と解凍、レンダリングなどの要因により、クライアントが経由するホップが増えるたびにパフォーマンスが影響を受ける可能性があります。影響を受ける領域は次のとおりです。

- 双方向オーディオ
- ファイル転送
- 汎用USBリダイレクト
- シームレス
- シンワイヤー

> **重要:**
>
> デフォルトでは、パススルーセッションで実行されているクライアントインスタンスによってマップされたクライアントドライブは、接続しているクライアントのクライアントドライブに制限されます。

Citrix Virtual DesktopセッションとCitrix Virtual Appセッション間の仮想チャネルのパススルー機能

Citrixが提供するほとんどの仮想チャネルは、Citrix Virtual Desktopsサーバー上のICAセッション内でWindows向けCitrix Workspaceアプリを使用する場合（パススルーセッションとも呼ばれます）、変更されずに動作します。

具体的には、Citrix Virtual Desktopsサーバーには、**picaPassthruHook**を実行するVDAフックがあります。このフックにより、クライアントはCPSサーバー上で実行されていると認識し、クライアントを従来のパススルーモードにします。

以下の従来の仮想チャネルとその機能がサポートされています。

- クライアント
- クライアントCOMポートマッピング
- クライアントドライブマッピング
- クライアントプリンターマッピング
- 汎用USB（パフォーマンス上の理由により制限あり）
- マルチメディアサポート
- スマートカードサポート
- SSON
- 透過的なキーパススルー

セキュリティとICA仮想チャネル

仮想チャネルの計画、開発、実装において、使用のセキュリティ確保は重要な部分です。このドキュメント全体にわたって、セキュリティの特定の領域への参照がいくつかあります。

ベストプラクティス

接続および**再接続**時に仮想チャネルを開きます。ログオフおよび**切断**時に仮想チャネルを閉じます。

仮想チャネル関数を使用するスクリプトを作成する際は、以下のガイドラインを念頭に置いてください。

仮想チャネルの命名:

最大32個の仮想チャネルを作成できます。32個のチャネルのうち17個は、特別な目的のために予約されています。

- 仮想チャネル名は7文字以内である必要があります。
- 最初の3文字はベンダー名に、次の4文字はチャネルタイプに予約されています。たとえば、**CTXAUD**はCitrixオーディオ仮想チャネルを表します。

仮想チャネルは、7文字（またはそれ以下）のASCII名で参照されます。ICAプロトコルの以前のバージョンでは、仮想チャネルは番号付けされていました。現在、番号はASCII名に基づいて動的に割り当てられるため、実装が容易になります。社内でのみ使用する仮想チャネルコードを開発しているユーザーは、既存の仮想チャネルと競合しない任意の7文字の名前を使用できます。数字と大文字小文字のASCIIのみを使用してください。独自の仮想チャネルを追加する際は、既存の命

名規則に従ってください。いくつかの事前定義されたチャネルがあります。事前定義されたチャネルはOEM識別子CTXで始まり、Citrixのみが使用できます。

ダブルホップサポート:

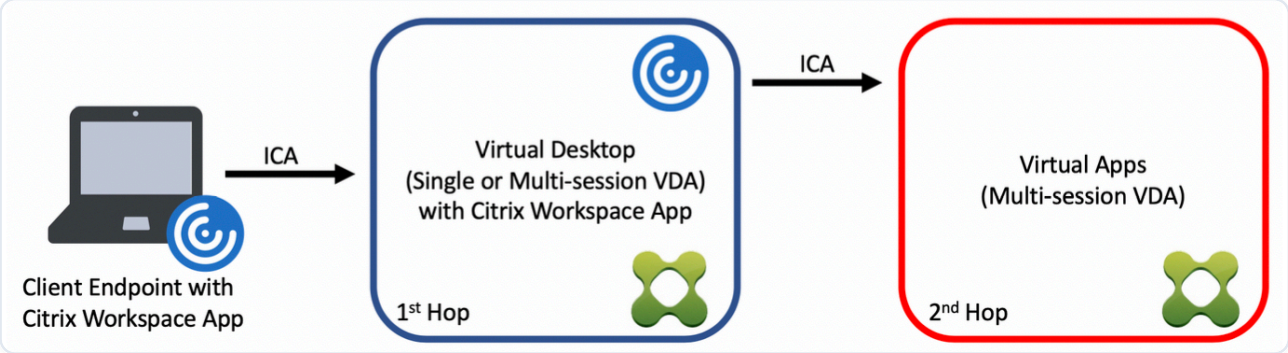
仮想チャネル	ダブルホップはサポートされていますか？
オーディオ	いいえ
ブラウザコンテンツリダイレクション	いいえ
CDM	はい
CEIP	いいえ
クリップボード	はい
コンティニュアム (MRVC)	いいえ
コントロール VC	はい
HTML5ビデオリダイレクト (v1)	はい
キーボード、マウス	はい
マルチタッチ	いいえ
NSAPVC	いいえ
印刷	はい
SensVC	いいえ
スマートカード	はい
ツイン	はい
USB VC	はい
USB VC を使用する WAYCOM デバイス -K2M	はい
Webカメラビデオ圧縮	はい
Windows Mediaリダイレクト	はい

参照

- ICA 仮想チャネル SDK
- Citrix Developer Network は、Citrix SDK の使用に関するすべての技術リソースとディスカッションの場です。このネットワークでは、SDK、サンプルコードとスクリプト、拡張機能とプラグイン、SDK ドキュメントにアクセスできます。また、Citrix Developer Network フォーラムも含まれており、各 Citrix SDK に関する技術的なディスカッションが行われています。

Citrix Virtual Apps and Desktops™におけるダブルホップ

Citrixクライアントセッションのコンテキストでは、「ダブルホップ」という用語は、Citrix Virtual Desktopセッション内で実行されているCitrix Virtual Appセッションを指します。次の図はダブルホップを示しています。



ダブルホップのシナリオでは、ユーザーがシングルセッションOS VDA（VDIとして知られる）またはマルチセッションOS VDA（公開デスクトップとして知られる）で実行されているCitrix Virtual Desktopに接続すると、それが最初のホップと見なされます。ユーザーが仮想デスクトップに接続した後、Citrix Virtual Apps™セッションを起動できます。それが2番目のホップと見なされます。

ダブルホップ展開モデルを使用して、さまざまなユースケースをサポートできます。Citrix Virtual Desktop環境とCitrix Virtual Apps環境が異なるエンティティによって管理されているケースは、一般的な例の1つです。この方法は、アプリケーションの互換性の問題を解決する上でも効果的です。

システム要件

Citrix Cloud™サービスを含むすべてのCitrix Virtual Apps and Desktopsエディションはダブルホップをサポートしています。

最初のホップでは、シングルセッションまたはマルチセッションOS VDAとCitrix Workspace Appのサポートされているバージョンを使用する必要があります。2番目のホップでは、マルチセッ

ションOS VDAのサポートされているバージョンを使用する必要があります。サポートされているバージョンについては、製品マトリックスページを参照してください。

最高のパフォーマンスと互換性を得るために、Citrixは、使用中のVDAバージョンと同じかそれ以降のバージョンのCitrixクライアントを使用することを推奨します。

最初のホップが、Citrix Virtual Appsセッションと組み合わされたサードパーティ製（Citrix以外）の仮想デスクトップソリューションを含む環境では、サポートはCitrix Virtual Apps環境に限定されます。サードパーティ製仮想デスクトップに関連する問題（Citrix Workspace™アプリの互換性、ハードウェアデバイスのリダイレクト、セッションパフォーマンスなどを含むがこれらに限定されない）が発生した場合、Citrixは限られた範囲で技術サポートを提供できます。トラブルシューティングの一環として、最初のホップにCitrix Virtual Desktopが必要になる場合があります。

ダブルホップにおけるHDX™の展開に関する考慮事項

一般に、ダブルホップの各セッションは一意であり、クライアント/サーバー機能は特定のホップに分離されています。このセクションでは、Citrix管理者が特に考慮する必要がある領域について説明します。Citrixは、特定の環境構成に対してユーザーエクスペリエンスとパフォーマンスが適切であることを確認するために、必要なHDX機能の徹底的なテストを実施することを推奨します。

グラフィック

最初のホップと2番目のホップで、デフォルトのグラフィック設定（選択的エンコード）を使用します。HDX 3D Proの場合、Citrixは、グラフィックアクセラレーションを必要とするすべてのアプリケーションを、VDAで利用可能な適切なGPUリソースを使用して最初のホップでローカルに実行することを強く推奨します。

遅延

エンドツーエンドの遅延は、全体的なユーザーエクスペリエンスに影響を与える可能性があります。最初のホップと2番目のホップ間の追加の遅延を考慮してください。これは、ハードウェアデバイスのリダイレクトにおいて特に重要です。

マルチメディア

オーディオおよびビデオコンテンツのサーバー側（セッション内）レンダリングは、最初のホップで最高のパフォーマンスを発揮します。2番目のホップでのビデオ再生では、最初のホップでのデコードと再エンコードが必要となり、その結果、帯域幅とハードウェアリソースの使用率が増加します。オーディオおよびビデオコンテンツは、可能な限り最初のホップに限定する必要があります。

USBデバイスのリダイレクト

HDXには、さまざまなUSBデバイスタイプをサポートするための汎用および最適化されたリダイレクトモードが含まれています。各ホップで使用されているモードに特に注意し、最良の結果を得るために以下の表を参照してください。汎用および最適化されたリダイレクトモードの詳細については、「汎用USBデバイス」を参照してください。

最初のホップ（VDIまたは公開デスクトップ）	2番目のホップ（仮想アプリ）	サポートに関する注意事項
最適化済み	最適化済み	推奨（デバイスサポートに基づく）。例：USBマスストレージ、TWAINスキャナー、Webカメラ、オーディオ。
汎用	汎用	最適化オプションが利用できないデバイスの場合。
汎用	最適化済み	技術的には可能ですが、デバイスのサポートが利用可能な場合は、両方のホップで最適化モードを使用することをお勧めします。
最適化済み	汎用	サポートされていません

注:

USBプロトコルの本質的なチャッティネス（頻繁な通信）のため、ホップ間でパフォーマンスが低下する可能性があります。機能と結果は、特定のデバイスおよびアプリケーションの要件によって異なります。デバイスリダイレクトのすべての場合において検証テストを強く推奨し、特にダブルホップシナリオでは重要です。

サポートの例外

ダブルホップセッションは、以下の例外を除き、ほとんどのHDX機能と機能をサポートします。

- ブラウザコンテンツリダイレクト
- ローカルアプリアクセス

- スカイプ フォー ビジネス向けリアルタイム最適化パック(/ja-jp/hdx-optimization/current-release.html)
- Microsoft Teams向け最適化

インストールと構成

各展開ステップを開始する前に、参照されている記事を確認して、展開中に表示される内容と指定する内容について学習してください。

Citrix Virtual Apps and Desktopsを展開するには、次の手順を使用します。

準備

インストール準備を確認し、必要なタスクをすべて完了してください。

- 概念、機能、以前のリリースとの違い、システム要件、およびデータベースに関する情報の入手先。
- コアコンポーネントをどこにインストールするかを決定する際の考慮事項。
- 権限とActive Directoryの要件。
- 利用可能なインストーラー、ツール、およびインターフェイスに関する情報。

コアコンポーネントのインストール

Delivery Controller、Web Studio、Citrix Director、およびCitrix License Serverをインストールします。Citrix StoreFrontもインストールできます。詳細については、コアコンポーネントのインストールまたはコマンドラインを使用したインストールを参照してください。

サイトの作成

コアコンポーネントをインストールしてStudioを起動すると、サイトの作成を求められます。

1つ以上のVirtual Delivery Agent (VDA) をインストールする

Windowsオペレーティングシステムを実行しているマシンにVDAをインストールします。これは、マスターイメージ上または各マシンに直接インストールできます。VDAのインストールまたはコマンドラインを使用したインストールを参照してください。Active Directoryを介してVDAをインストールする場合は、サンプルスクリプトが提供されています。

Linuxオペレーティングシステムを搭載したマシンについては、Linux Virtual Delivery Agentのガイダンスに従ってください。

Remote PC Access展開の場合、各オフィスPCにシングルセッションOS用VDAをインストールします。コアVDAサービスのみが必要な場合は、スタンドアロンの`VDAWorkstationCoreSetup.exe`インストーラーと既存の電子ソフトウェア配布（ESD）方法を使用してください。（インストールの準備で利用可能なVDAインストーラーについて説明しています。）

オプションコンポーネントのインストール

Citrix Universal Print Serverを使用する予定がある場合は、そのサーバーコンポーネントをプリントサーバーにインストールしてください。コアコンポーネントのインストールまたはコマンドラインを使用したインストールを参照してください。

StoreFrontがSAMLアサーションなどの認証オプションを使用できるようにするには、Citrix Federated Authentication Serviceをインストールします。

エンドユーザーが自分のユーザーアカウントをより詳細に制御できるようにするには、Self-Service Password Resetをインストールします。

オプションで、Citrix Virtual Apps™ and Desktops展開にCitrixコンポーネントを追加で統合します。

- Citrix Provisioningは、マスターイメージをターゲットデバイスにストリーミングしてマシンをプロビジョニングするオプションコンポーネントです。
- Citrix Gatewayは、アプリケーションとデータへのアクセスを保護するために、管理者に対してきめ細かなアプリケーションレベルのポリシーとアクション制御を提供するセキュアなアプリケーションアクセスソリューションです。
- Citrix SD-WANは、WANパフォーマンスを最適化するアプライアンスのセットです。

マシンカタログを作成する

Studioでサイトを作成すると、マシンカタログの作成に誘導されます。

カタログには、物理マシンまたは仮想マシン（VM）を含めることができます。仮想マシンはマスターイメージから作成できます。ハイパーバイザーまたはその他のサービスを使用してVMを提供する場合は、まずそのホスト上にマスターイメージを作成します。次に、カタログを作成するときに、そのイメージを指定します。このイメージはVMの作成時に使用されます。

デリバリーグループを作成する

Web Studioで最初のマシンカタログを作成すると、デリバリーグループの作成に誘導されます。

デリバリーグループは、選択したカタログ内のマシンにアクセスできるユーザーと、それらのユーザーが利用できるアプリケーションを指定します。

アプリケーショングループの作成（オプション）

デリバリーグループを作成した後、オプションでアプリケーショングループを作成できます。アプリケーショングループは、異なるデリバリーグループ間で共有されるアプリケーション、またはデリバリーグループ内のユーザーのサブセットによって使用されるアプリケーションに対して作成できます。

既知の制限事項

Citrix Workspace™アプリ for Windowsバージョン1912以前を使用すると、セッションがしばらくすると切断されます。この問題は、Citrix Workspaceアプリの新しいLTSRおよびCRバージョンで修正されています。 サポートされているリリースバージョンの詳細については、Citrix Workspaceアプリ for Windows / Citrix Receiver for Windows Long Term Service Releasesを参照してください。

マシンID

各マシンは、コンピューターアカウントとも呼ばれる一意のマシンIDを持つ必要があります。マシンIDは、マシン内でローカルに、またはディレクトリ内で作成および管理できます。Citrix®は、Active Directoryに参加している、Microsoft Entraハイブリッド参加している、またはドメインに参加していないマシンで仮想アプリケーションとデスクトップをホストすることをサポートしています。

マシンIDの種類

以下のマシンIDの種類がサポートされています。

マシンIDの種類	説明
AD参加済み	IDはオンプレミスのActive Directoryで作成および管理されます。プロビジョニングされたマシンは、割り当てられたマシンIDを使用してオンプレミスのActive Directoryに参加します。

マシンIDの種類	説明
Microsoft Entraハイブリッド参加済み	IDはオンプレミスのActive Directoryで作成され、Microsoft Entra Connectを介してMicrosoft Entra IDと同期されます。プロビジョニングされたマシンはオンプレミスのActive Directoryに参加します。その後、マシンはMicrosoft Entraハイブリッド参加済みになります。Microsoft Entraハイブリッド参加済みVMをインポートする場合、そのVMはCitrix Virtual Apps and DesktopsによってActive Directory参加済みVMとして扱われます。
ドメイン非参加	IDはマシン内でローカルに作成および管理されます。Citrix Virtual Apps and DesktopsへのVMのインポートはサポートされていません。

サポートされる構成

各シナリオでサポートされる構成の詳細は次のとおりです。

サポートされるインフラストラクチャ

マシンID	シトリックス バーチャル アプリケーションズ アンド デスクトップ™	シトリックス ワークスペース™	シトリックス ストアフロント	シトリックス ゲートウェイ サービス	シトリックス ゲートウェイ
AD参加済み	はい	はい	はい	はい	はい
Microsoft Entra 参加済み	いいえ	はい	いいえ	はい	いいえ
Microsoft Entraハイブリッド参加済み	はい	はい	はい	はい	はい
ドメイン非参加	はい	はい	いいえ	はい	いいえ

サポートされているワークスペース認証IDプロバイダー

マシンID	マイクロソフトエントラID	アクティブディレクトリ	ACTIVE DIRECTORYとトークン	オクタ	SAML	シトリックス ゲートウェイ	アダプティブ認証
AD参加済み	はい	はい	はい	はい	はい	はい	はい
Microsoft Entra ハイブリッド参加済み	はい	はい	はい	はい	はい	はい	はい
ドメイン非参加	はい	はい	はい	はい	はい	はい	はい

Active Directoryへの参加

Active Directoryは、認証と承認に必要です。Active DirectoryのKerberosインフラストラクチャは、Delivery Controllerとの通信の信頼性と機密性を保証するために使用されます。Kerberosの詳細については、Microsoftのドキュメントを参照してください。

システム要件の記事には、サポートされているフォレストおよびドメインの機能レベルが記載されています。ポリシーモデリングを使用するには、ドメインコントローラーがサポートされているすべてのサーバーOSで実行されている必要があります。これはドメインの機能レベルには影響しません。

この製品は以下をサポートします。

- **ユーザーアカウントとコンピューターアカウントが単一のActive Directoryフォレスト内のドメインに存在する展開。** ユーザーアカウントとコンピューターアカウントは、単一フォレスト内の任意のドメインに存在できます。この種類の展開では、すべてのドメイン機能レベルとフォレスト機能レベルがサポートされます。
- **ユーザーアカウントが、Controllerおよび仮想デスクトップのコンピューターアカウントを含むActive Directoryフォレストとは異なるActive Directoryフォレストに存在する展開。** この種類の展開では、Controllerおよび仮想デスクトップのコンピューターアカウントを含むドメインは、ユーザーアカウントを含むドメインを信頼する必要があります。フォレスト信頼また

は外部信頼を使用できます。この種類の展開では、すべてのドメイン機能レベルとフォレスト機能レベルがサポートされます。

- **Controllerのコンピューターアカウントが、仮想デスクトップのコンピューターアカウントを含む1つ以上の追加のActive Directoryフォレストとは異なるActive Directoryフォレストに存在する展開。** この種類の展開では、Controllerのコンピューターアカウントを含むドメインと、仮想デスクトップのコンピューターアカウントを含むすべてのドメインとの間に双方向の信頼が存在する必要があります。この種類の展開では、Controllerまたは仮想デスクトップのコンピューターアカウントを含むすべてのドメインが「Windows 2000ネイティブ」機能レベル以上である必要があります。すべてのフォレスト機能レベルがサポートされます。
- **書き込み可能なドメインコントローラー。** 読み取り専用ドメインコントローラーはサポートされていません。

オプションで、Virtual Delivery Agent（VDA）は、Active Directoryで公開されている情報を使用して、登録できるControllerを特定できます（検出）。この方法は主に下位互換性のためにサポートされており、VDAがControllerと同じActive Directoryフォレストにある場合にのみ利用できます。この検出方法については、Active Directory OUベースの検出およびCTX118976を参照してください。

> **注:**
>
> サイトの構成後にDelivery Controller™のコンピューター名またはドメインメンバーシップを変更しないでください。

複数のActive Directoryフォレスト環境での展開

複数のフォレストを持つActive Directory環境で、一方向または双方向の信頼が確立されている場合、名前解決と登録のためにDNSフォワーダーまたは条件付きフォワーダーを使用できます。適切なActive Directoryユーザーがコンピューターアカウントを作成できるようにするには、制御の委任ウィザードを使用します。このウィザードの詳細については、Microsoftのドキュメントを参照してください。

フォレスト間に適切なDNSフォワーダーが配置されていれば、DNSインフラストラクチャに逆引きDNSゾーンは不要です。

VDAとControllerが別々のフォレストにある場合、Active Directory名とNetBIOS名が異なっていても、`SupportMultipleForest`キーが必要です。VDAとDelivery Controllerにレジストリキーを追加するには、次の情報を使用してください。

> **注意:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix® は、レジストリエディターの誤った使用によって生じた問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。編集する前にレジストリをバックアップしてください。

> VDAで、以下を構成します: `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest`。

- 名前: `SupportMultipleForest`
- 種類: `REG_DWORD`
- データ: `0x00000001 (1)`

すべてのDelivery Controllerで、以下を構成します: `HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\SupportMultipleForest`。

- 名前: `SupportMultipleForest`
- 種類: `REG_DWORD`
- データ: `0x00000001 (1)`

DNS名前空間がActive Directoryの名前空間と異なる場合は、逆引きDNS構成が必要になる場合があります。

Kerberosよりも安全性の低いNTLM認証がVDAで意図せず有効になるのを避けるため、レジストリエントリが追加されました。このエントリは、下位互換性のために引き続き使用できる `SupportMultipleForest` エントリの代わりに使用できます。

VDAで、以下を構成します: `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`。

- 名前: `SupportMultipleForestDdcLookup`
- 種類: `REG_DWORD`
- データ: `0x00000001 (1)`

このレジストリキーは、初期登録プロセス中にNTLMベースの認証を削除できる、双方向信頼の複数フォレスト環境でDDCルックアップを実行します。

セットアップ中に外部信頼が設定されている場合、`ListOfSIDs`レジストリキーが必要です。Active Directory FQDNがDNS FQDNと異なる場合、またはドメインコントローラーを含むドメインのNetBIOS名がActive Directory FQDNと異なる場合も、`ListOfSIDs`レジストリキーが必要です。レジストリキーを追加するには、次の情報を使用します。

VDAの場合、レジストリキー`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs`を見つけます。

- 名前: `ListOfSIDs`
- 種類: `REG_SZ`
- データ: コントローラーのセキュリティ識別子 (SID)。(SIDは`Get-BrokerController`コマンドレットの結果に含まれています。)

外部信頼が設定されている場合、VDAで次の変更を行います:

1. ファイル`Program Files\Citrix\Virtual Desktop Agent\brokeragent.exe.config`を見つけます。
2. ファイルのバックアップコピーを作成します。
3. メモ帳などのテキスト編集プログラムでファイルを開きます。
4. テキスト`allowNtlm="false"`を見つけて、テキストを`allowNtlm="true"`に変更します。
5. ファイルを保存します。

`ListOfSIDs`レジストリキーを追加し、`brokeragent.exe.config`ファイルを編集した後、Citrix Desktop Serviceを再起動して変更を適用します。

次の表に、サポートされている信頼の種類を示します。

信頼の種類	推移性	方向	このリリースでサポートされています
親と子	推移的	双方向	はい
ツリー ルート	推移的	双方向	はい
外部	非推移的	一方向または双方向	はい
フォレスト	推移的	一方向または双方向	はい
ショートカット	推移的	一方向または双方向	はい

信頼の種類	推移性	方向	このリリースでサポートされています
レルム	推移的または非推移的	一方向または双方向	いいえ

複雑なActive Directory環境の詳細については、CTX134971 を参照してください。

次のステップ

オンプレミスActive Directory (AD) に参加しているマシンIDのIDプールを作成する方法については、「オンプレミスActive Directoryに参加しているマシンIDのIDプール」(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/identity-pools-different-machine-identity-join-types/identity-pool-on-premises-active-directory-joined.html)を参照してください。

Microsoft Entraハイブリッド参加済み

この記事では、システム要件セクションで概説されている要件に加えて、Microsoft Entra ハイブリッド参加済みカタログと Microsoft Intune に登録された Microsoft Entra ハイブリッド参加済みカタログのIDプールを作成するための要件について説明します。

Microsoft Entra ハイブリッド参加済みマシンは、オンプレミスADを認証プロバイダーとして使用します。それらをオンプレミスADのドメインユーザーまたはグループに割り当てることができます。Microsoft Entra ID のシームレスなSSOエクスペリエンスを有効にするには、ドメインユーザーをMicrosoft Entra IDに同期する必要があります。

> **注記:**
>
> Microsoft Entra ハイブリッド参加済みVMは、フェデレーションIDインフラストラクチャとマネージドIDインフラストラクチャの両方でサポートされています。

Microsoft Entra ハイブリッド参加の要件

- VDAの種類: シングルセッション (デスクトップのみ) またはマルチセッション (アプリとデスクトップ)
- VDAバージョン: 2212以降
- プロビジョニングの種類: Machine Creation Services™ (MCS)、永続的および非永続的
- 割り当ての種類: 専用およびプール

- ホスティングプラットフォーム: 任意のハイパーバイザーまたはクラウドサービス

Microsoft Entra ハイブリッド参加の制限事項

- Citrix Federated Authentication Service (FAS) を使用する場合、シングルサインオンは Microsoft Entra ID ではなくオンプレミスADに転送されます。この場合、ユーザーログオン時にプライマリ更新トークン (PRT) が生成されるように Microsoft Entra 証明書ベース認証を構成することをお勧めします。これにより、セッション内の Microsoft Entra リソースへのシングルサインオンが容易になります。そうしないと、PRTが存在せず、Microsoft Entra リソースへのSSOは機能しません。Citrix Federated Authentication Service (FAS) を使用してハイブリッド参加済みVDAへの Microsoft Entra シングルサインオン (SSO) を実現する方法については、「Hybrid-joined VDAs」を参照してください。
- マシンカタログの作成または更新中にイメージの準備をスキップしないでください。イメージの準備をスキップしたい場合は、マスターVMが Microsoft Entra または Microsoft Entra ハイブリッド参加済みではないことを確認してください。

Microsoft Entra ハイブリッド参加に関する考慮事項

- Microsoft Entra ハイブリッド参加済みマシンを作成するには、ターゲットドメインで `Write userCertificate` 権限が必要です。カタログ作成時に、その権限を持つ管理者の資格情報を入力してください。
- Microsoft Entra ハイブリッド参加プロセスはCitrixによって管理されます。マスターVMでWindowsによって制御される `autoWorkplaceJoin` を次のように無効にする必要があります。 `autoWorkplaceJoin` を手動で無効にする作業は、VDAバージョン2212以前の場合にのみ必要です。

  a. `gpedit.msc` を実行します。
  b. **コンピューターの構成 > 管理用テンプレート > Windows コンポーネント > デバイス登録** に移動します。
  c. **ドメイン参加済みコンピューターをデバイスとして登録する** を **無効** に設定します。

- マシンIDを作成する際に、Microsoft Entra IDと同期するように構成されている組織単位 (OU) を選択します。
- Windows 11 22H2ベースのマスターVMの場合、システム起動時にSYSTEMアカウントを使用して次のコマンドを実行するスケジュールされたタスクをマスターVMに作成します。マスターVMでタスクをスケジュールするこの作業は、VDAバージョン2212以前の場合にのみ必要です。

```
$VirtualDesktopKeyPath = 'HKLM:\Software\AzureAD\VirtualDesktop'

$WorkplaceJoinKeyPath = 'HKLM:
\SOFTWARE\Policies\Microsoft\Windows\WorkplaceJoin'

$MaxCount = 60



for ($count = 1; $count -le $MaxCount; $count++)

{

  if ((Test-Path -Path $VirtualDesktopKeyPath) -eq $true)

  {

    $provider = (Get-Item -Path
$VirtualDesktopKeyPath).GetValue("Provider", $null)

    if ($provider -eq 'Citrix')

    {

        break;

    }



    if ($provider -eq 1)

    {

        Set-ItemProperty -Path $VirtualDesktopKeyPath -Name "Provider"
-Value "Citrix" -Force

        Set-ItemProperty -Path $WorkplaceJoinKeyPath -Name
"autoWorkplaceJoin" -Value 1 -Force

        Start-Sleep 5

        dsregcmd /join
```

```
        break
    }
  }


  Start-Sleep 1
}
```

- デフォルトでは、Microsoft Entra Connectは30分ごとに同期します。プロビジョニングされたマシンがMicrosoft Entra ハイブリッド参加済みになるまで、初回起動時に最大30分かかることがあります。

Microsoft Intuneに登録されているMicrosoft Entra ハイブリッド参加済みカタログ

Microsoft Intuneに登録されているMicrosoft Entra ハイブリッド参加済みカタログ、永続的なシングルセッションおよびマルチセッションVMは、共同管理機能を持つデバイス資格情報を使用します。

共同管理により、Configuration ManagerとMicrosoft Intuneの両方を使用して、Windows 10以降のデバイスを同時に管理できます。詳細については、共同管理を参照してください。

Microsoft Intuneに登録されているMicrosoft Entra ハイブリッド参加済みカタログの前提条件

この機能を有効にする前に、以下を確認してください。

- Azure環境がMicrosoft Intuneを使用するためのライセンス要件を満たしていること。詳細については、Microsoftドキュメントを参照してください。
- 共同管理が有効になっている有効なConfiguration Manager展開があること。詳細については、Microsoftドキュメントを参照してください。

Microsoft Intuneに登録されているMicrosoft Entraハイブリッド参加カタログの要件

- VDAタイプ: シングルセッションまたはマルチセッション
- VDAバージョン: 2407以降
- プロビジョニングタイプ: Machine Creation Service (MCS)、永続的。Microsoft Intuneに登録されている非永続的なシングルセッションおよびマルチセッションVM用のMicrosoft Entraハイ

ブリッド参加カタログは現在プレビュー中です。詳細については、「ハイブリッドEntra ID参加の非永続VMのMicrosoft Intuneへの登録」を参照してください。

- 割り当てタイプ: 専用およびプール
- ホスティングプラットフォーム: 任意のハイパーバイザーまたはクラウドサービス

Microsoft Intuneに登録されているMicrosoft Entraハイブリッド参加カタログの制限事項

- マシンカタログの作成または更新時にイメージの準備をスキップしないでください。
- Configuration Managerのインターネットベースのクライアント管理 (IBCM) はサポートされていません。

Microsoft Intuneに登録されているMicrosoft Entraハイブリッド参加カタログの考慮事項

- カタログ内の多数のマシンが同時に電源オンになると、Intuneへの登録が遅れる場合があります。

  Microsoftは、特定の期間内に登録できるデバイスの数を制限するテナントごとのIntune登録制限を課しています。許可されるデバイスの数は、テナントに関連付けられているMicrosoft Intuneライセンスの数によって異なります。テナントの許容制限については、Microsoftアカウントチームにお問い合わせください。このアプローチは、大規模な環境でのMicrosoft Intune登録のスケーリングを向上させるのに役立ちます。

  永続マシンでは、すべてのデバイスがIntune登録を完了するまでに初期の待機時間が必要になる場合があります。

  非永続マシンでは、Autoscale™または手動の電源操作で同時電源操作を制限することを検討してください。

- Configuration ManagerのCloud Attachを構成します。詳細については、Microsoftドキュメントを参照してください。
- マスターVMにConfiguration Managerクライアントを手動でインストールし、`.\CCMSetup.exe /mp:SCCMServer /logon FSP=SCCMServer`でサイトコードを割り当てないでください。SCCMServerは、お使いの環境のSCCMサーバー名です。詳細については、Microsoftドキュメントを参照してください。
- MCSで作成されたマシンは、Active Directory Domain Servicesに公開されているサイト境界グループを見つけるために、自動サイト割り当てメカニズムを使用します。お使いの環境で**Configuration Manager**の境界と境界グループが構成されていることを確認してください。自動サイト割り当てが利用できない場合は、次のレジストリ設定を通じてマスターVMに静的Configuration Managerサイトコードを構成できます。

キー:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MachineIdentityServiceAgent\DeviceManagement
```

値の名前: `MdmSccmSiteCode`

値の型: **String**

値のデータ: `the site code to be assigned`

次のステップ

Microsoft Entra ハイブリッド参加カタログの ID プールの作成の詳細については、Microsoft Entra ハイブリッド参加マシン ID の ID プールを参照してください。

ドメイン非参加

この記事では、システム要件セクションに記載されている要件に加えて、Citrix Virtual Apps and Desktops を使用してドメイン非参加カタログを作成するための要件について説明します。

要件

- コントロールプレーン: サポートされる構成を参照してください。
- VDAの種類: シングルセッション (デスクトップのみ) またはマルチセッション (アプリとデスクトップ)
- VDAバージョン: 2311以降
- プロビジョニングの種類: Machine Creation Services™ (MCS)、永続的および非永続的
- 割り当ての種類: 専用およびプール
- ホスティングプラットフォーム: MCSでサポートされているすべてのプラットフォーム
- Rendezvous V2を有効にする必要があります

制限事項

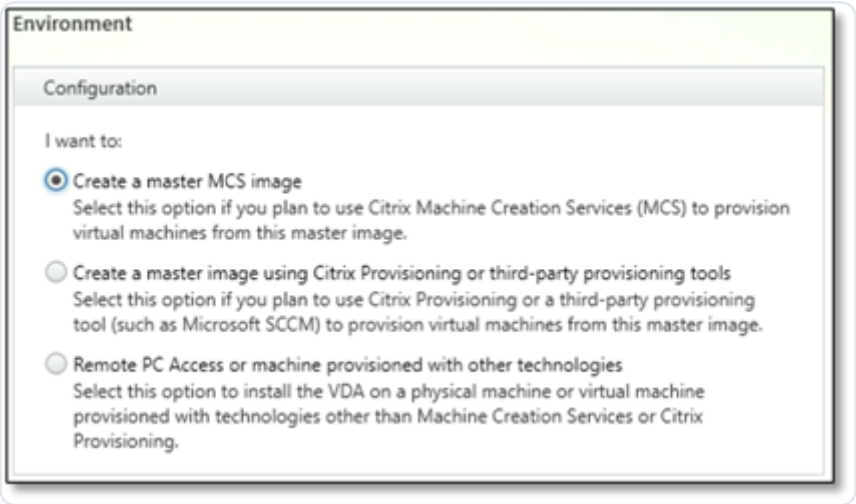
- サービス継続性はサポートされていません。
- マルチセッションのドメイン非参加VDAを使用する場合、ローカルユーザーのプロファイルデータは保持されず、ログオフ時に削除されます。

VDAのインストールと構成

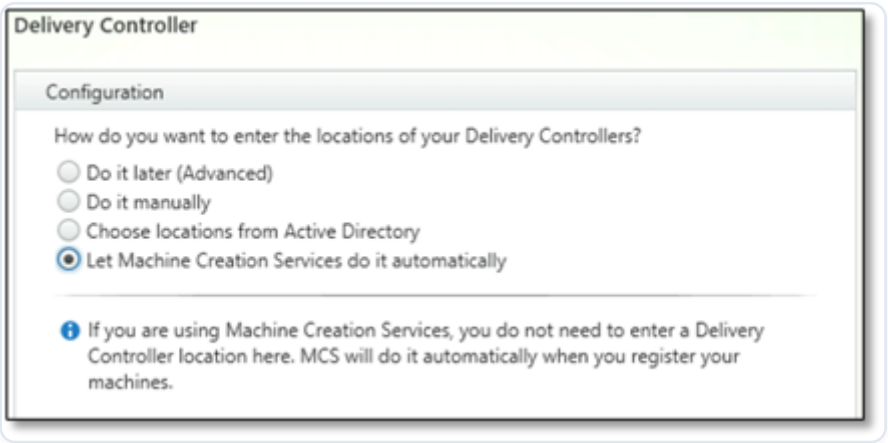
VDAをインストールする手順に従います。

1. インストールウィザードで次のオプションを選択してください。

   - 「環境」ページで、**マスターMCSイメージを作成**を選択します。



   - 「Delivery Controller™」ページで、**Machine Creation Servicesに自動的に実行させる**を選択します。



次のステップ

リソースの場所とホスティング接続が利用可能になったら、IDプールを作成します。ドメインに参加していないマシンIDのIDプールの作成について詳しくは、「ドメインに参加していないマシンIDのIDプール」を参照してください。

インストールを準備する

Citrix Virtual Apps and Desktops™ の展開は、以下のコンポーネントのインストールから始まります。このプロセスは、ファイアウォール内のユーザーにアプリケーションとデスクトップを配信するための準備です。

- 1つ以上のDelivery Controller

- シトリックス ディレクター
- シトリックス ストアフロント™
- シトリックス ライセンス サーバー
- 1つ以上のシトリックス バーチャル デリバリー エージェント (VDA)
- Universal Print Server、Federated Authentication Service、Self-Service Password Resetなどのオプションコンポーネントおよびテクノロジー

ファイアウォールの外部のユーザー向けには、Citrix Gatewayなどの追加コンポーネントをインストールして構成します。概要については、「Citrix Virtual Apps and DesktopsとCitrix Gatewayの統合」を参照してください。

> **注:**
>
> サーバーOSおよびワークステーションOSで、以下のMicrosoftの前提条件が満たされていることを確認してください。
>
> - Microsoft **Volume Shadow Copy** および **Microsoft Software Shadow Copy Provider** サービスが実行されていること。詳細については、「Volume Shadow Copy Service」を参照してください。
> - **MS-Defender** のバージョンは4.18.2105.5より高い必要があります。詳細については、「Microsoft Defender Antivirusのセキュリティインテリジェンスと製品の更新」を参照してください。
>
> 展開にWindows Serverワークロードが含まれる場合は、Microsoft RDSライセンスサーバーを構成してください。

製品ISOに含まれるフル製品インストーラーを使用して、多くのコンポーネントとテクノロジーを展開できます。VDAのインストールには、スタンドアロンVDAインストーラーを使用できます。スタンドアロンVDAインストーラーは、Citrixダウンロードサイトで入手できます。すべてのインストーラーは、グラフィカルインターフェイスとコマンドラインインターフェイスを提供します。「インストーラー」を参照してください。

製品ISOには、Active Directory内のマシンにVDAをインストール、アップグレード、または削除するサンプルスクリプトが含まれています。これらのスクリプトを使用して、Machine Creation Services (MCS) およびCitrix Provisioning (旧Provisioning Services) で使用されるイメージを管理

することもできます。詳細については、スクリプトを使用したVDAのインストールを参照してください。

インストール前に確認する情報

- 技術概要: 製品とそのコンポーネントについて理解を深めるため。
- セキュリティ: 展開環境を計画する際。
- 既知の問題: このバージョンで発生する可能性のある問題。
- データベース: システムデータベースとその構成方法について学習します。Controllerのインストール中に、サイトデータベースとして使用するためにSQL Server Expressをインストールできます。ほとんどのデータベース情報は、コアコンポーネントのインストール後にサイトを作成するときに構成します。
- Remote PC Access: ユーザーがオフィスにある物理マシンにリモートでアクセスできるようにする環境を展開する場合。
- 接続とリソース: アプリケーションやデスクトップ用のVMをホストまたはプロビジョニングするためにハイパーバイザーまたはその他のサービスを使用している場合。最初の接続は、サイトを作成するとき（コアコンポーネントのインストール後）に構成できます。それまでに仮想化環境をセットアップしてください。
- Microsoft System Center Configuration Manager: ConfigMgrを使用してアプリケーションやデスクトップへのアクセスを管理している場合、またはRemote PC AccessでWake on LAN機能を使用している場合。
- **パブリッククラウドホスト接続:** ハイブリッド権限ライセンスをお持ちの場合、パブリッククラウドへのホスト接続を作成できます。ハイブリッド権限ライセンスに関する情報については、ハイブリッド権限の更新を参照してください。パブリッククラウドの資格とこの変更の理由に関する情報については、CTX270373を参照してください。

コンポーネントのインストール場所

サポートされているプラットフォーム、オペレーティングシステム、およびバージョンについては、システム要件を確認してください。コンポーネントの前提条件は、特に記載がない限り自動的にインストールされます。Citrix StoreFrontおよびCitrix License Serverのサポートされているプラットフォームと前提条件については、それぞれのドキュメントを参照してください。

コアコンポーネントは、同じサーバーまたは異なるサーバーにインストールできます。

- すべてのコアコンポーネントを1つのサーバーにインストールすることは、評価、テスト、または小規模な本番展開で機能します。

- 将来の拡張に対応するため、コンポーネントを異なるサーバーにインストールすることを検討してください。たとえば、Controllerをインストールしたサーバーとは別のマシンにStudioをインストールすると、サイトをリモートで管理できます。
- ほとんどの運用環境では、コアコンポーネントを個別のサーバーにインストールすることをお勧めします。

  他のサーバーに他のコンポーネントをインストールする前に、Citrix License Serverとライセンスをインストールしてください。
- Server CoreOS（Delivery Controllerなど）にサポートされているコンポーネントをインストールするには、コマンドラインを使用する必要があります。このOSタイプにはグラフィカルインターフェイスがないため、Studioやその他のツールは別の場所にインストールし、それらをControllerサーバーにポイントしてください。

同じサーバーにDelivery Controller™とマルチセッションOS用VDAの両方をインストールできます。インストーラーを起動し、Delivery Controller（およびそのマシンにインストールしたいその他のコアコンポーネント）を選択します。その後、インストーラーを再度起動し、マルチセッションOS用の**Virtual Delivery Agent**を選択します。

各オペレーティングシステムに最新のアップデートが適用されていることを確認してください。

すべてのマシンのシステムクロックが同期されていることを確認してください。マシン間の通信を保護するKerberosインフラストラクチャには同期が必要です。

XenServerを使用している場合、仮想マシンの電源状態が登録済みと表示されていても、不明と表示されることがあります。この問題を解決するには、レジストリキー`HostTime`の値を編集して、ホストとの時刻同期を無効にします。

`HKEY_LOCAL_MACHINE\Software\Citrix\XenTools\HostTime="Local"`

`HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\XenTools\HostTime="Local"`

> **ヒント:**
>
> デフォルト値は`HostTime="UTC"`です。この値をUTC以外のもの（たとえば、`Local`）に変更してください。この変更により、ホストとの時刻同期が実質的に無効になります。

> Windows 10シングルセッションマシン向けの最適化ガイダンスは、CTX216252で入手できます。

コンポーネントをインストールしない場所:

- Active Directoryドメインコントローラーには、いかなるコンポーネントもインストールしないでください。
- SQL Serverクラスタリングインストール、SQL Serverミラーリングインストール、またはHyper-Vを実行しているサーバーのノードにControllerをインストールすることはサポートされていません。

この製品バージョンがサポートしていないWindows OSにVDAをインストールまたはアップグレードしようとすると、オプションを説明する記事へのメッセージが表示されます。

権限とActive Directoryの要件

コンポーネントをインストールするマシンでは、ドメインユーザーであり、ローカル管理者である必要があります。

スタンドアロンVDAインストーラーを使用するには、管理者特権を昇格させるか、**管理者として実行**を使用する必要があります。

インストールを開始する前に、Active Directory ドメインを構成してください。

- システム要件には、サポートされているActive Directoryの機能レベルが記載されています。Active Directoryへの参加には、詳細情報が含まれています。
- Active Directoryドメインサービスを実行しているドメインコントローラーが少なくとも1つ必要です。
- ドメインコントローラーには、Citrix Virtual Apps™ and Desktopsのコンポーネントをインストールしないでください。
- Studioで組織単位名を指定する際に、スラッシュ (/) を使用しないでください。

Citrixライセンスサーバーのインストールに使用されるWindowsユーザーアカウントは、委任管理のフル管理者として自動的に構成されます。

詳細については、以下を参照してください。

- セキュリティのベストプラクティス
- 委任管理
- Active Directory構成に関するMicrosoftのドキュメント

インストールのガイダンス、考慮事項、およびベストプラクティス

いずれかのコンポーネントのインストール中

- フルプロダクトメディアからDelivery Controller、Studio、License Server、またはDirectorをインストールまたはアップグレードする際に、Citrixインストーラーがマシン上の以前のWindowsインストールから再起動が保留中であることを検出すると、インストーラーは終了/リターンコード9で停止します。マシンの再起動を求められます。

  これはCitrixによって強制される再起動ではありません。以前にマシンにインストールされた他のコンポーネントが原因です。この状況が発生した場合は、マシンを再起動してからCitrixインストーラーを再度起動してください。

  コマンドラインインターフェイスを使用する場合、コマンドに `/no_pending_reboot_check` オプションを含めることで、保留中の再起動のチェックを回避できます。

- 通常、コンポーネントに前提条件がある場合、インストーラーはそれらが存在しない場合に展開します。一部の前提条件では、マシンの再起動が必要になる場合があります。
- インストール前、インストール中、インストール後にオブジェクトを作成するときは、各オブジェクトに一意の名前を指定してください。たとえば、ネットワーク、グループ、カタログ、リソースには一意の名前を付けてください。
- コンポーネントのインストールが正常に完了しなかった場合、インストールはエラーメッセージとともに停止します。正常にインストールされたコンポーネントは保持されます。それらを再インストールする必要はありません。
- コンポーネントをインストール（またはアップグレード）すると、Citrix Analyticsが自動的に収集されます。デフォルトでは、インストールが完了するとそのデータは自動的にCitrixにアップロードされます。また、コンポーネントをインストールすると、匿名データをアップロードするCitrix Customer Experience Improvement Program (CEIP)に自動的に登録されます。

  インストール中に、メンテナンスとトラブルシューティングのための診断情報を収集する他のCitrixテクノロジーに参加することも選択できます。これらのプログラムの詳細については、「Citrix Insight Services」を参照してください。

- VDAのインストールが失敗した場合、MSIアナライザーは失敗したMSIログを解析し、正確なエラーコードを表示します。既知の問題である場合、アナライザーはCTX記事を提案します。アナライザーはまた、失敗エラーコードに関する匿名化されたデータを収集します。このデータは、CEIPによって収集された他のデータとともに含まれます。CEIPへの登録を終了した場合、収集されたMSIアナライザーデータはCitrixに送信されなくなります。

VDAのインストール中

- Windows向けCitrix Workspace™アプリは利用可能ですが、VDAをインストールする際にはデフォルトではインストールされません。ユーザーまたは管理者は、Citrix Webサイトから Windows向けCitrix Workspaceアプリやその他のCitrix Workspaceアプリをダウンロードしてインストール（およびアップグレード）できます。または、それらのCitrix Workspaceアプリを StoreFrontサーバーから利用可能にすることもできます。StoreFrontのドキュメントを参照してください。
- Microsoft Print Spoolerサービスは有効にする必要があります。このサービスが無効になっている場合、VDAを正常にインストールすることはできません。
- ほとんどのサポートされているWindowsエディションには、Microsoft Media Foundationがすでにインストールされています。マシンにMedia Foundationがない場合（Nエディションなど）、いくつかのマルチメディア機能はインストールされず、動作しません。
  - Windows Mediaリダイレクト
  - HTML5 ビデオリダイレクト
  - HDX™ RealTime Webカメラリダイレクト

  制限を承諾するか、VDAのインストールを終了して、Media Foundationのインストール後に再開することができます。グラフィカルインターフェイスでは、この選択肢はメッセージで表示されます。コマンドラインでは、`/no_mediafoundation_ack`オプションを使用して制限を承諾できます。
- VDAをインストールすると、**Direct Access Users**という新しいローカルユーザーグループが自動的に作成されます。シングルセッションOS用VDAでは、このグループはRDP接続にのみ適用されます。マルチセッションOS用VDAでは、このグループはICA®およびRDP接続に適用されます。
- VDAは、通信するための有効なControllerアドレスを持っている必要があります。そうでない場合、セッションを確立できません。Controllerアドレスは、VDAのインストール時または後で指定できます。これを行う必要があることを忘れないでください。詳細については、「VDA登録」を参照してください。

VDAインストール後およびインストール中の再起動

VDAインストールの終了時に再起動が必要です。この再起動は、デフォルトで自動的に行われます。

VDAをバージョン7.17（またはそれ以降のサポートされているバージョン）にアップグレードする場合、アップグレード中に再起動が発生します。これは回避できません。

VDAのインストール中に必要な再起動の回数を最小限に抑えるには：

- VDAのインストールを開始する前に、サポートされている.NET Frameworkバージョンがインストールされていることを確認してください。
- WindowsマルチセッションOSマシンでは、VDAをインストールする前にRDSロールサービスをインストールして有効にしてください。

VDAをインストールする前にこれらの前提条件をインストールしない場合：

- グラフィカルインターフェイスまたは`/noreboot`オプションを使用しないコマンドラインインターフェイスを使用している場合、前提条件のインストール後にマシンは自動的に再起動します。
- `/noreboot`オプションを使用するコマンドラインインターフェイスを使用している場合、再起動を開始する必要があります。

VDAバージョンをアップグレードする際、アップグレード中に再起動が発生します。これは回避できません。

インストールまたはアップグレードの失敗時の復元

> **注:**

> この機能は、シングルセッションおよびマルチセッションVDAで利用できます。

> シングルセッションVDAのインストールまたはアップグレードが失敗し、「障害時の復元」機能が有効になっている場合、マシンはインストールまたはアップグレードが開始される前に設定された復元ポイントに戻されます。

マルチセッションVDAのインストールまたはアップグレードが失敗し、「障害発生時の復元」機能が有効になっている場合、マシンはインストールまたはアップグレードが開始される前に実行されたバックアップの状態に戻されます。

この機能が有効な状態でシングルセッションVDAのインストールまたはアップグレードが開始されると、インストーラーは実際のインストールまたはアップグレードを開始する前にシステム復元ポイントを作成します。VDAのインストールまたはアップグレードが失敗した場合、マシンは復元ポイントの状態に戻されます。`%temp%/Citrix`フォルダーには、展開ログと復元に関するその他の情報が含まれています。

この機能を有効にしてマルチセッションVDAのインストールまたはアップグレードを開始すると、インストーラーは実際のインストールまたはアップグレードを開始する前にサーバーバックアップを作成します。VDAのインストールまたはアップグレードが失敗した場合、マシンはバックアップ状態に戻されます。`%temp%/Citrix`フォルダーには、展開ログと復元に関するその他の情報が含まれています。サーバーバックアップの作成にかかる時間は、必要なバックアップのサイズとサーバーで利用可能なリソースの量に基づきます。バックアップは *C:\WindowsImageBackup\servername* に保存されます。

デフォルトでは、この機能は無効になっています。

この機能を有効にする予定がある場合は、GPO設定 (`Computer Configuration > Administrative Templates > System > System Restore`) によってシステム復元が無効になっていないことを確認してください。

> **注:**
>
> このGPO設定は、マルチセッションVDAの復元には適用されません。

> シングルセッションまたはマルチセッションVDAをインストールまたはアップグレードする際にこの機能を有効にするには：

- VDAインストーラーのグラフィカルインターフェイスを使用する場合（**Autostart**または復元オプションやサイレントオプションなしで`XenDesktopVDASetup.exe`コマンドを使用する場合など）は、**Summary**ページで**Enable automatic restore if update fails**チェックボックスをオンにします。

  インストール/アップグレードが正常に完了した場合、復元ポイント/バックアップは使用されませんが、保持されます。
- コマンドラインを使用して、`/enablerestore`または`/enablerestorecleanup`オプションのいずれかでVDAインストーラーを実行します。
  - `/enablerestorecleanup`オプションを使用し、インストール/アップグレードが正常に完了した場合、復元ポイント/サーバーバックアップは自動的に削除されます。
  - `/enablerestore`オプションを使用し、インストール/アップグレードが正常に完了した場合、復元ポイントは使用されませんが、保持されます。

インストーラー

フルプロダクトインストーラー

ISOで提供されているフルプロダクトインストーラーを使用すると、次のことができます。

- コアコンポーネント（Delivery Controller、Studio、Director、およびLicense Server）をインストール、アップグレード、または削除します。
- StoreFrontをインストールまたはアップグレードします。
- シングルセッションまたはマルチセッションOS用のWindows VDAをインストールまたはアップグレードします。
- Universal Print Server `UpsServer` コンポーネントをプリントサーバーにインストールします。
- Federated Authentication Serviceをインストールします。
- Session Recordingをインストールします。
- Workspace Environment Managementをインストールします。

> **注:**
>
> Workspace Environment Management™ Agent インストーラーはローカライズされていません。英語でのみ利用可能です。

1 人のユーザー (Web 開発など) 向けにマルチセッション OS からデスクトップを配信するには、製品版インストーラーのコマンドラインインターフェイスを使用します。詳細については、Server VDI を参照してください。

スタンドアロン VDA インストーラー

スタンドアロンVDAインストーラーは、Citrixダウンロードページから入手できます。（製品インストールメディアからは入手できません。）スタンドアロンVDAインストーラーは、フルプロダクトISOよりもはるかに小さく、次のような展開に容易に対応できます。

- ローカルにステージングまたはコピーされた電子ソフトウェア配布（ESD）パッケージを使用する
- 物理マシンを使用する
- リモートオフィスを持つ

デフォルトでは、自己解凍型スタンドアロンVDAのファイルは**Temp**フォルダーに抽出されます。フルプロダクトインストーラーを使用する場合よりも、**Temp**フォルダーに抽出する方がマシンにより多くのディスク容量が必要です。ただし、**Temp**フォルダーに抽出されたファイルは、インストール完了後に自動的に削除されます。または、絶対パスを指定して`/extract`コマンドを使用することもできます。

4つのスタンドアロンVDAインストーラーをダウンロードできます。

マルチセッションOS Virtual Delivery Agent (VDAServerSetup.exe):

マルチセッションOS用のVDAをインストールします。フルプロダクトインストーラーで利用可能なマルチセッションOS用VDAのすべてのオプションをサポートします。

シングルセッションOS Virtual Delivery Agent (VDAWorkstationSetup.exe):

シングルセッションOS用のVDAをインストールします。フルプロダクトインストーラーで利用可能なシングルセッションOS用VDAのすべてのオプションをサポートします。

シングルセッションOSコアサービス Virtual Delivery Agent (VDAWorkstationCoreSetup.exe):

Remote PC Access展開またはコアVDIインストール用に最適化されたシングルセッションOS用のVDAをインストールします。Remote PC Accessは物理マシンを使用します。コアVDIインストールは、イメージとして使用されていないVMです。このような展開に必要なVDA接続用のコアサービスのみをインストールします。そのため、フルプロダクトインストーラーまたは`VDAWorkstationSetup.exe`インストーラーで有効なオプションのごく一部のみをサポートします。

このインストーラーは、以下の目的で使用されるコンポーネントをインストールまたは含みません。

- アップブイ。
- Profile Management。Citrix Profile Managementをインストールから除外すると、Citrix Directorの表示に影響します。詳細については、「VDAのインストール」を参照してください。
- マシンIDサービス。
- シトリックス MCS IODriver
- Citrix バックアップと復元
- deviceTRUST
- uberAgent

- WEM

`VDAWorkstationCoreSetup.exe`インストーラーは、次のコンポーネントをインストールまたは含んでいません：Citrix Workspace app for Windows (CWA)、Citrix Secure Access Client (CSA)、Citrix User Personalization Layer (UPL)、Session Recording Agent (SRAGENT)、Citrix Assistant App (ASSISTANTAPP)。

`VDAWorkstationCoreSetup.exe`を使用することは、フルプロダクトまたは`VDAWorkstationSetup`インストーラーを使用してシングルセッションOS VDAをインストールすることと等価であり、以下のいずれかに該当します。

- グラフィカルインターフェイスの場合：**［環境］**ページで［Remote PC Access］オプションを選択します。
- コマンドラインインターフェイスの場合：`/remotepc`オプションを指定します。
- コマンドラインインターフェイスの場合：`/components vda`と、有効な追加コンポーネント名をすべてリストする`/exclude`オプションを指定します。

省略されたコンポーネント/機能は、後でフルプロダクトインストーラーを実行してインストールできます。この操作により、不足しているすべてのコンポーネントをインストールできます。

`VDAWorkstationCoreSetup.exe`インストーラーは、Browser Content Redirection MSIを自動的にインストールします。この自動インストールは、VDAリリース2003以降のサポート対象リリースに適用されます。

シングルセッションコアサービスVirtual Delivery Agent (VDASingleSessionCoreSetup.exe):

Windows 365 Cloud PCおよびRemote PCの展開で利用できる、新しい軽量なシングルセッションVDAメタインストーラーです。このインストーラーは、既存のVDAWorkstationCoreSetup.exeインストーラーをベースにしており、Profile Management、deviceTRUST、uberAgent、WEM、Backup and Restore、およびVDA Upgrade Agentとともに、必須のVDAコンポーネントを提供します。Backup and Restore機能は、コマンドラインオプション/enablerestoreまたは/enablerestorecleanupを使用して有効にできます。

これにより、パッケージサイズが大幅に削減され、クラウドベースのワークロードのインストール信頼性が向上します。最新のRemote PCシナリオ向けに設計されたこのインストーラーは、Windows 365およびRemote PCにCitrixワークロードを展開するための、簡素化された高性能なオプションを提供します。

シングルセッション VDA インストーラーを使用するためのベストプラクティス

シングルセッションオペレーティングシステムには、4種類のインストーラーが用意されています。フルプロダクト VDA インストーラーと VDAWorkstationSetup.exe インストーラーはすべてのコンポーネントのインストールを提供しますが、VDAWorkstationCoreSetup.exe および VDASingleSessionCoreSetup.exe インストーラーには一部のデフォルトおよび追加コンポーネントは含まれていません。

環境の安定性、一貫したパフォーマンス、および継続的なサポート性を維持するために、Citrix は、インストール、アップグレード、アンインストールを含むCitrix VDAのライフサイクル全体で、一貫したインストーラータイプを使用することを推奨しています。インストーラータイプを混在させると、特定のリスクが生じる可能性があります。

インストーラータイプの混在に関連するリスク：

シナリオ1： シングルセッションVDAがVDAWorkstationCoreSetup.exeまたはVDASingleSessionCoreSetup.exeインストーラーを使用して最初にインストールされ、その後フルプロダクトVDAインストーラーまたはVDAWorkstationSetup.exeインストーラーのいずれかでアップグレードされた場合、以前に除外されていたコンポーネントは、明示的に除外されない限り、アップグレード中にインストールされる可能性があります。

シナリオ2： シングルセッションVDAがフルプロダクトVDAインストーラーまたはVDAWorkstationSetup.exeを使用して最初にインストールされ、その後VDAWorkstationCoreSetup.exeまたはVDASingleSessionCoreSetup.exeを使用してアップグレードされた場合、コアサービスVDAインストーラーによってインストールされなかったコンポーネントはアップグレードから除外されます。これらのコンポーネントは、アップグレードプロセス中にアップグレードされることも、アンインストール中に削除されることもありません。

シナリオ3： シングルセッションVDAがVDAWorkstationCoreSetup.exeインストーラーを使用して最初にインストールされ、その後VDASingleSessionCoreSetup.exeでアップグレードされた場合、新しい機能が利用可能になります。次回VDAWorkstationCoreSetup.exeでアップグレードした場合、VDASingleSessionCoreSetup.exeによって新しく追加されたコンポーネントは、アップグレードプロセス中にアップグレードされることも、アンインストール中に削除されることもありません。

インストーラータイプの混在に対処するためのガイダンス：

インストーラータイプを混在させる必要がある場合は、アップグレードプロセス中に同じコンポーネントが含まれるようにすることが不可欠です。

インストーラータイプが誤って混在し、追加のコンポーネントがインストールされたり、特定のコンポーネントが管理対象外になったりした場合で、以前の環境を復元する必要がある場合は、次のように進めてください。

- **シナリオ1の場合：** プログラムのアンインストールまたは変更のためのWindows機能からVDAをアンインストールし、その後、最初にVDAをインストールしたインストーラー（VDAWorkstationCoreSetup.exeまたはVDASingleSessionCoreSetup.exe）を使用してVDAを再インストールします。
- **シナリオ2の場合：** 不足しているコンポーネントを、フルプロダクトVDAインストーラーまたはVDAWorkstationSetup.exeインストーラーを使用してアップグレードします。
- **シナリオ3の場合：** 新しい機能を引き続き活用する予定がある場合は、VDASingleSessionCoreSetup.exeインストーラーを使用して不足しているコンポーネントをアップグレードします。または、VDASingleSessionCoreSetup.exeでアップグレードした後に新しい機能を使用しない場合は、まずプログラムのアンインストールまたは変更のためのWindows機能からVDAをアンインストールし、その後VDAWorkstationCoreSetup.exeを使用してVDAを再インストールします。

Citrixインストールのリターンコード

インストールログには、コンポーネントのインストールの結果が、Microsoft の値ではなく Citrix の戻りコードとして含まれています。

- 0 = 成功
- 1 = 失敗
- 2 = 部分的な成功
- 3 = 部分的な成功と再起動が必要
- 4 = 失敗と再起動が必要
- 5 = ユーザーがキャンセル
- 6 = 不正なコマンドライン引数
- 7 = 新しいバージョンが見つかりました
- 8 = 成功と再起動が必要
- 9 = ファイルロック再起動
- 10 = 中止
- 11 = メディア失敗
- 12 = ライセンス失敗

- 13 = 事前チェック失敗
- 14 = 再起動保留中チェック中止
- 15 = PrecheckPass - これは、新しい /precheckonly コマンドラインオプションを使用した後に事前チェックが合格した場合に返されます。
- 16 = PrecheckFail - これは、新しい /precheckonly コマンドラインオプションを使用した後に事前チェックが失敗した場合に返されます。
- 17 = OptionalSoftwareFailed - これは、新しいオプションソフトウェアコンポーネントのいずれかのインストールに失敗し、「他の選択されたコンポーネントが失敗した場合でもVDAのインストールまたはアップグレードを続行する」が選択されている場合に返されます。

たとえば、Microsoft System Center Configuration Managerなどのツールを使用する場合、インストールログにリターンコード3が含まれていると、スクリプトによるVDAインストールが失敗したように見えることがあります。これは、VDAインストーラーが、ユーザーが開始する必要のある再起動（たとえば、サーバーでのRDSロールの前提条件のインストール後など）を待機している場合に発生する可能性があります。VDAのインストールは、すべての前提条件と選択されたコンポーネントがインストールされ、インストール後にマシンが再起動された場合にのみ成功と見なされます。

または、インストールをCMDスクリプト（Microsoftの終了コードを返します）でラップするか、Configuration Managerパッケージの成功コードを変更することもできます。

Windows Serverワークロード向けにMicrosoft RDSライセンスサーバーを構成する

この製品は、Windows 2016などのWindows Serverワークロードを提供するときに、Windows Serverのリモートセッション機能にアクセスします。これには通常、リモートデスクトップサービス クライアントアクセスライセンス（RDS CAL）が必要です。VDAは、RDS CALを要求するためにRDSライセンスサーバーに接続できる必要があります。ライセンスサーバーをインストールしてアクティブ化します。詳しくは、Microsoftドキュメント「リモートデスクトップサービスライセンスサーバーをアクティブ化する」を参照してください。概念実証環境では、Microsoftが提供する猶予期間を使用できます。

この方法では、このサービスにライセンスサーバー設定を適用させることができます。イメージ上のRDSコンソールで、ライセンスサーバーとユーザーごとのモードを構成できます。Microsoftグループポリシー設定を使用してライセンスサーバーを構成することもできます。詳しくは、Microsoftドキュメント「クライアントアクセスライセンス（CAL）を使用してRDS展開をライセンスする」を参照してください。

グループポリシー設定を使用してRDSライセンスサーバーを構成するには:

1. 利用可能なマシンにリモートデスクトップサービスライセンスサーバーをインストールします。このマシンは常に利用可能である必要があります。Citrix製品のワークロードは、このライセンスサーバーに到達できる必要があります。
2. Microsoftグループポリシーを使用して、ライセンスサーバーのアドレスとユーザーごとのライセンスモードを指定します。詳しくは、Microsoftドキュメント「RDセッションホストサーバーのリモートデスクトップライセンスモードを指定する」を参照してください。

Windows 10ワークロードには、適切なWindows 10ライセンスのアクティベーションが必要です。Windows 10ワークロードをアクティベートするには、Microsoftのドキュメントに従うことをお勧めします。

詳細情報

特定のホストタイプのリソースの場所を設定する場合:

- AWSクラウド環境
- XenServer仮想化環境
- Google Cloud環境
- Microsoft Azure Resource Managerクラウド環境
- マイクロソフト システム センター コンフィギュレーション マネージャー の環境
- マイクロソフト システム センター バーチャル マシン マネージャー の仮想化環境
- Nutanix仮想化環境
- Nutanixクラウドおよびパートナーソリューション
- VMware 仮想化環境
- VMware クラウドおよびパートナーソリューション

AWSクラウド環境

この記事では、Citrix Virtual Apps and Desktops で使用できるリソースの場所として AWS アカウントを設定する方法について説明します。このリソースの場所は、AWS EC2 および Amazon WorkSpaces Core マネージドインスタンスでワークロードをプロビジョニングするために使用されます。Amazon WorkSpaces Core マネージドインスタンスでサポートされている OS の種類のリストについては、「Amazon WorkSpaces Core マネージドインスタンスの VDA」を参照してください。

構成可能なさまざまなリソースの場所の比較: AWS EC2 用 MCS、Amazon WorkSpaces Core マネージドインスタンス用 MCS、および Amazon WorkSpaces Core バンドル用クイック展開。

AWS EC2 用 MCS	AMAZON WORKSPACES CORE マネージドインスタンス用 MCS	AMAZON WORKSPACES CORE バンドル用クイック展開
Citrix® は、AWS アカウントでの VM のプロビジョニングを処理します	Citrix は、AWS アカウントでの VM のプロビジョニングを処理します	Amazon は、AWS マネージド WorkSpaces アカウントでの VM のプロビジョニングを処理します
VM ライフサイクル管理のための高度な MCS ワークフロー	VM ライフサイクル管理のための高度な MCS ワークフロー	5 ステップの迅速で簡単なワークフロー
EC2 インスタンス	WorkSpaces Core マネージドインスタンス (AWS アカウントに直接起動されるオンデマンド EC2 インスタンスを利用)	WorkSpaces バンドル、完全に AWS マネージド容量 (より高いレベルの抽象化)
Microsoft 365 ライセンスのサポートなし	BYOL Microsoft 365 のサポート	BYOL Microsoft 365 のサポート
Windows サーバー、Windows デスクトップ、および リナックス	Windows サーバー、Windows デスクトップ、および リナックス	ウィンドウズ サーバー、ウィンドウズ デスクトップ
永続VMと非永続VM	永続VMと非永続VM	永続VMのみ
従量課金制のみ	従量課金制	月額固定料金のみ
シトリックス DaaS および シトリックス バーチャル アプリケーションズ アンド デスクトップ™	シトリックス DaaS および シトリックス バーチャルアップス アンド デスクトップス™	Citrix DaaS のみ

この記事のタスクを完了すると、リソースロケーションには次のコンポーネントが含まれます。

- 単一のアベイラビリティゾーン内にパブリックサブネットとプライベートサブネットを持つ仮想プライベートクラウド (VPC)。
- VPCのプライベートサブネットに配置され、Active Directoryドメインコントローラーと DNS サーバーの両方として実行されるインスタンス。

- VPCのパブリックサブネットで踏み台ホストとして機能するインスタンス。このインスタンスは、管理目的でプライベートサブネット内のインスタンスへのRDP接続を開始するために使用されます。リソースの場所の設定が完了したら、このインスタンスをシャットダウンして、簡単にアクセスできないようにすることができます。VDAインスタンスなど、プライベートサブネット内の他のインスタンスを管理する必要がある場合は、踏み台ホストインスタンスを再起動できます。

タスクの概要

パブリックサブネットとプライベートサブネットを持つ仮想プライベートクラウド (VPC) をセットアップします。 このタスクを完了すると、AWSはパブリックサブネットにElastic IPアドレスを持つNATゲートウェイを展開します。このアクションにより、プライベートサブネット内のインスタンスがインターネットにアクセスできるようになります。パブリックサブネット内のインスタンスは受信パブリックトラフィックにアクセスできますが、プライベートサブネット内のインスタンスはアクセスできません。

セキュリティグループを構成します。セキュリティグループは、VPC内のインスタンスのトラフィックを制御する仮想ファイアウォールとして機能します。パブリックサブネット内のインスタンスがプライベートサブネット内のインスタンスと通信できるようにするルールをセキュリティグループに追加します。また、これらのセキュリティグループをVPC内の各インスタンスに関連付けます。

DHCPオプションセットを作成します。Amazon VPCでは、DHCPおよびDNSサービスがデフォルトで提供されており、Active Directoryドメインコントローラーでの DNSの構成方法に影響します。AmazonのDHCPは無効にできず、AmazonのDNSはパブリックDNS解決にのみ使用でき、Active Directory名解決には使用できません。DHCPを介してインスタンスに渡されるドメインとネームサーバーを指定するには、DHCPオプションセットを作成します。このセットは、Active Directoryドメインサフィックスを割り当て、VPC内のすべてのインスタンスのDNSサーバーを指定します。インスタンスがドメインに参加したときにホスト (A) および逆引き参照 (PTR) レコードが自動的に登録されるようにするには、プライベートサブネットに追加する各インスタンスのネットワークアダプタープロパティを構成します。

踏み台ホストとドメインコントローラーをVPCに追加します。踏み台ホストを介して、プライベートサブネット内のインスタンスにログオンし、ドメインを設定してインスタンスをドメインに参加させることができます。

タスク1: VPCをセットアップする

1. AWSマネジメントコンソールから、**VPC**を選択します。
2. VPCダッシュボードから、**VPCを作成**を選択します。

3. **VPCなど**を選択します。
4. NATゲートウェイ ($) の下で、**1つのAZ内**または**AZごとに1つ**を選択します。
5. DNSオプションの下で、**DNSホスト名を有効にする**を選択したままにします。
6. 「**VPC の作成**」を選択します。AWS は、パブリックサブネットとプライベートサブネット、インターネットゲートウェイ、ルートテーブル、およびデフォルトのセキュリティグループを作成します。

タスク 2: セキュリティグループの構成

このタスクでは、VPC 用に次のセキュリティグループを作成および構成します:

- パブリックサブネット内のインスタンスに関連付けるためのパブリックセキュリティグループ。
- プライベートサブネット内のインスタンスに関連付けるためのプライベートセキュリティグループ。

セキュリティグループを作成するには:

1. VPC ダッシュボードで、「**Security Groups**」を選択します。
2. パブリックセキュリティグループ用のセキュリティグループを作成します。「**Create Security Group**」を選択し、グループの名前タグと説明を入力します。VPC で、以前に作成した VPC を選択します。「**Yes, Create**」を選択します。

パブリックセキュリティグループの構成

1. セキュリティグループリストから、パブリックセキュリティグループを選択します。
2. 「**インバウンドルール**」タブを選択し、「**編集**」を選択して、以下のルールを作成します。

タイプ	送信元
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	パブリックセキュリティグループを選択します。
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0

タイプ	送信元
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (セッションの信頼性)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. 完了したら、**保存**を選択します。
4. **［Outbound Rules］タブを選択し、［Edit］**を選択して、次のルールを作成します。

タイプ	送信先
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	0.0.0.0/0
ICMP	0.0.0.0/0

5. 完了したら、**保存**を選択します。

プライベートセキュリティグループを構成する

1. セキュリティグループのリストから、プライベートセキュリティグループを選択します。
2. パブリックセキュリティグループからのトラフィックを設定していない場合は、TCPポートを設定する必要があります。**［Inbound Rules］タブを選択し、［Edit］**を選択して、次のルールを作成します。

タイプ	送信元
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	パブリックセキュリティグループを選択します。
ICMP	パブリックセキュリティグループを選択します。

タイプ	送信元
TCP 53 (DNS)	パブリックセキュリティグループを選択します。
UDP 53 (DNS)	パブリックセキュリティグループを選択します。
80 (HTTP)	パブリックセキュリティグループを選択します。
TCP 135	パブリックセキュリティグループを選択します。
TCP 389	パブリックセキュリティグループを選択します。
UDP 389	パブリックセキュリティグループを選択します。
443 (HTTPS)	パブリックセキュリティグループを選択します。
TCP 1494 (ICA/HDX)	パブリックセキュリティグループを選択します。
TCP 2598 (セッションの信頼性)	パブリックセキュリティグループを選択します。
3389 (RDP)	パブリックセキュリティグループを選択します。
TCP 49152–65535	パブリックセキュリティグループを選択します。

3. 完了したら、**保存**を選択します。
4. **アウトバウンドルール**タブを選択し、**編集**を選択して、次のルールを作成します:

タイプ	宛先
すべてのトラフィック	プライベートセキュリティグループを選択します。

タイプ	宛先
すべてのトラフィック	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

5. 完了したら、**保存**を選択します。

タスク3：インスタンスの起動

次の手順を実行して、2つのEC2インスタンスを作成し、Amazonが生成するデフォルトの管理者パスワードを復号化します:

1. AWSマネジメントコンソールから、**EC2**を選択します。
2. EC2ダッシュボードから、**インスタンスの起動**を選択します。
3. Windows Serverマシンイメージとインスタンスタイプを選択します。
4. **インスタンスの詳細の設定**ページで、インスタンスの名前を入力し、以前に設定したVPCを選択します。
5. **サブネット**で、各インスタンスについて次の選択を行います。
   - Bastionホスト: パブリックサブネットを選択します。
   - ドメインコントローラー: プライベートサブネットを選択します。
6. **パブリックIPの自動割り当て**で、各インスタンスについて次の選択を行います。
   - Bastionホスト: **有効**を選択します。
   - ドメインコントローラー: **デフォルト設定を使用**または**無効**を選択します。
7. **ネットワークインターフェイス**で、ドメインコントローラーのプライベートサブネットのIP範囲内でプライマリIPアドレスを入力します。
8. 必要に応じて、**ストレージの追加**ページでディスクサイズを変更します。
9. **インスタンスのタグ付け**ページで、各インスタンスにわかりやすい名前を入力します。
10. **セキュリティグループの設定**ページで、**既存のセキュリティグループを選択する**を選択し、各インスタンスについて次の選択を行います。
    - Bastionホスト: パブリックセキュリティグループを選択します。
    - ドメインコントローラー: プライベートセキュリティグループを選択します。

11. 選択内容を確認し、**起動**を選択します。
12. 新しいキーペアを作成するか、既存のキーペアを選択します。新しいキーペアを作成する場合は、プライベートキー（.pem）ファイルをダウンロードし、安全な場所に保管してください。インスタンスのデフォルトの管理者パスワードを取得する際に、プライベートキーを提供する必要があります。
13. **インスタンスの起動**を選択します。**インスタンスの表示**を選択して、インスタンスのリストを表示します。新しく起動したインスタンスにアクセスする前に、すべてのステータスチェックに合格するまで待機します。
14. 各インスタンスのデフォルトの管理者パスワードを取得します:
    a. インスタンスリストから、インスタンスを選択し、「**接続**」を選択します。
    b. 「**RDP クライアント**」タブに移動し、「**パスワードの取得**」を選択し、プロンプトが表示されたら秘密鍵 (`.pem`) ファイルをアップロードします。
    c. 「**パスワードの復号**」を選択して、人間が読めるパスワードを取得します。AWSはデフォルトのパスワードを表示します。
15. 手順2から繰り返して、2つのインスタンスを作成します。
    - パブリックサブネットに1つの踏み台ホストインスタンス
    - ドメインコントローラーとして使用するプライベートサブネット内のインスタンスを1つ。

タスク4：DHCPオプションセットを作成する

1. VPCダッシュボードから、「**DHCPオプションセット**」を選択します。
2. 次の情報を入力します。
    - 名前タグ: セットのわかりやすい名前を入力します。
    - ドメイン名: ドメインコントローラーインスタンスを構成するときに使用する完全修飾ドメイン名を入力します。
    - ドメインネームサーバー: ドメインコントローラーインスタンスに割り当てたプライベートIPアドレスと、コンマで区切られた文字列 **AmazonProvidedDNS** を入力します。
    - NTPサーバー: このフィールドは空白のままにします。
    - NetBIOSネームサーバー: ドメインコントローラーインスタンスのプライベートIPアドレスを入力します。
    - NetBIOSノードタイプ: **2** と入力します。
3. **はい、作成します** を選択します。

4. 新しいセットをVPCに関連付けます。

    a. VPCダッシュボードから、**お使いのVPC** を選択し、以前に設定したVPCを選択します。

    b. **アクション > DHCPオプションセットの編集** を選択します。

    c. プロンプトが表示されたら、作成した新しいセットを選択し、**保存** を選択します。

タスク5: インスタンスの構成

1. RDPクライアントを使用して、踏み台ホストインスタンスのパブリックIPアドレスに接続します。プロンプトが表示されたら、管理者アカウントの資格情報を入力します。
2. 踏み台ホストインスタンスから、リモートデスクトップ接続を起動し、構成するインスタンスのプライベートIPアドレスに接続します。プロンプトが表示されたら、インスタンスの管理者資格情報を入力します。
3. プライベートサブネット内のすべてのインスタンスについて、DNS設定を構成します。

    a. **スタート > コントロールパネル > ネットワークとインターネット > ネットワークと共有センター > アダプターの設定の変更** を選択します。表示されているネットワーク接続をダブルクリックします。

    b. 「**プロパティ > インターネット プロトコル バージョン 4 (TCP/IPv4) > プロパティ**」を選択します。

    c. 「**詳細設定 > DNS**」を選択します。以下の設定が有効になっていることを確認し、「**OK**」を選択します。

        - この接続のアドレスをDNSに登録する
        - この接続のDNSサフィックスをDNS登録で使用する

4. ドメインコントローラーを構成するには:

    a. サーバーマネージャーを使用して、すべてのデフォルト機能と共にActive Directory ドメインサービス役割を追加します。

    b. インスタンスをドメインコントローラーに昇格させます。昇格中に、DNSを有効にし、DHCPオプションセットを作成したときに指定したドメイン名を使用します。プロンプトが表示されたらインスタンスを再起動します。

AWSの権限については、必要なAWS権限 - Amazon EC2および必要なAWS権限 - Amazon WorkSpaces Coreマネージドインスタンスを参照してください。

次のステップ

- コアコンポーネントをインストールする

- VDAのインストール
- サイトを作成する
- 接続の作成と管理については、以下を参照してください。
  - AWS EC2への接続
  - Amazon WorkSpaces Coreマネージドインスタンスへの接続

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Azure Local 環境

Azure Local (Azure Arc ベース) は、オンプレミスシステムをAzureに接続し、クラウドベースのサービス、監視、管理を可能にするハイパーコンバージドインフラストラクチャ (HCI) ソリューションです。

前提条件

- Azure Local クラスター: 2503 以降
  - ストレージパスが作成されていること
  - DHCPが有効な論理ネットワークが作成されていること
- Azure Local クラスターを展開するには、Microsoft ドキュメントのAzure Local の展開についてを参照してください。

考慮事項

- Windows 10 および 11 のマルチセッションワークロードはサポートされていません。

主な手順

Azure Local クラスターで MCS カタログを作成するための主要な手順は次のとおりです。

1. ホスト接続を作成します。
2. カタログを作成します。

次のステップ

- Azure Local への接続を作成するには、Azure Local への接続を参照してください。

詳細情報

- 接続とリソースの作成および管理

XenServer® 仮想化環境

XenServer は、運用管理を簡素化し、負荷の高いワークロード向けに高精細なユーザーエクスペリエンスを保証します。

XenServer をセットアップするには、インストール準備を参照してください。

次に行うこと

- コアコンポーネントのインストール
- VDA のインストール
- サイトの作成
- XenServer で接続を作成および管理するには、XenServer への接続を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Google Cloud環境

Citrix Virtual Apps and Desktops™ を使用すると、Google Cloud 上でマシンのプロビジョニングと管理を行うことができます。

要件

- Citrix Cloud™ アカウント。この記事で説明されている機能は、Citrix Cloud でのみ利用可能です。
- Google Cloud プロジェクト。このプロジェクトには、マシンカタログに関連付けられているすべてのコンピューティングリソースが保存されます。既存のプロジェクトでも新規のプロジェクトでもかまいません。
- Google Cloud プロジェクトで4つのAPIを有効にします。詳細については、「Enable Google Cloud APIs」を参照してください。
- Google Cloud サービスアカウント。サービスアカウントは、プロジェクトへのアクセスを有効にするためにGoogle Cloudに対して認証を行います。詳細については、「Configure and update service accounts」を参照してください。

- Google プライベートアクセスを有効にします。詳細については、「Enable-private-google-access」を参照してください。

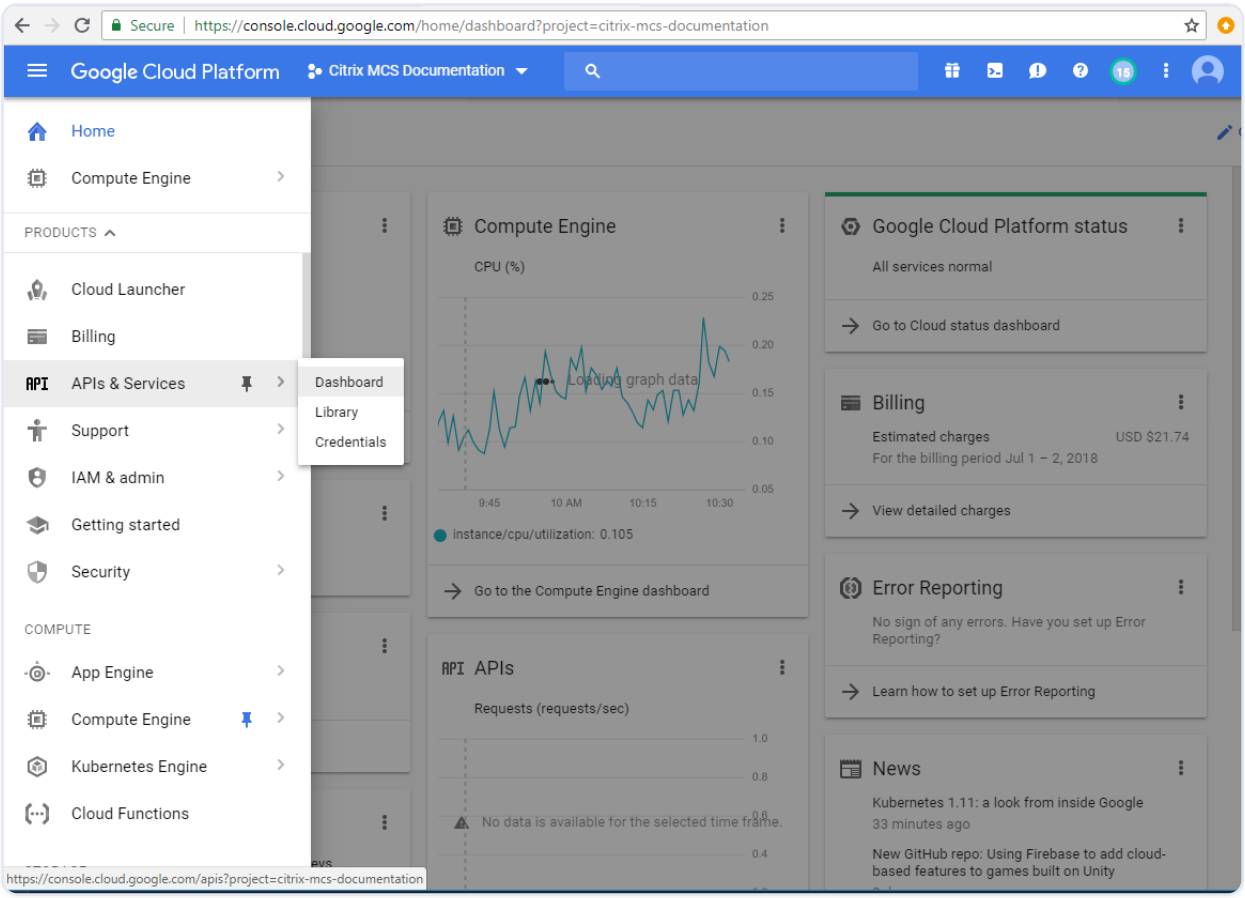
Google Cloud APIを有効にする

Web Studio を介して Google Cloud の機能を使用するには、Google Cloud プロジェクトで次の API を有効にします。

- コンピュート エンジン API
- クラウド リソース マネージャー API
- アイデンティティおよびアクセス管理 (IAM) API
- クラウドビルド API
- クラウド キー管理サービス (KMS)

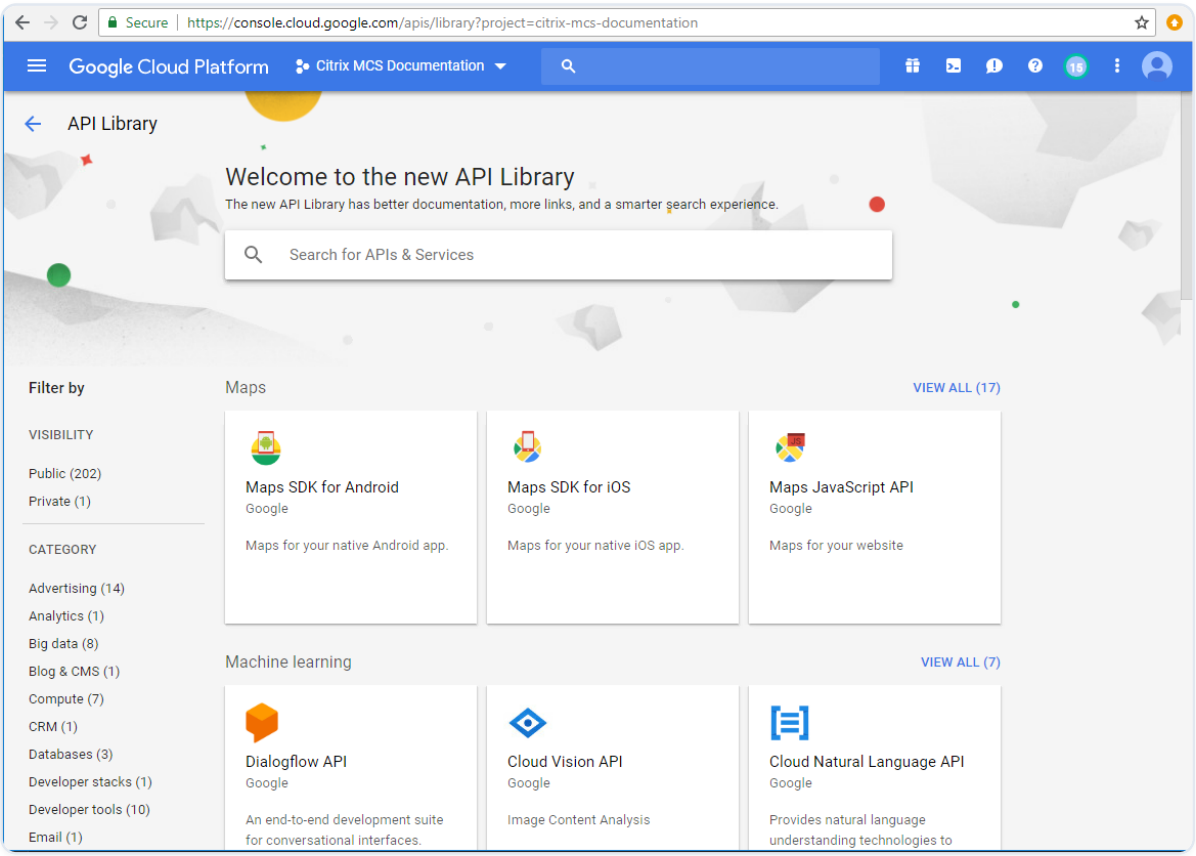
Google Cloudコンソールから、次の手順を実行します。

1. 左上のメニューで、**「APIとサービス」>「ダッシュボード」**を選択します。



2. **Dashboard** 画面で、Compute Engine API が有効になっていることを確認します。 有効になっていない場合は、次の手順に従います。

   a. 「**APIとサービス > ライブラリ**」に移動します。



b. 検索ボックスに「*Compute Engine*」と入力します。

c. 検索結果から「**Compute Engine API**」を選択します。

d. 「**Compute Engine API**」ページで、「**有効にする**」を選択します。

3. Cloud Resource Manager APIを有効にします。

a. 「**APIとサービス > ライブラリ**」に移動します。

b. 検索ボックスに「*Cloud Resource Manager*」と入力します。

c. 検索結果から「**Cloud Resource Manager API**」を選択します。

d. 「**Cloud Resource Manager API**」ページで、「**有効にする**」を選択します。APIのステータスが表示されます。

4. 同様に、**Identity and Access Management (IAM) API**と**Cloud Build API**を有効にします。

Google Cloud Shell を使用して API を有効にすることもできます。これを行うには:

1. Google コンソールを開き、Cloud Shell をロードします。
2. Cloud Shell で次の4つのコマンドを実行します。

- gcloud services enable compute.googleapis.com を実行します。
- gcloud services enable cloudresourcemanager.googleapis.com を実行します。

- gcloud services enable iam.googleapis.com を実行します。
- gcloud services enable cloudbuild.googleapis.com を実行します。

3. Cloud Shell がプロンプトを表示したら、**承認**をクリックします。

サービスアカウントの構成と更新

> **注:**
>
> GCP は、Cloud Build Service のデフォルトの動作とサービスアカウントの使用に関して、April 29, 2024 以降に変更を導入します。詳細については、Cloud Build Service Account Change を参照してください。April 29, 2024 より前に Cloud Build API が有効になっている既存の Google プロジェクトは、この変更の影響を受けません。ただし、April 29 以降も既存の Cloud Build Service の動作を維持したい場合は、Cloud Build API を有効にする前に、組織ポリシーを作成または適用して制約の適用を無効にすることができます。その結果、以下のコンテンツは April 29, 2024 以前 と April 29, 2024 以降 の2つに分かれています。新しい組織ポリシーを設定する場合は、セクション April 29, 2024 以前 に従ってください。

April 29, 2024 以前

Citrix Cloud は、Google Cloud プロジェクト内で3つの個別のサービスアカウントを使用します。

- *Citrix Cloud Service Account*: このサービスアカウントにより、Citrix Cloud は Google プロジェクトにアクセスし、マシンをプロビジョニングおよび管理できます。このサービスアカウントは、Google Cloud によって生成されたキーを使用して Google Cloud に対して認証を行います。

  このサービスアカウントは、ここに記載されているとおり手動で作成する必要があります。詳細については、「Citrix Cloud Service Account の作成」を参照してください。

  このサービスアカウントは、メールアドレスで識別できます。例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`。
- *Cloud Build サービスアカウント*: このサービスアカウントは、Google Cloud API を有効にするで言及されているすべての API を有効にすると、自動的にプロビジョニングされます。自動的に作成されたすべてのサービスアカウントを表示するには、**Google Cloud** コンソールで **IAM と管理 > IAM** に移動し、**Google 提供のロール付与を含める**チェックボックスを選択します。

  このサービスアカウントは、**プロジェクトID**と**cloudbuild**という単語で始まるメールアドレスで識別できます。例: `<project-id>@cloudbuild.gserviceaccount.com`

サービスアカウントに以下のロールが付与されていることを確認します。ロールを追加する必要がある場合は、Cloud Build サービスアカウントにロールを追加するに記載されている手順に従ってください。

  - Cloud Build サービスアカウント
  - Compute Instance 管理者
  - サービスアカウントユーザー

- *Cloud Compute サービスアカウント*: このサービスアカウントは、Compute API がアクティブ化されると、Google Cloud によって Google Cloud で作成されたインスタンスに追加されます。このアカウントには、操作を実行するための IAM 基本エディターロールがあります。ただし、より詳細な制御を行うためにデフォルトの権限を削除する場合は、以下の権限を必要とする **Storage Admin** ロールを追加する必要があります。

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

このサービスアカウントは、**プロジェクト ID** と **compute** という単語で始まるメールアドレスで識別できます。例: `<project-id>-compute@developer.gserviceaccount.com`。

CITRIX CLOUD サービスアカウントを作成する

Citrix Cloud サービスアカウントを作成するには、次の手順に従います。

1. Google Cloud コンソールで、**IAM と管理 > サービス アカウント**に移動します。
2. **サービス アカウント**ページで、**サービス アカウントを作成**を選択します。
3. **サービス アカウントの作成**ページで、必要な情報を入力し、**作成して続行**を選択します。
4. **このサービス アカウントにプロジェクトへのアクセス権を付与**ページで、**ロールを選択**ドロップダウンメニューをクリックし、必要なロールを選択します。さらにロールを追加する場合は、**+別のロールを追加**をクリックします。

   各アカウント（個人またはサービス）には、プロジェクトの管理を定義するさまざまなロールがあります。このサービス アカウントに次のロールを付与します。

   - Compute 管理者
   - Storage 管理者
   - Cloud Build 編集者

- サービス アカウント ユーザー
- クラウド データストア ユーザー
- Cloud KMS 暗号化オペレーター

Cloud KMS 暗号化オペレーターには、次の権限が必要です。

- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.get
- cloudkms.keyRings.list
- cloudkms.cryptoKeyVersions.useToDecrypt
- cloudkms.cryptoKeyVersions.useToEncrypt

> **注記:**
>
> 新しいサービスアカウントを作成する際に利用可能なロールの完全なリストを取得するには、すべてのAPIを有効にしてください。

5. **CONTINUE**をクリックします
6. **Grant users access to this service account**ページで、このサービスアカウントでアクションを実行するためのアクセス権を付与するユーザーまたはグループを追加します。
7. **DONE**をクリックします。
8. IAMメインコンソールに移動します。
9. 作成されたサービスアカウントを特定します。
10. ロールが正常に割り当てられていることを検証します。

考慮事項:

サービスアカウントを作成する際は、以下を考慮してください。

- **このサービスアカウントにプロジェクトへのアクセスを許可**および**このサービスアカウントへのユーザーアクセスを許可**の手順はオプションです。これらのオプションの構成手順をスキップすることを選択した場合、新しく作成されたサービスアカウントは、**IAMと管理 > IAM**ページに表示されません。

- サービスアカウントに関連付けられたロールを表示するには、オプションの手順をスキップせずにロールを追加します。このプロセスにより、構成されたサービスアカウントにロールが表示されるようになります。

CITRIX CLOUDサービスアカウントキー

Citrix DaaS で接続を作成するには、Citrix Cloud サービスアカウントキーが必要です。キーは認証情報ファイル (.json) に含まれています。キーを作成すると、ファイルは自動的にダウンロードされ、**ダウンロード**フォルダーに保存されます。キーを作成するときは、キーのタイプを JSON に設定してください。そうしないと、Web Studio で解析できません。

サービスアカウントキーを作成するには、**IAM と管理 > サービスアカウント**に移動し、Citrix Cloud サービスアカウントのメールアドレスをクリックします。**キー**タブに切り替えて、**キーを追加 > 新しいキーを作成**を選択します。キーのタイプとして**JSON**が選択されていることを確認してください。

> **ヒント:**
>
> Google Cloud コンソールの**サービスアカウント**ページを使用してキーを作成します。セキュリティ上の理由から、キーを定期的に変更することをお勧めします。既存の Google Cloud 接続を編集することで、新しいキーを Citrix Virtual Apps™ and Desktops アプリケーションに提供できます。

CITRIX CLOUD サービスアカウントにロールを追加する

Citrix Cloud サービスアカウントにロールを追加するには：

1. Google Cloud コンソールで、**IAM と管理 > IAM**に移動します。
2. **IAM > 権限**ページで、作成したサービスアカウントをメールアドレスで特定して見つけます。

   例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. 鉛筆アイコンを選択して、サービスアカウントのプリンシパルへのアクセスを編集します。
4. 選択したプリンシパルオプションの**「project-id」へのアクセスを編集**ページで、**別のロールを追加**を選択して、必要なロールをサービスアカウントに1つずつ追加し、**保存**を選択します。

CLOUD BUILD サービスアカウントにロールを追加する

Cloud Build サービスアカウントにロールを追加するには：

1. Google Cloud コンソールで、**IAM と管理 > IAM**に移動します。

2. 「**IAM**」ページで、**プロジェクト ID** と「**cloudbuild**」という単語で始まるメールアドレスで識別できる Cloud Build サービスアカウントを見つけます。

   例: `<project-id>@cloudbuild.gserviceaccount.com`

3. 鉛筆アイコンを選択して、Cloud Build アカウントの役割を編集します。
4. 選択したプリンシパルオプションの「**Edit access to "project-id" page**」で、「**ADD ANOTHER ROLE**」を選択して、必要な役割を Cloud Build サービスアカウントに1つずつ追加し、その後「**SAVE**」を選択します。

> **注:**
>
> すべてのAPIを有効にして、役割の完全なリストを取得します。

April 29, 2024 以降

Citrix Cloudは、Google Cloudプロジェクト内で2つの異なるサービスアカウントを使用します。

- *Citrix Cloudサービスアカウント*: このサービスアカウントにより、Citrix CloudはGoogleプロジェクトにアクセスし、マシンをプロビジョニングおよび管理できます。このサービスアカウントは、Google Cloudによって生成されたキーを使用してGoogle Cloudに認証します。

  このサービスアカウントは手動で作成する必要があります。

  このサービスアカウントは、メールアドレスで識別できます。例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`。
- *Cloud Computeサービスアカウント*: このサービスアカウントは、Google Cloud APIを有効にするで言及されているすべてのAPIを有効にすると、自動的にプロビジョニングされます。自動的に作成されたすべてのサービスアカウントを表示するには、**Google Cloud**コンソールで「**IAM & Admin > IAM**」に移動し、「**Include Google-provided role grants**」チェックボックスを選択します。このアカウントには、操作を実行するためのIAM基本編集者ロールがあります。ただし、より詳細な制御のためにデフォルトの権限を削除した場合、次の権限を必要とする**Storage Admin**ロールを追加する必要があります。
  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

このサービスアカウントは、**プロジェクトID**と「**compute**」という単語で始まるメールアドレスで識別できます。例: `<project-id>-compute@developer.gserviceaccount.com.`.

サービスアカウントに次のロールが付与されていることを確認します。

- Cloud Build サービスアカウント
- Compute Instance 管理者
- サービスアカウントユーザー

CITRIX CLOUD サービスアカウントを作成する

Citrix Cloud サービスアカウントを作成するには、次の手順に従います。

1. Google Cloud コンソールで、**IAM と管理 > サービスアカウント**に移動します。
2. **サービスアカウント**ページで、**サービスアカウントを作成**を選択します。
3. **サービスアカウントの作成**ページで、必要な情報を入力し、**作成して続行**を選択します。
4. 「**このサービスアカウントにプロジェクトへのアクセスを許可する**」ページで、「**ロールを選択**」ドロップダウンメニューをクリックし、必要なロールを選択します。さらにロールを追加する場合は、「**+別のロールを追加**」をクリックします。

   各アカウント（個人またはサービス）には、プロジェクトの管理を定義するさまざまなロールがあります。このサービスアカウントには、以下のロールを付与してください。

   - Compute 管理者
   - Storage 管理者
   - Cloud Build 編集者
   - サービスアカウント ユーザー
   - クラウドデータストア ユーザー
   - Cloud KMS Crypto オペレーター

   Cloud KMS Crypto オペレーターには、以下の権限が必要です。

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list

> **注:**

> 新しいサービスアカウントを作成する際に利用可能なロールの完全なリストを取得するには、すべてのAPIを有効にしてください。

5. **CONTINUE**をクリックします
6. **Grant users access to this service account**ページで、ユーザーまたはグループを追加して、このサービスアカウントでアクションを実行するアクセス権を付与します。
7. **DONE**をクリックします。
8. IAMメインコンソールに移動します。
9. 作成されたサービスアカウントを特定します。
10. ロールが正常に割り当てられていることを検証します。

考慮事項:

サービスアカウントを作成する際は、以下を考慮してください。

- **このサービスアカウントにプロジェクトへのアクセスを許可**および**このサービスアカウントへのユーザーアクセスを許可**の手順はオプションです。これらのオプションの構成手順をスキップすることを選択した場合、新しく作成されたサービスアカウントは、**IAMと管理 > IAM**ページに表示されません。
- サービスアカウントに関連付けられたロールを表示するには、オプションの手順をスキップせずにロールを追加します。このプロセスにより、構成されたサービスアカウントにロールが表示されるようになります。

CITRIX CLOUDサービスアカウントキー

Citrix DaaSで接続を作成するには、Citrix Cloudサービスアカウントキーが必要です。キーは資格情報ファイル（.json）に含まれています。キーを作成すると、ファイルは自動的にダウンロードされ、**ダウンロード**フォルダーに保存されます。キーを作成するときは、キーの種類をJSONに設定してください。そうしないと、Web Studioはそれを解析できません。

サービスアカウントキーを作成するには、**IAMと管理 > サービスアカウント**に移動し、Citrix Cloudサービスアカウントのメールアドレスをクリックします。**キー**タブに切り替え、**キーを追加 > 新しいキーを作成**を選択します。キータイプとして**JSON**を選択していることを確認してください。

> **ヒント:**

Google Cloudコンソールの**サービスアカウント**ページを使用してキーを作成します。セキュリティ上の理由から、キーを定期的に変更することをお勧めします。既存のGoogle Cloud接続を編集することで、新しいキーをCitrix Virtual Apps and Desktopsアプリケーションに提供できます。

CITRIX CLOUD サービスアカウントにロールを追加する

Citrix Cloud サービスアカウントにロールを追加するには、次の手順を実行します。

1. Google Cloud コンソールで、**IAM と管理 > IAM** に移動します。
2. **IAM > 権限**ページで、作成したサービスアカウントを電子メールアドレスで特定し、見つけます。

   例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. 鉛筆アイコンを選択して、サービスアカウントのプリンシパルへのアクセスを編集します。
4. 選択したプリンシパルオプションについて、**「project-id」へのアクセスを編集**ページで、**別のロールを追加**を選択して必要なロールをサービスアカウントに1つずつ追加し、次に**保存**を選択します。

CLOUD COMPUTE SERVICE ACCOUNT にロールを追加する

Cloud Compute Service Account にロールを追加するには、次の手順を実行します。

1. Google Cloudコンソールで、**IAMと管理 > IAM**に移動します。
2. **IAM**ページで、Cloud Computeサービスアカウントを見つけます。これは、**プロジェクトID**と**compute**という単語で始まるメールアドレスで識別できます。

   例えば、`<project-id>-compute@developer.gserviceaccount.com`
3. 鉛筆アイコンを選択して、Cloud Buildアカウントのロールを編集します。
4. 選択したプリンシパルオプションについて、**「project-id」へのアクセスを編集**ページで、**別のロールを追加**を選択して必要なロールをCloud Buildサービスアカウントに1つずつ追加し、次に**保存**を選択します。

注:

すべてのAPIを有効にして、ロールの完全なリストを取得します。

ストレージの権限とバケット管理

Citrix Virtual Apps and Desktopsは、Google Cloudサービスのクラウドビルド障害の報告プロセスを改善します。このサービスは、Google Cloudでビルドを実行します。Citrix Virtual Apps and Desktopsは、Google Cloudサービスがビルドログ情報をキャプチャする`citrix-mcs-cloud-build-logs-{region}-{5 random characters}`という名前のストレージバケットを作成します。このバケットには、30日後にコンテンツを削除するオプションが設定されています。このプロセスでは、接続に使用されるサービスアカウントに`storage.buckets.update`に設定されたGoogle Cloud権限が必要です。サービスアカウントにこの権限がない場合、Citrix Virtual Apps and Desktopsはエラーを無視し、カタログ作成プロセスを続行します。この権限がないと、ビルドログのサイズが増加し、手動でのクリーンアップが必要になります。

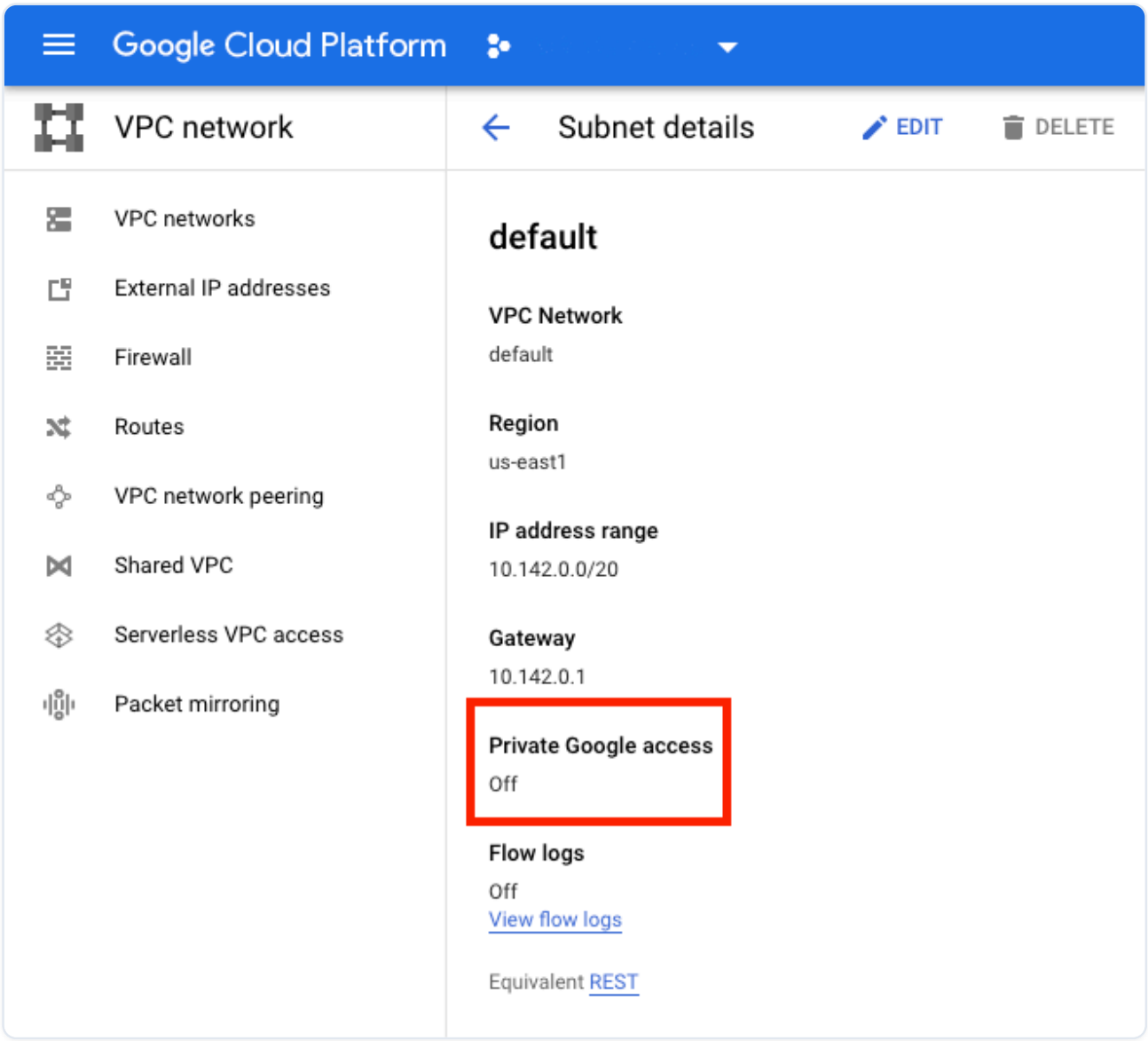
プライベート Google アクセスを有効にする

VMのネットワークインターフェースに外部IPアドレスが割り当てられていない場合、パケットは他の内部IPアドレスの宛先にのみ送信されます。プライベートアクセスを有効にすると、VMはGoogle APIおよび関連サービスで使用される外部IPアドレスのセットに接続します。

> **注記：**
>
> プライベートGoogleアクセスが有効になっているかどうかにかかわらず、パブリックIPアドレスを持つVMと持たないVMのすべてがGoogle Public APIにアクセスできる必要があります。これは、特にサードパーティのネットワークアプライアンスが環境にインストールされている場合に重要です。

MCSプロビジョニングのために、サブネット内のVMがパブリックIPアドレスなしでGoogle APIにアクセスできるようにするには、次の手順を実行します。

1. Google Cloudで、**VPC network configuration**にアクセスします。
2. サブネットの詳細画面で、「**Private Googleアクセス**」をオンにします。



詳細については、「プライベートGoogleアクセスを構成する」を参照してください。

重要:

ネットワークがVMのインターネットアクセスを防止するように構成されている場合、VMが接続されているサブネットに対してプライベートGoogleアクセスを有効にすることに関連するリスクを組織が負うことを確認してください。

次のステップ

- コアコンポーネントをインストールする
- VDAをインストールする
- サイトを作成する

- Google Cloud環境で接続を作成および管理する方法については、「Google Cloud環境への接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Microsoft Azure Resource Manager クラウド環境

Citrix Virtual Apps and Desktops™展開でMicrosoft Azure Resource Managerを使用して仮想マシンをプロビジョニングする場合、以下について理解しておいてください。

- マイクロソフト エントラ ID: `<https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-whatis/>`
- 同意フレームワーク: `<https://docs.microsoft.com/ja-jp/azure/active-directory/manage-apps/plan-an-application-integration>`
- サービスプリンシパル: `<https://docs.microsoft.com/ja-jp/azure/active-directory/develop/app-objects-and-service-principals/>`

Microsoft Azure Resource Managerをセットアップするには、「インストール準備」を参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- Azure環境での接続の作成と管理については、「Microsoft Azureへの接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成
- CTX219211: Microsoft Microsoft Entraアカウントのセットアップ
- CTX219243: XenAppおよびXenDesktopにAzureサブスクリプションへのアクセスを許可する
- CTX219271: サイト間VPNを使用してハイブリッドクラウドを展開する

マイクロソフト システムセンター コンフィギュレーションマネージャー環境

アプリケーションとデスクトップへのアクセスを管理するためにMicrosoft System Center Configuration Manager (Configuration Manager) を使用しているサイトは、以下のオプションを使用してCitrix Virtual Apps and Desktops™ にその使用を拡張できます。

- SCCM を使用した VDA のインストール。
- **Configuration Manager Wake Proxy 機能:** Remote PC Access の Wake on LAN 機能は Configuration Manager でサポートされています。詳細については、Wake on LAN - SCCM 統合を参照してください。
- **Citrix Virtual Apps and Desktops のプロパティ:** プロパティを使用すると、Configuration Manager を介して管理するCitrix Virtual Desktops™ を識別できます。(一部のバージョンでは、Configuration Manager は Citrix Virtual Apps and Desktops の旧称である XenApp および XenDesktop を使用しています。)

プロパティ

仮想デスクトップを管理するために、Microsoft System Center Configuration Manager でプロパティを利用できます。

Configuration Manager に表示されるブール型プロパティは、true または false ではなく、`1` または `0` として表示されます。

これらのプロパティは、`Root\Citrix\DesktopInformation` 名前空間の `Citrix_virtualDesktopInfo` クラスで利用できます。プロパティ名は Windows Management Instrumentation (WMI) プロバイダーから取得されます。

プロパティ	説明
`AssignmentType`	IsAssigned の値を設定します。有効な値は、`ClientIP`、`ClientName`、`None`、および `User` です (`IsAssigned` を `True` に設定します)。
`BrokerSiteName`	`HostIdentifier` と同じ値を返します。
`DesktopCatalogName`	デスクトップに関連付けられているマシンカタログ。

プロパティ	説明
`DesktopGroupName`	デスクトップに関連付けられているデリバリーグループ。
`HostIdentifier`	`BrokerSiteName`と同じ値を返します。
`IsAssigned`	デスクトップをユーザーに割り当てるための`True`。ランダムなデスクトップの場合は`False`に設定します。
`IsMasterImage`	環境に関する決定を可能にします。たとえば、プロビジョニングされたマシンではなく、イメージにアプリケーションをインストールします。有効な値は次のとおりです。イメージとして使用されるVM上の`True`。この値は、選択に基づいてインストール中に設定されるか、そのイメージからプロビジョニングされたVM上でクリアされます。
`IsVirtualMachine`	仮想マシンの場合は`True`、物理マシンの場合は`false`。
`OSChangesPersist`	デスクトップオペレーティングシステムイメージが再起動のたびにクリーンな状態にリセットされる場合は`False`。それ以外の場合は`true`。
`PersistentDataLocation`	Configuration Managerが永続データを保存する場所です。これはユーザーがアクセスできません。
`BrokerSiteName`, `DesktopCatalogName`, `DesktopGroupName`, `HostIdentifier`	デスクトップがControllerに登録されるときに決定されます。完全に登録されていないデスクトップの場合、それらはnullです。

プロパティを収集するには、Configuration Manager でハードウェアインベントリを実行します。プロパティを表示するには、Configuration Manager Resource Explorer を使用します。これらの場合、名前にはスペースが含まれるか、プロパティ名とわずかに異なります。たとえば、`BrokerSiteName` は `Broker Site Name` として表示されます。

- Citrix VDAからCitrix WMIプロパティを収集するようにConfiguration Managerを構成する

- Citrix WMIプロパティを使用してクエリベースのデバイスコレクションを作成する
- Citrix WMIプロパティに基づいてグローバル条件を作成する
- グローバル条件を使用してアプリケーション展開タイプの要件を定義する

`Root\ccm_vdi` 名前空間の Microsoft クラス `CCM_DesktopMachine` で Microsoft プロパティを使用することもできます。詳細については、Microsoft のドキュメントを参照してください。

マイクロソフト システムセンター バーチャル マシン マネージャー 仮想化環境

仮想マシンを提供する目的で、Hyper-VとMicrosoft System Center Virtual Machine Manager (VMM) を使用する場合は、このガイダンスに従ってください。

このリリースでは、システム要件に記載されているVMMバージョンがサポートされています。

> **注:**
>
> 混在するHyper-Vクラスター（異なるHyper-Vバージョンを実行しているサーバーを含む）はサポートされていません。

> Citrix Provisioning（旧Provisioning Services）およびMachine Creation Services™を使用して、以下をプロビジョニングできます。

- 第1世代でサポートされているデスクトップまたはサーバーOSのVM。
- セキュアブートのサポートを含む、第2世代でサポートされているデスクトップまたはサーバーOSのVM。

ハイパーバイザーのインストールと構成

> **重要:**
>
> すべてのDelivery Controllerは、VMMサーバーと同じフォレスト内にある必要があります。

1. サーバーにMicrosoft Hyper-VサーバーとVMMをインストールします。
2. すべてのControllerにSystem Center Virtual Machine Managerコンソールをインストールします。コンソールのバージョンは管理サーバーのバージョンと一致している必要があります。以

前のコンソールでも管理サーバーに接続できますが、バージョンが異なる場合、VDAのプロビジョニングは失敗します。

3. 次のアカウント情報を確認してください。

   Studioでホストを指定するために使用するアカウントは、関連するHyper-VマシンにVMM管理者またはVMM委任管理者である必要があります。このアカウントがVMMで委任管理者ロールのみを持っている場合、ホスト作成プロセス中にStudioにストレージデータが表示されません。

   Studio統合に使用されるユーザーアカウントは、各Hyper-Vサーバーのadministratorsローカルセキュリティグループのメンバーである必要もあります。この構成は、VMの作成、更新、削除などのVMライフサイクル管理をサポートします。

   Hyper-Vを実行しているサーバーにControllerをインストールすることはサポートされていません。

単一のSCVMMが異なるデータセンター内の複数のクラスターを管理する大規模な展開では、委任管理者のホストグループのスコープを制限できます。

ホストグループのスコープを制限するには、Microsoft System Center Virtual Machine Manager (VMM) コンソールで委任管理者ロールを使用します。

1. **ユーザーロールの作成ウィザード**で、ユーザーロールとして「ファブリック管理者（委任された管理者）」を選択します。
2. **メンバー**で、委任された管理者として使用するActive Directoryのユーザーアカウントを追加します。
3. **スコープ**で、委任された管理者にアクセスを許可するホストグループを選択します。
4. 委任された管理者ユーザーの資格情報を使用して、新しい**実行アカウント**を作成します。これらの資格情報を使用して、後でハイパーバイザー接続を作成します。メインの管理者ロールアカウントは使用しないでください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- SCVMM での接続の作成と管理については、Microsoft System Center Virtual Machine Manager への接続を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Nutanix 仮想化環境

Citrix Virtual Apps and Desktops を Nutanix AHV クラスターに接続するには、Nutanix AHV Prism Central ホスト接続を使用して Nutanix Prism Central 経由で接続します。このホスト接続は次のとおりです。

- 電源管理されたVDAとMCSプロビジョニングされたVDAの両方を含むマシンカタログをサポートします。
- テンプレートバージョンを使用して、AHVクラスター間でMCSマスターイメージの共有を可能にします。
- ホスト接続での証明書信頼を簡素化します。
- Cloud Connector への Nutanix プラグインのインストールが不要になります。

「Nutanix Prism Central on AHV」を参照してください。

Nutanix Acropolis をホスト接続として使用して、Citrix Virtual Apps and Desktops 展開でVMを提供する Nutanix Prism Element on AHV を使用することもできます。ただし、このセットアッププロセスでは、Citrix Virtual Apps and Desktops 環境に Nutanix プラグインをインストールして登録する必要があります。「Nutanix Prism Element on AHV」を参照してください。

Nutanix Acropolis MCS プラグインのインストールガイドの詳細については、「Nutanix Support Portal」を参照してください。

AHV 上の ニュータニックス プリズムセントラル

Citrix は、Citrix Virtual Apps and Desktops を Nutanix Prism Central on AHV と統合するプラグインを開発し、保守しています。このプラグインは Citrix Delivery Controller と統合されており、個別のプラグインをインストールする必要がありません。

Nutanix AHV Prism Central プラグインは、Citrix が管理する Delivery Controller にプレインストールされているため、Delivery Controller に個別にインストールする必要がありません。Citrix が管理するコンポーネントとサービスについては、「Technical overview」を参照してください。

前提条件

Nutanix AHV Prism Centralには、以下が必要です。

- Prism Central バージョン pc.2024.3 以降。サポートされているPrism Centralのバージョンの詳細については、「Supported Hypervisors for Citrix Virtual Apps and Desktops (MCS) and Citrix Provisioning (PVS)」を参照してください。
- Nutanix AHV クラスターには AOS バージョン 7.0 以降が必要です。
- Nutanix AHV クラスターは Prism Central に登録されている必要があります。
- Citrix 管理者アカウントには、ホスト接続、マシンカタログ、デリバリーグループを作成するための十分な権限が必要です。詳細については、「委任管理の構成」を参照してください。
- Citrix Cloud™ は Cloud Connector を介して Nutanix Prism Central と通信します。したがって、Nutanix Prism Central インスタンスは Cloud Connector からアクセスできる必要があります。

機能の制限事項

Nutanix Prism および API の制限により、Windows VM でゲストの再起動やゲストのシャットダウンなどの電源操作が失敗する場合があります。この問題を解決するには、VDA に設定を適用するために、ドキュメント「Prism または API から開始された電源操作が Windows VM で失敗する可能性がある」に記載されている Nutanix の指示に従うことをお勧めします。

主要な手順

1. Nutanix 仮想化環境をセットアップします。詳細については、「インストール準備」または「未使用のドメインをアクティブ化する」を参照してください。
2. Nutanix AHV Prism Central への接続を作成する
3. Nutanix マシンテンプレートバージョンを使用してマシンカタログを作成する。

AHV 上の ニュータニックス プリズムエレメント

AHV 上の Nutanix Prism Element では、Citrix Virtual Apps and Desktops が Nutanix ハイパーバイザーを持つリソースの場所にホスト接続を作成する必要があるすべての Delivery Controller に Nutanix プラグインをインストールする必要があります。

主要な手順

1. Nutanix プラグインをインストールして登録します。
2. Nutanix 仮想化環境をセットアップします。詳細については、「リソースの種類を追加する」または「未使用のドメインをアクティブ化する」を参照してください。
3. 接続を作成します。
4. マシンカタログを作成します。

Nutanixプラグインのインストールと登録

すべてのCloud ConnectorにNutanixプラグインをインストールして登録する手順を完了します。Nutanixプラグインのインストールについては、Nutanixドキュメントサイトを参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- Nutanix 環境での接続の作成と管理については、Nutanix への接続 を参照してください。

詳細情報

- 接続とリソースの作成と管理
- マシンカタログの作成

Nutanix クラウドおよびパートナーソリューション

Nutanix AHV プリズムセントラル

Citrix Virtual Apps and Desktops は、Citrix が管理する Nutanix AHV Prism Central プラグイン向けに、以下のクラウドハイパーバイザーで Nutanix Cloud Clusters (NC2) をサポートします。

- アマゾン ウェブ サービス (AWS)
- マイクロソフト アジュール

Nutanix クラウド クラスター

Citrix Virtual Apps and Desktops は、AWS および Azure 上の Nutanix Cloud Clusters をサポートします。Nutanix クラスターは、プライベートクラウドまたは複数のパブリッククラウドでアプリケーションを実行する方法を簡素化します。

NC2のセットアップの詳細については、以下を参照してください。

- AWS上でのNutanix Cloud Clustersの展開およびユーザーガイド
- Azure上でのNutanix Cloud Clustersの展開およびユーザーガイド。

要件

NC2 を使用するには、以下のいずれかのアカウントが必要です。

- Nutanixアカウント

- AWSの場合：次の権限を持つAWSアカウント。
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess
- Azureの場合:
  - 有効な「NC2 on Azure」ライセンス
  - 次のいずれかのロールを含むAzureアカウント：
    - グローバル管理者
    - クラウドアプリケーション管理者
    - アプリケーション管理者
    - すべての権限

NC2 on Azureの権限

```
Microsoft.Compute/register/action

Microsoft.Compute/availabilitySets/write

Microsoft.Compute/availabilitySets/delete

Microsoft.Compute/disks/read

Microsoft.Compute/disks/write

Microsoft.Compute/disks/delete

Microsoft.Compute/locations/usages/read

Microsoft.Compute/availabilitySets/read

Microsoft.Compute/virtualMachines/*

Microsoft.Compute/snapshots/*

Microsoft.Compute/images/*

Microsoft.Network/register/action
```

```
Microsoft.Network/natGateways/*

Microsoft.Network/networkInterfaces/*

Microsoft.Network/networkSecurityGroups/*

Microsoft.Network/publicIPAddresses/*

Microsoft.Network/virtualNetworks/*

Microsoft.Network/locations/usages/read

Microsoft.Storage/register/action

Microsoft.Storage/checknameavailability/read Microsoft.Storage/locations/
checknameavailability/read Microsoft.Storage/locations/usages/read

Microsoft.Storage/storageAccounts/write

Microsoft.Storage/storageAccounts/read

Microsoft.Storage/storageAccounts/delete Microsoft.Storage/
storageAccounts/blobServices/containers/clearLegalHold/action
Microsoft.Storage/storageAccounts/blobServices/containers/delete
Microsoft.Storage/storageAccounts/blobServices/containers/lease/action

Microsoft.Storage/storageAccounts/blobServices/containers/ read
Microsoft.Storage/storageAccounts/blobServices/containers/ write
Microsoft.Storage/storageAccounts/blobServices/read Microsoft.Storage/
storageAccounts/blobServices/write Microsoft.Storage/storageAccounts/
listAccountSas/action Microsoft.Storage/storageAccounts/listkeys/action
Microsoft.Storage/storageAccounts/listServiceSas/action Microsoft.Storage/
storageAccounts/regeneratekey/action Microsoft.Storage/storageAccounts/
revokeUserDelegationKeys/action Microsoft.ResourceHealth/
AvailabilityStatuses/read Microsoft.ResourceHealth/events/read

Microsoft.ResourceHealth/AvailabilityStatuses/current/read

Microsoft.ManagedIdentity/userAssignedIdentities/* Microsoft.Resources/
subscriptions/locations/read Microsoft.Resources/subscriptions/
resourceGroups/read Microsoft.Resources/subscriptions/resourceGroups/write
Microsoft.Resources/subscriptions/resourceGroups/delete
Microsoft.Resources/subscriptions/resourcegroups/deployments/read
```

```
Microsoft.Resources/subscriptions/resourcegroups/deployments/write
Microsoft.Resources/subscriptions/resourcegroups/resources/read
Microsoft.Resources/subscriptions/tagNames/read Microsoft.Resources/
subscriptions/tagNames/write Microsoft.Resources/subscriptions/tagNames/
delete Microsoft.Resources/subscriptions/tagNames/tagValues/write
Microsoft.Resources/subscriptions/tagNames/tagValues/read
Microsoft.Resources/subscriptions/tagNames/tagValues/delete
Microsoft.Resources/tags/read

Microsoft.Resources/tags/write

Microsoft.Resources/tags/delete

Microsoft.Resources/providers/read

Microsoft.Compute/sshPublicKeys/read

Microsoft.Compute/sshPublicKeys/write

Microsoft.Compute/sshPublicKeys/delete Microsoft.Compute/sshPublicKeys/
generateKeyPair/action Microsoft.Nutanix/Interfaces/read

Microsoft.Nutanix/Interfaces/write

Microsoft.Nutanix/Interfaces/delete

Microsoft.Nutanix/Nodes/read

Microsoft.Nutanix/Nodes/write

Microsoft.Nutanix/Nodes/delete

Microsoft.Nutanix/register/action

Microsoft.Network/virtualHubs/*

Microsoft.Network/routeTables/read

Microsoft.Network/routeTables/write

Microsoft.Network/routeTables/delete

Microsoft.Network/routeTables/join/action
```

```
Microsoft.Network/routeTables/routes/read Microsoft.Network/routeTables/
routes/write Microsoft.Network/routeTables/routes/delete
Microsoft.CostManagement/query/read

Microsoft.CostManagement/views/read Microsoft.CostManagement/
externalSubscriptions/query/read Microsoft.CostManagement/
externalSubscriptions/dimensions/read Microsoft.CostManagement/
externalSubscriptions/read Microsoft.CostManagement/
externalBillingAccounts/forecast/read

Microsoft.CostManagement/externalBillingAccounts/read

Microsoft.CostManagement/externalBillingAccounts/query/read
Microsoft.CostManagement/externalBillingAccounts/ externalSubscriptions/
read Microsoft.CostManagement/externalSubscriptions/forecast/read
Microsoft.CostManagement/operations/read Microsoft.CostManagement/
forecast/read

Microsoft.Network/virtualWans/write

Microsoft.Network/virtualWans/read

Microsoft.Network/virtualWans/delete Microsoft.Network/virtualWans/
virtualHubs/read Microsoft.Network/virtualWans/join/action
Microsoft.Network/virtualHubs/hubVirtualNetworkConnections/ read
Microsoft.Network/virtualHubs/hubVirtualNetworkConnections/ write
Microsoft.Network/virtualHubs/hubVirtualNetworkConnections/ delete
Microsoft.Network/privateEndpoints/pushPropertiesToResource/ action
Microsoft.Network/privateEndpoints/read

Microsoft.Network/privateEndpoints/write Microsoft.Network/
privateEndpoints/delete Microsoft.Network/privateDnsZones/read
Microsoft.Network/privateDnsZones/delete Microsoft.Network/
privateDnsZones/join/action Microsoft.Network/privateDnsZones/write
Microsoft.Network/privateEndpoints/privateDnsZoneGroups/ write

Microsoft.Network/privateEndpoints/privateDnsZoneGroups/read
Microsoft.Network/privateEndpoints/privateDnsZoneGroups/delete

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/add/action
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/
```

```
deleteBlobVersion/action

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/filter/
action Microsoft.Storage/storageAccounts/blobServices/containers/ blobs/
read Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/
read

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/write
Microsoft.Storage/storageAccounts/blobServices/containers/ blobs/write
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/filter/
action Microsoft.Storage/storageAccounts/blobServices/containers/blobs/
modifyPermissions/action
```

Nutanixクラスターの作成

1. Nutanixアカウントにログインします。
2. Nutanixクラスターオプションに移動し、**Launch**をクリックします。**Nutanix Console**が開きます。詳細については、以下を参照してください:
   - AWSでのNutanixクラスターの開始
   - マイクロソフト アジュール上のニュータニックス クラウド クラスター
3. 新しいVPCを作成するオプションを選択します。

クラスターが作成されたら、Nutanix Prism のアドレスを取得します。

トラブルシューティング

クラスター作成プロセスは、以下のエラーで失敗する可能性があります。

- **指定された時間内にクラスターを作成できませんでした。クラスターを削除しています**
- **ホスト Nutanix クラスター - ノード XXXXXXXXXXX: インスタンス i-xxxxxxxxxxxxx: ネットワークインターフェースのソース/宛先チェックを無効にするエラー.**
- **ホスト Nutanix クラスター - ノード XXXXXXXXXXX: インスタンス i-xxxxxxxxxxxxxx のネットワークインターフェース情報を取得できません**

クラスターの作成に失敗した場合は、別のリージョンで再作成してみてください。再試行する前に、Nutanix CloudFormation Stack (CFS) を必ず削除してください。

注:

他のリソースに加えて、Nutanix CFS は以下を作成します。

- Nutanix Cluster xxxxxxxxxxxx 10.0.0.0/16 という名前の VPC を 1 つ
- 2 つのサブネット 10.0.128.0/24 と 10.0.129.0/24
- 1つのインターネットゲートウェイ
- 1つのNATゲートウェイ

Prismサーバーアドレスの取得

1. NC2 クラスターを Prism Central サーバーに登録します。詳細については、「Registering a Cluster with Prism Central」を参照してください。
2. Prism Central サーバーのホスト名または IP アドレスをアドレスとして使用します。

ニュータニックス プリズム エレメント 用 NC2

Citrix Virtual Apps and Desktops は、Nutanix Prism Element プラグイン向けに、以下のクラウドハイパーバイザーで Nutanix Cloud Clusters (NC2) をサポートしています。

- アマゾン ウェブ サービス (AWS)

AWS上のニュータニックス クラウド クラスターズ

AWS 上の Nutanix Cloud Clusters の詳細については、「Nutanix Cloud Clusters on AWS Deployment and User Guide」を参照してください。

ヒント:

このサポートは、Nutanix のオンプレミス クラスターと同じ機能を提供します。サポートされるクラスターは、*Prism Element* の単一クラスターのみです。詳細については、こちらを参照してください。

AWS で NC2 を使用するには、次のアカウントが必要です。

- Nutanix アカウント
- 次の権限を持つ AWS アカウント:
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

Nutanixクラスターの作成、およびクラスター作成が失敗した場合のトラブルシューティングについては、Create a Nutanix ClusterおよびTroubleshootingを参照してください。

クラスターが作成されたら、**Nutanix Prism**のアドレスを取得します。

Prismサーバーアドレスの取得

1. **Nutanix Console**に移動します。
2. コンソールの右上隅で、**Launch Prism Element**リンクにマウスカーソルを合わせ、URLをコピーします。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- Nutanixクラウドおよびパートナーソリューションの接続の作成と管理については、Connection to Nutanix cloud and partner solutionsを参照してください。

詳細情報

- 接続とリソースの作成と管理
- マシンカタログの作成

Red Hat OpenShift 仮想化環境

Citrix® は、Citrix が管理する OpenShift プラグインを介して、Red Hat OpenShift ワークロードを管理します。このプラグインを使用すると、OpenShift クラスターへのホスティング接続とホスティングユニットの作成、カタログの作成、およびカタログ内のマシンの電源管理を行うことができます。

以下の構成がサポートされています。

- ネットワークオプション:
  - Linux Bridge および OVS Bridge: クラスターネットワークで利用可能です。
- ストレージオプション:
  - ローカルストレージ: ノード上の永続ストレージでサポートされています。
  - NetApp ストレージ: エンタープライズグレードの外部ストレージ統合でサポートされています。

主要な手順

- Red Hat OpenShift 環境をセットアップします。
- OpenShift クラスターへの接続とリソースを作成します。
- マシンカタログを作成します。
- デリバリーグループを作成します。

Red Hat OpenShift 環境をセットアップする

1. *OpenShift クラスターを作成し、クラスター API アドレスを取得します*: OpenShift コンソールで、クラスターをセットアップした後、**Home > Overview > Details** に移動し、クラスター API アドレスを取得します。
2. *サービスアカウントを作成し、OpenShiftコマンドラインインターフェース (CLI) (ocコマンド) を使用してサービスアカウントトークンを取得する*: サービスアカウントトークンは、サービスアカウントに関連付けられた認証資格情報です。サービスアカウントは、OpenShiftプラグインをOpenShiftで認証するために使用されます。各サービスアカウントは、1つの名前空間に関連付けられています。
3. *サービスアカウントの権限を構成する*: サービスアカウントは複数のロールを持つことができ、各ロールはOpenShiftプラグインがどのリソースに対してどのようなアクションを実行できるかを定義する権限で構成されます。ロールは**ロールバインディング**を介してバインドされ、**ロールバインディング**には次の2種類があります。

    a. **クラスターワイドロールバインディング**: OpenShiftからイベントを受信するために使用されます。 名前空間バインドロールバインディング: 特定の名前空間でVMを管理するために使用されます。

    b. **名前空間バインドロールバインディング**: 特定の名前空間でVMを管理するために使用されます。

4. *名前空間 (プロジェクト) を作成する*: OpenShiftの名前空間は、VMやネットワークなどのリソースをグループ化する分離された環境であり、より良い組織化とアクセス制御を可能にします。**名前空間**はKubernetesの用語であり、**プロジェクト**はOpenShiftの用語です。OpenShiftプラグインの観点からは、これらは同じです。VMを展開するには名前空間が必要です。OpenShiftコンソールまたはOpenShift Container Platform CLIを使用して名前空間を作成します。
5. *ターゲット名前空間の下にネットワークアタッチメント定義を1つ作成する*: ネットワークアタッチメント定義は、OpenShiftで実行されているVMのネットワーク構成を指定します。**Networking > NetworkAttachmentDefinitions**の下で、各名前空間のネットワークアタッチメント定義を確認できます。

6. *ストレージクラスを構成する*: ストレージクラスは、VMストレージがどのように割り当てられるかを定義します。**Storage > StorageClass**の下で、ストレージプロバイダーのリストを構成および確認できます。

サービスアカウントを作成する

1. ocコマンドラインツールをダウンロードして解凍します。
2. ログインIDを使用してOpenShiftコンソールにアクセスします。
3. ユーザープロファイルをクリックし、**Copy login command**をクリックします。
4. **Display Token**をクリックし、トークンをコピーします。
5. ocコマンドラインを使用してログインコマンドを実行します。例:

```
.\oc.exe login --token=<token> --server=<server address>
```

6. サービスアカウントを作成します。
   - デフォルトの名前空間の下にサービスアカウントを作成する場合は、次を実行します。

     ```
     .\oc.exe create sa <service account name>
     ```

   - 独自のネームスペースでサービスアカウントを作成する場合は、次を実行します。

     ```
     .\oc.exe create sa <service account name> -n mynamespace
     ```

7. シークレット用の `YAML` ファイルを作成します。例:
   - デフォルトのネームスペースでサービスアカウントを作成する場合:

     ```
     apiVersion: v1

     kind: Secret

     metadata:

     name: service account name

     annotations:

     kubernetes.io/service-account.name: service account name
     ```

```
type: kubernetes.io/service-account-token
```

- 独自のネームスペースでサービスアカウントを作成する場合:

```
apiVersion: v1

kind: Secret

metadata:

name: service account name

namespace: mynamespace

annotations:

kubernetes.io/service-account.name: service account name

 type: kubernetes.io/service-account-token
```

8. YAMLを適用します。

```
.\oc.exe apply -f <yamlFile.yaml>
```

注:

`oc` はトークンを取得するためのシークレットを記述します。トークンはパスワードとして使用されます。

サービスアカウントのロールとロールバインディングを作成する

クラスター全体のロールバインディングにより、サービスアカウントはクラスター全体のすべてのVMイベントを読み取る権限を持ち、OpenShiftプラグインがすべてのVM関連イベントに対して単一のイベントウォッチャーを維持できるようになります。 ネームスペースのロールバインディングにより、サービスアカウントはターゲットネームスペース内のVMを管理する権限を持ちます。 スクリプトを使用してロールを作成し、サービスアカウントにバインドできます。`<https://github.com/citrix/citrix-mcs-sdk-samples/tree/main/OpenShift/Hosting%20Connection/Role/>` を参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- 接続の作成と管理については、Red Hat OpenShiftへの接続 を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

VMware 仮想化環境

仮想マシンを提供するのにVMwareを使用する場合は、このガイダンスに従ってください。

vCenter Serverと適切な管理ツールをインストールします。(vSphere vCenter Linked Mode操作はサポートされていません。)

MCSを使用する予定がある場合は、vCenter ServerのDatastore Browser機能（`<https://kb.vmware.com/s/article/2101567>`に記載）を無効にしないでください。この機能を無効にすると、MCSは正しく動作しません。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- VMware環境での接続の作成と管理については、「Connection to VMware」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

VMware クラウドおよびパートナーソリューション

Citrix Virtual Apps and Desktops™ は、以下の VMware クラウドおよびパートナーソリューションをサポートしています。

- Azure VMware ソリューション (AVS)
- Google Cloud VMware エンジン
- Amazon Web Services (AWS) 上の VMware クラウド

Azure VMware ソリューション (AVS) 統合

Citrix Virtual Apps and Desktop サービスは AVS をサポートしています。AVS は、Azure インフラストラクチャによって作成された vSphere クラスターを含むクラウドインフラストラクチャを提供します。Citrix Virtual Apps and Desktop サービスを活用して、オンプレミス環境で vSphere を使用するのと同じ方法で、AVS を使用して VDA ワークロードをプロビジョニングできます。

AVS クラスターのセットアップ

Citrix Virtual Apps™ and Desktop サービスで AVS を使用できるようにするには、Azure で次の手順を実行します。

- ホストクォータを要求する
- Microsoft.AVS リソースプロバイダーを登録する
- ネットワークチェックリスト
- Azure VMware Solution プライベートクラウドを作成する
- Azure VMware Solution プライベートクラウドにアクセスする
- Azure で VMware プライベートクラウドのネットワークを構成する
- Azure VMware Solution の DHCP を構成する
- Azure VMware Solution にネットワークセグメントを追加する
- Azure VMware Solution 環境を確認する

AZURE ENTERPRISE AGREEMENTのお客様のホストクォータを要求する

Azure portal の ページで を選択し、次の情報を含めます。

- 問題の種類: 技術
- サブスクリプション: サブスクリプションを選択してください
- サービス: すべてのサービス > Azure VMware Solution
- リソース: 一般的な質問
- 概要: 容量が必要
- 問題の種類: 容量管理の問題
- 問題のサブタイプ: 追加のホストクォータ/容量に関する顧客からの要求

サポートチケットの に、 タブで次の情報を含めます。

- POC または本番環境
- リージョン名
- ホスト数
- その他の詳細

> **注：**
>
> AVSには最低3つのホストが必要であり、N+1ホストの冗長性を使用することをお勧めします。

> サポートチケットの詳細を指定したら、 を選択してAzureにリクエストを送信します。

MICROSOFT.AVSリソースプロバイダーを登録する

ホスト クォータを要求した後、リソース プロバイダーを登録します。

1. Azureポータルにサインインします。
2. Azureポータルメニューで、 を選択します。
3. メニューで、サブスクリプションを入力し、 を選択します。
4. サブスクリプションリストからサブスクリプションを選択します。
5. を選択し、検索バーに「**Microsoft.AVS**」と入力します。
6. リソースプロバイダーが登録されていない場合は、 を選択します。

ネットワークに関する考慮事項

AVSは、特定のネットワークアドレス範囲とファイアウォールポートを必要とするネットワークサービスを提供します。詳細については、「Azure VMware Solution のネットワーク計画チェックリスト」を参照してください。

AZURE VMWARE SOLUTION プライベートクラウドを作成する

環境のネットワーク要件を考慮した後、ASV プライベートクラウドを作成します。

1. Azureポータルにサインインします。
2. **新しいリソースの作成**を選択します。
3. **Marketplace の検索**テキストボックスに、*Azure VMware Solution*と入力し、リストから**Azure VMware Solution**を選択します。

Azure ASV プライベートクラウドのセットアップ(/en-us/citrix-virtual-apps-desktops/2511/media/azure-asv-create-solution.png) 画像

Azure VMware Solutionウィンドウで、:

1. **作成**を選択します。
2. タブをクリックします。
3. 以下の表の情報を使用して、フィールドに値を入力します。

フィールド	値
サブスクリプション	デプロイに使用するサブスクリプションを選択します。Azure サブスクリプション内のすべてのリソースはまとめて請求されます。
リソースグループ	プライベートクラウドのリソースグループを選択します。Azure リソースグループは、Azure リソースがデプロイおよび管理される論理コンテナです。または、プライベートクラウド用に新しいリソースグループを作成することもできます。
場所	east us などの場所を選択します。これは、計画フェーズで定義したリージョンです。
リソース名	Azure VMware Solution プライベートクラウドの名前を指定します。
SKU	AV36 を選択します。
ホスト	プライベートクラウドクラスターに割り当てられたホストの数を表示します。デフォルト値は 3 で、デプロイ後に増減できます。
アドレスブロック	プライベートクラウドの IP アドレスブロックを指定します。CIDR はプライベートクラウド管理ネットワークを表し、vCenter Server や NSX-T Manager などのクラスター管理サービスに使用されます。たとえば、10.175.0.0/22 のように /22 アドレス空間を使用します。アドレスは一意であり、他の Azure 仮想ネット

フィールド	値
	ワークやオンプレミスネットワークと重複しないようにする必要があります。
仮想ネットワーク	Azure VMware Solution ExpressRoute 回線はデプロイ後の手順として確立されるため、このフィールドは空白のままにします。

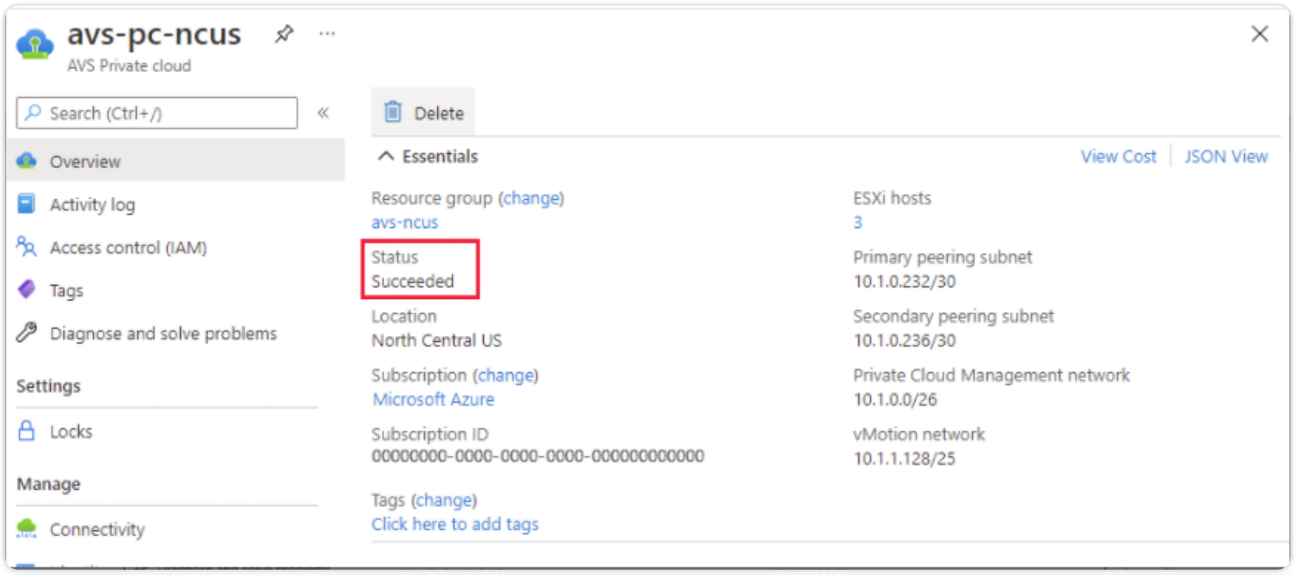
「**プライベートクラウドの作成**」画面で、次のようにします。

1. 「**場所**」フィールドで、AVS が存在するリージョンを選択します。リソースグループのリージョンは AVS リージョンと同じです。
2. 「**SKU**」フィールドで、「**AV36 Node**」を選択します。
3. 「**Address Block**」フィールドにIPアドレスを指定します。例: 10.15.0.0/22。
4. 「**Review + Create**」を選択します。
5. 情報を確認したら、「**Create**」をクリックします。

Azure ASV プライベートクラウドの作成(/en-us/citrix-virtual-apps-desktops/2511/media/azure-avs-create-private-cloud.png)

> **ヒント:**
>
> プライベートクラウドの作成には3〜4時間かかる場合があります。クラスターに単一のホストを追加するには30〜45分かかる場合があります。

> デプロイが成功したことを確認します。作成したリソースグループに移動し、プライベートクラウドを選択します。「**Status**」が「**Succeeded**」になったら、デプロイは完了です。



AZURE VMWARE SOLUTION プライベートクラウドへのアクセス

プライベートクラウドを作成したら、Windows VMを作成し、プライベートクラウドのローカルvCenterに接続します。
新しいWindows仮想マシンの作成

1. リソースグループで「**+ Add**」を選択し、「**Microsoft Windows 10/2016/2019**」を検索して選択します。
2. 「**Create**」をクリックします。
3. 必要な情報を入力し、「**Review + Create**」を選択します。
4. 検証が完了したら、「**作成**」を選択して仮想マシンの作成プロセスを開始します。

プライベートクラウドのローカルvCenterに接続する

1. クラウド管理者として**vSphere Client with VMware vCenter SSO**にサインインします。

   Azure ASV vSphere ログイン(/en-us/citrix-virtual-apps-desktops/2511/media/azure-avs-vsphere-login.png)
2. Azureポータルでプライベートクラウドを選択し、次に「**管理 > ID**」を選択します。

プライベートクラウドのvCenterとNSX-T ManagerのURLとユーザー資格情報が表示されます。

Azure ASV セットアップ vCenter(/en-us/citrix-virtual-apps-desktops/2511/media/azure-avs-setup-vcenter.png)

URLとユーザー資格情報を確認した後：

1. 前の手順で作成したVMに移動し、仮想マシンに接続します。

2. Windows VMでブラウザを開き、2つのブラウザタブでvCenterとNSX-T ManagerのURLに移動します。vCenterタブで、前のステップの*cloudadmin@vmcp.local*ユーザー資格情報を入力します。

AZUREでVMWAREプライベートクラウドのネットワークを構成する

ASVプライベートクラウドにアクセスした後、仮想ネットワークとゲートウェイを作成してネットワークを構成します。
仮想ネットワークを作成する

1. Azure portal にサインインします。
2. 以前に作成したリソースグループに移動します。
3. 「**+ 追加**」を選択して、新しいリソースを定義します。
4. 「**Marketplace を検索**」テキストボックスに「*virtual network*」と入力します。仮想ネットワークリソースを見つけて選択します。
5. 「**仮想ネットワーク**」ページで、「**作成**」を選択してプライベートクラウドの仮想ネットワークを設定します。
6. 「**仮想ネットワークの作成**」ページで、仮想ネットワークの詳細を入力します。
7. 「**基本**」タブで、仮想ネットワークの名前を入力し、適切なリージョンを選択して、「**次へ : IP アドレス**」をクリックします。
8. 「**IP アドレス**」タブの IPv4 アドレス空間の下に、以前に作成したアドレスを入力します。

> **重要:**

> プライベートクラウドを作成したときに使用したアドレス空間と重複しないアドレスを使用してください。

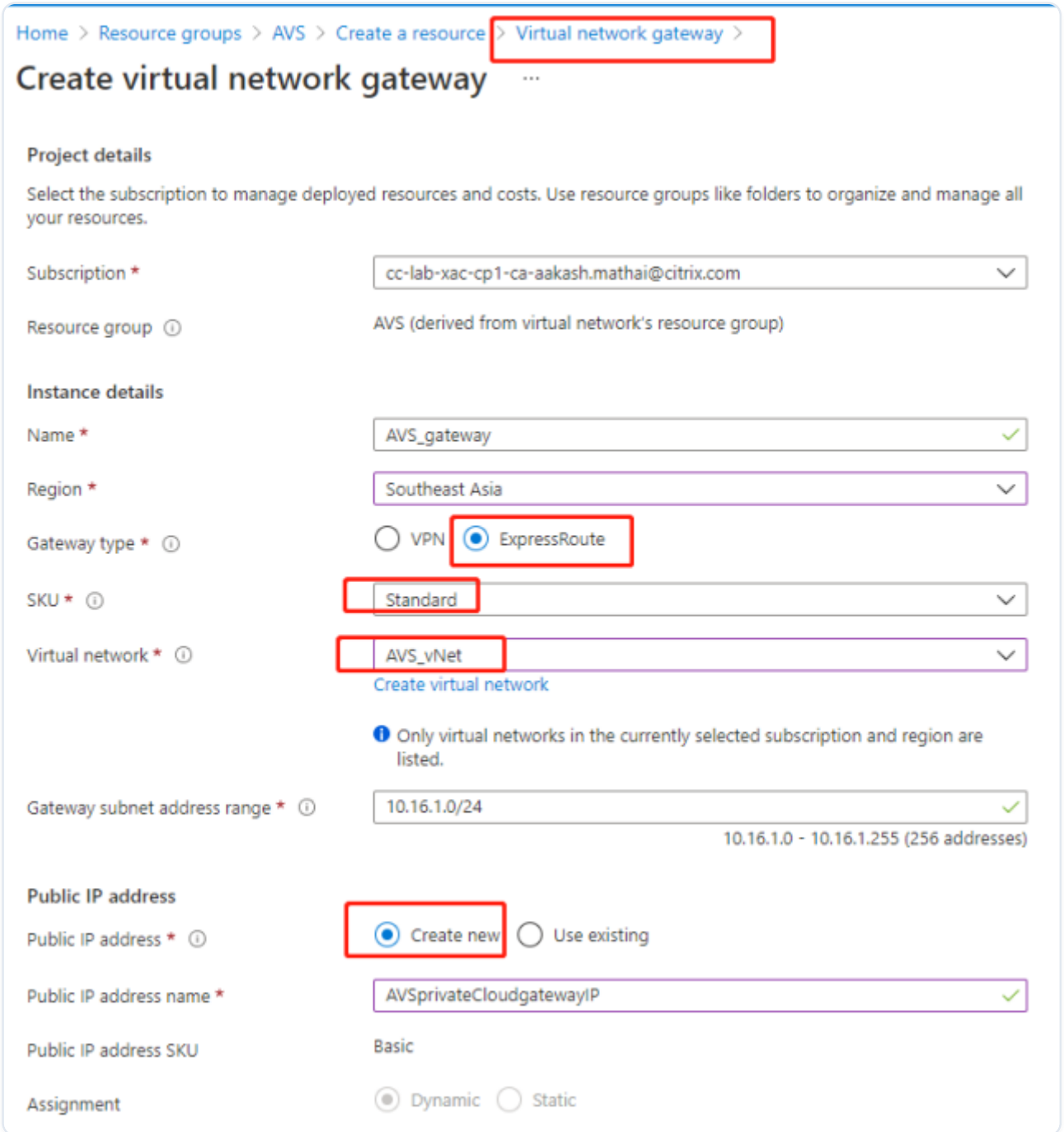
> アドレス空間を入力した後:

1. 「**+ サブネットの追加**」を選択します。
2. 「**サブネットの追加**」ページで、サブネットに名前と適切なアドレス範囲を割り当てます。
3. 「**追加**」をクリックします。
4. 「**確認 + 作成**」を選択します。
5. 情報を確認し、「**作成**」をクリックします。デプロイが完了すると、仮想ネットワークがリソースグループに表示されます。

仮想ネットワークゲートウェイを作成する

仮想ネットワークを作成した後、仮想ネットワークゲートウェイを作成します。

1. リソースグループで、**+ 追加**を選択して新しいリソースを追加します。
2. **Marketplace を検索**テキストボックスに「*virtual network gateway*」と入力します。仮想ネットワークリソースを見つけて選択します。
3. **仮想ネットワークゲートウェイ**ページで、**作成**をクリックします。
4. **仮想ネットワークゲートウェイの作成**ページの**基本**タブで、フィールドに値を入力します。
5. **確認 + 作成**をクリックします。



仮想ネットワークゲートウェイの構成を確認した後、**作成**をクリックして仮想ネットワークゲートウェイをデプロイします。 デプロイが完了したら、**ExpressRoute**接続をAzure AVSプライベートクラウドを含む仮想ネットワークゲートウェイに接続します。

EXPRESSROUTEを仮想ネットワークゲートウェイに接続する

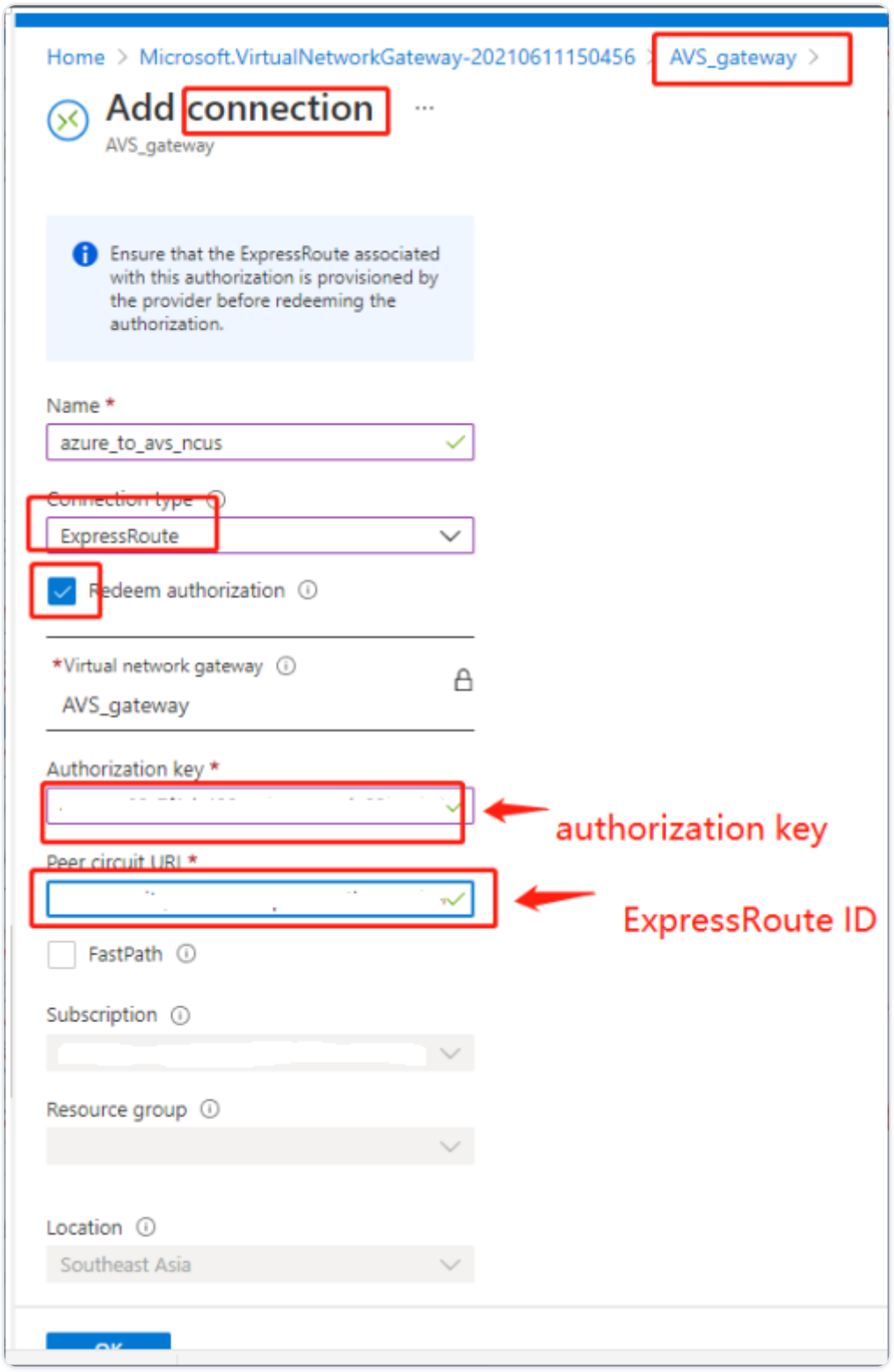
仮想ネットワークゲートウェイを展開した後、それとAzure AVSプライベートクラウドの間に接続を追加します。

1. ExpressRoute 承認キーを要求します。
2. Azure ポータルで、**Azure VMware Solution プライベートクラウド**に移動します。**管理 > 接続 > ExpressRoute**を選択し、**+ 承認キーを要求**を選択します。

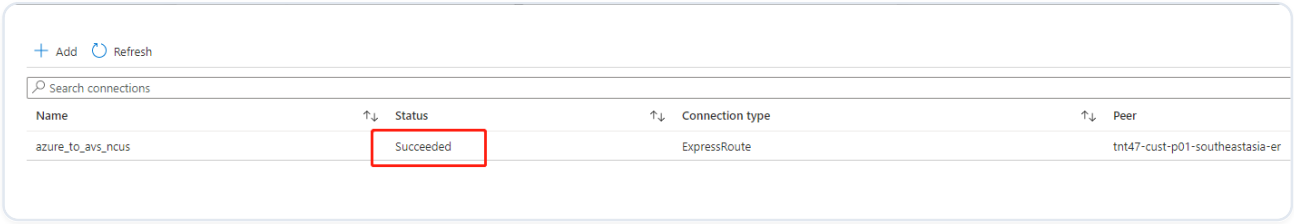
Azure ASV 承認キーの要求(/en-us/citrix-virtual-apps-desktops/2511/media/azure-avs-expressroute.png)

承認キーを要求した後：

1. キーの名前を入力し、**作成**をクリックします。キーの作成には約30秒かかる場合があります。作成されると、新しいキーはプライベートクラウドの承認キーのリストに表示されます。
2. **認証キー**と**ExpressRoute ID**をコピーします。これらはピアリングプロセスを完了するために必要です。認証キーはしばらくすると消えるため、表示されたらすぐにコピーしてください。
3. 使用する予定の**仮想ネットワークゲートウェイ**に移動し、**接続 > + 追加**を選択します。
4. **接続の追加**ページで、フィールドに値を入力し、**OK**を選択します。



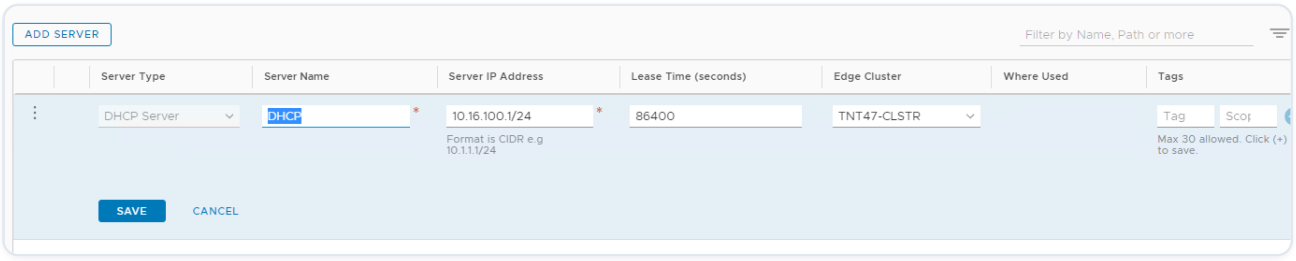
ExpressRoute回線と仮想ネットワーク間の接続が確立されます。



AZURE VMWARE SOLUTION の DHCP を構成する

ExpressRouteを仮想ゲートウェイに接続した後、DHCPを構成します。
NSX-T を使用して DHCP サーバーをホストする
NSX-T Manager で、次の手順を実行します。

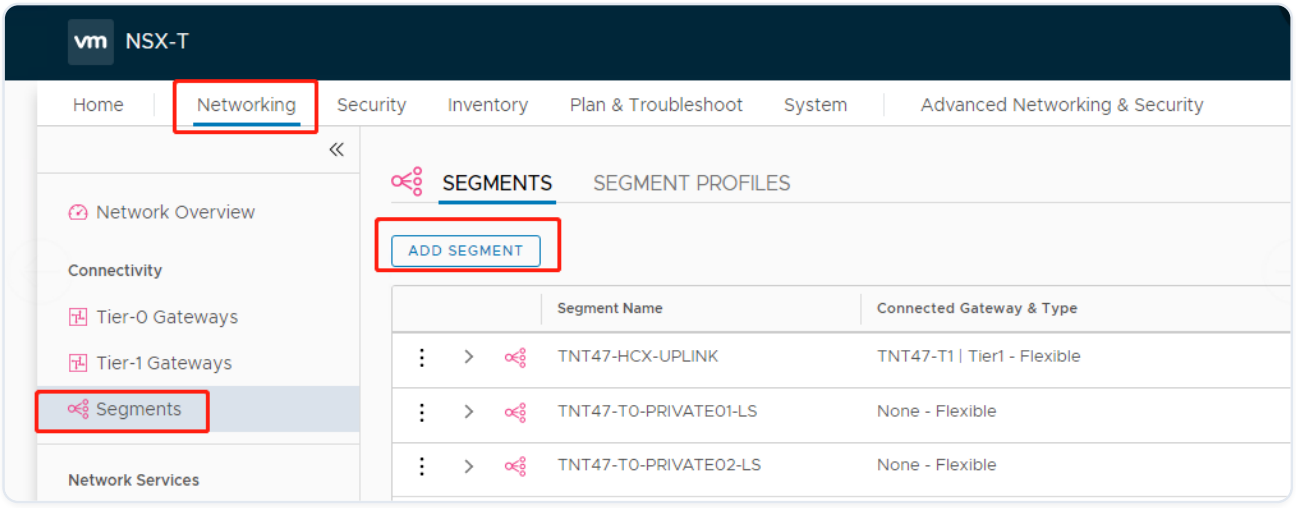
1. **ネットワーク > DHCP**を選択し、次に**サーバーの追加**を選択します。
2. **サーバーの種類**として**DHCP**を選択し、サーバー名と IP アドレスを入力します。
3. **保存**をクリックします。
4. **Tier 1 ゲートウェイ**を選択し、Tier-1 ゲートウェイの縦の省略記号を選択し、次に**編集**を選択します。
5. サブネットを追加するには、**IP 割り当てなしを設定**を選択します。
6. 「**Type**」には「**DHCP Local Server**」を選択します。
7. 「**DHCP Server**」には「**Default DHCP**」を選択し、「**Save**」をクリックします。
8. もう一度「**Save**」をクリックし、「**Close Editing**」を選択します。



AZURE VMWARE SOLUTIONでネットワークセグメントを追加する

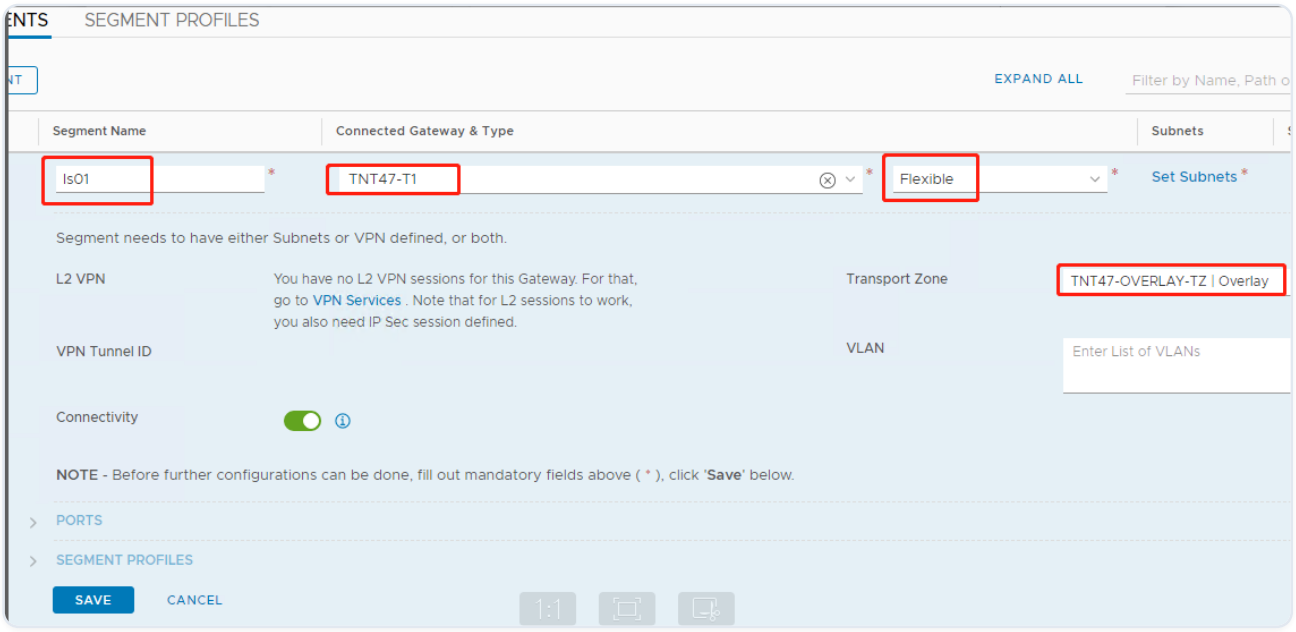
DHCPを設定したら、ネットワークセグメントを追加します。

ネットワークセグメントを追加するには、NSX-T Managerで **Networking> Segments** を選択し、**Add Segment** をクリックします。



Segments profile画面で：

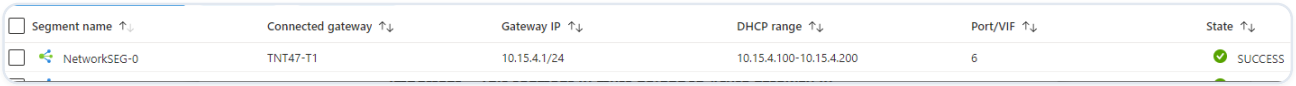
1. セグメントの**名前**を入力します。
2. 「**Connected Gateway**」として「**Tier-1 Gateway (TNTxx-T1)**」を選択し、「**Type**」は「**Flexible**」のままにします。
3. 事前設定されたオーバーレイ「**Transport Zone(TNTxx-OVERLAY-TZ)**」を選択します。
4. 「**Set Subnets**」をクリックします。



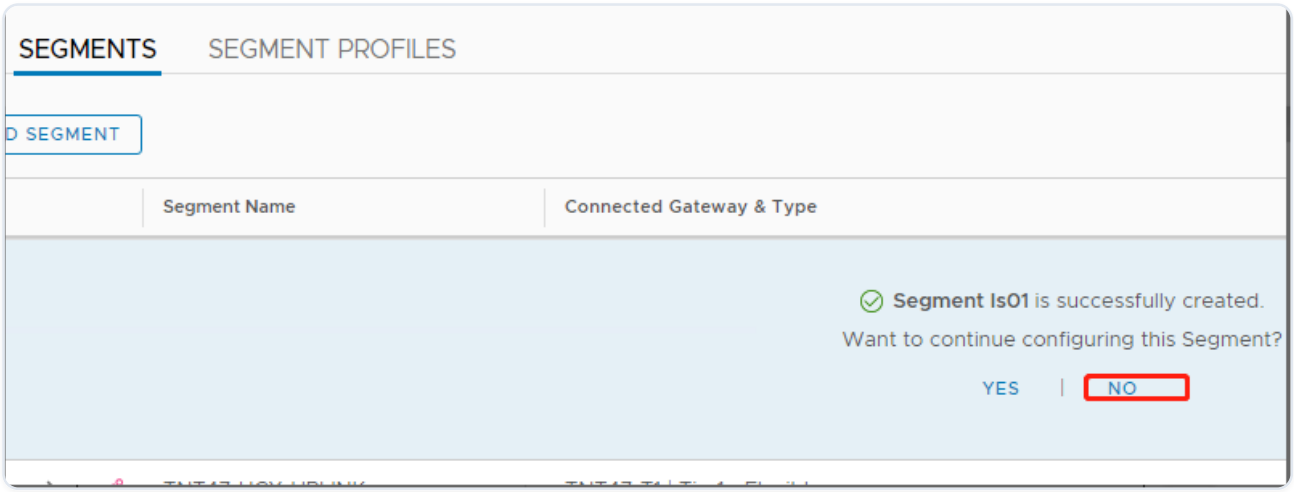
Subnetsセクションで：

1. ゲートウェイIPアドレスを入力します。
2. **Add**を選択します。

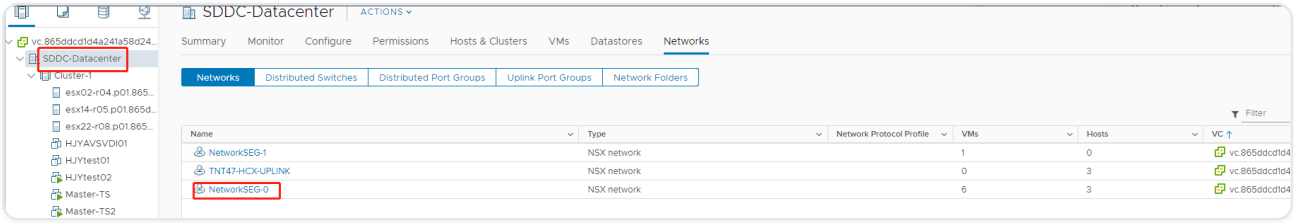
> **重要:**
>
> このセグメントIPアドレスは、Azureゲートウェイ IPアドレス (10.15.0.0/22) に属している必要があります。
>
> DHCP範囲はセグメントIPアドレスに属している必要があります。



セグメントの構成を続行するオプションを拒否するには、 を選択します:

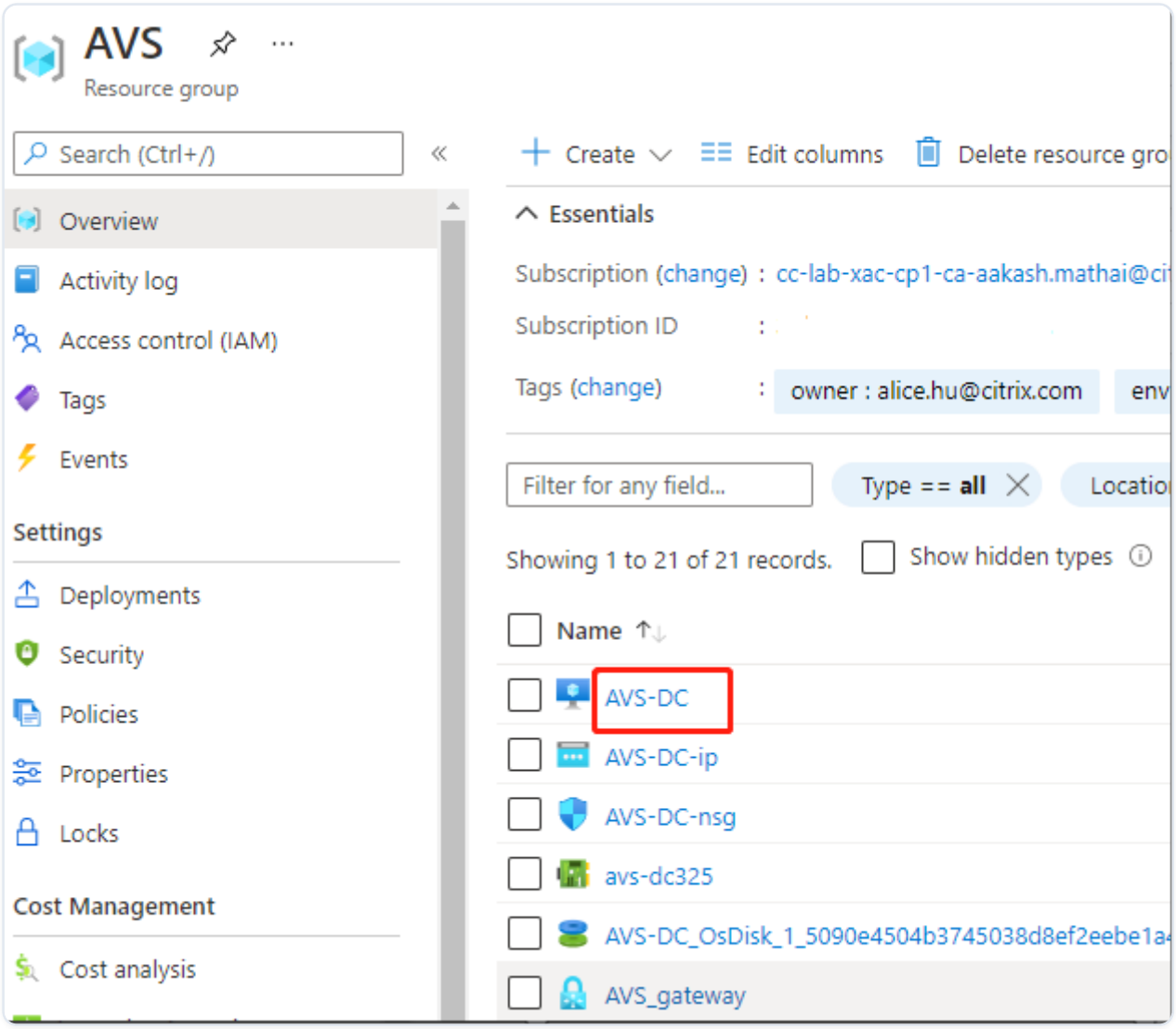


vCenterで、**Networking > SDDC-Datacenter**を選択します。

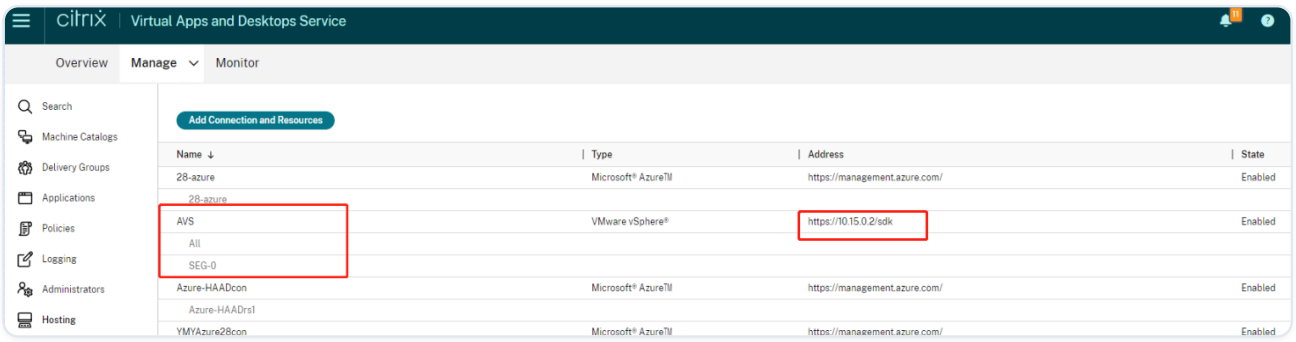


AZURE AVS環境を確認する

Azureリソースグループで直接接続とコネクタを設定します。



vCenterの資格情報で接続を確認します。



Google Cloud VMware エンジン

Citrix Virtual Apps and Desktopsを使用すると、VMwareベースのオンプレミスCitrixワークロードをGoogle Cloud VMware Engineに移行できます。

Google Cloud VMware Engineを構成する

次の手順では、Google Cloud VMware Engineでクラスターを取得してセットアップする方法について説明します。

VMWARE ENGINEポータルにアクセスする

1. **Google Cloud Console**で、ナビゲーションメニューをクリックします。
2. **Compute**セクションで、**VMware Engine**をクリックして、新しいブラウザタブでVMware Engineを開きます。

最初のプライベートクラウドを作成するための要件

Google Cloud VMware Engineへのアクセス権、利用可能なVMware Engineノードクォータ、および適切なIAMロールが必要です。プライベートクラウドの作成を続行する前に、次の要件を準備してください。

1. APIアクセスとノードクォータをリクエストします。詳細については、「APIアクセスとクォータのリクエスト」を参照してください。
2. VMware管理アプライアンスとHCX展開ネットワークに使用するアドレス範囲をメモします。詳細については、「ネットワーク要件」を参照してください。
3. VMware Engine Service Admin IAMロールを取得します。

最初のプライベートクラウドを作成する

1. VMware Engineポータルにアクセスします。
2. VMware Engineのホームページで、**プライベートクラウドを作成**をクリックします。ホスティングの場所とハードウェアノードの種類が一覧表示されます。
3. プライベートクラウドのノード数を選択します。少なくとも3つのノードが必要です。
4. VMware管理ネットワークのクラスレスドメイン間ルーティング（CIDR）範囲を入力します。
5. HCX展開ネットワークのCIDR範囲を入力します。

> **重要:**
>
> CIDR範囲は、オンプレミスまたはクラウドのサブネットと重複してはなりません。
> CIDR範囲は/27以上である必要があります。

6. **「確認して作成」** を選択します。
7. 設定を確認します。設定を変更するには、**「戻る」** をクリックします。
8. **「作成」** をクリックして、プライベートクラウドの作成を開始します。

VMware Engineが新しいプライベートクラウドを作成すると、いくつかのVMwareコンポーネントが展開され、プライベートクラウド内のクラスターの初期Autoscale™ポリシーが設定されます。

プライベートクラウドの作成には30分から2時間かかる場合があります。プロビジョニングが完了すると、メールが届きます。

GOOGLE CLOUD VMWARE ENGINE VPNゲートウェイのセットアップ

Google Cloud VMware Engineへの初期接続を確立するには、VPNゲートウェイを使用できます。これはOpenVPNベースのクライアントVPNであり、これを使用してVMware Software Defined Data Center (SDDC) vCenterに接続し、必要な初期構成を行うことができます。

VPNゲートウェイを展開する前に、SDDCが展開されているリージョンの **Edge Services** 範囲を構成します。これを行うには、次の手順を実行します。

1. **Google Cloud VMware Engine** ポータルにログオンし、**「ネットワーク」>「リージョン設定」** に移動します。**「リージョンの追加」** をクリックします。
2. SDDCが展開されているリージョンを選択し、**「インターネットアクセス」** と **「パブリックIPサービス」** を有効にします。
3. 計画中にメモしたEdge Services範囲を指定し、**「送信」** をクリックします。これらのサービスを有効にするには10〜15分かかります。

   完了すると、Edge Services は地域設定ページで **Enabled** と表示されます。これらの設定を有効にすると、パブリック IP を SDDC に割り当てることができ、これは VPN ゲートウェイを展開するための要件です。

VPNゲートウェイを展開するには：

1. **Google Cloud VMware Engine** ポータルで、**Network > VPN Gateways** に移動します。**Create New VPN Gateway** をクリックします。
2. VPN ゲートウェイの名前と、計画中に予約したクライアントサブネットを入力します。**Next** をクリックします。
3. VPN アクセスを許可するユーザーを選択します。**Next** をクリックします。
4. VPN 経由でアクセス可能にする必要があるネットワークを指定します。**Next** をクリックします。
5. 概要画面が表示されます。選択内容を確認し、**Submit** をクリックして VPN ゲートウェイを作成します。VPN Gateways ページには、新しい VPN ゲートウェイのステータスが **Creating** と表示されます。
6. ステータスが **Operational** に変わったら、新しい VPN ゲートウェイをクリックします。
7. VPN ゲートウェイ用に事前設定された OpenVPN プロファイルを含む ZIP ファイルをダウンロードするには、**Download my VPN configuration** をクリックします。UDP/1194 および

TCP/443 経由で接続するためのプロファイルが利用可能です。好みのものを選択して Open VPN にインポートし、接続します。

8. **Resources** に移動し、SDDC を選択します。

VPNを接続する

1. VPN ゲートウェイの設定を通じて、オンプレミスネットワークとプライベートクラウド間のポイントツーサイト接続を確立します。Set up Google Cloud VMware Engine VPN Gateway を参照してください。
2. Set up Google Cloud VMware Engine VPN Gateway でダウンロードした VPN 構成をアップロードします。
3. VPN クライアント（例: OpenVPN Connect）にインポートします。

詳細については、VPNを使用した接続を参照してください。

最初のサブネットを作成する

VMware EngineポータルからNSX-T Managerにアクセスする
サブネットの作成プロセスはNSX-Tで行われ、VMware Engineを介してアクセスします。NSX-T Managerにアクセスするには、次の手順を実行します。

1. **Google Cloud VMware Engine**ポータルにログオンします。
2. メインナビゲーションから、**Resources**に移動します。
3. サブネットを作成するプライベートクラウドに対応する**Private cloud name**をクリックします。
4. プライベートクラウドの詳細ページで、**vSphere Management Network**タブをクリックします。
5. NSX-T Managerに対応する**FQDN**をクリックします。
6. プロンプトが表示されたら、サインイン資格情報を入力します。vIDMを設定し、Active DirectoryなどのIDソースに接続している場合は、代わりにIDソースの資格情報を使用します。

> **注意:**
>
> 生成された資格情報は、プライベートクラウドの詳細ページから取得できます。

サブネットのDHCPサービスを設定する
サブネットを作成する前に、DHCPサービスを設定します。

NSX-T マネージャーで：

1. **Networking > DHCP**に移動します。ネットワークダッシュボードには、DHCPサービスが1つのTier-0と1つのTier-1ゲートウェイを作成することが示されます。
2. DHCPサーバーのプロビジョニングを開始するには、 をクリックします。
3. で を選択し、サーバー名とIPアドレスを入力します。
4. をクリックしてDHCPサービスを作成します。

このDHCPサービスを関連するTier-1ゲートウェイにアタッチするには、次の手順を実行します。デフォルトのTier-1ゲートウェイは、DHCPサービスによってすでにプロビジョニングされています。

1. を選択し、Tier-1ゲートウェイの縦の省略記号を選択してから、 を選択します。
2. フィールドで、 を選択します。
3. で を選択します。
4. で作成したDHCPサーバーを選択します。
5. をクリックします。
6. をクリックします。

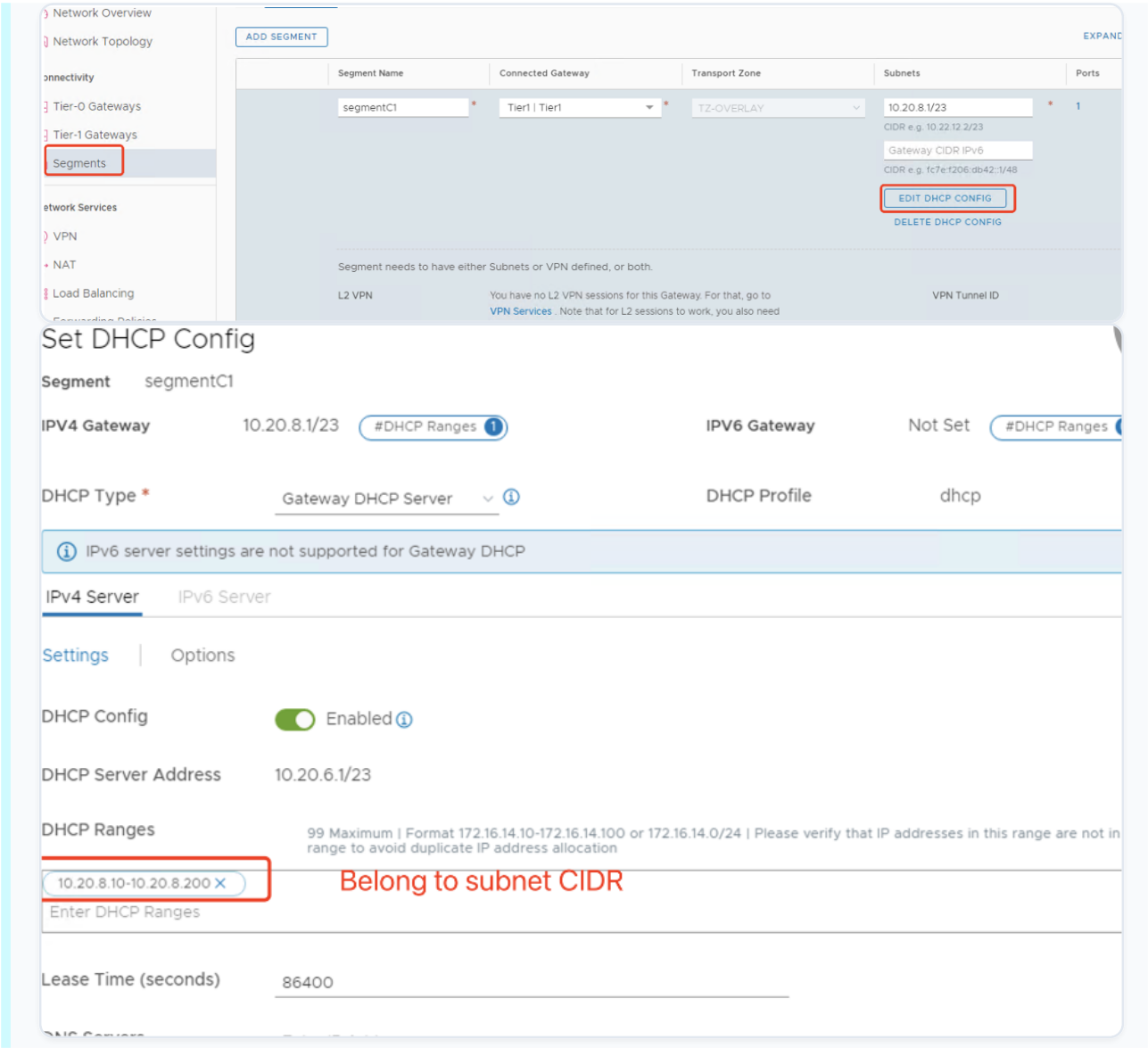
これで、NSX-Tでネットワークセグメントを作成できます。NSX-TでのDHCPの詳細については、VMware documentation for DHCPを参照してください。
NSX-T でネットワークセグメントを作成する
ワークロード VM の場合、プライベートクラウドの NSX-T ネットワークセグメントとしてサブネットを作成します。

1. NSX-T Managerで、 **>** に移動します。
2. をクリックします。
3. セグメントの名前を入力します。
4. 「**Connected Gateway**」として「**Tier-1**」を選択し、「Type」は「**Flexible**」のままにします。
5. 「**Set Subnets**」をクリックします。
6. 「**Add Subnets**」をクリックします。
7. 「**Gateway IP/Prefix Length**」にサブネット範囲を入力します。最後のオクテットが「**.1**」となるようにサブネット範囲を指定します。例: **10.12.2.1/24**。
8. DHCP範囲を指定し、**ADD**をクリックします。

9. 「**Transport Zone**」で、ドロップダウンリストから「**TZ-OVERLAY**」を選択します。
10. **Save**をクリックします。これで、VMの作成時にvCenterでこのネットワークセグメントを選択できるようになります。

特定のリージョンでは、プライベートサービスアクセスを使用して、VMware EngineからVPCネットワークへの一意のルートを最大100個設定できます。これには、たとえば、プライベートクラウド管理IPアドレス範囲、NSX-Tワークロードネットワークセグメント、HCXネットワークIPアドレス範囲が含まれます。この制限には、そのリージョン内のすべてのプライベートクラウドが含まれます。

> **注:**
>
> Google Cloudの構成の問題により、DHCP範囲設定を複数回構成する必要があります。したがって、Google Cloudの構成後にDHCP範囲設定を構成するようにしてください。DHCP範囲を構成するには、**EDIT DHCP CONFIG**をクリックします。



CITRIX STUDIOでGOOGLE CLOUD VMWARE接続を作成する

1. vCenterでマシンを作成します。
2. Citrix Studioを起動します。
3. ホスティングノードを選択し、**接続とリソースの追加**をクリックします。
4. **接続**画面で、**新しい接続の作成**を選択し、以下の詳細を入力します。

   接続とリソースの追加(/en-us/citrix-virtual-apps-desktops/2511/media/gcp-vmware-add-connection.png)

   a. **接続タイプ**として**VMware vSphere**を選択します。
   b. **接続アドレス**に、vCenterのプライベートIPアドレスを入力します。
   c. vCenterの資格情報を入力します。
   d. 接続名を入力します。

e. 仮想マシンを作成するツールを選択します。

5. **ネットワーク**画面で、NSX-Tサーバーで作成されたサブネットを選択します。
6. ウィザードを完了します。

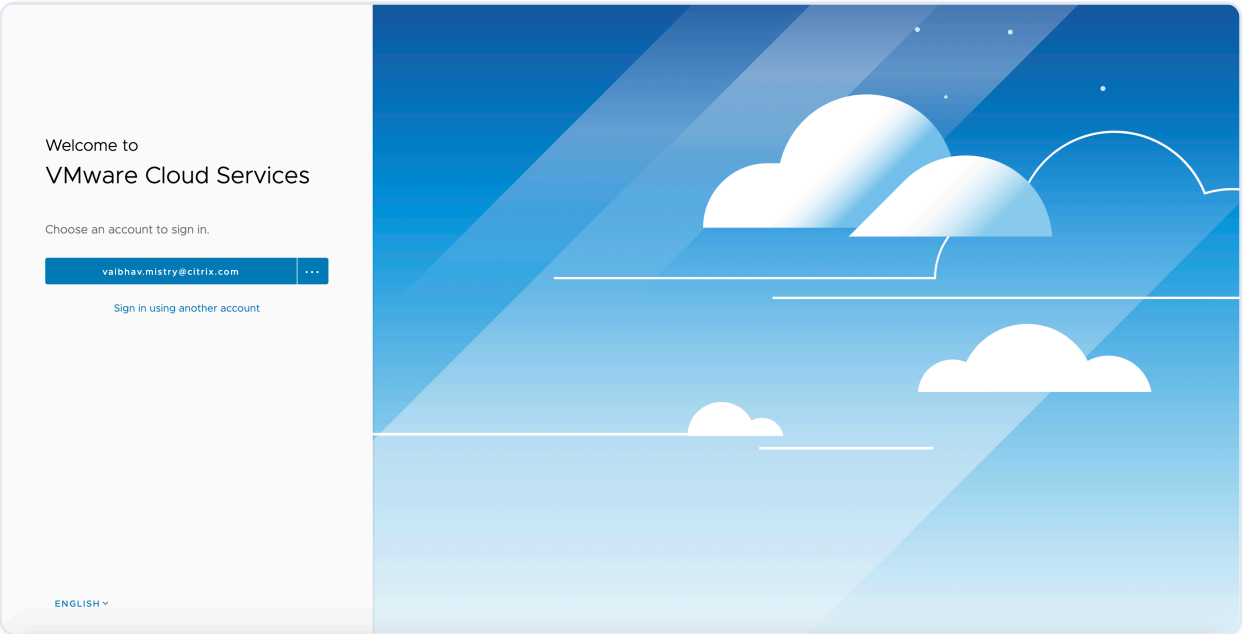
アマゾン ウェブ サービス (AWS) 上の VMware クラウド

Amazon Web Services (AWS) 上のVMware Cloudを使用すると、VMwareベースのオンプレミスCitrixワークロードをAWS Cloudに移行できます。

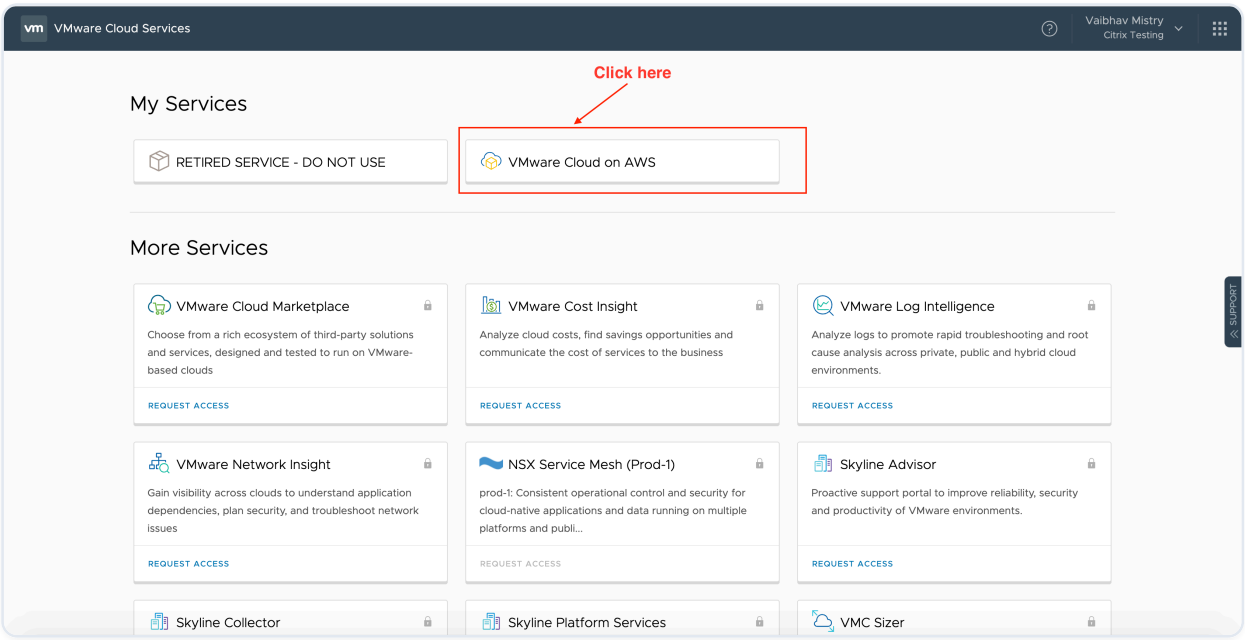
この記事では、AWS上にVMware Cloudをセットアップする手順について説明します。

VMware Cloud環境へのアクセス

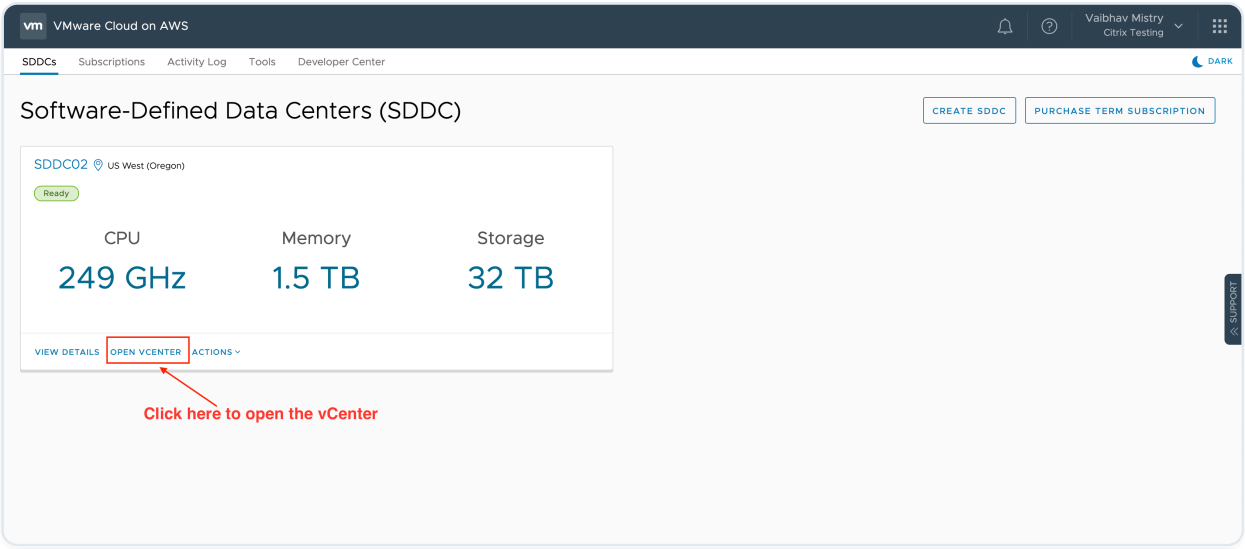
1. URL `<https://console.cloud.vmware.com/>` を使用してVMware Cloudサービスにログインします。



2. 「**VMware Cloud on AWS**」をクリックします。「Software-Defined Data Centers (SDDC)」ページが表示されます。

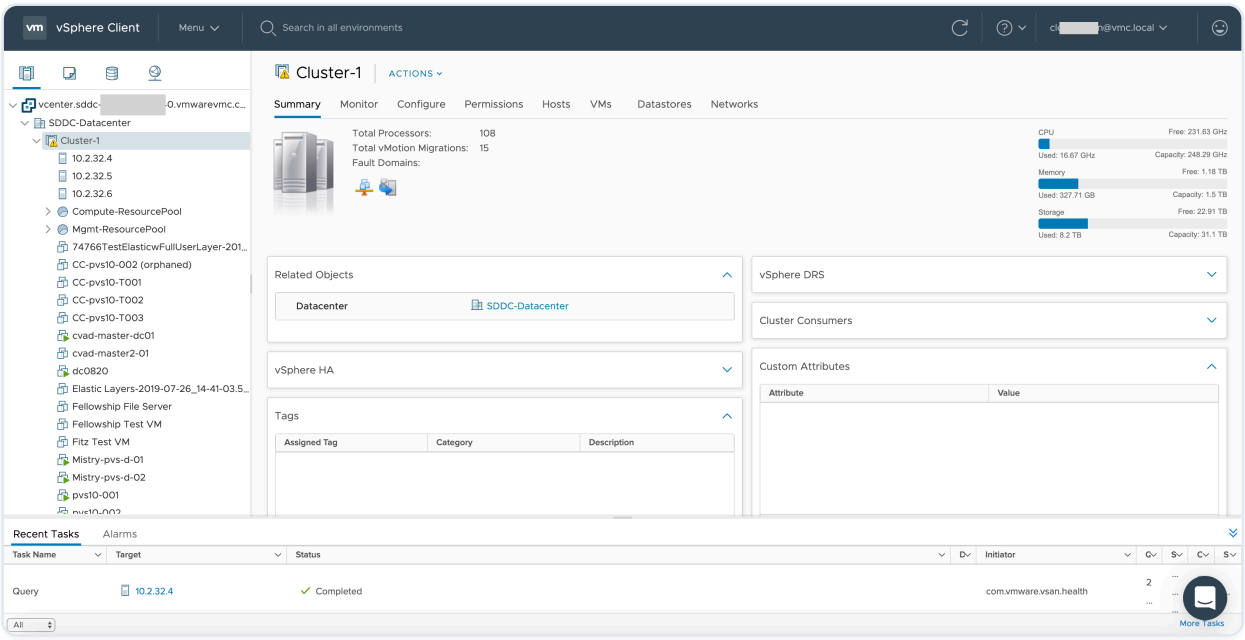


3. 「**OPEN VCENTER**」をクリックし、次に「**SHOW CREDENTIALS**」をクリックします。後で使用するために資格情報を控えておきます。



「資格情報を表示」(/en-us/citrix-virtual-apps-desktops/2511/media/show-credentials-vmc.png)

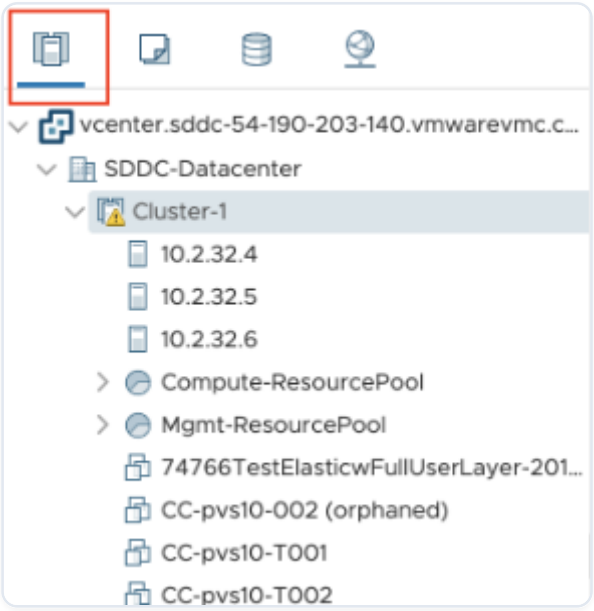
4. Webブラウザを開き、vSphere Web ClientのURLを入力します。
5. 控えておいた資格情報を入力し、「**Login**」をクリックします。vSphereクライアントのWebページは、オンプレミス環境と似ています。



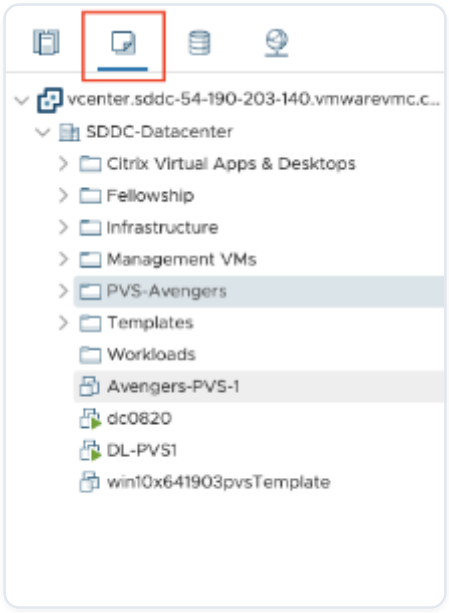
VMwareクラウド環境について

vSphereクライアントのWebページには4つのビューがあります。

- ホストとクラスタービュー：新しいクラスターを作成することはできませんが、クラウド管理者は複数のリソースプールを作成できます。



- VMとテンプレートビュー：クラウド管理者は多くのフォルダーを作成できます。



- ストレージビュー: Citrix Studioでホスティングユニットを追加する際、Workload Datastoreにのみアクセスできるため、**WorkloadDatastore**ストレージを選択してください。

  「ストレージビュー」(/en-us/citrix-virtual-apps-desktops/2511/media/storage-view.png)

- ネットワークビュー: VMwareクラウドネットワークと不透明なネットワークでは、アイコンが異なります。

  「ネットワークビュー」(/en-us/citrix-virtual-apps-desktops/2511/media/network-view.png)

クラスターを設定したら、接続とリソースの追加については、VMware仮想化環境を参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- 接続の作成と管理については、「VMware Cloudおよびパートナーソリューションへの接続」を参照してください。

詳細情報

- 接続とリソースを作成および管理する
- マシンカタログを作成する

コアコンポーネントをインストールする

重要:

- Citrix は、ライセンスコンプライアンスを含む正当な利益のために、基本的なライセンスデータを収集します。詳細については、「Citrix ライセンスデータ」を参照してください。
- ライセンスサーバーがバージョン 11.17.2 ビルド 53100 以降で実行されていることを確認してください。この前提条件を満たさない場合、Citrix Virtual Apps and Desktops サイトのアップグレードとサイト作成がブロックされます。

コアコンポーネントは、Citrix Delivery Controller™、Citrix Studio、Web Studio、Citrix Director、および Citrix License Server です。

注:

Citrix Studio は、オンプレミスの Citrix Virtual Apps and Desktops 展開を構成および管理できる Windows ベースの管理コンソールです。Web Studio は、Citrix Studio の次世代版であり、Citrix Studio と同等の機能を備えた Web ベースの管理コンソールです。Web Studio の詳細については、「Web Studio のインストール」を参照してください。

(2003 より前のバージョンでは、コアコンポーネントに Citrix StoreFront が含まれていました。**Citrix StoreFront** タイルをクリックするか、インストールメディアで利用可能なコマンドを実行することで、StoreFront を引き続きインストールできます。)

インストールを開始する前に、この記事と「インストールの準備」を確認してください。

この記事では、コアコンポーネントのインストール時のインストールウィザードのシーケンスについて説明します。コマンドラインの同等機能も提供されています。詳細については、「コマンドラインを使用したインストール」を参照してください。

ステップ 1. 製品ソフトウェアをダウンロードしてウィザードを起動する

Citrix アカウントの資格情報を使用して、Citrix Virtual Apps and Desktops™ のダウンロードページにアクセスします。製品の ISO ファイルをダウンロードします。

ファイルを解凍します。必要に応じて、ISO ファイルを DVD に書き込みます。

コアコンポーネントをインストールするマシンに、ローカル管理者アカウントを使用してログオンします。

DVD をドライブに挿入するか、ISO ファイルをマウントします。インストーラーが自動的に起動しない場合は、**AutoSelect** アプリケーションまたはマウントされたドライブをダブルクリックします。

ステップ 2. インストールする製品を選択する

コンポーネントインストーラーの製品選択ページ(/en-us/citrix-virtual-apps-desktops/2511/media/product-selector2-75.png)

インストールする製品（Virtual AppsまたはVirtual Apps and Desktops）の横にある**Start**をクリックします。

(マシンにCitrix Virtual Apps™ and Desktopsコンポーネントがすでにインストールされている場合、このページは表示されません。)

コマンドラインオプション: Citrix Virtual Apps をインストールするには `/xenapp` を使用します。このオプションを省略すると、Citrix Virtual Apps and Desktops がインストールされます。

ステップ 3. インストールするものを選択する

コンポーネントインストーラーのコンポーネント選択ページ(/en-us/citrix-virtual-apps-desktops/2511/media/what-to-install-2.png)

初めて使用する場合は、**Delivery Controller**を選択します。（後のページで、このマシンにインストールする特定のコンポーネントを選択します。）

すでにControllerをインストールしている場合（このマシンまたは別のマシンに）、別のコンポーネントをインストールするには、**Extend Deployment**セクションからコンポーネントを選択します。

コマンドラインオプション: `/components`

ステップ 4. ライセンス契約を読んで同意する

コンポーネントインストーラーのライセンス契約ページ(/en-us/citrix-virtual-apps-desktops/2511/media/core-license-75.png)

Licensing Agreementページで、ライセンス契約を読んだ後、内容を読んで同意したことを示します。次に、**Next**をクリックします。

ステップ 5. インストールするコンポーネントとインストール場所を選択する

コンポーネントインストーラーのコアコンポーネントページ(/en-us/citrix-virtual-apps-desktops/2511/media/core-components-75.png)

「**コアコンポーネント**」ページで：

- **場所：** デフォルトでは、コンポーネントは`C:\Program Files\Citrix`にインストールされます。ほとんどの展開では、デフォルトで問題ありません。別の場所を指定する場合は、ネットワークサービスに対する実行権限が必要です。
- **コンポーネント：** デフォルトでは、すべてのコアコンポーネントのチェックボックスが選択されています。概念実証、テスト、または小規模な本番展開では、すべてのコアコンポーネントを1台のサーバーにインストールしても問題ありません。大規模な本番環境では、CitrixはDirector、StoreFront、Secure Private Access、およびライセンスサーバーを別々のサーバーにインストールすることを推奨しています。

> **注：**
>
> 複数のサーバーにコンポーネントをインストールする場合は、他のサーバーに他のコンポーネントをインストールする前に、まずCitrixライセンスサーバーとライセンスをインストールしてください。ガイダンスについては、Citrix Virtual Apps and Desktopsのライセンスガイドの「自動インストール」セクションを参照してください。

> このマシンに必須のコアコンポーネントをインストールしないことを選択すると、アイコンで警告が表示されます。その警告は、そのコンポーネントをインストールする必要があることを通知しますが、必ずしもこのマシンにインストールする必要はありません。

Nextをクリックします。

コマンドラインオプション：`/installdir`、`/components`、`/exclude`

ハードウェアチェック

Delivery Controllerをインストールまたはアップグレードすると、ハードウェアがチェックされます。マシンに推奨RAM容量（5 GB）よりも少ないRAMしかない場合、インストーラーは警告を表示します。これはサイトの安定性に影響を与える可能性があります。詳細については、ハードウェア要件を参照してください。

グラフィカルインターフェイス： ダイアログボックスが表示されます。

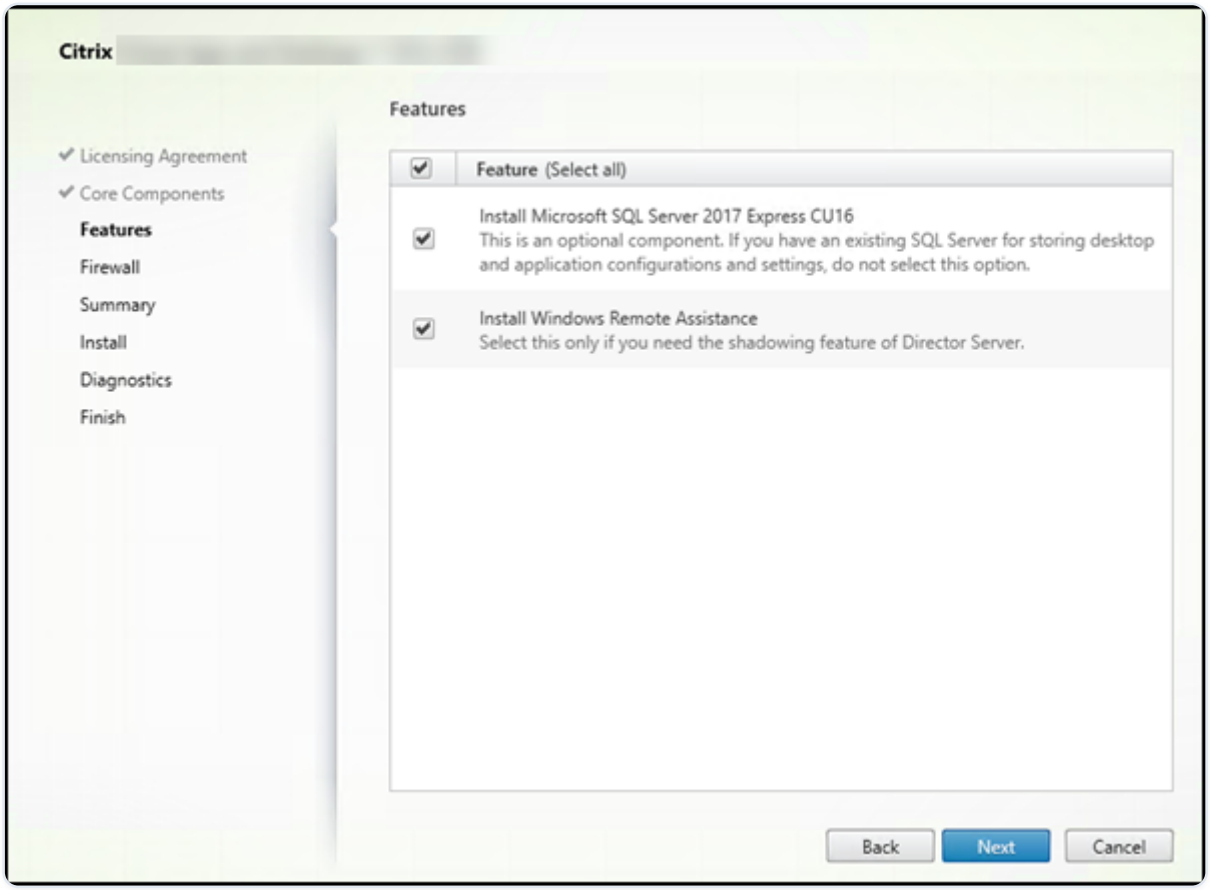
- 推奨：**キャンセル**をクリックしてインストールを停止します。マシンにRAMを追加してから、再度インストールを開始します。
- または、**次へ**をクリックしてインストールを続行します。サイトの安定性に問題が発生する可能性があります。

コマンドラインインターフェイス： インストール/アップグレードは終了します。インストールログには、検出された内容と利用可能なオプションを説明するメッセージが含まれています。

- 推奨：マシンにRAMを追加してから、再度コマンドを実行します。
- または、`/ignore_hw_check_failure` オプションを指定してコマンドを再度実行し、警告を上書きします。サイトで安定性の問題が発生する可能性があります。

アップグレード時に、OSまたはSQL Serverのバージョンがサポートされなくなった場合も通知されます。展開のアップグレードを参照してください。

手順 6. 機能の有効化または無効化



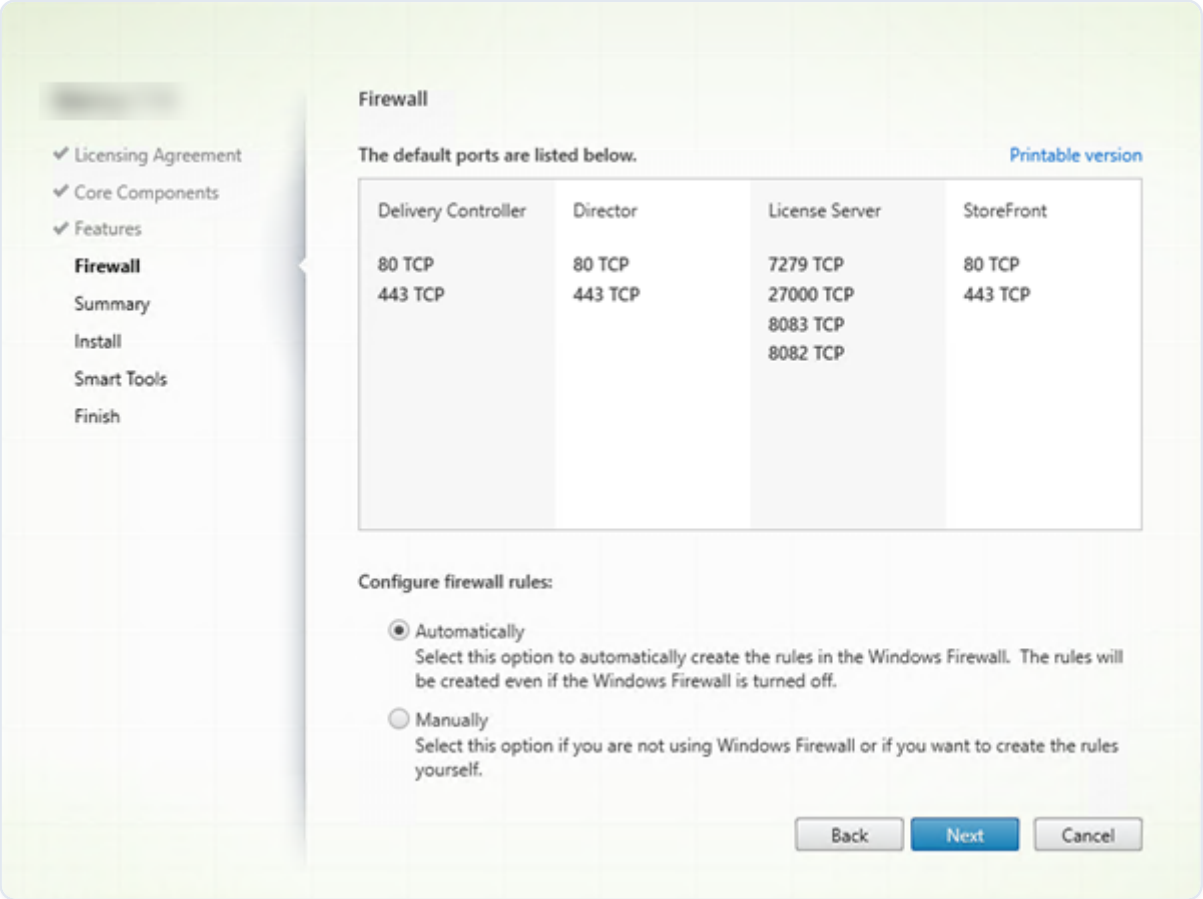
機能ページで、次の操作を行います。

- サイトデータベースとして使用するためにMicrosoft SQL Server Expressをインストールするかどうかを選択します。デフォルトでは、この選択は有効になっています。Citrix Virtual Apps and Desktopsデータベースに慣れていない場合は、データベースを確認してください。
- Directorをインストールすると、Windowsリモートアシスタンスが自動的にインストールされます。Directorのユーザーシャドウイングで使用するために、Windowsリモートアシスタンスでシャドウイングを有効にするかどうかを選択します。シャドウイングを有効にすると、TCPポート3389が開きます。デフォルトでは、この機能は有効になっています。ほとんどの展開では、デフォルト設定で問題ありません。この機能は、Directorをインストールしている場合にのみ表示されます。

Nextをクリックします。

コマンドラインオプション: `/nosql` (インストールを防止するため)、`/no_remote_assistance` (有効化を防止するため)

手順7. Windowsファイアウォールポートを開く



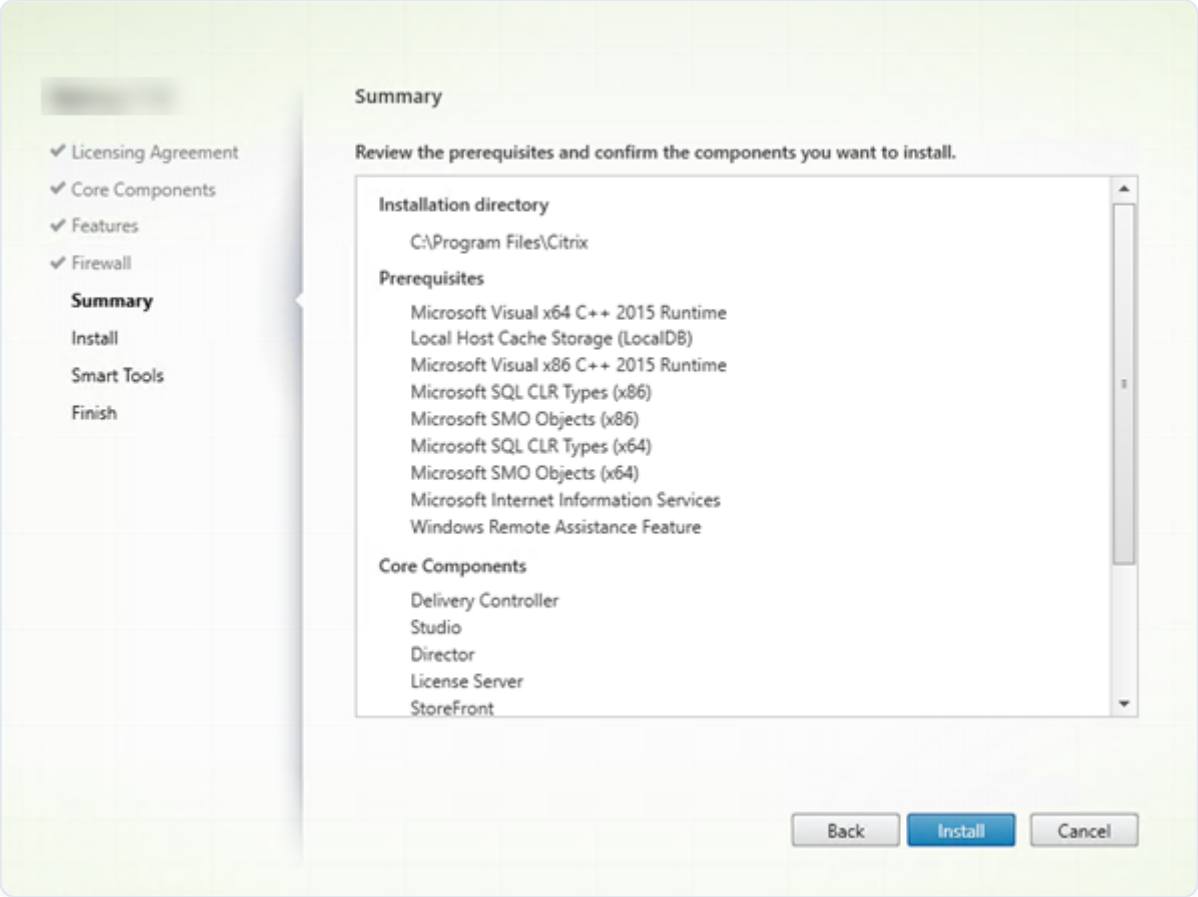
デフォルトでは、Windowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても、**ファイアウォール**ページ上のポートは自動的に開かれます。ほとんどの展開では、デフォルト設定で問題ありません。ポート情報については、ネットワークポートを参照してください。

Nextをクリックします。

(このグラフィックは、このマシンにすべてのコアコンポーネントをインストールしたときのポートリストを示しています。この種のインストールは通常、テスト展開のみを対象としています。)

コマンドラインオプション: `/configure_firewall`

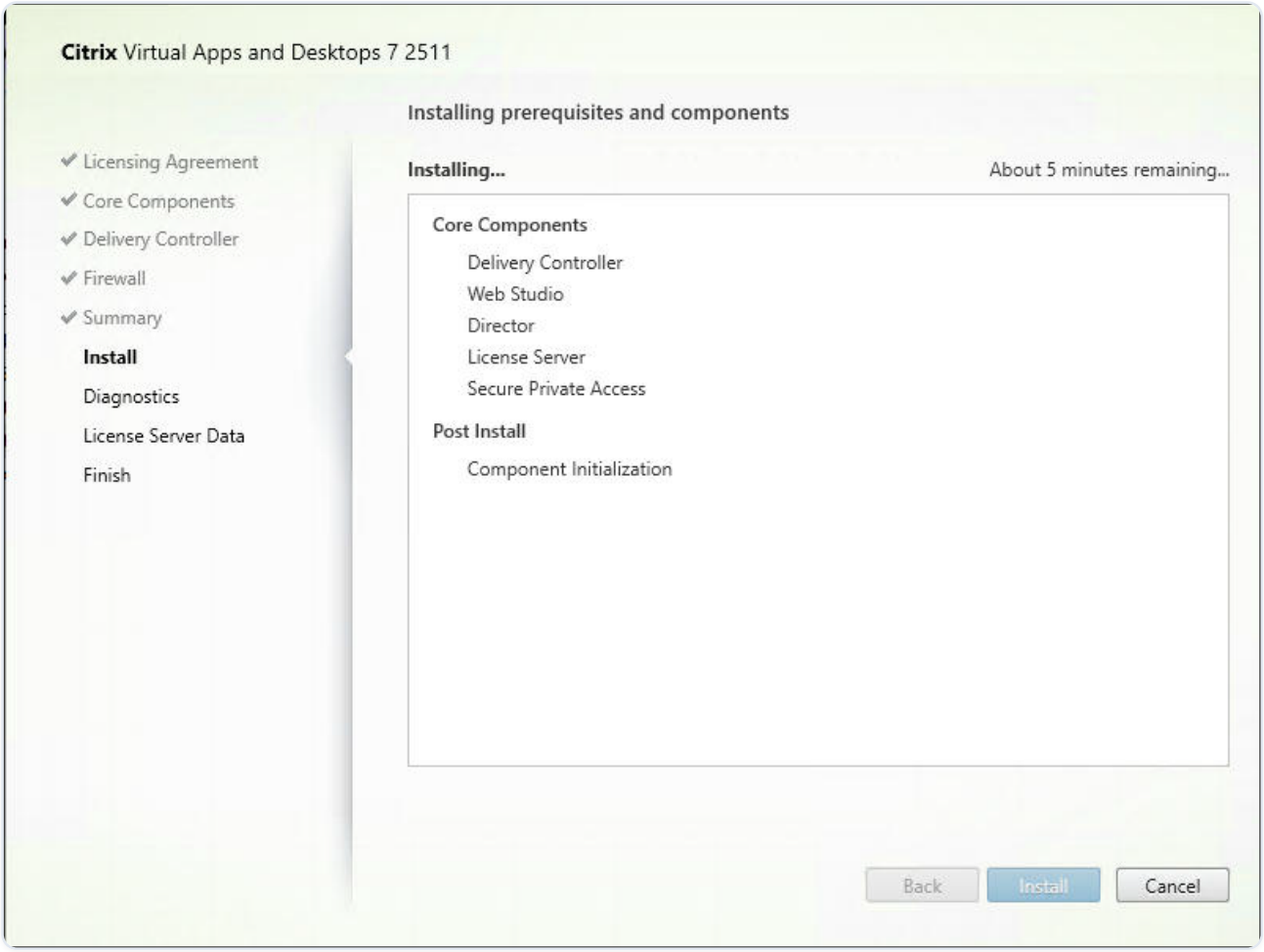
手順8. 前提条件を確認し、インストールを確定する



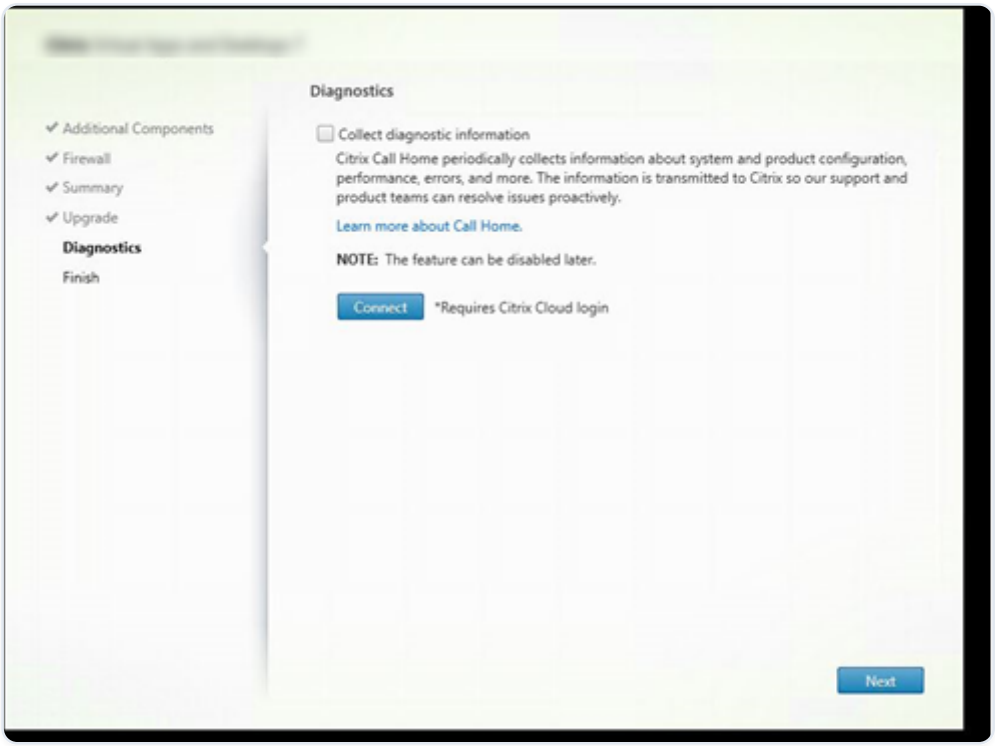
概要ページには、インストールされるものが表示されます。必要に応じて、**戻る**ボタンを使用して以前のウィザードページに戻り、選択を変更できます。

準備ができたら、**インストール**をクリックします。

ディスプレイにはインストールの進行状況が表示されます。



ステップ9. Cloud Software Groupとの診断情報の共有



診断ページで、Citrix Call Homeに参加するかどうかを選択します。

このページは、グラフィカルインターフェイスを使用してDelivery Controllerをインストールするときに表示されます。StoreFrontをインストールする場合（ただしControllerではない場合）、ウィザードはこのページを表示します。その他のコアコンポーネントをインストールする場合（ただしControllerまたはStoreFrontではない場合）、ウィザードはこのページを表示しません。

アップグレード中に、Call Homeがすでに有効になっている場合、またはインストーラーがCitrix Telemetry Serviceに関連するエラーを検出した場合、このページは表示されません。

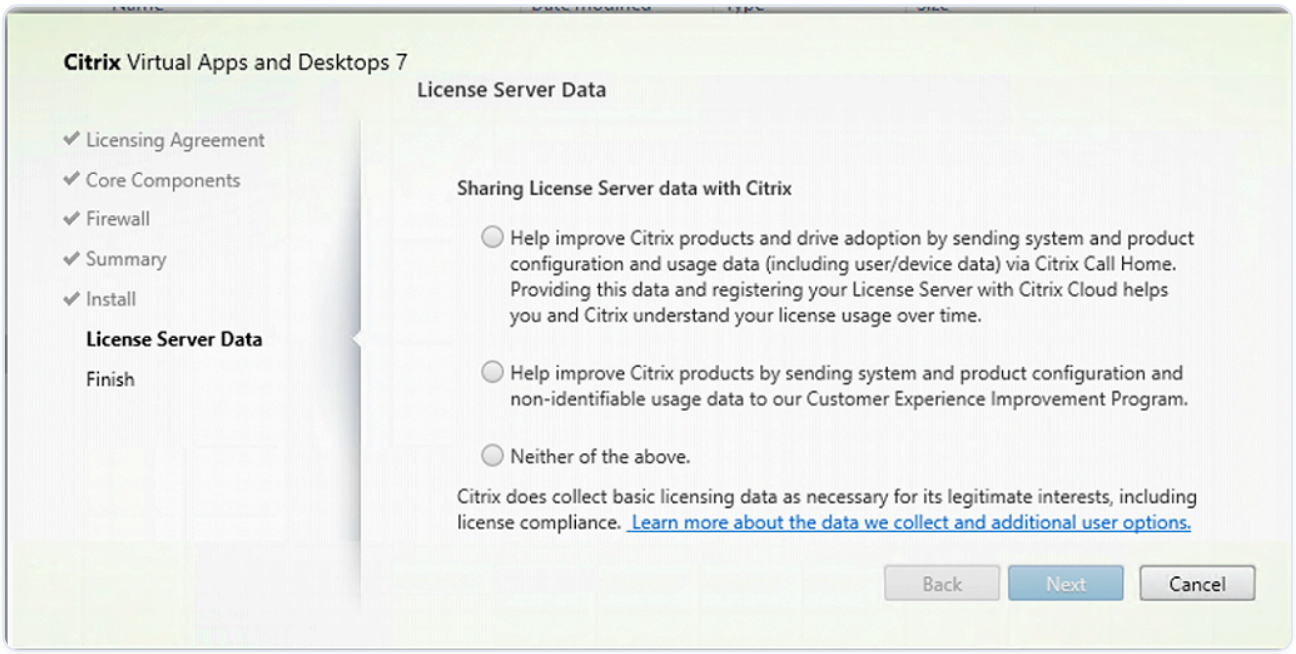
参加することを選択した場合（デフォルト）、**接続**をクリックします。プロンプトが表示されたら、Citrixアカウントの資格情報を入力します。登録の選択は、インストール後に変更できます。

資格情報が検証された後（または参加しないことを選択した場合）、**次へ**をクリックします。

診断ページで、最初に**診断情報を収集**を選択せずに**接続**をクリックした場合、**Citrix Insight Servicesに接続**ダイアログを閉じると、**次へ**ボタンが無効になります。次のページに進むことはできません。**次へ**ボタンを再度有効にするには、**診断情報を収集**を選択し、すぐに選択を解除します。

詳細については、Call Homeを参照してください。

ステップ 10. Cloud Software Group とのライセンスサーバーデータの共有



「**ライセンスサーバーデータ**」ページでは、お客様を支援するため、Call Home データまたはカスタマーエクスペリエンス向上プログラム (CEIP) データのいずれかを共有していただくようお願いしています。さらに、Cloud Software Group は、正当な利益のために必要に応じて、ライセンスコンプライアンスを含む基本的なライセンスデータの収集も要求します。

ライセンスサーバーデータページは、ライセンスサーバーをインストールしたときに表示されます。

- スタンドアロンとして。
- コアコンポーネントとして、Delivery Controller のインストール中に。

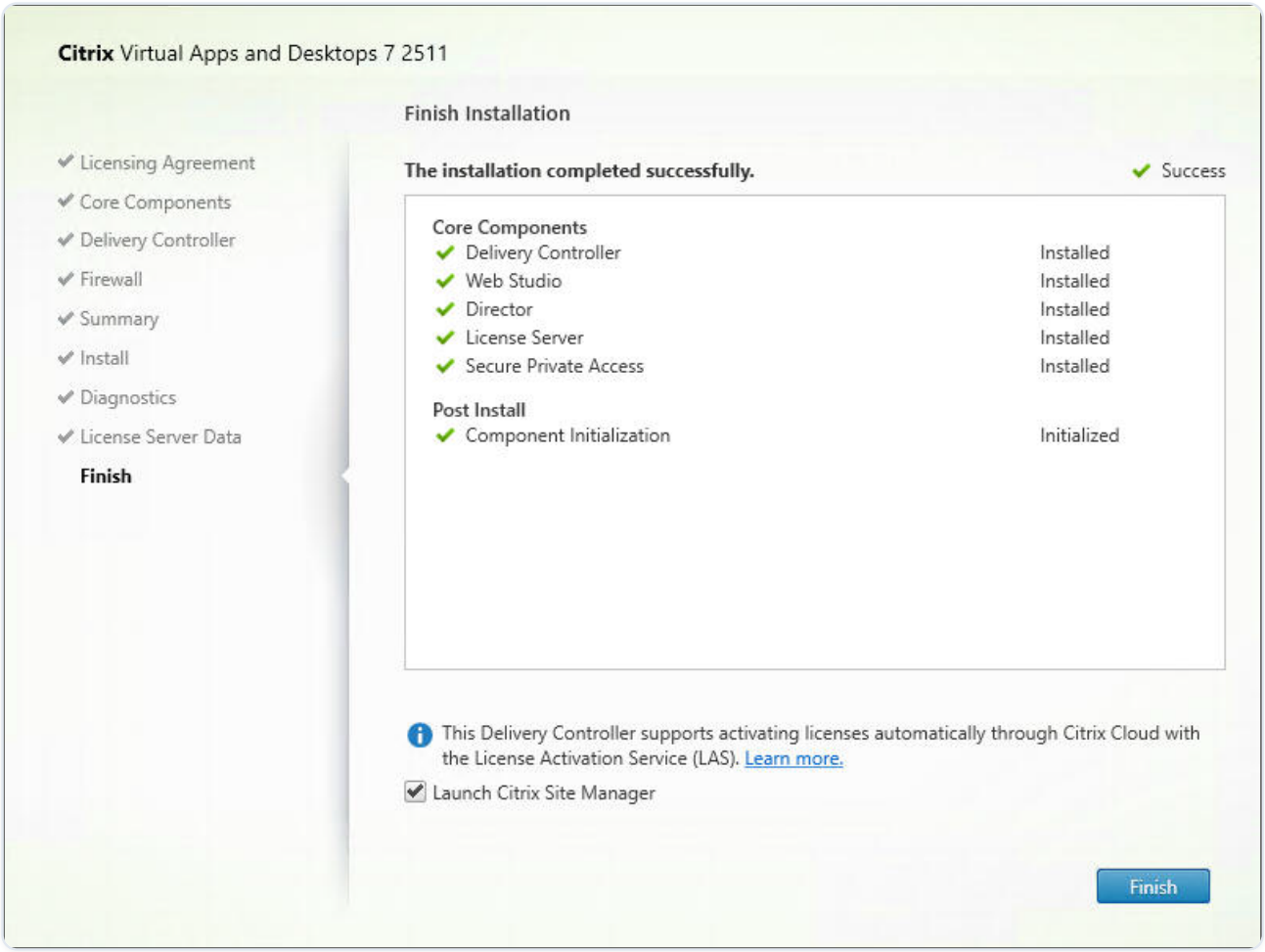
アップグレード中、構成がすでに `/CITRIX.opt:` ファイルで設定されている場合、このページは表示されません。

ライセンスサーバーは、ライセンスデータ、Call Home データ、CEIP データなど、いくつかの種類のユーザーデータを監視します。Call Home データおよび CEIP データの収集を有効にするには、参加を選択する必要があります (オプトイン)。

コマンドラインを使用してインストールする際に Call Home および CEIP データ収集を有効にする方法の詳細については、コアコンポーネントをインストールするためのコマンドラインオプション を参照してください。

Cloud Software Group のライセンスデータ収集の詳細については、Citrix ライセンスデータ収集プログラム を参照してください。

ステップ 11. このインストールを完了する



「**完了**」ページには、正常にインストールおよび初期化されたすべての前提条件とコンポーネントの緑色のチェックマークが表示されます。

完了をクリックします。

> **注:**
>
> バージョン2511にアップグレードすると、インストーラーはCitrix Studio（MMCベース）を自動的にアンインストールします。構成データはデータベースに保存されており、自動アンインストールの影響を受けません。

ステップ12. 残りのコアコンポーネントを他のマシンにインストールする

すべてのコアコンポーネントを1台のマシンにインストールした場合は、次のステップに進んでください。そうでない場合は、他のマシンでインストーラーを実行して他のコンポーネントをインストールします。他のサーバーにControllerを追加でインストールすることもできます。

次のステップ

必要なすべてのコンポーネントをインストールしたら、Web Studioを使用してサイトを作成します。

サイトを作成したら、VDAをインストールします。

いつでも、フルプロダクトインストーラーを使用して、以下のコンポーネントで展開を拡張できます。

- **Universal Print Serverサーバーコンポーネント:** プリントサーバーでインストーラーを起動します。

  a. **展開の拡張**セクションで、**Universal Print Server**を選択します。

  b. ライセンス契約に同意します。

  c. **ファイアウォール**ページでは、Windows Firewall Serviceが実行されている場合、ファイアウォールが有効になっていなくても、デフォルトでTCPポート7229と8080がファイアウォールで開かれます。ポートを手動で開きたい場合は、このデフォルトのアクションを無効にできます。

  このコンポーネントをコマンドラインからインストールするには、Universal Print Serverをインストールするためのコマンドラインオプションを参照してください。
- フェデレーション認証サービス。
- セッションレコーディング。
- ワークスペース環境管理。
- uberAgentのインストール
- deviceTRUST Agentのインストール
- WEM クイックスタートガイド

コマンドラインを使用したインストール

> **重要:**
>
> - アップグレード中で、現在のバージョンでPersonal vDiskまたはAppDisksソフトウェアが使用されているかインストールされている場合は、「PvD、AppDisks、およびサポートされていないホストの削除」を参照してください。

- Citrixは、ライセンスコンプライアンスを含む正当な利益のために、必要に応じて基本的なライセンスデータを収集します。詳細については、「Citrixライセンスデータ」を参照してください。

はじめに

この記事は、Windowsオペレーティングシステムを搭載したマシンへのコンポーネントのインストールに適用されます。Linuxオペレーティングシステム用VDAについては、「Linux Virtual Delivery Agents」を参照してください。

この記事では、製品インストールコマンドの発行方法について説明します。インストールを開始する前に、「Prepare to install」を確認してください。この記事には、利用可能なインストーラーの説明が含まれています。

コマンド実行の進行状況と戻り値を確認するには、元の管理者であるか、**管理者として実行**を使用する必要があります。詳しくは、Microsoftのコマンドに関するドキュメントを参照してください。

インストールコマンドを直接使用することに加えて、Active Directory内のマシンにVDAをインストール、アップグレード、または削除するサンプルスクリプトが製品ISOで提供されています。詳しくは、「Install VDAs using scripts」を参照してください。

このCitrix Virtual Apps and Desktopsのバージョンでサポートされていないバージョンにインストールまたはアップグレードしようとすると、オプションに関する情報を示すメッセージが表示されます。「以前のオペレーティングシステム」を参照してください。

Citrixがコンポーネントインストールの結果を報告する方法については、「Citrix installation return codes」を参照してください。

フル製品インストーラーを使用する

フル製品インストーラーのコマンドラインインターフェイスにアクセスするには：

1. Citrixから製品パッケージをダウンロードします。ダウンロードサイトにアクセスするには、Citrixアカウントの資格情報が必要です。
2. ファイルを解凍します。必要に応じて、ISOファイルをDVDに書き込みます。
3. コンポーネントをインストールするサーバーに、ローカル管理者アカウントを使用してログオンします。
4. DVDをドライブに挿入するか、ISOファイルをマウントします。
5. メディアの`\x64\XenDesktop Setup`ディレクトリから、適切なコマンドを実行します。

コアコンポーネントをインストールするには： コアコンポーネントをインストールするためのコマンドラインオプションに記載されているオプションを使用して、`XenDesktopServerSetup.exe` を実行します。

VDAをインストールするには： VDAをインストールするためのコマンドラインオプションに記載されているオプションを使用して、`XenDesktopVDASetup.exe` を実行します。

StoreFrontをインストールするには： インストールメディアの `x64 > StoreFront` フォルダーで `CitrixStoreFront-x64.exe` を実行します。

Universal Print Serverをインストールするには： Universal Print Serverをインストールするためのコマンドラインオプションのガイダンスに従ってください。

Federated Authentication Serviceをインストールするには: Citrixでは、グラフィカルインターフェイスを使用することをお勧めします。

Session Recordingをインストールするには： Session Recordingのガイダンスに従ってください。

Workspace Environment Managementをインストールするには： Workspace Environment Managementのガイダンスに従ってください。

Secure Private Accessをインストールするには： インストールメディアの `x64 > XenDesktop` Setupフォルダーで `XenDesktopSPASetup.exe` を実行します。Secure Private Accessをインストールするためのコマンドラインオプションのガイダンスに従ってください。

コアコンポーネントのインストール用コマンドラインオプション

`XenDesktopServerSetup.exe` コマンドを使用してコアコンポーネントをインストールする場合、以下のパラメーターオプションが有効です。オプションの詳細については、コアコンポーネントのインストールを参照してください。

> **注:**
>
> - コアコンポーネントをインストールするためのコマンドラインオプションを使用している間は、`/exclude` を使用しないでください。
> - `/components` を使用して1つのコンポーネントをアップグレードすると、他のコンポーネントもアップグレードされる可能性があります。これは、異なるコンポーネント間の互換性の問題を回避するためです。

- 1つのコンポーネントのみをアップグレードしたい場合は、そのコンポーネントの個別のインストーラーを使用してください。「展開のアップグレード」(/ja-jp/citrix-virtual-apps-desktops/2511/upgrade-migrate/upgrade.html) を参照してください。

- **/ceipoptin** *ceipoptin* など.

  Call Home データとカスタマーエクスペリエンス向上プログラム (CEIP) データの収集を有効にします。有効な値は次のとおりです。

  - `DIAGNOSTIC`: Citrix Licensing が Call Home データを収集できるようにするには、この値を選択します。
  - `ANONYMOUS`: Citrix Licensing が未識別の CEIP データ (ユーザーを特定しないデータ) を収集できるようにするには、この値を選択します。
  - `NONE`: Citrix Licensing による CEIP データの収集を無効にするには、この値を選択します。

  Call Home データ収集の詳細については、「Citrix Licensing Call Home」を参照してください。

  CEIP データ収集の詳細については、「Citrix Licensing Customer Experience Improvement Program」を参照してください。

  CEIPデータについて詳しくは、「Citrix Licensing CEIPデータ要素」(/ja-jp/licensing/current-release/license-server/licensing-data-collection-programs.html#citrix-licensing-ceip-data-elements) を参照してください。

  License Serverのライセンスデータについて詳しくは、「Citrix Licensing Data」(/ja-jp/licensing/current-release/license-server/licensing-data-collection-programs.html#citrix-licensing-compliance) を参照してください。

- **/components** *コンポーネント* ...

  インストールまたは削除するコンポーネントのコンマ区切りリスト。有効な値は次のとおりです。

  - `CONTROLLER`: コントローラー
  - `WEBSTUDIO`: スタジオ
  - `DESKTOPDIRECTOR`：ディレクター
  - `LICENSESERVER`：Citrixライセンスサーバー

- `SECUREPRIVATEACCESS`：セキュアプライベートアクセス

VDAのみをインストールし、他のCitrixコンポーネントのインストールを除外するには、/components vda を指定します。

このオプションは、VDAWorkstationCoreSetup_xxxx.exe インストーラーを使用する場合は無効です。そのインストーラーでは、Citrix Workspaceアプリやその他のCitrixコンポーネントをインストールできません。

このオプションを省略すると、すべてのコンポーネントがインストールされます（`/remove` オプションも指定されている場合は、削除されます）。

（2003より前のリリースでは、有効な値に `STOREFRONT™` が含まれていました。バージョン2003以降では、Use the full-product installer に記載されている専用のStoreFrontインストールコマンドを使用してください）。

- **前提条件のみ**

  選択したコンポーネントの前提条件のみがインストールされます。Citrix製品コンポーネントはインストールされません。

- **/configure_firewall**

  Windowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても、インストールされるコンポーネントが使用するWindowsファイアウォールのすべてのポートを開きます。サードパーティのファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ポートを手動で開く必要があります。

- **エクスペリエンスメトリックを無効にする**

  インストール、アップグレード、または削除中に収集された分析データがCitrixに自動的にアップロードされるのを防ぎます。

- **/help** または **/h**

  コマンドのヘルプを表示します。

- **/ignore_hw_check_failure**

  ハードウェアチェックが失敗した場合でも (たとえば、RAM 不足のため)、Delivery Controllerのインストールまたはアップグレードを続行できるようにします。詳細については、「ハードウェアチェック」を参照してください。

- **/ignore_site_test_failure**

Controller のアップグレード中にのみ有効です。通常、サイトテストの失敗は無視され、アップグレードは続行されます。省略された場合 (または false に設定された場合)、サイトテストの失敗があると、アップグレードを実行せずにインストーラーが失敗します。デフォルト = false

アップグレード中に、サポートされていない SQL Server バージョンが検出された場合、このオプションは無視されます。詳細については、「SQL Server バージョンチェック」を参照してください。

- **/インストールディレクトリ** *ディレクトリ*

  コンポーネントがインストールされる既存の空のディレクトリ。デフォルト = `c:\Program Files\Citrix`。

- **/ログパス** *パス*

  ログファイルの場所。指定されたフォルダーは存在している必要があります。インストーラーは作成しません。デフォルト = `TEMP%\Citrix\XenDesktop Installer`

- **/no_remote_assistance**

  Director のインストール時にのみ有効です。Windows リモートアシスタンスを使用するユーザーシャドウイング機能を無効にします。

- **再起動なし**

  インストール後の再起動を防止します。(ほとんどのコアコンポーネントでは、再起動はデフォルトで有効になっていません。)

- **再開しない**

  デフォルトでは、インストール中にマシンの再起動が必要な場合、再起動が完了するとインストーラーは自動的に再開します。デフォルトを上書きするには、`/noresume` を指定します。これは、メディアを再マウントする必要がある場合や、自動インストール中に情報を取得したい場合に役立ちます。

- **ノースキューエル**

  Controller をインストールするサーバーへの Microsoft SQL Server Express のインストールを防止します。このオプションを省略すると、サイトデータベースとして使用するために SQL Server Express がインストールされます。

  このオプションは、ローカルホストキャッシュに使用される SQL Server Express LocalDB のインストールには影響しません。

- **サイレント** または **パッシブ**

インストール中にユーザーインターフェイスは表示されません。インストールプロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **リムーブ**

  `/components`オプションで指定されたコアコンポーネントを削除します。

- **リムーブオール**

  インストールされているすべてのコアコンポーネントを削除します。

- **センドエクスペリエンスメトリクス**

  インストール、アップグレード、または削除中に収集された分析データをCitrixに自動的に送信します。このオプションを省略した場合（または`/disableexperiencemetrics`が指定された場合）、分析データはローカルで収集されますが、自動的には送信されません。

- **テンプディール** *directory*

  インストール中に一時ファイルを保持するディレクトリ。デフォルト = `c:\Windows\Temp`。

- **ゼナップ**

  Citrix Virtual Apps をインストールします。このオプションを省略すると、Citrix Virtual Apps and Desktops™ がインストールされます。

コアコンポーネントのインストール例

次のコマンドは、Delivery Controller™、Studio、Citrix Licensing、およびSQL Server Expressをサーバーにインストールします。コンポーネント通信に必要なファイアウォールポートは自動的に開かれます。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,webstudio,licenseserver /configure_firewall
```

次のコマンドは、Citrix Virtual Apps™ Controller、Studio、およびSQL Server Expressをサーバーにインストールします。コンポーネント通信に必要なファイアウォールポートは自動的に開かれます。

```
\x64\XenDesktop Setup\\XenDesktopServerSetup.exe /xenapp /components controller,webstudio /configure_firewall
```

次のコマンドは、Delivery Controller、Secure Private Access、およびSQL Server Expressをサーバーにインストールします。コンポーネント通信に必要なファイアウォールポートは自動的に開かれます。

`\x64\XenDesktop Setup XenDesktopServerSetup.exe /xenapp /components controller,secureprivateaccess /configure_firewall`

Citrix Virtual Apps and Desktopsバージョン2407から2411以降にアップグレードする場合、またはバージョン2411以降を新規インストールする場合は、最初にLicense Serverを最新バージョン（バージョン11.2.17ビルド51000）に更新してください。その後、Delivery Controllerをアップグレードします。これを怠ると、コマンドラインによるインストールおよびアップグレードが失敗します。License Serverと、Delivery Controller、Studio、Citrix Directorなどのコンポーネントをアップグレードするには、次のコマンドを実行します（マウントされたISOの\x64フォルダー内にいることを前提とします）。

1. 次を実行します。

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet
   ```

   ライセンスバイナリをローカルドライブのいずれかにコピーした場合は、次のコマンドを実行します。

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet /l install.log
   ```

2. 次を実行します。

   ```
   \x64\XenDesktop Setup\XenDesktopServerSetup.exe  /components "CONTROLLER,WEBSTUDIO,DESKTOPDIRECTOR" /CONFIGURE_FIREWALL
   ```

スタンドアロンVDAインストーラーを使用する

ダウンロードサイトにアクセスするには、Citrixアカウントの資格情報が必要です。インストールを開始する前に、管理者特権を昇格させるか、**管理者として実行**を使用する必要があります。

1. Citrixから適切なパッケージをダウンロードします。

   - マルチセッションOS Virtual Delivery Agent: `VDAServerSetup_xxxx.exe`
   - シングルセッションOS Virtual Delivery Agent: `VDAWorkstationSetup_xxxx.exe`
   - シングルセッションOSコアサービス Virtual Delivery Agent: `VDAWorkstationCoreSetup_xxxx.exe`

2. まずパッケージから既存のディレクトリにファイルを抽出し、インストールコマンドを実行するか、単にパッケージを実行します。

ファイルをインストールする前に抽出するには、絶対パスを指定して`/extract`を使用します。例: `C:\YourExtractFolder\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`。ディレクトリは存在している必要があります。存在しない場合、抽出は失敗します。その後、別のコマンドで、この記事に記載されている有効なオプションを使用して、適切なコマンドを実行します。

- `VDAServerSetup_XXXX.exe`の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`を実行します
- `VDAWorkstationCoreSetup_XXXX.exe`の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe`を実行します
- `VDAWorkstationSetup_XXXX.exe`の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`を実行します

ダウンロードしたパッケージを実行するには、その名前（`VDAServerSetup.exe`、`VDAWorkstationSetup.exe`、または`VDAWorkstationCoreSetup.exe`）を実行します。この記事に記載されている有効なオプションを使用してください。

フル製品インストーラーに慣れている場合：

- スタンドアロンの`VDAServerSetup.exe`または`VDAWorkstationSetup.exe`インストーラーを、名前以外は`XenDesktopVdaSetup.exe`コマンドであるかのように実行します。
- `VDAWorkstationCoreSetup.exe`インストーラーは、他のインストーラーで利用できるオプションのサブセットをサポートしているため、異なります。

インストールまたは削除するコンポーネントのコンマ区切りリスト。有効な値は次のとおりです。

- `VDA`: バーチャル デリバリー エージェント
- `CSA`: Citrix Secure Access™ クライアント
- `PLUGINS`: Windows用Citrix Workspace™アプリ
- `UPL`: Citrixユーザーパーソナライゼーションレイヤー (WS VDA のみ)
- `SRAGENT`: セッションレコーディングエージェント
- `ASSISTANTAPP`: Citrix アシスタント アプリ (WS VDA のみ)
- `CEAL`: Citrix エラスティック アプリ レイヤリング (TS VDA のみ)

VDAとCitrix Workspaceアプリ for Windowsをインストールするには、/components vda,pluginsを指定するか、コンポーネントをまったく指定しないでください。

このバージョン以降、Citrix Device Trust、Citrix uberAgent、およびCitrix Workspace Environment Management™ (WEM) Agentは、デフォルトのVDAインストールに統合されています。これらのコンポーネントはVDAセットアップの一部としてサイレントインストールされ、個別のコンポーネントとして管理されなくなりました。

> **注:**
>
> 環境内でCitrix uberAgent®の既存のスタンドアロンバージョンが検出された場合、インストーラーによってインストール、アップグレード、またはアンインストールされることはありません。

> VDAのみをインストールし、他のCitrixコンポーネントのインストールを除外するには、`/components vda`を指定します。

このオプションは、VDAWorkstationCoreSetup_xxxx.exeインストーラーを使用する場合は無効です。このインストーラーは、Citrix Workspaceアプリやその他のCitrixコンポーネントをインストールできません。

VDA をインストールするためのコマンドラインオプション

以下のオプションは、次のコマンド（インストーラー）のいずれか、または複数で有効です: `VDAServerSetup_xxxx.exe`、`VDAWorkstationSetup_xxxx.exe`、および `VDAWorkstationCoreSetup_xxxx.exe`。

オプションの詳細については、「VDAのインストール」を参照してください。

- **/コンポーネント** *コンポーネント*\[,*コンポーネント*\]

  インストールまたは削除するコンポーネントのコンマ区切りリスト。有効な値は次のとおりです。

  - `VDA`: 仮想配信エージェント
  - `PLUGINS`: Windows向けCitrix Workspaceアプリ
  - `CSA`: Citrix セキュアアクセス クライアント
  - `UPL`: Citrix ユーザーパーソナライゼーション レイヤー (WS VDA のみ)
  - `SRAGENT`: セッションレコーディングエージェント
  - `ASSISTANTAPP`: Citrix アシスタント アプリ (WS VDA のみ)
  - `CEAL`: Citrix エラスティック アプリ レイヤリング (TS VDA のみ)

VDAとWindows向けCitrix Workspaceアプリをインストールするには、`/components vda, plugins, CSA, UPL`を指定するか、コンポーネントをまったく指定しないでください。コンポーネントが指定されていない場合、デフォルトではVDA、SRAGENT、およびASSISTANTAPPのみがインストールされます。

VDAのみをインストールし、Citrix Workspaceアプリやその他のコンポーネントのインストールを除外するには、`/components vda`を指定します。

このオプションは、`VDAWorkstationCoreSetup_xxxx.exe`インストーラーを使用している場合は無効です。そのインストーラーではCitrix Workspaceアプリをインストールできません。

- **/onlyprereqs** (前提条件のみ)

  選択したコンポーネントの前提条件のみがインストールされます。Citrix 製品コンポーネントはインストールされません。

- **/controllers** "*controller* \[*controller*\]" (コントローラー)

  VDAが通信できるコントローラーのFQDNをスペースで区切り、半角の引用符で囲みます。`/site_guid`と`/controllers`の両方のオプションを指定しないでください。

- **/disableexperiencemetrics** (エクスペリエンスメトリックを無効にする)

  インストール、アップグレード、または削除中に収集された分析がCitrixに自動的にアップロードされるのを防ぎます。

- **/enable_hdx_ports**

  Windowsファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、VDAおよび有効な機能（Windowsリモートアシスタンスを除く）に必要なポートをWindowsファイアウォールで開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、「ネットワークポート」を参照してください。

  HDXアダプティブトランスポートが使用するUDPポートを開くには、この`/enable_hdx_ports`オプションに加えて、`/enable_hdx_udp_ports`オプションを指定します。

- **/enable_hdx_udp_ports**

  Windowsファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、HDXアダプティブトランスポートが使用するUDPポートをWindowsファイアウォールで開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用して

いない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、「ネットワークポート」を参照してください。

VDAが使用する追加のポートを開くには、この`/enable_hdx_udp_ports`オプションに加えて、`/enable_hdx_ports`オプションを指定します。

- **/enable_hdx_tls_dtls**

  HDX™ Direct V1用にTCPおよびUDPポート443を開きます。

- **/enable_real_time_transport**

  オーディオパケットにUDPを使用するかどうかを有効または無効にします（オーディオ用のRealTime Audio Transport）。この機能を有効にすると、オーディオパフォーマンスが向上する可能性があります。Windowsファイアウォールサービスが検出されたときにUDPポートを自動的に開く場合は、`/enable_hdx_ports`オプションを含めます。

- **/enable_remote_assistance**

  Directorで使用するためのWindowsリモートアシスタンスのシャドウイング機能を有効にします。このオプションを指定すると、Windowsリモートアシスタンスはファイアウォールで動的ポートを開きます。

- **/enablerestore** または **/enablerestorecleanup**

  （シングルセッションVDAのみ有効）VDAのインストールまたはアップグレードが失敗した場合に、復元ポイントへの自動復帰を有効にします。

  インストール/アップグレードが正常に完了した場合：

  - `/enablerestorecleanup`は、インストーラーに復元ポイントを削除するよう指示します。
  - `/enablerestore`は、使用されなかった場合でも、インストーラーに復元ポイントを保持するように指示します。

  詳細については、インストールまたはアップグレードの失敗時の復元を参照してください。

- **/ENABLE_SECURE_DEFAULTS**

  より安全な初期設定のために、さまざまな機能のデフォルト設定を有効から無効に変更します。関連する機能は次のとおりです: クライアントドライブリダイレクト、特殊フォルダーリダイレクト、ドラッグアンドドロップ、クライアントTWAINデバイスリダイレクト、クライアントUSBプラグアンドプレイデバイスリダイレクト、クライアントプリンターリダイレクト、クライアントクリップボードリダイレクト、クライアントマイク入力リダイレクト。

- **/enable_ss_ports**

  Windows ファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、画面共有に必要なポートをWindows ファイアウォールで開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、手動でファイアウォールを構成する必要があります。

- **/SKIPHDXDRIVERCHECK**

  VDAメタインストーラーへのHDX™ドライバーのチェックをスキップします。

- **/exclude** "*コンポーネント*"\[,"*コンポーネント*"\]

  1つまたは複数のコンマ区切りのオプションコンポーネント（それぞれを引用符で囲む）のインストールを防止します。たとえば、MCSによって管理されていないイメージにVDAをインストールまたはアップグレードする場合、Machine Identity Serviceコンポーネントは必要ありません。有効な値は次のとおりです。

マルチセッションOS	シングルセッションOS	シングルセッションOSコアサービス
`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`
`Citrix Backup and Restore`	`Citrix Backup and Restore`	`Citrix Browser Content Redirection`
`Citrix deviceTRUST®`	`Citrix deviceTRUST`	`Citrix deviceTRUST`
`uberAgent®`	`uberAgent`	`uberAgent`
`Citrix Secure Access Client`	`Citrix Secure Access Client`	`Citrix Secure Access Client`
`Citrix Workspace Environment Management™ Agent`	`Citrix Workspace Environment Management Agent`	`Citrix Workspace Environment Management Agent`
`Citrix Browser Content Redirection`	`Citrix Browser Content Redirection`	`Citrix Personalization for App-V - VDA`
`Citrix MCS IODriver`	`Citrix MCS IODriver`	`Citrix Telemetry Service`

マルチセッションOS	シングルセッションOS	シングルセッションOSコアサービス
Citrix Personalization for App-V - VDA	Citrix Personalization for App-V - VDA	Citrix Universal™ Print Client
Citrix Profile Management	Citrix Profile Management	Citrix Vda Log Capture Service
Citrix Profile Management WMI Plug-in	Citrix Profile Management WMI Plug-in	CSE Component
Citrix Rendezvous V2	Citrix Rendezvous V2	Director VDA Plug-in
Citrix Telemetry Service	Citrix Telemetry Service	Machine Management Provider
Citrix Universal Print Client	Citrix Universal Print Client	VDA Monitor Plug-in
Citrix Vda Log Capture Service	Citrix Vda Log Capture Service	VDA WMI Proxy Plug-in
Citrix VDA Upgrade Agent	Citrix VDA Upgrade Agent	
CSE Component	CSE Component	
Director VDA Plug-in	Director VDA Plug-in	
Machine Identity Service	Machine Identity Service	
Machine Management Provider	Machine Management Provider	
VDA Monitor Plug-in	User Personalization Layer	
VDA WMI Proxy Plug-in	VDA Monitor Plug-in	
	VDA WMI Proxy Plug-in	

マルチセッションOS	シングルセッションOS	シングルセッションOSコアサービス
`Citrix App Protection Component`	`Citrix App Protection Component`	`Citrix App Protection Component`
`Citrix HyperV Filter Driver`	`Citrix HyperV Filter Driver`	
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`
`Session Recording Agent`	`Session Recording Agent`	
`Elastic App Layering`	`Citrix Assistant App`	

Citrix Profile Management をインストールから除外する（`/exclude "Citrix Profile Management"`）と、Citrix Director を使用した VDA の監視とトラブルシューティングに影響します。「**ユーザーの詳細**」ページと「**エンドポイント**」ページでは、「パーソナライズ」パネルと「ログオン時間」パネルが失敗します。「**ダッシュボード**」ページと「**傾向**」ページでは、「平均ログオン時間」パネルに、Profile Management がインストールされているマシンに関するデータのみが表示されます。

サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrix Profile Management Service をインストールして実行することをお勧めします。Citrix Profile Management Service を有効にする必要はありません。

`/exclude` と `/includeadditional` の両方を同じコンポーネント名で指定した場合、そのコンポーネントはインストールされません。

`VDAWorkstationCoreSetup.exe`インストーラーを使用する場合、このオプションは無効です。そのインストーラーは、これらの項目の多くを自動的に除外します。

- **/h** または **/help**

  コマンドのヘルプを表示します。

- **/includeadditional** "*コンポーネント*"\[,"*コンポーネント*"\]

  1つまたは複数のコンマ区切りのオプションコンポーネント（それぞれが引用符で囲まれている）のインストールを含めます。このオプションは、Remote PC Access展開を作成してい

て、デフォルトで含まれていない他のコンポーネントをインストールしたい場合に役立ちます。有効な値は次のとおりです。

マルチセッションOS	シングルセッションOS
`Citrix Backup and Restore`	`Citrix Backup and Restore`
`Citrix MCS IODriver`	`Citrix MCS IODriver`
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`
`Citrix Profile Management`	`Citrix Profile Management`
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`
`Citrix Rendezvous V2`	`Citrix Rendezvous V2`
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`
`Citrix Web Socket Vda Registration Tool`	`Citrix Web Socket Vda Registration Tool`
`Machine Identity Service`	`Machine Identity Service`
	`User Personalization Layer`

同じコンポーネント名で`/exclude`と`/includeadditional`の両方を指定した場合、そのコンポーネントはインストールされません。

- **/installdir** *ディレクトリ*

  コンポーネントがインストールされる既存の空のディレクトリ。デフォルト = `c:\Program Files\Citrix`。

- **/install_mcsio_driver**

  使用しないでください。代わりに`/includeadditional "Citrix MCS IODriver"`または`/exclude "Citrix MCS IODriver"`を使用してください。

- **/logpath** *パス*

ログファイルの場所。指定されたフォルダーが存在している必要があります。インストーラーは作成しません。デフォルト = "%TEMP%\\Citrix\\XenDesktop Installer"

このオプションはグラフィカルインターフェイスでは利用できません。

- **/マスターイメージ**

  VM に VDA をインストールする場合にのみ有効です。VDA を、他のマシンを作成するために使用されるイメージとして設定します。このオプションは `/mastermcsimage` と同等です。

  `VDAWorkstationCoreSetup_xxxx.exe` インストーラーを使用する場合、このオプションは無効です。

- **/マスターMCSイメージ**

  このマシンがMachine Creation Servicesでイメージとして使用されることを指定します。このオプションは`/masterimage`と同等です。

- **/マスターPVSイメージ**

  このマシンが、Citrix Provisioning™ またはサードパーティのプロビジョニングツール（Microsoft System Center Configuration Manager など）を使用して VM をプロビジョニングするためのイメージとして使用されることを指定します。

- **/websockettoken** *WebSocket トークン*

  Web Socket VDAを作成します。WebSocketTokenは、必要なトークン用です。

- **/websockettokenfile** *WebSock トークンを含むファイル*

  Web Socket VDA を作成します。*WebSock トークンを含むファイル* は、必要なトークンを含むファイル用です。

- **/websockettokenstdin** <*WebSocket トークン*

  Web Socket VDA を作成します。<*WebSocketToken* は、STDIN によって渡される必須のトークン用です。

- **/no_mediafoundation_ack**

  Microsoft Media Foundation がインストールされていないこと、およびいくつかの HDX マルチメディア機能がインストールされず、動作しないことを確認します。このオプションを省略し、Media Foundation がインストールされていない場合、前提条件が満たされていないため、VDA のインストールは終了します。ほとんどのサポートされている Windows エディションには、N エディションを除き、Media Foundation がすでにインストールされています。Windows の機能 > メディア機能を *手動* で有効にした場合、Citrix Meta Installer が探すレジス

トリキーに値が設定されていない可能性があります。インストールプロセスを開始する前に、`SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\Windows-Features\WindowsMediaVersion` レジストリキーをチェックして、値が存在し、空でないことを確認してください。

- **デスクトップエクスペリエンスなし**

  拡張デスクトップエクスペリエンス機能は利用できなくなりました。このオプション（およびポリシー設定）は、指定されても無視されます。

  マルチセッション OS 用の VDA をインストールする場合にのみ有効です。拡張デスクトップエクスペリエンス機能の有効化を防止します。この機能は、拡張デスクトップエクスペリエンス Citrix ポリシー設定でも制御されます。

- **再起動なし**

  インストール後の再起動を防止します。VDA は再起動後まで使用できません。

- **再開なし**

  デフォルトでは、インストール中にマシンの再起動が必要な場合、再起動が完了するとインストーラーは自動的に再開します。デフォルトを上書きするには、`/noresume` を指定します。これは、メディアを再マウントする必要がある場合や、自動インストール中に情報を取得したい場合に役立ちます。

- **物理マシン**

  RemotePC インストールの場合、この引数を `/remotepc` とともに使用します。そうしないと、特定のユーザーシナリオで VDA が期待どおりに動作しない可能性があります。

- **/portnumber** *ポート*

  `/reconfig` オプションが指定されている場合にのみ有効です。VDA と Controller 間の通信を有効にするポート番号です。以前に構成されたポートは、ポート 80 でない限り無効になります。

- **/proxyconfig** 「*アドレスまたはPACファイルのパス*」

  環境内でGateway Serviceなどのサービスと Rendezvous V2プロトコルを使用する予定があり、アウトバウンド接続用にネットワークに非透過プロキシがある場合は、ここでプロキシを指定します。HTTPプロキシのみがサポートされています。Rendezvousプロトコルで使用するプロキシのアドレスまたはPACファイルのパス。このコマンドラインは、/includeadditional "Citrix Rendezvous V2"が使用されたかのように、Citrix Rendezvous V2を自動的にインストー

ルします。機能の詳細については、「Rendezvousプロトコル」(/ja-jp/citrix-daas/hdx/rendezvous-protocol.html)を参照してください。

  - プロキシアドレスの形式: `http://<url-or-ip>:<port>`
  - PACファイルの形式: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **サイレント** または **パッシブ**

  インストール中にユーザーインターフェイスは表示されません。インストールと構成プロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **/再構成**

  `/portnumber`、`/controllers`、または`/enable_hdx_ports`オプションと組み合わせて使用すると、以前に構成されたVDA設定をカスタマイズします。このオプションを`/quiet`オプションも指定せずに指定すると、VDAをカスタマイズするためのグラフィカルインターフェイスが起動します。

- **/リモートPC**

  Remote PC Access展開（シングルセッションOS）またはブローカー接続（マルチセッションOS）の場合にのみ有効です。追加コンポーネントのインストールを除外します（`/exclude`および`/includeadditional`オプションのコンポーネントリストを参照）。

  このオプションは、`VDAWorkstationCoreSetup.exe`インストーラーを使用する場合は無効です。そのインストーラーは、これらのコンポーネントのインストールを自動的に除外します。

  `/remotepc` は `/servervdi` オプションと互換性がありません。

- **/削除**

  `/components`オプションで指定されたコンポーネントを削除します。

- **/remove_appdisk_ack**

  AppDisks™ VDAプラグインがインストールされている場合、VDAインストーラーがそれをアンインストールすることを承認します。

- **/remove_pvd_ack**

  Personal vDiskがインストールされている場合、VDAインストーラーがそれをアンインストールすることを承認します。

- **/すべて削除**

VDAを削除します。Citrix Workspaceアプリ（インストールされている場合）は削除しません。

- **/REMOVEALLWITHCWA**

  VDA とともに CWA を削除します。

- **/エクスペリエンスメトリックを送信**

  インストール、アップグレード、または削除中に収集された分析データをCitrixに自動的に送信します。このオプションが省略されている場合（または`/disableexperiencemetrics`オプションが指定されている場合）、分析データはローカルで収集されますが、自動的には送信されません。

- **サーバーVDI**

  サポートされているWindowsマルチセッションマシンにシングルセッションOS用VDAをインストールします。Windowsマルチセッションマシンにマルチセッション OS用VDAをインストールする場合は、このオプションを省略してください。

  このオプションを使用する前に、「Server VDI」を参照してください。

  このオプションは、フルプロダクトVDAインストーラーでのみ使用してください。

- **/サイト_GUID** *GUID*

  サイトのActive Directory組織単位（OU）のグローバル一意識別子。これは、Active Directoryを検出（自動更新が推奨されるデフォルトの検出方法です）に使用している場合に、仮想デスクトップをサイトに関連付けます。サイトGUIDは、Studioに表示されるサイトプロパティです。`/site_guid`オプションと`/controllers`オプションの両方を指定しないでください。

- **一時ディレクトリ** *directory*

  インストール中に一時ファイルを保持するディレクトリ。デフォルト = `c:\Windows\Temp`。

  このオプションはグラフィカルインターフェイスでは利用できません。

- **仮想マシン**

  VMにVDAをインストールする場合にのみ有効です。VMに渡されるBIOS情報により、VMが物理マシンとして表示される場合に、インストーラーによる物理マシンの検出を上書きします。

  このオプションはグラフィカルインターフェイスでは利用できません。

- **/ゼノデスクトップクラウド**

  VDAがCitrix DaaS (Citrix Cloud™) 展開にインストールされていることを示します。

VDAインストールの例

フルプロダクトインストーラーでVDAをインストールする:

次のコマンドは、シングルセッションOSおよびCitrix Workspaceアプリ用のVDAを、VM上のデフォルトの場所にインストールします。このVDAはイメージとして使用され、MCSを使用してVMをプロビジョニングします。VDAは、`mydomain` ドメイン内の `Contr-Main` という名前のサーバー上のControllerに最初に登録されます。VDAはユーザーパーソナライゼーションレイヤーとWindowsリモートアシスタンスを使用します。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins /
controllers "Contr-Main.mydomain.local" /enable_hdx_ports /includeadditional
"user personalization layer" /mastermcsimage /enable_remote_assistance
```

VDAWorkstationCoreSetupスタンドアロンインストーラーでシングルセッションOS VDAをインストールする:

次のコマンドは、リモートPCアクセスまたはVDI展開で使用するために、シングルセッションOSにコアサービスVDAをインストールします。Citrix Workspaceアプリおよびその他の非コアサービスはインストールされません。Controllerのアドレスが指定され、Windowsファイアウォールサービス内のポートは自動的に開かれます。管理者が再起動を処理します。

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.com" /
enable_hdx_ports /noreboot
```

VDAをカスタマイズする

VDAをインストールした後、いくつかの設定をカスタマイズできます。製品メディアの `\x64\XenDesktop Setup` ディレクトリから、VDAのインストール用コマンドラインオプションで説明されている以下のオプションを1つ以上使用して、`XenDesktopVdaSetup.exe` を実行します。

- `/reconfigure` (VDAをカスタマイズする際に必須)
- `/h` または `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

VDAのトラブルシューティング

- デリバリーグループのStudio表示で、**詳細**ペインの**インストール済みVDAバージョン**エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンのWindowsのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされても、Delivery Controllerに登録されるまでは、ユーザーにアプリやデスクトップを配信できません。

  VDAの登録方法と登録の問題のトラブルシューティングについては、「VDA登録」を参照してください。

Universal Print Serverをインストールするためのコマンドラインオプション

次のオプションは、`XenDesktopPrintServerSetup.exe`コマンドで有効です。

- **/enable_upsserver_port**

このオプションが指定されていない場合、インストーラーはグラフィカルインターフェイスから**ファイアウォール**ページを表示します。インストーラーにWindowsファイアウォール規則を自動的に追加させるには**自動**を選択し、管理者が手動でファイアウォールを構成する場合は**手動**を選択します。

プリントサーバーにソフトウェアをインストールした後、Citrix Universal Print Server (UPS)のガイダンスに従ってUniversal Print Serverを構成します。

Secure Private Accessをインストールするためのコマンドラインオプション

次のオプションは両方で有効です:

1. CVADインストーラー: `XenDesktopSPASetup.exe`
2. SPAオンプレミスインストーラー: `SecurePrivateAccessSetup_XXXX.exe`

- **/enable_spa_ports**

  Windowsファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、Secure Private Accessに必要なWindowsファイアウォールのポートを開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、「ネットワークポート」を参照してください。

- **/SQLなし**

Secure Private Accessをインストールするサーバーへの Microsoft SQL Server Expressのインストールを防止します。このオプションが省略された場合、SQL Server Expressはサイトデータベースとして使用するためにインストールされます。

- **/ヘルプ または /h または /?**

  コマンドのヘルプを表示します

- **/再起動なし**

  インストール後の再起動を防止します。再起動するまでSecure Private Accessは使用できません。

- **/quiet または /passive**

  インストール中にユーザーインターフェイスは表示されません。インストールおよび構成プロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションが省略された場合、グラフィカルインターフェイスが起動します。

- **/削除**

  Secure Private Accessを削除します。

オプションの詳細については、Secure Private Access インストーラーを参照してください。

詳細情報

Citrix がコンポーネントインストールの結果を報告する方法については、Citrix インストールリターンコードを参照してください。

Web Studio をインストールする

> **注:**
>
> Citrix Studio (MMC Studio) はバージョン 2511 以降で削除され、サポートされなくなりました。この記事では、Web Studio が唯一使用される管理コンソールであることを前提としています。

はじめに

Web Studio は、Citrix Studio と完全に同等の機能を備えた Web ベースの管理コンソールです。Citrix DaaS Studio インターフェイス と同じルックアンドフィールで、ネイティブな Web エクスペリエンスを提供することで、管理エクスペリエンスを最新化します。

Web Studio は、Internet Information Service (IIS) がインストールされている任意の Windows サーバーに展開できます。展開オプションは次の2つです。

- 専用サーバーにインストールする:

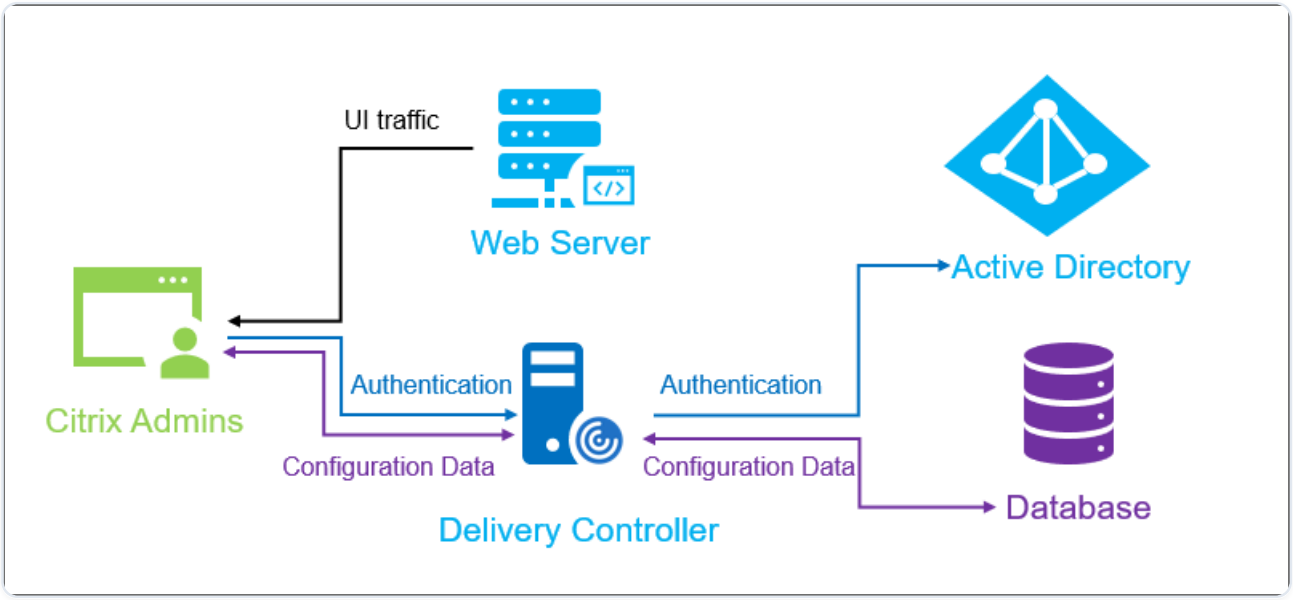
  パフォーマンスとスケーラビリティが重要となる大規模な環境では、Web Studio を専用サーバーにインストールすることをお勧めします。このサーバーは、オプションで Director もホストできます。

- Delivery Controller™ と統合する:

  迅速な展開やシンプルな環境では、Web Studio を Delivery Controller に直接インストールします。このアプローチは、管理オーバーヘッドを最小限に抑えることが優先される小規模な展開に最適です。

次の図は、Web Studio のアーキテクチャを示しています。

Web Studio のアーキテクチャ



Web Studio を起動して実行するための一般的なワークフローは次のとおりです。

1. (#install-web-studio-1)。
2. (#set-up-a-site)。
3. (#add-delivery-controllers-to-web-studio-for-management)。
4. (オプション) Delivery Controller のプロキシとして Web Studio を構成する(#optional-configure-web-studio-as-a-proxy-for-delivery-controllers)
5. 「(オプション) Pendoを無効にする」(#optional-enable-or-disable-pendo)。
6. Web Studioのセキュアなサーバー構成(#secure-server-configuration-for-web-studio)

7. 「Web Studioにサインインする」(#sign-in-to-web-studio)。

負荷分散されたWeb Studio展開をセットアップするには、この記事を参照してください。

Web Studioで利用可能な新機能

新機能の記事を参照してください。

システム要件

以下の表に、Studioのインストールと使用に関するサポート対象のオペレーティングシステム、ブラウザ、表示設定、およびハードウェア要件を示します。

サポートされているオペレーティングシステム

オペレーティングシステム	エディション	SERVER CORE のサポート
ウィンドウズ サーバー 2025	スタンダード、データセンター	はい
ウィンドウズ サーバー 2022	スタンダード、データセンター	はい
ウィンドウズ サーバー 2019	スタンダード、データセンター	はい
ウィンドウズ サーバー 2016	スタンダード、データセンター	はい

サポートされているブラウザー

ブラウザー	サポートされている最小バージョン
マイクロソフト エッジ	92
Firefox ESR (延長サポートリリース)	90
グーグル クローム	92
サファリ	14

表示要件

要件	値
推奨画面解像度	1440 × 1024

ハードウェア要件

リソース	最小要件
メモリ	1 GB RAM
ディスク容量	100 MB

Web Studio のインストール

以下の情報は、コアコンポーネントのインストールのガイダンスを補足するものです。Web Studioをインストールするには：

- Citrix Virtual Apps™ and Desktopsの製品版ISOインストーラーを使用してWeb Studioをインストールします。ISOインストーラーは、前提条件を確認し、不足しているコンポーネントをインストールし、Web Studio Webサイトをセットアップし（Delivery Controllerのインストールに含まれている場合はDelivery Controller上に）、基本的な構成を実行します。
- インストール時にWeb Studioが含まれていなかった場合は、インストーラーを使用してWeb Studioを追加します。
- Web Studioのインストール時に、Delivery ControllerのFQDNを入力するよう求められます。

> **注:**
>
> - 完全に機能させるために、Web StudioとDelivery Controllerを同じバージョンで実行することをお勧めします。
> - 複数のDelivery Controllerを追加できます。Web Studioはランダムな順序でそれらに接続を試みます。Web Studioが接続を試みているDelivery Controllerに到達できない場合、Web Studioは自動的に他のDelivery Controllerにフォールバックします。
> - **コアコンポーネント**でDirectorが選択され、インストールされている場合、ここで追加するDelivery ControllerはWeb StudioとDirectorの両方に使用されます。

- Delivery ControllerがTLS用に構成されている（推奨）場合、入力されたFQDNは、Delivery Controllerにインストールされている証明書の共通名またはサブジェクトの別名と一致する必要があります。
- Web Studioは、サイト名に関係なく、**Site ID = 1**の任意のIIS Webサイトにインストールできます。この機能により、**Default Web Site**の代わりにカスタムIISサイトでWeb Studioをホストできます。
  - ISOインストーラーを実行する前にIISがインストールされていない場合、インストーラーはIISを自動的に構成し、**Default Web Site**（サイトID = 1）の下にWeb Studioを展開します。インストール後、必要に応じてサイト名を変更できます。
  - IISがすでにインストールされている場合、**サイトID**が**1**である限り、希望する名前と物理パスでIISサイトを事前に作成できます。その後、Web Studioはそのサイトの直下にインストールされ、それ以上の構成は必要ありません。

デリバリーコントローラーの追加(/en-us/citrix-virtual-apps-desktops/2511/media/add-delivery-controller.png)

- **完了**ページで、インストールされたコンポーネントを確認し、**完了**をクリックします。

Site Managerの起動(/en-us/citrix-virtual-apps-desktops/2511/media/launch-site-manager.png)

注:

コマンドラインを使用してWeb Studioをインストールすることもできます。例: `.\XenDesktopServerSetup.exe /components webstudio /controllers "ddc1.studio.local" /configure_firewall /quiet`。詳細については、「」(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/install-command.html)を参照してください。

TLS 用の証明書を構成する

デフォルトでは、IISがHTTPS用にまだ構成されていない場合、インストーラーはサーバーのFQDNを証明書の共通名として使用して自己署名証明書を作成し、ポート443にバインドします。この動作により、ユーザーはローカルマシンからWeb Studioにアクセスできますが、他のマシンから接続するユーザーは、証明書が信頼されていないためセキュリティ警告が表示されます。この証明書を、エンタープライズまたは公開認証局 (CA) によって署名された証明書に置き換えることをお勧めします。詳細については、「」(/ja-jp/citrix-virtual-apps-desktops/2511/secure/tls-studio)

を参照してください。IISでTLS証明書がすでに構成されている場合、インストーラーは変更を行いません。

> **注:**
>
> Web Studio展開のセキュリティ保護について詳しくは、「」(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/install-core/install-web-studio/secure-web-studio)を参照してください。

サイトをセットアップする

Citrix Virtual Apps and Desktops展開 (サイトとも呼ばれます) をセットアップするには、Citrix Site Managerツールを使用します。このツールは、Delivery Controllerとともに自動的にインストールされます。

サイトをセットアップするには、次の手順に従います。

1. Delivery Controller で、デスクトップのスタートメニューを開き、**Citrix > Citrix Site Manager** を選択します。
2. Citrix Site Manager で、**Create a site** を選択します。サイトセットアップウィザードが表示されます。
3. サイトを作成し、その設定を次のように構成します。
   - **はじめに**ページで、サイトの名前を入力します。
   - **データベース**ページには、サイト、監視、および構成ログデータベースを設定するための選択肢が含まれています。詳細については、「手順3. データベース」を参照してください。
   - **ライセンス**ページで、ライセンスサーバーのアドレスを指定し、使用する（インストールする）ライセンスを示します。詳細については、「手順4. ライセンス」を参照してください。
4. **Summary** ページで、すべての設定を確認し、**Submit** をクリックします。

   このControllerのIPアドレスは、自動的にサイトに追加されます。

   > **注:**

> サイトを作成したユーザーは、そのサイトの完全な管理者になります。詳細については、「委任管理」を参照してください。

サイトの作成後に新しいControllerをインストールする場合は、そのControllerをサイトに追加する必要があります。詳細な手順は次のとおりです。

1. この新しいControllerでCitrix Site Managerを実行します。
2. **既存のサイトに参加**を選択します。
3. 既にサイトに追加されているControllerのアドレスを入力します。
4. **Submit**をクリックします。

管理のためにDelivery ControllerをWeb Studioに追加する

Studio構成ツールを使用して、管理のためにDelivery ControllerをWeb Studioに追加します。このツールはWeb Studioのインストールフォルダーにあります。

デフォルトでは、このツールは以下のデフォルトフォルダーにインストールされます。

- `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`

Web Studioで管理したいサイトに対して、以下の2つのDelivery Controller (`ddc1.studio.local` および `ddc2.studio.local`) を構成するとします。以下のPowerShellコマンドを実行します。

- `.\StudioConfig.exe --server "ddc1.studio.local,ddc2.studio.local"`

> **注:**
>
> - このツールにはコンピューター管理者権限が必要です。
> - IISサーバーのキャッシュ設定により、Delivery Controllerの構成変更がすぐに反映されない場合があります。すぐに反映させるには、Web Studioサーバーに移動し、インターネットインフォメーションサービス (IIS) マネージャーを開き、*Server_name* > **サイト** > *Web StudioがインストールされているIISサイト名 (サイトID = 1)* に移動して、Webサイトの管理ペインで **再起動** を選択します。
> - 新しいFQDNでDelivery Controllerを再展開する場合、`StudioConfig.exe` を使用してWeb Studioで、および `C:\Program Files\Citrix\Web Studio\Site\assets\json\manifest.json` ファイルでFQDNを更新します。`manifest.json` ファイルを更新しないと、古いFQDNがWeb Studioのサインインウィ

ンドウに表示されたままになります。その結果、サインイン時に新しいFQDNを代替として入力する必要があります。

- サポートされているすべてのパラメーターを表示するには、`StudioConfig.exe --help` を実行します。

(オプション) Web StudioをDelivery Controllerのプロキシとして構成する

デフォルトでは、Web Studioコンソールを使用して展開を管理する場合、Webブラウザーを介してWeb StudioサーバーとDelivery Controllerの両方に接続します。Web StudioサーバーをDelivery Controllerのプロキシとして構成するオプションが提供されています。その結果、展開を管理する際にはWeb Studioサーバーにのみ接続することになります。

このセクションでは、Web StudioサーバーをDelivery Controllerのプロキシとして構成する方法を説明します。Web StudioとDelivery Controllerは異なるサーバーにインストールされていることを前提としています。

開始する前に、展開に必要なすべてのコアコンポーネントがインストールされていることを確認してください。詳細については、「コアコンポーネントのインストール」を参照してください。

Web Studio のプロキシモードを有効にするには、次の手順に従います。

1. Web Studio サーバーで、Windows PowerShell を管理者として実行します。
2. 次のコマンドを実行します。`fqdn_of_webstudio_machine` は Web Studio サーバーの FQDN に置き換えてください。

   ```
   & "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --enableproxy --proxyserver "fqdn_of_webstudio_machine"
   ```

   注：

   ロードバランシングされたWeb Studio展開がある場合は、`fqdn_of_webstudio_machine` をロードバランサーサーバー（仮想サーバーとも呼ばれます）のFQDNに置き換えます。詳細については、「ロードバランシングされたWeb Studio展開のセットアップ」を参照してください。

Web Studioのプロキシモードを無効にするには、このPowerShellコマンドを実行します。

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --
disableproxy
```

(オプション) Pendo を有効または無効にする

バージョン 2411 以降、Web Studio は Pendo を統合しており、これはデフォルトで有効になっています。Pendo は、Citrix プライバシーポリシー に従って使用状況データを収集します。また、Web Studio の右下隅にアイコンを追加し、コンテキストに応じた機能情報とフィードバックオプションを提供します。使用状況データを共有したくない場合は、Studio 構成ツールを使用して Pendo を無効にできます。

このツールは Web Studio のインストールフォルダーにあります。デフォルトでは、ツールは次のフォルダーにインストールされます: `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`。

Pendo を無効にするには、次の手順に従います。

1. Web Studioにサインインします。右下隅にアイコンが表示されている場合、Pendoは有効になっています。
2. Web Studioサーバーで、管理者としてWindows PowerShellを実行します。 このPowerShellコマンドを実行します。

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --
disablependo
```

Pendoを有効にするには、このコマンドを実行します。

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --enablependo
```

Web Studioのセキュアなサーバー構成

セキュリティを強化するために、Web Studio をホストするサーバーに次のセキュリティ構成を適用します。これらの設定は、Web Studio 自体ではなく、サーバーレベルで適用されます。

中程度の強度の SSL 暗号スイート（SWEET32）を無効にする

Web Studio サーバーでは、SWEET32 攻撃に対して脆弱な中程度の強度の暗号スイート `TLS_RSA_WITH_3DES_EDE_CBC_SHA` が使用されている場合があります。 この暗号スイートを無効にするには、Web Studio サーバーで次の PowerShell コマンドを実行します。 `Disable-TlsCipherSuite -Name TLS_RSA_WITH_3DES_EDE_CBC_SHA`

非推奨の TLS 1.0 および 1.1 プロトコルを無効にする

TLS 1.0 と TLS 1.1 は非推奨であり、Web Studio サーバーでは有効にしないでください。 これらを無効にするには、次の手順を実行します。

1. レジストリエディター（`regedit.exe`）を開きます。
2. `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocol` に移動します。
3. 次のサブキーが存在しない場合は、作成します。
   - `TLS 1.0\Client`
   - `TLS 1.0\Server`
   - `TLS 1.1\Client`
   - `TLS 1.1\Server`
4. 各 `Client` キーと `Server` キーに、次の `DWORD (32-bit)` 値を作成します。
   - `Enabled` = `0`
   - `DisabledByDefault` = `1`（省略可能ですが推奨されます）
5. 変更を適用するためにサーバーを再起動します。

Web Studioにサインインする

1. デフォルトのポート番号 443 が使用されている場合は、`https://<address of the server hosting Web Studio>/Citrix/Studio` で Web Studio にアクセスします。別のポートが構成されている 場合は、`https://<address of the server hosting Web Studio>:<port number>/Citrix/Studio` を使用します。

   Web Studio に Delivery Controller を追加 しており、それらに到達可能な場合、サインインページが表示されます。

   > **注:**
   >
   > 次の場合に、**サインインできません** ページが表示されます。
   >
   > - サイトに Delivery Controller が指定されていません。接続するために Delivery Controller を追加するよう求められます。

> - 指定された Delivery Controller に到達できません。接続を確認するには、**テスト** をクリックします。または、代替の Delivery Controller を入力し、**接続** をクリックします。

2. **ユーザー名、パスワード、ドメイン**を入力します。
3. **サインイン**をクリックします。

次のステップ

1. VDAのインストール
2. Web Studioを使用して、次の方法で仮想アプリとデスクトップをユーザーに配信します。
    a. マシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create.html)
    b. デリバリーグループを作成する(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/delivery-groups-create.html)
    c. アプリケーショングループを作成する（オプション）(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/application-groups-create.html)

VDAのインストール

> **重要:**

> - アップグレード中で、現在のバージョンにPersonal vDiskまたはAppDisksソフトウェアがインストールされている場合は、(/ja-jp/citrix-virtual-apps-desktops/2511/upgrade-migrate/upgrade.html#remove-pvd-appdisks-and-unsupported-hosts)を参照してください。
> - Citrix®が配布するバイナリは署名されています。署名されたバイナリは、Citrixが生成した証明書または信頼できるサードパーティ証明書によって検証されていることを示します。

> Windowsマシン用のVDAには、マルチセッションOS用VDAとシングルセッションOS用VDAの2種類があります。（Linuxマシン用のVDAについては、(/ja-jp/linux-virtual-delivery-agent.html)ドキュメントを参照してください。）

インストールを開始する前に、(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/install-prepare.html)を確認し、すべての準備タスクを完了してください。

VDAをインストールする前に、コアコンポーネントをインストールします。VDAをインストールする前にサイトを作成することもできます。

この記事では、VDAをインストールする際のインストールウィザードの順序について説明します。コマンドラインの同等機能が提供されています。詳細については、(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/install-core/install-command)を参照してください。

ステップ1. 製品ソフトウェアをダウンロードしてウィザードを起動する

フルプロダクトインストーラーを使用している場合:

1. まだ製品ISOをダウンロードしていない場合:
    - Citrixアカウントの資格情報を使用して、Citrix Virtual Apps and Desktops™ダウンロードページにアクセスします。製品ISOファイルをダウンロードします。
    - ファイルを解凍します。必要に応じて、ISOファイルをDVDに書き込みます。
2. VDAをインストールするイメージまたはマシンでローカル管理者アカウントを使用します。DVDをドライブに挿入するか、ISOファイルをマウントします。インストーラーが自動的に起動しない場合は、マウントされたドライブ上の**AutoSelect**アプリケーションをダブルクリックします。

    インストールウィザードが起動します。

ステップ2. インストールする製品を選択する

コンポーネントインストーラーのインストールする製品ページ(/en-us/citrix-virtual-apps-desktops/2511/media/product-selector2-75.png)

インストールする製品の横にある**開始**をクリックします: Citrix Virtual AppsまたはCitrix Virtual Desktops。(マシンにCitrix Virtual AppsまたはCitrix Virtual Desktopsコンポーネントがすでにインストールされている場合、このページは表示されません。)

コマンドラインオプション: Citrix Virtual Appsをインストールするための`/xenapp`。このオプションを省略すると、Citrix Virtual Desktopsがインストールされます。

ステップ3. VDAを選択する

コンポーネントインストーラーのコンポーネント選択ページ(/en-us/citrix-virtual-apps-desktops/2511/media/what-to-install-2.png)

Virtual Delivery Agentエントリを選択します。インストーラーは、シングルセッションOSまたはマルチセッションOSのどちらで実行されているかを認識するため、適切なVDAタイプのみを提供します。

例えば、Windows Server 2019マシンでインストーラーを実行すると、マルチセッションOS用VDAオプションが利用可能です。シングルセッションOS用VDAオプションは提供されません。

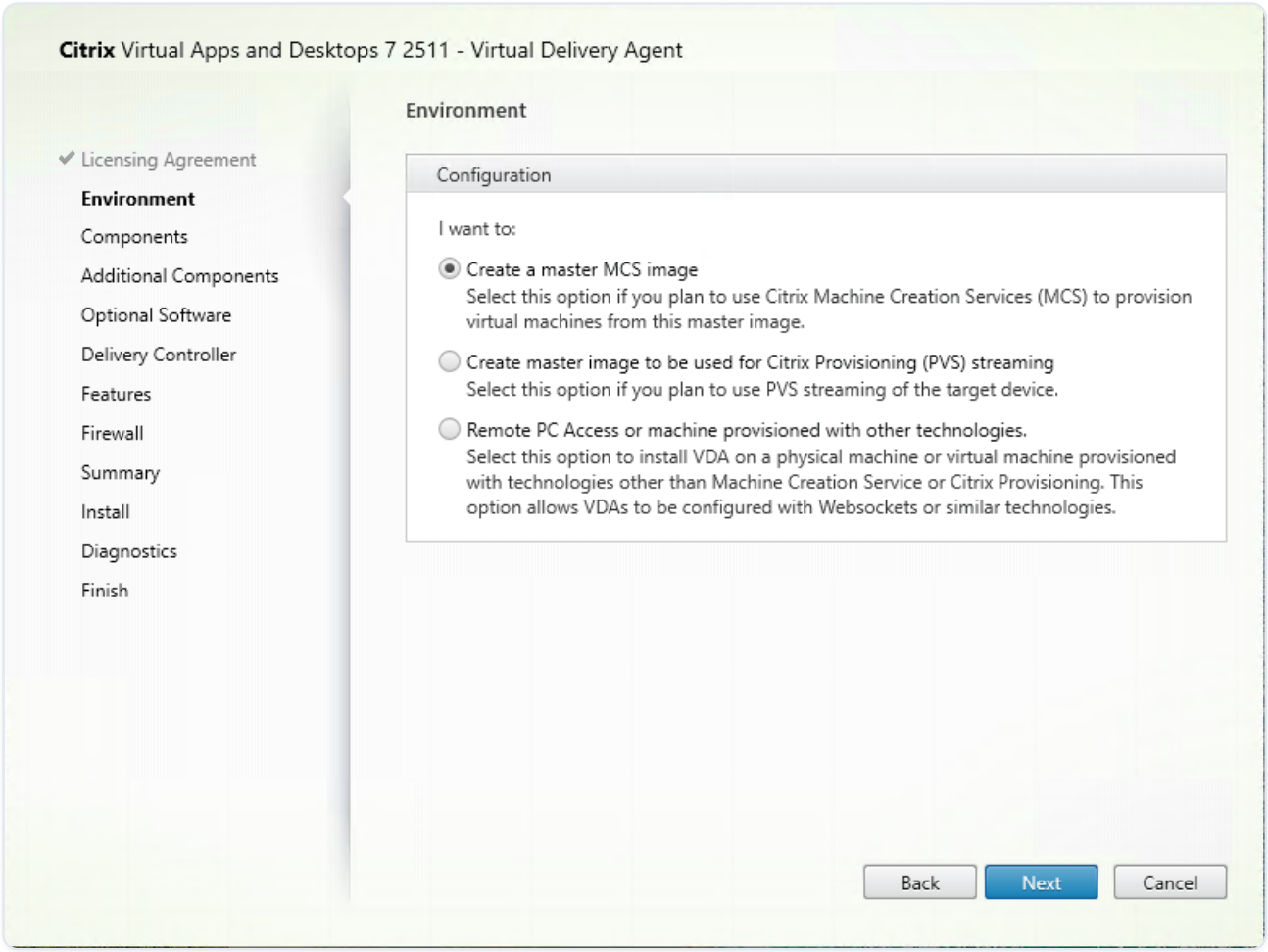
このCitrix Virtual Apps™ and Desktopsバージョンでサポートされていないオスにwindows VDAをインストール（またはアップグレード）しようとすると、オプションに関する情報に誘導するメッセージが表示されます。

スタンドアロンパッケージを使用している場合:

1. Citrixアカウントの資格情報を使用して、Citrix Virtual Apps™ and Desktopsのダウンロードページにアクセスします。適切なパッケージをダウンロードしてください。
    - `VDAServerSetup_2511.exe`: マルチセッションOS VDA *バージョン*
    - `VDAWorkstationSetup_2511.exe`: シングルセッションOS VDA *バージョン*
    - `VDAWorkstationCoreSetup_2511.exe`: シングルセッションOSコアサービスVDA *バージョン*
    - `VDASingleSessionCoreSetup_2511.exe`: 新しいシングルセッションOSコアサービスVDAバージョン
2. パッケージを右クリックし、**「管理者として実行」**を選択します。

    インストールウィザードが起動します。

ステップ4. VDAの使用方法を指定する



「環境」ページで、VDAの使用方法を指定します。このマシンをイメージとして使用して、さらに多くのマシンをプロビジョニングするかどうかを示します。

選択したオプションは、どのCitrix Provisioning™ツールが自動的にインストールされるか（もしあれば）、およびVDAインストーラーの「追加コンポーネント」ページのデフォルト値に影響します。

VDAをインストールすると、いくつかのMSI（プロビジョニング用およびその他）が自動的にインストールされます。これらのインストールを防止する唯一の方法は、コマンドラインインストールで`/exclude`オプションを使用することです。

次のいずれかを選択してください。

- **マスターMCSイメージを作成する：** Machine Creation Services™を使用してVMをプロビジョニングする予定がある場合は、このオプションを選択してVMイメージにVDAをインストールします。このオプションは、Machine Identity Serviceをインストールします。これがデフォルトのオプションです。

  コマンドラインオプション：`/mastermcsimage`または`/masterimage`

> **重要：**
>
> インストールメディアまたはISOイメージはローカルにマウントする必要があります。ソフトウェアのインストール目的でネットワークドライブからISOイメージをマウントすることはサポートされていません。

- **Citrix Provisioningまたはサードパーティのプロビジョニングツールを使用してマスターイメージを作成する：** Citrix Provisioningまたはサードパーティのプロビジョニングツール（Microsoft System Center Configuration Managerなど）を使用してVMをプロビジョニングする予定がある場合は、このオプションを選択してVMイメージにVDAをインストールします。

  コマンドラインオプション：`/masterpvsimage`
- （マルチセッションOSマシンでのみ表示）**サーバーへの仲介接続を有効にする：** 他のマシンをプロビジョニングするためのイメージとして使用されない物理マシンまたは仮想マシンにVDAをインストールするには、このオプションを選択します。

  コマンドラインオプション: `/remotepc`
- (シングルセッションOSマシンにのみ表示されます) **Remote PC Accessを有効にする:** 物理マシンにVDAをインストールしてRemote PC Accessで使用するには、このオプションを選択します。

  コマンドラインオプション: `/remotepc`

Nextをクリックします。

このページは表示されません。

- VDAをアップグレードする場合
- `VDAWorkstationCoreSetup_2507.exe`、`VDAServerSetup_2507.exe`、または`VDAWorkstationSetup_2507.exe`インストーラーを使用している場合

ステップ5. VDAをインストールする場所を選択します

VDAインストーラーのコンポーネントページ(/en-us/citrix-virtual-apps-desktops/2511/media/vda-ss-components.png)

> **注:**

> CWAとCSAは、コンポーネントページから新しいオプションソフトウェアページに移動しました。

> **コンポーネント**ページで:

- **場所:** デフォルトでは、VDAは`C:\Program Files\Citrix`にインストールされます。このデフォルトはほとんどの展開で問題ありません。別の場所を指定する場合、その場所にはネットワークサービスに対して`execute`権限が必要です。

Nextをクリックします。

ステップ6. 追加コンポーネントをインストールします

VDAインストーラーの追加コンポーネントページ(/en-us/citrix-virtual-apps-desktops/2511/media/vda-ss-addtnl-components.png)

追加コンポーネントページには、VDAとともに他の機能やテクノロジーのインストールを有効または無効にするためのチェックボックスが含まれています。コマンドラインインストールでは、`/exclude`または`/includeadditional`オプションを使用して、利用可能なコンポーネントを明示的に除外または含めることができます。

- **/includeadditional** "*コンポーネント*"\["*コンポーネント*"\] ...
- **/除外** "*コンポーネント*"\["*コンポーネント*"\] ...

次の表は、このページの項目のデフォルト設定を示しています。デフォルト設定は、**環境**ページで選択したオプションによって異なります。

追加コンポーネントページ	環境ページ：「MCSによるマスターイメージ」または「CITRIX PROVISIONINGによるマスターイメージ」が選択されている場合	環境ページ：「サーバーへのブローカー接続を有効にする」（マルチセッションOSの場合）または「リモートPCアクセス」（シングルセッションOSの場合）が選択されている場合
アプリパッケージ配信コンポーネント	選択されていません	選択されていません
Citrix VDAアップグレードエージェント	選択されていません	選択されていません
Citrixバックアップと復元	選択されていません	選択されていません

追加コンポーネントページ	環境ページ：「MCSによるマスターイメージ」または「CITRIX PROVISIONINGによるマスターイメージ」が選択されている場合	環境ページ：「サーバーへのブローカー接続を有効にする」（マルチセッションOSの場合）または「リモートPCアクセス」（シングルセッションOSの場合）が選択されている場合
シトリックス MCS IODriver	選択されていません	選択されていません
シトリックス Rendezvous V2	選択されていません	選択されていません

このページは、次の場合には表示されません。

- `VDAWorkstationCoreSetup.exe` インストーラーを使用している場合。また、追加コンポーネントのコマンドラインオプションはそのインストーラーでは無効です。
- VDA をアップグレードしていて、すべての追加コンポーネントがすでにインストールされている場合。一部の追加コンポーネントがすでにインストールされている場合、このページにはインストールされていないコンポーネントのみが表示されます。

次のチェックボックスをオンまたはオフにします。（コンポーネントはインストーラーで異なる順序で表示される場合があります。）

- **App Packages Delivery Component:** Microsoft App-V パッケージのアプリケーションを使用する場合は、このコンポーネントをインストールします。詳細については、「App-V アプリケーションの展開と配信」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "App Packages Delivery Component"`、コンポーネントのインストールを防止するには `/exclude "App Packages Delivery Component"`。

- **Citrix Profile Management:** このコンポーネントは、ユーザープロファイル内のユーザーの個人設定を管理します。詳細については、「Profile Management」を参照してください。

  Citrix Profile Managementをインストールから除外すると、Citrix DirectorでのVDAの監視とトラブルシューティングに影響します。**ユーザーの詳細**ページと**エンドポイント**ページでは、**パーソナライゼーション**パネルと**ログオン期間**パネルが機能しません。**ダッシュボード**ページと**トレンド**ページでは、**平均ログオン期間**パネルはProfile Managementがインストールされているマシンのみのデータを表示します。

サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrixは Citrix Profile Management Serviceをインストールして実行することをお勧めします。Citrix Profile Management Serviceを有効にする必要はありません。

コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Profile Management"`、コンポーネントのインストールを防止するには `/exclude "Citrix Profile Management"`。

- **Citrix Profile Management WMIプラグイン:** このプラグインは、WMI（Windows Management Instrumentation）オブジェクト（プロファイルプロバイダー、プロファイルタイプ、サイズ、ディスク使用量など）でProfile Managementのランタイム情報を提供します。WMIオブジェクトは、Directorにセッション情報を提供します。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Profile Management WMI Plug-in"`、コンポーネントのインストールを防止するには `/exclude "Citrix Profile Management WMI Plug-in"`。

注:

このバージョン以降、**Citrix Profile Management**および**Citrix Profile Management WMI Plug-in**はVDAの一部となり、**マスターイメージ/MCS/PVS**のユースケースでは自動的にインストールされます。これらのコンポーネントは、**Remote PC**のユースケースでは**デフォルトではインストールされません**。すべての場合において、インストールされたコンポーネントは自動的にアップグレードされます。コマンドラインの動作は、以前のリリースから変更されていません。

- **VDAアップグレードエージェント:** Citrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）の展開にのみ適用されます。VDAがVDAアップグレード機能に参加できるようにします。この機能を使用して、管理コンソールからカタログのVDAを即時またはスケジュールされた時間にアップグレードできます。このエージェントがインストールされていない場合、VDAインストーラーをマシンで実行することでVDAをアップグレードできます。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix VDA Upgrade Agent"`、コンポーネントのインストールを防止するには `/exclude "Citrix VDA Upgrade Agent"`。

- **ストレージ最適化のためのMCSIOライトキャッシュ:** Citrix MCS I/Oドライバーをインストールします。詳細については、ハイパーバイザーで共有されるストレージおよび一時データのキャッシュの構成を参照してください。

コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix MCS IODriver"`、コンポーネントのインストールを防止するには `/exclude "Citrix MCS IODriver"`。

- **プロキシ構成:** 環境でGateway Service、VDA Upgrade ServiceなどでRendezvousプロトコルを使用する予定があり、ネットワークにアウトバウンド接続用の非透過型プロキシがある場合は、このコンポーネントをインストールし、ここでプロキシを指定します。HTTPプロキシのみがサポートされています。

  このコンポーネントをインストールする場合は、**Rendezvousプロキシ構成**ページでプロキシのアドレスまたはPACファイルのパスを指定します。機能の詳細については、Rendezvousプロトコルを参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Rendezvous V2"`、コンポーネントのインストールを防止するには `/exclude "Citrix Rendezvous V2"`。

- **Citrix Backup and Restore:** VDAのインストールまたはアップグレードが失敗した場合、このコンポーネントはマシンをインストールまたはアップグレード前のバックアップ状態に戻すことができます。

  Microsoft の前提条件が インストール準備 に記載されているとおり満たされていることを確認してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Backup and Restore"`、コンポーネントのインストールを防止するには `/exclude "Citrix Backup and Restore"`。

  > **注：**
  >
  > MCSストレージ最適化が有効になっている場合、Windowsサーバーまたはデスクトップオペレーティングシステムのバックアップまたは復元が失敗する可能性があります。これを解決するには、メタインストーラーでMCSストレージ最適化オプションを無効にしてください。

ステップ7. オプションソフトウェアのインストール

☐

> **注：**
>
> オプションソフトウェアページは、Citrix Virtual Apps and Desktops 2503以降で追加された新機能であり、VDAに追加のCitrixソフトウェアをインストールするための柔軟性を顧客に提供します。

> Citrix Workspace™アプリとCitrix Secure Access™クライアントは、コンポーネントページからオプションソフトウェアページに移動されました。

> ユーザーパーソナライゼーションレイヤーも、追加コンポーネントページからオプションソフトウェアページに移動されました。その選択ロジックは、追加コンポーネントページにあったときと同じままです。つまり、ユーザーパーソナライゼーションレイヤーがすでにインストールされている場合、それは**必須**として選択され、コンポーネントはアップグレードされます。

> **オプションソフトウェア**ページで：

- **場所**: デフォルトでは、コンポーネントは `C:\Program Files\Citrix` にインストールされます。このデフォルトはほとんどの展開で問題ありません。別の場所を指定する場合、その場所にはネットワークサービスに対して `execute` のアクセス許可が必要です。
- **コンポーネント**: デフォルトでは、Citrix Workspace app for WindowsはVDAと一緒にインストールされません。`VDAWorkstationCoreSetup.exe` インストーラーを使用している場合、Citrix Workspace app for Windowsはインストールされないため、このチェックボックスは表示されません。

Nextをクリックします。

コマンドラインオプション: `'/installdir "C:\Program Files\VDA" /components "VDA","CSA","PLUGINS"` を使用して、Virtual Delivery Agent、Citrix Secure Access Client、Citrix deviceTRUST、Citrix uberAgent、およびCitrix Workspace appを指定されたディレクトリにインストールします。

> **注：**

VDAのインストール、アップグレード、またはアンインストール中に、Citrix Workspaceアプリおよびその他のコンポーネントをインストール、アップグレード、またはアンインストールすることを選択できます。これは、次のシナリオで可能です。

- VDAのインストールおよび2511へのアップグレード中に、コンポーネントとCWAプラグインを含めるか除外するかを選択できます。
  - デフォルトでは、**Citrix Workspaceアプリ (CWA)**、**Citrix Secure Access Client (CSA)**、**Citrix User Personalization Layer (UPL) (WS VDAのみ)**、および**Citrix Elastic App Layering (CEAL) (TS VDAのみ)** はインストール対象として選択されていませんが、必要に応じてインストール時に選択できます。

    Session Recording Agent (SRAGENT) および **Citrix Assistant App (ASSISTANTAPP) (WS VDAのみ)** はデフォルトでインストール対象として選択されていますが、必要に応じてインストール時に選択を解除できます。
  - **Citrix Device Trust**、**Citrix uberAgent**、および**Citrix Workspace Environment Management™ agent** はVDAに統合され、常にインストールされます。これらのコンポーネントは、GUIを使用してインストールする際には選択解除できません。**Citrix Device Trust** および **Citrix Workspace Environment Management™ agent** のインストールを回避するには、管理者はサポートされている `/exclude` コマンドラインオプションを使用する必要があります。ただし、uberAgentはGUIまたはコマンドライン (CLI) のいずれからもインストールから除外することはできません。
  - デフォルトでは、**Citrix Workspace Environment Management™ agent** は**Basic deployment**で実行されます。これは、WEMインフラストラクチャに接続しない機能が制限されたシングルマシンモードです。エージェントをCitrix CloudのWEMサービスまたはオンプレミス展開に接続してWEMの全機能を有効にするには、グループポリシーを通じて設定を構成します。詳細については、このWEM記事を参照してください。
  - **コマンドラインの変更**

    /components VDA CSA : このコマンドは、**VDA** と **CSA** (選択済み) をインストールし、さらに **Citrix Device Trust**、**Citrix uberAgent**、および **Citrix Workspace Environment Management agent** (デフォルトで統合済み) もインストールします。

    /components VDA : このコマンドは、**VDA** をインストールし、さらに **Citrix Device Trust**、**Citrix uberAgent**、および **Citrix Workspace Environment Management**

agent もインストールします。これらは現在VDA自体に統合されているためです。「/components」オプションとともにCitrix Device Trust、Citrix uberAgent、およびCitrix Workspace Environment Management agentを引数として指定した場合、VDAメタインストーラーはこれらの引数が「/components」オプションから削除されたことを示す通知をログに記録します。その後、VDAメタインストーラーはVDAのインストールまたはアップグレードを続行します。

/components : このコマンドは無効なコマンドであり、常にVDAを含める必要があります。必要に応じて、追加のコンポーネントをインストール対象として追加できます。

デフォルトで統合されたコンポーネントに`/exclude`コマンドを使用する : Citrix Virtual Apps and Desktops 2507 LTSRでは、`/exclude`オプションが常に優先されます。これは、デフォルトで統合されたコンポーネントのインストールを防止するために使用できます。例: `/exclude` "Citrix Device Trust","Citrix Universal Print Client"。このコマンドは、Citrix Workspace Environment Management agentとともにVDAをインストールしますが、Citrix Device TrustとCitrix Universal Print Clientはインストールしません。

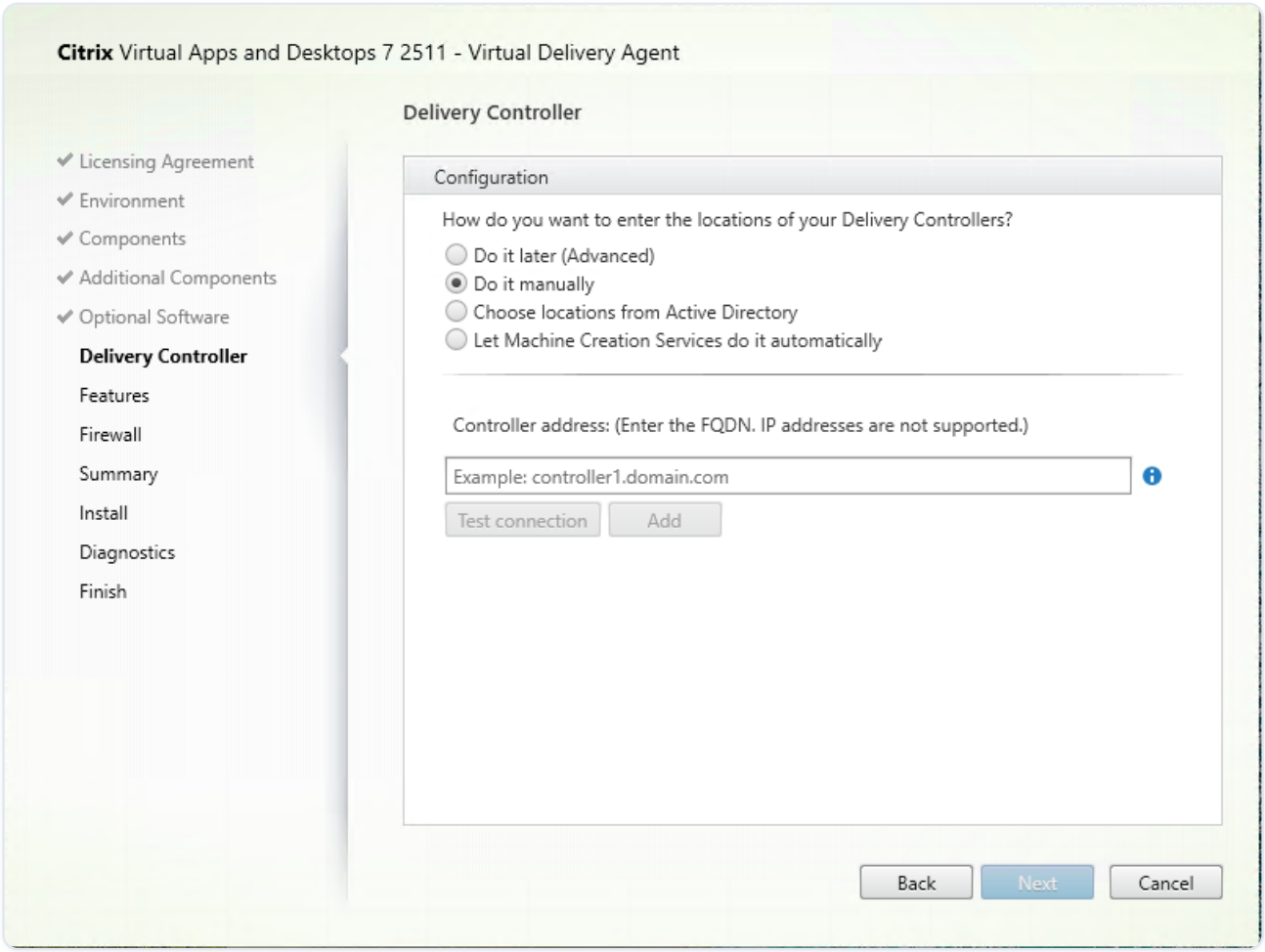
- VDAのアップグレード中に、Citrix Workspace app、Citrix Secure Access Client、Citrix User Personalization Layer、Session Recording Agent、Citrix Assistant App、およびElastic App LayeringがVDAにまだインストールされていない場合、それらをインストールすることを選択できます。
- VDAのアップグレード中に、Citrix Workspaceアプリおよびその他のインストール済みプラグインのバージョンをアップグレードできる場合、それらをアップグレードするオプションが表示されます。
- インストールまたはアップグレード中に、Citrix Workspaceアプリ (CWA) プラグインまたはコンポーネントのインストールまたはアップグレードが失敗した場合、チェックボックス **「選択したコンポーネントの失敗時でもVDAのアップグレードまたはインストールを続行する」** を選択することで、その失敗を上書きし、コアVDAのインストールを続行できます。
- VDAアンインストール中に、Citrix Workspaceアプリ (CWA) およびその他のインストール済みコンポーネントをアンインストールするかどうかを選択できます。デフォルトでは、CWAを除くすべてのコンポーネントが自動的にアンインストールされます。CWAは特別に扱われ、明示的に選択されない限り削除されません。

- **Citrix User Personalization Layer:** ユーザーパーソナライゼーションレイヤーのMSIをインストールします。詳しくは、「ユーザーパーソナライゼーションレイヤー」を参照してください。

  このコンポーネントは、シングルセッションのWindows 10マシンにVDAをインストールする場合にのみ表示されます。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "User Personalization Layer"`、コンポーネントのインストールを防止するには `/exclude "User Personalization Layer"`。

ステップ8. Delivery Controller™アドレス



Delivery Controllerページで、インストールされているControllerのアドレスを入力する方法を選択します。Citrixでは、VDAのインストール中にアドレスを指定することをお勧めします (**手動で実行**)。VDAは、この情報がないとControllerに登録できません。VDAが登録できない場合、ユーザーはそのVDA上のアプリケーションやデスクトップにアクセスできません。

- **手動で実行:** (デフォルト) インストールされているControllerのFQDNを入力し、**追加**をクリックします。複数のControllerをインストールしている場合は、それらのアドレスを追加します。

- **後で実行 (詳細設定):** このオプションを選択すると、ウィザードは続行する前にその操作を実行するかどうかを確認します。後でアドレスを指定するには、インストーラーを再実行するか、Citrixグループポリシーを使用します。ウィザードは**概要**ページでも通知します。
- **Active Directoryから場所を選択:** マシンがドメインに参加しており、ユーザーがドメインユーザーである場合にのみ有効です。
- **WebSocketトークンを使用:** WebSocket VDAを作成します。WebSocketTokenは、必要なトークン用です。
- **Machine Creation Servicesに自動的に実行させる:** MCSを使用してマシンをプロビジョニングする場合にのみ有効です。

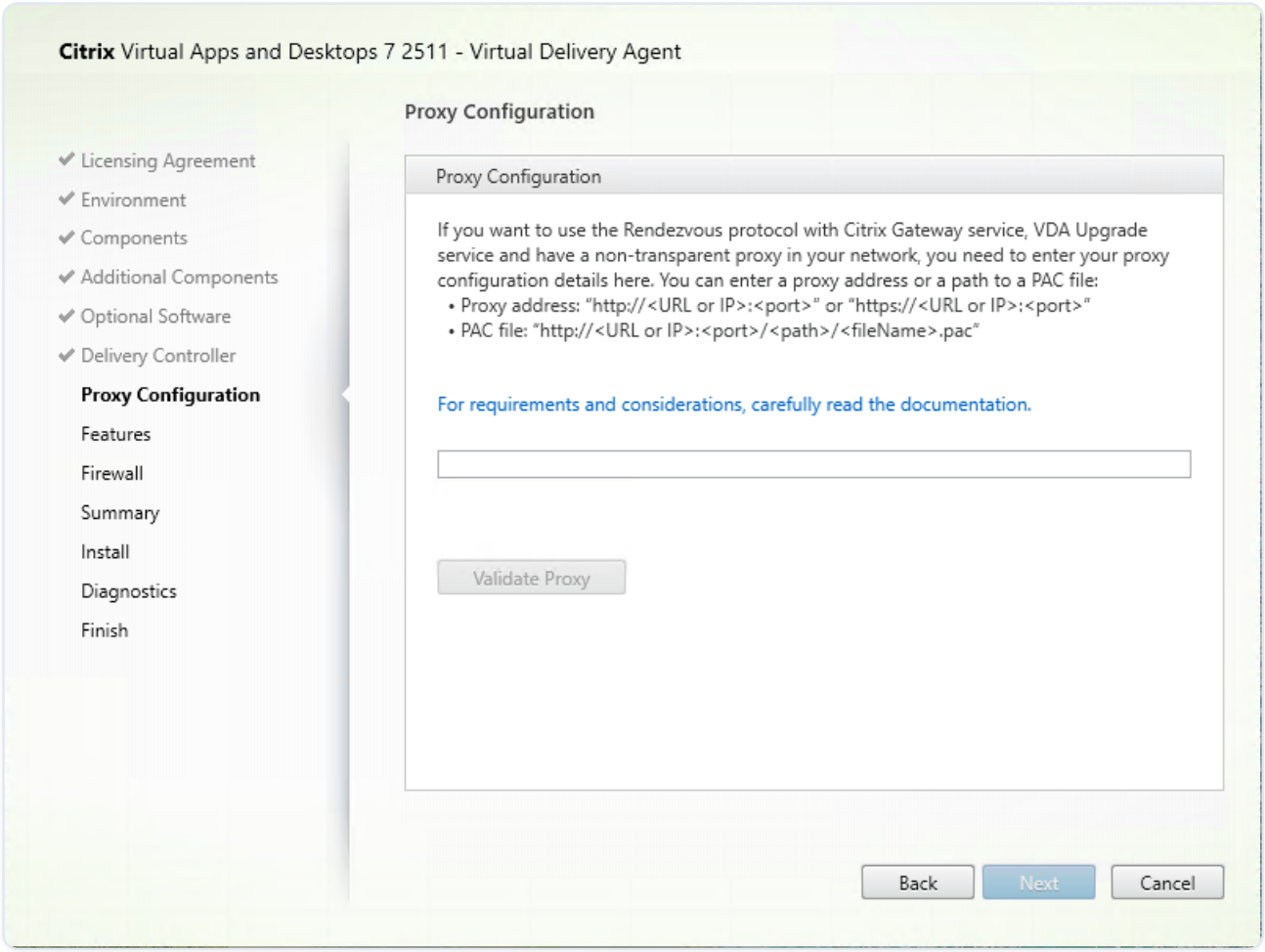
次へをクリックします。**後で実行 (詳細設定)**を選択した場合、後でControllerアドレスを指定することを確認するよう求められます。

その他の考慮事項:

- アドレスには英数字以外の文字を含めることはできません。
- VDAインストール時およびグループポリシーでアドレスを指定した場合、ポリシー設定はインストール時に指定された設定を上書きします。
- VDA登録を成功させるには、Controllerとの通信に使用されるファイアウォールポートが開いている必要があります。このアクションは、ウィザードの**ファイアウォール**ページでデフォルトで有効になっています。
- Controllerの場所を指定した後（VDAインストール中またはインストール後）、Controllerが追加または削除されたときにVDAを更新するために自動更新機能を使用できます。VDAがControllerを検出して登録する方法の詳細については、VDA登録を参照してください。

コマンドラインオプション：`/controllers`

ステップ9. プロキシ構成



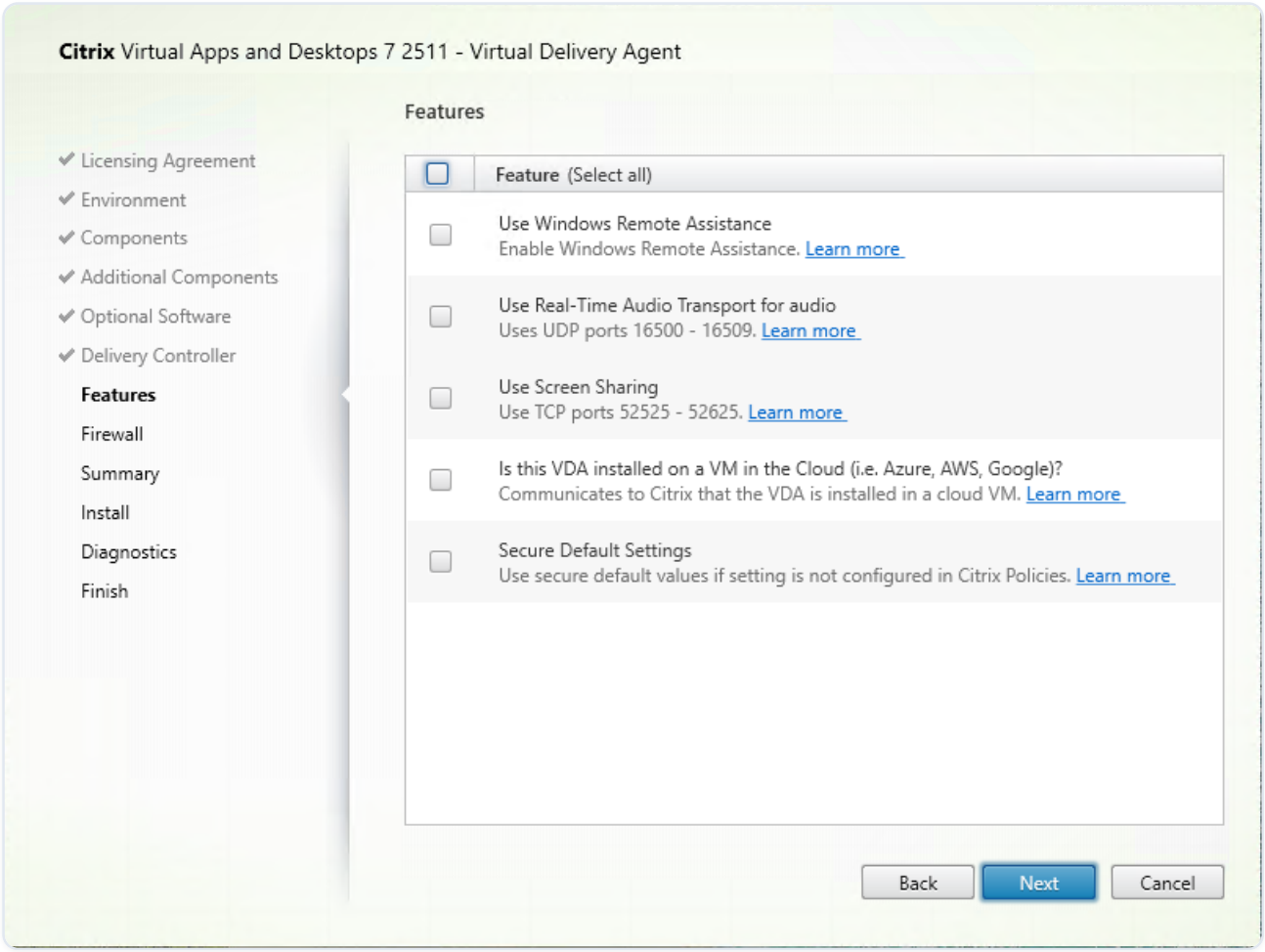
プロキシ構成ページは、**追加コンポーネント**ページで**プロキシ構成**チェックボックスを有効にした場合にのみ表示されます。

1. プロキシソースをプロキシアドレスで指定するか、PACファイルパスで指定するかを選択します。
2. プロキシアドレスまたはPACファイルパスを指定します。
   - プロキシアドレスの形式: `http://<url-or-ip>:<port>`
   - PACファイルの形式: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

接続テストを成功させるには、プロキシポートのファイアウォールが開いている必要があります。プロキシへの接続が確立できない場合でも、VDAインストールを続行するかどうかを選択できます。

コマンドラインオプション：`/proxyconfig`

ステップ10. 機能の有効化または無効化



「**機能**」ページで、チェックボックスを使用して、使用する機能を有効または無効にします。

- **Windows リモートアシスタンスを使用する:** この機能を有効にすると、Director のユーザーシャドウ機能で Windows リモートアシスタンスが使用されます。Windows リモートアシスタンスは、ファイアウォールで動的ポートを開きます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_remote_assistance`

- **オーディオにリアルタイムオーディオトランスポートを使用する:** ネットワークで VoIP が広く使用されている場合は、この機能を有効にします。この機能により、遅延が減少し、損失の多いネットワークでのオーディオの回復性が向上します。RTP over UDP トランスポートを使用してオーディオデータを送信できます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_real_time_transport`

- **画面共有を使用する:** 有効にすると、画面共有で使用されるポートが Windows ファイアウォールで開かれます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_ss_ports`

- **この VDA はクラウド内の VM にインストールされていますか:** この設定は、Citrix がテレメトリ目的でオンプレミスおよびサービス (Citrix Cloud™) VDA 展開のリソースロケーションを正しく識別するのに役立ちます。この機能は、顧客側の利用には影響しません。展開で Citrix DaaS を使用している場合は、この設定を有効にします (デフォルト = 無効)。

  コマンドラインオプション: `/xendesktopcloud`

- **セキュアなデフォルト設定:** このオプションは、よりセキュアな初期設定のために、さまざまな機能のデフォルト設定を有効から無効に変更します。関連する機能は、クライアントドライブリダイレクト、特殊フォルダーリダイレクト、ドラッグアンドドロップ、クライアント TWAIN デバイスリダイレクト、クライアント USB プラグアンドプレイデバイスリダイレクト、クライアントプリンターリダイレクト、クライアントクリップボードリダイレクト、およびクライアントマイクリダイレクトです。

コマンドラインオプション: `/ENABLE_SECURE_DEFAULTS`

Nextをクリックします。

ステップ 11. ファイアウォールポート

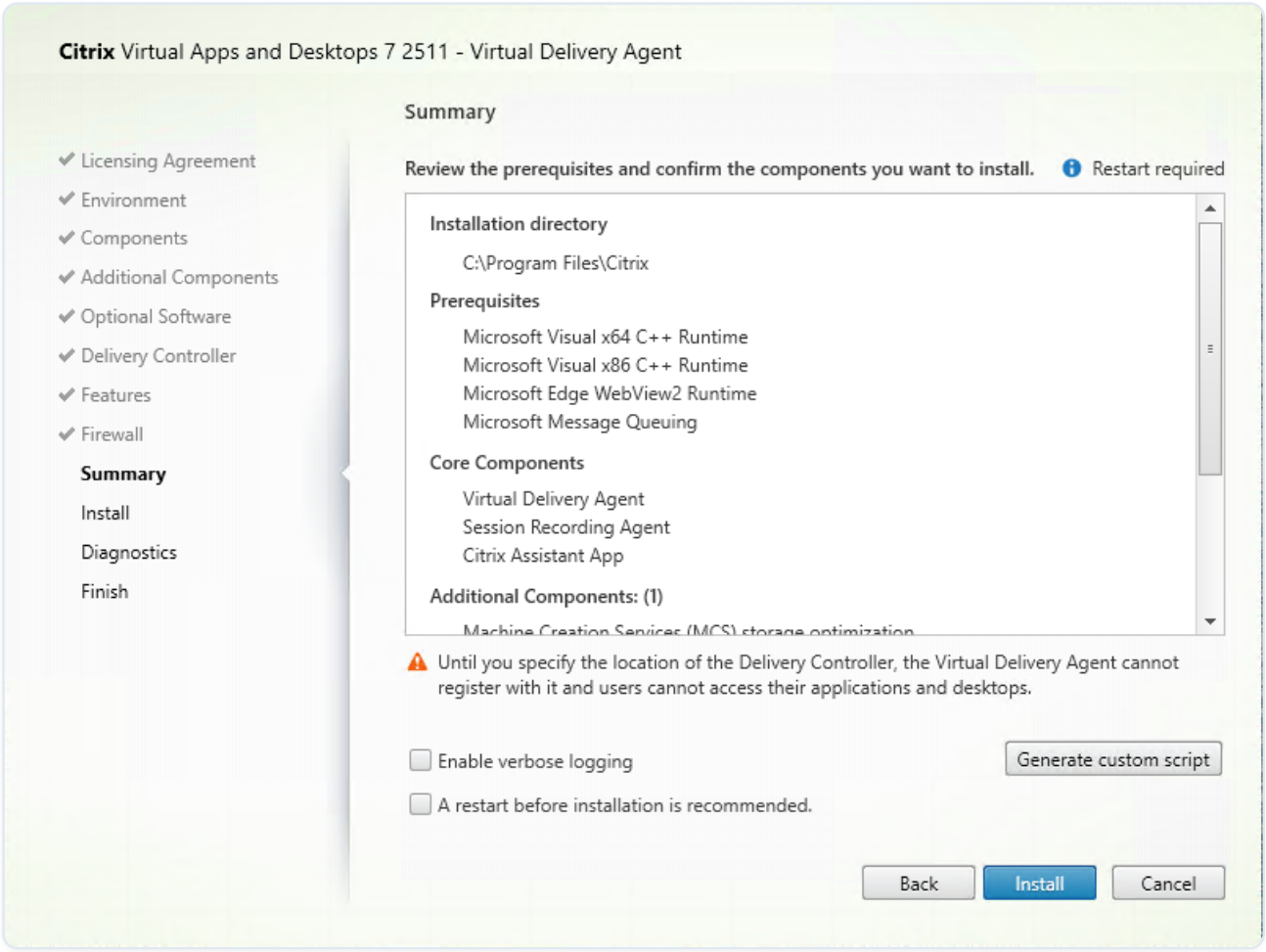
VDA インストーラーのファイアウォールページ(/en-us/citrix-virtual-apps-desktops/2511/media/vda-ss-firewall.png)

「**ファイアウォール**」ページでは、Windows ファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても、ポートはデフォルトで自動的に開かれます。このデフォルト設定は、ほとんどの展開で問題ありません。ポート情報については、「ネットワークポート」を参照してください。

「**次へ**」をクリックします。

コマンドラインオプション: `/enable_hdx_ports`

手順 12. 前提条件を確認し、インストールを確定する



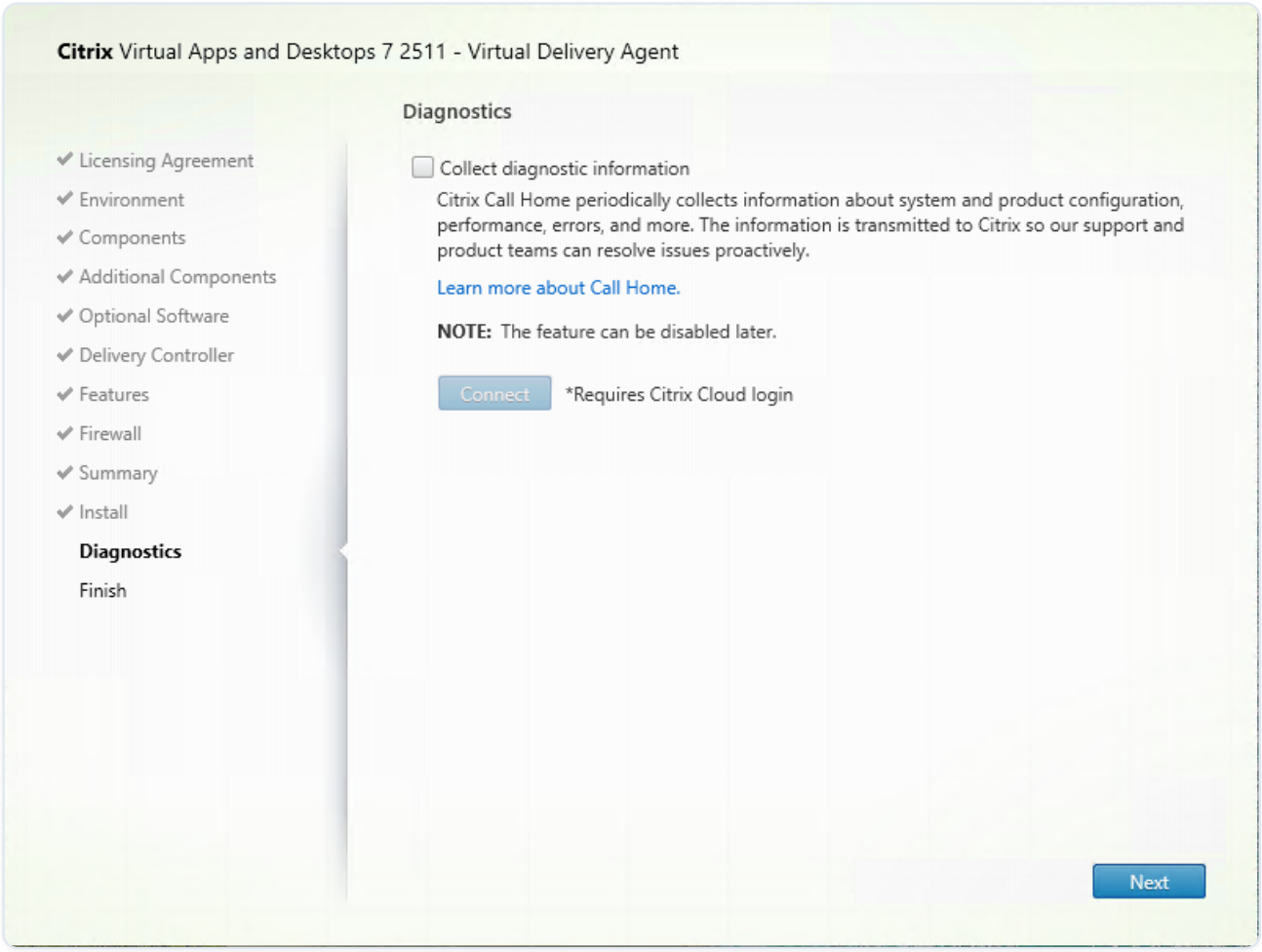
「**概要**」ページには、インストールされるものが一覧表示されます。「**戻る**」ボタンを使用して、以前のウィザードページに戻り、選択を変更できます。

準備ができたら、「**インストール**」をクリックします。

前提条件がまだインストールまたは有効になっていない場合、マシンが1回以上再起動する可能性があります。「インストールの準備」を参照してください。

> 「**注:**」:
>
> この時点で、「**概要**」ページにある「**カスタムスクリプトの生成**」ボタンをクリックして、現在のインストール選択に基づいてコマンドラインスクリプトを作成することもできます。このスクリプトは、無人モードでVDAをインストールまたはアップグレードするために再利用できます。

手順 13. 診断



「**診断**」ページで、Citrix Call Homeに参加するかどうかを選択します。参加することを選択した場合（デフォルト）、「**接続**」をクリックします。プロンプトが表示されたら、Citrixアカウントの資格情報を入力します。

資格情報が検証された後（または参加しないことを選択した場合）、「**次へ**」をクリックします。

フル製品インストーラーを使用している場合、「**診断**」ページで「**診断情報の収集**」を最初に選択せずに「**接続**」をクリックすると、「**Connect to Citrix Insight Services**」ダイアログを閉じると「**次へ**」ボタンが無効になります。次のページに進むことはできません。「**次へ**」ボタンを再度有効にするには、「**診断情報の収集**」を選択し、すぐに選択を解除します。

詳細については、「Call Home」を参照してください。

ステップ 14. このインストールを完了する

VDAインストーラーのインストール完了ページ(/en-us/citrix-virtual-apps-desktops/2511/media/vda-ss-finish.png)

完了ページには、正常にインストールおよび初期化されたすべての前提条件とコンポーネントの緑色のチェックマークが表示されます。

完了をクリックします。デフォルトでは、マシンは自動的に再起動します。この自動再起動を無効にすることはできますが、マシンが再起動するまでVDAは使用できません。

次のステップ

必要に応じて、上記のプロシージャを繰り返して、他のマシンまたはイメージにVDAをインストールします。

すべてのVDAをインストールしたら、Studioを起動します。まだサイトを作成していない場合、Studioはそのタスクに自動的に誘導します。それが完了すると、Studioはマシンカタログとデリバリーグループの作成に誘導します。参照：

- サイトの作成
- マシンカタログの作成
- デリバリーグループの作成

シトリックス オプティマイザー

Citrix Optimizerは、Windows OS用のツールであり、Citrix管理者がさまざまなコンポーネントを削除および最適化することでVDAを最適化するのに役立ちます。

VDAをインストールし、最終的な再起動を完了した後、Citrix Optimizerをダウンロードしてインストールします。CTX224676を参照してください。CTX記事には、ダウンロードパッケージと、Citrix Optimizerのインストールおよび使用に関する手順が含まれています。

VDAのカスタマイズ

インストール済みのVDAをカスタマイズするには：

1. プログラムの削除または変更」のWindows機能から、「**Citrix Virtual Delivery Agent**」または「**Citrix Remote PC Access/VDI Core Services VDA**」を選択します。その後、右クリックして「**変更**」を選択します。
2. 「**Virtual Delivery Agent設定のカスタマイズ**」を選択します。インストーラーが起動したら、以下を変更できます。

    - コントローラーアドレス
    - コントローラーに登録するためのTCP/IPポート (デフォルト = 80)
    - Windowsファイアウォールポートを自動的に開くかどうか

トラブルシューティング

- Citrixがコンポーネントインストールの結果を報告する方法については、Citrixインストールリターンコードを参照してください。
- 配信グループのStudio表示では、**詳細**ペインの「**インストール済みVDAバージョン**」エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンのWindowsの「プログラムと機能」表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされた後、Delivery Controllerに登録されるまで、ユーザーにアプリやデスクトップを配信できません。

  VDA登録方法と登録の問題のトラブルシューティング方法については、VDA登録を参照してください。

既知の制限事項

Citrix Workspaceアプリ for Windowsバージョン1912以前を使用すると、しばらくするとセッションが切断されます。この問題は、Citrix Workspaceアプリの新しいLTSRおよびCRバージョンで修正されています。 サポートされているリリースバージョンの詳細については、Citrix Workspaceアプリ for Windows / Citrix Receiver for Windows Long Term Service Releasesを参照してください。

VDAインストールに関連するWindows Defenderアクセス制御を構成する

お客様は、署名されていないバイナリのロードを禁止するために、Windows Defenderアクセス制御 (WDAC) 設定を構成します。VDAインストーラーを通じて配布される署名されていないバイナリは、VDAのインストールを制限するため、禁止されます。

Citrix® は現在、すべてのCitrix生成バイナリをCitrixコード署名証明書で署名しています。さらに、Citrixは、当社の製品とともに配布されるサードパーティ製バイナリも、それらのサードパーティ製バイナリを信頼できるバイナリとして認証する証明書で署名しています。

> **重要:**
>
> 署名されていないサードパーティ製バイナリを含む古いVDAから、署名されたバイナリを含む新しいVDAバージョンにアップグレードしても、常にアップグレードされたマシンに署名されたバイナリが配置されるとは限りません。 これは、システムのアップグレードが同じバージョンのバイナリを置き換えないというOS内のメカニズムによるものです。 サードパーティ製バイナリは署名されていますが、サードパーティによって制御されているその

バージョンはCitrixによって更新できないため、これらのバイナリは更新されません。この制限を回避するには、次の手順を実行します。

1. バイナリを許可リストに含めます。これにより、バイナリに署名する必要がなくなります。
2. 古いVDAをアンインストールし、新しいVDAをインストールします。これはVDAの新規インストールに似ており、署名されたバージョンがインストールされます。

ウィザードを使用して新しいベースポリシーを作成する

WDACを使用すると、信頼できるバイナリをシステムで実行できるように追加できます。WDACのインストール後、**Windows Defender Application Control Policy Wizard** が自動的に開きます。

バイナリを追加するには、新しいベースWDACポリシーを作成する必要があります。ベースポリシーを作成するためのCitrix推奨ガイドラインは、このセクションで提供されています。

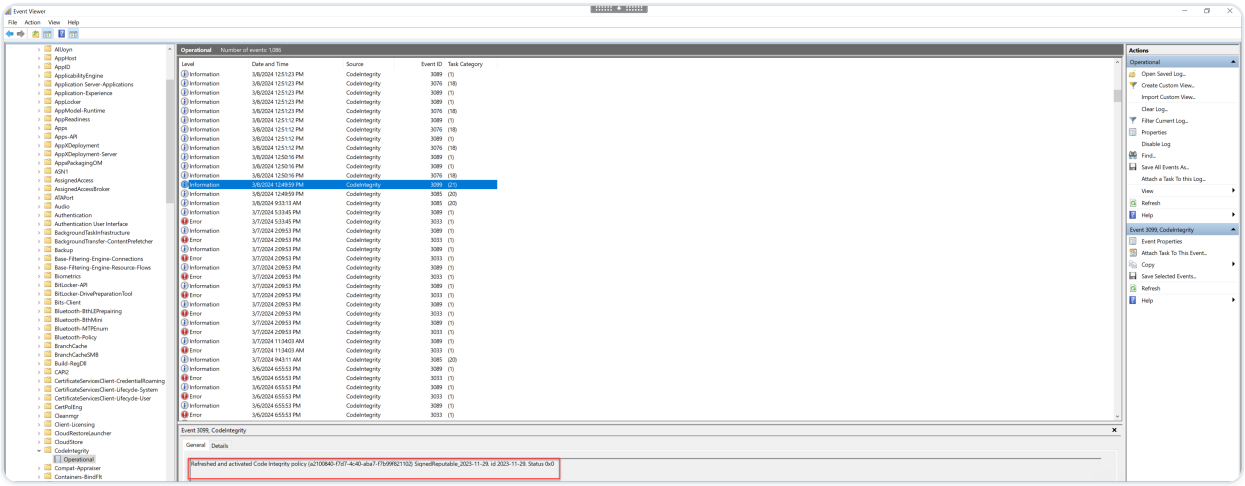
- Windowsオペレーティングコンポーネント、Microsoft Storeからインストールされたアプリ、すべてのMicrosoft署名済みソフトウェア、およびサードパーティのWindowsハードウェア互換ドライバーを承認するため、ベーステンプレートとして を選択します。
- 新しいWindows Defender Application Controlポリシーを適用する前にテストできるため、 を選択します。
- アプリケーションが識別され信頼されるレベルを指定し、参照ファイルを提供するために、の を追加します。ルールタイプとして「発行元」を選択することで、Citrix証明書のいずれかで署名された参照ファイルを選択できます。
- ルールを追加したら、`.XML` および `.CIP` ファイルが保存されているフォルダーに移動します。`.XML` ファイルには、ポリシーで定義されているすべてのルールが含まれています。任意のルールを変更、追加、または削除するように構成できます。
- WDACポリシーを展開する前に、`.XML` ファイルをバイナリ形式に変換する必要があります。WDACファイルは、`.XML` ファイルを `.CIP` ファイルに変換します。
- `.CIP`ファイルをC:\WINDOWS\System32\CodeIntegrity\CiPolicies\Activeにコピーして貼り付け、マシンを再起動します。生成されたポリシーは監査モードで適用されます。
- ベースポリシーを作成する手順については、ウィザードで新しいベースポリシーを作成するを参照してください。

このポリシーが適用されると、WDACは指定された発行元/CA機関によって署名されているCitrixファイルについて警告を発しません。

同様に、サードパーティによって署名されたファイルに対して発行元レベルのルールを作成できます。

適用されたポリシーを確認する

1. マシンが再起動されたら、**イベントビューアー**を開き、**アプリケーションとサービスログ > Microsoft > Windows > CodeIntegrity > Operational**に移動します。
2. 適用されたポリシーがアクティブになっていることを確認してください。



3. ポリシーに違反したログを探し、そのファイルのプロパティを確認します。まず、署名されていることを確認します。署名されていない場合で、このマシンがVDAアップグレードを経ている場合は、上記の制限事項で説明されているケースである可能性が高いです。署名されている場合は、このファイルは前述のように代替証明書で署名されている可能性があります。

Citrix証明書で署名されたCitrix生成ファイルの例は`C:\Windows\System32\drivers\picadm.sys`です。 Citrixサードパーティ証明書で署名されたサードパーティバイナリの例は`C:\Program Files\Citrix\IcaConfigTool\Microsoft.Practices.Unity.dll`です。

VDAのインストールとアップグレードの事前チェック

VDAのインストールとアップグレードのための分離された事前フライトチェックを導入し、お客様が進行する前に潜在的な問題を事前に特定できるようにします。このチェックは、すべての依存関係と前提条件を検証し、各条件について明確な合格/不合格ステータスを提供します。不合格が発生した場合は、具体的な推奨事項を含む詳細な修復ガイダンスが提供されます。実際のインストールまたはアップグレードプロセスは別個のものであり、事前チェックが完了した後に手動で開始する必要があります。

この記事では、VDAのインストールとアップグレードの事前チェックを実行する手順について説明します。

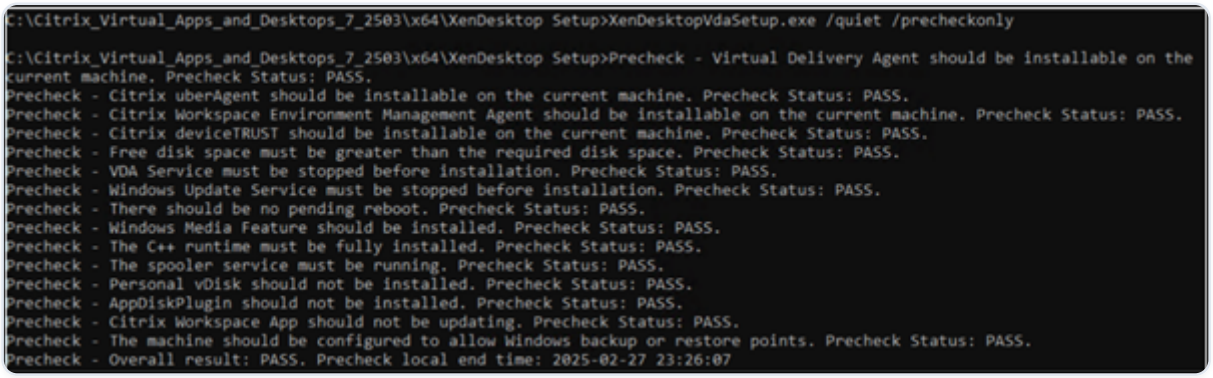
ステップ1. コマンドラインの実行

> **注:**
>
> - 事前チェックはコマンドラインモードでのみサポートされています。
> - このコマンドを実行しても、インストールまたはアップグレードは開始されません。

> 事前チェックを実行するには、インストールまたはアップグレードによく使用するコマンドに `/precheckonly` オプションを追加します。VDAのインストールまたはアップグレードのすべての事前チェック条件が確認されます。

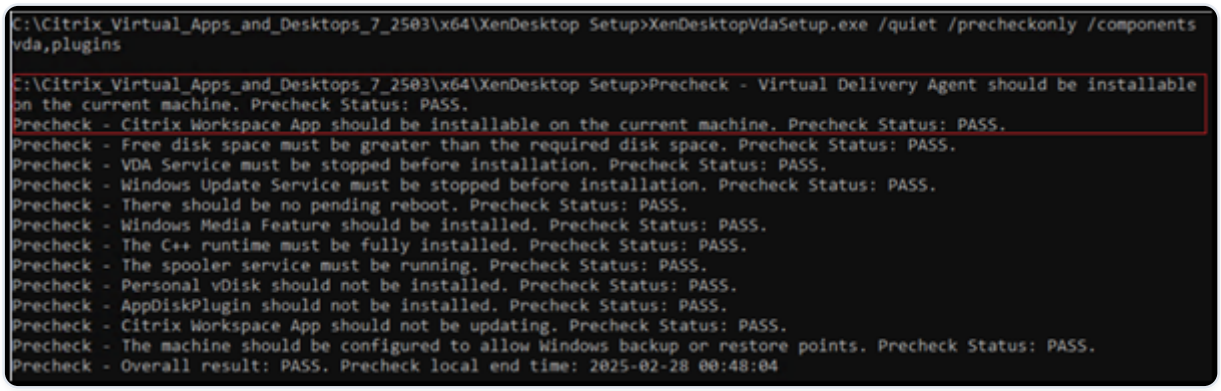
デフォルトのインストールとアップグレードの事前チェックを実行する

次のコマンドを実行して事前チェックを実行し、マシンの状態が許容できる状態であることを確認します。 `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly`



指定されたコンポーネントのインストールとアップグレードの事前チェックを実行する

インストールまたはアップグレードの前に特定のコンポーネントの前提条件を確認するには、コマンドに `/precheckonly` を追加します。 `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /components vda,plugins`



追加コンポーネント - Citrix Backup and Restore のインストールとアップグレードの事前チェックを実行する

コマンド `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly` は、オプションのチェックとして Citrix Backup and Restore コンポーネントの前提条件を確認します。オプションのチェックを除くすべての事前チェックが合格した場合、全体の結果は PASS となります。

追加コンポーネントの事前チェック(/en-us/citrix-virtual-apps-desktops/2511/media/precheck-for-additional-components.png)

以下のコマンドは、必須チェックの一部として Citrix Backup and Restore コンポーネントの前提条件を確認します。

- `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /includeadditional "Citrix Backup and Restore"`
- `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /enablerestore`
- `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /enablerestorecleanup`

Citrix Backup and Restoreの事前チェック(/en-us/citrix-virtual-apps-desktops/2511/media/precheck-for-citrix-backup-and-restore.png)

ステップ2. 事前チェック結果の表示

事前チェックの結果はコマンドラインに表示され、`%temp%/Citrix/XenDesktop Installer/XenDesktop Installation.log` にログ記録され、`%temp%/Citrix/XenDesktop Installer/PrecheckResult_{yyyyMMddHHmmss}.json` に保存されます。事前チェックが失敗した場合、全体の結果は `FAIL` となり、各問題に対する修正案が提示されます。

コマンドライン出力

コマンドラインの事前チェック結果には以下が含まれます。

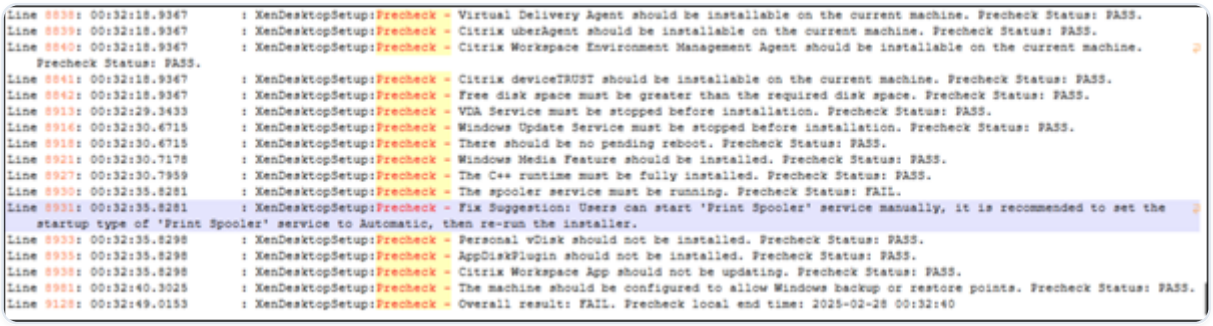
- 事前チェック基準
- 事前チェックステータス
- 失敗に対する修正案
- 全体の結果
- 終了時刻。

結果が`FAIL`の場合、修正案は「**Precheck - Fix Suggestion:**」で始まる行に記載されています。

ログ出力(/en-us/citrix-virtual-apps-desktops/2511/media/log-output.png)

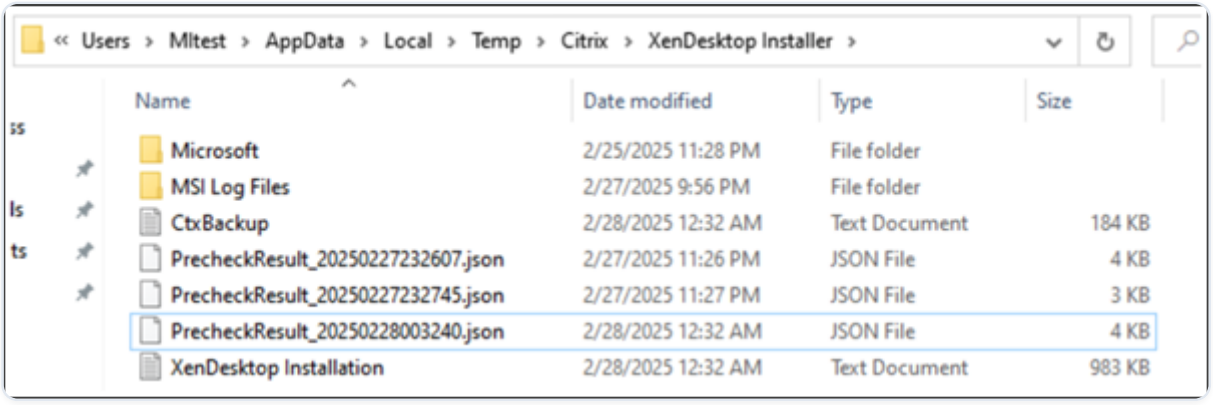
ログ出力

`XenDesktop Installation.log` の事前チェック結果は、コマンドラインに表示されるものと同じです。それらを見つけるには、ログファイルで `Precheck -` を検索してください。 全体的な結果が `FAIL` の場合、修正の提案は `Precheck - Fix Suggestion:` を含む行にあります。



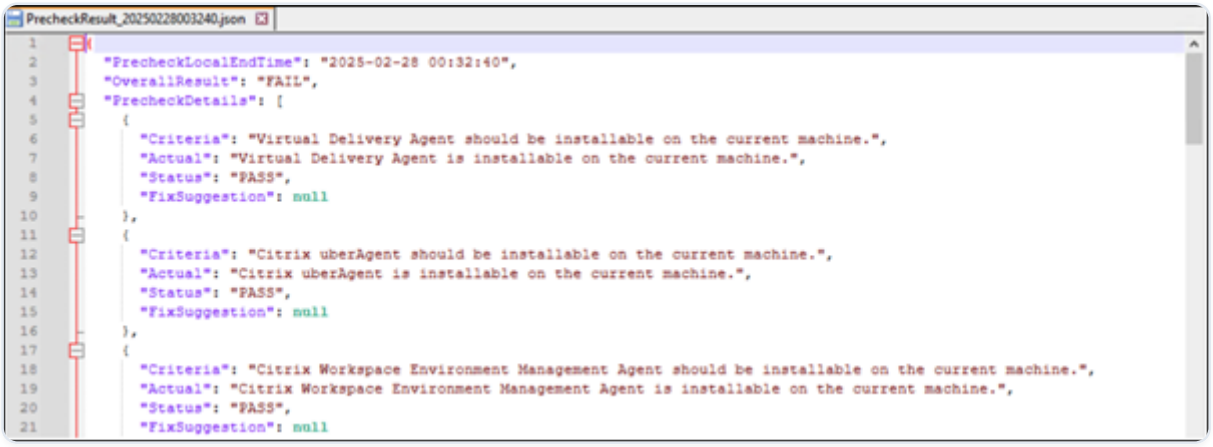
JSON 出力

`/quiet /precheckonly` を含むコマンドが実行されるたびに、`.json` ファイルが生成されます。ファイル名は `PrecheckResult_{yyyyMMddHHmmss}.json` で、タイムスタンプのサフィックスが付いています。

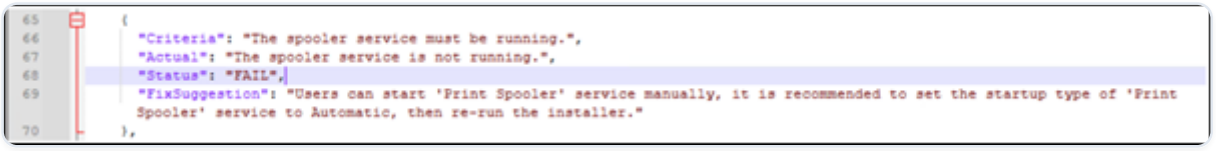


`.json` ファイルには以下が含まれます。

- 事前チェックのローカル終了時刻
- 全体的な結果
- 事前チェックの詳細
  - 基準
  - 実際の値
  - ステータス
  - 修正提案



`FAIL`のステータスを持つ各事前チェック項目に対する修正案は、`.json`ファイル内の事前チェックの詳細セクションに記載されています。



VDAメタインストーラーヘルパーツール

1. はじめに

VDAメタインストーラーヘルパーツールには、SCCMタスクシーケンスを介したVDAのインストールを支援する一連のツールと、インストールログを分析して潜在的な問題を特定するためのユーティリティが含まれています。

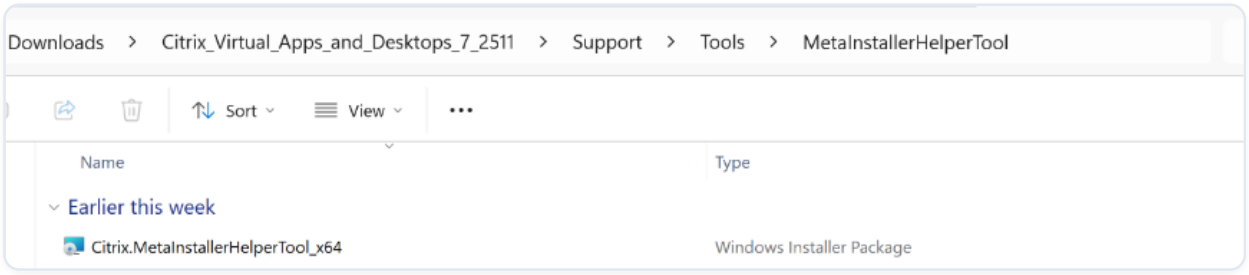
シンプルな MSI インストールと直感的なユーザーインターフェイスを備えたメタインストーラーヘルパーツールは、いくつかの重要な機能を提供します。

- **SCCMタスクシーケンスの確認:** このツールは、既存のSCCMタスクシーケンスを確認および検証し、VDAインストール要件との互換性を確保するのに役立ちます。

- **タスクシーケンスリファレンスの生成:** このツールは、参照タスクシーケンスを自動的に作成し、手動設定を最小限に抑えてVDAのインストールをSCCM展開ワークフローに統合するのに役立ちます。
- **VDAインストールログアナライザー:** このツールは、インストールログを確認して、エラー、警告、または障害を特定するのに役立ちます。このツールは、根本原因、考えられる解決策、および展開を成功させるための推奨事項を強調したレポートを生成します。

2. インストール

1. Citrix Virtual Apps and Desktops製品ISOをCitrix Virtual Apps and Desktopsダウンロードページからダウンロードします。
2. Citrix.MetaInstallerHelperTool_x64.msiを`\Support\Tools\MetaInstallerHelperTool`フォルダーから見つけます。



3. Citrix.MetaInstallerHelperTool_x64.msi をダブルクリックしてツールをインストールします。

> **注:**
>
> このツールは VDA の一部ではありません。VDA または任意のローカルデバイスにインストールできます。

4. インストール後、スタートメニューで「MetaInstallerHelperTool」を検索して、アプリケーションを管理者として起動します。

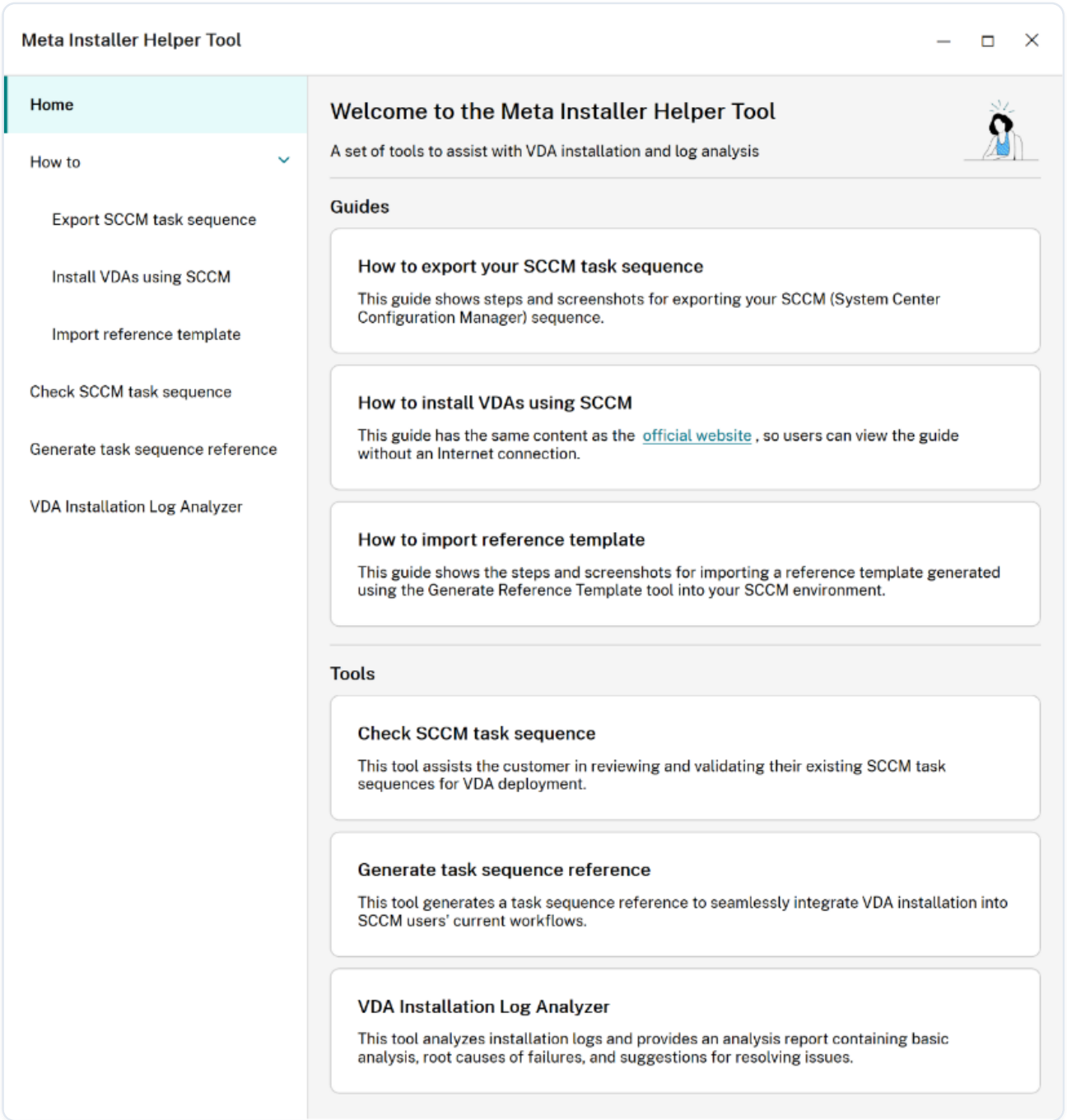


3. ユーザーインターフェイス (UI) の概要

アプリケーション「MetaInstallerHelperTool」を起動すると、直感的なナビゲーションと使いやすさを考慮して設計されたメインユーザーインターフェイスが表示されます。

「**Home**」セクションでは、「How to」セクションのガイドの説明と、SCCMシーケンスの確認、タスクシーケンステンプレートの生成、VDAインストールログの分析を行うツールの機能説明が提供されます。

これらのガイドとツールには、左側のナビゲーションパネルから対応するタブを選択することでアクセスできます。



「**How to**」セクションでは、タスクシーケンスのエクスポート、SCCMを使用したVDAのインストール、スクリーンショットと手順を含む参照テンプレートのインポートに関するガイドが提供されます。

- 「タスクシーケンスのエクスポート方法」を参照して、「SCCMタスクシーケンスの確認」ツールで使用するSCCMタスクシーケンスを取得してください。
- VDAをインストールするには、「SCCMを使用してVDAをインストールする方法」を参照してください。「SCCMタスクシーケンスの確認」ツールと「タスクシーケンステンプレートの生成」ツールもこのガイドを参照します。
- 「参照テンプレートのインポート方法」を参照して、「タスクシーケンステンプレートの生成」ツールで生成されたテンプレートを、参照テンプレートとしてSCCM環境にインポートしてください。

SCCMタスクシーケンスの確認、**タスクシーケンステンプレートの生成**、および**VDAインストールログアナライザー**の各セクションでは、Meta Installer Helper Toolの主要なタスクを実行できます。

4. ツール

1. SCCMタスクシーケンスの確認

   SCCM環境からエクスポートされたタスクシーケンスをアップロードして、レビューと検証を行います。

   このツールは、アップロードされたファイルがzipファイルであるか、必要なSCCMタスクシーケンスフォルダー構造、必要なオブジェクト.xmlファイル、および有効なタスクシーケンス定義が含まれているかを確認します。また、タスクシーケンスに基づいてコマンドラインパラメーター分析とインストール条件分析も行います。

   メタインストーラー SCCMチェック(/en-us/citrix-virtual-apps-desktops/2511/media/metainstaller-check-sccm.png)

2. タスクシーケンス参照の生成

   このツールは、SCCMを介したVDAインストールに関するCitrixの公式ガイドラインに従って、タスクシーケンステンプレートを生成します。

   これをSCCM環境にインポートして、VDAインストールをタスクシーケンスに組み込むための参照テンプレートとして使用できます。

   メタインストーラー タスクシーケンス生成(/en-us/citrix-virtual-apps-desktops/2511/media/metainstaller-generate-task-sequence.png)

3. VDA インストールログアナライザー

   自動モードを使用して VDA 上で直接インストールログを分析するか、VDA インストールログを含む .zip ファイルを手動でアップロードして分析します。

メタインストーラー ログアナライザー(/en-us/citrix-virtual-apps-desktops/2511/media/metainstaller-vda-log-analyzer.png)

VDA 上で **自動モード** で実行すると、ツールはログ保存パスを自動的に検出し、インストールログをローカルで分析します。分析結果は保存され、すべてのログファイルとレポートは単一の ZIP ファイルにパッケージ化されます。

メタインストーラー ログアナライザー 1(/en-us/citrix-virtual-apps-desktops/2511/media/metainstaller-vda-log-analyzer1.png)

手動モード では、分析のために VDA インストールログを含む .zip ファイルをアップロードする必要があります。デフォルトでは、ログファイルは次の場所に保存されます。 `%TEMP%\Citrix\XenDesktop Installer`

デフォルトのログパスが変更されている場合、Windowsレジストリで現在の場所を確認できます。 `Computer\HKLM\Software\Citrix\MetaInstall\LogPath`

ツールはアップロードされた.zipファイルを抽出し、その内容を分析し、分析結果を確認のために保存します。

メタインストーラー ログアナライザー 2(/en-us/citrix-virtual-apps-desktops/2511/media/metainstaller-vda-log-analyzer2.png)

スクリプトを使用してVDAをインストールする

> **注:**
>
> Citrixは、お客様の運用環境に合わせて調整されたスクリプトによって引き起こされる問題について責任を負いません。インストール関連のCitrixの問題については、Citrixサポートポータルを使用して、関連するインストールログとともにテクニカルサポートケースをオープンしてください。

> この記事は、Windowsオペレーティングシステムを搭載したマシンへのVDAのインストールに適用されます。Linuxオペレーティングシステム用VDAの詳細については、Linux Virtual Delivery Agentのドキュメントを参照してください。

インストールメディアには、Active Directory内のマシンにVirtual Delivery Agent (VDA) をインストール、アップグレード、または削除するサンプルスクリプトが含まれています。これらのスクリ

プトは、Machine Creation Services™およびCitrix Provisioning (旧Provisioning Services) で使用されるマスターイメージの保守にも使用できます。

必要なアクセス権：

- スクリプトには、VDAインストールコマンドが配置されているネットワーク共有への「Everyone読み取り」アクセス権が必要です。インストールコマンドは、製品版ISOでは `XenDesktopVdaSetup.exe`、スタンドアロンインストーラーでは `VDAWorkstationSetup.exe` または `VDAServerSetup.exe` です。
- ログの詳細は各ローカルマシンに保存されます。レビューと分析のために結果を一元的にログに記録するには、スクリプトには適切なネットワーク共有への「Everyone読み取りおよび書き込み」アクセス権が必要です。

スクリプト実行の結果を確認するには、中央ログ共有を調べます。取得されるログには、スクリプトログ、インストーラーログ、およびMSIインストールログが含まれます。各インストールまたは削除の試行は、タイムスタンプ付きのフォルダーに記録されます。フォルダーのタイトルは、PASSまたはFAILのプレフィックスで操作結果を示します。標準のディレクトリ検索ツールを使用して、中央ログ共有で失敗したインストールまたは削除を見つけることができます。これらのツールは、ターゲットマシンでローカルに検索する代替手段を提供します。

インストールを開始する前に、インストールの準備のタスクを読み、完了してください。

スクリプトを使用してVDAをインストールまたはアップグレードする

1. インストールメディアの\\Support\\AdDeploy\\からサンプルスクリプト**InstallVDA.bat**を入手します。Citrixは、スクリプトをカスタマイズする前に元のスクリプトのバックアップを作成することをお勧めします。
2. スクリプトを編集します。
    - インストールするVDAのバージョンを指定します: `SET DESIREDVERSION`。完全な値は、インストールメディアのProductVersion.txtファイルに記載されています。ただし、完全な一致は必須ではありません。
    - インストーラーが呼び出されるネットワーク共有を指定します。レイアウトのルート（ツリーの最上位）を指します。スクリプトの実行時に、適切なバージョンのインストーラー（32ビットまたは64ビット）が自動的に呼び出されます。例: `SET DEPLOYSHARE=\\fileserver1\share1`。
    - 集中ログを保存するためのネットワーク共有場所をオプションで指定します。例: `SET LOGSHARE=\\fileserver1\log1)`。

- コマンドラインを使用したインストールで説明されているように、VDA構成オプションを指定します。`/quiet`および`/noreboot`オプションは、スクリプトにデフォルトで含まれており、必須です: `SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT /NORESUME`。

3. グループポリシーのスタートアップスクリプトを使用して、スクリプトをマシンを含むOUに割り当てます。このOUには、VDAをインストールするマシンのみを含める必要があります。そのOU内のマシンが再起動されると、スクリプトはすべてのマシンで実行されます。サポートされているオペレーティングシステムを持つ各マシンにVDAがインストールされます。

スクリプトを使用してVDAを削除する

1. インストールメディアの\\Support\\AdDeploy\\からサンプルスクリプトUninstallVDA.batを入手します。Citrixは、元のスクリプトをカスタマイズする前にバックアップを作成することをお勧めします。
2. スクリプトを編集します。
   - 削除するVDAのバージョンを指定します: `SET CHECK\_VDA\_VERSION`。完全な値は、インストールメディアのProductVersion.txtファイル（例: 7.0.0.3018）に記載されています。ただし、完全一致は必須ではありません。
   - 集中ログを保存するためのネットワーク共有場所をオプションで指定します。
3. グループポリシーのスタートアップスクリプトを使用して、スクリプトをマシンを含むOUに割り当てます。このOUには、VDAを削除するマシンのみを含める必要があります。OU内のマシンが再起動されると、スクリプトはすべてのマシンで実行されます。VDAは各マシンから削除されます。

トラブルシューティング

- スクリプトは、スクリプトの実行状況を記述する内部ログファイルを生成します。スクリプトは、展開開始から数秒以内に`Kickoff_VDA_Startup_Script`ログを中央ログ共有にコピーします。これにより、全体的なプロセスが機能していることを確認できます。このログが期待どおりに中央ログ共有にコピーされない場合は、ローカルマシンを検査してさらにトラブルシューティングを行ってください。スクリプトは、各マシンの`%temp%`フォルダーに2つのデバッグログファイルを配置します。
  - `Kickoff_VDA_Startup_Script_<DateTimeStamp>.log`
  - `VDA_Install_ProcessLog_<DateTimeStamp>.log`

  スクリプトが次の状態であることを確認するために、これらのログを確認します。
  - 期待どおりに実行されている。

  - ターゲットオペレーティングシステムを適切に検出する。
  - `DEPLOYSHARE`共有の`ROOT`を指すように正しく構成されていること（`AutoSelect.exe`という名前のファイルが含まれています）。
  - `DEPLOYSHARE`と`LOG`の両方の共有に対して認証できること。

- Citrixがコンポーネントインストールの結果を報告する方法については、「Citrixインストールリターンコード」を参照してください。
- デリバリーグループのStudio表示では、**詳細**ペインの**インストール済みVDAバージョン**エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされても、Delivery Controllerに登録されるまでは、ユーザーにアプリやデスクトップを配信できません。

  VDA登録方法と登録の問題のトラブルシューティング方法については、「VDA登録」を参照してください。

コマンドラインでVDAをインストールまたはアップグレードするためのカスタムスクリプトを生成する

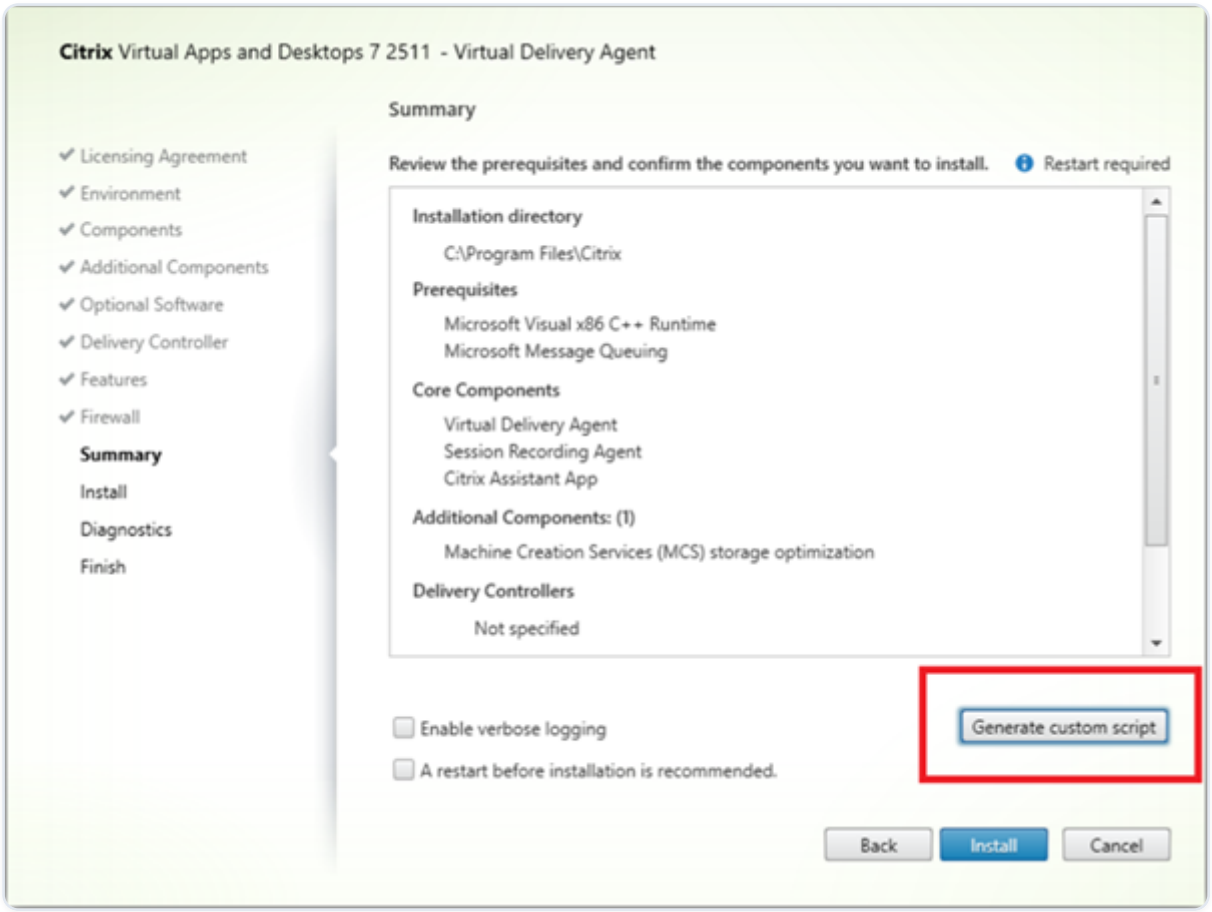
カスタムスクリプトの生成ボタンを使用すると、VDAインストールUIで行われた構成の選択に基づいて、バッチまたはスクリプトを作成できます。生成されたスクリプトはエクスポートして、コマンドラインから無人インストールまたはアップグレードを実行するために使用できます。この機能は、展開の自動化、構成の正確性の確保、手動スクリプト作成エラーの削減に役立ちます。

VDAインストールUIからコマンドラインスクリプトを生成するには、次の手順を使用します。

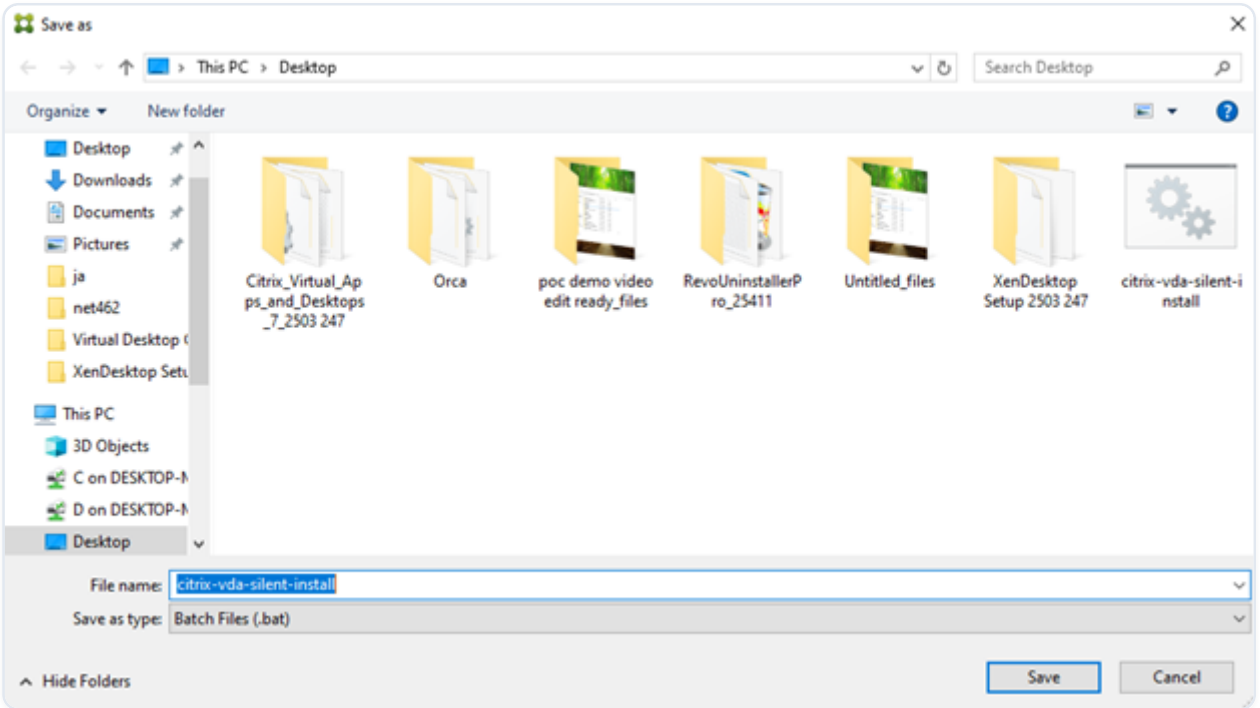
ステップ1：インストーラーUIからカスタムスクリプトを生成する

> **注:**
>
> この機能はUIモードでのみサポートされています。

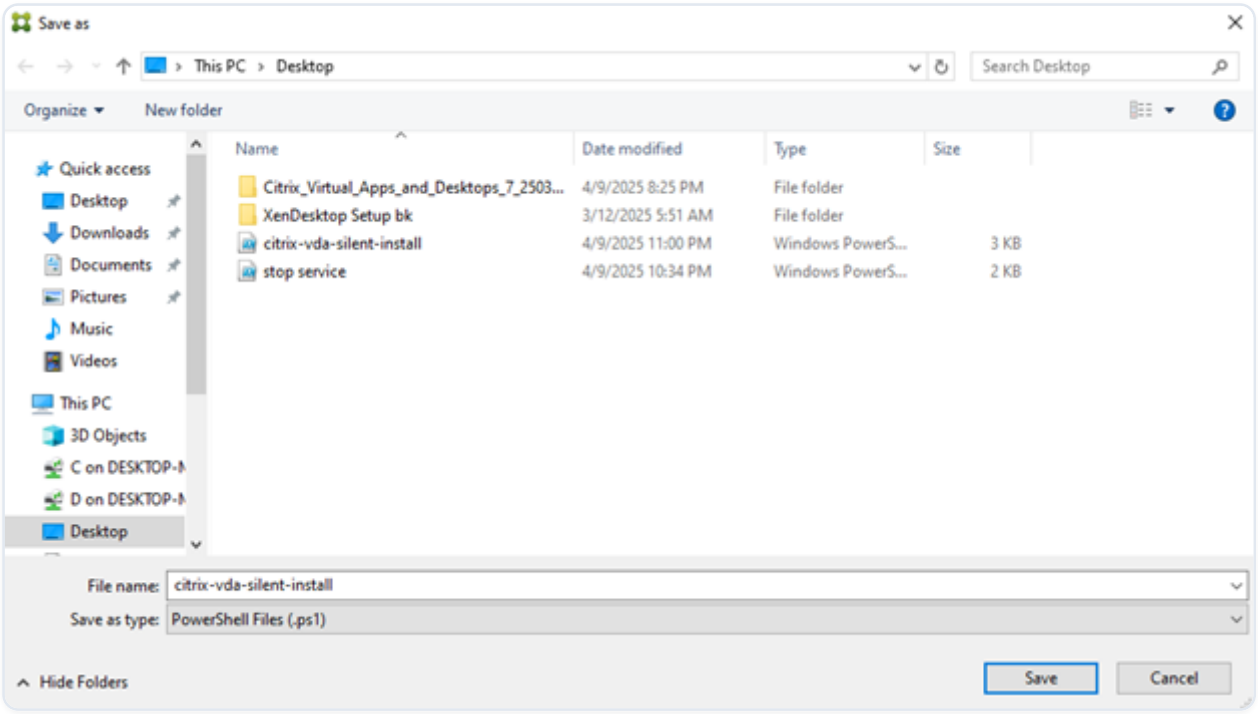
> 通常どおりUIでVDAのインストールオプションを構成します。**概要**ページで、**カスタムスクリプトの生成**を選択して、次のスクリーンショットに示すように、構成に基づいてコマンドラインスクリプトを作成します。



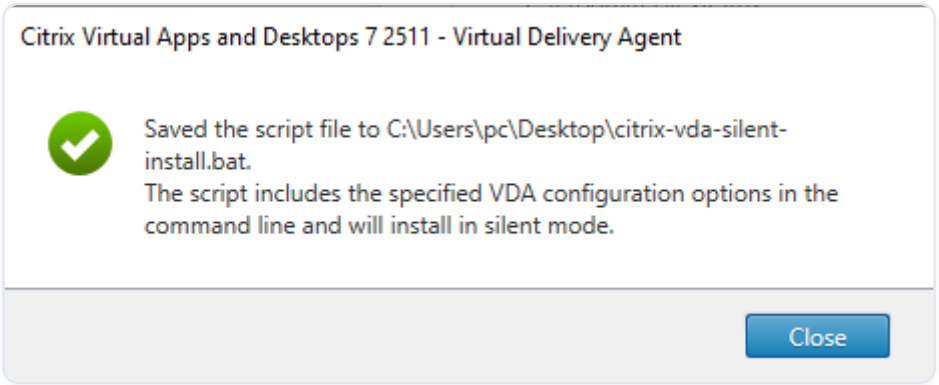
生成されたスクリプトを保存する場所を選択するダイアログボックスが表示されます。別のディレクトリを選択し、保存する前にスクリプトの名前を変更することもできます。



デフォルトでは、スクリプトはバッチ（.bat）ファイルとして保存されます。PowerShell（.ps1）スクリプトとして保存することもできます。

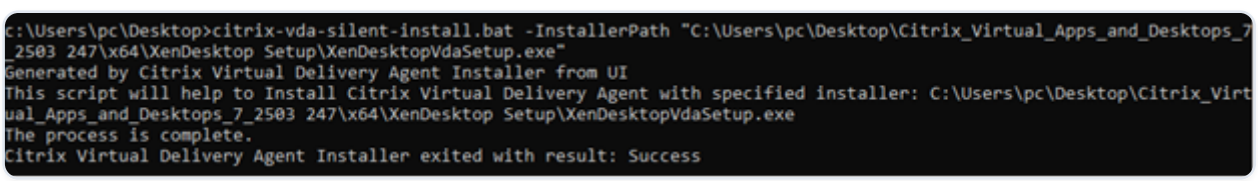


スクリプトが生成されて保存されると、ファイルの位置とスクリプトの目的を示す確認ダイアログが表示されます。生成されたスクリプトは、メモ帳などの任意のテキストエディターを使用して編集できます。スクリプトを実行する前に、インストーラーUIを終了してください。一度に実行できるVDAのインストールまたはアップグレードプロセスは1つだけです。

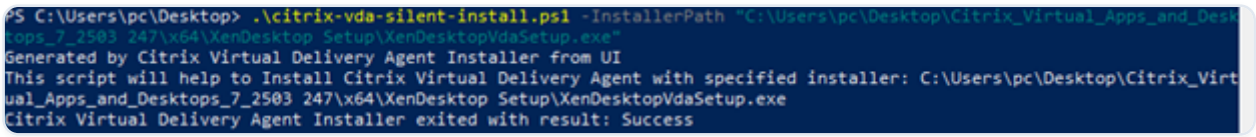


ステップ2. 生成されたスクリプトを使用してVDAをインストールまたはアップグレードする

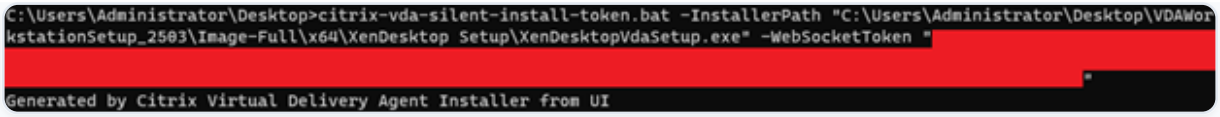
生成されたバッチファイルを使用してVDAをインストールまたはアップグレードする方法を次のスクリーンショットに示します。唯一の必須パラメーターは、VDAインストーラーへのパスです。インストーラーのパスが有効な場合、スクリプトはインストールまたはアップグレードを実行し、VDAインストーラーと同じ終了コードで終了します。プロセスの結果を示す読みやすい結果メッセージが表示されます。



生成されたPowerShellスクリプトを使用してVDAをインストールまたはアップグレードする方法を次のスクリーンショットに示します。唯一の必須パラメーターは、VDAインストーラーへのパスです。インストーラーのパスが有効な場合、スクリプトはインストールまたはアップグレードを実行し、VDAインストーラーと同じ終了コードで終了します。プロセスの結果を示す読みやすいステータスメッセージが表示されます。



> **注：**
>
> Delivery Controllerが登録トークンで構成されている場合は、次のスクリーンショットに示すようにスクリプトを実行します。



スクリプトには、次のパラメーターが必要です: `<Path-to-generated-script>`、`<Path-to-vda-installer>`、`<Websocket-token-value>`。

サードパーティ製VDAの展開方法

Microsoft System Center Configuration Manager (SCCM) や、Ansible、Microsoft Intunes などの同様のソフトウェア配布ツールを使用して Virtual Delivery Agent (VDA) を正常に展開するには、Citrix® は、VDA インストーラーを段階的に使用することを推奨します。

> **注:**
>
> 以下の記事では、Citrix が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、お客様のニーズに合わせてカスタマイズできます。Citrix は、お客様のニーズに合わせてこれに必要な更新や調整について責任を負いません。

- SCCM を使用した VDA のインストール
- Ansible を使用した VDA のインストール
- Microsoft Intune を使用した VDA のインストール

SCCM を使用した VDA のインストール

概要

Microsoft Endpoint Configuration Manager は、以前は System Center Configuration Manager (SCCM) と呼ばれており、企業全体のデバイスとアプリケーションの管理、展開、セキュリティを可能にする Windows 製品です。

> **注：**
>
> 以下の記事では、Citrix® が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、必要に応じてカスタマイズできます。Citrix は、顧客のニーズに合わせてこれに必要な更新や調整について責任を負いません。

推奨事項

- SCCM または類似のソフトウェア配布ツールを使用して Virtual Delivery Agent (VDA) を正常に展開するには、Citrix は 一連の手順で VDA インストーラーを使用する ことを推奨します。
- Citrix は、VDA のインストールまたはアップグレードの一部として VDA Cleanup Utility を使用することを推奨しません。VDA インストーラーが以前に失敗した場合にのみ、VDA Cleanup Utility を使用してください。

始める前に

VDA のインストール中に必要な再起動の回数は、環境によって異なります。例：

- 以前のソフトウェアインストールによる保留中の更新または再起動のために、再起動が必要になる場合があります。
- 以前に他のプロセスによってロックされていたファイルは、更新が必要になる場合があり、追加の再起動を強制します。
- VDA インストーラーの一部のオプションコンポーネント（Citrix Profile Management や Citrix Files など）は、再起動が必要になる場合があります。
- VDA をアップグレードする場合、それがインストールされているマシンは、セッションがない状態でメンテナンスモードになっている必要があります。
- マシンで VDA のインストールが初めて実行されると、使用されている VDA インストーラーがそのマシンにコピーされます。 VDA のインストールに関する詳細については、インストーラー を参照してください。

SCCM Task Sequencer が必要なすべての再起動を管理します。

SCCM を使用して VDA を展開するための主要な手順

次の手順では、仮想マシンで SCCM を使用して VDA を展開する方法について説明します。

1. VDA をインストールする。
2. 組織単位 (OU) を作成する。
3. マシンを検証する。
4. VDA を使用してコンテンツを配布する。

ステップ 1：VDA をインストールする

すべての前提条件を特定した後、**SCCM Task Sequencer** を使用して次のタスクを完了します。

1. インストールメディアのアクセス可能なコピーから、またはVDAスタンドアロンインストーラーのいずれかからVDAをインストールします。

   - `VDAWorkstationSetup_XXXX.exe`
   - `VDAServerSetup_XXXX.exe`
   - `VDAWorkstationCoreSetup_XXXX.exe`

   VDA インストーラーについて詳しくは、「インストーラー」を参照してください。

   > **注：**
   >
   > VDAをアップグレードする場合、それがインストールされているマシンは、セッションがない状態でメンテナンスモードになっている必要があります。

2. マシン上でVDAのインストールが初めて実行されると、使用されているVDAインストーラーはそのマシンにコピーされます。

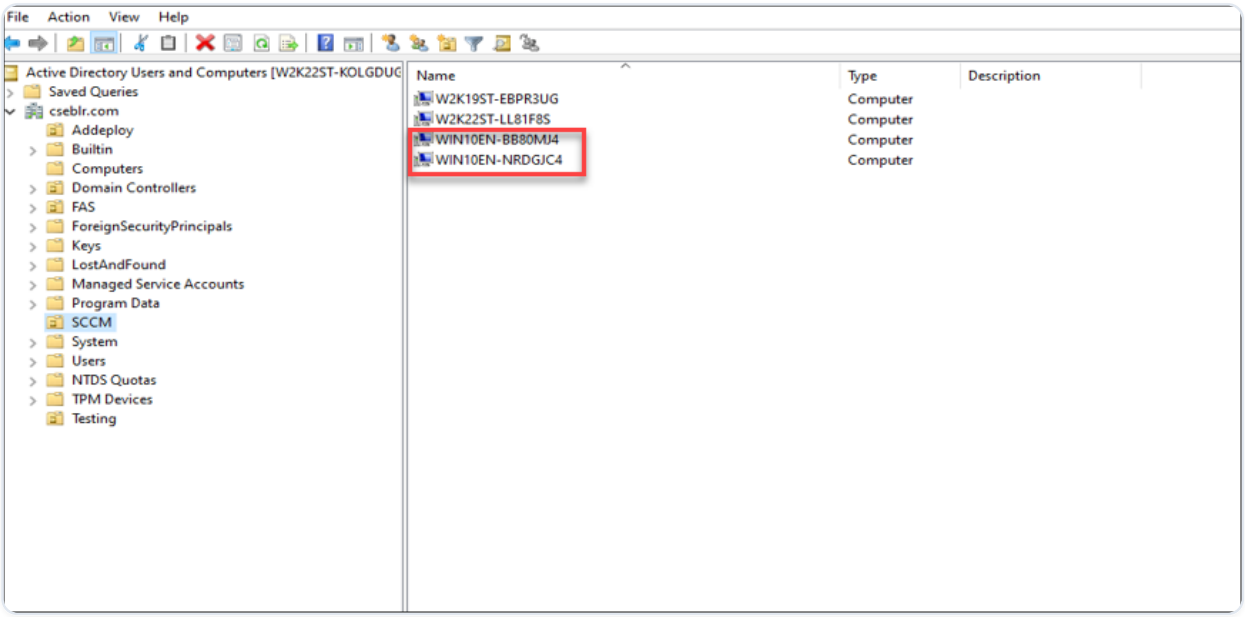
   - `VDAWorkstationCoreSetup_XXXX.exe` 以外のVDAインストーラーを使用する場合、VDAインストーラーは `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe` にコピーされます。
   - `VDAWorkstationCoreSetup_XXXX.exe` を使用する場合、VDAインストーラーは `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe.` にコピーされます。

3. VDAインストーラーのディレクトリの場所は、レジストリ `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall” “MetaInstallerInstallLocation”` にも保存されます。

4. コマンドラインオプションに`/NOREBOOT`、`/NORESUME`、および`/QUIET`を追加します。
   - `/QUIET`: インストール中にユーザーインターフェイスを表示しないようにします。これにより、SCCMがインストールプロセスを制御できます。
   - `/NOREBOOT`: VDAインストーラーが自動的に再起動するのを抑制します。SCCMは必要に応じて再起動をトリガーします。
   - `/NORESUME`: 通常、インストール中に再起動が必要な場合、VDAインストーラーはrunonceレジストリキー(`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`)を設定します。Windowsは、マシンが再起動したときにVDAインストーラーを開くためにこのキーを使用します。これはSCCMにとって問題となります。なぜなら、SCCMはインストールを監視して終了コードをキャプチャできないためです。

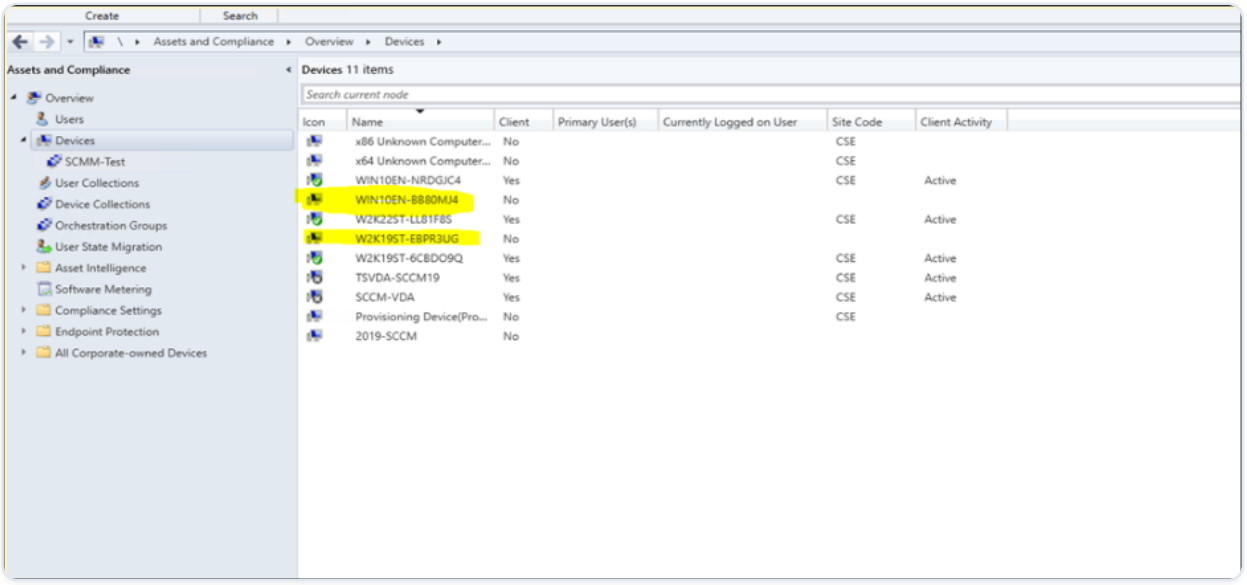
ステップ2：組織単位（OU）を作成する

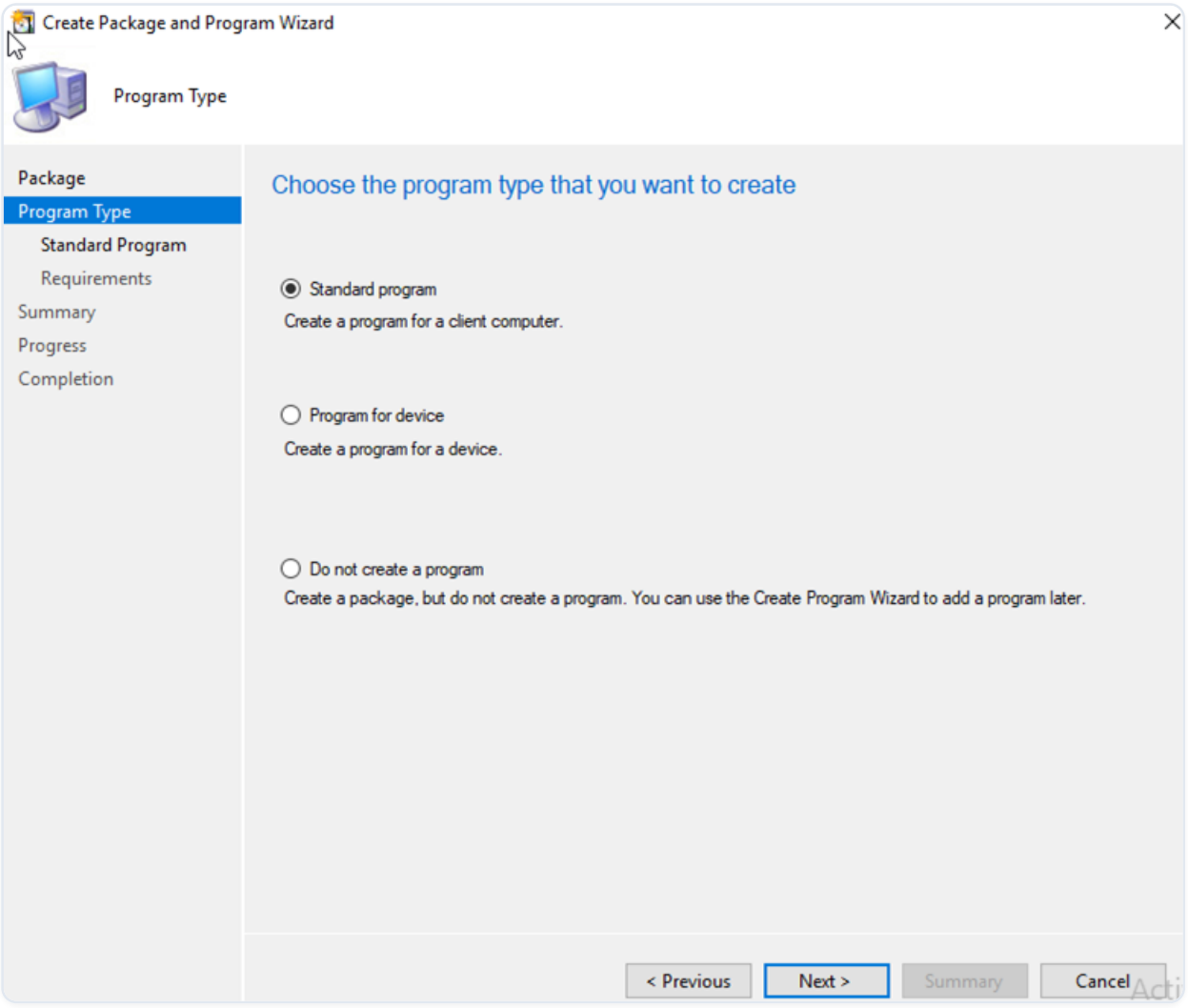
1. OU に追加するドメイン参加済み仮想マシンを 2 台作成します。仮想マシンが最初に作成されると、**Computers** フォルダーにあります。仮想マシンを **SCCM** フォルダーに移動します。
   例: WIN10EN-BB80MJ4.cseblr.com W2K19ST-EBPR3UG.cseblr.com



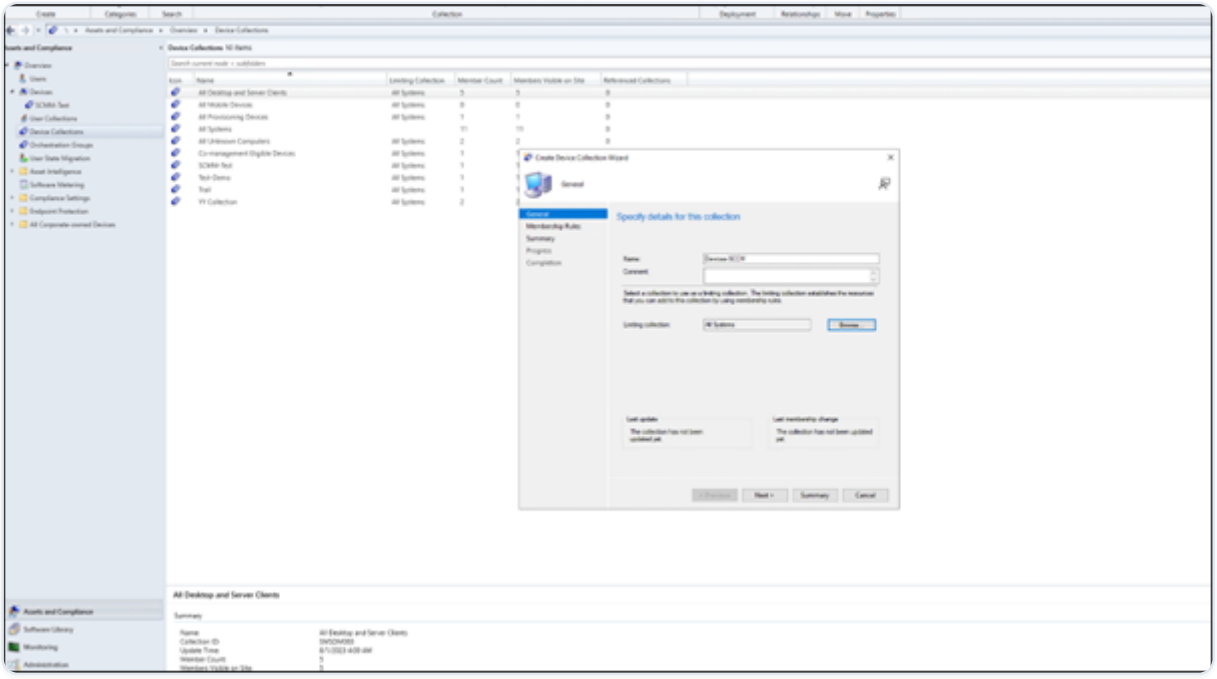
2. Microsoft Configuration Manager で、`\Administration\Overview\Hierarchy Configuration\Discovery Methods\` に移動します。
3. **Active Directory システム検出**をクリックし、**Active Directory システム検出を有効にする**チェックボックスを選択して、新しく作成された仮想マシンの自動検出を有効にします。
4. 新しいコンテナーを選択するには、アイコンをクリックします。
5. 「**Location**」セクションで、SCCM仮想マシンが配置されている「**Path**」を追加します。

6. `\Administration\Overview\Site Configuration\Sites` に移動し、SCCM VDA を右クリックします。
7. 「**Client Installation Settings > Client Push Installation**」を選択します。「**Client Push Installation Properties**」ウィンドウが開きます。
8. VM が `Enabled` に設定されると、以下の画像に示すように VM のリストが表示されます。

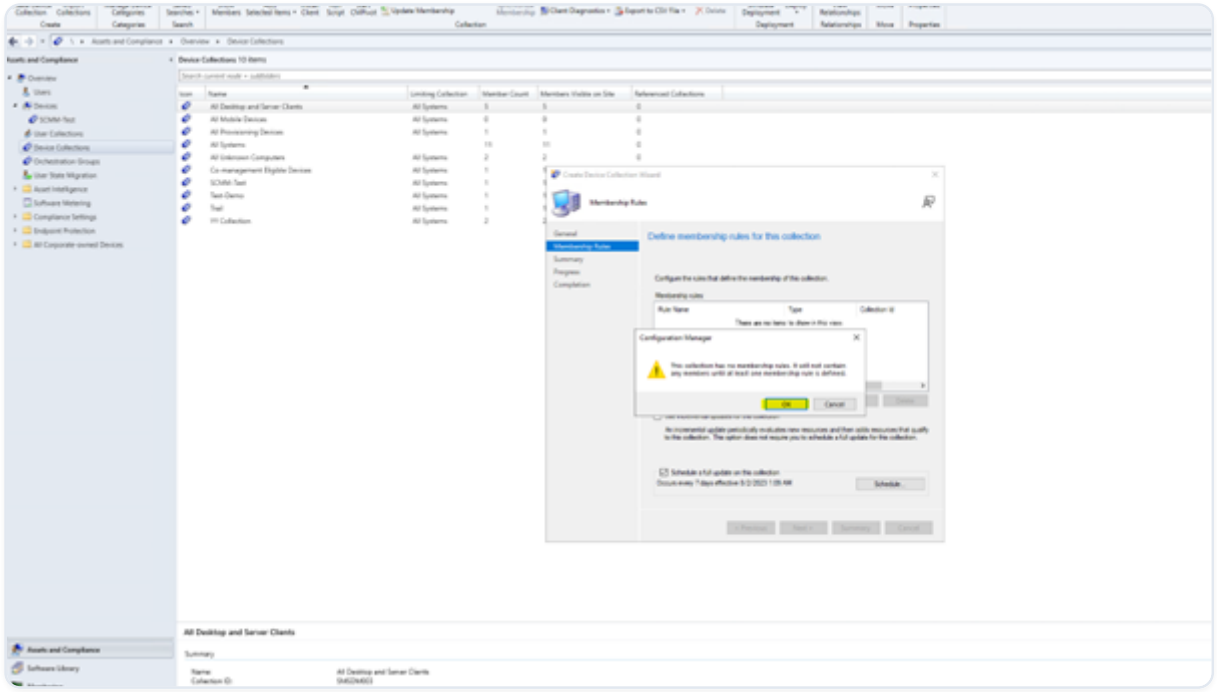




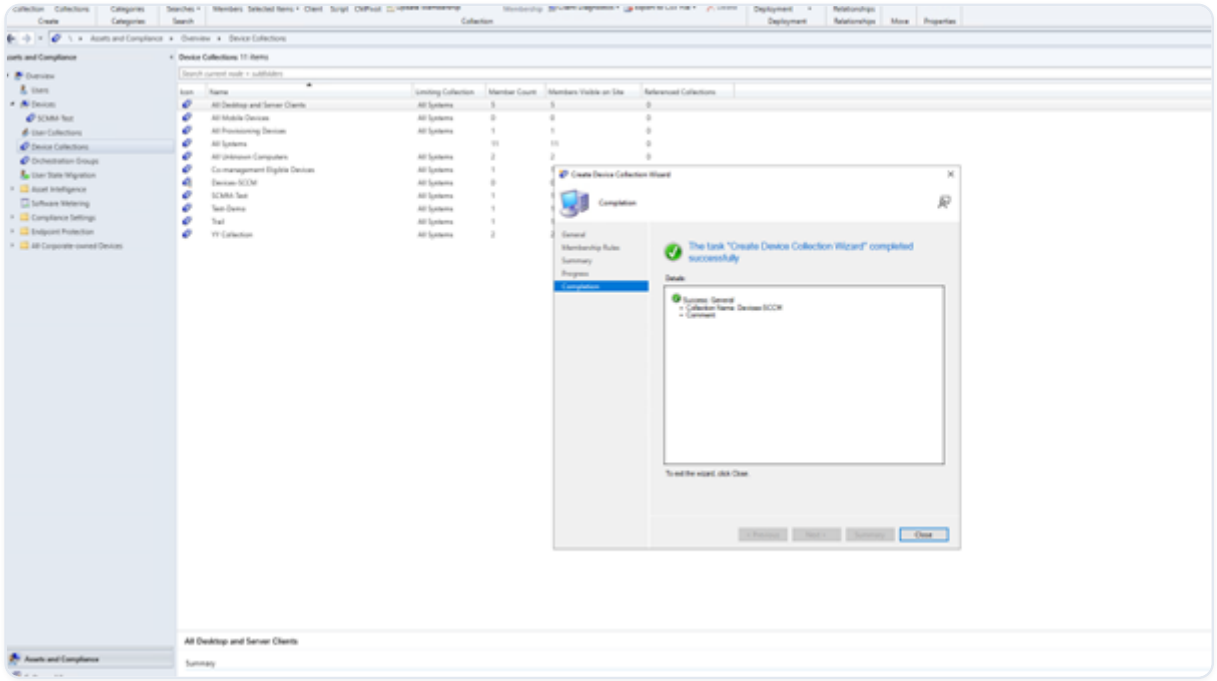
9. OU を作成するために「**Device collection**」を作成します。コレクション名の「**Name**」を入力します。



10. ウィザードの指示に従います。

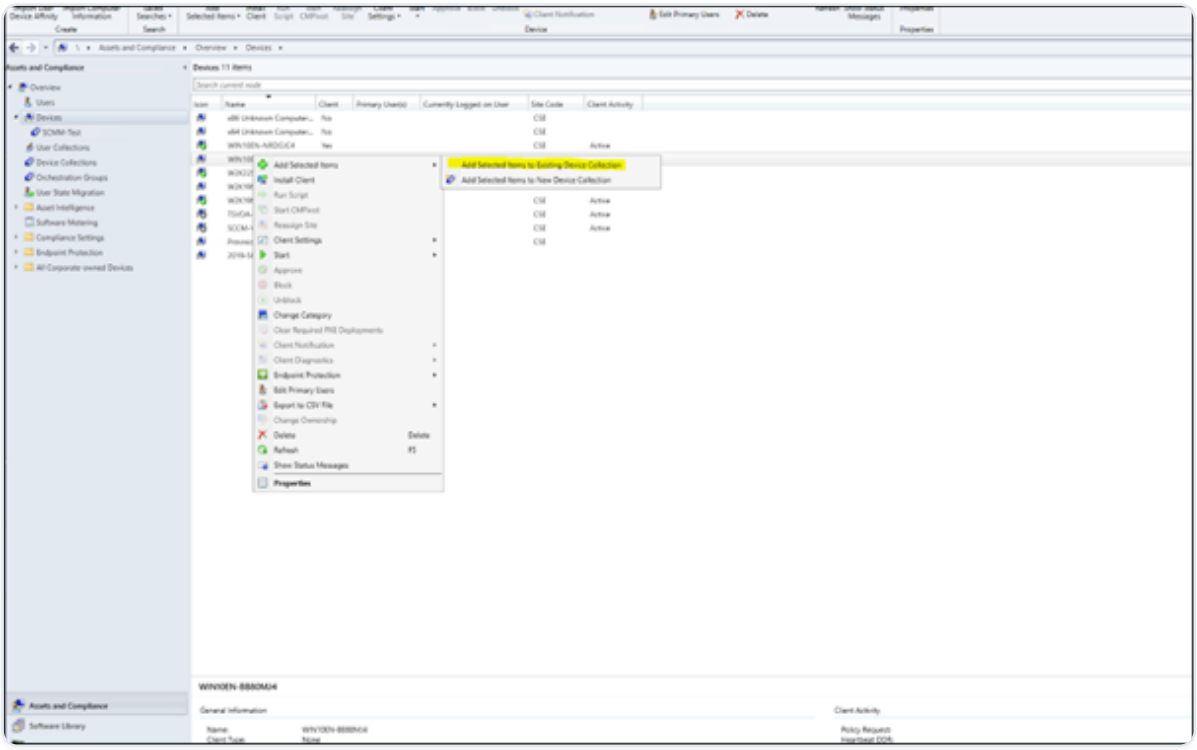


OU が作成されます。

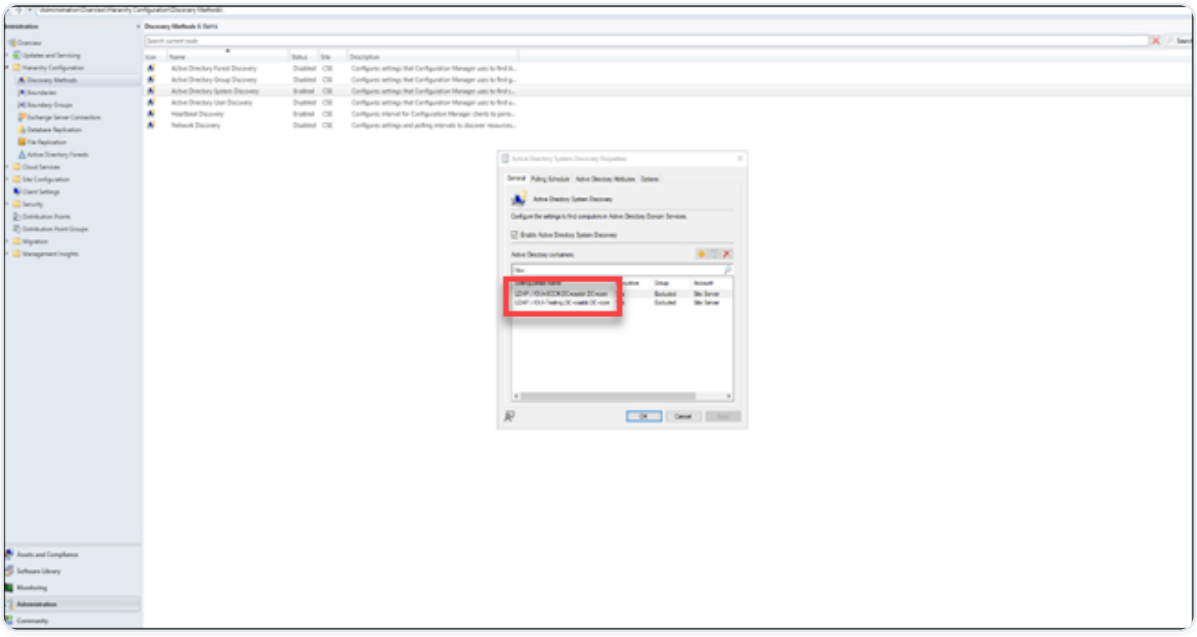


11. 作成した VM を新しく作成したデバイスコレクションに追加します。

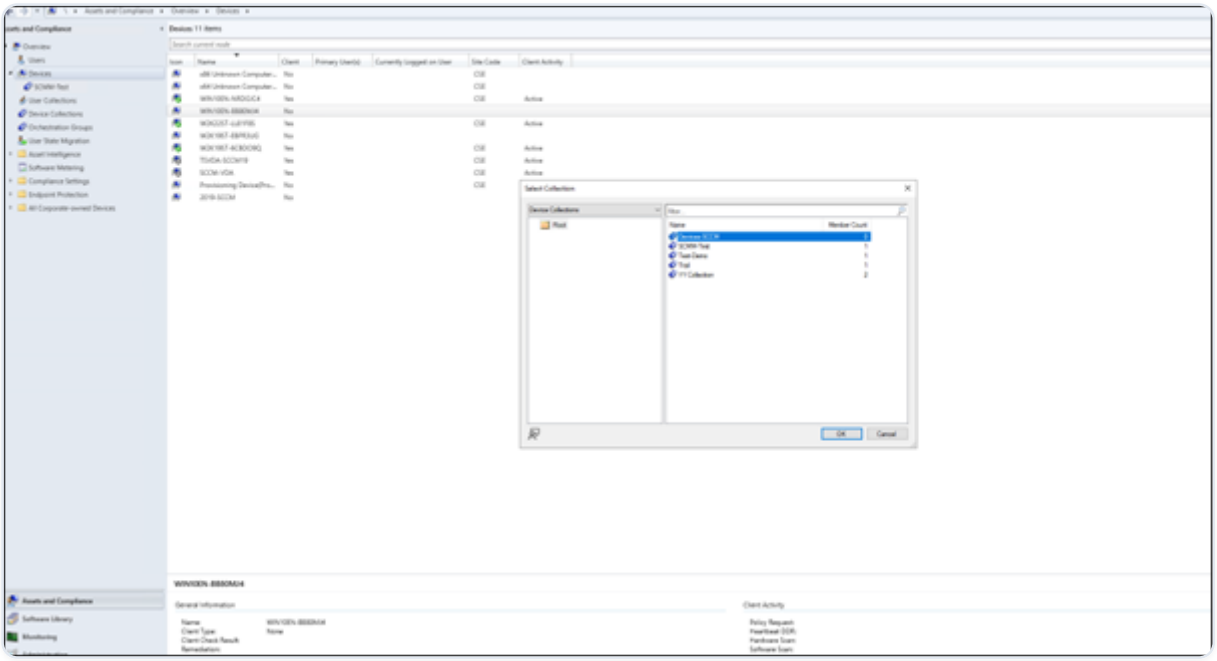
    a. VM を右クリックします。「**Add Selected Items > Add Selected Items to Existing Device Collection**」を選択します。



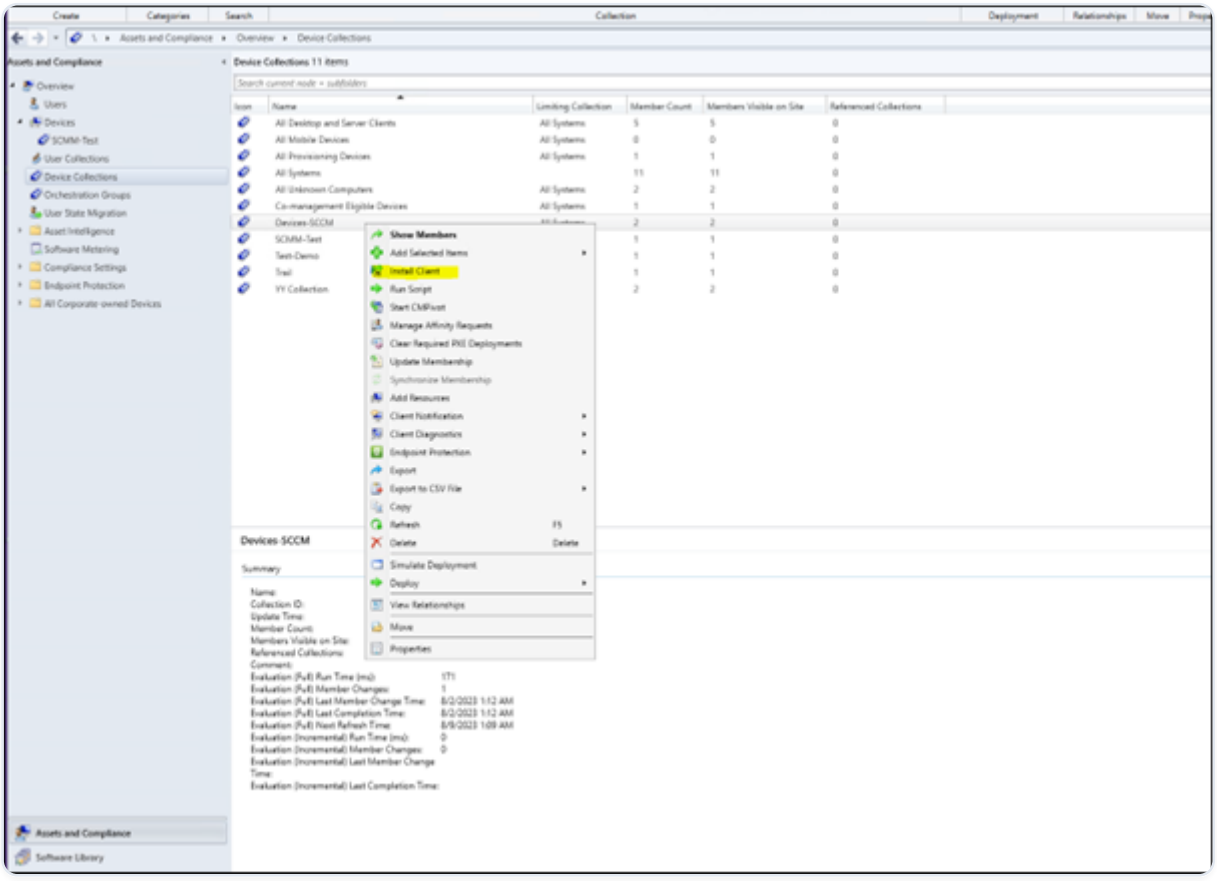
b. 「**コレクションの選択**」ウィンドウで、必要なデバイス名を選択します。この例では、`Devices-SCCM` です。



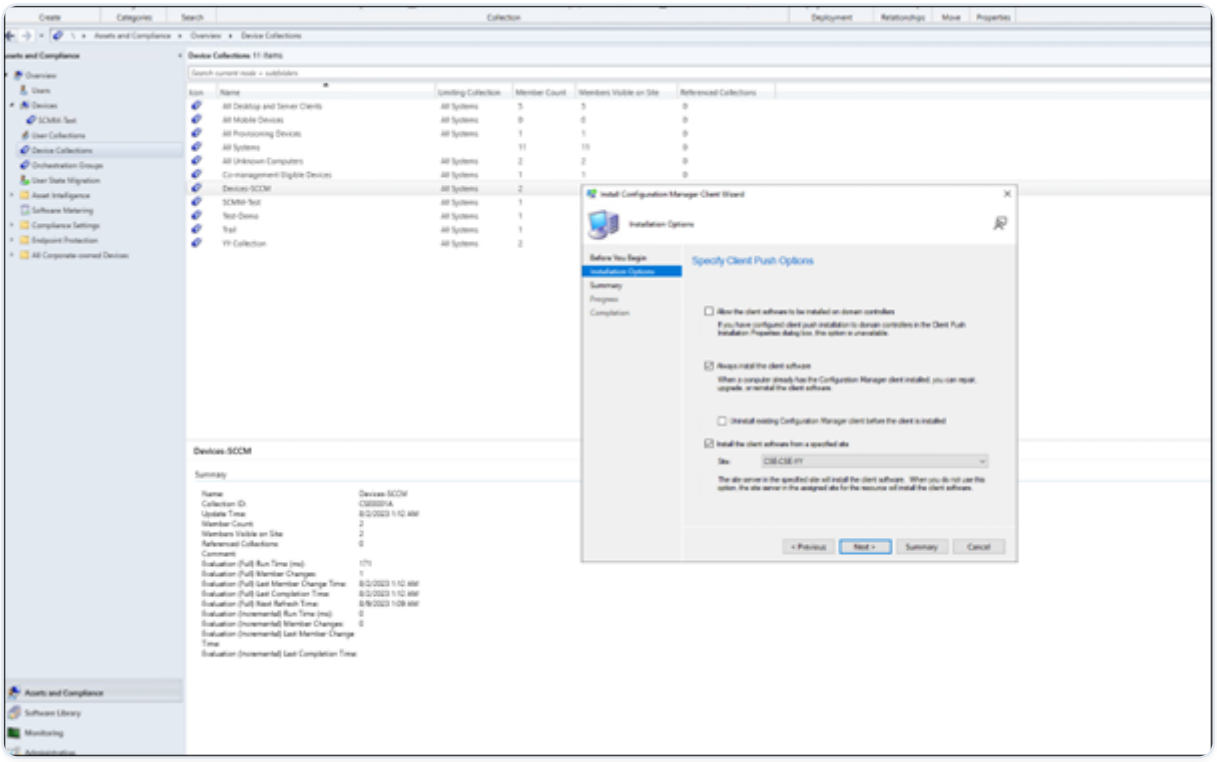
`Devices-SCCM` は、**資産とコンプライアンス > 概要 > デバイスコレクション**に表示されます。



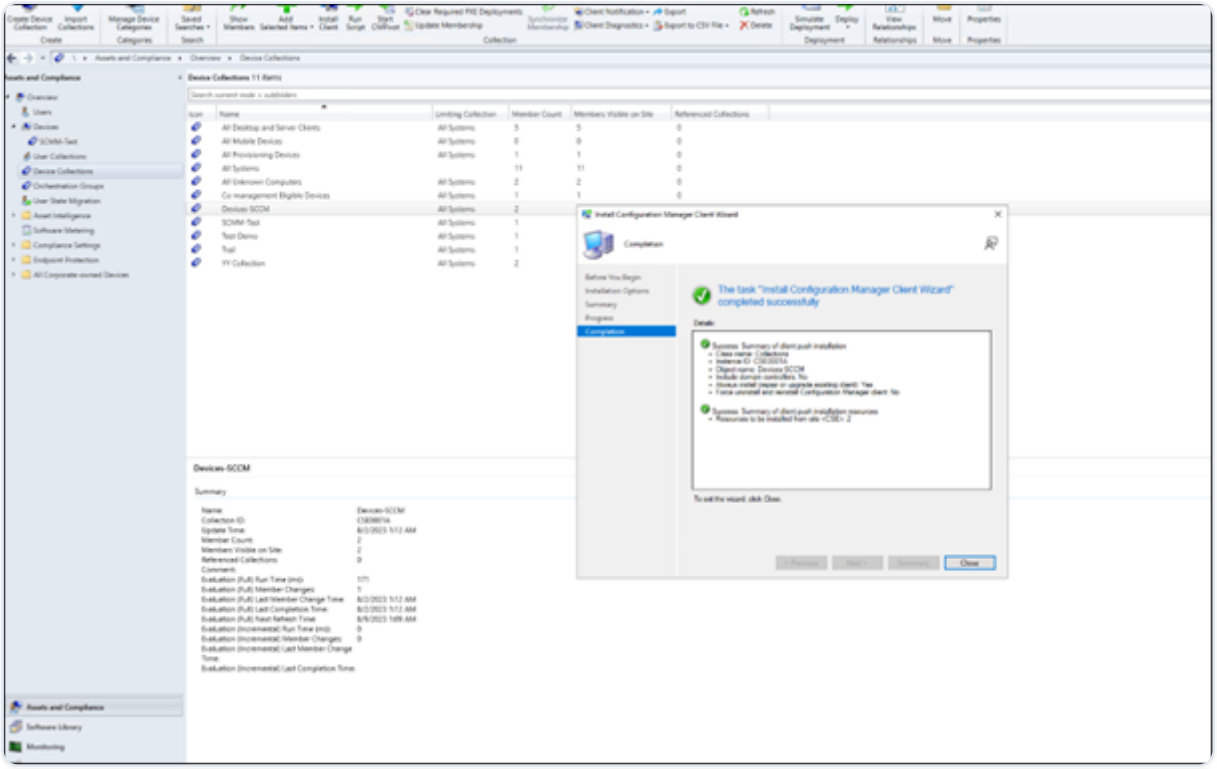
12. デバイスコレクターで「**クライアントのインストール**」を選択します。



13. 必要なインストール**サイト**を選択します。



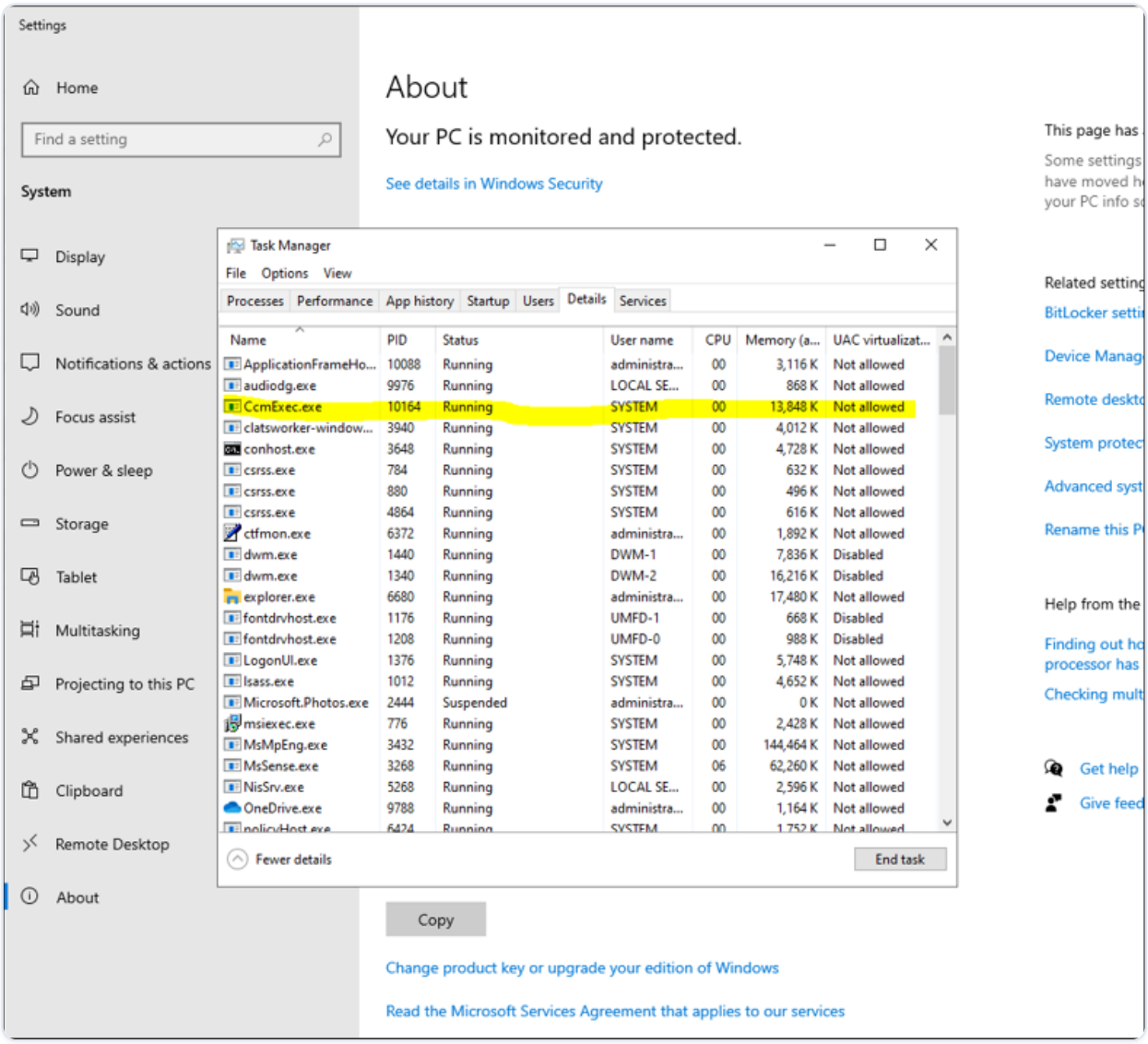
14. ウィザードの指示に従います。**Install Configuration Manager Client Wizard** が正常に完了しました。



詳細については、Microsoft ドキュメントのコレクションの管理を参照してください。

ステップ3：マシンの確認

1. クライアントマシンで、`CCMExec` プロセスが実行されていることを確認して、クライアントがインストールされていることを検証します。



2. SCCM上のVMでクライアントが実行されていることを確認します。

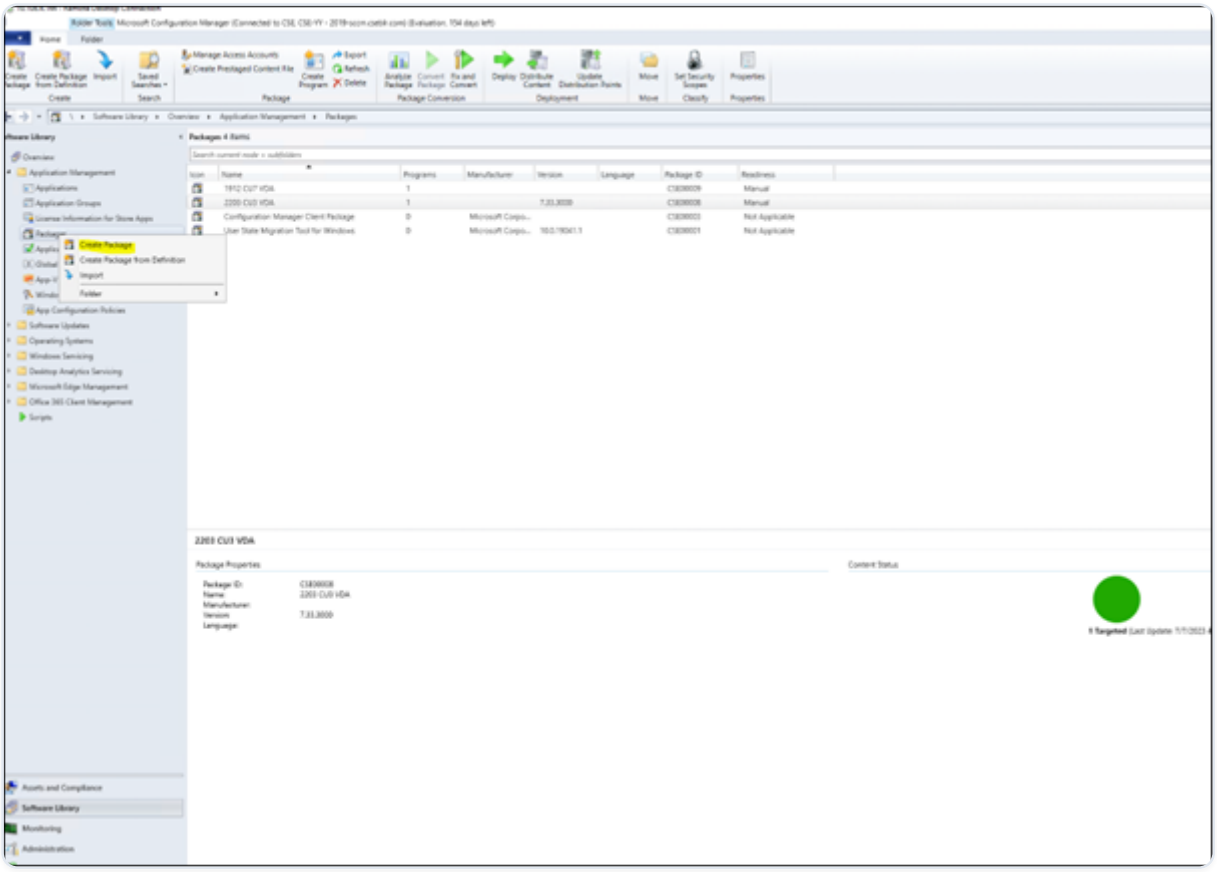
ステップ4: VDAを使用してコンテンツを配布する

以下の手順では、展開されたVDAを使用して、関連付けられた仮想マシンにコンテンツを配布する方法について説明します。

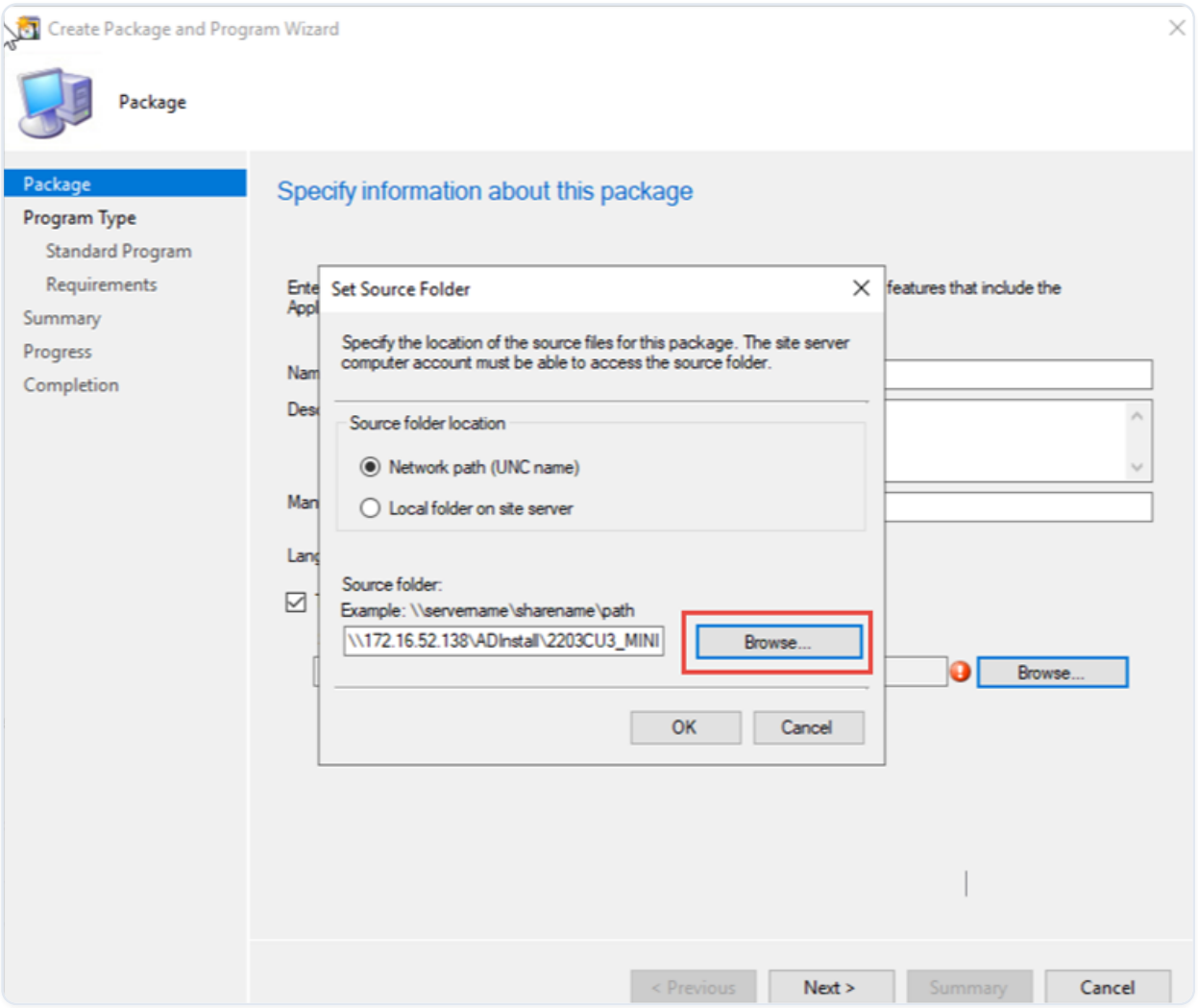
1. パッケージの作成
2. コンテンツを配布する(#distribute-content)

パッケージの作成

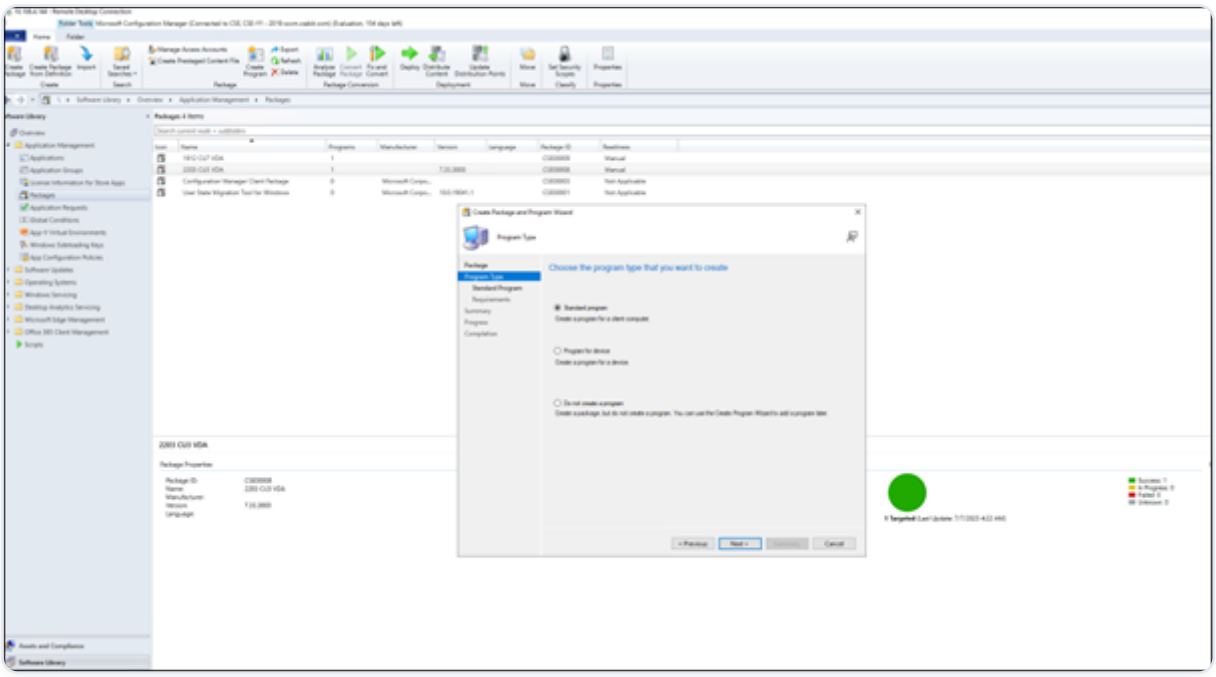
1. パッケージを作成するには、目的のVDAを右クリックし、**パッケージの作成**をクリックします。



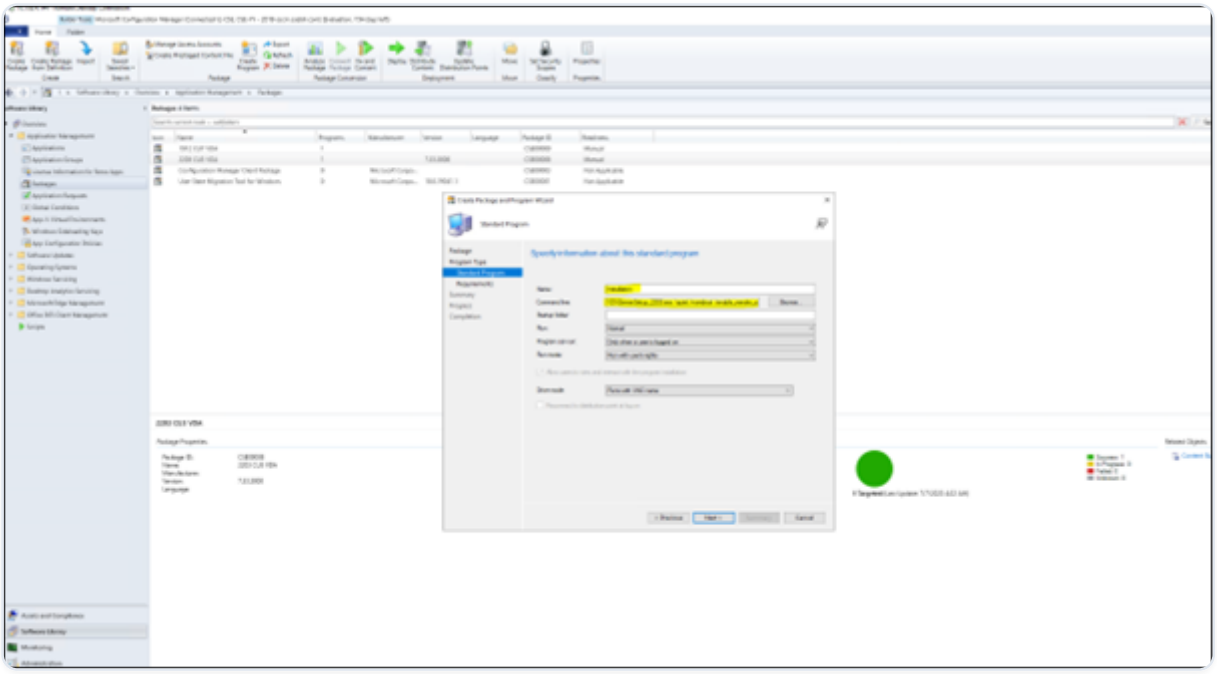
2. このパッケージのソースファイルの場所を指定するには、**参照**をクリックします。



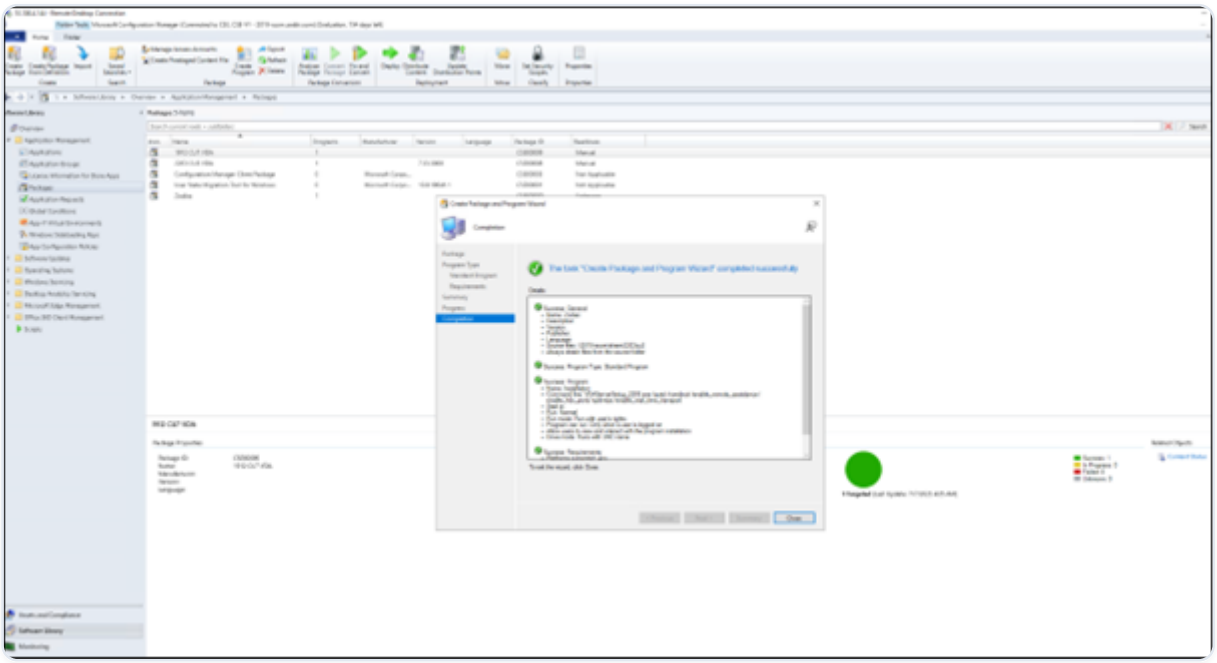
3. 目的のパッケージの種類を選択します。



4. パッケージの**名前**と**コマンドライン**を入力します。



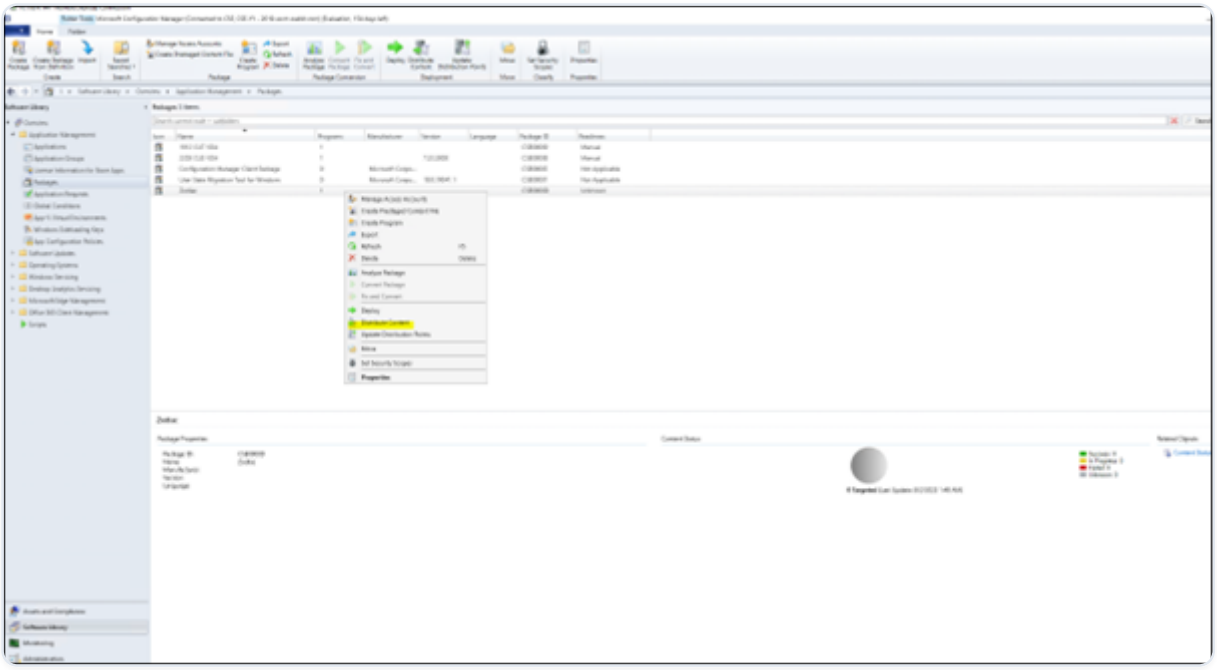
5. **次へ**をクリックします。



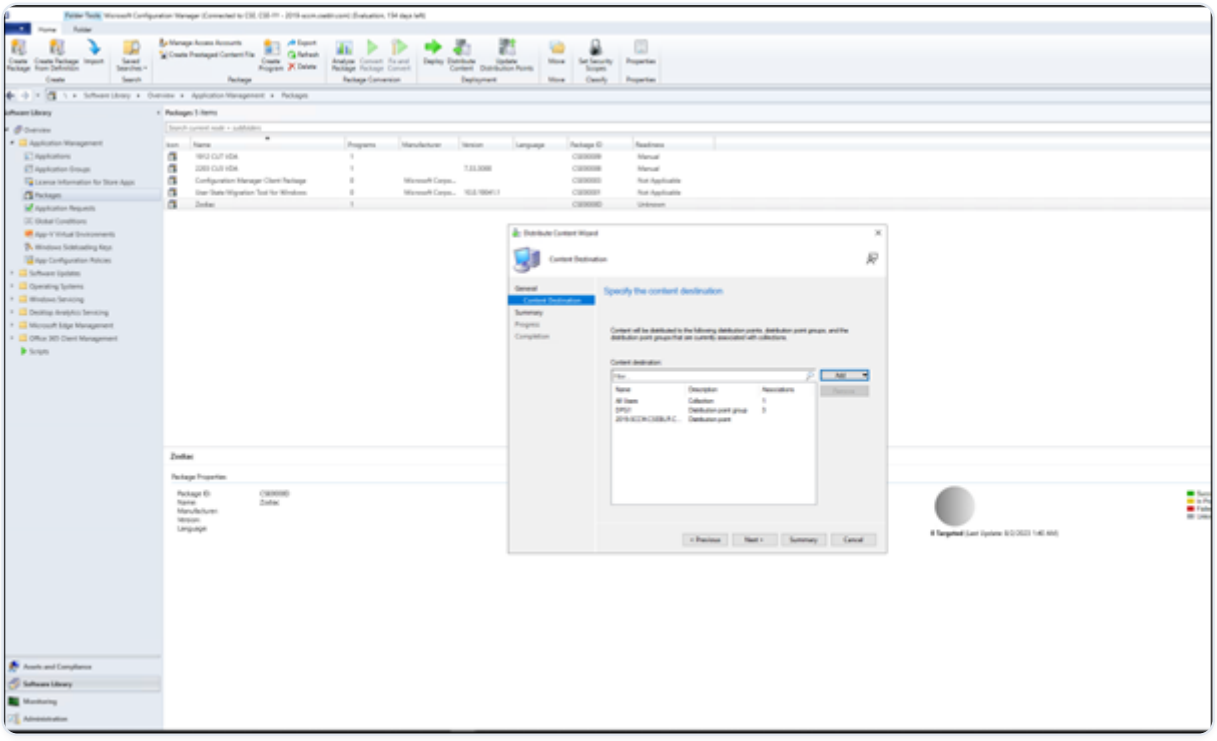
詳細については、Microsoft ドキュメントのConfiguration Manager のパッケージとプログラムを参照してください。

コンテンツの配布

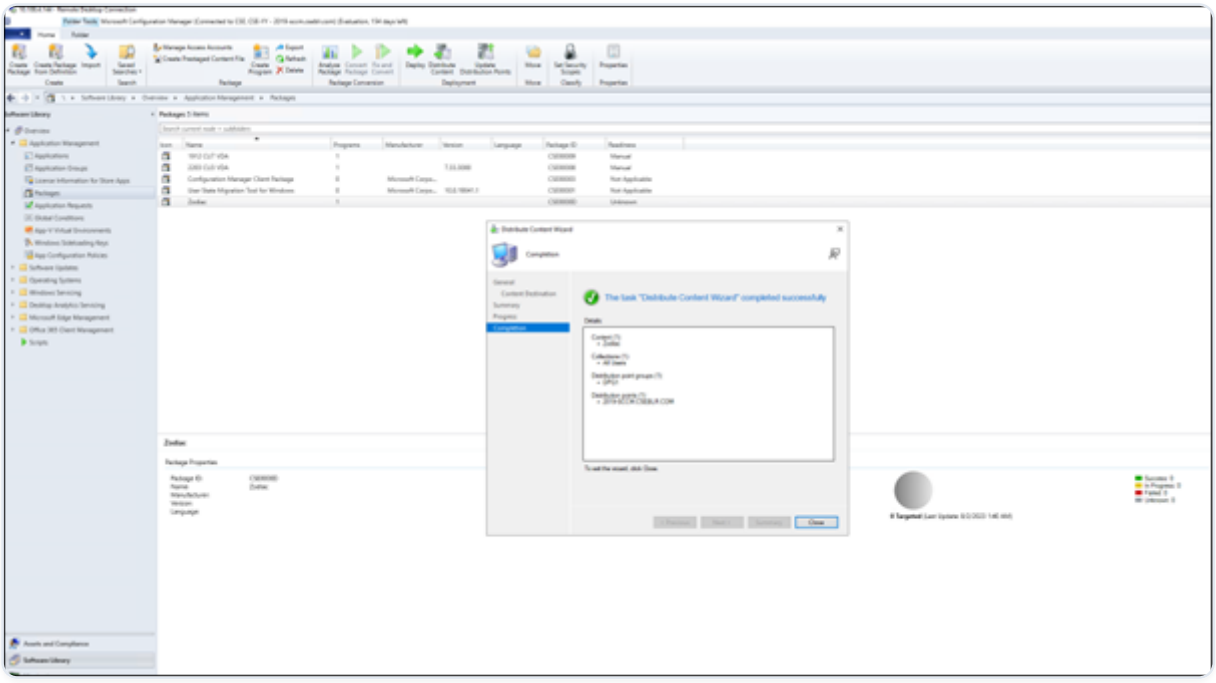
1. 作成したパッケージ名を右クリックします。
2. **コンテンツの配布**を選択します。



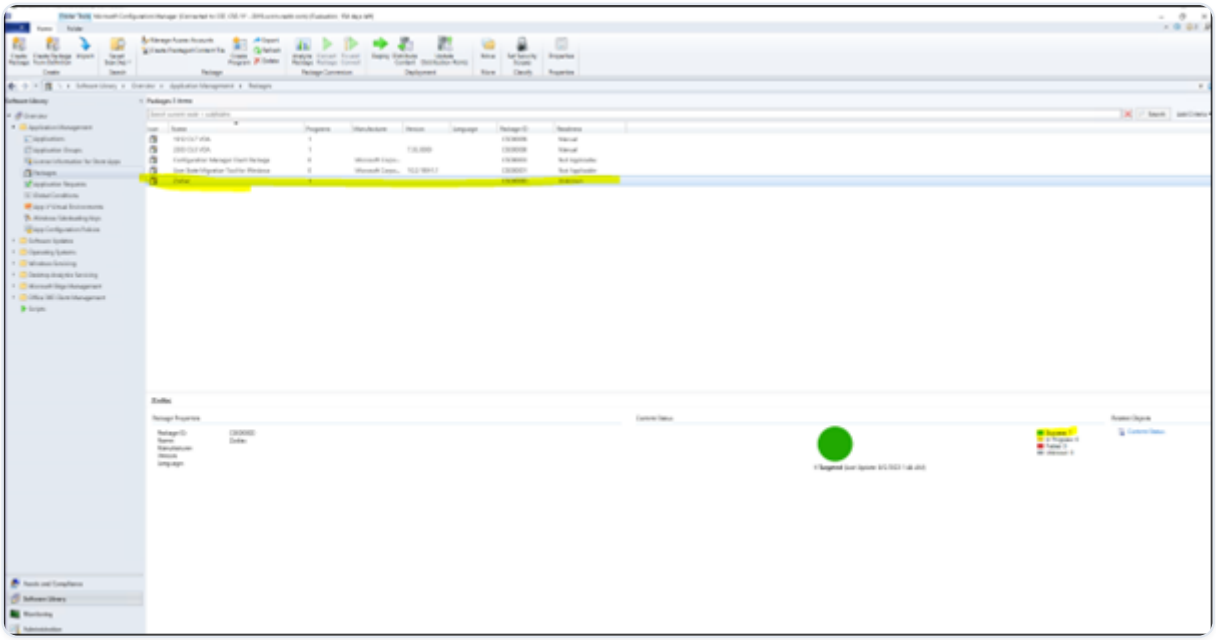
3. **コンテンツの配布ウィザード**ウィンドウで、作成したパッケージのソースファイルの場所を選択します。この例では、`2019-SCCM`です。**次へ**をクリックします。



4. パッケージ (この例では、`Zodiac`) が展開可能であることを確認します。



以下の画像は、パッケージが展開可能であることを示しています。

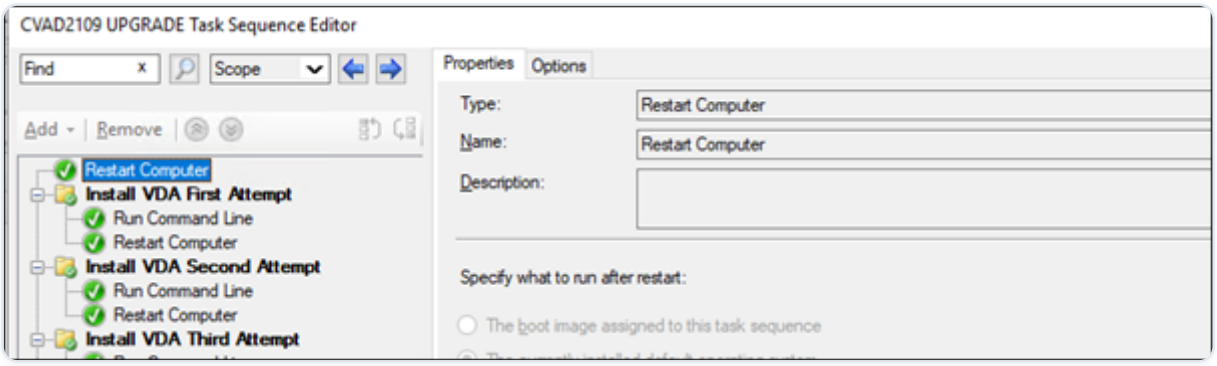


詳細については、Microsoft ドキュメントのConfiguration Manager のコンテンツを展開および管理するを参照してください。

SCCM を使用したインストールシーケンスの例

次の例は、インストールシーケンスを示しています。

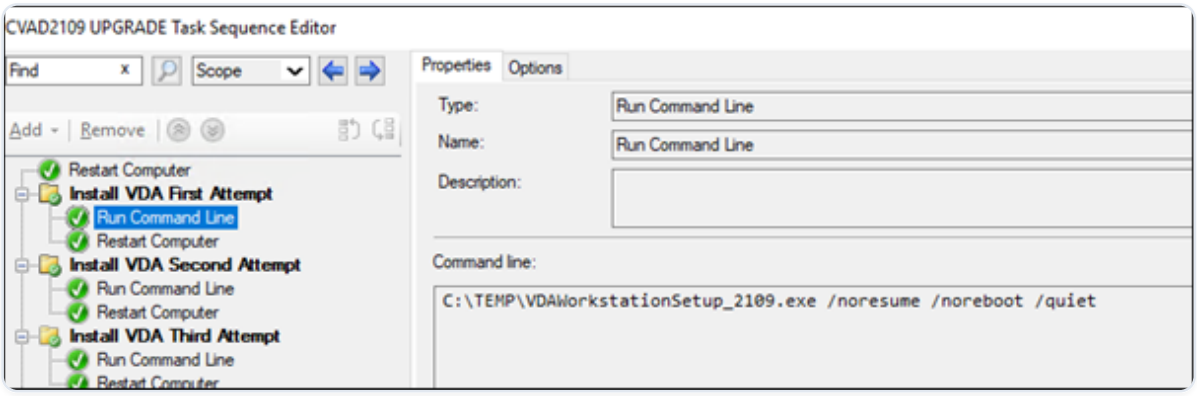
1. **コンピューターの再起動:** マシンを再起動して準備します。



2. **VDAのインストール（初回試行）：**VDAのインストールを開始します。

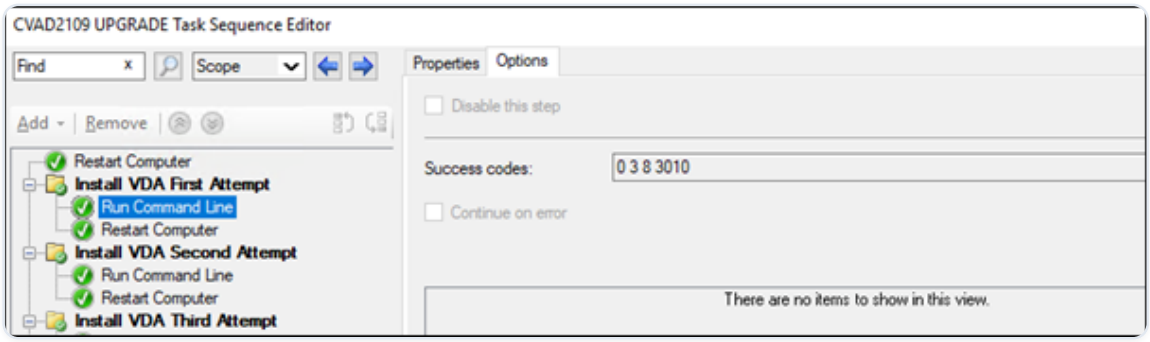
   a. `/quiet`、`/noreboot`、および`/noresume`オプションをコマンドラインオプションに追加します。

   b. 選択した VDA インストーラー (ローカルイメージまたは最小インストーラーのいずれか) を実行します。

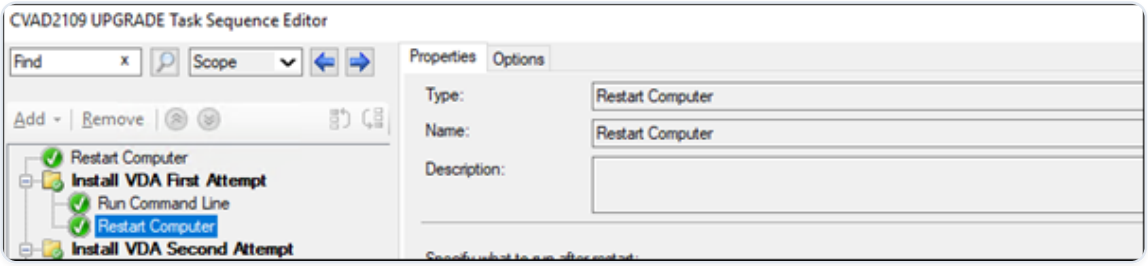


   c. SCCM はリターンコードをキャプチャする必要があります。

   - リターンコードが 0 または 8 の場合、インストールは完了しており、再起動が必要です。



   - リターンコードが3の場合、マシンを再起動し、**VDAのインストール（2回目試行）**に制御を渡します。



3. **VDAのインストール（2回目試行）：**VDAのインストールを続行します。

   a. **VDAのインストール（初回試行）**の後、ファイル`%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml`が存在する場合、インストールは完了しておらず、再起動が完了した後に続行する必要があります。



   b. **VDAのインストール（2回目試行）**は、ファイル`%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml`が存在しなくなるか、0または8以外のリターンコードが返されるまで繰り返されます。その他のリターンコードはエラーとして扱い、VDAのインストール（2回目試行）はエラーを報告して停止する必要があります。

   c. 適切なVDAインストーラー（ほとんどの場合`XenDesktopVdaSetup.exe`、`VDAWorkstationCoreSetup_XXXX.exe`が使用された場合は`XenDesktopRemotePCSetup.exe`）を、コマンドラインパラメーターなしでファイル`%programdata%\ Citrix\XenDesktopSetup\`ディレクトリから実行して、VDAのインストールを再開します。（VDAインストーラーは、インストーラーの初回実行時に保存したパラメーターを使用します。）

「アップグレードタスクシーケンスエディター」(/en-us/citrix-virtual-apps-desktops/2511/media/upgrade-task-sequence-editor.png)

   d. VDAインストーラーからのリターンコードを確認します。

      - 0または8：成功、インストール完了、再起動が必要です。

「インストール完了」(/en-us/citrix-virtual-apps-desktops/2511/media/success-installation-complete.png)

- 3: インストールは完了していません。マシンを再起動し、ファイル `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` が存在しなくなるか、0または8が返されるまで INSTALL VDA SECOND ATTEMPT を繰り返してください。その他のリターンコードはエラーとして扱い、INSTALL VDA SECOND ATTEMPT はエラーを報告して終了する必要があります。

リターンコードの詳細については、Citrixインストールのリターンコードを参照してください。

VDAインストールコマンドの例

利用可能なインストールオプションは、使用するインストーラーによって異なります。コマンドラインオプションの詳細については、以下の記事を参照してください。

- VDAのインストール
- コマンドラインを使用したインストール

REMOTE PC ACCESSのインストールコマンド

- 次のコマンドは、シングルセッションコア VDA インストーラー（`VDAWorkstationCoreSetup.exe`）を使用します。

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

- 次のコマンドは、シングルセッションフル VDA インストーラー（`VDAWorkstationSetup.exe`）を使用します。

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /physicalmachine /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

専用 VDI のインストールコマンド

- 次のコマンドは、シングルセッションフル VDA インストーラー（`VDAWorkstationSetup.exe`）を使用します。

  ```
  VDAWorkstationSetup.exe /quiet /components vda /controllers “control.domain.com” /enable_hdx_ports /enable_remote_assistance /noresume /noreboot
  ```

Microsoft Intune を使用した VDA のインストール

概要

この記事では、Microsoft Intune を使用して VDA を展開する方法について説明します。詳細については、Microsoft のドキュメントを参照してください。

注:

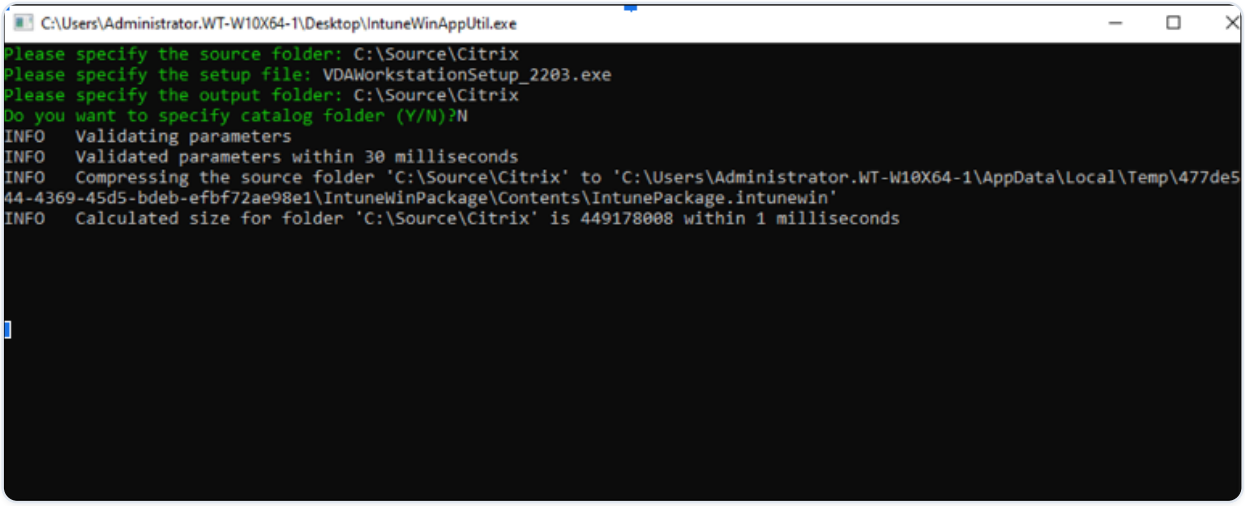
以下の記事は、Citrix® が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、お客様のニーズに合わせてカスタマイズできます。Citrix は、お客様のニーズに合わせてこれに必要な更新や調整について責任を負いません。

Microsoft Intune を使用して VDA を展開するための主要な手順

1. Citrix VDA のインストールを準備する。
2. Microsoft 365 開発者プログラムサブスクライバーを設定する。
3. アプリを追加して割り当てる。
4. 登録済みデバイスにアプリをインストールする。

ステップ 1: CITRIX VDA のインストールを準備する

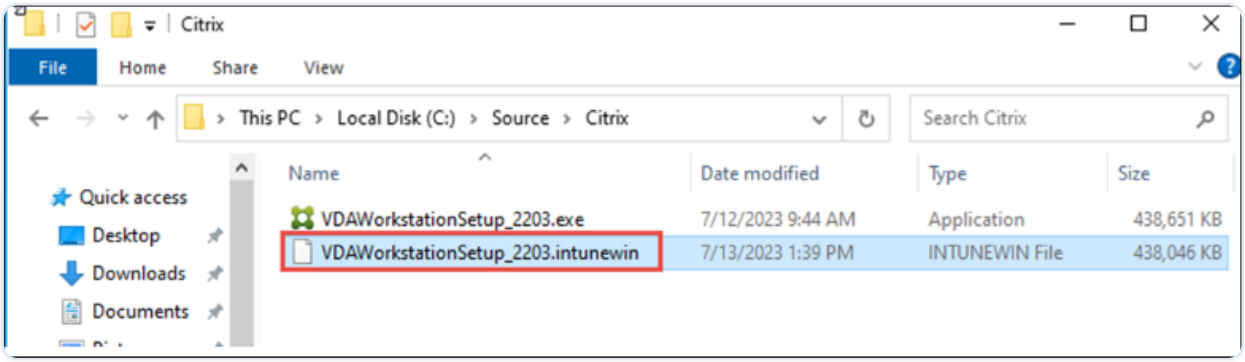
1. 更新された IntuneWinAppUtil.exe を GitHub からダウンロードします。
2. **管理者として実行**を使用して `IntuneWinAppUtil.exe` ファイルを実行します。
3. 次のデータを入力します。



a. **ソースフォルダーを指定してください**: アプリケーションのセットアップファイルが含まれているフォルダーを入力します。例: C:\source\Citrix。
b. **セットアップファイルを指定してください**: セットアップファイル名 (setup.exe や setup.msi など) を入力します。例: VDAWorkstationSetup_2203.exe。
c. **出力フォルダーを指定してください**: .intunewin ファイルを生成する出力フォルダーのパスを入力します。例: C:\source\Citrix。
d. **カタログフォルダーを指定しますか (Y/N)**: N と入力します。

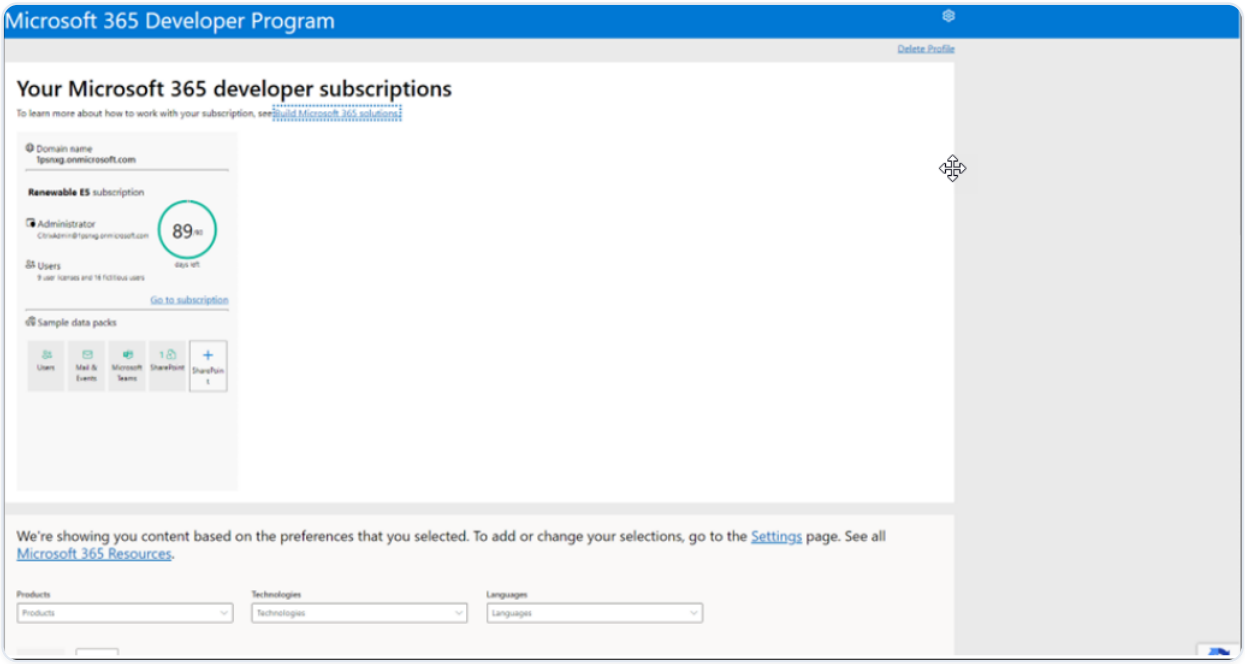
> **注:**
>
> **Win32 Content Prep Tool** の実行中は数分間お待ちください。`.intunewin` ファイルが生成されると、コマンドプロンプトの下部にステータスが 100% と表示されます。

4. プロセスが完了したら、出力フォルダー (この例では `C:\source\Citrix`) に移動して、Microsoft Intune 展開ファイルを取得します。
5. Microsoft Intune の無料試用版にサインアップします。

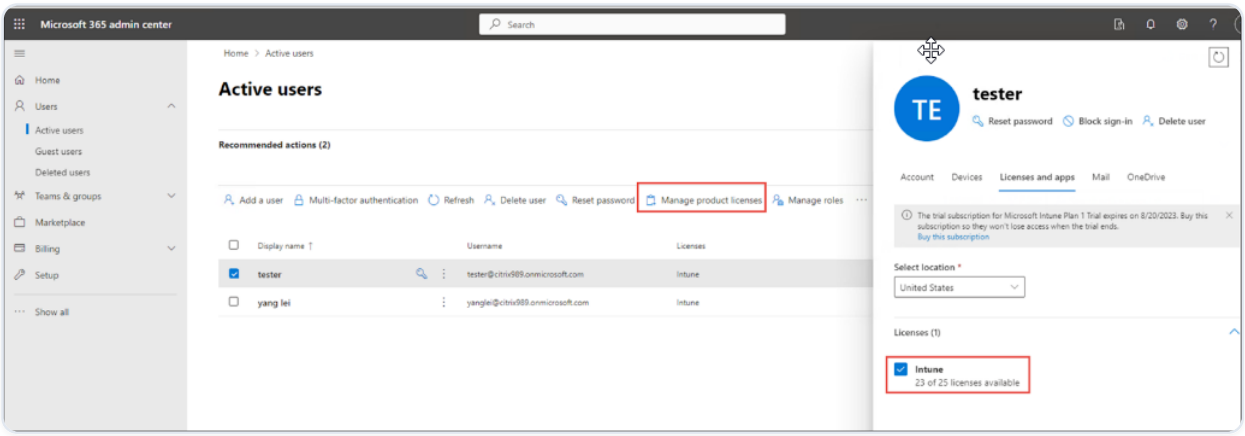


ステップ 2: MICROSOFT 365 DEVELOPER PROGRAM サブスクライバーを設定する

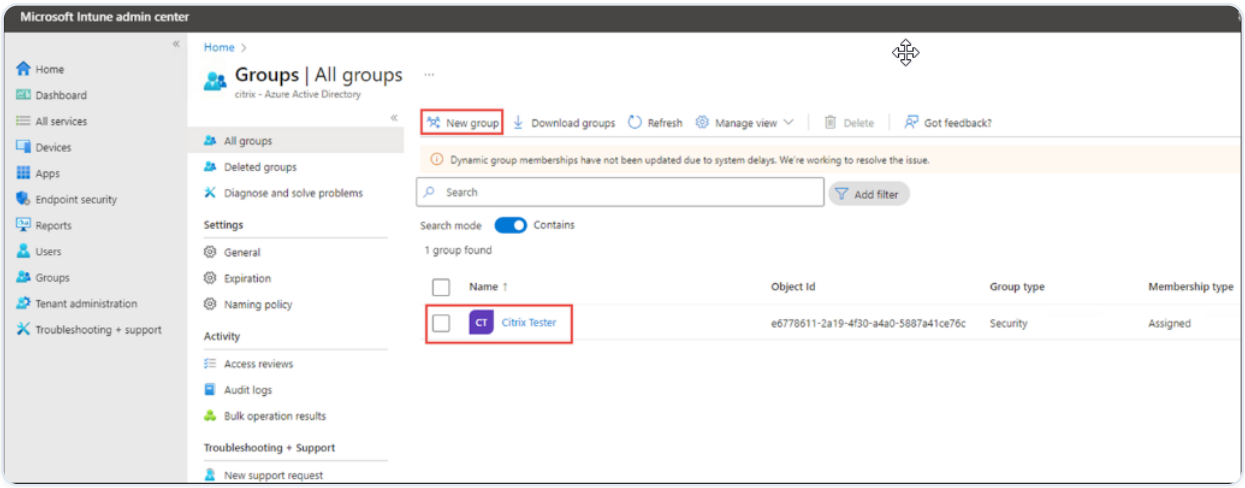
1. サブスクリプションをアクティブ化するために、インスタントサンドボックスを作成します。開発者サンドボックスを取得するには、Microsoft 365 Developer Program ダッシュボード に移動し、**新しいサブスクリプションの追加**を選択します。



2. Microsoft 365 管理センターでユーザーを作成し、そのユーザーにライセンスを割り当てます。



3. グループを作成します。



4. グループが作成されたら、MDM機関をグループに提供する必要があります。自動登録を設定します。アクティブ化には1分ほどかかる場合があります。 または、次の手順を実行して、MDM機関をグループに手動で追加することもできます。

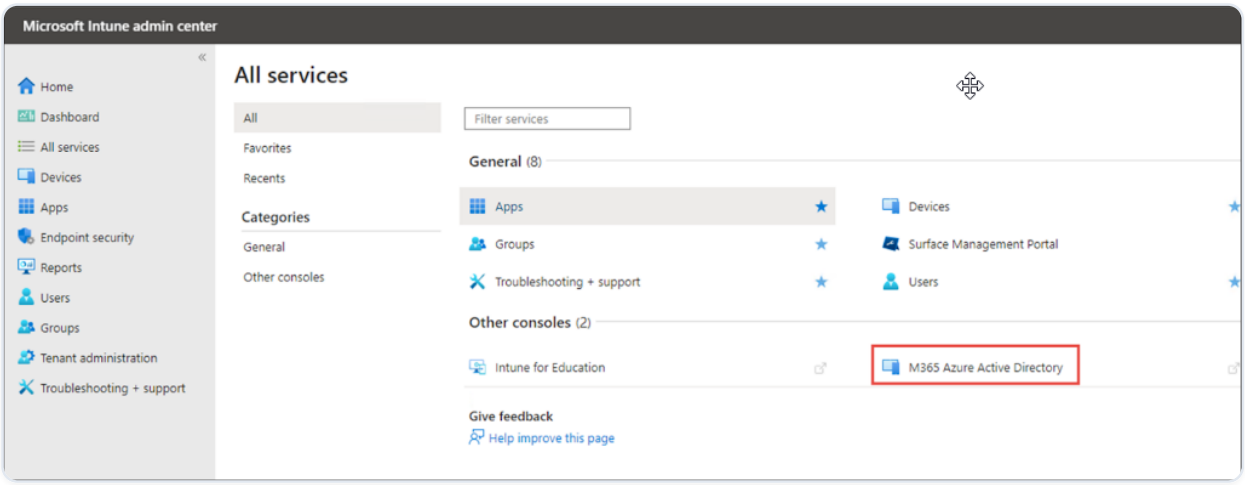
   a. **すべてのサービス > Microsoft Entra** に移動します。

   b. 「**設定 > モビリティ**」に移動し、「**Microsoft Intune**」を選択します。

   c. 作成したばかりのグループを選択します。これにより、MDMユーザー範囲のページが開きます。

   d. 「**保存**」をクリックします。

5. 「**すべてのサービス**」タブで、「**M365 Microsoft Entra ID**」をクリックします。



6. **この機能を使用するには、無料のPremium試用版を入手してください** をクリックします。

「Intune MDM」(/en-us/citrix-virtual-apps-desktops/2511/media/intune-mdm.png)

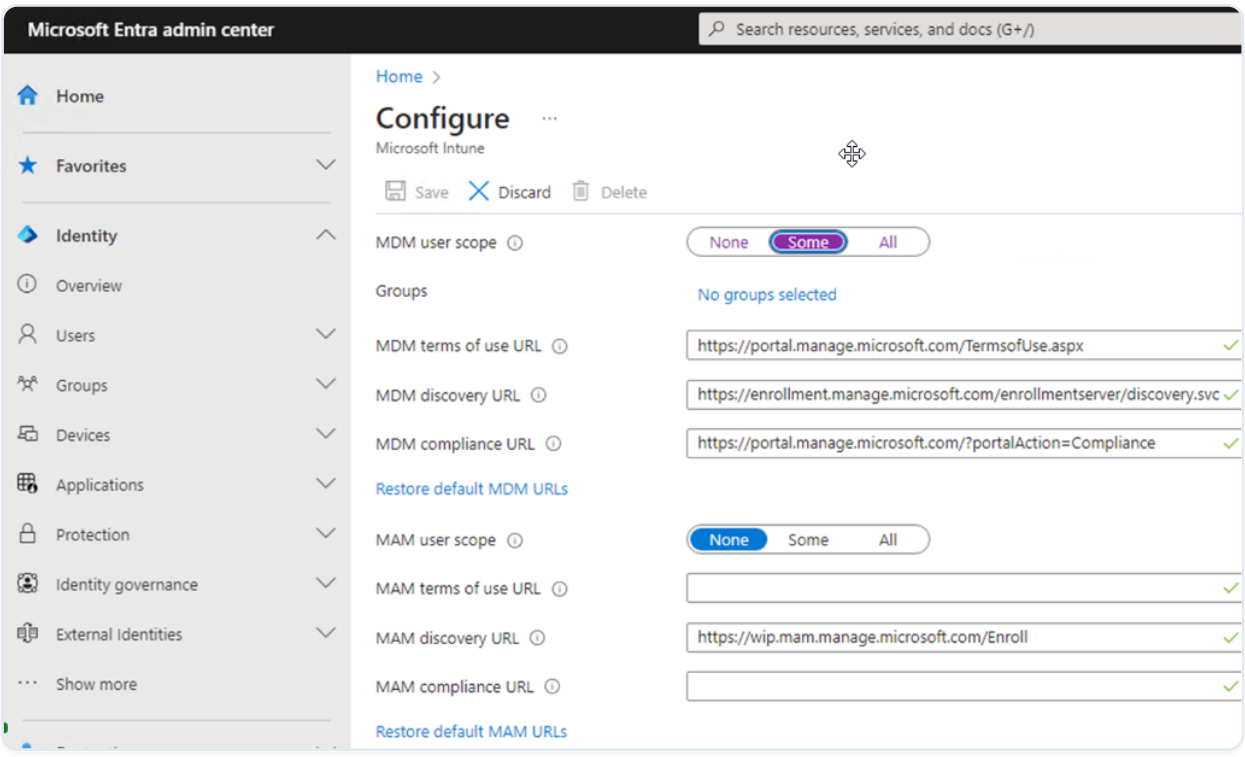
7. 「**アクティブ化**」をクリックします。

「MS Entraセンター」(/en-us/citrix-virtual-apps-desktops/2511/media/ms-entra-admin-center.png)

8. 次に、「**Microsoft Intune**」をクリックします。

「MS Intuneの選択」(/en-us/citrix-virtual-apps-desktops/2511/media/select-ms-intune.png)

9. 「**構成**」タブで、必要な構成を入力します。



10. グループを追加するには、「**グループが選択されていません**」をクリックします。

グループを選択(/en-us/citrix-virtual-apps-desktops/2511/media/intune-select-a-group.png)

11. デバイスを登録します。

    デバイスを登録(/en-us/citrix-virtual-apps-desktops/2511/media/intune-enrol-a-device.png)

12. 新しく作成したデバイスのコンプライアンスを`Compliant`に変更するためのデバイスコンプライアンスポリシーを作成します。

    コンプライアンスポリシー(/en-us/citrix-virtual-apps-desktops/2511/media/compliance-policy-intune.png)

13. 新しく作成したグループを追加するには、 タブに移動します。

    完全に管理(/en-us/citrix-virtual-apps-desktops/2511/media/intune-fully-managed-and-dedicated.png)

14. デバイスの登録を確認します。

    デバイスの登録(/en-us/citrix-virtual-apps-desktops/2511/media/intune-device-enrolment.png)

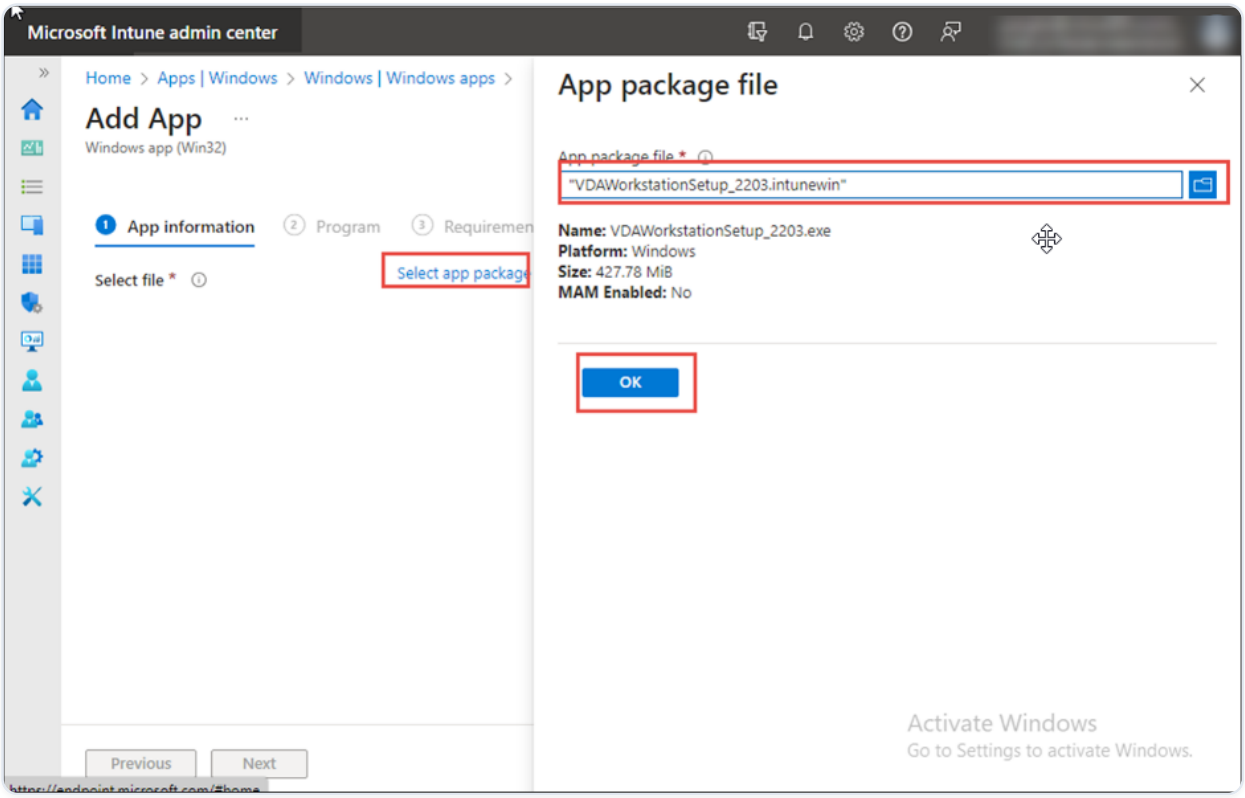
詳細については、Microsoft 365 developer programを参照してください。

ステップ3: アプリを追加して割り当てる

1. Microsoft Intune admin centerにサインインします。
2. **アプリ > すべてのアプリ > 追加**を選択するか、**アプリ > Windows > Windowsアプリ**に移動します。

    アプリの種類を選択(/en-us/citrix-virtual-apps-desktops/2511/media/ms-intune-admin-2.png)

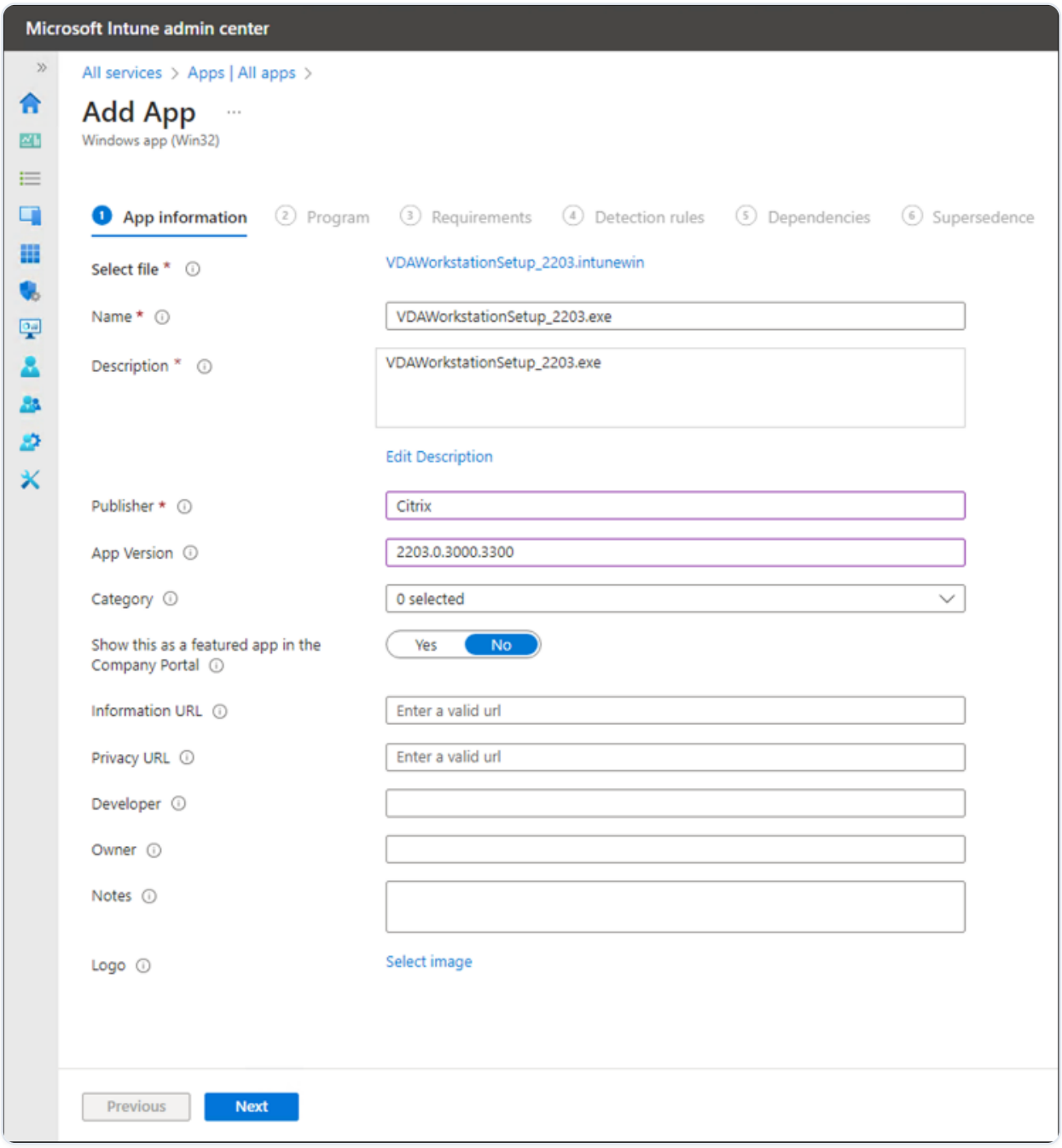
3. ペインで、 **>** を選択し、 をクリックします。
4. ペインで、 をクリックします。 をクリックします。
5. 拡張子`.intunewin`の準備済みファイルを選択します。準備済みファイルは、Citrix VDAのインストール準備のステップで作成されます。アプリに関する詳細情報を含むページが表示されます。



注:

- サーバーコアマシンを使用している場合は、VDAワークステーションコアを使用する必要があります。
- Windows 10デスクトップOSを使用している場合は、VDAワークステーションを使用する必要があります。
- サーバーOS（例：Windows 2022）を使用している場合は、VDAサーバーセットアップを使用する必要があります。
- この例では2203バージョンを使用していますが、これはすべてのバージョンに適用されます。

6. **App package file**ペインで**OK**をクリックします。
7. 次の画面で、「**アプリ情報**」タブの下で、アプリの「**名前**」を入力し、Windowsアプリの「**説明**」を入力します。「**発行元**」の名前を `Citrix` として入力し、ここで追加のアプリ情報を指定できます。「**次へ**」をクリックします。

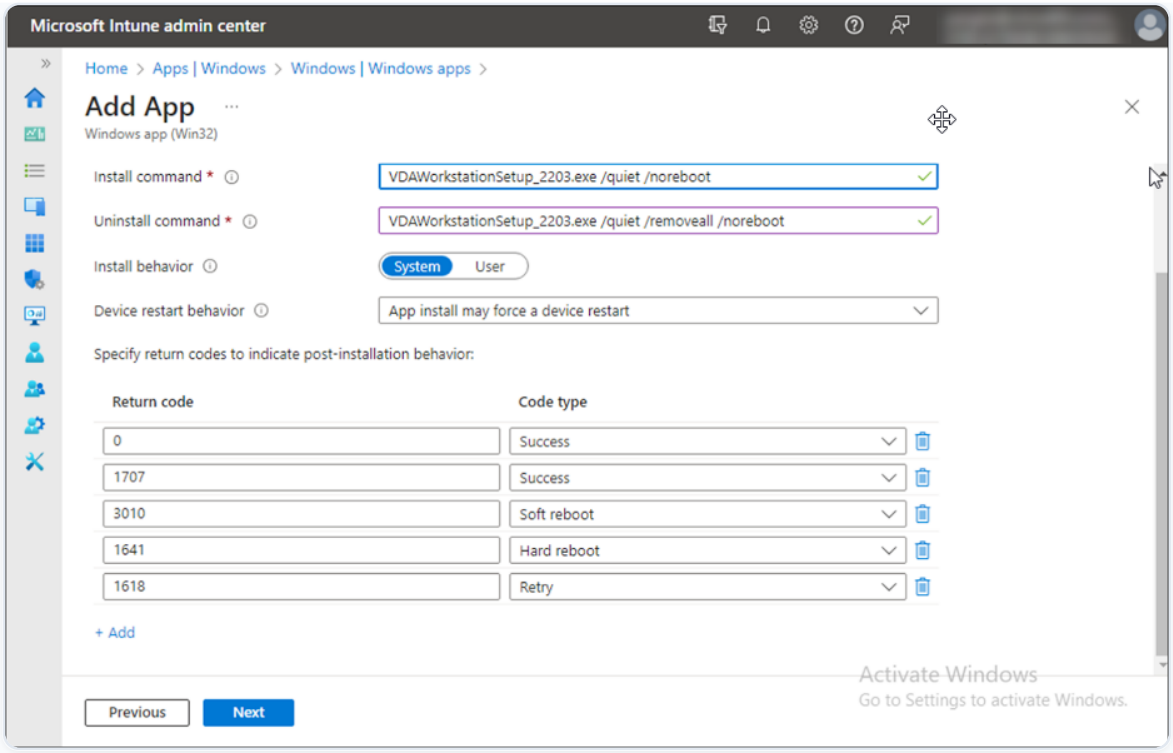


8. 次の画面で、次の値を入力します。

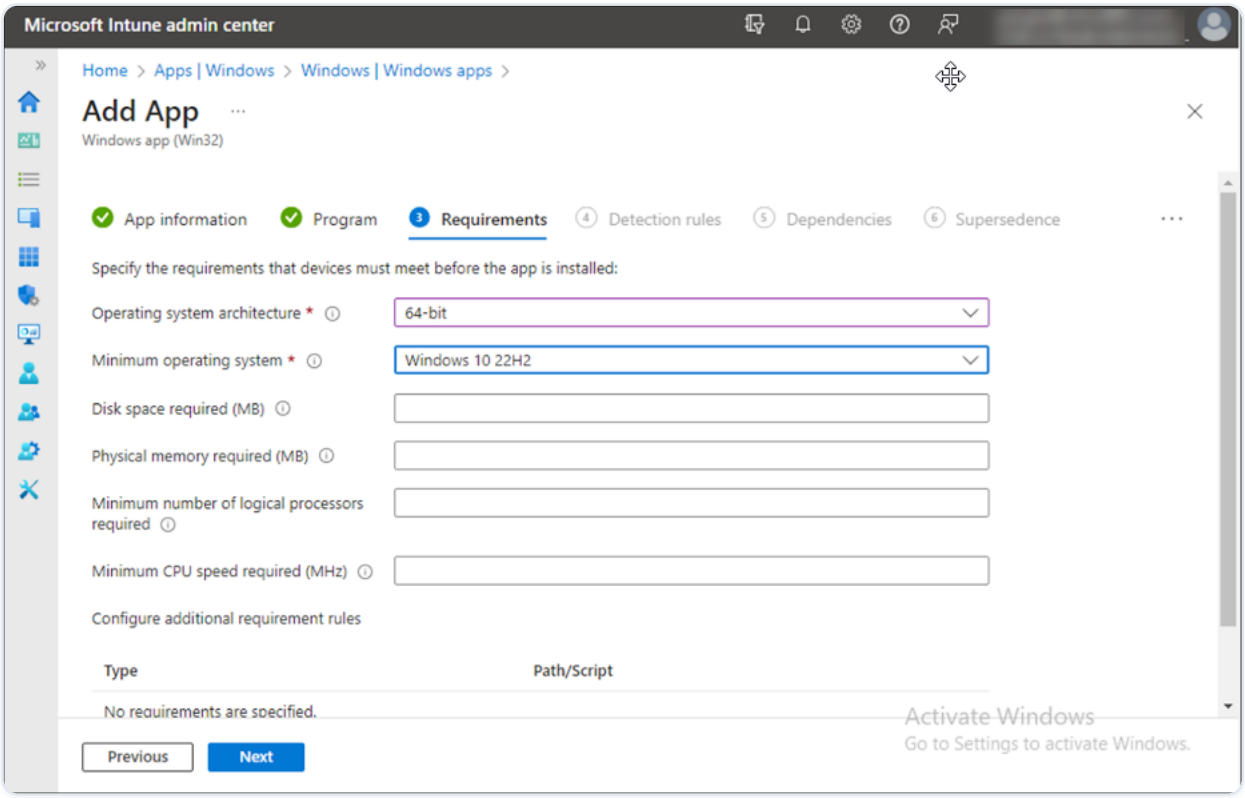
   - **インストールコマンド**: `VDAWorkstationSetup_2203.exe /quiet /noreboot`
   - **アンインストールコマンド**: `VDAWorkstationSetup_2203.exe /quiet /removeall /noreboot`
   - **インストール動作**:
     - **システム**: グループ内のすべてのデバイスにアプリをインストールするには、このオプションを選択します。
     - **ユーザー**: グループ内の特定のユーザーデバイスにのみアプリをインストールするには、このオプションを選択します。

9. 「**次へ**」をクリックします。

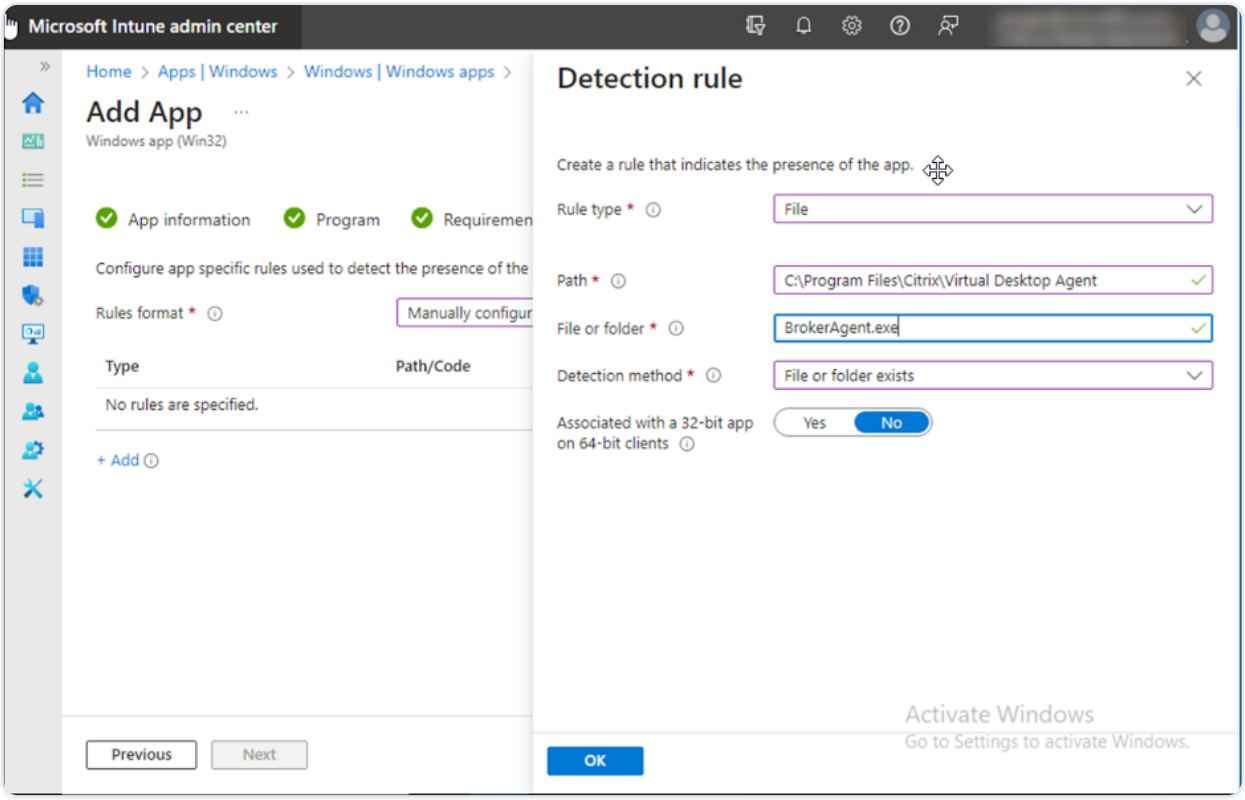
> **注:**
>
> - この例ではバージョン2203を使用していますが、どのバージョンでも使用できます。
> - コマンドに`/noreboot`を追加しても、インストールまたは展開中に再起動が発生しないという意味ではなく、強制的な再起動が適用されるだけです。 スクリプトの詳細については、「VDAのインストール用コマンドラインオプション」を参照してください。
> - **デバイスの再起動動作**については、「**Intuneは強制的にデバイスを再起動します**」を選択します。
> - **リターンコード**テキストボックスに、インストール後の成功のために`0`、`3`、および`8`を入力します。 その他のリターンコードについては、「Citrixインストールリターンコード」を参照してください。



10. 次の画面で、**要件**タブの下に、必要な値を入力します。「**次へ**」をクリックします。



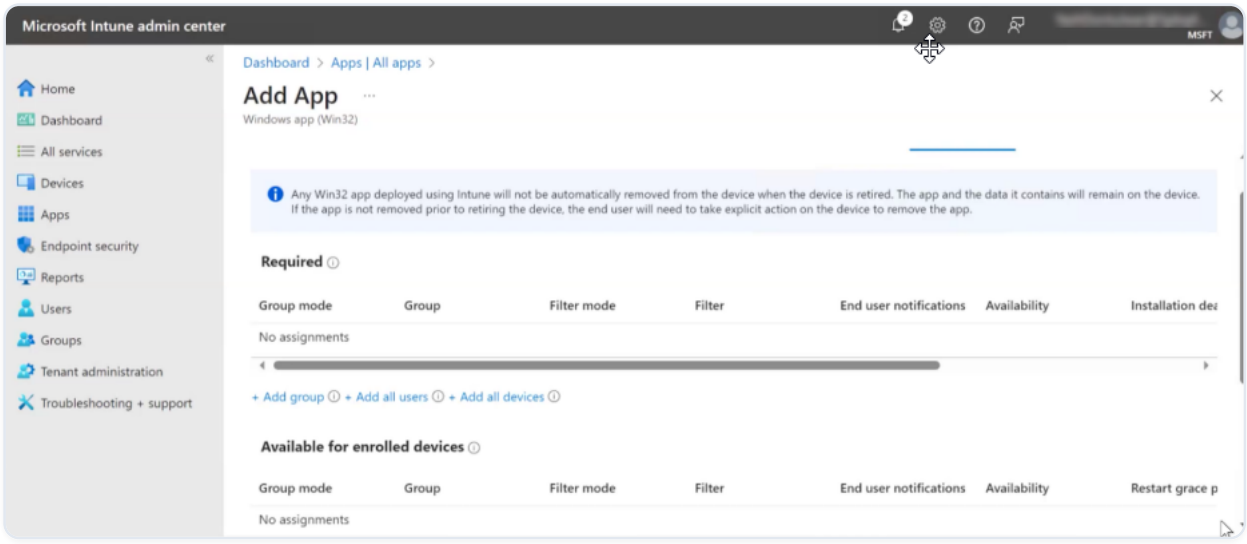
11. 次の画面で、**検出ルール**タブの下に、Brokerエージェントを追加するための**検出ルール**を追加します。「**OK**」をクリックします。



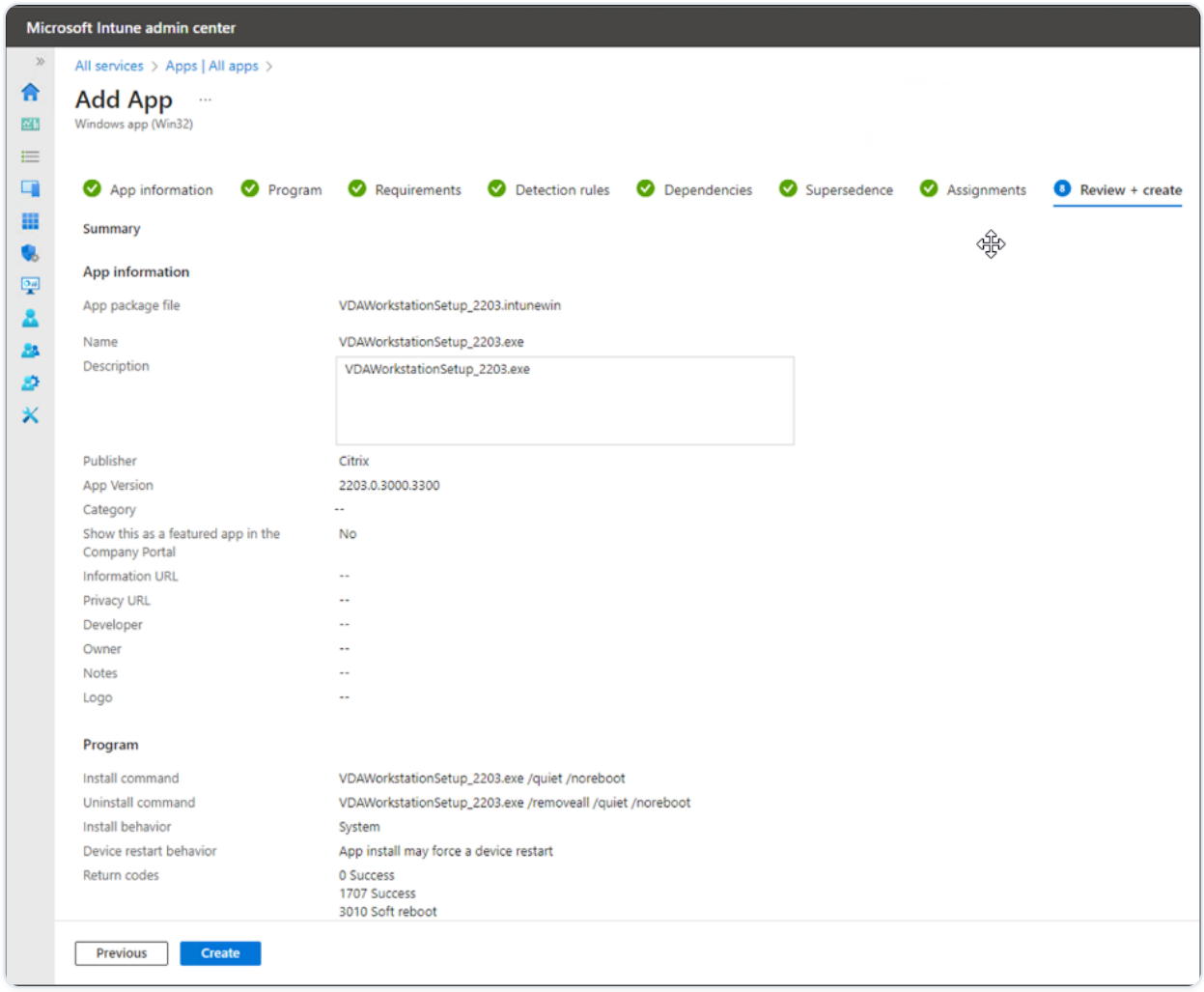
12. 「**割り当て**」タブで、デバイスを次のように追加できます。

- **必須**: 更新が自動的に行われるデバイス。

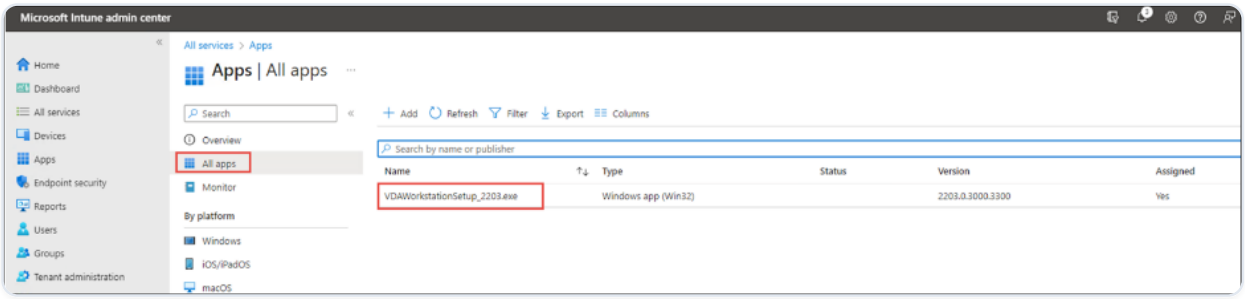
- **登録済みデバイスで利用可能**: 更新が手動で行われるデバイス。



13. 詳細を確認し、「**作成**」をクリックします。



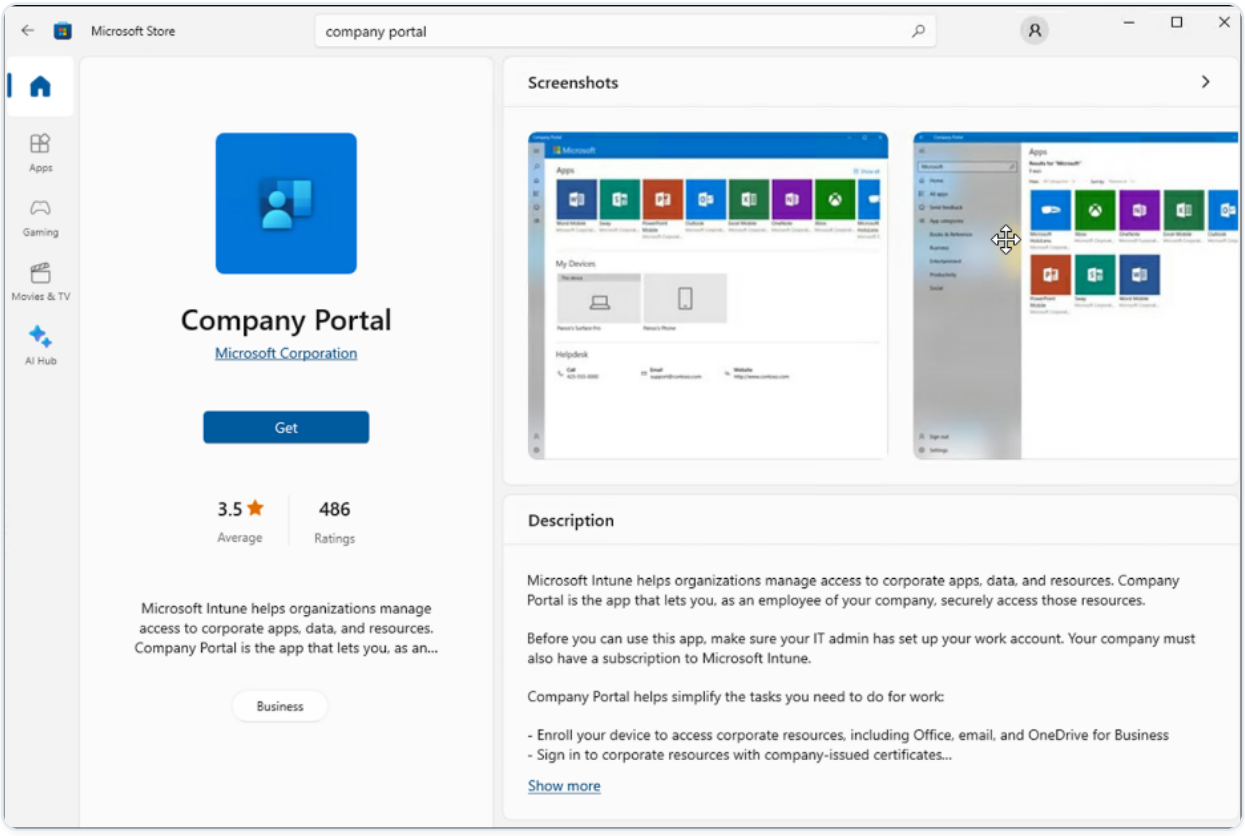
アプリが正常に割り当てられました。



詳細については、「アプリの追加と割り当て」を参照してください。

ステップ 4: 登録済みデバイスにアプリをインストールする

1. 登録済みのWindows 10デスクトップデバイスにサインインします。 デバイスはMicrosoft Intuneに登録されている必要があります。また、アプリに割り当てたグループに含まれるアカウントを使用してデバイスにサインインする必要があります。詳細については、Microsoftのドキュメントを参照してください。
2. 「**スタート**」メニューから、「**Microsoft Store**」を開きます。
3. 「**ポータルサイト**」アプリを検索し、インストールします。



4. 「**ポータルサイト**」アプリを実行します。
5. Microsoft Intuneを使用して追加したアプリをクリックします。 Intuneユーザーにアプリを正常に割り当てなかった場合、次のメッセージが表示されます。 `Your IT administrator did not make any apps available to you.`

6. **Install**をクリックします。

サイトを作成する

> **注:**
>
> - サイト作成中に、ハイブリッド権限ライセンスを有効にするライセンスを追加した後、サイト作成が完了するまで、パブリッククラウドホスト（Microsoft Azure、Google Cloud Platform、Amazon Web Servicesなど）は接続タイプリストに表示されません。
> - ライセンスアクティベーションサービスを有効にしている間、または有効にした後に、製品エディションやライセンスモデルを手動で変更しないでください。

> サイトとは、Citrix Virtual Apps and Desktops™展開に付ける名前です。これには、Delivery Controllerおよびその他のコアコンポーネント、Virtual Delivery Agent (VDA)、ホストへの接続、マシンカタログ、およびデリバリーグループが含まれます。サイトは、コアコンポーネントをインストールした後、最初のマシンカタログとデリバリーグループを作成する前に作成します。

ControllerがServer Coreにインストールされている場合は、Citrix Virtual Apps and Desktops SDKのPowerShellコマンドレットを使用してサイトを作成します。

サイトを作成すると、Citrixカスタマーエクスペリエンス向上プログラム（CEIP）に自動的に登録されます。CEIPは匿名統計と使用状況情報を収集し、Citrixに送信します。最初のデータパッケージは、サイト作成後約7日後にCitrixに送信されます。サイト作成後いつでも登録を変更できます。Web Studioの左ペインで**設定**を選択し、**Citrixカスタマーエクスペリエンス向上プログラム**の設定を見つけます。詳細については、`<http://more.citrix.com/XD-CEIP>`を参照してください。

サイトを作成したユーザーは、フル管理者になります。詳細については、委任管理を参照してください。

サイトを作成する前にこの記事を確認して、何が期待できるかを知っておいてください。

ステップ1. サイト作成ウィザードを開く - Citrix Site Manager

「Citrix Site Manager」というツールを使用して、Citrix Virtual Apps™ and Desktops の展開（サイトとも呼ばれます）をセットアップします。このツールは、Delivery Controller をインストールすると自動的にインストールされます。

このツールを実行するには、Delivery Controllerでデスクトップのスタートメニューを開き、**Citrix > Citrix Site Manager**を選択します。Web Studioのインストールを参照してください。

ステップ2. サイト名

はじめにページで、サイトの名前を入力します。

ステップ3. データベース

> **注:**
>
> バージョン2411以降、データベースにAzure SQL Managed Instanceを使用できます。
>
> 「**データベース**」ページには、サイト、監視、および構成ログデータベースを設定するための選択肢が含まれています。データベースのセットアップの選択肢と要件の詳細については、「データベース」を参照してください。
>
> **注:**
>
> SQL Server Always Onリスナーが TLS暗号化用に構成されている場合、データベース作成権限を持つ資格情報の入力を求められることがあります。有効な管理者資格情報を入力しても、データベースの作成は引き続き失敗します。SQL Server証明書に、サブジェクトの別名 (SAN) にリスナーのDNS名が含まれていることを確認してください。詳細については、`<https://docs.microsoft.com/ja-jp/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover#SSLcertificates>` を参照してください。
>
> サイトデータベースとしてSQL Server Expressをインストールすることを選択した場合（デフォルト）、そのソフトウェアのインストール後に再起動が発生します。サイトデータベースとしてSQL Server Expressソフトウェアをインストールしないことを選択した場合は、再起動は発生しません。

デフォルトのSQL Server Expressを使用しない場合は、サイトを作成する前にSQL Serverソフトウェアがマシンにインストールされていることを確認してください。「システム要件」にサポートされているバージョンが記載されています。

サイトにDelivery Controllerを追加したい場合で、すでに他のサーバーにControllerソフトウェアをインストールしている場合は、このページからそれらのControllerを追加できます。データベースを設定するスクリプトを生成する予定がある場合は、スクリプトを生成する前にControllerを追加してください。

ステップ4. ライセンス

「**ライセンス**」ページで、ライセンスサーバーのアドレスを指定し、使用する（インストールする）ライセンスを示します。

> **注:**
>
> - ライセンスサーバーがバージョン11.17.2ビルド53100以降で実行されていることを確認してください。この前提条件を満たさない場合、Citrix Virtual Apps and Desktopsサイトのアップグレードおよびサイトの作成がブロックされます。
> - License Activation Service (LAS) は、従来のCitrixレガシーライセンスに代わるクラウドベースのライセンスソリューションです。詳細については、以下を参照してください。
>   - Citrix Virtual Apps and Desktops ドキュメント: ライセンスアクティベーションサービス(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/licensing/license-activation-service)
>   - 「ライセンスドキュメント: License Activation Service」
> - License Activation Service の有効化中または有効化後に、製品エディションまたはライセンスモデルを手動で変更しないでください。

- ライセンスサーバーのアドレスを `name:[port]` の形式で指定します。*name* は、FQDN、NetBIOS、または IP アドレスである必要があります。FQDN を推奨します。ポート番号を省略すると、デフォルトは 27000 になります。**Connect** をクリックします。ライセンスサーバーへの接続が成功するまで、次のページに進むことはできません。
- 接続が確立されると、デフォルトで **Use an existing license** が選択されます。表示には、現在インストールされているライセンスに基づいて、この製品として構成できる互換性のある製品が一覧表示されます。
  - ライセンスサーバーが License Activation Service (LAS) を使用するように構成されている場合、メタインストーラーはエンタイトルメントを表示します。エンタイトルメントは、対応するライセンスの有効期限とともに提供されます。これらのライセンスのいずれかを

使用して、この製品をリストされている製品のいずれかとして構成する場合は、そのエントリを選択します。

- この製品で使用するためにライセンスを割り当ててダウンロード済み（Citrix Manage Licenses Tool を使用）だが、まだライセンスをインストールしていない場合：
  - **Browse for license file** をクリックします。
  - ファイルエクスプローラーで、ダウンロードしたライセンスを見つけて選択します。関連する製品が、サイト作成ウィザードの **Licensing** ページに表示されます。使用したいエントリを選択します。
- 目的の製品が表示されない場合、または割り当て済みでダウンロード済みのライセンスがない場合は、ライセンスを割り当て、ダウンロードしてインストールできます。これを行うには、ライセンスサーバーがインターネットにアクセスできる必要があります。目的の製品のライセンスアクセスコードが必要です。Citrix からそのコードがメールで送信されます。
  - **Allocate and download** をクリックします。
  - **Allocate Licenses** ダイアログで、Citrix から送信されたライセンスアクセスコードを入力します。**Allocate licenses** をクリックします。
  - 新しいライセンスに関連付けられた製品が、サイト作成ウィザードの **Licensing** ページに表示されます。使用したいエントリを選択します。

- または、**Use the free 30-day trial** を選択し、後でライセンスをインストールします。詳細については、ライセンスドキュメント を参照してください。

ステップ 5. 概要

Summary ページには、指定した情報が一覧表示されます。変更したい場合は、**Back** ボタンを使用します。完了したら、**Finish** をクリックします。

詳細情報

ホスト接続、ネットワーク、およびストレージ

アプリケーションとデスクトップを配信するためにハイパーバイザーまたはその他のサービスでVMを使用している場合、そのホストへの最初の接続をオプションで作成できます。その接続のストレージおよびネットワークリソースを指定することもできます。サイトを作成した後、この接続とリソースを変更し、さらに多くの接続を作成できます。詳細については、「接続とリソース」を参照してください。

- **接続**ページで指定された情報については、「接続とリソース」を参照してください。
  - ハイパーバイザーまたはその他のサービスでVMを使用していない場合（または、Web Studioを使用して専用ブレードPC上のデスクトップを管理する場合）は、接続の種類として**なし**を選択します。
  - Remote PC Accessサイトを構成していて、Wake on LAN機能を使用する予定がある場合は、**Microsoft System Center Virtual Machine Manager**または**Remote PC Wake on LAN**タイプを選択します。詳細については、「Wake on LAN」を参照してください。

  接続の種類に加えて、Citrixツール（Machine Creation Services™など）またはその他のツールを使用してVMを作成するかどうかを指定します。
- **ストレージ**および**ネットワーク**ページで指定された情報については、「ホストストレージ」、「ストレージ管理」、および「ストレージの選択」を参照してください。
- ハイブリッド権限ライセンスを所有しており、パブリッククラウドホスト接続（AWSなど）を追加している場合、それらの接続がここに一覧表示されます。それらのパブリッククラウドホスト接続を表示するには、追加後数分経ってからWeb Studioを更新してください。

リモートPCアクセス

Remote PC Accessの展開に関する情報については、「Remote PC Access」を参照してください。

Wake on LAN機能を使用する場合は、サイトを作成する前に、Microsoft System Center Configuration Managerで構成手順を完了してください。詳細については、「Configuration ManagerとRemote PC Access Wake on LAN」を参照してください。

接続とリソースの作成と管理

> **重要：**
>
> Citrix Virtual Apps and Desktops™ 7 2006以降、現在の展開で以下のいずれかのテクノロジーを使用している場合、それらのテクノロジーを使用するサポート終了（EOL）項目を削除した後にのみ、現在のリリースにアップグレードできます。
>
> - パーソナルvDisk (PvD)
> - AppDisks™

- パブリッククラウドホストの種類：Citrix CloudPlatform、Microsoft Azure Classic

詳細については、「PVD、AppDisks、およびサポートされていないホストの削除」を参照してください。

注：

バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

展開にパブリッククラウドホスト接続を使用する場合は、新規インストールまたは現在のリリースへのアップグレードを完了するためにHybrid Rights Licenseが必要です。

インストーラーがサポートされていないテクノロジーまたはHybrid Rights Licenseのないホスト接続を1つ以上検出すると、アップグレードが一時停止または停止し、説明メッセージが表示されます。インストーラーログには詳細が含まれています。詳細については、「展開のアップグレード」を参照してください。

Hybrid Rights Licenseがホスト接続に与える影響

Hybrid Rights Licenseの資格に基づいて、パブリッククラウドホストへのホスト接続が影響を受ける3つのシナリオがあります。

- パブリッククラウドホストへの新しいホスト接続を作成するには、Hybrid Rights Licenseが必要です。
- Hybrid Rights Licenseを所有しているがライセンスの有効期限が切れている場合、パブリッククラウドホストへの既存の接続は「資格なし」とマークされ、メンテナンスモードに入ります。既存のホスト接続がメンテナンスモードの場合、次のことはできません。
  - ホスト接続の追加または変更
  - カタログの作成とイメージの更新
  - 電源操作の実行
- 権限のないホスト接続が権限のあるものに変更されると、既存のホスティング接続が再度有効になります。

はじめに

サイトを作成するときに、ホスティングリソースへの最初の接続をオプションで作成できます。後で、その接続を変更したり、他の接続を作成したりできます。接続の構成には、サポートされているハイパーバイザーの中から接続タイプを選択すること、およびその接続のリソースから選択するストレージとネットワークが含まれます。

読み取り専用管理者は、接続とリソースの詳細を表示できます。接続とリソースの管理タスクを実行するには、完全な管理者である必要があります。詳細については、「委任管理」を参照してください。

接続タイプに関する情報の検索場所

サポートされている仮想化プラットフォームを使用して、Citrix Virtual AppsまたはCitrix Virtual Desktops環境でマシンをホストおよび管理できます。「システム要件」の記事に、サポートされている種類が記載されています。

詳細については、以下の情報源を参照してください。

- **XenServer (旧 シトリックス ハイパーバイザー™):**
  - XenServer仮想化環境。
  - XenServer® ドキュメント。
- **ニュータニックス アクロポリス:**
  - Nutanix仮想化環境。
  - Nutanix のドキュメント。
- **ヴイエムウェア:**
  - VMware仮想化環境。
  - VMware製品ドキュメント。
- **Microsoft ハイパーV:**
  - Microsoft System Center Virtual Machine Manager 仮想化環境 の記事。
  - Microsoft のドキュメント。
- **パブリッククラウドホスト接続 (AWS、Google Cloud、Microsoft Azure、Nutanix クラウドおよびパートナーソリューション、VMware クラウドおよびパートナーソリューション):** パブ

リッククラウドホストに関する情報については、「リソースタイプのセットアップ」を参照してください。

> **注:**
>
> 情報源は Citrix DaaS™ のドキュメントを参照するよう指示しています。Citrix DaaS 製品のパブリッククラウドホストに慣れている場合、オンプレミスバージョンにはいくつかの違いがあります。オンプレミスの Virtual Apps and Desktops では、管理インターフェイスは Web Studio と呼ばれます。サービスへの更新は約4週間ごとに展開されます。そのため、サービスで利用できる特定の機能がオンプレミスバージョンでは利用できない場合があります。

ホストストレージ

ストレージ製品は、サポートされているハイパーバイザーによって管理されている場合にサポートされます。Citrix サポートは、これらのストレージ製品ベンダーが問題のトラブルシューティングと解決を支援し、必要に応じてナレッジセンターにそれらの問題を文書化します。

マシンをプロビジョニングする際、データはタイプ別に分類されます。

- オペレーティングシステム (OS) データ。これにはマスターイメージが含まれます。
- 一時データ。このデータには、MCS でプロビジョニングされたマシンに書き込まれるすべての非永続データ、Windows ページファイル、ユーザープロファイルデータ、および ShareFile と同期されるすべてのデータが含まれます。このデータは、マシンが再起動するたびに破棄されます。

各データタイプに個別のストレージを提供することで、各ストレージデバイスの負荷を軽減し、パフォーマンスを向上させ、ホストの利用可能なリソースを最大限に活用できます。また、異なるデータタイプに適切なストレージを使用できるようになります。一部のデータでは、永続性と回復性が他のデータよりも重要です。

ストレージは共有（中央に配置され、どのホストからも独立しており、すべてのホストで使用される）することも、ハイパーバイザーにローカルに配置することもできます。たとえば、中央共有ストレージは、1つ以上のWindows Server 2012クラスター化ストレージボリューム（接続ストレージの有無にかかわらず）、またはストレージベンダーのアプライアンスである場合があります。中央ストレージは、ハイパーバイザーのストレージ制御パスやパートナープラグインを介した直接アクセスなど、独自の最適化を提供する可能性もあります。

一時データをローカルに保存することで、共有ストレージにアクセスするためにネットワークを介する必要がなくなります。また、共有ストレージデバイスの負荷も軽減されます。共有ストレージはより高価になる可能性があるため、データをローカルに保存することで費用を削減できます。これらの利点は、ハイパーバイザーサーバー上の十分なストレージの可用性と比較検討する必要があります。

接続を作成するときは、ハイパーバイザーによって共有されるストレージ、またはハイパーバイザーにローカルなストレージの2つのストレージ管理方法のいずれかを選択します。

一時データストレージに1つ以上のXenServerホストでローカルストレージを使用する場合は、プールの各ストレージ場所に一意の名前があることを確認してください。（XenCenter®で名前を変更するには、ストレージを右クリックして名前プロパティを編集します。）

ハイパーバイザーで共有されるストレージ

ハイパーバイザー間で共有されるストレージ方式は、長期的な永続性が必要なデータを中央に保存し、一元的なバックアップと管理を提供します。このストレージにはOSディスクが格納されます。

この方法を選択すると、一時的なマシンデータにローカルストレージ（同じハイパーバイザープール内のサーバー上）を使用するかどうかを選択できます。この方法は、共有ストレージ内のデータ（*一時データキャッシュ*と呼ばれる）ほど永続性や回復性を必要としません。ローカルディスクは、メインOSストレージへのトラフィックを削減するのに役立ちます。このディスクは、マシンの再起動ごとにクリアされます。ディスクはライトスルーメモリキャッシュを介してアクセスされます。一時データにローカルストレージを使用する場合、プロビジョニングされたVDAは特定のハイパーバイザーホストに紐付けられます。そのホストが故障すると、VMは起動できません。

例外: Microsoft System Center Virtual Machine Managerは、クラスター共有ボリューム（CSV）を使用する場合、ローカルストレージ上の一時データキャッシュディスクを許可しません。

一時データをローカルに保存するための接続を作成し、各VMのキャッシュディスクサイズとメモリサイズの非デフォルト値を有効にして構成します。デフォルト値は接続タイプに合わせて調整されており、ほとんどのケースで十分です。詳細については、「マシンカタログの作成」を参照してください。

ハイパーバイザーは、ディスクイメージをローカルで読み取りキャッシュすることにより、最適化テクノロジーを提供することもできます。たとえば、XenServerはIntelliCache™を提供し、中央ストレージへのネットワークトラフィックを削減します。

ハイパーバイザーのローカルストレージ

ハイパーバイザーにローカルなストレージ方式では、データをハイパーバイザーにローカルに保存します。この方式では、マスターイメージやその他のOSデータがサイト内のハイパーバイザーに転送されます。このプロセスは、最初のマシン作成時と将来のイメージ更新時に発生します。このプロセスにより、管理ネットワークでかなりのトラフィックが発生します。イメージ転送には時間がかかり、イメージは各ホストで異なるタイミングで利用可能になります。

接続とリソースを作成する

サイトの作成時に、最初の接続をオプションで作成できます。サイト作成ウィザードには、以下のセクションで説明する接続関連のページが含まれています。

サイトの作成後に接続を作成する場合は、手順1から開始します。

> **重要:**
>
> 接続を作成する前に、ホストリソース（ストレージとネットワーク）が利用可能である必要があります。

1. Web Studioにサインインします。
2. 左側のペインで**ホスティング**を選択します。
3. アクションバーで**接続とリソースの追加**を選択します。
4. ウィザードは以下のページに沿って案内します（特定のページコンテンツは選択した接続の種類によって異なります）。各ページを完了したら、**次へ**をクリックして**概要**ページに到達します。

接続

接続作成ウィザードの接続ページ(/en-us/citrix-virtual-apps-desktops/2511/media/add-conn-connection.png)

「**接続**」ページで：

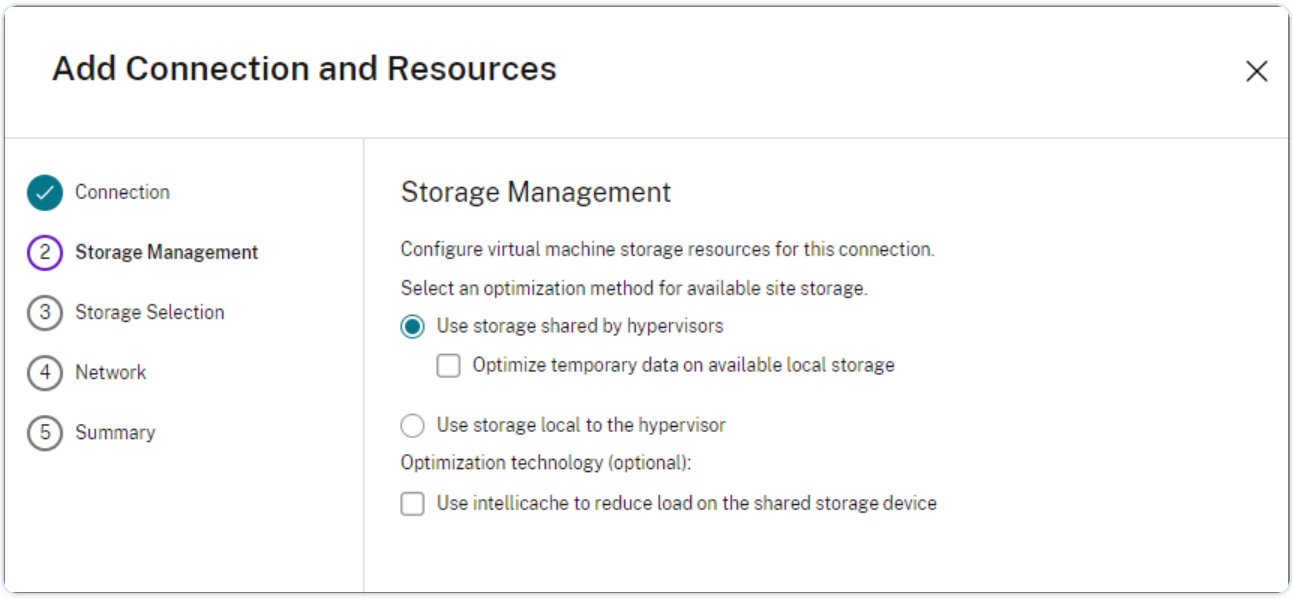
- 接続を作成するには、**新しい接続の作成**を選択します。既存の接続と同じホスト構成に基づいて接続を作成するには、**既存の接続を使用**を選択し、関連する接続を選択します。
- **接続の種類**フィールドで、使用しているハイパーバイザーを選択します。パブリッククラウドホスト接続は、ハイブリッドライツライセンスを使用している場合にのみドロップダウンリス

トに表示されます。または、PowerShellコマンド`Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false/trueを使用して、以下を取得できます。

  - サードパーティ製プラグインを含む、Citrixがサポートするすべてのハイパーバイザープラグインのリスト。
  - ハイパーバイザープラグインの可用性。可用性ステータスが**false**の場合、ハイパーバイザープラグインが正しくインストールされていないか、ハイブリッドライツライセンスの資格がないことが考えられます。

- 接続アドレスと資格情報フィールドは、選択した接続の種類によって異なります。要求された情報を入力してください。
- 接続名を入力します。この名前はWeb Studioに表示されます。
- 仮想マシンの作成に使用するツールを選択します：Web Studioツール（Machine Creation Services™やCitrix Provisioningなど）またはその他のツール。

ストレージ管理



ストレージ管理の種類と方法については、「ホストストレージ」を参照してください。

Hyper-VまたはVMwareホストへの接続を構成する場合は、クラスター名を参照して選択します。その他の接続タイプでは、クラスター名は要求されません。

ストレージ管理方法を選択します：ハイパーバイザー間で共有されるストレージ、またはハイパーバイザーにローカルなストレージ。

- ハイパーバイザーで共有されるストレージを選択した場合、利用可能なローカルストレージに一時データを保持するかどうかを指定します。（この接続を使用するマシンカタログで、デフォルト以外のサイズの一時ストレージを指定できます。）**例外：** クラスター共有ボリューム

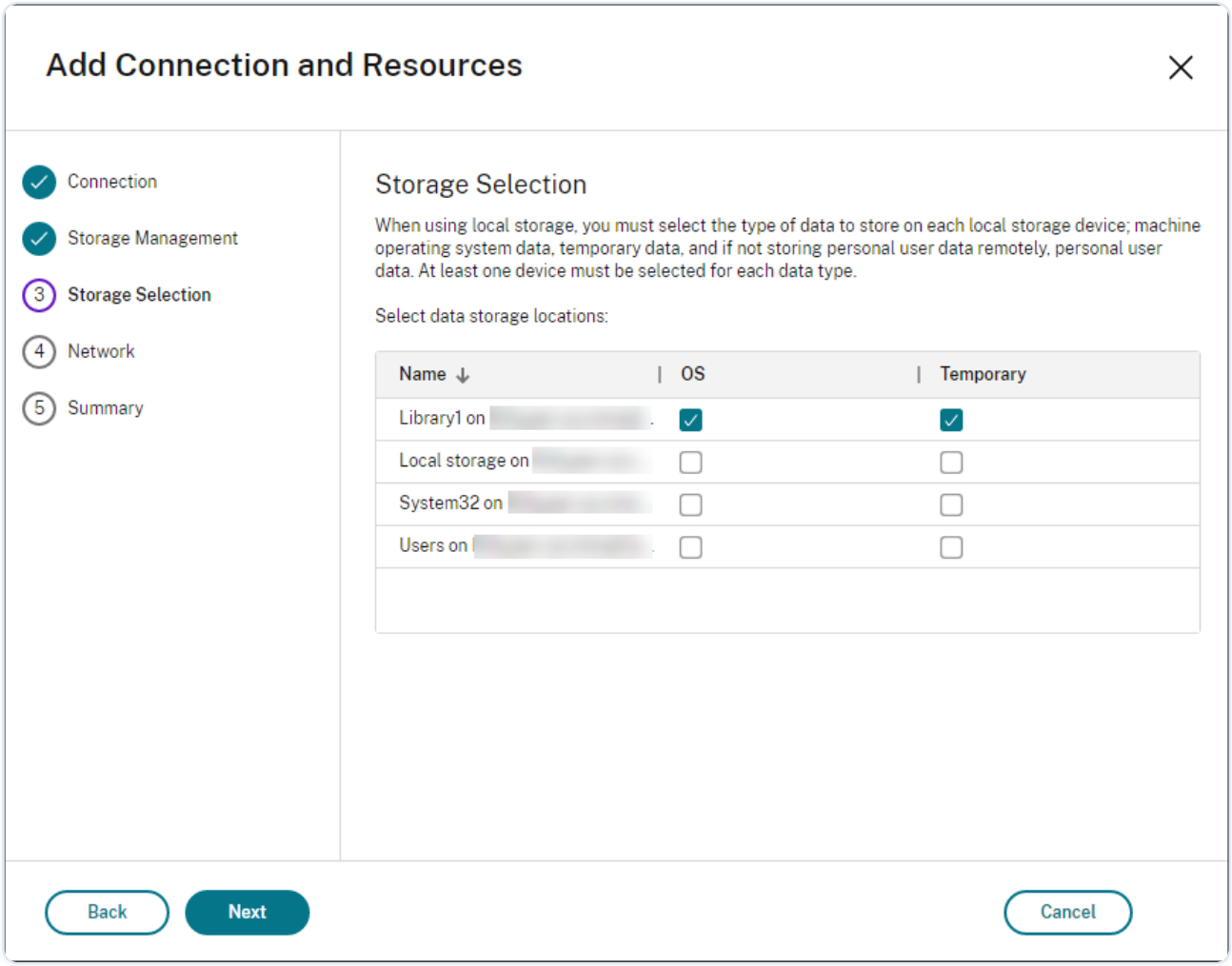
（CSV）を使用する場合、Microsoft System Center Virtual Machine Managerはローカルストレージ上の一時データキャッシュディスクを許可しません。Web Studioでそのストレージ管理設定を構成すると失敗します。

XenServerプールで共有ストレージを使用している場合、共有ストレージデバイスの負荷を軽減するためにIntelliCacheを使用するかどうかを指定します。「XenServer接続でのIntelliCacheの使用」を参照してください。

注:

XenServer、VMware、およびSCVMM仮想化環境では、OSディスクと同じストレージ場所にライトバックキャッシュ（WBC）ディスクを配置できます。この場合、**利用可能なローカルストレージ上の一時データを最適化する**を選択しないでください。

ストレージの選択



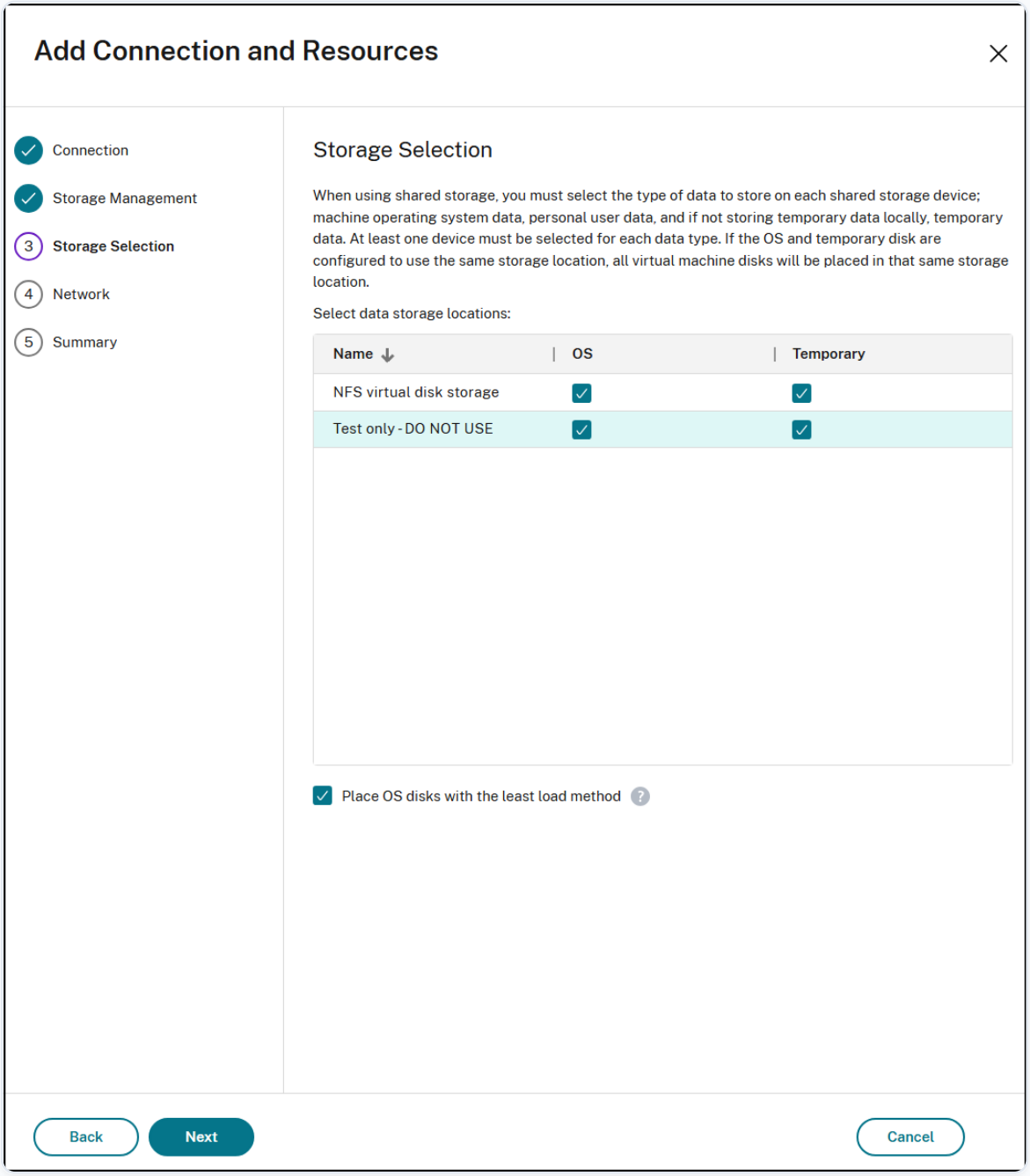
ストレージの選択について詳しくは、「ホストストレージ」を参照してください。

利用可能なデータタイプごとに、少なくとも1つのホストストレージデバイスを選択します。前のページで選択したストレージ管理方法によって、このページで選択できるデータタイプが決まります。ウィザードの次のページに進む前に、サポートされているデータタイプごとに少なくとも1つのストレージデバイスを選択してください。

注:

- XenServer、VMware、SCVMMの仮想化環境では、利用可能なOSストレージリストと利用可能な一時ストレージリストを同じに構成すると、MCSはライトバックキャッシュ（WBC）ディスクをOSディスクと同じストレージの場所に配置します。
- OSデータストレージの場所を2つ以上選択すると、**最小負荷方式でストレージの負荷分散を最適化**オプションが表示されます。このオプションを使用すると、ディスク割り当

てのために最も負荷の低いストレージリポジトリを選択できます。



- **概要**ページには、選択内容に応じてオプションが**有効**か**無効**かが表示されます。**詳細**パネルには、ストレージ割り当て方法の変更が表示されます。**OSストレージ**ページの**ストレージの編集**オプションを使用して調整できます。または、PowerShellを使用して同じ目標を達成することもできます。詳しくは、「VMの柔軟なストレージ場所オプション」を参照してください。

ストレージ管理ページで**ハイパーバイザーで共有されるストレージを使用**を選択し、**利用可能なローカルストレージ上の一時データを最適化**を選択すると、**ストレージの選択**ページで

> より多くの構成オプションを利用できます。たとえば、一時データに使用するローカルストレージデバイス（同じハイパーバイザープール内）を選択できます。

現在選択されているストレージデバイスの数が表示されます（上記のグラフィックでは「1つのストレージデバイスが選択されています」）。そのエントリにマウスカーソルを合わせると、選択されたデバイス名が表示されます。

1. 使用するストレージデバイスを変更するには、**選択**をクリックします。
2. **ストレージの選択**ダイアログボックスで、ストレージデバイスのチェックボックスをオンまたはオフにして、**OK**をクリックします。

ネットワーク

ネットワークページで、リソースの名前を入力します。この名前は、Web Studioに表示され、接続に関連付けられたストレージとネットワークの組み合わせを識別します。

VMが使用する1つ以上のネットワークを選択します。

概要

概要ページで、選択内容を確認します。完了したら、**完了**をクリックします。

注意: 一時データをローカルに保存すると、この接続を使用するマシンを含むマシンカタログを作成する際に、一時データストレージのデフォルト以外の値を構成できます。詳しくは、「マシンカタログの作成」を参照してください。

接続設定の編集

接続の名前を変更したり、接続を作成したりするためにこの手順を使用しないでください。これらは異なる操作です。現在ホストされているマシンのアドレスが変更された場合にのみ、アドレスを変更してください。別のアドレスを別のマシンに入力すると、接続のMachine Catalogsが破損します。

接続の**GPU**設定は変更できません。このリソースにアクセスするMachine Catalogsは、適切なGPU固有のマスターイメージを使用する必要があるためです。接続を作成してください。

1. Web Studioにサインインします。
2. 左ペインで**Hosting**を選択します。
3. 接続を選択し、アクションバーで**Edit Connection**を選択します。
4. 接続を編集する際に利用できる設定のガイダンスに従ってください。

5. 完了したら、**Apply**をクリックして変更を適用し、ウィンドウを開いたままにするか、**Save**をクリックして変更を適用してウィンドウを閉じます。

接続プロパティページ:

- 接続アドレスと資格情報を変更するには、**Edit settings...**を選択し、新しい情報を入力します。
- XenServer接続のハイアベイラビリティサーバーを指定するには、**Edit servers...**を選択し、サーバーを選択します。Citrixでは、プールマスターが故障した場合にXenServerとの通信を可能にするため、プール内のすべてのサーバーを選択することをお勧めします。

> **注:**
>
> HTTPSを使用しており、ハイアベイラビリティサーバーを構成する場合は、プール内のすべてのサーバーにワイルドカード証明書をインストールしないでください。各サーバーに個別の証明書が必要です。

Advancedページ:

- Remote PC Accessで使用されるMicrosoft System Center Configuration Manager (ConfMgr) Wake on LAN接続タイプの場合、**ConfMgr Wake Proxy**、マジックパケット、およびパケット送信情報を入力します。
- スロットリングしきい値設定を使用すると、接続で許可される最大電源アクション数を指定できます。これらの設定は、電源管理設定によって同時に起動するマシンの数が多すぎたり少なすぎたりする場合に役立ちます。各接続タイプには、ほとんどの場合に適切な特定のデフォルト値があり、変更してはなりません。
- 「**同時アクション (すべての種類)**」設定では、この接続で同時に発生できる最大絶対数と、この接続を使用するすべてのマシンの最大パーセンテージという2つの値を指定します。絶対値とパーセンテージ値の両方を指定する必要があります。適用される実際の制限は、これらの値の小さい方です。

  たとえば、34台のマシンがある展開で、「**同時アクション (すべての種類)**」が絶対値10、パーセンテージ値10に設定されている場合、適用される実際の制限は3です（つまり、34の10パーセントを最も近い整数に丸めたもので、絶対値10台のマシンよりも小さい値です）。
- 「**1分あたりの最大新規アクション数**」は絶対数です。パーセンテージ値はありません。
- 「**接続オプション**」フィールドには、Citrixサポート担当者の指示または明示的なドキュメントの指示がある場合にのみ情報を入力してください。

共有テナントページ:

この接続のサブスクリプションとAzure Compute Galleryを共有するテナントとサブスクリプションを追加します。これにより、カタログを作成または更新する際に、それらのテナントとサブスクリプションから共有イメージを選択できます。

- この接続に関連付けられているアプリケーションの「**アプリケーションID**」と「**アプリケーションシークレット**」を入力します。この情報を使用して、Azureに認証できます。セキュリティを確保するために、定期的にキーを変更することをお勧めします。
- 共有テナントとサブスクリプションを指定します。最大8つの共有テナントを追加できます。各テナントには、最大8つのサブスクリプションを追加できます。
- 完了したら、「**保存**」と「**適用**」をクリックします。

「**接続オプション**」フィールドには、Citrixサポート担当者の指示がある場合にのみ情報を入力してください。

ネットワークの編集

接続のネットワークを変更できます。次の手順を実行します。

1. 「**ホスティング**」に移動します。
2. 接続下のターゲットリソースを選択し、アクションバーで「**ネットワークの編集**」を選択します。
3. 仮想マシンが使用するネットワークを1つ以上選択します。
4. 「**保存**」をクリックして変更を保存し、終了します。

接続のメンテナンスモードをオンまたはオフにする

接続のメンテナンスモードをオンにすると、新しい電源操作がその接続に保存されているマシンに影響を与えるのを防ぎます。ユーザーは、マシンがメンテナンスモードの場合、そのマシンに接続できません。ユーザーがすでに接続している場合、メンテナンスモードはログオフ時に有効になります。

1. Web Studioにサインインします。
2. 左ペインで「**ホスティング**」を選択します。
3. 接続を選択します。メンテナンスモードをオンにするには、アクションバーで「**メンテナンスモードをオンにする**」を選択します。メンテナンスモードをオフにするには、「**メンテナンスモードをオフにする**」を選択します。

個々のマシンに対してメンテナンスモードをオンまたはオフにすることもできます。また、マシンカタログまたはデリバリーグループ内のマシンに対してメンテナンスモードをオンまたはオフにすることもできます。

接続を削除する

接続を削除すると、多数のマシンが削除され、データが失われる可能性があります。影響を受けるマシン上のユーザーデータがバックアップされているか、不要であることを確認してください。

接続を削除する前に、以下を確認してください。

- すべてのユーザーが接続に保存されているマシンからログオフしていること。
- 切断されたユーザーセッションが実行されていないこと。
- プールされたマシンと専用マシンのメンテナンスモードがオンになっていること。
- 接続で使用されているマシンカタログ内のすべてのマシンは電源がオフになります。

カタログによって参照されている接続を削除すると、そのマシンカタログは使用できなくなります。この接続がカタログによって参照されている場合、カタログを削除するオプションがあります。カタログを削除する前に、他の接続で使用されていないことを確認してください。

1. Web Studio にサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**接続の削除**を選択します。
4. この接続にマシンが格納されている場合、マシンを削除する必要があるかどうかが尋ねられます。削除する場合は、関連するActive Directoryコンピューターアカウントをどうするかを指定します。

接続の名前を変更またはテストする

1. Web Studio にサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**接続名の変更**または**接続のテスト**を選択します。

TLS証明書の信頼性をテストする

信頼されていない証明書が原因でホスト接続の停止が発生した場合、Web Studio で証明書を再信頼できます。再信頼するには：

1. 左ペインで**ホスティング**を選択します。

2. 証明書を再信頼したい接続を右クリックし、**TLS証明書の信頼性をテスト**を選択します。
3. 次のウィンドウでパスワードを入力し、**保存**をクリックします。
    - 証明書を再信頼する必要がある場合、証明書を信頼するオプションを含む警告ダイアログボックスが表示されます。
    - 証明書がすでに信頼されている場合、証明書が信頼されていることを示す成功ダイアログボックスが表示されます。

接続上のマシンの詳細を表示する

1. Web Studioにサインインします。
2. 左側のペインで**「ホスティング」**を選択します。
3. 接続を選択し、アクションバーで**「マシンの表示」**を選択します。

上部のペインには、接続を介してアクセスされるマシンが一覧表示されます。マシンを選択すると、下部のペインにその詳細が表示されます。開いているセッションのセッション詳細も提供されます。

検索機能を使用して、マシンをすばやく見つけます。ウィンドウ上部のリストから保存された検索を選択するか、新しい検索を作成します。マシン名の全部または一部を入力して検索するか、高度な検索に使用する式を作成できます。式を作成するには、**「展開」**をクリックし、プロパティと演算子のリストから選択します。

接続上のマシンを管理する

1. Web Studioにサインインします。
2. 左側のペインで**「ホスティング」**を選択します。
3. 接続を選択し、**「アクション」ペインで**「マシンの表示」**を選択します。
4. アクションバーで次のいずれかを選択します。一部のアクションは、マシンの状態と接続ホストの種類によっては利用できません。

アクション	説明
起動	マシンが電源オフまたは一時停止状態の場合に起動します。
一時停止	マシンをシャットダウンせずに一時停止し、マシンリストを更新します。

アクション	説明
シャットダウン	オペレーティングシステムにシャットダウンを要求します。
強制シャットダウン	マシンの電源を強制的にオフにし、マシンリストを更新します。
再起動	オペレーティングシステムにシャットダウンを要求し、その後マシンを再起動します。オペレーティングシステムがこれに応じられない場合、デスクトップは現在の状態のままになります。
メンテナンスモードを有効にする	マシンへの接続を一時的に停止します。この状態では、ユーザーはマシンに接続できません。ユーザーが接続している場合、メンテナンスモードはログオフ時に有効になります。（上記のように、接続を介してアクセスされるすべてのマシンに対してメンテナンスモードをオンまたはオフにすることもできます。）
デリバリーグループから削除	マシンをデリバリーグループから削除しても、そのデリバリーグループが使用するマシンカタログからは削除されません。マシンは、ユーザーが接続していない場合にのみ削除できます。マシンを削除している間、ユーザーが一時的に接続できないようにするには、メンテナンスモードをオンにします。
削除	マシンを削除すると、ユーザーはそのマシンにアクセスできなくなり、マシンはマシンカタログから削除されます。マシンを削除する前に、すべてのユーザーデータがバックアップされているか、または不要であることを確認してください。マシンは、ユーザーが接続していない場合にのみ削除できます。マシンを削除している間、ユーザーが一時的に接続できないようにするには、メンテナンスモードをオンにします。

マシンのシャットダウンを伴う操作の場合、マシンが10分以内にシャットダウンしないと、電源がオフになります。Windowsがシャットダウン中に更新プログラムをインストールしようとすると、更新が完了する前にマシンの電源がオフになるリスクがあります。

ストレージの編集

接続を使用するVMのオペレーティングシステムデータと一時データを保存するために使用されるサーバーのステータスを表示できます。また、各データタイプのストレージにどのサーバーを使用するかを指定することもできます。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**ストレージの編集**を選択します。
4. 左ペインで、データタイプ（オペレーティングシステムまたは一時）を選択します。
5. 選択したデータタイプに対して、1つ以上のストレージデバイスのチェックボックスをオンまたはオフにします。
6. **OK**をクリックします。

リスト内の各ストレージデバイスには、その名前とストレージステータスが含まれています。有効なストレージステータスの値は次のとおりです。

- **使用中:** ストレージはマシンの作成に使用されています。
- **廃止済み:** ストレージは既存のマシンにのみ使用されています。このストレージには新しいマシンは追加されません。
- **未使用:** ストレージはマシンの作成に使用されていません。

現在**使用中**のデバイスのチェックボックスをオフにすると、そのステータスは**廃止済み**に変わります。既存のマシンはそのストレージデバイスを引き続き使用し（データを書き込むこともできます）、そのため、マシンの作成に使用されなくなった後でも、その場所がいっぱいになる可能性があります。

リソースの削除、名前の変更、またはテスト

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. リソースを選択し、アクションバーで適切なエントリ（**リソースの削除**、**リソースの名前変更**、または**リソースのテスト**）を選択します。

VMの柔軟なストレージの場所オプション

マシンカタログ内のVMには、さまざまなストレージサービス（SR）が割り当てられます。異なるストレージでのVM割り当てのバランスを取るには、2つのオプションがあります。

- **強化された現在のラウンドロビン割り当て方法**: 常に同じ固定SRから開始するのではなく、MCSは最後に使用されたSRの直後のSRから割り当てを開始します。
- **最小負荷ベースの割り当て方法**: 同じマシンカタログ内の各SR上のVMの総数を比較することで決定される、最も負荷の低い場所にVMを配置します。たとえば、マシンカタログに100個のVMがあり、SR1に20個、SR2に30個、SR3に50個と分散されている場合、新しいVMは最初にSR1に割り当てられます。この方法により、SR1、SR2、SR3間の負荷がバランスされます。

この機能は次のとおりです。

- すべてのオンプレミスハイパーバイザー（VMware、XenServer、Hyper-V）に適用可能
- OS ディスクストレージにのみ適用可能。
- 既存の VM には適用されません

負荷ベースの割り当てオプションを実装するには、ホスト接続の作成または更新時に、カスタムプロパティ`Name="StorageBalanceType"` `Value="VMCountBasedLeastLoad`を追加します。このカスタムプロパティと値を使用しない場合、デフォルトで強化されたラウンドロビン方式が適用されます。

例:

- ホスト接続の作成時:

```
New-Item -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"StorageBalanceType`"
Value=`"VMCountBasedLeastLoad`" /></CustomProperties>"
-HypervisorConnectionName "Xen-Connection" -NetworkPath @("XDHyp:
\Connections\Xen-Connection\Network 0.network") -Path @("XDHyp:
\HostingUnits\XS-Network") -PersonalvDiskStoragePath @() -RootPath
"XDHyp:\Connections\Xen-Connection\" -StoragePath @("XDHyp:
\Connections\Xen-Connection\NFS virtual disk storage.storage")
```

- ホスト接続の更新時:

```
Set-Item  -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"StorageBalanceType`"
Value=`"VMCountBasedLeastLoad`" /></CustomProperties>" -Path @("XDHyp:
\HostingUnits\XS-Network")
```

孤立したAzureリソースの検出

孤立したリソースは、システム内に存在する使用されていないリソースであり、不要な費用につながる可能性があります。

クラウド管理者以外に、**ホスト**の下にある**ハイパーバイザーでホスト接続を使用して孤立したリソースを検出する**権限を持つ新しく作成されたロールは、孤立したリソースを検出できます。

この機能を使用すると、Citrix Virtual Apps and Desktopsサイトのホストにある孤立したAzureリソースを検出できます。

Web Studioで次の手順を実行します。

1. **管理**から、左ペインで**ホスティング**を選択します。
2. 接続を選択し、アクションバーで**孤立したリソースを検出**を選択します。**孤立したリソースを検出**ダイアログボックスに、孤立したリソースレポートが表示されます。
3. 孤立したリソースレポートを表示するには、**レポートの表示**を選択します。

または、PowerShellを使用して孤立したAzureリソースを検出することもできます。詳細については、「孤立したリソースのリストを取得する」を参照してください。

孤立したリソースの原因を理解し、その後の対処方法については、「Citrixで孤立したAzureリソースを効率的に管理する」を参照してください。

接続タイマー

ポリシー設定を使用して、3つの接続タイマーを構成できます。

- 「**最大接続タイマー**」：ユーザーデバイスと仮想デスクトップ間の途切れない接続の最大期間を決定します。「**セッション接続タイマー**」および「**セッション接続タイマー間隔**」ポリシー設定を使用します。
- 「**接続アイドルタイマー**」：ユーザーからの入力がない場合に、仮想デスクトップへの途切れないユーザーデバイス接続が維持される期間を決定します。「**セッションアイドルタイマー**」および「**セッションアイドルタイマー間隔**」ポリシー設定を使用します。

- **接続解除タイマー:** 接続が解除され、ロックされた仮想デスクトップが、セッションがログオフされるまでロックされたままになる時間を決定します。「**接続解除セッションタイマー**」および「**接続解除セッションタイマー間隔**」ポリシー設定を使用します。

これらの設定のいずれかを更新する場合は、展開全体で一貫性があることを確認してください。

詳細については、ポリシー設定のドキュメントを参照してください。

孤立したリソースのリストを取得する

MCSによって作成されたものの、MCSによって追跡されなくなった孤立したリソースのリストを取得できます。これは現在、Azure環境に適用されます。リストを取得するには、PowerShellコマンドを使用できます。接続を使用してフィルタリングできます。

デフォルトでは、**フル管理者**および**クラウド管理者**の役割にはこの権限が割り当てられています。他の役割にこのアクションを実行させるには、**ホスト**の下にある**ハイパーバイザーでホスト接続を使用して孤立したリソースを検出する**権限を割り当てます。詳細については、役割の作成と管理を参照してください。

> **注:**
>
> - プロビジョニングまたはイメージの更新が進行中の場合、PowerShellコマンドは拒否されます。
> - すべてのCitrixタグが付けられた顧客管理リソースは、孤立したリソースとして検出されます。ただし、そのリソースに値がtrueの別のタグCitrixDetectIgnoreを追加すると、孤立したリソースの検出中にそのリソースは無視されます。

制限事項

- 組み込みのフル管理者またはクラウド管理者ロールの管理者ユーザーのみが、PowerShellコマンドを実行して孤立したリソースのリストを取得できます。
- 孤立したリソースの誤認識を避けるため、孤立したリソースをフィルタリングしている間はVMの電源をオンにしないでください。
- 負荷が高い可能性がある場合、約2,000件のレコードが孤立として表示されます。

孤立したリソースのリストを表示するには：

1. **PowerShell**ウィンドウを開きます。

2. 次のコマンドを実行します。

    a. 接続UIDを取得します。接続UIDは、HypervisorConnectionUid属性の値です。

    ```
    Get-ChildItem xdhyp:\connections | where { $_.PluginId -like
    'Azure*' }"
    ```

    b. 孤立したリソースのリストを取得します。

    ```
    get-provorphanedresource -HypervisorConnectionUid <connection uid>
    ```

サブスクリプションIDから孤立リソースのリストを表示するには：

1. **PowerShell**ウィンドウを開きます。
2. 次のコマンドを実行します。

    a. サブスクリプションIDを使用して接続uidを見つけます。接続uidは HypervisorConnectionUid属性の値です。

    ```
    Get-ChildItem xdhyp:\connections | where { $_.CustomProperties
    -match '<subscriptionId>' }
    ```

    b. 孤立リソースのリストを取得します。

    ```
    get-provorphanedresource -HypervisorConnectionUid <connection uid>
    ```

注:

削除する前にリソースを慎重に確認してください。

ホスティング接続にWinHttp (netsh) プロキシサーバー設定を使用する

この機能強化により、ホスティング接続でWinHttp (netsh) プロキシサーバー設定をホスティング接続で使用できるようになります。これにより、プロキシ設定が簡素化され、他のCitrixサービスで使用されるプロキシ設定構成とも整合性が取れます。

この機能は、以下の仮想化環境に適用されます。

- XenServer
- Google クラウド
- マイクロソフト Azure
- ニュータニックス
- レッドハット オープンシフト
- ヴイエムウェア

ホスティング接続に、デリバリーコントローラーで構成されているWinHttp (netsh) プロキシサーバーを使用するには、このカスタムプロパティをホスティング接続に含めることができます。

```
<Property xsi:type="StringProperty"
Name="UseWinHttpProxyForHypervisorTraffic" Value="True" />
```

- このカスタムプロパティが`True`に設定されている場合、ハイパーバイザーへのAPI呼び出しは、`netsh winhttp set proxy`コマンドを介してマシン上で設定されている場合は、WinHttpプロキシサーバーを介してルーティングされます。
- このカスタムプロパティが`False`に設定されている場合、API呼び出しはDDCで構成されているすべてのプロキシサーバー（WinINetプロキシおよび.netプロキシを含む）を無視します。
- このカスタムプロパティがホスティング接続に存在しない場合、マシン用の`WinINet`または`.net`プロキシサーバー構成が使用されます。これは既存の動作です。

ユースケース

- 例1：ホスティング接続にカスタムプロパティが設定されていない場合

  ホスティング接続は、WinINetプロキシ構成、続いて.netプロキシ構成を読み取り、構成されている場合はプロキシ設定を使用します。いずれも構成されていない場合は、直接接続が作成されます。これは既存の動作であり、そのまま機能し続けます。

- 例2：ホスティング接続にカスタムプロパティが「True」に設定されている場合

  ホスティング接続はWinHttpプロキシ設定のみを読み取り、存在する場合はプロキシ設定を使用します。存在しない場合、ホスティング接続にはプロキシ設定は使用されません。

- 例3：カスタムプロパティがホスティング接続に値 = False で設定されている

  ホスティング接続はマシン上のプロキシ構成設定を読み取らず、プロキシなしでハイパーバイザーへの接続を試行します。

前提条件

PowerShellを使用してホスト接続を作成する際にカスタムプロパティを設定する前に、すべてのDesktop Delivery ControllerでWinHTTPプロキシを構成していることを確認してください。

構成手順

CLIを介してWinHttpプロキシ設定を使用する新しいホスティング接続を作成するには：

```
$CustomProperties = "<CustomProperties  xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<!-- Include any other hypervisor specific custom properties here -->

<Property xsi:type=`"StringProperty`"
Name=`"UseWinHttpProxyForHypervisorTraffic`" Value=`"True`" />

</CustomProperties>"



New-Item -ConnectionType $ConnectionType -HypervisorAddress @('https://
hypervisorhost1.example.com') -Path @('XDHyp:\Connections\
$ConnectionName') -Password $Password -UserName $User -CustomProperties
$CustomProperties
```

既存のホスティング接続にカスタムプロパティを設定するには：

1. 既存のホスティング接続からカスタムプロパティが存在する場合はコピーします。

   ```
   dir XDHyp:\Connections
   ```

2. ホスティング接続のカスタムプロパティをコピーし、以下を追加して変数に保存します。

   ```
   $CustomProperties

   <Property xsi:type=`"StringProperty`"
   Name=`"UseWinHttpProxyForHypervisorTraffic`" Value=`"True`" />
   ```

   例:

```
Example:

$CustomProperties = "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
Value=`"123`" />

<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
Value=`"https://management.azure.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
Value=`"https://login.microsoftonline.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`"
Value=`"core.windows.net`" />

<Property xsi:type=`"StringProperty`" Name=`"TenantId`"
Value=`"123abc`" />

<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`"
Value=`"`[ { 'Tenant':'123abc', 'Subscriptions':['345', '567'] } ]`"` /
><Property xsi:type=`"StringProperty`"
Name=`"UseWinHttpProxyForHypervisorTraffic`" Value=`"True`" />

</CustomProperties>"
```

既存のカスタムプロパティが空だった場合、カスタムプロパティを設定します:

```
$CustomProperties = "<CustomProperties  xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`"
Name=`"UseWinHttpProxyForHypervisorTraffic`" Value=`"True`" />

</CustomProperties>"
```

3. 既存のホスティング接続を更新するには、`Set-Item` コマンドを実行します。

```
Set-Item -CustomProperties $CustomProperties -LiteralPath @("XDHyp:
\Connections\$ConnectionName") -PassThru -UserName $User
-SecurePassword $Password
```

次のステップ

特定のホストタイプへの接続については、以下を参照してください:

- AWS への接続
- XenServer への接続
- Google Cloud 環境への接続
- Microsoft Azure への接続
- マイクロソフト システムセンター バーチャルマシンマネージャー への接続
- Nutanixへの接続
- Nutanixクラウドおよびパートナーソリューションへの接続
- VMwareへの接続
- VMwareクラウドおよびパートナーソリューションへの接続

初期展開プロセス中の場合は、マシンカタログを作成します。

AWS EC2への接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明します。以下の情報では、AWSクラウド環境に固有の詳細について説明します。

前提条件

AWS EC2への接続を作成する前に、以下を実行してください。

- リソースの場所としてAWSのセットアップを完了します。AWS仮想化環境を参照してください。
- Citrixがお客様に代わってAWSリソースを管理するためのIAMユーザーまたはロールのIAM権限を定義するポリシー。

IAM権限を定義する

ホスト接続を作成する前に、Citrixがお客様に代わってAWSアカウント内のリソースをプロビジョニングおよび管理するための適切な権限を付与するIAMユーザーまたはロールに対して、IAM権限ポリシーを適切に定義する必要があります。このセクションの情報を使用して、AWS上のCitrix

Virtual Apps and DesktopsのIAM権限を定義します。AmazonのIAMサービスでは、複数のユーザーを持つアカウントが許可されており、それらのユーザーはさらにグループに編成できます。これらのユーザーは、アカウントに関連する操作を実行する能力を制御するために、異なる権限を持つことができます。IAM権限の詳細については、IAM JSONポリシーリファレンスを参照してください。

IAM権限ポリシーを新しいユーザーグループに適用するには：

1. AWSマネジメントコンソールにログインし、ドロップダウンリストから**IAMサービス**を選択します。
2. **新しいユーザーグループの作成**を選択します。
3. 新しいユーザーグループの名前を入力し、**続行**を選択します。
4. **権限**ページで、**カスタムポリシー**を選択し、次に**選択**を選択します。
5. **権限ポリシー**の名前を入力します。
6. **ポリシー ドキュメント**セクションで、関連する権限を入力します。

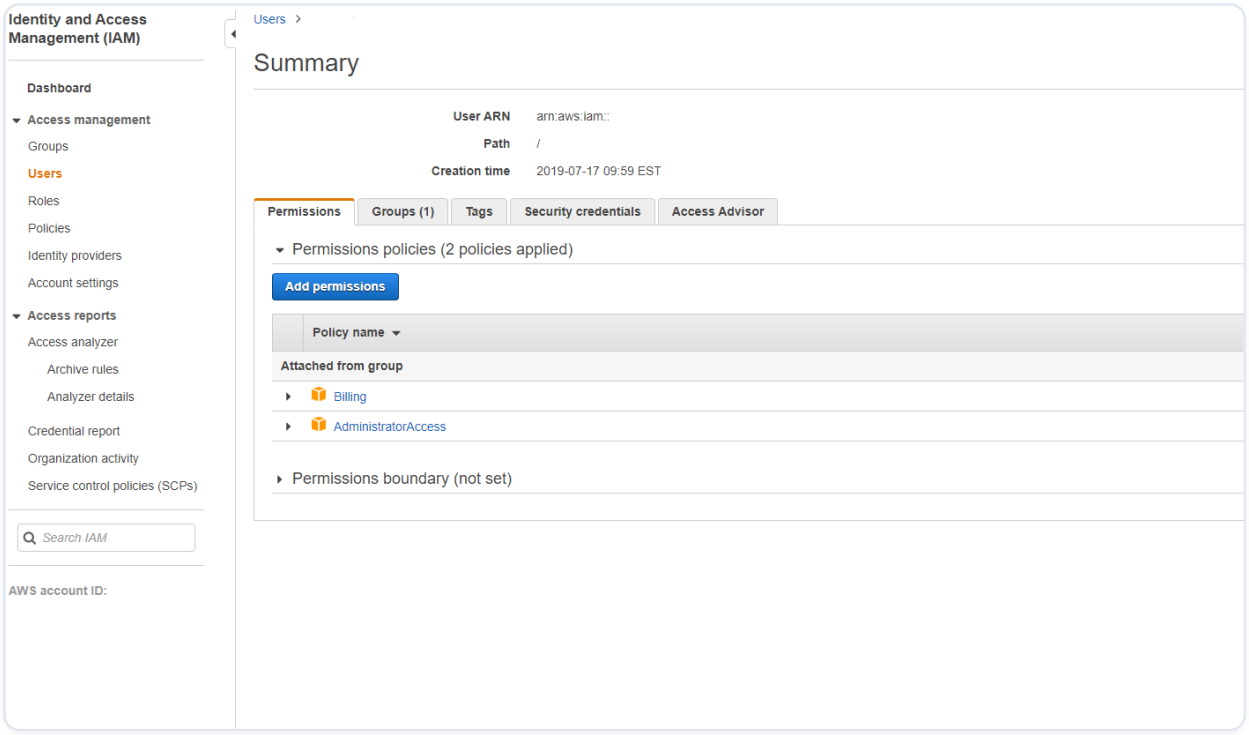
ポリシー情報を入力したら、**続行**を選択して、IAMアクセス許可ポリシーをユーザーグループに適用するプロセスを完了します。グループ内のユーザーには、Citrix Virtual Apps and Desktopsに必要なアクションのみを実行するアクセス許可が付与されます。

> **重要:**
>
> この記事の例で提供されているポリシーテキストを使用して、Citrix Virtual Apps and DesktopsがAWSアカウント内でアクションを実行するために使用するアクションを、特定のリソースに制限することなくリストします。Citrixは、テスト目的でこの例を使用することをお勧めします。本番環境では、リソースにさらなる制限を追加することを選択できます。

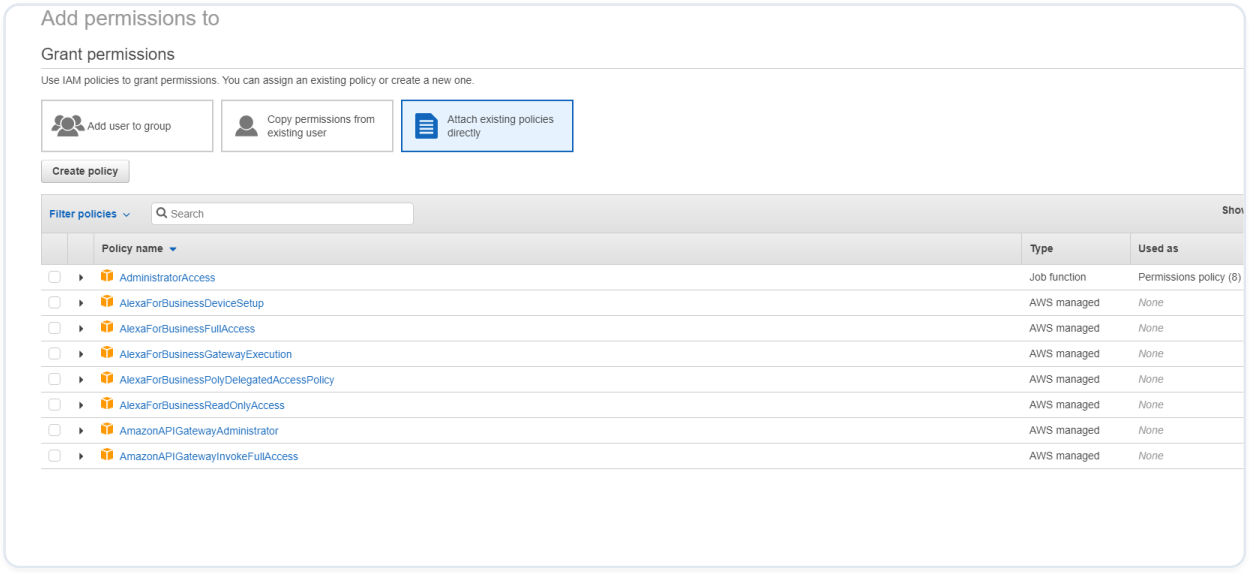
IAMアクセス許可を追加する

AWSマネジメントコンソールの**IAM**セクションでアクセス許可を追加します。

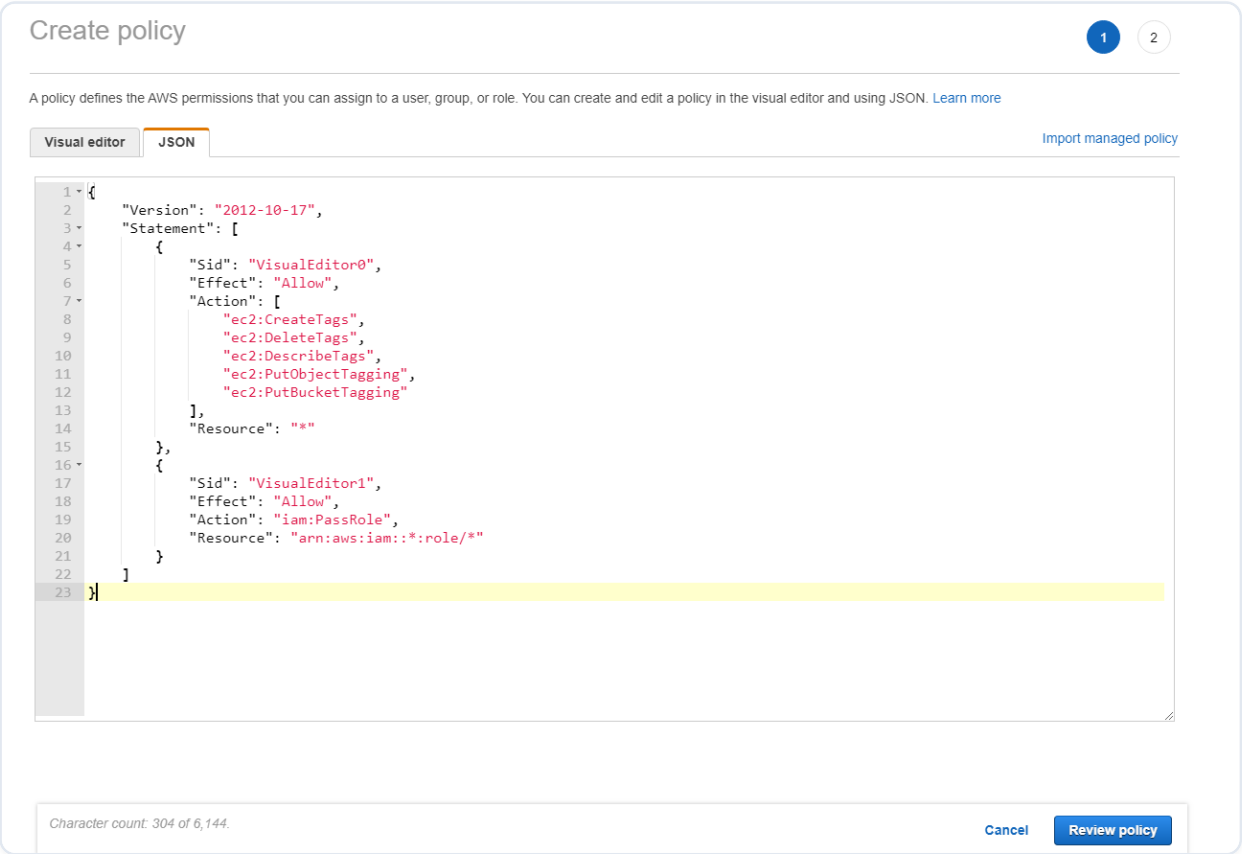
1. **概要**パネルで、**アクセス許可**タブを選択します。
2. **アクセス許可を追加**を選択します。



3. **アクセス許可の追加先**画面で、アクセス許可を付与します。



4. JSONセクションで、環境に必要なAWSアクセス許可を含めます。



接続を作成する

Amazon EC2への接続は、以下を使用して作成できます。

- ウェブスタジオ
- 「PowerShell コマンド」(#create-a-connection-using-powershell)

> **注:**
>
> プロキシサーバーまたはファイアウォールの制限を確認し、次のアドレスに接続できることを確認してください: `https://*.amazonaws.com`。また、Citrix Gateway service connectivityに記載されているすべてのアドレスに接続できることを確認してください。

> これらに接続できない場合、ホスト接続の作成または更新中に障害が発生する可能性があります。

Web Studioを使用した接続の作成

1. **Hosting > Add Connection and Resources** ページに移動します。
2. **接続**ページで、以下の手順に従って接続を構成します。

a. **Create a new connection**を選択します。

b. **Zone**で、AWS環境用に設定したリソースの場所を選択します。

c. 接続タイプとして**Amazon EC2**を選択します。

d. リソースをプロビジョニングする方法のいずれかを選択します。

- **Use this AWS account to provision resources**を選択した場合、**Use IAM user access key**または**Use IAM role**を選択します。IAMユーザーアクセスキーの場合、CitrixがAWSアカウントのリソースを管理するための適切なIAM権限ポリシーを持つIAMユーザーの**API key**と**Secret key**を入力します。IAMロールの場合、CitrixがAWSアカウントのリソースを管理するための適切なIAM権限ポリシーを持つassigned an IAM roleをDelivery Controllerインスタンスに割り当てていることを確認してください。詳細については、Role-based authentication guideを参照してください。
- **Use cross-account access to provision resources**を選択した場合、アカウントAのDelivery Controllerが引き受けてプロビジョニング操作を実行する必要がある、アカウントBのIAMロールの**ARN**を入力します。

e. 接続名を入力し、**Next**をクリックします。

3. **Virtual Machine Location**ページで、VMをプロビジョニングする場所を指定します。新しいVMを作成するためのクラウドリージョン、VPC、およびアベイラビリティゾーンを選択します。
4. 「**ネットワーク**」ページで：

a. 以前にアベイラビリティゾーンまたはローカルゾーンで選択したリソースの名前を入力します。

b. 前のメニューで構成したVPC内の1つ以上のサブネットを選択します。

5. 残りのページを順に進み、「**概要**」ページまでクリックします。
6. **完了**をクリックして、Amazon EC2へのホスト接続を作成します。

重要な考慮事項

Studioを使用して接続を作成する場合:

- CitrixがAWSリソースを管理するための適切なIAM権限を定義します。
- CitrixがAWSリソースを管理するためにIAMユーザーアクセスキーを使用する場合、APIキーとシークレットキーの値を指定する必要があります。これらの値を含むキーファイルをAWSからエクスポートし、インポートできます。また、リージョン、アベイラビリティゾーン、VPC

名、サブネットアドレス、ドメイン名、セキュリティグループ名、および資格情報も指定する必要があります。

- CitrixがAWSリソースを管理するためにIAMロールを使用する場合、すべてのDelivery Controllerに適切なIAM権限を持つロールを割り当てるようにしてください。詳細については、ロールベース認証ガイドを参照してください。
- ルートAWSアカウントの資格情報ファイル（AWSコンソールから取得）は、標準のAWSユーザー用にダウンロードされた資格情報ファイルと同じ形式ではありません。そのため、Citrix Virtual Apps and Desktopsは、APIキーとシークレットキーのフィールドに入力するためにこのファイルを使用できません。AWS Identity Access Management (IAM) 資格情報ファイルを使用していることを確認してください。
- ゾーンはアベイラビリティゾーンまたはローカルゾーンのいずれかです。

PowerShellを使用して接続を作成する

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. 次のコマンドを実行します。以下に例を示します。

```
$connectionName = "demo-hostingconnection"

$cloudRegion = "us-east-1"

$apiKey = "aaaaaaaaaaaaaaaaaaaa"

$apiSecret = “bbbbb”

$secureKey = ConvertTo-SecureString -String $apiSecret

$zoneUid = "00000000-0000-0000-0000-000000000000"

$connectionPath = "XDHyp:\Connections\" + $connectionName



$connection = New-Item -Path $connectionPath -ConnectionType "<name of
the connection>" -HypervisorAddress " "@("https://ec2.cn-
north-1.amazonaws.com.cn") -Persist -Scope @() -UserName $apiKey
-SecurePassword $secureKey -ZoneUid $zoneUid
```

```
New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid



$hostingUnitName = "demo-hostingunit"

$availabilityzone = "us-east-1a"

$vpcName = "Default VPC"

$jobGroup = [Guid]::NewGuid()

$hostingUnitPath = "XDHyp:\HostingUnits\" + $HostingUnitName

$rootPath = $connectionPath + "\" + $vpcName + ".virtualprivatecloud\"

$availabilityZonePath = @($rootPath + $availabilityzone +
".availabilityzone")

$networkPaths = (Get-ChildItem $availabilityZonePath[0] | Where
ObjectType -eq "Network") | Select-Object -ExpandProperty FullPath #
will select all the networks in the availability zone



New-Item -Path $hostingUnitPath -AvailabilityZonePath
$availabilityZonePath -HypervisorConnectionName $connectionName
-JobGroup $jobGroup -PersonalvDiskStoragePath @() -RootPath $rootPath
-NetworkPath $networkPaths
```

注:

ロールベース認証を使用して接続を作成するには、apiKey と apiSecret を `role_based_auth` として指定します。

制限事項

AWS コンソールで AWS Virtual Private Cloud (VPC) の名前を変更すると、Citrix Cloud™ の既存のホスティングユニットが破損します。ホスティングユニットが破損すると、カタログを作成した

り、既存のカタログにマシンを追加したりできなくなります。この問題を解決するには、AWS VPC の名前を元の名前に戻します。

クロスアカウントプロビジョニング

Delivery Controller を別の AWS アカウント (共有サービスアカウントまたはサイトコンポーネントアカウント) に配置し、クロスアカウントアクセス (クロスアカウント IAM ロール) を持つ IAM ロールと、別のセカンダリ AWS アカウント (ワークロードアカウント) に MCS プロビジョニングされたマシンカタログを配置するユースケースがあります。この場合、別の追加の Delivery Controller は不要です。このようなシナリオをサポートするために、この機能は VPC ピアリングと IAM ロールを使用したクロスアカウントアクセスを利用して、複数の AWS アカウントを管理する企業向けに異なる AWS アカウント間でのプロビジョニングを可能にします。

VPCピアリングを使用すると、Delivery Controllerと、異なるリージョンまたはアカウントにあるプロビジョニングされたVMが相互に通信できるようになります。

IAMロールを使用したクロスアカウントアクセスを使用すると、プライマリアカウント（Delivery Controllerアカウント）がIAMロールを引き受けて、セカンダリアカウント（マシンカタログVM）のAWSリソースにアクセスできるようになります。

Delivery Controllerがセカンダリアカウントのリソースにアクセスできるようにするには、セカンダリアカウントからIAMロールを引き受けた後、ホスト接続を作成します。

前提条件

クロスアカウントプロビジョニング用のホスト接続を作成する前に、以下を設定してください。

- VPC ピアリングを設定し、両方のリージョンまたはアカウントでセキュリティグループを構成します。VPC ピアリングの設定 を参照してください。
- IAM ロールを使用してクロスアカウントアクセスを委任します。IAM ロールを使用したクロスアカウントアクセスの委1任 を参照してください。

VPCピアリングを設定する

VPC Aがプライマリアカウント（アカウントA）にあり、Delivery ControllersとActive Directoryを持っていると仮定します。VPC Bはセカンダリアカウント（アカウントB）にあり、VMをプロビジョニングしたい場所です。

アカウントAとアカウントBの間にVPCピアリング接続を設定するには、次の手順を実行します。

1. VPCピアリング接続を作成します。参照:
    - 異なるアカウント、同じリージョン

- 異なるアカウント、異なるリージョン

2. VPC Aに移動し、パブリックサブネットに関連付けられているルートテーブルに移動します。
3. **Edit Routes > Add route** をクリックします。**Destination** 列にVPC BのCIDRブロックを追加し、**Target** 列に作成したVPCピアリングを追加します。
4. 手順2と3を繰り返しますが、VPC AとVPC Bのプライベートサブネットを使用します（VPC AのCIDRブロックを追加します）。VPCピアリング接続のルートテーブルを更新するを参照してください。
5. VPC Aに関連付けられているプライベートセキュリティグループに移動します。
6. **Actions** を選択し、次に **Edit inbound rules** を選択します。
7. **Add rule** を選択します。タイプには **All Traffic** を選択し、**Source Column** に以下を追加します。
   - 異なるリージョンの場合は、VPC BのCIDRブロックを追加します。
   - 異なるアカウントだが同じリージョンの場合は、VPC BのアカウントIDとプライベートセキュリティグループIDをスラッシュで区切って追加します（例: 123456789012/sg-1a2b3c4d）。
8. 手順5から7を繰り返しますが、VPC Bのプライベートセキュリティグループを使用します（ただし、VPC AのCIDRブロック、または同じリージョンだが異なるアカウントのVPC Aのアカウント IDとプライベートセキュリティグループIDを追加します）。ピアセキュリティグループを参照するようにセキュリティグループを更新するを参照してください。

> **注:**
>
> VPCピアリング接続の作成に料金はかかりません。ただし、アベイラビリティゾーン内のVPCピアリングは無料ですが、VPCピアリング接続を介したデータ転送が複数のアベイラビリティゾーンとリージョンをまたがって発生する場合、料金が発生します。VPCピアリング接続の料金を参照してください。

IAMロールを使用したクロスアカウントアクセスの委任

アカウント間で VPC ピアリングを設定した後、IAM ロールを使用してクロスアカウントアクセスを委任します。

IAMロールを使用したクロスアカウントアクセスにより、プライマリアカウント（デリバリーコントローラーアカウント）がIAMロールを引き受けて、セカンダリアカウント（マシンカタログVM）内のAWSリソースにアクセスできるようになります。

クロスアカウントリソースにアクセスするには、次の手順を実行します。

> **注意：**
>
> VPC Aはプライマリアカウント（アカウントA）にあり、Delivery ControllerとActive Directoryが含まれていると仮定します。VPC Bは、VMをプロビジョニングするセカンダリアカウント（アカウントB）にあります。

1. 前述の手順で、アカウント間でVPCピアリングを設定します。
2. アカウントBで、最小限のCitrix IAM権限を持つIAMロールとポリシーを作成します。IAMチュートリアル：IAMロールを使用してAWSアカウント間でアクセスを委任するを参照してください。このロールのARNが「arn:aws:iam::5678:role/citrix-role」であるとします。
3. ロール「arn:aws:iam::5678:role/citrix-role」に信頼ポリシーを追加し、IAMでのクロスアカウントリソースアクセスに従って、アカウントAのロール「arn:aws:iam::1234:role/primary-account-citrix-role」からアクセスできるようにします。
4. アカウントAで、前述の「primary-account-citrix role」という名前でIAMロールとポリシーを作成します。これにより、アカウントBのIAMロール（arn:aws:iam::5678:role/citrix-role）を引き受け、そのIAMロールを渡すことができます。
5. ロール「arn:aws:iam::1234:role/primary-account-citrix-role」をアカウントAのすべてのDelivery Controllerに割り当てます。

デリバリーコントローラーは、アカウントBからロール（"arn:aws:iam::5678:role/citrix-role"）を引き受けることができるようになりました。

クロスアカウントプロビジョニング用のホスト接続を作成する

VMをプロビジョニングするセカンダリアカウント（アカウントB）にホスト接続を作成します。これにより、アカウントAのDelivery Controllerは、アカウントBのロールを引き受けた後、アカウントBのリソースにアクセスできるようになります。

PowerShell コマンドを使用してホスト接続を作成し、次の2つのカスタムプロパティを追加します。

- `CrossAccountRoleArn`: `CrossAccountRoleArn` プロパティを指定しない場合、通常のホスト接続が作成されます。この場合、`MaximumAssumeRoleDurationInSeconds` が指定されていても無視されます。

- `MaximumAssumeRoleDurationInSeconds`: `DurationInSeconds` は900秒から3600秒の間である必要があります。デフォルトは900秒です。3600を超える値を指定した場合、`DurationInSeconds` は3600に設定されます。

例:

```
$connectionName = "cross-account-conn"

$cloudRegion = "us-east-1"

$apiKey = "role_based_auth"

$secretKey = "role_based_auth"

$zoneUid = "xxxxxx"

$secureKey = (ConvertTo-SecureString -String $secretKey -AsPlainText
-Force)

$connectionPath = "XDHyp:\Connections\" + $connectionName

$customProperties = '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="CrossAccountRoleArn"
Value="arn:aws:iam::5678:role/citrix-role" /><Property
xsi:type="StringProperty" Name="MaximumAssumeRoleDurationInSeconds"
Value="3600" />

"</CustomProperties>'



$connection = New-Item -Path $connectionPath -ConnectionType "AWS"
-HypervisorAddress "https://ec2.$($cloudRegion).amazonaws.com" -Persist
-Scope @() -UserName $apiKey -SecurePassword $secureKey -ZoneUid $zoneUid
-CustomProperties $customProperties
```

```
New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid
```

ホスト接続が作成されたら、Studio または PowerShell を使用してホスティングユニットを作成します。ただし、VPC とネットワークを選択してください。

接続を編集する

既存のホスト接続を編集して、次の操作を行うことができます。

- Citrixがリソースを管理するためのIAM権限を提供するオプションを変更する(#edit-options-to-provide-iam-permissions)
- ホスティング接続あたりの同時アクション（または同時マシン）の最大数を変更する(#modify-the-maximum-number-of-simultaneous-actions)
- スコープを変更する。
- PowerShellコマンドを使用して、エラスティックネットワークインターフェイス（ENI）あたりのセキュリティグループの最大数を構成する(#configure-security-groups-per-network-interface)

IAM権限を提供するオプションを編集する

1. 既存のAmazon EC2接続を右クリックします。
2. **Connection Properties（接続プロパティ）**ページで、**Edit settings（設定の編集）**をクリックします。
3. Citrixがリソースを管理するためのIAM権限を提供するオプションのいずれかを選択します。必要な詳細を入力し、**Save（保存）**をクリックします。

同時実行アクションの最大数を変更する

StudioでAmazon EC2のホスト接続を作成すると、以下のデフォルト値が表示されます。

オプション	絶対値	パーセンテージ
同時実行アクション（すべての種類）	125	100
1分あたりの新規アクションの最大数	150	n/a

オプション	絶対値	パーセンテージ
最大同時プロビジョニング操作	100	n/a

MCS は、デフォルトで最大 100 の同時プロビジョニング操作をサポートしています。

これらの値は、「**接続の編集**」画面のCitrix Studioの「**詳細設定**」セクションにアクセスして構成します。

または、Remote PowerShell SDK を使用して、環境に応じた最適な設定のために同時操作の最大数を設定できます。

PowerShellカスタムプロパティ `MaximumConcurrentProvisioningOperations` を使用して、AWSプロビジョニングの同時操作の最大数を指定します。

構成前:

- Cloud用のPowerShell SDKがインストールされていることを確認してください。
- `MaximumConcurrentProvisioningOperations` のデフォルト値が100であることを理解してください。

`MaximumConcurrentProvisioningOperations` の値をカスタマイズするには、次の手順を実行します。

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*` を実行して、Citrix固有のPowerShellモジュールをロードします。
3. `cd xdhyp:\Connections\` を入力します。
4. `dir` を入力して、接続を一覧表示します。
5. カスタムプロパティ文字列を変更または初期化します。
    - カスタムプロパティ文字列に値がある場合は、カスタムプロパティをメモ帳にコピーします。次に、`MaximumConcurrentProvisioningOperations` プロパティを希望の値に変更します。1〜1000の範囲で値を入力できます。 例: `<Property xsi:type="IntProperty" Name="MaximumConcurrentProvisioningOperations" Value="xyz"/>`。
    - カスタムプロパティ文字列が空またはnullの場合は、スキーマと `MaximumConcurrentProvisioningOperations` プロパティの両方に適切な構文を入力して文字列を初期化する必要があります。

6. **PowerShell** ウィンドウで、メモ帳から変更したカスタムプロパティを貼り付け、変更したカスタムプロパティに変数名を割り当てます。カスタムプロパティを初期化した場合は、構文の後に次の行を追加します。

   `$customProperties = '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><Property xsi:type="IntProperty" Name="MaximumConcurrentProvisioningOperations" Value="100"/></CustomProperties>'`。

   この文字列は`MaximumConcurrentProvisioningOperations`プロパティを100に設定します。カスタムプロパティ文字列では、`MaximumConcurrentProvisioningOperations`プロパティをニーズに合った値に設定する必要があります。

7. `Get-XDAuthentication`を入力します。これにより、資格情報の入力を求められます。
8. `$cred = Get-Credential`を実行します。これにより、パスワードのみ（または名前とパスワード）の入力を求められる場合があります。アプリケーションIDと関連するシークレットの入力を求められる場合もあります。ロールベース認証を使用する接続の場合、**role_based_auth**は名前とパスワードの両方です。それ以外の場合は、AWS API IDとシークレットを入力します。
9. `set-item -PSPath 'XDHyp:\Connections<connection-name>' -CustomProperties $customProperties -username $cred.username -Securepassword $cred.password`を実行します。*<connection-name>*を接続の名前に設定する必要があります。
10. 更新されたCustomProperties文字列を確認するために、`dir`を入力します。

ネットワークインターフェースごとのセキュリティグループを構成する

ホスト接続を編集する際、PowerShellコマンドを使用して、エラスティックネットワークインターフェイス（ENI）ごとに許可されるセキュリティグループの最大数を構成できるようになりました。AWSセキュリティグループのクォータ値については、「セキュリティグループ」を参照してください。

ネットワークインターフェースごとにセキュリティグループを構成するには:

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために、`asnp citrix*`を実行します。
3. `cd xdhyp:\Connections\`を実行します。
4. 接続を一覧表示するために、`dir`を実行します。

5. ネットワークインターフェイスごとにセキュリティグループを構成するには、次のPowerShellコマンドを実行します。

```
Set-HypHypervisorConnectionMetadata -HypervisorConnectionName aws -Name
"Citrix_MachineManagement_Options" -Value "
AwsMaxENISecurityGroupLimit=<number>"
```

> **注:**
>
> `AwsMaxENISecurityGroupLimit`に値を設定しない場合、デフォルト値の5が使用されます。

サービスエンドポイントURL

標準ゾーンサービスエンドポイントURL

MCSを使用すると、APIキーとAPIシークレットを持つ新しいAWS接続が追加されます。この情報と認証済みアカウントを使用して、MCSはAWS DescribeRegions EC2 API呼び出しを使用して、サポートされているゾーンについてAWSにクエリを実行します。クエリは汎用EC2サービスエンドポイントURL `https://ec2.amazonaws.com/` を使用して行われます。MCSを使用して、サポートされているゾーンのリストから接続するゾーンを選択します。優先されるAWSサービスエンドポイントURLは、そのゾーンに対して自動的に選択されます。ただし、サービスエンドポイントURLを作成した後で、そのURLを設定または変更することはできません。

必要なAWS権限

このセクションには、AWS権限の完全なリストが含まれています。機能が正しく動作するように、このセクションに記載されている権限の完全なセットを使用してください。

> **注:**
>
> `iam:PassRole` 権限は **role_based_auth** にのみ必要です。

ホスト接続の作成

AWSから取得した情報を使用して、新しいホスト接続が追加されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

VMの電源管理

VMの電源はオンまたはオフになります。

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

```
                "ec2:DescribeInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:RebootInstances",
                "ec2:DescribeInstanceStatus"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

VMの作成、更新、または削除

AWSインスタンスとしてプロビジョニングされたVMを使用して、マシンカタログが作成、更新、または削除されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
```

```
                "ec2:RevokeSecurityGroupEgress",

                "ec2:AuthorizeSecurityGroupIngress",

                "ec2:CreateImage",

                "ec2:CreateLaunchTemplate",

                "ec2:CreateSecurityGroup",

                "ec2:CreateTags",

                "ec2:CreateVolume",

                "ec2:DeleteVolume",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",
```

```
                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:CancelSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",



                "ec2:GetLaunchTemplateData",

                "ec2:DescribeVolumes",

                "ec2:DescribeVpcs",

                "ec2:DetachVolume",

                "ec2:DisassociateIamInstanceProfile",

                "ec2:RunInstances",

                "ec2:StartInstances",

                "ec2:StopInstances",

                "ec2:TerminateInstances"

            ],

            "Effect": "Allow",

            "Resource": "*"

        },

        {

            "Action": [

                "ec2:CreateSecurityGroup",
```

```
                "ec2:DeleteSecurityGroup"

            ],

            "Effect": "Allow",

            "Resource": "*"

        },

        {

            "Action": [

                "ebs:StartSnapshot",

                "ebs:GetSnapshotBlock",

                "ebs:PutSnapshotBlock",

                "ebs:CompleteSnapshot",

                "ebs:ListSnapshotBlocks",

                "ebs:ListChangedBlocks",

                "ec2:CreateSnapshot"

            ],

            "Effect": "Allow",

            "Resource": "*"

        }

    ]

}
```

注:

- 「SecurityGroups」に関連するEC2セクションは、カタログ作成時に準備VM用の分離セキュリティグループを作成する必要がある場合にのみ必要です。これが完了すると、これらの権限は不要になります。

VMのインポート

VMをインポートしてマシンカタログを作成します。

```
{

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

    "Statement": [

        {

            "Action": [

                "ec2:DescribeInstances",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeSubnets",

                "ec2:DescribeVolumes",

                "ec2:DescribeSpotInstanceRequests"

            ],

            "Effect": "Allow",

            "Resource": "*"

        }

    ]

}
```

注:

`ec2:DescribeSpotInstanceRequests` は、VMがインポートされるAWSリージョンにスポットインスタンスがある場合にのみ必要です。

ディスクの直接アップロードとダウンロード

直接ディスクアップロードは、マシンカタログプロビジョニングにおけるボリュームワーカーの要件を排除し、代わりにAWSが提供するパブリックAPIを使用します。この機能により、追加のストレージアカウントに関連するコストと、ボリュームワーカー操作を維持する複雑さが軽減されます。

注:

ボリュームワーカーのサポートは削除されました。マシンカタログのプロビジョニングには、ディスクの直接アップロードおよびダウンロードの権限が必要です。

以下の権限をポリシーに追加する必要があります。

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

重要:

- ボリュームワーカーAMIやボリュームワーカーVMなどのボリュームワーカーリソースなしで、既存のマシンカタログに新しいVMを追加できます。

- 以前にボリュームワーカーを使用していた既存のカタログを削除すると、ボリュームワーカーに関連するすべてのアーティファクトが削除されます。

作成されたボリュームのEBS暗号化

AMIが暗号化されている場合、またはEBSがすべての新しいボリュームを暗号化するように構成されている場合、EBSは新しく作成されたボリュームを自動的に暗号化できます。ただし、この機能を実装するには、IAMポリシーに次の権限を含める必要があります。

```
{

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

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",

                 "kms:DescribeKey",

                 "kms:GenerateDataKeyWithoutPlainText",

                 "kms:GenerateDataKey",

                 "kms:ReEncryptTo",

                 "kms:ReEncryptFrom"

            ],

            "Resource": "*"

        }

    ]
```

```
}
```

注:

ユーザーの判断により、リソースと条件ブロックを含めることで、権限を特定のキーに限定できます。例：**条件付きKMS権限**：

```
{

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

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",

                 "kms:DescribeKey",

                 "kms:GenerateDataKeyWithoutPlainText",

                 "kms:GenerateDataKey",

                 "kms:ReEncryptTo",

                 "kms:ReEncryptFrom"

            ],

            "Resource": [

                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-
a123-456d-a12b-a123b4cd56ef"
```

```
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

次のキーポリシーステートメントは、アカウントがIAMポリシーを使用してKMSキーに対するすべてのアクション (kms:*) の権限を委任することを許可するために必要な、KMSキーのデフォルトのキーポリシー全体です。

```
{
"Sid": "Enable IAM policies",
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::111122223333:root"
},
"Action": "kms:",
"Resource": ""
}
```

詳細については、AWS Key Management Serviceの公式ドキュメントを参照してください。

IAMロールベース認証

ロールベース認証をサポートするために、次の権限が追加されます。

```
{

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

     "Statement": [

        {

            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]

}
```

最小限のIAM権限ポリシー

以下のJSONは、現在サポートされているすべての機能に使用できます。このポリシーを使用すると、ホスト接続の作成、VMの作成、更新、削除、および電源管理を行うことができます。 このポリシーは、(#define-iam-permissions)セクションで説明されているようにユーザーに適用することも、**role_based_auth**セキュリティキーとシークレットキーを使用してロールベース認証を使用することもできます。

> **重要:**
>
> **role_based_auth**を使用するには、まずDelivery Controllerを設定する際に、Delivery Controller ec2インスタンスで目的のIAMロールを設定します。Web Studioを使用してホスティング接続を追加し、認証キーとシークレットにrole_based_authを指定します。これらの設定を持つホスティング接続は、ロールベース認証を使用します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
```

```
                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:CancelSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",

                "ec2:DescribeVolumes",

                "ec2:DescribeVpcs",
```

```
            "ec2:DetachVolume",
            "ec2:DisassociateIamInstanceProfile",
            "ec2:RebootInstances",
            "ec2:RunInstances",
            "ec2:StartInstances",
            "ec2:StopInstances",
            "ec2:TerminateInstances"
        ],
        "Effect": "Allow",
        "Resource": "*"
    },
    {
        "Action": [
            "ec2:CreateSecurityGroup",
            "ec2:DeleteSecurityGroup"
        ],
        "Effect": "Allow",
        "Resource": "*"
    },
    {
        "Action": [
            "ebs:StartSnapshot",
```

```
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
        }
    ]
}
```

注:

- SecurityGroupsに関連するEC2セクションは、カタログ作成時に準備VM用に隔離セキュリティグループを作成する必要がある場合にのみ必要です。これが完了すると、これらの権限は不要になります。
- KMSセクションは、EBSボリューム暗号化を使用する場合にのみ必要です。
- `iam:PassRole`権限セクションは、**role_based_auth**の場合にのみ必要です。
- 要件と環境に基づいて、フルアクセスではなく特定のリソースレベルの権限を追加できます。詳細については、AWSドキュメントのEC2リソースレベルの権限を解き明かすおよびAWSリソースのアクセス管理を参照してください。
- `ec2:CreateNetworkInterface`と`ec2:DeleteNetworkInterface`の権限は、ボリュームワーカー方式を使用している場合にのみ使用してください。

ホスト接続の権限を検証する

ホスト接続の権限を検証して、MCSマシンカタログの作成と管理に関連するタスクを実行できます。この実装は、VMの作成、削除、更新、VMの電源管理、EBS暗号化など、さまざまなシナリオで必要な不足している権限を事前に特定するのに役立ち、重要な時期にブロックされるのを防ぎます。

PowerShellコマンド `Test-HypHypervisorConnection` を使用して、ホスト接続の権限を検証できます。コマンドの結果はリストとしてキャプチャされ、リスト内の各項目は3つのセクションに分かれています。

- カテゴリ: ユーザーがMCSマシンカタログを作成および管理するために実行できるアクションまたはタスク。
- 是正措置: 管理者がユーザーの不足している権限の不一致を解決するために実行する必要がある手順。
- 不足している権限: カテゴリに不足している権限のリストです。

権限を検証するには、次の手順を実行します。

1. AWSへのホスト接続を作成します。
2. Delivery Controller™ホストからPowerShellウィンドウを開きます。
3. `asnp citrix*` を実行して、Citrix固有のPowerShellモジュールをロードします。
4. 次のコマンドを実行して、権限を検索するために必要な権限があるかどうかを確認します。

   ```
   Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\AWSCon"
   ```

5. 権限を検索するために必要な不足している権限を追加した後、次のコマンドを実行して、次のカテゴリに権限があるかどうかを確認します。

   - 作成、更新、削除
   - 電源管理
   - EBS暗号化

   ```
   Test-HypHypervisorConnection -LiteralPath "XDHyp:
   \Connections\AWSCon" [-SecurePassword -Password] "password" -UserName
   "" -CustomProperties ""
   ```

権限の追加の詳細については、IAM権限の追加を参照してください。

次に進む場所

- 初期展開プロセス中の場合は、マシンカタログの作成を参照してください。
- AWS固有の情報については、AWS EC2カタログの作成を参照してください。

詳細情報

- 接続とリソースの作成および管理
- AWS仮想化環境

アマゾン ワークスペース コア マネージドインスタンスへの接続

「接続とリソースの作成および管理」(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/connections)では、接続を作成するウィザードについて説明しています。以下の情報は、Amazon WorkSpaces Core マネージドインスタンスに固有の詳細を扱っています。

前提条件

Amazon WorkSpaces Core Managed Instancesへの接続を作成する前に、以下を実行してください。

- AWS をリソースの場所として設定を完了します。「AWS仮想化環境」(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/install-prepare/aws)を参照してください。
- IAM権限の定義 Citrix® がお客様に代わってAWSリソースを管理するためのIAMユーザーまたはロールのポリシー。
- 「サービスにリンクされたロールの作成」(#create-a-service-linked-role)。

IAM権限を定義する

ホスト接続を作成する前に、お客様に代わってAWSアカウント内のリソースをプロビジョニングおよび管理するために、Citrixに適切な権限を与えるIAMユーザーまたはロールに対して、IAM権限ポリシーを適切に定義する必要があります。このセクションの情報を使用して、Amazon WorkSpaces Core マネージドインスタンス上のCitrix Virtual Apps and DesktopsのIAM権限を定義してください。AmazonのIAMサービスでは、複数のユーザーを持つアカウントを許可しており、それらのユーザーはさらにグループに編成できます。これらのユーザーは、アカウントに関連する操作を実行する能力を制御するために、異なる権限を持つことができます。IAM権限の詳細については、IAM JSONポリシーリファレンスを参照してください。

> **注:**
>
> Citrixはお客様に代わってAWSアカウント内のリソースと自動化をプロビジョニングおよび管理するため、特定のタグやリソース命名規則に基づいたIAM権限ポリシーの設定はサポートされていません。

> 新しいユーザーグループにIAM権限ポリシーを適用するには：

1. AWSマネジメントコンソールにログインし、ドロップダウンリストから**IAMサービス**を選択します。
2. **新しいユーザーグループを作成**を選択します。
3. 新しいユーザーグループの名前を入力し、**続行**を選択します。
4. **Permissions**ページで、**Custom Policy**を選択します。
5. **Permissions policy**の名前を入力します。
6. **Policy Document**セクションで、関連する権限を入力します。

ポリシー情報を入力した後、**Continue**を選択して、IAM権限ポリシーのユーザーグループへの適用を完了します。グループ内のユーザーには、Citrix Virtual Apps and Desktopsに必要なアクションのみを実行する権限が付与されます。

> **重要:**
>
> この記事で提供されている例のポリシーテキストを使用して、Citrix Virtual Apps and DesktopsがAWSアカウント内でアクションを実行するために使用するアクションを、特定のリソースに制限することなくリストします。Citrixは、テスト目的でこの例を使用することを推奨します。本番環境では、リソースにさらなる制限を追加することを選択できます。

IAM権限を追加する

AWS Management Consoleの**IAM**セクションで権限を追加します。

1. **Summary**パネルで、**Permissions**タブを選択します。
2. **Add permissions**を選択します。
3. **Add Permissions to**画面で、権限を付与します。
4. JSONセクションで、お使いの環境のRequired AWS permissionsを含めます。

サービスにリンクされたロールを作成する

CitrixがCore V2 APIを呼び出す各AWSアカウントに対して、サービスにリンクされたロール (SLR) を作成します。

ロールを作成する手順：

- AWS マネジメントコンソールでコマンドラインインターフェイス (CLI) を開きます。

- CLI で次のコマンドを実行します。

```
aws iam create-service-linked-role --aws-service-name workspaces-instances.amazonaws.com
```

Amazon WorkSpaces Core マネジメントコンソールを使用して、サービスにリンクされたロールを構成することもできます。「サービスにリンクされたロールの作成 (コンソール)」を参照してください。

接続を作成する

Amazon WorkSpaces Core マネージドインスタンスへの接続は、次の方法で作成できます。

- ウェブスタジオ
- PowerShell コマンド

> **注:**
>
> プロキシサーバーまたはファイアウォールの制限を確認し、次のアドレスに接続できることを確認してください: `https://*.amazonaws.com` および `https://*.api.aws`。また、「Citrix Gateway サービス接続」に記載されているすべてのアドレスに接続できることを確認してください。

> これらに接続できない場合、ホスト接続の作成または更新中に失敗する可能性があります。

Web Studioを使用して接続を作成する

1. **「ホスティング」>「接続とリソースの追加」**ページに移動します。
2. **「接続」**ページで、次の手順に従って接続を構成します。
   a. **「新しい接続を作成」**を選択します。
   b. **「ゾーン」**で、AWS 環境用に設定したリソースの場所を選択します。
   c. 接続タイプとして **Amazon WorkSpaces Core** を選択します。
   d. **IAMユーザーアクセスキーを使用** または **IAMロールを使用** を選択します。

      IAMユーザーアクセスキーの場合は、CitrixがAWSアカウントのリソースを管理するために適切なIAM権限ポリシーを持つIAMユーザーの **APIキー** と **シークレットキー** を入力します。

IAMロールの場合は、CitrixがAWSアカウントのリソースを管理するために適切なIAM権限ポリシーを持つIAMロールをDelivery Controllerインスタンスに割り当てていることを確認してください。詳細については、ロールベース認証ガイドを参照してください。

e. 接続名を入力し、**「次へ」** をクリックします。

3. **仮想マシンの場所** ページで、VMをプロビジョニングする場所を指定します。新しいVMを作成するためのクラウドリージョン、VPC、およびアベイラビリティゾーンを選択します。
4. **ネットワーク** ページで:

   a. 以前にアベイラビリティゾーンまたはローカルゾーンで選択したリソースの名前を入力します。

   b. 前のメニューで構成したVPC内の1つ以上のサブネットを選択します。

5. **概要** ページまで残りのページをクリックして進みます。
6. **「完了」** をクリックして、Amazon WorkSpaces Coreマネージドインスタンスへのホスト接続を作成します。

重要な考慮事項

Web Studioを使用して接続を作成する場合：

- CitrixがAWSリソースを管理するための適切なIAM権限を定義します。
- CitrixがAWSリソースを管理するためにIAMユーザーアクセスキーを使用する場合、APIキーとシークレットキーの値を指定する必要があります。これらの値を含むキーファイルをAWSからエクスポートし、インポートできます。また、リージョン、アベイラビリティゾーン、VPC名、サブネットアドレス、ドメイン名、セキュリティグループ名、および資格情報も指定する必要があります。
- CitrixがAWSリソースを管理するためにIAMロールを使用する場合、すべてのDelivery Controllerに適切なIAM権限を持つロールを割り当てる必要があります。詳細については、ロールベース認証ガイドを参照してください。
- ルートAWSアカウントの資格情報ファイル（AWSコンソールから取得）は、標準のAWSユーザー用にダウンロードされた資格情報ファイルと同じ形式ではありません。そのため、Citrix Virtual Apps and Desktopsは、このファイルを使用してAPIキーとシークレットキーのフィールドに入力することはできません。AWS Identity Access Management (IAM) 資格情報ファイルを使用していることを確認してください。
- ゾーンはアベイラビリティゾーンまたはローカルゾーンのいずれかです。

PowerShellを使用して接続を作成する

1. PowerShellウィンドウを開きます。

2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. 次のコマンドを実行します。以下に例を示します。

```
$connectionName = "demo-hostingconnection"

$cloudRegion = "us-east-1"

$apiKey = "aaaaaaaaaaaaaaaaaaaa"

$apiSecret = “bbbbb”

$secureKey = ConvertTo-SecureString -String $apiSecret

$zoneUid = "00000000-0000-0000-0000-000000000000"

$connectionPath = "XDHyp:\Connections\" + $connectionName



$connection = New-Item -Path $connectionPath -ConnectionType
"AmazonWorkSpacesCoreMachineManagerFactory" -HypervisorAddress "
"https://workspaces-instances.$($cloudRegion).api.aws"" -Persist -Scope
@() -UserName $apiKey -SecurePassword $secureKey -ZoneUid $zoneUid



New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid



$hostingUnitName = "demo-hostingunit"

$availabilityzone = "us-east-1a"

$vpcName = "Default VPC"

$jobGroup = [Guid]::NewGuid()

$hostingUnitPath = "XDHyp:\HostingUnits\" + $HostingUnitName

$rootPath = $connectionPath + "\" + $vpcName + ".virtualprivatecloud\"
```

```
$availabilityZonePath = @($rootPath + $availabilityzone +
".availabilityzone")

$networkPaths = (Get-ChildItem $availabilityZonePath[0] | Where
ObjectType -eq "Network") | Select-Object -ExpandProperty FullPath #
will select all the networks in the availability zone



New-Item -Path $hostingUnitPath -AvailabilityZonePath
$availabilityZonePath -HypervisorConnectionName $connectionName
-JobGroup $jobGroup -PersonalvDiskStoragePath @() -RootPath $rootPath
-NetworkPath $networkPaths
```

注:

ロールベース認証を使用して接続を作成するには、apiKeyとapiSecretを `role_based_auth` として指定します。

制限事項

AWSコンソールでAWS Virtual Private Cloud (VPC) の名前を変更すると、Citrix Cloud™内の既存のホスティングユニットが破損します。ホスティングユニットが破損している場合、カタログを作成したり、既存のカタログにマシンを追加したりすることはできません。この問題を解決するには、AWS VPCの名前を元の名前に戻してください。

接続の編集

既存のホスト接続を編集して、次のことができます。

- CitrixがリソースをIAM権限を提供するオプションを変更する
- ホスティング接続あたりの同時アクション（または同時マシン）の最大数を変更する
- スコープを変更します。
- PowerShell コマンドを使用して、エラスティックネットワークインターフェイス (ENI) ごとに許可されるセキュリティグループの最大数を構成します。(#configure-security-groups-per-network-interface)

IAM権限を付与するためのオプションを編集する

1. 既存のAmazon WorkSpaces Core接続を右クリックします。
2. **Connection Properties**ページで、**Edit settings**をクリックします。
3. Citrixがリソースを管理するためのIAM権限を付与するオプションのいずれかを選択します。必要な詳細を入力し、**Save**をクリックします。

同時実行アクションの最大数を変更する

Amazon WorkSpaces Coreマネージドインスタンスの Studioでホスト接続を作成すると、以下のデフォルト値が表示されます。

オプション	絶対値	パーセンテージ
同時実行アクション (すべての種類)	125	100
1分あたりの新規アクションの最大数	150	該当なし
同時プロビジョニング操作の最大数	150	該当なし

MCS は、デフォルトで最大 150 の同時プロビジョニング操作をサポートします。

これらの値は、**接続の編集**画面の Citrix Studio の**詳細設定**セクションにアクセスして構成できます。

または、Remote PowerShell SDK を使用して、環境に応じた最適な設定のために同時操作の最大数を設定することもできます。

PowerShell カスタムプロパティ `MaximumConcurrentProvisioningOperations` を使用して、AWS の同時プロビジョニング操作の最大数を指定します。

構成前:

- Cloud 用 PowerShell SDK がインストールされていることを確認してください。
- `MaximumConcurrentProvisioningOperations` のデフォルト値は 150 であることを理解してください。

`MaximumConcurrentProvisioningOperations` の値をカスタマイズするには、次の手順を実行します。

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*`を実行して、Citrix固有のPowerShellモジュールをロードします。
3. `cd xdhyp:\Connections\` を入力します。
4. 接続を一覧表示するには、`dir` を入力します。
5. カスタムプロパティ文字列を変更または初期化します。
   - カスタムプロパティ文字列に値がある場合は、カスタムプロパティをメモ帳にコピーします。次に、`MaximumConcurrentProvisioningOperations` プロパティを希望の値に変更します。1〜1000の範囲の値を入力できます。 例: `<Property xsi:type="IntProperty" Name="MaximumConcurrentProvisioningOperations" Value="xyz"/>`。
   - カスタムプロパティ文字列が空またはnullの場合、スキーマと `MaximumConcurrentProvisioningOperations` プロパティの両方に適切な構文を入力して文字列を初期化する必要があります。
6. **PowerShell** ウィンドウで、メモ帳から変更したカスタムプロパティを貼り付け、変更したカスタムプロパティに変数を割り当てます。カスタムプロパティを初期化した場合は、構文の後に次の行を追加します。

   ```
   $customProperties = '<CustomProperties xmlns="http://
   schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
   www.w3.org/2001/XMLSchema-instance"><Property xsi:type="IntProperty"
   Name="MaximumConcurrentProvisioningOperations" Value="100"/></
   CustomProperties>'
   ```

   この文字列は、`MaximumConcurrentProvisioningOperations` プロパティを100に設定します。カスタムプロパティ文字列では、`MaximumConcurrentProvisioningOperations` プロパティをニーズに合った値に設定する必要があります。
7. 資格情報の入力を求める `Get-XDAuthentication` を入力します。
8. `$cred = Get-Credential` を実行します。パスワードのみ（または名前とパスワード）の入力を求められる場合があります。アプリケーションIDと関連するシークレットの入力を求められる場合もあります。ロールベース認証を使用する接続の場合、**role_based_auth** は名前とパスワードの両方です。それ以外の場合は、AWS API IDとシークレットを入力します。
9. `set-item -PSPath 'XDHyp:\Connections<connection-name>' -CustomProperties $customProperties -username $cred.username -Securepassword $cred.password` を実行します。*<connection-name>* を接続の名前に設定する必要があります。
10. 更新されたCustomProperties文字列を確認するには、`dir` を入力します。

ネットワークインターフェイスごとのセキュリティグループを構成する

ホスト接続を編集する際、PowerShellコマンドを使用して、エラスティックネットワークインターフェイス（ENI）ごとに許可されるセキュリティグループの最大数を構成できるようになりました。AWSセキュリティグループのクォータ値については、「セキュリティグループ」を参照してください。

ネットワークインターフェイスごとにセキュリティグループを構成するには:

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*` を実行します。
3. `cd xdhyp:\Connections\`を実行します。
4. 接続を一覧表示するには、`dir`を実行します。
5. ネットワークインターフェイスごとにセキュリティグループを構成するには、次のPowerShellコマンドを実行します。

```
Set-HypHypervisorConnectionMetadata -HypervisorConnectionName aws -Name
"Citrix_MachineManagement_Options" -Value "
AwsMaxENISecurityGroupLimit=<number>"
```

> **注:**
>
> `AwsMaxENISecurityGroupLimit`に値を設定しない場合、デフォルト値の5が使用されます。

サービスエンドポイントURL

標準ゾーンサービスエンドポイントURL

MCSを使用すると、APIキーとAPIシークレットを持つ新しいAmazon WorkSpaces Core Managed Instances接続が追加されます。この情報と認証済みアカウントを使用して、MCSはAWS EC2およびAmazon WorkSpaces Core Managed Instances API呼び出しを使用して、サポートされているリージョンとゾーンをAWSに照会します。このクエリは、Workspace Instances Service Endpoint URL `<https://workspaces-instances.us-east-1.api.aws/>` とEC2 Service Endpoint https:/ec2.us-east-1.api.aws/ を使用して行われます。

> **注:**

`<https://workspaces-instances.us-east-1.api.aws/>` に接続できることを確認してください。

必要なAWS権限

このセクションには、AWS権限の完全なリストが含まれています。機能が正しく動作するように、このセクションに記載されている権限の完全なセットを使用してください。

注:

`iam:PassRole` 権限は、CitrixがリソースをIAMロールを使用する場合にのみ必要です。

ホスト接続の作成

AWSから取得した情報を使用して、新しいホスト接続が追加されます。

```
{

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

    "Statement": [

        {

            "Action": [

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeSubnets",

                "ec2:DescribeVpcs",

                "ec2:DescribeRegions",

                "workspaces-instances:*"

            ],

            "Effect": "Allow",
```

```
            "Resource": "*"

        }

    ]

}
```

VMの電源管理

VMの電源はオンまたはオフにされます。

```
{

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

    "Statement": [

        {

            "Action": [

                "ec2:DescribeInstances",,

                "ec2:StartInstances",

                "ec2:StopInstances",

                "ec2:RebootInstances",

                "ec2:DescribeInstanceStatus"

            ],

            "Effect": "Allow",

            "Resource": "*"

        },

        {
```

```
            "Action": [
                "workspaces-instances:*"
            ],
            "Effect": "Allow",
             "Resource": "*"
        }


    ]


}
```

VMの作成、更新、または削除

AWSインスタンスとしてプロビジョニングされたVMを含むマシンカタログが作成、更新、または削除されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupEgress",
```

```
                "ec2:AuthorizeSecurityGroupIngress",

                "ec2:CreateImage",

                "ec2:CreateLaunchTemplate",

                "ec2:CreateSecurityGroup",

                "ec2:CreateTags",

                "ec2:CreateVolume",

                "ec2:DeleteVolume",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",
```

```
                "ec2:DescribeSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",
                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup"
            ],
            "Effect": "Allow",
```

```
            "Resource": "*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "workspaces-instances:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
```

```
    ]
}
```

注:

- SecurityGroupsに関連するEC2セクションは、カタログ作成時に準備VM用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが完了すると、これらの権限は不要になります。

ディスクの直接アップロードとダウンロード

次の権限をポリシーに追加する必要があります。

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

作成されたボリュームのEBS暗号化

AMIが暗号化されている場合、またはEBSがすべての新しいボリュームを暗号化するように構成されている場合、EBSは新しく作成されたボリュームを自動的に暗号化できます。ただし、この機能を実装するには、IAMポリシーに次の権限を含める必要があります。

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:GenerateDataKey",
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        }
    ]
}
```

注:

ユーザーの裁量により、リソースと条件ブロックを含めることで、権限を特定のキーに制限できます。例: **条件付きKMS権限**:

```
{

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

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",

                 "kms:DescribeKey",

                 "kms:GenerateDataKeyWithoutPlainText",

                 "kms:GenerateDataKey",

                 "kms:ReEncryptTo",

                 "kms:ReEncryptFrom"

            ],

            "Resource": [

                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-
a123-456d-a12b-a123b4cd56ef"

            ],

            "Condition": {

                "Bool": {

                    "kms:GrantIsForAWSResource": true

                }
```

```
            }

        }

    ]

}
```

次のキーポリシーステートメントは、アカウントがIAMポリシーを使用してKMSキーに対するすべてのアクション (kms:*) の権限を委任できるようにするために必要な、KMSキーのデフォルトのキーポリシー全体です。

```
{

"Sid": "Enable IAM policies",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::111122223333:root"

},

"Action": "kms:",

"Resource": ""

}
```

詳細については、AWS Key Management Serviceの公式ドキュメントを参照してください。

IAMロールベース認証

ロールベース認証をサポートするために、次の権限が追加されます。

```
{

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

     "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
        }
    ]
}
```

最小限のIAM権限ポリシー

以下のJSONは、現在サポートされているすべての機能に使用できます。このポリシーを使用して、ホスト接続の作成、VMの作成、更新、削除、および電源管理を行うことができます。 このポリシーは、IAM権限の定義セクションで説明されているようにユーザーに適用することも、ホスト接続を構成するときに**IAMロールを使用**を選択してロールベース認証を使用することもできます。

重要:

CitrixがリソースをIAMロールを使用するためを使用するには、まずDelivery Controllerのセットアップ時に、Delivery Controller ec2インスタンスで目的のIAMロールを構成します。Citrix Studioを使用して、ホスティング接続を追加し、**IAMロールを使用**オプションを選択します。これらの設定を持つホスティング接続は、ロールベースの認証を使用します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
```

```
                "ec2:AssociateIamInstanceProfile",

                "ec2:AuthorizeSecurityGroupEgress",

                "ec2:RevokeSecurityGroupEgress",

                "ec2:AuthorizeSecurityGroupIngress",

                "ec2:CreateImage",

                "ec2:CreateLaunchTemplate",

                "ec2:CreateNetworkInterface",

                "ec2:CreateTags",

                "ec2:CreateVolume",

                "ec2:DeleteLaunchTemplate",

                "ec2:DeleteNetworkInterface",

                "ec2:DeleteSecurityGroup",

                "ec2:DeleteSnapshot",

                "ec2:DeleteTags",

                "ec2:DeleteVolume",

                "ec2:DeregisterImage",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",
```

```
                "ec2:DescribeInstanceStatus",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",

                "ec2:DescribeVolumes",

                "ec2:DescribeVpcs",

                "ec2:DetachVolume",

                "ec2:DisassociateIamInstanceProfile",

                "ec2:RebootInstances",

                "ec2:RunInstances",

                "ec2:StartInstances",

                "ec2:StopInstances",

                "ec2:TerminateInstances"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
```

```
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:GenerateDataKey",
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "workspaces-instances:*"
            ],
            "Resource": "*"
        }


    ]
}
```

注：

- SecurityGroupsに関連するEC2セクションは、カタログ作成中に準備VM用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが完了すると、これらの権限は不要になります。
- KMSセクションは、EBSボリューム暗号化を使用する場合にのみ必要です。
- `iam:PassRole`権限セクションは、Citrixがリソースを管理するためにIAMロールを使用する場合にのみ必要です。
- 要件と環境に基づいて、フルアクセスではなく特定のリソースレベルの権限を追加できます。詳細については、AWSドキュメントのDemystifying EC2 Resource-Level PermissionsおよびAccess management for AWS resourcesを参照してください。
- ボリュームワーカー方式を使用している場合にのみ、`ec2:CreateNetworkInterface`および`ec2:DeleteNetworkInterface`権限を使用してください。

次のステップ

- 準備済みイメージの作成については、「Amazon WorkSpaces Coreマネージドインスタンス用の準備済みイメージを作成する」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- AWS仮想化環境
- Amazon WorkSpaces Core GitHub PowerShellの例については、「citrix-mcs-sdk-samples-Amazon WorkSpaces Core」を参照してください。

Azure Local への接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明します。以下の情報は、Azure Local 環境に固有の詳細を扱います。

ホスティング接続を作成する

ホスト接続は、以下を使用して作成できます。

- ウェブスタジオ
- PowerShell

Web Studio を使用する

1. Web Studio で、**ホスティング > 接続とリソースの追加**を開きます。
2. **接続**ページで、以下の手順に従って接続を構成します。
    a. **新しい接続の作成**を選択します。
    b. 接続の種類として、**Microsoft® Azure™ Arc**を選択します。
    c. Azure環境を選択します。
    d. ゾーンを選択します。オプションは、構成したすべてのリソースの場所です。
    e. 仮想マシンを作成するには、「**その他のツール**」を選択します。

    > **注:**
    >
    > 「**その他のツール**」を選択すると、ホスティングユニットなしでホスティング接続のみが作成されます。

    f. 「**次へ**」をクリックします。

3. 「**接続の詳細**」ページで、ウィザードのガイダンスに従って接続の詳細を入力します。既存のSPNを使用する場合は、SPNにサブスクリプションの共同作成者ロールが付与されていることを確認してください。詳細については、「必要なAzureローカル権限」を確認してください。
4. 「**スコープ**」ページで、この接続のスコープを1つ以上選択します。
5. 「**概要**」ページで、構成を確認し、「**完了**」をクリックします。

PowerShell を使用する

スクリプトのヘッダー

スクリプトのヘッダーで定義されている正しいパラメーター値を指定していることを確認してください。

```
$azureSubscription = "" # Azure Subscription ID


$azureTenantId = "" # Microsoft Entra Tenant ID


$appClientId = "" # Client ID of an Microsoft Entra application which is
grant with sufficient permissions


$appClientSecret = "" # Client secret of above client ID


$appClientSecretExpirationDateTimestamp = "" # Client secret expiration
date in epoch timestamp format


$region = "" # Azure region of your Azure Local cluster


$resourceGroupName = "" # Azure resource group of your Azure Local cluster
```

```
$zoneUid = "" # Zone UID of your resource location



$hostingConnectionName = "" # Name of the created hosting connection
```

ホスティング接続を作成する

```
asnp citrix*



[SecureString]$appClientSecretSecureString = $appClientSecret | ConvertTo-
SecureString -AsPlainText -Force



$conn = New-Item -ConnectionType "Custom" -CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
Value=`"$azureSubscription`" /><Property xsi:type=`"StringProperty`"
Name=`"ManagementEndpoint`" Value=`"https://management.azure.com/`" /
><Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
Value=`"https://login.microsoftonline.com/`" /><Property
xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"$azureTenantId`" /
></CustomProperties>" -HypervisorAddress @("https://
management.azure.com/") -Path @("XDHyp:\Connections\
$hostingConnectionName") -Persist -PluginId "AzureArcFactory" -Scope @()
-SecurePassword $appClientSecretSecureString -UserName $appClientId
-ZoneUid $zoneUid



New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$conn.HypervisorConnectionUid



Set-HypHypervisorConnectionMetadata -HypervisorConnectionUid
$conn.HypervisorConnectionUid -Name
Citrix_Orchestration_Hypervisor_Secret_Allow_Edit -Value true
```

```
Set-HypHypervisorConnectionMetadata -HypervisorConnectionUid
$conn.HypervisorConnectionUid -Name
Citrix_Orchestration_Hypervisor_Secret_Expiration_Date -Value
$appClientSecretExpirationDateTimestamp
```

ホスティングユニットを作成する

ホスティングユニットは、次の方法で作成できます。

- ウェブスタジオ
- PowerShell

ホスティングユニットを作成する：Web Studioを使用する

1. Web Studioで、**ホスティング > 接続とリソースの追加**を開きます。
2. 「**接続**」ページで、:
   - ホスティングユニットとともに新しいホスティング接続を作成するには、「**新しい接続の作成**」を選択し、次の操作を行います。
     a. 「**新しい接続の作成**」を選択します。
     b. 接続の種類として「**Microsoft® Azure™ Arc**」を選択します。
     c. Azure環境を選択します。
     d. ゾーンを選択します。オプションは、構成したすべてのリソースの場所です。
     e. 仮想マシンを作成するには、「**Citrixプロビジョニングツール（Machine Creation Services™ またはCitrix Provisioning）**」を選択します。
     f. 「**次へ**」をクリックします。
   - 既存のホスト接続からホスティングユニットを作成するには、 を選択し、関連する接続を選択します。
3. 「**接続の詳細**」ページで、ウィザードのガイダンスに従って接続の詳細を入力します。既存のSPNを使用する場合は、SPNにサブスクリプションの共同作成者ロールが付与されていることを確認してください。
4. 「**クラスターの選択**」ページで、リソースグループを参照し、ターゲットのAzure Localクラスターを選択します。

5. 「**ストレージの選択**」ページで、ウィザードの次のページに進む前に、サポートされているデータタイプごとに少なくとも1つのストレージデバイスを選択します。ストレージの選択の詳細については、「ホストストレージ」を参照してください。
6. 「**ネットワーク**」ページで、リソースの名前を入力します。この名前は、接続に関連付けられているストレージとネットワークの組み合わせを識別するためにStudioに表示されます。VMが使用するネットワークを1つ以上選択します。
7. 「**概要**」ページで、詳細を確認し、「**完了**」をクリックします。

PowerShellを使用してホスティングユニットを作成する

スクリプトのヘッダー

スクリプトのヘッダーで定義されている正しいパラメーター値を指定していることを確認してください。

```
$resourceGroupName = "" # Azure resource group of your Azure Local cluster


$clusterName = "" # Name of your Azure Local cluster


$storagePathName = "" # Storage path in your Azure Local cluster that
wants to be used in this hosting unit


$logicalNetworkName = "" # Logical network in your Azure Local cluster
that wants to be used in this hosting unit


$zoneUid = "" # Zone UID of your resource location


$hostingConnectionName = "" # Name of the created hosting connection
```

```
$hostingUnitName = "" # Name of the created hosting unit
```

ホスティングユニットを作成する

```
asnp citrix*



$guid = (New-Guid).Guid



New-HypStorage -StoragePath @("XDHyp:\Connections\$hostingConnectionName\
$region.region\$resourceGroupName.resourcegroup\cluster.folder\
$clusterName.cluster\storage.folder\$storagePathName.storage")
-StorageType "TemporaryStorage" -JobGroup $guid



New-Item -Path XDHyp:\HostingUnits -Name $hostingUnitName
-HypervisorConnectionName $hostingConnectionName -RootPath "XDHyp:
\Connections\$hostingConnectionName\$region.region\
$resourceGroupName.resourcegroup\cluster.folder\$clusterName.cluster"
-NetworkPath "XDHyp:\Connections\$hostingConnectionName\$region.region\
$resourceGroupName.resourcegroup\cluster.folder\
$clusterName.cluster\network.folder\$logicalNetworkName.network"
-StoragePath "XDHyp:\Connections\$hostingConnectionName\$region.region\
$resourceGroupName.resourcegroup\cluster.folder\
$clusterName.cluster\storage.folder\$storagePathName.storage" -JobGroup
$guid
```

必要なAzure Localの権限

共同作成者ロールは、すべてのリソースを管理するためのフルアクセス権を持ち、現在の機能セットで必要とされる以上の権限が含まれているものの、今後も最高の互換性を提供します。このセクションでは、Azure Localに必要な最小限の権限について詳しく説明します。

最小限の権限

VMの電源管理

```
"Microsoft.Resources/tenants/read",

"Microsoft.Resources/subscriptions/read",

"Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.AzureStackHCI/VirtualMachines/Read",

"Microsoft.AzureStackHCI/virtualMachineInstances/Read",

"Microsoft.AzureStackHCI/LogicalNetworks/Read",

"Microsoft.AzureStackHCI/StorageContainers/Read",

"Microsoft.AzureStackHCI/Clusters/Read",

"Microsoft.AzureStackHCI/VirtualMachineInstances/start/action",
```

```
"Microsoft.AzureStackHCI/VirtualMachineInstances/stop/action",

"Microsoft.AzureStackHCI/VirtualMachineInstances/restart/action"

"Microsoft.ExtendedLocation/CustomLocations/Read",

"Microsoft.KubernetesConfiguration/extensions/read",

"Microsoft.HybridCompute/machines/read"
```

仮想マシンの作成、更新、または削除

```
"Microsoft.Resources/tenants/read",

"Microsoft.Resources/subscriptions/read",

"Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
```

```
"Microsoft.HybridCompute/machines/read",

"Microsoft.HybridCompute/machines/write",

"Microsoft.HybridCompute/machines/delete",

"Microsoft.AzureStackHCI/Clusters/Read",

"Microsoft.AzureStackHCI/VirtualMachines/Read",

"Microsoft.AzureStackHCI/VirtualMachines/Write",

"Microsoft.AzureStackHCI/VirtualMachines/Delete",

"Microsoft.AzureStackHCI/virtualMachineInstances/Read",

"Microsoft.AzureStackHCI/virtualMachineInstances/Write",

"Microsoft.AzureStackHCI/virtualMachineInstances/Delete",

"Microsoft.AzureStackHCI/VirtualMachineInstances/start/action",
```

```
"Microsoft.AzureStackHCI/VirtualMachineInstances/stop/action",

"Microsoft.AzureStackHCI/VirtualMachineInstances/restart/action",

"Microsoft.AzureStackHCI/LogicalNetworks/Read",

"Microsoft.AzureStackHCI/LogicalNetworks/join/action",

"Microsoft.AzureStackHCI/StorageContainers/Read",

"Microsoft.AzureStackHCI/StorageContainers/deploy/action",

"Microsoft.AzureStackHCI/GalleryImages/Read",

"Microsoft.AzureStackHCI/GalleryImages/Write",

"Microsoft.AzureStackHCI/GalleryImages/Delete",

"Microsoft.AzureStackHCI/GalleryImages/deploy/action",

"Microsoft.AzureStackHCI/NetworkInterfaces/Read",
```

```
"Microsoft.AzureStackHCI/NetworkInterfaces/Write",

"Microsoft.AzureStackHCI/NetworkInterfaces/Delete",

"Microsoft.AzureStackHCI/VirtualHardDisks/Read",

"Microsoft.AzureStackHCI/VirtualHardDisks/Write",

"Microsoft.AzureStackHCI/VirtualHardDisks/Delete",

"Microsoft.AzureStackHCI/VirtualHardDisks/upload/action",

"Microsoft.AzureStackHCI/marketplaceGalleryImages/deploy/action",

"Microsoft.ExtendedLocation/CustomLocations/Read",

"Microsoft.ExtendedLocation/customLocations/deploy/action",

"Microsoft.KubernetesConfiguration/extensions/read",

"Microsoft.Compute/disks/read",
```

```
"Microsoft.Compute/disks/write",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/endGetAccess/action"
```

次のステップ

- Azure Localマシンカタログを作成するには、「Azure Localマシンカタログの作成」を参照してください。

詳細情報

- 「接続とリソース」

- 「マシンカタログの作成」

XenServer®への接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報は、XenServer仮想化環境に固有の詳細を扱っています。

> **注:**
>
> XenServerへの接続を作成する前に、まずXenServerアカウントをリソースの場所として設定を完了する必要があります。「XenServer仮想化環境」(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/install-prepare/xenserver.html)を参照してください。

XenServerへの接続を作成する

XenServer（旧Citrix Hypervisor™）への接続を作成する場合、VM Power Adminまたはそれ以上のレベルのユーザーの資格情報を提供する必要があります。

Citrixでは、XenServerとの通信を保護するためにHTTPSを使用することを推奨しています。HTTPSを使用するには、XenServerにインストールされているデフォルトの SSL証明書を置き換える必要があります。

XenServerサーバーで高可用性が有効になっている場合、高可用性を構成できます。Citrix Virtual Apps and Desktopsバージョン2507 LTSR以降では、HTTPSを使用しており、高可用性サーバーを構成したい場合、プール内のすべてのサーバーにワイルドカード証明書をインストールできます。ただし、2507 LTSRより前のバージョンでは、各サーバーに個別の証明書が必要です。

XenServerがvGPUをサポートしている場合、GPUの種類とグループを選択するか、パススルーすることができます。選択した項目に専用のGPUリソースがあるかどうかは、表示で示されます。

一時的なデータストレージとして1つ以上のXenServerホストでローカルストレージを使用する場合、プール内の各ストレージの場所が一意の名前を持つようにしてください。（XenCenter®で名前を変更するには、ストレージを右クリックして名前プロパティを編集します。）

Citrix Provisioning（旧Provisioning Services）およびMachine Creation Services™（MCS）を使用して、以下をプロビジョニングできます。

- サポートされているデスクトップまたはサーバーOS VM用のレガシーBIOS。
- セキュアブートを含む、サポートされているデスクトップまたはサーバーOS VM用のUEFI。

> **注:**
>
> MCSを構成する際には、プールオペレーター権限以上が必要です。

XenServer接続にIntelliCache™を使用する

IntelliCacheを使用すると、共有ストレージとローカルストレージの組み合わせを使用できるため、ホスト型VDI展開の費用対効果が高まります。これにより、パフォーマンスが向上し、ネットワークトラフィックが削減されます。ローカルストレージは共有ストレージからマスターイメージをキャッシュするため、共有ストレージへの読み取り回数が減少します。共有デスクトップの場合、差分ディスクへの書き込みはホスト上のローカルストレージに書き込まれ、共有ストレージには書き込まれません。

- IntelliCacheを使用する場合、共有ストレージはNFSである必要があります。
- Citrixでは、可能な限り最速のデータ転送を確保するために、高性能なローカルストレージデバイスを使用することをお勧めします。

IntelliCacheを使用するには、この製品とXenServerの両方で有効にする必要があります。

- XenServerをインストールするときは、**Enable thin provisioning (Optimized storage for Virtual Desktops)** を選択します。Citrixは、IntelliCacheが有効なサーバーと無効なサーバーが混在するプールをサポートしていません。詳細については、XenServerのドキュメントを参照してください。
- Citrix Virtual Apps and Desktops™では、IntelliCacheはデフォルトで無効になっています。この設定はXenServer接続を作成するときにのみ変更でき、後でIntelliCacheを無効にすることはできません。XenServer接続を追加するときは、次の手順を実行します。
  - ストレージの種類として **Shared** を選択します。
  - **Use IntelliCache** チェックボックスをオンにします。

必要なXenServer権限

XenServerの権限はロールベース（RBAC）です。XenServerのロールベースアクセス制御（RBAC）機能を使用すると、ユーザー、ロール、および権限を割り当てて、XenServerへのアクセス権を持つユーザーと、それらのユーザーが実行できるアクションを制御できます。XenServer RBACシステムは、ユーザー（またはユーザーグループ）を定義されたロール（名前付きの権限セット）にマッピングします。ロールには、特定の操作を実行するための関連するXenServer権限があります。

詳細については、「Role-based access control」を参照してください。

権限が増加する順序でのロール階層は次のとおりです。Read-Only → VM Operator → VM Admin → VM Power Admin → Pool Operator → Pool Admin。

次のセクションでは、各プロビジョニングタスクに必要な最小限のロールをまとめます。

ホスト接続の作成

タスク	必要な最小ロール
XenServerから取得した情報を使用してホスト接続を追加する	読み取り専用
ユーザーとその割り当てられた役割を表示する	読み取り専用

VMの電源管理

タスク	必要な最小限の役割
VMの電源をオンまたはオフにする	VMオペレーター

VMの作成、更新、または削除

タスク	必要な最小限の役割
既存のスナップショットスケジュールにVMを追加または削除する	VM 電源管理者
スナップショットスケジュールの追加、変更、削除	プールオペレーター
マスターイメージの公開	プールオペレーター（スイッチポートロックが必要）
マシンカタログの作成	プールオペレーター: スイッチポートロックが必要
VM の追加または削除 (GPU 対応 VM 以外)	VM 管理者
VM の追加または削除 (GPU 対応 VM)	プールオペレーター
仮想ディスクまたはCDデバイスの追加、削除、または構成	VM 管理者

タスク	必要な最小限の役割
タグの管理	VM オペレーター

RBACの役割と権限の詳細については、「RBACの役割と権限」を参照してください。

スイッチポートロックの詳細については、「スイッチポートロックの使用」を参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- XenServer 固有の情報については、XenServer カタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

Google Cloud環境への接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報は、Google Cloud環境に固有の詳細を扱っています。

> **注:**
>
> Google Cloud環境への接続を作成する前に、まずリソースロケーションとしてGoogle Cloudアカウントの設定を完了する必要があります。Google Cloud環境を参照してください。

接続の追加

接続とリソースの作成のガイダンスに従ってください。以下の説明では、ホスティング接続の設定について説明します。

1. **管理 > 構成**から、左側のペインで**ホスティング**を選択します。
2. アクションバーで**「接続とリソースの追加」**を選択します。
3. **「接続」ページで、「新しい接続の作成」と「Citrix provisioning™ tools」を選択し、「次へ」**を選択します。
    - **接続の種類**。メニューから**Google Cloud**を選択します。

- **接続名**。接続の名前を入力します。

4. 「**リージョン**」ページで、メニューからプロジェクト名を選択し、使用するリソースを含むリージョンを選択してから、「**次へ**」を選択します。
5. 「**ネットワーク**」ページで、リソースの名前を入力し、メニューから仮想ネットワークを選択し、サブセットを選択してから、「**次へ**」を選択します。リソース名は、リージョンとネットワークの組み合わせを識別するのに役立ちます。名前に「*(Shared)*」サフィックスが付いている仮想ネットワークは、共有VPCを表します。共有VPCのサブネットレベルのIAMロールを構成した場合、共有VPCの特定のサブネットのみがサブネットリストに表示されます。

> **注:**
>
> - リソース名には1～64文字を含めることができ、空白のみ、または文字`\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' )`を含めることはできません。

6. 「**Summary**」ページで情報を確認し、**Finish**を選択して「**Add Connection and Resources**」ウィンドウを終了します。

接続とリソースを作成すると、作成した接続とリソースが一覧表示されます。接続を構成するには、接続を選択し、アクションバーで該当するオプションを選択します。

同様に、接続の下に作成されたリソースを削除、名前変更、またはテストできます。これを行うには、接続の下のリソースを選択し、アクションバーで該当するオプションを選択します。

サービスエンドポイントURL

次のURLにアクセスできる必要があります。

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`
- `https://compute.googleapis.com`
- `https://storage.googleapis.com`
- `https://cloudbuild.googleapis.com`

Google Cloudプロジェクト

Google Cloudプロジェクトには基本的に2種類あります。

- プロビジョニングプロジェクト: この場合、現在の管理者アカウントがプロジェクト内のプロビジョニングされたマシンを所有します。このプロジェクトはローカルプロジェクトとも呼ばれます。
- 共有VPCプロジェクト: プロビジョニングプロジェクトで作成されたマシンが、共有VPCプロジェクトのVPCを使用するプロジェクトです。プロビジョニングプロジェクトに使用される管理者アカウントは、このプロジェクトで限られた権限、具体的にはVPCを使用する権限のみを持ちます。

GCP管理トラフィックのセキュアな環境を作成する

Google Cloudプロジェクトへのプライベートアクセスを許可できます。この実装により、機密データを処理するためのセキュリティが強化されます。これを実現するには、次のいずれかを実行できます。

- Cloud Buildサービスアカウントの VPCサービスコントロールの次のイングレスルールを含めます。この手順を実行する場合は、GCP管理トラフィックのセキュアな環境を作成するための以下の手順に従わないでください。

```
Ingress Rule 1

From:

Identities:

<ProjectID>@cloudbuild.gserviceaccount.com

Source > All sources allowed

To:

Projects =

All projects

Services =

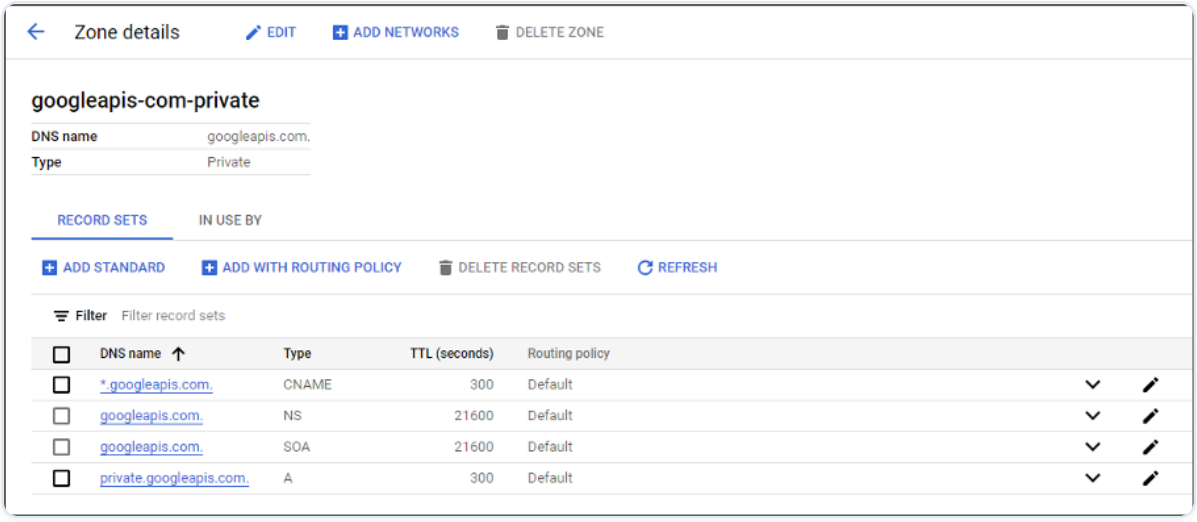
Service name: All services
```

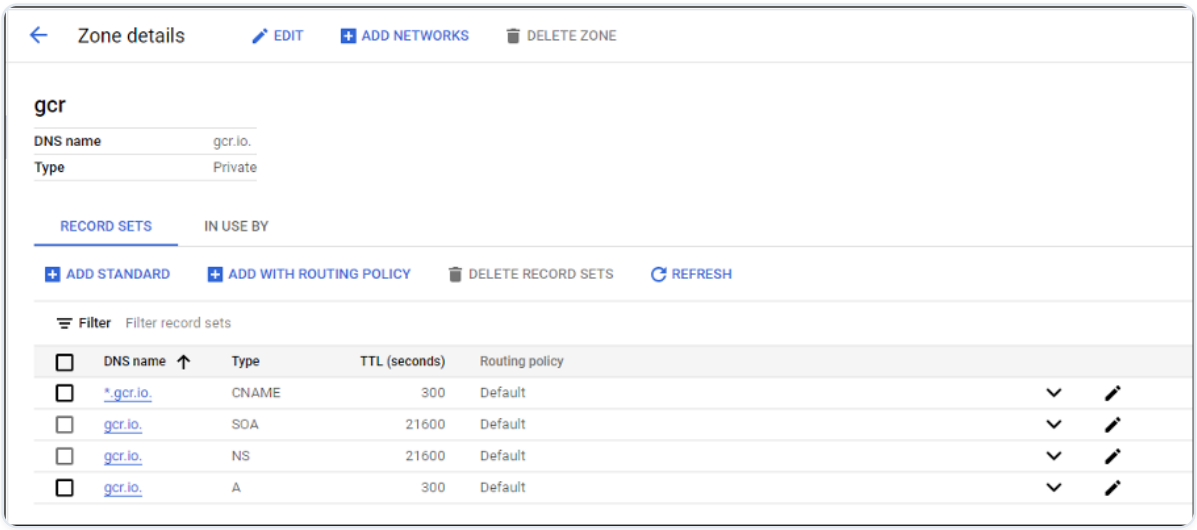
- プライベートワーカープールを使用している場合は、`CustomProperties` に `UsePrivateWorkerPool` を追加します。プライベートワーカープールの詳細については、「プライベートプール概要」を参照してください。

GCP管理トラフィックのセキュアな環境を作成するための要件

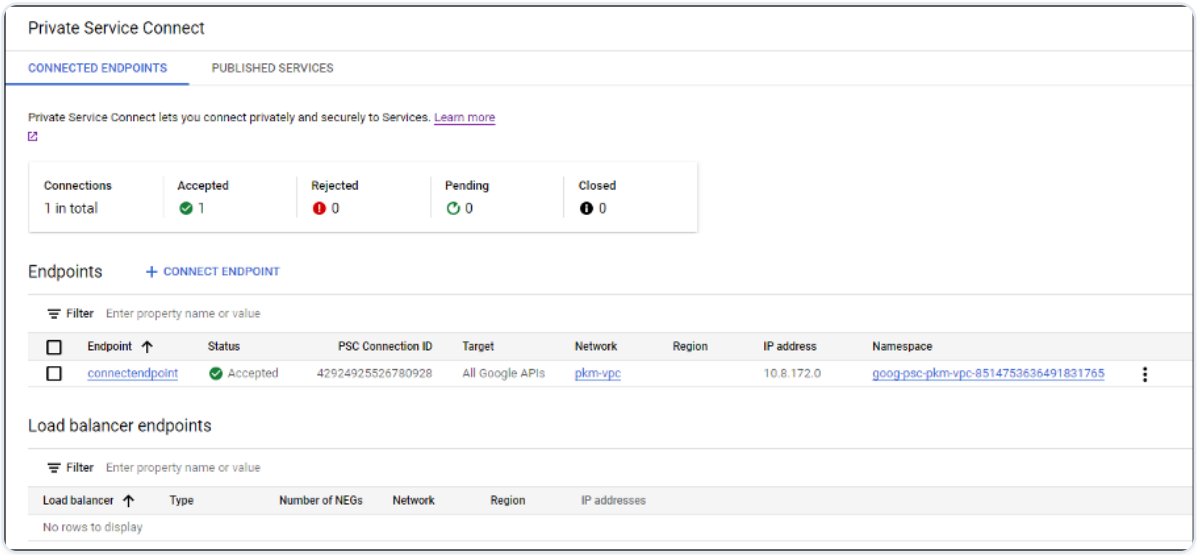
GCP管理トラフィックのセキュアな環境を作成するための要件は次のとおりです。

- カスタムプロパティを更新する際は、ホスティング接続がメンテナンスモードであることを確認してください。
- プライベートワーカープールを使用するには、次の変更が必要です。
  - Citrix Cloud™サービスアカウントには、次のIAMロールを追加します。
    - Cloud Build サービスアカウント
    - Compute Instance 管理者
    - サービスアカウントユーザー
    - サービスアカウントトークン作成者
    - Cloud Build WorkerPool オーナー
  - ホスティング接続の作成に使用するのと同じプロジェクトにCitrix Cloudサービスアカウントを作成します。
  - DNS構成で説明されているように、`private.googleapis.com`と`gcr.io`のDNSゾーンを設定します。

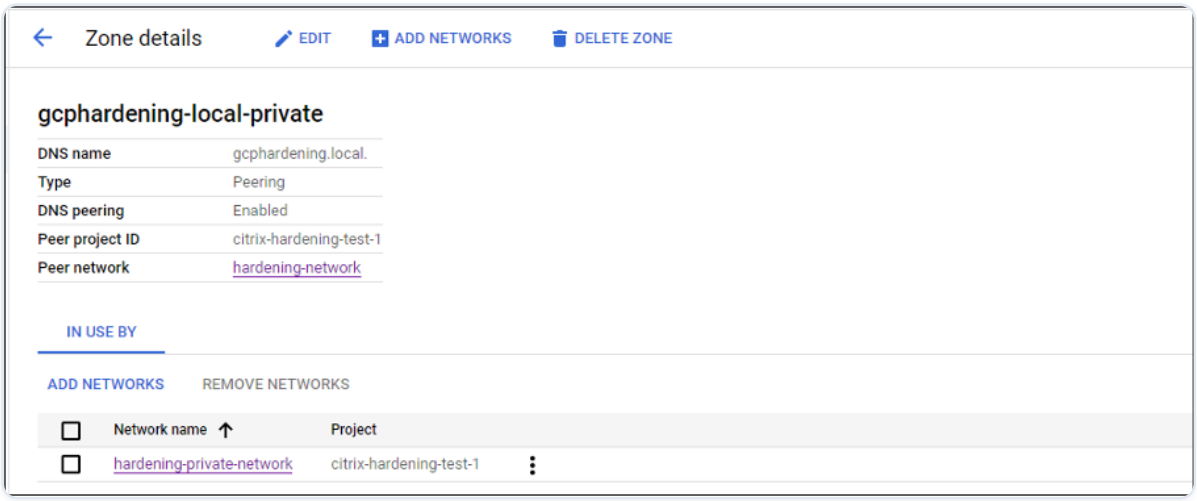




- プライベートネットワークアドレス変換 (NAT) を設定するか、プライベートサービス接続を使用します。詳細については、「エンドポイントを介した Google API へのアクセス」を参照してください。



- ピアリングされた VPC を使用している場合は、ピアリングされた VPC への Cloud DNS ゾーンピアリングを作成します。詳細については、「ピアリングゾーンの作成」を参照してください。



- VPC Service Controls で、API と VM がインターネットと通信できるようにエグレスルールを設定します。イングレスルールはオプションです。例:

```
Egress Rule 1

From:

Identities:ANY_IDENTITY

To:

Projects =

All projects

Service =

Service name: All services
```

プライベートワーカープールを有効にする

プライベートワーカープールを有効にするには、ホスト接続でカスタムプロパティを次のように設定します。

1. Delivery Controller ホストから PowerShell ウィンドウを開くか、Remote PowerShell SDK を使用します。Remote PowerShell SDK の詳細については、「SDK と API」を参照してください。
2. 次のコマンドを実行します。

   a. `Add-PSSnapin citrix®*`

b. `cd XDHyp:\Connections\`

c. `dir`

3. 接続から`CustomProperties`をメモ帳にコピーします。
4. プロパティ設定`<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool" Value="True"/>`を追加します。例：

```
```

<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.citrix.com/2014/xd/machinecreation">

<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool"
Value="True"/>

</CustomProperties>

```
```

5. PowerShellウィンドウで、変更されたカスタムプロパティに変数を割り当てます。例: `$customProperty = '<CustomProperties…</CustomProperties>'`。
6. `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"`を実行します。
7. `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"`を実行します。
8. `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force`を実行します。
9. 既存のホスト接続を更新するには、以下を実行します。

```
Set-Item -PassThru -Path @('XDHyp:\\Connections\\<ENTER YOUR CONNECTION
NAME HERE>') -SecurePassword $securePassword -UserName
$gcpServiceAccount -CustomProperties $customProperty
```

CMEKのグローバルキーとリージョンキーを指定する

注:

GCPにおけるCMEKのサポートは現在プレビュー段階です。

> GCPには、顧客管理の暗号化キー (CMEK) が2種類あります。

- リージョン：同じリージョン内のリソースのみが使用できる暗号化キー。
- グローバル：複数のリージョンのリソースが使用できる暗号化キー。

サービスアカウントがアクセスできるすべてのプロジェクトから、グローバルまたはリージョンの顧客管理暗号化キー (CMEK) を参照して使用できます。その後、そのキーを使用してCMEK対応のMCSマシンカタログを作成し、`Set-ProvScheme` コマンドを使用して既存のCMEK対応のMCSマシンカタログを更新できます。PowerShellを使用してCMEK対応カタログを作成する方法については、「カスタムプロパティを使用してCMEKでカタログを作成する」を参照してください。

この機能には、以下の2つのサービスアカウントに対する追加の権限が必要です。

- ホスティング接続が作成される現在のプロジェクトのサービスアカウント。
- 現在のプロジェクトのCompute Engineサービスエージェント (メールアドレス: `service-PROJECT_NUMBER@compute-system.iam.gserviceaccount.com` を持つもの)。詳細については、Compute Engine Service Agent を参照してください。

サービスアカウントでは、使用する暗号キーを持つプロジェクト (例: 共有プロジェクト) に次の役割を割り当てる必要があります。

- Cloud KMS 閲覧者
- クラウド KMS クリプトキー 暗号化/復号化

役割を割り当てない場合は、次の権限があることを確認してください:

- resourcemanager.projects.get
- cloudkms.keyRings.list
- cloudkms.keyRings.get
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.cryptoKeyVersions.useToDecrypt
- cloudkms.cryptoKeyVersions.useToEncrypt

暗号化キーを一覧表示する

PowerShellコマンドを使用して、同じプロジェクト内およびアクセス可能な他のすべてのプロジェクト内のグローバルおよびリージョンの暗号化キーを一覧表示できます。これを行うには:

1. Delivery Controller™ホストまたはリモートPowerShellからPowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`コマンドを実行します。
3. 暗号化キーを一覧表示するには、次のコマンドを実行します。例:

   - `encryptionKeys`フォルダーの内容を一覧表示するには:

     ```
     Get-ChildItem XDHyp:\HostingUnits\my-
     hostingunit\encryptionKeys.folder
     ```

   - 同じプロジェクト内のグローバル暗号化キーを取得するには:

     ```
     Get-Item XDHyp:\HostingUnits\my-
     hostingunit\encryptionKeys.folder\myglobalkeyring.globalkeyring\mygl
     obalkey.cryptokey
     ```

   - 同じプロジェクト内のリージョン暗号化キーを取得するには:

     ```
     Get-Item XDHyp:\HostingUnits\my-
     hostingunit\encryptionKeys.folder\regional-ring.keyring\shared-
     key.cryptokey
     ```

   - アクセス可能な別のプロジェクト（例: myanotherproject）からグローバル暗号化キーを取得するには:

     ```
     Get-Item XDHyp:\HostingUnits\my-
     hostingunit\encryptionKeys.folder\myanotherproject.project\shared-
     global-ring.globalkeyring\shared-key.cryptokey
     ```

   - アクセス可能な別のプロジェクト（例: myanotherproject）からリージョン暗号化キーを取得するには:

     ```
     Get-Item XDHyp:\HostingUnits\my-
     hostingunit\encryptionKeys.folder\myanotherproject .project.project\
     shared-uscentral.keyring\shared-uscentral-key.cryptokey
     ```

注:

- グローバルキーリングのキーリングインベントリアイテムの拡張子は`.globalkeyring`です。
- グローバルキーリングのIDには、`global`という単語が含まれています。

必要なGCP権限

このセクションには、GCP権限の完全なリストが含まれています。機能が正しく動作するように、このセクションに記載されている権限の完全なセットを使用してください。

注:

GCP は、April 29, 2024 以降、Cloud Build Services のデフォルトの動作とサービスアカウントの使用に変更を導入します。詳細については、Cloud Build Service Account Change を参照してください。April 29, 2024 より前に Cloud Build API が有効になっている既存の Google プロジェクトは、この変更の影響を受けません。ただし、April 29 以降も既存の Cloud Build Service の動作を維持したい場合は、API を有効にする前に、制約の適用を無効にする組織ポリシーを作成または適用できます。新しい組織ポリシーを設定した場合、このセクションの既存の権限と、**Before Cloud Build Service Account Change** とマークされている項目を引き続き使用できます。そうでない場合は、既存の権限と、**After Cloud Build Service Account Change** とマークされている項目に従ってください。

ホスト接続の作成

- プロビジョニングプロジェクトにおけるCitrix Cloudサービスアカウントに必要な最小限の権限:

```
compute.instanceTemplates.list

compute.instances.list

compute.networks.list

compute.projects.get

compute.regions.list
```

```
compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get
```

次のGoogle定義のロールには、上記に記載されている権限があります:

- コンピュート管理者
- クラウド データストア ユーザー

- 共有VPCプロジェクトにおけるCitrix Cloudサービスアカウントの共有VPCに必要な追加の権限:

```
compute.networks.list

compute.subnetworks.list

resourcemanager.projects.get
```

次のGoogle定義のロールには、上記に記載されている権限があります:

- コンピュートネットワークユーザー

- サービスアカウントでは、使用したい暗号鍵があるプロジェクト (例: 共有プロジェクト) に次のロールを割り当てる必要があります:

  - Cloud KMS 閲覧者
  - クラウド KMS 暗号鍵の暗号化/復号者

  ロールを割り当てない場合は、次の権限があることを確認してください:

  - resourcemanager.projects.get
  - cloudkms.keyRings.list
  - cloudkms.keyRings.get
  - cloudkms.cryptoKeys.get
  - cloudkms.cryptoKeys.list
  - cloudkms.cryptoKeyVersions.useToDecrypt
  - cloudkms.cryptoKeyVersions.useToEncrypt

VM の電源管理

電源管理のみのカタログの場合に、プロビジョニングプロジェクト内のCitrix Cloudサービスアカウントに必要な最小限の権限:

```
compute.instanceTemplates.list

compute.instances.list

compute.instances.get

compute.instances.reset

compute.instances.resume

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get

compute.zoneOperations.get
```

以下のGoogle定義ロールは、上記にリストされている権限を持っています。

- コンピュート管理者
- クラウド データストア ユーザー

VM の作成、更新、または削除

- プロビジョニングプロジェクト内のCitrix Cloudサービスアカウントに必要な最小限の権限:

```
cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list
```

```
compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.instances.setTags

compute.instances.start
```

```
compute.instances.stop

compute.instances.suspend

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get
```

```
compute.zones.list

iam.serviceAccounts.actAs

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

compute.networks.get

compute.resourcePolicies.use
```

以下のGoogle定義ロールは、上記にリストされている権限を持っています。

- コンピュート管理者
- ストレージ管理者
- Cloud Build 編集者
- サービスアカウントユーザー
- クラウドデータストア ユーザー

- Shared VPC プロジェクトの Citrix Cloud サービスアカウントが、Shared VPC プロジェクトの VPC とサブネットワークを使用してホスティングユニットを作成するために必要な、Shared VPC の追加の権限:

```
compute.firewalls.list

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zones.list

resourcemanager.projects.get
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- コンピュートネットワーク ユーザー
- クラウドデータストア ユーザー

MCSに準備指示ディスクをダウンロードする際に必要な最小限の権限:

- (Cloud Build サービスアカウントの変更前): これらの権限をプロビジョニングプロジェクトの Cloud Build サービスアカウントに割り当てます。
- (Cloud Build サービスアカウントの変更後): これらの権限をプロビジョニングプロジェクトの Cloud Compute サービスアカウントに割り当てます。

```
compute.disks.create

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use
```

```
compute.disks.useReadOnly

compute.images.get

compute.images.list

compute.images.useReadOnly

compute.instances.create

compute.instances.delete

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.machineTypes.list

compute.networks.get

compute.networks.list

compute.projects.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zones.list

iam.serviceAccounts.actAs
```

```
logging.logEntries.create

pubsub.topics.publish

resourcemanager.projects.get

source.repos.get

source.repos.list

storage.buckets.create

storage.buckets.get

storage.buckets.list

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- Cloud Build サービスアカウント (Cloud Build サービスアカウントの変更後は Cloud Compute サービスアカウント)
- Compute Instance 管理者
- サービスアカウントユーザー

- 準備指示ディスクを MCS にダウンロードする際に、Google Cloud Build サービスによってプロビジョニングプロジェクトの Cloud Compute サービスアカウントに必要とされる最小限の権限:

```
resourcemanager.projects.get

storage.objects.create

storage.objects.get
```

```
storage.objects.list
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- コンピュートネットワーク ユーザー
- ストレージアカウントユーザー
- クラウドデータストア ユーザー

MCSに準備指示ディスクをダウンロードする際に、共有VPCに必要とされる追加の権限:

- (Cloud Buildサービスアカウント変更前): プロビジョニングプロジェクトのCloud Buildサービスアカウントにこれらの権限を割り当てます。
- (Cloud Buildサービスアカウント変更後): プロビジョニングプロジェクトのCloud Computeサービスアカウントにこれらの権限を割り当てます。

```
compute.firewalls.list

compute.networks.list

compute.subnetworks.list

compute.subnetworks.use

resourcemanager.projects.get
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- コンピュートネットワーク ユーザー
- ストレージアカウントユーザー
- クラウドデータストア ユーザー

- プロビジョニングプロジェクトのCitrix CloudサービスアカウントのCloud Key Management Service (KMS) に必要な追加権限:

```
cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get
```

```
cloudkms.keyRings.list
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- コンピュート KMS 閲覧者

一般的な権限

以下は、MCS でサポートされているすべての機能に対するプロビジョニングプロジェクトの Citrix Cloud サービスアカウントの権限です。これらの権限は、今後最高の互換性を提供します。

```
resourcemanager.projects.get

cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete
```

```
compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.reset

compute.instances.resume
```

```
compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.instances.update

compute.instances.updateAccessConfig

compute.instances.updateDisplayDevice

compute.instances.updateSecurity

compute.instances.updateShieldedInstanceConfig

compute.instances.updateShieldedVmConfig

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create
```

```
compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get
```

```
storage.objects.list

cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list

compute.disks.list

compute.instances.setServiceAccount

compute.networks.get

compute.networks.use

compute.networks.useExternalIp

iam.serviceAccounts.actAs

compute.resourcePolicies.use

cloudkms.cryptoKeyVersions.useToDecrypt

cloudkms.cryptoKeyVersions.useToEncrypt
```

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Google Cloud Platform (GCP)固有の情報については、Google Cloud Platformカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

HPE Moonshotへの接続

(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/connections.html)では、接続を作成するウィザードについて説明しています。以下の情報は、HPE Moonshotに固有の詳細を説明しています。

> **注:**
>
> HPE Moonshotへの接続を作成する前に、まずHPEアカウントの設定を完了する必要があります。HPE Moonshot仮想化環境を参照してください。

接続を作成する

HPE Moonshotへの接続は、以下を使用して作成できます。

- ウェブスタジオ
- PowerShellコマンド

Web Studioを使用して接続を作成する

1. **接続とリソースの追加**ページで、接続の種類として**HPE Moonshot**を選択します。
2. Moonshot iLO Chassis Managerの接続アドレスを入力します。アドレスには、IPアドレス、ホスト名、またはFQDNを使用できます。
3. シャーシの管理者資格情報とわかりやすい接続名を入力します。

接続設定は、次のいずれかの状況で停止します。

- Citrix Virtual Apps and Desktops™が、エラーのある公開CA署名付き証明書を受信した場合：エラーメッセージが表示されます。画面の指示に従って問題を修正してください。そうしないと、接続の作成を続行できません。
- Citrix Virtual Apps™ and Desktopsが、プライベートCA署名付き証明書を受信した場合。警告ページが表示されます。受信したサムプリントをサーバーのものと比較して、証明書の有効性を確認します。有効な場合は、**証明書を信頼する**を選択し、**OK**をクリックして接続の作成を続行します。Citrix Virtual Apps and Desktopsは、その証明書を信頼し、将来の検証のためにサムプリントを保存します。

PowerShellコマンドを使用して接続を作成する

PowerShellコマンドを使用して接続を作成する場合、次の情報を提供します。

- IP: HPEサーバーのIPアドレス

- ユーザー名: HPEユーザー名
- パスワード: HPEパスワード

例:

```
New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata
@{"Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false"} -Path
@("XDHyp:\Connections\$connectionName") -Persist -PluginId
"HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
$UserName -sslthumbprint $SslThumbprint New-BrokerHypervisorConnection
-HypHypervisorConnectionUid $HypervisorConnectionID
```

注:

`sslthumbprint` パラメーターは、プライベートCA署名付き証明書の場合にのみ必要です。

証明書とサムプリントの検証

HPE Moonshot への接続を正常に作成するには、証明書にエラーがなく、サムプリントが正しい値である必要があります。証明書とサムプリントの検証に関連するユースケースは次のとおりです。

- パブリックCA署名付き証明書にエラーがあります。接続は正常に作成されません。エラーの詳細を確認し、問題を解決してください。
- エラーのないパブリックCA署名付き証明書。接続は正常に作成され、`SslThumbprints` の値は**Null**です。
- エラーがなく、`sslthumbprint` 値を持つプライベートCA署名付き証明書。正しい `SslThumbprints` 値で接続が正常に作成されます。
- 不正なサムプリント値を持つプライベートCA署名付き証明書。接続は正常に作成されません。
- エラーのないプライベートCA署名付き証明書。接続は正常に作成されます。接続作成時、`SSlThumbprints` は**Null**です。`SSlThumbprints` 値はサイトサービスによって値に更新されます。

注:

> Citrix Database と Moonshot サーバー間の証明書サムプリントの不一致により、Web Studio で警告がトリガーされます。ただし、この警告は MMC ベースの Studio には表示されません。

接続の管理

このセクションでは、接続を管理する方法について詳しく説明します。

- Web Studio を使用して証明書の問題を修正する
- PowerShell コマンドを使用してサムプリント値を更新する

証明書の問題を修正する

証明書の問題が発生すると、Citrix Virtual Apps and Desktops は HPE Moonshot 接続をブロックし、関連する HPE Moonshot ノードでのワークロードの配信と管理を妨げます。**ホスト接続**リストの接続の横にエラーアイコンが表示されます。特定の問題と解決策については、次の表を参照してください。

問題	解決策
公開 CA 署名証明書で証明書エラーが発生する	接続をクリックし、**トラブルシューティング**タブを選択します。エラーの詳細を表示し、問題を解決します。
受信した証明書がプライベート CA 署名であるか、期限切れである。	ホスト接続を編集して、証明書のサムプリントを更新します。詳細な手順: 1. 接続を選択し、**接続の編集**をクリックします。 2. **接続プロパティ**ページで、**設定の編集**をクリックします。 3. HPE Moonshotシャーシに接続するためのパスワードを入力し、**保存**をクリックします。

問題	解決策	
	4. 表示される**警告**ページで、受信したサムプリントをサーバーのものと比較して、証明書の有効性を確認します。 5. それらが同じ場合は、**証明書を信頼する**を選択し、**OK**をクリックします。	

サムプリント値を更新する

接続を作成した後、`Set-Item` PowerShellコマンドを使用して接続のサムプリント値を更新できます。たとえば、次のコマンドを実行します。

1. 接続の詳細を取得します。例:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

2. サムプリント値を更新します。例:

```
Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
Administrator -SslThumbprint xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
```

3. 更新されたサムプリント値を確認します。例:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

注:

`Set-Item`コマンドで不正確なサムプリント値を指定すると、更新は失敗します。

次のステップ

- 初期展開プロセス中の場合は、マシンカタログの作成を参照してください。

- AWS固有の情報については、HPE Moonshotマシンカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

Microsoft Azure への接続

「接続とリソースの作成および管理」(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/connections.html)では、接続を作成するウィザードについて説明しています。以下の情報は、Azure Resource Managerクラウド環境に固有の詳細を扱っています。

> **注:**
>
> Microsoft Azure への接続を作成する前に、リソースの場所として Azure アカウントの設定を完了する必要があります。「Microsoft Azure Resource Manager クラウド環境」を参照してください。

サービスプリンシパルと接続の作成

接続を作成する前に、接続がAzureリソースにアクセスするために使用するサービスプリンシパルを設定する必要があります。接続は2つの方法で作成できます。

- Web Studio を使用してサービスプリンシパルと接続を同時に作成する
- 以前に作成したサービスプリンシパルを使用して接続を作成する

このセクションでは、次のタスクを完了する方法について説明します。

- Web Studio を使用してサービスプリンシパルと接続を作成する
- (/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/connections/connection-azure-resource-manager.html#create-a-service-principal-using-powershell)
- (/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/connections/connection-azure-resource-manager.html#get-the-application-secret-in-azure)
- 既存のサービスプリンシパルを使用して接続を作成する](/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/connections/connection-azure-resource-manager.html#create-a-connection-using-an-existing-service-principal)

考慮事項

- Citrix®は、共同作成者ロールを持つサービスプリンシパルの使用を推奨しています。ただし、最小限の権限のリストについては、「最小限の権限」(#minimum-permissions)セクションを参照してください。
- 最初の接続を作成する際、Azure は必要な権限を付与するよう求めます。今後の接続では引き続き認証が必要ですが、Azure は以前の同意を記憶しているため、プロンプトは再度表示されません。
- 認証に使用されるアカウントには、Azure RBAC を使用してサブスクリプションでロールを割り当てる権限が必要です。例として、サブスクリプションの所有者、ロールベースのアクセス制御管理者、またはユーザーアクセス管理者などがあります。
- 認証に使用されるアカウントは、サブスクリプションのディレクトリのメンバーである必要があります。「職場または学校」アカウントと「個人用 Microsoft アカウント」の2種類のアカウントに注意してください。詳細については、CTX219211 を参照してください。
- 既存の Microsoft アカウントをサブスクリプションのディレクトリのメンバーとして追加して使用することはできますが、ユーザーが以前にディレクトリのリソースのいずれかにゲストアクセスを許可されていた場合、複雑な問題が発生する可能性があります。この場合、必要な権限が付与されていないプレースホルダーエントリがディレクトリに存在し、エラーが返されることがあります。

  これを修正するには、ディレクトリからリソースを削除し、明示的に再度追加します。ただし、このオプションは、アカウントがアクセスできる他のリソースに意図しない影響を与える可能性があるため、慎重に実行してください。
- 特定のアカウントが実際にはメンバーであるにもかかわらず、ディレクトリゲストとして検出される既知の問題があります。このような構成は、通常、古い確立されたディレクトリアカウントで発生します。回避策：適切なメンバーシップ値を持つアカウントをディレクトリに追加します。
- リソースグループは単にリソースのコンテナであり、自身のリージョン以外のリージョンのリソースを含むことができます。リソースグループのリージョンに表示されるリソースが利用可能であると期待している場合、これは混乱を招く可能性があります。
- 必要な数のマシンをホストするのに十分なネットワークとサブネットのサイズを確保してください。これにはある程度の先見性が必要ですが、Microsoft はアドレス空間容量に関するガイダンスを提供し、適切な値を指定するのに役立ちます。

Web Studio を使用してサービスプリンシパルと接続を作成する

> **重要：**

この機能は、Azure China サブスクリプションではまだ利用できません。

Web Studio を使用すると、サービスプリンシパルと接続の両方を単一のワークフローで作成できます。サービスプリンシパルは、接続に Azure リソースへのアクセスを許可します。サービスプリンシパルを作成するために Azure に認証すると、Azure にアプリケーションが登録されます。登録されたアプリケーションには、シークレットキー（クライアントシークレットまたはアプリケーションシークレットと呼ばれます）が作成されます。登録されたアプリケーション（この場合は接続）は、クライアントシークレットを使用して Microsoft Entra ID に認証します。

開始する前に、以下の前提条件を満たしていることを確認してください。

- サブスクリプションの Microsoft Entra テナントにユーザーアカウントがあること。
- 認証に使用されるアカウントには、Azure RBAC を使用してサブスクリプションでロールを割り当てる権限が必要です。例として、サブスクリプションの所有者、ロールベースのアクセス制御管理者、またはユーザーアクセス管理者などがあります。
- 認証には、グローバル管理者、アプリケーション管理者、またはアプリケーション開発者の権限が必要です。これらの権限は、ホスト接続の作成後に取り消すことができます。ロールの詳細については、「Microsoft Entra の組み込みロール」を参照してください。

接続とリソースの追加ウィザードを使用して、サービスプリンシパルと接続を同時に作成します。

1. **接続**ページで、**新しい接続の作成**、**Microsoft Azure**接続タイプ、およびAzure環境を選択します。
2. 仮想マシンを作成するために使用するツールを選択し、**次へ**を選択します。
3. **接続の詳細**ページで、AzureサブスクリプションIDと接続名を入力します。サブスクリプションIDを入力すると、**新規作成**ボタンが有効になります。

   注:

   接続名には 1～64 文字を含めることができ、空白のみ、または文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。

4. **新規作成**を選択し、Microsoft Entraアカウントのユーザー名とパスワードを入力します。
5. **サインイン**を選択します。

6. **同意**を選択して、Citrix Virtual Apps and Desktops™にリストされている権限を付与します。Citrix Virtual Apps and Desktopsは、指定されたユーザーに代わってAzureリソースを管理できるサービスプリンシパルを作成します。
7. **同意**を選択すると、ウィザードの**接続**ページに戻ります。

> **注:**
>
> Azure への認証が正常に完了すると、「**Create new**」ボタンと「**Use existing**」ボタンが消えます。「**Connection successful**」というテキストが緑色のチェックマークとともに表示され、Azure サブスクリプションへの接続が成功したことを示します。

8. 「**Connection Details**」ページで、「**Next**」を選択します。

> **注:**
>
> Azure への認証が正常に完了し、必要な権限の付与に同意するまで、次のページに進むことはできません。

9. 接続のリソースを構成します。リソースには、リージョンとネットワークが含まれます。
   - **リージョン**ページで、リージョンを選択します。
   - **ネットワーク**ページで、以下を実行します。
     - リージョンとネットワークの組み合わせを識別するために、1〜64文字のリソース名を入力します。リソース名には、空白のみを含めることや、文字`\/;:#.*?=<>|[]{}"'()'`を含めることはできません。
     - 仮想ネットワーク/リソースグループのペアを選択します。（同じ名前の仮想ネットワークが複数ある場合、ネットワーク名をリソースグループとペアにすることで、一意の組み合わせが提供されます。）前のページで選択したリージョンに仮想ネットワークがない場合は、そのページに戻り、仮想ネットワークがあるリージョンを選択してください。
10. **概要**ページで、設定の概要を確認し、**完了**を選択してセットアップを完了します。

アプリケーションIDを表示する

接続を作成した後、その接続がAzureリソースへのアクセスに使用するアプリケーションIDを表示できます。

接続とリソースの追加リストで、詳細を表示する接続を選択します。**詳細**タブにアプリケーションIDが表示されます。

PowerShellを使用してサービスプリンシパルを作成する

PowerShellを使用してサービスプリンシパルを作成するには、Azure Resource Managerサブスクリプションに接続し、以下のセクションで提供されているPowerShellコマンドレットを使用します。

次の項目を準備してください。

- **SubscriptionId:** VDAをプロビジョニングするサブスクリプションのAzure Resource Manager `SubscriptionID`。
- **ActiveDirectoryID**: Microsoft Entra IDに登録したアプリケーションのテナントID。
- **ApplicationName:** Microsoft Entra IDで作成するアプリケーションの名前。

詳細な手順は次のとおりです。

1. Azure Resource Manager サブスクリプションに接続します。

   ```
   Connect-AzAccount
   ```

2. サービスプリンシパルを作成する Azure Resource Manager サブスクリプションを選択します。

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-AzSubscription
   ```

3. ADテナントでアプリケーションを作成します。

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

4. サービスプリンシパルを作成します。

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

5. サービスプリンシパルにロールを割り当てます。

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

6. PowerShell コンソールの出力ウィンドウから ApplicationId をメモします。ホスト接続を作成する際に、その ID を指定します。

Azure でアプリケーションシークレットを取得する

既存のサービスプリンシパルを使用して接続を作成するには、まず Azure portal でサービスプリンシパルのアプリケーションIDとシークレットを取得する必要があります。

詳細な手順は次のとおりです。

1. Web Studio から、または PowerShell を使用して「**Application ID**」を取得します。
2. Azureポータルにサインインします。
3. Azureで、**Microsoft Entra ID**を選択します。
4. Microsoft Entra IDの**アプリの登録**から、アプリケーションを選択します。
5. **証明書とシークレット**に移動します。
6. **クライアントシークレット**をクリックします。

既存のサービスプリンシパルを使用して接続を作成する

サービスプリンシパルが既にある場合は、それを使用して Web Studio で接続を作成できます。

次の項目を準備してください。

- SubscriptionId
- ActiveDirectoryID (テナントID)
- アプリケーションID
- アプリケーションシークレット

  詳細については、「アプリケーションシークレットの取得」を参照してください。
- シークレットの有効期限

詳細な手順は次のとおりです。

接続とリソースの追加ウィザードで、次の操作を行います。

1. **接続**ページで、**新しい接続を作成**、**Microsoft Azure**接続の種類、およびAzure環境を選択します。
2. 仮想マシンの作成に使用するツールを選択し、**次へ**を選択します。
3. 「**接続の詳細**」ページで、Azure サブスクリプション ID と接続の名前を入力します。

> **注:**
>
> 接続名には 1～64 文字を含めることができ、空白のみ、または文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。

4. **既存のものを使用**を選択します。**既存のサービスプリンシパルの詳細**ウィンドウで、既存のサービスプリンシパルに対して次の設定を入力します。詳細を入力すると、**保存**ボタンが有効になります。**保存**を選択します。有効な詳細情報を提供するまで、このページから先に進むことはできません。

   - **サブスクリプションID**。AzureサブスクリプションIDを入力します。サブスクリプションIDを取得するには、Azureポータルにサインインし、**サブスクリプション > 概要**に移動します。
   - **Active Directory ID**（テナントID）。Azure ADに登録したアプリケーションのディレクトリ（テナント）IDを入力します。
   - **アプリケーションID**。Azure ADに登録したアプリケーションのアプリケーション（クライアント）IDを入力します。
   - **アプリケーションシークレット**。シークレットキー（クライアントシークレット）を作成します。登録されたアプリケーションは、このキーを使用してAzure ADに認証します。セキュリティ上の理由から、キーを定期的に変更することをお勧めします。キーは後で取得できないため、必ず保存してください。
   - **シークレットの有効期限**。アプリケーションシークレットの有効期限が切れる日付を入力します。シークレットキーの有効期限が切れる14日前から、**ホスティング**ノードの特定のホスト接続に警告アイコンが表示されます。ただし、シークレットキーの有効期限が切れると、エラーが発生します。

     > **注:**
     >
     > セキュリティ上の理由から、有効期限は現在から2年を超えることはできません。

   - **認証 URL**。このフィールドは自動的に入力され、編集できません。
   - **管理 URL**。このフィールドは自動的に入力され、編集できません。
   - **ストレージサフィックス**。このフィールドは自動的に入力され、編集できません。
   - **ディスクまたはスナップショットをアップロードまたはダウンロードするためのAzure BLOBストレージエンドポイント**。このフィールドは自動的に入力され、編集できません。
   - **Key Vaultサービス**。このフィールドは自動的に入力され、編集できません。
   - **サービスバスサフィックス**。このフィールドは自動的に入力され、編集できません。

AzureでMCSカタログを作成するには、以下のエンドポイントへのアクセスが必要です。これらのエンドポイントへのアクセスにより、ネットワークとAzureポータルおよびそのサービス間の接続が最適化されます。

- 認証URL: `https://login.microsoftonline.com`
- 管理URL: `https://management.azure.com`。これはAzure Resource Managerプロバイダー APIのリクエストURLです。管理のエンドポイントは環境によって異なります。たとえば、Azure Globalの場合は`https://management.azure.com`、Azure US Governmentの場合は`https://management.usgovcloudapi.net`です。
- ストレージサフィックス: `https://*.core.windows.net`。これは (*) ストレージサフィックスのワイルドカード文字です。例: `https://demo.table.core.windows.net`。
- ディスクまたはスナップショットをアップロードまたはダウンロードするためのAzure BLOBストレージエンドポイント: `https://*.storage.azure.net`。これは (*) BLOBストレージのインポートおよびエクスポート操作のワイルドカード文字です。例: `https://md-impexp-xxxxx.z[00-50].blob.storage.azure.net`。
- Key Vaultサービス: `https://*.vault.azure.net`。これは (*) Key Vault名のワイルドカード文字です。例: `https://<your-key-vault-name>.vault.azure.net`。
- サービスバスサフィックス: `https://*.servicebus.windows.net`。これは (*) グローバルAzureクラウドで作成された名前空間のワイルドカード文字です。例: `https://{serviceNamespace}.servicebus.windows.net/{path}`。

5. **保存**を選択すると、「**接続の詳細**」ページに戻ります。「**次へ**」を選択して次のページに進みます。
6. 接続のリソースを構成します。リソースは、リージョンとネットワークで構成されます。

   - ページで、リージョンを選択します。
   - ページで、次の操作を行います。

     - リージョンとネットワークの組み合わせを識別するために、1〜64文字のリソース名を入力します。リソース名には、空白のみ、または文字`\/;:#.*?=<>|[]{}"'()'`を含めることはできません。
     - 仮想ネットワーク/リソースグループのペアを選択します。(同じ名前の仮想ネットワークが複数ある場合、ネットワーク名をリソースグループとペアにすると、一意の組み合わせが提供されます。)前のページで選択したリージョンに仮想ネットワークがない場合は、そのページに戻り、仮想ネットワークがあるリージョンを選択してください。

7. ページで、設定の概要を確認し、 を選択してセットアップを完了します。

サービスプリンシパルと接続を管理する

このセクションでは、サービスプリンシパルと接続を管理する方法について詳しく説明します。

- Azureの調整設定を構成する
- Azureでイメージ共有を有効にする
- Web Studioを使用して共有テナントを接続に追加する
- PowerShellを使用してイメージ共有を実装する
- アプリケーションシークレットとシークレットの有効期限を管理する

Azureの調整設定を構成する

Azure Resource Managerは、サブスクリプションとテナントのリクエストを調整し、プロバイダーの特定のニーズに合わせて定義された制限に基づいてトラフィックをルーティングします。詳細については、MicrosoftサイトのResource Managerリクエストの調整を参照してください。サブスクリプションとテナントには制限があり、多数のマシンを管理することが問題になる場合があります。たとえば、多数のマシンを含むサブスクリプションでは、電源操作に関連するパフォーマンスの問題が発生する可能性があります。

> **ヒント:**
>
> 詳細については、「Machine Creation ServicesによるAzureパフォーマンスの向上」を参照してください。
>
> これらの問題を軽減するために、MCSの内部スロットリングを削除して、Azureから利用可能な要求クォータをより多く使用できます。

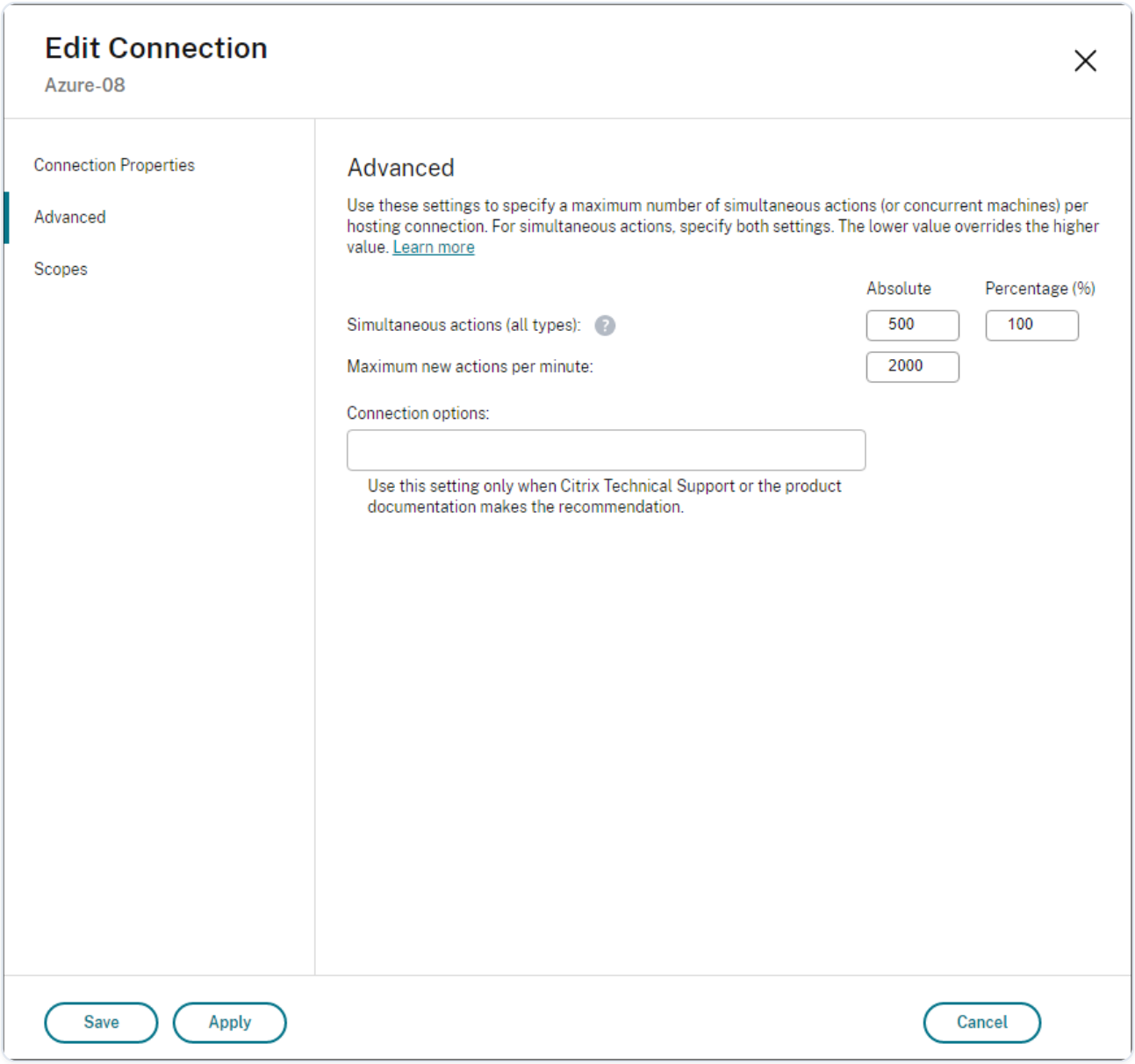
大規模なサブスクリプション（例えば1,000台のVMを含むもの）でVMの電源をオンまたはオフにする場合、以下の最適な設定をお勧めします。

- 絶対同時操作数: 500
- 1分あたりの最大新規操作数: 2000
- 操作の最大同時実行数: 500

特定のAzure接続に対してAzure操作を構成するには、Web Studioを使用します。

1. Web Studioで、左ペインで**ホスティング**を選択します。

2. 接続を選択します。
3. **接続の編集**ウィザードで、**詳細設定**を選択します。
4. **詳細設定**ページで、構成オプションを使用して、同時アクションの数、1分あたりの最大新規アクション数、および追加の接続オプションを指定します。



MCSはデフォルトで最大500の同時操作をサポートします。または、Remote PowerShell SDKを使用して、同時操作の最大数を設定できます。

同時Azureプロビジョニング操作の最大数を指定するには、**PowerShell**プロパティ `MaximumConcurrentProvisioningOperations` を使用します。このプロパティを使用する際は、以下を考慮してください。

- `MaximumConcurrentProvisioningOperations` のデフォルト値は 500 です。

- PowerShell コマンド `Set-item` を使用して、`MaximumConcurrentProvisioningOperations` パラメーターを構成します。

Azure でのイメージ共有を有効にする

マシンカタログを作成または更新する際に、異なる Azure テナントおよびサブスクリプションからの共有イメージ（Azure Compute Gallery を介して共有）を選択できます。テナント内またはテナント間でイメージ共有を有効にするには、Azure で必要な設定を行う必要があります。

- テナント内でのイメージ共有（サブスクリプション間）
- テナント間でのイメージ共有

テナント内でのイメージ共有（サブスクリプション間）

別のサブスクリプションに属する Azure Compute Gallery のイメージを選択するには、そのイメージをそのサブスクリプションのサービスプリンシパル (SPN) と共有する必要があります。

たとえば、Studio で次のように構成されているサービスプリンシパル (SPN 1) がある場合：

サービスプリンシパル: SPN 1

サブスクリプション: subscription 1

テナント: tenant 1

イメージは別のサブスクリプションにあり、Studio で次のように構成されています：

サブスクリプション: subscription 2

テナント: tenant 1

サブスクリプション 2 のイメージをサブスクリプション 1 (SPN 1) と共有する場合は、サブスクリプション 2 に移動し、リソースグループを SPN1 と共有します。

イメージは、Azure ロールベースのアクセス制御 (RBAC) を使用して、別の SPN と共有する必要があります。Azure RBAC は、Azure リソースへのアクセスを管理するために使用される承認システムです。Azure RBAC の詳細については、Microsoft ドキュメントの「Azure ロールベースのアクセス制御 (Azure RBAC) とは」を参照してください。アクセスを許可するには、リソースグループスコープで共同作成者ロールを持つサービスプリンシパルにロールを割り当てます。Azure ロールを割り当てるには、ユーザーアクセス管理者や所有者などの `Microsoft.Authorization/roleAssignments/write` 権限が必要です。別の SPN とイメージを共有する方法の詳細については、Microsoft ドキュメントの「Azure portal を使用して Azure ロールを割り当てる」を参照してください。

PowerShell コマンドを使用して別のサブスクリプションからイメージを選択する方法については、「別のサブスクリプションからイメージを選択する」を参照してください。

テナント間で画像を共有する

Azure Compute Gallery を使用してテナント間でイメージを共有するには、アプリケーション登録を作成します。

たとえば、2 つのテナント (テナント 1 とテナント 2) があり、イメージギャラリーをテナント 1 と共有したい場合は、次の手順を実行します。

1. テナント 1 のアプリケーション登録を作成します。詳細については、「アプリ登録を作成する」を参照してください。
2. ブラウザを使用してサインインを要求することで、テナント 2 にアプリケーションへのアクセスを許可します。`Tenant2 ID` をテナント 1 のテナント ID に置き換えます。`Application (client) ID` を作成したアプリケーション登録のアプリケーション ID に置き換えます。置き換えが完了したら、URL をブラウザに貼り付け、サインインプロンプトに従ってテナント 2 にサインインします。例:

   ```
   https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
   client_id=<Application (client)
   ID>&response_type=code&redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
   ```

   詳細については、「テナント 2 にアクセスを許可する」を参照してください。
3. テナント 2 のリソースグループにアプリケーションアクセスを許可します。テナント 2 としてサインインし、ギャラリーイメージがあるリソースグループにアプリケーション登録アクセスを許可します。詳細については、「テナント間で要求を認証する」を参照してください。

PowerShell コマンドを使用して、別のテナントのイメージからカタログを作成するには:

1. 共有テナント ID でホスティング接続のカスタムプロパティを更新する。
2. 別のテナントからイメージを選択する。

Web Studio を使用して共有テナントを接続に追加する

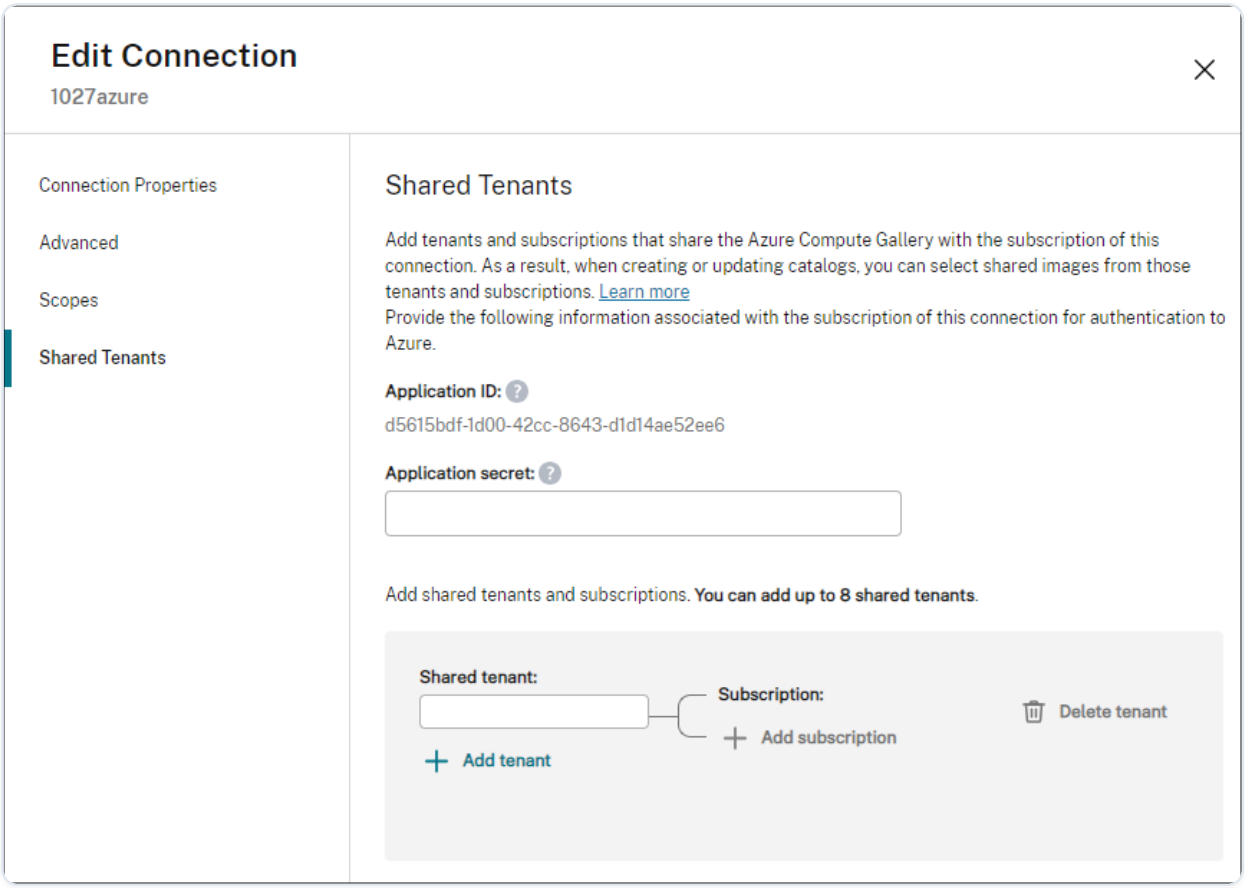
Web Studio でマシンカタログを作成または更新する際に、異なる Azure テナントおよびサブスクリプション (Azure Compute Gallery を介して共有) から共有イメージを選択できます。この機能では、関連するホスト接続の共有テナントおよびサブスクリプション情報を提供する必要があります。

注記:

テナント間でイメージ共有を有効にするために、Azure で必要な設定を構成していることを確認してください。詳細については、「テナント間でイメージを共有する」を参照してください。

接続については、次の手順を実行します。

1. Web Studio の左側のペインで、 を選択します。
2. 接続を選択し、アクションバーで を選択します。



3. で、次の操作を行います。

   - 接続のサブスクリプションに関連付けられているアプリケーション ID とアプリケーションシークレットを指定します。Citrix Virtual Apps™ and Desktops は、この情報を使用して Microsoft Entra ID に対して認証を行います。
   - 接続のサブスクリプションと Azure Compute Gallery を共有するテナントとサブスクリプションを追加します。共有テナントは最大 8 つ、各テナントのサブスクリプションは最大 8 つ追加できます。

4. 完了したら、 を選択して変更を適用し、ウィンドウを開いたままにするか、 を選択して変更を適用し、ウィンドウを閉じます。

PowerShellを使用したイメージ共有の実装

このセクションでは、PowerShellを使用してイメージを共有するプロセスについて説明します。

- 別のサブスクリプションからイメージを選択する
- 共有テナント ID を使用してホスティング接続のカスタムプロパティを更新する
- 別のテナントからイメージを選択する

別のサブスクリプションからイメージを選択する

同じAzureテナント内の別の共有サブスクリプションに属するAzure Compute Galleryのイメージを選択して、PowerShellコマンドを使用してMCSカタログを作成および更新できます。

1. ホスティングユニットのルートフォルダーに、Citrixは`sharedsubscription`という新しい共有サブスクリプションフォルダーを作成します。
2. テナント内のすべての共有サブスクリプションを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\sharedsubscription.folder"
```

3. 1つの共有サブスクリプションを選択し、その共有サブスクリプションのすべての共有リソースグループを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription"
```

4. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\
xyz.resourcegroup"
```

5. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\testgallery.gallery"
```

6. 1つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\sigtestdef.imagedefinition"
```

7. 次の要素を使用してMCSカタログを作成および更新します。

   - リソースグループ
   - ギャラリー
   - ギャラリーイメージ定義
   - ギャラリーイメージバージョン

   Remote PowerShell SDK を使用したカタログの作成方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

共有テナントIDでホスティング接続のカスタムプロパティを更新する

`Set-Item`を使用して、共有テナントIDとサブスクリプションIDでホスティング接続のカスタムプロパティを更新します。`CustomProperties`に`SharedTenants`プロパティを追加します。`Shared Tenants`の形式は次のとおりです。

```
[{"Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":
["7bb42f40-8d7f-4230-a920-be2781f6d5d9"]},{"Tenant":"50e83564-c4e5-4209-
b43d-815c45659564","Subscriptions":["06ab8944-6a88-47ee-
a975-43dd491a37d0"]}]
```

例：

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
Value=`"123`" />

<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
Value=`"https://management.azure.com/`" />
```

```
<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
Value=`"https://login.microsoftonline.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`"
Value=`"core.windows.net`" />

<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`" /
>

<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`"
Value=`"`[ { 'Tenant':'123abc', 'Subscriptions':['345', '567'] } ]`"` />

</CustomProperties>"

-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "advc345"
-SecurePassword

$psd
```

注:

複数のテナントを追加できます。各テナントは複数のサブスクリプションを持つことができます。

別のテナントからイメージを選択する

PowerShellコマンドを使用してMCSカタログを作成および更新するために、別のAzureテナントに属するAzure Compute Galleryのイメージを選択できます。

1. ホスティングユニットのルートフォルダーに、Citrixは`sharedsubscription`という名前の新しい共有サブスクリプションフォルダーを作成します。
2. すべての共有サブスクリプションを一覧表示します。

   ```
   Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
   ```

3. 1つの共有サブスクリプションを選択し、その共有サブスクリプションのすべての共有リソースグループを一覧表示します。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription
```

4. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\
xyz.resourcegroup
```

5. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery
```

6. 1つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery\hij.imagedefinition
```

7. 次の要素を使用してMCSカタログを作成および更新します。

   - リソースグループ
   - ギャラリー
   - ギャラリーイメージ定義
   - ギャラリーイメージバージョン

   Remote PowerShell SDK を使用してカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>` を参照してください。

アプリケーションシークレットとシークレットの有効期限を管理する

シークレットの有効期限が切れる前に、接続のアプリケーションシークレットを必ず変更してください。シークレットキーの有効期限が切れる14日前から、**ホスティング**ノードの特定のホスト接続に警告アイコンが表示されます。ただし、シークレットキーの有効期限が切れると、エラーが発生します。

AZURE でアプリケーションシークレットを作成する

Azure portal を介して接続のアプリケーションシークレットを作成できます。

1. **Microsoft Entra ID** を選択します。
2. Microsoft Entra ID の から、アプリケーションを選択します。
3. に移動します。
4. **>** をクリックします。
5. シークレットの説明を入力し、期間を指定します。完了したら、 を選択します。

> **注:**
>
> クライアントシークレットは後で取得できないため、必ず保存してください。

6. クライアントシークレットの値と有効期限をコピーします。
7. Web Studio で、対応する接続を編集し、**アプリケーションシークレット**と**シークレットの有効期限**フィールドの内容をコピーした値に置き換えます。

シークレットの有効期限を変更する

Web Studio を使用して、使用中のアプリケーションシークレットの有効期限を追加または変更できます。

> **注:**
>
> シークレットキーの有効期限が切れる14日前から、**Hosting** ノードの特定のホスト接続に警告アイコンが表示されます。

1. **接続とリソースの追加**ウィザードで、接続を右クリックし、**接続の編集**をクリックします。
2. **接続プロパティ**ページで、**シークレットの有効期限**をクリックして、使用中のアプリケーションシークレットの有効期限を追加または変更します。

事前作成されたネットワークセキュリティグループを使用する

Citrix に NSG の作成と変更を要求する代わりに、イメージ準備用の Deny-All ネットワークセキュリティグループを作成します。PowerShell コマンド `Set-Item` を使用してホスティングユニットのカスタムプロパティを編集し、Deny-All ネットワークセキュリティグループを提供するためのパラメーター `NsgForPreparation` を含めます。

前提条件

サービスプリンシパルに必要な以下のアクセス許可を構成します。

- `Microsoft.Network/networkSecurityGroups/join/action`: ネットワークセキュリティグループをサブネットまたはネットワークインターフェースに関連付ける
- `Microsoft.Network/networkSecurityGroups/read`: ネットワークセキュリティグループを取得する
- `Microsoft.Network/networkSecurityGroups/securityRules/read`: ルールを取得する

事前作成された Deny-All ネットワークセキュリティグループを追加する

事前作成されたDeny-Allネットワークセキュリティグループを追加するには、ホスティングユニットでカスタムプロパティを次のように設定します。

1. Remote PowerShell SDKを使用してPowerShellウィンドウを開きます。
2. 次のコマンドを実行します。

```
Add-PSSnapin citrix*.

cd XDHyp:\HostingUnits\

Dir
```

3. 詳細を取得するホスティングユニットを選択します。

```
Get-Item "XDHyp:\HostingUnits\<hostingunitname>"
```

4. CustomPropertiesをメモ帳にコピーし、プロパティ設定`<Property xsi:type="StringProperty`" Name=`"NsgForPreparation`" Value=`"{ResourceGroupName}/{NetworkSecurityGroupName}"/>`を追加します。例：

```
<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"NsgForPreparation`" Value=`{ResourceGroupName}/
{NetworkSecurityGroupName}`"/></CustomProperties>
```

5. PowerShell ウィンドウで、変更されたカスタムプロパティに変数を割り当てます。例:

```
$customProperty = "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"NsgForPreparation`" Value=`"{ResourceGroupName}/
{NetworkSecurityGroupName}`"/></CustomProperties>"
```

6. `$cred = Get-Credential` を実行します。プロンプトが表示されたら、接続資格情報を入力します。資格情報は Azure アプリケーション ID とシークレットです。
7. 次のコマンドを実行します。

```
Set-Item -PSPath XDHyp:\HostingUnits\<hostingunitname>
-CustomProperties $customProperty -username $cred.username
-Securepassword $cred.password
```

重要:

SubscriptionIdがありませんというメッセージが表示された場合は、カスタムプロパティ内のすべての二重引用符（“）をバッククォートと二重引用符（`”）に置き換えてください。

8. 更新された `CustomProperties` 設定を確認するには、`dir` を実行します。

注:

更新が反映されるまでに1分以上かかります。

ネットワークセキュリティグループの詳細を取得する

ネットワークセキュリティグループの詳細を取得するには、まずネットワークセキュリティグループを含むリソースグループを取得し、次にリソースグループ名に基づいてネットワークセキュリティグループを取得します。

1. ネットワークセキュリティグループを含むリソースグループを取得します。例：

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes":
["networksecuritygroup"]}'
```

2. リソースグループ名に基づいてネットワークセキュリティグループを取得します。例：

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType securitygroup -MaxRecords
5 -AdditionalDataFilter '{"location": ["eastus", "westus"],
"resourcegroup":["resourcegroupname"]}'
```

空のリソースグループをフィルターする

マシンカタログ作成時にマスターイメージ、マシンプロファイル、または準備済みイメージを選択する際に、空のリソースグループをフィルタリングするには、PowerShellコマンド `Get-HypInventoryItem` を使用します。

例:

- ページ内の最大レコード数を取得する:

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5
```

- ページ内の最大レコード数を取得し、特定のリソースを持つリソースコンテナを見つけるためにフィルタリングする。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
```

- スキップを使用してページを直接指定して取得し、特定のリソースを持つリソースコンテナを見つけるためにフィルタリングする。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -skip 20 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
```

- トークンを使用して次のページを取得し、特定のリソースを持つリソースコンテナを見つけるためにフィルタリングする。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
-ContinuationToken
'ew0KICAiJGlkIjogIjEiLA0KICAiTWF4Um93cyI6IDUsDQogICJSb3dzVG9Ta2lwIjogMj
UsDQogICJLdXN0b0NsdXN0ZXJVcmwiOiAiaHR0cHM6Ly9hcmctbmV1LTEzLXNmLmFyZy5jb
3JlLndpbmRvd3MubmV0Ig0KfQ=='
```

- Citrix内部タグを持つすべてのリソースグループを取得し、`MaxRecords` で最大レコード数を制限します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5
```

- Citrix内部タグを持つマシンプロファイル（マスターイメージ）をフィルタリングし、`MaxRecords` で最大レコード数を制限します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"templatespecversion"]}'
```

- Citrix内部タグを持つ準備済みイメージをフィルタリングし、`MaxRecords` で最大レコード数を制限します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
```

```
5 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion"]}'
```

- Citrix内部タグを持つマシンプロファイル（準備済みイメージ）をフィルタリングし、`MaxRecords` で最大レコード数を制限します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"templatespecversion"]}'
```

- Citrix内部タグを持つイメージをフィルタリングし、`MaxRecords` と場所で最大レコード数を制限します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion", "storageaccount"], "location": ["eastus",
"westus"]}'
```

- タグを考慮せずにすべてのリソースグループを取得する `CitrixResource`。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
50 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion", "storageaccount"]}' -Force $true
```

Azure Sovereign Airgapクラウド環境に接続する

Azure Sovereign Airgapクラウド環境は、分離されたネットワークドメイン上になければならない最高機密のワークロードに適しています。ホスト接続の作成時に、カスタムプロパティ `DisableInstanceDiscovery` を使用してAzure Sovereign Airgapクラウド環境に接続できます。

```
<Property xsi:type="StringProperty" Name="DisableInstanceDiscovery"
Value="true" />
```

Azureホスト接続の作成の詳細については、Create-HostingConnection.ps1を参照してください。

必要なAzure権限

このセクションには、Azure に必要な最小限の一般的な権限が含まれています。

最小限の権限

最小限の権限は、より優れたセキュリティ制御を提供します。ただし、追加の権限を必要とする新機能は、最小限の権限のみを使用しているため失敗します。

ホスト接続の作成

Azure から取得した情報を使用して、新しいホスト接続を追加します。

```
"Microsoft.Network/virtualNetworks/read",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/disks/read",

"Microsoft.Resources/providers/read",

"Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/tenants/read",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/securityRules/read"
```

VM の電源管理

マシンインスタンスの電源をオンまたはオフにします。

```
"Microsoft.Compute/virtualMachines/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/restart/action",
```

```
"Microsoft.Insights/diagnosticsettings/delete",

"Microsoft.Insights/diagnosticsettings/read",

"Microsoft.Insights/diagnosticsettings/write",
```

仮想マシンの作成、更新、または削除

マシンカタログを作成し、マシンを追加、削除、更新し、マシンカタログを削除します。

以下は、マスターイメージがマネージドディスクである場合、またはスナップショットがホスティング接続と同じリージョンにある場合に必要となる最小限の権限のリストです。

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",
```

```
"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
read",

"Microsoft.Compute/skus/read",

"Microsoft.Compute/virtualMachines/extensions/read",

"Microsoft.Compute/virtualMachines/extensions/write",

"Microsoft.Features/providers/features/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/locations/usages/read",

"Microsoft.Compute/capacityReservationGroups/capacityReservations/read"
```

以下の機能には、最小限の権限に加えて、以下の追加の権限が必要です。

- マスターイメージがホスティング接続と同じリージョンにあるストレージアカウント内の VHD である場合：

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",
```

- マスターイメージが共有イメージギャラリーのImageVersionである場合:

```
"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/read",
```

- マスターイメージがマネージドディスクである場合、スナップショットまたはVHDがホスティング接続のリージョンとは異なるリージョンにある場合:

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",
```

- Citrix管理のリソースグループを使用する場合:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
```

- マスターイメージを共有テナントまたはサブスクリプションのAzure Compute Gallery（旧Shared Image Gallery）に配置する場合:

```
"Microsoft.Compute/galleries/write",

"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/images/versions/write",

"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/versions/delete",

"Microsoft.Resources/subscriptions/read",
```

- Azure専用ホストサポートを使用する場合:

```
"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",

"Microsoft.Compute/hostGroups/hosts/read",
```

- カスタマーマネージドキー（CMK）でサーバー側暗号化（SSE）を使用する場合:

```
"Microsoft.Compute/diskEncryptionSets/read",
```

- ARMテンプレート（マシンプロファイル）を使用してVMを展開する場合:

```
"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/delete",

"Microsoft.Insights/DataCollectionRuleAssociations/Read",

"Microsoft.Insights/dataCollectionRules/read",
```

- Azure テンプレート仕様をマシンプロファイルとして使用する場合:

```
"Microsoft.Resources/templateSpecs/read",

"Microsoft.Resources/templateSpecs/versions/read",
```

アンマネージドディスクを使用したマシンの作成、更新、削除

マスターイメージがVHDであり、管理者が提供するリソースグループを使用する場合に必要な最小限の権限のリストは次のとおりです:

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",
```

```
"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/locations/usages/read",
```

コスト管理

VM の価格を取得するために必要な最小限の権限は次のとおりです。

```
"Microsoft.Consumption/pricesheets/read"
```

VM のコストを取得するために必要な最小限の権限は次のとおりです。

```
"Microsoft.CostManagement/query/read"
```

注:

Azureマシンカタログの**Cost Insights**タブを表示するには、**Cost Management > Manage > Read cost**権限（クラウド管理者にはデフォルト）が必要です。**Cost Insights**タブの詳細については、「カタログの詳細を表示」を参照してください。

一般的な権限

共同作成者ロールは、すべてのリソースを管理するためのフルアクセス権を持っています。この権限セットは、新機能の取得を妨げるものではありません。

現在の機能セットで必要とされる以上の権限が含まれていますが、以下の権限セットは将来にわたって最高の互換性を提供します。

```
"Microsoft.Compute/diskEncryptionSets/read",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/delete",

"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/images/versions/write",
```

```
"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/write",

"Microsoft.Compute/hostGroups/hosts/read",

"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
read",

"Microsoft.Compute/skus/read",

"Microsoft.Compute/virtualMachines/extensions/read",

"Microsoft.Compute/virtualMachines/extensions/write",
```

```
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/locations/usages/read",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/delete",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Resources/providers/read",
"Microsoft.Resources/subscriptions/locations/read",
```

```
"Microsoft.Resources/subscriptions/read",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Resources/tenants/read",
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
"Microsoft.Features/providers/features/read",
"Microsoft.Insights/DataCollectionRuleAssociations/Read",
"Microsoft.Insights/dataCollectionRules/read",
"Microsoft.Insights/diagnosticsettings/delete",
"Microsoft.Insights/diagnosticsettings/read",
"Microsoft.Insights/diagnosticsettings/write",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/securityRules/read",
```

```
"Microsoft.Compute/capacityReservationGroups/capacityReservations/read"
```

Azureの非シークレット環境でホスト接続を検証する

ホスト接続の権限を検証して、MCSマシンカタログの作成と管理に関連するタスクを実行できます。この実装は、VMの作成、削除、更新、VMの電源管理など、さまざまなシナリオに必要な不足している権限を事前に特定するのに役立ち、重要な時期にブロックされるのを回避できます。

PowerShellコマンド`Test-HypHypervisorConnection`を使用して、ホスト接続の権限を検証できます。コマンドの結果はリストとして取得され、リスト内の各項目は3つのセクションに分かれています。

- カテゴリ: ユーザーがMCSマシンカタログを作成および管理するために実行できるアクションまたはタスク。
- 修正措置: 管理者がユーザーの不足している権限の不一致を解決するために実行する必要がある手順。
- 不足している権限: カテゴリの不足している権限のリスト。

権限を検証するには、次の手順を実行します。

1. Azureへのホスト接続を作成します。
2. Delivery Controller™ホストからPowerShellウィンドウを開きます。
3. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
4. 接続をテストするために必要な権限があるかどうかを確認するには、次のコマンドを実行します。

   ```
   Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\AzureCon"
   ```

   SPNに必要なロールレベルの権限:

   - Microsoft.Authorization/roleDefinitions/read (サブスクリプションレベル、またはリソースグループが指定されている場合はリソースグループレベル)
   - Microsoft.Authorization/roleAssignments/read (サブスクリプションレベル、またはリソースグループが指定されている場合はリソースグループレベル)

   SPN に必要な API レベルの権限:

   Microsoft.Graph:

- Application.Read.All
- Directory.Read.All
- ServicePrincipalEndpoint.Read.All

5. アクセス許可を検索するために必要な不足しているアクセス許可を追加した後、次のコマンドを実行して、さまざまなカテゴリのアクセス許可があるかどうかを確認します。

   例:

   より高いレベルの承認が必要なサブスクリプションレベルで接続をテストするには:

   ```
   Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\ AzureCon
   -SecurePassword $password -UserName 922e65d5-38ae-4cf5-xxxx-xxxxxxxxx
   ```

   例:

   高レベルの承認なしでリソースグループレベルで接続をテストするには:

   ```
   Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\testles
   -CustomProperties $customProperties | Format-List
   ```

   注:

   リソースグループは接続固有の情報であるため、CustomPropertiesパラメーターはリソースグループレベルを提供するために使用されます。

   例:

   リソースグループレベルでより高いレベルの認証を持つ接続をテストするには:

   ```
   Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\testles
   -SecurePassword $password -UserName
   922e65d5-38ae-4cf5-832b-54122196b7dd -CustomProperties
   $customProperties
   ```

権限については、「必要なAzure権限」を参照してください。

Azureシークレット環境でホスト接続を検証する

PowerShellコマンド`Test-HypHypervisorConnection`を使用して、Azureシークレット環境でホスト接続が必要な権限を持っているかどうかを検証できます。

ただし、検証結果を正常に取得するには、既存のホスト接続を作成または更新して、カスタムプロパティ`AuthenticationObjectId`を持つようにします。このプロパティには、ホスティング接続に関連付けられたサービスプリンシパルのオブジェクトIDが格納されます。

> **注:**
>
> Azureポータルからサービスプリンシパルのオブジェクトを取得します。アプリケーションのIDは使用しないでください。

AuthenticationObjectId を含めるようにホスト接続を作成または更新する

`New-Item` を使用してホスト接続を作成し、`AuthenticationObjectId` をカスタムプロパティとして追加します。例：

```
New-Item -ConnectionType 'Azure' -HypervisorAddress @('http://
hypervisorhost1.example.com','http://hypervisorhost2.example.com')`

    -LoggingId $loggingId -Path @('XDHyp:\\Connections\\Example') -Persist
-Scope @() `

    -Password 'Password' -UserName 'root' -CustomProperties <Property
xsi:type="StringProperty" Name="AuthenticationObjectId" Value="Object ID
of the service principal"/>
```

`Set-Item`を使用して既存のホスト接続を更新し、`AuthenticationObjectId`をカスタムプロパティとして追加します。手順は次のとおりです。

1. Remote PowerShell SDKを使用してPowerShellウィンドウを開きます。
2. 次のコマンドを実行します:

```
Add-PSSnapin citrix*.

cd XDHyp:\Connections\
```

```
dir
```

3. 接続から `CustomProperties` をメモ帳にコピーし、プロパティ設定 `<Property xsi:type="StringProperty" Name="AuthenticationObjectId" Value="Object ID of the service principal"/>` を `CustomProperties` に追加します。
4. PowerShellウィンドウで、変更されたカスタムプロパティに変数を割り当てます。
5. `$cred = Get-Credential` を実行します。プロンプトが表示されたら、接続資格情報を入力します。資格情報は Azure アプリケーション ID とシークレットです。
6. `Set-Item -PSPath XDHyp:\Connections\<Connection_Name> -CustomProperties $customProperty -username $cred.username -Securepassword $cred.password` を実行します。
7. `dir` を実行して、更新された `CustomProperties` 設定を確認します。

```
Set-Item -PSPath XDHyp:\Connections\$connName -CustomProperties
<Property xsi:type="StringProperty" Name="AuthenticationObjectId"
Value="Object ID of the service principal"/> -username $cred.username
-Securepassword $cred.password
```

権限のホスト接続を検証する

必要な役割と権限のホスト接続を検証するには、次のコマンドを実行します。

- サブスクリプションレベルで役割と権限が割り当てられている場合：

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\<Your-
HostingConnection>
```

- リソースグループレベルで役割と権限が割り当てられている場合：

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\<Your-
HostingConnection>  -CustomProperties $CustomProperties



$CustomProperties = '<CustomProperties xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance" xmlns="http://schemas.citrix.com/2014/xd/
machinecreation">'`
```

```
+ '<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="ExampleResourceGroup" />'`

+ '</CustomProperties>'
```

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Azure固有の情報については、「Microsoft Azureカタログの作成」を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

マイクロソフト システムセンター バーチャル マシン マネージャーへの接続

接続を作成するウィザードについては、(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/connections.html)を参照してください。以下の情報は、Microsoft System Center Virtual Machine Manager (VMM) に固有の詳細を説明しています。

注:

VMMへの接続を作成する前に、まずVMMアカウントをリソースの場所として設定する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/install-prepare/msscvmm.html)を参照してください。

接続を作成する

MCSを使用してVMをプロビジョニングした場合は、接続作成ウィザードで次の操作を行います。

- ホストサーバーの完全修飾ドメイン名としてアドレスを入力します。
- 以前に設定した管理者アカウントの資格情報を入力します。このアカウントには、新しいVMを作成する権限が必要です。
- ダイアログボックスで、VMの作成時に使用するクラスターまたはスタンドアロンホストを選択します。

> **重要**
>
> 単一のHyper-Vホスト展開を使用している場合でも、クラスターまたはスタンドアロンホストを参照してください。

次のステップ

- 初期展開プロセス中の場合は、(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create.html)を参照してください。
- SMB 3ファイル共有でMCSを使用してマシンカタログを作成する場合は、(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create/create-machine-catalog-mscvmm.html)を参照してください。

詳細情報

- 接続とリソース(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/connections.html)
- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create.html)

Nutanixへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報は、Nutanixに固有の詳細を扱っています。

> **注:**
>
> Nutanixへの接続を作成する前に、まず、Nutanixアカウントをリソースの場所として設定を完了する必要があります。Nutanix仮想化環境を参照してください。

Nutanix AHV Prism Centralホスト接続

Nutanix AHV Prism Centralホスト接続を作成する前に、前提条件を参照してください。

以下のいずれかの方法で接続を作成できます。

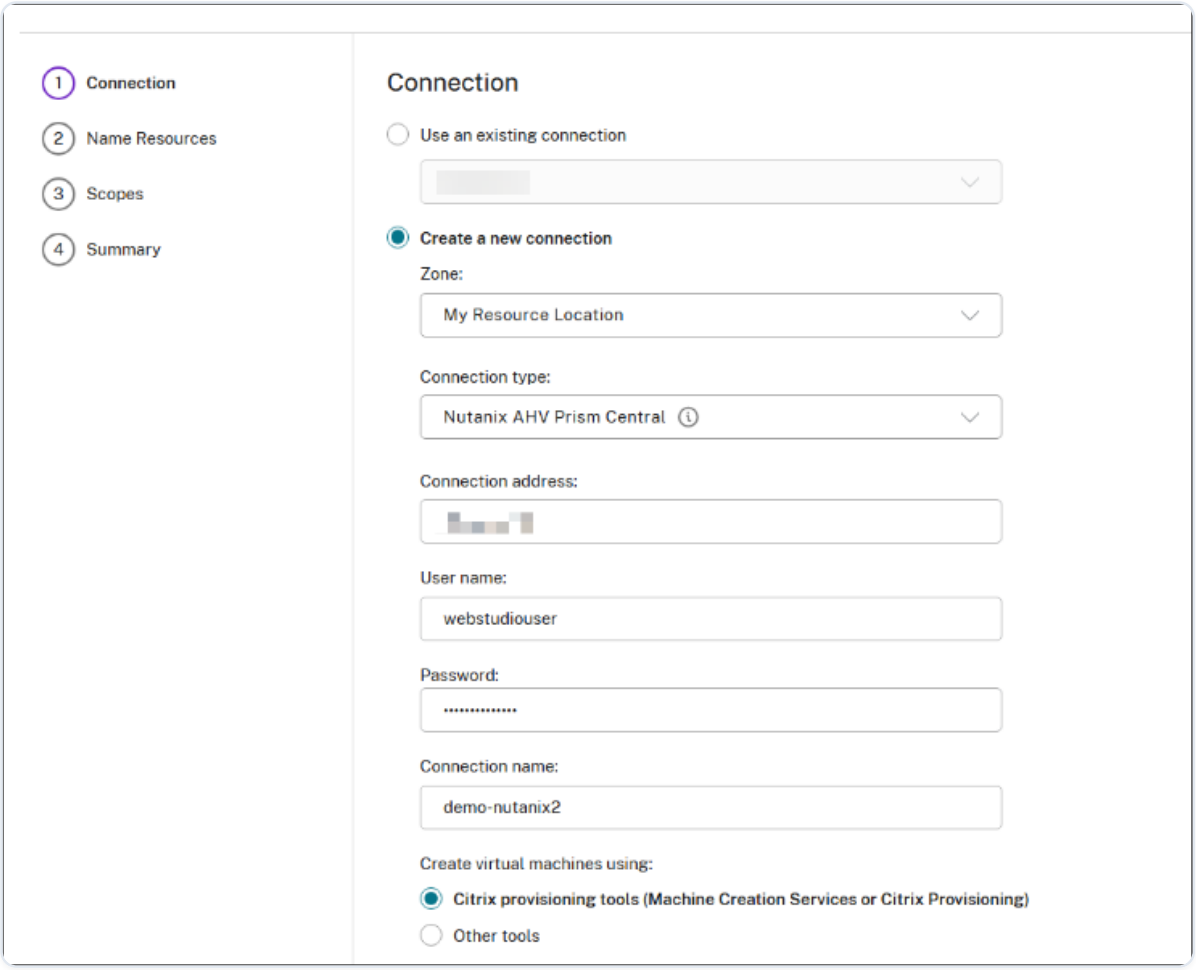
- ウェブスタジオ
- PowerShellコマンド

制限事項

- Nutanix AHV Prism Centralホスト接続は、テンプレートやネットワークなどの項目で重複するオブジェクト名をサポートしていません。カタログ作成のためにそのような項目を選択すると、予期しない動作につながる可能性があります。

Web Studio を使用して接続を作成する

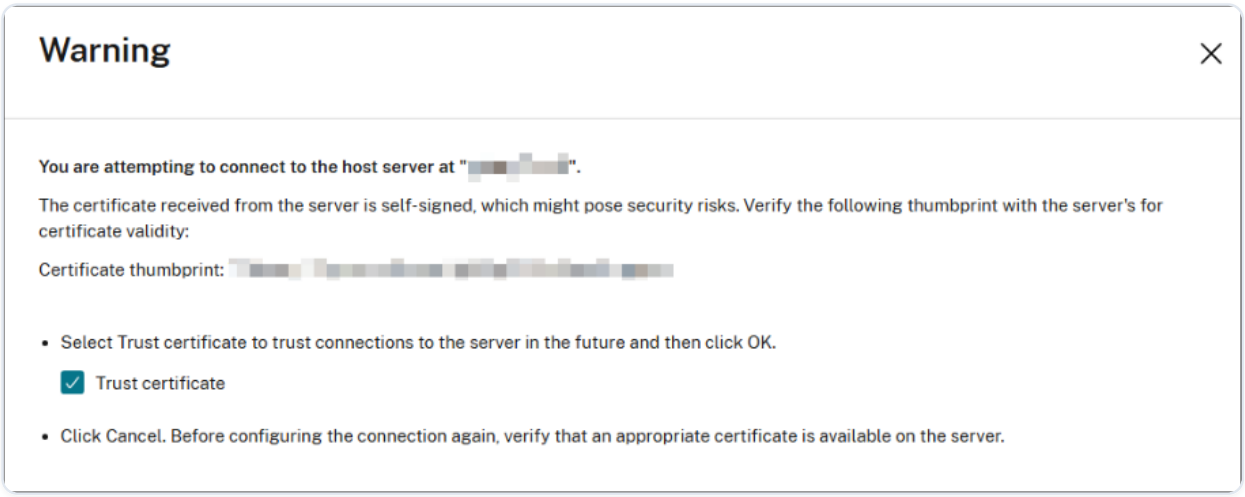
1. Citrix Cloudにサインインします。
2. **管理**をクリックします。
3. 左ペインで**ホスティング**を選択します。
4. アクションバーで**接続とリソースの追加**をクリックします。
5. **接続**ページで：
    a. **新しい接続を作成**を選択します。
    b. 接続の種類として**Nutanix AHV Prism Central**を選択します。
    c. Nutanix AHV Prism CentralのIPアドレスを接続アドレスとして入力します。
    d. 管理者資格情報とわかりやすい接続名を入力します。
    e. **Citrixプロビジョニングツール (Machine Creation Services™またはCitrix Provisioning)**を選択します。
    f. **Next**をクリックします。



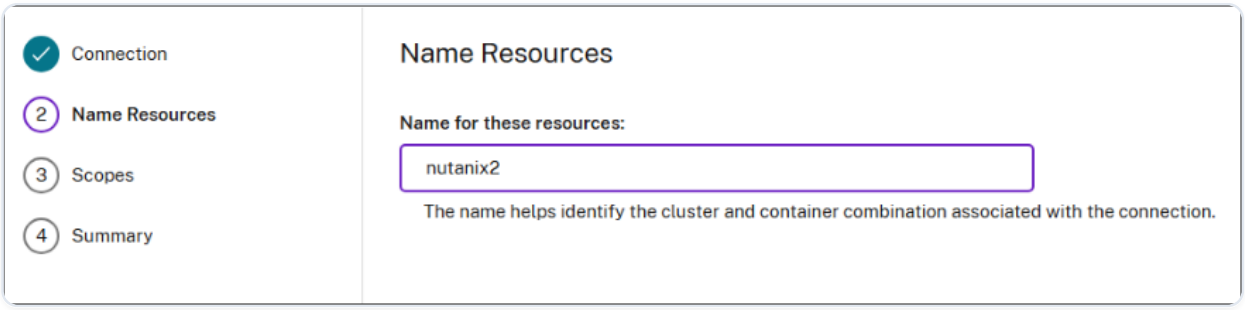
> **注：**
>
> ホスト接続の作成中、ネットワークまたはクラスターの選択は不要です。ホスティングユニット名のみが必要です。マシンカタログの作成時にネットワークとクラスターを選択します。

6. **次へ**をクリックすると、Citrix Virtual Apps and DesktopsはプライベートCA署名付き証明書を受信し、**警告**ページが表示されます。詳細については、「Nutanix Prism Centralへのセキュアな接続」を参照してください。

   受信したサムプリントをサーバーのサムプリントと比較して、証明書の有効性を確認します。有効な場合は、**証明書を信頼する**を選択し、**OK**をクリックして接続の作成を続行します。その後、Citrix Virtual Apps and Desktopsはその証明書を信頼し、将来の検証のためにサムプリントを保存します。



7. **リソースの名前**ページで、リソースの一意の名前を追加します。**次へ**をクリックします。



8. 「**スコープ**」ページで、このホストのスコープを1つ以上選択します。
9. 「**概要**」ページで、構成を確認し、「**完了**」をクリックします。

> **注:**
>
> Nutanix AHV Prism Central接続は、他の種類のNutanix接続と共存できます。

Nutanix Prism Centralへのセキュアな接続

Nutanix SSLサムプリント機能は、Nutanix Prism Centralハイパーバイザーへのホスト接続を確立する際の証明書の信頼を簡素化します。この機能により、信頼されていない証明書のサムプリントをサイトデータベースに保存できるようになり、Citrix Virtual Apps and Desktopsがハイパーバイザーを常に信頼済みとして認識するようになります。

Nutanixホスト接続を作成すると、「**警告**」ページが表示され、接続先のマシンの証明書が提示され、それを信頼するかどうかを決定できます。

PowerShellを使用して接続を作成する

1. PowerShellウィンドウを開きます。
2. `asnp citrix*`を実行します。

3. 次のパラメーターを設定します。

```
$ConnectionName = “Name of the connection”

$UserName = “Username of the account on hypervisor”

$ZoneUid =  “UID of the zone where the hosting connection will be created”

$HypervisorAddress = “The IP address of the hypervisor”

$SSLThumbprint =  “The Nutanix PC SSL thumbprint can be set using PowerShell SDK”

$connectionPath = "XDHyp:\Connections\" + $ConnectionName

$SecureUserInput = Read-Host "Enter the password for the user $($UserName)" -AsSecureString

$EncryptedUserInput = $SecureUserInput | ConvertFrom-SecureString

$SecurePass = ConvertTo-SecureString -String $EncryptedUserInput
```

4. 新しいホスティング接続の項目を作成します。例：

```
$connection = New-Item -Path @($connectionPath) -ConnectionType "Custom" -HypervisorAddress ` @($HypervisorAddress) -Persist -PluginId "AcropolisHypervisorPCFactory" -Scope @() ` -SecurePassword $SecurePass -SSLThumbprint @($SSLThumbprint) -UserName $UserName -ZoneUid ` $ZoneUid
```

5. ブローカーハイパーバイザー接続を作成します。例：

```
New-BrokerHypervisorConnection -HypHypervisorConnectionUid $connection.HypervisorConnectionUid
```

ホスティングユニットを作成する

PowerShellコマンドを使用してホスティングユニットを作成する場合、次の必須パラメーターを指定します。

- `$HostUnitName`: 作成するホスティングユニットの名前

- `ConnectionName`: 以前に作成したハイパーバイザー接続の名前

1. PowerShellウィンドウを開きます。
2. `add-pssnapin citrix*`を実行します。
3. ホスティングユニットを作成するためのPowerShellコマンドを実行します。例：

```
$hostUnitPath = "XDHyp:\HostingUnits\" + $HostUnitName

New-Item -Path @($hostUnitPath) -RootPath $connectionPath
-HypervisorConnectionName $ConnectionName -CustomProperties ""
-NetworkPath @() -StoragePath @()
```

注:

ホスト接続の作成中に、ネットワークまたはクラスターの選択は必要ありません。ホスティングユニット名のみが必要です。マシンカタログの作成中にネットワークとクラスターを選択してください。

ホスト接続の管理

既存のホスト接続は、以下を使用して管理できます。

- ウェブスタジオ
- PowerShell

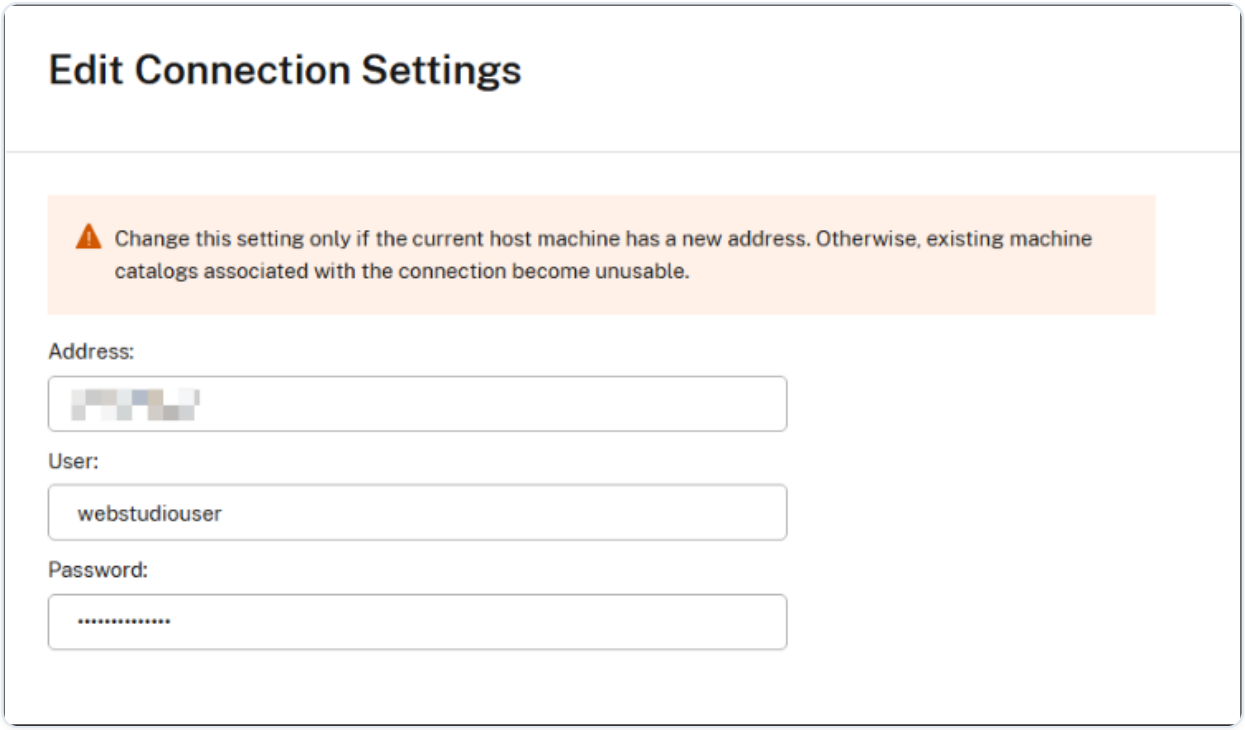
WEB STUDIO を使用してホスト接続を管理する

ホスト接続を作成したら、Web Studioの**ホスティング**ノードに移動し、接続を右クリックして次の操作を行います。

- **接続の削除**
- **接続の名前を変更**
- **接続の編集**
- **メンテナンスモードをオンにする**
- **マシンを表示**
- **接続のテスト**
- **TLS証明書の信頼をテスト**

WEB STUDIO を使用して接続を編集する

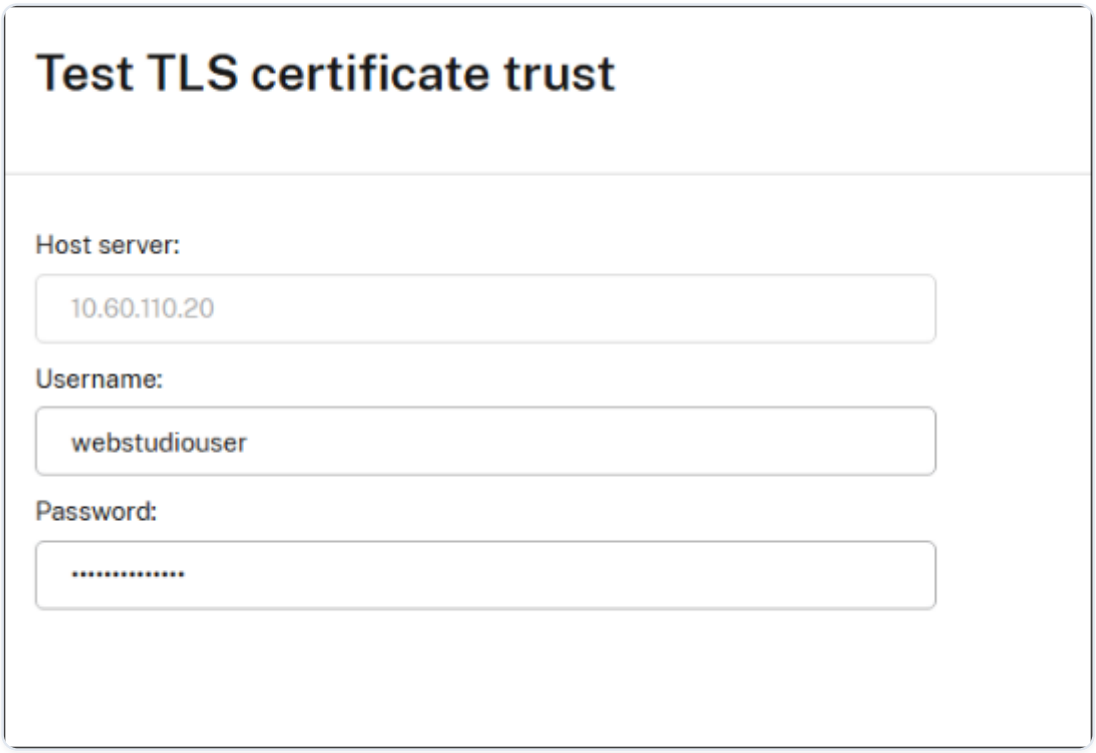
1. 接続を右クリックし、**接続の編集**をクリックします。
2. **接続プロパティ**ページで、**設定の編集**をクリックします。
3. **接続設定の編集**ページで、証明書情報を変更し、**保存**をクリックします。



4. 新しい証明書のサムプリントを信頼するには、**警告**ページで**証明書を信頼する**を選択します。

TLS 証明書の信頼をテストする

1. 接続を右クリックし、**TLS証明書の信頼をテスト**をクリックします。
2. **TLS証明書の信頼をテスト**ページで、証明書情報を変更し、**テスト**をクリックします。



テスト結果が成功しなかった場合は、Web Studio を使用した接続の編集 を使用して、接続の証明書情報を変更します。

POWERSHELL を使用したホスト接続の管理

PowerShell コマンドを使用して、次のことができます。

- ホスト接続のユーザー資格情報を変更または更新する。例:

```
$UserName = "Username of the account on hypervisor"

$SecureUserInput = Read-Host "Enter the password for the user $
($UserName)" -AsSecureString

$EncryptedUserInput = $SecureUserInput | ConvertFrom-SecureString

$SecurePass = ConvertTo-SecureString -String $EncryptedUserInput

Set-Item  -LiteralPath @("XDHyp:\Connections\<Host connection name>")
 -SecurePassword $SecurePass -UserName $UserName
```

- SSLThumbprint をリセットする。例:

```
$SSLThumbprint =  "The Nutanix PC SSL thumbprint value"

Set-Item  -LiteralPath @("XDHyp:\Connections\<Host connection name>")
```

```
 -SecurePassword $SecurePass -UserName $UserName -SSLThumbprint
$SSLThumbprint
```

必要な権限

Nutanix AHV Prism Central ホスト接続に使用される管理アカウントには、次の権限が必要です。

ホスト接続の作成

クラスター:

- クラスターの表示

VM の電源管理

AHV VM:

- ACPI 仮想マシンのシャットダウン
- ACPI 仮想マシンの再起動
- ゲスト仮想マシンの再起動
- ゲスト仮想マシンのシャットダウン
- 仮想マシンの電源オフ
- 仮想マシンの電源オン
- 仮想マシンのリセット
- 既存の仮想マシンの表示

クラスター:

- クラスターの表示

サブネット:

- サブネットの表示

VMのプロビジョニング

AHV VM:

- ACPI仮想マシンの再起動
- ACPI仮想マシンのシャットダウン
- 仮想マシンカテゴリの関連付け
- 新しい仮想マシンの作成
- 仮想マシンの作成

- 仮想マシンディスクの作成
- 仮想マシンNICの作成
- 既存の仮想マシンの削除
- 仮想マシンの削除
- 仮想マシンディスクの削除
- 仮想マシンGPUの削除
- 仮想マシンNICの削除
- 仮想マシンカテゴリの関連付け解除
- 仮想マシンCD-ROMの取り出し
- ゲスト仮想マシンの再起動
- ゲスト仮想マシンのシャットダウン
- 仮想マシンの電源オフ
- 仮想マシンの電源オン
- 仮想マシンのリセット
- 仮想マシンのスナップショット
- 仮想マシンの基本構成の更新
- 仮想マシンディスクの更新
- 仮想マシンディスクリストの更新
- 仮想マシンNICの更新
- 既存の仮想マシンの表示
- 仮想マシンの表示
- 仮想マシンCD-ROMの表示
- 仮想マシンディスクの表示
- 仮想マシンGPUの表示
- 仮想マシンNICの表示

AHV VMリカバリポイント:

- AHV VMリカバリポイントの表示

カテゴリ:

- カテゴリの表示

クラスター:

- クラスターの表示

ホスト:

- ホストの表示

イメージ:

- イメージの作成
- イメージの削除
- イメージの更新
- イメージの表示

リカバリポイント:

- リカバリポイントの作成
- リカバリポイントの削除
- リカバリポイントのレプリケート
- リカバリポイントの復元
- リカバリポイントの表示
- 仮想マシンリカバリポイントの表示

ストレージコンテナ:

- ストレージコンテナの表示
- ストレージコンテナデータストアの表示
- ストレージコンテナ統計の表示

ストレージポリシー:

- ストレージポリシーの表示

サブネット:

- サブネットの表示
- サブネットvNICの表示

タスク:

- タスクのキャンセル
- タスクの表示

VMリカバリポイント:

- VMリカバリポイントを削除
- VMリカバリポイントを復元
- VMリカバリポイントを表示

VMテンプレート:

- VMテンプレートを表示
- VMテンプレートのバージョンを表示
- VMテンプレートを展開

ボリュームグループ:

- ボリュームグループをAHV VMにアタッチ
- ボリュームグループをAHV VMからデタッチ
- ボリュームグループの表示
- ボリュームグループ詳細の表示

VPC:

- VPCを表示

Nutanix AHV、Nutanix AHV PC、またはNutanix AHV DRaaSホスト接続

1. Citrix Cloudにサインインします。
2. 「**管理**」をクリックします。
3. 左側のペインで を選択します。
4. アクションバーで をクリックします。
5. ページで、次の接続タイプを選択できます。

    - **Nutanix AHV**: Prism Element (PE) クラスターのアドレス、資格情報、および接続の名前を指定します。 ページで、ネットワークを選択し、ホスティングユニットの名前を指定します。

        > **注:**

> Nutanix AHV (Prism Element) をリソースとして使用してマシンを展開する場合、VM のディスクが格納されているコンテナを選択します。

- **Nutanix AHV PC**: Prism Central (PC) のアドレス、資格情報、および接続の名前を指定します。 ページで、リストからネットワーク、クラスターを選択し、ホスティングユニットの名前を指定します。

> **注:**
>
> 接続タイプ**Nutanix AHV PC**は、Azure 上の Nutanix Cloud Cluster (NC2) への接続を作成する場合にのみ使用されます。また、マシンカタログは、Azure 接続上の NC2 内の単一クラスターでのみホストできます。このタイプの接続には、Cloud Connector に Nutanix プラグインがインストールされている必要があります。

- **Nutanix AHV DRaaS**: アドレスとユーザー名を指定し、Nutanix DRaaS 資格情報ファイルに含まれる公開鍵と秘密鍵をインポートします (`.pem`)。(公開鍵と秘密鍵は、Nutanix DRaaS 管理者によって Nutanix DRaaS クラウドで生成されます。)
  - キーをインポートするには、資格情報ファイルを見つけてメモ帳 (または任意のテキストエディター) で開き、内容をコピーします。その後、**接続**ページに戻り、**キーのインポート**を選択し、内容を貼り付けて、**保存**を選択します。資格情報の内容や形式を変更しないでください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Nutanix固有の情報については、「Nutanixカタログの作成」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- Nutanix仮想化環境
- Nutanixクラウドおよびパートナーソリューション

Nutanix クラウドおよびパートナーソリューションへの接続

接続を作成するウィザードについては、接続とリソースの作成および管理を参照してください。以下の情報では、Nutanix クラウドおよびパートナーソリューションに固有の詳細について説明します。

Nutanix AHV Prism Central (ニュータニックス AHV プリズムセントラル)

Citrix Virtual Apps and Desktops は、Citrix が管理する Nutanix AHV Prism Central プラグイン向けに、以下のクラウドハイパーバイザーで Nutanix Cloud Clusters (NC2) をサポートしています。

- AWS
- Microsoft Azure (マイクロソフト アジュール)

> **注:**
>
> - AWS および Azure 上の NC2 への接続を作成する前に、クラウドプラットフォームでリソースを準備してください。Nutanix クラウドおよびパートナーソリューションを参照してください。
> - ホスティング接続の作成、VM の電源管理、およびカタログのプロビジョニングに必要な権限については、必要な権限を参照してください。

Azure および AWS 上の NC2 に接続する

Azure または AWS 上の Nutanix Cloud Cluster (NC2) に接続するには、展開済みの Prism Central インスタンスへのアクセスと、Prism Admin ロールを持つ資格情報が必要です。

ホスト接続は、以下を使用して作成できます。

- ウェブスタジオ
- PowerShell

接続に関する完全な情報については、Nutanix AHV Prism Central への接続を参照してください。

ニュータニックス プリズムエレメント

Citrix Virtual Apps and Desktops は、Nutanix Prism Element プラグイン向けに、以下のクラウドハイパーバイザーで Nutanix Cloud Clusters (NC2) をサポートしています。

- AWS

Nutanix Prism に接続する

Nutanix クラスターを作成した後、Nutanix Prism に接続します。 Nutanix Prism に接続するには：

1. 10.0.129.0/24 サブネットにバスティオン VM を作成します。
2. バスティオン VM に RDP 接続し、前のセクションでコピーした **Prism Element** の URL にアクセスします。
3. デフォルトの資格情報を使用してログインします: `admin:nutanix/4u`。パスワードを変更することを忘れないでください。

Nutanix クラスター上に VM を作成する

Nutanix Prism に接続した後、Nutanix クラスター上に VM を作成します。

VM がインターネットアクセスを必要とする場合

1. AWS コンソールに移動します。
2. Nutanix CFS によって作成されたものと同じ VPC 内に、新しいサブネット 10.0.130.0/24 を作成します。
3. このサブネットのルートテーブルにルートを追加し、すべての非ローカルトラフィックを上記の NAT ゲートウェイに転送します。
4. バスティオン VM に RDP 接続し、前のセクションでコピーした **Prism Element** の URL にアクセスしてログインします。
5. 新しいネットワークを追加します。**「Settings」>「Network Configuration」>「Create Subnet」**に移動します。AWSで使用されているものと同じサブネット10.0.130.0/24を使用します。
6. その新しいサブネット内にすべてのVM（AD、CC、VDAなど）を作成します。

VMにインターネットアクセスが不要な場合

1. 踏み台VMにRDP接続し、前のセクションでコピーした**Prism Element**のURLにアクセスしてログインします。
2. 新しいネットワークを追加します。**「Settings」>「Network Configuration」>「Create Subnet」**に移動します。サブネット10.0.129.0/24を使用します。
3. そのサブネット内にすべてのVM（AD、CC、VDAなど）を作成します。

> ヒント：

> VM の時刻とタイムゾーン情報が正しく設定されていることを確認してください。これは特に AD に当てはまります。

ホスト接続を作成する

1. Web Studioから、左ペインで**「Hosting」**を選択します。
2. **「Add Connection and Resources」**をクリックします。
3. **「Connection」画面で、「Create a new Connection」を選択し、「Connection address」**に`https://xxx.xxx.xxx.xxx:9440`を入力します。
4. UIに従ってウィザードを完了します。

> **注：**
>
> Nutanixゾーンでプラグインが使用されていない場合でも、Web StudioでNutanixオプションを利用できるようにするには、すべてのコネクタVMにNutanixプラグインがインストールされている必要があります。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Nutanix 固有の情報については、「Nutanix カタログの作成」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create/create-machine-catalog-nutanix.html)

詳細情報

- 接続とリソース
- Nutanix仮想化環境
- Nutanixクラウドおよびパートナーソリューション

Red Hat OpenShiftへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明します。以下の情報は、Red Hat OpenShiftに固有の詳細を扱っています。

> **注:**

> Red Hat OpenShiftへの接続を作成する前に、まずRed Hat OpenShiftのセットアップを完了する必要があります。「Red Hat OpenShift仮想化環境」(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/install-prepare/red-hat-open-shift.html)を参照してください。

接続を作成する

Red Hat OpenShiftクラスターへの接続は、以下を使用して作成できます。

- ウェブスタジオ
- PowerShell

Web Studioを使用して接続を作成する

1. Web Studioで、 > を開きます。
2. ページで、以下の手順に従って接続を構成します。
    a. を選択します。
    b. 接続の種類として を選択します。
    c. フィールドに、OpenShiftサーバーのIPアドレス、ホスト名、またはFQDNを入力します。
    d. サービスアカウントトークンと、わかりやすい接続名を入力します。
    e. **ゾーン名**フィールドでゾーンを選択します。オプションは、構成したすべてのリソースの場所です。
    f. 仮想マシンを作成するために、**その他のツール**を選択します。

    > **注:**
    >
    > 「**その他のツール**」を選択すると、ホスティングユニットなしでホスティング接続のみが作成されます。

3. **次へ**をクリックします。
4. 自己署名証明書が検出された場合、証明書のサムプリントが表示された警告ページが表示されます。続行するには:
    a. サムプリントをサーバーのものと比較して、証明書の有効性を確認します。
    b. 有効な場合は、「**証明書を信頼する**」を選択し、「**OK**」をクリックして接続設定を完了します。

証明書は信頼済みとしてマークされ、サムプリントは将来の検証のために保存されます。

5. **スコープ**ページで、このホストに対して1つ以上のスコープを選択します。
6. **概要**ページで、構成を確認し、**完了**をクリックします。

PowerShellコマンドを使用して接続を作成する

PowerShellコマンドを使用して接続を作成する場合、次の情報を提供します:

- ホスティング接続名
- クラスターAPIアドレス
- ユーザー名
- パスワード（サービスアカウントトークン）
- SSLサムプリント: これはCA証明書のサムプリントであり、APIサーバーのサムプリントではありません。サムプリントを指定せずにホスティング接続を作成しようとすると、サーバーがCA証明書のサムプリントを提供します。
- ゾーンUID

1. PowerShellウィンドウを開きます。
2. `add-pssnapin citrix®*`を実行します。
3. ホスティング接続を作成するには、次のコマンドを実行します。

   サムプリントを指定せずにホスティング接続を作成しようとすると、サーバーがCA証明書のサムプリントを提供します。例:

```
$newItemParameters = @{

ConnectionType= "Custom"

PluginId= "OpenShiftPluginFactory"

HypervisorAddress = "https://
api.myopenshiftclusteraddress.mydomain.local:6443"

Path= "XDHyp:\Connections\OpenShiftConnectionName"

Persist= $true

UserName= "__ServiceAccount__"
```

```
Password= "<service account token>"

ErrorVariable= "connectionError"

 }



& New-Item @newItemParameters




$newItemParameters["SSLThumbprint"] =
$connectionError[0].ErrorData.Thumbprint

$connection = & New-Item @newItemParameters

$brokerConnection = New-BrokerHypervisorConnection
-HypHypervisorConnectionUid $connection.HypervisorConnectionUid
```

ホスティングユニットを作成する

ホスティングユニットは、VMが作成される環境を表します。ホスティングユニットを作成するには、OpenShiftから次の入力が必要です。

- 名前空間
- ストレージクラス
- ネットワークアタッチメント定義

ホスティングユニットは名前空間にバインドされています。これは、1つのホスティングユニットが1つの名前空間のみにアクセスでき、その名前空間下のVMを管理することを意味します。

ホスティングユニットは、以下を使用して作成できます。

- ウェブスタジオ
- PowerShell

Web Studio を使用してホスティングユニットを作成する

1. **ホスティング > 接続とリソースの追加** に移動します。

2. **接続** ページで:

   - ホスティングユニットとともに新しいホスティング接続を作成するには、**新しい接続の作成** を選択し、次の操作を行います:

     a. 接続の種類として **Red Hat OpenShift** を選択します。

     b. **接続アドレス** フィールドに、OpenShift Server の IP アドレス、ホスト名、または FQDN を入力します。

     c. サービスアカウントトークンとわかりやすい接続名を入力します。

     d. **ゾーン名** フィールドでゾーンを選択します。オプションは、構成したすべてのリソースの場所です。

     e. 仮想マシンを作成するための **Citrix プロビジョニングツール (Machine Creation Services™ または Citrix Provisioning)** を選択します。

     f. **次へ** をクリックします。

     g. **警告** ページで、証明書の有効性を確認し、**証明書を信頼する** を選択します。

   - 既存のホスト接続からホスティングユニットを作成するには、**既存の接続を使用** を選択し、関連する接続を選択します。

3. **名前空間の選択** ページで、この接続の名前空間を選択します。
4. 「**ストレージの選択**」ページで、ウィザードの次のページに進む前に、サポートされているデータタイプごとに少なくとも1つのストレージデバイスを選択します。ストレージの選択の詳細については、「ホストストレージ」を参照してください。
5. 「**ネットワーク**」ページで、リソースの名前を入力します。この名前は、接続に関連付けられたストレージとネットワークの組み合わせを識別するためにStudioに表示されます。VMが使用するネットワークを1つ以上選択します。
6. 「**概要**」ページで、詳細を確認し、「**完了**」をクリックします。

PowerShell を使用してホスティングユニットを作成する

PowerShell コマンドを使用してホスティングユニットを作成する場合、以下の情報を提供します。

- ホスティング接続名
- ホスティングユニット名
- ターゲットの名前空間名
- StorageClasses 名

- NetworkAttachmentDefinition 名

1. PowerShell ウィンドウを開きます。
2. `add-pssnapin citrix*` を実行します。
3. ホスティングユニットを作成するために PowerShell コマンドを実行します。例:

```
$HostingConnectionName = "OpenShiftConnectionName"

$HostingUnitName = "HostingUnitName"

$TargetNamespace = "TargetNamespaceName"

$StorageClassToUse = "YourStorageClassesName"

$NetworkAttachmentDefinition = "YourNetworkAttachmentDefinitionName"

New-HypStorage `

-StoragePath @("XDHyp:\Connections\$HostingConnectionName\
$TargetNamespace.namespace\$StorageClassToUse.storage") `

-StorageType "TemporaryStorage"

New-Item `

-CustomProperties "" `

-HypervisorConnectionName $HostingConnectionName `

-NetworkPath @("XDHyp:\Connections\$HostingConnectionName\
$TargetNamespace.namespace\$NetworkAttachmentDefinition.network") `

-Path @("XDHyp:\HostingUnits\$HostingUnitName") -RootPath "XDHyp:
\Connections\$HostingConnectionName\$TargetNamespace.namespace" `

-StoragePath @("XDHyp:\Connections\$HostingConnectionName\
$TargetNamespace.namespace\$StorageClassToUse.storage")
```

次の手順

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。

- Red Hat OpenShift固有の情報については、Red Hat OpenShiftカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

VMwareへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報は、VMware仮想化環境に固有の詳細を扱っています。

> **注:**
>
> VMwareへの接続を作成する前に、まずVMwareアカウントをリソースの場所として設定する必要があります。VMware仮想化環境を参照してください。

接続を作成する

接続作成ウィザードで：

1. VMware接続タイプを選択します。
2. vCenter SDKのアクセスポイントのアドレスを指定します。
3. 以前に設定した、VMを作成する権限を持つVMwareユーザーアカウントの資格情報を指定します。ユーザー名は「ドメイン/ユーザー名」の形式で指定します。

VMware SSLサムプリント

VMware SSLサムプリント機能により、VMware vSphereハイパーバイザーへのホスト接続を手動で作成する必要がなくなります。接続を作成する前に、サイト内のDelivery Controllerとハイパーバイザーの証明書との間に信頼関係を手動で作成する必要はなくなりました。

VMware SSLサムプリント機能は、信頼されていない証明書のサムプリントをサイトデータベースに保存します。この構成により、ハイパーバイザーがコントローラーによって信頼されていなくても、Citrix Virtual Apps and Desktops™によって継続的に信頼されていると識別されることが保証されます。

StudioでvSphereホスト接続を作成する際、ダイアログボックスが表示され、接続先のマシンの証明書を表示できます。その後、それを信頼するかどうかを選択できます。

必要な権限

VMwareユーザーアカウントと、この記事に記載されている権限の一部またはすべてを持つ1つ以上のVMwareロールを作成します。ロールの作成は、ユーザーがいつでもさまざまなCitrix DaaS™操作を要求するために必要な権限の特定の粒度レベルに基づいて行います。ユーザー固有の権限をいつでも付与するには、**子に伝播**オプションを選択した状態で、データセンターレベルで、それぞれのロールに関連付けます。ただし、`StorageProfile`権限と特定の`Tags`権限については、**子に伝播**なしで、ルートvCenter Serverレベルで権限を適用します。各テーブルの注記を参照してください。

以下の表は、Citrix Virtual Apps™ および Desktops の操作と、VMware の最小限必要な権限との間のマッピングを示しています。

> **注:**
>
> 権限リストの表示名、特に *ユーザーインターフェイス* は、一部の vSphere バージョンで異なります。たとえば、vSphere 6.7 では、*ユーザーインターフェイス* 権限は、このページに記載されている必要な権限で説明されている **設定** および **メモリ** ではなく、**メモリの変更** および **設定の変更** です。

接続とリソースを追加する

SDK	ユーザーインターフェイス
システム. Anonymous、システム. Read、および システム. View	自動的に追加されます。組み込みの読み取り専用ロールを使用できます。

電源管理

SDK	ユーザーインターフェイス
VirtualMachine.Interact.PowerOff	仮想マシン > インタラクション > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > インタラクション > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > インタラクション > リセット
VirtualMachine.Interact.Suspend	仮想マシン > インタラクション > サスペンド
Datastore.Browse	Datastore > データストアの参照

マシンのプロビジョニング (Machine Creation Services™)

MCS を使用してマシンをプロビジョニングするには、次の権限が必要です。

SDK	ユーザーインターフェース
Datastore.AllocateSpace	データストア > スペースの割り当て
Datastore.Browse	データストア > データストアの参照
Datastore.FileManagement	データストア > 低レベルファイル操作
Network.Assign	ネットワーク > ネットワークの割り当て
Resource.AssignVMToPool	リソース > 仮想マシンをリソースプールに割り当て
VirtualMachine.Config.AddExistingDisk	仮想マシン > 構成 > 既存ディスクの追加
VirtualMachine.Config.AddNewDisk	仮想マシン > 構成 > 新規ディスクの追加
仮想マシン.構成.デバイスの追加または削除	仮想マシン > 構成 > デバイスの追加または削除
VirtualMachine.Config.AdvancedConfig	仮想マシン > 構成 > 詳細
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Config.CPUCount	仮想マシン > 構成 > CPU数変更
VirtualMachine.Config.Memory	仮想マシン > 構成 > メモリ変更
VirtualMachine.Config.Settings	仮想マシン > 構成 > 設定変更
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > 操作 > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > 操作 > リセット
VirtualMachine.Interact.Suspend	仮想マシン > 操作 > サスペンド
VirtualMachine.Inventory.CreateFromExisting	仮想マシン > インベントリ > 既存から作成
VirtualMachine.Inventory.Create	仮想マシン > インベントリ > 新規作成

SDK	ユーザーインターフェース
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除
VirtualMachine.Provisioning.Clone	仮想マシン > プロビジョニング > 仮想マシンのクローン作成
VirtualMachine.State.CreateSnapshot	vSphere 5.0 Update 2、vSphere 5.1 Update 1、およびvSphere 6.x Update 1: 仮想マシン > 状態 > スナップショットの作成。vSphere 5.5: 仮想マシン > スナップショット管理 > スナップショットの作成
VirtualMachine.Config.Rename	仮想マシン > 構成 > 名前の変更

イメージの更新とロールバック

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	データストア > スペースの割り当て
Datastore.Browse	データストア > データストアの参照
Datastore.FileManagement	データストア > 低レベルファイル操作
Network.Assign	ネットワーク > ネットワークの割り当て
Resource.AssignVMToPool	リソース > 仮想マシンをリソースプールに割り当てる
VirtualMachine.Config.AddExistingDisk	仮想マシン > 構成 > 既存のディスクを追加
VirtualMachine.Config.AddNewDisk	仮想マシン > 構成 > 新しいディスクを追加
VirtualMachine.Config.AdvancedConfig	仮想マシン > 構成 > 詳細設定
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > 操作 > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > 操作 > リセット

SDK	ユーザーインターフェイス
VirtualMachine.Inventory.CreateFromExisting	仮想マシン > インベントリ > 既存から作成
VirtualMachine.Inventory.Create	仮想マシン > インベントリ > 新規作成
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除
VirtualMachine.Provisioning.Clone	仮想マシン > プロビジョニング > 仮想マシンのクローン作成

準備されたイメージを共有する

異なるホスティング接続間で準備されたイメージを共有するには、ターゲットホスティング接続に次の権限が必要です。

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	データストア > スペースの割り当て
Network.Assign	ネットワーク > ネットワークの割り当て
Resource.AssignVMToPool	リソース > 仮想マシンをリソースプールに割り当てる
VirtualMachine.Config.デバイスの追加または削除	仮想マシン > 構成 > デバイスの追加または削除
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Config.Settings	仮想マシン > 構成 > 設定の変更
VirtualMachine.Inventory.Register	仮想マシン > インベントリ > 登録
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除

プロビジョニングされたマシンの削除

SDK	ユーザーインターフェイス
Datastore.Browse	データストア > データストアの参照
Datastore.FileManagement	Datastore > 低レベルファイル操作

SDK	ユーザーインターフェイス
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除

ストレージプロファイル

vSANまたはvVolデータストア上でカタログ作成中にストレージポリシーを表示、作成、または削除するには、次の権限が必要です。

SDK	ユーザーインターフェイス
StorageProfile.Update	プロファイル駆動型ストレージ > プロファイル駆動型ストレージの更新。vSphere 8の場合: VMストレージポリシー > VMストレージポリシーの更新
StorageProfile.View	プロファイル駆動型ストレージ > プロファイル駆動型ストレージの表示。vSphere 8の場合: VMストレージポリシー > VMストレージポリシーの表示

注:

ストレージプロファイルの権限は、**子への伝播**なしで、ルートvCenter Serverレベルで適用してください。

タグとカスタム属性

タグとカスタム属性を使用すると、vSphereインベントリで作成されたVMにメタデータを添付でき、これらのオブジェクトの検索とフィルタリングが容易になります。タグまたはカテゴリを作成、編集、割り当て、削除するには、次の権限が必須です。

SDK	ユーザーインターフェイス
InventoryService.Tagging.CreateTag	vSphereタグ付け > vSphereタグの作成

SDK	ユーザーインターフェイス
InventoryService.Tagging.CreateCategory	vSphereタグ付け > vSphereタグカテゴリの作成
InventoryService.Tagging.EditTag	vSphereタグ付け > vSphereタグの編集
InventoryService.Tagging.EditCategory	vSphereタグ付け > vSphereタグカテゴリの編集
InventoryService.Tagging.DeleteTag	vSphereタグ付け > vSphereタグの削除
InventoryService.Tagging.DeleteCategory	vSphereタグ付け > vSphereタグカテゴリの削除
InventoryService.Tagging.AttachTag	vSphere タグ付け > vSphere タグの割り当てまたは割り当て解除
InventoryService.Tagging.ObjectAttachable	vSphere タグ付け > オブジェクトへの vSphere タグの割り当てまたは割り当て解除
Global.ManageCustomFields	グローバル > カスタム属性の管理
Global.SetCustomField	グローバル > カスタム属性の設定

注：

- MCS がマシンカタログを作成すると、ターゲット VM に特別な名前タグが付けられます。これらのタグは、マスターイメージと MCS で作成された VM を区別し、MCS で作成された VM がイメージ準備に使用されるのを防ぎます。vCenter の `XdProvisioned` 属性の値によって違いを識別できます。MCS が VM を作成した場合、この属性は **True** に設定されます。
- `InventoryService.Tagging.AttachTag` 権限を、**子に伝播**せずに、ルート vCenter Server レベルで適用します。

暗号化操作

暗号化操作の権限は、誰がどの種類のオブジェクトに対してどの種類の暗号化操作を実行できるかを制御します。vSphere Native Key Provider は `Cryptographer.*` 権限を使用します。暗号化操作には、以下の最小限の権限が必要です。

注：

これらの権限は、vTPM を搭載した VM を使用して MCS マシンカタログを作成するために必要です。

SDK	ユーザーインターフェイス
Cryptographer.Access	特権 > すべての特権 > 暗号化操作 > 直接アクセス
Cryptographer.AddDisk	特権 > すべての特権 > 暗号化操作 > ディスクの追加
Cryptographer.Clone	特権 > すべての特権 > 暗号化操作 > クローン
Cryptographer.Encrypt	特権 > すべての特権 > 暗号化操作 > 暗号化
Cryptographer.EncryptNew	特権 > すべての特権 > 暗号化操作 > 新規暗号化
Cryptographer.Decrypt	特権 > すべての特権 > 暗号化操作 > 復号化
Cryptographer.Migrate	権限 > すべての権限 > 暗号化操作 > 移行
Cryptographer.ReadKeyServersInfo	権限 > すべての権限 > 暗号化操作 > KMS情報の読み取り

マシンのプロビジョニング (Citrix Provisioning™)

テンプレートをクローンして展開するためのこれらの権限は、Citrix Virtual Apps and Desktops セットアップウィザードおよびCitrix Provisioningコンソールを介したデバイスのエクスポートウィザードを使用してVMをプロビジョニングするために必要です。ホスティング接続の作成時に権限を設定します。マシンのプロビジョニング (Machine Creation Services) からのすべての権限と、以下の権限が必要です。

SDK	ユーザーインターフェイス
VirtualMachine.Config.AddRemoveDevice	仮想マシン > 構成 > デバイスの追加または削除
VirtualMachine.Config.CPUCount	仮想マシン > 構成 > CPU数の変更
VirtualMachine.Config.Memory	仮想マシン > 構成 > メモリ
VirtualMachine.Config.Settings	仮想マシン > 構成 > 設定
VirtualMachine.Provisioning.CloneTemplate	仮想マシン > プロビジョニング > テンプレートのクローン作成
VirtualMachine.Provisioning.DeployTemplate	仮想マシン > プロビジョニング > テンプレートの展開
VApp.Export	vApp > エクスポート

> **注:**
>
> `VApp.Export` は、マシンプロファイルを使用してMCSマシンカタログを作成するために必要です。

証明書を取得してインポートする

vSphere通信を保護するため、Citrix®はHTTPではなくHTTPSを使用することを推奨します。

HTTPSにはデジタル証明書が必要です。組織のセキュリティポリシーに準拠した認証局から発行されたデジタル証明書を使用してください。

認証局から発行されたデジタル証明書を使用できない場合は、VMwareがインストールした自己署名証明書を使用できます。この方法は、組織のセキュリティポリシーで許可されている場合にのみ使用してください。VMware vCenter証明書を各Delivery Controllerに追加します。

1. vCenter Serverを実行しているコンピューターの完全修飾ドメイン名 (FQDN) を、そのサーバーのホストファイル内の `%SystemRoot%/WINDOWS/system32/Drivers/etc/` に追加します。この手順は、vCenter Serverを実行しているコンピューターのFQDNがドメインネームシステムにまだ存在しない場合にのみ必要です。
2. 以下の3つの方法のいずれかを使用してvCenter証明書を取得します。

vCenterサーバーから。

a. vCenterサーバーからrui.crtファイルをDelivery Controllersでアクセス可能な場所にコピーします。

b. Controllerで、エクスポートされた証明書の場所に移動し、rui.crtファイルを開きます。

Web ブラウザーを使用して証明書をダウンロードします。 Internet Explorer を使用している場合は、Internet Explorer を右クリックし、**管理者として実行**を選択して証明書をダウンロードまたはインストールします。

a. Webブラウザを開き、vCenterサーバーへの安全なWeb接続を行います（例: `<https://server1.domain1.com)>`）。

b. セキュリティ警告を受け入れます。

c. 証明書エラーが表示されているアドレスバーをクリックします。

d. 証明書を表示し、 タブをクリックします。

e. プロンプトが表示されたら名前を指定して、**ファイルにコピーして .CER 形式でエクスポート**を選択します。

f. エクスポートされた証明書を保存します。

g. エクスポートされた証明書の場所に移動し、.CER ファイルを開きます。

管理者として実行している Internet Explorer から直接インポートします。

- Webブラウザを開き、vCenterサーバーへの安全なWeb接続を行います（例: `<https://server1.domain1.com)>`）。
- セキュリティ警告を受け入れます。
- 証明書エラーが表示されているアドレスバーをクリックします。
- 証明書を表示します。

3. 各Controllerの証明書ストアに証明書をインポートします。

a. **証明書のインストール**オプションをクリックし、**ローカルコンピューター**を選択して、**次へ**をクリックします。

b. **証明書をすべて次のストアに配置する**を選択し、**参照**をクリックします。**信頼されたユーザー**を選択し、**OK**をクリックします。**次へ**をクリックし、**完了**をクリックします。

インストール後にvSphereサーバーの名前を変更した場合は、新しい証明書をインポートする前に、そのサーバーで新しい自己署名証明書を生成する必要があります。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- VMware固有の情報については、「VMwareカタログの作成」を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

マシンID管理用サービスアカウント

サービスアカウントは、保存された資格情報のコンテナであり、ユーザーの操作なしで(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-identities)関連の操作を実行するように構成され、使用されます。マシンID管理の権限を必要とする操作の前に、サービスアカウントを作成してください。

MCSマシンカタログを構成して、サービスアカウントを次の目的で使用できます。

- Active Directoryでコンピューターアカウントを作成または削除する際に、毎回ドメイン資格情報を入力する必要がありません。
- 古いMicrosoft Entra参加済みまたはMicrosoft Intune登録済みデバイスを、Microsoft Entra IDまたはIntuneポータルを介して手動で削除することなく管理します。

サポートされているサービスアカウントの種類

Citrix®では、IDプロバイダーの種類に基づいて次のサービスアカウントの作成が可能です。

IDプロバイダーの種類	説明	資格情報
オンプレミスActive Directoryサービスアカウント	マシンカタログとコンピューターアカウントを、毎回ドメイン資格情報を入力することなく管理します。	オンプレミスActive Directoryユーザーアカウントのユーザー名とパスワード。

資格情報の保護

Citrixは、サービスアカウントの資格情報を顧客のサイトデータベースに保存します。Citrix Virtual Apps and Desktops展開では、サイトデータベースはテナント（顧客）ごとのデータベースであり、顧客のために実行されているサービスのみがアクセスできます。

保存された資格情報を保護するために、以下の対策も実施されています。

- 資格情報は、データベースに保存される前に**AES 256**暗号化を使用して暗号化されます。
- 暗号化キーはサイトごとに生成され、Delivery Controller™にローカルに保存されます。これは、お客様専用のサービスのみがアクセスできます。
- データベースへの接続は、TLS 1.2プロトコルを使用して暗号化されます。

オンプレミス Active Directory サービスアカウント

オンプレミスActive Directoryサービスアカウントは、特権ドメインユーザーアカウントのユーザー名とパスワードを保存するためのコンテナです。このユーザーアカウントは、Active Directory内のコンピューターアカウントを管理するのに十分な権限を持っている必要があります。Machine Creation Serviceは、このサービスアカウントを使用して、ドメイン資格情報を毎回入力することなく、コンピューターアカウント関連の操作を実行できます。

オンプレミスActive Directoryサービスアカウントを作成する

Studio または PowerShell を使用して、オンプレミス Active Directory サービスアカウントを作成します。

前提条件

オンプレミス Active Directory サービスアカウントを作成するには、次のタスクを完了していることを確認してください。

- Active Directoryまたは特定のOUでコンピューターオブジェクトを作成、更新、削除するのに十分な権限を持つドメインユーザーアカウントをActive Directoryに作成します。

Web Studio を使用する

1. 左側のペインで、「**管理者**」を選択します。
2. 「**サービスアカウント**」タブで、「**サービスアカウントの作成**」をクリックします。
3. **IDの種類** ページで、**オンプレミス Active Directory** を選択します。**次へ** をクリックします。
4. **資格情報** ページで、**資格情報の入力** をクリックして、サービスアカウントとして使用する特権ドメインユーザーアカウントのユーザー名とパスワードを入力します。
5. パスワードの有効期限を設定するか、期限なしのままにします。
6. このサービスアカウントのスコープを1つ以上選択します。
7. サービスアカウントの表示名と説明（オプション）を入力します。
8. **完了**をクリックして作成を完了します。

PowerShell を使用する

PowerShellコマンドを使用してオンプレミスのActive Directoryサービスを作成できます。例：

```
$credential = ConvertTo-SecureString -String $password -AsPlainText -Force

New-AcctServiceAccount -IdentityProviderType ActiveDirectory
-IdentityProviderIdentifier test.local -AccountId test\svcacct_mcs
-AccountSecret $credential -SecretExpiryTime 2030/08/15 -DisplayName
'scvacct_mcs' -Description 'Service account for test.local'
```

注:

`$password`は、指定されたドメインユーザーアカウントの一致するパスワードです。

マシンID関連のアクションを実行する

Active DirectoryまたはMicrosoft Entraハイブリッドベースの IDプールがサービスアカウントに関連付けられた後、ドメイン資格情報を入力することなく、さまざまなマシンID関連のアクションを実行できます。

- サービスアカウントを使用して新しいIDアカウントを作成するには

  ```
  New-AcctADAccount -IdentityPoolName MyPool -Count 2 -UseServiceAccount
  ```

- サービスアカウントを使用してIDアカウントを修復するには

  ```
  Repair-AcctADAccount -ADAccountName "Domain\account","Domain\account2"
  -UseServiceAccount
  ```

- サービスアカウントを使用してIDアカウントを削除するには

  ```
  Remove-AcctADAccount -IdentityPoolName MyPool -RemovalOption Delete
  -ADAccountName "Domain\account","domain\account2" -UserServiceAccount
  ```

次のステップ

- オンプレミスのActive Directory参加済みカタログを作成するには、オンプレミスのActive Directory参加済みマシンIDのIDプールを参照してください)。
- サービスアカウントを管理するには、サービスアカウントの管理を参照してください。

サービスアカウントの管理

サービスアカウントの管理は、それらが健全な状態を保ち、資格情報が最新であることを保証するための重要な側面です。この記事では、サービスアカウントの表示、名前変更、編集、テスト、および削除の手順について説明します。

サービスアカウントの詳細を表示する

1. 左側のペインで、**「Administrators」**を選択します。
2. **「Service Accounts」**タブを選択します。
3. サービスアカウントを選択し、下部のパネルでその詳細を表示します。下部のパネルで、各サービスアカウントのプロパティと、関連するマシンカタログおよびトラブルシューティングのヒントを確認してください。

次の場合、サービスアカウントの横にエラーまたは警告アイコンが表示されます。

- サービスアカウントが異常な状態である。
- サービスアカウントの資格情報の有効期限が近づいている。

「Troubleshooting」タブには、問題を診断して修正するための情報が提供されます。

> **注：**
>
> 問題を修正した後、サービスアカウントテストを実行してステータスを更新します。詳しくは、「サービスアカウントをテストする」を参照してください。

サービスの名前を変更する

1. 左側のペインで、**「Administrators」**を選択します。
2. **「Service Accounts」**タブを選択します。
3. サービスアカウントを選択し、**名前の変更**をクリックします。

サービスアカウントを編集する

1. 左側のペインで、**「管理者」**を選択します。
2. **サービスアカウント**タブを選択します。
3. サービスアカウントを選択し、**編集**をクリックします。

サービスアカウントをテストする

1. 左側のペインで、「**管理者**」を選択します。
2. **サービスアカウント**タブを選択します。
3. サービスアカウントを選択し、**サービスアカウントのテスト**をクリックします。

- オンプレミスのActive Directoryサービスアカウントの場合、テスト中に資格情報が検証されます。
- Microsoft Entraサービスアカウントの場合、アプリケーションIDとシークレット、および必要な権限がテスト中に検証されます。

推奨事項に従って問題を特定し、修正します。**トラブルシューティング**タブには、問題を診断して修正するための情報が記載されています。問題を修正したら、サービスアカウントをテストします。

サービスアカウントを削除する

サービスアカウントを削除する前に、そのサービスアカウントがどのMCSマシンカタログでも使用されていないことを確認してください。

1. 左側のペインで、「**管理者**」を選択します。
2. **サービスアカウント**タブを選択します。
3. サービスアカウントを選択し、**削除**をクリックします。

イメージ管理

はじめに

MCSカタログの作成または更新プロセスには、次の2つのフェーズがあります。

- マスタリング: ソースイメージが公開イメージに変換されます
- クローニング: 公開イメージから新しいVMが作成されます

イメージ管理機能により、MCSはマスタリングフェーズをプロビジョニングワークフロー全体から分離します。

単一のソースイメージからさまざまなMCSイメージバージョン（準備済みイメージ）を準備し、複数の異なるMCSマシンカタログで使用できます。また、同じ接続タイプのホスト接続内のホスティングユニット間で準備済みイメージバージョンを共有することもできます。この実装により、

ストレージと時間のコストが大幅に削減され、VMの展開とイメージの更新プロセスが簡素化されます。

このイメージ管理機能を使用する利点は次のとおりです。

- カタログを作成せずに、事前に準備済みイメージを生成します。
- カタログの作成や更新など、複数のシナリオで準備済みイメージを再利用します。
- カタログの作成または更新時間を大幅に短縮します。
- 同じ接続タイプのホスト接続内のホスティングユニット間で準備済みイメージバージョンを共有します。（AzureおよびVMwareのみ）

> **注:**
>
> - この機能は現在、Amazon WorkSpaces Core Managed Instances、Azure、Azure、Red Hat OpenShift、VMware仮想化、およびXenServer環境に適用できます。
> - 準備済みイメージを使用せずにMCSマシンカタログを作成できます。その場合、この機能の利点を得ることはできません。ただし、Amazon WorkSpaces Core Managed Instancesの場合、準備済みイメージバージョンのみを使用してMCSカタログを作成します。マスターイメージを直接使用してカタログを作成することはできません。

ユースケース

イメージ管理機能のユースケースの一部を次に示します。

- *バージョン管理*: イメージバージョンを使用すると、次のことが可能になります。
  - 特定のイメージに対するさまざまなイテレーションや更新を管理する。
  - さまざまな目的のために、イメージの複数のバージョンを維持する。
- *論理的なグループ化*: 複数のイメージ定義を作成して、次のことができます。
  - プロジェクト、部署、アプリケーション、デスクトップの種類など、さまざまな基準に基づいてイメージバージョンを論理的にグループ化する。
  - 組織内でイメージをより効率的に管理する。
- *イメージ共有*: 同じ接続タイプのホスト接続内のホスティングユニット間で、準備されたイメージバージョンを共有して、次のことができます。

- 異なるホスティングユニット間でイメージの一貫性と均一性を確保する。

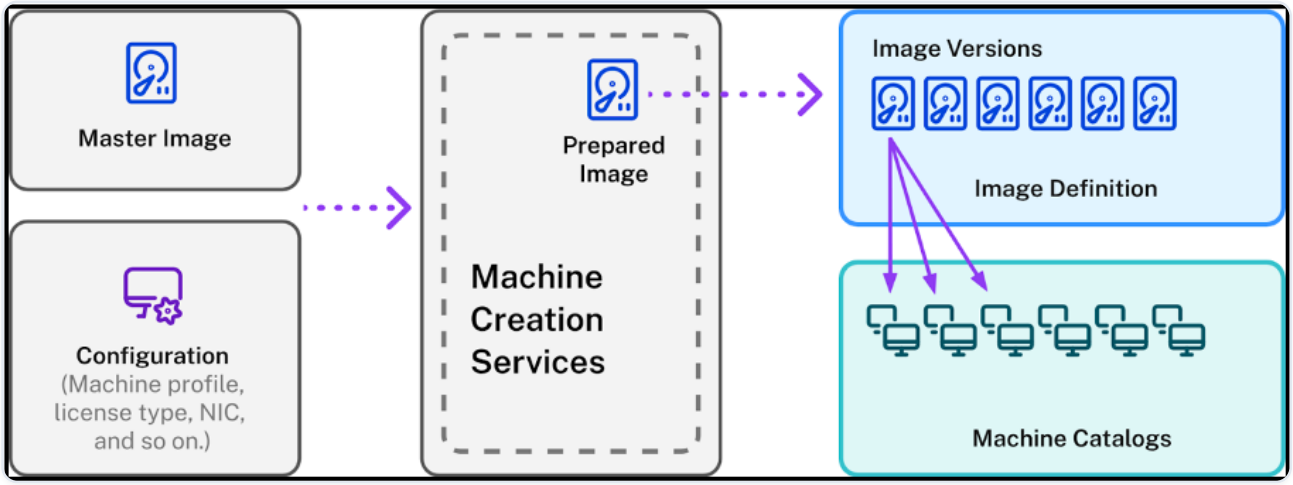
準備されたイメージとは?

イメージ管理機能により、MCSはマスタリングフェーズをカタログ作成または更新ワークフロー全体から切り離し、プロセスを2つの段階に分けます。

1. 単一のソースイメージから準備されたイメージを作成する。
2. 準備されたイメージを使用して、MCSマシンカタログを作成または更新する。

準備されたイメージは事前に作成できます。単一の準備されたイメージを使用して、複数のMCSプロビジョニング済みマシンカタログを作成または更新できます。

準備されたイメージが、イメージからWeb Studioを使用する際に、複数のMCSマシンカタログでどのように使用されるかを理解します。



イメージ定義: イメージ定義は、イメージのバージョンの論理的なグループ化です。イメージ定義には、以下の情報が含まれます。

- イメージが作成された理由
- 対象となるOS
- イメージの使用に関するその他の情報。

カタログはイメージ定義から作成されるのではなく、イメージ定義に基づいて作成されたイメージバージョンから作成されます。

イメージバージョン: イメージバージョンは、イメージ定義のバージョン管理を行います。1つのイメージ定義には複数のイメージバージョンを含めることができます。イメージバージョンを準備されたイメージとして使用し、カタログを作成または更新できます。ホスティングユニットが同じホ

スティング接続にあるかどうかにかかわらず、AzureとVMwareの両方の環境で、ホスティングユニット間でイメージバージョンを共有できます。

あるいは、PowerShellコマンドを使用してプロビジョニングスキームを作成し、カタログを作成または更新する場合は、環境に応じてマスターイメージバージョン仕様に基づいて準備されたイメージバージョン仕様を作成する必要があります。また、ホスティングユニットが同じホスティング接続にあるかどうかにかかわらず、Azure、VMware、およびAmazon WorkSpaces Core Managed Instancesの各環境で、ホスティングユニット間でイメージバージョン仕様を共有できます。

要件

- Windowsマスターイメージの場合、VDAイメージバージョン2311以降のみがサポートされます。MCS/IOコンポーネントは明示的に選択してインストールする必要があります。MCS I/O構成の有効化または無効化は、デフォルトでは有効になっていないため、マシンカタログの作成または更新時に決定する必要があります。

制限事項

現在、この機能は以下をサポートしていません。

- Azureでの複数NIC
- 永続データディスク機能
- マルチセッションの休止状態
- イメージタイプの変更
- Azureのホスティングユニット間で準備済みイメージバージョンを共有する場合、以下の共有方法は許可されていません。
    - 直接共有
    - パブリックコミュニティギャラリーへの共有

Web Studioを使用したイメージライフサイクル管理

Web Studioを使用する場合のイメージのライフサイクルは次のとおりです。

1. 準備済みイメージの作成: イメージ定義とその初期イメージバージョンを作成します。
2. 初期イメージバージョンからイメージバージョンを作成します。
3. 必要に応じて、仮想化環境内のホスティングユニットとイメージバージョンを共有します。
4. イメージバージョンを準備済みイメージとして使用して、カタログを作成します。

5. 別の準備済みイメージでマシンカタログを更新します。
6. イメージ定義とバージョンを管理する: イメージバージョンの名前と説明、およびイメージ定義の説明を編集します。
7. イメージバージョンを削除します。
8. イメージ定義を削除します。

または、PowerShell を使用してイメージを管理することもできます。「PowerShell を使用したイメージライフサイクル管理」を参照してください(#image-lifecycle-management-using-powershell)。

PowerShell を使用したイメージライフサイクル管理

PowerShell コマンドを使用してプロビジョニングスキームを作成する場合は、環境の必要に応じて、マスターイメージバージョン仕様に基づいて準備済みイメージバージョン仕様を作成する必要があります。

マスターイメージバージョン仕様: マスターイメージバージョン仕様は、イメージバージョンに追加または作成された特定のイメージです。ハイパーバイザー内の既存のイメージをマスターイメージバージョン仕様として追加するか、環境の必要に応じてマスターイメージバージョン仕様に基づいて準備済みイメージバージョン仕様を作成できます。準備済みイメージバージョン仕様は、複数のプロビジョニングスキームに使用できます。

Azure、VMware、および Amazon WorkSpaces Core Managed Instances の両方の環境で、同じホスティング接続内にあるかどうかにかかわらず、ホスティングユニット間でイメージバージョン仕様を共有することもできます。Azure では、Azure Compute Gallery (ACG) のディスク共有機能を使用して共有が実現されます。

PowerShellコマンドを使用する場合のイメージのライフサイクルは次のとおりです。

1. イメージを作成する:
    a. イメージ定義を作成します。
    b. 指定されたホスティング接続にイメージ定義の新しい構成を追加します。
    c. イメージバージョンを作成します。
    d. マスターイメージバージョン仕様を追加します。
    e. 準備済みイメージバージョン仕様を作成します。
2. 必要に応じて、仮想化環境内の別のホスティングユニットとイメージバージョン仕様を共有します。同じホスティング接続内にあるかどうかは問いません。

3. 準備済みイメージバージョン仕様を使用して MCS マシンカタログを作成する:

   a. ブローカーカタログを作成します。

   b. IDプールを作成します。

   c. `New-ProvScheme` コマンドを使用して、準備済みイメージバージョン仕様のUidパラメーターを持つプロビジョニングスキームを作成します。

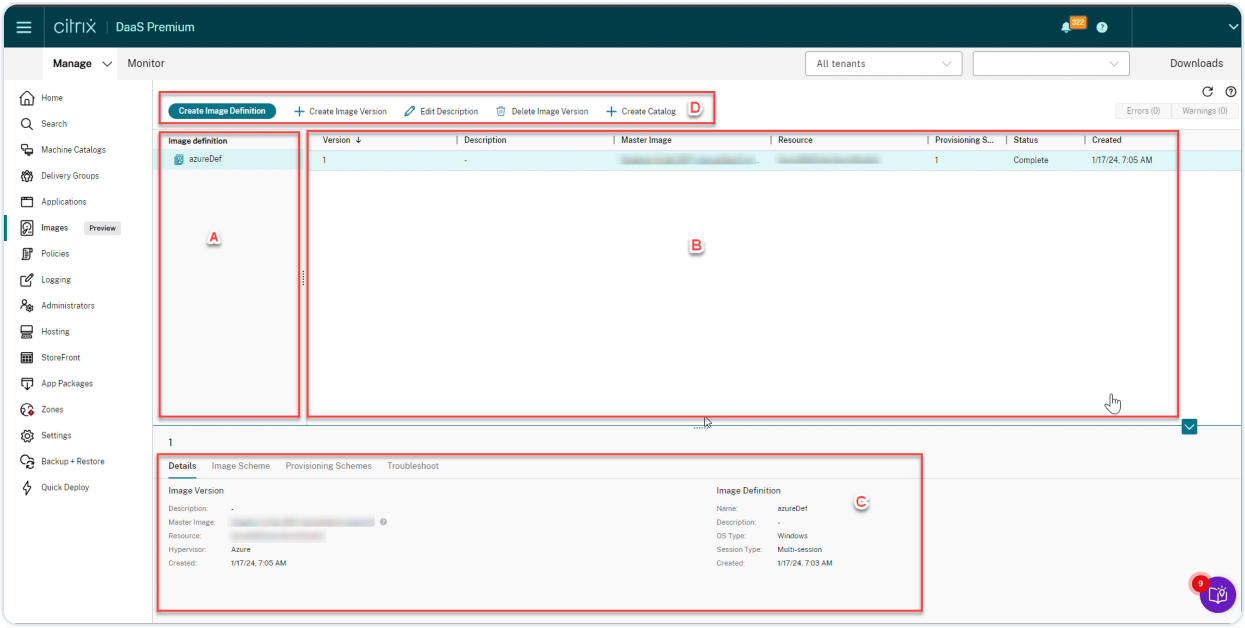
   d. ブローカーカタログをプロビジョニングスキームにリンクします。

4. MCSマシンカタログにVMを作成します。
5. `Set-ProvScheme` コマンドを使用して、プロビジョニングスキームの準備済みイメージバージョン仕様を変更します。
6. イメージ定義とバージョンを管理します: イメージバージョンとイメージ定義を編集します。
7. MCSマシンカタログを削除します: 削除順序は、マシンカタログ > 共有準備済みイメージバージョン仕様 (イメージ共有の場合) > 準備済みイメージバージョン仕様 > マスターイメージバージョン仕様 > イメージバージョン > 指定されたホスティング接続におけるイメージ定義の構成 > イメージ定義です。イメージバージョン仕様を削除する前に、準備済みイメージバージョン仕様がどのMCSマシンカタログにも関連付けられていないことを確認してください。

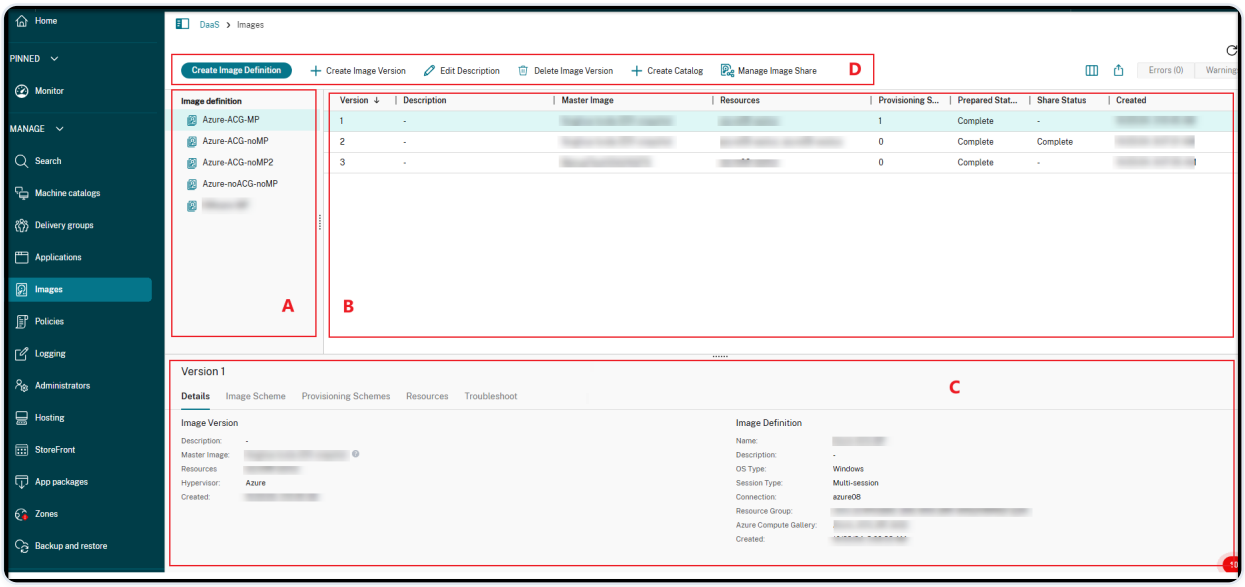
イメージノードについて理解する

イメージノードを使用して、MCSで準備されたイメージを作成および管理します。そのメインビューは4つの部分に分かれています。

- ホストユニット間で準備済みイメージが共有されていない場合



- ホストユニット間で準備済みイメージが共有されている場合:



ラベル	部分	説明
A	イメージ定義	以前に作成されたイメージ定義を一覧表示します。
B	イメージバージョン	選択したイメージ定義のイメージバージョンを表示します。
C	詳細	• **詳細**タブには、選択したイメージ定義またはバージョンに関する詳細情報（マスターイメージ、リソース、ハイパーバイザー、イメージ定義名、OS タイプ、セッションタイプなど）が表示されます。

ラベル	部分	説明
		• **イメージスキーム**タブには、ハードディスク、マシンサイズ、ライセンスタイプ、ディスク暗号化セット、マシンプロファイルなど、イメージの準備に使用されるテンプレートに関する情報が表示されます。 • **プロビジョニングスキーム**タブには、カタログの作成に使用されたプロビジョニングスキーム名が表示されます。 • **トラブルシューティング**タブには、選択したイメージバージョンのエラー状態が表示されます。 • イメージ共有の場合：**リソース**タブには、イメージバージョンの共有ステー

ラベル	部分	説明
		タスクが表示されます。
D	アクションバー	イメージ定義とバージョンに対して実行できるアクション（**イメージバージョンの作成**、**説明の編集**、**イメージ共有の管理**（準備済みイメージ共有の場合）、**イメージバージョンの削除**、**カタログの作成**など）を一覧表示します。

Azureサブスクリプションまたはテナント間で準備済みイメージを共有する

Azureプラットフォームで準備済みイメージをサブスクリプションまたはテナント間で共有するには、次の例に従ってください。

- **サービスプリンシパル**: SPN 1
- **サブスクリプション**: Subscription 1
- **テナント**: Tenant 1

このイメージを以下と共有します。

- **サービスプリンシパル**: SPN 2
- **サブスクリプション**: Subscription 2
- **テナント**: Tenant 2 (Tenant 1 と同じでもかまいません)

イメージを正常に共有して使用するには、**Subscription 1** のギャラリー、リソースグループ、またはサブスクリプションのスコープで、SPN 2 に次のアクセス許可を付与する必要があります。

- `Microsoft.Resources/subscriptions/read`
- `Microsoft.Compute/galleries/images/read`
- `Microsoft.Compute/galleries/images/versions/read`

> **注:**
>
> サブスクリプションまたはリソースに対するアクセス許可を持つサービスプリンシパルは、`Microsoft.Resources/subscriptions/read` アクセス許可を自動的に継承します。

または、**SPN 2** に組み込みロールの **Compute Gallery Image Reader** を割り当てます。

詳細な手順については、この Microsoft の記事 を参照してください。

次のステップ

- 準備済みイメージのマシンカタログを作成する
  - Amazon WorkSpaces Core マネージドインスタンス用の準備済みイメージを作成する
  - Amazon WorkSpaces Core マネージドインスタンスのカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/create-catalog-amazon-wsc.html)
  - Azure で準備済みイメージマシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/create-prepared-image-machine-catalogs-azure.html)
  - VMware で準備済みイメージマシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/create-prepared-image-machine-catalogs-vmware.html)
  - Red Hat OpenShift で準備済みイメージマシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/create-prepared-image-machine-catalogs-openshift.html)
  - XenServer で準備済みイメージマシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/create-prepared-image-machine-catalogs-xenserver.html)

準備済みイメージマシンカタログを作成する

準備済みイメージを作成し、その準備済みイメージを使用して、次の方法でMCSマシンカタログを作成します。

- ウェブスタジオ
- PowerShellコマンド

現在、Amazon WorkSpaces Core Managed Instances、Azure、Red Hat OpenShift、VMware、XenServer®仮想化環境で準備済みイメージマシンカタログを作成できます。

詳細情報

- イメージ管理

次のステップ

- Amazon WorkSpaces Coreで準備済みイメージを作成する および Amazon WorkSpaces Core カタログを作成する
- Azureで準備済みイメージマシンカタログを作成する
- VMwareで準備済みイメージマシンカタログを作成する
- Red Hat OpenShiftで準備済みイメージマシンカタログを作成する
- XenServerで準備済みイメージマシンカタログを作成する
- 準備済みイメージマシンカタログを管理する

Amazon WorkSpaces Coreマネージドインスタンス用の準備済みイメージを作成する

MCSマシンカタログを作成するには、準備済みイメージを作成します。準備済みイメージは、次の方法で作成できます。

- ウェブスタジオ
- PowerShellコマンド

主な手順

1. イメージ定義と初期イメージバージョンを作成します。
2. 初期イメージバージョンからイメージバージョンを作成します。

Web Studioを使用する

イメージ定義と初期イメージバージョンを作成する

イメージ定義と初期イメージバージョンを作成するには、次の手順を実行します。

1. Web Studioから、**［イメージ］ノードに移動し、［イメージ定義の作成］をクリックします。［はじめに］ページで［次へ］**をクリックします。
2. **［イメージ定義］ページで、イメージ定義の［OSの種類］と［セッションの種類］**を指定します。
3. **［イメージ］ページで、［リソース］**（設定された接続に適用可能なリソースのみが一覧表示されます）、イメージバージョンを作成するためのテンプレートとして使用するマスターイ

メージ、およびハードウェアプロパティを取得するためのマシンプロファイルを選択します。VMインスタンスまたは起動テンプレートバージョンからハードウェアプロパティを取得するためのマシンプロファイルを選択します。

> **注:**
>
> - イメージを選択する前に、マスターイメージにVDA 2311以降がインストールされており、MCSIOドライバーがVDAにインストールされていることを確認してください。
> - Instance Metadata Service (IMDS) V2 のみがサポートされており、IMDS V1 はサポートされていません。詳細については、「How Instance Metadata Service Version 2 works」を参照してください。

4. **Machine Specification** ページで、マシンサイズを選択します。マシンプロファイルのマシンサイズ（**Image** ページで選択）がデフォルトで選択されています。
5. **NICs** ページで、準備イメージ用の NIC を選択または追加します。各 NIC について、関連する VPC サブネットを選択します。
6. **Version Description** ページで、作成された初期イメージバージョンの説明を入力します。
7. **Summary** ページで、イメージ定義と作成された初期イメージバージョンの詳細を確認します。イメージ定義の名前と説明を入力します。**Finish** をクリックします。

イメージバージョンを作成する

イメージバージョンを使用すると、特定のイメージに対するさまざまなイテレーションや更新を管理できます。この機能により、さまざまな目的のためにイメージの複数のバージョンを維持できます。

初期イメージバージョンからイメージバージョンを作成するには、次の手順を実行します。

> **注:**
>
> すべてのイメージバージョンのホスティングユニットは同じである必要があります。

1. **Images** ノードに移動し、イメージバージョンまたはイメージ定義を選択して、**Create Image Version** をクリックします。

2. **Image definition** ページで、ホスティングユニットを変更し、そのイメージバージョンのマスターイメージとマシンプロファイルを再選択できます。
3. イメージバージョンの構成を初期構成済みイメージバージョンと異なるものにする場合は、**Create Image Version** ダイアログの **Machine Specification** および **NICs** ページで設定を構成します。
4. イメージバージョンの説明を追加します。**Finish** をクリックします。

> **注:**
>
> 何らかの理由でイメージバージョンの作成に失敗した場合、下部にある**トラブルシューティング**タブに**再試行**オプションが表示されます。

PowerShell を使用する

準備済みイメージバージョン仕様を作成するための詳細なPowerShellコマンドは次のとおりです。

1. `Test-ProvImageDefinitionNameAvailable command` を使用して、利用可能なイメージ定義名を確認します。例:

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
```

2. `New-ProvImageDefinition` コマンドを使用してイメージ定義を作成します。例:

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession
```

3. `Add-ProvImageDefinitionConnection`コマンドを使用して、指定されたホスティング接続にイメージ定義の新しい構成を作成します。

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName test-conn
```

4. `New-ProvImageVersion` コマンドを使用してイメージバージョンを作成します。例:

```
New-ProvImageVersion -ImageDefinitionName image1 -Description "version
1"
```

5. `Add-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様をイメージバージョンに追加します。例:

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
ImageVersionNumber  1 -HostingUnitName wsc -MasterImagePath "XDHyp:
\HostingUnits\wsc\win10-2411-ami (ami-00123456789abcdef).template”"
```

> **注:**
>
> ホスティングユニットの1つのイメージバージョンには、1つのマスターイメージバージョン仕様のみを追加できます。

6. `New-ProvImageVersionSpec`コマンドを使用して、マスターイメージバージョン仕様から準備済みイメージバージョン仕様を作成します。`SourceImageVersionSpecUid`パラメーターは`Add-ProvImageVersionSpec`コマンドから派生します。例：

```
New-ProvImageVersionSpec

-SourceImageVersionSpecUid  00000000-0000-0000-0000-00000000000

-MachineProfile 'XDHyp:\HostingUnits\wsc\w2022-2411
(lt-00123456789abcdef).launchtemplate\lt-00123456789abcdef
(1).launchtemplateversion' -RunAsynchronously
```

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を作成するためのPowerShellコマンドの完全なセットの例：

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession




Add-ProvImageDefinitionConnection -ImageDefinitionName image1
```

```
-HypervisorConnectionName wsc -CustomProperties $CustomProperties



$imageVersion = New-ProvImageVersion -ImageDefinitionName image1
-Description "version 1"



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -MasterImagePath "XDHyp:\HostingUnits\wsc\win10-2411-ami
(ami-00123456789abcdef).template”



New-ProvImageVersionSpec -MachineProfile 'XDHyp:
\HostingUnits\wsc\w2022-2411
(lt-00123456789abcdef).launchtemplate\lt-00123456789abcdef
(1).launchtemplateversion' -SourceImageVersionSpecUid
$SourceImageVersionSpec.ImageVersionSpecUid

Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
00000000-0000-0000-0000-00000000000-HostingUnitName wsc

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

注:

- イメージ定義内のすべてのイメージバージョン仕様は、同じホスティングユニットに属している必要があります。
- イメージバージョンには、1つのマスターイメージバージョン仕様と1つの準備済みイメージバージョン仕様のみを含めることができます。
- すべてのイメージバージョン仕様には、マシンプロファイルが必要です。

準備済みイメージをアベイラビリティゾーンとリージョン間で共有する

Amazon WorkSpaces Core マネージドインスタンスの場合、単一の準備済みイメージを、同じAWSリージョン内または異なるリージョン内の、異なるホスティングユニットに紐付けられた複数のアベイラビリティゾーン間で共有できるようになりました。これにより、1つの準備済みイメージを使用して、さまざまなアベイラビリティゾーンとリージョンでMCSマシンカタログを作成および更新できます。異なるリージョンの異なるAZ間で共有する場合、準備済みイメージのバージョンは元のリージョンから宛先リージョンにコピーされます。

単一の準備済みイメージを維持し、それを使用して、異なるホスティングユニットに紐付けられた複数のアベイラビリティゾーンとリージョン間でマシンカタログを作成および更新できます。これにより、イメージ管理のオーバーヘッドが大幅に削減され、展開全体の一貫性が確保され、プロビジョニングプロセスが合理化されます。また、既存のマシンカタログを、異なるアベイラビリティゾーンまたはリージョンからの準備済みイメージでシームレスに更新することもできます。

ユースケース

- **集中型イメージ管理:** 1つのアベイラビリティゾーン（例: `us-east-1a`）で準備済みイメージを作成します。その後、このイメージを同じ`us-east-1` AWSリージョン内の`us-east-1b`のような他のアベイラビリティゾーン、または異なる`us-west-1`リージョン内の`us-west-1a`に共有できます。これにより、単一のイメージで複数のホスティングユニットに対応でき、メンテナンスが簡素化されます。
- **効率的なカタログの作成と更新:** `AZ 1`で作成された準備済みイメージ（例: `us-east-1a`）を使用して、`AZ 1`に新しいカタログを作成できます。このイメージを`AZ 2`（例: `us-east-1b`）に共有した後、`AZ 2`の共有イメージを使用して、`AZ 2`にカタログを作成および更新できます。
- **クロスホスティングユニットおよびホスティング接続の展開:** 環境に同じまたは異なるAWSリージョンおよびAWSアカウントの下に複数のホスティングユニットがある場合、これらのホスティングユニット間で準備済みイメージを効率的に共有できます。

制限事項

- **同じAWSアカウント内での共有:** 現在の実装では、異なるAWSアカウント間での共有はできません。

重要な考慮事項

- **削除順序:** 元の準備済みイメージバージョン仕様を削除するには、まずその共有イメージバージョン仕様をすべて削除する必要があります。または、元の仕様と共有仕様を同時に削除する必要があります。

- **イメージバージョンの依存関係:** イメージバージョンを削除する場合、まずその特定のイメージバージョンに依存する共有構成をすべて削除する必要があります。元の（共有されていない）イメージから作成したカタログは、そのまま残すことができます。
- **カタログのバックポート可能性:** この機能が導入される前に展開した既存のマシンカタログを更新できます。カタログを最初に展開した場所とは異なるアベイラビリティゾーンまたはリージョンで作成した準備済みイメージを使用します。
- **完全な削除:** 準備済みイメージを削除すると、共有または最初に作成したどのアベイラビリティゾーンでも使用できなくなります。さらに、準備済みイメージバージョンに紐付けられているすべてのカタログが最初に削除されるまで、準備済みイメージバージョンを削除することはできません。

前提条件

この機能を構成または使用する前に、以下の条件を満たしていることを確認してください。

- お使いの環境は、Amazon WorkSpaces Core Managed Instances環境である必要があります。
- 同じAWSアカウントで、複数のホスティングユニット（それぞれ異なるアベイラビリティゾーンに紐付け可能）とホスト接続（それぞれ異なるリージョンに紐付け可能）を構成する必要があります。

Web Studio UI を使用して構成する

Web Studio UIを使用して、異なるホスティングユニットに紐付けられたアベイラビリティゾーン間で準備済みイメージを共有できます。

準備済みイメージを共有するには

1. Web Studioの**Images**ノードに移動し、他のアベイラビリティゾーンと共有したい準備済みイメージバージョンを選択します。
2. 上部のナビゲーションバーで**Manage Image Share**を選択し、選択したイメージバージョンのイメージ共有を管理します。
3. **Manage Image Share**ページで、イメージバージョンを共有したいリソースを1つ以上選択します。これらのリソースは、元のイメージバージョンとは異なるアベイラビリティゾーンに存在できます。
4. **Save**をクリックして、他のアベイラビリティゾーンのリソースでイメージバージョンを共有します。イメージバージョンは、選択した異なるリソース間で共有されるように更新されます。完了したら、イメージバージョンが共有されているアベイラビリティゾーンでカタログを作成するために、そのイメージバージョンを使用します。

準備済みイメージの共有を削除するには

1. Web StudioのImagesノードで、共有から削除したい準備済みイメージバージョンを選択します。
2. 上部のナビゲーションバーでManage Image Shareを選択し、選択したイメージバージョンのイメージ共有を管理します。
3. イメージバージョンの共有を停止したい1つ以上のリソース（アベイラビリティゾーン）のチェックボックスをオフにします。

> **注:**
>
> リソースには、共有イメージバージョンに関連付けられたカタログや、共有イメージバージョンから作成されたカタログが残っていてはなりません。削除する共有イメージバージョンから作成されたカタログは、まず削除する必要があります。

4. 「保存」をクリックして、クリアされたアベイラビリティゾーン間でのリソースの共有を削除します。イメージバージョンが更新され、それらのアベイラビリティゾーンでは共有されなくなります。

PowerShell を使用した構成

または、PowerShell コマンドを使用して、異なるホスティングユニットに紐付けられたアベイラビリティゾーン間で準備済みイメージを共有することもできます。

準備済みイメージを共有するには

1. 共有する準備済みイメージの `ImageVersionSpecUid` があることを確認します。これは、PowerShell で `Get-ProvImageVersionSpec` または同様の `Get-` コマンドを使用して取得できます。
2. 準備済みイメージを利用可能にするアベイラビリティゾーン（同じリージョンでも異なるリージョンでも可）の `HostingUnitName` を決定します。これは、その特定の AZ 用に構成したホスティングユニットの名前です。
3. ** `Add-ProvImageVersionSpecHostingUnit` コマンドを実行します。**次の PowerShell コマンドを使用します。 `<ImageVersionSpecUid>` をイメージの Uid に、 `<targetHostingUnitName>` をイメージバージョン仕様を共有するターゲットアベイラビリティゾーンのホスティングユニットの名前に置き換えます。

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
<ImageVersionSpecUid> -HostingUnitName <targetHostingUnitName>
```

4. 正常に実行されると、Web Studio UI でイメージのステータスが表示され、指定されたホスティングユニットと共有されたことが示されます。

準備済みイメージの共有を削除するには

1. 共有を削除する準備済みイメージの `ImageVersionSpecUid` があることを確認します。
2. 共有イメージを削除するアベイラビリティゾーンの `HostingUnitName` を決定します。
3. ** `Remove-ProvImageVersionSpecHostingUnit` コマンドを実行します。**次の PowerShell コマンドを使用します。 `<ImageVersionSpecUid>` をイメージの Uid に、 `<targetHostingUnitName>` をイメージバージョン仕様の共有を削除するターゲットアベイラビリティゾーンのホスティングユニットの名前に置き換えます。

```
Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
<ImageVersionSpecUid> -HostingUnitName <targetHostingUnitName>
```

次のステップ

- Amazon WorkSpaces Core Managed Instances のカタログを作成する方法については、「Amazon WorkSpaces Core Managed Instances のカタログを作成する」を参照してください。

詳細情報

- イメージ管理
- Amazon WorkSpaces Core GitHub PowerShell の例については、「citrix-mcs-sdk-samples-Amazon WorkSpaces Core」を参照してください。

Amazon WorkSpaces Core Managed Instances のカタログを作成する

マシンカタログの作成 では、マシンカタログを作成するウィザードについて説明します。以下の情報では、Amazon WorkSpaces Core マネージドインスタンスに固有の詳細について説明します。

注:

現在、永続VMと非永続VMの両方のカタログの作成（`CleanOnBoot` プロパティが `True` または `False`）がサポートされています。

前提条件

Amazon WorkSpaces Core マネージドインスタンスのカタログを作成する前に、次の作成を完了する必要があります。

1. Amazon WorkSpaces Core マネージドインスタンスへの接続。「Amazon WorkSpaces Core マネージドインスタンスへの接続」を参照してください。
2. 準備されたイメージ。「Amazon WorkSpaces Core マネージドインスタンス用の準備されたイメージを作成する」を参照してください。

イメージ準備中のネットワーク設定

イメージ準備中に、元のVMに基づいて準備用仮想マシン（VM）が作成されます。この準備用VMはネットワークから切断されます。準備用VMからネットワークを切断するために、すべてのインバウンドおよびアウトバウンドトラフィックを拒否するネットワークセキュリティグループが作成されます。このネットワークセキュリティグループは永続的であり、再利用されます。ネットワークセキュリティグループの名前は `Citrix.XenDesktop.IsolationGroup-GUID` で、GUIDはランダムに生成されます。

マシンプロファイルベースのマシンカタログ

マシンプロファイルを使用して、EC2インスタンス（VM）または起動テンプレートバージョンからハードウェアプロパティをキャプチャし、プロビジョニングされたマシンに適用できます。キャプチャされるプロパティには、テナンシータイプ、インスタンスタイプ、セキュリティグループ、ネットワークマッピング、EBSボリュームプロパティ、EBS最適化、CPUオプション、ハイバネーション機能、その他のサポートされているAWS構成などが含まれます。

マシンプロファイルの入力として、AWS EC2インスタンス（VM）またはAWS起動テンプレートバージョンを使用できます。

注:

- EBSボリュームプロパティは、マシンプロファイルからのみ派生します。

- Instance Metadata Service (IMDS) V2 のみがサポートされており、IMDS V1 はサポートされていません。詳細については、「How Instance Metadata Service Version 2 works」を参照してください。

AWS テナンシー

AWS は、共有テナンシー（デフォルトタイプ）と専用テナンシーの次のテナンシーオプションを提供します。共有テナンシーとは、異なる顧客の複数の Amazon WorkSpaces Core インスタンスが同じ物理ハードウェア上に存在する可能性があることを意味します。専用テナンシーとは、Amazon WorkSpaces Core インスタンスが、展開した他のインスタンスと同じハードウェア上でのみ実行されることを意味します。

注:

専用インスタンスのみがサポートされています（専用ホストは現在サポートされていません）。他の顧客は同じハードウェアを使用しません。

テナンシータイプはマシンプロファイルから取得されます

MCS を使用して AWS でマシンをプロビジョニングするカタログを作成すると、テナンシータイプはマシンプロファイルから取得されます。

- **共有ハードウェア**：この設定は、ほとんどの展開に適しています。複数の顧客が互いにやり取りすることはありませんが、ハードウェアを共有します。共有ハードウェアを使用することは、Amazon EC2 インスタンスを実行するための最も安価なオプションです。
- **専用インスタンス**：この設定は、特定のセキュリティまたはコンプライアンス要件を持つ展開により適しています。専用インスタンスを使用すると、他の AWS 顧客とは別のホストを持つという利点を享受できますが、ホスト全体に対して料金を支払う必要はありません。ホストの容量について心配する必要はありませんが、インスタンスに対してはより高い料金が課金されます。さらに、専用インスタンスは、Bring Your Own License (BYOL) のサポートが限定的です。

カタログを作成する

Amazon WorkSpaces Coreマネージドインスタンスのカタログを作成するには、準備済みイメージとマシンプロファイルが必要です。マシンプロファイルの入力として、AWS VMインスタンスまたはAWS起動テンプレートバージョンを使用できます。

カタログは以下を使用して作成できます。

- ウェブスタジオ
- PowerShell

Web Studioを使用してカタログを作成する

「イメージ」ノードからマシンカタログを作成する

イメージノードの**カタログの作成**オプションを使用して、イメージバージョンでカタログを作成します。

または、**マシンカタログ**ノードでカタログを作成する際にバージョンを選択し、カタログ作成ワークフローで準備されたイメージオプションにリンクすることもできます。「マシンカタログ」ノードからマシンカタログを作成するを参照してください。

イメージノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. イメージバージョンを選択し、**カタログの作成**をクリックします。**はじめに**ページで**次へ**をクリックします。
2. 「**マシン管理**」および「**イメージ**」ページでは、選択したイメージバージョンに基づいて設定が事前に選択されています。イメージページで、選択した準備済みイメージのメモを入力します。
3. 次のページで設定を完了します。
4. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。
5. **マシンカタログ**ノードに移動して、作成されたマシンカタログを表示します。

「マシンカタログ」ノードからマシンカタログを作成する

「マシンカタログ」ノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. 左側のナビゲーションペインで**マシンカタログ**をクリックします。
2. **マシンカタログの作成**をクリックします。**マシンカタログのセットアップ**ページが表示されます。
3. **マシンタイプ**ページで、カタログのマシンタイプ（例: **マルチセッションOS**）を選択します。
4. **マシン管理**ページで、次の設定を選択します。
    a. 「**電源管理されるマシン (仮想マシンやブレードPCなど)**」を選択します。
    b. 「**Citrixプロビジョニングテクノロジー**」を選択します。次に、「**Citrix Machine Creation Services™**」を選択します。

c. 「**リソース**」フィールドで、ホスト接続の作成時に構成したリソース（アベイラビリティゾーンまたはローカルゾーン）を選択し、「**次へ**」をクリックします。

5. 「**デスクトップエクスペリエンス**」ページで、ユーザーがログインしたときに使用するランダムまたは静的デスクトップのいずれかを選択します。静的デスクトップを選択した場合は、ユーザーがローカルディスクで行った変更を保存するかどうか（永続的または非永続的）をさらに指定します。
6. 「**イメージ**」ページで、「**イメージの選択**」をクリックして、マシンカタログ用の準備済みイメージを選択します。作成した準備済みバージョンを選択します。イメージのバージョン名をクリックします。選択したイメージバージョンの詳細を表示するには、下線が引かれているバージョン番号をクリックします。「**完了**」をクリックします。

   準備済みイメージに関連付けられたマシンプロファイルが表示され、そのハードウェアプロパティ（インスタンスタイプ、テナンシータイプ、ネットワークマッピング、セキュリティグループ、ボリュームプロパティなど）がカタログ内のマシンを作成するために使用されます。マシンプロファイルのソースを別のVMまたは起動テンプレートバージョンに変更するには、編集ボタンをクリックします。
7. 「**仮想マシン**」ページで、次の操作を行います。

   a. カタログのVM数を入力します。

   b. デフォルトのマシン仕様が表示されます。これはマシンプロファイルに基づいています。変更するには、編集アイコンを選択し、マシン仕様を選択します。
8. 「**NIC**」ページで、VMのNIC（またはENI）を選択します。
9. 「**マシンID**」ページで、カタログ内のマシンのマシンIDタイプを構成します。

   a. **ドメイン参加済みマシン（オンプレミスのActive DirectoryまたはMicrosoft Entraハイブリッド参加）**を構成するには、ドメインを選択し、このマシンカタログで作成するVMの新しいADアカウントを作成します。プロビジョニングされたVMは、選択したドメインに参加します。**ドメイン非参加マシン**をプロビジョニングするには、ドメイン非参加オプションを選択します。

   b. VM用に作成する新しいアカウントのアカウント命名スキームを指定します。
10. 「**ドメイン資格情報**」ページで、「**資格情報の入力**」をクリックして、選択したドメインの資格情報を入力します。プロンプトが表示されたら、管理者レベルのユーザー名とパスワードを入力します。当社の製品ドキュメントに従って、ドメイン資格情報を以前に保存している場合は、サービスアカウントを使用することもできます。
11. 「**概要**」ページが表示されるまで残りのページをクリックします。マシンカタログの名前を入力し、「**完了**」を選択してマシンカタログを作成します。

AWSローカルゾーンでのマシンカタログ作成に関する制限事項

- 特定のローカルゾーンは特定のハードウェア構成のみをサポートします（例：パースのローカルゾーンはGP3ボリュームをサポートせず、GP2のみをサポートします）。
- gp2はすべてのローカルゾーンで普遍的にサポートされており、すべてのローカルゾーンがgp3をサポートしているわけではないため、IDディスクの作成はデフォルトでgp2ボリュームタイプを使用します。
- 目的のローカルゾーンでサポートされているハードウェア仕様を持つマシンプロファイルを選択する必要があります。
- 準備されたイメージAMIスナップショットとIDディスクスナップショットは、デフォルトでローカルゾーンではなくリージョンに配置されます（ローカルゾーンでのEBSスナップショットサポートの可視性に関するAWSの制限のため）。
- 完全なEC2およびEBSサービスをサポートするローカルゾーンのみがサポート対象ゾーンです。

PowerShellを使用してカタログを作成する

準備済みイメージバージョン仕様とマシンプロファイルを使用してカタログを作成する

- `New-ProvScheme`コマンドを使用して、準備済みイメージバージョン仕様からMCS非永続マシンカタログを作成します。例:

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-CleanOnBoot
$true] [-MachineProfile <string>] [-ProvisioningSchemeType “MCS”]
```

- `New-ProvScheme`コマンドを使用して、準備済みイメージバージョン仕様からMCS永続マシンカタログを作成します。例:

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-CleanOnBoot
$false] [-MachineProfile <string>] [-ProvisioningSchemeType “MCS”]
```

カタログを作成するためのPowershellコマンドの完全なセットの例:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "wsccatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"
```

```
$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "domainname"
-IdentityPoolName "wsccatalog" -IdentityType "ActiveDirectory"  -
NamingScheme "aws##" -NamingSchemeType "Numeric" -Scope @()



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



$Task = New-ProvScheme -ProvisioningSchemeName wsccatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName wsc -IdentityPoolName wsccatalog -CleanOnBoot -Scope @()
-SecurityGroup @() -MachineProfile 'XdHyp:\HostingUnits\cvad-test-
scalestress\us-east-1a.availabilityzone\machine-profile-instance i
(i-0xxxxxxxx).vm' -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName wsccatalog



Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

マシンプロファイルを更新する

マシンプロファイルで最初にプロビジョニングされたカタログのマシンプロファイルを更新するには、以下を実行します。MCSマシンカタログの編集中に、マシンプロファイルソースのテナンシータイプとハイバネーション機能を変更することもできます。

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme `

-ProvisioningSchemeUid "<ID" `
```

```
-MachineProfile "XDHyp:\HostingUnits\abc\us-
east-1a.availabilityzone\citrix-cvad-machineprofile-instance
(i-0xxxxxxxx).vm"
```

PowerShellを使用して起動テンプレートバージョンでカタログを作成する

マシンプロファイル入力として起動テンプレートバージョンを使用してMCSマシンカタログを作成できます。また、マシンプロファイルカタログの入力をVMから起動テンプレートバージョンへ、または起動テンプレートバージョンからVMへ更新することもできます。

AWS EC2コンソールでは、起動テンプレートのインスタンス構成情報をバージョン番号とともに提供できます。マシンカタログの作成または更新時に、マシンプロファイル入力として起動テンプレートバージョンを指定すると、そのバージョンの起動テンプレートのプロパティがプロビジョニングされたVDA VMにコピーされます。

以下のプロパティは、マシンプロファイル入力を使用するか、`New-ProvScheme` または `Set-ProvScheme` コマンドでパラメーターとして明示的に指定できます。`New-ProvScheme` または `Set-ProvScheme` コマンドで指定された場合、これらのプロパティのマシンプロファイル値よりも優先されます。

- サービスオファリング
- ネットワーク

注:

マシンプロファイル起動テンプレートでサービスオファリングが提供されていない場合、または `New-ProvScheme` コマンドのパラメーターとして提供されていない場合、適切なエラーが発生します。

マシンプロファイル入力として起動テンプレートバージョンを使用してカタログを作成するには：

1. **PowerShell** ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために `asnp citrix*` を実行します。
3. 起動テンプレートの起動テンプレートバージョンの一覧を取得します。例：

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate> ls |
Select FullPath
```

4. 作成されていない場合は、IDプールを作成します。例：

```
New-AcctIdentityPool `

-IdentityPoolName "abc11" `

-NamingScheme "abc1-##" `

-NamingSchemeType Numeric `

-Domain "citrix-xxxxxx.local" `

-ZoneUid "xxxxxxxx" `
```

5. マシンプロファイル入力として起動テンプレートバージョンを使用してプロビジョニングスキームを作成します。例：

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `

-ImageVersionSpecUid ‘24dfb047-e867-527g-896c-25664xxxxx1t’ `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

6. プロビジョニングスキームをブローカーカタログとして登録します。例：

```
New-BrokerCatalog -Name "MPLT1" `

-AllocationType Random `
```

```
-Description "Machine profile catalog" `

-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `

-ProvisioningType Mcs `

-SessionSupport MultiSession `

-PersistUserChanges Discard
```

7. カタログの作成を完了します。

マシンプロファイルのソースを更新する

マシンプロファイルカタログの入力を、VMから起動テンプレートバージョンへ、または起動テンプレートバージョンからVMへ更新することもできます。例：

- マシンプロファイルカタログの入力をVMから起動テンプレートバージョンに更新するには：

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxxx
(1).launchtemplateversion"
```

- マシンプロファイルカタログの入力を起動テンプレートバージョンからVMに更新するには：

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-
east-1a.availabilityzone\apollo-non-persistent-vda-win2022-2
(i-08xxxxxxxx).vm"
```

OSディスクとIDディスクを暗号化する

OSディスクとIDディスク（Identity Disk）の暗号化に使用できるAWS KMSキー（カスタマー管理キーおよびAWS管理キー）を使用して、VMのカタログを作成できます。

- AWS管理キーは毎年自動的にローテーションされます。
- カスタマー管理キーは自動ローテーションがオプションであり、手動で管理できます。

KMSキーの詳細については、以下のAWSドキュメントを参照してください。

- AWS KMSの概念
- 自動キーローテーションの仕組み

OSディスクとIDディスクの暗号化には、以下のいずれかを構成します。

- 暗号化された準備済みイメージを使用します（例：KMSキーで暗号化されたEBSルートボリュームを含むインスタンスまたはスナップショットから作成されたAMI）
- 暗号化されたEBSルートボリュームを含むマシンプロファイルソース（VMまたは起動テンプレート）を使用します。

制限事項

次の制限事項を考慮してください。

- MCSは現在、準備済みイメージAMI上のディスクを1つのみサポートしています。
- 既存の暗号化されていないEBSボリュームやスナップショットを直接暗号化したり、既存の暗号化されたボリュームのKMSキーを変更したりすることはできません。これを行うには、次の手順を実行する必要があります。

  a. そのボリュームの新しいスナップショットを作成します。

  b. そのスナップショットから新しいボリュームを作成します

  c. 新しいボリュームを暗号化します。

以下のAWSドキュメントを参照してください。

- 暗号化されていないリソースを暗号化する
- EBSボリュームの自動またはデフォルト暗号化の制限: 既存および新規のAmazon EBSボリュームを自動的に暗号化する。

ディスク暗号化を使用してカタログを作成する

ディスク暗号化を使用して MCS マシンカタログを作成するには、次のものを使用できます。

- 準備済みイメージ（暗号化されたディスクを持つマスターイメージからイメージ管理を使用して作成）
- マシンプロファイル

マシンプロファイル入力を使用する際の考慮事項は次のとおりです。

- マシンプロファイル入力の KMS キーは、準備されたイメージの KMS キーよりも優先されます。
- マシンプロファイル入力が提供されない場合、準備されたイメージAMIのKMSキーがカタログVMのディスクを暗号化するために使用されます。
- マシンプロファイルにブロックデバイスマッピングが存在する場合、準備されたイメージテンプレート (AMI) とマシンプロファイルに存在するブロックデバイスは一致する必要があります。たとえば、AMIに`/dev/sda1`で定義されたデバイスがある場合、マシンプロファイルにも`/dev/sda1`で定義されたデバイスが必要です。
- マシンプロファイルソースにキーがなく、準備されたイメージが暗号化されていない場合、カタログVMのディスクは暗号化されません。
- 準備されたイメージが暗号化されている場合、マシンプロファイルソースVMまたは起動テンプレートには、有効な入力と見なされるために暗号化されたルートボリュームが必要です。

既存のカタログを変更する

`Set-ProvScheme` PowerShellコマンドを使用して、既存のカタログを次のように変更できます。

- 新しいKMSキーを含むボリュームを持つマシンプロファイル入力。
- イメージ管理を使用して、暗号化されたAMIを持つマスターイメージから作成された準備済みイメージ。

重要な考慮事項：

- カタログに追加された新しいVMのボリュームは、新しいKMSキーで暗号化されます。
- 既存のマシンプロファイルがある場合に暗号化設定を更新するには、新しいマシンプロファイルで`Set-ProvScheme`を実行します。
- 既存のカタログを、暗号化されたボリュームから暗号化されていないボリュームに変更することはできません。 暗号化された準備済みイメージAMIから暗号化されていない準備済みイメージAMIへのイメージ更新はできません。

VMインスタンスでNitroTPMとUEFIセキュアブートを有効にする

カタログを作成する際、NitroTPMおよび/またはUEFIセキュアブートが有効な準備済みイメージ (AMI) を選択できるようになりました。これにより、カタログ内のプロビジョニングされたVMもNitroTPMおよび/またはUEFIセキュアブートが有効になります。この実装により、VMが安全で信頼できるものになります。NitroTPMおよびUEFIセキュアブートの詳細については、Amazonドキュメントを参照してください。

制限事項

- NitroTPMとSecure Bootは現在、中国を除くすべてのAWSリージョン（AWS GovCloud (US) リージョンを含む）で利用できます。
- 既存のカタログでNitroTPMとUEFIセキュアブートを有効にすることはできません。NitroTPMとUEFIセキュアブートが有効なカタログが必要な場合は、新しいカタログを作成してください。

主要な手順

1. AWS環境をセットアップします。
2. AWSへの接続を作成します。
3. NitroTPMおよび/またはUEFIセキュアブートが有効なマスターイメージ（AMI）を作成します(#create-an-ami-that-supports-nitrotpm-and-uefi-secure-boot)。
4. マスターイメージから準備済みイメージを作成します。Amazon WorkSpaces Core Managed Instances 用の準備済みイメージを作成するを参照してください。
5. Web StudioのカタログメニューでNitroTPMとUEFIセキュアブートが有効な準備済みイメージを選択するか、PowerShellコマンドを使用してプロビジョニングスキームを作成する際に、マシンカタログを作成します。

作成されたカタログに追加されたVMは、NitroTPMおよびUEFIセキュアブートが有効になっています。

NitroTPMおよびUEFIセキュアブートをサポートするAMIを作成する

1. NitroTPMおよび/またはUEFIセキュアブートが有効になっているVMからAMIを作成できます。
   a. AWS Marketplaceイメージを使用してインスタンスを作成します。例：`TPM-Windows_Server-2022-English-Full-Base on the aws-marketplace`を検索します。
   b. シングルセッションまたはマルチセッションVDAをダウンロードします。
   c. そのVMからAMIを作成します。
2. register-imageコマンドを使用します。

   ```
   --boot-mode (string)

   --tpm-support (string)
   ```

   詳細については、register-imageを参照してください。

以下のAWSドキュメントを参照してください。

- EC2インスタンスタイプのサポートされているブートモードを決定する
- Amazon EC2インスタンスでNitroTPMを使用するための要件/。

Delivery Controller™ホストからPowerShellウィンドウを開いて、特定の項目を確認できます。

- サービス提供がNitroTPMまたはUEFIセキュアブートをサポートしているか

```
(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.BootMode

(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.NitroTpmSupportVersions
```

- テンプレートがNitroTPMまたはUEFIセキュアブートをサポートしているか

```
(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.BootMode



(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.TpmSupport
```

既存のカタログのサービス提供を更新する

`Set-ProvScheme`を使用して、既存のカタログのサービス提供を変更できます。この変更は、新しく追加されたVMに適用されます。ただし、次のシナリオではエラーが発生します。

AMIのブートモード	AMIはNITRO TPMをサポートしていますか？	サービス提供はNITROTPMとUEFIセキュアブートをサポートしていますか？
UEFI	いいえ	いいえ
レガシーBIOS	はい	いいえ
UEFI	はい	いいえ
UEFI優先	はい	いいえ

VM上のタグをコピーする

マシンプロファイルで指定されたNIC、およびディスク（IDディスク、ライトバックキャッシュディスク、OSディスク）のタグを、MCSマシンカタログで新しく作成されたVMにコピーできます。これらのタグは、マシンプロファイルのソース（AWS VMインスタンスまたはAWS起動テンプレートバージョン）のいずれかで指定できます。この機能は、永続および非永続マシンカタログとVMに適用されます。

> **注:**
>
> - AWS EC2コンソールでは、**起動テンプレートバージョンリソースタグ**の下に**ネットワークインターフェイスのタグ**の値が表示されません。ただし、PowerShellコマンド `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` を実行すると、タグの仕様を確認できます。
> - マシンプロファイルのソース（VMまたは起動テンプレートバージョン）に2つのネットワークインターフェイス（eni-1とeni-2）があり、eni-1にタグt1、eni-2にタグt2がある場合、VMは両方のネットワークインターフェイスのタグを取得します。

PowerShellを使用してVMインスタンスをフィルタリングする

マシンプロファイルVMとして使用するAWS VMインスタンスは、マシンカタログが正しく作成され機能するために互換性がある必要があります。マシンプロファイルの入力VMとして使用できるAWS VMインスタンスを一覧表示するには、`Get-HypInventoryItem` コマンドを使用できます。このコマンドは、ホスティングユニットで利用可能なVMのインベントリをページングおよびフィルタリングできます。

ページネーション：

Get-HypInventoryItem は、2つのページネーションモードをサポートしています。

- ページングモードでは、`-MaxRecords` と `-Skip` パラメーターを使用してアイテムのセットを返します。
  - `-MaxRecords`: デフォルトは **1** です。これは、返すアイテムの数を制御します。
  - `-Skip`: デフォルトは **0** です。これは、ハイパーバイザー内のリストの絶対的な先頭 (または絶対的な末尾) からスキップするアイテムの数を制御します。
- スクロールモードでは、`-MaxRecords`、`-ForwardDirection`、および `-ContinuationToken` パラメーターを使用してレコードのスクロールを許可します。

- `-ForwardDirection`: デフォルトは **True** です。これは `-MaxRecords` とともに使用され、一致するレコードの次のセットまたは前のセットのいずれかを返します。
- `-ContinuationToken`: `ContinuationToken` で指定されたアイテムを含まずに、その直後 (または `ForwardDirection` が **false** の場合は直前) のアイテムを返します。

ページネーションの例:

- 最も名前の小さいマシンテンプレートの単一レコードを返します。`AdditionalData` フィールドには `TotalItemsCount` と `TotalFilteredItemsCount` があります。

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template
```

- 最も低い名前を持つマシンのテンプレートのレコードを10件返すには:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 10 | select Name
```

- 最も高い名前で終わるレコードの配列を返すには:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ForwardDirection $False -MaxRecords 10 | select
Name
```

- 指定された `ContinuationToken` に関連付けられたマシンテンプレートから始まるレコードの配列を返します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ContinuationToken "ami-07xxxxxxxxx"
-MaxRecords 10
```

フィルタリング:

フィルタリングには、以下の追加のオプションパラメーターがサポートされています。これらのパラメーターは、ページネーションオプションと組み合わせることができます。

- `-ContainsName "my_name"`: 指定された文字列がAMI名の一部と一致する場合、そのAMIは `Get` の結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -ContainName ‘apollo’ | select
Name
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: AMIがこれらのタグの少なくとも1つを持っている場合、そのAMIは`Get`の結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -Tags '{"opex owner": "Not
tagged"}' | select Name
```

> **注:**
>
> 2つのタグ値がサポートされています。**Not Tagged** タグ値は、タグのリストに指定されたタグがない項目と一致します。**All values** タグ値は、タグの値に関係なくタグを持つ項目と一致します。それ以外の場合、一致は、項目がタグを持ち、その値がフィルターで指定された値と等しい場合にのみ発生します。

- `-Id "ami-0a2d913927e0352f3"`: AMIが指定されたIDと一致する場合、そのAMIは`Get`の結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -Id ami-xxxxxxxxxxxx
```

AdditionalDataパラメーターでのフィルタリング:

`AdditionalData`フィルターパラメーターは、テンプレートまたはVMを、その機能、サービス提供、またはAdditionalDataにある任意のプロパティに基づいて一覧表示します。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200).AdditionalData
```

互換性のないVMを示すために、`-Warn`パラメーターを追加することもできます。VMには、**Warning**という名前の`AdditionalData`フィールドが含まれます。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-015xxxxxxxx"
-Warn $true).AdditionalData
```

次のステップ

- Amazon WorkSpaces Coreカタログの管理については、Amazon WorkSpaces Coreマネージドインスタンスのカタログを管理するを参照してください。

詳細情報

- AWS仮想化環境
- Amazon WorkSpaces Coreマネージドインスタンスへの接続
- イメージ管理
- Amazon WorkSpaces Core Managed Instances 用の準備済みイメージを作成する
- Amazon WorkSpaces Core の GitHub PowerShell の例については、citrix-mcs-sdk-samples-Amazon WorkSpaces Coreを参照してください。

Azure で準備済みイメージのマシンカタログを作成する

準備済みイメージを作成し、その準備済みイメージを使用して、次の方法でMCSマシンカタログを作成します。

- ウェブスタジオ
- (#use-powershell)

準備済みイメージを使用して MCS マシンカタログを作成する主な手順は次のとおりです。

1. イメージ定義と初期イメージバージョンを作成します。
2. イメージバージョンを準備済みイメージとして使用してカタログを作成します。

Web Studio を使用する

イメージ定義と初期イメージバージョンを作成する

イメージ定義と初期イメージバージョンを作成するには、次の手順を実行します。

1. Web Studio から、**Images** ノードに移動し、**Create Image Definition** をクリックします。**Introduction** ページで **Next** をクリックします。
2. **Image Definition** ページで、イメージ定義の **OS type** と **Session type** を指定します。

3. 既存のリソースグループを選択するか、イメージリソースを保持するための新しいリソースグループを作成します。イメージ共有を有効にするには、Azure Compute Gallery で **Place image versions** を選択し、新しいギャラリーを作成するか、既存のギャラリーを使用してイメージバージョンを保持するかを選択します。
4. **Image** ページで、**Resources** (設定された接続に適用可能なリソースのみが一覧表示されます) と、イメージバージョンを作成するためのテンプレートとして使用するマスターイメージを選択します。**Use a machine profile** チェックボックスをオンにして、マシンプロファイルを選択できます。

   > **注:**
   >
   > - イメージを選択する前に、マスターイメージにVDA 2311以降がインストールされており、VDAにMCSIOドライバーがインストールされていることを確認してください。
   > - 機密VMタイプの準備済みイメージを使用してMCSカタログを作成する場合は、機密VMタイプのマスターイメージと機密VMタイプのマシンプロファイルを使用して準備済みイメージを作成します。機密VMタイプのマスターイメージとマシンプロファイルの準備については、(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure#azure-confidential-vms) を参照してください。

5. 「**ストレージとライセンスの種類**」ページで、イメージ準備プロセスの一部として使用するストレージとライセンスの種類を選択します。

   > **注:**
   >
   > 「**イメージ**」ページでマシンプロファイルを選択すると、マシンプロファイルのライセンスタイプはプロファイル設定に基づいて事前に選択されます。

6. 「**マシンの仕様**」ページで、マシンサイズを選択します。「**イメージ**」ページでマシンプロファイルを選択すると、マシンプロファイルのマシンサイズがデフォルトで選択されます。
7. 「**NIC**」ページで、準備イメージのNICを選択または追加します。各NICについて、関連する仮想ネットワークを選択します。

8. 「**ディスク設定**」ページで、顧客管理の暗号化キー (CMEK) を選択します。マシンプロファイルにCMEKがないが、マスターイメージにある場合、マスターイメージからCMEKが事前に選択されます。
9. 「**バージョン説明**」ページで、作成された初期イメージバージョンの説明を入力します。
10. 「**概要**」ページで、イメージ定義と作成された初期イメージバージョンの詳細を確認します。イメージ定義の名前と説明を入力します。「**完了**」をクリックします。

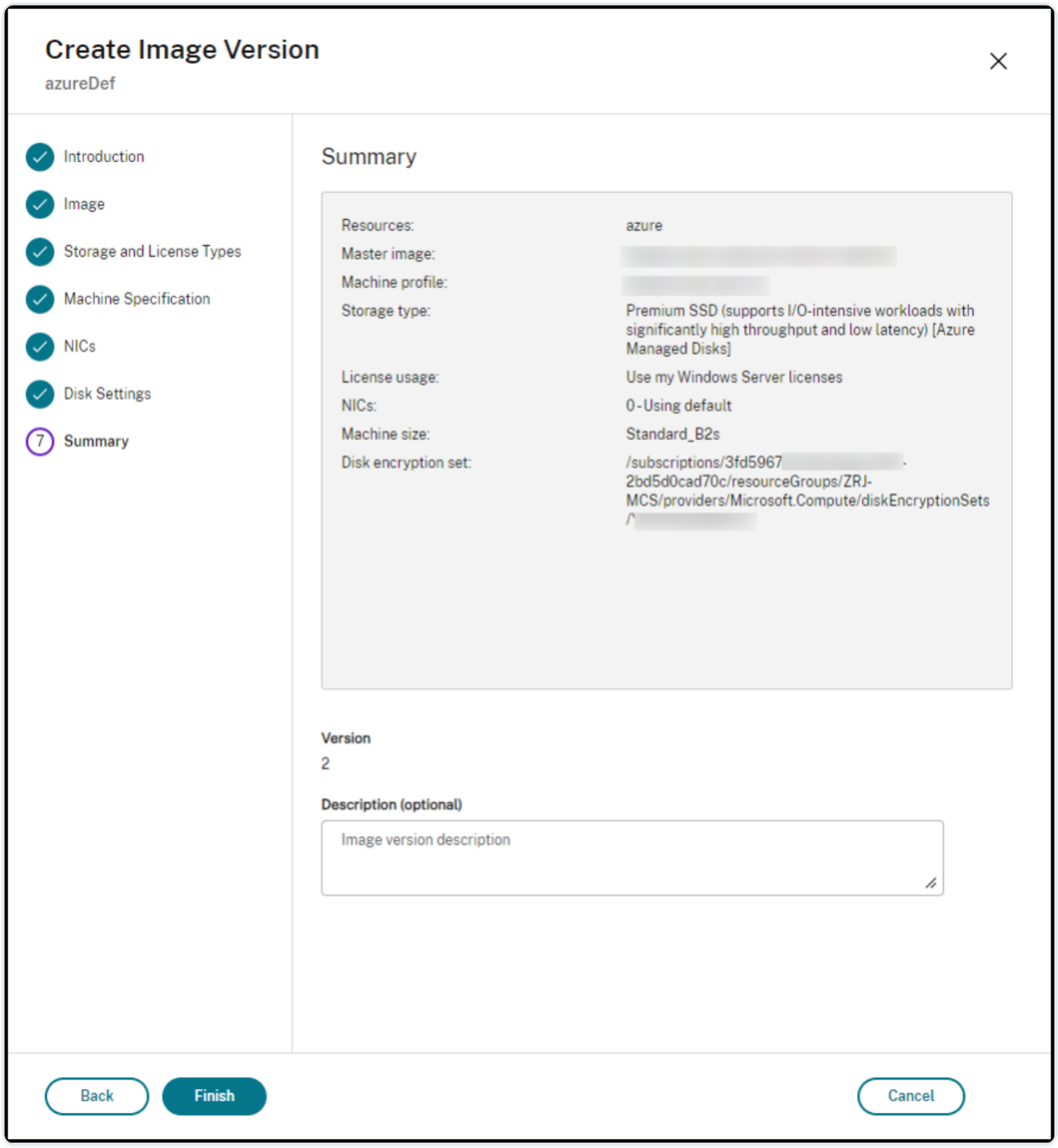
イメージバージョンを作成する

イメージバージョンを使用すると、特定のイメージに対するさまざまなイテレーションや更新を管理できます。この機能により、さまざまな目的のためにイメージの複数のバージョンを維持できます。

初期イメージバージョンからイメージバージョンを作成するには、次の手順を実行します。

> **注:**
>
> すべてのイメージバージョンのホスティングユニットは同じである必要があります。

1. 「**イメージ**」ノードに移動し、イメージバージョンまたはイメージ定義を選択して、「**イメージバージョンの作成**」をクリックします。
2. イメージ定義ページで、ホスティングユニットを変更し、そのイメージバージョンのマスターイメージとマシンプロファイルを再選択できます。
3. イメージバージョンの構成を最初に構成したイメージバージョンと異なるものにしたい場合は、「**イメージバージョンの作成**」ダイアログの「**ストレージとライセンスの種類**」、「**マシン仕様**」、「**NIC**」、「**ディスク設定**」ページで設定を構成します。
4. イメージバージョンの説明を追加します。「**完了**」をクリックします。



注:

何らかの理由でイメージバージョンの作成に失敗した場合、下部にある**トラブルシューティング**タブに**再試行**オプションが表示されます。

共有準備済みイメージ

Azureの異なるホスティングユニット間で準備済みイメージを共有するには、次の手順に従います。

1. イメージバージョンを右クリックし、**Manage Image Share**を選択します。Azure環境内のすべてのホスティングユニットが表示されます。イメージバージョンが作成されたリソースは、すべてのアクションに対して無効になっています。
2. イメージを共有するホスティングユニットを選択し、**保存**をクリックします。**共有ステータス**列には「進行中」と表示されます。
3. 共有ステータスの詳細については、**Resources**タブをクリックします。

> **注:**
>
> イメージバージョンの共有ステータスが進行中の場合、「**イメージバージョンの削除**」または「**イメージ共有の管理**」オプションは無効になります。

「イメージ」ノードからマシンカタログを作成する

「**イメージ**」ノードの「**カタログの作成**」オプションを使用して、イメージバージョンでカタログを作成します。

または、「**Machine Catalogs**」ノードでカタログを作成する際にバージョンを選択し、カタログ作成ワークフローで準備されたイメージオプションにリンクすることもできます。詳細については、(#create-a-machine-catalog-from-the-machine-catalogs-node)「Machine Catalogs」ノードからマシンカタログを作成するを参照してください。

「**イメージ**」ノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. イメージバージョンを選択し、「**Create catalog**」をクリックします。「**Introduction**」ページで「**Next**」をクリックします。
2. 「**Desktop Experience**」ページで、必要なデスクトップエクスペリエンスを選択します。
3. 「**Image**」ページから「**Disk Settings**」ページまで、設定は選択したイメージバージョンに基づいて事前に選択されています。
4. 「**Resource Group**」ページでは、新しいリソースグループを作成するか、既存のリソースグループを使用してこのカタログのリソースを配置するかを選択できます。
5. 以下のページで設定を完了します。
6. 「**Summary**」ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。「**Finish**」をクリックします。
7. 作成したマシンカタログを表示するには、「**Machine Catalogs**」ノードに移動します。

「Machine Catalogs」ノードからマシンカタログを作成する

マシンカタログノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. 左側のナビゲーションペインで「**Machine Catalogs**」をクリックします。
2. 「**Create Machine Catalog**」をクリックします。「**Machine Catalog Setup**」ページが表示されます。「**Introduction**」、「**Machine Type**」、「**Machine Management**」の各ページで「**Next**」をクリックします。
3. 「**Machine Management**」ページで、次の設定を選択します。
    a. 「**電源管理されているマシン（仮想マシンやブレードPCなど）**」を選択します。
    b. 「**Citrixプロビジョニングテクノロジー**」を選択します。次に、「**Citrix Machine Creation Services™**」を選択します。
    c. 「**リソース**」フィールドには、異なるゾーンに属するリソースが一覧表示されます。任意のAzureネットワークリソースを選択し、「**次へ**」をクリックします。
4. 「**イメージ**」ページで、マスターイメージタイプの場合は、次の手順に従います。
    a. マスターイメージを選択します。
    b. マスターイメージの下で、イメージを選択します。ブレードには、リソースと同じリージョンに属するすべてのイメージが一覧表示されます。
    c. 「**完了**」をクリックします。
    d. 準備済みイメージタイプの場合は、「**準備済みイメージ**」を選択します。
    e. 「**準備済みイメージ**」の下で、イメージ定義のイメージバージョンを選択します。必要に応じて、選択した準備済みイメージバージョンにメモを追加します。
    f. イメージバージョン名をクリックします。選択したイメージバージョンの詳細を表示するには、下線が引かれているバージョン番号をクリックします。
    g. 選択したイメージバージョンがマシンプロファイルで構成されている場合は、マシンプロファイルを選択します。選択したイメージバージョンがマシンプロファイルで構成されていない場合、マシンプロファイルを使用することはできません。
5. 次のページで設定を構成します。
6. 「**ディスク設定**」ページで、選択した準備済みイメージがディスク暗号化セットを使用している場合、その暗号化セットを削除することはできませんが、キーを別の暗号化キーに変更することはできます。
7. 「**リソースグループ**」ページで、新しいリソースグループを作成するか、既存のリソースグループを使用して、このカタログのリソースを配置するかを選択できます。

8. 次のページで設定を完了します。
9. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。

PowerShell を使用する

準備済みイメージを作成する

準備済みイメージバージョン仕様を作成するための詳細な PowerShell コマンドは次のとおりです。

1. `Test-ProvImageDefinitionNameAvailable command` を使用して、利用可能なイメージ定義名を確認します。例:

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
```

2. `New-ProvImageDefinition` コマンドを使用してイメージ定義を作成します。例:

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession
```

3. `Add-ProvImageDefinitionConnection` コマンドを使用して、指定されたホスティング接続でイメージ定義の新しい構成を作成します。

   `Add-ProvImageDefinitionConnection` の `CustomProperties` には、次のものが含まれます。これらのパラメーターを使用しない場合、デフォルト値が使用されます。

   - `ResourceGroups`: ベースディスクがあるリソースグループ。
   - `UseSharedImageGallery`: ベースディスクの種類のインジケーター。ACG (イメージ共有) には `true` を、スナップショットには `false` を使用します。
   - `ImageGallery`: ベースディスクがACGイメージバージョンである場合のギャラリー名。

   例:

   - スナップショットと顧客が提供するリソースグループの場合：

```
$CustomerOwnRsourceGroupProperties = @"

<CustomProperties xmlns="http:// schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
```

```
<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="yangj_image" />

</CustomProperties>

"@
```

- ACGと顧客が提供するリソースグループおよびイメージギャラリーの場合：

```
$CustomerOwnAllProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="rg" />

<Property xsi:type="StringProperty" Name="ImageGallery"
Value="gallery" />

</CustomProperties>

"@
```

- ACGと顧客が提供するリソースグループのみの場合：

```
$CustomerOwnResourceGroupProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="rg" />
```

```
</CustomProperties>

"@
```

- Citrix が管理する ACG、リソースグループ、およびイメージギャラリーの場合:

```
$CustomerOwnResourceGroupNothingProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

</CustomProperties>

"@
```

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName Azure28 [-CustomProperties $CustomProperties]
```

4. `New-ProvImageVersion` コマンドを使用してイメージバージョンを作成します。例:

```
New-ProvImageVersion -ImageDefinitionName image1 -Description "version
1"
```

5. `Add-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様をイメージバージョンに追加します。例:

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
ImageVersionNumber  1 -HostingUnitName azure -MasterImagePath "XDHyp:
\HostingUnits\azure\image.folder\azureresourcegroup.resourcegroup\win20
22-snapshot.snapshot"
```

注:

> ホスティングユニットのイメージバージョンには、マスターイメージバージョン仕様を1つだけ追加できます。

6. `New-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様から準備済みイメージバージョン仕様を作成します。例:

```
New-ProvImageVersionSpec

-SourceImageVersionSpecUid  c6e7384c-b2f8-46d6-9519-29a2c57ed3cb

-NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resou
rcegroup\azure-vnet-eastus.virtualprivatecloud\dev.network"}

-ServiceOffering"XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2ms.serviceofferin
g" -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"></CustomProperties>"
-RunAsynchronously
```

7. `Add-ProvImageVersionSpecHostingUnit` コマンドを使用して、すべてのホスティング接続で準備済みイメージバージョン仕様を別のホスティングユニットと共有することもできます。例:

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName AzureWest
```

> **注:**
>
> 1つのホスティングユニットと準備タイプには、準備済みインスタンスを1つのみ持つことができます。

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を作成するためのPowershellコマンドの完全なセットの例:

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession



$CustomProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

    <Property xsi:type="StringProperty" Name="ResourceGroups" Value="rg" /
>

    <Property xsi:type="StringProperty" Name="ImageGallery"
Value="gallery" />

</CustomProperties>

"@



Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName Azure28 -CustomProperties $CustomProperties



$imageVersion = New-ProvImageVersion -ImageDefinitionName image1
-Description "version 1"



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -MasterImagePath "XDHyp:
\HostingUnits\azure28\image.folder\abc.resourcegroup\def-
snapshot.snapshot"
```

```
New-ProvImageVersionSpec -NetworkMapping @{"0" = "XDHyp:
\HostingUnits\azure28\virtualprivatecloud.folder\East
US.region\virtualprivatecloud.folder\studio-mcs-
infrastructure.resourcegroup\studio-mcs-vnet-
eastus.virtualprivatecloud\mcs-dev.network" } -CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Server`" /></CustomProperties>" -ServiceOffering "XDHyp:
\HostingUnits\azure28\serviceoffering.folder\Standard_B2s.serviceoffering"
-SourceImageVersionSpecUid $SourceImageVersionSpec.ImageVersionSpecUid

Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName AzureWest

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

注:

- イメージ定義内のすべてのイメージバージョン仕様は、同じホスティングユニットに属している必要があります。
- イメージバージョンには、マスターイメージバージョン仕様を1つと、準備済みイメージバージョン仕様を1つだけ含めることができます。
- すべてのイメージバージョン仕様にはマシンプロファイルがあるか、またはどのイメージバージョン仕様にもマシンプロファイルがないかのいずれかである必要があります。

準備済みイメージバージョン仕様を使用してカタログを作成する

準備されたイメージバージョン仕様から、`New-ProvScheme`コマンドを使用してMCSマシンカタログを作成します。例：

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
```

```
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>][-ImageAssignmentNote <string>]
```

または、,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>][-ImageAssignmentNote <string>]
```

ACGイメージバージョン仕様を使用したい場合は、`UseSharedImageGallery`を`true`として設定します。例：

```
$provSchemeCustomProperties= @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

    <Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" />

</CustomProperties>

"@

New-ProvScheme -ProvisioningSchemeName assignimage -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `
```

```
    -IdentityPoolUid $IdentityPool.IdentityPoolUid `

    -CleanOnBoot -Scope @() -SecurityGroup @() `

    -ServiceOffering "XDHyp:
\HostingUnits\azure28\serviceoffering.folder\Standard_B2s.serviceoffering"
`

    -NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure28\virtualprivatecloud.folder\East
US.region\virtualprivatecloud.folder\studio-mcs-
infrastructure.resourcegroup\studio-mcs-vnet-
eastus.virtualprivatecloud\mcs-dev.network"} `

    -CustomProperties $provSchemeCustomProperties
```

カタログを作成するためのPowershellコマンドの完全なセットの例：

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "azurecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"



$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "azure.local"
-IdentityPoolName "azurecatalog" -IdentityType "ActiveDirectory"  -
NamingScheme "azure##" -NamingSchemeType "Numeric" -Scope @()



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



$Task = New-ProvScheme -ProvisioningSchemeName azurecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName azure -IdentityPoolName azurecatalog -CleanOnBoot -Scope
@() -SecurityGroup @() -ServiceOffering "XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2s.serviceoffering"
-NetworkMapping @{"0"="XDHyp:
```

```
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resource
group\azure-vnet-eastus.virtualprivatecloud\dev.network"}
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">    <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="true" /><Property
xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"StandardSSD_LRS`" /></CustomProperties>" -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName azurecatalog



Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

暗号化された準備済みイメージをリージョン、サブスクリプション、テナント間で共有する

Azure Compute Gallery (ACG) イメージは、ディスク暗号化セット (DES) で暗号化できます。ACG 共有機能を使用すると、暗号化された準備済みイメージを Azure のリージョン、サブスクリプション、テナント間で共有できます。ターゲットリソースは、準備済みイメージが属するサブスクリプションから、そのリージョン内の DES を選択する必要があります。その後、暗号化された準備済みイメージが共有されているリソースにマシンカタログを作成できます。

暗号化された準備済みイメージを共有するための主要な手順は次のとおりです。

1. 各リージョンでディスク暗号化セット (DES) を作成します。Microsoftドキュメント「Use the Azure portal to enable server-side encryption with customer-managed keys for managed disks」を参照してください。
2. AzureホストとAzure Compute Gallery (ACG) のイメージバージョン用のイメージ定義を作成し、準備済みイメージを暗号化するためのDESを指定します。「Create an image definition and initial image version」を参照してください。
3. 暗号化された準備済みイメージをリージョン、サブスクリプション、テナント間で共有します。Web StudioまたはPowerShellコマンドを使用できます。

暗号化された準備済みイメージが共有されているリソースにマシンカタログを作成できるようになりました。カタログの作成の詳細については、「Create a prepared image machine catalog in Azure」を参照してください。

> **注:**
>
> - プライマリリージョンが暗号化されていない場合、共有リージョンも DES を持つことはできません。
> - 2つのホストユニットが同じリージョンをターゲットとする場合、それらは同じ DES を持ちます。

Web Studioを使用して、暗号化されたイメージをリージョン、サブスクリプション、テナント間で共有する

1. イメージバージョンを右クリックし、 を選択します。リージョンとディスク暗号化セットを持つリソースが一覧表示されます。
2. イメージバージョンと共有するリソースを選択します。イメージバージョンが作成されたリソースは、すべてのアクションに対して無効になっています。リソースに対してDESが構成されていない場合は、ドロップダウンメニューからDESを選択します。

   > **注:**
   >
   > 同じリージョン内のリソースは、同じ暗号化キーを使用する必要があります。

3. をクリックします。
4. 共有ステータスの詳細については、 タブをクリックします。

   > **注:**
   >
   > - イメージバージョンの共有ステータスが進行中の場合、 または オプションは無効になります。
   > - リソースが正常に共有されると、DESは編集できなくなります。

PowerShellを使用して、暗号化されたイメージをリージョン、サブスクリプション、およびテナント間で共有する

`Add-ProvImageVersionSpecHostingUnit` コマンドを使用し、`CustomProperties` パラメーターを追加します。`CustomProperties` で、ターゲットリソースのDESを構成します。準備された暗号化イメージを共有する場合、各リソースは、準備されたイメージが属するサブスクリプションから、そのリージョン内のDESを選択します。例：

```
$CustomProperties = "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">"

 "<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
Value=`"/subscriptions/xxxxxx-7152-46c4-b061-xxxxxx70c/resourceGroups/
resourcegroup1/providers/Microsoft.Compute/diskEncryptionSets/desid1`" /
>"+

 "</CustomProperties>"

Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid <Guid>
-HostingUnitUid <Guid> -CustomProperties $CustomProperties
```

詳細情報

- イメージ管理

次のステップ

- 準備済みイメージマシンカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/manage-prepared-image-machine-catalogs.html)

Red Hat OpenShift で準備済みイメージマシンカタログを作成する

準備済みイメージを作成し、その準備済みイメージを使用して、次の方法で MCS マシンカタログを作成します。

- ウェブスタジオ
- PowerShell コマンド

準備済みイメージを使用して MCS マシンカタログを作成する主な手順は次のとおりです。

1. イメージ定義と初期イメージバージョンを作成します。
2. イメージバージョンを準備済みイメージとして使用してカタログを作成する

Web Studio を使用する

イメージ定義と初期イメージバージョンを作成する

イメージ定義と初期イメージバージョンを作成するには、次の手順を実行します。

1. Studio から、**［イメージ］**ノードに移動し、**［イメージ定義の作成］**をクリックします。**［はじめに］**ページで**［次へ］**をクリックします。
2. **［イメージ定義］**ページで、イメージ定義の**［OSの種類］**と**［セッションの種類］**を指定します。
3. **［イメージ］**ページで、**［リソース］**（設定された接続に適用可能なリソースのみが一覧表示されます）と、イメージバージョンを作成するためのテンプレートとして使用するマスターイメージを選択します。**［マシンプロファイルを使用する］**チェックボックスをオンにして、マシンプロファイルを選択できます。

   > **注:**
   >
   > イメージを選択する前に、マスターイメージに VDA 2311 以降がインストールされており、MCSIO ドライバーが VDA にインストールされていることを確認してください。

4. 「**マシン仕様**」ページで、マシンサイズを選択します。マシンプロファイルを選択した場合、そのマシンプロファイルから派生した仮想CPUカウントが表示され、変更することはできません。マシンプロファイルを選択しない場合、マスターイメージから派生したメモリサイズのみが表示されます。
5. 「**NIC**」ページで、準備イメージのNICを選択します。各NICについて、関連する仮想ネットワークを選択します。ホスティングユニットに関連付けられたNICは、デフォルトで選択されています。
6. 「**Version Description**」ページで、作成された初期イメージバージョンの説明を入力します。
7. 「**概要**」ページで、イメージ定義と作成された初期イメージバージョンの詳細を確認します。イメージ定義の名前と説明を入力します。「**完了**」をクリックします。

イメージバージョンを作成する

イメージバージョンを使用すると、特定のイメージに対するさまざまなイテレーションや更新を管理できます。この機能により、さまざまな目的のためにイメージの複数のバージョンを維持できます。

初期イメージバージョンからイメージバージョンを作成するには、次の手順を実行します。

1. 「**Images**」ノードに移動し、イメージバージョンまたはイメージ定義を選択して、「**Create Image Version**」をクリックします。
2. 「**イメージ**」ページで、このイメージバージョンのマスターイメージを再選択できます。
3. イメージバージョンの構成を、最初に構成されたイメージバージョンと異なるものにしたい場合は、「**イメージバージョンの作成**」ダイアログの「**マシン仕様**」ページと「**NIC**」ページで設定を構成します。
4. イメージバージョンの説明を追加します。「**完了**」をクリックします。

> **注:**
>
> 何らかの理由でイメージバージョンの作成が失敗した場合、下部にある「**トラブルシューティング**」タブに「**再試行**」オプションが表示されます。

「イメージ」ノードからマシンカタログを作成する

「**イメージ**」ノードの「**カタログの作成**」オプションを使用して、イメージバージョンでカタログを作成します。

または、**マシンカタログ**ノードでカタログを作成する際にバージョンを選択し、カタログ作成ワークフローで準備済みイメージオプションにリンクできます。「マシンカタログノードからマシンカタログを作成する」を参照してください(#create-a-machine-catalog-from-the-machine-catalogs-node)

「**イメージ**」ノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. イメージバージョンを選択し、「**カタログの作成**」をクリックします。「**はじめに**」ページで「**次へ**」をクリックします。
2. **マシン管理**ページで**次へ**をクリックします。
3. **デスクトップエクスペリエンス**ページで、必要なデスクトップエクスペリエンスを選択します。
4. **イメージ**ページから**仮想マシン**ページまで、設定は選択したイメージバージョンに基づいて事前に選択されています。
5. 次のページで設定を完了します。
6. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。
7. 作成したマシンカタログを表示するには、**マシンカタログ**ノードに移動します。

「マシンカタログ」ノードからマシンカタログを作成する

マシンカタログノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. 左側のナビゲーションペインで**マシンカタログ**をクリックします。
2. **マシンカタログの作成**をクリックします。**マシンカタログのセットアップ**ページが表示されます。**はじめに**、**マシンタイプ**、**マシン管理**の各ページで**次へ**をクリックします。
3. **イメージ**ページで：
   a. **準備済みイメージ**を選択します。
   b. 「**準備済みイメージ**」の下で、イメージ定義のイメージバージョンを選択します。
   c. イメージバージョン名をクリックします。選択したイメージバージョンの詳細を表示するには、下線が引かれているバージョン番号をクリックします。
4. 次のページで設定を構成します。
5. 「**概要**」ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。「**完了**」をクリックします。

PowerShell を使用する

準備済みイメージを作成する

準備済みイメージバージョン仕様を作成するための詳細な PowerShell コマンドは次のとおりです。

1. `Test-ProvImageDefinitionNameAvailable command` を使用して、利用可能なイメージ定義名を確認します。例:

   ```
   Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
   ```

2. `New-ProvImageDefinition` コマンドを使用してイメージ定義を作成します。例:

   ```
   New-ProvImageDefinition -ImageDefinitionName image2 -OsType Windows
   -VdaSessionSupport SingleSession
   ```

3. `Add-ProvImageDefinitionConnection`コマンドを使用して、指定されたホスティング接続でイメージ定義の新しい構成を作成します。例：

```
Add-ProvImageDefinitionConnection -ImageDefinitionUid
$imageDef.ImageDefinitionUid -HypervisorConnectionUid
"00000000-0000-0000-0000-000000000000"
```

4. `New-ProvImageVersion` コマンドを使用してイメージバージョンを作成します。例:

```
New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"
```

5. `Add-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様をイメージバージョンに追加します。例:

```
Add-ProvImageVersionSpec -MasterImagePath "XDHyp:
\HostingUnits\YourHostingUnitName\YourMasterImage.vm" -HostingUnitUid
"11111111-1111-1111-1111-111111111111" -ImageVersionUid
$imageVersion.ImageVersionUid
```

> **注:**
>
> ホスティングユニットのイメージバージョンには、マスターイメージバージョン仕様を1つだけ追加できます。

6. `New-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様から準備済みイメージバージョン仕様を作成します。例：

```
New-ProvImageVersionSpec -SourceImageVersionSpecUid
$masterImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{"1" =
"XDHyp:
\HostingUnits\YourHostingUnitName\YourNamespaceName.namespace\YourNetwo
rkAttachmentDefinition.network" }
```

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を作成するためのPowershellコマンドの完全なセットの例:

```
$imageDef = New-ProvImageDefinition -ImageDefinitionName "ImageDefinition"
-OsType "Windows" -VDASessionSupport "MultiSession"
```

```
$task = Add-ProvImageDefinitionConnection -ImageDefinitionUid
$imageDef.ImageDefinitionUid -HypervisorConnectionUid
"00000000-0000-0000-0000-000000000000"



$imageVersion = New-ProvImageVersion -ImageDefinitionName
"ImageDefinition"




$masterImageVersionSpec = Add-ProvImageVersionSpec -MasterImagePath
"XDHyp:\HostingUnits\YourHostingUnitName\YourMasterImage.vm"
-HostingUnitUid "11111111-1111-1111-1111-111111111111" -ImageVersionUid
$imageVersion.ImageVersionUid




$newProvImageVersionSpecResult = New-ProvImageVersionSpec
-SourceImageVersionSpecUid $masterImageVersionSpec.ImageVersionSpecUid
-NetworkMapping @{"1" = "XDHyp:
\HostingUnits\YourHostingUnitName\YourNamespaceName.namespace\YourNetworkA
ttachmentDefinition.network" }
```

注:

- イメージ定義内のすべてのイメージバージョン仕様は、同じホスティングユニットに属している必要があります。
- イメージバージョンには、マスターイメージバージョン仕様を1つ、準備済みイメージバージョン仕様を1つだけ含めることができます。

- すべてのイメージバージョン仕様はマシンプロファイルを持つか、またはどのイメージバージョン仕様もマシンプロファイルを持たないかのいずれかである必要があります。

準備済みイメージバージョン仕様を使用してカタログを作成する

`New-ProvScheme`コマンドを使用して、準備済みイメージバージョン仕様からMCSマシンカタログを作成します。例:

```
$getProvImageVersionSpecResult = Get-ProvImageVersionSpec
-ImageVersionSpecUid $newProvImageVersionSpecResult.ImageVersionSpecUid



New-ProvScheme -ImageVersionSpecUid
$newProvImageVersionSpecResult.ImageVersionSpecUid -ProvisioningSchemeName
"ProvSchemeImageDecoupling" -HostingUnitName "YourHostingUnitName"
-IdentityPoolName "YourIdentityPoolName" -NetworkMapping @{"1" = "XDHyp:
\HostingUnits\YourHostingUnitName\YourNamespaceName.namespace\YourNetworkA
ttachmentDefinition.network"}
```

詳細情報

- イメージ管理

次のステップ

- 準備済みイメージマシンカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/manage-prepared-image-machine-catalogs.html)

VMware で準備済みイメージのマシンカタログを作成する

準備済みイメージを作成し、その準備済みイメージを使用して、以下によって MCS マシンカタログを作成します。

- ウェブスタジオ
- (#use-powershell)

準備済みイメージを使用して MCS マシンカタログを作成する主な手順は次のとおりです。

1. イメージ定義と初期イメージバージョンを作成します。
2. イメージバージョンを準備済みイメージとして使用してカタログを作成します。

Web Studio を使用する

イメージ定義と初期イメージバージョンを作成する

イメージ定義と初期イメージバージョンを作成するには、次の手順を実行します。

1. Studio から、**イメージ**ノードに移動し、**イメージ定義の作成**をクリックします。**はじめに**ページで**次へ**をクリックします。
2. **イメージ定義**ページで、イメージ定義の**OS タイプ**と**セッションタイプ**を指定します。
3. **イメージ**ページで、**リソース**（設定された接続に適用可能なリソースのみが一覧表示されます）と、イメージバージョンを作成するためのテンプレートとして使用するマスターイメージを選択します。**マシンプロファイルを使用する**チェックボックスをオンにして、マシンプロファイルを選択できます。

   > **注:**
   >
   > イメージを選択する前に、マスターイメージにVDA 2311以降がインストールされており、MCSIOドライバーがVDAにインストールされていることを確認してください。

4. 「**マシン仕様**」ページで、マシンサイズを選択します。マシンプロファイルを選択した場合、マシンプロファイルから派生した仮想CPUカウントが表示され、変更できません。マシンプロファイルを選択しない場合、マスターイメージから派生したメモリサイズのみが表示されます。
5. 「**NIC**」ページで、準備イメージのNICを選択または追加します。各NICについて、関連する仮想ネットワークを選択します。マシンプロファイルを選択しない場合、マスターイメージに関連付けられたNICがデフォルトで選択されます。マシンプロファイルを選択した場合、NICはマシンプロファイルから派生し、その数は変更できません。
6. 「**バージョン説明**」ページで、作成された初期イメージバージョンの説明を入力します。
7. 「**概要**」ページで、イメージ定義と作成された初期イメージバージョンの詳細を確認します。イメージ定義の名前と説明を入力します。「**完了**」をクリックします。

イメージバージョンを作成する

イメージバージョンを使用すると、特定のイメージに対するさまざまなイテレーションや更新を管理できます。この機能により、さまざまな目的のためにイメージの複数のバージョンを維持できます。

初期イメージバージョンからイメージバージョンを作成するには、次の手順を実行します。

1. 「**イメージ**」ノードに移動し、イメージバージョンまたはイメージ定義を選択して、「**イメージバージョンを作成**」をクリックします。
2. 「**イメージ**」ページで、同じホスティング接続内のホスティングユニットを変更し、そのイメージバージョンのマスターイメージとマシンプロファイルを再選択できます。
3. イメージバージョンの構成を、最初に構成されたイメージバージョンと異なるものにしたい場合は、「**イメージバージョンを作成**」ダイアログの「**マシン仕様**」ページと「**NIC**」ページで設定を構成します。
4. イメージバージョンの説明を追加します。「**完了**」をクリックします。

> **注:**
>
> 何らかの理由でイメージバージョンの作成に失敗した場合、下部にある「**トラブルシューティング**」タブに「**再試行**」オプションが表示されます。

準備済みイメージを共有する

前提条件

準備済みイメージの共有は、コールドマイグレーションを使用して vCenter Server インスタンス間でイメージを複製します。異なるホスティング接続に属するホスティングユニットには、次の前提条件が適用されます。

- vCenter Server 間でのコールドマイグレーション: コールドマイグレーションには、両方の環境でクロス vCenter マイグレーションのサポートが必要です。
  - 両方のvCenter ServerはvSphere 7.0以降を実行している必要があります (vSphere 8.0以降を推奨)。
  - 拡張リンクモードは不要です。

  ポート要件: マイグレーションのために次のポートが開いていることを確認してください。

送信元	宛先	ポート	プロトコル	目的
ソース vCenter サーバー	ターゲット vCenter Server	443	TCP	vCenter間の API通信
ソースESXiホスト	ターゲット ESXiホスト	902	TCP	NFC (Network File Copy) データ転送

送信元	宛先	ポート	プロトコル	目的
ソースESXiホスト	ターゲットESXiホスト	8000	TCP	vMotionトラフィック

> **注:**
>
> ポートは双方向に開いている必要があります。移行では主に、データにNFC（ポート902）、管理にポート443を使用します。パスによってはポート8000が使用される場合があります。ソースvCenterは、クローン操作中にターゲットのSSL証明書サムプリントを検証する必要があります。

VMkernelアダプターの構成:

ESXIホスト	必要なサービス
ソースESXiホスト	プロビジョニングまたは管理
ターゲットESXiホスト	ソースと同じサービス (プロビジョニングまたは管理)

両側でVMkernelアダプターに同じトラフィックサービス（プロビジョニングまたは管理）を有効にする必要があります。不一致は移行の失敗を引き起こします。

vSphere Client を使用して、**Host > Configure > Networking > VMkernel adapters** の設定を確認します。

既知の制限事項：カスタムストレージポリシーは、vCenter間レプリケーション中に保持されません。ターゲットデータストアのデフォルトストレージポリシーが適用されます。

- vTPM対応マシンプロファイル：キープロバイダーの互換性。vTPMを持つプロファイルの場合、両方のvCenter Serverが互換性のあるキープロバイダーにアクセスできる必要があります。

要件	詳細
同じキープロバイダーへのアクセス	宛先vCenterは、ソースと同じキープロバイダーにアクセスできるか、Native Key

要件	詳細
	Providerをブリッジとして使用する必要があります。
キーマテリアル	外部KMSの場合：両方のvCenterは同じKMSクラスター（またはキーマテリアルを共有するKMSクラスター）に登録されている必要があります。
ネイティブキープロバイダー	両方のvCenter Serverでネイティブキープロバイダーを構成します。各vCenterのネイティブキープロバイダーは独立していますが、vSphereはこの組み合わせをvCenter間操作に受け入れます。ネイティブキープロバイダーは、ソースと宛先が外部KMSを共有していない場合でもブリッジとして機能できます。ネイティブキープロバイダーは、使用する前に両方のvCenterでバックアップする必要があります。

注:

ネイティブキープロバイダーは最も簡単なオプションです。両方のサーバーで構成し、バックアップしてください。外部KMSを使用する場合は、両方のvCenterが同じクラスターまたはキーマテリアルを共有していることを確認してください。**vTPM対応カタログのイメージ共有を有効にする前に、vSphere ClientのvCenter > 構成 > セキュリティ > キープロバイダーでキープロバイダーの構成を確認してください。**

準備済みイメージを異なるホストユニット間で共有する

準備済みイメージを異なるホスティングユニット間で共有するには、次の手順に従います。

1. イメージバージョンを右クリックし、**イメージ共有の管理**を選択します。VMware環境内のすべてのホスティングユニットが表示されます。イメージバージョンが作成された元となるリソースは、いかなる操作も無効になっています。
2. イメージを共有したいホスティングユニットを選択し、**保存**をクリックします。 **共有ステータス**列に**進行中**と表示されます。
3. 共有ステータスの詳細については、下部にある**リソース**タブをクリックします。

注:

イメージバージョンの共有ステータスが進行中の場合、**イメージバージョンの削除**または**イメージ共有の管理**オプションは無効になります。 異なるVMware接続内のホスティングユニットとイメージを共有するには、次の要件が満たされていることを確認してください。

- 2つの接続が相互に通信できること。
- ハイパーバイザーのバージョンが一貫していること。
- ソースホストとターゲットホストの両方の管理VMkernelアダプターでプロビジョニングサービスが有効になっていること。VMware vSphere Clientでのナビゲーションパスは、**Host > Configure > Networking > VMkernel adapters**です。

「イメージ」ノードからマシンカタログを作成する

イメージノードの**カタログの作成**オプションを使用して、イメージバージョンでカタログを作成します。

または、**マシンカタログ**ノードでカタログを作成する際にバージョンを選択し、カタログ作成ワークフローで準備されたイメージオプションにリンクすることもできます。マシンカタログノードからマシンカタログを作成するを参照してください。

「**イメージ**」ノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. イメージバージョンを選択し、「**カタログの作成**」をクリックします。「**はじめに**」ページで「**次へ**」をクリックします。
2. **デスクトップエクスペリエンス**ページで、必要なデスクトップエクスペリエンスを選択します。
3. **イメージ**ページから**仮想マシン**ページまで、設定は選択したイメージバージョンに基づいて事前に選択されています。
4. 次のページで設定を完了します。
5. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。
6. **マシンカタログ**ノードに移動して、作成されたマシンカタログを表示します。

「マシンカタログ」ノードからマシンカタログを作成する

マシンカタログノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. 左側のナビゲーションペインで**マシンカタログ**をクリックします。
2. **マシンカタログの作成**をクリックします。**マシンカタログのセットアップ**ページが表示されます。**はじめに**、**マシンタイプ**、**マシン管理**の各ページで**次へ**をクリックします。
3. **イメージ**ページで:
   a. **準備されたイメージ**を選択します。
   b. **準備されたイメージ**の下で、イメージ定義のイメージバージョンを選択します。
   c. 画像バージョン名をクリックします。選択した画像バージョンの詳細を表示するには、下線が引かれているバージョン番号をクリックします。
   d. 選択した画像バージョンがマシンプロファイルで構成されている場合は、マシンプロファイルを選択します。選択した画像バージョンがマシンプロファイルで構成されていない場合、マシンプロファイルを使用することを選択できません。
4. 次のページで設定を構成します。
5. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。

PowerShell を使用する

準備済みイメージを作成する

準備済みイメージバージョン仕様を作成するための詳細な PowerShell コマンドは次のとおりです。

1. `Test-ProvImageDefinitionNameAvailable command` を使用して、利用可能なイメージ定義名を確認します。例:

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
```

2. `New-ProvImageDefinition` コマンドを使用してイメージ定義を作成します。例:

```
New-ProvImageDefinition -ImageDefinitionName image2 -OsType Windows
-VdaSessionSupport SingleSession
```

3. `Add-ProvImageDefinitionConnection`コマンドを使用して、指定されたホスティング接続でイメージ定義の新しい構成を作成します。例：

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image2
-HypervisorConnectionName VMware
```

4. `New-ProvImageVersion` コマンドを使用してイメージバージョンを作成します。例:

```
New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"
```

5. `Add-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様をイメージバージョンに追加します。例:

```
$MasterImagePath = "XDHyp:\HostingUnits\vmware\win10-master.vm\win10-
master-snap.snapshot"

$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageVersion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName vmware
-MasterImagePath $MasterImagePath
```

> **注:**
>
> ホスティングユニットのイメージバージョンには、マスターイメージバージョン仕様を1つだけ追加できます。

6. `New-ProvImageVersionSpec`コマンドを使用して、マスターイメージバージョン仕様から準備済みイメージバージョン仕様を作成します。例：

```
New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping
@{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-VM Network.network"}
-VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
```

7. `Add-ProvImageVersionSpecHostingUnit`コマンドを使用して、同じホスティング接続内の別のホスティングユニットと、準備済みイメージバージョン仕様を共有することもできます。例：

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName VMwareabc
```

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を作成するための PowerShell コマンドの完全なセットの例:

```
New-ProvImageDefinition -ImageDefinitionName image2 -OsType Windows
-VdaSessionSupport Single



Add-ProvImageDefinitionConnection -ImageDefinitionName image2
-HypervisorConnectionName VMware



$imageVersion = New-ProvImageVersion -ImageDefinitionName image2



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -MasterImagePath "XDHyp:\HostingUnits\vmware\shuaiz-win10-
master.vm\shuaiz-win10-master-snap.snapshot"



New-ProvImageVersionSpec -SourceImageVersionSpecUid
$SourceImageVersionSpec.ImageVersionSpecUid `

    -NetworkMapping @{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-
VMNetwork.network"} `

    -VMCpuCount 2 -VMMemoryMB 4096
```

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName VMwareabc

 $PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

注:

- イメージ定義内のすべてのイメージバージョン仕様は、同じホスティングユニットに属している必要があります。
- イメージバージョンには、マスターイメージバージョン仕様を1つと、準備済みイメージバージョン仕様を1つのみ含めることができます。
- すべてのイメージバージョン仕様はマシンプロファイルを持つか、またはどのイメージバージョン仕様もマシンプロファイルを持たないかのいずれかである必要があります。

準備済みイメージバージョン仕様を使用してカタログを作成する

`New-ProvScheme`コマンドを使用して、準備済みイメージバージョン仕様からMCSマシンカタログを作成します。例：

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>][-ImageAssignmentNote <string>]
```

または、,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
```

```
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>][-ImageAssignmentNote <string>]
```

VMwareで準備されたイメージバージョンの仕様を使用してカタログを作成する例:

```
New-ProvScheme -ProvisioningSchemeName assignimage -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid `

    -HostingUnitName $hostingunit.c-IdentityPoolName
$IdentityPool.IdentityPoolName `

    -CleanOnBoot -Scope @() -SecurityGroup @() -VMCpuCount 2 -VMMemoryMB
8192 `

    -NetworkMapping @{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-VM
Network.network"}
```

カタログを作成するためのPowershellコマンドの完全なセットの例：

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "vmwarecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"

$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain
"vmware.local" -IdentityPoolName "vmwarecatalog" -IdentityType
"ActiveDirectory"  -NamingScheme "vmware##" -NamingSchemeType "Numeric"
-Scope @()

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image2 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"

$Task = New-ProvScheme -ProvisioningSchemeName vmwarecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName vmware -IdentityPoolName vmwarecatalog -CleanOnBoot
-Scope @() -SecurityGroup @() -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vmware\\DSwitch-VM Network.network"} -VMCpuCount 2
-VMMemoryMB 4096 -RunAsynchronously
```

```
Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName vmwarecatalog

Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

詳細情報

- イメージ管理

次のステップ

- 準備済みイメージマシンカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/manage-prepared-image-machine-catalogs.html)

XenServer® で準備済みイメージのマシンカタログを作成する

準備済みイメージを作成し、その準備済みイメージを使用して、次の方法でMCSマシンカタログを作成します。

- ウェブスタジオ
- (#use-powershell)

準備済みイメージを使用して MCS マシンカタログを作成する主な手順は次のとおりです。

1. イメージ定義と初期イメージバージョンを作成します。
2. イメージバージョンを準備済みイメージとして使用してカタログを作成します。

Web Studio を使用する

イメージ定義と初期イメージバージョンを作成する

イメージ定義と初期イメージバージョンを作成するには、次の手順を実行します。

1. Studioから、**イメージ**ノードに移動し、**イメージ定義の作成**をクリックします。**はじめに**ページで**次へ**をクリックします。
2. **イメージ定義**ページで、イメージ定義の**OSの種類**、**セッションの種類**、および**接続**を指定します。

3. **イメージ**ページで、**リソース**（設定された接続に適用可能なリソースのみが一覧表示されます）と、イメージバージョンを作成するためのテンプレートとして使用するマスターイメージを選択します。

   > **注:**
   >
   > - イメージを選択する前に、マスターイメージにVDA 2311以降がインストールされており、VDAにMCSIOドライバーがインストールされていることを確認してください。

4. 「**マシン仕様**」ページでは、マスターイメージから派生したメモリサイズのみが表示され、必要に応じて変更できます。
5. 「**NIC**」ページで、準備イメージのNICを選択します。各NICについて、関連する仮想ネットワークを選択します。マスターイメージに関連付けられているNICは、デフォルトで選択されています。
6. 「**バージョン説明**」ページで、作成された初期イメージバージョンの説明を入力します。
7. 「**概要**」ページで、イメージ定義と作成された初期イメージバージョンの詳細を確認します。イメージ定義の名前と説明を入力します。「**完了**」をクリックします。

イメージバージョンを作成する

イメージバージョンを使用すると、特定のイメージに対するさまざまなイテレーションや更新を管理できます。この機能により、さまざまな目的のためにイメージの複数のバージョンを維持できます。

初期イメージバージョンからイメージバージョンを作成するには、次の手順を実行します。

1. 「**イメージ**」ノードに移動し、イメージバージョンまたはイメージ定義を選択して、「**イメージバージョンの作成**」をクリックします。
2. 「**イメージ**」ページで、このイメージバージョンのマスターイメージを再選択できます。
3. イメージバージョンの構成を、最初に構成されたイメージバージョンと異なるものにする場合は、「**イメージバージョンの作成**」ダイアログの「**マシン仕様**」と「**NIC**」で設定を構成します。
4. イメージバージョンの説明を追加します。「**完了**」をクリックします。

> **注:**

> 何らかの理由でイメージバージョンの作成に失敗した場合、下部にある「**トラブルシューティング**」タブに「**再試行**」オプションが表示されます。

「イメージ」ノードからマシンカタログを作成する

「**イメージ**」ノードの「**カタログの作成**」オプションを使用して、イメージバージョンを使用してカタログを作成します。

または、**マシンカタログ**ノードでカタログを作成する際にバージョンを選択し、カタログ作成ワークフローで準備済みイメージオプションにリンクできます。「マシンカタログノードからマシンカタログを作成する」を参照してください。(#create-a-machine-catalog-from-the-machine-catalogs-node)

「**イメージ**」ノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. イメージバージョンを選択し、**「カタログの作成」をクリックします。「はじめに」ページで**「次へ」**をクリックします。
2. **「マシン管理」ページで**「次へ」**をクリックします。
3. **「デスクトップエクスペリエンス」**ページで、必要なデスクトップエクスペリエンスを選択します。
4. **「イメージ」ページから**「仮想マシン」**ページまで、設定は選択したイメージバージョンに基づいて事前選択されています。
5. 次のページで設定を完了します。
6. **「概要」ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**「完了」**をクリックします。
7. **「マシンカタログ」**ノードに移動して、作成されたマシンカタログを表示します。

「マシンカタログ」ノードからマシンカタログを作成する

マシンカタログノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. 左側のナビゲーションペインで**マシンカタログ**をクリックします。
2. **マシンカタログの作成**をクリックします。**マシンカタログのセットアップ**ページが表示されます。**はじめに**、**マシンタイプ**、**マシン管理**の各ページで**次へ**をクリックします。
3. **イメージ**ページで：
   a. **準備済みイメージ**を選択します。
   b. 「**準備済みイメージ**」の下で、イメージ定義のイメージバージョンを選択します。

c. イメージバージョンを選択します。選択したイメージバージョンの詳細を表示するには、下線が引かれているバージョン番号をクリックします。

4. 次のページで設定を完了します。
5. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。

PowerShell を使用する

準備済みイメージを作成する

準備済みイメージバージョン仕様を作成するための詳細な PowerShell コマンドは次のとおりです。

1. `Test-ProvImageDefinitionNameAvailable command` を使用して、利用可能なイメージ定義名を確認します。例:

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName xenimage1
```

2. `New-ProvImageDefinition` コマンドを使用してイメージ定義を作成します。例:

```
$ImageDefintion = New-ProvImageDefinition -ImageDefinitionName
xenimage1 -OsType Windows -VdaSessionSupport SingleSession
```

3. `Add-ProvImageDefinitionConnection` コマンドを使用して、指定されたホスティング接続でイメージ定義の新しい構成を作成します。

```
Add-ProvImageDefinitionConnection -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -HypervisorConnectionName
XenServer1
```

4. `New-ProvImageVersion` コマンドを使用してイメージバージョンを作成します。例:

```
$ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"
```

5. `Add-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様をイメージバージョンに追加します。例:

```
$MasterImagePath = "XDHyp:\HostingUnits\xenhu \win10-master.vm\win10-
master-snap.snapshot"

$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName xenhu
-MasterImagePath $MasterImagePath
```

注:

ホスティングユニットのイメージバージョンには、マスターイメージバージョン仕様を1つだけ追加できます。

6. `New-ProvImageVersionSpec`コマンドを使用して、マスターイメージバージョン仕様から準備済みイメージバージョン仕様を作成します。例：

```
New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping
@{"0"="XDHyp:\HostingUnits\xenhu\VM Network.network"}

-VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
```

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を作成するためのPowershellコマンド一式の例:

```
$ImageDefintion = New-ProvImageDefinition -ImageDefinitionName xenimage1
-OsType Windows -VdaSessionSupport SingleSession




Add-ProvImageDefinitionConnection -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -HypervisorConnectionName XenServer1



$ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"
```

```
$MasterImagePath = "XDHyp:\HostingUnits\xenhu \win10-master.vm\win10-
master-snap.snapshot"



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName xenhu -MasterImagePath
$MasterImagePath




New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{"0"="XDHyp:
\HostingUnits\xenhu\VM Network.network"}

 -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
```

注：

- イメージバージョンは、マスターイメージバージョン仕様を1つ、準備済みイメージバージョン仕様を1つのみ持つことができます。
- すべてのイメージバージョン仕様は、マシンプロファイルを持つか、またはどのイメージバージョン仕様もマシンプロファイルを持たないかのいずれかである必要があります。

準備済みイメージバージョン仕様を使用してカタログを作成する

`New-ProvScheme`コマンドを使用して、準備済みイメージバージョン仕様からMCSマシンカタログを作成します。例：

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
```

```
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

または、,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

XenServer で準備済みイメージバージョンの仕様を使用してカタログを作成する例：

```
New-ProvScheme -ProvisioningSchemeName assignimage -imageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid 1 `

  -HostingUnitName xenhu -IdentityPoolName poo1 `

  -CleanOnBoot -Scope @() -SecurityGroup @() -VMCpuCount 2 -VMMemoryMB
8192 `

  -NetworkMapping @{"0"="XDHyp:\HostingUnits\xenhu\VM Network.network"}
```

カタログを作成するためのPowershellコマンド一式の例：

```
$CatalogName = "XenCatalog"

$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" `

  -Name $CatalogName -PersistUserChanges "Discard" -ProvisioningType "MCS"
-Scope @() -SessionSupport "MultiSession"
```

```
$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "xen.local"
-IdentityPoolName $CatalogName `

  -IdentityType "ActiveDirectory"  -NamingScheme "xen##" -NamingSchemeType
"Numeric" -Scope @()




$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
xenimage1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"




$Task = New-ProvScheme -ProvisioningSchemeName $CatalogName
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid `

  -HostingUnitName xenhu -IdentityPoolName $CatalogName -CleanOnBoot
-Scope @() -SecurityGroup @() `

  -NetworkMapping @{"0"="XDHyp:\HostingUnits\xenhu\VM Network.network"}
-VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName $CatalogName




Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

詳細情報

- イメージ管理

次のステップ

- 準備済みイメージマシンカタログの管理

準備済みイメージのマシンカタログを管理する

既存のMCSマシンカタログを別の準備済みイメージで更新し、イメージ定義とバージョンを管理するには、以下を使用します。

- ウェブスタジオ
- PowerShell

Web Studioを使用する

マシンカタログを別の準備済みイメージで更新する

既存のMCSマシンカタログを別の準備済みイメージで更新するには、次の手順を実行します。

1. 左側のナビゲーションペインで をクリックし、更新するマシンカタログを選択します。右クリックして を選択します。
2. **Image** ページで、準備済みイメージを選択します。必要に応じて、選択した準備済みイメージにメモを追加します。

   > **注:**
   >
   > Azureに適用：ACGが有効になっていないイメージを選択し、後で **Place prepared image in Azure Compute Gallery** チェックボックスを選択して、イメージをギャラリーに配置することもできます。

3. 以前に割り当てられた準備済みイメージにロールバックするには、ウィザードの下部にある **Use previous image assignment for quick rollback** をクリックします。

   新しいウィンドウが開き、利用可能なすべての履歴イメージ割り当てのリストが表示されます。リストからイメージを選択すると、イメージページの準備済みイメージツリーで対応するバージョンが自動的に選択されます。

4. **ロールアウト戦略**ページで、選択した準備済みイメージでこのカタログを更新するタイミングを選択します。
5. ページで詳細を確認します。 をクリックします。

カタログに加えられたイメージ変更の履歴を確認できます。履歴を表示するには、次の手順を実行します。

1. マシンカタログを選択します。
2. タブの フィールドで、 をクリックします。

イメージ定義とバージョンを管理する

作成されたさまざまなイメージバージョンと定義の使用を管理するために、イメージ定義とバージョンを編集および削除できます。

イメージ定義を編集する

イメージ定義の名前と説明を編集できます。

イメージ定義を編集するには、次の手順を実行します。

1. **イメージ**ノードに移動し、イメージ定義を選択して、**イメージ定義の編集**を選択します。

イメージバージョンを編集する

イメージバージョンの説明を編集して、そのイメージバージョンの目的を指定できます。

イメージバージョンを編集するには、次の手順を実行します。

1. **イメージ**ノードに移動し、イメージバージョンを選択して、**説明の編集**を選択します。

イメージバージョンを削除する

イメージバージョンを削除するには、次の手順を実行します。

1. 「**イメージ**」ノードに移動し、イメージバージョンを選択し、「**イメージバージョンの削除**」を選択します。

> **注:**
>
> マシンカタログで使用されているイメージバージョンは削除できません。

イメージ定義を削除する

イメージ定義を削除するには、次の手順を実行します。

1. 「**イメージ**」ノードに移動し、イメージ定義を選択し、「**イメージ定義の削除**」を選択します。

> **注:**
>
> イメージバージョンが含まれているイメージ定義は削除できません。

PowerShell を使用する

準備されたイメージバージョンスペックを使用してカタログを更新する

`Set-ProvSchemeImage` コマンドを使用してカタログを更新できます。例:

```
Set-ProvSchemeImage -ProvisioningSchemeUid <Guid> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess][-
ImageAssignmentNote <string>]
```

または、,

```
Set-ProvSchemeImage -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess][-
ImageAssignmentNote <string>]
```

カタログを更新するためのPowerShellコマンドの完全なセットの例：

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 2 -Filter "PreparationType -eq 'Mcs'"



Set-ProvSchemeImage -ProvisioningSchemeName azurecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-RunAsynchronously -ImageAssignmentNote "Update from VST team"
```

プロビジョニングスキームのイメージ変更履歴を取得する

```
Get-ProvSchemeImageVersionSpecHistory -ProvisioningSchemeName azurecatalog
```

イメージ定義、イメージバージョン、および準備されたイメージバージョンスペックを削除する

イメージ定義、イメージバージョン、および準備済みイメージバージョンスペックを削除する前に、以下を考慮してください。

- イメージ定義にイメージバージョンが含まれている場合、そのイメージ定義は削除できません。
- イメージバージョンにイメージバージョンスペックが含まれている場合、そのイメージバージョンは削除できません。
- マスターイメージバージョンスペックが他の準備済みイメージバージョンスペックによって使用されている場合、そのマスターイメージバージョンスペックは削除できません。
- 準備済みイメージバージョンスペックがMCSマシンカタログによって使用されている場合、その準備済みイメージバージョンスペックは削除できません。
- ホスティングユニットが他の準備済みイメージバージョンスペックによって使用されている場合、そのホスティングユニットは削除できません。

詳細な手順は次のとおりです。

1. マシンカタログを削除します。例：

```
Remove-ProvScheme -ProvisioningScheneName decouplingCatalog
```

2. 共有準備済みイメージバージョンスペックを削除します。例：

```
Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid <uid>
-HostingUnitName AzureWest
```

3. 準備済みイメージバージョンスペックを削除します。例：

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec
-ImageDefinitionName image1 -ImageVersionNumber 1 -Filter
"PreparationType -eq 'Mcs'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
```

4. マスターイメージバージョンスペックを削除します。例：

```
$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronousl
```

> **注：**
>
> マスターイメージバージョンスペックは、関連付けられた準備済みイメージバージョンスペックがない場合にのみ削除できます。

5. イメージバージョンを削除します。例：

```
Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber
1
```

6. 指定されたホスティング接続内のイメージ定義の構成を削除します。例：

```
Remove-ProvImageDefinitionConnection -ImageDefinitionName xx
-HypervisorConnectionName xxx
```

7. イメージ定義を削除します。例:

```
Remove-ProvImageDefinition -ImageDefinitionName image1
```

準備されたイメージがホストユニット間で共有されていない場合のPowerShellコマンドの完全なセットの例:

```
Remove-ProvScheme -ProvisioningSchemeName decouplingCatalog



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"
```

```
Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously


$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"


Remove-ProvImageVersionSpec -ImageVersionSpecUid
$MasterImageVersionSpec.ImageVersionSpecUid -RunAsynchronously


Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber 1


Remove-ProvImageDefinition -ImageDefinitionName image1
```

準備されたイメージがホストユニット間で共有されている場合のPowerShellコマンドの完全なセットの例:

```
Remove-ProvScheme -ProvisioningSchemeName decouplingCatalog


Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid <uid>

-HostingUnitName AzureWest


$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"


Remove-ProvImageVersionSpec -ImageVersionSpecUid
```

```
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously



$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$MasterImageVersionSpec.ImageVersionSpecUid -RunAsynchronously



Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber 1



Remove-ProvImageDefinitionConnection -ImageDefinitionName xx
-HypervisorConnectionName xxx



Remove-ProvImageDefinition -ImageDefinitionName image1
```

イメージ定義とイメージバージョンの管理

イメージ定義の名前変更と編集、およびイメージバージョンの編集が可能です。

- `Rename-ProvImageDefinition`コマンドを使用してイメージ定義の名前を変更します。例:

  ```
  Rename-ProvImageDefinition -ImageDefinitionUid <Guid>
  -NewImageDefinitionName <string>
  ```

  または、,

  ```
  Rename-ProvImageDefinition -ImageDefinitionName <string>
  -NewImageDefinitionName <string>
  ```

- `Set-ProvImageDefinition`コマンドを使用してイメージ定義を編集します。例:

```
Set-ProvImageDefinition -ImageDefinitionUid <Guid> [-Description
<string>]
```

または、,

```
Set-ProvImageDefinition -ImageDefinitionName <string> [-Description
<string>]
```

- `Set-ProvImageVersion`コマンドを使用してイメージバージョンを編集します。例:

```
Set-ProvImageVersion -ImageVersionUid <Guid> [-Description <string>]
```

または、,

```
Set-ProvImageVersion -ImageDefinitionName <string> -ImageVersionNumber
<int> [-Description <string>]
```

イメージ定義、イメージバージョン、準備されたイメージバージョンの仕様、およびプロビジョニングスキームの詳細を取得する

- `Get-ProvImageDefinition`コマンドを使用してイメージ定義の詳細を取得します。例:

```
Get-ProvImageDefinition [-ImageDefinitionName <string>] [-
ImageDefinitionUid <Guid>] [-ReturnTotalRecordCount] [-MaxRecordCount
<int>] [-Skip <int>] [-SortBy <string>] [-Filter <string>]
```

- `Get-ProvImageVersion`コマンドを使用してイメージバージョンの詳細を取得します。例:
  - イメージ定義内のイメージバージョンを一覧表示するには、,

    ```
    Get-ProvImageVersion -ImageDefinitionUid <Guid>
    ```

    または、,

    ```
    Get-ProvImageVersion -ImageDefinitionName <string>
    ```

  - イメージバージョンの詳細を取得するには、,

```
Get-ProvImageVersion -ImageVersionUid <Guid>
```

または、,

```
Get-ProvImageVersion -ImageDefinitionName <string>
-ImageVersionNumber <int>
```

- `Get-ProvImageVersionSpec`コマンドを使用して、準備済みイメージバージョンの仕様を取得します。例:
  - イメージバージョン内のすべての準備済みイメージバージョン仕様を一覧表示するには、,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid>
```

  - 準備済みイメージバージョン仕様内のマスターイメージバージョン仕様を一覧表示するには、,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "None"'
```

  - マスターイメージに関連付けられているイメージバージョン内の準備済みイメージバージョン仕様を一覧表示するには、,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"'
```

  - イメージバージョン内の正常な準備済みイメージバージョンの仕様を取得するには、,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" -and ImageVersionSpecStatus
-eq "Complete"'
```

  - 準備済みイメージバージョン仕様の詳細を取得するには、,

```
Get-ProvImageVersionSpec -ImageVersionSpecUid <Guid>
```

- `Get-ProvScheme`コマンドを使用して、プロビジョニングスキームの詳細を取得します。例:

```
Get-ProvScheme [[-ProvisioningSchemeName] <String>] [-
ProvisioningSchemeUid <Guid>] [-ScopeId <Guid>] [-ScopeName <String>]
[-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-
SortBy <String>] [-Filter <String>] [-FilterScope <Guid>]
```

- `Get-ProvSchemeImageVersionSpecHistory`コマンドを使用して、プロビジョニングスキームの準備済みイメージバージョンの仕様履歴を取得します。例:

```
Get-ProvSchemeImageVersionSpecHistory [-ProvisioningSchemeName
<String>] [-ProvisioningSchemeUid <Guid>] [-ImageVersionSpecUid <Guid>]
[-ImageVersionSpecHistoryUid <Guid>] [-ReturnTotalRecordCount] [-
MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter
<String>] [-FilterScope <Guid>]
```

詳細情報

- イメージ管理

マシンカタログを作成する

重要:

Citrix Virtual Apps and Desktops™ 7 2006以降、現在の展開で以下のいずれかのテクノロジーを使用している場合、それらのテクノロジーを使用するサポート終了（EOL）アイテムを削除した後にのみ、現在のリリースに展開をアップグレードできます。

- パーソナルvDisk (PvD)
- AppDisks™
- パブリッククラウドホストの種類：Citrix CloudPlatform、Microsoft Azure Classic

詳細については、「PvD、AppDisks、およびサポートされていないホストの削除」を参照してください。

注:

バージョン2511以降、Citrix Web Studio (Webベース) はCitrix Virtual Apps and Desktops™ の唯一の管理コンソールです。Citrix Studio (MMCベース) はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

展開にパブリッククラウドホスト接続を使用する場合は、新規インストールまたは現在のリリースへのアップグレードを完了するためにハイブリッド権限ライセンスが必要です。

インストーラーがサポートされていないテクノロジーまたはHybrid Rights Licenseのないホスト接続を1つ以上検出すると、アップグレードは一時停止または停止します。説明メッセージが表示されます。インストーラーログには詳細が含まれています。詳細については、「展開のアップグレード」を参照してください。

はじめに

物理マシンまたは仮想マシンのコレクションは、マシンカタログと呼ばれる単一のエンティティとして管理されます。カタログ内のすべてのマシンは、マルチセッションOSまたはシングルセッションOS、およびWindowsまたはLinuxマシンといった同じ種類のオペレーティングシステムを持っています。

Web Studioは、サイトを作成した後、最初のマシンカタログを作成するようにガイドします。最初のカタログを作成した後、Web Studioは最初のデリバリーグループを作成するようにガイドします。後で、作成したカタログを変更したり、さらにカタログを作成したりできます。

ヒント:

既存の展開をアップグレードすると、Machine Creation Services (MCS) ストレージ最適化 (MCS I/O) 機能が有効になり、追加の構成は不要です。Virtual Delivery Agent (VDA) と Delivery Controller のアップグレードによって、MCS I/O のアップグレードが処理されます。

概要

VM のカタログを作成するときに、それらの VM をプロビジョニングする方法を指定します。Machine Creation Services™ (MCS) を使用できます。または、独自のツールを使用してマシンを提供することもできます。

考慮事項:

- MCS は、仮想マシンイメージからの単一のシステムディスクをサポートします。そのイメージに接続されている残りのデータディスクは無視されます。
- MCS を使用して VM をプロビジョニングする場合、カタログ内に同一の VM を作成するためにマスターイメージ (またはイメージのスナップショット) を提供します。カタログを作成する前に、まずツールを使用してマスターイメージを作成および構成します。このプロセスには、イメージに Virtual Delivery Agent (VDA) をインストールすることが含まれます。次に、Web Studio でマシンカタログを作成します。そのイメージ (またはスナップショット) を選択し、カタログに作成する VM の数を指定し、追加情報を構成します。
- マシンがすでに利用可能な場合でも、それらのマシン用に1つ以上のマシンカタログを作成する必要があります。
- PowerShell SDK を直接使用してカタログを作成する場合、イメージやスナップショットではなく、ハイパーバイザーテンプレート (**VMTemplates**) を指定できます。
- テンプレートを使用してカタログをプロビジョニングすることは、実験的な機能と見なされます。この方法を使用すると、仮想マシンの準備が失敗する可能性があります。その結果、テンプレートを使用してカタログを公開することはできません。

MCS または Citrix Provisioning™ を使用して最初のカタログを作成する場合、サイトを作成したときに構成したホスト接続を使用します。後で (最初のカタログとデリバリーグループを作成した後)、その接続に関する情報を変更したり、さらに接続を作成したりできます。

カタログ作成ウィザードを完了すると、正しく構成されていることを確認するためにテストが自動的に実行されます。テストが完了すると、テストレポートを表示できます。Web Studio からいつでもテストを実行できます。

> **注:**
>
> MCS は Windows 10 IoT Core および Windows 10 IoT Enterprise をサポートしていません。詳細については、Microsoft のサイトを参照してください。

> Citrix Provisioning ツールに関する技術的な詳細については、Citrix Virtual Apps and Desktops Image Managementを参照してください。

RDS ライセンスチェック

Web Studio は現在、Windows マルチセッション OS マシンを含むマシンカタログを作成する際に、有効な Microsoft RDS ライセンスのチェックを実行しません。Windows **マルチセッション**

OS マシンの Microsoft RDS ライセンスのステータスを表示するには、Citrix Director に移動します。Microsoft RDS ライセンスのステータスは、**マシン詳細**パネルで確認できます。このパネルは、**マシン詳細およびユーザー詳細**ページにあります。詳細については、「Microsoft RDS ライセンスの健全性」を参照してください。

VDA登録

ブローカーセッションを起動する際には、VDAをDelivery Controller™に登録する必要があります。未登録のVDAは、利用可能なリソースの活用不足につながる可能性があります。VDAが登録されない理由はさまざまですが、その多くは管理者がトラブルシューティングできます。Web Studioは、カタログ作成ウィザードで、またカタログからデリバリーグループにマシンを追加した後で、トラブルシューティング情報を提供します。

ウィザードを使用して既存のマシンを追加すると、コンピューターアカウント名のリストに、各マシンがカタログに追加するのに適しているかどうかが表示されます。各マシンの横にあるアイコンにカーソルを合わせると、そのマシンに関する情報メッセージが表示されます。

メッセージで問題のあるマシンが特定された場合は、そのマシンを削除するか、追加します。たとえば、マシンに関する情報が取得できない可能性があることを示すメッセージが表示された場合でも、そのマシンを追加してください。

詳細については、以下を参照してください。

- VDA登録のトラブルシューティングガイダンスについては、「CTX136668」を参照してください。
- 「VDAのバージョンと機能レベル」
- 「VDA登録方法」

MCSカタログ作成の概要

カタログ作成ウィザードで情報を提供した後の、デフォルトのMCSアクションの概要を以下に示します。

- マスターイメージ（スナップショットではない）を選択した場合、MCSはスナップショットを作成します。
- MCSはスナップショットの完全なコピーを作成し、ホスト接続で定義された各ストレージの場所にそのコピーを配置します。
- MCSはマシンをActive Directoryに追加し、一意のIDを作成します。

- MCSは、ウィザードで指定された数のVMを作成し、各VMに2つのディスクを定義します。各VMの2つのディスクに加えて、マスターも同じストレージの場所に保存されます。複数のストレージの場所が定義されている場合、それぞれに以下のディスクタイプが割り当てられます。
  - 読み取り専用で、作成されたばかりのVM間で共有されるスナップショットの完全なコピー。
  - 各VMに一意のIDを付与する、一意の16 MBのIDディスク。各VMはIDディスクを取得します。
  - VMへの書き込みを保存するための一意の差分ディスク。このディスクはシンプロビジョニングされており（ホストストレージでサポートされている場合）、必要に応じてマスターイメージの最大サイズまで増加します。各VMは差分ディスクを取得します。差分ディスクには、セッション中に行われた変更が保持されます。専用デスクトップの場合は永続的です。プールされたデスクトップの場合、デリバリーコントローラーを介して再起動するたびに削除され、新しいものが作成されます。
  - VDAバージョン2511以降のWindows VMの場合、MCSは各マシンに一意の`MachineGuid`を割り当てます。この`MachineGuid`は、VDAにインストールされている一部のソフトウェアのライセンス目的で使用されます。

または、静的デスクトップを提供するVMを作成する際に、カタログ作成ウィザードの**マシン**ページで、シック（完全コピー）VMクローンを指定できます。完全クローンは、すべてのデータストアにマスターイメージを保持する必要はありません。各VMは独自のファイルを持っています。

MCSストレージに関する考慮事項

MCSのストレージソリューション、構成、容量を決定する際には、多くの要因があります。以下の情報は、ストレージ容量に関する適切な考慮事項を提供します。

容量に関する考慮事項:

- ディスク

  DeltaまたはDifferencing (Diff) ディスクは、ほとんどのMCS展開において、各VMで最大のスペースを消費します。MCSによって作成される各VMには、作成時に最低2つのディスクが割り当てられます。

  - Disk0 = 差分ディスク: マスターベースイメージからコピーされたOSが含まれます。
  - Disk1 = IDディスク: 16 MB - 各VMのActive Directoryデータが含まれます。

  製品の進化に伴い、特定のユースケースや機能の消費を満たすために、さらにディスクを追加する必要がある場合があります。例:

  - MCS Storage Optimization は、各VMのライトキャッシュスタイルのディスクを作成します。XenServer、VMware、およびSCVMM仮想化環境では、ホスト接続の作成時に利用可能なOSストレージリストと利用可能な一時ストレージリストを同じに構成した場合、MCSはライトバックキャッシュ（WBC）ディスクをOSディスクと同じストレージ場所に配置します。
  - MCSは、前のセクションで説明したデルタディスクのシナリオとは対照的に、フルクローンを使用する機能を追加しました。

  ハイパーバイザーの機能も考慮に入れる必要があるかもしれません。例えば：

  - (/ja-jp/citrix-hypervisor/storage/intellicache.html)は、各XenServerのローカルストレージにリードディスクを作成します。このオプションにより、共有ストレージの場所に保持されている可能性のあるマスターイメージに対するIOPSを節約できます。

- ハイパーバイザーのオーバーヘッド

  異なるハイパーバイザーは、VMのオーバーヘッドとなる特定のファイルを使用します。ハイパーバイザーは、管理および一般的なログ記録操作にもストレージを使用します。以下のオーバーヘッドを含めるためのスペースを計算してください：

  - ログファイル
  - ハイパーバイザー固有のファイル。例えば：
    - VMwareは**VMストレージ**フォルダーにファイルを追加します。VMwareのベストプラクティスを参照してください。
    - 仮想マシンの合計サイズ要件を計算してください。仮想ディスクに20 GB、スワップファイルに16 GB、ログファイルに100 MBを使用し、合計36.1 GBを消費する仮想マシンを考慮してください。
  - XenServer のスナップショット; VMware のスナップショット。

- プロセスオーバーヘッド

  カタログの作成、マシンの追加、カタログの更新には、それぞれ固有のストレージへの影響があります。例：

  - (/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create.html)では、ベースディスクのコピーを各ストレージの場所にコピーする必要があります。
  - カタログに(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-manage.html)する場合、ベースディスクを各ストレージの場所にコピーする必要はありません。カタログの作成は、選択された機能によって異なります。

- (/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-manage#update-a-catalog)では、各ストレージの場所に余分なベースディスクを作成します。カタログの更新時には、カタログ内の各VMが一定期間2つの差分ディスクを持つため、一時的なストレージピークも発生します。

その他の考慮事項：

- **RAMサイズ設定:** I/O最適化ディスク、ライトキャッシュ、スナップショットファイルなど、特定のハイパーバイザーファイルとディスクのサイズに影響します。
- **シン/シックプロビジョニング:** シンプロビジョニング機能があるため、NFSストレージが推奨されます。

Machine Creation Services (MCS) ストレージ最適化

Machine Creation Services (MCS) ストレージ最適化機能は、MCS I/O とも呼ばれます。この機能は、Azure、GCP、XenServer、VMware、AWS、およびSCVMMでのみ利用可能です。

- ライトキャッシュコンテナは*ファイル*ベースであり、Citrix Provisioning に見られる機能と同じです。たとえば、Citrix Provisioning のライトキャッシュファイル名は `D:\vdiskdif.vhdx` で、MCS I/O のライトキャッシュファイル名は `D:\mcsdif.vhdx` です。
- ライトキャッシュディスクに書き込まれたWindowsクラッシュダンプファイルのサポートを含めることで、診断の改善を実現します。
- MCS I/O は、最適なマルチティアライトキャッシュソリューションを提供するために、*RAM にキャッシュし、ハードディスクにオーバーフローする*テクノロジーを保持しています。この機能により、管理者は各ティア（RAMとディスク）のコストとパフォーマンスのバランスを取り、目的のワークロード要件を満たすことができます。

ライトキャッシュ方式を*ディスク*ベースから*ファイル*ベースに更新するには、以下の変更が必要です。

1. MCS I/O はRAMのみのキャッシュをサポートしなくなりました。マシンカタログ作成時にWeb Studioでディスクサイズを指定してください。
2. VMのライトキャッシュディスクは、VMを初めて起動するときに自動的に作成およびフォーマットされます。VMが起動すると、ライトキャッシュファイル `mcsdif.vhdx` がフォーマットされたボリューム `MCSWCDisk` に書き込まれます。
3. ページファイルは、このフォーマットされたボリューム `MCSWCDisk` にリダイレクトされます。その結果、このディスクサイズはディスク領域の合計量を考慮します。これには、ディスクサイズと生成されたワークロードの差分にページファイルサイズを加えたものが含まれます。これは通常、VMのRAMサイズに関連付けられます。

MCS ストレージ最適化の更新の有効化

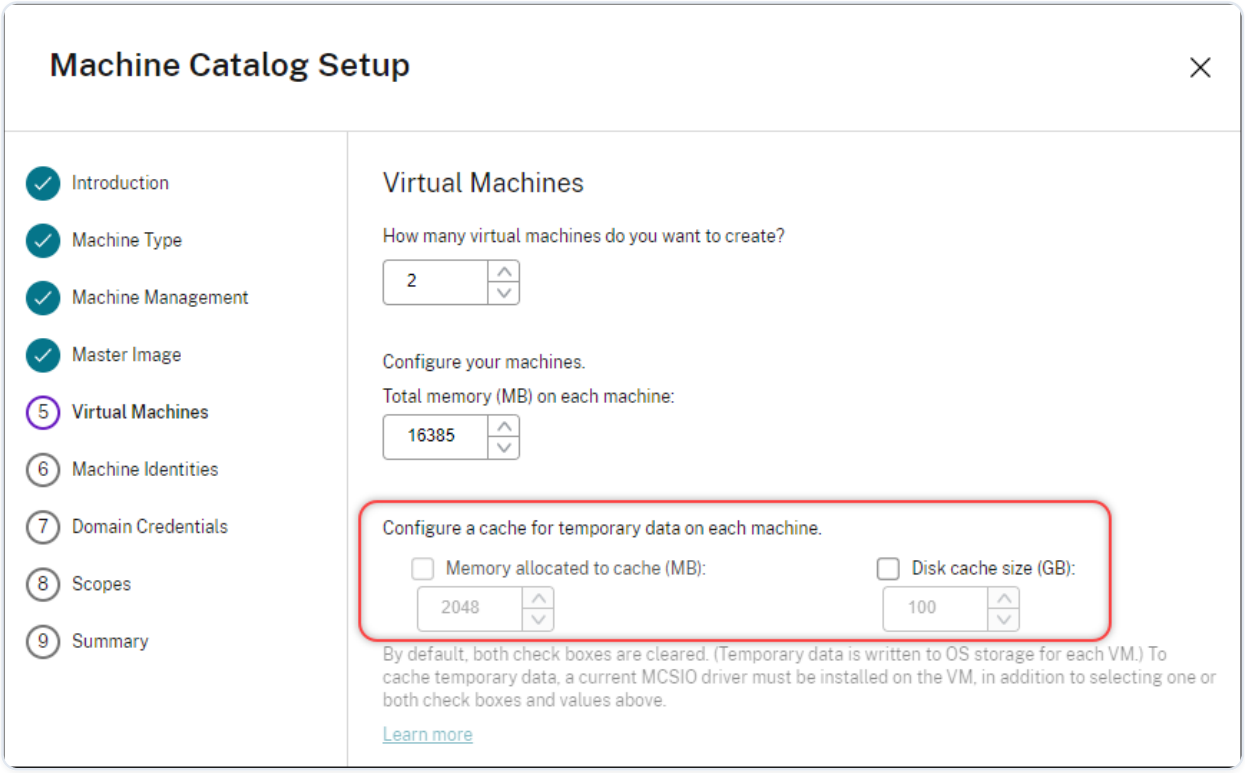
MCS I/O ストレージ最適化機能を有効にするには、Delivery Controller と VDA を Citrix Virtual Apps and Desktops の最新バージョンにアップグレードしてください。

注:

MCS I/O が有効になっている既存の展開をアップグレードする場合、追加の構成は不要です。VDA と Delivery Controller のアップグレードによって MCS I/O のアップグレードが処理されます。

MCSストレージ最適化の更新を有効にする際は、次の点を考慮してください。

- マシンカタログを作成する際、管理者は RAM とディスクサイズを構成できます。



- 既存のマシンカタログを、バージョン1903用に構成されたVDAを含む新しいVMスナップショットに更新すると、次の動作が発生します。新しいスナップショットは、既存のカタログのRAMおよびディスクサイズに対するMCS I/O設定を引き続き使用します。既存の生ディスクはフォーマットされます。

重要：

MCSストレージ最適化は、Citrix Virtual Apps and Desktopsバージョン1903で変更されました。このリリースでは、ファイルベースのライトキャッシュテクノロジーがサポートされ、パフォーマンスと安定性が向上しています。MCS I/Oによって提供される新しい機能は、以前のCitrix Virtual Apps and Desktopsリリースと比較して、より高いライトキャッシュストレージ要件を必要とする場合があります。Citrixは、割り当てられたワークフローと追加のページファイルサイズに十分なディスク容量があることを確認するために、ディスクサイズを再評価することを推奨します。ページファイルサイズは通常、システムRAMの量に関連しています。既存のカタログディスクサイズが不十分な場合は、マシンカタログを作成し、より大きなライトキャッシュディスクを割り当ててください。

MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てる

MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てることができます。この実装により、使用するアプリケーションのドライブ文字とMCS I/Oライトバックキャッシュディスクのドライブ文字との間の競合を回避できます。MCS I/Oライトバックキャッシュディスクにドライブ文字を割り当てるには、PowerShellコマンドを使用できます。サポートされているハイパーバイザーは、Azure、GCP、VMware、SCVMM、およびXenServerです。

注：

この機能には、VDAバージョン2305以降が必要です。

制限事項

- Windowsオペレーティングシステムのみに適用
- ライトバックキャッシュディスクに適用可能なドライブ文字: `E`から`Z`
- Azure一時ディスクがライトバックキャッシュディスクとして使用されている場合は適用されません
- 新しいマシンカタログを作成する場合にのみ適用

ライトバックキャッシュディスクにドライブ文字を割り当てる

ライトバックキャッシュディスクにドライブ文字を割り当てるには、次の手順を実行します。

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*`を実行します。

3. まだ作成されていない場合は、IDプールを作成します。
4. プロパティ `WriteBackCacheDriveLetter` を指定して、 `New-ProvScheme` コマンドを使用してプロビジョニングスキームを作成します。例：

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "<name>" `

-IdentityPoolName $schemeName `

-ProvisioningSchemeName $schemeName `

-InitialBatchSizeHint 1 `

-UseWriteBackCache -WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `

-MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
resources.resourcegroup\MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxxx2130aa
145ec77.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\name\
\virtualprivatecloud.folder\\East US.region\
\virtualprivatecloud.folder\\abcd-resources.resourcegroup\\abcd-
resources-vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.folder\
\Standard_D2s_v5.serviceoffering" `

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS"/>

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />
```

```
<Property xsi:type="StringProperty" Name="PersistOsDisk"
Value="false" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
Value="false" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-
group1" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

5. カタログの作成を完了します。詳しくは、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

マスターイメージを準備する

接続ホストの作成については、「接続とリソース」を参照してください。

マスターイメージには、オペレーティングシステム、非仮想化アプリケーション、VDA、およびその他のソフトウェアが含まれています。

知っておくと良いこと:

- マスターイメージは、クローンイメージ、ゴールデンイメージ、ベースVM、またはベースイメージとも呼ばれることがあります。ホストベンダーは異なる用語を使用します。
- ホストに、作成されるマシンの数に対応できる十分なプロセッサ、メモリ、ストレージがあることを確認してください。
- デスクトップおよびアプリケーションに必要なハードディスク容量を正しく構成します。この値は、後で変更したり、マシンカタログ内で変更したりすることはできません。

- Remote PC Accessマシンカタログでは、マスターイメージは使用されません。

マスターイメージに以下のソフトウェアをインストールして構成します:

- ハイパーバイザー用の統合ツール（Citrix VM Tools、Hyper-V Integration Services、VMware toolsなど）。この手順を省略すると、アプリケーションやデスクトップが正しく機能しない可能性があります。
- VDA。最新の機能にアクセスできるように、最新バージョンをインストールすることをお勧めします。マスターイメージにVDAをインストールしないと、カタログの作成が失敗します。
- 必要に応じて、ウイルス対策ソフトウェアや電子ソフトウェア配布エージェントなどのサードパーティ製ツール。ユーザーとマシンタイプに適した設定（更新機能など）でサービスを構成します。
- 仮想化しないサードパーティ製アプリケーション。Citrixでは、アプリケーションを仮想化することをお勧めします。仮想化により、アプリケーションの追加または再構成後にマスターイメージを更新する必要がなくなるため、コストが削減されます。また、インストールされるアプリケーションが少ないほど、マスターイメージのハードディスクサイズが小さくなり、ストレージコストが節約されます。
- App-Vアプリケーションを公開する予定がある場合は、推奨設定のApp-Vクライアント。App-VクライアントはMicrosoftから入手できます。
- MCSを使用する場合、Microsoft Windowsをローカライズする場合は、ロケールと言語パックをインストールします。プロビジョニング中にスナップショットが作成されると、プロビジョニングされたVMはインストールされているロケールと言語パックを使用します。

> **重要:**
>
> MCSを使用している場合は、マスターイメージでSysprepを実行しないでください。

> マスターイメージを準備するには：

1. ハイパーバイザーの管理ツールを使用してマスターイメージを作成し、オペレーティングシステムとすべてのサービスパックおよび更新プログラムをインストールします。vCPUの数を指定します。PowerShellを使用してマシンカタログを作成する場合も、vCPUの値を指定できます。Web Studioを使用してカタログを作成する場合、vCPUの数を指定することはできません。デスクトップとアプリケーションに必要なハードディスク容量を構成します。この値は後で変更したり、カタログ内で変更したりすることはできません。

2. ハードディスクがデバイスロケーション0に接続されていることを確認します。ほとんどの標準マスターイメージテンプレートではこのロケーションがデフォルトで構成されていますが、一部のカスタムテンプレートではそうでない場合があります。
3. マスターイメージに上記のソフトウェアをインストールして構成します。
4. MCSを使用しない場合は、マスターイメージをアプリケーションとデスクトップが属するドメインに参加させます。マスターイメージがマシンが作成されるホストで利用可能であることを確認します。MCSを使用している場合、マスターイメージをドメインに参加させる必要はありません。プロビジョニングされたマシンは、カタログ作成ウィザードで指定されたドメインに参加します。
5. Citrixでは、マスターイメージのスナップショットを作成して名前を付けることをお勧めします。カタログ作成時にスナップショットではなくマスターイメージを指定すると、Web Studioがスナップショットを作成します。そのスナップショットに名前を付けることはできません。

ボリュームライセンス認証

MCSは、WindowsオペレーティングシステムとMicrosoft Officeのアクティベーションを自動化および管理するためのボリュームライセンス認証をサポートしています。MCSがボリュームライセンス認証でサポートする3つのモデルは次のとおりです。

- キー管理サービス (KMS)
- Active Directoryベースの認証 (ADBA)
- マルチライセンス認証キー (MAK)

マシンカタログを作成した後で、アクティベーション設定を変更できます。

キー管理サービス (KMS)

KMSは、専用のシステムを必要とせず、他のサービスを提供するシステム上で簡単に共存できる軽量なサービスです。この機能は、Citrixがサポートするすべてのバージョンでサポートされています。イメージ準備中に、MCSはMicrosoft WindowsおよびMicrosoft OfficeのKMSリアームを実行します。コマンド `Set-Provserviceconfigurationdata` を実行することで、リアームをスキップできます。KMS認証の詳細については、「キー管理サービスを使用した認証」を参照してください。

> **注:**
>
> コマンド `Set-Provserviceconfigurationdata` の実行後に作成されたすべてのマシンカタログは、コマンドで指定されたものと同じ設定になります。

Active Directoryベースのアクティベーション (ADBA)

ADBAを使用すると、ドメイン接続を介してマシンを認証できます。マシンはドメインに参加するとすぐに認証されます。これらのマシンは、ドメインに参加し、ドメインと通信している限り、認証されたままになります。この機能は、Citrixがサポートするすべてのバージョンでサポートされています。Active Directoryベースの認証の詳細については、「Active Directoryベースの認証」を参照してください。

マルチライセンス認証キー (MAK)

MAKは、Microsoftサーバーの助けを借りてボリュームを認証し、Windowsシステムを認証する方法です。MicrosoftからMAKキーを購入する必要があります。このキーには、固定された認証回数が割り当てられています。Windowsシステムが認証されるたびに、認証回数が減少します。システムを認証する方法は2つあります。

- オンライン認証：認証したいWindowsシステムがインターネットにアクセスできる場合、プロダクトキーをインストールするとシステムは自動的にWindowsを認証します。このプロセスにより、対応するMAKの認証回数が1つ減少します。
- オフラインアクティベーション: Windowsシステムがオンラインアクティベーションのためにインターネットに接続できない場合、MCSはMicrosoftサーバーから確認IDとインストールIDを取得してWindowsシステムをアクティベートします。このアクティベーション方法は、非永続的なマシンカタログに役立ちます。

注:

- MCSはMAKを使用したMicrosoft Officeのアクティベーションをサポートしていません。
- 必要なVDAの最小バージョンは2303です。

主な要件

- Delivery Controllerはインターネットにアクセスできる必要があります。
- 更新する新しいイメージが元のイメージと異なるMAKキーを持っている場合は、新しいカタログを作成します。
- マスターイメージにMAKキーをインストールします。WindowsシステムにMAKキーをインストールする手順については、MAKアクティベーションの展開を参照してください。
- イメージ準備を使用しない場合：

a. `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`の下にレジストリDWORD値`Manual`を追加します。

b. 値を`1`に設定します。

アクティベーション数

MAKキーの残りアクティベーション数を表示したり、VMが2つ以上のアクティベーションを消費しているかどうかを確認したりするには、ボリュームアクティベーション管理ツール (VAMT) を使用します。VAMTのインストールを参照してください。

MAKを使用してWindowsシステムをアクティベートする

MAKを使用してWindowsシステムをアクティベートするには：

1. マスターイメージにプロダクトキーをインストールします。この手順で1つのアクティベーションカウントが消費されます。
2. MCSマシンカタログを作成します。
3. イメージ準備を使用しない場合：

   a. `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`の下にレジストリDWORD値`Manual`を追加します。

   b. 値を`1`に設定します。

   この方法では、オンラインアクティベーションのオプションが無効になります。
4. マシンカタログにVMを追加します。
5. VMの電源をオンにします。
6. オンラインアクティベーションかオフラインアクティベーションかに応じて、Windowsシステムがアクティベートされます。

   - オンラインアクティベーションの場合、プロダクトキーのインストール後に Windows システムがアクティベートされます。
   - オフラインアクティベーションの場合、MCS はプロビジョニングされた VM と通信して Windows システムのアクティベーションステータスを取得します。その後、MCS は Microsoft サーバーから確認 ID とインストール ID を取得します。これらの ID は Windows システムのアクティベーションに使用されます。

トラブルシューティング

プロビジョニングされたVMがインストール済みのMAKキーでアクティベートされない場合は、PowerShellウィンドウで`Get-ProvVM`または`Get-ProvScheme`コマンドを実行します。

- `Get-ProvScheme`コマンド：最新のマスターイメージからMCSマシンカタログに関連付けられているパラメーター`WindowsActivationType`を参照してください。
- `Get-ProvVM`コマンド。パラメーター`WindowsActivationType`、`WindowsActivationStatus`、`WindowsActivationStatusErrorCode`、および`WindowsActivationStatusError`を参照してください。

エラーを確認し、問題を解決するための手順を検証できます。

Web Studio を使用してマシンカタログを作成する

カタログを作成する前に：

- このセクションを読んで、選択する項目と提供する情報について学習してください。
- マシンをホストするハイパーバイザー、クラウドサービス、およびその他のリソースへの接続が作成されていることを確認してください。
- マシンをプロビジョニングするためにマスターイメージを作成した場合は、そのイメージにVDAがインストールされていることを確認してください。

カタログ作成ウィザードを開始するには：

1. これが最初に作成するカタログである場合、適切な選択肢（「マシンをセットアップし、アプリとデスクトップを実行するためのマシンカタログを作成する」など）に誘導されます。カタログ作成ウィザードが開きます。
2. すでにカタログを作成しており、別のカタログを作成したい場合は、次の手順に従ってください：

    a. Web Studio にサインインし、左ペインで **Machine Catalogs** を選択し、アクションバーで **Create Machine Catalog** を選択します。

    b. フォルダーを使用してカタログを整理するには、デフォルトの**Machine Catalogs**フォルダーの下にフォルダーを作成します。詳細については、(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-manage.html#create-a-catalog-folder)を参照してください。

    c. カタログを作成するフォルダーを選択し、**Create Machine Catalog** をクリックします。カタログ作成ウィザードが開きます。

ウィザードは次の項目について説明します。表示されるウィザードページは、選択内容によって異なります。

オペレーティングシステム

各カタログには、1種類のマシンのみが含まれます。1つ選択してください。

- **マルチセッションOS:** マルチセッションOSカタログは、ホストされた共有デスクトップを提供します。マシンはサポートされているバージョンのWindowsまたはLinuxオペレーティングシステムを実行できますが、カタログに両方を含めることはできません。（そのOSの詳細については、Linux VDAのドキュメントを参照してください。）
- **シングルセッションOS:** シングルセッションOSカタログは、さまざまなユーザーに割り当てることができるVDIデスクトップを提供します。
- **Remote PC Access:** Remote PC Accessカタログは、ユーザーに物理的なオフィスデスクトップマシンへのリモートアクセスを提供します。Remote PC Accessは、セキュリティを提供するためにVPNを必要としません。

マシン管理

このページは、リモートPCアクセスカタログを作成する際には表示されません。

マシン管理ページには、マシンの管理方法と、マシンの展開に使用するツールが示されます。

カタログ内のマシンをWeb Studioで電源管理するかどうかを選択します。

- マシンはWeb Studioで電源管理されます（例：VMまたはブレードPC）。このオプションは、ホストへの接続をすでに構成している場合にのみ使用できます。
- マシンはWeb Studioで電源管理されません（例：物理マシン）。

マシンがWeb Studioで電源管理されることを示した場合は、VMの作成に使用するツールを選択します。

- Citrix Provisioning テクノロジー
    - **Citrix Machine Creation Services (MCS)** MCSを使用してプロビジョニングおよびイメージ化されたVMのカタログを作成します。MCSは、マスターイメージからクローンされたイメージをそれらのVMにコピーします。
    - **Citrix Provisioning Services (PVS)** MCSを使用してプロビジョニングされ、PVSを使用してイメージ化されたVMのカタログを作成します。これらのVMはPVSターゲットデバイ

スとして機能し、PVSサーバーは単一の共有ディスクイメージをそれらにストリームできます。

> **注:**
>
> - このオプションは、Citrix Cloud™に登録されているPVSサイトでのみ利用可能であり、現在はAzureリソースに限定されています。
> - Citrix Provisioningカタログの作成中に、**Target Device**ページで、プロビジョニングするマシンのファームとサイトを選択するドロップダウンメニューに、存在しないファームとサイトがリストされている場合があります。回避策として、PowerShellコマンド`Unregister-HypPvsSite`を実行して、データベースからファームとサイトを削除できます。PowerShellコマンドの詳細については、「Unregister-HypPvsSite」を参照してください。

- **その他のサービスまたはテクノロジー** データセンターにすでに存在するマシンを管理するツール。Citrixでは、カタログ内のマシンの一貫性を確保するために、Microsoft System Center Configuration Managerまたはその他のサードパーティ製アプリケーションを使用することをお勧めします。

デスクトップの種類（デスクトップエクスペリエンス）

> **注:**
>
> **Desktop Experience**ページに表示されるオプションは、**Machine Type**ページで選択したマシンの種類によって異なります。

- **マルチセッションOS**マシンでは、ユーザーはログオンするたびにランダムなデスクトップを割り当てられます。次のいずれかのオプションを選択してください。
  - **はい、仮想デスクトップをホストするマシンのローカルディスクに変更を保存します。**（永続的）
  - **いいえ、すべての変更を破棄し、ユーザーがログオフするときに仮想デスクトップをクリアします。**（非永続的）

> **注:**

> 永続的なマルチセッションマシンでは、ユーザーがデスクトップに加えた変更は保存され、すべての承認済みユーザーがアクセスできます。

- **シングルセッションOS**マシンでは、**Desktop Experience**ページで次のオプションが表示されます。
  - **ユーザーがログオンするたびに、新しい（ランダムな）デスクトップに接続するようにします。**
  - **ユーザーがログオンするたびに、同じ（静的な）デスクトップに接続するようにします。**

    静的デスクトップの場合、ユーザーが行った変更をログオフ後に保存するか破棄するかをさらに決定できます。

仮想デスクトップをホストするマシンのローカルディスクに変更を保存する：永続的を選択すると、**Virtual Machines**ページで仮想マシンコピーモードの高速コピーまたは完全コピーオプションが利用可能になります。

ユーザーがログオフしたときに**すべての変更を破棄し、仮想デスクトップをクリアする: 非永続的**を選択した場合、**仮想マシン** ページで仮想マシンコピーモードを構成することはできません。

イメージとマシンプロファイル

このページは、MCS を使用して VM を作成する場合にのみ表示されます。

1. マシンカタログのイメージタイプを選択し、イメージを選択します。2種類のイメージタイプが利用可能です。
   - **マスターイメージ。** イメージ準備プロセスをまだ経ていないイメージ。カタログ作成が開始されると、イメージ準備プロセスが自動的に開始されます。

     > **注:**
     >
     > - MCS を使用している場合、マスターイメージで Sysprep を実行しないでください。
     > - スナップショットではなくマスターイメージを指定した場合、Web Studio はスナップショットを作成しますが、名前を付けることはできません。

- **準備済みイメージ。** イメージ準備プロセスを経ており、VM 作成に直接使用できるイメージ。カタログ作成時にマスターイメージではなく準備済みイメージを選択することで、より高速で信頼性の高いマシンカタログ作成と、合理化されたイメージライフサイクル管理が保証されます。必要に応じて、選択した準備済みイメージにメモを追加します。

  > **注:**
  >
  > - 準備済みイメージを使用して作成された VM は、休止状態をサポートしていません。
  > - 現在、準備済みイメージを使用したカタログ作成は、Azure および VMware 環境でのみ利用可能です。

  準備済みイメージの作成方法の詳細については、「イメージ管理（プレビュー）」を参照してください。

  イメージを選択する際、必要に応じて、選択したイメージにメモを追加できます。

  最新の製品機能を使用できるようにするには、マスターイメージに最新の VDA バージョンがインストールされていることを確認してください。デフォルトの最小 VDA 選択を変更しないでください。ただし、以前の VDA バージョンを使用する必要がある場合は、「VDA のバージョンと機能レベル」を参照してください。

  ウィザードで以前に選択したマシン管理テクノロジーと互換性のないスナップショットまたはVMを選択すると、エラーメッセージが表示されます。

2. 既存のVMをマシンプロファイルとして使用するには、**Use a machine profile**を選択し、その後、VMを選択します。

   > **注：**
   >
   > 現在、マシンプロファイルの使用は、Azure、AWS、GCP、およびVMware VMに限定されています。
   >
   > VMware展開の場合、マシンプロファイルを使用してマシンカタログを作成する際に、仮想マシンを保持するフォルダーを指定する必要があります。

仮想マシンフォルダーの場所を指定するには、カタログ作成ウィザードで**Virtual Machines**ページに移動し、**Select a folder to place the machines**セクションに移動して仮想マシンフォルダーの場所を選択します。指定されていない場合、システムは選択されたマシンプロファイルのフォルダーをデフォルトの場所と見なします。

3. AWS展開の場合、起動テンプレートをマシンプロファイルとして選択できます。
4. カタログの最小機能レベルを選択します。最新の製品機能を使用できるようにするには、マスターイメージに最新のVDAバージョンがインストールされていることを確認してください。

マシン

リモートPCアクセス カタログを作成している場合、このページは表示されません。

このページのタイトルは、**マシン管理**ページで選択した内容（**マシン**、**仮想マシン**、または**VMとユーザー**）によって異なります。

MCSを使用する場合：

- 作成する仮想マシンの数を指定します。作成しない場合は**0**（ゼロ）と入力します。後で、**Add machines**を実行して、空のカタログにVMを作成できます。
- 各VMが持つメモリ量（MB単位）を選択します。
- 作成された各VMにはハードディスクがあります。そのサイズはマスターイメージで設定されます。カタログでハードディスクのサイズを変更することはできません。
- デプロイに複数のゾーンが含まれている場合、カタログのゾーンを選択できます。
- 静的デスクトップVMを作成している場合は、仮想マシンコピーモードを選択します。「仮想マシンコピーモード」を参照してください(#virtual-machine-copy-mode)。
- vDiskを使用しないランダムデスクトップVMを作成している場合は、各マシンの一時データに使用するキャッシュを構成できます。「一時データ用のキャッシュを構成する」を参照してください(#configure-cache-for-temporary-data)。

その他のツールを使用する場合：

Active Directoryマシンアカウント名を追加（またはリストをインポート）します。VMを追加/インポートした後で、そのVMのActive Directoryアカウント名を変更できます。「**デスクトップエクスペリエンス**」ページで静的マシンを指定した場合、追加する各VMのActive Directoryユーザー名をオプションで指定できます。

名前を追加またはインポートした後、このページにいる間は「**削除**」ボタンを使用してリストから名前を削除できます。

他のツールを使用する場合（ただしMCSではない場合）：

追加（またはインポート）された各マシンに表示されるアイコンとツールヒントは、カタログに追加できない可能性のあるマシンや、Delivery Controllerに登録できないマシンを特定するのに役立ちます。詳しくは、「VDAのバージョンと機能レベル」を参照してください(#vda-versions-and-functional-levels)。

仮想マシン作成時にSIDを追加する

新しい仮想マシンを作成する際に、マシンを一意に識別するためにパラメータ`ADAccountSid`を追加できるようになりました。

これを行うには：

1. サポートされているIDタイプでカタログを作成します。
2. `NewProvVM`を使用してカタログにマシンを追加します。例：

```
New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID ")  -
RunAsynchronously
```

ただし、次の条件のいずれかに該当するマシンをプロビジョニングすることはできません。

- カタログIDプールにないADアカウント
- 利用可能な状態ではないADアカウント

仮想マシンのコピーモード

マシンページで指定するコピーモードによって、MCSがマスターイメージからシン（高速コピー）クローンを作成するか、シック（完全コピー）クローンを作成するかが決まります。(デフォルト = シンクローン)

- ストレージ使用効率の向上とマシン作成の高速化のために、高速コピークローンを使用します。
- マシン作成後のIOPSを削減し、データリカバリと移行サポートを向上させるために、完全コピークローンを使用します。

> **注:**
>
> 完全コピークローンアプローチは、マルチセッションまたはシングルセッションOS上の永続VMをプロビジョニングする場合にのみ利用可能です。

VDAバージョンと機能レベル

カタログの機能レベルは、カタログ内のマシンで利用できる製品機能を制御します。新しい製品バージョンで導入された機能を使用するには、新しいVDAが必要です。 ただし、以前のVDAバージョンのマシンは、そのカタログに登録できません。

マシン（または**デバイス**）ページの下部にあるメニューで、最小VDAレベルを選択できます。これにより、カタログの最小機能レベルが設定されます。デフォルトでは、オンプレミス展開の場合、最新の機能レベルが選択されます。Citrixの推奨に従って、常にVDAとコアコンポーネントを最新バージョンにインストールおよびアップグレードする場合は、この選択を変更する必要はありません。ただし、古いVDAバージョンを使い続ける必要がある場合は、正しい値を選択してください。

Citrix Virtual Apps and Desktopsのリリースには、新しいVDAバージョンが含まれていない場合や、新しいVDAが機能レベルに影響を与えない場合があります。そのような場合、機能レベルは、インストールまたはアップグレードされたコンポーネントよりも古いVDAバージョンを示すことがあります。各リリースの新機能の記事には、デフォルトの機能レベルの変更が示されています。

選択された機能レベルは、その上にあるマシンのリストに影響を与えます。リストでは、各エントリの横にあるツールチップが、その機能レベルでマシンのVDAがカタログと互換性があるかどうかを示します。

各マシンのVDAが選択された最小機能レベルを満たしていないか、それを超えていない場合、ページにメッセージが表示されます。ウィザードを続行できます。これらのマシンは、後でControllerに登録できない可能性があります。代わりに、次のことができます。

- 古いVDAを含むマシンをリストから削除し、VDAをアップグレードしてから、カタログに再度追加します。
- 最新の製品機能へのアクセスを妨げる、より低い機能レベルを選択します。

マシンが誤ったマシンタイプであるためにカタログに追加されなかった場合も、メッセージが投稿されます。例としては、サーバーをシングルセッションOSカタログに追加しようとしたり、ランダム割り当て用に作成されたシングルセッションOSマシンを静的マシンのカタログに追加したりする場合があります。

> **重要:**

> リリース1811では、追加の機能レベルである**1811（またはそれ以降）**が追加されました。このレベルは、将来のCitrix Virtual Apps and Desktops機能で使用することを目的としています。**7.9（またはそれ以降）**の選択はデフォルトのままです。このデフォルトは、現在すべての展開で有効です。

> **1811（またはそれ以降）**を選択した場合、そのカタログ内の以前のVDAバージョンはControllerに登録できません。ただし、カタログにバージョン1811以降のサポートされているVDAのみが含まれている場合、それらはすべて登録の対象となります。これには、バージョン1903および現在のリリースより前のその他の19XXリリースを含む、以降のCitrix Virtual Apps and Desktopsリリース用に構成されたVDAを含むカタログが含まれます。

一時データのキャッシュを構成する

MCSを使用してカタログ内のランダムな非永続マシンを管理する場合、マシンのI/Oパフォーマンスを向上させるためにライトバックキャッシュを有効にできます。

ライトバックキャッシュはMCSIOと呼ばれます。詳細については、こちらのブログ記事を参照してください。

前提条件

ライトバックキャッシュを有効にするには、カタログが以下の要件を満たしている必要があります。

- 一時データのストレージを指定する接続を使用します。詳細については、接続とリソースを参照してください。
- VDAはバージョン7.9以降であり、現在のMCSIOドライバーがインストールされている必要があります。

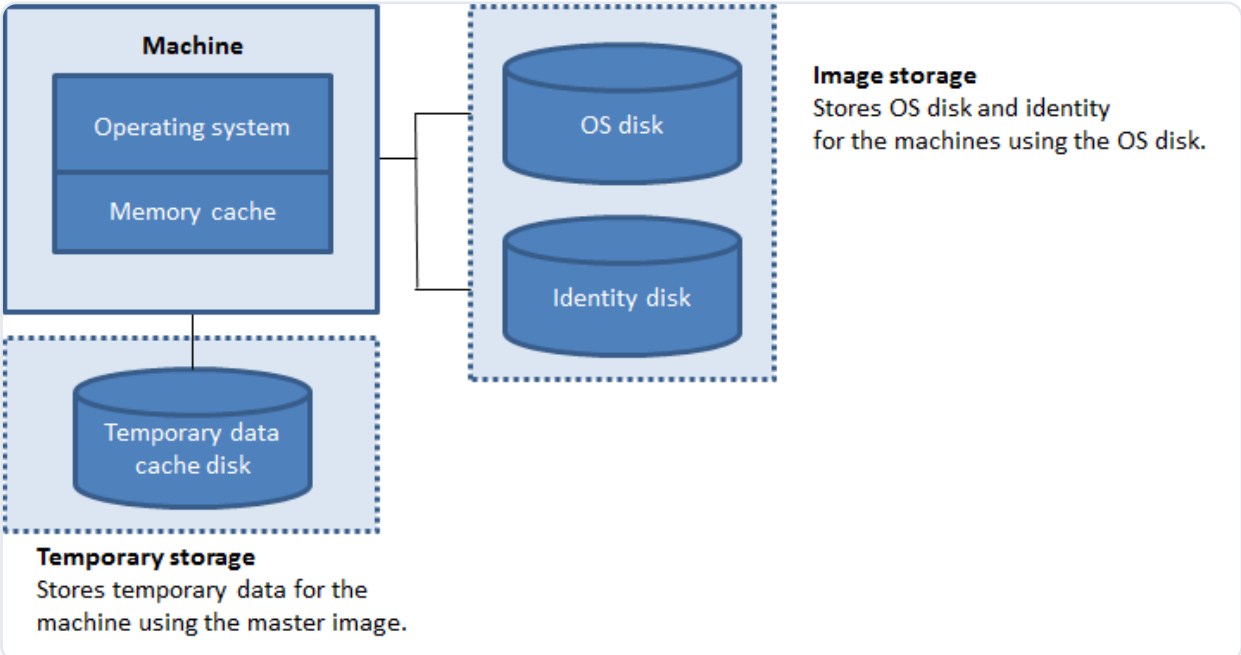
  > **注:**
  >
  > このドライバーのインストールは、VDAをインストールまたはアップグレードする際のオプションです。デフォルトでは、このドライバーはインストールされません。

- ディスクキャッシュのドライブ文字割り当てを有効にするには、VMは以下の追加要件を満たす必要があります。
  - オペレーティングシステム：Windows

- VDA バージョン: 2305 以降

考慮事項

- ライトバックキャッシュには、*メモリキャッシュ*と*ディスクキャッシュ*があります。デフォルトでは、接続タイプによってデフォルト値が異なります。一般的に、ほとんどの場合、デフォルト値で十分ですが、以下のために必要な領域を考慮してください。
  - Windows自体によって作成される一時データファイル（Windowsページファイルを含む）。
  - ユーザープロファイルデータ。
  - ユーザーのセッションに同期されるShareFileデータ。
  - セッションユーザーによって作成またはコピーされる可能性のあるデータ、またはユーザーがセッション内にインストールする可能性のあるアプリケーションによって作成またはコピーされる可能性のあるデータ。



- ディスクキャッシュがあり、メモリキャッシュがないライトバックキャッシュの構成は削除されました。一時データ用のキャッシュを有効にするには、**ディスクキャッシュサイズ (GB)** と **キャッシュに割り当てられるメモリ (MB)** を選択し、メモリキャッシュに0より大きいサイズを指定することをお勧めします。一時データは最初にメモリキャッシュに書き込まれます。メモリキャッシュが設定された制限に達すると、最も古いデータは一時データキャッシュディスクに移動されます。
- メモリキャッシュは、各マシン上の総メモリ量の一部です。したがって、**メモリキャッシュサイズ (MB) (推奨)** チェックボックスを有効にする場合は、各マシン上の総メモリ量を増やすことを検討してください。

- **メモリキャッシュサイズ (MB) (推奨)** チェックボックスをオフのままにすると、一時データは最小限のメモリを使用してディスクキャッシュに直接書き込まれます。
- **ディスクキャッシュサイズ (GB)** をデフォルト値から変更すると、パフォーマンスに影響を与える可能性があります。サイズは、ユーザー要件とマシンにかかる負荷に合わせる必要があります。

> **重要:**
>
> ディスクキャッシュの容量が不足すると、ユーザーセッションは使用できなくなります。

- **ディスクキャッシュサイズ** チェックボックスをオフにすると、キャッシュディスクは作成されません。この場合、すべての一時データを保持するのに十分な大きさの **キャッシュに割り当てられるメモリ** の値を指定します。これは、各VMに割り当てるための大量のRAMが利用可能な場合にのみ実現可能です。
- 両方のチェックボックスをオフにすると、一時データはキャッシュされません。各VMの差分ディスク（OSストレージ内）に書き込まれます。（これは、7.9より前のリリースでのプロビジョニングアクションです。）
- このカタログを使用してAppDiskを作成する予定がある場合は、キャッシュを有効にしないでください。
- マシンカタログの作成後、キャッシュ値を変更することはできません。

セキュリティ

セキュリティページは、AWS仮想化環境でマシンプロファイルを割り当てずにマシンカタログを作成する場合にのみ表示されます。**セキュリティ**ページを使用して、VMのセキュリティグループを構成します。これは、既存のマシンカタログを編集およびクローンする場合にも適用されます。

マシンプロファイルベースのマシンカタログを作成する場合、セキュリティグループの構成はマシンプロファイルから継承され、**セキュリティ**ページは表示されません。

ニック (複数のニック)

このページは、Remote PC Accessカタログを作成しているときには表示されません。

複数のNICを使用する予定がある場合は、各カードに仮想ネットワークを関連付けます。たとえば、一方のカードを特定のセキュアネットワークへのアクセスに割り当て、もう一方のカードを

より一般的に使用されるネットワークへのアクセスに割り当てることができます。このページからNICを追加または削除することもできます。

マシンアカウント

このページは、リモートPCアクセス カタログを作成する場合にのみ表示されます。

「**マシンアカウント**」ページで、ユーザーまたはユーザーグループに対応するActive Directoryマシンアカウントまたは組織単位（OU）を指定します。OU名にスラッシュ（/）を使用しないでください。

OUを追加する際に、ドメインがリストに表示されない場合は、次の操作を実行できます。

- 完全一致で検索します。
- すべてのドメインを参照して見つけます。

以前に構成した電源管理接続を選択するか、電源管理を使用しないことを選択できます。電源管理を使用したいが、適切な接続がまだ構成されていない場合は、後でその接続を作成し、マシンカタログを編集して電源管理設定を更新できます。

マシンのID

このページは、MCSを使用してVMを作成する場合にのみ表示されます。

カタログ内の各マシンには一意のIDが必要です。このページでは、カタログ内のマシンのIDを構成できます。マシンはプロビジョニング後にIDに参加します。カタログ作成後にIDタイプを変更することはできません。

このページで設定を構成するための一般的なワークフローは次のとおりです。

1. リストからIDを選択します。
2. アカウントを作成するか既存のアカウントを使用するか、およびそれらのアカウントの場所（ドメイン）を指定します。

次のいずれかのオプションを選択できます。

- **オンプレミスのActive Directory**。組織が所有し、その組織に属するActive Directoryアカウントでサインインするマシン。これらはオンプレミスに存在します。
- **Microsoft Entra ハイブリッド参加済み**。組織が所有し、その組織に属するActive Directory Domain Servicesアカウントでサインインするマシン。これらはクラウドとオンプレミスに存

在します。要件、制限、考慮事項については、「Microsoft Entra ハイブリッド参加済み」を参照してください。

> **注:**
>
> ◦ Microsoft Entraハイブリッド参加を使用する前に、Azure環境が前提条件を満たしていることを確認してください。「Microsoft Entraハイブリッド参加の構成」を参照してください。
>
> ◦ このオプションでは、マスターイメージがオペレーティングシステムの前提条件を満たしている必要があります。詳細については、「Microsoft Entraハイブリッド参加済みデバイス」を参照してください。

- **ドメインに参加していない**。どのドメインにも参加していないマシン。要件と制限については、「ドメインに参加していない」を参照してください。

> **重要:**
>
> - IDタイプとして**オンプレミスActive Directory**または**Microsoft Entraハイブリッド参加**を選択した場合、カタログ内の各マシンには対応するActive Directoryコンピューターアカウントが必要です。
> - **ドメイン非参加**のIDタイプでは、カタログの最小機能レベルとしてVDAバージョン2311以降が必要です。利用可能にするには、最小機能レベルを更新してください。

アカウントを作成する場合、マシンが存在するOUにコンピューターアカウントを作成する権限が必要です。カタログ内の各マシンは一意の名前を持つ必要があります。作成するマシンのアカウント命名規則を指定してください。詳細については、「マシンアカウント命名規則」を参照してください。

> **注:**
>
> OU名にスラッシュ（`/`）を使用しないようにしてください。

> 既存のアカウントを使用する場合は、アカウントを参照するか、**インポート**をクリックしてアカウント名を含む.csvファイルを指定します。インポートするファイルの内容は、次の形式を使用する必要があります。

- ADcomputeraccountname.domain

追加するすべてのマシンに対して十分なアカウントがあることを確認してください。Web Studioインターフェイスがそれらのアカウントを管理します。したがって、そのインターフェイスですべてのアカウントのパスワードをリセットできるようにするか、すべてのアカウントで同じパスワードを指定してください。

物理マシンまたは既存のマシンを含むカタログの場合、既存のアカウントを選択またはインポートし、各マシンをActive Directoryコンピューターアカウントとユーザーアカウントの両方に割り当てます。

マシンアカウント命名規則

カタログ内の各マシンは一意の名前を持つ必要があります。カタログを作成する際に、マシンアカウントの命名規則を指定する必要があります。名前に表示される連番または文字のプレースホルダーとして、ワイルドカード（ハッシュマーク）を使用します。

命名規則を指定する際は、次のルールに注意してください。

- 命名規則には少なくとも1つのワイルドカードを含める必要があります。すべてのワイルドカードはまとめて配置する必要があります。
- ワイルドカードを含む名前全体は、2文字以上15文字以下である必要があります。少なくとも1つの非数字文字と1つの#（ワイルドカード）文字を含める必要があります。
- 名前にスペースや次の文字を含めることはできません: `,~!@'$%\^&.(){\/*?"<>|=+[];:_".`。
- 名前はハイフン (-) で終わることはできません。

また、命名スキームを指定する際には、将来の拡張に十分な余裕を持たせてください。次の例を考えてみましょう。「veryverylong#」というスキームで1,000個のマシンアカウントを作成した場合、最後に作成されるアカウント名 (veryverylong1000) は16文字になります。したがって、この命名スキームでは、最大15文字を超えるマシン名が1つ以上生成されることになります。

シーケンシャル値が数字（0-9）か文字（A-Z）かを示すことができます。

- **0-9**。選択した場合、指定されたワイルドカードは連続する数字に解決されます。

> **注:**
>
> ワイルドカードが1つ (#) の場合、アカウント名は1から始まります。2つの場合、アカウント名は01から始まります。3つの場合、アカウント名は001から始まる、といった具合です。

- **A-Z**。選択した場合、指定されたワイルドカードは連続する文字に解決されます。

たとえば、PC-Sales-## という命名スキーム (かつ **0-9** が選択されている場合) では、PC-Sales-01、PC-Sales-02、PC-Sales-03などのアカウント名が生成されます。

オプションで、アカウント名の開始文字を指定できます。

- **0-9** を選択すると、アカウントは指定された数字から順に命名されます。前のフィールドで使用するワイルドカードの数に応じて、1桁以上の数字を入力します。たとえば、2つのワイルドカードを使用する場合は、2桁以上の数字を入力します。
- **A-Z** を選択すると、アカウントは指定された文字から順に命名されます。前のフィールドで使用するワイルドカードの数に応じて、1文字以上の文字を入力します。たとえば、2つのワイルドカードを使用する場合は、2文字以上の文字を入力します。

ドメイン資格情報

アカウント操作を実行する権限を持つ管理者の資格情報を入力します。詳細な手順は次のとおりです。

1. **資格情報の入力**をクリックします。Windowsセキュリティページが表示されます。
2. **ユーザー名**フィールドに、管理者のSamName、ユーザー名、またはユーザーSIDを入力します。
   - SamNameを入力すると、**ドメイン**フィールドが自動的に入力されます。
   - ユーザー名またはSIDを入力した場合、**ドメイン**フィールドにドメイン名またはSIDを入力することで、ユーザー検索を特定のドメインに限定できます。
3. **名前の確認**をクリックして、ユーザー名が有効か、または一意であるかを確認します。
4. **パスワード**フィールドに、管理者のドメインパスワードを入力します。
5. **完了**をクリックします。

> **注:**

> **マシンID**で選択したIDタイプが**Microsoft Entra ハイブリッド参加済み**の場合、入力する資格情報には`Write userCertificate`権限が付与されている必要があります。

概要、名前、および説明

「**概要**」ページで、指定した設定を確認します。カタログの名前と説明を入力します。この情報はWeb Studioに表示されます。

完了したら、**「完了」をクリックしてカタログの作成を開始します。 完了したら、**「完了」**を選択してカタログの作成を開始します。

マシンカタログに、新しいカタログがインラインの進行状況バーとともに表示されます。

作成の進行状況の詳細を表示するには：

1. マシンカタログにマウスカーソルを合わせます。
2. 表示されるツールヒントで、**詳細の表示**をクリックします。

   以下の項目を確認できる、段階的な進行状況グラフが表示されます。

   - ステップの履歴
   - 現在のステップの進行状況と実行時間
   - 残りのステップ

MCSの時刻同期

時刻同期は、マスターイメージと、結合されたマシンIDカタログのタイプによって決定されます。マスターイメージとカタログに応じて、次の時刻同期方法が適用されます。

マスターイメージ	カタログ	結果の時刻同期方法
NDJ	AD または Microsoft Entra ハイブリッド	デフォルトではNT5DSです。マスターイメージのレジストリ設定を使用して、MCSが時刻同期設定を変更するのを無効にできます。
NDJ	NDJ または Microsoft Entra ID	元の時刻同期設定と同じ

マスターイメージ	カタログ	結果の時刻同期方法
AD または Microsoft Entra ハイブリッド	AD または Microsoft Entra ハイブリッド	元の時刻同期設定と同じ
マイクロソフト エントラ ID	マイクロソフト エントラ ID	元の時刻同期設定と同じ

注:

元の時刻同期は、次のレジストリ設定によって制御され、変更できません。

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config

値: MaxAllowedPhaseOffset, MaxNegPhaseCorrection, and MaxPosPhaseCorrection

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

値: Type

MCSが時刻同期設定を変更するのを無効にするには、マスターイメージで次のレジストリ設定の値を設定します。

- `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix`
- 名前: TimeSyncMethodKeep
- 種類: DWORD
- 0 (または、値TimeSyncMethodKeepが構成されていない場合): 元の時刻同期設定を保持しません。
- 1: 元の時刻同期設定とデフォルトのパラメーター値を保持します。

カスタムプロパティの設定に関する重要な考慮事項

GCPおよびAzure環境では、`New-ProvScheme`と`Set-ProvScheme`でカスタムプロパティを正しく設定する必要があります。存在しないカスタムプロパティを指定すると、次のエラーメッセージが表示され、コマンドの実行に失敗します。

- Azureの場合: `Invalid property found: <invalid property>. Ensure that the CustomProperties parameter supports the property.`.
- GCPの場合: `Invalid property found: <invalid property>. Ensure that the value supplied for the property is supported in the Hypervisor.`.

トラブルシューティング

> **重要:**

> Web Studioを使用してマシンカタログを作成した後、`Get-ProvTask` PowerShellコマンドを使用して、マシンカタログ作成に関連するタスクを取得することはできません。この制限は、カタログが正常に作成されたかどうかにかかわらず、Web Studioがマシンカタログ作成後にそれらのタスクを削除するためです。

> Citrixでは、サポートチームが解決策を提供できるよう、ログを収集することをお勧めします。Citrix Provisioningを使用している場合は、次の手順でログファイルを生成します。

1. マスターイメージで、値1（DWORD (32ビット) 値として）を持つ次のレジストリキーを作成します: `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`。
2. マスターイメージをシャットダウンし、スナップショットを作成します。
3. Delivery Controllerで、次のPowerShellコマンドを実行します: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`。
4. そのスナップショットに基づいてカタログを作成します。
5. ハイパーバイザー上に準備VMが作成されたら、ログインしてC:\\のルートから次のファイル（Image-prep.logとPvsVmAgentLog.txt）を抽出します。
6. マシンをシャットダウンすると、その時点で障害が報告されます。
7. イメージ準備マシンの自動シャットダウンを再度有効にするには、次の PowerShell コマンドを実行します: `Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown`。

MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てる

MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てることができます。この実装により、使用するアプリケーションのドライブ文字とMCS I/Oライトバックキャッシュディスクのドライブ文字との間の競合を回避できます。これを行うには、PowerShellコマンドを使用します。サポートされているハイパーバイザーは、Azure、GCP、VMware、SCVMM、XenServerです。

> **注：**
>
> この機能には、VDAバージョン2305以降が必要です。

制限事項

- Windowsオペレーティングシステムのみに適用可能
- ライトバックキャッシュディスクに適用可能なドライブ文字: `E` から `Z`
- Azure一時ディスクがライトバックキャッシュディスクとして使用されている場合は適用されません
- 新しいマシンカタログを作成する場合にのみ適用可能

ライトバックキャッシュディスクにドライブ文字を割り当てる

ライトバックキャッシュディスクにドライブ文字を割り当てるには：

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*` を実行します。
3. IDプールがまだ作成されていない場合は作成します。詳細については、カタログの作成を参照してください。
4. `New-ProvScheme` コマンドと `WriteBackCacheDriveLetter` プロパティを使用してプロビジョニングスキームを作成します。例:

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "<name>" `

-IdentityPoolName $schemeName `
```

```
-ProvisioningSchemeName $schemeName `

-InitialBatchSizeHint 1 `

-UseWriteBackCache -WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `

-MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
resources.resourcegroup\MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxxx2130aa
145ec77.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\name\
\virtualprivatecloud.folder\\East US.region\
\virtualprivatecloud.folder\\abcd-resources.resourcegroup\\abcd-
resources-vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.folder\
\Standard_D2s_v5.serviceoffering" `

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS"/>

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk"
Value="false" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
Value="false" />
```

```
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-
group1" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

5. カタログの作成を完了します。

MCSマシンカタログを作成する前に構成を検証する

`New-ProvScheme`コマンドの`-validate`パラメーターを使用して、MCSマシンカタログを作成する前に構成設定を検証できます。このPowerShellコマンドをパラメーター付きで実行すると、誤ったパラメーターが使用されている場合や、パラメーターが別のパラメーターと競合している場合に、適切なエラーメッセージが表示されます。その後、エラーメッセージを使用して問題を解決し、PowerShellを使用してMCSマシンカタログを正常に作成できます。現在、この機能はAWS、Azure、GCP、およびVMwareの仮想化環境に適用できます。

注:

検証中は、実際のMCSマシンカタログを作成してはなりません。コマンドの結果を使用してエラーを修正し、その後で正常なカタログを作成する必要があります。したがって、`New-ProvScheme`コマンドを実行する際は、架空のIDプール名を使用してください。

構成を検証するには、次の手順を実行します。

1. Delivery ControllerホストからPowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. `New-ProvScheme`コマンドを実行し、`-validate`パラメーターを使用します。コマンドが機能するように、偽のIDプール名を提供します。例:

```
$result =New-ProvScheme  -CleanOnBoot -HostingUnitName "vSanRg"
-IdentityPoolName "mptmpcatalogdemo" -InitialBatchSizeHint 1  -
MasterImageVM "XDHyp:
\HostingUnits\vSanRg\Windows19MasterImage.vm\Citrix_XD_NonMachineProfil
```

```
eWin19Machines.snapshot" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vSanRg\\VM Network.network"} -ProvisioningSchemeName
"MachineProfileW10Machines"  -Scope @()

-VMCpuCount 2  -VM

MemoryMB 6143 -MachineProfile "XDHyp:\HostingUnits\vSanRg\TRW-Win11-
tpm-BL-TEMPLATE.template" -TenancyType Shared  -FunctionalLevel "L7_20"
-Validate

$result.TerminatingError | Format-List -Property *
```

エラーメッセージ:

```
ErrorData    : {[[ValidationFailureCount, xxx], [InvalidMemoryValue,
The memory size provided 6143 must be a multiple of 4 MB and must be
greater than or equal to 4 MB.], [InconsistentGuestOsSetting, The
GuestOs setting - windows9_64Guest of the selected machine profile does
not match with the setting - windows2019srv_64Guest of master image.
Please select a machine profile that matches the GuestOs setting of the
master image.], [InconsistentVtpmSetting, The vTPM setting of the
selected machine profile does not match with the selected master image.
Please select a machine profile that matches the vTPM setting of the
master image.], [InconsistentFirmwareSetting, The firmware setting -
efi of the selected machine profile does not match with the setting -
bios of master image. Please select a machine profile that matches the
firmware setting of the master image ErrorId      : ValidationFailure

ErrorMessage : ValidationFailure

Operation    : ValidatingInputs
```

4. 構成設定を検証した後、実際のIDプール名と正しいパラメーターを使用してMCSマシンカタログを作成できます。

VMをAzure Arcにオンボードする

Azure Arcを使用すると、組織はどこにホストされているVMなどのリソースを、Azureで実行されているかのように管理できます。Azure Arcを使用すると、Azure MonitorなどのAzureサービスを利用して、リソースの包括的な可視性とプロアクティブな管理を実現できます。

VM を Azure Arc にオンボードするには、`New-ProvScheme` コマンドを使用して MCS マシンカタログを作成します。`Set-ProvScheme` コマンドを使用して既存のカタログを更新することもできます。カタログに追加された新しい VM のみが Azure Arc にオンボードされます。

現在、この機能は、Citrix のすべてのオンプレミスハイパーバイザーである VMware、Nutanix、SCVMM に適用されます。

前提条件

MCS カタログで Azure Arc オンボーディングを有効にする前に、以下を考慮してください。

- 以下の Azure リソースグループ:
  - Arc サーバーの読み取り、作成、削除を行うための `Allows` アカウント。
  - VM 拡張機能、ライセンス、プライベートリンクスコープを管理するための `Allows` アカウント。
  - リソースグループスコープでサービスプリンシパルに割り当てられている `Azure Connected Machine Resource Administrator` ロール。

Azure portal を使用して Azure ロールを割り当てる を参照してください。

- 以下のマスターイメージ:
  - VDA: 2311 以降 (2411 を除く)。

    > **注記:**
    >
    > CVAD 2411では、Azure Arcオンボーディングはサポートされていません。

  - AzureConnectedMachineAgent エージェントがインストールされていること。MSI は、Microsoft のドキュメントの Windows または Linux セクションからダウンロードできます。

VM を Azure Arc にオンボードする手順

1. `AzureArcResourceManagement` の機能を持つサービスアカウントを設定します。

   サービスアカウントは、Microsoft Entra IDのようなIDプロバイダーにアクセスするための資格情報を保存することで、認証または承認に使用されます。各サービスアカウントは、単一のIDプロバイダーに紐付けられます。

`AzureArcResourceManagement capability`を使用してAzureADにアクセスするための新しいサービスアカウントを作成するには、以下を実行します。

```
New-AcctServiceAccount -IdentityProviderType “AzureAD”
-IdentityProviderIdentifier “tenant-id” -AccountId “application-id”
-AccountSecret “application-secret” -Capabilities
“AzureArcResourceManagement”
```

`application-id`は、Azure Connected Machine Resource Administratorロールが割り当てられたサービスプリンシパルと同じである必要があります。

2. サービスアカウントをIDプールに割り当てます。例:

```
Set-AcctIdentityPool -IdentityPoolUid “idn-pool-uid” -ServiceAccountUid
“service-account-uid”
```

3. 以下のArcパラメーターを使用してMCSカタログを作成または更新します。

- `EnableAzureArcOnboarding`: カタログでArcオンボーディングを有効にする必要があるかどうかを示します。
- `AzureArcSubscriptionId`: Arc接続されたVMが作成されるAzureサブスクリプションを示します。
- `AzureArcRegion`: Arc接続されたVMが作成されるAzureリージョンを示します。
- `AzureArcResourceGroup`: Arc接続されたVMが作成されるAzureリソースグループを示します。Azure Arcリソースグループの詳細については、を参照してください。

例: 新しいカタログでAzure Arcオンボーディングを有効にするには:

```
`New-ProvScheme -ProvisioningSchemeName "demo" -MasterImageVM "XDHyp:
\HostingUnits\hosting-unit\masterVMName.vm\masterSnapshotName.snapshot"
-HostingUnitName “hosting-unit” -IdentityPoolName “identity-pool”`



-EnableAzureArcOnboarding -AzureArcSubscriptionId “azure-sub”
-AzureArcResourceGroup “azure-resourcegroup” - AzureArcRegion “azure-
region”
```

例: 既存のカタログでAzure Arcオンボーディングを有効にするには:

```
Set-ProvScheme -ProvisioningSchemeName "demo" -EnableAzureArcOnboarding
$true -AzureArcSubscriptionId “azure-sub” -AzureArcResourceGroup
“azure-resourcegroup” - AzureArcRegion “azure-region”
```

例: 既存のカタログでAzure Arcオンボーディングを無効にするには:

```
Set-ProvScheme -ProvisioningSchemeName "demo" -EnableAzureArcOnboarding
$false:
```

4. カタログに新しいマシンを追加してArcをオンボードします。
5. VMの電源をオンにした後、Azureポータルで**AzureArcResourceGroup**の下に接続されたマシンとしてVMを確認する必要があります。

考慮事項

- Arc のオンボーディングは現在、新しい VM のみでサポートされています。そのため、`Set-ProvScheme` を使用して既存のカタログを更新した場合、新しく追加された VM のみが最初に電源がオンになったときに Arc にオンボーディングされます。
- Arc カスタムプロパティは、下位互換性のために既存のカタログで引き続きサポートされています。ただし、`EnableAzureArcOnboarding` のような Arc カスタムプロパティを使用して `New-ProvScheme` を実行すると、カタログの作成は失敗します。
- `EnableAzureArcOnboarding` を `true` として構成する場合、`New-ProvScheme` と `Set-ProvScheme` のすべてのパラメーターを追加する必要があります。

トラブルシューティング

`New-ProvScheme` を使用して SCVMM カタログを作成すると、次のエラーが発生する場合があります。

```
Master Image/Machine Profile's VM's device id is different than the
NetworkMapping's device id '0'. Please provide a device id that matches
the master image/machine profile.
```

その場合は、`New-ProvScheme` の `NetworkMapping` パラメーターで `DeviceId` を明示的に指定してください。例:

```
New-ProvScheme -ProvisioningSchemeType "MCS" -InitialBatchSizeHint 1
-HostingUnitName $HostingUnitName `

            -IdentityPoolName $CatalogName -MasterImageVM $MasterImage
-ProvisioningSchemeName $CatalogName `

            -VMCpuCount 2 -VMMemoryMB 4096  -EnableAzureArcOnboarding `

            -AzureArcSubscriptionId $AzureArcSubscription -AzureArcRegion
$AzureArcRegion `

            -AzureArcResourceGroup $AzureArcResourceGroup

            -NetworkMapping @{"FDDxxxxxx-xxxx-4xxx-9EBC-3xxxxxxxx"="XDHyp:
\HostingUnits\<hosting unit name>\abc.network"}
```

次のステップ

特定のクラウドサービスカタログの作成については、以下を参照してください。

- AWSカタログの作成
- XenServerカタログの作成
- Google Cloud Platformカタログの作成
- Microsoft Azureカタログの作成
- マイクロソフト システム センター バーチャル マシン マネージャー カタログの作成
- Nutanixカタログの作成
- VMware カタログを作成する

これが最初に作成するカタログである場合、Web Studio は デリバリーグループを作成するように案内します。

構成プロセス全体を確認するには、インストールと構成を参照してください。

Web Studio と PowerShell を使用して、Citrix Provisioning カタログを作成できます。 この実装には、次の利点があります。

- MCS と Citrix Provisioning カタログの両方を管理するための単一の統合コンソール。
- ID 管理ソリューション、オンデマンドプロビジョニングなど、Citrix Provisioning カタログの新機能を利用できます。

現在、この機能は Azure および VMware ワークロードでのみ利用可能です。ただし、VMware 環境では、PowerShell コマンドのみを使用してカタログを作成できます。詳細については、Citrix Studio で Citrix Provisioning カタログを作成するを参照してください。

詳細情報

- 接続とリソースの作成および管理
- 異なる参加タイプのカタログを作成する
- マシンカタログの管理

AWS EC2カタログを作成する

マシンカタログの作成では、マシンカタログを作成するウィザードについて説明します。以下の情報は、AWS EC2仮想化環境に固有の詳細を扱います。

> **注:**
>
> AWSカタログを作成する前に、AWSへの接続の作成を完了する必要があります。AWS EC2への接続を参照してください。

イメージ準備中のネットワーク設定

イメージ準備中に、元のVMに基づいて準備用仮想マシン（VM）が作成されます。この準備用VMはネットワークから切断されます。準備用VMからネットワークを切断するために、すべてのインバウンドおよびアウトバウンドトラフィックを拒否するネットワークセキュリティグループが作成されます。このネットワークセキュリティグループは永続化され、再利用されます。ネットワークセキュリティグループの名前は`Citrix.XenDesktop.IsolationGroup-GUID`で、GUIDはランダムに生成されます。

AWSテナンシー

AWSは以下のテナンシーオプションを提供します。

- 共有テナンシー（デフォルトタイプ）と専用テナンシー。共有テナンシーとは、異なる顧客の複数のAmazon EC2インスタンスが同じ物理ハードウェア上に存在する可能性があることを意味します。
- 専用テナンシーとは、デプロイした他のインスタンスと同じハードウェア上でのみEC2インスタンスが実行されることを意味します。他の顧客は同じハードウェアを使用しません。

AWSホストへのプロビジョニングの要件

- インポートされたBYOL（bring your own license）イメージ（AMI）。専用ホストでは、既存のライセンスを使用および管理します。
- プロビジョニング要求を満たすのに十分な利用率を持つ専用ホストの割り当て。
- **自動配置**を有効にする。

AWSテナンシーを設定するオプション

- **共有ハードウェアを使用**。この設定は、ほとんどの展開に適しています。複数の顧客が互いにやり取りすることはありませんが、ハードウェアの一部を共有します。共有ハードウェアを使用することは、Amazon EC2インスタンスを実行するための最も安価なオプションです。
- **専用ホストを使用**。Amazon EC2専用ホストは、EC2インスタンス容量が完全に専用化された物理サーバーであり、既存のソケットごとまたはVMごとのソフトウェアライセンスを使用できます。専用ホストには、インスタンスタイプに基づいて事前に設定された利用率があります。たとえば、C4 Largeインスタンスタイプの単一の割り当て済み専用ホストは、16インスタンスの実行に制限されています。詳細については、AWSサイトを参照してください。

  この設定は、ライセンス制限や専用ホストの使用を必要とするセキュリティ要件がある展開に適しています。専用ホストを使用すると、物理ホスト全体を所有し、時間単位で課金されます。そのホストを所有することで、追加料金なしで、そのホストが許可する数のEC2インスタンスを起動できます。
- **専用インスタンスを使用**。この設定は、特定のセキュリティ要件またはコンプライアンス要件がある展開により適しています。専用インスタンスを使用すると、他のAWS顧客とは別のホストを持つという利点を享受できますが、ホスト全体に対して料金を支払う必要はありません。ホストの容量について心配する必要はありませんが、インスタンスに対してはより高い料金が課金されます。

> **注：**
>
> カタログ作成またはイメージ更新タスクが進行中でない場合、利用可能な準備IDディスクを削除できます。

> Studioを使用してAWSテナンシーを構成するには、(#create-a-catalog-using-web-studio)を参照し、PowerShellを使用するには、(#configure-aws-dedicated-host-tenancy-using-the-powershell)を参照してください。

AWS運用リソースのタグ付け

Amazon マシンイメージ (AMI) は、Amazon Cloud 環境内で仮想マシンを作成するために使用される仮想アプライアンスの一種であり、一般に EC2 と呼ばれます。AMI を使用して、EC2 環境を使用するサービスを展開します。AWS 用の MCS を使用してマシンをプロビジョニングするカタログを作成するときは、そのカタログのゴールデンイメージとして機能する **AMI** を選択します。

> **重要:**
>
> 運用リソースのタグ付けを使用するには、マシンプロファイルと起動テンプレートの両方を使用してカタログを作成する必要があります。

> AWSカタログを作成するには、まずゴールデンイメージとするインスタンスのAMIを作成する必要があります。MCSはそのインスタンスからタグを読み取り、起動テンプレートに組み込みます。起動テンプレートのタグは、以下のものを含む、AWS環境で作成されたすべてのCitrix®リソースに適用されます。

- 仮想マシン
- VMディスク
- VMネットワークインターフェイス
- S3 バケット
- S3 オブジェクト
- 起動テンプレート
- AMI

カタログの作成中に、Studio および PowerShell を使用して運用リソースにタグを付けることができます。Studio の場合は、Web Studio を使用したカタログの作成 (「**イメージ**」ページ) を参照してください。PowerShell の場合は、PowerShell を使用した運用リソースのタグ付け を参照してください。

カタログを作成する

次のいずれかを使用してカタログを作成できます。

- ウェブスタジオ
- PowerShell

Web Studio を使用してカタログを作成する

1. 左側のナビゲーションペインで、 をクリックします。
2. をクリックします。「**マシンカタログのセットアップ**」ページが表示されます。
3. 「**マシンタイプ**」ページで、カタログのマシンタイプ (例: マルチセッション OS) を選択します。
4. 「**マシン管理**」ページで、次の設定を選択します。
   a. 電源管理されているマシン (仮想マシンやブレード PC など) を選択します。
   b. 「**Citrixプロビジョニングテクノロジー**」を選択します。次に、「**Citrix Machine Creation Services™**」を選択します。
   c. **リソース**フィールドで、ホスト接続の作成時に構成したリソース（アベイラビリティゾーンまたはローカルゾーン）を選択し、**次へ**をクリックします。
5. **デスクトップエクスペリエンス**ページで、ユーザーがログインしたときに使用するランダムまたは静的デスクトップを選択します。
6. **イメージ**ページで：
   a. カタログ内のすべてのマシンのマスターイメージとして使用するマシンのテンプレートを選択します。
   b. カタログ内のVMにマシンプロファイルから構成を継承させたい場合は、マシンプロファイルを選択します。デフォルトでは、**マシンプロファイルを使用**チェックボックスが選択されています。マシンプロファイルのソースを別のVMまたは起動テンプレートバージョンに変更するには、編集ボタンをクリックします。
   c. **運用リソースにマシンタグを適用**チェックボックスをオンにして、運用リソースにマシンタグを適用します。このオプションは、マシンのプロビジョニングを容易にするためにAWS環境で作成されたすべての項目にマシンタグを適用するかどうかを制御します。運用リソースは、カタログ作成の副産物として作成されます。これには、準備VMインスタンスやAMIなどの一時的および永続的なリソースの両方が含まれます。

> **注:**
>
> **セキュリティ**ページは、マシンプロファイルを割り当てずにマシンカタログを作成している場合にのみ表示されます。

7. 「**仮想マシン**」ページで：

a. カタログのVM数を入力します。

b. デフォルトのマシン仕様が表示されます。これはマシンプロファイルに基づいています。変更するには、編集アイコンを選択し、マシン仕様を選択します。

c. AWSテナンシーを構成します。「AWSテナンシーを構成するオプション」を参照してください。

d. プライマリマシンサイズが最大容量に達した場合に、セカンダリVMを構成することもできます。「**セカンダリサイズ**」（オプション）をクリックします。「**セカンダリマシンサイズ**」ウィンドウには、スポットVMタイプと通常VMタイプの両方を持つVMが一覧表示されます。最大10個のセカンダリマシンサイズを選択できます。10個のVMが選択されると、他のVMはそれ以上選択できなくなります。「**次へ**」をクリックします。「**セカンダリマシンサイズ**」ブレードでは、複数のマシンサイズを選択し、ドラッグアンドドロップで優先順位を変更できます。「**完了**」をクリックします。選択したマシンサイズは「セカンダリサイズ」（オプション）に表示されます。必要に応じて編集アイコンをクリックして編集します。

8. **セキュリティ**ページは、マシンプロファイルを割り当てずにマシンカタログを作成する場合にのみ表示されます。**セキュリティ**ページを使用して、VM のセキュリティグループを構成します。これは、既存のマシンカタログを編集およびクローン作成する場合にも適用されます。

   マシンプロファイルベースのマシンカタログを作成する場合、セキュリティグループの構成はマシンプロファイルから継承され、**セキュリティ**ページは表示されません。

9. **NIC**ページで、VMのNIC（またはENI）を選択します。

10. **ディスク設定**ページで、ライトバックキャッシュを有効にするかどうかを選択します。

11. **マシンID**ページで、ドメインを選択し、このマシンカタログで作成するVMの新しいADアカウントを作成して、カタログ内のマシンに対してオンプレミスのActive DirectoryまたはMicrosoft Entraハイブリッド参加を構成します。プロビジョニングされたVMは、選択したドメインに参加します。VM用に作成する新しいADアカウントのアカウント命名スキームを指定します。「次へ」をクリックします。

12. **ドメイン資格情報**ページで、**資格情報の入力**をクリックして、選択したドメインの資格情報を入力します。プロンプトが表示されたら、管理者レベルのユーザー名とパスワードを入力します。製品ドキュメントに従ってドメイン資格情報を以前に保存している場合は、サービスアカウントを使用することもできます。

13. **概要**ページが表示されるまで、残りのページをクリックします。マシンカタログの名前を入力し、**完了**を選択してマシンカタログを作成します。

AWSローカルゾーンでのマシンカタログ作成に関する制限事項

- 特定のローカルゾーンは特定のハードウェア構成のみをサポートします（たとえば、パースのローカルゾーンはGP3ボリュームをサポートせず、GP2のみをサポートします）。
- gp2のみがすべてのローカルゾーンで普遍的にサポートされており、すべてがgp3をサポートしているわけではないため、IDディスクの作成はデフォルトでgp2ボリュームタイプを使用します。
- 目的のローカルゾーンでサポートされているハードウェア仕様を持つマシンプロファイルを選択する必要があります。
- 準備済みイメージAMIスナップショットとIDディスクスナップショットは、デフォルトでローカルゾーンではなくリージョンに配置されます（ローカルゾーンでのEBSスナップショットサポートの可視性に関するAWSの制限のため）。
- 完全なEC2およびEBSサービスをサポートするローカルゾーンのみがサポート対象ゾーンです。

PowerShellを使用してカタログを作成する

PowerShell を使用して AWS 専用ホストのテナンシーを構成する

または、PowerShellを介してAWS専用ホストをプロビジョニングすることもできます。`TenancyType`パラメーターを`Host`に設定して、`New-ProvScheme`コマンドレットを使用します。

PowerShell を使用して運用リソースにタグを付ける

PowerShell を使用してリソースにタグを付けるには：

1. DDC ホストから PowerShell ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、コマンド `asnp citrix` を実行します。

プロビジョニングされた VM のリソースにタグを付けるには、カスタムプロパティ `AwsOperationalResourcesTagging` を使用します。例：

```
New-ProvScheme -ProvisioningSchemeName test

-CustomProperties “AwsOperationalResourcesTagging,true”

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

```
... <Other <standard provscheme parameters>
```

MCSIO が有効なカタログ

MCS Storage Optimization (MCSIO) は、ディスク操作をメモリまたは小型の高速ディスクにキャッシュすることで、VM のパフォーマンスを向上させます。PowerShell コマンドを使用して、MCSIO が有効な非永続カタログを作成できます。このようなカタログを作成するには、AMI インスタンスの準備中に VDA をインストールまたはアップグレードする際に、MCSIO ドライバーをインストールする必要があります。デフォルトでは、このドライバーはインストールされません。

MCSIO AMI の準備が完了したら（VDA のインストール時に MCSIO ドライバーをインストールに含めるオプションを選択した場合）、MCSIO が有効な非永続カタログを作成できます。

注：

Studio を使用してディスクキャッシュのみ（メモリキャッシュなし）で MCSIO を構成するオプションは、すべてのハイパーバイザーおよびクラウドサービス環境で削除されました。

MCSIO が有効なカタログを作成する

New-ProvScheme PowerShell コマンドに追加された4つのパラメーターは次のとおりです。

- `UseWriteBackCache`: 指定されたプロビジョニングスキームのキャッシュ（ライトバックキャッシュ）をオンにします
- `WriteBackCacheDiskSize`: キャッシュに使用される一時ディスクのサイズを GB 単位で指定します
- `WriteBackCacheMemorySize`: キャッシュに使用するメモリ量を MB 単位で指定します。これはオプションのパラメーターです。

注:

- `WriteBackCacheDiskSize` の値は、少なくとも 1 GB のキャッシュディスクストレージが必要なため、ゼロより大きくする必要があります。キャッシュディスクサイズは、OS ディスクサイズより大きくしてはいけません。

- `WriteBackCacheMemorySize` の値は、ゼロ以外で、マシンカタログのメモリサイズより小さくする必要があります。

MCSIOに影響するカスタムプロパティは次のとおりです。

- `WBCDiskStorageType`: AWSの一時ディスクに使用されるボリュームタイプを定義します。このパラメーターは、`volume-type[:iops][:throughput]` の形式で文字列引数を取ります。ボリュームタイプは次のとおりです。
  - gp2: このボリュームタイプではiopsおよびスループットパラメーターを使用しないでください
  - gp3: このボリュームタイプではiopsおよびスループットパラメーターを使用してください
  - io1: このボリュームタイプではiopsパラメーターのみを使用してください
  - io2: このボリュームタイプではiopsパラメーターのみを使用してください

  デフォルトのボリュームタイプは **gp2** です。
- `PersistWBC`: AWS インスタンスの電源がオフになったときに、キャッシュディスクを保持するか破棄するかを制御します。`true` に設定すると、キャッシュディスクは保持されます。`false` (デフォルト) に設定すると、キャッシュディスクは AMI インスタンスの電源がオンになっている間のみ作成および保持されます。
- `PersistOSDisk`: AWS インスタンスの電源がオフになったときに、OS ディスクを保持するか破棄するかを制御します。`true` に設定すると、OS ディスクは保持されます。`false` (デフォルト) に設定すると、OS ディスクは AMI インスタンスの電源がオンになっている間のみ作成および保持されます。

PowerShellウィンドウで、MCSIOが有効な非永続カタログを作成するには、次の手順を実行します。

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*` を実行します。
3. ブローカーカタログとIDプールを作成します。
4. プロビジョニングスキームを作成します。例：

```
$HostingUnitUid = '0xxxx1d9-bbfc-xxxf-bxxb-exxxxxe008b2'

$MasterImageVM = 'XDHyp:\HostingUnits\ctx-test\aws-apollo-non-
persistent-multi-mcsio-vda-win2022 (ami-0bf1810488acbxxxb).template'
```

```
$NetworkMap = @{ 'NetworkPath' = 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\10.0.128.0`/17
(vpc-0fa6e41d72507fxxx).network' }

$SecurityGroup = $( 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\private.securitygroup' )

$ServiceOffering = 'XDHyp:\HostingUnits\ctx-test\T3 Medium
Instance.serviceoffering'

$CustomProperties = 'WBCDiskStorageType,gp3:6000:250;PersistWBC,false'




$provScheme = New-ProvScheme -ProvisioningSchemeName $CatalogName
-HostingUnitUid $HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

- MasterImageVM $MasterImageVM `

-NetworkMap $NetworkMap `

-ServiceOffering $ServiceOffering `

-SecurityGroup $SecurityGroup `

-CustomProperties $CustomProperties `

-UseWriteBackCache -WriteBackCacheDiskSize 16 -WriteBackCacheMemorySize
256
```

5. カタログにVMを追加します。

MCSIOで起動パフォーマンスを向上させる

MCSIOを有効にし、`PersistWBC`と`PersistOSDisk`のカスタムプロパティを`tru`eに設定すると、VMの起動パフォーマンスを向上させることができます。この設定により、VMは新しいキャッシュディスクを初期化したり、テンプレートからルートディスクを再作成したりする必要がないため、より高速に起動できます。

PowerShellを使用してマシンプロファイルベースのマシンカタログを作成する

マシンプロファイルを使用して、EC2インスタンス（VM）または起動テンプレートバージョンからハードウェアプロパティをキャプチャし、プロビジョニングされたマシンに適用できます。キャプチャされるプロパティには、たとえば、EBSボリュームプロパティ、インスタンスタイプ、EBS最適化、CPUオプション、テナンシータイプ、休止状態機能、セキュリティグループ、およびその他のサポートされているAWS構成が含まれます。

マシンプロファイルの入力として、AWS EC2インスタンス（VM）またはAWS起動テンプレートバージョンを使用できます。

> **注:**
>
> EBSボリュームプロパティは、マシンプロファイルからのみ派生します。

重要な考慮事項

MCSマシンカタログを作成する際の重要な考慮事項：

- `New-ProvScheme`および`Set-ProvScheme`コマンドでマシンハードウェアプロパティパラメーターを追加すると、パラメーターで指定された値がマシンプロファイルの値よりも優先されます。
- `AwsCaptureInstanceProperties`を`true`として設定し、`MachineProfile`プロパティを設定しない場合、IAMロールとタグのみがキャプチャされます。
- `AwsCaptureInstanceProperties`と`MachineProfile`を同時に設定することはできません。

  > **注:**
  >
  > `AwsCaptureInstanceProperties` は非推奨です。

- マシンプロファイルが提供されていない場合は、以下のプロパティの値を明示的に指定する必要があります。
  - セキュリティグループ
  - ENI または仮想ネットワーク

- `AwsOperationalResourcesTagging` は、`AwsCaptureInstanceProperties` を有効にするか、マシンプロファイルを指定した場合にのみ有効にできます。

MCS マシンカタログを作成した後の重要な考慮事項は次のとおりです。

- マシンプロファイルベースのカタログから、非マシンプロファイルベースのカタログに変更することはできません。

マシンプロファイル入力でセキュリティグループを構成する

プロビジョニングされた VM に ENI (ネットワークインターフェイス) ごとにセキュリティグループが割り当てられる MCS マシンカタログを作成できます。これを行うには、異なるセキュリティグループが個別の ENI にマッピングされているマシンプロファイル入力 (EC2 インスタンスまたは起動テンプレート) を使用します。たとえば、マシンプロファイル入力に SG 1 を持つ ENI A と SG 2 を持つ ENI B がある場合、プロビジョニングされた VM も SG 1 を持つ ENI A と SG 2 を持つ ENI B を持つ必要があります。

ネットワークインターフェイスの詳細を取得する

インターフェイスの SubnetId、割り当てられたセキュリティグループ、および割り当てられたネットワークを含むネットワークインターフェイスデータレコードのリストを取得するには、以下のコマンドを実行します。

```
(Get-HypInventoryItem -LiteralPath 'XdHyp:\HostingUnits\cvad-test' –
ResourceType vm). AdditionalData
```

注:

MCS は現在、ネットワークインターフェイスごとに複数のネットワークを許可していません。

マシンプロファイルを使用してマシンカタログを作成する

マシンプロファイルを使用してマシンカタログを作成するには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために、`asnp citrix*`を実行します。
3. まだ作成されていない場合は、IDプールを作成します。例：

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain abcdf -NamingSchemeType Numeric
```

4. New-ProvSchemeコマンドを実行します。例：

```
New-ProvScheme -ProvisioningSchemeName demet-test-1

-HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1

-IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4

-CleanOnBoot

-MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-demet-
ami.0 (ami-0ca813xxxxxx061ef).template'

-MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-
east-1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).vm'
```

5. カタログの作成を完了します。

マシンプロファイルを更新する

マシンプロファイルで最初にプロビジョニングされたカタログのマシンプロファイルを更新するには、次の手順を実行します。MCSマシンカタログを編集する際に、マシンプロファイルソースのテナンシータイプと休止状態機能を変更することもできます。

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme `

-ProvisioningSchemeUid "<ID" `

-MachineProfile "XDHyp:\HostingUnits\abc\us-
east-1a.availabilityzone\citrix-cvad-machineprofile-instance
(i-0xxxxxxxx).vm"
```

PowerShellを使用して起動テンプレートバージョンでカタログを作成する

起動テンプレートバージョンをマシンプロファイル入力として使用して、MCSマシンカタログを作成できます。また、マシンプロファイルカタログの入力をVMから起動テンプレートバージョンに、または起動テンプレートバージョンからVMに更新することもできます。

AWS EC2コンソールでは、起動テンプレートのインスタンス構成情報とバージョン番号を提供できます。マシンカタログの作成または更新時に、起動テンプレートバージョンをマシンプロファイル入力として指定すると、そのバージョンの起動テンプレートのプロパティがプロビジョニングされたVDA VMにコピーされます。

以下のプロパティは、マシンプロファイル入力を使用するか、`New-ProvScheme`または`Set-ProvScheme`コマンドで明示的にパラメーターとして指定できます。`New-ProvScheme`または`Set-ProvScheme`コマンドで指定された場合、これらのプロパティのマシンプロファイル値よりも優先されます。

- サービス提供
- ネットワーク
- テナンシータイプ

> **注：**
>
> マシンプロファイルの起動テンプレートでサービス提供が指定されていない場合、または`New-ProvScheme`コマンドのパラメーターとして指定されていない場合、適切なエラーが発生します。

> 起動テンプレートバージョンをマシンプロファイル入力として使用してカタログを作成するには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. 起動テンプレートの起動テンプレートバージョンの一覧を取得します。例：

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate> ls |
Select FullPath
```

4. 作成されていない場合は、IDプールを作成します。例：

```
New-AcctIdentityPool `

-IdentityPoolName "abc11" `

-NamingScheme "abc1-##" `
```

```
-NamingSchemeType Numeric `

-Domain "citrix-xxxxxx.local" `

-ZoneUid "xxxxxxxx" `
```

5. 起動テンプレートバージョンをマシンプロファイル入力として使用してプロビジョニングスキームを作成します。例：

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-persistent-
vda-win2022 (ami-0axxxxxxxxxxx).template" `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

6. プロビジョニングスキームをブローカーカタログとして登録します。例：

```
New-BrokerCatalog -Name "MPLT1" `

-AllocationType Random `

-Description "Machine profile catalog" `

-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `

-ProvisioningType Mcs `

-SessionSupport MultiSession `

-PersistUserChanges Discard
```

7. カタログの作成を完了します。

マシンプロファイルソースを更新する

マシンプロファイルカタログの入力を、VMから起動テンプレートバージョンへ、または起動テンプレートバージョンからVMへ更新することもできます。例：

- マシンプロファイルカタログの入力をVMから起動テンプレートバージョンに更新するには：

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxxx
(1).launchtemplateversion"
```

- マシンプロファイルカタログの入力を起動テンプレートバージョンからVMに更新するには：

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-
east-1a.availabilityzone\apollo-non-persistent-vda-win2022-2
(i-08xxxxxxxxx).vm"
```

OS、ID、WBCディスクを暗号化する

AWS KMSキー（カスタマーマネージドキーおよびAWSマネージドキー）を使用して、OSディスク、IDディスク（ID）、ライトバックキャッシュディスク（WBC）の暗号化に使用できる、永続および非永続VMカタログを作成できます。

- AWSマネージドキーは毎年自動的にローテーションされます。
- カスタマーマネージドキーは自動ローテーションがオプションであり、手動で管理できます。

KMSキーの詳細については、以下のAWSドキュメントを参照してください:

- AWS KMS の概念
- 自動キーローテーションの仕組み

OS、ID、WBCディスクの暗号化には、次のいずれかを構成します。

- 暗号化されたマスターイメージを使用します (たとえば、KMSキーで暗号化されたEBSルートボリュームを含むインスタンスまたはスナップショットから作成されたAMI)

- 暗号化されたEBSルートボリュームを含むマシンプロファイルソース (VMまたは起動テンプレート) を使用します。

制限事項

以下の制限事項を考慮してください:

- MCS は現在、マスターイメージ AMI 上のディスクを 1 つのみサポートしています。
- 既存の暗号化されていない EBS ボリュームまたはスナップショットを直接暗号化したり、既存の暗号化されたボリュームの KMS キーを変更したりすることはできません。これを行うには、次の手順を実行する必要があります。

  a. そのボリュームの新しいスナップショットを作成します。

  b. そのスナップショットから新しいボリュームを作成します。

  c. 新しいボリュームを暗号化します。

以下の AWS ドキュメントを参照してください。

- 暗号化されていないリソースを暗号化する
- EBS ボリュームの自動またはデフォルトの暗号化の制限: 既存および新規の Amazon EBS ボリュームを自動的に暗号化する。

ディスク暗号化を使用してカタログを作成する

ディスク暗号化を使用して MCS マシンカタログを作成するには、次のものを使用できます。

- マスターイメージ
- マシンプロファイル

マシンプロファイル入力を使用する際の考慮事項は次のとおりです。

- マシンプロファイル入力のKMSキーは、マスターイメージのKMSキーよりも優先されます。
- マシンプロファイル入力が提供されない場合、マスターイメージAMIのKMSキーがカタログVMのディスクを暗号化するために使用されます。
- マシンプロファイルにブロックデバイスマッピングが存在する場合、マスターイメージテンプレート（AMI）とマシンプロファイルに存在するブロックデバイスは一致している必要があります。たとえば、AMIに`/dev/sda1`で定義されたデバイスがある場合、マシンプロファイルにも`/dev/sda1`で定義されたデバイスが必要です。
- マシンプロファイルソースにキーがなく、マスターイメージが暗号化されていない場合、カタログVMのディスクは暗号化されません。

- マスターイメージが暗号化されている場合、マシンプロファイルソースVMまたは起動テンプレートには、有効な入力と見なされるために暗号化されたルートボリュームが必要です。

既存のカタログを変更する

`Set-ProvScheme` PowerShellコマンドを使用して、既存のカタログを次のように変更できます。

- 新しいKMSキーを含むボリュームを持つマシンプロファイル入力。
- 新しいKMSキーで暗号化されたマスターイメージテンプレートAMI。

重要な考慮事項:

- カタログに追加された新しいVMのボリュームは、新しいKMSキーで暗号化されます。
- 既存のマシンプロファイルがある場合に暗号化設定を更新するには、新しいマシンプロファイルで`Set-ProvScheme`を実行します。
- 既存のカタログを暗号化されたボリュームから暗号化されていないボリュームに変更することはできません。 暗号化されたマスターAMIから暗号化されていないマスターAMIへのイメージ更新はできません。

VMインスタンスのNitroTPMとUEFIセキュアブートを有効にする

カタログを作成する際、NitroTPMおよび/またはUEFIセキュアブートが有効なマスターイメージ (AMI) を選択できるようになりました。これにより、カタログ内のプロビジョニングされたVMもNitroTPMおよび/またはUEFIセキュアブートが有効になります。この実装により、VMが保護され、信頼できるものになります。NitroTPMおよびUEFIセキュアブートの詳細については、Amazonドキュメントを参照してください。

制限事項

- 現在、NitroTPMとセキュアブートの両方を、中国を除くすべてのAWSリージョン (AWS GovCloud (US) リージョンを含む) で使用できます。
- 既存のカタログでNitroTPMとUEFIセキュアブートを有効にすることはできません。NitroTPMとUEFIセキュアブートが有効なカタログが必要な場合は、新しいカタログを作成してください。

主な手順

1. AWS環境をセットアップします。
2. AWSへの接続を作成します。
3. NitroTPMおよび/またはUEFIセキュアブートが有効なマスターイメージ（AMI）を作成する。

4. Web StudioのカタログメニューでNitroTPMとUEFIセキュアブートが有効なマスターイメージを選択するか、PowerShellコマンドを使用してプロビジョニングスキームを作成する際に、マシンカタログを作成します。

作成されたカタログに追加されたVMには、NitoTPMとUEFIセキュアブートが有効になっています。

NitroTPMとUEFIセキュアブートをサポートするAMIを作成する

1. NitroTPMおよび/またはUEFIセキュアブートが有効なVMからAMIを作成できます。
   a. AWS Marketplaceイメージを使用してインスタンスを作成します。例：`TPM-Windows_Server-2022-English-Full-Base on the aws-marketplace`を検索します。
   b. シングルセッションまたはマルチセッションVDAをダウンロードします。
   c. そのVMからAMIを作成します。
2. register-imageコマンドを使用します。

```
--boot-mode (string)

--tpm-support (string)
```

詳細については、register-imageを参照してください。

以下のAWSドキュメントを参照してください。

- EC2インスタンスタイプのサポートされているブートモードを決定する
- Amazon EC2インスタンスでNitroTPMを使用するための要件/.

Delivery Controller™ホストからPowerShellウィンドウを開いて、特定の項目を確認できます。

- サービスオファリングがNitroTPMまたはUEFIセキュアブートをサポートしている

```
(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.BootMode

(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.NitroTpmSupportVersions
```

- テンプレートがNitroTPMまたはUEFIセキュアブートをサポートしているか

```
(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.BootMode



(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.TpmSupport
```

既存のカタログのサービスオファリングを更新する

既存のカタログのサービスオファリングは、`Set-ProvScheme` を使用して変更できます。この変更は、新しく追加されたVMに適用されます。ただし、次のシナリオではエラーが発生します。

AMIの起動モード	AMIはNITRO TPMをサポートしていますか？	サービスオファリングはNITROTPMとUEFIセキュアブートをサポートしていますか？
UEFI	いいえ	いいえ
レガシーBIOS	はい	いいえ
UEFI	はい	いいえ
UEFI優先	はい	いいえ

VM上のタグをコピーする

マシンプロファイルで指定されたNIC、およびディスク（IDディスク、ライトバックキャッシュディスク、OSディスク）上のタグを、新しく作成されたMCSマシンカタログ内のVMにコピーできます。これらのタグは、いずれかのマシンプロファイルソース（AWS VMインスタンスまたはAWS起動テンプレートバージョン）で指定できます。この機能は、永続および非永続マシンカタログとVMに適用されます。

注:

- AWS EC2コンソールでは、**起動テンプレートバージョンリソースタグ**の下に**ネットワークインターフェイスのタグ付け**の値は表示されません。ただし、PowerShellコマンド `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` を実行してタグの仕様を確認できます。

- マシンプロファイルソース（VMまたは起動テンプレートバージョン）に2つのネットワークインターフェイス（eni-1とeni-2）があり、eni-1にタグt1、eni-2にタグt2がある場合、VMは両方のネットワークインターフェイスのタグを取得します。

PowerShellを使用してVMインスタンスをフィルタリングする

マシンプロファイルVMとして使用するAWS VMインスタンスは、マシンカタログが正しく作成および機能するために互換性がある必要があります。マシンプロファイル入力VMとして使用できるAWS VMインスタンスを一覧表示するには、`Get-HypInventoryItem` コマンドを使用できます。このコマンドは、ホスティングユニットで利用可能なVMのインベントリをページングおよびフィルターできます。

ページネーション：

Get-HypInventoryItemは、2つのページネーションモードをサポートしています。

- ページングモードでは、`-MaxRecords` および `-Skip` パラメーターを使用してアイテムのセットを返します。
  - `-MaxRecords`：デフォルトは **1** です。これは、返すアイテムの数を制御します。
  - `-Skip`: デフォルトは**0**です。これは、ハイパーバイザー内のリストの絶対的な先頭（または絶対的な末尾）からスキップする項目の数を制御します。
- スクロールモードでは、レコードのスクロールを可能にするために、`-MaxRecords`、`-ForwardDirection`、および`-ContinuationToken`パラメーターを使用します。
  - `-ForwardDirection`: デフォルトは**True**です。これは`-MaxRecords`と組み合わせて使用され、一致するレコードの次のセット、または一致するレコードの前のセットのいずれかを返します。
  - `-ContinuationToken`: `ContinuationToken`で指定された項目を含まずに、直後の項目（または`ForwardDirection`が**false**の場合は直前の項目）を返します。

ページネーションの例:

- 最も名前の小さいマシンテンプレートの単一レコードを返します。`AdditionalData`フィールドには`TotalItemsCount`と`TotalFilteredItemsCount`があります:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template
```

- 最も名前の小さいマシンテンプレートの10レコードを返すには：

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 10 | select Name
```

- 最も名前の大きいレコードで終わるレコードの配列を返します:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ForwardDirection $False -MaxRecords 10 | select
Name
```

- 指定された`ContinuationToken`に関連付けられたマシンテンプレートから始まるレコードの配列を返します:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ContinuationToken "ami-07xxxxxxxxx"
-MaxRecords 10
```

フィルタリング:

フィルタリングには、以下の追加のオプションパラメータがサポートされています。これらのパラメータは、ページネーションオプションと組み合わせることができます。

- `-ContainsName "my_name"`: 指定された文字列がAMI名の一部と一致する場合、そのAMIは`Get`結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -ContainName ‘apollo’ | select
Name
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: AMIがこれらのタグの少なくとも1つを持っている場合、それは`Get`結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -Tags '{"opex owner": "Not
tagged"}' | select Name
```

> **注:**

> 2つのタグ値がサポートされています。**タグなし**タグ値は、タグのリストに指定されたタグがない項目と一致します。**すべての値**タグ値は、タグの値に関係なくタグを持つ項目と一致します。それ以外の場合、一致は、項目がタグを持ち、その値がフィルターで指定されたものと等しい場合にのみ発生します。

- `-Id "ami-0a2d913927e0352f3"`: AMIが指定されたIDと一致する場合、`Get`結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -Id ami-xxxxxxxxxxxx
```

AdditionalDataパラメータでのフィルタリング:

`AdditionalData`フィルターパラメーターは、テンプレートまたはVMを、その機能、サービス提供、またはAdditionalDataにある任意のプロパティに基づいて一覧表示します。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200).AdditionalData
```

互換性のないVMを示すために、`-Warn`パラメータを追加することもできます。VMには、**Warning**という名前の`AdditionalData`フィールドが含まれています。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-015xxxxxxxxx"
-Warn $true).AdditionalData
```

VMのバックアップSKUリスト

パブリッククラウドでは、特定のEC2インスタンスタイプ（「プライマリSKU」）の容量が不足することがあります。プライマリVM構成が利用できない場合、VMは起動できず、時間の損失やビジネスの中断につながります。このようなシナリオに対処するため、容量関連の問題が発生した場合にMCSがフォールバックできるバックアップEC2インスタンスタイプ（「バックアップSKU」）のリストを提供します。

MCSマシンカタログの作成または更新時に、カスタムプロパティ`BackupVmConfiguration`を使用して、バックアップEC2インスタンスタイプ（「バックアップSKUリスト」）のリストを提供します。

プライマリEC2インスタンスが失敗した場合、MCSは指定された順序でバックアップEC2インスタンスタイプへのフォールバックを試みます。MCSが提供されたバックアップEC2インスタンスタイプのいずれにもフォールバックできない場合、エラーメッセージが表示されます。その後、プライマリEC2インスタンスの電源を再度オンにしてみてください。これが失敗した場合、MCSはバックアップEC2インスタンスタイプを再試行します。

バックアップSKUリストには、オンデマンドインスタンスを含めることができます。

この機能は、永続および非永続MCSマシンカタログの両方に適用されます。

重要な考慮事項

- バックアップSKUリストには、複数のバックアップEC2インスタンスタイプを指定できます。
- バックアップSKUリストは一意である必要があります。
- バックアップEC2インスタンスは、プライマリEC2インスタンスと同じにすることはできません。
- バックアップEC2インスタンスは、有効なAWSインスタンスタイプである必要があります。
- 重複するサービスオファリングを指定しないでください。例: `BackupVmConfiguration,t2.small|t3.small|t2.small` は無効です。
- リストで指定されたサービスオファリングは、マシンカタログ構成と互換性がある必要があります。たとえば、カタログがUEFIを使用しており、バックアップリストで指定されたサービスオファリングがそれをサポートしていない場合、カタログの作成または更新は事前チェック中に失敗します。
- 既存のカタログのバックアップSKUリストは、`Set-ProvScheme` PowerShellコマンドを使用して変更できます。既存のVMは、`Set-ProvVM` および `Set-ProvVMUpdateTimeWindow` PowerShellコマンドを使用して変更できます。

バックアップEC2インスタンスの構成

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*` を実行します。
3. ブローカーカタログを作成します。
4. IDプールを作成します。
5. カスタムプロパティ `BackupVmConfiguration` を使用してバックアップEC2インスタンスリストを追加し、プロビジョニングスキームを作成します。例:

```
$serviceOffering = "XDHyp:\HostingUnits\$hostingUnitName\T3 Medium
Instance.serviceoffering"

$customProperties =
"AwsCaptureInstanceProperties,false;AwsOperationalResourcesTagging,fals
e;BackupVmConfiguration,t2.small|t2.large|t3.small|t3.large;"

$createdProvScheme = New-ProvScheme -ProvisioningSchemeName
$provisioningSchemeName -HostingUnitName $hostingUnitName
-IdentityPoolName $provisioningSchemeName -NetworkMapping
$networkMapping -SecurityGroup $securityGroupPath -ServiceOffering
$serviceOffering -MasterImageVM $masterImageVm -CustomProperties
$customProperties
```

6. プロビジョニングスキームの一意のIDでBrokerCatalogを更新します。
7. VMを作成し、カタログに追加します。

AWSスポットインスタンスを使用したカタログの作成

オンデマンドインスタンスと比較して、スポットインスタンスは最大90%のコスト削減を提供します。スポットインスタンスは、容量が利用できなくなった場合、Amazon EC2によって中断される可能性があるため、重要度の低いアプリケーションやデスクトップにのみ適しています。

スポットインスタンスの詳細については、AWSドキュメントの「スポットインスタンス」を参照してください。

さらに、スポットインスタンスをプライマリEC2インスタンスタイプとバックアップEC2インスタンスの両方として使用できます。PowerShellを使用して、容量関連の問題が発生した場合にMCSがフォールバックできるバックアップEC2インスタンスタイプ（オンデマンドインスタンスとスポットインスタンスの両方になり得る「バックアップSKU」）のリストを提供できます。

重要な考慮事項

- Spotインスタンスのカタログは、マシンプロファイルワークフローでのみ作成する必要があります。
- 永続的なSpotインスタンスリクエストタイプのみがサポートされています。1回限りのSpotインスタンスリクエストはサポートされていません。
- **停止**および**休止**の中断動作のみがサポートされています。

- 既存のカタログの構成をオンデマンドからSpotインスタンスへ、またはその逆に変更できます。ただし、EC2インスタンスをオンデマンドからSpotに変更するのは複雑です。AWSドキュメント「オンデマンドからSpot料金へのEC2インスタンスの切り替え」を参照してください。
- プロビジョニングされたSpotインスタンスを削除するときは、既存のSpotインスタンスリクエストをキャンセルしてください。そうしないと、AWSが新しいSpotインスタンスを作成します。

AWS Spotインスタンスを使用してカタログを作成する手順

1. Spotインスタンスでマシンプロファイルソースを作成します。Spotインスタンスを作成する手順については、「Spotインスタンスリクエストの作成」を参照してください。
2. `New-ProvScheme` PowerShellコマンドを使用して、マシンプロファイルでマシンカタログを作成します。`Set-ProvScheme`コマンドを使用してカタログを更新できます。

バックアップSKUとしてSpotインスタンスを使用する

SpotインスタンスをプライマリEC2インスタンスタイプとバックアップEC2インスタンスの両方として使用できます。容量関連の問題が発生した場合にMCSがフォールバックできるバックアップEC2インスタンスタイプ（オンデマンドおよびSpotインスタンスである「バックアップSKU」）のリストをPowerShellを使用して提供できます。

> **注:**
>
> バックアップSKUリストに重複するSpotインスタンスを指定できます。例: `BackupVmConfiguration,t2.small:Spot|t2.small|t3.small` は有効です。

必要な権限

Spotインスタンスをプライマリまたはバックアップ EC2インスタンスとして使用する場合、次の権限が必要です。

- `ec2:DescribeSpotInstanceRequests`
- `ec2:CancelSpotInstanceRequests`

バックアップスポットインスタンスを構成する

1. PowerShellウィンドウを開きます。
2. `asnp citrix*` を実行して、Citrix固有のPowerShellモジュールをロードします。
3. ブローカーカタログを作成します。

4. IDプールを作成します。
5. カスタムプロパティ `BackupVmConfiguration` を使用してバックアップEC2インスタンスリストを追加し、プロビジョニングスキームを作成します。例:

```
$serviceOffering \= "XDHyp:\\HostingUnits\\$hostingUnitName\\T3 Medium
Instance.serviceoffering"

$customProperties \=
"AwsCaptureInstanceProperties,false;AwsOperationalResourcesTagging,fals
e;BackupVmConfiguration,t2.small|t2.large|t3.small:Spot|t3.large:Spot"


$createdProvScheme \= New-ProvScheme \-ProvisioningSchemeName
$provisioningSchemeName \-HostingUnitName $hostingUnitName \-
IdentityPoolName $provisioningSchemeName \-NetworkMapping
$networkMapping \-SecurityGroup $securityGroupPath \-ServiceOffering
$serviceOffering \-MasterImageVM $masterImageVm \-CustomProperties
$customProperties
```

6. プロビジョニングスキームの一意のIDでBrokerCatalogを更新します。
7. カタログにVMを作成して追加します。

次のステップ

- これが最初に作成されたカタログである場合、デリバリーグループの作成に誘導されます。
- 構成プロセス全体を確認するには、インストールと構成を参照してください。
- カタログを管理するには、マシンカタログの管理およびAWS EC2カタログの管理を参照してください。

詳細情報

- 接続とリソースを作成および管理する(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/connections)
- AWS EC2への接続(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/connections/connection-aws)
- マシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create)

Azure Localカタログを作成する

マシンカタログを作成するウィザードについては、マシンカタログの作成で説明しています。以下の情報は、Azure Local環境に固有の詳細を扱っています。

> **注：**
>
> Azure Localマシンカタログを作成する前に、Azure Localへの接続作成を完了する必要があります。詳しくは、(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/connections/connection-azure-local.html)を参照してください。

要件

- VDAバージョン：2507以降
- Windows 10/11 マルチセッションワークロードはサポートされていません

マスターイメージを作成する

マシンカタログを作成するには、マスターイメージが必要です。

MCSはAzure Local VMイメージをマスターイメージとして使用します。Azure Localクラスターでワークロードをプロビジョニングするために MCSを使用する前に、VDAがインストールされたAzure Local VMイメージを準備する必要があります。

1. Azureポータルを使用してAzure Local VMを作成します。
2. 作成したAzure Local VMに接続し、VDAと必要なソフトウェアをインストールします。
3. Windowsタスクスケジューラを使用して、VM起動時にシステムコンテキストで次のスクリプトを実行するスケジュールタスクを作成します。マスターイメージでタスクをスケジュールするこのタスクは、VDAバージョン2511以前の場合にのみ必要です。

```
$tagFileName = 'E6DA6616-8EC4-48E0-BE93-58CE6ACE3CFB.tag'


$foundDrive = $null


foreach ($drive in Get-PSDrive -PSProvider FileSystem) {
```

```
$tagPath = Join-Path $drive.Root $tagFileName

if (Test-Path $tagPath) {

    $foundDrive = $drive.Root

    break

}

}



if ([string]::IsNullOrEmpty($foundDrive)) { exit 0 }

$installScript = Join-Path $foundDrive 'install.ps1'

if (Test-Path $installScript) {

powershell.exe -NoProfile -ExecutionPolicy Bypass -File $installScript
```

```
} else { exit 1 }


sc.exe stop mocguestagent 2>$null


sc.exe delete mocguestagent 2>$null


Remove-Item 'HKLM:
\SYSTEM\CurrentControlSet\Services\EventLog\Application\mocguestagent'
-Recurse -Force -ErrorAction SilentlyContinue


$setupComplete = 'C:\Windows\Setup\Scripts\SetupComplete.cmd'


if (Test-Path $setupComplete) { & $setupComplete }
```

4. Azure Local VMを停止します。
5. 準備されたAzure Local VMからAzure Local VMイメージを作成するには、既存のAzure Local VMからVMイメージを作成するを参照してください。

注:

Azure Connected Machine エージェントバージョン 1.61 以降がインストールされ、オンボードされた Azure Local VM を使用してマスターイメージを準備する場合、エージェント構成ファイルの削除時にアクセス拒否が発生するため、イメージ準備プロセスで MCS のカタログ作成が失敗します。回避策として、マスターイメージの作成中に次の手順を実行します。`C:\ProgramData\AzureConnectedMachineAgent\Config\agentconfig.json` に移動し、ファイルを右クリックして を選択し、 属性のチェックボックスをオフにします。

カタログを作成する

Azure Local カタログを作成して、Azure Local 環境でマシンを作成、配信、および電源管理できます。

> **注:**
>
> - カタログ名の長さは 49 文字以下にする必要があります。
> - カタログ名またはマシン命名スキームで Microsoft Azure の予約語を使用しないでください。詳細については、Microsoft ドキュメント を参照してください。

カタログは以下を使用して作成できます。

- ウェブスタジオ
- PowerShell

Web Studio を使用してカタログを作成する

Azure Local 環境で MCS マシンカタログを作成できます。

マシンカタログセットアップウィザードで：

1. ページで、 または を選択します。
2. ページで:
   a. 「**電源管理されているマシン（仮想マシンやブレードPCなど）**」を選択します。
   b. 「**Citrixプロビジョニングテクノロジー**」を使用してマシンを展開することを選択します。
   c. Citrix Machine Creation Services (MCS) の下にあるAzure Localホスティングユニットを選択します。
3. 「**デスクトップエクスペリエンス**」ページで、マシンタイプページで選択したマシンタイプに応じてオプションを選択します。
4. **イメージ**ページで：
   a. マスターイメージを選択します。現在、Azure Localは準備済みイメージをサポートしていません。
   b. 選択したイメージにメモを追加できます。

> **注:**
>
> - マスターイメージを選択すると、OSタイプが自動的に入力されます。
> - マシンプロファイルはサポートされていません。

5. 「**NIC**」ページで、1つ以上のNICを選択し、各カードに仮想ネットワークを関連付けます。
6. 「**仮想マシン**」ページで：
   a. 作成する仮想マシンの数を指定します。作成しない場合は0を入力します。後で、マシンを追加することで、空のカタログにVMを作成できます。
   b. 各VMが持つメモリ量（MB単位）と仮想CPU数を指定します。
   c. I/Oパフォーマンスを向上させるために、マシンのライトバックキャッシュを構成します。
7. 画面の指示に従って残りの手順を完了してください。これらの手順にはAzure Local固有の情報は含まれていません。

Web Studioを使用してAzure Localカタログを作成し、Azure Localクラスター内の既存のマシンのパワーを配信および管理することもできます。

マシンカタログセットアップウィザードで：

1. **オペレーティングシステム**ページで、**マルチセッションOS**または**シングルセッションOS**を選択します。
2. **マシン管理**ページで、**電源管理されているマシン**を選択し、マシンの展開方法として**その他のサービスまたはテクノロジー**を選択します。
3. **仮想マシン**ページで、マシンとそのActive Directoryマシンアカウントを追加します。次のことができます。
   - マシンを手動で追加する: をクリックして、マシンを手動で追加します。 ウィンドウが表示されます。以前に作成したAzure Local接続を展開し、追加するVMを選択します。次に、関連するマシンアカウント名を追加します。
   - CSVファイルを使用してマシンを追加する: をクリックします。CSVファイルを使用してマシンを追加する方法については、「Use CSV files to bulk add machines to a catalog」を参照してください。
4. 画面の指示に従って残りの手順を完了してください。これらの手順にはAzure Local固有の情報は含まれていません。

PowerShellを使用してカタログを作成する

PowerShellコマンドを使用して、Azure Local環境にMCSマシンカタログを作成できます。

スクリプトのヘッダー

スクリプトのヘッダーで定義されている正しいパラメーター値を指定していることを確認してください。

```
$catalogName = "" # Name of the catalog you want to create



$masterImageResourceGroupName = "" # Name of resource group that the
master Azure Local VM image resides in



$catalogResourceGroup = "" # Name of resource group that the created VMs
reside in



$masterImage = "" # Name of the master Azure Local VM image you want to
use



$vNet = "" # Name of the logical network that the created VMs should be
attached to



$masterImagePath = "XDHyp:\HostingUnits\$hostingUnitName\image.folder\
$masterImageResourceGroupName.resourcegroup\$masterImage"



$networkMapping = @{"0"="XDHyp:\HostingUnits\$hostingUnitName\
\network.folder\$vNet.network"}



$customPropertiesXml = "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
```

```
www.w3.org/2001/XMLSchema-instance`"><Property xsi:type=`"StringProperty`"
Name=`"ResourceGroups`" Value=`"$catalogResourceGroup`" /><Property
xsi:type=`"StringProperty`" Name=`"OsType`" Value=`"Windows`" /></
CustomProperties>"
```

1つのVMでMCSカタログを作成する

エーエスエヌピー シトリックス*

マシンカタログを作成する

```
New-BrokerCatalog -AllocationType "Random" -IsRemotePC $false
-MinimumFunctionalLevel "L7_34" -Name $catalogName -PersistUserChanges
"Discard" -ProvisioningType "MCS" -SessionSupport "SingleSession"
```

IDプールを作成する

```
New-AcctIdentityPool -AllowUnicode $true -Domain "test.local"
-IdentityPoolName $catalogName -IdentityType "ActiveDirectory"
-NamingScheme "demoVM#" -NamingSchemeType "Numeric" -OU
"CN=Computers,DC=test,DC=local"
```

プロビジョニングスキームを作成する

```
New-ProvScheme -CleanOnBoot $true -CustomProperties $customPropertiesXml
-HostingUnitName $hostingUnitName -IdentityPoolName $catalogName
-MasterImageVM $masterImagePath -NetworkMapping $networkMapping
-ProvisioningSchemeName $catalogName -ProvisioningSchemeType "MCS"
-VMCpuCount 4 -VMMemoryMB 8192
```

カタログをプロビジョニングスキームにリンクする

```
$schemeUid =(Get-ProvScheme -ProvisioningSchemeName
$catalogName).ProvisioningSchemeUid.Guid



Set-BrokerCatalog -Name $catalogName -ProvisioningSchemeId $schemeUid
```

ADアカウントを作成する

```
New-AcctADAccount -Count 1 -IdentityPoolName $catalogName
```

VMをプロビジョニングする

```
New-ProvVM -ADAccountName "domain\demoVM1" -ProvisioningSchemeName
$catalogName
```

ブローカーカタログへのマシンの追加

```
New-BrokerMachine -CatalogName $catalogName -MachineName 'domain\demoVM1'
```

次のステップ

- これが最初に作成するカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- Azure Local VMの電源管理については、Azure Local VMの電源管理を参照してください。

詳細情報

- 接続とリソースの作成および管理
- Azure Local への接続
- マシンカタログの作成

XenServer®カタログを作成する

(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create.html)では、マシンカタログを作成するウィザードについて説明します。以下の情報は、XenServer仮想化環境に固有の詳細を扱っています。

> **注:**
>
> XenServerカタログを作成する前に、XenServerへの接続の作成を完了する必要があります。「XenServerへの接続」(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/connections/connection-citrix-hypervisor.html)を参照してください。

XenServer接続を使用してマシンカタログを作成する

GPU対応マシンには、専用のマスターイメージが必要です。これらのVMには、GPUをサポートするビデオカードドライバーが必要です。GPU対応マシンを構成して、VMがGPUを操作に使用するソフトウェアで動作できるようにします。

1. XenCenter®で、標準VGA、ネットワーク、およびvCPUを備えたVMを作成します。
2. VM構成を更新して、GPUの使用（パススルーまたはvGPUのいずれか）を有効にします。

3. サポートされているオペレーティングシステムをインストールし、RDPを有効にします。
4. Citrix VM ToolsとNVIDIAドライバーをインストールします。
5. Virtual Network Computing (VNC) 管理コンソールをクリアしてパフォーマンスを最適化し、その後VMを再起動します。
6. RDPを使用するように求められます。RDPを使用してVDAをインストールし、その後VMを再起動します。
7. 必要に応じて、他のGPUマスターイメージのベースラインテンプレートとしてVMのスナップショットを作成します。
8. RDPを使用して、XenCenterで構成され、GPU機能を使用する顧客固有のアプリケーションをインストールします。

制限事項

- Citrix Hypervisor 8.2 Cumulative Update 1でホストされているVMを持つCitrix Virtual Apps and Desktops展開が、単一のMCSカタログで複数のGFS2 SRを使用している場合、カタログ内のVMは展開中にVDIにアクセスできません。「VDI is currently in use」というエラーが報告されます。
- Citrix Hypervisor 8.2 Cumulative Update 1は、GFS2 SRを使用したMCSフルクローンVMをサポートしていません。

詳しくは、「制約事項」を参照してください。

これらの制約は、XenServer 8 以降には適用されません。

マシンプロファイルを使用してマシンカタログを作成する

MCSを使用してマシンをプロビジョニングするためのカタログを作成する際、マシンプロファイルを使用して仮想マシンからハードウェアプロパティをキャプチャし、カタログ内の新しくプロビジョニングされたVMに適用できます。`MachineProfile`パラメーターが使用されていない場合、ハードウェアプロパティはマスターイメージVMまたはスナップショットからキャプチャされます。

> **注:**
>
> 現在、マシンプロファイルの入力として使用できるのは VM のみです。

> MCSIO が有効になっている場合、MCS カタログの作成後にメモリとディスクキャッシュのサイズを更新できます。マシンプロファイル入力のパラメーターの値を上書きするために、次のパラメーターを明示的に構成できます。

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

マシンプロファイルを使用してカタログを作成するには：

1. PowerShellウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. ID プールを作成します。ID プールは、作成する VM の Active Directory (AD) アカウントのコンテナです。例：

```
New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -IdentityPoolName
"ExampleIdentityPool" -NamingScheme "abc1-##" -NamingSchemeType
"Numeric" -Scope @() -ZoneUid "xxxxxxxx"
```

4. Active Directoryで必要なADコンピューターアカウントを作成します。

```
$password = "password123" | ConvertTo-SecureString -AsPlainText -Force

New-AcctIdentity -IdentityPoolName "ExampleIdentityPool" -Count 10
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
```

5. `New-ProvScheme`コマンドを実行してカタログを作成します。例:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
-IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />
```

```
</CustomProperties>'

-MasterImageVM "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleVDA.vm\ExampleVDA.snapshot"
-ProvisioningSchemeName "ExampleCatalog" -Scope @() -SecurityGroup @()

-MachineProfile "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfile.vm"
```

6. プロビジョニングスキームをブローカーカタログとして登録します。例：

```
$ConfigZone = Get-ConfigZone | Where-Object { $_.Name -eq "xxxxxx" }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -Description
"Machine profile catalog" -ProvisioningSchemeId fe7df345-244e-4xxxx-
xxxxxxxxx -ProvisioningType Mcs -SessionSupport MultiSession
-PersistUserChanges Discard -ZoneUid ($ConfigZone.Uid)
```

7. カタログにVMを追加します。

新しいマシンプロファイルでカタログを更新するには：

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -MachineProfile
"XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfileVm.vm\ExampleMach
ineProfileSnapshot.snapshot"
```

   Set-ProvScheme コマンドの詳細については、Set-ProvSchemeを参照してください。

注:

- この場合、`Set-ProvScheme` コマンドはカタログ内の既存の VM のマシンプロファイルを変更しません。カタログに追加された新しく作成された VM のみが新しいマシンプロファイルを持ちます。
- マシンプロファイルベースのマシンカタログを、非マシンプロファイルベースのマシンカタログに変換することはできません。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、インストールと構成を参照してください。
- カタログを管理するには、マシンカタログの管理およびXenServerカタログの管理を参照してください。

詳細情報

- 接続とリソースの作成および管理
- XenServerへの接続
- マシンカタログの作成

Google Cloud Platformカタログを作成する

マシンカタログの作成では、マシンカタログを作成するウィザードについて説明します。以下の情報では、Google Cloud環境に固有の詳細について説明します。

注:

Google Cloud Platform (GCP) カタログを作成する前に、GCPへの接続の作成を完了する必要があります。Google Cloud環境への接続を参照してください。

マスターVMインスタンスと永続ディスクを準備する

ヒント:

永続ディスクは、仮想ディスクを指すGoogle Cloudの用語です。

マスターVMインスタンスを準備するには、計画しているマシンカタログ内のクローンVDAインスタンスに必要な構成と一致するプロパティを持つVMインスタンスを作成および構成します。この構成は、インスタンスのサイズと種類にのみ適用されるわけではありません。メタデータ、タグ、GPU割り当て、ネットワークタグ、サービスアカウントのプロパティなどのインスタンス属性も含まれます。

マスタリングプロセスの一環として、MCSはマスターVMインスタンスを使用してGoogle Cloudの*インスタンステンプレート*を作成します。このインスタンステンプレートは、マシンカタログを構成するクローンVDAインスタンスの作成に使用されます。クローンインスタンスは、インスタンステンプレートが作成されたマスターVMインスタンスのプロパティ（VPC、サブネット、永続ディスクのプロパティを除く）を継承します。

マスターVMインスタンスのプロパティを要件に合わせて構成したら、インスタンスを起動し、そのインスタンスの永続ディスクを準備します。

ディスクのスナップショットまたはディスクのイメージを手動で作成することをお勧めします。これにより、意味のある命名規則を使用してバージョンを追跡し、マスターイメージの以前のバージョンを管理するためのより多くのオプションが得られ、マシンカタログ作成の時間を節約できます。独自のスナップショットを作成しない場合、MCSが一時的なスナップショットを作成します（これはプロビジョニングプロセスの終了時に削除されます）。OSディスクまたはイメージのマルチリージョンスナップショットを手動で作成すると、異なるGCPリージョンのマシンカタログに同じマスターイメージを使用することもできます。

マシンカタログを作成する

マシンカタログは次の2つの方法で作成できます。

- Web Studioを使用してマシンカタログを作成する
- PowerShellを使用してマシンカタログを作成する

Web Studio を使用してマシンカタログを作成する

> **注:**
>
> マシンカタログを作成する前に、リソースを作成してください。マシンカタログを構成する際は、Google Cloud が定めた命名規則を使用してください。詳細については、バケットとオブジェクトの命名ガイドラインを参照してください。

> (/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create.html)のガイダンスに従ってください。以下の説明は、Google Cloud カタログに固有のものです。

1. Web Studio にサインインし、左側のペインで を選択します。
2. アクションバーで を選択します。
3. ページで、 を選択し、 を選択します。

- Citrix Virtual Apps and Desktops™ は、シングルセッションOSもサポートしています。

4. ページで、 と オプションを選択し、 を選択します。複数のリソースがある場合は、メニューから1つ選択します。
5. ページで、必要に応じてこれらの手順を完了し、 をクリックします。

   a. マスターイメージを選択します。次のイメージタイプを選択できます。

      - 仮想マシン（リージョンが選択されたホスティングユニットと同じもの）。
      - スナップショット（マルチリージョンスナップショットをサポート）。
      - OSイメージ（マルチリージョンのパブリックイメージおよび非パブリックイメージをサポート）。 単一テナンシー機能を使用する場合は、ノードグループプロパティが正しく構成されているイメージを必ず選択してください。(#enable-zone-selection)を参照してください。

   b. マシンプロファイルからマシンプロパティを継承するには、 を選択し、 タブまたは タブからプロファイルを選択します。

      > **注記:**
      >
      > - 現在、このカタログ内のVMは、選択されたマシンプロファイルからストレージ、マシンタイプ、ディスク暗号化の設定を継承します。
      > - インスタンステンプレートをマシンプロファイルとして選択した場合、すべてのゾーンがデフォルトで選択されます。必要に応じてゾーンを選択できます。

   c. カタログの最小機能レベルを選択します。

6. **ストレージの種類**ページで、このマシンカタログのオペレーティングシステムを格納するために使用するストレージの種類を選択します。以下の各ストレージオプションには、それぞれ独自の価格とパフォーマンス特性があります。（IDディスクは常にゾーン標準永続ディスクを使用して作成されます。）

   - 標準永続ディスク
   - バランス永続ディスク
   - SSD永続ディスク

   Google Cloudストレージオプションの詳細については、`<https://cloud.google.com/compute/docs/disks/>`を参照してください。

7. **仮想マシン**ページで、作成するVMの数を指定し、VMの詳細な仕様を確認してから、**次へ**を選択します。マシンカタログに単一テナントノードグループを使用する場合は、予約済みの単一テナントノードが利用可能なゾーン**のみ**を選択してください。ゾーン選択を有効にするを参照してください。
8. **ディスク設定**ページで、次の設定を構成できます。

   - ライトバックキャッシュを有効にするかどうかを選択します。ライトバックキャッシュを有効にすると、次のことができます。

     - 一時データをキャッシュするために使用するディスクとRAMのサイズを構成します。詳細については、一時データのキャッシュを構成するを参照してください。
     - ライトバックキャッシュディスクのストレージタイプを選択します。ライトバックキャッシュディスクに使用できるストレージオプションは次のとおりです。

       - 標準永続ディスク
       - バランス永続ディスク
       - SSD永続ディスク

       Google Cloudのストレージオプションの詳細については、「ストレージオプション」を参照してください。

     - ライトバックキャッシュディスクの種類を選択します。

       - **非永続ライトバックキャッシュディスクを使用する**。選択した場合、ライトバックキャッシュディスクはプロビジョニングされたVMに永続しません。ディスクは電源サイクル中に削除され、ディスクにリダイレクトされたデータはすべて失われます。
       - **永続ライトバックキャッシュディスクを使用する**。選択した場合、ライトバックキャッシュディスクはプロビジョニングされたVMに永続します。このオプションを有効にすると、ストレージコストが増加します。

   - MCSストレージ最適化（MCS I/O）が有効になっている場合、次のいずれかを実行できます。

     - 電源サイクル中にVDAのシステムディスクを保持するかどうかを選択します。詳細については、「MCSストレージ最適化の更新を有効にする」を参照してください。
     - メモリとディスクキャッシュのサイズを更新します。

- ディスクの内容を保護するために独自のキーを使用するかどうかを選択します。この機能を使用するには、まず独自の顧客管理暗号化キー（CMEK）を作成する必要があります。詳細については、「顧客管理暗号化キー（CMEK）を使用する」を参照してください。

  > **注:**
  >
  > Studioインターフェイスでのみ利用可能です。
  >
  > キーを作成した後、リストからいずれかのキーを選択できます。カタログを作成した後は、キーを変更できません。Google Cloudは、既存の永続ディスクまたはイメージでのキーのローテーションをサポートしていません。したがって、カタログをプロビジョニングした後、カタログは特定のバージョンのキーに紐付けられます。そのキーが無効化または破棄された場合、そのキーで暗号化されたインスタンスとディスクは、キーが再度有効化または復元されるまで使用できなくなります。

9. ページで、Active Directory アカウントを選択し、 を選択します。

   - **新しいActive Directoryアカウントを作成する**を選択した場合、ドメインを選択し、Active Directoryで作成されるプロビジョニング済みVMコンピューターアカウントの命名スキームを表す文字のシーケンスを入力します。アカウントの命名スキームは1〜64文字で、空白スペース、非ASCII文字、または特殊文字を含めることはできません。
   - 「**既存のActive Directoryアカウントを使用**」を選択した場合、「**参照**」を選択して、選択したマシン用の既存のActive Directoryコンピューターアカウントに移動します。

10. **ドメイン資格情報**ページで、「**資格情報の入力**」を選択し、ユーザー名とパスワードを入力して、「**保存**」を選択してから「**次へ**」を選択します。

    - 入力する資格情報には、Active Directoryアカウント操作を実行する権限が必要です。

11. **概要**ページで、情報を確認し、カタログの名前を指定して、「**完了**」を選択します。

    > **注：**
    >
    > バージョン2402以降、GCPカタログ名は以下の規則に準拠する必要があります。
    >
    > - 小文字で始まること。

- 小文字 (a-z)、数字、ハイフンのみを含めること。
- 小文字または数字で終わること。 これらの規則に準拠していない既存のGCPカタログの名前を変更しようとすると、エラーメッセージが表示され、更新された規則に従って名前を変更するように案内されます。

マシンカタログの作成には時間がかかる場合があります。マシンがターゲットノードグループに作成されていることを確認するには、Google Cloudコンソールに移動します。

手動で作成されたGoogle Cloudマシンをインポートする

*Google Cloudへの接続を作成*し、*Google Cloudマシンを含むカタログを作成*できます。その後、Citrix Virtual Apps™ and Desktopsを介してGoogle Cloudマシンを手動で電源サイクルできます。この機能を使用すると、次のことが可能になります。

- 手動で作成されたGoogle CloudマルチセッションOSマシンをCitrix Virtual Apps and Desktopsマシンカタログにインポートします。
- 手動で作成されたGoogle CloudマルチセッションOSマシンをCitrix Virtual Apps and Desktopsカタログから削除します。
- 既存のCitrix Virtual Apps and Desktopsの電源管理機能を使用して、Google Cloud WindowsマルチセッションOSマシンを電源管理します。たとえば、それらのマシンの再起動スケジュールを設定します。

この機能は、既存のCitrix Virtual Apps and Desktopsのプロビジョニングワークフローの変更や、既存機能の削除を必要としません。手動で作成したGoogle Cloudマシンをインポートする代わりに、Web StudioでMCSを使用してマシンをプロビジョニングすることをお勧めします。

共有仮想プライベートクラウド

共有仮想プライベートクラウド（VPC）は、共有サブネットが利用可能になるホストプロジェクトと、そのリソースを使用する1つ以上のサービスプロジェクトで構成されます。共有VPCは、共有企業Googleクラウド資産の一元的な制御、使用、および管理を提供するため、大規模なインストールに適したオプションです。詳細については、Googleドキュメントサイトを参照してください。

この機能により、Machine Creation Services（MCS）は、共有VPCに展開されたマシンカタログのプロビジョニングと管理をサポートします。このサポートは、ローカルVPCで現在提供されているサポートと機能的に同等ですが、次の2つの点で異なります。

1. ホスト接続の作成に使用されるサービスアカウントに追加の権限を付与する必要があります。このプロセスにより、MCSは共有VPCリソースにアクセスして使用できるようになります。
2. イングレスとエグレス用にそれぞれ1つずつ、2つのファイアウォールルールを作成する必要があります。これらのファイアウォールルールは、イメージマスタリングプロセス中に使用されます。

必要な新しい権限

ホスト接続を作成する際には、特定の権限を持つGoogle Cloudサービスアカウントが必要です。これらの追加権限は、共有VPCベースのホスト接続の作成に使用されるすべてのサービスアカウントに付与する必要があります。

> **ヒント:**
>
> これらの追加権限は、Citrix Virtual Apps and Desktopsにとって新しいものではありません。これらはローカルVPCの実装を容易にするために使用されます。共有VPCでは、これらの追加権限により、他の共有VPCリソースへのアクセスが可能になります。

> 共有VPCをサポートするために、ホスト接続に関連付けられたサービスアカウントに最大4つの追加権限を付与する必要があります。

1. **compute.firewalls.list** - この権限は必須です。これにより、MCSは共有VPCに存在するファイアウォールルールの一覧を取得できます。
2. **compute.networks.list** - この権限は必須です。これにより、MCSはサービスアカウントが利用できる共有VPCネットワークを識別できます。
3. **compute.subnetworks.list** – この権限は、VPCの使用方法によってオプションです。これにより、MCSは可視の共有VPC内のサブネットを識別できます。この権限はローカルVPCを使用する場合にすでに必要ですが、共有VPCホストプロジェクトでも割り当てる必要があります。
4. **compute.subnetworks.use** - この権限は、VPC の使用方法によってオプションです。プロビジョニングされたマシンカタログでサブネットリソースを使用するために必要です。この権限は、ローカル VPC を使用する場合にはすでに必要ですが、共有 VPC ホストプロジェクトでも割り当てる必要があります。

これらの権限を使用する際には、マシンカタログの作成に使用される権限の種類に基づいて異なるアプローチがあることを考慮してください。

- プロジェクトレベルの権限:

  - ホストプロジェクト内のすべてのShared VPCへのアクセスを許可します。
  - 権限 #3 と #4 をサービスアカウントに割り当てる必要があります。

- サブネットレベルの権限:
  - Shared VPC内の特定のサブネットへのアクセスを許可します。
  - 権限 #3 と #4 はサブネットレベルの割り当てに固有のものであるため、サービスアカウントに直接割り当てる必要はありません。

組織のニーズとセキュリティ基準に合ったアプローチを選択してください。

> **ヒント:**
>
> プロジェクトレベルとサブネットレベルの権限の違いの詳細については、Google Cloud のドキュメントを参照してください。

ファイアウォールルール

マシンカタログの準備中に、カタログのマスターイメージシステムディスクとして機能するマシンイメージが準備されます。このプロセスが発生すると、ディスクは一時的に仮想マシンに接続されます。このVMは、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを防止する分離された環境で実行する必要があります。これは、イングレス用とエグレス用の2つのすべて拒否ファイアウォールルールによって実現されます。Google CloudローカルVPCを使用する場合、MCSはこのファイアウォールをローカルネットワークに作成し、マスタリング用のマシンに適用します。マスタリングが完了すると、ファイアウォールルールはイメージから削除されます。

共有VPCを使用するために必要な新しい権限の数を最小限に抑えることをお勧めします。共有VPCはより上位の企業リソースであり、通常、より厳格なセキュリティプロトコルが導入されています。このため、ホストプロジェクトの共有VPCリソースに、イングレス用とエグレス用の2つのファイアウォールルールを作成してください。それらに最高の優先順位を割り当てます。次の値を使用して、これらの各ルールに新しいターゲットタグを適用します。

`citrix-provisioning-quarantine-firewall`

MCS がマシンカタログを作成または更新する際、このターゲットタグを含むファイアウォールルールを検索します。次に、ルールの正確性を確認し、カタログのマスターイメージの準備に使用されるマシンに適用します。ファイアウォールルールが見つからない場合、またはルールが見つかってもルールやその優先順位が正しくない場合は、次のようなメッセージが表示されます。

`"Unable to find valid INGRESS and EGRESS quarantine firewall rules for VPC <name> in project <project>. " Please ensure you have created 'deny all' firewall rules with the network tag 'citrix-provisioning-quarantine-firewall' and proper priority." "Refer to Citrix Documentation for details."`

共有 VPC の構成

Web Studio で共有 VPC をホスト接続として追加する前に、プロビジョニングする予定のプロジェクトからサービスアカウントを追加するために、次の手順を完了してください。

1. IAM ロールを作成します。
2. CVAD ホスト接続の作成に使用するサービスアカウントを、共有 VPC ホストプロジェクトの IAM ロールに追加します。
3. プロビジョニングする予定のプロジェクトから Cloud Build サービスアカウントを、共有 VPC ホストプロジェクトの IAM ロールに追加します。
4. ファイアウォールルールを作成します。

IAM ロールを作成する

ロールのアクセスレベルを決定します — *プロジェクトレベルアクセス*、または *サブネットレベルアクセス* を使用したより制限されたモデルのいずれかです。

IAM ロールのプロジェクトレベルアクセス。プロジェクトレベルの IAM ロールには、次の権限を含めます。

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

プロジェクトレベルのIAMロールを作成するには：

1. Google Cloudコンソールで、**IAM と管理 > ロール**に移動します。
2. **ロール**ページで、**ロールを作成**を選択します。
3. **ロールを作成**ページで、ロール名を指定します。**権限を追加**を選択します。
    a. **権限を追加**ページで、ロールに権限を個別に追加します。権限を追加するには、**テーブルをフィルタ**フィールドに権限の名前を入力します。権限を選択し、**追加**を選択します。
    b. **作成**を選択します。

サブネットレベルのIAMロール。このロールは、**ロールを作成**を選択した後、権限`compute.subnetworks.list`と`compute.subnetworks.use`の追加を省略します。このIAMアクセスレベルの場合、権限`compute.firewalls.list`と`compute.networks.list`を新しいロールに適用する必要があります。

サブネットレベルのIAMロールを作成するには：

1. Google Cloudコンソールで、**VPC ネットワーク** > **共有 VPC**に移動します。**共有 VPC**ページが表示され、ホストプロジェクトに含まれる共有VPCネットワークのサブネットが表示されます。
2. **共有 VPC**ページで、アクセスしたいサブネットを選択します。
3. 右上隅で、サービスアカウントを追加するために**メンバーを追加**を選択します。
4. **メンバーを追加**ページで、次の手順を完了します。
    a. **新しいメンバー**フィールドにサービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。
    b. **ロールを選択**フィールドを選択し、**Compute Network User**を選択します。
    c. **保存**を選択します。
5. Google Cloud コンソールで、**IAM と管理** > **ロール** に移動します。
6. **ロール** ページで、**ロールを作成** を選択します。
7. **ロールを作成** ページで、ロール名を指定します。**権限を追加** を選択します。
    a. **権限を追加** ページで、ロールに個別に権限を追加します。権限を追加するには、**テーブルをフィルタリング** フィールドに権限の名前を入力します。権限を選択し、**追加** を選択します。
    b. **作成** を選択します。

ホストプロジェクトのIAMロールにサービスアカウントを追加する

IAMロールを作成したら、ホストプロジェクトのサービスアカウントを追加するために次の手順を実行します。

1. Google Cloud コンソールで、ホストプロジェクトに移動し、次に **IAM と管理 > IAM** に移動します。
2. **IAM** ページで、サービスアカウントを追加するために **追加** を選択します。
3. **メンバーを追加** ページで:

a. **新しいメンバー** フィールドに、サービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。

b. ロールフィールドを選択し、作成したIAMロールを入力し、メニューからそのロールを選択します。

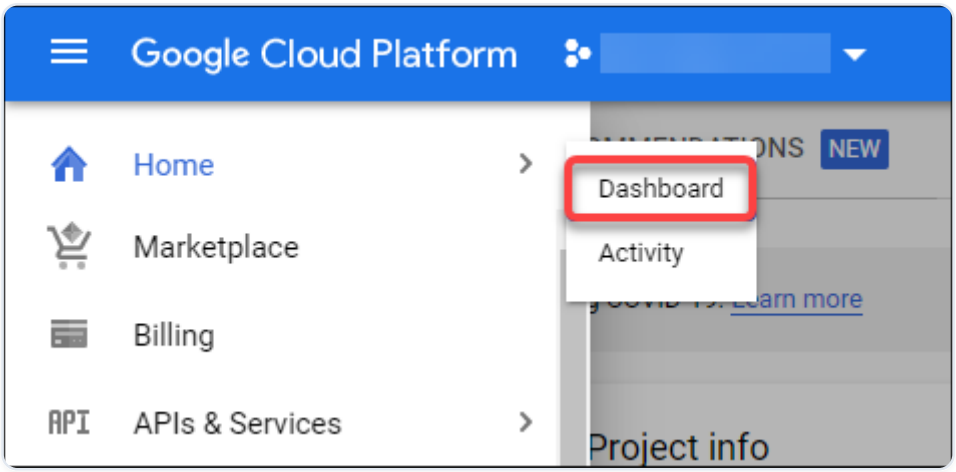
c. **保存** を選択します。

これで、サービスアカウントがホストプロジェクト用に構成されました。

クラウドビルドサービスアカウントを共有VPCに追加する

すべてのGoogle Cloudサブスクリプションには、プロジェクトID番号の後に `cloudbuild.gserviceaccount` が続くサービスアカウントがあります。例: `705794712345@cloudbuild.gserviceaccount`。

Google Cloudコンソールで**ホーム**と**ダッシュボード**を選択すると、プロジェクトのプロジェクトID番号を確認できます。



画面の **Project Info** エリアの下にある **Project Number** を見つけます。

Cloud Buildサービスアカウントを共有VPCに追加するには、次の手順を実行します。

1. Google Cloudコンソールで、ホストプロジェクトに移動し、**IAMと管理** > **IAM**に移動します。
2. 「**権限**」ページで、「**追加**」を選択してアカウントを追加します。
3. 「**メンバーを追加**」ページで、次の手順を実行します。

   a. 「**新しいメンバー**」フィールドにCloud Buildサービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。

   b. 「**ロールを選択**」フィールドを選択し、`Computer Network User` と入力して、メニューからロールを選択します。

   c. 「**保存**」を選択します。

ファイアウォールルールを作成する

マスタリングプロセスの一環として、MCSは選択されたマシンイメージをコピーし、それを使用してカタログのマスターイメージシステムディスクを準備します。マスタリング中、MCSはディスクを一時的な仮想マシンに接続し、その仮想マシンが準備スクリプトを実行します。このVMは、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを禁止する分離された環境で実行する必要があります。分離された環境を作成するために、MCSは2つの *すべて拒否* ファイアウォールルール（イングレスルールとエグレスルール）を必要とします。したがって、*ホストプロジェクト*に次の2つのファイアウォールルールを作成します。

1. Google Cloudコンソールで、ホストプロジェクトに移動し、**VPCネットワーク > ファイアウォール**に移動します。
2. **ファイアウォール**ページで、**ファイアウォールルールを作成**を選択します。
3. 「**ファイアウォールルールを作成**」ページで、以下を完了します。
   - **名前**。ルールの名前を入力します。
   - **ネットワーク**。イングレスファイアウォールルールが適用される共有 VPC ネットワークを選択します。
   - **優先度**。値が小さいほど、ルールの優先度が高くなります。小さい値（例: 10）をお勧めします。
   - **トラフィックの方向**。「**イングレス**」を選択します。
   - **一致時のアクション**。「**拒否**」を選択します。
   - **ターゲット**。デフォルトの「**指定されたターゲットタグ**」を使用します。
   - **ターゲットタグ**。`citrix-provisioning-quarantine-firewall`と入力します。
   - **ソースフィルター**。デフォルトの「**IP範囲**」を使用します。
   - **ソースIP範囲**。すべてのトラフィックに一致する範囲を入力します。`0.0.0.0/0`と入力します。
   - **プロトコルとポート**。「**すべて拒否**」を選択します。
4. 「**作成**」を選択してルールを作成します。
5. 手順1～4を繰り返して別のルールを作成します。「**トラフィックの方向**」には「**エグレス**」を選択します。

接続の追加

Google Cloud環境への接続を追加します。「接続を追加する」を参照してください。

ゾーン選択を有効にする

Citrix Virtual Apps and Desktops はゾーン選択をサポートしています。ゾーン選択を使用すると、VM を作成するゾーンを指定できます。ゾーン選択を使用すると、管理者は選択したゾーンに単一テナントノードを配置できます。単一テナンシーを構成するには、Google Cloud で以下を完了する必要があります。

- Google Cloud の単一テナントノードを予約する
- VDA マスターイメージを作成する

Google Cloud の単一テナントノードを予約する

単一テナントノードを予約するには、Google Cloud のドキュメントを参照してください。

> **重要:**
>
> ノードテンプレートは、ノードグループに予約されているシステムのパフォーマンス特性を示すために使用されます。これらの特性には、vGPU の数、ノードに割り当てられるメモリ量、およびノード上に作成されるマシンに使用されるマシンタイプが含まれます。詳細については、Google Cloud のドキュメントを参照してください。

VDA マスターイメージの作成

単一テナントノードにマシンを正常に展開するには、マスター VM イメージを作成する際に追加の手順を実行する必要があります。Google Cloud のマシンインスタンスには、*ノードアフィニティラベル*と呼ばれるプロパティがあります。単一テナントノードに展開されるカタログのマスターイメージとして使用されるインスタンスには、**ターゲットノードグループ**の名前と一致する*ノードアフィニティラベル*が必要です。これを実現するには、次の点に留意してください。

- 新しいインスタンスの場合、インスタンス作成時に Google Cloud コンソールでラベルを設定します。詳細については、単一テナント VM のプロビジョニングを参照してください。
- 既存のインスタンスの場合、**gcloud** コマンドラインを使用してラベルを設定します。詳細については、ノードアフィニティラベルの構成を参照してください。

> **注:**
>
> 共有 VPC で単一テナンシーを使用する場合は、共有仮想プライベートクラウドを参照してください。

マシンカタログを作成する

ノードアフィニティラベルを設定したら、マシンカタログを構成します。

顧客管理の暗号化キー (CMEK)

MCSカタログには、顧客管理の暗号化キー (CMEK) を使用できます。この機能を使用する場合、Google Cloud Key Management Service `CryptoKey Encrypter/Decrypter` ロールをCompute Engine Service Agentに割り当てます。Citrix Virtual Apps and Desktopsアカウントは、キーが保存されているプロジェクトで適切な権限を持っている必要があります。詳細については、Cloud KMSキーを使用してリソースを保護するを参照してください。

Compute Engine サービスエージェントは次の形式です: `service-<Project_Number>@compute-system.iam.gserviceaccount.com`。この形式は、デフォルトの Compute Engine サービスアカウントとは異なります。

> **注:**
>
> このCompute Engine Service Accountは、Google Consoleの**IAM権限**表示に表示されない場合があります。そのような場合は、Cloud KMSキーを使用してリソースを保護するで説明されているように、`gcloud` コマンドを使用してください。

Citrix Virtual Apps and Desktops アカウントに権限を割り当てる

Google Cloud KMSの権限は、さまざまな方法で構成できます。*プロジェクトレベル*のKMS権限、または*リソースレベル*のKMS権限のいずれかを提供できます。詳細については、権限とロールを参照してください。

プロジェクトレベルの権限

1つのオプションは、Citrix Virtual Apps and Desktops アカウントに Cloud KMS リソースを参照するためのプロジェクトレベルの権限を付与することです。これを行うには、カスタムロールを作成し、次の権限を追加します。

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

このカスタムロールをCitrix Virtual Apps and Desktopsに割り当てます。これにより、インベントリ内の関連プロジェクトでリージョンキーを参照できるようになります。

リソースレベルの権限

もう1つのオプションであるリソースレベルの権限については、Google Cloud コンソールで、MCS プロビジョニングに使用する `cryptoKey` に移動します。Citrix Virtual Apps and Desktops アカウントを、カタログプロビジョニングに使用するキーリングまたはキーに追加します。

> **ヒント:**
>
> このオプションでは、Citrix Virtual Apps and Desktops アカウントに Cloud KMS リソースに対するプロジェクトレベルのリスト権限がないため、インベントリでプロジェクトのリージョンキーを参照できません。ただし、以下で説明するように、`ProvScheme` カスタムプロパティで正しい `cryptoKeyId` を指定することで、CMEK を使用してカタログをプロビジョニングできます。

カスタムプロパティを使用した CMEK でのプロビジョニング

PowerShell を使用してプロビジョニングスキームを作成する ときに、`ProvScheme` `CustomProperties` で `CryptoKeyId` プロパティを指定します。例：

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId"
Value="<yourCryptoKeyId>" />

</CustomProperties>'
```

`cryptoKeyId` は次の形式で指定する必要があります。

`projectId:location:keyRingName:cryptoKeyName`

たとえば、ID が `my-example-project-1` のプロジェクトで、リージョン `us-east1` のキーリング `my-example-key-ring` にあるキー `my-example-key` を使用する場合、`ProvScheme` カスタム設定は次のようになります。

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
example-project-1:us-east1:my-example-key-ring:my-example-key" />
```

```
</CustomProperties>'
```

このプロビジョニングスキームに関連するすべての MCS プロビジョニング済みディスクとイメージは、この顧客管理暗号化キーを使用します。

ヒント:

グローバルキーを使用する場合、カスタムプロパティの場所は、上記の例の **us-east1** のような**リージョン**名ではなく、`global` と記述する必要があります。例: `<Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-example-project-1:global:my-example-key-ring:my-example-key" />`。

顧客管理キーのローテーション

Google Cloud は、既存の永続ディスクまたはイメージでのキーのローテーションをサポートしていません。マシンがプロビジョニングされると、作成時に使用されていたキーバージョンに紐付けられます。ただし、新しいバージョンのキーを作成でき、その新しいキーは、新しいマスターイメージでカタログが更新されたときに作成される、新しくプロビジョニングされたマシンまたはリソースに使用されます。

キーリングに関する重要な考慮事項

キーリングの名前を変更したり、削除したりすることはできません。また、これらを構成する際に予期せぬ料金が発生する可能性があります。キーリングを削除または除去すると、Google Cloudはエラーメッセージを表示します。

```
Sorry, you can't delete or rename keys or key rings. We were concerned
about the security implications of allowing multiple keys or key versions
over time to have the same resource name, so we decided to make names
immutable. (And you can't delete them, because we wouldn't be able to do a
true deletion--there would still have to be a tombstone tracking that this
name had been used and couldn't be reused).

We're aware that this can make things untidy, but we have no immediate
plans to change this.

If you want to avoid getting billed for a key or otherwise make it
unavailable, you can do so by deleting all the key versions; neither keys
```

```
nor key rings are billed for, just the active key versions within the
keys.
```

ヒント:

詳細については、「コンソールからのキーリングの編集または削除」を参照してください。

均一なバケットレベルのアクセス互換性

Citrix Virtual Apps and Desktopsは、Google Cloudの均一なバケットレベルのアクセス制御ポリシーと互換性があります。この機能は、ストレージバケットを含むリソースの操作を許可するために、サービスアカウントに権限を付与するIAMポリシーの使用を強化します。均一なバケットレベルのアクセス制御により、Citrix Virtual Apps and Desktopsは、アクセス制御リスト（ACL）を使用して、ストレージバケットまたはそこに保存されているオブジェクトへのアクセスを制御できます。Google Cloudの均一なバケットレベルのアクセスに関する概要情報については、均一なバケットレベルのアクセスを参照してください。構成情報については、均一なバケットレベルのアクセスを要求するを参照してください。

PowerShellを使用したマシンカタログの作成

このセクションでは、PowerShell を使用してカタログを作成する方法について詳しく説明します。

- 永続的なライトバックキャッシュディスクを持つカタログを作成する
- MCSIO で起動パフォーマンスを向上させる
- マシンプロファイルを使用してマシンカタログを作成する
- インスタンステンプレートとしてマシンプロファイルを持つマシンカタログを作成する
- PowerShellを使用してシールドされたVMを持つカタログを作成する
- 単一テナントノードにWindows 11 VMを作成する

永続的なライトバックキャッシュディスクを持つカタログを作成する

永続的なライトバックキャッシュディスクを持つカタログを構成するには、PowerShell パラメーター `New-ProvScheme` `CustomProperties` を使用します。

ヒント:

PowerShellパラメーターは、クラウドベースのホスティング接続でのみ使用してください。オンプレミスソリューション（XenServer®など）で永続的なライトバックキャッシュディスクを使用してマシンをプロビジョニングする場合、ディスクは自動的に永続化されるため、PowerShellは不要です。

このパラメーターは、MCSでプロビジョニングされたマシンに対してライトバックキャッシュディスクがどのように永続化されるかを決定するために使用される追加のプロパティ `PersistWBC` をサポートします。`PersistWBC` プロパティは、`UseWriteBackCache` パラメーターが指定され、`WriteBackCacheDiskSize` パラメーターがディスクが作成されることを示すように設定されている場合にのみ使用されます。

注:

この動作は、AzureとGCPの両方に適用されます。これらの環境では、デフォルトのMCSIOライトバックキャッシュディスクは電源サイクル時に削除され、再作成されます。ディスクを永続化することを選択することで、MCSIOライトバックキャッシュディスクの削除と再作成を回避できます。

`PersistWBC` プロパティを `true` に設定すると、Citrix Virtual Apps and Desktops 管理者が管理インターフェイスからマシンをシャットダウンしても、ライトバックキャッシュディスクは削除されません。

`PersistWBC` プロパティを `false` に設定すると、Citrix Virtual Apps and Desktops 管理者が管理インターフェイスからマシンをシャットダウンしたときに、ライトバックキャッシュディスクが削除されます。

注:

`PersistWBC` プロパティが省略されている場合、このプロパティはデフォルトで `false` に設定され、マシンが管理インターフェイスからシャットダウンされるとライトバックキャッシュは削除されます。

例えば、CustomPropertiesパラメーターを使用して `PersistWBC` を `true` に設定するには、次のようになります。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

注:

`PersistWBC` プロパティは、`New-ProvScheme` PowerShellコマンドレットを使用してのみ設定できます。作成後にプロビジョニングスキームの `CustomProperties` を変更しようとしても、マシンカタログや、マシンがシャットダウンされたときのライトバックキャッシュディスクの永続性には影響しません。

例えば、`New-ProvScheme` を設定してライトバックキャッシュを使用し、同時に `PersistWBC` プロパティを `true` に設定するには、次のようになります。

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"
```

```
-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

MCSIOで起動パフォーマンスを向上させる

MCSIOが有効になっている場合、AzureおよびGCPマネージドディスクの起動パフォーマンスを向上させることができます。この機能を構成するには、`New-ProvScheme` コマンドでPowerShell `PersistOSDisk` カスタムプロパティを使用します。`New-ProvScheme` に関連するオプションは次のとおりです。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->

````````Groups" Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />
```
```

```
</CustomProperties>
```

この機能を有効にするには、`PersistOSDisk`カスタムプロパティを`true`に設定します。例:

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

マシンプロファイルを使用してマシンカタログを作成する

Machine Creation Services (MCS) を使用してマシンをプロビジョニングするカタログを作成する場合、マシンプロファイルを使用して仮想マシンからハードウェアプロパティをキャプチャし、それらをカタログ内の新しくプロビジョニングされたVMに適用できます。`MachineProfile`パラメーターが使用されない場合、ハードウェアプロパティはマスターイメージVMまたはスナップショットからキャプチャされます。 明示的に定義する一部のプロパティ（例: `StorageType`、`CatalogZones`、`CryptoKeyIs`）は、マシンプロファイルから無視されます。

- マシンプロファイルを使用してカタログを作成するには、`New-ProvScheme`コマンドを使用します。例: `New-ProvScheme –MachineProfile "path to VM"`。`MachineProfile`パラメーターを指定しない場合、ハードウェアプロパティはマスターイメージVMからキャプチャされます。
- 新しいマシンプロファイルでカタログを更新するには、`Set-ProvScheme`コマンドを使用します。例: `Set-ProvScheme –MachineProfile "path to new VM"`。このコマンドは、カタログ内の既存のVMのマシンプロファイルを変更しません。カタログに追加された新しく作成されたVMのみが新しいマシンプロファイルを持ちます。
- マスターイメージを更新することもできますが、マスターイメージを更新してもハードウェアプロパティは更新されません。ハードウェアプロパティを更新したい場合は、`Set-ProvScheme`コマンドを使用してマシンプロファイルを更新する必要があります。これらの変更は、カタログ内の新しいマシンにのみ適用されます。既存のマシンのハードウェアプロパティを更新するには、`-StartsNow`および`-DurationInMinutes -1`パラメーターを指定して`Set-ProvVMUpdateTimeWindow`コマンドを使用できます。

> **注:**
>
> - `StartsNow`は、スケジュールされた開始時刻が現在の時刻であることを示します。
> - 負の数（例: –1）を持つ`DurationInMinutes`は、スケジュールの時間枠に上限がないことを示します。

マシンプロファイルをインスタンステンプレートとして使用してマシンカタログを作成する

マシンプロファイルの入力としてGCPインスタンステンプレートを選択できます。インスタンステンプレートはGCPの軽量リソースであるため、非常に費用対効果が高いです。

マシンプロファイルをインスタンステンプレートとして使用して新しいマシンカタログを作成する

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. 次のコマンドを使用して、GCPプロジェクト内のインスタンステンプレートを見つけます。

```
cd XDHyp:\HostingUnits\<HostingUnitName>\instanceTemplates.folder
```

4. NewProvSchemeコマンドを使用して、インスタンステンプレートとしてマシンプロファイルを持つ新しいマシンカタログを作成します。

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -HostingUnitName
<HostingUnitName> -IdentityPoolName <identity pool name> -MasterImageVM

XDHyp:\HostingUnits\<HostingUnitName> \Base.vm\Base.snapshot
-MachineProfile XDHyp:
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\mytemplate.tem
plate
```

   New-ProvSchemeコマンドの詳細については、https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/を参照してください。

5. PowerShell コマンドを使用してマシンカタログの作成を完了します。Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/ を参照してください。

既存のマシンカタログのマシンプロファイルをインスタンステンプレートに変更する

既存のマシンカタログのマシンプロファイルをインスタンステンプレートに変更する詳細な手順は次のとおりです。

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. 次のコマンドを実行します。

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -MachineProfile
XDHyp:
```

```
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\<TemplateName>
.template
```

Set-ProvSchemeコマンドの詳細については、https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/を参照してください。

PowerShell を使用して、シールドされたVMでカタログを作成する

シールドされたVMプロパティを持つMCSマシンカタログを作成できます。シールドされた仮想マシンは、セキュアブート、仮想トラステッドプラットフォームモジュール、UEFIファームウェア、整合性監視などの高度なプラットフォームセキュリティ機能を使用して、Compute Engineインスタンスの検証可能な整合性を提供する一連のセキュリティ制御によって強化されています。

MCSは、マシンプロファイルワークフローを使用してカタログを作成することをサポートしています。マシンプロファイルワークフローを使用する場合、VMインスタンスのシールドされたVMプロパティを有効にする必要があります。その後、このVMインスタンスをマシンプロファイルの入力として使用できます。

マシンプロファイルワークフローを使用して、シールドされたVMでMCSマシンカタログを作成するには。

1. Google Cloud コンソールでVMインスタンスのシールドされたVMオプションを有効にします。クイックスタート: シールドされたVMオプションを有効にするを参照してください。
2. VMインスタンスを使用して、マシンプロファイルワークフローでMCSマシンカタログを作成します。
    a. PowerShellウィンドウを開きます。
    b. `asnp citrix*`を実行して、Citrix固有のPowerShellモジュールをロードします。
    c. まだ作成されていない場合は、IDプールを作成します。
    d. `New-ProvScheme`コマンドを実行します。例：

```
New-ProvScheme -ProvisioningSchemeName <catalog-name>

-HostingUnitName gcp-hostint-unit

-MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-vda.vm

-MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
machine.vm
```

3. マシンカタログの作成を完了します。

新しいマシンプロファイルでマシンカタログを更新するには:

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme -ProvisioningSchemeName <catalog-name>

-MasterImageVM XDHyp:\HostingUnits\<hostin-unit>\catalog-vda.vm

-MachineProfile "DHyp:\HostingUnits\<hostin-unit>\catalog-machine.vm
```

`Set-ProvScheme` で行った変更を既存のVMに適用するには、`Set-ProvVMUpdateTimeWindow` コマンドを実行します。

1. `Set-ProvVMUpdateTimeWindow` コマンドを実行します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

2. VMを再起動します。

シングルテナントノードでWindows 11 VMを作成する

GCPでWindows 11 VMを作成できます。ただし、マスターイメージにWindows 11をインストールする場合は、マスターイメージ作成プロセス中にvTPMを有効にする必要があります。また、マシンプロファイルソース（VMまたはインスタンステンプレート）でvTPMを有効にする必要があります。

シングルテナントノードでWindows 11 VMを作成するための主要な手順は次のとおりです。

1. Google Cloud仮想化環境をセットアップします。詳細については、「Google Cloud environments」を参照してください。
2. VDAをインストールします。「Install VDAs」を参照してください。
3. Google Cloud環境への接続を作成します。詳細については、Google Cloud環境への接続を参照してください。
4. Windows 11 Bring Your Own License (BYOL) マスターイメージを作成し、そのイメージをGoogle Cloudにインポートします。Windows 11 BYOLマスターイメージの作成を参照してください。

5. マシンプロファイルソースを作成します。単一テナントノードにVMをプロビジョニングし、ソースマシンプロファイルのvTPMを有効にします。単一テナントノードでのVMのプロビジョニングを参照してください。
6. vTPMが有効なWindows 11マシンプロファイルソースを使用してMCSマシンカタログを作成します。マシンプロファイルソースは、単一テナントノードで説明されているものと同じインスタンスタイプである必要があります。Windows 11マシンプロファイルソースを使用したMCSマシンカタログの作成を参照してください。

Windows 11 BYOLマスターイメージを作成する

Windows 11 BYOLマスターイメージを作成し、そのマスターイメージをGoogle Cloudにインポートするには、2つのオプションがあります。

- Google Cloud Cloud Build Tools を使用する
- 他のハイパーバイザーでマスターイメージを作成する

GOOGLE CLOUD CLOUD BUILD TOOLS を使用する

1. Windows 11 ISO、GCP SDK、.NET framework、およびPowerShellインストーラーファイルをGCPストレージバケットにアップロードします。
2. クラウドビルド`.yaml`ファイルでファイルパスをパラメーターとして指定します。
3. コマンドラインから以下のCloud Buildを実行して、最終的なWindows 11イメージをビルドします。GCPは、GCPのDaisyワークフローを使用して、選択したプロジェクトでマスターイメージをブートストラップして作成し、そのマスターイメージはGCPにインポートされます。

```
gcloud compute instances import INSTANCE-NAME--source-uri=gs://BUCKET/
IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
machine-type=MACHINE-TYPE --zone=ZONE
```

> **注:**
>
> すべての大文字のテキストを実際のリソース詳細に置き換えてください。

詳細については、カスタムWindows BYOLイメージの作成を参照してください。

他のハイパーバイザーでマスターイメージを作成する

1. 他のハイパーバイザーを使用して Windows 11 マスターイメージを作成します。
2. マスターイメージを OVF 形式でローカルマシンにエクスポートします。

3. ローカルの gcloud CLI を使用して、OVF ファイルを GCP ストレージバケットにアップロードします。

```
gsutil cp LOCAL_IMAGE_PATH_OVF_FILES gs://BUCKET_NAME/
```

4. コマンドラインから以下のCloud Buildを実行して、最終的なWindows 11イメージをビルドします。GCPは、GCPのDaisyワークフローを使用して、選択したプロジェクトでマスターイメージをブートストラップして作成し、マスターイメージはGCPにインポートされます。

```
gcloud compute instances import INSTANCE-NAME --source-uri=gs://BUCKET/
IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
machine-type=MACHINE-TYPE --zone=ZONE
```

> **注:**
>
> すべての大文字のテキストを実際のリソースの詳細に置き換えてください。

単一テナントノードでのVMのプロビジョニング

単一テナントノードを使用して、VMを他のプロジェクトのVMから物理的に分離したり、同じホストハードウェア上にVMをグループ化したりできます。単一テナントノードの詳細については、GCPドキュメントの単一テナンシーの概要を参照してください。

単一テナントノードにVM（マシンプロファイルソース）をプロビジョニングする方法については、GCPドキュメントの単一テナントノードでのVMのプロビジョニングを参照してください。

> **注:**
>
> - ノードグループと同じインスタンスタイプとリージョンを選択します。
> - Shielded VMセクションでvTPMを有効にします。詳細については、クイックスタート: Shielded VMオプションを有効にするを参照してください。
> - ソースVMでBitlockerを無効にします。

Windows 11のマシンプロファイルソースを使用してMCSマシンカタログを作成する

Web StudioまたはPowerShellコマンドを使用して、Windows 11 VMを作成するためのMCSマシンカタログを作成できます。

注:

- マスターイメージには、Windows 11のスナップショットまたはVMを選択します。
- マシンプロファイルソースには、Windows 11 VMをマシンプロファイルとして選択します。マシンプロファイルソースは、単一テナントノードで説明されているものと同じインスタンスタイプである必要があります。

Web Studioの使用方法については、「Web Studioを使用してマシンカタログを作成する」(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create/create-machine-catalog-gcp#create-a-machine-catalog-using-web-studio)を参照してください。

PowerShellコマンドについては、「マシンプロファイルを使用してマシンカタログを作成する」(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create/create-machine-catalog-gcp#create-a-machine-catalog-using-a-machine-profile)を参照してください。

カタログを作成し、VM の電源をオンにすると、Google Cloud コンソールで単一テナントノード上で実行されている Windows 11 VM を確認できます。

継承されたラベルを持つ VM とディスク

MCSマシンカタログのVMとディスク（IDディスク、ライトキャッシュバックディスク、OSディスク）は、マシンプロファイルソース（GCP VMインスタンスまたはインスタンステンプレート）のラベルを継承できます。これらのラベルを使用して、異なるチーム（例：team:researchやteam:analytics）が所有するインスタンスを区別し、さらにコスト計算や予算編成に利用できます。ラベルの詳細については、GCPドキュメントラベルを使用してリソースを整理するを参照してください。

マシンプロファイルソースを使用して、新しいカタログを作成したり、既存のカタログを更新したり、既存のVMを更新してラベルを継承させたりできます。

この機能は、永続的および非永続的な MCS マシンカタログに適用されます。

次のことができます。

- 継承されたラベルを持つカタログを作成する

- 継承されたラベルを持つ既存のカタログを更新する
- 継承されたラベルを持つ既存のVMを更新する
- VMとブートディスクのラベルの情報を取得する
- VMを削除する

継承されたラベルを持つカタログを作成する

VMとディスクがマシンプロファイルソースからラベルを継承するMCSマシンカタログを作成するには、次の手順を実行します。

1. ラベル付きのマシンプロファイルソース（VMインスタンスまたはインスタンステンプレート）を作成します。ラベル付きVMの作成については、GCPドキュメントのラベル付きリソースの作成を参照してください。インスタンステンプレートはVMから作成され、VMで定義されたラベルを引き継ぎます。
2. Web StudioまたはPowerShellコマンドを使用してMCSカタログを作成します。
3. Web Studioを使用している場合は、**イメージ**ページで**マシンプロファイルを使用**を選択し、VMまたはテンプレートを選択します。
4. PowerShellコマンドを使用している場合、次の操作を行います。

    a. PowerShellウィンドウを開きます。

    b. asnp citrix* を実行します。

    c. IDプールを作成します。IDプールは、作成されるVMのActive Directory (AD) アカウントのコンテナです。

    d. Active Directoryで必要なADコンピューターアカウントを作成します。

    e. カタログを作成するには、`New-ProvScheme`コマンドを実行します。例:

    マシンプロファイル入力としてテンプレートを使用するNew-ProvScheme（永続カタログ）：

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

```
-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `
```

マシンプロファイル入力としてインスタンステンプレートを使用するNew-ProvScheme（非永続カタログ）：

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `

-CleanOnBoot
```

VMインスタンスをマシンプロファイル入力として使用するNew-ProvScheme (永続カタログ):

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

VMインスタンスをマシンプロファイル入力として使用するNew-ProvScheme (非永続カタログ):

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-CleanOnBoot
```

f. プロビジョニングスキームをブローカーカタログとして登録します。

g. カタログにVMを追加します。

継承されたラベルで既存のカタログを更新する

新しいマシンプロファイルを持つように既存のカタログを更新するには、Set-ProvSchemeコマンドを実行します。コマンドを実行すると、カタログに追加されたすべての新しいVMは、新しいマシンプロファイルソースのラベルを持ちます。非永続カタログは、次回の電源投入時に更新されます。

例えば:

インスタンステンプレートをマシンプロファイル入力として使用するSet-ProvScheme:

```
Set-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `
```

VMインスタンスをマシンプロファイル入力として使用するSet-ProvScheme:

```
Set-ProvScheme `

-ProvisioningSchemeName "catalog-name" `
```

```
-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

継承されたラベルで既存のVMを更新する

更新されたマシンプロファイルソースで既存のVMを更新するには、次のコマンドを実行します:

1. `Set-ProvScheme`
2. `Set-ProvVMUpdateTimeWindow`。例えば:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
   <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
   ```

3. VMを再起動します。

VMおよびブートディスクラベルの情報を取得する

VM作成後、`Get-Item`コマンドと`AdditionalData`パラメータを使用して、VMおよびブートディスクラベルの情報を取得できます。

VMラベルの情報を取得するには、次のコマンドを実行します。

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-
name\vm_name.vm).AdditionalData.Tags
```

ブートディスクラベルの情報を取得するには、次のコマンドを実行します。

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-name\vm_name.vm\bootdisk-
name.attacheddisk).AdditionalData.Tags
```

注:

さまざまなハイパーバイザー間で一貫性を保つため、GCPラベルを表示するのに「タグ」という用語を使用しています。

VMを削除する

カタログからVMを削除しても、GCPからVMを削除しない選択ができます。この場合、Citrixラベルのみが VMから削除されます。追加された他のすべてのラベルはVMから削除されません。Web StudioまたはPowerShellコマンドを使用してVMを削除できます。

WEB STUDIOの使用

1. VMを選択して右クリックします。
2. **「削除」**をクリックします。
3. **「仮想マシンをカタログから削除するが、仮想マシンは削除しない」**を選択します。

POWERSHELLコマンドの使用

`ForgetVM`パラメータを指定して`Remove-ProvVM`を実行します。詳細については、SDKドキュメントRemove-ProvVMを参照してください。

Google Cloud マーケットプレイス

Citrixが**Google Cloud Marketplace**で提供するイメージを参照して選択し、マシンカタログを作成できます。現在、MCSはこの機能に対してマシンプロファイルワークフローのみをサポートしています。

Google Cloud Marketplace で Citrix VDA VM 製品を検索するには、https://console.cloud.google.com/marketplace にアクセスしてください。

Google Cloud Marketplace のカスタムイメージまたは Citrix ready® イメージを使用して、マシンカタログのイメージを更新できます。

> **注:**
>
> マシンプロファイルにストレージタイプの情報が含まれていない場合、その値はカスタムプロパティから派生します。

> サポートされているGoogle Cloud Marketplaceイメージは次のとおりです。

- Windows 2019シングルセッション
- Windows 2019 マルチセッション
- ウブントゥ

Citrix対応イメージをマシンカタログ作成のソースとして使用する例:

```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \

-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \

-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
```

```
win2019-single-vda-v20220819.publicimage \

-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
```

次のステップ

- これが最初に作成するカタログである場合、Web Studio は デリバリーグループの作成 に誘導します。
- 構成プロセス全体を確認するには、インストールと構成 を参照してください。
- カタログを管理するには、マシンカタログの管理 および Google Cloud Platform カタログの管理 を参照してください。

詳細情報

- 接続とリソースを作成および管理する
- Google Cloud環境への接続
- マシンカタログを作成する

HPE Moonshot マシンカタログを作成する

(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create.html)は、マシンカタログを作成するウィザードについて説明しています。以下の情報は、HPE Moonshot環境に固有の詳細を扱っています。

注:

- HPE Moonshotへの接続を作成する
- 1つ以上のHPE Moonshotノードが利用可能であることを確認し、それらのノードにVDAをインストールしてください。
- 初期のHPE Moonshotカートリッジイメージの作成については、OS Deployment on Moonshotユーザーガイドを参照してください。

HPE Moonshotマシンカタログは、以下を使用して作成できます。

- ウェブスタジオ
- PowerShellコマンド

Web Studioを使用してマシンカタログを作成する

マシンカタログのセットアップウィザードで、:

1. **オペレーティングシステム**ページで、**マルチセッションOS**または**シングルセッションOS**を選択します。
2. **マシン管理**ページで、**電源管理されているマシン**と**別のサービスまたはテクノロジー**を選択します。
3. **仮想マシン**ページで、マシンとそのActive Directoryマシンアカウントを追加します。次のいずれかを実行できます。
   - **マシンの追加**をクリックして、マシンを手動で追加します。**VMの選択**ウィンドウが表示されます。以前に作成したHPE Moonshotシャーシ接続を展開し、追加するノード（VM）を選択します。次に、関連するマシンアカウント名を追加します。
   - マシンを一括追加するには、「**CSVファイルの追加**」をクリックします。CSVファイルを使用してマシンを追加する方法については、「CSVファイルを使用してカタログにマシンを一括追加する」を参照してください。

スコープページと**概要**ページには、HPE Moonshot固有の情報は含まれていません。

PowerShellコマンドを使用してマシンカタログを作成する

ブローカーカタログを作成し、マシンをブローカーカタログにインポートするには、`New-BrokerCatalog`および`New-BrokerMachine` PowerShellコマンドを実行します。

例:

```
New-BrokerCatalog  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -AllocationType "Random" -IsRemotePC $False
-MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "BurMC"
-PersistUserChanges "OnLocal" -ProvisioningType "Manual" -Scope @()
-SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc-4578-bc07-
bcf2a82d1463"

New-BrokerMachine  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -CatalogUid 3 -HostedMachineId "c10n1"
-HypervisorConnectionUid 4 -IsReserved $False -MachineName
"S-1-5-21-2589939477-3963209805-1860259709-1121"
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、「インストールと構成」を参照してください。
- カタログを管理するには、「マシンカタログの管理」および「HPE Moonshotカタログの管理」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- HPE Moonshotへの接続
- マシンカタログの作成

Microsoft Azureカタログの作成

(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create.html)では、マシンカタログを作成するウィザードについて説明しています。以下の情報は、Microsoft Azure Resource Managerクラウド環境に固有の詳細を扱っています。

> **注:**
>
> Microsoft Azureカタログを作成する前に、Microsoft Azureへの接続の作成を完了する必要があります。Microsoft Azureへの接続を参照してください。

マシンカタログの作成

マシンカタログは、次の2つの方法で作成できます。

- Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する
- PowerShellを使用してマシンカタログを作成する

Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する

イメージとは、マシンカタログ内のVMを作成するために使用される、Azure Compute Gallery内のイメージ定義のディスク、スナップショット、またはイメージバージョンを指します。マシンカタログを作成する前に、Azure Resource Managerでイメージを作成します。イメージに関する一般的な情報については、マシンカタログを作成するを参照してください。

> **注:**
>
> ホスト接続で構成されているリージョンとは異なるリージョンからのマスターイメージの使用は非推奨になりました。Azure Compute Galleryを使用して、マスターイメージを目的のリージョンにレプリケートしてください。

> MCSマシンカタログを作成する際、DHCPの有効化やライセンスの再アームなどの準備タスクを実行するために、元のVMに基づいて一時的なVMが作成されます。この一時的なVMは準備VMと呼ばれます。この準備VMの名前は**Preparati-84x9n**という形式に従い、最後の5文字は重複を避けるためにランダムに生成されます。この準備VMの命名規則は固定されており、カスタマイズできません。準備タスクが完了すると、準備VMは破棄されます。

準備VMからネットワークを切断するために、すべてのインバウンドおよびアウトバウンドトラフィックを拒否するネットワークセキュリティグループが作成されます。ネットワークセキュリティグループは、カタログごとに1回自動的に作成されます。ネットワークセキュリティグループの名前は`Citrix-Deny-All-a3pgu-GUID`で、GUIDはランダムに生成されます。例: `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`。

マシンカタログ作成ウィザードで:

- 「**マシンタイプ**」および「**マシン管理**」ページには、Azure固有の情報は含まれていません。マシンカタログの作成の記事のガイダンスに従ってください。
- **イメージ**ページで、このカタログにマシンを作成するためのテンプレートとして使用するイメージを選択します。

  使用するイメージの種類として**マスターイメージ**を選択する場合は、**イメージの選択**をクリックし、必要に応じてマスターイメージを選択するために次の手順に従います。

  a. (テナント内またはテナント間で共有イメージが構成されている接続にのみ適用) イメージが存在するサブスクリプションを選択します。

  b. リソースグループを選択します。

  c. Azure VHD、Azure Compute Gallery、またはAzureイメージバージョンに移動します。必要に応じて、選択したイメージにメモを追加します。

  イメージを選択する際は、次の点を考慮してください。

  - イメージにCitrix VDAがインストールされていることを確認します。

- VMにアタッチされたVHDを選択した場合、次のステップに進む前にVMをシャットダウンする必要があります。

注:

- カタログ内のマシンを作成した接続（ホスト）に対応するサブスクリプションは、緑色の点で示されます。その他のサブスクリプションは、Azure Compute Galleryがそのサブスクリプションと共有されているものです。これらのサブスクリプションでは、共有ギャラリーのみが表示されます。共有サブスクリプションの構成方法については、テナント内でイメージを共有する（サブスクリプション間）およびテナント間でイメージを共有するを参照してください。
- Trusted Launchが有効になっているイメージまたはスナップショットを選択する場合、**セキュリティの種類**としてTrusted Launchを持つマシンプロファイルを使用することが必須です。その後、マシンプロファイルでSecureBootとvTPMの値を指定することで、それらを有効または無効にできます。Trusted LaunchはShared Image Galleryではサポートされていません。Azure Trusted Launchの詳細については、`<https://docs.microsoft.com/ja-jp/azure/virtual-machines/trusted-launch>`を参照してください。
- Trusted Launchが有効なWindowsでエフェメラルOSディスクを使用してプロビジョニングスキームを作成できます。Trusted Launchが有効なイメージを選択する場合、vTPMが有効なTrusted Launchを持つマシンプロファイルを選択する必要があります。エフェメラルOSディスクを使用してマシンカタログを作成する方法については、「エフェメラルOSディスクを使用してマシンを作成する方法」を参照してください。
- イメージのレプリケーションが進行中の場合でも、イメージをマスターイメージとして選択し、セットアップを完了できます。ただし、イメージのレプリケーション中にカタログ作成が完了するまでに時間がかかる場合があります。MCSは、カタログ作成から1時間以内にレプリケーションが完了することを要求します。レプリケーションがタイムアウトすると、カタログ作成は失敗します。Azureでレプリケーションステータスを確認できます。レプリケーションがまだ保留中の場合、またはレプリケーションが完了した後に、もう一度試してください。
- Azureでマシンカタログのマスターイメージを選択すると、MCSは選択したマスターイメージとマシンプロファイルに基づいてOSの種類を識別します。MCSが識別できない場合は、マスターイメージに一致するOSの種類を選択してください。

- Gen2イメージを使用してGen2 VMカタログをプロビジョニングすることで、起動時間のパフォーマンスを向上させることができます。ただし、Gen1イメージを使用してGen2マシンカタログを作成することはサポートされていません。同様に、Gen2イメージを使用してGen1マシンカタログを作成することもサポートされていません。また、世代情報を持たない古いイメージはすべてGen1イメージです。

使用するイメージの種類として**準備済みイメージ**を選択した場合は、**イメージの選択**をクリックし、必要に応じて準備済みイメージを選択します。

VMの作成を成功させるには、イメージにCitrix VDA 2311以降がインストールされており、VDAにMCSIOが存在することを確認してください。

イメージを選択すると、**マシンプロファイルを使用（Microsoft Entra IDに必須）**チェックボックスが自動的に選択されます。**マシンプロファイルの選択**をクリックして、リソースグループのリストからVMまたはARMテンプレート仕様を参照します。カタログ内のVMは、選択したマシンプロファイルから構成を継承できます。

ARMテンプレート仕様がマシンカタログを作成するためのマシンプロファイルとして使用できることを確認するために検証します。ARMテンプレート仕様を検証する方法は2つあります。

- リソースグループリストからARMテンプレート仕様を選択した後、**次へ**をクリックします。ARMテンプレート仕様にエラーがある場合、エラーメッセージが表示されます。
- 次のPowerShellコマンドのいずれかを実行します。
  - `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  - `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

VMがマシンプロファイルから継承できる構成の例は次のとおりです。

- アクセラレーテッドネットワーク
- ブート診断
- ホストディスクキャッシュ（OSおよびMCSIOディスク関連）
- マシンサイズ（特に指定がない限り）
- VMに配置されたタグ

カタログを作成した後、イメージがマシンプロファイルから継承する構成を表示できます。**マシンカタログ**ノードでカタログを選択し、下部のペインで詳細を表示します。次に、**テンプ**

レートプロパティタブをクリックして、マシンプロファイルのプロパティを表示します。**タグ**セクションには最大3つのタグが表示されます。VMに配置されているすべてのタグを表示するには、**すべて表示**をクリックします。

MCSでAzure専用ホストにVMをプロビジョニングする場合は、**専用ホストグループを使用**チェックボックスを有効にしてから、リストからホストグループを選択します。ホストグループは、専用ホストのコレクションを表すリソースです。専用ホストは、1つ以上のVMをホストする物理サーバーを提供するサービスです。サーバーはAzureサブスクリプション専用であり、他のサブスクライバーと共有されることはありません。専用ホストを使用すると、AzureはVMがそのホストで実行されている唯一のマシンであることを保証します。この機能は、規制要件または内部セキュリティ要件を満たす必要があるシナリオに適しています。ホストグループとその使用に関する考慮事項の詳細については、「Azure 専用ホスト」を参照してください。

重要:

- Azure自動配置が有効になっているホストグループのみが表示されます。
- ホストグループを使用すると、ウィザードの後半で表示される**仮想マシン**ページが変更されます。選択したホストグループに含まれるマシンサイズのみがそのページに表示されます。また、可用性ゾーンは自動的に選択され、選択できません。

- **ストレージとライセンスの種類**ページは、Azure Resource Managerイメージを使用する場合にのみ表示されます。
  - **ストレージ冗長タイプ**を選択します。
    - ローカル冗長ストレージ (LRS): LRSを使用すると、利用可能なすべてのストレージタイプから選択できます。LRSを使用する場合、Azureは指定された可用性ゾーン内にのみ仮想マシン (VM) をデプロイします。
    - ゾーン冗長ストレージ (ZRS): ZRSはVM配置の柔軟性を高め、Azureは利用可能な任意のゾーンでVMを起動できます。これはローカル冗長ストレージ (LRS) に対する主要な利点であり、ディスクの元のゾーンにアクセスできなくなった場合でもVMの可用性を保証します。ただし、ZRSはPremium SSDおよびStandard SSDストレージタイプとのみ互換性があります。
  - マシンカタログに使用する**ストレージタイプ**を選択します。ストレージタイプによって、ウィザードの**仮想マシン**ページで提供されるマシンサイズが決まります。

- I/O負荷の高いワークロードを持つVMに適した、高性能で低遅延のディスクストレージオプションとして、「**Premium SSD**」を提供します。
- **Standard SSD**。低いIOPSレベルで一貫したパフォーマンスを必要とするワークロードに適した、費用対効果の高いストレージオプションを提供します。
- **Standard HDD**。遅延に影響されないワークロードを実行するVMに適した、信頼性の高い低コストのディスクストレージオプションを提供します。
- **Azureエフェメラルosディスク**。VMのローカルディスクを再利用してオペレーティングシステムディスクをホストする、費用対効果の高いストレージオプションを提供します。または、PowerShellを使用してエフェメラルOSディスクを使用するマシンを作成することもできます。詳細については、「Azure エフェメラルディスク」を参照してください。エフェメラルOSディスクを使用する際には、以下を考慮してください。
  - AzureエフェメラルOSディスクとMCS I/Oは同時に有効にすることはできません。
  - エフェメラルOSディスクを使用するマシンを更新するには、VMのキャッシュディスクまたは一時ディスクのサイズを超えないイメージを選択する必要があります。
  - ウィザードの後半で提供される**電源サイクル中にVMとシステムディスクを保持する**オプションは使用できません。

> **注:**
>
> - 選択したストレージの種類に関係なく、IDディスクは常にStandard SSDを使用して作成されます。
> - **ストレージ冗長性**として**ZRS**を選択した場合、**Premium SSD**と**Standard SSD**のみを選択するオプションが表示されます。

> Azure ストレージの種類とストレージレプリケーションの詳細については、以下を参照してください。

- `<https://docs.microsoft.com/ja-jp/azure/storage/common/storage-introduction/>`
- `<https://docs.microsoft.com/ja-jp/azure/virtual-machines/premium-storage-performance/>`
- `<https://docs.microsoft.com/ja-jp/azure/storage/common/storage-redundancy/>`

既存のWindowsライセンスまたはLinuxライセンスを使用するかどうかを選択します。

- Windowsライセンス：WindowsライセンスをWindowsイメージ（Azureプラットフォームサポートイメージまたはカスタムイメージ）とともに使用すると、AzureでWindows VMを低コストで実行できます。ライセンスには次の2種類があります。
  - **Windows Serverライセンス**。Windows ServerまたはAzure Windows Serverライセンスを使用でき、Azureハイブリッド特典を利用できます。詳細については、`<https://azure.microsoft.com/ja-jp/pricing/hybrid-benefit/>`を参照してください。Azureハイブリッド特典は、AzureでのVM実行コストを基本コンピューティング料金に削減し、Azureギャラリーからの追加のWindows Serverライセンスのコストを免除します。
  - **Windowsクライアントライセンス**。Windows 10およびWindows 11ライセンスをAzureに持ち込むことができ、追加のライセンスなしでAzureでWindows 10およびWindows 11 VMを実行できます。詳細については、「クライアントアクセスライセンスと管理ライセンス」を参照してください。

プロビジョニングされたVMがライセンス特典を使用しているかどうかは、次のPowerShellコマンドを実行して確認できます: `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`。

- Windows Serverライセンスタイプの場合、ライセンスタイプが**Windows_Server**であることを確認します。詳細な手順は`<https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/hybrid-use-benefit-licensing/>`で入手できます。
- Windows Client ライセンスタイプの場合、ライセンスタイプが **Windows_Client** であることを確認します。詳細な手順は `<https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/>` で入手できます。

または、`Get-Provscheme` PowerShell SDK を使用して検証を行うこともできます。例: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`。このコマンドレットの詳細については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/>` を参照してください。

- Linux ライセンス: BYOS (bring-your-own-subscription) Linux ライセンスでは、ソフトウェアの料金を支払う必要はありません。BYOS の料金には、コンピューティングハードウェア料金のみが含まれます。ライセンスには次の2種類があります。

- **RHEL_BYOS**: RHEL_BYOS タイプを正常に使用するには、Azure サブスクリプションで Red Hat Cloud Access を有効にします。
- **SLES_BYOS**: SLES の BYOS バージョンには、SUSE からのサポートが含まれています。

LicenseType の値を `New-ProvScheme` および `Set-ProvScheme` で Linux オプションに設定できます。

`New-ProvScheme` で LicenseType を RHEL_BYOS に設定する例:

```
New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "azureCatalog"
-RunAsynchronously -Scope @() -SecurityGroup @() -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" /><Property xsi:type="StringProperty"
Name="StorageAccountType" Value="StandardSSD_LRS" /><Property
xsi:type="StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /
><Property xsi:type="StringProperty" Name="OsType" Value="Linux" /
><Property xsi:type="StringProperty" Name="LicenseType"
Value="RHEL_BYOS" /></CustomProperties>'
```

`Set-ProvScheme` で LicenseType を SLES_BYOS に設定する例:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog"
-CustomProperties '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"><Property
xsi:type="StringProperty" Name="UseManagedDisks" Value="true" /
><Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" /><Property xsi:type="StringProperty"
Name="ResourceGroups" Value="hu-dev-mcs" /><Property
xsi:type="StringProperty" Name="OsType" Value="Linux" /><Property
xsi:type="StringProperty" Name="LicenseType" Value="SLES_BYOS" /></
CustomProperties>'
```

注:

> `LicenseType` の値が空の場合、デフォルト値は OsType の値に応じて Azure Windows Server License または Azure Linux License になります。

> LicenseType を空に設定する例:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog"
-CustomProperties '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"><Property
xsi:type="StringProperty" Name="UseManagedDisks" Value="true" /
><Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" /><Property xsi:type="StringProperty"
Name="ResourceGroups" Value="hu-dev-mcs" /><Property
xsi:type="StringProperty" Name="OsType" Value="Linux" /></
CustomProperties>'
```

ライセンスの種類とその利点については、以下のドキュメントを参照してください。

- `<https://docs.microsoft.com/ja-jp/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet>`
- `<https://docs.microsoft.com/ja-jp/azure/virtual-machines/linux/azure-hybrid-benefit-linux>`

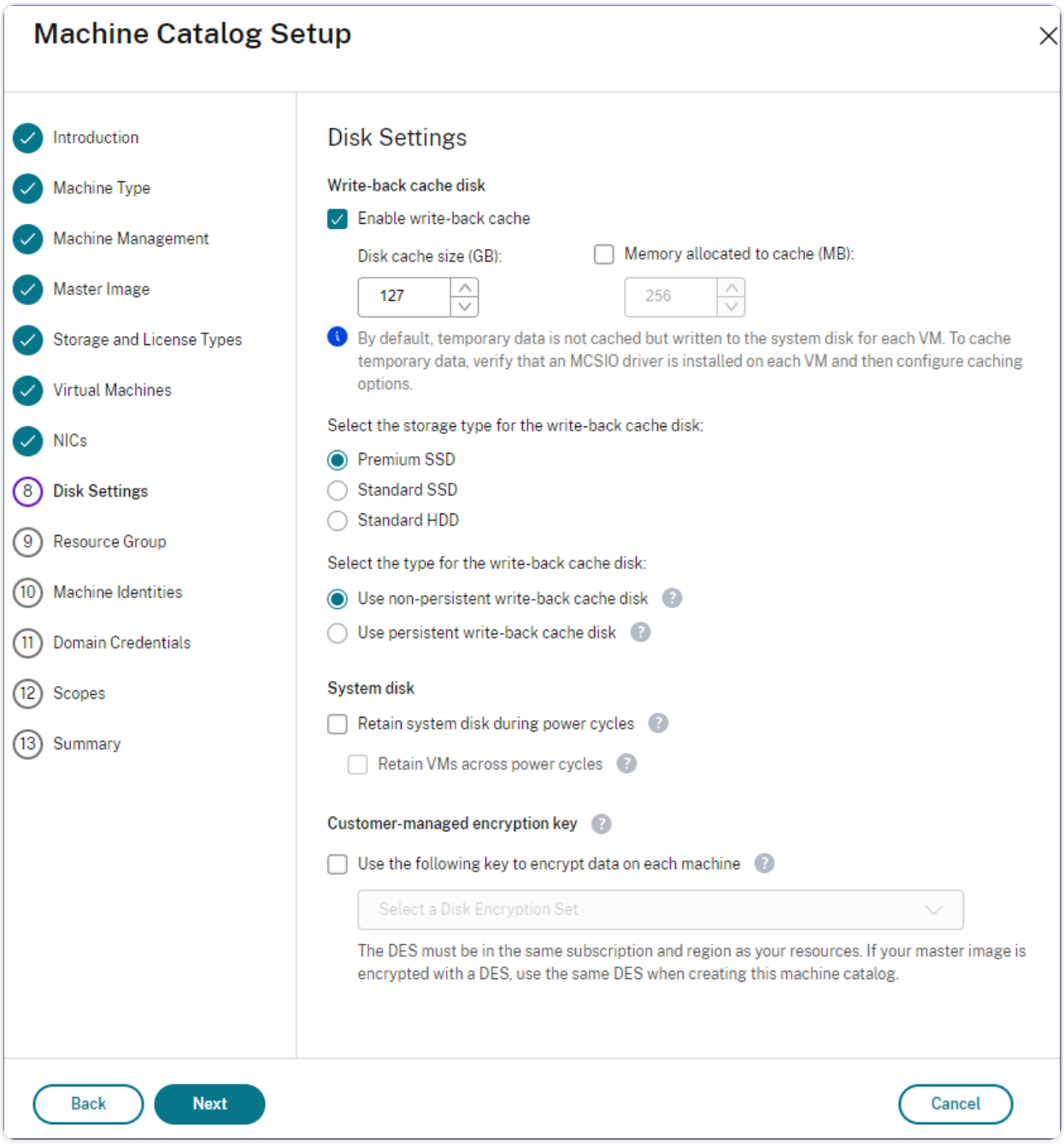
Azure Compute Gallery (旧称 Azure Shared Image Gallery) は、イメージを管理および共有するためのリポジトリです。これにより、組織全体でイメージを利用できるようになります。大規模な非永続マシンカタログを作成する際には、SIG にイメージを保存することをお勧めします。そうすることで、VDA OS ディスクのリセットが高速化されるためです。 を選択すると、セクションが表示され、さらに Azure Compute Gallery の設定を指定できます。

- **仮想マシンとイメージレプリカの比率**。Azure に保持させたい仮想マシンとイメージレプリカの比率を指定できます。デフォルトでは、Azure は 40 台の非永続マシンごとに 1 つのイメージレプリカを保持します。永続マシンの場合、その数はデフォルトで 1,000 です。
- **最大レプリカ数**。Azure に保持させたいイメージレプリカの最大数を指定できます。デフォルトは 100 です。

> **注:**

> イメージを保存するために、ACG にギャラリーが作成されます。このギャラリーは、VM 作成のために MCS からのみアクセス可能であり、**イメージの選択**ページには表示されません。

- **仮想マシン**ページで、作成する VM の数とマシンのサイズを指定します。カタログ作成後、カタログを編集してマシンのサイズを変更できます。
- **NIC**ページには、Azure固有の情報は含まれていません。マシンカタログの作成の記事のガイダンスに従ってください。
- **ディスク設定**ページで、ライトバックキャッシュを有効にするかどうかを選択します。MCS ストレージ最適化機能が有効になっている場合、カタログ作成時に次の設定を構成できます。これらの設定は、Azure と GCP の両方の環境に適用されます。



ライトバックキャッシュを有効にした後、以下を実行できます。

- 一時データのキャッシュに使用されるディスクとRAMのサイズを構成します。詳細については、「一時データのキャッシュを構成する」を参照してください。
- ライトバックキャッシュディスクのストレージタイプを選択します。ライトバックキャッシュディスクには、次のストレージオプションを使用できます。
  - プレミアム SSD
  - スタンダード SSD
  - スタンダード HDD

> **注:**
>
> 「**ストレージとライセンスの種類**」ページで「**ストレージ冗長性**」として「**ZRS**」を選択した場合、ライトバックキャッシュディスクのストレージ冗長性はデフォルトでZRSに設定されます。

- プロビジョニングされたVMに対してライトバックキャッシュディスクを永続化するかどうかを選択します。オプションを有効にするには、**ライトバックキャッシュを有効にする**を選択します。デフォルトでは、**非永続ライトバックキャッシュディスクを使用する**が選択されています。
- ライトバックキャッシュディスクの種類を選択します。
  - **非永続ライトバックキャッシュディスクを使用する**。選択した場合、ライトバックキャッシュディスクは電源サイクル中に削除されます。そこにリダイレクトされたデータはすべて失われます。VMの一時ディスクに十分なスペースがある場合、コストを削減するためにライトバックキャッシュディスクをホストするために使用されます。カタログ作成後、プロビジョニングされたマシンが一時ディスクを使用しているかどうかを確認できます。これを行うには、カタログをクリックし、「**テンプレートプロパティ**」タブの情報を確認します。一時ディスクが使用されている場合、「**非永続ライトバックキャッシュディスク**」と表示され、その値は「**はい（VMの一時ディスクを使用）**」となります。そうでない場合、「**非永続ライトバックキャッシュディスク**」と表示され、その値は「**いいえ（VMの一時ディスクを使用しない）**」となります。
  - **永続ライトバックキャッシュディスクを使用する**。選択した場合、ライトバックキャッシュディスクはプロビジョニングされたVMに対して永続化されます。このオプションを有効にすると、ストレージコストが増加します。

> **注記:**
>
> 以下のすべての条件が満たされている場合、カタログはWBCディスクにAzure一時ディスクを自動的に使用します。
>
> - MCSIOが有効になっている。
> - WBCディスクが非永続である。
> - VMサイズに、WBCディスクに十分な大きさの一時ディスクが含まれている。

> ◦ WBCディスクにドライブ文字が指定されていない。 この機能は、カタログの作成と編集の両方に適用され、ストレージコストの削減に役立ちます。

◦ 電源サイクル中にVDAのVMとシステムディスクを保持するかどうかを選択します。

電源サイクル中に VM とシステムディスクを保持する。ライトバックキャッシュを有効にするを選択した場合に利用可能です。デフォルトでは、VM とシステムディスクはシャットダウン時に削除され、起動時に再作成されます。VM の再起動時間を短縮したい場合は、このオプションを選択します。このオプションを有効にすると、ストレージコストも増加することに注意してください。

◦ **ストレージコスト削減**を有効にするかどうかを選択します。有効にすると、VMがシャットダウンしたときにストレージディスクをStandard HDDにダウングレードすることで、ストレージコストを節約できます。VMは再起動時に元の設定に戻ります。このオプションは、ストレージディスクとライトバックキャッシュディスクの両方に適用されます。または、PowerShellを使用することもできます。「VMシャットダウン時にストレージタイプを下位層に変更する」を参照してください。

> **注:**
>
> Microsoft は、VM シャットダウン中のストレージタイプの変更に制限を課しています。また、Microsoft は将来的にストレージタイプの変更をブロックする可能性もあります。詳細については、このMicrosoft の記事を参照してください。

◦ このカタログ内のマシンのデータを暗号化するかどうか、およびどの暗号化キーを使用するかを選択します。顧客管理キー (CMK) を使用したサーバー側暗号化により、マネージドディスクレベルで暗号化を管理し、カタログ内のマシンのデータを保護できます。デフォルト設定は、マシンプロファイルまたはマスターイメージのいずれかから継承され、プロファイルが優先されます。

  ◦ *マシンプロファイル*と*CMK*を使用している場合、**各マシン上のデータを暗号化するために次のキーを使用する**オプションが自動選択され、*マシンプロファイル*からのキーがデフォルトになります。

  ◦ *マシンプロファイル*とプラットフォーム管理キー (PMK) を使用しており、*マスターイメージ*が*CMK*で暗号化されている場合、**各マシン上のデータを暗号化するために次のキーを使用する**オプションが自動選択され、マスターイメージからのキーがデフォルトになります。

- *マシンプロファイルを使用しておらず、マスターイメージがCMKで暗号化されている*場合、**各マシン上のデータを暗号化するために次のキーを使用する**オプションが自動選択され、*マスターイメージ*からのキーがデフォルトになります。

詳細については、Azure サーバー側暗号化を参照してください。

- **リソースグループ** ページで、リソースグループを作成するか、既存のグループを使用するかを選択します。
  - リソースグループを作成することを選択した場合は、**次へ**を選択します。
  - 既存のリソースグループを使用することを選択した場合は、**利用可能なプロビジョニングリソースグループ**リストからグループを選択します。**注意**: カタログで作成するマシンを収容するのに十分なグループを選択してください。選択したグループが少なすぎるとメッセージが表示されます。後でカタログにVMを追加する予定がある場合は、必要最小限よりも多く選択することをお勧めします。カタログ作成後に、カタログにリソースグループを追加することはできません。

詳細については、Azure リソースグループを参照してください。

- **マシンID**ページで、IDタイプを選択し、このカタログ内のマシンのIDを構成します。VMを**Microsoft Entra参加済み**として選択した場合、それらをMicrosoft Entraセキュリティグループに追加できます。詳細な手順は次のとおりです。

  a. **IDタイプ**フィールドから、**Microsoft Entra参加済み**を選択します。**Microsoft Entraセキュリティグループ (オプション)**オプションが表示されます。

  b. **Microsoft Entraセキュリティグループ: 新規作成**をクリックします。

  c. グループ名を入力し、**作成**をクリックします。

  d. 画面の指示に従ってAzureにサインインします。 グループ名がAzureに存在しない場合、緑色のアイコンが表示されます。それ以外の場合、新しい名前を入力するよう求めるエラーメッセージが表示されます。

  e. VMのコンピューターアカウントの命名規則を入力します。

  カタログ作成後、Citrix Virtual Apps and Desktopsはユーザーに代わってAzureにアクセスし、セキュリティグループとグループの動的メンバーシップルールを作成します。このルールに基づいて、このカタログで指定された命名規則を持つVMは自動的にセキュリティグループに追加されます。

  異なる命名規則を持つVMをこのカタログに追加するには、Azureにサインインする必要があります。その後、Citrix Virtual Apps™ and DesktopsはAzureにアクセスし、新しい命名規則に基づいて動的メンバーシップルールを作成できます。

このカタログを削除する際、Azure からセキュリティグループを削除するには、Azure へのサインインも必要です。

- **ドメイン資格情報**ページと**概要**ページには、Azure固有の情報は含まれていません。(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create.html)記事のガイダンスに従ってください。

> **ヒント:**
>
> **概要**ページでは、Azureの公開価格リストに基づいて、このマシンカタログ内の仮想マシンの月額見積もりコストを表示できます。カタログをホストする接続がAzureで `Microsoft.Consumption/pricesheets/read` 権限を持っている場合、見積もりは組織の契約価格を使用して計算されます。
>
> コスト見積もりを選択して詳細情報を表示します。より正確な見積もりを得るには、日ごとの稼働時間、週ごとの稼働日数、使用状況に基づいた節約オプションなどの設定を調整してください。

ウィザードを完了します。

Azure一時ディスクがライトバックキャッシュディスクの対象となる条件

Azure一時ディスクをライトバックキャッシュディスクとして使用できるのは、以下のすべての条件が満たされている場合のみです。

- Azure一時ディスクは永続的なデータには適していないため、ライトバックキャッシュディスクは非永続的である必要があります。
- 選択したAzure VMサイズには一時ディスクが含まれている必要があります。
- エフェメラルOSディスクを有効にする必要はありません。
- ライトバックキャッシュファイルをAzure一時ディスクに配置することを受け入れます。
- Azure一時ディスクのサイズは、（ライトバックキャッシュディスクサイズ + ページングファイル用の予約スペース + 1 GBのバッファースペース）の合計サイズよりも大きい必要があります。

非永続的なライトバックキャッシュディスクのシナリオ

次の表は、マシンカタログの作成時に一時ディスクをライトバックキャッシュに使用する場合の3つの異なるシナリオについて説明しています。

シナリオ	結果
ライトバックキャッシュに一時ディスクを使用するためのすべての条件が満たされています。	WBCファイル `mcsdif.vhdx` は一時ディスクに配置されます。
一時ディスクには、ライトバックキャッシュの使用に十分なスペースがありません。	VHDディスク `MCSWCDisk` が作成され、WBCファイル `mcsdif.vhdx` がこのディスクに配置されます。
一時ディスクにはライトバックキャッシュの使用に十分なスペースがありますが、`UseTempDiskForWBC` が **false** に設定されています。	VHDディスク `MCSWCDisk` が作成され、WBCファイル `mcsdif.vhdx` がこのディスクに配置されます。

Azureテンプレート仕様の作成

AzureポータルでAzureテンプレート仕様を作成し、Web StudioおよびPowerShellコマンドで使用して、MCSマシンカタログを作成または更新できます。

既存のVM用のAzureテンプレート仕様を作成するには：

1. Azure portalに移動します。リソースグループを選択し、VMとネットワークインターフェースを選択します。上部にある**...**メニューから、**テンプレートのエクスポート**をクリックします。
2. カタログプロビジョニング用のテンプレート仕様を作成する場合は、**パラメーターを含める**チェックボックスをオフにします。JSONファイルで `parameters` と `variables` のセクションが次のようになっていることを確認します。

   ```
   "parameters": {},

   "variables": {}
   ```

3. **ダウンロード**をクリックして、テンプレートをJSONファイルとして保存します。
4. Azure portalで、**テンプレート仕様**を選択し、**テンプレートのインポート**をクリックします。
5. コンピューターに保存されているマシンプロファイル（JSON形式）を参照してインポートします。
6. **名前**、**サブスクリプション**、**リソースグループ**、**場所**、**バージョン**を指定します。**次へ: テンプレートの編集**をクリックします。

7. **確認と作成**を作成し、テンプレート仕様を作成します。
8. **テンプレート仕様**ページで、作成したばかりのテンプレート仕様を確認します。テンプレート仕様をクリックします。左側のパネルで、**バージョン**をクリックします。
9. **新しいバージョンの作成**をクリックして、新しいバージョンを作成できます。新しいバージョン番号を指定し、現在のテンプレート仕様に変更を加え、**確認と作成**をクリックしてテンプレート仕様の新しいバージョンを作成します。

以下のPowerShellコマンドを使用して、テンプレート仕様とテンプレートバージョンの情報を取得できます。

- テンプレートスペックの情報を取得するには、以下を実行します。

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec
```

- テンプレートスペックバージョンの情報を取得するには、以下を実行します。

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec\bgg1.0.templatespecversion
```

カタログの作成または更新でテンプレート仕様を使用する

マシンプロファイルの入力としてテンプレート仕様を使用して、MCSマシンカタログを作成または更新できます。これを行うには、Web StudioまたはPowerShellコマンドを使用できます。

- Web Studioについては、「Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する」を参照してください。
- PowerShellについては、Use template spec in creating or updating a catalog using PowerShellを参照してください。

Azureサーバー側暗号化

Citrix Virtual Apps and Desktopsは、Azure Key Vaultを介したAzureマネージドディスクの顧客管理暗号化キーをサポートしています。このサポートにより、独自の暗号化キーを使用してマシンカタログのマネージドディスクを暗号化することで、組織およびコンプライアンス要件を管理できます。詳細については、Server-side encryption of Azure Disk Storageを参照してください。

マネージドディスクでこの機能を使用する場合：

- ディスクの暗号化に使用されているキーを変更するには、`DiskEncryptionSet`で現在のキーを変更します。その`DiskEncryptionSet`に関連付けられているすべてのリソースは、新しいキーで暗号化されるように変更されます。
- キーを無効化または削除すると、そのキーを使用しているディスクを持つVMは自動的にシャットダウンします。シャットダウン後、キーが再度有効になるか、新しいキーを割り当てない限り、VMは使用できません。そのキーを使用しているカタログは電源をオンにできず、VMを追加することもできません。

顧客管理暗号化キーを使用する際の重要な考慮事項

この機能を使用する際は、以下を考慮してください。

- 顧客管理キーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンに存在する必要があります。
- 顧客管理キーで暗号化されたディスク、スナップショット、およびイメージは、別のリソースグループやサブスクリプションに移動できません。
- リージョンごとのディスク暗号化セットの制限については、Microsoftサイトを参照してください。

> **注:**
>
> Azureサーバー側暗号化の構成については、クイックスタート: Azureポータルを使用してKey Vaultを作成するを参照してください。

Azureカスタマーマネージド暗号化キー

マシンカタログを作成する際、カタログにプロビジョニングされたマシン上のデータを暗号化するかどうかを選択できます。カスタマーマネージド暗号化キーによるサーバー側暗号化を使用すると、マネージドディスクレベルで暗号化を管理し、カタログ内のマシン上のデータを保護できます。ディスク暗号化セット（DES）は、カスタマーマネージドキーを表します。この機能を使用するには、まずAzureでDESを作成する必要があります。DESは次の形式です。

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryptionSet`

リストからDESを選択します。選択するDESは、リソースと同じサブスクリプションおよびリージョンにある必要があります。

顧客管理キーを使用したマシンカタログの作成を参照してください。

ホストでのAzureディスク暗号化

ホストでの暗号化機能を備えたMCSマシンカタログを作成できます。現在、MCSはこの機能に対してマシンプロファイルワークフローのみをサポートしています。マシンプロファイルの入力として、VMまたはテンプレート仕様を使用できます。

この暗号化方法は、Azureストレージを介してデータを暗号化しません。VMをホストするサーバーがデータを暗号化し、その後、暗号化されたデータがAzureストレージサーバーを介して流れます。したがって、この暗号化方法はデータをエンドツーエンドで暗号化します。

制限事項：

ホストでのAzureディスク暗号化は次のとおりです。

- すべてのAzureマシンサイズでサポートされているわけではありません
- Azure ディスク暗号化と互換性がありません

ホストでの暗号化機能を持つマシンカタログを作成するには：

1. サブスクリプションでホストでの暗号化機能が有効になっているかどうかを確認します。これを行うには、`<https://learn.microsoft.com/ja-jp/rest/api/resources/features/get?tabs=HTTP/>`を参照してください。有効になっていない場合は、サブスクリプションでこの機能を有効にする必要があります。サブスクリプションで機能を有効にする方法については、`<https://learn.microsoft.com/ja-jp/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/>`を参照してください。
2. 特定のAzure VMサイズがホストでの暗号化をサポートしているかどうかを確認します。これを行うには、PowerShellウィンドウで次のいずれかを実行します。

   ```
   PS XDHyp:\Connections\<your connection>\east
   us.region\serviceoffering.folder>
   ```

   ```
   PS XDHyp:\HostingUnits\<your hosting unit>\serviceoffering.folder>
   ```

3. ホストでの暗号化が有効になっているVMまたはテンプレート仕様を、マシンプロファイルの入力としてAzureポータルで作成します。

- VMを作成する場合は、ホストでの暗号化をサポートするVMサイズを選択します。VMを作成すると、VMプロパティの**ホストでの暗号化**が有効になります。
- テンプレート仕様を使用したい場合は、`securityProfile`内でパラメータ`EncryptionAtHost`を**true**として割り当てます。

4. VMまたはテンプレート仕様のいずれかを選択して、マシンプロファイルワークフローでMCSマシンカタログを作成します。

   - OSディスク/データディスク：顧客管理キーとプラットフォーム管理キーを介して暗号化されます
   - エフェメラルOSディスク：プラットフォーム管理キーのみを介して暗号化されます
   - キャッシュディスク: 顧客管理キーとプラットフォーム管理キーによって暗号化されます

   Web StudioまたはPowerShellコマンドを実行して、マシンカタログを作成できます。

マシンプロファイルからホストでの暗号化情報を取得する

`AdditionalData`パラメータを指定してPowerShellコマンドを実行すると、マシンプロファイルからホストでの暗号化情報を取得できます。`EncryptionAtHost`パラメータが**True**の場合、マシンプロファイルでホストでの暗号化が有効になっていることを示します。

例: マシンプロファイルの入力がVMの場合、次のコマンドを実行します。

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def.v
m).AdditionalData
```

例: マシンプロファイルの入力がテンプレート仕様の場合、次のコマンドを実行します。

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def_t
emplatespec.templatespec\EncryptionAtHost.templatespecversion).AdditionalD
ata
```

マネージドディスクの二重暗号化

二重暗号化を使用してマシンカタログを作成できます。この機能で作成されたカタログはすべて、プラットフォームキーと顧客管理キーの両方でサーバー側で暗号化されます。Azure Key Vault、暗号化キー、およびディスク暗号化セット（DES）は、お客様が所有および保守します。

二重暗号化は、プラットフォーム側暗号化（デフォルト）と顧客管理暗号化（CMEK）です。したがって、暗号化アルゴリズム、実装、または侵害されたキーに関連するリスクを懸念するセキュリティに敏感な顧客である場合は、この二重暗号化を選択できます。永続的なOSディスクとデータディスク、スナップショット、およびイメージはすべて、二重暗号化によって保存時に暗号化されます。

注:

- Web StudioおよびPowerShellコマンドを使用して、二重暗号化されたマシンカタログを作成および更新できます。PowerShellコマンドについては、二重暗号化されたマシンカタログの作成を参照してください。
- 二重暗号化を使用してマシンカタログを作成または更新するには、マシンプロファイルに基づかないワークフローまたはマシンプロファイルに基づくワークフローを使用できます。
- マシンプロファイルに基づかないワークフローを使用してマシンカタログを作成する場合、保存されている`DiskEncryptionSetId`を再利用できます。
- マシンプロファイルを使用する場合、VMまたはテンプレート仕様をマシンプロファイルの入力として使用できます。

制限事項:

- 二重暗号化は、Ultra Disks または Premium SSD v2 ディスクではサポートされていません。
- 二重暗号化は、アンマネージドディスクではサポートされていません。
- カタログに関連付けられているDiskEncryptionSetキーを無効にすると、そのカタログのVMも無効になります。
- お客様が管理するキー（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）に関連するすべてのリソースは、同じサブスクリプションおよびリージョンにある必要があります。
- サブスクリプションごとに、リージョンあたり最大50個のディスク暗号化セットしか作成できません。

Azureリソースグループ

Azureプロビジョニングリソースグループは、ユーザーにアプリケーションとデスクトップを提供するVMをプロビジョニングする方法を提供します。リソースグループを作成するか、既存のリ

ソースグループを使用して、MCSマシンカタログにVMをプロビジョニングできます。複数のマシンカタログで同じリソースグループを使用できます。Azureリソースグループの詳細については、Microsoftドキュメントを参照してください。

Azureリソースグループの使用法

Azureリソースグループあたりの仮想マシン、マネージドディスク、スナップショット、およびイメージの数に制限はありません。（Azureリソースグループあたり240個のVM、800個のマネージドディスクという制限は削除されました。）

- フルスコープのサービスプリンシパルを使用してマシンカタログを作成する場合、MCSは1つのAzureリソースグループのみを作成し、そのグループをカタログに使用します。
- ナロースコープのサービスプリンシパルを使用してマシンカタログを作成する場合、カタログ用に空の、事前に作成されたAzureリソースグループを提供する必要があります。

Azureエフェメラルディスク

Azure エフェメラルディスクを使用すると、キャッシュディスク、一時ディスク、またはNVMeディスクを再利用して、Azure対応仮想マシンのOSディスクを保存できます。この機能は、標準のHDDディスクよりも高性能なSSDディスクを必要とするAzure環境で役立ちます。Azureエフェメラルディスクを使用してカタログを作成する方法については、「Azureエフェメラルディスクを使用したカタログの作成」を参照してください。

> **注:**
>
> 永続カタログは、エフェメラルOSディスクをサポートしていません。

> エフェメラルOSディスクを使用するには、プロビジョニングスキームでマネージドディスクと共有イメージギャラリーを使用する必要があります。

エフェメラルOS一時ディスクを保存する

エフェメラルOSディスクをVMの一時ディスク、リソースディスク、またはNVMeディスクに保存するオプションがあります。この機能により、キャッシュがない、またはキャッシュが不十分なVMでエフェメラルOSディスクを使用できます。このようなVMには、エフェメラルOSディスクを保存するための一時ディスク、リソースディスク、またはNVMeディスクがあります（例：`Ddv4`）。

次の点を考慮してください。

- エフェメラルディスクは、VMのキャッシュディスク、VMの一時（リソース）ディスク、またはNVMeディスクに保存されます。キャッシュディスクがOSディスクの内容を保持するのに十分な大きさでない限り、一時ディスクよりもキャッシュディスクが優先されます。
- 更新の場合、キャッシュディスクより大きく、一時ディスクより小さい新しいイメージは、エフェメラルOSディスクをVMの一時ディスクに置き換えることになります。

AzureエフェメラルディスクとMachine Creation Services (MCS) ストレージ最適化 (MCS I/O)

AzureエフェメラルOSディスクとMCS I/Oは同時に有効にできません。

重要な考慮事項は次のとおりです。

- エフェメラルOSディスクとMCS I/Oの両方を同時に有効にしてマシンカタログを作成することはできません。
- PowerShellパラメーター（`UseWriteBackCache`および`UseEphemeralOsDisk`）を`New-ProvScheme`または`Set-ProvScheme`で**true**に設定すると、適切なエラーメッセージが表示されて失敗します。
- 両方の機能が有効になっている既存のマシンカタログの場合、引き続き次のことができます。
  - マシンカタログを更新する。
  - VMを追加または削除する。
  - マシンカタログを削除する。

アジュール コンピュート ギャラリー

Azure Compute Gallery (旧称 Azure Shared Image Gallery) を、Azure で MCS プロビジョニングされたマシンの公開イメージリポジトリとして使用します。公開イメージをギャラリーに保存することで、OSディスクの作成とハイドレーションを高速化し、非永続VMの起動時間とアプリケーション起動時間を改善できます。共有イメージギャラリーには、次の3つの要素が含まれています。

- *ギャラリー*: イメージはここに保存されます。MCS は、各マシンカタログに対して1つのギャラリーを作成します。
- *ギャラリーイメージ定義*: この定義には、公開イメージに関する情報 (オペレーティングシステムの種類と状態、Azure リージョン) が含まれます。MCS は、カタログ用に作成された各イメージに対して1つのイメージ定義を作成します。
- *ギャラリーイメージバージョン*: 共有イメージギャラリー内の各イメージは複数のバージョンを持つことができ、各バージョンは異なるリージョンに複数のレプリカを持つことができます。各レプリカは、公開イメージの完全なコピーです。

注:

共有イメージギャラリー機能は、マネージドディスクとのみ互換性があります。レガシーマシンカタログでは使用できません。

詳細については、Azure Compute Galleryの概要を参照してください。

PowerShell を使用して Azure Compute Gallery イメージでマシンカタログを作成または更新する方法については、「Azure Compute Gallery イメージを使用してマシンカタログを作成または更新する」を参照してください。

Azure 機密 VM

Azure 機密コンピューティング VM は、仮想デスクトップがメモリ内で暗号化され、使用中に保護されることを保証します。

MCS を使用して、Azure 機密 VM を含むカタログを作成できます。このようなカタログを作成するには、マシンプロファイルワークフローを使用する必要があります。VM と ARM テンプレート仕様の両方をマシンプロファイルの入力として使用できます。

機密 VM タイプの Azure マスターイメージと機密 VM タイプの Azure マシンプロファイルを使用して準備済みイメージを作成し、この準備済みイメージを使用して MCS カタログを作成することもできます。

機密 VM に関する重要な考慮事項

サポートされている VM サイズと機密 VM を使用したマシンカタログの作成に関する重要な考慮事項は次のとおりです。

- 機密 VM でサポートされている VM サイズを確認するには、「サイズ」を参照してください。
- 機密 VM を使用してマシンカタログを作成します。
  - Web Studio および PowerShell コマンドを使用して、Azure 機密 VM を含むマシンカタログを作成できます。
  - Azure 機密 VM を含むマシンカタログを作成するには、マシンプロファイルベースのワークフローを使用する必要があります。VM またはテンプレート仕様をマシンプロファイルの入力として使用できます。

- マスターイメージとマシンプロファイルの入力は、両方とも同じ機密セキュリティタイプで有効にする必要があります。Azure のリソースによって、機密 VM タイプを示すラベルが異なります。

  Azure スナップショット、マネージドディスク、または仮想マシンのセキュリティタイプは次のとおりです。

  - ConfidentialVM_DiskEncryptedWithCustomerKey。
  - ConfidentialVM_DiskEncryptedWithPlatformKey。
  - ConfidentialVM_VMGuestStateOnlyEncryptedWithPlatformKey

  Azure ARM テンプレート仕様バージョンのセキュリティタイプは次のとおりです。

  - VMGuestStateOnly: VM ゲストの状態のみが暗号化された機密 VM
  - DiskWithVMGuestState: OSディスクとVMゲスト状態の両方がプラットフォーム管理キーまたは顧客管理キーで暗号化された機密VM。通常OSディスクとエフェメラルOSディスクの両方を暗号化できます。

- AdditionalDataパラメーターを使用して、マネージドディスク、スナップショット、Azure Compute Galleryイメージ、VM、ARMテンプレート仕様など、さまざまなリソースタイプの機密VM情報を取得できます。例：

  ```
  PS C:\Users\username> (get-item XDHyp:
  \HostingUnits\mynetwork\image.folder\username-dev-testing-
  rg.resourcegroup\username-dev-tsvda.vm).AdditionalData
  ```

  追加データフィールドは次のとおりです。

- DiskSecurityType
- ConfidentialVMDiskEncryptionSetId
- DiskSecurityProfiles

  マシンサイズの機密コンピューティングプロパティを取得するには、次のコマンドを実行します: `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

  追加データフィールドは`ConfidentialComputingType`です。

- マスターイメージまたはマシンプロファイルを、機密から非機密のセキュリティタイプへ、または非機密から機密のセキュリティタイプへ変更することはできません。

- 誤った構成に対しては、適切なエラーメッセージが表示されます。

マスターイメージとマシンプロファイルの準備

機密VMのセットを作成する前に、以下の手順に従ってマスターイメージとマシンプロファイルを準備してください。

1. Azureポータルで、次のような特定の構成で機密VMを作成します。
   - **セキュリティの種類**: 機密仮想マシン
   - **機密OSディスク暗号化**: 有効。
   - **キー管理**：プラットフォーム管理キーによる機密ディスク暗号化 機密VMの作成に関する詳細については、こちらのMicrosoft記事を参照してください。
2. 作成したVMでマスターイメージを準備します。作成したVMに必要なアプリケーションとVDAをインストールします。

   > **注:**
   >
   > VHDを使用した機密VMの作成はサポートされていません。代わりに、Azure Compute Gallery、マネージドディスク、またはスナップショットを使用してください。

3. 以下のいずれかの方法でマシンプロファイルを作成します。
   - 必要なマシンプロパティを備えている場合は、ステップ1で作成した既存のVMを使用します。
   - マシンプロファイルとしてARMテンプレート仕様を選択する場合は、必要に応じてテンプレート仕様を作成します。特に、*SecurityEncryptionType*や*diskEncryptionSet*（顧客管理キーの場合）など、機密VMの要件を満たすパラメーターを構成します。詳細については、(#create-an-azure-template-spec)を参照してください。

     > **注:**
     >
     > - マスターイメージとマシンプロファイルが同じセキュリティキータイプであることを確認してください。

> - 顧客管理キーによる機密OSディスク暗号化を必要とする機密VMを作成するには、マスターイメージとマシンプロファイルの両方でディスク暗号化セットIDが同じであることを確認してください。

機密VMタイプの準備済みイメージを使用してMCSカタログを作成する場合は、機密VMタイプのマスターイメージと機密VMタイプのマシンプロファイルを使用して準備済みイメージを作成します。準備済みイメージの作成については、(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/create-prepared-image-machine-catalogs-azure#create-an-image-definition-and-initial-image-version)を参照してください。

Web StudioまたはPowerShellコマンドを使用して機密VMを作成する

機密VMのセットを作成するには、マスターイメージと、目的の機密VMから派生したマシンプロファイルを使用してマシンカタログを作成します。

Web Studioを使用してカタログを作成するには、(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create)に記載されている手順に従ってください。以下の考慮事項に留意してください。

- 「**イメージ**」ページで、機密VM作成用に準備したマスターイメージとマシンプロファイルを選択します。マシンプロファイルの選択は必須であり、選択したマスターイメージと同じセキュリティ暗号化タイプに一致するプロファイルのみが選択可能です。
- 「**仮想マシン**」ページでは、機密VMをサポートするマシンサイズのみが選択肢として表示されます。
- 「**ディスク設定**」ページでは、選択したマシンプロファイルから継承されるため、ディスク暗号化セットを指定することはできません。

起動整合性監視

VMでセキュアブートと仮想トラステッドプラットフォームモジュール (vTPM) が有効になっており、`GuestAttestation`拡張機能がインストールされている場合、Microsoft Defender for CloudはVMが正常に起動することをリモートで検証できます。この監視は**起動整合性監視**と呼ばれます。起動整合性監視の詳細については、「起動整合性監視の概要」を参照してください。

マシンプロファイル（VMまたはテンプレート仕様）を使用して、MCSマシンカタログVM（永続VMおよび非永続VM）の起動整合性監視を有効にできます。起動整合性監視は、信頼できる起動と機密VMでのみサポートされています。

既存のカタログを更新して、`Set-ProvScheme`を使用して起動整合性対応マシンプロファイルを指すようにすることで、起動整合性を使用できます。カタログに追加された新しいVMは、整合性監視が有効になります。

また、`Set-ProvVmUpdateTimeWindow`、`Set-ProvVm`、または`Maintenance Cycles`を使用して、カタログ内の既存のVMを更新することもできます。以下を変換できます。

- 整合性監視なしの VM を整合性監視ありに
- 整合性監視ありの VM を整合性監視なしに

整合性監視が有効なマシンカタログを作成する

必要な権限:

次の権限があることを確認してください。

- `Microsoft.Compute/virtualMachines/extensions/read`
- `Microsoft.Compute/virtualMachines/extensions/write`

整合性監視が有効なMCSマシンカタログを作成するには、次の手順を実行します。

1. `GuestAttestation` 拡張機能がインストールされたマシンプロファイル (VM またはテンプレート仕様) を作成します。(以下のコンテンツへのリンク)
2. Web Studio または PowerShell コマンドを使用して、マシンプロファイル入力を利用して MCS マシンカタログを作成します。

   > **注:**
   >
   > `Get-Item` PowerShell コマンドを `AdditionalData` パラメーターとともに使用して、VM またはテンプレート仕様の `GuestAttestationExtensionEnabled` ステータスを確認できます。

3. カタログにVMを追加します。

GUESTATTESTATION拡張機能がインストールされ、有効化されたマシンプロファイルを作成する

整合性監視が有効なマシンプロファイル入力としてVMまたはテンプレート仕様を作成します。これはGuestAttestation拡張機能がインストールされていることを意味します。

整合性監視が有効なVMを作成するには、以下を実行します:

1. Azureポータルにサインインします。

2. 新しいVMを作成する場合は、次の手順を実行します。

   a. **セキュリティの種類**として**信頼された起動仮想マシン**または**機密仮想マシン**を選択します。

   b. **セキュリティ機能の構成**をクリックし、**整合性監視**チェックボックスを選択します。

   > **注:**
   >
   > 整合性監視には、セキュアブートと vTPM を有効にする必要があります。

3. **概要**ページで、**セキュリティの種類**セクションに移動し、**セキュリティの種類**が**信頼された起動**または**機密仮想マシン**であり、**整合性監視**が有効になっていることを確認します。
4. `GuestAttestation`がインストールされていることを確認するには、 **ページ**に移動します。

既存のVMの整合性監視を有効にするには、「整合性監視を有効にする - Azure portal」を参照してください。

`GuestAttestation`拡張機能がインストールされたテンプレート仕様を作成するには:

- テンプレート仕様を使用してGuestAttestationをインストールできます。「整合性監視を有効にする - テンプレート仕様」を参照してください。

  > **注記：**
  >
  > このテンプレート仕様の****で、アテステーションに使用するエンドポイントを構成できます。構成しない場合、Azureが構成するエンドポイントを決定します。

Azure Marketplace (アジュール マーケットプレイス)

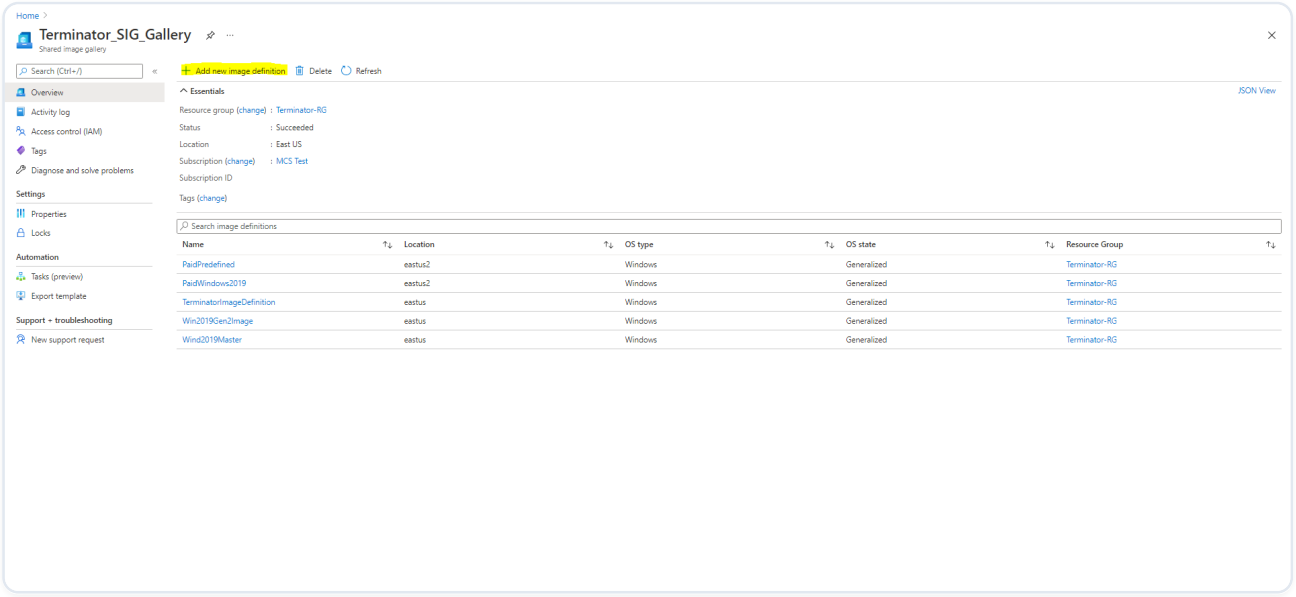
Citrix Virtual Apps and Desktops は、プラン情報を含むAzure上のマスターイメージを使用してマシンカタログを作成することをサポートしています。詳細については、「Microsoft Azure Marketplace」を参照してください。

> **ヒント:**

> 標準のWindows Serverイメージなど、Azure Marketplaceで見つかる一部のイメージには、プラン情報が追加されていません。Citrix Virtual Apps and Desktops の機能は、有料イメージ向けです。

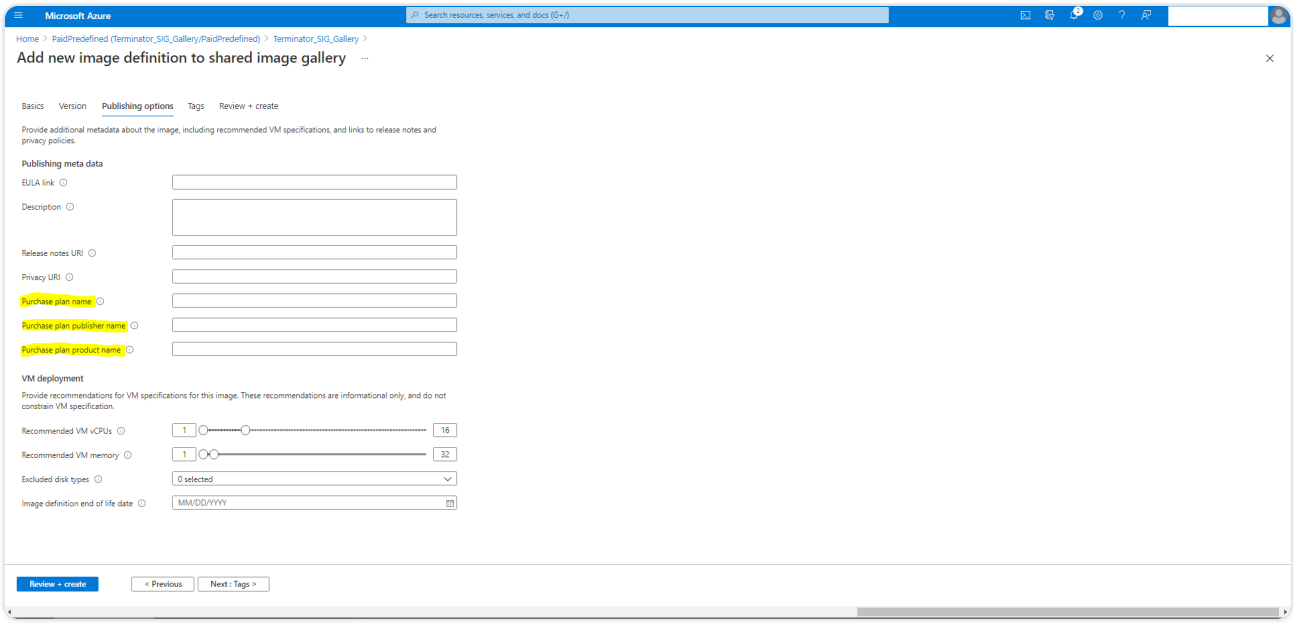
Shared Image Gallery で作成されたイメージに Azure プラン情報が含まれていることを確認します

このセクションの手順を使用して、Web Studio で Shared Image Gallery のイメージを表示します。これらのイメージは、オプションでマスターイメージとして使用できます。イメージを Shared Image Gallery に配置するには、ギャラリーでイメージ定義を作成します。

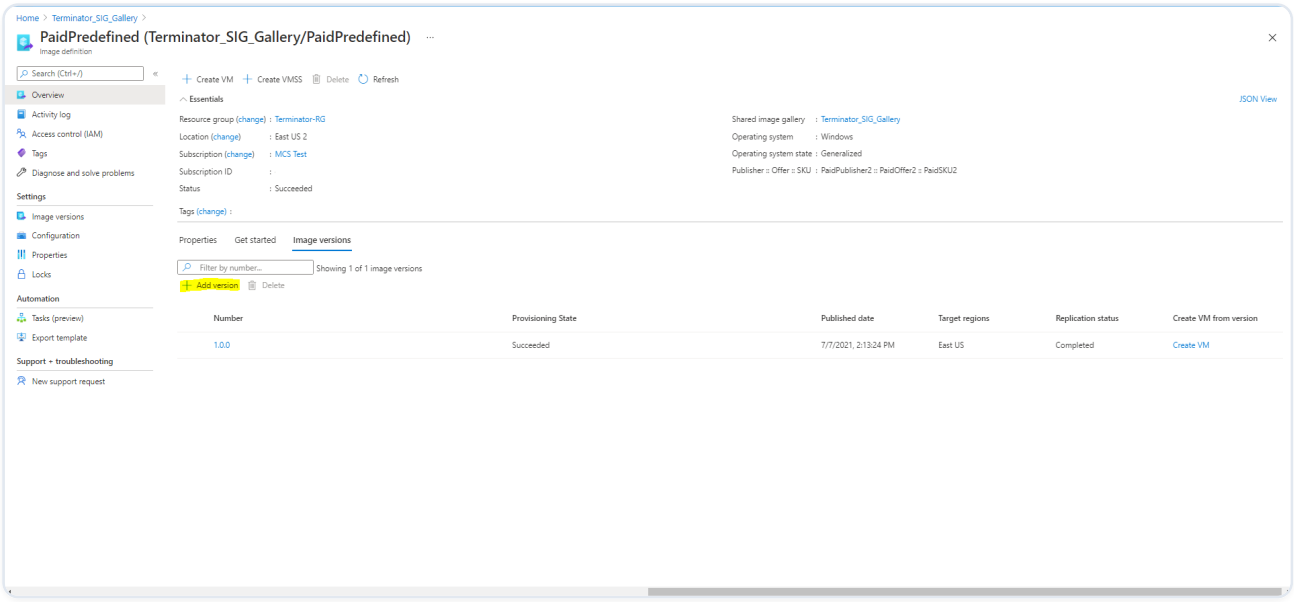


ページで、購入プラン情報を確認します。

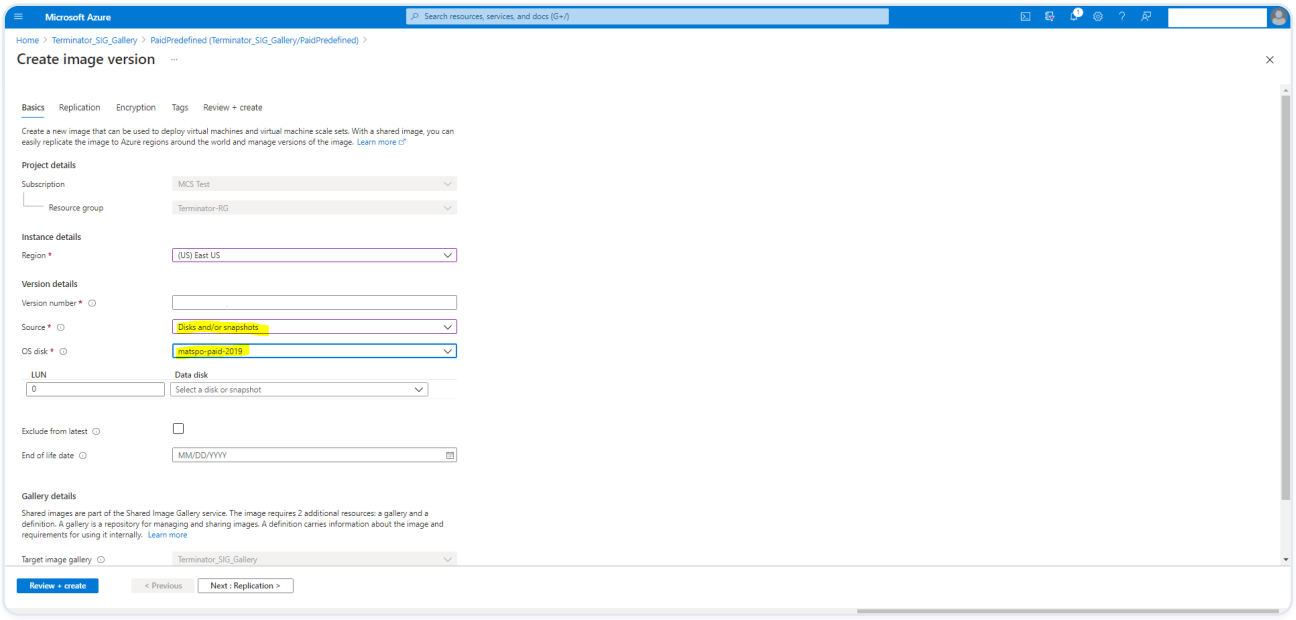
購入プラン情報フィールドは最初は空です。これらのフィールドに、イメージに使用された購入プラン情報を入力します。購入プラン情報を入力しないと、マシンカタログのプロセスが失敗する可能性があります。



購入プラン情報を確認後、定義内にイメージバージョンを作成します。これはマスターイメージとして使用されます。 をクリックします。



セクションで、イメージスナップショットまたはマネージドディスクをソースとして選択します。



オンデマンド容量予約VMのカタログを作成する

オンデマンド容量予約を使用すると、Azureリージョンまたは可用性ゾーンで任意の期間、コンピューティング容量を予約できます。Azureオンデマンド容量予約の詳細については、Microsoftドキュメント「オンデマンド容量予約」を参照してください。

マシンプロファイル（VMまたはテンプレート仕様）を使用して、オンデマンド容量予約付きのAzure VMのMCSマシンカタログを作成できます。また、既存のマシンカタログと既存のVMを更新して、オンデマンド容量予約を追加または削除することもできます。

この機能は、永続的および非永続的なマシンカタログに適用されます。

制限事項

この機能は以下には適用されません:

- スポットVM
- ホストグループ
- 休止状態が有効なVM

制限の詳細については、Microsoft ドキュメントの「制限事項」を参照してください。

オンデマンド容量予約VMのカタログを作成する手順

1. マシンプロファイルソース（VMまたはARMテンプレート仕様）を作成します。VMまたはARMテンプレート仕様の作成については、「VMを容量予約グループに関連付ける」を参照してください。

2. 次のPowerShellコマンドを実行して、マシンプロファイルでオンデマンド容量予約が有効になっているかどうかを確認します。マシンプロファイルでオンデマンド容量予約が有効になっている場合、`capacityReservationGroup id`が表示されます。

   例：

   マシンプロファイルソースがVMの場合、次のコマンドを実行します。

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-
   conn2\machineprofile.folder\fifthcolumn.resourcegroup\demand-
   capacity.vm").AdditionalData
   ```

   マシンプロファイルソースがテンプレート仕様の場合、次のコマンドを実行します。

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-
   conn2\machineprofile.folder\fifthcolumn.resourcegroup\fc-aeh-
   templatespec.templatespec\14.0.0-capacity-
   reservation.templatespecversion").AdditionalData
   ```

3. Web StudioまたはPowerShellコマンドを使用して、マシンプロファイルを使用してマシンカタログを作成します。

`Set-ProvScheme`コマンドを使用してカタログを更新できます。また、PowerShellコマンド`Set-ProvVmUpdateTimeWindow`を使用して既存のVMを更新することもできます。マシンプロファイルは次回の電源投入時に更新されます。

ネストされた仮想化

マスターVMをネストされた仮想化が有効になるように構成すると、そのマスターVMを使用して作成されたMCSマシンカタログ内のすべてのVMでネストされた仮想化が有効になります。この機能は、永続VMと非永続VMの両方に適用されます。既存のMCSマシンカタログと既存のVMを、イメージの更新を通じてネストされた仮想化を有効にするように更新できます。

現在、Dv3およびEv3 VMサイズのみがネストされた仮想化をサポートしています。

ネストされた仮想化の詳細については、Microsoftのブログ「Azureにおけるネストされた仮想化」を参照してください。

NVMeのみのSKU

通常、汎用、メモリ最適化、およびコンピューティング最適化VMの古い世代（D/Ev5およびそれ以前）はSCSIをサポートしています。新しい世代（Da/Ea/Fav6およびそれ以降）は通常、NVMeストレージインターフェイスのみをサポートしています。MCSは、Azure上の新しいVM SKUをサポートするためにNVMeストレージコントローラータイプをサポートしています。

NVMeの詳細については、Microsoftのドキュメント「NVMeに関する一般的なFAQ」を参照してください。

次のサービスオファリングを使用して MCS カタログを作成できます。

- SCSIとNVMeの両方をサポートしている場合、(#create-a-catalog-using-a-service-offering-that-supports-both-scsi-and-nvme)を参照してください。
- NVMeのみをサポートしている場合、(#create-a-catalog-using-a-service-offering-that-supports-only-nvme)を参照してください。

制限事項

- NVMeをサポートするすべてのサービスオファリングが、同時にTrusted Launchをサポートするわけではありません。
- NVMeはGen 1 VMではサポートされていません。
- 一部のOSイメージはNVMeをサポートしていない場合があります。その場合、Azure UIでNVMeオプションはグレー表示されます。

SCSI と NVMe の両方をサポートするサービスオファリングを使用してカタログを作成する

1. マスターイメージとして使用する VM を作成します。

   a. NVMeをサポートするマーケットプレイスイメージを使用します。NVMeをサポートするAzure Marketplaceイメージのリストは、リモート NVMe 用のサポートされている OS イメージで確認できます。

   b. VMのOSディスクのスナップショットを取得し、`New-ProvScheme`コマンドの`MasterImageVM`パラメーターで使用するか、マネージドディスクを直接使用します。

      マスターイメージがNVMeをサポートしているかどうかを、以下のいずれかの方法で確認します。

      - `Get-Item`の`AdditionalData`フィールドにある`SupportedDiskControllerTypes`を確認します。例:

```
(get-item XDHyp:
\HostingUnits\mynetwork\image.folder\abc.resourcegroup\deg-
snapshot).AdditionalData
```

`SupportedDiskControllerTypes`は`SCSI, NVMe`である必要があります。

- Azure CLIとPowerShellを使用する

2. NVMeとSCSIの両方をサポートするサービスオファリングを使用します。
3. NVMeが有効になっているマシンプロファイルとしてVMまたはテンプレート仕様を使用します。`DiskControllerType`がNVMeに設定されている任意のVMを使用します。VMを直接マシンプロファイルとして使用するか、テンプレートをエクスポートしてテンプレート仕様をマシンプロファイルとして使用します。

NVMeのみをサポートするサービスオファリングを使用してカタログを作成する

1. マスターイメージとして使用するVMを作成します。NVMeをサポートするマーケットプレイスイメージを使用します。NVMeをサポートするAzure Marketplaceイメージのリストは、リモートNVMeでサポートされるOSイメージで確認できます。
2. NVMeのみをサポートするサービスオファリングを使用します。

> **注:**
>
> サービスオファリングがNVMeをサポートしているため、カタログでNVMeを有効にするために`NVMe`に設定された`DiskControllerType`を持つマシンプロファイルは必要ありません。ただし、マシンプロファイルを使用する場合は、`DiskControllerType`が`NVMe`に設定されているか、空白であるか、指定されていない必要があります。

既存の永続VMを変更する

NVMe構成は、VMが作成された後に変更することはできません。永続VMのNVMe構成を変更する方法は、VMを再デプロイすることです。これを行うロジックは次のとおりです。

1. VMの現在の状態を保存します。
2. 既存のVMの電源をオンにした後、VMが再デプロイを必要とするかどうかを検出します。
   a. 構成の変更がNVMeからNVMe、またはSCSIからSCSIである場合、VMの再展開は不要です。
   b. 構成の変更がSCSIからNVMe、またはその逆である場合、VMを再展開して再作成します。

PowerShellを使用してマシンカタログを作成する

このセクションでは、PowerShell を使用してカタログを作成する方法について詳しく説明します。

- 非永続的なライトバックキャッシュディスクを持つカタログを作成する
- 永続的なライトバックキャッシュディスクを持つカタログを作成する
- MCSIOで起動パフォーマンスを向上させる
- PowerShellを使用してカタログを作成または更新する際にテンプレート仕様を使用する
- 信頼された起動機能を持つマシンカタログ
- マシンプロファイルプロパティ値を使用する
- 顧客管理の暗号化キーを使用してマシンカタログを作成する
- 二重暗号化を使用してマシンカタログを作成する
- Azureエフェメラルディスクを持つカタログを作成する
- Azure専用ホスト
- Azure Compute Galleryイメージを使用してマシンカタログを作成または更新する
- 共有イメージギャラリーを構成する
- 指定された可用性ゾーンにマシンをプロビジョニングする
- ストレージの種類
- Azure Spot VMを使用してカタログを作成する(#create-a-catalog-using-azure-spot-vms)
- バックアップVMサイズを構成する
- すべてのリソースのタグをコピーする
- Azure Monitor Agentがインストールされたカタログ VMのプロビジョニング(#provision-catalog-vms-with-azure-monitor-agent-installed)

非永続的なライトバックキャッシュディスクを持つカタログの作成

非永続的なライトバックキャッシュディスクを持つカタログを構成するには、PowerShellパラメーター`New-ProvScheme CustomProperties`を使用します。カスタムプロパティ`UseTempDiskForWBC`は、ライトバックキャッシュファイルを保存するためにAzureの一時ストレージを使用することを受け入れるかどうかを示します。一時ディスクをライトバックキャッシュディスクとして使用する場合は、`New-ProvScheme`を実行するときにこれをtrueに構成する必要があります。このプロパティが指定されていない場合、パラメーターはデフォルトで**False**に設定されます。

例えば、`CustomProperties`パラメーターを使用して`UseTempDiskForWBC`を**true**に設定する場合：

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="true"/
> `

</CustomProperties>'
```

注:

ライトバックキャッシュファイルにAzureローカル一時ストレージを使用するようにマシンカタログをコミットした後、後でVHDを使用するように変更することはできません。

永続的なライトバックキャッシュディスクを持つカタログを作成する

永続的なライトバックキャッシュディスクを持つカタログを構成するには、PowerShellパラメーター`New-ProvScheme CustomProperties`を使用します。このパラメーターは、MCSプロビジョニングされたマシンに対してライトバックキャッシュディスクがどのように永続化するかを決定するために使用される追加のプロパティ`PersistWBC`をサポートします。`PersistWBC`プロパ

ティは、`UseWriteBackCache`パラメーターが指定され、`WriteBackCacheDiskSize`パラメーターがディスクが作成されることを示すように設定されている場合にのみ使用されます。

`PersistWBC`をサポートする前の`CustomProperties`パラメーターで見つかったプロパティの例は次のとおりです。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

</CustomProperties>
```

これらのプロパティを使用する場合、`CustomProperties`パラメーターからプロパティが省略されていると、それらはデフォルト値を含むことに注意してください。`PersistWBC`プロパティには、**true**または**false**の2つの可能な値があります。

`PersistWBC`プロパティを**true**に設定すると、Citrix Virtual Apps and Desktops管理者がWeb Studioを使用してマシンをシャットダウンしても、ライトバックキャッシュディスクは削除されません。

`PersistWBC`プロパティを**false**に設定すると、Citrix Virtual Apps and Desktops管理者がWeb Studioを使用してマシンをシャットダウンしたときに、ライトバックキャッシュディスクが削除されます。

注:

`PersistWBC`プロパティが省略された場合、プロパティはデフォルトで**false**になり、Web Studioを使用してマシンがシャットダウンされるとライトバックキャッシュは削除されます。

例えば、`CustomProperties`パラメータを使用して`PersistWBC`をtrueに設定するには：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

重要:

`PersistWBC`プロパティは、`New-ProvScheme` PowerShellコマンドレットを使用してのみ設定できます。プロビジョニングスキームの`CustomProperties`を作成後に変更しようとしても、マシンカタログには影響せず、マシンがシャットダウンされた場合の書き込みキャッシュディスクの永続性にも影響しません。

例えば、`New-ProvScheme`を書き込みキャッシュを使用するように設定し、`PersistWBC`プロパティをtrueに設定します：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"
```

```
-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

MCSIOで起動パフォーマンスを向上させる

MCSIOが有効になっている場合、AzureおよびGCPマネージドディスクの起動パフォーマンスを向上させることができます。この機能を構成するには、`New-ProvScheme`コマンドでPowerShell `PersistOSDisk`カスタムプロパティを使用します。`New-ProvScheme`に関連するオプションは次のとおりです：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->

````````Groups" Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />
```
```

```
</CustomProperties>
```

この機能を有効にするには、`PersistOSDisk`カスタムプロパティを`true`に設定します。例：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

PowerShell を使用してカタログを作成または更新する際にテンプレート仕様を使用する

テンプレート仕様をマシンプロファイルの入力として使用して、MCSマシンカタログを作成または更新できます。これを行うには、Web StudioまたはPowerShellコマンドを使用できます。

Web Studioについては、「Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する」を参照してください。(#create-a-machine-catalog-using-an-azure-resource-manager-image-in-web-studio)

PowerShell コマンドを使用する手順:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*` を実行します。
3. カタログを作成または更新します。
    - カタログを作成するには:
        a. テンプレート仕様をマシンプロファイルの入力として使用して、`New-ProvScheme` コマンドを使用します。例:

```
New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
image.folder/fgthj.resourcegroup/nab-ws-
vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>

[-LoggingId <Guid>]

[-BearerToken <String>][-AdminAddress <String>]

[<CommonParameters>]
```

        b. カタログの作成を完了します。

- カタログを更新するには、テンプレート仕様をマシンプロファイルの入力として使用して、`Set-ProvScheme`コマンドを使用します。例:

```
Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
Us.region/vm.folder/MasterDisk.vm'

MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/testing.templatespec/V1.templatespecversion'

[-ProvisioningSchemeName] <String>

[-CustomProperties <String>][-ServiceOffering <String>] [-PassThru]

[-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <String>]
[<CommonParameters>]
```

Trusted Launch を使用したマシンカタログ

Trusted Launch を使用してマシンカタログを正常に作成するには、以下を使用します。

- Trusted Launch が有効なマスターイメージ。マシンプロファイルを使用する必要がありますが、マシンプロファイルが Trusted Launch 対応である必要はありません。Trusted Launch が有効なマスターイメージと Trusted Launch が有効でないマシンプロファイルを使用すると、マスターイメージとマシンプロファイルの Trusted Launch 構成が一致しないため、警告メッセージが表示されます。
- Trusted Launch をサポートする VM サイズ
- Trusted Launch をサポートする Windows VM バージョン。現在、Windows 10、Windows 11、Windows Server 2016、2019、および 2022 が Trusted Launch をサポートしています。

Citrix Virtual Apps and Desktops の提供インベントリアイテムを表示し、VM サイズが Trusted Launch をサポートしているかどうかを判断するには、次のコマンドを実行します。

1. PowerShell ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、**asnp citrix*** を実行します。
3. 次のコマンドを実行します。

```
$s = (ls XDHyp:\HostingUnits\<name of hosting
unit>\serviceoffering.folder\"<VM size>.serviceoffering)
```

4. `$s | select -ExpandProperty Additionaldata` を実行します。

5. `SupportsTrustedLaunch` 属性の値を確認します。
    - `SupportsTrustedLaunch` が**True**の場合、VMサイズはTrusted Launchをサポートしています。
    - `SupportsTrustedLaunch` が**False**の場合、VMサイズはTrusted Launchをサポートしていません。

Azure の PowerShell に従い、Trusted Launch をサポートする VM サイズを判別するには、次のコマンドを使用できます。

```
(Get-AzComputeResourceSku | where {$_.Locations.Contains($region) -and
($_.Name -eq "<VM size>") })[0].Capabilities
```

Azure PowerShell コマンドの実行後に、VM サイズが Trusted Launch をサポートするかどうかを説明する例を次に示します。

- *例 1*: Azure VM が第 1 世代のみをサポートしている場合、その VM は Trusted Launch をサポートしません。したがって、Azure PowerShell コマンドの実行後も `TrustedLaunchDisabled` 機能は表示されません。
- *例 2*: Azure VM が第 2 世代のみをサポートし、`TrustedLaunchDisabled` 機能が **True** の場合、第 2 世代の VM サイズは Trusted Launch でサポートされません。
- *例 3*: Azure VM が第 2 世代のみをサポートし、PowerShell コマンドの実行後に `TrustedLaunchDisabled` 機能が表示されない場合、第 2 世代の VM サイズは Trusted Launch でサポートされます。

Azure 仮想マシンの Trusted Launch の詳細については、Microsoft ドキュメント「Trusted Launch for Azure virtual machines」を参照してください。

Trusted Launch を使用してマシンカタログを作成する

1. Trusted Launch が有効なマスターイメージを作成します。Microsoft ドキュメント「Trusted Launch VM Images」を参照してください。
2. セキュリティの種類を **trusted launch virtual machines** として VM またはテンプレート仕様を作成します。VM またはテンプレート仕様の作成の詳細については、Microsoft ドキュメント「Deploy a trusted launch VM」を参照してください。
3. Web Studio または PowerShell コマンドを使用してマシンカタログを作成します。
    - Web Studio を使用する場合は、「Web Studio で Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

- PowerShell コマンドを使用する場合は、VM またはテンプレート仕様をマシンプロファイルの入力として `New-ProvScheme` コマンドを使用します。カタログを作成するためのコマンドの完全なリストについては、「カタログの作成」を参照してください。

  VM をマシンプロファイルの入力とする `New-ProvScheme` の例:

  ```
  New-ProvScheme -CleanOnBoot -HostingUnitName "name"
  -IdentityPoolName "name" -InitialBatchSizeHint 1

  -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
  fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

  -MachineProfile "XDHyp:
  \HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<mac
  hine profile vm.vm>"

  -ProvisioningSchemeName <String>

  -HostingUnitName <String>

  -IdentityPoolName <String>

  [-ServiceOffering <String>][-CustomProperties <String>]

  [<CommonParameters>]
  ```

  `New-ProvScheme` をマシンプロファイル入力として使用したテンプレート仕様の例:

  ```
  New-ProvScheme -CleanOnBoot -HostingUnitName "name"
  -IdentityPoolName "name" -InitialBatchSizeHint 1

  -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
  fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

  MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
  fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

  -ProvisioningSchemeName <String>

  -HostingUnitName <String>

  -IdentityPoolName <String>
  ```

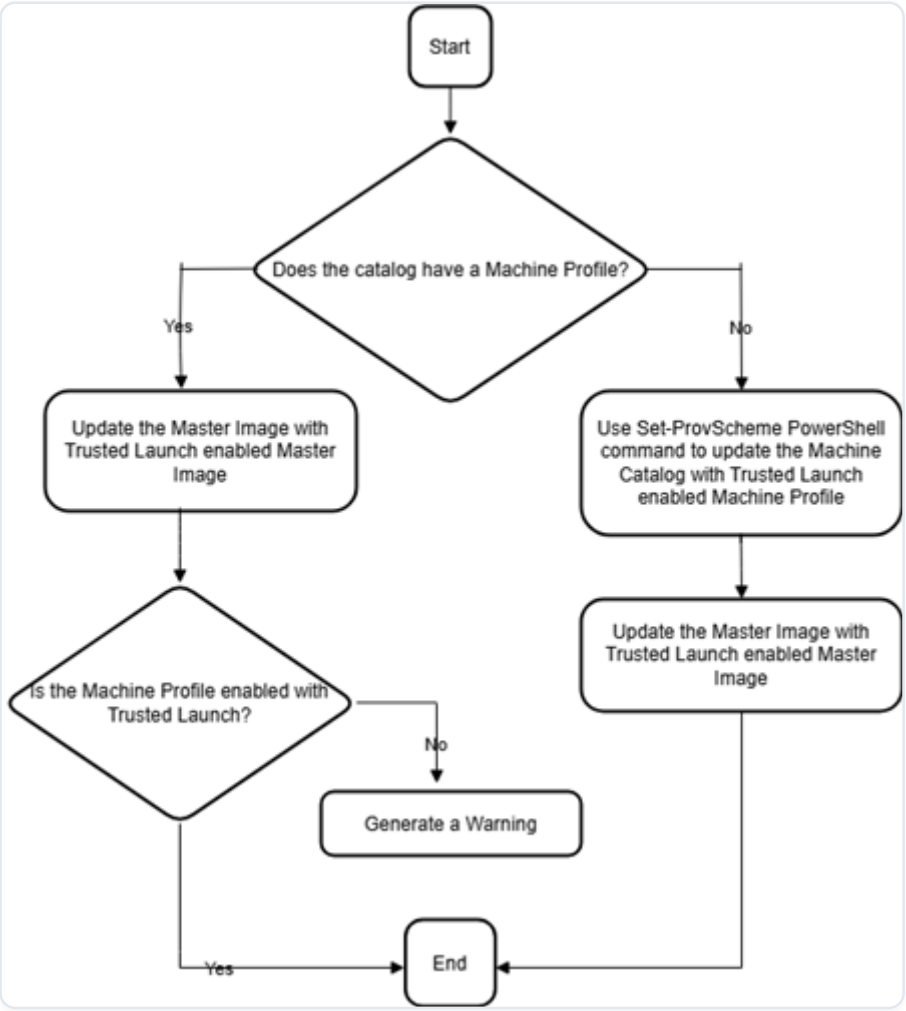
```
[-ServiceOffering <String>][-CustomProperties <String>]

[<CommonParameters>]
```

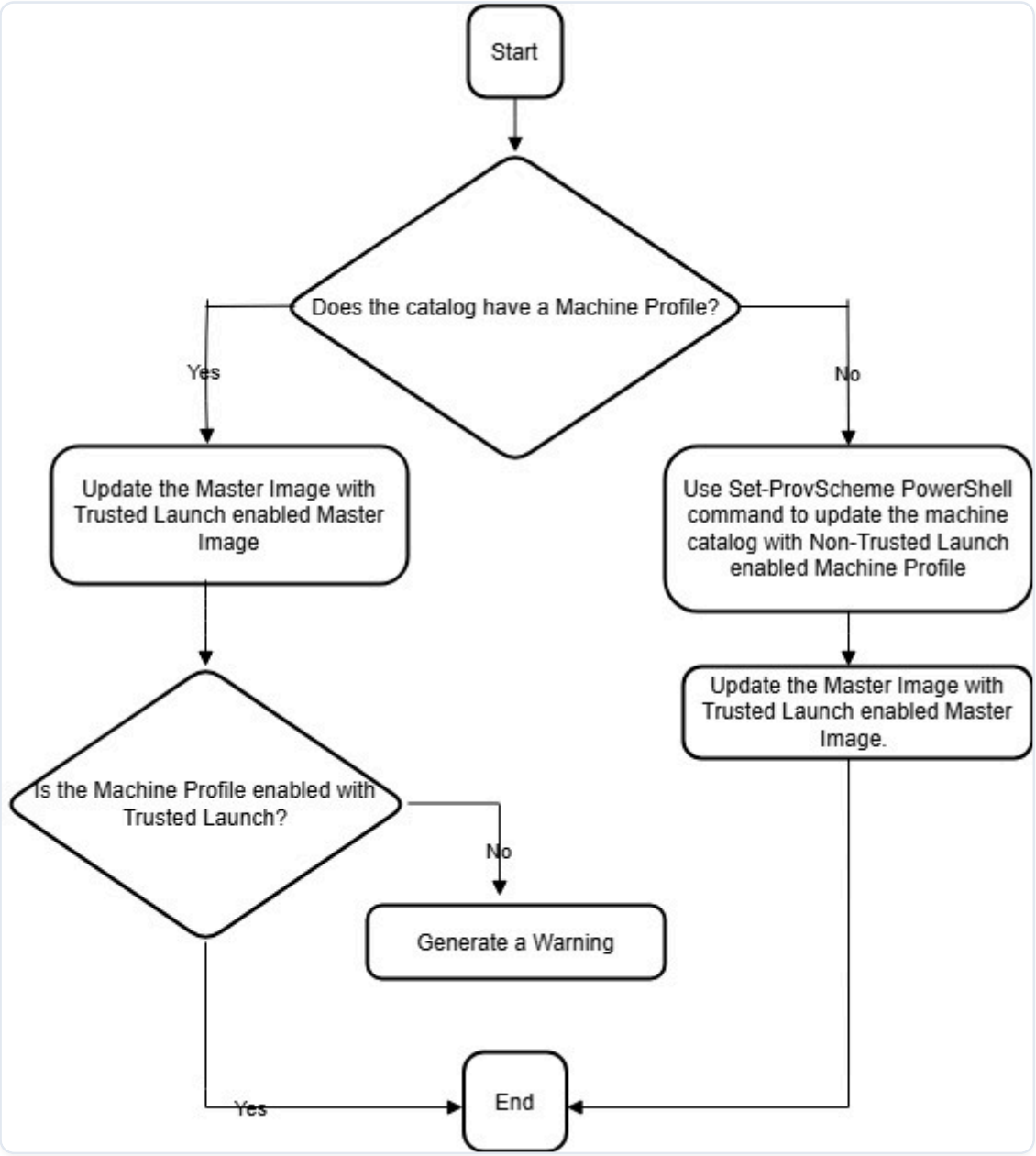
トラステッド起動でマシンカタログを更新する

永続および非永続の両方のマシンカタログを更新できます。

永続マシンカタログの場合:



非永続マシンカタログの場合:



トラステッド起動でマシンカタログを作成する際のエラー

トラステッド起動でマシンカタログを作成する際に、以下のシナリオで適切なエラーが発生します。

シナリオ	エラー
アンマネージドカタログの作成時にマシンプロファイルを選択した場合	`MachineProfileNotSupportedForUnmanagedCatalog`
セキュリティの種類としてトラステッド起動を使用するマスターイメージソースでマネージドカタログを作成する際に、マシンプロファイルを選択しない場合	`MachineProfileNotFoundForTrustedLaunchMasterImage`

シナリオ	エラー
マスターイメージのセキュリティタイプとは異なるセキュリティタイプのマシンプロファイルを選択した場合	`SecurityTypeConflictBetweenMasterImageAndMachineProfile`
カタログ作成時に、Trusted Launchをサポートしないサイズを選択し、Trusted Launchをサポートするマスターイメージを使用した場合	`MachineSizeNotSupportTrustedLaunch`

マシンプロファイルプロパティ値の使用

マシンカタログは、カスタムプロパティで定義されている次のプロパティを使用します。

- アベイラビリティゾーン
- 専用ホストグループID
- ディスク暗号化セットID
- OSの種類
- ライセンスの種類
- ストレージの種類

これらのカスタムプロパティが明示的に定義されていない場合、プロパティ値は、マシンプロファイルとして使用されるARMテンプレート仕様またはVMから設定されます。さらに、`ServiceOffering`が指定されていない場合、マシンプロファイルから設定されます。

> **注:**
>
> マシンプロファイルに一部のプロパティが欠落しており、カスタムプロパティで定義されていない場合、該当する箇所ではプロパティのデフォルト値が適用されます。

> 次のセクションでは、`New-ProvScheme`と`Set-ProvScheme`におけるいくつかのシナリオについて説明します。この場合、`CustomProperties`はすべてのプロパティが定義されているか、値がMachineProfileから派生しています。

- New-ProvSchemeのシナリオ

- MachineProfileにすべてのプロパティがあり、CustomPropertiesが定義されていない場合。
  例:

  `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

  次の値がカタログのカスタムプロパティとして設定されます:

  ```
  Get-ProvScheme | select CustomProperties

  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance">

  <Property xsi:type="StringProperty" Name="StorageAccountType"
  Value="<mpA-value>"/>

  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
  value>"/>

  <Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
  value>"/>

  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
  Value="<mpA-value>"/>

  <Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
  Value="<mpA-value>"/>

  <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
  value>"/>

  </CustomProperties>
  ```

- MachineProfileに一部のプロパティがあり、CustomPropertiesが定義されていない場合。
  例: MachineProfileにはLicenseTypeとOsTypeのみがあります。

  `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

  次の値がカタログのカスタムプロパティとして設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
value>"/>

</CustomProperties>
```

- MachineProfileとCustomPropertiesの両方で、すべてのプロパティが定義されている場合。例:

  `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

  カスタムプロパティが優先されます。次の値がカタログのカスタムプロパティとして設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="<CustomPropertiesA-value>"/>
```

```
<Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones"
Value="<CustomPropertiesA-value>"/>

</CustomProperties>
```

- MachineProfileで一部のプロパティが定義され、CustomPropertiesで一部のプロパティが定義されている場合。例:
  - CustomPropertiesはLicenseTypeとStorageAccountTypeを定義します
  - MachineProfileはLicenseType、OsType、およびZonesを定義します

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
value>"/>

</CustomProperties>
```

- 一部のプロパティはMachineProfileで定義され、一部のプロパティはCustomPropertiesで定義されています。さらに、ServiceOfferingは定義されていません。例:
  - CustomProperties は StorageType を定義します
  - MachineProfile は LicenseType を定義します

```
New-ProvScheme -MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mp
.vm"

-ServiceOffering "XDHyp:
\HostingUnits\azureunit\serviceoffering.folder\<explicit-machine-
size>.serviceoffering"
```

カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<explicit-machine-size>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="explicit-storage-type"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="value-
from-machineprofile"/>

</CustomProperties>
```

- OsTypeがCustomPropertiesにもMachineProfileにもない場合、次のようになります:
  - 値はマスターイメージから読み取られます。
  - マスターイメージがアンマネージドディスクの場合、OsTypeはWindowsに設定されます。例:

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -MasterImageVM "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-image.manageddisk"`

マスターイメージからの値は、この場合Linuxとして、カスタムプロパティに書き込まれます。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="OSType" Value="Linux"/>

</CustomProperties>
```

- Set-ProvSchemeのシナリオ
  - 既存のカタログで、次のものを含む:
    - `StorageAccountType` と OSタイプ の カスタムプロパティ
    - ゾーンを定義するMachineProfile `mpA.vm`
  - 更新:
    - StorageAccountType を定義する MachineProfile mpB.vm
    - LicenseType と OsType を定義する新しいカスタムプロパティセット $CustomPropertiesB

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm" -CustomProperties $CustomPropertiesB`

以下の値がカタログのカスタムプロパティとして設定されます。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
```

```
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesB-value>"/>

    </CustomProperties>
```

- 既存のカタログで：
  - S`torageAccountType` と OsType の CustomProperties
  - StorageAccountType と LicenseType を定義する MachineProfile `mpA.vm`
- 更新：
  - StorageAccountType と OsType を定義する新しい一連のカスタムプロパティ $CustomPropertiesB。

`Set-ProvScheme -CustomProperties $CustomPropertiesB`

以下の値がカタログのカスタムプロパティとして設定されます。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mp-A-
value>"/>
```

```
</CustomProperties>
```

- 既存のカタログで：
  - `StorageAccountType` と OsType の CustomProperties
  - Zones を定義する MachineProfile `mpA.vm`
- 更新：
  - StorageAccountType と LicenseType を定義する MachineProfile mpB.vm
  - `ServiceOffering` は指定されていません

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm"`

カタログのカスタムプロパティとして、次の値が設定されます。

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<value-from-machineprofile>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<prior-
CustomProperties-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpB-
value>"/>

</CustomProperties>
```

VMごとに複数のNICを持つカタログを作成または更新する

MCS は、VM ごとに複数の NIC をサポートしています。VM 上の複数の NIC を複数のサブネットに関連付けることができますが、これらのサブネットは同じ仮想ネットワーク (VNet) 内にある必要があります。PowerShell コマンドを使用して、次の操作を実行できます。

- VM 上に複数の NIC を持つカタログを作成する
- 既存のカタログ構成を更新して、VM 上に複数の NIC を持たせ、新しく作成された VM が複数の NIC を持つようにする
- 既存の VM を更新して複数の NIC を持たせる

マシンプロファイルに基づかないマシンカタログと、マシンプロファイルに基づくマシンカタログを作成または更新して、VM 上に複数の NIC を持たせることができます。現在、マシンプロファイルに基づくマシンカタログの場合、マシンプロファイルソースで指定されているのと同じ数の NIC しか持つことができません。

アクセラレーテッドネットワーキングなどのプロパティは、マシンプロファイルソースから派生します。

> **注:**
>
> VM サイズは、同じ数の NIC と対応するアクセラレーテッドネットワーキングをサポートしている必要があります。そうでない場合、エラーが発生します。

> 選択した VM サイズに関連付けられている NIC の最大数を取得できます。PowerShell `get-item` コマンドを `AdditionalData` パラメーターとともに実行すると、`MaxNetworkInterfaces` と呼ばれる PowerShell プロパティに最大 NIC 数が表示されます。

NICの最大数を取得する

NICの最大数を取得するには：

1. Delivery Controller™ ホストから **PowerShell** ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために `asnp citrix*` を実行します。
3. 利用可能なすべてのVMサイズを一覧表示するために `Get-ChildItem -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder"` を実行します。

4. `get-item -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder\Standard_M416ms_v2.serviceoffering").AdditionalData` を実行します。
5. 最大NIC数を確認するために `MaxNetworkInterfaces` をチェックします。

仮想マシンに複数のNICを持つカタログを作成する

仮想マシンに複数のNICを持つカタログを作成するには、次の手順を実行します。

1. Delivery ControllerホストからPowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために `asnp citrix*` を実行します。
3. まだ作成されていない場合は、IDプールを作成します。
4. プロビジョニングスキームを作成します。

   - マシンプロファイルに基づかないマシンカタログを作成する場合は、`NetworkMappings` パラメーターを指定して`New-ProvScheme`コマンドを実行します。`NetworkMappings`パラメーターに複数のサブネットを追加できます。例：

     ```
     New-Provscheme -NetworkMappings
     @{"0"="subnetpath1";"1"="subnetpath1"}
     ```

   - マシンプロファイルに基づいたマシンカタログを作成する場合：

     a. 複数のNICを持つVMをAzureに作成します。詳細については、「複数のNICを持つWindows仮想マシンの作成と管理」を参照してください。新しいVMを作成し、Azureポータルの「ネットワーク」ページでネットワークインターフェイスをアタッチすることもできます。

     b. VMをマシンプロファイル入力として、`New-ProvScheme`コマンドを実行します。

     注:

     マシンプロファイルベースのマシンカタログを作成する場合、`NetworkMappings`の数はマシンプロファイルの`NetworkInterfaceCount`と同じである必要があります。`NetworkInterfaceCount`は、`Get-item -Path "machine profile path"`の`AdditionalData`から取得できます。

5. カタログの作成を完了します。

VMに複数のNICを持たせるようにカタログを更新する

VMに複数のNICを持たせるようにカタログを更新するには、次の手順を実行します。

1. Delivery ControllerホストからPowerShellウィンドウを開きます。
2. `asnp citrix*`を実行して、Citrix固有のPowerShellモジュールをロードします。
3. プロビジョニングスキームを更新します:

   - マシンプロファイルベースではないマシンカタログを作成する場合は、`NetworkMappings`パラメーターを指定して`Set-ProvScheme`コマンドを実行します。`NetworkMappings`パラメーターに複数のサブネットを追加できます。例:

     ```
     Set-Provscheme -NetworkMappings
     @{"0"="subnetpath1";"1"="subnetpath1"}
     ```

   - マシンプロファイルに基づいてマシンカタログを作成する場合：

     a. Azureで複数のNICを持つVMを作成します。詳細については、複数のNICを持つWindows仮想マシンの作成と管理を参照してください。

     b. VMをマシンプロファイル入力として、`Set-ProvScheme`コマンドを実行します。

既存のVMを更新して、VMに複数のNICを持たせる

`Set-ProvVMUpdateTimeWindow`を使用して既存のVMを更新することもできます。また、更新時間枠中に既存のVMでパワーサイクルを実行することもできます。

Azure Monitor Agentがインストールされたカタログ VMをプロビジョニングする

Azure監視は、AzureおよびオンプレミスTM環境からのテレメトリデータを収集、分析、および処理するために使用できるサービスです。

Azure Monitor Agent (AMA) は、仮想マシンなどのコンピューティングリソースから監視データを収集し、そのデータをAzure Monitorに配信します。現在、イベントログ、Syslog、パフォーマンスメトリックの収集をサポートしており、Azure Monitor MetricsおよびAzure Monitor Logsのデータソースに送信します。

監視データ内のVMを一意に識別して監視を有効にするには、AMAが拡張機能としてインストールされたMCSマシンカタログのVMをプロビジョニングできます。

要件

- 権限: (/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/connections/connection-azure-resource-manager#required-azure-permissions)に指定されている最小限のAzure権限と、Azure Monitorを使用するための以下の権限があることを確認してください。
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- データ収集ルール: Azure portal でデータ収集ルールを設定します。DCR の設定については、データ収集ルールを作成する を参照してください。DCR はプラットフォーム固有 (Windows または Linux) です。必要なプラットフォームに応じて DCR を作成してください。 AMA は、データ収集ルール (DCR) を使用して、VM などのリソースと、Azure Monitor Metrics や Azure Monitor Logs などのデータ ソース間のマッピングを管理します。
- 既定のワークスペース: Azure portal でワークスペースを作成します。ワークスペースの作成については、Log Analytics ワークスペースを作成するを参照してください。ログとデータを収集すると、その情報はワークスペースに保存されます。ワークスペースには一意のワークスペース ID とリソース ID があります。ワークスペース名は、特定のリソース グループ内で一意である必要があります。ワークスペースを作成したら、データ ソースとソリューションを設定して、そのデータをワークスペースに保存します。
- 監視拡張機能のホワイトリスト登録: 拡張機能`AzureMonitorWindowsAgent`と`AzureMonitorLinuxAgent`は、Citrixが定義したホワイトリスト登録済みの拡張機能です。ホワイトリスト登録済みの拡張機能のリストを表示するには、PoSHコマンド`Get-ProvMetadataConfiguration`を使用します。
- マスターイメージ: Microsoftは、既存のマシンから新しいマシンを作成する前に、既存のマシンから拡張機能を削除することを推奨しています。拡張機能が削除されない場合、残存ファイルや予期しない動作につながる可能性があります。詳細については、既存のVMからVMを再作成する場合を参照してください。

AMA を有効にしてカタログ VM をプロビジョニングするには:

1. マシンプロファイルテンプレートを設定します。
   - VMをマシンプロファイルテンプレートとして使用する場合：
     a. Azure portal で VM を作成します。

b. VMの電源を入れます。

c. **リソース**の下のデータ収集ルールにVMを追加します。これにより、テンプレートVMにエージェントのインストールが呼び出されます。

> **注:**
>
> Linuxカタログを作成する必要がある場合は、Linuxマシンを設定します。

- テンプレート仕様をマシンプロファイルテンプレートとして使用する場合：

a. テンプレート仕様を設定します。

b. 生成されたテンプレート仕様に、次の拡張機能とデータ収集ルール関連付けを追加します。

```
{

"type": "Microsoft.Compute/virtualMachines/extensions",

"apiVersion": "2022-03-01",

"name": "<vm-name>/AzureMonitorWindowsAgent",

"dependsOn": [

    "Microsoft.Compute/virtualMachines/<vm-name>"

],

"location": "<azure-region>",

"properties": {

    "publisher": "Microsoft.Azure.Monitor",

    "type": "AzureMonitorWindowsAgent",

    "typeHandlerVersion": "1.0",

    "autoUpgradeMinorVersion": true,
```

```
    "enableAutomaticUpgrade": true

}

},

 {

    "type": "Microsoft.Insights/dataCollectionRuleAssociations",

    "apiVersion": "2021-11-01",

    "name": "<associatio-name>",

    "scope": "Microsoft.Compute/virtualMachines/<vm-name>",

    "dependsOn": [

     "Microsoft.Compute/virtualMachines/<vm-name>",

    "Microsoft.Compute/virtualMachines/<vm-name>/extensions/
AzureMonitorWindowsAgent"

    ],

    "properties": {

       "description": "Association of data collection rule.
Deleting this association will break the data collection for this
Arc server.",

     "dataCollectionRuleId": "/subscriptions/<azure-
subscription>/resourcegroups/<azure-resource-group>/providers/
microsoft.insights/datacollectionrules/<azure-data-collection-
rule>"

     }

    }
```

2. 既存のMCSマシンカタログを作成または更新します。

- 新しいMCSカタログを作成するには:
  a. Web Studio で、その VM またはテンプレート仕様をマシンプロファイルとして選択します。
  b. カタログを作成するための次の手順に進みます。
- 既存の MCS カタログを更新するには、次の PoSH コマンドを使用します。
  - 新しい VM に更新されたマシンプロファイルテンプレートを取得させるには、次のコマンドを実行します。

```
Set-ProvScheme -ProvisioningSchemeName "name"

-MachineProfile "XDHyp:
\HostingUnits\Unit1\machineprofile.folder\abc.resourcegroup\ab-
machine-profile.vm"
```

  - 既存の VM を更新されたマシンプロファイルテンプレートで更新するには：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

3. カタログVMの電源をオンにします。
4. Azureポータルに移動し、モニター拡張機能がVMにインストールされていること、およびVMがDCRのリソースの下に表示されていることを確認します。数分後、監視データがAzure Monitorに表示されます。

トラブルシューティング

Azure Monitor Agentのトラブルシューティングガイダンスについては、以下を参照してください。

- https://learn.microsoft.com/ja-jp/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/ja-jp/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

顧客管理の暗号化キーでマシンカタログを作成する

顧客管理の暗号化キーを使用してマシンカタログを作成する詳細な手順は次のとおりです。

1. PowerShellウィンドウを開きます。

2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. `cd xdhyp:/`を入力します。
4. `cd .\HostingUnits\(your hosting unit)`を入力します。
5. `cd diskencryptionset.folder`を入力します。
6. ディスク暗号化セットのリストを取得するには、`dir`を入力します。
7. ディスク暗号化セットのIDをコピーします。
8. ディスク暗号化セットのIDを含めるカスタムプロパティ文字列を作成します。例:

```
$customProperties = "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"Standard_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"persistWBC`"
Value=`"False`" />

<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"false`" />

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/resourceGroups/
abc/providers/Microsoft.Compute/diskEncryptionSets/abc-des`"/>

</CustomProperties>
```

9. まだ作成されていない場合は、IDプールを作成します。例:

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain def.local -NamingSchemeType Numeric
```

10. New-ProvSchemeコマンドを実行します。例:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\azure-
res2\image.folder\def.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-res2\
\virtualprivatecloud.folder\def.resourcegroup\def-
vnet.virtualprivatecloud\subnet1.network"}

-ProvisioningSchemeName "name"

-ServiceOffering "XDHyp:\HostingUnits\azure-
res2\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-MachineProfile "XDHyp:
\HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<machin
e profile vm.vm>"

-CustomProperties $customProperties
```

11. マシンカタログの作成を完了します。

二重暗号化されたマシンカタログを作成する

Web Studio および PowerShell コマンドを使用して、二重暗号化されたマシンカタログを作成および更新できます。

二重暗号化されたマシンカタログを作成する詳細な手順は次のとおりです。

1. プラットフォーム管理キーと顧客管理キーを使用してAzure Key VaultとDESを作成します。Azure Key VaultとDESの作成方法については、「マネージドディスクの保存時の二重暗号化を有効にするためにAzureポータルを使用する」を参照してください。
2. ホスティング接続で利用可能なDiskEncryptionSetsを参照するには:
    a. **PowerShell**ウィンドウを開きます。
    b. 次のPowerShellコマンドを実行します。
        i. `asnp citrix*`
        ii. `cd xdhyp:`:
        iii. `cd HostingUnits`

iv. `cd YourHostingUnitName` (例えば azure-east)

v. `cd diskencryptionset.folder`

vi. `dir`

カスタムプロパティを使用してカタログを作成または更新するには、`DiskEncryptionSet` のIDを使用できます。

3. マシンプロファイルワークフローを使用する場合は、VMまたはテンプレート仕様をマシンプロファイルの入力として作成します。

   - VMをマシンプロファイルの入力として使用する場合:

     a. Azure PortalでVMを作成します。

     b. **ディスク>キー管理** に移動し、任意の `DiskEncryptionSetID` でVMを直接暗号化します。

   - テンプレート仕様をマシンプロファイルの入力として使用する場合:

     a. テンプレートで、`properties>storageProfile>osDisk>managedDisk` の下に `diskEncryptionSet` パラメーターを追加し、二重暗号化DESのIDを追加します。

4. マシンカタログを作成します。

   - Web Studioを使用している場合は、マシンカタログの作成 の手順に加えて、次のいずれかを実行します。

     ◦ マシンプロファイルベースのワークフローを使用しない場合は、**ディスク設定** ページで、**各マシンのデータを暗号化するために次のキーを使用する** を選択します。次に、ドロップダウンメニューから二重暗号化DESを選択します。カタログの作成を続行します。

     ◦ マシンプロファイルワークフローを使用している場合は、**イメージ**ページでマスターイメージとマシンプロファイルを選択します。マシンプロファイルのプロパティにディスク暗号化セットIDがあることを確認してください。

     カタログで作成されたすべてのマシンは、選択したDESに関連付けられているキーによって二重に暗号化されます。

   - PowerShellコマンドを使用する場合は、次のいずれかを実行します。

     ◦ マシンプロファイルベースのワークフローを使用しない場合は、`New-ProvScheme` コマンドにカスタムプロパティ `DiskEncryptionSetId` を追加します。例：

```
New-ProvScheme -CleanOnBoot -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />

</CustomProperties>'

-HostingUnitName "Redacted"

-IdentityPoolName "Redacted"

-InitialBatchSizeHint 1

-MasterImageVM "Redacted"

-NetworkMapping @{"0"="Redacted"}

-ProvisioningSchemeName "Redacted"

-ServiceOffering "Redacted"
```

- マシンプロファイルベースのワークフローを使用する場合は、`New-ProvScheme` コマンドでマシンプロファイル入力を指定します。例：

```
New-ProvScheme -CleanOnBoot

-HostingUnitName azure-east

-IdentityPoolName aio-ip

-InitialBatchSizeHint 1
```

```
-MasterImageVM XDHyp:\HostingUnits\azure-
east\image.folder\abc.resourcegroup\fgb-vda-snapshot.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-
east\virtualprivatecloud.folder\apa-
resourceGroup.resourcegroup\apa-resourceGroup-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName aio-test

-MachineProfile XDHyp:\HostingUnits\azure-
east\machineprofile.folder\abc.resourcegroup\abx-
mp.templatespec\1.0.0.templatespecversion
```

5. リモートPowerShell SDKを使用してカタログの作成を完了します。リモートPowerShell SDKを使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/ を参照してください。カタログで作成されたすべてのマシンは、選択したDESに関連付けられているキーによって二重に暗号化されます。

暗号化されていないカタログを二重暗号化を使用するように変換する

マシンカタログの暗号化の種類（カスタムプロパティまたはマシンプロファイルを使用）を更新できます。

- マシンプロファイルベースのワークフローを使用しない場合は、`Set-ProvScheme` コマンドにカスタムプロパティ DiskEncryptionSetId を追加します。例：

```
Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/12345678-xxxx-1234-1234-123456789012/resourceGroups/
Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/
SampleEncryptionSet" />

</CustomProperties>'
```

- マシンプロファイルベースのワークフローを使用する場合は、`Set-ProvScheme` コマンドでマシンプロファイル入力を指定します。例：

```
Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
XDHyp:\HostingUnits\azure-
east\machineprofile.folder\aelx.resourcegroup\elx-
mp.templatespec\1.0.0.templatespecversion
```

成功すると、カタログに追加するすべての新しいVMは、選択したDESに関連付けられているキーによって二重に暗号化されます。

カタログが二重暗号化されていることを確認する

- ウェブスタジオで：
  a. **マシンカタログ**に移動します。
  b. 確認するカタログを選択します。画面下部にある**テンプレートプロパティ**タブをクリックします。
  c. 「**Azure Details**」の下で、「**Disk Encryption Set**」のディスク暗号化セットIDを確認します。カタログのDES IDが空白の場合、カタログは暗号化されていません。
  d. Azure Portalで、DES IDに関連付けられているDESの暗号化タイプがプラットフォーム管理キーと顧客管理キーであることを確認します。
- PowerShellコマンドを使用する:
  a. **PowerShell**ウィンドウを開きます。
  b. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*` を実行します。
  c. マシンカタログの情報を取得するには、`Get-ProvScheme` を使用します。例:

```
Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
```

  d. マシンカタログの DES ID カスタムプロパティを取得します。例:

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-1234-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />
```

e. Azure Portal で、DES ID に関連付けられている DES の暗号化の種類がプラットフォーム管理キーと顧客管理キーであることを確認します。

Azureエフェメラルディスクでカタログを作成する

エフェメラルディスクを使用するには、`New-ProvScheme` の実行時にカスタムプロパティ `UseEphemeralOsDisk` を **true** に設定する必要があります。

> **注:**
>
> カスタムプロパティ`UseEphemeralOsDisk`が**false**に設定されているか、値が指定されていない場合、プロビジョニングされたすべてのVDAはプロビジョニングされたOSディスクを使い続けます。

以下は、プロビジョニングスキームで使用するカスタムプロパティの例です。

```
"CustomProperties": [

            {

                "Name": "UseManagedDisks",

                "Value": "true"

            },

            {

                "Name": "StorageType",

                "Value": "Standard_LRS"

            },

            {

                "Name": "UseSharedImageGallery",

                "Value": "true"

            },
```

```
            {
                "Name": "SharedImageGalleryReplicaRatio",
                "Value": "40"
            },
            {
                "Name": "SharedImageGalleryReplicaMaximum",
                "Value": "10"
            },
            {
                "Name": "LicenseType",
                "Value": "Windows_Server"
            },
            {
                "Name": "UseEphemeralOsDisk",
                "Value": "true"
            }
        ],
```

カタログのエフェメラルディスクを構成する

カタログのAzureエフェメラルOSディスクを構成するには、`Set-ProvScheme`で`UseEphemeralOsDisk`パラメーターを使用します。`UseEphemeralOsDisk`パラメーターの値を**true**に設定します。

> **注:**

この機能を使用するには、`UseManagedDisks`と`UseSharedImageGallery`のパラメーターも有効にする必要があります。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk"
Value="true" />

</CustomProperties>'
```

エフェメラルディスクに関する重要な考慮事項

`New-ProvScheme`を使用してエフェメラルOSディスクをプロビジョニングするには、次の制約を考慮してください。

- カタログに使用されるVMサイズは、エフェメラルOSディスクをサポートしている必要があります。
- VMサイズに関連付けられているキャッシュまたは一時ディスクのサイズは、OSディスクのサイズ以上である必要があります。
- 一時ディスクのサイズは、キャッシュディスクのサイズよりも大きくする必要があります。

以下の際にもこれらの問題を考慮してください:

- プロビジョニングスキームを作成する際。
- プロビジョニングスキームを変更する際。
- イメージを更新する際。

Azure専用ホスト

MCSを使用して、Azure専用ホストにVMをプロビジョニングできます。Azure専用ホストにVMをプロビジョニングする前に、次の点に注意してください。

- ホストグループを作成します。
- そのホストグループにホストを作成します。
- カタログと仮想マシンを作成するために十分なホスト容量が予約されていることを確認してください。

次のPowerShellスクリプトを使用して、ホストテナンシーが定義されたマシンのカタログを作成できます。

```
New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <Property xsi:type="StringProperty" Name="HostGroupId"
Value="myResourceGroup/myHostGroup" />

 ...other Custom Properties...

 </CustomProperties>
```

MCSを使用してAzure専用ホストに仮想マシンをプロビジョニングする場合、次の点を考慮してください。

- *専用ホスト*はカタログのプロパティであり、カタログ作成後に変更することはできません。専用テナンシーは現在、Azureではサポートされていません。
- `HostGroupId`パラメーターを使用する場合、ホスティングユニットのリージョンに、事前に構成されたAzureホストグループが必要です。
- Azureの自動配置が必要です。この機能は、ホストグループに関連付けられたサブスクリプションをオンボードする要求を行います。詳細については、「Azure専用ホスト上のVMスケールセット - パブリックプレビュー」を参照してください。自動配置が有効になっていない場合、MCSはカタログ作成中にエラーをスローします。

Azure Compute Galleryイメージを使用してマシンカタログを作成または更新する

マシンカタログの作成に使用するイメージを選択する際、Azure Compute Galleryで作成したイメージを選択できます。

これらのイメージを表示するには、次の操作を行う必要があります。

1. Citrix Virtual Apps and Desktopsサイトを構成します。
2. Azure Resource Managerに接続します。

3. Azureポータルで、リソースグループを作成します。詳細については、「ポータルを使用してAzure Compute Galleryを作成する」を参照してください。
4. リソースグループ内にAzure Compute Galleryを作成します。
5. Azure Compute Gallery内にイメージ定義を作成します。
6. イメージ定義で、イメージバージョンを作成します。

Azure Compute Gallery のイメージを使用してマシンカタログを作成または更新するには、次の PowerShell コマンドを使用します。

1. PowerShell ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group")
```

4. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group\sharedImageGallery.sharedimagegallery")
```

5. 1つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group\sharedImageGallery.sharedimagegallery\sigtestimage.imagedefinitio
n")
```

6. 次の要素を使用してMCSカタログを作成および更新します。
   - リソースグループ
   - ギャラリー
   - ギャラリーイメージ定義
   - ギャラリーイメージバージョン

Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/ を参照してください。

共有イメージギャラリーの構成

共有イメージギャラリーをサポートするプロビジョニングスキームを作成するには、`New-ProvScheme`コマンドを使用します。プロビジョニングスキームでこの機能を有効または無効にし、レプリカ比率とレプリカの最大値を変更するには、`Set-ProvScheme`コマンドを使用します。

Shared Image Gallery 機能をサポートするために、プロビジョニングスキームに3つのカスタムプロパティが追加されました。

`UseSharedImageGallery`

- 公開されたイメージの保存に Shared Image Gallery を使用するかどうかを定義します。**True** に設定すると、イメージは Shared Image Gallery イメージとして保存され、それ以外の場合はスナップショットとして保存されます。
- 有効な値は**True**と**False**です。
- プロパティが定義されていない場合、デフォルト値は**False**です。

`SharedImageGalleryReplicaRatio`

- マシンとギャラリーイメージバージョンレプリカの比率を定義します。
- 有効な値は0より大きい整数です。
- プロパティが定義されていない場合、デフォルト値が使用されます。永続OSディスクのデフォルト値は1000で、非永続OSディスクのデフォルト値は40です。

`SharedImageGalleryReplicaMaximum`

- 各ギャラリーイメージバージョンに対するレプリカの最大数を定義します。
- プロパティが定義されていない場合、デフォルト値は100です。
- プロパティが定義されていない場合、デフォルト値は100です。

> **ヒント:**

> MCSプロビジョニングされたカタログの公開イメージを保存するためにShared Image Galleryを使用する場合、MCSはカタログ内のマシンの数、レプリカ比率、およびレプリカ

の最大値に基づいてギャラリーイメージバージョンのレプリカ数を設定します。レプリカ数は、カタログ内のマシンの数をレプリカ比率で割って（最も近い整数値に切り上げて）、その値を最大レプリカ数で上限を設けることによって計算されます。たとえば、レプリカ比率が20で最大値が5の場合、0〜20台のマシンには1つのレプリカが作成され、21〜40台には2つのレプリカ、41〜60台には3つのレプリカ、61〜80台には4つのレプリカ、81台以上には5つのレプリカが作成されます。

ユースケース: Shared Image Gallery のレプリカ比率とレプリカ最大値を更新する

既存のマシンカタログは Shared Image Gallery を使用しています。`Set-ProvScheme` コマンドを使用して、カタログ内のすべての既存マシンおよび将来のマシンのカスタムプロパティを更新します。

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

ユースケース：スナップショットカタログを Shared Image Gallery カタログに変換する

このユースケースの場合：

1. `UseSharedImageGallery` フラグを**True**に設定して `Set-ProvScheme` を実行します。オプションで `SharedImageGalleryReplicaRatio` および `SharedImageGalleryReplicaMaximum` プロパティを含めます。
2. カタログを更新します。
3. 強制的に更新するために、マシンの電源を入れ直します。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
```

```
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

ヒント:

`SharedImageGalleryReplicaRatio`と`SharedImageGalleryReplicaMaximum`のパラメーターは必須ではありません。`Set-ProvScheme`コマンドが完了しても、Shared Image Galleryイメージはまだ作成されていません。カタログがギャラリーを使用するように構成されると、次回のカタログ更新操作で公開されたイメージがギャラリーに保存されます。カタログ更新コマンドは、ギャラリー、ギャラリーイメージ、およびイメージバージョンを作成します。マシンの電源を入れ直すと、マシンが更新され、必要に応じてレプリカ数が更新されます。その時点から、既存のすべての非永続マシンはShared Image Galleryイメージを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはイメージを使用して作成されます。古いスナップショットは数時間以内に自動的にクリーンアップされます。

ユースケース: 共有イメージギャラリーカタログをスナップショットカタログに変換する

このユースケースの場合：

1. `UseSharedImageGallery` フラグを **False** に設定するか、未定義のままにして `Set-ProvScheme` を実行します。
2. カタログを更新します。
3. 強制的に更新するために、マシンの電源を入れ直します。

例：

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
```

ヒント：

スナップショットから共有イメージギャラリーカタログへの更新とは異なり、各マシンのカスタムデータは新しいカスタムプロパティを反映するようにまだ更新されていません。元の共有イメージギャラリーのカスタムプロパティを表示するには、次のコマンドを実行します: `Get-ProvVm -ProvisioningSchemeName catalog-name`。`Set-ProvScheme` コマンドが完了しても、イメージスナップショットはまだ作成されていません。カタログがギャラリーを使用しないように構成されると、次回のカタログ更新操作で公開されたイメージがスナップショットとして保存されます。その時点から、既存のすべての非永続マシンはスナップショットを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはスナップショットから作成されます。マシンの電源を入れ直すと更新され、その時点でカスタムマシンデータが更新され、`UseSharedImageGallery` が **False** に設定されていることが反映されます。古い共有イメージギャラリーのアセット（ギャラリー、イメージ、バージョン）は、数時間以内に自動的にクリーンアップされます。

指定されたアベイラビリティゾーンにマシンをプロビジョニングする

Azure環境では、特定の可用性ゾーンにマシンをプロビジョニングできます。これはPowerShellを使用して実現できます。

注：

- ゾーンが指定されていない場合、MCSはAzureにリージョン内にマシンを配置させます。複数のゾーンが指定されている場合、MCSはそれらのゾーンにマシンをランダムに分散します。
- **ストレージとライセンスの種類**ページでストレージ冗長性としてZRSを選択した場合、ゾーンの選択を解除してAzureにVMアベイラビリティゾーンを管理させることを推奨する警告が表示されます。この警告は、アベイラビリティゾーンを持つマシンプロファイルまたはホストグループを選択した場合にのみ表示されます。

PowerShellを介してアベイラビリティゾーンを構成する

PowerShellを使用して、`Get-Item` を使用して提供インベントリアイテムを表示できます。例えば、*米国東部リージョン*の `Standard_B1ls` サービス提供を表示するには：

```
$serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-
name\East US.region\serviceoffering.folder\Standard_B1ls.serviceoffering"
```

ゾーンを表示するには、アイテムの`AdditionalData`パラメーターを使用します:

`$serviceOffering.AdditionalData`

可用性ゾーンが指定されていない場合、マシンのプロビジョニング方法に変更はありません。

PowerShellを介してアベイラビリティゾーンを構成するには、`New-ProvScheme`操作で利用可能な **Zones** カスタムプロパティを使用します。**Zones** プロパティは、マシンをプロビジョニングするアベイラビリティゾーンのリストを定義します。これらのゾーンには、1つ以上のアベイラビリティゾーンを含めることができます。例えば、ゾーン1と3の場合は`<Property xsi:type="StringProperty" Name="Zones" Value="1, 3"/>`です。

プロビジョニングスキームのゾーンを更新するには、`Set-ProvScheme`コマンドを使用します。

無効なゾーンが提供された場合、プロビジョニングスキームは更新されず、無効なコマンドを修正する方法に関する指示を提供するエラーメッセージが表示されます。

> **ヒント:**

> 無効なカスタムプロパティを指定すると、プロビジョニングスキームは更新されず、関連するエラーメッセージが表示されます。

ストレージの種類

MCSを使用するAzure環境の仮想マシンには、異なるストレージの種類を選択します。ターゲットVMの場合、MCSは以下をサポートします。

- OSディスク: プレミアムSSD、SSD、またはHDD
- ライトバックキャッシュディスク: プレミアムSSD、SSD、またはHDD

これらのストレージの種類を使用する場合、以下を考慮してください。

- 選択したストレージの種類をVMがサポートしていることを確認してください。
- 構成でAzureエフェメラルディスクを使用している場合、ライトバックキャッシュディスク設定のオプションは表示されません。

> **ヒント:**

> `StorageType` はOSタイプとストレージアカウント用に構成されています。`WBCDiskStorageType` はライトバックキャッシュストレージタイプ用に構成されています。通常のカタログの場合、`StorageType` が必要です。`WBCDiskStorageType` が構成されていない場合、`StorageType` が `WBCDiskStorageType` のデフォルトとして使用されます。

> WBCDiskStorageType が構成されていない場合、StorageType が WBCDiskStorageType のデフォルトとして使用されます。

ストレージの種類を構成する

VMのストレージの種類を構成するには、`New-ProvScheme` の `StorageType` パラメーターを使用します。`StorageType` パラメーターの値をサポートされているストレージタイプのいずれかに設定します。

以下は、プロビジョニングスキームにおける `CustomProperties` パラメーターの設定例です。

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>'
```

ゾーン冗長ストレージを有効にする

カタログ作成時にゾーン冗長ストレージを選択できます。これにより、Azure マネージドディスクが複数の可用性ゾーンに同期的にレプリケートされ、あるゾーンで障害が発生した場合でも、他のゾーンの冗長性を利用して復旧できます。

ストレージタイプのカスタムプロパティで **Premium_ZRS** と **StandardSSD_ZRS** を指定できます。ZRS ストレージは、既存のカスタムプロパティを使用するか、**MachineProfile** テンプレートを介して設定できます。ZRS ストレージは、`-StartsNow` および `-DurationInMinutes -1` パ

ラメーターを持つ `Set-ProvVMUpdateTimeWindow` コマンドでもサポートされており、既存のマシンを LRS から ZRS ストレージに変更できます。

制限事項:

- マネージドディスクのみをサポート
- プレミアムおよび標準ソリッドステートドライブ (SSD) のみでサポート
- `StorageTypeAtShutdown` ではサポートされていません
- 特定のリージョンでのみ利用可能です。
- 大規模に ZRS ディスクを作成すると、Azure のパフォーマンスが低下します。そのため、最初の電源投入時には、マシンを小規模なバッチ (一度に 300 台未満) で起動してください。

ゾーン冗長ストレージをディスクストレージタイプとして設定する

初期カタログ作成時にゾーン冗長ストレージを選択することも、既存のカタログでストレージタイプを更新することもできます。

POWERSHELL コマンドを使用してゾーン冗長ストレージを選択する

`New-ProvScheme` PowerShell コマンドを使用して Azure で新しいカタログを作成する場合、`StorageAccountType` の値として `Standard_ZRS` を使用します。 例:

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_ZRS" />
```

この値を設定すると、それが適切に使用できるかどうかを判断する動的 API によって検証されます。ZRS の使用がカタログに対して有効でない場合、次の例外が発生する可能性があります。

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: StorageTypeAtShutdownカスタムプロパティは、ZRSストレージでは使用できません。
- **StorageAccountTypeNotSupportedInRegion**: この例外は、ZRSをサポートしていないAzureリージョンでZRSストレージを使用しようとすると発生します。
- **ZrsRequiresManagedDisks**: ゾーン冗長ストレージはマネージドディスクでのみ使用できます。

ディスクストレージの種類は、次のカスタムプロパティを使用して設定できます。

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> **注:**
>
> カタログ作成時、カスタムプロパティが設定されていない場合は、マシンプロファイルのOSディスク`StorageType`が使用されます。

マシンプロファイルからVMとNICの診断設定をキャプチャする

マシンカタログの作成時、既存のマシンカタログの更新時、および既存のVMの更新時に、マシンプロファイルからVMとNICの診断設定をキャプチャできます。

VMまたはテンプレート仕様をマシンプロファイルのソースとして作成できます。

主な手順

1. Azureで必要なIDを設定します。これらのIDはテンプレート仕様で指定する必要があります。
    - ストレージアカウント
    - ログ分析ワークスペース
    - 標準ティアの価格設定を持つイベントハブの名前空間
2. マシンプロファイルのソースを作成します。
3. 新しいマシンカタログを作成するか、既存のカタログを更新するか、既存のVMを更新します。

Azureで必要なIDを設定する

Azureで次のいずれかを設定します。

- ストレージアカウント
- ログ分析ワークスペース
- 標準ティアの価格設定を持つイベントハブの名前空間

ストレージアカウントを設定する

Azureで標準ストレージアカウントを作成します。テンプレート仕様では、ストレージアカウントの完全なresourceIdを`storageAccountId`として指定します。

VMがストレージアカウントにデータをログ記録するように設定されると、データは`insights-metrics-pt1m`コンテナーの下で見つけることができます。

ログ分析ワークスペースを設定する

ログ分析ワークスペースを作成します。テンプレート仕様では、ログ分析ワークスペースの完全なresourceIdをworkspaceIdとして指定します。

VMがワークスペースにデータをログ記録するように設定されると、Azureのでデータをクエリできます。Azureので次のコマンドを実行すると、リソースによってログ記録されたすべてのメトリックの数を表示できます。

```
AzureMetrics | summarize Count=count() by ResourceId
```

イベントハブを設定する

Azure portal でイベントハブをセットアップするには、次の手順を実行します。

1. 標準ティアの価格設定でイベントハブ名前空間を作成します。
2. 名前空間の下にイベントハブを作成します。
3. イベントハブの下にある **Capture** に移動します。Avro 出力タイプでキャプチャするには、トグルをオンにします。
4. ログをキャプチャするために、既存のストレージアカウントに新しいコンテナを作成します。
5. テンプレート仕様で、`eventHubAuthorizationRuleId` を次の形式で指定します: `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. イベントハブの名前を指定します。

VM がイベントハブにデータをログ記録するように設定されると、データは構成されたストレージコンテナにキャプチャされます。

マシンプロファイルソースを作成する

VM またはテンプレート仕様をマシンプロファイルソースとして作成できます。

診断設定を含む VM ベースのマシンプロファイルを作成する

VM をマシンプロファイルとして作成する場合は、まずテンプレート VM 自体に診断設定を設定します。Microsoft ドキュメントの Azure Monitor の診断設定 に記載されている詳細な手順を参照してください。

VM または NIC に診断設定が関連付けられていることを確認するには、次のコマンドを実行します。

```
az monitor diagnostic-settings list --resource-group matspo --resource
matspo-tog-cc2659 --resource-type microsoft.network/networkInterfaces
```

```
az monitor diagnostic-settings list --resource-group matspo --resource
matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
```

診断設定を含むテンプレートスペックベースのマシンプロファイルを作成する

診断設定がすでに有効になっているVMを使用し、それをARMテンプレートスペックにエクスポートする場合、これらの設定はテンプレートに自動的に含まれません。ARMテンプレート内で診断設定を手動で追加または変更する必要があります。

ただし、VMをマシンプロファイルとして使用する場合、MCSは、重要な診断設定が正確にキャプチャされ、MCSカタログ内のリソースに適用されることを保証します。

1. VMとNICを定義する標準テンプレート仕様を作成します。
2. スペックに従って診断設定をデプロイするための追加リソースを追加します: Microsoft.Insights diagnosticSettings。スコープには、テンプレート内のVMまたはNICを部分的なIDを持つ名前で参照します。たとえば、テンプレートスペック内のtest-VMという名前のVMにアタッチされた診断設定を作成する場合、スコープを次のように指定します。

   ```
   "scope": "microsoft.compute/virtualMachines/test-VM",
   ```

3. テンプレート仕様をマシンプロファイルのソースとして使用します。

診断設定を含むカタログを作成または更新する

マシンプロファイルソースを作成した後、`New-ProvScheme`コマンドを使用してマシンカタログを作成したり、`Set-ProvScheme`コマンドを使用して既存のマシンカタログを更新したり、`Request-ProvVMUpdate`コマンドを使用して既存のVMを更新したりできます。

ページファイルの場所の決定

ページファイルの場所は、次のシナリオに従って決定されます。

注:

デフォルトのページファイルの場所は OS ディスクです。

シナリオ	場所
ページファイル設定がカスタムプロパティで指定されている場合	カスタムプロパティで指定されているとおり
エフェメラルOSディスクまたは休止状態が有効になっている	OSディスク
VMに一時ディスクがある	一時ディスク
MCS I/O が有効になっています	WBCディスク

ページファイル設定のシナリオ

次の表は、イメージ準備中およびプロビジョニングスキームの更新中に発生する可能性のあるページファイル設定のシナリオの一部を示しています。

期間	シナリオ	結果
イメージ準備	プロビジョニングスキームで指定したVMサイズに一時ディスクがないにもかかわらず、ソースイメージのページファイルを一時ディスクに設定する	ページファイルはOSに配置されます
イメージの準備	プロビジョニングスキームで指定するVMサイズには一時ディスクがありますが、ソースイメージのページファイルをOSディスクに設定します。	ページファイルは一時ディスクに配置されます。
イメージの準備	ソースイメージのページファイルを一時ディスクに設定し、プロビジョニングスキームでエフェメラルOSディスクを有効にします。	ページファイルはOSディスクに配置されます。
プロビジョニングスキームの更新	VDAバージョンが2311より前の場合に、プロビジョニングスキームの更新を試みます。	警告とともにページファイル設定を変更します。

期間	シナリオ	結果
プロビジョニングスキームの更新	VDAバージョンが2311以降の場合に、プロビジョニングスキームの更新を試みます。	(#page-file-location-determination)の[ページファイルの場所の決定]に従って、ページファイルの場所を決定します。

ページファイル設定の指定

PowerShellコマンドを使用して、場所やサイズを含むページファイル設定を指定できます。これにより、(#page-file-location-determination)のに従ってMCSによって決定されたページファイル設定が上書きされます。これは、マシンカタログ作成中に次の`New-ProvScheme`コマンドを実行することで行えます。

重要な考慮事項

カタログ作成を進める前に、以下を考慮してください。

- すべてのカスタムプロパティ（'PageFileDiskDriveLetterOverride'、'InitialPageFileSizeInMB'、'MaxPageFileSizeInMB'）を`New-ProvScheme`コマンドで指定するか、または何も指定しないでください。
- この機能はCitrix Studioではサポートされていません。
- 初期ページファイルサイズは16 MBから16777216 MBの間である必要があります。
- 最大ページファイルサイズは、初期ページファイルサイズ以上で、かつ16777216 MB未満である必要があります。
- 初期ページファイルサイズと最大ページファイルサイズの両方を同時にゼロに設定できます。

> **注:**
>
> 既存のカタログに新しく追加されたVMのページファイル設定を、マスターイメージを更新することなく変更できます。ページファイル設定を変更するには、VDAバージョン2311以降が必要です。PowerShellコマンドを使用してページファイル設定を変更できます。詳細については、「ページファイル設定の変更」を参照してください。

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "zijinnet" `
```

```
-IdentityPoolName "PageFileSettingExample" `

-ProvisioningSchemeName "PageFileSettingExample" `

-InitialBatchSizeHint 1 `

-MasterImageVM "XDHyp:\HostingUnits\zijinnet\image.folder\neal-zijincloud-
resources.resourcegroup\CustomWin10VDA_OsDisk_1_9473d7c8a6174b2c8284c7d3ef
eea88f.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\zijinnet\
\virtualprivatecloud.folder\\East US.region\\virtualprivatecloud.folder\
\neal-zijincloud-resources.resourcegroup\\neal-zijincloud-resources-
vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\zijinnet\\serviceoffering.folder\
\Standard_B2ms.serviceoffering" `

-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride"
Value="d"/> `

<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
Value="2048"/> `

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB"
Value="8196"/> `

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `
```

```
</CustomProperties>'
```

ページファイル設定の変更

既存のカタログに新しく追加されたVMのページファイル設定を、マスターイメージを更新することなく変更できます。現在、この機能はAzure環境のみに適用されます。

ページファイル設定を変更するには、VDAバージョン2311以降が必要です。PowerShellコマンドを使用してページファイル設定を変更できます。

Azure環境で変更できるページファイル設定は次のとおりです。

- `PageFileDiskDriveLetterOverride`
- `InitialPageFileSizeInMB`
- `MaxPageFileSizeInMB`

既存のカタログのページファイル設定を変更する

既存のマシンカタログのページファイル設定を変更するには、`Set-ProvScheme` コマンドを実行します。この場合、更新はカタログに追加された新しいVMにのみ適用されます。例：

```
Set-ProvScheme -ProvisioningSchemeName $schemeName -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="StandardSSD_LRS" />

<Property xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride"
Value="D" />

<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
Value="2048" />

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB"
Value="8196" />

<Property xsi:type="StringProperty" Name="LicenseType"
```

```
Value="Windows_Client" />

<Property  xsi:type="StringProperty" Name="Zones" Value="1" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="neal-
test-group1" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

注:

ライトバックキャッシュを有効にして、PowerShell コマンドを使用して `PageFileDiskDriveLetterOverride` を `C:` に設定しようとすると、MCS IO ドライバーはページファイルを自動的に正しいディスクドライブにリダイレクトし、`C:` にはリダイレクトしません。

Azure Spot VMを使用してカタログを作成する

Azure Spot VMを使用すると、Azureの未使用のコンピューティング能力を大幅なコスト削減で活用できます。ただし、Azure Spot VMを割り当てる機能は、現在の容量と価格設定に依存します。そのため、Azureは強制排除ポリシーに従って、実行中のVMを強制排除したり、VMの作成に失敗したり、VMの電源をオンにできなかったりする可能性があります。したがって、Azure Spot VMは、一部の重要でないアプリケーションやデスクトップに適しています。詳細については、「Azure Spot Virtual Machinesの使用」を参照してください。

制限事項

- すべてのVMサイズがAzure Spot VMでサポートされているわけではありません。詳細については、「制限事項」を参照してください。

  VMサイズがSpot VMをサポートしているかどうかを確認するには、次のPowerShellコマンドを実行します。VMサイズがSpot VMをサポートしている場合、`SupportsSpotVM` は**True**になります。

  ```
  (Get-Item "XDHyp:\HostingUnits\azure-res-
  conn2\serviceoffering.folder\Standard_D2ds_v4.serviceoffering").
  AdditionalData
  ```

- 現在、Azure Spot VMは休止状態をサポートしていません。

要件

Azure Spot VMカタログのマシンプロファイルソース（VMまたはテンプレート仕様）を作成する際、Azure Spot Instanceを選択するか（VMを使用する場合）、`priority`を`Spot`として設定する必要があります（テンプレート仕様を使用する場合）。

Azure Spot VMを使用してカタログを作成する手順

1. マシンプロファイルソース（VMまたは起動テンプレート）を作成します。

   - Azureポータルを使用してVMを作成する方法については、「Azureポータルを使用してAzure Spot Virtual Machinesを展開する」を参照してください。
   - テンプレートスペックを作成するには、テンプレートスペック内の **resources > type: Microsoft.Compute/virtualMachines > properties** の下に以下のプロパティを追加します。例:

     ```
     "priority": "Spot",

     "evictionPolicy": "Deallocate",

     "billingProfile": {

     "maxPrice": 0.01

     }
     ```

注:

- 強制排除ポリシーは **Deallocate** または **Delete** にすることができます。
- 非永続VMの場合、MCSは常に強制排除ポリシーを **Delete** に設定します。VMが強制排除された場合、非永続ディスク（例: OS disk）とともに削除されます。永続ディスク（例: Identity disk）は削除されません。ただし、カタログタイプが永続的であるか、`PersistOsDisk`カスタムプロパティがTrueに設定されている場合、OS diskは永続的です。同様に、`PersistWbc`カスタムプロパティが **True** に設定されている場合、WBC diskは永続的です。

- 永続VMの場合、MCSは常に強制排除ポリシーをDeallocateに設定します。VMが強制排除された場合、割り当て解除されます。ディスクに変更は加えられません。
- 最大価格は、1時間あたりに支払う意思のある価格です。**Capacity Only** を使用している場合、これは **-1** です。最大価格は、null、-1、またはゼロより大きい小数である必要があります。詳細については、Pricing を参照してください。

2. 以下のPowerShellコマンドを実行して、マシンプロファイルがAzure Spot VM対応であるかどうかを確認できます。`SpotEnabled` パラメータが **True** で、`SpotEvictionPolicy` が **Deallocate** または **Delete** に設定されている場合、マシンプロファイルはAzure Spot VM対応です。例:

   - マシンプロファイルのソースがVMの場合、以下のコマンドを実行します。

     ```
     (Get-Item "XDHyp:\HostingUnits\azure-res-
     conn2\machineprofile.folder\fifthcolumn.resourcegroup\kb-spot-
     delete.vm"). AdditionalData
     ```

   - マシンプロファイルのソースがテンプレートスペックの場合、以下のコマンドを実行します。

     ```
     (Get-Item "XDHyp:\HostingUnits\azure-res-
     conn2\machineprofile.folder\fifthcolumn.resourcegroup\fc-aeh-
     templatespec.templatespec\14.0.0-spot-
     delete.templatespecversion").AdditionalData
     ```

3. `New-ProvScheme` PowerShellコマンドを使用して、マシンプロファイルでマシンカタログを作成します。

`Set-ProvScheme` コマンドを使用してカタログを更新できます。既存のVMをPowerShellコマンド `Set-ProvVmUpdateTimeWindow` を使用して更新することもできます。マシンプロファイルは次回の電源投入時に更新されます。

実行中のAzure Spot VMでの強制排除

コンピューティング容量が利用できない場合、または1時間あたりの価格が設定された最大価格よりも高い場合、Azureは実行中のSpot VMを強制排除します。デフォルトでは、強制排除の通知はされません。VMは単にフリーズし、強制排除されます。Microsoftは、強制排除を監視するためにScheduled Eventsを使用することを推奨しています。Continuously monitor for eviction を参照して

ください。VM内からスクリプトを実行して、強制排除前に通知を受け取ることもできます。例えば、MicrosoftはPythonでポーリングスクリプト ScheduledEvents.cs を提供しています。

トラブルシューティング

- プロビジョニングされたVMのcustomMachineDataで、`Get-ProvVM` コマンドを使用してSpot VMのプロパティを確認できます。priorityフィールドが **Spot** に設定されている場合、Spotが使用されています。
- VMがAzure PortalでSpotを使用しているかどうかを確認できます。

  a. Azure PortalでVMを見つけます。

  b. **概要**ページに移動します。

  c. 下にスクロールして、**Azure Spot**セクションを見つけます。

    - Spotが使用されていない場合、このフィールドは空です。
    - Spotが使用されている場合、**Azure Spot**および**Azure Spot eviction policy**フィールドが設定されます。

1. 構成ページで、VMの課金プロファイルまたは1時間あたりの最大価格を確認できます。

バックアップVMサイズの構成

パブリッククラウドでは、特定のVMサイズの容量が不足することがあります。また、Azure Spot VMを使用している場合、VMはAzureの容量要件に基づいていつでも強制排除される可能性があります。Azureの容量不足やSpot VMの電源投入失敗といった場合、MCSはバックアップVMサイズにフォールバックします。MCSマシンカタログの作成または更新時に、カスタムプロパティ `BackupVmConfiguration` を使用してバックアップVMサイズのリストを提供できます。MCSは、リストで指定された順序でバックアップVMサイズにフォールバックしようとします。

MCSがVMに特定のバックアップVMサイズを使用する場合、次回のシャットダウンまたは休止状態要求までその構成を使い続けます。次回の電源投入時、MCSはプライマリVMサイズを起動しようとします。失敗した場合、MCSはリストに従って再度バックアップVMサイズを起動しようとします。

この機能は、以下でサポートされています。

- マシンプロファイルを使用するカタログ
- 永続的および非永続的MCSマシンカタログ
- 現在のところAzure環境

制限事項

以下の構成はサポートされていません。

- Azure は、Azure 仮想マシンの休止状態 に記載されているように、休止状態の VM のサイズ変更を許可しません。VM は **停止** 状態である必要があります。したがって、サイズを変更する前に、MCS は休止状態をクリアするために割り当て解除要求を発行します。これにより、VM の休止状態が失われます。その後、MCS はさまざまなバックアップサイズを繰り返し処理し、VM サイズを更新して電源をオンにします。
- 永続的な VM の場合、以下のシナリオはサポートされていません。
  - VM はリソースディスクの一時ストレージをサポートしていますが、バックアップ VM サイズはサポートしていません。
  - VM にはリソースディスクの一時ストレージがありませんが、バックアップ VM サイズはそれをサポートしています。
  - VM は `DiskControllerType` **SCSI** を使用しますが、バックアップ VM サイズは `DiskControllerType` **NVMe** のみをサポートします。
  - VM は `DiskControllerType` **NVMe** を使用しますが、バックアップ VM サイズは `DiskControllerType` **SCSI** のみをサポートします。
- MCSIO が有効な非永続 VM の場合、ライトバックキャッシュディスクがリソースディスクの一時ストレージを使用していると、一時ストレージのないサイズへの切り替えはサポートされません。
- 既存の VM またはプライマリ VM サイズは休止状態が有効になっていますが、バックアップ VM サイズは休止状態をサポートしていません。

重要な考慮事項

- リストには複数のバックアップ VM サイズを指定できます。バックアップ VM サイズを多く指定するほど、電源操作が成功する可能性が高まります。
- リストは一意である必要があります。
- リスト内の各 VM のインスタンスタイププロパティを追加できます。タイプは **Spot** または **Regular** のいずれかです。タイプが指定されていない場合、MCS は VM を **Regular** と見なします。
- 既存のカタログのバックアップ VM サイズリストは、`Set-ProvScheme` PowerShell コマンドを使用して変更できます。
- カタログに関連付けられたプロビジョニングスキームから作成された既存の VM は、`Set-ProvVMUpdateTimeWindow` コマンドを使用して更新できます。

- `Set-ProvVM`コマンドを使用して、選択した数の既存のMCS VMのバックアップVMサイズリストを構成できます。ただし、更新を適用するには、`Set-ProvVMUpdateTimeWindow`を使用してVMの更新時間枠を設定し、その時間枠内でVMを起動します。VMで`Set-ProvVm`コマンドが使用された場合、プロビジョニングスキーム上のリストが後で更新されても、VMはその特定のVMに設定されたバックアップVMサイズリストを引き続き使用します。`Set-ProvVM`を`-RevertToProvSchemeConfiguration`と組み合わせて使用すると、VMにプロビジョニングスキーム上のバックアップリストを使用させることができます。

バックアップVMサイズでカタログを作成する

> **注:**
>
> Studio UIがフリーズする問題を解決するには、PowerShellコマンドの実行中にすべてのシングルクォートを`"`に置き換えてください。

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. ブローカーカタログを作成します。このカタログには、作成される予定のマシンが格納されます。
4. IDプールを作成します。これは、作成されるマシン用に作成されたADアカウントのコンテナになります。
5. マシンプロファイルを使用してプロビジョニングスキームを作成します。バックアップ構成の構成方法を参照してください。
6. プロビジョニングスキームの一意のIDで`BrokerCatalog`を更新します。
7. VMを作成してカタログに追加します。

既存のカタログを更新する

`Set-ProvScheme`コマンドを使用してプロビジョニングスキームを更新できます。バックアップ構成の構成方法を参照してください。

既存のVMを更新する

`Set-ProvVMUpdateTimeWindow` PowerShellコマンドを使用して、カタログ内の既存のVMを更新できます。このコマンドは、指定された時間枠内の次回の電源投入時に、カタログに関連付けられたプロビジョニングスキームから作成されたVMを更新します。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartTimeInUTC "3/12/2022 3am" -DurationInMinutes 60`
```

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartsNow -DurationInMinutes 60
```

選択した既存のMCS VMのバックアップVMサイズリストを`Set-ProvVM`コマンドを使用して構成できます。ただし、更新を適用するには、`Set-ProvVMUpdateTimeWindow`を使用してVMの更新時間枠を設定し、その時間枠内でVMを起動します。例：

1. 選択した既存のMCS VMのバックアップVMサイズリストを構成するには、`Set-ProvVM`コマンドを実行します。例：

   ```
   Set-ProvVM -ProvisioningSchemeName "name" -VMName "Vm-001"

   -CustomProperties

   "<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
   machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
   instance`">

   <Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
   Value=`"true`" />

   <Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
   Value=`"Premium_LRS`" />

   <Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
   Value=`"Windows_Server`"/>

   <Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
   Value=`"true`"/>  <Property xsi:type=`"StringProperty`"
   Name=`"BackupVmConfiguration`" Value=`"[{&amp;quot;ServiceOffering&amp;quot;:
   &amp;quot;Standard_D2as_v4&amp;quot;, &amp;quot;Type&amp;quot;: &amp;quot;Spot&amp;quot;},
   {&amp;quot;ServiceOffering&amp;quot;: &amp;quot;Standard_D2s_v3&amp;quot;,
   &amp;quot;Type&amp;quot;: &amp;quot;Regular&amp;quot;}, {&amp;quot;ServiceOffering&amp;quot;:
   &amp;quot;Standard_D2s_v3&amp;quot;, &amp;quot;Type&amp;quot;: &amp;quot;Spot&amp;quot;}]`"/>
   </CustomProperties>"
   ```

2. 更新を適用するには、`Set-ProvVMUpdateTimeWindow`コマンドを実行します。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartsNow -DurationInMinutes 60
```

すべてのリソースにタグをコピーする

マシンプロファイルで指定されたタグを、マシンカタログ内の新しい VM または既存の VM の複数の NIC やディスク（OS ディスク、ID ディスク、ライトバックキャッシュディスク）など、すべてのリソースにコピーできます。マシンプロファイルのソースは、VM または ARM テンプレート仕様にすることができます。

注:

リソースにタグを保持するには、タグに関するポリシーを追加するか（タグコンプライアンスのポリシー定義を割り当てるを参照）、マシンプロファイルソースにタグを追加する必要があります。

前提条件

そのVMのVM、ディスク、NICにタグを付けるには、マシンプロファイルソース（VMまたはARMテンプレート仕様）を作成します。

- VMをマシンプロファイルの入力として使用したい場合は、AzureポータルでVMとすべてのリソースにタグを適用します。Azureポータルでタグを適用するを参照してください。
- ARMテンプレート仕様をマシンプロファイルの入力として使用したい場合は、各リソースの下に次のタグブロックを追加します。

```
 "tags": {

"TagC": "Value3"

},
```

注:

テンプレート仕様には、最大1つのディスクと少なくとも1つのNICを含めることができます。

新しいマシンカタログ内のVMのリソースにタグをコピーする

1. VMまたはARMテンプレート仕様をマシンプロファイルの入力として使用して、非永続または永続カタログを作成します。
2. VMをカタログに追加して電源をオンにします。マシンプロファイルで指定されたタグが、そのVMの対応するリソースにコピーされていることを確認する必要があります。

> **注：**
>
> マシンプロファイルで提供されるNICの数と、VMで使用するNICの数に不一致がある場合、エラーが発生します。

既存のVMのリソース上のタグを変更する

1. すべてのリソースにタグを付けたマシンプロファイルを作成します。
2. 既存のマシンカタログを、更新されたマシンプロファイルで更新します。例：

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName>
-MachineProfile <PathToYourMachineProfile>
```

3. 更新を適用するVMの電源をオフにします。
4. VMのスケジュールされた更新を要求します。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <YourCatalogName>  -
VMName machine1 -StartsNow -DurationInMinutes -1
```

5. VMの電源をオンにします。
6. マシンプロファイルで指定されたタグが、対応するリソースにコピーされていることを確認する必要があります。

> **注：**
>
> マシンプロファイルで提供されるNICの数と、`Set-ProvScheme`で提供されるNICの数に不一致がある場合、エラーが発生します。

事前フォーマットされたWBCディスクカタログを作成する

プロビジョニングされたマシンの起動パフォーマンスを向上させるために、事前フォーマットされたWBCディスクカタログを作成できます。この機能を実装するには、WBCが有効なAzureカタログを作成し、追加のカスタムプロパティ`PreformatWriteBackCache`を`True`として含めます。

既存のカタログは、`Set-ProvScheme`コマンドを使用してWBCディスクサイズを更新できます。

この機能は、MCSがマスタリングフェーズを全体的なプロビジョニングワークフローから分離するイメージ管理ワークフローと互換性があります。イメージ管理の詳細については、「イメージ管理」を参照してください。

WBCが有効で、`PreformatWriteBackCache`が`True`であるAzureカタログを作成する例：

```
$customProperties = @'

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="PreformatWriteBackCache"
Value="true" />

</CustomProperties>

'@



New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName "provisioningschemename" `

-HostingUnitName "hostingunitname" `

-IdentityPoolName "identitypoolnamename" `

-MasterImageVM "XDHyp:
\HostingUnits\AzureHostingUnit\image.folder\rg.resourcegroup\masterImage.m
anageddisk" `

-CustomProperties $customProperties `
```

```
-NetworkMapping $networkMapping `

-UseWriteBackCache `

-WriteBackCacheDiskSize 30
```

既存のカタログのWBCディスクキャッシュサイズを更新する例：

```
Set-ProvScheme -ProvisioningSchemeName provisioningschemename
-WriteBackCacheDiskSize 127
```

MCSプロビジョニングされたCitrix Provisioning™カタログのシャットダウン時にWBCディスクを削除

AzureでMCSプロビジョニングされたCitrix Provisioningカタログを作成する際、WBCディスクを非永続的にプロビジョニングできます (`PersistWBC` をFalseとして)。この構成により、AzureでMCSプロビジョニングされたCitrix ProvisioningカタログのVMをシャットダウンした後、ライトバックキャッシュ (WBC) ディスクを削除できます。

条件：

この機能が動作するためには、カスタムプロパティ `PreformatWriteBackCache` を `True` として設定する必要があります。

`PersistWBC` が `False` で、 `PreformatWriteBackCache` が `True` であるAzureカタログを作成する例：

```
$customProperties = @'

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PreformatWriteBackCache"
Value="true" />

</CustomProperties>

'@
```

```
New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName "provisioningschemename" `

-HostingUnitName "hostingunitname" `

-IdentityPoolName "identitypoolnamename" `

-MasterImageVM "XDHyp:
\HostingUnits\AzureHostingUnit\image.folder\rg.resourcegroup\masterImage.m
anageddisk" `

-CustomProperties $customProperties `

-NetworkMapping $networkMapping `

-UseWriteBackCache `

-WriteBackCacheDiskSize 30
```

既存のカタログを`Set-ProvScheme`コマンドを使用して更新し、`PersistWBC`カスタムプロパティを更新することもできます。

データディスクのプロビジョニング

AzureのMCSマシンカタログの、MCSによって作成された永続または非永続VMに、永続データディスクを作成して割り当てることができます。

データディスクは、イメージソースとしてマネージドディスクからプロビジョニングする必要があります。

データディスクのプロパティ

データディスクは、プロパティがカスタムプロパティで指定されていない場合、カスタムプロパティまたはOSディスクテンプレートからプロパティを継承します。

- カスタムプロパティから派生したプロパティ
  - `DiskEncryptionSetId`
  - `Zones`
  - `StorageType`

- カスタムプロパティで指定されていない場合、OSディスクテンプレートから派生するプロパティ
  - `DiskEncryptionSetId`
  - `Zones`
  - `StorageType`

> **注:**
>
> - カスタムプロパティまたはOSディスクテンプレートでゾーン冗長ストレージ（ZRS）が指定されていない場合、データディスクはOSディスクおよびIDディスクと同じゾーンに配置されます。
> - タグはOSディスクテンプレートからのみ派生します。

制限事項

現在、以下の操作はサポートされていません。

- 複数のデータディスクのプロビジョニング。
- 非永続データディスクのプロビジョニング。
- テンプレートを使用したデータディスクの作成。
- 既存のカタログとVMをデータディスクを使用するように変更する。
- データディスクをリセットする。
- データディスクのイメージ更新。
- マネージドディスク以外のソースを使用する。
- データディスクをAzure Compute Gallery (ACG) に保存する。
- データディスクに`StorageTypeAtShutdown`を使用する

データディスクを含むカタログを作成する

データディスクを含むMCSマシンカタログをプロビジョニングするには、`New-ProvScheme` PowerShellコマンドに次のパラメーターを含めます。

- `DataDisk`: 有効なManagedDiskタイプのインベントリアイテムへのパス。
- `DataDiskPersistence`: `DataDisk`が永続的か非永続的かを示すため。ただし、現在サポートされているのは永続的なデータディスクのみです。

例:

```
New-ProvScheme  -CleanOnBoot -HostingUnitName "<HostingUnitName >"
-IdentityPoolName "<IdentityPoolName >" -InitialBatchSizeHint 1
-MasterImageVM disk.manageddisk -NetworkMapping <NetworkMapping >
-ProvisioningSchemeName "<ProvisioningSchemeName >" -DataDisk "XDHyp:
\HostingUnits\Azure-Resources-1\image.folder\<resourcegroupname>\xxxx-
datadisk.manageddisk"  -DataDiskPersistence "Persistent"  -Scope @()
-VMCpuCount 4  -VMMemoryMB 6144  -TenancyType Shared  -FunctionalLevel
"L7_20"
```

データディスクが使用中かどうかを判断する

データディスクがVMに割り当てられているかどうかを確認するには、次の手順を実行します。

- `Get-ProvVm`を実行し、VMの`CustomVmData`を確認します。VMがデータディスクを使用している場合、役割が`DiskRole.DataDisk`のディスクレコードがあります。
- AzureポータルでVMの下にデータディスクが存在するかどうかを確認します。

データディスクを削除する

カタログを削除した場合、`forgetVM` または `purgeDBOnly` オプションを使用しない限り、データディスクは削除されます。VM を削除した場合、`forgetVM` または `purgeDBOnly` オプションを使用しない限り、データディスクは削除されます。

アンマネージドディスクからマネージドディスクへの移行

On September 30, 2025, Azure はアンマネージドディスク（つまり、VHD）を正式に廃止します。既存のアンマネージドディスクを使用している VM は、期限後に停止され、割り当てが解除されます。

ただし、MCS でプロビジョニングされた VM をアンマネージドディスクからマネージドディスクに移行することで、Azure のアンマネージドディスク廃止計画によるサービス停止を回避できます。

VM に接続されているすべてのアンマネージドディスクが変換されます。これには、ID ディスク、OS ディスク、および WBC ディスク (使用されている場合) が含まれます。

Azure のアンマネージドディスク廃止計画の詳細については、「Migrate your Azure unmanaged disks by September 30, 2025」を参照してください。

ユースケース

この機能は、永続的および非永続的な MCS プロビジョニングカタログに適用されます。

また、オンデマンド VM と非オンデマンド (レガシー) VM の両方の移行をサポートしています。

- オンデマンド VM: 既存のディスクをアンマネージドディスクからマネージドディスクに移行して、Azure の更新されたサポートに合わせます。
- 非オンデマンド (レガシー) VM: レガシーまたは非オンデマンド VM は、アンマネージドディスクのみをサポートしています。この機能を使用して、レガシー VM をオンデマンドに変換すると同時に、マネージドディスクに移行します。

オンデマンドプロビジョニングの詳細については、「Azure オンデマンドプロビジョニング」を参照してください。

制限事項

- マシンカタログまたは VM がマネージドディスクに変換されると、アンマネージドディスクに戻すことはできません。
- 非オンデマンド (レガシー) VMの場合、移行プロセスにはそれらをオンデマンドプロビジョニングに変換することが含まれます。ディスクのみを変換して非オンデマンドVMを使い続けることはできません。

重要な考慮事項

- 変換は自動的に行われません。電源投入操作の一部として行われます。
- VMに対して複数の更新が要求された場合、ディスク変換が優先されます。追加の更新は、次回の電源投入まで延期されます。
- VMが正常に変換され、電源が投入されると、コストを節約するためにVMのVHDはクリーンアップされます。ストレージアカウント自体はクリーンアップされません。
    - ストレージアカウントにベースディスクがまだ存在する可能性があります。カタログの更新を実行すると、新しいスナップショット (またはACG) ベースディスクが作成されます。
    - カタログ内のすべてのVMが変換され、新しいベースディスクが作成されると、空のストレージアカウントを削除できます。

必要な権限

アンマネージドディスクからマネージドディスクへの変換を許可するには、Azureサービスプリンシパルで次の権限が必要です。

```
Microsoft.Compute/virtualMachines/convertToManagedDisks/write
```

構成手順

オンデマンドカタログの場合:

1. `Set-ProvScheme` (または永続VMの場合は`Set-ProvVM`) を実行して、`UseManagedDisks` を `True` に更新します。例:

```
Set-ProvScheme -ProvisioningSchemeName "<provscheme-name>"
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"UseManagedDisks`" Value=`"true`" /></CustomProperties>"
```

```
Set-ProvVM -ProvisioningSchemeName "<provscheme-name>" -VMName "<vm-
name>" -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" /
></CustomProperties>"
```

2. `Set-ProvVMUpdateTimeWindo`w` を実行して更新を適用します。この例では、更新はVMの次回の電源投入時に適用されます。

```
Set-ProvVmUpdateTimeWindow -ProvisioningSchemeName "<provscheme-name>"
-VMName "<vm-name>"
```

3. VMの電源を入れます。

非オンデマンド (レガシー) カタログの場合:

1. `Set-ProvScheme` を実行して (永続VMの場合は `Set-ProvVM`)、`Set DeploymentSchema` を `1.1` に構成します。例:

```
Set-ProvScheme -ProvisioningSchemeName "<provscheme-name>"
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"DeploymentSchema`" Value=`"1.1`" /></CustomProperties>"
```

```
Set-ProvVM -ProvisioningSchemeName "<provscheme-name>" -VMName "<vm-
name>" -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"DeploymentSchema`" Value=`"1.1`" /
></CustomProperties>
```

2. `Set-ProvVMUpdateTimeWindow` を実行して更新を適用します。この例では、更新はVMの次回の電源投入時に適用されます。

```
Set-ProvVmUpdateTimeWindow -ProvisioningSchemeName "<provscheme-name>"
-VMName "<vm-name>"
```

3. VMの電源をオンにします。

トラブルシューティング

VMがアンマネージドディスクからマネージドディスクへの変換に失敗した場合:

- `UseManagedDisks` または `DeploymentSchema` のカスタムプロパティが正しく設定されていることを確認します:
  - `Set-ProvScheme` を使用している場合は、`Get-ProvScheme` を実行してProvSchemeカスタムプロパティを確認します。詳細については、Get-ProvSchemeを参照してください。
  - `Set-ProvVM` を使用している場合は、`Get-ProvVMConfiguration` を実行して、更新されたカスタムプロパティを持つ新しい構成がVMにあることを確認します。詳細については、Set-ProvVMを参照してください。
- Azureサービスプリンシパルに次のアクセス許可が存在することを確認します:
  - `Microsoft.Compute/virtualMachines/convertToManagedDisks/write`
- `Get-ProvOperationEvent` を実行して、プロビジョニングスキームの警告を表示します。詳細については、Get-ProvOperationEventを参照してください。例:

```
Get-ProvOperationEvent -LinkedObjectType ProvisioningScheme
-LinkedObjectUid <your-provscheme-id>
```

次の手順

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成に誘導します
- 構成プロセス全体を確認するには、インストールと構成を参照してください
- カタログを管理するには、マシンカタログの管理およびMicrosoft Azureカタログの管理を参照してください

詳細情報

- 接続とリソースの作成および管理
- マイクロソフト アジュール リソース マネージャーへの接続
- マシンカタログの作成

マイクロソフト システムセンター バーチャルマシンマネージャー カタログの作成

マシンカタログの作成では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Microsoft System Center Virtual Machine Manager（VMM）仮想化環境に固有の詳細を扱っています。

> **注:**
>
> VMMカタログを作成する前に、VMMへの接続の作成を完了する必要があります。Microsoft System Center Virtual Machine Managerへの接続を参照してください。

マスターVMの作成

1. マスターVMにVDAをインストールし、パフォーマンスを向上させるためにデスクトップを最適化するオプションを選択します。
2. バックアップとして使用するために、マスターVMのスナップショットを作成します。
3. 仮想デスクトップを作成します。

SMB 3ファイル共有上のMCS

VMストレージにSMB 3ファイル共有上のMCSで作成されたマシンカタログの場合、資格情報が以下の要件を満たしていることを確認してください。これらの要件により、ControllerのHypervisor

Communications Library（HCL）からの呼び出しがSMBストレージに正常に接続されることが保証されます。

- VMMユーザーの資格情報には、SMBストレージへの完全な読み取り/書き込みアクセス権が含まれている必要があります。
- VMライフサイクルイベント中のストレージ仮想ディスク操作は、VMMユーザー資格情報を使用してHyper-Vサーバー経由で実行されます。

SMBストレージを使用する場合、Controllerから個々のHyper-Vマシンへの認証資格情報セキュリティサポートプロバイダー（CredSSP）を有効にします。このプロセスは、Windows Server 2012上のHyper-VとVMM 2012 SP1で使用します。詳細については、CTX137465を参照してください。

HCLは`CredSSP`を使用してHyper-Vマシンへの接続を開きます。この機能は、Kerberosで暗号化されたユーザー資格情報をHyper-Vマシンに渡します。リモートHyper-Vマシン上のセッションでの**PowerShell**コマンドは、提供された資格情報（この場合はVMMユーザーの資格情報）で実行され、ストレージへの通信コマンドが正しく機能するようにします。

以下のタスクでは、HCLで生成され、SMB 3.0ストレージに対して動作するようにHyper-Vマシンに送信されるPowerShellスクリプトを使用します。

- **マスターイメージの統合**: マスターイメージは、MCSプロビジョニングスキーム（マシンカタログ）を作成します。新しく作成されたディスクからVMを作成できるようにマスターVMをクローンしてフラット化します（そして元のマスターVMへの依存関係を削除します）。

  root\\virtualization\\v2名前空間のConvertVirtualHardDisk

  例:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)

$result
```

- **差分ディスクの作成:** マスターイメージを統合して生成されたマスターイメージから差分ディスクを作成します。その後、差分ディスクは新しいVMに接続されます。

  root\\virtualization\\v2名前空間のCreateVirtualHardDisk

  例:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.CreateVirtualHardDisk($vhdastext);

$result
```

- **IDディスクのアップロード:** HCLはIDディスクをSMBストレージに直接アップロードできません。そのため、Hyper-VマシンがIDディスクをストレージにアップロードしてコピーする必要があります。Hyper-VマシンはControllerからディスクを読み取ることができないため、HCLはまず次のようにHyper-Vマシン経由でIDディスクをコピーする必要があります。

  a. HCLは、管理者共有を介してIDをHyper-Vマシンにアップロードします。

  b. Hyper-Vマシンは、PowerShellリモートセッションで実行されているPowerShellスクリプトを介して、ディスクをSMBストレージにコピーします。Hyper-Vマシン上にフォルダーが作成され、そのフォルダーのアクセス許可はVMMユーザーのみにロックされます（リモートPowerShell接続を介して）。

  c. HCLは、管理者共有からファイルを削除します。

  d. HCLがIDディスクのHyper-Vマシンへのアップロードを完了すると、リモートPowerShellセッションはIDディスクをSMBストレージにコピーします。その後、Hyper-Vマシンから削除します。

  IDディスクフォルダーは、削除された場合でも再利用できるように再作成されます。

- **IDディスクのダウンロード**: アップロードと同様に、IDディスクはHyper-Vマシンを介してHCLに渡されます。以下のプロセスでは、Hyper-Vサーバー上にVMMユーザー権限のみを持つフォルダーが存在しない場合に作成します。

  a. Hyper-Vマシンは、PowerShellスクリプトを介して、ディスクをSMBストレージからローカルのHyper-Vストレージにコピーします。このスクリプトは、PowerShell V3リモートセッションで実行されます。

  b. HCLは、Hyper-Vマシンの管理者共有からディスクをメモリに読み込みます。

  c. HCL は管理者共有からファイルを削除します。

マシンプロファイルを使用してカタログを作成する

System Center Virtual Machine Manager (SCVMM) 環境では、マシンプロファイルを使用して MCS マシンカタログを作成および更新できます。vTPM を有効にできます。また、マシンプロファイル VM のカスタムタグをプロビジョニングされた VM に追加することもできます。

重要な考慮事項

- マスターイメージはスナップショットのみで、VM にすることはできません。
- マシンプロファイルのソースとして使用できるのは VM のみです。
- VTPM は Hyper-V コンソールから構成でき、SCVMM コンソールからは構成できません。
- マスターイメージで vTPM が有効になっている場合、マシンプロファイルソースで vTPM を有効にする必要があります。
- vTPM は第2世代のマシンでのみサポートされています。
- 以下のパラメータは、個別に指定された場合、マシンプロファイルでキャプチャされた値を上書きします。
  - VMCpuCount
  - VMMemoryMB
  - ディスクストレージ
- カスタムタグは、マスターイメージからではなく、マシンプロファイルからのみ継承されます。`CitrixProvisioningSchemeId` タグはデフォルトで VM に追加されます。`CitrixProvisioningSchemeId` タグを含めたくない場合は、ホスティングユニットの作成時に `-NoVmTagging` パラメータを追加します。例:

```
New-Item -HypervisorConnectionName  $ConnectionName `

    -NetworkPath @($NetworkPath) `

    -Path @($HostingUnitPath) `

    -PersonalvDiskStoragePath @() `

    -RootPath $RootPath `

    -StoragePath @($StoragePath) `

    -NoVmTagging

    ```
```

- `Set-ProvScheme` コマンドを使用して、既存のカタログを更新できます。
```

- MCSIO が有効になっている場合、MCS カタログの作成後にメモリとディスクキャッシュのサイズを更新できます。

マシンプロファイルを使用してマシンカタログを作成する

1. マシンプロファイルのソースとなるVMを作成します。詳細については、「VMM ファブリックで仮想マシンをプロビジョニングする」を参照してください。**世代**は一度選択すると変更できません。SCVMM で次の操作を実行できます。
   - vTPM を有効にするには:
     a. VM を作成したら、Hyper-V ホストにログインし、**Hyper-V マネージャー**でVMを見つけます。
     b. VM を右クリックし、**設定**に移動します。
     c. **セキュリティ**で、**トラステッドプラットフォームモジュールを有効にする**チェックボックスをオンにします。
2. **PowerShell** ウィンドウを開きます。
3. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix®*` を実行します。
4. ブローカーカタログを作成します。このカタログには、これから作成されるマシンが格納されます。
5. ID プールを作成します。これは、作成されるマシン用に作成された AD アカウントのコンテナになります。
6. マシンプロファイルを使用してプロビジョニングスキームを作成します。例:

```
New-ProvScheme -HostingUnitName "<hostingunit name>"

-IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1\<path
to the checkpoint/snapshot>"

-ProvisioningSchemeName "<catalogname>"  -MachineProfile "XDHyp:\<path
to the machine profile VM>"
```

7. プロビジョニングスキームの一意の ID でブローカーカタログを更新します。
8. VM を作成してカタログに追加します。

既存のカタログを更新する

Set-ProvSchemeコマンドを使用して、既存のカタログを更新できます。例：

```
Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile
"XDHyp:\<path to the machine profile VM>"
```

VMを削除する

カタログからVMを削除しても、SCVMMからVMを削除しない選択ができます。この場合、`CitrixProvisioningSchemeId`タグはVMからのみ削除されます。カスタムタグはVMから削除されません。Web StudioまたはPowerShellコマンドを使用してVMを削除できます。

WEB STUDIO を使用して VM を削除する

1. VMを選択して右クリックします。
2. **削除**」をクリックします。
3. **仮想マシンをカタログから削除しますが、仮想マシンは削除しません**を選択します。

POWERSHELLコマンドの使用

`ForgetVM`パラメーターを指定した`Remove-ProvVM`。詳細については、以下を参照してください。

- タグを削除する
- ハイパーバイザーアクセスなしでマシンを削除する

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループを作成するように案内します。
- 構成プロセス全体を確認するには、インストールと構成を参照してください。
- カタログを管理するには、マシンカタログを管理するおよびMicrosoft System Center Virtual Machine Managerカタログを管理するを参照してください。

詳細情報

- 接続とリソースの作成および管理
- マイクロソフト システムセンター バーチャルマシンマネージャー への接続
- マシンカタログの作成

Nutanixカタログを作成する

(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create)は、マシンカタログを作成するウィザードについて説明しています。以下の情報は、Nutanix仮想化環境に特化した詳細を扱っています。

> **注:**
>
> Nutanixカタログを作成する前に、Nutanixへの接続の作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/connections/connection-nutanix)を参照してください。

Nutanixマシンテンプレートバージョンを使用してマシンカタログを作成する

Citrix管理のNutanix AHV Prism Centralホスト接続を使用してMCSプロビジョニングされたマシンカタログを作成する場合、ベースイメージはNutanix VMテンプレートバージョンから作成されます。主な利点は、Nutanix Prism CentralがVMテンプレートを複数のクラスター間で利用できることです。その結果、Citrix管理者は、それらのカタログが異なるNutanixクラスター上にある場合でも、単一のNutanix VMテンプレートバージョンを複数のMCSマシンカタログのマスターVMとして使用できます。

テンプレートバージョンをマシンプロファイルのソースとして選択することもできます。マスターイメージのテンプレートバージョンは、新しいカタログのマシンプロファイルのデフォルトとなります。ただし、マシンプロファイルのテンプレートバージョンを変更することは可能です。以下のハードウェアプロパティがマシンプロファイルから取得されます：CPU、メモリ、ソケットあたりのコア数、GPU、およびカテゴリ。オプションで、CPU、メモリ、ソケットあたりのコア数のプロパティを指定して、選択したマシンプロファイルの設定を上書きすることもできます。

> **注:**
>
> カテゴリは、仮想マシン、クラスター、イメージなどのエンティティをグループ化および管理し、ポリシーや自動化を適用するために使用されるキーと値のペアです。

> カタログを作成する前に、マスターVMを作成し、Nutanix Prism CentralでVMテンプレートバージョンに変換してください。手順については、Nutanixのドキュメントを参照してください。

以下の方法でカタログを作成できます。

- (#create-a-machine-catalog-using-web-studio)。既存のVMを使用してカタログを作成することもできます。(#create-a-machine-catalog-with-existing-machines-power-managed)を参照してください。
- (#create-a-machine-catalog-using-powershell-commands)

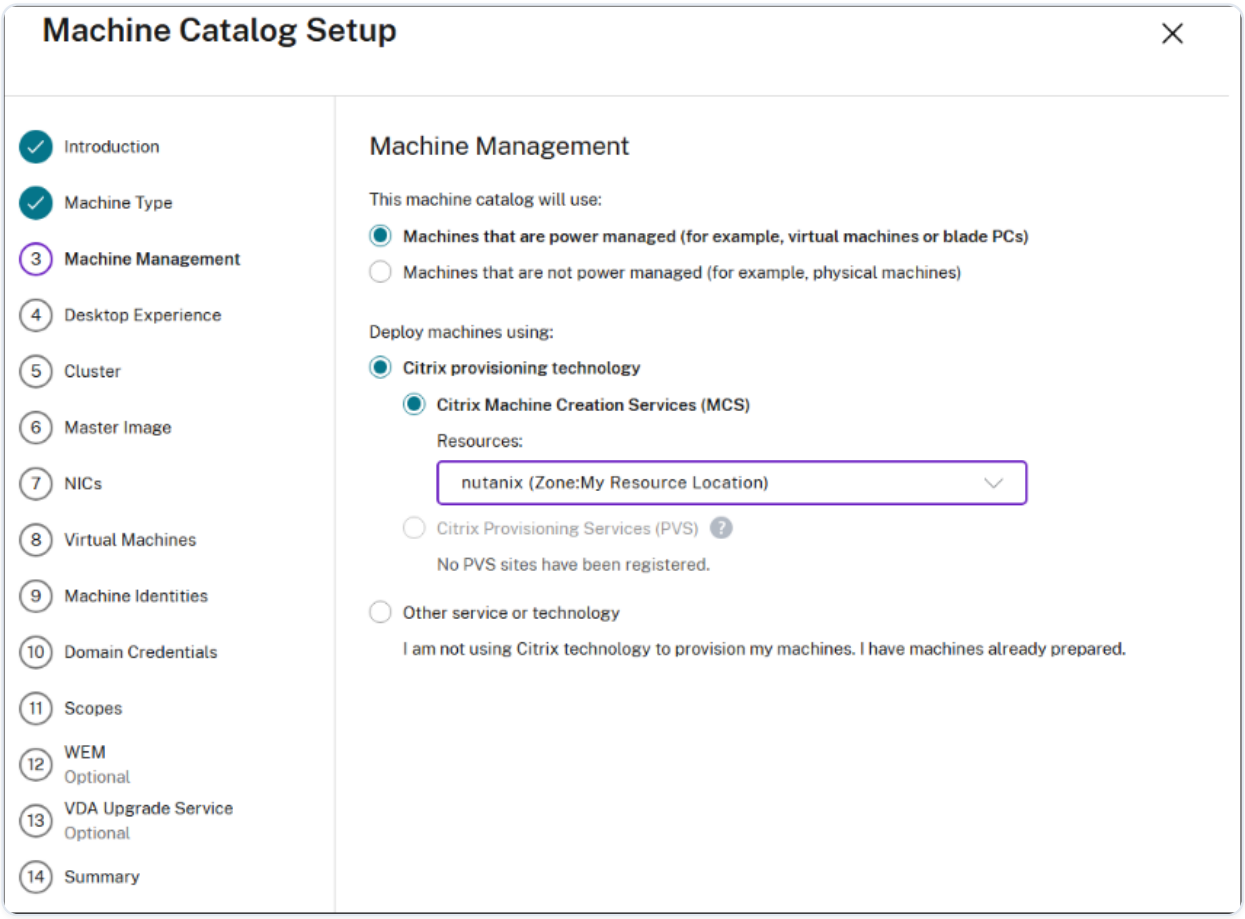
制限事項

- 同じサブネットに複数のNICを接続することはサポートされていません。
- Nutanixの制限により、各MCSプロビジョニング済みマシンカタログには、オーバーレイネットワーク、VLANベーシックサブネット、VLANサブネットの中から、単一タイプのネットワークのNICのみを割り当てることができます。
- 一部のシナリオでは、非永続マシンカタログのMCSマスターイメージを更新すると、潜在的な問題を引き起こす可能性があります。詳細については、「Secure Boot and vTPM in Nutanix Prism Central」を参照してください。
- Nutanix VMテンプレートをマスターイメージとして選択する場合、テンプレート名またはテンプレートバージョン名に**#** や **&** のような文字を含めてはなりません。

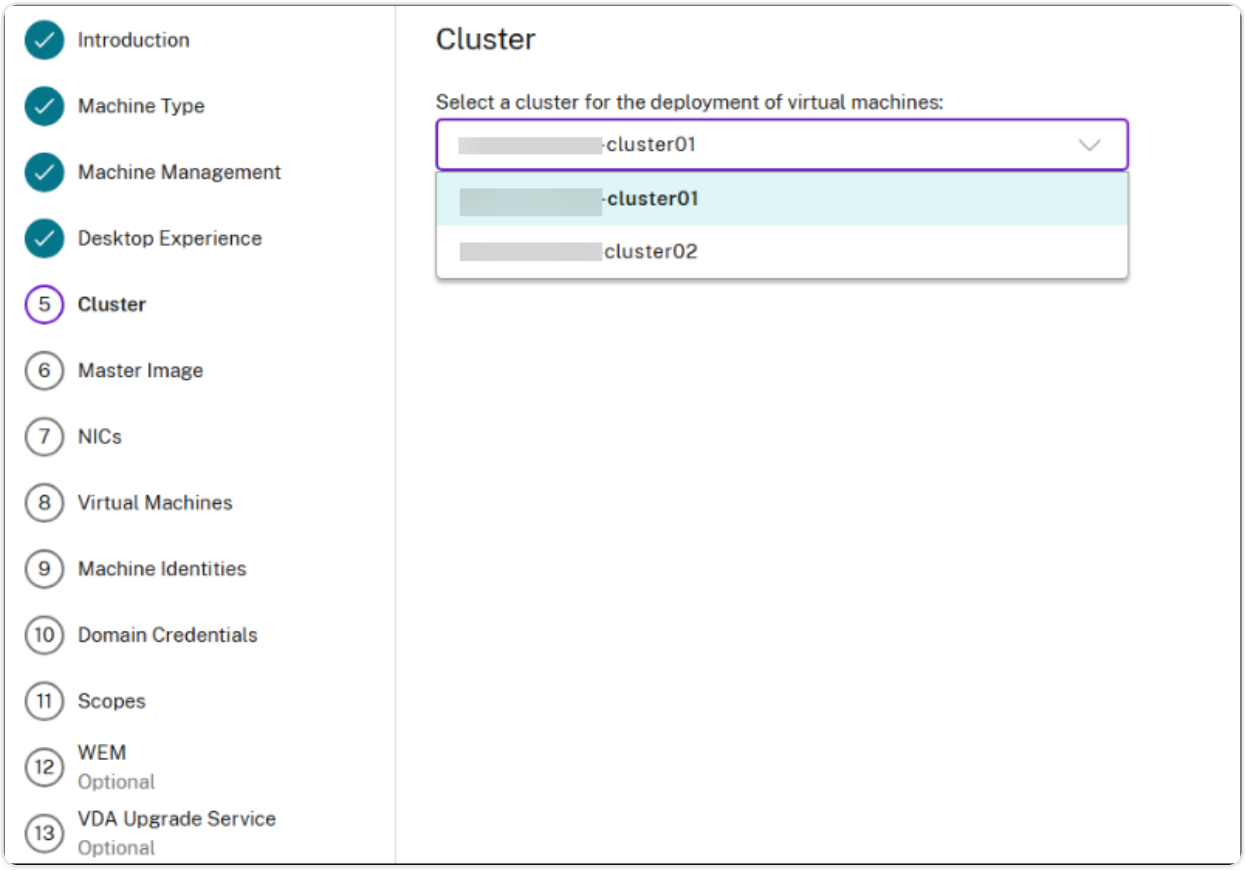
Web Studioを使用してマシンカタログを作成する

マシンカタログセットアップウィザードで：

1. **マシンタイプ**ページで、**マルチセッションOS**、**シングルセッションOS**、または**リモートPCアクセス**を選択します。
2. **マシン管理**ページで、展開方法として**電源管理されているマシン**と**Citrix Machine Creation Services™**を選択します。**リソース**を選択します。

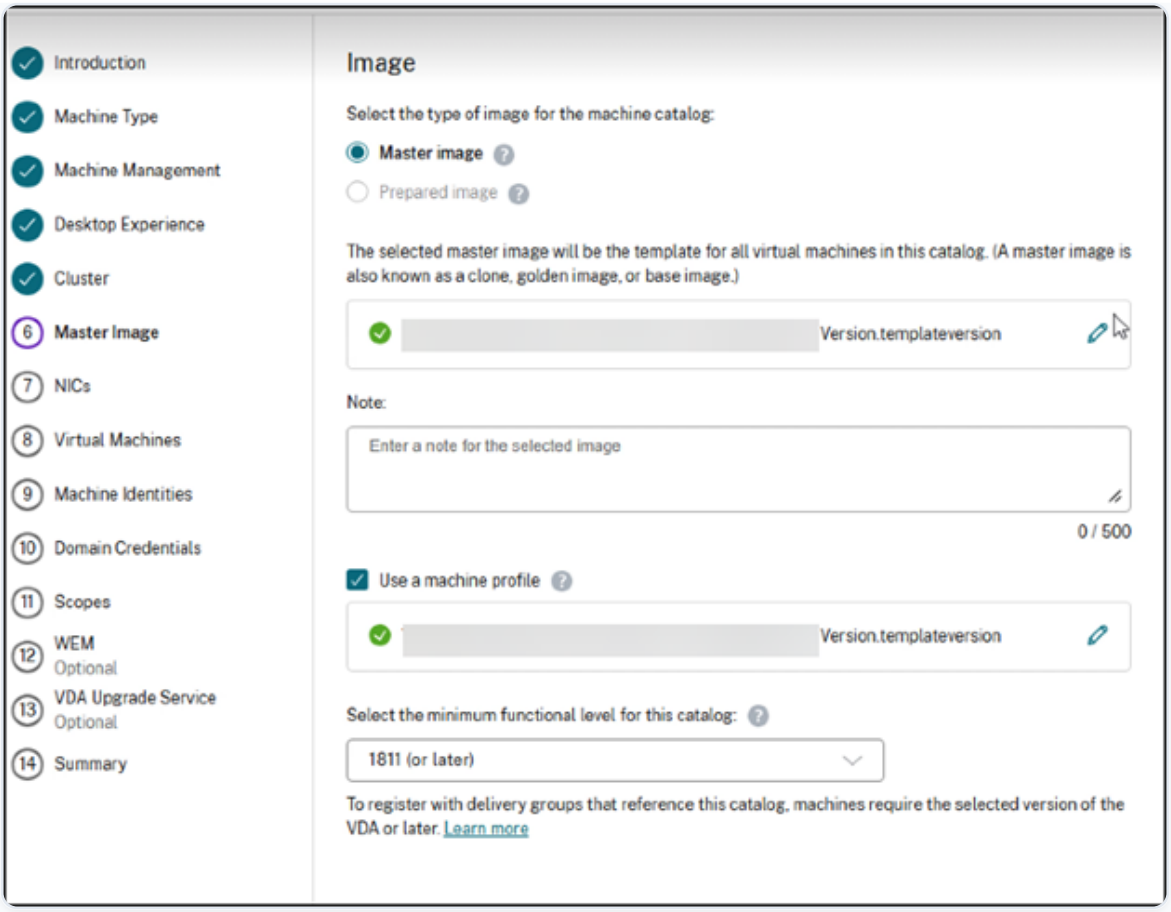


3. **デスクトップエクスペリエンス**ページで、2つのオプションのいずれかを選択します。
4. **クラスター**ページで、VMの展開に使用するクラスターを選択します。

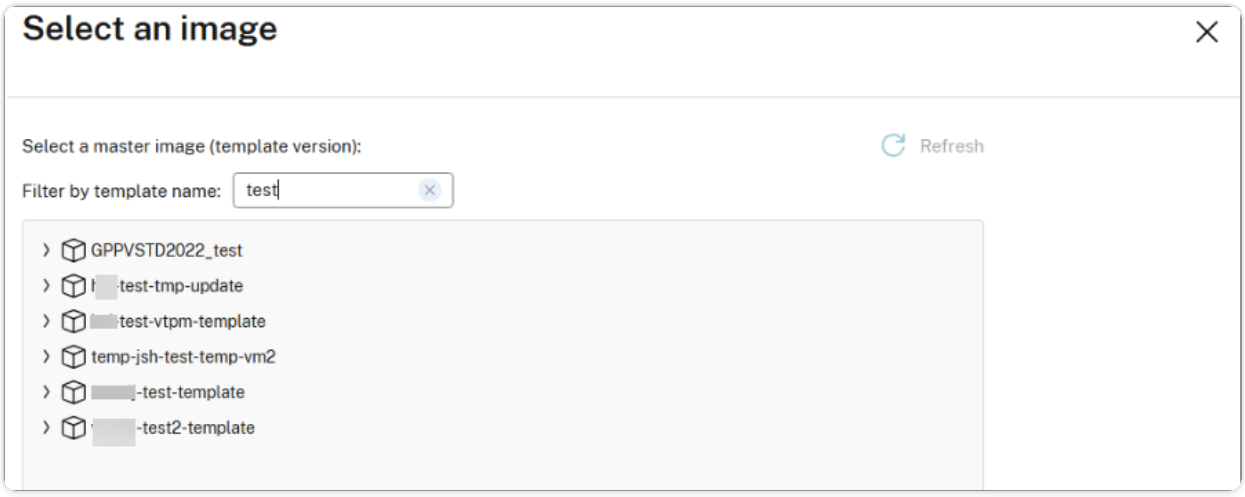


5. **マスターイメージ**ページで、**マスターイメージ**をクリックし、マスターイメージ（テンプレートバージョン）を選択します。マシンテンプレートを名前でフィルタリングできます。マスターイメージのテンプレートバージョンは、新しいカタログのマシンプロファイルとしてデフォルトで設定されます。ただし、マシンプロファイルのテンプレートバージョンを変更できます。

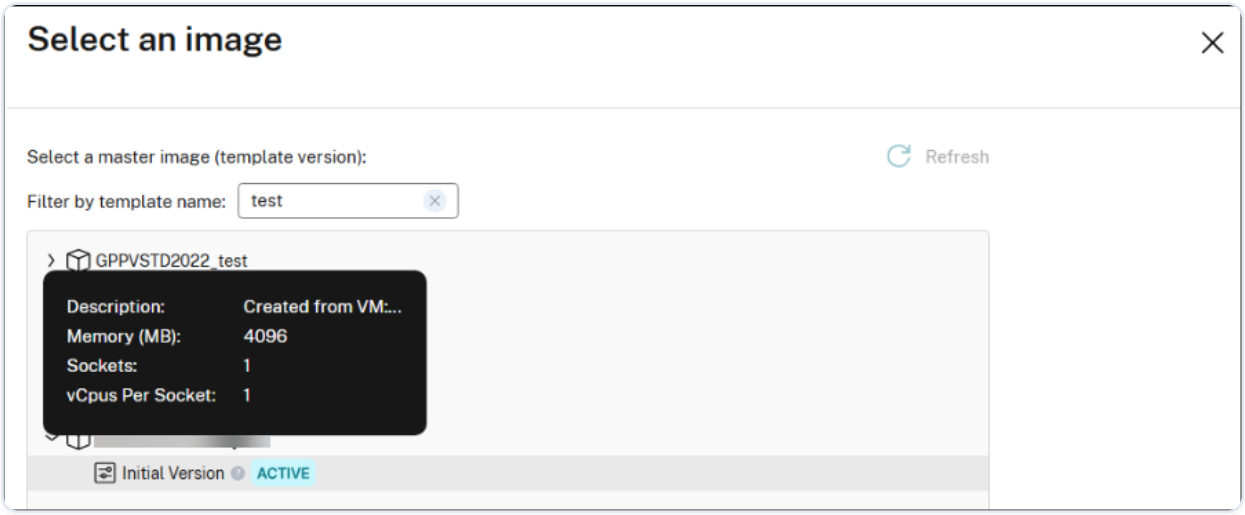
> **注:**
>
> 単一のNutanix VMテンプレートバージョンを、複数のMCSマシンカタログのマスターVMとして使用できます。それらのカタログが異なるNutanixクラスター上にある場合でも同様です。



名前でマシンテンプレートをフィルタリングする:

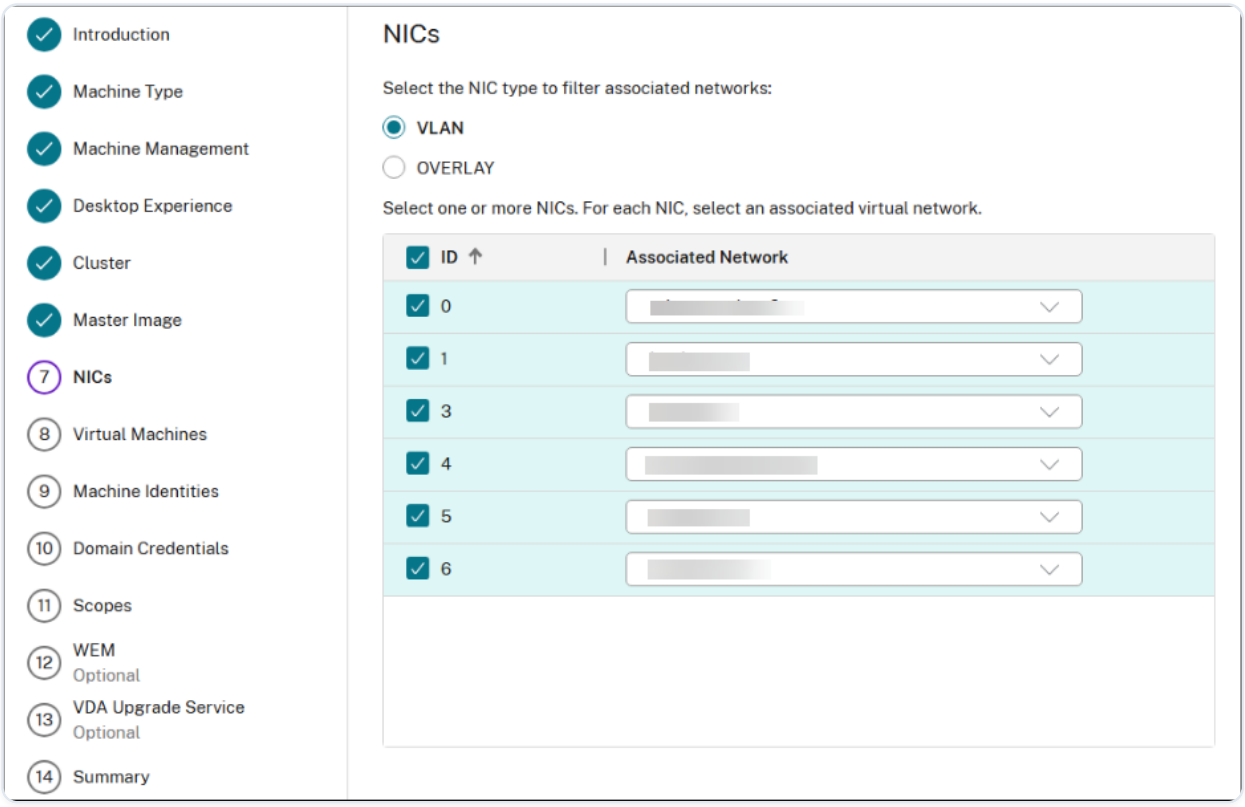


テンプレートの説明を参照してください:



6. **NIC**ページで:

   - 関連付けられたネットワークをフィルタリングするためにNICタイプを選択します。
   - マスターイメージに含まれる1つ以上のNICを選択し、各NICに関連付けられた仮想ネットワークを選択します。



7. **仮想マシン**ページで、作成する仮想マシンの数を示し、各マシンの合計メモリ (MB)、仮想CPU、およびCPUあたりのコア数を構成します。これらの値は、マシンプロファイルから自動的に入力されます。
8. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。

マシンプロファイルのエクスポート

マシンカタログで使用されているマシンプロファイルをJSONファイルにエクスポートできます。

1. マシンカタログを選択し、**テンプレートプロパティ**タブに移動します。
2. **マシンプロファイル**の詳細で、**最終バージョン**の横にある**エクスポート**をクリックします。

PowerShellコマンドを使用してマシンカタログを作成する

1. PowerShell ウィンドウを開きます。
2. `asnp citrix*` を実行します。
3. まだ作成されていない場合は、ID プールを作成します。例:

```
New-AcctIdentityPool    -Domain "<string>" -IdentityPoolName "<string>"
-IdentityType "ActiveDirectory"  -NamingScheme "DemoVM-##"
-NamingSchemeType "Numeric" -ZoneUid "GUID" -Scope @()
```

4. プロビジョニングスキームを作成します。

例: マシンプロファイルなし

```
New-ProvScheme -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"ClusterId`"
Value=`"00062c63-1fb0-58c9-4fc8-5c2573352378`" /><Property
xsi:type=`"StringProperty`" Name=`"CPUCores`" Value=`"1`" /></
CustomProperties>" -HostingUnitName "<Hosting unit name>"
-IdentityPoolName "<string>" -InitialBatchSizeHint 1  -MasterImageVM
"XDHyp:\HostingUnits\<Hosting Unit Name>\Templates.folder\<template
name>.template\<template version name>.templateversion" -NetworkMapping
@{"5"="XDHyp:\HostingUnits\<Hosting unit name>\Clusters.folder\<Cluster
Name>.cluster\<Network name>.network"} -ProvisioningSchemeName
"<Catalog name>" -ProvisioningSchemeType "MCS" -RunAsynchronously
-Scope @() -VMCpuCount 2 -VMMemoryMB 10240
```

例: マシンプロファイルあり

マシンプロファイルを使用して、テンプレートバージョンからハードウェアプロパティをキャプチャし、プロビジョニングされたVMに適用します。マシンプロファイルを指定しない場合、ハードウェアプロパティはマスターイメージテンプレートバージョンからキャプチャされます。

注:

- OSディスク、vTPM、およびセキュアブートのプロパティは、マシンプロファイルが使用されている場合でも、常にマスターイメージからキャプチャされます。
- OSディスクはマシンプロファイルから読み取られないため、ディスクレスVMを作成し、それをマシンプロファイルに使用できるテンプレートバージョンに変換できます。
- マシンプロファイルテンプレートバージョンの完全なJSON仕様が保存されているため、Prism Centralからテンプレートバージョンを削除してもVMを作成できます。

マシンプロファイルからキャプチャされるプロパティは次のとおりです。

プロパティ	APIでのプロパティ名 (GETTEMPLATEVERSIONBYID)	コメント/参照
CPU	numSockets	
RAM	memorySizeBytes	
コア	numCoresPerSocket	
カテゴリ	カテゴリ	カテゴリ管理
GPU	GPU	GPU概要ビュー
コアあたりのスレッド数	numThreadsPerCore	aCLI-VM
NUMAノード	numNumaNodes	
VCPUハードピンニングを有効にする	isVcpuHardPinningEnabled	
CPUパススルーを有効にする	isCpuPassthroughEnabled	
メモリオーバーコミットを有効にする	isMemoryOvercommitEnabled	Prism Central (AHV) を使用した VM の作成
GPUコンソールアクセスを有効にする	isGpuConsoleEnabled	
CPUホットプラグを有効にする	isCpuHotplugEnabled	
SCSIコントローラーを有効にする	isScsiControllerEnabled	
タイムゾーン	hardwareClockTimezone	Prism Central (AHV) を介したVMの作成
AHVブランディングを有効にする	isBrandingEnabled	

プロパティ	APIでのプロパティ名 (GETTEMPLATEVERSIONBYID)	コメント/参照
VGAコンソールを有効にする	isVgaConsoleEnabled	
VM	isAgentVm	Prism Central (AHV) を介したVMの作成

注記:

同じマスターイメージテンプレートバージョンを使用して、さまざまなマシンプロファイルを持つ異なるカタログを作成できます。各プロファイルには、上記の異なるプロパティセットが含まれます。たとえば、Nutanixポリシーにリンクできる異なるカテゴリを割り当てたり、CPU/メモリを調整したり、メモリオーバーコミット設定を変更したり、複数のGPUを追加または削除したりできます。

`CustomProperties`の`VMCpuCount`、`VMMemoryMB`、`CPUCores`などのコマンドラインパラメーターは、指定することができ、これらのパラメーターの値はマシンプロファイルテンプレートバージョンよりも優先されます。指定しない場合、これらは指定されたマシンプロファイルから読み取られます。

```
$customProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <StringProperty Name="ClusterId"
Value="00062c63-1fb0-58c9-4fc8-5c2573352378" />

    <StringProperty Name="CPUCores" Value="2" />

</CustomProperties>

"@
```

```
New-ProvScheme -HostingUnitName "<Hosting unit name>" `

           -IdentityPoolName "<string>" `

           -InitialBatchSizeHint 1 `

           -MasterImageVM "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<template name>.template\<template version
name>.templateversion" `

           -MachineProfile "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<template name for machine
profile>.template\<template version name>.templateversion" `

           -NetworkMapping @{"0"="XDHyp:\HostingUnits\<Hosting unit
name>\Clusters.folder\<Cluster Name>.cluster\<Network name>.network"} `

           -ProvisioningSchemeName "<Catalog name>" `

           -ProvisioningSchemeType "MCS" `

           -CustomProperties $customProperties `

           -RunAsynchronously `

           -VMCpuCount 2 `

           -Scope @()
```

5. プロビジョニングスキームをブローカーカタログとして登録します。例:

```
New-BrokerCatalog -AllocationType "Random" -IsRemotePC $False  -
MinimumFunctionalLevel "L7_20" -Name "<Catalog Name>"
-PersistUserChanges "Discard" -ProvisioningType "MCS"    -
SessionSupport "MultiSession" -ZoneUid "GUID"  -ProvisioningSchemeId
fe7df345-244e-4xxxx-xxxxxxxxx `  -Scope @()
```

既存のマシンでマシンカタログを作成する（電源管理対象）

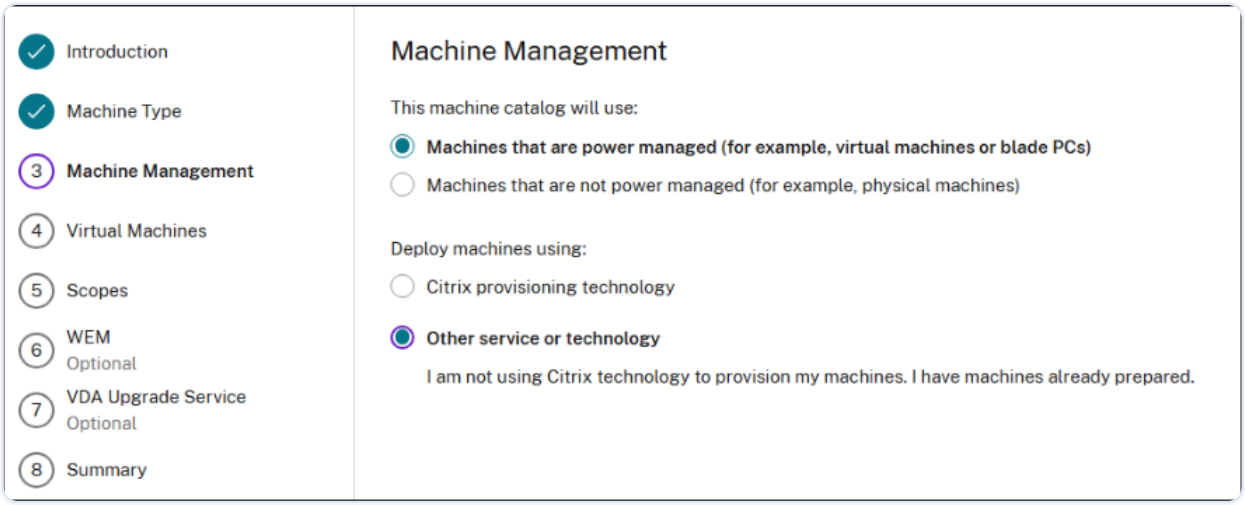
既存のマシン（電源管理）を使用してマシンカタログを作成できます。

- ウェブスタジオ
- PowerShell

Web Studio を使用して既存のマシン（電源管理）でマシンカタログを作成する

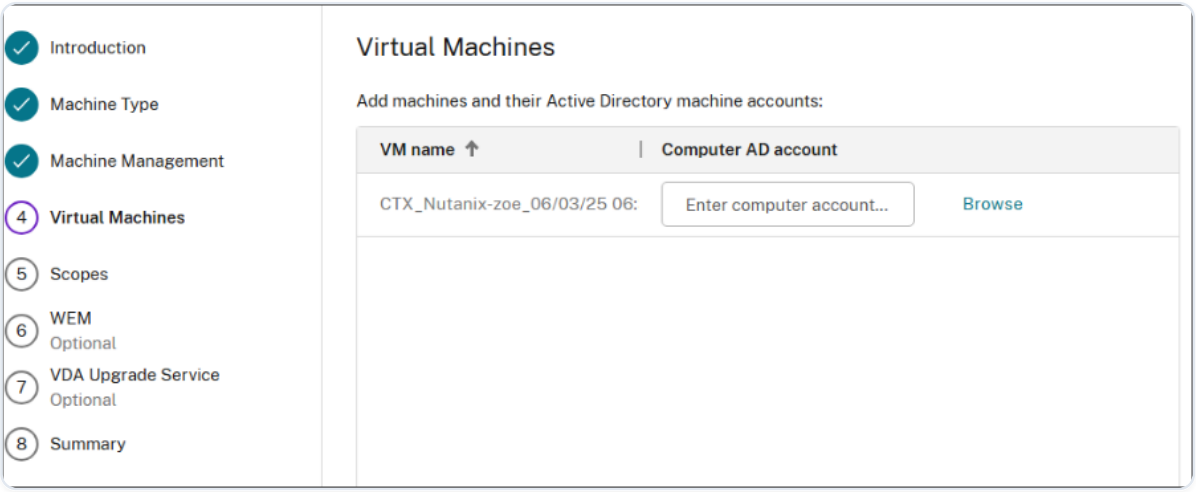
マシンカタログセットアップウィザードで：

1. **オペレーティングシステム**ページで、**マルチセッションOS**または**シングルセッションOS**を選択します。
2. **マシン管理**ページで、**電源管理されているマシン**と**その他のサービスまたはテクノロジー**を選択します。



3. **仮想マシン**ページで、マシンとそのActive Directoryマシンアカウントを追加します。次のいずれかを実行できます。

   - **CSVファイルからインポート**をクリックして、マシンを一括追加します。
   - **マシンの追加**をクリックして、マシンを手動で追加します。**VMの選択**ウィンドウが表示されます。以前に作成したNutanix AHV Prism Central接続を展開し、追加するVMを選択します。次に、関連するマシンアカウント名を追加します。



4. **スコープ**ページと**概要**ページには、Nutanix AHV Prism Centralに固有の情報は含まれていません。

PowerShell を使用して既存のマシン（電源管理）でマシンカタログを作成する

1. PowerShellウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. ユーザーに割り当てられる電源管理されたVMを持つカタログを作成します。例:

```
New-BrokerCatalog -AllocationType "Permanent"  -IsRemotePC $False
-MachinesArePhysical $False  -Name "<Catalog Name>" -PersistUserChanges
"OnLocal" -ProvisioningType "Manual" -Scope @() -SessionSupport
"SingleSession" -ZoneUid "fb202053-8c35-4db2-a299-a8d9538ec6be"
```

4. カタログにVMを追加します。例:

```
New-BrokerMachine  -CatalogUid 6 -HostedMachineId "d859caf3-4bf0-447b-
b012-8af0594c7d88" -HypervisorConnectionUid 1 -IsReserved $False  -
MachineName "S-1-5-21-1334627847-1250330507-3910179295-100245"
```

Nutanixスナップショットを使用してマシンカタログを作成する

このセクションでは、Nutanix Acropolis（Prism Element）ホスト接続を使用してMCSプロビジョニングされたマシンカタログを作成する方法について説明します。カタログを作成する前に、Nutanixでマスターイメージとスナップショットを作成してください。詳しくは、Nutanixのドキュメントを参照してください。

マシンカタログセットアップウィザードで:

- **Container**または**Cluster and Container**ページはNutanix固有です。
  - Nutanix AHV XIをリソースとして使用してマシンを展開する場合、**Container**ページで、VMのIDディスクが配置されるコンテナを選択します。
  - Nutanix AHV PCをリソースとして使用してマシンを展開する場合、**Cluster and Container**ページが表示されます。VMの展開に使用するクラスターを選択し、次にコンテナを選択します。
- **Image**ページで、イメージスナップショットを選択します。必要に応じて、Acropolisコンソールを使用してスナップショットの名前を変更します。スナップショットの名前を変更した場合は、カタログ作成ウィザードを再起動して、更新されたリストを表示してください。

- **Virtual Machines**ページで、仮想CPUの数とvCPUあたりのコア数を指定します。
- **NICs**ページで、関連するネットワークをフィルター処理するNICタイプを選択します。このオプションは、Nutanix AHV PC接続でのみ利用可能です。
- **Machine Identities**、**Domain Credentials**、**Scopes**、および**Summary**ページには、Nutanix固有の情報は含まれていません。

制限事項

Nutanixホスト接続（特にNutanix AHVプラグイン2.7.1およびNutanix AHVプラグイン2.5.1）でMCSカタログを作成すると、プロビジョニングされたVMのハードディスクサイズがWeb Studioに誤って表示されます。

- Nutanix AHV プラグイン 2.7.1: 表示されるサイズは、実際のストレージサイズよりも小さい (1 GB)。
- Nutanix AHV プラグイン 2.5.1: 表示されるサイズは、実際のストレージサイズよりも小さい (32 GB)。

ただし、マスターイメージVMがVM内のスナップショットである場合、これは設計どおりに機能します。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、インストールと構成を参照してください。
- カタログを管理するには、マシンカタログの管理およびNutanixカタログの管理を参照してください。

詳細情報

- 接続とリソースの作成および管理
- Nutanixへの接続
- Nutanixクラウドおよびパートナーソリューションへの接続
- マシンカタログの作成

Red Hat OpenShiftカタログを作成する

「(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create.html)」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Red Hat OpenShift仮想化環境に固有の詳細を扱っています。

注:

Red Hat OpenShiftカタログを作成する前に、Red Hat OpenShiftへの接続とホスティングユニットの作成を完了してください。「(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/connections/connection-redhat-openshift.html)」を参照してください。

マスターイメージVMを作成する

マシンカタログを作成するには、マスターイメージVMが必要です。

1. ログインIDを使用してOpenShiftコンソールにアクセスします。
2. **Virtualization > VirtualMachines**に移動して、マスターイメージVMを含むVMのリストを表示します。
3. マスターイメージを作成します。マスターイメージを作成する際は、マスターイメージVMにストレージデバイスが1つだけであることを確認してください。

注:

- クラスター環境に対する顧客の要件に従って、ルーティング可能なNADがマスターイメージVMに追加されていることを確認してください。
- マスターイメージがドメインに参加している場合、カタログ作成に使用された後、ドメイン信頼が失われる可能性があります。この問題は、OpenShift環境の制限により、Citrix Virtual Apps and Desktops™ 2503に影響します。回避策は、マスターイメージでドメインに参加しないことです。Citrixは、ネットワーク分離機能を強化するためにRed Hatと協力しています。
- Red Hat OpenShift仮想化環境でMCSマシンカタログを作成する場合、異なるオペレーティングシステムタイプを持つマスターイメージとマシンプロファイルを使用することはできません。これは、Red Hat OpenShiftが各OSタイプを管理する方法によるものです。したがって、マスターイメージとしてWindows VMを使用し、マシンプロファイルとして非Windows（例：Linux）VMを使用すること、またはその逆はサポートされていません。
- 現在、`InstanceType`を使用して作成されたVMは、マスターイメージとしてサポートされていません。

カタログを作成する

OpenShift環境でマシンを作成、配信、電源管理するためにOpenShiftカタログを作成できます。

- Web Studio を使用してカタログを作成する(#create-a-catalog-using-web-studio)
- PowerShellコマンドを使用してカタログを作成する(#create-a-catalog-using-powershell-commands)

Web Studioを使用してカタログを作成する

Web Studioを使用して、マシンプロファイルありまたはなしでRed Hat OpenShift環境にMCSマシンカタログを作成できます。VMはマシンプロファイルの入力として使用されます。

マシンカタログセットアップウィザードで：

1. **「Operating System」**ページで、**「Multi-session OS」**または**「Single-session OS」**を選択します。
2. 「Machine Management」ページで、次の操作を行います。
   - **「電源管理されているマシン（例：仮想マシンまたはブレードPC）」**を選択します。
   - **Citrixプロビジョニングテクノロジー**Citrix Machine Creation Services™ (MCS)**を使用してマシンを展開することを選択します。
   - Citrix Machine Creation Services (MCS) の下にあるOpenshiftホスティングユニットを選択します。
3. **「Desktop Experience」**ページで、**「Machine Type」**ページで選択したマシンタイプに応じてオプションを選択します。
4. **Image** ページで:
   a. マスターイメージを選択します。現在、Openshiftは準備済みイメージをサポートしていません。
   b. 選択したイメージにメモを追加できます。
   c. 「マシンプロファイルを使用」チェックボックスをオンにして、マシンプロファイルを選択できます。
   d. 最新の製品機能を使用できるようにするには、マスターイメージに最新のVDAバージョンがインストールされていることを確認してください。デフォルトの最小VDA選択を変更しないでください。ただし、以前のVDAバージョンを使用する必要がある場合は、「VDAバージョンと機能レベル」を参照してください。
5. **NIC**ページで、1つまたは複数のNICを選択し、各カードに仮想ネットワークを関連付けます。

6. **仮想マシン**ページで、次の操作を行います。

    a. 作成する仮想マシンの数を指定します。作成しない場合は0（ゼロ）を入力します。後で、マシンを追加して空のカタログのVMを作成できます。

    b. 各VMのメモリ量（MB単位）を選択します。

    c. ランダムな非永続カタログを作成している場合、I/Oパフォーマンスを向上させるために、マシンのライトバックキャッシュを有効にできます。「一時データのキャッシュを構成する」(/ja-jp/citrix-daas/install-configure/machine-catalogs-create.html#configure-cache-for-temporary-data)を参照してください。

7. 画面の指示に従って、OpenShift固有の情報を含まない残りの手順を完了します。

Studioを使用してOpenShiftカタログを作成し、OpenShift環境内の既存のマシンの能力を提供および管理することもできます。次の手順を実行します。

マシンカタログセットアップウィザードで：

1. **オペレーティングシステム**ページで、**マルチセッションOSまたはシングルセッションOS**を選択します。
2. **マシン管理**ページで、**電源管理されているマシンと別のサービスまたはテクノロジ**を選択します。
3. **仮想マシン**ページで、マシンとそのActive Directoryマシンアカウントを追加します。次のことができます。

    - *マシンを手動で追加する*：**マシンの追加**をクリックして、マシンを手動で追加します。**VMの選択**ウィンドウが表示されます。以前に作成したOpenShift接続を展開し、追加するノード（VM）を選択します。次に、関連付けられたマシンアカウント名を追加します。
    - *CSVファイルを使用してマシンを追加する*：**CSVファイルの追加**をクリックして、マシンを一括追加します。CSVファイルを使用してマシンを追加する方法については、「CSVファイルを使用してマシンをカタログに一括追加する」(/ja-jp/citrix-daas/install-configure/machine-catalogs-manage.html#use-csv-files-to-bulk-add-machines-to-a-catalog)を参照してください。

4. 画面の指示に従って、OpenShift固有の情報を含まない残りの手順を完了します。

PowerShellコマンドを使用してカタログを作成する

PowerShell コマンドを使用して、Red Hat OpenShift 環境に MCS マシンカタログを作成できます。マシンプロファイルを使用しても使用しなくても、マシンカタログを作成できます。VM はマシンプロファイルの入力として使用されます。

1. PowerShellウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. PowerShellコマンドを実行して、
    a. IDプールを作成する
    b. ADアカウントを作成する
    c. マシンプロファイルを使用しても使用しなくても、永続VMを持つMCSマシンカタログを作成する。
    d. カタログにVMを追加する
    e. ブローカーカタログを作成する
    f. 新しいVMにブローカーマシンを追加する

以下はスクリプトの例です。

IDプールを作成する

```
New-AcctIdentityPool `

    -IdentityPoolName "IdentityPoolName" `

    -ZoneUid "00000000-0000-0000-0000-000000000000" `

    -NamingScheme "vm###" `

    -NamingSchemeType "Numeric" `

    -AllowUnicode `

    -Domain "MyDomain.local" `

    -AdminAddress "MyDDC.MyDomain.Local"
```

ADアカウントを作成する

```
New-AcctADAccount `

    -IdentityPoolUid "11111111-1111-1111-1111-111111111111" `

    -ADUserName "MyDomain\MyUserName" `

    -ADPassword SecurePassword `
```

```
    -Count 1 `

    -AdminAddress "MyDDC.MyDomain.Local"
```

永続マシンを使用したプロビジョニングスキームを作成する (マシンプロファイルなし)

```
New-ProvScheme `

    -ProvisioningSchemeName "ProvisioningSchemeName" `

    -HostingUnitName "HostingUnitName" `

    -IdentityPoolName "IdentityPoolName" `

    -ProvisioningSchemeType "MCS" `

    -MasterImageVM "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MasterImageVM.vm"
`

    -NetworkMapping @{"0" = "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MyNetwork.network"
 } `

    -VMCpuCount 1 `

    -VMMemoryMB 4096 `

    -InitialBatchSizeHint 1 `

    -AdminAddress "MyDDC.MyDomain.Local"
```

永続マシンを使用したプロビジョニングスキームを作成する (マシンプロファイルあり)

```
New-ProvScheme `

    -ProvisioningSchemeName "ProvisioningSchemeName" `

    -HostingUnitName "HostingUnitName" `

    -IdentityPoolName "IdentityPoolName" `
```

```
    -ProvisioningSchemeType "MCS" `

    -MasterImageVM "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MasterImageVM.vm"
`

    -NetworkMapping @{"0" = "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MyNetwork.network"
 } `

    -VMCpuCount 1 `

    -VMMemoryMB 4096 `

    -InitialBatchSizeHint 1 `

    -AdminAddress "MyDDC.MyDomain.Local" `

    -MachineProfile "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MachineProfileVM.v
m"
```

新しいPROVVMを作成する

```
New-ProvVM `

    ProvisioningSchemeName "ProvisioningSchemeName" `

    ADAccountName "MyDomain\vm001" `

    AdminAddress "MyDDC.MyDomain.Local"



Lock-ProvVM `

    -ProvisioningSchemeName "ProvisioningSchemeName" `

    -Tag "Brokered" `

    -VMID "TargetNamespace:vm001"
```

新しいブローカーカタログを作成する

```
New-BrokerCatalog `

    -Name "ProvisioningSchemeName" `

    -ProvisioningType "MCS" `

    -SessionSupport "MultiSession" `

    -AllocationType "Random" `

    -PersistUserChanges "OnLocal" `

    -ZoneUid "00000000-0000-0000-0000-000000000000" `

    -AdminAddress "MyDDC.MyDomain.Local"
```

ブローカーカタログのメタデータを設定する

```
Set-BrokerCatalogMetadata `

    -CatalogId "1" `

    -Name "Citrix_DesktopStudio_IdentityPoolUid" `

    -Value "11111111-1111-1111-1111-111111111111"



Set-BrokerCatalog `

    -Name "ProvisioningSchemeName " `

    -ProvisioningSchemeId "22222222-2222-2222-2222-222222222222"
```

新しいPROVVM用のブローカーマシンを作成する

```
New-BrokerMachine `

    -CatalogUid "33333333-3333-3333-3333-333333333333" `

    -AdminAddress "MyDDC.MyDomain.Local" `
```

```
    -MachineName "S-0-0-00-0000000000-0000000000-000000000-000000"
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、「」(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure.html)を参照してください。
- 電源管理については、Red Hat OpenShift VMの電源管理 を参照してください

詳細情報

- 接続とリソースを作成および管理する
- Red Hat OpenShiftへの接続
- マシンカタログを作成する

VMwareカタログを作成する

「マシンカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create.html)では、マシンカタログを作成するウィザードについて説明しています。以下の情報は、VMware仮想化環境に固有の詳細を扱っています。

> **注:**
>
> VMwareカタログを作成する前に、VMwareへの接続の作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/connections/connection-vmware-virtualization-environments.html)を参照してください。

マスターVMを作成する

マスターVMを使用して、マシンカタログでユーザーデスクトップとアプリケーションを提供します。ハイパーバイザーで、次の操作を行います。

1. マスターVMにVDAをインストールし、パフォーマンスを向上させるデスクトップの最適化オプションを選択します。
2. バックアップとして使用するために、マスターVMのスナップショットを作成します。

注:

MCSを使用して、vSAN 8.0環境でVMをプロビジョニングできます。

マシンプロファイルを使用してマシンカタログを作成する

マシンプロファイルを使用してMCSマシンカタログを作成できます。マシンプロファイルの入力元はVMwareテンプレートです。マシンプロファイルは、VMwareテンプレートからハードウェアプロパティを取得し、カタログ内の新しくプロビジョニングされたVMに適用します。

注:

- マスターイメージ入力（スナップショット）とマシンプロファイル入力（VMwareテンプレート）は、vTPMが有効であるか、vTPMが無効であるかのいずれかである必要があります。このルールは、`New-ProvScheme`と`Set-ProvScheme`の両方に適用されます。
- マスターイメージでvTPMが有効になっている場合、VMwareテンプレートはマスターイメージと同じVMソースからのみ取得できます。
- 暗号化ストレージポリシーはフルクローンのみをサポートします。
- マシンプロファイルベースのカタログは、提供されたVMwareテンプレートを利用してストレージコントローラー情報を収集し、接続された仮想ディスクに依存します。テンプレートには、仮想マシンの仮想ディスクを構成するために使用されるストレージコントローラー情報を取得するために必要な仮想ディスクが含まれている必要があります。

カタログへのVMのプロビジョニングを許可するには、マシンプロファイル内のVMwareテンプレートがカタログのライフサイクル中に存在する必要があります。VMwareテンプレートがない場合、新しいVMをプロビジョニングすることはできません。VMwareテンプレートが削除された場合は、`Set-ProvScheme`コマンドを使用して新しいテンプレートを提供する必要があります。

- MCSはVMwareテンプレートのプロパティをキャプチャします。Get-Provschemeコマンドを使用して、VMwareテンプレートの保存されたプロパティを参照する新しいVMwareテンプレートを作成できます。
- あるいは、マシンカタログとプロビジョニングされたVMが存在する場合、MCSでプロビジョニングされたマシンを使用して新しいVMwareテンプレートを作成することもできます。

- MCSIOが有効な場合、MCSカタログ作成後にメモリとディスクキャッシュのサイズを更新できます。

異なるOSに基づいて、異なる構成でマシンカタログを作成できます。

- マスターイメージにWindows 11がインストールされている場合、マスターイメージに対してvTPMを有効にすることが要件となります。したがって、マシンプロファイルのソースであるVMwareテンプレートにはvTPMがアタッチされている必要があります。
- vTPMがアタッチされていないマスターイメージにWindows 10がインストールされている場合、マシンプロファイルのソースとして非vTPM VMwareテンプレートを使用してマシンカタログを作成できます。

暗号化ストレージポリシーが適用されたマシンプロファイルテンプレートを使用して、フルコピーディスクモードでマシンカタログを作成できる別の構成があります。

マシンプロファイルをインプットとしてPowerShellコマンドを使用してマシンカタログを作成するには：

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix®*`を実行します。
3. 次のコマンドを実行します。

    - vTPMがアタッチされたVMwareテンプレートをマシンプロファイル入力のソースとして、Windows 11がインストールされたマスターイメージでマシンカタログを作成するには：

    ```
    $identityPool = New-AcctIdentityPool  -IdentityPoolName "<string>"

    -NamingScheme "<string>-###"

    -NamingSchemeType Numeric

    -Domain "<domain name"

    -ZoneUid "<Uid>"  -Scope @()
    ```

    ```
    $provScheme =New-ProvScheme  -CleanOnBoot

    -HostingUnitName "vSanRg"

    -IdentityPoolName "<string>"
    ```

```
-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<network name>.network"}

-ProvisioningSchemeName "<string>"

-Scope @() -VMCpuCount 4

-VMMemoryMB 6144

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template" -TenancyType Shared

-FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False

-MinimumFunctionalLevel 'L7_9'

-Name "<catalog name>"

-ProvisioningType 'MCS'

-Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- マシンプロファイルのソースとしてNon-vTPM VMwareテンプレートを使用し、Windows10がインストールされたマスターイメージでマシンカタログを作成するには：

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###" -NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-CleanOnBoot -HostingUnitName "<string>"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4  -
VMMemoryMB 8192

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template"

-TenancyType Shared  -FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False

-MinimumFunctionalLevel 'L7_9' -Name "<string>" -ProvisioningType
'MCS' -Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- 暗号化ストレージポリシーが適用されたマシンプロファイルテンプレートを使用して、フルコピーディスクモードでマシンカタログを作成するには：

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###"

-NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-HostingUnitName "<string>"

-IdentityPoolName "<string>"
```

```
-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"

-Scope @() -VMCpuCount 4  -VMMemoryMB 8192 -MachineProfile "XDHyp:
\HostingUnits\<hosting unit name>\<template name>.template"

-TenancyType Shared

-FunctionalLevel "L7_20" -UseFullDiskCloneProvisioning
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"  -IsRemotePC $False

-MinimumFunctionalLevel 'L7_9'

-Name "<string>" -ProvisioningType 'MCS' -Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

マシンプロファイルを更新するには、Set-ProvSchemeコマンドを使用します。例：

```
Set-ProvScheme -ProvisioningSchemeName 'name' -IdentityPoolName 'name'
-MachineProfile 'XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template'
```

複数のNICの確認

マシンプロファイルと、`New-ProvScheme`および`Set-ProvScheme`コマンドの`NetworkMapping`パラメーターを使用する場合、複数のNICの事前チェック中にさまざまなエラーメッセージが表示されます。

複数のNICの事前チェックリストは次のとおりです。

- マシンプロファイルテンプレートからのNIC数のみが使用され、検証されます。これらのNICが指すネットワークは、ホスティングユニットネットワークに対して使用または検証されません。
- マシンプロファイルテンプレートのNIC数がホスティングユニットのネットワーク数よりも多い場合、エラーメッセージが表示されます。
- マシンプロファイルテンプレートのNIC数がゼロの場合、エラーメッセージが表示されます。マシンプロファイルテンプレートのNIC数が1の場合：
  - `New-ProvScheme`または`Set-ProvScheme`コマンドでネットワークマッピングが指定されておらず、ホスティングユニットネットワークが1つである場合、ホスティングユニットネットワークが使用されます。
  - ネットワークマッピングが指定されている場合、それが有効であれば、指定されたネットワークマッピングが使用されます。
- マシンプロファイルテンプレートのNIC数が1より大きい場合、またはホスティングユニットネットワーク数が1より大きい場合：
  - コマンドで有効なネットワークマッピングが必要であり、各NICのマッピングを提供する必要があります（つまり、NetworkMappingの数はマシンプロファイルのNIC数と同じである必要があります）。
  - ホスティングユニット内で複数のNICを同じネットワークにマッピングすることはできません。
  - `NetworkMapping`の数とマシンプロファイルのNIC数は、ホスティングユニットのネットワーク数以下である必要があります。
  - 0からn-1までの各IDに対して`NetworkMapping`を提供する必要があります。ここでnはマシンプロファイルテンプレート内のネットワークアダプターの数です。

トラブルシューティング

カタログの作成に失敗した場合は、CTX294978を参照してください。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成に案内します。
- 構成プロセス全体を確認するには、インストールと構成を参照してください。
- カタログを管理するには、マシンカタログの管理とVMwareカタログの管理を参照してください。

詳細情報

- 接続とリソースの作成および管理
- VMwareへの接続
- マシンカタログの作成

異なるマシンID結合タイプのIDプール

MCSを使用すると、マシンをオンプレミスAD参加済み、Microsoft Entraハイブリッド参加済み、またはドメイン非参加としてプロビジョニングできます。

Web Studioでマシンを構成する方法については、「マシンカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create#machine-identities)を参照してください。

異なるマシンID参加タイプのIDプールを作成する方法の詳細については、以下を参照してください。

- オンプレミスActive Directory参加済みマシンIDのIDプール
- Microsoft Entraハイブリッド参加済みマシンIDのIDプール
- ドメインに参加していないマシンIDのIDプール

オンプレミスActive Directory参加済みマシンIDのIDプール

この記事では、オンプレミスActive Directory参加済みマシンIDのIDプールを作成する方法について説明します。

Web Studioを使用する

以下の情報は、マシンカタログの作成のガイダンスを補足するものです。

1. **マシンID**ページで、次の操作を行います。

    a. IDの種類として**オンプレミスActive Directory**を選択します。

    b. Active Directory アカウントオプションを選択します。

    - **新しいActive Directoryアカウントを作成する**:
        - **新しいActive Directoryアカウントを作成する**を選択し、既存のIDプールを使用して新しいアカウントを作成する場合は、それらのアカウントのドメインを選択し、アカウント命名スキームを指定します。
        - **新しいActive Directoryアカウントを作成する**を選択し、既存のIDプールを使用して新しいアカウントを作成する場合は、リストからIDプールを選択します。
    - **既存のActive Directoryアカウントを使用する**: CSVファイルから参照またはインポートし、パスワードをリセットするか、すべてのアカウントに同じパスワードを指定できます。

    c. **次へ**をクリックします。

2. **ドメイン資格情報**ページで、サービスアカウントを選択するか、資格情報を手動で入力します。サービスアカウントについては、「オンプレミスActive Directoryサービスアカウント」を参照してください。

サービスアカウントの関連付けを変更する

関連付けられているサービスアカウントを変更したり、既存のMCSマシンカタログに新しい関連付けを追加したりするには、「**マシンカタログの編集**」ページを使用します。

- サービスアカウントを追加するには、「**サービスアカウント**」ページで「**サービスアカウントの選択**」をクリックします。
- サービスアカウントの関連付けを変更するには、「**サービスアカウント**」ページで編集アイコンをクリックします。

PowerShell を使用する

オンプレミスのサービスアカウントをIDプールに関連付けることで、オンプレミスのサービスアカウントをMCSで作成されたマシンカタログに関連付けることができます。IDプールを作成するか、既存のIDプールを更新して、サービスアカウントに関連付けることができます。

例: 新しいIDプールを作成し、サービスアカウントに関連付けるには、以下を実行します。

```
New-AcctIdentityPool -IdentityType ActiveDirectory -IdentityPoolName
MyPool -NamingScheme Acc#### -Domain MyDomain.com -NamingSchemeType
Numeric -OU "CN=MyOU,DC=MyDomain,DC=com" -ServiceAccountUid
$serviceAccountUid
```

例: 既存のIDプールを更新してサービスアカウントに関連付けるには、以下を実行します。

```
$identityPoolUid = (Get-ProvScheme -ProvisioningSchemeName
"MyProvScheme").IdentityPoolUid

Set-AcctIdentityPool -IdentityPoolUid $identityPoolUid -ServiceAccountUid
$serviceAccountUid
```

注:

`$serviceAccountUid`は、オンプレミスのActive Directoryサービスアカウントの有効なUIDである必要があります。

Microsoft Entra ハイブリッド参加済みマシンIDのIDプール

この記事では、以下のIDプールを作成する方法について説明します。

- Microsoft Entra ハイブリッド参加済みカタログ
- Microsoft Intune に登録されている Microsoft Entra ハイブリッド参加済みカタログ

要件、制限、考慮事項については、Microsoft Entra ハイブリッド参加済みを参照してください。

Microsoft Entra ハイブリッド参加済みカタログを作成する

Web Studio を使用する

以下の情報は、マシンカタログの作成のガイダンスを補足するものです。

カタログ作成ウィザードの**マシンID**ページで:

- **Microsoft Entra ハイブリッド参加済み**を選択します。作成されたマシンは組織によって所有され、その組織に属するActive Directoryアカウントでサインインされます。
- デバイス管理のために作成されたマシンをMicrosoft Intune (Configuration Managerを含む) に登録するには、**Configuration Managerを使用してマシンをMicrosoft Intuneに登録する**を選

択します。カタログ作成中のエラーを回避するには、マスターイメージが次の要件を満たしていることを確認してください。

- VDAバージョン2405以降がインストールされていること。
- サイトコードが割り当てられていない**Configuration Managerクライアント**がインストールされていること。詳細については、このMicrosoft記事を参照してください。

> **注：**
>
> IDタイプとして**Microsoft Entra ハイブリッド参加済み**を選択した場合、カタログ内の各マシンには、対応するADコンピューターアカウントが必要です。

PowerShell を使用する

以下は、Web Studio での操作に相当する PowerShell の手順です。Remote PowerShell SDK を使用してカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>` を参照してください。

オンプレミスのAD参加済みカタログとMicrosoft Entraハイブリッド参加済みカタログの違いは、IDプールとマシンアカウントの作成にあります。

Microsoft Entra ハイブリッド参加カタログのアカウントとともにIDプールを作成するには：

```
New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -Domain
"corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -NamingScheme
"HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU
"CN=AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"

New-AcctIdentity -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
-ADUserName "corp\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -All
-ADUserName "corp\admin1" -ADPassword $password
```

> **注：**

`$password` は、書き込み権限を持つ AD ユーザーアカウントの一致するパスワードです。

Microsoft Entra ハイブリッド参加済みカタログの作成に使用されるその他のコマンドはすべて、従来のオンプレミス AD 参加済みカタログの場合と同じです。

Microsoft Entra ハイブリッド参加プロセスのステータスを表示する

Web Studio では、デリバリーグループ内の Microsoft Entra ハイブリッド参加済みマシンが電源オン状態の場合に、Microsoft Entra ハイブリッド参加プロセスのステータスが表示されます。ステータスを表示するには、Search を使用してそれらのマシンを特定し、下部ペインの タブで各マシンの を確認します。 には、次の情報が表示されます。

- Microsoft Entra ハイブリッド参加済み
- まだ Microsoft Entra ID に参加していません

注：

- マシンが最初に電源オンになったときに、Microsoft Entra ハイブリッド参加が遅延する場合があります。これは、デフォルトのマシン ID 同期間隔（Microsoft Entra Connect の 30 分）が原因です。マシンは、マシン ID が Microsoft Entra Connect を介して Microsoft Entra ID に同期された後にのみ、Microsoft Entra ハイブリッド参加状態になります。
- マシンが Microsoft Entra ハイブリッド参加状態にならない場合、それらは Delivery Controller に登録されません。登録ステータスは と表示されます。

また、Web Studio を使用して、マシンが利用できない理由を知ることができます。そのためには、 ノードでマシンをクリックし、下部ペインの タブで を確認し、ツールチップを読んで追加情報を確認します。

トラブルシューティング

マシンがMicrosoft Entraハイブリッド参加に失敗した場合は、次の操作を行います。

- マシンアカウントがMicrosoft Entra IDポータルを通じてMicrosoft Entra IDに同期されているか確認します。同期されている場合、**Not yet joined to Microsoft Entra ID**と表示され、登録が保留中であることを示します。

  マシンアカウントをMicrosoft Entra IDに同期するには、以下を確認してください。

  - マシンアカウントが、Microsoft Entra IDと同期するように構成されているOU内にあること。**userCertificate**属性を持たないマシンアカウントは、同期するように構成されているOU内にあってもMicrosoft Entra IDに同期されません。
  - マシンアカウントに**userCertificate**属性が設定されていること。属性を表示するには、Active Directory Explorerを使用します。
  - マシンアカウントが作成された後、Microsoft Entra Connectが少なくとも1回同期されている必要があります。同期されていない場合は、Microsoft Entra Connectマシンの PowerShellコンソールで`Start-ADSyncSyncCycle -PolicyType Delta`コマンドを手動で実行して、即時同期をトリガーします。

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix**の下にある**DeviceKeyPairRestored**の値を照会して、Microsoft Entraハイブリッド参加用のCitrix管理対象デバイスキーペアがマシンに正しくプッシュされているか確認します。

  値が1であることを確認します。そうでない場合、考えられる理由は次のとおりです。

  - プロビジョニングスキームに関連付けられているIDプールの`IdentityType`が`HybridAzureAD`に設定されていません。これは`Get-AcctIdentityPool`を実行して確認できます。
  - マシンがマシンカタログと同じプロビジョニングスキームを使用してプロビジョニングされていない。
  - マシンがローカルドメインに参加していない。ローカルドメイン参加は、Microsoft Entraハイブリッド参加の前提条件です。

- MCSプロビジョニング済みマシンで`dsregcmd /status /debug`コマンドを実行して、診断メッセージを確認します。

  - Microsoft Entra ハイブリッド参加が成功した場合、コマンドラインの出力で**AzureAdJoined**と**DomainJoined**が**YES**になります。
  - そうでない場合、問題をトラブルシューティングするにはMicrosoftのドキュメントを参照してください: `<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current>`。
  - エラーメッセージ「**Server Message: The user certificate is not found on the device with id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**」が表示された場合は、ユーザー証明書を修復するために、以下のPowerShellコマンドを実行します。

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
UserCertificate
```

ユーザー証明書の問題に関する詳細については、CTX566696を参照してください。

Microsoft Intune に登録されている Microsoft Entra ハイブリッド参加カタログを作成する

永続的なシングルセッションおよびマルチセッションVM向けに、Microsoft Intune に登録されている Microsoft Entra ハイブリッド参加カタログの共同管理が有効なカタログを作成できます。共同管理が有効なカタログは、StudioとPowerShellの両方を使用して作成できます。

Web Studio を使用する

以下の情報は、マシンカタログの作成のガイダンスを補足するものです。

マシンカタログのセットアップウィザードで:

- **マシンID**ページで、**Microsoft Entra ハイブリッド参加**を選択し、次に**Configuration ManagerでマシンをMicrosoft Intuneに登録**を選択します。このアクションを使用すると、Configuration ManagerとMicrosoft Intune（つまり、共同管理）がVMを管理します。

PowerShell を使用する

以下は、Studio の手順に相当する PowerShell の手順です。

Remote PowerShell SDKを使用して、Configuration ManagerでマシンをMicrosoft Intuneに登録するには、`New-AcctIdentityPool`の`DeviceManagementType`パラメーターを使用します。この機能には、カタログがMicrosoft Entra ハイブリッド参加済みであり、Microsoft Entra IDが適切なMicrosoft Intuneライセンスを所有している必要があります。

Microsoft Entra ハイブリッド参加カタログと共同管理が有効なカタログの違いは、IDプールの作成にあります。例:

```
New-AcctIdentityPool -AllowUnicode -DeviceManagementType "IntuneWithSCCM"
IdentityType="HybridAzureAD" -IdentityPoolName "CoManagedCatalog"
-NamingScheme "CoManaged-VM-##" -NamingSchemeType "Numeric" -Scope @()
-ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
```

トラブルシューティング

マシンがMicrosoft Intuneへの登録に失敗した場合、または共同管理状態に到達できない場合は、以下を実行してください。

- Intuneライセンスを確認する

  Microsoft Entra テナントに適切な Intune ライセンスが割り当てられているか確認します。Microsoft Intune のライセンス要件については、Microsoft Intune licensing を参照してください。

- Microsoft Entra ハイブリッド参加の状態を確認します

  MCS でプロビジョニングされたマシンが Microsoft Entra ハイブリッド参加済みであるか確認します。Microsoft Entra ハイブリッド参加済みでない場合、そのマシンは共同管理の対象になりません。Microsoft Entra ハイブリッド参加の問題のトラブルシューティングについては、トラブルシューティングを参照してください。

- 共同管理の適格性を確認します

  - MCS でプロビジョニングされたマシンに、予期される Configuration Manager サイトが正しく割り当てられているか確認します。割り当てられたサイトを取得するには、影響を受けるマシンで次の PowerShell コマンドを実行します。

    ```
    (New-Object -ComObject "Microsoft.SMS.Client").GetAssignedSite()
    ```

  - VM にサイトが割り当てられていない場合は、次のコマンドを使用して Configuration Manager サイトが自動的に検出されるか確認します。

    ```
    (New-Object -ComObject "Microsoft.SMS.Client").AutoDiscoverSite()
    ```

  - サイトコードが検出できない場合は、Configuration Manager 環境で境界と境界グループが適切に構成されていることを確認してください。詳細については、Considerations を参照してください。
  - Configuration Manager クライアントのサイト割り当てに関する問題がないか、`C:\Windows\CCM\Logs\ClientLocation.log` を確認してください。
  - マシンの共同管理の状態を確認します。影響を受けるマシンで **Configuration Manager コントロールパネル**を開き、**General** タブに移動します。共同管理プロパティの値は **Enabled** である必要があります。そうでない場合は、`C:\Windows\CCM\Logs\CoManagementHandler.log` の下のログを確認してください。

- Intune 登録を確認します

  すべての前提条件が満たされていても、マシンが Microsoft Intune への登録に失敗する場合があります。Intune 登録の問題については、**Application and Services Logs > Microsoft >**

Windows > DeviceManagement-Enterprise-Diagnostics-Provider の下の Windows イベントログを確認してください。

非ドメイン参加型マシンIDのIDプール

この記事では、Citrix Virtual Apps and Desktops を使用して、非ドメイン参加型カタログのIDプールを作成する方法について説明します。

要件、制限、考慮事項については、非ドメイン参加型を参照してください。

マシンカタログを作成する前に、次のものが必要です。

1. 新しいリソースの場所
    - Citrix Cloud™ 管理UI > 左上のハンバーガーメニュー > **リソースの場所** に移動します。
    - **+ リソースの場所** をクリックします。
    - 新しいリソースの場所の名前を入力し、**保存** をクリックします。
2. ホスティング接続を作成します。詳細については、接続の作成と管理セクションを参照してください。

Citrix Virtual Apps™ and Desktops を使用すると、ワークグループまたは非ドメイン参加型マシンに基づいてカタログを作成できます。非ドメイン参加型マシンの作成は、アカウントIDプールがどのように作成されるかによって異なります。アカウントIDプールは、カタログプロビジョニング中にMCSがマシン名を作成および追跡するために使用するメカニズムです。

Web Studio の使用

以下の情報は、マシンカタログの作成のガイダンスを補足するものです。

カタログ作成ウィザードで：

- **マシンID** ページで、**非ドメイン参加型** を選択します。作成されたマシンはどのドメインにも参加していません。

> **注:**
>
> 「**ドメインに参加していない**」識別タイプでは、カタログの最小機能レベルとしてVDAのバージョン2311以降が必要です。利用可能にするには、必要に応じて最小機能レベルを更新してください。

PowerShell を使用する

Remote PowerShell SDKを使用して、ドメインに参加していないカタログ用のIDプールを作成できます。

PowerShellパラメーターの**WorkgroupMachine**と**IdentityType**を使用して、ドメインに参加していないカタログ用のIDプールを作成します。これらのパラメーターにより、ドメイン管理者資格情報を含むすべてのAD固有のパラメーターを指定する必要がなくなります。

```
New-AcctIdentityPool -AllowUnicode -IdentityType "Workgroup"
-WorkgroupMachine -IdentityPoolName "NonDomainJoinedCatalog" -NamingScheme
"NDJ-VM-##" -NamingSchemeType "Numeric" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"
```

ドメインに参加していないカタログを作成するために使用される他のすべてのコマンドは、従来のオンプレミスActive Directoryに参加しているカタログの場合と同じです。

マシンカタログを管理する

注:

バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

マシンカタログへのマシンの追加または削除、名前の変更、説明の変更、またはカタログのActive Directoryコンピューターアカウントの管理を行うことができます。

カタログの保守には、各マシンが最新のOSアップデートを適用していることを確認することも含まれます。これには、ウイルス対策の更新、オペレーティングシステムのアップグレード、または構成の変更が含まれます。

- Machine Creation Services™ (MCS) を使用して作成されたプールされたランダムマシンを含むカタログは、カタログで使用されるマスターイメージを更新し、その後マシンを更新することでマシンを保守します。この方法により、多数のユーザーマシンを効率的に更新できます。

- 静的で永続的に割り当てられたマシンを含むカタログ、およびリモートPCアクセス マシンカタログの場合、ユーザーマシンの更新はWeb Studioの外部で管理します。このタスクは、個別に、またはサードパーティのソフトウェア配布ツールを使用して一括で実行します。

ホストハイパーバイザーへの接続の作成と管理については、「接続とリソース」を参照してください。

> **注:**
>
> MCSはWindows 10 IoT CoreおよびWindows 10 IoT Enterpriseをサポートしていません。詳細については、Microsoftサイトを参照してください。

永続インスタンスについて

永続的または専用インスタンスを使用して作成されたMCSカタログを更新する場合、カタログ用に作成された新しいマシンはすべて更新されたイメージを使用します。既存のインスタンスは引き続き元のインスタンスを使用します。イメージの更新プロセスは、他の種類のカタログと同じ方法で行われます。以下を考慮してください。

- 永続ディスクカタログの場合、既存のマシンは新しいイメージに更新されませんが、カタログに追加される新しいマシンは新しいイメージを使用します。
- 非永続ディスクカタログの場合、マシンイメージはマシンがリセットされるたびに更新されます。
- 永続的なマシンカタログの場合、イメージを更新すると、それを使用するカタログインスタンスも更新されます。
- 永続的ではないカタログの場合、マシンごとに異なるイメージを使用したい場合は、イメージを別々のカタログに配置する必要があります。

マシンカタログを管理する

マシンカタログは、次の2つの方法で管理できます。

- Web Studioの使用
- PowerShellを使用する

Web Studioを使用する

このセクションでは、Web Studioを使用してカタログを管理する方法について詳しく説明します。

- マシンカタログの管理
  - はじめに
  - 永続インスタンスについて
- マシンカタログの管理
- Web Studioの使用
- カタログの詳細の表示
  - カタログへのマシンの追加
  - カタログからマシンを削除する(#delete-machines-from-a-catalog)
- カタログを編集する(#edit-a-catalog)
- カタログの名前を変更する(#rename-a-catalog)
- カタログを別のゾーンに移動する(#move-a-catalog-to-a-different-zone)
- カタログを削除する(#delete-a-catalog)
- (#Azure のレガシー MCS カタログをマシンプロファイルベースのカタログに変換する)
- カタログ内のActive Directoryコンピューターアカウントを管理する(#manage-active-directory-computer-accounts-in-a-catalog)
- カタログを更新する(#update-a-catalog)
  - マスターイメージを更新または作成する(#update-or-create-a-master-image)
  - マスターイメージを変更する(#change-the-master-image)
  - マスターイメージをロールバックする(#roll-back-the-master-image)
- 機能レベルを変更する、または変更を元に戻す(#change-the-functional-level-or-undo-the-change)
- カタログをクローンする(#clone-a-catalog)
- フォルダーを使用してカタログを整理する(#organize-catalogs-using-folders)
  - カタログフォルダーを作成する(#create-a-catalog-folder)
  - カタログを移動する
  - カタログフォルダーを管理する
- VDAをアップグレードする
- カタログ作成を再試行する

- トークンを使用してMCS以外でプロビジョニングされたVDAを登録する
- PowerShellを使用する
- カタログに関連付けられている警告とエラーを取得する
- イメージに説明を追加する
- OSディスクをリセットする
- 既存のプロビジョニングスキームのネットワーク設定を変更する
- マシンカタログのバージョンを管理する
- マシンプロファイルに基づかないマシンカタログをマシンプロファイルに基づくマシンカタログに変換する
- アクティブなコンピューターアカウントのID情報を修復する
  - 条件
  - IDディスクをリセットする
- 既存のマシンカタログのキャッシュ構成を変更する
  - 要件
  - キャッシュ構成を変更する
- ローカルファイル共有アクセスによるVDA更新サポート
  - PowerShellコマンドレット
  - 前提条件
  - ファイル共有権限の設定方法
  - ローカルファイル共有からのVDA更新
- トラブルシューティング
- 次のステップ

カタログの詳細を表示

1. 検索機能を使用して、特定のマシンカタログを見つけます。手順については、インスタンスの検索を参照してください。
2. 検索結果から、必要に応じてカタログを選択します。
3. カタログ列の説明については、次の表を参照してください。
4. カタログ列の説明については、次の表を参照してください。

列	説明
マシンカタログ	カタログの名前と割り当ての種類。割り当ての種類には以下が含まれます。
	• ランダム: カタログ内のマシンはユーザーにランダムに割り当てられます。
	• 永続: カタログ内のマシンはユーザーに永続的に割り当てられます。
マシンタイプ	カタログ内のマシンでサポートされているセッションの種類。可能な値には以下が含まれます。
	• OSタイプ: マルチセッションOS (仮想); ユーザーデータ: 破棄。
	• OSタイプ: マルチセッションOS (仮想); ユーザーデータ: ローカルディスク上
	• OSの種類: シングルセッションOS (Remote PC Access)
	• OSの種類: シングルセッションOS (仮想); ユーザーデータ: 破棄
	• OSの種類: シングルセッションOS (仮想); ユーザーデータ: ローカルディスク上
マシン数	カタログ内のマシン数とプロビジョニング方法。可能なプロビジョニング方法には、Machine Creation Services (MCSマシン)、手動、Citrix Provisioning™ Services があります。
割り当て済み数	デリバリーグループに割り当てられているカタログ内のマシンの数。
フォルダー	**マシンカタログ**ツリー内でのカタログの場所。カタログが存在するフォルダーの名前 (末尾のバックスラッシュを含む) を表示しま

列	説明
	す。カタログがルートレベルにある場合は `-` と表示されます。
VDAアップグレード	VDAアップグレードの状態。可能な値は、未構成、スケジュール済み、利用可能、最新です。
イメージステータス	カタログのイメージ更新のステータス。非永続マシンカタログにのみ適用されます。可能な値は、完全に更新済み、部分的に更新済み、更新保留中、準備中です。

5. 選択したカタログの詳細については、下部の詳細ペインにあるタブをクリックします。

タブ	説明
詳細	マシンタイプ、プロビジョニング方法、サービスアカウント、OS、VDAバージョンなど、主要なマシンカタログ設定を要約し、リソースをすばやく表示および管理できます。
テンプレートプロパティ	MCSでプロビジョニングされたカタログでのみ利用可能です。
	選択したカタログの詳細なプロビジョニング情報を表示します。以下を含みます。
	• マシンテンプレートプロパティ
	• ハイパーバイザー固有の詳細
	• マシンプロファイルプロパティ
マシン	選択したカタログ内のマシン名のページ分割されたリストを表示します。
デリバリーグループ	Remote PCカタログで利用可能です。
	選択したカタログに関連付けられているデリバリーグループを表示します。デリバリーグ

タブ	説明
	ループ名とカタログの関連付けが表示されます。
タグ	マルチテナント環境では利用できません。
	選択したマシンカタログに割り当てられているタグのタグ名と説明を表示します。
ワークスペース環境管理	WEMサービスがプロビジョニングされ、アクセス可能な場合にのみ表示されます。
	Workspace Environment Managementシステムの最適化設定を表示します。
コストインサイト	Azure MCSカタログにのみ適用され、これが表示されます
	• 過去30日間に発生した総コスト。
	• 現在の30日間の総コストと、前の30日間の期間との比較。
	このタブを表示するには、Citrixの**コスト管理 > 管理 > コストの読み取り**権限（クラウド管理者にはデフォルト）が必要です。コストの詳細を表示するには、`Microsoft.CostManagement/query/read` Azure権限が必要です。
トラブルシューティング	推奨されるアクションとともに、カタログのエラーまたは警告を表示します。

マシンをカタログに追加する

開始する前に:

- 仮想化ホストに、追加のマシンを収容するのに十分なプロセッサ、メモリ、ストレージがあることを確認してください。
- 未使用のActive Directoryコンピューターアカウントが十分にあることを確認してください。既存のアカウントを使用している場合、追加できるマシンの数は利用可能なアカウントの数によって制限されます。

- Web Studioを使用して追加のマシン用のActive Directoryコンピューターアカウントを作成する場合、適切なドメイン管理者権限が必要です。

カタログにマシンを追加するには:

1. Web Studioにサインインします。
2. 左ペインで**マシンカタログ**を選択します。
3. マシンカタログを選択し、アクションバーで**マシンの追加**を選択します。
4. 追加する仮想マシンの数を選択します。
5. 追加するVMの数に対して既存のActive Directoryアカウントが不足している場合は、アカウントが作成されるドメインと場所を選択します。アカウントの命名スキームを指定し、連番または文字が表示される場所にハッシュマークを使用します。OU名にスラッシュ（/）を使用しないでください。名前を数字で始めることはできません。たとえば、PC-Sales-##（0-9が選択されている場合）という命名スキームは、PC-Sales-01、PC-Sales-02、PC-Sales-03などのコンピューターアカウントになります。
6. 既存のActive Directoryアカウントを使用する場合は、アカウントを参照するか、**インポート**をクリックしてアカウント名を含む.csvファイルを指定します。追加するすべてのマシンに対して十分なアカウントがあることを確認してください。Web Studioはこれらのアカウントを管理します。Web Studioにすべてのアカウントのパスワードをリセットさせるか、すべてのアカウントで同じである必要があるアカウントパスワードを指定します。

マシンはバックグラウンドプロセスとして作成され、多数のマシンを作成する場合は時間がかかることがあります。Web Studioを閉じてもマシンの作成は続行されます。

カタログからマシンを削除する

マシンカタログからマシンを削除すると、ユーザーはアクセスできなくなるため、マシンを削除する前に以下を確認してください。

- ユーザーデータがバックアップされているか、不要になっていること。
- すべてのユーザーがログオフしていること。メンテナンスモードをオンにすると、マシンへの新しい接続が停止します。
- マシンが電源オフになっていること。

カタログからマシンを削除するには：

1. Web Studioにサインインします。
2. 左ペインで**マシンカタログ**を選択します。

3. カタログを選択し、アクションバーで**マシンを表示**を選択します。
4. 1つ以上のマシンを選択し、アクションバーで**削除**を選択します。

削除するマシンを削除するかどうかを選択します。マシンを削除することを選択した場合、それらのマシンのActive Directoryアカウントを保持するか、無効にするか、削除するかを指定します。

カタログを編集する

1. **説明**ページで、カタログの説明を変更します。
2. 左ペインで**マシンカタログ**を選択します。
3. カタログを選択し、アクションバーで**マシンカタログの編集**を選択します。
4. **スコープ**ページで、スコープを変更します。
5. **NIC**ページで、次のアクションを実行します。

   - NICのサブネットマッピングを変更するには、**関連ネットワーク**フィールドからネットワークを選択します。
   - サブネットマッピングを追加するには、**NICの追加**を選択し、**関連ネットワーク**フィールドからネットワークを選択して、**保存**をクリックします。

   カタログに関連付けられているホストに存在するサブネットのみが、**関連ネットワーク**フィールドに表示されます。

   マシンプロファイルのないAzureマシンカタログにのみNICを追加できます。

   > **注:**
   >
   > - AWSマシンカタログの場合、同じサブネットを複数のNICにマッピングすることはできません。
   > - マシンプロファイルを持つマシンカタログの場合、カタログ上のNICの数は、マシンプロファイル上のNICの数と等しくなければなりません。
   > - この機能は、IBM Cloudハイパーバイザーではサポートされていません。
   > - この機能は、Nutanixハイパーバイザーの場合、Nutanix Prism Elementでのみサポートされています。

6. カタログの種類によっては、他のページが表示される場合があります。

Azure Resource Managerイメージを使用して作成されたカタログの場合、以下のページが表示されます。変更は、後でカタログに追加するマシンにのみ適用されることに注意してください。既存のマシンは変更されません。

- **Virtual Machines** ページで、マシンのサイズと、マシンを作成するアベイラビリティゾーンを変更します。

  > **注：**
  >
  > - カタログがサポートするマシンサイズのみが表示されます。
  > - 必要に応じて、**Show only machine sizes used in other machine catalogs** を選択して、マシンサイズリストをフィルターします。
  > - Azureカタログの場合、**Storage and License Types** ページで **Storage redundancy** が **ZRS** の場合、ゾーン選択をクリアしてAzureにVMアベイラビリティゾーンを管理させることを示唆する警告が表示されます。

- **Machine Profile** ページで、マシンプロファイルを使用するか変更するかを選択します。

  > **注：**
  >
  > Azureカタログの場合、アベイラビリティゾーンを含むマシンプロファイルを変更し、ストレージ冗長性にZRSを選択すると、ゾーン選択をクリアするよう促す警告が表示されます。

- (カタログが専用グループホストで構成されている場合にのみ表示) **Dedicated host group** ページで、ホストグループを変更するかどうかを選択します。
- **Storage and License Types** ページで、ストレージ冗長タイプ (Azureカタログの場合)、ストレージタイプ、ライセンスタイプ、およびAzure Computer Gallery設定 (「**Place prepared image in Azure Gallery**」が使用されている場合にのみ利用可能) を変更するかどうかを選択します。

> **注:**

> 新しく選択した設定が現在のマシンサイズをサポートしていない場合、設定を変更するとマシンサイズの設定がリセットされることを通知する警告ダイアログボックスが表示されます。続行を選択すると、**Virtual Machines**メニューの横に赤い点が表示され、新しいマシンサイズを選択するように促されます。

- **License Type**ページで、WindowsライセンスまたはLinuxライセンスの設定を変更するかどうかを選択します。

リモートPCアクセスカタログの場合、次のページが表示されます。

- **Power Management**ページで、電源管理設定を変更し、電源管理接続を選択します。
- **Organizational Units**ページで、Active Directory OUを追加または削除します。

7. **Apply**をクリックして変更を適用し、**Save**をクリックして終了します。

カタログの名前を変更する

1. Web Studioにサインインします。
2. 左ペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**Rename Machine Catalog**を選択します。
4. 新しい名前を入力します。

カタログを別のゾーンに移動する

展開に複数のゾーンがある場合、カタログをあるゾーンから別のゾーンに移動できます。

カタログを、そのカタログ内のVMを含むハイパーバイザーとは異なるゾーンに移動すると、パフォーマンスに影響します。

1. Web Studioにサインインします。
2. 左ペインで**マシンカタログ**を選択します。
3. カタログを選択し、アクションバーで**移動**を選択します。
4. カタログを移動するゾーンを選択します。

カタログを削除する

カタログを削除する前に、以下を確認してください。

- すべてのユーザーがログオフしており、切断されたセッションは実行されていません。

- カタログ内のすべてのマシンでメンテナンスモードがオンになっており、新しい接続が確立できないこと。
- カタログ内のすべてのマシンが電源オフになっていること。
- カタログはデリバリーグループに関連付けられていません。つまり、デリバリーグループにはそのカタログのマシンが含まれていません。

カタログを削除するには：

1. Web Studioにサインインします。
2. 左ペインで**マシンカタログ**を選択します。
3. カタログを選択し、アクションバーで**マシンカタログの削除**を選択します。
4. カタログ内のマシンを削除するかどうかを指定します。マシンを削除することを選択した場合、それらのマシンのActive Directoryコンピューターアカウントを保持するか、無効にするか、削除するかを指定します。

Azure のレガシー MCS カタログをマシンプロファイルベースのカタログに変換する

マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換するには、次の手順を実行します。

1. **マシンカタログ**ページで、変換する**マシンカタログ**名を右クリックし、**マシンカタログの編集**を選択します。
2. **マシンカタログの編集 > マシンプロファイル**ページで、**マシンプロファイルを使用する (Microsoft Entra ID に必須)**チェックボックスをオンにします。
3. **マシンプロファイルの選択**をクリックします。
4. **マシンプロファイルの選択**ページで、マシンプロファイルとして使用する仮想マシンまたは起動テンプレートを選択します。
5. 現在の設定の一部が新しいマシンプロファイルの設定と異なる場合は、使用する設定に必要なオプションを選択し、**続行**をクリックします。
6. **適用**をクリックします。

> **注:**
>
> 現在、この機能はAzure、AWS、VMwareでのみサポートされています。

カタログ内のActive Directoryコンピューターアカウントを管理する

マシンカタログ内のActive Directoryアカウントを管理するには、次の操作を実行できます。

- シングルセッションOSおよびマルチセッションOSカタログからActive Directoryコンピューターアカウントを削除して、未使用のマシンアカウントを解放します。これらのアカウントは、他のマシンで使用できます。
- カタログにマシンが追加されたときにコンピューターアカウントがすでに存在するようにアカウントを追加します。OU名にスラッシュ (/) を使用しないでください。

Active Directoryアカウントを管理するには：

1. Web Studio にサインインします。
2. 左側のペインで、**マシンカタログ**を選択します。
3. カタログを選択し、アクションバーで**ADアカウントの管理**を選択します。
4. コンピューターアカウントを追加するか削除するかを選択します。アカウントを追加する場合は、アカウントのパスワードをどうするかを指定します。すべてリセットするか、すべてのアカウントに適用されるパスワードを入力します。

   現在のアカウントパスワードが不明な場合は、パスワードをリセットできます。パスワードリセットを実行する権限が必要です。パスワードを入力すると、インポート時にアカウントのパスワードが変更されます。アカウントを削除する際は、Active Directory内のアカウントを保持するか、無効にするか、削除するかを選択します。

カタログからマシンを削除したり、カタログを削除したりする際に、Active Directoryアカウントを保持するか、無効にするか、削除するかを指定します。

カタログを更新する

カタログ内のマシンを更新する前に、マスターイメージのコピーまたはスナップショットを保存することをお勧めします。データベースには、各マシンカタログで使用されたマスターイメージの履歴レコードが保持されます。カタログ内のマシンを以前のバージョンのマスターイメージに戻す（ロールバックする）ことができます。ユーザーがデスクトップに展開した更新プログラムで問題が発生した場合に、このタスクを実行します。これにより、ユーザーのダウンタイムが最小限に抑えられます。マスターイメージを削除、移動、または名前変更しないでください。それらを使用してカタログを元に戻すことはできません。

マシンが更新されると、自動的に再起動します。

マスターイメージを更新または作成する

マシンカタログを更新する前に、既存のマスターイメージを更新するか、ホストハイパーバイザー上に新しいマスターイメージを作成します。

1. ハイパーバイザーで、現在のVMのスナップショットを取得し、そのスナップショットに意味のある名前を付けます。このスナップショットは、必要に応じてカタログ内のマシンを元に戻す（ロールバックする）ために使用できます。
2. 必要に応じて、マスターイメージの電源をオンにし、ログオンします。
3. 更新プログラムをインストールするか、マスターイメージに必要な変更を加えます。
4. VMの電源を切ります。
5. VMのスナップショットを作成します。Web Studioでカタログが更新されたときに認識される、意味のある名前を付けます。Web Studioでスナップショットを作成することもできますが、Citrixではハイパーバイザー管理コンソールを使用して作成することをお勧めします。その後、Web Studioでそのスナップショットを選択します。このプロセスにより、自動生成された名前ではなく、意味のある名前と説明を提供できます。GPUマスターイメージの場合、マスターイメージはXenServer®コンソールからのみ変更できます。

マスターイメージを変更する

カタログ内のすべてのマシンに更新プログラムを準備して展開するには：

1. Web Studioにサインインします。
2. 左ペインで**マシンカタログ**を選択します。
3. カタログを選択し、アクションバーで**マスターイメージの変更**を選択します。
4. **イメージ**ページで、展開するホストとイメージを選択します。

> **ヒント：**
>
> MCSで作成されたカタログの場合、イメージにメモを追加して注釈を付けることができます。メモには最大500文字を含めることができます。マスターイメージを変更するたびに、メモを追加したかどうかにかかわらず、メモ関連のエントリが作成されます。メモを追加せずにカタログを更新した場合、エントリはnull (-)として表示されます。イメージのメモ履歴を表示するには、カタログを選択し、下部ペインで**テンプレートプロパティ**をクリックし、**メモ履歴の表示**をクリックします。

5. **ロールアウト戦略**ページで、マシンカタログ内のマシンを新しいマスターイメージで更新するタイミング（次回のシャットダウン時または即時）を選択します。

> **注：**
>
> **ロールアウト戦略**ページは、ロールアウトが非永続VMにのみ適用されるため、永続VMでは利用できません。

6. **概要**ページで情報を確認し、**完了**をクリックします。各マシンは更新後に自動的に再起動します。

更新の進行状況を追跡するには、**マシンカタログ**でカタログを見つけて、インラインの進行状況バーと段階的な進行状況グラフを表示します。

Web StudioではなくPowerShell SDKを直接使用してカタログを更新する場合は、ハイパーバイザーテンプレート（**VMTemplates**）を指定します。これをイメージまたはイメージのスナップショットの代替として使用します。

Azure ベースのマシンカタログに新しいマスターイメージを展開するには:

1. Web Studio から、左側のペインで を選択します。
2. Azure カタログを選択し、アクションバーで を選択します。
3. ページで、 の下にあるイメージを選択します。ブレードには、リソースと同じリージョンに属するすべてのイメージが一覧表示されます。

展開戦略:

次回のシャットダウン時にイメージを更新すると、現在使用されていないマシン、つまりアクティブなユーザーセッションがないマシンにすぐに影響します。使用中のシステムは、現在のアクティブセッションが終了したときに更新を受け取ります。以下を考慮してください。

- 該当するマシンでの更新が完了するまで、新しいセッションを起動することはできません。
- シングルセッションOSマシンでは、マシンが使用されていないとき、またはユーザーがログオンしていないときに、マシンはすぐに更新されます。
- 子マシンを持つマルチセッションOSの場合、再起動は自動的に行われません。更新されたマスターイメージを適用するには、Studio、PowerShell、またはWorkspaceを使用してマシンを再起動します。マシンまたはハイパーバイザーからの再起動では、更新は適用されません。

> **ヒント:**
>
> ホスト接続の詳細設定を使用して、再起動されるマシンの数を制限します。これらの設定を使用して、特定のカタログに対して実行されるアクションを変更します。詳細設定はハイパーバイザーによって異なります。

マスターイメージをロールバックする

更新された、または新しいマスターイメージを展開した後、それをロールバックできます。このプロセスは、新しく更新されたマシンで問題が発生した場合に必要になることがあります。ロールバックすると、カタログ内のマシンは最後に動作していたイメージにロールバックされます。新しいイメージを必要とする新機能は利用できなくなります。展開と同様に、マシンのロールバックには再起動が含まれます。

1. Web Studio にサインインします。
2. 左側のペインで を選択します。
3. カタログを選択し、アクションバーで**マスターイメージのロールバック**を選択します。
4. ロールアウト操作に関する前のセクションで説明されているように、以前のマスターイメージをマシンに適用するタイミングを指定します。

ロールバックは、元に戻す必要があるマシンにのみ適用されます。新しいまたは更新されたマスターイメージで更新されていないマシンは、通知メッセージを受信せず、強制的にログオフされることもありません。

ロールバックの進行状況を追跡するには、 でカタログを見つけて、インラインの進行状況バーと段階的な進行状況グラフを表示します。

機能レベルを変更または変更を元に戻す

マシンのVDAを新しいバージョンにアップグレードした後、マシンカタログの機能レベルを変更します。Citrixは、すべての最新機能にアクセスできるように、すべてのVDAを最新バージョンにアップグレードすることを推奨します。

マシンカタログの機能レベルを変更する前に、次の点に注意してください。

- アップグレードされたマシンを起動して、Controllerに登録させます。このプロセスにより、Web Studioはカタログ内のマシンがアップグレードを必要としていることを判断できます。

カタログの機能レベルを変更するには：

1. Web Studioにサインインします。
2. 左ペインで**マシンカタログ**を選択します。
3. カタログを選択します。下部ペインの**詳細**タブにバージョン情報が表示されます。
4. **機能レベルの変更**を選択します。Web Studioがカタログのアップグレードが必要であると検出した場合、メッセージが表示されます。プロンプトに従います。1台以上のマシンをアップグレードできない場合、その理由を説明するメッセージが表示されます。すべてのマシンが適切に機能するように、Citrixは**変更**をクリックして続行する前に、マシンの問題を解決することをお勧めします。

カタログの変更が完了した後、カタログを選択し、アクションバーで**機能レベルの変更を元に戻す**を選択することで、マシンを以前のVDAバージョンに戻すことができます。

カタログをクローンする

カタログを複製する前に、次の考慮事項に注意してください。

- オペレーティングシステムおよびマシン管理に関連する設定は変更できません。複製されたカタログは、元のカタログからこれらの設定を継承します。

> **注:**
>
> 複製するAzureカタログを選択し、マスターイメージを選択した場合、ブレードにはリソースと同じリージョンに属するすべてのイメージが一覧表示されます。

- カタログのクローン作成には時間がかかる場合があります。必要に応じて、**「進行状況を非表示」**を選択して、バックグラウンドでクローン作成を実行します。
- クローンされたカタログは元のカタログの名前を継承し、サフィックス`Copy`が付きます。名前は変更できます。カタログの名前を変更するを参照してください。
- クローン作成が完了したら、クローンされたカタログをデリバリーグループに割り当ててください。

1. Web Studioにサインインし、左ペインで**「マシンカタログ」**を選択します。
2. カタログを選択し、アクションバーで**「クローン」**を選択します。
3. **「選択したマシンカタログのクローン」ウィンドウで、クローンされたカタログの設定を表示し、必要に応じて設定を構成します。**「次へ」**を選択して次のページに進みます。
4. **「概要」ページで、設定の概要を確認し、**「完了」**を選択してクローン作成を開始します。

5. 必要に応じて、**「進行状況を非表示」**を選択して、バックグラウンドでクローン作成を実行します。

フォルダーを使用してカタログを整理する

フォルダーを作成してカタログを整理し、簡単にアクセスできるようにすることができます。たとえば、イメージタイプ別や組織構造別にカタログを整理できます。

> **ヒント:**
>
> アクションバーの右上にある**フォルダー**アイコンをクリックすると、マシンカタログノードのデフォルト表示（フォルダー表示またはリスト表示）を設定できます。

カタログフォルダーを作成する

開始する前に、まずカタログの整理方法を計画してください。次の点を考慮してください。

- フォルダーは最大5階層までネストできます（デフォルトのルートフォルダーを除く）。
- カタログフォルダーには、カタログとサブフォルダーを含めることができます。
- Web Studioのすべてのノード（**マシンカタログ**、**デリバリーグループ**、**アプリケーション**、**アプリケーショングループ**など）は、バックエンドで同じフォルダーツリーを共有します。フォルダーの名前変更や移動時に名前の競合を避けるため、異なるノード間で最上位フォルダーには一意の名前を使用してください。

  `New-BrokerAdminFolder` SDKコマンドレットを使用してフォルダーを作成し、それを**マシンカタログ**ノードの下に表示させたい場合は、`Set-BrokerAdminFolderMetadata`コマンドレットを使用して`ContainsMachineCatalogs`メタデータを追加する必要があります。

  例:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsMachineCatalogs -Value true
  ```

カタログフォルダーを作成するには、次の手順に従います。

1. 左ペインで**マシンカタログ**を選択します。
2. フォルダー階層でフォルダーを選択し、**アクション**バーで**フォルダーの作成**を選択します。
3. 新しいフォルダーの名前を入力し、**完了**をクリックします。

> **ヒント:**
>
> 意図しない場所にフォルダーを作成した場合でも、正しい場所にドラッグして移動できます。

カタログを移動する

カタログはフォルダー間で移動できます。詳細な手順は次のとおりです。

1. 左側のペインで を選択します。
2. フォルダー別にカタログを表示します。フォルダー階層の上にある をオンにすると、すべてのカタログを一度に表示することもできます。
3. カタログを右クリックし、 を選択します。
4. カタログを移動するフォルダーを選択し、 をクリックします。

> **ヒント:**
>
> カタログをフォルダーにドラッグできます。

カタログフォルダーの管理

カタログフォルダーを削除、名前変更、移動できます。

フォルダーとそのサブフォルダーにカタログが含まれていない場合にのみ、フォルダーを削除できます。

フォルダーを管理するには、以下の手順に従います。

1. 左側のペインで を選択します。
2. フォルダー階層でフォルダーを選択し、必要に応じて バーでアクションを選択します。
   - フォルダーの名前を変更するには、 を選択します。
   - フォルダーを削除するには、 を選択します。
   - フォルダを移動するには、**Move Folder** を選択します。
3. 画面の指示に従って、残りの手順を完了します。

VDAのアップグレード

Studioインターフェイスを使用して、VDAを簡単にアップグレードできます。詳細および段階的なガイダンスについては、Citrix VDA Upgrade Service ドキュメントを参照してください。

カタログ作成を再試行する

> **注:**
>
> この機能はMCSカタログにのみ適用されます。

> 失敗したカタログにはエラーアイコンが表示されます。詳細を確認するには、各カタログの**トラブルシューティング**タブに移動します。カタログ作成を再試行する前に、以下の考慮事項に注意してください。

- まずトラブルシューティング情報を確認し、問題を解決してください。この情報には、検出された問題が記述されており、それらを解決するための推奨事項が提供されています。
- オペレーティングシステム および マシン管理 に関連する設定は変更できません。カタログは、元の設定を継承します。
- 作成には時間がかかる場合があります。必要に応じて、**進行状況を非表示**を選択して、バックグラウンドで作成を実行します。

カタログの作成を再試行するには、次の手順を実行します。

1. Web Studioから、左側のペインで**マシンカタログ**を選択します。
2. カタログを選択し、その**トラブルシューティング**タブに移動します。
3. 再試行のハイパーリンクをクリックして、カタログの作成を再試行します。
4. 表示されるウィザードで、必要に応じて設定を変更します。変更する必要がない場合は、直接**概要**ページに移動できます。
5. 完了したら、**完了**を選択して作成を開始します。

トークンを使用してMCS以外のプロビジョニング済みVDAを登録する

非MCSプロビジョニングVDAの登録トークンを生成および管理できるようになりました。この実装により、MCSでVDAをプロビジョニングすることなく、WebSocket経由でVDA登録が可能になります。この機能は、Linux Virtual Delivery Agent、macOS用Citrix Virtual Delivery Agent、およびCitrix Virtual Apps™ and Desktopsを使用する非ドメイン参加VDAもサポートします。

始める前に

1. サイトを構成します。詳細については、サイトの作成を参照してください。
2. Delivery ControllerにTLS証明書をインストールします。詳細については、ControllerにTLSサーバー証明書をインストールするを参照してください。
3. Delivery Controllerを信頼するために、VDAにルートCAおよび中間CAをインストールします。
4. Delivery ControllerでWebSocket接続を有効にします。サイトに存在する各Delivery Controllerで次のコマンドを実行します。

```
New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy"
-Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -Force
```

> **注:**
>
> WebSocketを有効にした後、Delivery Controllerを再起動してください。

登録トークンの生成

Citrix以外のプロビジョニングマシンに対してトークンベースの登録を有効にすることを決定したら、まずマシンカタログごとにトークンを生成し、VDAインストール管理者と共有する必要があります。

登録トークンの特徴：

- 登録範囲：1〜5000台のVDAマシン
- 有効期間：最大14日間

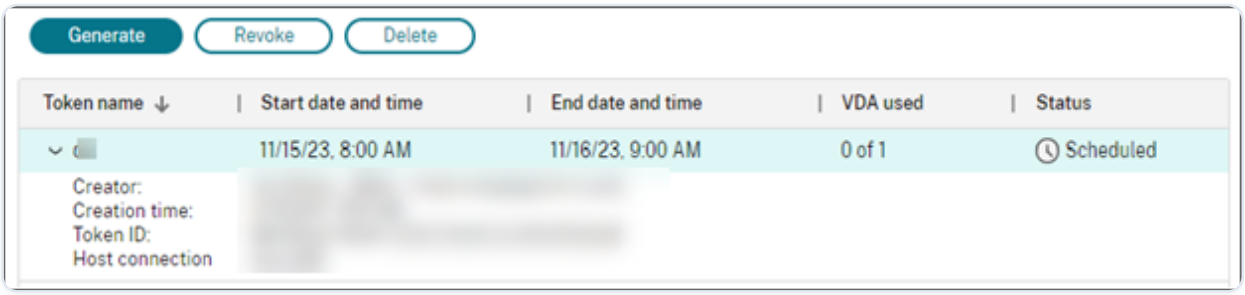
Web Studioを使用してカタログのトークンを生成するには、次の手順に従います。

1. **Web Studio > マシンカタログ**で、非MCSプロビジョニングカタログを見つけます。このカタログには、**マシン数**列に**プロビジョニング方法: 手動**と表示されています。
2. カタログを右クリックし、**登録トークンの管理**を選択します。
3. 表示される**登録トークンの生成**ページで、次のトークン情報を提供します。
   - トークンの名前を入力します。
   - 有効期間を入力します。期間は14日以内である必要があります。トークンは指定された期間のみ有効です。

- (オプション) トークンで登録されたVDAの電源管理のためにホスト接続を選択します。オプションには、このカタログのゾーン下のすべてのホスト接続が含まれます。
- トークンの使用制限（1〜5000）を入力します。

4. **生成**をクリックします。
5. 表示される**トークンが正常に生成されました**ウィンドウで、トークンをコピーして安全な場所に保存するか、**ダウンロード**をクリックして**ダウンロード**フォルダーにダウンロードします。

   トークンリストにトークンレコードが表示されます。



6. VDAインストール管理者とトークンを共有します。

   マシンにVDAとトークンをインストールする方法について詳しくは、「VDAのインストール」を参照してください。

トークンの管理

トークンを失効させ、VDA登録に使用できないようにするには、2つのオプションがあります。

- 取り消し：トークンを取り消しますが、ログ記録のためにリストに残します。
- 削除：トークンを取り消し、リストから削除します。

> **注:**

> 期限切れのトークンは14日後に自動的に削除されます。

WebSocket VDA登録ツールを使用してマシンをカタログに登録する

WebSocket VDA登録ツールは、VDAマシン向けのトークンベースの登録を容易にします。このツールは、登録トークンを使用してVDAをマシンカタログに追加することで、接続をWebSocket接続に変換するのに役立ちます。

> **注:**

> このツールは、どのマシンカタログにも登録されていないVDAマシンを登録するために設計されています。

> 登録ツールを実行するには、以下の手順に従ってください。

1. VDAにログオンします。
2. ツール `EnrollMachine.exe` を `C:\Program Files\Citrix\Virtual Desktop Agent\Web Socket Vda Enrollment Tool` で探します。
3. 適切な入力パラメーターを指定してツールを実行します。例: `EnrollMachine.exe -websocket_token_string:xxxxxxxxx`

次の表は、登録ツールの入力パラメータについて説明しています。

パラメータ名	必須	説明	例
`-websocket_token_stdin`	はい	登録トークンを読み取ります。	`.\EnrollMachine.exe -websocket_token_stdin`
`-websocket_token_string`		コマンドラインパラメータから登録トークンを直接読み取ります。	`.\EnrollMachine.exe -websocket_token_string:<token>`
`-websocket_token_file:[token-file-path]`		指定されたパスから登録トークンを読み取ります。	`.\EnrollMachine.exe -websocket_token_file:C:\token\test2.txt`
`log:[log-file-path]`	いいえ	登録ツールのログを表示します。	`.\EnrollMachine.exe log:[C:\ProgramData\Citrix\EnrollMachine\`

パラメータ名	必須	説明	例
			`EnrollMachine.txt]`
`-help`	いいえ	短いヘルプテキストを表示します。	`.\EnrollMachine.exe -help`

登録が成功すると、ツールとログに成功メッセージが表示されます。Web Studioにサインインして、VDAマシンがカタログに追加され、マシンのステータスが登録済みであることを確認してください。

トラブルシューティング

デフォルトでは、登録ツールのログは次の場所にあります。

`C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt`

ログに別のパスを指定した場合は、`log:[log-file-path]` を使用してログを取得できます。

次の表に、登録ツールによって返されるコードを示します。

コード	文字列	説明
0	成功	VDAがマシンカタログに正常に追加されました。
-1	無効な引数	登録トークンの入力パラメーターが無効です。
-2	ブローカーエージェントが見つかりません	ブローカーエージェントサービスが見つかりません。
-3	トークンが無効です	入力されたトークンが無効です。
-4	TokenMissingRequiredClaims	トークンに必要なクレーム（例：CustomerId、登録URI）が不足しています。
-5	InternalError	一般的なエラーが発生しました。

コード	文字列	説明
-6	TimedOut	タスクがタイムアウトしました。
-7	FailedToDetermineMachineADJoinedStatus	マシンのAD参加ステータスを返すサービスが失敗しました。
-8	ADMachineFailedToFindSid	ADマシンのSidを返すサービスが失敗しました。
-9	EnrollRequestFailed	HTTPエラーによりリクエストが失敗しました。
-10	EnrollResponseMissingRequiredFields	登録ツールの応答にパラメーター `VirtualSiteId` がありません。
-11	InsufficientPermission	このタスクを実行するために必要な権限がありません。
-12	FailedToDetermineMachineAadJoinedStatus	マシンのAD参加ステータスをチェックするサービスでエラーが発生しました。
-13	AadMachineFailedToFindDeviceId	システムによって追加された追加パラメーター `AAD device id` が空です。
-14	AadDeviceIdNotValid	システムによって追加された追加パラメーター `AAD device id` は有効なGUIDではありません。
-15	NoValidMacAddress	無効なMACアドレスです。
-16	FailedToGetComputerHostNameForVdaInstanceName	追加パラメーター `VdaInstanceName` を設定するために、コンピューターのホスト名を取得できませんでした。

コード	文字列	説明
-17	VirtualDesktopAgentRegistryKeyFailedToOpen	デリバリーコントローラーのリストを書き込むために、VDAレジストリキーを開けませんでした。
-18	失敗したトークンが最大数に達しました	失敗したトークンが最大数に達しました。

PowerShell を使用する

このセクションでは、PowerShellを使用してカタログを管理する方法について詳しく説明します。

- カタログに関連付けられた警告とエラーを取得する
- イメージに説明を追加する
- OS ディスクをリセットする
- 既存のプロビジョニングスキームのネットワーク設定を変更する
- マシンカタログのバージョンを管理する
- 非マシンプロファイルベースのマシンカタログをマシンプロファイルベースのマシンカタログに変換する
- アクティブなコンピューターアカウントのID情報を修復する
- 既存のマシンカタログのキャッシュ構成を変更する
- ローカルファイル共有アクセスによるVDA更新のサポート

カタログに関連付けられた警告とエラーを取得する

履歴のエラーと警告を取得して、MCS マシンカタログの問題を理解し、それらの問題を修正できます。

PowerShellコマンドを使用して、次のことができます。

- エラーまたは警告のリストを取得する
- 警告の状態を**新規**から**確認済み**に変更する
- エラーまたは警告を削除する

PowerShellコマンドを実行するには:

1. PowerShell ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。

エラーと警告のリストを取得するには：

`Get-ProvOperationEvent` コマンドを実行します。

- パラメーターなしの場合：すべてのエラーと警告を取得します
- `LinkedObjectType` および `LinkedObjectUid` パラメーターを使用する場合：特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告を取得します
- `EventId` パラメーターを使用する場合：このイベント ID に一致する特定のエラーまたは警告を取得します
- `Filter`パラメーターを使用: カスタマイズされたフィルターでエラーまたは警告を取得します

エラーまたは警告の状態を **New** から **Acknowledged** に変更するには：

`Confirm-ProvOperationEvent` コマンドを実行します。

- `EventId`パラメーターを使用: このイベントIDに一致する特定のエラーまたは警告の状態を設定します。特定のイベントまたは警告の`EventId`は、`Get-ProvOperationEvent`コマンドの出力として取得できます。
- `LinkedObjectType`および`LinkedObjectUid`パラメーターを使用: 特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告の状態を設定します
- `All` パラメーターを使用: すべてのエラーと警告の状態を**確認済み**に設定します

エラーまたは警告を削除するには：

`Remove-ProvOperationEvent` コマンドを実行します。

- `EventId` パラメーターを使用: このイベント ID に一致する特定のエラーまたは警告を削除します。特定のイベント ID の`EventId`は、`Get-ProvOperationEvent` コマンドの出力として取得できます。
- `LinkedObjectType` および `LinkedObjectUid` パラメーターを使用: 特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告を削除します。
- `All` パラメーターを使用: すべてのエラーと警告を削除します。

詳細については、Citrix PowerShell SDKを参照してください。

ハイパーバイザーアクセスなしでマシンを削除する

VM またはプロビジョニングスキームを削除する場合、MCS は VM から、場合によってはベースディスクからもタグを削除する必要があります。これにより、削除オプションに含まれるリソースが MCS によって追跡または識別されなくなります。ただし、これらのリソースの一部はハイパーバイザーを介してのみアクセス可能です。ハイパーバイザーアクセスがない場合でも、データベースから VM、ベースディスク、ACG 内のイメージなどの VM リソースオブジェクトを削除するには、`Remove-ProvVM` PowerShell の `PurgeDBOnly` オプションを使用します。

このオプションは以下で有効になります:

- すべてのサポートされているハイパーバイザー
- 永続的および非永続的 VM

制限事項

-PurgeDBOnly コマンドと -ForgetVM コマンドを同時に使用することはできません。

PurgeDBOnly コマンドを使用する

PowerShell コマンド `Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -ForgetVM` を実行すると、次のようなシナリオで削除操作が失敗する可能性があります。

- ホスト接続がメンテナンスモードになっている
- 無効な資格情報
- 認証の失敗
- 不正な操作
- ハイパーバイザーに到達できない

> **注:**
>
> Remove-provVM -ForgetVM は永続的な VM のみを対象とします。リスト内の VM のいずれかが非永続的である場合、操作は失敗します。

> ハイパーバイザーに到達できないために操作が失敗すると、次のプロンプトが表示されます。

`Try to use -PurgeDBOnly option to clean DDC database.`.

`Remove-ProvVM` PowerShell コマンドで `-PurgeDBOnly` オプションを使用して、MCS データベースから VM の参照を削除します。例：

```
Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -PurgeDBOnly
```

イメージに説明を追加する

マシンカタログのイメージ更新に関連する変更について、情報を提供する説明を追加できます。この機能を使用して、カタログの作成時、またはカタログの既存のマスターイメージを更新する際に説明を追加します。カタログ内の各マスターイメージの情報を表示することもできます。イメージの説明を追加または表示するには、次のコマンドを使用します。

- マスターイメージを使用してマシンカタログを作成する際にメモを追加するには、`NewProvScheme`コマンドで`MasterImageNote`パラメーターを使用します。例：

  ```
  C:\PS>New-ProvScheme -ProvisioningSchemeName <name> -HostingUnitName
  <name> -IdentityPoolName <name> -MasterImageVM

  XDHyp:\HostingUnits\<hosting unit name>\<vm name>.vm\Base.snapshot
  -MasterImageNote "Note"
  ```

- マシンカタログに関連付けられているマスターイメージを更新するには、`Publish-ProvMasterVMImage`コマンドで`MasterImageNote`パラメーターを使用します。例：

  ```
  C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName <name>
  -MasterImageVM XDHyp:\HostingUnits\<hosting unit name>\<vm
  name>.vm\base.snapshot -MasterImageNote "Note"
  ```

- 各イメージの情報を表示するには、Get-ProvSchemeMasterVMImageHistoryコマンドを使用します。例：

  ```
  C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
  MyScheme -Showall
  ```

ロールバックの進行状況を追跡するには、 でカタログを見つけて、インラインの進行状況バーと段階的な進行状況グラフを表示します。

次のような特定のシナリオでは、ロールバックできません。（ オプションは表示されません）。

- ロールバックする権限がありません。

- カタログがMCSを使用して作成されていません。
- カタログがOSディスクのイメージを使用して作成されています。
- カタログの作成に使用されたスナップショットが破損しています。
- カタログ内のマシンに対するユーザーの変更が保持されません。
- カタログ内のマシンが実行中です。

OSディスクをリセットする

MCSで作成されたマシンカタログ内の永続VMのOSディスクをリセットするには、PowerShellコマンド`Reset-ProvVMDisk`を使用します。現在、この機能はAWS、Azure、XenServer、Google Cloud、SCVMM、VMwareの仮想化環境に適用できます。

PowerShellコマンドを正常に実行するには、以下を確認してください。

- ターゲットVMが永続MCSカタログ内にあること。
- MCSマシンカタログが正常に機能していること。
- これは、プロビジョニングスキームとホストが存在し、プロビジョニングスキームに正しいエントリがあることを意味します。
- ハイパーバイザーがメンテナンスモードになっていないこと。
- ターゲットVMがシャットダウンされ、メンテナンスモードになっていること。

OSディスクをリセットするには、次の手順を実行します。

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために、**asnp citrix***を実行します。
3. 次のいずれかの方法でPowerShellコマンド`Reset-ProvVMDisk`を実行します。
    - VMのリストをコンマ区切りリストとして指定し、各VMでリセットを実行します。

      ```
      Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc","def")
      -OS
      ```

    - VMのリストを`Get-ProvVM`コマンドからの出力として指定し、各VMでリセットを実行します。

      ```
      (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk "abc"
      -OS
      ```

- 名前で単一のVMを指定します。

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
```

- `Get-ProvVM`コマンドによって返された各VMに対して個別のリセットタスクを作成します。各タスクがハイパーバイザーの機能チェック、各VMの接続チェックなど、同じ冗長なチェックを実行するため、これは効率的ではありません。

```
Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk
-ProvisioningSchemeName "xxx" -OS
```

4. リセットされるVMのリストと、回復不能な操作であるという警告メッセージが表示された確認プロンプトが表示されます。回答を入力せずに**Enter**キーを押すと、それ以上のアクションは実行されません。

> **注：**
>
> リセットプロセスが完了するまで、VMをメンテナンスモードから解除したり、電源をオンにしたりしないでください。

> PowerShellコマンド`-WhatIf`を実行して、実行されるアクションを表示し、アクションを実行せずに終了できます。

確認プロンプトを以下のいずれかの方法でバイパスすることもできます。

- `-Force` パラメーターを指定します。

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
-Force
```

- `-Confirm:$false`パラメーターを指定します。

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
-Confirm:$false
```

- `Reset-ProvVMDisk`を実行する前に、`$ConfirmPreference`を**None**に変更します。

```
PS C:\Windows\system32> $ConfirmPreference='None'

PS C:\Windows\system32> $ConfirmPreference

None

PS C:\Windows\system32> Reset-ProvVMDisk -ProvisioningSchemeName
"xxx" -VMName "abc" -OS
```

5. `Reset-ProvVMDisk` コマンドによって返されたタスクのステータスを取得するには、`Get-ProvTask` を実行します。

既存のプロビジョニングスキームのネットワーク設定を変更する

既存のプロビジョニングスキームのネットワーク設定を変更して、新しいVMが新しいサブネットワーク上に作成されるようにすることができます。ネットワーク設定を変更するには、`Set-ProvScheme` コマンドで `-NetworkMapping` パラメーターを使用します。

> **注:**
>
> この機能は、Citrix Virtual Apps and Desktops 2203 LTSR CU3以降のバージョンでサポートされています。

既存のプロビジョニングスキームのネットワーク設定を変更するには、次の手順を実行します。

1. PowerShellウィンドウで、コマンド `asnp citrix*` を実行してPowerShellモジュールをロードします。
2. 変更するネットワークパスに移動するには、`(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` を実行します。
3. 新しいネットワーク設定に変数を割り当てます。例：

   ```
   $NewNetworkMap = @{"0"= "XDHYP:\HostingUnits\MyNetworks\Network
   0.network"}
   ```

4. `Set-ProvScheme -ProvisioningSchemeName "name" -NetworkMapping $NewNetworkMap` を実行します。

5. 既存のプロビジョニングスキームの新しいネットワーク設定を確認するには、`(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` を実行します。

マシンカタログのバージョンを管理する

MCSマシンカタログが`Set-ProvScheme`コマンドで更新されると、現在の構成がバージョンとして保存されます。その後、PowerShellコマンドを使用して、マシンカタログのさまざまなバージョンを管理できます。次のことができます。

- マシンカタログのバージョンリストを表示する
- 以前のバージョンを使用してマシンカタログを更新する
- そのマシンカタログのVMで使用されていないバージョンを手動で削除する
- マシンカタログによって保持される最大バージョン数を変更する（デフォルトは99）

バージョンには、マシンカタログの次の情報が含まれます。

- VMCpuCount
- VMMemoryMB
- CustomProperties
- ServiceOffering
- MachineProfile
- NetworkMapping
- SecurityGroup

マシンカタログのさまざまなバージョンを管理するには、次のコマンド（例として提供）を実行します。

- マシンカタログのさまざまなバージョンの構成詳細を表示するには:

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
```

- マシンカタログの特定のバージョンの構成詳細を表示するには:

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version 2
```

- マシンカタログに関連付けられているバージョンの総数を表示するには:

```
(Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count
```

- 以前のバージョンを使用してマシンカタログを更新するには:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
```

- そのマシンカタログのVMで使用されていないバージョンを手動で削除するには:

```
Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version
3
```

- マシンカタログで保持される最大バージョン数を設定します（デフォルトは99）。この設定は、すべてのカタログに適用されます。たとえば、この場合、すべてのMCSプロビジョニング済みカタログに対して最大15バージョンが保持されます。

```
Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -Value
15
```

バージョン数が最大バージョン数に達した場合、マシンカタログ内のいずれかのVMで古いバージョンが使用されていると、新しいバージョンを作成できません。その場合は、次のいずれかを実行してください:

- マシンカタログによって保持される最大バージョン数の制限を増やします。
- 古いバージョンを使用している一部のVMを更新して、それらの古いバージョンがどのVMからも参照されなくなり、削除できるようにします。

マシンプロファイルに基づかないマシンカタログを、マシンプロファイルに基づくマシンカタログに変換する

VM、テンプレート仕様（Azureの場合）、起動テンプレート（AWSの場合）、またはVMwareテンプレート（VMwareの場合）をマシンプロファイルの入力として使用して、マシンプロファイルに基づかないマシンカタログをマシンプロファイルに基づくマシンカタログに変換できます。カタログに追加された新しいVMは、明示的なカスタムプロパティによって上書きされない限り、マシンプロファイルからプロパティ値を取得します。

注:

既存のマシンプロファイルに基づくマシンカタログを、マシンプロファイルに基づかないマシンカタログに変更することはできません。

これを行うには:

1. VMを含み、マシンプロファイルを含まない永続的または非永続的なマシンカタログを作成します。
2. **PowerShell** ウィンドウを開きます。
3. マシンプロファイルからマシンカタログに追加された新しいVMにプロパティ値を適用するには、`Set-ProvScheme` コマンドを実行します。例:

   - Azureの場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile XDHyp:
     \HostingUnits\<HostingUnitName>\machineprofile.folder\<ResourceGroup
     Name>\<TemplateSpecName>\<VersionName>
     ```

   - AWSの場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile "XDHyp:
     \HostingUnits\<hosting-unit>\<launch-
     template>.launchtemplate\<launch-template-
     version>.launchtemplateversion"
     ```

   - VMwareの場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-prov-scheme"
     -MachineProfile "XDHyp:\HostingUnits\my-hosting-unit\my-
     template.template"
     ```

     注:

     VMwareテンプレートから `FolderID` が派生するのを避けるため、`FolderID` をカスタムプロパティとして設定します。

アクティブなコンピューターアカウントのID情報を修復する

ID関連の問題があるアクティブなコンピューターアカウントのID情報をリセットできます。マシンパスワードと信頼キーのみをリセットするか、IDディスクのすべての構成をリセットするかを選択できます。この実装は、永続的および非永続的な両方のMCSマシンカタログに適用できます。

> **注:**
>
> 現在、この機能はAWS、GCP、Azure、SCVMM、XenServer、およびVMwareの仮想化環境でサポートされています。

条件

IDディスクを正常にリセットするには、以下を確認してください。

- VMをシャットダウンし、メンテナンスモードに設定します
- PowerShellコマンドにパラメーター -OS を含めないでください

IDディスクのリセット

IDディスクをリセットするには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. ID情報をリセットします。
    - マシンのパスワードと信頼キーのみをリセットするには、次のコマンドを実行します。

      ```
      Repair-AcctIdentity -IdentityAccountName TEST\VM1
      -PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
      -Target IdentityInfo
      ```

      コマンドで使用されるパラメーターの説明は次のとおりです。

      - IdentityAccountName：修復する必要があるIDアカウントの名前。
      - PrivilegedUserName：IDプロバイダー（ADまたはAzureAD）に対する書き込み権限を持つユーザーアカウント。
      - PrivilegedUserPassword：PrivilegedUserNameのパスワード。

    - Target：修復アクションのターゲット。アカウントのパスワード/信頼キーを修復するためのIdentityInfo、およびMicrosoft Entraハイブリッド参加済みマシンIDのユーザー証明書属性を修復するためのUserCertificateを指定できます。

- IDディスクのすべての構成をリセットするには、次の順序で次のコマンドを実行します。

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1
-PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
-Target IdentityInfo
```

```
Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>  -
Identity
```

- IDディスクを完全に再作成するには:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name>
-Identity -Recreate
```

> **注:**
>
> マシンがVDAバージョン2511以降を使用するWindowsマシンの場合、`-Recreate` の設定に関係なく、以前と同じ `MachineGuid` を引き続き使用します。

4. 「**y**」と入力してアクションを確定します。`-Force` パラメーターを使用して確認プロンプトをスキップすることもできます。例：

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name>
-Identity -Force
```

5. 更新されたIDディスク設定を確認するには、`Get-ProvVM -ProvisioningSchemeName <name -VMName <name>` を実行します。IDディスクの属性（例：`IdentityDiskId`）は更新されている必要があります。`StorageId` と `IdentityDiskIndex` は変更してはいけません。

既存のマシンカタログのキャッシュ構成を変更する

MCSIOが有効な非永続カタログを作成した後、Set-ProvSchemeコマンドを使用して次のパラメーターを変更できます。

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

この機能は現在、以下に適用されます。

- GCPおよびMicrosoft Azure環境、および
- MCSIOが有効な非永続カタログ

要件

キャッシュ構成を変更するための要件は次のとおりです。

- 最新バージョンのVDA（2308以降）に更新します。
- 既存のマシンカタログに対してパラメーター `UseWriteBackCache` を有効にします。`UseWriteBackCache` が有効なマシンカタログを作成するには、`New-ProvScheme` を使用します。例：

```
New-ProvScheme -ProvisioningSchemeName $CatalogName -HostingUnitUid
$HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

-MasterImageVM $MasterImage `

-ServiceOffering $ServiceOffering `

-NetworkMap $NetworkMap `

-SecurityGroup $SecurityGroup `

-UseWriteBackCache -WriteBackCacheDiskSize 8
```

キャッシュ構成を変更する

Set-ProvSchemeコマンドを実行します。例：

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.ProvisioningSchemeName
-WriteBackCacheDisk32 -WriteBackCacheMemorySize 128
```

注:

- `WriteBackCacheDiskSize` の値は、少なくとも 1 GB のキャッシュディスクストレージが必要なため、ゼロより大きくする必要があります。
- `WriteBackCacheMemorySize` の値は、マシンカタログのメモリサイズよりも小さくする必要があります。
- これらの変更は、変更後にカタログに追加された新しいVMにのみ影響します。既存のVMはこれらの変更の影響を受けません。

ローカルファイル共有アクセスによるVDA更新サポート

PowerShellコマンドレットを介してVDAインストーラーの場所を指定することで、各VDAがCitrix Managed Azure CDNから新しいVDAインストーラーを取得できるようにするためのネットワークルールを提供する手間を省くことができます。

PowerShellコマンドレット

ローカルファイル共有からインストーラーを使用できるようにする、**New-VusCatalogSchedule** および **New-VusMachineUpgrade** コマンドレットに追加された2つの新しいオプションパラメーター

- **VdaWorkstationPackageUri** - ワークステーションOS VDAインストーラーへのUNCパスを指定するため
- **VdaServerPackageUri** - サーバーOS VDAインストーラーへのUNCパスを指定するため

前提条件

- VDA 2311に付属するVUSエージェントインストーラー
- VDAアップグレードエージェントをバージョン7.40.0.35以降にアップグレード（VDAインストーラーバージョン2311以降を使用）
- Virtual Apps and Desktops Remote PowerShell SDK バージョン 7.40 以降（Jan 10, 2024 以降にリリース）

ファイル共有のアクセス許可を設定する方法

VDAインストーラーパッケージを含むネットワーク共有には、ローカルシステム（NT AUTHORITY\SYSTEMプリンシパル）として実行されるVDAアップグレードエージェントサービスに対する読み取りアクセス権が必要です。

- **ドメイン参加済みファイル共有のアクセス許可**

VDAマシンがドメインに参加している場合、**ローカルシステム**アカウント（VUAはローカルシステムとして実行）は、ネットワーク共有にアクセスする際にコンピューターの資格情報を使用します。

最小特権のアクセス許可は、Domain Computers に **読み取り** アクセスを付与することで設定できます。

a. ファイルを共有するネットワーク上のユーザーを選択します。
b. **詳細な共有設定**をクリックし、**ファイルとプリンターの共有**をオンにします。

- **ドメインに参加していないファイル共有のアクセス許可**

VDAマシンがドメインに参加していない場合、**ローカルシステム**アカウント（VUAはローカルシステムとして実行）は、ネットワーク共有にアクセスする際に**ANONYMOUS LOGON**を使用します。

a. 共有フォルダーを選択します。
b. パスワード保護を無効にします。
    a. フォルダーの**プロパティ**に移動します。
    b. **ネットワークと共有センター**を選択します。
    c. **パスワード保護共有**をオフにします。
c. **詳細な共有**をクリックして、共有アクセス許可を付与します。
    a. **アクセス許可**を選択します。
    b. **ANONYMOUS LOGON**に**読み取り**共有権限を付与します。
d. フォルダーのアクセス許可を付与するには、**セキュリティタブ**を選択します。
    a. 共有フォルダーにアクセス許可を追加するには、**編集**をクリックします。
    b. **ANONYMOUS LOGON**にフォルダーのアクセス許可を付与する共有フォルダーを選択します。
e. **ファイルとプリンターの共有**を有効にするには、**詳細設定**をクリックします。
f. 共有フォルダー名を**ネットワークアクセスセキュリティポリシー**に追加します。

> **注:**
>
> 変更をすぐに有効にするには、マシンを再起動します。

ローカルファイル共有からのVDAアップデート

1. VDAインストーラーをダウンロードし、共有ファイルに配置します。

   注:

   Virtual Upgrade Serviceを使用すると、Current ReleaseトラックまたはLTSRトラックのいずれかを選択できます。

   例: マシンカタログがCurrent Release 2311に設定されており、VDAバージョンが2305の場合、VDAをバージョン2311にアップグレードする必要があります。

   a. 弊社のWebサイトの**ダウンロード**ページに移動します。
   b. 製品として**Citrix Virtual Apps and Desktops**を選択します。
   c. **Citrix Virtual Apps and Desktops 7 2311, All Editions** という項目を選択します。
   d. 「**製品ISOに含まれるが個別にパッケージ化されているコンポーネント**」の展開可能な項目からVDAインストーラーを選択します。

2. カタログの種類に基づいて、関連するVDAインストーラーを選択します。

   - カタログの種類が**マルチセッション**の場合は、「**Multi-session OS VDA installer**」をダウンロードします。
   - カタログの種類が**シングルセッション**の場合は、「**Single-session OS VDA installer**」をダウンロードします。
   - カタログの種類が**Remote PC Access**の場合は、「**Single-session OS Core Services VDA installer**」をダウンロードします。

注:

ファイル共有インストーラーのバージョンは、VUSによってクラウドに公開された最新のインストーラーバージョンと**正確に**一致している必要があります。

VMのストレージ移行

VMwareおよびXenServer環境では、既存のVMのディスクストレージを古いストレージから新しいストレージに移動できます。移行中、MCSは電源管理、OSディスクのリセットなどのVM機能を保持します。新しいディスクストレージを使用して、新しいVMをマシンカタログに追加することもできます。これを行うには、PowerShellコマンド `Move-ProvVMDisk` を使用します。

フルクローン永続VMと非永続VMを移行できます。

- 永続的なフルクローンVMの場合：OSディスク、IDディスク、およびMCSプロビジョニングされていないディスク。
- 非永続VMの場合：OSディスク、IDディスク、およびライトバックキャッシュ（WBC）ディスク。

新しいストレージは、次の条件を満たす必要があります。

- 古いストレージと同じクラスター内にある必要があります。
- VMが実行されているホストは、古いデータストアと新しいデータストアの両方にアクセスできる必要があります。

ディスクストレージを移行する

ディスクストレージを移行するには：

1. 既存のホスティングユニットに宛先ストレージを追加します。宛先ストレージを追加するには、PowerShellコマンド `Add-Hyphostingunitstorage` を実行します。

   古いストレージに新しいVMを追加したくない場合は、古いストレージを **Superseded** に変更します。これはStudioまたはPowerShellコマンドを使用して実行できます。Studioについては、「ストレージの編集」を参照してください。または、`Set-Hyphostingunitstorage` を実行し、`Superseded` を `true` に設定して、古いストレージでの新しいVMの作成を無効にします。

   > **注:**
   >
   > 非永続VMの場合：
   >
   > - WBCを使用している場合は、ホスティングユニットでWBC宛先ストレージを構成します。

- OS宛先ストレージが構成されている場合、WBC（使用されている場合）はOS宛先ストレージと互換性がある必要があります。
- OS宛先ストレージが構成されていない場合、WBC（使用されている場合）は現在のOSストレージと互換性がある必要があります。

2. VMをシャットダウンし、**メンテナンスモード**をオンにします。
3. プロビジョニングスキーム、ホスティングユニット、OSディスクストレージ、およびWBCディスクストレージに関する情報を取得します。
   - OSストレージ情報については、`ProvResourceInStorage` を実行します。例：

     ```
     $result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName
     xxxxx

     $result

     $result.ProvResourceInStorage | Format-List -Property *
     ```

   - WBCストレージ情報については`TemporaryStorageInfo`を実行します。例:

     ```
     $result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName
     xxxxx

     $result

     $result.TemporaryStorageInfo | Format-List -Property *
     ```

4. OSディスク、IDディスク、およびWBCディスク（非永続VMに適用）を、`Move-ProvVMDisk` PowerShellコマンドを使用して宛先ストレージに移行します。

注:

- 常にOSディスクとIDディスクをDiskTypeおよび`DestinationStorageId`パラメーターで指定します。
- OSディスクとIDディスクの`DestinationStorageId`は同じである必要があります。

例:

永続VM：

```
(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk
-ProvisioningSchemeName "myFullCloneProvScheme" -VMName "machine01"
-DiskType OS,Identity -DestinationStorageId datastore1,datastore1
```

重要:

永続VMの場合、すべてのディスクが移動されます。移動するディスクを選択することはできません。

非永続VM：

```
(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk
-ProvisioningSchemeName "myCleanOnBootProvScheme" -VMName "machine01"
-DiskType OS,Identity,WBC -DestinationStorageId None,None,datastore1
```

重要:

- 特定のディスクを移行したくない場合は、`DestinationStorageId`パラメーターの値を`None`に設定します。
- VMにWBCディスクがある場合は、WBCディスクを`DiskType`パラメーターに追加し、必要な情報を`DestinationStorageId`パラメーターに追加します。

既存のMCSプロビジョニング済みカタログを準備済みイメージマシンカタログに移行する

既存のMCSプロビジョニング済みマシンカタログは、PowerShellコマンド`Set-ProvSchemeImage`を使用して準備済みイメージマシンカタログに変換できます。ただし、移行後にレガシーカタログに戻すことはできません。現在、この機能はAzureおよびVMware仮想化環境に適用されます。

制限事項

次の制限事項を考慮してください。

- MCSカタログが永続データディスクを使用している場合、そのカタログを準備済みイメージを使用するように移行することはできません。
- MCSカタログがアンマネージドディスクを使用している場合、そのカタログを準備済みイメージを使用するように移行することはできません。

準備済みイメージマシンカタログへの移行

移行するには、次の手順を実行します。

1. StudioまたはPowerShellコマンドを使用して、イメージ定義とイメージバージョンを作成します。イメージ定義とイメージバージョンを作成する手順については、以下を参照してください。
   - アジュール:
     - ウェブ Studio
     - PowerShell
   - ヴイエムウェア：
     - ウェブスタジオ(https://docs.citrix.com/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/create-prepared-image-machine-catalogs-vmware#use-web-studio)
     - PowerShell
2. プロビジョニングスキームのUIDを取得するには、`Get-ProvScheme`コマンドを実行します。例:

   ```
   Get-ProvScheme -ProvisioningSchemeName <name> | select
   ProvisioningSchemeName, ProvisioningSchemeUid
   ```

3. イメージ定義名、イメージバージョン仕様のUIDを取得するには、`Get-ProvImageVersionSpec`コマンドを実行します。例:

   ```
   Get-ProvImageVersionSpec -ImageDifinitionName <name> -Filter
   {IsPrepared -eq $true} | select ImageDefinitionName ImageVersionSpecUId
   ```

4. 既存のMCSプロビジョニング済みマシンカタログを準備済みイメージマシンカタログに移行するには、`Set-ProvSchemeImage`コマンドを実行します。例:

```
Set-ProvSchemeImage -ProvisioningSchemeName [ProvisioningSchemeName]
-ImageVersionSpecUid [ImageVersionSpecUid]
```

5. カタログが移行されたことを確認するには、`Get-ProvScheme`コマンドを実行します。例:

```
Get-ProvScheme -ProvisioningSchemeName <name> | select
ProvisioningSchemeName, ProvisioningSchemeUid, ImageVersionSpecUid
```

トラブルシューティング

- 「電源状態不明」のステータスを持つマシンについては、ガイダンスとしてCTX131267を参照してください。
- 継続的に不明な電源状態を示すVMを修正するには、継続的に不明な電源状態を示すVMを修正する方法を参照してください。

次のステップ

特定のクラウドサービスカタログの管理については、以下を参照してください。

- AWSカタログの管理
- XenServerカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-manage/manage-machine-catalog-citrix-hypervisor.html)
- Google Cloud Platformカタログの管理
- Microsoft Azureカタログの管理
- マイクロソフト システム センター バーチャル マシン マネージャー カタログの管理(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-manage/manage-machine-catalog-mscvmm.html)
- VMwareカタログの管理

AWS EC2カタログを管理する

マシンカタログを管理するウィザードについては、(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-manage.html)で説明しています。以下の情報は、AWS EC2クラウド環境に固有の詳細を扱っています。

> **注:**
>
> AWSカタログを管理する前に、AWSカタログの作成を完了する必要があります。AWS EC2カタログの作成を参照してください。

タグを削除する

カタログまたはVMを作成すると、MCSによって作成されたタグが以下のリソースに作成されます。

- 仮想マシン
- ルートディスクボリューム
- 識別ディスクボリューム
- NIC
- ルートディスクイメージ (AMI)
- 起動テンプレート
- AMIまたはルートディスクのスナップショット

Citrix®データベースからVMとマシンカタログを削除し、MCSによって作成されたタグを削除できます。以下を使用できます。

- マシンカタログから単一のVMまたはVMのリストからVMとMCSによって作成されたタグを削除するには、`Remove-ProvVM`を`ForgetVM`パラメーターとともに使用します。
- Citrixデータベースからマシンカタログを、マシンカタログからリソースを削除するために、`ForgetVM`パラメーターを指定して`Remove-ProvScheme`を実行します。

この機能は、永続VMにのみ適用されます。

これを行うには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために、`asnp citrix*`を実行します。
3. VMを削除する前に、VMのロックを解除します。例：

```
Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
```

4. VM、マシンカタログ、およびMCSによって作成されたタグをリソースから削除するには、次のいずれかのコマンドを実行します。

   - Citrixデータベースから VMを、VMからタグを削除するために、`ForgetVM`を指定して`Remove-ProvVM`を実行します。例：

     ```
     Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"
     -ForgetVM
     ```

   - Citrixデータベースからマシンカタログを、マシンカタログからリソースを削除するために、`Remove-ProvScheme`を実行します。例：

     ```
     Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -ForgetVM
     ```

5. VMがDelivery Controller™から削除されていることを確認しますが、ハイパーバイザーからは削除されていません。

   a. `Get-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"`を実行します。これは何も返さないはずです。

   b. AWS EC2コンソールに移動します。VMは表示されますが、タグは削除されています。以下のリソースからタグが削除されます。

      - 仮想マシン
      - ルートディスクボリューム
      - 識別ディスクボリューム
      - NIC

6. マシンカタログを削除した場合、カタログがDelivery Controllerから削除されていることを確認します。

   a. `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`を実行します。これはエラーを返すはずです。

   b. AWS EC2コンソールで、以下のリソースが削除されていることを確認します。

      - ルートディスクイメージ (AMI)
      - 起動テンプレート
      - AMIまたはルートディスクのスナップショット

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
IDディスク	"名前": "VMName_IdentityDisk"
	"Xd構成": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
イメージ	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
NIC	"説明": "XD NIC"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OSディスク	"Name": "VMName_rootDisk"
	"XdConfig" は "XdProvisioned=True" です
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "Citrixリソース": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
PrepVM	"Name": "準備 - カタログ名 - xxxxxxxxxx"
	"XdConfig": "XdProvisioned=true"

リソース名	タグ
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "Citrix リソース": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
公開済みスナップショット	"XdConfig": "XdProvisioned=true"
	ボリュームワーカーAMIのスナップショットでない場合、"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
テンプレート	[when AwsCaptureInstanceProperties = true] "XdConfig": "XdProvisioned=true"
	[when AwsCaptureInstanceProperties = true] "Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "CitrixResource": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
カタログ内のVM	"Xd構成": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "CitrixResource": ""
	[when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:id":"lt-xxxx"

リソース名	タグ
	[when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:version": "n"
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
ボリュームワーカーAMI	"Xdコンフィグ": "Xdプロビジョンド=true"
ボリュームワーカーブートストラッパー	"ネーム": "XenDesktop® テンプ"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixVolumeWorkerBootstrapper": ""
ボリュームワーカーインスタンス	"名前": "Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx"
	"Xd構成": "Xdプロビジョニング済み=true"

詳細情報

- 接続とリソースの作成および管理
- AWS EC2への接続
- マシンカタログの作成
- AWS EC2カタログの作成
- マシンカタログの管理

Amazon WorkSpaces Core マネージドインスタンスのカタログを管理する

(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-manage)では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Amazon WorkSpaces Core マネージドインスタンスに固有の詳細を扱います。

> **注:**
>
> Amazon WorkSpaces Core マネージドインスタンスのカタログを管理する前に、Amazon WorkSpaces Core マネージドインスタンスのカタログの作成を完了する必要があります。詳細については、「Amazon WorkSpaces Core マネージドインスタンスのカタログを作成する」を参照してください。

タグを削除する

カタログまたはVMを作成すると、以下のリソースにタグが作成されます。

- 仮想マシン
- ルートディスクボリューム
- 識別ディスクボリューム
- 弾力性のあるネットワークインターフェース (ENI)
- ルートディスクイメージ (AMI)
- 起動テンプレート
- AMIまたはルートディスクのスナップショット

Citrix®データベースからVMとマシンカタログを削除し、Citrixが作成したタグを削除できます。以下を使用できます。

- マシンカタログから単一のVMまたはVMのリストからVMとCitrixが作成したタグを削除するには、`ForgetVM`パラメーターを指定した`Remove-ProvVM`を使用します。

  > **注:**
  >
  > `ForgetVM`パラメーターを使用すると、Citrixのプロビジョニングスキームデータベースからが削除されますが、VMはハイパーバイザーに残ります。

- `ForgetVM`パラメーターを指定して`Remove-ProvScheme`を実行し、Citrixデータベースからマシンカタログを削除し、マシンカタログからリソースを削除します。

これを行うには：

1. **PowerShell** ウィンドウを開きます。

2. `asnp citrix*` を実行して、Citrix固有のPowerShellモジュールをロードします。
3. VMを削除する前に、VMのロックを解除します。例:

```
Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
```

4. 次のいずれかのコマンドを実行して、VM、マシンカタログ、およびリソースからCitrixが作成したタグを削除します。

   - `ForgetVM` を指定して `Remove-ProvVM` を実行し、Citrixデータベースから VMを削除し、VMからCitrixが作成したタグを削除します。例:

     ```
     Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"
     -ForgetVM
     ```

   - `Remove-ProvScheme`を実行して、Citrixデータベースからマシンカタログを削除し、マシンカタログからリソースを削除します。例：

     ```
     Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -ForgetVM
     ```

5. VMがDelivery Controller™から削除されているが、ハイパーバイザーからは削除されていないことを確認します。

   a. `Get-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"`を実行します。これは何も返さないはずです。

   b. AWS EC2コンソールに移動します。VMは表示されますが、Citrixが作成したタグは削除されています。以下のリソースからCitrixが作成したタグが削除されます。

      - 仮想マシン
      - ルートディスクボリューム
      - 識別ディスクボリューム
      - ENI

6. マシンカタログを削除した場合は、そのカタログがDelivery Controllerから削除されていることを確認します。

   a. `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`を実行します。これはエラーを返すはずです。

   b. AWS EC2コンソールで、以下のリソースが削除されていることを確認します。

- ルートディスクイメージ (AMI)
- 起動テンプレート
- AMIまたはルートディスクのスナップショット

MCSによって作成されたリソースを識別する

以下は、MCSがAWSプラットフォーム上のリソースに追加するタグです。表のタグは「"key":"value"」として表されています。

リソース名	タグ
IDディスク	"名前": "VMName_IdentityDisk"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
イメージ	"Xd設定": "Xdプロビジョニング済み=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
ENI	"説明": "XD Nic"
	"XdConfig": "XdProvisioned=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OS ディスク	"名前": "VMName_rootDisk"
	"Xd構成": "XdProvisioned=True"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
PrepVM	"Name": "準備 - カタログ名 - xxxxxxxxxx"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

リソース名	タグ
公開済みスナップショット	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
テンプレート	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
カタログ内のVM	"XdConfig": "XdProvisioned=true"
	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

詳細情報

- AWS仮想化環境
- Amazon WorkSpaces Coreマネージドインスタンスへの接続
- イメージ管理
- Amazon WorkSpaces Coreマネージドインスタンス用の準備済みイメージを作成する
- Amazon WorkSpaces Core マネージドインスタンスのカタログを作成する
- 準備済みイメージのマシンカタログを管理する

Google Cloud Platformカタログを管理する

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Google Cloud環境に固有の詳細を扱います。

> **注:**
>
> Google Cloud Platformカタログを管理する前に、Google Cloud Platformカタログの作成を完了する必要があります。Google Cloud Platformカタログの作成を参照してください。

マシンカタログの管理

カタログにマシンを追加したり、マシンを更新したり、更新をロールバックしたりするには、「マシンカタログの管理」を参照してください。

電源管理

Citrix DaaS™を使用すると、Google Cloudマシンの電源管理を行うことができます。左ペインの**検索**ノードを使用して、電源管理したいマシンを見つけます。以下の電源操作が利用可能です。

- 削除
- 起動
- 再起動
- 強制再起動
- シャットダウン
- 強制シャットダウン
- デリバリーグループに追加
- タグの管理
- メンテナンスモードをオンにする

Autoscaleを使用してGoogle Cloudマシンを電源管理することもできます。これを行うには、Google Cloudマシンをデリバリーグループに追加し、そのデリバリーグループでAutoscaleを有効にします。Autoscaleの詳細については、「Autoscale」を参照してください。

PowerShellを使用してプロビジョニングされたマシンを更新する

`Set-ProvScheme` コマンドはプロビジョニングスキームを変更します。ただし、既存のマシンには影響しません。PowerShell コマンド `Set-ProvVMUpdateTimeWindow` を使用すると、現在のプロビジョニングスキームを既存の永続マシンまたは非永続マシン、あるいはマシンセットに適用できます。現在、GCP では、この機能でサポートされているプロパティの更新はマシンプロファイルです。

更新できるもの:

- 単一のVM
- 特定のVMのリスト、またはプロビジョニングスキームIDに関連付けられているすべての既存VM
- 特定のVMのリスト、またはプロビジョニングスキーム名に関連付けられているすべての既存VM

既存のVMを更新するには：

1. 既存のマシンの構成を確認します。例えば、,

```
Get-ProvScheme | select ProvisioningSchemeName,
ProvisioningSchemeVersion
```

2. プロビジョニングスキームを更新します。例えば、,

```
`Set-ProvScheme –ProvisioningSchemeName "my-catalog" –MachineProfile
"XDHyp:\HostingUnits\<hosting-unit>\machineprofileinstance.vm"
```

3. VMの現在のプロパティが現在のプロビジョニングスキームと一致しているか、およびVMに保留中の更新アクションがあるかを確認します。例えば、,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

   特定のバージョンのマシンを見つけることもできます。例:

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
ProvisioningSchemeVersion
```

4. 既存のマシンを更新します。

   - すべての既存のマシンを更新するには：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

   - 特定のリストのマシンを更新するには：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

   - `Get-ProvVM`の出力に基づいてマシンを更新するには：

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
-DurationInMinutes -1
```

5. 更新がスケジュールされているマシンを見つけます。例えば、,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

6. マシンを再起動します。次回の電源投入時に、プロパティの変更が既存のマシンに適用されます。以下のコマンドを使用して更新されたステータスを確認できます。

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

既存のカタログのディスク関連のカスタムプロパティを変更する

既存のカタログおよびカタログの既存のVMの、以下のディスク関連のカスタムプロパティを変更できます。

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

注:

- `StorageType` プロパティはOSディスク用です
- `PersistOsDisk` プロパティは、ライトバックキャッシュが有効な非永続カタログにのみ設定できます

この実装により、カタログ作成後でも異なるディスクに異なるストレージタイプを選択できるようになり、さまざまなストレージタイプに関連する価格のバランスを取ることができます。

これを行うには、PowerShell コマンド `Set-ProvScheme` と `Set-ProvVMUpdateTimeWindow` を使用します。

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix®*`を実行します。
3. カスタムプロパティを取得するには、`Get-ProvVM -VMName <VM name>` を実行します。
4. カスタムプロパティ文字列を変更します。
   a. カスタムプロパティをメモ帳にコピーし、カスタムプロパティを変更します。
   b. **PowerShell** ウィンドウで、メモ帳から変更したカスタムプロパティを貼り付け、変更したカスタムプロパティに変数名を割り当てます。例:

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com/2014/xd/
machinecreation xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="CatalogZones" Value="" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" /
>

<Property xsi:type="StringProperty" Name="PersistOSDisk"
Value="true" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="pd-standard" />

<Property xsi:type="StringProperty" Name="StorageType" Value="pd-
standard" />

</CustomProperties>'
```

5. 既存のカタログを更新します。例:

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName>
-CustomProperties $cp
```

6. 既存の VM を更新します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

7. VMを再起動します。次回の電源投入時に、カスタムプロパティの変更が既存のVMに適用されます。

誤ったマシン削除からの保護

Citrix DaaS を使用すると、Google Cloud 上の MCS リソースを保護して、誤って削除されるのを防ぐことができます。プロビジョニングされた VM を構成するには、`deletionProtection` フラグを TRUE に設定します。

デフォルトでは、MCS または Google Cloud プラグインを介してプロビジョニングされた VM は、InstanceProtection が有効な状態で作成されます。この実装は、永続カタログと非永続カタログの両方に適用されます。非永続カタログは、インスタンスがテンプレートから再作成されるときに更新されます。既存の永続マシンについては、Google Cloud コンソールでフラグを設定できます。フラグの設定の詳細については、Google ドキュメントサイト を参照してください。永続カタログに追加される新しいマシンは、`deletionProtection` が有効な状態で作成されます。

`deletionProtection` フラグを設定した VM インスタンスを削除しようとすると、リクエストは失敗します。ただし、`compute.instances.setDeletionProtection` 権限が付与されているか、IAM の **Compute Admin** ロールが割り当てられている場合は、フラグをリセットしてリソースを削除できるようにすることができます。

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
IDディスク	"CitrixResource": "内部"
	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
イメージ	"CitrixResource": "内部"
	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OSディスク	"CitrixResource": "内部"

リソース名	タグ
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
PrepVM	"CitrixResource": "内部"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
公開スナップショット	"CitrixResource": "内部"
ストレージバケット	"Citrixresource": "インターナル"
テンプレート	"CitrixResource": "内部"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
カタログ内のVM	"CitrixResource": "内部"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"。プラグインは、MCSでプロビジョニングされたVMにこのラベルも追加します: "citrix-provisioning-scheme-id": "provSchemeId"。このラベルを使用して、GCPコンソールでカタログによってフィルタリングできます。
WBCディスク	"CitrixResource": "内部"
	シトリックスプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

注:

MCSによって作成されたリソースとして識別するために**CitrixResource**タグが追加されている場合、VMはCitrixインベントリに表示されません。タグを削除または名前変更することで、表示させることができます。

詳細情報

- 接続とリソースの作成および管理
- Google Cloud環境への接続
- マシンカタログの作成
- Google Cloud Platform カタログを作成する
- マシンカタログの管理

HPE Moonshot カタログの管理

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明しています。以下の情報は、HPE Moonshot カタログに固有の詳細を扱っています。

> **注:**
>
> HPE Moonshotカタログを管理する前に、HPE Moonshotカタログの作成を完了する必要があります。

電源管理

Citrix Virtual Apps and Desktops™では、HPE Moonshotマシンの電源管理を行うことができます。電源管理を行うマシンを見つけるには、ナビゲーションペインの**検索**ノードを使用します。以下の電源操作が利用可能です。

- 起動
- シャットダウン
- 強制シャットダウン
- 再起動
- リセット

> **注:**
>
> **一時停止**および**再開**の電源操作はサポートされていません。

詳細情報

- 接続とリソースの作成と管理
- HPE Moonshotへの接続(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/connections/connection-hpe-moonshot.html)
- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create.html)
- HPE Moonshotマシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create/create-machine-catalog-hpe-moonshot.html)
- マシンカタログの管理(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-manage.html)

Microsoft Azureカタログを管理する

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Microsoft Azure Resource Managerクラウド環境に固有の詳細を扱います。

> **注:**
>
> Microsoft Azureカタログを管理する前に、Microsoft Azureカタログの作成を完了する必要があります。Microsoft Azureカタログの作成を参照してください。

VMシャットダウン時にストレージタイプを下位層に変更する

VMをシャットダウンするときに、管理ディスクのストレージタイプを下位層に切り替えることで、ストレージコストを節約できます。これを行うには、`StorageTypeAtShutdown`カスタムプロパティを使用します。

VMをシャットダウンすると、ディスクのストレージタイプは下位層（`StorageTypeAtShutdown`カスタムプロパティで指定）に変更されます。VMの電源をオンにすると、ストレージタイプは元の状態（`StorageType`カスタムプロパティまたは`WBCDiskStorageType`カスタムプロパティで指定）に戻ります。

> **重要:**
>
> ディスクはVMが少なくとも一度電源オンになるまで存在しません。したがって、VMを最初に電源オンにしたときにストレージタイプを変更することはできません。

要件

- 管理ディスクに適用されます。これは、カスタムプロパティ`UseManagedDisks`をtrueに設定することを意味します。
- 永続OSディスクを持つ永続および非永続カタログに適用されます。これは、カスタムプロパティ`persistOsDisk`をtrueに設定することを意味します。
- 永続WBCディスクを持つ非永続カタログに適用されます。これは、カスタムプロパティ`persistWBC`をtrueに設定することを意味します。

制限

- Microsoftによると、ディスクタイプは1日2回までしか変更できません。Microsoftドキュメントを参照してください。Citrixによると、VMの開始または割り当て解除アクションがあるたびに`StorageType`の更新が行われます。したがって、VMあたりの電源アクションの数を1日2回に制限してください。たとえば、朝にVMを開始するための電源アクションを1回、夕方にVMを割り当て解除するための電源アクションを1回とします。

ストレージの種類を下位層に変更する

手順を進める前に、要件と制限を参照してください。

1. カスタムプロパティ`StorageTypeAtShutdown`を追加し、値をStandard_LRS (HDD)に設定して、`New-ProvScheme`を使用してカタログを作成します。PowerShellを使用してカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

   > **注:**
   >
   > `StorageTypeAtShutdown`が空またはStandard_LRS (HDD)以外の値を持つ場合、操作は失敗します。

   永続カタログの作成中にカスタムプロパティを設定する例：

   ```
   $customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
   2014/xd/machinecreation"

   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

   <Property xsi:type="StringProperty" Name="UseManagedDisks"
   Value="true" />
   ```

```
<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

非永続カタログの作成中にカスタムプロパティを設定する例：

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
```

```
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

> **注:**
>
> マシンプロファイルを使用する場合、カスタムプロパティは`MachineProfile`で定義されたプロパティよりも優先されます。

2. VMをシャットダウンし、AzureポータルでVMのストレージタイプを確認します。ディスクのストレージタイプは、`StorageTypeAtShutdown`カスタムプロパティで指定されたように、下位の層に変更されます。
3. VMをオンにします。ディスクのストレージの種類は、以下に記載されているストレージの種類に戻ります。
   - OSディスクの`StorageType`カスタムプロパティ
   - WBCディスクの`WBCDiskStorageType`カスタムプロパティ（`CustomProperties`で指定した場合のみ）。それ以外の場合は、`StorageType`に記載されているストレージの種類に戻ります。

既存のカタログに`StorageTypeAtShutdown`を適用する

手順を進める前に、要件と制限を参照してください。

既存のカタログにVMを追加するには、`Set-ProvScheme`を使用します。この機能は、`Set-ProvScheme`の実行後に追加された新しいVMに適用されます。既存のマシンには影響しません。

既存のカタログにVMを追加する際にカスタムプロパティを設定する例：

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'



$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName



Set-ProvScheme -ProvisioningSchemeName $ProvScheme.ProvisioningSchemeName
-CustomProperties $customProperties
```

既存のVMのストレージタイプをシャットダウン時に下位層に変更する

手順を進める前に、要件と制限を参照してください。

VMがシャットダウンされているときに、既存のVMのストレージタイプを下位の層に変更することで、ストレージコストを節約できます。これを行うには、`StorageTypeAtShutdown`カスタムプロパティを使用します。

VMのシャットダウン時に、カタログ内の既存マシンのストレージタイプを下位層に変更するには：

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために、`asnp citrix®*`を実行します。
3. `Get-Provscheme -ProvisioningSchemeName $CatalogName`を実行します。
4. カスタムプロパティ文字列を変更します。

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

5. 既存のカタログのプロビジョニングスキームを更新します。この更新は、`Set-ProvScheme`の実行後に追加された新しいVMに適用されます。

```
Set-ProvScheme -ProvisioningSchemeName $CatalogName -CustomProperties
$customProperties
```

6. 既存のVMを更新して、`StorageTypeAtShutdown`を有効にします。

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName $CatalogName
-StartsNow -DurationInMinutes -1
```

7. 次回マシンを起動すると、マシンの`StorageTypeAtShutdown`プロパティが更新されます。ストレージタイプは次回のシャットダウン時に変更されます。
8. カタログ内の各VMの`StorageTypeAtShutdown`値を表示するには、次のコマンドを実行します。

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach { $vmName =
$_.VMName; $storageTypeAtShutdown = ($_.CustomVmData | ConvertFrom-
Json).StorageTypeAtShutdown.DiskStorageAccountType; return New-Object
```

```
psobject -Property @{ "VMName" = $vmName; "StorageTypeAtShutdown" =
$storageTypeAtShutdown } }
```

プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する

`Set-ProvScheme`コマンドはプロビジョニングスキームを変更します。ただし、既存のマシンには影響しません。PowerShellコマンド`Set-ProvVMUpdateTimeWindow`を使用すると、現在のプロビジョニングスキームを既存の永続マシンまたは非永続マシン、あるいはマシンセットに適用できます。また、既存のMCSプロビジョニング済みマシンの構成更新のタイムスロットをスケジュールすることもできます。スケジュールされたタイムスロット中の電源オンまたは再起動により、スケジュールされたプロビジョニングスキームの更新がマシンに適用されます。現在、Azureでは、`ServiceOffering`、`MachineProfile`、および以下のカスタムプロパティを更新できます。

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

注:

- Azure環境でマネージドディスクを使用するカタログの場合、`StorageType`、`WBCDiskStorageType`、および`IdentityDiskStorageType`のカスタムプロパティのみを更新できます。
- `Set-ProvVMUpdateTimeWindow`を2回実行した場合、最新のコマンドが有効になります。

更新できるもの:

- 単一のVM

- 特定のVMのリスト、またはプロビジョニングスキームIDに関連付けられているすべての既存のVM
- プロビジョニングスキーム名 (マシンカタログ名) に関連付けられている特定のVMまたはすべての既存VMのリスト

プロビジョニングスキームに以下の変更を加えると、Azureの永続カタログの場合、VMインスタンスが再作成されます:

- `MachineProfile`を変更する
- 削除 `LicenseType`
- 削除 `DedicatedHostGroupId`

> **注:**
>
> 既存のマシンのOSディスクとそのすべてのデータはそのまま残り、新しいVMがディスクに接続されます。

既存のVMを更新する前に:

1. 既存のマシンの構成を確認します。例えば、,

   ```
   Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
   ```

2. プロビジョニングスキームを更新します。例えば、,

   - マシンプロファイルの入力としてVMを使用する場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-catalog" -MachineProfile
     "XDHyp:\HostingUnits\<hosting-unit>\machineprofile.folder\<resource-
     group>.resourcegroup\<virtual-machine>.vm"
     ```

   - マシンプロファイルの入力としてテンプレート仕様を使用する場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-catalog"

     -MachineProfile "XDHyp:\HostingUnits\<hosting-
     unit>\machineprofile.folder\<resource-
     ```

```
group>.resourcegroup\<template-spec>.templatespec\<template-spec-
version>.templatespecversion"

-ServiceOffering "XDHyp:\HostingUnits\<hosting-
unit>\serviceoffering.folder\<service-offering>.serviceoffering"
```

- サービスオファリングのみを使用する場合:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -ServiceOffering
"XDHyp:\HostingUnits\<hosting-unit>\serviceoffering.folder\<service-
offering>.serviceoffering"
```

3. VMの現在のプロパティが現在のプロビジョニングスキームと一致しているか、およびVMに保留中の更新アクションがあるかを確認します。例えば、,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

特定のバージョンを持つマシンを見つけることもできます。たとえば、,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
ProvisioningSchemeVersion
```

既存のマシンに次回の再起動時に適用される更新を要求するには：

1. 既存のマシンを更新し、次回の再起動時に更新が適用されるようにするには、次のコマンドを実行します。

   - 既存のすべてのマシンを更新する場合。例：

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
   -StartsNow -DurationInMinutes -1
   ```

   - 特定のマシンのリストを更新する場合。例：

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
   -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
   ```

   - Get-ProvVM の出力に基づいてマシンを更新する場合。例：

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
-DurationInMinutes -1
```

注：

- `StartsNow` は、スケジュールされた開始時刻が現在の時刻であることを示します。
- `DurationInMinutes` に負の数（例：–1）を指定すると、スケジュールの時間枠に上限がないことを示します。

2. 更新がスケジュールされているマシンを見つけます。例：

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

3. マシンを再起動します。次回の電源投入時に、プロパティの変更が既存のマシンに適用されます。更新されたステータスは、次のコマンドを使用して確認できます。例：

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

スケジュールされた時間枠内で次回起動時に最新のプロビジョニング設定に更新されるようにVMをスケジュールするには：

1. 次のコマンドを実行します。

- 開始時刻を現在時刻として更新をスケジュールするには

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName vm1 -StartsNow -DurationInMinutes 120
```

- 週末に更新をスケジュールするには

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
-VMName “vm1” -StartTimeInUTC “10/15/2022 9:00am” -DurationInMinutes
(New –TimeSpan –Days 2).TotalMinutes
```

> **注：**
>
> - `VMName` はオプションです。指定しない場合、更新はカタログ全体に対してスケジュールされます。
> - `StartTimeInUTC` の代わりに、`StartsNow` を使用して、スケジュール開始時刻が現在時刻であることを示します。
> - `DurationInMinutes` はオプションです。デフォルトは120分です。負の数（例: –1）は、スケジュールの時間枠に上限がないことを示します。

2. 更新ステータスを確認します。

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
```

3. VM の電源を入れます。スケジュールされた時間枠の後にマシンの電源を入れた場合、構成の更新は適用されません。スケジュールされた時間枠内にマシンの電源を入れた場合、,
   - マシンがオフになっていて、
     - マシンの電源を入れない場合、構成の更新は適用されません
     - マシンの電源を入れる場合、構成の更新が適用されます
   - マシンが電源オンの場合、かつ
     - マシンを再起動しない場合、構成の更新は適用されません
     - マシンを再起動する場合、構成の更新が適用されます

構成の更新をキャンセルするには:

単一のVM、複数のVM、またはカタログ全体の構成更新をキャンセルすることもできます。構成更新をキャンセルするには:

1. `Clear-ProvVMUpdateTimeWindow` を実行します。例:
   - 単一のVMに対してスケジュールされた構成更新をキャンセルするには:

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
-VMName “vm1”
```

- 複数のVMに対してスケジュールされた構成の更新をキャンセルするには：

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog"
-VMName "vm1","vm2"
```

> **注：**
>
> VM は同じカタログのものである必要があります。

個々のVMのプロパティを更新する

永続的なMCSマシンカタログ内の個々のVMのプロパティは、PowerShellコマンド`Set-ProvVM`を使用して更新できます。ただし、更新はすぐに適用されません。更新を適用するには、PowerShellコマンド`Set-ProvVMUpdateTimeWindow`を使用して時間枠を設定する必要があります。

この実装により、マシンカタログ全体を更新することなく、個々のVMを効率的に管理できます。現在、この機能はAzure環境にのみ適用されます。

現在、更新できるプロパティは次のとおりです。

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

この機能を使用すると、次のことができます。

- VMのプロパティを更新する
- マシンカタログの更新後もVMで更新されたプロパティを保持する
- VMに適用された構成の更新を元に戻す

VMのプロパティを更新する前に：

1. 「**PowerShell**」ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. 既存のマシンカタログの構成を確認します。例：

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

4. 更新を適用するVMの構成を確認します。例：

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

VMのプロパティを更新する

VMのプロパティを更新するには、次の手順を実行します。

1. 更新を適用するVMの電源を切ります。
2. VMのプロパティを更新します。たとえば、VMのストレージタイプ (`StorageType`) カスタムプロパティを更新する場合は、次を実行します。

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

マシンカタログ内の2つのVMのプロパティを同時に更新できます。例：

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2
-CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

> **注：**
>
> 更新はすぐに適用されません。

3. 更新が指定されているプロパティのリストと構成バージョンを取得します。例：

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -VMName
machine1
```

`Version`のプロパティ値と、更新するプロパティ（この場合は`StorageType`）を確認します。

4. 構成バージョンを確認します。例：

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion`のプロパティ値を確認します。更新はまだ適用されていません。VMはまだ古い構成のままです。

5. スケジュールされた更新を要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog
-StartsNow -DurationInMinutes -1
```

スケジュールされた更新の詳細については、プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する を参照してください。

> **注:**
>
> 保留中のプロビジョニングスキームの更新も適用されます。

6. VMを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

7. 構成バージョンを確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion` のプロパティ値を確認します。更新が適用されました。VMは新しい構成になりました。

8. VMにさらに構成アップデートを適用するには、VMをオフにして、手順を繰り返します。

マシンカタログの更新後にVMで更新されたプロパティを保持する

VMで更新されたプロパティを保持するには、以下を実行します。

1. 更新を適用するVMをシャットダウンします。

2. マシンカタログを更新します。たとえば、VMサイズ (`ServiceOffering`) とストレージタイプ (`StorageType`) を変更したい場合は、次を実行します。

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -ServiceOffering
Standard_E4_v3 -CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

3. マシンカタログの構成詳細を取得します。例:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

`ProvisioningSchemeVersion` が1つ増えました。VMサイズとストレージタイプも更新されています。

4. VMのプロパティを更新します。たとえば、VMにマシンプロファイルを提供します。

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-MachineProfile "XDHyp:\HostingUnits\<hosting-
unit>\machineprofile.folder\<resource-group>.resourcegroup\<template-
spec>.templatespec\<template-spec-version>.templatespecversion"
```

> **注:**
>
> マシンプロファイルの入力には、タグと異なるVMサイズ (`ServiceOffering`) が指定されています。

5. VM上の構成更新とマシンカタログの更新をマージした後にVMが持つことになるプロパティのリストを取得します。例：

```
Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName
AzureCatalog -VMName machine1
```

> **注:**
>
> VMに対するすべてのアップデートは、マシンカタログで行われたアップデートを上書きします。

6. VMに対してスケジュールされた更新を要求します。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -VMName
machine1 -StartsNow -DurationInMinutes -1
```

7. VMを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

   VMは、マシンプロファイルから派生した更新済みのVMサイズを保持します。マシンプロファイルで指定されたタグ値もVMに適用されます。ただし、ストレージタイプは最新のプロビジョニングスキームから派生します。

8. VMの構成バージョンを取得します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

   `ProvisioningSchemeVersion` と `ProvVMConfigurationVersion` は最新バージョンを表示します。

VMに適用された構成の更新を元に戻す

1. VMに更新を適用した後、VMをシャットダウンします。
2. 次のコマンドを実行して、VMに適用された更新を削除します。例:

```
Set-ProvVM -RevertToProvSchemeConfiguration -ProvisioningSchemeName
AzureCatalog -VMName machine1
```

3. VMに対してスケジュールされた更新を要求します。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -VMName
machine1 -StartsNow -DurationInMinutes -1
```

4. VMを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

5. VMの構成バージョンを確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion` の値が、マシンカタログの構成バージョンになります。

ディスク暗号化の変更

Azure仮想化環境でディスク暗号化を変更し、次の操作を実行できます。

- `New-ProvScheme` コマンドを使用して、マスターイメージのDESとは異なるディスク暗号化セット（DES）を持つMCSマシンカタログを作成します。例:

```
$customProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="DiskEncryptionSetId" Name="Zones" Value="/
subscriptions/XXXXXXXXXXXXXXXXXXXXXXXXXXXX/resourceGroups/testrsg/
providers/Microsoft.Compute/diskEncryptionSets/test-diskEncryptionSet"/
>

</CustomProperties>

"@

New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName $provisioningSchemeName `

-HostingUnitName $hostingUnitName `

-IdentityPoolName $identityPoolName `

-InitialBatchSizeHint $numberOfVms `

-masterImagePath $masterImagePath `

-NetworkMapping $networkMapping `

-CustomProperties $customProperties
```

- `Set-ProvScheme` および `Set-ProvVMUpdateTimeWindow` コマンドを使用して、既存のMCSマシンカタログと既存のVMのディスク暗号化タイプを、あるDESキーから別のDESキーに変更します。VMを再起動すると、更新されたDESキーが表示されます。例:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties

Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- 以前CMEKが有効になっていなかったMCSマシンカタログとVMを、`Set-ProvScheme` および `Set-ProvVMUpdateTimeWindow` コマンドを使用して、顧客管理の暗号化キー（CMEK）暗号化（DES）、ホストでのディスク暗号化、または二重暗号化を持つように更新します。さまざまな暗号化タイプの詳細については、Azureサーバー側暗号化、ホストでのAzureディスク暗号化、およびマネージドディスクの二重暗号化を参照してください。
- `Set-ProvScheme` および `Set-ProvVMUpdateTimeWindow` コマンドを使用して、以前暗号化されていた既存のMCSマシンカタログとVMを非暗号化に更新します。例:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- プライベートエンドポイントでディスク暗号化を有効にします（`ProxyHypervisorTrafficThroughConnector` で有効化されたホスト接続を使用したMCSマシンカタログ）。プライベートエンドポイントでディスク暗号化を有効にする方法については、プライベートエンドポイントでディスク暗号化を有効にするを参照してください。

プライベートエンドポイントでディスク暗号化を有効にする

Azureの制限により、現在、プライベートエンドポイントに対して顧客管理キーによるサーバー側暗号化を使用することはできません。ただし、既存のMCSマシンカタログとプライベートエンドポイントを持つVMをDESキーで暗号化するように更新することは可能です。

プライベートエンドポイントを持つ既存のマシンカタログを更新する

プライベートエンドポイントを持つ既存のマシンカタログを更新する詳細な手順は次のとおりです。

1. `ProxyHypervisorTrafficThroughConnector` を介してディスク暗号化なしでカタログを作成します。
2. `DiskEncryptionSetId` を使用してカタログを更新するには、`Set-ProvScheme` を実行します。

> **注：**
>
> `DiskEcryptionSetId` は、`CustomProperties` または `MachineProfile` を介して構成できます。`CustomProperties` と `MachineProfile` の両方で定義されている場合、`CustomProperties` で定義されているプロパティが適用されます。

`CustomProperties` を使用する場合の例:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1"/>
```

```
</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

MachineProfile を使用する場合の例: ディスク暗号化が有効な VM、またはディスク暗号化設定を含むテンプレート仕様を使用します:

```
Set-ProvScheme -ProvisioningSchemeName azure-catalog -MachineProfile
"XDHyp:
\HostingUnits\azureunit\machineprofile.folder\testrg.resourcegroup\new-
template.vm"
```

または、Web Studioを使用してマシンプロファイルを更新することもできます。

3. 既存のカタログ VM を更新するには、`Set-ProvVMUpdateTimeWindow` を実行します。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

4. VM を再起動すると、Azure portal の VM ディスクで更新されたディスク暗号化を確認できます。
5. 新しいカタログ VM を追加する前にディスク暗号化を解除するには、`Set-ProvScheme` を実行します。

注：

プライベートエンドポイントカタログを更新しているため、この手順が必要です。この手順を実行しないと、カタログに新しい VM を追加しようとしたときにエラーが発生します。

例:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
```

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

6. カタログに新しい VM を追加します。

個々のカタログ VM を更新する

個々のカタログ VM を更新する詳細な手順は次のとおりです。

1. `ProxyHypervisorTrafficThroughConnector` を介してディスク暗号化なしでカタログを作成します。
2. `Set-ProvVM` を実行して、カタログVMを `DiskEncryptionSetId` で更新します。

> **注:**
>
> The `DiskEcryptionSetId` は、`CustomProperties` または `MachineProfile` のいずれかを使用して構成できます。

`CustomProperties` を使用する場合の例:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />

</CustomProperties>'

Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01
-CustomProperties $customProperties
```

MachineProfile を使用する場合の例:

```
Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01
-MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\testrg.resourcegroup\new-
template.vm"
```

3. `Set-ProvVMUpdateTimeWindow` を実行して、既存のカタログVMを更新します。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01 -StartsNow -DurationInMinutes -1
```

4. VMを再起動すると、AzureポータルでVMディスク上の更新されたディスク暗号化を確認できます。
5. 新しいVMをカタログに追加します。

既存のカタログのWBCディスクとして一時ディスクを使用する

既存のMCSマシンカタログのライトバックキャッシュディスク（WBC）ディスクとしてAzure一時ディスクを使用できます。`Set-ProvScheme` PowerShellコマンドを使用して、既存のカタログとVMを更新します。

前提条件

既存のカタログは、次の条件を満たしている必要があります。

> **注:**
>
> 既存のカタログが以下の要件を満たしていない場合、WBCディスクは一時ディスク内に配置されません。

- MCSIOが有効になっている: カスタムプロパティ `WriteBackCacheMemorySize`、`WriteBackCacheDiskSize`、および `UseWriteBackCache` が有効になっています。
- エフェメラルOSディスクが有効になっていない。
- WBCは非永続的である: `PersistWBC` は `false` です。
- `UseTempDiskForWBC` が null または false です。
- 一時ディスクのサイズは、（ライトバックキャッシュディスクサイズ + ページングファイル用の予約済み領域 + 1 GB のバッファースペース）の合計サイズよりも大きくする必要があります。

> **重要:**
>
> 一時ディスクがあるサービスオファリングから一時ディスクがないサービスオファリングへの変更、またはその逆の変更は許可されていません。

既存のカタログを更新する

既存のカタログを更新するには、次のコマンドを実行します。

1. 既存のカタログで `Set-ProvScheme` を実行して、`UseTempDiskForWBC` を `true` に更新します。例:

```
Set-ProvScheme -ProvisioningSchemeName name -CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Standard_LRS`"/><Property
xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"True`"/
><Property xsi:type=`"StringProperty`" Name=`"ManagedDisksPreview`"
Value=`"False`"/><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"False`"/><Property
xsi:type=`"StringProperty`" Name=`"UseTempDiskForWBC`" Value=`"True`"/
><Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
Value=`"False`"/></CustomProperties>"
```

2. カタログに新しいマシンを追加して電源を入れます。新しい VM には、一時ディスク内に WBC ディスクがあります。

Azure VM、スナップショット、OS ディスク、およびギャラリーイメージ定義の情報を取得する

Azure VMに関する情報（OSディスクと種類、スナップショット、ギャラリーイメージ定義など）を表示できます。この情報は、マシンカタログが割り当てられている場合、マスターイメージ上のリソースに対して表示されます。この機能を使用して、LinuxまたはWindowsイメージを表示および選択します。PowerShellプロパティ`TemplateIsWindowsTemplate`が`AdditionDatafield`パラメーターに追加されました。このフィールドには、Azure固有の情報（VMの種類、OSディスク、ギャラリーイメージ情報、OSの種類情報）が含まれています。
`TemplateIsWindowsTemplate`を**True**に設定するとOSの種類がWindowsであることを示し、`TemplateIsWindowsTemplate`を**False**に設定するとOSの種類がLinuxであることを示します。

> **ヒント:**
>
> `TemplateIsWindowsTemplate` PowerShell プロパティによって表示される情報は、Azure API から派生しています。このフィールドが空の場合があります。たとえば、データディスクからのスナップショットには `TemplateIsWindowsTemplate` フィールドが含まれていません。これは、OS の種類をスナップショットから取得できないためです。

> たとえば、PowerShell を使用して、Windows OS の種類に対して Azure VM `AdditionData` パラメーターを **True** に設定します。

```
PS C:\Users\username> (get-item XDHyp:
\HostingUnits\mynetwork\image.folder\username-dev-testing-
rg.resourcegroup\username-dev-tsvda.vm).AdditionalData

Key Value

ServiceOfferingDescription Standard_B2ms

HardDiskSizeGB 127

ResourceGroupName FENGHUAJ-DEV-TESTING-RG

ServiceOfferingMemory 8192

ServiceOfferingCores 2

TemplateIsWindowsTemplate True

ServiceOfferingWithTemporaryDiskSizeInMb 16384

SupportedMachineGenerations Gen1,Gen2
```

MCS カタログのクローンを作成する

既存の永続的および非永続的MCSカタログを複数のカタログに分割します。元のプロビジョニングスキームのクローンを作成することで、VMの特定のサブセットに異なるカタログレベルのポリシーと構成を適用できます。この機能は、組織内の異なる機能的役割（財務や役員など）が、標準ユーザーと比較して異なるリソース構成（バックアップ制限など）を必要とする場合に特に役立ちます。

使用例

管理者は大規模なVMカタログを管理しています。役員チームは、標準ポリシーで許可されているよりも多くのバックアップを必要とします。管理者は`Copy-ProvScheme`コマンドを使用して、既存のカタログプロビジョニングスキームを新しいカタログにクローンします。これにより、管理者は新しい役員カタログに専用のバックアップポリシーを適用しつつ、組織の他の部分の元の設定を維持できます。

適用範囲

- Azure 環境
- 永続的および非永続的 MCS カタログ
- MCS プロビジョニングされた Citrix Provisioning カタログ

制限事項

- **プロビジョニングスキーム:** プロビジョニングスキームの最新バージョンのみがコピーされます。
- **バックアップスケジュール**: バックアップスケジュールは新しいカタログにコピーされません。新しいカタログには独自のバックアップスケジュールを設定する必要があります。
- **IDプール**: ID関連オブジェクトはクローンされず、同じ`ADAccountIdentityPool`を使用して共有されたままになります。
- **デリバリーグループ**: クローン作成プロセス中に、デリバリーグループの操作とユーザー割り当ては変更または関連付けられません。

重要な考慮事項

- **リソースグループ (ターゲットの場所)**:
  - `TargetLocation` (Azure リソースグループ) を指定しない場合:
    - Citrix 管理のリソースグループの場合、新しい Citrix 管理のリソースグループが作成されます。
    - BYO (Bring Your Own) リソースグループの場合、新しいプロビジョニングスキームのリソースは同じリソースグループに作成されます。
  - `TargetLocation` を提供する場合:
    - リソースは、指定されたリソースグループに作成されます。
    - 指定されたリソースグループは、Azureにすでに存在している必要があります。

- **ベースディスクスナップショット**: リソースグループの構成に関係なく、ベースディスクスナップショットのコピーは常に作成されます。

前提条件

- 既存のプロビジョニングスキーム (ソースカタログ) が利用可能である必要があります。
- ターゲットの場所を指定する場合、ターゲットの Azure リソースグループが存在している必要があります。

PowerShellを使用した構成

1. PowerShellウィンドウを開きます。
2. 必要なパラメーター: `SourceProvisioningSchemeName` (または `SourceProvisioningSchemeUid`) と `TargetProvisioningSchemeName` を使用して、`Copy-ProvScheme` コマンドを実行します。

   例1: プロビジョニングスキームを名前でコピーする。

   この例では、「Backup」という名前のスキームを「TestCopy」という名前の新しいスキームにコピーします。

   ```
   Copy-ProvScheme -SourceProvisioningSchemeName Backup
   -TargetProvisioningSchemeName TestCopy
   ```

   例2：Uidでプロビジョニングスキームを特定のリソースグループにコピーする

   この例では、Uid を使用してスキームをコピーし、「TestRg」という名前のターゲットリソースグループを指定します。

   ```
   Copy-ProvScheme -SourceProvisioningSchemeUid 771e205d-1ee5-4ad2-b044-
   ecf3d7f24ec7 -TargetProvisioningSchemeName TestCopy -TargetLocation
   TestRg
   ```

MCS によって作成されたリソースを識別する

以下は、MCSがリソースに追加するタグです。表のタグは「key」:「value」として表されます。

リソース名	タグ
ID ディスク	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

リソース名	タグ
	"CitrixResource" : "内部"
イメージ	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
NIC	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
OSディスク	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
PrepVM	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
公開スナップショット	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
リソースグループ	"CitrixResource" : "内部"
	CitrixSchemaVersion: 2.0
	"シトリックスプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
ストレージアカウント	"シトリックスプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
カタログ内のVM	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

リソース名	タグ
	"CitrixResource" : "内部"
WBCディスク	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"

注:

CitrixResourceタグがMCSによって作成されたリソースとして識別するために追加されている場合、VMはCitrixインベントリに表示されません。タグを削除または名前変更して、表示させることができます。

タグの削除

カタログまたはVMを作成すると、以下のリソースにタグが作成されます。

- リソースグループ
- 仮想マシン
- OSディスク
- 識別ディスク
- ネットワークインターフェイス
- ストレージアカウント

CitrixデータベースからVMとマシンカタログを削除し、タグを削除できます。以下を使用できます。

- マシンカタログから単一のVMまたはVMのリストからVMとタグを削除するには、`ForgetVM`パラメーターを指定した`Remove-ProvVM`を使用します。
- Citrixデータベースからマシンカタログを削除し、マシンカタログ全体からタグを削除するには、`ForgetVM`パラメーターを指定した`Remove-ProvScheme`を使用します。

この機能は、永続VMにのみ適用されます。

これを行うには：

1. **PowerShell**ウィンドウを開きます。

2. Citrix固有のPowerShellモジュールをロードするには、**asnp citrix***を実行します。
3. CitrixデータベースからVMを削除し、VMからタグを削除するには、`Remove-ProvVM`を実行します。 例：

```
Remove-ProvVM -ProvisioningSchemeName “ProvisioningSchemeName” -VMName
“vmname” -ForgetVM
```

4. Citrixデータベースからマシンカタログを削除し、マシンカタログからタグを削除するには、`Remove-ProvScheme`を実行します。例：

```
Remove-ProvScheme -ProvisioningSchemeName “ProvisioningSchemeName”
-ForgetVM
```

> **注:**
>
> `Remove-ProvScheme`で`ForgetVM`パラメーターを使用すると、プロビジョニングスキームがBYORG（Bring Your Own Resource Group）またはCitrix管理リソースグループのいずれかに存在する場合、MCSはベースディスクスナップショットを含むすべてのスナップショットを削除します。

詳細情報

- 接続とリソースの作成および管理
- Microsoft Azureへの接続
- マシンカタログの作成
- Microsoft Azureカタログの作成
- マシンカタログの管理

マイクロソフト システムセンター バーチャルマシンマネージャー カタログの管理

マシンカタログの管理ウィザードについて説明します。(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-manage.html)以下の情報は、Microsoft System Center Virtual Machine Manager (VMM) 仮想化環境に固有の詳細を扱います。

> **注:**

> VMMカタログを管理する前に、VMMカタログの作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create/create-machine-catalog-mscvmm.html)「Microsoft System Center Virtual Machine Manager カタログの作成」を参照してください。

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
準備VM	タグ文字列は次のとおりです: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	カスタムプロパティエントリ: "XdConfig:"XdProvisioned=True"
カタログ内のVM	タグ文字列は次のとおりです: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	カスタムプロパティエントリ: "XdConfig:"XdProvisioned=True"

詳細情報

- 接続とリソースを作成および管理する
- マイクロソフト システムセンター バーチャルマシンマネージャーへの接続
- マシンカタログを作成する
- Microsoft System Center Virtual Machine Managerカタログを作成する
- マシンカタログを管理する

Nutanixカタログの管理

(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-manage)では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Nutanix AHV Prism Central環境に固有の詳細を扱っています。

> **注:**
>
> Nutanix AHV Prism Centralでマシンカタログを管理する前に、Nutanix AHV Prism Centralでマシンカタログの作成を完了する必要があります。「Nutanixカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-create/create-machine-catalog-nutanix)を参照してください。

Nutanix AHV Prism Centralでマシンカタログを管理するには、次の方法を使用できます。

- ウェブスタジオ
- PowerShell

Web Studioの使用

Web Studio を使用して Nutanix AHV Prism Central 上でマシンカタログを管理するためのオプションは次のとおりです。

オプション	説明
マシンの追加	マシンカタログにVMを作成して追加します。
マシンカタログの削除	マシンカタログを削除します。同時にVMを削除するか、永続VMをそのまま残すかを選択できます。
マスターイメージを変更	カタログ内のすべてのVMのテンプレートとして使用されるマスターイメージを変更します。
マシンプロファイルを追加または変更	マシンプロファイルのテンプレートバージョンを変更するか、既存のカタログにマシンプロファイルを追加します。
構成セットを管理	カタログをWorkspace Environment Management™構成セットにバインドするか、別の構成に切り替えます。
マシンカタログを編集	NICや仮想マシンなど、カタログの構成を変更します。
マシンを表示	**検索**ノードに移動して、カタログに属するすべてのVMを表示します。

オプション	説明
マシンカタログの名前を変更	カタログ名を変更します。
VDAをアップグレード	カタログごとにVDAをアップグレードします。この機能は、静的永続マシンにのみ適用されます。
機能レベルを変更	カタログの最小機能レベルを選択します。機能レベルを設定すると、すべての機能が利用可能になります。
マシンカタログのテスト	カタログにエラーまたは警告があるかどうかをテストします。
タグの管理	タグを作成、編集、削除します。カタログに適用するタグを選択します。
マシンカタログの移動	カタログを別のフォルダーに移動します。

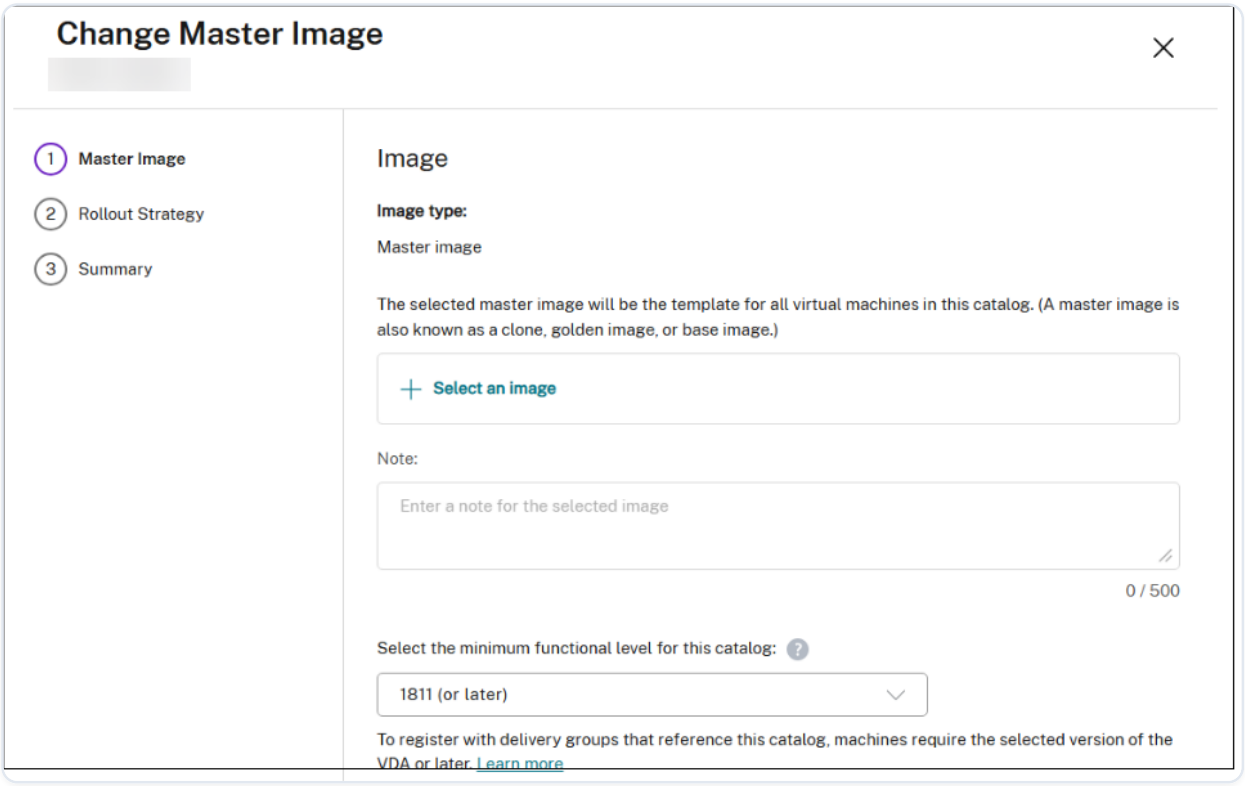
注:

現在、［**クローン**］ オプションは利用できません。

マスターイメージの変更

カタログのマスターイメージを変更するには、次の手順に従います。

1. ［**マシンカタログ**］ ページで、更新するマシンカタログを右クリックし、［**マスターイメージの変更**］ を選択します。
2. ［**マスターイメージの変更**］ ページで、［**イメージの選択**］ をクリックします。



3. **［イメージの選択］** ページで、テンプレートを展開し、マスターイメージとして使用するテンプレートバージョンを選択します。マシンテンプレートは名前でフィルタリングできます。
4. 「**ロールアウト戦略**」ページで、更新を適用するタイミングを選択します。

> **注：**
>
> Nutanix AHV Prism Centralホスト接続プラグインを使用するMCSプロビジョニングされた非永続カタログの場合、マスターイメージを更新してブート構成をレガシーとUEFIの間で切り替えると、既存のVMが次回の起動時に開始できなくなります。 マスターイメージを更新すると、OSディスクのみが更新されます。ハードウェアプロパティは変更されません。ハードウェアプロパティを更新するには、「マシンプロファイルの追加または変更」、「NICの変更」、および「VM構成の変更」を参照してください。

マシンプロファイルの追加または変更

カタログのマシンプロファイルを追加または変更するには、次の手順に従います。

1. 「**マシンカタログ**」ページで、変更するマシンカタログを右クリックし、「**マシンカタログの編集**」を選択します。
2. 「**マシンプロファイル**」ページで、,

- マシンカタログにすでにマシンプロファイルがある場合は、鉛筆アイコンをクリックして別のマシンプロファイルテンプレートバージョンを選択します。テンプレート名でフィルタリングできます。マシンプロファイルの設定を確認します。
- マシンカタログにマシンプロファイルがない場合は、「マシンプロファイルを使用」を選択し、マシンプロファイルを選択します。マシンプロファイルの設定を確認します。

3. 「**仮想マシン**」ページには、選択したマシンプロファイルテンプレートバージョンに従って更新された構成が反映されている必要があります。

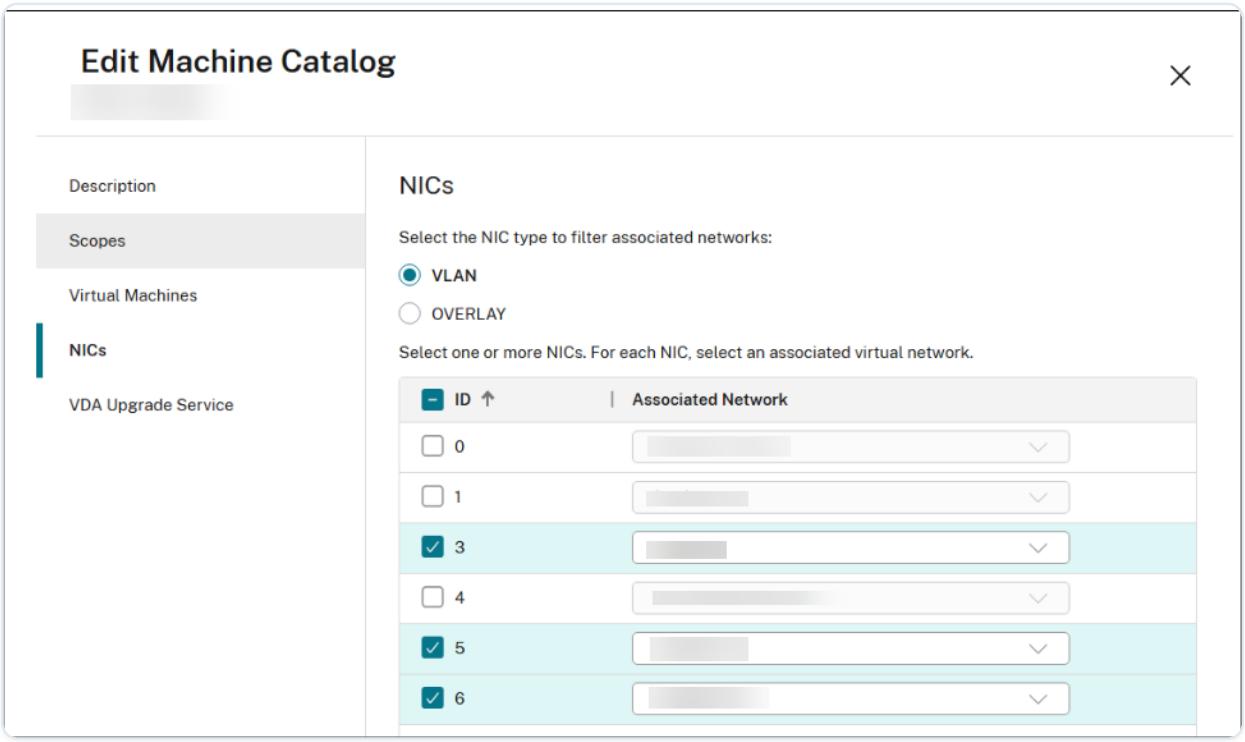
NICの変更

カタログのNICを変更するには、次の手順に従います。

1. 「**マシンカタログ**」ページで、変更するマシンカタログを右クリックし、「**マシンカタログの編集**」を選択します。
2. **NIC**ページで:

   a. NICの種類を選択します

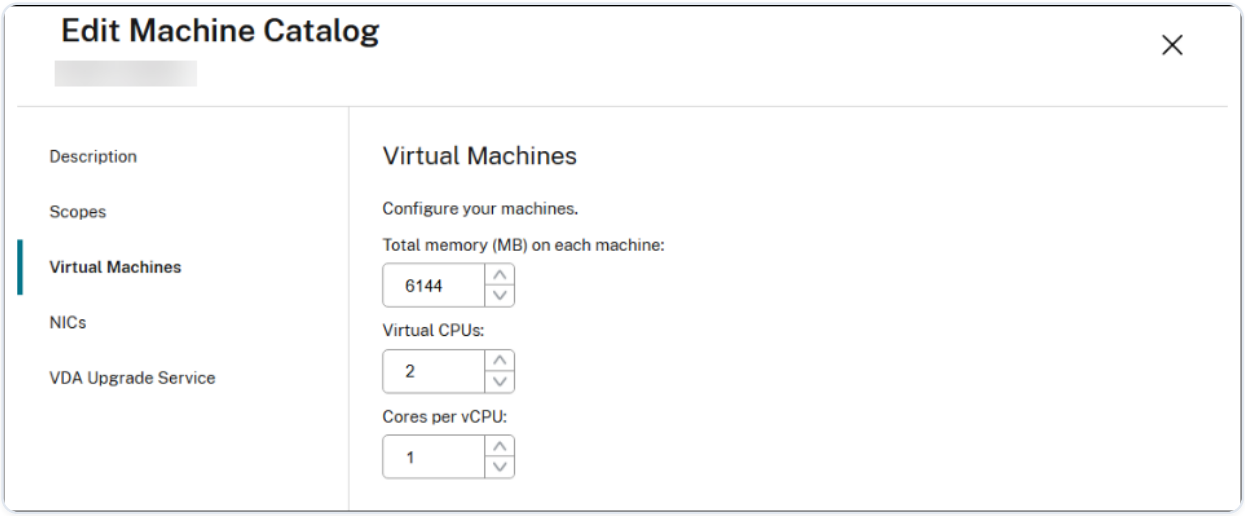
   b. ボックスをオンまたはオフにしてNICを選択し、各NICに関連付けられた仮想ネットワークを選択します。



VMの構成を変更する

メモリ、CPU数、vCPUあたりのコア数など、VMの構成を変更するには、次の手順に従います。

1. **マシンカタログ**ページで、変更するマシンカタログを右クリックし、**マシンカタログの編集**を選択します。
2. **仮想マシン**ページで、上下の矢印を使用するか、値を直接入力して、VMのメモリ、CPU数、vCPUあたりのコア数を調整します。



PowerShell を使用する

マスターイメージを変更する

必要なパラメーターは次のとおりです。

- `ProvisioningSchemeName`: 編集するプロビジョニングスキームの名前。
- `MasterImage`: 新しいマスターイメージへのリテラルパス。

次のコマンドを実行します。例:

```
Set-ProvSchemeMetadata  -Name "ImageManagementPrep_DoImagePreparation"
-ProvisioningSchemeName "<ProvisioningSchemeName>" -Value "True"



Publish-ProvMasterVMImage  -MasterImageVM "<Literal path to the new master
image- template version> -ProvisioningSchemeName
"<ProvisioningSchemeName>" -RunAsynchronously
```

> **注:**

> マスターイメージを更新すると、OSディスクのみが更新されます。ハードウェアプロパティは変更されません。ハードウェアプロパティを更新するには、マシンプロファイルの追加または変更、NICの変更、およびNICとVMの構成の変更を参照してください。

マシンプロファイルを追加または変更する

`Set-ProvScheme`コマンドを使用します。

- 新しいマシンプロファイルでカタログを更新する場合、または
- マシンプロファイルを持たない既存のカタログを、ハードウェア仕様のソースとしてマシンプロファイルの使用を開始するように更新する場合。

> **注：**
>
> これにより、カタログ内の既存のVMのハードウェア仕様は更新されません。カタログに追加された新しいVMのみが、指定されたマシンプロファイルからのハードウェア仕様を持ちます。

> マシンプロファイルを変更するか、既存のカタログをマシンプロファイルの使用を開始するように変換するには：

```
Set-ProvScheme -ProvisioningSchemeName <ProvScheme Name> `

               -MachineProfile "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<Template Name>.template\<Template Version
Name>.templateversion"
```

上書きされたハードウェア仕様でマシンプロファイルを変更するには：

特定の設定は、特定のコマンドラインパラメータを使用して構成できます。`CustomProperties`の`VMCpuCount`や`VMMemoryMB`、`CPUCores`などのこれらのコマンドラインパラメータは、マシンプロファイルテンプレートバージョンの値よりも優先されます。

```
$customProperties = @"

    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

        <StringProperty Name="ClusterId"
```

```
Value="00062c63-1fb0-58c9-4fc8-5c2573352378" />

        <StringProperty Name="CPUCores" Value="2" />

    </CustomProperties>

"@



Set-ProvScheme -ProvisioningSchemeName <ProvScheme Name> `

               -MachineProfile "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<Template Name>.template\<Template Version
Name>.templateversion" `

               -CustomProperties $customProperties `

               -VMCpuCount 4 `

               -VMMemoryMB 4096
```

NICとVMの構成を変更する

必須パラメータは次のとおりです。

- `ProvisioningSchemeName`：編集するプロビジョニングスキームの名前。
- `NetworkMapping`：更新されたネットワークマッピング。

次のコマンドを実行します。例：

```
Set-ProvScheme  -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property xsi:type=`"StringProperty`"
Name=`"ClusterId`" Value=`"000xxxx-1fb0-xxxxx-4fc8-5c257335xxxx`" /
><Property xsi:type=`"StringProperty`" Name=`"CPUCores`" Value=`"1`" /></
CustomProperties>"  -NetworkMapping @{"6"="XDHyp:\HostingUnits\<Hosting
Unit Name>\Clusters.folder\<Cluster Name>\<Network name>.network"}
-ProvisioningSchemeName "<ProvisioningSchemeName>" -VMCpuCount 4
```

詳細情報

- 接続とリソースの作成および管理

- Nutanixへの接続
- Nutanixクラウドおよびパートナーソリューションへの接続
- マシンカタログの作成
- Nutanixカタログの作成
- マシンカタログの管理

VMwareカタログの管理

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、VMware仮想化環境に固有の詳細を扱っています。

> **注:**
>
> VMwareカタログを管理する前に、VMwareカタログの作成を完了する必要があります。「VMwareカタログを作成する」を参照してください。

マシンカタログのフォルダーIDを更新する

MCSマシンカタログのフォルダーIDは、`Set-ProvScheme`コマンドのカスタムプロパティで`FolderId`を指定することで更新できます。フォルダーIDの更新後に作成されたVMは、この新しいフォルダーIDの下に作成されます。このプロパティが`CustomProperties`で指定されていない場合、VMはマスターイメージが配置されているフォルダーの下に作成されます。

マシンカタログのフォルダーIDを更新するには、次の手順を実行します。

1. Webブラウザーを開き、**vSphere Web Client**のURLを入力します。
2. 資格情報を入力し、**ログイン**をクリックします。
3. **vSphere Web Client**でVM配置フォルダーを作成します。
4. PowerShellウィンドウを開きます。
5. **asnp citrix®***を実行して、Citrix固有のPowerShellモジュールをロードします。
6. `Set-ProvScheme`の`CustomProperties`で`FolderID`を指定します。この例では、フォルダーIDの値は`group-v2406`です。

```
Set-ProvScheme -ProvisioningSchemeUid
"50bb319c-2e83-4a37-9ea1-94f630687372" -CustomProperties
"<CustomProperties xmlns=""http://schemas.citrix.com/2014/xd/
machinecreation"" xmlns:xsi=""http://www.w3.org/2001/XMLSchema-
```

```
instance""><Property xsi:type=""StringProperty"" Name=""FolderId""
Value=""group-v2406"" /></CustomProperties>"
```

7. Studioを使用してマシンカタログにVMを追加します。
8. vSphere Web Clientで新しいVMを確認します。新しいVMは新しいフォルダーの下に作成されます。

vSphereでフォルダーIDを検索する

VM のフォルダー ID を見つけるには、任意の ESXi または vCenter サーバーシステムで Managed Object Browser (MOB) にアクセスします。

MOB は、すべての ESX/ESXi および vCenter サーバーシステムに組み込まれている Web ベースのサーバーアプリケーションです。この vSphere ユーティリティを使用すると、VM、データストア、リソースプールなどのオブジェクトに関する詳細情報を表示できます。

1. Web ブラウザーを開き、`http://x.x.x.x/mob` と入力します。ここで、x.x.x.x は vCenter Server または ESX/ESXi ホストの IP アドレスです。例: `<https://10.60.4.70/mob>`。
2. MOB の **Home** ページで、プロパティ **content** の値をクリックします。
3. **rootFolder** の値をクリックします。
4. **childEntity** の値をクリックします。
5. **vmFolder** の値をクリックします。
6. フォルダー ID は **childEntity** の値にあります。

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
準備用 VM	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"Xd構成":"Xdプロビジョニング済み=True"
カタログ内のVM	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"XdConfig:"XdProvisioned=True"

詳細情報

- 接続とリソースの作成および管理
- VMwareへの接続
- マシンカタログの作成
- VMwareカタログを作成する
- マシンカタログの管理

電源管理

Citrix Virtual Apps and Desktops™ を使用すると、さまざまなサポート対象のハイパーバイザーとクラウドサービスで、MCSでプロビジョニングされたVMの電源を管理できます。電源管理操作により、以下が提供されます。

- 最適なユーザーエクスペリエンス
- コスト管理と電力節約

利用可能な電源操作は次のとおりです。

- 起動
- シャットダウン
- 再起動
- サスペンド
- 再開
- 強制再起動
- 強制シャットダウン

> **注:**
>
> - 非永続VMの場合、電源サイクル（シャットダウン/起動および再起動）によりOSディスクがリセットされます。
> - 電源操作の機能と動作は、ハイパーバイザーまたはクラウドサービスによって異なります。

> この記事では、特定のサポート対象ハイパーバイザーに関連する主要な電源管理機能について説明します。

- AWS VMの電源管理(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/power-management/power-manage-aws-vms.html)
- Azure VMの電源管理(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/power-management/power-manage-azure-vms.html)

AWS VMの電源管理

必要な権限については、「Required AWS permissions」を参照してください。

インスタンスの休止

休止プロセスでは、インスタンスのインメモリ状態と、プライベートIPアドレスおよびElastic IPアドレスが保存され、中断したところから正確に再開できます。

インスタンスに休止が指示されると、インメモリ状態がルートEBSボリュームのファイルに書き込まれ、その後シャットダウンされます。Amazon EBSボリュームは、インスタンスにアタッチできる耐久性のあるブロックレベルのストレージデバイスです。ボリュームをインスタンスにアタッチすると、物理ハードドライブと同じように使用できます。インスタンスのルートEBSボリュームを暗号化します。暗号化により、メモリからEBSボリュームにコピーされる機密データが適切に保護されます。EBS暗号化の詳細については、「Amazon EBS encryption」を参照してください。

サポートされているインスタンスの休止には、次の制限があります。

- インスタンスメモリ（RAM）は最大150 GBまでのみサポートされます
- UEFIブートモードはサポートされていません
- EBSボリュームタイプとしてサポートされているのは、汎用SSDとプロビジョンドIOPS SSDのみです。

休止をサポートするVMを作成する

休止をサポートするVMを作成するには：

1. ホスト接続を作成します。「Connection to AWS」を参照してください。
2. EBSルートが暗号化され、**Stop-Hibernate**プロパティが有効になっているインスタンスを起動します。インスタンスの起動方法、ルートEBSボリュームの暗号化、および休止の有効化の詳細については、`<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html/>`を参照してください。このインスタンスをマスターイメージとして使用してAMIを作成します。

3. マスターイメージを準備します。

   a. マスターイメージにVDAをインストールします。Citrixでは、最新の機能にアクセスできるように、最新バージョンをインストールすることをお勧めします。マスターイメージにVDAをインストールしないと、カタログの作成が失敗します。VDAのインストール方法の詳細については、「Install VDAs」を参照してください。

   b. マスターイメージを、アプリケーションとデスクトップが属するドメインに参加させます。マスターイメージが、マシンが作成されるホストで利用可能であることを確認します。

4. そのインスタンスからAMIを作成します。インスタンスからAMIを作成する方法については、「Amazon EC2インスタンスからAMIを作成する」を参照してください。

5. `New-ProvScheme`コマンドを使用してマシンカタログを作成します。`AwsCaptureInstanceProperties`カスタムプロパティを**True**に設定します。Web StudioでAWSインスタンスプロパティを有効にする方法については、「**Web StudioでのAWSインスタンスプロパティの適用と運用リソースのタグ付け**」を参照してください。

   ```
   New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot

   -CustomProperties "AwsCaptureInstanceProperties,true;"

   -HostingUnitName "xxx" -IdentityPoolName $catalog_name
   -InitialBatchSizeHint 1

   -MasterImageVM "xyz.template" -NetworkMapping @{"0"="XDHyp:
   \HostingUnits\MyConn\\us-east-2a.availabilityzone\10.0.0.0``/24
   (vpc-0f1771e45671aedcd).network"}

   -ProvisioningSchemeName $catalog_name

   -RunAsynchronously -Scope @() -SecurityGroup @("xxx") -ServiceOffering
   "xxx"
   ```

   PowerShell コマンドを使用してマシンカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/>` を参照してください。

ハイバネート可能な VM は、次の場合に作成されます。

- **Stop-Hibernate**プロパティが有効になっているマスターイメージから作成されたAMIを選択した場合。
- マスターVMがドメインに参加しており、VDAがインストールされている場合。
- 休止状態を処理できる正しいVMサイズ（サービス提供）を選択した場合。

New-ProvSchemeコマンドは、次の場合に適切なエラーメッセージとともに失敗します。

- マスターVMで休止状態が有効になっているが、サービス提供が休止状態を処理できない場合。
- マスターVMがドメインに参加しておらず、VDAがインストールされていない場合。

サービス提供とAMIの休止状態

サービス提供とAMI（テンプレート）の休止状態を取得するには、次のコマンドを実行します。

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b(ami-0e6c5b33a52d2a6b6).template'`
- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

既存の休止状態対応プロビジョニングスキームのサービス提供を更新する

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering
<String>
```

サービス提供に互換性がない場合、システムは例外メッセージを表示します。

休止状態をサポートするマシンカタログを作成する

マシンカタログを作成する際、休止状態をサポートするマシンプロファイルを使用できます。

1. カタログ作成ウィザードで、マシンプロファイルの選択まで指示に従います。
2. **Machine Template**ページで、**Select a machine profile**をクリックし、マシンプロファイルを選択します。
3. **Virtual Machine**ページで、**Edit**アイコンをクリックし、VMを選択します。

> **注:**

> マシンプロファイルで休止状態が有効になっている場合、システムは休止状態にできるVMのみを表示します。

4. 画面の指示に従ってすべての設定を完了します。**Summary**ページには、カタログの休止状態が表示されます。

> **注:**
>
> マシンカタログの編集で、マシンプロファイルを休止状態が有効なものに変更すると、それに応じてVMを再構成するように求められます。

休止状態をサポートするマシンカタログを更新する

既存のマシンカタログを、休止状態をサポートしないマシンカタログで更新しようとすると、適切なエラーメッセージが表示されて更新が失敗します。

休止状態のVMの電源管理

休止状態のVMに対して、以下の電源管理操作を実行できます。

1. 実行状態のVMをサスペンドする。
2. サスペンド状態のVMを再開する。
3. サスペンド状態のVMを再起動する。

Azure VM の電源管理

必要な権限については、「必要なAzure権限」を参照してください。

Azureオンデマンドプロビジョニング

Azureオンデマンドプロビジョニングでは、プロビジョニングが完了した後、Citrix Virtual Apps and Desktops™ が電源オンアクションを開始したときにのみVMが作成されます。

MCSを使用してAzure Resource Managerでマシンカタログを作成する場合、Azureオンデマンドプロビジョニング機能は次のとおりです。

- ストレージコストを削減します
- カタログ作成を高速化します

MCSカタログを作成すると、Azure portalにリソースグループ内のネットワークセキュリティグループ、ネットワークインターフェイス、ベースイメージ、およびIDディスクが表示されます。

Azure portalには、Citrix Virtual Apps™ and Desktops が電源オンアクションを開始するまでVMは表示されません。次の違いを持つ2種類のマシンがあります。

- プールされたマシンの場合、オペレーティングシステムディスクとライトバックキャッシュはVMが存在する場合にのみ存在します。コンソールでプールされたマシンをシャットダウンすると、VMはAzure portalに表示されません。マシンを定期的にシャットダウンする場合（たとえば、勤務時間外）、ストレージコストを大幅に節約できます。
- 専用マシンの場合、オペレーティングシステムディスクはVMが最初に電源オンされたときに作成されます。Azure portalのVMは、マシンIDが削除されるまでストレージに残ります。コンソールで専用マシンをシャットダウンしても、VMはAzure portalに表示されたままになります。

注:

オンデマンドプロビジョニング機能の前に作成されたAzureカタログ（「レガシー」カタログ）のサポートは非推奨です。したがって、Azureレガシーカタログ VMを再作成してください。カタログはオンデマンドとしてプロビジョニングされ、ストレージコストを節約できます。

電源サイクル時にプロビジョニングされた仮想マシンを保持する

電源サイクル時にプロビジョニングされた仮想マシンを保持するかどうかを選択します。PowerShellパラメーター `New-ProvScheme CustomProperties` を使用します。このパラメーターは、プロビジョニングされた仮想マシンが電源サイクル時に永続化するかどうかを決定するために使用される追加のプロパティ `PersistVm` をサポートします。電源オフ時に仮想マシンを永続化するには `PersistVm` プロパティを **true** に設定し、電源オフ時に仮想マシンが保持されないようにするにはプロパティを **false** に設定します。

注記：

`PersistVm` プロパティは、`CleanOnBoot` および `UseWriteBackCache` プロパティが有効なプロビジョニングスキームにのみ適用されます。非永続仮想マシンに対して `PersistVm` プロパティが指定されていない場合、それらは電源オフ時にAzure環境から削除されます。

次の例では、`New-ProvScheme CustomProperties` パラメーターは `PersistVm` プロパティを**true**に設定します。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
resourcegroup" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>
```

次の例では、`New-ProvScheme CustomProperties`パラメーターは、`PersistVM`を**true**に設定することでライトバックキャッシュを保持します。

```
 New-ProvScheme

 -AzureAdJoinType "None"

 -CleanOnBoot

 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageType`" Value=`"Standard_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"false`" /
><Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"PersistVm`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"ResourceGroups`" Value=`"demo-resourcegroup`" /><Property
xsi:type=`"StringProperty`" Name=`"LicenseType`"
```

```
Value=`"Windows_Client`" /></CustomProperties>"

 -HostingUnitName "demo"

 -IdentityPoolName "NonPersistent-MCSIO-PersistVM"

 -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-
test.resourcegroup\demo-snapshot.snapshot"

 -NetworkMapping @ {"0"="XDHyp:\HostingUnits\demo\
\virtualprivatecloud.folder\East US.region\virtualprivatecloud.folder\ji-
test.resourcegroup\jitest-vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"

 -ServiceOffering "XDHyp:
\HostingUnits\demo\serviceoffering.folder\Standard_B2ms.serviceoffering"
-UseWriteBackCache

 -WriteBackCacheDiskSize 127

 -WriteBackCacheMemorySize 256
```

ヒント：

`PersistVm`プロパティは、プロビジョニングされた仮想マシンを保持するかどうかを決定します。`PersistOsdisk`プロパティは、OSディスクを永続化するかどうかを決定します。プロビジョニングされた仮想マシンを保持するには、まずOSディスクを保持します。仮想マシンを削除せずにOSディスクを削除しないでください。`PersistVm`パラメーターを指定せずに`PersistOsdisk`プロパティを使用できます。

ストレージタイプの変更失敗時の電源オン動作をカスタマイズする

電源オン時に、Azureでの障害により、管理ディスクのストレージタイプが目的のタイプに変更できない場合があります。このようなシナリオでは、VMはオフのままで、障害メッセージが送信されます。ただし、ストレージが構成されたタイプに復元できない場合でもVMの電源をオンにするか、VMをオフのままにするかを選択できます。

- カスタムプロパティ`FailSafeStorageType`を**true**（デフォルト設定）として構成した場合、または`New-ProvScheme`または`Set-ProvScheme`コマンドで指定しない場合：

  - 電源オン時に、VMは誤ったストレージタイプで電源がオンになります。
  - シャットダウン時に、VMは誤ったストレージタイプでオフのままになります。

- `New-ProvScheme`または`Set-ProvScheme`コマンドでカスタムプロパティ`FailSafeStorageType`を**false**として構成した場合：
  - 電源オン時に、VMは誤ったストレージタイプでオフのままになります。
  - シャットダウン時に、VMは誤ったストレージタイプでオフのままになります。

マシンカタログを作成するには：

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix®*`を実行します。
3. まだ作成されていない場合は、IDプールを作成します。
4. `New-ProvScheme`でカスタムプロパティを追加します。例：

```
New-ProvScheme -HostingUnitName "Azure-Resources-1" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\Azure-
Resources-1\image.folder\abc.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\Azure-
Resources-1\ght.folder\abc.resourcegroup\abc-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "name"

-ServiceOffering "XDHyp:\HostingUnits\Azure-
Resources-1\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown`"
Value=`"Standard_LRS`" />
```

```
<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"true`" />

</CustomProperties>"
```

5. マシンカタログを作成します。Remote PowerShell SDKを使用してカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

既存のマシンカタログを更新して、`FailSafeStorageType`カスタムプロパティを含めます。この更新は既存のVMには影響しません。

1. `Set-ProvScheme`コマンドでカスタムプロパティを更新します。例：

```
Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "

<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"false`" />

</CustomProperties>"
```

Set-ProvScheme で行われた変更を既存の VM に適用するには、`-StartsNow` および `-DurationInMinutes -1` パラメータを指定して `Set-ProvVMUpdateTimeWindow` コマンドを実行します。

1. `-StartsNow` および `-DurationInMinutes -1` パラメータコマンドを指定して `Set-ProvVMUpdateTimeWindow` コマンドを実行します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

2. VMを再起動します。

休止状態対応 VM を作成する

Azure環境では、休止状態をサポートするMCSマシンカタログを作成できます。この機能を使用すると、VMを中断し、ユーザーが再度サインインしたときにVMの以前の状態に再接続できます。

休止状態機能は以下に適用されます。

- シングルセッションOS
- 永続VMと非永続VM
- 静的およびランダム (プールされた) VDI デスクトップ

VDI デスクトップが静的かランダムかに関わらず、VM を休止状態にした後、同じセッションに再開できます。

このセクションでは、以下を参照してください。

- 前提条件
- 制限事項
- 休止状態対応のマシンカタログを作成および管理する
- 既存の休止状態対応 VM 用のマシンカタログを作成する
- 休止状態プロパティを確認する
- VM の電源管理 (手動および自動)

休止状態を使用するための前提条件

休止状態を使用するには、以下のタスクを完了していることを確認してください。

- Windows と Linux の両方のマスターイメージに Azure VM エージェントをインストールします。Windows イメージのページファイルは一時ディスクに配置できます。マシンカタログで休止状態が有効になっている場合、MCS はページファイルの場所をベースディスクの C: ドライブに設定します。
- MCS は、生成されたリソースの休止状態プロパティを自動的に設定します。休止状態をサポートするために、マスターリソースのプロパティを構成する必要はありません。
- サブスクリプションで休止状態をサポートする VM サイズを使用してください。
- VM が休止状態機能を継承できるように、休止状態対応のマシンプロファイル (VM またはテンプレート仕様) を作成します。VM の作成については、休止状態の開始 を参照してください。

> **注:**
>
> Microsoftによると、OSディスクから休止状態が有効なVMを展開できます。この機能は現在一部のリージョンでサポートされており、まもなくすべてのリージョンで利用可能になります。詳細については、「OSディスクから休止状態が有効なVMを展開する」を参照してください。

テンプレート仕様を作成するには、次の手順を実行します。

a. Azure Portalを開きます。テンプレートで使用する構成を持つVMを選択します。左ペインで**テンプレートのエクスポート**を選択します。
b. **パラメーターを含める**チェックボックスをオフにします。コンテキストをコピーし、たとえば`VMExportTemplate.json`のようなJSONファイルとして保存します。
c. テンプレートでパラメーター`hibernationEnabled`が`true`であることを確認します。パラメーターが`true`でない場合は、使用したVM構成を確認してください。テンプレートファイルでサポートされているVMサイズを指定できます。ただし、カタログの作成時にマシンサイズを指定することもできます。
d. ネットワークインターフェースリソースのテンプレートをJSONファイル`VMExportTemplate.json`に追加します。その結果、2つのリソースを持つARMテンプレートファイルができます。
e. **Azure Portal > テンプレート仕様 > テンプレートのインポート > ローカルテンプレートファイルの選択**を選択し、このテンプレートファイルをARMテンプレート仕様としてインポートします。
f. ARMテンプレート仕様が作成されたら、マシンプロファイルとして使用できます。

> **注:**
>
> Citrix Studioに同期されるまで数分かかる場合があります。

詳細については、Microsoftドキュメント休止状態を使用するための前提条件を参照してください。

制限事項

- シングルセッションOSマシンカタログ（永続的および非永続的）のみがサポートされています。

- エフェメラルOSディスクとMCS I/O機能は、Azureの休止状態をサポートしていません。
- 休止状態は、自動Windowsアップデート中に失敗する可能性があります。

詳細については、Microsoftドキュメントを参照してください。

休止状態対応のマシンカタログを作成および管理する

休止状態対応VMを作成するには、以下を使用して休止状態対応マシンカタログを作成および管理できます。

- Web Studio、または
- PowerShellコマンド

WEB STUDIOを使用してカタログを作成する

1. **マシンカタログの作成**を選択します。カタログ作成ウィザードが開きます。
2. **マシンタイプ**ページで、このカタログの**シングルセッションOS**マシンタイプを選択します。
3. **マシン管理**ページで、次のように設定を選択します。
   a. 「**電源管理されているマシン（仮想マシンやブレードPCなど）**」を選択します。
   b. 「**Citrix Machine Creation Services™ (MCS)**」を選択します。
4. **デスクトップエクスペリエンス**ページで、必要に応じてランダムまたは静的デスクトップエクスペリエンスを選択します。
5. **イメージ**ページで、マスターイメージを選択します。**マシンプロファイルを使用**チェックボックスをオンにし、休止状態をサポートするマシンプロファイルを選択します。ツールヒントをクリックして、マシンプロファイルが休止状態をサポートしているかどうかを確認します。

   > **注:**
   >
   > Azureマネージドマスターイメージを選択すると、ブレードにはリソースと同じリージョンに属するすべてのイメージが一覧表示されます。

6. **ストレージとライセンスの種類**ページで、このカタログに使用するストレージとライセンスを選択します。
7. **仮想マシン**ページで、VM の数、VM サイズ、および可用性ゾーンを選択します。

   > **注:**

> ハイバネーションをサポートするマシンサイズのみが選択肢として表示されます。

8. **NIC**ページで、VM に使用させる NIC を追加します。
9. **ディスク設定**ページで、ライトバックキャッシュディスクのストレージの種類とサイズを選択します。
10. **リソースグループ**ページで、VM をプロビジョニングするリソースグループを選択します。
11. **マシン ID**ページで、**新しい Active Directory アカウントを作成**を選択します。次に、アカウントの命名スキームを指定します。
12. **ドメイン資格情報**ページで、**資格情報を入力**をクリックします。ターゲットの Active Directory ドメインでアカウント作成を実行するために、ドメイン資格情報を入力します。
13. **概要**ページで、マシンカタログの名前を入力し、**完了**をクリックします。

MCS マシンカタログの作成が完了したら、カタログリストでカタログを見つけ、**テンプレートプロパティ**タブをクリックします。パラメーター**休止状態**の値は**サポート済み**である必要があります。

マシンカタログを編集する場合は、以下の制限事項を考慮してください。

- 現在のマシンカタログが休止状態をサポートしている場合、次のことはできません。
  - VM サイズを休止状態に対応しないものに変更する。
  - マシンプロファイルを休止状態にできないものに変更します。
- 現在のマシンカタログが休止状態をサポートしていない場合、次のことはできません。
  - 現在、Web Studio を使用してマシンプロファイルを休止状態にできるものに変更する。

既存の休止状態対応 VM を管理するためのマシンカタログを作成する

休止状態対応 VM をすでに所有しており、それらを一時停止および再開したい場合は、それらの VM を電源管理のためにインポートするマシンカタログを作成します。

> **注：**
>
> 休止状態対応 VM と非対応 VM の両方を含むマシンカタログを作成できます。ただし、休止状態関連の機能が必要な場合は、休止状態対応 VM のみを含むマシンカタログを作成する必要があります。

> Web Studio を使用して既存の休止状態対応 VM のカタログを作成するには、画面の指示に従って手順を完了し、次の主要な設定に注意してください。

1. **マシン管理**ページで、**電源管理されているマシン**を選択し、マシンの展開方法として**その他のサービスまたはテクノロジー**を選択します。
2. **仮想マシン**ページで、休止状態対応 VM のみを追加またはインポートします。

POWERSHELL コマンドを使用してマシンカタログを作成する

休止状態を使用するためのすべての要件を満たした後、`New-ProvScheme`コマンドを使用して休止状態対応マシンカタログを作成できます。Remote PowerShell SDK を使用してカタログを作成する方法については、「New-ProvScheme」を参照してください。

カタログの作成中に、次の PowerShell コマンドを使用して、VM サイズとマシンプロファイルが休止状態をサポートしているかどうかを確認できます。

- VM サイズの場合、次のコマンドを実行し、プロパティ`supportsHibernation`が**True**であるかどうかを確認します。例：

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath
@("XDHyp:\HostingUnits\ <VirtualNetwork> \serviceoffering.folder") |
select Name, AdditionalData | ConvertTo-Json
```

- マシンプロファイルの場合、次のコマンドを実行し、プロパティ`supportsHibernation`が**True**であるかどうかを確認します。例：

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath
@("XDHyp:\HostingUnits\ <VirtualNetwork>
\machineprofile.folder\abc.resourcegroup")|select Name, AdditionalData|
ConvertTo-Json
```

マシンカタログを編集する場合は、次の制限事項を考慮してください。

- 現在のマシンカタログがハイバネーションをサポートしている場合、次のことはできません。
  - VMサイズをハイバネーション非対応のものに変更する
  - マシンプロファイルをハイバネーション非対応のものに変更する
- 現在のマシンカタログがハイバネーションをサポートしていない場合、次のことはできません。

    - 現在、Web Studioを使用してマシンプロファイルをハイバネーション対応のものに変更する。

Remote PowerShell SDKを使用してカタログのVMサイズとマシンプロファイルを変更する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/>`を参照してください。

ハイバネーションプロパティの確認

PowerShellコマンドを使用して、マシンカタログ、VM、およびブローカーマシンのハイバネーションプロパティを確認できます。

- プロビジョニングスキームのハイバネーションプロパティを確認するには、次のPowerShellコマンドを実行します。`HibernationEnabled`パラメーターは`True`である必要があります。

```
(Get-ProvScheme -provisioningSchemeName <YourSchemeName>).VMMetadata
-join "" |  ConvertFrom-Json | Select HibernationEnabled
```

- プロビジョニングVMのハイバネーションプロパティを確認するには、次のPowerShellコマンドを実行します。`SupportsHibernation`パラメーターは`True`である必要があります。

```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json |
Select SupportsHibernation
```

- ブローカーマシンのハイバネーション容量を確認するには、次のPowerShellコマンドを実行します。**Suspend**および**Resume**電源アクションは、ハイバネーション機能を示します。

```
(Get-BrokerMachine -MachineName
<YourMachineName>).SupportedPowerActions
```

ハイバネーション対応VMの電源管理

ハイバネーション対応VMに対して、次の電源管理操作を実行できます。

- 実行状態のVMを**一時停止**する
- **再開**: サスペンド状態からVMを再開する
- **強制シャットダウン**: サスペンド状態からVMを強制シャットダウンする
- **強制再起動**: サスペンド状態からVMを強制再起動する

詳細については、以下を参照してください。

- 一時停止
- 再開

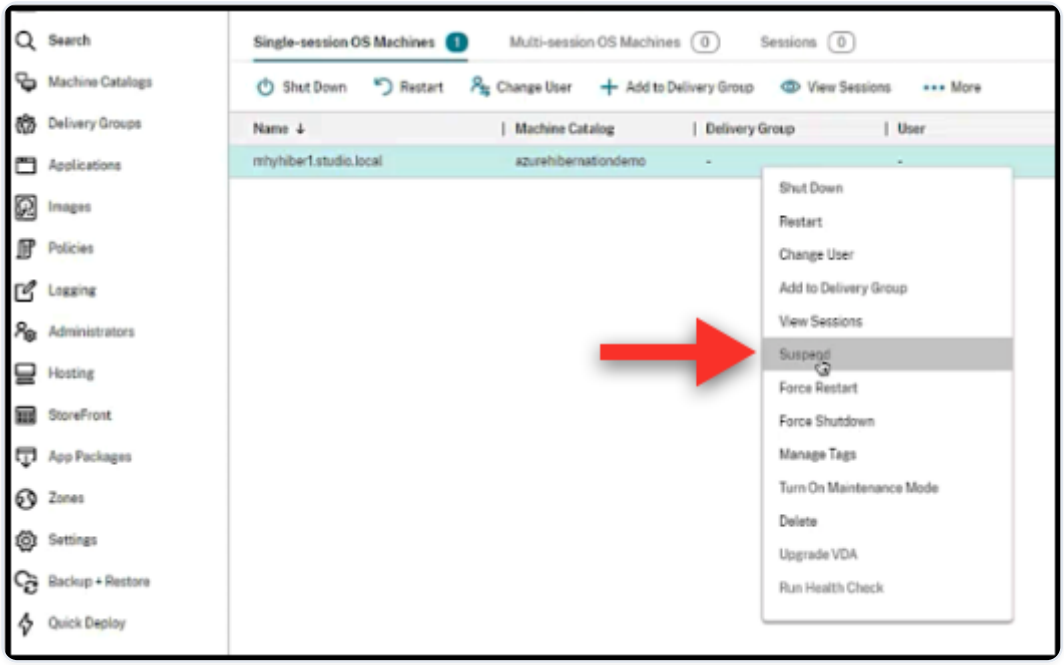
一時停止

次のいずれかの方法でVMをサスペンドできます。

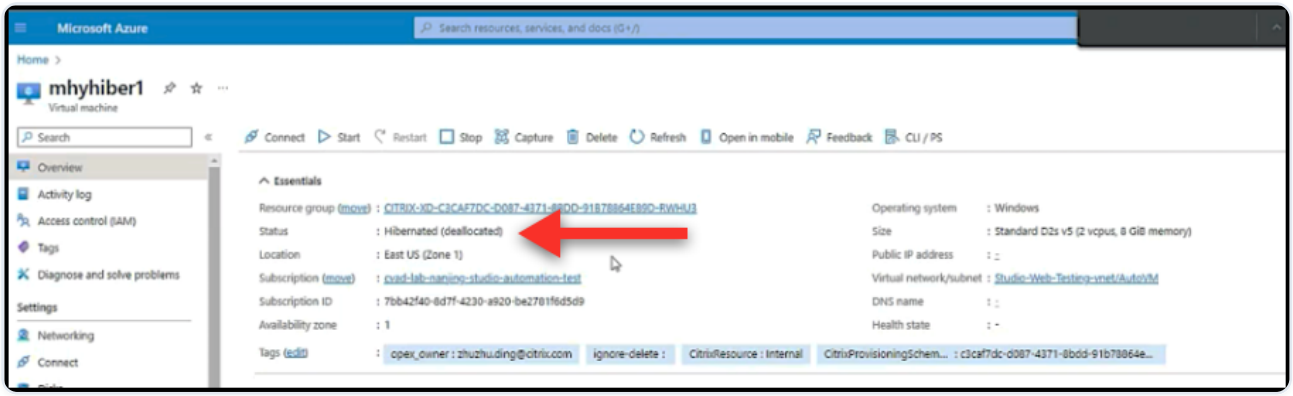
- Web Studioを使用して**手動で**
- タイムアウトポリシーを使用して**自動的に**: 詳細については、「その他の設定」を参照してください。

VMを手動で一時停止するには：

1. VMを右クリックし、 を選択します。 をクリックしてアクションを確定します。 が から に変わります。



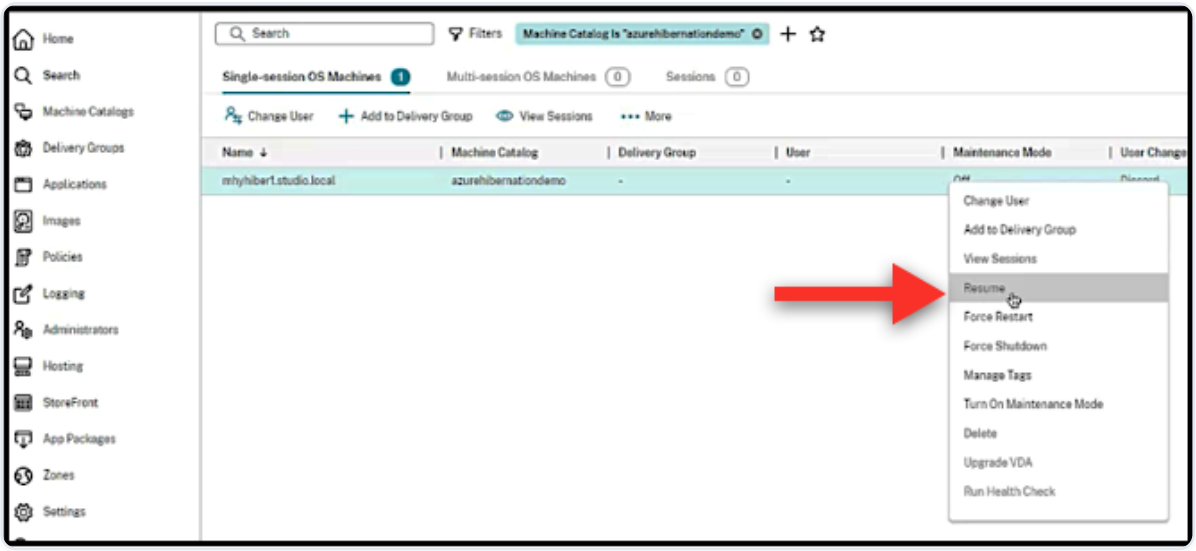
AzureポータルでVMのステータスを確認できます。



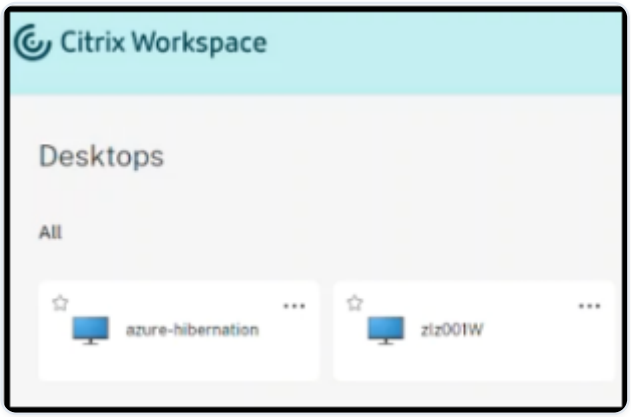
再開

休止状態のVMを再開するには、次のいずれかの方法を使用します。

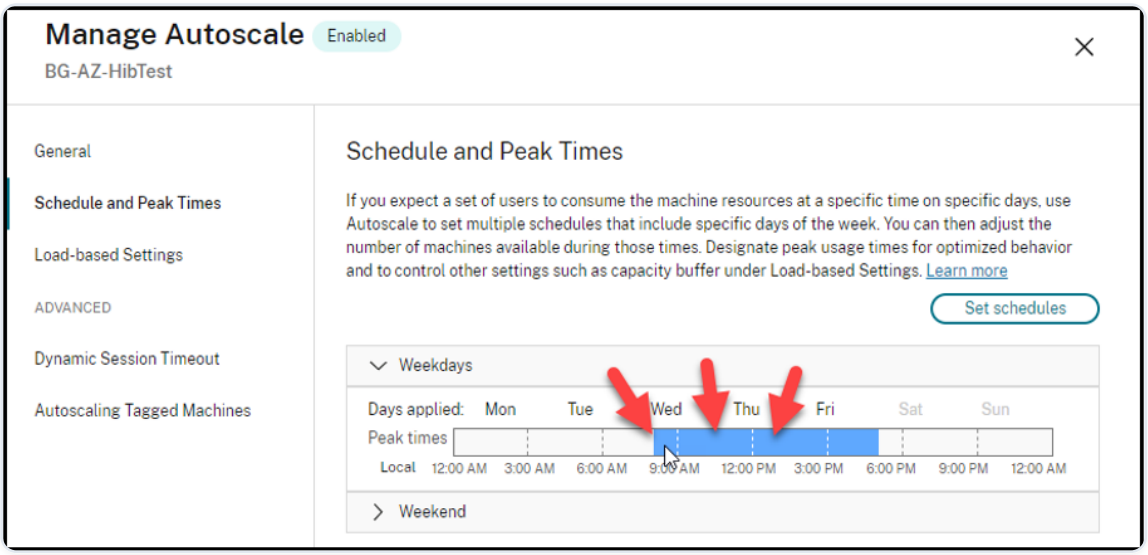
- **手動で：**
  - 管理者はWeb Studioを使用してVMを再開できます。



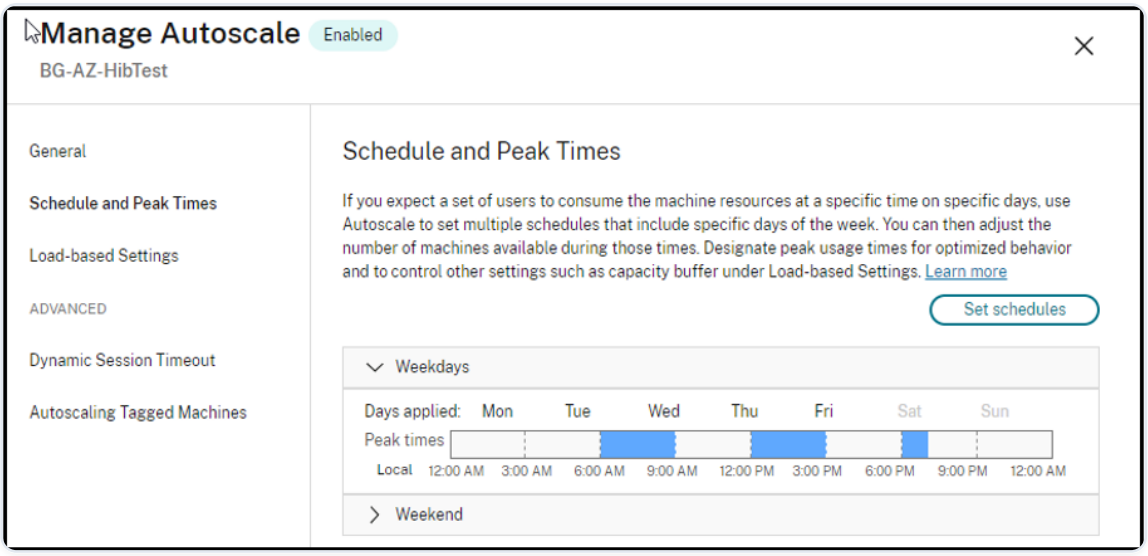
  - エンドユーザーは、デスクトップアイコンをクリックすると、Citrix Workspace™メニューを使用してVMを起動できます。



- **自動的に：**
  - ピーク時間を正しく構成すると、Autoscale™は休止状態のマシンを自動的に起動できます。タイムスケジュールをクリックして、ピーク時間を30分間隔で設定できます。各青いフレームは、ピーク時間としてマークされたタイムスロットを表します。ピーク時間には、連続したタイムスロットと非連続のタイムスロットを設定できます。
    - 連続したタイムスロット



- 連続しない時間帯



注:

Autoscaleの管理 > 負荷ベースの設定で、**アクション**が**中断**として構成されている場合、そのデリバリーグループ内のすべてのVMが休止機能を備えていることを確認してください。そうでない場合、休止できないVMは実行を継続します。

オートスケール負荷ベース設定の管理(/en-us/citrix-virtual-apps-desktops/2511/media/azure-hibernation-autoscale.png)

休止状態の失敗に関する警告メッセージを取得する

MCSプロビジョニング済みおよび既存の休止状態対応VMの休止状態の失敗の場合に、PowerShellコマンド`Get-ProvOperationEvent`を使用して警告メッセージを取得できます。PowerShellコマンドの詳細については、SDKドキュメントGet-ProvOperationEventを参照してください。

これを行うには：

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. 休止状態の失敗の場合に警告メッセージを取得するために`Get-ProvOperationEvent`を実行します。

```
Get-ProvOperationEvent -filter { OperationName -eq "Suspend" }
```

出力：

```
EventAdditionalData : Error code = OperationNotAllowed and Error
message = The Hibernate-Deallocate Operation cannot be performed on a
VM that has extension 'AzureHibernateExtension' in failed state. For
more information, see https://aka.ms/hibernate-resume/errors. Error
details from the extension : Enabling

                  hibernate failed. Response from the powercfg command.
Exit Code: 1. Error message:

                  Hibernation failed with the following error: The
request is not supported.



                  The following items are preventing hibernation on
this system.

                    The current Device Guard configuration has disabled
hibernation.

                    An internal system component has disabled
hibernation.

                            Hypervisor
```

```
                  Status: 409

                  ErrorCode: OperationNotAllowed



                  Content:

                  {

                    "error": {

                      "code": "OperationNotAllowed",

                      "message": "The Hibernate-Deallocate Operation
cannot be performed on a VM that has extension
'AzureHibernateExtension' in failed state. For more information, see
https://aka.ms/hibernate-resume/errors. Error details from the
extension : Enabling hibernate failed. Response from the

                  powercfg command. Exit Code: 1. Error message:
\nHibernation failed with the following error: The request is not
supported.\r\r\n\r\nThe following items are preventing hibernation on
this system.\r\n\tThe current Device Guard configuration has disabled
hibernation.\r\n\tAn internal system

                  component has disabled hibernation.
\r\n\t\tHypervisor"

                    }

                  }

EventCategory       : Warning

EventDateTime       : 1/11/2024 4:18:31 AM

EventId             : 0

EventMessage        : Failed to suspend machine my-resource-group/my-
vm.

EventSeverity       : Important
```

```
EventSource          : AzureRmPlugin

EventState           : New

LinkedObjectType     : ProvisioningScheme

LinkedObjectUid      : 589cb600-6e65-479f-9d47-9715c4732366

OperationName        : Suspend

OperationTargetName  : my-resource-group/my-vm

OperationTargetType  : VirtualMachine

OperationType        : PowerManagement

Recommendation       :
```

休止状態の問題のトラブルシューティング

休止状態と信頼できる起動VM機能の両方を有効にしようとしたときに、ゲストOSの構成が正しくない場合、次のエラーメッセージが表示されます。

エラーコード	エラーメッセージ
OperationNotAllowed	拡張機能「AzureHibernateExtension」が失敗状態のVMでは、休止状態解除操作を実行できません。詳細については、`<https://aka.ms/hibernate-resume/errors/>`を参照してください。拡張機能からのエラー詳細：休止状態の有効化に失敗しました。powercfg コマンドからの応答。終了コード：1。エラーメッセージ：次のエラーで休止状態に失敗しました：要求はサポートされていません。以下の項目がこのシステムでの休止状態を妨げています。**現在のDevice Guard構成により休止状態が無効になっています。内部システムコンポーネントにより休止状態が無効になっています。**

この問題を解決するには、ゲストVM内で仮想化が有効になっていることを確認してください。たとえば、Windows環境でHyper-Vが有効になっていることを確認します。Microsoft Windowsの制限によると、信頼できる起動がVMで有効になっている場合にのみ、ネストされた仮想化で休止状態がサポートされます。

警告メッセージの詳細については、Microsoft ドキュメント「VM の休止状態のトラブルシューティング」を参照してください。

> **注:**
>
> VMの再開の失敗に関連するエラーメッセージは、今後のリリースで提供される予定です。

詳細情報

Citrix Azureの休止状態の詳細については、Citrix Tech Zoneの記事を参照してください。

Red Hat OpenShift VMの電源管理

Citrix Virtual Apps and Desktops™では、Red Hat OpenShift VMの電源管理を行うことができます。ナビゲーションペインの検索ノードを使用して、電源管理するマシンを見つけます。

次の電源操作が利用可能です。

- 起動
- シャットダウン
- 強制シャットダウン
- 再起動

> **注:**
>
> リセット、一時停止、再開の電源操作はサポートされていません。

セキュリティポリシー

この記事では、サポートされているさまざまなクラウドサービスにおけるセキュリティ機能について説明します。セキュリティ機能には、次のものがあります。

- セキュリティグループ(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/security-policies/security-group.html)
- セキュアブート(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/security-policies/secure-boot.html)
- 暗号化機能(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/security-policies/encryption-capabilities.html)

セキュアブートとvTPM

セキュアブートは、システムの起動を担当するUnified Extensible Firmware Interface (UEFI) の機能です。これにより、起動プロセス中に信頼できるソフトウェアのみがロードされることが保証されます。

Trusted Platform Module (TPM) は、暗号鍵やその他の機密データを安全に保存するハードウェアチップです。Virtual Trusted Platform Module (vTPM) はTPM と同じ機能を実行しますが、ソフトウェアで暗号コプロセッサ機能を実行します。TPM はセキュリティを強化できますが、セキュアブートの要件ではありません。

サポートされているハイパーバイザーの詳細については、以下を参照してください。

- AWS のセキュアブートとNitroTPM
- Google Cloud Platform のセキュアブートとvTPM
- Microsoft Azure のセキュアブートとvTPM
- Nutanix Prism Central のセキュアブートとvTPM
- ヴイエムウェアでの vTPM(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/security-policies/secure-boot.html#vtpm-in-vmware)
- XenServer® のセキュアブートとvTPM

AWS のセキュアブートとNitroTPM

AWS 環境では、NitroTPM および/またはUEFI セキュアブートが有効になっているマスターイメージ (AMI) を選択できます。そのため、カタログ内のプロビジョニングされたVM もNitroTPM および/またはUEFI セキュアブートが有効になっています。この実装により、VM は保護され、信頼できるものになります。NitroTPM およびUEFI セキュアブートの詳細については、Amazon ドキュメント を参照してください。NitroTPM およびUEFI セキュアブートが有効なカタログの作成については、VM インスタンスのNitroTPM およびUEFI セキュアブートを有効にする を参照してください。

Google Cloud Platform のセキュアブートとvTPM

Google Cloud Platform (GCP) でシールドされた仮想マシンをプロビジョニングできます。シールドされたVM の検証可能な整合性は、次の機能を使用して実現されます。

- セキュアブート
- vTPM対応メジャーブート
- 整合性監視

シールドされたVMでカタログを作成するためのPowerShellの使用方法について詳しくは、「Using PowerShell to create a catalog with shielded VM」を参照してください。

> **注:**
>
> マスターイメージにWindows 11をインストールする場合は、マスターイメージ作成プロセス中にvTPMを有効にする必要があります。また、カタログ作成にマシンプロファイルを使用する場合は、マシンプロファイルソース（VMまたはインスタンステンプレート）でvTPMを有効にする必要があります。単一テナントノードでWindows 11 VMを作成する方法については、「単一テナントノードでWindows 11 VMを作成する」を参照してください。

Microsoft AzureにおけるセキュアブートとvTPM

Azure環境では、Trusted Launchが有効なマシンカタログを作成できます。Azureは、第2世代VMのセキュリティを向上させるシームレスな方法としてTrusted Launchを提供します。Trusted Launchは、高度で永続的な攻撃手法から保護します。Trusted Launchを有効にするには、マシンプロファイルベースのカタログ構成を使用します。Trusted Launchの根幹にあるのは、VMのSecure Bootです。Trusted Launchは、クラウドによるリモートアテステーションを実行するためにvTPMも使用します。これは、プラットフォームの健全性チェックと、信頼に基づいた意思決定のために使用されます。Secure BootとvTPMは個別に有効にできます。 Trusted Launchでマシンカタログを作成する方法の詳細については、「Trusted Launchを使用したマシンカタログ」を参照してください。

Nutanix Prism CentralにおけるセキュアブートとvTPM

MCS は、Nutanix Prism Central を使用して、vTPM、UEFI、および Secure Boot を備えたマシンカタログの作成をサポートしています。vTPM および UEFI Secure Boot が有効なマスターイメージ (テンプレート) を選択できます。

Nutanix Prism Centralでは、UEFI Secure BootはvTPMを必要としません。ただし、vTPMをVMにリンクするには、Secure Bootが有効かどうかにかかわらず、VMがUEFIブートされている必要があります。

さらに、vTPM、UEFI、および Secure Boot が有効な VM は、Nutanix Prism Central からインポートでき、Citrix Virtual Apps and Desktops によって電源管理できます。

NutanixはvTPMとUEFIセキュアブートをサポートしています。以下を参照してください。

- AHV での vTPM (仮想トラステッドプラットフォームモジュール) サポート.
- VMのSecure Bootサポート
- Virtual Trusted Platform ModuleでAHV VMを保護する

VMware における vTPM

MCS は vTPM を使用したマシンカタログの作成をサポートしています。マスターイメージに Windows 11 がインストールされている場合、マスターイメージで vTPM を有効にすることが必須です。マシンプロファイルベースの構成が使用され、vTPM が有効になっている場合、カタログ内の VM は VM テンプレートから同じ vTPM コンテンツを継承します。マシンプロファイルが使用されておらず、マスターイメージで vTPM が有効になっている場合、カタログ内の VM は空の vTPM を持ちます。詳細については、「マシンプロファイルを使用したマシンカタログの作成」を参照してください。

XenServer® のセキュアブートと vTPM

XenServer は、サポートされている一部の VM オペレーティングシステムで UEFI セキュアブートを提供します。セキュアブートは、署名されていない、署名が正しくない、または変更されたバイナリが起動中に実行されるのを防ぎます。セキュアブートを強制する UEFI 対応 VM では、すべてのドライバーが署名されている必要があります。詳細については、「ゲスト UEFI とセキュアブート」を参照してください。

XenServer 8 では、UEFI セキュアブートに vTPM は必要ありません。ただし、vTPM を VM にリンクするには、その VM がセキュアブートが有効かどうかにかかわらず、UEFI で起動されている必要があります。Windows 11 VM にはリンクされた vTPM が必要であり、提供されたテンプレートから Windows 11 VM が作成されるときに自動的に作成されます。その他のオペレーティングシステムの場合、vTPM はオプションです。詳細については、「vTPM」を参照してください。

暗号化機能

暗号化機能は、共有仮想マシンホスト上の悪意のあるゲストによる攻撃や、ホスト上のすべての仮想マシンを管理するハイパーバイザー制御ソフトウェアによる攻撃から、仮想マシンのコンテンツを保護します。

サポートされているクラウドサービスの詳細については、以下を参照してください。

- AWS の暗号化機能
- Google Cloud Platform の暗号化機能
- Microsoft Azure の暗号化機能

AWS の暗号化機能

このセクションでは、AWS 仮想化環境における暗号化機能について説明します。

自動暗号化

アカウントで作成された新しい Amazon EBS ボリュームとスナップショットコピーの自動暗号化を有効にできます。詳細については、「自動暗号化」を参照してください。

Google Cloud Platform の暗号化機能

このセクションでは、Google Cloud Platform (GCP) 仮想化環境における暗号化機能について説明します。

Google マネージド暗号化キーが許可するよりもキー操作をより詳細に制御する必要がある場合は、顧客管理の暗号化キーを使用できます。顧客管理の暗号化キーを使用する場合、オブジェクトがバケットに保存されるときに Cloud Storage によってキーで暗号化され、リクエスターに提供されるときに Cloud Storage によって自動的に復号化されます。詳細については、「顧客管理の暗号化キー」を参照してください。

MCS カタログに顧客管理の暗号化キー (CMEK) を使用できます。詳細については、「顧客管理の暗号化キー (CMEK) の使用」を参照してください。

Microsoft Azure の暗号化機能

このセクションでは、Azure仮想化環境における暗号化機能について説明します。

Azureサーバー側暗号化

ほとんどのAzureマネージドディスクは、サーバー側暗号化（SSE）を使用してデータを保護し、セキュリティおよびコンプライアンスのコミットメントを満たすのに役立つAzure Storage暗号化で暗号化されています。Citrix Virtual Apps and Desktopsは、Azure Key Vaultを介したAzureマ

ネージドディスクの顧客管理暗号化キーをサポートしています。詳細については、Azureサーバー側暗号化を参照してください。

ホストでのAzureディスク暗号化

ホストでの暗号化機能を備えたMCSマシンカタログを作成できます。

この暗号化方法は、Azureストレージを介してデータを暗号化しません。VMをホストするサーバーがデータを暗号化し、その後、暗号化されたデータがAzureストレージサーバーを介して流れます。したがって、この暗号化方法はデータをエンドツーエンドで暗号化します。

ホストでの暗号化機能を持つMCSマシンカタログの作成に関する詳細については、ホストでのAzureディスク暗号化を参照してください。

Azure二重暗号化

二重暗号化は、プラットフォーム側暗号化（デフォルト）と顧客管理暗号化（CMEK）です。したがって、暗号化アルゴリズム、実装、または侵害されたキーに関連するリスクを懸念するセキュリティ意識の高いお客様は、この二重暗号化を選択できます。永続的なOSおよびデータディスク、スナップショット、イメージはすべて、二重暗号化によって保存時に暗号化されます。詳細については、マネージドディスクの二重暗号化を参照してください。

Azure機密VM

Azure機密コンピューティングVMは、仮想デスクトップがメモリ内で暗号化され、使用中に保護されることを保証します。

MCSを使用して、Azure機密VMを含むカタログを作成できます。このようなカタログを作成するには、マシンプロファイルワークフローを使用する必要があります。マシンプロファイルの入力として、VMとARMテンプレート仕様の両方を使用できます。

詳細については、Azure機密VMを参照してください。

マシンの負荷分散

負荷分散は、組織がクラウドのあらゆる利点を活用しながら、望ましいコストバランスを達成するのに役立ちます。負荷分散はデリバリーグループレベルで構成されます。

> **注：**
>
> 負荷分散は、マルチセッションOSマシンにのみ適用されます。

> 負荷分散には2つのオプションがあります。

- 水平負荷分散
- 垂直負荷分散

デフォルトでは、水平負荷分散が有効になっています。

水平負荷分散： 水平負荷分散モデルでは、受信ユーザーセッションは利用可能な最も負荷の低いマシンに割り当てられます。この例を考えてみましょう。展開環境で2つのVDAがあると仮定します。1つはアクティブなユーザーセッション（ユーザー1）を持ち、2番目のユーザー（ユーザー2）はセッションを待っています。水平負荷分散アルゴリズムは、より有利な負荷インデックスのため、ユーザー2をVDA 2に割り当てます。したがって、水平アルゴリズムはすべての利用可能なVDAにセッションを分散するため、負荷が減少してもマシンがシャットダウンするのを妨げる可能性があります。

垂直負荷分散： 垂直負荷分散モデルでは、セッションは最も負荷インデックスの高いVDAに割り当てられます。これにより、受信ユーザーセッションを他のユーザーがすでに使用しているVDAに統合し、電源をオンにしてユーザーセッションに備えておく必要があるVDAの数を減らすことができます。水平負荷分散で述べたのと同じ展開環境を考えてみましょう。ユーザー1はVDA 1に割り当てられ、垂直負荷分散アルゴリズムがユーザー2のセッションに適用されます。VDA 1の負荷インデックスが高いため、ユーザー2はVDA 1に割り当てられます。したがって、すべての受信セッションは、高負荷インデックスのウォーターマークに達するまで、最も負荷の高いVDAに割り当てられます。その後初めて、他のVDAがセッションの受信を開始します。

サイトレベルでの負荷分散設定

すべてのデリバリーグループに対して負荷分散を構成できます（サイト全体の構成）。

Studioからこの機能を構成するには、左ペインで**設定**を選択します。**マシンの負荷分散セッション**の下のオプションを選択します。

または、PowerShellを使用して、サイト全体で垂直負荷分散を有効または無効にすることもできます。`Set-BrokerSite` コマンドレットで `UseVerticalScalingForRdsLaunches` 設定を使用します。`UseVerticalScalingForRdsLaunches` 設定の値を表示するには、`Get-BrokerSite` を使用します。詳細については、コマンドレットのヘルプを参照してください。

> **ヒント：**

> マシンがホストできるセッションの最大数を指定するには、最大セッション数 ポリシー設定を使用します。

デリバリーグループレベルでの負荷分散設定

ロードバランシングはデリバリーグループレベルで構成でき、サイトレベルから継承されたロードバランシング設定を上書きできます。

これは、デリバリーグループの作成時または既存のデリバリーグループの編集時に構成できます。手順2. 負荷分散を参照してください。

ロード管理

負荷管理はサーバーの負荷を測定し、現在の環境条件でどのサーバーを選択するかを決定します。この選択は以下に基づいています。

- **サーバーメンテナンスモードの状態**: マルチセッションOSマシンは、メンテナンスモードがオフの場合にのみ負荷分散の対象となります。
- **サーバー負荷インデックス**: マルチセッションOSマシンを提供するサーバーが接続を受信する可能性を決定します。このインデックスは、セッション数やCPU、ディスク、メモリ使用量などのパフォーマンスメトリックの設定といった負荷評価子の組み合わせです。負荷評価子は、負荷管理ポリシー設定で指定されます。デフォルトでは、負荷インデックスは計算にセッション数のみを使用し、CPU、ディスク、またはメモリは負荷管理ポリシー設定で構成されるまで使用しません。ポリシー設定の詳細については、負荷管理ポリシー設定を参照してください。

  サーバー負荷インデックスが10000の場合、サーバーが完全にロードされていることを示します。他のサーバーが利用できない場合、ユーザーはセッションを起動したときに、デスクトップまたはアプリケーションが現在利用できないというメッセージを受け取る可能性があります。 負荷インデックスは、Director (Monitor)、Studio検索、およびSDKで監視できます。

  コンソール表示で、**サーバー負荷インデックス**列（デフォルトでは非表示）を表示するには、マシンを選択し、列ヘッダーを右クリックして、**列の選択**を選択します。**マシンカテゴリ**で、**負荷インデックス**を選択します。

  SDKでは、`Get-BrokerMachine` cmdletを使用します。詳細については、CTX202150を参照してください。
- **同時ログオン許容ポリシー設定**: サーバーへの同時ログオン要求の最大数。（この設定は、XenApp 6.xバージョンでの負荷スロットリングに相当します。）」

すべてのサーバーが同時ログオン許容設定以上である場合、次のログオン要求は保留中のログオンが最も少ないサーバーに割り当てられます。複数のサーバーがこれらの基準を満たす場合、負荷インデックスが最も低いサーバーが選択されます。同時ログオン許容を参照してください。

> **ヒント:**
>
> ログオン許容設定を適用し、指定された数を超える同時ログオンを失敗させるには、`Set-BrokerServiceConfigurationData Core.LogonToleranceIsHardLimit -SettingValue $true`を実行します。

デリバリーグループの作成

> **注：**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> デリバリーグループは、1つ以上のマシンカタログから選択されたマシンの集合です。デリバリーグループは、どのユーザーがそれらのマシンにアクセスできるか、および利用可能なアプリケーションとデスクトップを定義します。

デリバリーグループの作成は、サイトとマシンカタログを設定した後の次のステップです。後で初期設定を変更したり、必要に応じて追加のデリバリーグループを作成したりできます。

一部の機能と設定は、既存のデリバリーグループを編集する場合にのみ構成可能です。詳細については、「デリバリーグループの管理」を参照してください。

始める前に

デリバリーグループを作成する前に：

- 必要な選択肢と情報を理解するために、この記事を確認してください。

- ハイパーバイザー、クラウドサービス、またはマシンをホストするその他のリソースへの接続が作成されていることを確認してください。
- 仮想マシンまたは物理マシンを含むマシンカタログが利用可能であることを確認してください。

デリバリーグループを作成するには：

1. デリバリーグループなしでサイトとマシンカタログを作成した場合、Web Studioはデリバリーグループを作成するための正しい開始場所に案内します。

ウィザードのページ

サイトとマシンカタログを作成したが、デリバリーグループを作成していない場合、Web Studioはデリバリーグループを作成するための正しい開始点に案内します。

配信グループをすでに作成していて、別のグループを作成したい場合は、次の手順に従います。

1. を選択します。
2. アクションペインで、 を選択します。
3. デリバリーグループを整理するには、デフォルトの フォルダーの下にフォルダーを作成できます。詳細については、「フォルダーの作成」を参照してください。
4. グループを作成するフォルダーを選択し、 をクリックします。グループ作成ウィザードが開きます。
5. ウィザードは ページから開始します。このページは、今後の起動時にスキップするように選択できます。その後、次の表に示すように、いくつかのページが表示されます。各ページを完了したら、 をクリックして最終ページに進みます。

	マルチセッションOS	シングルセッションOS静的（割り当て済み）	シングルセッションOS共有（プール済み）	リモートPCアクセス
ページ	マシン	マシン	マシン	マシン
	ロードバランシング	配信タイプ	ユーザー	ユーザー
	ユーザー	ユーザー	アプリケーション	アプリケーション

	マルチセッションOS	シングルセッションOS静的（割り当て済み）	シングルセッションOS共有（プール済み）	リモートPCアクセス
	アプリケーション	アプリケーション	デスクトップ	デスクトップ割り当てルール
	デスクトップ	デスクトップ割り当てルール	アプリ保護	アプリ保護
	アプリ保護	アプリ保護	スコープ	スコープ
	スコープ	スコープ	ライセンス契約	ライセンス契約
	ライセンス契約	ライセンス契約	ポリシーセット	ポリシーセット
	ポリシーセット	ポリシーセット	ローカルホストキャッシュ	概要
	概要	概要	概要	

注:

- 選択したシングルセッションOS静的マシンカタログに利用可能な割り当て済みマシンがある場合、(**マシン**ページの直後に)**マシン割り当て**ページが表示されます。
- Local Host Cache settingページは、電源管理されたシングルセッションのプールされたマシンを含むデリバリーグループでのみ利用可能です。

マシンページ

1. シングルセッションのサスペンド対応VMのみを含むデリバリーグループを作成するには、 を選択します。

注:

この機能は、シングルセッションのサスペンド対応マシンにのみ適用されます。

2. マシンカタログを選択し、そのカタログから使用するマシンの数を選択します。

重要な考慮事項

- カタログを選択する際、リストには、少なくとも1つの未使用マシンがあるカタログのみが表示されます。
- 1つのカタログは、複数のデリバリーグループにマシンを提供できます。1つのマシンは、1つのデリバリーグループでのみ使用できます。デリバリーグループにマシンを追加すると、Web Studioはデフォルトで同じカタログを提案します。
- 1つのデリバリーグループは、複数のカタログからマシンを使用できます。ただし、それらのカタログには同じマシンタイプ (マルチセッションOS、シングルセッションOS、または Remote PC Access) が含まれている必要があります。デリバリーグループ内のすべてのマシンは、同じ割り当てタイプ (プール型または静的) である必要があります。つまり、デリバリーグループ内でマシンタイプを混在させることはできません。
- Citrixは、すべてのマシンで最新のVDAバージョンを使用することを推奨します。
- **Remote PC Access**の場合、サイトを作成すると、**Remote PC Access Machines**という名前のカタログと、**Remote PC Access Desktops**という名前のデリバリーグループが自動的に作成されます。**Remote PC Access Machines**カタログ内の各マシンは、デリバリーグループに自動的に関連付けられます。
- 次の互換性チェックが実行されます。
    - MinimumFunctionalLevelは互換性がある必要があります
    - SessionSupportは互換性がある必要があります
    - AllocationTypeはSingleSessionと互換性がある必要があります
    - Remote PC Access は Remote PC Access カタログとのみ互換性があります。

マシンの割り当てページ

「**マシン**」ページで選択されたシングルセッションOS静的マシンカタログに、割り当て済みの利用可能なマシンがある場合、「**マシン割り当て**」ページが利用可能です。

このページを使用して、このデリバリーグループ内のマシンについて、ユーザーの割り当てとデスクトップの表示名を管理します。

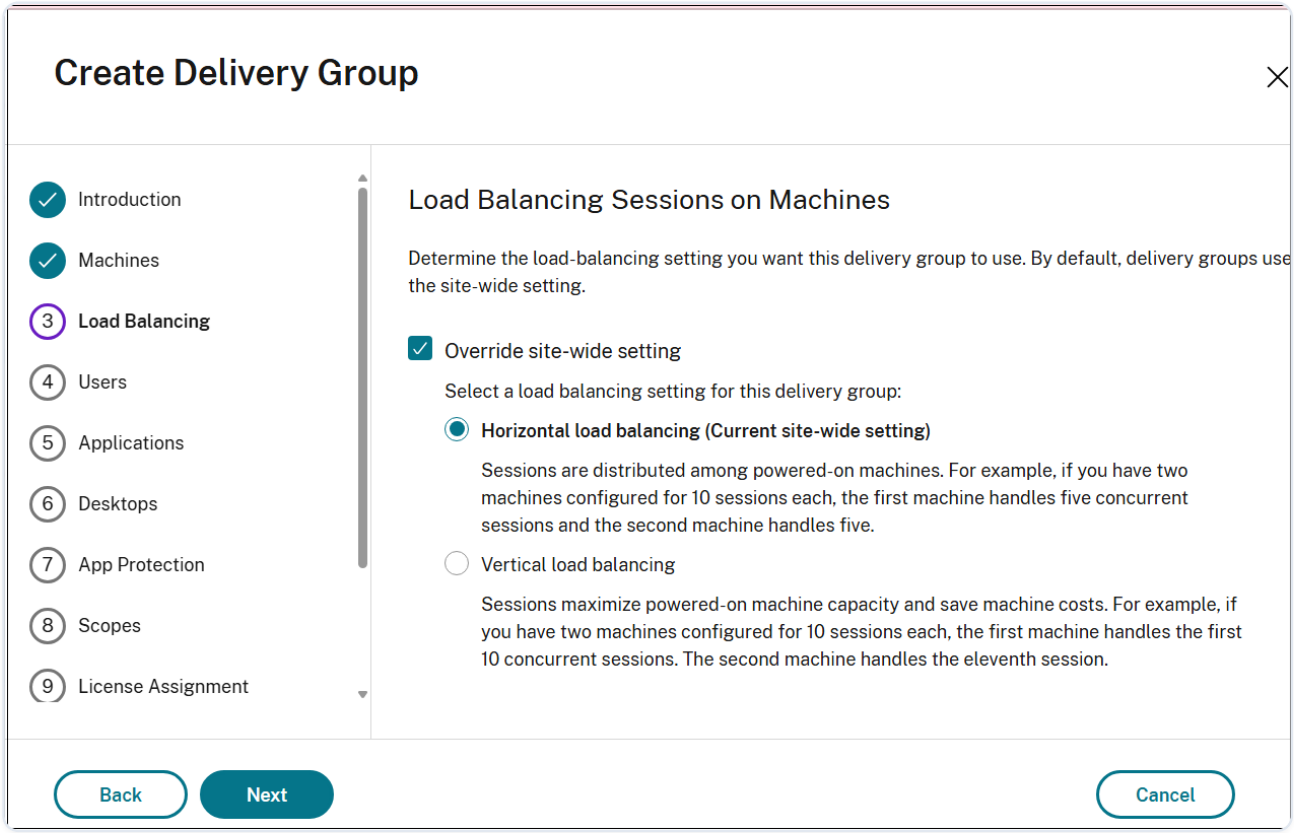
- デスクトップ表示名を管理するには、**表示名**フィールドを使用します。
- **参照**をクリックして、ユーザーまたはグループを選択します。

負荷分散ページ

マシンの負荷分散セッションページは、マルチセッションOSマシンで利用できます。

このページを使用して、このデリバリーグループで使用する負荷分散設定を構成します。デフォルトでは、デリバリーグループはサイト全体の負荷分散設定を使用します。

1. このデリバリーグループの負荷分散設定を構成するには、**サイト全体の設定を上書き**チェックボックスを選択します。
2. 必要に応じて、**水平負荷分散**または**垂直負荷分散**オプションを選択します。水平負荷分散と垂直負荷分散の方法については、マシンの負荷分散を参照してください。



垂直負荷分散を選択する場合は、同時ログオン許容数および最大セッション数ポリシーが適切に構成されていることを確認してください。

配信の種類ページ

「**配信の種類**」ページは、シングルセッションOS静的（割り当て済み）マシンにのみ表示されます。

このページを使用して、カタログ内のマシンを構成し、ユーザーにデスクトップまたはアプリケーションを配信します。

1. **アプリケーション**または**デスクトップ**のいずれかを選択します。両方を有効にすることはできません。

> **注:**
>
> マルチセッションOSまたはシングルセッションOSのランダム（プールされた）カタログからマシンを選択した場合、配信タイプはアプリケーションとデスクトップであると見なされます。アプリケーション、デスクトップ、またはその両方を配信できます。

ユーザーページ

ユーザーページはすべてのマシンタイプで利用できます。ただし、ページ上のオプションはマシンタイプによって異なります。

このページを使用して、ユーザーがデリバリーグループ内のリソースにアクセスする方法を指定します。

ユーザーアクセス制御の仕組み

デリバリーグループでのユーザーアクセスは、アクセス設定を作成または編集する際に指定されたユーザーリストを通じて制御されます。

- 以下の条件を *すべて* 満たすユーザーは、デリバリーグループ内の**アプリケーション**にアクセスできます。
  - このデリバリーグループ内のリソース（アプリとデスクトップ）へのアクセス権を持っていること。デフォルトでは、アクセスは展開のユーザーアクセスリスト（Active Directory内のユーザー）によって決定され、これはStudioでは構成されません。デリバリーグループ内のユーザーの追加または削除を参照してください。
  - このグループ内のアプリケーションへのアクセス権を持っていること。デフォルトでは、アプリケーションエンタイトルメントポリシー規則にはすべてのユーザーが含まれます。詳細については、PowerShell SDK `BrokerAppEntitlementPolicyRule` コマンドレットを参照してください。
  - このアプリケーションを含むアプリケーショングループにアクセスできる。
- 以下の *両方* の条件を満たすユーザーは、デリバリーグループ内のデスクトップにアクセスできます。
  - このデリバリーグループ内のリソース（アプリとデスクトップ）にアクセスできる。デフォルトでは、アクセスは展開のユーザーアクセスリスト（Active Directoryのユーザー）によって決定され、これはStudioでは構成されません。デフォルトのユーザー範囲から

ユーザーを追加または削除できます。「デリバリーグループでのユーザーの追加または削除」を参照してください。

- このグループ内のデスクトップにアクセスできる。詳細については、「デスクトップ（またはデスクトップ割り当てルールページ）」を参照してください。

構成手順

1. デリバリーグループ内のリソースの使用を許可または制限するオプションのいずれかを選択します。

   - **認証済みユーザーがリソースを使用することを許可する:** アプリケーションとデスクトップにアクセスするには、指定したユーザーとグループメンバーが、スマートカードやユーザー名とパスワードなどの資格情報をStoreFront™またはCitrix Workspace™アプリに提示する必要があります。（シングルセッションOSマシンを含むデリバリーグループの場合、後でデリバリーグループを編集してユーザーデータ（ユーザーのリスト）をインポートできます。）
   - **リソースの使用を制限する:** または、ユーザーまたはユーザーグループを**許可リスト**に追加することで、デリバリーグループの使用を制限できます。**許可リスト**のユーザーのみが、デリバリーグループ内のアプリとデスクトップにアクセスできます。**ブロックリストの追加**をクリックして、ユーザーとユーザーグループをブロックリストに追加することもできます。これにより、ユーザーは選択したデリバリーグループ内のアプリとデスクトップを使用できなくなります。ブロックリストは、許可リスト内のユーザーをブロックする場合にのみ意味があります。

2. マルチセッションOSマシンの場合、ユーザーがStoreFrontまたはCitrix Workspaceアプリに資格情報を提示せずにアプリケーションとデスクトップにアクセスできるようにするには、**認証されていない（匿名）ユーザーへのアクセスを許可する。資格情報は不要**を選択します。たとえば、キオスクではアプリケーションに資格情報が必要な場合がありますが、Citrixアクセスポータルとツールには必要ありません。

   - 認証されていないユーザーアカウントは、セッションが起動されるとオンデマンドで作成され、AnonXYZという名前が付けられます。XYZは一意の3桁の値です。
   - 認証されていないユーザーセッションのアイドルタイムアウトはデフォルトで10分であり、クライアントが切断されると自動的にログオフされます。再接続、クライアント間のローミング、およびWorkspace Controlはサポートされていません。

3. ユーザーのホームゾーンに十分なリソースがある場合に、セッションが他の利用可能なゾーンにデフォルトで設定されるのを防ぐには、**セッションをユーザーのホームゾーンで起動することを要求する（構成されている場合）**を選択します。

4. デバイスや現在のセッションの有無にかかわらず、セッションを追跡させたい場合は、**ユーザーとともにクライアントデバイス間でセッションローミングを許可する**を選択します。「セッションローミング」を参照してください。

次の表は、**ユーザー**ページでの選択肢について説明しています。

アクセスを有効にする対象	ユーザーとユーザーグループを追加/割り当てますか？	「認証されていないユーザーにアクセスを許可する」チェックボックスを有効にしますか？
認証済みユーザーのみ	はい	いいえ
認証されていないユーザーのみ	いいえ	はい
認証済みユーザーと未認証ユーザーの両方	はい	はい

アプリケーションページ

「**アプリケーション**」ページは、すべてのマシンタイプで利用できます。ただし、追加できるアプリケーションは、マシンタイプによって異なります。

このページを使用して、このグループのデスクトップにパッケージ化されたアプリケーションを追加できます。

重要な考慮事項

- パッケージ化されたアプリケーションをデリバリーグループに追加できます。これらのアプリケーションを含むパッケージは、ユーザーがデスクトップまたはリモートPCにサインインするたびに自動的にマウントされます。
- デフォルトでは、追加する新しいアプリケーションは「Applications」という名前のフォルダーに配置されます。別のフォルダーを指定することもできます。詳細については、アプリケーションの記事を参照してください。
- アプリケーションをデリバリーグループに追加するとき、または後で、そのアプリケーションのプロパティを変更できます。詳細については、アプリケーションの記事を参照してください。
- アプリケーションを追加しようとしたときに、同じ名前のアプリケーションがそのフォルダーに存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。拒否した場合、アプリケーションはそのアプリケーションフォルダー内で一意になるようにサフィックスを付けて追加されます。

- 複数のデリバリーグループにアプリケーションを追加する場合、すべてのデリバリーグループでそのアプリケーションを表示する権限がないと、表示の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが追加されたすべてのデリバリーグループを含むようにスコープを拡張してください。
- 同じ名前の2つのアプリケーションを同じユーザーに公開する場合、アプリケーション名（ユーザー向け）プロパティを変更してください。そうしないと、ユーザーはCitrix Workspaceアプリで重複した名前を目にすることになります。

構成手順

1. アプリケーションソースを表示するには、**追加**メニューを選択します。

    - **スタートメニューから:** デリバリーグループに割り当てられている、現在登録されているVDAのいずれかを介してアプリケーションが検出されます。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。追加したいアプリケーションを選択し、**OK**を選択します。
    - **手動で:** デリバリーグループ内のVDAまたはネットワーク上の別の場所にあるアプリケーション。このソースを選択すると、新しいページが開き、次の方法で追加するアプリケーションを指定できます。

        - 実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、および管理者とユーザー向けの表示名を入力します。
        - デリバリーグループ内のVDAからアプリケーションを選択します。これを行うには、**参照**をクリックし、VDAにアクセスするための資格情報を入力し、VDAへの接続を待ってから、VDAからアプリケーションを選択します。選択したアプリケーションのプロパティは、ページ上のフィールドに自動的に入力されます。

    - **既存:** 以前に展開に追加されたアプリケーション（おそらく別のデリバリーグループ内）。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。追加したいアプリケーションを選択し、**OK**を選択します。
    - **アプリケーションパッケージ:** App-V、MSIX、MSIX app attach、またはFlexAppアプリケーションパッケージ内のアプリケーション。このソースを選択すると、**パッケージからアプリケーションを追加**ページが起動します。アプリケーションパッケージソースを選択し、表示されたリストから追加したいアプリケーションを選択し、**OK**を選択します。

    > **注:**

> ◦ このオプションは、サイトにアプリケーションパッケージが構成されていない場合、グレー表示されます。

> \> - MSIXまたはMSIXアプリ添付アプリを公開するには、デリバリーグループの機能レベルが2106以降である必要があります。FlexAppアプリの場合、機能レベルは2206以降である必要があります。機能レベルの要件が満たされていない場合、**Application package source**ドロップダウンリストの対応するオプションはグレー表示されます。

- **アプリケーショングループ:** 展開内に存在するアプリケーショングループ。

アプリケーションソースまたはアプリケーションが利用できないか無効な場合、それは表示されないか、選択できません。たとえば、展開にアプリケーションが追加されていない場合、**既存**ソースは利用できません。または、アプリケーションが選択されたマシンカタログ内のマシンのサポートされているセッションタイプと互換性がない場合があります。

デスクトップ（またはデスクトップ割り当てルール）ページ

このページのタイトルは、ウィザードで以前に選択したマシンカタログによって異なります。

- マルチセッションまたはプールされたシングルセッションマシンを含むカタログを選択した場合、このページは**デスクトップ**というタイトルになります。
- シングルセッションの静的マシンを含むカタログを選択し、**配信タイプ**ページで「デスクトップ」を指定した場合、このページは**デスクトップ割り当てルール**というタイトルになります。

> **注:**
>
> シングルセッションの静的マシンを含むカタログを選択し、**配信タイプ**ページで「アプリケーション」を指定した場合、このページは表示されません。

1. （オプション）デリバリーグループのデフォルトのデスクトップアイコンを更新するには、**変更**を選択します。このアイコンは、個々のデスクトップに別のアイコンが設定されていない限り、グループ内のすべてのデスクトップに適用されます。
2. **追加**を選択します。ダイアログボックスで、:

   a. **表示名**と**説明**のフィールドに、Citrix Workspaceアプリに表示する情報を入力します。

b. マルチセッションまたはプールされたシングルセッションOSマシンについて：デスクトップにタグ制限を追加するには、**このタグを持つマシンへの起動を制限する**を選択し、メニューからタグを選択します。

c. ラジオボタンを使用して、次のいずれかを実行できます。

   i. **このデリバリーグループにアクセスできるすべてのユーザーにデスクトップの使用を許可する。** デリバリーグループ内のすべてのユーザーは、デスクトップを起動できます（プールされたマシンを持つグループの場合）。または、デスクトップを起動したときにマシンを割り当てられます（シングルセッションの静的マシンを持つグループの場合）。

   ii. **デスクトップの使用を制限する**には、ユーザーとユーザーグループを「**許可リスト**」に追加します。「**許可リスト**」のユーザーのみがデスクトップにアクセスできます。「**ブロックリストの追加**」をクリックして、ユーザーとユーザーグループをブロックリストに追加することもできます。これにより、選択したデリバリーグループ内のデスクトップをユーザーが使用できなくなります。ブロックリストは、許可リスト内のユーザーをブロックする場合にのみ意味があります。

d. グループにシングルセッションの静的マシンが含まれている場合は、ユーザーあたりのデスクトップの最大数を指定します。これは1以上の値である必要があります。この設定は必須ではありません。マシンを手動で割り当てることも、RemotePCを使用してマシンを自動的に割り当てることもできます。

e. （オプション）「**変更**」を選択して、プールされたデスクトップのデスクトップアイコン、またはシングルセッションの静的デスクトップのデスクトップ割り当てルールを更新します。指定されたアイコンは、デリバリーグループレベルで設定されたデフォルトのアイコンを上書きします。

f. デスクトップ（マルチセッションマシン用）またはデスクトップ割り当てルール（シングルセッション静的マシン用）を有効または無効にします。デスクトップを無効にすると、デスクトップの配信が停止します。デスクトップ割り当てルールを無効にすると、ユーザーへのデスクトップの自動割り当てが停止します。

g. ダイアログボックスでの作業が完了したら、**OK**を選択します。

サイト内のデスクトップの最大インスタンス数（PowerShellのみ）

サイト内のデスクトップの最大インスタンス数を構成するには（PowerShellのみ）：

- PowerShellで、適切なBrokerEntitlementPolicyRuleコマンドレットをMaxPerEntitlementInstancesパラメーターとともに使用します。たとえば、次のコマンドレットは、`tsvda-desktop` ルールを変更して、サイトで許可されるデスクトップの同時インスタ

ンスの最大数を2に設定します。2つのデスクトップインスタンスが実行されているときに、3番目のサブスクライバーがデスクトップを起動しようとすると、エラーが発生します。

```
Set-BrokerEntitlementPolicyRule -Name tsvda-desktop
-MaxPerEntitlementInstances 2
```

- ガイダンスについては、Get-Helpコマンドレットを使用してください。例：`Get-Help Set-BrokerEntitlementPolicyRule-Parameter MaxPerEntitlementInstances`。

アプリ保護ページ

アプリ保護ページは、すべてのマシンタイプで利用できます。

このページを使用して、Citrix公開アプリケーションとデスクトップのセキュリティを強化できます。

次の情報は、Citrix Virtual Apps and Desktopsドキュメントのアプリ保護 記事を補足するものです。

- 有効なアプリ保護エンタイトルメントが必要です。アプリ保護機能を購入するには、Citrixの営業担当者にお問い合わせください。
- アプリ保護にはXML信頼が必要です。XML信頼を有効にするには、**設定 > XML信頼を有効にする** に移動します。

保護は以下の条件で適用されます。

- **画面キャプチャ防止**：
  - WindowsおよびmacOSでは、保護されたコンテンツのウィンドウのみが空白になります。保護されたウィンドウが最小化されていない場合、アプリ保護はアクティブになります。
  - Linuxでは、キャプチャ全体が空白になります。保護されたウィンドウが最小化されているかどうかにかかわらず、アプリ保護はアクティブになります。
- **キーロギング防止**：保護されたウィンドウがフォーカスされている場合に有効になります。保護を無効にするには、別のウィンドウにフォーカスを変更します。

スコープページ

スコープページは、すべてのマシンタイプで利用できます。

このページを使用して、組織に関連する方法でオブジェクト（例: 接続、カタログ、デリバリーグループ）をグループ化します。

ライセンス割り当てページ

ライセンス割り当てページは、すべてのマシンタイプで利用できます。

このページを使用して、デリバリーグループで使用するライセンスを指定します。デフォルトでは、デリバリーグループはサイトライセンスを使用します。詳細については、マルチタイプライセンスを参照してください。

ポリシーセットページ

ポリシーセットページは、すべてのマシンタイプで利用できます。

このページを使用して、このデリバリーグループが使用するポリシーセットを指定します。

ローカルホストキャッシュ設定ページ

このページは、電源管理されたシングルセッションのプールされたマシンを含むデリバリーグループでのみ利用できます。

デフォルトでは、電源管理されたプールされたマシンは、データ漏洩のリスクがあるため、ローカルホストキャッシュ (LHC) モードでは利用できません。このデフォルトの動作を変更し、LHCモードで新しいユーザー接続に利用できるようにするには、**リソースを常に利用可能にする**を選択します。

または、PowerShell コマンドを使用してデフォルトの動作を変更することもできます。詳細については、「アプリケーションとデスクトップのサポート」を参照してください。

> **重要:**
>
> 電源管理されたシングルセッションのプールされたマシンへのアクセスを有効にすると、以前のユーザーセッションのデータや変更が後続のセッションに存在してしまう可能性があります。

ローカルホストキャッシュでの1回限りの使用のプールされたデスクトップ

ローカルホストキャッシュ (LHC) の停止中、プールされたデスクトップは1回限り使用できます。これは、対応可能なVDAにハイジーンブロブを発行し、再起動を開始することで実現されます。このプロセスにより、停止からの復旧時にデスクトップのクリーンな状態が保証されます。対応できないマシンやレガシーマシンでは、再利用が明示的に有効になっている場合にのみ参加します。この機能は、停止時の可用性をよりシームレスにすることで、顧客満足度を向上させます。

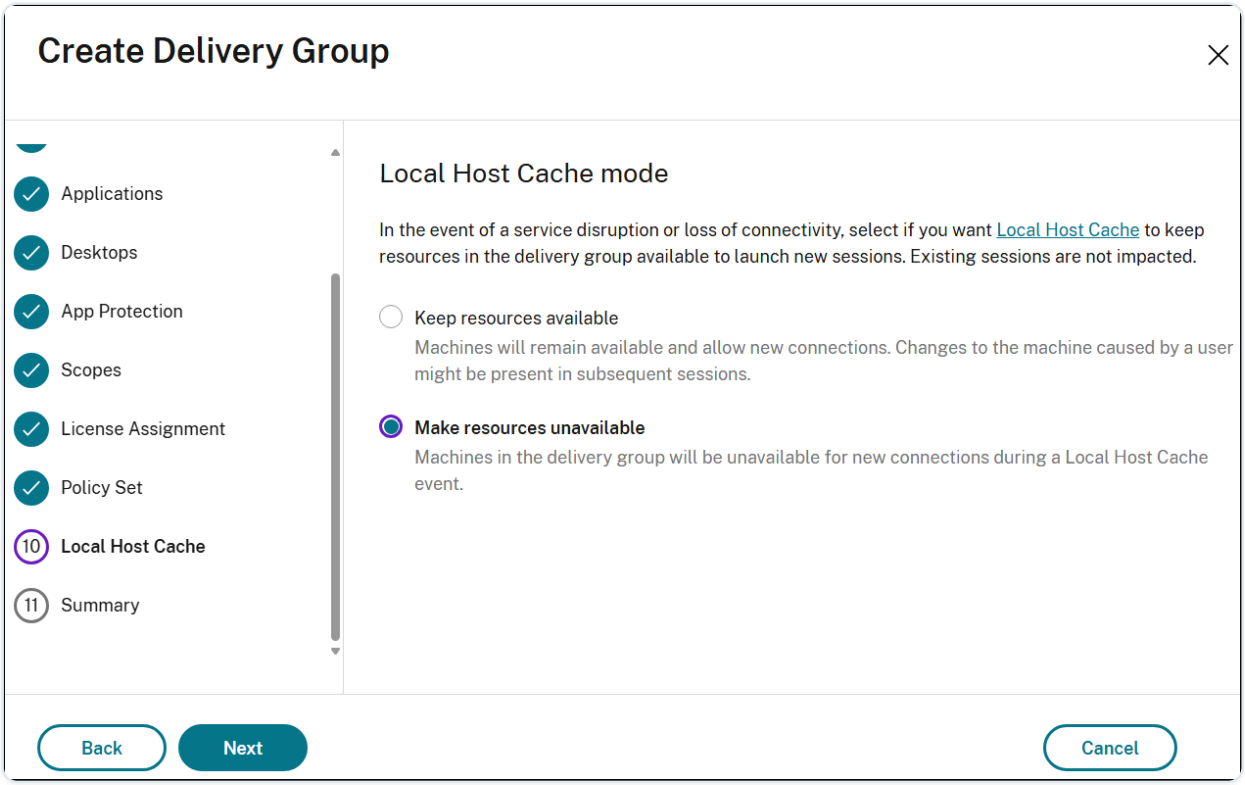
前提条件

- 完全なハイジーン適用にはVDAバージョン2407以降が必要です。レガシーVDA（VDAバージョン2407以前）は、再利用が有効になっている場合にのみ使用できます。これらのVDAは、ハイジーンブロブや強制再起動を受け取りません。
- シングルセッションマシンを含むマシンカタログ。

プールされたデスクトップの1回限りの使用を構成する

1. VDAビルド2407以降を使用して、シングルセッションマシンを含むMCSカタログを作成します。
2. 対応するデリバリーグループを作成します。Remote PowerShell からデリバリーグループの `ReuseMachinesWithoutShutdownInOutage` デスクトップグループ設定を `false` に設定するか、デリバリーグループの作成時に Web Studio の **ローカルホストキャッシュモード** ページで **リソースを利用不可にする** を選択します。

```
Set-BrokerDesktopGroup -Name "name"
-ReuseMachinesWithoutShutdownInOutage $false
```



3. 構成が完了すると、LHC停止モード中にマシンは1回限りの使用が可能になります。LHC停止モードが解除されると、汚染されたマシンは再起動され、再度使用できるようになります。

> **注:**

> マシンは、最新の電源投入後にユーザーセッションが開始されると、汚染済みとして分類されます。汚染されていないマシンとは、最新の電源投入イベント以降、ユーザーセッションが起動されていないマシンを指します。

概要ページ

デリバリーグループの名前を入力します。オプションで、Citrix WorkspaceアプリとStudioに表示される説明を入力することもできます。

概要情報を確認し、**「完了」**をクリックします。

制限事項

デスクトップをクライアント IP アドレスに割り当てる機能は、非常に限られたクライアントの種類と構成でのみ機能します。クライアント IP アドレスに基づいてアクセスフィルタリングを実行すると、クラウドクライアントにはパブリック IP アドレスが使用されます。

マージグループを使用したカナリアデプロイメントの有効化（プレビュー）

マージグループを使用して、アプリケーションおよびデスクトップリソースのカナリアデプロイメントモデルを実装します。この機能を使用すると、同じリソースの複数のバージョンを公開しながら、エンドユーザーには単一のアイコンとして表示できます。

マージグループを使用すると、特定のユーザーグループを同じリソースの異なる実装バージョンに誘導できます。ユーザーの一部（5%など）を新しいバージョンのテストに指定し、残りのユーザーは安定版を使用させることができます。新しいバージョンで問題が発生した場合でも、ユーザーのエクスペリエンスを中断することなく、簡単に安定版にフェールオーバーできます。この機能は、再列挙や構成変更を必要とせずに、高可用性と災害復旧の両方のシナリオをサポートします。

使用例

アプリケーションの異なるバージョンが利用可能な場合にユーザーエクスペリエンスを合理化するには、マージグループ機能の使用を検討してください。たとえば、Microsoft Word 2016とMicrosoft Word 2019がある場合、2つの別々のアイコンを表示する代わりに、それらを1つのアイコンにグループ化します。マージグループ機能を使用すると、システムは特定のユーザーに対してどのバージョンのアプリケーション（たとえば、Word 2016またはWord 2019）を起動するかを決定できます。

制限事項

マージグループ内のユーザーが優先するリソースが一時的に利用できない場合（例：メンテナンスモード中）、ブローカーはフォールバックリソースでセッションを起動します。ユーザーが再接続する前に優先リソースが再び利用可能になった場合、ブローカーはフォールバックリソース上の既存のセッションに再接続するのではなく、優先リソースで新しいセッションを作成します。

影響：ユーザーは各リソースで1つずつ、2つのアクティブなセッションを持つことになりますが、優先リソース上のセッションにのみアクセスできます。フォールバックリソース上の切断されたセッションはアクセス不能になります。

回避策：管理者はStudioから孤立したセッションをログオフするか、それをホストしているマシンを再起動できます。

マージグループを構成するコマンド

> **注：**
>
> 詳細なコマンドの説明については、SDKドキュメントを参照してください。

アクション	コマンド	説明
マージグループの作成	`New-BrokerMergeGroup`	指定された名前と説明（オプション）でマージグループを作成します。
マージグループの設定	`Set-BrokerMergeGroup`	マージグループの名前、説明、MergeGroupSetUid、およびDefaultResourceUidを設定します。DefaultResourceはマージグループのアイコンリソースです。Citrix Workspaceアプリでは、マージグループはこのリソースのアイコンを継承します。
マージグループの削除	`Remove-BrokerMergeGroup`	指定されたマージグループを削除します。マージグループにマージ済みリソー

アクション	コマンド	説明
		スが含まれている場合、削除は失敗します。そのようなマージグループを削除するには、`Force` パラメーターが必要です。これにより、マージグループとその関連する `MergedResources` の両方がマージグループ内で削除されます。
マージ済みリソースの作成	`New-BrokerMergedResource`	サイトに新しいマージ済みリソースを作成します。applicationUid または EntitlementPolicyRuleUid (共有/ランダムデスクトップグループ) を持つマージ済みリソースを作成します。これは、アプリケーションリソースまたはエンタイトルメントポリシー規則の単なるラッパーでもあります。マージ済みリソースを削除しても、アプリケーションまたはエンタイトルメントポリシー規則は削除されません。
マージ済みリソースの設定	`Set-BrokerMergedResource`	`MergedResource` オブジェクトのプロパティを設定します。Users パラメーターは、マージ済みリソースに関連付けられている以前のユーザーをすべて削除し、新しいリスト (または単一のユーザー) をこのマージ済みリソースのユーザーリストとして設定します。既存のユーザーリストにユーザーを追加したい場

アクション	コマンド	説明
		合は、`AddUsers` パラメーターを使用できます。既存のユーザーリストからユーザーを削除したい場合は、`RemoveUsers` パラメーターを使用できます。
マージ済みリソースの削除	`Remove-BrokerMergedResource`	指定されたマージ済みリソースを削除します。

詳細情報

- デリバリーグループの管理
- アプリケーション

デリバリーグループの管理

> **注:**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

この記事では、管理コンソールからデリバリーグループを管理する手順について説明します。グループ作成時に指定した設定を変更するだけでなく、デリバリーグループの作成時には利用できないその他の設定も構成できます。

手順のカテゴリには、全般、ユーザー、マシン、セッションが含まれます。一部のタスクは複数のカテゴリにまたがります。たとえば、「ユーザーがマシンに接続するのを防ぐ」はマシンのカテゴリで説明されていますが、ユーザーにも影響します。あるカテゴリでタスクが見つからない場合は、関連するカテゴリを確認してください。

その他の関連情報を含む記事：

- アプリケーションには、デリバリーグループ内のアプリケーションの管理に関する情報が含まれています。
- デリバリーグループの管理には、Delivery Group Administratorの組み込みロール権限が必要です。詳細については、委任管理を参照してください。

全般

- グループの詳細を表示
- 優先プロパティを変更
- デリバリーの種類を変更
- StoreFront™アドレスを変更
- 機能レベルを変更
- リモートPCアクセスデリバリーグループを管理する
- フォルダーを使用してデリバリーグループを整理する
- アプリ保護を管理する
- デリバリーグループの一時停止機能を変更する

グループの詳細を表示

1. 検索機能を使用して特定のデリバリーグループを見つけます。手順については、インスタンスの検索を参照してください。
2. 検索結果から、必要に応じてグループを選択します。
3. グループの列の説明については、次の表を参照してください。
4. このグループに関する詳細情報については、下部の詳細ペインにあるタブをクリックします。

列	説明
デリバリーグループ	グループ名とセッションの種類。セッションの種類には、シングルセッションOSとマルチセッションOSがあります。
配信	このグループから配信されるリソースの種類。指定できる値には、アプリケーション、デスクトップ、およびアプリケーションとデスクトップがあります。デリバリーグループが専用マシンで構成されている場合、「静的マシン割り当て」と表示されます。

列	説明
使用中のセッション	セットアップされているマシンの数と、切断状態のマシンの数。
割り当て済み数	デリバリーグループに割り当てられているカタログ内のマシンの数。
フォルダー	**デリバリーグループ**ツリー内でのグループの場所。グループが存在するフォルダーの名前（末尾のバックスラッシュを含む）が表示されます。グループがルートレベルにある場合は `-` と表示されます。

優先プロパティの変更

優先プロパティは、ユーザーがデリバリーグループからリソースにアクセスして起動する方法を制御します。デリバリーグループの優先プロパティを変更するには、次の手順に従います。

1. Studioで、左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**を選択します。
3. **基本設定**ページで、次の表の設定を変更します。
4. 加えた変更を適用してウィンドウを開いたままにするには、**適用**を選択します。または、変更を適用してウィンドウを閉じるには、**OK**を選択します。

設定	説明
説明	Citrix Workspace™（またはStoreFront）が使用し、ユーザーに表示されるテキスト。
デリバリーグループを有効にする	デリバリーグループが有効になっているかどうか。
タイムゾーン	このデリバリーグループのマシンが存在するタイムゾーン。この設定は、新しく作成されたデリバリーグループの**設定 > 日付と時刻**で設定されたタイムゾーンを自動的に表示します。必要に応じて、デリバリーグループに別のタイ

設定	説明	
	ムゾーンを選択できます。ドロップダウンメニューには、サイトでサポートされているタイムゾーンが一覧表示されます。 **注：** デリバリーグループのタイムゾーンを変更すると、そのデリバリーグループ内のマシンが再起動する可能性があります。これを避けるため、タイムゾーン設定は稼働時間外に変更してください。	
Secure ICA® を有効にする	ICAプロトコルを暗号化するSecureICAを使用して、デリバリーグループ内のマシンとの通信を保護します。デフォルトのレベルは128ビットです。レベルはSDKを使用して変更できます。Citrix®は、パブリックネットワークを通過する際にTLS暗号化などのより多くの暗号化方法を使用することを推奨します。また、SecureICAはデータ整合性をチェックしません。	

デリバリーグループのデリバリーの種類を変更する

デリバリーの種類は、グループが提供できるもの（アプリケーション、デスクトップ、またはその両方）を示します。

アプリケーションのみまたは**デスクトップとアプリケーション**のタイプを**デスクトップのみ**のタイプに変更する前に、グループからすべてのアプリケーションを削除してください。

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. **デリバリータイプ**ページで、目的のデリバリータイプを選択します。

4. 加えた変更を適用してウィンドウを開いたままにするには、「**適用**」をクリックします。または、変更を適用してウィンドウを閉じるには、「**保存**」をクリックします。

StoreFrontアドレスの変更

1. 左ペインで「**デリバリーグループ**」を選択します。
2. グループを選択し、アクションバーで「**編集**」をクリックします。
3. 「**StoreFront**」ページで、StoreFront URLを選択または追加します。これらのURLは、デリバリーグループ内の各マシンにインストールされているCitrix Workspace™アプリによって使用されます。
4. 加えた変更を適用してウィンドウを開いたままにするには、「**適用**」をクリックします。または、変更を適用してウィンドウを閉じるには、「**保存**」をクリックします。

左側のペインで**［StoreFront］**を選択して、StoreFrontサーバーアドレスを指定することもできます。

機能レベルの変更

デリバリーグループの機能レベルは、そのマシン上のVDAと、デリバリーグループで使用されているマシンを含むマシンカタログをアップグレードした後に変更します。

開始する前に:

- Citrix Provisioning™（旧Provisioning Services）を使用している場合は、Citrix Provisioningコンソールで VDAバージョンをアップグレードします。
- アップグレードされたVDAを含むマシンを起動し、Delivery Controllerに登録できるようにします。このプロセスにより、デリバリーグループでアップグレードが必要なものがコンソールに通知されます。
- 以前のVDAバージョンを引き続き使用する必要がある場合、新しい製品機能は利用できません。詳細については、アップグレードドキュメントを参照してください。

デリバリーグループの機能レベルを変更するには：

1. 左側のペインで、**［デリバリーグループ］**を選択します。
2. グループを選択し、アクションバーの**機能レベルの変更**をクリックします。**機能レベルの変更**アクションは、アップグレードされたVDAが検出された場合にのみ表示されます。
3. **変更**をクリックします。

ディスプレイには、どのマシンが機能レベルに変更できないか、およびその理由が表示されます。その後、変更アクションをキャンセルし、マシンの問題を解決してから、変更アクションを再度実行できます。

変更が完了したら、マシンを以前の状態に戻すことができます。デリバリーグループを選択し、アクションバーで**機能レベルの変更を元に戻す**を選択します。

Remote PC Accessデリバリーグループの管理

Remote PC Accessマシンカタログ内のマシンが割り当てられていない場合、そのマシンは、そのカタログに関連付けられたデリバリーグループに一時的に割り当てられます。この一時的な割り当てにより、後でマシンをユーザーに割り当てることができます。

デリバリーグループとマシンカタログの関連付けには優先度値があります。優先度は、マシンがシステムに登録されるとき、またはユーザーがマシン割り当てを必要とするときに、マシンに割り当てられるデリバリーグループを決定します。値が小さいほど優先度が高くなります。Remote PC Accessマシンカタログに複数のデリバリーグループ割り当てがある場合、ソフトウェアは最も優先度の高い一致を選択します。この優先度値を設定するには、PowerShell SDKを使用します。

Remote PC Accessマシンカタログは、最初に作成されたときにデリバリーグループに関連付けられます。後でカタログに追加されたマシンアカウントまたは組織単位は、デリバリーグループに追加できます。この関連付けは、オフまたはオンに切り替えることができます。

デリバリーグループとのRemote PC Accessマシンカタログの関連付けを追加または削除するには：

1. 左側のペインで**デリバリーグループ**を選択します。
2. Remote PC Accessグループを選択します。
3. **詳細**セクションで、**マシンカタログ**タブをクリックし、Remote PC Accessカタログを選択します。
4. 関連付けを追加または復元するには、**デスクトップの追加**をクリックします。関連付けを削除するには、**関連付けの削除**をクリックします。

フォルダーを使用してデリバリーグループを整理する

フォルダーを作成して、デリバリーグループを整理し、簡単にアクセスできるようにすることができます。

> **ヒント:**

> アクションバーの右上にある**フォルダー**アイコンをクリックすると、Delivery Groupsノードのデフォルトビュー（フォルダービューまたはリストビュー）を設定できます。

必要な役割

デフォルトでは、デリバリーグループフォルダーを作成および管理するには、Cloud Administrator、Full Administrator、またはDelivery Group Administratorの組み込み役割が必要です。必要に応じて、デリバリーグループフォルダーの作成と管理のための役割をカスタマイズできます。詳しくは、「必要な権限」を参照してください。

デリバリーグループフォルダーを作成する

開始する前に、デリバリーグループの整理方法を計画してください。次の点を考慮してください。

- フォルダーは最大5レベルまでネストできます（デフォルトのルートフォルダーを除く）。
- フォルダーには、デリバリーグループとサブフォルダーを含めることができます。
- Web Studioのすべてのノード（**Machine Catalogs**、**Delivery Groups**、**Applications**、**Application Groups**など）は、バックエンドで同じフォルダーツリーを共有します。フォルダーの名前変更や移動時に名前の競合を避けるため、異なるノード間で最上位フォルダーに一意の名前を使用してください。

  `New-BrokerAdminFolder` SDKコマンドレットを使用してフォルダーを作成し、それを**Delivery Groups**ノードの下に表示させたい場合は、`Set-BrokerAdminFolderMetadata`コマンドレットを使用して`ContainsDeliveryGroups`メタデータを追加する必要があります。

  例:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsDeliveryGroups -Value true
  ```

デリバリーグループフォルダーを作成するには、次の手順に従います。

1. 左ペインで**Delivery Groups**を選択します。
2. フォルダー階層でフォルダーを選択し、**アクション**バーで**Create Folder**を選択します。
3. 新しいフォルダーの名前を入力し、**Done**をクリックします。

> **ヒント:**
>
> 意図しない場所にフォルダーを作成した場合でも、正しい場所にドラッグできます。

デリバリーグループを移動する

デリバリーグループはフォルダー間で移動できます。詳細な手順は次のとおりです。

1. 左ペインで を選択します。
2. フォルダー別にグループを表示します。フォルダー階層の上にある をオンにして、すべてのグループを一度に表示することもできます。
3. グループを右クリックし、 を選択します。
4. グループの移動先のフォルダーを選択し、 をクリックします。

> **ヒント:**
>
> グループをフォルダーにドラッグできます。

デリバリーグループフォルダーの管理

デリバリーグループフォルダーの削除、名前の変更、移動が可能です。

フォルダーとそのサブフォルダーにデリバリーグループが含まれていない場合にのみ、フォルダーを削除できることに注意してください。

フォルダーを管理するには、次の手順に従います。

1. 左ペインで を選択します。
2. フォルダー階層でフォルダーを選択し、必要に応じて**アクション**バーでアクションを選択します。
   - フォルダーの名前を変更するには、**「フォルダー名の変更」**を選択します。
   - フォルダーを削除するには、**「フォルダーの削除」**を選択します。
   - フォルダーを移動するには、**「フォルダーの移動」**を選択します。
3. 画面の指示に従って、残りの手順を完了してください。

必要な権限

次の表に、デリバリーグループフォルダーに対してアクションを実行するために必要な権限を示します。

アクション	必要な権限
デリバリーグループフォルダーの作成	デリバリーグループフォルダーを作成
デリバリーグループフォルダーを削除	デリバリーグループフォルダーを削除
デリバリーグループフォルダーを移動	デリバリーグループフォルダーを移動
デリバリーグループフォルダーの名前を変更	デリバリーグループフォルダーを編集
デリバリーグループをフォルダーに移動	デリバリーグループフォルダーを編集およびデリバリーグループのプロパティを編集

アプリ保護の管理

アプリ保護に関する補足情報です。以下の詳細に注意してください。

- 有効なアプリ保護エンタイトルメントが必要です。アプリ保護機能を購入するには、Citrixの営業担当者にお問い合わせください。
- アプリ保護にはXML信頼が必要です。XML信頼を有効にするには、**設定 > XML信頼を有効にする**に移動します。
- 画面キャプチャ防止について：
  - WindowsおよびmacOSでは、保護されたコンテンツのウィンドウのみが空白になります。保護されたウィンドウが最小化されていない場合、アプリ保護はアクティブになります。
  - Linuxでは、キャプチャ全体が空白になります。保護されたウィンドウが最小化されているかどうかにかかわらず、アプリ保護はアクティブになります。

デリバリーグループのアプリ保護方法を選択するには、次の手順に従います。

1. 左側のペインで **デリバリーグループ** を選択します。
2. グループを選択し、アクションバーで**編集**を選択します。
3. **アプリ保護**ページで、次のオプションを確認できます。

オプション	説明
適用しない	この設定を適用しない場合は、このオプションを選択します。
このデリバリーグループに適用	**Anti-keylogging** および/または **Anti key capturing** オプションを選択します。これら

オプション	説明
	の各設定にカーソルを合わせると、ツールチップに詳細が表示されます。
コンテキストに応じて適用	この設定を適用するには、**アクセス ポリシー設定**ページでアクセス ポリシーを構成します。
	1. 左ペインで をクリックし、 をクリックします。
	1. ページで、次の操作を行います。
	- i. を入力し、必要に応じて設定を構成します。
	- ii. 「**Filter**」フィールドと「**Value**」フィールドに詳細を入力し、「**Done**」をクリックします。新しいポリシーが「**App Protection**」ページに表示されます。このポリシーに必要な設定を有効にします。
	- iii. 「**Save**」をクリックします。

4. 「**デリバリーグループ**」ページで、「**デリバリーグループ**」を選択し、下部にある「**詳細**」タブをクリックします。適用された新しい「**アプリ保護**」設定が表示されます。

デリバリーグループのサスペンド機能を変更する

デリバリーグループのサスペンド機能を必須またはオプションにする：

- **必須** - デリバリーグループには、サスペンド可能なVMのみを含めることができます。
- **オプション** - デリバリーグループには、サスペンド可能なVMとサスペンドできないVMの両方を含めることができます。

始める前に

デリバリーグループ内のすべてのVMがサスペンド可能である場合にのみ、デリバリーグループのサスペンド機能を`Required`に変更できます。

デリバリーグループのサスペンド機能を変更するには：

1. Web Studioから、左ペインの**Delivery Groups**に移動します。

2. グループを選択し、アクションバーの**Change Suspend Capability**をクリックします。
3. 「**Yes**」をクリックして操作を確定します。

ユーザー

このセクションでは、次のトピックについて説明します。

- ユーザーの追加または削除
- デリバリーグループ内のデスクトップおよびアプリへのユーザーアクセスを制限する
- デリバリーグループ内のリソースへのアクセスを制限する
- アクセスポリシーのユーザー範囲を構成する

デリバリーグループでのユーザーの追加または削除

ユーザーに関する詳細については、「ユーザー」を参照してください。

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. ページで：
    - ユーザーを追加するには、**追加**をクリックし、追加するユーザーを指定します。
    - ユーザーを削除するには、1人以上のユーザーを選択し、**削除**をクリックします。
    - 認証されていないユーザーによるアクセスを許可するには、チェックボックスをオンまたはオフにします。
4. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

ユーザーリストのインポートまたはエクスポート

物理的なシングルセッションOSマシンを含むデリバリーグループの場合、デリバリーグループの作成後に.csvファイルからユーザー情報をインポートできます。ユーザー情報を.csvファイルにエクスポートすることもできます。.csvファイルには、以前の製品バージョンのデータを含めることができます。

CSVファイルの最初の行には、コンマで区切られた2つの列ヘッダーが含まれている必要があります。最初のヘッダーが`Machine Account`で、2番目のヘッダーが`User Names`であることを確認してください。（追加のヘッダーを含めることはできますが、サポートされていません。）ファイルの以降の行には、コンマ区切りのデータが含まれます。`Machine Account`のエントリは、コンピューターSID、FQDN、またはドメインとコンピューター名のペアにすることができます。

ユーザー情報をインポートまたはエクスポートするには：

1. 左側のペインで**［デリバリーグループ］**を選択します。
2. グループを選択し、アクションバーで**［編集］**をクリックします。
3. **［マシン割り当て］ページで、［リストのインポート］または［リストのエクスポート］**を選択し、ファイルの場所を参照します。
4. **［適用］をクリックして変更を適用し、ウィンドウを開いたままにします。または、［保存］**をクリックして変更を適用し、ウィンドウを閉じます。

デリバリーグループ内のデスクトップとアプリへのアクセスを制限する

以下のタスクを実行することで、デリバリーグループ内のリソースへのユーザーアクセスを管理できます。

- 特定のユーザーへのデスクトップアクセスを制限する
- 特定のユーザーへのアプリケーションアクセスを制限する

特定のユーザーへのデスクトップアクセスを制限する

以下の*両方*の条件を満たすユーザーは、デリバリーグループ内のデスクトップにアクセスできます。

- このデリバリーグループ内のリソース（アプリとデスクトップ）へのアクセス権を持っている。

  デフォルトでは、アクセスは展開のユーザーアクセスリストによって決定され、これはStudioでは構成されません。デフォルトのユーザー範囲からユーザーを追加または削除できます。デリバリーグループでユーザーを追加または削除するを参照してください。
- このグループ内のデスクトップへのアクセス権を持っている。

  詳細については、「手順 8. デスクトップ (またはデスクトップ割り当てルール)」を参照してください。

特定のユーザーへのデスクトップアクセスを制限するには、「デリバリーグループの作成および編集時にデスクトップの使用を制限する」を参照してください。

特定のユーザーへのアプリケーションアクセスを制限する

次の *すべての*条件を満たすユーザーは、デリバリーグループ内のアプリケーションにアクセスできます。

- このデリバリーグループ内のリソース (アプリとデスクトップ) にアクセスできます。

デフォルトでは、アクセスは展開のユーザーアクセスリストによって決定されますが、これはStudioでは構成されません。デフォルトのユーザー範囲からユーザーを追加または削除できます。デリバリーグループでユーザーを追加または削除するを参照してください。

- このグループ内のアプリケーションにアクセスできます。

  デフォルトでは、アプリケーションエンタイトルメントポリシー規則にはすべてのユーザーが含まれます。詳細については、PowerShell SDK `BrokerAppEntitlementPolicyRule` コマンドレットを参照してください。必要に応じて、このセクションで説明されている手順を使用して、デリバリーグループ内のアプリケーションへのユーザーアクセスを制限できます。

- このアプリケーションを含むアプリケーショングループにアクセスできます。

デリバリーグループレベルで特定のユーザーへのアプリケーションアクセスを制限するには、次の手順に従います。

1. Studioの左ペインで、 を選択します。
2. デリバリーグループを選択し、アクションバーで を選択します。
3. アプリケーションアクセスを制限するには、次の手順に従います。

   a. 左ペインで、 をクリックします。

   b. 特定のユーザーがアプリケーションにアクセスできるようにするには、**アプリケーションの使用を制限**を選択し、**許可リスト**領域で**追加**をクリックして、含めるユーザーまたはユーザーグループを指定します。

   c. 特定のユーザーがアプリケーションにアクセスできないようにするには、**ブロックリスト**領域で**追加**をクリックし、除外するユーザーまたはユーザーグループを指定します。

注:

- **アプリケーションの使用を制限**を選択しても、許可リストとブロックリストの両方を空のままにした場合、このグループのアプリケーションはどのユーザーも使用できません。
- **アプリケーションの使用を制限**を選択し、許可リストを空のままにした場合、**ブロックリスト**のユーザーを除くすべてのユーザーがアプリケーションを使用できます。

デリバリーグループ内のリソースへのアクセスを制限する

デリバリーグループ内のリソースへのユーザーアクセスを制限するために行った変更は、使用する方法に関係なく、以前の設定を上書きします。次のことができます。

- **委任管理スコープを使用して管理者アクセスを制限する：** 管理者がすべてのアプリケーションにアクセスできるスコープと、特定のアプリケーションのみにアクセスできる別のスコープを作成して割り当てることができます。詳しくは、「」(/ja-jp/citrix-virtual-apps-desktops/2511/secure/delegated-administration)を参照してください。
- **スマートアクセス ポリシー式を使用してユーザーアクセスを制限する:** 特定のデリバリーグループへのユーザーアクセスを制御するために、アクセス ポリシー ルールを構成できます。例：
  - ユーザーのサブセットへのアクセスを制限し、許可されたユーザーデバイスを指定します。
  - Workspace（StoreFrontではない）を介して接続しているユーザーへのアクセスを制限します。
  - 特定のWorkspace URLを介して接続しているユーザーへのアクセスを制限します。

このセクションでは、アクセス ポリシー ルールを使用してデリバリーグループへのユーザーアクセスを制限する方法について説明します。

- アクセス ポリシー ルールについて
- アクセス ポリシー ルールを追加する
- Web Studioを使用してアクセス ポリシー ルールを管理する(#manage-access-policy-rules-using-web-studio)
- PowerShellを使用してポリシー ルールを追加および調整する(#add-and-manage-access-policy-rules-using-powershell)

アクセス ポリシー規則について

デリバリーグループに対して複数のアクセス ポリシー ルールを構成できます。デリバリーグループ内のアプリとデスクトップは、ユーザーの接続が、定義したアクセス ポリシー ルール（順序に関係なく）のいずれかに一致する場合に、ユーザーのStoreFrontまたはWorkspaceに表示されます。

各規則は個別に有効または無効にできます。無効な規則は、アクセス ポリシーが評価されるときに無視されます。

アクセス ポリシー(/en-us/citrix-virtual-apps-desktops/2511/media/delivery-groups-access-policy-defaults.png)

Web Studioでは、アクセス ポリシー リストに以下のデフォルトのSmartAccessポリシー ルールが含まれています。必要に応じて、さらに追加できます。

- **Citrix Gateway接続。** このポリシーでは、Citrix Gatewayを介して行われたユーザー接続のみが、デリバリーグループ内のリソースにアクセスできます。Device PostureまたはNetwork Location機能が有効になっている場合にWorkspaceを介して行われたユーザー接続も、Citrix Gatewayを介した接続と見なされます。
- **Citrix Gateway以外の接続。** このポリシーでは、Citrix Gatewayを介さずに行われたユーザー接続のみが、デリバリーグループ内のリソースにアクセスできます。

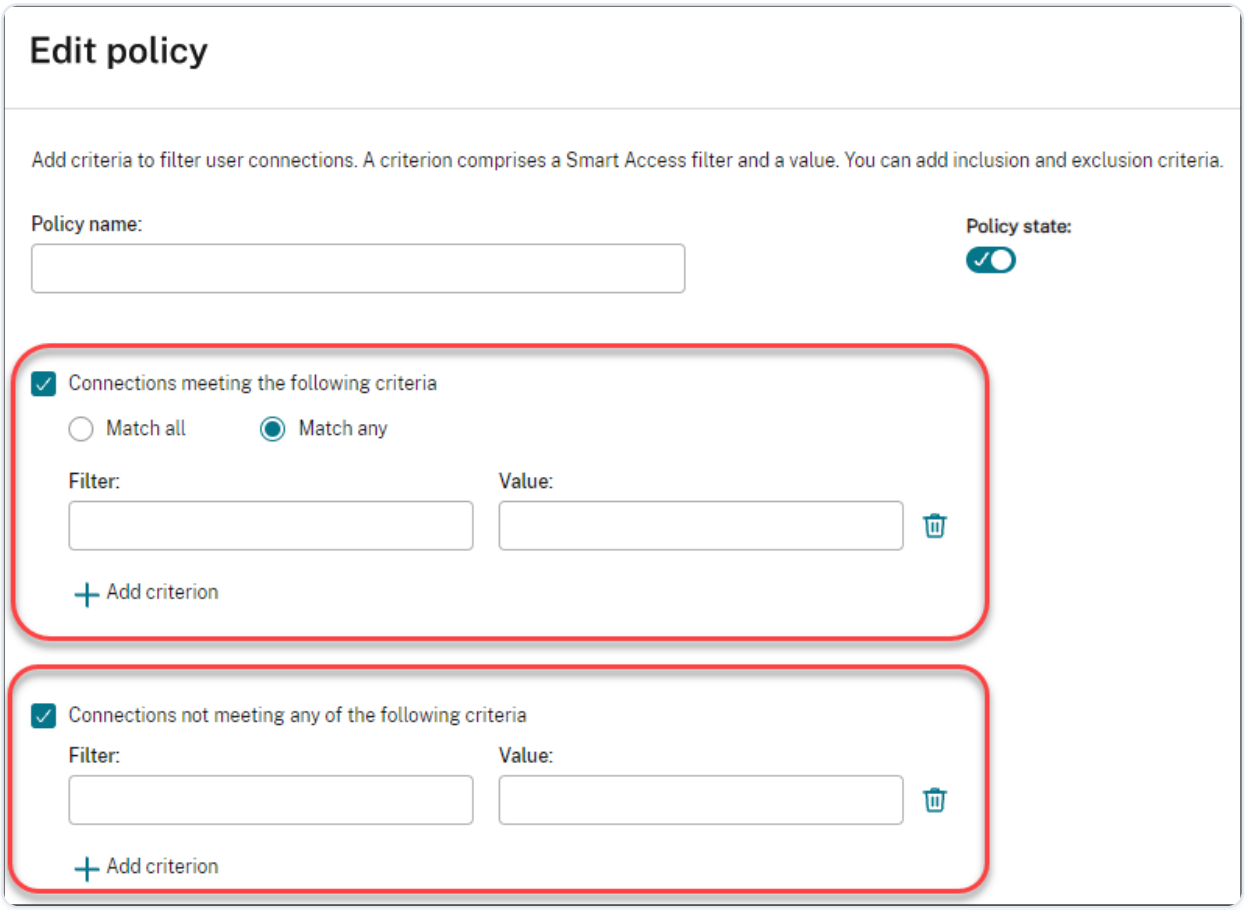
> **注:**
>
> - デフォルトのルールが新しく構成されたルールを上書きしないようにするには、デフォルトのルールを無効にするか、新しいポリシーで使用されているフィルターを除外するようにルールを調整する必要があります。
> - デフォルトのポリシーは削除できませんが、無効にすることはできます。ポリシーを無効にするには、**編集**アイコンをクリックし、**ポリシーの状態**を**無効**に変更します。
> - ポリシーリストには、PowerShellコマンドを使用して追加された規則も表示されます。これらのポリシーは削除できますが、Web Studioで編集することはできません。

Web Studioを使用してアクセス ポリシー ルールを追加する

アクセス ポリシー規則は、一連のフィルターで構成されます。フィルターについて詳しくは、この記事を参照してください。アクセス ポリシー規則を追加するときは、必要に応じて複数の条件フィルターを規則に追加します。

Web Studioを使用してデリバリーグループのポリシーを追加するには、次の手順に従います。

1. コンソールで、左側のペインの **「Delivery Groups」** を選択します。
2. グループを選択し、アクションバーの **「Edit」** をクリックします。
3. **「Access Policy」** ページで、**「Add」** をクリックします。**「Add Policy」** ページが表示されます。



4. 「**Policy name**」 フィールドに、ポリシーのわかりやすい名前を入力します。名前は展開内で一意である必要があります。
5. 許可されるユーザー接続の基準を定義するには、次の手順に従います。

   a. 「**以下の条件を満たす接続**」を選択します。

   b. 「**Add criterion**」 をクリックします。

   c. 「**Filter**」 フィールドに、使用するフィルターの名前を入力します。「**Value**」 フィールドに、フィルターの希望する値を入力します。たとえば、Workspace (StoreFront ではなく) を介して接続されたユーザーのみがこのデリバリーグループのリソースにアクセスできるようにするには、「**Filter**」 に `Citrix-Via-Workspace` を、「**Value**」 に `True` を入力します。

   d. さらに基準を追加するには、手順 b ～ c を繰り返します。

   e. 基準間の関係を選択します。

      - 「**Match any**」。構成されたフィルター基準のいずれかを満たす受信ユーザー接続の場合にのみアクセスを許可します。
      - 「**Match all**」。構成されたフィルター基準のすべてを満たす受信ユーザー接続の場合にのみアクセスを許可します。

6. 禁止されるユーザー接続の基準を定義するには、次の手順に従います。

   a. 「**次の条件のいずれも満たさない接続**」を選択します。

   b. 「**条件の追加**」をクリックします。

   c. **フィルター**フィールドに、使用するフィルターの名前を入力します。**値**フィールドに、フィルターの目的の値を入力します。たとえば、`example.cloud.com` Workspace URL を介して接続しているユーザーがこのデリバリーグループのリソースにアクセスするのを禁止する場合などです。**フィルター**には`Citrix.Workspace.UsingDomain`を、**値**には`example.cloud.com`を入力します。

   d. さらに条件を追加するには、手順 b～c を繰り返します。

   > **注:**
   >
   > 構成された条件のいずれかを満たすユーザー接続は、このデリバリーグループのリソースへのアクセスを禁止されます。

7. **完了**をクリックします。

   新しいポリシーがポリシーリストに表示されます。

8. この新しいポリシーでカバーされる接続との意図しない重複を避けるために、デフォルトのポリシー規則を確認および調整します。既存のポリシーを調整するには、次の方法を使用します。

   - デフォルトのポリシー規則を無効にします。
   - 新しいポリシーの包含基準に追加したSmartAccessフィルターを除外するように、デフォルトのポリシー規則を構成します。詳しくは、「Web Studioを使用したポリシー規則の管理」および「PowerShellを使用したアクセスポリシー規則の追加と管理」を参照してください。

> **重要:**
>
> 「アクセスポリシー規則について」で説明されているように、ユーザーの接続がデリバリーグループ内の1つ以上のポリシー規則に一致すると、ユーザーはそのリソースへのアクセス権を取得します。したがって、規則を作成した後、新しい規則でカバーされる接続との意図しない重複を避けるために、既存の規則を慎重に確認および調整する必要があります。

Web Studioを使用したアクセスポリシー規則の管理

包含条件と除外条件を使用して、デフォルトのポリシーを調整できます。たとえば、それらの接続のサブセットへのアクセスを制限するには、次の手順に従います。

1. デフォルトのポリシーを編集します。
2. **次のいずれかの条件を満たす接続**を選択します。
3. 許可されたユーザーアクセスシナリオのSmartAccessポリシー式を追加、編集、または削除します。

詳細については、Citrix Gatewayのドキュメントを参照してください。

PowerShellを使用してアクセスポリシー規則を追加および管理する

デリバリーグループのアクセスポリシー規則を追加および管理するには、次のPowerShellコマンドレットを使用できます。

- New-BrokerAccessPolicyRule
- Get-BrokerAccessPolicyRule
- Set-BrokerAccessPolicyRule
- BrokerAccessPolicyRule の名前を変更する
- BrokerAccessPolicyRule を削除する

詳細については、Citrix Developer Documentationの関連記事を参照してください。

アクセス ポリシーのユーザー スコープを構成する

デリバリー グループ内のすべてのアクセス ポリシーは、デフォルトで同じユーザー セットに適用されます。Studio、PowerShell、またはRest APIを使用して、特定のユーザーに適用されるようにアクセス ポリシーを構成できます。

Studioを使用して指定したユーザーにアクセス ポリシーを適用するには、次の手順に従います:

1. Studioから、左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**デリバリーグループの編集**を選択します。
3. **ユーザー**ページで、**コンテキストアクセスを使用**を選択します。
4. 構成するアクセス ポリシーを選択し、**ユーザーアクセススコープ**をクリックします。**ユーザーアクセススコープ**ページが表示されます。
5. このポリシーを適用する認証済みユーザーを定義するには：

- このポリシーを *すべての認証済みユーザーに適用するには、**すべての認証済みユーザーがリソースを使用することを許可する**を選択します。
- このポリシーを特定のユーザーに適用するには、**リソースの使用を制限する**が選択されたままにします。次に、許可リストとブロックリストを使用して、このポリシーのユーザーを追加または削除します。

6. 資格情報を提供しないユーザーにこのアクセス ポリシーを適用するには、**未認証（匿名）ユーザーへのアクセスを許可する。資格情報は不要**を選択します。

マシン

- マシンのユーザー割り当てを管理する
- マシンのユーザーへの割り当てを変更する
- 電源管理されたシングルセッションのプールされたVDAでローカルホストキャッシュを有効にする
- ユーザーあたりの最大マシン数を変更する
- マシンを更新する
- デスクトップのタグ制限を追加、変更、または削除する
- マシンを削除する(#remove-a-machine-from-a-delivery-group)
- ユーザーがマシンに接続できないようにする（メンテナンスモード）(#prevent-users-from-connecting-to-a-machine-maintenance-mode-in-a-delivery-group)
- マシンをシャットダウンして再起動する(#shut-down-and-restart-machines-in-a-delivery-group)
- マシンの再起動スケジュールを作成および管理する(#create-and-manage-restart-schedules-for-machines-in-a-delivery-group)
- 1回限りの再起動スケジュールを有効にする(#enable-one-time-restart-schedule)
- マシンの電源を管理する(#power-manage-machines-in-a-delivery-group)

マシンに対するユーザー割り当ての管理

デリバリーグループ内のマシンのユーザー割り当てを管理します。デリバリーグループにデスクトップ割り当てルールが構成されている場合、マシンは最初のデスクトップ起動時にユーザーにランダムに割り当てられ、ユーザー割り当てが変更されない限り、ユーザーに割り当てられたままになります。割り当てられていないマシンを特定のユーザーに手動で割り当てたい場合、またはマシンの既存のユーザー割り当てを変更したい場合は、このトピックで説明されている手順に

従って変更を行ってください。これらの手順を使用すると、ユーザーに割り当てられたマシンのCitrix Workspaceアプリに表示される名前を変更することもできます。

詳細な手順は次のとおりです。

1. Studioで、左ペインから**Delivery Groups**を選択します。
2. グループを選択し、アクションバーで**Edit**を選択します。
3. 左ペインで**Machine Allocation**を選択します。グループ内の各マシンの以下の詳細が表示されます。
    - **マシン名:** マシンの名前が表示されます。
    - **表示名:** Citrix Workspaceアプリでのマシンの表示名が表示されます。
    - **ユーザー:** このマシンに割り当てられているユーザーが表示されます。デスクトップ割り当てルールが構成されている場合、マシンは最初のデスクトップ起動時にユーザーにランダムに割り当てられ、ユーザー割り当てが変更されない限り、ユーザーに割り当てられたままになります。
4. マシンを見つけ、ユーザーを割り当てるか、そのユーザー割り当てを変更します。
    - **参照**をクリックしてユーザーを参照します。
    - **ユーザー**列に、ユーザー名をセミコロンで区切って入力します。
    - **CSVファイルからインポート**をクリックして、CSVファイルを使用して設定の詳細をインポートします。
    - **変更**をクリックして、マシンのデスクトップアイコンを更新します。指定されたアイコンは、マシンレベルでのみ設定されたデフォルトアイコンを上書きします。
5. (オプション) マシンがユーザーに割り当てられている場合は、必要に応じて表示名を変更します。

> **注:**
>
> 表示名フィールドは、マシンがユーザーに割り当てられている場合にのみ有効になります。
>
> - マシンがデスクトップ割り当てルールに基づいてユーザーに割り当てられている場合、このフィールドにはそのルールで構成された表示名が表示されます。

- マシンが手動でユーザーに割り当てられており、このフィールドが空白の場合、デリバリーグループの公開名（指定されている場合）がマシンの表示名として使用されます。公開名が指定されていない場合は、デリバリーグループの名前が使用されます。デリバリーグループの公開名はPowerShellでのみ指定できることに注意してください。

6. **適用**を選択して変更を適用し、ウィンドウを開いたままにします。または、**OK**を選択して変更を適用し、ウィンドウを閉じます。

デリバリーグループ内のマシンのユーザーへの割り当てを変更する

MCSでプロビジョニングされたシングルセッションOSマシンの割り当てを変更できます。マルチセッションOSマシンまたはCitrix Provisioningでプロビジョニングされたマシンの割り当ては変更できません。

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. 「**デスクトップ**」または「**デスクトップ割り当てルール**」ページ（ページタイトルはデリバリーグループが使用するマシンカタログの種類によって異なります）で、新しいユーザーを指定します。
4. 加えた変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

電源管理されたシングルセッションのプールされたVDAでローカルホストキャッシュを有効にする

デフォルトでは、電源管理されたシングルセッションのプールされたマシンは、ローカルホストキャッシュモードでは使用できません。デリバリーグループごとにデフォルトの動作を上書きできます。詳細な手順は次のとおりです。

1. Studioで、左側のペインで**デリバリーグループ**を選択します。

   グループリストで、MCSまたはCitrix Provisioningによってプロビジョニングされたシングルセッションのプールされたマシンを含むグループには、警告アイコンが表示されます。
2. 必要に応じてグループを選択し、アクションバーで**編集**を選択します。
3. **ローカルホストキャッシュ**ページで、**リソースを常に利用可能にする**を選択します。
4. 加えた変更を適用してウィンドウを開いたままにするには、**適用**を選択します。または、変更を適用してウィンドウを閉じるには、**OK**を選択します。

または、PowerShellコマンドを使用してデフォルトの動作を上書きすることもできます。詳細については、「アプリケーションとデスクトップのサポート」を参照してください。

> **重要：**
>
> 電源管理されたシングルセッションのプールされたマシンへのアクセスを有効にすると、以前のユーザーセッションからのデータと変更が後続のセッションに存在する可能性があります。

デリバリーグループ内のユーザーあたりの最大マシン数を変更する

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. 「**デスクトップ割り当てルール**」ページで、ユーザーあたりの最大デスクトップ数を設定します。
4. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

デリバリーグループ内のマシンを更新する

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**マシンの表示**をクリックします。
3. マシンを選択し、アクションバーで**マシンの更新**をクリックします。

別のイメージを選択するには、**イメージ**を選択し、スナップショットを選択します。

変更を適用してマシンユーザーに通知するには、**「エンドユーザーへのロールアウト通知」**を選択します。次に、以下を指定します。

- マスターイメージを更新するタイミング: 今すぐ、または次回の再起動時
- 再起動の配布時間（グループ内のすべてのマシンの更新を開始するまでの合計時間）
- ユーザーに再起動が通知されるかどうか
- ユーザーが受信するメッセージ

デスクトップのタグ制限を追加、変更、または削除する

タグ制限の追加、変更、削除は、起動対象となるデスクトップに予期せぬ影響を与える可能性があります。「タグ」の考慮事項と注意点を確認してください。

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. **デスクトップ**ページで、デスクトップを選択し、**編集**をクリックします。
4. タグ制限を追加するには、**タグを持つマシンへの起動を制限する**を選択し、タグを選択します。
5. タグ制限を変更または削除するには、次のいずれかを実行します。
   - 別のタグを選択します。
   - **このタグを持つマシンへの起動を制限する**のチェックを外して、タグ制限を削除します。
6. **適用**をクリックして変更を適用し、ウィンドウを開いたままにします。または、**保存**をクリックして変更を適用し、ウィンドウを閉じます。

デリバリーグループからマシンを削除する

マシンを削除すると、デリバリーグループから削除されます。デリバリーグループが使用するマシンカタログからは削除されません。したがって、そのマシンは別のデリバリーグループに割り当てることができます。

マシンは、削除する前にシャットダウンする必要があります。マシンを削除している間、ユーザーがマシンに接続するのを一時的に停止するには、シャットダウンする前にマシンをメンテナンスモードにします。

マシンには個人データが含まれている可能性があるため、別のユーザーにマシンを割り当てる前に注意してください。マシンの再イメージングを検討してください。

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**マシンの表示**をクリックします。
3. マシンがシャットダウンされていることを確認します。
4. マシンを選択し、アクションバーで**デリバリーグループから削除**をクリックします。

マシンが使用する接続を介して、デリバリーグループからマシンを削除することもできます。

デリバリーグループ内のマシンへのユーザー接続を防止する (メンテナンスモード)

マシンへの新しい接続を一時的に停止する必要がある場合は、デリバリーグループ内の1台またはすべてのマシンでメンテナンスモードをオンにできます。これは、パッチを適用したり、管理ツールを使用したりする前に行うことがあります。

- マルチセッションOSマシンがメンテナンスモードの場合、ユーザーは既存のセッションに接続できますが、新しいセッションを開始することはできません。
- シングルセッションOSマシン（またはリモートPCアクセスを使用するPC）がメンテナンスモードの場合、ユーザーは接続または再接続できません。現在の接続は、切断またはログオフするまで接続されたままになります。

メンテナンスモードをオンまたはオフにするには：

1. 左側のペインで、**デリバリーグループ**を選択します。
2. グループを選択します。
3. デリバリーグループ内のすべてのマシンでメンテナンスモードをオンにするには、アクションバーで**メンテナンスモードをオンにする**をクリックします。

   1台のマシンでメンテナンスモードをオンにするには、アクションバーで**マシンの表示**をクリックします。マシンを選択し、アクションバーで**メンテナンスモードをオンにする**をクリックします。
4. デリバリーグループ内の1台またはすべてのマシンでメンテナンスモードをオフにするには、上記の手順に従いますが、アクションバーで**メンテナンスモードをオフにする**をクリックします。

Windowsリモートデスクトップ接続（RDC）の設定も、マルチセッションOSマシンがメンテナンスモードであるかどうかに影響します。以下のいずれかが発生した場合、メンテナンスモードはオンになります。

- 前述のとおり、メンテナンスモードがオンに設定されている。
- RDCが**このコンピューターへの接続を許可しない**に設定されている。
- RDCが**このコンピューターへの接続を許可しない**に設定されていない。**リモートホスト構成ユーザーログオンモード**の設定が、**再接続を許可するが、新しいログオンを禁止する**または**再接続を許可するが、サーバーが再起動されるまで新しいログオンを禁止する**のいずれかである。

以下のメンテナンスモードをオンまたはオフにすることもできます。

- 接続。その接続を使用しているマシンに影響します。
- マシンカタログ。そのカタログ内のマシンに影響します。

デリバリーグループ内のマシンをシャットダウンして再起動する

この手順は、Remote PC Accessマシンではサポートされていません。

1. 左ペインで****を選択します。
2. グループを選択し、アクションバーで**マシン表示**をクリックします。
3. マシンを選択し、アクションバーで次のいずれかのエントリをクリックします。

    - : マシンの電源を強制的にオフにし、マシンの一覧を更新します。
    - : オペレーティングシステムにシャットダウンを要求し、その後マシンを再起動します。オペレーティングシステムがこれに応じられない場合、マシンは現在の状態のままになります。
    - : オペレーティングシステムを強制的にシャットダウンし、その後マシンを再起動します。
    - : マシンをシャットダウンせずに一時停止し、マシンの一覧を更新します。
    - : オペレーティングシステムにシャットダウンを要求します。

強制ではないアクションの場合、マシンが10分以内にシャットダウンしないと、電源がオフになります。Windowsがシャットダウン中に更新プログラムのインストールを試みる場合、更新が完了する前にマシンの電源がオフになるリスクがあります。

Citrixでは、シングルセッションOSマシンのユーザーがセッション内で**シャットダウン**を選択できないようにすることをお勧めします。詳細については、Microsoftのポリシーに関するドキュメントを参照してください。

接続上で(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/connections.html)マシンをシャットダウンして再起動することもできます。

デリバリーグループ内のマシンの再起動スケジュールを作成および管理する

> **注:**
>
> - Autoscale™が有効なデリバリーグループに再起動スケジュールが適用されると、そのマシンは電源がオフにされるだけで、Autoscaleが電源をオンにするのを待ちます。
> - ランダムなシングルセッションマシンに再起動スケジュールが適用されると、コストを節約するために、それらのマシンは再起動されるのではなく電源がオフになります。マシンの電源をオンにするにはAutoscaleを使用することをお勧めします。
> - デリバリーグループのタイムゾーンを変更すると、そのデリバリーグループ内のマシンが再起動される可能性があります。これを避けるため、タイムゾーン設定は稼働時間外に変更するようにしてください。

再起動スケジュールは、デリバリーグループ内のマシンが定期的に再起動される時期を指定します。デリバリーグループに対して1つ以上のスケジュールを作成できます。スケジュールは次のいずれかに影響します。

- グループ内のすべてのマシン。
- グループ内の1つ以上の（ただしすべてではない）マシン。マシンは、マシンに適用するタグによって識別されます。これはタグ制限と呼ばれます。タグがアクションをそのタグを持つアイテムのみに制限するためです。

たとえば、すべてのマシンが1つのデリバリーグループにあるとします。すべてのマシンを週に1回再起動し、経理チームが使用するマシンを毎日再起動したいとします。これを実現するには、すべてのマシンに対して1つのスケジュールを設定し、経理のマシンのみに対して別のスケジュールを設定します。

スケジュールには、再起動が開始される曜日と時刻、および期間が含まれます。

スケジュールを有効または無効にできます。スケジュールを無効にすることは、テスト中、特別な期間中、またはスケジュールが必要になる前に準備する際に役立ちます。

管理コンソールから自動電源オンまたはシャットダウンにスケジュールを使用することはできません。再起動のみに使用できます。

スケジュールの重複

複数のスケジュールが重複する可能性があります。上記の例では、両方のスケジュールが経理のマシンに影響します。これらのマシンは日曜日に2回再起動される可能性があります。スケジューリングコードは、同じマシンが意図したよりも頻繁に再起動されるのを避けるように設計されていますが、保証はできません。

- スケジュールが開始時刻と継続時間で正確に一致する場合、マシンが再起動されるのは1回だけである可能性が高くなります。
- スケジュールが開始時刻と継続時間で異なるほど、複数回の再起動が発生する可能性が高くなります。
- スケジュールによって影響を受けるマシンの数も、重複の可能性に影響します。例として、すべてのマシンに影響する週次スケジュールは、それぞれに指定された期間に応じて、経理用マシンの日次スケジュールよりも早く再起動を開始する可能性があります。

再起動スケジュールの詳細については、「再起動スケジュールの内部」を参照してください。

再起動スケジュールの表示

1. 左ペインで**Delivery Groups**を選択します。

2. グループを選択し、アクションバーで**編集**をクリックします。
3. **再起動スケジュール**ページを選択します。

ページには、設定されている各スケジュールについて次の情報が含まれています。

- スケジュール名
- 使用されているタグ制限（ある場合）
- マシンの再起動が実行される頻度
- マシンユーザーが通知を受け取るかどうか
- スケジュールが有効になっているかどうか

タグの追加（適用）

タグ制限を使用する再起動スケジュールを構成する場合は、スケジュールが影響するマシンにタグが追加されていることを確認してください。上記の例では、経理チームが使用する各マシンにタグが適用されています。詳細については、「タグ」を参照してください。

1台のマシンに複数のタグを適用できますが、再起動スケジュールで指定できるタグは1つだけです。

1. 左側のペインで**デリバリーグループ**を選択します。
2. スケジュールによって制御されるマシンを含むグループを選択します。
3. **マシンの表示**をクリックし、タグを追加するマシンを選択します。
4. アクションバーで**タグの管理**をクリックします。
5. タグが存在する場合は、タグ名の横にあるチェックボックスをオンにします。タグが存在しない場合は、**作成**をクリックし、タグの名前を指定します。タグが作成されたら、新しく作成されたタグ名の横にあるチェックボックスをオンにします。
6. **タグの管理**ダイアログで**保存**をクリックします。

再起動スケジュールを作成する

> **注:**
>
> 再起動スケジュールは、電源管理されているすべてのマルチセッションマシンと、電源管理されていないマルチセッションマシンに適用できます。

1. 左側のペインで**デリバリーグループ**を選択します。

2. グループを選択し、アクションバーで**編集**をクリックします。
3. **再起動スケジュール**ページで、**追加**をクリックします。
4. **再起動スケジュールの追加**ページで：

   - スケジュールを有効にするには、**はい**を選択します。スケジュールを無効にするには、**いいえ**を選択します。
   - スケジュールの名前と説明を入力します。
   - **タグへの制限**については、タグの制限を適用します。
   - **メンテナンスモードのマシンを含める**については、メンテナンスモードのマシンをこのスケジュールに含めるかどうかを選択します。代わりにPowerShellを使用するには、「メンテナンスモードのマシンに対するスケジュールされた再起動」を参照してください。
   - **再起動の頻度**については、再起動の発生頻度（毎日、毎週、毎月、または1回）を選択します。**毎週**または**毎月**を選択した場合、1つ以上の特定の日を指定できます。
   - **繰り返し間隔**については、スケジュールを実行する頻度を指定します。
   - **開始日**については、スケジュールの初回実行の開始日を指定します。
   - **再起動の開始時刻**については、24時間形式で再起動を開始する時刻を指定します。

     - **再起動の期間**：
     - 応答しないセッションを持つマシンを強制的に再起動するには、**強制再起動**を選択し、次のいずれかのオプションを選択します。

       - **すべてのマシンを一度に再起動**
       - **指定した時間内にすべてのマシンを再起動**し、**時間**または**分**で時間を指定します。

     - 再起動する前にすべてのセッションがドレインされるのを待つには、**グレースフル再起動**を選択します。

       グレースフル再起動を使用するように構成された再起動スケジュールを開始すると：

       - デリバリーグループに属するすべてのアイドル状態のマシンは、すぐに再起動されます。
       - 1つ以上のセッションがアクティブなデリバリーグループに属する各マシンは、すべてのセッションがログオフされると再起動されます。

     > **注:**

> グレースフル再起動スケジュールは、電源管理されているマシンのみを再起動できます。

- で、再起動が開始される前に、該当するマシンに通知メッセージを表示するかどうかを決定します。デフォルトでは、メッセージは表示されません。
- 再起動が開始される15分前にメッセージを表示することを選択した場合、最初のメッセージの後に5分ごとにメッセージを繰り返すことができます。デフォルトでは、メッセージは繰り返されません。
- 通知のタイトルとテキストを入力します。デフォルトのテキストはありません。

  メッセージに再起動までのカウントダウンを含める場合は、変数 **%m%** を含めます。すべてのマシンを同時に再起動することを選択しない限り、メッセージは再起動前の適切なタイミングで各マシンに表示されます。

5. **完了**をクリックして変更を適用し、**再起動スケジュールの追加**ウィンドウを閉じます。
6. **適用**をクリックして行った変更を適用し、ウィンドウを開いたままにします。または、**保存**をクリックして変更を適用し、ウィンドウを閉じます。

ドレイン後の再起動

PowerShell を使用してマシンの再起動スケジュールを作成または更新する場合 (`New-BrokerRebootSchedulev2` または `Set-BrokerRebootSchedulev2`)、別の再起動期間値を使用できます。

`-UseNaturalReboot <Boolean>` パラメーターでドレイン後の再起動機能を有効にすると、すべてのセッションがドレインされた後にすべてのマシンが再起動されます。再起動時刻になると、マシンはドレイン状態になり、すべてのセッションがログオフされると再起動されます。

この機能は、シングルセッションまたはマルチセッションマシンを含むデリバリーグループでサポートされています。このオプションは、電源管理されているマシンと電源管理されていないマシンの両方で使用できます。

オンプレミス環境では、この機能は PowerShell を使用する場合にのみサポートされます。この機能は Web Studio では利用できません。

再起動スケジュールの編集、削除、有効化、または無効化

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. **再起動スケジュール**ページで、スケジュールのチェックボックスを選択します。

- スケジュールを編集するには、**編集**をクリックします。再起動スケジュールの作成のガイダンスに従って、スケジュール構成を更新します。
- スケジュールを有効または無効にするには、**編集**をクリックします。**再起動スケジュールを有効にする**チェックボックスをオンまたはオフにします。
- スケジュールを削除するには、 をクリックします。削除を確認します。スケジュールを削除しても、影響を受けるマシンに適用されているタグには影響しません。

データベースの停止により、スケジュールされた再起動が遅延しました

> **注:**
>
> この機能はPowerShellでのみ利用可能です。

> デリバリーグループ内のマシン (VDA) のスケジュールされた再起動が開始される前にサイトデータベースの停止が発生した場合、停止が終了すると再起動が開始されます。これにより、予期しない結果が生じる可能性があります。

たとえば、デリバリーグループの再起動を非稼働時間中（午前3時開始）に発生するようにスケジュールしたとします。スケジュールされた再起動が開始される1時間前（午前2時）にサイトデータベースの停止が発生しました。停止は6時間（午前8時まで）続きました。再起動スケジュールは、Delivery Controllerとサイトデータベース間の接続が復元されたときに開始されます。VDAの再起動は元のスケジュールから5時間後に開始され、稼働時間中にVDAが再起動することになります。

この状況を回避するために、`New-BrokerRebootScheduleV2`および`Set-BrokerRebootScheduleV2`コマンドレットで`MaxOvertimeStartMins`パラメーターを使用できます。この値は、再起動スケジュールが開始できる、スケジュールされた開始時刻を超える最大分数を示します。

- データベース接続がその時間内（スケジュールされた時間 + `MaxOvertimeStartMins`）に復元された場合、VDAの再起動が開始されます。
- データベース接続がその時間内に復元されなかった場合、VDAの再起動は開始されません。
- このパラメーターが省略されているか、値がゼロの場合、停止期間に関係なく、データベースへの接続が復元されたときにスケジュールされた再起動が開始されます。

詳細については、コマンドレットのヘルプを参照してください。この機能は PowerShell でのみ利用できます。Web Studio で再起動スケジュールを構成する際には、この値を設定できません。

メンテナンスモードのマシンのスケジュールされた再起動

> **注:**
>
> この機能はPowerShellでのみ利用可能です。オプション `IgnoreMaintenanceMode` は、Citrix Virtual Apps™ and Desktops 7 2006以降でサポートされています。

> 再起動スケジュールがメンテナンスモードのマシンに影響するかどうかを示すには、`BrokerRebootScheduleV2` コマンドレットで `IgnoreMaintenanceMode` オプションを使用します。

たとえば、次の cmdlet は、メンテナンスモードではないマシンに加えて、メンテナンスモードのマシンを再起動するスケジュールを作成します。

```
New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup>
-IgnoreMaintenanceMode $true
```

次のコマンドレットは、既存の再起動スケジュールを変更します。

```
Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode $true
```

詳細については、コマンドレットのヘルプを参照してください。この機能はPowerShellでのみ利用可能です。

1回限りの再起動スケジュールを有効にする

PowerShell を使用して1回限りの再起動スケジュールを有効にする場合は、次の `BrokerCatalogRebootSchedule` PowerShell コマンドを使用して、再起動スケジュールを作成、変更、削除します。

- Get-BrokerCatalogRebootSchedule
- New-BrokerCatalogRebootSchedule
- Set-BrokerCatalogRebootSchedule
- ブローカーカタログ再起動スケジュールを削除
- ブローカーカタログ再起動スケジュール名を変更

制限事項:

- タイムゾーンが構成されていないカタログに関連付けられたカタログ再起動スケジュールは作成されますが、開始されません。

- カタログ再起動スケジュールが作成されると、その再起動スケジュールはデリバリーグループに属するカタログVMでのみ実行されます。

例、,

- Feb 3, 2022の午前2時から午前4時の間に開始するように、**BankTellers**という名前のカタログ内のVMの再起動スケジュールを作成するには。

```
C:\PS> New-BrokerCatalogRebootSchedule -Name BankTellers -CatalogName
BankTellers  -StartDate "2022-02-03" -StartTime "02:00" -Enabled $true
-RebootDuration 120
```

- UID 17のカタログ内のVMの再起動スケジュールを、Feb 3, 2022の午前1時から午前5時の間に開始するように作成するには。再起動の10分前に、各VMは、すべてのユーザーセッションで、タイトルが**WARNING: Reboot pending**、メッセージが**Save your work**のメッセージボックスを表示するように設定されます。

```
C:\PS> New-BrokerCatalogRebootSchedule -Name 'Update reboot'
-CatalogUid 17 -StartDate "2022-02-03" -StartTime "01:00" -Enabled
$true -RebootDuration 240 -WarningTitle "WARNING: Reboot pending"
-WarningMessage "Save your work" -WarningDuration 10
```

- **Old Name** という名前のカタログ再起動スケジュールを **New Name** に変更します。

```
C:\PS> Rename-BrokerCatalogRebootSchedule -Name "Old Name" -NewName
"New Name"
```

- UID 1 を持つすべてのカタログ再起動スケジュールを表示し、その後、UID 1 を持つカタログ再起動スケジュールを **New Name** に変更します。

```
C:\PS> Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
```

- **Accounting**という名前のカタログ再起動スケジュールを、各VMの再起動の10分前に、タイトルが**WARNING: Reboot pending, and the message**、メッセージが**Save your work**のメッセージを表示するように設定します。このメッセージは、そのVM上のすべてのユーザーセッションに表示されます。

```
C:\PS> Set-BrokerCatalogRebootSchedule -Name Accounting -WarningMessage
"Save your work" -WarningDuration 10 -WarningTitle "WARNING: Reboot
pending"
```

- 無効になっているすべての再起動スケジュールを表示し、すべての無効な再起動スケジュールを有効にします。

```
C:\PS> Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
BrokerCatalogRebootSchedule -Enabled $true
```

- UID 17を持つカタログ再起動スケジュールを、各VMの再起動の15分前、10分前、5分前に「**Rebooting in %m% minutes**」というメッセージを表示するように設定します。

```
C:\PS> Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Rebooting in
%m% minutes." -WarningDuration 15 -WarningRepeatInterval 5
```

- 「**MyCatalog**」という名前のカタログのタイムゾーンを構成します。

```
C:\PS> Set-BrokerCatalog -Name "MyCatalog" -TimeZone &lt;TimeZone>
```

デリバリーグループ内のマシンの電源管理

仮想シングルセッションOSマシンのみ電源管理が可能で、物理マシン（リモートPCアクセスを含む）はできません。GPU機能を備えたシングルセッションOSマシンは一時停止できないため、電源オフ操作は失敗します。マルチセッションOSマシンについては、再起動スケジュールを作成できます。

プールされたマシンを含むデリバリーグループでは、仮想シングルセッションOSマシンは次のいずれかの状態になります。

- ランダムに割り当てられ、使用中
- 未割り当てで未接続

静的マシンを含むデリバリーグループでは、仮想シングルセッションOSマシンは次のようになります。

- 永続的に割り当てられ、使用中
- 永続的に割り当てられ、未接続（ただし準備完了）

- 未割り当てで未接続

通常の使用時、静的デリバリーグループには通常、永続的に割り当てられたマシンと未割り当てのマシンの両方が含まれます。最初は、デリバリーグループ作成時に手動で割り当てられたマシンを除き、すべてのマシンが未割り当てです。ユーザーが接続すると、マシンは永続的に割り当てられます。これらのデリバリーグループ内の未割り当てマシンは完全に電源管理できますが、永続的に割り当てられたマシンは部分的にしか管理できません。

- **プールとバッファ:** プールされたデリバリーグループおよび未割り当てマシンを持つ静的デリバリーグループの場合、プール（このインスタンスでは）とは、電源オン状態に保たれ、ユーザーが接続する準備ができている未割り当てまたは一時的に割り当てられたマシンのセットです。ユーザーはログオン直後にマシンを取得します。プールサイズ（電源オン状態に保たれるマシンの数）は、時間帯によって構成可能です。静的デリバリーグループの場合、SDKを使用してプールを構成します。

  バッファとは、プール内のマシンの数がしきい値を下回ったときに電源がオンになる、未割り当てマシンの追加のスタンバイセットです。しきい値はデリバリーグループサイズのパーセンテージです。大規模なデリバリーグループの場合、しきい値を超えるとかなりの数のマシンがオンになる可能性があります。したがって、デリバリーグループのサイズを慎重に計画するか、SDKを使用してデフォルトのバッファサイズを調整してください。
- **電源状態タイマー:** 電源状態タイマーを使用すると、ユーザーが指定された時間切断された後にマシンを一時停止できます。たとえば、ユーザーが少なくとも10分間切断された場合、勤務時間外にマシンは自動的に一時停止します。

  タイマーは、平日と週末、およびピーク時と非ピーク時の間隔で構成できます。
- **永続的に割り当てられたマシンの部分的な電源管理:** 永続的に割り当てられたマシンについては、電源状態タイマーを設定できますが、プールやバッファは設定できません。マシンは各ピーク期間の開始時にオンになり、各非ピーク期間の開始時にオフになります。消費されたマシンを補うために利用可能になるマシンの数について、未割り当てマシンで行うようなきめ細かな制御はできません。

仮想シングルセッションOSマシンの電源管理

1. 左ペインで**Delivery Groups**を選択します。
2. グループを選択し、アクションバーで**Edit Delivery Group**をクリックします。
3. **Power Management**ページで、**Power manage machines**から**Weekdays**を選択します。デフォルトでは、平日は月曜日から金曜日です。
4. ランダムなデリバリーグループの場合、**Machines to be powered on**で**Edit**をクリックし、平日のプールサイズを指定します。次に、電源をオンにするマシンの数を選択します。

5. **Peak hours**で、各日のピーク時間とオフピーク時間を設定します。
6. 平日のピーク時間と非ピーク時間の電源状態タイマーを設定します。**During peak hours > When disconnected**で、デリバリーグループ内の切断されたマシンを一時停止するまでの遅延（分単位）を指定し、**Suspend**を選択します。**During off-peak hours > When disconnected**で、デリバリーグループ内のログオフされたマシンをシャットダウンするまでの遅延を指定し、**Shutdown**を選択します。このタイマーは、ランダムなマシンを含むデリバリーグループでは使用できません。
7. **Power manage machines**から**Weekend**を選択し、週末のピーク時間と電源状態タイマーを設定します。
8. **Apply**をクリックして変更を適用し、ウィンドウを開いたままにします。または、**Save**をクリックして変更を適用し、ウィンドウを閉じます。

SDKを使用して、次の操作を実行します。

- 電源状態タイマーに応じてマシンを一時停止するのではなくシャットダウンするか、タイマーを接続解除ではなくログオフに基づいて設定する場合。
- デフォルトの平日と週末の定義を変更します。
- 電源管理を無効にします。詳しくは、「CTX217289」を参照してください。

切断されたセッションで異なる期間に移行するVDIマシンの電源管理

> **重要:**
>
> この機能強化は、切断されたセッションを持つVDIマシンにのみ適用されます。ログオフされたセッションを持つVDIマシンには適用されません。

> 以前のリリースでは、アクション (切断アクション = 「**中断**」または「**シャットダウン**」) が必要な期間に移行する VDI マシンは、電源がオンのままでした。このシナリオは、アクション (切断アクション = 「**何もしない**」) が不要な期間 (ピーク時またはオフピーク時) にマシンが切断された場合に発生しました。

Citrix Virtual Apps and Desktops 7 1909 以降、指定された切断時間が経過すると、移行先の期間に構成されている切断アクションに応じて、マシンは中断または電源オフされます。

たとえば、VDI デリバリーグループに次の電源ポリシーを構成します。

- `PeakDisconnectAction` を「Nothing」に設定します。

- `OffPeakDisconnectAction` を「Shutdown」に設定します。
- `OffPeakDisconnectTimeout` を「10」に設定します。

電源ポリシーの切断アクションについて詳しくは、https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy および https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/ を参照してください。

以前のリリースでは、ピーク時にセッションが切断された VDI マシンは、ピークからオフピークに移行しても電源がオンのままでした。Citrix Virtual Apps and Desktops 7 1909 以降、期間移行時に `OffPeakDisconnectAction` および `OffPeakDisconnectTimeout` ポリシーアクションが VDI マシンに適用されます。その結果、マシンはオフピークに移行してから 10 分後に電源がオフになります。

以前の動作 (つまり、切断されたセッションでピークからオフピーク、またはオフピークからピークに移行するマシンに対して何もしない) に戻す場合は、次のいずれかを実行します。

- `LegacyPeakTransitionDisconnectedBehaviour` レジストリ値を `1` に設定します。これは、以前の動作を有効にする *true* と同等です。デフォルトでは、値は `0` (つまり *false*) であり、期間移行時に切断電源ポリシーアクションがトリガーされます。
  - パス: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer`
  - 名前: `LegacyPeakTransitionDisconnectedBehaviour`
  - 種類: `REG_DWORD`
  - データ: `0x00000001 (1)`
- `Set-BrokerServiceConfigurationData` PowerShell コマンドを使用して設定を構成します。例:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

電源ポリシーアクションを期間の移行時に適用する前に、マシンは以下の条件を満たしている必要があります。

- セッションが切断されていること。
- 保留中の電源アクションがないこと。
- 異なる時間帯に移行するVDI (シングルセッション) デリバリーグループに属していること。

- 特定の時間帯 (ピーク時またはオフピーク時) にセッションが切断され、電源アクションが割り当てられている期間に移行すること。

カタログの電源オン状態の VDA の割合を変更する

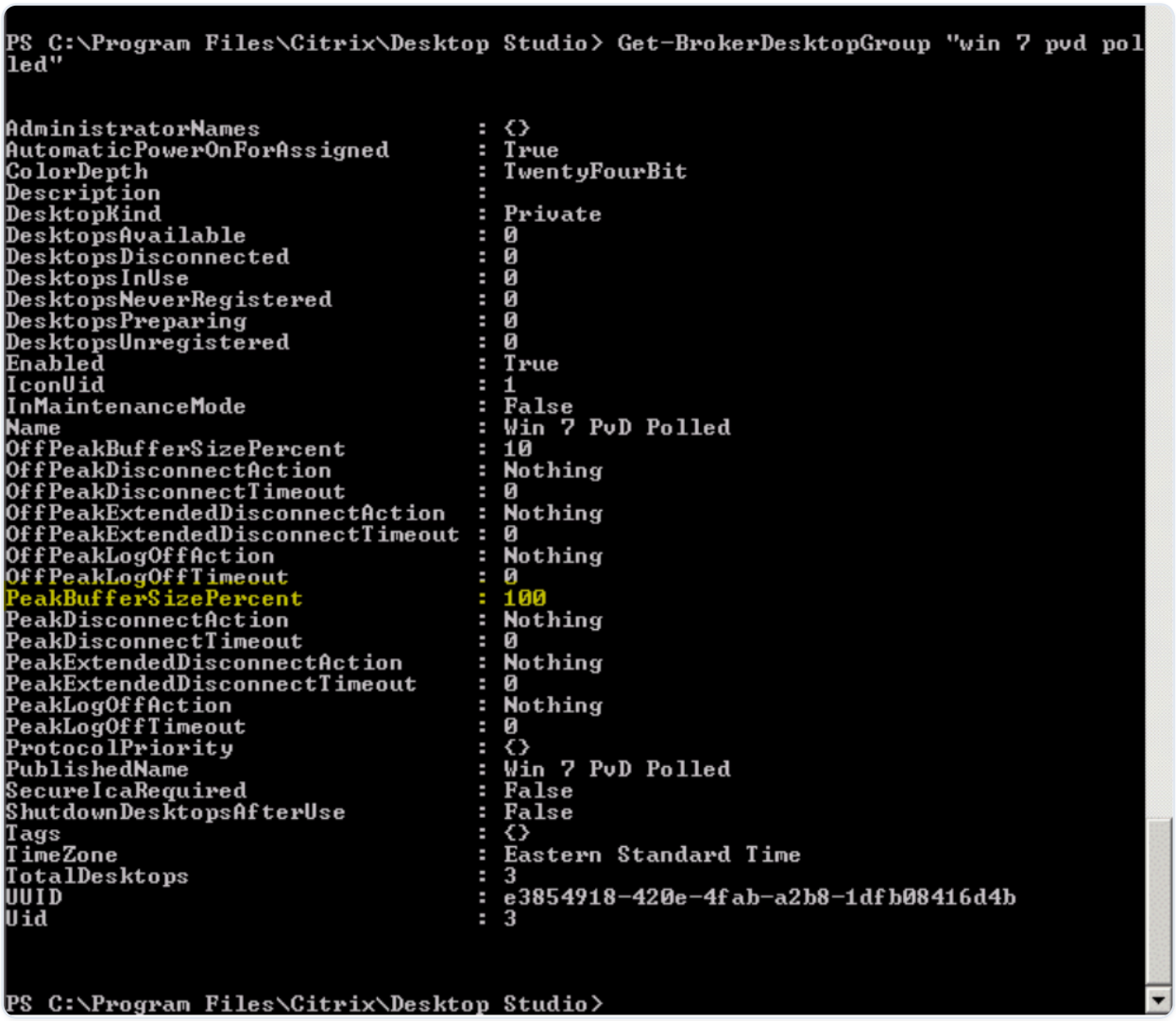
1. デリバリーグループの **電源管理** セクションから、デリバリーグループのピーク時間を調整します。
2. デスクトップグループ名をメモします。
3. 管理者権限でPowerShellを起動し、以下のコマンドを実行します。「Desktop Group Name」を、変更されたVDAの実行割合を持つデスクトップグループの名前に置き換えます。

   ```
   asnp Citrix*
   ```

   ```
   # Set-BrokerDesktopGroup "Desktop Group Name" -PeakBufferSizePercent 100
   ```

   値が 100 の場合、VDA の 100% が準備完了状態であることを意味します。
4. 以下のコマンドを実行してソリューションを確認します。

   ```
   #Get-BrokerDesktopGroup "Desktop Group Name"
   ```



変更が有効になるまで最大1時間かかる場合があります。

ユーザーがログオフした後にVDAをシャットダウンするには、次のように入力します。

```
# Set-BrokerDesktopGroup "Desktop Group Name" -ShutDownDesktopsAfterUse $True
```

ピーク時間中にVDAを再起動して、ユーザーがログオフした後に利用できるようにするには、次のように入力します。

```
# Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssignedDuringPeak $True
```

セッション

- セッションのログオフまたは切断、またはユーザーへのメッセージ送信
- セッションの事前起動とセッションの維持を構成する
- メンテナンスモードのマシンから切断された場合のセッション再接続を制御する

- セッションローミングを構成する

セッションのログオフまたは切断

1. 左ペインで**デリバリーグループ**を選択します。
2. デリバリーグループを選択し、アクションバーで**マシン表示**を選択します。
3. 中央ペインでマシンを選択し、アクションバーで**セッション表示**を選択してから、セッションを選択します。
    - または、中央ペインで**セッション**タブを選択し、セッションを選択します。
4. セッションからログオフするには、アクションバーで**ログオフ**を選択します。セッションが閉じられ、ユーザーはログアウトされます。マシンが特定のユーザーに割り当てられていない限り、他のユーザーが利用できるようになります。
5. セッションを切断するには、アクションバーで**切断**を選択します。アプリケーションはセッション内で実行を継続し、マシンはそのユーザーに割り当てられたままになります。ユーザーは同じマシンに再接続できます。

シングルセッションOSマシンでは、未使用のセッションを自動的に処理するように電源状態タイマーを構成できます。詳細については、「電源管理されたマシン」を参照してください。

デリバリーグループにメッセージを送信する

1. 左ペインで**デリバリーグループ**を選択します。
2. デリバリーグループを選択し、アクションバーで**マシン表示**を選択します。
3. 中央ペインで、メッセージを送信するマシンを選択します。
4. アクションバーで**セッション表示**を選択します。
5. 中央ペインで、すべてのセッションを選択し、アクションバーで**メッセージの送信**を選択します。
6. メッセージを入力し、**OK**をクリックします。必要に応じて、重大度レベルを指定できます。オプションには、**重大**、**質問**、**警告**、**情報**があります。

または、Citrix Directorを使用してメッセージを送信することもできます。詳細については、「ユーザーへのメッセージ送信」を参照してください。

デリバリーグループでセッションの事前起動とセッションの維持を構成する

これらの機能は、マルチセッションOSマシンでのみサポートされています。

セッションの事前起動とセッションの維持機能は、指定されたユーザーがアプリケーションにすばやくアクセスできるようにします。これは、要求される前にセッションを開始すること（セッションの事前起動）と、ユーザーがすべてのアプリケーションを閉じた後もアプリケーションセッションをアクティブに保つこと（セッションの維持）によって実現されます。

デフォルトでは、セッションの事前起動とセッションの維持は使用されません。セッションは、ユーザーがアプリケーションを起動したときに開始され（起動され）、セッション内の最後に開いたアプリケーションが閉じられるまでアクティブなままです。

考慮事項:

- デリバリーグループはアプリケーションをサポートしている必要があり、マシンはマルチセッションOS用のVDA（最小バージョン7.6）を実行している必要があります。
- これらの機能は、Windows版Citrix Workspaceアプリを使用している場合にのみサポートされ、追加のCitrix Workspaceアプリ構成も必要です。手順については、お使いのWindows版Citrix Workspaceアプリの製品ドキュメントで「セッションの事前起動」を検索してください。
- HTML5版Citrix Workspaceアプリはサポートされていません。
- セッションの事前起動を使用している場合、ユーザーのマシンがサスペンドモードまたは休止状態になった場合、事前起動は機能しません（セッションの事前起動設定に関わらず）。ユーザーは自分のマシン/セッションをロックできます。ただし、ユーザーがCitrix Workspaceアプリからログオフすると、セッションは終了し、事前起動は適用されなくなります。
- セッションの事前起動を使用している場合、物理クライアントマシンはサスペンドまたは休止状態の電源管理機能を使用できません。クライアントマシンのユーザーはセッションをロックできますが、ログオフしてはいけません。
- 事前起動されたセッションと維持されているセッションは、接続されている場合にのみ同時ライセンスを消費します。ユーザー/デバイスライセンスを使用している場合、ライセンスは90日間有効です。デフォルトでは、未使用の事前起動されたセッションと維持されているセッションは15分後に切断されます。この値はPowerShell（`New/Set-BrokerSessionPreLaunch` コマンドレット）で構成できます。
- これらの機能が互いに補完し合うように調整するには、ユーザーのアクティビティパターンを慎重に計画し、監視することが不可欠です。最適な構成は、ユーザーがより早くアプリケーションを利用できるというメリットと、ライセンスの使用とリソースの割り当てにかかるコストとのバランスを取ります。
- Citrix Workspaceアプリで、セッションの事前起動を特定の時刻にスケジュールすることもできます。

未使用の事前起動セッションと残存セッションがアクティブなままになる期間

ユーザーがアプリケーションを起動しない場合に、未使用のセッションがアクティブなままになる期間を指定する方法はいくつかあります。構成されたタイムアウトとサーバー負荷のしきい値です。これらすべてを構成できます。最初に発生したイベントにより、未使用のセッションが終了します。

- **タイムアウト:** 構成されたタイムアウトは、未使用の事前起動セッションまたは維持セッションがアクティブなままになる分数、時間、または日数を指定します。タイムアウトを短く設定しすぎると、事前起動セッションは、ユーザーに迅速なアプリケーションアクセスというメリットを提供する前に終了してしまいます。タイムアウトを長く設定しすぎると、サーバーに十分なリソースがないため、受信ユーザー接続が拒否される可能性があります。

  このタイムアウトは、管理コンソールからではなく、SDKからのみ有効にできます (`New/Set-BrokerSessionPreLaunch` コマンドレット)。タイムアウトを無効にすると、そのデリバリーグループのコンソール表示や**デリバリーグループの編集**ページには表示されません。

- **しきい値:** サーバー負荷に基づいて事前起動セッションと残存セッションを自動的に終了することで、サーバーリソースが利用可能であると仮定して、セッションが可能な限り開いたままになることを保証します。未使用の事前起動セッションと残存セッションは、新しいユーザーセッションにリソースが必要なときに自動的に終了されるため、接続拒否を引き起こしません。

  2つのしきい値を構成できます。デリバリーグループ内のすべてのサーバーの平均負荷率と、グループ内の単一サーバーの最大負荷率です。しきい値を超えると、プリローンチまたはリンガー状態が最も長かったセッションが終了します。負荷がしきい値を下回るまで、セッションは1分間隔で1つずつ終了します。しきい値を超えている間は、新しいプリローンチセッションは開始されません。

Controllerに登録されていないVDAを持つサーバー、およびメンテナンスモードのサーバーは、完全にロードされていると見なされます。予期しない停止が発生すると、容量を解放するためにプリローンチセッションとリンガーセッションが自動的に終了します。

セッションのプリローンチを有効にするには

1. グループを選択し、アクションバーで をクリックします。
2. ページで、セッションを起動するタイミングを選択してセッションのプリローンチを有効にします。

   - ユーザーがアプリケーションを起動したとき。これがデフォルト設定です。セッションのプリローンチは無効になっています。

- デリバリーグループ内の任意のユーザーがCitrix Workspaceアプリ for Windowsにログオンしたとき。
- ユーザーおよびユーザーグループのリスト内のいずれかのユーザーがCitrix Workspaceアプリ for Windowsにログオンしたとき。このオプションを選択する場合は、ユーザーまたはユーザーグループも指定してください。

アプリケーションのプリローンチセッションページ(/en-us/citrix-virtual-apps-desktops/2511/media/dws-session-2.png)

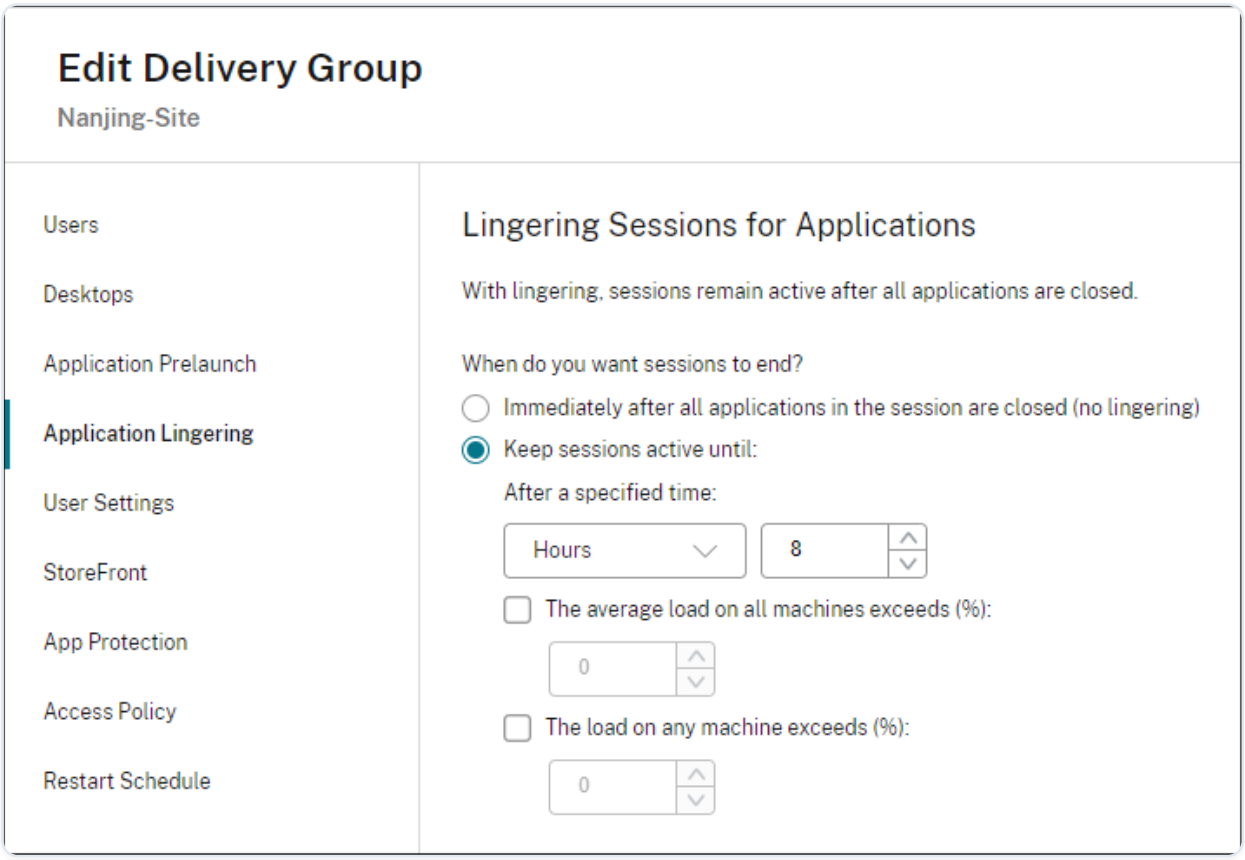
3. ユーザーがアプリケーションを起動すると、プリローンチされたセッションは通常のセッションに置き換えられます。ユーザーがアプリケーションを起動しない場合（プリローンチされたセッションが未使用の場合）、次の設定がそのセッションがアクティブなままになる期間に影響します。

   - 指定された時間間隔が経過したとき。時間間隔は変更できます（1〜99日、1〜2376時間、または1〜142,560分）。
   - デリバリーグループ内のすべてのマシンの平均負荷が指定された割合（1〜99%）を超えたとき。
   - デリバリーグループ内のいずれかのマシンの負荷が指定された割合（1〜99%）を超えたとき。

   まとめ：プリローンチされたセッションは、ユーザーがアプリケーションを起動する、指定された時間が経過する、または指定された負荷しきい値を超える、のいずれかのイベントが発生するまでアクティブなままです。

セッションの維持を有効にするには

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**デリバリーグループの編集**をクリックします。
3. **アプリケーションの維持**ページで、**セッションをアクティブなままにする期間**を選択して、セッションの維持を有効にします。



4. ユーザーが別のアプリケーションを起動しない場合、残存セッションがアクティブなままになる期間に影響する設定がいくつかあります。

   - 指定された時間間隔が経過した場合。時間間隔は、1〜99日、1〜2376時間、または1〜142,560分に変更できます。
   - デリバリーグループ内のすべてのマシンの平均負荷が指定された割合（1〜99%）を超えた場合。
   - デリバリーグループ内のいずれかのマシンの負荷が指定された割合（1〜99%）を超えた場合。

   まとめ: 残存セッションは、ユーザーがアプリケーションを起動する、指定された時間が経過する、または指定された負荷しきい値を超える、のいずれかのイベントが発生するまでアクティブなままです。

メンテナンスモードのマシンから切断された場合のセッション再接続を制御する

> **注：**
>
> この機能はPowerShellでのみ利用可能です。

> メンテナンスモードのマシンで切断されたセッションが、デリバリーグループ内のマシンに再接続できるかどうかを制御できます。

バージョン2106より前では、メンテナンスモードのマシンから切断されたシングルセッションのプールされたデスクトップセッションの再接続は許可されていませんでした。バージョン2106以降では、メンテナンスモードのマシンから切断された後の再接続（セッションの種類に関係なく）を許可または禁止するようにデリバリーグループを構成できます。

デリバリーグループを作成または編集する際（`New-BrokerDesktopGroup`、`Set-BrokerDesktopGroup`）、`-AllowReconnectInMaintenanceMode <boolean>`パラメーターを使用して、メンテナンスモードのマシンから切断されたマシンへの再接続を許可または禁止します。

- true に設定されている場合、セッションはグループ内のマシンに再接続できます。
- false に設定されている場合、セッションはグループ内のマシンに再接続できません。

デフォルト値:

- シングルセッション: 無効
- マルチセッション: 有効

セッションローミングの構成

デフォルトでは、デリバリーグループに対してセッションローミングが有効になっています。セッションはユーザーとともにクライアントデバイス間をローミングします。ユーザーがセッションを起動し、別のデバイスに移動すると、同じセッションが使用され、アプリケーションは両方のデバイスで同時に利用可能になります。複数のデバイスでアプリケーションを表示できます。アプリケーションは、デバイスや現在のセッションの有無にかかわらず追従します。多くの場合、アプリケーションに割り当てられたプリンターやその他のリソースも追従します。または、PowerShellを使用することもできます。詳しくは、「セッションローミング」を参照してください。

アプリケーションのセッションローミングを構成する

アプリケーションのセッションローミングを構成するには、次の手順に従います。

1. コンソールで、左側のペインの を選択します。
2. グループを選択し、アクションバーで を選択します。
3. ページで、 チェックボックスをオンにして、セッションローミングを有効にします。

    - 有効にすると、ユーザーがアプリケーションセッションを起動して別のデバイスに移動した場合、同じセッションが使用され、両方のデバイスで利用可能になります。無効にすると、セッションはデバイス間をローミングしなくなります。

4. **「OK」**を選択して変更を適用し、ウィンドウを閉じます。

デスクトップのセッションローミングを構成する

デスクトップのセッションローミングを構成するには、次の手順に従います。

1. コンソールで、左側のペインの**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで を選択します。
3. **デスクトップ**ページで、デスクトップを選択し、**編集**を選択します。
4. **セッションローミング**チェックボックスをオンにして、セッションローミングを有効にします。

- 有効にすると、ユーザーがデスクトップを起動してから別のデバイスに移動した場合、同じセッションが使用され、両方のデバイスでアプリケーションが利用可能になります。無効にすると、セッションはデバイス間をローミングしなくなります。

OKを選択して変更を適用し、ウィンドウを閉じます。

アプリケーション

デリバリーグループのアプリケーションを表示および追加します。

1. コンソールで、左ペインの**デリバリーグループ**を選択します。
2. グループを選択します。このグループにアプリケーションが含まれている場合、アクションバーに**アプリケーションの表示**が表示されます。
3. **アプリケーションの表示**を選択します。このグループで利用可能なすべてのアプリケーションが表示される**アプリケーション**ノードに移動します。
4. このグループにアプリケーションを追加するには、**デリバリーグループ**ノードに移動し、グループを選択して、アクションバーで**アプリケーションの追加**を選択します。

VDA上のCitrix Secure Access™ Clientからのシームレスなログオン

VDAに存在するCitrix Secure Access (CSA) クライアントからCitrix Secure Private Accessへのシングルサインオン (SSO) を使用して、Citrix Workspaceにシームレスにログオンできます。この機能は、シングルセッションVDAとマルチセッションVDAの両方に適用されます。

これを実現する手順は次のとおりです。

1. 既存のデリバリーグループを編集してSPA SSOを有効にします。例:

```
Set-BrokerDesktopGroup -Name &lt;String> -SpaSsoEnabled 1
```

2. Get -BrokerDesktopGroup PowerShellコマンドを使用して、デリバリーグループのSPA SSOのステータスを確認します。例:

```
Get-BrokerDesktopGroup -Name &lt;String> -property 'SpaSsoEnabled'
```

3. SPAで、アプリケーションとポリシーを作成します。TCP/UDPアプリの構成およびアプリケーションのアクセスポリシーの構成を参照してください。
4. シングルセッションまたはマルチセッションVDAにRDP接続し、最新のCSAエージェントをインストールします。
5. Citrix Workspace を開き、シングルセッションまたはマルチセッションVDAにログオンします。

トラブルシューティング

- Delivery Controllerに登録されていないVDAは、ブローカーセッションの起動時に考慮されません。これにより、利用可能なはずのリソースが十分に活用されないことになります。VDAが登録されない理由はさまざまであり、その多くは管理者がトラブルシューティングできます。詳細表示には、カタログ作成ウィザードと、デリバリーグループにカタログを追加した後のトラブルシューティング情報が表示されます。

  デリバリーグループを作成した後、デリバリーグループの詳細ペインには、登録可能だが登録されていないマシンの数が表示されます。たとえば、1台以上のマシンが電源オンでメンテナンスモードではないが、現在Controllerに登録されていない場合などです。「登録されていないが、登録されるべき」マシンを表示するときは、詳細ペインの**トラブルシューティング**タブで考えられる原因と推奨される是正措置を確認してください。

  機能レベルに関するメッセージについては、VDAのバージョンと機能レベルを参照してください。

  VDA登録のトラブルシューティングについては、CTX136668を参照してください。
- デリバリーグループの表示では、詳細ペインの**インストールされているVDAバージョン**が、マシンに実際にインストールされているバージョンと異なる場合があります。マシンのWindowsのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- **電源状態不明**のマシンについては、CTX131267を参照してください。

アプリケーショングループの作成

> **注:**

> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

アプリケーショングループを使用すると、アプリケーションのコレクションを管理できます。異なるデリバリーグループ間で共有されるアプリケーション、またはデリバリーグループ内のユーザーのサブセットによって使用されるアプリケーションに対して、アプリケーショングループを作成します。アプリケーショングループはオプションであり、同じアプリケーションを複数のデリバリーグループに追加する代わりに利用できます。デリバリーグループを複数のアプリケーショングループに関連付けたり、アプリケーショングループを複数のデリバリーグループに関連付けたりできます。

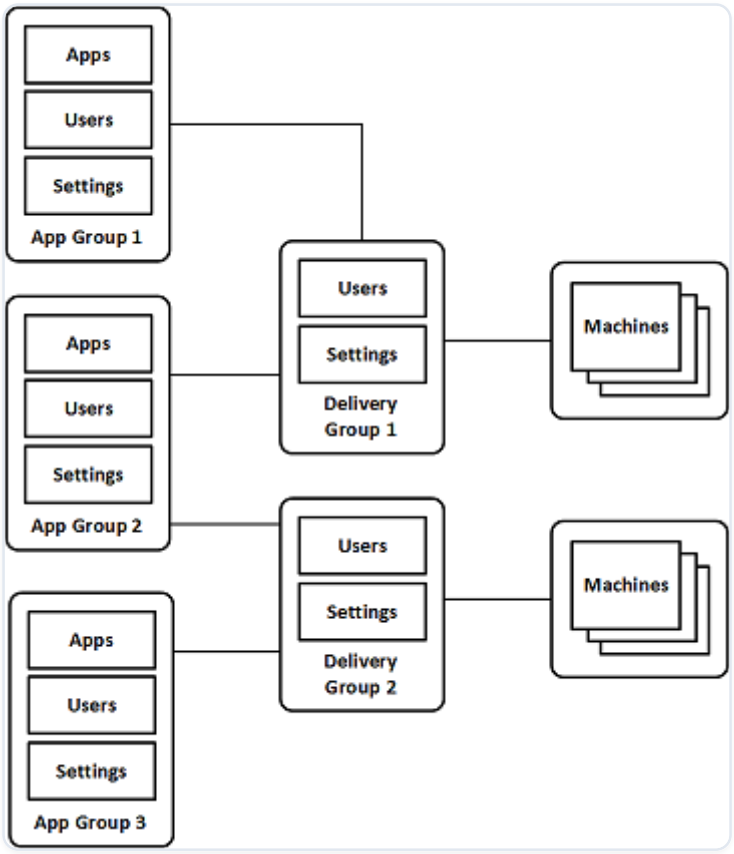
アプリケーショングループを使用すると、より多くのデリバリーグループを使用する場合と比較して、アプリケーション管理とリソース制御の利点が得られます。

- アプリケーションとその設定を論理的にグループ化することで、それらのアプリケーションを単一の単位として管理できます。たとえば、同じアプリケーションを個々のデリバリーグループに一度に1つずつ追加（公開）する必要はありません。
- アプリケーショングループ間のセッション共有により、リソース消費を節約できます。その他のケースでは、アプリケーショングループ間のセッション共有を無効にすることが有益な場合があります。
- タグ制限機能を使用すると、選択したデリバリーグループ内のマシンのサブセットのみを考慮して、アプリケーショングループからアプリケーションを公開できます。タグ制限を使用すると、既存のマシンを複数の公開タスクに使用できるため、追加のマシンを展開および管理するコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）するものと考えることができます。タグ制限のあるアプリケーショングループまたはデスクトップを使用すると、デリバリーグループ内のマシンのサブセットを分離してトラブルシューティングする際に役立ちます。

構成例

例 1:

以下の図は、アプリケーショングループを含むCitrix Virtual Apps™ and Desktopsの展開を示しています。



この構成では、アプリケーションはデリバリーグループではなくアプリケーショングループに追加されます。デリバリーグループは、どのマシンが使用されるかを指定します。（図には示されていませんが、マシンはマシンカタログ内にあります。）

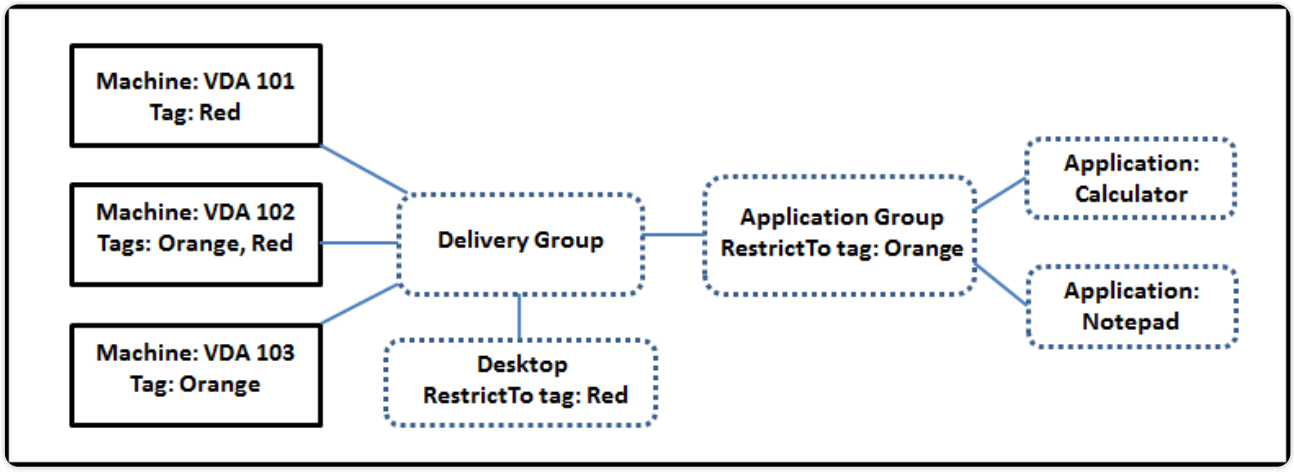
アプリケーショングループ1はデリバリーグループ1に関連付けられています。アプリケーショングループ1のアプリケーションには、アプリケーショングループ1で指定されたユーザーがアクセスします。これらのグループは、デリバリーグループ1のユーザーリストにも含まれている場合にのみ表示されます。この構成は、アプリケーショングループのユーザーリストが、関連付けられたデリバリーグループのユーザーリストのサブセット（制限）であるというガイダンスに従います。アプリケーショングループ1の設定（アプリケーショングループ間のアプリケーションセッション共有、関連付けられたデリバリーグループなど）は、そのグループ内のアプリケーションとユーザーに適用されます。デリバリーグループ1の設定は、アプリケーショングループ1と2がそのデリバリーグループに関連付けられているため、それらのアプリケーショングループのユーザーに適用されます。

アプリケーショングループ2は、2つのデリバリーグループ（1と2）に関連付けられています。これらの各デリバリーグループには、アプリケーショングループ2内で優先度が割り当てられ、アプリケーションが起動されたときにデリバリーグループがチェックされる順序を示します。優先度が同じデリバリーグループはロードバランスされます。アプリケーショングループ2で指定されたユーザーは、アプリケーショングループ2内のアプリケーションにアクセスできます。ただし、そ

れらのユーザーはデリバリーグループ1とデリバリーグループ2のユーザーリストにも表示されている必要があります。

例 2:

このシンプルなレイアウトでは、タグ制限を使用して、特定のデスクトップおよびアプリケーションの起動にどのマシンが考慮されるかを制限します。このサイトには、1つの共有デリバリーグループ、1つの公開デスクトップ、および2つのアプリケーションで構成された1つのアプリケーショングループがあります。



3台のマシン（VDA 101～103）のそれぞれにタグが追加されています。

アプリケーショングループは「Orange」タグ制限で作成されました。その各アプリケーションは、そのデリバリーグループ内で「Orange」タグを持つマシン（VDA 102および103）でのみ起動されます。

アプリケーショングループ（およびデスクトップ）でタグ制限を使用するためのより包括的な例とガイダンスについては、「タグ」を参照してください。

ガイダンスと考慮事項

Citrixでは、アプリケーションをアプリケーショングループまたはデリバリーグループのいずれかに追加し、両方には追加しないことをお勧めします。そうしないと、2つのグループタイプにアプリケーションが存在することによる複雑さが増し、管理がより困難になる可能性があります。

デフォルトでは、アプリケーショングループは有効になっています。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

デフォルトでは、アプリケーショングループ間のアプリケーションセッション共有は有効になっています。「アプリケーショングループ間のセッション共有」を参照してください。

Citrixでは、デリバリーグループを現在のバージョンにアップグレードすることをお勧めします。このプロセスには以下が必要です。

1. デリバリーグループで使用されているマシン上のVDAをアップグレードする。
2. それらのマシンを含むマシンカタログのアップグレード。
3. デリバリーグループのアップグレード。

詳細については、Manage delivery groupsを参照してください。

アプリケーショングループを使用するには、コアコンポーネントがバージョン7.9以降である必要があります。

アプリケーショングループを作成するには、Delivery Group Administratorの組み込みロールの委任管理権限が必要です。詳細については、Delegated administrationを参照してください。

この記事では、アプリケーションを複数のアプリケーショングループに「関連付ける」ことについて説明します。これは、利用可能なソースからそのアプリケーションのインスタンスを追加する操作とは異なります。同様に、デリバリーグループは、互いの追加やコンポーネントではなく、アプリケーショングループに関連付けられます。

アプリケーショングループでのセッション共有

アプリケーションセッション共有が有効になっている場合、すべてのアプリケーションは同じアプリケーションセッションで起動します。これにより、より多くのアプリケーションセッションを起動するコストが削減され、コピー＆ペースト操作など、クリップボードを使用するアプリケーション機能を利用できるようになります。ただし、状況によってはセッション共有をクリアできます。

アプリケーショングループを使用する場合、アプリケーションセッション共有を次の3つの方法で構成できます。これらは、デリバリーグループのみを使用する場合に利用できる標準のセッション共有動作を拡張するものです。

- アプリケーショングループ間でのセッション共有が有効。
- 同じアプリケーショングループ内のアプリケーション間でのみセッション共有が有効。
- セッション共有が無効。

アプリケーショングループ間のセッション共有

アプリケーショングループ間でアプリケーションセッション共有を有効にすることも、または、同じアプリケーショングループ内のアプリケーションのみにアプリケーションセッション共有を制限するために無効にすることもできます。

- **アプリケーショングループ間のセッション共有を有効にすることが役立つ例:**

  アプリケーショングループ1には、WordやExcelなどのMicrosoft Officeアプリケーションが含まれています。アプリケーショングループ2には、メモ帳や電卓などの他のアプリケーションが含まれており、両方のアプリケーショングループは同じデリバリーグループにアタッチされています。両方のアプリケーショングループにアクセスできるユーザーが、Wordを起動してアプリケーションセッションを開始し、次にメモ帳を起動します。コントローラーが、ユーザーの既存のWord実行セッションがメモ帳の実行に適していると判断した場合、メモ帳は既存のセッション内で起動されます。既存のセッションからメモ帳を実行できない場合（たとえば、タグ制限によってセッションが実行されているマシンが除外されている場合など）、セッション共有を使用するのではなく、適切なマシン上に新しいセッションが作成されます。

- **アプリケーショングループ間のセッション共有を無効にすることが役立つ例:**

  同じマシンにインストールされている他のアプリケーションとうまく相互運用できないアプリケーションのセットを含む構成。たとえば、同じソフトウェアスイートの2つの異なるバージョン、または同じWebブラウザの2つの異なるバージョンなどです。ユーザーが同じセッションで両方のバージョンを起動することを許可しない方がよいでしょう。

  ソフトウェアスイートの各バージョンに対してアプリケーショングループを作成し、各バージョンのアプリケーションを対応するアプリケーショングループに追加します。これらのアプリケーショングループのそれぞれでグループ間のセッション共有が無効になっている場合、それらのグループで指定されたユーザーは、同じセッションで同じバージョンのアプリケーションを実行できます。ユーザーは同時に他のアプリケーションを実行できますが、同じセッションでは実行できません。異なるバージョンのアプリケーション、またはアプリケーショングループに含まれていないアプリケーションを起動すると、そのアプリケーションは新しいセッションで起動されます。

このアプリケーショングループ間のセッション共有機能は、セキュリティサンドボックス機能ではありません。これは完璧ではなく、ユーザーが他の手段（たとえば、Windows Explorer経由など）でアプリケーションをセッションに起動するのを防ぐことはできません。

マシンが容量に達している場合、新しいセッションは開始されません。必要に応じて、セッション共有を使用して、マシンの既存のセッションで新しいアプリケーションが開始されます。

アプリケーションセッション共有が許可されているアプリケーショングループに対してのみ、プレローンチセッションを利用可能にできます。（セッションリンガー機能を使用するセッションは、すべてのアプリケーショングループで利用可能です。）これらの機能は、アプリケーショングループに関連付けられている各デリバリーグループで有効にして構成する必要があります。アプリケーショングループでは構成できません。

デフォルトでは、アプリケーショングループを作成すると、アプリケーショングループ間のアプリケーションセッション共有が有効になります。グループ作成時にこれを変更することはできません。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/application-groups-manage.html)を参照してください。

アプリケーショングループ内のセッション共有を無効にする

同じアプリケーショングループ内のアプリケーション間でアプリケーションセッション共有を防止できます。

- **アプリケーショングループ内のセッション共有を無効にすることが役立つ例:**

  ユーザーに、別々のモニターでアプリケーションの複数の同時フルスクリーンセッションにアクセスさせたい場合。

  アプリケーショングループを作成し、そこにアプリケーションを追加します。

デフォルトでは、アプリケーショングループを作成すると、アプリケーションセッション共有が有効になります。グループ作成時にこの設定を変更することはできません。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/application-groups-manage.html)を参照してください。

アプリケーショングループを作成する

アプリケーショングループを作成するには：

1. Web Studioにサインインします。
2. 左ペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
3. フォルダーを使用してアプリケーショングループを整理するには、**アプリケーショングループ**ルートフォルダーの下にフォルダーを作成します。詳しくは、「フォルダーを使用したアプリケーショングループの整理」を参照してください。
4. グループを作成するフォルダーを選択し、**アプリケーショングループの作成**をクリックします。グループ作成ウィザードが**はじめに**ページで起動します。このページは、次回以降のウィザード起動時に表示しないように設定できます。
5. ウィザードに従って、以下に説明するページで設定を構成します。各ページでの設定が完了したら、**概要**ページに到達するまで**次へ**を選択します。

手順1. デリバリーグループ

デリバリーグループページには、すべてのデリバリーグループと、各グループに含まれるマシンの数が一覧表示されます。

- **互換性のあるデリバリーグループ**の一覧には、選択可能なデリバリーグループが含まれます。互換性のあるデリバリーグループには、ランダム（永続的または静的に割り当てられていない）なマルチセッションまたはシングルセッションOSマシンが含まれます。
- **互換性のないデリバリーグループ**の一覧には、選択できないデリバリーグループが含まれます。各エントリには、静的に割り当てられたマシンが含まれるなど、互換性がない理由が説明されています。

アプリケーショングループは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。

以下の両方の条件が満たされている場合、デスクトップのみを配信する共有マシンを含むデリバリーグループも選択できます。

- デリバリーグループに共有マシンが含まれており、XenDesktopバージョン7.9より前のバージョンで作成されている。
- デリバリーグループの編集権限がある。

アプリケーショングループ作成ウィザードがコミットされると、デリバリーグループの種類は自動的に「デスクトップとアプリケーション」に変換されます。

関連付けられたデリバリーグループがないアプリケーショングループを作成できますが（アプリケーションを整理するため、または現在使用されていないアプリケーションのストレージとして機能させるためなど）、少なくとも1つのデリバリーグループが指定されるまで、そのアプリケーショングループをアプリケーションの配信に使用することはできません。また、デリバリーグループが指定されていない場合、**スタートメニューから**ソースからアプリケーショングループにアプリケーションを追加することはできません。

選択したデリバリーグループは、アプリケーションの配信に使用されるマシンを指定します。アプリケーショングループに関連付けるデリバリーグループの横にあるチェックボックスをオンにします。

タグ制限を追加するには、「**タグを持つマシンへの起動を制限する**」を選択し、ドロップダウンリストからタグを選択します。

手順2. ユーザー

アプリケーショングループでアプリケーションユーザーを指定します。前のページで選択したデリバリーグループ内のすべてのユーザーとユーザーグループを許可するか、それらのデリバリーグループから特定のユーザーとユーザーグループを選択します。指定されたユーザーに利用を制限する場合、デリバリーグループで指定されたユーザーのうち、アプリケーショングループで指定されたユーザーのみが、このグループのアプリケーションにアクセスできます。基本的に、アプリケーショングループのユーザーリストは、デリバリーグループのユーザーリストに対するフィルターとして機能します。

認証されていないユーザーによるアプリケーションの使用の有効化または無効化は、アプリケーショングループではなく、デリバリーグループでのみ利用できます。

展開でユーザーリストがどこに指定されているかについては、「ユーザーリストの指定場所」を参照してください。

ステップ3. アプリケーション

知っておくと良いこと:

- デフォルトでは、追加する新しいアプリケーションは**アプリケーション**という名前のフォルダーに配置されます。別のフォルダーを指定することもできます。アプリケーションを追加しようとしたときに、同じ名前のアプリケーションがそのフォルダーに存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。提案された一意の名前に同意すると、その新しい名前でアプリケーションが追加されます。そうでない場合は、追加する前に自分で名前を変更する必要があります。詳細については、「アプリケーションフォルダーの管理」を参照してください。
- アプリケーションのプロパティ（設定）は、追加時または後で変更できます。「アプリケーションプロパティの変更」を参照してください。同じ名前の2つのアプリケーションを同じユーザーに公開する場合、Web Studioで**アプリケーション名（ユーザー向け）**プロパティを変更してください。そうしないと、ユーザーはCitrix Workspaceアプリで重複した名前を目にすることになります。
- アプリケーションを複数のアプリケーショングループに追加する場合、それらのすべてのグループでアプリケーションを表示するのに十分な権限がないと、表示の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが追加されたすべてのグループを含むようにスコープを拡張してください。

アプリケーションソースを表示するには、ドロップダウンメニューから「**追加**」をクリックします。

- **スタートメニューから:** 選択したデリバリーグループ内のマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスを選択し、**OK**をクリックします。

  以下のいずれかを選択した場合、このソースは選択できません。

  - 関連付けられたデリバリーグループがないアプリケーショングループ。
  - 関連付けられたデリバリーグループにマシンが含まれていないアプリケーショングループ。
  - マシンが含まれていないデリバリーグループ。

- **手動で定義:** サイト内またはネットワーク内の別の場所にあるアプリケーション。このソースを選択すると、新しいページが起動し、実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、および管理者とユーザーの表示名を入力します。この情報を入力したら、**OK**をクリックします。
- **既存:** 以前にサイトに追加されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。追加するアプリケーションのチェックボックスを選択し、**OK**をクリックします。サイトにアプリケーションがない場合、このソースは選択できません。
- **App-V:** App-Vパッケージ内のアプリケーション。このソースを選択すると、新しいページが起動し、そこで**App-V server**または**Application Library**を選択します。表示されたリストから、追加するアプリケーションのチェックボックスを選択し、**OK**をクリックします。詳細については、「App-Vアプリケーションの展開と配信」を参照してください。App-Vがサイト用に構成されていない場合、このソースは選択できません（または表示されない場合があります）。

前述のとおり、「**追加**」ドロップダウンメニューの一部のエントリは、そのタイプの有効なソースがない場合、選択できません。互換性のないソースはまったくリストされません（たとえば、アプリケーショングループにアプリケーショングループを追加することはできないため、アプリケーショングループを作成する際にはそのソースはリストされません）。

ステップ4. スコープ

このページは、以前にカスタムスコープを作成した場合にのみ表示されます。デフォルトでは、**すべて**のスコープが選択されています。詳細については、「委任管理」を参照してください。

ステップ5. 概要

アプリケーショングループの名前を入力します。説明を（オプションで）入力することもできます。

概要情報を確認し、**「完了」**をクリックします。

アプリケーショングループの管理

> **注:**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

この記事では、作成したアプリケーショングループを管理する方法について説明します。

アプリケーショングループまたはデリバリーグループでアプリケーションを管理する方法については、アプリケーションを参照してください。これには、次の方法が含まれます。

- アプリケーショングループ内のアプリケーションを追加または削除する。
- アプリケーショングループの関連付けを変更する。

アプリケーショングループの管理には、Delivery Group Administratorの組み込みロールの委任管理権限が必要です。詳細については、委任管理を参照してください。

アプリケーショングループを有効または無効にする

アプリケーショングループが有効になっている場合、そのグループに追加されたアプリケーションを配信できます。アプリケーショングループを無効にすると、そのグループ内の各アプリケーションが無効になります。ただし、それらのアプリケーションが他の有効なアプリケーショングループにも関連付けられている場合、それらの他のグループから配信できます。アプリケーションがアプリケーショングループに関連付けられたデリバリーグループに明示的に追加された場合、アプリケーショングループを無効にしても、それらのデリバリーグループ内のアプリケーションには影響しません。

アプリケーショングループは作成時に有効になります。グループ作成時にこの構成を変更することはできません。

1. 左ペインで**「アプリケーション」**を選択し、**「アプリケーショングループ」**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**「アプリケーショングループの編集」**を選択します。
3. **「設定」**ページで、**「アプリケーショングループを有効にする」**チェックボックスをオンまたはオフにします。
4. ウィンドウを開いたままにするには**適用**をクリックし、変更を適用してウィンドウを閉じるには**保存**をクリックします。

アプリケーショングループ間のアプリケーションセッション共有を有効または無効にする

アプリケーショングループ間のセッション共有は、アプリケーショングループの作成時に有効になります。グループの作成時にこの構成を変更することはできません。詳細については、「アプリケーショングループとのセッション共有」を参照してください。

1. 左ペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **設定**ページで、**アプリケーショングループ間のアプリケーションセッション共有を有効にする**チェックボックスをオンまたはオフにします。
4. ウィンドウを開いたままにするには**適用**をクリックし、変更を適用してウィンドウを閉じるには**保存**をクリックします。

アプリケーショングループ内でのアプリケーションセッション共有を無効にする

同じアプリケーショングループ内のアプリケーション間でのセッション共有は、アプリケーショングループの作成時にデフォルトで有効になります。アプリケーショングループ間でのアプリケーションセッション共有を無効にしても、同じアプリケーショングループ内のアプリケーション間でのセッション共有は有効のままです。

PowerShell SDKを使用して、アプリケーショングループに含まれるアプリケーション間のアプリケーションセッション共有を無効にしたアプリケーショングループを構成できます。状況によっては、このオプションが望ましい場合があります。たとえば、ユーザーにシームレスではないアプ

リケーションを別々のモニターで全画面表示のアプリケーションウィンドウで起動させたい場合があります。

アプリケーショングループ内でアプリケーションセッション共有を無効にすると、そのグループ内の各アプリケーションは新しいアプリケーションセッションで起動します。同じアプリケーションを実行している適切な切断されたセッションが利用可能な場合、そのセッションは再接続されます。たとえば、メモ帳を実行している切断されたセッションでメモ帳を起動する場合、新しいセッションを作成する代わりにそのセッションが再接続されます。複数の適切な切断されたセッションが利用可能な場合、ランダムではあるが決定論的な方法で、いずれかのセッションが再接続のために選択されます。同じ状況でこの状況が再発生した場合、同じセッションが選択されますが、それ以外の場合、セッションは必ずしも予測可能ではありません。

PowerShell SDKを使用して、既存のアプリケーショングループ内のすべてのアプリケーションのアプリケーションセッション共有を無効にするか、アプリケーションセッション共有を無効にしたグループを作成します。

PowerShellコマンドレットの例

セッション共有を無効にするには、Broker PowerShellコマンドレット `New-BrokerApplicationGroup` または `Set-BrokerApplicationGroup` を使用し、パラメーター `SessionSharingEnabled` を `False` に、パラメーター `SingleAppPerSession` を `True` に設定します。

- たとえば、グループ内のすべてのアプリケーションでアプリケーションセッション共有が無効になっているアプリケーショングループを作成するには：

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False
  -SingleAppPerSession $True
  ```

- 例えば、既存のアプリケーショングループ内のすべてのアプリケーション間でアプリケーションセッション共有を無効にするには、次のようにします。

  ```
  Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False
  -SingleAppPerSession $True
  ```

考慮事項

- `SingleAppPerSession` プロパティを有効にするには、`SessionSharingEnabled` プロパティを False に設定する必要があります。これら2つのプロパティを同時に有効にすることはできません。`SessionSharingEnabled` パラメーターは、アプリケーショングループ間のセッション共有を指します。

- アプリケーションセッション共有は、アプリケーショングループに関連付けられているがデリバリーグループには関連付けられていないアプリケーションでのみ機能します。デリバリーグループに直接関連付けられているすべてのアプリケーションは、デフォルトでセッションを共有します。
- アプリケーションが複数のアプリケーショングループに割り当てられている場合、グループの設定が競合しないようにしてください。たとえば、あるグループのオプションが `True` に設定され、別のグループのオプションが `False` に設定されている場合、予期しない動作が発生します。

アプリケーショングループの名前を変更する

1. 左ペインで を選択し、 タブを選択します。
2. アプリケーショングループを選択し、アクションバーで を選択します。
3. 新しい一意の名前を指定し、 をクリックします。

アプリケーショングループとのデリバリーグループ関連付けの追加、削除、または優先順位の変更

アプリケーショングループは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。

以下の両方の条件が満たされている場合、デスクトップのみを配信する共有マシンを含むデリバリーグループを選択することもできます。

- デリバリーグループに共有マシンが含まれており、バージョン7.9より前に作成されている。
- 「デリバリーグループの編集」権限を持っている必要があります。

ダイアログがコミットされると、デリバリーグループの種類は自動的に「デスクトップとアプリケーション」に変換されます。

1. 左ペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **デリバリーグループ**ページを選択します。
4. デリバリーグループを追加するには、**追加**をクリックします。利用可能なデリバリーグループのチェックボックスをオンにします。(互換性のないデリバリーグループは選択できません。) 選択が完了したら、**OK**をクリックします。

5. デリバリーグループを削除するには、削除するグループのチェックボックスをオンにして、**削除**をクリックします。プロンプトが表示されたら削除を確定します。
6. デリバリーグループの優先度を変更するには、デリバリーグループのチェックボックスをオンにして、**優先度の編集**をクリックします。優先度 (0 = 最高) を入力し、**OK**をクリックします。
7. 加えた変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。変更を適用してウィンドウを閉じるには、**保存**をクリックします。

アプリケーショングループのタグ制限を追加、変更、または削除する

タグ制限の追加、変更、削除は、アプリケーション起動の対象となるマシンに予期せぬ影響を与える可能性があります。タグの考慮事項と注意点を確認してください。

1. 左側のペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **デリバリーグループ**ページを選択します。
4. タグ制限を追加するには、**タグを持つマシンへの起動を制限する**を選択し、ドロップダウンリストからタグを選択します。
5. タグ制限を変更または削除するには、別のタグを選択するか、**Restrict launches to machines with this tag** のチェックを外してタグ制限を完全に削除します。
6. 加えた変更を適用してウィンドウを開いたままにするには **Apply** をクリックし、変更を適用してウィンドウを閉じるには **Save** をクリックします。

アプリケーショングループのユーザーを追加または削除する

ユーザーの詳細については、「アプリケーショングループの作成」を参照してください。

1. 左ペインで **Applications** を選択し、**Application Groups** タブを選択します。
2. アプリケーショングループを選択し、アクションバーで **Edit Application Group** を選択します。
3. **Users** ページを選択します。関連付けられているデリバリーグループのすべてのユーザーにアプリケーショングループ内のアプリケーションの使用を許可するか、特定のユーザーとグループのみに許可するかを指定します。ユーザーを追加するには、**Add** をクリックし、追加するユーザーを指定します。ユーザーを削除するには、1人以上のユーザーを選択し、**Remove** をクリックします。
4. 加えた変更を適用してウィンドウを開いたままにするには **Apply** をクリックし、変更を適用してウィンドウを閉じるには **Save** をクリックします。

アプリケーショングループでアプリケーションアイコンを追加、変更、または削除する

アプリケーションアイコンを追加、変更、または削除するには、次の手順を実行します。

1. 左ペインで **Applications** を選択します。
2. **Applications** タブで、アプリケーションを選択し、**Properties** を選択します。

   アプリケーショングループレベルで変更を行うには、**Application Groups** タブに移動し、グループ内のアプリケーションを選択して、**Properties** を選択します。
3. **Delivery** ページを選択し、**Change** を選択します。**Select Icon** ウィンドウが表示されます。
4. **Select Icon** ウィンドウで、次のいずれかを実行します。

   - アイコンを追加するには、**追加**を選択し、アイコンを参照します。
   - アイコンを削除するには、アイコンを選択してから**削除**を選択します。
   - アイコンを変更するには、アプリケーションのアイコンを選択します。

   > **重要：**
   >
   > - サイズが200 KBを超えるアイコンは追加できません。
   > - .iconファイルのみ追加できます。
   > - 組み込みアイコンは削除できません。
   > - 使用中のアプリケーションのアイコンは削除できません。

5. 変更を適用してウィンドウを閉じるには、**保存**を選択します。

アプリケーショングループのスコープを変更する

スコープは、作成した場合にのみ変更できます（「すべてのスコープ」は編集できません）。詳しくは、「委任管理」を参照してください。

1. 左ペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **スコープ**ページを選択します。スコープの横にあるチェックボックスをオンまたはオフにします。

4. 行った変更を適用してウィンドウを開いたままにするには**適用**をクリックし、変更を適用してウィンドウを閉じるには**保存**をクリックします。

アプリケーショングループのスコープを変更する

スコープは、作成した場合にのみ変更できます (すべてのスコープは編集できません)。詳細については、「委任管理」を参照してください。

1. 左側のペインで を選択し、次に タブを選択します。
2. アプリケーショングループを選択し、次にアクションバーで を選択します。
3. ページを選択します。変更するスコープの横にあるチェックボックスをオンまたはオフにします。
4. 加えた変更を適用してウィンドウを開いたままにするには、 を選択します。または、変更を適用してウィンドウを閉じるには、 を選択します。

アプリケーショングループを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに関連付けられている必要があります。アプリケーショングループを削除した結果、1つ以上のアプリケーションがどのグループにも属さなくなる場合、そのグループを削除するとそれらのアプリケーションも削除されるという警告が表示されます。その後、削除を確定またはキャンセルできます。

アプリケーションを削除しても、元のソースから削除されるわけではありません。ただし、再度利用可能にする場合は、再度追加する必要があります。

1. 左ペインで**アプリケーション**を選択し、**アプリケーション グループ**タブを選択します。
2. アプリケーション グループを選択し、アクション バーで**グループの削除**を選択します。
3. プロンプトが表示されたら、削除を確定します。

フォルダーを使用してアプリケーション グループを整理する

フォルダーを作成してアプリケーション グループを整理し、簡単にアクセスできるようにすることができます。

必要な役割

デフォルトでは、以下の組み込みロールのいずれかを持っている場合、アプリケーション グループのフォルダーを作成および管理できます。

- クラウド管理者
- フル管理者

- アプリケーション グループ管理者

カスタム ロールを作成することで、管理アクションを他のユーザーに委任できます。次の表に、各アクションに必要な権限を示します。

アクション	必要な権限
アプリケーション グループ フォルダーの作成	アプリケーション グループ フォルダーの作成
アプリケーション グループ フォルダーの削除	アプリケーション グループ フォルダーの削除
アプリケーション グループ フォルダーの移動	アプリケーション グループ フォルダーの移動
アプリケーショングループフォルダーの名前を変更	アプリケーショングループフォルダーの編集
アプリケーショングループをフォルダーに移動	アプリケーショングループフォルダーの編集、アプリケーショングループプロパティの編集

詳しくは、「役割の作成と管理」を参照してください。

フォルダーの作成と管理

アクションバーまたは右クリックメニューを使用して、アプリケーショングループフォルダーを作成および管理できます。さらに、アプリケーショングループまたはフォルダーをフォルダーツリー内の目的の場所にドラッグすることもできます。

知っておくと良いこと:

- フォルダーは最大5レベルまでネストできます (デフォルトのルートフォルダーを除く)。
- フォルダーには、アプリケーショングループとサブフォルダーを含めることができます。フォルダーは、そのフォルダーとサブフォルダーにアプリケーショングループが含まれていない場合にのみ削除できます。
- Web Studioのすべてのノード（例: **マシンカタログ**、**デリバリーグループ**、**アプリケーション**、**アプリケーショングループ**）は、バックエンドで同じフォルダーツリーを共有します。フォルダーの名前変更または移動時に名前の競合を避けるため、異なるノード間で、最上位フォルダーに一意の名前を使用してください。

  `New-BrokerAdminFolder` SDKコマンドレットを使用してフォルダーを作成し、それを**アプリケーショングループ**ノードの下に表示させたい場合は、`Set-`

`BrokerAdminFolderMetadata` コマンドレットを使用して `ContainsApplicationGroups` メタデータを追加する必要があります。

例:

```
Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
ContainsApplicationGroups -Value true
```

リモートPCアクセス

注:

バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

リモートPCアクセスは、Citrix Virtual Apps™ and Desktopsの機能であり、組織が従業員に企業リソースへのリモートアクセスを安全に簡単に許可できるようにします。Citrixプラットフォームは、ユーザーが物理的なオフィスPCにアクセスできるようにすることで、この安全なアクセスを可能にします。ユーザーがオフィスPCにアクセスできれば、仕事に必要なすべてのアプリケーション、データ、リソースにアクセスできます。リモートPCアクセスは、テレワークに対応するための他のツールの導入や提供の必要性を排除します。たとえば、仮想デスクトップやアプリケーション、およびそれらに関連するインフラストラクチャなどです。

リモートPCアクセスは、仮想デスクトップとアプリケーションを提供するCitrix Virtual Apps and Desktopsのコンポーネントと同じものを使用します。その結果、リモートPCアクセスの展開と構成の要件およびプロセスは、仮想リソースを提供するためのCitrix Virtual Apps and Desktopsの展開に必要なものと同じです。この統一性により、一貫性のある統合された管理エクスペリエンスが提供されます。ユーザーは、Citrix HDX™を使用してオフィスPCセッションを配信することで、最高のユーザーエクスペリエンスを得られます。

この機能は、**リモートPCアクセス**タイプのマシンカタログで構成されており、以下の機能を提供します。

- OUを指定してマシンを追加する機能。この機能により、PCの一括追加が容易になります。

- オフィスWindows PCにログオンするユーザーに基づいた自動ユーザー割り当て。シングルユーザーおよび複数ユーザーの割り当てをサポートしています。デフォルトでは、次に割り当てられていないマシンに複数のユーザーが自動的に割り当てられます。自動割り当てをシングルユーザーに制限するには、Web Studioにサインインし、**設定**に移動して、**リモートPCアクセスでの複数ユーザーの自動割り当てを有効にする**設定をオフにします。

Citrix Virtual Apps and Desktopsは、他の種類のマシンカタログを使用することで、物理PCのより多くのユースケースに対応できます。これらのユースケースには以下が含まれます。

- 物理Linux PC
- プールされた物理PC（つまり、ランダムに割り当てられ、専用ではない）

> **注:**
>
> サポートされているOSバージョンの詳細については、シングルセッションOSおよびLinux VDAのVDAのシステム要件を参照してください。

> オンプレミス展開の場合、リモートPCアクセスはCitrix Virtual Apps and Desktops AdvancedまたはPremiumライセンスでのみ有効です。セッションは、他のCitrix Virtual Desktops™セッションと同じ方法でライセンスを消費します。Citrix Cloudの場合、リモートPCアクセスはCitrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）およびWorkspace Premium Plusで有効です。

考慮事項

Citrix Virtual Apps and Desktops全般に適用されるすべての技術要件と考慮事項はRemote PC Accessにも適用されますが、物理PCのユースケースにより関連性が高い、または排他的なものもあります。

> **重要:**
>
> Windows 11物理システム（および一部のWindows 10を実行しているシステム）には、仮想化ベースのセキュリティ機能が含まれており、その結果、VDAソフトウェアがそれらを仮想マシンとして誤って検出します。この問題を軽減するには、以下のオプションがあります。

- VDAコマンドラインインストールの一部として、「/remotepc」オプションとともに「/physicalmachine」オプションを使用する
- 前述のオプションを使用しなかった場合は、VDAのインストール後に次のレジストリ値を追加します `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
  - 名前: ForceEnableRemotePC
  - 種類: DWORD
  - データ: 1

展開に関する考慮事項

Remote PC Accessの展開を計画する際には、いくつかの一般的な決定を行う必要があります。

- 既存のCitrix Virtual Apps and Desktops展開にRemote PC Accessを追加できます。このオプションを選択する前に、次の点を考慮してください。
  - 現在のDelivery ControllerまたはCloud Connectorは、Remote PC Access VDAに関連する追加の負荷をサポートするのに適切なサイズですか？
  - オンプレミスサイトのデータベースおよびデータベースサーバーは、Remote PC Access VDAに関連する追加の負荷をサポートするのに適切なサイズですか？
  - 既存のVDAと新しいRemote PC Access VDAの合計が、サイトごとにサポートされる最大VDA数を超えることはありませんか？
- VDAは、自動化されたプロセスを通じてオフィスPCに展開する必要があります。利用可能なオプションは次のとおりです。
  - SCCMなどの電子ソフトウェア配信 (ESD) ツール: SCCMを使用してVDAをインストールする。
  - 展開スクリプト: スクリプトを使用してVDAをインストールする。
- Remote PC Accessのセキュリティに関する考慮事項を確認してください。

注：

Remote PC Access を設計する際には、リモート PC の GPU に接続され、現在構成/動作している物理モニターの数を考慮する必要があります。モニターが Citrix セッションで使用さ

れていなくても、GPU によって検出された場合、そのモニターの存在は GPU がサポートする最大モニター数制限にカウントされます。

マシンカタログに関する考慮事項

必要なマシンカタログの種類は、ユースケースによって異なります。

- Remote PC Accessマシンカタログ
  - Windows専用PC
  - Windows専用マルチユーザーPC。このユースケースは、複数のユーザーが異なるシフトでリモートからアクセスできる物理的なオフィスPCに適用されます。
  - プールされたWindows PC。このユースケースは、コンピューターラボのように、複数のランダムなユーザーがアクセスできる物理PCに適用されます。
- シングルセッションOSマシンカタログ
  - 静的 - 専用Linux PC
  - ランダム - プールされたLinux PC

マシンカタログの種類を特定したら、次の点を考慮してください。

- マシンは一度に1つのマシンカタログにのみ割り当てることができます。
- 委任管理を容易にするために、地理的な場所、部門、または各カタログの管理を適切な管理者に委任しやすくするその他のグループに基づいてマシンカタログを作成することを検討してください。
- マシンアカウントが存在するOUを選択する際は、より詳細な粒度を得るために下位レベルのOUを選択してください。そのような粒度が必要ない場合は、上位レベルのOUを選択できます。たとえば、Bank/Officers/Tellers の場合、より詳細な粒度を得るには **Tellers** を選択します。それ以外の場合は、要件に基づいて **Officers** または **Bank** を選択できます。
- Remote PC Access マシンカタログに割り当てられた後にOUを移動または削除すると、VDAの関連付けに影響を与え、将来の割り当てで問題が発生します。したがって、マシンカタログのOU割り当ての更新がActive Directoryの変更計画に考慮されるように、適切に計画してください。
- OU構造のためにマシンカタログにマシンを追加するOUを選択するのが難しい場合、OUを選択する必要はありません。後でPowerShellを使用してカタログにマシンを追加できます。デスクトップの割り当てがデリバリーグループで正しく構成されていれば、ユーザーの自動割り当

ては引き続き機能します。ユーザー割り当てとともにマシンカタログにマシンを追加するサンプルスクリプトは、GitHubで入手できます。

- 統合Wake on LANは、**Remote PC Access**タイプのマシンカタログでのみ利用可能です。

Linux VDAに関する考慮事項

以下の考慮事項は、Linux VDAに固有のものです。

- 物理マシンでは、Linux VDAを非3Dモードでのみ使用してください。NVIDIAドライバーの制限により、HDX 3Dモードが有効になっている場合、PCのローカル画面をブラックアウトできず、セッションのアクティビティが表示されます。この画面を表示することはセキュリティリスクです。
- 物理Linuxマシンには、シングルセッションOSタイプのマシンカタログを使用します。
- Linuxマシンでは、自動ユーザー割り当ては利用できません。
- ユーザーがすでにPCにローカルでログオンしている場合、StoreFront™からPCを起動しようとすると失敗します。
- 省電力オプションはLinuxマシンでは利用できません。

技術要件と考慮事項

このセクションでは、物理PCの技術要件と考慮事項について説明します。

- 以下はサポートされていません。
  - KVMスイッチ、またはセッションを切断する可能性のあるその他のコンポーネント。
  - オールインワンPCやNVIDIA Optimus搭載のノートPCおよびPCを含むハイブリッドPC。
  - デュアルブートマシン。
- キーボードとマウスはPCに直接接続してください。モニターや、電源を切ったり切断したりできるその他のコンポーネントに接続すると、これらの周辺機器が利用できなくなる可能性があります。入力デバイスをモニターなどのコンポーネントに接続する必要がある場合は、それらのコンポーネントの電源を切らないでください。
- PCはActive Directory Domain Servicesドメインに参加している必要があります。
- セキュアブートはWindows 10およびWindows 11でのみサポートされています。
- PCにはアクティブなネットワーク接続が必要です。信頼性と帯域幅を向上させるには、有線接続が推奨されます。
- Wi-Fiを使用する場合は、以下を実行してください。

a. 電源設定でワイヤレスアダプターをオンのままにするように設定します。

b. ユーザーがログオンする前にワイヤレスネットワークに自動的に接続できるように、ワイヤレスアダプターとネットワークプロファイルを構成します。そうしないと、ユーザーがログオンするまでVDAは登録されません。ユーザーがログオンするまで、PCはリモートアクセスに利用できません。

c. Delivery ControllerまたはCloud ConnectorがWi-Fiネットワークから到達可能であることを確認してください。

- ノートPCでRemote PC Accessを使用できます。ノートPCがバッテリーではなく電源に接続されていることを確認してください。ノートPCの電源オプションをデスクトップPCのオプションと一致するように構成します。例：

  a. 休止状態機能を無効にします。

  b. スリープ機能を無効にします。

  c. 「蓋を閉じたときの動作」を「**何もしない**」に設定します。

  d. 「電源ボタンを押したときの動作」を「**シャットダウン**」に設定します。

  e. ビデオカードとNICの省電力機能を無効にします。

- Remote PC Accessは、Windows 10を搭載したSurface Proデバイスでサポートされています。前述のラップトップと同じガイドラインに従ってください。
- ドッキングステーションを使用している場合、ラップトップのドッキング解除と再ドッキングが可能です。ラップトップをドッキング解除すると、VDAはWi-Fi経由でDelivery ControllerまたはCloud Connectorに再登録されます。ただし、ラップトップを再ドッキングしても、ワイヤレスアダプターを切断しない限り、VDAは有線接続に切り替わりません。一部のデバイスには、有線接続が確立されたときにワイヤレスアダプターを切断する組み込み機能が提供されています。その他のデバイスでは、ワイヤレスアダプターを切断するためにカスタムソリューションまたはサードパーティ製ユーティリティが必要です。前述のWi-Fiに関する考慮事項を確認してください。

  Remote PC Accessデバイスでドッキングとドッキング解除を有効にするには、次の手順を実行します。

  a. **スタート**メニューで、**設定 > システム > 電源とスリープ**を選択し、**スリープ**を**なし**に設定します。

  b. **デバイスマネージャー > ネットワークアダプター > イーサネットアダプター**で、**電源の管理**に移動し、**電力の節約のために、コンピューターでこのデバイスの電源をオフにできるようにする**のチェックを外します。**このデバイスで、コンピューターのスタンバイ状態を解除できるようにする**がオンになっていることを確認します。

- 同じオフィスPCにアクセスできる複数のユーザーは、Citrix Workspaceで同じアイコンを見ます。ユーザーがCitrix Workspaceにログオンしたときに、そのリソースがすでに別のユーザーによって使用されている場合、利用不可として表示されます。
- オフィスPCにアクセスする各クライアントデバイス（例：自宅のPC）にCitrix Workspaceアプリをインストールします。

構成シーケンス

このセクションでは、**Remote PC Access**タイプのマシンカタログを使用する場合にRemote PC Accessを構成する方法の概要を説明します。その他の種類のマシンカタログの作成方法については、マシンカタログの作成を参照してください。

1. オンプレミスサイトのみ - 統合されたWake on LAN機能を使用するには、「Wake on LAN」に記載されている前提条件を構成します。
2. Remote PC Access用に新しいCitrix Virtual Apps and Desktopsサイトが作成された場合：

   a. **Remote PC Access**サイトタイプを選択します。

   b. 「**電源管理**」ページで、デフォルトのRemote PC Accessマシンカタログの電源管理を有効または無効にするかを選択します。この設定は、後でマシンカタログのプロパティを編集して変更できます。Wake on LANの構成の詳細については、「Wake on LAN」を参照してください。

   c. 「**ユーザー**」ページと「**マシンアカウント**」ページで情報を入力します。

   これらの手順を完了すると、**Remote PC Access Machines**という名前のマシンカタログと、**Remote PC Access Desktops**という名前のデリバリーグループが作成されます。
3. 既存のCitrix Virtual Apps and Desktopsサイトに追加する場合：

   a. 種類が**Remote PC Access**のマシンカタログを作成します（ウィザードの「オペレーティングシステム」ページ）。マシンカタログの作成方法の詳細については、「マシンカタログの作成」を参照してください。ターゲットPCがRemote PC Accessで使用できるよう、正しいOUを割り当ててください。

   b. マシンカタログ内のPCへのユーザーアクセスを提供するために、デリバリーグループを作成します。デリバリーグループの作成方法の詳細については、「デリバリーグループの作成」を参照してください。デリバリーグループを、PCへのアクセスを必要とするユーザーを含むActive Directoryグループに割り当ててください。
4. オフィスPCにVDAを展開します。

- シングルセッションOSコアVDAインストーラー（VDAWorkstationCoreSetup.exe）を使用することをお勧めします。
- シングルセッションフルVDAインストーラー（VDAWorkstationSetup.exe）を`/remotepc/physicalmachine`オプションとともに使用することもできます。これは、コアVDAインストーラーを使用した場合と同じ結果になります。

> **注:**
>
> RemotePCのインストールでは、特定のユーザーシナリオでVDAが期待どおりに動作するように、`/physicalmachine`引数を`/remotepc`とともに使用します。

- ヘルプデスクチームがCitrix Directorを介してリモートサポートを提供できるように、Windowsリモートアシスタンスを有効にすることを検討してください。これを行うには、`/enable_remote_assistance`オプションを使用します。詳細については、「コマンドラインを使用したインストール」を参照してください。
- Directorでログオン期間情報を表示するには、シングルセッションフルVDAインストーラーを使用し、**Citrix User Profile Management WMI Plugin**コンポーネントを含める必要があります。このコンポーネントを含めるには、`/includeadditional`オプションを使用します。詳細については、「コマンドラインを使用したインストール」を参照してください。
- SCCMを使用してVDAを展開する方法については、「SCCMを使用したVDAのインストール」を参照してください。
- 展開スクリプトを使用してVDAを展開する方法については、「スクリプトを使用したVDAのインストール」を参照してください。

ステップ2～4を正常に完了すると、ユーザーがPCにローカルでログインしたときに、自分のマシンに自動的に割り当てられます。

5. ユーザーには、オフィスPCにリモートでアクセスするために使用する各クライアントデバイスにCitrix Workspaceアプリをダウンロードしてインストールするよう指示してください。Citrix Workspaceアプリは`https://www.citrix.com/downloads/`またはサポートされているモバイルデバイスのアプリケーションストアから入手できます。

レジストリを介して管理される機能

> **注意:**

> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターは、ご自身の責任において使用してください。編集する前に、必ずレジストリをバックアップしてください。

複数ユーザーの自動割り当てを無効にする

各Delivery Controller™で、次のレジストリ設定を追加します。

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- 名前: AllowMultipleRemotePCAssignments
- 種類: DWORD
- データ: 0

スリープモード (最小バージョン 7.16)

Remote PC Accessマシンをスリープ状態にするには、VDAにこのレジストリ設定を追加し、マシンを再起動します。再起動後、オペレーティングシステムの省電力設定が適用されます。事前設定されたアイドルタイマーが経過すると、マシンはスリープモードに入ります。マシンがスリープから復帰すると、Delivery Controllerに再登録されます。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: DisableRemotePCSleepPreventer
- 種類: DWORD
- データ: 1

セッション管理

既定では、ローカルユーザーがそのマシンでセッションを開始すると (CTRL+ALT+DELを押すことで)、リモートユーザーのセッションは自動的に切断されます。この自動的な動作を防ぐには、オフィスPCに以下のレジストリエントリを追加し、その後、マシンを再起動します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: SasNotification
- 種類: DWORD
- データ: 1

既定では、接続メッセージがタイムアウト期間内に確認されない場合、リモートユーザーがローカルユーザーよりも優先されます。この動作を構成するには、この設定を使用します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: RpcaMode
- 種類: DWORD
- データ:
  - 1 - 指定されたタイムアウト期間内にメッセージングUIに応答しない場合、リモートユーザーが常に優先されます。この設定が構成されていない場合、この動作が既定となります。
  - 2 - ローカルユーザーが優先されます。

Remote PC Accessモードを適用するためのタイムアウトは、デフォルトで30秒です。このタイムアウトは構成できますが、30秒未満に設定しないでください。タイムアウトを構成するには、このレジストリ設定を使用します。

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: RpcaTimeout
- 種類: DWORD
- データ: タイムアウトの秒数（10進数値）

ユーザーが強制的にコンソールアクセスを取得したい場合: ローカルユーザーは、10秒の間にCtrl+Alt+Delを2回押すことで、リモートセッションのローカル制御を取得し、切断イベントを強制できます。

レジストリの変更とマシンの再起動後、リモートユーザーが使用中のPCにローカルユーザーがCtrl+Alt+Delを押してログオンしようとすると、リモートユーザーにプロンプトが表示されます。このプロンプトは、ローカルユーザーの接続を許可するか拒否するかを尋ねます。接続を許可すると、リモートユーザーのセッションは切断されます。

セッション管理のログ記録

リモートPCアクセスには、アクティブなICA®セッションを持つPCに誰かがアクセスしようとしたときにログを記録するログ機能が追加されました。これにより、不要なアクティビティや予期しないアクティビティがないか環境を監視し、インシデントを調査する必要がある場合にそのようなイベントを監査できます。

イベントはWindowsイベントビューアーを使用してログに記録され、**Applications and Services > Citrix > HostCore > ICA Service > Admin**にあります。

Remote PC Accessを使用すると、3つの異なるイベントがログに記録されます。

Ctrl+Alt+Delイベント

このイベントは、アクティブなリモートセッション中にローカルユーザーがコンソールキーボードでCtrl+Alt+Delを押したときに表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベントID: 43, 44, 45
- ソース: ICA サービス

イベント ID 43

このイベントIDは、SasNotification レジストリ値が存在しない場合、または SasNotification レジストリ値が 0 の場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to automatically disconnect the
remote session.
```

イベント ID 44

このイベントIDは、SasNotification レジストリ値が 1 で、RpcaMode レジストリ値が 1 の場合、または RpcaMode レジストリ値が存在しない場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user. The
user preference is set to remote user.
```

イベント ID 45

このイベントIDは、SasNotification レジストリ値が 1 で、RpcaMode レジストリ値が 2 の場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user.

The user preference is set to local user.
```

リモートセッション切断イベント

このイベントは、さまざまな理由でリモートセッションが切断された場合に表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベント ID: 46, 47, 48
- ソース: ICA Service

イベントID 46

このイベントIDは、リモートセッションが切断され、SasNotificationレジストリ値が存在しないか、SasNotificationレジストリ値が0である場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected.
```

イベントID 47

このイベントIDは、リモートユーザーがセッションの切断に同意し、SasNotificationレジストリ値が1であり、RpcaModeレジストリ値が1であるか、RpcaModeレジストリ値が2であるか、またはRpcaModeレジストリ値が存在しない場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected
because the user accepted the request to disconnect the session.
```

イベントID 48

このイベントIDは、リモートユーザーが指定されたタイムアウト期間内に切断要求を拒否せず、SasNotificationレジストリ値が1であり、RpcaModeレジストリ値が2である場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected
because the user did not decline the disconnection request within the
configured timeout period (&lt;timeout period>).
```

Ctrl+Alt+Del 2回押下イベント

このイベントは、10秒以内にCtrl+Alt+Delが2回押された場合に表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベントID: 49
- ソース: ICA Service

イベントID 49

このイベントIDは、Ctrl+Alt+Delが10秒以内に2回押されたときに表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been forcibly
disconnected.
```

ウェイク・オン・LAN

Remote PC AccessはWake on LANをサポートしており、ユーザーは物理PCをリモートで起動できます。この機能により、ユーザーは使用していないときにオフィスPCの電源を切ったままにして、エネルギーコストを節約できます。また、誤ってマシンの電源が切れてしまった場合でも、リモートアクセスを可能にします。

Wake on LAN機能を使用すると、デリバリーコントローラーからの指示があった場合、PC上で実行されているVDAから、そのPCが存在するサブネットにマジックパケットが直接送信されます。これにより、追加のインフラストラクチャコンポーネントやマジックパケット配信のためのサードパーティソリューションに依存することなく、この機能が動作します。

制限事項

Wake on LAN機能を使用するRemote PC Accessは、ピーク時の自動電源オンをサポートしていません。

システム要件

Wake on LAN機能を使用するためのシステム要件は次のとおりです。

- コントロールプレーン:
  - シトリックス DaaS™
  - Citrix Virtual Apps and Desktops 2009以降のバージョン
- 物理PC:
  - VDAバージョン2009以降
  - Windows 10またはWindows 11。サポートの詳細については、VDAシステム要件を参照してください。
  - BIOS/UEFIでWake on LANが有効になっていること
  - Windows構成内のネットワークアダプターのプロパティでWake on LANが有効になっていること

Wake on LANの構成

Studioを使用したWake on LANの構成

Wake on LAN接続を作成するには:

1. 左側のペインで、**Hosting**ノードを選択します。
2. **接続とリソースの追加**を選択します。
3. ウィザードの**接続**ページで、以下を指定します:
   a. 接続の種類: Remote PC Wake on LAN
   b. ゾーン名: Remote PC Accessカタログが存在するゾーンを選択します
   c. 接続名: Wake on LAN接続の名前を入力します
4. 接続とリソースの追加ウィザードの残りの手順を完了します。

Remote PC Access マシンカタログにWake on LAN接続を追加するには:

1. 新しいRemote PC Accessマシンカタログを作成している場合は、マシンカタログセットアップウィザードの**マシンタイプ**ページでドロップダウンリストを使用して接続を追加できます。
2. 既存のマシンカタログにWake on LAN接続を追加する場合は:
   a. 左側の**マシンカタログ**ノードに移動します。

b. 適切なRemote PC Accessマシンカタログを選択します。
c. マシンカタログを右クリックするか、上部の**その他**メニューを選択します。
d. **マシンカタログの編集**を選択します。
e. **電源管理**ページで、**はい**を選択します。
f. ドロップダウンリストから適切な接続を選択します。
g. **保存**を選択します。

> **注:**
>
> Studioを介したWake on LANの設定は、現時点ではCitrix DaaSでのみ利用可能です。

PowerShell を使用して Wake on LAN を構成する

PowerShellを使用してWake on LANを構成するには:

1. まだ Remote PC Access マシンカタログがない場合は、作成します。
2. まだ Wake on LAN ホスト接続がない場合は、作成します。
3. Wake on LAN ホスト接続の一意の識別子を取得します。
4. Wake on LAN ホスト接続をマシンカタログに関連付けます。

Wake on LAN ホスト接続を作成するには：

```
# Load Citrix SnapIns

Add-PSSnapIn -Name "*citrix*"



# Provide the name of the Wake on LAN host connection

[string]$connectionName = "Remote PC Access Wake on LAN"



# Create the hypervisor connection

$hypHc = New-Item -Path xdhyp:\Connections `
```

```
                -Name $connectionName `

                -HypervisorAddress "N/A" `

                -UserName "woluser" `

                -Password "wolpwd" `

                -ConnectionType Custom `

                -PluginId VdaWOLMachineManagerFactory `

                -CustomProperties "<CustomProperties></CustomProperties>"
`

                -Persist



$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid



# Wait for the connection to be ready before trying to use it

while (-not $bhc.IsReady)

{

    Start-Sleep -s 5

    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid

}
```

ホスト接続の準備ができたら、次のコマンドを実行してホスト接続の一意の識別子を取得します。

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"

$hypUid = $bhc.Uid
```

接続の一意の識別子を取得したら、次のコマンドを実行して、その接続を Remote PC Access マシンカタログに関連付けます。

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog
-RemotePCHypervisorConnectionUid $hypUid
```

設計上の考慮事項

Remote PC Access で Wake on LAN を使用する予定がある場合は、次の点を考慮してください。

- 複数のマシンカタログで同じWake on LANホスト接続を使用できます。
- あるPCが別のPCを起動するには、両方のPCが同じサブネット内にあり、同じWake on LANホスト接続を使用している必要があります。PCが同じマシンカタログにあるか、異なるマシンカタログにあるかは関係ありません。
- ホスト接続は特定のゾーンに割り当てられます。展開に複数のゾーンが含まれている場合は、各ゾーンにWake on LANホスト接続が必要です。これはマシンカタログにも当てはまります。
- マジックパケットは、グローバルブロードキャストアドレス255.255.255.255を使用してブロードキャストされます。このアドレスがブロックされていないことを確認してください。
- そのサブネット内のマシンを起動できるようにするには、Wake on LAN接続ごとに、サブネット内に少なくとも1台のPCが電源オンになっている必要があります。

運用上の考慮事項

Wake on LAN機能を使用する際の考慮事項は次のとおりです。

- VDAは、統合されたWake on LAN機能を使用してPCを起動できるようになる前に、少なくとも1回は登録する必要があります。
- Wake on LANはPCを起動するためにのみ使用できます。再起動やシャットダウンなどの他の電源操作はサポートしていません。
- Wake on LAN接続が作成されると、Web Studioに表示されます。ただし、Citrix Virtual Apps and Desktopsオンプレミスを使用している場合、Web Studio内でそのプロパティを編集することはサポートされていません。
- マジックパケットは次の2つの方法のいずれかで送信されます。

a. ユーザーが自分のPCへのセッションを起動しようとし、VDAが未登録の場合
b. 管理者がWeb StudioまたはPowerShellから手動で電源オンコマンドを送信した場合

- デリバリーコントローラーはPCの電源状態を認識していないため、Web Studioでは電源状態の下に**サポートされていません**と表示されます。デリバリーコントローラーは、VDA登録状態を使用してPCがオンかオフかを判断します。

トラブルシューティング

モニターのブランキングが機能しない

アクティブなHDXセッション中にWindows PCのローカルモニターが空白にならない場合（ローカルモニターにセッションで発生していることが表示される場合）、それはGPUベンダーのドライバーの問題である可能性があります。この問題を解決するには、次のレジストリ値を設定して、Citrix Indirect Display driver (IDD) にグラフィックカードのベンダードライバーよりも高い優先順位を与えます。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- 名前: CitrixIDD
- 種類: DWORD
- データ: 3

ディスプレイドライバーの優先順位とモニターの作成の詳細については、Knowledge Centerの記事CTX237608を参照してください。

セッション管理通知が有効になっているマシンでCtrl+Alt+Delを選択すると、セッションが切断されます

SasNotificationレジストリ値によって制御されるセッション管理通知は、VDAでRemote PC Accessモードが有効になっている場合にのみ機能します。物理PCでHyper-Vの役割または仮想化ベースのセキュリティ機能が有効になっている場合、そのPCは仮想マシンとして報告されます。VDAが仮想マシン上で実行されていることを検出すると、Remote PC Accessモードを自動的に無効にします。Remote PC Accessモードを有効にするには、次のレジストリ値を追加します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: ForceEnableRemotePC
- 種類: DWORD
- データ: 1

設定を有効にするには、PCを再起動します。

診断情報

リモートPCアクセスに関する診断情報は、Windowsアプリケーションイベントログに書き込まれます。情報メッセージはスロットリングされません。エラーメッセージは、重複するメッセージを破棄することによってスロットリングされます。

- 3300（情報）: マシンがカタログに追加されました
- 3301（情報）: マシンがデリバリーグループに追加されました
- 3302（情報）: マシンがユーザーに割り当てられました
- 3303 (エラー): 例外

電源管理

Remote PC Accessの電源管理が有効になっている場合、サブネット指向ブロードキャストでは、Controllerとは異なるサブネットにあるマシンを起動できないことがあります。サブネット指向ブロードキャストを使用してサブネット間で電源管理が必要で、AMTサポートが利用できない場合は、Wake-upプロキシまたはユニキャスト方式を試してください。これらの設定が電源管理接続の詳細プロパティで有効になっていることを確認してください。

アクティブなリモートセッションはローカルのタッチスクリーン入力を記録します

VDA が Remote PC Access モードを有効にすると、マシンはアクティブなセッション中にローカルのタッチスクリーン入力を無視します。物理 PC で Hyper-V ロールまたは仮想化ベースのセキュリティ機能が有効になっている場合、その PC は仮想マシンとして報告されます。VDA が仮想マシン上で実行されていることを検出すると、Remote PC Access モードを自動的に無効にします。Remote PC Access モードを有効にするには、次のレジストリ設定を追加します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: ForceEnableRemotePC
- 種類: DWORD
- データ: 1

設定を有効にするには、PC を再起動してください。

その他のリソース

以下は Remote PC Access に関するその他のリソースです。

- ソリューション設計ガイダンス: Remote PC Access Design Decisions。

- Remote PC Access アーキテクチャの例: Citrix Remote PC Access ソリューションのリファレンスアーキテクチャ。

コンテンツを公開する

> **注:**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> Microsoft WordドキュメントやWebリンクなどのリソースへのURLまたはUNCパスであるアプリケーションを公開できます。この機能は公開コンテンツとして知られています。コンテンツを公開する機能により、ユーザーへのコンテンツ配信方法に柔軟性が加わります。既存のアクセス制御とアプリケーション管理の恩恵を受けることができます。また、コンテンツを開くためにローカルアプリケーションを使用するか、公開アプリケーションを使用するかを指定することもできます。

公開されたコンテンツは、StoreFront™およびCitrix Workspace™アプリの他のアプリケーションと同様に表示されます。ユーザーはアプリケーションにアクセスするのと同じ方法でアクセスします。クライアントでは、リソースは通常どおり開きます。

- ローカルにインストールされたアプリケーションが適切な場合、それが起動されてリソースが開かれます。
- ファイルタイプ関連付けが定義されている場合、公開されたアプリケーションが起動されてリソースが開かれます。

PowerShell SDKを使用してコンテンツを公開します。Web Studioを使用してコンテンツを公開することはできません。ただし、公開後にWeb Studioを使用してアプリケーションのプロパティを編集することはできます。

構成の概要と準備

コンテンツの公開には、次の主要なプロパティを持つ`New-BrokerApplication`コマンドレットを使用します。（すべてのコマンドレットプロパティの説明については、コマンドレットのヘルプを参照してください。）

```
New-BrokerApplication –ApplicationType PublishedContent
-CommandLineExecutable location -Name app-name -DesktopGroup delivery-
group-name
```

`ApplicationType`プロパティは`PublishedContent`である必要があります。

`CommandLineExecutable`プロパティは、公開されたコンテンツの場所を指定します。255文字の制限で、以下の形式がサポートされています。

- HTML Webサイトアドレス（例: `<http://www.citrix.com>`）
- Webサーバー上のドキュメントファイル（例: `https://www.citrix.com/press/pressrelease.doc`）
- FTPサーバー上のディレクトリ（例: `ftp://ftp.citrix.com/code`）
- FTPサーバー上のドキュメントファイル (例: `ftp://ftp.citrix.com/code/Readme.txt` >)
- UNCディレクトリパス (例: `file://myServer/myShare or \\\\myServer\\myShare`)
- UNCファイルパス (例: `file://myServer/myShare/myFile.asf` または `\\myServer\myShare\myFile.asf`)

正しいSDKがあることを確認してください。

- Citrix DaaS (旧Citrix Virtual Apps and Desktopsサービス) の展開の場合、Citrix Virtual Apps and Desktops Remote PowerShell SDKをダウンロードしてインストールします。
- オンプレミスのCitrix Virtual Apps and Desktops展開の場合、Delivery Controllerとともにインストールされているの PowerShell SDKを使用します。公開コンテンツアプリケーションを追加するには、最低バージョン7.11のDelivery Controllerが必要です。

以下の手順では例を使用します。例では次のようになります。

- マシンカタログが作成されています。
- `PublishedContentApps` という名前のデリバリーグループが作成されています。このグループは、カタログからマルチセッションOSマシンを使用します。WordPadアプリケーションがグループに追加されています。
- デリバリーグループ名、`CommandLineExecutable` の場所、およびアプリケーション名が割り当てられます。

はじめに

PowerShell SDKを含むマシンで、PowerShellを開きます。

次のコマンドレットは、適切なPowerShell SDKスナップインを追加し、返されたデリバリーグループレコードを割り当てます。

`Add-PsSnapin Citrix* $dg = Get-BrokerDesktopGroup –Name PublishedContentApps`

Citrix DaaSを使用している場合は、Citrix Cloud™の資格情報を入力して認証します。複数の顧客がいる場合は、1つを選択します。

URLを公開する

場所とアプリケーション名を割り当てた後、次のコマンドレットは、Citrixのホームページをアプリケーションとして公開します。

```
$citrixUrl = "https://www.citrix.com/"

$appName = "Citrix Home Page"



New-BrokerApplication –ApplicationType PublishedContent –
CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.Uid
```

成功を確認します:

- StoreFrontを開き、PublishedContentAppsデリバリーグループ内のアプリケーションにアクセスできるユーザーとしてログオンします。表示には、デフォルトのアイコンを持つ新しく作成されたアプリケーションが含まれます。アイコンのカスタマイズについては、`<https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/>`を参照してください。
- **Citrix Home Page**アプリケーションをクリックします。URLは、デフォルトのブラウザのローカルで実行されているインスタンスの新しいタブで起動します。

UNCパスにあるリソースを公開する

この例では、管理者はすでに`PublishedResources`という名前の共有を作成しています。場所とアプリケーション名を割り当てた後、次のコマンドレットはその共有内のRTFファイルとDOCXファイルをリソースとして公開します。

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\\PublishedResources\\PublishedRTF.rtf"

$rtfAppName = "PublishedRTF"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $rtfUNC -Name $rtfAppName

-DesktopGroup $dg.Uid



$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx"

$docxAppName = "PublishedDOCX"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $docxUNC -Name $docxAppName

-DesktopGroup $dg.Uid
```

成功を確認する:

- StoreFrontウィンドウを更新して、新しく公開されたドキュメントを表示します。
- **PublishedRTF**および**PublishedDOCX**アプリケーションをクリックします。各ドキュメントは、ローカルで実行されているWordPadで開きます。

PublishedContentアプリケーションの表示と編集

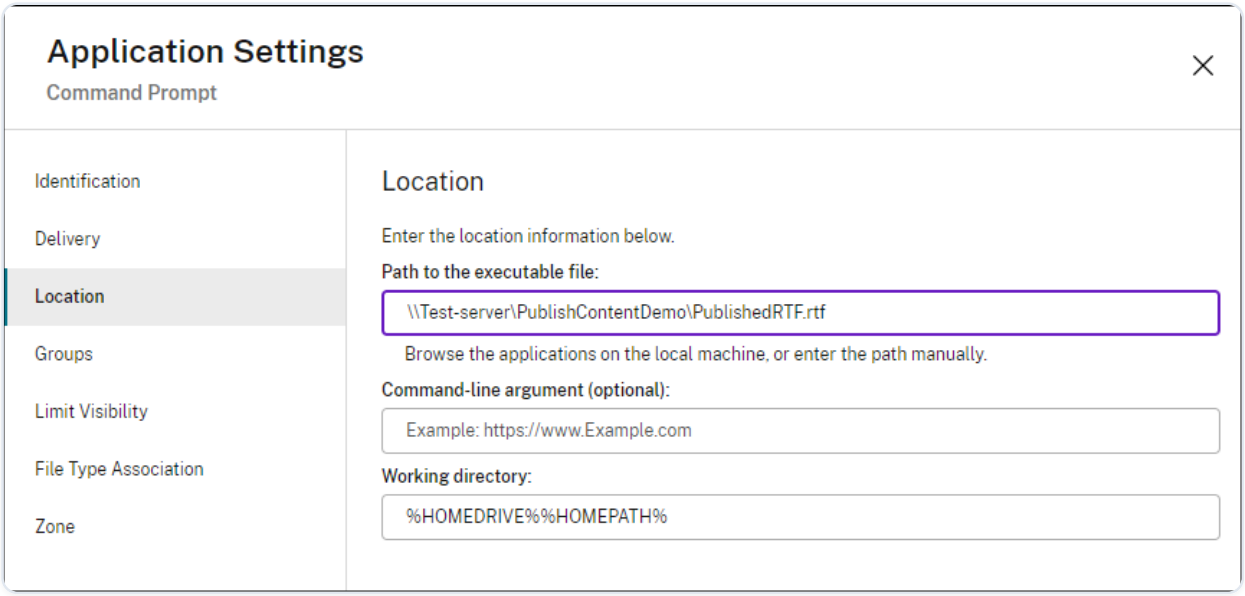
公開されたコンテンツは、他のアプリケーションタイプで使用するのと同じ方法で管理します。

`PublishedContent`アプリケーションを表示および編集するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**アプリケーション**を選択します。
2. **アプリケーション**タブで、PublishedContentアプリケーションを選択し、**プロパティ**を選択します。

アプリケーションのプロパティ（ユーザーの可視性、グループの関連付け、ショートカットなど）は、公開されたコンテンツに適用されます。ただし、**場所**ページでは、コマンドライン引数または作業ディレクトリのプロパティを変更することはできません。

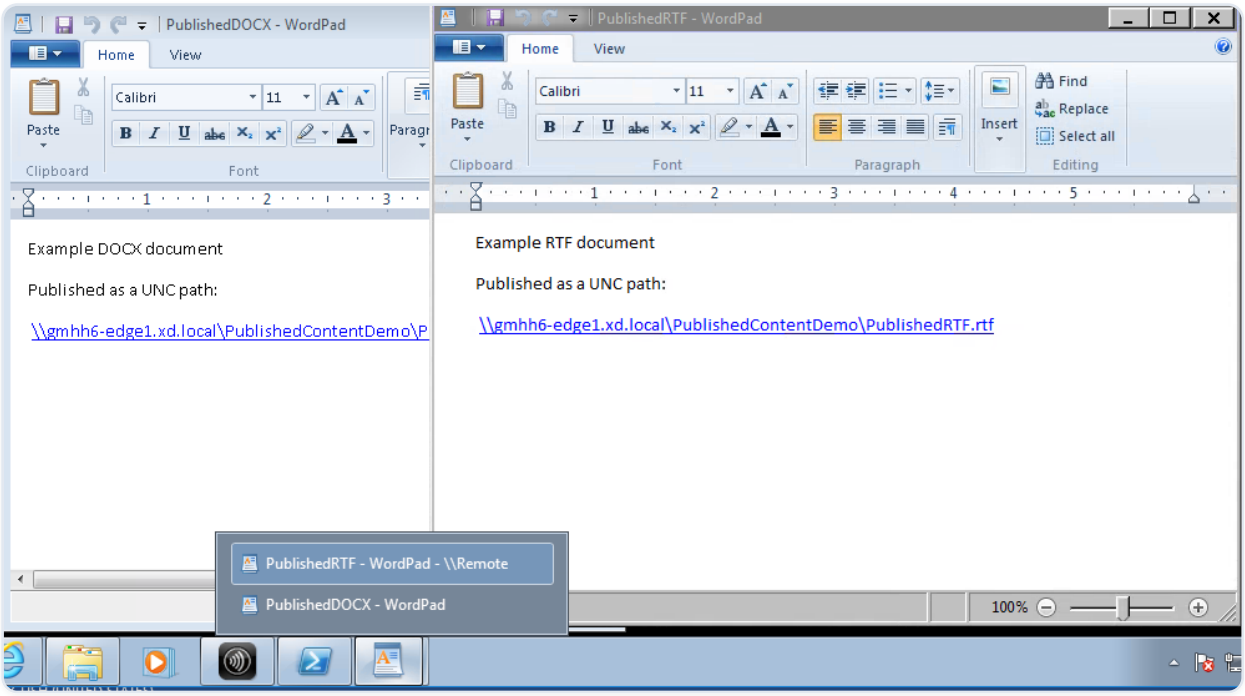
3. リソースを変更するには、そのページの**実行可能ファイルへのパス**フィールドを修正します。



4. 公開アプリケーションを使用して`PublishedContent`アプリケーション（ローカルアプリケーションではなく）を開くには、次の手順に従います。

   この例では、公開されたWordPadアプリケーションが編集され、.rtfファイル用のファイルタイプ関連付けが作成されます。

   a. デリバリーグループのメンテナンスモードをオンにします。
   b. **ファイルタイプ関連付け**プロパティを編集します。
   c. 完了したら、メンテナンスモードをオフにします。
   d. StoreFrontを更新してファイルタイプ関連付けの変更を読み込み、**PublishedRTF**および**PublishedDOCX**アプリケーションをクリックします。違いに注目してください。**PublishedDOCX**は引き続きローカルのWordPadで開きます。しかし、**PublishedRTF**はファイルタイプ関連付けにより、公開されたWordPadで開くようになりました。



詳細情報

- マシンカタログの作成
- デリバリーグループの作成
- アプリケーションプロパティの変更

サーバー VDI

Server VDI (Virtual Desktop Infrastructure) 機能を使用して、単一ユーザー向けにサーバーオペレーティングシステムからデスクトップを配信します。

- エンタープライズ管理者は、サーバーオペレーティングシステムをVDIデスクトップとして配信できます。これは、エンジニアやデザイナーなどのユーザーにとって価値のあるものです。
- サービスプロバイダーは、クラウドからデスクトップを提供できます。これらのデスクトップは、Microsoft Services Provider License Agreement (SPLA) に準拠しています。

サポート:

- Citrix Virtual Apps and Desktops™ および Citrix DaaS (旧 Citrix Virtual Apps and Desktops service) の展開では、Server VDI は Windows Server 2022 および Windows Server 2019 でサポートされています。
- すべての Server VDI 展開は、ユーザーパーソナライゼーションレイヤーテクノロジーをサポートしています。

- Server VDI がスキャナーなどの TWAIN デバイスで動作するには、Windows Server のデスクトップエクスペリエンス機能をインストールする必要があります。
- 以下の機能は Server VDI では使用できません。
  - ホスト型アプリケーション
  - ローカルアプリアクセス
  - 直接（ブローカーなし）デスクトップ接続
  - リモートPCアクセス

Server VDI のインストールと構成

1. インストール用に Windows サーバーを準備します。
   - Windows Server Manager を使用して、リモートデスクトップサービス役割サービスがインストールされていないことを確認します。以前にインストールされていた場合は、削除してください。これらの役割サービスがインストールされていると、VDA のインストールは失敗します。
   - **各ユーザーを単一セッションに制限する** プロパティが有効になっていることを確認します。Windows サーバーで、ターミナルサーバー設定のレジストリを編集します。

     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server`

     `DWORD fSingleSessionPerUser = 1`
2. Citrix Virtual Apps and Desktops インストーラーのコマンドラインインターフェイスを使用して、サポートされているサーバーまたはサーバーマスターイメージに VDA をインストールし、`/servervdi` オプションを指定します。（デフォルトでは、インストーラーのグラフィカルインターフェイスは、サーバーオペレーティングシステム上のWindowsシングルセッションOS VDAをブロックします。コマンドラインを使用すると、この動作が上書きされます。）次のいずれかのコマンドを使用します。
   - Citrix Virtual Apps™ and Desktops 展開の場合:
     - `XenDesktopVdaSetup.exe /servervdi`
     - `VDAWorkstationSetup.exe /servervdi`
   - Citrix DaaS™ 展開の場合:
     - `VDAWorkstationSetup.exe /servervdi`

   その他のオプション:

- Delivery Controller または Cloud Connector を指定するには、`/controllers` を使用します。
- ファイアウォールを手動で構成する場合を除き、ファイアウォールでポートを開くには `/enable_hdx_ports` を使用します。
- イメージに VDA をインストールし、そのイメージから MCS を使用してサーバー VM を作成する場合は、`/mastermcsimage` (または `/masterimage`) を使用します。
- すべてのオプションの詳細については、「コマンドラインを使用したインストール」を参照してください。

3. Server VDI用のマシンカタログを作成します。カタログ作成ウィザードで:
   - 「**オペレーティングシステム**」ページで、「**シングルセッションOS**」を選択します。
   - 「**概要**」ページで、管理者向けに、Server VDI であることを明確に識別できるマシンカタログ名と説明を指定します。これは、カタログがServer VDIをサポートしていることをStudioで示す唯一のインジケーターです。

   Studioで検索を使用すると、VDAがマルチセッションマシンにインストールされている場合でも、Server VDIカタログは「**シングルセッションOSマシン**」タブに表示されます。
4. デリバリーグループを作成し、作成したServer VDIカタログを選択します。

VDAのインストール中にDelivery ControllerまたはCloud Connectorを指定しなかった場合は、後で指定することを忘れないでください。詳しくは、「VDA登録」(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/vda-registration.html)を参照してください。

ユーザーパーソナライゼーションレイヤー

> **注:**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

Citrix Virtual Apps and Desktopsのユーザーパーソナライゼーションレイヤー機能は、非永続的なマシンカタログの機能を拡張し、セッション間でユーザーのデータとローカルにインストールされたアプリケーションを保持します。基盤となるCitrix App Layeringテクノロジーを

> 搭載したユーザーパーソナライゼーションレイヤー機能は、非永続的なマシンカタログでCitrix ProvisioningおよびMachine Creation Services™ (MCS) をサポートします。

マスターイメージ内のVirtual Delivery Agentとともに、ユーザーパーソナライゼーションレイヤーコンポーネントをインストールします。VHDファイルは、ユーザーがローカルにインストールしたアプリケーションを保存します。イメージにマウントされたVHDは、ユーザー自身の仮想ハードドライブとして機能します。

> **重要:**
>
> Citrix Virtual Apps™ and Desktopsでユーザーパーソナライゼーションレイヤーを展開するか、イメージテンプレートで有効になっているApp Layeringユーザーレイヤーを展開することはできますが、両方を同時に展開することはできません。App Layering内のレイヤーにユーザーパーソナライゼーションレイヤー機能をインストールしないでください。

> この機能はPersonal vDisk (PvD) に代わるものであり、非永続的（プールされた）デスクトップ環境でユーザーに永続的なワークスペースエクスペリエンスを提供します。

ユーザーパーソナライゼーションレイヤー機能を展開するには、この記事で詳述されている手順を使用してインストールおよび構成します。

アプリケーションのサポート

以下の例外を除き、ユーザーがデスクトップにローカルでインストールするすべてのアプリケーションは、ユーザーパーソナライゼーションレイヤーでサポートされます。

例外

以下のアプリケーションは例外であり、ユーザーパーソナライゼーションレイヤーではサポートされません。

- MS OfficeやVisual Studioなどのエンタープライズアプリケーション。
- ネットワークスタックまたはハードウェアを変更するアプリケーション。例: VPNクライアント。
- ブートレベルドライバーを持つアプリケーション。例：ウイルススキャナー。
- ドライバー ストアを使用するドライバーを持つアプリケーション。例：プリンター ドライバー。

> **注:**
>
> Windowsグループポリシーオブジェクト（GPO）を使用してプリンターを利用可能にすることができます。

サポートされていないアプリケーションをローカルにインストールすることをユーザーに許可しないでください。代わりに、これらのアプリケーションはマスターイメージに直接インストールしてください。

ローカルユーザーまたは管理者アカウントを必要とするアプリケーション

ユーザーがアプリケーションをローカルにインストールすると、そのアプリはユーザーレイヤーに格納されます。その後、ユーザーがローカルユーザーまたはグループを追加または編集しても、その変更はセッションを超えて保持されません。

> **重要:**
>
> 必要なローカルユーザーまたはグループは、マスターイメージに追加してください。

要件

ユーザーパーソナライゼーションレイヤー機能には、以下のコンポーネントが必要です。

- Citrix Virtual Apps and Desktops 7 1909 以降のバージョン
- Virtual Delivery Agent (VDA)、バージョン1912以降
- Citrix Provisioning™、バージョン1909以降
- Windowsファイル共有（SMB）、またはオンプレミスAD認証が有効なAzure Files

OSがシングルセッションとして展開されている場合、以下のWindowsバージョンでユーザーパーソナライゼーションレイヤー機能を展開できます。サポートは、シングルセッション上の単一ユーザーに限定されます。

- ウィンドウズ 11 エンタープライズ x64
- Windows 10 Enterprise x64、バージョン1607以降
- Windows Server 2019 (Azure Filesがサポートされています)
- Windows Server 2022 (Azure Filesがサポートされています)

Citrix Virtual Apps and Desktops 7の場合、User personalization layersでのAzure Filesの使用は、Windows Server 2022、Windows Server 2019、およびWindows 10クライアントでサポートされています。

> **注:**

> サーバーOSを使用している場合、Server VDIのみがサポートされます。展開の詳細については、Server VDIの記事を参照してください。

> ユーザーパーソナライゼーションレイヤーは、マシンごとに一度に1人のユーザーのみをサポートし、その後、ディスクをリセットするためにマシンを再起動する必要があります。ユーザーパーソナライゼーションレイヤーは、マルチセッションサーバーオペレーティングシステムでは使用できず、シングルセッションサーバーシステムでのみ使用できます。ユーザーパーソナライゼーションレイヤーは、非永続デスクトップでのみサポートされます。

> ユーザーパーソナライゼーションレイヤー機能がインストールされている場合は、アンインストールします。最新リリースをインストールする前に、マスターイメージを再起動します。

ファイル共有を設定する

ユーザーパーソナライゼーションレイヤー機能には、Windows Server Message Block (SMB) ストレージが必要です。Windowsファイル共有を作成するには、使用しているWindowsオペレーティングシステムの通常の手順に従ってください。

Azureベースのカタログでは Azure Filesを使用する方法の詳細については、ユーザーパーソナライゼーションレイヤー用のAzure Filesストレージを設定するを参照してください。

推奨事項

ユーザーパーソナライゼーションレイヤーの展開を成功させるには、このセクションの推奨事項に従ってください。

マイクロソフト システムセンター コンフィギュレーションマネージャー (SCCM)

ユーザーパーソナライゼーションレイヤー機能でSCCMを使用している場合は、VDI環境でイメージを準備するためのMicrosoftのガイドラインに従ってください。詳細については、このMicrosoft TechNet記事を参照してください。

ユーザーレイヤーのサイズ

ユーザーレイヤーは、ディスク上のスペースが使用されるにつれて拡張するシンプロビジョニングディスクです。ユーザーレイヤーに許可されるデフォルトサイズは10 GBで、これは推奨される最小値です。

> **注:**
>
> インストール中に値がゼロ (0) に設定されている場合、デフォルトのユーザーレイヤーサイズは10 GBに設定されます。

> ユーザーレイヤーのサイズを変更したい場合は、**ユーザーレイヤーサイズ**ポリシーに別の値を入力できます。**オプション: GB単位のユーザーレイヤーサイズの横にあるをクリックします。**の下にある、**ステップ5: デリバリーグループのカスタムポリシーを作成する**を参照してください。

ユーザーレイヤーサイズを上書きするためのツール（オプション）

ユーザーレイヤーファイル共有にクォータを定義するWindowsツールを使用して、ユーザーレイヤーサイズを上書きできます。

以下のMicrosoftクォータツールのいずれかを使用して、**Users**という名前のユーザーレイヤーディレクトリにハードクォータを設定します。

- ファイルサーバーリソースマネージャー (FSRM)
- クォータマネージャー

> **注:**
>
> クォータを増やすと、新しいユーザーレイヤーに影響し、既存のレイヤーを拡張します。クォータを減らすと、新しいユーザーレイヤーのみに影響します。既存のユーザーレイヤーのサイズが縮小することはありません。

ユーザーパーソナライゼーションレイヤーを展開する

ユーザーパーソナライゼーション機能を展開する際は、Web Studio内でポリシーを定義します。その後、そのポリシーを、機能が展開されているマシンカタログにバインドされたデリバリーグループに割り当てます。

マスターイメージにユーザーパーソナライゼーションレイヤーの設定がない場合、サービスはアイドル状態のままであり、オーサリングアクティビティを妨げません。

マスターイメージでポリシーを設定すると、サービスはマスターイメージ内でユーザーレイヤーを実行してマウントしようとします。マスターイメージは予期しない動作や不安定性を示します。

ユーザーパーソナライゼーションレイヤー機能を展開するには、以下の手順をこの順序で完了します。

- ステップ1：Citrix Virtual Apps and Desktops環境の可用性を確認します。
- ステップ2：マスターイメージを準備します。
- ステップ3：マシンカタログを作成します。
- ステップ4：デリバリーグループを作成します。
- ステップ5：デリバリーグループのカスタムポリシーを作成します。

> **注:**
>
> イメージ上のWindows 10をアップグレードした後、初めてログインするのに通常よりも時間がかかります。ユーザーのレイヤーは新しいバージョンのWindows 10用に更新する必要があり、それによってログオン時間が増加します。

ステップ 1: Citrix Virtual Apps and Desktops 環境が利用可能であることを確認する

この新機能を使用するために、Citrix Virtual Apps and Desktops 環境が利用可能であることを確認してください。セットアップの詳細については、「Citrix Virtual Apps and Desktops のインストールと構成」を参照してください。

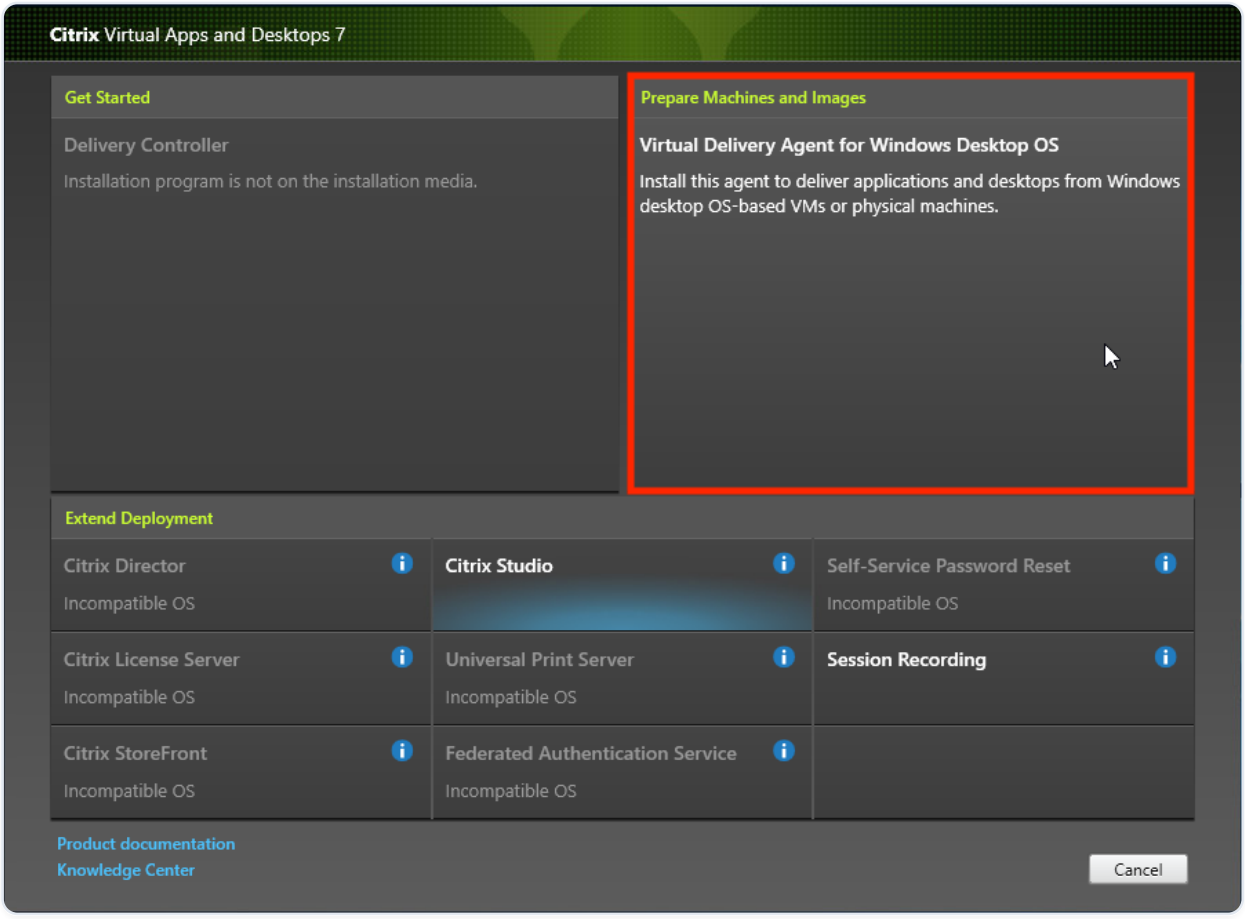
ステップ 2: マスターイメージを準備する

マスターイメージを準備するには:

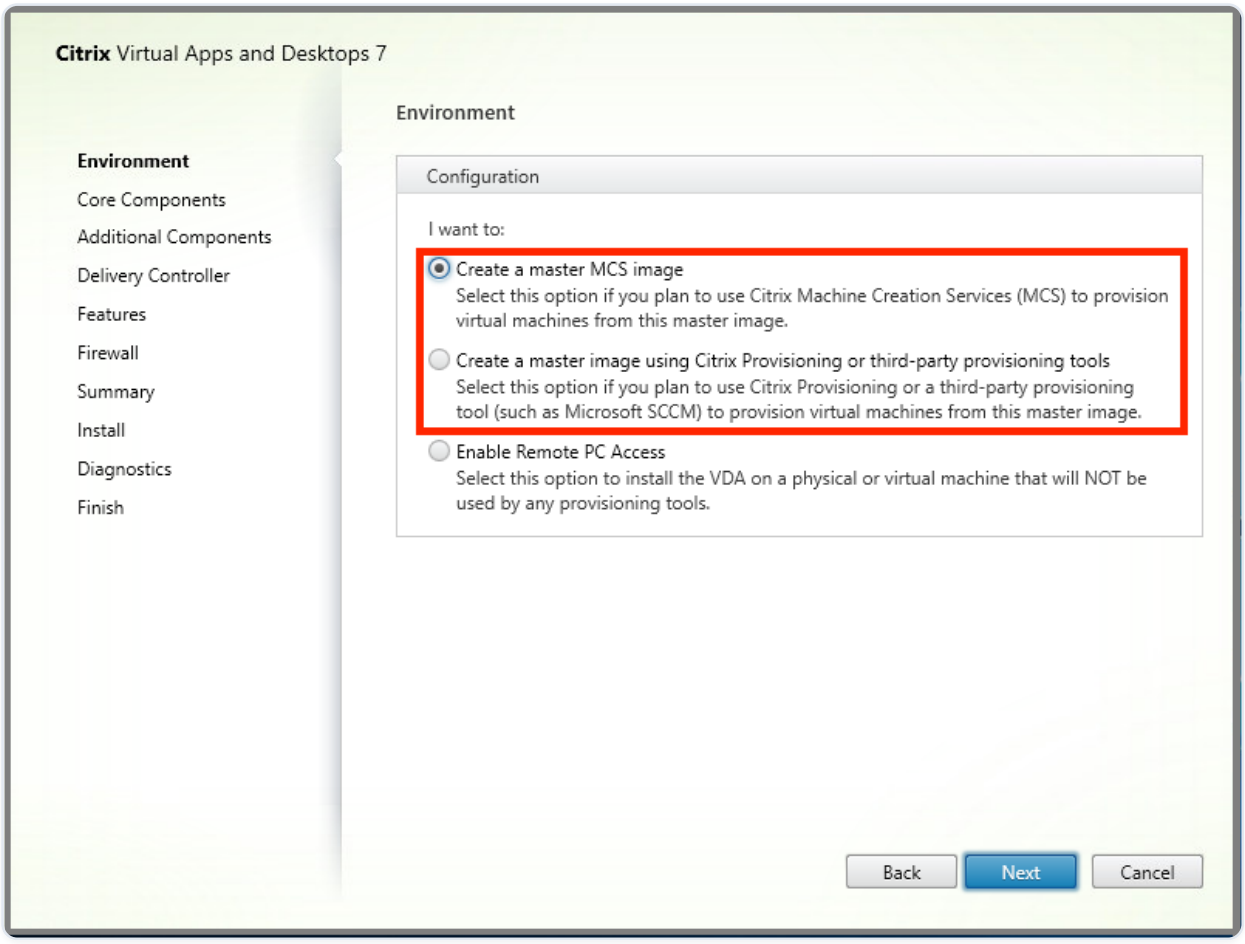
1. マスターイメージを見つけます。組織のエンタープライズアプリケーションと、ユーザーが一般的に役立つと感じるその他のアプリをインストールします。
2. Server VDI を展開する場合は、Server VDI の記事の手順に従ってください。オプションコンポーネントである**ユーザーパーソナライゼーションレイヤー**を必ず含めてください。詳細については、VDA インストール用のコマンドラインオプション を参照してください。
3. Windows 10 を使用している場合は、Virtual Delivery Agent (VDA) 1912 以降をインストールします。古いバージョンの VDA がすでにインストールされている場合は、まず古いバージョン

をアンインストールします。新しいバージョンをインストールする際は、オプションコンポーネントである**Citrix ユーザーパーソナライゼーションレイヤー**を次のように選択してインストールしてください。

a. **Virtual Delivery Agent for Windows Desktop OS**タイルをクリックします。

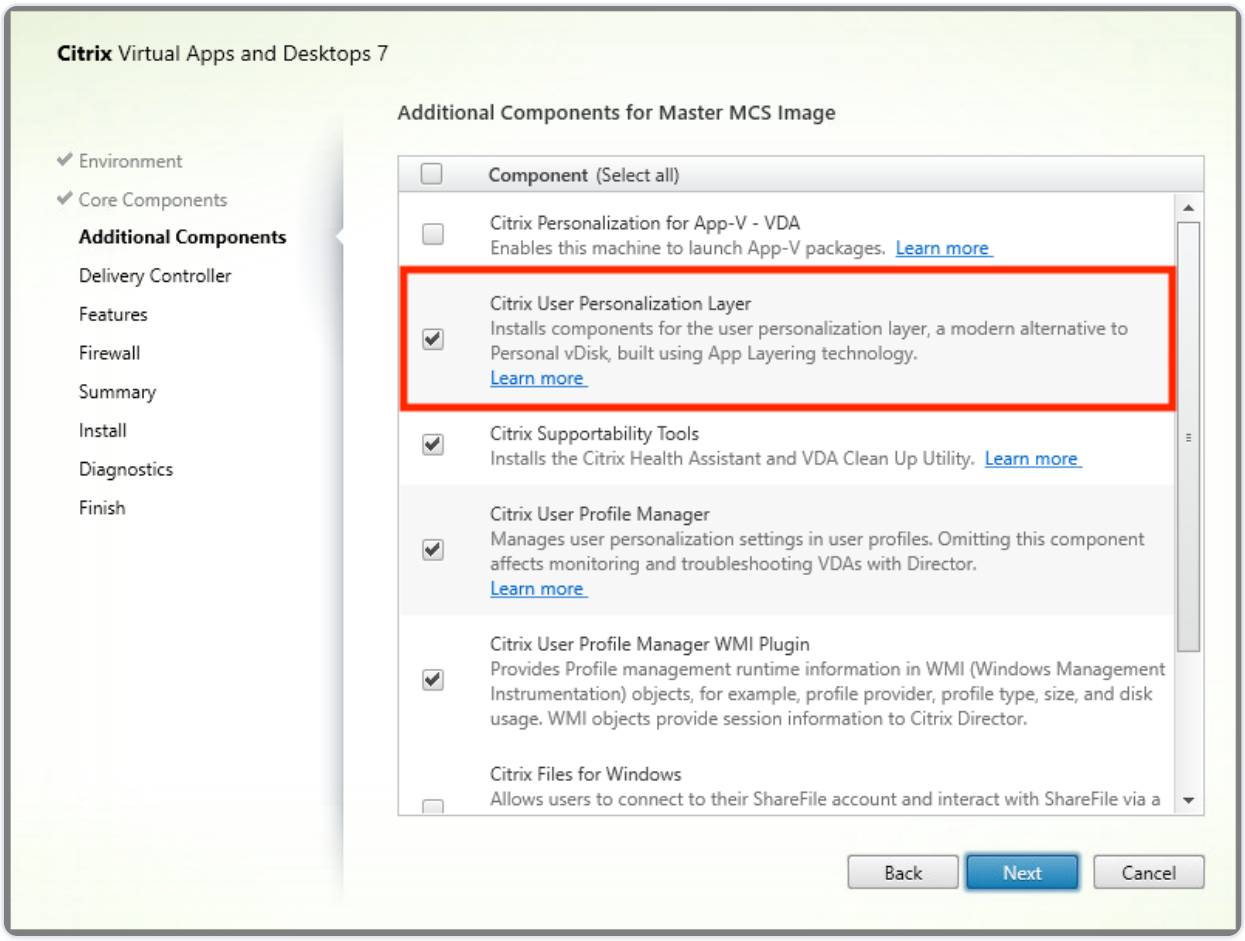


a. **環境:「マスター MCS イメージを作成」**または**「Citrix Provisioning またはサードパーティのプロビジョニングツールを使用してマスターイメージを作成」**のいずれかを選択します。



a. **コアコンポーネント:** 「次へ」をクリックします。

b. **追加コンポーネント:** 「**Citrix ユーザーパーソナライゼーションレイヤー**」をオンにします。



a. 残りのインストール画面を進み、必要に応じて VDA を構成し、「**インストール**」をクリックします。インストール中にイメージが1回以上再起動します。

4. **Windows Update**を無効のままにします。ユーザーパーソナライゼーションレイヤーのインストーラーは、イメージ上の Windows Update を無効にします。更新は無効のままにしてください。

イメージをWeb Studioにアップロードする準備ができました。

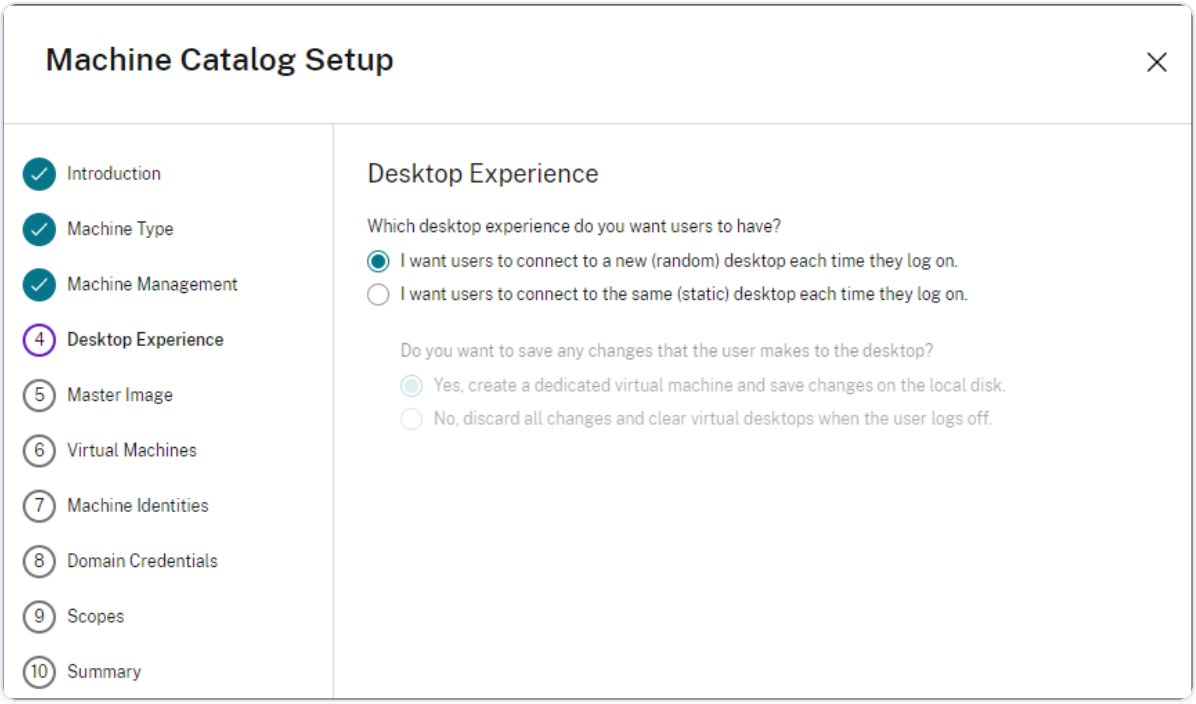
> **注:**
>
> ユーザーパーソナライゼーションレイヤー (UPL) を単にアップグレードしたい場合は、新しいバージョンの UPL とスタンドアロンパッケージを使用してアップグレードできます。VDA をアップグレードする必要はありません。

Step 3: マシンカタログを作成する

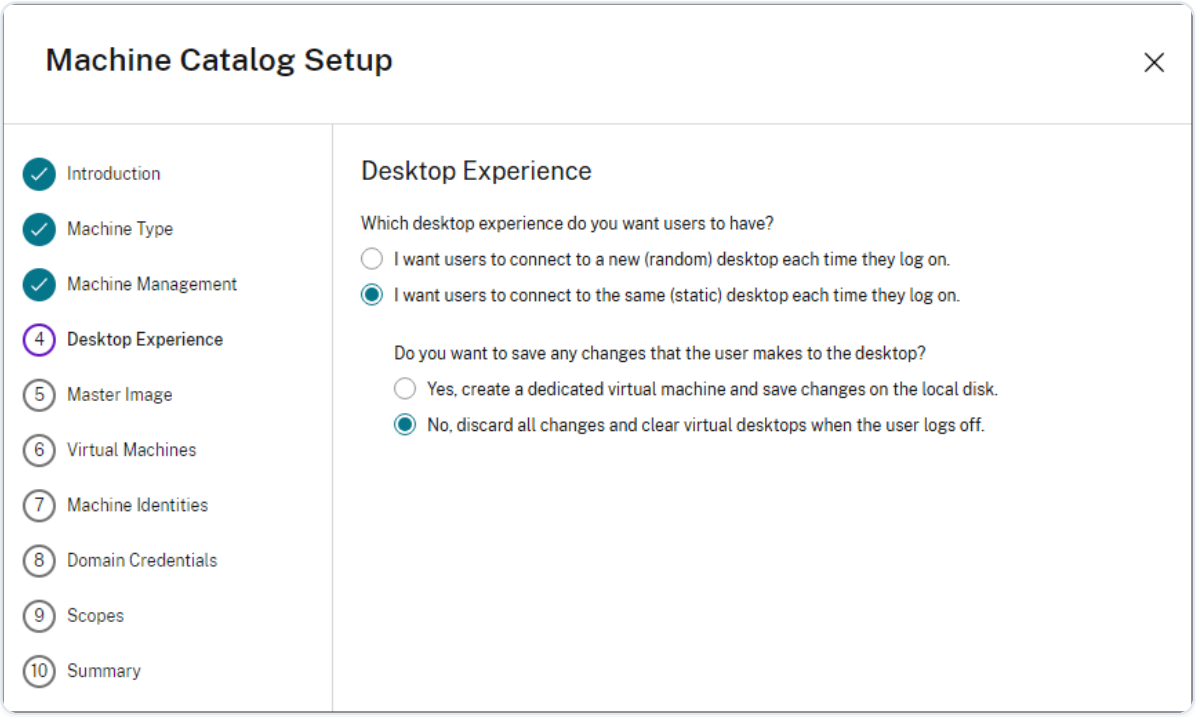
Web Studioで、マシンカタログを作成する手順に従います。カタログ作成時に以下のオプションを使用します。

1. **オペレーティングシステム**を選択し、**シングルセッションOS**に設定します。
2. **マシン管理**を選択し、**電源管理されているマシン**に設定します。たとえば、仮想マシンやブレードPCなどです。
3. **デスクトップエクスペリエンス**を選択し、以下の例のように、**プール型ランダム**または**プール型静的**カタログタイプに設定します。

   - **プールされたランダム:**



   - **プール型静的:** プール型静的を選択した場合、以下のスクリーンショットに示すように、ユーザーがログオフしたときにすべての変更を破棄し、仮想デスクトップをクリアするようにデスクトップを構成します。



注:

ユーザーパーソナライゼーションレイヤーは、Citrix Personal vDiskを使用するように構成されたプール型静的カタログ、または専用仮想マシンとして割り当てられたカタログをサポートしていません。

4. MCSを使用している場合は、**イメージ**と、前のセクションで作成したイメージのスナップショットを選択します。
5. 環境に合わせて、残りのカタログプロパティを構成します。

Step 4: デリバリーグループを作成する

作成したマシンカタログのマシンを含む**デリバリーグループ**を作成および構成します。詳細については、デリバリーグループの作成を参照してください。

ステップ 5: デリバリーグループのカスタムポリシーを作成する

Virtual Delivery Agent内でユーザーレイヤーのマウントを有効にするには、構成パラメータを使用して以下を指定します。

- ネットワーク上のどこでユーザーレイヤーにアクセスするか。
- ユーザーレイヤーディスクがどのくらいのサイズまで拡張するのを許可するか。

パラメータをWeb Studioでカスタムポリシーとして定義し、デリバリーグループに割り当てます。

1. Web Studio にサインインし、左ペインで を選択します。

   Studioでポリシーを選択(/en-us/citrix-virtual-apps-desktops/2511/media/upl-studio-select-policies.png)

2. アクションバーで を選択します。 ウィンドウが表示されます。
3. 検索フィールドに`user layer`と入力します。利用可能なポリシーのリストに次の3つのポリシーが表示されます。

   - ユーザーレイヤーの除外
   - ユーザーレイヤーリポジトリパス
   - ユーザーレイヤーサイズ (GB)

   > **注:**
   >
   > サイズを増やすと、新しいユーザーレイヤーに影響し、既存のユーザーレイヤーが拡張されます。サイズを減らすと、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

   ユーザーレイヤーポリシーの選択(/en-us/citrix-virtual-apps-desktops/2511/media/user-layer-policies.png)

4. **User Layer Repository Path**の横のチェックボックスをオンにして、**編集**をクリックします。**設定の編集**ウィンドウが表示されます。
5. **Value** フィールドにパスを入力し、**Save** をクリックします。

   - **パス形式:** `\\server-name-or-address\share-name\folder`
   - **パスの例:** `\\Server\Share\UPLUsers`
   - **結果のパスの例: CoolCompanyDomainのAlex**という名前のユーザーの場合、パスは次のとおりです。`\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`

   リポジトリパス(/en-us/citrix-virtual-apps-desktops/2511/media/upl-user-layer-repo-enter-path-no-variables.png)

`%USERNAME%`と`%USERDOMAIN%`変数、マシン環境変数、およびActive Directory (AD) 属性を使用してパスをカスタマイズできます。これらの変数を展開すると、明示的なパスになります。

環境変数の例:

- **パス形式:** `\\Server-name-or-address\share-name\folder-with-environment-variables`
- **パスの例:** `\\Server\Share\UPLUserLayers\%USERNAME%\%USERDOMAIN%`
- **結果のパスの例: CoolCompanyDomainのAlex**という名前のユーザーの場合、パスは次のようになります。`\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`

環境変数を含むリポジトリパス(/en-us/citrix-virtual-apps-desktops/2511/media/upl-user-layer-repo-enter-path-variables.png)

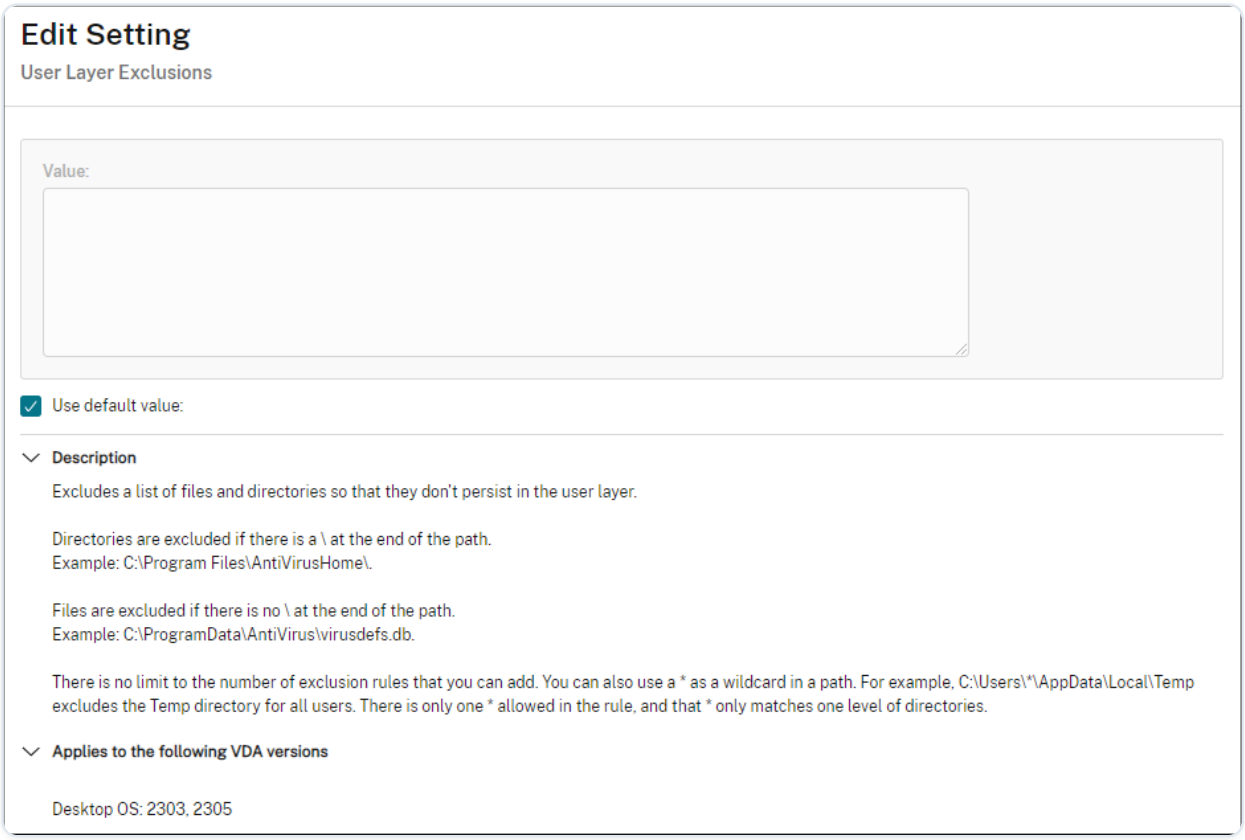
カスタム AD 属性の例:

- パス形式: `\\Server-name-or-address\share-name\AD-attribute`
- パスの例: `\\Server\share#sAMAccountName#`
- 結果のパスの例: `\\Server\share\JohnSmith` (現在のユーザーに対して #sAMAccountName# が JohnSmith に解決される場合)

6. オプション: **ユーザーレイヤーサイズ (GB)** の横にあるチェックボックスをオンにして、**編集**をクリックします。

   ユーザーレイヤーリポジトリパス(/en-us/citrix-virtual-apps-desktops/2511/media/upl-select-user-layer-size.png)

   設定の編集ウィンドウが表示されます。
7. オプション: デフォルト値の **10 GB** を、各ユーザーレイヤーが拡張できる最大サイズに変更します。**保存**をクリックします。
8. オプション: **ユーザーレイヤーの除外**の横にあるチェックボックスをオンにして、**編集**をクリックします。



9. オプション: 除外するファイルとフォルダーを指定し、**保存**をクリックします。詳細については、Citrix App Layering のドキュメントを参照してください。
10. **次へ**をクリックして、割り当てるユーザーとマシンを構成します。この画像で強調表示されている**デリバリーグループの割り当て**リンクをクリックします。

    ユーザーレイヤーリポジトリパス(/en-us/citrix-virtual-apps-desktops/2511/media/upl-delivery-group-assign.png)
11. **デリバリーグループ**メニューで、前のセクションで作成したデリバリーグループを選択します。**OK**をクリックします。

    デリバリーグループを選択(/en-us/citrix-virtual-apps-desktops/2511/media/upl-delivery-group-select.png)
12. ポリシーの名前を入力します。チェックボックスをオンにしてポリシーを有効にし、**完了**をクリックします。

    ユーザーレイヤーポリシー名(/en-us/citrix-virtual-apps-desktops/2511/media/upl-name-policy.png)

ユーザーレイヤーフォルダーのセキュリティ設定を構成する

ドメイン管理者として、ユーザーレイヤーのストレージの場所を複数指定できます。各ストレージの場所 (デフォルトの場所を含む) に `\Users` サブフォルダーを作成します。次の設定を使用して、各場所を保護します。

設定名	値	適用先	
作成者/所有者	変更	サブフォルダーとファイルのみ	
所有者の権利	変更	サブフォルダーとファイルのみ	
ユーザーまたはグループ	フォルダーの作成/データの追加。フォルダーの横断/ファイルの実行。フォルダーの一覧表示/データの読み取り。属性の読み取り	選択したフォルダーのみ	
システム	フルコントロール	選択されたフォルダー、サブフォルダー、およびファイル	
ドメイン管理者、および選択された管理者グループ	フルコントロール	選択されたフォルダー、サブフォルダー、およびファイル	

ユーザーレイヤーメッセージ

ユーザーがユーザーレイヤーにアクセスできない場合、次のいずれかの通知メッセージが表示されます。

- **ユーザーレイヤーが使用中です**

  `We were unable to attach your user layer because it is in use. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **ユーザーレイヤーが利用できません**

`We were unable to attach your user layer. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **ユーザーサインアウト後にシステムがリセットされませんでした**

`This system was not shut down properly. Please log off immediately and contact your system administrator.`.

トラブルシューティング時に使用するログファイル

ログファイル ulayersvc.log には、変更がログに記録されるユーザーパーソナライゼーションレイヤーソフトウェアの出力が含まれています。

```
C:\ProgramData\Unidesk\Logs\ulayersvc.log
```

ユーザーレイヤー/UPL領域の再利用

ユーザーがログオフするたびにVHDXファイルを自動的に圧縮するために、**User Layer/UPL領域の再利用**を使用できます。 詳細については、「User Layer/UPL領域の再利用」(/ja-jp/citrix-app-layering/4/layer/enable-user-layers.html#user-layerupl-space-reclamation)を参照してください。

制限事項

ユーザーパーソナライズレイヤー機能をインストールおよび使用する際は、以下の制限事項に留意してください。

- App Layering内のレイヤーにユーザーパーソナライズレイヤーソフトウェアを展開しようとしないでください。Citrix Virtual Apps and Desktopsでユーザーパーソナライズレイヤーを展開するか、App Layeringイメージテンプレートでユーザーレイヤーを有効にするかのいずれかにしてください（両方は不可）。どちらのプロセスでも、必要なユーザーレイヤーが生成されます。
- 永続的なマシンカタログでユーザーパーソナライズレイヤー機能を構成しないでください。
- セッションホストは使用しないでください。
- 新しいOSインストールを実行しているイメージ（Windows 10の同じバージョンであっても）でマシンカタログを更新しないでください。ベストプラクティスは、マシンカタログの作成時に使用したのと同じマスターイメージ内でOSの更新を適用することです。
- ブート時ドライバーまたはその他の早期ブートパーソナライズは使用しないでください。
- PvDデータをユーザーパーソナライズレイヤー機能に移行しないでください。

- 完全なApp Layering製品からの既存のユーザーレイヤーをユーザーパーソナライズレイヤー機能に移行*しないでください*。
- 異なるマスターOSイメージを使用して作成されたユーザーレイヤーにアクセスするために、ユーザーレイヤーのSMBパスを変更*しないでください*。
- ユーザーがセッションからログアウトして再度ログインすると、新しいセッションはプール内の別のマシンで実行されます。VDI環境では、Microsoft Software Centerは、最初のマシンではアプリケーションを**インストール済み**と表示しますが、2番目のマシンでは**利用不可**と表示します。

  アプリケーションの実際の状態を確認するには、ユーザーにSoftware Centerでアプリケーションを選択し、**インストール**をクリックするように指示します。その後、SCCMはステータスを実際の値に更新します。
- ユーザーパーソナライズレイヤー機能が有効になっているVDA内でSoftware Centerを起動すると、すぐに停止することがあります。この問題を回避するには、Microsoftの「Implementing SCCM in a XenDesktop VDI environment」に関する推奨事項に従ってください。また、Software Centerを起動する前に、`ccmexec`サービスが実行されていることを確認してください。
- グループポリシー（コンピューターの構成）では、ユーザーレイヤーの設定がマスターイメージに適用された設定を上書きします。したがって、GPOを使用してコンピューターの構成で行った変更は、次回のセッションログイン時に常にユーザーに適用されるとは限りません。

  この問題を回避するには、次のコマンドを発行するユーザーログオンスクリプトを作成します。

  ```
  gpupdate /force
  ```

  例えば、ある顧客は、各ユーザーログイン時に次のコマンドを実行するように設定しました。

  ```
  gpudate /Target:Computer /force
  ```

  最良の結果を得るには、ユーザーがログインした後で、コンピューター設定への変更をユーザーレイヤーに直接適用します。
- ドメインユーザーアカウントは、マスターイメージに最後にログインしたユーザーであってはなりません。そうしないと、そのイメージからプロビジョニングされたマシンで問題が発生する可能性があります。
- 純粋なMicrosoft Entra環境でUPLが有効になっている場合、Azureで実行されているWindowsの根本的な問題により、カスタム証明書は保持されません。Microsoftが将来の機能強化でこの問題を修正した場合、この記事を更新します。

コンポーネントの削除

コンポーネントを削除するには、プログラムの削除または変更を行うWindows機能を使用することをお勧めします。または、コマンドラインまたはインストールメディア上のスクリプトを使用してコンポーネントを削除することもできます。

コンポーネントを削除しても、前提条件は削除されず、ファイアウォール設定も変更されません。たとえば、Delivery Controller™を削除しても、SQL Serverソフトウェアとデータベースは削除されません。

Web Interfaceを含む以前の展開からControllerをアップグレードした場合は、Web Interfaceコンポーネントを個別に削除する必要があります。インストーラーを使用してWeb Interfaceを削除することはできません。

以下に記載されていない機能の削除については、その機能のドキュメントを参照してください。

準備

Controllerを削除する前に、サイトから削除してください。詳細については、「Controllerの削除」を参照してください。

StudioとDirectorを削除する前に、それらを閉じます。

Windowsのプログラムの削除または変更機能を使用してコンポーネントを削除する

Windowsのプログラムの削除または変更機能から：

- Controller、Studio、Director、License Server、またはStoreFrontを削除するには、**Citrix Virtual Apps *version*** または **Citrix Virtual Apps and Desktops™ *version*** を右クリックし、**Uninstall** を選択します。インストーラーが起動します。削除するコンポーネントを選択します。

  または、**Citrix StoreFront** を右クリックし、**Uninstall** を選択してStoreFront™を削除することもできます。

- VDAを削除するには、**Citrix Virtual Delivery Agent *version*** を右クリックし、**Uninstall** を選択します。インストーラーが起動し、削除するコンポーネントを選択できます。デフォルトでは、削除後にマシンは自動的に再起動します。
- Universal Print Serverを削除するには、**Citrix Universal™ Print Server** を右クリックし、**Uninstall** を選択します。

コマンドラインを使用してコアコンポーネントを削除する

`\x64\XenDesktop Setup`ディレクトリから、`XenDesktopServerSetup.exe`コマンドを実行します。

- 1つまたは複数のコンポーネントを削除するには、`/remove` および `/components` オプションを指定します。
- すべてのコンポーネントを削除するには、`/removeall` オプションを指定します。

コマンドとパラメーターの詳細については、「コマンドラインを使用したインストール」を参照してください。

例えば、次のコマンドはWeb Studioを削除します。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components webstudio
```

アップグレード中に、`\x64\Licensing\CitrixLicensing.exe /quiet` または `\x64\Licensing\CitrixLicensing.exe /quiet /l install.log` コマンドを使用して最初にライセンスサーバーをインストールし、次にコアコンポーネントをインストールした場合は、同じ順序でアンインストールしてください。

1. コマンドラインを使用してライセンスサーバーをアンインストールします。

   ```
   CitrixLicensing.exe /quiet /uninstall /l uninstall.log
   ```

2. GUIまたはコマンドラインを使用してコンポーネントをアンインストールします。詳細については、「コンポーネントの削除」を参照してください。

コマンドライン `XenDesktopServerSetup.exe` または `removeall` を使用してライセンスサーバーとコンポーネントをアンインストールする場合は、レジストリエントリと残りのファイルをクリーンアップしてください。

レジストリエントリをクリーンアップするには：

1. レジストリキー `Citrix Licensing` を検索し、そのエントリを削除します。ほとんどの場合、エントリは次の場所で見つけることができます。

   ```
   "Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Cur
   rentVersion\Uninstall\
   ```

2. レジストリキーの **Uninstall String** が指すフォルダーを削除します。

コマンドラインを使用してVDAを削除する

`\x64\XenDesktop Setup`ディレクトリから、`XenDesktopVdaSetup.exe`コマンドを実行します。

- 1つ以上のコンポーネントを削除するには、`/remove`オプションと`/components`オプションを使用します。例えば、VDAとCitrix Workspaceアプリを削除するには、`/remove /components vda,plugin`を使用します。
- `/removeall`オプションはVDAのみを削除します。Citrix Workspaceアプリは削除しません。

コマンドとパラメーターの詳細については、コマンドラインを使用したインストール を参照してください。

デフォルトでは、削除後にマシンが自動的に再起動します。

Active Directoryでスクリプトを使用してVDAを削除するには、スクリプトを使用したVDAのインストールまたは削除 を参照してください。

アップグレードと移行

注：

従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきたファイルベースのライセンスシステムは、April 15, 2026にサポート終了 (EOL) となります。License Activation Service (LAS) は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。April 15, 2026以降、Citrixオンプレミスコンポーネントをアクティベートおよびライセンス供与する唯一の方法はLASになります。サポートを継続するには、Citrix Virtual Apps and Desktopsの展開がLAS互換バージョンである必要があります。LAS互換の最小要件となるCVADバージョンは次のとおりです。

- CVAD 2203 LTSR CU7
- CVAD 2402 LTSR CU3
- CVAD 2507 LTSR
- CVAD 2411

ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrixは、これらの要件を遵守しない場合、Citrixが法律上または衡平法上持つ可能性のあるその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止する場合があります。これらの要件は、法律または規制によって禁止されている場合は適用されません。

はじめに

アップグレードすると、新しいマシンやサイトをセットアップすることなく、展開がCitrix Virtual Apps and Desktops™ 7 **Current Release (CR)** に変更されます。これはインプレースアップグレードとして知られています。

アップグレードすると、利用資格のある最新の機能とテクノロジーにアクセスできます。アップグレードには、以前のバージョンからの修正、明確化、および機能強化も含まれる場合があります。

アップグレードの概要

1. アップグレードを開始する前に、展開のアップグレード の記事を確認してください。これは、アップグレードの準備と実装方法を学ぶための主要な情報源です。
2. 現在のカスタマーサクセスサービスの日付が有効であり、期限切れになっていないことを確認してください。詳細については、カスタマーサクセスサービスの更新ライセンス の記事を参照してください。
3. 準備に関するガイダンスを完了します。
4. コアコンポーネントをアップグレードするためにインストーラーを実行します。
5. システムデータベースとサイトをアップグレードします。
6. イメージ上のVDA（またはマシンに直接）をアップグレードします。
7. その他のコンポーネントをアップグレードします。

各準備およびアップグレードの手順については、展開のアップグレードで詳しく説明しています。

アップグレード可能なバージョン

Citrix Virtual Apps™ and Desktops 2507 LTSR へは、以下からアップグレードできます。

- Virtual Apps and Desktops 2402 LTSR（CUの有無にかかわらず、CU2までを含む）
- Virtual Apps and Desktops 2203 LTSR（CUの有無にかかわらず、CU6までを含む）
- Citrix Virtual Apps and Desktopsの現在サポートされているCRバージョン

> 注:
>
> - アップグレードプロセスを開始する前に、Citrix®は、管理された環境でアップグレードをテストし、特定の要件を満たしていることを確認することを推奨します。さらに、シームレスな移行を確実にするために、廃止リストや既知の問題を含むすべての関連製品ドキュメントを確認することをお勧めします。このアプローチは、本番システムへの潜在的な中断を軽減し、全体的なアップグレードエクスペリエンスを向上させるのに役立ちます。 サポートされているバージョンのリストの詳細については、製品マトリックスを参照してください。

よくある質問

このセクションでは、Citrix Virtual Apps and Desktopsのアップグレードに関するよくある質問に回答します。

- **Virtual Apps and Desktops環境をアップグレードする正しい順序は何ですか？**

  推奨されるアップグレードシーケンスの図と説明については、アップグレードシーケンスおよびアップグレード手順を参照してください。

- **私のサイトには複数のDelivery Controller（異なるゾーンにあります）があります。一部のみをアップグレードした場合、どうなりますか？同じメンテナンス期間中にサイト内のすべてのControllerをアップグレードする必要がありますか？**

  各Controller上のさまざまなサービスが相互に通信するため、すべてのDelivery Controllerを同じメンテナンスウィンドウ中にアップグレードすることがベストプラクティスです。異なるバージョンを維持すると問題が発生する可能性があります。メンテナンスウィンドウ中に、Controllerの半分をアップグレードし、サイトをアップグレードしてから、残りのControllerをアップグレードすることをお勧めします。詳細については、アップグレード手順を参照してください。

- **最新バージョンに直接アップグレードできますか、それとも段階的なアップグレードを行う必要がありますか？**

  アップグレード先のバージョンの **新機能** の記事で明示的に記載されていない限り、ほとんどの場合、中間リリースをスキップして最新バージョンにアップグレードできます。

- **お客様はLong Term Service Release (LTSR) 環境からCurrent Releaseにアップグレードできますか？**

  はい。お客様は長期にわたってLong Term Service Releaseにとどまる必要はありません。お客様は、ビジネス要件と機能に基づいて、LTSR環境をCurrent Releaseに移行できます。

- **コンポーネントの混在バージョンは許可されていますか？**

  各サイト内では、すべてのコンポーネントを同じバージョンにアップグレードすることをCitrixは推奨しています。一部のコンポーネントで以前のバージョンを使用することはできますが、最新バージョンのすべての機能が利用できない場合があります。詳細については、混在環境に関する考慮事項を参照してください。

- **Current Releaseはどのくらいの頻度でアップグレードする必要がありますか？**

Current Release は、リリース日から 6 か月後に End of Maintenance (EOM) に達します。Citrix は、お客様が最新の Current Release を採用することを推奨しています。Current Release は、リリース日から 18 か月後に End of Life (EOL) に達します。

- **推奨されるのは、LTSRへのアップグレードですか、それともCRへのアップグレードですか？**

  Current Release (CR) は、最新かつ最も革新的なアプリ、デスクトップ、およびサーバー仮想化の機能を提供します。これにより、最先端のテクノロジーを維持し、競合他社の一歩先を行くことができます。

  Long Term Service Release（LTSR）は、長期間同じベースバージョンを維持することを好む大規模なエンタープライズ本番環境に最適です。

> For details, see [Servicing Options](https://www.citrix.com/support/citrix-customer-success-services/citrix-virtual-apps-and-desktops-servicing-options.md).

- **ライセンスをアップグレードする必要がありますか？**

  現在のライセンスの有効期限が切れておらず、アップグレード先のリリースで有効であることを確認してください。CTX111618を参照してください。更新については、Customer Success Services renewal licensesを参照してください。

- **アップグレードにはどのくらい時間がかかりますか？**

  展開のアップグレードにかかる時間は、インフラストラクチャとネットワークによって異なります。そのため、正確な時間をお伝えすることはできません。

- **ベストプラクティスは何ですか？**

  準備ガイダンスを理解し、それに従ってください。

- **Citrix Virtual Apps and Desktopsサイトのアップグレードにはsysadmin権限が必要ですか？**

  いいえ。Windows認証（デフォルト）を使用する標準的なサイトアップグレードの場合、既存のデータベース（サイト、ログ、監視）に対するdb_owner権限があれば、サイトマネージャーがスキーマを更新するのに十分です。sysadminは、主に最初のサイト作成時、またはプロセスが新しいデータベースとサーバーレベルのログインを自動的に作成する必要がある場合にのみ必要です。

- **アップグレード中にサイトマネージャーが管理者権限を要求することがあるのはなぜですか？**

  アップグレードにサーバーレベルのアクションが必要な場合、サイトマネージャーは管理者権限を確認することがあります。たとえば、次のとおりです。

  - 新しいDelivery Controllerの追加：これには、Delivery ControllerのマシンID用の新しいSQLログインの作成が必要です。
  - ログインの変更：`securityadmin`または`dbcreator`ロールを必要とするアクションは、sysadminの要求に簡略化されることがよくあります。
  - 自動作成：サイトマネージャーが、事前準備されたスクリプトを使用するのではなく、新しいデータベース構造を自動的に作成したり、ユーザーをマッピングしたりするタスクを負っている場合。

- **Citrix管理者にsysadmin権限を付与せずにデータベースをアップグレードできますか？**

  はい、手動アップグレードを実行することでアップグレードできます。Citrix管理者はSite Managerを使用してアップグレードSQLスクリプトを取得し、そのスクリプトをデータベース所有者に提供してデータベースのアップグレードを実行します。データベースがアップグレードされた後、Citrix管理者はSite Managerに戻り、アップグレードプロセス全体を完了します。

- **Citrixサービスはなぜマシンアカウントで実行されるのですか？**

  Citrixサービスは、デフォルトでネットワークサービスアカウントで実行されます。これは、サーバーが自身のID（マシンアカウント、例えばDOMAIN\SERVER$）を使用して、手動のパスワード管理なしに他のサーバーやSQLデータベースと安全に通信できるためです。この設定はWindows認証に依存しており、Active Directory内の既存の信頼関係を利用するため、SQLへの接続において最も安全で推奨される方法です。

- **サポートされているオペレーティングシステムは何ですか？**

  アップグレード先のバージョンのシステム要件の記事に、サポートされているOSが記載されています。

  現在の展開でサポートされなくなったオペレーティングシステムを使用している場合は、以前のオペレーティングシステムを参照してください。

- **サポートされているVMware vSphere (vCenter + ESXi) のバージョンは何ですか？**

  CTX131239には、サポートされているホストとバージョン、および既知の問題へのリンクが記載されています。

- **私のバージョンはいつEOLになりますか？**

  製品マトリックスを確認してください。

- **最新リリースにおける既知の問題は何ですか？**

  - シトリックス バーチャル アプリケーションズ アンド デスクトップス
  - StoreFront

- シトリックス プロビジョニング
- シトリックス ライセンス サーバー
- Windows向けCitrix Workspaceアプリ

詳細情報

Long Term Service Release (LTSR) の展開の更新には、累積更新プログラム (CU) が使用されます。CU は LTSR のベースラインコンポーネントを更新し、各 CU には独自のメタインストーラーが含まれています。

各 CU には専用のドキュメントがあります。たとえば、2203 LTSR の場合、最新の CU については、その LTSR の「**新機能**」ページのリンクを確認してください。各 CU ページには、サポートされているバージョン情報、手順、および CU ダウンロードパッケージへのリンクが含まれています。

移行

クラウドへの移行

Citrix Virtual Apps and Desktopsの自動構成ツールを使用して、オンプレミス展開をクラウドに移行できます。詳しくは、「クラウドへの移行」を参照してください。

レガシー移行

移行とは、以前の展開から新しいバージョンにデータを移動することです。このプロセスには、新しいコンポーネントのインストールと新しいサイトの作成、古いファームからのデータのエクスポート、そして新しいサイトへのデータのインポートが含まれます。

XenApp および XenDesktop のバージョンを移行するための、または以前の Citrix Virtual Apps and Desktops のバージョンを移行するためのサポートされているツールやスクリプトはありません。この製品ドキュメントで説明されている Citrix Virtual Apps and Desktops のバージョンについては、*アップグレード*がサポートされています。

以前のXenApp 6.xの移行コンテンツについては、以下を参照してください。スクリプトも記事もサポートまたは保守されていません。

- XenApp 6.x バージョン用のオープンソース移行スクリプトは`<https://github.com/citrix/xa65migrationtool>`で入手できます。Citrix はこれらの移行スクリプトをサポートまたは保守していません
- 7.x での変更点

- XenApp 6.5 ワーカーを新しい VDA にアップグレードする
- XenApp 6.x を移行する

展開のアップグレード

注:

従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきたファイルベースのライセンスシステムは、April 15, 2026にサポート終了 (EOL) となります。(/ja-jp/licensing/current-release/license-activation-service.html) (LAS) は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。April 15, 2026以降、Citrixオンプレミスコンポーネントをアクティベートおよびライセンス供与する唯一の方法はLASになります。サポートを継続するには、Citrix Virtual Apps and Desktopsのデプロイメントが LAS互換バージョンである必要があります。LAS互換の最小要件となるCVADバージョンは次のとおりです。

- CVAD 2203 LTSR CU7
- CVAD 2402 LTSR CU3
- CVAD 2507 LTSR
- CVAD 2411

ご質問やご不明な点がある場合は、カスタマーケアにお問い合わせください。Citrixは、これらの要件を遵守しない場合、Citrixが法律または衡平法上持つ可能性のあるその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止する場合があります。これらの要件は、法律または規制によって禁止されている場合は適用されません。

はじめに

注:

この記事では、Web Studioを含む展開のアップグレードについて説明します。Citrix Studioを含むアップグレードについては、Citrix Virtual Apps and Desktops™ 7 2212以前の同等の記事を参照してください。

> 新しいマシンやサイトを最初にセットアップすることなく、特定の展開を新しいバージョンにアップグレードできます。これはインプレースアップグレードと呼ばれます。

アップグレードできるCitrix Virtual Apps and Desktopsのバージョンについては、(/ja-jp/citrix-virtual-apps-desktops/2511/upgrade-migrate.html#versions-you-can-upgrade)を参照してください。

Citrix Virtual Apps and Desktopsのいずれかのリリースにアップグレードする前に、現在のCustomer Success Servicesの有効期限が切れていないことを確認してください。詳細については、(/ja-jp/licensing/current-release/customer-success-services.html#customer-success-services-renewal-licenses)の記事を参照してください。

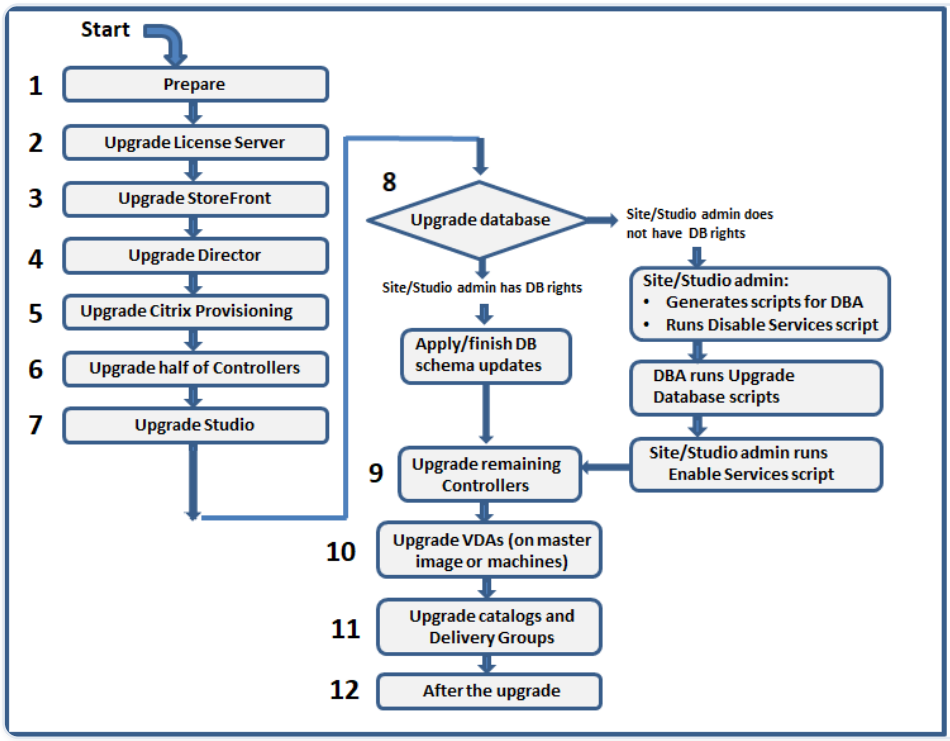
アップグレードを開始するには、新しいバージョンのインストーラーを実行して、以前にインストールされたコアコンポーネント、VDA、および特定のその他のコンポーネントをアップグレードします。次に、データベースとサイトをアップグレードします。

新しいバージョンが提供されている場合、フルプロダクトインストーラー（およびスタンドアロンVDAインストーラー）でインストールできる任意のコンポーネントをアップグレードできます。フルプロダクトインストーラーでインストールされないその他のコンポーネント（Citrix Provisioning™やProfile Managementなど）については、そのコンポーネントのドキュメントを参照してください。ホストのアップグレードについては、適切なドキュメントを参照してください。

アップグレードを開始する前に、この記事のすべての情報を確認してください。

アップグレードシーケンス

次の図は、アップグレードシーケンスの手順を示しています。アップグレード手順には、図の各ステップの詳細が含まれています。



注:

障害を回避するため、新しいマシンカタログの作成、マシンカタログの削除、デリバリーグループ内のマシンの更新など、プロビジョニングおよびデリバリーグループ関連のタスクを実行する前に、すべてのDelivery Controllerとデータベースをアップグレードする必要があります。

ハイブリッド権限ライセンス

ハイブリッド権限ライセンスは、顧客が永続ライセンスからクラウドサービスサブスクリプションに移行またはアップグレードする際に、クラウドサービスサブスクリプションに加えて提供される期間ベースのサブスクリプションライセンスです。DaaSサブスクリプションでハイブリッド権限アドオンを購入することもできます。

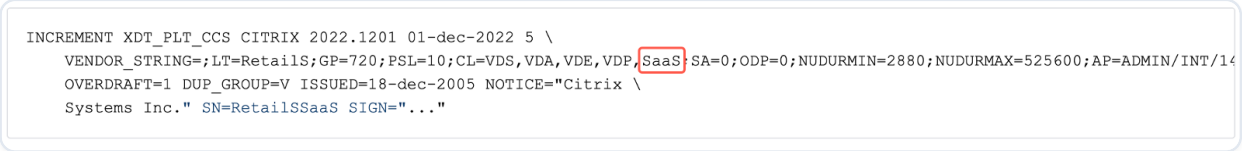
SaaS属性を持つハイブリッドライセンスをお持ちの場合、Citrix Virtual Apps™ and Desktops LTSR 2203以降にアップグレードすると、Citrix Virtual Apps and Desktops LTSR 1912では利用できなかった機能にアクセスできるようになります。これらの機能には、Microsoft Azure、AWS EC2、Google Cloudなどのパブリッククラウドでのワークロードのプロビジョニングとホスティングが含まれます。新しいライセンスファイルを展開する前に、ライセンスサーバーを最新バージョンに更新してください。この前提条件を満たさない場合、Citrix Virtual Apps and Desktopsサイトのアップグレードとサイトの作成がブロックされます。

SaaS属性のないハイブリッドライツライセンスにアクセスできる場合は、次の手順に従ってSaaS属性を持つ新しいハイブリッドライツライセンスにアクセスしてください。

注:

- 新しいライセンスコードが記載されたメールが届きます。詳しくは、「ライセンスアクセスコードの使用」を参照してください。
- 既存のライセンスは取り消されます。取り消されたライセンスはライセンスサーバーから削除し、その後新しいライセンスをインストールする必要があります。詳しくは、「ライセンスファイルの削除」を参照してください。

1. citrix.comのライセンス管理ポータルにアクセスし、クラウドプロビジョニング権限が有効になっている（SaaS属性を持つ）新しいハイブリッド権限ライセンスファイルをダウンロードします。詳細については、ライセンスのダウンロードを参照してください。次の画像は、インクリメントセクションにSaaS属性を持つハイブリッド権限ライセンスファイルを示しています。



2. ハイブリッド権限ライセンスファイルをライセンスサーバーにインストールします。詳しくは、「ライセンスのインストール」を参照してください。
3. ライセンスのエディションまたはモデルに変更がある場合は、brokerコマンドを実行してエディションとモデルを設定してから、インプレースアップグレードを開始してください。Brokerコマンドについて詳しくは、「Broker PowerShell SDK」セクションを参照してください。

Citrix Virtual Apps and DesktopsのCurrent ReleasesおよびLong Term Service Releasesでのパブリッククラウドのサポートについて詳しくは、「CTX270373」を参照してください。

アップグレード手順

主要な製品コンポーネントのほとんどは、コンポーネントを含むマシンで製品インストーラーを実行することでアップグレードできます。

1台のマシンに複数のコンポーネント（Studioやライセンスサーバーなど）が含まれている場合、製品メディアにそれらのソフトウェアの新しいバージョンが含まれていれば、そのマシン上のすべてのコンポーネントがアップグレードされます。

インストーラーを使用するには：

- フル製品インストーラーのグラフィカルインターフェイスを実行するには、マシンにログオンし、メディアを挿入するか、新しいリリースのISOドライブをマウントします。**AutoSelect**をダブルクリックします。
- コマンドラインインターフェイスを使用するには、適切なコマンドを発行します。「コマンドラインを使用したインストール」を参照してください。

手順1：準備

アップグレードを開始する前に、準備が整っていることを確認してください。必要なタスクを読み、完了してください。

- PVD、AppDisks™、およびサポートされていないホストの削除
- PvDまたはAppDiskコンポーネントを持つVDA
- 制限事項
- 混合環境に関する考慮事項(#mixed-environment-considerations)
- 以前のオペレーティングシステム(#earlier-operating-systems)
- 準備(#preparation)
- 事前サイトテスト(#preliminary-site-tests)
- SQL Serverのバージョンチェック(#sql-server-version-check)

ステップ2：ライセンスサーバーのアップグレード

インストールにCitrixライセンスサーバーソフトウェアの新しいバージョンが含まれている場合は、他のコンポーネントよりも先にこのコンポーネントをアップグレードしてください。

まだライセンスサーバーが新しいバージョンと互換性があるかどうかを判断していない場合は、他のコアコンポーネントをアップグレードする前に、ライセンスサーバーでインストーラーを実行することが不可欠です。

ステップ3：StoreFront™のアップグレード

インストールメディアに新しいバージョンのStoreFrontソフトウェアが含まれている場合は、StoreFrontサーバーを含むマシンでインストーラーを実行します。

- グラフィカルインターフェイスで、 セクションから を選択します。
- コマンドラインから、Citrix Virtual Apps and Desktopsインストールメディアの`x64`フォルダーにある`CitrixStoreFront-x64.exe`を実行します。

ステップ4：Directorのアップグレード

インストールメディアに新しいバージョンのDirectorソフトウェアが含まれている場合は、Directorを含むマシンでインストーラーを実行します。

ステップ5：Citrix Provisioningのアップグレード

Citrix Provisioningのインストールメディアは、Citrix Virtual Apps and Desktopsのインストールメディアとは別に提供されています。Citrix Provisioningサーバーおよびターゲットデバイスソフトウェアのインストールとアップグレードの方法については、Citrix Provisioning製品ドキュメントを参照してください。

ステップ6：Delivery Controller の半分をアップグレードする

たとえば、サイトに4つのControllerがある場合、そのうちの2つでインストーラーを実行します。

Controller の半分をアクティブなままにしておくことで、ユーザーはサイトにアクセスできます。VDAは残りのControllerに登録できます。Controllerの数が少ないため、サイトの容量が低下する場合があります。アップグレードは、最終的なデータベースアップグレード手順中に新しいクライアント接続を確立する際に、一時的な中断のみを引き起こします。アップグレードされたControllerは、サイト全体がアップグレードされるまで要求を処理できません。

サイトにControllerが1つしかない場合、アップグレード中は動作しません。

実際のアップグレードが開始される前に、最初のControllerでサイトの事前テストが実行されます。詳細については、サイトの事前テストを参照してください。

> **注：**
>
> Site Managerは、Delivery Controllerとともに自動的にアップグレードされます。

ステップ7：Web Studio をアップグレードする

Web Studio をまだアップグレードしていない場合（別のコンポーネントと同じマシンにあったため）、Studio が含まれているマシンでインストーラーを実行します。

> **注：**

Web Studio をアップグレードした後、バージョン情報がすぐに更新されない場合があります。Web Studio がすでに最新であるにもかかわらず、アップグレードを促されることがあります。この問題に対処するには、Web Studio サーバーに移動し、Internet Information Services (IIS) マネージャーを開き、 > > に移動して、 ペインで を選択します。

ステップ8：データベースとサイトをアップグレードする

注：

障害を回避するには、新しいマシンカタログの作成、マシンカタログの削除、デリバリーグループ内のマシンの更新など、プロビジョニングおよびデリバリーグループ関連のタスクを実行する前に、すべてのDelivery Controllerとデータベースをアップグレードする必要があります。

SQL Serverデータベースのスキーマを更新するために必要な権限については、準備を確認してください。

- SQL Serverデータベースのスキーマを更新する十分な権限がある場合は、データベースの自動アップグレードを開始できます。データベースとサイトを自動的にアップグレードするに進んでください。
- データベースの十分な権限がない場合は、スクリプトを使用する手動アップグレードを開始し、データベース管理者（必要な権限を持つユーザー）の助けを借りて続行できます。手動アップグレードの場合、Site Managerユーザーがスクリプトを生成し、サービスを有効/無効にするスクリプトを実行します。データベース管理者は、SQLCMDユーティリティまたはSQLCMDモードのSQL Server Management Site Managerを使用して、データベーススキーマを更新する他のスクリプトを実行します。データベースとサイトを手動でアップグレードするに進んでください。
- マルチゾーン展開があり、データベースとサイトを自動的にアップグレードしたい場合は、サイトのSQL Serverデータベースをホストするのと同じゾーンでdbschemaアップグレードを実行することをCitrixは推奨します。そうしないと、データベースとサイトの自動アップグレードが失敗する可能性があります。

Citrix は、アップグレード前にデータベースをバックアップすることを強く推奨します。CTX135207 を参照してください。データベースのアップグレード中は、製品サービスが無効にな

ります。その間、Controller はサイトの新しい接続を仲介できないため、慎重に計画してください。

データベースとサイトを自動的にアップグレードする

1. アップグレードされたDelivery ControllerでSite Managerを起動します。
2. サイトのアップグレードを自動的に開始することを示し、準備ができたことを確認します。

データベースとサイトのアップグレードが進行します。

データベースとサイトを手動でアップグレードする

1. アップグレードされたDelivery ControllerでSite Managerを起動します。
2. サイトを手動でアップグレードすることを示します。ウィザードはライセンスサーバーの互換性を確認し、確認を求めます。
3. データベースをバックアップしたことを確認します。

   ウィザードは、スクリプトとアップグレード手順のチェックリストを生成して表示します。アップグレード対象の製品バージョン以降、データベースのスキーマが変更されていない場合、そのスクリプトは生成されません。たとえば、ログデータベースのスキーマが変更されない場合、`UpgradeLoggingDatabase.sql` スクリプトは生成されません。
4. 以下のスクリプトを記載されている順序で実行します。

   - `DisableServices.ps1`: サイトマネージャーユーザーは、製品サービスを無効にするために、Controller上でこのPowerShellスクリプトを実行します。
   - `UpgradeSiteDatabase.sql`: データベース管理者は、Siteデータベースを含むサーバー上でこのSQLスクリプトを実行します。
   - `UpgradeMonitorDatabase.sql`: データベース管理者は、Monitorデータベースを含むサーバー上でこのSQLスクリプトを実行します。
   - `UpgradeLoggingDatabase.sql`: データベース管理者は、Configuration Loggingデータベースを含むサーバー上でこのSQLスクリプトを実行します。このデータベースが変更された場合（たとえば、ホットフィックスを適用した後など）にのみ、このスクリプトを実行してください。
   - `EnableServices.ps1`: サイトマネージャーユーザーは、製品サービスを有効にするために、Controller上でこのPowerShellスクリプトを実行します。

   データベースのアップグレードが完了し、製品サービスが有効になると、Site Managerは環境と構成を自動的にテストし、HTMLレポートを生成します。問題が特定された場合は、データ

ベースのバックアップを復元できます。問題を解決した後、データベースを再度アップグレードできます。

5. チェックリストのタスクを完了したら、**アップグレードの完了**をクリックします。

ステップ 9: 残りのDelivery Controllerをアップグレードする

残りのDelivery Controllerをアップグレードします。アップグレードが完了したら、Site Managerを閉じて再度開きます。その後、Site Managerから、Delivery Controllerのサービスをサイトに登録するために追加のサイトアップグレードを実行するよう求められる場合があります。

ステップ 10: VDAをアップグレードする

> **重要:**
>
> VDAをバージョン1912以降にアップグレードする場合は、「VDAを1912以降にアップグレードする」を参照してください。

> VDAを含むマシンで製品インストーラーを実行します。

Machine Creation Services™とマスターイメージを使用してマシンを作成した場合、ホストに移動し、マスターイメージ上のVDAをアップグレードします。利用可能なVDAインストーラーのいずれかを使用できます。

- グラフィックインターフェイスのガイダンスについては、「VDAをインストールする」を参照してください。
- コマンドラインのガイダンスについては、「コマンドラインを使用したインストール」を参照してください。

Citrix Provisioningを使用してマシンを作成した場合は、アップグレードに関するガイダンスについて「Citrix Provisioning製品ドキュメント」を参照してください。

手順 11: マシンカタログとデリバリーグループを更新する

- アップグレードされたVDAを使用するマシンでカタログを更新する。
- アップグレードされたVDAを使用するマシンでカタログをアップグレードする。
- アップグレードされたVDAを使用するマシンでデリバリーグループをアップグレードする。

手順 12: アップグレード後

展開内の他のコンポーネントをアップグレードします。ガイダンスについては、以下の製品ドキュメントを参照してください。

- StoreFront
- AppDNA
- シトリックス アプリケーションレイヤリング
- HDX リアルタイム最適化パック
- プロファイル管理
- Citrix プロビジョニング
- セッションレコーディング
- ワークスペース環境管理

Microsoft SQL Server Express LocalDB ソフトウェアを新しいバージョンに置き換える必要がある場合は、「SQL Server Express LocalDB の置き換え」を参照してください。(#replace-sql-server-express-localdb).

Dbschemaのアップグレード

展開を更新すると、複数のデータベーススキーマをアップグレードできます。次の表に、そのプロセスでアップグレードされるデータベーススキーマを示します。

From\To	1912 CU1	1912 CU2	1912 CU3	1912 CU4	1912 CU5	2203
7.15 RTM or 7.15 CU releases	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 RTM	Config	Site, Config	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU1		Site	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU2			Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU3				Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU4					Site, Config	Site; Monitor; Config; Logging
1912 CU5						Site; Monitor; Config; Logging
2112						Site; Monitor; Config

用語の定義:

- サイト: サイトデータストア。Dbschemaの更新はサイトデータストアに対して行われます。
- モニター: モニターデータストア。Dbschemaの更新はモニターデータストアに対して行われます。
- Config: 構成テーブル。Studioのバージョン、ライセンス情報、またはその両方が構成テーブルで更新されます。
- ロギング: ロギングデータストア。Dbschemaの更新はロギングデータストアに対して行われます。

VDAを2203以降にアップグレードする

Personal vDisk (PvD) コンポーネントが VDA にインストールされていた場合、その VDA はバージョン 2203 以降にアップグレードできません。新しい VDA を使用するには、現在の VDA をアンインストールしてから、新しい VDA をインストールする必要があります。

この指示は、PvD を使用したことがない場合でも適用されます。

以前のバージョンで PvD コンポーネントがインストールされた可能性がある方法は次のとおりです。

- VDA インストーラーのグラフィカルインターフェイスで、PvD は **追加コンポーネント** ページでオプションでした。
- コマンドラインでは、`/baseimage` オプションによってPvDがインストールされました。このオプションを指定した場合、またはこのオプションを含むスクリプトを使用した場合、PvDがインストールされました。

VDAにPvDがインストールされているかどうかわからない場合は、マシンまたはイメージ上で新しいVDA（2203以降）のインストーラーを実行してください。

- PvDがインストールされている場合、互換性のないコンポーネントがあることを示すメッセージが表示されます。
  - グラフィカルインターフェイスから、メッセージを含むページで**キャンセル**をクリックし、インストーラーを閉じたいことを確認します。
  - CLIからは、コマンドは表示されたメッセージとともに単に失敗します。
- PvDがインストールされていない場合、アップグレードが続行されます。

対処法

VDAにPvDがインストールされていない場合は、通常のアップグレード手順に従ってください。

VDAにPvDがインストールされている場合：

1. 現在のVDAをアンインストールします。
2. 新しいVDAをインストールします。

Windows 10 (1607以前、更新なし) マシンでPvDを継続して使用する場合は、VDA 7.15 LTSRが最新のサポート対象バージョンです。

> **注:**

> *XenAppおよびXenDesktop 7.15 LTSRでWindows 7デスクトップとPersonal vDiskを使用できますか？*

> Citrixは、2016年1月に発表されたXenAppおよびXenDesktop 7.6 LTSRからPersonal vDisk (PvD) を除外しました。さらに、CitrixはPvDテクノロジーの非推奨を発表し、今後Citrix App Layeringの使用を開始するよう顧客に推奨しています。Citrix App Layering（バージョン4.4以降）は、XenAppおよびXenDesktop 7.15 LTSRの互換性のあるコンポーネントです。しかし、Windows 7上の既存のPvD展開を持つ顧客がCitrix App Layeringテクノロジーに移行するのを支援するため、CitrixはXenAppおよびXenDesktop 7.15 LTSR累積更新プログラム（CU）を通じて、Windows 7デスクトップ用のPvD展開に対する期間限定のサポートをJan 14, 2020まで提供することを決定しました。PvDコンポーネントは、Jan 14, 2020以降、LTSR CUから削除され、サポートされなくなります。また、Jan 14, 2020以降にWindows 7でPvDを使用すると、LTSRサイトは非準拠となります。さらに、Windows 10用のPvDは7.15 LTSRから引き続き除外されています。したがって、顧客は7.15 LTSRサイトでこれを使用しないでください。

PvD、AppDisks、およびサポートされていないホストを削除する

Citrix Virtual Apps and Desktops 7 Current Release展開では、以下のテクノロジーとホストタイプはサポートされていません。

- カタログ内のユーザーのVMの隣にデータを保存するための**Personal vDisks (PvD)**。ユーザーパーソナライゼーションレイヤー機能がユーザーの永続性を処理するようになりました。
- デリバリーグループで使用されるアプリケーションを管理するための**AppDisks**。
- **ホストタイプ:** Azure Classic、CloudPlatform (元のCitrix製品)。
    - このリリースでサポートされているホストタイプについては、システム要件を参照してください。

現在の展開でPvDまたはAppDisksを使用している場合、あるいはサポートされていないホストタイプ (例: Microsoft Azure Classic) への接続がある場合、それらのテクノロジーを使用する項目を削除した後にのみ、バージョン2006 (またはそれ以降のサポートされているバージョン) にアップグレードできます。現在の展開でパブリッククラウドホスト接続 (例: AWS) を使用している場合は、アップグレードする前にハイブリッドライツライセンスがあることを確認してください。インストーラーがサポートされていないテクノロジーまたはハイブリッドライツライセンスのないホスト接続を1つ以上検出すると、アップグレードは一時停止または停止し、説明メッセージが表示されます。インストーラーログには詳細が含まれています。

アップグレードを確実に成功させるために、サポートされていない項目を削除するための該当するガイダンスを確認し、それに従ってください。

- PvDを削除
- AppDisk を削除する
- サポートされていないホスト項目を削除する

展開でPvDまたはAppDisksを使用していなかったとしても、関連するMSIが以前のVDAインストールまたはアップグレードに含まれていた可能性があります。VDAをバージョン2006（またはそれ以降のサポートされているバージョン）にアップグレードする前に、たとえ一度も使用していなくても、そのソフトウェアを削除する必要があります。グラフィカルインターフェイスを使用する場合、その削除は自動的に行われるか、CLIを使用する際に削除オプションを含めることができます。詳細については、PvDまたはAppDisksコンポーネントを持つVDAのアップグレードを参照してください。

PvDを削除する

PvDを使用するように構成されているすべてのマシンを削除するまで、展開のアップグレードは成功しません。これはカタログとデリバリーグループに影響します。

グループとカタログからPvDを削除するには：

1. Studioから、PvDを使用するカタログのマシンを含むデリバリーグループがある場合、(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/delivery-groups-manage.html#remove-a-machine-from-a-delivery-group)そのマシンをグループから削除します。
2. Studioから、PvDを使用するマシンを含む(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/machine-catalogs-manage.html#delete-a-catalog)すべてのカタログを削除します。

VDAのアップグレード: 展開のアップグレードでは、VDAにAppDiskまたはPvDコンポーネントがインストールされているかどうかは検出されません。ただし、VDAインストーラーは検出します。詳細については、(#vdas-that-have-pvd-or-appdisks-components)を参照してください。

PvDの代わりにApp Layeringを使用する予定がある場合は、データの移行に関する情報については(/ja-jp/citrix-virtual-apps-desktops/2511/1912-ltsr/install-configure/personal-vdisk/migrate-to-app-layering.html)を参照してください。

AppDiskを削除する

展開のアップグレードは、AppDiskを使用するすべてのデリバリーグループからAppDiskを削除し、その後AppDisk自体を削除するまで続行できません。

1. Studioナビゲーションペインで**デリバリーグループ**を選択します。

2. グループを選択し、アクションペインで**AppDiskの管理**をクリックします。
3. グループからAppDiskを削除するアクションをクリックします。
4. AppDiskを使用する各デリバリーグループに対して、手順2と3を繰り返します。
5. Studioナビゲーションペインで**AppDisk**を選択します。
6. AppDiskを選択し、AppDiskを削除するアクションをクリックします。
7. 各AppDiskについて、手順5と6を繰り返します。

VDAのアップグレード: 展開のアップグレードでは、VDAにAppDiskまたはPvDコンポーネントがインストールされているかどうかは検出されません。ただし、VDAインストーラーは検出します。詳細については、(#vdas-that-have-pvd-or-appdisks-components)を参照してください。

サポートされていないホストアイテムを削除する

サイトがCitrix CloudPlatformやMicrosoft Azure Classicなどのサポートされていないホストタイプに接続している場合、バージョン2006（またはそれ以降のサポートされているバージョン）への展開のアップグレードは続行できません。アップグレードを試みる前に、以下のタスクを完了してください。

Studioから：

- サポートされていないホストへのすべての接続を削除します。
- デリバリーグループに、サポートされていないホストのマスターイメージで作成されたカタログからのマシンが含まれている場合、それらのマシンをグループから削除します。
- サポートされていないホストのマスターイメージを使用して作成されたすべてのカタログを削除します。

PvDまたはAppDisksコンポーネントがインストールされているVDA

PvDおよびAppDisksテクノロジーを有効にするコンポーネントがVDAにインストールされている場合、それらのコンポーネントが削除されるまで、そのVDAはアップグレードできません。

> **注：**
>
> バージョン1912にアップグレードする場合、現在のVDAをアンインストールしてから新しいVDAをインストールする必要がありました。このバージョンでは、Citrixがコンポーネントを削除してアップグレードを続行するかどうかを尋ねられます。

> AppDiskおよびPvDコンポーネントは、それらのテクノロジーを一度も使用していなくても、以前のVDAバージョンでインストールされている可能性があります。

- グラフィカルインターフェイス：VDAインストーラーの**追加コンポーネント**ページには、**Citrix AppDisk / Personal vDisk**オプションが含まれていました。7.15 LTSRおよびそれ以前の7.xリリースでは、このオプションがデフォルトで有効になっていました。したがって、デフォルトを受け入れた場合（または、提供されたリリースでこのオプションを明示的に有効にした場合）、そのコンポーネントがインストールされていました。
- CLI：`/baseimage`オプションを指定すると、コンポーネントがインストールされました。

対処法

VDAインストーラーが現在インストールされているVDAでAppDisksまたはPvDコンポーネントを検出しない場合、アップグレードは通常どおり続行されます。

インストーラーが現在インストールされているVDAでAppDisksまたはPvDコンポーネントを検出した場合：

- グラフィカルインターフェイス: アップグレードが一時停止します。サポートされていないコンポーネントを自動的に削除するかどうかを尋ねるメッセージが表示されます。**OK** をクリックすると、コンポーネントは自動的に削除され、アップグレードが続行されます。
- CLI: コマンドの失敗を避けるため、コマンドに次のオプションを含めます。
  - `/remove_appdisk_ack`
  - `/remove_pvd_ack`

制限事項

アップグレードには次の制限が適用されます。

- **コンポーネントの選択的インストール:** 新しいバージョンにコンポーネントをインストールまたはアップグレードしても、アップグレードが必要な他のコンポーネント（別のマシン上）をアップグレードしないことを選択した場合、Studio が通知します。たとえば、アップグレードに Controller と Studio の新しいバージョンが含まれているとします。Controller はアップグレードしたが、Studio がインストールされているマシンでインストーラーを実行しなかった場合、Studio をアップグレードするまで、Studio はサイトの管理を続行できません。

  VDA をアップグレードする必要はありませんが、利用可能なすべての機能を使用できるように、すべての VDA をアップグレードすることをお勧めします。
- **早期リリースまたはテクノロジプレビューバージョン:** 早期リリース、テクノロジプレビュー、またはプレビューバージョンからアップグレードすることはできません。

- **以前のオペレーティングシステム上のコンポーネント:** Microsoft または Citrix がサポートしなくなったオペレーティングシステムに現在の VDA をインストールすることはできません。詳しくは、「」(#earlier-operating-systems)を参照してください。
- **混在環境/サイト:** 以前のバージョンのサイトと現在のバージョンのサイトを継続して実行する必要がある場合は、「」(#mixed-environment-considerations)を参照してください。
- **製品の選択:** 以前のバージョンからアップグレードする場合、インストール時に設定された製品（Citrix Virtual Apps または Citrix Virtual Apps and Desktops）を選択または指定することはありません。

混在環境に関する考慮事項

アップグレードする際は、エディションとバージョンで利用可能なすべての新機能と強化された機能にアクセスできるように、すべてのコンポーネントと VDA をアップグレードすることをお勧めします。

たとえば、以前の Controller バージョンを含む展開で現在の VDA を使用することはできますが、現在のリリースで追加された新機能は利用できない場合があります。最新ではないバージョンを使用している場合、VDA 登録の問題が発生することもあります。

一部の環境では、すべてのVDAを最新バージョンにアップグレードできない場合があります。その場合、マシンカタログを作成する際に、マシンにインストールされているVDAバージョンを指定できます。(これは機能レベルと呼ばれます。)デフォルトでは、この設定は推奨される最小VDAバージョンを指定します。ほとんどの展開では、デフォルト値で十分です。カタログにデフォルトよりも古いVDAが含まれている場合にのみ、設定を以前のバージョンに変更することを検討してください。マシンカタログ内でVDAバージョンを混在させることは推奨されません。

カタログがデフォルトの最小VDAバージョン設定で作成され、1台以上のマシンにデフォルトバージョンよりも古いVDAがある場合、それらのマシンはControllerに登録できず、動作しません。

詳細については、VDAバージョンと機能レベルを参照してください。

異なるバージョンを持つ複数のサイト

環境に異なる製品バージョン（たとえば、XenDesktop 7.18サイトとCitrix Virtual Apps and Desktops 1909サイト）のサイトが含まれている場合、CitrixはStoreFrontを使用して異なる製品バージョンからのアプリケーションとデスクトップを集約することを推奨します。詳細については、StoreFrontのドキュメントを参照してください。

混在環境では、各リリースに対応するStudioおよびDirectorのバージョンを引き続き使用しますが、異なるバージョンは別々のマシンにインストールされていることを確認してください。

以前のオペレーティングシステム

サポートされているオペレーティングシステム（OS）バージョンを実行しているマシンに、コンポーネントの以前のバージョンをインストールしたとします。現在、より新しいコンポーネントバージョンを使用したいと考えていますが、そのOSはコンポーネントの現在のバージョンではサポートされていません。

たとえば、Windows Server 2016マシンにサーバーVDAをインストールしたとします。現在、そのVDAを現在のリリースにアップグレードしたいが、アップグレード先の現在のリリースではWindows Server 2016がサポートされていません。

許可されていないオペレーティングシステムにコンポーネントをインストールまたはアップグレードしようとすると、「このオペレーティングシステムにはインストールできません」などのエラーメッセージが表示されます。

これらの考慮事項は、Current ReleaseおよびLong Term Service Releaseバージョンのアップグレードに適用されます。（LTSRバージョンにCUを適用することには影響しません。）

サポートされているOSについては、以下のリンクを参照してください。

- Citrix Virtual Apps and Desktops (現在のリリース):
  - デリバリーコントローラー、スタジオ、ディレクター、VDA、ユニバーサルプリントサーバー
  - フェデレーション認証サービス
  - StoreFront (/ja-jp/storefront.html)、Self-Service Password Reset (/ja-jp/self-service-password-reset.html)、および Session Recording (/ja-jp/session-recording.html) については、現在のリリースのシステム要件の記事を参照してください。
- LTSRについては、お使いのLTSRバージョンとCUのコンポーネントリストを参照してください。（メインのCitrix Virtual Apps and Desktops (/ja-jp/citrix-virtual-apps-desktops/2511.html) 製品ドキュメントページからLTSRバージョンを選択してください。）

無効なオペレーティングシステム

次の表は、現在のリリースでコンポーネントのインストール/アップグレードに無効な以前のオペレーティングシステムを示しています。各OSでサポートされる最新の有効なコンポーネントバージョンと、インストールおよびアップグレードが無効になったコンポーネントバージョンを示しています。

表内のオペレーティングシステムには、サービスパックと更新プログラムが含まれます。

オペレーティングシステム	コンポーネント/機能	最新の有効なバージョン	インストール/アップグレードが不可能になったバージョン
Windows 7および Windows 8	VDA	7.15 LTSR	7.16
Windows 7および Windows 8	その他のインストーラーコンポーネント	7.17	7.18
Windows 10 1607 以前のバージョン	VDA	7.15 LTSR	7.16
Windows 10 x86 バージョン	VDA	1906.2.0	1909
Windows サーバー 2008 R2	VDA	7.15 LTSR	7.16
Windows サーバー 2008 R2	その他のインストーラーコンポーネント	7.17	7.18
Windows サーバー 2012	VDA	7.15 LTSR	7.16
Windows サーバー 2012	その他のインストーラーコンポーネント	7.17	7.18
ウィンドウズ サーバー 2012 R2	その他のインストーラーコンポーネント *	1912 LTSR	2003
ウィンドウズ サーバー 2012 R2	サーバー VDI	7.15 LTSR	7.16
Windows サーバー 2016	サーバー VDI	7.15 LTSR	7.16

Windows XP および Windows Vista は、7.x のコンポーネントまたはテクノロジーには無効です。

* Delivery Controller、Studio、Director、およびVDAに適用されます。

実行できること

選択肢があります。次のことができます。

- 現在のOSを継続して使用する(#continue-with-the-current-os)
- マシンの再イメージ化またはアップグレード(#reimage-or-upgrade-the-machine)
- 新しいマシンを追加してから古いマシンを削除する(#add-new-machines-and-then-remove-old-machines)

現在のOSを継続して使用する

これらの方法はVDAで実行可能です。以前のOSを搭載したマシンの使用を継続する場合は、次のいずれかを選択できます。

- インストール済みのコンポーネントバージョンを継続して使用する。
- 最新の有効なコンポーネントバージョンをダウンロードし、そのバージョンにコンポーネントをアップグレードする。（これは、最新の有効なコンポーネントバージョンがまだインストールされていないことを前提としています。）

たとえば、Windows 7 SP1マシンに7.14 VDAがインストールされているとします。Windows 7 OSマシンで有効な最新のVDAバージョンは、XenApp and XenDesktop 7.15 LTSRです。7.14を継続して使用するか、7.15 LTSR VDAをダウンロードしてVDAをそのバージョンにアップグレードすることができます。これらの以前のVDAバージョンは、より新しいバージョンのDelivery Controllerを含む展開で動作します。たとえば、7.15 LTSR VDAは、Citrix Virtual Apps and Desktops 7 1808 Controllerに接続できます。

マシンの再イメージ化またはアップグレード

これらの方法は、VDAおよびコアコンポーネント（Delivery Controllerなど）がインストールされていないその他のマシンで実行可能です。次のいずれかを選択してください。

- マシンをサービスから外し（メンテナンスモードをオンにしてすべてのセッションを閉じさせ）、サポートされているWindows OSバージョンに再イメージ化し、その後、コンポーネントの最新バージョンをインストールできます。
- VDAマシンで再イメージ化せずにOSをアップグレードするには、まずアップグレード先のOSでサポートされているVDAバージョンをインストールするか、OSのアップグレード後にVDAをアップグレードする必要があります。そうしないと、Citrixソフトウェアはサポートされなくなります。VDAをアンインストールせずにインプレースアップグレードを実行する場合、以下の最小OSバージョンにアップグレードできます。
    - Windows 11（2023-07 Cumulative Update for Windows 11 (KB5028185)以降がインストールされているもの、ビルド22621.1992以降）。

  - Windows 10（2023-07 Dynamic Update for Windows 10 (KB5028311)がインストールされているもの）。

- アップグレードを計画しているWindowsバージョンが上記のガイドラインに合致しない場合、OSをアップグレードする前にVDAをアンインストールし、OSアップグレード完了後にサポートされているVDAバージョンをインストールする必要があります。

新しいマシンを追加し、古いマシンを削除する

この方法は、Delivery Controller™またはその他のコアコンポーネントを含むマシンでOSをアップグレードする必要がある場合に実行可能です。

Citrixは、サイト内のすべてのControllerが同じOSを持つことを推奨しています。以下のアップグレードシーケンスは、異なるControllerが異なるOSを持つ期間を最小限に抑えます。

1. サイト内のすべての Delivery Controller のスナップショットを取得し、サイトデータベースをバックアップします。
2. サポートされているオペレーティングシステムを搭載したクリーンなサーバーに新しいDelivery Controllerをインストールします。
3. 新しいコントローラーをサイトに追加します。
4. 現在のリリースで無効なオペレーティングシステムで実行されているControllerを削除します。Controllerの削除に関する推奨事項については、「(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/delivery-controllers.html) 」を参照してください。

準備

アップグレードを開始する前に、以下の情報を確認し、必要なタスクを完了してください。

> **注:**
>
> VDAのアップグレードはアップグレードシーケンスの後半で行われますが、アップグレードを開始する前にインストーラーを選択し、手順を確認して、何が予想されるかを知っておくことをお勧めします。

インストーラーとインターフェイスを選択する

コンポーネントをアップグレードするには、製品ISOのフルプロダクトインストーラーを使用します。VDAは、フルプロダクトインストーラーまたはスタンドアロンVDAインストーラーのいずれ

かを使用してアップグレードできます。すべてのインストーラーは、グラフィカルインターフェイスとコマンドラインインターフェイスを提供します。

詳細については、インストーラー を参照してください。

インストールの詳細: 準備作業を完了し、インストーラーを起動する準備ができたら、インストール記事には、表示される内容 (グラフィカルインターフェイスを使用している場合) または入力する内容 (コマンドラインインターフェイスを使用している場合) が示されています。

- グラフィカルインターフェイスを使用してコアコンポーネントをインストール/アップグレードする
- コマンドラインを使用してコアコンポーネントをインストール/アップグレードする
- グラフィカルインターフェイスを使用してVDAをインストール/アップグレードする
- コマンドラインを使用してVDAをインストール/アップグレードする

シングルセッションOSの場合、4種類のインストーラーが利用可能です。Citrixでは、インストール、アップグレード、アンインストールを含むCitrix VDAのライフサイクル全体で、一貫したインストーラータイプを使用することを推奨しています。詳細については、「シングルセッションVDAインストーラーを使用するためのベストプラクティス」を参照してください。

VDAを現在のリリースにアップグレードすると、アップグレードプロセス中にマシンの再起動が発生します。(この要件は7.17リリースから始まりました。)これは回避できません。再起動後、アップグレードは自動的に再開されます（コマンドラインで`/noresume`を指定しない限り）。

データベースアクション

サイト、監視、および構成ログデータベースをバックアップします。「CTX135207」の手順に従ってください。アップグレード後に問題が発見された場合、バックアップを復元できます。

サポートされなくなったSQL Serverバージョンのアップグレードについては、「SQL Serverバージョンチェック」を参照してください。(これは、サイト、モニター、および構成ログデータベースに使用されるSQL Serverを指します。)

Microsoft SQL Server Express LocalDBは、ローカルホストキャッシュで使用するために自動的にインストールされます。以前のバージョンを置き換える必要がある場合、新しいバージョンはSQL Server Express LocalDB 2019である必要があります。コンポーネントとサイトをアップグレードした後にSQL Server Express LocalDBを新しいバージョンに置き換える方法の詳細については、「SQL Server Express LocalDBを置き換える」を参照してください。

Citrixライセンスが最新であることを確認する

Citrixライセンスの管理に関する包括的な情報については、「Citrixライセンスのアクティブ化、アップグレード、および管理」を参照してください。

フルプロダクトインストーラーを使用してライセンスサーバーをアップグレードできます。または、ライセンスコンポーネントを個別にダウンロードしてアップグレードすることもできます。「アップグレード」を参照してください。

アップグレードする前に、Customer Success Services / Software Maintenance / Subscription Advantageの有効期限が新しい製品バージョンに対応していることを確認してください。日付は2021.11.15以降である必要があります。

Citrixライセンスサーバーの互換性を確認する

Citrixライセンスサーバーが新しいバージョンと互換性があることを確認してください。これには2つの方法があります。

- 他のCitrixコンポーネントをアップグレードする前に、Delivery Controllerを含むマシンでISOレイアウトから`XenDesktopServerSetup.exe`インストーラーを実行します。互換性の問題がある場合、インストーラーは推奨される解決手順とともにそれを報告します。
- インストールメディアの`XenDesktop Setup`ディレクトリから、コマンド`.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`を実行します。表示でライセンスサーバーが互換性があるかどうかが示されます。ライセンスサーバーに互換性がない場合は、ライセンスサーバーをアップグレードしてください。

StoreFrontの変更をバックアップする

アップグレードを開始する前に、`C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`内のファイルを変更している場合（たとえば、*default.ica*や*usernamepassword.tfrm*など）、各ストアについてそれらをバックアップしてください。アップグレード後、それらを復元して変更を元に戻すことができます。

アプリケーションとコンソールを閉じる

アップグレードを開始する前に、管理コンソールやPowerShellセッションなど、ファイルロックを引き起こす可能性のあるすべてのプログラムを閉じます。

マシンを再起動すると、ファイルロックがすべて解除され、保留中のWindowsアップデートがないことが保証されます。

アップグレードを開始する前に、サードパーティの監視エージェントサービスをすべて停止して無効にします。

適切な権限があることを確認する

ドメインユーザーであることに加えて、製品コンポーネントをアップグレードするマシンではローカル管理者である必要があります。

サイトデータベースとサイトは、自動または手動でアップグレードできます。データベースの自動アップグレードの場合、Studioユーザーの権限には、SQL Serverデータベーススキーマを更新する機能（たとえば、`db_securityadmin`または`db_owner`データベースロール）が含まれている必要があります。詳細については、「データベース」を参照してください。

Studioユーザーがこれらの権限を持っていない場合、手動データベースアップグレードを開始すると、スクリプトが生成されます。Studioユーザーは、Studioから一部のスクリプトを実行します。データベース管理者は、SQL Server Management Studioなどのツールを使用して、他のスクリプトを実行します。

その他の準備タスク

- 必要に応じて、テンプレートをバックアップし、ハイパーバイザーをアップグレードします
- 事業継続計画で定められているその他の準備タスクをすべて完了します。

サイトの事前テスト

Delivery Controllerとサイトをアップグレードすると、実際のアップグレードが始まる前に、サイトの事前テストが実行されます。これらのテストでは、以下を確認します。

- サイトデータベースにアクセスでき、バックアップ済みである
- 重要なCitrixサービスへの接続が正しく機能している
- Citrixライセンスサーバーのアドレスが利用可能である
- 構成ログデータベースにアクセスできる
- パブリッククラウドホスト接続（例：AWS）を追加する場合は、ハイブリッド権限ライセンスがあることを確認してください。そうしないと、予備サイトテストが一時停止または停止し、説明メッセージが表示されます。

テストの実行後、結果のレポートを表示できます。検出された問題を修正し、テストを再度実行できます。予備サイトテストを実行せず、問題を解決しないと、サイトの動作に影響を与える可能性があります。

テスト結果を含むレポートは、インストールログと同じディレクトリにあるHTMLファイル（`PreliminarySiteTestResult.html`）です。そのファイルが存在しない場合は作成されます。ファイルが存在する場合は、その内容が上書きされます。

テストを実行する

- インストーラーのグラフィカルインターフェイスを使用してアップグレードする場合、ウィザードにはテストを開始してレポートを表示できるページが含まれています。テストが実行され、レポートを確認し、見つかった問題を解決した後、テストを再実行できます。テストが正常に完了したら、 をクリックしてウィザードを続行します。
- コマンドラインインターフェイスを使用してアップグレードする場合、テストは自動的に実行されます。デフォルトでは、テストが失敗した場合、アップグレードは実行されません。レポートを確認し、問題を解決した後、コマンドを再実行してください。

Citrixは、Controllerとサイトのアップグレードを続行する前に、常に予備サイトテストを実行し、すべての問題を解決することを推奨します。テストを実行するわずかな時間で得られる潜在的なメリットは十分にあります。ただし、この推奨されるアクションを上書きすることもできます。

- グラフィカルインターフェイスでアップグレードする場合、テストをスキップしてアップグレードを続行することを選択できます。
- コマンドラインからアップグレードする場合、テストをスキップすることはできません。デフォルトでは、サイトテストが失敗すると、アップグレードを実行せずにインストーラーが失敗します。通常、`/ignore_site_test_failure` オプションを含めると、テストの失敗は無視され、アップグレードが続行されます。(例外については、SQL Server のバージョンチェック を参照してください。)

複数のControllerをアップグレードする場合

1つのControllerでアップグレードを開始し、その後、同じサイト内の別のControllerでアップグレードを開始した場合（最初のアップグレードが完了する前）：

- 最初のControllerで予備サイトテストが完了した場合、他のControllerのウィザードには予備サイトテストページは表示されません。
- 他のControllerでアップグレードを開始したときに、最初のControllerでのテストが進行中の場合、他のControllerのウィザードにサイトテストページが表示されます。ただし、最初のControllerでのテストが完了すると、最初のControllerからのテスト結果のみが保持されます。

サイトの健全性に関連しないテストの失敗

- メモリ不足が原因で予備サイトテストが失敗した場合は、より多くのメモリを確保してからテストを再実行してください。
- アップグレードの権限はあるが、サイトテストを実行する権限がない場合、予備サイトテストは失敗します。これを解決するには、テストを実行する権限を持つユーザーアカウントでインストーラーを再実行してください。

SQL Serverバージョンの確認

Citrix Virtual Apps and Desktopsの展開を成功させるには、サイト、モニター、および構成ログデータベースにサポートされているバージョンのMicrosoft SQL Serverが必要です。サポートされなくなったSQL ServerバージョンでCitrix展開をアップグレードすると、機能上の問題が発生し、サイトはサポート対象外となります。

アップグレード先のCitrixリリースでサポートされているSQL Serverのバージョンについては、そのリリースのシステム要件の記事を参照してください。

Controllerをアップグレードする際、Citrixインストーラーは、サイト、モニター、および構成ログデータベースに使用されている現在インストールされているSQL Serverのバージョンを確認します。

- チェックの結果、現在インストールされているSQL Serverのバージョンが、アップグレード先のCitrixリリースでサポートされているバージョンではないと判断された場合：
  - グラフィカルインターフェイス：アップグレードはメッセージとともに停止します。「**了解**」をクリックし、次に「**キャンセル**」をクリックしてCitrixインストーラーを閉じます。（アップグレードを続行することはできません。）
  - コマンドラインインターフェイス：コマンドは失敗します（コマンドに`/ignore_db_check_failure`オプションを含めた場合でも）。

  SQL Serverのバージョンをアップグレードしてから、Citrixのアップグレードを再度開始してください。
- チェックで現在インストールされているSQL Serverのバージョンを特定できない場合は、現在インストールされているバージョンがアップグレード先のバージョンでサポートされているかどうかを確認してください（システム要件）。
  - グラフィカルインターフェイス: アップグレードがメッセージとともに停止します。
    - 現在インストールされているSQL Serverのバージョンがサポートされている場合は、**I understand**をクリックしてメッセージを閉じ、**Next**をクリックしてCitrixのアップグレードを続行します。
    - 現在インストールされているSQL Serverのバージョンがサポートされていない場合は、**I understand**をクリックしてメッセージを閉じ、**Cancel**をクリックしてCitrixのアップグレードを終了します。SQL Serverをサポートされているバージョンにアップグレードしてから、Citrixのアップグレードを再度開始してください。
  - コマンドラインインターフェイス：コマンドはメッセージとともに失敗します。メッセージを閉じた後：

- 現在インストールされているSQL Serverのバージョンがサポートされている場合は、`/ignore_db_check_failure`オプションを指定してコマンドを再度実行します。
- 現在インストールされているSQL Serverのバージョンがサポートされていない場合は、SQL Serverをサポートされているバージョンにアップグレードします。コマンドを再度実行してCitrixのアップグレードを開始します。

SQL Serverのアップグレード

新しいSQL Serverサーバーを起動してサイトデータベースを移行する場合、接続文字列を更新する必要があります。

サイトが現在、サイトデータベースにSQL Server Expressを使用している場合（Citrixがサイト作成時に自動的にインストールしたもの）：

1. 最新のSQL Server Expressバージョンをインストールします。
2. データベースをデタッチします。
3. データベースを新しいSQL Server Expressにアタッチします。
4. 接続文字列を移行します。

詳しくは、「接続文字列の構成」およびMicrosoft SQL Serverの製品ドキュメントを参照してください。

SQL Server Express LocalDBの置き換え

Microsoft SQL Server Express LocalDBは、Local Host Cacheがスタンドアロンで使用するSQL Server Expressの機能です。Local Host Cacheは、SQL Server Express LocalDB以外のSQL Server Expressのコンポーネントを必要としません。

Delivery Controller を Citrix Virtual Apps and Desktops バージョン 2203 LTSR 以降のバージョンにアップグレードする場合、サポートされるバージョンは SQL Server Express LocalDB 2019 または SQL Server Express LocalDB 2022 です。

SQL Server Express LocalDB を更新する方法は2つあります。

- 自動更新
- 手動更新

自動更新

Delivery Controller をアップグレードすると、メタインストーラーは互換性のある最新バージョンの SQL Server Express LocalDB を自動的にインストールします。メタインストーラーは古い

LocalDB バージョンをアンインストールしません。新しいバージョンが正しく動作することを確認した後、古いバージョンを手動でアンインストールする必要があります。

新しい SQL Server Express LocalDB のインストールを確認する

古いバージョンをアンインストールする前に、新しい SQL Server Express LocalDB のインストールが正しく動作していることを確認してください。

1. コマンドプロンプトを使用して SqlLocalDB インスタンスに移動します。
    - SQL LocalDB 2014 の場合: `cd C:\Program Files\Microsoft SQL Server\120\Tools\Binn`
    - SQL LocalDB 2017 の場合: `cd C:\Program Files\Microsoft SQL Server\140\Tools\Binn`
    - SQL LocalDB 2019 の場合: `cd C:\Program Files\Microsoft SQL Server\150\Tools\Binn`
    - SQL LocalDB 2022 の場合: `cd C:\Program Files\Microsoft SQL Server\160\Tools\Binn`
2. `SqlLocalDB i` を実行します。

    CitrixHA と MSSQLLocalDB の2つのファイルが表示されるはずです。

手動更新

前提条件

- Citrix Virtual Apps and Desktopsのインストールメディア。
- Windows SysinternalsツールボックスのPsExecツール。

手順

1. Citrix Virtual Apps and Desktops のコンポーネント、データベース、およびサイトのアップグレードを完了します。(これらのデータベースアップグレードは、サイト、監視、および構成ログデータベースに影響します。SQL Server Express LocalDB を使用するローカルホストキャッシュデータベースには影響しません。)
2. SQL Server Express LocalDB を更新する Delivery Controller にログオンします。
3. Microsoft から PsExec をダウンロードし、その Delivery Controller 上のアクセスしやすい場所 (例: C:\Temp) に配置します。
4. Windows システムサービスから、Delivery Controller 上の Citrix High Availability Service を停止します。

5. Delivery Controller でコマンドプロンプトを開き、PsExec がある場所 (例: `C:\Temp`) に移動し、Network Service アカウントでコマンドプロンプトを昇格させるために、次のコマンドを実行します。

```
psexec -i -u "NT AUTHORITY\NETWORKSERVICE" cmd
```

6. コマンドプロンプトが Network Service アカウントとして実行されていることを確認するために、`whoami` を実行します。次の出力が得られるはずです: `nt authority\networkservice`。
7. コマンドプロンプトを使用して、SQL LocalDB インスタンスに移動します。
   - SQL LocalDB 2014からアップグレードする場合:

```
cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
```

   - SQL LocalDB 2017からアップグレードする場合:

```
cd "C:\Program Files\Microsoft SQL Server\140\Tools\Binn"
```

   - SQL LocalDB 2019からアップグレードする場合:

```
cd "C:\Program Files\Microsoft SQL Server\150\Tools\Binn"
```

8. SQL LocalDBインスタンスを停止して削除します: `CitrixHA`。

```
SqlLocalDB stop CitrixHA



SqlLocalDB delete CitrixHA
```

9. Delivery Controllerから以下のファイルを削除します:

```
C:\Windows\ServiceProfiles\NetworkService\HADatabaseName.*

C:\Windows\ServiceProfiles\NetworkService\HADatabaseName_log.*

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName.* (if
```

```
exists)

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName_log.*
(if exists)
```

10. プログラムを削除するためのネイティブなWindows機能を使用して、Delivery Controllerから既存のSQL LocalDB SQL Server Expressをアンインストールします。
11. アンインストールが完了したら、Delivery Controllerを再起動します。
12. WindowsシステムサービスからDelivery Controller上のCitrix High Availability Serviceを停止します。
13. Citrix Virtual Apps and Desktopsインストールメディアを Delivery Controllerにマウントします。
14. Delivery ControllerにSQL Server Express LocalDB 2022を管理者としてインストールします。
    a. Citrix Virtual Apps and Desktopsインストールメディアの `Support > SQLLocalDB` フォルダーにある `sqllocaldb.msi` ファイルを使用します。たとえば、インストールメディアが `E drive` ドライブ文字にマウントされている場合、ファイルは `E:\Support\SQLLocalDB\sqllocaldb.msi` にあります。インストールを完了するには再起動が必要です。
    b. 新しいSQL LocalDBは `C:\Program Files\Microsoft SQL Server\160\Tools\Binn` にある必要があります。
15. WindowsシステムサービスからDelivery Controller上のCitrix High Availability Serviceを開始します。
16. Delivery Controllerのコマンドプロンプトで、 `C:\Program Files\Microsoft SQL Server\160\Tools\Binn` に移動し、 `SqlLocalDB i` を実行してCitrixHAインスタンスが作成されたことを確認します。返されたインスタンスのリストに `CitrixHA` が含まれている必要があります。

> **注:**
>
> Citrix High Availability Serviceの開始後、CitrixHAデータベースが作成されるまでに最大15分かかる場合があります。

17. 必要に応じてHigh Availability Service（セカンダリブローカー）が引き継ぐことができることを確認するために、ローカルホストキャッシュデータベースファイルが作成されていることを確認します。

    a. Delivery Controllerで、`C:\Windows\ServiceProfiles\NetworkService`を参照します。

    b. `HaDatabaseName.mdf`と`HaDatabaseName_log.ldf`が作成されていることを確認します。

18. 残りのDelivery Controllerで手順を繰り返します。

セキュリティ保護

FIDO2認証

FIDO2およびWebAuthnを使用したローカル認証と仮想認証

ユーザーは、FIDO2 セキュリティキーと、TPM 2.0 および Windows Hello を搭載した統合生体認証デバイスを使用して、仮想セッション内で FIDO2 または WebAuthn を利用するアプリケーションに認証できます。

FIDO2の詳細については、「FIDO2: WebAuthn & CTAP」を参照してください。

この機能の使用方法については、「FIDO2 redirection」を参照してください。

> **注**
>
> この機能は、WebAuthnまたはFIDO2を使用した仮想セッションへのログオンをサポートしていません。この機能は、仮想セッション内のアプリケーションでこれらの認証方法を使用することのみを許可します。

前提条件と構成

サポートマトリックス

セッションホストのオペレーティングシステム	WEBアプリケーション認証	UWPアプリケーション認証
ウィンドウズ サーバー 2016	USBリダイレクト経由でサポート	サポートされていません
ウィンドウズ サーバー 2019	サポートされています	サポートされていません
Windows Server 2022 (ウィンドウズ サーバー 2022)	サポートされています	サポートされています

セッションホストのオペレーティングシステム	WEBアプリケーション認証	UWPアプリケーション認証
Windows Server 2025 (ウィンドウズ サーバー 2025)	サポートされています	サポートされています
ウィンドウズ 10	サポートされています	サポートされています
ウィンドウズ 11	サポートされています	サポートされています

> **注:**
>
> 上記の認証方法のサポートは、基盤となるオペレーティングシステムの機能によって異なります。

詳細については、以下の要件を確認してください。

Webアプリケーション認証

要件

WebアプリケーションでFIDO2およびWebAuthn認証を使用するための要件は次のとおりです。

CITRIX® コントロールプレーン

- シトリックス バーチャル アプリケーションズ アンド デスクトップ™ 2203 以降

セッションホスト

- オペレーティングシステム
  - Windows 10 22H2以降
  - ウィンドウズ 11
  - Windows Server 2019 以降のバージョン
- VDA
  - Windows: バージョン2203以降

クライアントデバイス

- オペレーティングシステム

    - Windows 10 22H2以降
    - ウィンドウズ 11
    - Linux: Workspace app for Linuxのシステム要件を参照してください。
    - Mac: Workspace app for Macのシステム要件を参照してください。
- Workspaceアプリ
    - Windows: バージョン2402以降
    - Linux: 2303以降
    - Mac: 2307以降

WEBブラウザーの要件

- 32ビットおよび64ビットブラウザー

サポートされている認証方法

- FIDO2セキュリティキー
- Windows ハロー
    - TPM 2.0
    - 統合生体認証
        - 顔認証
        - 指紋スキャナー
    - WebAuthn
- パスキー

注:

- 上記の認証方法のサポートは、基盤となるクライアントオペレーティングシステムの機能に依存します。
- パスキーは、Windows 10クライアントデバイスおよび/またはセッションホストではサポートされていません。

UWPアプリケーション認証

Citrix Virtual Apps™ and Desktops 2112 のリリースにより、Citrix は UWP アプリケーションでの WebAuthn および FIDO2 認証をサポートします。

Microsoft Teams、Microsoft Outlook for Office 365、OneDriveなどのアプリケーションは、Microsoft Entra IDへのリンクとして認証にUWPアプリケーションを使用します。Citrixは現在、これらのアプリケーションを認証するためにFIDO2の使用をサポートしています。

要件

UWPアプリケーションでFIDO2およびWebAuthn認証を使用するための要件は次のとおりです。

CITRIXコントロールプレーン

- シトリックス バーチャル アプリケーションズ アンド デスクトップ 2112 以降

セッションホスト

- オペレーティングシステム
  - Windows 10 22H2以降
  - ウィンドウズ 11
  - ウィンドウズ サーバー 2022 以降
- VDA
  - Windows: バージョン2203以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 22H2以降
  - ウィンドウズ 11
  - Linux: Workspace app for Linuxのシステム要件を参照してください。
  - Mac: Workspace app for Macのシステム要件を参照してください。
- Workspaceアプリ
  - Windows: バージョン2402以降
  - Linux: 2303 以降
  - Mac: 2307 以降

UWPアプリケーションの要件

- 32ビットおよび64ビットアプリケーション

サポートされる認証方法

- FIDO2セキュリティキー
- Windows ハロー
  - TPM 2.0
  - 統合された生体認証
    - 顔認識
    - 指紋スキャナー
  - WebAuthn
  - パスキー

> **注:**
>
> 上記に挙げた認証方法のサポートは、基盤となるオペレーティングシステムの機能に依存します。

> FIDO2リダイレクトが、クライアント、VDA、またはオペレーティングシステムでサポートされていないために利用できないシナリオでは、USBベースのFIDO2キーをUSBリダイレクトを使用してリダイレクトできます。 FIDO2リダイレクトが利用可能なシナリオでも、USBリダイレクトを使用してUSBベースのFIDO2キーをリダイレクトすることが可能です。この場合、FIDO2リダイレクトを無効にし、適切なUSBリダイレクトルールを構成する必要があります。 USBリダイレクトルールを使用してFIDO2キーを構成する方法の詳細については、USBリダイレクトデバイスルールのドキュメントを参照してください。

構成

FIDO2リダイレクトはデフォルトで有効になっています。Chrome、Edge、Brave、Firefoxブラウザで実行されているアプリケーションに認証するために、追加の構成は必要ありません。

FIDO2認証を必要とするその他のアプリケーションを使用している企業の場合、レジストリに追加の構成が必要です。詳細については、高度な構成を参照してください。

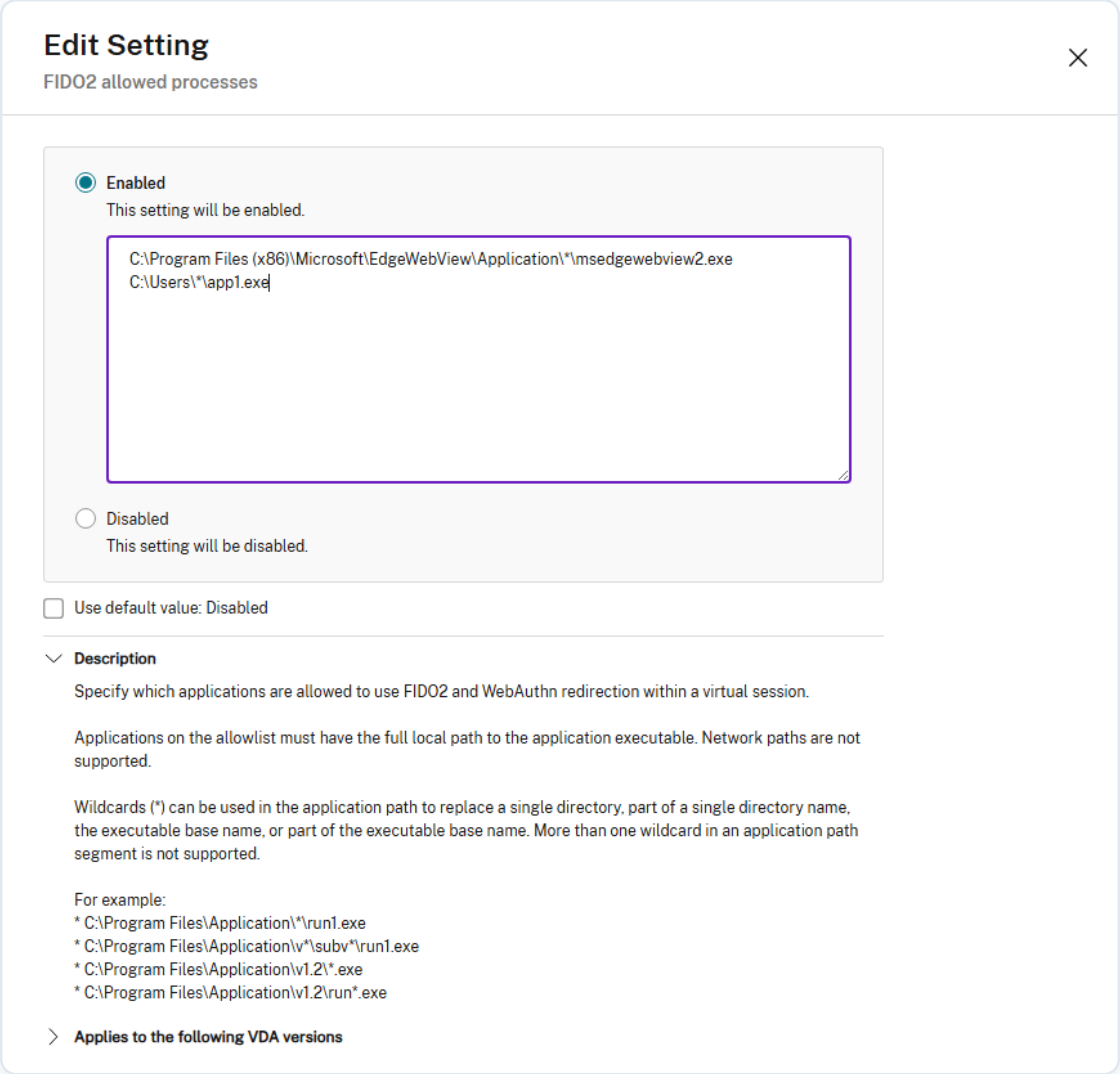
カスタムアプリケーションの高度な構成

Chrome、Edge、Firefox、Brave以外のWebアプリケーションを使用している企業の場合、HDXセッション内でFIDO2リダイレクトが機能するように、以下の変更を行う必要があります。

1. Studioで**FIDO2許可プロセス**ポリシー設定を構成します。

   - テキストフィールドにアプリケーションのフルパスを追加します。ポリシー設定の使用方法に関する追加の詳細は、ポリシーセクションで確認できます。

> **注：**
>
> ワイルドカード (*) の使用がサポートされています。アプリケーションのバージョンに基づいてディレクトリ名や実行可能ファイル名が変更される場合、またはアプリケーションがユーザープロファイルにインストールされている場合にワイルドカードを使用できます。



2. 次のレジストリキーと値を追加します。

   a. 64ビットアプリケーションの場合（例：「app1.exe」）：

      - キー:
        `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\app1.exe`

   b. 32ビットアプリケーションの場合：

      - キー:
        `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHo`

3. app1.exeでFIDO2リダイレクトを有効にするためにレジストリ値を設定した後、VDAを再起動します。

注：

- ステップ2と3は`msedgewebview2.exe`には必要ありません。
- レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような重大な問題が発生する可能性があります。Citrixは、.
- レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。
- レジストリエディターの使用は、ご自身の責任で行ってください。編集する前に、必ずレジストリをバックアップしてください。

トラブルシューティング

FIDO2リダイレクトの問題をトラブルシューティングするには、次の手順に従ってください。

1. **システム要件を確認する**

   a. Citrixの公式ドキュメントに基づいて、FIDO2リダイレクトのシステム要件が満たされていることを確認します。

2. **デバイス接続を確認する**

   a. 物理FIDO2キーの場合:

      i. FIDO2キーが正しく挿入され、クライアントエンドポイントで認識されていることを確認します。

ii. オペレーティングシステムのデバイスマネージャー（例: Windowsのデバイスマネージャー、macOSのシステム情報）を使用して、デバイスが認識され、機能していることを確認します。

iii. デバイスが検出されない場合:

i. キーを挿し直すか、別のUSBポートを使用してみてください。

ii. ハードウェアの問題を除外するために、別のデバイスでキーをテストします。

b. 組み込み認証機能（例: Windows Helloなど）の場合 -

i. クライアントデバイスで機能が有効になり、構成されていることを確認します。

c. クライアントデバイスがFIDO2キーを認識しない場合、CitrixはそれをHDXセッションにリダイレクトできないため、これは重要です。

3. **Citrixポリシー設定と構成を確認する**

a. CitrixポリシーでFIDO2/WebAuthnリダイレクトおよびUSBリダイレクトの設定を確認してください。

i. FIDO2リダイレクトポリシーが有効になっています。

ii. EdgeWebView2またはカスタムデスクトップアプリケーションが使用されている場合、**FIDO2許可プロセス**ポリシー設定に適切なファイルパスが追加されます。

iii. 汎用USBリダイレクトを使用してデバイスをリダイレクトするためのFIDO2キーに対して、デバイスルールが**設定されていません**。

b. Citrixコンポーネントが最近更新された場合、構成が新しいバージョンと一致していることを確認してください。

4. **診断にHDX Monitorを使用する**

a. HDXセッションを起動し、WebブラウザまたはUWPアプリケーションを開いて認証ページに移動します。

b. サインイン方法としてセキュリティキー、Webauthn、またはFIDO2を選択します。FIDO2呼び出しがリダイレクトされた結果として、wfica32.exeプロセスからのダイアログプロンプトが表示されるはずです (添付のスクリーンショットを参照)。そうでない場合：

i. キーが汎用USB仮想チャネルを使用してリダイレクトされていないことを確認してください。キーがHDXセッション内でリダイレクトされている場合、「セキュリティキーをUSBポートに挿入してください」というダイアログプロンプトが表示される可能性

があります。これを解決するには、USBリダイレクトを無効にするか、セキュリティキーがHDXセッション内でリダイレクトされていないことを確認してください。

ii. HDXセッションでHDX Monitorを開き、**FIDO2 - Webauthnリダイレクト**ノードに移動します。

iii. FIDO2リダイレクト許可ポリシーが**True**に設定されており、FIDO2/WebAuthn認証を必要とするアプリケーションが**FIDO2リダイレクトフックアプリケーション**にリストされていることを確認します。アプリケーションが存在しない場合は、高度な構成の情報に基づいて、適切なレジストリの場所に追加してください。

iv. FIDO2/WebAuthn認証を必要とするアプリケーションのフルパスが**FIDO2許可プロセス**ポリシー設定にリストされていることを確認します。フルパスが存在しない場合は、Studioの**FIDO2許可プロセス**ポリシー設定に追加します。詳細については、構成セクションを参照してください。

v. (レガシー) レガシーレジストリベースの設定を使用してFIDO2リダイレクトが構成されている場合、Studioの**FIDO2許可プロセス**ポリシー設定に構成を移行し、FIDO2/WebAuthn認証を必要とするアプリケーションのフルパスが含まれていることを確認してください。詳細については、構成セクションを参照してください。

> **注:**
>
> セッションホストにHDX Monitorがまだインストールされていない場合、Citrix Virtual Apps and Desktopsインストーラーの Supportフォルダーからインストールできます。

1. **ログを収集し、テクニカルサポートに連絡する**

   a. 上記の手順を実行しても問題が解決しない場合 -

      i. HDX Monitor の出力、Citrix Workspace アプリ、および VDA CDF ログを収集します。

      ii. 実行したすべてのトラブルシューティング手順と、発生したエラーメッセージを文書化します。

      iii. IT サポートチームまたは Citrix Support に連絡し、収集した情報を提供して、より迅速な解決を図ります。

Citrix Virtual Apps and Desktops™ を Citrix Gateway と連携させて統合する

StoreFront™ サーバーは、公開されたリソースとデータへのアクセスを管理するために展開および構成されます。リモートアクセスの場合、StoreFront の前に Citrix Gateway を追加することをお勧めします。

> **注:**
>
> Citrix Virtual Apps and Desktops を Citrix Gateway と統合する方法の詳細な構成手順については、StoreFront のドキュメントを参照してください。

次の図は、Citrix Gateway を含む簡素化された Citrix 展開の例を示しています。Citrix Gateway は StoreFront と通信し、Citrix Virtual Apps™ and Desktops によって提供されるアプリとデータを保護します。ユーザーデバイスは Citrix Workspace™ アプリを実行して、セキュアな接続を作成し、アプリ、デスクトップ、ファイルにアクセスします。

Citrix Gateway を含む簡素化された Citrix 展開(/en-us/citrix-virtual-apps-desktops/2511/media/sample-deployment-overview.png)

ユーザーは Citrix Gateway を使用してログオンし、認証します。Citrix Gateway は DMZ に展開され、保護されています。2 要素認証が構成されています。ユーザー資格情報に基づいて、ユーザーには関連するリソースとアプリケーションが提供されます。アプリケーションとデータは適切なサーバー上にあります（図には示されていません）。セキュリティ上機密性の高いアプリケーションとデータには、個別のサーバーが使用されます。

セキュリティに関する考慮事項とベストプラクティス

> **注:**
>
> 組織は、規制要件を満たすために特定のセキュリティ標準に準拠する必要がある場合があります。このようなセキュリティ標準は時間とともに変化するため、このドキュメントではこの主題については扱いません。セキュリティ標準とCitrix製品に関する最新情報については、Citrix Trust Centerを参照してください。

ファイアウォール

環境内のすべてのマシンを、必要に応じてエンクレーブ境界を含め、境界ファイアウォールで保護します。

環境内のすべてのマシンは、パーソナルファイアウォールによって保護されている必要があります。コアコンポーネントとVDAをインストールする際、Windowsファイアウォールサービスが検出された場合（ファイアウォールが有効になっていない場合でも）、コンポーネントと機能の通信に必要なポートを自動的に開くように選択できます。また、これらのファイアウォールポートを手動で構成することもできます。別のファイアウォールを使用する場合は、手動で構成する必要があります。必要なポートの詳細については、「Tech Paper: Communication Ports Used by Citrix Technologies」を参照してください。

従来の環境をこのリリースに移行する場合、既存の境界ファイアウォールの再配置や新しい境界ファイアウォールの追加が必要になることがあります。たとえば、データセンター内の従来のクライアントとデータベースサーバーの間に境界ファイアウォールがあるとします。このリリースを使用する場合、その境界ファイアウォールは、仮想デスクトップとユーザーデバイスが一方にあり、データセンター内のデータベースサーバーとDelivery Controllerがもう一方にあるように配置する必要があります。したがって、データベースサーバーとControllerを格納するために、データセンター内にエンクレーブを作成することを検討してください。また、ユーザーデバイスと仮想デスクトップの間に保護を設けることも検討してください。

> **注:**
>
> TCPポート1494と2598はICAとCGPに使用されるため、データセンター外のユーザーがアクセスできるようにファイアウォールで開かれている可能性が高いです。Citrixは、管理インターフェイスが意図せず攻撃にさらされる可能性を避けるため、これらのポートを他の目的で使用しないことを推奨します。ポート1494と2598は、Internet Assigned Number Authority (http://www.iana.org/) に正式に登録されています。

Delivery Controller™とのセキュアな通信

HTTPSを使用した通信の暗号化

StoreFrontとNetScaler Gatewayは、HTTPまたはHTTPSを介してDelivery Controllerで実行されているXMLサービスと通信します。構成によっては、VDAはWebSocketを使用してDelivery Controllerと通信する場合があります。Directorは、HTTPまたはHTTPSを介してODataを使用して

監視データと通信します。HTTPSを有効にし、HTTPを無効にすることをお勧めします。これには、Delivery ControllerでTLSを有効にする必要があります。

- StoreFrontをHTTPSを使用して接続するように構成するには、(/ja-jp/storefront/current-release/configure-manage-stores/manage-controllers#add-resource-feeds-for-citrix-virtual-apps-and-desktops)および(/ja-jp/storefront/current-release/integrate-with-citrix-gateway-and-citrix-adc/configure-citrix-gateway#add-citrix-gateway-appliance)を参照してください。
- NetScaler GatewayをHTTPSを使用してDelivery Controllerに接続するように構成するには、「NetScaler GatewayでのSecure Ticket Authorityの構成」を参照してください。

セキュリティキー

承認されたStoreFrontサーバーとNetScalerサーバーのみがクラウドコネクタ経由でDaaSに接続できるように、セキュリティキーを使用できます。XML信頼を有効にしている場合は、これが特に重要です。

XML信頼

デフォルトでは、StoreFrontが列挙や起動などのアクションのためにデリバリーコントローラーに接続する場合、DaaSがユーザーを認証し、ユーザーのグループメンバーシップを確認できるように、StoreFrontはユーザーのActive Directory資格情報を渡す必要があります。ただし、ドメインパススルー、スマートカード、SAMLなどの他の認証方法を使用する場合、StoreFrontはActive Directoryパスワードを持っていません。この場合、「XML信頼」を有効にする必要があります。XML信頼が有効になっている場合、Citrix Virtual Apps and Desktopsは、ユーザーのパスワードを検証することなく、アプリケーションの列挙や起動など、ユーザーに代わってStoreFrontがアクションを実行することを許可します。XML信頼を有効にする前に、セキュリティキーまたはファイアウォールやIPsecなどの別のメカニズムを使用して、信頼できるStoreFrontサーバーのみがデリバリーコントローラーに接続できるようにしてください。

XML信頼設定の確認、有効化、または無効化には、Citrix Virtual Apps and Desktops PowerShell SDKを使用します。

- XML信頼設定の現在の値を確認するには、`Get-BrokerSite`を実行し、`TrustRequestsSentToTheXMLServicePort`の値を調べます。
- XML信頼を有効または無効にするには、パラメーター`TrustRequestsSentToTheXmlServicePort`を指定して`Set-BrokerSite`を実行します。

VDAとDelivery Controller間の通信

VDAがコントローラーと通信するためのメカニズムは2つあります。

- ウィンドウズ コミュニケーション ファウンデーション

  Windows Communication Foundation (WCF) のメッセージレベル保護は、Delivery ControllerとVDA間の通信を保護します。これにより、TLSを使用した追加のトランスポートレベル保護の必要がなくなります。VDAとDelivery Controller間の通信に使用されるデフォルトポートは80です。ただし、ポートをカスタマイズできます。詳細については、VDAのカスタマイズを参照してください。

  WCFにおけるメッセージセキュリティの詳細については、MicrosoftのドキュメントWCFにおけるメッセージセキュリティを参照してください。

  WCF構成では、ControllerとVDA間の相互認証にKerberosを使用します。暗号化には256ビットキーのCBCモードでAESを使用します。メッセージの整合性にはSHA-1を使用します。

  Microsoftによると、WCFで使用されるセキュリティプロトコルは、WS-SecurityPolicy 1.2を含むOASIS（Organization for the Advancement of Structured Information Standards）の標準に準拠しています。また、Microsoftは、WCFがSecurity Policy 1.2に記載されているすべてのアルゴリズムスイートをサポートしていると述べています。

  ControllerとVDA間の通信にはbasic256アルゴリズムスイートが使用され、そのアルゴリズムは前述のとおりです。

  WCF構成では、メッセージレベルのセキュリティ暗号化とともに、SOAP over HTTPプロトコルを使用します。

- WebSockets

  これはWCFの最新の代替手段です。VDAからDelivery Controllerへの通信にはTLSポート443のみを使用するという利点があります。現在、MCSでプロビジョニングされたマシンでのみ利用可能です。詳細については、「VDAとDelivery Controller間のWebSocket通信」(/ja-jp/citrix-virtual-apps-desktops/2511/secure/websocket-vda-support)を参照してください。

Delivery ControllerとLicense Server間のセキュアな通信

Delivery ControllerはHTTPS経由でLicense Serverと通信します。デフォルトでは自己署名証明書を使用しますが、これをエンタープライズまたはパブリック認証局が発行した証明書に置き換えることをお勧めします。詳細については、Citrix Licensing ManagerおよびWeb Services for Licensingで使用される証明書の手動インストールを参照してください。

WebブラウザとWeb StudioおよびDirector間の通信を保護する

Web StudioとDirectorは、Delivery Controllerと同じマシン、または別のマシンにインストールできます。ユーザーはWebブラウザを使用してWeb StudioとDirectorに接続します。デフォルトでは、

Web Studioは自己署名証明書を使用してHTTPSを有効にしますが、スタンドアロンでインストールされたDirectorはHTTPSを構成しません。適切な証明書を使用して、Web StudioとDirectorでTLSを有効にすることをお勧めします(/ja-jp/citrix-virtual-apps-desktops/2511/secure/tls-studio)。

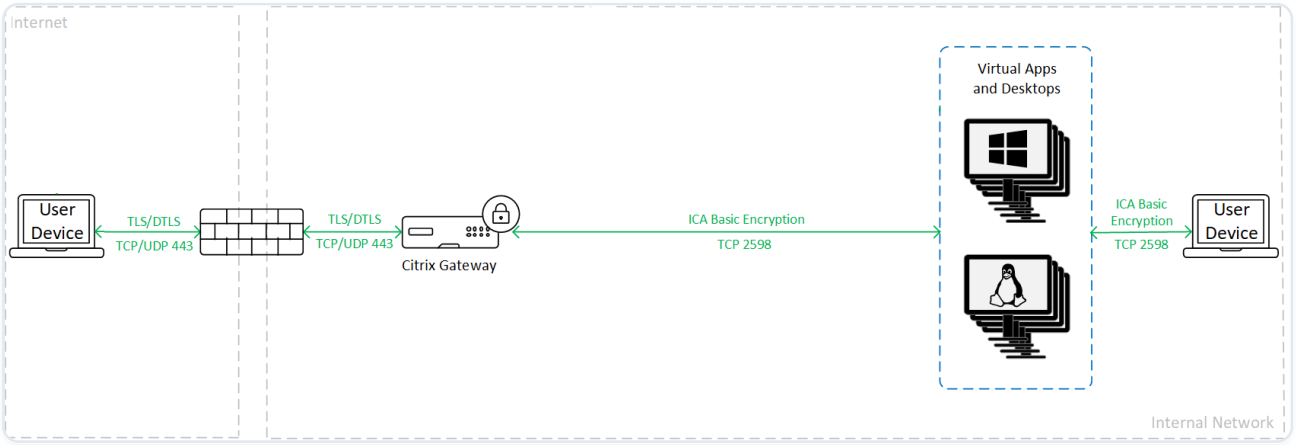
ICA®通信の保護

Citrix Virtual Apps and Desktops™は、クライアントとVDA間のICAトラフィックを保護するためのいくつかのオプションを提供します。利用可能なオプションは次のとおりです。

- **基本暗号化:** デフォルト設定です。
- **SecureICA:** RC5 (128ビット) 暗号化を使用してセッションデータを暗号化できます。
- **VDA TLS/DTLS:** TLS/DTLSを使用したネットワークレベルの暗号化を可能にします。

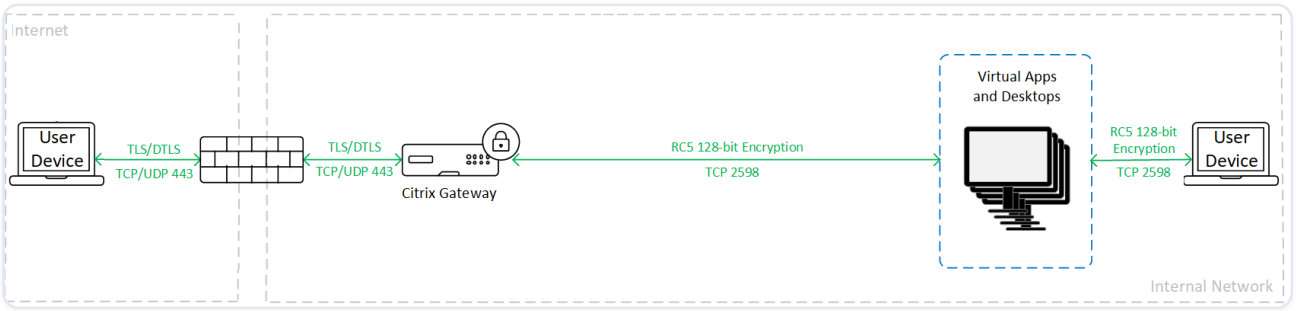
基本暗号化

基本暗号化を使用する場合、トラフィックは次の図に示すように暗号化されます。



SecureICA

SecureICAを使用すると、トラフィックは次の図に示すように暗号化されます。



詳細については、セキュリティポリシー設定を参照してください。

> **注1：**

> SecureICAは、Workspace app for HTML5ではサポートされていません。

> **注2：**

> Citrix SecureICAはICA/HDXプロトコルの一部ですが、Transport Layer Security (TLS) のような標準準拠のネットワークセキュリティプロトコルではありません。

VDA TLS/DTLS

VDA TLS/DTLS暗号化を使用すると、トラフィックは次の図に示すように暗号化されます。

TLS/DTLS使用時のトラフィック暗号化(/en-us/citrix-virtual-apps-desktops/2511/media/vda-tls.png)

VDA TLS/DTLSを構成するには、「VDA上のTLS設定」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2511/secure/tls-vda).

仮想チャネル

環境で許可されるCitrix以外の仮想チャネルを制御するには、「仮想チャネル許可リスト」を使用します。(/ja-jp/citrix-virtual-apps-desktops/2511/secure/virtual-channel-security).

プリントサーバーとのセキュアな通信

Virtual Delivery Agent (VDA) とUniversal Print Server間のTCPベースの接続でTLSを有効にできます。詳細については、「Universal Print Server上のTransport Layer Security (TLS)」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2511/secure/tls-ups).

サイトデータベースとの安全な通信

サイトデータベースへのTLSを有効にする方法については、「CTX137556」を参照してください。

VDAマシンのセキュリティ

一般的な推奨事項

VDAが最新のオペレーティングセキュリティ更新プログラムとウイルス対策ソフトウェアで常に最新の状態に保たれていることを確認してください。

アプリケーションセキュリティ

非管理者ユーザーが悪意のある操作を実行するのを防ぐため、Citrix®は、VDAホスト上のインストーラー、アプリケーション、実行可能ファイル、およびスクリプトに対してWindows AppLockerルールを構成することを推奨します。

8.3形式のファイル名

VDAで8.3形式のファイル名を無効にできます。「Microsoft fsutil documentation」を参照してください。

データストレージに関する考慮事項

デスクトップ環境は、プールされたデスクトップや専用デスクトップなど、さまざまな種類のデスクトップで構成されている場合があります。ユーザーは、プールされたデスクトップなど、ユーザー間で共有されるデスクトップにデータを保存してはなりません。ユーザーが専用デスクトップにデータを保存した場合、そのデスクトップが後で他のユーザーに利用可能になった場合は、そのデータを削除する必要があります。

ユーザーアカウント管理

アカウント管理にはWindowsのベストプラクティスを適用してください。Machine Creation ServicesまたはProvisioning Servicesによって複製される前に、テンプレートまたはイメージ上にアカウントを作成しないでください。保存された特権ドメインアカウントを使用してタスクをスケジュールしないでください。共有Active Directoryマシンアカウントを手動で作成しないでください。これらの慣行は、マシン攻撃がローカルの永続的なアカウントパスワードを取得し、それらを使用して他のユーザーに属するMCS/PVS共有イメージにログオンするのを防ぐのに役立ちます。

ユーザーには、必要な機能のみを付与してください。Microsoft Windowsの特権は、通常の方法でデスクトップに引き続き適用されます。つまり、ユーザー権利の割り当てを通じて特権を構成し、グループポリシーを通じてグループメンバーシップを構成します。このリリースの利点の1つは、デスクトップが保存されているコンピューターに対する物理的な制御を付与することなく、ユーザーにデスクトップへの管理者権限を付与できることです。

デスクトップの特権を計画する際には、次の点に注意してください。

- デフォルトでは、非特権ユーザーがデスクトップに接続すると、自分のユーザーデバイスのタイムゾーンではなく、デスクトップを実行しているシステムのタイムゾーンが表示されます。ユーザーがデスクトップを使用する際にローカルタイムを表示できるようにする方法については、「デリバリーグループの管理」の記事を参照してください。

- デスクトップの管理者であるユーザーは、そのデスクトップを完全に制御できます。デスクトップが専用デスクトップではなくプールされたデスクトップである場合、そのユーザーは、将来のユーザーを含む、そのデスクトップの他のすべてのユーザーに関して信頼できる必要があります。デスクトップのすべてのユーザーは、この状況によってデータセキュリティに永続的なリスクが生じる可能性があることを認識しておく必要があります。この考慮事項は、単一ユーザーのみが使用する専用デスクトップには適用されません。そのユーザーは、他のどのデスクトップの管理者であってもなりません。
- デスクトップの管理者であるユーザーは、一般的に、悪意のあるソフトウェアを含むソフトウェアをそのデスクトップにインストールできます。また、そのユーザーは、デスクトップに接続されているネットワーク上のトラフィックを監視または制御できる可能性もあります。

ログオン権限の管理

ログオン権限は、ユーザーアカウントとコンピューターアカウントの両方に必要です。Microsoft Windowsの特権と同様に、ログオン権限は通常の方法でデスクトップに適用され続けます。ユーザー権利の割り当てを通じてログオン権限を構成し、グループポリシーを通じてグループメンバーシップを構成します。

Windowsのログオン権限は、ローカルログオン、リモートデスクトップサービス経由のログオン、ネットワーク経由のログオン（ネットワークからこのコンピューターにアクセス）、バッチジョブとしてログオン、サービスとしてログオンです。

コンピューターアカウントの場合、コンピューターには必要なログオン権限のみを付与します。「ネットワークからこのコンピューターにアクセス」のログオン権限は、デリバリーコントローラーのコンピューターアカウントに必要です。

ユーザーアカウントの場合、ユーザーには必要なログオン権限のみを付与します。

Microsoftによると、デフォルトでは、Remote Desktop Usersグループには「リモートデスクトップサービス経由でのログオンを許可」のログオン権限が付与されています（ドメインコントローラーを除く）。

組織のセキュリティポリシーによっては、このグループをそのログオン権限から削除するよう明示的に規定している場合があります。次のアプローチを検討してください。

- マルチセッションOS用Virtual Delivery Agent (VDA) は、Microsoft Remote Desktop Servicesを使用します。Remote Desktop Usersグループを制限付きグループとして構成し、Active Directoryグループポリシーを介してグループのメンバーシップを制御できます。詳細については、Microsoftのドキュメントを参照してください。

- シングルセッションOS用VDAを含むCitrix Virtual Apps™ and Desktopsの他のコンポーネントでは、Remote Desktop Usersグループは不要です。したがって、これらのコンポーネントの場合、Remote Desktop Usersグループは「リモートデスクトップサービス経由でのログオンを許可」のログオン権限を必要としません。削除できます。さらに：
  - リモートデスクトップサービスを介してそれらのコンピューターを管理する場合は、そのようなすべての管理者がすでにAdministratorsグループのメンバーであることを確認してください。
  - リモートデスクトップサービスを介してそれらのコンピューターを管理しない場合は、それらのコンピューターでリモートデスクトップサービス自体を無効にすることを検討してください。

ログイン権限「リモートデスクトップサービス経由でのログオンを拒否」にユーザーとグループを追加することは可能ですが、ログオン拒否権限の使用は一般的に推奨されません。詳細については、Microsoftのドキュメントを参照してください。

Delivery Controllerのセキュリティ

Delivery Controller上のWindowsサービス

Delivery Controllerのインストールにより、以下のWindowsサービスが作成されます。

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService): VMのMicrosoft Active Directoryコンピューターアカウントを管理します。
- Citrix Analytics (NT SERVICE\CitrixAnalytics): サイト管理者が承認した場合、Citrixが使用するためのサイト構成の使用状況情報を収集します。その後、この情報をCitrixに送信し、製品の改善に役立てます。
- Citrix App Library (NT SERVICE\CitrixAppLibrary): AppDiskの管理とプロビジョニング、AppDNA統合、およびApp-Vの管理をサポートします。
- Citrix Broker Service (NT SERVICE\CitrixBrokerService): ユーザーが利用できる仮想デスクトップまたはアプリケーションを選択します。
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging): 管理者がサイトに対して行ったすべての構成変更およびその他の状態変更を記録します。
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService): 共有構成のためのサイト全体のリポジトリ。
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin): 管理者に付与された権限を管理します。

- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest): 他の Delivery Controller サービスのセルフテストを管理します。
- Citrix Host Service (NT SERVICE\CitrixHostService): Citrix Virtual Apps または Citrix Virtual Desktops 展開で使用されるハイパーバイザーインフラストラクチャに関する情報を保存し、コンソールがハイパーバイザープール内のリソースを列挙するために使用する機能も提供します。
- Citrix Machine Creation Services (NT SERVICE\CitrixMachineCreationService): デスクトップ VM の作成をオーケストレーションします。
- Citrix Monitor Service (NT SERVICE\CitrixMonitor): Citrix Virtual Apps または Citrix Virtual Desktops のメトリックを収集し、履歴情報を保存し、トラブルシューティングおよびレポートツール用のクエリインターフェイスを提供します。
- Citrix StoreFront Service (NT SERVICE\ CitrixStorefront): StoreFront の管理をサポートします。（StoreFront コンポーネント自体の一部ではありません。）
- Citrix StoreFront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService): StoreFrontの特権管理操作をサポートします。(StoreFrontコンポーネント自体の一部ではありません。)
- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService): メインサイトデータベースからローカルホストキャッシュに構成データを伝播します。
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService): メインサイトデータベースが利用できない場合に、ユーザーが利用できる仮想デスクトップまたはアプリケーションを選択します。

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これらは、他のCitrixコンポーネントと一緒にインストールされた場合にも作成されます。

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc): Citrixサポートが使用するための診断情報の収集をサポートします。
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService): Citrixによる分析のために診断情報を収集し、管理者が分析結果と推奨事項を表示してサイトの問題の診断に役立てられるようにします。

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これは現在使用されていません。有効になっている場合は、無効にしてください。

- Citrix リモートブローカープロバイダー (NT SERVICE\XaXdCloudProxy)

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これらは現在使用されていませんが、有効にする必要があります。無効にしないでください。

- Citrix オーケストレーションサービス (NT SERVICE\CitrixOrchestration)
- Citrix トラストサービス (NT SERVICE\CitrixTrust)

Citrix StoreFront™ Privileged Administration Serviceを除き、これらのサービスには、「サービスとしてログオン」のログオン権限と、「プロセスのメモリクォータの調整」、「セキュリティ監査の生成」、「プロセスレベルトークンの置き換え」の特権が付与されています。これらのユーザー権限を変更する必要はありません。これらの特権はDelivery Controllerでは使用されず、自動的に無効になります。

Citrix StoreFront Privileged AdministrationサービスとCitrix Telemetry Serviceを除き、前述のDelivery Controller Windowsサービスは、NETWORK SERVICE IDとしてログオンするように構成されています。これらのサービス設定を変更しないでください。

Citrix Config Synchronizer Serviceは、Delivery Controller上のローカル管理者グループにNETWORK SERVICEアカウントが属している必要があります。これにより、ローカルホストキャッシュが正しく機能します。

Citrix StoreFront Privileged Administration サービスは、ローカルシステム (NT AUTHORITY\SYSTEM) としてログオンするように構成されています。これは、通常サービスでは利用できない Delivery Controller StoreFront の操作 (Microsoft IIS サイトの作成を含む) に必要です。サービス設定を変更しないでください。

Citrix Telemetry Service は、サービス固有の ID としてログオンするように構成されています。

Citrix Telemetry Service は無効にできます。このサービスと、すでに無効になっているサービスを除き、これらの Delivery Controller Windows サービスを他に無効にしないでください。

ログオン権限の管理

VDA のコンピューターアカウントには、「ネットワークからこのコンピューターにアクセス」のログオン権限が必要です。詳細については、「Active Directory OU ベースの Controller 検出」を参照してください。

クライアントアクセス

クライアントアクセスは通常、Citrix StoreFront を展開することで提供されます。StoreFront のセキュリティ保護の詳細については、「StoreFront のドキュメント」を参照してください。

リモートユーザーが StoreFront および VDA に安全に接続できるようにするには、NetScaler® Gateway を展開します。

Citrix では、クライアントが Citrix Workspace アプリを使用して StoreFront に接続することを推奨しています。詳細については、各オペレーティングシステム用の Citrix Workspace アプリのドキュメント のセキュリティセクションを参照してください。または、ユーザーは Web ブラウザーを使用して StoreFront にアクセスすることもできます。

ユーザーが Citrix Workspace™ アプリ以外のアプリケーションを実行する能力が制限されているシンクライアントをユーザーに提供することを検討してください。デバイスが組織によって管理されている場合は、オペレーティングシステムのセキュリティ更新プログラムとウイルス対策ソフトウェアの展開を確実にするためのポリシーを導入する必要があります。ただし、多くの場合、ユーザーは組織の管理外にある管理されていないデバイスから接続できる必要があります。次の機能の使用を検討してください。

- Endpoint Analysis は、オペレーティングシステムやウイルス対策などのセキュリティ情報をエンドポイントでスキャンし、セキュリティ要件を満たさないクライアントへのアクセスを拒否します。
- App Protection は、キーロガーと画面キャプチャをブロックします。

混在バージョン環境

VDA のバージョンが Delivery Controller と異なる場合など、混在バージョン環境は一部のアップグレード中に避けられません。ベストプラクティスに従い、異なるバージョンの Citrix コンポーネントが共存する時間を最小限に抑えてください。混在バージョン環境では、たとえばセキュリティポリシーが一律に適用されない場合があります。

> **注:**
>
> これは他のソフトウェア製品にも共通しています。以前のバージョンの Active Directory を使用すると、新しいバージョンの Windows ではグループポリシーが部分的にしか適用されません。

> 以下のシナリオでは、特定の混在バージョンCitrix環境で発生する可能性のあるセキュリティ問題について説明します。Citrix Receiver 1.7を使用して、XenApp and XenDesktop 7.6 Feature Pack 2のVDAを実行している仮想デスクトップに接続すると、ポリシー設定 **デスクトップとクライアント間のファイル転送を許可する** がサイトで有効になりますが、XenApp and XenDesktop 7.1を実行しているDelivery Controllerでは無効にできません。これは、製品の後のバージョンでリリースされたポリシー設定を認識しないためです。このポリシー設定により、ユーザーはファイルを仮想デスクトップにアップロードおよびダウンロードできるようになり、これがセキュリティ問題となります。この問題を回避するには、Delivery

> Controller（またはStudioのスタンドアロンインスタンス）をバージョン7.6 Feature Pack 2にアップグレードし、グループポリシーを使用してポリシー設定を無効にします。または、影響を受けるすべての仮想デスクトップでローカルポリシーを使用します。

Remote PC Accessのセキュリティに関する考慮事項

Remote PC Access は、以下のセキュリティ機能を実装しています。

- スマートカードの使用がサポートされています。
- リモートセッションが接続されると、オフィスのPCのモニターは空白で表示されます。
- Remote PC Accessは、CTRL+ALT+DELおよびUSB対応のスマートカードと生体認証デバイスを除くすべてのキーボードおよびマウス入力をリモートセッションにリダイレクトします。
- SmoothRoamingは単一ユーザーのみがサポートされます。
- ユーザーがオフィスPCにリモートセッションを接続している場合、そのユーザーのみがオフィスPCのローカルアクセスを再開できます。ローカルアクセスを再開するには、ユーザーはローカルPCでCtrl-Alt-Delを押し、リモートセッションで使用されたものと同じ資格情報でログオンします。システムに適切なサードパーティのCredential Provider統合がある場合、ユーザーはスマートカードを挿入するか、生体認証を利用してローカルアクセスを再開することもできます。このデフォルトの動作は、グループポリシーオブジェクト（GPO）を介して高速ユーザー切り替えを有効にするか、レジストリを編集することで上書きされます。

> **注:**
>
> Citrixでは、VDA管理者権限を一般セッションユーザーに割り当てないことを推奨しています。

自動割り当て

デフォルトでは、Remote PC Accessは複数のユーザーのVDAへの自動割り当てをサポートしています。XenDesktop 5.6 Feature Pack 1では、管理者はRemotePCAccess.ps1 PowerShellスクリプトを使用してこの動作を上書きできます。このリリースでは、複数の自動リモートPC割り当てを許可または禁止するためにレジストリエントリを使用します。この設定はサイト全体に適用されます。

> **注意:**

> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

> 自動割り当てを単一ユーザーに制限するには：

サイト内の各Controllerで、次のレジストリエントリを設定します。

```
HKEY_LOCAL_MACHINE\Software\Citrix|DesktopServer

Name: AllowMultipleRemotePCAssignments

Type: REG_DWORD

Data: 0 = Disable multiple user assignment, 1 = (Default) Enable multiple
user assignment.
```

既存のユーザー割り当てがある場合は、VDAがその後、単一の自動割り当ての対象となるように、SDKコマンドを使用してそれらを削除します。

- VDAから割り当てられているすべてのユーザーを削除します。`$machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine`
- デリバリーグループからVDAを削除します。`$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`

物理的なオフィスPCを再起動します。

証明書を管理する

TLSは、2つの当事者間の信頼を確立するために証明書を使用します。サービスを提供する各サーバーに適切な証明書をインストールし、そのサーバーに接続するマシンがその証明書を信頼することを確認する必要があります。証明書に署名するためのオプションは次のとおりです。

- 自己署名証明書。これらは推奨されません。これらの証明書は、信頼する必要がある他のマシンに手動でコピーする必要があるため、管理が困難です。
- エンタープライズ認証局。既存のPKIが導入されている場合、これは通常、内部デバイス間で使用する証明書に署名するための最も簡単なオプションです。

- 公開認証局。これには、ドメインの所有権を認証局に証明する必要があります。管理されていないクライアントデバイスは、主要な公開認証局からの証明書を信頼するように通常は事前設定されているという利点があります。

新しい証明書を作成する

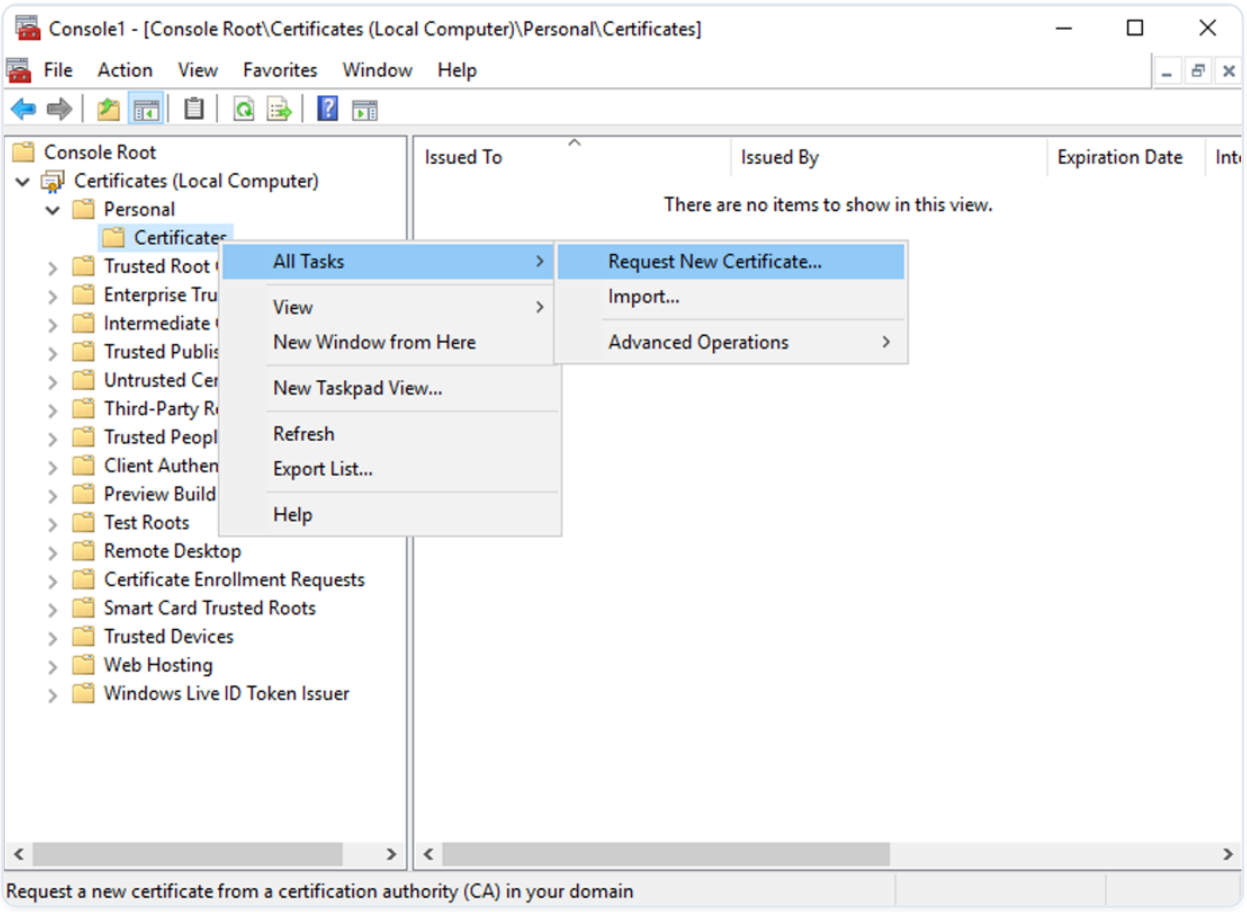
証明書の作成については、組織のポリシーと手順に従ってください。

Microsoft証明機関を使用して証明書を作成する

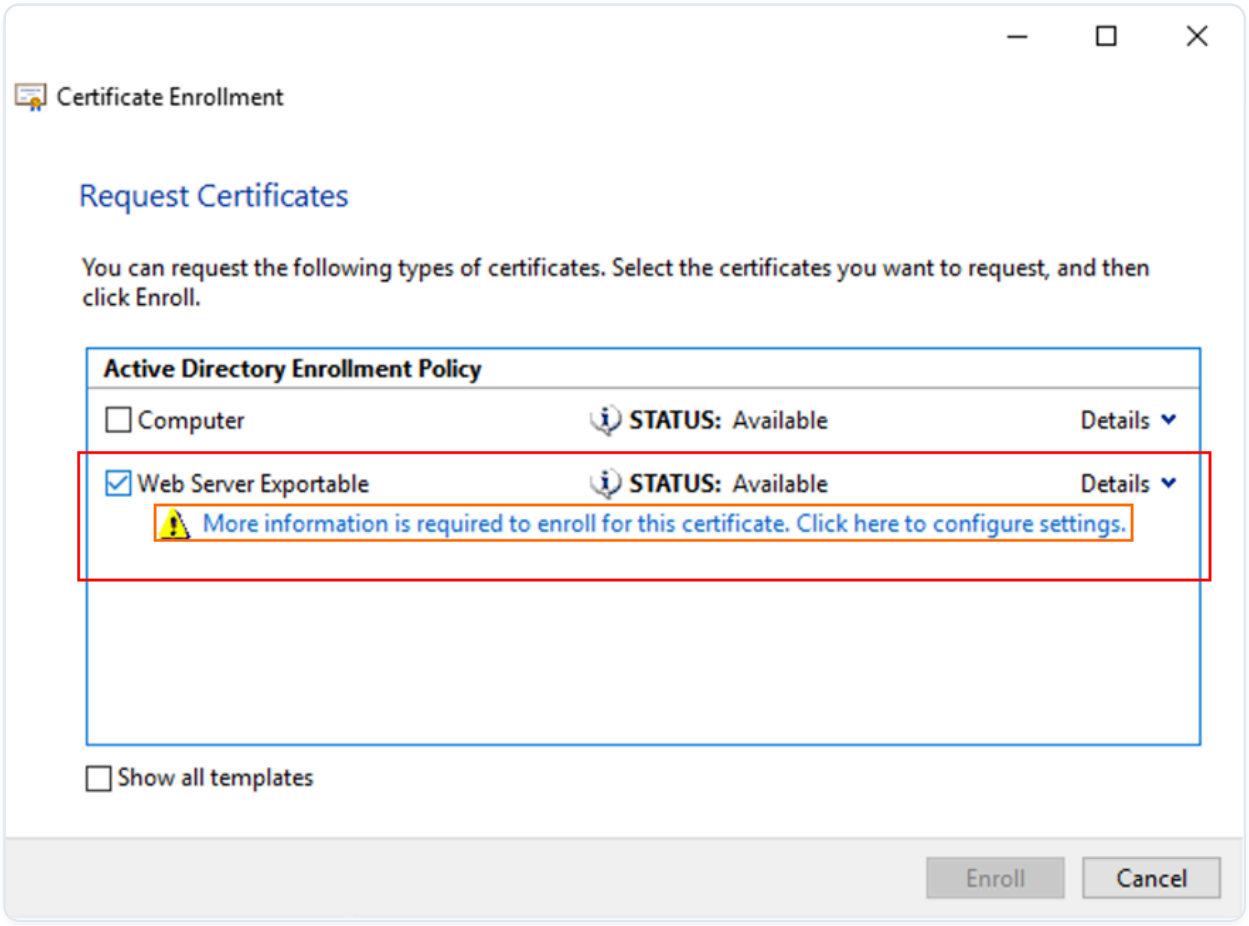
Microsoft証明機関がActive DirectoryドメインまたはDelivery Controllerが参加している信頼されたフォレストに統合されている場合、証明書MMCスナップインの証明書登録ウィザードから証明書を取得できます。Microsoft証明機関は、Webサーバーでの使用に適した証明書テンプレートを公開している必要があります。

ルート証明書は、グループポリシーを使用してドメイン上の他のマシンに自動的に展開されます。したがって、ドメイン上の他のすべてのマシンは、Microsoft証明機関を使用して作成された証明書を信頼します。ドメイン上にないマシンがある場合は、ルート認証局証明書をエクスポートして、それらのマシンにインポートする必要があります。

1. サーバーで、MMCコンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、「コンピューターアカウント」を選択します。
2. **個人 > 証明書**を展開し、**すべてのタスク > 新しい証明書の要求**コンテキストメニューコマンドを使用します。



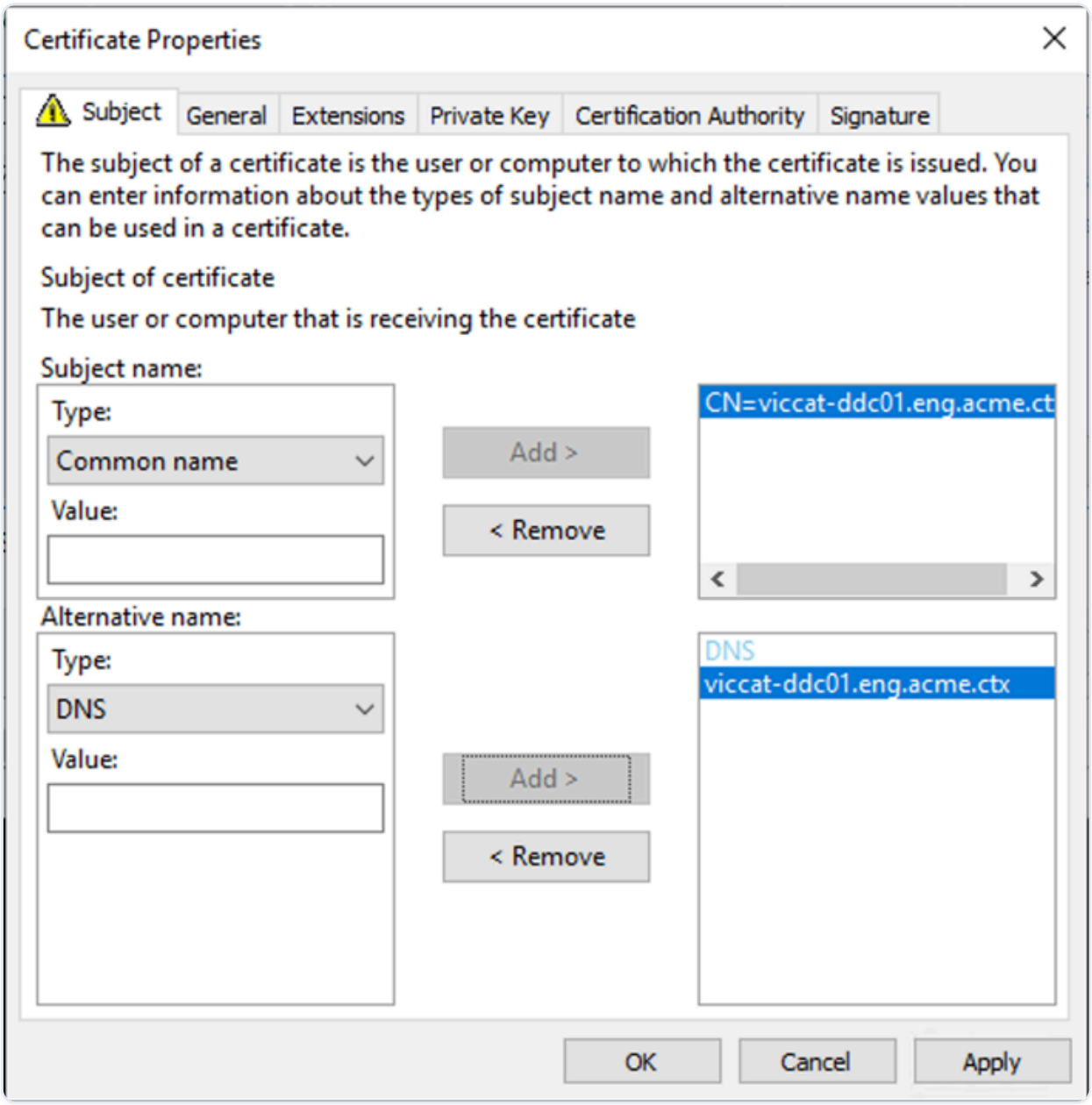
3. **次へ**をクリックして開始し、**次へ**をクリックして、Active Directory登録から証明書を取得することを確認します。
4. **Web Server Exportable**などの適切なテンプレートを選択します。テンプレートがSubjectの値を自動的に提供するように設定されている場合は、詳細を指定せずに**登録**をクリックできます。それ以外の場合は、**この証明書を登録するには詳細情報が必要です。ここをクリックして設定を構成してください。**をクリックします。



5. 証明書テンプレートの詳細を指定するには、**詳細**矢印ボタンをクリックして、以下を構成します。

   サブジェクト名: を選択し、サーバーの FQDN を追加します。

   代替名: を選択し、サーバーの FQDN を追加します。



6. **OK**を押します。
7. **登録**を押して証明書を作成します。証明書の一覧に表示されます。

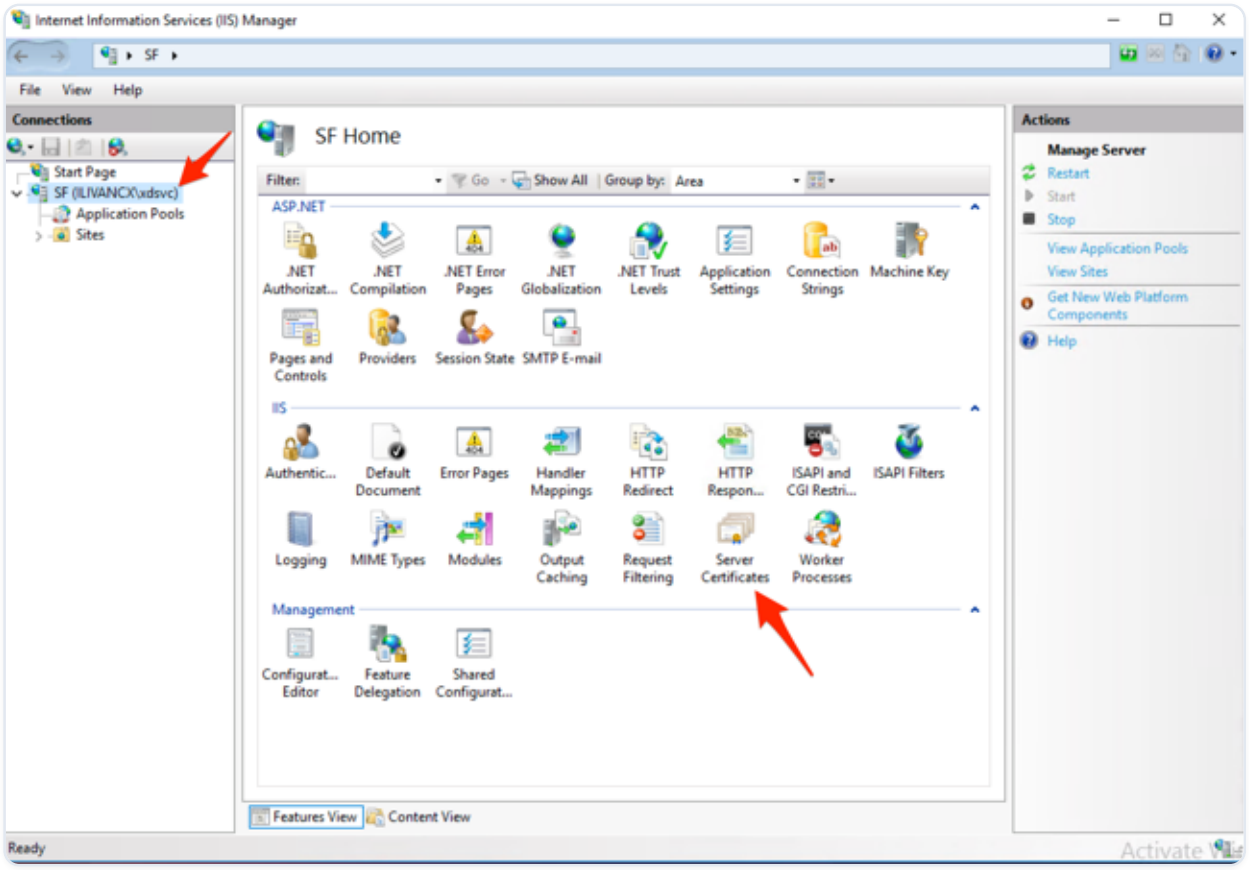
   個人証明書のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2511/media/personal-certificates.png)

IIS を使用して証明書要求を作成する

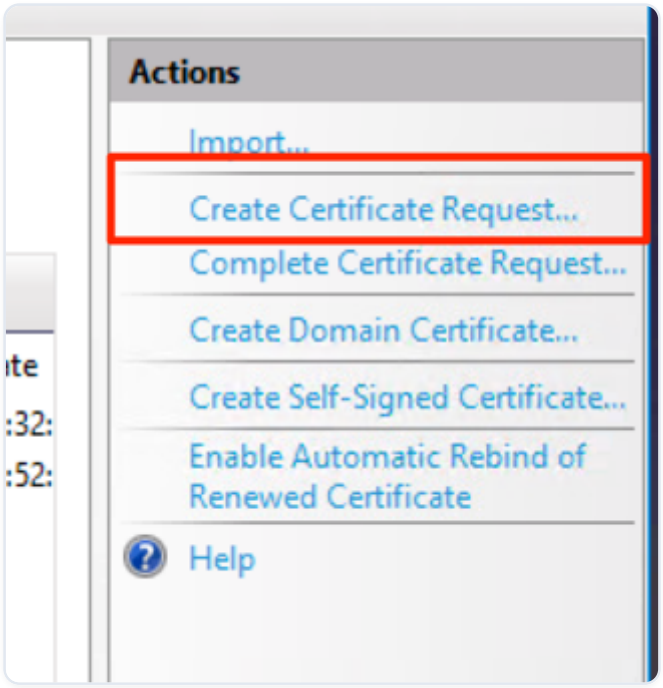
IIS がサーバーにインストールされている場合は、次の手順を実行します。

1. **インターネットインフォメーションサービス（IIS）マネージャー**を開きます。
2. 接続リストでサーバーノードを選択します。

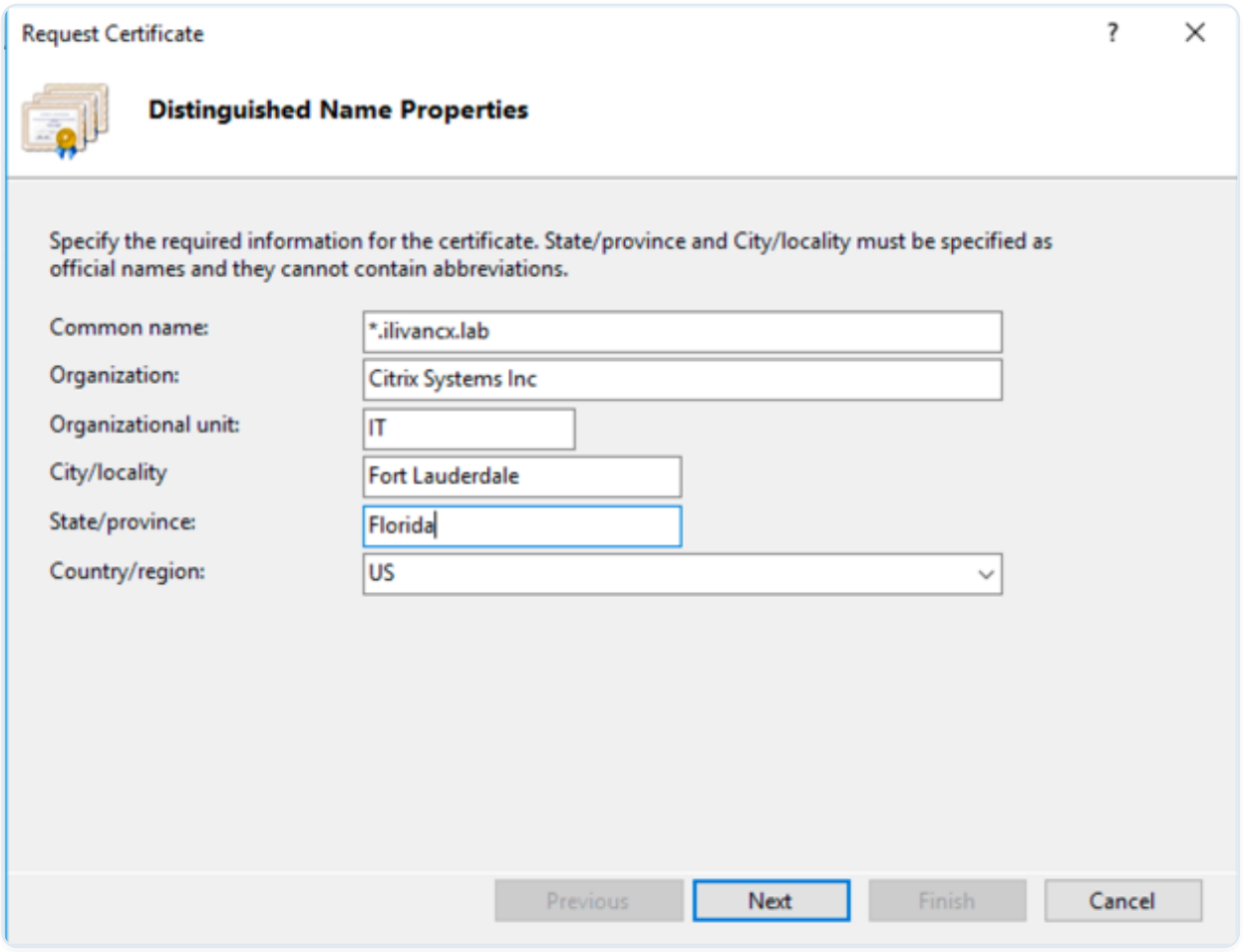
3. **サーバー証明書**を開きます。



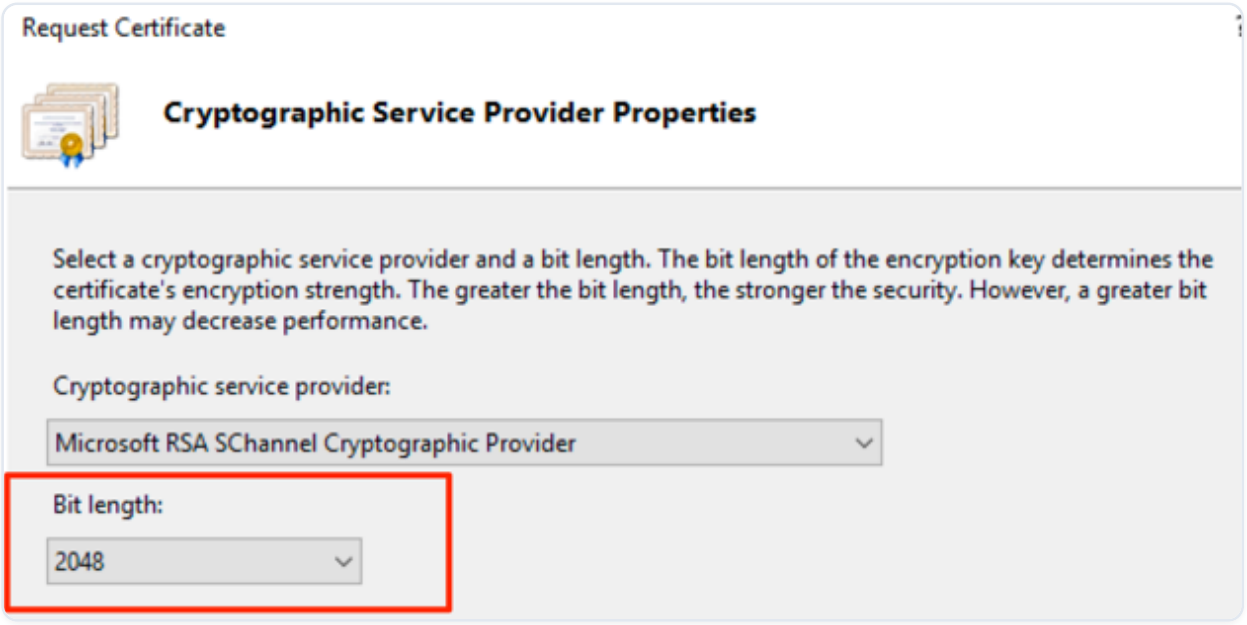
4. **操作**ペインから、**証明書の要求の作成...**を選択します。



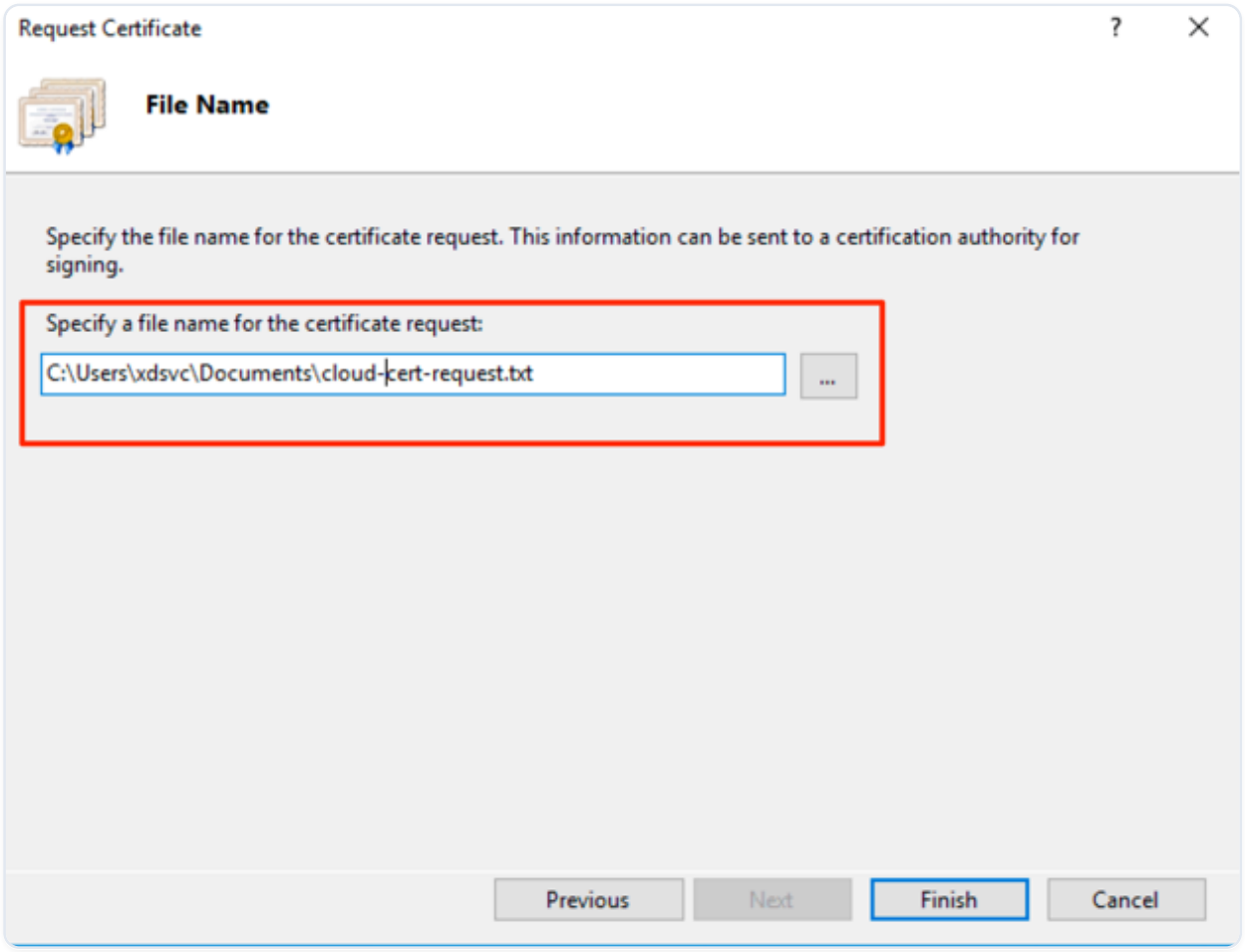
5. **識別名プロパティ**を入力します。



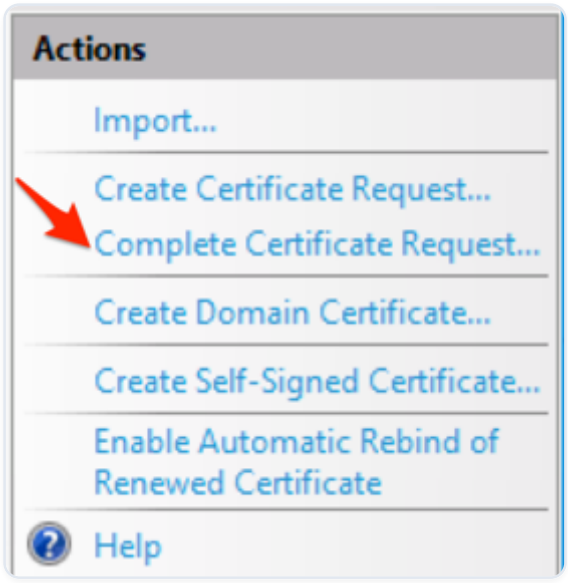
6. 「**暗号化サービスプロバイダーのプロパティ**」画面で、「**暗号化サービスプロバイダー**」はデフォルトのままにします。キーサイズは**2048**以上に設定します。



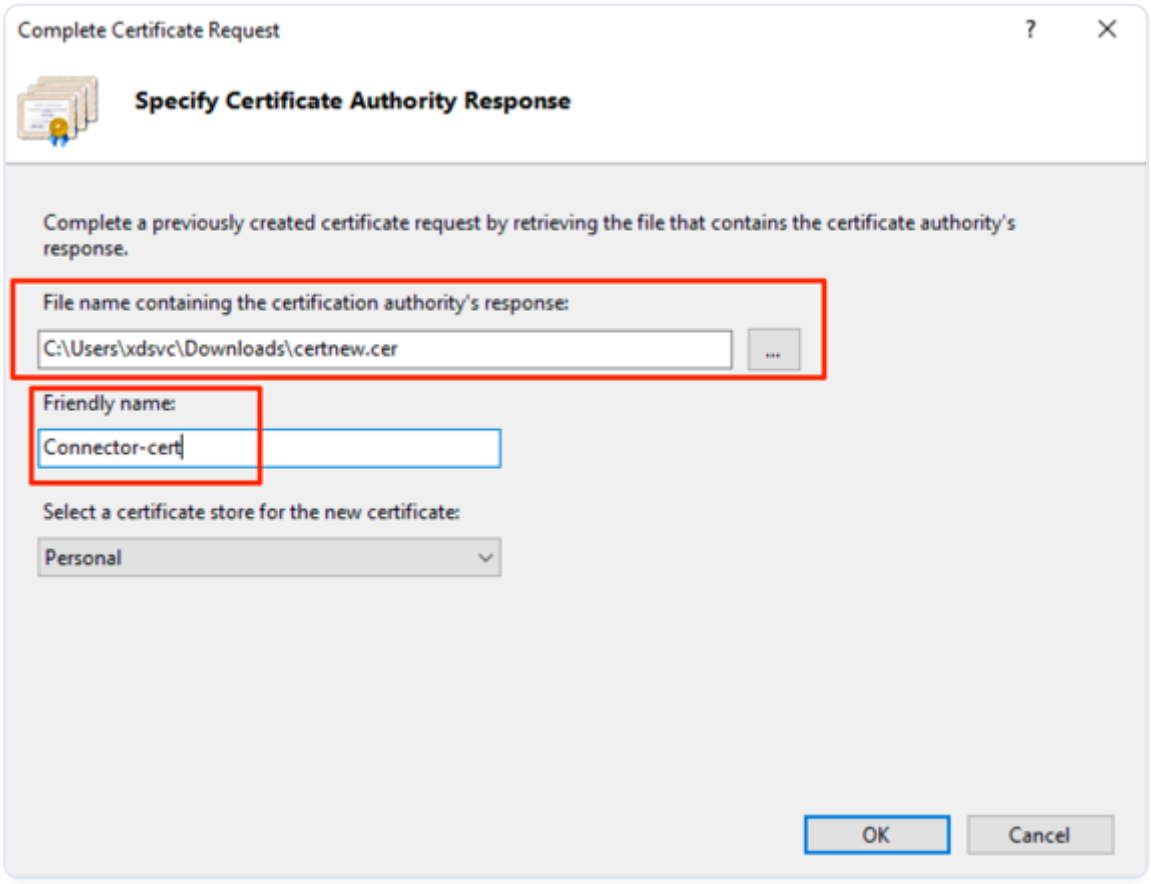
7. ファイル名を選択し、「**完了**」を押します。



8. CSRを証明機関にアップロードします。
9. 証明書を受け取ったら、「**操作**」ペインから「**証明書要求の完了...**」を選択します。



10. 証明書を選択し、「**フレンドリ名**」を入力して「**OK**」を押します。



サブジェクトの別名を設定する方法はありません。そのため、証明書は共通名を使用して指定されたサーバーに限定されます。

証明書スナップインから証明書署名要求を作成する

証明書MMCスナップイン内から、証明書署名要求を作成できます。これにより、証明書を提供する証明機関に送信できるファイルが生成されます。その後、ローカルの秘密鍵と結合するために証明書をインポートする必要があります。

1. サーバーでMMCコンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら「コンピューターアカウント」を選択します。
2. 「**個人**」>「**証明書**」を展開します。
3. 「**すべてのタスク**」>「**高度な操作**」>「**カスタム要求の作成**」を選択します。
4. 「**開始する前に**」で、「**次へ**」を選択します。
5. 「**証明書登録ポリシーの選択**」画面で、適切な既存のポリシーを選択するか、「**登録ポリシーなしで続行**」を選択します。
6. 「**カスタム要求**」画面で、登録ポリシーを使用している場合は、利用可能な場合は「**Webサーバーエクスポート可能**」などの適切なテンプレートを選択します。
7. 「**証明書情報**」画面で、「**詳細**」を展開し、「**プロパティ**」を選択します。

8. 「**証明書のプロパティ**」ウィンドウの「**全般**」タブで、適切なフレンドリ名を入力します。
9. 「**サブジェクト**」タブで:
    a. **サブジェクト名**の下で、**共通名**を選択し、サーバーのFQDNを入力します。ワイルドカードを入力できます。**追加**を選択します。
    b. **サブジェクト名**の下で、組織、組織単位、地域、都道府県、国に適切な値を追加します。
    c. **代替名**の下で、**DNS**を選択します。サーバーのFQDNを追加します。複数のサーバーFQDNまたはワイルドカードFQDNを追加できます。
10. **拡張機能**タブで、次のようにします。
    - 「**キー使用法**」で、「**デジタル署名**」と「**キーの暗号化**」を追加します。
    - 「**拡張キー使用法 (アプリケーションポリシー)**」で、「**サーバー認証**」と「**クライアント認証**」を追加します。
11. 「**秘密キー**」タブで。
    - 「**暗号化サービスプロバイダー (CSP) の選択**」で、適切なプロバイダーを選択します。
    - 「**キーオプション**」で、適切なキーサイズを選択します。RSAプロバイダーの場合、最小で2048のキーサイズを使用します。セキュリティを強化するために4096を選択することもできますが、パフォーマンスにわずかな影響があります。
    - 「**キーオプション**」で、「**秘密キーをエクスポート可能にする**」を選択します。
12. **OK**を選択します。
13. **次へ**を選択します。
14. 「**参照**」を選択し、要求を保存します。
15. 「**完了**」を選択します。
16. CSR を証明機関にアップロードします。
17. 証明書を受け取ったら、プライベートキーにリンクされるように、同じサーバーで(#import-existing-certificate)インポートします。

新しい自己署名証明書を作成する

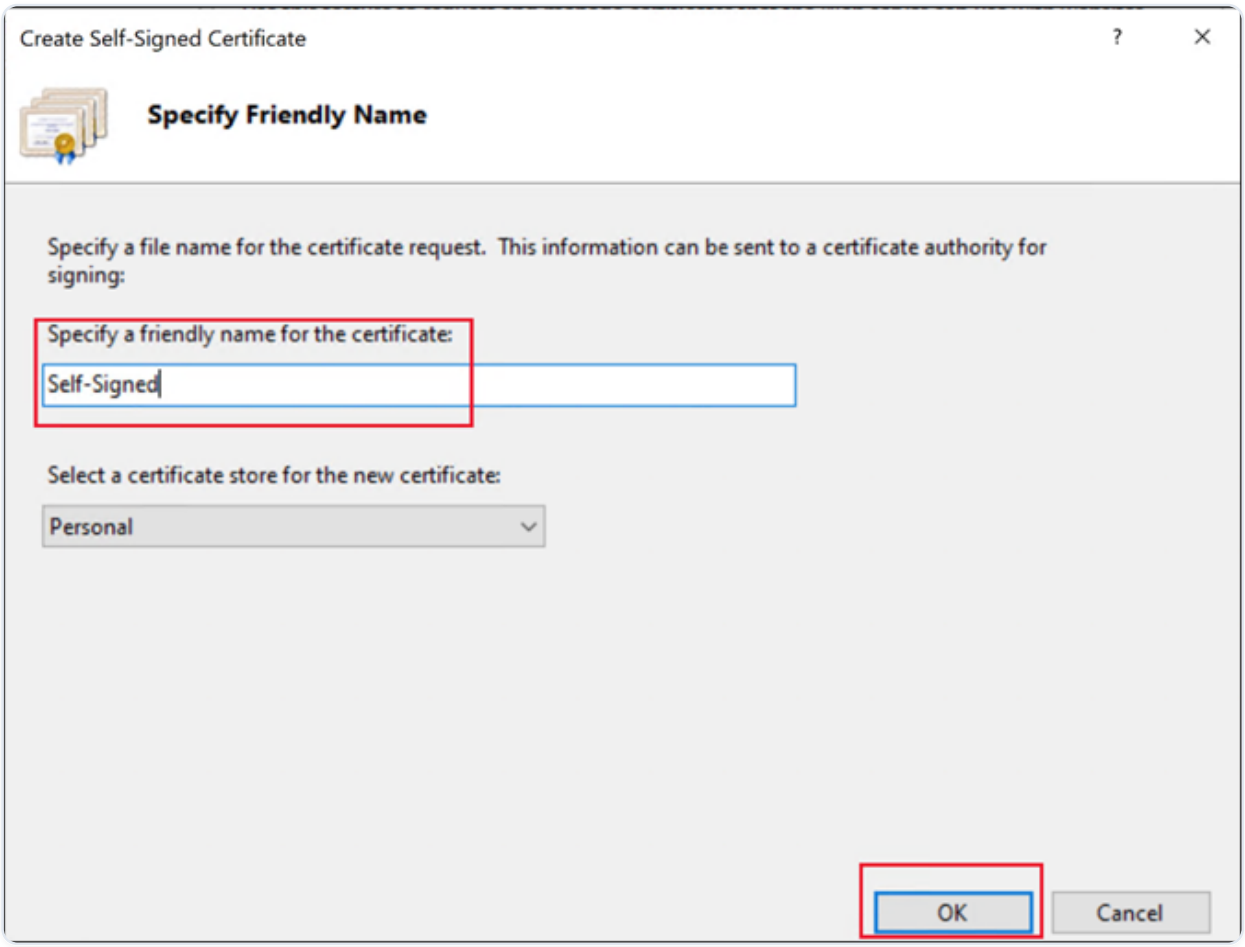
自己署名証明書は、デリバリーコントローラー™とWeb Studioのインストール中に作成されます。新しい自己署名証明書を生成し、既存の証明書と置き換えることができます。

IISマネージャーを使用して

IISがサーバーにインストールされている場合、次の手順を実行できます。

1. 管理者としてサーバーにログオンします。
2. IISマネージャーを開きます
3. **サーバー証明書**を開きます
4. **操作**ペインで、「**自己署名証明書の作成**」を選択します。

   サーバー証明書(/en-us/citrix-virtual-apps-desktops/2511/media/server-certificates.png)
5. 「**自己署名証明書の作成**」で、証明書の名前を入力し、「**OK**」をクリックします。自己署名証明書が作成されます。



PowerShellを使用して

PowerShellを使用して自己署名証明書を作成できます。

```
$certSubject = "CN=myddc.example.com" # The FQDN of the server.

$friendlyName = "Self-Signed-3"

$expireYears = 5
```

```
## Create new self-signed certificate under LocalMachine\My

$certificate = New-SelfSignedCertificate -Subject $certSubject
-CertStoreLocation "Cert:\LocalMachine\My\" -KeyExportPolicy Exportable
-KeySpec Signature -KeyLength 2048 -KeyAlgorithm RSA -HashAlgorithm SHA256
-FriendlyName $friendlyName -NotAfter $
([System.DateTime]::Now.AddYears($expireYears))



# Add to trusted root certificates

$rootCertStore = Get-Item "Cert:\LocalMachine\Root\"

$rootCertStore.Open([System.Security.Cryptography.X509Certificates.OpenFla
gs]::ReadWrite)

$rootCertStore.Add($certificate)
```

既存の証明書をインポートする

以下のいずれかの方法を使用して、既存の証明書をサーバーにインポートできます。

証明書のインポートウィザード

1. PFXファイルをダブルクリックするか、ファイルを右クリックして「**PFXのインストール**」を選択します。これにより、「**証明書のインポートウィザード**」が開きます。
2. 「**ストアの場所**」で、「**ローカルコンピューター**」を選択します。

   証明書のインポートウィザードのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2511/media/certificate-import-wizard.png)
3. 必要に応じてパスワードを入力します。

   証明書のインポートウィザード、秘密キー保護ステップのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2511/media/key-protection.png)
4. を選択します。サーバー証明書の場合は、 を選択します。このマシンから信頼したいルート証明書または自己署名証明書である場合は、 を選択します。

   証明書のインポートウィザード、証明書ストアステップのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2511/media/certificate-store.png)

コンピューター証明書の管理コンソールを使用する

1. コンピューター証明書の管理コンソールを開き、適切な証明書ストアに移動します。サーバー証明書の場合、通常は「**個人**」 > 「**証明書**」です。ルート証明書または自己署名証明書を信頼するには、「**信頼されたルート証明機関**」 > 「**証明書**」を選択します。
2. 証明書を右クリックし、「**すべてのタスク**」>「**インポート...**」を選択します。

   コンピューター証明書の管理コンソール(/en-us/citrix-virtual-apps-desktops/2511/media/manage-computer-certificates-console.png)
3. 「**参照...**」を選択し、ファイルを選択します。
4. 必要に応じてパスワードを入力します。

PowerShellを使用する

証明書をインポートするには、PowerShell コマンドレット Import-PfxCertificate を使用します。たとえば、証明書 `certificate.pfx` をパスワード `123456` で個人証明書ストアにインポートするには、次のコマンドを実行します。

```
Import-PfxCertificate -Password $(ConvertTo-SecureString -String "123456"
-AsPlainText -Force) -CertStoreLocation Cert:\LocalMachine\My\ -FilePath .
\Desktop\certificate.pfx
```

信頼されたルート証明書をインポートするには、`CertStoreLocation` を `Cert:\LocalMachine\Root\` に設定します。

秘密キーなしで証明書をエクスポートする

証明書を他のデバイスにインポートして信頼できるようにエクスポートするには、秘密キーを除外する必要があります。

1. コンピューター証明書の管理を開きます。「**個人**」>「**証明書**」に移動し、エクスポートする証明書を選択します。
2. 「**操作**」メニューから「**すべてのタスク**」を選択し、次に「**エクスポート**」を選択します。

   エクスポートメニューのある証明書管理のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2511/media/certificate-export.png)
3. 「**いいえ、秘密キーをエクスポートしません**」を選択し、「**次へ**」を押します。

   証明書のエクスポート(/en-us/citrix-virtual-apps-desktops/2511/media/certificate-export-no-private-key.png)

4. 形式「**DER encoded binary X.509 (.CER)**」（デフォルト）を選択し、「**次へ**」を押します。
5. ファイル名を入力し、「**次へ**」を押します。

   「証明書のエクスポートウィザード、ファイル名」のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2511/media/certificate-export-file.png)
6. 「**完了**」を選択します。

   「証明書のエクスポートウィザード、エクスポート成功」のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2511/media/certificate-export-complete.png)

秘密キー付きで証明書をエクスポートする

他のサーバーで使用できるように証明書をエクスポートするには、秘密キーを含める必要があります。

1. コンピューター証明書の管理を開きます。「**個人**」>「**証明書**」に移動し、エクスポートする証明書を選択します。
2. 「**操作**」メニューから「**すべてのタスク**」を選択し、次に「**エクスポート**」を選択します。

   エクスポートメニューがある証明書管理のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2511/media/certificate-export.png)
3. 「**はい、秘密キーをエクスポートします**」を選択し、次に「**次へ**」を選択します。

   「証明書のエクスポート」(/en-us/citrix-virtual-apps-desktops/2511/media/certificate-export-private-key.png)
4. 「**セキュリティ**」タブでパスワードを入力し、次に「**次へ**」を選択します。

   「証明書のエクスポートウィザード、セキュリティ手順」のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2511/media/certificate-export-password.png)
5. ファイル名を入力し、「**次へ**」を選択します。

   「証明書のエクスポートウィザード、ファイル名」のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2511/media/certificate-export-file.png)
6. 「**完了**」を選択します。

   証明書のエクスポートウィザード、エクスポート成功のスクリーンショット](/en-us/citrix-virtual-apps-desktops/2511/media/certificate-export-complete.png)

証明書をPEM形式に変換する

デフォルトでは、Windowsは秘密鍵を含む.pfxファイルとしてPKCS#12形式で証明書をエクスポートします。NetScaler® Gatewayまたはライセンスサーバーで証明書を使用するには、証明書と秘密鍵をPEM形式の別々のファイルに抽出する必要があります。これはopensslを使用して実行できます。

証明書をPEM形式でエクスポートするには、以下を実行します。

```
openssl pkcs12 -in name.pfx -clcerts -nokeys -out name.cer
```

既存のパスワードと新しいパスフレーズの入力を求められます

キーをPEM形式でエクスポートするには、以下を実行します。

```
openssl pkcs12 -in name.pfx -nocerts -out name.key
```

証明書の信頼

- 公開認証局の証明書を使用する場合、デバイスには通常、ルート証明書が事前に構成されています。
- エンタープライズ認証局を使用する場合は、その証明書を信頼する必要があるすべてのデバイスにルート証明書を展開する必要があります。Active Directory証明書サービスを使用している場合、ルート証明書はグループポリシーを使用してドメイン上のすべてのマシンにも展開されます。NetScalerゲートウェイや他のドメイン上のマシンなど、ドメインに参加していないマシンには、ルート証明書を手動でインポートする必要があります。
- 自己署名証明書を使用している場合は、証明書を信頼する必要があるすべてのマシンに手動でインストールする必要があります。

Windowsから自己署名証明書または信頼されたルート証明書をエクスポートするには、秘密鍵なしで証明書をエクスポートするを参照してください。

Windowsが証明書を信頼するようにするには、**信頼されたルート証明機関**ストアに証明書をインポートする必要があります。PowerShellを使用する場合は、ストア**Cert:\\LocalMachine\Root**を入力します。

NetScalerが証明書を信頼するには、まず証明書をPEM形式に変換するし、次にルート証明書をインストールする必要があります。

スマートカード

スマートカードおよび同等のテクノロジーは、この記事で説明されているガイドライン内でサポートされています。Citrix Virtual Apps または Citrix Virtual Desktops™ でスマートカードを使用するには、次の手順を実行します。

- スマートカードの使用に関する組織のセキュリティポリシーを理解します。これらのポリシーには、たとえば、スマートカードの発行方法やユーザーがスマートカードを保護する方法が記載されている場合があります。これらのポリシーの一部は、Citrix Virtual Apps™ または Citrix Virtual Desktops 環境で再評価する必要がある場合があります。
- スマートカードで使用するユーザーデバイスの種類、オペレーティングシステム、および公開アプリケーションを決定します。
- スマートカードテクノロジーと、選択したスマートカードベンダーのハードウェアおよびソフトウェアに精通してください。
- 分散環境でデジタル証明書を展開する方法を理解します。

> **注:**
>
> スマートカードの登録は、高速スマートカードではサポートされていません。高速スマートカードが無効になっている場合、スマートカードの登録は機能する可能性がありますが、スマートカードとミドルウェアの種類によって異なります。仮想セッションを介したスマートカードの登録に関する Citrix Virtual Apps and Desktops との統合およびサポートについては、スマートカードおよびミドルウェアベンダーにお問い合わせください。

スマートカードの種類

エンタープライズおよびコンシューマー向けスマートカードは、同じ寸法、電気コネクタを持ち、同じスマートカードリーダーに適合します。

エンタープライズ用途のスマートカードには、デジタル証明書が含まれています。これらのスマートカードは Windows Logon をサポートしており、ドキュメントやメールのデジタル署名および暗号化用のアプリケーションでも使用できます。Citrix Virtual Apps and Desktops™ はこれらの用途をサポートしています。

コンシューマー用途のスマートカードにはデジタル証明書は含まれていません。共有シークレットが含まれています。これらのスマートカードは、支払い（チップと署名またはチップとPINのクレジットカードなど）をサポートできます。Windows Logon や一般的な Windows アプリケーションはサポートしていません。これらのスマートカードを使用するには、特殊な Windows アプ

リケーションと適切なソフトウェアインフラストラクチャ（たとえば、支払いカードネットワークへの接続を含む）が必要です。Citrix Virtual Apps または Citrix Virtual Desktops でこれらの特殊なアプリケーションをサポートする方法については、Citrix の担当者にお問い合わせください。

エンタープライズスマートカードには、同様の方法で使用できる互換性のある同等品があります。

- スマートカードと同等の USB トークンは、USB ポートに直接接続します。これらの USB トークンは通常、USB フラッシュドライブと同じくらいのサイズですが、携帯電話で使用される SIM カードと同じくらい小さい場合もあります。これらは、スマートカードと USB スマートカードリーダーの組み合わせとして表示されます。
- Windows Trusted Platform Module (TPM) を使用する仮想スマートカードは、スマートカードとして表示されます。これらの仮想スマートカードは、Citrix Workspace app (最小バージョン Citrix Receiver 4.3) を使用して、Windows 8 および Windows 10 でサポートされています。
    - XenApp and XenDesktop 7.6 FP3より前のバージョンのCitrix Virtual Apps and Desktops（旧XenApp and XenDesktop）は、仮想スマートカードをサポートしていません。
    - 仮想スマートカードの詳細については、「仮想スマートカードの概要」を参照してください。

    注: 「仮想スマートカード」という用語は、ユーザーコンピューターに保存されているデジタル証明書を指す場合もあります。これらのデジタル証明書は、厳密にはスマートカードと同等ではありません。

Citrix Virtual Apps and Desktopsのスマートカードサポートは、Microsoft Personal Computer/Smart Card (PC/SC) 標準仕様に基づいています。最低要件として、スマートカードおよびスマートカードデバイスは、基盤となるWindowsオペレーティングシステムによってサポートされ、対象となるWindowsオペレーティングシステムを実行するコンピューターで使用するためにMicrosoft Windows Hardware Quality Labs (WHQL) によって承認されている必要があります。ハードウェアのPC/SC準拠に関する追加情報については、Microsoftのドキュメントを参照してください。他の種類のユーザーデバイスもPS/SC標準に準拠している場合があります。詳細については、「Citrix Readyプログラム」を参照してください。

通常、各ベンダーのスマートカードまたは同等のものには、個別のデバイスドライバーが必要です。ただし、スマートカードがNIST Personal Identity Verification (PIV) 標準などの標準に準拠している場合、さまざまなスマートカードに単一のデバイスドライバーを使用できる可能性があります。デバイスドライバーは、ユーザーデバイスとVirtual Delivery Agent (VDA) の両方にインストールする必要があります。デバイスドライバーは、Citrixパートナーから入手できるスマートカードミドルウェアパッケージの一部として提供されることが多く、このスマートカードミドルウェア

パッケージは高度な機能を提供します。デバイスドライバーは、Cryptographic Service Provider (CSP)、Key Storage Provider (KSP)、またはミニドライバーとも呼ばれることがあります。

Windowsシステム用の以下のスマートカードとミドルウェアの組み合わせは、Citrixによってそのタイプの代表的な例としてテストされています。ただし、他のスマートカードとミドルウェアも使用できます。Citrix互換のスマートカードとミドルウェアの詳細については、`<http://www.citrix.com/ready>`を参照してください。

ミドルウェア	対応カード
Gemalto .NETカード用ミニドライバー	ジェムアルト ドットネット v2以降

他の種類のデバイスでのスマートカードの使用に関する情報については、そのデバイスのCitrix Workspace™アプリのドキュメントを参照してください。

リモートPCアクセス

スマートカードは、Windows 10、Windows 8、またはWindows 7を実行している物理的なオフィスPCへのリモートアクセスでのみサポートされます。

以下のスマートカードは、Remote PC Accessでテストされました。

ミドルウェア	対応カード
Gemalto .NET ミニドライバー	Gemalto .NET v2以降

高速スマートカード

高速スマートカードは、既存のHDX PC/SCベースのスマートカードリダイレクトに対する改善です。待機時間の長いWAN環境でスマートカードが使用される場合のパフォーマンスを向上させます。待機時間が長い場合、パフォーマンスの向上は顕著になります（例: Windowsの高速スマートカードログオンでは15秒、PC/SCベースのスマートカードリダイレクトでは1分以上かかる場合と比較して）。

高速スマートカードは、現在サポートされているWindows VDAが搭載されたホストマシンでデフォルトで有効になっています。ホスト側で高速スマートカードを無効にするには（診断目的など）、'Disable Cryptographic Redirection'レジストリ設定をゼロ以外の値に設定します。

```
HKLM\SOFTWARE\Citrix\SmartCard

CryptographicRedirectionDisable (DWORD)
```

クライアント側で高速スマートカードを有効にするには、関連するStoreFrontサイトの*default.ica*ファイルにSmartCardCryptographicRedirection ICAパラメーターを含めます。

```
[WFClient]

SmartCardCryptographicRedirection=On
```

さらに、クライアント側では、高速スマートカードを以下のレジストリ設定で強制的に有効または無効にできます（診断目的など）。

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceEnableCryptographicRedirection （ゼロ以外のDWORDとして）

または

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceDisableCryptographicRedirection （ゼロ以外のDWORDとして）

クライアントマシンが64ビットの場合、32ビットレジストリハイブを指定する必要があります（`WOW6432Node`を使用）。

制限事項:

- Citrix Workspaceアプリfor Windowsのみが高速スマートカードをサポートします。default.icaファイルで高速スマートカードを構成した場合でも、Windows用ではないCitrix Workspaceアプリは、既存のPC/SCリダイレクトを依然として使用します。
- 高速スマートカードがサポートする唯一のダブルホップシナリオは、両方のホップで高速スマートカードが有効になっているICA® > ICAです。高速スマートカードはICA > RDPダブルホップシナリオをサポートしないため、これらのシナリオは機能しません。
- 高速スマートカードは次世代暗号化をサポートしていません。そのため、高速スマートカードは楕円曲線暗号 (ECC) スマートカードをサポートしていません。
- 高速スマートカードは、読み取り専用キーコンテナー操作のみをサポートしています。
- 高速スマートカードは、スマートカードPINの変更をサポートしていません。

VDAバージョン2203およびWindows向けCitrix Workspaceアプリバージョン2202（またはそれ以降）以降、高速スマートカードは次世代暗号化 (CNG) と互換性があります。さらに、楕円曲線暗号 (ECC) スマートカードは、ECDSAとECDHの両方で、P-256、P-384、P-521ビットの以下の曲線に対応しています。

VDAバージョン2203以降、高速スマートカードは、同じユーザーのログオンセッション内のアプリケーション間でスマートカードPINをキャッシュする機能を追加します。例えば、**セッションPINキャッシュ**が有効になっており、エンドユーザーが以前にOutlookにスマートカードPINを提供している場合、その後Wordを使用してドキュメントに署名すると、Wordはすでにキャッシュされているスマートカード PIN（Outlookに送信されたもの）を使用します。**セッションPINキャッシュ**は、ユーザーがスマートカードPINを入力する回数を減らすことで、ユーザーエクスペリエンスを向上させます。さらに、スマートカードがVDAへのログオンに使用される場合、Windowsスマートカードログオン PINをオプションで**セッションPINキャッシュ**に保存できます。これにより、ユーザーエクスペリエンスがさらに向上します。

セッションPINキャッシュはデフォルトで無効になっています。VDA上の以下のレジストリ設定で有効化および制御できます。

HKLM\SOFTWARE\Citrix\SmartCard: で:

- `EnablePinSessionCache` をDWORDとして (有効にするにはゼロ以外)
- `EnableLogonPinSessionCache` をDWORDとして (有効にするにはゼロ以外)
- `PinSessionCacheEntryStaleTimeout` をDWORDとして (エントリが古くなるまでの秒数、デフォルトは1時間)

スマートカードリーダーの種類

スマートカードリーダーは、ユーザーデバイスに内蔵されている場合と、ユーザーデバイスに別途接続されている場合（通常はUSBまたはBluetooth経由）があります。USBチップ/スマートカードインターフェースデバイス (CCID) 仕様に準拠した接触型カードリーダーがサポートされています。これらには、ユーザーがスマートカードを挿入するスロットまたはスワイプ機能があります。Deutsche Kreditwirtschaft (DK) 規格では、接触型カードリーダーを4つのクラスに定義しています。

- クラス1スマートカードリーダーは最も一般的で、通常はスロットを備えています。クラス1スマートカードリーダーは、通常、オペレーティングシステムに付属の標準CCIDデバイスドライバーでサポートされます。
- クラス2スマートカードリーダーには、ユーザーデバイスからアクセスできないセキュアキーパッドも搭載されています。クラス2スマートカードリーダーは、セキュアキーパッドが統合

されたキーボードに組み込まれている場合があります。クラス2スマートカードリーダーについては、Citrixの担当者にお問い合わせください。セキュアキーパッド機能を有効にするには、リーダー固有のデバイスドライバーが必要になる場合があります。

- クラス3スマートカードリーダーには、セキュアディスプレイも搭載されています。クラス3スマートカードリーダーはサポートされていません。
- クラス4スマートカードリーダーには、セキュアトランザクションモジュールも搭載されています。クラス4スマートカードリーダーはサポートされていません。

> **注:**
>
> スマートカードリーダーのクラスは、USBデバイスクラスとは関係ありません。

> スマートカードリーダーは、ユーザーデバイスに適切なデバイスドライバーをインストールして使用する必要があります。

サポートされているスマートカードリーダーについては、使用しているCitrix Workspaceアプリのドキュメントを参照してください。Citrix Workspaceアプリのドキュメントでは、サポートされているバージョンがスマートカードに関する記事またはシステム要件に関する記事に記載されています。

ユーザーエクスペリエンス

スマートカードのサポートは、Citrix Virtual Apps and Desktopsに統合されており、特定のICA/HDXスマートカード仮想チャネルを使用します。これはデフォルトで有効になっています。

重要：スマートカードリーダーに汎用USBリダイレクトを使用しないでください。これはスマートカードリーダーではデフォルトで無効になっており、有効にした場合でもサポートされません。

同じユーザーデバイスで複数のスマートカードと複数のリーダーを使用できますが、パススルー認証を使用している場合は、ユーザーが仮想デスクトップまたはアプリケーションを起動するときに、スマートカードを1枚だけ挿入する必要があります。アプリケーション内でスマートカードを使用する場合（デジタル署名や暗号化機能など）、スマートカードの挿入やPINの入力に関する追加のプロンプトが表示されることがあります。これは、複数のスマートカードが同時に挿入されている場合に発生する可能性があります。

- スマートカードがすでにリーダーに挿入されているにもかかわらず、スマートカードの挿入を求めるプロンプトが表示された場合は、［キャンセル］を選択する必要があります。

- PINの入力を求められた場合は、PINを再度入力する必要があります。

カード管理システムまたはベンダーユーティリティを使用してPINをリセットできます。

重要:

Citrix Virtual AppsまたはCitrix Virtual Desktopsセッション内で、Microsoft Remote Desktop Connectionアプリケーションでスマートカードを使用することはサポートされていません。これは「ダブルホップ」の使用として説明されることがあります。

スマートカードを展開する前に

- スマートカードリーダー用のデバイスドライバーを入手し、ユーザーデバイスにインストールします。多くのスマートカードリーダーは、Microsoftが提供するCCIDデバイスドライバーを使用できます。
- スマートカードベンダーからデバイスドライバーと暗号化サービスプロバイダー（CSP）ソフトウェアを入手し、ユーザーデバイスと仮想デスクトップの両方にインストールします。ドライバーとCSPソフトウェアはCitrix Virtual Apps and Desktopsと互換性がある必要があります。互換性についてはベンダーのドキュメントを確認してください。ミニドライバーモデルをサポートおよび使用するスマートカードを使用する仮想デスクトップの場合、スマートカードミニドライバーは自動的にダウンロードされますが、http://catalog.update.microsoft.comまたはベンダーから入手することもできます。また、PKCS#11ミドルウェアが必要な場合は、カードベンダーから入手してください。
- 重要：Citrixでは、Citrixソフトウェアをインストールする前に、物理コンピューターにドライバーとCSPソフトウェアをインストールしてテストすることをお勧めします。
- Windows 10でInternet Explorerを使用してスマートカードを使用するユーザーの場合、Citrix Receiver™ for WebのURLを信頼済みサイトリストに追加します。Windows 10では、Internet Explorerは信頼済みサイトに対してデフォルトで保護モードで実行されません。
- 公開鍵インフラストラクチャ（PKI）が適切に構成されていることを確認します。これには、Active Directory環境で証明書とアカウントのマッピングが正しく構成されており、ユーザー証明書の検証が正常に実行できることを確認することが含まれます。
- 展開が、Citrix WorkspaceアプリやStoreFrontなど、スマートカードで使用される他のCitrixコンポーネントのシステム要件を満たしていることを確認します。
- サイト内の以下のサーバーへのアクセスを確保します。

- スマートカード上のログオン証明書に関連付けられているユーザーアカウントのActive Directoryドメインコントローラー
- デリバリーコントローラー™
- Citrix StoreFront (シトリックス ストアフロント)
- シトリックス ゲートウェイ/シトリックス アクセス ゲートウェイ 10.x
- VDA
- （Remote PC Accessの場合、オプション）：Microsoft Exchange Server

スマートカードの使用を有効にする

ステップ 1. カード発行ポリシーに従って、ユーザーにスマートカードを発行します。

ステップ2. (オプション) リモートPCアクセスを有効にするために、スマートカードを設定します。

ステップ3. スマートカードのリモート処理のために、Delivery ControllerとStoreFrontをインストールして構成します（まだインストールされていない場合）。

ステップ4. スマートカードの使用のためにStoreFrontを有効にします。詳細については、StoreFrontのドキュメントの「スマートカード認証の構成」を参照してください。

ステップ5. スマートカードの使用のためにCitrix Gateway/Access Gatewayを有効にします。詳細については、NetScalerのドキュメントの「認証と承認の構成」および「Web Interfaceを使用したスマートカードアクセスの構成」を参照してください。

ステップ6. スマートカードの使用のためにVDAを有効にします。

- VDAに必要なアプリケーションと更新プログラムがあることを確認します。
- ミドルウェアをインストールします。
- スマートカードのリモート処理を設定し、ユーザーデバイス上のCitrix Workspaceアプリと仮想デスクトップセッションの間でスマートカードデータの通信を有効にします。

ステップ7. スマートカードの使用のためにユーザーデバイス（ドメイン参加済みまたは非ドメイン参加済みのマシンを含む）を有効にします。詳細については、StoreFrontのドキュメントの「スマートカード認証の構成」を参照してください。

- 証明機関のルート証明書と発行証明機関の証明書をデバイスのキーストアにインポートします。
- ベンダーのスマートカードミドルウェアをインストールします。

- Windows用Citrix Workspaceアプリをインストールして構成します。その際、グループポリシー管理コンソールを使用してicaclient.admをインポートし、スマートカード認証を有効にしてください。

ステップ8. 展開をテストします。テストユーザーのスマートカードを使用して仮想デスクトップを起動し、展開が正しく構成されていることを確認します。可能なすべてのアクセスメカニズム（例：Internet ExplorerおよびCitrix Workspaceアプリを介したデスクトップへのアクセス）をテストします。

スマートカードリーダーの挿入回数を追跡する

スマートカードのリモート処理を使用すると、SCardGetStatusChange関数を使用して、スマートカードがリーダーに挿入または取り外された回数を追跡できます。この関数は、監視するリーダーごとに1つずつ、SCARD_READERSTATEデータ構造の配列を更新します。各SCARD_READERSTATEのdwEventStateフィールドの上位ワード（16ビット）には、リーダーカウントが含まれています。詳細については、Microsoftの記事「SCardGetStatusChangeA function」および「SCARD_READERSTATEA structure」を参照してください。

「**リーダー挿入回数レポート**」設定は、デフォルトで無効になっています。追跡を有効にするには、次のレジストリキーを追加します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

名前: EnableReaderInsertCountReporting

種類: DWORD

値: ゼロ以外の任意の値

セッションが切断されると、カウントはゼロにリセットされます。

「**リーダー挿入回数レポート**」は、サードパーティのスマートカードミドルウェアと互換性があります。

スマートカードの展開

この製品バージョンおよびこのバージョンを含む混在環境では、以下の種類のスマートカード展開がサポートされています。その他の構成も動作する可能性がありますが、サポートされていません。

タイプ	STOREFRONT™ 接続
ローカルのドメイン参加済みコンピューター	直接接続
ドメイン参加済みコンピューターからのリモートアクセス	Citrix Gateway 経由で接続
ドメインに参加していないコンピューター	直接接続
ドメインに参加していないコンピューターからのリモートアクセス	Citrix Gateway経由で接続
Desktop Applianceサイトにアクセスするドメインに参加していないコンピューターおよびシンクライアント	Desktop Applianceサイト経由で接続
XenApp® Services URLを介してStoreFrontにアクセスするドメイン参加済みコンピューターおよびシンクライアント	XenApp Services URL を介して接続

展開タイプは、スマートカードリーダーが接続されているユーザーデバイスの特性によって定義されます。

- デバイスがドメイン参加済みか、非ドメイン参加済みか。
- デバイスがStoreFrontにどのように接続されているか。
- 仮想デスクトップとアプリケーションを表示するためにどのソフトウェアが使用されているか。

さらに、Microsoft WordやMicrosoft Excelなどのスマートカード対応アプリケーションをこれらの展開で使用できます。これらのアプリケーションを使用すると、ユーザーはドキュメントにデジタル署名したり、暗号化したりできます。

バイモーダル認証

これらの各展開において可能な場合、Receiverはスマートカードの使用とユーザー名およびパスワードの入力のいずれかを選択できるようにすることで、バイモーダル認証をサポートします。これは、スマートカードが使用できない場合（たとえば、ユーザーが自宅に忘れた場合やログオン証明書の有効期限が切れた場合）に役立ちます。

非ドメイン参加デバイスのユーザーはReceiver for Windowsに直接ログオンするため、ユーザーが明示的な認証にフォールバックできるようにすることができます。バイモーダル認証を構成する

と、ユーザーは最初にスマートカードとPINを使用してログオンするように求められますが、スマートカードに問題が発生した場合は明示的な認証を選択するオプションがあります。

Citrix Gatewayを展開する場合、ユーザーは自分のデバイスにログオンし、Receiver for WindowsによってCitrix Gatewayへの認証を求められます。これは、ドメイン参加済みデバイスと非ドメイン参加済みデバイスの両方に適用されます。ユーザーは、スマートカードとPIN、または明示的な資格情報のいずれかを使用してCitrix Gatewayにログオンできます。これにより、Citrix Gatewayログオンに対してバイモーダル認証をユーザーに提供できます。Citrix GatewayからStoreFrontへのパススルー認証を構成し、スマートカードユーザーの資格情報検証をCitrix Gatewayに委任することで、ユーザーはStoreFrontにサイレント認証されます。

複数のActive Directoryフォレストに関する考慮事項

Citrix環境では、スマートカードは単一のフォレスト内でサポートされます。フォレストをまたがるスマートカードログオンには、すべてのユーザーアカウントへの直接的な双方向フォレスト信頼が必要です。スマートカードを含むより複雑なマルチフォレスト展開（つまり、信頼が一方通行であるか、異なるタイプである場合）はサポートされていません。

リモートデスクトップを含むCitrix環境でスマートカードを使用できます。この機能は、ローカル（スマートカードが接続されているユーザーデバイス上）またはリモート（ユーザーデバイスが接続するリモートデスクトップ上）にインストールできます。

スマートカード取り外しポリシー

製品に設定されているスマートカード取り外しポリシーは、セッション中にリーダーからスマートカードを取り外した場合に何が起こるかを決定します。スマートカード取り外しポリシーは、Windowsオペレーティングシステムを介して構成および処理されます。

ポリシー設定	デスクトップの動作
何もしない	何もしない。
ワークステーションをロックする	デスクトップセッションが切断され、仮想デスクトップがロックされます。
強制ログオフ	ユーザーは強制的にログオフされます。ネットワーク接続が失われ、この設定が有効になっている場合、セッションがログオフされ、ユーザーはデータを失う可能性があります。
リモートターミナルサービスセッションの場合に切断する	セッションが切断され、仮想デスクトップがロックされます。

証明書失効チェック

証明書失効チェックが有効になっており、ユーザーが無効な証明書を含むスマートカードをカードリーダーに挿入した場合、ユーザーは証明書に関連するデスクトップまたはアプリケーションを認証またはアクセスできません。たとえば、無効な証明書がメールの復号化に使用された場合、メールは暗号化されたままになります。認証に使用されるものなど、カード上の他の証明書がまだ有効な場合、それらの機能はアクティブなままになります。

展開例：ドメイン参加済みコンピューター

この展開では、Desktop Viewer を実行し、StoreFront に直接接続するドメイン参加済みユーザーデバイスを使用します。

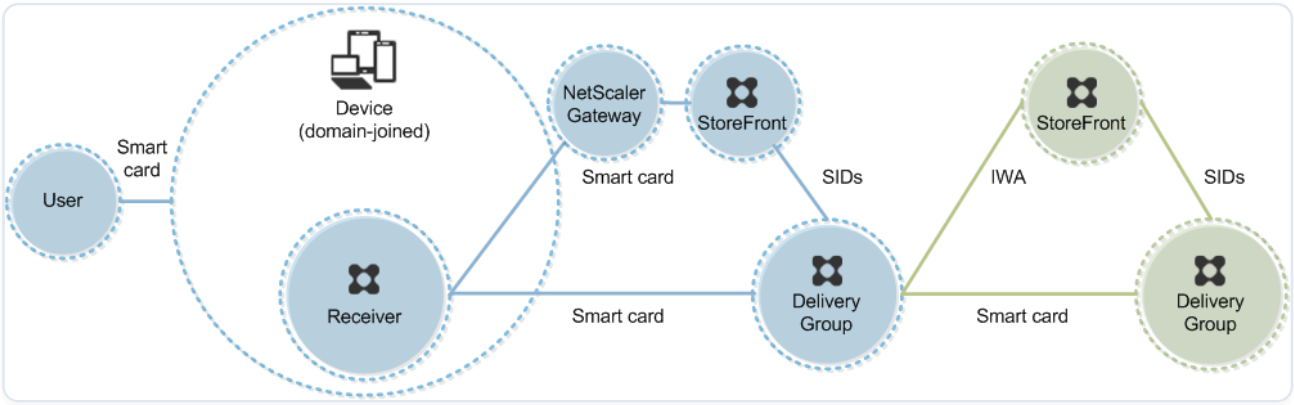
展開例：ドメイン参加済みコンピューター(/en-us/citrix-virtual-apps-desktops/2511/media/smartcard1_1.png)

ユーザーはスマートカードとPINを使用してデバイスにログオンします。Receiverは、統合Windows認証 (IWA) を使用してユーザーをStoreFrontサーバーに認証します。StoreFrontは、ユーザーセキュリティ識別子 (SID) をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、Receiverでシングルサインオン機能が構成されているため、PINの入力を再度求められることはありません。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに認証します。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: ドメイン参加済みコンピューターからのリモートアクセス

この展開には、Desktop Viewerを実行し、Citrix Gateway/Access Gatewayを介してStoreFrontに接続するドメイン参加済みのユーザーデバイスが含まれます。



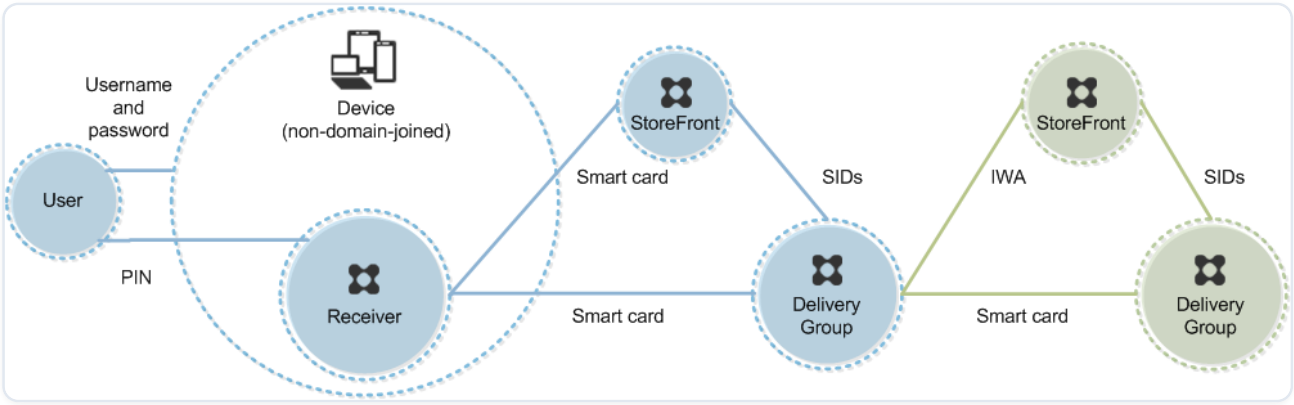
ユーザーはスマートカードとPINを使用してデバイスにログオンし、その後Citrix Gateway/Access Gatewayに再度ログオンします。この2回目のログオンは、Receiverがこの展開でバイモーダル認証を許可しているため、スマートカードとPIN、またはユーザー名とパスワードのいずれかで行うことができます。

ユーザーはStoreFrontに自動的にログオンし、StoreFrontはユーザーセキュリティ識別子 (SID) をCitrix Virtual Apps™またはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、Receiverでシングルサインオン機能が構成されているため、PINの入力を再度求められることはありません。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに認証します。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例：ドメインに参加していないコンピューター

この展開には、Desktop Viewerを実行し、StoreFrontに直接接続するドメインに参加していないユーザーデバイスが含まれます。



ユーザーはデバイスにログオンします。通常、ユーザーはユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンの資格情報はオプションです。この展開ではバイモーダル認証が可能であるため、Receiverはユーザーにスマートカードと PIN、またはユーザー名とパスワードのいずれかを要求します。その後、ReceiverはStoreFrontに認証します。

StoreFrontは、ユーザーセキュリティ識別子 (SID) をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、この展開ではシングルサインオン機能が利用できないため、PINの入力を再度求められます。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFront

サーバーに認証します。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例：ドメインに参加していないコンピューターからのリモートアクセス

この展開では、Desktop Viewer を実行し、StoreFront に直接接続するドメインに参加していないユーザーデバイスが使用されます。

展開例: ドメインに参加していないコンピューターからのリモートアクセス(/en-us/citrix-virtual-apps-desktops/2511/media/smartcard4_1.png)

ユーザーはデバイスにログオンします。通常、ユーザーはユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンの資格情報はオプションです。この展開ではバイモーダル認証が可能であるため、Receiver はユーザーにスマートカードとPIN、またはユーザー名とパスワードのいずれかを要求します。その後、Receiver はStoreFrontに対して認証を行います。

StoreFront はユーザーセキュリティ識別子 (SID) を Citrix Virtual Apps または Citrix Virtual Desktops に渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、この展開ではシングルサインオン機能が利用できないため、ユーザーは再度PINの入力を求められます。

この展開は、2台目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2台目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示された構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: ドメイン非参加コンピューター

この展開では、Desktop Lock を実行し、Desktop Appliance サイトを介してStoreFrontに接続する可能性のある、ドメインに参加していないユーザーデバイスが使用されます。

Desktop Lock は、Citrix Virtual Apps、Citrix Virtual Desktops、および VDI-in-a-Box とともにリリースされる別のコンポーネントです。これはDesktop Viewerの代替であり、主に再利用されたWindowsコンピューターとWindowsシンクライアント向けに設計されています。Desktop Lock は、これらのユーザーデバイスのWindowsシェルとタスクマネージャーを置き換え、ユーザーが基盤となるデバイスにアクセスするのを防ぎます。Desktop Lock を使用すると、ユーザーは Windows Server MachineデスクトップとWindows Desktop Machineデスクトップにアクセスできます。Desktop Lock のインストールはオプションです。

ユーザーはデバイスにログオンします。通常、ユーザーはユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンの資格情報はオプションです。この展開ではバイモーダル認証が可能であるため、Receiverはユーザーにスマートカードと PIN、またはユーザー名とパスワードのいずれかを要求します。その後、ReceiverはStorefrontに対して認証を行います。

ユーザーはスマートカードを使用してデバイスにログオンします。デバイスでDesktop Lockが実行されている場合、デバイスはキオスクモードで実行されているInternet Explorerを介してDesktop Applianceサイトを起動するように構成されます。サイト上のActiveXコントロールはユーザーにPINを要求し、それをStoreFrontに送信します。StoreFrontはユーザーセキュリティ識別子 (SID) をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。割り当てられたデスクトップグループのアルファベット順リストで最初に利用可能なデスクトップが起動します。

この展開は、2台目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2台目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示された構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: ドメイン非参加コンピューターからのリモートアクセス

この展開では、Desktop Lock を実行し、XenApp Services URLを介してStoreFrontに接続するドメインに参加しているユーザーデバイスが使用されます。

Desktop Lock は、Citrix Virtual Apps、Citrix Virtual Desktops、および VDI-in-a-Box とともにリリースされる別のコンポーネントです。これはDesktop Viewerの代替であり、主に再利用されたWindowsコンピューターとWindowsシンクライアント向けに設計されています。Desktop Lockは、これらのユーザーデバイスのWindowsシェルとタスクマネージャーを置き換え、ユーザーが基盤となるデバイスにアクセスするのを防ぎます。Desktop Lock を使用すると、ユーザーはWindows Server MachineデスクトップとWindows Desktop Machineデスクトップにアクセスできます。Desktop Lock のインストールはオプションです。

ユーザーがデバイスにログオンします。通常、ユーザーはユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンの資格情報はオプションです。この展開ではバイモーダル認証が可能なため、Receiverはスマートカードと PIN、またはユーザー名とパスワードのいずれかをユーザーに要求します。その後、ReceiverはStorefrontに対して認証を行います。

A user logs on to a device using a smart card and PIN. If Desktop Lock is running on the device, it authenticates the user to a Storefront server using Integrated Windows Authentication (IWA).

StoreFront passes the user security identifiers (SIDs) to Citrix Virtual Apps or Citrix Virtual Desktops. When the user starts a virtual desktop, the user is not prompted for a PIN again because the single sign-on feature is configured on Receiver.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

スマートカードによるパススルー認証とシングルサインオン

パススルー認証

スマートカードによる仮想デスクトップへのパススルー認証は、Windows 10、Windows 8、および Windows 7 SP1 Enterprise および Professional Edition を実行しているユーザーデバイスでサポートされています。

スマートカードによるホスト型アプリケーションへのパススルー認証は、Windows Server 2012 および Windows Server 2008 R2 SP1 を実行しているサーバーでサポートされています。

スマートカードホスト型アプリケーションでパススルー認証を使用するには、サイトの認証方法として「スマートカードによるパススルー」を構成する際に、Kerberos の使用を有効にしてください。

注：スマートカードによるパススルー認証の利用可能性は、以下を含む（ただしこれらに限定されない）多くの要因に依存します。

- パススルー認証に関する組織のセキュリティポリシー。
- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアのPINキャッシュポリシー。

スマートカードによるパススルー認証は、Citrix StoreFront で構成されます。詳細については、StoreFront のドキュメントを参照してください。

シングルサインオン

シングルサインオンは、仮想デスクトップおよびアプリケーションの起動時にパススルー認証を実装する Citrix の機能です。この機能は、ドメイン参加済み、StoreFront への直接接続、およびドメイン参加済み、NetScaler 経由の StoreFront へのスマートカード展開で使用でき、ユーザーが

PIN を入力する回数を減らすことができます。これらの展開タイプでシングルサインオンを使用するには、StoreFront サーバーにある default.ica ファイルで以下のパラメーターを編集します。

- ドメイン参加済み、StoreFront への直接接続スマートカード展開 — DisableCtrlAltDel を Off に設定
- ドメイン参加済み、NetScaler 経由の StoreFront へのスマートカード展開 — UseLocalUserAndPassword を On に設定

これらのパラメーターの設定に関する詳細な手順については、StoreFrontまたはCitrix Gatewayのドキュメントを参照してください。

シングルサインオン機能の可用性は、以下を含むがこれに限定されない多くの要因に依存します。

- シングルサインオンに関する組織のセキュリティポリシー。
- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアのPINキャッシュポリシー。

注:

ユーザーがスマートカードリーダーが接続されたマシン上のVirtual Delivery Agent (VDA) にログオンすると、スマートカードやパスワードなど、以前に成功した認証モードを表すWindowsタイルが表示されることがあります。その結果、シングルサインオンが有効になっている場合、シングルサインオンタイルが表示されることがあります。ログオンするには、シングルサインオンタイルは機能しないため、ユーザーは**ユーザーの切り替え**を選択して別のタイルを選択する必要があります。

Delivery Controller で TLS を有効にする

デフォルトでは、HTTP と HTTPS の両方が有効になっています。HTTPS は、サーバーの FQDN を共通名として使用する自己署名証明書を使用しますが、これは StoreFront™ や Web ブラウザでは信頼されません。

delivery controller™ で TLS を有効にするには、次の操作を行う必要があります。

- すべての Delivery Controller でサーバー証明書を取得、インストール、および登録します。詳細については、「証明書のリクエストとインストール」を参照してください。

- TLS 証明書を使用してポートを構成します。詳細については、「証明書のインストール」を参照してください。
- モニターサービスで HTTPS を有効にする。
- HTTP を無効にして HTTPS トラフィックを強制します。詳細については、「HTTPS トラフィックのみを強制する」を参照してください。
- オプションで、Controller が HTTP および HTTPS トラフィックをリッスンするために使用するポートを変更できます。詳細については、「HTTP または HTTPS ポートの変更」を参照してください。

証明書のリクエストとインストール

TLS を使用するには、共通名またはサブジェクトの別名がサーバーの FQDN と一致する証明書をインストールする必要があります。delivery controller の前にロードバランサーを使用している場合は、サーバーとロードバランサーの両方の FQDN をサブジェクトの別名として含めます。詳細については、「証明書」を参照してください。StoreFront が delivery controller に接続するには、RSA デジタル署名アルゴリズムを使用する必要があります。StoreFront は ECDSA アルゴリズムを使用する証明書をサポートしていません。

SSL/TLS リスナーポートの構成

Web Studio および Director の一部としてインストールされている IIS Windows コンポーネントが同じサーバーにインストールされている場合は、IIS を使用して TLS を構成できます。詳細については、「Web Studio および Director で TLS を有効にする」を参照してください。それ以外の場合は、PowerShell を使用して証明書を構成するには、次の手順を実行します。

1. 既存の証明書がバインドされているかを確認するには、コマンドプロンプトを開いて `netsh http show sslcert` を実行します。

   ```
   netsh http show sslcert
   ```

2. 既存のバインドがある場合は、それを削除します。

   ```
   netsh http delete sslcert ipport=0.0.0.0:443
   ```

   既存のバインディングで指定されていた場合は、`0.0.0.0:443` を特定の IP アドレスとポートに置き換えます。

3. 以前にインストールした証明書のサムプリントを見つけます。サムプリントを表示するには、**コンピューター証明書の管理**を開き、証明書を参照して開き、**詳細**タブに移動します。

サムプリントを示す証明書のプロパティのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2511/media/certificate-thumbprint.png)

または、PowerShellを使用することもできます。たとえば、次のスクリプトは、共通名がサーバーのホスト名と一致する証明書を検索し、サムプリントを出力します。

```
$HostName =
([System.Net.Dns]::GetHostByName(($env:computerName))).Hostname

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.Subject -match ("CN=" + $HostName)}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $
($Thumbprint)" -Foreground Yellow
```

証明書の共通名がホスト名と一致しない場合、これは失敗します。ホスト名に対して複数の証明書がある場合、これは連結された複数のサムプリントを返し、適切なサムプリントを選択する必要があります。

次の例では、フレンドリ名で証明書を検索します。

```
$friendlyName = "My certificate name"

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.FriendlyName -eq $friendlyNam}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $friendlyName: $
($Thumbprint)" -Foreground Yellow
```

指定されたフレンドリ名を持つ証明書が複数ある場合、これは連結された複数のサムプリントを返し、適切なサムプリントを選択する必要があります。

4. 証明書をポートにバインドするには、`netsh http add sslcert`コマンドを使用します。

```
netsh http add sslcert ipport=[IP address]:443 certhash=[certificate
hash] appid=[application GUID] disablelegacytls=enable
```

- `ipport`: IPアドレスとポート。0.0.0.0:443を使用すると、すべてのIPアドレスに適用されます。代わりに特定のIPアドレスを指定することもできます。
- `certhash`: 前のステップで特定した証明書のサムプリント。

- `appid`: シトリックス ブローカー サービスの GUID。

  > **注:**
  >
  > 証明書を更新または再バインドする際は、任意のGUIDではなく、Broker Serviceに関連付けられた特定の`appid`を使用してください。 Citrix Broker Serviceの正しい`appid`を見つけるには:

  a. 管理者としてPowerShellコマンドウィンドウを開き、次のコマンドを実行します。

  ```
  Get-WmiObject -Class Win32_Product | Select-String -Pattern
  "broker"
  ```

  b. 出力でCitrix Broker ServiceのIdentifyingNumber (GUID) を見つけます（例：`{D333C884-187F-447C-8C67-463F33989C8F}`）。このGUIDを`appid`パラメーターに使用します。

- `disablelegacytls=enable`: レガシーバージョンのTLSを無効にします。このパラメーターはWindows 2022以降で利用可能です。Windows 2022ではTLS 1.0と1.1を無効にします。Windows 2025では、TLS 1.0と1.1がデフォルトで無効になっているため、これは不要です。

例えば、すべてのIPアドレスで、サムプリント`bc96f958848639fd101a793b87915d5f2829b0b6`の証明書をポート`443`にバインドするには、次のコマンドを実行します。

```
netsh http add sslcert ipport=0.0.0.0:443
certhash=bc96f958848639fd101a793b87915d5f2829b0b6 appid={91fe7386-
e0c2-471b-a252-1e0a805febac} disablelegacytls=enable
```

HTTPSが有効になったら、StoreFront展開 とNetScaler Gatewayを構成して、デリバリーコントローラーへの接続にHTTPではなくHTTPSを使用するようにします。

HTTPS 用のモニターサービス OData API を構成する

モニターサービスは、Citrix® およびサードパーティアプリケーションがデータを照会できるように、OData v3 および v4 API を提供します。Director は OData API V3 を使用して監視サービスに接続します。HTTPS 用のモニター OData API を構成するには、次の手順を実行します。

1. 次のPowerShellを実行します。

```
$serviceGroup = Get-ConfigRegisteredServiceInstance -ServiceType
Monitor | Select -First 1 ServiceGroupUid

Remove-ConfigServiceGroup -ServiceGroupUid
$serviceGroup.ServiceGroupUid

& 'C:\Program Files\Citrix\Monitor\Service\citrix.monitor.exe'
-ConfigureFirewall -RequireODataTls –OdataPort 443 -RequireODataSdkTls
–OdataSdkPort 443

get-MonitorServiceInstance | register-ConfigServiceInstance

Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-
MonitorServiceGroupMembership
```

2. テキストエディターでファイル `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` を開きます。要素 `<add key="owin:baseAddress" value="http://localhost/citrix/monitor/odata/v4" />` を見つけて、`<add key="owin:baseAddress" value="https://localhost/citrix/monitor/odata/v4" />` に変更します。

暗号スイートを構成する

暗号スイートの順序リストには、`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` または `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` の暗号スイート（またはその両方）を含める必要があります。また、これらの暗号スイートは、`TLS_DHE_` の暗号スイートよりも前に配置する必要があります。

1. Microsoft グループポリシーエディターを使用して、**コンピューターの構成 > 管理用テンプレート > ネットワーク > SSL 構成設定** に移動します。
2. ポリシー「SSL 暗号スイートの順序」を編集します。デフォルトでは、このポリシーは「未構成」に設定されています。このポリシーを「有効」に設定します。
3. スイートを正しい順序に並べ替えます。使用しない暗号スイートは削除します。

`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` または `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` が、`TLS_DHE_` の暗号スイートよりも前に配置されていることを確認してください。

Microsoft Learn で、TLS 暗号スイートの順序の構成 も参照してください。

HTTPS トラフィックのみを強制する

XML Service を構成して HTTP トラフィックを無視することをお勧めします。

1. `regedit` を実行します
2. `HKLM\Software\Citrix\DesktopServer\` を開きます
3. `XmlServicesEnableNonSsl` という名前の新しい DWORD 値を作成し、0 に設定します。
4. ブローカーサービスを再起動します。

HTTPS トラフィックを無視するために作成できる対応するレジストリ DWORD 値 `XmlServicesEnableSsl` があります。これが 0 に設定されていないことを確認してください。

HTTP または HTTPS ポートを変更する

デフォルトでは、Controller 上の XML サービスは、HTTP トラフィックにはポート 80 を、HTTPS トラフィックにはポート 443 をリッスンします。デフォルト以外のポートを使用できますが、Controller を信頼できないネットワークに公開することによるセキュリティリスクに注意してください。デフォルトを変更するよりも、スタンドアロンの StoreFront サーバーを展開する方が望ましいです。

Controller で使用されるデフォルトの HTTP または HTTPS ポートを変更するには、Studio から次のコマンドを実行します:

```
BrokerService.exe -StoreFrontPort <http-port> -StoreFrontTlsPort <https-port>
```

ここで:

- `<http-port>` は HTTP トラフィックのポート番号です
- `<https-port>` は HTTPS トラフィックのポート番号です。

> **注:**
>
> ポートを変更した後、Studio はライセンスの互換性とアップグレードに関するメッセージを表示する場合があります。この問題を解決するには、次の PowerShell コマンドレットシーケンスを使用してサービスインスタンスを再登録します:

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS
|

Unregister-ConfigRegisteredServiceInstance

Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |

Register-ConfigServiceInstance
```

Web StudioおよびDirectorでTLSを有効にする

HTTPSを有効にすることで、Web StudioおよびDirectorへの接続を保護するために常にTLSを使用することをお勧めします。この記事では、Web StudioおよびDirectorを構成して、信頼された証明書を使用し、HTTPS経由で安全なアクセスを確保する方法について説明します。

デフォルトの動作

Web Studioをインストールすると、インストーラーは自己署名証明書を作成し、現在のサーバーのポート443にバインドします。ローカルサーバー上のWebブラウザーからHTTPS経由でWeb StudioおよびDirectorにアクセスできます。

ただし、別のマシンからHTTPS経由でWeb StudioまたはDirectorにアクセスしようとすると、ブラウザーは証明書を信頼しないため、セキュリティエラーを表示します。

> **注：**
>
> Web StudioなしでDirectorをインストールした場合、インストーラーは自己署名証明書を作成しません。

HTTPS経由で安全なアクセスを有効にする

Web Studioサーバー以外のマシンからHTTPS経由でWeb StudioまたはDirectorへのアクセスを許可するには、次の手順に従います。

1. 信頼された証明書を作成またはインポートする。
2. IISで証明書をポート443にバインドする。
3. (オプション) HTTP Strict Transport Security (HSTS) を有効にする。

4. Web Studioがプロキシとして構成されていない場合（クライアントマシンがWeb StudioとDelivery Controllerの両方に接続する場合）、Delivery ControllerでTLSを有効にする。

> **注：**
>
> 自己署名証明書の使用は、各マシンで手動構成が必要なため推奨されません。詳細については、自己署名証明書を使用するを参照してください。

信頼された証明書を作成またはインポートする

サーバーに接続するマシンによって信頼されている、エンタープライズまたはパブリック証明機関からの証明書を使用することをお勧めします。

詳細については、新しい証明書の作成 および 既存の証明書のインポート を参照してください。証明書の共通名またはサブジェクトの別名は、ユーザーがWeb StudioまたはDirectorに接続するために使用するFQDNと一致している必要があります。サーバーの前にロードバランサーが展開されている場合は、ロードバランサーのFQDNを使用してください。

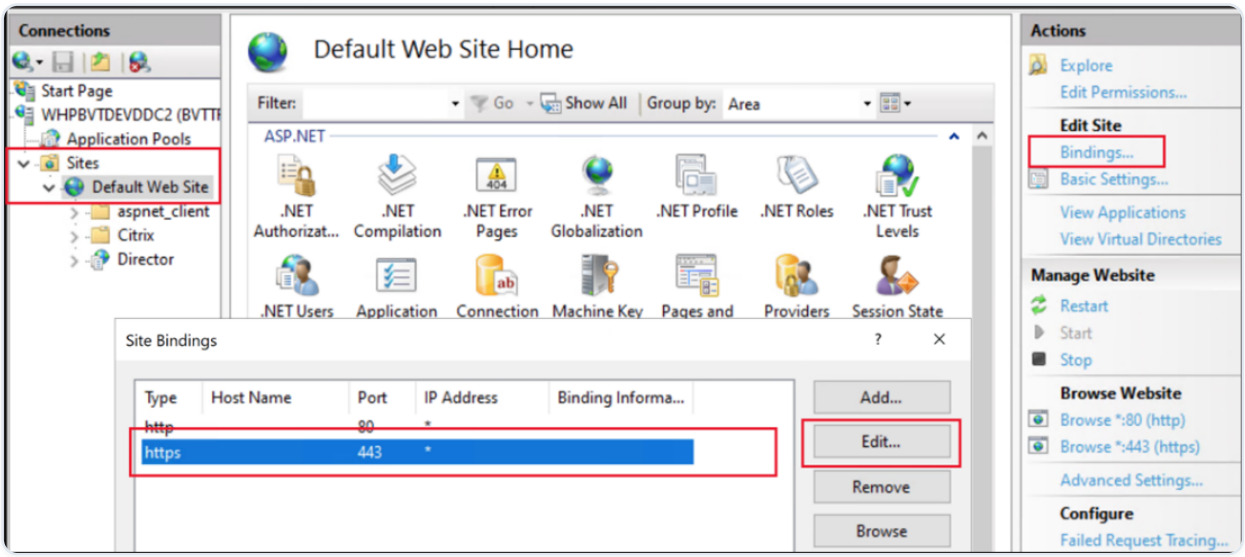
証明書をポート443にバインドする

信頼された証明書を作成またはインポートした後、IISでポート `443` にバインドします。これは、インストール前またはインストール後に行うことができます。ポート `443` の証明書バインドがすでに構成されている場合、インストーラーは変更を行いません。

> **注:**
>
> デフォルトでは、Web StudioとDirectorはセキュアなHTTPSアクセスにポート443を使用します。必要に応じてポート番号を変更できます。詳細については、デフォルトのポート番号の変更 を参照してください。

> 証明書をポート `443` にバインドするには、次の手順に従います。

1. 管理者としてサーバーにログオンします。
2. IISマネージャーを開き、**サイト > 既定のWebサイト > バインド** に移動します。
3. 種類が **https** の既存のバインドがある場合は、それを選択して **編集...** をクリックします。**https** バインドがない場合は、**追加** をクリックします。



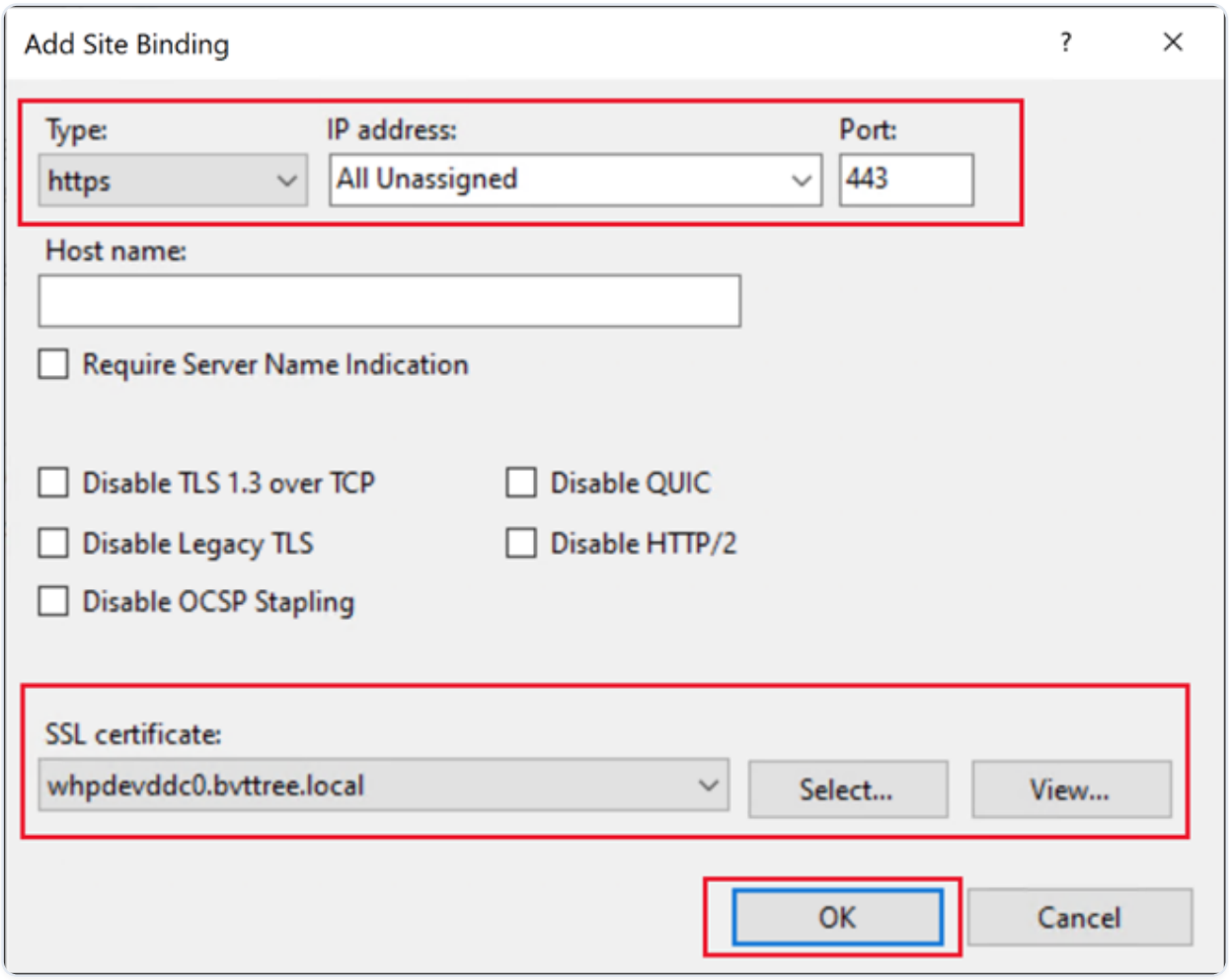
4. サイトバインドを作成または編集します。

   a. 新しいバインドの場合は、種類を **https** に、ポートを `443` に設定します。

   b. 適切なSSL証明書を選択します。

   c. Windows Server 2022以降では、必要に応じて**レガシーTLSを無効にする**を選択して、ユーザーが最新のTLSバージョンのみを使用して接続できるようにします。

   d. **OK**をクリックします。



または、PowerShellを使用して証明書を変更することもできます。たとえば、次のスクリプトは、指定された共通名を持つ証明書を検索し、それをすべてのIPアドレス、ポート443にバインドし、レガシーTLSバージョンを無効にします。

```
$certSName = 'CN=whpdevddc0.bvttree.local'  # The subject name of the
certificate

$certificate = Get-ChildItem -Path Cert:\LocalMachine\My\ | ? {$_.Subject
-eq $certSName}

netsh http add sslcert ipport=0.0.0.0:443 certhash=$
($certificate.Thumbprint) certstorename=My appid="{91fe7386-e0c2-471b-
a252-1e0a805febac}" disablelegacytls=enable
```

`appid` は、どのアプリケーションが証明書を追加したかを識別するために使用できる任意のGUIDであることに注意してください。

自己署名証明書を使用する

既存の自己署名証明書を使用できますが、サーバーにアクセスする各マシンを手動で構成する必要があるため、推奨されません。

Web Studio に接続する必要があるマシンに自己署名証明書をインストールするには、次の手順を実行します。

1. Web StudioおよびDelivery Controllerサーバーから既存の自己署名証明書をエクスポートします。
2. サーバーにアクセスする必要があるマシンの**信頼されたルート証明書**ストアに証明書をインポートします。

(オプション) HTTP Strict Transport Security (HSTS) を有効にする

HTTP Strict Transport Security (HSTS) は、サイトにアクセスする際にHTTPSのみを使用するようWebブラウザに指示します。ユーザーがHTTPを使用してURLにアクセスしようとすると、ブラウザは自動的にHTTPSに切り替わります。この設定により、クライアント側とサーバー側の両方で安全な接続検証が保証されます。ブラウザは、設定された期間、この検証を維持します。

Windows Server 2019 以降では、IIS で HSTS を構成できます。

1. **インターネット インフォメーション サービス (IIS) マネージャー**を開きます。
2. **既定のWebサイト** (または適切なWebサイト) を選択します。
3. 右側の**操作**ペインで、**HSTS...**を選択します。
4. **有効**を選択し、最大有効期間を入力します。例として、1年間の場合は31536000と入力します。
5. **HTTPをHTTPSにリダイレクト**を選択します。

   > **注：**
   >
   > Web Studioは、Studio Webサイトにアクセスする際にHTTPをHTTPSにリダイレクトする**URL書き換え**ルールを自動的に構成します。ただし、このオプションはDirectorおよびIISサイト上の他のすべてのアプリケーションにも適用されます。

6. **OK**をクリックします。

   HSTS設定のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2511/media/iis-hsts.png)

(オプション) デフォルトのポート番号を変更する

デフォルトでは、Web StudioとDirectorはセキュアなHTTPSアクセスにポート443を使用します。このポート番号を変更するには、`Default Web Site`で目的のポートのサイトバインディングを作成するために、以下の手順に従います。

手順:

1. Web Studioをホストしているサーバーで、**インターネットインフォメーションサービス (IIS) マネージャー**を開きます。
2. **接続**ペインで、サーバーノードを展開し、**サイト**の下にある**既定のWebサイト**を選択します。
3. 右側の**操作**ペインで、**バインディング**をクリックします。
4. **サイトバインディング**ウィンドウで、**追加**をクリックします。
5. サイトバインディングの追加ウィンドウで、新しいバインディングに対して以下を設定します。
    a. **種類**: **https** を選択します。
    b. **IPアドレス**: 適切なIPアドレスを選択するか、該当する場合は「すべて未割り当て」のままにします。
    c. **ポート**: 目的のポート番号を入力します (例: 444)。
    d. **SSL証明書**: セキュアな通信のために適切なSSL証明書を選択します。

> **注:**
>
> Delivery Controller™ と Web Studio が別々のマシンにインストールされており、サーバーに他のサービスや Web サイトが展開されていない場合は、ポート 443 を削除できます。そうでない場合は、オーケストレーションサービスや他の FMA サービスとの通信問題を避けるために、このポートを維持してください。

6. 「**OK**」をクリックしてバインディングを保存し、「**サイトバインディング**」ウィンドウを閉じます。
7. **IIS マネージャー** で、サーバーノードをクリックし、**操作** ペインで **再起動** をクリックして新しいバインディングを適用します。

(オプション) HTTPS リダイレクトを無効にする

Web Studio をインストールすると、デフォルトで、すべての HTTP アクセスは HTTPS に自動的にリダイレクトされます。このリダイレクトを無効にして HTTP アクセスを許可することも可能です。このアプローチは、HTTP アクセスをブロックするための他の対策を講じている場合にのみ推奨されます。Web Studio の前に TLS 終端ロードバランサーがある場合でも、ロードバランサーと Web Studio の間で HTTPS を使用することをお勧めします。

1. Web Studio サーバーにログオンします。
2. **インターネット インフォメーション サービス (IIS) マネージャー** を開き、*Server_name* **> サイト > 既定の Web サイト > URL 書き換え** に移動します。
3. 次のスクリーンショットに示すように、**https へのリダイレクト** の **受信規則** を無効にします。

   HTTPS リダイレクトを無効にする(/en-us/citrix-virtual-apps-desktops/2511/media/studio-disable-https-redirect.png)

IIS で HSTS を有効にしている場合は、**Http から Https へのリダイレクト** もクリアする必要があります。

VDA で TLS / DTLS を有効にする

Citrix Workspace™ アプリと Virtual Delivery Agent (VDA) 間の TLS 接続を有効にするには、次のタスクを完了します。

- VDA に証明書をインストールします。詳細については、「証明書の要求とインストール」を参照してください。
- VDA がインストールされているマシンで TLS を構成します。(便宜上、VDA がインストールされているマシンは、以降「VDA」と呼びます。) Citrix が提供する PowerShell スクリプトを使用して TLS/DTLS を構成することを強くお勧めします。詳細については、「PowerShell スクリプトを使用して VDA で TLS を構成する」を参照してください。ただし、TLS/DTLS を手動で構成する場合は、「VDA で TLS を手動で構成する」を参照してください。
- Studio で一連の PowerShell コマンドレットを実行して、VDA を含むデリバリーグループで TLS を構成します。詳細については、「デリバリーグループで TLS を構成する」を参照してください。

要件と考慮事項:

- コンポーネントのインストール、サイトの作成、マシンカタログの作成、およびデリバリーグループの作成を行った後で、デリバリーグループと VDA で TLS を構成します。

- デリバリーグループで TLS を構成するには、Controller アクセスルールを変更する権限が必要です。フル管理者にはこの権限があります。
- VDA で TLS を構成するには、VDA がインストールされているマシンで Windows 管理者である必要があります。
- Machine Creation Services™ または Provisioning Services によってプロビジョニングされたプールされた VDA では、再起動時に VDA マシンイメージがリセットされ、以前の TLS 設定が失われます。VDA が再起動されるたびに PowerShell スクリプトを実行して、TLS 設定を再構成してください。

デリバリーグループには、TLS が構成されている VDA と TLS が構成されていない VDA が混在することはできません。デリバリーグループの TLS を構成する前に、そのデリバリーグループ内のすべての VDA に対して TLS がすでに構成されていることを確認してください。

VDA で TLS を構成すると、インストールされている TLS 証明書のアクセス許可が変更され、ICA® Service に証明書の秘密キーへの読み取りアクセス権が付与され、ICA Service に次の情報が通知されます。

- TLS に使用する証明書ストア内の証明書。
- TLS 接続に使用する TCP ポート番号。

  Windows ファイアウォール (有効な場合) は、この TCP ポートでの受信接続を許可するように構成する必要があります。この構成は、PowerShell スクリプトを使用すると自動的に行われます。
- 許可するTLSプロトコルのバージョン。

  > **重要:**
  >
  > Citrixでは、TLS 1.2以降を使用することをお勧めします。SSLおよびそれ以前のバージョンのTLSは非推奨です。
  >
  > サポートされているTLSプロトコルバージョンには階層があります（低いものから高いものへ）：SSL 3.0、TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3。許可される最小バージョンを指定します。そのバージョンまたはそれより高いバージョンを使用するすべてのプロトコル接続が許可されます。

  たとえば、最小バージョンとしてTLS 1.1を指定した場合、TLS 1.1、TLS 1.2、TLS 1.3プロトコル接続が許可されます。最小バージョンとしてSSL 3.0を指定した場合、サポートされてい

るすべてのバージョンの接続が許可されます。最小バージョンとしてTLS 1.3を指定した場合、TLS 1.3接続のみが許可されます。

- 許可するTLS暗号スイート。

  暗号スイートは、接続に使用される暗号化を選択します。クライアントとVDAは、異なる暗号スイートのセットをサポートできます。クライアント（Citrix Workspaceアプリ）が接続し、サポートされているTLS暗号スイートのリストを送信すると、VDAはクライアントの暗号スイートの1つを、VDA自身の構成済み暗号スイートのリストにある暗号スイートの1つと照合し、接続を受け入れます。一致する暗号スイートがない場合、VDAは接続を拒否します。

  VDAは、3つの暗号スイートセット（コンプライアンスモードとも呼ばれます）をサポートしています：GOV（政府）、COM（商用）、およびALL。許容される暗号スイートは、Windows FIPSモードにも依存します。Windows FIPSモードの詳細については、`<http://support.microsoft.com/kb/811833>`を参照してください。次の表に、各セットの暗号スイートを示します。

暗号スイート	すべて	COM	GOV	すべて	COM	GOV
FIPSモード	オフ	オフ	オフ	オン	オン	オン
TLS_AES_256_GCM_SHA384	X		X	X		X
TLS_AES_128_GCM_SHA256	X			X		X
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	X		X	X		X
TLS_ECDHE_RSA_WITH	X		X	X		X

暗号スイート	すべて	COM	GOV	すべて	COM	GOV
_AES_256_CBC_SHA384						
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	X	X		X	X	

注:

VDAはDHE暗号スイート（例：TLS_DHE_RSA_WITH_AES_256_GCM_SHA384、TLS_DHE_RSA_WITH_AES_256_CBC_SHA、TLS_DHE_RSA_WITH_AES_128_GCM_SHA256、TLS_DHE_RSA_WITH_AES_128_CBC_SHA）をサポートしていません。Windowsによって選択された場合、接続は失敗します。

NetScaler Gatewayを使用している場合は、バックエンド通信の暗号スイートサポートに関する情報について、NetScalerのドキュメントを参照してください。TLS暗号スイートのサポートについては、「Citrix ADCアプライアンスで利用可能な暗号」を参照してください。DTLS暗号スイートのサポートについては、「DTLS暗号のサポート」を参照してください。

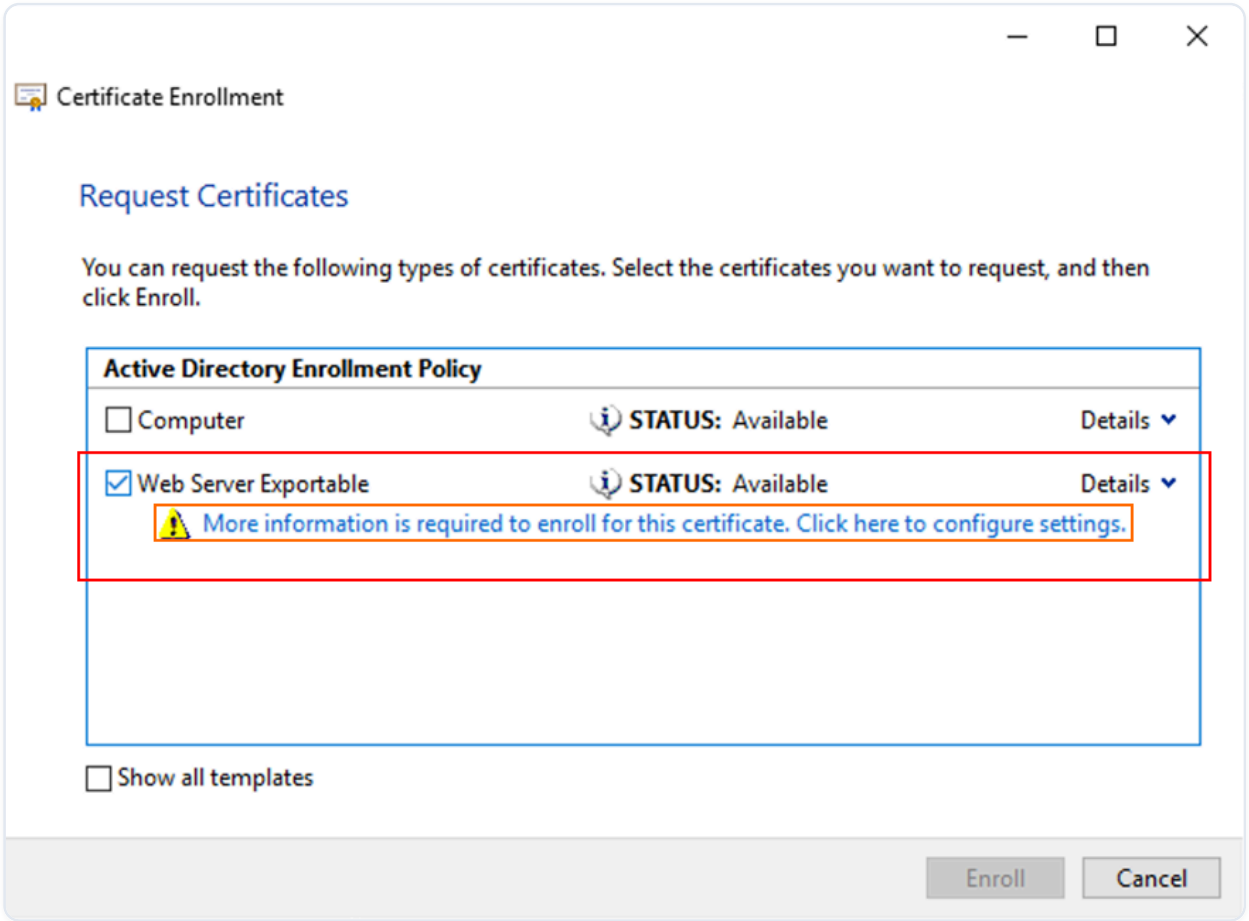
証明書の要求とインストール

TLSを使用するには、代替名にVDAのFQDNが含まれる証明書をインストールする必要があります。証明書は、VDAに直接接続する（Citrix Gateway経由ではない）すべてのクライアントから信頼されている必要があります。証明書を簡単に展開できない管理対象外のデバイスがVDAに接続できるようにするには、NetScaler® Gatewayの展開を検討してください。

Microsoft証明機関を使用して証明書を作成する

クライアントとVDAが信頼されたフォレストにあり、Microsoft証明機関がある場合、証明書MMCスナップインの証明書登録ウィザードから証明書を取得できます。

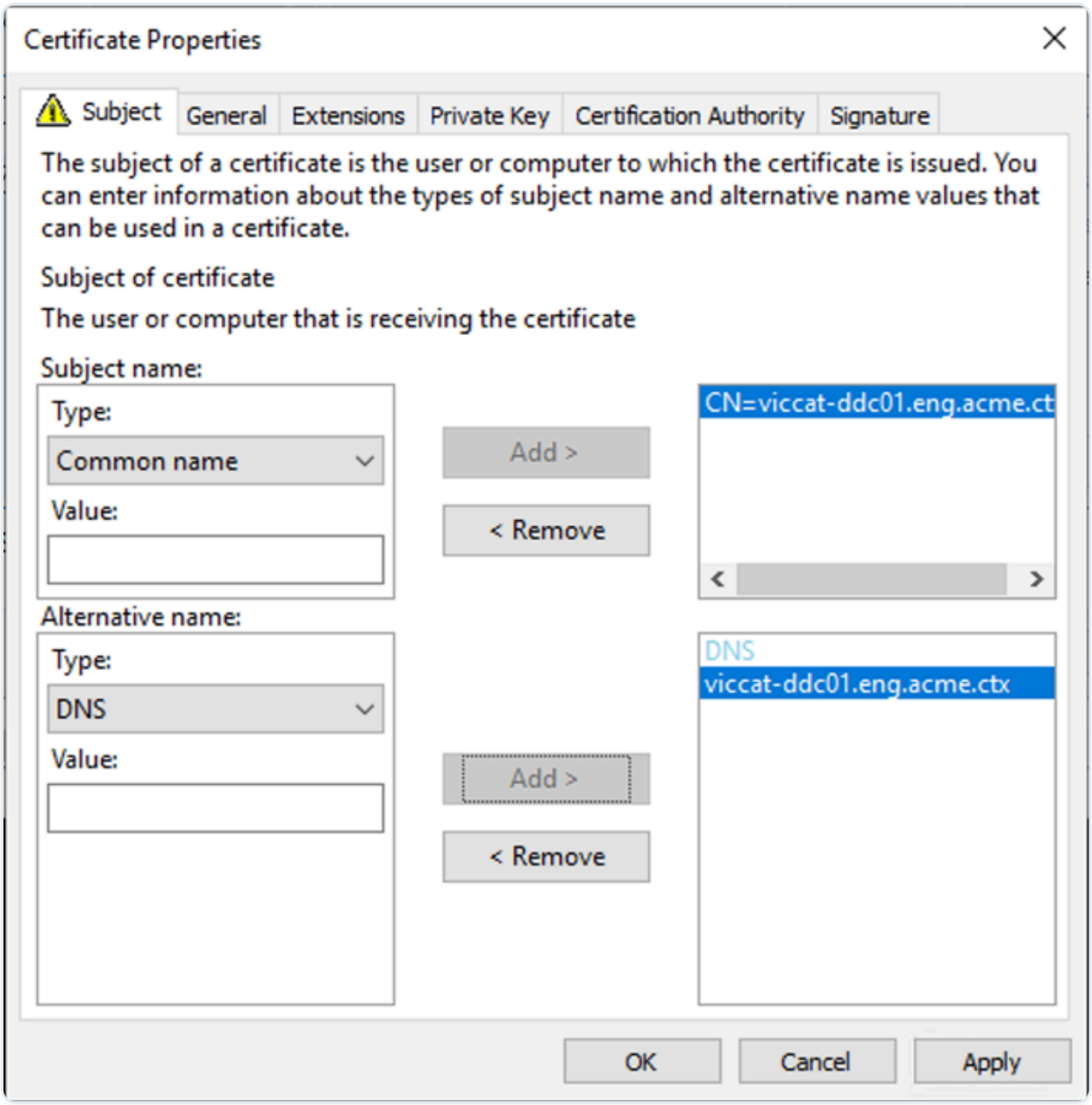
1. VDAで、MMCコンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、コンピューターアカウントを選択します。
2. **個人 > 証明書**を展開し、コンテキストメニューコマンド**すべてのタスク > 新しい証明書の要求**を使用します。
3. 開始するには**次へ**をクリックし、Active Directory登録から証明書を取得することを確認するために**次へ**をクリックします。
4. サーバー認証証明書のテンプレートを選択します。デフォルトのWindows **コンピューター**または**Webサーバー（エクスポート可能）**のいずれも使用できます。テンプレートが件名の値を自動的に提供するように設定されている場合は、**詳細を指定せずに登録**をクリックできます。



5. 証明書テンプレートの詳細を指定するには、**詳細**をクリックして、以下を構成します。

   サブジェクト名 — 種類として**共通名**を選択し、VDAのFQDNを追加します。

   代替名 — タイプ**DNS**を選択し、VDAのFQDNを追加します



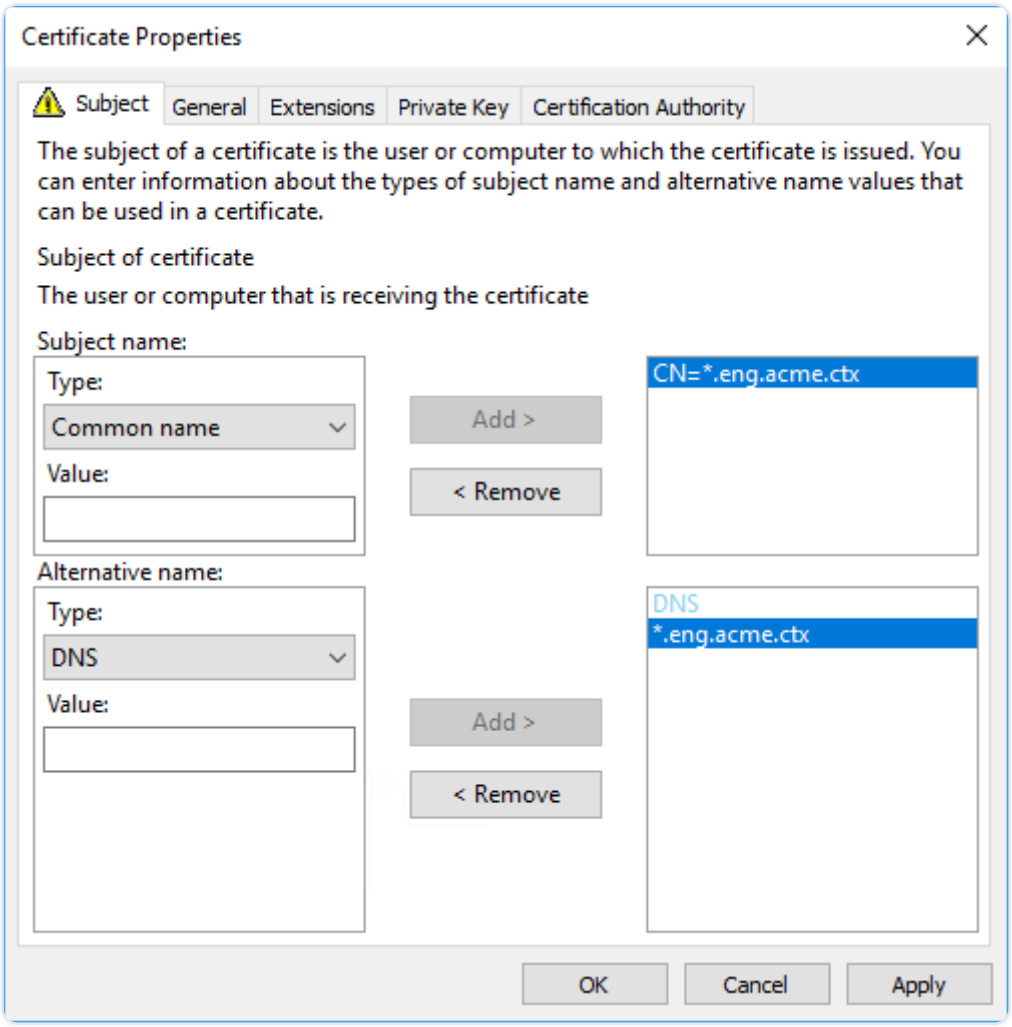
注:

Active Directory証明書サービス証明書自動登録を使用して、VDAへの証明書の発行と展開を自動化します。これについては、証明書の自動登録を有効にするで説明されています。

ワイルドカード証明書を使用すると、単一の証明書で複数のVDAを保護できます。

サブジェクト名 — タイプ**共通名**を選択し、VDAの*.primary.domainを入力します

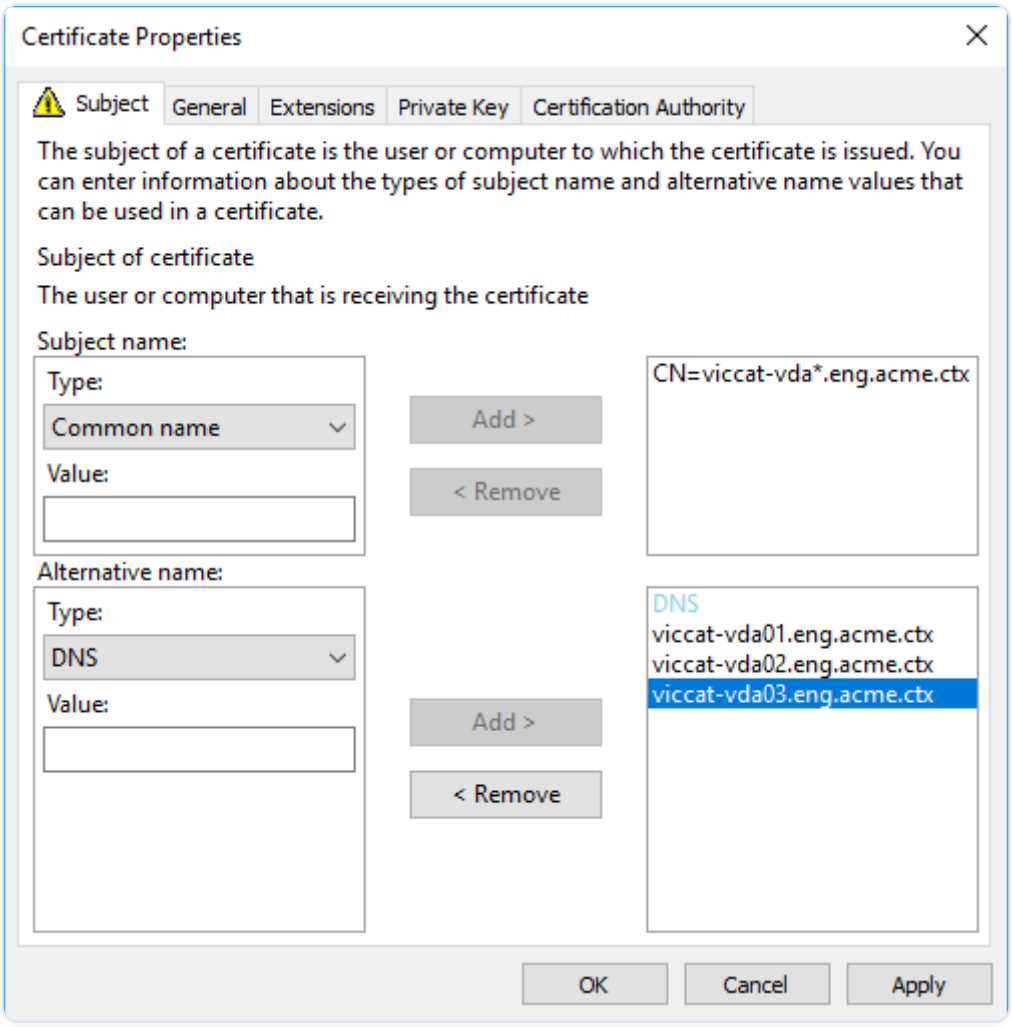
代替名 — タイプ**DNS**を選択し、VDAの*.primary.domainを追加します



SAN証明書を使用すると、単一の証明書で複数の特定のVDAを保護できます。

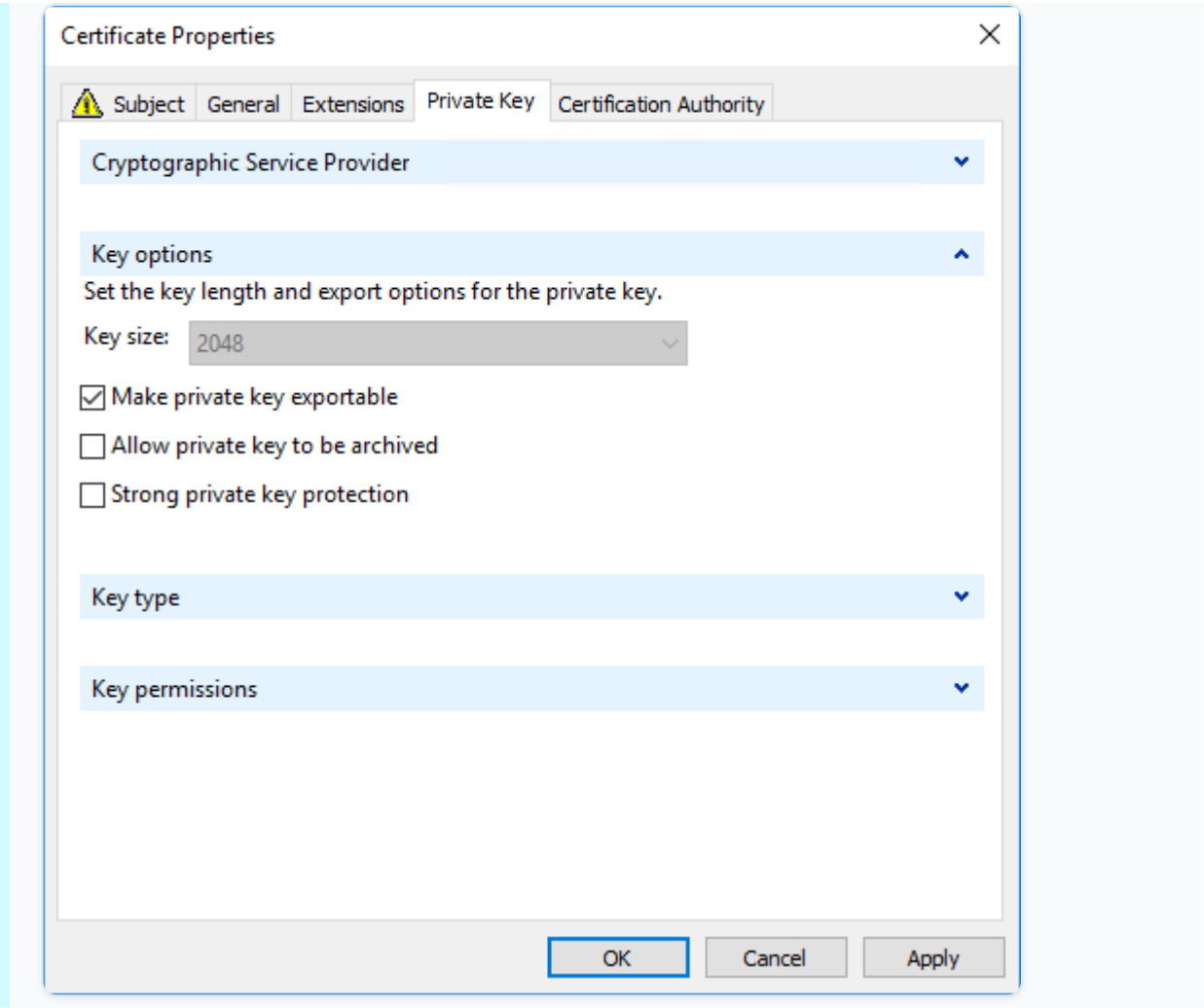
サブジェクト名 — タイプ **共通名** を選択し、証明書の使用状況を識別するのに役立つ文字列を入力します。

代替名 — タイプ**DNS**を選択し、各VDAのFQDNのエントリを追加します。最適なTLSネゴシエーションを確保するために、代替名の数を最小限に抑えてください。



注:

ワイルドカード証明書とSAN証明書の両方で、プライベートキーのタブで**秘密キーをエクスポート可能にする**が選択されている必要があります。



PowerShellスクリプトを使用してVDAでTLSを構成する

証明書ストアの［ローカルコンピューター］>［個人］>［証明書］領域にTLS証明書をインストールします。その場所に複数の証明書がある場合は、証明書のサムプリントをPowerShellスクリプトに指定します。

> **注:**
>
> XenAppおよびXenDesktop 7.15 LTSR以降、PowerShellスクリプトはVDAのFQDNに基づいて正しい証明書を検索します。VDAのFQDNに対して単一の証明書のみが存在する場合、サムプリントを指定する必要はありません。

Enable-VdaSSL.ps1スクリプトは、VDAでTLSリスナーを有効または無効にします。このスクリプトは、インストールメディアの*Support* > *Tools* > *SslSupport*フォルダーにあります。

TLSを有効にすると、DHE暗号スイートは無効になります。ECDHE暗号スイートは影響を受けません。

TLSを有効にすると、スクリプトは指定されたTCPポートの既存のWindowsファイアウォール規則をすべて無効にします。次に、ICAサービスがTLS TCPポートとUDPポートでのみ受信接続を受け入れることを許可する新しい規則を追加します。また、次のWindowsファイアウォール規則も無効にします。

- Citrix ICA（デフォルト：1494）
- Citrix CGP（デフォルト：2598）
- Citrix WebSocket（デフォルト：8008）

その結果、ユーザーはTLSまたはDTLSを使用してのみ接続できます。TLSまたはDTLSなしでは、ICA/HDX、セッションの信頼性を備えたICA/HDX、またはWebSocket経由のHDXを使用できません。

> **注:**
>
> DTLSは、UDPリアルタイムトランスポート経由のICA/HDXオーディオ、またはICA/HDX Framehawkではサポートされていません。
>
> 「ネットワークポート」を参照してください。(/ja-jp/tech-zone/build/tech-papers/citrix-communication-ports.html#citrix-virtual-apps-and-desktops).

このスクリプトには、以下の構文の説明と追加の例が含まれています。Notepad++などのツールを使用してこの情報を確認できます。

> **重要:**
>
> EnableまたはDisableパラメーターと、CertificateThumbPrintパラメーターを指定します。その他のパラメーターはオプションです。

構文

```
Enable-VdaSSL {-Enable | -Disable} -CertificateThumbPrint "<thumbprint>" [-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"\<suite>"]
```

パラメーター	説明
有効化	VDAにTLSリスナーをインストールして有効にします。このパラメーターまたはDisableパラメーターのいずれかが必要です。
無効化	VDA上のTLSリスナーを無効にします。このパラメーターまたはEnableパラメーターのいずれかが必要です。このパラメーターを指定した場合、他のパラメーターは無効になります。
証明書のサムプリント "<thumbprint>"	証明書ストア内のTLS証明書のサムプリント。引用符で囲みます。スクリプトは、指定されたサムプリントを使用して、使用する証明書を選択します。このパラメーターを省略すると、誤った証明書が選択されます。
SSLポート <port>	TLSポート。デフォルト: 443
SSL最小バージョン "<version>"	引用符で囲まれた最小TLSプロトコルバージョン。有効な値: `SSL_3.0`、`TLS_1.0` (デフォルト)、`TLS_1.1`、`TLS_1.2`、および `TLS_1.3`。`TLS_1.3` には Windows 11 または Windows Server 2022 以降が必要です。
SSLサイファースイート "<suite>"	引用符で囲まれたTLS暗号スイート。有効な値: 「GOV」、「COM」、および「ALL」(デフォルト)。

例

次のスクリプトは、TLSプロトコルバージョン値をインストールして有効にします。サムプリント (この例では「12345678987654321」として表されます) は、使用する証明書を選択するために使用されます。

```
Enable-VdaSSL -Enable -CertificateThumbPrint "12345678987654321"
```

次のスクリプトは、TLSリスナーをインストールして有効にし、TLSポート400、GOV暗号スイート、および最小TLS 1.2プロトコル値を指定します。サムプリント (この例では「12345678987654321」として表されます) は、使用する証明書を選択するために使用されます。

```
Enable-VdaSSL -Enable

-CertificateThumbPrint "12345678987654321"

-SSLPort 400 -SSLMinVersion "TLS_1.2"

-SSLCipherSuite "All"
```

次のスクリプトは、VDA上のTLSリスナーを無効にします。

```
Enable-VdaSSL -Disable
```

VDAでTLSを手動で構成する

VDAでTLSを手動で構成する場合、各VDAの適切なサービスに対して、TLS証明書の秘密キーへの一般的な読み取りアクセス権を付与します。WindowsシングルセッションOS用VDAの場合はNT SERVICE\PorticaService、WindowsマルチセッションOS用VDAの場合はNT SERVICE\TermService。VDAがインストールされているマシンで:

ステップ1。Microsoft管理コンソール (MMC) を起動します: > > 。

手順 2. MMCに証明書スナップインを追加します。

1. > を選択します。
2. を選択し、 をクリックします。
3. 「このスナップインは常に次の証明書を管理します:」というプロンプトが表示されたら、「コンピューターアカウント」を選択し、 をクリックします。
4. 「このスナップインで管理するコンピューターを選択してください」というプロンプトが表示されたら、「ローカルコンピューター」を選択し、 をクリックします。

手順 3。 > > で、証明書を右クリックし、 > を選択します。

手順 4。 アクセス制御リストエディターに「(FriendlyName) の秘密キーのアクセス許可」が表示されます。ここで (FriendlyName) は TLS 証明書の名前です。次のいずれかのサービスを追加し、読み取りアクセス権を付与します。

- WindowsシングルセッションOS用VDAの場合、「PORTICASERVICE」
- Windows Multi-session OS 用 VDA の場合、「TERMSERVICE」

手順 5。 インストールされている TLS 証明書をダブルクリックします。証明書のダイアログで、タブを選択し、一番下までスクロールします。 をクリックします。

手順 6。 regedit を実行し、HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd に移動します。

1. SSL Thumbprint キーを編集し、TLS 証明書の拇印の値をこのバイナリ値にコピーします。 ダイアログボックスの不明な項目（「0000」や特殊文字など）は無視しても問題ありません。
2. SSLEnabled キーを編集し、DWORD 値を 1 に変更します。（後で SSL を無効にするには、DWORD 値を 0 に変更します。）
3. デフォルト設定を変更する場合（オプション）は、同じレジストリパスで以下を使用します。

   SSLPort DWORD – SSL ポート番号。デフォルト: 443。

   SSLMinVersion DWORD – 1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.2, 5 = TLS 1.3。デフォルト: 2 (TLS 1.0)。

   SSLCipherSuite DWORD – 1 = GOV、2 = COM、3 = ALL。デフォルト: 3 (すべて)。

手順 7。 TLS の TCP および UDP ポートがデフォルトの 443 ではない場合、Windows ファイアウォールで開いていることを確認します。（Windows ファイアウォールで受信規則を作成する際は、そのプロパティで「接続を許可する」と「有効」のエントリが選択されていることを確認してください。）

手順 8。 他のアプリケーションやサービス（IIS など）が TLS の TCP ポートを使用していないことを確認します。

手順 9。 マルチセッション VDA の場合、変更を有効にするにはマシンを再起動します。（シングルセッション VDA マシンを再起動する必要はありません。）

ステップ 10. 接続の問題を回避するために、VDA でサポートされている暗号スイートが最も高い優先順位を持つように、Windows の暗号スイートの優先順位を変更します。

> **重要:**

> 以下に示すグループポリシーの変更は、システムを再起動した後にのみ有効になります。

> MCSまたはPVSでプロビジョニングされた非永続セッションホストを使用している場合は、これらの設定をマスターイメージに適用する必要があります。

オプション1:

グループポリシーエディターを使用して、 > > > > > に移動します。次の暗号スイートがリストの最上位にあることを確認してください。

```
TLS_AES_256_GCM_SHA384_P384

TLS_AES_256_GCM_SHA384_P256

TLS_AES_128_GCM_SHA256_P384

TLS_AES_128_GCM_SHA256_P256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

注:

TLS_AES_256_GCM_SHA384およびTLS_AES_128_GCM_SHA256は、Windows 11およびWindows Server 2022以降にのみ適用されます。古いオペレーティングシステムを使用している場合は、これらの暗号スイートをリストに含めないでください。

リストされている暗号スイートは、楕円曲線 P384 または P256 も指定しており、「curve25519」が選択されないようにします。FIPS モードは「curve25519」の使用を妨げません。

リストから暗号スイートを削除する必要はありません。これらの設定はシステム全体に適用されるため、暗号スイートを削除する場合は、セッションホストで実行されているアプリケーションやサービスによってそれらが必要とされないことを確認する必要があります。

オプション2:

グループポリシーエディターを使用して、 > > > > > に移動します。次の暗号スイートがリストの最上位にあることを確認してください。

```
TLS_AES_256_GCM_SHA384

TLS_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
```

注:

TLS_AES_256_GCM_SHA384およびTLS_AES_128_GCM_SHA256は、Windows 11およびWindows Server 2022以降にのみ適用されます。古いオペレーティングシステムを使用している場合は、これらの暗号スイートをリストに含めないでください。

リストから暗号スイートを削除する必要はありません。これらの設定はシステム全体に適用されるため、暗号スイートを削除する場合は、セッションホストで実行されているアプリケーションやサービスによってそれらが必要とされないことを確認する必要があります。

グループポリシーエディターを使用して、 > > > > > に移動します。設定を有効にし、リストに次の曲線を含めます。

```
NistP384

NistP256
```

注:

これにより、「curve25519」が選択されないようにします。FIPSモードは「curve25519」の使用を妨げません。

> VDAは、グループポリシーリストと、選択されたコンプライアンスモード（COM、GOV、またはALL）のリストの両方に表示される場合にのみ、暗号スイートを選択します。暗号スイートは、クライアント（Citrix Workspaceアプリ）から送信されるリストにも表示されている必要があります。

デリバリーグループでTLSを構成する

TLS接続用に構成したVDAを含む各デリバリーグループに対して、この手順を完了します。

1. StudioからPowerShellコンソールを開きます。
2. **Get-BrokerAccessPolicyRule -DesktopGroupName '\<*delivery-group-name*>' \| Set-BrokerAccessPolicyRule -HdxSslEnabled $true**を実行します。
3. **Set-BrokerSite -DnsResolutionEnabled $true**を実行します。

自動登録を使用したプールされたVDAのSSL有効化

プールされたVDAを使用する場合、マスターイメージに証明書を追加すると、すべてのVDAが同じイメージを共有します。ワイルドカード証明書を使用できますが、欠点は、いずれかのVDAが侵害された場合、この強力な証明書により、すべてのVDAに属するHDX™接続が危険にさらされることです。

代わりに、より安全な代替策として、Microsoft Active Directory証明書サービスを活用して、グループポリシーを使用して証明書を自動的にプロビジョニングする方法があります。VDA上でスタートアップスクリプトを使用して、新しい証明書を動的にプロビジョニングし、VDAでSSLを有効にすることができます。

このアプローチは、シングルセッションデスクトップVDAでのみ機能することに注意してください。マルチセッションVDAの場合、証明書が自動的にプロビジョニングされる前に、起動プロセス中にICAリスナーが早すぎる段階で起動されます。

Active Directory証明書サービスは内部のエンタープライズ証明機関を使用するため、すべてのWindowsインストールによって自動的に信頼されるわけではありません。クライアントが企業によって管理され、ドメインフォレストの一部である場合、信頼されたCA証明書はグループポリシーを使用して自動的に配布できます。BYODやその他のドメインに参加していないデバイスの場合、信頼されたCA証明書を何らかのメカニズム（ダウンロードリンクの提供など）でユーザーに配布するか、NetScaler Gatewayを使用する必要があります。

証明書の自動登録を有効にする

まず、VDA ドメインフォレスト内のサーバーに Active Directory 証明書サービスロールがインストールされており、エンタープライズ CA が提供されていることを確認してください。そうでない場合、自動登録はできません。

VDA は起動ごとに証明書要求を送信するため、これによりエンタープライズ CA に通常よりもかなり高い負荷がかかる可能性があることに注意してください。負荷に対応できるよう、CA サーバーに十分な CPU とメモリを割り当て、本番環境に移行する前に、常にラボ環境で展開のスケーラビリティをテストしてください。

グループポリシー管理エディターで、SSLが有効なプールされたVDAを含む組織単位に適用される新しいポリシーを次のように作成します。

1. コンピューターの構成 -> ポリシー -> Windows の設定 -> セキュリティの設定 -> 公開キーのポリシー を展開します
2. 「証明書サービス クライアント – 自動登録ポリシー」オブジェクトのプロパティを編集します
3. 以下のスクリーンショットに示すように構成します。
4. 自動証明書要求コンテナーを右クリックし、新規 -> 自動証明書要求... を選択します.
5. 自動証明書要求セットアップウィザードで、 をクリックします
6. コンピューター証明書テンプレートが選択されていることを確認し、 をクリックします
7. をクリックします

登録ポリシーのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2511/media/ssltask-autoenrollment-policy.png)

Windows マスターイメージの準備

`Support\Tools\SslSupport` フォルダーにある製品インストールメディアから Enable-VdaSsl.ps1 スクリプトを VDA マスターイメージにコピーします。マスターイメージには、HDX SSL 接続に使用する証明書を含めないでください。証明書は、MCS または PVS マシンカタログが作成されるときにプロビジョニングされます。次に、次のように新しいスケジュールされたタスクを作成します（スケジュールされたタスクは今すぐ実行しないでください）。

1. タスクスケジューラを開きます。
2. **操作**ペインで、「**タスクの作成...**」を押します。
3. 「全般」タブで：
    - `Enable VDA SSL` のような**名前**を入力します。

- **ユーザーまたはグループの変更...** をクリックし、「ユーザーまたはグループの選択」ダイアログボックスで `SYSTEM` を入力して **OK** をクリックします。

タスク作成の「アクション」タブのスクリーンショット (/en-us/citrix-virtual-apps-desktops/2511/media/ssltask-general.png)

4. 「トリガー」タブを選択します。
5. **新規...** をクリックします。「**新しいトリガー**」ダイアログで：
   a. **タスクの開始**を**イベント時**に設定します。
   b. **ログ**を **Microsoft-Windows-CertificateServicesClient-Lifecycle-System/Operational** に設定します。
   c. **ソース**を **Microsoft-Windows-CertificateServicesClient-Lifecycle-System** に設定します。
   d. **イベント ID** を `1006` に設定します。
   e. **OK** をクリックしてトリガーを保存します。

「新しいトリガー」ウィンドウのスクリーンショット (/en-us/citrix-virtual-apps-desktops/2511/media/ssltask-trigger.png)

6. 「**アクション**」タブを選択します。
7. **新規...** をクリックします。
8. 「**新しいアクション**」ダイアログで：
   a. 「**アクション**」を「**プログラムの開始**」に設定します
   b. プログラム/スクリプトフィールドに、`powershell.exe`と入力します
   c. 引数の追加フィールドに、PowerShellスクリプトへのパスを含めて`-ExecutionPolicy RemoteSigned Enable-VdaSsl.ps1 -Enable -Confirm:$False`と入力します。
   d. **OK**を押してアクションを保存します

新しいアクションウィンドウのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2511/media/ssltask-action.png)

9. **OK**を押してタスクを保存します

トラブルシューティング

接続エラーが発生した場合は、VDAのシステムイベントログを確認してください。

Windows向けCitrix Workspaceアプリを使用しているときに、TLSエラーを示す接続エラーが表示された場合は、Desktop Viewerを無効にしてから、もう一度接続を試してください。接続が引き続き失敗しても、基になるTLS問題の説明が提供される場合があります。（たとえば、証明機関に証明書を要求するときに誤ったテンプレートを指定したなど。）

HDX Adaptive Transportを使用するほとんどの構成は、Citrix Workspaceアプリ、Citrix Gateway、およびVDAの最新バージョンを使用するものを含め、DTLSで正常に動作します。Citrix WorkspaceアプリとCitrix Gatewayの間でDTLSを使用し、Citrix GatewayとVDAの間でDTLSを使用する一部の構成では、追加のアクションが必要です。

次の場合、追加のアクションが必要です。

- Citrix ReceiverのバージョンがHDX Adaptive TransportとDTLSをサポートしている場合：Receiver for Windows (4.7, 4.8, 4.9)、Receiver for Mac (12.5, 12.6, 12.7)、Receiver for iOS (7.2, 7.3.x)、またはReceiver for Linux (13.7)

かつ、以下のいずれかが当てはまる場合：

- Citrix GatewayのバージョンはVDAへのDTLSをサポートしているが、VDAのバージョンはDTLSをサポートしていない（バージョン7.15以前）。
- VDAのバージョンはDTLSをサポートしている（バージョン7.16以降）が、Citrix GatewayのバージョンはVDAへのDTLSをサポートしていない。

Citrix Receiver™ からの接続が失敗するのを避けるには、次のいずれかを実行します。

- Citrix Receiverを、Receiver for Windowsバージョン4.10以降、Receiver for Mac 12.8以降、またはReceiver for iOSバージョン7.5以降に更新する。
- Citrix Gatewayを、VDAへのDTLSをサポートするバージョンに更新する。
- VDAをバージョン7.16以降に更新する。
- VDAでDTLSを無効にする。
- HDX Adaptive Transportを無効にする。

> **注：**
>
> Receiver for Linuxの適切なアップデートはまだ利用できません。Receiver for Android（バージョン3.12.3）は、HDX Adaptive TransportおよびCitrix Gateway経由のDTLSをサポートしていないため、影響を受けません。

VDAでDTLSを無効にするには、VDAファイアウォール構成を変更してUDPポート443を無効にします。「ネットワークポート」を参照してください(/ja-jp/tech-zone/build/tech-papers/citrix-communication-ports.html#citrix-virtual-apps-and-desktops)。

TLS と HTML5 ビデオリダイレクト、およびブラウザコンテンツリダイレクト

HTML5 ビデオリダイレクトとブラウザコンテンツリダイレクトを使用して、HTTPS Web サイトをリダイレクトできます。これらの Web サイトに挿入された JavaScript は、VDA で実行されている Citrix HDX HTML5 ビデオリダイレクトサービスへの TLS 接続を確立する必要があります。これを実現するために、HTML5 ビデオリダイレクトサービスは、VDA の証明書ストアに 2 つのカスタム証明書を生成します。サービスを停止すると、証明書は削除されます。

HTML5 ビデオリダイレクトポリシーは、デフォルトで無効になっています。

ブラウザコンテンツリダイレクトは、デフォルトで有効になっています。

HTML5ビデオリダイレクトの詳細については、「マルチメディアポリシー設定」を参照してください(/ja-jp/citrix-virtual-apps-desktops/2511/policies/reference/ica-policy-settings/multimedia-policy-settings.html#html5-video-redirection)。

ユニバーサルプリントサーバーでTLSを有効にする

Virtual Delivery Agent (VDA) とユニバーサルプリントサーバー間のTCPベースの接続には、トランスポート層セキュリティ (TLS) プロトコルがサポートされています。

警告:

Windowsレジストリでの作業を含むタスクの場合、レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。レジストリエディターはご自身の責任において使用してください。編集する前に必ずレジストリをバックアップしてください。

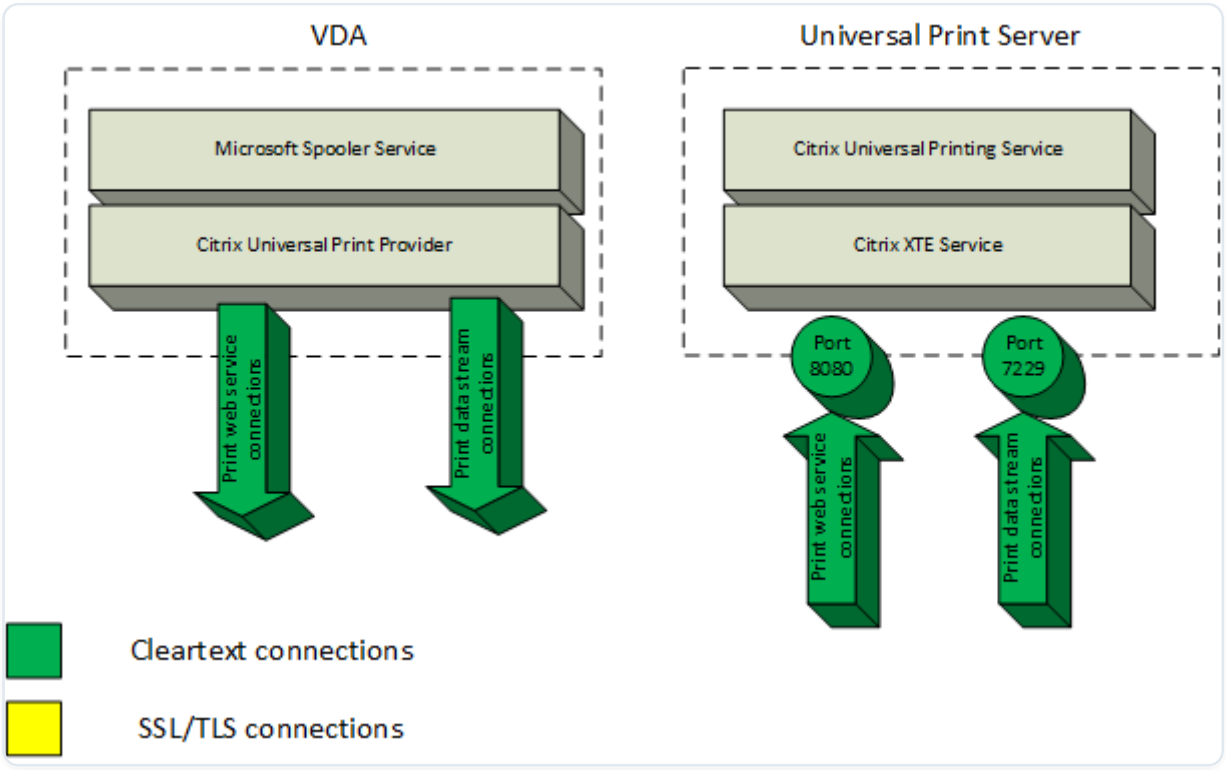
VDAとユニバーサルプリントサーバー間の印刷接続の種類

クリアテキスト接続

以下の印刷関連の接続は、VDAから発信され、ユニバーサルプリントサーバー上のポートに接続します。これらの接続は、**SSL enabled** ポリシー設定が **Disabled** (デフォルト) に設定されている場合にのみ行われます。

- クリアテキスト印刷Webサービス接続 (TCPポート 8080)
- クリアテキスト印刷データストリーム (CGP) 接続 (TCPポート 7229)

Microsoftサポート記事「Service overview and network port requirements for Windows」では、Microsoft Windows Print Spoolerサービスが使用するポートについて説明しています。このドキュメントのSSL/TLS設定は、Windows Print Spoolerサービスによって行われるNetBIOSおよびRPC接続には適用されません。**Universal Print Server enable** ポリシー設定が **Enabled with fallback to Windows' native remote printing** に設定されている場合、VDAはWindows Network Print Provider (win32spl.dll) をフォールバックとして使用します。

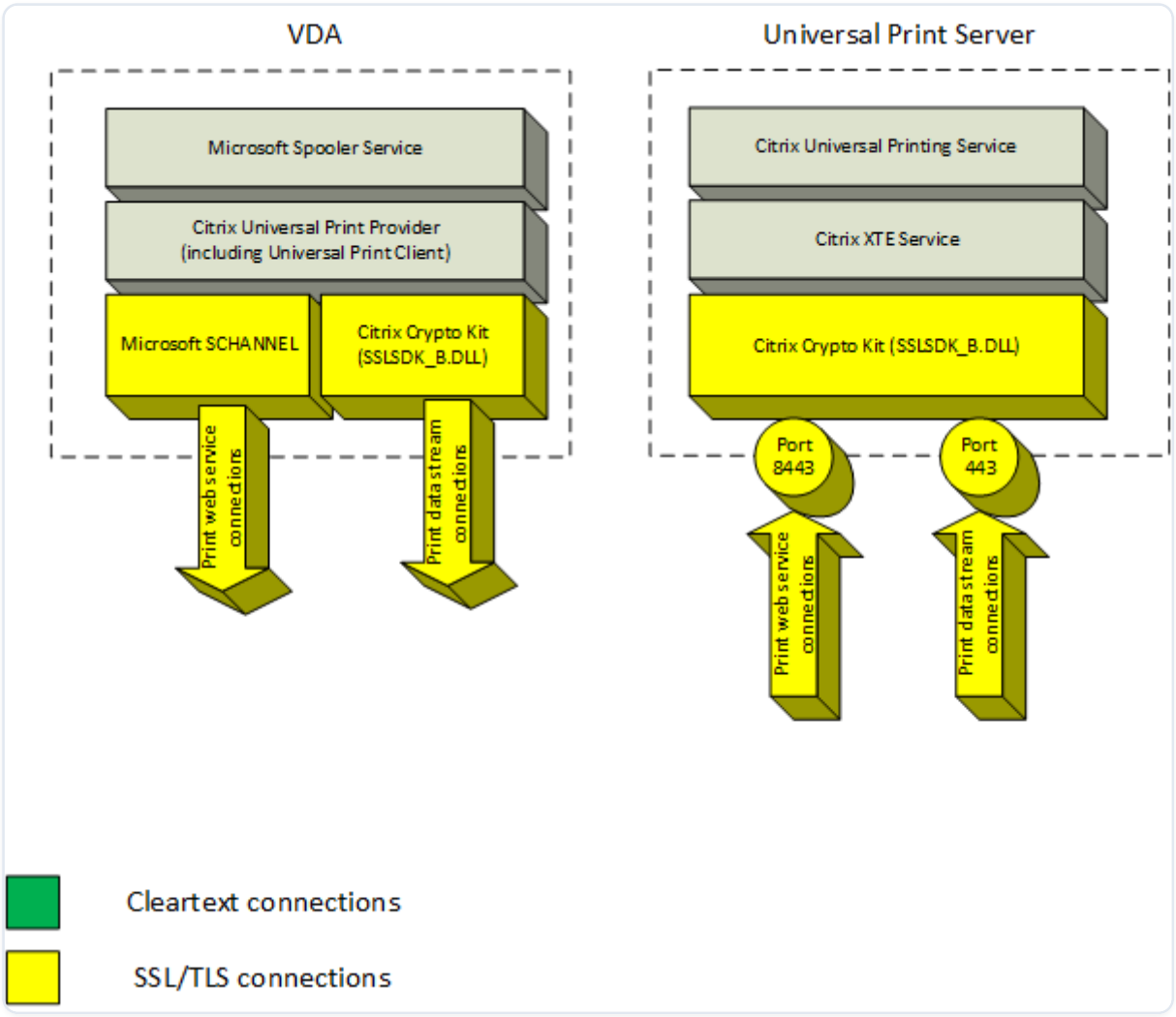


暗号化された接続

これらの印刷関連のSSL/TLS接続は、VDAから発信され、ユニバーサルプリントサーバー上のポートに接続します。これらの接続は、**SSL enabled** ポリシー設定が **Enabled** に設定されている場合にのみ行われます。

- 暗号化された印刷Webサービス接続 (TCPポート 8443)

- 暗号化された印刷データストリーム (CGP) 接続 (TCPポート 443)



SSL/TLS クライアント構成

VDA は SSL/TLS クライアントとして機能します。

Microsoftグループポリシーとレジストリを使用して、暗号化された印刷Webサービス接続（TCPポート8443）のためにMicrosoft SCHANNEL SSPを構成します。Microsoftサポート記事のTLS Registry Settingsには、Microsoft SCHANNEL SSPのレジストリ設定が記載されています。

VDAでグループポリシーエディターを使用して、**コンピューターの構成 > 管理用テンプレート > ネットワーク > SSL構成設定 > SSL暗号スイートの順序**に移動します。TLS 1.3が設定されている場合は、次の順序を選択します。

TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256

TLS 1.2 が設定されている場合は、次の順序を選択します。

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

注:

このグループポリシー設定が構成されている場合、VDAは、接続が両方のSSL暗号スイートリストに表示されている場合にのみ、暗号化された印刷Webサービス接続（デフォルトポート：8443）の暗号スイートを選択します。

- グループポリシーSSL暗号スイート順序リスト
- 選択されたSSL暗号スイートポリシー設定（COM、GOV、またはALL）に対応するリスト

このグループポリシー構成は、VDA上の他のTLSアプリケーションおよびサービスにも影響します。アプリケーションが特定の暗号スイートを必要とする場合は、このグループポリシー暗号スイート順序リストに追加する必要がある場合があります。

重要:

TLS 構成のグループポリシーの変更は、オペレーティングシステムの再起動後にのみ有効になります。

Citrix ポリシーを使用して、暗号化された印刷データストリーム (CGP) 接続 (TCP ポート 443) の SSL/TLS 設定を構成します。

SSL/TLS サーバー構成

ユニバーサルプリントサーバーはSSL/TLSサーバーとして機能します。

SSL/TLS設定を構成するには、`Enable-UpsSsl.ps1` PowerShellスクリプトを使用します。

Universal Print ServerにTLS証明書をインストールする

HTTPSの場合、VDAによって信頼されているSSLサーバー証明書をUniversal Print Serverにインストールする必要があります。Universal Print Serverの証明書を要求するには、Microsoft Active Directory証明書サービスまたは別の認証局を使用します。

マイクロソフト Active Directory 証明書サービスを使用して証明書を登録/要求する際は、以下の考慮事項に留意してください。

1. 証明書をローカルコンピューターの**個人**証明書ストアに配置します。
2. 証明書のサブジェクト識別名（Subject DN）の**共通名**属性を、Universal Print Serverの完全修飾ドメイン名（FQDN）に設定します。これは証明書テンプレートで指定します。
3. 証明書要求と秘密キーの生成に使用される暗号化サービスプロバイダー（CSP）を**Microsoft Enhanced RSA and AES Cryptographic Provider (Encryption)**に設定します。これは証明書テンプレートで指定します。
4. キーサイズを2048ビット以上に設定します。これは証明書テンプレートで指定します。

証明書の作成とインストールについて詳しくは、「証明書の管理」を参照してください。

Universal Print ServerでのSSLの構成

Universal Print Server上のXTEサービスは、受信接続をリッスンします。SSLが有効になっている場合、SSLサーバーとして機能します。受信接続には、印刷コマンドを含む印刷Webサービス接続と、印刷ジョブを含む印刷データストリーム接続の2種類があります。これらの接続でSSLを有効にできます。SSLは、これらの接続の機密性と整合性を保護します。デフォルトでは、SSLは無効になっています。

SSLの構成に使用されるPowerShellスクリプトは、インストールメディアにあり、ファイル名は次のとおりです。`\Support\Tools\SslSupport\Enable-UpsSsl.ps1.`.

Universal Print Serverでのリスニングポート番号の構成

これらは、XTE Service のデフォルトポートです。

- クリアテキスト印刷Webサービス（HTTP）TCPポート: 8080
- クリアテキスト印刷データストリーム (CGP) TCPポート: 7229
- 暗号化された印刷Webサービス (HTTPS) TCPポート: 8443
- 暗号化された印刷データストリーム (CGP) TCPポート: 443

Universal Print Server で XTE Service が使用するポートを変更するには、管理者として PowerShell で次のコマンドを実行します (Enable-UpsSsl.ps1 PowerShell スクリプトの使用に関する注意点については、後のセクションを参照してください)。

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` または `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`
3. `Start-Service CitrixXTEServer`

Universal Print Server での TLS 設定

負荷分散構成で複数の Universal Print Server を使用している場合は、すべての Universal Print Server で **TLS** 設定が一貫して構成されていることを確認してください。

Universal Print Server で TLS を構成すると、インストールされている TLS 証明書のアクセス許可が変更され、Universal Printing Service に証明書の秘密キーへの読み取りアクセス権が付与されます。また、Universal Printing Service に次の情報が通知されます。

- TLS に使用する証明書ストア内の証明書。
- TLS 接続に使用する TCP ポート番号。

Windows ファイアウォール (有効な場合) は、これらの TCP ポートでの受信接続を許可するように構成する必要があります。この構成は、Enable-UpsSsl.ps1 PowerShell スクリプトを使用すると自動的に行われます。

- 許可する TLS プロトコルのバージョン。

Universal Print Server は、TLS プロトコルバージョン 1.3 および 1.2 をサポートしています。許可される最小バージョンを指定します。

デフォルトの TLS プロトコルバージョンは 1.2 です。

> **注:**
>
> Citrix Virtual Apps and Desktops バージョン 2311 以降、TLS 1.1 および 1.0 はサポートされなくなりました。

- 許可する TLS 暗号スイート。

暗号スイートは、接続に使用される暗号化アルゴリズムを選択します。VDA と Universal Print Server は、異なる暗号スイートのセットをサポートできます。VDA が接続し、サポートされている TLS 暗号スイートのリストを送信すると、Universal Print Server はクライアントの暗号スイートの 1 つを、自身の構成済み暗号スイートのリストにある暗号スイートの 1 つと照合し、接続を受け入れます。一致する暗号スイートがない場合、Universal Print Server は接続を拒否します。

Universal Print Server は、OPEN、FIPS、および SP800-52 ネイティブ Crypto Kit モード用に、GOV(ernment)、COM(mercial)、および ALL という名前の以下の暗号スイートセットをサポートしています。許容される暗号スイートは、**SSL FIPS Mode** ポリシー設定と Windows FIPS モードにも依存します。Windows FIPS モードの詳細については、この Microsoft サポート記事 を参照してください。

暗号スイート (優先順位の降順)	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_AES256_GCM_SHA384	X		X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA384	X		X	X		X	X		X

暗号スイート (優先順位の降順)	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_AES256_CBC_SHA	X	X		X	X		X	X	

PowerShellスクリプトを使用してUniversal Print ServerでTLSを構成する

証明書ストアの**ローカルコンピューター > 個人 > 証明書**領域にTLS証明書をインストールします。その場所に複数の証明書がある場合は、`Enable-UpsSsl.ps1` PowerShellスクリプトに証明書のサムプリントを指定します。

> **注：**
>
> PowerShellスクリプトは、Universal Print ServerのFQDNに基づいて正しい証明書を検索します。Universal Print ServerのFQDNに対して単一の証明書のみが存在する場合、証明書のサムプリントを指定する必要はありません。

> `Enable-UpsSsl.ps1` スクリプトは、VDAからUniversal Print ServerへのTLS接続を有効または無効にします。このスクリプトは、インストールメディアの**Support > Tools > SslSupport**フォルダーにあります。

TLSを有効にすると、スクリプトはUniversal Print ServerのTCPポートに対する既存のWindowsファイアウォールルールをすべて無効にします。その後、XTEサービスがTLS TCPおよびUDPポートでのみ受信接続を受け入れることを許可する新しいルールを追加します。また、以下のWindowsファイアウォールルールも無効にします。

- クリアテキスト印刷Webサービス接続 (デフォルト: 8080)

- クリアテキスト印刷データストリーム (CGP) 接続 (デフォルト: 7229)

その結果、VDAはTLSを使用している場合にのみこれらの接続を行うことができます。

注：

TLSを有効にしても、VDAからUniversal Print ServerへのWindows Print Spooler RPC/SMB接続には影響しません。

重要：

最初のパラメーターとして**Enable**または**Disable**のいずれかを指定します。ローカルコンピューターの個人証明書ストアにUniversal Print ServerのFQDNを持つ証明書が1つしかない場合、CertificateThumbprintパラメーターはオプションです。その他のパラメーターはオプションです。

構文

```
Enable-UpsSSL.ps1 -Enable [-HTTPPort &lt;port&gt;] [-CGPPort &lt;port&gt;] [-HTTPSPort &lt;port&gt;] [-CGPSSLPort &lt;port&gt;] [-SSLMinVersion &lt;version&gt;] [-SSLCipherSuite &lt;name&gt;] [-CertificateThumbprint &lt;thumbprint&gt;] [-FIPSMode &lt;Boolean&gt;] [-ComplianceMode &lt;mode&gt;]

Enable-UpsSSL.ps1 -Disable [-HTTPPort &lt;portnum&gt;] [-CGPPort &lt;portnum&gt;]
```

パラメーター	説明
有効	XTEサーバーでSSL/TLSを有効にします。このパラメーターまたはDisableパラメーターのいずれかが必要です。
無効	XTEサーバーでSSL/TLSを無効にします。このパラメーターまたはEnableパラメーターのいずれかが必要です。
CertificateThumbprint `"<thumbprint>"`	ローカルコンピューターの個人証明書ストアにあるTLS証明書のサムプリントを引用符で囲んで指定します。スクリプトは、指定されたサ

パラメーター	説明
	ムプリントを使用して、使用する証明書を選択します。
HTTPポート `<port>`	クリアテキスト印刷Webサービス（HTTP/SOAP）ポート。デフォルト：8080
CGPポート `<port>`	クリアテキスト印刷データストリーム（CGP）ポート。デフォルト：7229
HTTPSポート `<port>`	暗号化された印刷Webサービス（HTTPS/SOAP）ポート。デフォルト：8443
CGPSSLポート `<port>`	暗号化された印刷データストリーム（CGP）ポート。デフォルト：443
SSLMinVersion `"<version>"`	引用符で囲まれた最小TLSプロトコルバージョン。有効な値：「TLS_1.2」および「TLS_1.3」。デフォルト：TLS_1.2。
SSLCipherSuite `"<name>"`	引用符で囲まれたTLS暗号スイートパッケージの名前。有効な値：「GOV」、「COM」、および「ALL」（デフォルト）。
FIPSモード `<Boolean>`	XTEサーバーでFIPS 140モードを有効または無効にします。有効な値: FIPS 140モードを有効にする場合は$true、FIPS 140モードを無効にする場合は$false。

例

次のスクリプトはTLSを有効にします。サムプリント（この例では「12345678987654321」として表されています）は、使用する証明書を選択するために使用されます。

```
Enable-UpsSsl.ps1 –Enable -CertificateThumbprint "12345678987654321"
```

次のスクリプトはTLSを無効にします。

```
Enable-UpsSsl.ps1 –Disable
```

FIPSモードの構成

米国連邦情報処理標準（FIPS）モードを有効にすると、Universal Print Serverの暗号化された接続にはFIPS 140準拠の暗号化のみが使用されるようになります。

クライアントでFIPSモードを構成する前に、サーバーでFIPSモードを構成してください。

ウィンドウズ FIPSモードの有効化/無効化については、マイクロソフトのドキュメントサイトを参照してください。

クライアントでのFIPSモードの有効化

Delivery Controller™でWeb Studioを実行し、Citrixポリシー設定の**UPS FIPS Mode**を**Enabled**に設定します。Citrixポリシーを有効にします。

各VDAで以下を実行します。

1. Windows FIPSモードを有効にします。
2. VDAを再起動します。

サーバーでのFIPSモードの有効化

各Universal Print Serverで、次の操作を実行します。

1. Windows FIPSモードを有効にします。
2. 管理者としてこのPowerShellコマンドを実行します: `stop-service CitrixXTEServer, UpSvc`
3. `Enable-UpsSsl.ps1` スクリプトを `-Enable -FIPSMode $true` パラメータで実行します。
4. Universal Print Serverを再起動します。

クライアントでのFIPSモードの無効化

Web Studioで、Citrixポリシー設定の**UPS FIPS Mode**を**Disabled**に設定します。Citrixポリシーを有効にします。また、**UPS FIPS Mode** Citrixポリシー設定を削除することもできます。

各VDAで、次の操作を実行します。

1. Windows FIPSモードを無効にします。
2. VDAを再起動します。

サーバーでのFIPSモードの無効化

各Universal Print Serverで、次の操作を実行します。

1. Windows FIPSモードを無効にします。
2. 管理者としてこのPowerShellコマンドを実行します: `stop-service CitrixXTEServer, UpSvc`
3. `Enable-UpsSsl.ps1` スクリプトを `-Enable -FIPSMode $false` パラメーターで実行します。
4. Universal Print Server を再起動します。

> **注:**
>
> SSL プロトコルバージョンが TLS 1.3 に設定されている場合、FIPS モードはサポートされません。

SSL/TLS プロトコルバージョンの構成

デフォルトの SSL/TLS プロトコルバージョンは TLS 1.2 です。TLS 1.2 と TLS 1.3 は、本番環境での使用が推奨される SSL/TLS プロトコルバージョンです。トラブルシューティングのために、非本番環境で一時的に SSL/TLS プロトコルバージョンを変更する必要がある場合があります。

SSL 2.0 および SSL 3.0 は Universal Print Server ではサポートされていません。

サーバーでの SSL/TLS プロトコルバージョンの設定

各 Universal Print Server でこれを行います。

1. 管理者として次の PowerShell コマンドを実行します: `stop-service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1` スクリプトを `-Enable -SSLMinVersion` バージョンパラメーターで実行します。テストが完了したら、これを TLS 1.2 または TLS 1.3 に戻すことを忘れないでください。
3. Universal Print Server を再起動します。

クライアントでの SSL/TLS プロトコルバージョンの設定

Studio で、**SSL Protocol Version** ポリシー設定を目的のプロトコルバージョンに設定し、ポリシーを有効にします。

VDA のオペレーティングシステムが選択した TLS バージョンをサポートしていることを確認してください。Windows でサポートされている TLS バージョンについては、Microsoft Learn - TLS

protocol version support を参照してください。デフォルトを上書きするようにレジストリを構成するには、Microsoft Learn - TLS, DTLS, and SSL protocol version settings を参照してください。

トラブルシューティング

接続エラーが発生した場合は、Universal Print Server上のC:\Program Files (x86)\Citrix\XTE\logs\error.logファイルを確認してください。

SSL/TLSハンドシェイクが失敗した場合、このログファイルにエラーメッセージ**SSL handshake from client failed**が表示されます。このような失敗は、VDAとUniversal Print ServerのSSL/TLSプロトコルバージョンが一致しない場合に発生する可能性があります。

Universal Print Serverのホスト名を含む以下のポリシー設定で、Universal Print ServerのFQDNを使用します。

- セッションプリンター
- プリンターの割り当て
- 負荷分散用のUniversal Print Server

Universal Print ServerとVDAでシステムクロック（日付、時刻、タイムゾーン）が正しいことを確認してください。

仮想チャネル許可リスト

The virtual channel allow list is a feature that allows you to control which non-Citrix virtual channels are allowed in your environment. By default, the virtual channel allow list feature is enabled. As a result, only Citrix virtual channels are allowed to open in Citrix Virtual Apps and Desktops™ sessions. If there is a need to use custom virtual channels, whether homegrown or from a third party, these need to be explicitly added to the allow list.

構成

仮想チャネル許可リストはデフォルトで有効になっています。この機能は、Citrixポリシーの以下の設定を使用して構成できます。

- **仮想チャネル許可リスト**: この機能を有効または無効にし、仮想チャネルをリストに追加します。
- **仮想チャネル許可リストログスロットリング**: 仮想チャネル許可リストイベントログのスロットリング期間を設定します。
- **仮想チャネル許可リストログ記録**: 仮想チャネル許可リストのログレベルを設定します。

仮想チャネルを許可リストに追加する

仮想チャネルを許可リストに追加するには、以下の情報が必要です。

1. コードで定義されている仮想チャネル名。最大7文字です。例: `CTXCVC1`。
2. VDAマシン上で仮想チャネルを開くプロセスのパス。例: `C:\Program Files\Application\run.exe`。

必要な情報が揃ったら、仮想チャネル許可リストポリシー設定を使用して、仮想チャネルを許可リストに追加する必要があります。リストに仮想チャネルを追加するには、仮想チャネル名の後にコンマ、そして仮想チャネルにアクセスするプロセスのパスを入力します。複数のプロセスがある場合は、各プロセスをコンマで区切って追加できます。

単一プロセスの場合

前の例を使用して、以下のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe
```

複数のプロセスの場合

複数のプロセスがある場合は、次のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

ワイルドカードの使用

ワイルドカード (*) の使用がサポートされています。アプリケーションのバージョンに基づいてディレクトリ名または実行可能ファイル名が変更される場合、またはサードパーティコンポーネントがユーザープロファイルにインストールされている場合に、ワイルドカードを使用できます。

次のシナリオでワイルドカードを使用できます。

- 完全なディレクトリ名を置き換える場合。 例: `C:\Program Files\Application*\run1.exe`
- ディレクトリ名の一部を置き換える場合。 例: `C:\Program Files\Application\v*\run1.exe`
- 実行可能ファイル名を置き換える場合。 例: `C:\Program Files\Application\v1.2*.exe`
- 実行可能ファイル名の一部を置き換える場合。 例: `C:\Program Files\Application\v1.2\run*.exe`

次の制限が適用されます。

- ワイルドカードは単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルが `C:\Program Files\Application\v1.2\run1.exe` にある場合
  - 許可: `C:\Program Files\Application*\run1.exe`
  - 不許可: `C:\Program Files*\run1.exe`
- エントリにはファイル名拡張子を含める必要があります。
  - 許可: `C:\Program Files\Application\v1.2*.exe`
  - 許可されていません: `C:\Program Files\Application\v1.2*`
- すべてのパスはローカルである必要があります。

注:

- ネットワークパスは許可されていません。
- ワイルドカードのサポートは、Citrix Virtual Apps™ and Desktops 2206 から利用可能です。
- ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2203 LTSR の CU2 から利用可能です。

システム環境変数の使用

システム環境変数を使用して、許可リスト内の信頼されたプロセスの定義を簡素化できます。`%programfiles%`、`%programfiles(x86)%`、`%systemdrive%`、`%systemroot%` など、標準で提供されている任意の変数を使用できます。

カスタム環境変数も、システムレベルで定義されている限り使用できます。

以下に、標準で提供されている環境変数の例を示します。

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

以下に、カスタムシステム環境変数の例を示します。

- カスタム変数名: `app`
- カスタム変数値: `%programfiles%\Application\`
- 許可リストエントリ: `CTXCVC1,%app%\run.exe`

> **注:**
>
> ユーザー環境変数はサポートされていません。

> 環境変数サポートは、Citrix Virtual Apps and Desktops バージョン 2209 から利用可能です。

仮想チャネル名とプロセスを取得する

VDAマシン上で仮想チャネルの名前とそれを開くプロセスを取得する最も簡単な方法は、仮想チャネルを提供した開発者またはサードパーティベンダーから情報を取得することです。

または、機能のログを適用し、以下の手順に従うことで情報を取得できます。

1. カスタム仮想チャネルのクライアントおよびサーバーコンポーネントが配置されたら、仮想アプリケーションまたは仮想デスクトップを起動します。
2. VDAマシンのシステムイベントログで、カスタム仮想チャネルの名前と、それを開こうとしたプロセスを探します。利用可能なイベントの詳細については、イベントログを参照してください。
3. セッションからログアウトします。
4. 特定された仮想チャネルとプロセスに対して、仮想チャネル許可リストポリシー設定にエントリを追加します。
5. マシンを再起動します。
6. VDAが登録されたら、仮想アプリケーションまたは仮想デスクトップを実行して、カスタム仮想チャネルが正常に開くことを検証します。

Citrix仮想チャネルに関する考慮事項

すべての組み込みCitrix仮想チャネルは信頼されており、追加設定なしで開くことができます。ただし、以下の2つの機能は、外部依存関係のため、許可リストに明示的なエントリが必要です。

- マルチメディアリダイレクト
- Skype for Business 用 HDX リアルタイム最適化パック

マルチメディアリダイレクト

システムのメディアプレーヤーとしてWindows Media Player以外のメディアプレーヤーを使用する場合、それを信頼されたプロセスとして許可リストに追加する必要があります。許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXMM`
- プロセス: VDAマシンで使用されるメディアプレーヤーへのパス。例: `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`。
- 許可リストエントリ: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

Skype for Business 用 HDX リアルタイム最適化パック

許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXRMEP`
- プロセス: VDAマシン内のSkype for Business実行可能ファイルへのパス。これはSkype for Businessのバージョンやカスタムインストールパスの使用によって異なる場合があります。例: `C:\Program Files\Microsoft Office\root\Office16\lync.exe.`.
- 許可リストエントリ: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

VDA と Delivery Controller™ 間の WebSocket 通信

この記事では、WCF通信の代替として、VDAとDelivery Controller間の通信にWebSocket接続を設定する方法について説明します。これにより、VDAからDelivery Controllerへの通信にTLSポート443のみを使用するという利点が得られます。

動作の仕組み

以下のセクションでは、Delivery ControllerとVDA間のWebSocket通信のワークフローについて説明します。

通常のブローカリング操作中

1. Citrix Virtual Apps and Desktops™管理者は、Machine Creation Service (MCS) を使用してVDAをプロビジョニングすることでプロセスを開始します。

2. MCSプロビジョニングプロセス中に、MCSは各VDAの公開鍵と秘密鍵のペアを生成し、Delivery Controller上のFMA信頼サービスに公開鍵を登録します。MCSは、公開鍵と秘密鍵のペアをVDAのIDディスク下のファイルとして保存します。
3. VDAマシンが起動すると、VDAマシンにインストールされているMCSエージェントは、IDディスクからキーペアを読み取り、この情報をVDAレジストリの場所に書き込みます。
4. VDAにインストールされているブローカーエージェントは、レジストリからキーペアを読み取り、秘密鍵で署名されたサービスキーを含むSSL対応のWebSocketリクエストをDelivery Controllerに生成します。
5. Delivery Controllerは、FMA信頼サービスからの公開鍵を使用して、署名されたサービスキー認証ヘッダーを検証します。
6. 検証が完了すると、システムはVDAとDelivery Controller間のWebSocket接続を確立します。

LHCモードがアクティブになるとき

LHCのWebSocketサポートを有効にすると、LHCモード中にVDAがHigh Availability ServiceとのWebSocket接続を確立しようとした際、High Availability Serviceはローカルデータベースからの公開鍵を使用して、署名されたサービスキー認証ヘッダーを検証します。これによりWebSocket接続が認証され、LHCモードでもVDAとDelivery Controller間のWebSocket接続が成功します。

WebSocketのサポート

開始する前に

1. サイトを構成します。詳細については、「サイトの作成」を参照してください。
2. Delivery Controller に TLS 証明書をインストールします。詳細については、「Controller に TLS サーバー証明書をインストールする」を参照してください。
3. Delivery Controller を信頼するために、VDA にルートCAと中間CAをインストールします。

手順

WebSocket接続をセットアップするには、以下の手順に従ってください。

1. Delivery Controller で WebSocket 接続を有効にします。サイト内の各 Delivery Controller で次のコマンドを実行します。

   ```
   New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy" -Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -Force
   ```

2. WebSocket を有効にした後、Broker Service を再起動します。

3. LHC モードの WebSocket サポートを有効にします。サイト内の各 Delivery Controller で次のコマンドを実行します。

```
New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\LHC" -Name
"WebSocketEnabledLhc" -PropertyType "DWord" -Value 1 -Force
```

4. MCS プロビジョニングを使用して、AD に参加している VDA 用のマシンカタログを作成します。詳細については、「マシンカタログの作成」を参照してください。
5. デリバリーグループを作成し、VDA を追加します。詳細については、「デリバリーグループの作成」を参照してください。
6. VDA で WebSocket 接続を有効にします。VDA で次の PowerShell コマンドを実行します。

```
New-ItemProperty
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAgent
\WebSocket" -Name "Enabled" -PropertyType "DWord" -Value 1 -Force
```

- WebSocketが有効になっているか確認するには、次のレジストリキーの値を確認します。`Enabled`の値は1である必要があります。

  キー:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAge
  nt\WebSocket
  ```

  名前: Enabled

  種類: REG_DWORD

  値: 1

HDX接続

アダプティブトランスポート

アダプティブトランスポートは、Citrix Virtual Apps and Desktops™ のメカニズムであり、優先トランスポートプロトコルを使用してHDXセッションの接続を確立し、優先プロトコルでの接続が利用できない場合はTCPへのフォールバックを提供します。

次のトランスポートプロトコルがサポートされています。

- 啓発されたデータ転送 (EDT)
- 伝送制御プロトコル (TCP)

構成

アダプティブトランスポートはデフォルトで有効になっています。アダプティブトランスポートは、次のモードで動作するように構成できます。

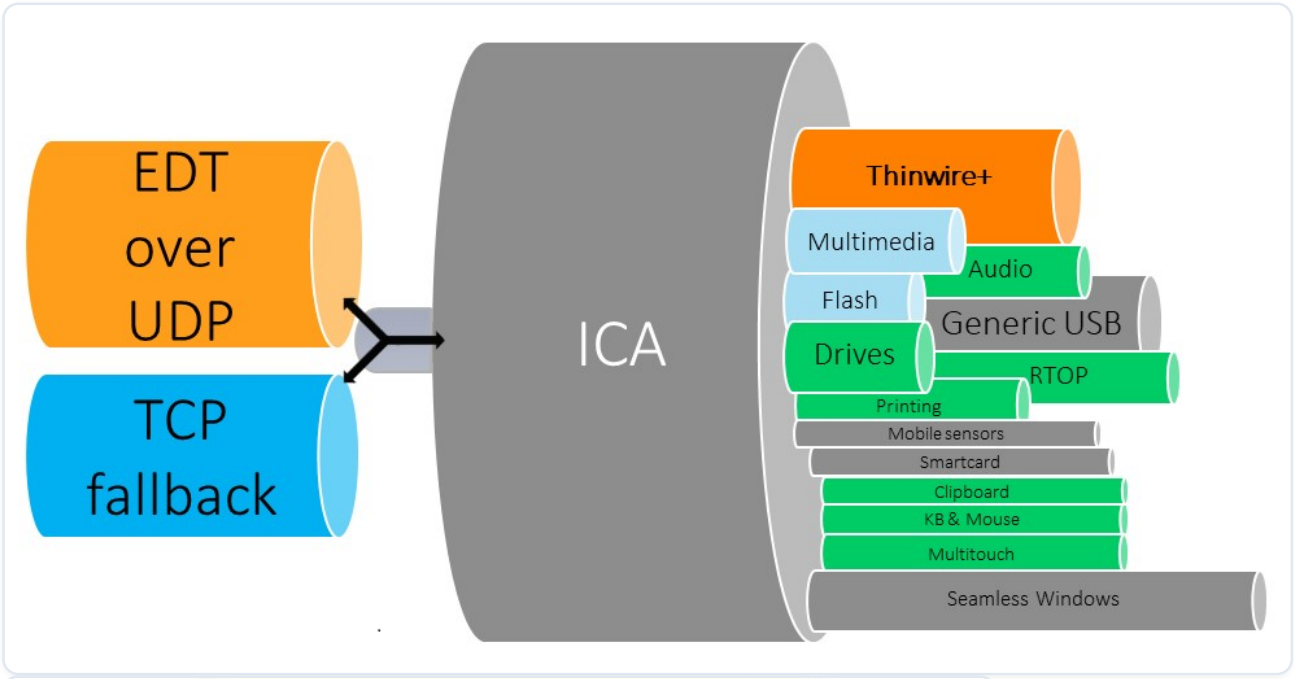
- **優先**: (デフォルト) クライアントは優先プロトコルで接続を試行し、優先プロトコルでの接続が利用できない場合はTCPにフォールバックします。
- **診断モード**: クライアントは優先プロトコルのみを使用して接続を試行します。TCPへのフォールバックは無効になります。
- **オフ**: クライアントはTCPのみを使用して接続を試行します。

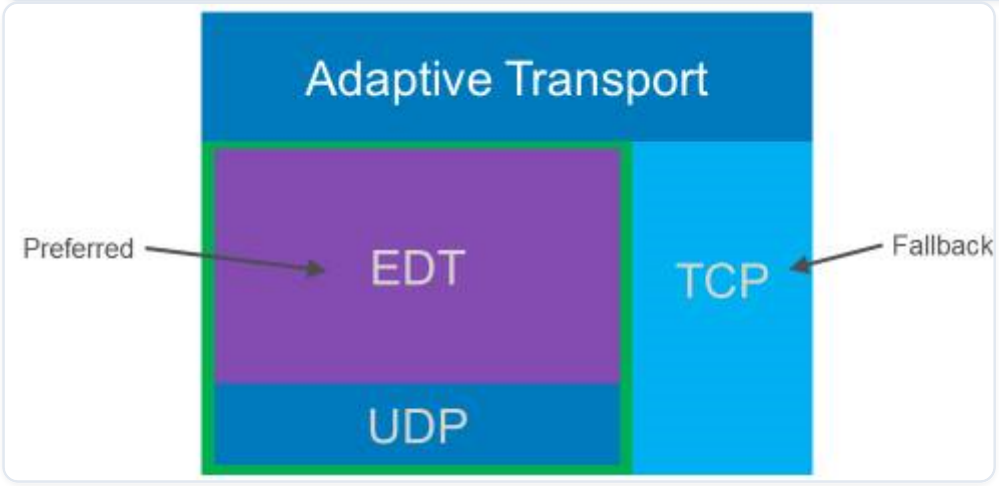
仕組み

Adaptive Transport が `Preferred` に設定されている場合、クライアントは優先プロトコルとTCPの両方でセッションへの接続を並行して試行します。これにより、優先プロトコルで接続できず、クライアントがTCPの使用にフォールバックする必要がある場合に、接続時間を最適化できます。TCPを使用して接続が確立された場合、クライアントは5分ごとにバックグラウンドで優先プロトコルでの接続を試行します。

Adaptive Transport が `Diagnostic mode` に設定されている場合、クライアントは優先プロトコルのみを使用してセッションに接続します。クライアントが優先プロトコルを使用して接続を確立できない場合、TCPの使用にフォールバックせず、接続は失敗します。

Adaptive Transport が `Off` に設定されている場合、**Adaptive Transport** は無効になり、クライアントはTCPのみを使用してセッションに接続します。





システム要件

アダプティブトランスポートとEDTを使用するための要件は次のとおりです。

- コントロールプレーン
  - シトリックス DaaS (旧 シトリックス バーチャルアプリ™ アンド デスクトップサービス)
  - Citrix Virtual Apps and Desktops: 現在サポートされているバージョン
- バーチャル デリバリー エージェント
  - Windows: 現在サポートされているバージョン（2402以降を推奨）
  - Linux: 現在サポートされているバージョン（2402以降を推奨）

- シトリックス ワークスペース™ アプリ
  - Windows: 現在サポートされているバージョン（2402以降を推奨）
  - Linux: 現在サポートされているバージョン（2402以降を推奨）
  - Mac: 現在サポートされているバージョン（2402以降を推奨）
  - iOS: Apple App Storeで入手可能な最新バージョン
  - Android: Google Playで入手可能な最新バージョン
- シトリックス NetScaler® ゲートウェイ
  - 14.1.12.30 以降（推奨）
  - 13.1.17.42 以降（13.1-52.19 以降を推奨）

> **注：**
>
> Linux VDA の詳細については、Linux Virtual Delivery Agent のドキュメントを参照してください。

ネットワーク要件

以下は、アダプティブトランスポートでEDTを使用するためのネットワーク要件です。

セッションホスト

セッションホストにWindows Defender ファイアウォールなどのファイアウォールがある場合、内部接続のために以下のインバウンドトラフィックを許可する必要があります。

説明	送信元	プロトコル	ポート
内部接続 - セッションの信頼性が有効	クライアント	UDP	2598
内部接続 - セッションの信頼性が無効			1494
内部接続 - HDX™ DirectまたはVDA SSL			443

注:

VDAインストーラーは、Windows Defender ファイアウォールに適切な受信規則を追加します。別のファイアウォールを使用している場合は、上記の規則を追加する必要があります。

内部ネットワーク

次の表は、お使いのネットワークでEDTを使用するために必要なファイアウォール規則を示しています。

説明	プロトコル	送信元	宛先	宛先ポート
直接内部接続 - セッションの信頼性が有効	UDP	クライアントネットワーク	VDAネットワーク	2598
直接内部接続 - セッションの信頼性が無効				1494
直接内部接続 - HDX DirectまたはVDA SSL				443
ネットスケーラー ゲートウェイ		NetScaler SNIP		2598
ネットスケーラー ゲートウェイ - VDA SSL				443

注:

Citrix Gateway Service を使用している場合、EDT をトランスポートプロトコルとして使用するには、**Rendezvous** を有効にする必要があります。システムおよびネットワーク要件については、Rendezvous ドキュメントを参照してください。

クライアントネットワーク

以下の表は、クライアントデバイスの接続要件を示しています。

説明	プロトコル	ソース	宛先	宛先ポート
内部接続 - セッションの信頼性が有効	UDP	クライアントIP	VDAネットワーク	2598
内部接続 - セッションの信頼性が無効				1494
内部接続 - HDX Direct または SSL VDA				443
外部接続 - NetScaler Gateway			NetScaler Gateway のパブリック IP アドレス	443
外部接続 - Citrix Gateway Service			Citrix Gateway サービス	443

注:

Citrix Gateway Service を使用している場合、クライアントは `<https://*.*.nssvc.net>` に到達できる必要があります。`<https://*.*.nssvc.net>` を使用してすべてのサブドメインを許可できない場合は、代わりに `<https://*.c.nssvc.net>` と `<https://*.g.nssvc.net>` を使用できます。詳細については、Knowledge Center の記事 CTX270584 を参照してください。

適応型データ転送

Enlightened Data Transport (EDT) は、ユーザーデータグラムプロトコル (UDP) 上に構築されたCitrix独自のトランスポートプロトコルです。困難な長距離接続で優れたユーザーエクスペリエンスを提供しながら、サーバーのスケーラビリティを維持します。EDTは、信頼性の低いネットワー

ク上のすべてのICA®仮想チャネルのデータスループットを向上させ、より良く、より一貫したユーザーエクスペリエンスを提供します。

Adaptive Transport が有効な場合、EDTが推奨プロトコルです。

知っておくべきこと

- NetScaler® GatewayおよびCitrix Gateway Serviceで **MTU Discovery** とEDTを使用するには、**Session Reliability** を有効にする必要があります。
- パケットの断片化は、パフォーマンスの低下や、場合によってはセッションを開けない原因となることがあります。これを防ぐには、EDT MTUをネットワークに適した値に調整する必要があります。EDT MTU Discoveryを使用するか、非標準MTUのネットワークでEDTを使用する場合のMSSの構成方法に記載されている手動による回避策を使用できます。
- NetScaler GatewayでEDTの使用を有効にする方法の詳細については、NetScaler GatewayでEnlightened Data Transportをサポートするように構成するを参照してください。

EDT MTU検出

MTU Discoveryにより、EDTはセッションを確立する際に最大転送ユニット (MTU) を自動的に決定できます。これにより、パフォーマンスの低下やセッションの確立失敗につながる可能性のあるEDTパケットの断片化を防ぎます。

MTU Discoveryはデフォルトで有効になっています。無効にする必要がある場合は、詳細についてレジストリで管理されるHDX機能を参照してください。

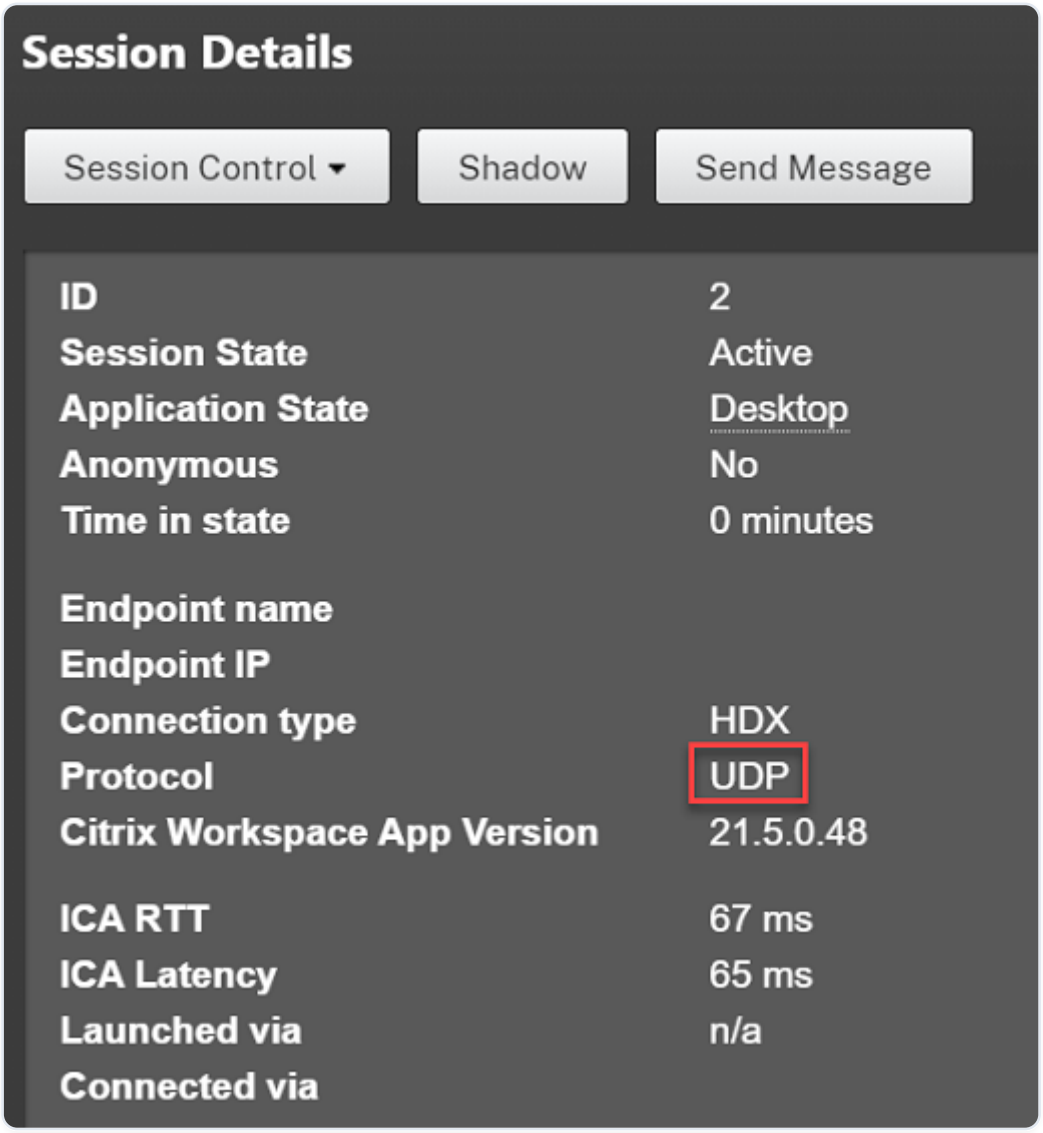
非対称パスを介した動的ルーティングによりセッションのMTUが変更される可能性があるシナリオでは、MTU DiscoveryはセッションのMTUを検出してそれに応じて調整することもできます。再検出はデフォルトで無効になっています。有効にするには、レジストリで管理されるHDX機能を参照してください。

> **注:**
>
> - MTU Discoveryが機能するには、**Session Reliability** を有効にする必要があります。
> - Multi-Stream ICAでのMTU Discoveryは、VDAバージョン2209以降で利用可能です。

トラブルシューティング

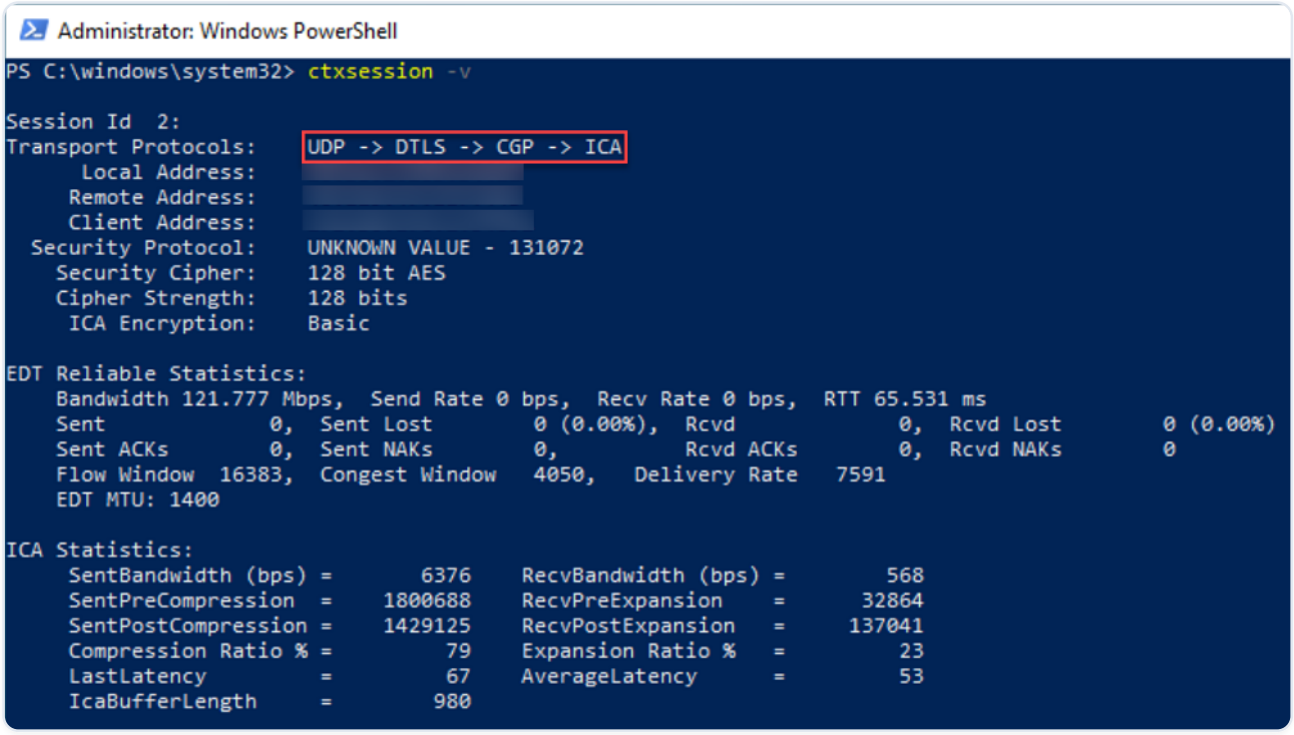
セッションのトランスポートプロトコルとしてEDTが使用されていることを確認するには、DirectorまたはVDA上の `CtxSession.exe` コマンドラインユーティリティを使用できます。

Directorでセッションを検索し、**詳細**を選択します。**接続の種類**が`HDX™`で**プロトコル**が`UDP`の場合、EDTがセッションのトランスポートプロトコルとして使用されています。



CtxSession.exeユーティリティを使用するには、セッション内でコマンドプロンプトまたはPowerShellを起動し、`ctxsession.exe`を実行します。詳細な統計情報を表示するには、`ctxsession.exe -v`を実行します。EDTが使用されている場合、トランスポートプロトコルは次のいずれかを表示します。

- **UDP > ICA®** (セッションの信頼性が無効)
- **UDP > CGP > ICA** (セッションの信頼性が有効)
- **UDP > DTLS > CGP > ICA** (ICAはDTLSでエンドツーエンド暗号化されています)



EDTでセッションが接続に失敗する場合

アダプティブトランスポートと**EDT**のトラブルシューティングを行うには、次の事項をお勧めします。

1. システム要件、ネットワーク要件、既知の問題、および注意事項を確認し、すべての項目が対処されていることを確認してください。
2. StudioまたはGPOにCitrix®ポリシーがあり、目的の**HDXアダプティブトランスポート**設定を上書きしていないか確認します。
3. クライアントに、目的のHDXアダプティブトランスポート設定を上書きする設定がないか確認します。これは、GPO設定、オプションのWorkspaceアプリ管理用テンプレートを使用して構成された設定、またはレジストリやクライアントの構成ファイルでの**HDXoverUDP**設定の手動構成である可能性があります。
4. マルチセッションVDAマシンでは、UDPリスナーがアクティブであることを確認します。VDAマシンでコマンドプロンプトを開き、`netstat -a -p udp`を実行します。詳しくは、HDX Enlightened Data Transportプロトコルを確認する方法を参照してください。
5. ネットワークファイアウォールとVDAマシン上で実行されているファイアウォールの両方で、適切なファイアウォールルールが構成されているか確認します。
6. NetScaler® GatewayまたはCitrix Gateway Serviceをバイパスして、内部で直接セッションを起動し、使用中のプロトコルを確認します。セッションがEDTを使用している場合、VDAはNetScaler GatewayまたはCitrix Gateway Serviceを介した外部接続にEDTを使用する準備ができています。

7. EDTが直接内部接続では機能するが、NetScaler GatewayまたはCitrix Gateway Serviceを介するセッションでは機能しない場合：

   - **セッションの信頼性**が有効になっていることを確認します。
   - NetScaler Gatewayを使用している場合は、Enlightened Data TransportおよびHDX Insightをサポートするように NetScaler Gatewayを構成するに記載されている必要な構成に準拠していることを確認してください。

8. Citrix Gateway Serviceを使用している場合は、Rendezvousが有効になっていて機能していることを確認します。
9. ユーザーの接続に非標準のMTUが必要かどうかを確認します。実効MTUが1500バイト未満の接続では、EDTパケットの断片化が発生し、パフォーマンスに影響を与えたり、セッション起動の失敗を引き起こしたりする可能性があります。この問題は、VPN、一部のWi-Fiアクセスポイント、および4Gや5Gなどのモバイルネットワークを使用する場合によく発生します。MTU検出が有効になっているか、非標準MTUのネットワークでEDTを使用する場合のMSSの構成方法に記載されているようにカスタムMTUを設定していることを確認してください。

既知の問題

- 非対称ネットワークパスは、NetScaler GatewayまたはCitrix Gateway Serviceを介さない接続でMTU検出が失敗する原因となる可能性があります。この問題に対処するには、VDAバージョン2103以降にアップグレードしてください。
- NetScaler Gatewayを使用している場合、非対称ネットワークパスがMTU検出の失敗を引き起こす可能性があります。これは、Gatewayの問題により、EDTパケットヘッダーのDon't Fragment（DF）ビットが伝播されないためです。この問題の修正は、ファームウェアリリース13.1ビルド17.42以降で利用可能です。修正を有効にする方法の詳細については、NetScaler Gatewayのドキュメントを参照してください。
- DS-Liteネットワークを介して接続するユーザーの場合、MTU検出が失敗することがあります。一部のモデムでは、パケット処理が有効になっている場合にDFビットが尊重されず、MTU検出が断片化を検出できなくなります。この状況では、以下のオプションが利用可能です。

  - ユーザーのモデムでパケット処理を無効にします。
  - **MTU検出**を無効にし、非標準MTUのネットワークでEDTを使用する場合のMSSの構成方法に記載されているようにハードコードされたMTUを使用します。
  - セッションにTCPの使用を強制するために**アダプティブトランスポート**を無効にします。ユーザーの一部のみが影響を受ける場合は、他のユーザーがEDTを引き続き使用できるように、クライアント側で無効にすることを検討してください。

HDX™ ダイレクト

Citrixが提供するリソースにアクセスする場合、HDX Directにより、直接通信が可能な場合は内部および外部のクライアントデバイスの両方がセッションホストと安全な直接接続を確立できます。

システム要件

HDX Directを使用するためのシステム要件は以下のとおりです。

- コントロールプレーン
  - シトリックス ダーズ™
  - シトリックス バーチャル アプリケーションズ アンド デスクトップス™ 2503 以降
- 仮想配信エージェント (VDA)
  - Windows: バージョン 2503 以降
- Workspaceアプリ
  - Windows: バージョン 2503 以降
  - Linux: バージョン 2411 以降
  - Mac: バージョン 2411 以降
- アクセス層
  - シトリックス ワークスペース™
  - シトリックス Storefront™ 2503 以降
  - Citrix Gateway サービス
  - シトリックス NetScaler® ゲートウェイ

ネットワーク要件

HDX Direct を使用するためのネットワーク要件は以下のとおりです。

セッションホスト

セッションホストに Windows Defender ファイアウォールなどのファイアウォールがある場合、内部接続のために以下の受信トラフィックを許可する必要があります。

説明	送信元	プロトコル	ポート
直接内部接続	クライアント	TCP	443
直接内部接続	クライアント	UDP	443

注:

VDA インストーラーは、Windows Defender ファイアウォールに適切な受信規則を追加します。別のファイアウォールを使用する場合は、上記の規則を追加する必要があります。

クライアントネットワーク

以下の表は、内部および外部ユーザー向けのクライアントネットワークについて説明しています。

内部ユーザー

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
直接内部接続	TCP	クライアントネットワーク	1024–65535	VDAネットワーク	443
直接内部接続	UDP	クライアントネットワーク	1024–65535	VDAネットワーク	443

外部ユーザー

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
STUN (外部ユーザーのみ)	UDP	クライアントネットワーク	1024–65535	インターネット (下記の注記を参照)	3478, 19302
外部ユーザー接続	UDP	クライアントネットワーク	1024–65535	データセンターのパブリックIPアドレス	1024–65535

データセンターネットワーク

以下の表は、内部ユーザーと外部ユーザー向けのデータセンターネットワークについて説明しています。

内部ユーザー

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
直接内部接続	TCP	クライアントネットワーク	1024–65535	VDAネットワーク	443
直接内部接続	UDP	クライアントネットワーク	1024–65535	VDAネットワーク	443

外部ユーザー

説明	プロトコル	ソース	ソースポート	宛先	宛先ポート
STUN (外部ユーザーのみ)	UDP	VDAネットワーク	1024–65535	インターネット (下記の注記を参照)	3478, 19302
外部ユーザー接続	UDP	DMZ / 内部ネットワーク	1024–65535	VDAネットワーク	55000–55250
外部ユーザー接続	UDP	VDAネットワーク	55000–55250	クライアントのパブリックIP	1024–65535

注:

VDAとWorkspaceアプリの両方が、以下のサーバーに同じ順序でSTUNリクエストを送信しようとします。

- stun.cloud.com:3478

- stun.cloudflare.com:3478
- stun.l.google.com:19302

HDX Directポート範囲ポリシー設定を使用して外部ユーザー接続のデフォルトポート範囲を変更する場合、対応するファイアウォール規則はカスタムポート範囲と一致する必要があります。

構成

HDX Directはデフォルトで無効になっています。この機能は、Citrixポリシーの**HDX Direct**設定を使用して構成できます。

- **HDX Direct**: 機能を有効または無効にするため。
- **HDX Directモード**: **HDX Direct**が内部クライアントのみで利用可能か、内部クライアントと外部クライアントの両方で利用可能かを決定します。
- **HDX Directポート範囲**: VDAが外部クライアントからの接続に使用するポート範囲を定義します。

必要に応じて、HDX Directで使用されるSTUNサーバーのリストは、以下のレジストリ値を編集することで変更できます。

- キー：HKLM\SOFTWARE\Citrix\HDX-Direct
- 値の型: REG_MULTI_SZ
- 値の名前：STUNServers
- データ：stun.cloud.com:3478 stun.cloudflare.com:3478 stun.l.google.com:19302

注：

外部ユーザー向けのHDX Directは、トランスポートプロトコルとしてEDT (UDP) を使用する場合にのみ利用可能です。したがって、アダプティブトランスポート を有効にする必要があります。

考慮事項

HDX Directを使用する際の考慮事項は次のとおりです。

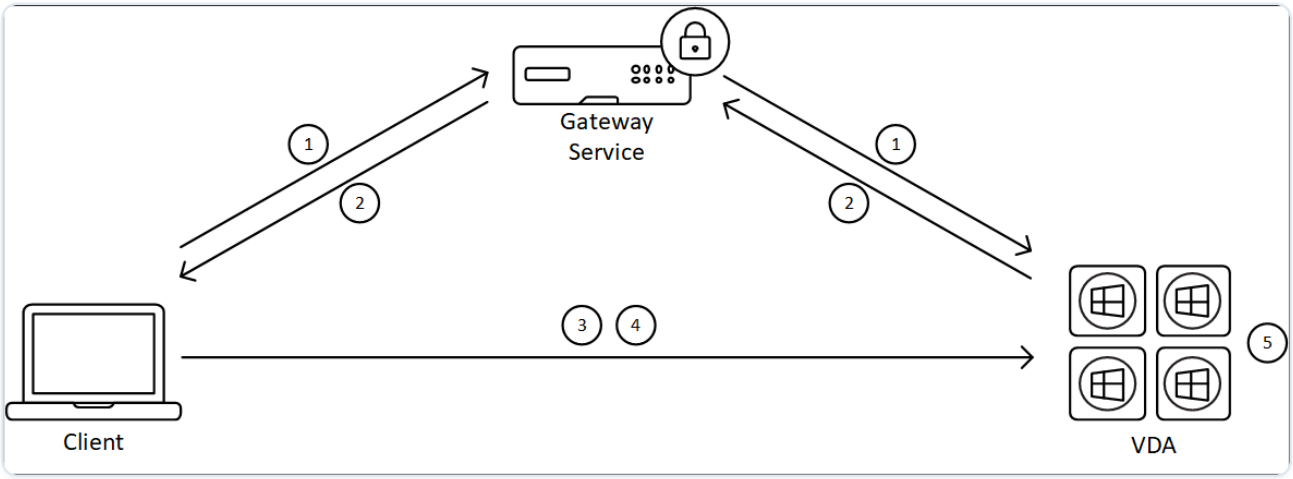
- 外部ユーザー向けのHDX Directは、トランスポートプロトコルとしてEDT (UDP) を使用する場合にのみ利用可能です。したがって、**アダプティブトランスポート**を有効にする必要があります。
- **HDX Insight**を使用している場合、**HDX Direct**を使用すると、セッションがNetScaler Gatewayを介してプロキシされなくなるため、HDX Insightのデータ収集が妨げられることに注意してください。

動作の仕組み

HDX Directを使用すると、直接通信が可能な場合にクライアントがセッションホストへの直接接続を確立できます。HDX Directを使用して直接接続が行われる場合、自己署名証明書が使用され、ネットワークレベルの暗号化 (TLS/DTLS) で直接接続を保護します。

内部ユーザー

次の図は、内部ユーザーのHDX Direct接続プロセスの概要を示しています。



1. クライアントはGateway Serviceを介してHDXセッションを確立します。
2. 接続が成功すると、VDAはHDX接続を介して、VDAマシンのFQDN、そのIPアドレスのリスト、およびVDAマシンの証明書をクライアントに送信します。
3. クライアントはIPアドレスをプローブし、VDAに直接到達できるかを確認します。
4. クライアントが共有されたいずれかのIPアドレスでVDAに直接到達できる場合、クライアントはVDAとの直接接続を確立します。この接続は、ステップ(2)で交換された証明書と一致する証明書を使用して(D)TLSで保護されます。
5. 直接接続が正常に確立されると、セッションは新しい接続に転送され、Gateway Serviceへの接続は終了します。

> **注:**

> 上記のステップ2で接続を確立した後、セッションはアクティブになります。その後の手順は、ユーザーが仮想アプリケーションまたはデスクトップを使用する能力を遅らせたり、妨げたりすることはありません。その後の手順のいずれかが失敗した場合でも、ユーザーのセッションを中断することなく、Gatewayを介した接続は維持されます。

従来の直接接続

Storefront、Direct Workload Connectionを備えたWorkspace、または内部専用接続用に構成されたWorkspaceを使用する場合、まずGatewayを介してルーティングする必要なく、クライアントとセッションホスト間で直接接続が確立されます。

これらの場合、接続は本質的に直接的であるため、HDX Directはトリガーされません。ただし、HDX Directが有効になっている場合、これらの接続はHDX Direct証明書を利用してセッションを保護します。

外部ユーザー

次の図は、外部ユーザー向けのHDX Direct接続プロセスの概要を示しています。

HDX Direct接続プロセス(/en-us/citrix-virtual-apps-desktops/2511/media/hdx-direct-connection-process.png)

1. クライアントはGateway Serviceを介してHDXセッションを確立します。
2. 接続が成功すると、クライアントとVDAの両方がSTUNリクエストを送信し、それぞれのパブリックIPアドレスとポートを検出します。
3. STUNサーバーはクライアントとVDAに応答し、それぞれのパブリックIPアドレスとポートを返します。
4. HDX接続を介して、クライアントとVDAはそれぞれのパブリックIPアドレスとUDPポートを交換し、VDAは証明書をクライアントに送信します。
5. VDAはクライアントのパブリックIPアドレスとUDPポートにUDPパケットを送信します。クライアントはVDAのパブリックIPアドレスとUDPポートにUDPパケットを送信します。
6. VDAからのメッセージを受信すると、クライアントはセキュアな接続要求で応答します。
7. DTLSハンドシェイク中に、クライアントは証明書がステップ(4)で交換された証明書と一致することを確認します。検証後、クライアントは認証トークンを送信します。これでセキュアな直接接続が確立されます。
8. 直接接続が正常に確立されると、セッションは新しい接続に転送され、Gateway Serviceへの接続は終了します。

> **注:**
>
> 上記のステップ2で接続が確立された後、セッションはアクティブになります。その後の手順は、ユーザーが仮想アプリケーションまたはデスクトップを使用する能力を遅らせたり、妨げたりすることはありません。その後の手順のいずれかが失敗した場合でも、Gatewayを介した接続はユーザーのセッションを中断することなく維持されます。

証明書管理

概要

HDX™ Direct接続は、ネットワークレベルの暗号化によって保護されています。これを容易にするため、各セッションホストは一意の自己署名ルートCA証明書と、その自己署名ルートCA証明書によって署名された対応するサーバー証明書を持っています。

このソリューションには、次の利点があります。

- **セキュリティの合理化:** HDX Direct接続は、環境内で証明書を管理する管理上のオーバーヘッドなしに保護されます。
- **攻撃対象領域の削減:** 各ホストは一意のキーと証明書のセットを持つため、攻撃対象領域は単一のホストに限定されます。
- **非永続環境のセキュリティ強化:** 非永続セッションホストを持つ環境では、再起動時に新しいキーと証明書が生成されるため、セキュリティがさらに強化されます。

セッションホスト

Citrix ClxMtp Service と **Citrix Certificate Manager Service** は、各セッションホストで証明書を管理する責任を負う2つのサービスです。ClxMtp Serviceはキーの生成とローテーションを処理し、Certificate Manager Serviceは証明書を生成および管理します。

自己署名ルートCAとサーバー証明書の2つの証明書が作成されます。どちらも2年間の有効期間で発行されますが、キーがローテーションされると置き換えられます。さらに、非永続マシンが再起動するたびに新しい証明書が生成されます。

各証明書の詳細は次のとおりです。

- **自己署名ルートCA**
  - 証明書発行先: CA-Citrix-Certificate-Manager
  - 証明書発行元: CA-Citrix-Certificate-Manager

- 発行者詳細: 組織はCitrix Systems, Inc.です。

- **サーバー証明書**
  - 発行先: \<ホストFQDN\> (例: FTLW11-001.ctxlab.net)
  - 発行元はCA-Citrix-Certificate-Managerです。
  - 発行者の詳細: 組織はCitrix Systems, Inc.です。

> **注：**
>
> Citrix Certificate Manager Serviceは、2048ビットキーを利用するRSA証明書を生成します。
>
> Citrix Certificate Manager Serviceによって作成された既存のマシン証明書があり、サブジェクト名がマシンのFQDNと一致しない場合、新しい証明書が生成されます。

キーのローテーション

Citrix ClxMtp Serviceは、6か月ごとにキーを自動的にローテーションします。ただし、セッションホストのレジストリでローテーションカウンターを増やすことで、手動でキーのローテーションをトリガーできます。

キーをローテーションするには、次の値を更新します。

- キー: SOFTWARE\Citrix\ClxMtpConnectorSvcRotateKeyPairs
- 値の型: DWORD
- 値の名前: ClxMtpRotateRequestCounter
- データ: 整数 (10進数)

> **注：**
>
> 初めてキーをローテーションする場合:
>
> 1. ClxMtpConnectorSvcRotateKeyPairsキーを作成します。
> 2. ClxMtpRotateRequestCounter値を1に作成して設定します。

その後のキーのローテーションでは、ClxMtpRotateRequestCounter値を1増やします。

値が更新されると、**Citrix ClxMtp Service**は再起動を必要とせずにキーを自動的にローテーションします。その後、**Citrix Certificate Manager Service**は新しいキーを検出すると、自動的に新しい証明書を生成します。

クライアントデバイス

ルートCA証明書は、確立済みの安全で信頼された接続パスを介して、WorkspaceまたはStorefront™によってクライアントに送信されます。これにより、CA証明書をクライアントデバイスの証明書ストアに配布する必要がなくなり、クライアントがHDX Direct接続を保護するために使用される証明書を信頼することが保証されます。

カスタム証明書の使用

HDX Directは、独自のPKIによって発行および管理される証明書の使用をサポートしています。以下の手順では、証明書のインストール方法、必要な権限の構成方法、セッションマネージャーサービスへのバインド方法、および必要なTLSリスナーの有効化方法について説明します。

1. マシンでHDX Directが無効になっている場合は、手順2に進みます。HDX Directが有効になっている場合は、以下の手順に従います。
    a. レジストリエディター (regedit.exe) を開き、**HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd** に移動します。
    b. **SSLEnabled** の値を **0** に設定します。
    c. **HKLM\Software\Citrix\HDX-Direct** に移動します。
    d. **HdxDirectCaInTls** の値を **0** に設定します。
2. PKIによって発行された適切な証明書を、マシンの証明書ストアにインストールします。
3. セッションマネージャーサービスに、証明書の秘密キーへの読み取りアクセス権を付与します。
    a. Microsoft 管理コンソール (**MMC**) を起動します: > > mmc.exe。
    b. **>** に移動します。
    c. を選択し、 をクリックします。
    d. を選択し、 をクリックします。
    e. を選択し、 をクリックします。
    f. **> >** に移動します。

g. 適切な証明書を右クリックし、 **>** を選択します。

h. 次のいずれかのサービスを追加し、読み取りアクセス権を付与します。

- **シングルセッションVDA**の場合: `NT SERVICE\PorticaService`
- **マルチセッションVDA**の場合: `NT SERVICE\TermService`

i. をクリックし、次に をクリックします。

4. 証明書をセッションマネージャーサービスにバインドします。

a. 証明書のサムプリントを取得します (証明書をダブルクリック > >)。

b. レジストリエディター (regedit.exe) を開き、**HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd** に移動します。

c. **SSLThumbprint** の値を編集し、証明書のサムプリントを貼り付けます。

5. Citrix TLS リスナーを有効にします。

a. 同じレジストリの場所で、**SSLEnabled** の値を **1** に設定します。

6. HDX Direct を有効にします（Citrix ポリシー 内）。

Citrix Virtual Apps and Desktops のインストールメディアには、これらのタスクのいくつかを自動化する PowerShell スクリプト (Enable-VdaSSL.ps1) が含まれています。

- 証明書のキーのアクセス許可を設定する
- 証明書をセッションマネージャーサービスにバインドする
- Citrix TLS リスナーを有効にする

このスクリプトは、Support > Tools > SslSupport ディレクトリにあります。詳細については、「PowerShell スクリプトを使用して VDA で TLS を構成する」を参照してください。

> **注：**
>
> 独自の証明書を使用している場合、セッションホストに接続するデバイスには、正しいルート CA 証明書と中間 CA 証明書がインストールされている必要があります。

NAT互換性

外部ユーザーデバイスとセッションホスト間の直接接続を確立するために、HDX™ DirectはNATトラバーサルのためにホールパンチングを利用し、クライアントデバイスとセッションホストのパブリックIPアドレスおよびポートマッピングの交換を容易にするためにSTUNを利用します。これは、VoIP、ユニファイドコミュニケーション、P2Pソリューションの仕組みに似ています。

ファイアウォールやその他のネットワークコンポーネントが、STUNリクエストおよびHDXセッションのUDPトラフィックを許可するように構成されている限り、外部ユーザー向けのHDX Directは機能すると予想されます。ただし、ユーザーとセッションホストのネットワークのNATタイプが互換性のない組み合わせになり、HDX Directが失敗する特定のシナリオがあります。

検証

クライアントおよびセッションホスト上のNATタイプとフィルタリングは、STUNTMANのSTUNクライアントユーティリティを使用して検証できます。

1. stunprotocol.orgからターゲットプラットフォームに適したパッケージをダウンロードし、内容を抽出します。
2. ターミナルプロンプトを開き、内容が抽出されたディレクトリに移動します。
3. NATバインディングおよび動作テストを実行するには、次のコマンドを実行します。
   `stunclient.exe stunserver2025.stunprotocol.org --mode behavior`
4. バインディングテストと動作テストが成功した場合、**binding test**と**behavior test**の両方が成功を報告し、NATの動作が指定されます。



テストが失敗した場合、**binding test**および/または**behavior test**が失敗を報告します。



5. NATバインディングおよびフィルタリングテストを実行するには、次のコマンドを実行します。 `stunclient.exe stunserver2025.stunprotocol.org --mode filtering`
6. バインディングテストとフィルタリングテストが成功した場合、**binding test**と**filtering test**の両方が成功を報告し、NATフィルタリングタイプが指定されます。

テストが失敗した場合、**binding test**および/または**filtering test**が失敗を報告します。

上記のテストを実行した後、以下の表を確認して、NATの動作とフィルタリングの組み合わせに基づいて、外部ユーザー向けのHDX Directが機能すると予想されるかどうかを判断してください。

クライアントNATの動作	クライアントNATフィルタリング	セッションホストNATの動作	セッションホストNATフィルタリング	動作すると予想されますか？
エンドポイント独立マッピング	任意	エンドポイント独立マッピング	任意	はい
エンドポイント独立マッピング	エンドポイント独立フィルタリング	アドレス依存マッピング	任意	はい
エンドポイント独立マッピング	アドレス依存フィルタリング	アドレス依存マッピング	任意	いいえ
エンドポイント独立マッピング	アドレスおよびポート依存フィルタリング	アドレス依存マッピング	任意	いいえ
エンドポイント独立マッピング	エンドポイント独立フィルタリング	アドレスおよびポート依存マッピング	エンドポイント独立フィルタリング	はい
エンドポイント独立マッピング	アドレス依存フィルタリング	アドレス依存マッピング	任意	いいえ
エンドポイント独立マッピング	アドレスおよびポート依存フィルタリング	アドレス依存マッピング	任意	いいえ
アドレス依存マッピング	任意	エンドポイント独立マッピング	エンドポイント独立フィルタリング	はい
アドレス依存マッピング	任意	エンドポイント独立マッピング	アドレス依存フィルタリング	いいえ
アドレス依存マッピング	任意	エンドポイント独立マッピング	アドレスおよびポート依存フィルタリング	いいえ

クライアントNATの動作	クライアントNATフィルタリング	セッションホストNATの動作	セッションホストNATフィルタリング	動作すると予想されますか？
アドレス依存マッピング	任意	アドレス依存マッピング	任意	いいえ
アドレス依存マッピング	任意	アドレスおよびポート依存マッピング	任意	いいえ
アドレスおよびポート依存マッピング	任意	エンドポイント独立マッピング	エンドポイント独立フィルタリング	はい
アドレスおよびポート依存マッピング	任意	エンドポイント独立マッピング	アドレス依存フィルタリング	なし
アドレスおよびポート依存マッピング	任意	エンドポイント独立マッピング	アドレスおよびポート依存フィルタリング	なし
アドレスおよびポート依存マッピング	任意	アドレス依存マッピング	任意	なし
アドレスおよびポート依存マッピング	任意	アドレスおよびポート依存マッピング	任意	なし
失敗	任意	任意	任意	なし
任意	任意	失敗	任意	なし
失敗	任意	失敗	任意	いいえ

トラブルシューティング

HDX Direct が直接接続を正常に確立したことを確認するには、VDA マシンで `CtxSession.exe` ユーティリティを使用できます。

`CtxSession.exe` ユーティリティを使用するには、セッション内でコマンドプロンプトまたは PowerShell を起動し、`ctxsession.exe -v` を実行します。**HDX Direct** 接続が正常に確立された場合、**HDX Direct Status** は `Connected` です。

HDX Direct のトラブルシューティング(/en-us/citrix-virtual-apps-desktops/2511/media/hdx-direct-troubleshooting.png)

セッションホストのイベントログで、HDX™ Direct 接続が正常に確立されたか、失敗したかに関する情報を確認することもできます。詳細については、「**イベントログ**」セクションを参照してください。

> 注:
>
> 環境とセッションホストで利用可能な IP アドレスの数によっては、HDX Direct 接続が確立されるまでに最大 5 分かかる場合があります。

HDX Direct が直接接続を確立できない場合

HDX Direct が直接接続を確立できない場合は、次の手順を確認してください。

1. 使用している VDA バージョンと Workspace アプリバージョンが、システム要件に従ってこの機能をサポートしていることを確認してください。
2. HDX Direct を有効にするポリシーが VDA に適用されており、この機能を無効にする優先度の高い他のポリシーがないことを確認してください。
3. 目的の HDX Direct モードを設定するポリシーが VDA に適用されており、この構成を上書きする優先度の高い他のポリシーがないことを確認してください。
4. Citrix ClxMtp Service がセッションホストで実行されていることを確認してください。
5. Citrix Certificate Manager Service がセッションホストで実行されていることを確認してください。実行されていない場合は、手動で起動してみてください。HDX Direct が無効になっている場合、このサービスは自動的に停止します。
6. セッションホストに自己署名ルート CA 証明書があるかどうかを確認してください。
    a. 発行先: `CA-Citrix-Certificate-Manager`
    b. 発行元: `CA-Citrix-Certificate-Manager`
    c. 発行者の詳細: 組織はCitrix Systems, Inc.です。
7. セッションホストに自己署名サーバー証明書があるか確認します。

a. 発行先: `<host FQDN>` (例: FTLW11-001.ctxlab.net)

b. 発行元: `CA-Citrix-Certificate-Manager`

c. 発行者情報: 組織はCitrix Systems, Inc.です。

8. 証明書が見つからない場合は、Citrixテクニカルサポートにお問い合わせください。
9. 証明書が存在する場合:

a. セッションホストでCitrix Certificate Manager Serviceを停止します。

b. 自己署名ルートCA証明書と自己署名サーバー証明書の両方を削除します。

c. セッションホストでCitrix Certificate Manager Serviceを開始します。サービスは開始されると新しい証明書を作成します。

10. 内部ユーザーの場合:

a. セッションホストのファイアウォールが、HDX over EDTおよびHDX over TCPの場合に、それぞれUDP 443またはTCP 443の受信トラフィックをブロックしていないことを確認してください。

b. ネットワークファイアウォールが、クライアントネットワークとセッションホストネットワーク間のUDP 443およびTCP 443のトラフィックをブロックしていないことを確認してください。

11. 外部ユーザーの場合：

a. セッションホストにSTUNサーバーのリストが含まれていることを確認します。

- キー: HKLM\SOFTWARE\Citrix\HDX-Direct
- 値の型: REG_MULTI_SZ
- 値の名前: STUNServers
- データ: stun.cloud.com:3478 stun.cloudflare.com:3478 stun.l.google.com:19302

b. クライアントとセッションホストのNATタイプを確認し、その組み合わせが正常に機能することを確認します。詳細については、「NAT互換性」セクションを参照してください。

c. クライアントまたはセッションホストのいずれかでNATテストが失敗した場合:

i. システムでファイアウォールが実行されている場合は、UDP 3478での送信トラフィックをブロックしていないことを確認してください。

ii. ネットワークファイアウォールがUDP 3478での送信トラフィックをブロックしていないことを確認してください。

iii. ファイアウォールがSTUNサーバーの応答をブロックしていないことを確認してください。

d. ネットワークファイアウォールに、必要なすべてのトラフィックを許可するための適切なルールが構成されていることを確認してください。詳細については、「ネットワーク要件」セクションを参照してください。

e. HDX Directポート範囲ポリシー設定を使用してデフォルトのポート範囲を変更する場合は、ファイアウォールルールがカスタムポート範囲に設定されていることを確認してください。

イベントログ

以下のイベントがVDAマシンのイベントログに記録されます:

ログ	ID	送信元	レベル	説明
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/Operational	1	HDX ダイレクト	情報	`<username>` 内部ユーザーのHDX Direct接続が確立されました。
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/Operational	2	HDX ダイレクト	情報	`<username>` 外部ユーザーのHDX Direct接続が確立されました。
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/オペレーション	3	HDX ダイレクト	情報	ユーザー `<username>` のHDX Direct接続に失敗しました。
アプリケーションとサービスログ > Citrix-HostCore-HDX	4	HDX ダイレクト	情報	STUNサーバー `<URL:PORT>` は、ユーザー `<username>` のセッションホストIPおよび

ログ	ID	送信元	レベル	説明
Direct/オペレーション				ポートマッピングとして、以下を提供しました: `<IP>:<PORT>` 。
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/オペレーション	5	HDX ダイレクト	情報	ユーザー `<username>` のセッションホストは、設定されたSTUNサーバーのいずれからも応答を受信しませんでした。
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/ Operational	6	HDXダイレクト	情報	クライアントは、ユーザー `<username>` の外部マッピングとして `<IP>:<PORT>` を提供しました。
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/ Operational	7	HDXダイレクト	情報	クライアントは、ユーザー `<username>` の外部マッピングを提供しませんでした。

既知の問題

- Rendezvousが無効になっている場合、Gateway Serviceを使用するWorkspace環境では、外部ユーザー向けのHDX Directが失敗する可能性があります。この問題を解決するには、Rendezvous が有効になっていることを確認してください。

- **HDX Direct** がすでに有効になっているマシンでVDAのインプレースアップグレードを実行すると、HDX Directが動作しなくなる場合があります。この問題を解決するには、次の手順を実行してください。

  a. セッションホスト上でCitrix Certificate Manager Serviceを停止します。
  b. 自己署名ルートCA証明書と自己署名サーバー証明書を削除します。
  c. レジストリを開きます。
  d. `HKLM\Software\Citrix\HDX-Direct` キーを削除します。
  e. `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd` にアクセスします。
  f. **SSLEnabled** の値を `0` に設定します。
  g. **SSLThumbprint** の値の内容を削除します。
  h. **Citrix Certificate Managerサービス**を開始します。

セキュアな HDX™

Secure HDXは、トラフィックパス内のネットワーク要素がHDXトラフィックを検査できないようにするアプリケーションレベル暗号化 (ALE) ソリューションです。これは、AES-256-GCM暗号化を使用して、Citrix Workspace™アプリ (クライアント) とVDA (セッションホスト) の間でアプリケーションレベルで真のエンドツーエンド暗号化 (E2EE) を提供することによって実現されます。

システム要件

以下の一覧は、Secure HDXを使用するためのシステム要件を示しています。

- コントロールプレーン
  - シトリックス DaaS™
  - シトリックス Virtual Apps and Desktops™ 2503 以降
- セッションホスト
  - オペレーティングシステム
    - Windows 10 22H2 バージョン
    - Windows 11 22H2以降
    - ウィンドウズ サーバー 2019 以降
  - バーチャル デリバリー エージェント (VDA)

    - Windows: バージョン2503以降
    - Linux: バージョン2407以降

- Workspaceアプリ
    - Windows: バージョン 2503 以降
    - Linux: バージョン 2408 以降
    - Mac: バージョン 2409 以降
    - Chrome OS: バージョン 2409 以降
    - HTML5: バージョン 2408 以降
    - Android: バージョン 2503 以降
    - iOS: バージョン 2503 以降
- アクセス層
    - シトリックス ワークスペース
    - Citrix StoreFront™ 2402 以降

> **注：**
>
> Linux VDA で Secure HDX を構成する方法の詳細については、Linux VDA のドキュメントを参照してください。

構成

Secure HDX はデフォルトで無効になっています。この機能は、Citrix ポリシーの Secure HDX 設定を使用して構成できます。

セキュアHDX: 機能の有効/無効を定義します。

> **重要:**
>
> Secure HDX を有効にするデリバリーグループで Secure ICA® が有効になっている場合は、まず Secure ICA を無効にする必要があります (デリバリーグループの編集 > ユーザー設定)。

HDXインサイトとスマートコントロール

Secure HDX が有効になっている場合に NetScaler Gateway で HDX Insight と SmartControl を使用するための要件は次のとおりです。

- NetScaler 14.1 Build 47.46 以降。
- **ネットワークテレメトリ**は Citrix ポリシーで有効にする必要があります。
- **セッションの信頼性**を有効にする必要があります。この設定はデフォルトで有効になっているため、無効にするポリシーがないことを確認してください。

> **注:**
>
> Secure HDX を使用した HDX Insight と SmartControl は、次のシナリオでのみ利用可能です。
>
> - 転送プロトコルとして TCP を使用する接続
> - IPv4 を使用する接続
> - 次の Workspace アプリバージョンを使用するクライアント:
>   - Windows: 2503 以降
>   - Mac: 2505 以降
>   - Linux: 2508 以降

考慮事項

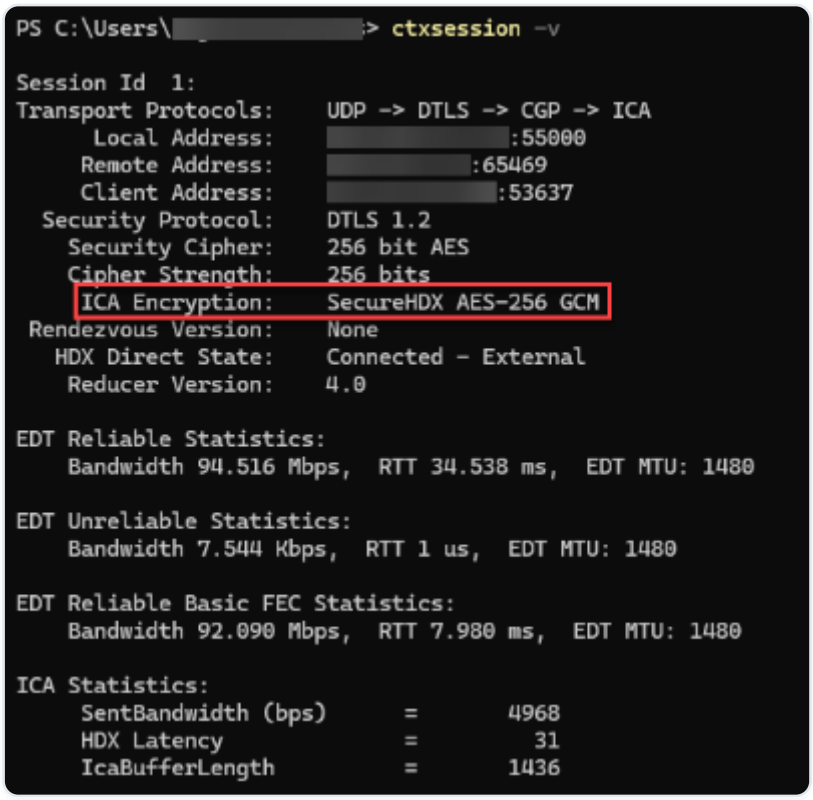
Secure HDX を使用する際の考慮事項は次のとおりです。

- ユーザーが Secure HDX が有効なセッションホストに、その機能をサポートしないクライアントを使用して接続しようとすると、接続は拒否されます。
- Secure HDX でサポートされるのは、コネクタレスワークロードのサービス継続性 のみです。標準バージョンのサービス継続性を使用している場合、クラウドサービスの停止が発生すると、Secure HDX が有効になっているセッションホストには接続できません。
- Secure HDX が有効になっている場合、Multi-Stream ICA はサポートされません。
- HDX トラフィックの検査に依存するサードパーティ製ソリューションを使用している場合、Secure HDX を有効にすると HDX トラフィックが暗号化されるため、それらのソリューションは機能しなくなります。

トラブルシューティング

Secure HDX がアクティブであることを確認するには、VDA マシンで `ctxsession.exe` ユーティリティを使用します。

`CtxSession.exe`ユーティリティを使用するには、セッション内でコマンドプロンプトまたはPowerShellを開き、`ctxsession.exe -v`を実行します。Secure HDXが使用されている場合、ICA Encryptionには`SecureHDX AES-256 GCM`と表示されます。



セッションでSecure HDXが有効にならない場合

- 使用中のVDAバージョンがシステム要件に従ってこの機能をサポートしていることを確認してください。
- Secure HDX を有効にするポリシーが VDA に適用されており、その機能を無効にする優先度の高い他のポリシーがないことを確認してください。
- Secure HDXを構成したときにセッションホストがすでに実行されていた場合は、変更を有効にするためにマシンを再起動してください。

ネットワーク テレメトリ

ネットワークメトリックは、Citrixセッションのトラブルシューティングにとって重要です。なぜなら、Citrixセッションのパフォーマンスと安定性は、基盤となるネットワークの状態に大きく依存しているからです。ローカルアプリケーションとは異なり、Citrixセッションはインタラクティ

ブなデスクトップまたはアプリケーションのエクスペリエンスをネットワーク経由でストリーミングします。これは、ネットワークの不安定性やボトルネックがユーザーのパフォーマンス認識に直接影響することを意味します。

Citrix MonitorおよびDirectorで利用可能なネットワークメトリックの詳細については、「セッションパフォーマンスの問題の診断」を参照してください。

システム要件

ネットワークテレメトリを使用するためのシステム要件は次のとおりです。

- コントロールプレーン
  - シトリックス DaaS
  - シトリックス バーチャルアプリおよびデスクトップ 2503以降
- バーチャル デリバリー エージェント (VDA)
  - Windows: バージョン2503以降
  - Linux: バージョン2507以降
  - Mac: バージョン2507以降
- Workspaceアプリ
  - Windows: バージョン2503以降
  - Linux: バージョン2508以降
  - Mac: バージョン 2505 以降
- アクセス層
  - シトリックス ワークスペース
  - シトリックス ストアフロント 2402 以降
  - シトリックス ゲートウェイ サービス
  - シトリックス ネットスケーラー ゲートウェイ 14.1 ビルド 47.46 以降

ネットワーク要件

Citrix Gateway Service を使用している場合、追加のネットワーク要件はありません。ただし、NetScaler Gateway を使用している場合は、ネットワークテレメトリを使用するための追加要件があり、それらを以下に示します。

セッションホスト

セッションホストに Windows Defender ファイアウォールなどのファイアウォールがある場合、NetScaler Gateway からの接続に対して、以下の受信トラフィックを許可する必要があります。

説明	送信元	プロトコル	ポート
Gateway からの接続	NetScaler SNIP	TCP	443

> **注記:**
>
> VDA インストーラーは、Windows Defender ファイアウォールに適切な受信規則を追加します。別のファイアウォールを使用する場合は、上記の規則を追加する必要があります。

内部ネットワーク

内部ネットワークのファイアウォール要件は次のとおりです。

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
Gatewayからの接続	TCP	NetScaler SNIP	1024-65535	VDAネットワーク	443

構成

ネットワークテレメトリはデフォルトで無効になっています。この機能は、Studio の Citrix ポリシーで以下の設定を使用して構成できます。

- **ネットワークテレメトリ:** 機能の有効/無効を定義します。

考慮事項

ネットワークテレメトリを使用する際の考慮事項は次のとおりです。

- 現在、ネットワークテレメトリが有効になっている場合、NetScaler Gateway で EDT はサポートされていません。ネットワークテレメトリを有効にすると、セッションは強制的に TCP を使用します。
- ネットワークテレメトリが有効になっている場合、NetScaler Gateway から VDA への接続はネットワークレベルで暗号化されます。証明書管理の詳細については、「HDX Direct 証明書管

理」を参照してください。これは HDX Direct を有効にするものではないことに注意してください。

仮想チャネル許可リスト

仮想チャネル許可リストは、Citrix以外の仮想チャネルのうち、どれを環境で許可するかを制御できる機能です。デフォルトでは、仮想チャネル許可リスト機能は有効になっています。その結果、Citrix Virtual Apps and Desktops™セッションでは、Citrix仮想チャネルのみが開くことが許可されます。自社開発のものであっても、サードパーティ製のものであっても、カスタム仮想チャネルを使用する必要がある場合は、これらを明示的に許可リストに追加する必要があります。

構成

仮想チャネル許可リストはデフォルトで有効になっています。この機能は、Citrixポリシーの以下の設定を使用して構成できます。

- **仮想チャネル許可リスト**: この機能を有効または無効にし、仮想チャネルをリストに追加します。
- **仮想チャネル許可リストログスロットリング**: 仮想チャネル許可リストのイベントログ記録のスロットリング期間を設定します。
- **仮想チャネル許可リストログ記録**: 仮想チャネル許可リストのログ記録レベルを設定します。

仮想チャネルを許可リストに追加する

仮想チャネルを許可リストに追加するには、以下の情報が必要です。

1. コードで定義されている仮想チャネル名。これは最大7文字の長さです。例: `CTXCVC1`。
2. VDAマシン上で仮想チャネルを開くプロセスへのパス。例: `C:\Program Files\Application\run.exe`。

必要な情報が揃ったら、仮想チャネル許可リストポリシー設定を使用して仮想チャネルを許可リストに追加する必要があります。仮想チャネルをリストに追加するには、仮想チャネル名の後にコンマ、そして仮想チャネルにアクセスするプロセスへのパスを入力します。複数のプロセスがある場合は、各プロセスをコンマで区切って追加できます。

単一のプロセスの場合

前の例を使用して、以下のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe
```

複数のプロセスの場合

複数のプロセスがある場合は、次のエントリをリストに追加します。

`CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe`

ワイルドカードの使用

ワイルドカード (*) の使用がサポートされています。アプリケーションのバージョンに基づいてディレクトリ名や実行可能ファイル名が変更される場合、またはサードパーティコンポーネントがユーザーのプロファイルにインストールされている場合に、ワイルドカードを使用できます。

次のシナリオでワイルドカードを使用できます。

- 完全なディレクトリ名を置き換える場合。 例: `C:\Program Files\Application*\run1.exe`
- ディレクトリ名の一部を置き換える場合。 例: `C:\Program Files\Application\v*\run1.exe`
- 実行可能ファイル名を置き換える場合。 例: `C:\Program Files\Application\v1.2*.exe`
- 実行可能ファイル名の一部を置き換える場合。 例: `C:\Program Files\Application\v1.2\run*.exe`

次の制限が適用されます。

- ワイルドカードは、単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルが `C:\Program Files\Application\v1.2\run1.exe` にある場合
  - 許可: `C:\Program Files\Application*\run1.exe`
  - 不許可: `C:\Program Files*\run1.exe`
- エントリにはファイル名拡張子を含める必要があります。
  - 許可: `C:\Program Files\Application\v1.2*.exe`
  - 不許可: `C:\Program Files\Application\v1.2*`
- すべてのパスはローカルである必要があります。

> **注:**

- ネットワークパスは許可されていません。
- ワイルドカードのサポートは、Citrix Virtual Apps™ and Desktops 2206 から利用可能です。
- ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2203 LTSR のCU2から利用可能です。

システム環境変数の使用

システム環境変数を使用して、許可リスト内の信頼されたプロセスの定義を簡素化できます。`%programfiles%`、`%programfiles(x86)%`、`%systemdrive%`、`%systemroot%` などの、すぐに使用できる変数を使用できます。

カスタム環境変数も使用できますが、システムレベルで定義されている必要があります。

次の例は、すぐに使用できる環境変数を示しています。

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

次の例は、カスタムシステム環境変数を示しています。

- カスタム変数名: `app`
- カスタム変数値: `%programfiles%\Application\`
- 許可リストエントリ: `CTXCVC1,%app%\run.exe`

注:

ユーザー環境変数はサポートされていません。

環境変数のサポートは、Citrix Virtual Apps and Desktops バージョン 2209 以降で利用できます。

仮想チャネル名とプロセスを取得する

VDAマシン上で仮想チャネル名とそれを開くプロセスを取得する最も簡単な方法は、仮想チャネルを提供した開発者またはサードパーティベンダーから情報を入手することです。

または、機能のログを適用し、次の手順に従って情報を取得することもできます。

1. カスタム仮想チャネルのクライアントコンポーネントとサーバーコンポーネントが配置されたら、仮想アプリケーションまたは仮想デスクトップを起動します。
2. VDAマシンのシステムイベントログで、カスタム仮想チャネルの名前と、それを開こうとしたプロセスを探します。利用可能なイベントの詳細については、「イベントログ」を参照してください。
3. セッションからログアウトします。
4. 特定された仮想チャネルとプロセスについて、仮想チャネル許可リストポリシー設定にエントリを追加します。
5. マシンを再起動します。
6. VDAが登録されたら、仮想アプリケーションまたは仮想デスクトップを実行して、カスタム仮想チャネルが正常に開くことを検証します。

Citrix仮想チャネルに関する考慮事項

すべての組み込みCitrix仮想チャネルは信頼されており、追加設定なしで開くことができます。ただし、以下の2つの機能は外部依存関係があるため、許可リストに明示的なエントリが必要です。

- マルチメディアリダイレクト
- スカイプ フォー ビジネス 用 HDX RealTime Optimization Pack

マルチメディアリダイレクト

Windows Media Player以外のメディアプレーヤーをシステムメディアプレーヤーとして使用する場合、それを信頼されたプロセスとして許可リストに追加する必要があります。許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXMM`
- プロセス: VDAマシンで使用されるメディアプレーヤーへのパス。例: `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`。
- 許可リストエントリ: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

スカイプ フォー ビジネス 用 HDX RealTime Optimization Pack

許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXRMEP`

- プロセス: VDAマシン内のSkype for Business実行可能ファイルへのパス。これはSkype for Businessのバージョンやカスタムインストールパスの使用によって異なる場合があります。例: `C:\Program Files\Microsoft Office\root\Office16\lync.exe.`.
- 許可リストエントリ: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

トラブルシューティング

カスタム仮想チャネルが開かない場合は、次の手順を確認してください。

1. 正しいVDAバージョンを使用していることを確認してください。
2. 仮想チャネル許可リストにカスタム仮想チャネルを含むポリシーがVDAに適用されており、この構成を上書きする優先度の高い他のポリシーがないことを確認してください。
3. VDAのイベントログを確認し、報告されている仮想チャネル名が許可リストで定義されているものと一致することを確認してください。

    a. 複数のプロセスがある場合は、仮想チャネルを許可リストに追加するで説明されているように、これらが適切に定義されていることを確認してください。

    b. 定義されたプロセスパスでワイルドカードを使用している場合は、ワイルドカードの使用のガイドラインに従っていることを確認してください。

    c. 定義されたプロセスパスで環境変数を使用している場合は、システム環境変数の使用のガイドラインに従っていることを確認してください。

イベントログ

次のイベントがVDAマシンのイベントログに記録されます。

シングルセッションVDA

次のイベントがシングルセッションVDAマシンのイベントログに記録されます。

ログ名	ID	送信元	レベル	説明
システム	2001	`Picadd`	情報	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開かれました

ログ名	ID	送信元	レベル	説明
システム	2002	`Picadd`	警告	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開くことができません
システム	2003	`Picadd`	情報	`<username>` がカスタム仮想チャネル `<vcName>` を開きました
システム	2004	`Picadd`	警告	`<username>` がカスタム仮想チャネル `<vcName>` を開こうとしました
システム	2005	`Picadd`	エラー	ポリシー `<pathInPolicy>` で指定されたパスはプロセスパスに解決できません
システム	2007	`Picadd`	情報	ロードされたプロセスパスは `<processPath>` です
システム	2008	`Picadd`	エラー	VCポリシーパス内の環境変数 `<varName>` が見つかりません

マルチセッションVDA

マルチセッションVDAマシンのイベントログに次のイベントが記録されます:

ログ名	ID	送信元	レベル	説明
システム	13	`Rpm`	情報	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開かれました
システム	14	`Rpm`	警告	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開くことができません
システム	15	`Rpm`	情報	`<username>` がカスタム仮想チャネル `<vcName>` を開きました
システム	16	`Rpm`	警告	`<username>` がカスタム仮想チャネル `<vcName>` を開こうとしました
システム	17	`Rpm`	エラー	ポリシー `<pathInPolicy>` で指定されたパスをプロセスパスに解決できません

ログ名	ID	送信元	レベル	説明
システム	18	`Rpm`	情報	ロードされたプロセスパスは `<processPath>` です
システム	19	`Rpm`	エラー	VCポリシーパス内で環境変数 `<varName>` が見つかりません

既知のサードパーティ仮想チャネル

以下は、カスタムCitrix®仮想チャネルを使用する既知のサードパーティソリューションです。このリストには、カスタムCitrix仮想チャネルを使用するすべてのソリューションが含まれているわけではありません。

- カーナー
- ControlUp
- シスコ ウェブエックス チームズ
- シスコ ウェブエックス ミーティングス バーチャル デスクトップ ソフトウェア
- deviceTrust
- エピック ワープ ドライブ
- エピック スリングショット
- インプリバタ ワンサイン
- ミッドマーク IQパス クライアント エクステンションズ
- ニュアンス パワーマイク クライアント エクステンションズ
- ニュアンス ドラゴン メディカル ネットワーク エディション 360 vSync
- ズーム ミーティングス for VDI
- アルティマ IA-Connect

関連する仮想チャネルを許可リストに追加するための詳細情報を取得するには、ソリューションのベンダーにお問い合わせください。または、(/ja-jp/citrix-virtual-apps-desktops/2511/secure/virtual-channel-security.html#obtain-virtual-channel-names-and-processes)セクションに記載されている手順に従ってください。

DVC用仮想チャネル許可リスト

DVC用仮想チャネル許可リストを使用して、環境で許可されるカスタム動的仮想チャネルを制御できます。デフォルトでは、動的仮想チャネルは許可されていません。動的仮想チャネルが必要な場合は、それらを明示的に許可リストに追加する必要があります。

構成

DVC の仮想チャネル許可リストはデフォルトで有効になっています。この機能は、Citrix® ポリシーの次の設定を使用して構成できます。

- DVC の仮想チャネル許可リスト: この機能を有効または無効にし、動的仮想チャネルをリストに追加します。
- 仮想チャネル許可リストのログスロットリング: 仮想チャネル許可リストのイベントログのスロットリング期間を設定します。
- 仮想チャネル許可リストのログ記録: 仮想チャネル許可リストのログレベルを設定します。

許可リストへの動的仮想チャネルの追加

許可リストに動的仮想チャネルを追加するには、次の情報が必要です。

1. クライアント上のDVCプラグインの名前。例: `DvcPlugin1.dll`。
2. DVCリスナーの名前。例: `ListenerName1`。
3. VDAマシン上で動的仮想チャネルにアクセスするプロセスのパス。例: `C:\Program Files\Application\run.exe`。

必要な情報が揃ったら、DVC の仮想チャネル許可 リストポリシー設定を使用して、動的仮想チャネルを許可リストに追加する必要があります。動的仮想チャネルをリストに追加するには、セッションホストで DVC にアクセスするプロセスのパスを入力し、その後にコンマ、クライアント側プラグイン名、コンマ、およびプラグインで使用されるリスナー名を入力します。複数のリスナー名はコンマで区切って追加できます。

単一リスナーの場合

前の例を使用して、次のエントリをリストに追加します。 `C:\Program Files\App\run1.exe,DvcPlugin1,ListenerName1`

複数リスナーの場合

複数のリスナーがある場合は、リストに次のエントリを追加します。 `C:\Program Files\App\run1.exe,DvcPlugin1,ListenerName1,ListenerName2`

ワイルドカードの使用

ワイルドカード (*) の使用がサポートされています。アプリケーションのバージョンに基づいてディレクトリ名または実行可能ファイル名が変更される場合、またはサードパーティコンポーネントがユーザープロファイルにインストールされている場合に、ワイルドカードを使用できます。

次のシナリオでワイルドカードを使用できます。

- 完全なディレクトリ名を置き換える場合。例: `C:\Program Files\App*\run1.exe`
- ディレクトリ名の一部を置き換える場合。例: `C:\Program Files\App\v*\run1.exe`
- 実行可能ファイル名を置き換える場合。例: `C:\Program Files\App\v1.2*.exe`
- 実行可能ファイル名の一部を置き換える場合。例: `C:\Program Files\App\v1.2\run*.exe`

次の制限が適用されます。

- ワイルドカードは、単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルが `C:\Program Files\App\v1.2\run1.exe` にある場合
  - 許可される例: `C:\Program Files\App*\run1.exe`
  - 許可されない例: `C:\Program Files*\run1.exe`
- エントリにはファイル名拡張子を含める必要があります。
  - 許可: `C:\Program Files\App\v1.2*.exe`
  - 不許可: `C:\Program Files\App\v1.2*`
- すべてのパスはローカルである必要があります。

デバイス

HDX™は、あらゆる場所のあらゆるデバイスで高精細なユーザーエクスペリエンスを提供します。デバイスセクションの記事では、以下のデバイスについて説明します。

- スキャン
- 汎用USBデバイス
- クライアントドライブマッピング
- モバイルおよびタッチスクリーンデバイス
- シリアルデバイス
- 特殊キーボード
- Webカメラ

最適化されたUSBデバイスと汎用USBデバイス

最適化されたUSBデバイスとは、Citrix Workspace™アプリが特定のサポートを提供しているデバイスです。たとえば、HDX Multimedia仮想チャネルを使用してWebカメラをリダイレクトする機能などです。汎用デバイスとは、Citrix Workspaceアプリで特定のサポートがないUSBデバイスです。

デフォルトでは、汎用USBリダイレクトは、汎用モードに設定しない限り、最適化された仮想チャネルサポートを持つUSBデバイスをリダイレクトできません。

一般的に、USBデバイスは汎用モードよりも最適化モードの方が優れたパフォーマンスを発揮します。ただし、最適化モードではUSBデバイスが完全な機能を持たない場合があります。その機能に完全にアクセスするには、汎用モードに切り替える必要があるかもしれません。

USB大容量記憶装置では、Citrix®ポリシーによって制御されるクライアントドライブマッピングまたは汎用USBリダイレクト、あるいはその両方を使用できます。主な違いは次のとおりです。

汎用USBリダイレクトとクライアントドライブマッピングの両方のポリシーが有効になっており、セッションの開始前または開始後に大容量記憶装置が挿入された場合、クライアントドライブマッピングを使用してリダイレクトされます。

これらの条件が真の場合、マスストレージデバイスは汎用USBリダイレクトを使用してリダイレクトされます。

- 汎用USBリダイレクトとクライアントドライブマッピングポリシーの両方が有効になっています。
- デバイスが自動リダイレクト用に構成されています。
- マスストレージデバイスがセッション開始前または開始後に挿入されます。

詳細については、`<http://support.citrix.com/article/CTX123015>`を参照してください。

機能	クライアントドライブマッピング	汎用USBリダイレクト
デフォルトで有効	はい	いいえ
読み取り専用アクセス設定可能	はい	いいえ
暗号化されたデバイスアクセス	はい、仮想セッション上でデバイスにアクセスする前に暗号化が解除されている場合。	シトリックス バーチャル デスクトップ™ のみ

スキャン

TWAINリダイレクト

はじめに

ユーザーは、クライアントエンドポイントに接続されたTWAIN準拠のスキャナーを使用して、Citrix HDX™セッション内のアプリケーションからドキュメントをスキャンできます。Citrixスキャンモジュールは、スキャン要求をクライアントエンドポイントにリダイレクトして要求を処理します。完了すると、スキャンされた情報はVDAホストに送り返されます。

要件

Citrixコントロールプレーン

- シトリックス仮想アプリおよびデスクトップ™ 1912 以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ 11
  - ウィンドウズ サーバー 2022 以降
- VDA
  - バージョン1912以降
- アプリケーション
  - 32ビットアプリケーション
  - 64ビットアプリケーション

> **注:**
>
> - セッションホストで64ビットアプリケーションのスキャン機能を有効にするには、64 ビット TWAIN データソースマネージャー (twaindsm.dll) が必要です。このコンポーネントはオペレーティングシステムによってプリインストールされていません。
> - 64ビットスキャンアプリケーションにこのファイルが含まれていない場合は、アプリケーションベンダーに連絡して64ビット twaindsm.dll を入手してください。
> - 入手したら、管理者はセッションホスト上の **System32** フォルダーにファイルを手動でコピーし、その後マシンを再起動する必要があります。

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ 11
- Workspaceアプリ
  - Windows: バージョン1912以降
- スキャナー

- TWAIN準拠スキャナー
- クライアントエンドポイントにTWAINドライバーをインストールする

構成

TWAINリダイレクトはデフォルトで有効になっています。TWAINリダイレクトを構成し、スキャンエクスペリエンスを最適化するために、以下のポリシー設定が利用可能です。

- **クライアントTWAINデバイスリダイレクト:** TWAINリダイレクトを有効または無効にする。
- **TWAIN圧縮レベル:** クライアントからVDAに転送される画像の圧縮レベルを設定する。

詳細については、「TWAINデバイスのポリシー設定」を参照してください。

トラブルシューティング

TWAINリダイレクト機能は、このURLからダウンロードできる公開テストアプリTwackerでテストできます。

HDXセッション内でTWAIN機能を検証するには、以下の手順に従ってください。

1. VDAホストに**Twacker**をインストールします。
2. **Twacker**（32ビットまたは64ビットバージョン）を起動します。
3. **File > Select Source**をクリックし、リストからスキャナーを選択します。
4. **File > Acquire**をクリックします。
5. **Scan button**をクリックしてスキャナーをテストします。

Twackerが正常にスキャンできる場合、**Citrix Virtual Apps™ and Desktops**のセットアップが以下であることを確認できます。

- TWAINリダイレクトを使用するように正しく構成されている
- すべてのローカルクライアントデバイス要件を満たしている

特定のアプリケーション内でスキャンに関する問題がまだ発生する場合は、ソフトウェアの問題である可能性が高いです。

WIA デバイス

デジタルカメラやスキャナーなどのWIAデバイスは、WIAフレームワークを使用して、サーバーでホストされている画像処理アプリケーションと通信します。

前提条件

- スキャナーはWIA準拠である必要があります。
- WIAドライバーをローカルデバイスにインストールします。サーバーには必要ありません。
- スキャナーをローカルに接続します（例：USB経由）。
- スキャナーがTWAINドライバーではなく、ローカルのWindows Image Acquisitionサービスを使用していることを確認します。
- テストに使用されるユーザーアカウントに、ICA®セッション内の帯域幅を制限するポリシーが適用されていないことを確認します。たとえば、クライアントUSBリダイレクト帯域幅制限などです。

要件

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ 11
  - ウィンドウズ サーバー 2022 以降
- VDA
  - バージョン2511以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ 11
- Workspaceアプリ
  - Windows: バージョン2411以降

構成

WIAリダイレクトはデフォルトで無効になっています。Citrix®ポリシーで次の設定を有効にできます。

- WIAリダイレクト: この設定は、ユーザーがユーザーデバイス上のWIAデバイスにアクセスすることを許可または禁止します。

Citrix Virtual Apps and Desktops 2511 以降では、VDA側の追加のレジストリ変更は必要ありません。

既知の問題

ポリシー設定については、「WIAデバイスポリシー設定」を参照してください。

SANE リダイレクト

はじめに

ユーザーは、ChromeOSおよびLinuxエンドポイントからCitrix®セッション内のTWAINアプリケーションからドキュメントをスキャンできます。ユーザーがアプリケーションからドキュメントをスキャンしようとすると、Citrixスキャンモジュールはリクエストをクライアントエンドポイントにリダイレクトしてスキャナーからのスキャンを実行し、スキャンが完了するとファイルはVDAに送信されます。

要件

Citrixコントロールプレーン

- シトリックス バーチャル アプリケーションズ アンド デスクトップス™ 2411 以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ 11
  - Windows Server 2019 以降のバージョン
- VDA
  - バージョン2411以降

クライアントデバイス

- オペレーティングシステム
  - ChromeOS v129以降
- Workspaceアプリ
  - ChromeOS: バージョン2409以降

- Linux: バージョン2508.10以降

- スキャナー
  - スキャナーは、基盤となるクライアントオペレーティングシステムでサポートされている必要があります。
  - USB経由でクライアントエンドポイントにローカルに接続されている必要があります。

構成

この機能を有効にするための追加設定は不要です。この機能はデフォルトで有効になっています。

> **注:**
>
> この機能を無効にするには、Web Studio/DaaSコンソールを開きます。SANEスキャナーリダイレクトポリシー設定を「禁止」に設定します。

トラブルシューティング

イベントログ

管理者は、さまざまなスキャン関連のイベントメッセージを表示できます。

VDAホストのイベントビューアーに記録される、さまざまなスキャン関連操作のイベントメッセージを以下に示します。これらは、イベントソースとしてHDX™ Scannerを使用して、Windowsログのアプリケーションセクションで表示できます。

イベントID	イベントテキスト	説明
2	AllowScannerSANERedirectionポリシーが無効になっています。スキャナーはリダイレクトされません。	SaneRedirectionポリシーが無効になっていることを示します。
3	スキャン詳細: ページ - '[pages]'、アプリケーション - '[application]'、スキャナー - '[scanner]'、ユーザー - '[user]'、1ページあたりの平均時間 - '[time]'ミリ秒。	スキャンが完了したときに生成されます。

イベントID	イベントテキスト	説明
101	スキャンするページが見つかりません。	ドキュメントが検出されなかったときに生成されます。
102	スキャン失敗 - デバイスのドキュメントフィーダーが詰まっています。	スキャナーのドキュメントフィーダーでの紙詰まりが原因でスキャンが失敗した場合に生成されます。
103	スキャン失敗 - '[failure]'。スキャナーアプリケーションを閉じて再起動してください。	サポートされていない操作、ファイル終端エラー、アクセス拒否エラーなどのエラーが原因でスキャンが失敗した場合に生成されます。
104	アプリケーションでメモリ障害が発生しました。アプリケーションを再起動してください。	メモリ不足が原因でスキャンが失敗した場合に生成されます。
201	ユーザーによってスキャン操作がキャンセルされました。	ユーザーによってスキャン操作がキャンセルされた場合に生成されます。
202	スキャン中にセッションが切断されました。	スキャン中にHDXセッションが切断された場合に生成されます。
203	'[capability]' のTWAINとSANE間の変換はサポートされていません。スキャナー/アプリケーションがサポートされているか確認してください。	指定された機能のTWAINとSANE間の変換がサポートされていないことを示します。
205	スキャナー '[scanner]' をアクティブに設定できませんでした。スキャナーの電源が入っていて接続されているか確認してください。	スキャナーへの接続を開くのに失敗した場合に生成されます。

イベントID	イベントテキスト	説明
206	スキャナーが見つかりません。スキャナーの電源が入っていて、接続されているか確認してください。	クライアントエンドポイントでスキャナーが検出されない場合に生成されます。

既知の制限事項

1. ネットワーク認証されたスキャナーはサポートされていません。
2. VDA上のFujitsu Paperstreamアプリなど、一部の独自スキャンアプリケーションでは、リダイレクトされたスキャナーがサポート対象として表示されない場合があります。
3. ネイティブUIを使用する場合、ページ幅、ページ高さ、用紙サイズ、明るさ、コントラストなど、一部のスキャナー設定は、サードパーティAPIの制限により尊重されない場合があります。

USBデバイス

はじめに

汎用USBリダイレクト機能により、クライアントマシンからHDX™セッションへのUSBデバイスのリダイレクトが可能になり、エンドユーザーはHDXセッションで幅広い汎用USBデバイスを操作できるようになります。これは、ユーザーが最適化されたサポートがない、または不適切な特殊デバイスを使用する必要があるシナリオで役立ちます。

> **注:**
>
> 仮想チャネルサポートに最適化されていないUSBデバイスは、生のUSBリダイレクトを使用して汎用USB仮想チャネルにフォールバックします。

仕組み?

汎用USBリダイレクトは低レベルで機能し、クライアントマシンとXenDesktop®仮想デスクトップ間でUSB要求および応答メッセージをリダイレクトします。

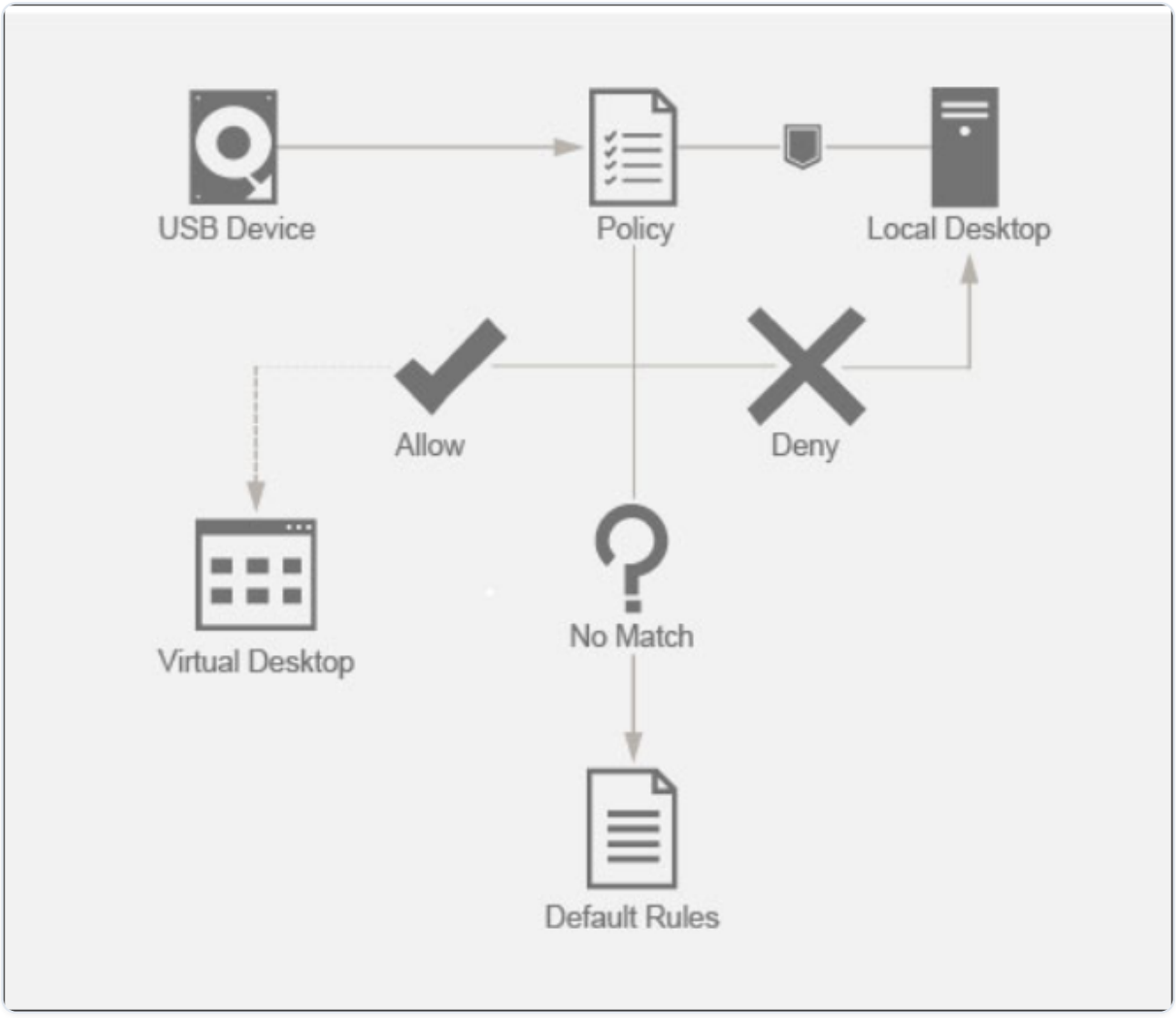
これにより、クライアントマシンに互換性のあるデバイスドライバーが必要なくなり、ドライバーは仮想デスクトップでのみサポートされることが想定されます。USBリダイレクトポリシー規則は、DDCポリシー規則が評価および適用された後で、クライアント側のポリシーとデフォルト規

則が尊重されるように、特定の優先順位に従います。これにより、Citrix管理者は、不正なデバイスや偽装されたデバイスがセッション内にリダイレクトされるのを防ぐことができます。

さらに、リモートセッションへのアクセスを試みる不正なデバイスのイベントログを監査およびフラグ付けすることができ、管理者はデータ漏洩を防ぐための追加措置を講じることができます。

ユーザーがUSBデバイスを接続すると、セッションホストは一致が見つかるまで各ポリシー規則に対して連続してチェックします。いずれかのデバイスに対する最初の一致が最終的なものと見なされます。

- 最初の一致が許可規則である場合、デバイスは仮想デスクトップにリダイレクトされます。
- 最初の一致が拒否規則である場合、デバイスはセッションにリダイレクトされず、ローカルユーザーデバイスでのみ使用できます。一致が見つからない場合は、デフォルト規則が使用されます。



汎用USBリダイレクトとの互換性

これらのCitrix Workspace™アプリは、汎用USBリダイレクトをサポートしています。

- Windows向けCitrix Workspaceアプリについては、Windows向けCitrix Workspaceアプリを参照してください。
- Mac向けCitrix Workspaceアプリについては、Mac向けCitrix Workspaceアプリを参照してください。
- Linux向けCitrix Workspaceアプリについては、Linux向けCitrix Workspaceアプリを参照してください。
- Chrome OS向けCitrix Workspaceアプリについては、Chrome向けCitrix Workspaceアプリを参照してください。

Citrix Workspaceアプリのバージョンについては、Citrix Workspaceアプリの機能マトリックスを参照してください。

構成

USBリダイレクトはデフォルトで無効になっています。Citrix®ポリシーで以下の設定を使用して、汎用USBリダイレクトを構成できます。

- **クライアントUSBデバイスリダイレクト**: USBリダイレクトを有効または無効にする
- **クライアントUSBデバイスリダイレクトルール**: 特定のデバイスアクション、つまり特定のデバイスへのアクセスを許可または拒否するように指定する
- **クライアントUSBデバイスリダイレクトルール (バージョン2)**: USBデバイスのフィルタリング、分割、自動接続のルールを指定する
- **クライアントUSBデバイス最適化ルール**: 最適化を無効にするか、最適化モードを変更する
- **既存のUSBデバイスの自動接続を許可する**: HDX™セッション開始時にクライアントエンドポイントに接続されている既存のUSBデバイスの自動接続を許可または防止する
- **新しく接続されたUSBデバイスの自動検出を許可する**: HDXセッション中にクライアントエンドポイントに接続されたUSBデバイスの自動接続を許可または防止する

詳細については、「USBポリシー設定」を参照してください。

USBリダイレクトの構成方法

デフォルトでは、USBリダイレクトの構成は無効になっています。これを使用するには、USBリダイレクトポリシーと特定のリダイレクトルールをDDCで有効にして構成する必要があります。

> **注:**
>
> バージョン2212より前のコンポーネントを使用している場合、またはLinux/Mac版Workspaceアプリを使用している場合は、USBリダイレクトの構成方法の詳細について「レガシーUSBリダイレクト構成」を参照してください。

汎用USBリダイレクトの有効化

1. **Citrix Web Studio™ポリシー**を開き、**［ポリシー］**タブをクリックします。
2. **ポリシーの作成**をクリックし、**ICA® > USBデバイスポリシー**を展開します。
3. **クライアントUSBデバイスリダイレクトポリシー**を編集します。
4. **許可**を選択し、**保存**をクリックします。

USBリダイレクトポリシー規則の作成

ユーザーがUSBデバイスをVirtual Desktopにリダイレクトしようとすると、一致が見つかるまで各USBポリシー規則に対して順番にチェックされます。いずれかのデバイスに対する最初の一致が最終と見なされます。最初の一致が**許可**規則である場合、一致したデバイスは仮想デスクトップにリダイレクトが許可されます。最初の一致が**拒否**規則である場合、一致したデバイスはローカルデスクトップでのみ利用可能です。一致が見つからない場合は、デフォルトの規則が使用されます。

デバイス規則

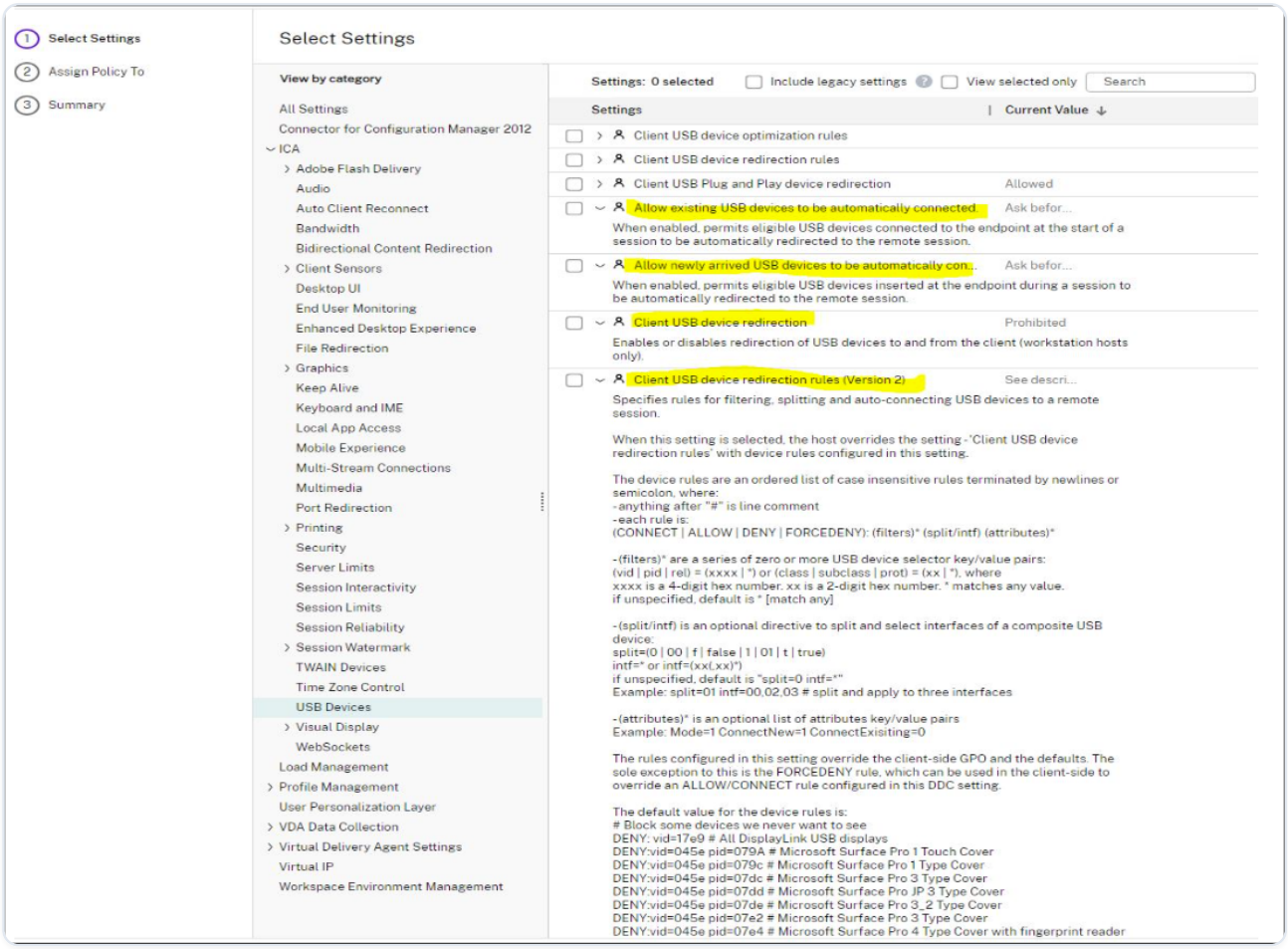
通常のUSBデバイスと同様に、ポリシーまたはエンドポイント上のクライアントCitrix Workspace™アプリ構成で設定されたデバイス規則は、転送するデバイスを選択します。Citrix Workspaceアプリはこれらの規則を使用して、どのUSBデバイスをリモートセッションへの転送を許可または防止するかを決定します。

各規則は、アクションキーワード（**Allow、Connect、またはDeny**）、コロン（:）、およびエンドポイントのUSBサブシステムにある実際のデバイスと一致する0個以上のフィルターパラメーターで構成されます。これらのフィルターパラメーターは、すべてのUSBデバイスが自身を識別するために使用するUSBデバイス記述子メタデータに対応しています。

デバイス規則はプレーンテキストであり、各規則は1行に記述され、#文字の後にオプションのコメントが続きます。規則は上から下へ（優先順位の降順で）照合されます。デバイスまたは子インターフェイスに一致する最初の規則が適用されます。同じデバイスまたはインターフェイスを選択する後続の規則は無視されます。

例: 許可: VID=1050 PID=0421 #Device1 **例:** 接続: VID=xxxx PID=yyyy Class=03 #Device2

キーワード	説明
CONNECT	このキーワードを使用して、USB仮想チャネル経由でのデバイスのリダイレクトを許可し、セッション起動時および挿入時の自動リダイレクトを有効にします。
ALLOW	このキーワードを使用して、USB仮想チャネル経由でデバイスのリダイレクトを許可します。
拒否	このキーワードを使用して、USB仮想チャネル経由でデバイスがリダイレクトされるのを拒否します。



DDC でポリシーを設定する:

1. **Citrix Web Studio ポリシー**」を開き、「**ポリシー**」タブをクリックします。
2. **ポリシーの作成**」をクリックし、「**ICA > USB デバイス ポリシー**」を展開します。
3. **クライアント USB デバイス リダイレクト規則**」を編集します (「**バージョン 2**」)。

4. リダイレクトする必要がある各USBデバイスの説明に記載されている例に基づいて値を設定し、をクリックします。

   例：許可：VID=056A PID=00A4 #STU-430 拒否：Class=08 subclass=05 # マスストレージ

   > **注:**
   >
   > Citrix管理者が**デフォルト値を使用**をチェックして**保存**をクリックすると、デフォルトルールはVDAの以下のレジストリにあります。
   >
   > **注意!**
   >
   > レジストリエディターを使用する前に、この記事の最後にある免責事項を参照してください。
   >
   > `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

> **注記:**
>
> ポリシーは、グループポリシーデバイスルールを使用してクライアントデバイスに設定できますが、CVADおよびCWAの新しいバージョンでは不要になりました。
>
> USBデバイスのレガシー構成については、「レガシーUSBリダイレクト構成」を参照してください。

USB デバイスの自動リダイレクトを構成する (オプション)

USBサポートが有効になっている場合、USBデバイスは自動的にリダイレクトされます。また、USBユーザー設定は、USBデバイスを自動的に接続するように設定されています。すべてのUSBデバイスをリダイレクトすることが常に最適とは限りません。ユーザーは、自動的にリダイレクトされないUSBデバイスリストからデバイスを明示的にリダイレクトできます。USBデバイスが一覧表示されたりリダイレクトされたりするのを防ぐには、クライアントエンドポイントまたはDDCポリシーのいずれかでDeviceRulesを使用します。 このポリシーは、DDC、GPOを使用したクライアント、Citrix Workspace Preferences、またはCDViewerのConnectionsタブのいずれかで設定できます。これらのすべての方法は以下に説明されています。

DDCでのポリシー設定:

USBデバイスの自動リダイレクトを許可するためにDDCで設定できるポリシーは2つあります。

- 既存のUSBデバイスの自動接続を許可する
- 新しく接続されたUSBデバイスの自動接続を許可する

a. **Citrix Web Studio policies**を開き、**Policies**タブをクリックします。
b. **Create Policy**をクリックし、**ICA > USB Devices policies**を展開します。
c. 既存のUSBデバイスの自動接続を**許可**する設定を編集します。
d. **Use default value**チェックボックスをオフにし、ドロップダウンメニューから**Automatically redirect available USB devices**を選択して、**Save**をクリックします。
e. 新しく接続されたUSBデバイスの自動接続を**許可**する設定を編集します。
f. **Use default value**チェックボックスをオフにし、ドロップダウンメニューから**Automatically redirect available USB devices**を選択して、**Save**をクリックします。

USBデバイスリダイレクトルールの理解

CitrixクライアントUSBリダイレクトを使用する場合、異なるルールがどのように優先順位付けされ、適用されるかを理解することが重要です。これは一連の指示のようなもので、システムは特定の順序でルールをチェックし、特定のデバイスに対して最初に見つかったルールが適用されます。その**同じデバイス**に対してリストのさらに下に見つかった他のルールは無視されます。

デバイスルールが評価される順序は次のとおりです。

- **クライアントUSBデバイスリダイレクトルール (バージョン2)**: このポリシー設定によって構成されたデバイスルールには、最も高い優先順位が与えられます。特定のデバイスに対するルールがここで見つかった場合、そのルールが適用され、その特定のデバイスに対する他のルールは考慮されません。
- **クライアントUSBデバイスリダイレクトルール**: 次に、Citrix Studio内のこのレガシー設定で定義されたルールが続きます。バージョン2ポリシーでデバイスのルールが見つからなかった場合、システムはこのポリシー設定で定義されたルールをチェックします。ここでも、デバイスのルールが見つかった場合、それが適用され、システムはその特定のデバイスに対するルールの検索を停止します。

> **注:**

> 上記のポリシー設定は、Studioで**クライアントUSBデバイスリダイレクトルール (バージョン2)が設定されていない場合、またはCitrix Workspaceアプリ for Windows**のバージョンが2212より古い場合にのみ適用されます。

- **クライアント側グループポリシーオブジェクト (GPO)**: 両方のStudioポリシー設定をチェックした後でもデバイスに適用されるルールがない場合、システムはクライアント側グループポリシーオブジェクトを介して構成されたルールに従います。
- **クライアント側レジストリ設定**: 最後に、クライアント側レジストリ設定が最も低い優先順位で適用されます。

この階層により、特定のデバイスに対してより具体的または新しい構成が優先され、USBデバイスリダイレクトを管理するための明確で予測可能な方法が提供されます。階層が評価順序を決定する一方で、上位レベルでデバイスに対して見つかったルールは、**同じデバイス**に対する下位レベルでのルールの適用を妨げることを覚えておくことが重要です。 ただし、下位レベルで設定されたルールが完全に無視されるわけではなく、まだルールが適用されていないデバイスに対しては評価されます。

この階層的なアプローチは、**下位互換性**も保証します。Citrix Virtual Apps and Desktops™またはCitrix Workspaceアプリの古いバージョンからアップグレードする場合、既存のクライアント側構成は保持されます。これにより、企業管理者は、即座の中断なしに、Studioのより高度な**バージョン2デバイスルール**ポリシー設定への移行パスを計画する時間を確保できます。

例:

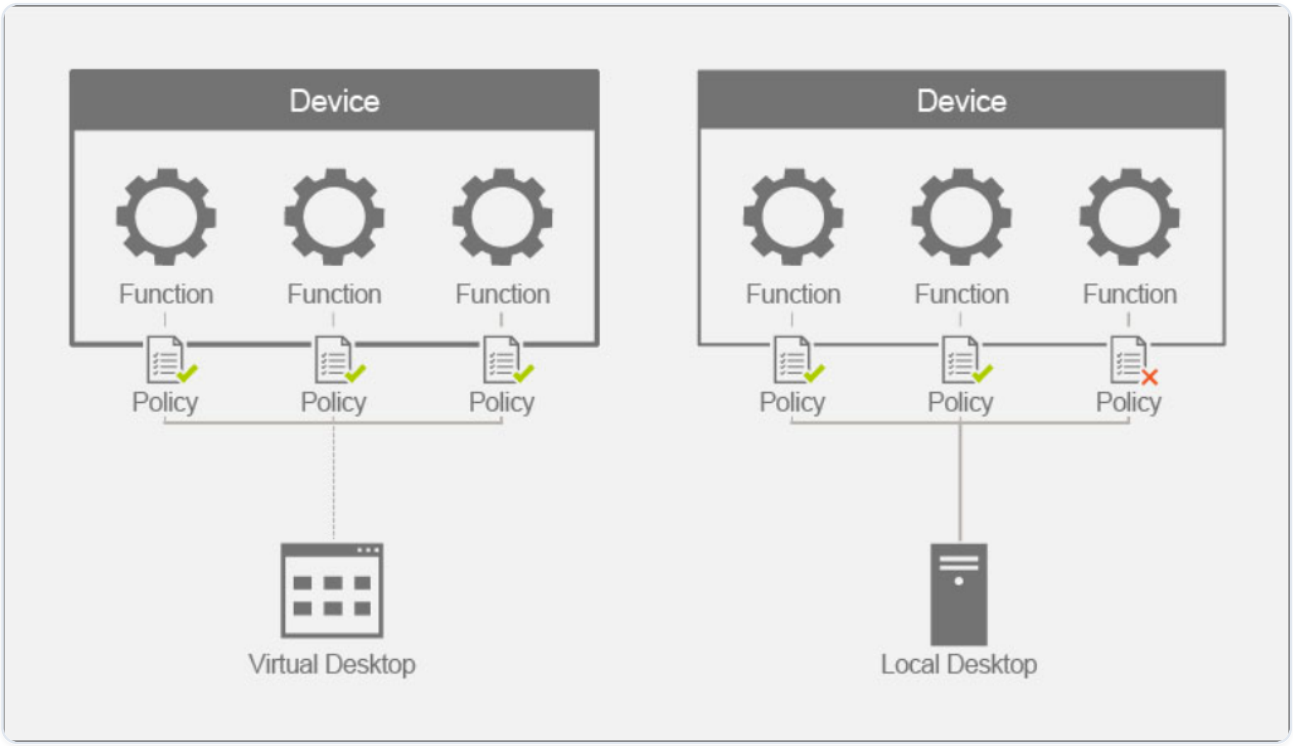
例えば、ベンダーID (VID) `xxxx`、プロダクトID (PID) `yyyy`を持つ特定のUSBデバイスがあるとします。

- Citrix Studioの**クライアントUSBデバイスリダイレクトルール (バージョン2)**ポリシー設定で、`CONNECT VID=xxxx PID=yyyy`というルールセットがあります。
- 別途、クライアント側**グループポリシーオブジェクト (GPO)**で、同じデバイスに対して`DENY`というルールが`DENY: VID=xxxx PID=yyyy`あります。

このデバイスがクライアントエンドポイントに接続されると、システムはまずバージョン2のStudioポリシーのルールを評価します。システムは`CONNECT`ルール`VID=xxxx PID=yyyy`を見つけます。このルールは最も高い優先順位レベルにあるため、すぐに適用されます。その後、システムはこの特定のデバイスに対するそれ以上のルールを無視します。したがって、クライアント側のGPOに`DENY`ルールが存在しても、それは無視され、デバイスは正常にリダイレクトされます。

複合デバイスとデバイス分割

複合USBデバイスは、コンピューターに接続された複数の独立したUSBデバイスのように機能する単一のデバイスです。1つのUSBコネクタを持ちますが、それぞれ独自の機能セットを持つ複数のインターフェースをコンピューターに公開できます。ユーザーが複合USBデバイスを接続すると、ホストデバイスはすべての機能（インターフェース）を各ポリシールールに対してチェックします。いずれかの機能（インターフェース）に対する最初の一致が拒否ルールである場合、そのルールは複合デバイスにとって最終的なものと見なされ、デバイスは拒否されます。機能（インターフェース）に対する最初の一致が許可ルールである場合、ホストデバイスは次の機能（インターフェース）に対してルールの一致を続行します。ポリシールールによって機能（インターフェース）が拒否されない場合、複合デバイスは許可されます。複合デバイスに対する最終的な一致が拒否ルールである場合、デバイスはローカルデスクトップでのみ利用可能であり、それ以外の場合は仮想デスクトップにリダイレクトされます。一致が見つからない場合は、デフォルトルールが使用されます。



デバイスリダイレクトルール (バージョン2) ポリシーで適切なルールを使用することで、複合デバイスの特定の機能のみを許可するように複合デバイスを分割できます。たとえば、FIDO2キーのHID機能のみを使用し、スマートカード機能は使用したくない場合があります。その場合、以下に示すようにルールを設定します。

1. Connect: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikeyシリーズ5のFIDO2 HID機能は許可されています。
2. Deny: VID=1050 PID=0407 split=01 intf=02 #Yubikeyシリーズ5のスマートカード機能はブロックされています。

ヒント:

新しいポリシールールを作成する際は、USBウェブサイトで入手できるUSBクラスコードを参照してください。

署名パッドの構成

1. VDAホストに適切なデバイスドライバーをインストールします。
2. **Citrix Web Studio™**で**クライアントUSBデバイスリダイレクト**ポリシー設定を有効にします。
3. **クライアントUSBデバイスリダイレクトルール (バージョン2)** ポリシー設定を編集します。
    a. リダイレクトする必要がある署名パッドの**VID**と**PID**情報を設定し、**保存**をクリックします。例: **Connect**: VID=06A8 PID=0057 class=03 #Topaz HSB
4. ポリシー設定**クライアントUSBデバイス最適化ルール**を編集します。
    a. モードとその他のデバイス情報を設定します。例: Mode=00000004 VID=06A8 PID=0057 class=03 #キャプチャモードで動作する入力デバイス
5. **既存のUSBデバイスの自動接続を許可する**ポリシー設定を編集します。
6. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択し、「**保存**」をクリックします。
7. ポリシー設定「**新しく接続されたUSBデバイスの自動接続を許可**」を編集します。
8. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択し、「**保存**」をクリックします。

これらの設定が構成されると、以降のセッション起動ではデバイスが自動的にリダイレクトされ、エンドユーザーによる追加のアクションは不要になります。

注:

VIDとPIDを、リダイレクトするデバイスの実際のVIDとPIDに置き換えます。

USBリダイレクトを使用したBloombergキーボードの構成

1. **Citrix Web Studio**でポリシー設定「**クライアントUSBデバイスリダイレクト**」を有効にします。
2. Bloomberg 5キーボードは、ポリシー設定「**クライアントUSBデバイスリダイレクト規則（バージョン2）**」でデフォルトで設定されており、管理者による追加のアクションは不要です。
3. ポリシー設定「**既存のUSBデバイスの自動接続を許可**」を編集します。
4. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択し、「**保存**」をクリックします。
5. ポリシー設定「**新しく接続されたUSBデバイスの自動接続を許可**」を編集します。
6. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択し、「**保存**」をクリックします。

これらの設定が構成されると、Bloombergキーは以降のHDX™セッションで自動的に表示され、エンドユーザーによる追加のアクションは不要になります。

USBリダイレクトを使用したFIDO2キーの構成

Citrixは、HDXセッションでFIDO2キーを使用するためにFIDO2リダイレクトを使用することを推奨します。ただし、代わりにUSBリダイレクトを使用してFIDO2キーをリダイレクトする必要がある状況も考えられます。これには、クライアント、VDA、またはオペレーティングシステム（例: Windows Server 2016）で機能がサポートされていないため、FIDO2リダイレクトが利用できないシナリオが含まれます。

キーで複数のモードが有効になっているが、HDXセッションではその一部のみを許可したいという状況も考えられます。たとえば、FIDO2とOTPは許可したいが、スマートカードはブロックしたい場合などです。

以下の手順は、USBリダイレクトを使用してFIDO2キーを構成する方法を示しています (Yubikey vid=1050, pid=0407)。

1. **Citrix Web Studio**で**クライアントUSBデバイスリダイレクト**ポリシー設定を有効にします。
2. **クライアントUSBデバイスリダイレクト規則 (バージョン2)** ポリシー設定を編集します。
    a. セッションでリダイレクトされるFIDO2キーの**VID**と**PID**情報、および分割デバイス構成を設定し、**保存**をクリックします。
    b. **Connect**: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikeyシリーズ5で許可されるFIDO2 HID機能。

c. **Deny**: VID=1050 PID=0407 split=01 intf=02 # Yubikeyシリーズ5のスマートカード機能はブロックされます。

3. ポリシー設定**既存のUSBデバイスの自動接続を許可する**を編集します。
4. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクトする**を選択して、**保存**をクリックします。
5. ポリシー設定**新しく接続されたUSBデバイスの自動接続を許可する**を編集します。
6. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクトする**を選択して、**保存**をクリックします。

これらの設定が構成されると、FIDO2キーボードは以降のHDXセッションで自動的に表示され、追加のエンドユーザー操作は不要になります。

USBリダイレクトを使用した3Dマウスの構成

現在、3dConnexion SpaceMouseドライバーはワークステーションOS（Windows 10およびWindows 11）でのみサポートされています。サーバーOSでは動作しません。ワークステーションOSでSpaceMouse Enterprise（vid=046D, pid=C016）を構成する手順は次のとおりです。

1. VDAホストに最新のWindowsドライバーをインストールします。
2. 「**Citrix Web Studio**」で「**クライアントUSBデバイスリダイレクト**」ポリシー設定を有効にします。
3. **クライアントUSBデバイスリダイレクト規則（バージョン2）**ポリシー設定を編集します。

   a. リダイレクトする必要がある署名パッドの**VID**と**PID**情報を追加し、**保存**をクリックします。例：**接続**: VID=046D PID=C016 #SpaceMouse Enterprise

4. ポリシー設定**クライアントUSBデバイス最適化規則**を編集します。

   a. モードとその他のデバイス情報を設定します。例：Mode=00000004 VID=046D PID=C016 class=03 #キャプチャモードで動作する入力デバイス

5. ポリシー設定**既存のUSBデバイスの自動接続を許可する**を編集します。
6. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクトする**」を選択して、**保存**をクリックします。
7. ポリシー設定**新しく接続されたUSBデバイスの自動接続を許可する**を編集します。
8. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクトする**」を選択して、**保存**をクリックします。

異なるデバイス規則を使用してUSBリダイレクトで2つ以上のデバイスを構成する

複数のデバイスを異なるデバイス規則でHDXセッション内にリダイレクトできます。管理者は、一方のデバイスを自動的にリダイレクトし、もう一方のデバイスはエンドユーザーにリダイレクトのオプションを提供したい場合があります。異なる規則で2つのデバイスを構成する手順は次のとおりです。

1. 「**Citrix Web Studio**」で「**クライアントUSBデバイスリダイレクト**」ポリシー設定を有効にします。
2. **クライアントUSBデバイスリダイレクト規則（バージョン2）**ポリシー設定を編集します。
    a. セッション内の適切なデバイスルールでリダイレクトする2つのデバイスの**VID**と**PID**情報を追加し、**保存**をクリックします。
    b. **許可**: VID=0911 PID=0c1c #Phillips スピーチマイク.
    c. **接続**: VID=06A8 PID=0043 class=03 # Topaz HSB 署名パッド
3. ポリシー設定**既存のUSBデバイスの自動接続を許可する**を編集します。
4. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクトする**を選択して、**保存**をクリックします。
5. ポリシー設定**新しく接続されたUSBデバイスの自動接続を許可する**を編集します。
6. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクトする**を選択して、**保存**をクリックします。

これらの設定が構成されると、Topaz HSB 署名パッドは以降のHDXセッションで自動的に表示され、追加のエンドユーザー操作は必要ありません。一方、Phillips スピーチマイクは、エンドユーザーがConnection CenterまたはCDViewerのタブでリダイレクトを有効にする必要があります。

トラブルシューティング

USBリダイレクト関連の問題をトリアージするには、次の手順に従ってください。

1. USBリダイレクトのシステム要件が満たされていることを確認します。これには、正しいCVADおよびCWAバージョン、サポートされているデバイス、および検討中のOSプラットフォーム上のデバイスドライバーが含まれます。
2. お使いの環境で使用されているコンポーネントのバージョンとプラットフォームに基づいて、構成が適切であることを確認してください。(/ja-jp/citrix-virtual-apps-desktops/2511/devices/usb-devices/legacy-usb-redirection-configuration.html)を必要とするコンポーネントの詳細については、「レガシーUSBリダイレクト構成」の注記を参照してください。

3. デバイスがクライアントによって列挙されたデバイスの下にリストされていることを確認します。

    a. Workspace Preferencesツールバー: WorkspaceアプリのPreferencesツールバーのタブに列挙されているデバイスを確認します（**CWAアイコン > Connection Center > Preferences**を右クリック…タブをクリック）。

    b. `CtxUsbDiagnostics.exe`（推奨）：このツールをコマンドプロンプトウィンドウで実行します。出力には、特定のセッションのデバイス固有の情報が表示されます。デバイスがリダイレクトされているかどうか、また、デバイスルールセットがデバイスのリダイレクトを妨げているかどうかを示します。詳細については、(/ja-jp/citrix-virtual-apps-desktops/2511/devices/usb-devices/usb-diagnostics-tool.html)を参照してください。

    c. USBViewまたはその他のサードパーティツール: エンドポイント/クライアントマシンでUSBViewのようなサードパーティツールを実行し、デバイスがエンドポイントで検出されていることを確認します。

4. デバイスが列挙されている場合:

    a. 特定のデバイスについてCtxUsbDiagnosticsツールの出力に拒否ルールが表示される場合は、Studioで構成されているポリシーを確認し、バージョン2ポリシーでルールが正しく設定されていることを確認します。拒否ルールがStudioポリシーに表示されない場合は、クライアント側ポリシー、そして最後にクライアント側デフォルトの順に確認して、一致する拒否ルールを見つけます。

    b. CtxUsbDiagnosticsの出力に拒否ルールがない場合、CWAはPreferencesウィンドウのタブ（デバイス > デバイスの管理）で適切なボタンをチェック/クリックすることでデバイスのリダイレクトを許可します。一度リダイレクトされたデバイスはセッションで利用可能になります。これは、HDXセッションでデバイスマネージャー/USBViewまたは同様のアプリケーションを確認することで検証できます。

5. セッション内にデバイスが表示されない場合:

    a. VDAホストに正しいデバイスドライバーが正しくインストールされていない可能性があります。VDAホストに最新バージョンのデバイスドライバーが正しくインストールされていることを確認してください。一部のデバイスドライバーはターミナルサーバーマシンではサポートされていないため、リダイレクトしようとしているデバイスがそうでないことを確認してください。

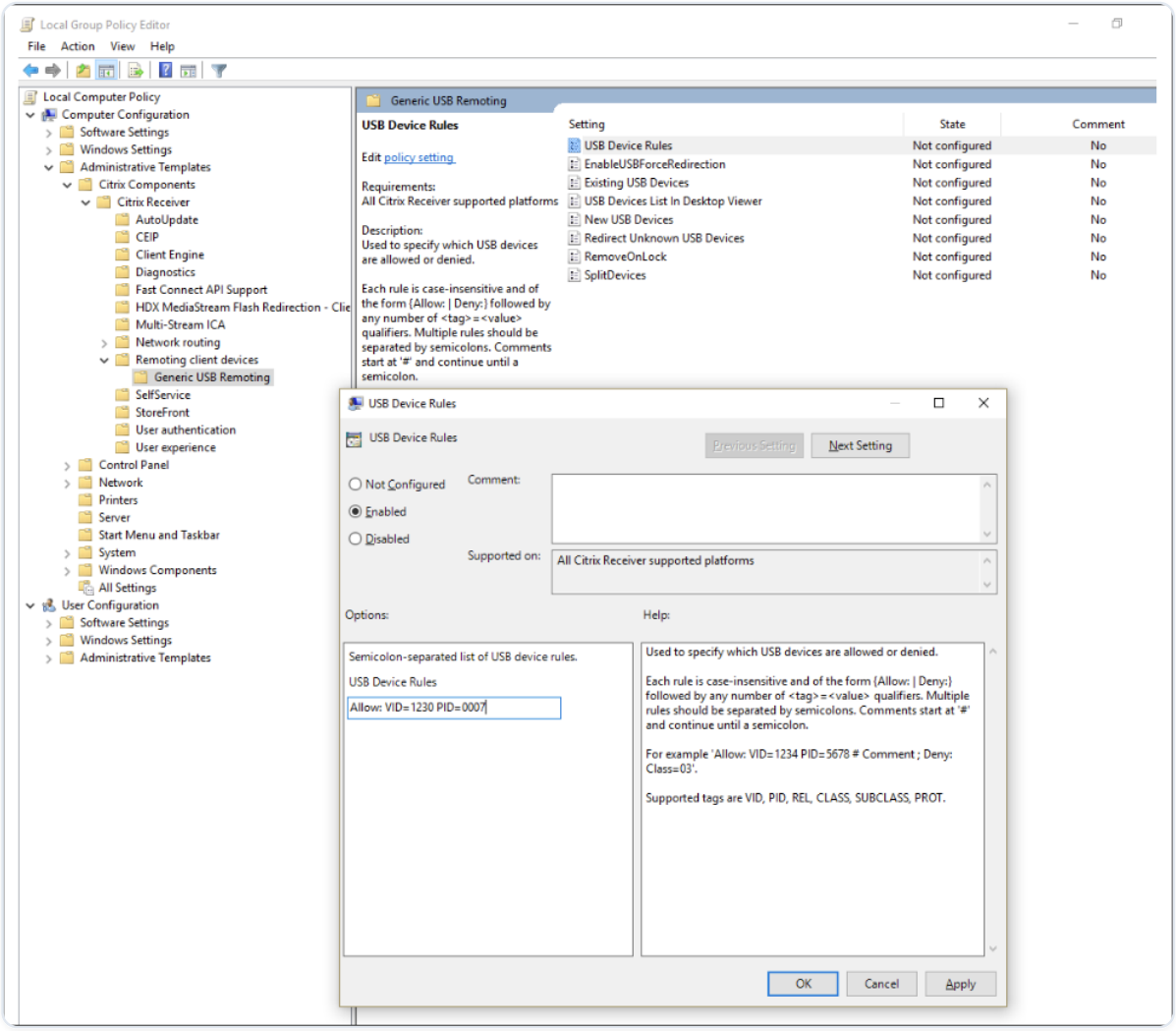
    b. デバイスがクライアントエンドポイントで使用されていないことを確認します。一部のデバイスはクライアントエンドポイントにもドライバーのインストールが必要であり、これによりセッションでのリダイレクトが妨げられる可能性があります。

6. クライアントエンドポイントでUSB関連のルールが正しく設定されていることを確認します。

   a. **Windows 向け CWA** :

      i. クライアント上のグループポリシー (これに関する詳細とSSを追加) が適切に設定されており、Studioで設定されたルールと競合していないことを確認します。

      ii. クライアントのレジストリ内のデフォルトルールを確認します。



`(HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules) are appropriately set and not in conflict with the rules set in Studio and client group policy.`.

   b. CWA for Linux - CWA for Linux の問題のトリアージについては、CWA for Linux の USB ドキュメントを参照してください。

   c. CWA for Mac - CWA for Mac の問題のトリアージについては、CWA for Mac を参照してください。

> **注:**

- TSVDAでは、オーディオデバイスはデフォルトでUSBリダイレクトの使用がブロックされています。これらのデバイスを使用する推奨される方法は、最適化されたオーディオVCを使用することです。
- USB複合デバイスは、デバイスを分割するための正しいデバイスリダイレクトルールが設定されていても、自動的に分割されない場合があります。この問題は、デバイスが低電力モードになっているために発生します。このような場合、低電力モードになった子デバイスがデバイスリストに表示されないことがあります。この問題を解決するには、以下の回避策を使用できます。
  - セッションを切断し、USB デバイスを挿入して、セッションに再接続します。
  - USBデバイスを抜き差しします。この操作により、デバイスは低電力モードから復帰します。
- USBバッテリーセーバー設定がバッテリー寿命を最適化するために有効になっている場合があります。クライアントエンドポイントがスリープ状態になると、USBデバイスが切断されることがあります。このようなシナリオでは、セッションでデバイスを再度表示するために、デバイスを切断して再接続する必要がある場合があります。

イベントログ

管理者は、ユーザーがリダイレクトしようとする不正なデバイスを監視し、適切な措置を講じることができるようになりました。以下に、リダイレクトが許可されているデバイスと許可されていないデバイスについて、VDA ホストのイベントビューアーに記録されるイベントメッセージの一部を示します。

Id	1000
Name	UsbEventAcceptDevice
Severity	Informational
Facility	System
Text	The Citrix USB Service allows the USB Device with Product ID: %2, Vendor ID: %3, and Device ID: %4 to be remoted.
Comment	This message logs the device info of a device redirected in an HDX session

Id	1001
Name	UsbEventPolicyRejectsDeviceV1
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the legacy “Client USB device redirection rules” policy rule.
Arguments	

Id	1002
Name	UsbEventPolicyRejectsDeviceV2
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules (Version 2)" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the "Client USB device redirection rules (Version 2)" policy rule. For instance, if the studio policy rule allows an approved set of devices and denies all other devices and an end user tries to create a new rule on the client endpoint via group policy, this event will get logged. This message would be indicative of an unauthorized device redirection attempt.
Arguments	

USB 診断ツール

`CtxUsbDiagnostics.exe` は、Citrix 管理者がクライアントで発生する USB デバイスのリダイレクトの問題を迅速に診断し、解決するのに役立つ VDA 上のコマンドラインツールです。このユーティリティツールは、HDX セッション内でリダイレクトに失敗するクライアントに接続された USB デバイスに関連する構成の問題をトリアージするために必要な重要な情報を収集します。

注：

- ツールがシステムレベルの操作を実行するために必要な権限を持っていることを確認するには、管理者としてコマンドプロンプトまたは PowerShell を実行する必要があります。

- `CtxUsbDiagnostics.exe` は `C:\Program Files\Citrix\HDX\bin\CtxUsbDiagnostics.exe` にあります。 そして、すでに環境変数の一部です。このパスに移動する必要はなく、管理者権限でコマンドプロンプトからこのツールを直接実行できます。

要件

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
  - Windows Server 2016 またはそれ以降
- VDA
  - Windows: Citrix Virtual Apps and Desktops™ のバージョン 2311 またはそれ以降

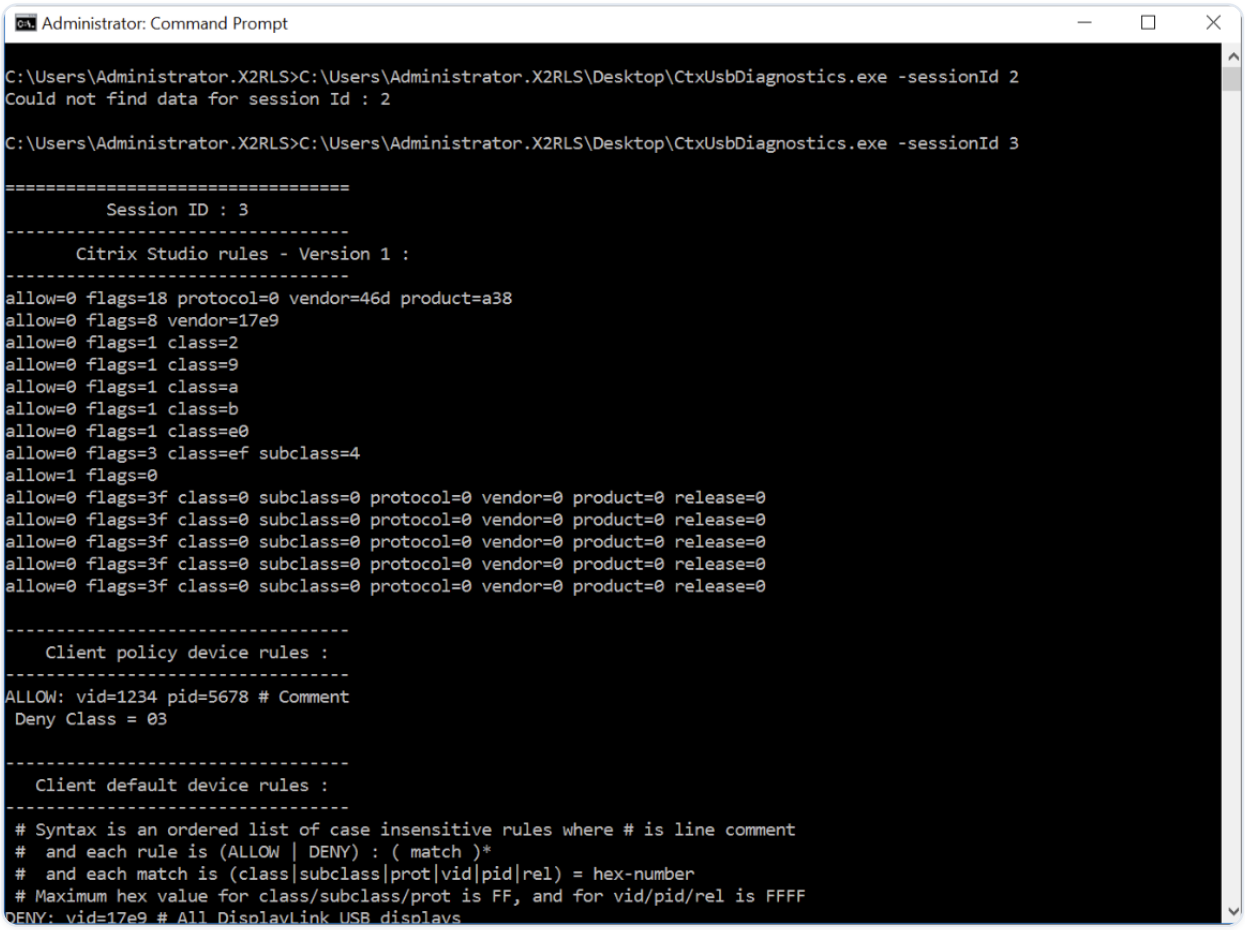
クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
- ワークスペースアプリ
  - Windows: バージョン 2311 以降

このツールで何ができますか?

このツールは現在、以下を提供します。

- セッションID
- VDAデバイスポリシー（Studioで設定されたデバイスルール）
- クライアントデバイスとクライアントデバイスポリシー（デバイスルール）
- デバイスのリスト、そのリダイレクト状態、および許可または拒否された理由



> **注：**
>
> 管理者は、すべてのアクティブなセッションのデバイス情報を確認できます。

表示される情報

- **Citrix Studioルール - バージョン 1/2**
  - DDCルールは、Studioにおけるレガシーな「**クライアントUSBデバイスリダイレクトルール**」または「**クライアントUSBデバイスリダイレクトルール（バージョン2）**」ポリシーの使用を示します。このセクションに記載されている情報は、Citrix®管理者が構成したすべてのルールを一覧表示します。

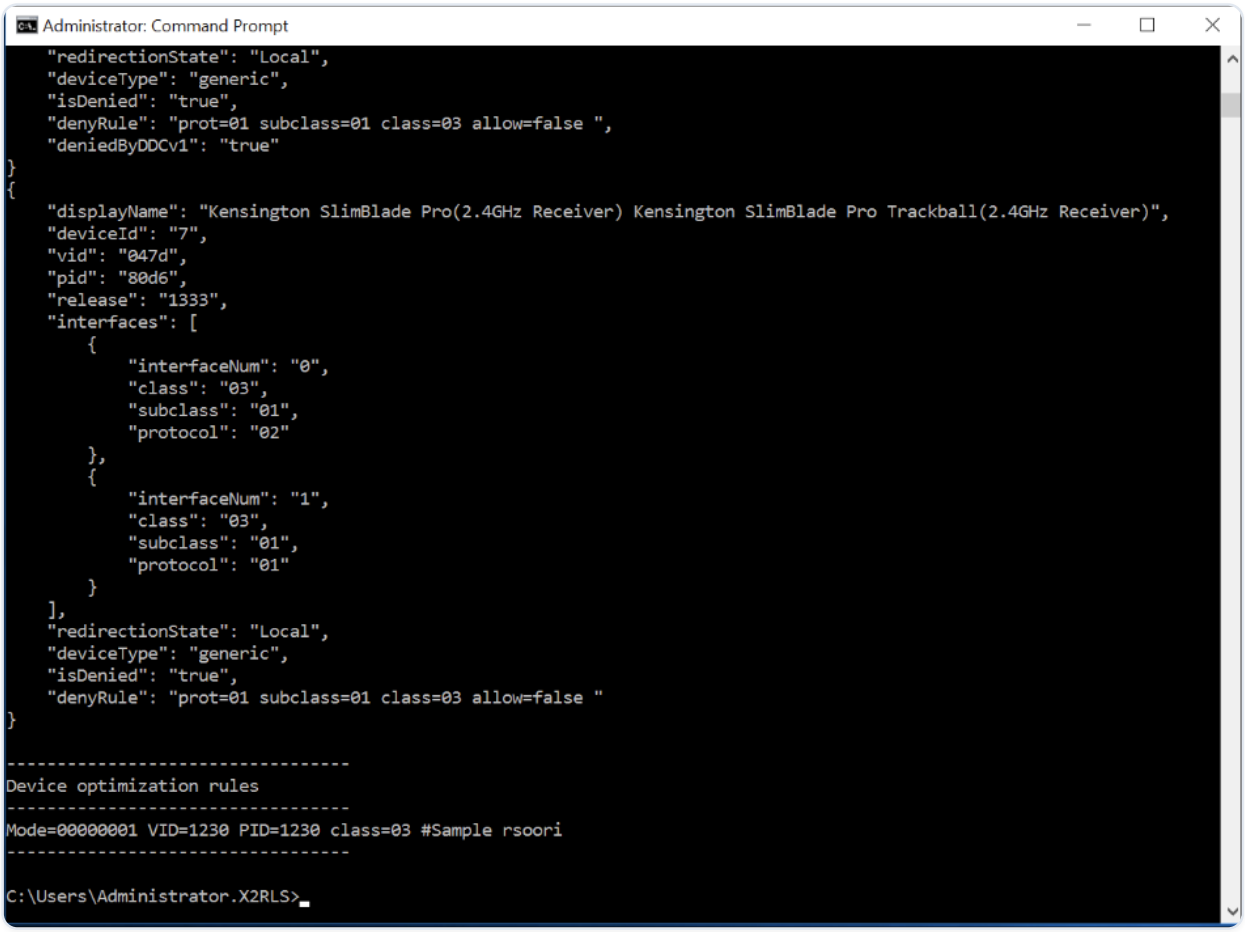
```
C:\Program Files\Citrix\HDX\bin>CtxUsbDiagnostics.exe

---------------------------------
          Session ID : 1
---------------------------------
       Citrix Studio rules - Version 2 :
---------------------------------
DENY: vid=046D pid=0A38
# Block some devices we never want to see
DENY: vid=17e9 # All DisplayLink USB displays
```

- **クライアントの既定のデバイス規則**
  - このセクションには、クライアントのレジストリに設定されているルールが一覧表示されます。

```
---------------------------------
  Client default device rules :
---------------------------------
 # Syntax is an ordered list of case insensitive rules where # is line comment
 #  and each rule is (ALLOW | DENY) : ( match )*
 #  and each match is (class|subclass|prot|vid|pid|rel) = hex-number
 # Maximum hex value for class/subclass/prot is FF, and for vid/pid/rel is FFFF
DENY: vid=17e9 # All DisplayLink USB displays
CONNECT: vid=1188 pid=A101 # Bloomberg 5 Biometric module
DENY: vid=1188 pid=A001 split=01 intf=00 # Bloomberg 5 Primary keyboard
CONNECT: vid=1188 pid=A001 split=01 intf=01 # Bloomberg 5 Keyboard HID
DENY: vid=1188 pid=A301 split=01 intf=02 # Bloomberg 5 Keyboard Audio Channel
CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # Bloomberg 5 Keyboard Audio HID
DENY: class=02 # Communications and CDC-Control
DENY: class=09 # Hub devices
DENY:vid=045e pid=079A # Microsoft Surface Pro 1 Touch Cover
DENY:vid=045e pid=079c # Microsoft Surface Pro 1 Type Cover
DENY:vid=045e pid=07dc # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07dd # Microsoft Surface Pro JP 3 Type Cover
DENY:vid=045e pid=07de # Microsoft Surface Pro 3_2 Type Cover
DENY:vid=045e pid=07e2 # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07e4 # Microsoft Surface Pro 4 Type Cover with fingerprint reader
DENY:vid=045e pid=07e8 # Microsoft Surface Pro 4_2 Type Cover
DENY:vid=03eb pid=8209 # Surface Pro Atmel maXTouch Digitizer
ALLOW:vid=056a pid=0315 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=0314 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=00fb class=03 # Wacom DTU tablet
DENY: class=03 subclass=01 prot=01 # HID Boot keyboards
DENY: class=03 subclass=01 prot=02 # HID Boot mice
DENY: class=0a # CDC-Data
DENY: class=0b # Smartcard
DENY: class=e0 # Wireless controller
DENY: class=ef subclass=04 # Miscellaneous network devices
ALLOW: # Otherwise allow everything else
```

- **デバイス最適化ルール**
  - このセクションには、「クライアントUSBデバイス最適化ルール」で設定されているデバイス最適化ルールが一覧表示されます。



デバイスリスト

このセクションには、クライアントエンドポイントに接続されている各デバイスに関する貴重な情報（ハードウェア情報、リダイレクトされているかどうか、正しいデバイスリダイレクトルールが設定されているかどうかなど）が一覧表示されます。

タグ名	説明
displayName	デバイスの一般名を一覧表示します。
ベンダーID	ベンダーID
製品ID	製品ID
インターフェース	複合デバイスが複数の子デバイスに分割されている場合、このサブセクションにはすべてのインターフェースが一覧表示されます。
InterfaceNum	インターフェース記述子のインデックスを示します
クラス	クラスコード

タグ名	説明
サブクラス	サブクラスコード
プロトコル	プロトコル
redirectionState	**Local** は、デバイスがICA®セッションでリダイレクトされていないことを示します。**ThisSession** は、デバイスがICAセッションでリダイレクトされていることを示します。**OtherSession** は、デバイスが別のICAセッションでリダイレクトされていることを示します。
deviceType	「**generic**」は、デバイスに最適化された仮想チャネルがなく、トラフィックがUSB仮想チャネルを介して流れていることを示します。「**optimized**」は、デバイスに関連付けられたデータ転送が専用の仮想チャネルを介して行われていることを意味します。
isDenied	「**true**」は、管理者が設定したポリシー規則によりデバイスがリダイレクトされないことを示します。`false` は、適用されたポリシーによりデバイスがリダイレクトされることを示します。
denyRule	このフィールドは、**isDenied** が `true` に設定されている場合に役立ちます。これは、デバイスがリダイレクトされない原因となっているポリシー内の特定の規則を管理者に伝えます。

レガシーUSBリダイレクトの構成

バージョン2212より前のコンポーネントを使用している場合、またはLinux版CWAを使用している場合は、このガイドに従って環境でUSBリダイレクトを構成してください。

汎用USBリダイレクトの有効化

1. **Citrix Web Studio™ポリシー**を開き、**ポリシー**タブをクリックします。
2. **ポリシーの作成**をクリックし、**ICA® > USBデバイスポリシー**を展開します。
3. **クライアントUSBデバイスリダイレクト**ポリシー設定を編集します。

4. **許可**を選択し、**保存**をクリックします。

USBリダイレクトポリシー規則の作成

ユーザーがUSBデバイスを仮想デスクトップにリダイレクトしようとすると、一致が見つかるまで各USBポリシー規則に対して順番にチェックされます。いずれかのデバイスに対する最初の一致が最終と見なされます。最初の一致が許可規則である場合、一致したデバイスは仮想デスクトップへのリダイレクトが許可されます。最初の一致が拒否規則である場合、一致したデバイスはローカルデスクトップでのみ利用可能です。一致が見つからない場合は、デフォルトの規則が使用されます。

Studioコンソールで適切なデバイス規則を設定する:

1. **Citrix Web Studioポリシー**を開き、**ポリシー**タブをクリックします。
2. **ポリシーの作成**をクリックし、**ICA > USBデバイスポリシー**を展開します。
3. **クライアントUSBデバイスリダイレクト規則**ポリシー設定を編集します。
4. リダイレクトする必要がある各USBデバイスの説明に記載されている例に基づいて値を設定し、をクリックします。 例： Allow: VID=056A PID=00A4 #STU-430 Deny: Class=08 subclass=05 # Mass Storage

> **注：**

> Citrix®管理者が「デフォルト値を使用」をチェックし、「保存」をクリックすると、VDAの以下のレジストリでデフォルト規則が見つかります。

> **注意:**

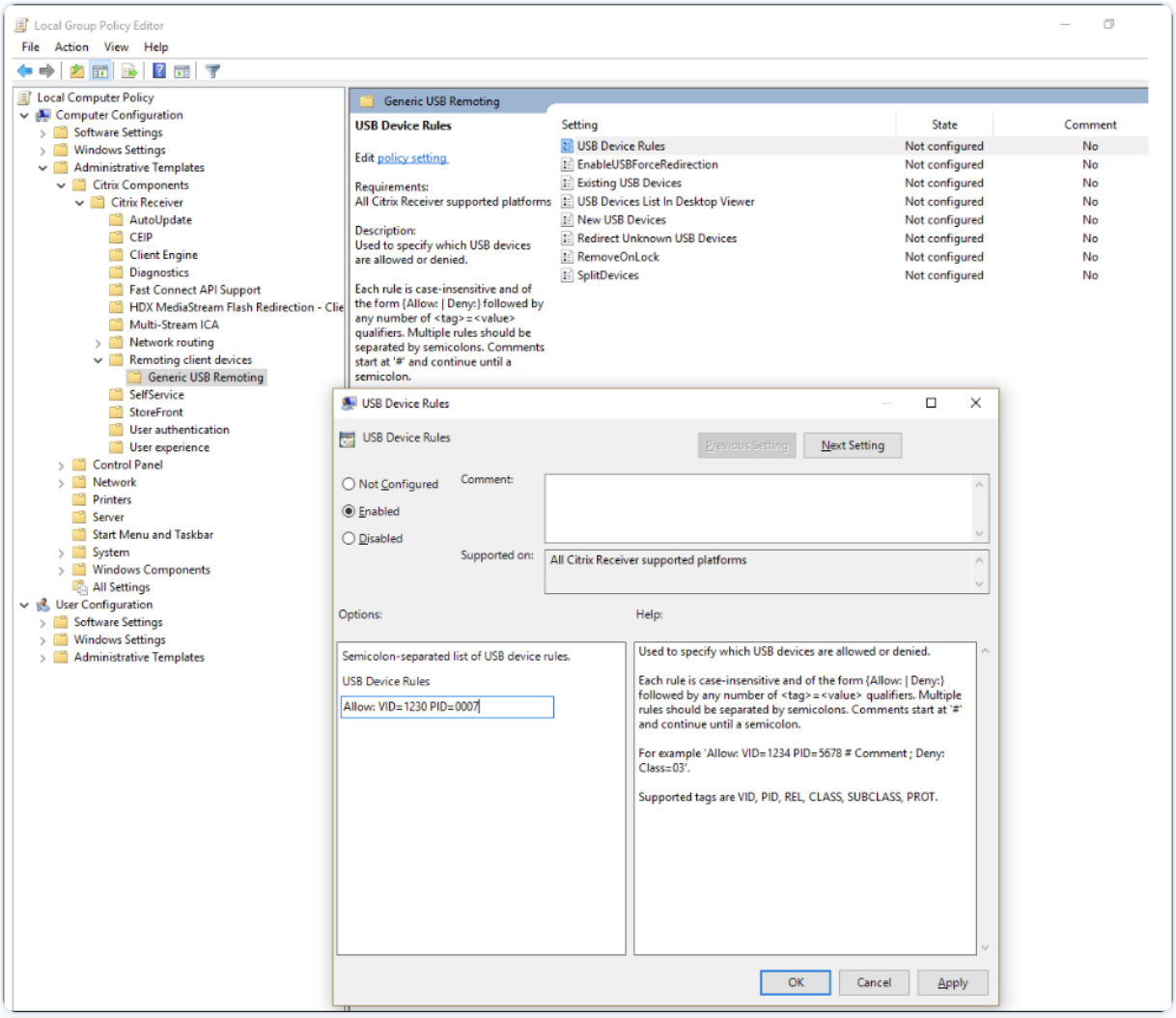
> レジストリエディターを使用する前に、この記事の最後にある免責事項を参照してください。 `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

クライアントで適切なGPOを設定する:

1. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrix Components > Citrix Receiver™ > リモートクライアントデバイス > Generic USB Remoting**に移動します。
2. **USBデバイスルール**設定を開き、**有効**に設定します。この例のようにUSBデバイスルールを追加します。 Allow: VID=1230 PID=0007 ルールは、ベンダーID 1230および製品ID 0007のデバイスを許可します。

注:

特定のデバイスがデバイスルールリストの最上位にある必要がある場合は、Allow: VID=xxxx PID=xxxx ルールを使用します。



注:

USBViewやConnectionツールバーなどのツールを使用して、VIDやPIDなどのデバイスの詳細を特定できます。

USBデバイスの自動リダイレクトを構成する

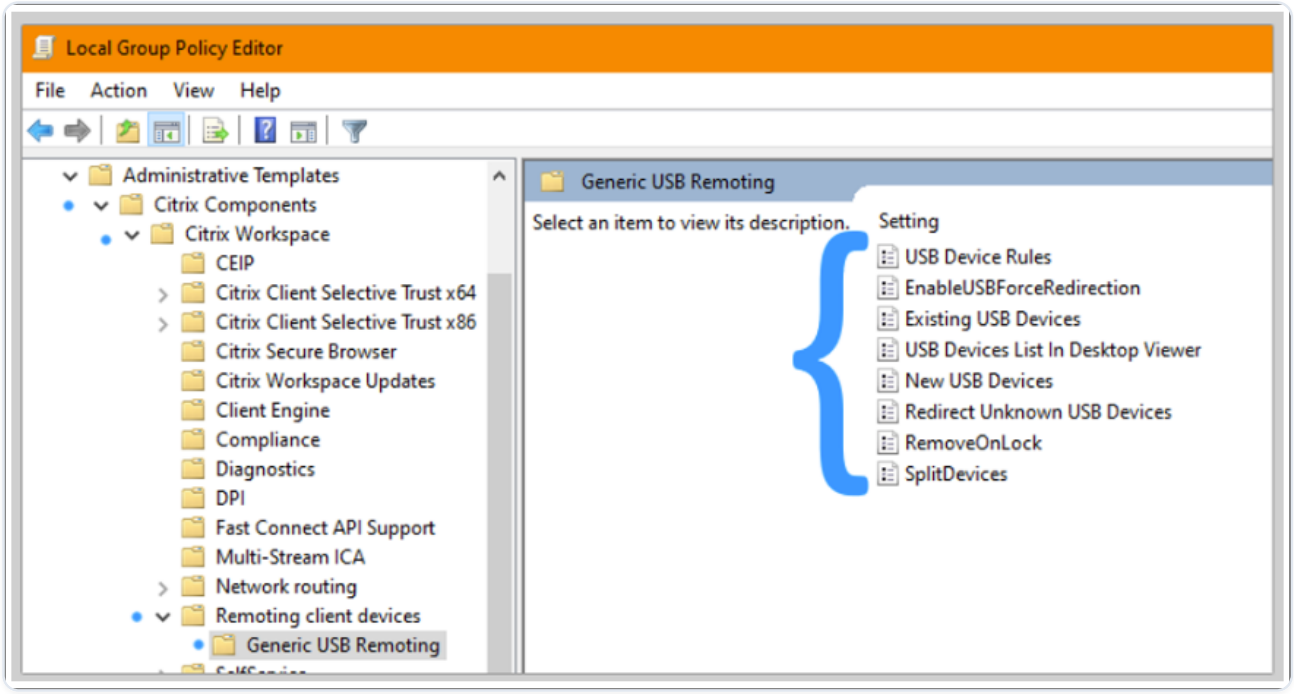
USBサポートが有効になっている場合、USBデバイスは自動的にリダイレクトされます。また、USBユーザー設定はUSBデバイスを自動的に接続するように設定されています。すべてのUSBデ

バイスをリダイレクトすることが常に最善とは限りません。ユーザーは、自動的にリダイレクトされないUSBデバイスリストからデバイスを明示的にリダイレクトできます。USBデバイスがリストされたりリダイレクトされたりするのを防ぐには、クライアントエンドポイントでDeviceRulesポリシー設定を使用します。

このポリシーは、GPO、クライアント側レジストリ、Citrix Workspace™ Preferences、またはCDViewerのConnectionsタブを使用してクライアントで設定できます。これらの方法はすべて以下に説明されています。

クライアントでGPOを使用する:

1. 「**ローカル グループ ポリシー エディター**」を開き、「**管理用テンプレート > Citrix コンポーネント > Citrix Receiver > リモート処理クライアント デバイス > 汎用 USB リモート処理**」に移動します。
2. 「**新しい USB デバイス**」を開き、「**有効**」を選択して「**OK**」をクリックします。
3. 「**既存の USB デバイス**」を開き、「**有効**」を選択して「**OK**」をクリックします。



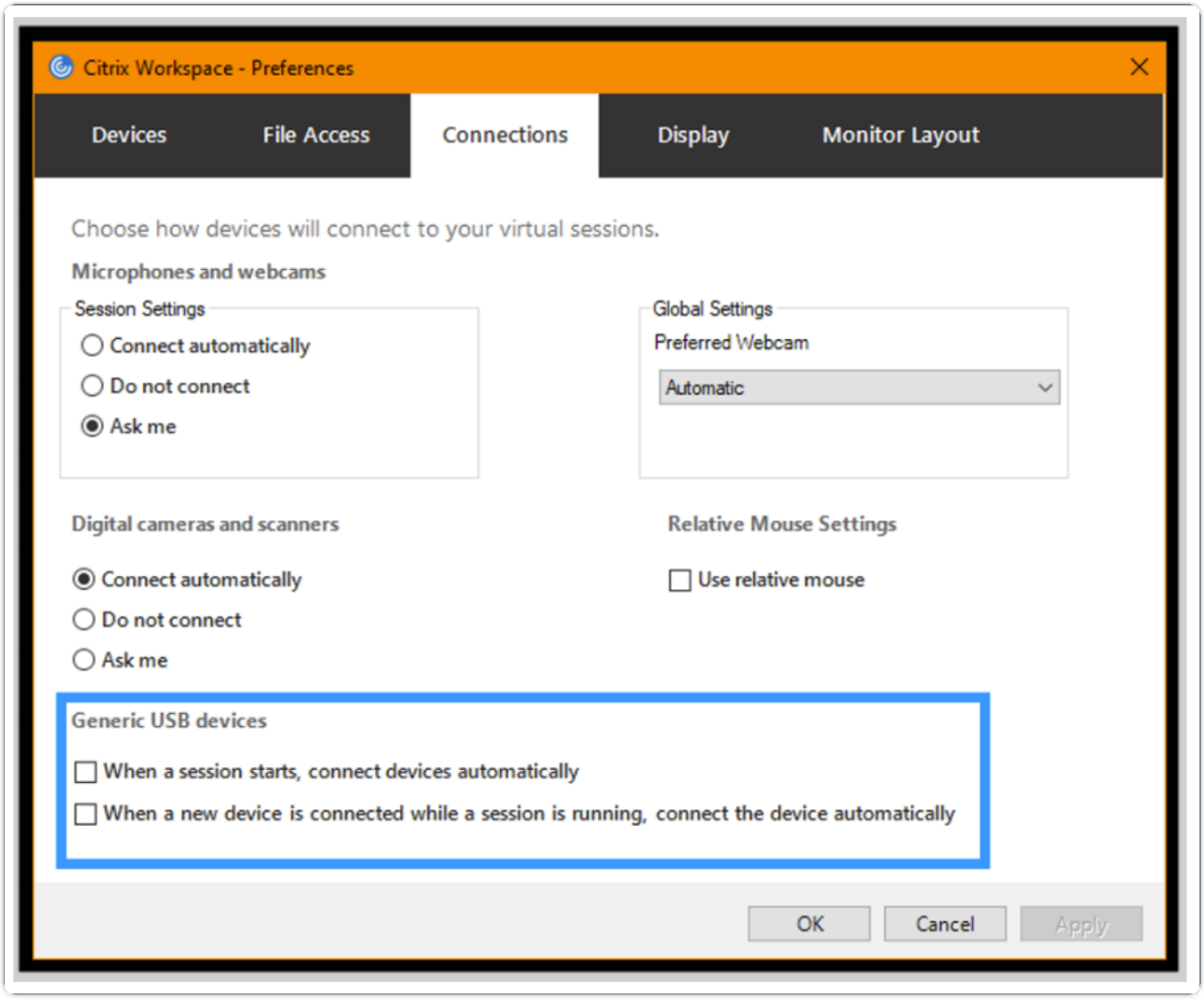
Citrix Connection Center を使用する場合:

1. 「**Citrix Workspace Preferences > Connections**」に移動してください。
2. 次のオプションが選択されていることを確認します。
   a. セッション開始時にデバイスを自動的に接続する
   b. セッション実行中に新しいデバイスが接続された場合、そのデバイスを自動的に接続する。

3. 「**OK**」をクリックします。

CDViewer 接続ツールバーを使用する場合:

1. セッション開始後、「**CDViewer**」ドロップダウンをクリックし、「**Citrix Workspace Preferences > Connections**」タブを選択します。
2. 次のオプションが選択されていることを確認します。
   a. セッション開始時にデバイスを自動的に接続する
   b. セッション実行中に新しいデバイスが接続された場合、そのデバイスを自動的に接続する。
3. ポリシーを保存するには、**適用**と**OK**をクリックします。



クライアントベースの構成の場合、レジストリキーはクライアントデバイスの次の場所に設定されます。

> **注意:**

> レジストリエディターを使用する前に、この記事の最後にある免責事項を参照してください。 `HKLM\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB`

異なるデバイスルールでUSBリダイレクトを使用して2つ以上のデバイスを構成する

複数のデバイスを、異なるデバイスルールでHDX™セッション内にリダイレクトできます。管理者は、一方のデバイスを自動的にリダイレクトし、もう一方のデバイスはエンドユーザーにリダイレクトのオプションを提供したい場合があります。以下に、異なるルールで2つのデバイスを構成する手順を示します。

1. **Citrix Web Studio**で**クライアントUSBデバイスリダイレクト**ポリシー設定を有効にします。
2. クライアント側のGPOで**USBデバイスルール**設定を編集します。
    a. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrixコンポーネント > Citrix Receiver > クライアントデバイスのリモート処理 > Generic USB Remoting**に移動します。
    b. **USBデバイスルール設定**を開き、設定を有効にします。この例のようにUSBデバイスルールを追加します。**Allow: VID=0911 PID=0c1c**ルールは、**ベンダーID 0911**および**製品ID 0c1c**を持つデバイスを許可しますが、自動的にはリダイレクトされません。**Connect: VID=06A8 PID=0043**ルールは、ステップ3で述べた自動リダイレクトポリシーが設定されている場合、**ベンダーID 06A8**および**製品ID 0043**を持つデバイスを自動的にリダイレクトします。
    c. **Allow**: VID=0911 PID=0c1c #Phillips スピーチマイク。
    d. **Connect**: VID=06A8 PID=0043 class=03 # Topaz HSB シグネチャパッド
3. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrixコンポーネント > Citrix Receiver > クライアントデバイスのリモート処理 > Generic USB Remoting**に移動します。
4. **新しいUSBデバイス**を開き、**有効**を選択して**OK**をクリックします。
5. **既存のUSBデバイス**を開き、**有効**を選択して、**OK**をクリックします。

これらの設定が完了すると、Topaz署名パッドはHDXセッション内で自動的にリダイレクトされ、セッション内でPhillipsスピーチマイクをリダイレクトするには、追加のエンドユーザー操作 (接続センターまたはCD Viewerのデバイスタブでリダイレクトオプションを選択) が必要になります。

> **注:**

上記の手順2と3の設定は、クライアント側のレジストリ値 **DeviceRules** (GenericUSBキー (HKLM\SOFTWARE\Wow6432Citrix\ICA Client\GenericUSB) の下) に直接適用することもできますが、これは推奨される方法ではありません。

汎用USBリダイレクトとクライアントドライブに関する考慮事項

HDX™テクノロジーは、ほとんどの一般的なUSBデバイスに対して**最適化されたサポート**を提供します。最適化されたサポートは、WAN経由でのパフォーマンスと帯域幅効率を向上させ、ユーザーエクスペリエンスを改善します。最適化されたサポートは、特に高遅延またはセキュリティに敏感な環境において、通常は最良の選択肢です。

HDXテクノロジーは、最適化されたサポートがない、または不適切な特殊なデバイスに対して**汎用USBリダイレクト**を提供します。例を次に示します。

- USBデバイスに、マウスやWebカメラのボタンが多いなど、最適化されたサポートに含まれない高度な機能がある場合。
- ユーザーが最適化されたサポートに含まれない機能を必要とする場合。
- USBデバイスが、試験測定機器や産業用コントローラーなどの特殊なデバイスである場合。
- アプリケーションが、USBデバイスとしてデバイスへの直接アクセスを必要とする場合。
- USBデバイスにWindowsドライバーしか利用できない場合。たとえば、スマートカードリーダーには、Android版Citrix Workspace™アプリ用のドライバーが利用できない場合があります。
- Citrix Workspaceアプリのバージョンが、この種類のUSBデバイスに対して最適化されたサポートを提供していない場合。

汎用USBリダイレクトでは、次のようになります。

- ユーザーはユーザーデバイスにデバイスドライバーをインストールする必要がありません。
- USBクライアントドライバーはVDAマシンにインストールされます。

重要:

- 汎用USBリダイレクトは、最適化されたサポートと組み合わせて使用できます。汎用USBリダイレクトを有効にする場合は、汎用USBリダイレクトと最適化されたサポートの両方について、Citrix USBデバイスポリシー設定を構成してください。

- クライアントUSBデバイス最適化規則のCitrixポリシー設定は、特定のUSBデバイスに対する汎用USBリダイレクトの特定のポリシー設定です。ここに記載されている最適化されたサポートには適用されません。

USBデバイスのパフォーマンスに関する考慮事項

ネットワークの遅延と帯域幅は、一部の種類のUSBデバイスで汎用USBリダイレクトを使用する場合、ユーザーエクスペリエンスとUSBデバイスの動作に影響を与える可能性があります。たとえば、タイミングに敏感なデバイスは、高遅延で低帯域幅のリンクでは正しく動作しない場合があります。可能な場合は、代わりに最適化されたサポートを使用してください。

一部のUSBデバイスは、使用可能にするために高い帯域幅を必要とします。たとえば、3Dマウス（通常、高い帯域幅を必要とする3Dアプリで使用されます）などです。帯域幅を増やすことができない場合でも、帯域幅ポリシー設定を使用して他のコンポーネントの帯域幅使用量を調整することで、問題を軽減できる場合があります。詳細については、クライアントUSBデバイスリダイレクトの帯域幅ポリシー設定と、マルチストリーム接続ポリシー設定を参照してください。

USBデバイスのセキュリティに関する考慮事項

一部のUSBデバイスは、スマートカードリーダー、指紋リーダー、署名パッドなど、本質的にセキュリティに敏感です。USBストレージデバイスなどの他のUSBデバイスは、機密データである可能性のあるデータを送信するために使用できます。

USBデバイスは、マルウェアを配布するためによく使用されます。Citrix WorkspaceアプリとCitrix Virtual Apps and Desktops™の設定により、これらのUSBデバイスからのリスクを軽減できますが、排除することはできません。この状況は、汎用USBリダイレクトまたは最適化されたサポートのどちらが使用されるかに関わらず適用されます。

重要:

セキュリティに敏感なデバイスとデータについては、常にHDX接続を保護してください。クライアントとVDA間の通信を参照してください。

必要なUSBデバイスのサポートのみを有効にしてください。このニーズを満たすように、汎用USBリダイレクトと最適化されたサポートの両方を構成してください。

USBデバイスを安全に使用するためのガイダンスをユーザーに提供してください。

- 信頼できる情報源から入手したUSBデバイスのみを使用してください。
- オープンな環境でUSBデバイスを放置しないでください。たとえば、インターネットカフェでのフラッシュドライブなどです。
- 複数のコンピューターでUSBデバイスを使用するリスクを説明してください。

USBマスストレージデバイスのセキュリティ制御

USBマスストレージデバイスには、最適化されたサポートが提供されます。このサポートは、Citrix Virtual Apps and Desktopsのクライアントドライブマッピングの一部です。ユーザーがログオンすると、ユーザーデバイス上のドライブが仮想デスクトップ上のドライブ文字に自動的にマッピングされます。ドライブは、マッピングされたドライブ文字を持つ共有フォルダーとして表示されます。クライアントドライブマッピングを構成するには、**クライアントリムーバブルドライブ**設定を使用します。この設定は、ICAポリシー設定のファイルリダイレクトポリシー設定セクションにあります。

USB大容量記憶装置では、クライアントドライブマッピングまたは汎用USBリダイレクト、あるいはその両方を使用できます。これらはCitrix®ポリシーを使用して制御します。主な違いは次のとおりです。

機能	クライアントドライブマッピング	汎用USBリダイレクト
デフォルトで有効	はい	いいえ
読み取り専用アクセスを構成可能	はい	いいえ

注:

USBリダイレクトは、たとえば50 Kbpsのような低帯域幅接続でもサポートされています。ただし、大きなファイルのコピーは機能しません。

クライアントドライブマッピング

クライアントドライブマッピングにより、クライアントエンドポイント上のストレージドライブがCitrix HDX™セッション内で利用可能になり、ファイルやフォルダーをクライアントからセッションホストへ、またはその逆に転送できるようになります。この機能は、読み取りおよび書き

込み権限の両方でデフォルトで有効になっています。ユーザーがマップされたクライアントデバイス上のファイルやフォルダーを追加または変更できないようにするには、**読み取り専用クライアントドライブアクセス**ポリシー設定を有効にします。この設定をポリシーに追加する際は、**クライアントドライブリダイレクト**設定が**許可**に設定されており、ポリシーにも追加されていることを確認してください。

セキュリティ上の予防措置として、エンドポイントドライブはデフォルトで実行権限なしでマップされます。ユーザーがマップされたクライアントドライブから直接実行可能ファイルを実行できるようにするには、セッションホストの**ExecuteFromMappedDrive**レジストリ値を編集します。詳細については、「**レジストリを通じて管理されるHDX機能**」セクションの「マップされたクライアントドライブ」を参照してください。

要件

CDMを使用するための要件は次のとおりです。

Citrixコントロールプレーン

- シトリックス Virtual Apps and Desktops™ 1912 以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1809以降
  - ウィンドウズ サーバー 2016 以降
  - Linux: Linux VDAのシステム要件を参照してください
- VDA
  - Windows: Citrix Virtual Apps™ and Desktops 1912以降のバージョンが必要です。
  - Linux: Linux VDAのドキュメントを参照してください

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Linux: Workspace app for Linuxのシステム要件を参照してください。

関連ポリシー

CDM設定については、ポリシー設定リファレンスセクションを参照してください。

ダブルホップシナリオ

CDMはダブルホップシナリオでサポートされています。デフォルトでは、クライアントエンドポイントのドライブはセカンドホップセッションにマップされ、ファーストホップのドライブは利用できません。ただし、クライアントエンドポイントのドライブの代わりに、ファーストホップのドライブがセカンドホップセッションにマップされるように設定することも可能です。

この機能を構成するには、以下のレジストリ値を編集します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientDrive\
- 値の名前: NativeDriveMapping
- 値の型: REG_SZ
- 値のデータ:
  - True - 最初のホップセッションのドライブを2番目のホップセッションにマップします
  - False - クライアントエンドポイントのドライブを2番目のホップセッションにマップします

> **注:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。レジストリエディターの使用は、お客様ご自身の責任において行ってください。編集する前に、必ずレジストリをバックアップしてください。

モバイルデバイスとタッチスクリーンデバイス

Citrix Virtual Apps and Desktops™ を使用すると、ユーザーはモバイルおよびタッチスクリーンクライアントデバイスから公開アプリケーションやデスクトップにアクセスできます。

要件

Citrix® コントロールプレーン

- シトリックス Virtual Apps™ and Desktops 1912 以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1903 以降
  - Windows 11 21H2 以降
- VDA
  - ウィンドウズ: Citrix Virtual Apps and Desktops バージョン 7.15 以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
- Windows 用 Citrix Workspace™ アプリ バージョン 1808 以降

Windows Continuum を使用するタッチスクリーンデバイスのタブレットモード

Continuum は、クライアントデバイスの使用方法に適応する Windows 10 の機能です。VDA は、タッチ対応クライアントでキーボードまたはマウスの存在を検出すると、クライアントをデスクトップモードにします。キーボードまたはマウスが存在しない場合、VDA はクライアントをタブレット/モバイルモードにします。この検出は、セッションの接続時および再接続時、ならびにセッション中にキーボードまたはマウスが接続または切断されたときに発生します。

この機能はデフォルトで有効になっています。この機能を無効にするには、ポリシー設定 タブレットモード切り替えポリシー設定 を構成します。

上記のタッチスクリーンデバイスの要件に加えて、Windows Continuumには以下が必要です。

ゼノサーバー (旧 シトリックス ハイパーバイザー™)

- Citrix Hypervisor 8.2 またはそれ以降のバージョン

- ラップトップ/タブレットの切り替えを許可するには、XenServer CLI コマンドを実行します。
  xe vm-param-set uuid=\<VM_UUID\> platform:acpi_laptop_slate=1

重要:

メタデータ設定を変更した後に既存のマシンカタログのベースイメージを更新しても、以前にプロビジョニングされたVMには影響しません。XenServer VMのベースイメージを変更した後、カタログを作成し、ベースイメージを選択して、新しいMachine Creation Services™ (MCS) マシンをプロビジョニングします。

セッションホスト

- オペレーティングシステム
  - Windows 10 1903 以降
  - Windows 11 21H2 以降
- VDA
  - Windows: バージョン 7.16 以降
  - **現在のオペレーティングシステム構成の制限により、ユーザーは最初のICA®セッションを開始してVDAを再起動した後、ドロップダウンメニューから以下のオプションを設定する必要があります。**
    - **設定 > システム > タブレットモード**
      - ハードウェアに適したモードを使用する
      - 常に切り替える（確認しない）

タブレットモードは、タッチスクリーンにより適したユーザーインターフェイスを提供します。

- ボタンが少し大きくなります。
- スタート画面と起動するすべてのアプリが全画面で開きます。
- タスクバーに「戻る」ボタンが含まれます。
- タスクバーからアイコンが削除されます。

ファイルエクスプローラーにアクセスできます。

Windows 10 は、この更新された BIOS に基づいて、ターゲット仮想マシンに GPIO ドライバーをロードします。これは、仮想マシン内でタブレットモードとデスクトップモードを切り替えるために使用されます。

Citrix Workspace app for HTML5 は Windows Continuum 機能に対応していません。

デスクトップモードは、PCとキーボード、マウスを使用するのと同じ方法で操作する従来のユーザーインターフェイスを提供します。

Microsoft Surface Pro および Surface Book 用のペン

Windows Inkベースのアプリケーションで標準のペン機能に対応しています。サポートには、ポインティング、消去、筆圧、Bluetooth信号、およびオペレーティングシステムのファームウェアとペンモデルに応じたその他の機能が含まれます。たとえば、筆圧は最大4096レベルまで可能です。この機能はデフォルトで有効になっています。

ペン機能のサポート要件は次のとおりです。

Citrixコントロールプレーン

- Citrix Virtual Apps and Desktops 1903 以降のバージョン
- Citrix DaaS (サービス)

セッションホスト

- オペレーティングシステム
  - Windows 10 1809以降
  - Windows 11 21H2 以降
- VDA
  - Windows では、Citrix Virtual Apps and Desktops 1903 以降が必要です。

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809以降
  - Windows 11 21H2以降
- Windows版Citrix Workspaceアプリ バージョン1902以降

Windows Inkとペン機能のデモンストレーションについては、このグラフィックをクリックしてください:



この機能を無効または有効にするには、レジストリで管理される機能の一覧にあるMicrosoft Surface ProおよびSurface Bookペンを参照してください。

既知の問題

ペンサポートに関する既知の問題は次のとおりです:

- Windows Server 2k22 の OS の制限により、ユーザーは 2k22 サーバーアプリケーションまたはデスクトップに接続している場合、コントロールパネルでペンのショートカットを設定したり、ペン/インクの設定を調整したりすることはできません。
- OSの制限により、ペン対応のWindows 11クライアントからペンのショートカットが認識されません。

シリアルポート

ほとんどの新しいPCには、内蔵のシリアル（COM）ポートがありません。USBコンバーターを使用すると、ポートを簡単に追加できます。シリアルポートに適したアプリケーションには、センサー、コントローラー、古いチェックリーダー、パッドなどがよく含まれます。一部のUSB仮想COMポートデバイスは、Windowsが提供するドライバー（usbser.sys）の代わりに、ベンダー固有のドライバーを使用します。これらのドライバーを使用すると、USBデバイスの仮想COMポートを強制的に設定できるため、異なるUSBソケットに接続しても変更されません。これは、**デバイスマネージャー > ポート (COM と LPT) > プロパティ**から、またはデバイスを制御するアプリケーションから行うことができます。

クライアントCOMポートマッピングを使用すると、ユーザーのエンドポイントのCOMポートに接続されたデバイスを仮想セッション中に使用できます。これらのマッピングは、他のネットワークマッピングと同様に使用できます。

各COMポートには、オペレーティングシステムのドライバーがCOM1やCOM2などのシンボリックリンク名を割り当てます。アプリケーションは、そのリンクを使用してポートにアクセスします。

> **重要:**

デバイスがUSBを直接使用してエンドポイントに接続できるからといって、汎用USBリダイレクトを使用してリダイレクトできるとは限りません。一部のUSBデバイスは仮想COMポートとして機能し、アプリケーションは物理シリアルポートと同じ方法でアクセスできます。オペレーティングシステムはCOMポートを抽象化し、ファイル共有のように扱うことができます。仮想COMの2つの一般的なプロトコルは、CDC ACMまたはMCTです。RS-485ポートを介して接続すると、アプリケーションがまったく機能しない場合があります。RS-485をCOMポートとして使用するには、RS-485-to-RS232コンバーターを入手してください。 **重要:**

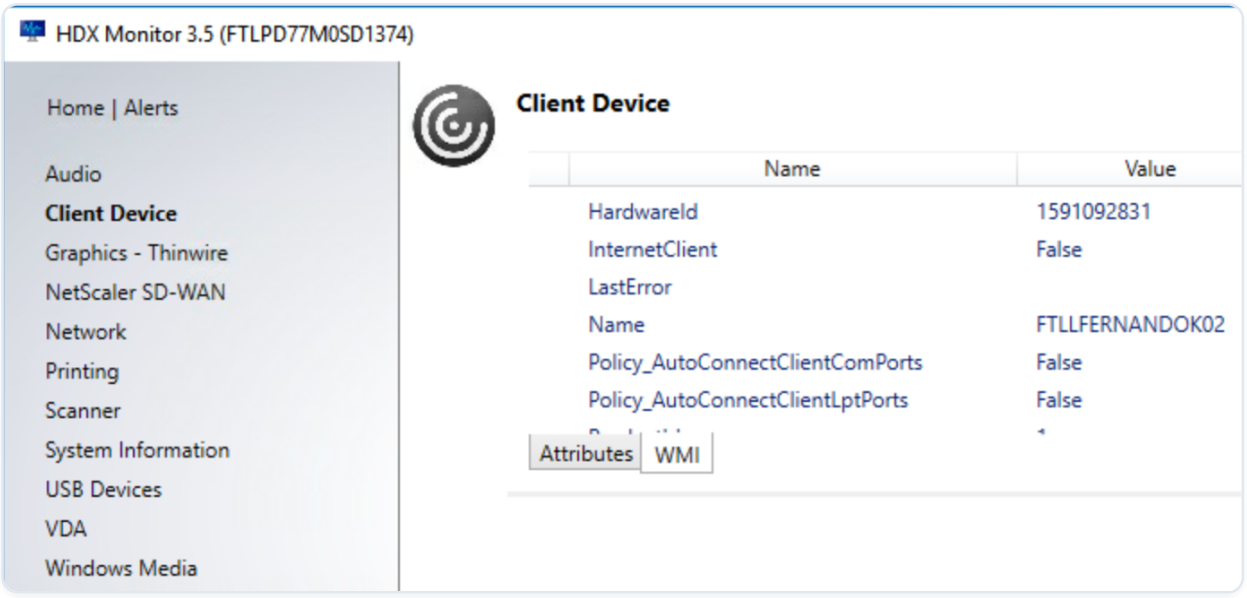
一部のアプリケーションは、デバイス（署名パッドなど）がクライアントワークステーションのCOM1またはCOM2に接続されている場合にのみ、一貫して認識します。

クライアントCOMポートをサーバーCOMポートにマッピングする

クライアントCOMポートをCitrix®セッションにマッピングするには、次の3つの方法があります。

- Studioポリシー。ポリシーの詳細については、「ポートリダイレクトポリシー設定」を参照してください。
- VDAコマンドプロンプト。
- リモートデスクトップ（ターミナルサービス）構成ツール。

1. **クライアントCOMポートリダイレクト**ポリシーと**クライアントCOMポートの自動接続Studio**ポリシーを有効にします。適用後、一部の情報はHDX™ Monitorで利用できます。



2. **クライアントCOMポートの自動接続**でポートのマッピングに失敗した場合は、手動でポートをマッピングするか、ログオンスクリプトを使用できます。VDAにログオンし、コマンドプロンプトウィンドウで次のように入力します。

   NET USE COMX: `\CLIENT\COMZ`:

   または

   NET USE COMX: `\CLIENT\CLIENTPORT:COMZ`:

   X はVDA上のCOMポートの番号です（1～9のポートをマッピングできます）。**Z** はマッピングするクライアントCOMポートの番号です。

   操作が成功したことを確認するには、VDAコマンドプロンプトで「**NET USE**」と入力します。表示されるリストには、マップされたドライブ、LPTポート、およびマップされたCOMポートが含まれます。

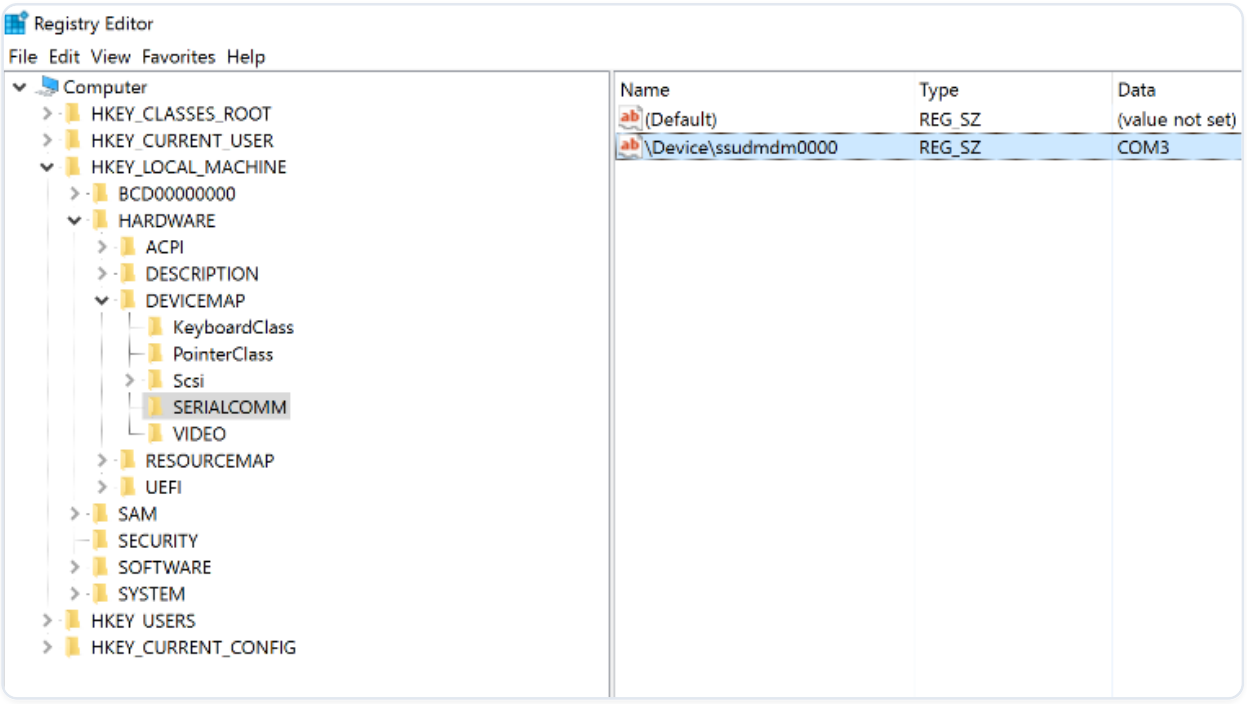
3. 仮想デスクトップまたはアプリケーションでこのCOMポートを使用するには、ユーザーデバイスアプリケーションをインストールし、マップされたCOMポート名を指定します。たとえば、クライアント上のCOM1をサーバー上のCOM3にマップする場合、VDAにCOMポートデバイスアプリケーションをインストールし、セッション中にCOM3を指定します。このマップされたCOMポートは、ユーザーデバイス上のCOMポートと同様に使用します。

重要:

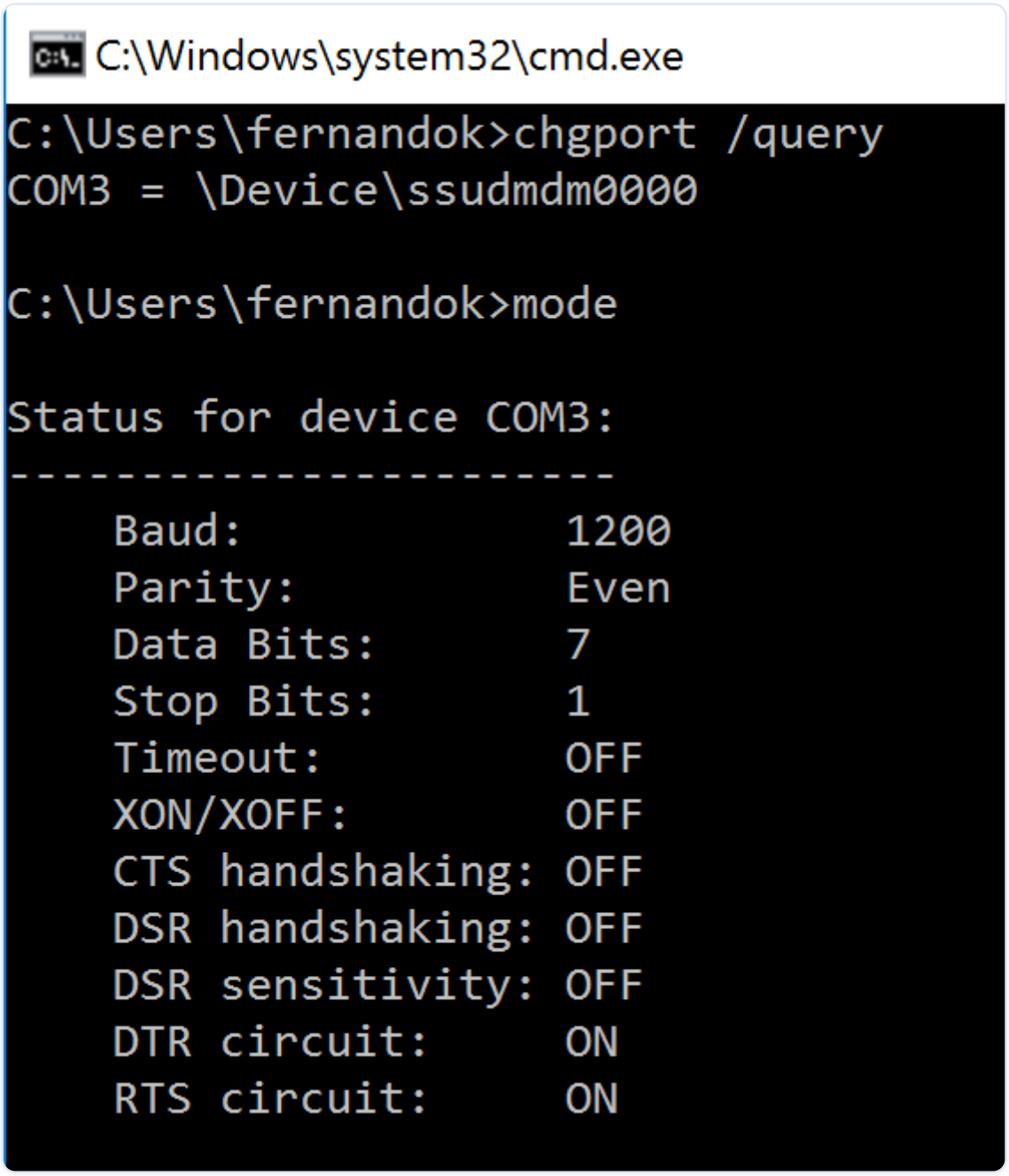
COMポートマッピングはTAPI互換ではありません。Windows Telephony Application Programming Interface（TAPI）デバイスをクライアントCOMポートにマッピングすることはできません。TAPIは、アプリケーションがデータ、FAX、音声通話の電話機能を制御するための標準的な方法を定義します。TAPIは、ダイヤル、応答、通話終了などのシグナリングを管理します。また、保留、転送、会議通話などの補足サービスも管理します。

トラブルシューティング

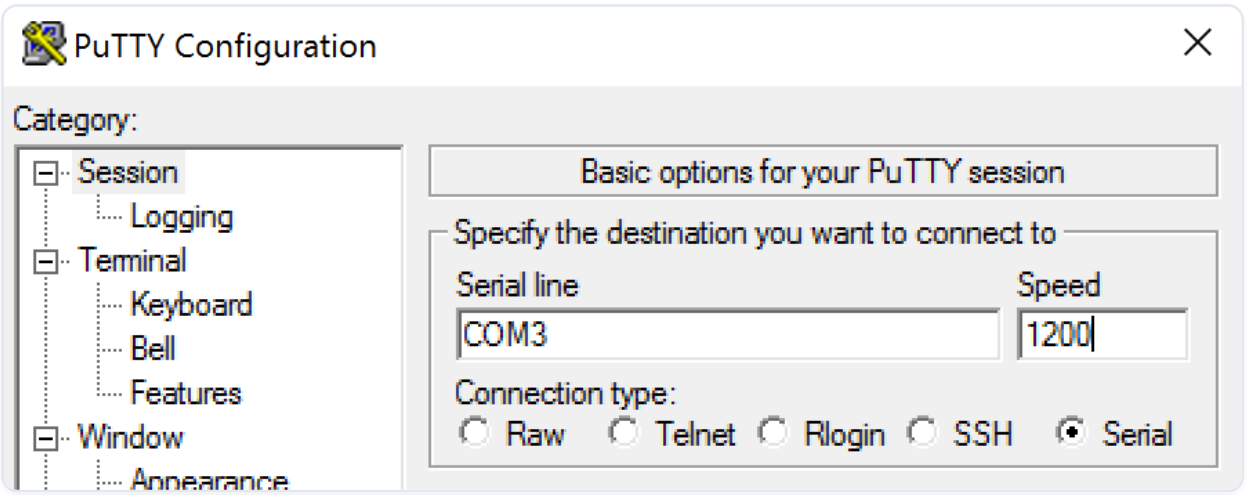
1. Citrixをバイパスして、エンドポイントからデバイスに直接アクセスできることを確認してください。ポートがVDAにマップされていない間は、Citrixセッションに接続されていません。デバイスに付属のトラブルシューティング手順に従い、まずローカルで動作することを確認してください。 デバイスがシリアルCOMポートに接続されている場合、ここに示されているハイブにレジストリキーが作成されます。



この情報は、コマンドプロンプトで「**chgport /query**」を実行することでも確認できます。



デバイスのトラブルシューティング手順が利用できない場合は、PuTTYセッションを開いてみてください。**Session** を選択し、**Serial line** でCOMポートを指定します。



ローカルコマンドウィンドウで **MODE** を実行できます。出力には、使用中のCOMポートと、PuTTYセッションで必要となるボーレート/パリティ/データビット/ストップビットが表示される場合があります。PuTTY接続が成功した場合は、**Enter** を押してデバイスからのフィードバックを確認します。入力した文字が画面に繰り返されたり、応答されたりする場合があります。この手順が失敗した場合、仮想セッションからデバイスにアクセスすることはできません。

2. ローカルのCOMポートをVDAにマッピングし（ポリシーまたは **NET USE COMX: \\\CLIENT\COMZ:** を使用）、前の手順と同じPuTTY手順を繰り返しますが、今回はVDA PuTTYから実行します。PuTTYがエラー **Unable to open connection to COM1. Unable to open serial port** を表示しない場合、別のデバイスがCOM1を使用している可能性があります。
3. **chgport /query** を実行します。VDA上の組み込みWindowsシリアルドライバーが \Device\Serial0をVDAのCOM1ポートに自動割り当てしている場合は、次の手順を実行します。 A. VDAでCMDを開き、**NET USE.** と入力します。

   B. VDA上の既存のマッピング（例：COM1）を削除します。

   NET USE COM1 /DELETE

   C. デバイスをVDAにマッピングします。

   NET USE COM1: `\CLIENT\COM3` :

   D. VDA上のアプリケーションをCOM3にポイントします。

   最後に、ローカルのCOMポート（例：COM3）をVDA上の別のCOMポート（COM1以外、例：COM3）にマッピングしてみてください。アプリケーションがそれにポイントされていることを確認してください。 **NET USE COM3: \\\CLIENT\COM3**
4. ポートがマッピングされているのにPuTTYは動作しているがデータが通過しない場合、競合状態である可能性があります。アプリケーションがマッピングされる前にポートに接続して開いてしまい、マッピングをロックしている可能性があります。次のいずれかを試してください。

   - 同じサーバーで公開されている2番目のアプリケーションを開きます。ポートがマッピングされるまで数秒待ってから、ポートを使用しようとする実際のアプリケーションを開きます。
   - StudioのかわりにActive DirectoryのグループポリシーエディターからCOMポートリダイレクトポリシーを有効にします。これらのポリシーは **Client COM port redirection** と **Auto connect client COM ports** です。このように適用されたポリシーは、Studioポリシーよりも前に処理され、COMポートが確実にマッピングされるようにします。Citrixポリシーは

VDAにプッシュされ、次の場所に保存されます。 `HKLN\SOFTWARE\Policies\Citrix\<user session ID\>`

- ユーザーにこのログオンスクリプトを使用するか、アプリケーションを公開する代わりに、まずVDA上のマッピングを削除し、仮想COMポートを再マッピングしてからアプリケーションを起動する.batスクリプトを公開します。

@echo off NET USE COM1 /delete NET USE COM2 /delete NET USE COM1: \\\CLIENT\COM1: NET USE COM2: \\\CLIENT\COM2: MODE COM1: BAUD=1200 (または必要な値) MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (または必要な値) START C:\\Program Files\\\<Your Software Path>\\\<your_software.exe>

5. SysinternalsのProcess Monitorは最後の手段のツールです。VDAでツールを実行する際、COM3、picaser.sys、CdmRedirector、特に\<your_app\>.exeのようなオブジェクトを見つけてフィルターします。エラーはAccess Deniedまたは類似の形で表示される場合があります。

特殊キーボード

Bloombergキーボード

> **警告:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になる可能性のある深刻な問題が発生する場合があります。Citrix®は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。レジストリエディターの使用は、お客様ご自身の責任において行ってください。編集する前に必ずレジストリをバックアップしてください。

Citrix Virtual Apps and Desktops™は、Bloombergモデル5、モデル4 Starboardキーボード（およびそれ以前のモデル3）をサポートしています。このキーボードにより、金融業界のお客様は、キーボードの特殊機能を使用して金融市場データにアクセスし、迅速な取引を実行できます。

> **重要:**

> Bloombergキーボードは1つのセッションでのみ使用することをお勧めします。複数の同時セッション（1つのクライアントから複数のセッションへ）でキーボードを使用することはお勧めしません。

> Bloombergキーボードは、1つの物理シェルに複数のUSBデバイスを搭載したUSB複合デバイスです。

- キーボード。
- 指紋リーダー。
- 音量を上げ下げしたり、スピーカーとマイクをミュートしたりするキーを備えたオーディオデバイス。このデバイスには、オンボードスピーカー、マイク、およびマイクとヘッドセット用のジャックが含まれています。
- これらすべてのデバイスをシステムに接続するためのUSBハブ。

要件:

- Citrix Workspace™ app for Windowsが接続するセッションは、USBデバイスをサポートしている必要があります。
- Bloombergキーボードモデル5をサポートするには、Linux版Citrix Workspaceアプリ2207以降が必要です。
- Bloombergキーボードモデル5をサポートするには、Windows版Citrix Workspaceアプリ2109以降が必要です。
- Bloombergキーボードモデル3および4をサポートするには、Windows版Citrix Workspaceアプリ1808以降、またはWindows版Citrix Receiver 4.8以降が必要です。
- モデル4でKVMモード（KVM経由でルーティングされた1本のUSBケーブルを含む2本のUSBケーブル）を使用するには、Windows版Citrix Workspaceアプリ1808以降、またはWindows版Citrix Receiver 4.12以降が必要です。

Citrix Workspace app for WindowsでのBloombergキーボードの構成については、Bloombergキーボードの構成を参照してください。

Bloombergキーボードのサポートを有効にするには、レジストリを介して管理される機能のリストでBloombergキーボードを参照してください。

サポートを確認する:

Citrix WorkspaceアプリでBloombergキーボードのサポートが有効になっているかを確認するには、Desktop ViewerがBloombergキーボードのデバイスを正しく報告しているかを確認します。

デスクトップシナリオ:

Desktop Viewerを開きます。Bloombergキーボードのサポートが有効になっている場合、Desktop ViewerにはUSBアイコンの下に3つのデバイスが表示されます。

Bloomberg 5キーボードの場合:

- ブルームバーグLP ブルームバーグ バイオメトリック モジュール
- Bloomberg LP Keyboard（2つのインターフェイスを持つ複合デバイス）
- Bloomberg LP Keyboard Audio（3つのインターフェイスを持つ複合デバイス）

Bloomberg 3および4キーボードの場合:

- ブルームバーグ 指紋スキャナー
- Bloombergキーボードの機能
- Bloomberg LPキーボード 2013

シームレスアプリケーションのみのシナリオ:

Citrix Workspaceアプリの通知領域アイコンから**接続センター**メニューを開きます。Bloombergキーボードのサポートが有効になっている場合、3つのデバイスが**デバイス**メニューに表示されます。

これらの各デバイスのチェックマークは、それらがセッションにリモート接続されていることを示します。

Windows VDAでのダブルホップにおけるキーイベントシーケンス処理のサポート

この機能により、クライアントデバイスが非WindowsでUnicodeモードで動作している場合、Windows Virtual Desktop Agent (VDA) でキーイベントが順次送信されるようになります。これにより、以下のような特定の入力関連の問題が解決されます。

1. RDPをセカンドホップとするダブルホップシナリオ。
    - ドイツ語キーボードレイアウトを使用している場合、**AltGr**キーを押しながら**q**を押すと、出力は**@**になるはずです。しかし、この機能がない場合、実際の出力は**q**になります。
2. キーショートカット機能
    - Android版Citrix Workspace™ App (CWA) を使用している場合、Windows VDAで**Alt+Tab**ショートカットが常に機能しないことがあります。

この機能を有効にすることで、これらの入力の不整合が解決されます。これにより、正確なキーイベント処理とユーザビリティの向上が保証されます。

この機能はデフォルトで無効になっています。この機能の切り替えは、レジストリ設定で `EnableSendUnicodeKeyQueue` です。

新しいレジストリ `HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\icawd\EnableSendUnicodeKeyQueue` DWORD = 0/1 が使用され、値が1の場合に新しい実装に切り替わります。

デフォルトでは、値は0です。

> **注:**
>
> ダブルホップ使用シナリオの場合、上記のレジストリキーを1stホップのWindows VDAに設定します。

Windows - キーボードおよびIMEサポートツール

これは、キーボードと入力メソッドエディターに関連する問題を診断できるセルフサービスコマンドラインツールです。

さまざまなユーザー要件を満たし、プラットフォームの汎用性を提供し、ユーザーにパーソナライズされたニーズを提供するために、キーボードと入力方式エディター (IME) の機能は、VDA と Citrix Workspace™ アプリケーションにおけるさまざまな構成と機能に依存しています。

VDAまたはクライアント側の設定が正しくないと、予期しない入力動作が発生する可能性があります。

ただし、Citrix®はいくつかの一般的な使用シナリオに推奨設定を提供しており、これらの推奨事項は診断結果にも含まれています。

このツールを使用すると、以下のカテゴリの問題を特定できます。

- **キーボードタイプ不一致:** VDAキーボードタイプとクライアントキーボードタイプをチェックし、不一致がないか確認します。たとえば、VDAが101英語キーボードを使用しているのに、クライアントが日本語106キーボードを使用している場合などです。この診断は、JP 106/109キーボードおよびKO 103/106キーボードの使用例を対象としています。

- **キーボードレイアウト同期モードの不一致:** キーボードレイアウト同期設定、レジストリ設定、グループポリシーをチェックし、特定の環境における同期モード構成の問題を解決します。
- **クライアントキーボードレイアウトとVDAキーボードレイアウトの不一致:** クライアントキーボードレイアウトがVDAキーボードレイアウトと同じであるかを確認します。
- **リモート言語バーがアプリケーションセッションに表示されない:** エンドユーザーがアプリケーションセッションを起動し、複数のキーボードレイアウトを使用している場合に、リモート言語バーが表示されているかを確認します。

このコマンドラインツールは Windows VDA にホストされています - `CtxKbImeDiagnostics.exe`。 コマンドラインインターフェイスは以下のとおりです。

インターフェース	説明	注
`CtxKbimeDiagnostics`	現在のICA®セッションのみの診断結果を表示	ユーザーが管理者権限を持っている場合、すべてのアクティブなICAセッションの診断を表示します。ユーザーが管理者権限を持っていない場合、現在のユーザーのICAセッションの診断を表示します。
`CtxKbimeDiagnostics [-v]`	現在のセッションの設定情報と診断結果を表示	ユーザーが管理者権限を持っている場合、すべてのアクティブなICAセッションの診断を表示します。
`CtxKbimeDiagnostics [-v] [-s Session_Id]`	このセッションの設定情報と診断結果を表示	
`CtxKbimeDiagnostics [-s Session_Id]`	セッションを指定し、そのセッションの診断結果を表示	管理者権限は他のICAセッションを照会できます/通常ユーザーは自身のICAセッションのみを照会できます
`CtxKbimeDiagnostics [-s Session_Id] [-v]`	セッションを指定し、そのセッションのすべての設定情報と診断結果を表示	管理者権限は他のICAセッションを照会できます。通常ユーザーは自身のICAセッションのみを照会できます。

インターフェース	説明	注
`CtxKbimeDiagnostics [-h]`	サポートされている引数/パラメーターと例を表示	「ヘルプ」インターフェース
`CtxKbimeDiagnostics [-V]`	現在のツールバージョンを表示	

注:

このバージョンでは、クライアントとしてCWA Windowsのみがサポートされています。

グラフィックス

Citrix HDXグラフィックスには、Citrix Virtual Apps and Desktopsからのリッチグラフィックスアプリケーションの配信を最適化する、広範なグラフィックスアクセラレーションおよびエンコーディング技術が含まれています。これらのグラフィック技術は、グラフィックスを多用する仮想アプリケーションをリモートで操作する際に、物理デスクトップを使用するのと同じエクスペリエンスを提供します。

グラフィックスレンダリングには、ソフトウェアまたはハードウェアを使用できます。ソフトウェアレンダリングには、ソフトウェアラスタライザーと呼ばれるサードパーティライブラリが必要です。たとえば、WindowsにはDirectXベースのグラフィックス用のWARPラスタライザーが含まれています。場合によっては、代替のソフトウェアレンダラーを使用したいと思うかもしれません。ハードウェアレンダリング（ハードウェアアクセラレーション）には、グラフィックスプロセッサ（GPU）が必要です。

HDX™ Graphicsは、最も一般的なユースケース向けに最適化されたデフォルトのエンコーディング構成を提供します。Citrixポリシーを使用することで、IT管理者はさまざまな要件を満たし、望ましいユーザーエクスペリエンスを提供するために、グラフィックス関連のさまざまな設定を構成することもできます。

シンワイヤー

Thinwire は、Citrix Virtual Apps™ and Desktops で使用される Citrix のデフォルトのディスプレイリモート処理テクノロジーです。

ディスプレイリモートテクノロジーにより、あるマシンで生成されたグラフィックスを、通常はネットワーク経由で別のマシンに送信して表示できます。グラフィックスは、キーボード入力やマウス操作などのユーザー入力の結果として生成されます。

HDX スリーディー プロ

Citrix Virtual Apps and DesktopsのHDX 3D Pro機能により、ハードウェアアクセラレーションにグラフィックス処理ユニット（GPU）を使用して最高のパフォーマンスを発揮するデスクトップとアプリケーションを配信できます。これらのアプリケーションには、OpenGLおよびDirectXベースの3Dプロフェッショナルグラフィックスアプリケーションが含まれます。標準VDAはDirectXのGPUアクセラレーションのみをサポートします。

WindowsシングルセッションOS向けGPUアクセラレーション

HDX 3D Proを使用すると、ホストされたデスクトップの一部として、またはシングルセッションOSマシン上のアプリケーションとして、グラフィックスを多用するアプリケーションを配信できます。HDX 3D Proは、物理ホストコンピューター（デスクトップ、ブレード、ラックワークステーションを含む）と、XenServer®、vSphere、Hyper-V（パススルーのみ）ハイパーバイザーが提供するGPUパススルーおよびGPU仮想化テクノロジーをサポートします。

GPUパススルーを使用すると、専用のグラフィックス処理ハードウェアに排他的にアクセスできるVMを作成できます。ハイパーバイザーに複数のGPUをインストールし、これらのGPUのそれぞれにVMを1対1で割り当てることができます。

GPU仮想化を使用すると、複数の仮想マシンが単一の物理GPUのグラフィックス処理能力に直接アクセスできます。

WindowsマルチセッションOS向けGPUアクセラレーション

HDX 3D Proを使用すると、WindowsマルチセッションOSセッションで実行されているグラフィックスを多用するアプリケーションをサーバーのグラフィックス処理ユニット（GPU）でレンダリングできます。OpenGL、DirectX、Direct3D、およびWindows Presentation Foundation（WPF）のレンダリングをサーバーGPUに移行することで、グラフィックスレンダリングがサーバーCPUの速度を低下させることはありません。また、ワークロードがCPUとGPUの間で分割されるため、サーバーはより多くのグラフィックスを処理できます。

フレームホーク

> **重要:**
>
> Citrix Virtual Apps and Desktops 7 1903以降、Framehawkはサポートされなくなりました。代わりに、Thinwireをアダプティブトランスポートを有効にして使用してください。

> Framehawkは、ブロードバンドワイヤレス接続（Wi-Fiおよび4G/LTEセルラーネットワーク）を使用するモバイルワーカー向けのディスプレイリモートテクノロジーです。Framehawkは、スペクトル干渉やマルチパス伝播の課題を克服し、仮想アプリおよびデスクトップのユーザーにスムーズでインタラクティブなユーザーエクスペリエンスを提供します。

テキストベースのセッションウォーターマーク

テキストベースのセッションウォーターマークは、データ盗難を抑止し、追跡を可能にするのに役立ちます。この追跡可能な情報は、写真やスクリーンキャプチャを使用してデータを盗む者への抑止力として、セッションデスクトップに表示されます。テキストのレイヤーであるウォーターマークを指定できます。ウォーターマークは、元のドキュメントの内容を変更することなく、セッション画面全体に表示できます。テキストベースのセッションウォーターマークにはVDAサポートが必要です。

アダプティブ リフレッシュ レート

新しいスケーラビリティの改善により、HDXは仮想モニターのリフレッシュレートをターゲットFPSポリシー設定に一致させます。アダプティブ リフレッシュ レート (ARR) は、シングルセッションVDAとマルチセッションVDAの両方で利用でき、GPUアクセラレーションシナリオと非GPUシナリオの両方で機能します。

損失許容モード

損失許容モードは、パケット損失が検出されたときにセッションがインタラクティブな状態を維持するように徹底的に再設計されています。

関連情報

- HDX 3D プロ
- WindowsシングルセッションOSのGPUアクセラレーション
- WindowsマルチセッションOSのGPUアクセラレーション
- フレームホーク
- シンワイヤー
- テキストベースのセッションウォーターマーク

シンワイヤー

Thinwire を搭載した HDX™ Graphics は、高性能で、適応性が高く、効率的なリモートデスクトップおよびアプリケーションエクスペリエンスを提供する Citrix の高度な表示テクノロジーです。

Thinwire は、グラフィックデータをインテリジェントに分析、キャッシュ、圧縮することで、多様なネットワーク条件やエンドポイントデバイス全体で最適なパフォーマンスを保証します。

エイチディーエックス™ スリーディー プロ

HDX 3D Pro（現在はHDX Graphicsとして知られています）は、要求の厳しいグラフィックワークロード向けに、高性能なユーザーエクスペリエンスを提供します。デフォルトでは、GPUを活用してDirectXおよびOpenGLアプリケーションの両方にハードウェアアクセラレーションを提供します。この機能は、以前はHDX 3D Proに関連付けられていましたが、追加のポリシーや構成を必要とせずに、すべてのユーザーがすぐに利用できるようになりました。

ハードウェアアクセラレーションを使用すると、設計、エンジニアリング、マルチメディア制作などの分野で使用されるものを含め、最もグラフィック負荷の高いアプリケーションでも、ユーザーにシームレスで応答性の高いエクスペリエンスを提供できます。

Citrix Virtual Apps and Desktops™のHDX 3D Pro機能により、ハードウェアアクセラレーションのためにグラフィック処理ユニット（GPU）を使用して最高のパフォーマンスを発揮するデスクトップとアプリケーションを提供できます。これらのアプリケーションには、OpenGLおよびDirectXベースの3Dプロフェッショナルグラフィックアプリケーションが含まれます。標準VDAはDirectXのGPUアクセラレーションのみをサポートします。

HDX 3D Proポリシー設定については、「3Dグラフィックワークロードの最適化」(/ja-jp/citrix-virtual-apps-desktops/2511/policies/reference/ica-policy-settings/graphics-policy-settings.html#optimize-for-3d-graphics-workload)を参照してください。

サポートされているすべてのCitrix Workspaceアプリは、3Dグラフィックで使用できます。複雑な3Dワークロード、高解像度モニター、マルチモニター構成、および高フレームレートアプリケーションで最高のパフォーマンスを得るには、Citrix Workspaceアプリ for WindowsおよびCitrix Workspaceアプリ for Linuxの最新バージョンをお勧めします。サポートされているCitrix Workspaceアプリのバージョンに関する詳細については、Citrix Workspaceアプリのライフサイクルマイルストーンを参照してください。

3Dプロフェッショナルアプリケーションの例は次のとおりです。

- コンピューター支援設計、製造、エンジニアリング (CAD/CAM/CAE) アプリケーション
- 地理情報システム (GIS) ソフトウェア
- 医用画像処理通信システム (PACS)
- 最新のOpenGL、DirectX、NVIDIA CUDA、OpenCL、およびWebGLバージョンを使用するアプリケーション
- 並列コンピューティングにNVIDIA Compute Unified Device Architecture (CUDA) GPUを使用する、計算負荷の高い非グラフィックアプリケーション

HDX 3D Proは、あらゆる帯域幅で最高のユーザーエクスペリエンスを提供します。

- WAN接続の場合：1.5 Mbpsという低い帯域幅のWAN接続でも、インタラクティブなユーザーエクスペリエンスを提供します。
- LAN接続の場合：LAN接続でローカルデスクトップと同等のユーザーエクスペリエンスを提供します。

  複雑で高価なワークステーションを、グラフィック処理をデータセンターに移動して一元管理することで、よりシンプルなユーザーデバイスに置き換えることができます。

特殊なユースケース向けのロスレス圧縮オプション

HDX 3D Proは、医用画像処理など、ピクセルパーフェクトなグラフィックが必要なアプリケーションをサポートするために、CPUベースのロスレスコーデックも提供します。真のロスレス圧縮は、より多くのネットワークリソースと処理リソースを消費するため、特殊なユースケースでのみ推奨されます。

ロスレス圧縮を使用する場合：

- 通知領域アイコンであるグラフィックステータスインジケーターのロスレスインジケーターは、表示されている画面がロッシーフレームかロスレスフレームかをユーザーに通知します。このアイコンは、**視覚品質**ポリシー設定で**ロスレスにビルド**が指定されている場合に役立ちます。送信されるフレームがロスレスの場合、ロスレスインジケーターは緑色に変わります。

  ロスレス-1(/en-us/citrix-virtual-apps-desktops/2511/media/lossless-indicator1.png)

  ロスレス-2(/en-us/citrix-virtual-apps-desktops/2511/media/lossless-indicator2.png)
- ロスレススイッチを使用すると、ユーザーはセッション中にいつでも**常にロスレス**モードに変更できます。セッション内で**ロスレス**を選択またはクリアするには、アイコンを右クリックして**ピクセルパーフェクトに切り替え**をクリックするか、ショートカットALT+SHIFT+1を使用します。
  - ロスレス圧縮の場合：HDX 3D Proは、ポリシーで選択されたコーデックに関係なく、ロスレスコーデックを圧縮に使用します。
  - ロッシー圧縮の場合：HDX 3D Proは、デフォルトまたはポリシーで選択された元のコーデックを使用します。 ロスレススイッチの設定は、以降のセッションでは保持されません。すべての接続でロスレスコーデックを使用するには、**視覚品質ポリシー**設定で**常にロスレス**を選択します。

セッション内でロスレスを選択または選択解除するためのデフォルトのショートカットALT+SHIFT+1を上書きできます。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator`で新しいレジストリ設定を構成します。

- 名前：HKEY_LOCAL_MACHINE_HotKey、種類：文字列
- ショートカットの組み合わせを構成する形式は、C=0|1, A=0|1, S=0|1, W=0|1, K=val です。キーはコンマ「,」で区切る必要があります。キーの順序は問いません。
- A、C、S、W、Kはキーであり、C=Control、A=ALT、S=SHIFT、W=Win、K=有効なキーです。Kに許可される値は、0〜9、a〜z、および任意の仮想キーコードです。
- 例： F10の場合、K=0x79を設定 Ctrl + F10の場合、C=1, K=0x79を設定 Alt + Aの場合、A=1, K=a または A=1, K=A または K=A, A=1を設定 Ctrl + Alt + 5の場合、C=1, A=1, K=5 または A=1, K=5, C=1を設定 Ctrl + Shift + F5の場合、A=1, S=1, K=0x74を設定

HDX 3D Proのユーザーエクスペリエンスを最適化する

複数のユーザーが帯域幅の制限された接続を共有している場合（たとえば、支店など）、各ユーザーが利用できる帯域幅を制限するために、「Overall session bandwidth limit」ポリシー設定を使用することをお勧めします。この設定を使用すると、ユーザーがログオンおよびログオフする際に利用可能な帯域幅が大きく変動しないようにします。HDX 3D Proは利用可能なすべての帯域幅を使用するように自動的に調整されるため、ユーザーセッション全体で利用可能な帯域幅が大きく変動すると、パフォーマンスに悪影響を及ぼす可能性があります。 たとえば、20人のユーザーが60 Mbpsの接続を共有している場合、各ユーザーが利用できる帯域幅は、同時接続ユーザー数に応じて3 Mbpsから60 Mbpsの間で変動する可能性があります。このシナリオでユーザーエクスペリエンスを最適化するには、ピーク時にユーザーごとに必要な帯域幅を決定し、常にこの量にユーザーを制限してください。 3Dマウスのユーザーの場合、Generic USB Redirection仮想チャネルの優先度を0に上げることをお勧めします。仮想チャネルの優先度を変更する方法については、Knowledge Centerの記事CTX128190を参照してください。 HDX Monitorツールを使用して、HDX視覚化テクノロジーの動作と構成を検証し、HDXの問題を診断およびトラブルシューティングします。このツールは、Citrix Virtual Apps™ and Desktopsのインストールメディアの**Support**フォルダーにあります。

GPU アクセラレーション

HDX™ Graphicsは、Virtual Delivery Agent (VDA) とエンドポイントデバイスの両方でGPUハードウェアをシームレスに活用します。

以前はHDX 3D Proとして知られていたこの標準で提供されるハードウェアアクセラレーションは、デフォルトで有効になっており、シングルセッションおよびマルチセッションオペレーティン

グシステムの両方で、グラフィックを多用するDirectXおよびOpenGLアプリケーションのパフォーマンスを大幅に向上させます。

Citrix Virtual Apps and Desktops™は、Windowsマルチセッションosセッションで実行されるグラフィックを多用するアプリケーションを、サーバーのグラフィック処理ユニット（GPU）でレンダリングすることをサポートします。OpenGL、DirectX、Direct3D、およびWindows Presentation Foundation (WPF) のレンダリングをサーバーのGPUに移行することで、サーバーのCPUをより効率的に使用できます。

Windows Serverはマルチユーザーオペレーティングシステムであるため、複数のユーザーがGPU仮想化（vGPU）を必要とせずに、Citrix Virtual Apps™によってアクセスされるGPUを共有できます。

レジストリの編集を伴う手順については、注意してください。レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。レジストリエディターは自己責任で使用してください。編集する前にレジストリをバックアップしてください。

GPU 共有

GPU 共有により、リモートデスクトップセッションで OpenGL および DirectX アプリケーションの GPU ハードウェアレンダリングが可能になります。次の特性があります。

- アプリケーションのスケーラビリティとパフォーマンスを向上させるために、ベアメタルまたは仮想マシンで使用できます。
- 複数の同時セッションでGPUリソースを共有できます（ほとんどのユーザーは専用GPUのレンダリングパフォーマンスを必要としません）。
- 特別な設定は不要です。

GPUは、ハイパーバイザーおよびGPUベンダーの要件に従って、フルパススルーモードまたは仮想GPU（vGPU）モードのいずれかでWindows Server仮想マシンに割り当てることができます。物理Windows Serverマシンへのベアメタル展開もサポートされています。

GPU共有は、特定のグラフィックカードに依存しません。

- 仮想マシンの場合、使用中のハイパーバイザーと互換性のあるグラフィックカードを選択してください。XenServerのハードウェア互換性リストについては、「Hypervisor Hardware Compatibility List」を参照してください。

- ベアメタルで実行する場合、オペレーティングシステムによって有効化された単一のディスプレイアダプターを使用することをお勧めします。ハードウェアに複数のGPUがインストールされている場合、デバイスマネージャーを使用して、1つを除くすべてを無効にしてください。

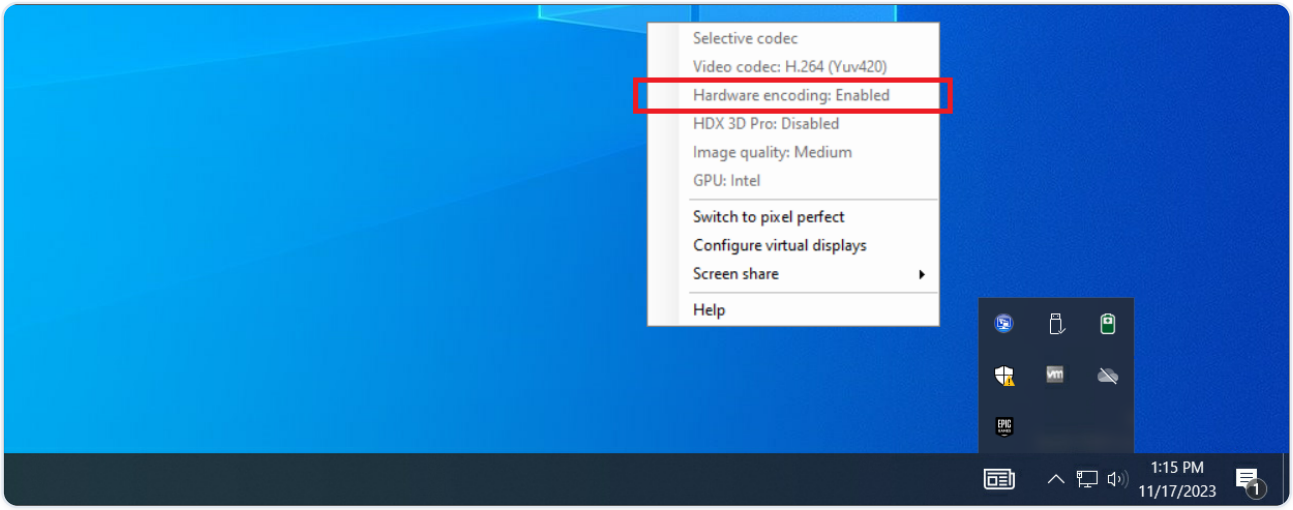
GPU Sharing を使用したスケーラビリティは、いくつかの要因によって異なります。

- 実行されているアプリケーション
- 消費するビデオ RAM の量
- グラフィックカードの処理能力

一部のアプリケーションは、他のアプリケーションよりもビデオRAMの不足をうまく処理します。ハードウェアが過負荷になると、グラフィックカードドライバーの不安定化やクラッシュが発生する可能性があります。このような問題を避けるため、同時実行ユーザーの数を制限してください。

- NVIDIA GPUおよびIntel Iris Proグラフィックスプロセッサ用の高性能ビデオエンコーダーへのアクセス。ポリシー設定（デフォルトで有効）がこの機能を制御し、H.264エンコーディング（利用可能な場合）にハードウェアエンコーディングの使用を許可します。このようなハードウェアが利用できない場合、VDAはソフトウェアビデオコーデックを使用したCPUベースのエンコーディングにフォールバックします。詳細については、「グラフィックポリシー設定」を参照してください。

GPU アクセラレーションが機能していることを確認するには、グラフィックステータスインジケーターを使用できます。



DirectX、Direct3D、および WPF レンダリング

DirectX、Direct3D、および WPF レンダリングは、ディスプレイドライバーインターフェイス（DDI）バージョン 9ex、10、または 11 をサポートする GPU を搭載したサーバーでのみ利用できます。

- Windows Server 2016以降では、RDセッションホストサーバー上のRemote Desktop Services (RDS) セッションは、Microsoft Basic Render Driverをデフォルトのアダプターとして使用します。Windows Server 2016以降のRDSセッションでGPUを使用するには、グループポリシーの**ローカルコンピューターポリシー** \> **コンピューターの構成** \> **管理用テンプレート** \> **Windowsコンポーネント** \> **Remote Desktop Services** \> **リモートデスクトップセッションホスト** \> **リモートセッション環境**で、**すべてのRemote Desktop Servicesセッションにハードウェアのデフォルトグラフィックアダプターを使用する**設定を有効にします。
- WPFアプリケーションがサーバーのGPUを使用してレンダリングできるようにするには、Windows Multi-session OSセッションを実行しているサーバーのレジストリに設定を作成します。レジストリ設定の詳細については、レジストリで管理される機能のリストにある「Windows Presentation Foundation (WPF) レンダリング」を参照してください。

CUDAまたはOpenCLアプリケーションのGPUアクセラレーション

ユーザーセッションで実行されているCUDAおよびOpenCLアプリケーションのGPUアクセラレーションは、デフォルトで無効になっています。

CUDA アクセラレーション機能を使用するには、レジストリ設定を有効にします。詳細については、レジストリで管理される機能のリストにある「CUDA または OpenCL アプリケーションの GPU アクセラレーション」を参照してください。

10ビットハイダイナミックレンジ (HDR)

10ビットハイダイナミックレンジ (HDR) 仮想デスクトップセッションでは、強化されたエンコードおよびデコード機能を使用して、拡張された色域、より高いコントラストと明るさで高品質の画像とビデオをレンダリングできます。

システム要件

エンドポイント:

- NVIDIA GPU向けWindows用Citrix Workspace™アプリ2209以降
- エンドポイント上で10ビットHEVC (H.265) 444デコードをサポートするNVIDIA GPU

- 10ビットHDR対応モニター。ディスプレイ設定を使用して、すべてのモニターで10ビットHDRを有効にする必要があります。

サーバー:

- NVIDIA GPU向けWindowsシングルセッションOS VDA 2209以降、およびIntel GPU向けVDA 2308以降
- VDA上で10ビットHEVC 444エンコードをサポートするNVIDIA GPU

必要なポリシー

エンドポイント:

- グラフィックのH.265デコードを有効にする

サーバー:

- 3Dグラフィックワークロード向けに最適化
- グラフィックステータスインジケーター (オプション)

サーバー構成

10ビットHDR対応のエンドポイントモニターでCitrix®セッションを起動すると、HDRセッションがデフォルトで有効になります。マルチモニターHDRセッションでは、すべてのエンドポイントモニターで10ビットHDRが有効になっている必要があります。HDRセッションは、ウィンドウモードと全画面モードの両方でサポートされます。

参照白色レベル

この設定は、ニット値によって白色輝度レベルを定義します。セッション内の相対的なHDR画面の明るさを制御します。デフォルト値は80ニットです。異なるニット値を定義するには、次のレジストリキーを設定します。

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- 種類: REG_DWORD
- 名前: RefWhiteLevel

設定を有効にするには、セッションのサイズを変更するか、セッションを切断して再起動する必要があります。

EDIDのオーバーライド

VDAをHDRセッションでエンドポイントモニターのEDIDを使用するように構成できます。これにより、色域と輝度範囲を一致させることで、モニターの表示機能を最大限に活用できます。デフォルトでは、HDRセッションはHDR1000対応のディスプレイを想定しています。 エンドポイントモニターのEDIDは、NVIDIAまたはその他のツールを使用してエクスポートできます。次のレジストリキーを使用してVDAに適用します。

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- 種類: REG_BINARY
- 名前: EDIDオーバーライド

EDIDをレジストリに保存する際、コンマ、スペース、または特殊文字を含めてはなりません。オーバーライドEDIDを有効にするには、サインアウトして新しいセッションを起動します。

視覚的にロスレスなエクスペリエンス

視覚的にロスレスなエクスペリエンスを実現するには、次のポリシーを有効にします。

- 視覚的にロスレスな圧縮を許可する
- 視覚的品質: 常にロスレスまたはロスレスに構築

ポリシーが設定された後、グラフィックスステータスインジケーターを使用して、イメージ品質スライダーを使用するか、ピクセルパーフェクトモードに切り替えることで、HDRセッションの品質を制御できます。

Windowsの画面ロックを許可する

このポリシーを使用すると、画面ロックを含むすべてのWindowsディスプレイタイムアウトを、ワークステーションOS上のCitrix Virtual Desktopセッションに適用できます。この設定は、Citrix StudioのCitrixグループポリシーオブジェクトを使用して設定できます。

デフォルトでは、この設定が有効になっていない場合、アクティブなセッション中にCitrix Virtual Desktopはセッションロック、スクリーンセーバー、またはディスプレイオフのタイムアウトに応答しません。

ワークステーションVDAでパスワード保護されたスクリーンセーバーが構成されている場合、スクリーンセーバーのタイムアウトに達したときにCitrix Virtual Desktopセッションが自動的にロックされるようにするには、この設定を有効にする必要があります。

VDAでディスプレイオフタイムアウトが構成されている場合にこの設定を有効にすると、そのタイムアウトの期限切れにより、ユーザーがセッションとの対話を再開するまで更新されないセッションになります。たとえば、表示されている時間は更新されず、新しい通知も表示されません。

その他の考慮事項

- 仮想GPUで最大4台のモニターで10ビットHDRセッションを起動できます。
- 次の場合、Citrixセッションは8ビットの非HDRモードに戻ります。
  - いずれかのエンドポイントモニターで10ビットHDRが有効になっていない場合
  - 画面共有を有効にする。
  - VDAで仮想ディスプレイレイアウトを設定する。
  - **視覚的にロスレス圧縮を許可**ポリシーを設定せずにピクセルパーフェクトモードに切り替える。

アダプティブ リフレッシュレート

適応型リフレッシュレートを使用すると、HDX™ は仮想モニターのリフレッシュレートを設定されたターゲットFPSポリシーに一致させます。適応型リフレッシュレートは、シングルセッションVDAとマルチセッションVDAの両方で、優れたパフォーマンスとスケーラビリティを提供します。

ターゲットフレームレート(/en-us/citrix-virtual-apps-desktops/2511/media/targetframerate_60.png)

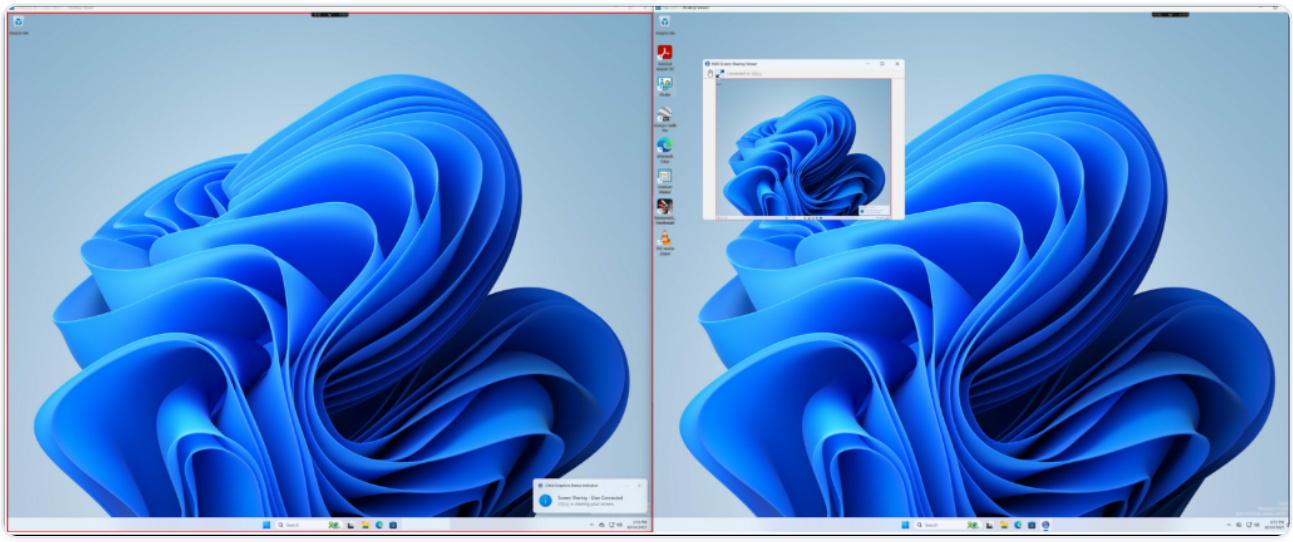
DirectX診断ツール(/en-us/citrix-virtual-apps-desktops/2511/media/directx-diagnostic-tool.png)

> **注**
>
> 適応型リフレッシュレートは、Citrix Indirect DisplayまたはIDDが使用されている場合（Citrix Virtual Apps and Desktops™のデフォルトに従って）にのみ利用可能であり、ベンダー提供のディスプレイアダプターを使用している場合は利用できません。

HDX画面共有

HDX画面共有は、Citrix Virtual Apps and Desktopsに組み込まれたネイティブな高性能機能であり、ユーザーが仮想セッション画面をリアルタイムで他のユーザーと共有できるようにします。低遅延と高品質を実現するように設計されており、サードパーティのソフトウェアソリューションを

実装することなく、コラボレーション、サポート、トレーニングのシナリオでシームレスなエクスペリエンスを提供します。



HDX画面共有機能はHDXプロトコルに直接統合されており、共有セッションが安全かつ効率的で、セッションパフォーマンスへの影響を最小限に抑えることができます。

HDX画面共有を使用すると、ユーザーはキーボードとマウスの制御を含むCitrixセッションのコンテンツ全体を、1人以上の参加者と共有できます。

この機能は高解像度ディスプレイをサポートし、最大8台のモニターに対応できます。

HDX画面共有は、Windows、Linux、macOSを含むすべてのVDAプラットフォームで利用でき、クロス互換性を提供します。これは、Windows VDAのユーザーがLinuxおよびmacOS VDAのユーザーと画面を共有できることを意味し、その逆も可能です。

さらに、HDX画面共有はクライアントコンポーネントに依存しないため、モバイルデバイスを含むすべてのクライアントプラットフォームでアクセス可能です。

主要な概念

- **共有者:** 仮想デスクトップセッションから画面共有を開始し、仮想セッションのデスクトップを他のユーザーに表示するユーザー
- **閲覧者:** 共有者のセッションに接続して画面を閲覧するユーザー（または複数のユーザー）。画面共有参加者とも呼ばれます。
- **接続コード:** 共有者が閲覧者に共有セッションへのアクセスを提供するために使用する、システム生成の一意のセキュリティコード。
- **グラフィックステータスインジケーター:** 画面共有セッションの開始、停止、管理のためのコントロールを提供する、通知領域にあるユーザーインターフェイス要素。

- **画面共有プレーヤー:** 閲覧者が共有者のセッションを閲覧するために使用するセッション内ツール。

ユースケースと使用例のシナリオ

HDX Screen Sharing を適切に構成し活用することで、IT サポートから共同開発、トレーニングまで、さまざまな組織のニーズに対応できます。

シナリオ 1: IT ヘルプデスクとリモートサポート

IT 管理者は、ユーザーが仮想デスクトップ内で経験している問題をトラブルシューティングする必要があります。問題を再現しようとする代わりに、IT 管理者は Citrix Director から HDX Screen sharing を介して Remote Assist を開始できます。 管理者はユーザーの正確な画面をリアルタイムで確認でき、問題の特定と解決が迅速になります。キーボードとマウスの制御を要求する機能により、管理者は直接操作を行うことができます。 HDX Screen sharing は、CVAD 2511 以降のバージョンから Citrix Director にも統合されています。Citrix Director を介した HDX Screen sharing の使用に関する詳細については、Citrix Director ドキュメントを参照してください。

シナリオ 2: エンドユーザーとの共同作業

エンジニアのチームが、仮想デスクトップ内のグラフィックを多用するアプリケーションで複雑な 3D モデルに取り組んでいます。彼らは一緒にデザインをレビューし、リアルタイムで調整を行う必要があります。

1 人のエンジニアがセッションを共有でき、チーム全体がモデルを表示し、変更を提案し、さらには交代でアプリケーションを制御して編集を行うこともできます。これにより、ファイルの書き出しやサードパーティの画面共有ツールを使用する必要がなくなります。

シナリオ 3: 従業員のオンボーディングとトレーニング

新入社員が独自の基幹業務アプリケーションの使用方法を学んでいます。トレーナーは、新入社員の仮想セッション内で直接アプリケーションの機能をデモンストレーションできます。

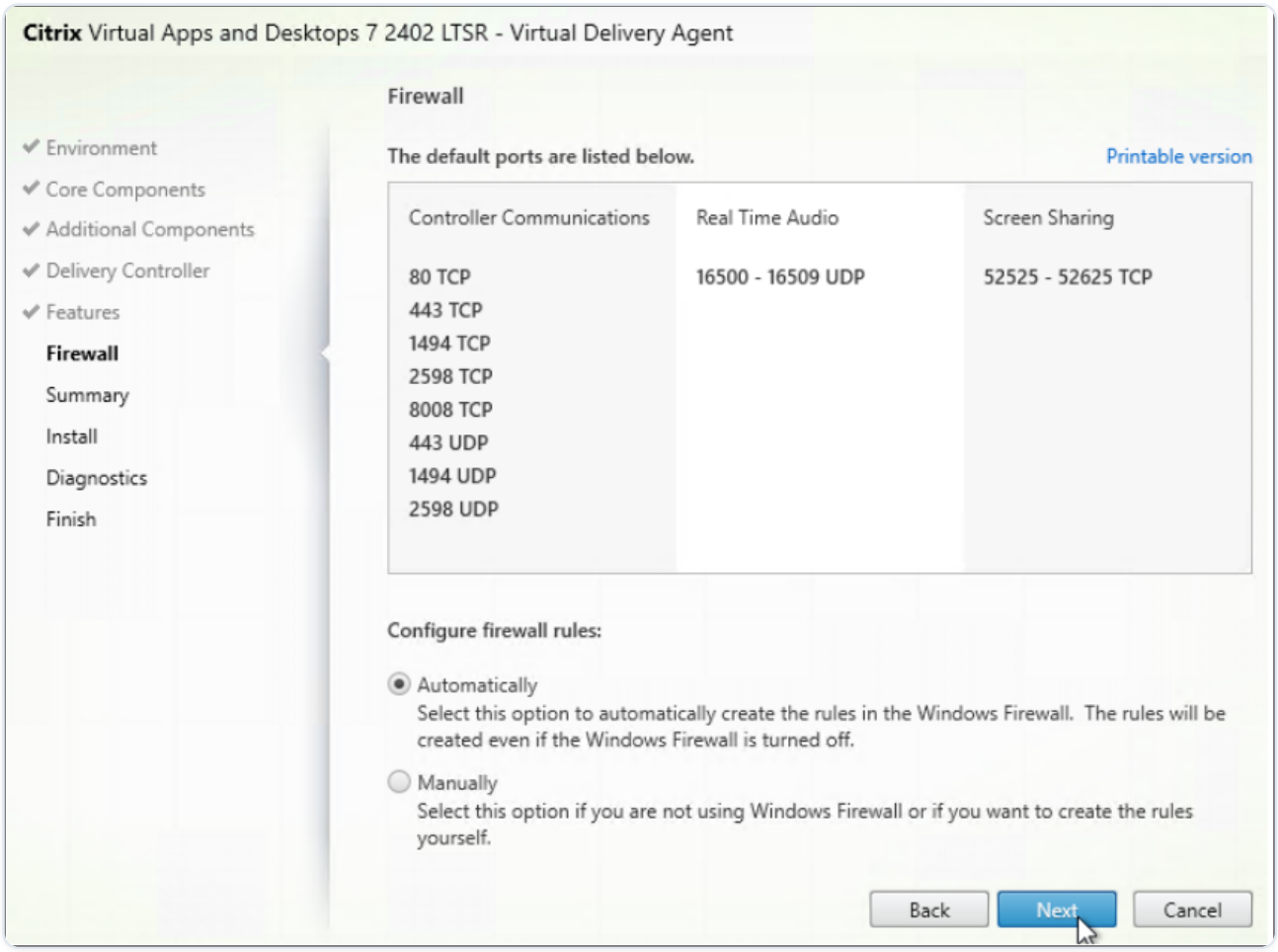
トレーナーは新入社員を段階的に指導できます。色付きの境界線インジケーター (赤または黄) は、セッションが共有されていることを明確に示し、学習環境の視覚的な合図となります。

システム要件

HDX Screen sharing はすべての VDA プラットフォームでサポートされていますが、特定のプラットフォームでは追加要件がある場合があります。詳細については以下を参照してください。

HDX Screen sharing は、デフォルトで 52525 から 52625 の範囲の TCP ポートを使用します。

VDA バージョン 2112 以降をインストールする際、VDA インストーラーは HDX Screen sharing のデフォルトのファイアウォールポートを自動的に開くように構成できます。



VDA のインストール中にこれが実行されなかった場合、またはカスタムポート範囲が構成されている場合は、VDA 上でこれらのポートを手動で開いてください。

注:

セッションをホストするVDAと、共有セッションに接続するマシンの間に、ネットワーク接続が必要です。

1つの画面共有セッションには最大64人のビューアーが接続できます。ポート範囲は、画面共有を開始できるマルチセッション環境の最大ユーザー数を制御します。ユーザーごとに1つのポートが必要です。

注:

セッションに接続されているすべてのモニターが共有されます。個別のモニターを選択することはできません。

AV1およびH.265ビデオコーデックと10ビットカラーモードはサポートされていません。アクティブな画面共有中は、セッションは自動的にH.264ビデオエンコーディングにフォールバックします。画面共有セッションが終了すると、AV1とH.265が再び利用可能になります。

ウィンドウズ VDA

- Windows: シングルセッションまたはマルチセッションOS VDA
- グラフィックステータスインジケーターを有効にする必要があります。

注:

デスクトップセッションのみ共有できます。

リナックス VDA

- 複数のLinux VDA間でセッション共有が行われる場合、キーボード入力の問題を回避するために、同じVDAバージョンにアップグレードすることをお勧めします。
- Citrix Workspace™アプリをスキャンコードモードを使用するように構成することをお勧めします。
- システムトレイアイコンを有効にする必要があります。

Linux VDAのHDX画面共有に関する詳細については、HDX画面共有に関するLinux VDAドキュメントを参照してください。

macOS VDA

- Qt 5、リビジョン5.15.13以降。

HDX画面共有に関するすべてのVDAで統一されたユーザーエクスペリエンスを合わせるには、Qtフレームワークをインストールする必要があります。最小互換バージョンはQt 5（リビジョン5.15.13以降）です。

VDA への Qt 5 のインストールは、たとえば homebrew を使用して、次の コマンドを実行することで実行できます。

```
brew install qt@5
```

MacOS VDA 向けの HDX 画面共有に関する詳細については、HDX 画面共有に関する MacOS VDA ドキュメントを参照してください。

構成

HDX 画面共有はデフォルトで無効になっており、この機能は Citrix® ポリシーを通じて有効化および構成できます。

これらのポリシーにより、HDX 画面共有の構成をきめ細かく制御できます。

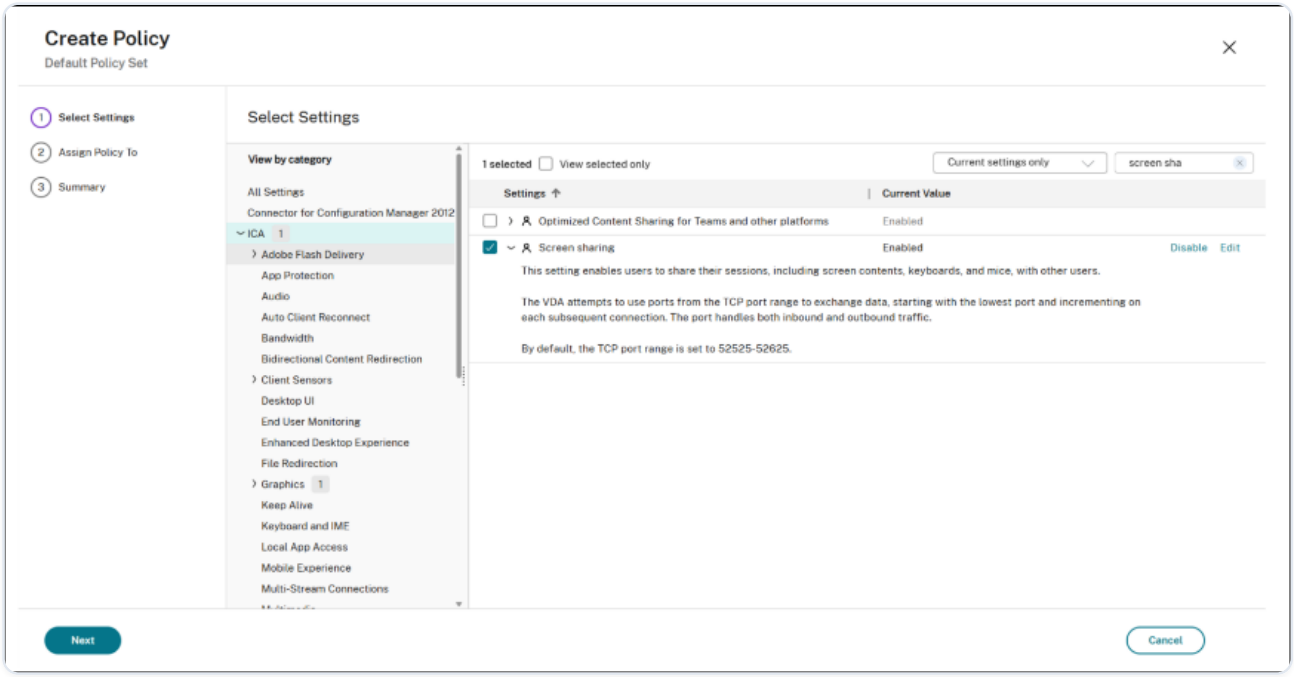
エンドユーザー向け HDX 画面共有の有効化

HDX 画面共有はデフォルトで無効になっています。エンドユーザーが HDX 画面共有を介して画面を共有できるようにするには、機能を次のように有効化および構成する必要があります。

- HDX 画面共有ポリシーを有効にする
- グラフィックステータスインジケーターを有効にする
- **オプション:** VDA ファイアウォールでカスタムポートを構成して開く

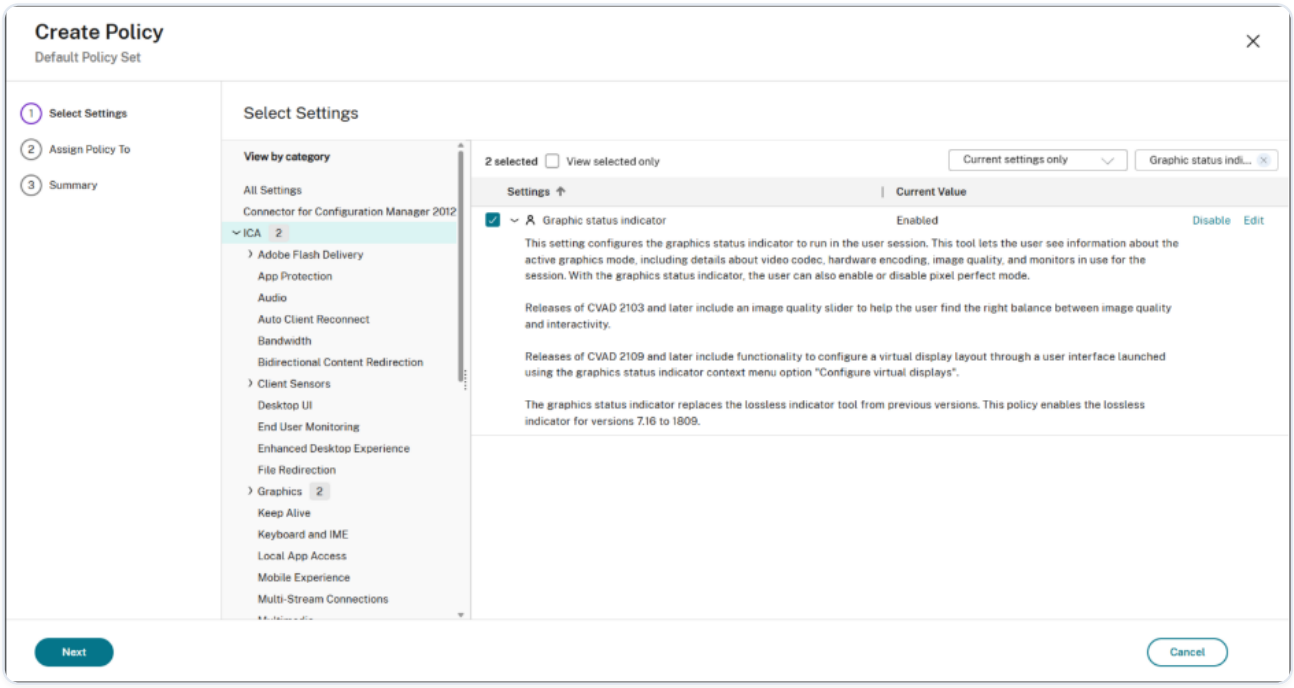
ステップ1: HDX画面共有を有効にする

HDX画面共有を有効にするには、**画面共有**ポリシーを参照し、ポリシーを**有効**に設定します。



ステップ2: グラフィックステータスインジケーターを有効にする

グラフィックステータスインジケーターを参照し、ポリシーを**有効**に設定します。



追加のHDX画面共有構成

デフォルトでは、HDX画面共有は通信に以下のTCPポートを使用します。

- TCP開始ポート: 52525
- TCP終了ポート: 52625

デフォルトのTCPポート範囲は、「HDX画面共有ポート」ポリシーで調整できます。

TCPポート範囲を調整するには、「HDX画面共有ポート」ポリシーを参照し、ポート範囲を目的のポート範囲に設定します。

ポート構成は、マルチセッションVDAで画面を共有する同時ユーザーの数を制限するために使用できます。

> **注:**
>
> ポート構成は、DirectorのHDX画面共有と重複しないようにしてください。

> HDX画面共有接続コードは、デフォルトでは期限切れにならず、画面共有セッション中にそのセッションに参加するために無期限に使用できます。

セキュリティを強化するために、接続コードが期限切れになるタイムアウト設定を構成できます。指定されたタイムアウト期間が経過すると、以前に生成された接続コードは無効になり、新しい

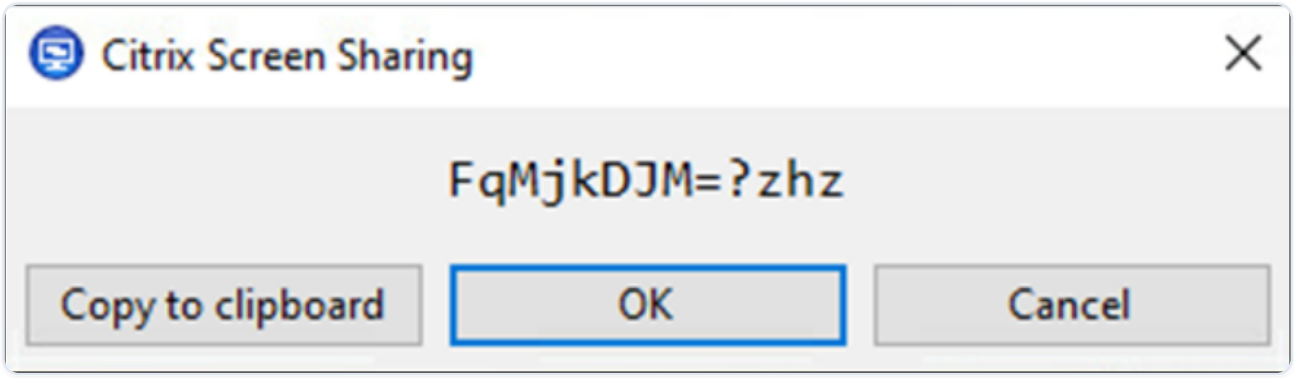
ユーザーはこのコードを使用して画面共有セッションに参加できなくなります。共有者は新しいセッション接続コードを再生成する必要があります。

さらに、画面共有セッションが開始され、設定されたタイムアウト期間内に視聴者が接続しなかった場合、画面共有は自動的に停止します。画面共有を再開するには、共有者はHDX画面共有を再起動し、接続コードを共有する必要があります。

HDX画面共有セッションのタイムアウトを構成するには、「HDX画面共有タイムアウト」ポリシーを参照し、希望のタイムアウト値を分単位で設定します。

接続コードの構成 (プレビュー)

デフォルトでは、HDX画面共有は40文字の接続コードを使用します。CVAD 2411以降、管理者はHDX画面共有用の新しい短い接続コードの使用を構成できます。新しい接続コードは13文字と短く、共有者が将来の視聴者に接続コードを口頭で伝えやすくするために、曖昧な文字は含まれていません。



現在、設定はVDAのレジストリ設定として提供されています。新しい、より短い接続コードは、古いVDAとの下位互換性を 提供しないことに注意してください。

> **注**:
>
> 新しい短い接続コードは、古いVDAとの下位互換性を提供しません。

前提条件

VDA - CVAD 2411以降

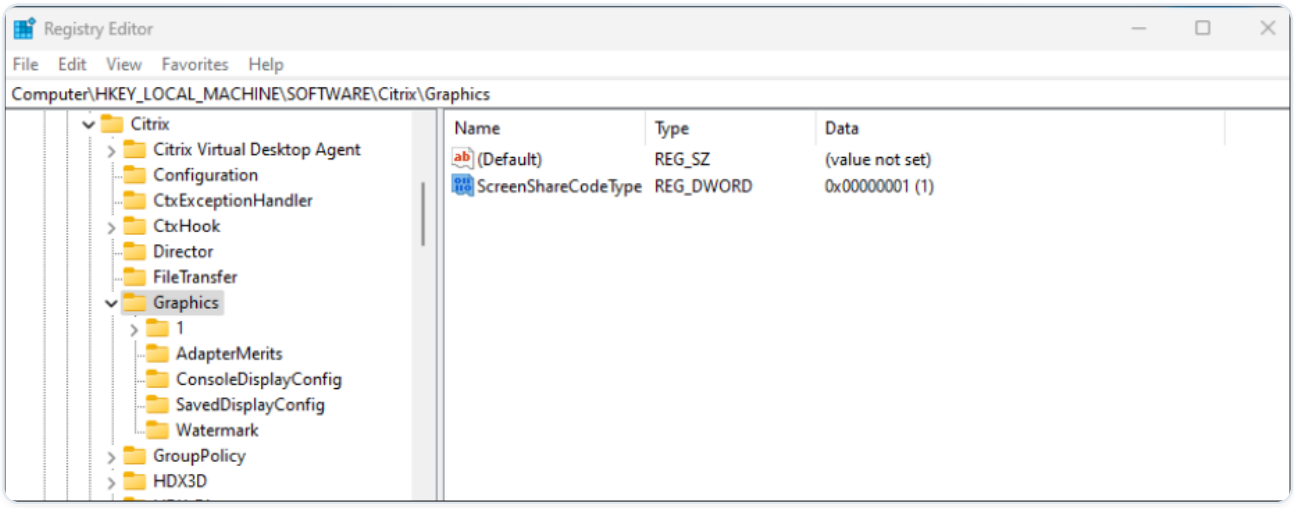
接続構成

新しい短い接続コードを有効にするには：

1. regedit.exeを使用してWindowsレジストリエディターを開きます。

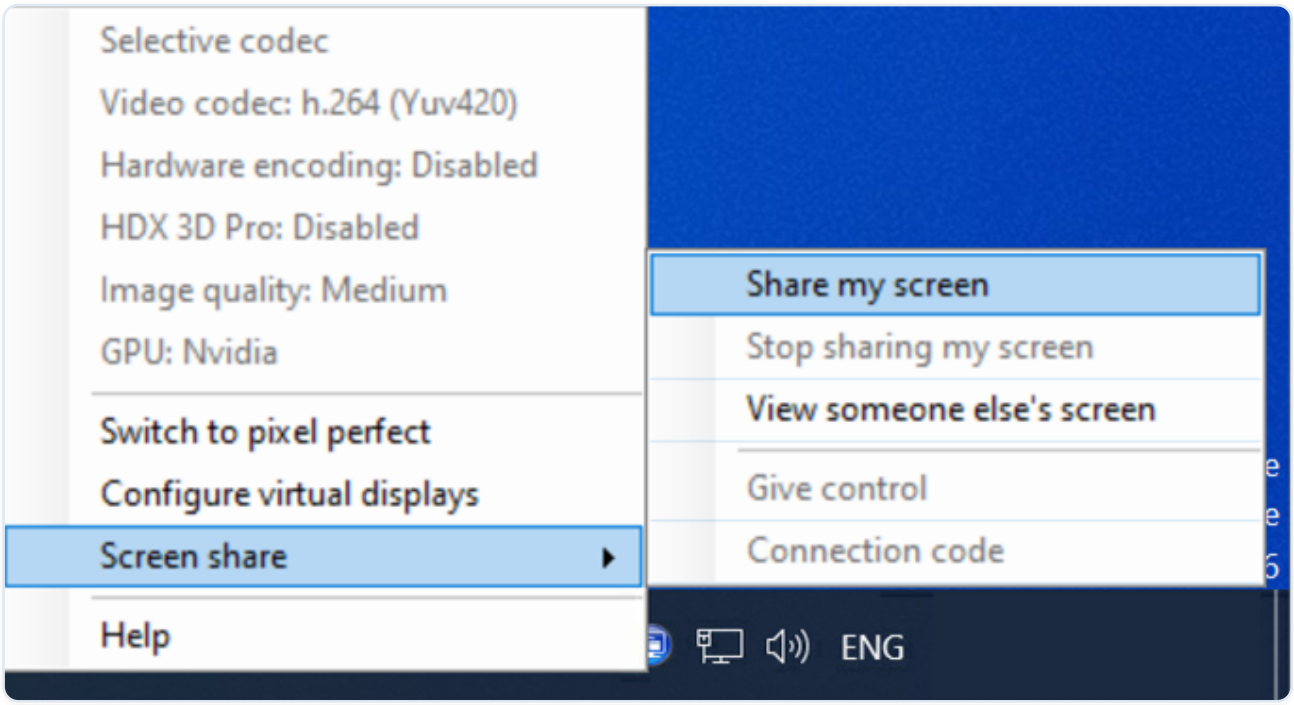
2. `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\ScreenShare` に移動します
3. **DWORD** 値 **CodeType** を作成し、その値を 1 に設定します。

このキーは、使用する接続コードを制御します。0 は古い長い接続コード、1 は新しい短いコード用です。



画面共有セッションの開始

共有者としてセッションを共有するには、Windowsの通知領域にあるHDXグラフィックステータスインジケーターアイコンを探します。それを右クリックしてメニューを表示し、「画面共有」>「自分の画面を共有」を選択します。



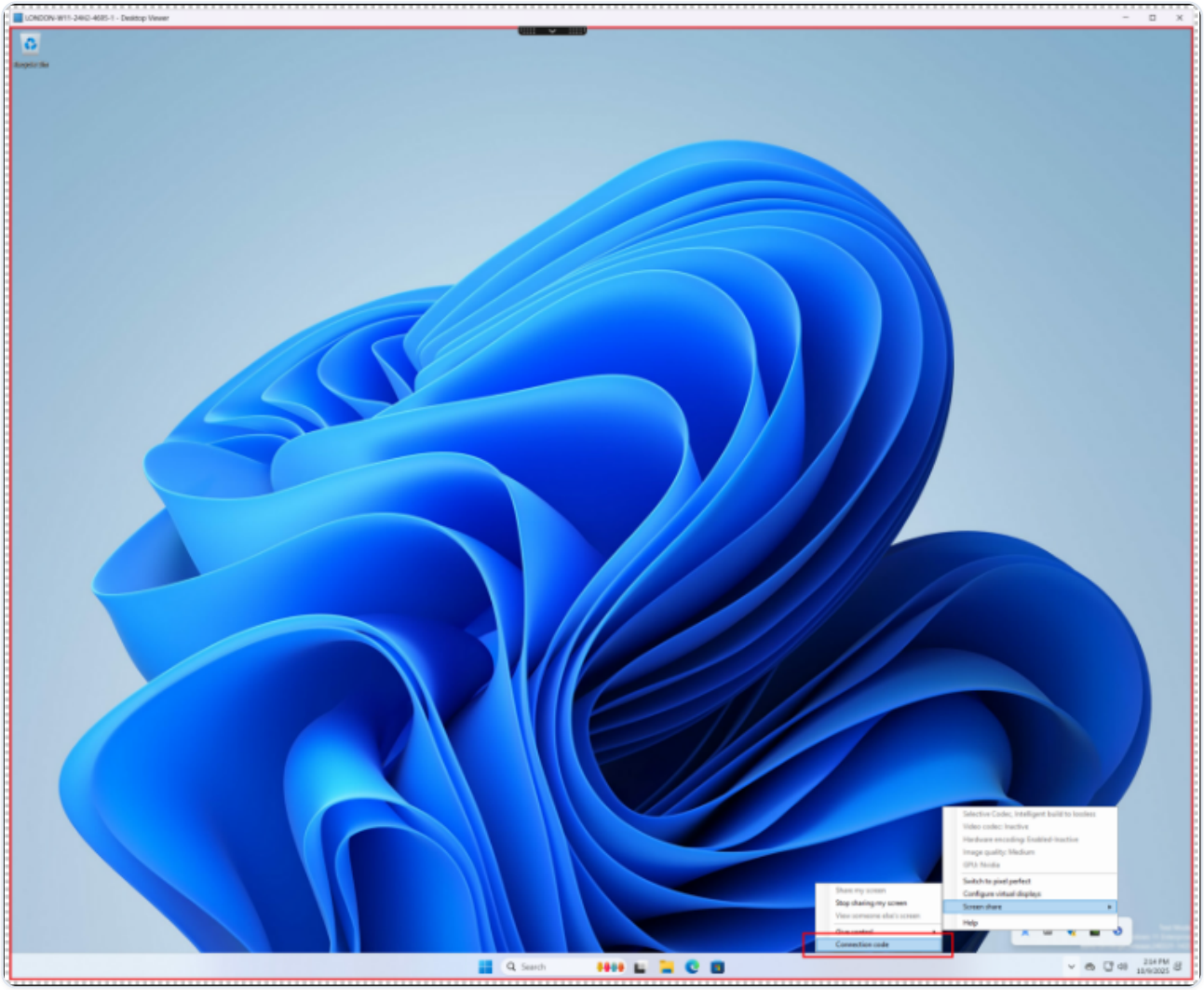
画面共有が開始されると、画面共有セッションに参加するために使用できる接続コードを含むダイアログボックスが表示されます。このコードは、1 人以上の視聴者が画面共有セッションに接続するために使用できます。

「クリップボードにコピー」をクリックするか、ダイアログボックスに表示されている接続コードを手動で選択してコピーします。

接続コードは、電子メールアプリケーションや Microsoft Teams などの任意のアプリケーションに貼り付けて、他のユーザーに配布できます。

接続コードがコピーされたら、「OK」をクリックするか、右上隅の x をクリックしてダイアログボックスを閉じることができます。

セッションが共有されている間はいつでも、「画面共有」>「接続コード」メニューオプションから現在アクティブな接続コードを取得できます。



注:

接続コードを共有する相手には注意してください。接続コードを共有したすべてのユーザーは、アクティブな画面共有セッションに接続できる可能性があります。

> 画面共有セッションが開始されると、Citrixセッションの周囲に黄色の枠が表示され、HDX画面共有がアクティブであるが、まだ視聴者が参加していないことを示します。

(/en-us/citrix-virtual-apps-desktops/2511/media/screen-share-7.png)

視聴者が画面共有セッションに接続すると、枠の色が赤に変わり、画面共有セッションがアクティブで視聴者が接続されていることを示します。

(/en-us/citrix-virtual-apps-desktops/2511/media/screen-share-8.png)

Citrixセッションで複数の画面がアクティブになっている場合、すべての画面が画面共有を介して共有され、視聴者はセッション内の接続されているすべての画面を見ることができることに注意してください。

現在、セッション内で単一のモニターまたは接続されているモニターのサブセットのみを共有する機能はサポートされていません。

デフォルトでは、最大100人の視聴者が単一の画面共有セッションに接続できますが、この制限はCitrix管理者が制限する場合があります。

新しい接続コードを再生成する

接続コードがアクティブである限り、新しいユーザーは接続コードを使用して画面共有セッションに参加できます。コードの有効期限が切れている場合、既存の視聴者は接続されたままになりますが、新しいユーザーは画面共有セッションに接続できなくなります。新しいユーザーがセッションに接続できるようにするには、新しい接続コードを再生成する必要があります。

新しい接続コードは、セッションが共有されている間であればいつでも、「画面共有」>「接続コード」メニューオプションから取得できます。

(/en-us/citrix-virtual-apps-desktops/2511/media/screen-share-9.png)

画面共有の停止

画面共有を停止するには、Windows通知領域にあるHDXグラフィックステータスインジケーターアイコンを探します。それを右クリックしてメニューを表示し、「画面共有」>「画面の共有を停止」を選択します。画面共有はすぐに停止し、現在のすべての視聴者はセッションから切断されます。画面共有が停止したことを示す赤い枠は消えます。

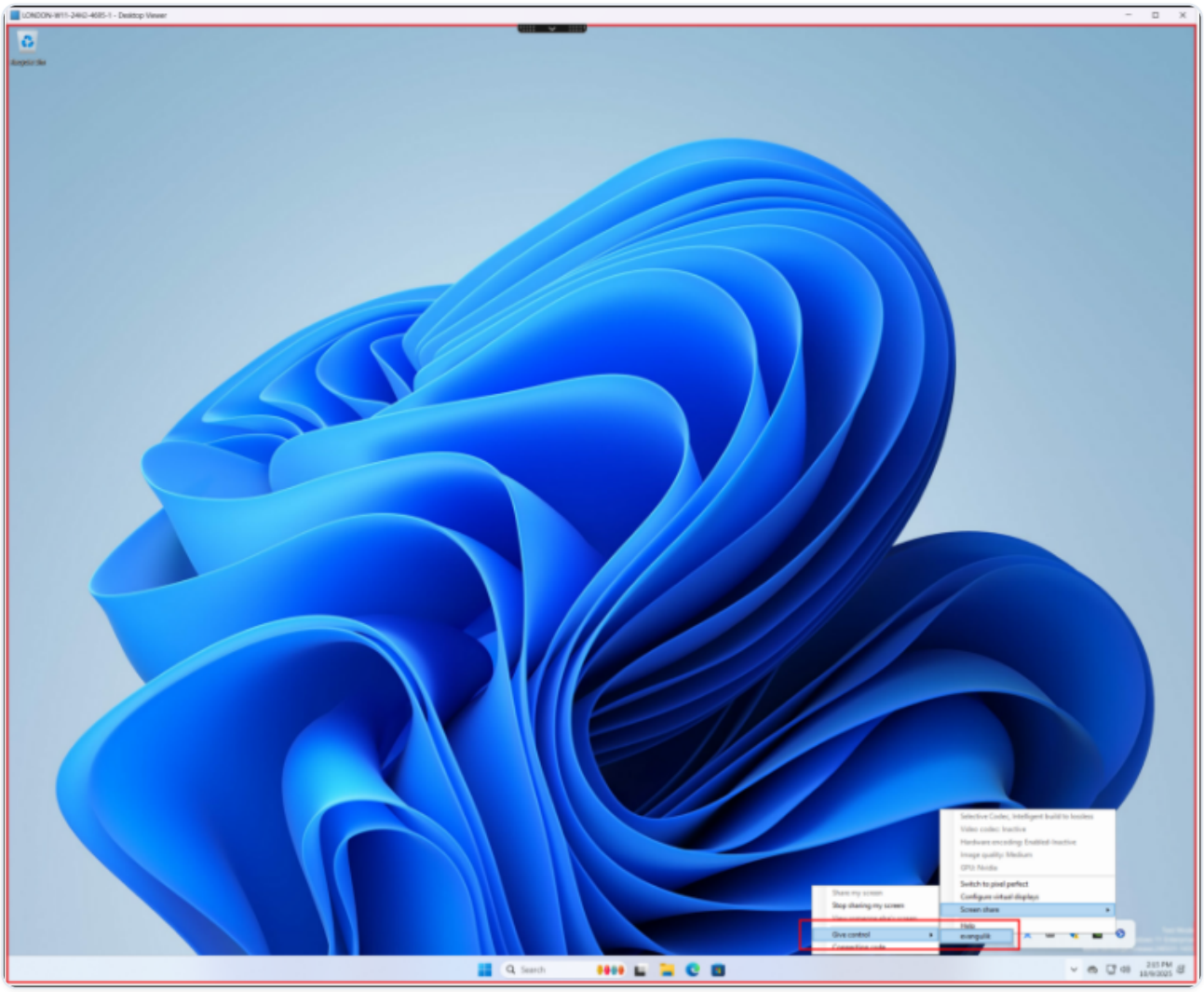
(/en-us/citrix-virtual-apps-desktops/2511/media/screen-share-10.png)

マウスとキーボードの制御を許可する

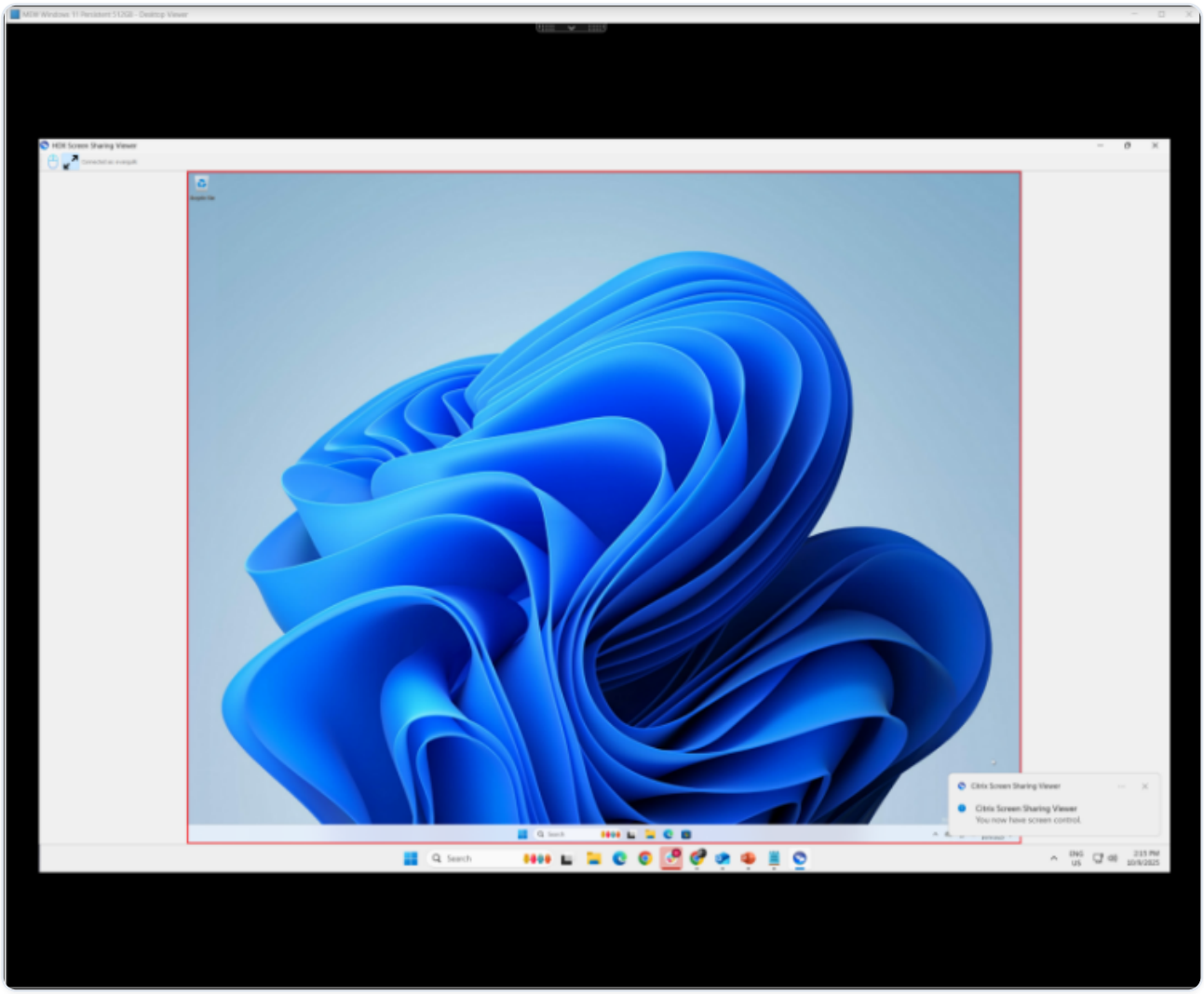
画面共有セッション中の任意の時点で、共有者として、マウスとキーボードの制御を特定のビューアーに引き渡すことができます。

引き渡されると、そのビューアーは Citrix セッションであなたのマウスとキーボードの完全な制御をあなたと共有します。

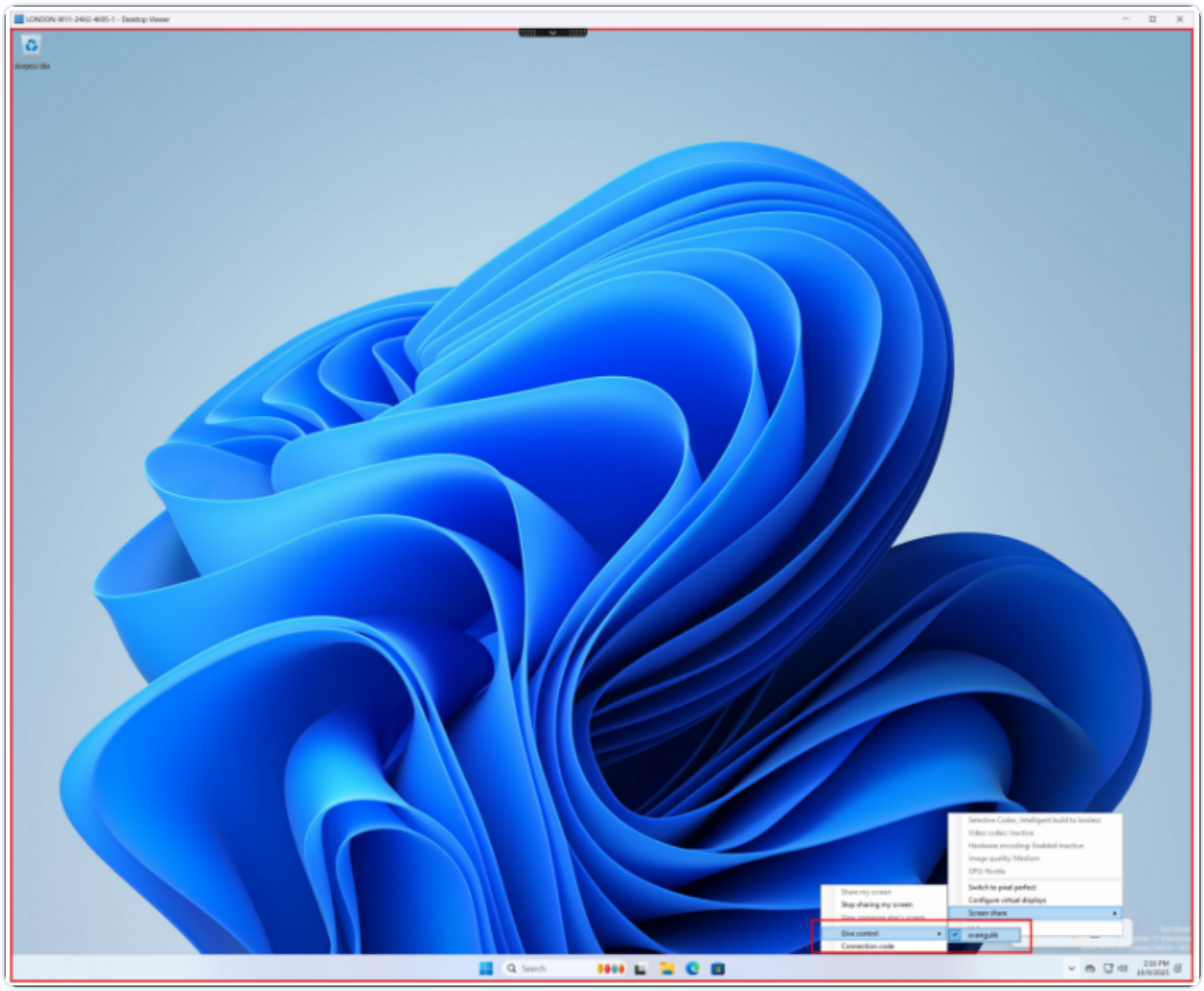
マウスとキーボードの制御を共有するには、Windows通知領域にあるグラフィックステータスインジケーターアイコンを開きます。それを右クリックしてメニューを表示し、「Screen share」>「Give control」を選択し、アクティブなビューアーのいずれかを選択して制御を引き渡します。



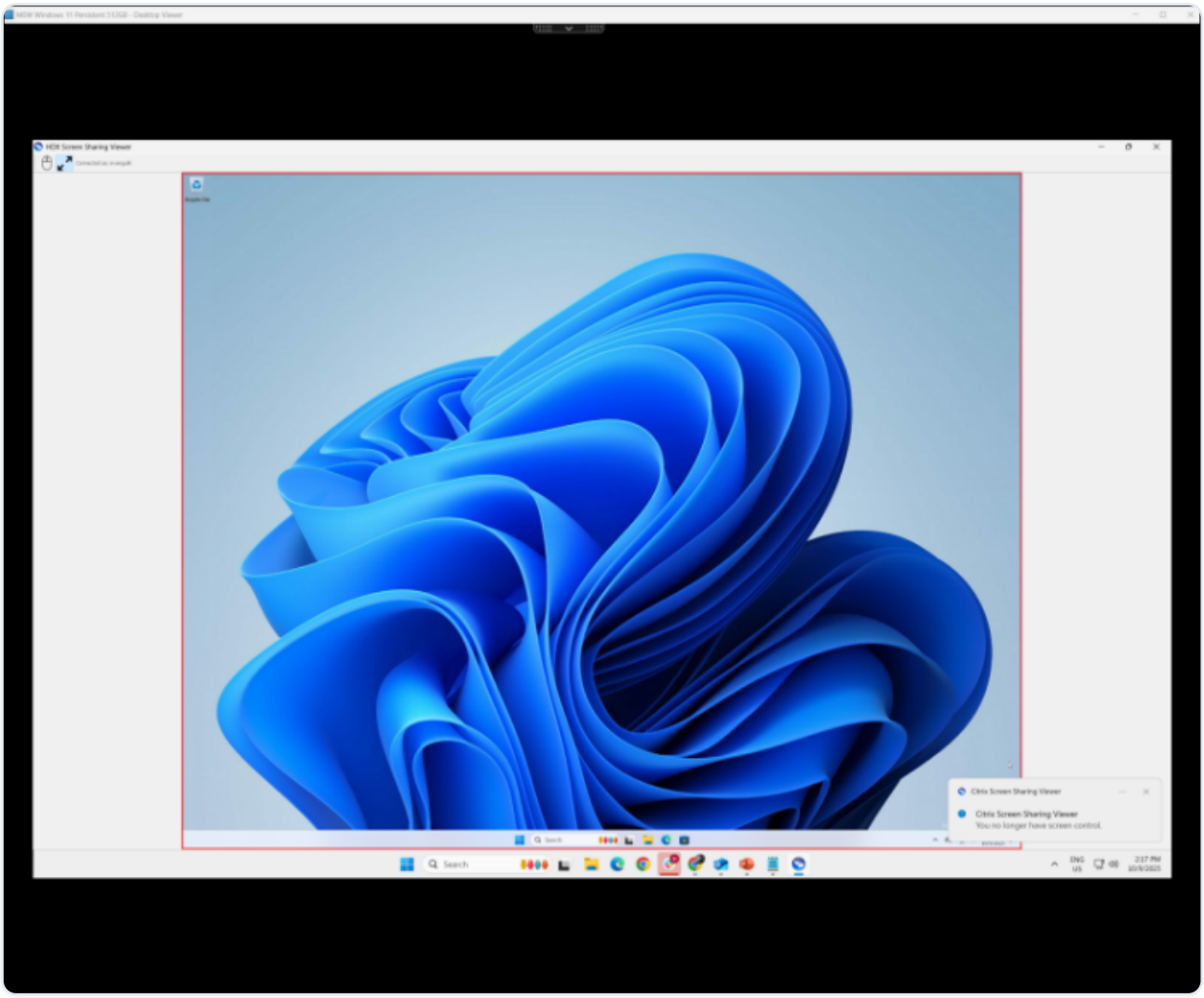
選択されたビューアーには、マウスとキーボードの制御権があることを示す通知が届きます。



マウスとキーボードの共有を停止し、制御を取り戻すには、Windows の通知領域にあるグラフィックステータスインジケーターアイコンを開きます。それを右クリックしてメニューを表示し、「画面共有」>「制御を付与」を選択し、アクティブなビューアーの選択を解除します。

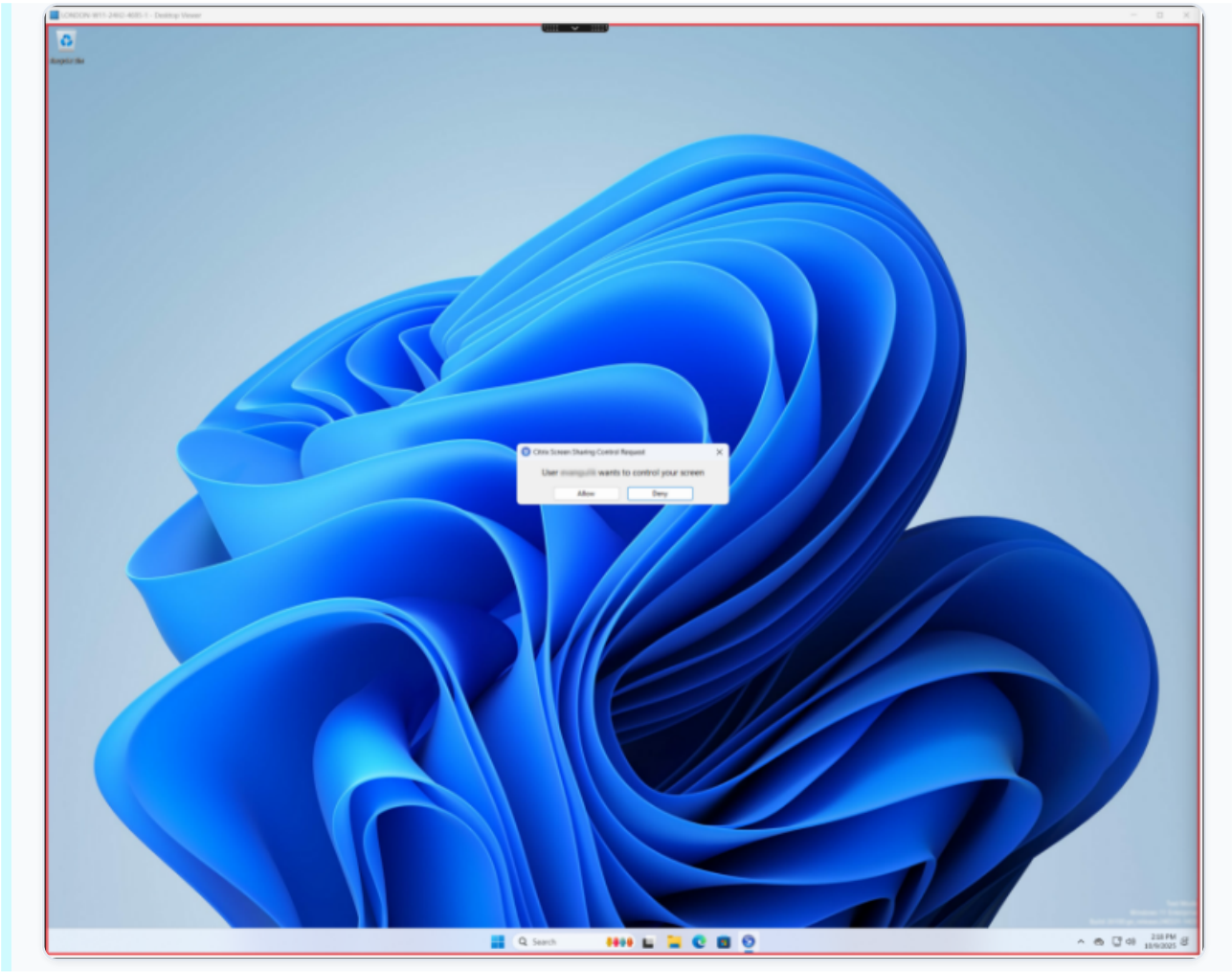


ビューアーには、マウスとキーボードの制御を失ったことが通知されます。



注:

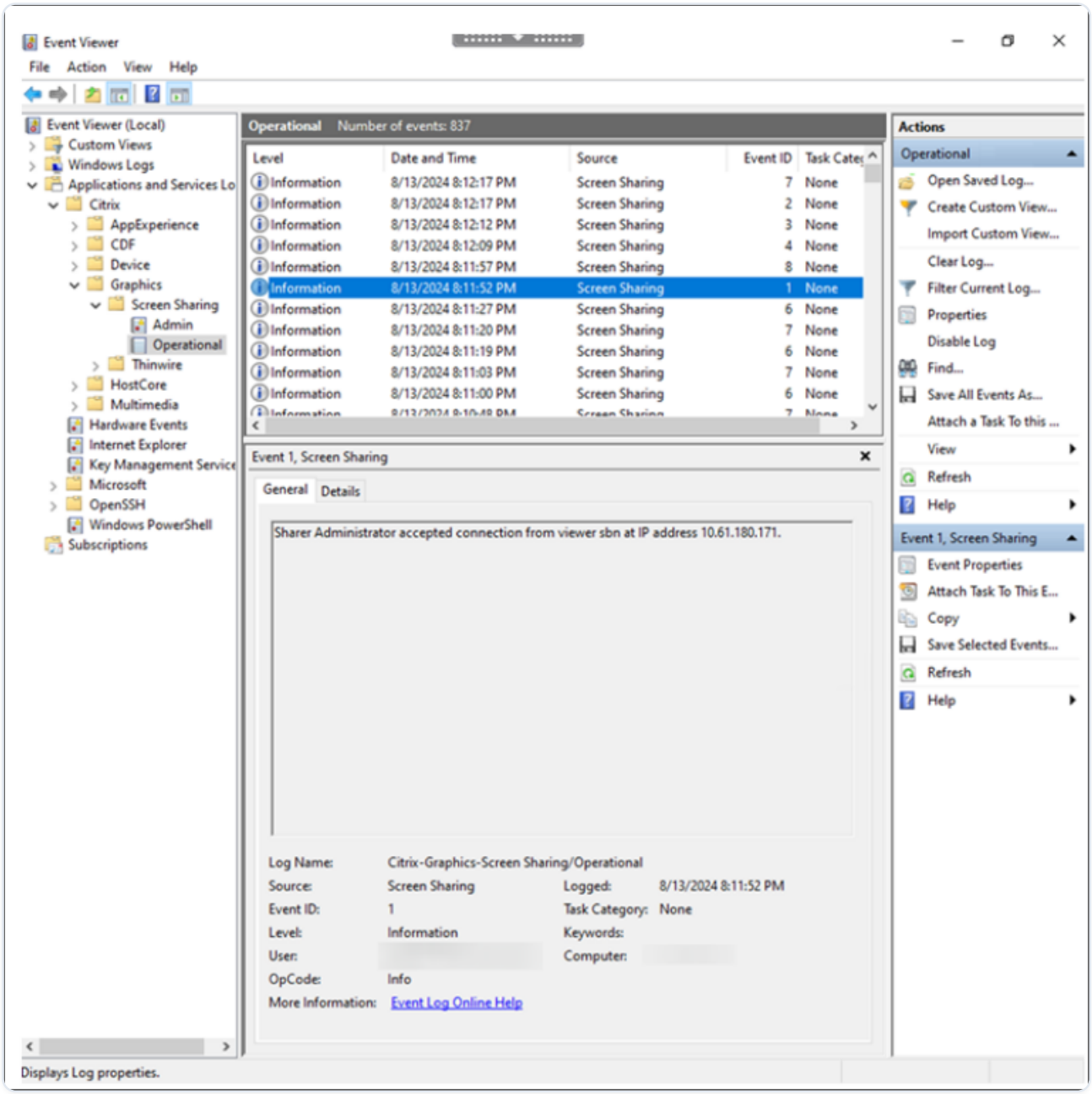
マウスとキーボードの制御は、一度に1人のビューアーとのみ共有できます。ビューアーはマウスとキーボードの制御を要求することもできます。この場合、要求が通知され、その要求を許可するか拒否するかを選択できます。



イベントログ

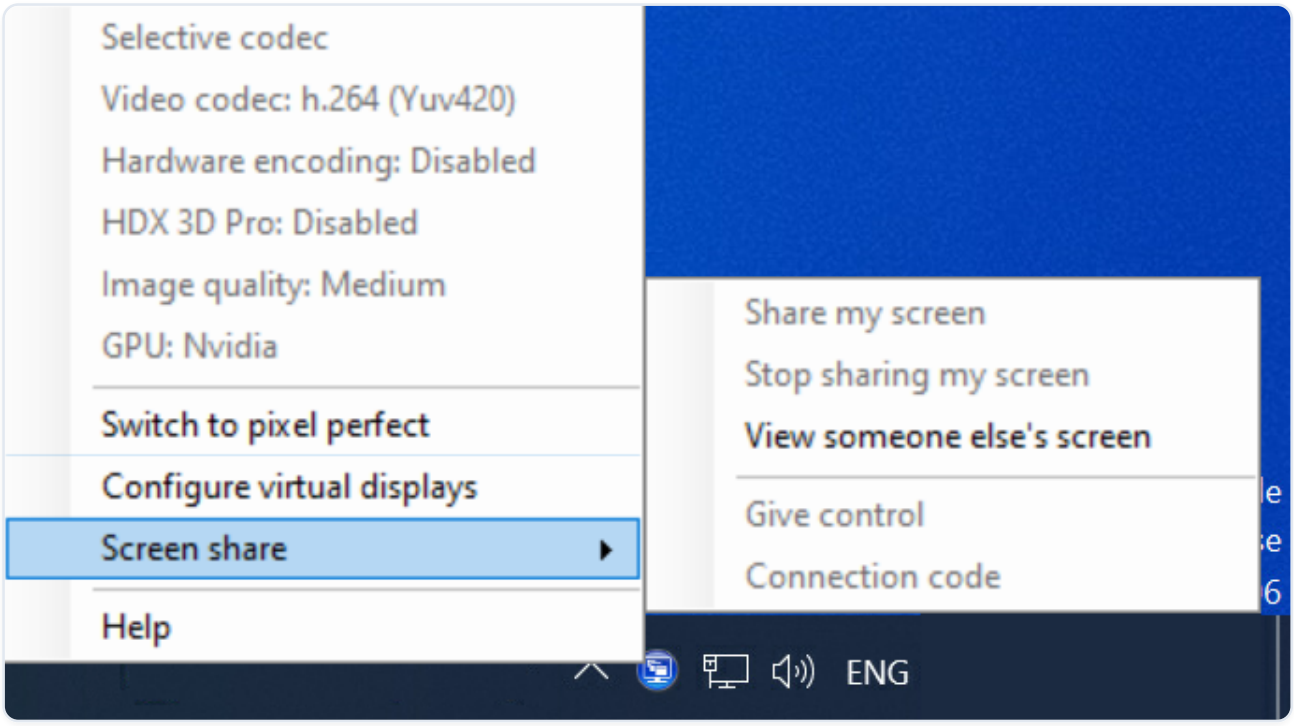
セキュリティおよび監査の目的で、共有者VDAでの画面共有イベントが収集およびログに記録されるようになりました。これにより、管理者は共有者VDAでの画面共有アクティビティを追跡できます。画面共有 セッション中に、以下の情報とイベントがログに記録されます。

- 共有の開始/停止 – 画面共有セッションの開始と停止を示すイベント
- 接続要求 – 接続を要求したビューアのIPとユーザー名、使用された接続コード、および接続決定（認証失敗または共有者の決定による接続許可/拒否）
- 画面制御要求 – 画面制御を要求したビューアのIPとユーザー名、および決定（許可/拒否）
- ビューアのアクション – 画面共有セッションから切断した、または共有者の画面の制御を解除したビューアのIPとユーザー名。



画面共有セッションの表示

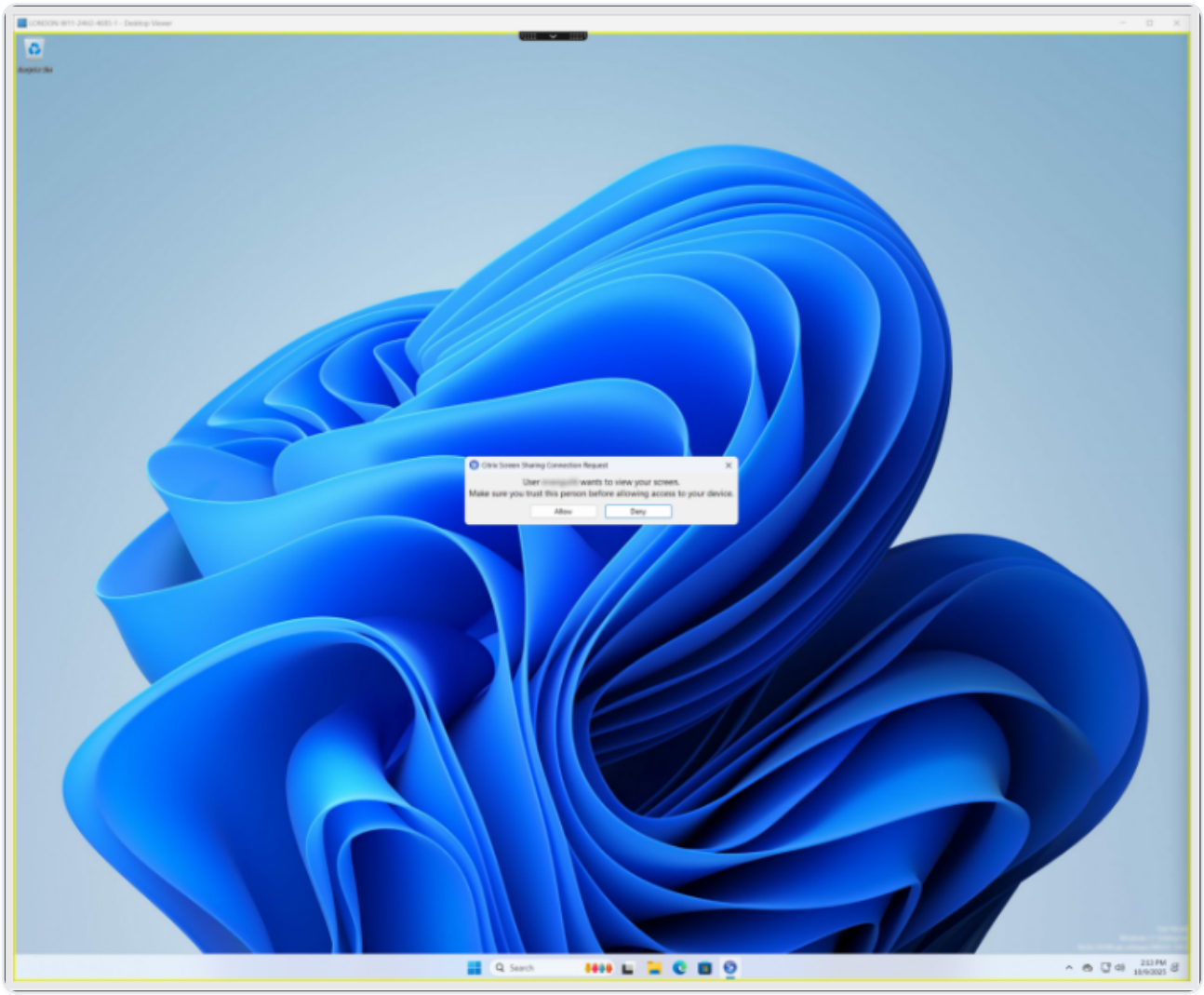
他のユーザーのセッションに接続するには、Windows通知領域にあるHDXグラフィックステータスインジケーターアイコンを探します。右クリックしてメニューを表示し、「画面共有」>「他のユーザーの画面を表示」を選択します。



接続コードの入力を求められます。HDX画面共有者がこのコードを提供しています。セッションを共有しているユーザーから提供されたセッションの接続文字列をテキストボックスに入力または貼り付けます。

「接続」をクリックすると、接続コードが検証され、検証が成功すると、共有者のセッションへの画面共有接続が確立され、画面共有ビューアーが自動的に開き、共有者の画面（または複数の画面）が表示されます。

セッションに接続すると、共有者の画面共有セッションへの参加が共有者に通知されます。



ディスプレイのスケーリングの調整

共有者が自分のモニター解像度よりも高い解像度を使用している場合、またはセッション中に複数のモニターを使用している場合、画面共有プレーヤーは自動的に解像度を調整します。スケーリングを無効にして共有者のモニターのネイティブ解像度を表示するには、画面共有プレーヤーの左上隅にある対角線矢印を選択します。

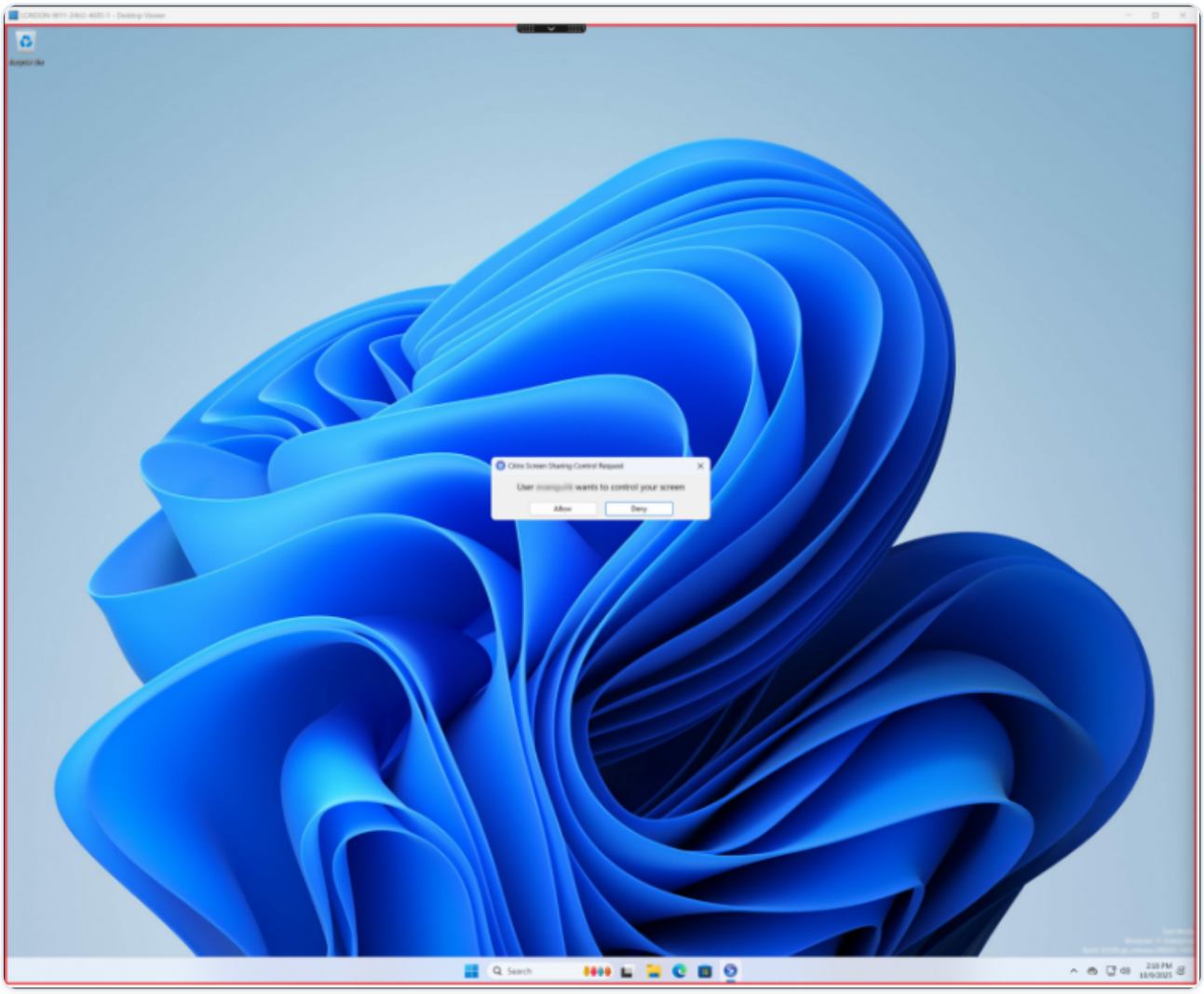
画面共有セッションから切断する

画面共有セッションから切断するには、いつでも画面共有プレーヤーを閉じます。再接続するには、接続コードが期限切れになっていない場合、同じコードを使用して共有者との画面共有セッションに再参加できます。接続コードが期限切れになっている場合、共有者は新しいコードを再生成する必要があります。接続コードの有効期限は、管理者が設定できる接続タイムアウト画面共有ポリシーによって制御されます。

マウスとキーボードの制御を要求する

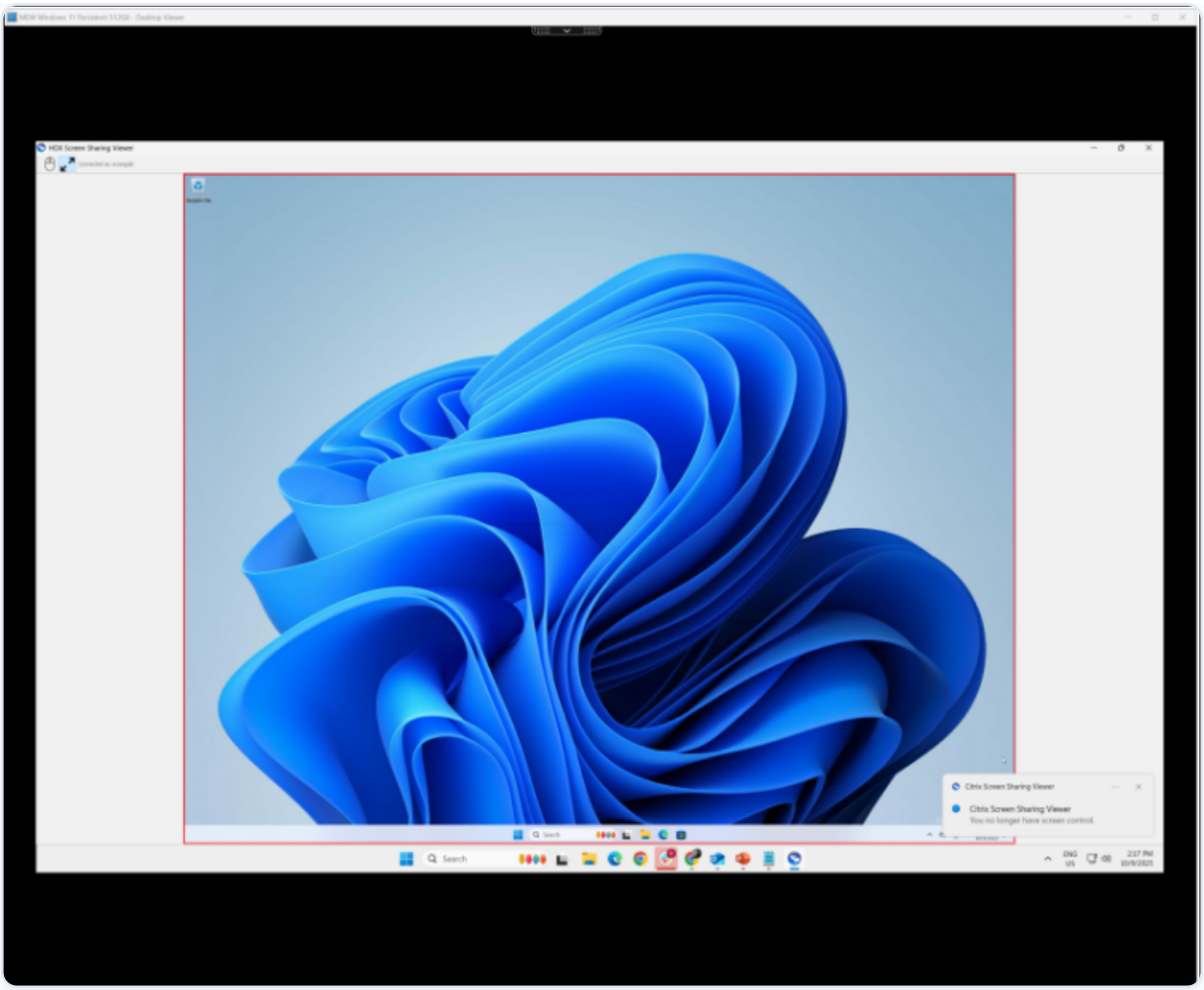
既定では、共有者は画面共有セッションにおいてマウスとキーボードを完全に制御します。閲覧者は、共有者に対してマウスとキーボードの制御を要求できます。

マウスとキーボードの制御を要求するには、画面共有ビューアーの左上にある「マウスアイコン」をクリックします。共有者にはあなたのリクエストが通知され、それを許可または拒否できます。共有者がマウスとキーボードの制御のリクエストを承認すると、閲覧者であるあなたと画面共有の共有者の両方がセッション内でマウスとキーボードの制御を共有します。



注:

共有者はいつでもマウスとキーボードの排他的な制御を取り戻すことができます。



仮想ディスプレイレイアウト

仮想ディスプレイ構成を使用すると、ライブセッション内のVDAで、セッションモニターごとに仮想ディスプレイレイアウトを定義できます。この機能により、各セッションモニターを個別に複数の仮想モニターに分割できます。

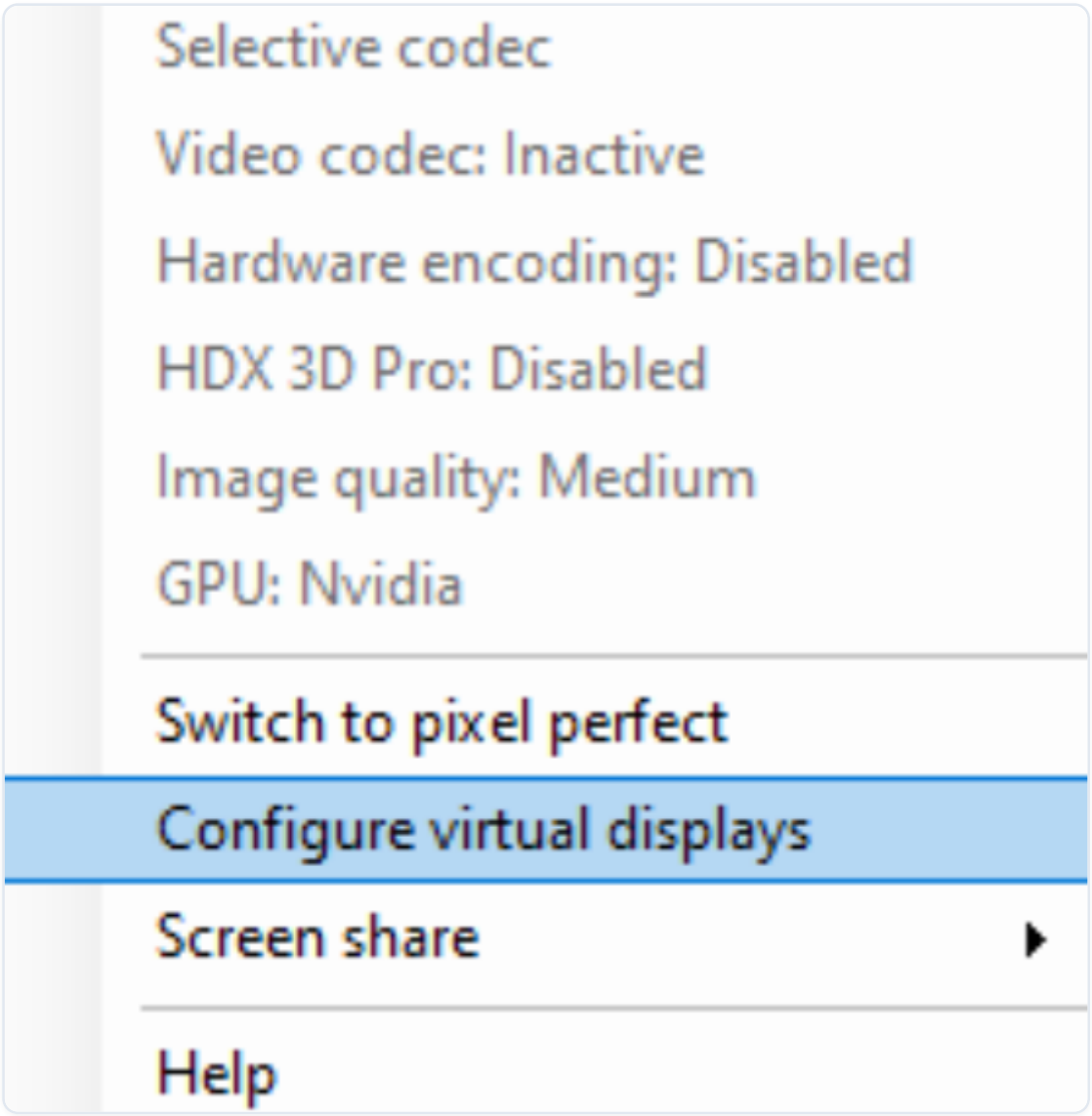
仮想ディスプレイ構成UIを使用すると、ライブセッション内のVDAで、セッションモニターごとに仮想ディスプレイレイアウトを定義できます。この機能により、各セッションモニターを個別に複数の仮想モニターに分割できます。リモートデスクトップでは、合計8つの仮想モニターに分割できます。また、ディスプレイのセッションプライマリモニターとDPI設定を更新することもできます。

システム要件

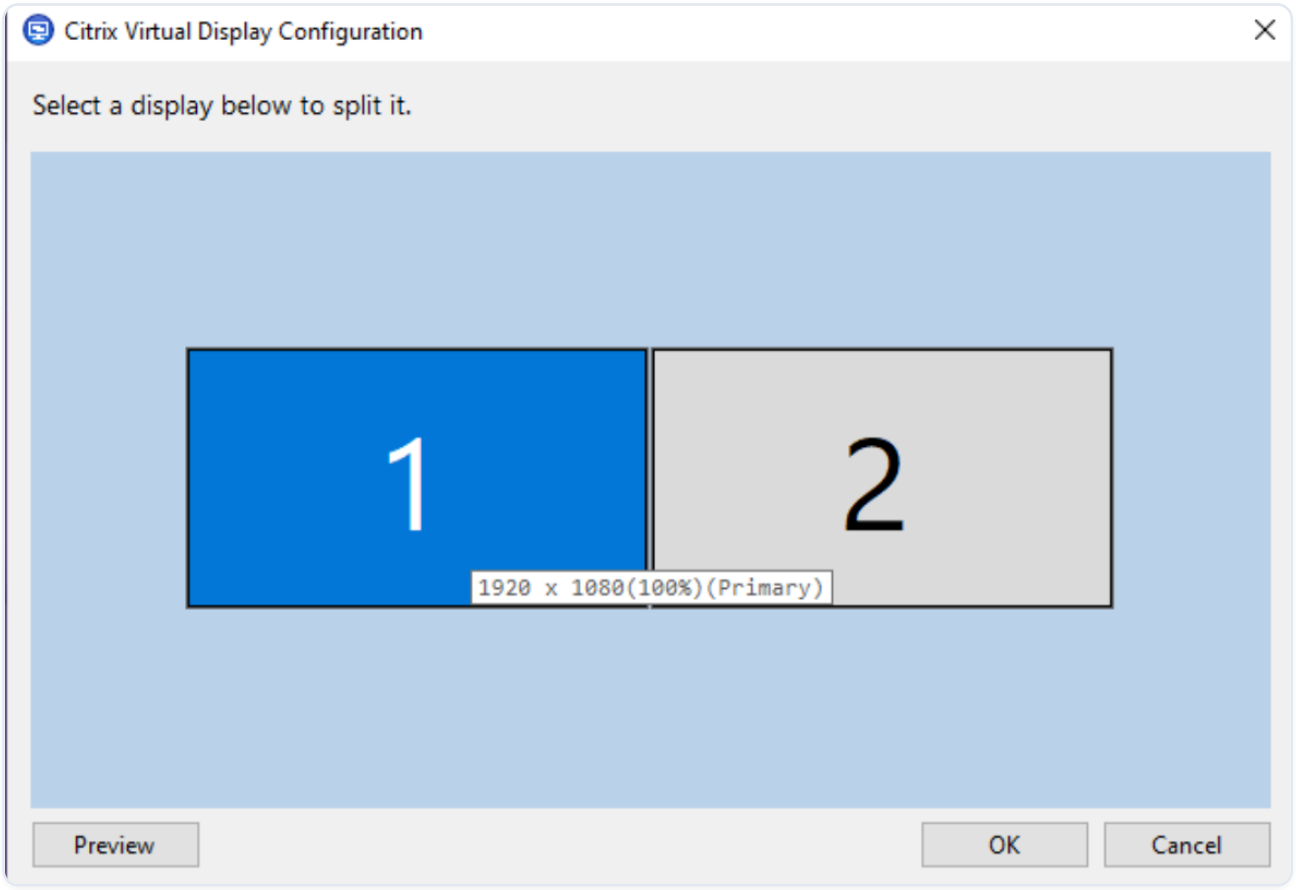
- Windows: シングルセッションまたはマルチセッションOS VDA
- グラフィックステータスインジケーターポリシーを有効にする必要があります。
- デスクトップセッションのみ構成できます。

構成

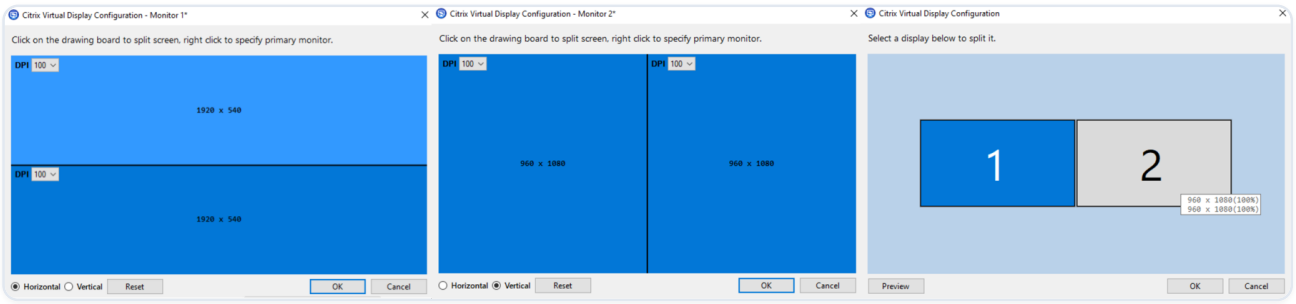
仮想ディスプレイレイアウトを構成するには、グラフィックステータスインジケーターアイコンを右クリックし、オプションを選択します。仮想ディスプレイ構成UIが起動します。



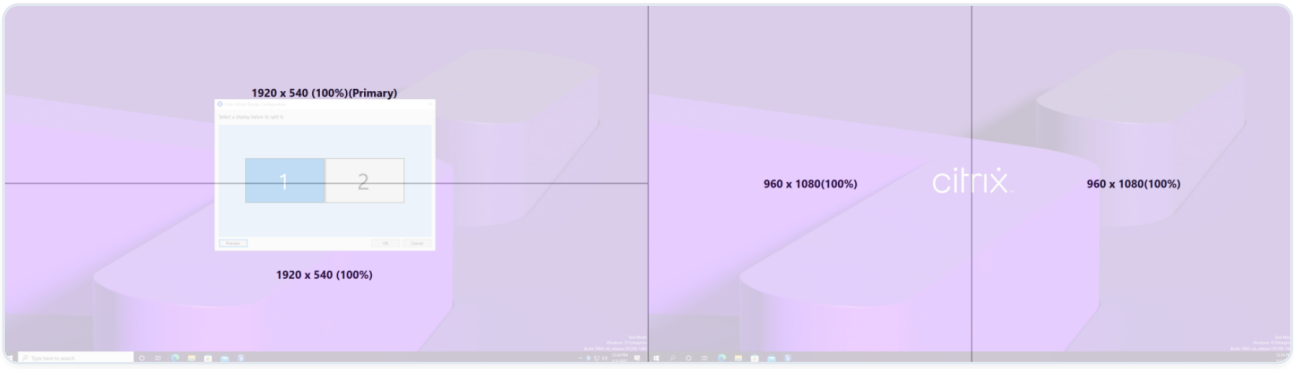
UIには現在のセッションディスプレイレイアウトが表示され、青色はセッションのプライマリモニターを示します。ディスプレイにカーソルを合わせると、ツールチップが表示されます。このツールチップには、特定のセッションモニターに定義されている現在の仮想ディスプレイレイアウトに関する情報が表示されます。



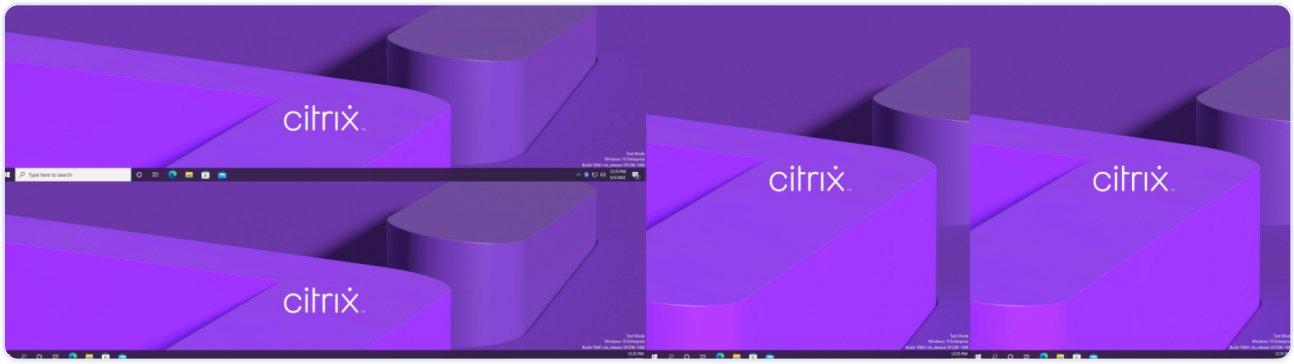
ディスプレイを選択すると、対話型UIに移行し、選択したセッションモニターの仮想ディスプレイを構成できます。水平線または垂直線を描画して、画面を仮想モニターに分割できます。画面は、セッションモニターの解像度の指定された割合に基づいて分割されます。仮想ディスプレイを右クリックしてプライマリモニターとしてマークし、DPIドロップダウンリストを使用して仮想ディスプレイの優先スケーリング係数を設定します。仮想ディスプレイレイアウトを定義したら、 をクリックしてレイアウトを一時的に保存するか、 をクリックして変更を破棄します。 を使用して、構成を元に戻し、セッションモニターの元のレイアウトを復元できます。



現在構成されている仮想ディスプレイレイアウトをプレビューするには、 ボタンをクリックします。セッション内の仮想ディスプレイの予想される位置と解像度を強調表示するウィンドウが表示されます。



OKをクリックして、仮想ディスプレイレイアウトをすぐに適用して保存します。**キャンセル**をクリックしてUIを閉じ、すべての変更を破棄します。



その他の考慮事項

- 必要な最小仮想ディスプレイ解像度は640 x 480です。
- UIで定義された仮想ディスプレイDPIは、指定されたディスプレイ解像度に対するOSのスケーリングサポートに依存します。
- この機能をCitrix Workspace™アプリの既存の仮想ディスプレイ機能と同時に使用しないでください。
- プレビュー機能はServer 2016ではサポートされていません。

セッションベースのウォーターマーク

テキストベースのセッションウォーターマークは、データ盗難を抑止し、追跡を可能にするのに役立ちます。この追跡可能な情報は、写真やスクリーンキャプチャを使用してデータを盗む者への抑止力として、セッションデスクトップに表示されます。テキストのレイヤーであるウォーターマークを指定できます。

ウォーターマークは、元のドキュメントの内容を変更することなく、セッション画面全体に表示できます。テキストベースのセッションウォーターマークには、VDAのサポートが必要です。

> **重要:**

> テキストベースのセッションウォーターマークは、セキュリティ機能ではありません。このソリューションはデータ盗難を完全に防ぐものではありませんが、ある程度の抑止力と追跡可能性を提供します。この機能を使用しても完全な情報追跡可能性を保証するものではありませんが、必要に応じて他のセキュリティソリューションと組み合わせて使用することをお勧めします。

> セッションウォーターマークはテキストであり、ユーザーに配信されるセッションに適用されます。セッションウォーターマークには、データ盗難を追跡するための情報が含まれています。最も重要なデータは、スクリーンイメージが取得された現在のセッションのログオンユーザーのIDです。データ漏洩をより効果的に追跡するために、サーバーまたはクライアントのインターネットプロトコルアドレスや接続時間などの他の情報を含めます。

ユーザーエクスペリエンスを調整するには、セッションウォーターマークポリシー設定 を使用して、画面上の配置とウォーターマークの外観を構成します。

要件:

仮想デリバリーエージェント:

マルチセッションOS 7.17 シングルセッションOS 7.17

制限事項:

- ローカルアプリアクセス、Windowsメディアリダイレクト、MediaStream、ブラウザコンテンツリダイレクト、HTML5ビデオリダイレクトが使用されているセッションでは、セッションウォーターマークはサポートされません。セッションウォーターマークを使用するには、これらの機能が無効になっていることを確認してください。
- セッションが全画面ハードウェアアクセラレーションモード（全画面H.264またはH.265エンコーディング）で実行されている場合、セッションウォーターマークはサポートされず、表示されません。
- これらのHDX™ポリシーを設定すると、ウォーターマーク設定は有効にならず、セッション表示にウォーターマークは表示されません。

ビデオコーデックにハードウェアエンコーディングを使用 を **有効** **圧縮にビデオコーデックを使用** を **画面全体**

- これらのHDXポリシーを設定すると、動作は未定義となり、ウォーターマークが表示されない場合があります。

ビデオコーデックにハードウェアエンコーディングを使用 を **有効** **圧縮にビデオコーデックを使用** を **優先する場合にビデオコーデックを使用**

ウォーターマークが表示されるようにするには、**ビデオコーデックにハードウェアエンコーディングを使用する** を **無効** に設定するか、または **圧縮にビデオコーデックを使用する** を **アクティブに変更される領域の場合** または **ビデオコーデックを使用しない** に設定します。

- セッションウォーターマークは、Thinwireグラフィックモードのみをサポートします。
- セッションレコーディングを使用している場合、記録されたセッションにはウォーターマークは含まれません。
- Windowsリモートアシスタンスを使用している場合、ウォーターマークは表示されません。
- ユーザーが画面をキャプチャするために **Print Screen** キーを押した場合、VDA側でキャプチャされた画面にはウォーターマークは含まれません。キャプチャされた画像がコピーされるのを防ぐための対策を講じることをお勧めします。

シンワイヤー

Thinwire は、Citrix HDX の中核となるディスプレイリモートテクノロジーであり、Citrix Virtual Apps and Desktops™ 環境でスムーズでインタラクティブな視覚体験を提供します。

Thinwire は、画面コンテンツを分析し、変更を特定し、画面上のグラフィックデータをエンコードして、VDA からユーザーのエンドポイントデバイスへのネットワーク経由での効率的な送信を可能にします。これにより、情報が可能な限り効率的に送信され、特に困難なネットワーク条件下で帯域幅の消費を最小限に抑え、パフォーマンスを最適化します。

Thinwire を搭載した HDX™ Graphics は、高性能で適応性のある効率的なリモートデスクトップおよびアプリケーションエクスペリエンスを提供するように設計された Citrix の高度なディスプレイテクノロジーです。グラフィックデータをインテリジェントに分析および圧縮することで、Thinwire は多様なネットワーク条件とエンドポイントデバイス全体で最適なパフォーマンスを保証します。

HDX GraphicsとThinwireの主な機能

- **アダプティブディスプレイ圧縮:** Thinwire は、コンテンツタイプとネットワーク条件に基づいて圧縮アルゴリズムを動的に調整し、画質と帯域幅効率のバランスを確保します。この適応性により、帯域幅が制限された環境でもスムーズなパフォーマンスが可能です。
- **グラフィック処理ユニット:** HDX Graphics は、VDA で利用可能な場合、ハードウェアエンコーディングのために GPU の機能を自動的に活用します。

- **効率的なマルチメディアリダイレクト:** マルチメディアコンテンツをローカルレンダリングのためにエンドポイントに直接リダイレクトすることで、Thinwire はサーバー側の処理とネットワーク負荷を軽減し、ユーザーにシームレスなマルチメディア体験をもたらします。
- **最適化されたテキストおよび画像レンダリング:** ロスレステキスト圧縮やインテリジェントな画像キャッシュなどの技術を利用して、Thinwire は鮮明なテキストとシャープな画像を提供し、可読性と視覚的な明瞭さを向上させます。
- **高解像度ディスプレイのサポート:** Thinwire は、最大8台のモニターまでの高解像度およびマルチモニター設定を効率的に処理し、さまざまなディスプレイ構成で一貫した高品質の視覚体験をユーザーに提供します。
- **高フレームレートのサポート:** HDX は最大120フレーム/秒 (fps) のフレームレートをサポートし、高モーションアプリケーションやシナリオでスムーズで応答性の高いパフォーマンスを保証します。この機能は、特にゲーム、ビデオ編集、その他のグラフィック負荷の高いワークロードにおいて、ユーザーエクスペリエンスを向上させます。
- **10ビットハイダイナミックレンジ:** 10ビットハイダイナミックレンジ (HDR) 仮想デスクトップセッションでは、拡張された色域、より高いコントラストと明るさで高品質の画像とビデオをレンダリングするために、強化されたエンコードおよびデコード機能を使用できます。

Microsoft の Remote Desktop Protocol (RDP)、VMware の Blast Extreme、Amazon の NICE DCV などの他の業界ソリューションと比較して、Citrix の HDX Graphics と Thinwire は、現代のリモートワーク環境の要求を満たすように調整された包括的な機能セットを提供することで際立っています。さまざまなネットワーク条件に適応する能力と、効率的なリソース利用および優れた画質を組み合わせることで、堅牢で柔軟なリモートディスプレイソリューションを求める組織にとって主要な選択肢としての地位を確立しています。

HDX Graphics は、エンコードとレンダリングのハードウェアアクセラレーションのために、VDA 上のサーバー側グラフィック処理ユニット (GPU) をサポートします。HDX Graphics は、GPU の存在を自動的に検出し、その機能を自動的に使用します。

VDA に GPU を追加することは、グラフィックデザイン、ビデオレンダリング、3D CAD、データ処理および視覚化アプリケーションなどのユースケースで、グラフィック負荷の高いアプリケーションを高速化するのにも役立ちます。

Thinwire の構成

Thinwire は、その構成に応じて異なるグラフィックエンコードモードで動作できます。Thinwire の主な構成ポリシーは、「圧縮にビデオコーデックを使用する」ポリシーです。

- 優先する場合に使用 (デフォルト)
- 頻繁に変化する領域向け

- 画面全体の場合
- ビデオコーデックを使用しない

以下のセクションでは、各モードについて詳しく説明します。

圧縮設定にビデオコーデックを使用する	テキスト	画像	動画とビデオ	ユースケース
優先する場合に使用 (GPU)	ロスレス	JPEG	インテリジェントビルドからロスレス/ビデオコーデック*	グラフィックを多用するアプリケーションを含む、ほとんどのワークロードのデフォルト
推奨される場合に使用（GPUなし）	ロスレス	JPEG	ビデオコーデック	ほとんどのワークロードのデフォルト
頻繁に変化する領域向け	ロスレス	JPEG	ビデオコーデック	
画面全体向け	ビデオコーデック	ビデオコーデック	ビデオコーデック	ゲームのようなグラフィックを多用するアプリケーションで、ビルド・トゥ・ロスレスが推奨されない場合
ビデオコーデックを使用しない	ロスレス	JPEG	アダプティブJPEG	セッションの対話性よりも画質が優先される場合。GPU使用率が最小限に抑えられるため、最高の拡張性。

*インテリジェントビルドトゥロスレスは、特定の条件が満たされた場合にのみ使用されます。

ほとんどのユースケースでは、Thinwire の設定をデフォルトのままにしておくことで、最高のパフォーマンスと表示品質が得られます。

さまざまなユースケースの詳細については、Techzone ドキュメントの HDX Graphics の設計上の決定事項 を参照してください。

Thinwire フルスクリーンエンコーダー

概要

Citrix Virtual Apps and Desktops™ 2503 以降のリリースに伴い、「3Dグラフィックワークロード向けに最適化」ポリシーは非推奨となり、削除されました。

このポリシーは、特定のグラフィック負荷の高いワークロードに対して、強化された機能と改善されたユーザーエクスペリエンスを提供するフルスクリーンエンコーダーに置き換えられました。

フルスクリーンエンコーダーは、「圧縮にビデオコーデックを使用」ポリシーを「画面全体に対して」に設定することで構成できます。

フルスクリーンエンコーダーは、グラフィック負荷の高いワークロードに対して堅牢なパフォーマンスを提供しつつ、構成を簡素化します。画面分析や帯域幅の最適化を行わず、画面全体がビデオコーデックを使用してエンコードされるため、フレームレートとインタラクティブ性を最大化します。

このモードは、一貫したグラフィック忠実度が最重要である3Dアプリケーションやワークロードに特に適しています。

フルスクリーンエンコーダーの主な利点は、YUV444色空間を活用できることです。さらに、フルスクリーンエンコーディングは、セレクティブエンコーダーと比較して、最大120フレーム/秒（FPS）という最高のフレームレートを提供できますが、その結果、より多くの帯域幅とリソースを使用します。

フルスクリーンエンコーダーを使用する場合

グラフィックを多用するアプリケーションの場合、フルスクリーンエンコーダーを試す前に、ビルドトゥロスレスを検討する必要があります。ビルドトゥロスレスは、視覚品質ポリシーを「ビルドトゥロスレス」に設定し、「圧縮にビデオコーデックを使用」ポリシーをデフォルト設定の「優先時に使用」のままにすることで設定できます。

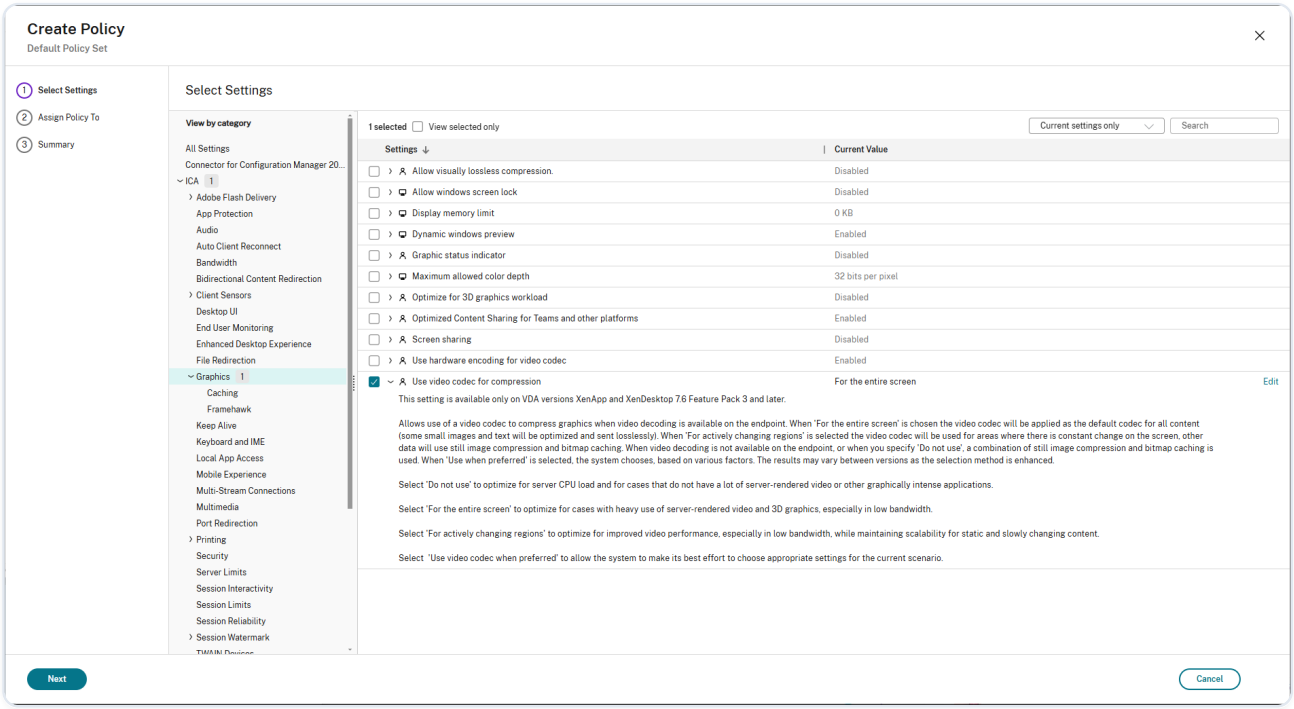
フルスクリーンエンコーダーは、YUV444カラースペースをサポートしているため（「視覚的にロスレスを許可」ポリシーを参照）、より高い動画品質が必要な場合にのみ推奨されます。ビデオ編集は、この追加の忠実度が必要となる良い例ですが、これはかなり高い帯域幅コストを伴います。

構成

フルスクリーンエンコーダーを有効にするには:

1. Citrix Studioでグラフィックポリシー設定に移動します。
2. 「圧縮にビデオコーデックを使用する」ポリシーを見つけます。
3. ポリシーを「画面全体」に設定します。
4. ポリシーの変更を適用し、デリバリーグループに伝播します。

コーデックの動作と構成に関する追加の詳細については、A自動ビデオコーデック構成 のドキュメントを参照してください。

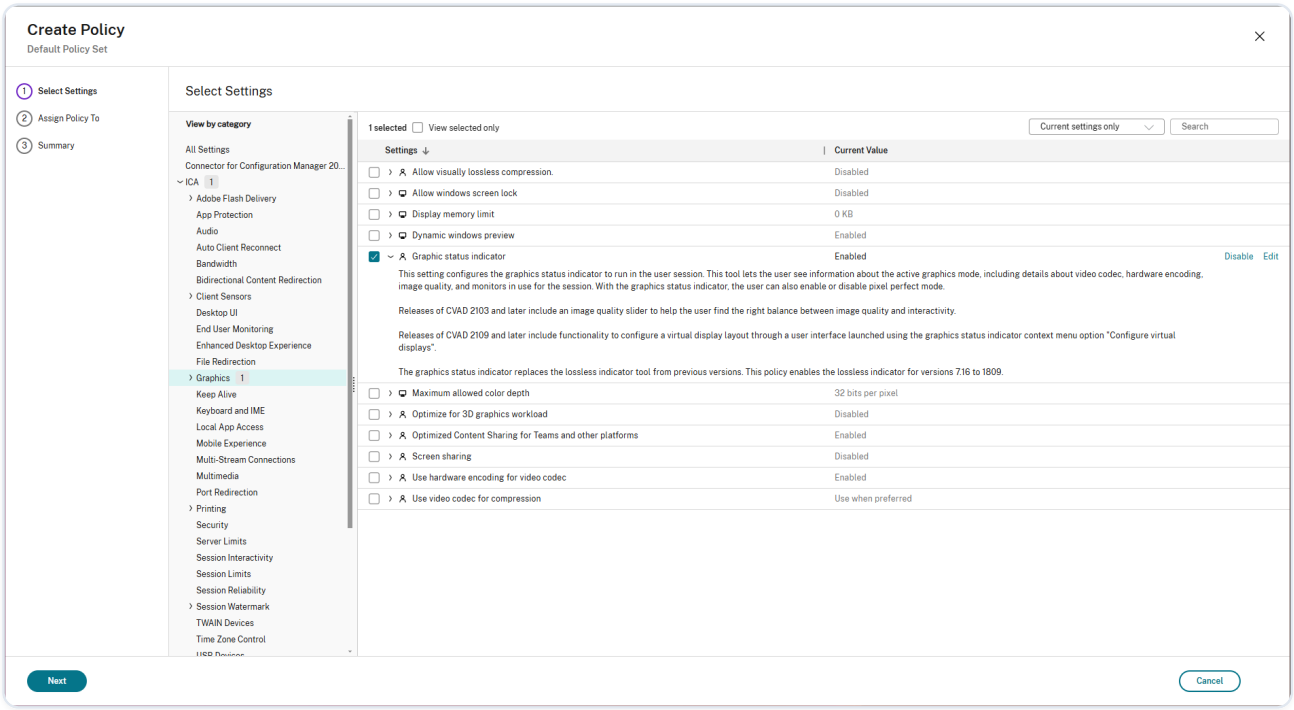


監視

フルスクリーンエンコーダーを監視するには、セッション内でグラフィックスステータスインジケーターを使用できます。現在、グラフィックスステータスインジケーターはデフォルトでは有効になっていません。

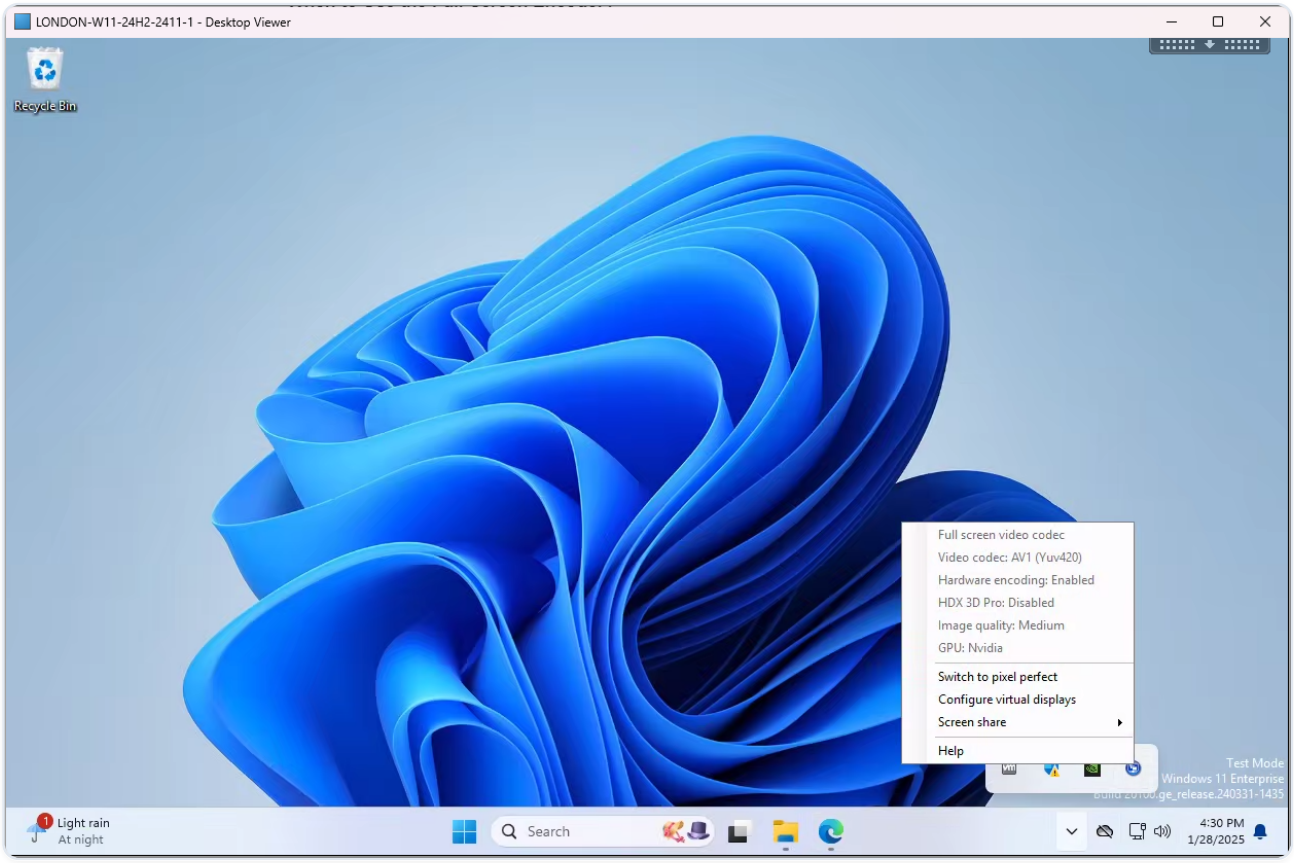
グラフィックスステータスインジケーターを有効にするには：

1. Citrix Studioでグラフィックスポリシー設定に移動します。
2. 「グラフィックスステータスインジケーター」ポリシーを見つけます。
3. ポリシーを「有効」に設定します。
4. ポリシーの変更をデリバリーグループに適用して伝播します。



グラフィックスステータスインジケーターは、リモートセッションのタスクトレイで利用可能になります。

フルスクリーンエンコーダーを使用すると、グラフィックスステータスインジケーターは次のように表示されます。



Thinwire 選択的エンコーダー

選択的エンコーディングは、Thinwireのデフォルトの動作モードです。このモードでは、Thinwireは画面コンテンツをリアルタイムで分析し、最適な視覚品質、セッション忠実度、および帯域幅使用量のために、画面の各部分をエンコードする最適な方法を選択します。

選択的エンコードは以下を使用します。

- テキスト: ロスレスエンコーディング
- 単純な画像と単色: ロスレスエンコーディング
- 複雑な画像/写真画像: JPEGエンコーディング
- 一時的なコンテンツと動画: ビデオコーデック、YUV 4:2:0カラーモードのH.264 / H.265 / AV1。

選択的エンコーディングには以下の特徴があります。

- アダプティブディスプレイ: Thinwireのアダプティブディスプレイテクノロジーは、動画（ビデオ、移動中の3D）を識別し、画像が移動している画面の部分でビデオコーデックを使用します。
- インテリジェントビルドトゥロスレス: GPUが存在する場合、インテリジェントビルドトゥロスレスは、動きが検出されたときに最高のセッションインタラクティビティを提供し、動きが停止したときにピクセルパーフェクトな画像を保証するために使用できます。Thinwireは、応答時間監視や画面アクティビティなど、いくつかの要因に基づいて、モニターごとにインテリジェントビルドトゥロスレスを自動的に有効にします。
- ハードウェアアクセラレーション: Virtual Delivery Agent (VDA) にGPUが存在する場合、フルスクリーンエンコーダーはGPUを活用してハードウェアアクセラレーションによるエンコーディングを行い、CPU使用率を削減し、パフォーマンスを向上させます。
- 自動ビデオコーデック選択: 使用されるビデオコーデックは、VDAとクライアントの機能に基づいて動的に選択されます。サポートされるコーデックは次のとおりです。
  - AV1: 効率性と高品質な圧縮のために推奨されます。
  - H.265 (HEVC): AV1をサポートしないシステムのためのフォールバックとして使用されます。
  - H.264 (AVC): レガシーまたは低機能のシナリオ、またはVDAにGPUが存在しない場合に使用されます。

構成

選択的エンコードはデフォルトの動作モードであるため、追加の構成は不要です。デフォルトでは、サーバー側GPUが利用可能な場合、選択的エンコードはIntelligent Build to Losslessを使用します。

選択的エンコーディングを明示的に設定するには：

1. Citrix Studio でグラフィックポリシー設定に移動します。
2. 「圧縮にビデオコーデックを使用する」ポリシーを見つけます。
3. ポリシーを「優先する場合に使用」に設定します。
4. ポリシーの変更を適用し、デリバリーグループに伝播します。

グラフィックエンコーダー(/en-us/citrix-virtual-apps-desktops/2511/media/policy-default.png)

Intelligent Build to Losslessは、Citrix Virtual Apps and Desktops™バージョン2503で導入されました。2503より前のCVADバージョンでは、Intelligent Build to Losslessなしで選択的エンコードが機能します。

GPUを搭載したVDAでインテリジェントビルドトゥロスレスなしで選択的エンコーディングを使用するには（2503より前のバージョンのレガシー動作を設定するため）：

1. Citrix Studio でグラフィックポリシー設定に移動します。
2. 「圧縮にビデオコーデックを使用する」ポリシーを見つけます。
3. ポリシーを「アクティブに変更される領域の場合」に設定します。
4. ポリシーの変更を適用し、デリバリーグループに伝播します。

グラフィックエンコーダー(/en-us/citrix-virtual-apps-desktops/2511/media/policy-foractivelychangingregions.png)

2503より前のバージョンでは、「use when preferred」と「for actively changing regions」は同じでした。2503では、「use when preferred」のデフォルト設定には、GPUが利用可能な場合に「Intelligent Build to lossless」が含まれます。GPUがない場合、「use when preferred」は「for actively changing regions」と同じです。

インテリジェントロスレスへのビルド

前提条件

Intelligent Build to Lossless は、GPU 対応 VDA のすべてのユースケースで新しいデフォルトモードです。

VDA

Intelligent Build to Losslessは、Windows、Linux、MacのVDAで利用可能です。

重要な点として、CVADのバージョン要件はオペレーティングシステムによって異なります。

- **Windows VDA:** CVAD 2503以降
- **Linux VDA:** CVAD 2503以降
- **macOS VDA:** 2507 以降

VDA ハードウェア: サーバー側 GPU が必要です (NVIDIA、AMD、または Intel)。

詳細については、Linux VDA向けIntelligent Build to Losslessを参照してください。

> **注**:
>
> Intelligent Build to Losslessは、GPUのないVDAでは利用できません。

Citrix Workspace™ アプリ

Citrix Workspaceアプリ: 現在サポートされているすべてのバージョン。

Intelligent Build to Lossless はクライアントのハードウェアに依存せず、クライアント側 GPU の有無にかかわらず、すべてのクライアントで動作します。

インテリジェントビルドトゥロスレスを使用するタイミング?

インテリジェントビルドトゥロスレスは、すべてのワークロードとネットワークシナリオに適しています。特に、混合ワークロードや、ハイエンドの金融トレーダーのようにエンドユーザーが複数のモニターや高解像度ディスプレイを使用するユースケースに最適です。

インテリジェントビルドトゥロスレスは、Citrix Virtual Apps and Desktops™ バージョン2503以降を実行し、サーバー側GPUを搭載しているVDAでは、デフォルトで有効になっています。

追加のエンドポイント要件はありません。ただし、Citrix®は常に、利用可能な最新のCWAクライアントバージョンを使用することを推奨しています。

VDAのバージョン	サーバー側GPU	インテリジェントビルドトゥロスレス
VDAバージョン2503以前	はい	いいえ

VDAのバージョン	サーバー側GPU	インテリジェントビルドトゥロスレス
VDAバージョン2503以前	いいえ	いいえ
VDA 2503以降	**はい**	**はい**
VDA2503以降	いいえ	いいえ

Citrixは、以下のシナリオでIntelligent Build to Losslessの使用を推奨します。

医用画像処理：

X線、MRI、CTスキャンなどの診断画像を閲覧する際に、圧縮アーティファクトが詳細を不明瞭にし、臨床精度を損なう可能性がある場合。

3D CAD/CAMおよびエンジニアリング：

複雑で精巧なモデルや設計図を扱う際、設計と製造の両方において、正確な線の鮮明さが不可欠です。

プリプレスおよびグラフィックデザイン：

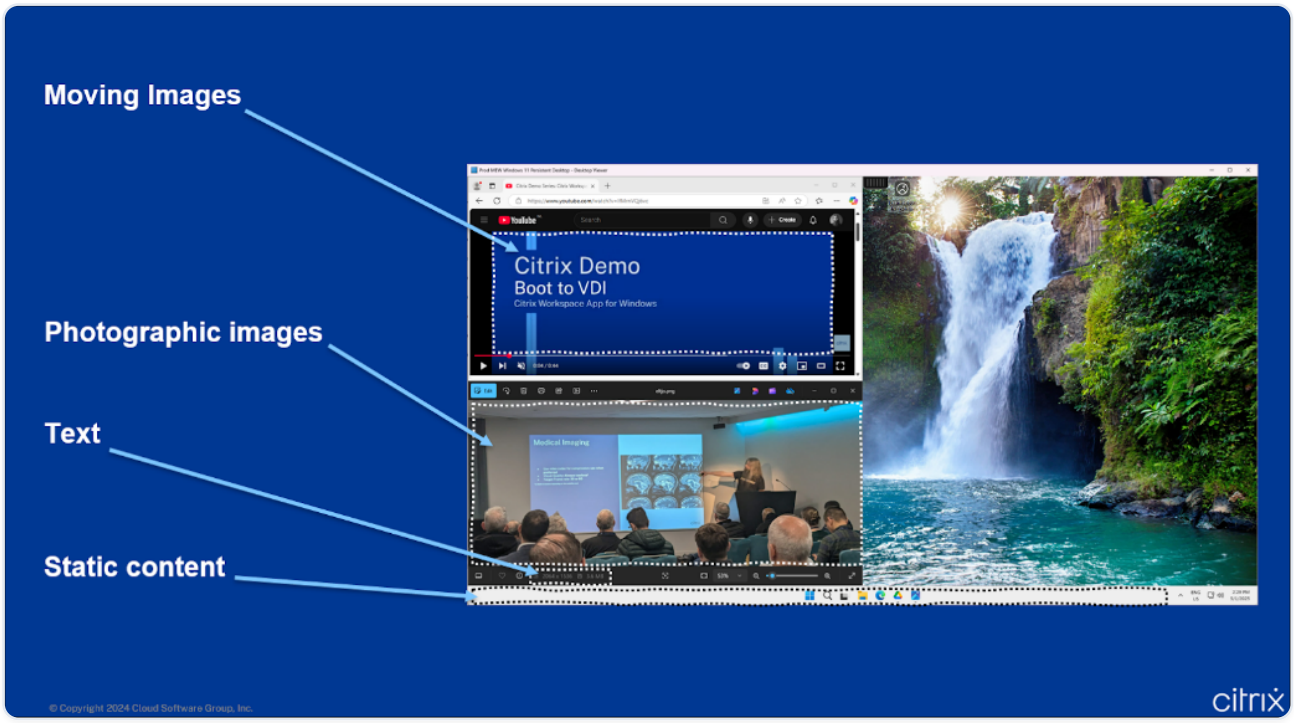
カラープルーフ、高解像度画像、またはテキストレイアウトを確認する際に、品質管理のために実際の高品質なソース素材を見ることが求められる場合。

金融サービス：

複数の高解像度モニターを使用する際に、トレーディングフロアで高密度なリアルタイムデータを表示する場合、静的なチャートや数値の絶対的な鮮明さが分析に不可欠です。

動作の仕組み?

この機能は、HDX™ Thinwire ディスプレイプロトコルの一部として動作します。



1. Thinwire が動画を含む画面領域を検出すると、VDA とクライアントの機能に応じて、設定されたビデオコーデック（H.264、H.265、または AV1）を使用してその領域をエンコードします。これにより、フレームレートと応答性が優先されます。
2. 画面の領域が静止状態になると（つまり、動きが検出されなくなると）、Thinwire は静止領域に対する一連の洗練された更新を通じて、その領域を徐々にロスレス状態に構築します。

構成

Citrix Virtual Apps and Desktops™ リリース 2503 以降では、サポートされているGPUを搭載したVDAでインテリジェントビルドトゥロスレスがデフォルトで有効になっています。これを有効にするためにポリシーを作成する必要はありません。この動作は、「ビデオコーデックを使用して圧縮する」ポリシーの状態によって制御されます。

インテリジェントビルドトゥロスレスを有効にするには (デフォルトの動作)

「ビデオコーデックを使用して圧縮する」ポリシーを*未構成*のままにします。または、「*ビデオコーデックを使用して圧縮する*」ポリシーを明示的に「*優先する場合に使用*」に設定することもできます。

インテリジェントビルドトゥロスレスを無効にするには (非推奨)

「ビデオコーデックを使用して圧縮する」ポリシーを明示的に「アクティブに変更される領域の場合」に設定します。

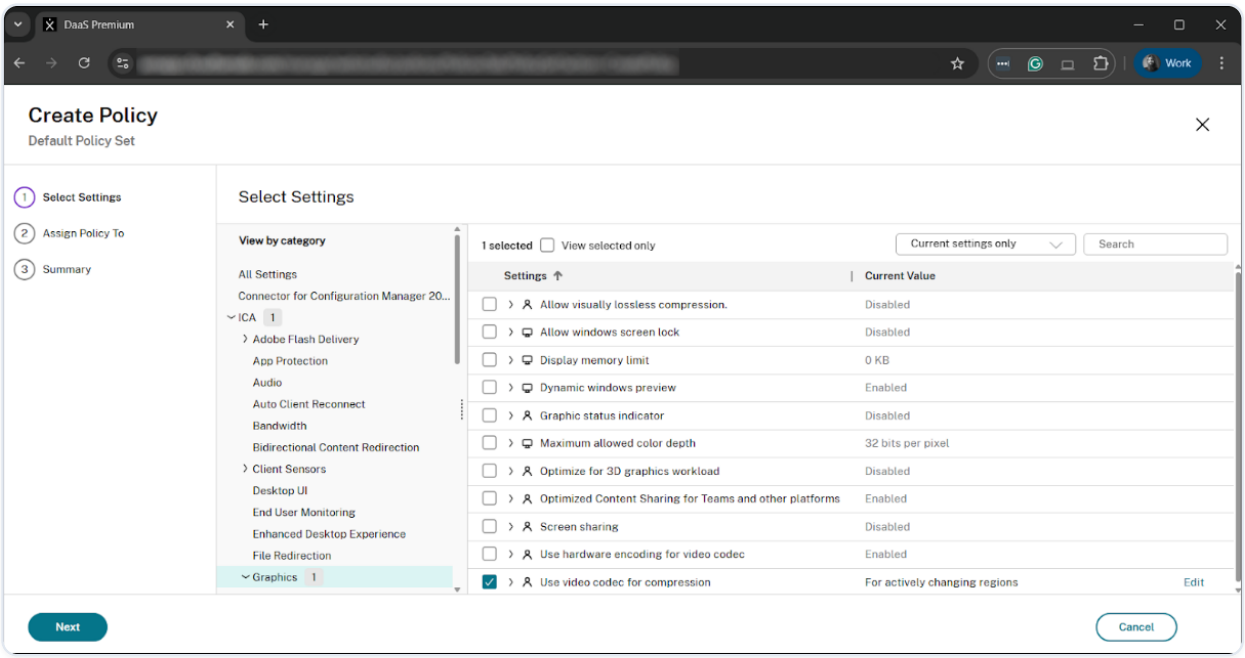
「アクティブに変更される領域の場合」を選択すると、Thinwireはサーバー側GPUを搭載した2503より前のVDAと同様に選択的エンコードを使用します。

ステップバイステップの手順

Citrix Studioを使用してインテリジェントビルドトゥロスレスポリシーを明示的に無効にするには、以下の手順に従ってください。

CITRIX STUDIO (GUIを使用)

1. Citrix Studioを**開きます**。
2. 左側のペインで、**ポリシー**に移動します。
3. **ポリシーの作成**をクリックするか、ターゲットユーザーまたはデリバリーグループに適用される既存のポリシーを編集します。
4. ポリシー構成ウィンドウで、検索バーを使用して「**ビデオコーデックを使用して圧縮する**」ポリシーを見つけます。このポリシーは、**ICA®** > **グラフィック**カテゴリの下にあります。
5. ポリシーを**選択**し、**編集**をクリックします。
6. デフォルトでは、このポリシーは**優先時に使用**に設定されています。**デフォルト値を使用**オプションのチェックを外します。
7. 活発に変化する領域に対して値をに変更します。
8. **OK**をクリックしてポリシー設定を保存します。
9. ポリシーが有効になっていること、適切に優先順位が付けられていること、および適切な**デリバリーグループ**またはユーザーフィルターに適用されていることを確認します。



> **注:**

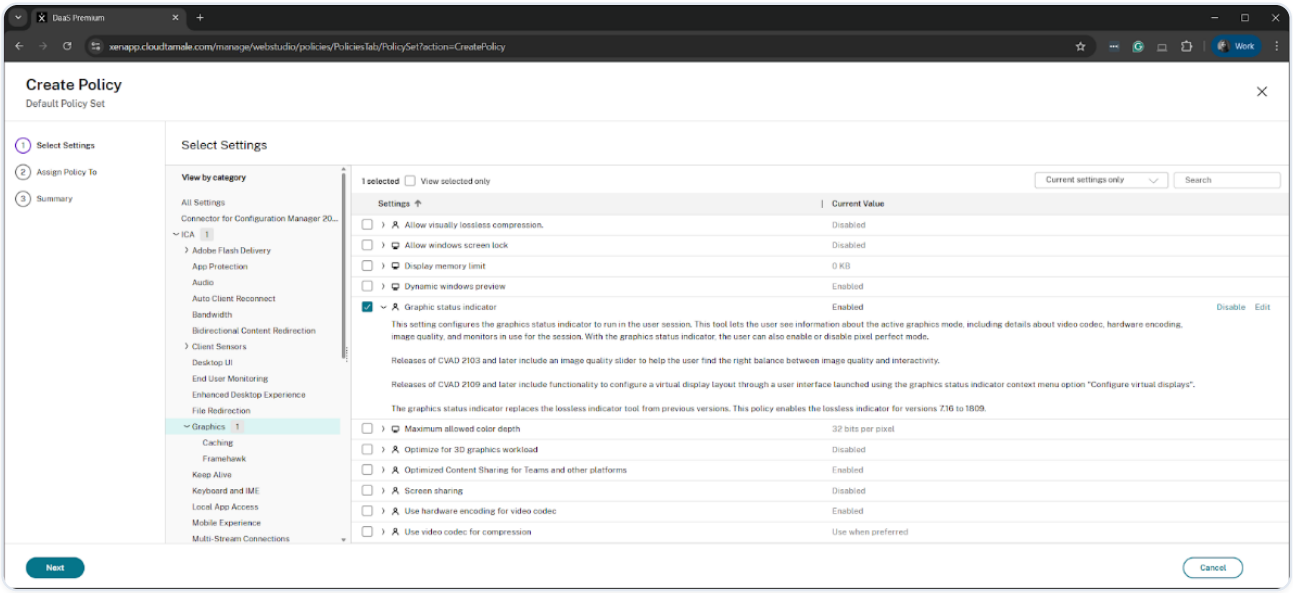
> ビジュアル品質ポリシーが明示的に「Build to Lossless」または「Always Lossless」に設定されている場合、これらの設定が常に優先され、新しいインテリジェントビルドツーロスレス機能よりも優先されます。最良の結果を得るには、「ビジュアル品質」ポリシーと「圧縮にビデオコーデックを使用する」設定をデフォルト値のままにしてください。

インテリジェント ビルド トゥ ロスレスの監視

Intelligent Build to Lossless は、Citrix® セッション内から Graphics Status Indicator を使用して監視できます。現在、Graphics Status Indicator はデフォルトでは有効になっていません。

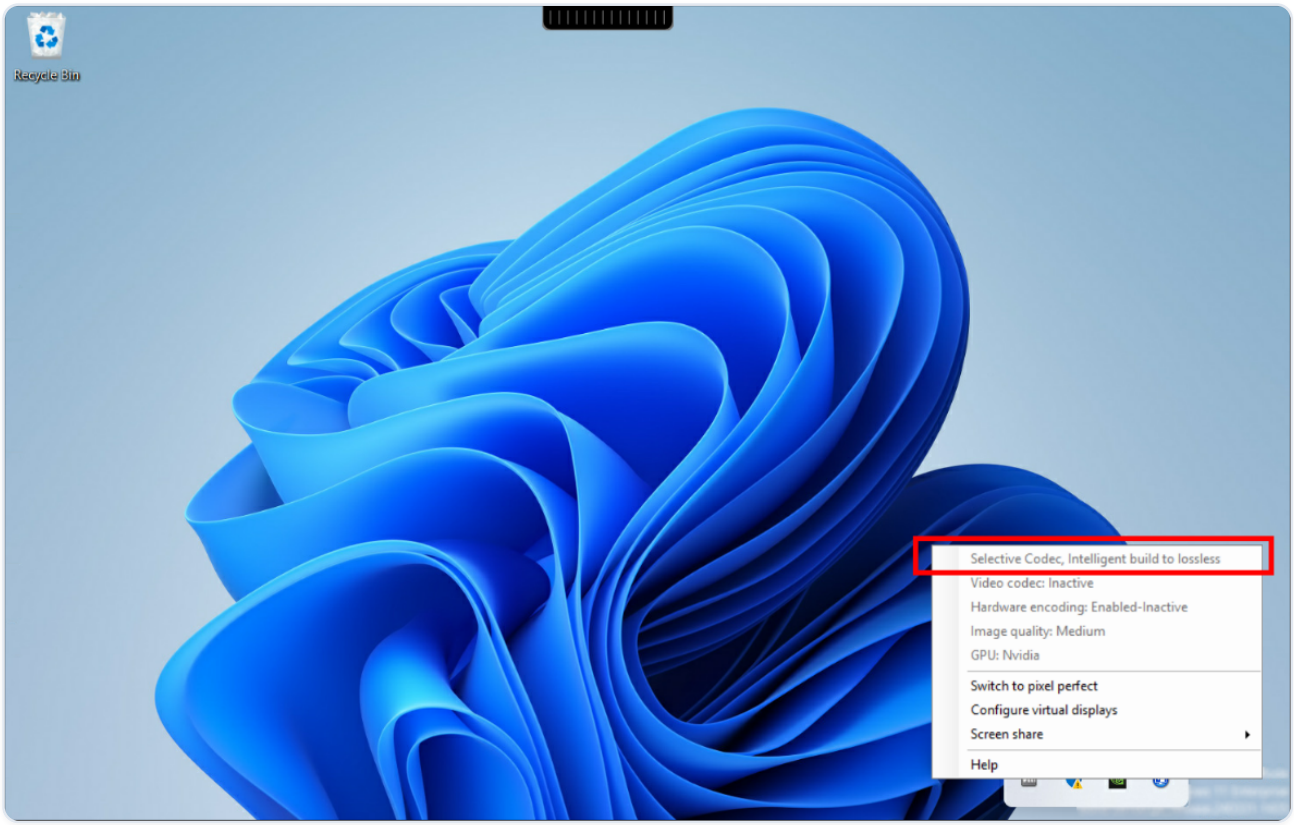
Graphics Status Indicator を有効にするには

1. Citrix Studio を開きます。
2. 左側のペインで、**ポリシー**に移動します。
3. **ポリシーの作成**をクリックするか、ターゲットユーザーまたはデリバリーグループに適用される既存のポリシーを編集します。
4. ポリシー構成ウィンドウで、検索バーを使用して、**ICA® > グラフィックス** カテゴリの下にある**Graphics Status Indicator** ポリシーを見つけます。
5. **ポリシー**を選択し、**有効にする**をクリックします。
6. **OK**をクリックしてポリシー設定を保存します。
7. ポリシーが有効になっており、正しく優先順位が付けられ、適切な**デリバリーグループ**またはユーザーフィルターに適用されていることを確認します。

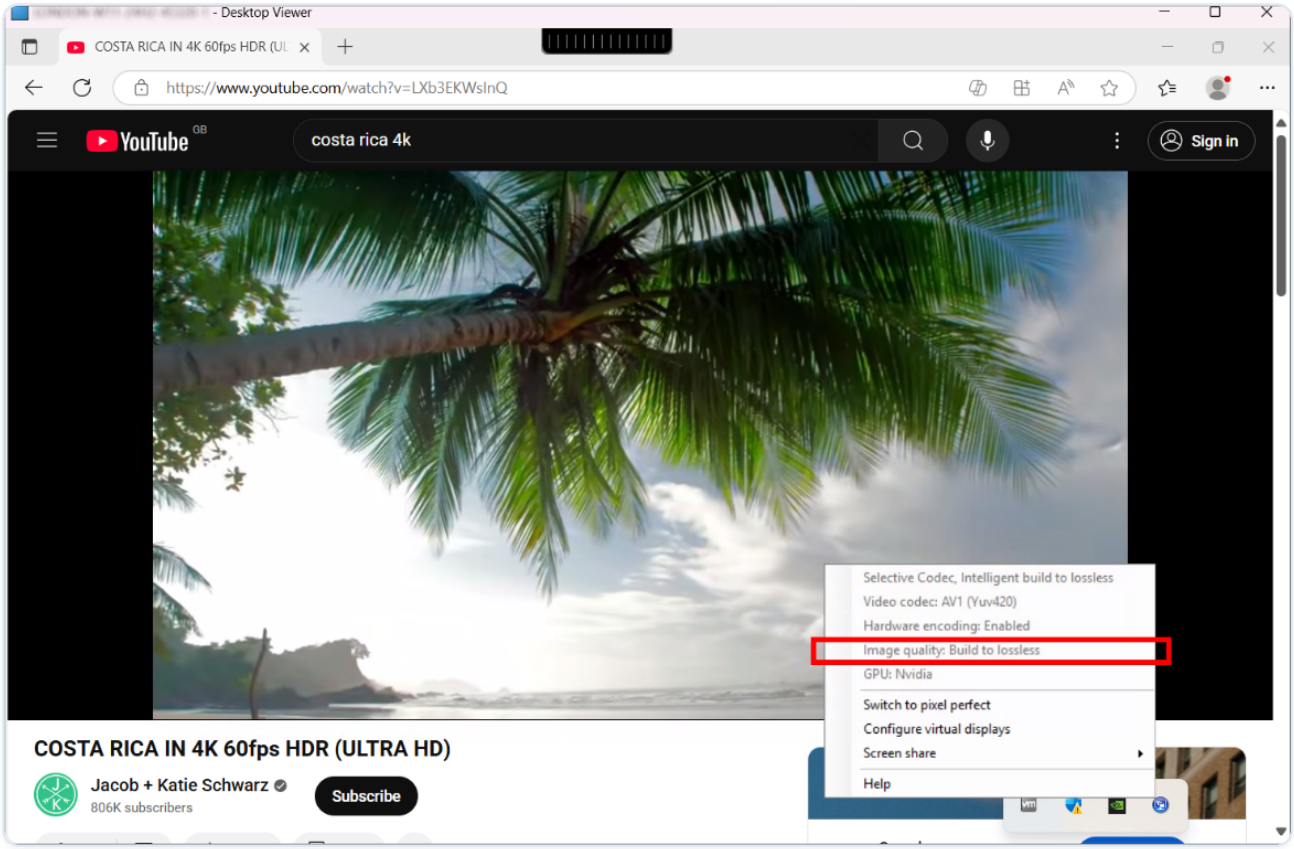


Intelligent Build to Lossless がユーザーセッションで利用可能であるが、まだアクティブ化されていない場合、セッションは通常の Selective Encoding を使用し、Graphics Status Indicator は、これを最上行に「Selective Codec, Intelligent Build to Lossless」と表示します。Intelligent Build to

Lossless がまだ有効になっていないため、「Visual Quality」には、現在構成されている視覚品質（例：低、中、高）が表示されます。

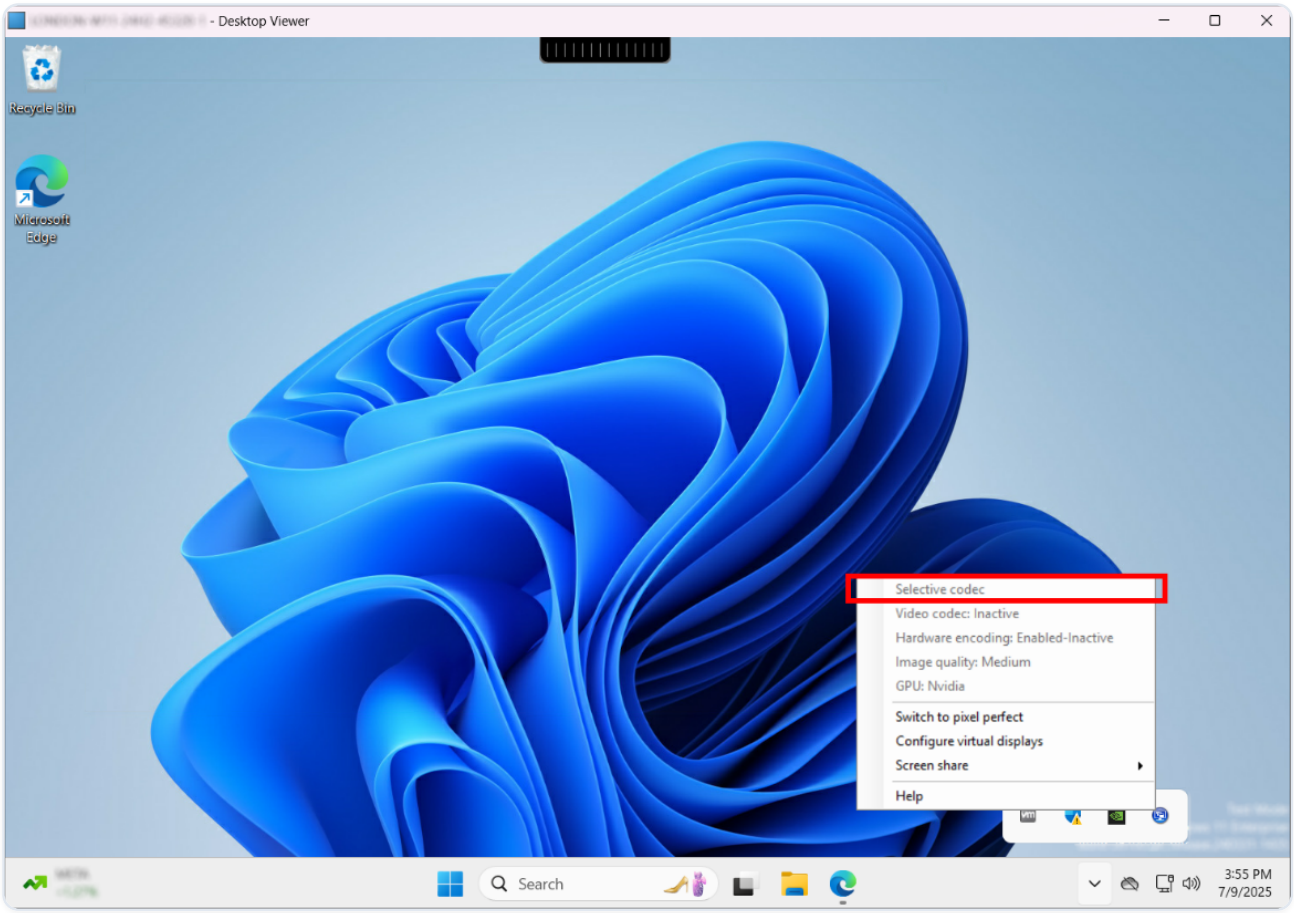


Thinwire が1つ以上の接続されたモニターで Intelligent Build to Lossless を有効にするのに好ましい条件を検出すると、Graphics Status Indicator は、4行目の Visual Quality を「Build to Lossless」に変更します。これが、Intelligent Build to Lossless がアクティブであることを示す主要な指標です。



ThinwireがBuild to Losslessの必要性がなくなったと判断すると、ピクセルパーフェクトな画像に徐々に構築し、その後、通常のSelective Encodingに戻ります。グラフィックステータスインジケーターは、画質を構成済みのVisual Qualityモード（例：低、中、高）に戻します。

Intelligent Build to Losslessが利用できない場合（例えば、2503より前のリリースのVDAを使用している場合、サーバー側GPUのないVDAを使用している場合、またはIntelligent Build to Losslessが明示的に無効になっている場合）、グラフィックステータスインジケーターは、代わりに最上段に「Selective Codec」と表示します。



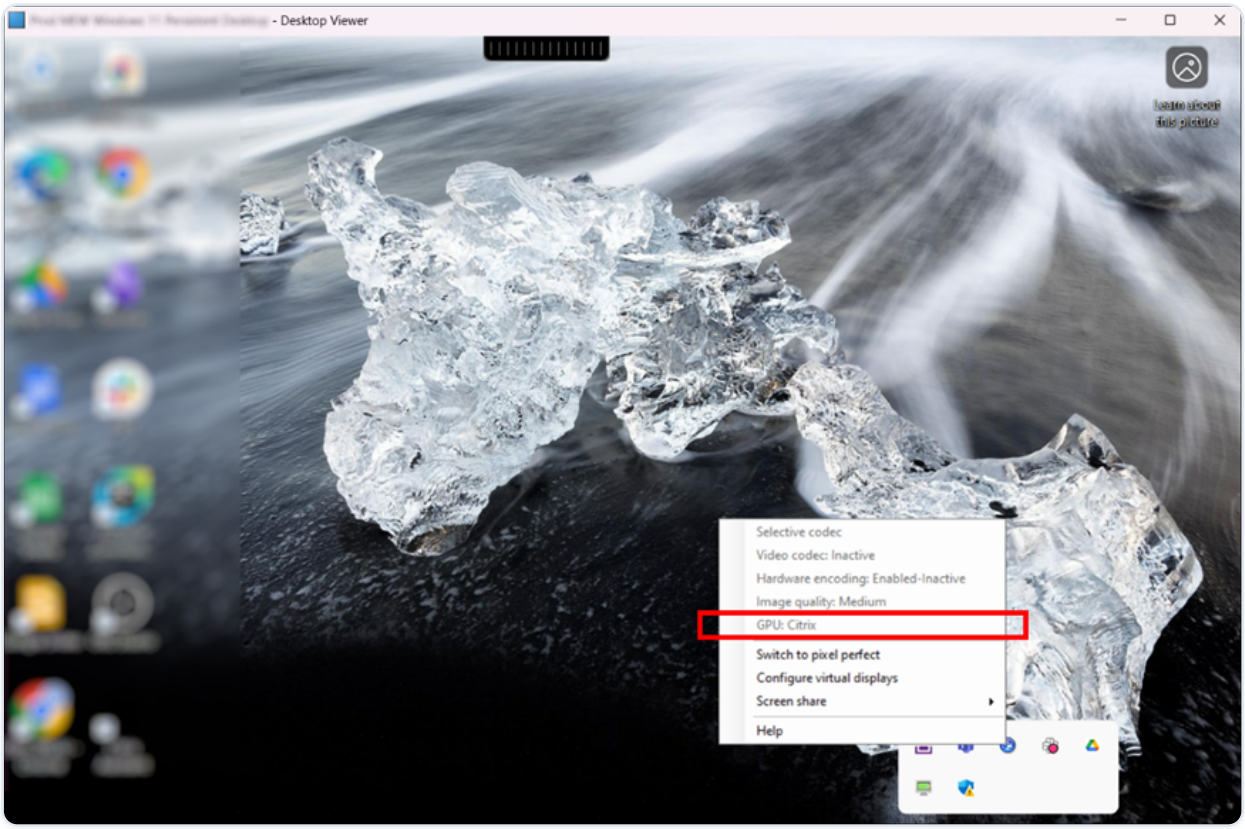
Intelligent Build to Losslessのより詳細なテストと監視のために、どのモニターがBuild to Losslessモードであるかを示すモニターごとの視覚インジケーターを有効にすることもできます。

この設定はテストとトラブルシューティングのみを目的としており、製品環境では使用しないでください。詳細については、Intelligent Build to Losslessの視覚インジケーターを有効にするためのKB記事を参照してください。

トラブルシューティング

セッションでIntelligent Build to Losslessが利用できない場合は、以下の要件を確認してください。

1. VDAがバージョン2503以降で実行されていることを確認してください。
2. セッションでサーバー側のGPUが利用可能であることを確認してください。これを検証する最も簡単な方法は、グラフィックスステータスインジケーターを使用して、GPUの行にGPUベンダー名（例：NVIDIA、Intel、AMD）が表示されているかを確認することです。GPUが存在せず利用できない場合、GPUベンダー名には「Citrix」と表示されます。



または、Citrix Monitorを使用して、VDAのサーバー側GPUの有無を確認し、GPU使用率のトラブルシューティングを行うことができます。

3. 「圧縮にビデオコーデックを使用する」ポリシーが、設定されていない（デフォルト値を使用している）か、または「優先する場合に使用」に設定されていることを検証してください。

ポリシーモデリングウィザードを使用して、ポリシーがセッションに正しく適用されているかを確認できます。

DaaS側の詳細については、ポリシープロセスを参照してください。

ビデオコーデックは使用しないでください

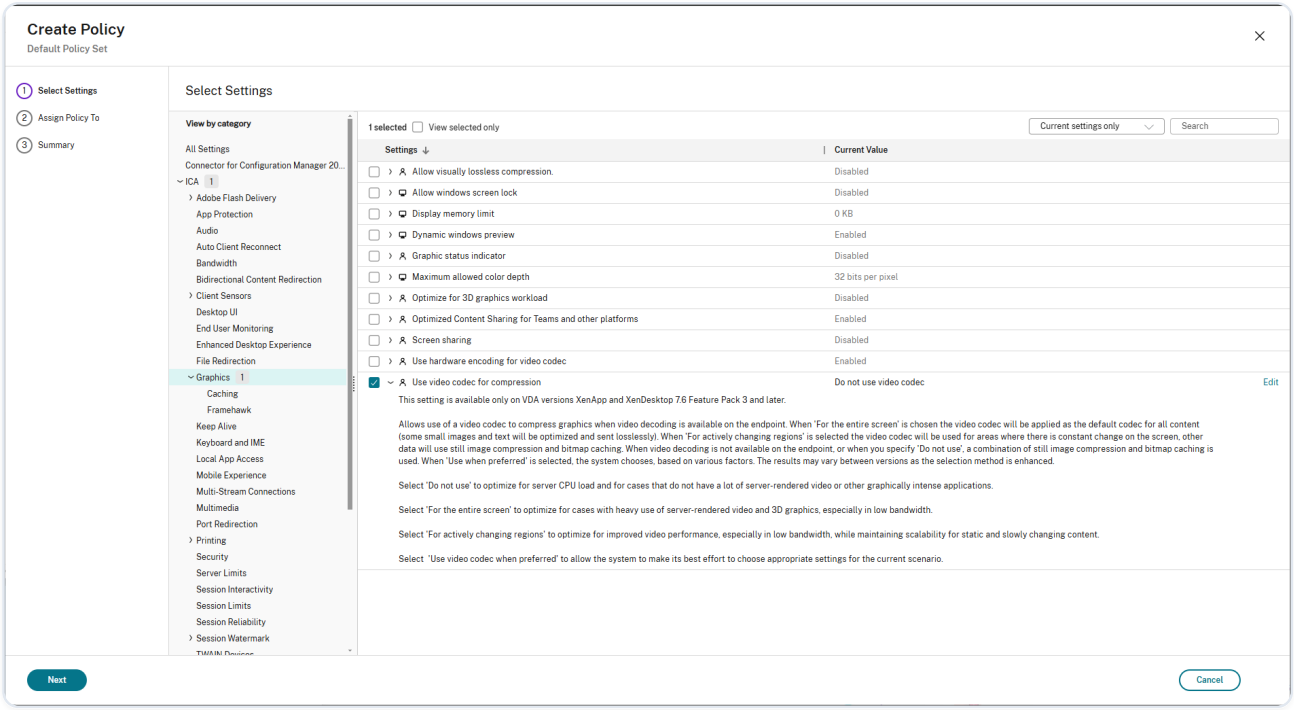
リモートセッションのエンコードにビデオコーデックを使用することにはいくつかの利点があり、高速で比較的軽量です。ビデオコーデックは動画の処理に特化しており、リモートセッションでよくあるように、動画の処理に非常に優れています。

しかし、画質や色精度が最重要である場合など、ビデオコーデックの使用が最善の解決策ではないシナリオもあります。当社の選択的エンコーダーは、ほとんどの場合、画面のどの部分がビデオコーデックによるエンコードの恩恵を受けるかを非常にうまく判断しますが、Thinwireに画面圧縮のためにビデオコーデックを一切使用しないように強制することもできます。

Thinwireがビデオコーデックを使用しないように設定されている場合、Twinwireは圧縮にJPEGとロスレスRLEのみを使用し、可能な限り最高の画質を維持します。Thinwireは、選択的エンコードまたはフルスクリーンエンコードを使用する場合よりも、かなり多くの帯域幅を使用します。

構成

Thinwireポリシー「圧縮にビデオコーデックを使用する」を「ビデオコーデックを使用しない」に設定します。

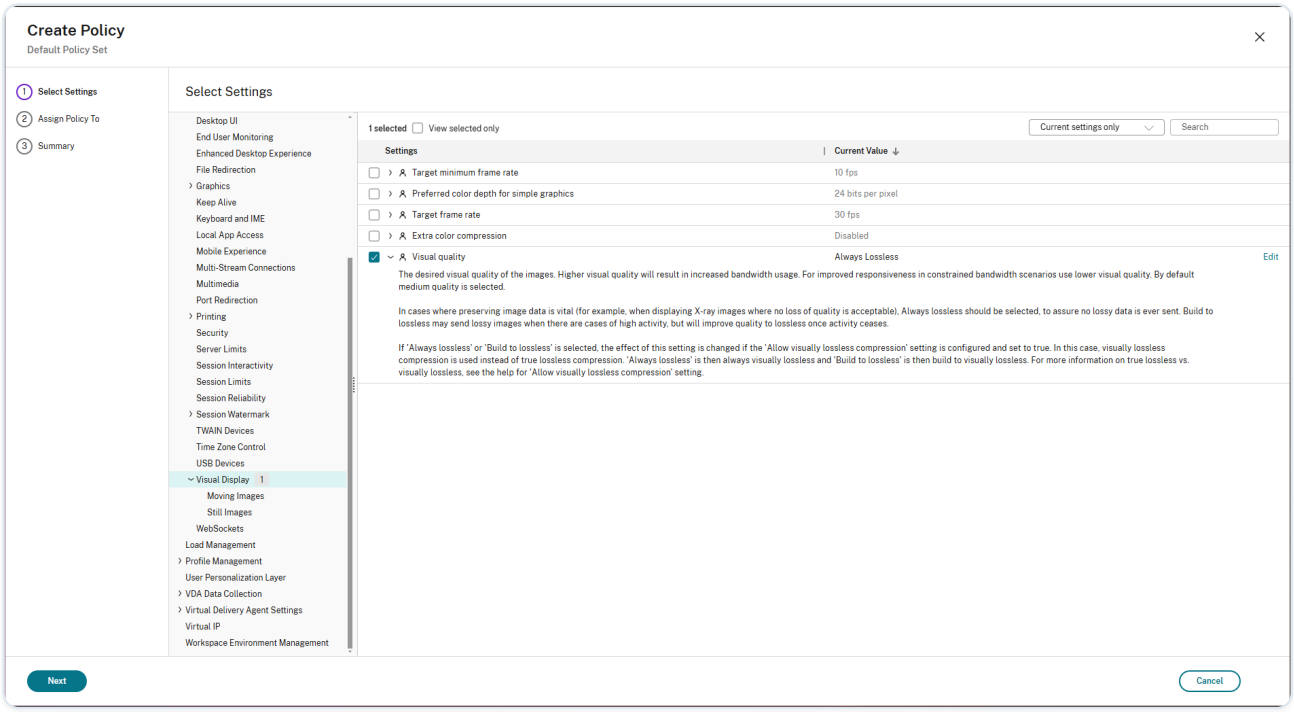


常時ロスレスモード

常時ロスレスモードを使用すると、クライアントにイメージの非可逆データが送信されないことが保証されます。これは、すべてのフレームがロスレスコーデックでのみエンコードされ、品質がピクセルパーフェクトになることを意味します。

常時ロスレスの圧縮率は、他のモードを使用する場合ほど良くありません。また、常時ロスレスモードを設定すると、かなりの帯域幅が使用されます。帯域幅が十分に利用できない場合、これはインタラクティブ性に大きな影響を与える可能性があります。

Citrix®は、ロスレスの画質が必要とされる特定のユースケース（医療画像処理のユースケースなど）でのみ、この設定の使用を推奨します。

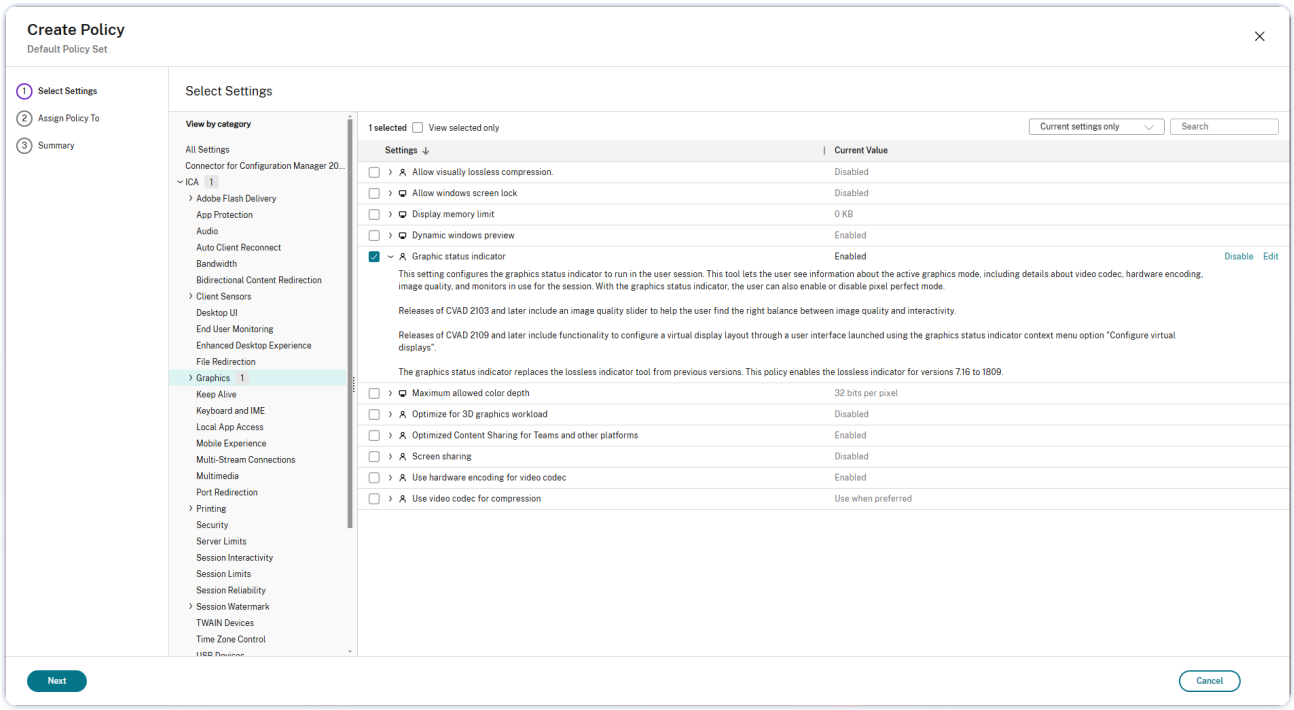


常時ロスレスモードを明示的に設定するだけでなく、グラフィックステータスインジケーターが利用可能な場合、エンドユーザーはセッション中にロスレスモードを切り替えることもできます。

現在、グラフィックステータスインジケーターはデフォルトでは有効になっていません。

グラフィックステータスインジケーターを有効にするには：

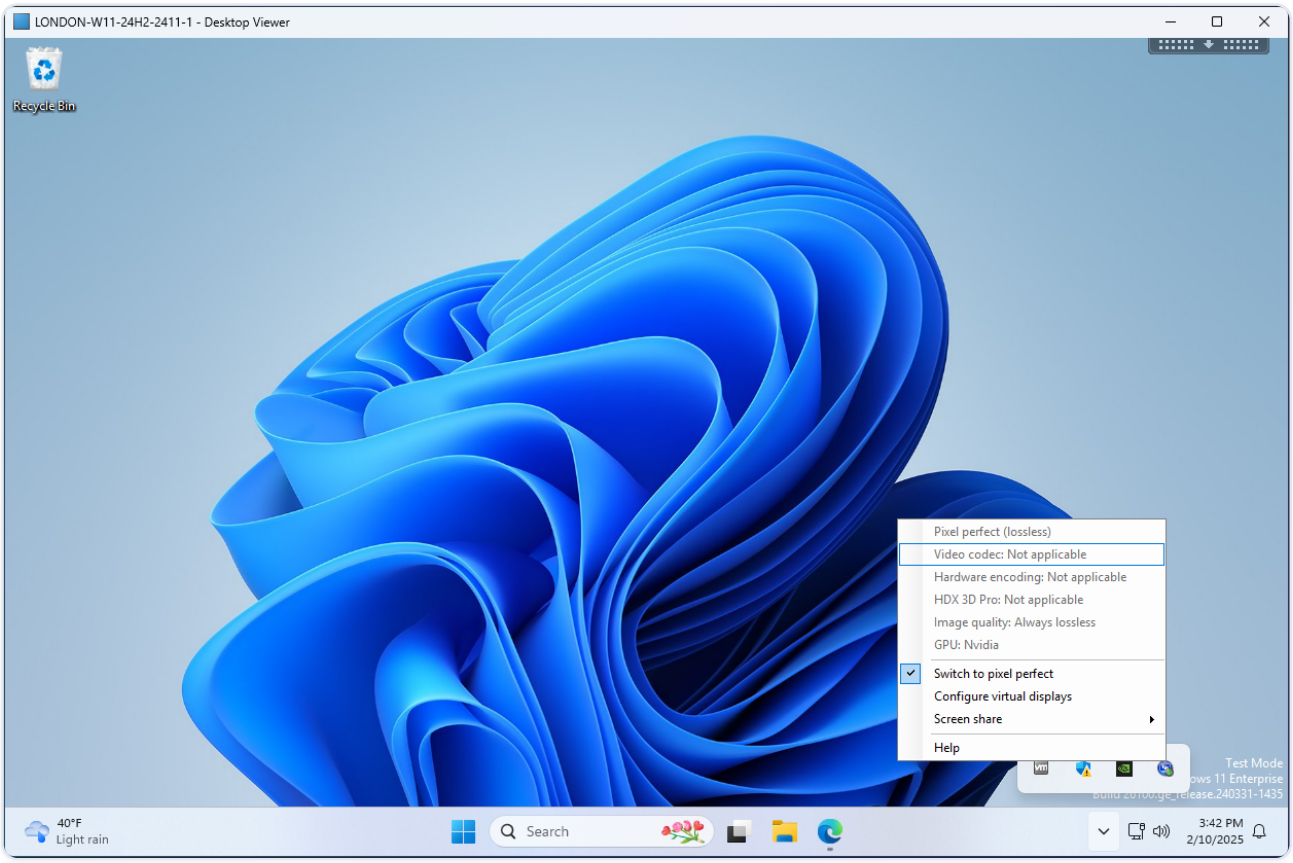
1. Citrix Studio でグラフィックポリシー設定に移動します。
2. 「グラフィックステータスインジケーター」ポリシーを見つけます。
3. ポリシーを「有効」に設定します。
4. ポリシーの変更を適用し、デリバリーグループに伝播します。



エンドユーザーとして常時ロスレスモードを切り替えるには：

1. タスクトレイでグラフィックステータスインジケーターを見つけます。
2. VDAのタスクトレイにあるグラフィックスステータス 1. 1. インジケーターを右クリックします。
3. 「ピクセルパーフェクトに切り替える」を選択します。

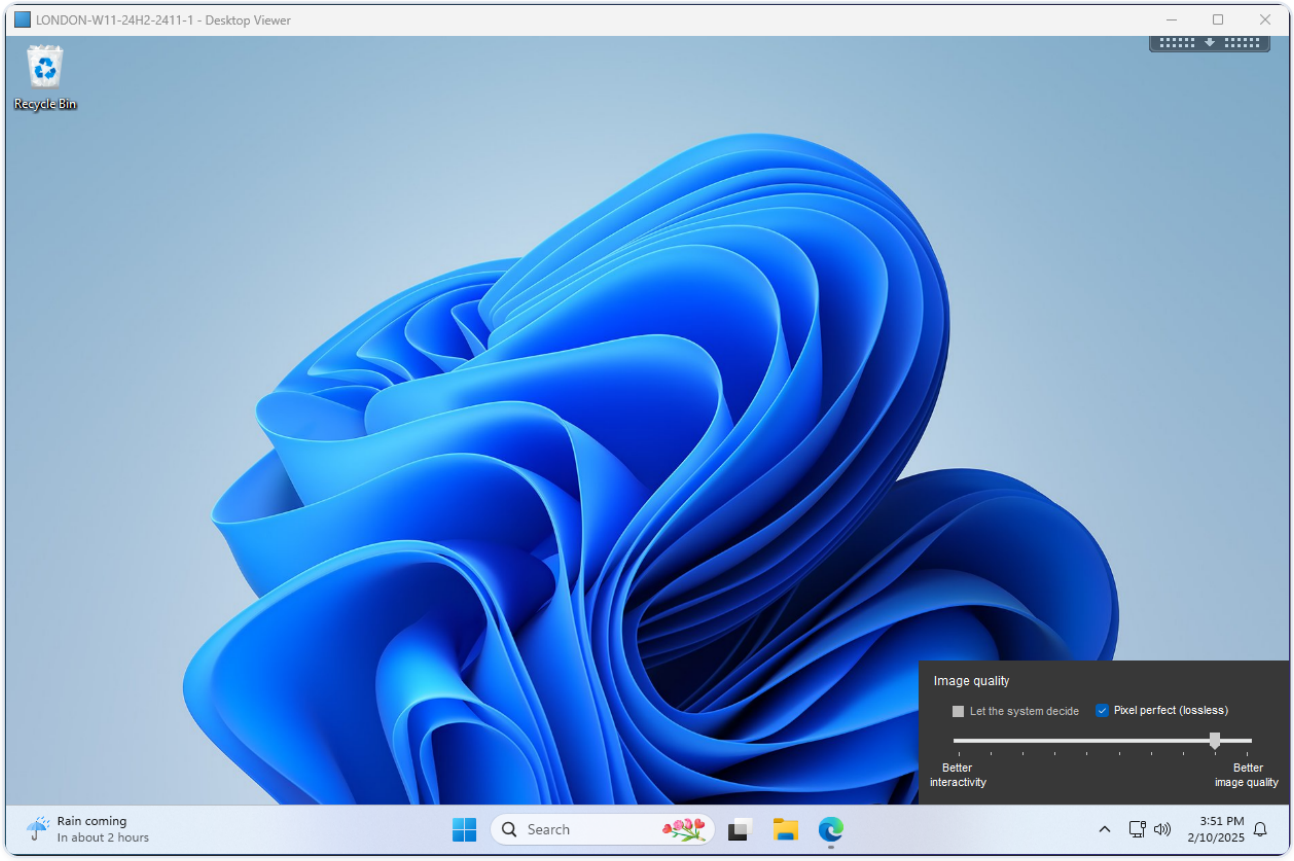
グラフィックスステータスインジケーターのアイコンに緑色のインジケーターが表示され、ロスレスモードが有効になっていることを示します。



または、:

1. タスクトレイにあるグラフィックスステータスインジケーターを見つけます。
2. VDAのタスクトレイにあるグラフィックスステータスインジケーターをクリックします。
3. 「システムに決定させる」の選択を解除します。
4. 「ピクセルパーフェクト (ロスレス)」を選択します。

グラフィックスステータスインジケーターのアイコンに緑色のインジケーターが表示され、ロスレスモードが有効になっていることを示します。



カラースペース

これは、YUV 4:2:0およびYUV 4:4:4の色空間と色圧縮設定について説明する新しいセクションです。

概要

選択された色空間によって、HDX™ Graphicsがどの色圧縮モード（クロマサブサンプリングとも呼ばれる）を使用するかが決まります。デフォルトでは、HDX GraphicsはYUV 4:2:0クロマサブサンプリングを使用します。

クロマサブサンプリングは、VDAからクライアントにビデオデータを送信するために必要な帯域幅を削減するために使用される技術です。人間の目は色の変化（クロミナンス）よりも明るさ（ルミナンス）の変化に敏感であるため、送信される色情報の量を減らすことで機能します。

4:2:0、4:2:2、4:4:4のような比率で示される、さまざまなクロマサブサンプリング方式が存在します。これらの比率は、ルミナンス情報に対してサンプリングされるクロミナンス情報の量を表します。

4:4:4 - クロマサブサンプリングなし。すべての色情報が保持されます。これにより、最高の画質と色精度が得られますが、最も多くの帯域幅を必要とします。

4:2:0 - クロミナンス情報は、水平方向と垂直方向の両方で2分の1にサブサンプリングされます。これにより、最大の帯域幅削減が実現されますが、目に見える色のアーティファクトが発生する可能性があります。



Citrix HDXグラフィックスは、仮想デスクトップ環境での帯域幅使用量を最適化するためにクロマサブサンプリングを利用します。デフォルトでは、HDXは画面コンテンツのエンコードにYUV 4:2:0を使用します。これにより、一般的なオフィス生産性アプリケーション/ほとんどのユースケースにおいて、画質と帯域幅効率の良好なバランスが提供されます。

画面全体がビデオコーデック（フルスクリーンエンコーダーを使用）でエンコードされると、色圧縮によってテキストのような高コントラストの詳細が劣化し、ぼやけて読みにくくなることがあります。

医療画像処理、ビデオ編集、CAD/CAMアプリケーションなど、色精度が最も重要となるシナリオでは、HDXはYUV 4:4:4もサポートしています。

これにより、エンコード中に色情報が失われないことが保証され、可能な限り最高の画像忠実度と色精度が提供されます。YUV 4:4:4 は YUV 4:2:0 よりも大幅に多くの帯域幅を使用することに注意してください。

帯域幅の輻輳に関連する問題を回避するために、本番環境でYUV 4:4:4を有効にする前に、テストシナリオで帯域幅の使用量を検証してください。

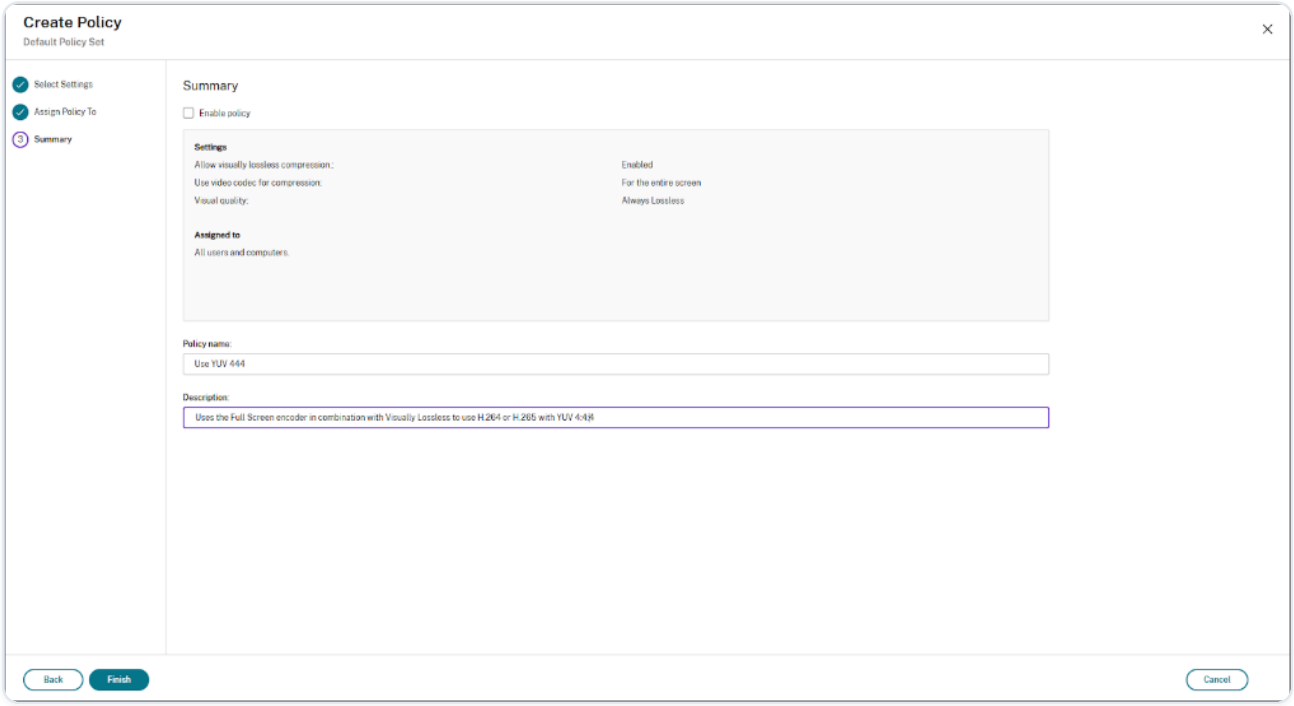
構成

YUV 4:4:4 を使用してより高い画質と色精度を実現するには、Citrix Studio 内でいくつかの HDX™ ポリシー設定を調整して YUV 4:4:4 を有効にする必要があります。

圧縮にビデオコーデックを使用: これを「画面全体」に設定すると、ビデオコーデック (および選択したクロマサブサンプリング) が画面全体のコンテンツに適用されます。

視覚品質: 帯域幅の消費よりも画質を優先するには、「ロスレスにビルド」または「常にロスレス」を選択します。

視覚的にロスレスを許可: 視覚的にロスレスな圧縮を可能にするには、このポリシーを有効にします。



デフォルトでは、ThinwireはH.264 YUV 4:4:4を使用し、クライアントで互換性のあるハードウェアが検出された場合、Thinwireは自動的にH.265 YUV 4:4:4ハードウェアデコードを使用します。

H.265 YUV 4:4:4 を使用すると、社内テストでは、H.264 4:4:4 と比較して1秒あたりのフレーム数 (FPS) が4倍増加し、H.265 の優れた効率性により、H.264 と比較してフレームあたりのサイズが2.5倍削減されることが示されています。

高解像度ディスプレイ

Citrix Virtual Apps and Desktops™ を使用して高解像度ディスプレイ（6K、8K、および同等のメガピクセル数）を展開するお客様は、パフォーマンスの問題や、マウストラッキングの不整合、ディスプレイのスケーリング、DPI関連の問題などを経験する可能性があります。

一般的なオフィスモニターの従来の解像度は4K、6K、または8Kであり、「K」表記は水平解像度を示します。

6Kディスプレイの例としては、Apple Pro Display XDR (解像度 6016 × 3384) と Dell UltraSharp U3224KB (解像度 6144 × 3456) があります。

現在、8Kモニターはごくわずかしか入手できませんが、その一例として、7680 x 4320 の解像度を持つ Dell UltraSharp UP3218K があります。

Barco は、モニターの解像度ではなく、MP またはメガピクセル数でリストしています。最新の Barco モニターは、6848 x 4560 の解像度を謳う 32MP モニターです。

Citrix® は、ハードウェアリソースに応じて最大8台のモニターをサポートします。使用するGPUによっては、この最大値に他のハードウェア制限がある場合があります。

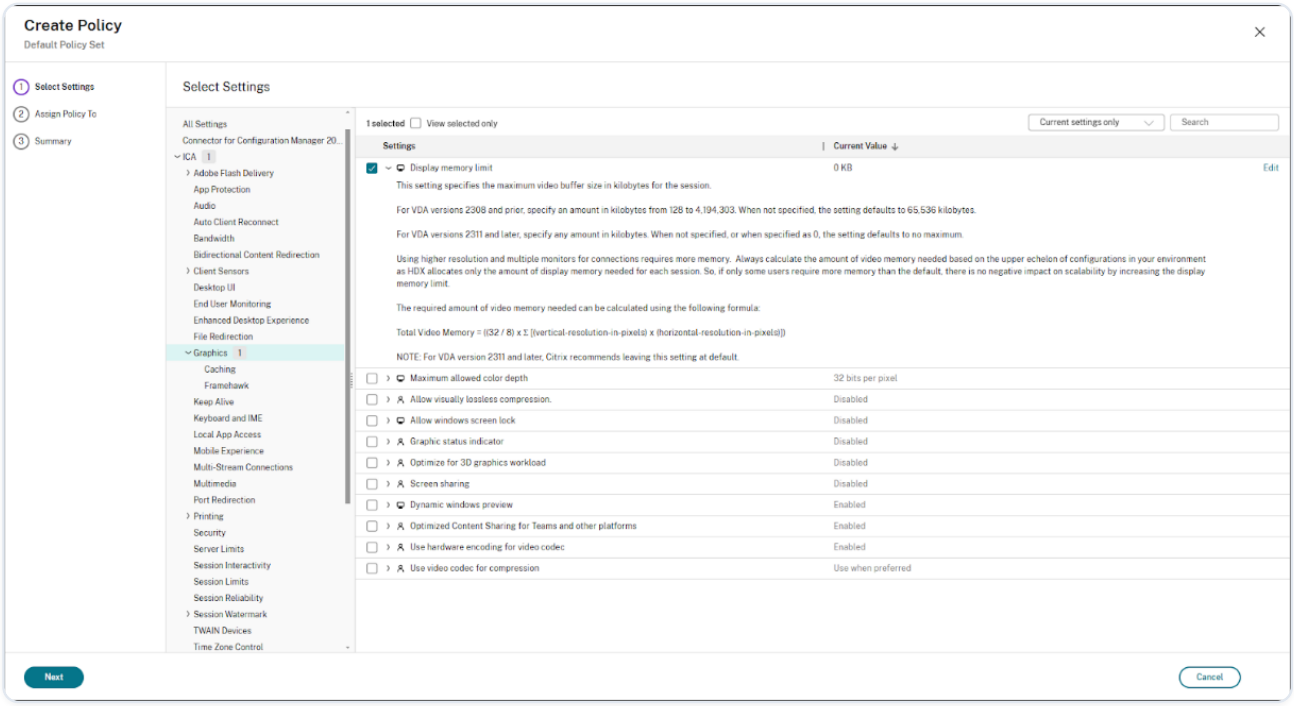
高解像度ディスプレイでのパフォーマンスを最適化し、潜在的な問題を軽減するために、CitrixはCVAD 2402の使用を推奨しています。

VDAバージョン2402以降

VDA 2402 以降の場合、「ディスプレイメモリ制限」ポリシーをデフォルトの 0 のままにします。これはディスプレイメモリ制限がないことを意味します。これにより、VDA は必要なディスプレイメモリを動的に割り当てることができます。

以前の VDA バージョン (2402 より前)

CVAD 2402以降へのアップグレードが不可能な場合は、「Display memory limit」ポリシーを最大値の4,194,303 KBに構成してください。これにより、VDAに利用可能な最大ディスプレイメモリが提供されます。



パフォーマンスとスケーラビリティに関する考慮事項

高解像度とモニターの数は、セッションパフォーマンスとサーバーのスケーラビリティに直接影響します。

高解像度化と複数のモニターの使用により、帯域幅の消費量が増加します。帯域幅の制約は、フレームレートを制限し、画質を低下させる可能性があり、その結果、セッションのインタラクティブ性とユーザーエクスペリエンスに影響を与えます。

エンドポイントデバイスは、目的のディスプレイ構成をサポートするために、十分なハードウェアリソースを利用できる必要があります。これは、十分なCPUリソース、場合によってはグラフィックワークロードを処理できるGPUが必要であることを意味する可能性があります。

グラフィックのロス許容モード

システム要件

- Citrix Virtual Delivery Agent (VDA) バージョン 2311 以降
- Windows向け Citrix Workspace™ アプリ 2311 以降。

> **注:**
>
> この機能が動作するためには、グラフィックポリシーの**HDX™ Adaptive Transport (EDT)とロス許容モード**の両方を有効にする必要があります。

重要な要件に関する考慮事項

帯域幅のしきい値

CVAD 2507以降のバージョンでは、グラフィックのロス許容モードをアクティブにするには、最低30 Mbpsの帯域幅が必要です。待機時間とパケット損失のしきい値が満たされていても、利用可能なセッション内帯域幅が30 Mbpsを下回る場合、この機能は有効になりません。この帯域幅のしきい値はハードコードされた値であり、構成することはできません。

構成

この機能は、Web StudioまたはグループポリシーCitrix®ポリシーによって管理されます。

グラフィックの損失許容モードは、デフォルトで有効になっています。

- ポリシー: グラフィックの損失許容モード
- デフォルト: 有効

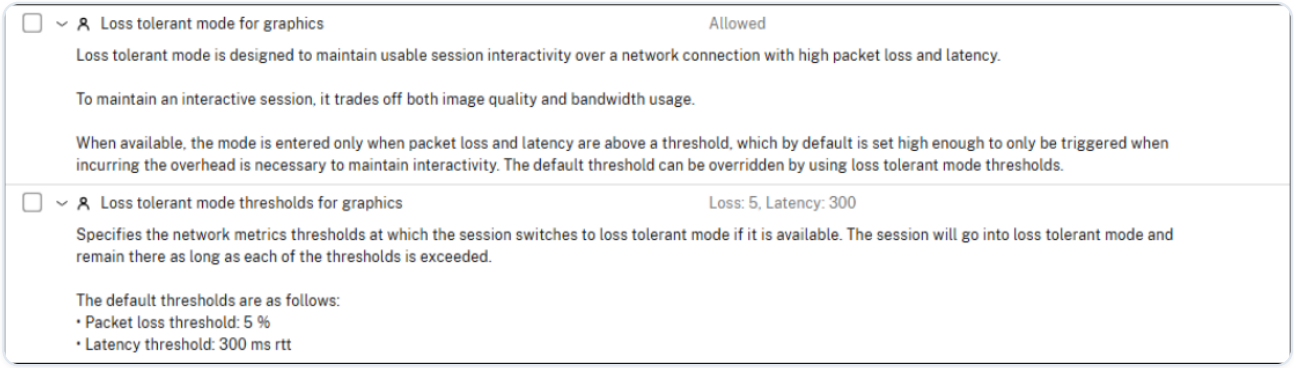
グラフィックの損失許容モード機能をオフにするには、このポリシーを**無効**に設定します。

グラフィックの損失許容モードのしきい値を構成するには:

- ポリシー: グラフィックの損失許容モードのしきい値
- デフォルト値:
    - パケット損失: 5%

- 遅延: 300 ms

このポリシーを使用すると、グラフィックの損失許容モードをトリガーするネットワーク状態のしきい値を調整できます。このモードは、パケット損失と遅延の両方の値が満たされるか超えられ、利用可能な帯域幅が30 Mbps以上である場合にアクティブになります。

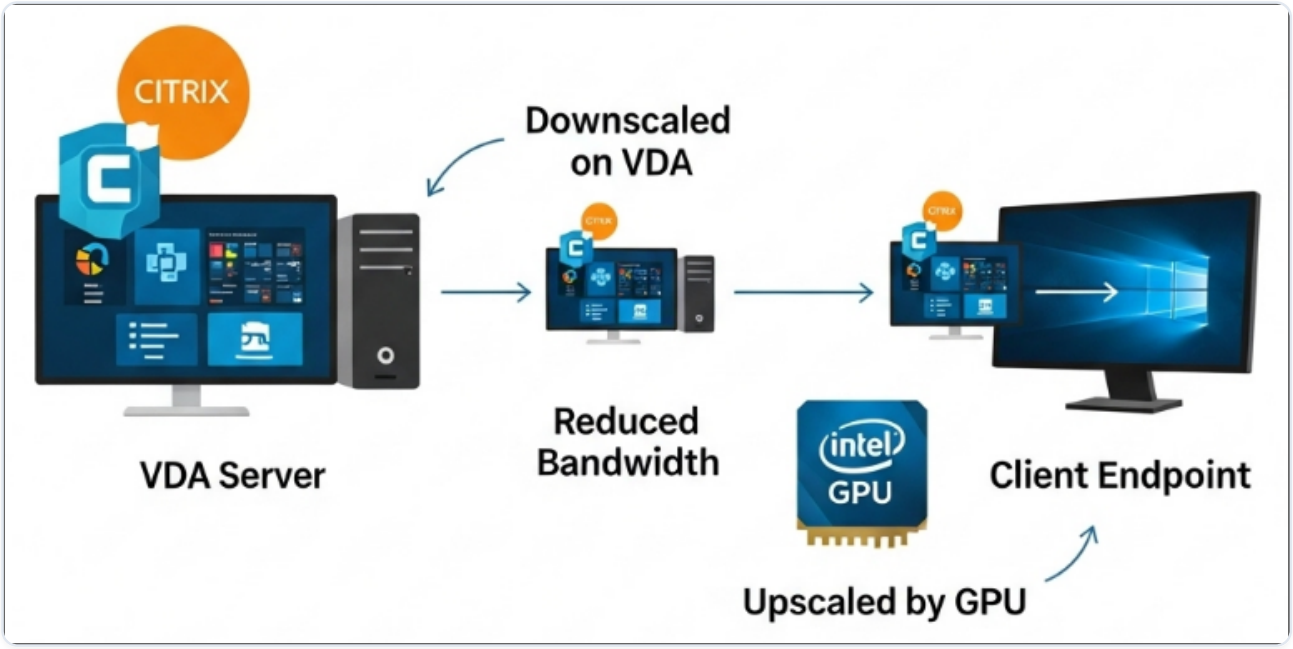


HDX™ グラフィックス スーパーレゾリューション アップスケーリング (プレビュー)

Intel GPU 向けの HDX グラフィックス超解像度アップスケーリング プレビューは、Citrix® と Intel の新しい共同開発です。

Citrix Virtual Apps and Desktops™ 2507 の新しいプレビュー機能である Citrix HDX グラフィックス スーパーレゾリューション アップスケーリングにより、セッションパフォーマンスを向上させ、帯域幅の消費を大幅に削減します。

Citrix HDX は、超解像度アップスケーリングのサポートを追加した最初のリモートプロトコルです。この業界初の技術適応は、Virtual Desktop Agent (VDA) 上のビデオ解像度に追加の圧縮をシームレスに適用し、互換性のあるエンドポイントのグラフィックス処理ユニット (GPU) を利用して、品質に目立った劣化やエンドポイントのパフォーマンスへの悪影響を与えることなく、元の解像度に戻します。



このテクノロジーは現在、このプレビューで一部の Intel エンドポイント GPU で利用可能です。詳細については、システム要件を参照してください。

動作の仕組み

グラフィックを多用するアプリケーションの配信は、特に高解像度や複数のディスプレイを使用する場合、本質的に大量の帯域幅を消費する可能性があります。

HDX™ グラフィックスの超解像度アップスケーリングを使用すると、混合ワークロードの帯域幅使用量を削減できます。

HDX グラフィックスの超解像度アップスケーリングでは、VDA はエンコード中にビデオ解像度に追加の圧縮を適用します。その後、クライアントは GPU を使用して、領域を元の解像度と品質に自動的にアップスケールします。このプロセスはエンドユーザーにとってシームレスであり、目立った品質の低下を引き起こしたり、エンドポイントのパフォーマンスに影響を与えたりすることはありません。

すべてのCitrix®ワークロードは、HDXグラフィックスの超解像度アップスケーリング技術の恩恵を受けます。この技術はサーバー側のGPUの有無に依存しないため、HDXグラフィックスの超解像度アップスケーリングは、高価なサーバー側のGPUを必要とせずに帯域幅の消費を削減できます。

サーバー側のGPUが利用可能な場合、HDXグラフィックスの超解像度アップスケーリングは、H.265やAV1などの新しいビデオコーデックと連携して動作できます。

ユースケース

例えば、高解像度のビデオコンテンツを伴う高解像度ワークロードや、統合グラフィックスを搭載した第10世代以降のIntel CPUを搭載したエンドポイントは、Citrix HDXグラフィックスの超解

像度アップスケーリング技術によるアップスケーリングのために統合GPUの機能を活用することで、帯域幅使用量の削減とユーザーエクスペリエンスの向上という恩恵を受けます。

システム要件

VDAの要件

- Windows VDA 2507以降
- Citrix HDX™グラフィックの超解像度アップスケーリングは、サーバー側GPUの有無に関わらず機能します。
- VDAに追加の要件はありません。

クライアント要件

- Windows 版 Citrix Workspace™ アプリ 2507 GA 以降

このプレビューでは、以下のクライアント側Intel GPUがサポートされています。

- Intel Arc Aシリーズグラフィックス
- Intel Iris Xe MAXグラフィックス
- Intel 第10世代 (Ice Lake世代以降)

Citrixは、最新のIntel GPUドライバーを使用することを推奨します。Intelドライバーのアップデートは、公式のIntelドライバーダウンロードページから直接入手できます。

ポリシー

HDXグラフィックの超解像度アップスケーリングは、デフォルトの選択的エンコーディングでの使用を目的として設計されています。

以下のポリシーが設定されていることを確認してください。

圧縮にビデオコーデックを使用する: **優先する場合にのみ使用** または **アクティブに変化する領域の場合** に設定します。

プレビューの場合、HDXグラフィックの超解像度テクノロジーはH.264ビデオエンコーディングと互換性があります。

有効にすると、H.265またはAV1互換のサーバー側GPUが利用可能な場合でも、H.264ビデオエンコーディングが強制されます。

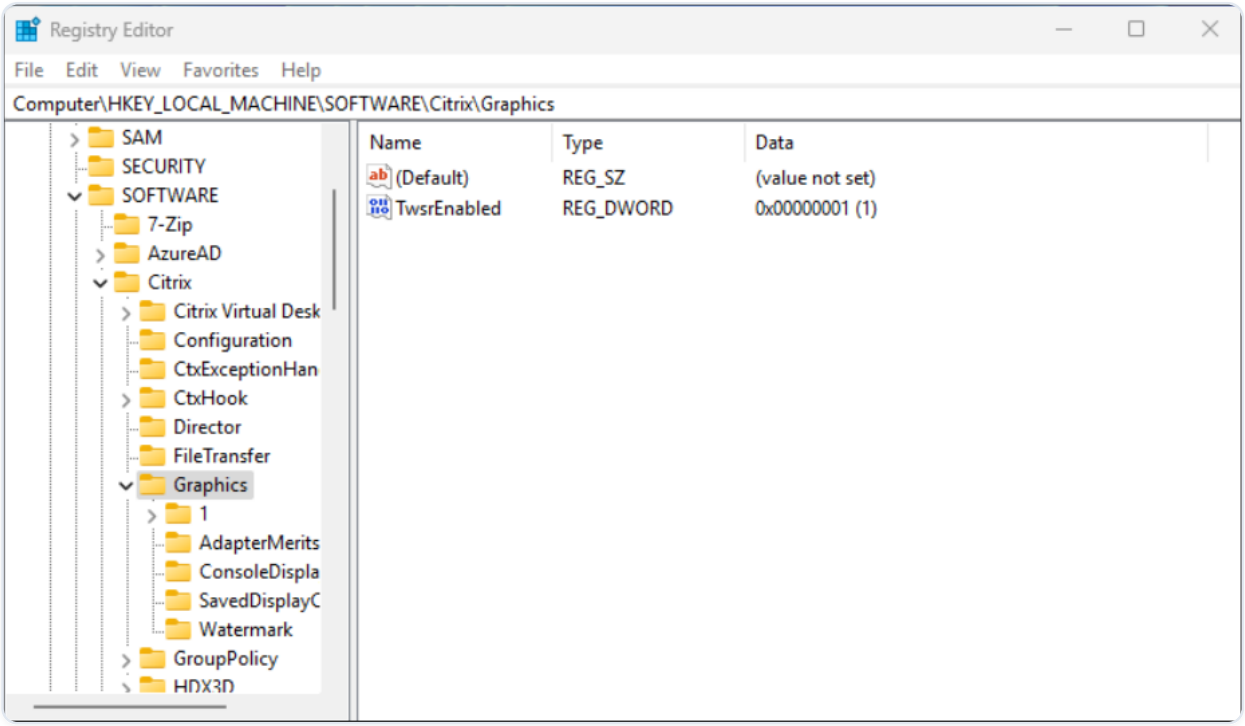
追加のポリシーを設定する必要はありません。

構成

VDAで有効にする

HDX™グラフィックスの超解像度アップスケーリングプレビューは、VDAで以下のレジストリエントリを作成することで有効にできます。

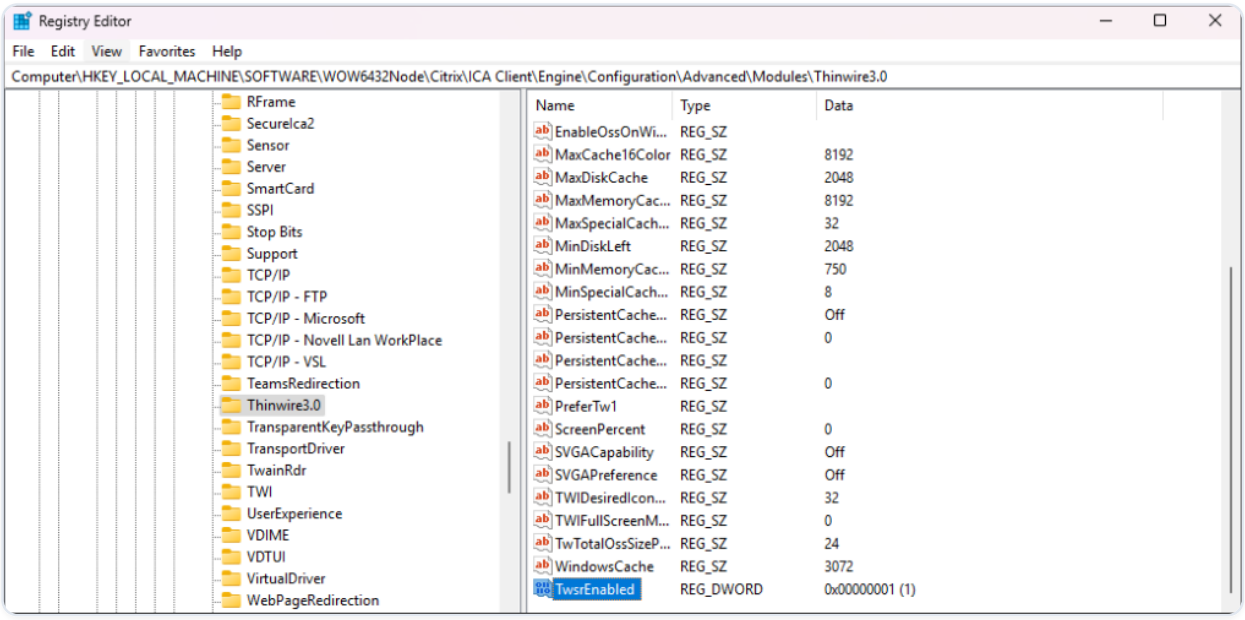
1. Windowsレジストリエディター (regedit.exe) を開きます。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\Graphics\` に移動します。
3. TwsrEnabledという名前のDWORD値を作成し、値を1に設定します。



クライアントで有効にする

クライアントでHDXグラフィックスの超解像度アップスケーリングプレビューを有効にするには、以下のレジストリエントリを作成する必要があります。

1. Windowsレジストリエディター (regedit.exe) を開きます。
2. `HKEY_LOCAL_MACHINE\Software\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Thinwire3.0\` に移動します。
3. TwsrEnabledという名前のDWORD値を作成し、値を1に設定します。



注:

この機能が動作するには、両方のレジストリキーが構成されており、クライアントデバイスがシステム要件を満たしている必要があります。

監視とトラブルシューティング

既知の問題

現在、HDX™ グラフィック超解像度アップスケーリングのプレビュー実装には既知の問題はありません。

重要な考慮事項

このプレビューでは、HDXグラフィック超解像度アップスケーリングは、一部のIntel GPUおよび統合グラフィックを搭載したCPUでのみ利用可能です。サポートされている構成のリストについては、システム要件を参照してください。

HDXグラフィック超解像度アップスケーリングはクライアントのCPUには影響しませんが、クライアントのGPUには影響を与えます。高フレームレートで大規模なビデオコンテンツ領域をアップスケーリングする場合、これはクライアント全体のパフォーマンスに影響を与える可能性があります。HDXグラフィック超解像度アップスケーリングを評価する際は、クライアントのパフォーマンスを監視してください。

制限事項

> **注:**
>
> Intel Lunar Lake CPUとセカンダリディスクリートGPUを搭載したエンドポイントなど、マルチGPUエンドポイントはプレビューではサポートされていません。
>
> さらに、Intel GPUは接続されているすべてのモニターを駆動する必要があります。

サポートされていないシナリオ

現在、HDXグラフィック超解像度アップスケーリングのプレビューでは、デフォルトのSelective Encodingのみがサポートされています。

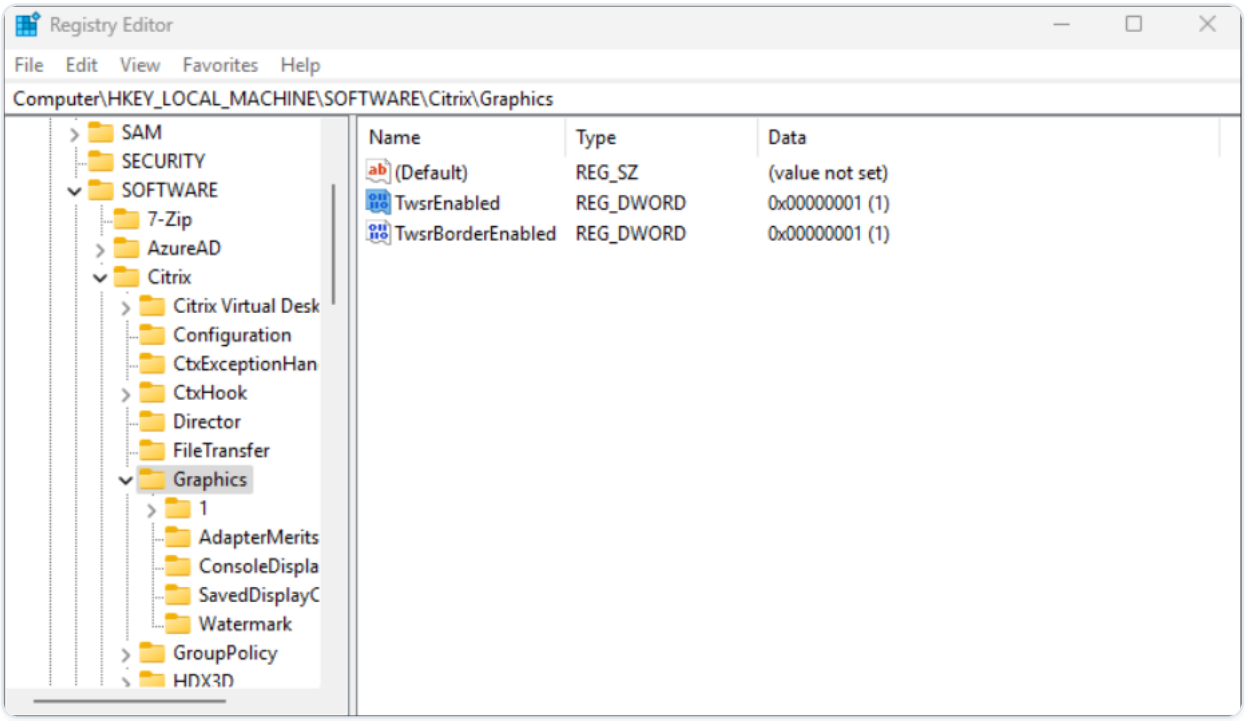
このプレビューでは、以下のシナリオはサポートされていません。

- ロスレスモードへのビルドはサポートされていません。
- 常時ロスレスモードはサポートされていません。
- 全画面エンコードはサポートされていません。 YUV 4:4:4での視覚的にロスレスはサポートされていません。

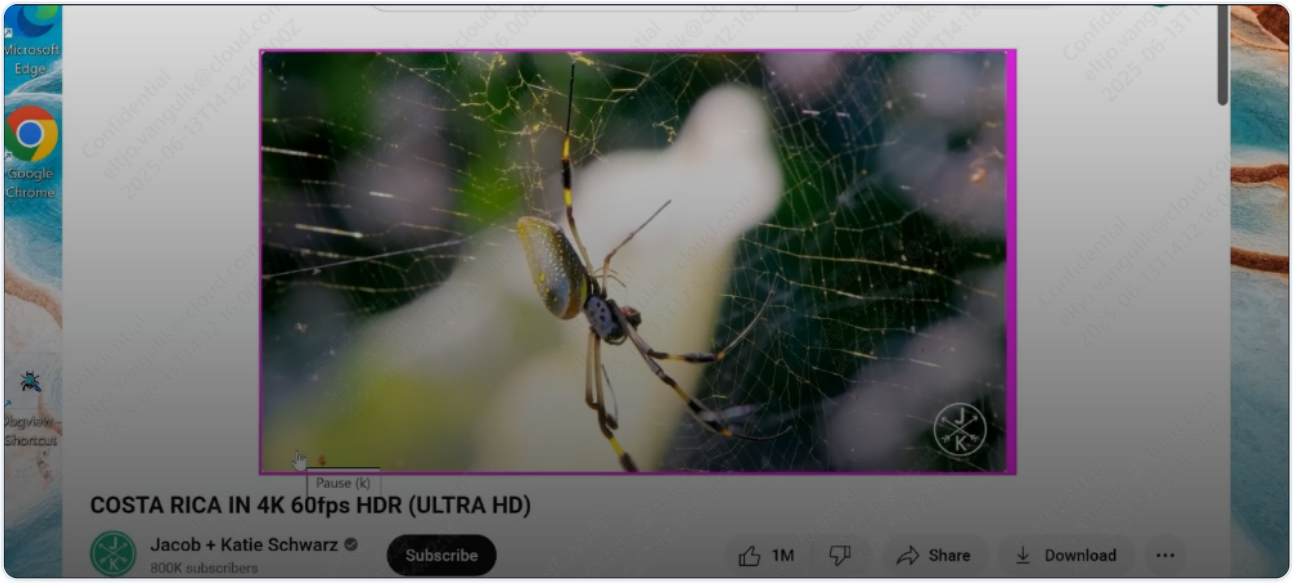
監視とトラブルシューティング

監視目的で、アップスケールされているビデオ領域の周囲に境界線を描画することで、画面のどの部分が現在アップスケールされているかを示す視覚的なインジケーターを有効にできます。視覚的なインジケーターを有効にするには、VDAで以下のレジストリ設定を有効にしてください。

1. VDAでWindowsレジストリエディター (regedit.exe) を開きます。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\Graphics\.`に移動します。
3. TwsrBorderEnabledという名前のDWORD値を作成し、値を1に設定します。



境界線を有効にすると、HDXグラフィックの超解像度アップスケーリングを使用してアクティブにアップスケールされている領域の周囲に紫色の境界線が表示されます。



全体的なクライアントパフォーマンスを監視するには、顧客はクライアントのタスクマネージャーにある**パフォーマンス**タブを利用できます。

シームレス

Citrix Published Applications は Citrix Virtual Apps and Desktops の主要な機能です。これにより、顧客は完全なデスクトップを必要とせずに、個々の Windows または Linux アプリケーションをユーザーに直接配信できます。

これにより、ユーザーはアプリケーションをローカルでインストールおよび管理する必要がなくなり、ワークフローが簡素化され、IT部門の負担が軽減されます。ユーザーは、完全なリモートデスクトップ環境と対話する代わりに、アプリケーションウィンドウと直接対話することで、シームレスで合理化されたエクスペリエンスを実現します。

シームレス(/en-us/citrix-virtual-apps-desktops/2511/media/seamless-1.png)

公開アプリケーション（シームレスアプリケーションとも呼ばれる）の背後にあるテクノロジーにより、アプリケーションはリモートサーバー上で実際に動作しているにもかかわらず、ユーザーのローカルデバイス上で直接実行されているかのようにユーザーに配信されます。これは、アプリケーションがホストされているWindows Serverデスクトップを隠し、アプリケーションをユーザーにシームレスに提示することで実現されます。

シームレスアプリケーションは、Windows VDA と Linux VDA の両方で利用できます。Windows VDA の場合、シームレスアプリケーションは、Microsoft Windows Server オペレーティングシステムを実行する TSVDA と、Microsoft Windows 10 または Windows 11 を実行する WSVDA の両方をサポートします。

シームレスアプリケーションには、次のような多くの利点があります。

- **ユーザーエクスペリエンスの向上:** ユーザーは、基盤となるオペレーティングシステムを気にすることなく、どのデバイスからでもアプリケーションにアクセスできます。
- **セキュリティの向上:** アプリケーションはリモートサーバー上で実行されるため、マルウェアやその他の脅威から保護するのに役立ちます。
- **ITコストの削減:** シームレスアプリケーションは、アプリケーションの管理と展開を簡素化することで、ITコストの削減に役立ちます。
- **一元管理:** アプリケーションは一元的に管理および更新できるため、IT管理が簡素化され、組織全体で一貫性が確保されます。これにより、パッチ、更新、および新しいアプリケーションの展開に必要な時間と労力が削減されます。

- **アプリケーションの互換性:** 標準化されたサーバー環境でアプリケーションを実行することで、異なるクライアントオペレーティングシステムやハードウェア構成から生じる可能性のある互換性の問題を軽減できます。
- **合理化されたアプリケーション配信:** Citrixは、HDX™のような高度なテクノロジーを活用して、公開デスクトップと公開アプリケーションの両方で、帯域幅が制限された接続でも、ユーザーにリッチでインタラクティブなエクスペリエンスを提供します。
- **異種アプリケーションのサポート:** 管理者は、LinuxアプリケーションをWindowsアプリケーションと並行して公開できるため、両方のプラットフォームからアプリケーションにシームレスにアクセスできます。

シームレスアプリケーションを公開する

> **注:**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

展開でデリバリーグループのみを使用している場合（アプリケーショングループは使用していない場合）、アプリケーションをデリバリーグループに追加します。アプリケーショングループも使用している場合は、通常、代わりにアプリケーションをアプリケーショングループに追加します。このガイダンスにより、管理が容易になります。アプリケーションは常に、少なくとも1つのデリバリーグループまたはアプリケーショングループに属している必要があります。

アプリケーションの追加ウィザードでは、1つ以上のデリバリーグループ、または1つ以上のアプリケーショングループを選択できますが、両方を同時に選択することはできません。後でアプリケーションのグループ関連付けを変更することはできますが（たとえば、アプリケーションをアプリケーショングループからデリバリーグループに移動するなど）、ベストプラクティスとしては、そのような複雑さを追加することは推奨されません。アプリケーションは1種類のグループに保持してください。

アプリケーションを複数のグループに関連付けると、それらのすべてのグループでアプリケーションを表示するための十分な権限がない場合、可視性の問題が発生する可能性があります。そのよ

うな場合は、より高い権限を持つ管理者に相談するか、アプリケーションが関連付けられているすべてのグループを含むようにスコープを拡張してください。

同じ名前のアプリケーションを2つ（異なるグループからであっても）同じユーザーに公開する場合、Web Studioで`Application name (for user)`プロパティを変更してください。そうしないと、ユーザーはCitrix Workspace™アプリで重複した名前を目にすることになります。

アプリケーションのプロパティ（設定）は、追加時または後で変更できます。アプリケーションが配置されているアプリケーションフォルダーも、アプリケーションの追加時または後で変更できます。

詳細については、以下を参照してください。

- 「デリバリーグループの作成」(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/delivery-groups-create.html)
- アプリケーショングループの作成
- タグ

アプリケーションの追加

アプリケーションは、デリバリーグループまたはアプリケーショングループを作成する際に追加できます。これらの手順については、デリバリーグループの作成およびアプリケーショングループの作成で詳しく説明されています。以下の手順では、グループ作成後にアプリケーションを追加する方法について説明します。

知っておくと良いこと：

- Remote PC Accessデリバリーグループにアプリケーションを追加することはできません。
- アプリケーションの追加ウィザードを使用して、デリバリーグループまたはアプリケーショングループからアプリケーションを削除することはできません。これは別の操作です。

1つ以上のアプリケーションを追加するには：

1. 左ペインで**アプリケーション**を選択し、アクションバーで**アプリケーションの追加**を選択します。
2. アプリケーションの追加ウィザードが**はじめに**ページとともに起動します。このページは、今後のウィザード起動時に表示しないように設定できます。
3. ウィザードは、**グループ**、**アプリケーション**、および**概要**の各ページを案内します。各ページの作業が完了したら、**次へ**をクリックして**概要**ページに進みます。

単一のデリバリーグループまたはアプリケーショングループにアプリケーションを追加する場合の、手順1の代替方法：

- **1つのデリバリーグループにのみアプリケーションを追加する場合：** 手順1で、Web Studioの左ペインで**デリバリーグループ**を選択し、中央ペインでデリバリーグループを選択してから、アクションバーで**アプリケーションの追加**を選択します。ウィザードには**グループ**ページが表示されません。
- **1つのアプリケーショングループにのみアプリケーションを追加する場合：** 手順1で、Web Studioの左ペインで**アプリケーション**を選択し、中央ペインでアプリケーショングループを選択してから、アクションバーのアプリケーショングループ名の下にある**アプリケーションの追加**エントリを選択します。ウィザードには**グループ**ページが表示されません。

グループページ

このページには、サイト内のすべてのデリバリーグループが一覧表示されます。アプリケーショングループも作成している場合は、アプリケーショングループとデリバリーグループが一覧表示されます。どちらかのグループを選択できますが、両方のグループを同時に選択することはできません。つまり、アプリケーショングループとデリバリーグループに同時にアプリケーションを追加することはできません。通常、アプリケーショングループを使用している場合は、デリバリーグループではなくアプリケーショングループにアプリケーションを追加します。

アプリケーションを追加するときは、少なくとも1つのデリバリーグループ（または、利用可能な場合はアプリケーショングループ）の横にあるチェックボックスをオンにします。すべてのアプリケーションは、常に少なくとも1つのグループに関連付けられている必要があります。

アプリケーションページ

アプリケーションソースを表示するには、**追加**をクリックします。

- **スタートメニューから:** 選択したデリバリーグループ内のマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスを選択し、**OK**をクリックします。

  このソースは、(1)関連付けられたデリバリーグループがないアプリケーショングループを選択した場合、(2)関連付けられたデリバリーグループにマシンが含まれていないアプリケーショングループを選択した場合、または(3)マシンが含まれていないデリバリーグループを選択した場合は、選択できません。

- **手動：** デリバリーグループ内のVDAまたはネットワーク上の別の場所にあるアプリケーション。このソースを選択すると、新しいページが開き、次の方法で追加するアプリケーションを指定できます。
  - 実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、および管理者とユーザーの表示名を入力します。
  - デリバリーグループ内のVDAからアプリケーションを選択します。これを行うには、**参照**をクリックし、VDAにアクセスするための資格情報を入力し、VDAへの接続を待ってから、VDAからアプリケーションを選択します。選択したアプリケーションのプロパティが、ページのフィールドに自動的に入力されます。
- **既存:** 以前にサイトに追加されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスを選択し、**OK**をクリックします。

  サイトにアプリケーションがない場合、このソースは選択できません。
- **アプリケーションパッケージ:** App-V、MSIX、MSIX app attach、またはFlexAppアプリケーションパッケージ内のアプリケーション。このソースを選択すると、**パッケージからアプリケーションを追加**ページが起動します。アプリケーションパッケージのソースを選択し、表示されたリストから追加したいアプリケーションを選択し、**OK**を選択します。詳細については、「アプリパッケージの展開と配信」を参照してください。
- **アプリケーショングループ:** アプリケーショングループ。このソースを選択すると、アプリケーショングループのリストが表示された新しいページが起動します。（表示には各グループ内のアプリケーションもリストされますが、個々のアプリケーションではなくグループのみを選択できます。）選択したグループ内の現在および将来のすべてのアプリケーションが追加されます。追加するアプリケーショングループのチェックボックスを選択し、**OK**をクリックします。

  このソースは、(1) アプリケーショングループがない場合、または (2) 選択したデリバリーグループがアプリケーショングループをサポートしていない場合（たとえば、静的に割り当てられたマシンを持つデリバリーグループ）には選択できません。

表に示されているように、**追加**リストの一部のソースは、そのタイプの有効なソースがない場合、選択できません。互換性のないソース（たとえば、アプリケーショングループにアプリケーショングループを追加できないなど）はリストに含まれません。選択したグループに既に追加されているアプリケーションは選択できません。

このページまたは後で、アプリケーションのプロパティ（設定）を変更できます。

デフォルトでは、追加されたアプリケーションは`Applications`という名前のアプリケーションフォルダーに配置されます。このページまたは後で、アプリケーションを変更できます。同じ名前のアプリケーションが同じフォルダーに存在する場合にアプリケーションを追加しようとすると、追加するアプリケーションの名前を変更するよう求められます。提示された新しい名前を受け入れるか、拒否してアプリケーションの名前を変更するか、別のフォルダーを選択できます。たとえば、「**アプリケーション**」フォルダーに`app`が既に存在し、そのフォルダーに`app`という名前の別のアプリケーションを追加しようとすると、新しい名前`app_1`が提示されます。

概要ページ

10個以下のアプリケーションを追加する場合、それらの名前は**追加するアプリケーション**にリストされます。10個を超えるアプリケーションを追加する場合、合計数が指定されます。

概要情報を確認し、**「完了」**をクリックします。

アプリケーションのグループ関連付けを変更する

アプリケーションを追加した後、そのアプリケーションが関連付けられているデリバリーグループとアプリケーショングループを変更できます。

アプリケーションを別のグループにドラッグできます。これは、アクションバーのコマンドを使用する代替手段です。

アプリケーションが複数のデリバリーグループに関連付けられている場合（アプリケーショングループを使用するか直接関連付けるかに関わらず）、グループの優先順位を使用して、複数のグループが評価される順序を指定できます。グループは、アクセスポリシー、ユーザーリスト、スマートアクセスタグなどの要因に基づいて考慮対象から除外でき、グループから選択される特定のマシンは、ゾーン設定、起動準備、タグ制限などの要因によって影響を受ける可能性があります。デフォルトでは、すべてのグループの優先順位は0（最高）です。デリバリーグループの優先順位が同じ場合、最も負荷の低いデリバリーグループがアプリケーションの起動に選択されます。この場合、垂直ロードバランシングは考慮されません。

アプリケーションは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。また、共有マシンを含むデリバリーグループでデスクトップのみを配信する場合、(1)デリバリーグループに共有マシンが含まれており、XenDesktop 7.xバージョン7.9より前に作成された場合、および(2)`Edit delivery group`権限がある場合にも選択できます。プロパティダイアログがコミットされると、デリバリーグループの種類は自動的に`desktops and applications`に変換されます。

1. Web Studioにサインインし、左ペインで**「アプリケーション」**を選択してから、アプリケーションを選択します。

2. アクションバーで**「プロパティ」**を選択します。
3. **「グループ」**ページを選択します。

    - グループを追加するには、**「追加」をクリックし、「アプリケーショングループ」または「デリバリーグループ」を選択します。（アプリケーショングループを作成していない場合、唯一の項目は**「デリバリーグループ」**です。）次に、1つ以上の利用可能なグループを選択します。アプリケーションと互換性のないグループ、またはすでにアプリケーションに関連付けられているグループは選択できません。
    - グループを削除するには、1つ以上のグループを選択し、**「削除」**をクリックします。グループの関連付けを削除した結果、アプリケーションがどのグループとも関連付けられなくなる場合、アプリケーションが削除されることを警告されます。
    - グループの優先度を変更するには、グループを選択し、**「優先度の編集」をクリックします。優先度値を選択し、**「OK」**をクリックします。

4. 完了したら、**「適用」をクリックして変更を適用し、ウィンドウを開いたままにするか、**「OK」**をクリックして変更を適用し、ウィンドウを閉じます。

アプリケーションの複製、有効化または無効化、名前変更、または削除

次のアクションが利用可能です。

- **複製:** 異なるパラメーターやプロパティを持つ別のバージョンを作成するために、アプリケーションを複製したい場合があります。アプリケーションを複製すると、一意のサフィックスが自動的に付加されて名前が変更され、元のアプリケーションの隣に配置されます。また、アプリケーションを複製してから、別のグループに追加したい場合もあります。(複製後、アプリケーションを移動する最も簡単な方法はドラッグすることです。)
- **有効化または無効化:** アプリケーションの有効化と無効化は、デリバリーグループまたはアプリケーショングループの有効化と無効化とは異なるアクションです。
- **名前の変更:** 一度に1つのアプリケーションのみ名前を変更できます。アプリケーションの名前を変更しようとして、同じ名前のアプリケーションが同じフォルダーまたはグループに存在する場合、別の名前を指定するように求められます。
- **削除:** アプリケーションを削除すると、そのアプリケーションが関連付けられていたデリバリーグループおよびアプリケーショングループから削除されますが、元々アプリケーションを追加するために使用されたソースからは削除されません。アプリケーションの削除は、デリバリーグループまたはアプリケーショングループから削除するアクションとは異なります。

アプリケーションを複製、有効化、無効化、名前変更、または削除するには：

1. 左ペインで**アプリケーション**を選択します。

2. 中央ペインで1つまたは複数のアプリケーションを選択し、アクションバーで適切なタスクを選択します。
3. プロンプトが表示されたら、アクションを確認します。

デリバリーグループからアプリケーションを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに関連付けられている（属している）必要があります。アプリケーションをデリバリーグループから削除しようとして、そのアプリケーションがどのデリバリーグループまたはアプリケーショングループとの関連付けも失われる場合、続行するとアプリケーションが削除されることが通知されます。その場合、そのアプリケーションを配信したい場合は、有効なソースから再度追加する必要があります。

1. 左ペインで**デリバリーグループ**を選択します。
2. デリバリーグループを選択します。中央下ペインの**アプリケーション**タブで、削除するアプリケーションを選択します。
3. アクションバーから**アプリケーションの削除**を選択します。
4. 削除を確認します。

アプリケーショングループからアプリケーションを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに属している必要があります。アプリケーションをアプリケーショングループから削除しようとして、その結果、そのアプリケーションがどのグループにも属さなくなる場合、続行するとアプリケーションが削除されることが通知されます。そのような場合、そのアプリケーションを配信したい場合は、有効なソースから再度追加する必要があります。

1. 左ペインで「**アプリケーション**」を選択します。
2. 中央ペインでアプリケーショングループを選択し、1つ以上のアプリケーションを選択します。
3. アクションバーで「**アプリケーショングループから削除**」を選択します。
4. 削除を確定します。

アプリケーションのプロパティを変更する

アプリケーションのプロパティは、一度に1つしか変更できません。

アプリケーションのプロパティを変更するには：

1. 左ペインで「**アプリケーション**」を選択します。
2. アプリケーションを選択し、アクションバーで「**アプリケーションプロパティの編集**」を選択します。
3. 変更したいプロパティを含むページを選択します。
4. 完了したら、「**適用**」をクリックして行った変更を適用しウィンドウを開いたままにするか、「**OK**」をクリックして変更を適用しウィンドウを閉じます。

以下の一覧では、ページが括弧内に示されています。

プロパティ	ページ
Citrix Workspaceアプリにアプリケーションが表示されるカテゴリまたはフォルダー	配信
コマンドライン引数。公開アプリケーションにパラメーターを渡すを参照	場所
アプリケーションが利用可能なデリバリーグループおよびアプリケーショングループ	グループ
説明	識別
ファイル名拡張子とファイルの種類関連付け: アプリケーションが自動的に開く拡張子	ファイルの種類関連付け
アイコン	配信
StoreFront™のキーワード	識別
制限。アプリケーション制限の構成を参照	配信
名前: ユーザーおよび管理者が参照する名前	識別
実行可能ファイルへのパス。「公開アプリケーションへのパラメーターの受け渡し」を参照してください(#pass-parameters-to-published-applications)	場所
ユーザーのデスクトップ上のショートカット: 有効または無効	配信

プロパティ	ページ
可視性: Citrix Workspaceアプリでアプリケーションを表示できるユーザーを制限します。非表示のアプリケーションでも起動できます。利用不可かつ非表示にするには、別のグループに追加します。	可視性の制限
作業ディレクトリ	場所

アプリケーションの変更は、現在のアプリケーションユーザーがセッションからログオフするまで有効にならない場合があります。

アプリケーション制限を構成する

アプリケーションの使用状況を管理するために、アプリケーション制限を構成します。たとえば、アプリケーション制限を使用して、アプリケーションに同時にアクセスするユーザーの数を管理できます。同様に、アプリケーション制限は、リソースを大量に消費するアプリケーションの同時インスタンスの数を管理するためにも使用できます。この制限は、サーバーのパフォーマンスを維持し、サービスの劣化を防ぐのに役立ちます。

この機能は、Controller によって仲介されるアプリケーションの起動数（Citrix Workspace アプリや StoreFront からの起動など）を制限するものであり、他の方法で起動できる実行中のアプリケーションの数を制限するものではありません。これは、アプリケーション制限が同時使用を管理する際に管理者を支援するものの、すべてのシナリオで強制力を持つわけではないことを意味します。たとえば、Controller が停止モードの場合、アプリケーション制限は適用できません。

デフォルトでは、同時に実行できるアプリケーションインスタンスの数に制限はありません。アプリケーション制限の設定はいくつかあります。それらのいずれか、またはすべてを構成できます。

- デリバリーグループ内のすべてのユーザーによるアプリケーションの同時インスタンスの最大数。
- デリバリーグループ内のユーザーごとのアプリケーションのインスタンス数（1つ）。
- マシンごとのアプリケーションの同時インスタンスの最大数（PowerShell のみ）。

制限が構成されている場合、ユーザーが構成された制限を超えるアプリケーションインスタンスを起動しようとすると、エラーメッセージが生成されます。複数の制限が構成されている場合、最初に到達した制限でエラーが報告されます。

アプリケーション制限の使用例：

- **同時インスタンス数の最大制限:** デリバリーグループで、アプリケーション `Alpha` の同時インスタンスの最大数を15に構成します。その後、そのデリバリーグループのユーザーは、そのアプリケーションの15個のインスタンスを同時に実行します。そのデリバリーグループのいずれかのユーザーが `Alpha` を起動しようとすると、エラーメッセージが生成されます。構成された同時アプリケーションインスタンス制限（15）を超えるため、`Alpha` は起動されません。
- **ユーザーごとのインスタンス数制限:** 別のデリバリーグループで、アプリケーション `Beta` のユーザーごとのインスタンス数オプションを有効にします。ユーザーのTonyはアプリケーション `Beta` を正常に起動します。その日の後半、そのアプリケーションがTonyのセッションでまだ実行されている間に、彼は `Beta` の別のインスタンスを起動しようとします。ユーザーごとのインスタンス数制限を超えるため、エラーメッセージが生成され、`Beta` は起動されません。
- **同時インスタンス数の最大制限とユーザーごとのインスタンス数制限:** 別のデリバリーグループで、同時インスタンスの最大数を10に構成し、アプリケーション `Delta` のユーザーごとのインスタンス数オプションを有効にします。その後、そのデリバリーグループの10人のユーザーがそれぞれ `Delta` のインスタンスを実行している場合、そのデリバリーグループの他のユーザーが `Delta` を起動しようとすると、エラーメッセージが表示されます。`Delta` は起動されません。現在の10人の `Delta` ユーザーのいずれかがそのアプリケーションの2番目のインスタンスを起動しようとすると、エラーメッセージが表示され、2番目のインスタンスは起動されません。
- **マシンごとの同時インスタンス数の最大制限とタグ制限の使用:** アプリケーション `Charlie` には、特定のサーバーで同時に実行できるインスタンスの数を決定するライセンスおよびパフォーマンス要件があります。これらの要件は、サイト内のすべてのサーバーで同時に実行できるインスタンスの数も決定します。

  アプリケーションのインスタンス数/マシン制限は、サイト内の任意のサーバーに影響します（特定のデリバリーグループ内のマシンだけでなく）。サイトに3台のサーバーがあるとします。アプリケーション `Charlie` の場合、マシンごとのアプリインスタンス制限を2に構成します。したがって、サイト全体でアプリケーション `Charlie` のインスタンスは6つまでしか起動できません。（これは、3台の各サーバーでCharlieのインスタンスが2つという制限です。）

  アプリケーションの使用をデリバリーグループ内の特定のコンピューターのみに制限するには（サイト全体のすべてのコンピューターでのインスタンス制限に加えて）：

  - これらのマシンにタグ付け機能を使用します。
  - そのアプリケーションのマシンごとのインスタンス数の最大制限を構成します。

アプリケーションがControllerの仲介以外の方法（たとえば、Controllerが停止モードの場合など）で起動され、構成された制限を超過した場合、ユーザーは制限を超過しないように十分な数のインスタンスを閉じるまで、それ以上のインスタンスを起動できません。制限を超過したインスタンスは強制的にシャットダウンされません。ユーザーが閉じるまで継続して実行が許可されます。

セッションローミングを無効にする場合は、ユーザーごとのアプリケーション制限（1インスタンス）を無効にします。ユーザーごとのアプリケーション制限（1インスタンス）を有効にする場合は、新しいデバイスで新しいセッションを許可する2つの値のいずれも構成しないでください。ローミングについて詳しくは、「セッション」を参照してください。

デリバリーグループごとの最大インスタンス数制限と、ユーザーごとの1インスタンス制限を構成するには：

1. 左ペインで**「アプリケーション」**を選択し、アプリケーションを選択します。
2. アクションバーで**「アプリケーションプロパティの編集」**を選択します。
3. **「配信」**ページで、次のいずれかのオプションを選択します。
   - **アプリケーションの無制限の使用を許可する**。同時に実行できるインスタンスの数に制限はありません。これがデフォルトです。
   - **アプリケーションの制限を設定する**。制限の種類は2つあります。いずれかまたは両方を指定します。
     - マシンごとに同時に実行できるインスタンスの最大数を指定します
     - ユーザーごとにアプリケーションのインスタンスを1つに制限する
4. **「OK」をクリックして変更を適用しダイアログボックスを閉じるか、**「適用」**をクリックして変更を適用しダイアログボックスを開いたままにします。

マシンごとの最大インスタンス数制限を構成するには（PowerShellのみ）：

- PowerShellで（Citrix Cloud™展開の場合はRemote PowerShell SDKを、オンプレミス展開の場合はPowerShell SDKを使用して）、適切な `BrokerApplication` コマンドレットを `MaxPerMachineInstances` パラメーターとともに指定します。
- ガイダンスについては、`Get-Help` コマンドレットを使用してください。例:

```
Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
```

公開アプリケーションにパラメーターを渡す

アプリケーションのプロパティの**場所**ページを使用して、コマンドラインを入力し、公開アプリケーションにパラメーターを渡します。

公開アプリケーションをファイルの種類に関連付けると、`"%*"` (二重引用符で囲まれたパーセント記号とアスタリスク記号) がアプリケーションのコマンドラインの末尾に追加されます。これらの記号は、ユーザーデバイスに渡されるパラメーターのプレースホルダーとして機能します。

公開アプリケーションが期待どおりに起動しない場合は、そのコマンドラインに正しい記号が含まれていることを確認してください。デフォルトでは、`"%*"` 記号が追加されると、ユーザーデバイスから提供されるパラメーターが検証されます。ユーザーデバイスから提供されるカスタマイズされたパラメーターを使用する公開アプリケーションの場合、コマンドライン検証をバイパスするために、`"%**"` 記号がコマンドラインに追加されます。アプリケーションのコマンドラインにこれらの記号が表示されない場合は、手動で追加してください。

実行可能ファイルへのパスにスペースを含むディレクトリ名 (`"C:\Program Files"` など) が含まれている場合は、そのスペースがコマンドラインの一部であることを示すために、アプリケーションのコマンドラインを二重引用符で囲みます。これを行うには、パスを二重引用符で囲み、さらに`%*` 記号を別の二重引用符で囲みます。パスの閉じ引用符と`%*` 記号の開き引用符の間にスペースを含めるようにしてください。

たとえば、公開アプリケーションであるWindows Media Playerのコマンドラインは次のとおりです。

```
"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"
```

> **注:**
>
> 公開アプリケーションを起動するためのコマンドラインの最大文字数 (引数を含む) は203です。

公開アプリケーションでのセッションサインアウトの問題のトラブルシューティング

アプリケーションを公開する場合、公開アプリケーションのメインの実行可能ファイルのみが指定されます。しかし、一部のアプリケーションは、バックグラウンドで実行され、メインの公開アプリケーションが閉じられたときに、対応するメインの実行可能ファイルによって閉じられない追加の (子) プロセスを生成する場合があります。追加のプロセスは、実行されるスクリプトや、`Run` や `RunOnceKey` のような特定のレジストリキーからも作成される可能性があります。これらのアプリケーションは、正常なサインアウトを妨げ、セッションが残存したりハングしたりする原因となり、セッションが閉じられず、ユーザーがサインアウトされない結果となる可能性があります。

この場合、Citrix Director を使用してこれらのセッションをリセットまたは終了する必要があります。

セッションが適切にサインアウトされない問題を特定し、トラブルシューティングするために、Citrix は3つのレジストリエントリを提供しています。これらの問題によりセッションが適切にログオフされないことの特定とトラブルシューティングは、次の3段階のプロセスです。

1. どのセッションが公開アプリケーションによって正常なサインアウトを妨げているかを特定する
2. それらの公開アプリケーションが追加の (子) プロセスを生成するかどうかを特定する
3. これらのプロセスを指定されたレジストリエントリに追加して、サインアウトを妨げないようにする

ステップ2：公開アプリケーションが追加の（子）プロセスを生成するかどうかを特定する

公開アプリケーションが正常なサインアウトを妨げていると特定されたら、次のステップは、このアプリケーションの実行中に追加のプロセスが生成されるかどうかを判断することです。

公開アプリケーションが閉じられたときに、正常なサインアウトをブロックしているプロセスがあるかどうかを判断するには、`HKCU\Software\CitrixVolatile\Seamless\Sessions\[ID]\LogoffCheckerBlockingProcess` を参照してください。

以下の例では、キー `LogoffCheckerBlockingProcess` に次のエントリが含まれています。

```
PhoneExperienceHost.exe

SkypeApp.exe

SkypeBackgroundHost.exe
```

これらのプロセスが正常なサインアウトを妨げていました。

注:

確認したいセッションの正しいセッションIDで を置き換えてください。

ステップ3：これらのプロセスを指定されたレジストリエントリに追加して、サインアウトを妨げないようにする

これらのプロセスを以下のレジストリキーに追加することで、今後のセッションでサインアウトが妨げられるのを防ぐことができます。

```
Add the process file name to the following registry key:

Caution! Refer to the Disclaimer at the end of this article before using the Registry Editor.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

Value Name:LogoffCheckSysModules

Type:REG_SZ

String:MyAppName.exe
```

`LogoffCheckSysModules` の詳細については、公開アプリケーションからの正常なログオフによりセッションがアクティブ状態になる を参照してください。

ステップバイステップのトラブルシューティングガイド

1. テスト対象のVDAでリモートレジストリサービスを開始します。
   a. コントロールパネルで、**管理ツール > サービス** を選択します。
   b. **リモートレジストリサービス** を右クリックし、**プロパティ** を選択します。
   c. **スタートアップの種類** で、ドロップダウンメニューから **自動** を選択します。

   公開アプリケーションのレジストリ(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-registry.png)
2. テスト対象のVDAでWindowsファイアウォールをオフにするか、ポート455を有効にする受信ファイアウォール規則を作成します。
   a. コントロールパネルで、**Windows Defender ファイアウォール > 詳細設定**を選択します。
   b. **受信の規則**を右クリックし、**新しい規則**を選択します。
   c. **新しい受信の規則ウィザード**で、**ポート**を選択します。
   d. **プロトコルおよびポート**ページで、**TCP および特定のローカルポート**を選択します。ローカルポートとして `445` を入力します。

e. **操作**ページで、**接続を許可する**を選択します。

f. 新しい受信規則を適用するファイアウォールプロファイルを選択します。

g. ファイアウォール規則に名前を付け、**完了**を選択して**新しい受信の規則ウィザード**を終了します。

公開アプリケーションのファイアウォールポート(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-firewall-port.png)

3. 同じドメイン上の別のVM（DC、DDC、または別のVDAでも可）から、`Regedit` を実行し、リモートレジストリに接続します。

   公開アプリケーションのレジストリエディター(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-registry-editor.png)

4. テスト対象のVDAのIPアドレスを入力し、**OK**をクリックします。`regedit` ツリーには、テスト対象のVDAのブランチが表示されるはずです。

   公開アプリケーションのregedit(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-regedit.png)

5. **コマンドプロンプト**公開アプリケーションを開きます。

   公開アプリの管理(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-manage.png)

   Citrix Workspace に **コマンドプロンプト** アプリが表示されます。

   公開アプリのコマンドプロンプト(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-cmd-prompt.png)

6. クライアントで**接続センター**を開きます。これは、開いているシームレスアプリを閉じた後にセッションがサインアウトされたときに監視するために使用されます。以下の画像で、コマンドプロンプトプロセス`c:\Windows\system32\cmd.exe`がリモートVDIでアクティブになっていることがわかります。

   公開アプリの接続(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-citrix-workspace-connection-center.png)

7. **regedit**が実行されているVDAから、次のリモートIPロケーションに移動します。
   `HKEY_USERS\S-1-X-XX-XXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXX\SOFTWARE\CitrixVolatile\Seamless\Sessions\X\`

   > **注:**

> 新しいセッションを開くたびにこのパスは変更されます。

8. ここで読み取るキーは 2 つあります (ここでは変更しないでください)。**LogoffCheckBlockingProcess** と **LogoffCheckerBlockingVisibleProcess** です。これらのキーは、サインアウトをブロックしているプログラムを表示します。最初のキーには、それが開いていてまだ閉じられていないため、`C:\Windows\System32\cmd.exe` が表示されているはずです。

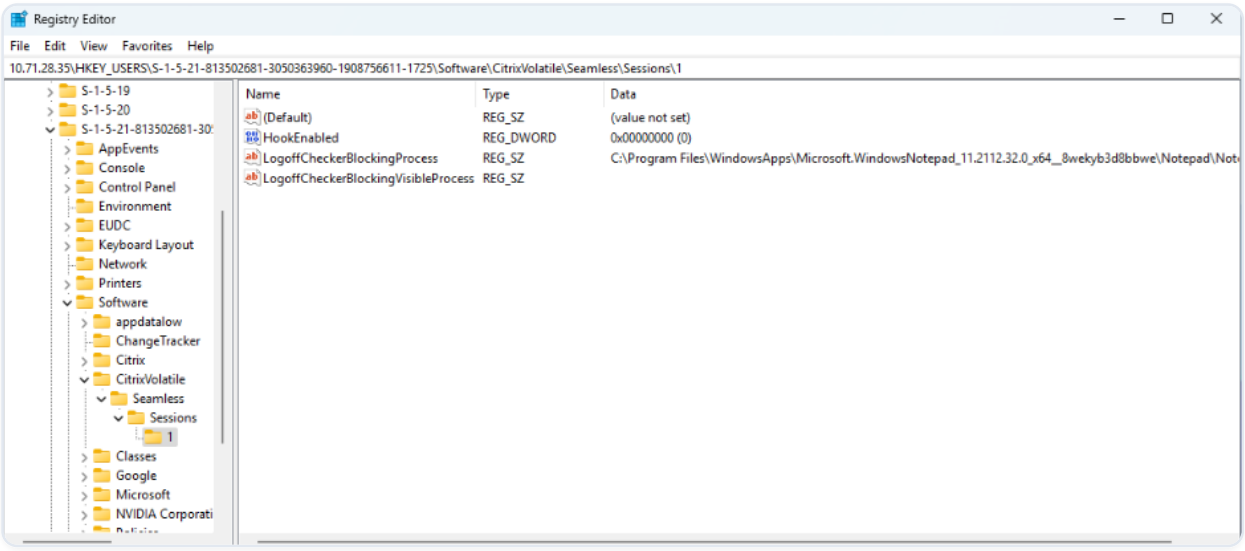
> **注:**
>
> **LogoffCheckBlockingProcess**と**LogoffCheckerBlockingVisibleProcess**は手動で編集してはいけません。これらのレジストリ値を手動で編集すると、セッションが不安定になる可能性があります。

> 公開アプリ2(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-regedit-2.png)

9. 右上隅の**X**をクリックして**Seamless CMD**を終了します。
10. セッションが閉じるかどうか接続センターを確認します。閉じるまでに最大30秒かかる場合があります。閉じれば、正常なサインアウトを妨げたアプリケーションやプロセスはなかったことになります。

    正常なサインアウト(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-bwd.png)
11. セッションが閉じなかった場合は、F5 キーで **regedit** の出力を更新します。
12. **LogoffCheckBlockingProcess**と**LogoffCheckerBlockingVisibleProcess**の内容を再度確認します。CMDは表示されなくなっているはずですが、別のプロセスがリストされているはずです。現在セッションのサインアウトをブロックしているプロセスがここに表示されている必要があります。

    この場合、コマンドプロンプトが閉じられる前に公開されたコマンドプロンプトから**Notepad.exe**が開かれており、このリモートのメモ帳プロセスが正常なサインアウトを妨げています。



13. この実行可能ファイルのパスと、それが表示されたキーをメモし、リモートツリーの下にある次のレジストリキーに入力します。

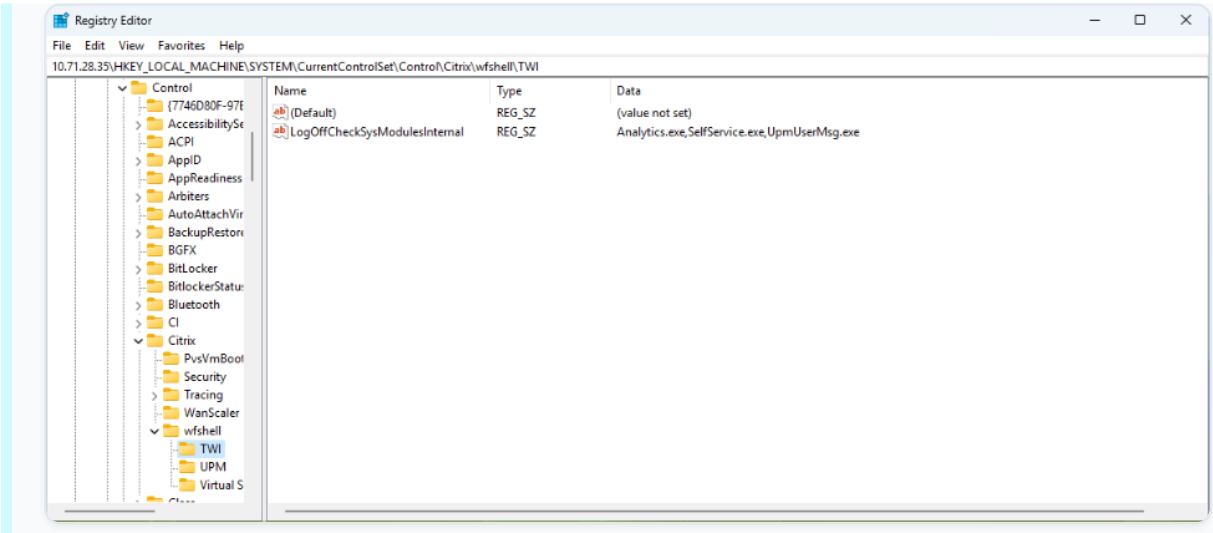
    - **LogoffCheckBlockingProcess** に表示される場合:

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckSysModulesInterna`

    - **LogoffCheckerBlockingVisibleProcess** に表示される場合:

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckVisibleSysModules`

> **注:**
>
> キーにすでに1つ以上のエントリがある場合は、末尾にコンマを追加し、そのコンマの後に新しいエントリを配置します。



14. クライアントの接続センターからセッションをサインアウトし、リモートアプリケーションを再度開きます。

15. リモートアプリケーションを閉じてから30秒以内にセッションが自動的にサインアウトされるまで、手順9〜16を繰り返します。

> **注:**
>
> トラブルシューティング後、必要に応じて、リモートレジストリアクセスを許可するために一時的なファイアウォールの変更を元に戻します。

公開アプリケーションを開くときにWindowsの免責事項メッセージを全画面表示で見るためにLogonUIを変更する方法

認証パススルーが発生しないシナリオにおいて、**LogonUI**ウィンドウのスケーリングが改善されました。**LogonUI**ウィンドウは、使用されているモニターの解像度とDPI設定に基づいてスケーリングされ、これにより、**LogonUI**ウィンドウ全体がクリッピングなしで表示されることが保証されます。

ピクセル単位のウィンドウサイズは、レジストリで手動で設定することもできます。

1. **ファイル名を指定して実行**コマンドで`regedit`を使用して**レジストリエディター**を開きます。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`にアクセスします。
3. 2つの新しいDWORDキー、**LogonUIWidth**と**LogonUIHeight**を作成します。
4. **LogonUI**ウィンドウに必要な幅と高さ（ピクセル単位）にキーの値を設定します。

   LogonUIウィンドウのサイズを手動で設定すると、自動スケーリングは無効になります。

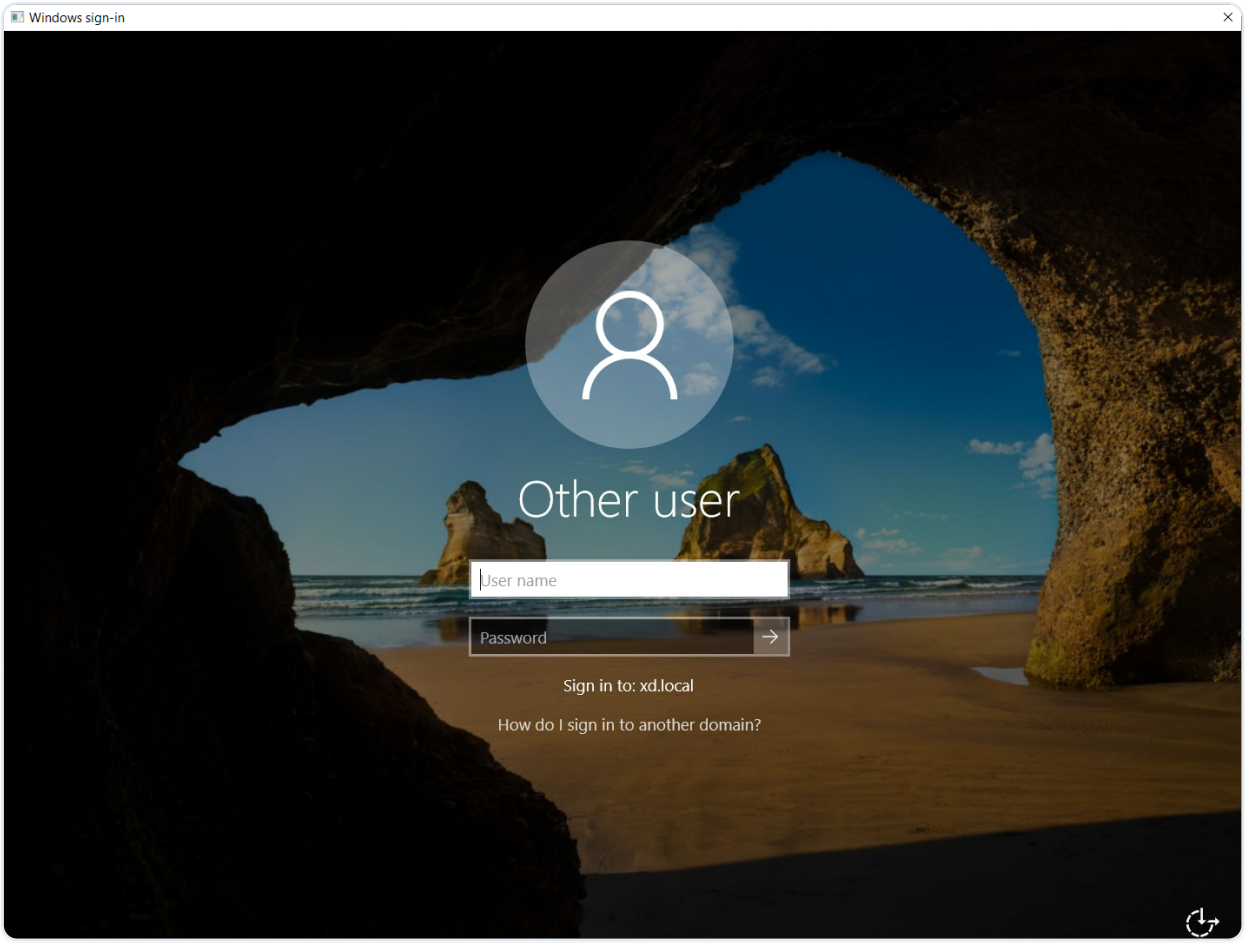
> **注：**
>
> これらのレジストリパスは2407以降変更されました。古いレジストリ値は無視され、非推奨です。

> デフォルトでは、**LogonUI**ウィンドウには閉じるボタン付きのタイトルバーが含まれており、これによりエンドユーザーは必要に応じてセッションから切断できます。

タイルバーを無効にする

次のレジストリキーを使用して、**LogonUI**ウィンドウのタイルバーを無効にできます。

1. **ファイル名を指定して実行** コマンドで `regedit` を使用してレジストリエディターを開きます。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\` にアクセスします。
3. 新しいDWORDキー: **LogonUICaption** を作成し、そのキーの値を `0` に設定します。



アプリケーションフォルダーの管理

デフォルトでは、デリバリーグループに追加する新しいアプリケーションは、**Applications**という名前のフォルダーに配置されます。デリバリーグループの作成時、アプリケーションの追加時、または後で別のフォルダーを指定できます。

知っておくと便利な情報:

- Applicationsフォルダーの名前を変更したり削除したりすることはできませんが、そのフォルダーに含まれるすべてのアプリケーションを、作成した他のフォルダーに移動することはできます。

- フォルダー名には1〜64文字を含めることができます。スペースも使用できます。
- フォルダーは最大5レベルまでネストできます。
- フォルダーにアプリケーションを含める必要はありません。空のフォルダーも許可されます。
- フォルダーは、移動したり、作成時に別の場所を指定したりしない限り、Web Studioでアルファベット順に表示されます。
- 各フォルダーが異なる親フォルダーを持つ限り、同じ名前のフォルダーを複数持つことができます。同様に、各アプリケーションが異なるフォルダーにある限り、同じ名前のアプリケーションを複数持つことができます。
- フォルダー内のアプリケーションを表示するには`View Applications`権限が必要です。アプリケーションを含むフォルダーを削除、名前変更、または削除するには、そのフォルダー内のすべてのアプリケーションに対して`Edit Application Properties`権限が必要です。
- 以下のほとんどの手順では、Web Studioのアクションバーを使用してアクションを要求します。または、右クリックメニューを使用するか、アイテムをドラッグすることもできます。たとえば、意図しない場所にフォルダーを作成または移動した場合、ドラッグアンドドロップで正しい場所に移動できます。
- Web Studioのすべてのノード（**マシンカタログ**、**デリバリーグループ**、**アプリケーション**、**アプリケーショングループ**など）は、バックエンドで同じフォルダーツリーを共有します。フォルダーの名前変更や移動の際に名前の競合を避けるため、異なるノード間で最上位フォルダーには一意の名前を使用してください。

  `New-BrokerAdminFolder` SDK コマンドレットを使用してフォルダーを作成し、それを**アプリケーション**ノードの下に表示させたい場合は、`Set-BrokerAdminFolderMetadata`コマンドレットを使用して`ContainsApplications`メタデータを追加する必要があります。

  例:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsApplications -Value true
  ```

アプリケーションフォルダーを管理するには、左ペインで**アプリケーション**を選択します。以下のリストを参考にしてください。

- **すべてのフォルダーを表示するには（ネストされたフォルダーを除く）：** フォルダーリストの上にある**すべて表示**をクリックします。
- **最上位レベルにフォルダーを作成するには（ネストしない）：** **アプリケーション**フォルダーを選択します。新しいフォルダーを**アプリケーション**以外の既存のフォルダーの下に配置する

には、そのフォルダーを選択します。次に、アクションバーで**フォルダーの作成**を選択します。名前を入力します。

- **フォルダーを移動するには：** フォルダーを選択し、アクションバーで**フォルダーの移動**を選択します。ネストされたフォルダーが含まれている場合を除き、一度に1つのフォルダーしか移動できません。（フォルダーを移動する最も簡単な方法は、ドラッグすることです。）
- **フォルダーの名前を変更するには：** フォルダーを選択し、アクションバーで**フォルダー名の変更**を選択します。名前を入力します。
- **フォルダーを削除するには：** フォルダーを選択し、アクションバーで**フォルダーの削除**を選択します。アプリケーションや他のフォルダーを含むフォルダーを削除すると、それらのオブジェクトも削除されます。アプリケーションを削除すると、デリバリーグループからのアプリケーション割り当ては削除されますが、マシンからは削除されません。
- **アプリケーションをフォルダーに移動するには：** 1つまたは複数のアプリケーションを選択します。次に、アクションバーで**アプリケーションの移動**を選択します。フォルダーを選択します。

デリバリーグループまたはアプリケーショングループを作成する際に、**アプリケーション**ページで追加するアプリケーションをフォルダーに配置することもできます。デフォルトでは、追加されたアプリケーションは**アプリケーション**フォルダーに入ります。**変更**をクリックしてフォルダーを選択または作成します。

公開デスクトップでのアプリケーションのローカル起動を制御する

ユーザーが公開デスクトップ内から公開アプリケーションを起動するときに、そのアプリケーションをデスクトップセッション内で起動するか、公開アプリケーションとして起動するかを制御できます。Citrix Workspaceアプリは、VDA上のWindowsレジストリでアプリケーションのインストールパスを検索し、存在する場合はアプリケーションのローカルインスタンスを起動します。それ以外の場合は、ホストされたアプリケーションのインスタンスが起動されます。VDAにインストールされていないアプリケーションを起動すると、ホストされたアプリケーションが起動されます。詳細については、「vPrefer起動」を参照してください。

PowerShell（Citrix Cloud展開ではRemote PowerShell SDKを使用し、オンプレミス展開ではPowerShell SDKを使用）で、このアクションを変更できます。

`New-Broker` Applicationまたは`Set-BrokerApplication` コマンドレットで、`LocalLaunchDisabled` オプションを使用します。例：

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

デフォルトでは、このオプションの値はfalse（`-LocalLaunchDisabled $false`）です。公開デスクトップ内から公開アプリケーションを起動すると、アプリケーションはそのデスクトップセッション内で起動されます。

オプションの値をtrue（`-LocalLaunchDisabled $true`）に設定すると、公開アプリケーションが起動されます。これにより、公開デスクトップ（Windows用Citrix Workspaceアプリを使用）から公開アプリケーションへの個別の追加セッションが作成されます。

要件と制限事項:

- アプリケーションの`ApplicationType`値は`HostedOnDesktop`である必要があります。
- このオプションは、適切なPowerShell SDKを介してのみ利用できます。Web Studioのグラフィカルインターフェイスでは現在利用できません。
- このオプションには、最低限StoreFront 3.14、Citrix Receiver for Windows 4.11、およびDelivery Controller 7.17が必要です。

アプリケーショングループ

> **注:**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

アプリケーショングループを使用すると、アプリケーションのコレクションを管理できます。異なるデリバリーグループ間で共有されるアプリケーション、またはデリバリーグループ内のユーザーのサブセットによって使用されるアプリケーションに対して、アプリケーショングループを作成します。アプリケーショングループはオプションです。これらは、同じアプリケーションを複数のデリバリーグループに追加する代替手段を提供します。デリバリーグループを複数のアプリケーショングループに関連付けたり、アプリケーショングループを複数のデリバリーグループに関連付けたりできます。

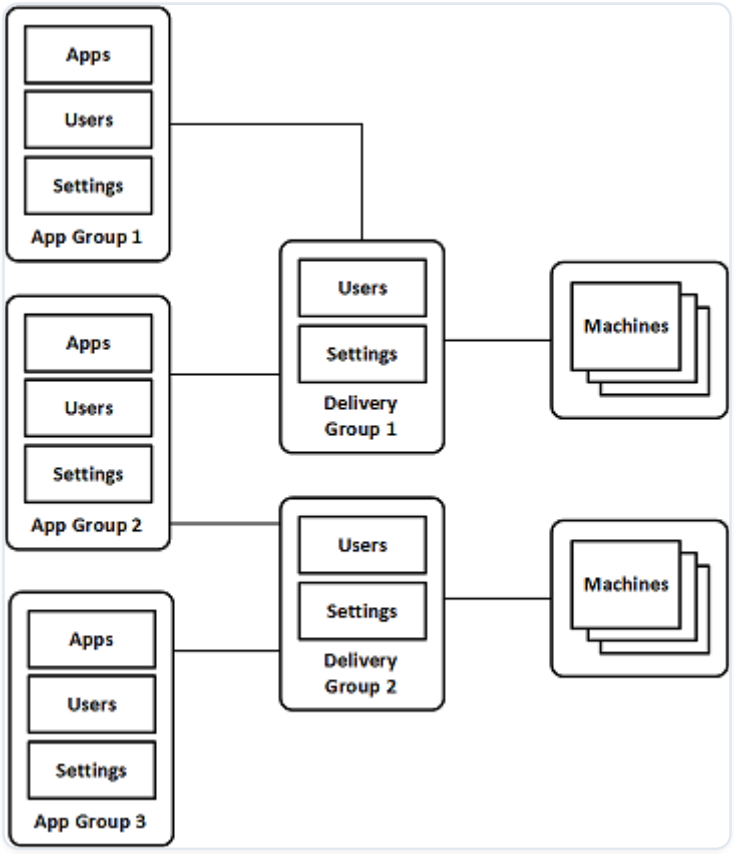
アプリケーショングループを使用すると、より多くのデリバリーグループを使用する場合と比較して、アプリケーション管理とリソース制御の利点が得られます。

- アプリケーションとその設定を論理的にグループ化することで、それらのアプリケーションを単一の単位として管理できます。たとえば、同じアプリケーションを個々のデリバリーグループに一度に1つずつ追加（公開）する必要はありません。
- アプリケーショングループ間のセッション共有により、リソース消費を節約できます。その他の場合、アプリケーショングループ間のセッション共有を無効にすることが有益な場合もあります。
- タグ制限機能を使用して、選択したデリバリーグループ内のマシンのサブセットのみを考慮して、アプリケーショングループからアプリケーションを公開できます。タグ制限を使用すると、既存のマシンを複数の公開タスクに使用できるため、追加のマシンの展開と管理に関連するコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）するものと考えることができます。タグ制限付きのアプリケーショングループまたはデスクトップを使用することは、デリバリーグループ内のマシンのサブセットを分離してトラブルシューティングする際に役立ちます。

構成例

例 1:

次の図は、アプリケーショングループを含むCitrix Virtual Apps™ and Desktopsの展開を示しています。



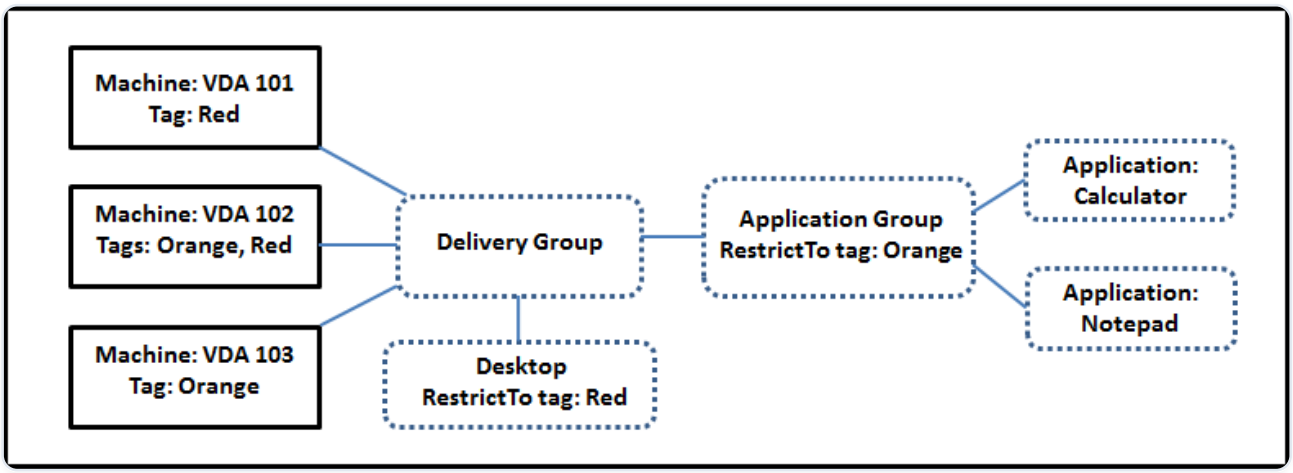
この構成では、アプリケーションはデリバリーグループではなくアプリケーショングループに追加されます。デリバリーグループは、どのマシンが使用されるかを指定します。（図には示されていませんが、マシンはマシンカタログ内にあります。）

アプリケーショングループ1はデリバリーグループ1に関連付けられています。アプリケーショングループ1で指定されたユーザーがアプリケーショングループ1のアプリケーションにアクセスします。これらのグループは、デリバリーグループ1のユーザーリストにも含まれている場合にのみ表示されます。この構成は、アプリケーショングループのユーザーリストが、関連付けられたデリバリーグループのユーザーリストのサブセット（制限）であるというガイダンスに従います。アプリケーショングループ1の設定（アプリケーショングループ間のアプリケーションセッション共有、関連付けられたデリバリーグループなど）は、そのグループ内のアプリケーションとユーザーに適用されます。デリバリーグループ1の設定は、アプリケーショングループ1と2のユーザーに適用されます。これは、これらのアプリケーショングループがそのデリバリーグループに関連付けられているためです。

アプリケーショングループ2は、2つのデリバリーグループ（1と2）に関連付けられています。これらのデリバリーグループのそれぞれには、アプリケーショングループ2で優先順位が割り当てられており、アプリケーションが起動される際にデリバリーグループがチェックされる順序を示します。優先順位が同じデリバリーグループは、負荷分散されます。アプリケーショングループ2のアプリケーションには、アプリケーショングループ2で指定されたユーザーがアクセスします。ただし、それらのユーザーはデリバリーグループ1とデリバリーグループ2のユーザーリストにも含まれている必要があります。

例 2:

このシンプルなレイアウトでは、タグ制限を使用して、特定のデスクトップおよびアプリケーションの起動に考慮されるマシンを制限します。このサイトには、1つの共有デリバリーグループ、1つの公開デスクトップ、および2つのアプリケーションで構成された1つのアプリケーショングループがあります。



3台のマシン（VDA 101～103）のそれぞれにタグが追加されています。

アプリケーショングループは「Orange」タグ制限付きで作成されました。その各アプリケーションは、そのデリバリーグループ内で「Orange」タグを持つマシン（VDA 102および103）でのみ起動されます。

アプリケーショングループ（およびデスクトップ）でタグ制限を使用するためのより包括的な例とガイダンスについては、「タグ」を参照してください。

ガイダンスと考慮事項

Citrixでは、アプリケーションをアプリケーショングループまたはデリバリーグループのいずれかに追加することを推奨しており、両方に追加することは推奨していません。そうしないと、2つのグループタイプにアプリケーションが存在することで複雑さが増し、管理がより困難になる可能性があります。

デフォルトでは、アプリケーショングループは有効になっています。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

デフォルトでは、アプリケーショングループ間のアプリケーションセッション共有は有効になっています。「アプリケーショングループ間のセッション共有」を参照してください。

Citrixでは、デリバリーグループを現在のバージョンにアップグレードすることをお勧めします。このプロセスには、次のものが必要です。

1. デリバリーグループで使用されているマシン上のVDAをアップグレードする。
2. それらのマシンを含むマシンカタログのアップグレード。
3. デリバリーグループのアップグレード。

詳細については、「デリバリーグループの管理」を参照してください。

アプリケーショングループを使用するには、コアコンポーネントが最小バージョン7.9である必要があります。

アプリケーショングループを作成するには、デリバリーグループ管理者組み込みロールの委任管理権限が必要です。詳細については、「委任管理」を参照してください。

この記事では、アプリケーションを複数のアプリケーショングループに「関連付ける」ことについて言及しています。これは、利用可能なソースからそのアプリケーションのインスタンスを追加する操作とは区別されます。同様に、デリバリーグループは、互いの追加やコンポーネントではなく、アプリケーショングループに関連付けられます。

アプリケーショングループとのセッション共有

アプリケーションセッション共有が有効になっている場合、すべてのアプリケーションは同じアプリケーションセッションで起動します。これにより、より多くのアプリケーションセッションを起動するコストが削減され、コピー＆ペースト操作など、クリップボードを使用するアプリケーション機能の使用が可能になります。ただし、状況によってはセッション共有をクリアできます。

アプリケーショングループを使用する場合、デリバリーグループのみを使用する場合に利用できる標準のセッション共有動作を拡張する、次の3つの方法でアプリケーションセッション共有を構成できます。

- アプリケーショングループ間でセッション共有が有効。
- 同じアプリケーショングループ内のアプリケーション間でのみセッション共有が有効。
- セッション共有が無効。

アプリケーショングループ間のセッション共有

アプリケーショングループ間でアプリケーションセッション共有を有効にすることも、または、同じアプリケーショングループ内のアプリケーションにのみアプリケーションセッション共有を制限するために無効にすることもできます。

- **アプリケーショングループ間のセッション共有を有効にすることが役立つ例:**

  アプリケーショングループ1には、WordやExcelなどのMicrosoft Officeアプリケーションが含まれています。アプリケーショングループ2には、メモ帳や電卓などの他のアプリケーションが含まれており、両方のアプリケーショングループは同じデリバリーグループに接続されています。両方のアプリケーショングループにアクセスできるユーザーが、Wordを起動してアプリケーションセッションを開始し、次にメモ帳を起動します。コントローラーが、Wordを実行しているユーザーの既存のセッションがメモ帳の実行に適していると判断した場合、メモ帳は既存のセッション内で開始されます。メモ帳が既存のセッションから実行できない場合（たとえば、タグ制限によってセッションが実行されているマシンが除外される場合など）、セッション共有を使用するのではなく、適切なマシン上に新しいセッションが作成されます。

- **アプリケーショングループ間のセッション共有を無効にすることが役立つ例:**

  同じマシンにインストールされている他のアプリケーションとうまく相互運用できないアプリケーションのセットを含む構成。同じソフトウェアスイートの2つの異なるバージョンや、同じWebブラウザの2つの異なるバージョンなど。ユーザーが同じセッションで両方のバージョンを起動することを許可しない方がよい場合。

  ソフトウェアスイートの各バージョンに対してアプリケーショングループを作成し、ソフトウェアスイートの各バージョンのアプリケーションを対応するアプリケーショングループに追

加します。これらのアプリケーショングループのそれぞれでグループ間のセッション共有が無効になっている場合、それらのグループで指定されたユーザーは、同じセッションで同じバージョンのアプリケーションを実行できます。ユーザーは同時に他のアプリケーションを実行できますが、同じセッションでは実行できません。異なるバージョンのアプリケーションのいずれか、またはアプリケーショングループに含まれていないアプリケーションを起動すると、そのアプリケーションは新しいセッションで起動されます。

このアプリケーショングループ間のセッション共有機能は、セキュリティサンドボックス機能ではありません。これは完璧ではなく、ユーザーが他の手段（たとえば、Windowsエクスプローラー経由など）でセッションにアプリケーションを起動するのを防ぐことはできません。

マシンが容量に達している場合、新しいセッションは開始されません。新しいアプリケーションは、セッション共有を使用して、必要に応じてマシンの既存のセッションで開始されます。

アプリケーションセッション共有が許可されているアプリケーショングループでのみ、事前起動セッションを利用できます。（セッションリンガー機能を使用するセッションは、すべてのアプリケーショングループで利用できます。）これらの機能は、アプリケーショングループに関連付けられている各デリバリーグループで有効にして構成する必要があります。アプリケーショングループでは構成できません。

デフォルトでは、アプリケーショングループを作成すると、アプリケーショングループ間のアプリケーションセッション共有が有効になります。グループの作成時にこれを変更することはできません。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

アプリケーショングループ内のセッション共有を無効にする

同じアプリケーショングループ内のアプリケーション間でのアプリケーションセッション共有を防ぐことができます。

- **アプリケーショングループ内のセッション共有を無効にすることが役立つ例:**

  ユーザーが、別々のモニターでアプリケーションの複数の同時フルスクリーンセッションにアクセスできるようにしたい場合。

  アプリケーショングループを作成し、そこにアプリケーションを追加します。

デフォルトでは、アプリケーショングループを作成すると、アプリケーションセッション共有が有効になります。グループの作成時にこの設定を変更することはできません。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

アプリケーショングループを作成する

アプリケーショングループを作成するには：

1. Web Studioにサインインします。
2. 左ペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
3. フォルダーを使用してアプリケーショングループを整理するには、**アプリケーショングループ**ルートフォルダーの下にフォルダーを作成します。詳しくは、「フォルダーを使用したアプリケーショングループの整理」を参照してください。
4. グループを作成するフォルダーを選択し、**アプリケーショングループの作成**をクリックします。グループ作成ウィザードが**はじめに**ページで起動します。このページは、今後のウィザード起動時に表示しないように設定できます。
5. ウィザードに従って、以下のページで設定を構成します。各ページでの作業が完了したら、**次へ**を選択して**概要**ページに進みます。

手順1. デリバリーグループ

デリバリーグループページには、すべてのデリバリーグループと、各グループに含まれるマシンの数が表示されます。

- **互換性のあるデリバリーグループ**の一覧には、選択可能なデリバリーグループが含まれています。互換性のあるデリバリーグループには、ランダムな（永続的または静的に割り当てられていない）マルチセッションまたはシングルセッションOSマシンが含まれています。
- **互換性のないデリバリーグループ**の一覧には、選択できないデリバリーグループが含まれています。各エントリには、静的に割り当てられたマシンが含まれているなど、互換性がない理由が説明されています。

アプリケーショングループは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。

以下の両方の条件が満たされている場合、デスクトップのみを配信する共有マシンを含むデリバリーグループを選択することもできます。

- デリバリーグループに共有マシンが含まれており、XenDesktopバージョン7.9より前に作成されていること。
- デリバリーグループの編集権限があること。

アプリケーショングループ作成ウィザードがコミットされると、デリバリーグループの種類は自動的に「デスクトップとアプリケーション」に変換されます。

関連付けられたデリバリーグループがないアプリケーショングループを作成できますが（アプリケーションを整理するため、または現在使用されていないアプリケーションのストレージとして機能させるためなど）、少なくとも1つのデリバリーグループが指定されるまで、そのアプリケーショングループをアプリケーションの配信に使用することはできません。また、デリバリーグループが指定されていない場合、**スタート**メニューソースからアプリケーショングループにアプリケーションを追加することはできません。

選択したデリバリーグループは、アプリケーションの配信に使用されるマシンを指定します。アプリケーショングループに関連付けるデリバリーグループの横にあるチェックボックスをオンにします。

タグ制限を追加するには、**タグを持つマシンへの起動を制限する**を選択し、ドロップダウンリストからタグを選択します。

手順2. ユーザー

アプリケーショングループでアプリケーションユーザーを指定します。前のページで選択したデリバリーグループ内のすべてのユーザーとユーザーグループを許可するか、それらのデリバリーグループから特定のユーザーとユーザーグループを選択します。指定されたユーザーに利用を制限する場合、デリバリーグループで指定されたユーザーのうち、アプリケーショングループで指定されたユーザーのみが、このグループのアプリケーションにアクセスできます。基本的に、アプリケーショングループのユーザーリストは、デリバリーグループのユーザーリストに対するフィルターとして機能します。

認証されていないユーザーによるアプリケーションの使用の有効化または無効化は、アプリケーショングループではなく、デリバリーグループでのみ利用できます。

展開でユーザーリストが指定される場所については、「ユーザーリストが指定される場所」を参照してください。

ステップ3. アプリケーション

知っておくと良いこと:

- デフォルトでは、追加する新しいアプリケーションは**アプリケーション**という名前のフォルダーに配置されます。別のフォルダーを指定することもできます。アプリケーションを追加しようとして、同じ名前のアプリケーションがそのフォルダーに存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。提案された一意の名前に同意すると、その新しい名前でアプリケーションが追加されます。そうでない場合は、追加する前に自分で名前を変更する必要があります。詳細については、「アプリケーションフォルダーの管理」を参照してください。

- アプリケーションのプロパティ（設定）は、追加時または後で変更できます。「アプリケーションプロパティの変更」を参照してください。同じ名前の2つのアプリケーションを同じユーザーに公開する場合、Web Studioで**アプリケーション名（ユーザー向け）**プロパティを変更してください。そうしないと、ユーザーはCitrix Workspaceアプリで重複した名前を目にすることになります。
- アプリケーションを複数のアプリケーショングループに追加する場合、それらのすべてのグループでアプリケーションを表示する十分な権限がないと、表示の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが追加されたすべてのグループを含むようにスコープを拡張してください。

アプリケーションソースを表示するには、ドロップダウンメニューから「**追加**」をクリックします。

- **スタートメニューから**：選択したデリバリーグループ内のマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、「**OK**」をクリックします。

  以下のいずれかを選択した場合、このソースは選択できません。

  - 関連付けられたデリバリーグループがないアプリケーショングループ。
  - 関連付けられたデリバリーグループにマシンが含まれていないアプリケーショングループ。
  - マシンが含まれていないデリバリーグループ。

- **手動で定義:** サイト内またはネットワーク内の別の場所にあるアプリケーション。このソースを選択すると、実行可能ファイルのパス、作業ディレクトリ、オプションのコマンドライン引数、管理者およびユーザーの表示名を入力する新しいページが起動します。この情報を入力したら、**OK**をクリックします。
- **既存**: 以前にサイトに追加されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスを選択し、**OK**をクリックします。サイトにアプリケーションがない場合、このソースは選択できません。
- **App-V**: App-Vパッケージ内のアプリケーション。このソースを選択すると、**App-Vサーバー**または**アプリケーションライブラリ**を選択する新しいページが起動します。表示された画面から、追加するアプリケーションのチェックボックスを選択し、**OK**をクリックします。詳しくは、「App-Vアプリケーションの展開と配信」を参照してください。サイトでApp-Vが構成されていない場合、このソースは選択できません（または表示されない場合があります）。

前述のとおり、**追加**ドロップダウンメニューの一部のエントリは、その種類の有効なソースがない場合、選択できません。互換性のないソースはまったく表示されません（たとえば、アプリケーショングループにアプリケーショングループを追加することはできないため、アプリケーショングループを作成する際にはそのソースは表示されません）。

ステップ4. スコープ

このページは、以前にカスタムスコープを作成した場合にのみ表示されます。デフォルトでは、**すべて**のスコープが選択されています。詳しくは、「委任管理」を参照してください。

手順5. 概要

アプリケーショングループの名前を入力します。必要に応じて、説明を入力することもできます。

概要情報を確認し、**完了**をクリックします。

公開コンテンツ

> **注:**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> Microsoft WordドキュメントやWebリンクなど、リソースへのURLまたはUNCパスであるアプリケーションを公開できます。この機能は公開コンテンツとして知られています。コンテンツを公開する機能により、ユーザーへのコンテンツ配信方法に柔軟性が加わります。既存のアクセス制御とアプリケーション管理の恩恵を受けることができます。また、コンテンツを開くためにローカルアプリケーションを使用するか、公開アプリケーションを使用するかを指定することもできます。

公開されたコンテンツは、StoreFront™およびCitrix Workspace™アプリの他のアプリケーションと同様に表示されます。ユーザーはアプリケーションにアクセスするのと同じ方法でアクセスします。クライアントでは、リソースは通常どおり開きます。

- ローカルにインストールされたアプリケーションが適切な場合、それが起動されてリソースが開かれます。

- ファイルの種類に関連付けが定義されている場合、公開されたアプリケーションが起動されてリソースが開かれます。

コンテンツはPowerShell SDKを使用して公開します。Web Studioを使用してコンテンツを公開することはできません。ただし、公開後にWeb Studioを使用してアプリケーションのプロパティを編集することはできます。

構成の概要と準備

コンテンツの公開には、次の主要なプロパティを持つ `New-BrokerApplication` コマンドレットを使用します。（すべてのコマンドレットプロパティの説明については、コマンドレットのヘルプを参照してください。）

```
New-BrokerApplication –ApplicationType PublishedContent
-CommandLineExecutable location -Name app-name -DesktopGroup delivery-
group-name
```

`ApplicationType` プロパティは `PublishedContent` である必要があります。

`CommandLineExecutable` プロパティは、公開コンテンツの場所を指定します。以下の形式がサポートされており、255文字の制限があります。

- HTMLウェブサイトアドレス（例: `<http://www.citrix.com>`）
- ウェブサーバー上のドキュメントファイル（例: `https://www.citrix.com/press/pressrelease.doc`）
- FTPサーバー上のディレクトリ（例: `ftp://ftp.citrix.com/code`）
- FTPサーバー上のドキュメントファイル（例: `ftp://ftp.citrix.com/code/Readme.txt`>）
- UNC ディレクトリパス (例: `file://myServer/myShare or \\\\myServer\\myShare`)
- UNC ファイルパス (例: `file://myServer/myShare/myFile.asf` または `\\myServer\myShare\myFile.asf`)

正しいSDKがあることを確認してください。

- Citrix DaaS (旧Citrix Virtual Apps and Desktopsサービス) の展開の場合、ダウンロード して、Citrix Virtual Apps and Desktops Remote PowerShell SDKをインストールします。
- オンプレミスのCitrix Virtual Apps and Desktops展開の場合、Delivery Controllerとともにインストールされているの PowerShell SDKを使用します。公開コンテンツアプリケーションを追加するには、最低バージョン7.11のDelivery Controllerが必要です。

以下の手順では例を使用します。例では、:

- マシンカタログが作成されています。
- `PublishedContentApps` という名前のデリバリーグループが作成されています。このグループは、カタログからマルチセッションOSマシンを使用します。WordPadアプリケーションがグループに追加されています。
- デリバリーグループ名、`CommandLineExecutable` の場所、およびアプリケーション名が割り当てられます。

はじめに

PowerShell SDKを含むマシンでPowerShellを開きます。

次のコマンドレットは、適切なPowerShell SDKスナップインを追加し、返されたデリバリーグループレコードを割り当てます。

`Add-PsSnapin Citrix* $dg = Get-BrokerDesktopGroup –Name PublishedContentApps`

Citrix DaaSを使用している場合は、Citrix Cloud™の資格情報を入力して認証します。複数の顧客がいる場合は、1つを選択します。

URLを公開する

場所とアプリケーション名を割り当てた後、次のコマンドレットは、Citrixのホームページをアプリケーションとして公開します。

```
$citrixUrl = "https://www.citrix.com/"

$appName = "Citrix Home Page"



New-BrokerApplication –ApplicationType PublishedContent –
CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.Uid
```

成功を確認します:

- StoreFrontを開き、PublishedContentAppsデリバリーグループ内のアプリケーションにアクセスできるユーザーとしてログオンします。デフォルトのアイコンを持つ新しく作成されたアプリケーションが表示されます。アイコンのカスタマイズについては、`<https://`

`www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/>`を参照してください。

- **Citrix Home Page**アプリケーションをクリックします。URLは、ローカルで実行されているデフォルトブラウザの新しいタブで起動します。

UNCパスにあるリソースを公開する

この例では、管理者は`PublishedResources`という名前の共有をすでに作成しています。場所とアプリケーション名を割り当てた後、以下のコマンドレットはその共有内のRTFファイルとDOCXファイルをリソースとして公開します。

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\\PublishedResources\\PublishedRTF.rtf"

$rtfAppName = "PublishedRTF"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $rtfUNC -Name $rtfAppName

-DesktopGroup $dg.Uid



$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx"

$docxAppName = "PublishedDOCX"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $docxUNC -Name $docxAppName

-DesktopGroup $dg.Uid
```

成功を確認します:

- StoreFrontウィンドウを更新して、新しく公開されたドキュメントを表示します。

- **PublishedRTF**および**PublishedDOCX**アプリケーションをクリックします。各ドキュメントは、ローカルで実行されているWordPadで開きます。

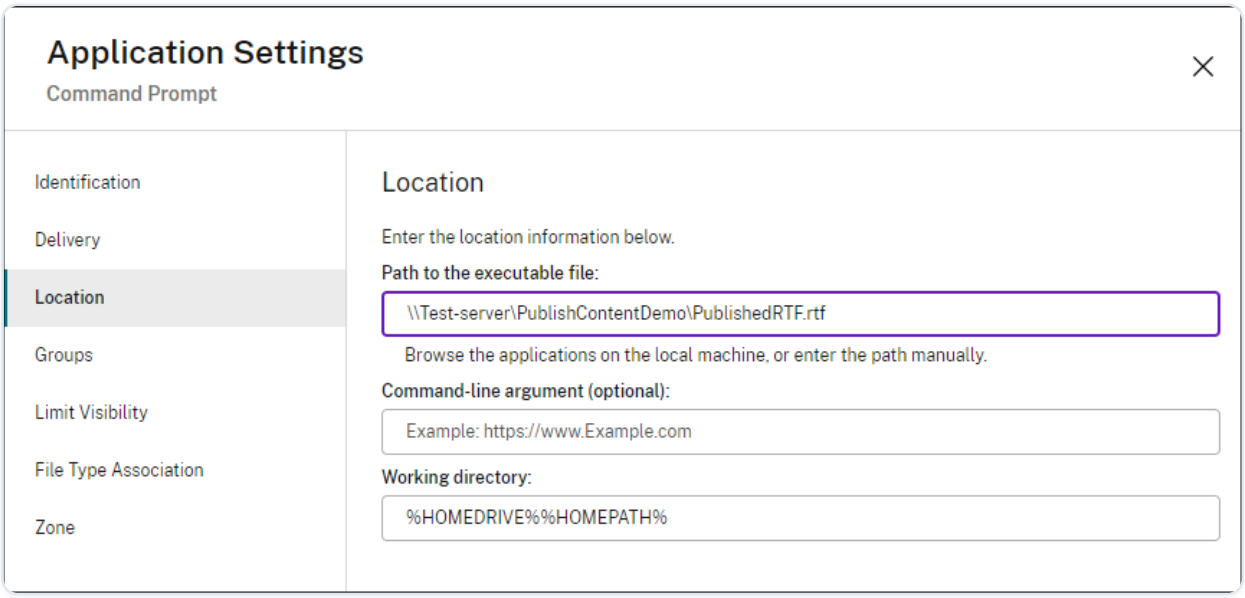
PublishedContentアプリケーションの表示と編集

公開されたコンテンツは、他のアプリケーションタイプに使用するのと同じ方法で管理します。

`PublishedContent`アプリケーションを表示および編集するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**Applications**を選択します。
2. **Applications**タブで、PublishedContentアプリケーションを選択し、**Properties**を選択します。

   アプリケーションプロパティ（ユーザーの可視性、グループの関連付け、ショートカットなど）は、公開されたコンテンツに適用されます。ただし、**場所**ページでは、コマンドライン引数または作業ディレクトリのプロパティを変更することはできません。
3. リソースを変更するには、そのページの**実行可能ファイルへのパス**フィールドを変更します。

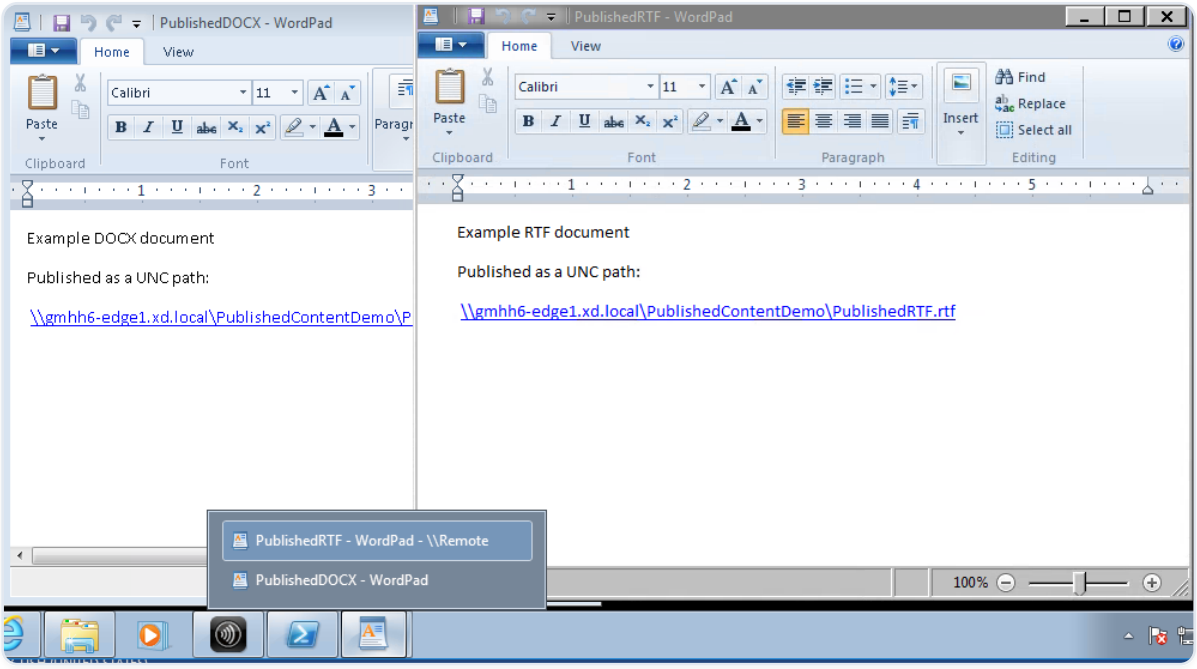


4. 公開されたアプリケーションを使用して`PublishedContent`アプリケーションを開く（ローカルアプリケーションではなく）には、次の手順に従います。

   この例では、公開されたWordPadアプリケーションが編集され、.rtfファイル用のファイルタイプ関連付けが作成されます。

   a. デリバリーグループのメンテナンスモードをオンにします。
   b. **ファイルタイプ関連付け**プロパティを編集します。
   c. 完了したら、メンテナンスモードをオフにします。

d. StoreFrontを更新してファイルタイプ関連付けの変更を読み込み、次に**PublishedRTF**および**PublishedDOCX**アプリケーションをクリックします。違いに注目してください。**PublishedDOCX**は引き続きローカルのWordPadで開きます。ただし、**PublishedRTF**はファイルタイプ関連付けにより、公開されたWordPadで開くようになりました。



詳細情報

- マシンカタログを作成する
- デリバリーグループを作成する
- アプリケーションプロパティを変更する

アプリケーションパッケージ

アプリケーションパッケージは、Citrix®が管理する事前構成済みのアプリケーション展開です。これにより、アプリケーションを仮想化でき、ユーザーデバイスのオペレーティングシステムやインターフェイスから独立してアプリケーションが実行されることを意味します。

アプリケーションパッケージは、アプリケーション管理を簡素化し、ITオーバーヘッドを削減し、アプリケーションがライフサイクル全体を通じて安全かつ機能的であることを保証します。

Citrix は、ユーザーにアプリケーションを配信するために、以下のパッケージングテクノロジーをサポートしています。

- App-Vアプリケーション
- MSIXおよびMSIX app attachアプリケーション

- FlexAppアプリケーション
- Elastic Appアプリケーション
- Cloudpagingアプリケーション

この記事では、Citrix Virtual Apps and Desktops™ 環境でこれらのパッケージ化されたアプリケーションを展開および配信する方法について説明します。

注:

- バージョン2511以降、Citrix Virtual Apps and Desktops™の唯一の管理コンソールはCitrix Web Studio（Webベース）です。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。
- アプリケーションパッケージの展開と配信にWeb StudioとCitrix Studioを相互に利用することはお勧めしません。それぞれ異なるメカニズムを使用しているため、App-Vサーバー情報が一方では正しく表示されるが、もう一方では表示されないといった不一致が生じる可能性があります。また、Citrix StudioはApp-Vのみをサポートしていることにも注意してください。

App-V アプリケーション

Application Virtualization (App-V) は、エンドユーザーのデバイスにインストールすることなく、アプリケーションをストリーミングしてアクセスできるようにする Microsoft のテクノロジーです。Citrix Virtual Apps and Desktops は App-V を使用してアプリケーションを配信でき、さまざまなクライアントマシン間でアプリケーションを管理するための集中化された効率的な方法を提供します。

App-Vパッケージアプリケーションを配信する際に操作するコンポーネントと概念の詳細については、Microsoftのドキュメント: Windowsクライアント向けApplication Virtualization (App-V) の概要を参照してください。

重要な用語

- **管理サーバー**: App-Vインフラストラクチャを管理するための一元化されたコンソールを提供し、App-Vデスクトップクライアントとリモートデスクトップサービスクライアントの両方に仮想アプリケーションを配信します。App-V管理サーバーは、管理者が要求するセキュリ

ティ、メータリング、監視、データ収集を認証、要求、提供します。このサーバーは、Active Directoryとサポートツールを使用してユーザーとアプリケーションを管理します。

- **公開サーバー**: 特定のユーザー向けにApp-Vクライアントにアプリケーションを提供し、ストリーミング用の仮想アプリケーションパッケージをホストします。管理サーバーからパッケージを取得します。
- **動的構成ファイル**: App-Vパッケージは、動的構成ファイルを使用してカスタマイズできます。これらのファイルは、パッケージに適用されると、その特性を変更するために使用できます。たとえば、追加のアプリケーションショートカットや動作を定義するために使用できます。詳細については、「動的構成ファイル」(#dynamic-configuration-files)を参照してください。

動的構成ファイル

Citrix App-Vは、両方の種類の動的構成ファイルをサポートしています。ファイル設定は、アプリケーションの起動時に適用されます。

- **展開構成ファイル**は、すべてのユーザーに対してマシン全体の構成を提供します。これらのファイルは`<packageFileName>_DeploymentConfig.xml`という名前で、適用されるApp-Vパッケージと同じフォルダーにあることが想定されています。これらのファイルは、シングルおよびデュアル管理管理でサポートされています。
- **ユーザー構成ファイル**は、パッケージに対するユーザーごとのカスタマイズをサポートするユーザー固有の構成を提供します。シングル管理は、`<packageFileName>_[UserSID | Username | GroupSID |GroupName_]UserConfig.xml`という形式で命名され、適用されるApp-Vパッケージと同じフォルダーにあるユーザー構成ファイルをサポートします。

  特定のパッケージに対して複数のユーザー構成ファイルが存在する場合、それらは次の優先順位で適用されます。

  a. ユーザーSID
  b. ユーザー名
  c. ADグループSID（最初に見つかったものが優先）
  d. ADグループ名（最初に見つかったものが優先）
  e. デフォルト

  例:

```
MyAppVPackage_S-1-5-21-000000001-0000000001-000000001-001_UserConfig.xml

MyAppVPackage_joeblogs_UserConfig.xml
```

```
MyAppVPackage_S-1-5-32-547_UserConfig.xml

MyAppVPackage_Power Users_UserConfig.xml

MyAppVPackage_UserConfig.xml
```

注:

ファイル名のユーザー固有の部分は、オプションで末尾に配置することもできます (例: `MyAppVPackage_UserConfig_joeblogs.xml`)。

重要:

パッケージ内のアプリケーションでユーザーセッションが開いている場合、動的展開構成に変更を適用することはできません。他のユーザー (ただし現在のユーザーではない) がパッケージ内のアプリケーションを開いている場合は、動的ユーザー構成ファイルに変更を適用できます。

動的構成ファイルの場所

単一管理者管理では、Citrix App-Vコンポーネントは、App-Vパッケージと同じフォルダーにある動的構成ファイルのみを処理します。

パッケージ内のアプリケーションが起動されると、対応する動的構成ファイルへの変更が再適用されます。動的構成ファイルがパッケージとは異なる場所にある場合は、マッピングファイルを使用してパッケージを展開構成ファイルにマッピングします。

マッピングファイルを作成するには:

1. 新しいテキストファイルを開きます。
2. 各動的構成ファイルについて、`<PackageGuid> : path`の形式を使用してパッケージへのパスを指定する行を追加します。

   例:

   ```
   F1f4fd78ef044176aad9082073a0c780 : c:\widows\file\packagedeploy.xml
   ```

3. ファイルを`ctxAppVDynamicConfigurations.cfg`として、パッケージと同じフォルダーに保存します。

App-Vパッケージと同じUNC共有上のディレクトリ階層全体が、パッケージ内のアプリケーションが起動されるたびに、このファイルを求めて再帰的に上位検索されます。

方法

App-Vパッケージを配信および管理するには、次の方法を使用できます:

- **デュアル管理者**: この方法では、Citrix Virtual Apps and Desktops と App-V サーバーが連携してパッケージを配信および管理します。この方法では、Citrix Virtual Apps and Desktops が App-V サーバーの状態のスナップショットビューを定期的に更新する必要があります。これには、ハードウェア、インフラストラクチャ、および管理のオーバーヘッドが発生します。Citrix Virtual Apps and Desktops と App-V サーバーは、特にユーザー権限に関して同期を維持する必要があります。

  この方法は、App-VとCitrixが密接に連携する展開で最適に機能します。この方法では:

  - **App-V管理サーバー**が動的構成ファイルを処理します。
  - **VDAマシンにインストールされているApp Packages Delivery Component**: アプリケーションの起動に必要な適切な公開サーバーの登録を管理します。

  これにより、適切なタイミングでユーザーに対して公開サーバーが同期されます。公開サーバーは、構成されている設定を使用して、アプリパッケージのライフサイクル（ログオン時の更新や接続グループなど）の他の側面を維持します。
- **シングル管理者**: アプリケーションパッケージはネットワーク共有に保存されます。Citrix Virtual Apps and Desktops は、パッケージを独立して配信および管理します。

  この方法により、展開においてApp-Vサーバーとデータベースインフラストラクチャが不要になるため、オーバーヘッドが削減されます。

  この方法では、App-Vパッケージをネットワーク共有に保存し、その場所からメタデータを環境にアップロードします。その後、VDAマシンにインストールされているApp Packages Delivery Componentが、次のようにアプリケーションを管理および配信します。

  - アプリケーションが起動されたときに、展開構成ファイルとユーザー構成ファイルを処理します。
  - ホストマシン上のパッケージのライフサイクルのすべての側面を管理します。

> **注：**

- 両方の管理方法を同時に使用できます。つまり、アプリケーションをデリバリーグループに追加する場合、アプリケーションはApp-Vサーバーまたはネットワーク共有にあるApp-Vパッケージから取得できます。
- 両方の管理方法を同時に使用していて、App-Vパッケージが両方の場所に動的構成ファイルを持っている場合、App-Vサーバー（デュアル管理）のファイルが使用されます。
- Web Studioのナビゲーションペインで App packagesを選択すると、パッケージ名と種類が表示されます。**パッケージの種類**列は、パッケージの配信に使用されるテクノロジーと、**アプリケーションライブラリ**で参照されている場所を示します。パッケージを選択すると、詳細ペインにパッケージ内のアプリケーションとショートカットが一覧表示されます。

MSIXおよびMSIXアプリアタッチアプリケーション

MSIXは、すべてのWindowsアプリに最新のパッケージングエクスペリエンスを提供するWindowsアプリパッケージ形式です。MSIXは、Win32、.NET、UWPアプリなど、さまざまなWindowsアプリケーションタイプに適しています。

MSIXアプリアタッチは、仮想ハードディスクに事前に展開されたMSIXパッケージを利用します。これにより、パッケージの内容をストリーミングするのではなく、必要に応じてターゲットマシンにマウントできます。展開時間の短縮、ネットワークトラフィックの削減、ターゲットマシンでのIOPSの低減に貢献できますが、アプリアタッチディスクの作成と維持には追加の作業が必要です。

Citrix Virtual Apps and Desktopsは、VDAマシンにインストールされている**App Packages Delivery Component**を介して、MSIXおよびMSIXアプリアタッチアプリケーションをユーザーに提供します。このコンポーネントは、ホストマシン上のパッケージのライフサイクルのあらゆる側面を管理します。

MSIXおよびMSIXアプリアタッチの詳細については、Microsoftのドキュメント: MSIX documentation および App Attach in Azure Virtual Desktop をそれぞれ参照してください。

注記:

- デスクトップおよびサーバーVDA上のネイティブMSIXパッケージと、デスクトップVDAのみで、`.vhd`、`.vhdx`、および`.cim`ディスクイメージ形式のMSIXアプリアタッチをサポートしています。
- MicrosoftはServer 2019向けにAppAttachの実装を提供していません。AppAttachはServer 2022および2025に存在しますが、Microsoftはこれらのバージョンでのサポートを提供していません。したがって、弊社もServer 2022および2025でのAppAttachをサポートしていません。
- Windows Server 2019でサイドローディングを有効にします。
- VDAがパッケージの署名に使用されている証明書を信頼していることを確認してください。

FlexAppアプリケーション

FlexAppは、Liquidwareが開発したアプリケーションレイヤリングソリューションで、従来のアプリケーションインストールプロセスを介して基盤となるベースイメージを変更することなく、任意のアプリケーションをWindowsセッションにアタッチします。

FlexApp Oneアプリケーションは、単一の共有可能なファイルにカプセル化されており、Windowsセッションに追加のアプリケーションレイヤーを必要とせずに動作できます。ユーザーはコンテナファイルをクリックしてアプリケーションを起動でき、これにより1つまたは複数のアプリケーションがWindowsワークスペースに迅速に統合されます。

Citrixは、VDAマシンにインストールされているApp Packages Delivery ComponentとFlexApp配信エージェントを介して、FlexAppアプリケーションをユーザーに提供します。これら2つのコンポーネントは、ホストマシン上のパッケージのライフサイクルのあらゆる側面を管理します。

Elastic Appアプリケーション

Elastic App technology は、Citrix App Layering の機能であり、アプリケーションレイヤーをベースイメージにインストールするのではなく、ログオン時にユーザーに動的に割り当てることができます。Elastic App technology を使用すると、アプリケーションは異なる仮想マシン間でユーザーに追従し、マスターイメージを肥大化させることなく、必要なアプリに常にアクセスできるようにします。

Citrix Virtual Apps and Desktops は、Citrix Personalization コンポーネントと Application Layering Enterprise Layer Manager (ELM) を介して、Elastic App アプリケーションをユーザーに提供します。これら2つのコンポーネントは、ホストマシン上のパッケージのライフサイクルのあらゆる側

面を管理します。Application Layering Enterprise Layer Manager の詳細については、Citrix App Layering™ ドキュメントを参照してください。

Cloudpaging アプリケーション

Cloudpaging は、Numecent のアプリケーションストリーミングテクノロジーであり、ベースイメージに変更を加えることなく、Windows セッションにアプリケーションを配信します。

Cloudpaging を使用すると、コードのごく一部（通常は10%未満）のみが最初にストリーミングされるため、アプリケーションはほぼ瞬時に起動します。残りのコンポーネントは、ユーザーがアクセスしたときにバックグラウンドでストリーミングされ、シームレスなエクスペリエンスを提供します。

Citrix 環境では、VDA 上の App Packages Delivery Component が Numecent Cloudpaging Player と連携してアプリケーションのライフサイクルを管理します。Citrix コンポーネントが配信をオーケストレーションし、Cloudpaging Player がセッション内でのオンデマンドストリーミングと実行を処理します。

構成要件

次の構成の詳細を考慮してください。

クラウドページング プレイヤー と LogoffCheckSysModules

Cloudpaging コンテナで仮想公開アプリケーションを使用する場合、セッションのログオフを許可するには、次の設定を構成します。

設定	値
レジストリキー	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI`
値の名前	`LogoffCheckSysModules`
値の型	`REG_SZ`
値のデータ	`CoreHelper.exe`

ホワイトリスト登録用のURL

標準のURLホワイトリスト登録要件に加えて、VDAは次のエンドポイントへのアクセスを必要とします。

パラメーター	値
URL	`external-api.cloudpager.net`
ポート	443
クライアント	Cloudpager PoSh モジュール
Webベースのフォワードプロキシ構成	• アウトバウンドアクセスが許可されている • 認証バイパスが必要
説明	Cloudpager PowerShellモジュール

オプションで、Cloudpagerの検出のみを実行するために使用されるVDAを持つ専用のデリバリーグループを作成し、必要なホワイトリスト登録済みURLを制限できます。**VDAバージョン2511以降**と**App packages Delivery Component**がインストールされているマシンでデリバリーグループを作成することをお勧めします。

Cloudpagerクライアントのネットワークおよびファイアウォールの要件の詳細については、Numecentナレッジベースの記事を参照してください。

アプリケーションパッケージの展開と配信

前提条件

App-V、MSIX、MSIX app attach、FlexAppパッケージ、Elastic Appアプリケーション、およびCloudpagingパッケージの配信をサポートするには、まずVDAマシンに**App Packages Delivery Component**をインストールする必要があります。詳細については、VDAマシンにApp Packages Delivery Componentをインストールするを参照してください。

VDAマシンへのApp Packages Delivery Componentのインストール

App Packages Delivery Componentは、App-V、MSIX、MSIX app attach、FlexApp、Elastic App、およびCloudpaging形式のアプリケーションパッケージの公開プロセスを管理します。このコンポーネントは、VDAをインストールする際にデフォルトではインストールされません。コンポーネントは、VDAのインストール中またはインストール後にインストールできます。

VDAのインストール中にコンポーネントをインストールするには、次のいずれかの方法を使用します。

- インストールウィザードで、**追加コンポーネント**ページに移動し、**App Packages Delivery Component**チェックボックスを選択します。
- コマンドラインインターフェースで、`/includeadditional "Citrix Personalization for App-V – VDA"` オプションを使用します。

VDAのインストール後にコンポーネントをインストールするには、次の手順に従います。

1. VDAマシンで、**コントロールパネル > プログラム > プログラムと機能**に移動し、**Citrix Virtual Delivery Agent**を右クリックして、**変更**を選択します。
2. 表示されるウィザードで、**追加コンポーネント**ページに進み、**App Packages Delivery Component**チェックボックスを有効にします。

注:

- Microsoft App-V Desktop Client は、ユーザーデバイスで App-V パッケージから仮想アプリケーションを実行するコンポーネントです。Windows 10 (1607 以降) および Windows Server 2019 以降には、この App-V クライアントソフトウェアがすでに含まれています。VDA マシンでのみ有効にする必要があります。詳細については、この Microsoft ドキュメント記事を参照してください: App-V インボックスクライアントを有効にする。
- FlexApp アプリケーションの場合は、App Packages Delivery Component とともに VDA に FlexApp One Agent をインストールします。
- Elastic App アプリケーションの場合は、App Packages Delivery Component とともに VDA に App Layering 対応イメージをインストールします。
- Cloudpaging アプリケーションの場合は、App Packages Delivery Component とともに VDA に Cloudpaging Playerをインストールします。

FlexApp One Agent をインストールする

1. VDA で管理者コマンドプロンプトを起動します。
2. 任意の FlexApp One Package のネットワークパスを見つけます。
3. 次のコマンドを入力します。

```
\\path\to\any\FlexAppOnePackage.exe --install
```

4. 表示されるプロンプトをすべて承認します。

App Layering 対応イメージをインストールする

1. アプリレイヤリングを設定します。 Citrix App Layering ドキュメントの指示に従ってください。プロセスには以下が含まれます。
   a. Enterprise Layer Manager (ELM) を設定します。
   b. ゴールド OS イメージをインポートします。
   c. プラットフォームレイヤーを作成します。
   d. アプリケーションレイヤーを作成します。
   e. ELMで、配信したい各アプリケーションレイヤーに対して、**Studio App Packagesでの使用を有効にする**チェックボックスを選択します。
2. VDAマシンにElastic Layeringコンポーネントを含むイメージをインストールします。以下のいずれかの方法を使用できます。
   a. Elastic Layeringが有効な状態でELMからイメージを展開します。
   b. マシンにVDAを手動でインストールし、セットアップ中にElastic Layeringコンポーネントを選択します。

Cloudpaging Playerをインストールする

1. VDAで管理者コマンドプロンプトを開きます。
2. Cloudpaging Playerインストーラーが含まれているフォルダーに移動します。
3. 以下のコマンドを実行して、プレーヤーをサイレントインストールし、SaaSコンソールURLを設定します。必要に応じてプレースホルダーの値を置き換えてください。

```
cloudpaging-player-setup-x64-release.exe /S /v"/qn ADDLOCAL=ALL
REG_BASTOKENPATHORURL=https://your-tenant-url/api/token"
```

4. (オプション) インストール後に、以下のレジストリ値を確認して構成を検証します。
   - **パス:** `HKEY_LOCAL_MACHINE\SOFTWARE\Numecent\StreamingCore\Settings\Launcher`
   - **名前:** `BaseTokenPathOrURL`
   - **データ:** 値は、インストール時に指定したURLと一致する必要があります。

パッケージ化されたアプリケーションを配信する

前提条件のインストールが完了したら、ユーザーにパッケージアプリケーションを配信するには、次の手順を実行します。

1. アプリケーションパッケージをネットワーク共有に保存する。
2. アプリケーションパッケージを環境にアップロードする。
3. デリバリーグループにアプリケーションを追加する。
4. 相互依存するApp-Vパッケージの自動配信を有効にするには、分離グループを作成します。

アプリケーションパッケージをネットワーク共有に保存する

インフラストラクチャをセットアップしたら、アプリケーションパッケージを生成し、UNCまたはSMBネットワーク共有、あるいはAzureファイル共有などのネットワークロケーションに保存します。

詳細な手順は次のとおりです。

1. アプリケーションパッケージを生成します。詳細については、Microsoftのドキュメント「App-V仮想化アプリケーションの作成と管理」を参照してください。
2. アプリケーションパッケージをネットワークロケーションに保存します。
   - **App-V Single Admin**の場合: パッケージと対応する動的構成ファイル（App-V）をUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
   - **App-V Dual Admin**の場合：UNCパスからApp-V管理サーバーにパッケージを公開します。（HTTP URLからの公開はサポートされていません。）
   - **MSIXまたはMSIX app attach**の場合: パッケージをUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
   - **FlexApp**の場合: パッケージをUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
   - **Elastic App**の場合: パッケージをUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
3. VDAがパッケージの保存パスに対する読み取り権限を持っていることを確認してください。
   - ADドメイン内のUNCまたはSMBネットワーク共有にパッケージを保存する場合、VDAマシンに保存パスへの読み取り権限を付与します。そのためには、マシンのADアカウントに共有への読み取り権限を明示的に付与するか、その権限を持つADグループにアカウントを含めることができます。

- Azureファイル共有にパッケージを保存する場合、まずAzureの保存パスに対するユーザーアカウントの読み取り権限を付与します。次に、VDAマシンで実行されている `ctxAppVService` を、そのユーザーアカウントを使用してパッケージ保存パスにアクセスするように構成します。詳細な手順については、ユーザーログオンアカウントの変更を参照してください。

ユーザーログオンアカウントの変更

以下の2つのシナリオでユーザーログオンアカウントを変更します。

- リンクされたADアカウントを使用してAzureファイル共有上のパッケージにアクセスする場合:
  - Microsoft Entra IDはファイル共有上のマシンアカウントに読み取り権限を付与しないため、接続エンティティはマシンアカウントではなくユーザーアカウントである必要があります。
- MSIXおよびMSIX AppAttachパッケージにサービスが含まれている場合:
  - パッケージは、非管理者ユーザーに公開される前に、ローカルマシン上で管理者権限を持つユーザーアカウントを使用して公開される必要があります。これは、パッケージ化されたサービスをインストールするために必要であり、パッケージはマシンではなくユーザーにのみ公開できるため、デフォルトのLocalServiceアカウントは不適切です。

VDAは `ctxAppVService` を呼び出して、パッケージ保存パスにアクセスし、管理者権限を必要とする操作を実行します。デフォルトでは、 `ctxAppVService` はマシンのLocalServiceアカウントのコンテキストで実行され、マシンのIDを使用してADに認証するため、上記のシナリオには適していません。

いずれの場合も、サービスは、ローカルで管理者権限を持ち、パッケージの保存場所（SMB共有またはAzureファイル共有）への読み取りアクセス権が付与されているADユーザーアカウントを使用するように再構成する必要があります。手順は次のとおりです。

1. **サービス**を開始し、**ctxAppVService**を右クリックして、**プロパティ**を選択します。
2. 「**ログオン**」タブで、「**このアカウント**」を選択します。
   a. ローカル管理者権限とパッケージストレージパスへの読み取り権限を持つユーザーアカウントを入力します
   b. ユーザーのパスワードを2回入力します。
3. **OK**をクリックします。

環境にアプリケーションパッケージをアップロードする

必要に応じてアプリケーションパッケージをネットワークの場所に保存した後、配信のために環境にアップロードします。必要に応じて、以下のいずれかの方法を使用します。

- 一括アップロード
- 1つずつアップロード

準備

Citrix Virtual Apps and Desktops は、パッケージ検出のためのネットワークロケーションへの接続を設定するために VDA マシンを使用します。したがって、事前にデリバリーグループを作成し、グループ内の少なくとも1つの VDA が次の要件を満たしていることを確認してください。

- VDAバージョン:
  - App-Vパッケージを検出するには: 2203以降
  - MSIXおよびMSIXアプリ添付パッケージを検出するには: 2209以降
  - FlexAppパッケージを検出するには: 2311以降およびFlexApp Agentソフトウェア
  - ElasticAppパッケージを検出するには: 2511以降およびApp Layering対応イメージ
  - Cloudpagingパッケージを検出するには: 2511以降およびCloudpaging Playerソフトウェア
- App Packages Delivery Component: インストール済み
- パッケージの場所に対するアクセス許可: 読み取り (詳細については、Store application packages on network sharesを参照してください。)
- 電源: オン
- 状態: 登録済み

アプリケーションパッケージを一括アップロードする

ネットワーク上の場所にあるパッケージを環境にアップロードします。アップロードする前に、次の項目が準備されていることを確認してください。

- Preparationsの要件を満たすデリバリーグループ
- ネットワークの場所のパス

パッケージを一括でアップロードするには、次の手順に従います。

1. 左側のペインで、**App packages**を選択します。
2. **Packeage discovery**タブで、**Create discovery profile**ボタンをクリックします。**Create discovery profile**ページが表示されます。

3. **Name**フィールドに、プロファイルの説明的な名前を入力します。
4. **Delivery group**フィールドで、**Select a delivery group**をクリックします。次に、Preparationsで述べられている要件を満たすデリバリーグループを選択し、**OK**をクリックします。
5. **Location type**フィールドで、パッケージの保存場所に応じて、**Microsoft App-V server**、**Network share**、または**Numecent Cloudpager**を選択し、対応する設定を完了します。
   - 「**Microsoft App-V サーバー**」を選択した場合は、次の情報を入力します。
     - 管理サーバーのURL。例: `http://appv-server.example.com`
     - 管理サーバー管理者のログイン資格情報。
     - 公開サーバーのURLとポート番号。例: `http://appv-server.example.com:3330`
   - 「**ネットワーク共有**」を選択した場合は、次の情報を指定します。
     - ネットワーク共有のUNCパスを入力します (例: `\\Package-Server\apps\`)。*Elastic App*パッケージの場合は、ELMの**System's Network File Share SMB path**からUNCパスを入力します。
     - アップロードするパッケージの種類を選択します。オプションには、**App-V**、**MSIX**、**MSIX app attach**、**FlexApp**、および**Elastic App**が含まれます。
     - パッケージのサブフォルダーを検索するかどうかを指定します。

       > **注:**
       >
       > `cim`イメージを含むフォルダー構造でMSIX app attachパッケージを検索する場合は、**サブフォルダーを検索**を選択していることを確認してください。そうしないと、ディスクが正しく検出されません。

   - 「**Numecent Cloudpager**」を選択した場合は、次の情報を入力します。
     - CloudpagerコンソールのURL。例: `https://cloudpagerconsole.my.org`
     - PowerShell APIキー。
     - AppLauncher MSID。
6. **検出プロファイルの作成**をクリックします。

「**検出プロファイルの作成**」ページが閉じ、新しく追加されたプロファイルがプロファイルリストに表示されます。Citrix Virtual Apps and Desktopsは、デリバリーグループ内のVDAを使用してパッケージを環境にアップロードします。アップロードが完了すると、「ステータス」フィールドに「*インポート成功*」と表示されます。対応するパッケージは「**パッケージ**」タブに表示されます。

> 「**注:**」:
>
> ソースの場所でパッケージの更新を確認し、環境にインポートするには、プロファイルリストで場所を選択し、**更新の確認** をクリックします。

アプリケーションパッケージを1つずつアップロードする

ネットワーク共有からアプリケーションパッケージを環境にアップロードします。アップロードする前に、次の項目を準備してください。

- (#preparations)に記載されている要件を満たすデリバリーグループ
- ネットワークの場所のパス。

パッケージを環境にアップロードするには、次の手順に従います。

1. 左側のペインで、「**アプリパッケージ**」を選択します。
2. 「**パッケージ**」タブで、「**パッケージの追加**」ボタンをクリックします。「**パッケージの追加**」ページが表示されます。
3. 「**デリバリーグループ**」フィールドで、「**デリバリーグループの選択**」をクリックします。次に、(#preparations)に記載されている要件を満たすデリバリーグループを選択し、「**OK**」をクリックします。
4. 「**パッケージのフルパス**」フィールドに、必要に応じてパスを入力します。
   - 複数のパッケージを一度にアップロードするには、セミコロン (`;`) で区切って、それらのフルパスを入力します。例: `\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - ネットワーク共有にあるすべてのパッケージをアップロードするには、ストレージパスを入力します。例: `\\package-Server\apps\`
5. 「**パッケージの追加**」をクリックします。

   アプリケーションパッケージが「**パッケージ**」タブに表示されます。

アプリケーションをデリバリーグループに追加する

アプリケーションパッケージが環境に完全にアップロードされたら、必要に応じてそのアプリケーションを1つ以上のデリバリーグループに追加します。その結果、それらのデリバリーグループに関連付けられているユーザーは、アプリケーションにアクセスできるようになります。

注:

- パッケージ化されたアプリケーションは、デリバリーグループを介してシングルセッションVDAおよびマルチセッションVDAに配信できます。
- デフォルトでは、エンドユーザーは、*シングルセッション*（または*デスクトップ*）VDAに関連付けられているデリバリーグループに割り当てられたすべてのパッケージ化されたアプリケーションにアクセスできます。*デスクトップ*VDA上のパッケージ化されたアプリケーションの可視性を特定のユーザーまたはグループに制限するには、**アプリケーション**ノードに移動し、アプリケーションを選択してから、**アプリケーションプロパティの編集 > 可視性の制限**を選択して変更を加えます。「アプリケーションの可視性を制限する」を参照してください。

パッケージ内の1つ以上のアプリケーションを複数のデリバリーグループに追加するには、次の手順に従います。

1. 左側のペインで、**アプリパッケージ**を選択します。
2. **パッケージ**タブで、必要に応じてパッケージを選択します。
3. アクションバーで、**デリバリーグループの追加**をクリックします。**アプリケーションをデリバリーグループに割り当てる**ページが表示されます。
4. 必要に応じてパッケージ内の1つ以上のアプリケーションを選択し、**次へ**をクリックします。
5. デリバリーグループのリストで、アプリケーションを割り当てるグループを選択し、**次へ**をクリックします。

注:

- MSIXまたはMSIXアプリ添付パッケージを選択した場合、VDAバージョンが2106以降のデリバリーグループのみがリストに表示されます。

- *FlexApp*パッケージを選択した場合、VDAバージョンが2402以降のデリバリーグループのみがリストに表示されます。
- *Elastic App* パッケージを選択した場合、VDA バージョンが 2511 以降のデリバリーグループのみがリストに表示されます。
- *Cloudpaging* パッケージを選択した場合、VDA バージョンが 2511 以降のデリバリーグループのみがリストに表示されます。

6. **完了**をクリックします。

さまざまなパッケージのアプリケーションを複数のデリバリーグループに追加するには、次の手順に従います。

1. 左ペインで、**App Packages**を選択します。
2. **アプリケーション**タブで、**アプリケーションの追加**を選択します。
3. **グループ**ページで、必要に応じて1つ以上のデリバリーグループを選択します。
4. **アプリケーション**ページで、次のように1つ以上のアプリケーションパッケージを選択します。
   a. **追加**をクリックし、**アプリケーションパッケージ**を選択します。
   b. 必要なパッケージプロファイルの種類（例：App-V Single Admin）を選択します。この種類のすべてのパッケージが表示されます。
   c. 必要に応じて1つ以上のパッケージを選択します。
   d. **OK**をクリックし、**次へ**をクリックします。
   e. 異なるパッケージタイプのアプリケーションをさらに追加するには、手順aからdを繰り返します。
5. **完了**をクリックします。

次の場合に、パッケージ化されたアプリケーションをデリバリーグループに追加することもできます。

- 配信グループを作成する。詳細については、配信グループの作成を参照してください。
- 既存の配信グループまたはアプリケーショングループを編集する。詳細については、アプリケーションの追加を参照してください。

（オプション）App-Vパッケージの分離グループを作成する

相互依存するApp-Vパッケージの自動配信を可能にするために、分離グループを作成できます。

注:

分離グループは、App-Vシングル管理者方式でサポートされています。App-Vデュアル管理者方式を使用している場合は、Microsoft App-Vインフラストラクチャで*接続グループ*を作成することで、同じ目標を達成できます。詳細については、このMicrosoftドキュメント記事を参照してください：接続グループファイルについて。

分離グループについて

分離グループとは、仮想環境を作成するために同じWindows Sandboxで実行する必要がある、相互依存するアプリケーションパッケージの集合です。Citrix App-V分離グループは、App-V接続グループと似ていますが、同じではありません。分離グループには、次の2種類のパッケージが含まれます。

- **明示的なアプリケーションパッケージ**：特定のライセンス要件を持つアプリケーション。これらのアプリケーションを配信グループに追加することで、特定のユーザー範囲に制限できます。
- **自動アプリケーションパッケージ**：配信グループに追加されているかどうかにかかわらず、常にすべてのユーザーが利用できるアプリケーション。

たとえば、アプリケーション`app-a`を実行するにはJRE 1.7が必要です。app-a（*明示的*とマーク）とJRE 1.7（*自動*とマーク）を含む分離グループを作成できます。次に、`app-a`のApp-Vパッケージを1つ以上の配信グループに追加します。ユーザーがapp-aを起動すると、JRE 1.7が自動的に展開されます。

ユーザーが分離グループ内で*明示的*とマークされたApp-Vアプリケーションを起動すると、Citrix Virtual Apps and Desktopsは、配信グループ内のアプリケーションに対するユーザーのアクセス許可を確認します。ユーザーがアプリケーションにアクセスする権限を持っている場合、同じ分離グループ内の*自動*アプリケーションパッケージはすべてユーザーに利用可能になります。

*自動*パッケージをどの配信グループにも追加する必要はありません。分離グループ内に別の*明示的*アプリケーションパッケージがある場合、そのパッケージは同じ配信グループ内にある場合にのみユーザーに利用可能になります。

APP-V分離グループを作成する

分離グループを作成し、相互依存するアプリケーションパッケージを追加します。詳細な手順は次のとおりです。

1. 「**分離グループ**」タブで、「**分離グループの追加**」をクリックします。

2. 分離グループの名前と説明を入力します。環境内のすべてのApp-V Single Adminパッケージが「**利用可能なパッケージ**」リストに表示されます。
3. 「**利用可能なパッケージ**」リストから必要に応じてアプリケーションを選択し、右矢印をクリックします。選択したアプリケーションが「**分離グループ内のパッケージ**」リストに表示されます。
4. 「**展開**」フィールドで、アプリケーションに対して「**明示的**」または「**自動**」を選択します。
5. 手順2〜3を繰り返して、さらにパッケージを追加します。
6. リスト内のパッケージの順序を調整するには、上矢印または下矢印をクリックします。
7. 「**保存**」をクリックします。

> **注:**
>
> 分離グループの構成により、VDA上にApp-V接続グループが作成されます。展開シナリオは複雑になる可能性があり、App-Vクライアントは一度に1つのアクティブな接続グループにのみ存在するパッケージをサポートします。同じパッケージを、同じデリバリーグループに追加されている2つの異なる分離グループに追加することは避けることをお勧めします。

ベストプラクティス

- App-Vパッケージを展開するには、PowerShellコマンド `Enable-AppV` を使用してVDAでApp-Vサブシステムを有効にします。
- MSIX（およびAppAttach）パッケージを展開するには、VDAがパッケージの署名に使用されている証明書を信頼する必要があります。
- Windows Server 2019では、MSIXパッケージを展開するためにサイドローディングを有効にします。Windows 10、11、Windows Server 2022、および2025ではサイドローディングは不要です。
- App AttachはWindows Server 2019ではまったく実装されておらず、Windows Server 2022または2025ではMicrosoft（およびCitrix）によって現在サポートされていません。

詳細設定

以下の高度なトピックでは、基本的なアプリパッケージのワークフローを超えて、Citrix Virtual Apps and Desktops でパッケージ化されたアプリケーションがどのように検出、更新、配信されるかを微調整するための追加の構成オプションと制御について説明します。

パッケージ化されたアプリケーションの公開を自動化する

PowerShellコマンドを使用して、パッケージ化されたアプリケーションの公開を自動化できます。

Delivery Controller™上で、以下のPowerShellコマンドを実行します:

1. パッケージ検出モジュールに存在するコマンドをロードするには:

```
Import-Module "D:
\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
```

> **注:**
>
> パッケージ検出モジュールのバージョンは、Citrix Virtual Apps and Desktops ISOの、手順1で述べたパスにあります。

2. パッケージ検出モジュールは、公開するパッケージタイプをサポートするCitrix Virtual Apps and DesktopsバージョンのISOから取得する必要があります。つまり、FlexAppOneアプリケーションには2311以降が必要です。最新の利用可能なものを使用することをお勧めします。
3. 関連するデリバリーグループIDとパッケージ化されたアプリケーションIDを取得するには:

```
Get-BrokerDesktopGroup | Format-Table Uid, Name

Get-AppLibAppVApplication | Format-Table Uid, Name
```

4. パッケージを公開し、適切なBrokerMachineConfigurationsを作成するには:

```
Publish-PackagedApplication -AppLibararyApplicationUid
<AppLibararyApplication.Uid > -DesktopGroupUid <DesktopGroup.Uid>
```

5. Broker構成を同期するには（これらは後でVDA上のBrokerエージェントに送信されます）:

```
Update-DesktopGroupMachineConfigurations -DesktopGroupUid
<DesktopGroup.Uid>
```

> **注:**

> PowerShellコマンドラインを介してデリバリーグループからパッケージ化されたアプリケーションを公開または削除した後には、PowerShellコマンド `Update-DesktopGroupMachineConfigurations` を必ず実行してください。そうしないと、公開されたアプリケーションに関する情報がVDAに正しく送信されず、起動に失敗します。

アプリケーションの可視性を制限する

Citrix Virtual Apps and Desktops環境では、パッケージからのアプリケーションがデスクトップに公開されると、システムはそれらのアプリケーションに対するActive Directory (AD) のユーザーおよびグループの可視性設定を尊重します。ただし、ユーザーがパッケージ内の1つのアプリケーションのみに可視性を持っている場合でも、個々のパッケージコンポーネントはVDA上で細分化できないため、パッケージ全体が仮想デスクトップ（またはシームレスアプリ）セッションに展開される必要があります。さらに、VDAバージョン2503より前では、最初の公開後にアプリケーションの可視性を低下させる変更を行っても、その後のデスクトップ起動時に以前公開されたパッケージのクリーンアップは行われません。さらに、デスクトップとワークスペースの可視性など、他の可視性レイヤーはこれらのAD可視性割り当ての上に動作します。

パッケージ化されたアプリケーションがWorkspaceに表示されるべきか、ユーザーのVDIデスクトップセッションに展開されるべきかを制御できます。パッケージ化されたアプリケーションが公開されたら、PowerShellコマンド `Set-BrokerApplication -Name "MyApp" -PackagedApplicationVisibility "Workspace|Desktop|WorkspaceAndDesktop"` を使用して、`BrokerApplictaion` の `PackagedApplicationVisibility` プロパティを更新できます。

`PackagedApplicationVisibility` のデフォルト値は `WorkspaceAndDesktop` です。

値 `Workspace`: アプリはWorkspaceAppにのみ表示され、シームレスなAppLaunchで利用できますが、ユーザーが開始するデスクトップセッションには自動的に公開されません。

値 `Desktop`: アプリのアイコンをWorkspaceAppから非表示にし、シームレスなAppLaunchでは利用できなくなりますが、ユーザーがADグループ設定を通じてアクセスできる場合は、アプリをユーザーのデスクトップセッションに展開できます。

> **注:**
>
> シングルセッション静的デスクトクトップに公開されたパッケージアプリケーションは、この設定で構成された値に関係なく、Workspace Appでは利用できません。

App-Vフルインフラストラクチャからシングル管理者ワークフローへの移行

Microsoft App-Vフルインフラストラクチャ（デュアル管理者）は、サポート終了が近づいています。App-Vパッケージやその他のサポートされているコンテナ形式の提供を継続するには、Citrixシングル管理者モデルに移行してください。

シングル管理者モデルは、App-V管理サーバーと公開サーバーへの依存関係を排除し、Studioでパッケージ管理を一元化します。

シングル管理者モデルの利点

シングル管理者ワークフローに移行することで、アーキテクチャが簡素化され、パッケージ管理が効率化されます。

簡素化されたアーキテクチャ

シングル管理者モデルでは、VDAはファイル共有から直接パッケージを取得します。Citrixはメタデータ、公開、および分離ロジックを管理します。

機能	フルインフラストラクチャ（デュアル管理者）	シングル管理者（CITRIX管理）
管理	App-V 管理コンソール	シトリックス スタジオ または ウェブ スタジオ
データベース	必須 (SQL Server)	なし (メタデータはCitrixサイトデータベースに保存されます)
公開	App-V 公開サーバー	シトリックス VDA (`ctxAppVService`)
パッケージソース	UNC共有 (管理サーバーと同期)	UNC共有、SMB共有、またはAzure Files
ロジック	接続グループ	Citrix アイソレーション グループ

戦略的利点

Single Adminに移行することで、**同期ラグ**も解消されます。

- Dual Admin モデルでは、App-V 管理サーバーを同期し、その後 Studio を同期する必要があります。

- Single Admin モデルでは、ファイル共有上のパッケージを更新し、Studio で を選択すると、更新されたパッケージは次回のユーザーログオン時に利用可能になります。

移行ワークフロー

既存の App-V フルインフラストラクチャを Citrix Single Admin ワークフローに移行するには、次の手順に従います。

1. ステップ 1: ターゲット環境を準備する
2. ステップ 2: パッケージを Citrix ライブラリにインポートする

ステップ 1: ターゲット環境を準備する

パッケージをインポートする前に、インフラストラクチャと VDA が Single Admin モデルをサポートする準備ができていることを確認してください。

1. **共有リポジトリ**

   a. `.appv` パッケージをホストする UNC 共有を特定します。

   b. VDA マシンアカウント（例: ドメインコンピューター）が、共有と NTFS の両方のアクセス許可に対して **読み取り** アクセス権を持っていることを確認してください。

2. **VDA**

   すべてのVDAに**App Packages Delivery Component**がインストールされていることを確認してください。インストール後にこのコンポーネントを追加するには、次の手順を実行します。

   a. VDA インストーラーを実行します。

   b. で を選択します。

   c. 「**App Packages Delivery Component**」を追加します。

3. **「XML構成ファイル」**

   `_DeploymentConfig.xml` と `_UserConfig.xml` ファイルを、対応する `.appv` ファイルと*同じ*フォルダーに移動します。

   Single Adminモデルでは、VDAは中央のApp-Vデータベースからではなく、ファイル共有上のパッケージフォルダーから構成ファイルを読み取ります。

ステップ2：パッケージをCitrixライブラリにインポートする

環境を準備したら、既存のApp-VパッケージをCitrixアプリケーションライブラリにインポートします。

1. Citrix Studioで、**構成** > **App Packages**に移動します。
2. 完全に移行する場合は、App-V管理サーバーへの既存の接続をすべて削除します。
3. **パッケージの追加**を選択し、パッケージのUNCパスを指定します。
4. Citrixはフォルダーをスキャンし、パッケージ名、バージョン、およびアプリケーションIDをCitrixアプリケーションライブラリにインポートします。

インポート後、必要に応じてアプリケーションをデリバリーグループに割り当てることができます。

> **注:**
>
> **vPreferポリシー（オプション）**：アプリケーションをリモートサーバーにリダイレクトする代わりにローカルVDAで起動したい場合は、VDAで**vPrefer** GPOを有効にしてください。

App-Vアプリケーションのトラブルシューティング（シングル管理者モデル）

App-Vパッケージ（シングル管理者モデル）が起動しない、またはユーザーセッションに表示されない場合は、以下のガイダンスを使用して一般的な問題を特定し、解決してください。

問題	説明	解決策
パッケージの検出と「カタログ化に失敗しました」エラー	Studioでパッケージを追加すると、ファイルにアクセスできないか、メタデータが無効であることを示すエラーが表示されます。	1. 権限を確認します。Delivery Controllerマシンアカウント（例：`DOMAIN\DDC01$`）が、パッケージをホストするUNCパスの共有レベルとNTFSレベルの両方で**読み取り**権限を持ってい

問題	説明	解決策	
		ることを確認してください。 2. XMLの整合性を確認します。`.appv` ファイルと `_DeploymentConfig.xml` ファイルのファイル名プレフィックスが同じで、同じフォルダーにあることを確認してください。	
アプリケーションの起動に失敗する (エラーコード: 0x80070005 または 0x80040154)	ユーザーがアプリケーションアイコンをクリックすると、**Citrix スプラッシュ** 画面が表示されますが、アプリケーションは開きません。	1. VDAコンポーネントを確認します。**App Packages Delivery Component** がVDAにインストールされていることを確認してください。次のファイルが存在することを確認してください: `C:\Program Files\Citrix\AppV\ctxAppVService.exe`。	

問題	説明	解決策	
		2. VDAのアクセス許可を確認します。 VDAはファイル共有からパッケージをプルするため、VDAマシンアカウント（例: `DOMAIN\VDA-HR01$`）はUNCパスへの**読み取り**アクセス権を持っている必要があります。 3. App-V クライアントの構成を検証します。 • VDA で次の PowerShell コマンドを実行します: `Get-AppvClientConfiguration`。 • パッケージにスクリプトが必要な場合は、`EnablePackageScripts` が `$True` に設定されていることを確認してください。	

問題	説明	解決策	
分離グループの競合	Excel アドインなどのプラグインは、その親アプリケーションを認識できません。	1. Studio で、**App Packages** > **Isolation Groups** に移動します。 2. 両方のパッケージが同じ分離グループに追加されていることを確認します。シングル管理者モデルでは、VDA上のApp-Vクライアントが、Delivery Controllerによって配信される構成に基づいて、それらのアプリケーションの仮想接続を管理します。	
初回起動が遅い (バッファリング)	AutoCADやArcGISなどの大規模なApp-Vパッケージの初回起動には数分かかります。	1. VDAで、次のレジストリを確認します `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\AppV\Client\Streaming`	

問題	説明	解決策	
		2. その後の起動パフォーマンスを向上させるため、`Autoload`を`2` (以前使用したすべてのパッケージを自動ロードする)に設定します。 3. ネットワークパフォーマンスを確認します。ネットワーク共有でのSMB署名またはウイルス対策スキャンが転送速度を制限していないことを確認してください。	

便利なPowerShellコマンド（VDAで実行）

CitrixがパッケージをVDAに正常に配信したかどうかを確認するには、PowerShellウィンドウで次のコマンドを実行します。

コマンド	目的
`Get-AppvClientPackage`	VDAに現在キャッシュされているか、公開されているすべてのApp-Vパッケージを表示します。
`Get-CtxAppvPackage`	Citrixエージェントによって管理されているパッケージを表示します。
`Start-Service ctxAppVService`	Citrix App-Vオーケストレーションサービスを再起動します。

UWP アプリケーションを公開する

ユニバーサル Windows プラットフォーム (UWP) アプリについては、以下の Microsoft ドキュメントを参照してください。

- ユニバーサル Windows プラットフォーム (UWP) アプリとは
- Windows パッケージマネージャー

要件と制限

Citrix Virtual Apps and Desktops™ は、以下の Windows マシン上の VDA で UWP アプリを使用することをサポートしています。

- Windows 10 以降のバージョン
- Windows Server 2016 以降のバージョン

VDA はバージョン 7.11 以降である必要があります。

UWPアプリを使用する場合、以下のCitrix Virtual Apps™ and Desktopsの機能はサポートされていないか、制限されています。

- ファイルタイプの関連付けはサポートされていません。
- ローカルアプリアクセスはサポートされていません。
- 動的プレビュー: セッションで実行中のアプリが重なっている場合、プレビューにはデフォルトのアイコンが表示されます。動的プレビューに使用される Win32 API は、UWP アプリではサポートされていません。
- アクションセンターのリモート処理: UWP アプリは、セッション内のメッセージを表示するためにアクションセンターを使用できます。これらのメッセージは現在、ユーザーに表示するためにエンドポイントにリダイレクトされません。

同じサーバーから UWP アプリと非 UWP アプリを起動することはサポートされていません。代わりに、UWP アプリと非 UWP アプリを別々のデリバリーグループまたはアプリケーショングループに配置してください。

マシンにインストールされているすべてのUWPアプリが列挙されるため、Citrix®はWindows Storeへのユーザーアクセスを無効にすることを推奨します。これにより、あるユーザーがインストールしたUWPアプリが別のユーザーによってアクセスされるのを防ぎます。

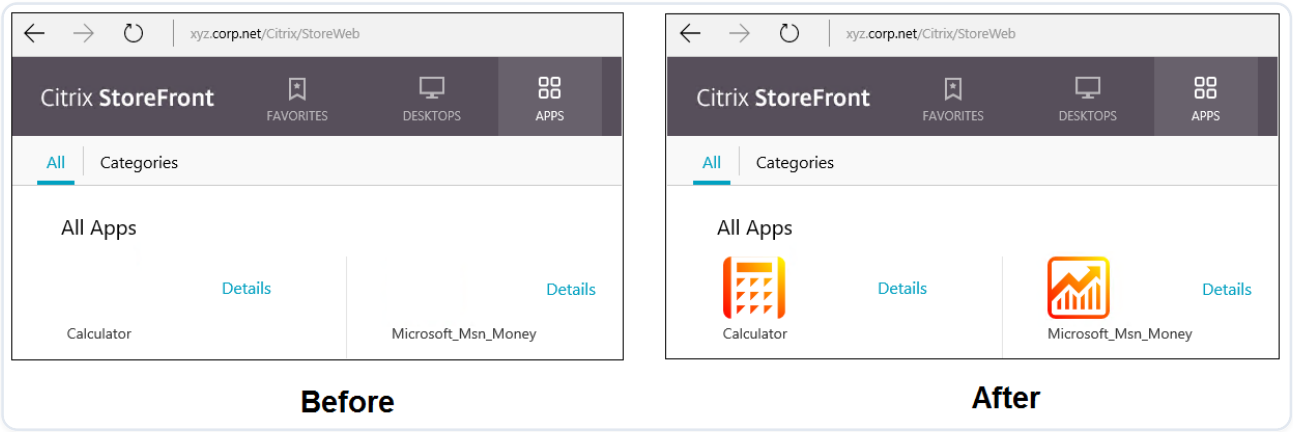
サイドローディング中、UWPアプリはマシンにインストールされ、他のユーザーが使用できるようになります。別のユーザーがアプリを起動すると、アプリがインストールされ、OSはそのAppXデータベースを更新して、そのユーザーによって「インストール済み」であることを示します。

固定ウィンドウまたはシームレスウィンドウで起動された公開済みUWPアプリから開始された正常なログオフは、VDAセッションが閉じないようにし、ユーザーを強制的にログオフさせる可能性があります。この場合、VDAセッションに残っているいくつかのプロセスが、セッションが適切に閉じないようにします。これを解決するには、VDAセッションの終了を妨げているプロセスを特定し、CTX891671のガイダンスに従って、「LogoffCheckSysModules」レジストリキー値に追加します。

UWPアプリのアプリケーション表示名と説明が正しくない場合があります。アプリケーションをデリバリーグループに追加する際に、これらのプロパティを編集して修正してください。

その他の問題については、既知の問題を確認してください。

現在、一部のUWPアプリは透明度が有効な白いアイコンを使用しており、StoreFront表示の白い背景に対してアイコンが見えなくなることがあります。この問題を回避するには、背景を変更できます。たとえば、StoreFrontマシンでファイル`C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`を編集します。ファイルの最後に`.storeapp-icon {background-image: radial-gradient( circle at top right, yellow, red ); }`を追加します。以下のグラフィックは、この例の変更前と変更後を示しています。



Windows Server 2016以降のバージョンでは、UWPアプリの起動時にサーバーマネージャーも起動する場合があります。これを防ぐには、`HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon`レジストリキーを使用して、ログオン時のサーバーマネージャーの自動起動を無効にできます。詳細については、`<https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/>`を参照してください。

UWPアプリのインストールと公開

UWPアプリのサポートはデフォルトで有効になっています。

VDA（またはマスターイメージ）に1つ以上のUWPアプリをインストールするには、次のいずれかの方法を使用します。

- Windows Store for Businessからオフラインインストールを完了し、Deployment Image Servicing and Management (DISM)などのツールを使用してアプリをデスクトップイメージに展開します。詳細については、Windows Package Managerを参照してください。
- アプリをサイドロードします。詳細については、Windowsクライアントデバイスで基幹業務 (LOB) アプリをサイドロードするを参照してください。
- 各対象ユーザー向けに、Windows Store for Businessから直接UWPアプリをインストールします。

Citrix Virtual AppsまたはCitrix Virtual Desktops™で1つ以上のUWPアプリを追加（公開）するには：

1. マシンにUWPアプリがインストールされたら、UWPアプリをデリバリーグループまたはアプリケーショングループに追加します。これは、グループの作成時または後で行うことができます。**アプリケーション**ページで、**追加**メニューから**スタートメニューから**を選択します。
2. アプリケーションリストが表示されたら、公開するUWPアプリを選択します。
3. ウィザードを続行するか、編集ダイアログを閉じます。

VDAでユニバーサルアプリの使用を無効にするには、`HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle`にレジストリ設定**EnableUWASeamlessSupport**を追加し、**0**に設定します。

UWPアプリのアンインストール

`Remove-AppXPackage`のようなコマンドでUWPアプリをアンインストールすると、その項目は管理者に対してのみアンインストールされます。アプリを起動して使用した可能性のあるユーザーのマシンからアプリを削除するには、各マシンで削除コマンドを実行します。1つのコマンドですべてのユーザーのマシンからAppXパッケージをアンインストールすることはできません。

Linux VDA 公開アプリケーション

Linux VDAバージョン7.13で、Citrixはサポートされているすべてのシームレスアプリケーション機能を追加しました。この機能を使用するために、特定のインストール手順は必要ありません。

> **ヒント:**

Linux VDAバージョン1.4で、Citrixは非シームレス公開アプリケーションとセッション共有のサポートを追加しました。

Citrix Studioを使用したアプリケーションの公開

デリバリーグループを作成するとき、または既存のデリバリーグループにアプリケーションを追加するときに、Linux VDAにインストールされているアプリケーションを公開できます。このプロセスは、Windows VDAにインストールされているアプリケーションを公開するのと同様です。詳しくは、Citrix Virtual Apps and Desktopsのドキュメント（使用しているCitrix Virtual Apps and Desktopsのバージョンに基づく）を参照してください。

注:

- デリバリーグループを構成するときは、デリバリーの種類が**デスクトップとアプリケーション**または**アプリケーション**に設定されていることを確認してください。
- アプリケーションとデスクトップのデリバリーには、個別のVDAとデリバリーグループを作成することをお勧めします。
- シームレスアプリケーションを使用するには、StoreFrontでシームレスモードを無効にしないでください。シームレスモードはデフォルトで有効になっています。「TWIMode=Off」を設定してすでに無効にしている場合は、「TWIMode=On」に変更するのではなく、この設定を削除してください。そうしないと、公開されたデスクトップを起動できない可能性があります。

制限事項

Linux VDAは、単一ユーザーによる同じアプリケーションの複数の同時インスタンスの起動をサポートしていません。

アプリセッションでは、アプリケーションに固有のショートカットのみが期待どおりに機能します。

既知の問題

アプリケーションの公開中に、以下の既知の問題が確認されています。

- 非矩形ウィンドウはサポートされていません。ウィンドウの角にサーバー側の背景が表示される場合があります。

- 公開アプリケーションからのウィンドウコンテンツのプレビューはサポートされていません。
- 複数のLibreOfficeアプリケーションを実行している場合、これらのアプリケーションはプロセスを共有するため、Citrix Studioには最初に起動されたアプリケーションのみが表示されます。
- 「Dolphin」のような公開されたQt5ベースのアプリケーションでは、アイコンが表示されない場合があります。この問題を解決するには、`<https://wiki.archlinux.org/title/Qt>`の記事を参照してください。
- Linuxアプリケーションには、使用中のアプリケーションに関する情報を含む「バージョン情報」ウィンドウがよくあり、詳細情報へのWebリンクがこれらのウィンドウによく見られます。「バージョン情報」ウィンドウのWebリンクをクリックすると、**calc**、**gedit**、**calendar**、**LibreOffice Suite**などの公開アプリケーション内からWebブラウザが起動される可能性があります。意図しないWebブラウザの起動は、アプリケーションの分離を迂回し、セキュリティを侵害する可能性があります。この問題に対処するには、以下の手順を実行してデフォルトのWebブラウザを変更します。

  a. カスタムの場所にnone.shファイルを作成します。例：

  ```
  sudo mkdir /home/none



  sudo touch /home/none/none.sh



  sudo chmod +x /home/none/none.sh
  ```

  b. none.shファイルに次の行を追加します。

  ```
  #!/bin/bash



  echo "NONE"
  ```

  c. sudoを使用して/etc/xdg/mimeapps.listファイルを作成し、その後、mimeapps.listファイルに次の行を追加します。

```
[Default Applications]


text/html=none.desktop


x-scheme-handler/http=none.desktop


x-scheme-handler/https=none.desktop


x-scheme-handler/about=none.desktop


x-scheme-handler/unknown=none.desktop
```

d. sudoを使用して/usr/share/applications/none.desktopファイルを作成し、その後、none.desktopファイルに次の行を追加します。

```
[Desktop Entry]


Encoding=UTF-8


Version=1.0


Type=Application


Terminal=false
```

```
Exec=/home/none/none.sh

Name=None

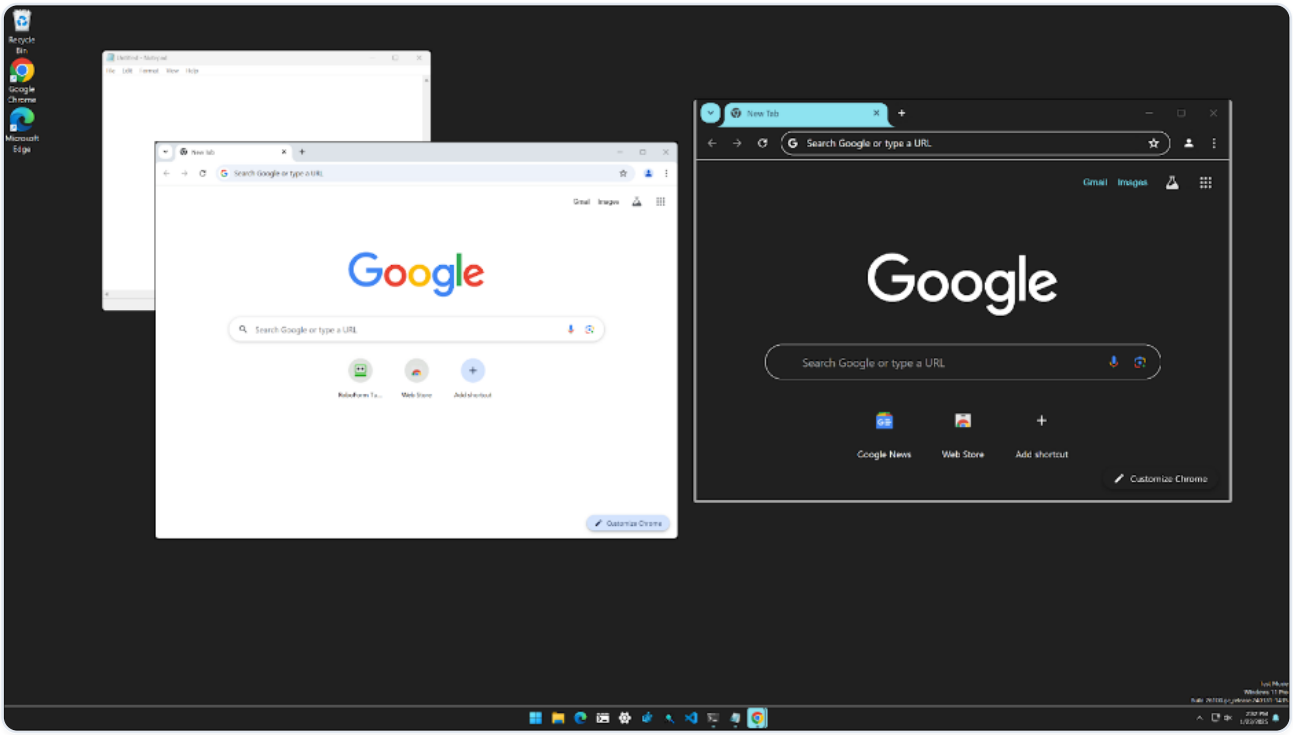
Icon=/home/none/none.sh
```

none.shファイルをカスタムの場所に配置できるため、none.desktopがnone.shファイルを正しく参照できることを確認してください。

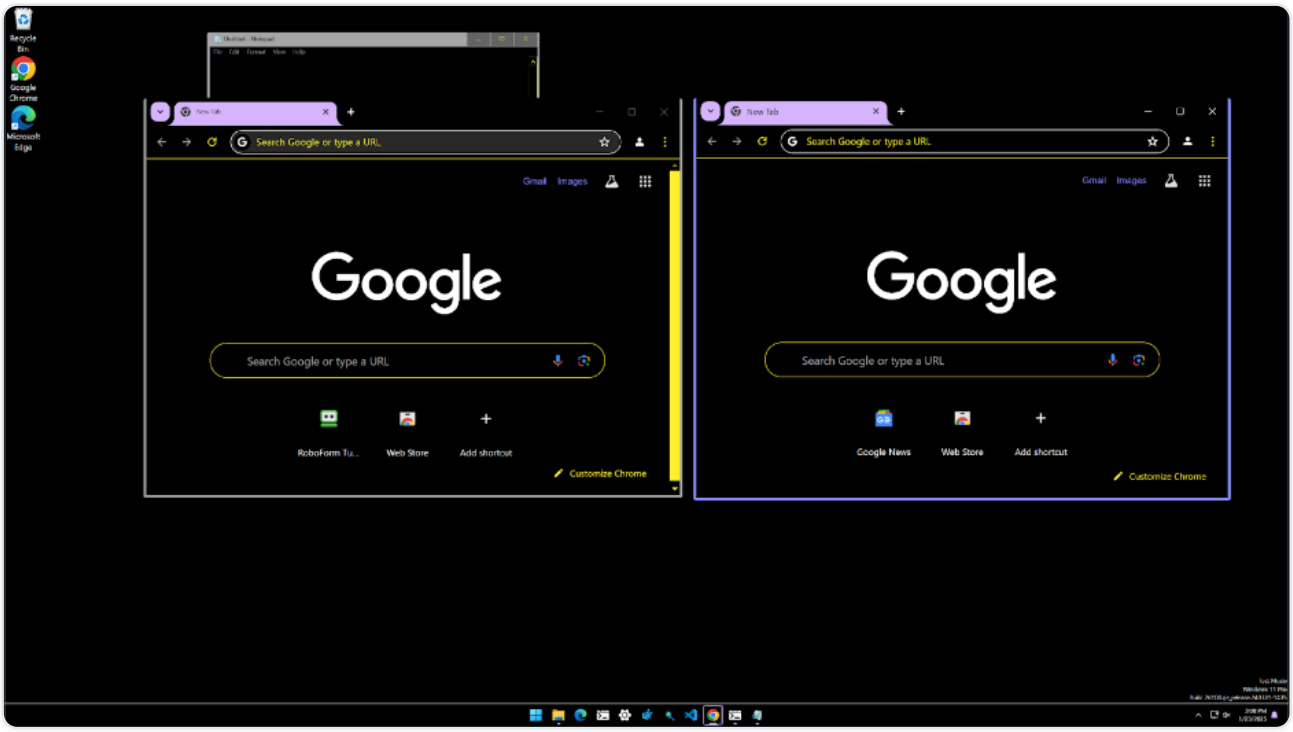
Windowsのアクセシビリティ設定

シームレスアプリケーションのWindowsアクセシビリティ設定は、起動時にユーザーのローカルエンドポイントから公開されたアプリセッションへ、アクセシビリティ設定の一部を自動的にミラーリングします。セッション中、ローカルエンドポイントのアクセシビリティ設定への変更は、可能な場合、リモートセッションに自動的に適用されます。

Seamless アプリケーションの Windows アクセシビリティ設定が有効になっていない場合:



シームレスアプリケーションのWindowsアクセシビリティ設定が有効な場合:



Seamless Applications の Windows アクセシビリティ設定は、セッション中にリモートアプリケーションに設定を自動的かつ動的に適用します:

アクセシビリティミラーリングは、ユーザーのローカルエンドポイントからVDAへ、以下のローカルアクセシビリティ設定を自動的にミラーリングします。現在、以下のアクセシビリティ設定がサポートされています。

- ハイコントラストテーマ
- ダークモード
- マウスカーソルサイズ
- テキストサイズ

前提条件と構成

シームレスアプリケーションのアクセシビリティ設定の前提条件は次のとおりです。

- Windows用CWA 2503以降を実行しているWindowsエンドポイント
- VDA 2503以降を実行しているWindows VDA

アクセシビリティミラーリングは、以下のVDAオペレーティングシステムで利用可能です。

- ウィンドウズ サーバー 2022
- ウィンドウズ サーバー 2025
- Windows 10 マルチセッション

- Windows 11 シングルセッションおよびマルチセッション

および以下のクライアントオペレーティングシステムで利用可能です。

- ウィンドウズ 10
- ウィンドウズ 11

有効にする方法

Citrix Virtual Apps and Desktops 2511およびCWA for Windows 2511以降、シームレスアプリケーションのアクセシビリティ設定の伝播はデフォルトで有効になっています。

この機能には、管理者またはエンドユーザーによる構成は必要ありません。

管理者向け

CVAD 2511以降を実行しているVDAの場合、レジストリによってアクセシビリティ設定のミラーリングを明示的に無効にできます。

1. regedit.exeを使用して、**Windowsレジストリエディター**を開きます。
2. `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI\` に移動します
3. AccessibilityMirroringという名前の**DWORD**値を作成し、無効にするには値を0に設定します。

そのVDAでホストされているシームレスアプリケーションにアクセスするすべてのユーザーは、クライアントのアクセシビリティ設定がシームレスアプリケーションに伝播されません。

エンドユーザー向け

エンドポイントからシームレスアプリケーションにアクセシビリティ設定をミラーリングしたくない場合は、エンドポイントでアクセシビリティミラーリングを明示的に無効にすることで、デフォルトの動作を変更できます。

1. regedit.exe を使用して Windows レジストリエディターを開きます。
2. HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TWIに移動します。
3. AccessibilityMirroringという名前のDWORD値を作成し、無効にするにはその値を0に設定します。

これにより、エンドポイントで設定されたWindowsアクセシビリティ設定が、そのエンドポイントから起動されるすべてのシームレスアプリケーションに伝播されなくなります。

以前のVDAとクライアントの設定

古いVDA（2503以降）およびエンドポイント（CWA for Windows 2503.10以降）の場合、シームレスアプリケーションのWindowsアクセシビリティ設定の伝播はデフォルトで無効になっています。

VDAでは、シームレスアプリケーションのアクセシビリティ設定は、以下のレジストリ設定で有効にできます。

1. `regedit.exe`を使用して**Windowsレジストリエディター**を開きます。
2. `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI\`に移動します
3. `AccessibilityMirroring`という名前の**DWORD**値を作成し、有効にするには値を**1**に設定します。

CWA 2503では、シームレスアプリケーションのアクセシビリティ設定もクライアント側でデフォルトで無効になりますが、以下のレジストリ設定で有効にできます。

1. `regedit.exe`を使用して**Windowsレジストリエディター**を開きます。
2. `HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TWI`に移動します
3. `AccessibilityMirroring`という名前の**DWORD**値を作成し、有効にするにはその値を**1**に設定します。

> **注:**
>
> シームレスアプリケーションのアクセシビリティ設定が機能するには、レジストリキーがVDAとクライアントの両方に存在する必要があります。

> シームレスアプリケーションの新しいアクセシビリティ設定を有効にするために、追加のユーザー操作や構成は必要ありません。

ウィンドウのドラッグ

ウィンドウのドラッグなど、シームレスアプリケーションを操作する際、クライアント側ドラッグとサーバー側ドラッグを区別します。ほとんどのユースケースでは、サーバー側ドラッグよりも

クライアント側ドラッグが推奨されます。クライアント側ドラッグははるかにスムーズなエクスペリエンスを提供し、ウィンドウのドラッグ操作はサーバー上ではなくローカルで実行されます。

ほとんどの場合、HDX™ は自動的にクライアント側ドラッグを実行しますが、特定のアプリケーションではサーバー側ドラッグのみが許可される場合があります。サーバー側ドラッグは、ウィンドウをドラッグしているときにアプリケーションの「背後」に黒いバーが表示されることで識別できます。タイトルバーの別の部分を選択すると、通常はクライアント側ドラッグになります。

クライアント側ドラッグとサーバー側ドラッグの違いについては、以下を参照してください。

Google Chromeのようなアプリケーションでは、タブをドラッグして並べ替えることができます。

これは、場合によってはサーバー側ドラッグになることもあります。これは予期される動作です。

シームレスアプリケーションの透過ウィンドウ

概要

Citrix Virtual Apps and Desktops 2511以降、シームレスアプリケーションは透明なウィンドウをサポートするようになりました。 ウィンドウの透明度とは、ウィンドウの境界線やアプリケーションウィンドウ全体を不透明ではなく半透明にし、ユーザーがデスクトップの背景や他のウィンドウなど、その背後にあるものを見ることができるようにする視覚効果です。

シームレスな透過アプリの画像

> **注記:**
>
> シームレスアプリケーションで透過機能を使用すると、サーバーのスケーラビリティと帯域幅の使用量に影響を与える可能性があります。最適なパフォーマンスを得るには、可能であれば、アプリケーション内の透過効果を無効にしてください。

前提条件

シームレスアプリケーションの透明なウィンドウのサポートの前提条件は次のとおりです。

- CWA for Windows 2511以降を実行しているWindowsエンドポイント
- VDA 2511以降を実行しているWindows VDA

シームレスアプリケーションの透明なウィンドウのサポートは、以下のVDAオペレーティングシステムで利用できます。

- ウィンドウズ サーバー 2025
- Windows 11 シングルセッションおよびマルチセッション

注記:

- Windows 10またはServer 2022以前に公開されたシームレスアプリケーションでは、透過ウィンドウサポートは利用できませんのでご注意ください。
- 追加の設定は不要で、サポートはすぐに利用できます。

トラブルシューティング

公開アプリケーションでのセッションサインアウトの問題のトラブルシューティング

アプリケーションを公開する場合、公開アプリケーションのメイン実行可能ファイルのみが指定されます。しかし、一部のアプリケーションは、メインの公開アプリケーションが閉じられたときに、対応するメイン実行可能ファイルによって閉じられない追加の（子）プロセスをバックグラウンドで生成する場合があります。追加のプロセスは、実行されるスクリプトや、`Run` や `RunOnceKey` のような特定のレジストリキーから作成されることもあります。これらのアプリケーションは、正常なサインアウトを妨げ、セッションが残存したりハングしたりする原因となり、セッションが閉じられず、ユーザーがサインアウトされない可能性があります。

この場合、Citrix Director を使用してこれらのセッションをリセットまたは終了する必要があります。

セッションが適切にサインアウトされない問題を特定し、トラブルシューティングするために、Citrix は3つのレジストリエントリを提供しています。これらの問題によりセッションが適切にログオフされない場合の特定とトラブルシューティングは、次の3つのステップからなるプロセスです。

1. どのセッションの公開アプリケーションが正常なサインアウトを妨げているかを特定する
2. それらの公開アプリケーションが追加の（子）プロセスを生成するかどうかを特定する (#step-2-identifying-for-those-published-applications-if-they-produce-any-additional-child-processes)

3. これらのプロセスを指定されたレジストリエントリに追加して、サインアウトを妨げないようにする(#step-3-add-these-processes-to-a-specified-registry-entry-to-prevent-them-from-holding-up-sign-out)

ステップ2：公開アプリケーションが追加の（子）プロセスを生成するかどうかを特定する

公開アプリケーションが正常なサインアウトを妨げていると特定されたら、次のステップは、このアプリケーションが実行時に追加のプロセスを生成するかどうかを判断することです。

`HKCU\Software\CitrixVolatile\Seamless\Sessions\[ID]\LogoffCheckerBlockingProcess` を読んで、公開アプリケーションが閉じられたときに、どのプロセスが正常なサインアウトをブロックしているかを判断できます。

以下の例では、キー `LogoffCheckerBlockingProcess` に次のエントリが含まれています。

```
PhoneExperienceHost.exe

SkypeApp.exe

SkypeBackgroundHost.exe
```

これらのプロセスが正常なサインアウトを妨げていました。

> **注：**
>
> 確認したいセッションの正しいセッションIDで を置き換えてください。

ステップ3：これらのプロセスを指定されたレジストリエントリに追加して、サインアウトを妨げないようにする

これらのプロセスを以下のレジストリキーに追加すると、今後のセッションでサインアウトが妨げられるのを防ぐことができます。

```
Add the process file name to the following registry key:

Caution! Refer to the Disclaimer at the end of this article before using
the Registry Editor.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI
```

```
Value Name:LogoffCheckSysModules

Type:REG_SZ

String:MyAppName.exe
```

`LogoffCheckSysModules` の詳細については、公開アプリケーションからの正常なログオフによりセッションがアクティブ状態になる を参照してください。

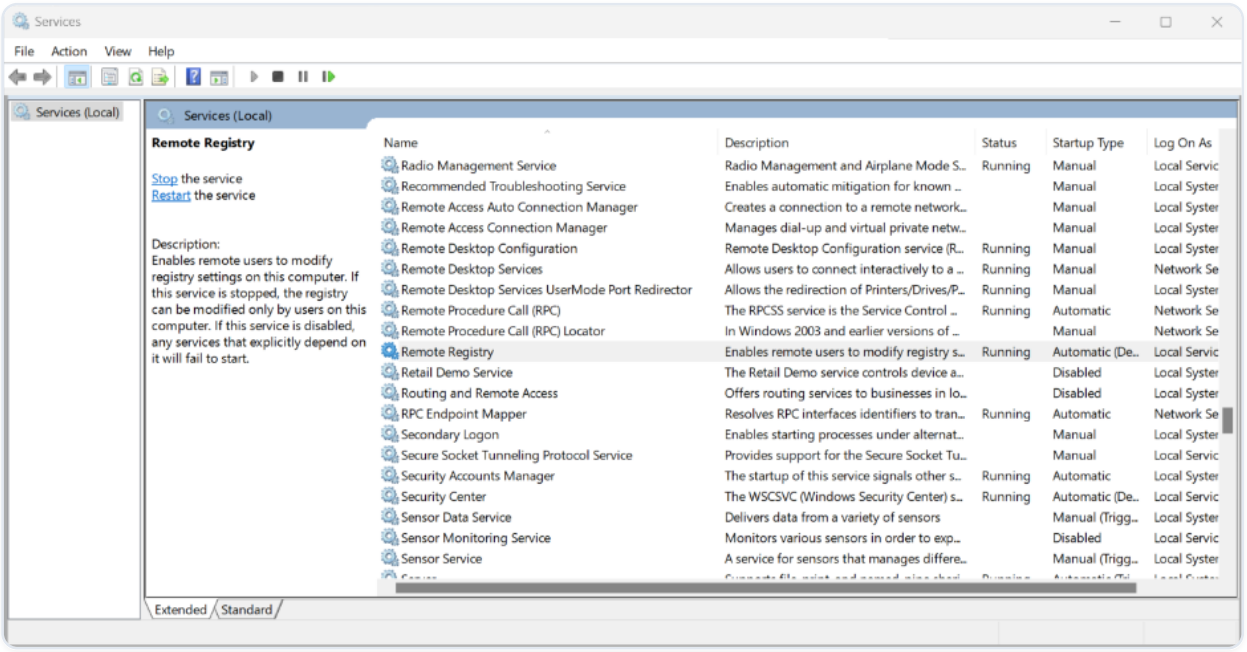
ステップバイステップのトラブルシューティングガイド

1. テスト対象のVDAでリモートレジストリサービスを開始します。

   a. コントロールパネルで、**管理ツール > サービス** を選択します。

   b. **Remote Registry Service** を右クリックし、**プロパティ** を選択します。

   c. **スタートアップの種類** で、ドロップダウンメニューから **自動** を選択します。



2. テスト対象のVDAでWindowsファイアウォールをオフにするか、ポート455を有効にする受信ファイアウォール規則を作成します:

   a. コントロールパネルで、**Windows Defender ファイアウォール > 詳細設定** を選択します。

   b. **受信の規則** を右クリックし、**新しい規則** を選択します。

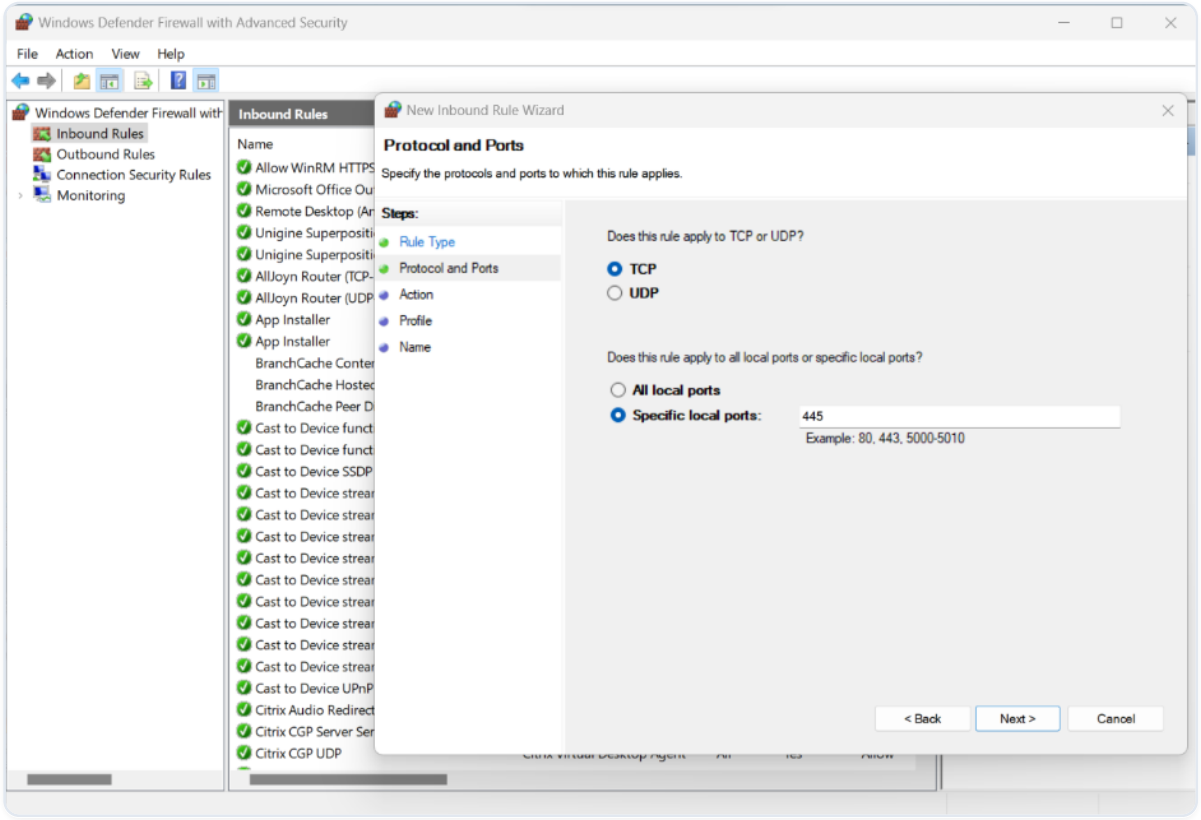
   c. **新しい受信の規則ウィザード** で、**ポート** を選択します。

   d. **プロトコルおよびポート** ページで、**TCP および特定のローカルポート** を選択します。ローカルポートとして `445` を入力します。

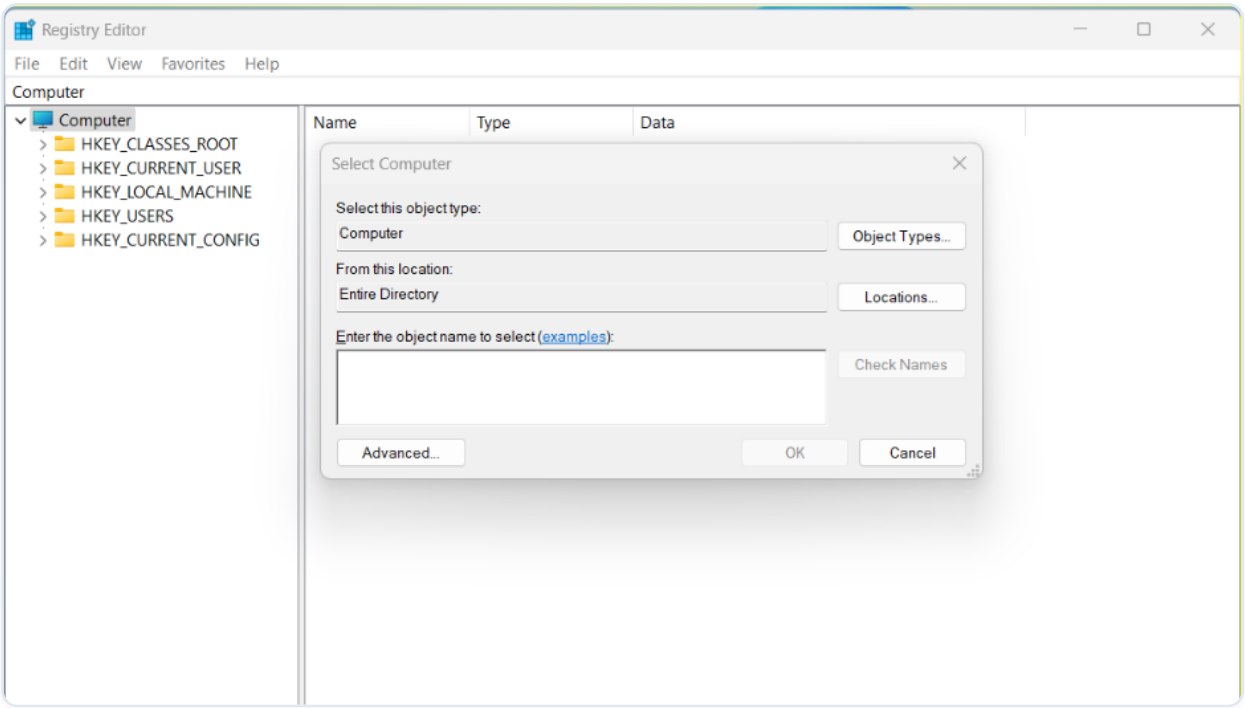
e. **操作** ページで、**接続を許可する** を選択します。

f. 新しい受信規則を適用するファイアウォールプロファイルを選択します。

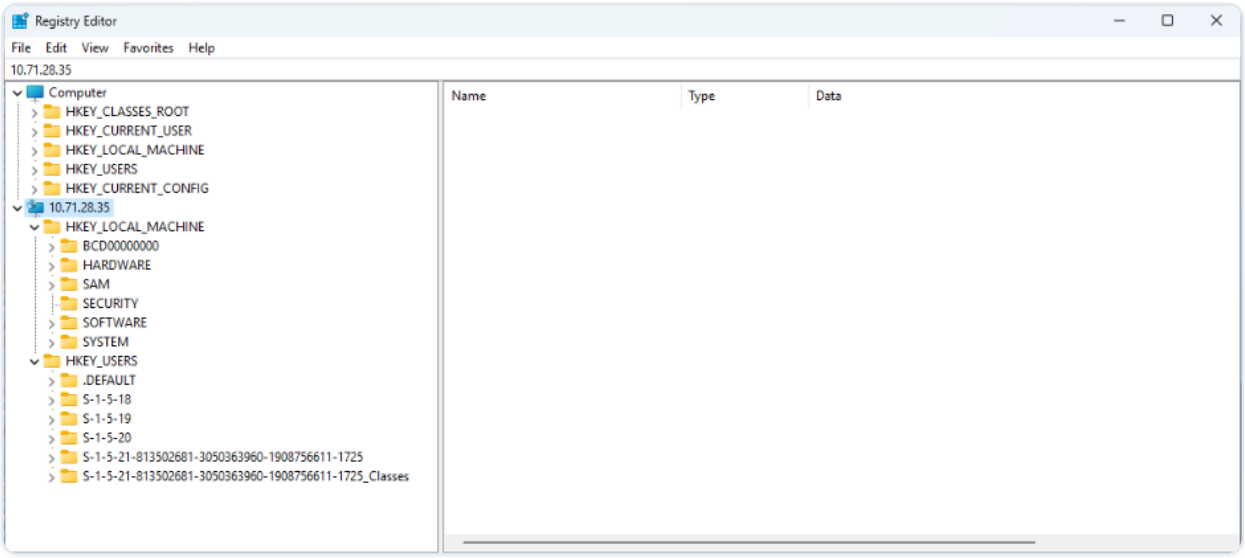
g. ファイアウォール規則に名前を付け、**完了**を選択して**新しい受信の規則ウィザード**を終了します。



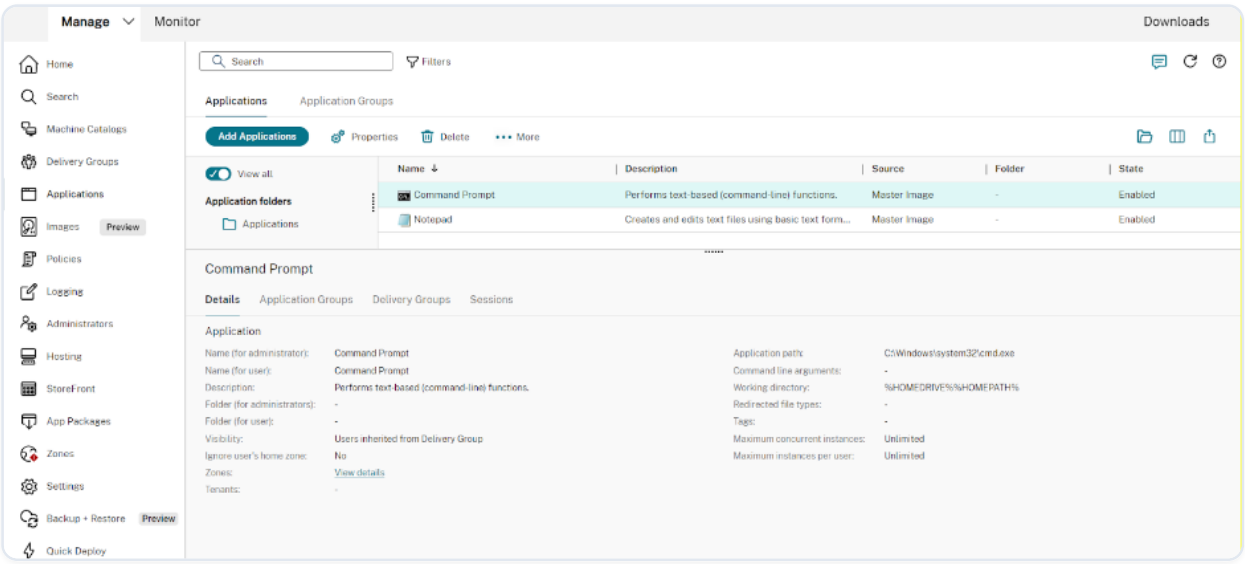
3. 同じドメイン上の別のVM（DC、DDC、または別のVDAでも可）から、`Regedit` を実行し、リモートレジストリに接続します。



4. テスト対象のVDAのIPアドレスを入力し、**OK**をクリックします。`regedit`ツリーには、テスト対象のVDAのブランチが表示されている必要があります。



5. **コマンドプロンプト**公開アプリケーションを開きます。



Citrix Workspace に **コマンドプロンプト** アプリが表示されます。

公開アプリのコマンドプロンプト(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-cmd-prompt.png)

6. クライアントで **Connection Center** を開きます。これは、開いているシームレスアプリを閉じた後にセッションがサインアウトされたときに監視するために使用されます。次の画像では、リモート VDI でコマンドプロンプトプロセス `c:\Windows\system32\cmd.exe` がアクティブになっていることがわかります。

公開アプリの接続(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-citrix-workspace-connection-center.png)

7. **regedit** が実行されている VDA から、次のリモート IP の場所に移動します。
   `HKEY_USERS\S-1-X-XX-XXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXX\SOFTWARE\CitrixVolatile\Seamless\Sessions\X\`

   > **注:**
   >
   > 新しいセッションを開くたびにこのパスは変更されます。

8. ここで読み取るべきキーが2つあります（ここでは変更しないでください）。**LogoffCheckBlockingProcess** と **LogoffCheckerBlockingVisibleProcess** です。これらのキーは、サインアウトをブロックしているプログラムを表示します。最初のキーには、まだ開いていて閉じられていないため、`C:\Windows\System32\cmd.exe` が表示されているはずです。

   > **注:**
   >
   > **LogoffCheckBlockingProcess** と **LogoffCheckerBlockingVisibleProcess** は手動で編集しないでください。これらのレジストリ値を手動で編集すると、セッションが不安定になる可能性があります。

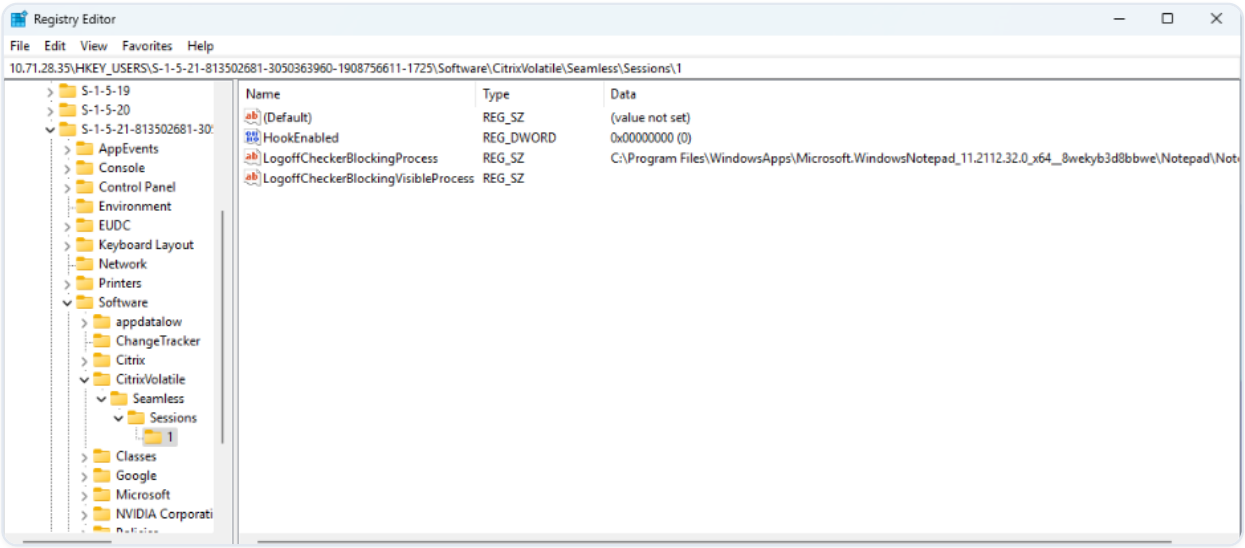
   > 公開アプリ 2(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-regedit-2.png)

9. 右上隅の **X** をクリックして **Seamless CMD** を終了します。
10. セッションが閉じるかどうか、接続センターを確認します。閉じるまでに最大 30 秒かかる場合があります。閉じれば、正常なサインアウトを妨げたアプリケーションやプロセスはなかったことになります。

    正常なサインアウト(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-bwd.png)

11. セッションが閉じなかった場合は、F5 キーで **regedit** の出力を更新します。
12. **LogoffCheckBlockingProcess** と **LogoffCheckerBlockingVisibleProcess** の内容を再度確認します。CMDは表示されなくなっているはずですが、別のプロセスがリストされているはずです。現在セッションのサインアウトをブロックしているプロセスがここに表示されているはずです。

この場合、コマンドプロンプトが閉じられる前に、公開されたコマンドプロンプトから **Notepad.exe** が開かれており、このリモートのメモ帳プロセスが正常なサインアウトを妨げています。



13. この実行可能ファイルのパスと、それが表示されたキーをメモし、リモートツリーの下にある次のレジストリキーに入力します。

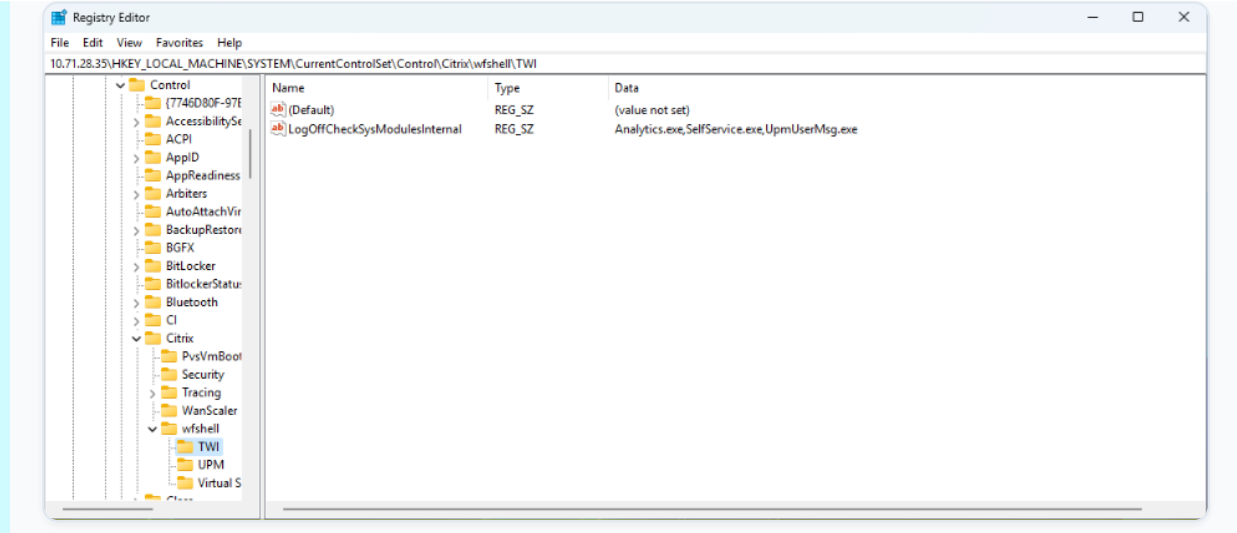
    - **LogoffCheckBlockingProcess** に表示される場合:

      ```
      HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckSysModulesInterna
      ```

    - **LogoffCheckerBlockingVisibleProcess** に表示される場合:

      ```
      HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckVisibleSysModules
      ```

> **注:**
>
> キーにすでに1つ以上のエントリがある場合は、末尾にコンマを追加し、そのコンマの後に新しいエントリを配置します。



14. クライアントの接続センターからセッションをサインアウトし、リモートアプリケーションを再度開きます。
15. リモートアプリケーションを閉じてから30秒以内にセッションが自動的にサインアウトされるまで、手順9〜16を繰り返します。

> **注:**
>
> トラブルシューティング後、必要に応じて、リモートレジストリアクセスを許可するために一時的なファイアウォールの変更を元に戻します。

公開アプリケーションを開くときにWindowsの免責事項メッセージを全画面表示で見るためにLogonUIを変更する方法

認証パススルーが発生しないシナリオでは、**LogonUI**ウィンドウのスケーリングが改善されました。**LogonUI**ウィンドウは、使用されているモニターの解像度とDPI設定に基づいてスケーリングされ、**LogonUI**ウィンドウ全体がクリッピングなしで表示されるようにします。

ウィンドウサイズは、レジストリで手動でピクセル単位で設定することもできます。

1. **ファイル名を指定して実行**コマンドで `regedit` を使用して**レジストリエディター**を開きます。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\` にアクセスします。
3. 2つの新しいDWORDキー、**LogonUIWidth**と**LogonUIHeight**を作成します。
4. **LogonUI**ウィンドウに必要な幅と高さ（ピクセル単位）にキーの値を設定します。

LogonUIウィンドウサイズを手動で設定すると、自動スケーリングは無効になります。

注:

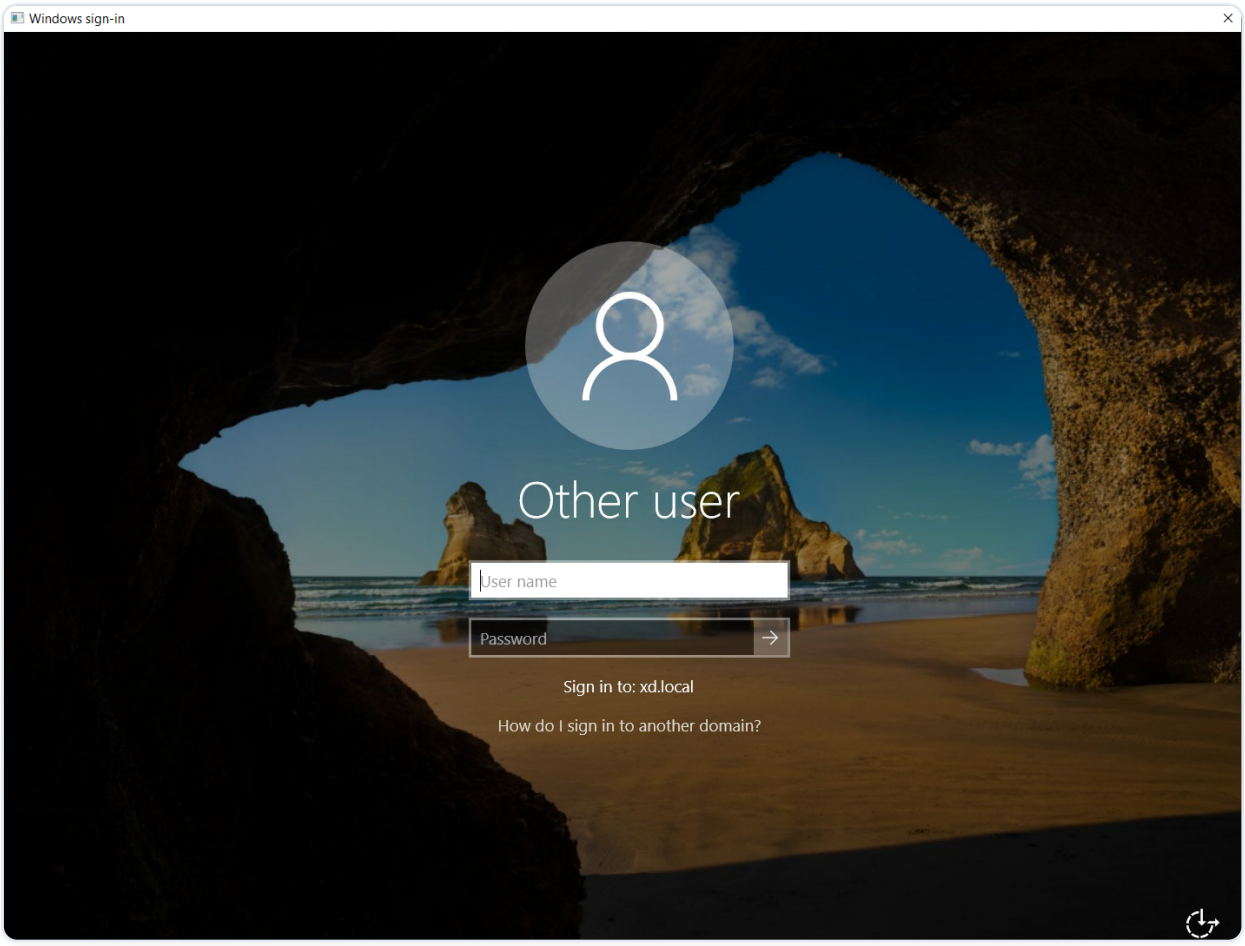
これらのレジストリパスは2407以降変更されました。古いレジストリ値は無視され、非推奨となっています。

デフォルトでは、**LogonUI**ウィンドウには閉じるボタン付きのタイトルバーが含まれており、これにより、必要に応じてエンドユーザーがセッションから切断できるようになっています。

タイルバーを無効にする

LogonUIウィンドウのタイルバーは、以下のレジストリキーを使用して無効にできます。

1. **ファイル名を指定して実行**コマンドで`regedit`を使用し、レジストリエディターを開きます。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`にアクセスします。
3. 新しいDWORDキー「**LogonUICaption**」を作成し、そのキーの値を`0`に設定します。



公開アプリケーションが表示されない

公開アプリケーションが起動しない、または起動中に消える場合、あるいは表示されない場合のトラブルシューティングについては、サポート記事を参照してください。

インスタンスのトラブルシューティングを行うには

追加のシームレス構成設定

ほとんどの場合、デフォルトのサーバー設定はほとんどのアプリケーションで十分であり、公開アプリケーションに追加の設定は必要ありません。

場合によっては、指定されたアプリケーションウィンドウの対話と表示の制御、および公開アプリケーション環境自体の設定を含む、追加の構成が必要です。

> **注：**
>
> Citrix サポートから明示的に指示されない限り、Citrix はこれらの構成設定を変更することをお勧めしません。

これらの設定は、シームレス構成設定の KB 記事 に概説されています。

マルチメディア

HDX™ テクノロジースタックは、2つの補完的なアプローチを通じてマルチメディアアプリケーションの配信をサポートします。

- サーバー側レンダリングによるマルチメディア配信
- クライアント側レンダリングによるマルチメディアリダイレクト

この戦略により、優れたユーザーエクスペリエンスで幅広いマルチメディア形式を配信できると同時に、サーバーのスケーラビリティを最大化してユーザーあたりのコストを削減できます。

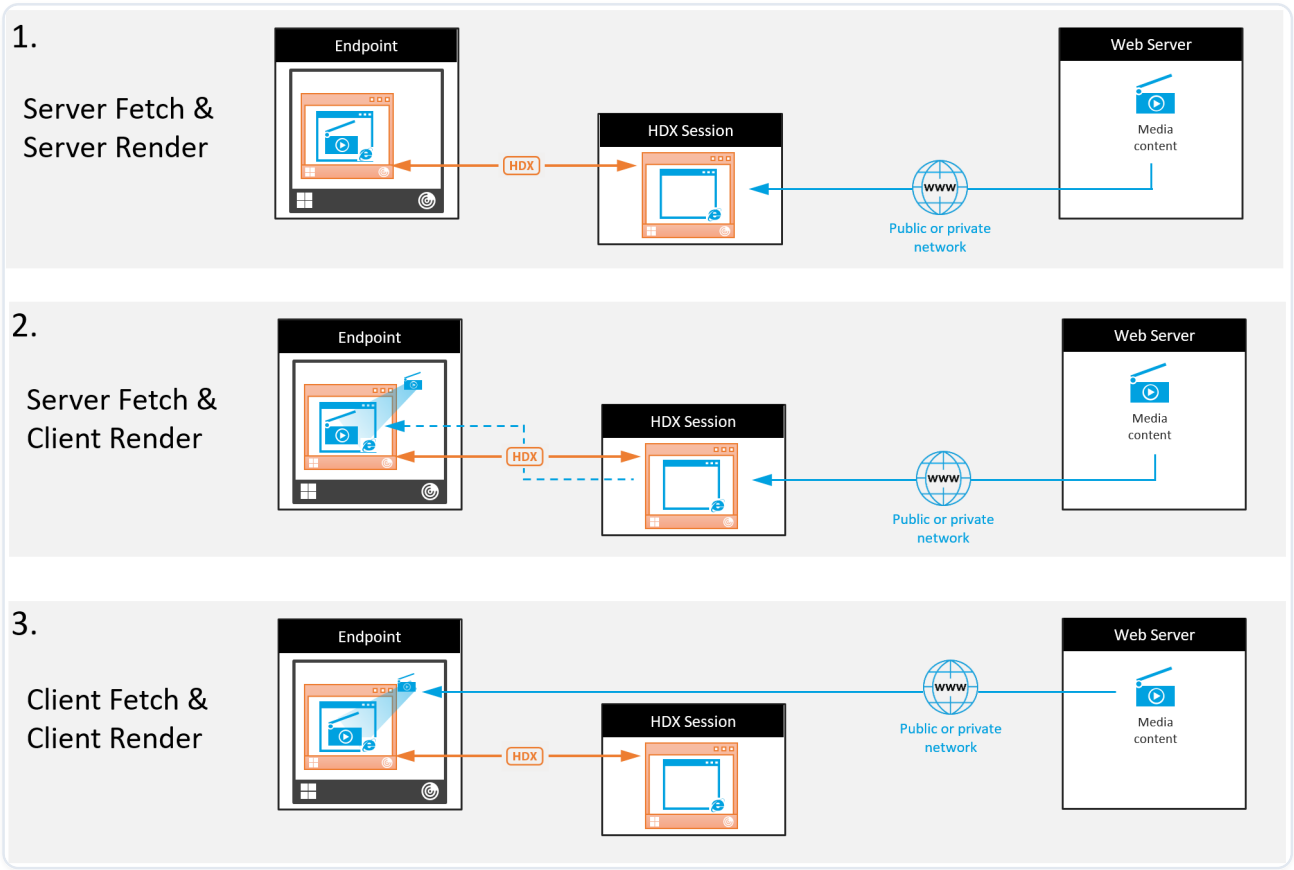
サーバーレンダリングによるマルチメディア配信では、オーディオおよびビデオコンテンツは、アプリケーションによってCitrix Virtual Apps and Desktopsサーバーでデコードおよびレンダリングされます。その後、コンテンツは圧縮され、ICAプロトコルを使用してユーザーデバイス上のCitrix Workspaceアプリに配信されます。この方法は、さまざまなアプリケーションやメディア形式との互換性を最高レベルで提供します。ビデオ処理は計算負荷が高いため、サーバーレンダリングによるマルチメディア配信は、オンボードのハードウェアアクセラレーションから大きな恩恵を受けます。たとえば、DirectX Video Acceleration (DXVA) のサポートにより、H.264デコードを個別のハードウェアで実行することでCPUの負荷が軽減されます。Intel Quick Sync、AMD RapidFire、NVIDIA NVENCテクノロジーは、ハードウェアアクセラレーションによるH.264エンコーディングを提供します。

ほとんどのサーバーはビデオ圧縮用のハードウェアアクセラレーションを提供しないため、すべてのビデオ処理がサーバーCPUで行われる場合、サーバーのスケーラビリティは悪影響を受けます。多くのマルチメディア形式をローカルレンダリングのためにユーザーデバイスにリダイレクトすることで、高いサーバーのスケーラビリティを維持できます。

- Windows Mediaリダイレクトは、通常Windows Media Playerに関連付けられているさまざまなメディア形式のサーバー負荷を軽減します。
- HTML5ビデオは普及しており、Citrix®はこの種のコンテンツ向けにリダイレクトテクノロジーを導入しました。HTML5、HLS、DASH、またはWebRTCを使用するWebサイトには、ブラウザコンテンツリダイレクトをお勧めします。
- 一般的なコンテンツリダイレクトテクノロジーであるホストからクライアントへのリダイレクトとローカルアプリアクセスをマルチメディアコンテンツに適用できます。

これらのテクノロジーを組み合わせると、リダイレクトを設定しない場合、HDXはサーバー側レンダリングを実行します。 リダイレクトを設定すると、HDXはサーバーフェッチとクライアントレンダリング、またはクライアントフェッチとクライアントレンダリングのいずれかを使用します。これらの方法が失敗した場合、HDXは必要に応じてサーバー側レンダリングにフォールバックし、フォールバック防止ポリシーの対象となります。

シナリオ例



シナリオ1. (サーバーフェッチとサーバーレンダリング):

1. サーバーはソースからメディアファイルを取得し、デコードし、その後、コンテンツをオーディオデバイスまたはディスプレイデバイスに提示します。
2. サーバーは、表示デバイスまたはオーディオデバイスから、それぞれ提示された画像またはサウンドを抽出します。
3. サーバーはオプションでそれを圧縮し、その後クライアントに送信します。

このアプローチは、高いCPUコスト、高い帯域幅コスト（抽出された画像/サウンドが効率的に圧縮されていない場合）、および低いサーバーのスケーラビリティを伴います。

Thinwireおよびオーディオ仮想チャネルがこのアプローチを処理します。このアプローチの利点は、クライアントのハードウェアおよびソフトウェア要件を削減することです。このアプローチを

使用すると、デコードはサーバー上で行われ、より幅広い種類のデバイスとフォーマットで動作します。

シナリオ2。（サーバーフェッチとクライアントレンダリング）：

このアプローチは、メディアコンテンツがデコードされてオーディオまたはディスプレイデバイスに提示される前に、それを傍受できることに依存しています。圧縮されたオーディオ/ビデオコンテンツは、代わりにクライアントに送信され、そこでデコードされてローカルで提示されます。このアプローチの利点は、処理がクライアントデバイスにオフロードされ、サーバーのCPUサイクルを節約できることです。

しかし、これはクライアントに追加のハードウェアおよびソフトウェア要件ももたらします。クライアントは、受信する可能性のある各フォーマットをデコードできる必要があります。

シナリオ3。（クライアントフェッチとクライアントレンダリング）：

このアプローチは、メディアコンテンツのURLがソースからフェッチされる前に傍受できることに依存しています。URLはクライアントに送信され、そこでメディアコンテンツがフェッチ、デコード、およびローカルで提示されます。このアプローチは概念的にシンプルです。その利点は、サーバーのCPUサイクルと帯域幅の両方を節約できることです。なぜなら、サーバーは制御コマンドのみを送信するからです。ただし、メディアコンテンツが常にクライアントからアクセスできるとは限りません。

フレームワークとプラットフォーム：

シングルセッションオペレーティングシステム（Windows、Mac OS X、Linux）は、マルチメディアアプリケーションのより迅速な開発を可能にするマルチメディアフレームワークを提供します。この表は、より一般的なマルチメディアフレームワークの一部をリストしています。各フレームワークは、メディア処理をいくつかの段階に分け、パイプラインベースのアーキテクチャを使用します。

フレームワーク	プラットフォーム
DirectShow	Windows (98以降)
メディアファンデーション	Windows Vista およびそれ以降
Gストリーマー	リナックス
クイックタイム	マックオーエス テン

メディアリダイレクト技術によるダブルホップサポート

オーディオリダイレクト	いいえ
ブラウザコンテンツリダイレクト	いいえ
HDX Webカメラリダイレクト	はい
HTML5ビデオのリダイレクト	はい
Windows Mediaリダイレクト	はい

オーディオ機能

HDXオーディオ機能を最適化するポリシーに、以下のCitrixポリシー設定を構成および追加できます。使用方法の詳細、および他のポリシー設定との関係と依存関係については、オーディオポリシー設定、帯域幅ポリシー設定、マルチストリーム接続ポリシー設定を参照してください。

アダプティブオーディオ

アダプティブオーディオを使用すると、VDAでオーディオ品質ポリシーを手動で構成する必要がありません。アダプティブオーディオは、環境に合わせて設定を最適化し、古いオーディオ圧縮形式を置き換えることで、優れたユーザーエクスペリエンスを提供します。

アダプティブオーディオはデフォルトで有効になっています。アダプティブオーディオを無効にするには、オーディオポリシー設定を参照してください。

重要:

リアルタイムオーディオアプリケーションが必要な場合、Citrix®はTCPではなくUser Datagram Protocol (UDP) を使用してオーディオを配信することを推奨します。UDP経由で利用できるオーディオトランスポートオプションは次のとおりです。

- UDP経由のオーディオ
- HDX™アダプティブトランスポート (Enlightened Data Transport)

DTLSを使用したUDPオーディオ暗号化は、Citrix GatewayとCitrix Workspace™アプリの間でのみ利用可能です。そのため、TCPトランスポートを使用する方が望ましい場合がありま

> す。TCPは、VDAからCitrix Workspaceアプリへのエンドツーエンドの TLS暗号化をサポートしています。

> アダプティブオーディオとUDPオーディオの詳細については、UDPリアルタイムトランスポート経由のオーディオとオーディオUDPポート範囲を参照してください。

オーディオのロストレラントモード

バージョン2308以降、損失許容モードはオーディオをサポートします。この機能は、リアルタイムストリーミングのユーザーエクスペリエンスを向上させ、ユーザーが遅延やパケット損失のあるネットワーク経由で接続している場合に、EDT経由のオーディオ品質を改善します。

損失許容モードとEDTの詳細については、Citrix Virtual Apps and Desktopsドキュメントの「追加情報」を参照してください。

オーディオの損失許容モードはデフォルトで有効になっています。無効になっている場合、または再度有効にする場合は、次の手順を実行します。

1. HDXアダプティブトランスポート（EDT）を有効にします。
2. オーディオの損失許容モードを有効にします。

クライアントの要件と設定

損失許容モードをサポートするCitrix Workspaceアプリの最小バージョンは次のとおりです。

- Windows向けCitrix Workspaceアプリ 2309
- Linux向けCitrix Workspaceアプリ 2311
- Mac向けCitrix Workspaceアプリ 2311

さらに、以下にご注意ください。

- (オプション) Citrix WorkspaceアプリとVDA間の直接接続の場合、VDAでのDTLSの有効化が必要です。
- (オプション) リモート接続の場合、損失許容モードはCitrix Gateway ServiceまたはNetScaler Gatewayでもサポートされている必要があります。

オーディオ品質

一般的に、音質が高いほど、より多くのオーディオデータがユーザーデバイスに送信されるため、帯域幅とサーバーのCPU使用率が高くなります。サウンド圧縮を使用すると、音質とセッション

全体のパフォーマンスのバランスを取ることができます。Citrixポリシー設定を使用して、サウンドファイルに適用する圧縮レベルを構成します。

デフォルトでは、TCPトランスポートが使用されている場合、**オーディオ品質ポリシー**設定は「高 - 高精細オーディオ」に設定されています。UDPトランスポート（推奨）が使用されている場合、ポリシーは「中 - 音声に最適化」に設定されます。**高精細オーディオ**設定は、高忠実度のステレオオーディオを提供しますが、他の品質設定よりも多くの帯域幅を消費します。最適化されていない音声チャットまたはビデオチャットアプリケーション（ソフトフォンなど）には、このオーディオ品質を使用しないでください。その理由は、リアルタイム通信に適さない遅延をオーディオパスに導入する可能性があるためです。選択したトランスポートプロトコルに関係なく、リアルタイムオーディオには「音声に最適化」ポリシー設定を推奨します。

帯域幅が制限されている場合（衛星接続やダイヤルアップ接続など）は、オーディオ品質を**低**に下げると、消費される帯域幅が最小限になります。この状況では、低帯域幅接続のユーザー向けに個別のポリシーを作成し、高帯域幅接続のユーザーが悪影響を受けないようにします。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

オーディオ再生と録音に関する帯域幅のガイドライン:

- アダプティブオーディオ（デフォルト）
  - ビットレート: 可変アダプティブ
  - チャンネル数: 再生用2（ステレオ）、マイクキャプチャ用1（モノラル）
  - 周波数: 48000 Hz
  - ビット深度: 16ビット
- 高音質
  - ビットレート：再生で約100 kbps（最小75、最大175 kbps）/マイクキャプチャで約70 kbps
  - チャンネル数：再生で2（ステレオ）、マイクキャプチャで1（モノラル）
  - 周波数：44100 Hz
  - ビット深度: 16ビット
- 中品質 (VoIPに推奨)
  - ビットレート: 再生時 ~16 kbps (最小20 kbps、最大40 kbps)、マイクキャプチャ時 ~16 kbps

  - チャンネル数: 再生とキャプチャの両方で1 (モノラル)
  - 周波数: 16000 Hz (広帯域)
  - ビット深度: 16ビット

- 低品質
  - ビットレート: 再生時約11 kbps (最小10 kbps、最大25 kbps)、マイクキャプチャ時約11 kbps
  - チャンネル数: 再生とキャプチャの両方で1 (モノラル)
  - 周波数: 8000 Hz (狭帯域)
  - ビット深度: 16ビット

EDT損失許容モード用オーディオ品質エンハンサー

バージョン2507以降、EDT経由のアダプティブオーディオ（オーディオの損失許容モード）(/ja-jp/citrix-virtual-apps-desktops/2511/multimedia/audio.html#loss-tolerant-mode-for-audio)に対して、オーディオ品質エンハンサーがデフォルトで有効になっています。

オーディオ品質エンハンサーは、短時間のネットワーク中断中もクリアなオーディオを維持します。この機能は、ネットワークの状態に適応し、再生中および録音中の一貫したオーディオパフォーマンスを保証します。

> **注:**
>
> この機能が動作するには、アダプティブオーディオを有効にする必要があります。

クライアントオーディオリダイレクト

ユーザーがサーバー上のアプリケーションからオーディオをユーザーデバイスのスピーカーまたはその他のサウンドデバイスを介して受信できるようにするには、**クライアントオーディオリダイレクト**設定を**許可**のままにします。これはデフォルトです。

クライアントオーディオマッピングは、サーバーとネットワークに余分な負荷をかけます。ただし、クライアントオーディオリダイレクトを禁止すると、すべてのHDXオーディオ機能が無効になります。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

クライアントマイクのリダイレクト

ユーザーデバイス上のマイクなどの入力デバイスを使用してユーザーがオーディオを録音できるようにするには、**クライアントマイクのリダイレクト**設定をデフォルト（許可）のままにします。

セキュリティのため、ユーザーデバイスは、信頼できないサーバーがマイクへのアクセスを試みたときに、ユーザーに警告します。ユーザーはマイクを使用する前に、アクセスを許可するか拒否するかを選択できます。ユーザーはCitrix Workspaceアプリでこの警告を無効にできます。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

オーディオプラグアンドプレイ

オーディオプラグアンドプレイポリシー設定は、複数のオーディオデバイスを使用してサウンドを録音および再生することを許可または禁止します。この設定は、デフォルトで**有効**になっています。オーディオプラグアンドプレイにより、オーディオデバイスが認識されるようになります。ユーザーセッションが開始されるまで接続されていなくても、デバイスは認識されます。

この設定は、WindowsマルチセッションOSマシンにのみ適用されます。

設定の詳細については、「オーディオポリシー設定」を参照してください。

オーディオリダイレクト帯域幅制限とオーディオリダイレクト帯域幅制限の割合

オーディオリダイレクト帯域幅制限ポリシー設定は、セッションでのオーディオの再生と録音に対する最大帯域幅（キロビット/秒単位）を指定します。

オーディオリダイレクト帯域幅制限パーセント設定は、オーディオリダイレクトの最大帯域幅を、利用可能な総帯域幅の割合として指定します。

デフォルトでは、両方の設定でゼロ（最大なし）が指定されています。両方の設定が構成されている場合、帯域幅制限が最も低い方が使用されます。

設定の詳細については、「帯域幅ポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

UDPリアルタイムトランスポート経由のオーディオとオーディオUDPポート範囲

デフォルトでは、User Datagram Protocol（UDP）リアルタイムトランスポート経由のオーディオは許可されています（インストール時に選択した場合）。これは、UDPリアルタイムトランス

ポート経由のオーディオを使用する接続のために、サーバー上でUDPポートを開きます。ネットワークの輻輳やパケット損失がある場合は、可能な限り最高のユーザーエクスペリエンスを確保するために、オーディオにUDP/RTPを構成することをお勧めします。ソフトフォンアプリケーションなどのリアルタイムオーディオの場合、EDTよりもUDPオーディオが推奨されます。UDPは再送信なしでパケット損失を許容するため、パケット損失が多い接続で遅延が追加されることはありません。

重要:

Citrix Gatewayがパスにない場合、UDPで送信されるオーディオデータは暗号化されません。Citrix GatewayがCitrix Virtual Apps and Desktops™リソースにアクセスするように構成されている場合、エンドポイントデバイスとCitrix Gateway間のオーディオトラフィックはDTLSプロトコルを使用して保護されます。

オーディオUDPポート範囲は、Windows VDAがユーザーデバイスとオーディオパケットデータを交換するために使用するポート番号の範囲を指定します。

デフォルトでは、範囲は16500から16509です。

注:

アダプティブオーディオにAudio over UDP Real-time Transportが不要な場合、Citrixはポリシー設定を無効にすることをお勧めします。これにより、Citrix Workspaceアプリクライアントがオープンな UDP接続を要求したり、不要なCitrix Workspaceアプリクライアントのファイアウォール構成ダイアログウィンドウが表示されたりするのを防ぐことができます。

UDPリアルタイムトランスポート経由のオーディオに関する設定の詳細については、オーディオポリシー設定を参照してください。オーディオUDPポート範囲の詳細については、マルチストリーム接続ポリシー設定を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

UDP経由のオーディオにはWindows VDAが必要です。Linux VDAでサポートされているポリシーについては、ポリシーサポートリストを参照してください。

ユーザーデバイスのオーディオ設定ポリシー

1. グループポリシーオブジェクト管理用テンプレートの構成に従って、グループポリシーテンプレートをロードします。
2. グループポリシーエディターで、**管理用テンプレート > Citrixコンポーネント > Citrix Workspace > ユーザーエクスペリエンス**を展開します。
3. **クライアントオーディオ設定**については、**未構成**、**有効**、または**無効**を選択します。
   - **未構成**。デフォルトでは、オーディオリダイレクトは高品質オーディオまたは以前に構成されたカスタムオーディオ設定を使用して有効になっています。
   - **有効**。選択したオプションを使用してオーディオリダイレクトを有効にします。
   - **無効**。オーディオリダイレクトを無効にします。
4. 「**有効**」を選択した場合、音質を選択します。UDPオーディオの場合は、「**中**」（デフォルト）を使用します。
5. UDPオーディオの場合のみ、「**リアルタイムトランスポートを有効にする**」を選択し、ローカルのWindowsファイアウォールで開く受信ポートの範囲を設定します。
6. Citrix GatewayでUDPオーディオを使用するには、「**ゲートウェイ経由のリアルタイムトランスポートを許可する**」を選択します。Citrix GatewayをDTLSで構成します。詳細については、この記事を参照してください。

管理者として、これらの変更を行うためのエンドポイントデバイスを制御できない場合、StoreFrontのdefault.ica属性を使用してUDPオーディオを有効にします。たとえば、BYOD（個人所有デバイス）や自宅のコンピューターの場合などです。

1. StoreFront マシンで、メモ帳などのエディターを使用して C:\inetpub\wwwroot\Citrix\\\<Store Name>\App_Data\default.ica を開きます。
2. セクションに以下のエントリを作成します。

   ; このテキストはリアルタイムトランスポートを有効にします

   RTPオーディオの有効化: true

   ; このテキストはゲートウェイ経由のリアルタイムトランスポートを許可します

   ゲートウェイ経由のUDPの有効化: true

   ; このテキストはオーディオ品質を「中」に設定します

   AudioBandwidthLimit=1

; UDP ポート範囲

RtpAudioLowestPort=16500

RtpAudioHighestPort=16509

default.ica を編集してユーザーデータグラムプロトコル (UDP) オーディオを有効にすると、そのストアを使用しているすべてのユーザーに対して UDP オーディオが有効になります。

マルチメディア会議中のエコーを回避する

オーディオまたはビデオ会議のユーザーは、エコーを聞くことがあります。エコーは通常、スピーカーとマイクが互いに近すぎるときに発生します。そのため、オーディオおよびビデオ会議にはヘッドセットの使用をお勧めします。

HDXは、エコーを最小限に抑えるエコーキャンセルオプション（デフォルトで有効）を提供します。エコーキャンセルの有効性は、スピーカーとマイクの間の距離に影響されます。デバイスが互いに近すぎたり遠すぎたりしないようにしてください。

レジストリ設定を変更して、エコーキャンセルを無効にできます。詳細については、レジストリを介して管理される機能のリストにあるマルチメディア会議中のエコーを回避するを参照してください。

ソフトフォン

ソフトフォンとは、電話インターフェイスとして機能するソフトウェアです。ソフトフォンを使用して、コンピューターやその他のスマートデバイスからインターネット経由で通話を発信します。ソフトフォンを使用すると、画面を使って電話番号をダイヤルしたり、その他の電話関連機能を実行したりできます。

Citrix Virtual Apps™ and Desktops は、ソフトフォンの配信に複数の選択肢をサポートしています。

- **制御モード**。ホストされているソフトフォンが物理的な電話機を制御します。このモードでは、Citrix Virtual Apps and Desktopsサーバーを介してオーディオトラフィックは流れません。
- **HDX RealTime最適化ソフトフォンサポート（推奨）**。メディアエンジンはユーザーデバイス上で実行され、Voice over Internet Protocolトラフィックはピアツーピアで流れます。例については、以下を参照してください。
  - Microsoft Teams向けHDX最適化
  - Microsoft Skype for Businessの配信を最適化するHDX RealTime Optimization Pack

  - (https://www.cisco.com/c/en/us/products/unified-communications/jabber-softphone-for-vdi/index.html) (旧称 VXME)
  - (https://www.cisco.com/c/en/us/td/docs/collaboration/meeting_center/wvdi/wvdi-b-admin-guide/wvdi-b-admin-guide_chapter_010.html)
  - アバイア VDI エクイノックス (旧称 VDI コミュニケーター)
  - Zoom VDI プラグイン
  - ジェネシス ピュアエンゲージ クラウド
  - Nuance Dragon PowerMic ディクテーションデバイス

- **ローカルアプリアクセス**。Citrix Virtual Apps and Desktopsの機能で、ソフトフォンなどのアプリケーションをWindowsユーザーデバイス上でローカルに実行しながら、仮想/公開デスクトップとシームレスに統合されているように見せることができます。この機能は、すべてのオーディオ処理をユーザーデバイスにオフロードします。詳細については、Local App Access and URL redirectionを参照してください。
- **HDX RealTime汎用ソフトフォンサポート**。ICA経由のVoice over Internet Protocol。

汎用ソフトフォンサポート

Generic softphone supportを使用すると、データセンター内のXenAppまたはXenDesktopで、変更されていないソフトフォンをホストできます。オーディオトラフィックは、Citrix ICAプロトコル（UDP/RTPの使用が望ましい）を介して、Citrix Workspaceアプリを実行しているユーザーデバイスに送信されます。

Generic softphone supportは、HDX RealTimeの機能です。このソフトフォン配信アプローチは、特に次の場合に役立ちます。

- ソフトフォンを配信するための最適化されたソリューションが利用できず、ユーザーがLocal App Accessを使用できるWindowsデバイスを使用していない場合。
- ソフトフォンの最適化された配信に必要なメディアエンジンがユーザーデバイスにインストールされていないか、ユーザーデバイスで実行されているオペレーティングシステムのバージョンで利用できない場合。このシナリオでは、Generic HDX RealTimeが貴重なフォールバックソリューションを提供します。

Citrix Virtual Apps and Desktopsを使用してソフトフォンを配信する際の考慮事項は2つあります。

- ソフトフォンアプリケーションが仮想/公開デスクトップにどのように配信されるか。
- オーディオがユーザーのヘッドセット、マイク、スピーカー、またはUSB電話機との間でどのように配信されるか。

Citrix Virtual Apps and Desktopsには、汎用ソフトフォン配信をサポートするための多数のテクノロジーが含まれています。

- リアルタイムオーディオの高速エンコードと帯域幅効率のためのOptimized-for-Speechコーデック。
- 低遅延オーディオスタック。
- ネットワーク遅延が変動してもオーディオをスムーズにするためのサーバー側ジッターバッファ。
- サービス品質のためのパケットタグ付け (DSCPおよびWMM)。
    - RTPパケット (レイヤー3) 用のDSCPタグ付け。
    - Wi-Fi 用のWMMタグ付け。

Windows、Linux、Chrome、Mac版のCitrix Workspaceアプリも、Voice over Internet Protocolに対応しています。Windows版Citrix Workspaceアプリは、以下の機能を提供します。

- クライアント側ジッターバッファ - ネットワーク遅延が変動してもスムーズなオーディオを保証します。
- エコーキャンセル - ヘッドセットを使用しない作業者向けに、マイクとスピーカー間の距離の許容範囲を広げます。
- オーディオプラグアンドプレイ - セッションを開始する前にオーディオデバイスを接続する必要はありません。いつでも接続できます。
- オーディオデバイスルーティング - ユーザーは着信音をスピーカーに、音声パスをヘッドセットに振り分けることができます。
- マルチストリームICA - ネットワーク上で柔軟なサービス品質ベースのルーティングを可能にします。
- ICAは4つのTCPストリームと2つのUDPストリームをサポートします。UDPストリームの1つは、RTPを介したリアルタイムオーディオをサポートします。

Citrix Workspaceアプリの機能の概要については、「Citrix Receiver Feature Matrix」を参照してください。

システム構成の推奨事項

クライアントハードウェアとソフトウェア: 最適なオーディオ品質を得るには、最新バージョンのCitrix Workspaceアプリと、音響エコーキャンセル (AEC) 機能を備えた高品質のヘッドセットをお勧めします。Windows、Linux、Mac版のCitrix Workspaceアプリは、Voice over Internet Protocol

をサポートしています。また、Dell WyseはThinOS (WTOS) 向けにVoice over Internet Protocolをサポートしています。

CPUに関する考慮事項: VDA上のCPU使用率を監視し、各仮想マシンに2つの仮想CPUを割り当てる必要があるかどうかを判断します。リアルタイムの音声とビデオはデータ集約型です。2つの仮想CPUを構成すると、スレッド切り替えの遅延が減少します。したがって、Citrix Virtual Desktops™ VDI環境では2つのvCPUを構成することをお勧めします。

2つの仮想CPUを持つことは、物理CPUの数を2倍にすることを必ずしも意味しません。物理CPUはセッション間で共有できるためです。

セッションの信頼性機能に使用されるCitrix Gateway Protocol (CGP) もCPU消費量を増加させます。高品質のネットワーク接続では、この機能を無効にすることでVDA上のCPU消費量を削減できます。強力なサーバーでは、上記のいずれのステップも不要な場合があります。

UDPオーディオ: UDP経由のオーディオは、ネットワークの輻輳とパケット損失に対して優れた耐性を提供します。利用可能な場合は、TCPの代わりにUDPを使用することをお勧めします。

LAN/WAN構成: 良好なリアルタイムオーディオ品質のためには、ネットワークの適切な構成が不可欠です。通常、過剰なブロードキャストパケットがジッターを引き起こす可能性があるため、仮想LAN (VLAN) を構成する必要があります。IPv6対応デバイスは多くのブロードキャストパケットを生成する可能性があります。IPv6サポートが不要な場合は、それらのデバイスでIPv6を無効にできます。Quality of Serviceをサポートするように構成してください。

WAN接続の使用設定: LANおよびWAN接続でボイスチャットを使用できます。WAN接続では、オーディオ品質は接続の遅延、パケット損失、およびジッターに依存します。WAN接続のユーザーにソフトフォンを提供する場合は、データセンターとリモートオフィス間でNetScaler® SD-WANを使用することをお勧めします。これにより、高いQuality of Serviceが維持されます。NetScaler SD-WANは、UDPを含むMulti-Stream ICAをサポートしています。また、単一のTCPストリームの場合、さまざまなICA仮想チャネルの優先順位を区別して、優先度の高いリアルタイムオーディオデータが優先的に処理されるようにすることが可能です。

DirectorまたはHDX Monitorを使用して、HDX構成を検証します。

リモートユーザー接続: Citrix Gatewayは、UDP/RTPトラフィックをネイティブに（TCPでのカプセル化なしで）配信するためにDTLSをサポートしています。 ポート443経由のUDPトラフィックに対してファイアウォールを双方向に開きます。

コーデックの選択と帯域幅の消費: ユーザーデバイスとデータセンター内のVDA間では、**Optimized-for-Speech**コーデック設定（ミディアム品質オーディオとも呼ばれます）を使用する

ことをお勧めします。VDAプラットフォームとIP-PBX間では、ソフトフォンは構成またはネゴシエートされたコーデックを使用します。例:

- G711は良好な音声品質を提供しますが、コールあたり80キロビット/秒から100キロビット/秒の帯域幅を必要とします（ネットワークレイヤー2のオーバーヘッドによって異なります）。
- G729は良好な音声品質を提供し、コールあたり30キロビット/秒から40キロビット/秒の低い帯域幅を必要とします（ネットワークレイヤー2のオーバーヘッドによって異なります）。

仮想デスクトップへのソフトフォンアプリケーションの配信

XenDesktop®仮想デスクトップにソフトフォンを配信するには、2つの方法があります。

- アプリケーションは仮想デスクトップイメージにインストールできます。
- アプリケーションはMicrosoft App-Vを使用して仮想デスクトップにストリーミングできます。このアプローチは、仮想デスクトップイメージが整理された状態に保たれるため、管理上の利点があります。仮想デスクトップにストリーミングされた後、アプリケーションは通常の方法でインストールされたかのようにその環境で実行されます。すべてのアプリケーションがApp-Vと互換性があるわけではありません。

ユーザーデバイスとの間のオーディオ配信

汎用HDX RealTimeは、ユーザーデバイスとの間でオーディオを配信する2つの方法をサポートしています。

- **Citrix Audio Virtual Channel**。Citrix Audio Virtual Channelはオーディオ転送専用に設計されているため、一般的に推奨されます。
- **Generic USB Redirection**。ユーザーデバイスがCitrix Virtual Apps and Desktopsサーバーへの LANまたはLANに似た接続上にある場合、ボタンまたはディスプレイ（あるいはその両方）を備えたオーディオデバイス、ヒューマンインターフェースデバイス（HID）をサポートします。

Citrix オーディオ仮想チャネル

双方向のCitrixオーディオ仮想チャネル（CTXCAM）により、オーディオをネットワーク経由で効率的に配信できます。Generic HDX RealTimeは、ユーザーのヘッドセットまたはマイクからのオーディオを取得して圧縮します。その後、ICA経由で仮想デスクトップ上のソフトフォンアプリケーションに送信します。同様に、ソフトフォンのオーディオ出力は圧縮され、逆方向にユーザーのヘッドセットまたはスピーカーに送信されます。この圧縮は、ソフトフォン自体が使用する圧縮（G.729やG.711など）とは独立しています。これは、Optimized-for-Speechコーデック（中品質）を使用して行われます。その特性は、Voice over Internet Protocolに最適です。エンコード時間が短く、ネットワーク帯域幅はピーク時で約56キロビット/秒（各方向28 Kbps）しか消費しま

せん。このコーデックはデフォルトのオーディオコーデックではないため、Studioコンソールで明示的に選択する必要があります。デフォルトはHDオーディオコーデック（高品質）です。このコーデックは高忠実度のステレオサウンドトラックに優れていますが、Optimized-for-Speechコーデックと比較してエンコードが遅くなります。

汎用 USB リダイレクト

Citrix Generic USB Redirectionテクノロジー（CTXGUSB仮想チャネル）は、複合デバイス（オーディオとHID）およびアイソクロナスUSBデバイスを含むUSBデバイスをリモートで利用するための汎用的な手段を提供します。このアプローチは、LAN接続されたユーザーに限定されます。その理由は、USBプロトコルがネットワーク遅延に敏感であり、かなりのネットワーク帯域幅を必要とする傾向があるためです。アイソクロナスUSBリダイレクトは、一部のソフトフォンを使用する場合にうまく機能します。このリダイレクトは、優れた音声品質と低遅延を提供します。ただし、Citrix Audio Virtual Channelはオーディオトラフィックに最適化されているため、こちらが推奨されます。主な例外は、ボタン付きのオーディオデバイスを使用している場合です。たとえば、データセンターにLAN接続されたユーザーデバイスに接続されたUSB電話などです。この場合、Generic USB Redirectionは、ソフトフォンに信号を送り返すことで機能を制御する、電話機またはヘッドセットのボタンをサポートします。デバイス上でローカルに機能するボタンには問題ありません。

オーディオ診断コマンドラインツール

VDA上のオーディオ診断コマンドラインツールは、オーディオポリシー、構成、データ転送に関連するセッションデータを照会するために使用できます。

使用方法

コマンドプロンプトを開き、`C:\Program Files\Citrix\HDX\bin`フォルダーから`CtxAudio.exe`を実行します。

- 管理者としてツールを実行すると、すべてのアクティブなICAセッションのオーディオ情報が表示されます。
- 非管理者としてツールを実行すると、現在のユーザーのICAセッションのオーディオ情報が表示されます。

出力

このツールは、セッション内のオーディオ関連の問題の診断に役立つさまざまな構成設定を出力します。

セクション	説明
ポリシー情報	現在のセッションに適用されているオーディオポリシー。
設定情報	レジストリに保存されているオーディオ関連の構成設定。
状態情報	現在のセッションに適用されているオーディオの状態、バージョン、コーデック、およびトランスポート。
デバイス情報	セッションで使用されているデバイス名、その役割、およびステータス。

> **注:**
>
> 出力は、マルチセッション (TS) VDA またはシングルセッション VDA (WSVDA) のどちらでツールを実行するかによって異なります。

制限事項

クライアントにオーディオデバイスをインストールし、オーディオリダイレクトを有効にしてRDSセッションを開始すると、オーディオファイルが再生に失敗し、エラーメッセージが表示されることがあります。

回避策として、RDSマシンにレジストリキーを追加し、その後マシンを再起動します。詳細については、レジストリで管理される機能のリストにあるオーディオの制限を参照してください。

ブラウザコンテンツリダイレクト

はじめに

Browser Content Redirection (BCR) は、Citrix Virtual Apps and Desktops™ 環境におけるウェブブラウジングのユーザーエクスペリエンスを向上させます。ウェブページのレンダリングをユーザーのローカルマシンにオフロードすることで、BCR はサーバーの負荷を軽減し、特に複雑なウェブサイトやリソースを大量に消費するウェブサイトのパフォーマンスを向上させます。

動作の仕組み

BCR は Citrix Workspace™ アプリを利用して、ユーザーデバイス上にセキュアなブラウジング環境を作成します。ユーザーが許可されたウェブページにアクセスすると、ブラウザウィンドウのビューポートがクライアントにリダイレクトされます。その後、クライアント側のブラウザエンジンはローカルマシンのリソースを活用してページをレンダリングし、読み込み時間の短縮とよりスムーズなインタラクションを実現します。

ブラウザのビューポートのみがリダイレクトされることに注意してください。ビューポートとは、ブラウザでコンテンツが表示される長方形の領域です。ビューポートには、アドレスバー、お気に入りツールバー、ステータスバーなどは含まれません。これらの項目はユーザーインターフェイスにあり、VDA のブラウザで引き続き実行されます。

bcr(/en-us/citrix-virtual-apps-desktops/2511/media/bcr.png)

主な利点

Browser Content Redirection はウェブトラフィックをインテリジェントに管理し、インフラストラクチャへの負担を軽減しながら、ユーザーに優れたエクスペリエンスを提供します。

これらが組織にどのように役立つかをご紹介します。

- **コスト削減:** リソースを大量に消費するWebページをユーザーデバイスにオフロードすることで、貴重なサーバーリソースを解放し、帯域幅の消費を削減します。これにより、ハードウェアコストとネットワークコストが削減されます。
- **ユーザーエクスペリエンスの向上:** グラフィックを多用するウェブサイトでも、よりスムーズで応答性の高いブラウジングエクスペリエンスをユーザーに提供します。ネイティブのようなパフォーマンスを提供し、遅延をなくし、生産性を向上させます。
- **セキュリティの向上:** 内部および外部リソースへのアクセスを許可しながら、セキュアな環境を維持します。
- **柔軟性の向上:** 基本的なWebブラウジングから、プロキシトラバーサルやSSO認証を必要とする複雑なWebアプリケーションまで、幅広いユースケースをサポートします。Citrix Web Studio™ のきめ細かなポリシー制御により、リダイレクト設定を簡単に管理できます。

システム要件

サーバー側コンポーネント

シトリックス バーチャル アプリケーションズ アンド デスクトップス

- 長期サービスリリース

  - 最小要件 - サポート終了していないLTSR版Citrix Virtual Apps and Desktopsリリース
  - 推奨 - Citrix Virtual Apps and Desktops 2402 以降
- 現在のリリース
  - 最小要件 - サポート終了していないCR版Citrix Virtual Apps and Desktopsリリース
  - 推奨 - 最新のCitrix Virtual Apps and Desktopsリリース

ブラウザコンポーネント

- ブラウザ
  - マイクロソフト エッジ
  - グーグル クローム
- ブラウザリダイレクト拡張機能
  - Google Chrome ストア
  - Microsoft Edge ストア
- 最高のパフォーマンスを得るために、ブラウザの最新バージョンを使用することをお勧めします。

> **注:**
>
> ブラウザコンテンツリダイレクトまたは双方向コンテンツリダイレクトを有効にするには、Microsoft Edgeアドオンストアからブラウザリダイレクト拡張機能を使用する予定がある場合、Virtual Delivery Agent (VDA) バージョン2503があることを確認してください。古いVDAバージョンでは、Microsoft Edgeブラウザ内でChromeウェブストアから拡張機能をインストールすることで、同じ機能を実現できます。

> 上記で提供されている拡張機能リンクは一般提供 (GA) されており、本番環境レベルの展開に関連しています。GA拡張機能に加えて、CitrixはGoogle Chrome Storeで特にベータ版 (GA + 1) 拡張機能も公開しています。

> Citrixは、今後のアップデートがテストされ、問題が早期に報告されるように、顧客がベータ版のテストユーザーを持つことを推奨しています。これにより、GA拡張機能が正式に展開される際にスムーズなプロセスが保証されます。

> 拡張機能のリリースは通常、Citrix Workspaceアプリのリリースと一致します。

クライアント側コンポーネント

ウィンドウズ

- Windows 10 または 11
- Citrix Workspaceアプリ
  - 最小要件 - サポート終了していないCitrix Workspaceアプリ
  - 推奨
    - 長期サービスリリース - Citrix Workspace App for Windows 2402 CU4 以降、Citrix Workspace App for Windows 2507
    - 現行リリース - Citrix Workspace App 2405以降

> **注:**
>
> - Citrix WorkspaceアプリWindows LTSRリリース1912および2203.1では、ブラウザコンテンツリダイレクトはサポートされていません。
> - ブラウザコンテンツリダイレクトに必要なクライアント側ブラウザエンジンは、Citrix WorkspaceアプリのCurrent Releasesにデフォルトでインストールされます。
> - Citrix Workspaceアプリ2402 LTSRリリースでは、ブラウザコンテンツリダイレクトに必要なクライアント側ブラウザエンジンはデフォルトではインストールされません。管理者はADDLOCALスイッチを利用して、Citrix Workspaceアプリの上にBCRブラウザコンポーネントをインストールできます。
> - Windows向けCitrix Workspaceアプリ2507以降、ブラウザコンテンツリダイレクト（BCR）はモジュールコンポーネントとして管理されますが、引き続きCitrix Workspaceアプリに同梱されます。BCRコンポーネントは、LTSRバージョンでもデフォルトでインストールされるようになり、CRとLTSR間の一貫性が確保されます。さらに、通常のCitrix Workspaceアプリのリリースサイクルとは別に、独立したアップデートや暫定パッチが必要な状況向けにスタンドアロンのBCRパッケージが公開されます。詳細については、Citrix WorkspaceアプリWindowsドキュメントを参照してください。

リナックス

- Citrix Workspaceアプリ
  - 最小要件 - サポート終了（EOL）ではない任意のCitrix Workspaceアプリ
  - 推奨 - Citrix Workspaceアプリ2408以降 詳細については、Citrix Workspaceアプリ for Linuxのドキュメントを参照してください。

> **注：**
>
> Linux向けCitrix Workspaceアプリ2601以降、ブラウザコンテンツリダイレクト（BCR）はモジュールコンポーネントとして管理されます。BCRコンポーネントは、引き続きLinux向けCitrix Workspaceアプリに同梱され、デフォルトでインストールされます。これにより、一貫したユーザーエクスペリエンスが保証されます。さらに、通常のCitrix Workspaceアプリのリリースサイクルとは別に、独立したアップデートや暫定パッチが必要な状況向けにスタンドアロンのBCRパッケージが公開されます。詳細については、Citrix WorkspaceアプリLinuxドキュメントを参照してください。

ChromeOS

- Citrix Workspaceアプリ
  - Chromeウェブストアの最新バージョン

MacOS

- Citrix Workspaceアプリ
  - 最小要件 - Citrix Workspace App for Mac 2411 以降

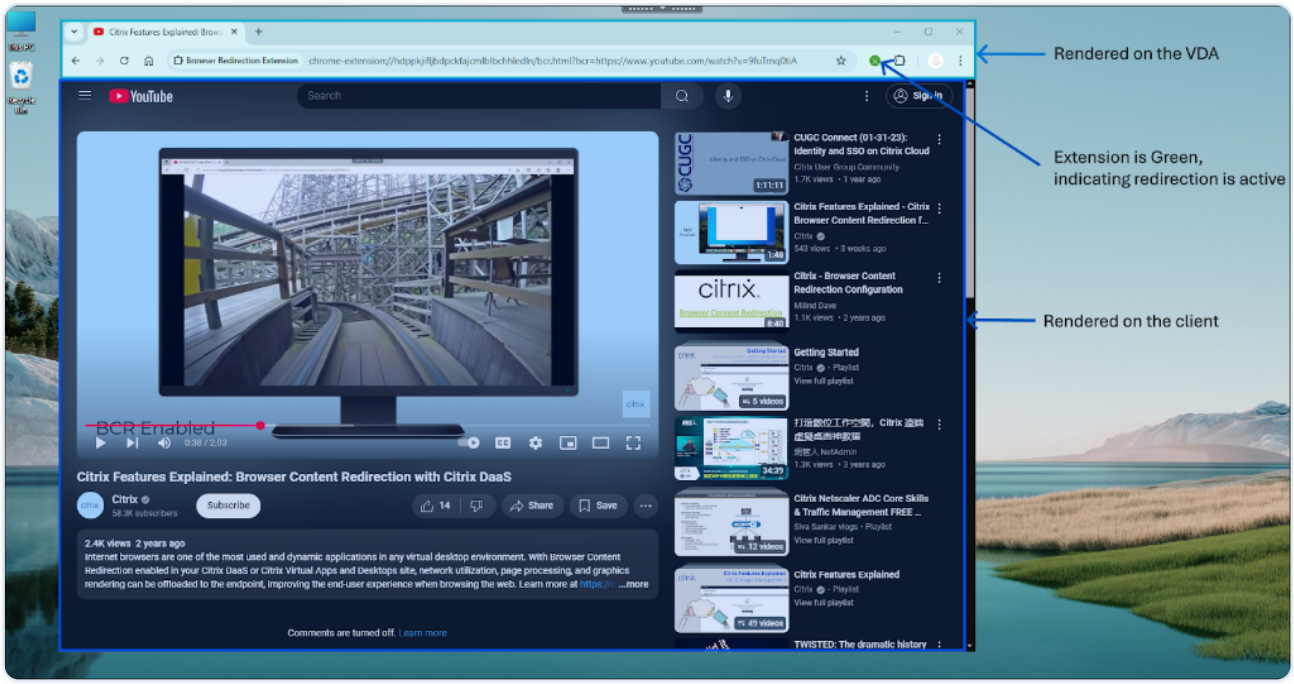
> **注:**
>
> - macOSの場合、ブラウザコンテンツリダイレクトパッケージはCitrix Workspaceアプリとは独立しており、常に最新バージョンです。したがって、このパッケージは、指定された最小バージョンよりも新しい複数のCWAバージョンと互換性があります。
> - Citrix Workspaceアプリ for Macへの依存がないため、ブラウザコンテンツリダイレクトのバージョン番号はCitrix Workspaceアプリ for Macのバージョンとは一致しません。

- クライアント側のブラウザエンジンはCitrix Workspace App Macにはパッケージ化されていません。Mac用のクライアント側はCitrix Downloadsからダウンロードしてインストールしてください。
- IntelおよびARMパッケージは別々です。したがって、macOSエンドポイントに適したバージョンをインストールする必要があります。
- Mac版Citrix Workspaceアプリ2511.1以降、モジュラーBCRコンポーネントはデフォルトでインストールされますが、Citrix Workspaceアプリにはパッケージ化されていません。これにより、Citrix Downloadsからコンポーネントを手動でダウンロードしてインストールする必要がなくなります。スタンドアロンのBCRパッケージは、通常のCitrix Workspaceアプリのリリースサイクル外で独立した更新や暫定パッチが必要な状況のために公開されます。詳細については、Citrix Workspace App Mac documentationを参照してください。

設定手順

1. システム要件に従って、クライアント側およびサーバー側コンポーネントをインストールします
    - 拡張機能の展開の詳細については、「拡張機能の展開」セクションを参照してください
2. Studioポリシーを構成します
    - Web Studioポリシーは、さまざまなユースケースに合わせてブラウザコンテンツリダイレクトを構成するためのきめ細かな方法を提供します
    - 基本的なポリシーにより、管理者はブラウザコンテンツリダイレクトで許可/不許可にする必要があるURLを構成できます
    - URLはワイルドカードで構成できます
3. サポートされているWebブラウザを開き、許可されたURLに移動します
    - 許可リストで一致が見つかった場合、ウェブサイトはクライアントにリダイレクトされます。
    - Citrix Workspaceアプリは、シームレスなエクスペリエンスのために、ビューポートをVDA側のブラウザにブレンドします。
4. 拡張機能のロゴの色は、コンテンツリダイレクトのステータスを示します。
    - 緑：アクティブで接続済み

- 灰色：現在タブで非アクティブ/アイドル状態
- 赤：破損/動作していません



注:

- HTML5ビデオリダイレクトとブラウザコンテンツリダイレクトは独立した機能です。この機能が動作するためにHTML5ビデオリダイレクトポリシーは必要ありません。ただし、Citrix HDX™ HTML5ビデオリダイレクトサービスはブラウザコンテンツリダイレクトに使用されます。
- すべての設定はWeb Studioを介して行い、レジストリキーを使用しないことをお勧めします。

機能と構成オプション

ブラウザコンテンツリダイレクトは、さまざまな顧客環境のユースケースに合わせて構成するためのさまざまな方法を提供します。ポリシー設定の詳細については、ブラウザコンテンツリダイレクトポリシー設定を参照してください。

リダイレクトメカニズム

クライアントフェッチクライアントレンダー

デフォルトでは、ブラウザコンテンツリダイレクトはこのモードで動作します。つまり、クライアント側のブラウザエンジンがウェブページに直接アクセスします。これには、クライアントネットワークからウェブページへの必要なアクセスが必要です。クライアントフェッチクライアントレンダーのシナリオでは、Citrix VDAからクライアントへのネットワーク、CPU、およびRAMの使用量をすべてオフロードし、ブラウザコンテンツリダイレクトを構成する最も最適な方法です。

ポリシー構成オプション

- ブラウザコンテンツリダイレクト：許可
- ブラウザコンテンツリダイレクトACL構成
  - リダイレクトする必要があるURLを指定します。デフォルトでは、YouTubeのみがリダイレクト用に構成されています。
- ブラウザコンテンツリダイレクトブロックリスト構成
  - 特定のURL/サブURLのリダイレクトをブロックするためのオプションの構成オプション。最大限のカスタマイズを実現するには、このオプションを上記のオプションと組み合わせて活用してください。

サーバーフェッチクライアントレンダー

この場合、クライアント側のブラウザエンジンは、仮想チャネルを使用してVDAを介してWebサーバーからコンテンツにアクセスし、フェッチします。このオプションは、クライアントがインターネットにアクセスできない場合（シンクライアントなど）に役立ちます。VDAでのCPUとRAMの消費は少ないですが、ICA®仮想チャネルで帯域幅が消費されます。

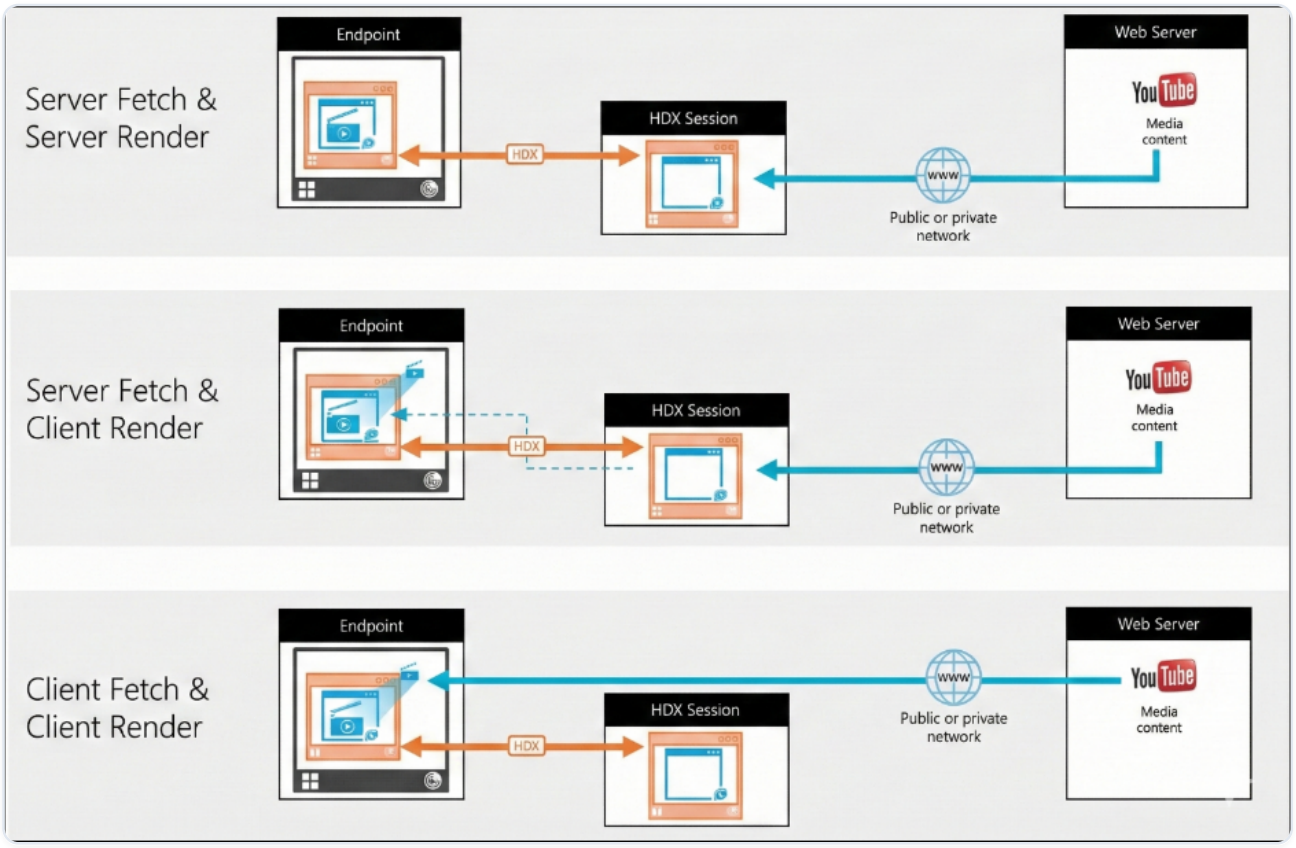
このシナリオには3つの動作モードがあります。「プロキシ」という用語は、VDAがインターネットアクセスを取得するためにアクセスするプロキシデバイスを指します。

ポリシー構成オプション

- クライアントフェッチクライアントレンダーセクションで指定されたポリシーに加えて、以下を構成します。
- ブラウザコンテンツリダイレクトプロキシ構成
  - **直接または透過的:** サーバーフェッチクライアントレンダーを活用し、VDAからWebページへの直接アクセスまたは透過プロキシアクセスがある場合に、これを構成します。ポリシーにはキーワード「DIRECT」を構成する必要があります。

- **明示的プロキシ:** サーバーフェッチクライアントレンダーを活用し、VDAからWebページへの明示的プロキシアクセスがある場合に、これを構成します。
- **PACファイル:** 指定されたURLをフェッチするために、VDA内のブラウザが適切なプロキシサーバーを自動的に選択できるPACファイルに依存している場合に、これを構成します。

フォールバックモード



クライアントリダイレクトが失敗する場合があります。たとえば、クライアントマシンがインターネットに直接アクセスできない場合、エラー応答がVDAに戻されることがあります。このような場合、VDA上のブラウザはページを再読み込みし、サーバー上でレンダリングできます。

認証の処理

認証サイト

Browser Content Redirectionの現在の実装では、リダイレクトメカニズムに関わらず、Browser Content RedirectionがWebサイトへのログインを処理できるように、認証サイトを設定する必要があります。

例:

1. ブラウザコンテンツリダイレクトACL構成で`<https://www.youtube.com/>`*のみが構成されており、認証サイトが構成されていない場合、BCRはウェブサイトにサインインする際にサーバー側レンダリングにフォールバックし、そこで処理を続行します。
2. この場合、BCRが認証サイトを処理できるようにするには、`<https://www.accounts.google.com/>`* および必要に応じてIdP Webサイトなどの他の認証サイトを設定します。各Webサイトのサインインは異なる動作をするため、必ずリストしてください。
3. 設定されている場合、BCRは認証を処理します。たとえば、クライアントフェッチクライアントレンダリングの場合、認証もクライアント側のブラウザエンジンから行われ、シームレスなサインインエクスペリエンスが提供されます。

ポリシー構成オプション

リダイレクトメカニズムのセクションで言及されているポリシーに加えて、Browser Content Redirection認証サイトポリシーを構成します。

> **注:**
>
> - BCRクライアント側ブラウザは、リダイレクトされたウィンドウが閉じられた後、Cookie（認証を含む）を保持しません。これは、BCRウィンドウが完全に閉じられて再度開かれたときに、Webサイトに再ログインする必要があるという形で現れます。
> - BCRクライアント側ブラウザは、VDA側ブラウザからCookieを読み取りません。したがって、ユーザーのパーソナライゼーションと設定はVDAブラウザと同期されません。

統合Windows認証

Browser Content Redirectionは、VDAと同じドメイン内で統合Windows認証 (IWA) とともに構成されている場合、ウェブサイトへのシームレスな認証方法を提供できます。

ポリシー構成オプション

- Browser Content Redirection統合Windows認証サポートポリシーを構成します。

シングルサインオンを有効にする前に、以下を完了してください。

- Kerberosインフラストラクチャを構成して、ホスト名から構築されたサービスプリンシパル名 (SPN) のチケットを発行します。例: HTTP/serverhostname.com。
- サーバーフェッチクライアントレンダリングの場合: サーバーフェッチモードでブラウザコンテンツリダイレクトを使用する場合は、VDAでDNSが適切に構成されていることを確認してください。

- クライアントフェッチクライアントレンダリングの場合: クライアントフェッチモードでブラウザコンテンツリダイレクトを使用する場合は、クライアントデバイスでDNSが適切に構成されており、オーバーレイからWebサーバーのIPアドレスへのTCP接続を許可していることを確認してください。

プロキシ認証

ブラウザコンテンツリダイレクトは、サーバーからコンテンツをフェッチする際に、Webプロキシへのシームレスな認証方法を提供できます。有効にすると、ブラウザコンテンツリダイレクトはKerberosサービスチケットを自動的に取得して使用し、プロキシで認証します。

ポリシー構成オプション

- ブラウザコンテンツリダイレクトのサーバーフェッチプロキシ認証ポリシーを構成します。

サーバーフェッチプロキシ認証ポリシーを有効にする前に、以下を完了してください。

- PAC ファイルを設定して、ダウンストリームの Web プロキシを介してトラフィックをルーティングし、プロキシが Kerberos 認証を使用するように設定する必要があります。

サーバー側証明書検証

ブラウザコンテンツリダイレクトは、証明書検証のサポートによりさらに強化されました。クライアントからリダイレクトされたウェブサイトにアクセスする際、クライアントオーバーレイブラウザは、サーバーまたはMitMプロキシからの証明書を信頼しない場合があります。このような場合、BCRはVDAの証明書ストアに対してホストまたはプロキシの証明書を検証できるようになりました。

最小要件

この機能はデフォルトで有効になっており、以下の要件が満たされれば構成は不要です。

- シトリックス バーチャルアプリおよびデスクトップ 2507
- Citrix Workspace アプリ (Windows用) 2511
- Citrix Workspace アプリ (Linux用) 2604
- ブラウザコンテンツリダイレクト拡張機能 (ChromeまたはEdge) 25.11以降。

シングルサインオンのサポート

ブラウザコンテンツリダイレクトは、シングルサインオンのサポートにより、VDA側での認証とCookie共有を可能にし、合理化されたユーザーエクスペリエンスを提供します。この機能強化により、冗長なログインが不要になり、BCRセッション全体で認証とCookieの永続性が維持されるため、BCRウィンドウが閉じられた後でも生産性が向上します。このシームレスなエクスペリエ

ンスは、認証がクライアントではなくVDAから行われることを保証することで、セキュリティをさらに強化します。

この機能の詳細については、「シングルサインオンのサポート」セクションを参照してください。

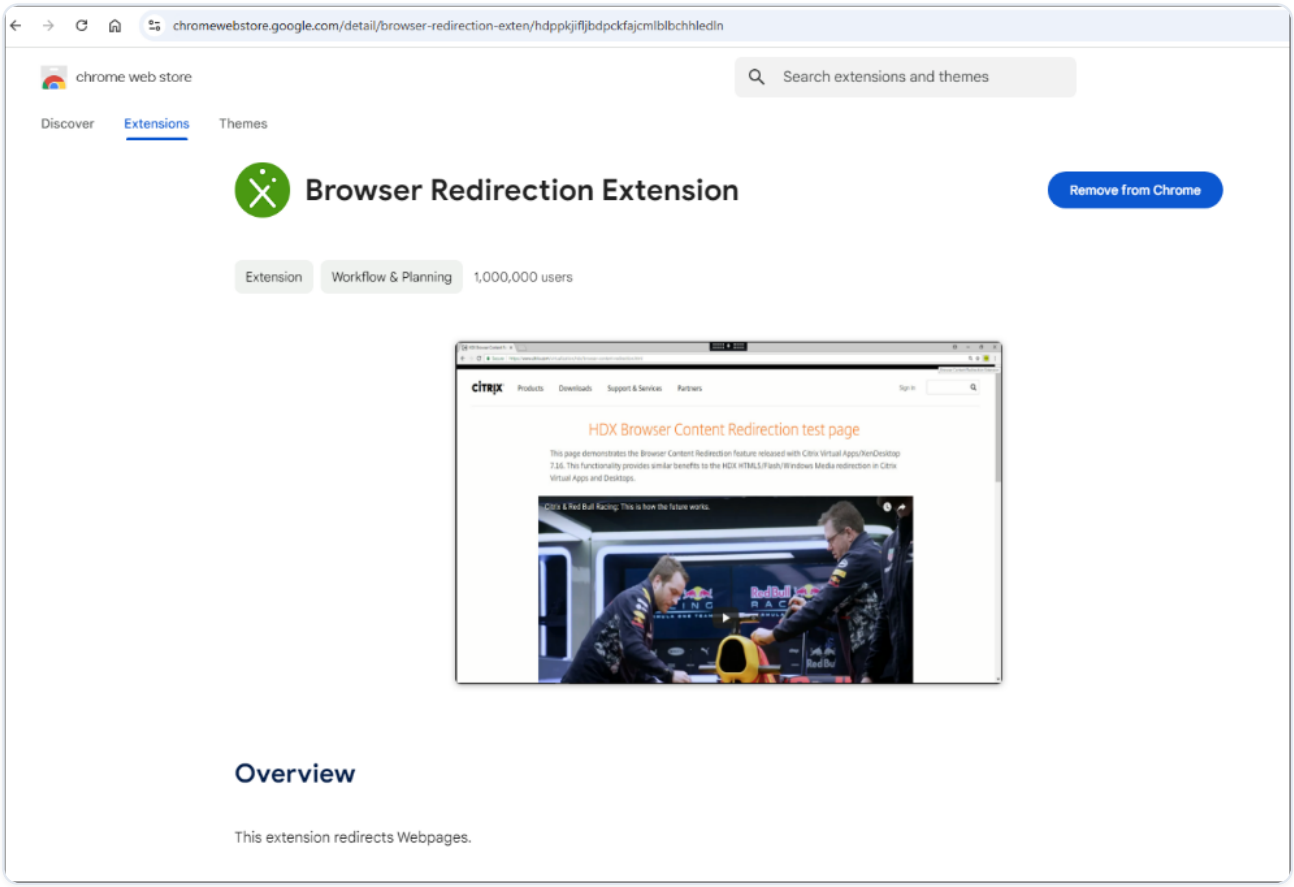
ユースケース

ブラウザコンテンツリダイレクト (BCR) は、特にリソースを大量に消費し、企業で頻繁にアクセスされる幅広いウェブサイトで利用できます。これには、YouTubeのようなビデオストリーミングプラットフォームが含まれ、レンダリングをエンドポイントデバイスにオフロードすることで、サーバー負荷を大幅に軽減し、コストを節約できます。さらに、BCRは、ビデオ会議やコラボレーションツール (Google Meet、Teams Web、Zoom Web) などのユニファイドコミュニケーションアプリケーションや、コンタクトセンターアプリケーション (Genesys Cloud) にも最適であり、スムーズなパフォーマンスと強化されたユーザーエクスペリエンスを保証します。BCRを活用することで、企業はリソースを最適化し、さまざまなウェブベースアプリケーションの効率を向上させることができます。特定のウェブサイトの設定方法については、CTX238236を参照してください。

拡張機能の展開

手動で展開

ブラウザリダイレクト拡張機能は、ChromeおよびEdgeのウェブストアで公開されています。この拡張機能は、クライアント側ではなく、VDA上のブラウザにのみ必要です。拡張機能をインストールするには、Chrome / Edgeウェブストアに移動し、「Browser redirection extension」を検索して、それぞれのブラウザに追加します。この方法は個々のユーザーに有効です。多数のユーザーに拡張機能を展開するには、グループポリシーを使用して拡張機能を展開します。



グループポリシーを使用して展開する

前提条件

- **アクセス:** グループポリシーを構成するマシン上またはActive Directory環境内で、管理者権限が必要です。
- **ADMXファイル:** お使いのChromeのバージョンに対応するGoogle Chrome ADMXファイル（管理用テンプレート）をダウンロードします。これらはGoogle Chrome Enterprise ヘルプページで入手できます。
- **Edgeテンプレート:** Microsoft Edgeの管理用テンプレート（ADMXファイル）をMicrosoft Edge Enterprise ランディングページからダウンロードします。
- **拡張機能IDと更新URL:** Citrix Browser Content Redirection拡張機能の拡張機能IDと更新URL。

GOOGLE CHROMEの手順

1. ADMXファイルのインポート:
    - Chrome ADMX ファイルを管理用テンプレート用の中央ストアにコピーします。これは通常、ドメインコントローラー上の %SystemRoot%\PolicyDefinitions です。
2. グループポリシー管理を開く:
    - グループポリシー管理コンソール（gpmc.msc）を起動します。

3. GPOの作成または編集:
    - 新しいグループポリシーオブジェクト（GPO）を作成するか、拡張機能を展開したいユーザーまたはコンピューターに適用される既存のものを編集します。
4. 拡張機能設定に移動:
    - GPOエディターで、以下に移動します。
        - ユーザーの構成 > 管理用テンプレート > 従来の管理用テンプレート (ADM) > Google > Google Chrome > 拡張機能
5. 「強制インストールするアプリと拡張機能のリストを構成する」を有効にします。
    - このポリシー設定をダブルクリックし、「有効」を選択します。
    - 「強制インストールするアプリと拡張機能のリストを構成する」設定が無効に設定されている場合、拡張機能はすべてのユーザーのChromeから自動的に削除されます。
6. 拡張機能IDと更新URLを追加します。
    - 「表示」ボタンをクリックします。
    - 拡張機能IDと更新URLを次の形式で入力します: <extension_id>;<update_url>
    - 値: hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx (更新URL)
7. GPOを適用します。
    - Active Directory構造内の適切な組織単位 (OU) にGPOをリンクします。
8. グループポリシーを更新:
    - ターゲットマシンで、gpupdate /force を実行してポリシーをすぐに適用するか、ポリシーが自動的に更新されるのを待ちます。

MICROSOFT EDGE の手順

1. ADMXファイルをインポートします。
    - Edge ADMX ファイルを、管理用テンプレート用の中央ストア (%SystemRoot%\PolicyDefinitions) にコピーします。
2. グループポリシー管理を開きます。
    - グループポリシー管理コンソール (gpmc.msc) を起動します。

3. GPO を作成または編集します。
    - 新しい GPO を作成するか、既存の GPO を編集します。
4. 拡張機能の設定に移動します。
    - GPO エディターで、以下に移動します。
        - コンピューターの構成 > ポリシー > 管理用テンプレート > Microsoft Edge > 拡張機能
5. 「サイレントインストールされる拡張機能を制御する」を有効にします。
    - このポリシー設定をダブルクリックし、「有効」を選択します。
6. 拡張機能 ID と更新 URL を追加します。
    - 「表示」ボタンをクリックします。
    - 拡張機能 ID と更新 URL を、<extension_id>;<update_url> の形式で入力します。
    - 値: hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx (更新 URL)
7. GPO を適用します。
    - GPOをActive Directory構造内の適切な組織単位 (OU) にリンクします。
8. グループポリシーを更新します。
    - ターゲットマシンで、gpupdate /forceを実行するか、自動更新を待ちます。

強制アプリを構成する(/en-us/citrix-virtual-apps-desktops/2511/media/configure-force-apps.png)

強制インストールされたアプリ(/en-us/citrix-virtual-apps-desktops/2511/media/force-installed-apps-bcr.png)

トラブルシューティング

トラブルシューティング情報については、ナレッジセンターの記事「ブラウザコンテンツリダイレクトのトラブルシューティング方法」を参照してください。

ブラウザコンテンツリダイレクトの制限事項

サーバー側の制限事項 (VDA)

ブラウザコンテンツリダイレクトは、以下のユースケースをサポートできません。記載されているシナリオまたは新しいシナリオで機能強化が必要な場合は、Citrix製品チームにお問い合わせください。

- ポップアップウィンドウは、ブラウザコンテンツリダイレクトではサポートされていません。
- ブラウザコンテンツリダイレクトが使用されている場合、HTML5ビデオリダイレクトポリシーは無効にする必要があります。
- セッションの切断/再接続のシナリオでは、BCRを再度有効にするためにVDAブラウザウィンドウを更新する必要があります。
- BCR化されたウィンドウからの印刷およびファイルのダウンロードはサポートされていません。
- ブラウザコンテンツリダイレクトをブラウザプロファイル共有と併用する場合、複数のプロファイルでのSSO永続性はサポートされていません。
- シークレットモードまたはプライベートブラウジングモードは、ブラウザコンテンツリダイレクトではサポートされていません。

クライアント側の制限 (CWA)

- ブラウザコンテンツリダイレクトは、ARMhfフレームワークではサポートされていません。
- BCRは、1つのブラウザで最大25個のリダイレクトされたタブ、および2つのブラウザで合計30個のリダイレクトされたタブをサポートします。

シングルサインオンのサポート

はじめに

Browser Content Redirectionは、シングルサインオンのサポートにより、VDA側での認証とCookie共有を可能にし、効率化されたユーザーエクスペリエンスを提供します。

この機能強化により、重複するログインが排除され、BCRウィンドウが閉じられた後でもBCRセッション全体で認証とCookieの永続性が維持されるため、生産性が向上します。

このシームレスなエクスペリエンスは、認証がクライアントではなくVDAから行われるようにすることで、セキュリティをさらに強化します。

シングルサインオンなしの場合

- BCR内で認証されたページを開くと、ユーザーは毎回資格情報を再入力する必要があり、SSOの永続性が失われました。
- SSOはBCRウィンドウが開いている間のみ維持されました。ウィンドウを閉じて再度開くと、ユーザーはログインプロセスを繰り返す必要がありました。
- 認証フローはクライアントから行われたため、管理者はクライアントデバイスからセキュアな認証サイトへのネットワークアクセスを提供する必要がありました。

シングルサインオンありの場合

- VDAブラウザからSSOがシームレスに保持されるため、ユーザーは資格情報の入力を求められなくなります (VDAで既に認証されている場合)。
- 認証はVDAから行われるため、クライアント側のネットワーク要件と露出が制限され、セキュリティ体制が向上し、大幅に改善された中断のないエクスペリエンスが提供されます。

最小要件

- Citrix バーチャルアプリおよびデスクトップ 2507
- Citrix Workspace アプリ Windows 向け 2511
- Citrix Workspace アプリ Linux 用 2601
- ブラウザリダイレクト拡張機能 (Chrome または Edge) 25.11 以降

サポートされている認証シーケンス

現在、BCRシングルサインオンでサポートされている認証シーケンスには2つのタイプがあります。

リダイレクトベースの認証

この標準的な方法では、アプリケーションはHTTPリダイレクトを使用して、ユーザーを認証専用ページに強制的に誘導します。

たとえば、ユーザーが必要なセッションCookieなしで `<https://my.intranet.app>` にアクセスしようとすると、Webアプリケーションは `<https://my.intranet.app/auth>` のような認証エンドポイントへのHTTP 302リダイレクトで応答します。

ユーザーがそのページで認証に成功すると、ブラウザは元のアプリケーションURLにリダイレクトされ、必要な認証Cookieが含まれるようになります。

ページ内フォームベース認証

この方法では、ログインインターフェイスを動的に表示しながら、ユーザーを目的のアプリケーションURLに留めます。

たとえば、ユーザーが `<https://my.intranet.app>` のような保護されたページに移動すると、必要なCookieがないため、リダイレクトをトリガーすることなく、ページが認証フォームを直接読み込みます。このプロセスには、ページインターフェイスとIDP (Identity Provider) の間でいくつかの内部的なやり取りが含まれる場合があります。これらのやり取りは、最終的に有効なCookieが提供され、利用されて、ユーザーが元のページのコンテンツにアクセスできるようになるまで続きます。

> **注:**
>
> 上記のメカニズムでシナリオがカバーされておらず、上記のメカニズムを使用するようにWeb アプリを設定できない場合は、Citrix 製品チームにお問い合わせください。

構成

ステップ0: はじめに

BCRでシングルサインオンを構成する方法は2つあります。構成方法の選択は、目的のBCRウェブサイトの認証メカニズムと、シングルサインオンをサポートするために複数のウェブアプリケーションを構成する必要がある柔軟性によって異なります。

方法1: この方法では、Web Studioの既存のBCRポリシーを使用して、シングルサインオンのサポートを実現します。

シングルサインオンのサポートが導入される前は、ブラウザコンテンツリダイレクト認証サイトポリシーを使用して、認証（または中間ページ）に使用されるURLを指定し、フローの中断がないようにクライアントにリダイレクトしていました。

シングルサインオンのサポートが導入されたことで、BCRはVDA側のブラウザの認証Cookieを活用するようになり、そのため、認証サイトポリシーのURLは、代わりにブラウザコンテンツリダイレクトブロックリストポリシーで構成する必要があります。これにより、認証がVDAを介して行われるようになります。

方法2: この方法は方法1と同様のロジックで動作しますが、URLは代わりにJSON (`bcrconfig.json`) を介して構成され、ホストされているJSON URLがBCR ACLポリシーで呼び出されます。JSON構成は、追加の柔軟性を提供します。

1. 企業は環境内で複数のWebアプリケーションを使用しており、各アプリケーションは実装に基づいて異なる認証メカニズムを使用する場合があります。新しいJSONメソッドにより、構成がより直感的で堅牢かつスケーラブルになります。
2. **ページ内フォームベース認証**を扱う場合、方法1では、そのような構成をサポートする既存のポリシーがないため、特定の認証Cookieを設定する方法が提供されません。したがって、Webサイトで**ページ内フォームベース認証**が必要な場合、JSONが唯一の方法です。

将来を見据えると、JSONはより堅牢な機能を導入するためのスケーラブルな方法を提供するため、CitrixはJSONベースの構成を推奨します。

ステップ1：認証メカニズムの決定

構成に使用するメソッドを決定するには、まずアプリケーションがどのような認証メカニズムを使用しているかを判断する必要があります。ウェブアプリケーションの認証方法を正確に判断する最善の方法は、ウェブアプリケーション管理者に連絡することです。

それが選択肢にない場合は、BCR拡張機能が**インストールされていない状態で**認証フローを実行しながら、ブラウザの開発者ツールのタブで要求/応答のやり取りを検査する必要があります。次の結果は、認証タイプを判断するのに役立ちます。

リダイレクトベース認証の場合: ステータス列で1つ以上の302 (リダイレクト) 応答を探します。302応答には、認証ページを指すロケーションヘッダーが含まれているはずです。このページURLは、方法1を使用している場合はブラウザコンテンツリダイレクトブロックリストポリシーに、方法2を使用している場合は`bcrconfig.json`ファイルのアプリ構成の`denyList`セクションに設定する必要があります。

ページ内フォームベース認証の場合: メソッド列で複数のPOSTリクエストを探します。POSTリクエストに対する後の応答の1つは、Webアプリ固有の認証Cookieを含むset-cookieヘッダーを返す必要があります。このCookieは、`bcrconfig.json`ファイルのアプリ構成のCookieセクションに設定する必要があります。方法1はページ内フォームベース認証をサポートしていないため、このシナリオでは方法2が唯一の構成オプションです。

例: github.comの例を次に示します。この方法は、BCRでリダイレクトしたい任意のウェブサイトに使用でき、適切な構成があることを確認できます。

1. **Chrome**を開き、**CTRL+SHIFT+I**を押して開発者ツールを表示します。
2. **Network**タブをクリックします。
3. **Preserve log**設定をオンにします。
4. ネットワークログを簡素化するために、**Doc**フィルターをクリックします。
5. **Name**の横を右クリックし、**URL**列を追加します。

6. 開発者ツールを開いたまま、**github.com**にアクセスします。
7. **github.com**にサインインします。
8. github.comの初期ページからログオン後の宛先までのすべての中間ホップをメモします。
9. 上記で指定された認証タイプを決定するために、要求/応答ヘッダーを分析します。

ステップ2：構成方法を選択する

1. リダイレクトベースの認証のみを扱っており、さまざまなニーズを持つ複数のWebアプリケーション（例：リダイレクトベースの認証を使用するWebアプリケーションと、ページ内フォームベースの認証を使用する別のWebアプリケーション）をリダイレクトする必要がない場合は、方法1を選択してシングルサインオンを構成できます。
2. ページ内フォームベースの認証を扱っている場合、または異なる認証メカニズムを持つ複数のWebアプリケーションを扱っている場合、あるいはリダイレクトベースの認証のみであってもより柔軟性を求める場合は、方法2を選択できます。

ステップ3：構成

方法1：既存のポリシーでBCRシングルサインオンを構成する

1. `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDXMediaStream key: Dword BrowserProfileSharing value 1`に以下のレジストリ値を作成して、VDAで機能を有効にします。
2. ブラウザーコンテンツリダイレクトACL構成ポリシーを、リダイレクトするWebサイトで構成します。この点での構成変更はありません。
3. 認証サイトポリシーにすでにURLが設定されている場合は、それらをブラウザコンテンツリダイレクトブロックリストポリシーにコピーし、認証サイトポリシーを無効にします。
4. 以前に認証/仲介サイトを設定していない場合は、仲介URLを特定し（BCR拡張機能が**インストールされていない状態で**認証フローを実行中に、ブラウザの開発者ツールのタブにあるリクエスト/レスポンスのやり取りから）、それらをブロックリストに設定します。

方法2：JSONでBCRシングルサインオンを構成する

bcrconfig.json の作成

`bcrconfig.json`には複数のWebアプリ構成を含めることができます。BCR拡張機能は、要求されたURLをapps配列内のいずれかのアプリによって指定された`allowList`のいずれかに一致させようとし、関連するルールを動的に適用して、ページのリダイレクトとシングルサインオン処理をどのように処理するかを決定します。BCR拡張機能がWebアプリをどのように扱うかを制御するために、以下のキーを使用できます（JSON仕様に従って、*ブール値*は小文字である必要があることに注意してください - **true**または**false**のみ）。

- **appName** : これは主に拡張機能の内部およびログ記録の目的で使用されます。
- **allowList** : アプリには `allowList` に少なくとも1つのURLを含める必要があります。これは、クライアントがページをレンダリングし、VDAではないようにリダイレクトされることを意図したURLです。複数のURLを定義でき、ワイルドカードも受け入れられます。ワイルドカードルールは、ブラウザコンテンツリダイレクトACL構成とまったく同じです。たとえば、すべてのGoogleアプリをリダイレクトするように構成するには、次の配列を使用します。

- **denyList** : 認証が必要なときにWebアプリケーションがユーザーをリダイレクトするURLを定義します。この構成は、主にリダイレクトベースの認証に不可欠ですが、一部のフォームベースの認証フローで特定のリダイレクトを防ぐためにも使用できます。このキーにリストされているURLは、サーバー側の認証が行われるようにリダイレクトされません。プロファイル共有が不要な場合に、ドメインの特定のサブURLがクライアントにリダイレクトされないように制限するためにも使用できます。
- **profileSharing** : これは、シングルサインオン認証Cookieおよびユーザー設定を保存するその他のCookieが共有されるように設定する必要があるキー値であり、サーバー側とクライアント側でレンダリングされるページ間の一貫した動作を保証します。
- **cookies** : ユーザーにプロンプトを表示せずにWebアプリケーションをロードするために必要な1つ以上の認証Cookieを定義します。拡張機能は、ここにリストされているすべてのCookieが指定されたWebアプリURLに設定されていると検出されるまで、クライアント側のリダイレクトを防ぎます。この設定は、主にページ内フォームベースの認証に使用されますが、特定のシナリオでdenyListを指定することに加えて、リダイレクトベースの認証にも利用できます。
- **deleteClientCache**: `bcrconfig.json` 構成メカニズムが使用されている場合、BCRクライアントはセキュリティ強化のためにデフォルトでブラウザキャッシュを削除します。このプロセスは、ユーザーがリダイレクトされたすべてのタブを閉じるか、セッションで初めてリダイレクトされたページを開始したときに発生します。この動作を防ぐには、このキーの値を**false**に設定します。クライアントデバイスが信頼されている場合、このキーを**false**に設定するとユーザーエクスペリエンスが向上します。クライアントデバイスが信頼されていない場合、このキーを設定しない（または）このキーを**true**に設定すると、セキュリティ体制が強化されます。
- **schemaVersion** : これは主に拡張機能の内部およびログ記録の目的で使用されます。本稿執筆時点では、その値は**2511**に設定されている必要があります。

構成例

```
{

  "apps": [
```

```
{
  "appName": "myWebApp1",
  "allowList": [
    "https://myWebApp1.com/*"
  ],
  "denyList": [],
  "requires": {
    "profileSharing": false,
    "cookies": []
  }
},
{
  "appName": "myWebApp2",
  "allowList": [
    "https://myWebApp2.com/*"
  ],
  "denyList": [
    "https://myWebApp2.com/authPortal/*"
  ],
  "requires": {
    "profileSharing": true,
    "cookies": []
```

```
    }
  },
  {
    "appName": "myWebApp3",
    "allowList": [
      "https://*.myWebApp3.com/"
    ],
    "denyList": [
      "https://myWebApp3.com/authPortal/*"
    ],
    "requires": {
      "profileSharing": true,
      "cookies": [
        "requiredAuthCookie1",
        "requiredAuthCookie2"
      ]
    }
  }
],
"preferences": {
  "deleteClientCache": true
},
```

```
  "schemaVersion": "2511"

}
```

以下にサンプル`bcrconfig.json`ファイルを示します。その要素については、以下で詳しく説明します。

上記の JSON 構造には、異なる構成を持つ 3 つのアプリが含まれています。

myWebApp1 シナリオ、SSO なし:

- `allowList`キーの文字列配列値は、`<https://myWebApp1.com>`内のすべてのパスをクライアントにリダイレクトする必要があることを指定します。ただし、`denyList`キーにリストされている値がある場合は除きます。
- `denyList`キーの文字列配列値は空であるため、認証サイトのリダイレクトは防止されません。したがって、認証は厳密にサーバー側で保持されません。
- `profileSharing`キーのブール値は**false**に設定されているため、`allowList`エントリに関連するCookieはクライアントと共有されません。
- cookiesキーの文字列配列は空ですが、`profileSharing`共有キーが**false**に設定されているため、いずれにしても無視されます。

myWebApp2、リダイレクトベースの認証シナリオ:

- `allowList`キーの文字列配列値は、`<https://myWebApp2.com>`内のすべてのパスをクライアントにリダイレクトする必要があることを指定します。ただし、`denyList`キーにリストされている値がある場合は除きます。
- `denyList`キーの文字列配列値は、**myWebApp2.com**ドメイン下の`/authPortal/`で始まるパスがクライアント側のリダイレクトを防止され、サーバー側の認証が実行できるように指定します。
- `profileSharing` キーのブール値が **true** に設定されているため、allowList エントリに関連するクッキーはクライアントと共有され、シングルサインオンが実行されます。
- cookiesキーの文字列配列は空であるため、拡張機能はサーバー側認証後に特定のCookieが設定されるのを待たずに、クライアントと共有されます。

myWebApp3、フォームベースの認証シナリオ:

- `allowList`キーの文字列配列値は、`<https://myWebApp3.com>`内のすべてのパスをクライアントにリダイレクトする必要があることを指定します。ただし、`denyList`キーにリストされている値がある場合は除きます。
- `denyList`キーの文字列配列値は、**myWebApp3.com**ドメイン下の`/authPortal/`で始まるパスがクライアント側のリダイレクトを防止され、サーバー側の認証が実行できるように指定します。
- `profileSharing`キーのブール値は**true**に設定されているため、`allowList`エントリに関連するCookieはクライアントと共有されます。
- cookies キーの文字列配列にクッキー名が含まれているため、拡張機能はサーバー側認証後にこのクッキーが設定されるのを待ちます。`allowList` の関連 URL のクッキーはクライアントと共有され、クライアント側のリダイレクトが発生します。

設定

- `deleteClientCache` キーが **true** に設定されているため、BCR クライアントはセキュリティ強化のためにデフォルトでブラウザキャッシュを削除します。これは、キーが設定されていない場合でもデフォルトの動作です。

BCR ポリシーの構成

`bcrconfig.json` を作成したら、以下の手順に従って Browser Content Redirection ACL configuration を構成し、JSON ファイルのコンテンツを使用します。

- ファイルに `.bcrconfig.json` 拡張子を付けて名前を付けます。例: `myrules.bcrconfig.json`
- JSON ファイルを VDA からアクセス可能な Web サーバーでホストし、URL をメモします。

> **注:**
>
> サーバーはファイルのダウンロードを許可する必要があります。Microsoft IIS サイトは、デフォルトで JSON ファイルのダウンロードを許可しています。

- Citrix Studio の で、前の手順で取得した URL を 設定に追加します。

> **注:**
>
> 設定の他のエントリはそのまま残すことができます。競合が発生した場合、BCR 拡張機能は `bcrconfig.json` 設定を優先します。Citrix は、管理の容易さ、アプリケーション

> レベルの構成、およびスケーラビリティのために、構成全体を JSON に移行することを推奨します。

- ポリシーを保存し、セッションを起動してポリシー構成をテストします。

> **注:**
>
> ポリシーを設定した後、ホストされている `bcrconfig.json` ファイルはいつでも編集して調整できます。ファイルは、BCR 拡張機能を実行しているメインのブラウザプロセスが起動または再起動したときにのみ再ロードされ、変更が適用されます。

> **注記:**
>
> - 要するに、ポリシーの観点からは、Browser Content Redirectionポリシー（これはデフォルトで有効になっています）を有効にし、JSONファイルを指すURLでBrowser Content Redirection ACL構成ポリシーを構成するだけで済みます。
> - JSON 構成は現在、以下のポリシーに適用され、それらを柔軟にします。ただし、残りのポリシーは以前と同じ動作を継続します。
>   - **ブラウザコンテンツリダイレクト ACL 構成:** ACL 内の URL は、`allowList` キーを介して JSON で構成できるようになりました。
>   - **ブラウザコンテンツリダイレクトブロックリスト構成:** ブロックリストは、`denyList` キーを介して JSON で構成できるようになりました。
>   - **ブラウザコンテンツリダイレクト認証サイト:** 認証サイトも、`denyList` キーを介して JSON で構成できます。

HDX™ ビデオ会議およびWebカメラのビデオ圧縮

> **警告:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になる深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤った使用に

> よって生じる問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

> ウェブカメラは、HDXウェブカメラビデオ圧縮またはHDXプラグアンドプレイ汎用USBリダイレクトを使用して、仮想セッション内で実行されているアプリケーションによって使用できます。モードを切り替えるには、**Citrix Workspace™アプリ > 環境設定 > デバイス**を使用します。Citrixは、可能な限り常にHDXウェブカメラビデオ圧縮を使用することを推奨します。HDX汎用USBリダイレクトは、HDXビデオ圧縮とのアプリケーション互換性の問題がある場合、またはウェブカメラの高度なネイティブ機能が必要な場合にのみ推奨されます。パフォーマンスを向上させるために、CitrixはVirtual Delivery Agentに少なくとも2つの仮想CPUを搭載することを推奨します。

ユーザーがHDXウェブカメラビデオ圧縮から切り替えるのを防ぐには、**ICA®ポリシー設定 > USB デバイスポリシー**設定の下にあるポリシー設定を使用してUSBデバイスリダイレクトを無効にします。Citrix Workspaceアプリのユーザーは、Desktop Viewerの「マイクとウェブカメラ」設定で**マイクまたはウェブカメラを使用しない**を選択することで、デフォルトの動作を上書きできます。

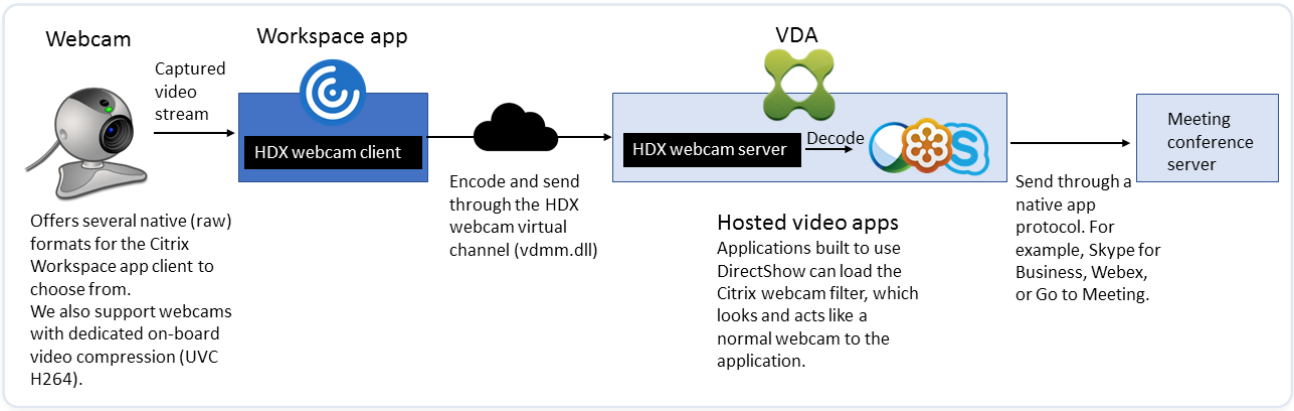
HDXウェブカメラビデオ圧縮

HDXウェブカメラビデオ圧縮は、**最適化された**ウェブカメラモードとも呼ばれます。このタイプのウェブカメラビデオ圧縮は、H.264ビデオを仮想セッションで実行されているビデオ会議アプリケーションに直接送信します。VDAリソースを最適化するために、HDXウェブカメラ圧縮はウェブカメラビデオのエンコード、トランスコード、デコードを行いません。この機能はデフォルトで有効になっています。

サーバーからビデオ会議アプリへの直接ビデオストリーミングを無効にするには、VDAでレジストリキーを0に設定します。詳細については、レジストリを通じて管理される機能のリストにあるウェブカメラビデオ圧縮を参照してください。

ビデオストリーミングリソースのデフォルト機能を無効にすると、HDXウェブカメラビデオ圧縮は、クライアントオペレーティングシステムの一部であるマルチメディアフレームワークテクノロジーを使用して、キャプチャデバイスからのビデオを傍受し、トランスコードして圧縮します。キャプチャデバイスの製造元は、OSカーネルストリーミングアーキテクチャに接続するドライバーを提供します。

クライアントはウェブカメラとの通信を処理します。その後、クライアントはビデオを適切に表示できるサーバーにのみ送信します。サーバーはウェブカメラと直接やり取りしませんが、その統合によりデスクトップで同じエクスペリエンスが得られます。Workspaceアプリは、帯域幅を節約し、WANシナリオでの回復力を向上させるためにビデオを圧縮します。



HDXウェブカメラビデオ圧縮には、**マルチメディア会議**ポリシーを有効にする必要があります。このポリシーはデフォルトで有効になっています。

ウェブカメラがハードウェアエンコードをサポートしている場合、HDXビデオ圧縮はデフォルトでハードウェアエンコードを使用します。ハードウェアエンコードは、ソフトウェアエンコードよりも多くの帯域幅を消費する可能性があります。ソフトウェア圧縮を強制するには、クライアントのレジストリキーを編集します。詳細については、レジストリを通じて管理される機能のリストにあるウェブカメラソフトウェア圧縮を参照してください。

HDXウェブカメラビデオ圧縮の要件

HDXウェブカメラビデオ圧縮は、Citrix Workspaceアプリの以下のバージョンをサポートしています。

プラットフォーム	プロセッサ
Citrix Workspace アプリケーション for Windows	Citrix Workspaceアプリ for Windowsは、XenAppおよびXenDesktop 7.17以降で、32ビットおよび64ビットアプリのWebカメラビデオ圧縮をサポートします。以前のバージョンでは、Citrix Workspaceアプリ for Windowsは32ビットアプリのみをサポートします。
Citrix Workspace アプリケーション for Mac	Citrix Workspaceアプリ for Mac 2006以降は、XenAppおよびXenDesktop 7.17以降で、64ビットアプリのWebカメラビデオ圧縮をサポートします。以前のバージョンでは、Citrix Workspaceアプリ for Macは32ビットアプリのみをサポートします。
Citrix Workspace アプリケーション for Linux	Citrix Workspaceアプリ for Linuxは、仮想デスクトップ上で32ビットおよび64ビットの両方のアプリをサポートします。

プラットフォーム	プロセッサ
Citrix Workspace アプリケーション for Chrome	一部のARM ChromebookはH.264エンコーディングをサポートしていないため、最適化されたHDX Webカメラビデオ圧縮を使用できるのは32ビットアプリのみです。

Media Foundationベースのビデオアプリケーションは、Windows 10以降およびWindows Server 2019以降でHDX Webカメラビデオ圧縮をサポートします。詳細については、Knowledge Centerの記事CTX132764を参照してください。

その他のユーザーデバイス要件:

- サウンドを生成するための適切なハードウェア。
- DirectShow互換のWebカメラ（Webカメラのデフォルト設定を使用）。ハードウェアエンコーディング対応のWebカメラは、クライアント側のCPU使用率を削減します。
- HDX Webカメラビデオ圧縮の場合、可能であれば、カメラメーカーから入手したWebカメラドライバーをクライアントにインストールします。デバイスドライバーのインストールはサーバー上では不要です。

異なるWebカメラは異なるフレームレートを提供し、明るさやコントラストのレベルも異なります。Webカメラのコントラストを調整することで、アップストリームトラフィックを大幅に削減できます。Citrixは、初期機能検証のために以下のWebカメラを使用しています。

- Microsoft LifeCam VXモデル（2000、3000、5000、7000）
- クリエイティブ ライブ！カム オプティア プロ
- ロジクール クイックカム メッセンジャー
- ロジクール C600、C920
- HP デラックス ウェブカメラ

優先ビデオフレームレートを調整するには、クライアントでレジストリキーを編集します。詳細については、レジストリで管理される機能のリストにあるWebcam video compression frame rateを参照してください。

高解像度Webカメラストリーミング

サーバー上のビデオ会議アプリケーションは、サポートされているフォーマットタイプに基づいてWebカメラのフォーマットと解像度を選択します。セッションが開始されると、クライアントはWebカメラ情報をサーバーに送信します。アプリケーションからWebカメラを選択します。

Webカメラとビデオ会議アプリケーションが高解像度レンダリングをサポートしている場合、アプリケーションは高解像度を使用します。すべてのWebカメラ解像度をサポートしています。

この機能には、Citrix Workspace app for Windows バージョン1808以降、またはCitrix Receiver for Windows バージョン4.10以降が必要です。

レジストリキーを使用して、この機能を無効化および有効化できます。詳細については、レジストリで管理される機能のリストにある高解像度Webカメラストリーミングを参照してください。

メディアタイプのネゴシエーションが失敗した場合、HDXはデフォルトのVGA解像度（640 x 480 ピクセル）にフォールバックします。クライアントのレジストリキーを使用して、デフォルトの解像度を構成できます。カメラが指定された解像度をサポートしていることを確認してください。詳細については、レジストリで管理される機能のリストにあるHigh-definition webcam resolutionを参照してください。

HDX Webカメラビデオ圧縮は、プラグアンドプレイの汎用USBリダイレクトと比較して帯域幅を大幅に少なく使用し、WAN接続でも良好に機能します。帯域幅を調整するには、クライアントのレジストリキーを設定します。詳細については、レジストリで管理される機能のリストにある高解像度Webカメラ帯域幅を参照してください。

ビット/秒単位で値を入力します。帯域幅を指定しない場合、ビデオ会議アプリケーションはデフォルトで350000 bpsを使用します。

HDXプラグアンドプレイ汎用USBリダイレクト

HDX プラグアンドプレイ汎用USBリダイレクト（アイソクロナス）は、**汎用**ウェブカメラモードとも呼ばれます。HDX プラグアンドプレイ汎用USBリダイレクトの利点は、シンクライアント/エンドポイントにドライバーをインストールする必要がないことです。USBスタックは仮想化されており、ローカルクライアントに接続したものはすべてリモートVMに送信されます。リモートデスクトップは、ネイティブに接続したかのように動作します。Windowsデスクトップは、ハードウェアとのすべてのやり取りを処理し、正しいドライバーを見つけるためにプラグアンドプレイロジックを実行します。ほとんどのウェブカメラは、ドライバーがサーバーに存在すれば動作し、ICA経由で動作できます。汎用ウェブカメラモードは、ネットワーク経由でUSBプロトコルを使用して非圧縮ビデオを送信するため、大幅に多くの帯域幅（毎秒数メガビット）を使用します。

HTML5 マルチメディアリダイレクト

> **注:**

> HTML5 マルチメディアリダイレクトは、将来のリリースで廃止される予定です。お客様は、機能の継続性を確保するため、推奨される代替テクノロジーであるブラウザコンテンツリダイレクト (BCR) への移行をお勧めします。

> HTML5 マルチメディアリダイレクトは、HDX™ MediaStream のマルチメディアリダイレクト機能を拡張し、HTML5 のオーディオとビデオを含めます。マルチメディアコンテンツのオンライン配信、特にモバイルデバイスへの配信の増加により、ブラウザ業界はオーディオとビデオを提示するためのより効率的な方法を開発しました。

Flash は標準でしたが、プラグインが必要であり、すべてのデバイスで動作せず、モバイルデバイスではバッテリー消費量が多くなります。YouTube、Netflix、および Mozilla、Google、Microsoft の新しいブラウザバージョンなどの企業は HTML5 に移行しており、それを新しい標準にしています。

HTML5 ベースのマルチメディアには、独自のプラグインと比較して多くの利点があります。以下のようなものがあります。

- 企業に依存しない標準 (W3C)
- 簡素化されたデジタル著作権管理 (DRM) ワークフロー
- プラグインによって引き起こされるセキュリティ問題なしにパフォーマンスの向上

HTTP プログレッシブダウンロード

HTTP プログレッシブダウンロードは、HTML5 をサポートする HTTP ベースの擬似ストリーミング方式です。プログレッシブダウンロードでは、HTTP Web サーバーからダウンロード中に、ブラウザが単一ファイル (単一品質でエンコードされたもの) を再生します。ビデオは受信時にドライブに保存され、ドライブから再生されます。ビデオを再視聴する場合、ブラウザはキャッシュからビデオを読み込むことができます。

プログレッシブダウンロードの例については、HTML5 ビデオ リダイレクト テスト ページ を参照してください。ウェブページ内のビデオ要素を検査し、HTML5 ビデオタグ内のソース (mp4 コンテナ形式) を見つけるには、ブラウザの開発者ツールを使用します。

HTML5 と Flash の比較

機能	HTML5	フラッシュ
独自のプレーヤーが必要	いいえ	はい
モバイルデバイスで実行	はい	一部

機能	HTML5	フラッシュ
さまざまなプラットフォームでの実行速度	高	低速
iOSでサポート	はい	いいえ
リソース使用量	少ない	その他
より高速に読み込む	はい	いいえ

要件

mp4形式のプログレッシブダウンロードのリダイレクトのみをサポートしています。WebMやDASH/HLSのようなアダプティブビットレートストリーミング技術はサポートしていません。

以下をサポートしており、ポリシーを使用してこれらを制御します。詳細については、「マルチメディアポリシー設定」を参照してください。

- サーバー側レンダリング
- サーバーフェッチクライアントレンダリング
- クライアント側フェッチおよびレンダリング

Citrix Workspace™アプリおよびCitrix Receiver™の最小バージョン:

- Windows用Citrix Workspaceアプリ1808
- Windows用シトリックス レシーバー 4.5
- Linux用Citrix Workspaceアプリ1808
- Linux用シトリックス レシーバー 13.5

最小VDAブラウザバージョン	WINDOWS オーエス バージョン/ビルド/SP
インターネット エクスプローラー 11.0	Windows 10 の x86 (1607 RS1) 版および x64 (1607 RS1) 版； Windows 7 の x86 版および x64 版； Windows Server 2016 RTM 14393 (1607)； Windows Server 2012 R2
Firefox 47 証明書を手動でFirefox証明書ストアに追加するか、Windowsの信頼された証明書ストアから証明書を検索するようにFirefoxを設定します。詳細については、`https://`	Windows 10 の x86 (1607 RS1) 版および x64 (1607 RS1) 版； Windows 7 の x86 版および x64 版； Windows Server 2016 RTM 14393 (1607)； Windows Server 2012 R2

最小VDAブラウザバージョン	WINDOWS オーエス バージョン/ビルド/SP
`wiki.mozilla.org/CA:AddRootToFirefox` を参照してください。	
クローム 51	Windows 10 32ビット版 (1607 RS1) および 64ビット版 (1607 RS1)； Windows 7 32ビット版および 64ビット版； Windows サーバー 2016 RTM 14393 (1607)； Windows サーバー 2012 R2

HTML5ビデオリダイレクトソリューションのコンポーネント

- **HdxVideo.js** - Webサイト上のビデオコマンドをインターセプトするJavaScriptフック。HdxVideo.jsは、セキュアWebSocket (SSL/TLS) を使用してWebSocketServiceと通信します。
- **WebSocket SSL証明書**
  - CA (ルート) の場合: **Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX In-Product CA) 場所: **証明書 (ローカルコンピューター) > 信頼されたルート証明機関 > 証明書**。
  - エンドエンティティ (リーフ) の場合: **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX Service) 場所: **証明書 (ローカルコンピューター) > 個人 > 証明書**。
- **WebSocketService.exe** - ローカルシステムで実行され、SSL終端とユーザーセッションマッピングを実行します。127.0.0.1ポート9001でTLSセキュアWebSocketをリッスンします。
- **WebSocketAgent.exe** - ユーザーセッションで実行され、WebSocketServiceコマンドの指示に従ってビデオをレンダリングします。

HTML5ビデオのリダイレクトを有効にするにはどうすればよいですか?

このリリースでは、この機能は管理されたWebページでのみ利用可能です。HTML5マルチメディアコンテンツが利用可能なWebページに、HdxVideo.js JavaScript（Citrix Virtual Apps and Desktopsインストールメディアに含まれています）を追加する必要があります。たとえば、社内トレーニングサイトのビデオなどです。

Adaptive Bitrateテクノロジー（たとえば、HTTP Live Streaming (HLS) や Dynamic Adaptive Streaming over HTTP (DASH)）に基づいたyoutube.comのようなWebサイトはサポートされていません。

詳細については、「*マルチメディアポリシー設定*」を参照してください。

トラブルシューティングのヒント

WebページがHdxVideo.jsを実行しようとすると、エラーが発生する可能性があります。JavaScriptの読み込みに失敗すると、HTML5リダイレクトメカニズムも失敗します。ブラウザの開発者ツールウィンドウでコンソールを検査し、HdxVideo.jsに関連するエラーがないことを確認してください。例:

リダイレクト画像(/en-us/citrix-virtual-apps-desktops/2511/media/redirection7.png)

Microsoft Teams の最適化 (新規)

Citrix® は、VDI 環境で Microsoft Teams のオーディオとビデオを最適化する 2 つの方法をサポートしています。Citrix HDX™ 最適化と、Microsoft の Teams 向け新規 VDI ソリューションです。クラシック Teams はサポート終了となりましたので、このページで説明されている最適化アプローチは、現在の Microsoft Teams クライアントに適用されます。

> **注:**

> Microsoft は、Windows エンドポイントにおける WebRTC ベースの Citrix HDX Optimization for Microsoft Teams の非推奨化を発表しました。2つのマイルストーンが適用されます。

> - October 1, 2026 - サポート終了: Microsoft または Citrix による公式サポートは終了します。
> - April 1, 2027 - 提供終了: WebRTCベースの最適化は機能しなくなります。レガシー最適化のためのCitrix Studioポリシーは適用されなくなります。

> お客様は Teams 向け新規 VDI ソリューションへの移行を推奨されます。この変更は Windows エンドポイントのみに影響します。macOS、Linux、ChromeOS、および HTML5 エンドポイントは影響を受けません。詳細については、Microsoft Blog を参照してください。

最適化アプローチ

- **Citrix HDX Optimization (MTOP)**: Citrix と Microsoft の共同ソリューションで、Citrix が所有する仮想チャネル (CTXMTOP) を使用します。メディアオフロードは Citrix Workspace™ アプリの `HdxRtcEngine` によって処理されます。このソリューションは従来 MTOP と呼ばれています。
- **Teams 向け新規 VDI ソリューション**: Microsoft が所有および管理する新しい最適化で、Microsoft が所有する仮想チャネル (MSTEAMS、MSTEAM1、MSTEAM2) を使用します。Windows および Mac エンドポイントで利用可能です。詳細については、Microsoft ドキュメントの New VDI solution for Teams を参照してください。

主な違い

CITRIX HDX最適化	TEAMS 向け新規 VDI ソリューション
最適化は Citrix と Microsoft の共同ソリューションであり、Citrix が所有する仮想チャネル (CTXMTOP) を使用します。	最適化ソリューションは Microsoft が所有および管理しており、Microsoft が所有する仮想チャネル (MSTEAMS、MSTEAM1、MSTEAM2) を使用します。
メディアオフロードは、Citrix Workspaceアプリにある`HdxRtcEngine`によって処理されます。	メディアオフロードは、WindowsおよびMacエンドポイント上のSlimCoreメディアエンジンによって処理されます。
Citrix Workspaceアプリのインストールを除いて、エンドポイントに追加のコンポーネントは不要です。	追加コンポーネント - **Teams VDI Plugin** は、さまざまな方法でエンドポイントに展開する必要があります。このプラグインは、SlimCoreメディアエンジンのダウンロードと更新を管理します。
エンドポイントプラットフォームで利用可能 - Windows、macOS、Linux、およびChromeOS。	エンドポイントプラットフォームで利用可能 - WindowsおよびMac。
新機能は、CitrixとMicrosoftが連携して管理します。	新機能はMicrosoftによって管理されます。ユーザーは、Citrix HDX最適化では利用できない一部の新機能にアクセスできます。
関連するコンポーネントに応じて、CitrixとMicrosoftの両方によってサポートされます。お客様はCitrixまたはMicrosoftのいずれかにケー	Microsoftが所有およびサポートします。Citrixは、Citrix Workspaceアプリ、仮想チャネル許可リスト、プラグイン展開メカニズムなど、

CITRIX HDX最適化	TEAMS 向け新規 VDI ソリューション
スをオープンでき、必要に応じて適切なチームにリダイレクトされます。	関連するCitrixコンポーネントをサポートします。

相互運用性とローミング

Citrix HDX最適化とTeams向け新しいVDIソリューションは並行して存在できますが、Teamsクライアントは一度にそのうちの1つのみを使用します。

- Teamsアプリの起動時に、次の順序で最適化が選択されます。Teams向けの新VDIソリューション、次にCitrix HDX最適化 (WebRTC)、次に標準のオーディオ/ビデオリダイレクト。
- Teams向けの新VDIソリューションが失敗した場合、TeamsはWebRTCではなく、標準のオーディオ/ビデオリダイレクトに直接フォールバックします。選択を再実行し、適切な最適化を選択するには、Teamsアプリの再起動が必要です。
- エンドポイント間のローミングはシームレスであり、Teamsアプリの再起動は不要です。これには、ユーザーがTeams向け新しいVDIソリューションをサポートするエンドポイントとサポートしないエンドポイントの間をローミングする場合も含まれます。

Citrix HDX™ 最適化

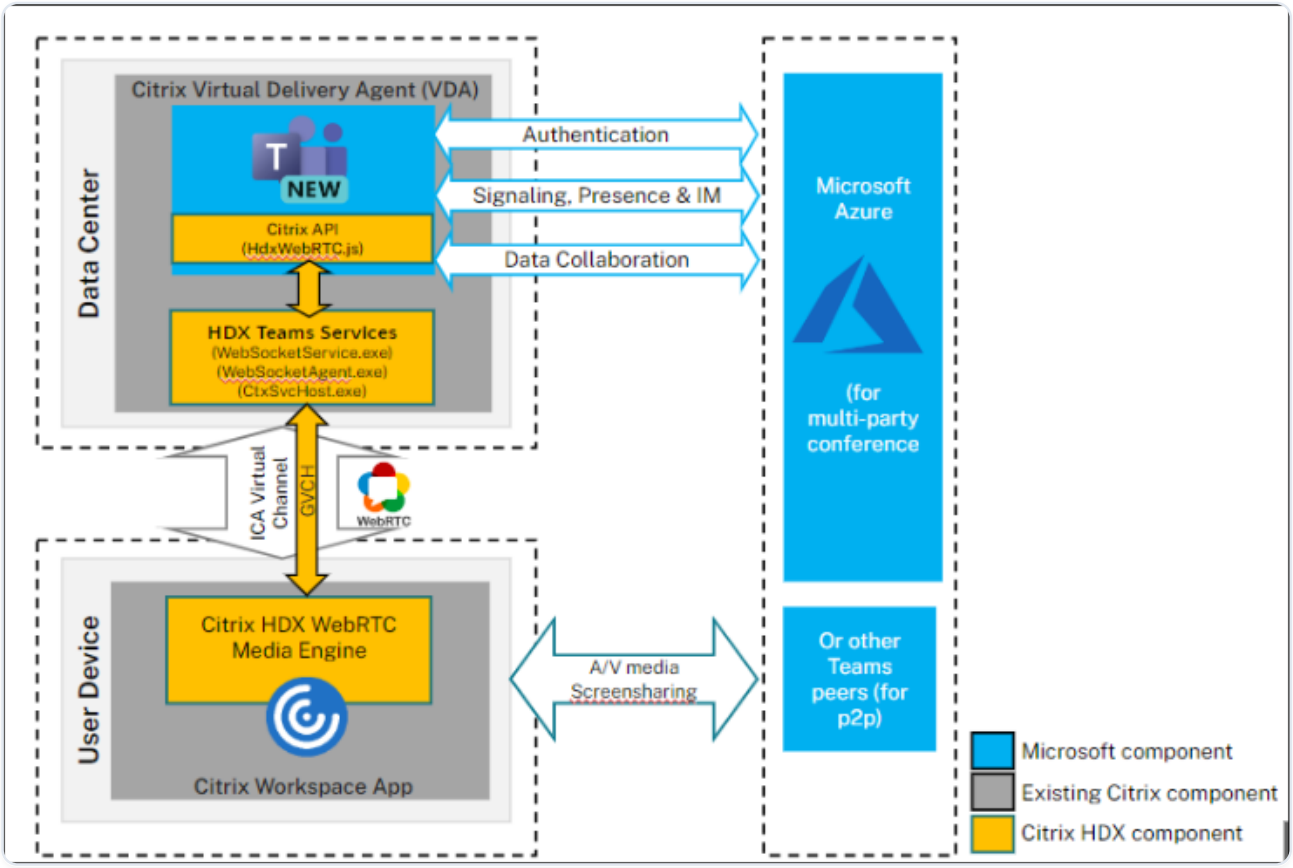
> **注:**

> Microsoft は、Windows エンドポイントにおける Microsoft Teams 向け WebRTC ベースの HDX 最適化の非推奨を発表しました。2つのマイルストーンが適用されます。

> - October 1, 2026 - サポート終了: Microsoft または Citrix による公式サポートは終了します
> - April 1, 2027 - 提供終了: Microsoft は、Windows エンドポイント向け HDX WebRTC 最適化の非推奨を発表しました。WebRTC ベースの最適化は機能しなくなります。従来の最適化に関する Citrix Studio ポリシーは適用されなくなります。

> お客様は、Microsoft Teams 向けの新 VDI ソリューション (SlimCore) への移行が推奨されます。この変更は Windows エンドポイントのみに影響し、macOS、Linux、ChromeOS、および HTML5 エンドポイントには影響しません。詳細については、Microsoft Blog を参照してください。

Citrix HDX (WebRTC 最適化) では、オフロードされたメディアの処理を担当するエンドポイント上のメディアエンジン (HdxRtcEngine) は Citrix Workspace™ アプリに組み込まれており、Citrix Workspace アプリをインストールすると、エンジンも自動的にインストールされます。



システム要件

このセクションでは、新しい Teams クライアントをサポートするために必要な最小バージョンと推奨バージョンについて説明します。最小バージョンでは、一部の重要なバグ修正や最新機能が利用できない場合があることに注意してください。最新の修正と機能で最高の体験を得るには、推奨バージョンを展開してください。

VDI オペレーティングシステム

詳細については、Microsoft ドキュメントに記載されている推奨事項を参照してください。

注:

- Windows Server 2016 はサポートされていません。Citrix は、それに応じてアップグレードを計画することをお勧めします。

- バージョンは頻繁に更新されるため、ここに記載されているバージョンはサポート終了となる可能性があります。したがって、さまざまなコンポーネントのサポートされているバージョンを使用していることを確認するために、Citrix Workspace app および Citrix Virtual Apps and Desktops の製品ライフサイクルページを参照してください。
- Citrix Virtual Apps and Desktops™ 1912 LTSR を使用している場合、2024 年 12 月にサポート終了となるため、Citrix はアップグレードを計画することをお勧めします。

仮想配信エージェント (VDA)

最小バージョン	推奨バージョン
1912 LTSR CU8+; 2203 LTSR (任意の CU); 2212 CR	2203 LTSR CU5+ (または) 2402 LTSR およびそれ以降のCRバージョン

シトリックス ワークスペース アプリ

最小バージョン	推奨バージョン
Windows 2203 LTSR (最新の累積更新プログラム)； Windows 2302 CR； Linux 2207； Mac 2302； Chrome/HTML5 2301	ウィンドウズ 2402 LTSR；ウィンドウズ 2405 CR；リナックス 2405；マック 2405；ChromeOS/HTML5 2405

展開

1. VDI に新しい Teams クライアントをインストールします。詳細については、「VDI 用の新しい Teams を展開する」を参照してください。
2. 新しい Teams を最適化するために、VDA で次のレジストリキーを構成します。

   - **場所**: `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`
   - **キー (REG_Multi_SZ)**: `ProcessWhitelist`
   - **値**: `msedgewebview2.exe`

   > **注:**
   >
   > Citrix Virtual Apps and Desktops 2402 LTSR (または) Citrix Virtual Apps and Desktops 2203 LTSR CU5+ 以降では、`msedgewebview2.exe` レジストリエントリはデフォルトで許可リストに含まれているため、手動で構成する必要はありません。

3. Microsoft Teams redirection ポリシーが有効になっていることを確認してください。このポリシーはデフォルトで有効になっています。
4. クライアント側で追加の構成は必要ありません。ウィザードの指示に従ってCitrix Workspaceアプリをインストールしてください。

App レイヤリング

新しいMicrosoft Teamsはインストール方法が変更され、C:\Program Files\WindowsApps にインストールされるようになりました。この変更をサポートするには、App Layeringバージョン2403.2以降を実行する必要があります。この修正を含むアップグレードディスクは、App Layering downloads ページからダウンロードできます。

詳細については、App Layering ドキュメントを参照してください。

Citrix プロファイル管理

New Microsoft Teams のローミングを有効にする方法については、Citrix Profile Management のドキュメントを参照してください。Citrix Profile Management の現在の最小バージョンガイダンスは 2402 LTSR (または) 2203 LTSR CU5+ です。

ネットワークに関する考慮事項

新しいTeamsのネットワーク要件は、従来のTeamsと変わりません。したがって、従来のTeamsドキュメントのNetwork Requirement セクションを参照してください。

機能リファレンス

パフォーマンスとユーザーエクスペリエンスを向上させる最適化されたオーバーレイクリッピング

CVAD 2511以降、HDX Microsoft Teams OptimizationやUCSDK Optimizationなどの機能におけるリダイレクトされたビデオオーバーレイを処理するメカニズムは、ユーザーエクスペリエンスとサーバーパフォーマンスの両方を向上させるために再設計されました。

主な利点

- **視覚的な精度の向上:** この機能強化により、ポップアップメニューや通知などのアプリケーション要素がビデオコンテンツの背後に誤って表示される視覚的な不具合が解消されます。新しいロジックにより、すべてのコンポーネントが正しい順序でレンダリングされ、よりシームレスで予測可能なエクスペリエンスが提供されます。
- **パフォーマンスの向上:** この最適化により、Virtual Delivery AgentでのCPU使用率が大幅に削減されます。古いリソース集約型のポーリング方法を、より効率的なグラフィックベースのアプローチに置き換えることで、この変更はサーバーのスケーラビリティを向上させ、より高いユーザー密度を可能にします。

注:

この機能は、将来のバージョンのMicrosoft Teams（またはその他のUCSDKパートナーアプリケーション）に依存し、Citrix Workspace App for Windows 2511が必要です。

機能マトリックスとバージョンサポート

バージョンは頻繁に更新されるため、ここで言及されている一部の古いバージョンはサポート終了となる可能性があります。したがって、異なるコンポーネントのサポートされているバージョンを使用していることを確認するために、Citrix Workspace App および Citrix Virtual Apps and Desktops の製品ライフサイクルページを参照してください。

注:

- ここで言及されているバージョンは、特定の機能がサポートされる最小バージョン、またはNew Teamsがサポートされる最小バージョンのうち、いずれか高い方です。
- 最小バージョンセクションに記載されているCitrix Virtual Apps™ and Desktops 1912 LTSR CU8+は、2024年12月にサポート終了となるため、以下の表には記載されていません。ただし、それまでは引き続きサポートされるバージョンです。
- Citrix Virtual Apps and Desktopsの最小バージョンが `N/A` である機能は、VDA側からの変更が一切なかったことを意味します。

機能	VDA (最小バージョン)	CITRIX WORKSPACE APP FOR WINDOWS (最小バージョン)	MAC版 CITRIX WORKSPACEアプリ (最小バージョン)	LINUX版 CITRIX WORKSPACEアプリ (最小バージョン)	CHROMEOS版 CITRIX WORKSPACEアプリ (最小バージョン)
オーディオ/ビデオ (P2Pおよび会議)	2203 LTSR (任意のCU)、2212 CR	2203 LTSR 最新CU、2302 CR	2302	2207	2301

機能	VDA (最小バージョン)	CITRIX WORKSPACE APP FOR WINDOWS (最小バージョン)	MAC版 CITRIX WORKSPACEアプリ (最小バージョン)	LINUX版 CITRIX WORKSPACEアプリ (最小バージョン)	CHROMEOS版 CITRIX WORKSPACEアプリ (最小バージョン)
画面共有	2203 LTSR (任意のCU)、2212 CR	2203 LTSR 最新CU、2302 CR	2302	2207	2301
i. 画面インジケーターの赤い枠線	2203 LTSR (任意のCU)、2212 CR	2203 LTSR 最新CU、2302 CR	2302	2207	いいえ
ii. キャプチャをDesktop Viewerに制限	2203 LTSR (任意のCU)、2212 CR	2203 LTSR 最新CU、2302 CR	2302	2207	いいえ
iii. マルチモニター	2203 LTSR (任意のCU)、2212 CR	2203 LTSR 最新CU、2302 CR	2302	2207	いいえ
DTMF	N/A	2203 LTSR 最新CU、2302 CR	2302	2207	2301
プロキシサーバーのサポート	N/A	2203 LTSR 最新CU、2302 CR	2302	2207	2305
アプリ共有	2203 LTSR (任意のCU)、2212 CR	2203 LTSR 最新CU、2302 CR	2302	2209	いいえ

機能	VDA (最小バージョン)	CITRIX WORKSPACE APP FOR WINDOWS (最小バージョン)	MAC版 CITRIX WORKSPACEアプリ (最小バージョン)	LINUX版 CITRIX WORKSPACEアプリ (最小バージョン)	CHROMEOS版 CITRIX WORKSPACEアプリ (最小バージョン)
ライブキャプション	N/A	2203 LTSR 最新CU、2302 CR	2302	2207	2303
ダイナミックe911	N/A	2203 LTSR 最新CU、2302 CR	2302	2207	2301
制御を付与	N/A	2203 LTSR 最新 CU、2302 CR	2302	2207	いいえ
制御を要求	N/A	2203 LTSR 最新 CU、2302 CR	2302	2207	2303
マルチウィンドウ	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新 CU、2302 CR	2302	2207	2303
会議の文字起こし	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新 CU、2302 CR	2302	2207	2303
背景のぼかし	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新 CU、2302 CR	2302	2212	2303
画面共有 (App	2203 LTSR (任意の	2402 LTSR, 2309.1 CR	2308	2311	いいえ

機能	VDA (最小バージョン)	CITRIX WORKSPACE APP FOR WINDOWS (最小バージョン)	MAC版 CITRIX WORKSPACEアプリ (最小バージョン)	LINUX版 CITRIX WORKSPACEアプリ (最小バージョン)	CHROMEOS版 CITRIX WORKSPACEアプリ (最小バージョン)
Protection使用時)	CU), 2212 CR				
サイマルキャスト	2203 LTSR (任意のCU), 2212 CR	2402 LTSR, 2305 CR	2305	2305	2312
セカンダリリンガー	2203 LTSR (任意のCU)、2212 CR	2402 LTSR、2307.1 CR	2308	2308	2312
システムオーディオを共有	2203 LTSR (任意のCU)、2212 CR	2402 LTSR、2403 CR	2405	2402	いいえ

トラブルシューティングとその他の考慮事項

新しいTeamsについては、CTX253754、Microsoft Teamsのトラブルシューティングを参照してください。新しいTeamsに関連する最新情報については、CTX585013を参照してください。

既知の制限事項

Citrix Workspaceアプリの制限事項

- HID サポート - 通話の応答と終了はサポートされていません。音量の上げ下げはサポートされています。
- ユーザーは VDA 上でスニッピングツールを使用している間、Microsoft Teams のコンテンツのスクリーンショットを撮ることはできません。ただし、クライアント側でスニッピングツールを使用した場合、コンテンツをキャプチャできます。
- システムオーディオ共有の制限事項

- RAVE および BCR リダイレクトされたアプリまたはタブで画面を共有している場合、この機能を使用してオーディオを共有することはできません。
- この機能は公開デスクトップでのみサポートされています。

VDAに関する制限事項

- 公開された（シームレスな）アプリケーションとしての新しいTeamsはサポートされていません。
  - CVAD 2402 LTSR、2203 LTSR CU5 以降で修正済み
- Citrix WorkspaceアプリのHigh DPI設定を「はい」に構成すると、リダイレクトされたビデオウィンドウがずれて表示されます。この制限は、モニターのDPIスケーリング係数が100%を超えて設定されている場合に発生します。
- Microsoft Teams 2.1は、一度に1つのWebカメラのリダイレクトのみをサポートします。ただし、シングルセッションVDAでは、複数のWebカメラのリダイレクトやプラグアンドプレイ（PnP）Webカメラのリダイレクトはサポートしていません。

Citrix WorkspaceアプリとVDAに関する制限事項

- 最適化された通話の音量は、クライアントマシンの音量バーを使用してのみ制御できます。VDA上では制御できません。

Microsoftからの制限事項の詳細については、「VDIでサポートされていない機能」を参照してください。

Teams向け新しいVDIソリューション

> **注:**
>
> Teams 向け新しい VDI ソリューションは、現在、Citrix® 上の Windows および Mac エンドポイント向けに一般提供されています。このソリューションには、最小限の Microsoft Teams バージョンが必要です。「システム要件」(#system-requirements) を参照してください。

Teams向け新しいVDIソリューションでは、MicrosoftはCitrix Virtual Channel SDKを使用してカスタム仮想チャネルを構築します。エンドポイントでは、メディアは`HdxRtcEngine`ではなく、Microsoftメディアエンジン (SlimCore) にオフロードされます。カスタム仮想チャネルは、VDA上のTeamsとエンドポイント上のメディアエンジン間の通信を伝送します。

注:

Microsoftは、WindowsエンドポイントにおけるWebRTCベースのCitrix HDX™ Optimization for Microsoft Teamsの廃止を発表しました。2つのマイルストーンが適用されます。

- October 1, 2026 - サポート終了: MicrosoftまたはCitrixによって公式にサポートされなくなります。
- April 1, 2027 - 提供終了: WebRTCベースの最適化は機能しなくなります。レガシー最適化のためのCitrix Studioポリシーは適用されなくなります。

お客様は、Teams 向け新しい VDI ソリューションへの移行が推奨されます。この変更は Windows エンドポイントのみに影響します。macOS、Linux、ChromeOS、および HTML5 エンドポイントは影響を受けません。詳細については、Microsoft Blog を参照してください。

このソリューションは Microsoft が所有および管理しています。Citrix は、関連する Citrix コンポーネント（Citrix Workspace™ アプリ、仮想チャネル許可リスト、およびこのページで説明されているプラグイン展開メカニズム）をサポートします。Microsoft が所有するアーキテクチャと詳細については、Microsoft ドキュメントのTeams 向け新しい VDI ソリューション を参照してください。

アーキテクチャ(/en-us/citrix-virtual-apps-desktops/2511/media/ms-slimcore-optimization.png)

システム要件

このセクションでは、Teams向け新しいVDIソリューションをサポートするために必要な最小バージョンと推奨バージョンを一覧表示します。最小バージョンでは、一部の重要なバグ修正や最新機能が利用できない場合があります。最良のエクスペリエンスを得るには、推奨バージョンを展開してください。

バーチャル デリバリー エージェント (VDA)

注:

2203 LTSR CU2以前、または2303 CR以前をご利用の場合は、これらのバージョンの制限を理解し、アップグレードを計画するためにCTX682593を参照してください。

最小バージョン	推奨バージョン
2203 LTSR CU3; 2305 CR	2203 LTSR CU5+; 2402 LTSR およびそれ以降のCR

Windows版 Citrix Workspaceアプリ

最小バージョン	推奨バージョン
2203 LTSR (最新CU); 2302 CR	2402 LTSR; 2405 CR以降

Mac向けCitrix Workspaceアプリ

最小バージョン	推奨バージョン
2508.10	2607 またはそれ以降

MacエンドポイントにはmacOS 14、15、または26が必要です。macOS 26では、Citrix Workspaceアプリ2511以降が必要です。Citrix Workspaceアプリ for Mac 2508.10では、プラグインを手動でインストールする必要があります。Citrix Workspaceアプリ、Client App Management、またはVirtual channel plug-in managerを介してプラグインをインストールするオプションは、Citrix Workspaceアプリ for Mac 2603以降で利用可能です。

最小Microsoft Teamsバージョン、エンドポイントOS要件、およびハードウェア要件については、Microsoftドキュメントを参照してください。

コンポーネント

- 新しいTeams `vdiBridge`: Teamsにバンドルされているサーバー側の仮想チャネルモジュール。
- カスタム仮想チャネル（VC）: Microsoft Teamsが所有するカスタムVC。
- プラグイン: クライアント側のVC DLL。メディアエンジンのダウンロードとクリーンアップを担当します。
- メディアエンジン（SlimCore）: MicrosoftがMSIXパッケージとして提供する、オペレーティングシステム固有のメディアエンジン。

展開

1. 前提条件に記載されているMicrosoft Teamsのバージョンがあることを確認してください。
2. Microsoft Teamsの仮想チャネルを許可するように、**仮想チャネル許可リスト**ポリシーを構成します。これらのチャネルにより、Teamsクライアントはクライアント側のプラグインに接続できます。詳細については、仮想チャネルセキュリティを参照してください。

   このソリューションには、3つのカスタム仮想チャネルが必要です。ワイルドカードを使用して、`ms-teams.exe`実行可能ファイルとカスタム仮想チャネルを許可します。

   ```
   MSTEAMS,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

   MSTEAM1,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

   MSTEAM2,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe
   ```

   注:

   - VDA 2603以降では、これら3つの仮想チャネルがデフォルトで許可されます。これらのバージョンでは、Studioポリシーの構成は不要です。
   - 仮想チャネル許可リストポリシーのワイルドカードは、CVAD 2203 LTSR CU2以降、またはCitrix Virtual Apps and Desktops™ 2206 CR以降で利用できます。
   - ポリシーを有効にするには、VDAマシンを再起動する必要があります。
   - MSTeamsのインストールパスはMSIXアプリケーションであるため変更されるため、ワイルドカードが必要です。上記に示されている正確な行を許可してください。

3. このソリューションは、Citrixポリシーではなく、Microsoft Teams側のポリシーによって制御されます。デフォルトで有効になっています。特定のユーザーグループに対して有効または無効にするには、Microsoftのドキュメントを参照してください。
4. エンドポイントにTeamsプラグインを展開します。Teamsプラグインをインストールするオプションを参照してください。
5. メディアエンジンのステージングと登録、およびMSIXのインストールをブロックできるグループポリシーについては、Microsoftのドキュメントを参照してください。

Teamsプラグインをインストールするオプション

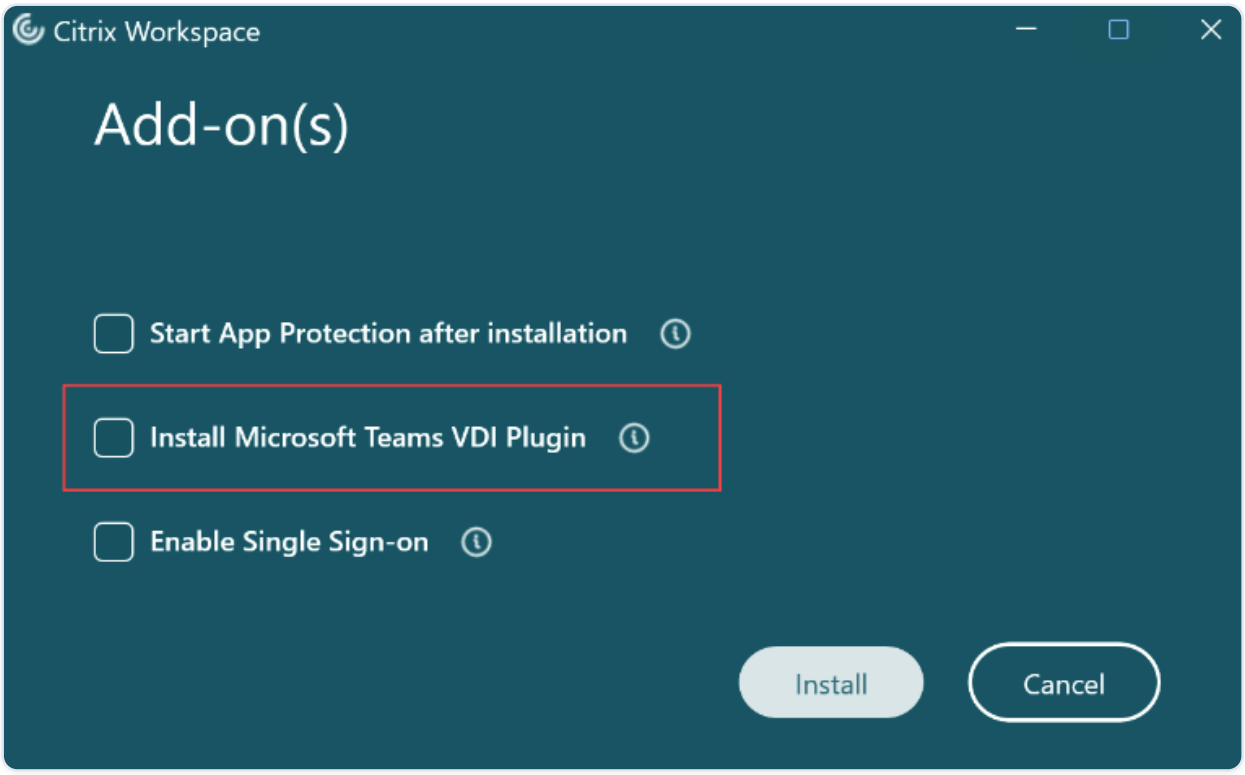
インストール方法に関係なく、プラグインはエンドポイントのCitrix Workspaceアプリの場所に配置されます。

- Windows (`MsTeamsPluginCitrix.dll`): 64ビット `C:\Program Files (x86)\Citrix\ICA Client` ; 32ビット `C:\Program Files\Citrix\ICA Client`
- Mac: `/Applications/Utilities/MsTeamsVdi.Plugin.app`

> **注:**
>
> - Windowsでは、仮想チャネルが正しく開くように、Citrix Workspaceアプリを管理者モードでインストールしてください。Citrix Workspaceアプリのユーザーごとのインストールはサポートされていません。
> - Citrix WorkspaceアプリがMicrosoft Storeからインストールされている場合、Microsoft Teams VDIプラグインはサポートされません。
> - エンドポイントにCitrix Workspaceアプリが見つからない場合、プラグインのインストールは停止します。
> - Windowsでは、プラグインとCitrix Workspaceアプリは同じアーキテクチャである必要があります。32ビットのCitrix Workspaceアプリは64ビットのプラグインをロードできません。
> - プラグインはアップグレードまたは修復できますが、ダウングレードはできません。また、アクティブなセッションがない場合にのみ可能です。

オプション1: Citrix Workspaceアプリのインストールによる方法

- **Windows:** 新規インストールまたは手動アップグレード中に、**アドオン**ページで**Microsoft Teams VDI プラグインのインストール**を選択します。Citrix Workspaceアプリ for Windows 2508以降では、このオプションはデフォルトで選択されています。インストールをスキップするには、このチェックを外します。アップグレードでは、以前の選択が記憶されます。



`/InstallMSTeamsPlugin`スイッチを使用してコマンドラインからインストールすることもできます。たとえば、`CitrixWorkspaceApp.exe /InstallMSTeamsPlugin=Y`はプラグインをインストールし、`/InstallMSTeamsPlugin=N`はインストールを防止します。

新規インストールの場合、最小要件はCitrix Workspaceアプリ for Windows 2402 LTSRです。インプレースアップグレードの場合、最小要件はCitrix Workspaceアプリ for Windows 2405 CRです。最新の詳細については、「サードパーティ製プラグインのインストール」を参照してください。

- **Mac:** Citrix Workspaceアプリのインストール中にプラグインをインストールするオプションは、Citrix Workspaceアプリ for Mac 2603以降で利用可能であり、ユーザー操作が必要です。Citrix Workspaceアプリ for Mac 2607では、プラグインがデフォルトで自動的にインストールされます。Citrix Workspaceアプリ for Mac 2508.10では、プラグインを手動でインストールします。「オプション2：プラグインを直接ダウンロードする」を参照してください。

オプション2: プラグインを直接ダウンロードする

- **Windows:** MSIをダウンロードし、SCCMやIntuneなどのツールを使用して、サポートされている任意のCitrix Workspaceアプリのバージョンに展開します。
  - 32ビットCitrix Workspaceアプリ：aka.ms/plugin
  - 64ビットCitrix Workspaceアプリ：aka.ms/plugin_x64
  - ArmベースのCitrix Workspaceアプリ：aka.ms/plugin_arm64

- **Mac:** aka.ms/macpluginからプラグインをダウンロードし、JAMFなどのツールを使用して展開します。

オプション3: クライアントアプリ管理 (旧Global App Configurationサービス)

クライアントアプリ管理（旧Global App Configurationサービス、またはGACS）は、管理対象および非管理対象のエンドポイントのアプリ設定を管理し、エンドポイント全体にTeamsプラグインを展開できます。Macでは、Citrix Workspaceアプリ for Mac 2603以降が必要です。「Microsoft Teams VDIプラグイン管理」を参照してください。

オプション4: 仮想チャネルプラグインマネージャー

仮想チャネルプラグインマネージャーは、クライアントエンドポイント全体にプラグインを展開します。これには、Teams向けの新VDIソリューションを含む、エンドポイントコンポーネントを必要とするアプリケーションが含まれます。VDAで実行されているアプリケーションを検出し、ユーザーにエンドポイントへのプラグインのインストールを促します。管理者はBYODシナリオでこれを使用できます。Macでは、Citrix Workspaceアプリ for Mac 2603以降が必要です。「仮想チャネルプラグインマネージャー」を参照してください。

プラグインの更新シナリオ

プラグインがオプション1、3、または4を通じてインストールされている場合、CitrixはTeamsプラグインの更新をシームレスに処理します。プラグインが手動でインストールされている場合 (オプション2)、Citrixは更新を処理しません。

- プラグインの自動更新のために、Citrix Workspaceアプリの自動更新がオンになっていることを確認してください。
- Citrix Workspaceアプリ for Windows 2405以降であることを確認してください。Citrix Workspaceアプリ for Windows 2508以降では、Citrix Workspaceアプリが自動更新されるとプラグインが自動的にインストールされます。
- Citrixはプラグインのアンインストールを処理しません。必要に応じて、プラグインを個別にアンインストールしてください。

注：

CitrixはTeamsプラグインの更新を処理しますが、メディアエンジンの更新は処理しません。Microsoftがメディアエンジンを提供し、更新します。

Citrix公開アプリとしてのTeams

Citrix Virtual Appsアプリケーションとして公開されたTeamsは、必要なすべてのコンポーネントが最小バージョンを満たしている場合、このソリューションで最適化できます。必要なバージョンと既知の制限については、Microsoftドキュメントを参照してください。

相互運用性とローミング

Teams向け新規VDIソリューションとCitrix HDX最適化がどのように相互運用し、ローミングがどのように動作するかについては、Microsoft Teamsの最適化 を参照してください。

ネットワークに関する考慮事項

Microsoftドキュメントのネットワークに関する考慮事項を参照してください。

機能サポート

機能セットと実装はMicrosoftが所有しています。Microsoftドキュメントの機能リストを参照してください。

トラブルシューティング

Microsoft Teamsクライアントは最適化ステータスを報告し、最適化が失敗した場合はエラーコードを報告します。これらのステータスインジケーターとエラーコードはMicrosoftによって定義されています。完全なリストとエンドツーエンドのトラブルシューティングについては、MicrosoftドキュメントのTeams向けNew VDIソリューションのトラブルシューティングを参照してください。

Citrix Monitorは、このソリューションの最適化状態を可視化します。セッションの詳細にあるセッショントポロジビューには、アプリケーションが最適化されているかどうか、およびプラグインマネージャー、プラグインとそのバージョン、仮想チャネルの状態、仮想チャネル許可リストのステータスなど、不足しているコンポーネントが示されます。詳細については、リアルタイム通信最適化の可視性を参照してください。

一部のMicrosoftエラーコードは、Citrix側の構成を示しています。一般的なCitrixの確認事項：

- Teamsクライアントがカスタム仮想チャネルがブロックされていると報告した場合（Microsoftエラー2003）、仮想チャネル許可リストにMSTEAMS、MSTEAM1、およびMSTEAM2が含まれていることを確認してください。
- Teamsクライアントがプラグインが検出されないと報告した場合（Microsoftエラー2000）、プラグインがインストールされ、ロードされていることを確認してください。Process Explorerで`wfica32.exe`を選択し、下部ペインを表示して、DLLタブで`MsTeamsPluginCitrix.dll`を確認してください。

- Teamsクライアントがサポートされていないバージョンを報告した場合（Microsoftエラー2004）、サポートされているバージョンにアップグレードしてください。システム要件を参照してください。

既知の制限事項

機能と実装はMicrosoftが所有しています。Microsoftのドキュメントで既知の問題を参照してください。

Microsoft Teams (Classic) の最適化

> **注:**
>
> 新しいMicrosoft Teams 2.1は、VDAで一般提供されるようになりました。このMicrosoft Teamsバージョンは、WebRTC (VDI 1.0) を使用したCitrix Microsoft Teams最適化と互換性があります。

> Citrix Virtual Apps and Desktops 2402以降、`msedgewebview2.exe` レジストリエントリはデフォルトで許可リストに含まれているため、手動で構成する必要はありません。

> 公開アプリケーションは、新しいMicrosoft Teamsでサポートされるようになりました。

> Citrixは、Citrix Virtual Apps and Desktops™およびCitrix Workspace™アプリを使用して、デスクトップベースのMicrosoft Teamsの最適化を提供します。デフォルトでは、必要なすべてのコンポーネントがCitrix WorkspaceアプリとVirtual Delivery Agent (VDA) にバンドルされています。

Microsoft Teamsの最適化には、VDA側のHDX™サービスと、コマンドを受信するためにMicrosoft Teamsホストアプリとインターフェイスするための APIが含まれています。これらのコンポーネントは、制御仮想チャネル (CTXMTOP) をCitrix Workspaceアプリ側のメディアエンジンに開きます。エンドポイントはマルチメディアをローカルでデコードして提供し、Citrix Workspaceアプリウィンドウをホストされた Microsoft Teamsアプリに戻します。

認証とシグナリングは、他のMicrosoft Teamsサービス（チャットやコラボレーションなど）と同様に、Microsoft Teamsホストアプリでネイティブに行われます。オーディオ/ビデオのリダイレクトはこれらに影響しません。

`CTXMTOP` はコマンドおよび制御仮想チャネルです。つまり、Citrix WorkspaceアプリとVDAの間でメディアは交換されません。

クライアントフェッチ/クライアントレンダリングのみが利用可能です。

このビデオデモンストレーションでは、Citrix仮想環境でMicrosoft Teamsがどのように機能するかを理解できます。



Microsoft Teamsのインストール

CitrixとMicrosoftは、Microsoft Teamsの最新バージョンを使用し、常に最新の状態に保つことを推奨しています。 リリース日が現在のバージョンのリリース日より90日以上古いMicrosoft Teamsデスクトップアプリのバージョンはサポートされていません。 サポートされていないMicrosoft Teamsデスクトップアプリのバージョンは、ユーザーにブロックページを表示し、アプリの更新を要求します。

最新バージョンについては、「Microsoft Teamsアプリ (デスクトップおよびMac) の更新履歴」を参照してください。

「Microsoft Teams のマシン全体へのインストールガイドライン」に従うことをお勧めします。`AppData` に Microsoft Teams をインストールする .exe インストーラーの使用は避けてください。代わりに、コマンドラインから `ALLUSER=1` フラグを使用して `C:\Program Files (x86)\Microsoft\Teams` にインストールしてください。

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1 ALLUSERS=1
```

この例では、`ALLUSERS=1` パラメーターも使用します。このパラメーターを設定すると、Microsoft Teams Machine-Wide Installer が **コントロールパネル** の **プログラムと機能** に表示されます。また、コンピューターのすべてのユーザーに対して、Windows の設定の **アプリと機能** にも表示されます。すべてのユーザーは、管理者資格情報があれば Microsoft Teams をアンインストールできます。

`ALLUSERS=1` と `ALLUSER=1` の違いを理解することが重要です。`ALLUSERS=1` パラメーターは、非 VDI 環境と VDI 環境の両方で使用できます。`ALLUSER=1` パラメーターは、マシンごとのインストールを指定するために VDI 環境でのみ使用してください。

`ALLUSER=1` モードでは、新しいバージョンがリリースされても Microsoft Teams アプリケーションは自動更新されません。このモードは、Windows Server または Windows 10 のランダム/プールされたカタログからのホスト型共有アプリやデスクトップなど、非永続的な環境に推奨されま

す。詳細については、「MSI を使用した Microsoft Teams のインストール」(VDI インストールセクション) を参照してください。

Windows 10 の専用永続 VDI 環境があるとします。Microsoft Teams アプリケーションを自動更新し、Microsoft Teams を `Appdata/Local` の下にユーザーごとにインストールしたい場合は、`.exe` インストーラーまたは `ALLUSER=1` なしの MSI を使用してください。

注:

Citrix は、ゴールデンイメージに Microsoft Teams をインストールする前に VDA をインストールすることを推奨します。このインストール順序は、`ALLUSER=1` フラグを有効にするために必要です。VDA をインストールする前に仮想マシンに Microsoft Teams をインストールした場合は、Microsoft Teams をアンインストールして再インストールしてください。

Remote PC Access の場合

Citrix は、VDA のインストール後に Microsoft Teams バージョン 1.4.00.22472 以降をインストールすることを推奨します。そうしないと、Microsoft Teams が VDA を期待どおりに検出するために、サインアウトして再度サインインする必要があります。バージョン 1.4.00.22472 以降には、Microsoft Teams の起動時およびサインイン時に実行される VDA 検出のための拡張ロジックが含まれています。これらのバージョンには、アクティブなセッションタイプ識別 (HDX、RDP、またはクライアントマシンへのローカル接続) も含まれています。ローカル接続の場合、以前のバージョンの Microsoft Teams は、特定の機能や UI 要素 (ブレイクアウトルーム、会議やチャットのポップアウトウィンドウ、会議のリアクションなど) を検出して無効にできない場合があります。

重要:

ローカルセッションから HDX セッションにローミングし、Microsoft Teams がバックグラウンドで開いたまま実行されている場合、HDX で正しく最適化するには、Microsoft Teams を終了して再起動する必要があります。 逆に、最適化された HDX セッションを介してリモートで Microsoft Teams を使用している場合は、HDX セッションを切断し、デバイスで同じ Windows セッションにローカルで再接続します。オフィスで作業している場合は、Microsoft Teams が Remote PC Access の状態 (HDX またはローカル) を正しく検出できるように、Microsoft Teams を再起動する必要があります。これは、Microsoft Teams が VDI モードを評価できるのはアプリの起動時のみであり、バックグラウンドで既に実行されている間ではないためです。再起動しないと、Microsoft Teams はポップアウトウィンドウ、ブレイクアウトルーム、会議のリアクションなどの機能を読み込めない場合があります。

App Layering の場合

Citrix App Layering を使用して VDA と Microsoft Teams のインストールを異なるレイヤーで管理している場合、コマンドラインから `ALLUSER=1` フラグを使用して Microsoft Teams をインストールする前に、Windows VDA 上にレジストリキーを作成する必要があります。詳細については、「マルチメディア」の「*Citrix App Layering を使用した Microsoft Teams の最適化*」セクションを参照してください。

プロファイル管理の推奨事項

Windows Server およびプールされた VDI Windows 10 環境には、マシン全体のインストーラーを使用することをお勧めします。

コマンドラインから MSI に **ALLUSER=1** フラグが渡されると (マシン全体のインストーラー)、Microsoft Teams アプリは `C:\Program Files (x86)` (~300 MB) にインストールされます。このアプリは、ログに `AppData\Local\Microsoft\TeamsMeetingAddin` を、ユーザー固有の設定、ユーザーインターフェイスの要素のキャッシュなどに `AppData\Roaming\Microsoft\Teams` (~600〜700 MB) を使用します。

重要:

ローカルセッションからHDXセッションにローミングし、Microsoft Teamsがバックグラウンドで開いたまま実行されている場合、HDXで正しく最適化するには、Microsoft Teamsを終了して再起動する必要があります。 逆に、最適化されたHDXセッションを介してMicrosoft Teamsをリモートで使用している場合は、HDXセッションを切断し、デバイスで同じWindowsセッションにローカルで再接続します。オフィスで作業している場合は、Microsoft TeamsがリモートPCアクセス状態（HDXまたはローカル）を正しく検出できるように、Microsoft Teamsを再起動する必要があります。これは、Microsoft TeamsがVDIモードを評価できるのはアプリ起動時のみであり、バックグラウンドで既に実行されている間は評価できないためです。再起動しないと、Microsoft Teamsはポップアウトウィンドウ、ブレイクアウトルーム、会議のリアクションなどの機能を読み込めない可能性があります。

App Layeringの場合

Citrix App Layeringを使用してVDAとMicrosoft Teamsのインストールを異なるレイヤーで管理する場合、コマンドラインから`ALLUSER=1`フラグを使用してMicrosoft Teamsをインストールする前に、Windows VDA上にレジストリキーを作成する必要があります。詳細については、「」(/ja-jp/

citrix-virtual-apps-desktops/2511/policies/reference/hdx-registry-settings.html#multimedia)の「*Citrix App Layeringを使用したMicrosoft Teamsの最適化*」セクションを参照してください。

プロファイル管理の推奨事項

Windows ServerおよびプールされたVDI Windows 10環境には、マシン全体のインストーラーを使用することをお勧めします。

コマンドラインからMSIに**ALLUSER=1**フラグ（全ユーザー向けインストーラー）が渡されると、Microsoft Teamsアプリは`C:\Program Files (x86)`（約300 MB）にインストールされます。このアプリは、ログに`AppData\Local\Microsoft\TeamsMeetingAddin`を、ユーザー固有の構成、ユーザーインターフェイス要素のキャッシュなどに`AppData\Roaming\Microsoft\Teams`（約600〜700 MB）を使用します。

> **重要:**
>
> 代わりに、その後のユーザーログオンによって **AppData** に最終インストールがトリガーされます。

マシン全体のインストーラー

以下は、Windows Server 64ビットVMにMicrosoft Teamsの全ユーザー向けインストーラーをインストールすることによって作成されるフォルダー、デスクトップショートカット、およびレジストリの例です。

フォルダー:

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

デスクトップショートカット:

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

レジストリ:

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

- 名前: `Teams`
- 種類: `REG_SZ`
- 値: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> **注:**
>
> レジストリの場所は、基盤となるオペレーティングシステムとビット数によって異なります。

推奨事項

- Microsoft Teamsのレジストリキーを削除して自動起動を無効にすることをお勧めします。これにより、同時に発生する多数のログオン（たとえば、勤務開始時など）によるVMのCPUスパイクを防ぐことができます。
- 仮想デスクトップにGPU/vGPUがない場合、パフォーマンスを向上させるために、Microsoft Teamsの**設定**で**GPUハードウェアアクセラレーションを無効にする**ことをお勧めします。この設定 (`"disableGpu":true`) は、 `desktop-config.json` の `%Appdata%\Microsoft\Teams` に保存されています。ログオンスクリプトを使用してそのファイルを編集し、値を `true` に設定できます。
- Citrix Workspace Environment Management™ (WEM)を使用している場合は、Microsoft Teamsのプロセッサ消費を管理するために**CPUスパイク保護**を有効にしてください。

ユーザーごとのインストーラー

`.exe` インストーラーを使用する場合、インストールプロセスが異なります。すべてのファイルはAppDataに配置されます。

フォルダー:

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

デスクトップショートカット:

`C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe"`

レジストリ:

`HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

ベストプラクティス

ベストプラクティスの推奨事項は、ユースケースシナリオに基づいています。 非永続的な設定でMicrosoft Teamsを使用する場合、効率的なMicrosoft Teamsランタイムデータ同期のためにプロファイルキャッシュマネージャーが必要です。プロファイルキャッシュマネージャーを使用すると、ユーザーセッション中に適切なユーザー固有の情報がキャッシュされます。たとえば、ユーザー固有の情報には、ユーザーデータ、プロファイル、設定が含まれます。これら2つのフォルダーのデータを同期します。

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

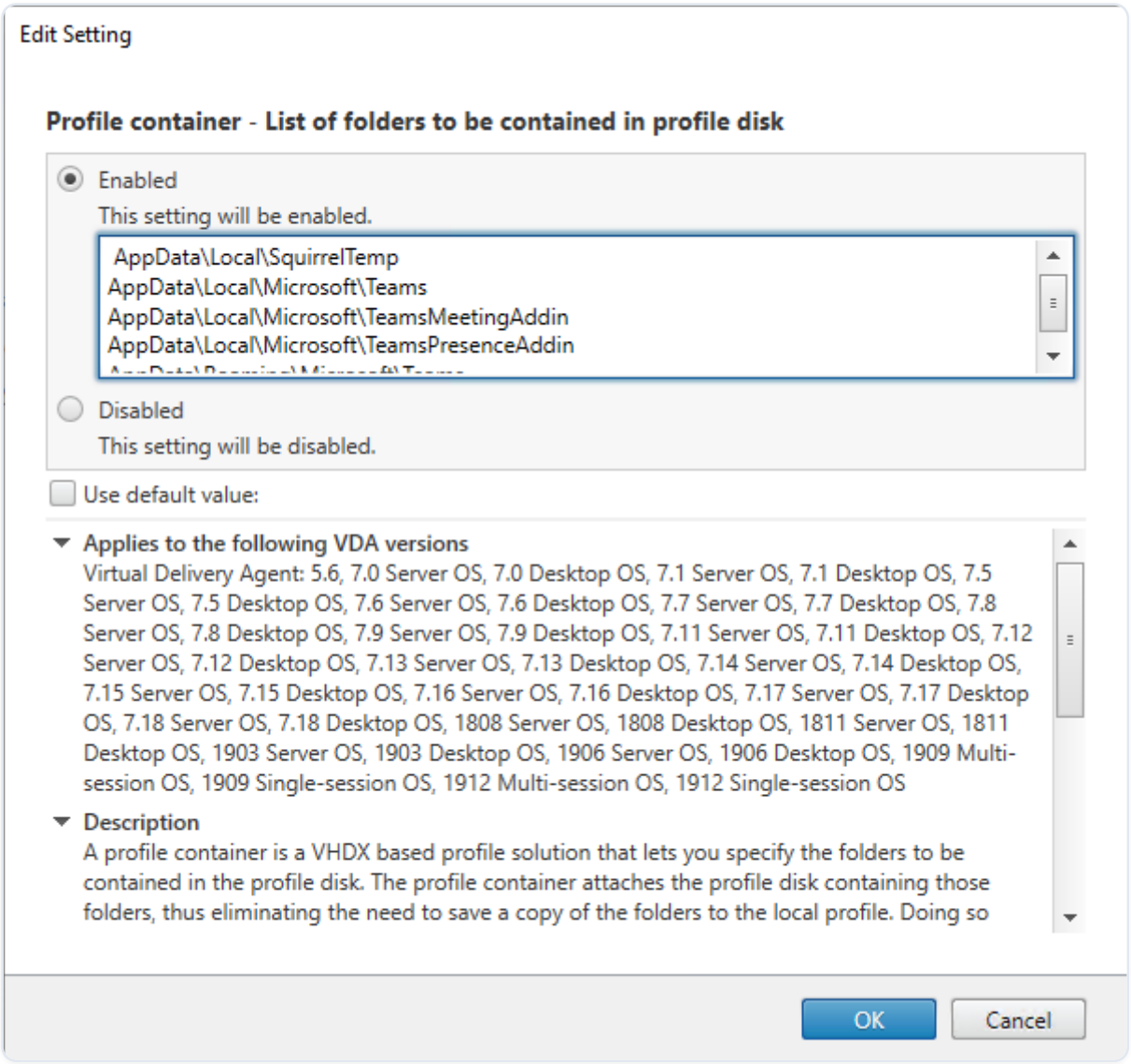
非永続的セットアップ向けの Microsoft Teams キャッシュコンテンツ除外リスト

Microsoft ドキュメントに記載されているように、Microsoft Teams のキャッシュフォルダーからファイルとディレクトリを除外します。この操作により、ユーザーのキャッシュサイズを削減し、非永続的セットアップをさらに最適化できます。

ユースケース: シングルセッションシナリオ

このシナリオでは、エンドユーザーは一度に1つの場所でMicrosoft Teamsを使用します。同時に2つのWindowsセッションでMicrosoft Teamsを実行する必要はありません。一般的な仮想デスクトップ展開では、各ユーザーに1つのデスクトップが割り当てられ、Microsoft Teamsは仮想デスクトップに1つのアプリケーションとして展開されます。 Citrix Profileコンテナを有効にし、ユーザーごとのインストーラーにリストされているユーザーごとのディレクトリをコンテナにリダイレクトすることをお勧めします。

1. ゴールデンイメージにMicrosoft Teams マシン全体インストーラー (**ALLUSER=1**) を展開します。
2. Citrix Profile Management を有効にし、適切な権限でユーザープロファイルストアを設定します。
3. 次のProfile Managementポリシー設定を有効にします: **ファイルシステム > 同期 > プロファイルコンテナ – プロファイルディスクに含めるフォルダーのリスト。**



この構成内のすべてのユーザーごとのディレクトリをリストします。これらの設定は、Citrix Workspace Environment Management (WEM) サービスを使用して構成することもできます。

4. 適切なデリバリーグループに設定を適用します。
5. ログインして展開を検証します。

システム要件

推奨される最小バージョン - Delivery Controller (DDC) 1906.2

以前のバージョンを使用している場合は、Microsoft Teams の最適化を有効にするを参照してください。

サポートされているオペレーティングシステム:

- Windows Server 2022、2019、2016、2012R2 Standard および Datacenter Edition、および Server Core オプション

最小バージョン - Virtual Delivery Agent (VDA) 1906.2

サポートされているオペレーティングシステム:

- ウィンドウズ 11
- Windows 10 64-bit、バージョン 1607 以降。VM ホスト型アプリは、Citrix Workspace アプリ for Windows 2109.1 以降でサポートされています。
- Windows Server 2022、2019、2016、および 2012 R2 (Standard および Datacenter エディション)

要件:

- BCR_x64.msi - Microsoft Teams の最適化コードを含み、GUI から自動的に起動する MSI。VDA インストールにコマンドラインインターフェイスを使用している場合は、除外しないでください。

推奨バージョン – Citrix Workspace アプリ for Windows 最新 CR および最小バージョン – Citrix Workspace アプリ 1907 for Windows

- ウィンドウズ 11。
- Windows 10 (32 ビット版および 64 ビット版、Embedded エディションを含む) (Windows 7 のサポートはバージョン 2006 で終了しました) (Windows 8.1 のサポートはバージョン 2204.1 で終了しました)。
- Windows 10 IoT エンタープライズ 2016 LTSB (v1607) および 2019 LTSC (v1809)。
- サポートされるプロセッサ (CPU) アーキテクチャ: x86 および x64 (ARM はサポートされていません)。
- エンドポイント要件: ピアツーピアのビデオ会議中に 720p HD 解像度をサポートできる、約 2.2〜2.4 GHz のデュアルコア CPU。
- Intel Turbo Boost または AMD Turbo Core を搭載し、少なくとも 2.4 GHz までブーストできる、ベース速度が低い (~1.5 GHz) デュアルコアまたはクアッドコア CPU。
- 検証済み HP Thin Client: t630/t640、t730/t740、mt44/mt45。
- 検証済み Dell Thin Client: 5070、5470 Mobile TC および AIO。
- 検証済み 10ZiG Thin Client: 4510 および 5810q。
- 検証済みエンドポイントの完全なリストについては、「Thin Clients」を参照してください。
- Citrix Workspaceアプリには、少なくとも600 MBの空きディスク容量と1 GBのRAMが必要です。

- Microsoft .NET Frameworkの最小要件はバージョン4.8です。Citrix Workspaceアプリは、システムに.NET Frameworkが存在しない場合、自動的にダウンロードしてインストールします。

管理者は、Microsoft Teams Optimization policyを変更することで、最適化モードでMicrosoft Teamsを開始/無効化できます。Citrix Workspaceアプリで最適化モードで開始するユーザーは、Microsoft Teamsを無効にできません。

最小バージョン - Linux向けCitrix Workspaceアプリ2006

詳しくは、Linux向けCitrix WorkspaceアプリのドキュメントのOptimization for Microsoft Teamsを参照してください。

ソフトウェア:

- `GStreamer` 1.0以降、またはCairo 2
- `libc++-9.0`以降
- `libgdk` 3.22以降
- OpenSSL 1.1.1d
- `libnsl`
- Ubuntu 20.04以降

認証の強化:

- Libsecretライブラリ
- libunwind-12ライブラリ。詳しくは、Adding the libunwind-12 library dependency for llvm-12を参照してください。

ハードウェア:

- ピアツーピアのビデオ会議通話中に720p HD解像度をサポートできる、最低1.8 GHzのデュアルコアCPU
- ベース速度1.8 GHz、Intel Turbo Boostの高速が2.9 GHz以上のデュアルコアまたはクアッドコアCPU

検証済みエンドポイントの完全なリストについては、Thin Clientsを参照してください。

詳細については、Citrix Workspaceアプリをインストールするための前提条件を参照してください。

`/opt/Citrix/ICAClient/config/module.ini`ファイルで**VDWEBRTC**フィールドの値をOffに更新することで、Microsoft Teamsの最適化を無効にできます。デフォルトはVDWEBRTC=Onです。更新が完了したら、セッションを再起動してください。(ルート権限が必要です)。

最小バージョン - Mac用Citrix Workspaceアプリ2012

サポートされているオペレーティングシステム:

- macOS カタリナ (10.15)。
- macOS Big Sur 11.0.1以降。
- macOS モントレー。

サポートされる機能:

- オーディオ
- ビデオ
- 画面共有の最適化 (送受信)

> **注:**

> 画面共有を機能させるには、Citrix Viewerアプリがmacosの「セキュリティとプライバシー」設定へのアクセスを必要とします。ユーザーは、**Appleメニュー > システム設定 > セキュリティとプライバシー > プライバシータブ > 画面収録**でこの設定を構成し、**Citrix Viewer**を選択します。

> Microsoft Teamsの最適化は、Citrix Workspaceアプリ2012以降およびmacOS 10.15でデフォルトで機能します。

Microsoft Teamsの最適化を無効にする場合は、ターミナルでこのコマンドを実行し、Citrix Workspaceアプリを再起動してください。

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

最小バージョン - ChromeOSの最新バージョンで実行されているChromeOS用Citrix Workspaceアプリの最新バージョン

ハードウェア:

- Intel i3、クアッドコア2.4 GHzと同等以上の性能を持つプロセッサ。

サポートされる機能:

- オーディオ
- ビデオ
- 画面共有の最適化（受信および送信） - デフォルトで無効になっています。有効にする方法については、これらの設定を参照してください。

シングルサーバーのスケーラビリティ

このセクションでは、単一の物理ホストでサポートできるユーザー数または仮想マシン（VM）数を推定するための推奨事項とガイダンスを提供します。これは一般にCitrix Virtual Apps™ and Desktopsシングルサーバーのスケーラビリティ（SSS）と呼ばれます。Citrix Virtual Apps（CVA）またはセッション仮想化のコンテキストでは、ユーザー密度としても一般に知られています。その目的は、主要なハイパーバイザーを実行している単一のハードウェアで、いくつのユーザーまたはVMを実行できるかを明らかにすることです。

> **注:**
>
> このセクションでは、SSS を推定するためのガイダンスを説明します。このガイダンスは一般的なものであり、お客様固有の状況や環境に必ずしも特化したものではない場合があります。Citrix Virtual Apps and Desktops の SSS を真に理解する唯一の方法は、Login VSI のようなスケーラビリティまたはロードテストツールを使用することです。Citrix は、SSS を迅速に推定するためだけに、このガイダンスとこれらの簡単なルールを使用することを推奨します。ただし、ハードウェアを購入したり、財務上の決定を下したりする前に、結果を検証するために Login VSI または選択したロードテストツールを使用することをCitrixは推奨します。

ハードウェア (テスト対象システム)

- デル パワーエッジ R740
- Intel Xeon (Gold) 6126 @ 2.60 GHz (最大ターボ 3.70 GHz)、ソケットあたり 12 コア、ハイパースレッディング有効のデュアルソケット
- 382 GB の RAM
- ローカル SSD RAID 0 ストレージ (11 ディスク) 6 TB

ソフトウェア

Citrix Virtual Apps and Desktops 2106 を実行する Windows 2019 (TSVDA) を搭載した単一の仮想マシン (40 論理プロセッサ) VMware ESXi 6.7

用語

- ナレッジワーカーのワークロード: Acrobat Reader、Freemind/Java、フォトビューアー、Edge、および Excel、Outlook、PowerPoint、Word などの MS Office アプリが含まれます。
- ベースライン: ナレッジワーカーのワークロード (Microsoft Teams なし) で実行されるサーバーのスケーラビリティテスト。
- Microsoft Teams ワークロード: ナレッジワーカーの一般的なワークロード + Microsoft Teams。

Microsoft Teams のストレステスト方法

- Microsoft Teams は HDX で最適化されています。そのため、すべてのマルチメディア処理はエンドポイントまたはクライアントにオフロードされ、測定の一部ではありません。
- ワークロードが開始される前に、すべての Microsoft Teams プロセスが停止または強制終了されます。
- Microsoft Teams を開く（コールドスタート）。
- Microsoft Teams の読み込みにかかる時間と、Microsoft Teams のプライマリウィンドウのフォーカスを取得する時間を測定します。
- キーボードショートカットを使用してチャットウィンドウに切り替えます。
- キーボードショートカットを使用してカレンダーウィンドウに切り替えます。
- キーボードショートカットを使用して、特定のユーザーにチャットメッセージを送信します。
- キーボードショートカットを使用して Microsoft Teams ウィンドウに切り替えます。

結果

- Microsoft Teams ワークロード（81ユーザー）では、ベースライン（137ユーザー）と比較して、スケーラビリティに40%の影響があります。
- サーバー容量を約40%（CPU）増やすと、ベースラインワークロードの場合と同じユーザー数に戻ります。
- Microsoft Teams ワークロードでは、ベースラインと比較して20%の追加メモリが必要です。
- ユーザーあたりのストレージサイズを512〜1024 MB増やします。

- IOPS書き込みが約50%増加し、IOPS読み取りが約100%増加します。Microsoft Teams は、ストレージが遅い環境では大きな影響を与える可能性があります。

機能マトリックスとバージョンサポート

機能	MICROSOFT TEAMS（最小バージョン）	VDA (最小バージョン)	CITRIX WORKSPACEアプリ FOR WINDOWS CR (最小バージョン)	CITRIX WORKSPACEアプリ FOR MAC (最小バージョン)	CITRIX WORKSPACEアプリ FOR LINUX (最小バージョン)	CITRIX WORKSPACEアプリ FOR CHROME OS (最小バージョン)
オーディオ/ビデオ (P2Pおよび会議)	現在のバージョンから90日前	1906	1907	2009	2004	2105.5
画面共有	現在のバージョンから90日前	1906	1907	2012	2006	2105.5
i. 画面インジケーターの赤い枠線	現在のバージョンから90日前	1906	2002	2012	2006	いいえ
ii. キャプチャをDesktop Viewerに制限	現在のバージョンから90日前	1906	2009.5	2012	2006	いいえ
iii. マルチモニター	現在のバージョンから90日前	1912 CU6+	2106 (1)	2106	2106	いいえ
DTMF	現在のバージョ	N/A	2102	2101	2101	2111.1

機能	MICROSOFT TEAMS (最小バージョン)	VDA (最小バージョン)	CITRIX WORKSPACEアプリ FOR WINDOWS CR (最小バージョン)	CITRIX WORKSPACEアプリ FOR MAC (最小バージョン)	CITRIX WORKSPACEアプリ FOR LINUX (最小バージョン)	CITRIX WORKSPACEアプリ FOR CHROME OS (最小バージョン)
	ンから90日前					
プロキシサーバーのサポート	現在のバージョンから90日前まで	N/A	2012 (2)	2104 (3)	2101 (3)	2305
アプリ共有	現在のバージョンから90日前まで	2109	2109.1	2203.1	2209	いいえ
ライブキャプション	現在のバージョンから90日前	N/A (4)	2109.1	2109	2109	2303
ダイナミックe911	現在のバージョンから90日前	N/A	2112.1	2112	2112	2112
制御を付与	現在のバージョンから90日前	N/A	2112.1	2203.1	不可	不可
制御を要求	現在のバージョンから90日前	N/A	2112.1	2203.1	2203	2303

機能	MICROSOFT TEAMS (最小バージョン)	VDA (最小バージョン)	CITRIX WORKSPACEアプリ FOR WINDOWS CR (最小バージョン)	CITRIX WORKSPACEアプリ FOR MAC (最小バージョン)	CITRIX WORKSPACEアプリ FOR LINUX (最小バージョン)	CITRIX WORKSPACEアプリ FOR CHROME OS (最小バージョン)
マルチウィンドウ	1.5.00.11865	2112, 1912 CU6 (5)	2112.1	2203.1	2203	2303
会議の文字起こし	現在のバージョンから90日遡ったもの	2112.1, 1912 CU6+	2112	2203.1	2203	2303
背景ぼかし	現在のバージョンから90日遡ったもの	2112, 1912 CU6+	2207	2301	2212	2303

1. CD Viewerは全画面モードのみ。SHIFT+F2はサポートされていません。
2. Negotiate/Kerberos、NTLM、Basic、およびDigest。`Pac`ファイルもサポートされています。
3. 匿名のみ。
4. VDAが2112以降の場合、ライブキャプションは、Citrix Workspaceアプリのバージョンが Mac用2203.1、Linux用2203、またはWindows用2112の場合にのみ機能します。これは、Microsoft Teamsがシングルウィンドウ UIモードまたはマルチウィンドウモードの場合、ライブキャプションの動作が異なるためです。
5. マルチウィンドウは2112 VDAで導入されましたが、VDA 1912 LTSR CU6リリースにバックポートされました。

> **注:**

- **Citrix Workspace app for Windows 1912 CU6（またはそれ以降）**に記載されているすべての機能は、Citrix Workspace app for Windows 2203.1 LTSR CU1に適用されます。
- Microsoftは、Microsoft Teamsでのシングルウィンドウモードのサポートを非推奨にしました。これに対応するため、VDAを1912 CU6+ LTSRに、Citrix Workspaceアプリを2203 CU2+以降にアップグレードする必要があります。これらはMultiWindowモードをサポートしています。

Microsoft Teamsの最適化を有効にする

Microsoft Teamsの最適化を有効にするには、Microsoft Teams redirectionポリシーに記載されている管理ポリシーを使用します。このポリシーはデフォルトで**ON**になっています。このポリシーが有効になっていることに加え、HDXはCitrix Workspaceアプリのバージョンが最低要件を満たしていることを確認します。ポリシーを有効にし、Citrix Workspaceアプリのバージョンがサポートされている場合、VDA上の**HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport**は自動的に**1**に設定されます。Microsoft Teamsは、VDIモードでロードするためにこのキーを読み取ります。

注:

バージョン1906.2以降のVDA、またはManageコンソール（Studio）でポリシーが利用できない古いコントローラーバージョン（バージョン7.15など）を使用している場合でも、VDAを最適化できます。Microsoft TeamsのHDX最適化は、VDAでデフォルトで有効になっています。

About > Versionをクリックすると、**Citrix HDX Optimized**の凡例が表示されます。

Citrix向けに最適化された凡例(/en-us/citrix-virtual-apps-desktops/2511/media/teams-opt.png)

Citrix HDX Not Connected と表示される場合、Citrix APIはMicrosoft Teamsにロードされています。APIのロードはリダイレクトへの最初のステップですが、スタックの後続の部分でエラーが発生しています。エラーはVDAサービスまたはCitrix Workspaceアプリにある可能性が最も高いです。

Citrix向けに最適化されていない凡例(/en-us/citrix-virtual-apps-desktops/2511/media/teams-not-conn.png)

凡例が表示されない場合、Microsoft TeamsはCitrix APIの読み込みに失敗しています。通知領域のアイコンを右クリックしてMicrosoft Teamsを終了し、再起動してください。Manageポリシーが**Prohibited**に設定されておらず、Citrix Workspaceアプリのバージョンがサポートされていることを確認してください。

Citrix凡例なし(/en-us/citrix-virtual-apps-desktops/2511/media/teams-no-api.png)

> **重要: セッションの再接続**

- 接続が変更された場合、HDX最適化セッションを取得するためにMicrosoft Teamsを再起動する必要がある場合があります。たとえば、サポートされていないエンドポイント（iOS、Android、または古いバージョンのWindows/Linux/Mac用Workspaceアプリ）からサポートされているエンドポイント（Windows/Linux/Mac/ChromeOS/HTML5用Workspaceアプリ）にローミングする場合、またはその逆の場合です。
- VDAにMicrosoft Teamsの.exeインストーラーを使用してアプリをインストールした場合も、Microsoft Teamsの再起動が必要です。.exeインストーラーは、永続VDI展開に推奨されます。そのような場合、HDXセッションが切断状態にある間にMicrosoft Teamsが自動更新されることがあります。そのため、HDXセッションに再接続するユーザーは、Microsoft Teamsが最適化されて実行されていないことに気づきます。
- ローカルセッションからHDXセッションにローミングする場合、HDXで最適化するためにMicrosoft Teamsを再起動する必要があります。この操作は、リモートPCアクセスシナリオで必要です。

ネットワーク要件

Microsoft Teamsは、会議や多人数通話のためにMicrosoft 365のメディアプロセッササーバーに依存しています。また、Microsoft Teamsは、以下のシナリオでMicrosoft 365トランスポートリレーに依存しています。

- ポイントツーポイント通話の2つのピアが直接接続できない場合
- 参加者はメディアプロセッサに直接接続できません。

したがって、ピアとMicrosoft 365クラウド間のネットワークの状態が通話のパフォーマンスを決定します。ネットワーク計画に関する詳細なガイドラインについては、Microsoft 365 network connectivity principlesを参照してください。

クラウド音声およびビデオの全体的な展開に影響を与える可能性のあるリスクと要件を特定するために、環境を評価することをお勧めします。 Skype for Business Network Assessment Toolを使用して、ネットワークがMicrosoft Teamsに対応しているかどうかをテストします。サポート情報については、Supportを参照してください。

Real Time Protocol (RTP) トラフィックに関する主要なネットワーク推奨事項の概要

- 支店から可能な限り直接Microsoft 365ネットワークに接続します。
- 支店で十分な帯域幅を計画し、提供します。
- 各支店のネットワーク接続と品質を確認します。
- 支店で以下のいずれかを使用する必要がある場合は、RTP/UDPトラフィック (Citrix WorkspaceアプリのHdxRtcEngine.exeによって処理される) が妨げられないことを確認してください。
  - プロキシサーバーのバイパス
  - ネットワークSSLインターセプト
  - ディープパケットインスペクションデバイス
  - VPNヘアピン（可能であればスプリットトンネリングを使用）

> **重要: VPNスプリットトンネル構成**

> HdxRtcEngine.exeトラフィックはVPNトンネルから迂回させ、ユーザーのローカルインターネット接続を使用してサービスに直接接続できるようにする必要があります。これを実現する方法は、使用されるVPN製品とマシンプラットフォームによって異なりますが、ほとんどのVPNソリューションでは、このロジックを適用するためのポリシーの簡単な構成が可能です。VPNプラットフォーム固有のスプリットトンネルガイダンスの詳細については、この Microsoft記事を参照してください。

> WorkspaceアプリのWebRTCメディアエンジン (HdxRtcEngine.exe) は、クライアントにオフロードされるマルチメディアストリームにSecure Real-time Transport Protocol (SRTP) を使用します。SRTPはRTPに機密性と認証を提供します。この機能では、対称鍵 (DTLSでネゴシエートされる) を使用して、AES暗号化方式でメディアと制御メッセージを暗号化します。

良好なユーザーエクスペリエンスのために、以下のメトリックが推奨されます。

メトリック	エンドポイントからMICROSOFT 365
遅延 (片道)	< 50 ミリ秒
遅延 (RTT)	< 100 ミリ秒
パケット損失	15秒間隔で1%未満
パケット到着間隔ジッター	15秒間隔で30ミリ秒未満

詳細については、「Microsoft Teams 向けに組織のネットワークを準備する」を参照してください。

帯域幅要件については、Microsoft Teams の最適化では、オーディオ (OPUS/G.722/PCM G711) およびビデオ (H264) 用にさまざまなコーデックを使用できます。

ピアは、セッション記述プロトコル (SDP) Offer/Answer を使用して、通話確立プロセス中にこれらのコーデックをネゴシエートします。 Citrix のユーザーあたりの最小推奨事項は次のとおりです。

タイプ	帯域幅	コーデック
音声 (双方向)	約 90 kbps	G.722
音声 (双方向)	約 60 kbps	オーパス*
ビデオ (双方向)	約 700 kbps	H264 360p で 30 fps 16:9
画面共有	約 300 kbps	H264 1080p、15フレーム/秒

* Opusは、6 kbpsから510 kbpsまでの定ビットレートおよび可変ビットレートエンコーディングをサポートしています。

OpusとH264は、ピアツーピアおよび電話会議に推奨されるコーデックです。

> **重要:**

> パフォーマンスに関して、クライアントマシンでのCPU使用率では、デコードよりもエンコードの方がコストがかかります。LinuxおよびWindows版Citrix Workspaceアプリで、最大エンコード解像度をハードコードできます。(/ja-jp/citrix-workspace-app-for-windows/

> configure.html#encoder-performance-estimator)および(/ja-jp/citrix-workspace-app-for-linux/configure-xenapp.html#optimization-for-microsoft-teams)を参照してください。

プロキシサーバー

プロキシの場所に応じて、以下を考慮してください。

- VDAでのプロキシ構成:

  VDAで明示的なプロキシサーバーを構成し、localhostへの接続をプロキシ経由でルーティングすると、リダイレクトは失敗します。プロキシを正しく構成するには、**Internet Options > Connections > LAN Settings > Proxy Servers**で**Bypass proxy servers for local address**設定を選択し、`127.0.0.1:9002`をバイパスする必要があります。

  PACファイルを使用する場合、PACファイルからのVDAプロキシ構成スクリプトは、`wss://127.0.0.1:9002`に対して**DIRECT**を返す必要があります。そうでない場合、最適化は失敗します。スクリプトが**DIRECT**を返すことを確認するには、`shExpMatch(url, "wss://127.0.0.1:9002/*")`を使用します。

- Citrix Workspaceアプリでのプロキシ構成:

  支社がプロキシ経由でインターネットにアクセスするように構成されている場合、以下のバージョンがプロキシサーバーをサポートします。

  - Citrix Workspaceアプリ for Windows バージョン 2012 (Negotiate/Kerberos、NTLM、Basic、Digest。`Pac`ファイルもサポートされています)
  - Citrix Workspaceアプリ for Windows バージョン 1912 CU5 (Negotiate/Kerberos、NTLM、Basic、Digest。`Pac`ファイルもサポートされています)
  - Citrix Workspaceアプリ for Linux バージョン 2101 (匿名認証)
  - Citrix Workspaceアプリ for Mac バージョン 2104 (匿名認証)

以前のバージョンのCitrix Workspaceアプリを搭載したクライアントデバイスは、プロキシ構成を読み取ることができません。これらのデバイスは、トラフィックをMicrosoft 365 TURNサーバーに直接送信します。

> **重要:**

- クライアントデバイスがDNS解決を行うためにDNSサーバーに接続できることを確認してください。クライアントデバイスは、以下のMicrosoft Teamsリレーサーバーの FQDN を解決できる必要があります。
  - `worldaz.relay.teams.microsoft.com`
  - `inaz.relay.teams.microsoft.com`
  - `uaeaz.relay.teams.microsoft.com`
  - `euaz.relay.teams.microsoft.com`
  - `usaz.relay.teams.microsoft.com`
  - `turn.dod.teams.microsoft.us`
  - `turn.gov.teams.microsoft.us`

DNS要求が失敗した場合、外部ユーザーとのP2P通話およびメディア確立を伴う会議通話は失敗します。

- 会議サーバーの場所は、最初の参加者の仮想デスクトップの場所に基づいて選択されます（クライアントではありません）。

通話の確立とメディアフローパス

可能な場合、Citrix WorkspaceアプリのHDX WebRTCメディアエンジン（HdxRtcEngine.exe）は、ピアツーピア通話でUser Datagram Protocol (UDP) を介した直接的なネットワークSecure Real-time Transport Protocol (SRTP) 接続を確立しようとします。UDPの高ポートがブロックされている場合、メディアエンジンはTCP/TLS 443にフォールバックします。

HDXメディアエンジンは、候補の検出と接続の確立のために、ICE、Session Traversal Utilities for NAT (STUN)、およびTraversal Using Relays around NAT (TURN) をサポートしています。このサポートは、エンドポイントがDNS解決を実行できる必要があることを意味します。

2つのピア間、またはピアと会議サーバー間に直接パスがなく、多人数通話または会議に参加しているシナリオを考えてみましょう。HdxRtcEngine.exeは、Microsoft 365のMicrosoft Teamsトランスポートリレーサーバーを使用して、他のピアまたは会議がホストされているメディアプロセッサに到達します。クライアントマシンは、3つのMicrosoft 365サブネットIPアドレス範囲と4つのUDPポート（UDPがブロックされている場合はフォールバックとしてTCP/TLS 443）にアクセス

できる必要があります。詳細については、通話設定およびOffice 365のURLとIPアドレス範囲ID 11のアーキテクチャ図を参照してください。

ID	カテゴリ	アドレス	宛先ポート
11	最適化が必要	13.107.64.0/18, 52.112.0.0/14, 52.122.0.0/15	**UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (フォールバック)

これらの範囲には、Azure Load Balancer をフロントエンドとするトランスポートリレーとメディアプロセッサの両方が含まれます。 Microsoft Teams トランスポートリレーは STUN および TURN 機能を提供しますが、ICE エンドポイントではありません。また、Microsoft Teams トランスポートリレーは、メディア、TLS を終端したり、トランスコーディングを行ったりしません。他のピアまたはメディアプロセッサにトラフィックを転送する際に、TCP (HdxRtcEngine.exe が TCP を使用する場合) を UDP にブリッジできます。

Workspace app WebRTC メディアエンジンは、Microsoft 365 クラウド内の最も近い Microsoft Teams トランスポートリレーに接続します。メディアエンジンは、エニーキャスト IP とポート 3478〜3481 UDP (ワークロードごとに異なる UDP ポートですが、多重化が発生する可能性があります)、またはフォールバック用に 443 TCP/TLS を使用します。通話品質は、基盤となるネットワークプロトコルに依存します。UDP は常に TCP よりも推奨されるため、ブランチオフィスで UDP トラフィックに対応できるようにネットワークを設計することをお勧めします。

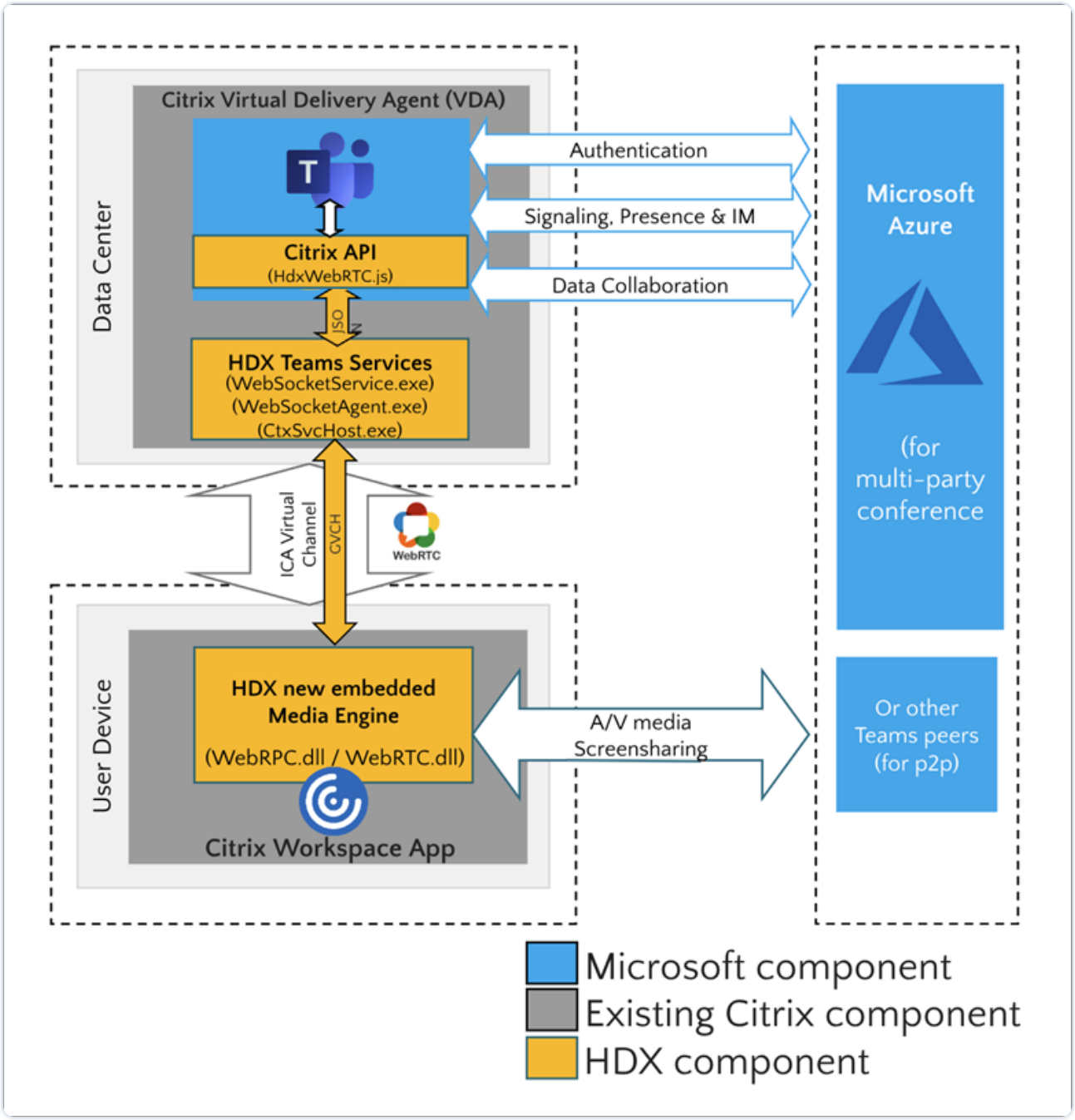
Microsoft Teams が最適化モードでロードされ、HdxRtcEngine.exe がエンドポイントで実行されている場合、ICE の障害により、通話設定の失敗や、音声/ビデオが片方向のみになる可能性があります。通話が完了できない場合やメディアストリームが全二重でない場合は、まずエンドポイントの **Wireshark トレース**を確認してください。ICE 候補収集プロセスについて詳しくは、「Support」セクションの「ログの収集」を参照してください。

> **注：**
>
> エンドポイントがインターネットにアクセスできない場合でも、両方のユーザーが同じ LAN 上にあれば、ピアツーピア通話を行うことができます。会議は失敗します。この場合、通話設定が開始されるまでに 30 秒のタイムアウトがあります。

通話設定

このアーキテクチャ図を、通話フローシーケンスの視覚的な参照として使用してください。対応する手順は図に示されています。

アーキテクチャ



1. Microsoft Teams を起動します。
2. Microsoft Teams は O365 に対して認証を行います。テナントポリシーが Microsoft Teams クライアントにプッシュダウンされ、関連する TURN およびシグナリングチャネル情報がアプリに中継されます。

3. Microsoft Teams は VDA で実行されていることを検出し、Citrix JavaScript API に API 呼び出しを行います。
4. Microsoft Teams 内の Citrix JavaScript は、VDA で実行されている WebSocketService.exe へのセキュアな WebSocket 接続を開き、これによりユーザーセッション内で WebSocketAgent.exe が生成されます。
5. WebSocketAgent.exe は、Citrix HDX Microsoft Teams Redirection Service (CtxSvcHost.exe) を呼び出すことにより、汎用仮想チャネルをインスタンス化します。
6. Citrix Workspace アプリの wfica32.exe (HDX エンジン) は、HdxRtcEngine.exe と呼ばれる新しいプロセスを生成します。これは、Microsoft Teams の最適化に使用される新しい WebRTC エンジンです。
7. Citrix メディアエンジンと Teams.exe は双方向の仮想チャネルパスを持ち、マルチメディア要求の処理を開始できます。

   -----ユーザー通話------

8. **ピア A** が **通話** ボタンをクリックします。Teams.exe は Microsoft 365 の Microsoft Teams サービスと通信し、**ピア B** とのエンドツーエンドのシグナリングパスを確立します。Microsoft Teams は HdxRtcEngine に一連のサポートされている通話パラメーター（コーデック、解像度など、Session Description Protocol (SDP) オファーとして知られる）を要求します。これらの通話パラメーターは、シグナリングパスを使用して Microsoft 365 の Microsoft Teams サービスに、そしてそこから他のピアに中継されます。
9. SDP オファー/アンサー（シングルパスネゴシエーション）はシグナリングチャネルを介して行われ、ICE 接続チェック（STUN バインド要求を使用した NAT およびファイアウォールトラバーサル）が完了します。その後、Secure Real-time Transport Protocol (SRTP) メディアは HdxRtcEngine.exe と他のピア（会議の場合は Microsoft 365 会議サーバー）の間で直接流れます。

マイクロソフト フォンシステム

Phone System は、Microsoft 365 クラウドで Microsoft Teams を使用して通話制御と PBX を可能にする Microsoft のテクノロジーです。Microsoft Teams の最適化は、Microsoft 365 Calling Plans または Direct Routing を使用して Phone System をサポートします。Direct Routing を使用すると、追加のオンプレミスソフトウェアなしで、サポートされている独自のセッションボーダーコントローラーを Microsoft Phone System に直接接続できます。 通話キュー、転送、保留、ミュート、通話の再開がサポートされています。

DTMF

デュアルトーン多周波 (DTMF) 機能は、Citrix Workspace アプリの以下のバージョン (およびそれ以降) でサポートされています。

- Citrix Workspace アプリ for Windows バージョン 2102
- シトリックス ワークスペース アプリ Windows 用 LTSR 1912 CU5 (Windows 10 OS のみ)
- Citrix Workspace アプリ for Linux バージョン 2101
- Citrix Workspace アプリ for Mac バージョン 2101
- Citrix Workspace アプリ for ChromeOS バージョン 2111.1

動的 e911 のサポート

バージョン 2112 以降、Citrix Workspace アプリは動的な緊急通報をサポートしています。Microsoft Calling Plans、Operator Connect、および Direct Routing で使用する場合、次のことが可能になります。

- 緊急通報の設定とルーティング。
- セキュリティ担当者への通知。

通知は、VDA で実行されている Microsoft Teams クライアントではなく、エンドポイントで実行されている Citrix Workspace アプリの現在の場所に基づいて提供されます。

Ray Baum 法では、911 通報者の派遣可能な場所を適切な公共安全応答拠点 (PSAP) に送信することが義務付けられています。HDX を使用した Microsoft Teams の最適化は、Citrix Workspace アプリの以下のバージョンで使用する場合、Ray Baum 法に準拠しています。

- Citrix Workspace アプリ for Windows バージョン 2112.1 以降
- Citrix Workspace アプリ for Linux バージョン 2112 以降
- Citrix Workspace アプリ for Mac バージョン 2112 以降
- ChromeOS バージョン 2112 以降の Citrix Workspace アプリ

動的な緊急通報を有効にするには、管理者はMicrosoft Teams管理センターを使用して、ネットワークまたは緊急ロケーションマップを作成するために以下を構成する必要があります。

- ネットワーク設定
- ロケーション情報サービス (LIS)

動的緊急通報の詳細については、Microsoft のドキュメントを参照してください。

Citrix Workspace アプリが Microsoft Teams に中継する派遣可能な位置情報は次のとおりです。

- イーサネット/スイッチ接続用のリンク層検出プロトコル (LLDP) を使用したシャーシ ID / ポート ID。イーサネット/スイッチ (LLDP) は以下でサポートされています。
  - Windows バージョン 8.1 および 10
  - macOS。LLDP 有効化ソフトウェアが必要です。LLDP 有効化ソフトウェアをダウンロードするには、`www.microsoft.com` にアクセスし、LLDP 有効化ソフトウェアを検索してください。
  - Linux。シンクライアントのオペレーティングシステム (OS) ディストリビューションに LLDP ライブラリを含める必要があります。
- Citrix Workspace アプリがインストールされているエンドポイントの WLAN BBSID および {IPv4-IPv6; サブネット; MAC アドレス}。
  - サブネットおよび WiFi ベースのロケーションは、Windows、Linux、および Mac 用 Workspace アプリでサポートされています。
- 緯度と経度 (Citrix Workspace アプリがインストールされている OS レベルでユーザー権限が付与されている場合 (権限は HDX RTC Engine に設定されています))
  - すべての Workspace アプリプラットフォームでサポートされています。ただし、Citrix Workspace for Linux の場合、シンクライアントの OS ディストリビューションに `libgps` ライブラリを含める必要があります (>sudo apt-get install libgps23 gpsd lldpd)。

ファイアウォールの考慮事項

ユーザーがMicrosoft Teamsクライアントを使用して最適化された通話を初めて開始すると、**Windowsファイアウォール**の設定に関する警告が表示されることがあります。この警告は、HdxTeams.exeまたはHdxRtcEngine.exe（HDX Overlay Microsoft Teams）の通信を許可するようユーザーに求めます。

ファイアウォールの警告](/en-us/citrix-virtual-apps-desktops/2511/media/firewall1.png)

Windows Defender Firewall > Advanced Securityコンソールで、**受信の規則**の下に次の4つのエントリが追加されます。必要に応じて、より制限の厳しい規則を適用することもできます。

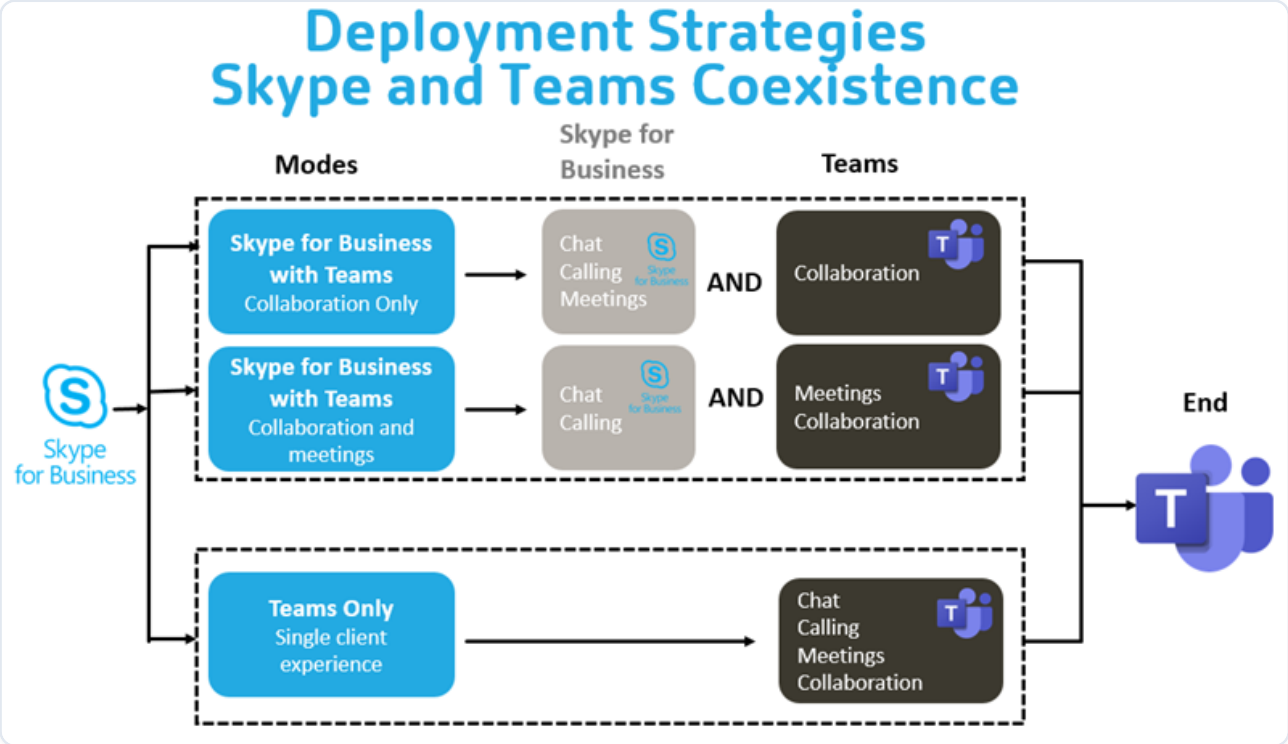
ファイアウォールの受信規則](/en-us/citrix-virtual-apps-desktops/2511/media/firewall2.png)

マイクロソフト チームズ と スカイプ フォー ビジネス の共存

Microsoft TeamsとSkype for Businessは、機能が重複する2つの個別のソリューションとして並行して展開できます。 詳細については、「Microsoft TeamsとSkype for Businessの共存と相互運用性を理解する」を参照してください。

Citrix RealTime Optimization PackとMicrosoft Teamsマルチメディアエンジン用のHDX最適化は、環境で設定された構成を尊重します。例としては、アイランドモードや、Microsoft TeamsとのSkype for Businessコラボレーションなどがあります。また、Microsoft TeamsとのSkype for Businessコラボレーションと会議も含まれます。

周辺機器へのアクセスは、一度に1つのアプリケーションにのみ許可されます。たとえば、通話中にRealTime Media Engineによるウェブカメラアクセスは、通話中にイメージングデバイスをロックします。デバイスが解放されると、Microsoft Teamsで利用可能になります。



Citrix SD-WAN™: Microsoft Teams向けに最適化されたネットワーク接続

最適なオーディオおよびビデオ品質には、低遅延、低ジッター、低パケット損失のMicrosoft 365クラウドへのネットワーク接続が必要です。支店拠点のCitrix Workspaceアプリユーザーからの Microsoft Teamsオーディオビデオ RTPトラフィックを、インターネットに接続する前にデータセンターにバックホールすると、過剰な遅延が発生する可能性があります。また、WANリンクで輻輳を引き起こす可能性もあります。Citrix SD-WANは、Microsoft 365のネットワーク接続原則に従ってMicrosoft Teamsの接続を最適化します。Citrix SD-WANは、Microsoft RESTベースの Microsoft 365 IPアドレスとWebサービス、および近接DNSを使用して、Microsoft Teamsトラフィックを識別、分類、および誘導します。

多くの地域で、ビジネスブロードバンドインターネット接続は、断続的なパケット損失、過剰なジッター期間、および停止に悩まされています。

Citrix SD-WANは、ネットワークの状態が不安定または劣化している場合に、Microsoft Teamsのオーディオ/ビデオ品質を維持するための2つのソリューションを提供します。

- Microsoft Azureを使用している場合、Azure VNETに展開されたCitrix SD-WAN仮想アプライアンス（VPX）は、高度な接続最適化を提供します。これらの最適化には、シームレスなリンクフェイルオーバーとオーディオパケットレーシングが含まれます。
- Citrix SD-WANのお客様は、Citrix Cloud™ Directサービスを通じてMicrosoft 365に接続できます。このサービスは、すべてのインターネット向けトラフィックに対して信頼性の高い安全な配信を提供します。

支社のインターネット接続の品質が問題にならない場合、遅延を最小限に抑えるだけで十分な場合があります。遅延を最小限に抑えるには、Microsoft TeamsのトラフィックをCitrix SD-WANブランチアプライアンスから最寄りのMicrosoft 365フロントドアに直接誘導します。詳細については、「Citrix SD-WAN Office 365 optimization」を参照してください。

シトリックス SD-WAN](/en-us/citrix-virtual-apps-desktops/2511/media/sd-wan.png)

マルチウィンドウ会議とチャット

Windows版Microsoft Teamsでは、複数の会議またはチャットウィンドウを使用できます。ポップアウト機能の詳細については、Microsoft 365サイトの「Microsoft Teams Pop-Out Windows for Chats and Meetings」を参照してください。

> **注:**
>
> この機能は、Citrix Workspaceアプリ for Windows 2112.1、Mac 2203、Linux 2203、ChromeOS 2303でサポートされています。VDA 2112以降が必要で、1912 CU6+ LTSRにバックポートされました。

背景のぼかしと背景効果

Citrix Workspaceアプリ for Windows、Mac、Linux、ChromeOS/HTML5は、HDXによるMicrosoft Teamsの最適化において、背景のぼかしと背景効果をサポートしています。

背景をぼかすか、デフォルトの画像に置き換えることで、会話をシルエット（体と顔）に集中させ、予期せぬ邪魔を避けることができます。この機能は、P2Pまたは電話会議で使用できます。

> **注:**

> この機能はMicrosoft TeamsのUI/ボタンと統合されています。マルチウィンドウサポートは、VDAを2112以降にアップデートする必要がある前提条件です。詳細については、「Multi-window meetings and chat」を参照してください。

> 背景のぼかしと効果に関するMicrosoft TeamsのUIコントロールには、以下の最小バージョンが必要です。

- Citrix Workspaceアプリ Windows用 2207
- Citrix Workspaceアプリ Mac用 2301
- Citrix Workspaceアプリ Linux用 2307
- Citrix Workspaceアプリ ChromeOS 用 2303

制限事項:

- Microsoft Teamsのデフォルト画像で背景画像を置き換える間、クライアントはインターネットに接続されている必要があります。
- 管理者およびユーザー定義の背景画像の置き換えは、Microsoft Teams UIではサポートされていません。カスタム背景画像は、画像がクライアントにも保存されている場合、クライアントの構成設定を使用して構成できます。

カスタム背景画像の設定

以下のレジストリキーは、Microsoft Teams UIを使用してこの機能を制御する予定がない場合、または管理者がデフォルトの動作を上書きしたい場合にのみ必要です。たとえば、エンドポイントの性能が十分でないため、背景のぼかしを無効にする場合などです。

Windowsの場合

カスタム背景画像を設定するには、管理者またはエンドユーザーがクライアントまたはエンドポイントで以下のレジストリキーを構成する必要があります。

場所: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- 名前: VideoBackgroundEffect
- 種類: DWORD
- 値: 0 (無効), 1 (有効), 2 (背景画像の置き換え)

値を1に設定すると、背景がぼかされます。この値は、エンドユーザーまたは管理者が設定できます。

値を2に設定した場合、**VideoBackgroundImage**キーも存在する必要があります。この値は管理者のみが設定できます。以下のキーは、背景画像を置き換えたい場合のみ必要であり、ぼかしには必要ありません。

- 名前: VideoBackgroundImage
- 種類: REG_SZ
- 値: my_image_name.jpeg

ビデオの背景画像は、`C:\Program Files (x86)\Citrix\ICA Client`ディレクトリに存在する必要があります。

このレジストリ設定は、Microsoft Teams UIセレクターなしでCitrix Workspaceアプリ2206の背景のぼかしや画像の置き換えを有効にするためにも使用できます。言い換えれば、環境またはVDAがマルチウィンドウをサポートしていない場合でも、Citrix Workspaceアプリ2206以降でHKCUレジストリの回避策を適用して同様の結果を達成できますが、ユーザーはHDXセッションまたはMicrosoft Teams通話中に機能を制御することはできません。

レジストリキーの変更は、HDXセッションが接続したときにのみ有効になります。

Macの場合

ユーザーがダウンロードした画像の場所: */Users/username/Downloads/any_image.png*

次のコマンドを実行して、カスタム画像をデフォルト画像として設定します。

`defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2`

`defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "/Users/username/Downloads/any_image.png"`

Linuxの場合

ユーザーがダウンロードした画像の場所: */home/username/Downloads/any_image.jpg*

ファイル */var/.config/citrix/hdx_rtc_engine/config.json* を作成し、次の構成キーをJSON形式で追加します。例:

```
{



"VideoBackgroundEffect":2,
```

```
"VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"



}
```

HTML5の場合

1. **HTML5Client**フォルダー内の**configuration.js**ファイルに移動します。
2. 「**backgroundEffects**」属性を追加し、属性を「**true**」に設定します。例：

```
'features' : {

    'msTeamsOptimization' :

    {

        'backgroundEffects' : true

    }

}
```

3. 変更を保存します。

クライアントCPU消費に関する考慮事項

ぼかし機能はCPUへの負荷が少ないですが、消費量の増加が予想されます。たとえば、4コア、1.5 GHz Intel® Pentium® Silverチップ（TurboBoostで最大2.8 GHz）を搭載したシンクライアントでは、背景のぼかしによりCPU使用率が約2%増加します。平均CPU使用率は20%未満です。

Microsoft Teamsのギャラリービューとアクティブスピーカー

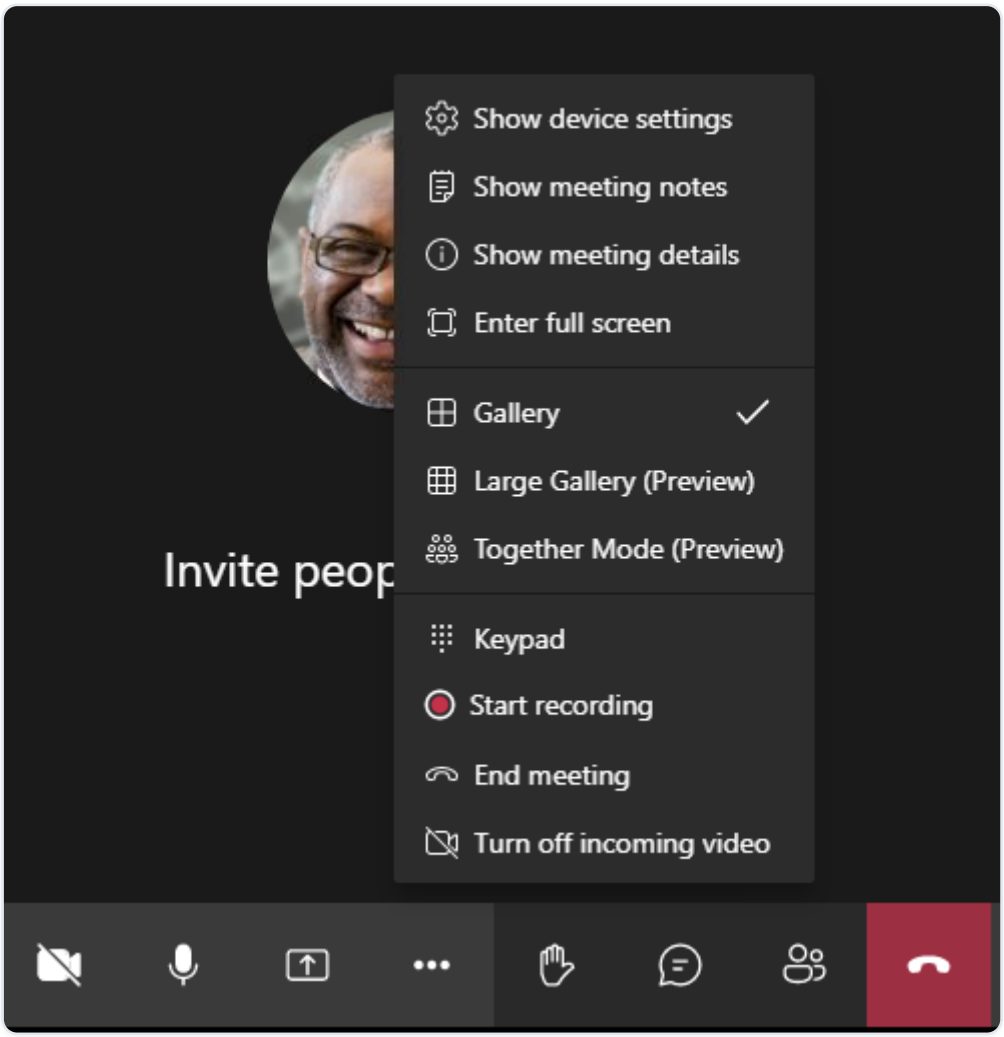
Microsoft Teamsは、**ギャラリー**、**大規模ギャラリー**、および**Together**モードのレイアウトをサポートしています。

Microsoft Teamsは、4人の参加者のビデオストリームを2x2のグリッドで表示します（**ギャラリー**として知られています）。この場合、Microsoft Teamsはデコードのために4つのビデオストリームをクライアントデバイスに送信します。4人を超える参加者がビデオを共有している場合、画面には最後に発言した4人のアクティブスピーカーのみが表示されます。

Microsoft Teamsは、最大7x7のグリッドを持つ大規模ギャラリービューも提供します。その結果、Microsoft Teams会議サーバーは単一のビデオフィードを合成し、デコードのためにクライアントデバイスに送信するため、CPU消費量が削減されます。この単一のマトリックス形式のフィードには、ユーザーのセルフプレビュービデオも含まれる場合があります。

最後に、Microsoft Teamsは新しい会議エクスペリエンスの一部である**Togetherモード**をサポートしています。AIセグメンテーション技術を使用して参加者を共有背景にデジタル配置することで、Microsoft Teamsはすべての参加者を同じ講堂に配置します。

ユーザーは、会議中に省略記号メニューで**ギャラリー**、**大規模ギャラリー**、または**Togetherモード**のレイアウトを選択することで、これらのモードを制御できます。



ビデオのアスペクト比の制約のサポート（Citrix Workspaceアプリ for Windows 2102、Citrix Workspaceアプリ for Linux 2106、Citrix Workspaceアプリ for MAC 2106以降）：

- **フレームに合わせる**オプションは、ギャラリー/大規模ギャラリービューで利用できます。このオプションは、サブウィンドウに収まるようにビデオサイズをトリミングします。一方、**フレームにフィット**は、ビデオの側面に黒いバー（レターボックス）を表示するため、トリミングは行われません。

次の表は、ギャラリーレイアウトと大規模ギャラリーレイアウトの比較を示しています。

	ギャラリービュー 2X2 (デフォルト)	大規模ギャラリービュー
レイアウト / グリッド	4人の参加者のビデオストリームを含む2x2グリッドを表示します。画面には直近で最もアクティブな4人の発言者のみが表示され、他の参加者はグリッドに表示されません。	49人の参加者のビデオストリームを含む7x7グリッドを表示します。
ミキシング技術	メディアルーターは、各参加者からの個別のストリームをすべてのユーザーに転送します。	中央の会議サーバーがすべてのオーディオまたはビデオをミキシングおよびトランスコードし、各参加者向けにカスタマイズされた複合レイアウトを作成します。この処理により、追加の遅延が発生する場合があります。
アクティブスピーカー	新しいアクティブスピーカーは、グリッド内で最もアクティブでないスピーカーと置き換わります。	アクティブか非アクティブかに関わらず、すべての参加者を表示します。
エンドポイントでのエンコード	Simulcastが有効になっている場合、1つ以上のビデオストリームがエンドポイントでエンコードされることがあります。Simulcastのサポートに関する詳細については、Simulcastを参照してください。	Simulcastが有効になっている場合、1つ以上のビデオストリームがエンドポイントでエンコードされることがあります。Simulcastのサポートに関する詳細については、Simulcastを参照してください。
エンドポイントでのデコード	各参加者は最大4つの個別のメディアストリームを受信します。これにより、HdxRtcEngine.exeによるエンドポイントでのCPU消費量が増加します（デコード/レンダリングのため）。	各参加者は、オーディオとビデオの単一ストリームのみを受け取ります。この設定により、エンドポイントでのCPU消費が削減されます。

	ギャラリービュー 2X2 (デフォルト)	大規模ギャラリービュー
最大解像度	720p。4人の参加者がビデオを共有している場合、ビデオフィードあたりの最大解像度は360pです。4人未満の参加者がビデオを共有している場合、ビデオフィードあたりの解像度は高くなる可能性があります。	複合レイアウトまたはミキシングの場合は720p。複合レイアウトでは、参加者ごとに高品質のビデオストリームは必要ありません。この条件により、各送信者は解像度またはアップロードビットレートを削減します。
「低速ユーザー」の問題	送信者は、各モダリティ（オーディオ/ビデオ/画面共有）の品質を、参加者間の最低共通ネットワーク品質に調整します。このマルチメディアストリームは、その後、他のすべての参加者に転送されます。結果として、ネットワーク状態の悪い参加者は、通話中の他の全員の品質に影響を与えます。	最低共通ネットワーク品質のシナリオの影響を受けにくい。会議サーバーは、個々の参加者のネットワーク状態に基づいて異なる品質を提供します。
セルフプレビュー	リアルタイムで自分を小さなサムネイルで表示します。	自分をサムネイルで表示し、残りのビデオフィードと混合します。結果として、メインのビデオレイアウトに自分が含まれているのが、多少の遅延を伴って表示されることがあります。

Microsoft Teamsでの画面共有

Microsoft Teamsは、ビデオベースの画面共有（VBSS）に依存しており、共有されているデスクトップをH264などのビデオコーデックで効率的にエンコードし、高精細ストリームを作成します。HDX最適化を使用すると、受信する画面共有はビデオストリームとして扱われます。

Windows、Linux、Mac向けのCitrix Workspaceアプリ2109以降、およびChromeOS向けのCitrix Workspaceアプリ2303以降では、ユーザーは画面とビデオカメラを同時に共有できます。

以前のバージョンでは、ビデオ通話中に相手がデスクトップの共有を開始すると、元のカメラビデオフィードは一時停止されます。代わりに、画面共有ビデオフィードが表示されます。その後、相手は手動でカメラ共有を再開する必要があります。

PowerPoint Liveに関する注意

PowerPoint Liveからコンテンツを共有している場合、この制限はありません。その場合、他のピアは引き続きあなたのウェブカメラとコンテンツを見ることができ、他のスライドを確認するために前後に移動できます。このシナリオでは、スライドはVDAでレンダリングされます。PowerPoint Liveのスライドデッキにアクセスするには、「Share tray」ボタンをクリックして提案されたPowerPointスライドのいずれかを選択するか、「Browse」をクリックしてコンピューターまたはOneDrive上のPowerPointファイルを見つけます。

送信画面共有も最適化され、Citrix Workspaceアプリにオフロードされます。この場合、メディアエンジンはCitrix Desktop Viewer (CDViewer.exe) ウィンドウのみをキャプチャして送信し、その周囲には赤い枠線が描画されます。Desktop Viewerと重なっているローカルアプリケーションはキャプチャされません。

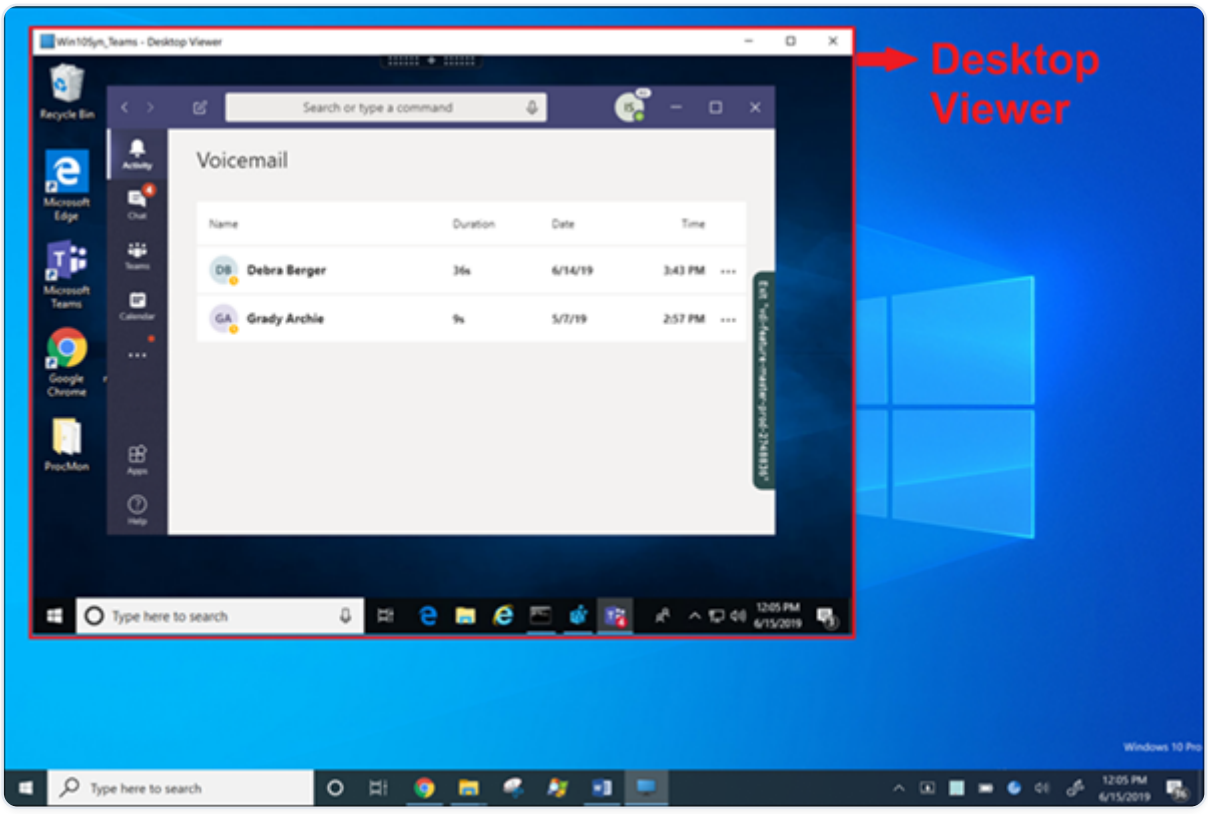
注

画面共有を有効にするには、Mac版Citrix Workspaceアプリで特定の権限を設定します。詳細については、システム要件を参照してください。

既知の制限:

- Desktop Viewerが無効になっている場合、またはDesktop Lockが使用されている場合、Microsoft Teamsの画面ピッカーでマルチモニター選択は利用できません。Desktop Viewerは、`.ICA`ファイルテンプレートを編集するか、`StoreFront web.config`によって無効にされることがあります。SHIFT+F2ホットキーはマルチモニター画面共有と互換性がありません。
- Workspaceアプリのバージョン2106より古い場合、プライマリモニターのみが共有されます。通話中の他のピアに見せるには、仮想デスクトップ内のアプリケーションをプライマリモニターにドラッグしてください。

- Citrix Workspaceアプリを仮想モニターレイアウト機能（単一の物理モニターの論理パーティション）で構成している場合、マルチモニター画面共有が機能しないことがあります。この場合、すべての仮想モニターは複合画像として共有されます。
- Windows版Citrix Workspaceアプリの古いバージョン（1907から2008まで）では、クライアントマシンで実行されているローカルアプリケーションも共有されます。この共有は、ローカルアプリがDesktop Viewerの上に重ねて表示されている場合にのみ可能です。この動作は、2009.6以降および1912 CU5以降で削除されました。
- 画面共有中に、ウィンドウモードから全画面表示に切り替えると、画面共有が停止します。画面共有を機能させるには、一度停止してから再度共有する必要があります。
- Optimized Microsoft Teamsでは、共有コントロールを特定の場所にピン留めすることはできません。
- 最小化されたアプリを共有すると、そのアプリのタイトルバーも共有される場合があります。



シームレスアプリケーションからの画面共有:

Microsoft Teamsをスタンドアロンのシームレスアプリケーションとして公開している場合、画面共有は物理エンドポイントのローカルデスクトップをキャプチャします。Citrix Workspaceアプリの最小バージョン1909が必要です。

アプリ共有

Citrix Workspaceアプリ for Windows 2112.1およびVDA 2112以降、Microsoft Teamsはアプリ共有をサポートしています。

Citrix Workspaceアプリ for Windows 2109、Mac 2203、Linux 2209、およびVDA 2109以降、Microsoft Teamsは仮想セッションで実行されている特定のアプリの画面共有をサポートしています。最適化されたMicrosoft Teamsを使用して、Javaなどのカスタム社内アプリケーションを共有することもできます。特定のアプリを共有するには：

1. リモートセッション内でMicrosoft Teamsアプリに移動します。
2. Microsoft Teams UIで**コンテンツを共有**をクリックします。
3. 会議で共有するアプリを選択します。選択したアプリの周囲に赤い枠が表示され、通話中のピアは共有されたアプリを見ることができます。

別のアプリを共有するには、もう一度**コンテンツを共有**をクリックして、新しいアプリを選択します。

アプリ共有を無効にするには、VDAの`HKLM\SOFTWARE\Citrix\Graphics`に次のレジストリキーを作成します。 名前: `UseWsProvider` 種類: `DWORD` 値: 0

> **注:**
>
> - アプリを最小化すると、Microsoft Teamsは共有アプリの最後の画像を表示します。画面共有を再開するには、ウィンドウを最大化できます。
> - 画面共有は、VDA側でのウィンドウのキャプチャに依存します。コンテンツは最大レートでCitrix Workspaceアプリに中継されます。最大レートは1秒あたり30フレームです。Citrix Workspaceアプリは、コンテンツをピアまたは会議サーバーに転送します。

> Microsoft Teamsのアプリ共有](/en-us/citrix-virtual-apps-desktops/2511/media/ms-teams-app-sharing.png)

特定のアプリの画面共有に関する既知の制限事項：

- アプリを画面共有しているとき、マウスカーソルは表示されません。
- アプリを共有中に最小化すると、スクリーンピッカーにはアプリのアイコンのみが表示されます。アプリのサムネイルはスクリーンピッカーでプレビューされません。アプリを最大化するまで、コンテンツを共有できず、赤い枠も表示されません。
- LAAアプリは、VDAの最適化されたMicrosoft Teamsでデスクトップアプリと共有できるアプリのリストを表示します。ただし、リストからアプリを選択しても、期待どおりの結果にならない場合があります。

アプリ保護との互換性 特定のアプリの画面共有は、HDX最適化されたMicrosoft Teamsのアプリ保護機能と互換性があります。アプリ保護が有効になっているデリバリーグループからアプリまたはデスクトップを起動した場合、特定のアプリを画面共有できます。

Microsoft Teams UIで**コンテンツを共有**をクリックすると、スクリーンピッカーから**デスクトップ**オプションが削除されます。開いているアプリを共有するには、**ウィンドウ**オプションのみを選択できます。

> **注:**
>
> アプリ保護が有効になっているデリバリーグループからアプリまたはデスクトップを起動した場合、Citrix Workspaceアプリ for Windows 2202以前を使用していると、受信ビデオまたは画面共有を表示できません。

Microsoft Teamsで制御を付与および要求する

この機能は、Citrix Workspaceアプリの以下のバージョンでサポートされています（VDAバージョンやオペレーティングシステム、シングルセッションまたはマルチセッションには依存しません）。

- Citrix Workspaceアプリ for Windows バージョン2112.1以降
- Citrix Workspaceアプリ for Mac バージョン2203.1以降
- Citrix Workspaceアプリ for Linux バージョン2203以降
- ChromeOS 版 Citrix Workspace アプリ バージョン 2303 以降

Microsoft Teams通話中に参加者が画面を共有している場合、制御を要求できます。制御を取得すると、共有画面に対して選択、編集、その他のキーボードおよびマウス操作を行うことができます。

画面が共有されているときに制御を取得するには、Microsoft Teams UIの**制御を要求**ボタンをクリックします。画面を共有している会議参加者は、要求を許可または拒否できます。

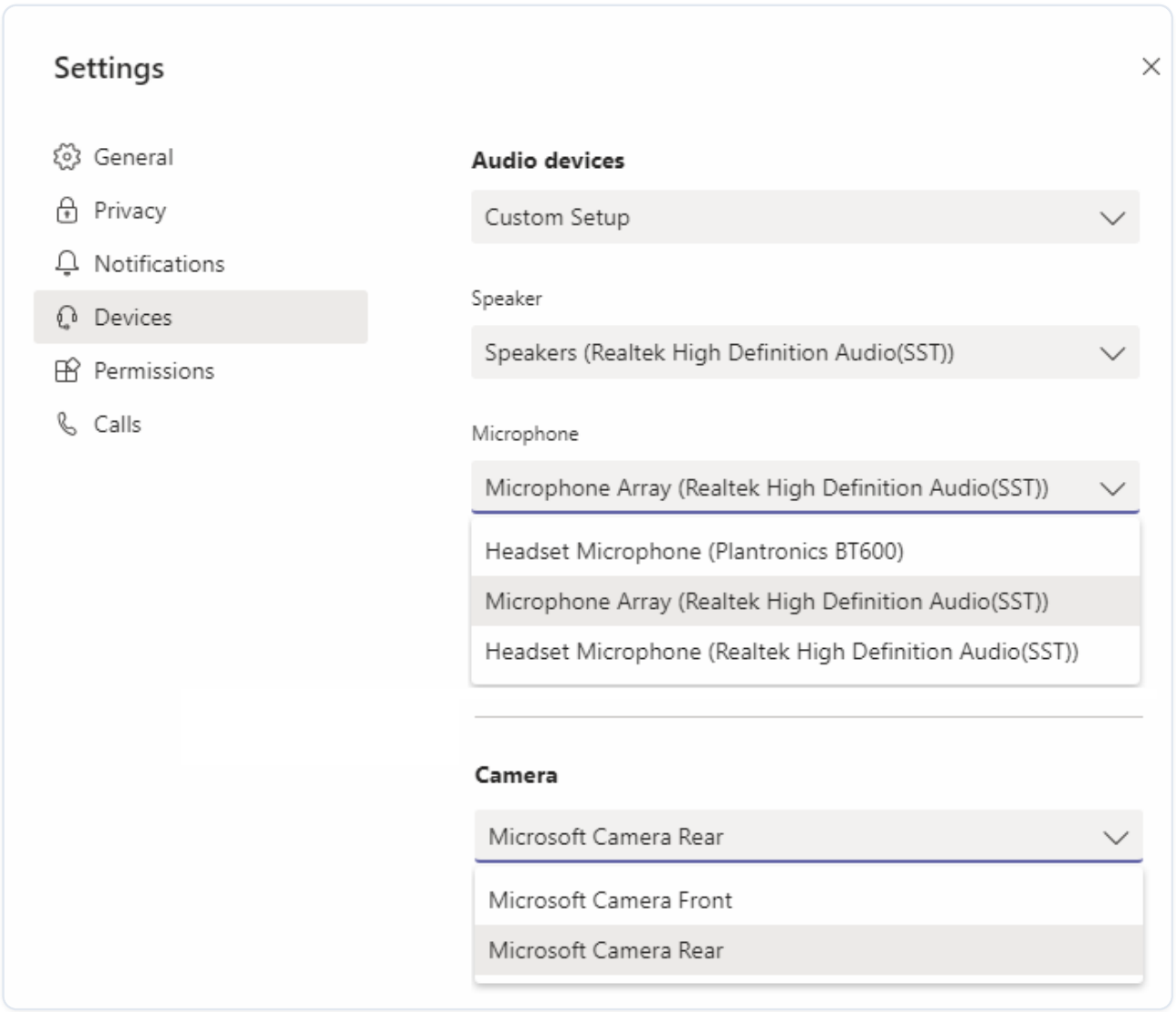
制御中は、共有画面の選択、編集、その他の変更を行うことができます。これらの操作には、キーボードとマウスの両方を使用できます。完了したら、 をクリックします。

> **制限事項:**

- ユーザーが単一のアプリを共有している場合 (アプリ共有とも呼ばれます)、制御の付与と要求は利用できません。デスクトップ全体またはモニターを共有する必要があります。
- コントロールバーを特定の場所に固定する機能は利用できません。

Microsoft Teamsでの周辺機器

Microsoft Teams の最適化が有効な場合、Citrix Workspace アプリは周辺機器（ヘッドセット、マイク、カメラ、スピーカーなど）にアクセスします。その後、周辺機器は Microsoft Teams UI（**設定 > デバイス**）に適切に表示されます。



Microsoft Teamsはデバイスに直接アクセスしません。代わりに、メディアの取得、キャプチャ、処理のためにWorkspaceアプリのWebRTCメディアエンジンに依存します。Microsoft Teamsは、ユーザーが選択できるようにデバイスを一覧表示します。

Microsoft Teams のアクティブ中に挿入された周辺機器は、デフォルトでは選択されません。Microsoft Teams UI の > 画面から周辺機器を手動で選択する必要があります。周辺機器が選択されると、Microsoft Teams は周辺機器の情報をキャッシュします。その結果、同じエンドポイントからセッションに再接続すると、周辺機器が自動的に選択されます。

推奨事項:

- エコーキャンセレーション内蔵の Microsoft Teams 認定ヘッドセット。マイクとスピーカーが別々のデバイスにある追加の周辺機器を使用するセットアップでは、エコーが発生する可能性があります。例としては、マイク内蔵のウェブカメラとスピーカー付きモニターがあります。外部スピーカーを使用する場合は、マイクからできるだけ離して配置してください。また、音がマイクに屈折する可能性のある表面からも離して配置してください。詳細については、`www.microsoft.com` にアクセスし、Microsoft Teams 認定ヘッドセットを検索してください。
- Microsoft Teams 認定カメラ。ただし、Skype for Business 認定周辺機器も Microsoft Teams と互換性があります。詳細については、<www.microsoft.com> にアクセスし、Microsoft Teams 認定カメラと Skype for Business 認定周辺機器を検索してください。
- Citrix Workspace アプリのメディアエンジンは、オンボード H.264 エンコーディング（UVC 1.1 および 1.5）を実行するウェブカメラでの CPU オフロードを利用できません。

注:

Windows用Workspaceアプリ2009.6は、24ビットまたは96 kHzを超える周波数のオーディオ形式に対応した周辺機器を取得できるようになりました。

HdxTeams.exe（Windows 用 Citrix Workspace アプリ 2009 以前の場合）は、以下の特定のオーディオデバイス形式（チャンネル、ビット深度、サンプルレート）のみをサポートします。

- 再生デバイス: 最大2チャンネル、16ビット、最大96,000 Hzの周波数
- 録音デバイス: 最大4チャンネル、16ビット、最大96,000 Hzの周波数

1つのスピーカーまたはマイクが予期される設定と一致しない場合でも、Microsoft Teamsでのデバイス列挙は失敗し、**設定 > デバイス**の下に**なし**と表示されます。

HdxTeams.exeの**Webrpc**ログには、この種類の情報が表示されます。

`Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing...`.

`Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't create audio module!` !

回避策として、特定のデバイスを無効にするか、次の手順を実行します。

1. **サウンドコントロールパネル** (mmsys.cpl) を開きます。
2. 再生デバイスまたは録音デバイスを選択します。
3. **プロパティ > 詳細設定**に移動し、設定をサポートされているモードに変更します。

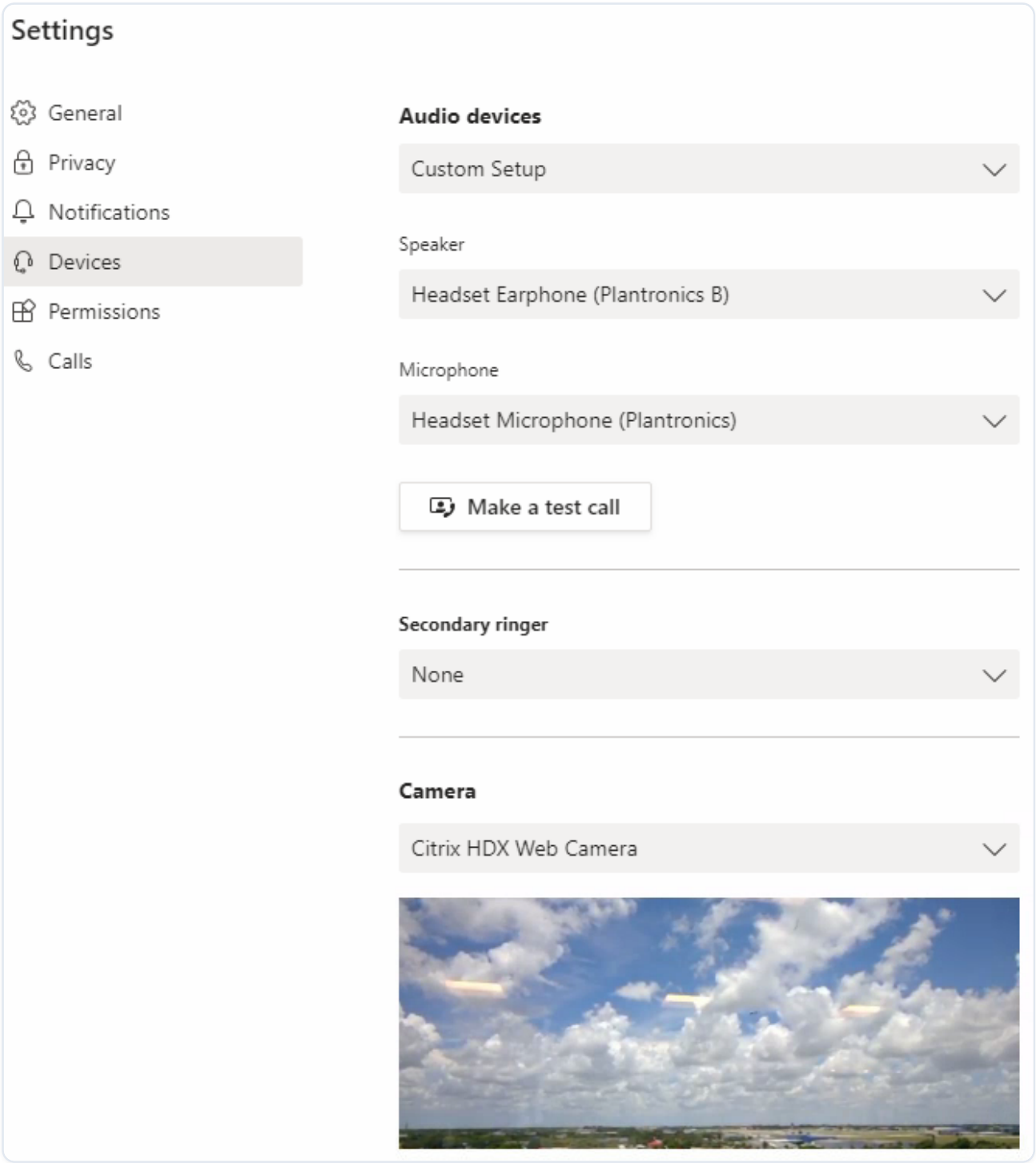
フォールバックモード

Microsoft Teamsが最適化されたVDIモード（Microsoft Teams/バージョン情報/バージョンで「Citrix HDX Not Connected」と表示される）でロードに失敗した場合、VDAはレガシーHDXテクノロジーにフォールバックします。レガシーHDXテクノロジーには、Webカメラリダイレクト、クライアントオーディオ、マイクリダイレクトなどがあります。Microsoft Teamsの最適化をサポートしないWorkspaceアプリのバージョン/プラットフォームOSを使用している場合、フォールバックレジストリキーは適用されません。 フォールバックモードでは、周辺機器はVDAにマッピングされます。周辺機器は、仮想デスクトップにローカルで接続されているかのようにMicrosoft Teamsアプリに表示されます。

VDAでレジストリキーを設定することにより、フォールバックメカニズムをきめ細かく制御できるようになりました。詳細については、レジストリで管理される機能のリストにあるMicrosoft Teamsフォールバックモードを参照してください。

この機能には、Microsoft Teamsバージョン1.3.0.13565以降が必要です。

Microsoft Teamsアプリの**設定 > デバイス**タブで、最適化モードか非最適化モードかを判断するには、カメラ名が主な違いとなります。Microsoft Teamsが非最適化モードでロードされた場合、レガシーHDXテクノロジーが起動します。Webカメラ名には、次の図に示すように**Citrix HDX**のサフィックスが付いています。スピーカーとマイクのデバイス名は、最適化モードと比較してわずかに異なる（または切り詰められている）場合があります。



レガシーHDXテクノロジーを使用する場合、Microsoft Teamsはオーディオ、ビデオ、画面共有の処理をエンドポイントのCitrix WorkspaceアプリWebRTCメディアエンジンにオフロードしません。代わりに、HDXテクノロジーはサーバーサイドレンダリングを使用します。ビデオをオンにすると、VDAで高いCPU消費が予想されます。リアルタイムオーディオのパフォーマンスは最適ではない可能性があります。

既知の制限事項

Citrixの制限事項

Citrix Workspaceアプリの制限事項：

- HIDボタン - 通話の応答と終了はサポートされていません。音量アップとダウンはサポートされています。
- Microsoft Teamsの管理センターにおけるQoS設定は、VDIユーザーには適用されません。
- ユーザーは、VDAでSnipping Toolを使用している間、Microsoft Teamsのコンテンツのスクリーンショットを撮ることはできません。ただし、クライアント側でSnipping Toolを使用した場合、コンテンツをキャプチャできます。

VDAの制限事項：

- **Citrix Workspace アプリの高 DPI** 設定を `Yes` に構成すると、リダイレクトされたビデオウィンドウがずれて表示されます。この制限は、モニターの DPI スケーリング係数が 100% を超える値に設定されている場合に発生します。

Citrix Workspace アプリと VDA の制限事項:

- 最適化された通話の音量は、クライアントマシンの音量バーを使用してのみ制御できます。VDA上では制御できません。

サイマルキャスト

WindowsおよびMac上の最適化されたMicrosoft Teamsビデオ会議通話でサイマルキャストがサポートされています。Linuxについては、シンクライアントベンダーにお問い合わせください。 サイマルキャストにより、すべての発信者にとって最適な通話エクスペリエンスとなるよう適切な解像度に調整することで、異なるエンドポイント間でのビデオ会議通話の品質とエクスペリエンスが向上します。

この改善されたエクスペリエンスにより、各ユーザーは、エンドポイントの機能、ネットワークの状態など、いくつかの要因に応じて、異なる解像度（たとえば、720p、360pなど）で複数のビデオストリームを配信する場合があります。受信側のエンドポイントは、処理できる最高の品質の解像度を要求し、それによってすべてのユーザーに最適なビデオエクスペリエンスを提供します。

> **注:**
>
> この機能は、Microsoft Teamsからのアップデートが展開された後にのみ利用可能です。ETAについては、`<https://www.microsoft.com/>` にアクセスし、Microsoft 365ロードマップ

を検索してください。Microsoftによってアップデートが展開されたら、ドキュメントの更新と発表についてはCTX253754 を確認してください。

Microsoftの制限事項

- 3x3ギャラリービューはサポートされていません。Microsoft Teamsの依存関係 – 3x3グリッドがいつ利用可能になるかについてはMicrosoftにお問い合わせください。
- Skype for Businessとの相互運用性は音声通話に限定されており、ビデオ機能はありません。
- 送受信ビデオストリームの最大解像度は720pです。
- PSTN通話の呼び出し音はサポートされていません。
- ダイレクトルーティングのメディアバイパスはサポートされていません。
- ブロードキャストおよびライブイベントのプロデューサーとプレゼンターの役割はサポートされていません。参加者ロールはサポートされていますが、最適化されていません（代わりにVDAでレンダリングされます）。
- Microsoft Teamsのズームインおよびズームアウト機能はサポートされていません。
- ロケーションベースルーティングとメディアバイパスはサポートされていません。
- 通話のマージはサポートされていません（ユーザーインターフェイスにオプションが表示されません）。

CitrixとMicrosoftの制限事項

- 画面共有を行う際、**システムオーディオを含める**オプションは利用できません。
- サイマルキャストはChromeOSではサポートされていません。

今後のMicrosoft Teamsシングルウィンドウ のEOL

January 31, 2024に、MicrosoftはVDI Microsoft Teams最適化を使用する際のシングルウィンドウUIに対するMicrosoft Teamsのサポートを終了し、マルチウィンドウエクスペリエンスのみをサポートします。Microsoftは9/8/2023にM365s管理センター（投稿ID: MC674419）でこの非推奨化について通知しました。 マルチウィンドウ機能に関する公開されている詳細は、Tech Communityの記事「New Meeting and Calling Experience in Microsoft Teams」で確認できます。

注記:

Citrixは、ビデオおよび画面共有のために最適化モードでMicrosoft Teamsを引き続き使用するには、VDAとCitrix Workspaceアプリをサポートされているバージョンにアップグレード

することを推奨します。インフラストラクチャとエンドポイントをマルチウィンドウをサポートするようにアップグレードしない場合、通話、ビデオ通話、および画面共有は最適化されなくなります。これにより、通話品質の問題、遅延の増加、およびサーバーへの負荷の増加が発生する可能性があります。

次の表は、Citrix VDIでMicrosoft Teamsの最適化された通話を継続して使用するために必要なVDAおよびCitrix Workspaceアプリの最小バージョン、LTSRバージョン、推奨バージョンを示しています。

コンポーネント	最小バージョン (1)	LTSRサポートバージョン (2)	推奨バージョン (3)
マイクロソフトTeams	1.5.00.11865	該当なし	最新
VDA	1912 CU6 LTSR, 2109 CR, 2203 LTSR	1912 CU8+, 2203 LTSR CU2+ (4)	2308 CR+
Windows向けCitrix Workspaceアプリ	2112.1 CR	2203 CU2+ (4)	2309 CR+
Mac向けCitrix Workspaceアプリ	2203 CR	該当なし	2308 CR+
Linux向けCitrix Workspaceアプリ	2202 CR	該当なし	2308 CR+
ChromeOSまたはHTML5向けCitrix Workspaceアプリ	2303 CR	該当なし	2309 CR+

注：

1. 最小バージョン：これは、マルチウィンドウが初めて導入されたバージョンです。ここに記載されている最小バージョンの一部は、サポート終了となっている場合があります。

2. LTSRサポート対象バージョン：これは、Citrixがマルチウィンドウ向けにサポートしているLTSRバージョンです。これらのLTSRリリースの古いバージョンは動作する可能性がありますが、新しいLTSR CUバージョンがリリースされると、それらのバージョンに対するサポートは利用できなくなります。LTSRサポートポリシーの詳細については、`<https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX205549/faq-citrix-virtual-apps-and-desktops-and-citrix-hypervisor-long-term-service-release-ltsr>`を参照してください。
3. 推奨バージョン：これは、ユーザー/顧客がソフトウェアのアップグレードを選択した場合にCitrixが推奨するソフトウェアのバージョンです。これらはすべてCRバージョンです。
4. VDAおよびCWAのベースバージョンであるバージョン2203 LTSRには、マルチウィンドウ機能が含まれています。これらのバージョンは、正式にサポートされている最新のCUに置き換えられています。お客様は、これらのサポートされていないバージョンを自己責任で引き続き使用できます。Citrixは、LTSRリリースをご利用のお客様に最新のCUへのアップグレードを推奨します。

WebRTCからのSDP形式（Plan B）の非推奨のお知らせ

Citrixは、今後のリリースでWebRTCからの現在のSDP形式（Plan B）のサポートを非推奨にする予定です。最適化されたMicrosoft Teamsの機能に対応するには、WebRTCでUnified Planを使用する必要があります。

影響を受ける製品

Citrix Workspaceアプリの今後のリリースでは、Citrix Workspaceアプリの次期リリースを搭載したエンドポイントと、Citrix Workspaceアプリ2108以前のバージョンを搭載したエンドポイント間の通話はサポートされません。この通話の非互換性には、1912 LTSR Citrix Workspaceアプリクライアント（CWA）が含まれます。影響を受けるCWAクライアントは次のとおりです。

- Windows向けCitrix Workspaceアプリ
- Linux向け Citrix Workspace アプリ
- Mac向けCitrix Workspaceアプリ
- Chrome向けCitrix Workspaceアプリ

Plan B の代替

Citrix Workspaceアプリのバージョン2109より古いものを使用している場合、サポートされているバージョン（できれば最新のCRリリース）にアップグレードする必要があります。そうしないと、将来のリリースまたは新しいエンドポイントとの通話は接続に失敗します。将来のリリースとフェデレーション通信パートナー間の通話も、フェデレーションパートナーがCitrix Workspaceをアップグレードしていない場合、完了に失敗する可能性があります。

Citrix Workspaceアプリバージョン2108は、2023年3月にサポート期限を終了しました。より新しいバージョンにアップグレードする必要があります。詳細については、Citrix Workspaceアプリのバージョンサポートに関するWorkspace Appを参照してください。

Plan Bの非推奨化に関する詳細については、WebRTCドキュメントを参照してください。

追加情報

- Microsoft Teamsの監視、トラブルシューティング、サポート
- Microsoft TeamsデスクトップアプリをVMに展開する
- MSIを使用してMicrosoft Teamsをインストールする (VDIインストールセクション)
- シンクライアント
- Skype for Business ネットワーク評価ツール
- Microsoft Teams と Skype for Business の共存と相互運用性を理解する

Microsoft Teamsの監視、トラブルシューティング、サポート

Teamsの監視

このセクションでは、HDX を使用した Microsoft Teams の最適化を監視するためのガイドラインを提供します。 最適化モードで実行しており、`HdxRtcEngine.exe` がクライアントマシンで実行されている場合、VDA 上の `WebSocketAgent.exe` というプロセスがセッションで実行されています。アプリケーションを表示するには、Director の **Activity Manager** を使用します。

](/en-us/citrix-virtual-apps-desktops/2511/media/teams-activity-manager.png)

Microsoft Teams の最適化ステータスは、Director > **ユーザー詳細**ページ > **セッション詳細**パネル > **MS Teams 最適化**フィールドで確認できます。Microsoft Teams が最適化されていることは、クリアなオーディオとビデオなど、より良いユーザーエクスペリエンスのために不可欠です。この機能は、VDA バージョン 2311 以降で利用可能です。サポートされている Citrix Workspace™ アプリのバージョンは、「Microsoft Teams の最適化」に記載されています。Director は、Microsoft Teams が公開アプリケーションとして、または公開デスクトップ内で実行されている場合にの

み、Microsoft Teams の最適化ステータスを表示します。 詳細については、「Microsoft Teams の最適化ステータス」を参照してください。

VDA の最小バージョン 1912 以降では、Citrix HDX Monitor (最小バージョン 3.11) を使用してアクティブな Teams 通話を監視できます。Citrix Virtual Apps and Desktops 製品 ISO には、フォルダー `layout\image-full\Support\HDX Monitor` に最新の `hdxmonitor.msi` が含まれています。 VDA の最小バージョン 1912 以降では、Citrix HDX Monitor (最小バージョン 3.11) を使用してアクティブな Microsoft Teams 通話を監視できます。Citrix Virtual Apps and Desktops 製品 ISO には、フォルダー `layout\image-full\Support\HDX Monitor` に最新の `hdxmonitor.msi` が含まれています。

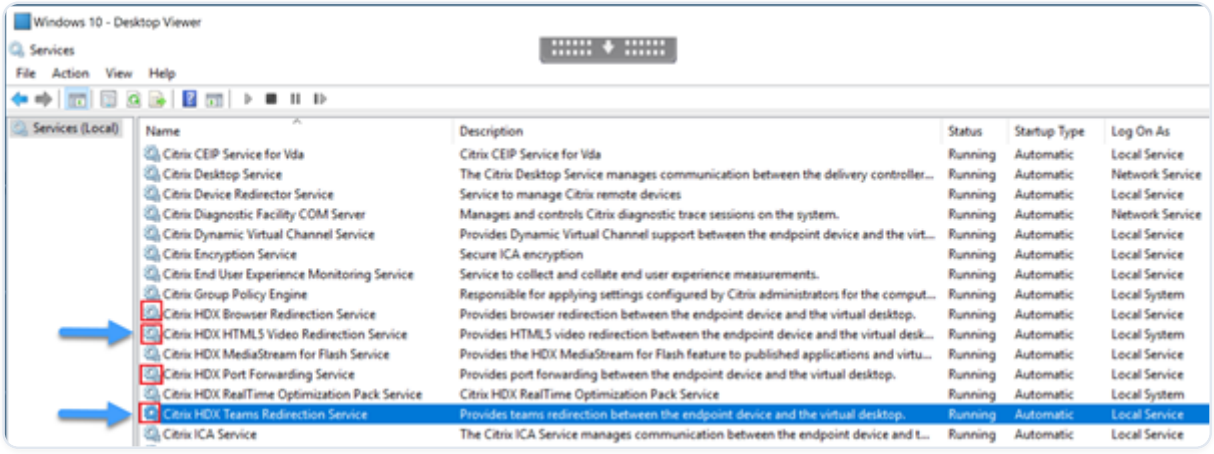
詳しくは、Knowledge Centerの記事「CTX253754」の「*監視*」を参照してください。

トラブルシューティング

このセクションでは、Microsoft Teams の最適化を使用する際に発生する可能性のある問題に対するトラブルシューティングのヒントを提供します。詳細については、「CTX253754」を参照してください。

バーチャル デリバリー エージェント上で

BCR_x64.msi によって4つのサービスがインストールされます。そのうち2つのみがVDAでのMicrosoft Teamsリダイレクトを担当します。



- **Citrix HDX Teams Redirection Service** は、Microsoft Teams で使用される仮想チャネルを確立します。このサービスは CtxSvcHost.exe に依存しています。
- **Citrix HDX HTML5 Video Redirection Service** は、127.0.0.1:9002 TCP でリッスンする WebSocketService.exe として実行されます。WebSocketService.exe は、主に2つの機能を実行します。

i. **セキュアな WebSocket のための TLS 終端** は、Microsoft Teams アプリ内のコンポーネントである vdiCitrixPeerConnection.js からセキュアな WebSocket 接続を受信します。Process Monitor で追跡できます。証明書の詳細については、セクション (TLS と HTML5 ビデオのリダイレクト、およびブラウザコンテンツのリダイレクト) を参照してください。

一部のアンチウイルスおよびデスクトップセキュリティソフトウェアは、`WebSocketService.exe`とその証明書の適切な機能に干渉します。Citrix HDX HTML5ビデオリダイレクトサービスが`services.msc`コンソールで実行されている場合でも、netstatで確認すると、localhost `127.0.0.1:9002` TCPソケットがリスニングモードになっていません。サービスを再起動しようとすると、ハングアップします（「停止中…」）。`WebSocketService.exe`プロセスに適切な除外を適用してください。

「プロセスモニター」(/en-us/citrix-virtual-apps-desktops/2511/media/team-process-monitor.png)

ii. **ユーザーセッションマッピング。**Microsoft Teamsアプリケーションが起動すると、WebSocketService.exeはVDAのユーザーセッションでWebSocketAgent.exeプロセスを開始します。WebSocketService.exeはLocalSystemアカウントとしてセッション0で実行されます。

「WebSocketAgent.exeサービス」(/en-us/citrix-virtual-apps-desktops/2511/media/websocketservice-websocketagent.png)

VDAでWebSocketService.exeサービスがアクティブなリッスン状態にあるかどうかを確認するには、`netstat`を使用できます。

管理者として実行しているコマンドプロンプトウィンドウから`netstat -anob -p tcp`を実行します。

「netstatの例を実行」(/en-us/citrix-virtual-apps-desktops/2511/media/teams-netstat.png)

接続が成功すると、状態はESTABLISHEDに変わります。

「netstatの成功例」(/en-us/citrix-virtual-apps-desktops/2511/media/teams-netstat-success.png)

> **重要:**
>
> WebSocketService.exeは、127.0.0.1:9001と127.0.0.1:9002の2つのTCPソケットでリッスンします。ポート9001は、ブラウザコンテンツリダイレクトとHTML5ビデオリダイレクトに使用されます。ポート9002は、Microsoft Teamsリダイレクトに使用されます。Teams.exeとWebSocketService.exe間の直接通信を妨げる可能性のあるプロキシ構成がVDAのWindows

OSにないことを確認してください。Internet Explorer 11で明示的なプロキシを構成すると（**インターネットオプション > 接続 > LANの設定 > プロキシサーバー**）、接続が割り当てられたプロキシサーバーを経由する場合があります。手動および明示的なプロキシ設定を使用する場合は、**ローカルアドレスにはプロキシサーバーを使用しない**がチェックされていることを確認してください。

サービスの位置と説明

サービス	WINDOWS SERVER OSの実行可能ファイルへのパス	ログオンアカウント	説明
Citrix HTML5 ビデオリダイレクトサービス	"C:\Program Files (x86)\Citrix\System32\WebSocketService.exe" /service	ローカルシステムアカウント	仮想デスクトップとエンドポイントデバイス間でメディアリダイレクトを実行するために必要な初期フレームワークを、複数のHDXマルチメディアサービスに提供します。
Citrix HDX ブラウザコンテンツリダイレクトサービス	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g BrowserRedirSvcs	このアカウント (ローカルサービス)	エンドポイントデバイスと仮想デスクトップ間でブラウザコンテンツリダイレクトを提供します。
Citrix ポートフォワーディングサービス	"C:\プログラムファイル (x86)\Citrix\システム32\CtxSvcHost.exe" -g PortFwdSvcs	このアカウント (ローカルサービス)	ブラウザコンテンツリダイレクトのために、エンドポイントデバイスと仮想デスクトップ間でポートフォワーディングを提供します。
Citrix HDX Teams リダイレクトサービス	"C:\プログラムファイル (x86)\Citrix\システム32\CtxSvcHost.exe" -g TeamsSvcs	ローカルシステムアカウント	エンドポイントデバイスと仮想デスクトップ間でMicrosoft Teamsのリダイレクトを提供します。

シトリックス ワークスペース アプリ

ユーザーのエンドポイントでは、Windows版Citrix WorkspaceアプリがHdxTeams.exeまたはHdxRtcEngine.exeという新しいサービスをインスタンス化します。これは、Microsoft TeamsがVDAで起動され、ユーザーがセルフプレビューで通話しようとしたり、周辺機器にアクセスしようとしたりするときに行われます。このサービスが表示されない場合は、以下を確認してください。

1. 少なくともWindows版Workspaceアプリバージョン1905がインストールされていることを確認してください。Workspaceアプリのインストールパスに HdxTeams.exeまたはHdxRtcEngine.exeとwebrpc.dllバイナリが表示されますか？
2. ステップ1を検証した場合は、HdxTeams.exeまたはHdxRtcEngine.exeが起動されているかを確認するために、以下を実行してください。
    a. VDA上のMicrosoft Teamsを終了します。
    b. VDAでservices.mscを起動します。
    c. Citrix HDX Teams Redirection Serviceを停止します。
    d. ICA®セッションを切断します。
    e. ICAセッションに接続します。
    f. Citrix HDX Teams Redirection Serviceを開始します。
    g. Citrix HDX HTML5 Video Redirection Serviceを再起動します。
    h. VDA上でMicrosoft Teamsを起動します。
3. クライアントエンドポイントでHdxTeams.exeまたはHdxRtcEngine.exeがまだ起動されていない場合は、以下を実行してください。
    a. VDA を再起動します。
    b. クライアントエンドポイントを再起動します。

サポート

Citrix と Microsoft は、Microsoft Teams の最適化を使用して、Citrix Virtual Apps and Desktops™ からの Microsoft Teams の配信を共同でサポートしています。この共同サポートは、両社間の緊密な連携の結果です。有効なサポート契約があり、このソリューションで問題が発生した場合は、問題の原因となっていると思われるコードのベンダーにサポートチケットをオープンしてください。つまり、Teams の場合は Microsoft、最適化コンポーネントの場合は Citrix です。 Citrix または Microsoft がチケットを受け取り、問題をトリアージし、必要に応じてエスカレートします。各社のサポートチームに連絡する必要はありません。

問題が発生した場合は、Teams UI で **>** をクリックすることをお勧めします。VDA側のログは、技術的な問題をより迅速に解決するために、CitrixとMicrosoft間で自動的に共有されます。

ログの収集

HDXメディアエンジンログは、ユーザーのマシン（VDA上ではない）で見つけることができます。問題が発生した場合は、必ずログをサポートケースに添付してください。

Windows ログ:

Windows ログは、**HDXTeams** フォルダー（AppData/Local/Temp/HDXTeams または AppData/Local/Temp/HdxRtcEngine）内の %TEMP% にあります。webrpc_Day_Month_timestamp_Year.txt という名前の .txt ファイルを探してください。Citrix Workspaceアプリの新しいバージョン（Citrix Workspaceアプリ 2009.5 以降など）を使用している場合は、ログを AppData\Local\Temp\HdxRtcEngine に保存します。

各セッションはログ用の個別のフォルダーを作成します。

Mac ログ:

1. VDWEBRTC ログ - 仮想チャネルの実行を記録します。

   場所：`/Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt`

2. HdxRtcEngine ログ - HdxRtcEngine 上のプロセスの実行を記録します。

   場所: `$TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log`

   HdxRtcEngineログはデフォルトで有効になっています。

3. Webrpcログ - webrtcライブラリのラップアップの実行を記録する最も重要なログです。

   場所: `/Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log`

Linuxログ：

Linuxログは`/tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/`フォルダーにあります。 Webrtcログ：`/tmp/webrpc/<current date>/webrtc.log` カーネルログ：`/var/log/syslog`

ICE/STUN/TURN/ログ：

通話を確立する際には、次の4つのICEフェーズが必要です。

- 候補収集

- 候補交換
- 接続チェック (STUNバインド要求)
- 候補昇格

HdxRtcEngine.exeログでは、以下のエントリが関連するInteractive Connectivity Establishment (ICE) エントリです。これらのエントリは、通話設定が成功するために必要です。収集段階のサンプルスニペットを以下に示します。

```
RPCStubs Info: -> device id = \\?
\display#int3470#4&1835d135&0&uid13424#{65e8773d-8f56-11d0-
a3b9-00a0c9223196}\{bf89b5a5-61f7-4127-a279-e187013d7caf} label =
Microsoft Camera Front groupId =



webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1

webrtcapi.RTCPeerConnection Info: setLocalDescription.

>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveLocalOffer



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Gathering



[…]

>>> begin:sdp

candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
generation 0 ufrag oVk6 network-id 1

<<< end:sdp
```

```
[…]

>>> begin:sdp

candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay raddr
73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1 network-cost
10

<<< end:sdp

[…]

>>> begin:sdp

candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx raddr
10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id 1

<<< end:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Complete
webrtcapi.RTCPeerConnection Info: setRemoteDescription.

>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveRemotelOffer
```

複数のICE候補がある場合、優先順位は次のとおりです。

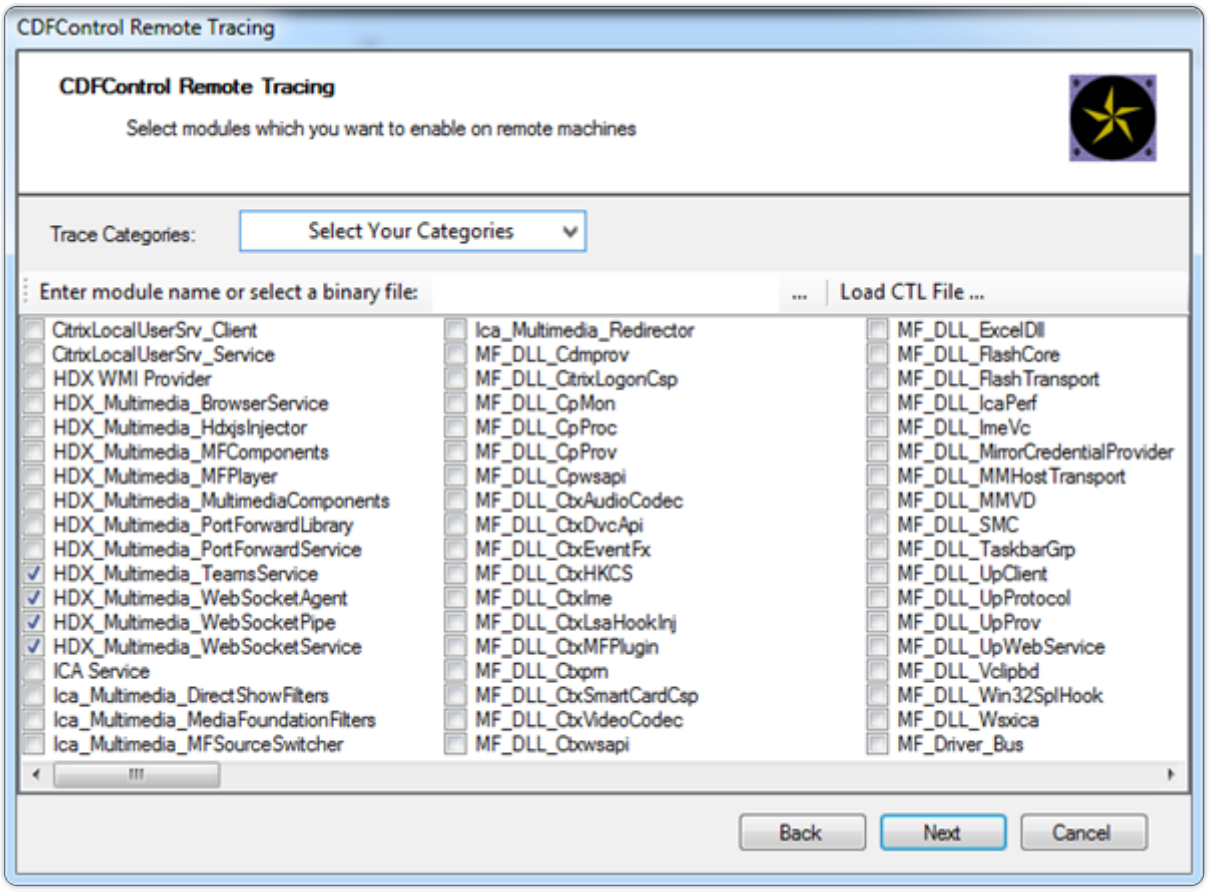
1. ホスト
2. ピア反射型
3. サーバー反射型

4. トランスポートリレー

問題が発生し、それを一貫して再現できる場合は、Microsoft Teamsで**ヘルプ > 問題の報告**をクリックすることをお勧めします。Microsoftにケースをオープンした場合、技術的な問題を解決するためにログがCitrixとMicrosoftの間で共有されます。 Citrixサポートに連絡する前にCDFトレースをキャプチャすることも有益です。詳細については、Knowledge Centerの記事CDFcontrolを参照してください。

CDF トレースを収集するための推奨事項については、Knowledge Center の記事 Recommendations for Collecting the CDF Traces を参照してください。

VDA側CDFトレース - 次のCDFトレースプロバイダーを有効にします。



Workspaceアプリ側CDFトレース - 次のCDFトレースプロバイダーを有効にします。

Workspace App 側の CDF トレース(/en-us/citrix-virtual-apps-desktops/2511/media/team-cwa-cdf-traces.png)

- IcaClient_DriversVd_TeamsRedir (オプション)
- IcaClient_Multimedia_HdxTeams (Citrix Workspace app 2012 以降が必要)

仮想チャネルプラグインマネージャー

はじめに

仮想チャネルプラグインマネージャーは、指定されたアプリケーション向けにクライアントエンドポイント全体にプラグインを展開するように設計されています。プラグインマネージャーは、VDAで実行されている特定のアプリケーションを検出し、アプリケーションの実行時に最高の体験を得るために、エンドポイントにプラグインをインストールするようユーザーに促します。

ユーザーは、プラグインをインストールするか、スキップするか、またはインストールを拒否するかを選択できます。プラグインマネージャーは、管理対象か非管理対象かを問わず、すべてのエンドポイントでプラグインを管理する柔軟性を提供します。

例: Microsoft Teams は新しいアーキテクチャ (SlimCore Optimization) を採用しており、最適化を機能させるにはエンドポイントにプラグインをインストールする必要があります。仮想チャネルプラグインマネージャーは、エンドポイント全体にプラグインを展開できます。詳細については、「Teams 向けの新しい VDI ソリューション」を参照してください。

システム要件

仮想チャネルプラグインマネージャーの最小要件は次のとおりです。

- 仮想デスクトップエージェント (VDA)
  - 2411 CR
- DDC
  - クラウド 121 リリース
  - 2407 CR
- Citrix Workspace™ アプリ (Citrix Workspace アプリ)
  - Citrix Workspace アプリ Windows 用 2409
- シトリックス ワークスペース アプリ マック 2508

> **注:**
>
> この機能は現在、Windowsエンドポイントに適用されます。

サポートされるアプリケーション

- 現在サポートされているアプリケーションは以下のとおりです:
    - Microsoft Teams - Teams向け新しいVDIソリューション を参照してください

仮想チャネルプラグインマネージャーの概要

機能の理解

Citrix® は、顧客の環境が複雑になる可能性があり、管理対象および非管理対象のエンドポイント全体にプラグインを展開するにはかなりの労力が必要であることを理解しています。この機能は、そのプロセスを簡素化するように設計されています。

この機能には2つのコンポーネントが含まれています。1つはVDA側（検出プロセス）、もう1つはCitrix Workspace™ App側（インストーラープロセス）です。管理者が、ポリシーの有効化、レジストリエントリの作成、監視するアプリケーションの指定など、上記の前提条件を満たすと、次のようになります。

- VDA側の検出プロセスは、エンドユーザーが仮想デスクトップにログオンすると、アプリケーションの起動を監視します
- 検出プロセスはCitrix Workspace App側に通知し、指定されたアプリケーションを最適化するために必要なプラグインをインストールするようユーザーに促します
- ユーザーの画面には、プラグインに関する簡単な詳細情報が記載されたポップアップが表示されます。ユーザーは、プラグインをインストールするか、スキップするか、またはインストールしないことを選択できます
    - ユーザーがインストールプロセスをスキップした場合、そのセッションではポップアップが再度表示されることはありません。インストールプロンプトは、セッションの再接続時に表示されます。
    - ユーザーがプラグインをインストールしないことを選択した場合、その選択はユーザープロファイルに記録され、管理者が確認できるようになります。
- ユーザーがプラグインをインストールすることを選択した場合、Citrix Workspace App側がエンドポイントにプラグインをダウンロードしてインストールします。
    - インストールが成功すると、プラグインを有効にするためにセッションを再接続するよう促すメッセージがユーザーに表示されます。ユーザーはすぐに再接続するか、成功メッセージを閉じて後で再接続するかを選択できます。
    - インストールが失敗した場合、ユーザーにはエラーメッセージが表示され、失敗は管理者が確認できるように記録されます。

仮想チャネルプラグインマネージャーの構成

展開

1. Microsoft Teamsリダイレクトポリシーが有効になっているか確認します。詳細については、Microsoft Teamsリダイレクトポリシーを参照してください。

   監視対象のアプリケーションに関わらず、このポリシーを有効にする必要があります。今後、より多くのアプリケーションがサポートされ、Microsoft Teamsの代わりにそれらのアプリケーションを監視したい場合でも、このポリシーは有効にしておく必要があります。このポリシーはデフォルトで有効になっています。

2. 仮想チャネルプラグインマネージャーポリシーを有効にする必要があります。ポリシーを有効にする方法の詳細については、仮想チャネルプラグインマネージャーポリシー設定を参照してください。

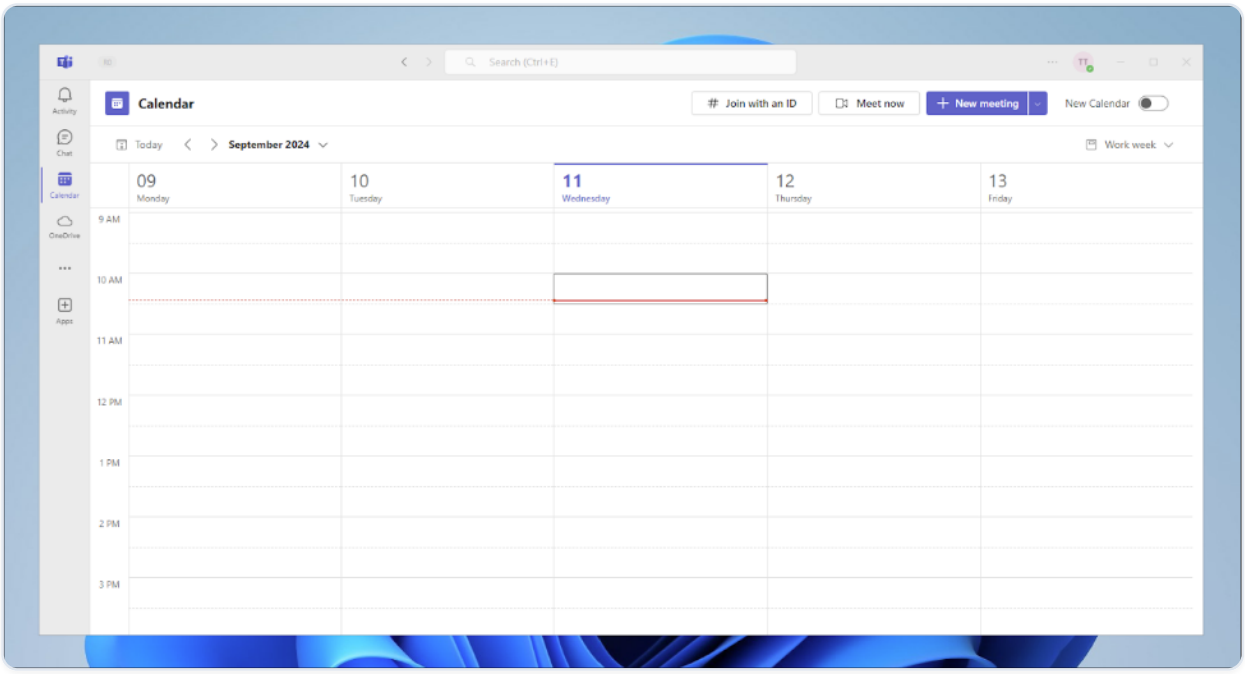
   このポリシーは、Citrix Studioのマルチメディアポリシー設定で利用できます。このポリシーを有効にすると、監視するアプリケーション名（例：「Microsoft Teams」）を指定できます。このポリシーはデフォルトで無効になっています。

3. Citrix Workspace™アプリはシステム全体モードでインストールする必要があります。

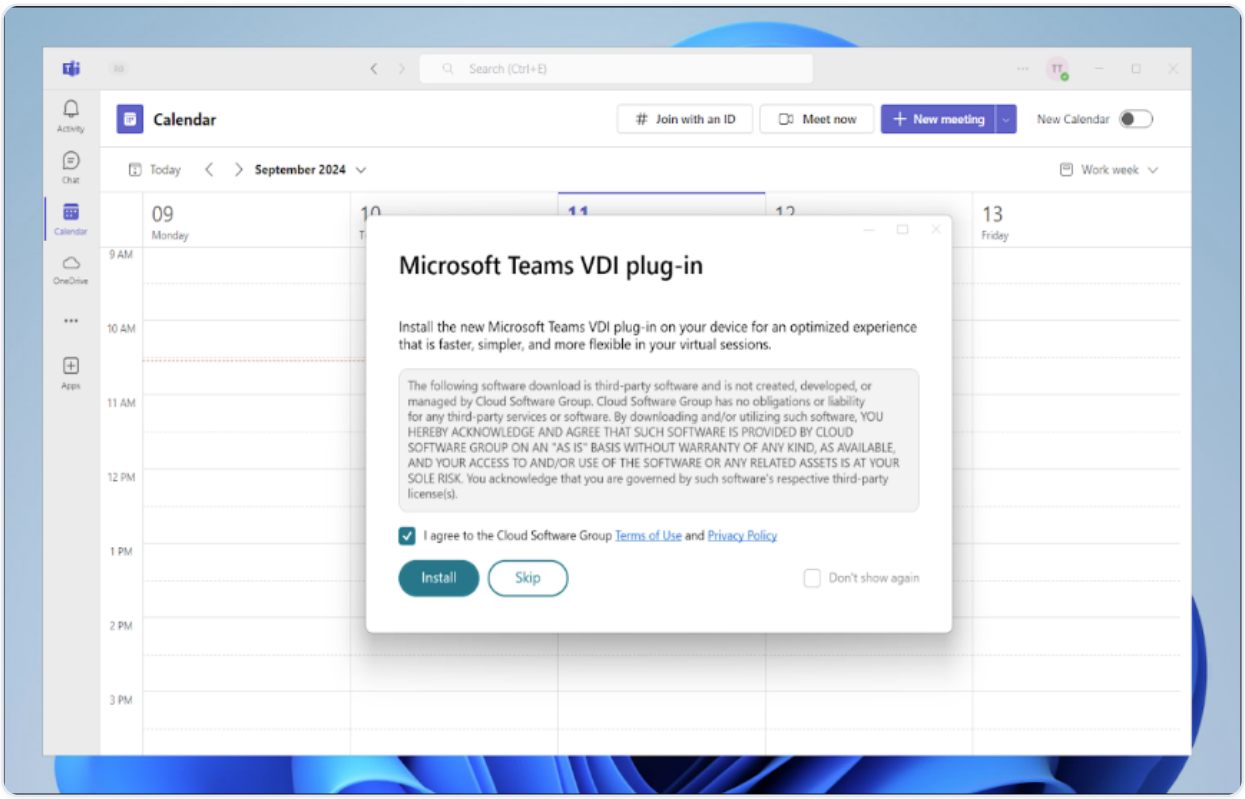
> **注:**
>
> プラグインは、サードパーティのCDNからエンドポイントにダウンロードされます。たとえば、Microsoft Teamsを選択した場合、プラグインはMicrosoft CDNからダウンロードされます。したがって、エンドポイントはサードパーティのCDNにアクセスできる必要があります。そうでない場合、プラグインのインストールは失敗します。

手順

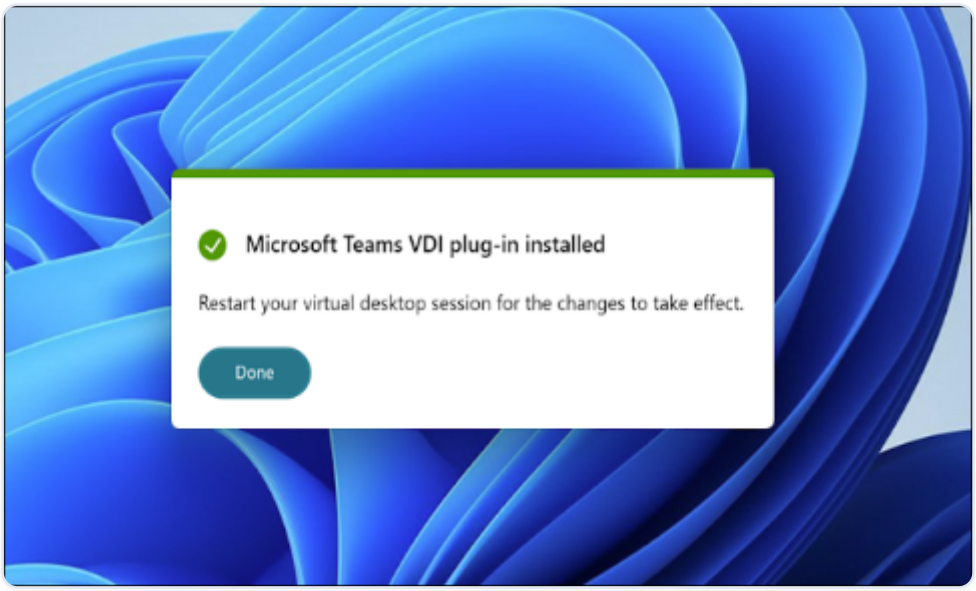
1. ユーザーはCitrixセッションでアプリケーションを起動します。例：Microsoft Teams。



2. ユーザーは、より良いエクスペリエンスのために、エンドポイントにTeams VDIプラグインをインストールするためのポップアップを受け取ります。プラグインはエンドポイントにインストールされるため、ポップアップはセッション内ではなくセッションの上に表示されます。



3. ユーザーがインストールボタンをクリックすると、プラグインがインストールされます。変更を有効にするには、仮想デスクトップセッションを再起動する必要があります。



既知の問題と制限事項

- 2407 VDAでは、機能を有効にするためのポリシーに加えて、以下のレジストリ設定をVDA上で1に設定する必要があります。このレジストリ設定は、2411 VDA以降では自動的に許可され、構成する必要はありません。

  `HKLM\SOFTWARE\Citrix\HDXMediaStream

  Name: EnableAppDetector Type: DWORD`
- その他の制限事項は追加予定です

Unified Communications SDK の最適化

はじめに

Citrix Virtual Apps and Desktops は、幅広いエンドポイントデバイスでユーザーにアプリケーションを配信できます。これらのアプリケーションの多くには、オーディオおよびビデオ会議のようなリアルタイム通信 (RTC) 機能が含まれています。しかし、仮想化環境でこれらのアプリケーションを配信する際には、課題が生じる可能性があります。従来の配信方法では、メディアストリーム (オーディオ/ビデオ) をクライアントデバイスからデータセンター内のVDIサーバーにルーティングし、その後エンドポイントに送り返します。この「ヘアピン化」は、特に帯域幅を大量に消費するオーディオおよびビデオ通話において、サーバーに不要なトラフィックと処理オーバーヘッドをもたらします。

Citrix Unified Communications SDK (UCSDK) は、テクノロジーベンダーがこれらのRTCアプリケーションをCitrix環境で使用するために最適化できるようにするテクノロジーです。アプリケーションが最適化されると、ローカルデスクトップで実行されているアプリケーションと同等か、

それ以上のユーザーエクスペリエンスを提供できます。今日の世の中では、シームレスなリアルタイム通信は生産性とコラボレーションに不可欠です。仮想環境内でアプリケーションを使用する場合、音声通話やビデオ通話、画面共有、その他の通信機能がローカルデスクトップと同じくらいスムーズに動作することが重要です。最適化されたアプリケーションは、このエクスペリエンスを提供します。

この製品ドキュメントでは、Citrixのお客様がUCSDK最適化アプリケーションを学習し、展開するために必要なすべてを詳述しています。

動作の仕組み

Citrixは、VDI内のリアルタイム通信アプリケーション向けに最適化された配信方法を提供しています。このアプローチでは、Unified Communications SDK (UCSDK) を活用して、仮想化されたアプリケーションを次の2つの部分に分割します。

- **ユーザーインターフェイス (UI):** ユーザーインターフェイスは仮想ホスト内に残り、仮想デスクトップまたはアプリケーションウィンドウ内にシームレスに表示されます。
- **メディアエンジン:** メディア処理タスク (オーディオおよびビデオのエンコード/デコード) は、ユーザーのローカルデバイスにオフロードされます。これにより、サーバーの負荷が最小限に抑えられ、ネットワーク使用量が最適化されます。

通常、Citrixはリアルタイム通信分野のテクノロジーベンダーにUCSDKを提供し、それらのアプリケーションにUCSDKを統合するために協力しています。統合されると、UCSDK最適化アプリケーションを使用するCitrixのお客様は、強化されたエクスペリエンスを得ることができます。Citrix UCSDKは、カスタムの社内アプリケーションが構築されている場合にも、Citrixのお客様が利用できます。ただし、ほとんどの場合、お客様はUCSDKを利用して開発する必要はなく、最適化されたエクスペリエンスを実現するためにCitrix環境とアプリケーションを構成するだけで済みます。

> **注:**
>
> Citrix WebRTC SDK (または) HDX™最適化アプリケーションへの参照は、Citrix UCSDKとの統合を示しており、互換的に使用できます。

主な利点

Citrix UCSDKで最適化されたアプリケーションを使用する場合、次のことが期待できます。

- プロセッサ集約型のメディアエンコード/デコードをCitrix Virtual Delivery Agent (VDA) からクライアントエンドポイントにオフロードすることにより、メディア処理パフォーマンスが向上し、エンドユーザーの全体的な応答性が向上します。
- Citrix VDAでのCPUおよび帯域幅使用量の削減により、IT部門はホストあたりより多くの同時実行ユーザーをサポートできるようになり、企業はCitrix仮想デスクトップの展開を費用対効果の高い方法で拡張できます。
- 最適化されたエンドポイントがレガシー仮想デスクトップの寿命を延ばし、ホストインフラストラクチャの必要性を削減するため、企業にとっての総所有コストが削減され、これにより設備投資と運用コストを長期的に削減できます。
- Windows、Mac、Linux、ChromeOS、HTML5のエンドポイントプラットフォームに対応。

ユースケース

UCSDKは、WebRTC標準に準拠するリアルタイム通信アプリケーションを最適化するために特別に構築されています。以下に、主要なシナリオと、UCSDKを使用できる/すでに使用しているWebRTCベースのアプリケーションの種類を示します。

- **Contact Center as a Service (CCaaS) / クラウドコンタクトセンタープラットフォーム:** 主に複数のチャネルにわたる顧客とのやり取りを管理し、エージェントのワークフローを最適化します。
    - 例: アマゾンコネクト, トゥイリオ, アバイア エクスペリエンス プラットフォーム, トークデスク, コンテンツグル
- **Unified Communications as a Service (UCaaS) / クラウドビジネスコミュニケーション:** 音声、ビデオ、チームメッセージング、プレゼンスを統合し、包括的なビジネスコミュニケーションを実現します。
    - 例: リングセントラル、エイトバイエイト、インターメディア、アルカテル・ルーセント レインボー
- **Communications Platform as a Service (CPaaS):** リアルタイム通信機能をカスタムアプリケーションに直接組み込むためのAPIを提供します。
    - 例: トゥイリオ、リボン・コミュニケーションズ
- **エンタープライズビデオ会議およびコラボレーション:** 高品質のビデオ会議、カンファレンス、高度なコラボレーション機能のための専用プラットフォームです。
    - 例: Pexip

- **金融取引通信:** 金融市場の独自の、高性能でコンプライアンスに準拠した通信ニーズのために設計されています。
    - 例: IPC Unigy
- **仮想学習およびトレーニングプラットフォーム:** インタラクティブで高品質な仮想教室およびトレーニング体験のために設計されています。
    - 例: ビテロ

Citrix UCSDKの基盤となるWebRTCにより、その最適化機能はWebRTCベースのあらゆる通信アプリケーションに拡張できます。これにより、リアルタイムインタラクションにWebRTCを利用する幅広いアプリケーションの最適化が可能になります。これらのアプリケーションが現在UCSDKで最適化されているとリストされていなくても、最適化を希望するユースケースやアプリケーションがあれば、Citrixにお問い合わせいただくことをお勧めします。

UCSDK アーキテクチャ

UCSDK アーキテクチャ (/en-us/citrix-virtual-apps-desktops/2511/media/ucsdk-architecture.png)

- ベンダーアプリケーション: これは、UCSDK を統合した、デスクトップベースまたはブラウザベースのサードパーティ製リアルタイム通信アプリケーションです。
- UCSDK JS: UCSDK JS は、ベンダーアプリケーションがオーディオ/ビデオをエンドポイントにオフロードするために利用する API を提供します。
- HdxRtcEngine: これは、Citrix Workspaceアプリに組み込まれたWebRTCメディアエンジンで、オフロードされたオーディオ/ビデオ通話を処理します。

SDKがロードされて使用されると、リダイレクトが成功した場合、クライアントエンドポイントで`HdxRtcEngine.exe`プロセスが起動します。クライアントエンドポイントで`HdxRtcEngine.exe`が起動すると、すべてのシグナリングおよびペイロードデータはCitrix VDAからクライアントエンドポイントに流れ、クラウドに到達し、クライアントエンドポイントに戻ってからVDAに転送されます。たとえば、フローの完全な往復は次のようになります。

`Vendor App -> CitrxWebrtc.js SDK -> Citrix VDA components -> Citrix Client Endpoint components -> Cloud -> Citrix Client Endpoint components -> Citrix VDA components -> CitrxWebrtc.js SDK -> Vendor App`

システム要件

システム要件は、UCSDKの最新バージョンである5.0.0で必要となるCitrixコンポーネントのさまざまなバージョンを示しています。SDKの以前のバージョンおよび特定の機能要件に関する互換性の詳細については、以下のバージョンと機能マトリックス表を参照してください。

> **注:**
>
> お客様が UCSDK に追加された機能を使用するには、ベンダーアプリケーションが適切な UCSDK バージョンを統合し、その機能を有効にしていること、および環境で適切な VDA および CWA バージョンを使用していることを確認してください。

完全な互換性のあるバージョン

「完全に互換性のあるバージョン」とは、これらのCitrixコンポーネントのバージョンを最新バージョンのUCSDKと組み合わせて使用することで、お客様が利用可能なすべての機能を利用できることを示します。現在の最新バージョンであるUCSDK 5.0.0の場合、Citrixコンポーネントの完全に互換性のあるバージョンは以下のとおりです。

- **シトリックス バーチャルアプリ™ および デスクトップ:** 2603
- **シトリックス ワークスペースアプリ ウィンドウズ:** 2603
- **Citrix Workspace App Mac:** リリース予定
- **Citrix Workspace アプリ リナックス:** 2603
- **Citrix Workspace App ChromeOS/HTML5:** リリース予定

> **注:**
>
> UCSDK最適化は、すべてのエンドポイントプラットフォーム：Windows、Mac、Linux、ChromeOS、およびHTML5でサポートされています。上記のリストで特定のエンドポイントプラットフォームに対して**リリース予定**と表示されている場合、それは最新のUCSDK機能と完全に互換性のあるバージョンがまだリリースされていないことを意味します。したがって、お客様は、新しいUCSDKを使用している場合でも、既存の機能を引き続き使用するために、Citrix Workspaceアプリの古いバージョンを使用できます。

構成

UCSDKの機能は、ベンダーが統合したUCSDKのバージョンとベンダーが有効にした機能、Citrix Virtual Apps and Desktops、および使用中のCitrix Workspaceアプリのバージョンの3つの要因に依存します。

Citrix側では、最適化されたアプリケーションが最適化されるように、以下が構成されていることを確認してください。

1. Microsoft Teamsリダイレクトポリシーがオンになっていることを確認します。詳細については、マルチメディアポリシー設定を参照してください。このポリシーはデフォルトでオンになっています。
2. `CitrixWebrtc.js` SDKを利用するサードパーティのElectronまたはブラウザベースのアプリケーションは、デフォルトではサポートされていません。`CtxHdxWebSocketService` (`WebSocketService.exe`) は、許可リストにないアプリケーションからの接続を許可しません。目的のアプリケーションバイナリ実行可能ファイル名をホワイトリストレジストリキーに追加する必要があります。

VDA上

- キーパスを作成します: `HKLM\Software\WOW6432Node\Citrix\WebSocketService`
- キー名: `ProcessWhitelist`
- タイプ: `MULTISZ`
- キー値: `Mytestapp.exe`

複数のアプリケーションがある場合は、各アプリケーションを新しい行に入力します。テキストファイルからコピー＆ペーストしたり、コンマを挿入したりしないでください。指定された名前がアプリケーションの実行可能ファイル名と一致していることを確認してください。このレジストリ値は大文字と小文字を区別しません。

アプリケーションが本格的なデスクトップアプリケーションではなくブラウザ経由でアクセスされる場合、レジストリ値で例えば `chrome.exe` を許可する必要があります。

上記のレジストリが正常に構成されたら、VDA を再起動するか、`CtxHdxWebSocketService` を再起動してホワイトリストの設定を完了します。

クライアント上

設定は不要です。Citrix Workspace アプリをインストールするだけです。

各ベンダーは非常に特定のアプリケーション名を持っている場合があります。したがって、WebSocketService で許可する必要があるアプリケーション名を特定するには、現在のベンダーサポート セクションにリンクされているベンダーのドキュメントを参照してください。

機能リファレンス

Smart Sync による通話接続時間の短縮

UCSDK 5.0.0 で導入された Smart Sync 機能は、VDA とクライアントエンドポイント間の通信を効率化することで、通話接続時間を短縮します。この機能強化により、全体的に通話設定が高速化され、特に高遅延ネットワーク環境で最も顕著なパフォーマンス向上をもたらします。

Citrix は、この機能を活用するために、顧客がアプリケーションベンダーに連絡して UCSDK 5.0.0 にアップグレードすることを推奨します。

> **注:**
>
> この機能は UCSDK 5.0.0 と Citrix Workspace アプリのみに依存します。正確なクライアントバージョンについては、バージョンと機能マトリックス を参照してください。VDA のバージョン依存性はないため、以前のサポート対象 VDA も引き続き使用できます。

パフォーマンスとユーザーエクスペリエンスを向上させる最適化されたオーバーレイクリッピング

CVAD 2511以降、HDX Microsoft Teams最適化やUCSDK最適化などの機能におけるリダイレクトされたビデオオーバーレイを処理するメカニズムは、ユーザーエクスペリエンスとサーバーパフォーマンスの両方を向上させるために再設計されました。

主な利点

- **視覚的な正確性の向上:** この機能強化により、ポップアップメニューや通知などのアプリケーション要素がビデオコンテンツの背後に誤って表示される視覚的な不具合が解消されます。新しいロジックにより、すべてのコンポーネントが正しい順序でレンダリングされ、よりシームレスで予測可能なエクスペリエンスが提供されます。
- **パフォーマンスの向上:** この最適化により、Virtual Delivery AgentでのCPU使用率が大幅に削減されます。古いリソースを大量に消費するポーリング方法を、より効率的なグラフィックベースのアプローチに置き換えることで、この変更はサーバーのスケーラビリティを向上させ、より高いユーザー密度を可能にします。

注:

この機能は、将来のバージョンのMicrosoft Teams（またはその他のUCSDKパートナーアプリケーション）に依存し、Citrix Workspace App for Windows 2511が必要です。

バージョンと機能マトリックス

バージョン更新は頻繁に行われるため、特定のバージョンがサポートされていることを確認するには、Citrix Virtual Apps and Desktops および Citrix Workspace app の製品ライフサイクルページを参照してください。多くの古い機能については、表に記載されているバージョンは、このドキュメントの執筆時点での最終サポート対象のCurrent Release (CR) バージョンです。

機能	UCSDK バージョン	VDA	CWA ウィンドウズ	CWA MAC	CWA リナックス	CWA CHROME OS/ HTML5
オーディオ/ビデオ (P2P & 会議)	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2312
画面共有	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2312
DTMF	3.1.0	2203 LTSR 最新CU / 2311 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2312
プロキシサーバーのサポート	3.1.0	2203 LTSR 最新CU / 2311 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2312
アプリ共有	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	N/A

機能	UCSDK バージョン	VDA	CWA ウィンドウズ	CWA MAC	CWA リナックス	CWA CHROME OS/ HTML5
動的 e911	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2312
マルチウィンドウ	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2312
SDP 統合プランのサポート	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2312
ストリーム解像度 / サイマルキャスト	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2312
リモートオーディオ (ループ付き)	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2405
ブラウザベースの UCSDK (ブートストラップサポート)	4.0.2	2407 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2312
Web HID API	4.0.2	2203 LTSR 最新 CU / 2311 CR	2409.10	2411	2411	2505

機能	UCSDK バージョン	VDA	CWA ウィンドウズ	CWA MAC	CWA リナックス	CWA CHROME OS/ HTML5
ウェブオーディオAPI	4.0.2	2203 LTSR 最新 CU / 2311 CR	2405	2405	2405	該当なし
ICE の再起動	4.1.0	2203 LTSR 最新 CU / 2311 CR	2503.2	2503	2503	2502.10
画面録画 (プレビュー)[1]	4.1.0	2503	2503.2	該当なし	該当なし	該当なし
SmartSync	5.0.0	2203 LTSR 最新 CU / 2311 CR	2603	該当なし	2604	該当なし

注:

画面録画用の新しいポリシーを導入したため、CVAD 2503に付属するdelivery controller™のバージョン2503が必要です。

現在のベンダーサポート

複数のサードパーティベンダーが、Unified Communications SDK を自社製品に統合しています。ベンダーとそのサポートドキュメントの現在のリストを以下に示します。

ベンダー	ドキュメント
スプリンクラー	Citrix Media Offloading (音声通話向け)
マイクロソフト ダイナミクス 365	Dynamics 365 Contact Center ドキュメント

ベンダー	ドキュメント
アマゾン コネクト	Citrix Cloud Desktops 向け Amazon Connect オーディオの最適化
リングセントラル	Citrix VDI 環境での RingCentral の使用
ファイブナイン	Citrix 環境における Five9 WebRTC
トゥイリオ	Citrix VDI 上の トゥイリオ フレックス
アバイア	Citrix 向け Avaya Experience Platform Public Cloud VDI ソリューション
8x8	デスクトップおよびウェブ向け 8x8 Work との Citrix VDI 統合
コンテンツ・グル	コンテンツ・グル Citrix 統合
リボン・コミュニケーションズ	リボン・コミュニケーションズ Citrix WebRTC SDK
インターメディア	Citrix Virtual Apps and Desktops での Intermedia Unite のインストール
アルカテル・ルーセント・レインボー	Rainbow デスクトップアプリケーション向け Citrix の最適化
トークデスク	トークデスク エージェント・ワークスペース VDI コネクト
IPC	IPC ユニジー ソフトクライアント Citrix VDI
ヴィテロ	Citrix VDI 向け ヴィテロ・インスパイア
ペクシプ	Citrix Pexip Infinity Docs で Connect デスクトップアプリを展開する
ズーム ウェブアプリ	Zoom Web App の WebRTC リダイレクトを構成する

トラブルシューティング

トラブルシューティング情報については、Citrix Unified Communications SDK で最適化されたアプリのトラブルシューティング ガイダンスを参照してください。

既知の問題と制限事項

このセクションでは、現在認識されている既知の問題と制限事項について説明します。

一般的なコンテンツリダイレクト

クライアントフォルダーリダイレクト

クライアントフォルダーリダイレクトは、クライアント側のファイルがホスト側のセッションでアクセス可能になる方法を変更します。サーバーでクライアントドライブマッピングのみを有効にすると、クライアント側のフルボリュームは、Universal Naming Convention (UNC) リンクとしてセッションに自動的にマップされます。サーバーでクライアントフォルダーリダイレクトを有効にし、ユーザーがユーザーデバイスでそれを構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

ユーザーが指定したフォルダーのみが、セッション内でUNCリンクとして表示されます。つまり、ユーザーデバイス上の完全なファイルシステムではなく、指定されたフォルダーのみが表示されます。レジストリを介してUNCリンクを無効にすると、クライアントフォルダーはセッション内でマップされたドライブとして表示されます。

クライアントフォルダーリダイレクトは、WindowsシングルセッションOSマシンでのみサポートされています。

外部USBドライブのクライアントフォルダーリダイレクトは、デバイスの取り外しや再接続時には保存されません。

サーバーでクライアントフォルダーリダイレクトを有効にします。次に、クライアントデバイスで、リダイレクトするフォルダーを指定します。クライアントフォルダーオプションを指定するために使用するアプリケーション (CtxCFRUI.exe) は、このリリースで提供されるCitrix Workspaceアプリに含まれています。

要件:

サーバーの場合:

- ウィンドウズ サーバー 2022
- Windows Server 2019、StandardおよびDatacenterエディション

クライアントの場合:

- ウィンドウズ 10

- ウィンドウズ 11

サーバーでクライアントフォルダーリダイレクトを有効にするには、レジストリで管理される機能のリストにあるクライアントフォルダーリダイレクトを参照してください。

ユーザーデバイスで、リダイレクトするフォルダーを指定します:

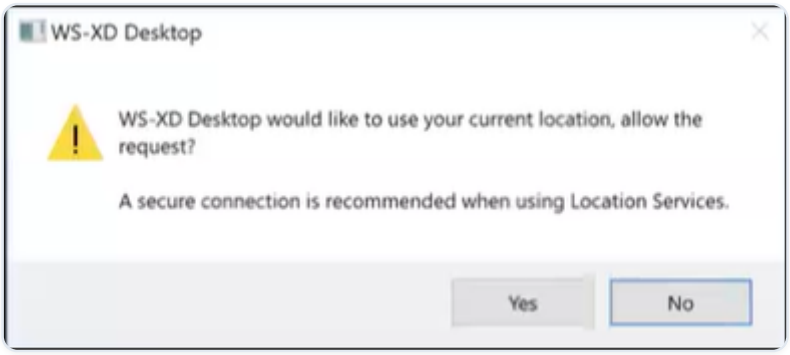
1. Citrix Workspace™アプリの最新バージョンがインストールされていることを確認します。
2. Citrix Workspaceアプリのインストールディレクトリから、CtxCFRUI.exeを起動します **(..\Citrix\ICA Client\CtxCFRUI.exe)**。
3. **カスタム**ラジオボタンを選択し、フォルダーを追加、編集、または削除します。
4. 設定を有効にするには、セッションを切断して再接続します。

クライアント位置情報リダイレクト

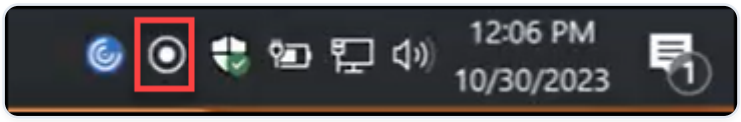
クライアント位置情報リダイレクトを有効にすると、VDAでホストされているアプリとデスクトップセッションが、クライアントの現在の位置情報にシームレスにアクセスできるようになります。マルチセッションオペレーティングシステム（TS VDAまたはマルチセッションWS VDA）では、各セッションは接続されたクライアントによって提供される独自の場所を持ちます。この機能を使用すると、位置情報に依存するVDA上のアプリケーションは、クライアントの正確な位置情報を取得できます。

詳細については、Microsoftドキュメントを参照してください。

クライアント位置情報リダイレクトが有効になり、サーバー側とクライアント側の両方で位置情報へのアクセスが許可されると、位置情報にアクセスするアプリケーションまたはデスクトップを起動したときに、クライアントは次のダイアログボックスで現在の位置情報を共有するように求めます。



クライアント位置情報リダイレクトを有効にすると、VDAでホストされているアプリまたはデスクトップが現在の位置情報を照会したときに、クライアントのタスクバーに次のアイコンが表示されます。



システム要件

サーバーの場合：

- シングルセッション（Win10/11）またはマルチセッション（Win 11 22H2およびServer 2022 23H2以降）OS VDA
- Windows、iOS、またはAndroid用Citrix Workspace™アプリ

構成

この機能が動作するには、Citrix®ポリシーを使用してクライアント位置情報リダイレクトを有効にする必要があります。クライアント位置情報リダイレクトはデフォルトで無効になっています。

クライアント位置情報リダイレクトを有効にするには、次の手順を実行します。

Windows VDAおよびクライアント側で：

1. **設定 > プライバシー > 位置情報**で、次のオプションを有効にします。
    - **このデバイスでの位置情報へのアクセスを許可する**
    - **アプリがあなたの位置情報にアクセスすることを許可する**
    - **デスクトップアプリがあなたの位置情報にアクセスすることを許可する**
2. マルチセッションOSの場合、**位置情報の上書き**設定を有効にします。

Controller/DDC側で:

Studio > ポリシー > 位置情報 > 設定 > アプリケーションがクライアントデバイスの物理的な位置情報を使用することを許可するポリシーを有効にします。 詳細については、クライアントセンサーポリシー設定を参照してください。

双方向コンテンツリダイレクト

双方向コンテンツリダイレクトにより、Webブラウザ内のHTTPまたはHTTPS URL、あるいはアプリケーションに埋め込まれたURLを、Citrix VDAセッションとクライアントエンドポイント間で双方向に転送できます。Citrixセッションで実行されているブラウザに入力されたURLは、クライアントのデフォルトブラウザを使用して開くことができます。逆に、クライアントで実行されているブラウザに入力されたURLは、公開アプリケーションまたはデスクトップのいずれかを使用し

て、Citrixセッションで開くことができます。双方向コンテンツリダイレクトの一般的なユースケースには、次のものがあります。

- 開始ブラウザがソースへのネットワークアクセスを持たない場合のWeb URLのリダイレクト。
- ブラウザの互換性およびセキュリティ上の理由によるWeb URLのリダイレクト。
- CitrixセッションまたはクライアントでWebブラウザを実行したくない場合に、アプリケーションに埋め込まれたWeb URLをリダイレクトする。

システム要件

- シングルセッションまたはマルチセッションOS VDA
- Windows 用 Citrix Workspace™ アプリ 2311 以降
- Linux 用 Citrix Workspace™ アプリ 2503 以降
- Mac用 Citrix Workspace™ アプリ 2607以降

ブラウザー：

- Citrix Browser Redirection 拡張機能を備えたGoogle Chrome
  - Google Chrome拡張機能
- Citrix ブラウザリダイレクト拡張機能を搭載したMicrosoft Edge
  - Microsoft Edge拡張機能

構成

Citrix Virtual Apps and Desktops™ バージョン 2311 以降、双方向コンテンツリダイレクトは Citrix Studio を介してのみ構成されます。以前のリリースでは、クライアントエンドポイントと Studio の両方でポリシー設定が構成されていました。双方向コンテンツリダイレクトはデフォルトで無効になっています。

VDA の構成については、**ICA ポリシー**設定の双方向コンテンツリダイレクトを参照してください。

ブラウザーリダイレクトを機能させるには、表示されているコマンドを使用して、元のブラウザー（URL のリダイレクト元）にブラウザー拡張機能を登録する必要があります。使用しているブラウザーに基づいて、必要に応じて VDA とクライアントでコマンドを実行します。

ブラウザー	VDA	クライアント
グーグル クローム	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regChrome	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regChrome
マイクロソフト Edge	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regEdge	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regEdge
利用可能なすべてのブラウザー	コマンド: "%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regall	コマンド: "%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regall

ブラウザ拡張機能を登録解除するには:

ブラウザ	VDA	クライアント
グーグル クローム	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregChrome	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregChrome
マイクロソフト エッジ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregEdge	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregEdge
利用可能なすべてのブラウザ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregall	"%ProgramFiles(x86)%\シトリックス\ICA クライアント\リダイレクター.exe" /すべて登録解除

注:

- これらのコマンドを管理者権限でコマンドプロンプト (CMD) ウィンドウで実行します。

- register コマンドを実行すると、Chrome および Edge ブラウザーは、初回起動時に Citrix Browser Redirection Extension を有効にするようユーザーに求めます。
- 登録コマンドは、Browser Redirection Extension をネイティブメッセージングホストにリンクさせ、これにより拡張機能がネイティブコードと通信できるようになります。これがないと、ブラウザーは通信をブロックします。
- ブラウザー拡張機能は、Google Chrome ウェブストアから手動でインストールすることもできます。Microsoft Edge アドオンストアから Browser Redirection Extension を使用するには、Virtual Delivery Agent (VDA) バージョン 2503 以降が必要です。古い VDA バージョンの場合は、Microsoft Edge ブラウザー内で Google Chrome ウェブストアから拡張機能をインストールしてください (Chrome ウェブストアから Microsoft Edge に拡張機能を追加する を参照)。
- システム要件に記載されている Citrix Workspace アプリのバージョンは、双方向コンテンツリダイレクトと OAuth リダイレクトの両方をサポートするために必要な最小バージョンです。
- Mac の場合: 公証済みアプリケーションに関する macOS のセキュリティ要件のため、カスタム OAuth コールバック URL スキームは Citrix に事前登録する必要があり、インストール後に動的に変更することはできません。デフォルトでは `citrix-oauth-redir` のみがサポートされています。URL スキームを登録するには、Citrix 製品チームにお問い合わせください。

Citrix VDA からクライアントへのワイルドカードリダイレクト

双方向コンテンツリダイレクトは、リダイレクトする URL を定義する際にワイルドカードの使用をサポートしています。双方向コンテンツリダイレクトを構成するには、構成 の手順を参照してください。

VDA からクライアントへのカスタムプロトコルリダイレクト

双方向コンテンツリダイレクトは、Citrix VDA からクライアントへのカスタムプロトコルのリダイレクトをサポートしています。HTTP または HTTPS 以外のプロトコルがサポートされています。双方向コンテンツリダイレクトを構成するには、構成 の手順を参照してください。

Web Studio で、**双方向コンテンツリダイレクト**でカスタムプロトコルを設定します。

注:

- これらのコマンドを実行するには、管理者権限が必要です。
- クライアントには、プロトコルを処理するために登録されたアプリケーションが必要です。そうでない場合、URL はクライアントにリダイレクトされますが、起動に失敗します。
- Chrome および Edge ブラウザーで入力または起動するカスタムプロトコル URL はサポートされておらず、リダイレクトされません。
- 以下のプロトコルはサポートされていません: `rtsp://, rtspu://, pnm://, mms://`。

その他の考慮事項

- ブラウザの要件と構成は、リダイレクトを開始するブラウザにのみ適用されます。リダイレクトが成功した後にURLが開かれる宛先ブラウザは、サポート対象とは見なされません。VDAからクライアントにURLをリダイレクトする場合、サポートされるブラウザ構成はVDA上でのみ必要です。逆に、クライアントからVDAにURLをリダイレクトする場合、サポートされるブラウザ構成はクライアント上でのみ必要です。リダイレクトされたURLは、方向に応じて、クライアントまたはVDAのいずれかの宛先マシンで構成されたデフォルトのブラウザに渡されます。VDAとクライアントで同じブラウザタイプを使用する必要はありません。
- リダイレクトルールがループ構成にならないことを確認してください。たとえば、VDAポリシーが`https://www.citrix.com`をリダイレクトするように設定され、クライアントポリシーが同じURLをリダイレクトするように設定されている場合、無限ループが発生します。
- URL短縮サービスはサポートされていません。
- クライアントからVDAへのリダイレクトには、Windowsクライアントが管理者権限でインストールされている必要があります。
- 宛先ブラウザがすでに開いている場合、リダイレクトされたURLは新しいタブで開きます。そうでない場合、URLは新しいブラウザウィンドウで開きます。
- 双方向コンテンツリダイレクトは、ローカルアプリアクセス (LAA) が有効になっている場合は機能しません。

ホストからクライアントへのリダイレクト

ホストからクライアントへのリダイレクトにより、Citrix®セッションで実行されているアプリケーションにハイパーリンクとして埋め込まれたURLを、ユーザーのエンドポイントデバイス上

の対応するアプリケーションを使用して開くことができます。ホストからクライアントへのリダイレクトの一般的なユースケースには、次のものがあります。

- Citrixサーバーがソースへのインターネットまたはネットワークアクセスを持たない場合のWebサイトのリダイレクト。
- セキュリティ、パフォーマンス、互換性、またはスケーラビリティの理由から、Citrixセッション内でWebブラウザを実行することが望ましくない場合のWebサイトのリダイレクト。
- URLを開くために必要なアプリケーションがCitrixサーバーにインストールされていない場合の特定のURLタイプのリダイレクト。

ホストからクライアントへのリダイレクトは、Webページでアクセスしたり、Citrixセッションで実行されているWebブラウザのアドレスバーに入力したりするURLを対象としていません。Webブラウザでのリダイレクトについては、双方向URLリダイレクトまたはブラウザコンテンツリダイレクトを参照してください。

システム要件

- マルチセッションOS VDA
- サポートされているクライアント:
  - Windows 用 Citrix Workspace™ アプリ
  - Mac 用 Citrix Workspace アプリ
  - Linux 用 Citrix Workspace アプリ
  - HTML5 用 Citrix Workspace アプリ
  - Chrome 用 Citrix Workspace アプリ

クライアントデバイスには、URLタイプのリダイレクトを処理するためのアプリケーションがインストールされ、構成されている必要があります。

構成

この機能を有効にするには、ホストからクライアントへのリダイレクト Citrixポリシーを使用します。**ホストからクライアントへのリダイレクト**は、デフォルトで無効になっています。ホストからクライアントへのリダイレクトポリシーを有効にすると、Citrix Launcherアプリケーションは Windowsサーバーに登録され、URLをインターセプトしてクライアントデバイスに送信できるようになります。

次に、必要なURLタイプのデフォルトアプリケーションとしてCitrix Launcherを使用するようにWindowsグループポリシーを構成する必要があります。CitrixサーバーVDAで、ServerFTAdefaultPolicy.xmlファイルを作成し、次のXMLコードを挿入します。

```
<?xml version="1.0" encoding="UTF-8"?>



<DefaultAssociations>



<Association Identifier="http" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



<Association Identifier="https" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



</DefaultAssociations>
```

グループポリシー管理コンソールから、**コンピューターの構成 > 管理用テンプレート > Windowsコンポーネント > エクスプローラー > 既定の関連付け構成ファイルの設定**に移動し、ServerFTAdefaultPolicy.xmlファイルを保存します。

注:

Citrixサーバーにグループポリシー設定がない場合、WindowsはURLを開くためのアプリケーションを選択するようユーザーに促します。

デフォルトでは、次のURLタイプのリダイレクトをサポートしています。

- HTTP
- HTTPS
- RTSP

- RTSPU
- PNM
- MMS

リダイレクト用のリストに、追加の標準またはカスタムURLタイプを含めるには、以前に参照したServerFTAdefaultPolicy.xmlファイルに新しい**Association Identifier**行を作成します。例：

```
<Association Identifier="ftp" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="mailto" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="customtype1" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="customtype2" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

リストにURLタイプを追加するには、クライアント構成も必要です。Windowsクライアントで以下のレジストリキーと値を作成します。

> **注:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような重大な問題が発生する可能性があります。レジストリエディターの誤った使用によって生じた問題が解決されることをCitrixは保証できません。レジストリエディターの使用は、お客様ご自身の責任において行ってください。編集する前に必ずレジストリをバックアップしてください。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- 値の名前: ExtraURLProtocols
- 値の型: REG_SZ
- 値のデータ: 必要なURLタイプをセミコロンで区切って指定します。URLのオーソリティ部分より前のすべてを含めます。例: `ftp://;mailto:;customtype1://;custometype2://`

URLの種類はWindowsクライアントにのみ追加できます。上記のレジストリ設定がないクライアントは、Citrixセッションへのリダイレクトを拒否します。クライアントには、指定されたURLの種類を処理するようにインストールおよび構成されたアプリケーションが必要です。

デフォルトのリダイレクトリストからURLタイプを削除するには、サーバーVDAで以下のレジストリキーと値を作成します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前: DisableServerFTA
- 値の型: DWORD
- 値のデータ: 1
- 値の名前: NoRedirectClasses
- 値の型: REG_MULTI_SZ
- 値のデータ: `http`、`https`、`rtsp`、`rtspu`、`pnm`、または`mms`のいずれかの値を組み合わせて指定します。複数の値を別々の行に入力します。例:

`http`

`https`

`rtsp`

特定のWebサイトのセットに対してホストからクライアントへのリダイレクトを有効にするには、サーバーVDAでレジストリキーと値を作成します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前: ValidSites
- 値の型: REG_MULTI_SZ
- 値のデータ: 完全修飾ドメイン名 (FQDN) の任意の組み合わせを指定します。複数のFQDNを別々の行に入力します。プロトコルなしでFQDNのみを含めます (`http://` または `https://`)。FQDNには、ワイルドカード文字としてアスタリスク (`*`) を左端の位置にのみ含めることができます。このワイルドカードは、RFC 6125のルールに準拠した単一レベルのドメインに一致します。例:

`www.exmaple.com`

`*.example.com`

> **注:**
>
> **ValidSites**キーを**DisableServerFTA**キーおよび**NoRedirectClasses**キーと組み合わせて使用することはできません。

サーバーVDAのデフォルトブラウザ構成

このセクションで参照されているホストからクライアントへのリダイレクトを有効にすると、サーバーVDA上の以前のデフォルトのブラウザー構成がすべて上書きされます。Web URLがリダイレクトされない場合、Citrix Launcherは、`command_backup` レジストリキーで構成されているブラウザーにURLを渡します。このキーはデフォルトでInternet Explorerを指していますが、別のブラウザーへのパスを含むように変更できます。詳しくは、レジストリで管理される機能の一覧にある「サーバーVDAのデフォルトのブラウザー構成」を参照してください。

ローカルアプリアクセスとURLリダイレクト

はじめに

ローカルアプリアクセスは、ローカルにインストールされたWindowsアプリケーションを、デスクトップを切り替えることなくホスト型デスクトップ環境にシームレスに統合します。ローカルアプリアクセスを使用すると、次のことが可能になります。

- 物理的なラップトップ、PC、またはその他のデバイスにローカルにインストールされているアプリケーションに、仮想デスクトップから直接アクセスできます。
- 柔軟なアプリケーション配信ソリューションを提供します。仮想化できない、またはIT部門が保守していないローカルアプリケーションをユーザーが持っている場合でも、それらのアプリケーションは仮想デスクトップにインストールされているかのように動作します。
- アプリケーションが仮想デスクトップとは別にホストされている場合のダブルホップ遅延を解消します。これを行うには、公開されたアプリケーションへのショートカットをユーザーのWindowsデバイスに配置します。
- 次のようなアプリケーションを使用します。
  - GoToMeetingなどのビデオ会議ソフトウェア。
  - まだ仮想化されていない特殊なアプリケーションやニッチなアプリケーション。
  - ユーザーデバイスからサーバーへ、そしてサーバーからユーザーデバイスへ大量のデータを転送する可能性のあるアプリケーションや周辺機器。たとえば、DVDバーナーやTVチューナーなど。

Citrix Virtual Apps and Desktops™では、ホスト型デスクトップセッションはURLリダイレクトを使用してローカルアプリアクセスアプリケーションを起動します。URLリダイレクトにより、アプリケーションは複数のURLアドレスで利用可能になります。デスクトップセッション内のブラウザーで埋め込みリンクを選択すると、ローカルブラウザー（ブラウザーのURLブロックリストに基づく）が起動します。ブロックリストにないURLに移動すると、そのURLはデスクトップセッションで再度開かれます。

URLリダイレクトはデスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。アプリケーションセッションで使用できる唯一のリダイレクト機能は、ホストからクライアントへのコンテンツリダイレクトであり、これはサーバーFTA（ファイルタイプ関連付け）リダイレクトの一種です。このFTAは、HTTP、HTTPS、RTSP、MMSなどの特定のプロトコルをクライアントにリダイレクトします。たとえば、HTTPで埋め込みリンクのみを開く場合、リンクはクライアントアプリケーションで直接開きます。URLブロックリストまたは許可リストのサポートはありません。

Local App Accessが有効になっている場合、ローカルで実行されているアプリケーション、ユーザーがホストするアプリケーションからのリンクとして、またはデスクトップ上のショートカットとしてユーザーに表示されるURLは、次のいずれかの方法でリダイレクトされます。

- ユーザーのコンピューターからホスト型デスクトップへ
- Citrix Virtual Apps™ and Desktopsサーバーからユーザーのコンピューターへ
- 起動された環境でレンダリングされる（リダイレクトされない）

特定のWebサイトからのコンテンツのリダイレクトパスを指定するには、Virtual Delivery AgentでURL許可リストとURLブロックリストを構成します。これらのリストには、URLリダイレクトポリシー設定を指定する複数文字列のレジストリキーが含まれています。詳しくは、ローカルアプリアクセス ポリシー設定を参照してください。

URLは、以下の例外を除き、VDAでレンダリングできます。

- 地域/ロケール情報 — msn.comやnews.google.comなど、ロケール情報を必要とするWebサイト（地域に基づいて国固有のページを開きます）。たとえば、VDAが英国のデータセンターからプロビジョニングされ、クライアントがインドから接続している場合、ユーザーはin.msn.comが表示されることを期待しますが、実際にはuk.msn.comが表示されます。
- マルチメディアコンテンツ — リッチメディアコンテンツを含むWebサイトは、クライアントデバイスでレンダリングされると、エンドユーザーにネイティブなエクスペリエンスを提供し、高遅延ネットワークでも帯域幅を節約します。この機能は、Silverlightなどの他のメディアタイプを含むサイトをリダイレクトします。このプロセスは安全な環境で行われます。つま

り、管理者が承認したURLはクライアントで実行され、残りのURLはVDAにリダイレクトされます。

URLリダイレクトに加えて、FTAリダイレクトを使用できます。FTAは、セッションでファイルが検出されたときにローカルアプリケーションを起動します。ローカルアプリが起動された場合、ローカルアプリはそのファイルを開くためにファイルへのアクセス権を持っている必要があります。したがって、ネットワーク共有上またはクライアントドライブ上（クライアントドライブマッピングを使用）にあるファイルのみをローカルアプリケーションを使用して開くことができます。たとえば、PDFファイルを開く際に、PDFリーダーがローカルアプリである場合、そのPDFリーダーを使用してファイルが開きます。ローカルアプリはファイルに直接アクセスできるため、ファイルを開くためにICA®を介したファイルのネットワーク転送は発生しません。

要件、考慮事項、および制限事項

WindowsマルチセッションOS用VDAおよびWindowsシングルセッションOS用VDAの有効なオペレーティングシステムで、ローカルアプリアクセスをサポートしています。ローカルアプリアクセスには、Citrix Workspaceアプリ for Windowsバージョン4.1（最小）が必要です。以下のブラウザーがサポートされています。

- Edge、最新バージョン
- Firefox、最新バージョンおよび延長サポートリリース
- Chrome、最新バージョン

ローカルアプリアクセスとURLリダイレクトを使用する際の以下の考慮事項と制限事項を確認してください。

- ローカルアプリアクセスは、すべてのモニターにまたがる全画面の仮想デスクトップ向けに設計されています。
    - ウィンドウモードで実行される仮想デスクトップ、またはすべてのモニターをカバーしない仮想デスクトップでローカルアプリアクセスを使用すると、ユーザーエクスペリエンスが混乱する可能性があります。
    - 複数モニター — 1つのモニターが最大化されると、そのセッションで起動されたすべてのアプリケーションのデフォルトデスクトップになります。このデフォルトは、後続のアプリケーションが通常別のモニターで起動される場合でも発生します。
    - この機能は1つのVDAをサポートします。複数の同時VDAとの統合はありません。
- 一部のアプリケーションは予期しない動作をし、ユーザーに影響を与える可能性があります。

- ドライブ文字は、仮想デスクトップのC:ドライブではなくローカルのC:ドライブのように表示されるため、ユーザーを混乱させる可能性があります。
- 仮想デスクトップで利用可能なプリンターは、ローカルアプリケーションでは利用できません。
- 昇格された権限を必要とするアプリケーションは、クライアントホスト型アプリケーションとして起動できません。
- シングルインスタンスアプリケーション（Windows Media Playerなど）に対する特別な処理はありません。
- ローカルアプリケーションは、ローカルマシンのWindowsテーマで表示されます。
- 全画面表示アプリケーションはサポートされていません。これには、PowerPointのスライドショーやデスクトップ全体を覆うフォトビューアなど、全画面で開くアプリケーションが含まれます。
- ローカルアプリアクセスは、ローカルアプリケーションのプロパティ（クライアントのデスクトップやスタートメニューのショートカットなど）をVDAにコピーします。ただし、ショートカットキーや読み取り専用属性などの他のプロパティはコピーしません。
- 重複するウィンドウの順序の処理方法をカスタマイズするアプリケーションは、予測できない結果をもたらす可能性があります。たとえば、一部のウィンドウが非表示になることがあります。
- ショートカットはサポートされていません。これには、マイコンピュータ、ごみ箱、コントロールパネル、ネットワークドライブのショートカット、フォルダーのショートカットが含まれます。
- 以下のファイルの種類とファイルはサポートされていません：カスタムファイルの種類、関連付けられたプログラムがないファイル、zipファイル、隠しファイル。
- タスクバーのグループ化は、32ビットと64ビットが混在するクライアントホスト型またはVDAアプリケーションではサポートされていません。つまり、32ビットのローカルアプリケーションと64ビットのVDAアプリケーションのグループ化はサポートされていません。
- COMを使用してアプリケーションを起動することはできません。たとえば、Officeアプリケーション内から埋め込みOfficeドキュメントをクリックした場合、プロセスの起動が検出されず、ローカルアプリケーションの統合が失敗します。

- ユーザーが別の仮想デスクトップセッション内から仮想デスクトップを起動するダブルホップシナリオはサポートされていません。
- URLリダイレクトは、明示的なURLのみをサポートします (ブラウザのアドレスバーに表示されるURL、またはブラウザ内ナビゲーションで見つかるURL。これはブラウザによって異なります)。

- URLリダイレクトは、デスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。
- VDAセッションのローカルデスクトップフォルダーでは、ユーザーがファイルを作成することはできません。
- ローカルで実行されているアプリケーションの複数のインスタンスは、仮想デスクトップ用に確立されたタスクバー設定に従って動作します。ただし、ローカルで実行されているアプリケーションへのショートカットは、それらのアプリケーションの実行中のインスタンスとグループ化されません。ホストされているアプリケーションの実行中のインスタンスや、ホストされているアプリケーションへのピン留めされたショートカットともグループ化されません。ユーザーは、タスクバーからローカルで実行されているアプリケーションのウィンドウのみを閉じることができます。ユーザーはローカルアプリケーションウィンドウをデスクトップのタスクバーとスタートメニューにピン留めできますが、これらのショートカットを使用するとアプリケーションが常に起動するとは限りません。
- **Allow Local App Access** ポリシー設定を **Enabled** に設定した場合、ブラウザコンテンツリダイレクトはサポートされません。デフォルトでは、Local App Access は禁止されています。

Windowsとの連携

Local App AccessのWindowsとの連携には、次の動作が含まれます。

- Windows 8およびWindows Server 2012のショートカットの動作
  - クライアントにインストールされているWindowsストアアプリケーションは、Local App Accessショートカットの一部として列挙されません。
  - 画像ファイルとビデオファイルは、デフォルトでWindowsストアアプリケーションを使用して開かれます。ただし、Local App AccessはWindowsストアアプリケーションを列挙し、デスクトップアプリケーションでショートカットを開きます。
- ローカルプログラム
  - Windows 7の場合、フォルダーはスタートメニューで利用できます。
  - Windows 8の場合、Local Programsは、ユーザーがスタート画面からカテゴリとして **すべてのアプリ** を選択した場合にのみ利用できます。すべてのサブフォルダーがLocal Programsに表示されるわけではありません。
- アプリケーション向けのWindows 8グラフィック機能
  - デスクトップアプリケーションはデスクトップ領域に制限され、スタート画面とWindows 8スタイルのアプリケーションによって覆われます。

  - ローカルアプリアクセスアプリケーションは、マルチモニターモードではデスクトップアプリケーションのように動作しません。マルチモニターモードでは、スタート画面とデスクトップが異なるモニターに表示されます。

- Windows 8とローカルアプリアクセスのURLリダイレクト

  - Windows 8のInternet Explorerではアドオンが有効になっていないため、URLリダイレクトを有効にするにはデスクトップ版Internet Explorerを使用してください。
  - Windows Server 2012では、Internet Explorerはデフォルトでアドオンを無効にします。URLリダイレクトを実装するには、Internet Explorerの拡張構成を無効にします。その後、Internet Explorerのオプションをリセットして再起動し、標準ユーザー向けにアドオンが有効になっていることを確認します。

ローカルアプリアクセスとURLリダイレクトの構成

Citrix Workspace™アプリでローカルアプリアクセスとURLリダイレクトを使用するには：

- ローカルクライアントマシンにCitrix Workspaceアプリをインストールします。Citrix Workspaceアプリのインストール中に両方の機能を有効にするか、グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にすることができます。
- **Allow Local App Access**ポリシー設定を**Enabled**に設定します。URLリダイレクトのURL許可リストおよびブロックリストポリシー設定も構成できます。詳しくは、「ローカルアプリアクセスのポリシー設定」を参照してください。

ローカルアプリアクセスとURLリダイレクトを有効にする

すべてのローカルアプリケーションでローカルアプリアクセスを有効にするには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**Policies**をクリックします。
2. アクションバーで、**Create Policy**をクリックします。
3. Create Policyウィンドウで、検索ボックスに「Allow Local App Access」と入力し、**Select**をクリックします。
4. Edit Settingウィンドウで、**Allowed**を選択します。デフォルトでは、**Allow local app access**ポリシーは禁止されています。この設定が許可されている場合、VDAは公開アプリケーションとローカルアプリアクセスのショートカットをセッションで有効にするかどうかをエンドユーザーが決定できるようにします。（この設定が禁止されている場合、公開アプリケーションとローカルアプリアクセスのショートカットはどちらもVDAでは機能しません。）このポリシー設定は、マシン全体とURLリダイレクトポリシーに適用されます。

5. Create Policyウィンドウで、検索ボックスに「URL redirection allow list」と入力し、**Select**をクリックします。URLリダイレクト許可リストは、リモートセッションのデフォルトブラウザーで開くURLを指定します。
6. 「設定の編集」ウィンドウで、URLを追加するために**追加**をクリックし、その後、**OK**をクリックします。
7. 「ポリシーの作成」ウィンドウで、検索ボックスに「URLリダイレクトブロックリスト」と入力し、その後、**選択**をクリックします。URLリダイレクトブロックリストは、エンドポイントで実行されているデフォルトのブラウザにリダイレクトされるURLを指定します。
8. 「設定の編集」ウィンドウで、URLを追加するために**追加**をクリックし、その後、**OK**をクリックします。
9. 「設定」ページで、**次へ**をクリックします。
10. 「ユーザーとマシン」ページで、該当するデリバリーグループにポリシーを割り当て、その後、**次へ**をクリックします。
11. 「概要」ページで、設定を確認し、その後、**完了**をクリックします。

Citrix Workspaceアプリのインストール中にすべてのローカルアプリケーションでURLリダイレクトを有効にするには、次の手順に従います。

1. マシン上のすべてのユーザーに対してCitrix Workspaceアプリをインストールするときに、URLリダイレクトを有効にします。これにより、URLリダイレクトに必要なブラウザーアドオンも登録されます。
2. コマンドプロンプトから、以下のいずれかのオプションを使用してCitrix Workspaceアプリをインストールするための適切なコマンドを実行します。
   - CitrixReceiver.exeの場合は、`/ALLOW_CLIENTHOSTEDAPPSURL=1`を使用します。
   - CitrixReceiverWeb.exeの場合は、`/ALLOW_CLIENTHOSTEDAPPSURL=1`を使用します。

グループポリシーエディターを使用してローカルアプリアクセス テンプレートを有効にする

> **注:**
>
> - グループポリシーエディターを使用してローカルアプリアクセス テンプレートを有効にする前に、receiver.admx/admlテンプレートファイルをローカルGPOに追加します。

- Windows向けCitrix Workspaceアプリのテンプレートファイルは、CitrixBase.admx/CitrixBase.admlを%systemroot%\policyDefinitionsフォルダーに追加した場合のみ、ローカルGPOの**管理用テンプレート > Citrixコンポーネント > Citrix Workspace**フォルダーにあります。

グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にするには、次の手順に従います。

1. **gpedit.msc**を実行します。
2. **コンピューターの構成 > 管理用テンプレート > 従来の管理用テンプレート (ADM) > Citrix Components > Citrix Workspace > ユーザーエクスペリエンス**に移動します。
3. **ローカルアプリアクセス設定**をクリックします。
4. **有効**を選択し、次に**URLリダイレクトを許可**を選択します。URLリダイレクトの場合、このドキュメントの後半にある「*ブラウザアドオンの登録*」セクションで説明されているコマンドラインを使用してブラウザアドオンを登録します。

公開アプリケーションのみにアクセスを提供する

レジストリエディターまたはPowerShell SDKを使用して、公開アプリケーションへのアクセスを提供できます。

レジストリエディターについては、レジストリを介して管理される機能のリストにある「公開アプリケーションのローカルアプリアクセス」を参照してください。

PowerShell SDKを使用するには：

1. Delivery Controller™が実行されているマシンでPowerShellを開きます。
2. 次のコマンドを入力します: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`。

クラウドサービス展開で**ローカルアプリアクセスアプリケーションの追加**にアクセスするには、Citrix DaaS Remote PowerShell SDKを使用します。詳しくは、「Citrix DaaS Remote PowerShell SDK」を参照してください。

1. インストーラーをダウンロードします:

   `<https://download.apps.cloud.com/CitrixPoshSdk.exe>`
2. これらのコマンドを実行します:

a. `asnp citrix.*`.

b. `Get-XdAuthentication`

3. 次のコマンドを入力します: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`。

該当する前の手順を完了したら、以下の手順に従って続行します。

1. Web Studioにサインインし、左側のペインで**アプリケーション**を選択します。
2. 上部中央ペインで、空白領域を右クリックし、コンテキストメニューから**Add Local App Access Application**を選択します。アクションバーの**Add Local App Access Application**をクリックすることもできます。アクションバーにAdd Local App Access Applicationオプションを表示するには、**Refresh**をクリックします。
3. ローカルアプリアクセスアプリケーションを公開します。

   - ローカルアプリケーションアクセスウィザードが起動し、はじめにページが表示されます。このページは、今後のウィザードの起動時に表示しないように設定できます。
   - ウィザードは、以下で説明するグループ、場所、識別、配信、および概要の各ページを案内します。各ページの作業が完了したら、概要ページに到達するまで**次へ**をクリックします。
   - グループページで、新しいアプリケーションを追加するデリバリーグループを1つ以上選択し、**次へ**をクリックします。
   - ページで、ユーザーのローカルマシン上のアプリケーションの完全な実行可能パスを入力し、アプリケーションが配置されているフォルダーへのパスを入力します。Citrixでは、システム環境変数パスを使用することをお勧めします。例: %ProgramFiles(x86)%\Internet Explorer\iexplore.exe。
   - 識別ページで、デフォルト値を受け入れるか、必要な情報を入力してから**次へ**をクリックします。
   - ページで、このアプリケーションをユーザーに配信する方法を構成し、**次へ**をクリックします。選択したアプリケーションのアイコンを指定できます。また、仮想デスクトップ上のローカルアプリケーションへのショートカットを、スタートメニュー、デスクトップ、またはその両方に表示するかどうかを指定できます。
   - 概要ページで設定を確認し、**完了**をクリックしてローカルアプリケーションアクセスウィザードを終了します。

ブラウザアドオンを登録する

> **注:**
>
> URLリダイレクトに必要なブラウザアドオンは、コマンドラインから/ALLOW_CLIENTHOSTEDAPPSURL=1オプションを使用してCitrix Workspaceアプリをインストールする際に自動的に登録されます。

> 次のコマンドを使用して、1つまたはすべてのアドオンを登録および登録解除できます。

- クライアントデバイスにアドオンを登録するには: \<*client-installation-folder*>\redirector.exe /reg\<*browser*>
- クライアントデバイスのアドオンを登録解除するには: \<*client-installation-folder*>\redirector.exe /unreg\<*browser*>
- VDAにアドオンを登録するには: \<*VDAinstallation-folder*>\VDARedirector.exe /reg\<*browser*>
- VDAのアドオンを登録解除するには: \<*VDAinstallation-folder*>\VDARedirector.exe /unreg\<*browser*>

ここで、\<*browser*> はInternet Explorer、Firefox、Chrome、またはAllです。

たとえば、次のコマンドは、Citrix Workspaceアプリを実行しているデバイスにInternet Explorerアドオンを登録します。

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

次のコマンドは、WindowsマルチセッションOS VDAにすべてのアドオンを登録します。

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

ブラウザ間のURLインターセプト

- デフォルトでは、Internet Explorerは指定されたURLをリダイレクトします。URLがブロックリストにない場合でも、ブラウザまたはWebサイトが別のURLにリダイレクトすると、最終的なURLはリダイレクトされません。ブロックリストにある場合でもリダイレクトされません。

URLリダイレクトが正しく機能するようにするには、ブラウザからプロンプトが表示されたときにアドオンを有効にします。インターネットオプションを使用しているアドオン、またはプロンプトに表示されるアドオンが無効になっている場合、URLリダイレクトは正しく機能しません。

- Firefoxのアドオンは常にURLをリダイレクトします。

アドオンがインストールされると、Firefoxは新しいタブページにアドオンをインストールすることを許可するか、または防止するかを尋ねます。機能が動作するようにアドオンを許可してください。

- Chromeアドオンは、入力されたURLではなく、常にナビゲートされた最終URLをリダイレクトします。

拡張機能は外部からインストールされています。拡張機能を無効にすると、ChromeでURLリダイレクト機能が動作しません。シークレットモードでURLリダイレクトが必要な場合は、ブラウザ設定でそのモードでの拡張機能の実行を許可してください。

ログオフ時および切断時のローカルアプリケーションの動作を構成する

> **注:**
>
> これらの手順に従って設定を構成しない場合、デフォルトでは、ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは実行を継続します。再接続後、ローカルアプリケーションが仮想デスクトップで利用可能な場合、それらは再統合されます。

ログオフ時および切断時のローカルアプリケーションの動作を構成するには、レジストリを介して管理される機能のリストにあるログオフ時および切断時のローカルアプリケーションの動作を参照してください。

印刷

効率的な印刷管理は、Citrix Virtual Apps and Desktops™ (CVAD) 環境における生産的で効率的なIT運用の要です。ユーザーは印刷リソースへのシームレスで信頼性の高いアクセスを必要とし、管理者は印刷インフラストラクチャを構成、管理、保護、トラブルシューティングするための堅牢なツールを必要とします。

このドキュメントは、既存のナレッジベースを刷新し、IT管理者にCVAD印刷のあらゆる側面を徹底的に理解させることを目的とした、包括的な専門家レベルのガイドとして機能します。

印刷は、多くのビジネスワークフローにとって依然として基本的な要件です。Citrix Virtual Apps™ and Desktops (CVAD) 環境では、仮想セッションから物理デバイスへの印刷要求を効率的に管理することは、ユーザーのセッションと物理プリンターハードウェアとの分離により、固有の課題を提示します。

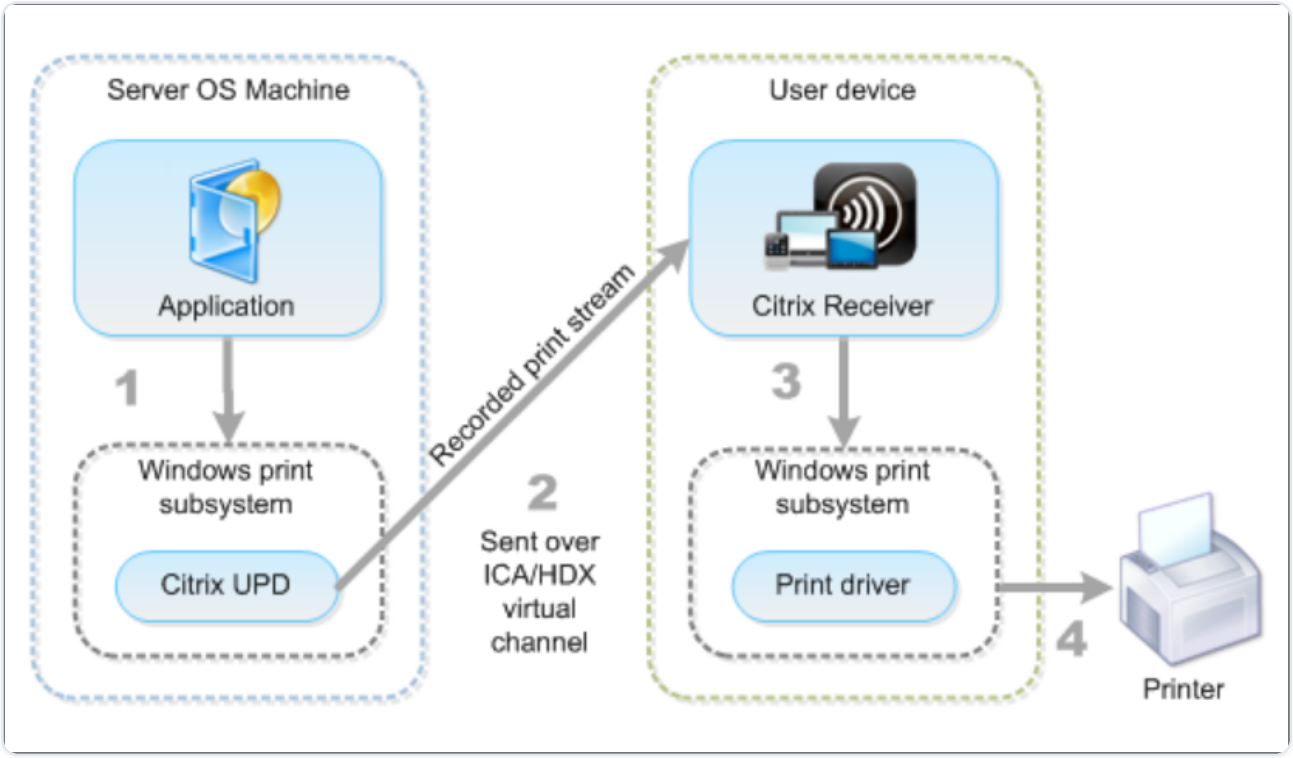
CVADは、このギャップを埋めるために設計された包括的なテクノロジーとポリシーのスイートを提供し、最適なパフォーマンスと管理の簡素化を目指しながら、多様なプリンタータイプ、ネットワーク条件、ユーザー要件に対応する柔軟性を提供します。

Citrix Universal™ プリントドライバー (UPD)

Citrix Universal Print Driver (UPD) は単一のドライバーではなく、サーバー (VDA) とクライアント (Workspace アプリがインストールされたエンドポイント) の両方にコンポーネントを含む技術です。

- **サーバーコンポーネント:** VDA とともにインストールされ、「Citrix Universal Printer」（EMF 形式を使用）や「Citrix XPS Universal Printer」（XPS 形式を使用）などの実際の汎用プリントドライバーが含まれます。PDF および PS 形式のサポートも含まれます。その役割は、VDA 上で実行されているアプリケーションによって生成された印刷出力を、デバイスに依存しない形式でキャプチャすることです。
- **クライアントコンポーネント:** Citrix Workspace™ アプリのインストールに含まれており、このコンポーネントは VDA から送信された印刷ストリームを受信します。その後、エンドポイントデバイス上のローカル Windows 印刷サブシステムと連携し、ターゲットプリンター用にローカルにインストールされている適切なデバイス固有のドライバーを使用して印刷ジョブをレンダリングします。

次の図は、Universal Print ドライバーのコンポーネントと、デバイスにローカルに接続されたプリンターの一般的なワークフローを示しています -



UPD の主な目標は、Citrix® 環境内でのプリンタードライバー管理を簡素化することです。VDA 上で組み込みドライバーを使用することで、管理者は、不安定性や競合の一般的な原因となる、潜在的に数百もの異なるメーカー固有のドライバーをインストールおよび保守する手間を省くことができます。UPD は、幅広いプリンターとの互換性を目指し、仮想セッションとクライアントの印刷機能との間にユニバーサルなインターフェースを提供します。

サポートされている形式

UPD テクノロジーは、いくつかの印刷データ形式をサポートしており、印刷ジョブの処理方法とレンダリング方法に柔軟性をもたらします。

- **EMF (Enhanced Metafile Format):** 「Citrix Universal Printer」ドライバーで使用されるデフォルトの形式です。32ビットの Windows ネイティブベクター形式です。EMF を使用した印刷は一般的に効率的ですが、レンダリングには通常 Windows ベースのクライアントエンドポイントが必要です。
- **XPS (XML Paper Specification):** 「Citrix XPS Universal Printer」ドライバーで使用されます。XPS は Microsoft が開発した XML ベースのページ記述言語であり、PDF と概念が似ており、プラットフォームに依存しないように設計されています。
- **PS (PostScript):** Adobe が開発したページ記述言語で、複雑なグラフィックやタイポグラフィの処理能力で知られており、出版業界や様々なプリンター、複合機でよく使用されます。Linux クライアントは、UPD で PostScript 印刷をよく利用します。

- **PDF:** PDF は、ドキュメント交換に広く使用されているオープン標準です。テキスト、フォント、グラフィック、および表示に必要なその他の情報を含む、固定レイアウトのフラットドキュメントの完全な記述をカプセル化します。プラットフォームに依存しないように設計されており、異なるシステムやアプリケーション間でドキュメントの忠実性を維持するのに理想的です。

UPD を使用すると、いくつかの潜在的な利点があります。

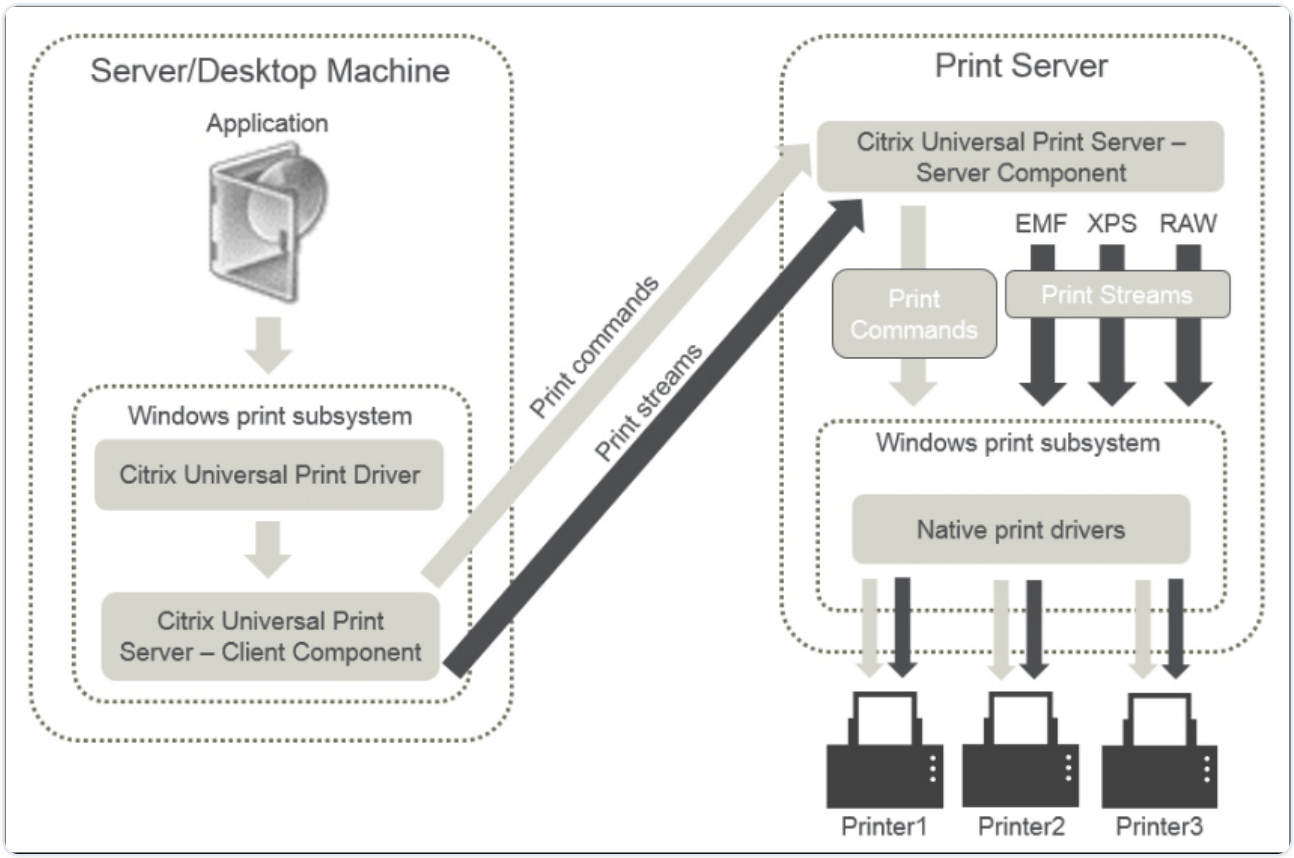
- **ドライバー管理の削減:** VDA イメージに必要なドライバーの数を大幅に削減し、イメージの作成とメンテナンスを簡素化します。
- **安定性の向上:** ドライバーが少ないほど、潜在的な競合が少なくなり、ドライバー関連のスプーラークラッシュやシステム不安定性のリスクが低減されます。
- **印刷ジョブの最適化:** 特定のUPD形式、特にEMFは、ネイティブドライバーと比較して、印刷ジョブのサイズが小さくなることがあります。
- **高度な機能のサポート:** クライアント上のネイティブドライバーが、Microsoftの標準的なPrint Capabilityテクノロジーを通じてこれらの機能を公開している場合、EMFおよびXPS UPDコンポーネントは、高度な印刷機能（例：ステープル、トレイ選択）をサポートできます。

構成

シトリックス ユニバーサル™ プリントサーバー (UPS)

UPS は、ネットワーク印刷を最適化および管理するために設計されたオプションの Citrix® コンポーネントです。これは次の2つの部分で構成されています。

- **UPServer** コンポーネントは、ネットワーク内の1つ以上のWindowsプリントサーバーにインストールされます。
- **UPClient** コンポーネントは、VDA インストールの一部です。ポリシーによって有効にされると、VDA は UPServer と通信してネットワークプリンターへの接続を確立し、通常は Citrix Universal Print Driver (UPD) を活用します。



UPS には、特に WAN リンクを介したネットワーク印刷や大規模な環境において、いくつかの利点があります。

- ネットワークの最適化: VDA と UPServer 間で送信される印刷データは最適化および圧縮され、帯域幅の消費を削減します。これは特に WAN 接続において重要です。
- 集中型ドライバー管理: ネットワークプリンターに Citrix UPD を活用できるため、VDA に多数のネイティブプリンタードライバーをインストールおよび管理する必要がなくなります。
- 高可用性: 複数の UPServer 間での負荷分散と、サーバーが利用できなくなった場合の自動フェイルオーバーをサポートします。

要件

- Microsoft Visual C++ 2015–2022 再頒布可能パッケージ
- Microsoft .NET Framework 4.8 (最低バージョン)
- UPServer の OS 要件
  - ウィンドウズ サーバー 2025
  - ウィンドウズ サーバー 2022
  - ウィンドウズ サーバー 2019

構成/セットアップ手順

この機能はデフォルトで無効になっています。関連する設定と構成は、「Universal Print Server」テンプレートにあります。このテンプレートのポリシー設定を使用して、Universal Print server のエクスペリエンスをさらにカスタマイズおよび最適化できます。

有効化設定に加えて、いくつかのポリシー設定で UPS の動作を微調整できます。

- 通信用のポート構成 (HTTP/SOAP、CGP、およびそれらの SSL/TLS 同等物)。
- 印刷ストリームの入力帯域幅制限。
- 負荷分散用のUPServerのリスト。 フェイルオーバー検出のサービス停止しきい値。
- Webサービス接続のタイムアウト。
- セキュアな通信のためのSSL/TLS構成設定。

詳細については、Citrix UPSポリシー設定を参照してください。

ベストプラクティス

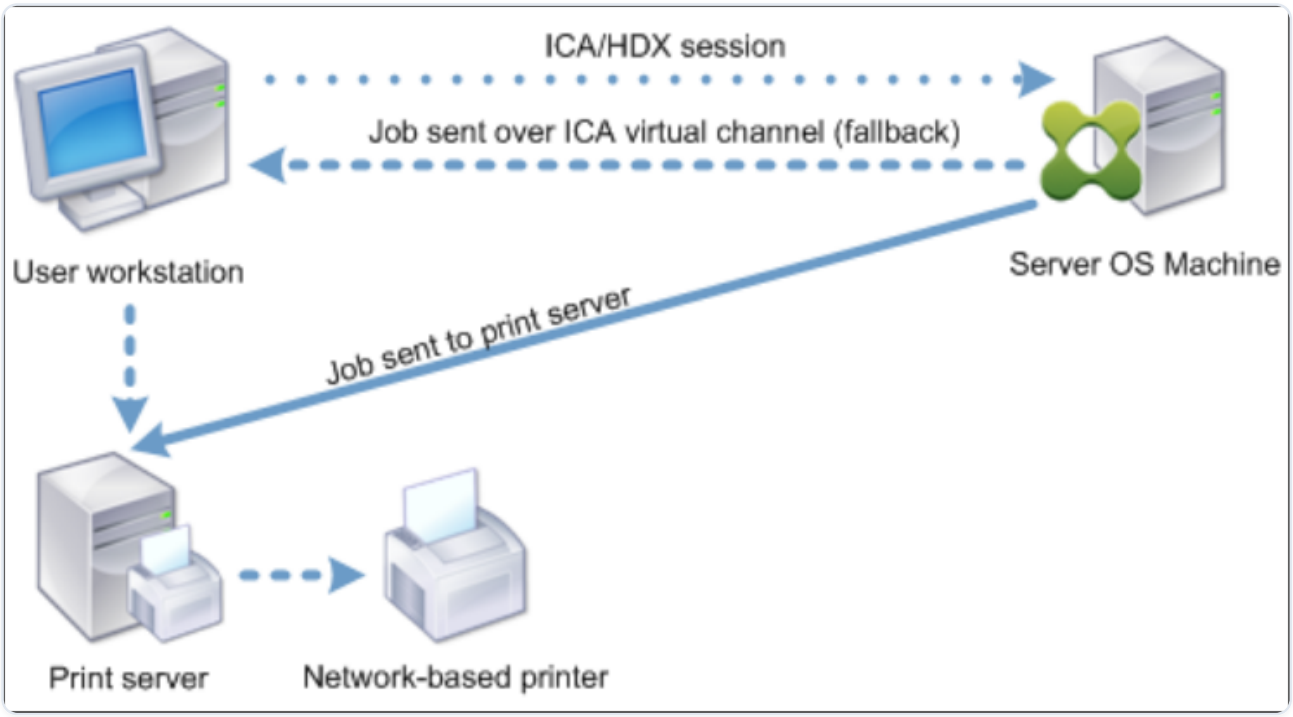
- WANリンクを介したネットワーク印刷にUPSを使用して、パフォーマンスを最適化します。
- Citrix Universal Print Driver (UPD) を利用して、VDAでのドライバー管理を削減します。
- 高可用性のために、複数のUPServer間で負荷分散を構成します。

ユースケース

Citrix は、WAN リンクを伴うリモートプリントサーバーのシナリオにおいて、UPS を明示的に推奨しています。また、VDA ドライバーのフットプリントを最小限に抑えたい、ネットワーク印刷のパフォーマンスを向上させたい、ネットワーク印刷の高可用性を提供したい、またはネットワークロケーションに基づいて近接印刷を実装したい環境にも最適です。ネットワークプリンターに直接接続できないシンクライアントは、VDA を介して UPS を活用できます。

ネットワークプリンター

ここでは、印刷ジョブはVDAからネットワーク経由でネットワークプリントサーバー（標準のWindowsプリントサーバーまたはCitrix Universal™ Print Serverのいずれか）に直接送信されます。この経路は、VDAと同じローカルエリアネットワーク（LAN）上にあるプリンターの場合、一般的に高速です。これは、直接接続が有効になっている場合のネットワークプリンターのデフォルトの経路です。公開されたアプリケーションまたはデスクトップがプリントサーバーにアクセスできない場合、またはネイティブプリンタードライバーがマルチセッションOSマシンにインストールされていない場合、印刷ジョブはICA接続経由でルーティングされるようにフォールバックします。



要件

- 必要なプリンタードライバーは、ネットワークプリンターをホストするプリントサーバーの種類によって異なります。
  - プリンターが標準のWindowsプリントサーバーでホストされている場合、対応するネイティブプリンタードライバーがVDAにインストールされている必要があります。
  - プリンターがCitrix Universal Print Server (UPS) でホストされている場合、接続にはネイティブドライバーまたはCitrix UPDのいずれかを使用できます。
- VDAからプリントサーバーへのネットワーク接続。
- ログインしているユーザーに対する適切な権限。

ネットワークプリンターの接続と構成に関するガイダンス（ポリシー設定）

- UNCパス（例: “\\PrintServer\PrinterName”）経由でプリンターを接続します。
- **セッションプリンター:** この方法の主要なポリシーです。管理者はUNCパスを入力するか、ネットワークを参照してプリンターを追加します。特定のユーザー、グループ、クライアントIPなどを対象とするフィルターをポリシーに適用できます。
- **プリンター割り当て:** 複数のユーザーまたはデバイスに多数のプリンターを同時に割り当てるのに役立つ代替ポリシーです。これにより、セッションプリンターと、それらの割り当てのデフォルトプリンターの両方を設定できます。

ベストプラクティス（ネットワークプリンターへの直接接続を許可）

- ルーティング（VDAからサーバーへの直接接続、またはクライアント/ICA経由）には、「ネットワークプリンターへの直接接続」ポリシーを検討してください。
    - 有効にすると（デフォルト設定）、LAN経由での印刷パフォーマンスは最適になります。このシナリオでの印刷トラフィックは圧縮されません。
    - VDAとプリントサーバーが同じネットワークにない場合（WANシナリオ）は、このポリシー設定を無効にしてください。これにより、印刷トラフィックはクライアントエンドポイントを経由し、ICA®圧縮を利用するようになりますが、遅延が発生します。

直接接続を有効にすると、LANパフォーマンスが向上しますが、VDAとプリントサーバー間のネットワークトラフィックは圧縮されません。無効にすると、トラフィックはクライアント経路を経由し、ICA圧縮を利用するようになります。これはWANシナリオに有利ですが、遅延が追加されます。

ユースケース

仮想セッションから共有の部門プリンターまたはオフィスプリンターに直接アクセスする。VDAにネイティブドライバーがインストールされている必要があります。

制限事項

不利なネットワーク条件（WAN）では、印刷パフォーマンスが低下します。さらに、ドライバー管理はIT管理者にとって大きな負担となります。

トラブルシューティング

体系的なアプローチ

複雑なCitrix Virtual Apps and Desktops™ (CVAD)環境での印刷問題のトラブルシューティングには、当てずっぽうではなく、体系的なアプローチが必要です。推奨されるプロセスは次のとおりです。

1. **症状の特定:** 問題を明確に定義します (例: プリンターが表示されない、ジョブが停止する、出力が間違っている、印刷が遅い)。
2. **範囲の特定:** 誰が影響を受けているか (1人のユーザー、複数のユーザー、特定のアプリケーション)、どのプリンターが関係しているか、およびどのVDAまたはクライアントデバイスで問題が発生しているかを判断します。

3. **基本事項の確認:** ネットワーク接続 (VDAからプリントサーバー、クライアントからVDA) を確認し、プリンターがオンラインであり、Citrix® の外部で機能していることを確認し、クライアントからのローカル印刷 (リダイレクトの問題の場合) を確認します。
4. **ポリシーの確認:** Citrix Group Policy Modelingウィザードなどのツールを使用するか、VDAで適用されているポリシー設定を確認して、影響を受けるユーザー/セッションに適用されている関連するCitrixポリシー設定を調べます。ポリシー設定が意図どおりに構成されており、明らかな競合がないことを確認します。
5. **ログの調査:** VDA、クライアントデバイス、およびプリントサーバー (該当する場合) のWindowsイベントログ (アプリケーションログ、システムログ、PrintServiceログ) を確認します。有効になっている場合は、Citrix固有のログを確認します。3
6. **コンポーネントのテスト:** 問題を特定のコンポーネントに分離することを試みます – 別のアプリケーションから印刷を試す、別のプリンターを試す、汎用ドライバー (UPDやMicrosoft XPS Document Writerなど) でテストする、Print SpoolerサービスとCitrix Print Managerサービスのステータスを確認します。
7. **リソースの参照:** 製品ドキュメント、サポート記事、コミュニティフォーラムを活用し、既知の問題と解決策を探します。

一般的な問題と解決策

現場で報告されている一般的な印刷問題と推奨されるトラブルシューティング手順の一部を以下に示します。

- **プリンターの自動作成の失敗 / セッションにプリンターが表示されない:**
    - **考えられる原因:** クライアントプリンターリダイレクトポリシーが無効になっている; クライアントプリンターの自動作成ポリシーが「なし」に設定されているか、誤ってフィルターされている; クライアントデバイスのプリントスプーラーの問題; Workspaceアプリの問題; クライアントとVDA間のネットワーク接続の問題; Citrix Print Managerサービス (CpSvc.exe) がVDAで実行されていないかクラッシュしている; VDAに必要なプリンタードライバーがない (ネイティブドライバーが必要な場合); Citrixポリシーがセッションに正しく適用されていない。
    - **トラブルシューティング手順:**
        a. クライアントプリンターリダイレクトポリシーが「許可」されており、ユーザー/セッションに対してクライアントプリンターの自動作成が正しく構成されていることを確認します。
        b. VDA上のCpSvc.exeサービスのステータスを確認します。必要に応じて再起動します。

c. VDAとクライアントの両方でWindows Print Spoolerサービスのステータスを確認します。必要に応じて再起動します。
d. 基本的なネットワーク接続を確認します。
e. クライアントデバイスでローカルに印刷をテストします。
f. 互換性のあるWorkspaceアプリのバージョンがインストールされていることを確認します。
g. CpSvcまたはプリンター作成に関連するエラーがないか、VDAイベントログを確認します。
h. VDAでポリシーの更新を強制します (gpupdate /force)。
i. 適用されているポリシーをVDAで確認し、期待される設定が存在することを確認します。
j. ネイティブドライバーが必要な場合は、VDAにインストールされていることを確認します。
k. VDAのローカル/グループポリシーでRDS/ターミナルサーバーのプリンターリダイレクト設定を確認します。
l. VDAレジストリ内の孤立したプリンターエントリを探してクリーンアップします。

- **Print Spoolerのクラッシュ / サービスが応答しない (VDAまたはプリントサーバー上):**
  - **潜在的な原因:** 欠陥のある、または互換性のないプリンタードライバー (多くの場合サードパーティ製); キュー内の破損した印刷ジョブ; ドライバーの競合; システムリソースの不足。
  - **トラブルシューティングの手順:**
    a. Windows イベントログを使用して、障害のあるプロセス/モジュールを特定します (アプリケーションログには、スプーラーのクラッシュが頻繁に表示されます)。
    b. Print Spooler サービスの再起動を試みます。
    c. 再起動に失敗した場合、または問題が繰り返される場合は、印刷キューを手動でクリアしてみてください (スプーラーサービスを停止し、C:\Windows\System32\spool\PRINTERS 内のファイルを削除し、スプーラーサービスを開始します)。
    d. 問題のあるプリンタードライバーを特定して削除します。完全に削除するには、レジストリの編集が必要になる場合があります。
    e. Citrix UPDまたは汎用Microsoftドライバーでテストします。
    f. レジストリ内の孤立したプリントプロセッサを確認し、クリーンアップします。

- **ポリシーの競合 / 設定の無視:**
  - **考えられる原因:** GPO設定がCitrixポリシーを上書きしている。Citrixポリシーの優先順位またはフィルターが競合している。ポリシー処理中にエラーが発生している。
  - **トラブルシューティングの手順:**
    a. Citrixグループポリシーモデリングウィザードを使用して、影響を受けるユーザー/VDAに対するポリシー適用をシミュレートします。
    b. ポリシーフィルター（ユーザーグループ、クライアントIPなど）が正しいことを確認します。
    c. Studio/Web Studioでポリシーの優先順位を確認します。
    d. Citrixポリシーの問題を特定するために、VDAのOUでGPOの継承を一時的にブロックします。
    e. VDA上のポリシー処理結果を調べます（例: gpresult /h report.htmlを使用）。
    f. ユーザー/VDAに適用されるポリシーセットを簡素化し、競合を見つけるためにポリシーを段階的に追加し直します。
- **ドライバーの問題（全般 - 互換性、破損、マッピング）:**
  - **考えられる原因:** ドライバーがVDA OSまたはCitrixバージョンと互換性がない。ドライバーのインストールが破損している。ポリシーで必要なドライバーがVDAにない。複数のドライバー間の競合。プリンタードライバーマッピングポリシーの設定が正しくない。
  - **トラブルシューティングの手順：**
    a. Citrix UPDを使用して印刷を試行します（ユニバーサルプリンタードライバー使用ポリシーを設定します）。
    b. 適用されたポリシーに基づいて、正しいドライバー（ネイティブまたはUPD）が選択されていることを確認します。
    c. 必要なネイティブドライバーがVDAに正しくインストールされていることを確認します（使用する場合）。
    d. ドライバーがCVADおよびVDA OSバージョンと互換性があるか、ベンダーのドキュメントを確認します。
    e. 問題のあるドライバーをクリーンに再インストールします（アンインストール、再起動、インストール）。
    f. プリンタードライバーマッピングポリシーのルールを慎重に確認し、テストします。
    g. VDAにインストールされているドライバーの数を最小限に抑えます。

- **印刷速度の低下 / パフォーマンスの問題：**
  - **考えられる原因:** ネットワークの輻輳または高遅延（特にWAN）。大規模で複雑な印刷ジョブ（高解像度グラフィックなど）。非効率なプリンタードライバー。印刷最適化（圧縮、キャッシュ）が無効になっているか、誤って設定されている。非効率なルーティング（低速WAN経由の直接接続など）。
  - **トラブルシューティングの手順：**
    a. VDA、クライアント、およびプリントサーバー間のネットワークパスとパフォーマンスを分析します。
    b. 印刷用のCitrix帯域幅制限ポリシーを設定します。
    c. ユニバーサル印刷ポリシーを介して、UPD最適化（画像圧縮、フォント/画像キャッシュ）を有効にして構成します。
    d. WANリンクの場合、圧縮されたICA®チャネル経由でトラフィックを強制するために、「印刷サーバーへの直接接続」ポリシーを無効にします。
    e. UPSを使用している場合は、ネットワークに最適に構成されていることを確認してください。
    f. 印刷ジョブ自体を分析し、可能であれば解像度または複雑さを軽減します。
    g. 別のドライバー（例：UPDとネイティブ）でテストします。
- **出力の誤り（文字の欠落、書式設定エラー、向きの誤り）：**
  - **考えられる原因：** ドキュメント/アプリケーションに必要なVDA上のフォントの欠落。不適切なフォント置換。プリンタードライバーの非互換性。特定のUPD形式（例：EMFとXPS）に関する問題。アプリケーションのバグ。ローカルクライアントプリンターで有効になっている高度な印刷機能との競合。
  - **トラブルシューティングの手順:**
    a. 必要なすべてのフォントがVDAにインストールされていることを確認します。
    b. ユニバーサルドライバーの優先ポリシーの順序を変更してみてください（例：EMFの前にXPSを試す）。
    c. 別のアプリケーションから同じドキュメントを印刷してテストします。
    d. 別の物理プリンターまたは仮想プリンター（例：Microsoft XPS Document Writer）に印刷してテストします。
    e. 別のプリンタードライバー（UPDとネイティブ、または異なるネイティブバージョン）を使用してみてください。

f. アプリケーションの印刷設定とページ設定を確認します。

g. クライアントデバイスのローカルプリンターのプロパティで「詳細な印刷機能」を無効にします。

h. ユーザー設定とポリシーで印刷の向きの設定を確認します。

- **Citrix Print Manager Service (CpSvc.exe) のクラッシュまたは応答停止:**
  - **考えられる原因:** 応答しないプリンタードライバーがレジストリに孤立したオブジェクトを残している。印刷に関連するCitrixポリシーデータが破損している。システムリソースの競合。
  - **トラブルシューティングの手順:**

    a. VDAレジストリから孤立したプリンターおよび印刷プロセッサのエントリをクリーンアップする手順に従います。まずPrint SpoolerサービスとCpSvcサービスを停止する必要があります。

    b. 問題のあるプリンタードライバーを特定して削除します。

    c. VDA上のCitrixポリシーキャッシュフォルダー/レジストリキーをクリーンアップし、ポリシーの強制更新を検討してください。

    d. VDAのリソース使用量 (CPU、メモリ) を監視します。

    e. CpSvcサービスとPrint Spoolerサービスを再起動します。

- **PDFプリンターの問題:**
  - **考えられる原因:** PDFユニバーサルプリンターの自動作成ポリシーが無効になっている。VDAまたはWorkspaceアプリのバージョンが互換性がない。クライアントエンドポイントにPDFビューアーがインストールされていない。サポートされていないブラウザーが使用されている (例: Edge) またはHTML5構成エラー (CSPヘッダー、config.js)。
  - **トラブルシューティングの手順:**

    a. PDFユニバーサルプリンターの自動作成ポリシーが有効になっており、適用されていることを確認します。

    b. VDAとWorkspaceアプリが最小バージョン要件を満たしていることを確認します。

    c. サポートされているPDFビューアー (例: Adobe Reader、Chrome) がクライアントにインストールされ、デフォルトとして設定されていることを確認します。

    d. HTML5 Workspaceアプリを使用している場合は、ブラウザの互換性を確認し、configuration.jsとCSPヘッダーの設定を確認します。

    e. ポリシー変更後にCitrixセッションを再起動します。

基本的なエンドユーザーのトラブルシューティング

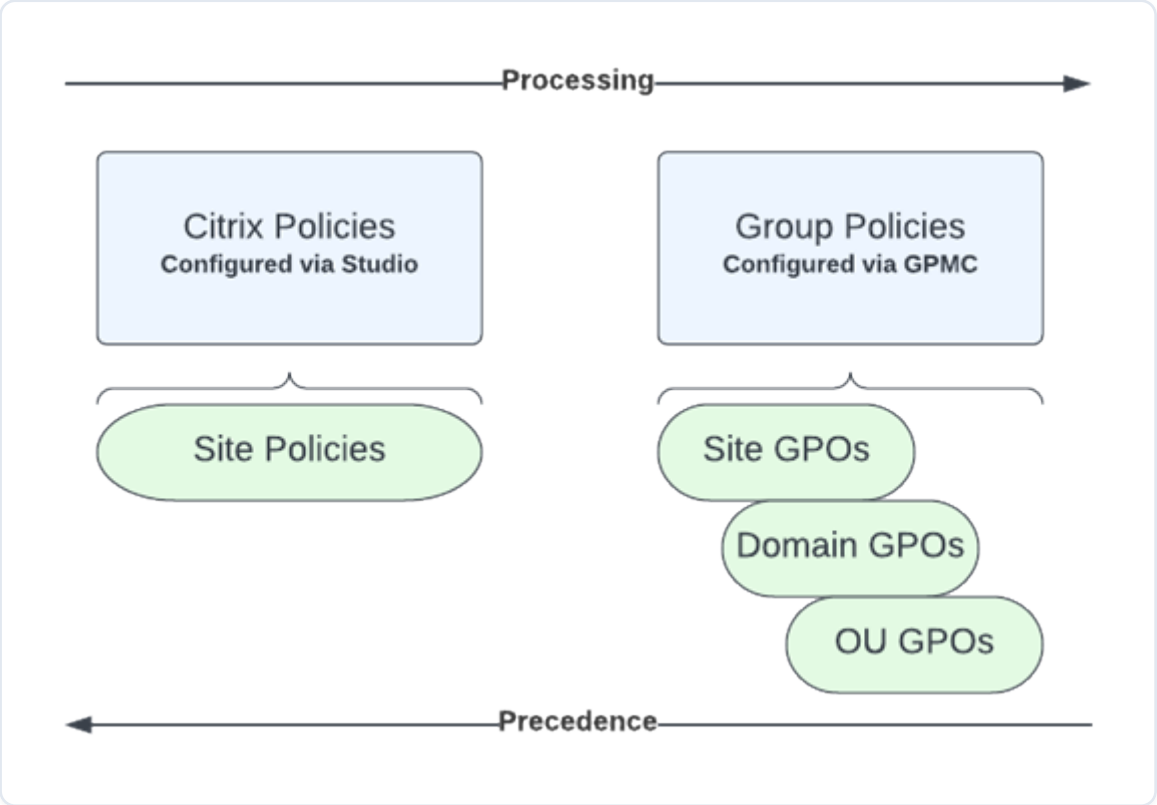
組織のポリシーで許可されている場合、簡単な印刷の問題を経験しているユーザーは、IT部門にエスカレートする前に、基本的な手順で問題を解決できる場合があります。

- HDX™セッションから完全にログオフし、再度ログインします。
- エンドポイントデバイス上のローカルプリンターのステータスを確認します (オンラインであること、一時停止されていないこと、エラーがないことを確認してください)。
- ローカルのエンドポイントデバイスを再起動します。

ポリシー

ポリシーは、ユーザー、デバイス、または接続タイプのグループに対して、セッション、帯域幅、セキュリティがどのように管理されるかを定義する設定の集合体です。

ポリシー設定は、物理マシン、仮想マシン、またはユーザーに適用できます。設定は、ローカルレベルの個々のユーザー、またはActive Directoryのセキュリティグループに適用できます。構成は特定の基準とルールを定義します。ポリシーを具体的に割り当てない場合、設定はすべての接続に適用されます。



ポリシーはネットワークの異なるレベルで適用できます。組織単位GPOレベルに配置されたポリシー設定は、ネットワーク上で最も高い優先順位を持ちます。ドメインGPOレベルのポリシーは、サイトグループポリシーオブジェクトレベルのポリシーを上書きします。サイトグループポリシーオブジェクトレベルは、MicrosoftおよびCitrixローカルポリシーレベルの両方における競合するポリシーを上書きします。

すべてのCitrixローカルポリシーは、Web Studioコンソールで作成および管理され、サイトデータベースに保存されます。グループポリシーは、Microsoftグループポリシー管理コンソール (GPMC)

を使用して作成および管理され、Active Directoryに保存されます。Microsoftローカルポリシーは、Windowsオペレーティングシステムで作成され、レジストリに保存されます。

Studioは、モデリングウィザードを使用して、管理者がテンプレートとポリシー内の構成設定を比較し、競合する設定や冗長な設定を排除できるようにします。管理者はGPMCを使用してGPOを設定し、設定を構成できます。また、それらをネットワークの異なるレベルのターゲットユーザーセットに適用することもできます。

これらのGPOはActive Directoryに保存されます。これらの設定の管理へのアクセスは、セキュリティ上の理由からほとんどのIT担当者に対して制限されています。

設定は、優先順位と条件に従ってマージされます。無効な設定は、下位の有効な設定を上書きします。未構成のポリシー設定は無視され、下位の設定を上書きしません。

ローカルポリシーは、Active Directoryのグループポリシーと競合する可能性もあり、状況によっては互いに上書きし合うことがあります。

すべてのポリシーは次の順序で処理されます。

1. エンドユーザーはドメイン資格情報を使用してマシンにログオンします。
2. 資格情報はドメインコントローラーに送信されます。
3. Active Directoryはすべてのポリシー (エンドユーザー、エンドポイント、組織単位、ドメイン) を適用します。
4. エンドユーザーはCitrix Workspace™アプリにログオンし、アプリケーションまたはデスクトップにアクセスします。
5. CitrixおよびMicrosoftのポリシーは、エンドユーザーとリソースをホストするマシンに対して処理されます。
6. Active Directoryはポリシー設定の優先順位を決定します。その後、それらをエンドポイントデバイスのレジストリと、リソースをホストするマシンに適用します。
7. エンドユーザーがリソースからログオフします。エンドユーザーおよびエンドポイントデバイスに対するCitrixポリシーは、アクティブではなくなります。
8. エンドユーザーがユーザーデバイスからログオフすると、GPOユーザーポリシーが解放されます。
9. エンドユーザーがデバイスの電源を切ると、GPOマシンポリシーが解放されます。

ユーザー、デバイス、およびマシンのグループに対してポリシーを作成する場合、一部のメンバーは異なる要件を持つ可能性があり、一部のポリシー設定に例外が必要になることがありま

す。例外は、ポリシーが誰または何に影響するかを決定するStudioおよびGPMCのフィルターによって作成されます。

> **注:**
>
> 同じGPO内でWindowsポリシーとCitrixポリシーを混在させることはサポートされていません。

概要

> **注:**
>
> バージョン2511以降、Citrix Web Studio™（Webベース）は、Citrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

ポリシーとは、ユーザー、デバイス、または接続の種類グループに対して、セッション、帯域幅、セキュリティがどのように管理されるかを定義する設定の集合です。Citrix®ポリシーは、これらの側面を一元的に管理する効率的な方法を提供します。各ポリシーには、環境に合わせて調整された複数の設定とフィルター（オブジェクト割り当て）を含めることができます。

ポリシー管理ツール

- ウェブスタジオ

  Web Studioを使用して作成されたポリシーはサイトデータベースに保存され、以下のいずれかが発生したときに更新がVDAにプッシュされます。

  - そのVDAがブローカーに登録されたとき
  - ユーザーがセッションを起動したとき

- グループポリシー管理コンソール（GPMC）

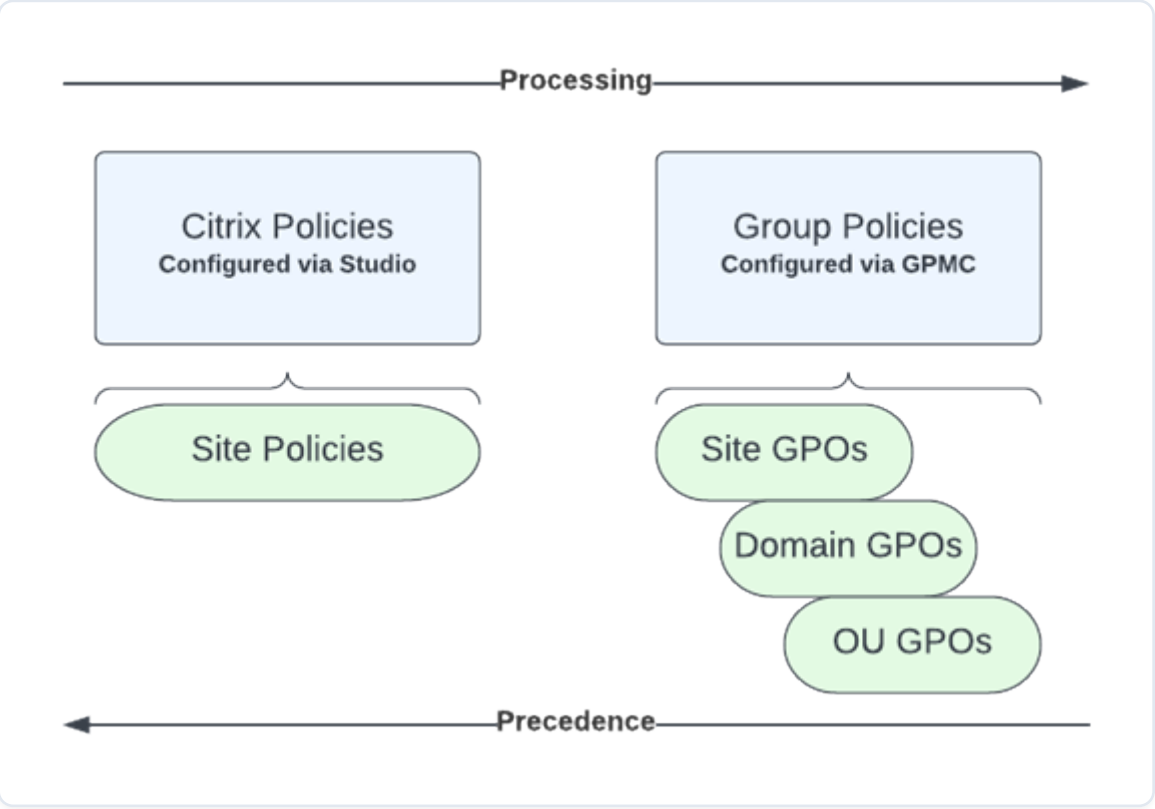
ネットワーク環境でActive Directoryを使用しており、グループポリシーを管理する権限がある場合は、GPMCを使用してポリシーを作成および編集できます。

GPMCでは、必要な設定とフィルターを使用してグループポリシーオブジェクト（GPO）を構成できます。これらのポリシーは、Web Studioで構成されたポリシーよりも優先されます。詳細については、CTX238166を参照してください。

ポリシー処理の順序

グループポリシー設定は、次の順序で処理されます。

1. サイトレベルのGPO（サイトデータベースに保存）
2. ドメインレベルGPO
3. 組織単位 (OU) GPO



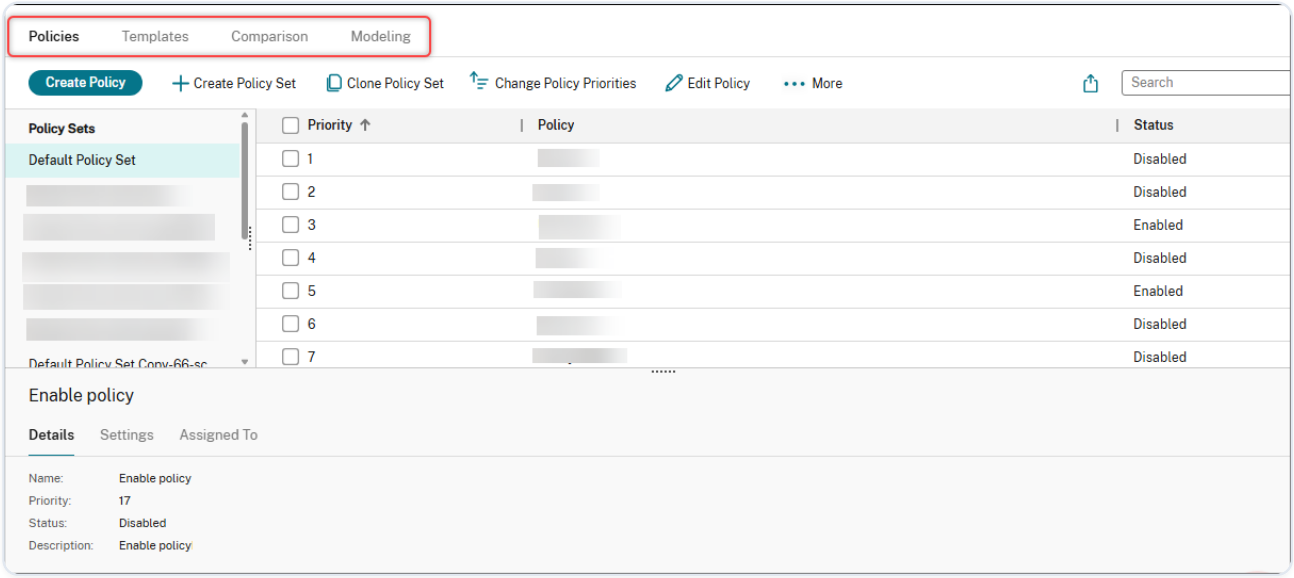
同じポリシーに対して2つのGPOで異なる設定が適用されている場合、最後に処理されたポリシー設定が以前に処理された設定を上書きします。この構成は、ポリシー設定が次の順序で優先されることを意味します。

1. OU GPO (最高優先度)
2. ドメインレベルGPO
3. サイトレベルGPO (最低優先度)

競合する設定を持つ複数のポリシーを使用している場合は、ポリシーの優先順位を割り当てることで優先順位を制御できます。詳細については、「ポリシー割り当ての例外を管理する」を参照してください。

Web Studio > ポリシーインターフェイスについて

ポリシー、設定、またはテンプレートにアクセスするには、Web Studioにサインインし、左側のペインで**ポリシー**を選択します。



- **ポリシー**タブでは、ポリシーセットとポリシーを作成および管理できます。ポリシーセットからポリシーを選択すると、次のタブが表示されます。
  - **概要**: ポリシー名、優先度、ステータス、および説明が表示されます。
  - **設定**: 構成されているすべての設定を一覧表示します。
  - **割り当て先**: 割り当てられたデリバリーグループが表示されます。割り当てを編集または削除できます。ポリシーは、セッションを実行しているデスクトップのデリバリーグループに基づいて適用されます。詳細については、「ポリシーを作成する」を参照してください。
- 「**テンプレート**」タブでは、ポリシーテンプレートを作成し、Citrix提供のテンプレートとカスタムテンプレートを管理できます。テンプレートを選択すると、次のタブが表示されます。
  - 「**説明**」: テンプレートの目的を説明します。
  - 「**設定**」: 構成された設定を一覧表示します。詳細については、「テンプレートの作成」を参照してください。

- 「**比較**」タブでは、ポリシーまたはテンプレートの設定を他のものと比較できます。この機能を使用して、コンプライアンスまたは相違点を確認します。詳細については、「ポリシーとテンプレートの比較」を参照してください。
- 「**モデリング**」タブでは、接続シナリオをシミュレートし、有効なポリシー結果を表示できます。詳細については、「ポリシーのシミュレーションと評価」を参照してください。

ポリシー構成ワークフロー

Web Studioを使用してCitrixポリシーを構成するには、次のワークフローに従います。

1. ポリシーの作成。
   a. ポリシー設定を構成します。

      環境に必要な設定を追加および構成します。

   b. ポリシーを割り当てます。

      ポリシーを適切なマシンオブジェクトとユーザーオブジェクトに割り当てます。
2. ポリシーの優先順位の設定。

   どの設定が優先されるかを決定するために、ポリシーを優先順位で並べ替えます。
3. 有効なポリシーの確認。

   ポリシーモデリングウィザードを使用して、適用された設定を確認します。

テンプレートを作成する

> **注:**
>
> バージョン2511以降、Citrix Web Studio™（Webベース）は、Citrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

テンプレートは、ポリシーを作成するための事前定義された開始点を提供します。Citrixでは、特定の環境とネットワーク条件に最適化された組み込みテンプレートを提供しています。これらのテンプレートを使用して、次のことができます。

- サイト間で共有する独自のポリシーとテンプレートを作成する。
- 展開間の比較時に参照します。たとえば、`when using the Citrix template X or Y...`。
- テンプレートをインポートまたはエクスポートすることで、Citrixサポートまたは信頼できるサードパーティとポリシー構成を共有する。

組み込みテンプレート

以下の組み込みテンプレートが利用可能です。

- **非常に高精細なユーザーエクスペリエンス**。このテンプレートは、ユーザーエクスペリエンスを最大化するデフォルト設定を適用します。複数のポリシーが優先順位に従って処理されるシナリオでこのテンプレートを使用します。
- **高いサーバー拡張性**。このテンプレートを適用して、サーバーリソースを節約します。このテンプレートは、ユーザーエクスペリエンスとサーバーの拡張性のバランスを取ります。単一サーバーでホストできるユーザー数を増やしながら、優れたユーザーエクスペリエンスを提供します。このテンプレートは、グラフィックの圧縮にビデオコーデックを使用せず、サーバー側のマルチメディアレンダリングを防止します。
- **高いサーバー拡張性 - レガシーOS**。この高いサーバー拡張性テンプレートは、Windows Server 2008 R2またはWindows 7以前を実行しているVDAにのみ適用されます。このテンプレートは、これらのオペレーティングシステムにより効率的なレガシーグラフィックモードに依存しています。
- **NetScaler SD-WAN向けに最適化**。Citrix Virtual Desktops™の配信を最適化するために、NetScaler SD-WANを使用している支社のユーザーにこのテンプレートを適用します。（NetScaler SD-WANはCloudBridge®の新しい名称です）。
- **WAN向けに最適化**。このテンプレートは、共有WANを使用する支社のタスクワーカーや、低帯域幅接続のリモートロケーションのタスクワーカーを対象としています。ワーカーは、グラフィックがシンプルなユーザーインターフェイスと、ほとんどマルチメディアコンテンツを含まないアプリケーションにアクセスします。このテンプレートは、ビデオ再生エクスペリエンスと一部のサーバー拡張性を犠牲にして、帯域幅効率を最適化します。
- **WAN向けに最適化 - レガシーOS**。このテンプレートは、Windows Server 2008 R2またはWindows 7以前を実行しているVDAにのみ適用されます。このテンプレートは、これらのオペレーティングシステムにより効率的なレガシーグラフィックモードに依存しています。
- **セキュリティと制御**。リスク許容度が低い環境で、Citrix Virtual Apps and Desktops でデフォルトで有効になっている機能を最小限に抑えるために、このテンプレートを使用します。このテンプレートには、以下の機能へのアクセスを無効にする設定が含まれています。

- 印刷
- クリップボード
- 周辺機器
- ドライブマッピング
- ポートリダイレクト
- ユーザーデバイスでのFlashアクセラレーション

このテンプレートを適用すると、より多くの帯域幅を使用し、サーバーあたりのユーザー密度が低下する可能性があります。

組み込みテンプレートのデフォルト設定を使用することをお勧めしますが、**WANテンプレート**の**セッション全体の帯域幅制限**など、一部の設定は、管理者が展開固有の調整を行えるように未構成のままになっています。

テンプレートのデフォルト設定画像(/en-us/citrix-virtual-apps-desktops/2511/media/template-default-settings.png)

XenApp®およびXenDesktop® 7.6 FP3より前の展開（ポリシー管理およびVDA）を使用しており、高サーバー拡張性またはWAN向け最適化テンプレートが必要な場合は、該当するレガシーOSバージョンのこれらのテンプレートを使用してください。

> **注:**
>
> 組み込みテンプレートはCitrixが作成および更新します。これらのテンプレートを変更または削除することはできません。

テンプレートの作成

テンプレートからテンプレートを作成するには：

1. Web Studioで、左側のペインで**ポリシー**を選択します。
2. **テンプレート**タブを選択し、次にテンプレートを作成する元のテンプレートを選択します。
3. **テンプレートの作成**タブを選択します。**設定の選択**画面が表示されます。
4. テンプレートに含めるポリシー設定を選択して構成します。
5. 「**次へ**」をクリックします。「**概要**」画面が表示されます。
6. テンプレートの名前を入力します。

7. **完了**をクリックします。新しいテンプレートが**テンプレート**タブに表示されます。

ポリシーに基づいてテンプレートを作成するには：

1. Web Studioで、左側のペインで**ポリシー**を選択します。
2. **ポリシー**タブで、テンプレートを作成する元のポリシーを選択します。
3. **その他**タブをクリックします。
4. **テンプレートとして保存**を選択します。**設定の選択**画面が表示されます。
5. テンプレートに含める新しいポリシー設定を選択して構成します。
6. 「**次へ**」をクリックします。「**概要**」画面が表示されます。
7. テンプレートの名前と説明を入力し、「**完了**」をクリックします。

ポリシーを作成する

> **注:**
>
> バージョン2511以降、Citrix Web Studio™（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

ポリシーは次の2つの部分を定義します。

- ユーザー、デバイス、または接続タイプのグループに対して、セッション、帯域幅、セキュリティがどのように管理されるかを定義する設定のグループ。
- ポリシーを割り当てるユーザーとマシン。ポリシーを作成する前に、それが影響するユーザーまたはデバイスのグループを決定します。職務機能、接続タイプ、デバイスプラットフォーム、または地理的な場所に基づいてポリシーを作成することをお勧めします。

ポリシーを作成するときは、ポリシーテンプレートの設定に基づいて作成し、必要に応じてカスタマイズできます。また、ゼロから開始して必要な設定を手動で追加することもできます。このセクションでは、次のトピックについて説明します。

- ポリシーの仕組み
- ゼロからポリシーを作成する

- テンプレートからポリシーを作成する

> **ヒント**
>
> グループにポリシーが既に存在する場合は、新しいポリシーを作成するのではなく、既存のポリシーを編集することを検討してください。特定の機能を有効にするためだけ、または特定のユーザーを除外するためだけにポリシーを作成することは避けてください。

ポリシーの仕組み

ユーザーがログオンすると、接続の割り当てに一致するすべてのポリシーが特定されます。これらのポリシーは優先度によってランク付けされ、任意の設定の複数のインスタンスが比較されます。各設定について、最も優先度の高いポリシーの値が適用されます。優先度の高いポリシーが設定を無効にしている場合、その設定は、それが有効になっている優先度の低いポリシーをすべて上書きします。構成されていない設定は無視されます。

> **重要:**
>
> Active Directory と Citrix ポリシーの両方をグループポリシー管理コンソールを使用して構成している場合、割り当てと設定が期待どおりに適用されないことがあります。詳細については、CTX127461 を参照してください。

フィルターなしのポリシー

デフォルトポリシーとして、**Unfiltered** というポリシーが提供されています。

- Web Studio で Citrix® ポリシーを管理する場合、Unfiltered ポリシーの設定は、サイト内のすべてのサーバー、デスクトップ、および接続に適用されます。
- 設定を適用するには、サイトと接続がポリシーを含む GPO のスコープ内にある必要があります。

  例: **Sales** OU にリンクされ、すべての米国の営業チームメンバーを含む **Sales-US** という名前の GPO があります。この GPO は、いくつかのユーザー設定を含む **Unfiltered** ポリシーで構成されています。営業マネージャーがログオンすると、ユーザーが **Sales-US** GPO に属しているため、**Unfiltered** ポリシー設定が適用されます。

割り当てモード

割り当てモードは、接続基準がどのように一致するかに基づいてポリシーが適用されるかどうかを制御します。

- **許可** (デフォルト): 接続が割り当て条件に一致する場合にのみポリシーを適用します。
- **拒否**: 接続が条件に一致しない場合にポリシーを適用します。

例 1: 同じ割り当てタイプ、異なるモード

ポリシー 1 には以下が含まれます:

- 割り当て A: 営業グループ、モード = 許可
- 割り当て B: 営業マネージャーのアカウント、モード = 拒否

ユーザーは営業グループに属していますが、拒否割り当てが優先されます。営業マネージャーがログオンしても、ポリシーは適用されません。

例 2: 異なる割り当てタイプ、同じモード

ポリシー2には以下が含まれます。

- 割り当て C: 営業グループ (ユーザー)、モード = 許可
- 割り当て D: 企業 IP 範囲 (クライアント IP)、モード = 許可

ポリシーは、両方の割り当てが満たされた場合にのみ適用されます。営業マネージャーがオフィスからログオンした場合、両方の条件が満たされ、ポリシーが適用されます。

ポリシー 3 には以下が含まれます。

- 割り当て E: 営業グループ (ユーザー)、モード = 許可
- 割り当て F: NetScaler Gateway 接続 (アクセス制御)、モード = 許可

営業マネージャーがオフィスから (NetScaler 経由ではなく) ログオンした場合、割り当て F は満たされないため、ポリシーは適用されません。

ポリシー設定: 親子関係

一部のポリシー設定は親設定に依存します。たとえば、子設定が利用可能になる前に、**セッション全体の帯域幅制限**を構成する必要があります。

Web Studioでポリシーを構成する際、子設定にカーソルを合わせると、最初にどの親を設定する必要があるかを確認できます。親が無効になっている場合、関連する子設定は自動的に無効になります。

依存するポリシー設定の図(/en-us/citrix-virtual-apps-desktops/2511/media/dependent-policy-settings.png)

次の表に、親設定とそれに対応する子設定を示します。

親ポリシー	依存子ポリシー
セッション全体の帯域幅制限	オーディオリダイレクトの帯域幅制限の割合
	クリップボードリダイレクトの帯域幅制限の割合
	COMポートリダイレクトの帯域幅制限の割合
	ファイルリダイレクトの帯域幅制限の割合
	HDX™ MediaStream マルチメディアアクセラレーションの帯域幅制限の割合
	LPTポートリダイレクトの帯域幅制限の割合
	プリンターリダイレクトの帯域幅制限の割合
	クライアントUSBデバイスリダイレクト帯域幅制限の割合
	TWAINデバイスリダイレクト帯域幅制限の割合
双方向コンテンツリダイレクトを許可する	クライアントにリダイレクトされる許可されたURL
	VDAにリダイレクトされる許可されたURL
CPU使用率	CPU使用率から除外されるプロセスの優先度
レガシーグラフィックモード	プログレッシブ圧縮レベル
セッションウォーターマークを有効にする	ウォーターマークのカスタムテキスト
	セッションウォーターマークスタイル
	ウォーターマークの透明度

親ポリシー	依存子ポリシー
HDXアダプティブトランスポート	オーディオのロス許容モード

ポリシー設定の状態

一部のポリシー設定には、次のいずれかの状態があります。

- **許可**または**禁止**: 設定によって制御されるアクションを許可または防止します。場合によっては、ユーザーがセッション内で設定のアクションを管理することを許可または防止されます。たとえば、メニューアニメーションが「許可」に設定されている場合、ユーザーはセッション内でそれを制御できます。
- **有効**または**無効**: 設定をオンまたはオフにします。優先度の高いポリシーで設定が無効になっている場合、優先度の低いポリシーで有効になっていても適用されません。

セキュアなデフォルト設定

VDAインストール中にセキュアなデフォルト設定が有効になっている場合、ポリシー設定の優先順位は次のとおりです。

1. カスタマイズされた設定
2. セキュアなデフォルト設定
3. デフォルト設定

セキュアなデフォルト値を表示するには：

1. Web Studioで、左ペインの**ポリシー**をクリックします。
2. **ポリシー**タブで、**ポリシーの作成**をクリックします。
3. **設定の選択**テーブルで、現在の値が**許可**になっている設定にマウスオーバーすると、**セキュアなデフォルト値: 禁止**が表示されます。

   セキュアなデフォルト設定(/en-us/citrix-virtual-apps-desktops/2511/media/secure-default-setting.png)

ポリシー設定の有効性

一部の設定は、一緒に使用して有効にする必要があります。たとえば、ユーザーがローカルデバイス上のネットワークドライブにアクセスできるようにするには、次の手順を実行します。

- **クライアントドライブリダイレクト**を有効にする必要があります
- **クライアントネットワークドライブ**も含まれている必要があります

クライアントドライブリダイレクトが無効になっている場合、**クライアントネットワークドライブ**が有効になっていても、ユーザーはネットワークドライブにアクセスできません。

一般に、マシン関連の設定の変更は、VDAが再起動するか、ユーザーがログオンしたときに有効になります。ユーザー関連の設定の変更は、次回のログオン時に適用されます。

ポリシーに設定を追加する際、「デフォルト値を使用する」を選択して変更を防止できます。このオプションは手動設定を無効にし、以前に入力された値に関係なく、デフォルト値のみを適用します。

ベストプラクティス

- ポリシーは個々のユーザーではなくグループに割り当てます。グループにポリシーを割り当てると、グループへのユーザーの追加または削除時に割り当てが自動的に更新されます。
- 未使用のポリシーは無効にします。設定が追加されていないポリシーは、不要な処理オーバーヘッドを発生させます。

ポリシーを最初から作成する

ポリシーを作成するには:

1. Web Studioで、左側のペインで**ポリシー**をクリックします。
2. **ポリシー**タブで、**ポリシーの作成**をクリックします。
3. **設定の選択**ページで、設定を選択して構成し、**次へ**をクリックします。
4. **ポリシーの割り当て先**ページで、このポリシーが存在するポリシーセットを選択し、次にポリシーを割り当てるオブジェクトを選択します。**次へ**をクリックします。
5. **概要**ページで、次の設定を完了します。
    a. ポリシーの名前と説明を入力します。
    b. ポリシーを有効にするには、**ポリシーを有効にする**を選択します。
6. **完了**をクリックします。

手順1: ポリシー設定の選択と構成

ポリシー設定は機能別にグループ化されています。たとえば、プロファイル管理に関連する設定は、**プロファイル管理**カテゴリの下にあります。

設定には次の2種類があります。

- **コンピューター設定**: マシンに適用され、仮想デスクトップの起動時に（ユーザーがログオンしていなくても）有効になります。これらは仮想デスクトップの動作を定義します。
- **ユーザー設定**: ユーザーが接続または再接続したときに適用されます。これらはユーザーエクスペリエンスを定義します。

設定を選択して構成するには:

1. 「**設定の選択**」ページで、VDAバージョン別に設定を表示するには、右上のドロップダウンリストオプションから次のいずれかを選択します。
   - **すべての設定**: すべてのVDAバージョンのすべての設定を表示します。
   - **現在の設定のみ**: 現在のVDAバージョンのみの設定を表示します。
   - **レガシー設定のみ**: 非推奨のVDAバージョンのみの設定を表示します。
2. 設定を検索するには、検索ボックスに設定の完全な名前または部分的な名前を入力します。
3. 設定を選択します。**有効**をクリックしてオンにするか、**編集**をクリックして値を指定します。
4. ステップ3を繰り返して、ポリシーの他の設定を選択して構成します。

> **注:**
>
> ポリシー設定は、有効、無効、または未構成にすることができます。デフォルトでは、ポリシー設定は構成されていません。つまり、ポリシーに追加されていません。設定は、ポリシーに追加された場合にのみ適用されます。

ステップ2：ポリシー割り当てを指定する

ポリシー割り当ては、ポリシーが適用されるユーザーとマシンを定義します。割り当てがポリシーの動作にどのように影響するかについては、「ポリシーのしくみ」を参照してください。

ポリシー割り当てを指定するには：

1. **ポリシーの割り当て先**ページで、**フィルターされたユーザーとコンピューター**を選択します。
2. 割り当て（*フィルター*とも呼ばれます）を指定して、ユーザーまたはコンピューターを選択します。利用可能な割り当てタイプについては、次の表を参照してください。

> **注:**

- 割り当てを指定しないか、無効にした場合、ポリシーは**すべて**の接続に適用されます。
- ポリシーの*割り当て*は、ポリシーの*フィルター*とも呼ばれます。詳細については、ポリシーのフィルターを作成、変更、または削除するおよびフィルターはどのように適用されますか？を参照してください。

割り当ての種類	説明
アクセスコントロール	クライアントが接続するアクセスコントロール条件 • **接続タイプ**: NetScaler® Gateway を使用しているかどうかにかかわらず、ポリシーを接続に適用するかどうか。*NetScaler Gatewayファーム名* - NetScaler Gateway仮想サーバーの名前。*アクセス条件* - 使用するエンドポイント分析ポリシーまたはセッションポリシーの名前。 • **NetScaler Gatewayファーム名**: NetScaler Gateway仮想サーバーの名前。*アクセス条件* - 使用するエンドポイント分析ポリシーまたはセッションポリシーの名前。 • **アクセス条件**: 使用するエンドポイント分析ポリシーまたはセッ

割り当ての種類	説明	
	ションポリシーの名前。	
Citrix SD-WAN™	ユーザーセッションがCitrix SD-WANを介して起動されるかどうか。**注:** 1つのポリシーに追加できるCitrix SD-WAN割り当ては1つだけです。	
クライアントIPアドレス	セッションへの接続に使用されるユーザーデバイスのIPアドレス: IPv4の例: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24; IPv6の例: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54	
クライアント名	ユーザーデバイスの名前。完全一致: ClientABCName。ワイルドカードの使用: Client*Name。	
クライアントプラットフォーム	セッションへの接続に使用されるユーザーデバイスの OS タイプ (Windows、Linux、iOS、Android、HTML5 など)。必要な VDA バージョン: 2503 以降。	
デリバリーグループ	デリバリーグループのメンバーシップ。	
デリバリーグループの種類	デスクトップまたはアプリケーションの種類: プライベートデスクトップ、共有デスクトップ、プライベー	

割り当ての種類	説明
	トアプリケーション、または共有アプリケーション。
組織単位 (OU)	組織単位。
タグ	タグ。**注:** このポリシーは、タグ付けされたすべてのマシンに適用されます。アプリケーションタグは含まれません。
ユーザーまたはグループ	ユーザーまたはグループ名。ユーザーとグループでサポートされているIDタイプには、Active Directory、Microsoft Entra ID、Okta、Google Cloudが含まれます。必要なVDAバージョン: 2507以降。

テンプレートからポリシーを作成する

Citrix提供またはカスタムテンプレートに基づいてポリシーを作成できます。結果として得られるポリシーは、元のテンプレートとは独立しています。

テンプレートからポリシーを作成するには:

1. Web Studioで、左側のペインで**ポリシー**を選択します。
2. **テンプレート**タブを選択し、使用するテンプレートを選択します。
3. アクションバーで**テンプレートからポリシーを作成**をクリックします。選択したテンプレートで事前構成されたすべての設定が表示された**ポリシーの作成**ページが表示されます。
4. 必要に応じて設定を変更したり、設定を追加したりしてから、**次へ**をクリックします。
5. **ポリシーの割り当て先**ページで、このポリシーが存在するポリシーセットを選択し、ポリシーを割り当てるオブジェクトを選択します。**次へ**をクリックします。
6. **概要**ページで、ポリシーの名前と説明を入力します。
7. **完了**をクリックします。新しいポリシーは、**ポリシー**タブの指定されたポリシーセットに表示されます。

次のステップ

- ポリシーの優先順位付け
- ポリシーのシミュレーションと評価

ポリシーセットの作成

> **注：**
>
> バージョン2511以降、Citrix Web Studio™（Webベース）は、Citrix Virtual Apps and Desktops™ の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> ポリシーセットは、Citrix Virtual Apps and Desktopsにおけるオブジェクトであり、ポリシーを集約して、簡素化されたロールベースのアクセスと容易な管理を可能にします。作成後、スコープとデリバリーグループがポリシーセットに割り当てられ、承認された管理者のみが、関連するユーザーとマシンに適用されるポリシーを管理できるようになります。

ポリシーセットは、Citrix® ポリシーを論理グループに編成することで、より効率的に管理するのに役立ちます。ポリシーセットをデリバリーグループに割り当てると、デリバリーグループはそのセット内のポリシーのみを使用します。

このセクションでは、ポリシーセットの動作、作成と割り当ての方法、およびスコープとフィルターとの相互作用について説明します。

利点

ポリシーセットには、いくつかの主要な利点があります。

- 分散型管理者チーム向けのロールベースのアクセス制御
- 合併、買収、統合の簡素化
- 制限された障害ドメイン
- ポリシーのマルチテナントサポート

次の表は、ポリシーがポリシーセットの有無にかかわらずどのように機能するかを比較したものです。

ポリシーセットなし	ポリシーセットあり
すべてのポリシー、設定、フィルター（割り当て）、および優先度は、1つの中央の場所で管理されます。	各ポリシーセットには、独自のポリシー、設定、フィルター（割り当て）、および優先度があります。
1つのポリシーを管理する場合、すべてのポリシーを管理する必要があります。	フル管理者は、特定のポリシーセットを個別に管理する機能を下位レベルの管理者に委任できます。
大規模で分散された環境のポリシーは、複雑になり管理が困難になります。	大規模で分散された環境のポリシーは、簡単に分割して管理できます。

動作の仕組み

ポリシーセットはデリバリーグループに割り当てられ、特定の管理者にスコープが設定されます。セット内のポリシーは、引き続きフィルター（割り当て）を使用して、どのユーザーまたはマシンに適用されるかを決定します。

主な動作:

- ポリシーセットはデリバリーグループに割り当てられます
  - デリバリーグループは一度に1つのポリシーセットのみを使用できます。
  - 1つのポリシーセットを複数のデリバリーグループに割り当てることができます。
  - デリバリーグループにポリシーセットが割り当てられていない場合、**デフォルトポリシーセット**を使用します。
- ポリシーがセット内にあるかどうかにかかわらず、ポリシーのフィルターは引き続き適用されます。
- ポリシーセットは、1つまたは複数のスコープを持つことができます。
  - スコープは、管理者が管理できるオブジェクト（例：接続、カタログ、デリバリーグループ、アプリケーショングループ）の集合を表します。
  - 管理者は、承認された管理者のみがポリシーセットを表示または編集できるように、ポリシーセットのスコープを定義できます。スコープは、ポリシーセットの作成時または後でセットを編集するときに設定できます。
- デフォルトで、**デフォルトポリシーセット**には**このリソースのスコープ制御をバイパス**が選択されています。この設定により、ポリシーセットはすべての管理者から表示されたままになり

ます。スコープ制御を適用するには、ポリシーセットを編集し、**このリソースのスコープ制御をバイパス**チェックボックスをオフにしてから、目的のスコープを選択します。

ポリシーフィルターと割り当ては、ポリシーセットがない場合と同じように機能します。詳細については、「フィルターの適用方法」を参照してください。

ポリシーセットを有効にする

Web Studioで、 > に移動し、 設定をオンにします。

注:

- ポリシーセットを作成する前に、ポリシーセットを有効にする必要があります。
- ポリシーセットを有効にすると、既存のすべてのポリシーが**デフォルトポリシーセット**にグループ化されます。このセットは、別のセットを割り当てない限り、すべてのデリバリーグループに自動的に割り当てられます。新しいポリシーセットがデリバリーグループに割り当てられると、そのグループはデフォルトポリシーセットの使用を停止します。

ポリシーセットを作成する

管理者チームや会社の論理的な区分を反映するようにポリシーセットを作成できます。たとえば、地理的地域、事業部門、または特定のユースケースごとにポリシーセットを作成できます。

ポリシーセットは次の2つの方法で作成できます。

- ポリシーセットを最初から作成する
- 既存のポリシーセットをコピーして作成する

または、Citrix Virtual Apps and Desktops PowerShell SDKを使用してポリシーセットを作成および管理することもできます。

ゼロからポリシーセットを作成する

1. Web Studioで、左ペインの**** ノードを選択します。
2. タブをクリックします。
3. を選択します。
4. タブをクリックし、ポリシーセットの名前と説明を入力します。

5. 「**割り当て**」タブをクリックし、1つ以上のデリバリーグループを選択します。
6. 「**スコープ**」タブをクリックし、ポリシーセットを適用できるオブジェクトを定義するスコープを選択します。
7. 「**作成**」をクリックして完了します。

ポリシーセットの複製

1. Web Studioで、左側のペインにある「**ポリシー**」ノードを選択します。
2. 「**ポリシー**」タブをクリックします。
3. 「**ポリシーセットの複製**」を選択します。
4. ポリシーセットの名前を更新します。
5. ポリシーセットの割り当てを更新または作成し、「**次へ**」をクリックします。
6. 複製されたポリシーセットに含めるポリシーを選択またはクリアします。
7. ポリシーのスコープを更新します。
8. **Create** をクリックします。

ポリシーの優先順位付け

> **注:**
>
> バージョン2511以降、Citrix Web Studio™（Webベース）は、Citrix Virtual Apps and Desktops™ の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> 複数のポリシーが接続に適用される場合、Citrix Virtual Apps and Desktopsはそれらを優先順位に従って評価します。数値が小さいほど優先度が高くなります（1が最高）。ポリシー間で競合する設定がある場合、最も優先度の高いポリシーの設定が適用されます。

Web Studio または PowerShell を使用してポリシーの優先順位を変更できます。

Web Studio を使用してポリシーの優先順位を変更する

1. **Web Studio**で、左ペインの**ポリシー**を選択します。

2. **ポリシー**タブで、アクションバーから**ポリシーの優先順位の変更**を選択します。
3. **ポリシーの優先順位の変更**ページで、以下のいずれかの方法を使用してポリシーを並べ替えます。
   - ポリシーをドラッグして目的の位置に移動します。
   - **上** または **下** 矢印アイコンをクリックして、1つ位置を移動します。
   - **一番上** または **一番下** 矢印アイコンをクリックして、最初または最後の位置に移動します。
   - **編集** アイコンをクリックし、優先順位番号を入力して、**保存** をクリックします。
4. **保存** をクリックして変更を適用します。

PowerShell を使用してポリシーの優先順位を変更する

`Set-GpoPolicyPriority.ps1` スクリプトを使用して、プログラムでポリシーの優先順位を並べ替えます。このスクリプトは、ポリシー名とターゲットの優先順位番号を受け入れ、内部でポリシー GUID を解決し、`Set-BrokerGpoPolicyPriorities` を使用して更新された順序を適用します。Web Studio コンソールの代わりに自動化によってポリシーの優先順位を管理する場合に、このアプローチを使用します。

ネイティブの `Set-BrokerGpoPolicyPriorities` コマンドレットは、ポリシー GUID の完全に順序付けられたリストを必要とします。このスクリプトは、ポリシー名と希望する優先順位を受け入れることでその複雑さを解消し、その後、GUID の解決を自動的に処理します。

始める前に

スクリプトを実行する前に、以下の要件を満たしていることを確認してください。

- Broker SDKがインストールされている、サポート対象バージョンのCitrix Virtual Apps and Desktops
- スクリプトは、Citrix Broker SDKがインストールされているDelivery Controller™で実行する必要があります
- PowerShellスナップイン: `Citrix.Broker.Admin.V2`（スクリプトによって自動的にロードされます）

スクリプトを実行する

1. `Set-GpoPolicyPriority.ps1`をDelivery Controllerにコピーします。
2. Delivery Controller で PowerShell セッションを開きます。

3. 必要なパラメーターを指定してスクリプトを実行します。

```
.\Set-GpoPolicyPriority.ps1 -PolicyName "<PolicyName>" -NewPriority
<Number>
```

`<PolicyName>`をポリシー名に、`<Number>`をターゲットの優先順位に置き換えます。

スクリプトは、現在の優先順位とターゲットの優先順位を出力し、変更を確認し、検証ステップを実行します。スクリプトが適用する前の並べ替えの詳細な表示のために、`-Verbose`を追加します。

パラメーター

パラメーター	必須	説明
`-PolicyName`	はい	優先順位を変更するポリシーの名前
`-NewPriority`	はい	ターゲットの優先順位 (1 = 最高)。ポリシーを最高位に移動するには0または負の数を使用し、最低位に移動するにはポリシー数を超える数を使用します。
`-PolicySetGuid`	いいえ	特定のポリシーセットのGUID。`DefaultSitePolicies`をターゲットにする場合は省略します。

例

デフォルトのポリシーセットでポリシーを最高の優先順位に設定します。

```
.\Set-GpoPolicyPriority.ps1 -PolicyName "MyPolicy" -NewPriority 1
```

ポリシーを最低の優先順位に設定します。

```
.\Set-GpoPolicyPriority.ps1 -PolicyName "MyPolicy" -NewPriority 9999
```

特定のポリシーセットでポリシーを優先順位5に設定します。

```
.\Set-GpoPolicyPriority.ps1 -PolicyName "MyPolicy" -NewPriority 5
-PolicySetGuid "12345678-1234-1234-1234-123456789012"
```

ポリシー割り当ての例外を管理する

注:

バージョン2511以降、Citrix Web Studio™（Webベース）は、Citrix Virtual Apps and Desktops™ の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

フィルターを使用してユーザー、ユーザーデバイス、またはマシンのグループにポリシーを割り当てるとき、グループの一部のメンバーには異なる設定が必要になる場合があります。このような場合でも、個々のメンバーごとに完全に個別のポリシーを作成することなく対応できます。

グループ内の特定のユーザーまたはマシンに対して、次の方法で例外を作成できます。

- それらのグループメンバー専用の個別のポリシーを作成し、より高い優先順位を付与する
- ポリシーに追加された割り当てに *拒否* モードを使用する

例外に拒否モードを使用する

モードが*拒否*に設定された割り当ては、ポリシーが割り当て基準に一致しない接続に適用されることを意味します。たとえば、ポリシーに次の割り当てが含まれているとします。

- *割り当てA*: クライアントIPアドレス割り当て範囲 `208.77.88.*`、モード = *許可*。
- *割り当てB*: 特定のユーザーアカウント、モード = *拒否*。

このポリシーは、指定されたIP範囲から接続するユーザーに適用されますが、*割り当てB* で定義されたユーザーは**除外されます**。

注:

ポリシーの割り当て手順で、**有効にする**チェックボックスをオフにすると、割り当てが無効になります。ポリシーに有効な割り当てがない場合、そのポリシーはサイト内のすべてのオブジェクトに適用されます。

関連コンテンツ

- ポリシーの優先順位付け
- ポリシーのシミュレーションと評価

ポリシーのシミュレーションと評価

注:

バージョン2511以降、Citrix Web Studio™（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

Web Studioの比較ツールとポリシーモデリングツールを使用して、構成の検証、ポリシーの動作テスト、および展開前にどの設定が適用されるかの評価を行います。

注:

- **モデリング**タブは、お客様のリクエストによって有効化された場合にのみ利用可能です。
- フィルターが適用された有効なポリシーのみがモデル化されます。無効なポリシーは適用されず、フィルターが適用されていない有効なポリシーは常に適用されます。

ポリシーとテンプレートの比較

Web Studioの比較機能を使用して、ポリシー、テンプレート、またはデフォルト設定間の違いを表示します。これにより、構成の一貫性を検証し、ベストプラクティスへの準拠を維持し、予期しない動作のトラブルシューティングを行うことができます。

次のことができます。

- ポリシーまたはテンプレートの設定を別のものと比較する
- 設定をデフォルト値と比較する
- ポリシー間の競合する構成または不足している構成を特定する

ポリシーとテンプレートを比較するには：

1. Web Studioで、左ペインの**ポリシー**を選択します。
2. 「**比較**」タブをクリックし、「**選択**」をクリックします。
3. 比較するポリシーまたはテンプレートを選択します。
4. (オプション) デフォルト設定を含めるには、「**デフォルト設定と比較**」を選択します。
5. 「**比較**」をクリックします。設定が列に表示されます。
    - すべての設定を表示するには、「**すべての設定を表示**」を選択します。
    - デフォルトビューに戻るには、「**共通設定を表示**」を選択します。

ポリシーモデリングウィザードを実行する

1. Web Studioで、「**ポリシー**」を選択します。
2. 「**モデリング**」タブを選択します。
3. アクションバーで「**ポリシーモデリング**」を選択します。
4. 「**はじめに**」ページを読み、「**次へ**」をクリックします。
5. ユーザーまたはコンピューターを選択します。コンテナ、特定のユーザー、またはコンピューターを参照することもできます。「**次へ**」をクリックします。
6. フィルターエビデンスを選択します。オプションで、「**デリバリーグループ**」、「**タグ**」、「**クライアントIPアドレス**」などの詳細を指定してシミュレーションを絞り込みます。「**次へ**」をクリックします。
7. 概要を確認し、「**実行**」をクリックします。

モデリング結果の表示と管理

ウィザードの実行後、レビュー、操作、エクスポートが可能なレポートが生成されます。

レポートの確認

- ドロップダウンメニューを使用して、「**すべての設定**」、「**コンピューター設定**」、または「**ユーザー設定**」を表示します。

- 特定の設定を検索します。
- 設定をクリックして、その設定が適用された理由または適用されなかった理由を確認します。
- 結果をJSONまたはHTML形式でエクスポートします。

レポートの管理

シミュレーションの実行後、アクションバーで次のオプションを使用できます。

オプション	説明
モデリングレポートの表示	結果を確認またはエクスポートします。
ポリシーモデリングの再実行	同じ基準を使用して再度実行します。
モデリングレポートの削除	現在のレポートを削除します。

結果ポリシーセット (RSoP) を使用したポリシー適用の評価

接続が期待どおりに動作しない場合、ポリシーの競合が原因である可能性があります。優先度の高いポリシーは、他のポリシーを上書きできます。結果ポリシーセット (RSoP) を使用して、特定の接続にどの設定が適用されるかを評価します。

2つのRSoP方法が利用可能です。

- **Citrixグループポリシーモデリングウィザード**

  ユーザーと割り当て条件を指定して、接続シナリオをシミュレートします。

- **グループポリシーの結果**

  ユーザーおよびVirtual Delivery Agent (VDA) に適用されるCitrixポリシーのレポートを生成します。

> **注:**
>
> **Web Studio**で作成されたサイトポリシー設定は、グループポリシー管理コンソール (GPMC) からCitrixグループポリシーモデリングウィザードを実行しても、結果ポリシーセットには含まれません。最も包括的な結果を得るには、GPMCのみを使用してポリシーを作成する場合を除き、**Web Studio**からポリシーモデリングウィザードを開始してください。

ポリシーの問題のトラブルシューティング

ユーザー、IPアドレス、およびその他の割り当てられたオブジェクトには、複数のポリシーが同時に適用される可能性があり、予期しない動作につながることがあります。

ポリシーモデリングウィザードを実行してもユーザー接続にポリシーが適用されない場合、次の理由が考えられます。

- 評価基準に一致する割り当てを持つポリシーがない。
- 割り当てに一致するポリシーに設定が構成されていない。
- 割り当てに一致するポリシーが無効になっている。

これらの問題を解決するには：

- 関連するポリシーを有効にします。
- 各ポリシーに少なくとも1つの設定を構成します。

> **注:**
>
> ダブルホップシナリオ（たとえば、シングルセッションOS VDAがマルチセッションOS VDAに接続する場合）では、Citrixポリシーはシングルセッション OS VDAをユーザーデバイスとして扱います。セカンドホップ用にキャッシュされたイメージは、ファーストホップマシンに適用されます。

Directorで適用されているポリシーを表示する

管理者以外のユーザーは、**Director** を使用して、ユーザーセッションに適用されるポリシーを表示できます。これは、Web Studioへのアクセスを必要とせずに、どのポリシー設定が有効になっているかを確認するのに役立ちます。

レガシーMMCグループポリシーテンプレートをWeb Studioに移行する

> **注:**
>
> バージョン2511以降、Citrix Web Studio™（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報

については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

レガシーMMC Studioグループポリシーテンプレートは、MMC Studioが実行されているローカルコンピューターの管理者のユーザープロファイルに保存されます。Web Studioテンプレートはサイトデータベースに保存され、どのコンピューターからでもすべての管理者がアクセスできます。これら2つの形式間には直接のエクスポートまたはインポートパスがないため、ポリシーを仲介役として使用してレガシーテンプレートを移行します。

始める前に

- レガシーテンプレートが保存されているMMC Studioのインストールにアクセスできることを確認してください。
- Web Studio が同じ Citrix Virtual Apps and Desktops サイトにアクセスできることを確認してください。
- 移行後に設定を確認できるように、レガシーテンプレートの設定をメモしておいてください。

テンプレートを移行する

1. MMC Studioで、移行したいテンプレートに移動します。
2. **アクション**ペインで、**テンプレートからポリシーを作成**を選択します。
3. ウィザードに従ってポリシーを作成します。便宜上、テンプレートと同じ名前を使用してください。
4. ポリシーがWeb Studioに表示されるまで最大5分間待ちます。この時間は、サイトサービスがポリシーデータをMMC形式からWeb Studio形式に変換するために必要です。
5. Web Studioを開き、左ペインで**ポリシー**を選択します。
6. ポリシーリストにポリシーが表示されていることを確認します。
7. ポリシーを選択し、リボンで**...その他**を選択して**テンプレートとして保存**をクリックします。
8. ウィザードに従ってWeb Studioテンプレートを作成します。

移行後、テンプレートはサイトデータベースに保存され、任意のコンピューターからWeb Studioを使用するすべての管理者がアクセスできます。

移行の確認

1. Web Studioで、**Policies**ノードの**Templates**タブを選択します。

2. 移行されたテンプレートが表示されていることを確認します。
3. 設定が元のMMCテンプレートと一致することを確認するために比較します。

移行を確認したら、元のMMCテンプレートを廃止できます。MMCテンプレートは、作成されたコンピューターにローカルに残ります。

例

次の例は、複数のサイトで共有される透かし構成を含む、*透かし設定*という名前のテンプレートを移行する方法を示しています。

1. MMC Studioで、*Watermark Settings*テンプレートを見つけます。**Actions**ペインで、**Create Policy from Template**をクリックします。

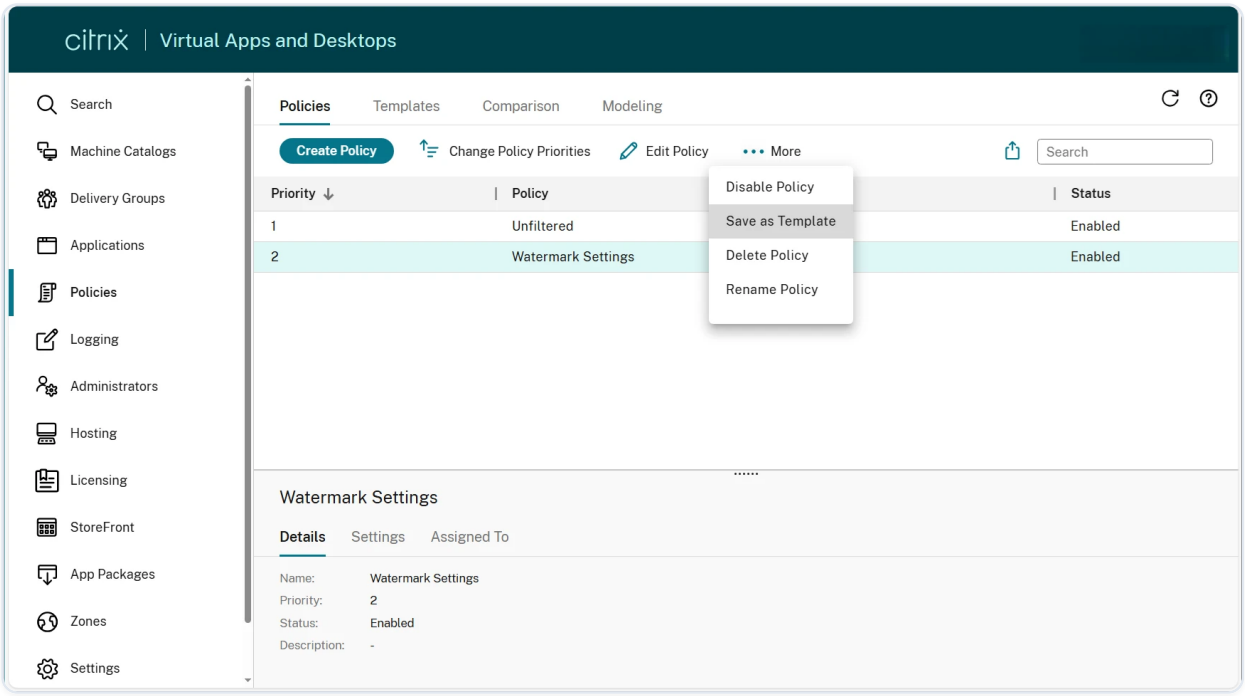
   MMCテンプレート(/en-us/citrix-virtual-apps-desktops/2511/media/policy-migrate-example1.png)
2. ウィザードに従ってポリシーを作成します。便宜上、テンプレートと一致するようにポリシーに*Watermark Settings*という名前を付けます。

   テンプレートからポリシーを作成(/en-us/citrix-virtual-apps-desktops/2511/media/policy-migrate-example2.png)
3. 最大5分間待ってからWeb Studioを開きます。ポリシーリストに*Watermark Settings*ポリシーが表示されていることを確認します。

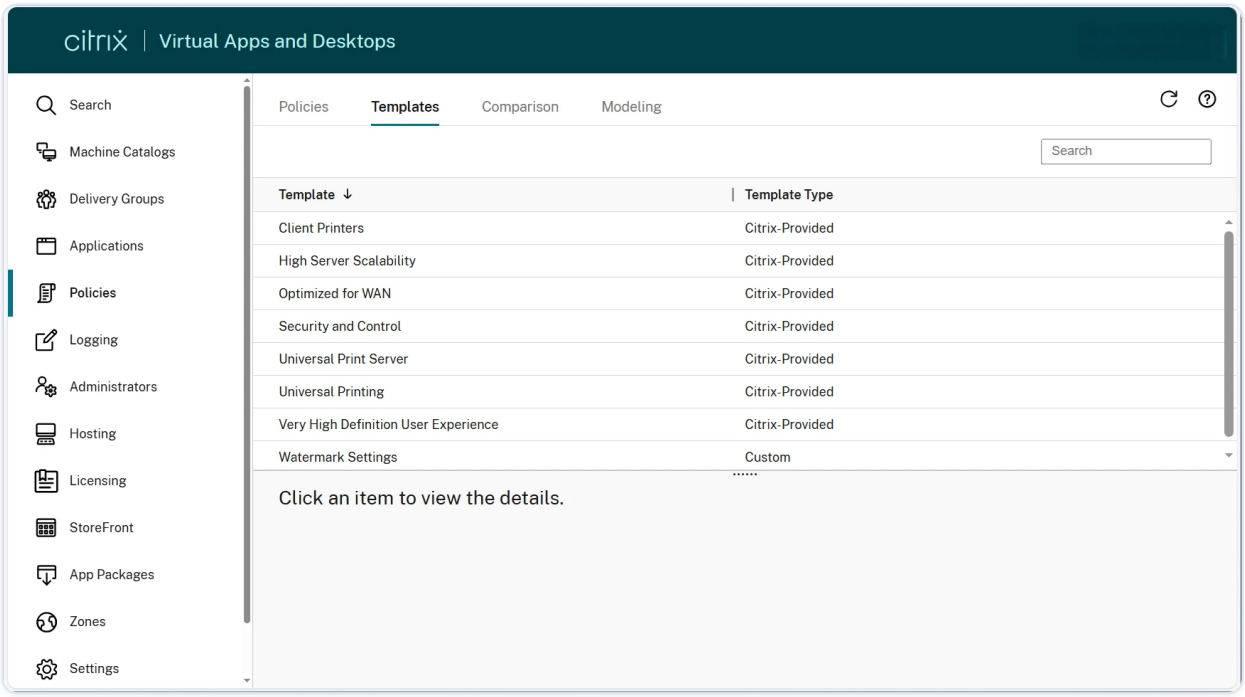
   Web Studioでポリシーを表示(/en-us/citrix-virtual-apps-desktops/2511/media/policy-migrate-example3.png)

   > **注:**
   >
   > この時点では、テンプレートはまだ**テンプレート**タブに表示されていません。ポリシーは仲介役であり、次のステップでWeb Studioテンプレートを作成するために使用します。

4. *ウォーターマーク設定*ポリシーを選択し、リボンで**...その他**を選択して**テンプレートとして保存**をクリックします。



5. ウィザードに従ってWeb Studioテンプレートを作成します。
6. 「**テンプレート**」タブを選択します。*Watermark Settings*テンプレートは、サイトにアクセスできるすべてのコンピューターから、すべての管理者が表示およびアクセスできるようになりました。



関連コンテンツ

Web Studioでのテンプレートの管理について詳しくは、「ポリシーテンプレートの管理」を参照してください。

アップグレード後に非推奨のポリシー設定を削除する

Citrix® が製品コンポーネントを非推奨にすると、関連するポリシー設定は無効になります。アップグレード後、`GpoClean.ps1` を使用して、Citrix Virtual Apps and Desktops™ ポリシーからこれらの非推奨設定を特定して削除します。これには、結果として空になるポリシーも含まれます。

始める前に

スクリプトを実行する前に、以下の要件を満たしていることを確認してください。

- **Broker SDK** と **Group Policy Management** がインストールされている、サポート対象バージョンの Citrix Virtual Apps and Desktops
- Delivery Controller™ 上の **Citrix ポリシー管理** 権限

> **注:**
>
> スクリプトは、`Citrix.Broker.Admin.V2` と `Citrix.Common.GroupPolicy` スナップインを自動的にロードします。

非推奨のポリシー設定を削除する

非推奨のポリシー設定を削除するには、`GpoClean.ps1` を実行します。

1. **Citrix policy administration** 権限を持つ Delivery Controller に `GpoClean.ps1` をコピーします。
2. Delivery Controller で PowerShell セッションを開きます。
3. スクリプトを実行します。パラメーターは不要です。

```
.\GpoClean.ps1
```

> **注:**
>
> 設定ごとの詳細なログ記録には、`-Verbose` を追加します: `.\GpoClean.ps1 -Verbose`。

スクリプトは2つのフェーズで実行されます。

フェーズ	内容
フェーズ1	`Test-BrokerDesktopPolicy`を実行し、`DeprecatedSetting`エラーを特定し、影響を受ける各設定を`NotConfigured`に設定します
フェーズ2	`Test-BrokerDesktopPolicy`を再実行し、構成された設定がないポリシー（`PolicyHasNoSettings`）を特定して削除します

すべての変更は、1回の書き込み操作で保存されます。削除された設定とポリシーの数が概要として報告されます。非推奨の設定が見つからない場合、スクリプトは変更なしで終了します。

注:

`Unfiltered`ポリシーは、構成された設定が含まれていない場合でも、削除されることはありません。

関連コンテンツ

各リリースでの非推奨設定の詳細については、「ポリシーの変更」を参照してください。

ポリシー設定リファレンス

ポリシーには、ポリシーが適用されるときに適用される設定が含まれます。このセクションの説明では、機能を有効にするためにより多くの設定が必要かどうか、または設定に類似しているかどうかも示します。

クイックリファレンス

次の表に、ポリシー内で構成できる設定を示します。左の列で完了したいタスクを見つけ、右の列で対応する設定を見つけてください。

すべてのポリシー設定の完全なリストは、.CHM (Compiled HTML) 形式および .CSV 形式で利用できます。これらのファイルは、ブローカー (デリバリーコントローラー) がインストールされているサーバーの`\program files\citrix\grouppolicy`フォルダーにあります。ポリシー設定の最新バージョンは、こちらをクリックしてダウンロードすることもできます。

オーディオ

このタスクの場合	このポリシー設定を使用する
複数のオーディオデバイスの使用を許可するかどうかを制御する	オーディオプラグアンドプレイ
ユーザーデバイスのマイクからのオーディオ入力を許可するかどうかを制御する	クライアントマイクのリダイレクト
ユーザーデバイスのオーディオ品質を制御する	オーディオ品質
ユーザーデバイスのスピーカーへのオーディオマッピングを制御する	クライアントオーディオリダイレクト

ユーザーデバイスの帯域幅

使用される帯域幅を制限するには	このポリシー設定を使用
クライアントオーディオマッピング	オーディオリダイレクト帯域幅制限またはオーディオリダイレクト帯域幅制限パーセント
ローカルクリップボードを使用した切り取りと貼り付け	クリップボードリダイレクト帯域幅制限またはクリップボードリダイレクト帯域幅制限パーセント
セッションでのローカルクライアントドライブへのアクセス	ファイルリダイレクト帯域幅制限またはファイルリダイレクト帯域幅制限パーセント
HDX™ MediaStreamマルチメディアアクセラレーション	HDX MediaStreamマルチメディアアクセラレーション帯域幅制限またはHDX MediaStreamマルチメディアアクセラレーション帯域幅制限パーセント
クライアントセッション	セッション全体の帯域幅制限
印刷	プリンターリダイレクト帯域幅制限またはプリンターリダイレクト帯域幅制限率
TWAINデバイス（カメラやスキャナーなど）	TWAINデバイスリダイレクト帯域幅制限またはTWAINデバイスリダイレクト帯域幅制限率

使用される帯域幅を制限するには	このポリシー設定を使用
USBデバイス	クライアントUSBデバイスリダイレクト帯域幅制限またはクライアントUSBデバイスリダイレクト帯域幅制限率

クライアントドライブとユーザーデバイスのリダイレクト

このタスクの場合	このポリシー設定を使用する
ユーザーがサーバーにログオンしたときに、ユーザーデバイス上のドライブが接続されるかどうかを制御します	クライアントドライブの自動接続
サーバーとローカルクリップボード間での切り取りと貼り付けによるデータ転送を制御します	クライアントクリップボードリダイレクト
ユーザーデバイスからドライブがマップされる方法を制御します	クライアントドライブリダイレクト
セッション内でユーザーのローカルハードドライブが利用可能かどうかを制御します	クライアント固定ドライブとクライアントドライブリダイレクト
ユーザーのローカルフロッピーディスクドライブがセッションで利用可能かどうかを制御します	クライアントフロッピーディスクドライブとクライアントドライブリダイレクト
ユーザーのネットワークドライブがセッションで利用可能かどうかを制御します	クライアントネットワークドライブとクライアントドライブリダイレクト
ユーザーのローカルCD、DVD、またはBlu-rayドライブがセッションで利用可能かどうかを制御します	クライアント光学ドライブとクライアントドライブリダイレクト
ユーザーのローカルリムーバブルドライブがセッションで利用可能かどうかを制御します	クライアントリムーバブルドライブとクライアントドライブリダイレクト
ユーザーのTWAINデバイス（スキャナーやカメラなど）がセッションで利用可能かどうかを制御し、画像データ転送の圧縮を制御します	クライアントTWAINデバイスリダイレクト；TWAIN圧縮リダイレクト

このタスクの場合	このポリシー設定を使用する
USBデバイスがセッションで利用可能かどうかを制御します	クライアントUSBデバイスリダイレクトとクライアントUSBデバイスリダイレクト規則
WAN経由でのクライアントディスクへのファイルの書き込みとコピーの速度を向上させます	非同期書き込みを使用します

コンテンツリダイレクト

このタスクの場合	このポリシー設定を使用する
サーバーからユーザーデバイスへのコンテンツリダイレクトを使用するかどうかを制御します	ホストからクライアントへのリダイレクト

デスクトップUI

このタスクの場合	このポリシー設定を使用する
ユーザーセッションでデスクトップの壁紙を使用するかどうかを制御します	デスクトップの壁紙
ウィンドウのドラッグ中にウィンドウの内容を表示する	ドラッグ中のウィンドウの内容を表示

グラフィックとマルチメディア

> **重要:**

> Flashポリシーは、古いVDAを使用している顧客が新しいコントローラー（たとえば、バージョン1912コントローラー）を使用し、引き続きFlashを使用できるようにするためにのみ残されています。このVDAバージョンはFlashをサポートしていません。

このタスクの場合	このポリシー設定を使用します
仮想デスクトップからユーザーデバイスに送信される1秒あたりの最大フレーム数を制御します	ターゲットフレームレート
ユーザーデバイスに表示される画像の視覚的な品質を制御します	視覚的品質
セッションでアクセスしたときにWebサイトがFlashコンテンツを表示できるかどうかを制御します	Flashサーバー側コンテンツ取得URLリスト。Flash URL互換性リスト。Flashビデオフォールバック防止ポリシー設定。Flashビデオフォールバック防止エラー*.swf
サーバーでレンダリングされたビデオの圧縮を制御します	圧縮にビデオコーデックを使用。ビデオコーデックにハードウェアエンコードを使用
HTML5マルチメディアWebコンテンツのユーザーへの配信を制御します	HTML5ビデオのリダイレクト

マルチストリームネットワークトラフィックの優先順位付け

このタスクの場合	このポリシー設定を使用
複数の接続にわたるICA®トラフィックのポートを指定し、ネットワークの優先順位を確立します	マルチポートポリシー
サーバーとユーザーデバイス間のマルチストリーム接続のサポートを有効にします	マルチストリーム（コンピューターおよびユーザー設定）

印刷

このタスクの場合	このポリシー設定を使用します
ユーザーデバイスでのクライアントプリンターの作成を制御します	クライアントプリンターの自動作成とクライアントプリンターのリダイレクト
プリンタープロパティの保存場所を制御します	プリンタープロパティの保持

このタスクの場合	このポリシー設定を使用します
クライアントまたはサーバーのどちらが印刷要求を処理するかを制御します	印刷サーバーへの直接接続
ユーザーが自分のユーザーデバイスに接続されているプリンターにアクセスできるかどうかを制御します	クライアントプリンターのリダイレクト
クライアントプリンターとネットワークプリンターを自動的に作成する際のネイティブWindowsドライバーのインストールを制御します。	インボックスプリンタードライバーの自動インストール
ユニバーサルプリンタードライバーを使用するタイミングを制御します。	ユニバーサルプリントドライバーの使用
ローミングユーザーセッション情報に基づいてプリンターを選択します。	デフォルトプリンター
ユニバーサルプリントサーバーの負荷分散とフェイルオーバーしきい値の設定	負荷分散用のユニバーサルプリントサーバー。ユニバーサルプリントサーバーのサービス停止しきい値

注:

ポリシーを使用して、デスクトップまたはアプリケーションセッションでスクリーンセーバーを有効にすることはできません。スクリーンセーバーを必要とするユーザーの場合、スクリーンセーバーはユーザーデバイス上で実装できます。

デフォルトポリシー設定

以下の表は、ポリシー設定、そのデフォルト値、およびそれらが適用されるVirtual Delivery Agent (VDA) のバージョンを示しています。

ICA®

名前	デフォルト設定	VDA
アダプティブトランスポート	オフ。優先される場合に使用します	VDA 7.13〜7.15、VDA 7.16以降
クライアントクリップボードリダイレクト	許可	すべてのVDAバージョン
クライアントクリップボード書き込み許可形式	形式は指定されていません	VDA 7.6以降
デスクトップの起動	禁止	マルチセッションOS用VDA 7以降
ICAリスナーポート番号	1494	すべてのVDAバージョン
クライアント接続中の非公開プログラムの起動	禁止	マルチセッションOS用VDA 7以降
クリップボードのクライアントからセッションへの転送サイズを制限	無効	VDA 2009
クリップボードのセッションからクライアントへの転送サイズを制限	無効	VDA 2009
損失許容モード	許可	VDA 2003。注: 損失許容モードはまだ利用できません。このバージョンのVDAは、利用可能になった際にサポートします。
損失許容しきい値	損失許容モードが利用可能な場合: パケット損失: 5%、遅延: 300 ms (RTT)	VDA 2003以降
Rendezvousプロトコル	無効	Citrix Cloudを介して確立されたHDXセッションにのみ適用されます。

名前	デフォルト設定	VDA
クライアントクリップボードへの書き込みを制限	禁止	VDA 7.6以降
セッションクリップボードへの書き込みを制限	禁止	VDA 7.6以降
セッションクリップボード書き込み許可形式	形式は指定されていません	VDA 7.6以降
タブレットモードの切り替え	有効	VDA 7.16以降。VDA 7.14および7.15 LTSRの場合は、レジストリを使用してこの設定を構成します。
仮想チャネル許可リスト	有効	VDA 2109以降
セッションメトリック収集	許可	7.42以降

ICA/アドビ フラッシュ配信/フラッシュ リダイレクト

名前	デフォルト設定	VDA
Flashビデオのフォールバック防止	未構成	VDA 7.6 FP3 から現在まで
Flashビデオのフォールバック防止エラー *.swf	VDA 7.6 FP3 から現在まで	

ICA/オーディオ

名前	デフォルト設定	VDA
アダプティブオーディオ	有効	Citrix Virtual Apps and Desktops™ 2109以降を使用するVDAの、シングルセッションOSおよびマルチセッションOSの両方のセッションに適用されます。
UDPリアルタイムトランスポート経由のオーディオ	許可	すべてのVDAバージョン

名前	デフォルト設定	VDA
オーディオプラグアンドプレイ	許可	マルチセッションOS 7以降のVDA
オーディオ品質	高 - 高精細オーディオ	すべてのVDAバージョン
クライアントオーディオリダイレクト	許可	すべてのVDAバージョン
クライアントマイクのリダイレクト	許可	すべてのVDAバージョン
オーディオの損失許容モード	禁止	VDAバージョン2411およびそれ以前

ICA/自動クライアント再接続

名前	デフォルト設定	VDA
自動クライアント再接続	許可	すべてのVDAバージョン
自動クライアント再接続認証	認証を要求しない	すべてのVDAバージョン
自動クライアント再接続ログ	自動再接続イベントをログに記録しない	すべてのVDAバージョン
自動クライアント再接続タイムアウト	120秒	VDA 7.13から現在まで
再接続UIの透明度レベル	80%	VDA 7.13から現在まで

ICA/帯域幅

名前	デフォルト設定	VDA
オーディオリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
オーディオリダイレクト帯域幅制限（パーセント）	0	すべてのVDAバージョン

名前	デフォルト設定	VDA
クライアントUSBデバイスリダイレクト帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
クライアントUSBデバイスリダイレクト帯域幅制限の割合	0	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
クリップボードリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
クリップボードリダイレクト帯域幅制限の割合	0	すべてのVDAバージョン
COMポートリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン。VDA 7.0～7.8の場合、この設定はレジストリを使用して構成します。
COMポートリダイレクト帯域幅制限（パーセント）	0	すべてのVDAバージョン。VDA 7.0から7.8については、レジストリを使用してこの設定を構成します
ファイルリダイレクト帯域幅制限	ゼロ Kbps	すべてのVDAバージョン
ファイルリダイレクト帯域幅制限（パーセント）	0	すべてのVDAバージョン
HDX MediaStreamマルチメディアアクセラレーション帯域幅制限	ゼロ Kbps	VDA 5.5、5.6 FP1、マルチセッションOS向けVDA 7およびシングルセッションOS向けVDA 7から現在のマルチセッションOS向けVDAおよびシングルセッションOS向けVDAまで

名前	デフォルト設定	VDA
HDX MediaStreamマルチメディアアクセラレーション帯域幅制限（パーセント）	0	VDA 5.5、5.6 FP1、マルチセッションOS向けVDA 7から現在まで、シングルセッションOS向けVDA 7から現在まで
LPTポートリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン。VDA 7.0～7.8の場合、この設定はレジストリを使用して構成します
LPTポートリダイレクト帯域幅制限の割合	0	すべてのVDAバージョン。VDA 7.0～7.8の場合、この設定はレジストリを使用して構成します
セッション全体の帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
プリンターリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
プリンターリダイレクト帯域幅制限の割合	0	すべてのVDAバージョン
TWAIN デバイスリダイレクト帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
TWAIN デバイスリダイレクト帯域幅制限の割合	0	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/双方向コンテンツリダイレクト

名前	デフォルト設定	VDA
双方向コンテンツリダイレクトを許可する	禁止	VDA 7.13以降

名前	デフォルト設定	VDA
クライアントにリダイレクトされる許可されたURL	空白	VDA 7.13 以降
VDAにリダイレクトされる許可されたURL	空	VDA 7.13 以降
双方向コンテンツリダイレクト構成	無効	VDA 2311 以降

ICA/ブラウザコンテンツリダイレクト

名前	デフォルト設定	VDA
ブラウザコンテンツリダイレクト	許可	VDA 7.16 以降
ブラウザコンテンツリダイレクトACL構成	`https://www.youtube.com/*`	VDA 7.16 以降
ブラウザコンテンツリダイレクトの統合Windows認証サポート	禁止	VDA 2106 以降
ブラウザコンテンツリダイレクトのプロキシ構成	空	VDA 7.16 以降
ブラウザコンテンツリダイレクトのサーバーフェッチWebプロキシ認証	禁止	VDA 2012 以降

ICA/クライアントセンサー

名前	デフォルト設定	VDA
アプリケーションがクライアントデバイスの物理的な位置情報を使用することを許可する	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/デスクトップUI

名前	デフォルト設定	VDA
デスクトップコンポジションリダイレクト	無効 (7.6 FP3以降); 有効 (5.6から7.6 FP2まで)	VDA 5.6、シングルセッションOS用VDA 7から7.15まで
デスクトップコンポジションリダイレクトのグラフィック品質	中	VDA 5.6、シングルセッションOS用VDA 7から7.15まで
デスクトップの壁紙	許可	すべてのVDAバージョン
メニューアニメーション	許可	すべてのVDAバージョン
ドラッグ中にウィンドウの内容を表示	許可	すべてのVDAバージョン

ICA/エンドユーザー監視

名前	デフォルト設定	VDA
ICAラウンドトリップ計算	有効	すべてのVDAバージョン
ICAラウンドトリップ計算間隔	15秒	すべてのVDAバージョン
アイドル接続のICAラウンドトリップ計算	無効	すべてのVDAバージョン

ICA/強化されたデスクトップエクスペリエンス

名前	デフォルト設定	VDA
拡張デスクトップエクスペリエンス	許可	マルチセッションOS 7以降のVDA

ICA/ファイルリダイレクト

名前	デフォルト設定	VDA
クライアントドライブの自動接続	許可	すべてのVDAバージョン

名前	デフォルト設定	VDA
クライアントドライブのリダイレクト	許可	すべてのVDAバージョン
クライアントの固定ドライブ	許可	すべてのVDAバージョン
クライアントのフロッピーディスクドライブ	許可	すべてのVDAバージョン
クライアントのネットワークドライブ	許可	すべてのVDAバージョン
クライアントの光学ドライブ	許可	すべてのVDAバージョン
クライアントのリムーバブルドライブ	許可	すべてのVDAバージョン
ホストからクライアントへのリダイレクト	無効	マルチセッションOS用VDA 7以降
クライアントドライブ文字の保持	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
クライアントドライブへの読み取り専用アクセス	無効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
特殊フォルダーのリダイレクト	許可	Web Interface展開のみ。マルチセッションOS用VDA 7以降
非同期書き込みの使用	無効	すべてのVDAバージョン

ICA/グラフィック

名前	デフォルト設定	VDA
視覚的にロスレスな圧縮を許可	無効	VDA 7.6以降

名前	デフォルト設定	VDA
表示メモリ制限	65,536 Kb	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
表示モードの劣化の優先順位	まず色深度を劣化させる	すべてのVDAバージョン
動的ウィンドウプレビュー	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
グラフィックステータスインジケーター	無効	VDA 7.16以降
イメージキャッシュ	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
レガシーグラフィックモード	無効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
最大許容色深度	32ビット/ピクセル	すべてのVDAバージョン
ディスプレイモードが低下した場合にユーザーに通知	無効	マルチセッションOS用VDA 7以降
3Dグラフィックワークロード向けに最適化	無効	VDA 7.17以降
キューイングとトッシング	有効	すべてのVDAバージョン
画面共有	無効	VDA 2112
圧縮にビデオコーデックを使用	優先される場合にビデオコーデックを使用	VDA 7.6 FP3から現在まで
ビデオコーデックにハードウェアエンコードを使用	有効	VDA 7.11から現在まで

ICA/グラフィック/キャッシュ

名前	デフォルト設定	VDA
永続キャッシュしきい値	3,000,000 ビット/秒	マルチセッションOS用VDA 7から現在まで

ICA/グラフィックス/Framehawk

名前	デフォルト設定	VDA
Framehawkディスプレイチャネル	無効	VDA 7.6 FP2 以降
Framehawkディスプレイチャネルのポート範囲	3224,3324	VDA 7.6 FP2 以降

ICA/キープアライブ

名前	デフォルト設定	VDA
ICAキープアライブタイムアウト	60秒	すべてのVDAバージョン
ICAキープアライブ	ICAキープアライブメッセージを送信しない	すべてのVDAバージョン

ICA/キーボードおよびIME

名前	デフォルト設定	VDA
クライアントキーボードレイアウト同期およびIMEの改善	無効	1912 LTSR CU2以降にのみ適用されます。
Unicodeキーボードレイアウトマッピング	許可 (2407, 2411, 2503); 禁止 (以前のバージョン, 2507)	1912 LTSR CU2以降にのみ適用されます。
キーボードレイアウト切り替えポップアップメッセージボックスを非表示にする	禁止	1912 LTSR CU2以降にのみ適用されます。

ICA/ローカルアプリアクセス

名前	デフォルト設定	VDA
ローカルアプリアクセスを許可	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
URLリダイレクトブロックリスト	サイトは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
URLリダイレクト許可リスト	サイトは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/モバイルエクスペリエンス

名前	デフォルト設定	VDA
自動キーボード表示	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
タッチ最適化デスクトップの起動	許可	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降。この設定は無効になっており、Windows 10およびWindows Server 2016マシンでは利用できません。
コンボボックスのリモート処理	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/マルチメディア

名前	デフォルト設定	VDA
HTML5 ビデオリダイレクト	禁止	VDA 7.12 から現在まで

名前	デフォルト設定	VDA
ビデオ品質の制限	未構成	マルチセッションOS用VDA 7から現在まで、シングルセッションOS用VDA 7から現在まで
Microsoft Teams リダイレクト	許可	マルチセッションOS用VDA 1906から現在まで、シングルセッションOS用VDA 1906から現在まで。
マルチメディア会議	許可	すべてのVDAバージョン
WAN経由のWindows Media マルチメディアリダイレクトの最適化	許可	マルチセッションOS用VDA 7～現在、シングルセッションOS用VDA 7～現在
WAN経由のWindows Media マルチメディアリダイレクトの最適化にGPUを使用	禁止	マルチセッションOS用VDA 7～現在、シングルセッションOS用VDA 7～現在
Windows Mediaフォールバック防止	未構成	VDA 7.6 FP3～現在
Windows Mediaクライアント側コンテンツフェッチ	許可	マルチセッションOS用VDA 7～現在、シングルセッションOS用VDA 7～現在
Windows Mediaリダイレクト	許可	すべてのVDAバージョン
Windows Mediaリダイレクトバッファサイズ	5秒	VDA 5、5.5、5.6 FP1から現在まで
Windows Mediaリダイレクトバッファサイズの使用	無効	VDA 5、5.5、5.6 FP1から現在まで

ICA/マルチストリーム接続

名前	デフォルト設定	VDA
UDP経由のオーディオ	許可	マルチセッションOS 7以降のVDA

名前	デフォルト設定	VDA
オーディオUDPポート範囲	16500、16509	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
マルチポートポリシー	プライマリポート (2598) は高優先度です	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
マルチストリームコンピューター設定	無効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
マルチストリームユーザー設定	無効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
マルチストリーム仮想チャネルストリーム割り当て設定	デフォルトのストリーム割り当てについては、Multi-Stream virtual channel assignment setting を参照してください	VDA 2003

ICA/ポートリダイレクト

名前	デフォルト設定	VDA
クライアントCOMポートの自動接続	無効	すべてのVDAバージョン。VDA 7.0〜7.8の場合、この設定はレジストリを使用して構成します
クライアントLPTポートの自動接続	無効	すべてのVDAバージョン。VDA 7.0〜7.8の場合、この設定はレジストリを使用して構成します

名前	デフォルト設定	VDA
クライアントCOMポートのリダイレクト	禁止	すべてのVDAバージョン。VDA 7.0～7.8の場合、この設定はレジストリを使用して構成します
クライアントLPTポートのリダイレクト	禁止	すべてのVDAバージョン。VDA 7.0～7.8の場合、この設定はレジストリを使用して構成します

ICA/印刷

名前	デフォルト設定	VDA
クライアントプリンターリダイレクト	許可	すべてのVDAバージョン
デフォルトプリンター	デフォルトプリンターをクライアントのメインプリンターに設定	すべてのVDAバージョン
プリンターの割り当て	ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用される	すべてのVDAバージョン
プリンターの自動作成イベントログ設定	エラーと警告をログに記録	すべてのVDAバージョン
セッションプリンター	プリンターは指定されていません	すべてのVDAバージョン
プリンターが作成されるまで待機する（デスクトップ）	無効	すべてのVDAバージョン

ICA/印刷/クライアントプリンター

名前	デフォルト設定	VDA
クライアントプリンターを自動作成する	すべてのクライアントプリンターを自動作成する	すべてのVDAバージョン

名前	デフォルト設定	VDA
汎用ユニバーサルプリンターを自動作成する	無効	すべてのVDAバージョン
クライアントプリンター名	標準プリンター名	VDA 5.6
印刷サーバーへの直接接続	有効	すべてのVDAバージョン
プリンタードライバーのマッピングと互換性	ルールは指定されていません	すべてのVDAバージョン
プリンタープロパティの保持	クライアントに保存されていない場合にのみプロファイルに保持	すべてのVDAバージョン
保持および復元されたクライアントプリンター	許可	VDA 5、5,5、5.6 FP1

ICA/Printing/Drivers

名前	デフォルト設定	VDA
インボックスプリンタードライバーの自動インストール	有効	すべてのVDAバージョン
ユニバーサルドライバーの優先順位	イーエムエフ; エックスピーエス; ピーシーエルファイブシー; ピーシーエルフォー; ピーエス	すべてのVDAバージョン
ユニバーサルプリントドライバーの使用	要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用する	すべてのVDAバージョン

ICA/印刷/ユニバーサルプリントサーバー

名前	デフォルト設定	VDA
Universal Print Serverの有効化	無効	すべてのVDAバージョン

名前	デフォルト設定	VDA
Universal Print Server印刷データストリーム (CGP) ポート	7229	すべてのVDAバージョン
Universal Print Server印刷ストリーム入力帯域幅制限 (kbps)	0	すべてのVDAバージョン
Universal Print Server Web サービス (HTTP/SOAP) ポート	8080	すべてのVDAバージョン
ロードバランシング用ユニバーサルプリントサーバー	VDAバージョン7.9から現在まで	
ユニバーサルプリントサーバーのサービス停止しきい値	180 (秒)	VDAバージョン7.9から現在まで

ICA/印刷/ユニバーサル印刷

名前	デフォルト設定	VDA
ユニバーサル印刷EMF処理モード	プリンターに直接スプール	すべてのVDAバージョン
ユニバーサル印刷画像圧縮制限	最高品質 (ロスレス圧縮)	すべてのVDAバージョン
ユニバーサル印刷の最適化のデフォルト	画像圧縮: 希望する画質 = 標準品質、ヘビーウェイト圧縮を有効にする = False; 画像とフォントのキャッシュ: 埋め込み画像のキャッシュを許可する = True; 管理者以外のユーザーによるこれらの設定の変更を許可する = False;	すべてのVDAバージョン
ユニバーサル印刷のプレビュー設定	自動作成されたプリンターまたは汎用ユニバーサルプリンターでは印刷プレビューを使用しない	すべてのVDAバージョン

名前	デフォルト設定	VDA
ユニバーサル印刷の印刷品質制限	制限なし	すべてのVDAバージョン

ICA/セキュリティ

名前	デフォルト設定	VDA
SecureICAの最小暗号化レベル	基本	マルチセッションOS用VDA 7以降

ICA/サーバー制限

名前	デフォルト設定	VDA
サーバーアイドルタイマー間隔	0ミリ秒	マルチセッションOS用VDA 7以降

ICA/セッション制限

名前	デフォルト設定	VDA
切断されたセッションタイマー	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
リモートPCアクセス切断セッションタイマー	無効	シングルセッションOS用VDA 7以降
切断セッションタイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッション接続タイマー	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッション接続タイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
セッションアイドルタイマー	有効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッションアイドルタイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降

ICA/セッションの信頼性

名前	デフォルト設定	VDA
セッションの信頼性接続	許可	すべてのVDAバージョン
セッションの信頼性ポート番号	2598	すべてのVDAバージョン
セッションの信頼性タイムアウト	180秒	すべてのVDAバージョン

ICA/タイムゾーン制御

名前	デフォルト設定	VDA
レガシークライアントのローカル時刻を推定する	有効	マルチセッションOS 7以降のVDA
セッション切断またはログオフ時にシングルセッションOSのタイムゾーンを復元する	有効	現在のVDAバージョン
クライアントのローカル時刻を使用する	サーバーのタイムゾーンを使用する	すべてのVDAバージョン

ICA/TWAINデバイス

名前	デフォルト設定	VDA
クライアントTWAINデバイスリダイレクト	許可	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
TWAIN圧縮レベル	中	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/USBデバイス

名前	デフォルト設定	VDA
クライアントUSBデバイス最適化ルール	有効 (VDA 7.6 FP3以降); 無効 (VDA 7.11以降); デフォルトでは、ルールは指定されていません	VDA 7.6 FP3 以降
クライアントUSBデバイスリダイレクト	禁止	すべてのVDAバージョン
クライアントUSBデバイスリダイレクト規則	規則は指定されていません	すべてのVDAバージョン
クライアントUSBプラグアンドプレイデバイスリダイレクト	許可	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/ビジュアルディスプレイ

名前	デフォルト設定	VDA
簡易グラフィックの優先色深度	ピクセルあたり24ビット	VDA 7.6 FP3から現在まで
ターゲットフレームレート	30 フレーム/秒	すべてのVDAバージョン

名前	デフォルト設定	VDA
視覚品質	中	マルチセッションOS用VDA 7から現在まで、シングルセッションOS用VDA 7から現在まで

ICA/ビジュアルディスプレイ/動画

名前	デフォルト設定	VDA
最小画像品質	標準	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7から現在まで、シングルセッションOS用VDA 7から現在まで
動画圧縮	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
プログレッシブ圧縮レベル	なし	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
プログレッシブ圧縮しきい値	2,147,483,647 キロビット/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
目標最小フレームレート	10 フレーム/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

注:

目標最小フレームレートポリシーは非推奨になりました。

ICA/視覚表示/静止画像

名前	デフォルト設定	VDA
追加の色圧縮	無効	すべてのVDAバージョン
追加の色圧縮のしきい値	8,192 キロビット/秒	すべてのVDAバージョン
高負荷圧縮	無効	すべてのVDAバージョン
非可逆圧縮レベル	中	すべてのVDAバージョン
非可逆圧縮しきい値	2,147,483,647 ケービーピーエス	すべてのVDAバージョン

ICA/WebSockets

名前	デフォルト設定	VDA
WebSockets接続	禁止	マルチセッションOS 7以降のVDA、シングルセッションOS 7以降のVDA
WebSocketsポート番号	8008	マルチセッションOS 7以降のVDA、シングルセッションOS 7以降のVDA
WebSockets信頼済みオリジンサーバーリスト	ワイルドカード「*」は、すべてのReceiver for Web URLを信頼するために使用されます	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

負荷管理

名前	デフォルト設定	VDA
同時ログオン許容数	2	マルチセッションOS用VDA 7以降
CPU使用率	無効	マルチセッションOS用VDA 7以降

名前	デフォルト設定	VDA
CPU使用率から除外されるプロセスの優先度	標準以下または低	マルチセッションOS用VDA 7以降
ディスク使用量	無効	マルチセッションOS用VDA 7以降
最大セッション数	250	マルチセッションOS用VDA 7以降
メモリ使用量	無効	マルチセッションOS用VDA 7以降
メモリ使用量のベース負荷	ゼロ負荷: 768 MB	マルチセッションOS用VDA 7以降

プロファイル管理/詳細設定

名前	デフォルト設定	VDA
自動構成を無効にする	無効	すべてのVDAバージョン
問題が発生した場合にユーザーをログオフする	無効	すべてのVDAバージョン
ロックされたファイルへのアクセス時の再試行回数	5	すべてのVDAバージョン
ログオフ時にインターネットCookieファイルを処理する	無効	すべてのVDAバージョン

プロファイル管理/基本設定

名前	デフォルト設定	VDA
アクティブライトバック	無効	すべてのVDAバージョン
プロファイル管理を有効にする	無効	すべてのVDAバージョン

名前	デフォルト設定	VDA
除外されたグループ	無効。すべてのユーザーグループのメンバーが処理されます。	すべてのVDAバージョン
オフラインプロファイルサポート	無効	すべてのVDAバージョン
ユーザーストアへのパス	ウィンドウズ	すべてのVDAバージョン
ローカル管理者のログオンを処理する	無効	すべてのVDAバージョン
処理されたグループ	無効。すべてのユーザーグループのメンバーが処理されます。	すべてのVDAバージョン

プロファイル管理/クロスプラットフォーム設定

名前	デフォルト設定	VDA
クロスプラットフォーム設定ユーザーグループ	無効。処理済みグループで指定されたすべてのユーザーグループが処理されます	すべてのVDAバージョン
クロスプラットフォーム設定を有効にする	無効	すべてのVDAバージョン
クロスプラットフォーム定義へのパス	無効。パスは指定されていません。	すべてのVDAバージョン
クロスプラットフォーム設定ストアへのパス	無効。Windows\PM_CMが使用されます。	すべてのVDAバージョン
クロスプラットフォーム設定作成のソース	無効	すべてのVDAバージョン

プロファイル管理/ファイルシステム/除外

名前	デフォルト設定	VDA
除外リスト - ディレクトリ	無効。ユーザープロファイル内のすべてのフォルダーが同期されます。	すべてのVDAバージョン
除外リスト - ファイル	無効。ユーザープロファイル内のすべてのファイルが同期されます。	すべてのVDAバージョン

プロファイル管理/ファイルシステム/同期

名前	デフォルト設定	VDA
同期するディレクトリ	無効。除外されていないフォルダーのみが同期されます。	すべてのVDAバージョン
同期するファイル	無効。除外されていないファイルのみが同期されます。	すべてのVDAバージョン
ミラーリングするフォルダー	無効。フォルダーはミラーリングされません。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト

名前	デフォルト設定	VDA
管理者アクセスを許可する	無効	すべてのVDAバージョン
ドメイン名を含める	無効	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/AppData(Roaming)

名前	デフォルト設定	VDA
AppData(Roaming)パス	無効。場所は指定されていません。	すべてのVDAバージョン
AppData(Roaming)のリダイレクト設定	コンテンツは、AppData(Roaming)パスのポ	すべてのVDAバージョン

名前	デフォルト設定	VDA
	リシー設定で指定されたUNCパスにリダイレクトされます	

プロファイル管理/フォルダーリダイレクト/連絡先

名前	デフォルト設定	VDA
連絡先パス	無効。場所は指定されていません。	すべてのVDAバージョン
連絡先のリダイレクト設定	コンテンツは、**連絡先パス ポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダー リダイレクト/デスクトップ

名前	デフォルト設定	VDA
デスクトップパス	無効。場所は指定されていません。	すべてのVDAバージョン
デスクトップのリダイレクト設定	コンテンツは、**デスクトップパス ポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダー リダイレクト/ドキュメント

名前	デフォルト設定	VDA
ドキュメントパス	無効。場所は指定されていません。	すべてのVDAバージョン
ドキュメントのリダイレクト設定	コンテンツは、**ドキュメントパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ダウンロード

名前	デフォルト設定	VDA
ダウンロードパス	無効。場所は指定されていません。	すべてのVDAバージョン
ダウンロードのリダイレクト設定	コンテンツは、**ダウンロードパスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/お気に入り

名前	デフォルト設定	VDA
お気に入りパス	無効。場所は指定されていません。	すべてのVDAバージョン
お気に入りのリダイレクト設定	コンテンツは、**お気に入りパスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/リンク

名前	デフォルト設定	VDA
リンクパス	無効。場所は指定されていません。	すべてのVDAバージョン
リンクのリダイレクト設定	コンテンツは、**リンクパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ミュージック

名前	デフォルト設定	VDA
ミュージックパス	無効。場所は指定されていません。	すべてのVDAバージョン

名前	デフォルト設定	VDA
ミュージックのリダイレクト設定	コンテンツは、**ミュージックパスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ピクチャ

名前	デフォルト設定	VDA
ピクチャパス	無効。場所は指定されていません。	すべてのVDAバージョン
ピクチャのリダイレクト設定	コンテンツは、**ピクチャパスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/保存されたゲーム

名前	デフォルト設定	VDA
保存されたゲームパス	無効。場所は指定されていません。	すべてのVDAバージョン
保存されたゲームのリダイレクト設定	コンテンツは、「**保存されたゲームパスポリシー**」設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/検索

名前	デフォルト設定	VDA
検索パス	無効。場所は指定されていません。	すべてのVDAバージョン
検索のリダイレクト設定	コンテンツは、**検索パスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/スタートメニュー

名前	デフォルト設定	VDA
スタートメニューパス	無効。場所は指定されていません。	すべてのVDAバージョン
スタートメニューのリダイレクト設定	コンテンツは、スタートメニューパスポリシー設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ビデオ

名前	デフォルト設定	VDA
ビデオパス	無効。場所は指定されていません。	すべてのVDAバージョン
ビデオのリダイレクト設定	コンテンツは、**ビデオパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/ログ設定

名前	デフォルト設定	VDA
Active Directory のアクション	無効	すべてのVDAバージョン
一般情報	無効	すべてのVDAバージョン
一般的な警告	無効	すべてのVDAバージョン
ログの有効化	無効	すべてのVDAバージョン
ファイルシステムのアクション	無効	すべてのVDAバージョン
ファイルシステム通知	無効	すべてのVDAバージョン
ログオフ	無効	すべてのVDAバージョン
ログオン	無効	すべてのVDAバージョン

名前	デフォルト設定	VDA
ログファイルの最大サイズ	1048576	すべてのVDAバージョン
ログファイルへのパス	無効。ログファイルはデフォルトの場所 (%SystemRoot%\System32\Logfiles\UserProfileManager) に保存されます。	すべてのVDAバージョン
パーソナライズされたユーザー情報	無効	すべてのVDAバージョン
ログオン時およびログオフ時のポリシー値	無効	すべてのVDAバージョン
レジストリアクション	無効	すべてのVDAバージョン
ログオフ時のレジストリの相違点	無効	すべてのVDAバージョン

プロファイル管理/プロファイルの処理

名前	デフォルト設定	VDA
キャッシュされたプロファイルを削除するまでの遅延	0	すべてのVDAバージョン
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効	すべてのVDAバージョン
ローカルプロファイルの競合処理	ローカルプロファイルを使用する	すべてのVDAバージョン
既存のプロファイルの移行	ローカルおよび移動	すべてのVDAバージョン
テンプレートプロファイルへのパス	無効。新しいユーザープロファイルは、ユーザーが最初にログオンするデバイスのデフォルトユーザープロファイルから作成されます。	すべてのVDAバージョン

名前	デフォルト設定	VDA
テンプレートプロファイルがローカルプロファイルを上書きする	無効	すべてのVDAバージョン
テンプレートプロファイルが移動プロファイルを上書きする	無効	すべてのVDAバージョン
すべてのログオンでCitrix®必須プロファイルとして使用されるテンプレートプロファイル	無効	すべてのVDAバージョン

プロファイル管理/レジストリ

名前	デフォルト設定	VDA
除外リスト	無効。ユーザーがログオフすると、HKCUハイブ内のすべてのレジストリキーが処理されます。	すべてのVDAバージョン
インクルージョンリスト	無効。ユーザーがログオフすると、HKCUハイブ内のすべてのレジストリキーが処理されます。	すべてのVDAバージョン

プロファイル管理/ストリーム配信ユーザープロファイル

名前	デフォルト設定	VDA
常にキャッシュ	無効	すべてのVDAバージョン
常にキャッシュサイズ	0 Mb	すべてのVDAバージョン
プロファイルストリーミング	無効	すべてのVDAバージョン
ストリーミングされたユーザープロファイルグループ	無効。OU内のすべてのユーザープロファイルは通常どおり処理されます。	すべてのVDAバージョン

名前	デフォルト設定	VDA
保留中のエリアロックファイルのタイムアウト (日数)	1日	すべてのVDAバージョン

レシーバー

名前	デフォルト設定	VDA
StoreFront™アカウントリスト	ストアは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ユーザーパーソナライゼーションレイヤー

名前	デフォルト設定	VDA
ユーザーレイヤーリポジトリパス	無効。パスは指定されていません。	VDA 19.12以降のバージョン
ユーザーレイヤーサイズ（GB）	10 GB。ユーザーレイヤーは、設定されたサイズまで拡張するシンプロビジョニングディスクです。ユーザーレイヤーのサイズが小さくなることはありません。	VDA 19.12以降のバージョン

仮想配信エージェント

名前	デフォルト設定	VDA
コントローラー登録IPv6ネットマスク	ネットマスクは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
コントローラー登録ポート	80	すべてのVDAバージョン
コントローラーSID	SIDは指定されていません	すべてのVDAバージョン
コントローラー	コントローラーは指定されていません	すべてのVDAバージョン

名前	デフォルト設定	VDA
コントローラーの自動更新を有効にする	有効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
IPv6コントローラー登録のみを使用する	無効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
サイトGUID	GUIDは指定されていません	すべてのVDAバージョン

バーチャル デリバリー エージェント/HDX 3D Pro

名前	デフォルト設定	VDA
ロスレスを有効にする	有効	VDA 5.5、5.6 FP1
HDX 3D Pro品質設定	VDA 5.5、5.6 FP1	

仮想配信エージェント/監視

名前	デフォルト設定	VDA
プロセス監視を有効にする	無効	VDA 7.11以降
リソース監視を有効にする	有効	VDA 7.11以降

仮想IP

名前	デフォルト設定	VDA
仮想IPループバックサポート	無効	VDA 7.6から現在まで
仮想IP仮想ループバックプログラムリスト	なし	VDA 7.6 から現在まで

ICA® ポリシー設定

> **注:**

> このページでは、ICAポリシー設定の説明とサポートされている構成値を提供します。ポリシーの操作の詳細については、「ポリシーの操作」セクションを参照してください。

アダプティブトランスポート

この設定は、EDTをプライマリとして、TCPをフォールバックとしてデータ転送を許可または防止します。

デフォルトでは、アダプティブトランスポートは有効（**優先**）になっており、可能な場合はEDTが使用され、TCPにフォールバックします。必要に応じて設定を変更できます。

- **優先**。可能な場合はEDT経由のアダプティブトランスポートが使用され、TCPにフォールバックします。
- **診断モード**。EDTが強制的にオンになり、TCPへのフォールバックは無効になります。この設定はトラブルシューティングの場合にのみ推奨されます。
- **オフ**。TCPが強制的にオンになり、EDTは無効になります。

詳細については、「アダプティブトランスポート」を参照してください。

ドラッグアンドドロップ設定

この設定は、クライアントと仮想アプリケーションまたはデスクトップの間でのファイルのドラッグを許可または防止します。デフォルトでは、ドラッグアンドドロップポリシーは無効になっています。必要に応じて、このポリシーを有効にできます。

アプリケーション起動待機タイムアウト

この設定は、セッションが最初のアプリケーションの起動を待機するミリ秒単位の待機タイムアウト値を指定します。アプリケーションの起動がこの期間を超えると、セッションは終了します。

デフォルトの時間（10,000ミリ秒）を選択するか、ミリ秒単位の数値を指定できます。

クライアントクリップボードリダイレクト

この設定は、ユーザーデバイス上のクリップボードがサーバー上のクリップボードにマッピングされることを許可または禁止します。

デフォルトでは、クリップボードのリダイレクトは許可されています。

セッションとローカルクリップボード間のコピー＆ペーストデータ転送を禁止するには、**禁止**を選択します。ユーザーは、セッション内で実行されているアプリケーション間では引き続きデータをコピー＆ペーストできます。

この設定を許可した後、クライアント接続でクリップボードが消費できる最大許容帯域幅を構成します。**クリップボードリダイレクト帯域幅制限**または**クリップボードリダイレクト帯域幅制限率**の設定を使用します。

クライアントクリップボード書き込み許可形式

「**クライアントクリップボード書き込みの制限**」設定が「**有効**」の場合、ホストクリップボードデータはクライアントエンドポイントと共有できません。この設定を使用して、特定のデータ形式をクライアントエンドポイントクリップボードと共有することを許可できます。この設定を使用するには、これを有効にして、許可する特定の形式を追加します。

次のクリップボード形式はシステム定義です。

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT

- CF_DISPENHMETAFILE
- CF_HTML

以下のカスタム形式は、XenApp and XenDesktop および Citrix Virtual Apps and Desktops™ で事前定義されています。

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- CFX_FILE

HTML形式はデフォルトで無効になっています。この機能を有効にするには:

- **クライアントクリップボードリダイレクト** が **許可** に設定されていることを確認します。
- **クライアントクリップボード書き込みの制限** が **有効** に設定されていることを確認します。
- **クライアントクリップボード書き込み許可形式** に **CF_HTML** (およびサポートしたいその他の形式) のエントリを追加します。

カスタム形式をさらに追加できます。カスタム形式名は、システムに登録される形式と一致している必要があります。形式名は大文字と小文字を区別します。

クライアントクリップボードリダイレクト ポリシーが **禁止** に設定されている場合、または **クライアントクリップボード書き込みの制限** ポリシーが **無効** に設定されている場合、この設定は適用されません。

> **注:**
>
> HTML形式のクリップボードコピーサポート (CF_HTML) を有効にすると、コピーされたコンテンツのソースから宛先にスクリプトがコピーされます。コピーを進める前に、ソースを信頼できることを確認してください。スクリプトを含むコンテンツをコピーした場合、それらは宛先ファイルをHTMLファイルとして保存して実行した場合にのみアクティブになります。

クリップボードのクライアントからセッションへの転送サイズを制限する

この設定は、ユーザーが単一のコピー＆ペースト操作中にクライアントエンドポイントから仮想セッションに転送できるクリップボードデータの最大サイズを指定します。

クリップボードの転送サイズを制限するには、**クリップボードのクライアントからセッションへの転送サイズを制限する**設定を有効にします。次に、**サイズ制限**フィールドにキロバイト単位の値を入力して、ローカルクリップボードとセッション間のデータ転送サイズを定義します。

既定では、この設定は無効になっており、クライアントからセッションへの転送に制限はありません。

HDX™ ダイレクト

HDX Directを使用すると、直接通信が可能な場合にクライアントがセッションホストとの直接接続を自動的に確立できます。接続はネットワークレベルの暗号化を使用して安全に確立されます。

HDX Direct モード

HDX Directは、内部および外部クライアントのセッションホストとの直接接続を確立するために使用できます。この設定は、HDX Directが内部クライアントのみに利用可能か、内部クライアントと外部クライアントの両方に利用可能かを決定します。

内部のみに設定されている場合、HDX Direct は内部ネットワーク内のクライアントに対してのみ直接接続を確立しようとします。

「内部」および**「外部」**に設定されている場合、HDX Directは内部および外部クライアントに対して直接接続を確立しようとします。

既定では、HDX Direct は内部クライアントのみに設定されています。

HDX Direct ポート範囲

外部ユーザーからの接続に HDX Direct が使用するポートの範囲です。 既定では、HDX Direct はポート範囲 55000～55250 を使用します。

クリップボードのセッションからクライアントへの転送サイズを制限する

この設定は、ユーザーが単一のコピー＆ペースト操作中に仮想セッションからクライアントエンドポイントに転送できるクリップボードデータの最大サイズを指定します。

クリップボードの転送サイズを制限するには、**クリップボードのセッションからクライアントへの転送サイズを制限する**設定を有効にします。次に、**サイズ制限**フィールドにキロバイト単位の値を入力して、セッションとローカルクリップボード間のデータ転送サイズを定義します。

既定では、この設定は無効になっており、セッションからクライアントへの転送に制限はありません。

クライアントクリップボードへの書き込みを制限する

この設定が**有効**になっている場合、ホストクリップボードデータはクライアントエンドポイントと共有できません。**クライアントクリップボードへの書き込みを許可する形式**設定を有効にすることで、特定の形式を許可できます。

デフォルトでは、この設定は**無効**です。

セッションクリップボードへの書き込みを制限する

この設定が**有効**になっている場合、クライアントクリップボードデータはセッションアプリケーションと共有できません。**セッションクリップボードへの書き込みを許可する形式**設定を有効にすることで、特定の形式を許可できます。

デフォルトでは、この設定は**無効**です。

セッションクリップボードへの書き込みを許可する形式

セッションクリップボードへの書き込みを制限する設定が**有効**な場合、クライアントのクリップボードデータはセッションアプリケーションと共有できません。この設定を使用して、特定のデータ形式をセッションクリップボードと共有することを許可できます。

以下のクリップボード形式はシステム定義です。

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP

- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

以下のカスタム形式は、XenAppおよびXenDesktop、Citrix Virtual Apps™ and Desktopsで事前定義されています。

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

HTML形式はデフォルトで無効になっています。この機能を有効にするには：

- **クライアントクリップボードリダイレクト**が**許可**に設定されていることを確認します。
- **セッションクリップボード書き込みの制限**が**有効**に設定されていることを確認します。
- **セッションクリップボード書き込み許可形式**に**CF_HTML**（およびサポートしたいその他の形式）のエントリを追加します。

さらにカスタム形式を追加できます。カスタム形式名は、システムに登録される形式と一致している必要があります。形式名は大文字と小文字を区別します。

この設定は、**クライアントクリップボードリダイレクト**ポリシーが**禁止**に設定されている場合、または**セッションクリップボード書き込みの制限**ポリシーが**無効**に設定されている場合には適用されません。

> **注:**
>
> HTML形式のクリップボードコピーサポート (CF_HTML) を有効にすると、コピーされたコンテンツのソースから宛先にスクリプトがコピーされます。コピーを進める前に、ソースを信頼できることを確認してください。スクリプトを含むコンテンツをコピーした場合、それらは宛先ファイルをHTMLファイルとして保存して実行した場合にのみ有効になります。

デスクトップの起動

この設定は、VDA Direct Access Usersグループの非管理者ユーザーがICA接続を使用してそのVDA上のセッションに接続することを許可または禁止します。

デフォルトでは、非管理者ユーザーはこれらのセッションに接続できません。

この設定は、RDP接続を使用しているVDAダイレクトアクセスユーザーグループ内の非管理者ユーザーには影響しません。これらのユーザーは、この設定が有効または無効になっている場合でもVDAに接続できます。この設定は、VDAダイレクトアクセスユーザーグループに属していない非管理者ユーザーには影響しません。これらのユーザーは、この設定が有効または無効になっている場合、VDAに接続できません。

FIDO2リダイレクト

この設定は、FIDO2リダイレクトを有効または無効にします。FIDO2リダイレクトにより、ユーザーは仮想マシン内のローカルエンドポイントFIDO2コンポーネントを活用できます。ユーザーは、TPM 2.0とWindows Helloを搭載したデバイスで、FIDO2セキュリティキーまたは統合生体認証を介して仮想セッションを認証できます。

この設定が**許可**されている場合、ユーザーはローカルエンドポイント機能を使用してFIDO2認証を行うことができます。デフォルトでは、この設定は**許可**されています。

FIDO2許可プロセス

この設定により、管理者は仮想セッション内でFIDO2およびWebAuthnリダイレクトの使用が許可されるアプリケーションを指定できます。

許可リスト内のアプリケーションには、アプリケーション実行可能ファイルへの完全なローカルパスが必要です。ネットワークパスはサポートされていません。

アプリケーションパスでは、ワイルドカード(*)を使用して、単一のディレクトリ、ディレクトリ名の一部、実行可能ファイルのベース名、または実行可能ファイルのベース名の一部を置き換えることができます。

ICAリスナー接続タイムアウト

この設定は、ICAプロトコルを使用した接続が完了するまでの最大待機時間を指定します。

デフォルトでは、最大待機時間は120,000ミリ秒、つまり2分です。

ICAリスナーポート番号

この設定は、サーバー上のICAプロトコルによって使用されるTCP/IPポート番号を指定します。

デフォルトでは、ポート番号は1494に設定されています。

有効なポート番号は0～65535の範囲内である必要があり、他のよく知られているポート番号と競合してはなりません。ポート番号を変更した場合は、新しい値を有効にするためにサーバーを再起動してください。サーバーのポート番号を変更した場合は、サーバーに接続するすべてのCitrix Workspace™アプリまたはプラグインでも変更する必要があります。

キーボードと入力方式エディター (IME)

この設定は、次の項目を有効または無効にします。

- 動的キーボードレイアウト同期
- 入力方式エディター (IME)
- Unicodeキーボードレイアウトマッピング
- キーボードレイアウト切り替え通知ダイアログメッセージの表示/非表示
- タッチデバイスのエンドユーザー向け自動タッチキーボード表示

1. Web Studioで、**キーボードとIME**を選択します。
2. VDAでの動的キーボードレイアウト同期と汎用クライアント入力方式エディター (IME) 機能を制御するには、**クライアントキーボードレイアウト同期とIMEの改善**を選択します。以下を構成できます。

   無効 - 動的キーボードレイアウト同期と汎用クライアント入力方式エディター (IME)。

   動的なクライアントキーボードレイアウト同期をサポート - 動的なキーボードレイアウト同期を有効にします。

   動的クライアントキーボードレイアウト同期とIMEの改善をサポート - 動的キーボードレイアウト同期と汎用クライアント入力方式エディター (IME) の両方を有効にします。
3. 「**Unicode キーボードレイアウトマッピングを有効にする**」を選択して、Unicode キーボードマッピングを有効または無効にします。
4. 「**キーボードレイアウト切り替えポップアップメッセージボックスを非表示にする**」を選択して、ユーザーがクライアントキーボードレイアウトを変更したときに、キーボードレイアウトが同期中であることを示すメッセージを表示するかどうかを制御します。メッセージが表示されないように設定した場合、ユーザーは誤った文字入力が発生しないように、入力する前に数秒待つ必要があります。
5. 「**自動キーボード表示**」を選択して、入力フィールドに入るときまたは離れるときに、クライアント側のソフト/タッチキーボードが自動的に表示または非表示になることを許可または禁止します。

デフォルト設定：

- **クライアントキーボードレイアウトの同期とIMEの改善**
  - ウィンドウズ サーバー 2019/2022/2025、およびマルチセッションのウィンドウズ 10/11では無効
  - シングルセッションのWindows 10/11では有効
- **Unicode キーボードレイアウトマッピング**
  - 禁止（Unicode キーボードレイアウトマッピングはデフォルトで無効であることを示します。エンドユーザーがCWAでUnicode入力モードを使用している場合は、設定して許可する必要があります）
- **キーボードレイアウト切り替えポップアップメッセージボックスを非表示にする**
  - 禁止（ポップアップメッセージボックスが表示されることを示します）
- **自動キーボード表示**
  - 禁止（入力フィールドに入るときまたは離れるときに、クライアント側のソフト/タッチキーボードが自動的に表示または非表示にならないことを示します）

このポリシーは、ポリシー設定の**説明**セクションに記載されているレジストリ設定を置き換えます。

ログオフチェッカーの起動遅延

この設定は、ログオフチェッカーの起動を遅延させる期間を指定します。このポリシーを使用して、クライアントセッションがセッションを切断するまでに待機する時間（秒単位）を設定します。

この設定は、ユーザーがサーバーからログオフするのにかかる時間も増加させます。

ロス耐性モード

> **重要:**
>
> - この機能には、Windows 用 Citrix Workspace アプリ 2002 以降が必要です。VDA のこのバージョンは、利用可能になり次第、これをサポートします。

- グラフィックのロス耐性モードは、Citrix Gateway および Citrix Gateway Service でサポートされています。このモードは、直接接続の場合にのみ利用可能です。

この設定は、グラフィックのロス耐性モードを有効または無効にします。

デフォルトでは、グラフィックのロス耐性モードは**許可**されています。

許可されている場合、パケット損失と遅延がしきい値を超えると、このモードに入ります。しきい値は、ロス耐性しきい値ポリシーを使用して設定できます。

ロス耐性しきい値

ロス耐性モードが利用可能な場合、この設定は、セッションがグラフィックのロス耐性モードに切り替わるネットワークメトリックのしきい値を指定します。

デフォルトのしきい値は次のとおりです。

- パケット損失: 5%
- 遅延: 300 ms (RTT)

詳細については、ロス耐性モードを参照してください。

オーディオの損失許容モード

この設定は、オーディオの損失許容モードを有効または無効にします。

有効にすると、オーディオは損失許容モードで送信されます。

デフォルトでは、オーディオの損失許容モードは**禁止**されています。

ポリシーを有効にするには、オーディオポリシーの損失許容モードのレジストリを**許可**に編集します。

オーディオの損失許容モードを有効にするには、EDTトランスポートが必要です。

Rendezvous プロトコル

この設定は、Citrix Gateway Serviceを使用する際のHDXセッションのプロキシ方法を変更します。有効にすると、HDXトラフィックはCitrix Cloud Connectorを経由しなくなります。代わりに、VDAはCitrix Gateway Serviceに直接アウトバウンド接続を確立します（Cloud Connectorのスケーラビリティが向上します）。

重要:

Citrix Cloud™の機能トグルとHDXポリシー設定がこの機能を制御します。Citrix Cloudの機能トグルはデフォルトで有効になっていますが、HDX設定はデフォルトで無効になっています。HDX設定は、Citrix Gateway Serviceを介して確立されたHDXセッションにのみ影響します。この設定は、クライアントとVDA間で直接確立されたセッションや、オンプレミスのCitrix Gatewayを介して確立されたセッションには影響しません。

詳細については、Rendezvousプロトコルを参照してください。

Rendezvousプロキシ構成

この設定により、Rendezvousプロトコルで使用する明示的なプロキシを構成できます。透過プロキシを使用している場合、この設定を有効にする必要はありません。

デフォルトでは、この設定は無効になっています。

無効にすると、VDAはGateway ServiceとのRendezvous接続を確立しようとするときに、非透過プロキシを介してアウトバウンドトラフィックをルーティングしません。

有効にすると、VDAは、この設定で定義されたプロキシを介してGateway ServiceとのRendezvous接続を確立しようとします。

VDAは、Rendezvous接続にHTTPおよびSOCKS5プロキシの使用をサポートしています。Rendezvous接続にプロキシを使用するようにVDAを構成するには、この設定を有効にする必要があります。また、プロキシのアドレスまたはPACファイルへのパスを指定します。例：

- プロキシアドレス：`http://<URL or IP>:<port>` または `socks5://<URL or IP>:<port>`
- PACファイル：`http://<URL or IP>/<path>/<filename>.pac`

  VDAバージョン2103は、PACファイルを使用したプロキシ構成でサポートされる最小バージョンです。SOCKS5プロキシのPACファイルスキーマの詳細については、「プロキシ構成」を参照してください。

注:

SOCKS5プロキシのみがEDTを介したデータ転送をサポートしています。HTTPプロキシの場合は、ICAのトランスポートプロトコルとしてTCPを使用します。

> 詳細については、「Rendezvousプロトコル」を参照してください。

クライアント接続中の非公開プログラムの起動

この設定は、サーバー上でRDPを介して初期アプリケーションの起動を許可するかどうかを指定します。

デフォルトでは、サーバー上でRDPを介して初期アプリケーションを起動することは許可されていません。

セッションメトリックの収集

この設定により、CitrixはVDAとWorkspace間のユーザーおよびマシンセッションメトリックを収集し、ユーザーエクスペリエンスを向上させることができます。

オペレーティングシステム、稼働時間、コンピューターシステム情報、ビデオコントローラーの詳細、VDAバージョン、展開タイプ、ドメイン参加ステータスなどのデータがCitrixによって収集されます。さらに、製品改善の取り組みを支援するために、いくつかのセッション構成、パフォーマンスおよび信頼性データも収集できます。お客様体験向上プログラムの詳細については、以下を参照してください。

- `<https://more.citrix.com/XD-CEIP>`
- `<https://docs.citrix.com/ja-jp/linux-virtual-delivery-agent/current-release/configure/administration/linux-vda-data-collection-program>`
- `<https://docs.citrix.com/ja-jp/mac-vda/configure/session/supportability-service>`

既定では、この設定は有効になっています。

タブレットモード切り替えポリシー設定

タブレットモード切り替えは、VDA上のStoreアプリ、Win32アプリ、およびWindowsシェルの外観と動作を最適化します。これは、電話やタブレットなどの小型フォームファクターデバイス、またはタッチ対応デバイスから接続する際に、仮想デスクトップを自動的にタブレットモードに切り替えることで実現されます。

このポリシーが無効になっている場合、VDAはユーザーが設定したモードになり、クライアントの種類に関係なく、常に同じモードを維持します。

自動クライアント再接続ポリシー設定

自動クライアント再接続セクションには、セッションの自動再接続を制御するためのポリシー設定が含まれています。

自動クライアント再接続

この設定により、接続が中断された後に同じクライアントによる自動再接続を許可または禁止します。

Citrix Receiver for Windows 4.7以降およびCitrix Workspaceアプリ1808以降では、自動クライアント再接続はCitrix Studioからのポリシー設定のみを使用します。Studioでこれらのポリシーを更新すると、自動クライアント再接続がサーバーからクライアントに同期されます。以前のバージョンのCitrix Receiver for Windowsで自動クライアント再接続を構成するには、Studioポリシーを使用し、レジストリまたはdefault.icaファイルを変更します。

自動クライアント再接続を許可すると、接続が切断されたときに中断された場所からユーザーが作業を再開できます。自動再接続は、切断された接続を検出し、ユーザーをセッションに再接続します。

セッションIDと資格情報へのキーを含むCitrix Workspace™アプリのCookieが使用されない場合、自動再接続によって新しいセッションが開始される可能性があります。つまり、既存のセッションに再接続するのではなく、新しいセッションが開始されます。Cookieの有効期限が切れている場合、Cookieは使用されません。たとえば、再接続の遅延や、資格情報を再入力する必要がある場合などに、Cookieの有効期限が切れることがあります。ユーザーが意図的に切断した場合、自動クライアント再接続はトリガーされません。

再接続が進行中の場合、セッションウィンドウはグレー表示されます。カウントダウンタイマーは、セッションが再接続されるまでの残り時間を表示します。セッションがタイムアウトすると、切断されます。

アプリケーションセッションの場合、自動再接続が許可されていると、通知領域にカウントダウンタイマーが表示されます。このタイマーは、セッションが再接続されるまでの残り時間を指定します。Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルするまで、セッションへの再接続を試行します。

ユーザーセッションの場合、自動再接続が許可されていると、Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルしない限り、指定された期間セッションへの再接続を試行します。デフォルトでは、この期間は2分です。この期間を変更するには、ポリシーを編集します。

デフォルトでは、自動クライアント再接続は許可されています。ポリシーを**禁止**に設定することで無効にできます。

自動クライアント再接続認証

この設定は、自動クライアント再接続に認証が必要かどうかを指定します。

ユーザーが最初にログオンすると、資格情報は暗号化されてメモリに保存され、暗号化キーを含むCookieが作成されます。CookieはCitrix Workspaceアプリに送信されます。この設定が構成されている場合、Cookieは使用されません。代わりに、Citrix Workspaceアプリが自動的に再接続を試行するときに、資格情報を要求するダイアログボックスがユーザーに表示されます。

デフォルトでは、認証は不要です。

自動クライアント再接続ログ

この設定は、イベントログへの自動クライアント再接続の記録を有効または無効にします。

ログ記録が有効な場合、サーバーのシステムログは、成功および失敗した自動再接続イベントに関する情報をキャプチャします。サイトは、すべてのサーバーの再接続イベントの結合されたログを提供しません。

デフォルトでは、ログ記録は無効です。

自動クライアント再接続のタイムアウト

デフォルトでは、自動クライアント再接続のタイムアウトは120秒に設定されており、自動クライアント再接続のタイムアウトの最大設定可能値は300秒です。このポリシーを使用してタイムアウト値を設定します。

再接続UIの透明度レベル

この設定により、セッションの信頼性再接続中にXenAppまたはXenDesktop®セッションウィンドウに適用される不透明度レベルを指定できます。

デフォルトでは、再接続UIの透明度は80%に設定されています。

オーディオポリシー設定

オーディオセクションには、パフォーマンスを低下させることなく、ユーザーデバイスがセッションでオーディオを送受信できるようにするポリシー設定が含まれています。

アダプティブオーディオ

この設定は、アダプティブオーディオを有効または無効にします。このポリシーを有効にすると、最高のユーザーエクスペリエンスを提供するために、オーディオ品質設定が動的に調整されます。

この設定は、Citrix Virtual Apps and Desktops™ 2109以降を使用するVDAのシングルセッションOSおよびマルチセッションOSセッションの両方に適用されます。

この設定が禁止されている場合、オーディオ品質ポリシーが適用されます。詳しくは、「オーディオ品質」を参照してください。

デフォルトでは、アダプティブオーディオポリシーは有効になっています。

UDPリアルタイムトランスポート経由のオーディオ

この設定は、User Datagram Protocol (UDP) を使用してRTP経由でVDAとユーザーデバイス間でオーディオを送受信することを許可または禁止します。この設定が無効になっている場合、オーディオはTCP経由で送受信されます。

デフォルトでは、UDP経由のオーディオは許可されています。

オーディオプラグアンドプレイ

この設定は、複数のオーディオデバイスを使用してサウンドを録音および再生することを許可または禁止します。

デフォルトでは、複数のオーディオデバイスの使用は許可されています。

この設定は、WindowsマルチセッションOSマシンにのみ適用されます。

オーディオ品質

この設定は、ユーザーセッションで受信されるサウンドの品質レベルを指定します。

デフォルトでは、サウンド品質は「高 - 高精細オーディオ」に設定されています。

サウンド品質を制御するには、次のいずれかのオプションを選択します。

- 低帯域幅接続の場合は、「低 - 低速接続用」を選択します。ユーザーデバイスに送信されるサウンドは最大16 Kbpsに圧縮されます。この圧縮により、サウンドの品質は大幅に低下しますが、低帯域幅接続でも適切なパフォーマンスが得られます。
- Voice over Internet Protocolアプリケーションを配信するために音声用に最適化された「中」を選択します。この設定は、512 Kbps未満の回線や、著しい輻輳およびパケット損失があるような困難なネットワーク接続でメディアアプリケーションを配信します。このコーデックはエンコード時間が高速であるため、サーバー側のメディア処理が必要な場合に、ソフトフォンやユニファイドコミュニケーションアプリケーションでの使用に最適です。

  ユーザーデバイスに送信されるオーディオは、最大64 Kbpsに圧縮されます。この圧縮により、ユーザーデバイスで再生されるオーディオの品質は中程度に低下しますが、低遅延で低帯域幅の消費を実現します。Voice over Internet Protocolの品質が不十分な場合は、「Audio over

UDP Real-time Transport」ポリシー設定が「許可」に設定されていることを確認してください。

現在、UDP経由のリアルタイムトランスポート（RTP）は、このオーディオ品質が選択されている場合にのみサポートされます。このオーディオ品質は、低速（512 Kbps未満）回線のような困難なネットワーク接続でメディアアプリケーションを配信する場合でも使用します。また、ネットワークに輻輳やパケット損失がある場合にも使用します。

- 帯域幅が豊富で音質が重要な接続の場合は、「高 - 高精細オーディオ」を選択します。クライアントはネイティブレートでサウンドを再生できます。サウンドはCD品質まで維持される高音質レベルで圧縮され、最大112 Kbpsの帯域幅を使用します。この量のデータを送信すると、CPU使用率が増加し、ネットワーク輻輳が発生する可能性があります。

帯域幅は、オーディオの録音中または再生中にのみ消費されます。両方が同時に発生する場合、帯域幅の消費量は2倍になります。

最大帯域幅を指定するには、**オーディオリダイレクト帯域幅制限**または**オーディオリダイレクト帯域幅制限率**の設定を構成します。

クライアントオーディオリダイレクト

この設定は、サーバーでホストされているアプリケーションが、ユーザーデバイスにインストールされているサウンドデバイスを介してサウンドを再生できるかどうかを指定します。この設定は、ユーザーがオーディオ入力を録音できるかどうかも指定します。

デフォルトでは、オーディオリダイレクトは許可されています。

この設定を許可した後、オーディオの再生または録音によって消費される帯域幅を制限できます。オーディオによって消費される帯域幅の量を制限すると、アプリケーションのパフォーマンスが向上する可能性がありますが、オーディオ品質が低下する可能性もあります。帯域幅は、オーディオの録音中または再生中にのみ消費されます。両方が同時に発生する場合、帯域幅の消費量は2倍になります。最大帯域幅を指定するには、「**オーディオリダイレクト帯域幅制限**」または「**オーディオリダイレクト帯域幅制限パーセント**」設定を構成します。

WindowsマルチセッションOSマシンでは、複数のオーディオデバイスをサポートするために、**オーディオプラグアンドプレイ**設定が有効になっていることを確認してください。

重要：クライアントオーディオリダイレクトを禁止すると、すべてのHDX™オーディオ機能が無効になります。

クライアントマイクのリダイレクト

この設定は、クライアントマイクのリダイレクトを有効または無効にします。有効にすると、ユーザーはセッションでマイクを使用してオーディオ入力を録音できます。

デフォルトでは、マイクのリダイレクトは許可されています。

セキュリティのため、デバイスによって信頼されていないサーバーがマイクにアクセスしようとすると、ユーザーに警告が表示されます。ユーザーはアクセスを許可するかどうかを選択できます。ユーザーはCitrix Workspace™アプリで警告を無効にできます。

WindowsマルチセッションOSマシンでは、複数のオーディオデバイスをサポートするために、オーディオプラグアンドプレイ設定が有効になっていることを確認してください。

ユーザーデバイスで**クライアントオーディオリダイレクト**設定が無効になっている場合、このルールは効果がありません。

帯域幅ポリシー設定

帯域幅セクションには、クライアントセッションの帯域幅使用に関連するパフォーマンスの問題を回避するためのポリシー設定が含まれています。

重要: これらのポリシー設定を**マルチストリームポリシー**設定と併用すると、予期しない結果が生じる可能性があります。ポリシーでマルチストリーム設定を使用する場合は、これらの帯域幅制限ポリシー設定が含まれていないことを確認してください。

オーディオリダイレクト帯域幅制限

この設定は、ユーザーセッションでオーディオを再生または録音するために許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**オーディオリダイレクト帯域幅制限の割合**設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

オーディオリダイレクト帯域幅制限の割合

この設定は、オーディオの再生または録音に許可される最大帯域幅制限を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**オーディオリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

この設定を構成する場合は、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

クライアントUSBデバイスリダイレクト帯域幅制限

この設定は、クライアントとの間でUSBデバイスをリダイレクトするために許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**クライアントUSBデバイスリダイレクト帯域幅制限（パーセント）**設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

クライアントUSBデバイスリダイレクトの帯域幅制限（パーセント）

この設定は、USBデバイスのクライアントとの間のリダイレクトに許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値は指定されていません（ゼロ）。

この設定に値を入力し、**クライアントUSBデバイスリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

クリップボードリダイレクト帯域幅制限

この設定は、セッションとローカルクリップボード間のデータ転送に許可される最大帯域幅を指定します。許可される最大帯域幅は、1秒あたりのキロビット単位で指定されます。

デフォルトでは、最大値は指定されていません（ゼロ）。

この設定に値を入力し、**クリップボードリダイレクト帯域幅制限（パーセント）**設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

クリップボードリダイレクト帯域幅制限（パーセント）

この設定は、セッションとローカルクリップボード間のデータ転送に許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値は指定されていません（ゼロ）。

この設定に値を入力し、**クリップボードリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

COMポートリダイレクト帯域幅制限

> **注：**
>
> Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、クライアント接続でCOMポートにアクセスするために許可される最大帯域幅をキロビット/秒で指定します。この設定の値と**COMポートリダイレクト帯域幅制限（パーセント）**設定の値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

COMポートリダイレクト帯域幅制限（パーセント）

注：Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、クライアント接続でCOMポートにアクセスするために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値は指定されていません（ゼロ）。

この設定の値と**COMポートリダイレクト帯域幅制限**設定の値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

ファイルリダイレクト帯域幅制限

この設定は、ユーザーセッションでクライアントドライブにアクセスするために許可される最大帯域幅を指定します。許可される最大帯域幅はキロビット/秒で指定されます。

デフォルトでは、最大値は指定されていません（ゼロ）。

この設定の値と**ファイルリダイレクト帯域幅制限（パーセント）**設定の値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

ファイルリダイレクト帯域幅制限（パーセント）

この設定は、クライアントドライブへのアクセスに許可される最大帯域幅制限を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**ファイルリダイレクト帯域幅制限**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

HDX™ MediaStream マルチメディアアクセラレーション帯域幅制限

この設定は、HDX MediaStream マルチメディアアクセラレーションを使用してストリーミングオーディオおよびビデオを配信するために許可される最大帯域幅制限を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**HDX MediaStream マルチメディアアクセラレーション帯域幅制限の割合**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

HDX MediaStream マルチメディアアクセラレーション帯域幅制限の割合

この設定は、HDX MediaStream マルチメディアアクセラレーションを使用してストリーミングオーディオおよびビデオを配信するために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**HDX MediaStream マルチメディアアクセラレーション帯域幅制限**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

LPTポートリダイレクト帯域幅制限

注：Virtual Delivery Agent 7.0～7.8の場合、この設定はレジストリを使用して構成します。詳しくは、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、単一ユーザーセッションでLPTポートを使用する印刷ジョブに許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**LPTポートリダイレクト帯域幅制限の割合**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

LPTポートリダイレクト帯域幅制限の割合

注：Virtual Delivery Agent 7.0～7.8の場合、この設定はレジストリを使用して構成します。「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、単一のクライアントセッションでLPTポートを使用する印刷ジョブの帯域幅制限を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**LPTポートリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合は、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

セッション全体の帯域幅制限

この設定は、ユーザーセッションで利用可能な総帯域幅を、1秒あたりのキロビット単位で指定します。

適用可能な最大帯域幅の上限は20 Mbps (20,000 Kbps)です。デフォルトでは、最大値（ゼロ）は指定されていません。

クライアント接続によって消費される帯域幅の量を制限すると、クライアント接続外の他のアプリケーションが限られた帯域幅を競合している場合にパフォーマンスが向上する可能性があります。

プリンターリダイレクト帯域幅制限

この設定は、ユーザーセッションでクライアントプリンターにアクセスするために許可される最大帯域幅を指定します。許可される最大帯域幅は、1秒あたりのキロビット単位で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**Printer redirection bandwidth limit percent** 設定にも値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

プリンターリダイレクトの帯域幅制限の割合

この設定は、クライアントプリンターにアクセスするために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**Printer redirection bandwidth limit** 設定にも値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**Overall session bandwidth limit** 設定も構成する必要があります。

TWAINデバイスリダイレクトの帯域幅制限

この設定は、公開アプリケーションからTWAINイメージングデバイスを制御するために許可される最大帯域幅を指定します。許可される最大帯域幅は、1秒あたりのキロビット単位で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**TWAIN device redirection bandwidth limit percent** 設定にも値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

TWAINデバイスリダイレクトの帯域幅制限の割合

この設定は、公開アプリケーションからTWAINイメージングデバイスを制御するために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**TWAIN device redirection bandwidth limit** 設定にも値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**Overall session bandwidth limit** 設定も構成する必要があります。

双方向コンテンツリダイレクトポリシー設定

双方向コンテンツリダイレクトセクションには、クライアントからVDAへ、およびVDAからクライアントへのURLリダイレクトを有効または無効にするポリシー設定があります。

サーバーポリシーはStudioで設定されます。Citrix Workspace™アプリバージョン2311以降、この設定は、Studioで非推奨となった以下の3つのレガシー設定に置き換わります。

- 双方向コンテンツリダイレクトを許可する
- VDAにリダイレクトされる許可されたURL
- クライアントにリダイレクトされる許可されたURL

また、Windowsクライアント上の以下の3つのローカルグループポリシーオブジェクト (GPO) 設定も置き換わります。

- 双方向コンテンツリダイレクト
- 双方向コンテンツリダイレクトのオーバーライド
- OAuthリダイレクト

この設定が有効になっている場合、公開されたアプリまたはデスクトップに接続すると、双方向コンテンツリダイレクトを構成するためのクライアントからVDAへの設定がクライアントに送信されます。

構成(/en-us/citrix-virtual-apps-desktops/2511/media/bidirectional-content-redirection-configuration.png)

この設定が構成されている場合、Studioおよびクライアント上のレガシー設定よりも優先されます。Citrix®は、予期しない動作を避けるために、新しいポリシー設定のみを使用し、レガシー設定を削除することを推奨します。

VDAとDDCがバージョン2311以降を実行している場合、クライアントポリシーを設定してはいけません。そうでない場合、クライアントポリシーはCitrix Workspaceアプリのグループポリシーオブジェクト管理テンプレートから設定されます。

Citrixは、クライアントからURLへのリダイレクトのために、ホストからクライアントへのリダイレクトとLocal App Accessを提供しています。ただし、Citrixは、ドメイン参加済みWindowsクライアントには双方向コンテンツリダイレクトを使用することを推奨します。

Citrix は、この機能を構成するために Studio の新しい UI を使用することをお勧めします。

ワイルドカードリダイレクト

双方向コンテンツリダイレクトは、リダイレクトする URL を定義する際にワイルドカードの使用をサポートします。詳細および双方向コンテンツリダイレクトの構成については、構成 の手順を参照してください。 Studio で、`hostToClientUrls` 配列または `clientToHostUrls` 配列内の `url` キーの値として JSON 文字列を編集して、ワイルドカード URL を設定します。

> **注:**
>
> - 無限ループを避けるため、`hostToClientUrls` と `clientToHostUrls` に同じ URL を設定しないでください。

- トップレベルドメインはサポートされていません。たとえば、`<https://www.citrix.*>` や `<http://www.citrix.co*>` はリダイレクトされません。

双方向コンテンツリダイレクトの構成

この機能を構成し始めるには、このポリシーを `Enabled` に設定し、**URL の管理**をクリックします。以下の構成を設定します。

- **VDA からクライアントへのリダイレクト**
- **クライアントから VDA へのリダイレクト**

VDA からクライアントへのリダイレクト

VDA からクライアントに URL をリダイレクトするには、1 行に 1 つの URL を入力します。ワイルドカードも使用できます。 OAuth リダイレクトを使用すると、クライアントエンドポイントのブラウザを使用して認証を実行し、トークンを VDA に送り返すことができます。

利点:

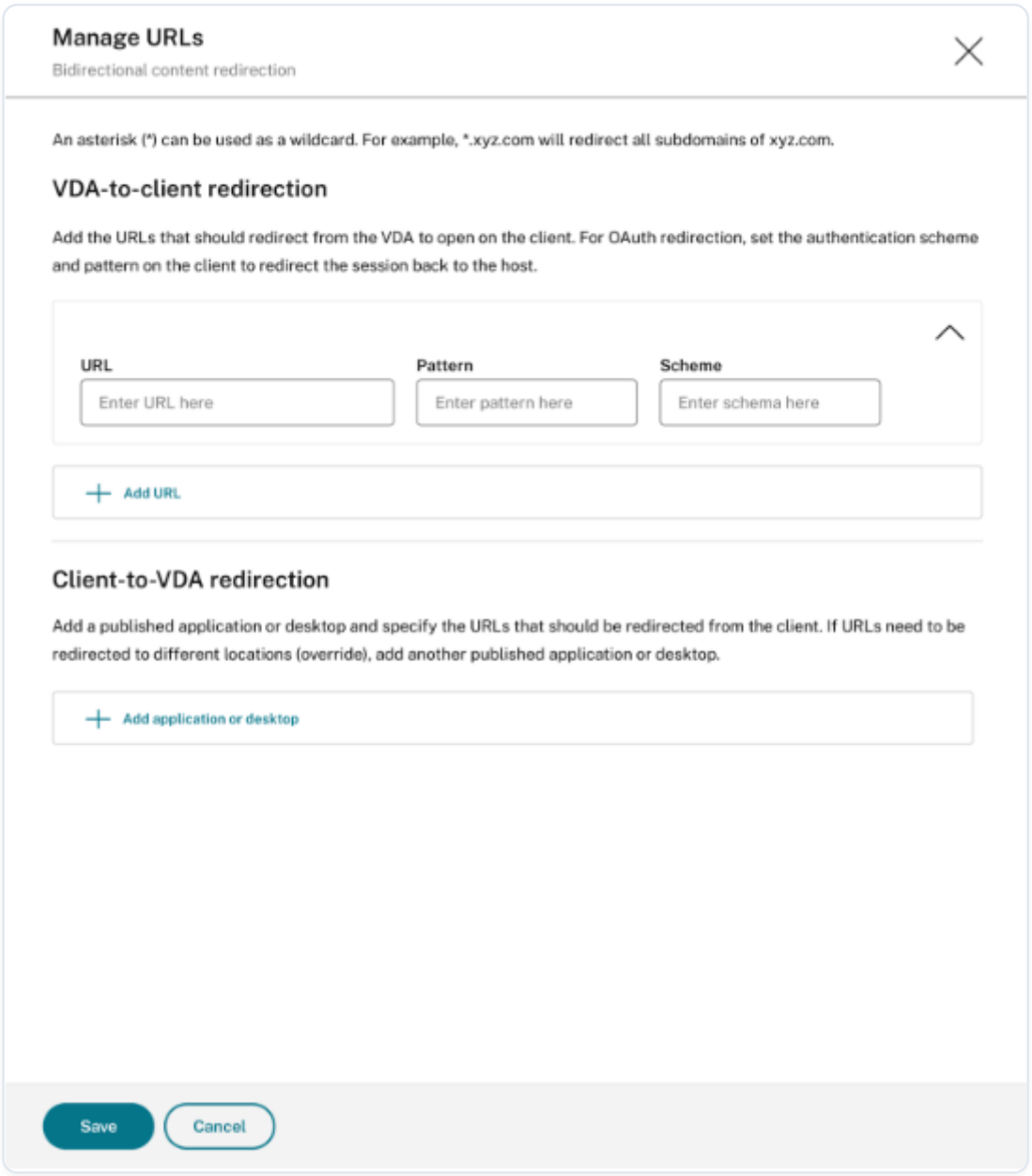
- ホストされた環境にこれらの資格情報を保存することを回避できます。
- エンドポイントで利用可能で、VDA では利用できない生体認証機能を使用できます。

構成:

URLのVDAからクライアントへのリダイレクトを構成するには、以下を指定します。

- **URL** (必須) VDAからクライアントで開くようにリダイレクトする必要があるURLを追加します。**OAuthリダイレクト**の場合、セッションをホストにリダイレクトするために、クライアントで認証スキームとパターンを設定します。
- **パターン**: (オプション) VDAからクライアントへのURLリダイレクトを介してクライアントにリダイレクトされると、OAuth認証フローが開始されたかのように追跡されるURL正規表現です。フローが完了すると（結果のスキームまたはリダイレクトURLパターンが開かれることで検出される）、その結果のURLは、そのフローを開始したホストVDAにリダイレクトされます。
- **スキーム**: (オプション) **スキーム**が指定されている場合、終了URLは `<scheme>://<something>` の形式であると想定されます。スキームが指定されていない（空である）場合を考えます。その場合、元の結果のURLパターンは、正規表現キャプチャグループ（パターンで指定する必要がある）を介してパターンから抽出され、元のURLは `citrix-oauth-redir://` リダイレクトURLを使用するように書き換えられます。フローが完了すると、元のリダイレクトURLはホスト（VDA）にリダイレクトされます。この場合、OAuth認証サーバー

は`citrix-oauth-redir://byIndex/1 (2, 3, ... N)`リダイレクトURLを許可するように構成する必要があります。



注:

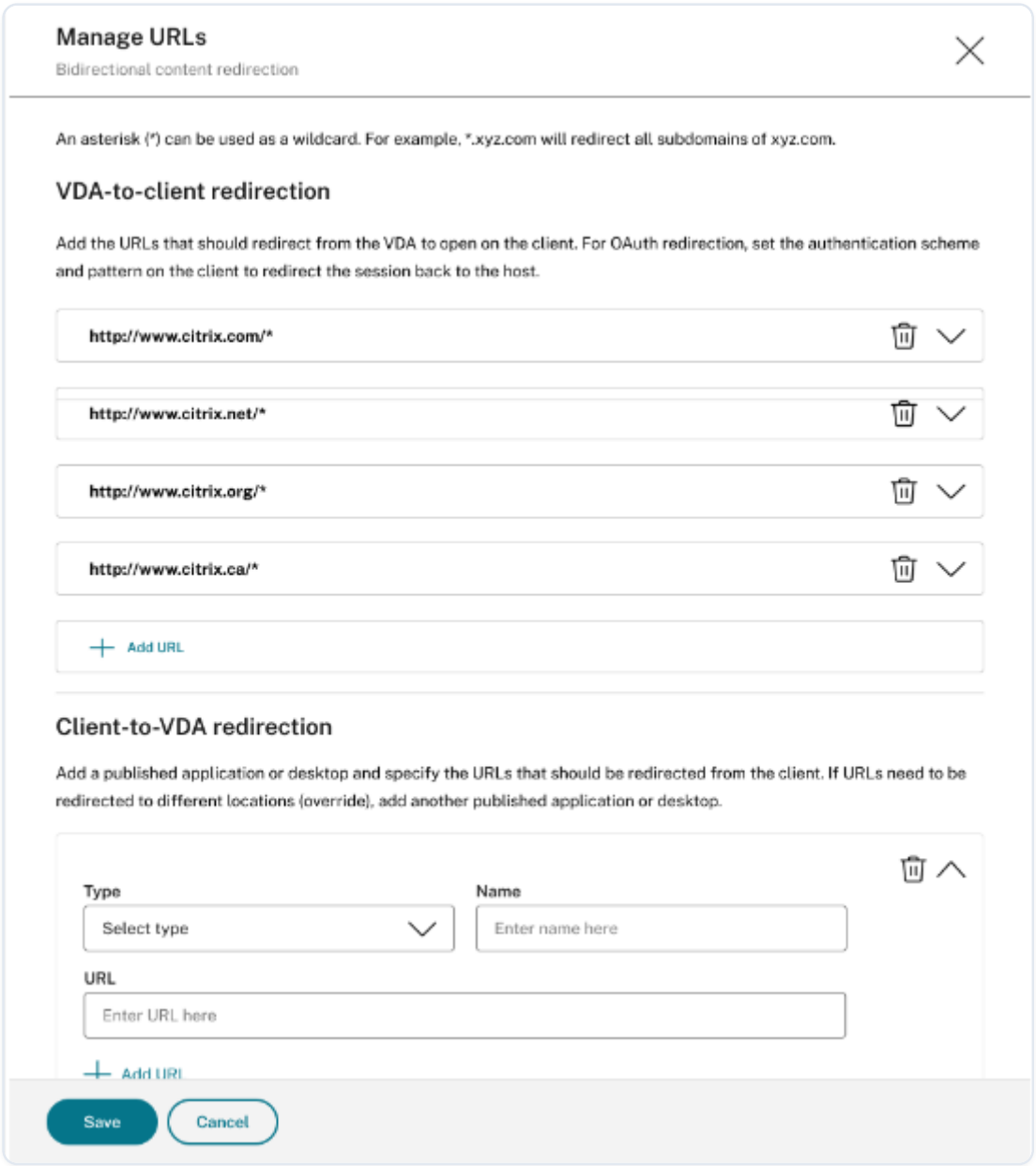
パターンと**スキーム**はどちらもオプションですが、**パターン**が指定されている場合は、**スキーム**も指定する必要があります。

クライアントからVDAへのリダイレクト

クライアントからVDAにURLをリダイレクトするには、次の手順を実行します。

1. クライアントURLの宛先を構成します。

2. 公開アプリケーションまたは公開デスクトップのいずれかを選択します。
3. そのリソースの名前を指定します。
4. そのリソースにリダイレクトする必要があるすべてのURLを追加します。 新しいアプリケーションまたはデスクトップを追加し、そのリソースにリダイレクトするURLを指定することで、このデフォルトのリソースを上書きできます。



OAuth リダイレクト

OAuth リダイレクトを使用すると、クライアントエンドポイントブラウザを使用して認証し、トークンをVDAに送り返すことができます。

利点：

- これらの資格情報をホスト環境に保存することを回避できます。

- エンドポイントで利用可能で、VDAでは利用できない生体認証機能を使用できます。

URLのOAuthリダイレクトを構成するには、次のパラメーターを指定します。

- **oAuthRedirectionPattern**: (オプション) VDAからクライアントへのURLリダイレクトを介してクライアントにリダイレクトされるときに、OAuth認証フローが開始されたかのように追跡され、フローが完了したとき（結果のスキームまたはリダイレクトURLパターンが開かれることによって検出される）、その結果のURLがフローを開始したホストVDAにリダイレクトされるURL正規表現。
- **oAuthScheme**: (オプション) スキームが指定されている場合、終了URLは `<scheme>://<something>` の形式であると想定されます。スキームが指定されていない（空である）とします。その場合、元の結果のURLパターンは、正規表現キャプチャグループ（パターンで指定する必要がある）を介してパターンから抽出され、元のURLは `citrix-oauth-redir://` リダイレクトURLを使用するように書き換えられます。フローが完了すると、元のリダイレクトURLはホスト（VDA）にリダイレクトされます。この場合、OAuth認証サーバーは `citrix-oauth-redir://byIndex/1 (2, 3, ... N)` リダイレクトURLを許可するように構成する必要があります。

クライアントからVDAへのリダイレクトの場合、リダイレクトするリソースごとに **clientToHostConfig** を作成します。 各リソースには、次のパラメーターを含めます。

- **publishedAppOrDesktopNameType**: (必須) Studioで構成された公開デスクトップ（「Desktop」）または公開アプリケーション（「Application」）のいずれか。リソースが無効な場合、リダイレクトは正しく機能しません。
- **publishedAppOrDesktopName**: (必須) Studioで構成されたリソース名。
- **clientToHostUrls**: (必須) クライアントからホスト（VDA）にリダイレクトされるURLのリスト。ワイルドカードが許可されます。

既知の制限

PowerShellを使用してカスタムURLスキーム（HTTPまたはHTTPSではない）でブラウザを起動すると、カスタムURLはクライアントにリダイレクトされません。

ブラウザコンテンツリダイレクトポリシー設定

ブラウザコンテンツリダイレクト (BCR) は、Citrix Virtual Apps and Desktops™ 環境内でのWebブラウジングのユーザーエクスペリエンスを向上させます。Webページのレンダリングをユーザーのローカルマシンにオフロードすることで、BCRはサーバー負荷を軽減し、特に複雑なWebサイトやリソースを大量に消費するWebサイトのパフォーマンスを向上させます。 このドキュメント

では、ブラウザコンテンツリダイレクトで利用可能な各ポリシー設定オプションについて詳しく説明します。

ブラウザコンテンツリダイレクト

この設定は、ブラウザコンテンツリダイレクトの主要なオン/オフスイッチとして機能します。

- **機能:** Webページがサーバーでレンダリングされるか、ローカルデバイスでレンダリングされるかを決定します。有効にすると、Citrix Workspace™ アプリは、よりスムーズなエクスペリエンスのために、Webコンテンツをデバイスでフェッチして表示しようとします。それが失敗した場合、サーバーでのレンダリングにフォールバックします。
- **オプション:**
  - **許可:** (デフォルト) ブラウザコンテンツリダイレクトを有効にします。
  - **禁止:** ブラウザコンテンツリダイレクトを無効にします。
- **注意点:** 許可されている場合、Citrix Workspace アプリはクライアントフェッチとクライアントレンダリングを試行します。クライアントフェッチとクライアントレンダリングが失敗した場合、ブラウザコンテンツリダイレクトはサーバー側レンダリングにフォールバックします。サーバーフェッチとクライアントレンダリングを有効にするには、「ブラウザコンテンツリダイレクトプロキシ構成」設定を有効にします。

ブラウザコンテンツリダイレクトACL構成

この設定により、ブラウザコンテンツリダイレクトの使用を許可または禁止するWebサイト (URL) のリストを作成できます。

- **機能:** ブラウザコンテンツリダイレクトで最適化されるWebサイトをきめ細かく制御できます。Webサイト全体または特定のページを指定できます。
- **動作:**
  - **許可されるURL:** このリストにあるWebサイトは、そのコンテンツがデバイスに表示されます。ワイルドカード (*) *を使用して、複数のページまたはサブドメインを含めることができます (例:* `<https://www.example.com/>` または `<http://*.example.com/>`)。URLのプロトコル内ではワイルドカードは許可されません。
- **デフォルト:** `<https://www.youtube.com/*>`
- **例:**
  - **許可されるパターン:** <http://www.xyz.com/index.html, `<https://www.xyz.com/*>` , `<http://www.xyz.com/*videos>` *> , `<http://*.xyz.com/<>` >

- **許可されないパターン:** `<http://*.*.com/>`
- URL にパスを指定することで、より詳細な粒度を実現できます。たとえば、`<https://www.xyz.com/sports/index.html>` を指定すると、index.html ページのみがリダイレクトされます。

ブラウザコンテンツリダイレクトのブロックリスト構成

この設定は、「ブラウザコンテンツリダイレクト ACL 構成」設定と連携して機能します。

- **機能:** ACL 構成で許可されている場合でも、特定の Web サイトやページをブロックできるようにすることで、追加の制御レイヤーを提供します。ブロックリストが優先されます。
- **動作:** ACL 構成で一般的に許可されている場合でも、デバイスにリダイレクトしたくない Web サイトやページを指定します。
- **デフォルト:** URL は構成されていません
- **ワイルドカード:** ACL 構成と同様に、ワイルドカード (*) を使用して複数のページやサブドメインをブロックできます。
- **例:** Web サイトの index.html ページのみをブロックするには、次のように入力します: `<https://www.example.com/sports/index.html>`

ブラウザーコンテンツリダイレクト認証サイト

この設定では、ブラウザコンテンツリダイレクトが、ログインに外部 ID プロバイダー (IdP) を使用する Web サイトでどのように機能するかを管理できます。

- **機能:** 認証のために別の Web サイトにリダイレクトされた場合でも (Web サイトが Okta やその他のサービスをログインに使用する場合など)、ブラウザコンテンツリダイレクトがアクティブな状態を維持するようにします。
- **動作:** 認証 Web サイトの URL をこのリストに追加して、ログイン中にリダイレクトプロセスが中断されないようにします。
- **デフォルト:** URLは構成されていません
- **例:** www.example.com が認証に www.example.okta.com を使用する場合、www.example.com/ をブラウザコンテンツリダイレクトACL構成に追加し、認証Webサイト www.example.okta.com をブラウザコンテンツリダイレクト認証サイトに追加します。
- **詳細情報:** 詳細については、Citrix Knowledge Centerの記事 CTX238236 および「ブラウザコンテンツリダイレクト」の「マルチメディア」セクションを参照してください。

ブラウザコンテンツリダイレクトのプロキシ構成

この設定により、ブラウザコンテンツリダイレクトがネットワークのプロキシサーバーをどのように使用するかをより詳細に制御できます。また、環境でクライアントフェッチクライアントレンダリングが許可されていない場合に、サーバーフェッチクライアントレンダリングを容易にします。

- **機能:** Citrix Workspaceアプリに、Webコンテンツの取得にサーバーフェッチ方式の使用を強制します。有効にすると、常にサーバーからコンテンツを取得し、デバイスに表示しようとします。
- **オプション:**
  - 明示的プロキシ: 特定のプロキシサーバーを使用します。プロキシサーバーのアドレスとポート番号を指定する必要があります（例：`<http://proxy.example.com:80>`）。
    - 許可されるパターン:
    - http://<hostname/ip address\>:\<port\> | 例: `<http://proxy.example.citrix.com:80>` `<http://10.10.10.10:8080>`
  - PAC/WPAD: PACファイルまたはWPADを使用して、プロキシ設定を自動的に決定します。PACファイルのURLを指定する必要があります（例：`<http://wpad.myproxy.com:30/configuration/pac/Proxy.pac>`）。
    - PAC/WPADファイルの許可されるパターン:
    - http://<hostname/ip address\>:<port\>/<path\>/<Proxy\>.pac | 例: `<http://wpad.myproxy.com:30/configuration/pac/Proxy.pac>`
    - https://<hostname/ip address\>:<port\>/<path\>/<wpad.dat\> | 例: `<http://10.10.10.10/configuration/pac/wpad.dat>`
  - 直接/透過: プロキシサーバーを使用しないか、透過プロキシを使用します。
    - キーワード「DIRECT」を構成する
    - キーワードは大文字と小文字を区別します
- **デフォルト:** 禁止 (無効)

ブラウザコンテンツリダイレクトの統合Windows認証サポート

この設定により、統合Windows認証 (IWA) を使用するWebサイトへのログインが簡素化されます。

- **機能:** ブラウザコンテンツリダイレクトが既存のWindows資格情報を使用してWebサイトに自動的にログインできるようにします。これにより、ユーザー名とパスワードを繰り返し入力する必要がなくなります。
- **オプション:**
  - **許可:** IWAを使用するWebサイト向けにシングルサインオン (SSO) を有効にします。
  - **禁止:** (既定値) SSOを無効にし、毎回資格情報を入力する必要があります。

ブラウザコンテンツリダイレクトサーバーフェッチプロキシ認証

この設定は、サーバーからコンテンツをフェッチする際に、ブラウザコンテンツリダイレクトがWebプロキシとどのように連携するかを制御します。

- **機能:** ブラウザコンテンツリダイレクトがWindows資格情報を使用してプロキシサーバーで認証できるようにし、Webコンテンツへの安全なアクセスを確保します。
- **動作:** 有効にすると、ブラウザコンテンツリダイレクトはKerberosサービスチケットを自動的に取得して使用し、プロキシで認証します。
- **要件:** PACファイルを構成して、ダウンストリームWebプロキシを介してトラフィックをルーティングし、プロキシがKerberos認証を使用するように設定する必要があります。
- **オプション:**
  - **許可:** プロキシサーバーとのKerberos認証を有効にします。
  - **禁止:** (既定値) ブラウザコンテンツリダイレクトは、プロキシで認証するために基本認証またはその他の利用可能な資格情報を使用します。

クライアントセンサーポリシー設定

「**クライアントセンサー**」セクションには、ユーザーセッションでモバイルデバイスのセンサー情報がどのように処理されるかを制御するためのポリシー設定が含まれています。

アプリケーションによるクライアントデバイスの物理的な位置情報の使用を許可する

この設定は、モバイルデバイス上のセッションで実行されているアプリケーションが、ユーザーデバイスの物理的な位置情報を使用できるかどうかを決定します。

デフォルトでは、位置情報の使用は禁止されています。

この設定が禁止されている場合、アプリケーションが位置情報を取得しようとすると、「アクセス拒否」の値が返されます。

この設定が許可されている場合、ユーザーはCitrix Workspace™アプリの位置情報へのアクセス要求を拒否することで、位置情報の使用を禁止できます。AndroidおよびiOSデバイスでは、各セッションで位置情報が最初に要求されたときにプロンプトが表示されます。

「アプリケーションによるクライアントデバイスの物理的な位置情報の使用を許可する」設定を使用するホスト型アプリケーションを開発する際は、以下を考慮してください。

- 位置情報が有効なアプリケーションが位置情報の利用可能性に依存しないようにしてください。その理由は次のとおりです。
  - ユーザーが位置情報へのアクセスを許可しない場合があります。
  - アプリケーションの実行中に位置情報が利用できない、または変更される場合があります。
  - ユーザーが、位置情報をサポートしていない別のデバイスからアプリケーションセッションに接続する場合があります。
- 位置情報が有効なアプリケーションは、次の要件を満たす必要があります。
  - 位置情報機能をデフォルトでオフにする。
  - アプリケーションの実行中に、ユーザーがその機能を許可または禁止するオプションを提供する。
  - アプリケーションがキャッシュする位置データをクリアするオプションをユーザーに提供します。(Citrix Workspaceアプリは位置データをキャッシュしません。)
- 位置情報対応アプリケーションは、位置情報の粒度を管理する必要があります。この管理により、取得されたデータがアプリケーションの目的に適切であることが保証されます。また、関連するすべての法域の規制に準拠します。
- 位置情報サービスを使用する場合は、安全な接続 (TLS または VPN の使用など) を強制します。Citrix Workspaceアプリを信頼できるサーバーに接続します。
- 位置情報サービスの使用に関して、法的助言を得ることを検討してください。

デスクトップUIポリシー設定

デスクトップUIセクションには、デスクトップの壁紙、メニューアニメーション、ドラッグイメージなどの視覚効果を制御するポリシー設定が含まれています。これらのポリシー設定は、クライアント接続で使用される帯域幅の管理に役立ちます。帯域幅の使用量を制限することで、WANでのアプリケーションパフォーマンスを向上させることができます。

> **重要:**

このリリースでは、レガシーグラフィックモードおよびデスクトップコンポジションリダイレクト（DCR）はサポートされていません。このポリシーは、以下を使用する場合の旧バージョンとの互換性のためのみに含まれています。

- XenApp 7.15 LTSR
- XenDesktop 7.15 LTSR
- Windows 7およびWindows 2008 R2を使用している以前のVDAリリース。

デスクトップコンポジションリダイレクト

この設定は、ユーザーによりスムーズなWindowsデスクトップエクスペリエンスを提供するために、ローカルのDirectXグラフィックレンダリングに以下の処理能力を使用するかどうかを指定します。

- ユーザーデバイス上のグラフィック処理ユニット（GPU）
- または、,
- ユーザーデバイス上の統合グラフィックプロセッサ（IGP）

有効にすると、**デスクトップコンポジションリダイレクト**は、サーバーの高いスケーラビリティを維持しながら、応答性の高いWindowsエクスペリエンスを提供します。

デフォルトでは、**デスクトップコンポジションリダイレクト**は無効になっています。

デスクトップコンポジションリダイレクトの選択を解除し、ユーザーセッションで必要となる帯域幅を削減するには、この設定をポリシーに追加する際に**無効**を選択します。

デスクトップコンポジションリダイレクトのグラフィック品質

この設定は、デスクトップコンポジションリダイレクトに使用されるグラフィックの品質を指定します。

デフォルトは「高」です。

「高」、「中」、「低」、または「ロスレス」の品質から選択します。

デスクトップの壁紙

この設定は、ユーザーセッションでの壁紙の表示を許可または禁止します。

デフォルトでは、ユーザーセッションで壁紙を表示できます。

デスクトップの壁紙を選択解除し、ユーザーセッションで必要な帯域幅を削減するには、この設定をポリシーに追加するときに「**禁止**」を選択します。

メニューアニメーション

この設定は、ユーザーセッションでのメニューアニメーションを許可または禁止します。

デフォルトでは、メニューアニメーションは許可されています。

メニューアニメーションは、アクセシビリティのためのMicrosoftの個人設定です。有効にすると、短い遅延の後、スクロールまたはフェードインによってメニューが表示されます。メニューの下部には矢印アイコンが表示されます。その矢印をポイントするとメニューが表示されます。

このポリシー設定が「**許可**」に設定されており、メニューアニメーションのMicrosoft個人設定が有効になっている場合、デスクトップでメニューアニメーションが有効になります。

> **注:**
>
> メニューアニメーションのMicrosoft個人設定への変更は、デスクトップに影響します。セッション終了時にデスクトップが変更を破棄するように設定している場合を考慮してください。この場合、メニューアニメーションを有効にしているユーザーは、その後のセッションでメニューアニメーションを利用できない可能性があります。メニューアニメーションを必要とするユーザーのために、デスクトップのメインイメージでMicrosoft設定を有効にするか、デスクトップがユーザーの変更を保持するようにしてください。

ドラッグ中のウィンドウコンテンツの表示

この設定は、画面上でウィンドウをドラッグする際にウィンドウコンテンツの表示を許可または禁止します。

デフォルトでは、ウィンドウコンテンツの表示は許可されています。

「**許可**」に設定すると、ウィンドウをドラッグしたときにウィンドウ全体が移動するように見えます。「**禁止**」に設定すると、ドロップするまでウィンドウのアウトラインのみが移動するように見えます。

エンドユーザー監視ポリシー設定

エンドユーザー監視セクションには、セッションのトラフィックを測定するためのポリシー設定が含まれています。

エンドポイント位置情報データ収集

デフォルトでは、このポリシーは無効になっています。 有効にすると、エンドポイントデバイスのパブリックIPアドレス、国、都市、インターネットサービスプロバイダー（ISP）を含むエンドポイント位置情報が収集されます。 収集されたデータは、Citrix DirectorまたはMonitorの**セッションパフォーマンス**タブで、選択したユーザーセッションに対して表示されます。

エンドポイントネットワーク遅延測定間隔

デフォルトでは、このポリシーは無効になっています。 この設定は、エンドポイントがネットワーク遅延を測定する頻度を秒単位で指定します。 有効にすると、収集されたデータは、選択したユーザーセッションの**セッションパフォーマンス**タブの下にあるCitrix DirectorまたはMonitorに表示されます。

エンドポイント統計間隔

ネットワークインターフェースタイプ、信号強度、リンク速度、スループット（送信）、スループット（受信）などのエンドポイント統計は、DirectorまたはMonitor UIのセッショントポロジでエンドポイントテレメトリとして利用できます。このテレメトリは、エンドユーザーセッションの問題のトリアージに役立ちます。 エンドポイント統計間隔は、DirectorまたはMonitor UIのセッショントポロジでエンドポイントテレメトリが更新される頻度を秒単位で示します。デフォルトでは、エンドポイントテレメトリは有効になっており、60秒ごとに更新されます。 収集されたデータは、Citrix DirectorまたはMonitorの**セッションパフォーマンス**タブで、選択したユーザーセッションに対して表示されます。

ICA®ラウンドトリップ計算

この設定は、アクティブな接続に対してICAラウンドトリップ計算が実行されるかどうかを決定します。

デフォルトでは、アクティブな接続の計算は有効になっています。

デフォルトでは、各ICAラウンドトリップ測定の開始は遅延されます。この遅延は、ユーザーインタラクションを示すトラフィックが発生するまで続きます。この遅延は無期限に続く可能性があり、ICAラウンドトリップ測定がICAトラフィックの唯一の原因となるのを防ぐように設計されています。

ICAラウンドトリップ計算間隔

この設定は、ICAラウンドトリップ計算が実行される頻度を秒単位で指定します。

デフォルトでは、ICAラウンドトリップは15秒ごとに計算されます。

アイドル接続のICAラウンドトリップ計算

この設定は、アイドル接続に対してICAラウンドトリップ計算が実行されるかどうかを決定します。

デフォルトでは、アイドル接続に対して計算は実行されません。

デフォルトでは、各ICAラウンドトリップ測定の開始は遅延されます。この遅延は、ユーザー操作を示すトラフィックが発生するまで続きます。この遅延は無期限に続く可能性があり、ICAラウンドトリップ測定がICAトラフィックの唯一の原因となるのを防ぐように設計されています。

強化されたデスクトップエクスペリエンスポリシー設定

強化されたデスクトップエクスペリエンスポリシー設定は、ローカルのWindows 7デスクトップのように見えるサーバーオペレーティングシステム上でセッションを実行します。

デフォルトでは、この設定は許可されています。

仮想デスクトップ上にWindowsクラシックテーマのユーザープロファイルが存在する場合、このポリシーはそのユーザーに強化されたデスクトップエクスペリエンスを提供しません。Windows 7テーマのユーザープロファイルを持つユーザーが、Windows Server 2012を実行している仮想デスクトップにログオンする場合を考えます。また、このポリシーが構成されていないか、無効になっている場合、そのユーザーはテーマの適用に失敗したことを示すエラーメッセージを目にします。

どちらの場合も、ユーザープロファイルをリセットすることで問題が解決します。

アクティブなユーザーセッションを持つ仮想デスクトップでポリシーを無効にすると、それらのセッションのインターフェイスはWindows 7およびWindowsクラシックデスクトップで一貫性がなくなります。この不整合を避けるために、このポリシー設定を変更した後、仮想デスクトップを再起動してください。その後、仮想デスクトップ上のすべてのローミングプロファイルを削除します。Citrix®は、プロファイル間の不整合を避けるために、仮想デスクトップ上の他のユーザープロファイルも削除することを推奨しています。

環境でローミングユーザープロファイルを使用しているとします。この場合、プロファイルを共有するすべての仮想デスクトップで、強化されたデスクトップエクスペリエンス機能が有効または無効になっていることを確認してください。

Citrixは、サーバーオペレーティングシステムとクライアントオペレーティングシステムを実行している仮想デスクトップ間でローミングプロファイルを共有することを推奨していません。クライアントおよびサーバーオペレーティングシステムのプロファイルは異なります。両方のタイプ間でローミングプロファイルを共有すると、ユーザーが両者の間を移動する際にプロファイルプロパティに不整合が生じる可能性があります。

ファイルリダイレクトポリシー設定

ファイルリダイレクトセクションには、クライアントドライブマッピングおよびクライアントドライブ最適化に関連するポリシー設定が含まれています。

クライアントドライブの自動接続

この設定は、ユーザーがログオンしたときのクライアントドライブの自動接続を許可または禁止します。

デフォルトでは、自動接続は許可されています。

この設定をポリシーに追加する場合は、自動接続したいドライブの種類の設定を有効にしてください。たとえば、ユーザーのCD-ROMドライブの自動接続を許可するには、この設定と**クライアント光学ドライブ**設定を構成します。

以下のポリシー設定が関連しています。

- **クライアントドライブリダイレクト**
- **クライアントフロッピーディスクドライブ**
- **クライアント光学ドライブ**
- **クライアント固定ドライブ**
- **クライアントネットワークドライブ**
- **クライアントリムーバブルドライブ**

クライアントドライブリダイレクト

この設定は、ユーザーデバイス上のドライブとの間でファイルリダイレクトを有効または無効にします。

既定では、ファイルリダイレクトは有効になっています。

> **注:**
>
> クライアントドライブリダイレクトポリシー設定は、汎用USBリダイレクトを使用してセッションにマップされたドライブには適用されません。

> 有効にすると、ユーザーはすべてのクライアントドライブにファイルを保存できます。無効にすると、すべてのファイルリダイレクトが防止されます。この構成は、個々のファイルリ

> ダイレクト設定の状態に関係なく適用されます。個々のファイルリダイレクト設定には、クライアントフロッピードライブとクライアントネットワークドライブが含まれます。

関連するポリシー設定は次のとおりです。

- **クライアントフロッピードライブ**
- **クライアント光学ドライブ**
- **クライアント固定ドライブ**
- **クライアントネットワークドライブ**
- **クライアントリムーバブルドライブ**

クライアント固定ドライブ

この設定により、ユーザーはユーザーデバイス上の固定ドライブへのファイルアクセスまたは保存を許可または禁止されます。

既定では、クライアント固定ドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合は、**クライアントドライブリダイレクト**設定が存在し、許可に設定されていることを確認してください。これらの設定が無効になっている場合、クライアント固定ドライブはマップされず、**クライアント固定ドライブ**設定の状態に関係なく、ユーザーはこれらのドライブに手動でアクセスできません。

ユーザーがログオンしたときに固定ドライブが自動的に接続されるように、**クライアントドライブの自動接続**設定を構成します。

クライアントフロッピードライブ

この設定により、ユーザーはユーザーデバイス上のフロッピードライブにアクセスしたりファイルを保存したりできるようになります。

デフォルトでは、クライアントフロッピードライブへのアクセスは許可されています。

この設定をポリシーに追加するときは、**クライアントドライブのリダイレクト**設定が存在し、許可に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントフロッピーディスクドライブはマップされず、**クライアントフロッピーディスクドライブ**設定の状態に関係なく、ユーザーはこれらのドライブに手動でアクセスできません。

ユーザーがログオンしたときにフロッピーディスクドライブが自動的に接続されるようにするには、「**クライアントドライブの自動接続**」設定を構成します。

クライアントネットワークドライブ

この設定は、ユーザーがユーザーデバイスを介してネットワーク（リモート）ドライブにファイルにアクセスしたり保存したりすることを許可または禁止します。

デフォルトでは、クライアントネットワークドライブへのアクセスは許可されています。

この設定をポリシーに追加するときは、**クライアントドライブのリダイレクト**設定が存在し、許可に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントネットワークドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、**クライアントネットワークドライブ**設定の状態に関係なく適用されます。

ユーザーがログオンしたときにネットワークドライブが自動的に接続されるようにするには、「**クライアントドライブの自動接続**」設定を構成します。

クライアント光学ドライブ

この設定では、ユーザーが以下にアクセスしたり、ファイルを保存したりすることを許可または禁止します。

- ユーザーデバイス上のCD-ROM
- ユーザーデバイス上のDVD-ROM
- ユーザーデバイス上のBD-ROMドライブ。

デフォルトでは、クライアント光学ドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合、「**クライアントドライブのリダイレクト**」設定が存在し、「**許可**」に設定されていることを確認してください。これらの設定が無効になっている場合、クライアント光学ドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、「**クライアント光学ドライブ**」設定の状態にかかわらず適用されます。

ユーザーがログオンしたときに光学ドライブが自動的に接続されるようにするには、「**クライアントドライブの自動接続**」設定を構成します。

クライアントリムーバブルドライブ

この設定により、ユーザーはユーザーデバイス上のUSBドライブへのファイルアクセスまたは保存を許可または禁止されます。

デフォルトでは、クライアントリムーバブルドライブへのアクセスは許可されています。

この設定をポリシーに追加する際は、**クライアントドライブのリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。これらの設定が無効になっている場合、クライ

アントリムーバブルドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、**クライアントリムーバブルドライブ**設定の状態に関係なく適用されます。

ユーザーがログオンしたときにリムーバブルドライブが自動的に接続されるように、**クライアントドライブの自動接続**設定を構成します。

ホストからクライアントへのリダイレクト

この設定により、URLおよび一部のメディアコンテンツのファイルタイプ関連付けを有効または無効にし、ユーザーデバイスで開くことができます。無効にすると、コンテンツはサーバーで開かれます。

デフォルトでは、ファイルタイプ関連付けは無効になっています。

この設定を有効にすると、以下のURLタイプがローカルで開かれます。

- HTTP
- HTTPS
- リアルプレイヤーおよびクイックタイム (RTSP)
- リアルプレーヤーとクイックタイム (RTSPU)
- レガシー Real Player (PNM)
- マイクロソフト メディア サーバー (MMS)

クライアントドライブ文字の保持

この設定により、クライアントドライブをセッション内で同じドライブ文字にマップすることを有効または無効にします。

デフォルトでは、クライアントドライブ文字は保持されません。

この設定をポリシーに追加する場合は、**クライアントドライブのリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。

読み取り専用クライアントドライブアクセス

この設定は、ユーザーとアプリケーションが以下を行うことを許可または禁止します。

- マップされたクライアントドライブ上にファイルを作成する
- マップされたクライアントドライブ上のファイルを変更する
- マップされたクライアントドライブ上のフォルダーを変更する

デフォルトでは、マップされたクライアントドライブ上のファイルとフォルダーは変更できます。

「有効」に設定されている場合、ファイルとフォルダーは読み取り専用権限でアクセスできます。

この設定をポリシーに追加する場合は、**クライアントドライブのリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。

特殊フォルダーのリダイレクト

この設定により、Citrix Workspace™ appおよびWeb Interfaceのユーザーは、セッションからローカルのドキュメントおよびデスクトップの特殊フォルダーを表示することを許可または禁止します。

デフォルトでは、特殊フォルダーのリダイレクトは許可されています。

この設定は、ポリシーを通じてフィルター処理されたオブジェクトが特殊フォルダーのリダイレクトを持つことを、他の場所に存在する設定に関係なく、禁止します。この設定が禁止されている場合、StoreFront™、Web Interface、またはCitrix Workspace appに指定された関連設定はすべて無視されます。

特殊フォルダーのリダイレクトを許可するユーザーを定義するには、**Allowed**を選択し、この機能を有効にしたいユーザーにフィルターを適用したポリシーにこの設定を含めます。この設定は、他のすべての特殊フォルダーリダイレクト設定を上書きします。

ユーザーがローカルハードドライブ上のファイルにアクセスしたり保存したりすることを禁止するポリシー設定は、特殊フォルダーのリダイレクトが機能することも禁止します。これは、特殊フォルダーのリダイレクトがユーザーデバイスと対話する必要があるために発生します。

この設定をポリシーに追加する場合は、**Client fixed drives**設定が存在し、Allowedに設定されていることを確認してください。

ファイル転送ポリシー

デフォルトでは、ファイル転送は有効になっています。これらのポリシーは、Web Studioの**User setting - ICA\File Redirection**にあります。ファイル転送ポリシーを使用する際は、以下を考慮してください。

- **File transfer for Citrix Workspace app for Chrome OS/HTML5** - ユーザーがCitrix Virtual Apps and Desktopsセッションとデバイス間でファイルを転送することを許可または禁止します。
- **Upload file for Citrix Workspace app for Chrome OS/HTML5** - ユーザーがデバイスからCitrix Virtual Apps and Desktopsセッションにファイルをアップロードすることを許可または禁止します。

- **Download file for Citrix Workspace app for Chrome OS/HTML5** - ユーザーがCitrix Virtual Apps and Desktopsセッションからデバイスにファイルをダウンロードすることを許可または禁止します。

> **注:**
>
> ファイル転送ポリシーは、Citrix Workspace app for HTML5およびCitrix Workspace app for Chrome OSにのみ適用されます。

非同期書き込みの使用

この設定は、非同期ディスク書き込みを有効または無効にします。

デフォルトでは、非同期書き込みは無効になっています。

非同期ディスク書き込みは、WAN経由でのファイル転送速度とクライアントディスクへの書き込み速度を向上させることができます。WANは通常、比較的高帯域幅で高遅延が特徴です。ただし、接続またはディスクに障害が発生した場合、書き込み中のクライアントファイルは未定義の状態になる可能性があります。この未定義の状態が発生した場合、ポップアップウィンドウが影響を受けるファイルをユーザーに通知します。ユーザーは、再接続時またはディスク障害が修正されたときに中断されたファイル転送を再開するなどの是正措置を講じることができます。

Citrix®は、リモート接続が必要で、良好なファイルアクセス速度を持つユーザーに対してのみ、非同期ディスク書き込みを有効にすることを推奨します。また、接続またはディスク障害が発生した場合に、失われたファイルやデータを容易に回復できるユーザーに対しても推奨します。

この設定をポリシーに追加する際は、**クライアントドライブリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。この設定が無効になっている場合、非同期書き込みは行われません。

クリップボードリダイレクト

クリップボードリダイレクトは、Citrix Virtual Apps and Desktops™の基本的な機能であり、ユーザーのローカルエンドポイントと仮想Citrixセッション間でデータをシームレスにコピーアンドペーストすることを可能にします。

クリップボードリダイレクトにより、ユーザーはテキスト、画像、ファイルなどのデータを、ローカルデバイスで実行されているアプリケーションとCitrixセッション内のアプリケーション間でコピーアンドペーストできます。これは、ユーザーデバイス上のクリップボードをVDA上のク

リップボードにマッピングすることで実現されます。デフォルトでは、クリップボードリダイレクトは許可されています。

クリップボードリダイレクトは、HDX™プロトコル内の個別の仮想チャネルを介して機能します。ファイル転送とドラッグアンドドロップには、追加の仮想チャネルが使用されます。ユーザーがローカルデバイスでデータをコピーすると、Citrix Workspace™アプリがそのデータを傍受し、セッションで実行されているアプリケーションに貼り付けられるようにします。実際のデータは、VDA上のアプリケーションにデータが貼り付けられた場合に転送されます。Citrixセッションからクライアントにコピーする場合は、このプロセスが逆になります。

クライアントからセッションへ、およびセッションからクライアントへのクリップボードリダイレクトのこの組み合わせは、双方向クリップボードリダイレクトとも呼ばれます。

> **注：**
>
> 詳細については、「Citrix Virtual Channels」を参照してください。

主要な概念

クライアントからセッションへ (Endpoint to Session または クライアントからVDAへ とも呼ばれます)。ユーザーのローカルデバイスでコピーされたデータ（クリップボードに置かれたデータ）は、仮想セッション内に貼り付けられるようになります。

セッションからクライアントへ (Session to Endpoint または VDAからクライアントへ とも呼ばれます)。仮想セッション内のアプリケーションからコピーされたデータは、ユーザーのローカルデバイスに貼り付けられるようになります。

クロスセッション (セッション間またはVDA間)。あるCitrixセッションからコピーされたデータを、ローカルエンドポイントのクリップボードに保存することなく、別のCitrixセッションに貼り付けることができる新しいクリップボード転送方法です。この機能は、Citrix Virtual Apps™ and Desktops バージョン2507でプレビュー機能として利用でき、クロスセッションクリップボード交換機能と呼ばれています。詳細については、「クロスセッションクリップボード」を参照してください。

設定

クリップボードリダイレクトは、Citrix®ポリシーによって制御されます。これらのポリシーは、クリップボードリダイレクトの動作を細かく調整するためのさまざまな設定を提供します。

デフォルトでは、双方向クリップボードリダイレクトが有効になっています。ユーザーは、Citrixセッションからローカルエンドポイントへ、またその逆へデータをコピーして貼り付けることができます。

コア設定

コアとなるクリップボードリダイレクトの設定は、「クライアントクリップボードリダイレクトポリシー」です。このポリシーは、クリップボードリダイレクトが許可されるかどうかを制御します。デフォルトでは、クリップボードリダイレクトは許可されています。

クリップボードリダイレクトを無効にすると、Citrix仮想環境外への機密データの偶発的または悪意のある転送を防ぐことで、セキュリティが向上します。また、クリップボードを介して潜在的に有害なデータがCitrix環境に導入されるのを防ぐのにも役立ちます。ただし、これはエンドユーザーエクスペリエンスに悪影響を与える可能性があります。

クリップボードリダイレクトを禁止するには、「クライアントクリップボードリダイレクトポリシー」を「禁止」に設定します。

リダイレクト(/en-us/citrix-virtual-apps-desktops/2511/media/prohibit_clipboard_redirection.png)

「禁止」に設定されている場合、クリップボードリダイレクトは完全に無効になり、他のすべてのクリップボード関連ポリシーは無視されます。

ユーザーは、Citrixセッション内で実行されているアプリケーションとローカルエンドポイントデバイスの間でデータをコピーして貼り付けることができます。ただし、Citrixセッションとの間でコピー＆ペーストはできません。

方向別クリップボード制御

方向別クリップボード制御を使用すると、管理者はクリップボードデータフローの方向をきめ細かく制御できます。これは、単方向クリップボード制御とも呼ばれます。

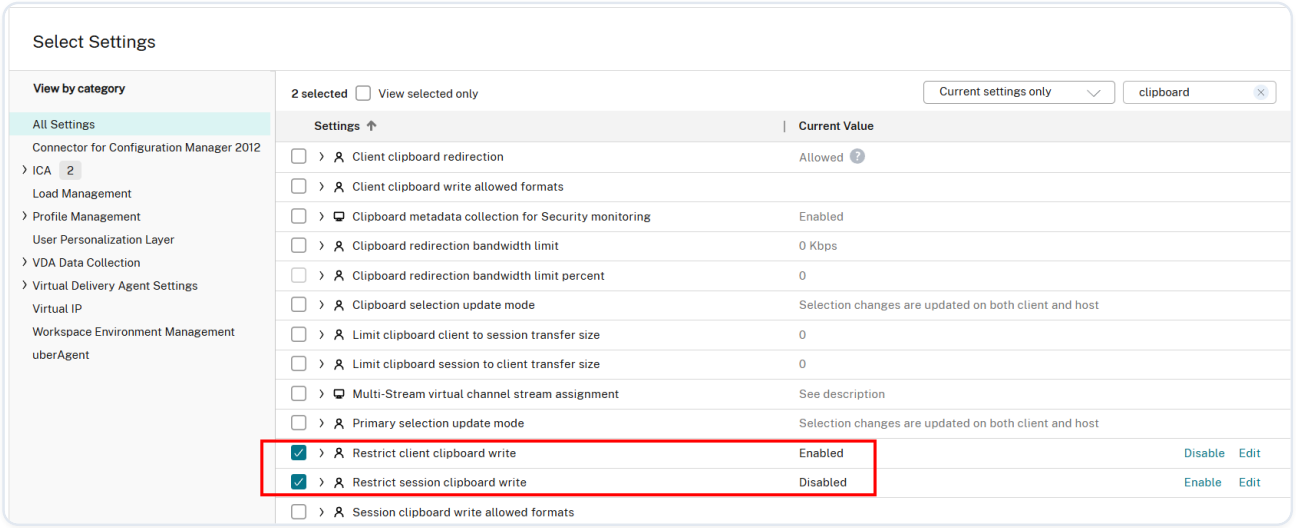
単方向制御には、主に2つのモードがあります。

- **クライアントからセッションへ:** この構成では、「クライアントクリップボード書き込みの制限」ポリシーが使用され、クリップボードデータは、ユーザーのエンドポイントデバイス（クライアント）からリモートCitrixセッションへ排他的に流れることが許可されます。これは、ユーザーがローカルマシンから情報をコピーし、Citrixセッション内で実行されているアプリケーションに貼り付けることができることを意味しますが、Citrixセッションからデータをコピーしてローカルマシンに貼り付けることはできません。このモードは、セキュアなセッションから制御の少ないエンドポイントへのデータ漏洩が重大な懸念事項であるシナリオで役立ちます。

- **セッションからクライアントへ:** この構成では、「セッションクリップボード書き込みの制限」ポリシーにより、クリップボードデータはCitrixセッションからクライアントデバイスへ排他的に流れることが許可されます。ユーザーは、リモートセッション内のアプリケーションから情報をコピーし、ローカルマシンに貼り付けることができますが、ローカルマシンからデータをコピーしてCitrixセッションに貼り付けることはできません。この設定は、エンドポイントからセキュアなCitrix環境への潜在的に悪意のあるデータや不正なデータの導入を防ぐことが主な目的である場合によく使用されます。

次の表は、一方向クリップボード制御に関するCitrixクリップボードポリシーについて説明します。

クリップボードの方向性	クリップボードポリシー
双方向 - セッションからクライアント、およびクライアントからセッション	クライアントクリップボードリダイレクト: 有効 (デフォルト)
一方向 - クライアントからセッションのみ	クライアントクリップボードリダイレクト: 有効 (デフォルト)
クライアントクリップボード書き込みの制限: 有効	一方向 - セッションからクライアントのみ
クライアントクリップボードリダイレクト: 有効 (デフォルト)	セッションクリップボード書き込みの制限: 有効



上記の例では、両方の方向性クリップボードポリシーが強調表示されており、この構成では、「クライアントクリップボード書き込みの制限」設定が「有効」に設定されているため、クライアントからセッションへのクリップボードリダイレクトのみが許可されます。

クリップボード形式の制御

Citrixクリップボード形式制御ポリシーは、特定のクリップボード形式へのデータ転送を制限することでクリップボードのセキュリティを強化し、セッションとクライアント間、およびその逆方向でコピー＆ペーストできるデータの種類を制御します。これにより、特定のクリップボードデータ形式を選択的に許可または拒否できます。

クリップボード交換形式は、マルチメディアプログラムから複雑なスプレッドシートやワープロまで、多様なアプリケーション間で情報をシームレスに転送できるようにするために使用されます。これらの形式は、コピー、切り取り、貼り付けが可能なデータの構造とエンコーディングを定義し、アプリケーションが交換されるコンテンツを理解し処理できるようにします。

たとえば、Webブラウザからテキストをコピーして Word文書に貼り付ける場合、クリップボードはテキストベースの形式を使用します。しかし、コピーされたコンテンツに画像、表、リッチテキスト形式が含まれている場合、クリップボードは元の外観と構造を保持するために、RTF（リッチテキスト形式）やHTML（ハイパーテキストマークアップ言語）のようなより高度な形式を利用します。同様に、CADプログラムとプレゼンテーションツールのような特殊なアプリケーション間でデータを交換する場合、クリップボードはグラフィックデータや複雑なデータの正確な表現を保証するために、アプリケーション固有の形式または一般的なメタファイル形式を使用することがあります。

クリップボード形式制御ポリシーは、方向性クリップボード制御ポリシーと連携して機能するように設計されています。

クリップボード形式制御を使用すると、管理者は許可される形式を決定できます。たとえば、次のようになります。

- 両方向でプレーンテキストのみを許可する
- セッションからクライアントへのクリップボード転送をプレーンテキストと画像のみに許可する

または、クライアントからセッションへの貼り付けを特定の形式に制限しつつ、セッションからクライアントへの貼り付けはすべての形式を許可する組み合わせも可能です。

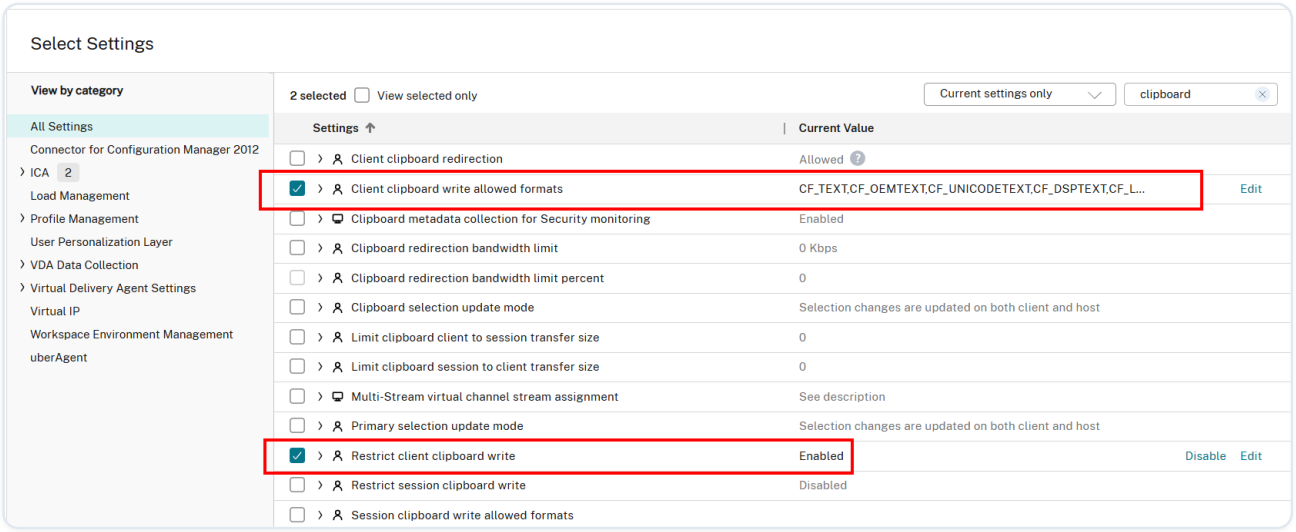
クリップボード形式の動作を制御する主要なポリシーは2つあります。

クライアントクリップボード書き込み許可形式: このポリシーは、リモートセッションからクライアントクリップボードに書き込みが許可されるクリップボードデータ形式を明示的に規定します。たとえば、管理者はこのポリシーを設定して、プレーンテキストのみがクライアントにコピーされるようにし、潜在的に悪意のあるリッチテキスト、画像、またはファイルの転送を防ぐことができます。

セッションクリップボード書き込み許可形式: 次に、このポリシーは、クライアントからリモートセッションにコピーが許可されるクリップボードデータ形式を指定します。このポリシーは、リモート環境に転送できる情報の種類を制御するために不可欠です。組織はこれをプレーンテキストのみに制限し、ユーザーが誤ってまたは意図的に機密ファイルや画像をローカルマシンからセキュリティの低い、または不正なリモートアプリケーションに貼り付けることを防ぐことができます。

> **注:**
>
> クリップボードの許可形式は、対応する単方向クリップボードポリシーも設定されている場合にのみ評価されます。

> クライアントクリップボードの書き込み形式をテキストベースのデータ形式のみに制限するには、「クライアントクリップボード書き込みを制限」ポリシーと「クライアントクリップボード書き込み許可形式」の両方を構成する必要があります。この例では、「クライアントクリップボード書き込みを制限」を**有効**に設定し、「クライアントクリップボード書き込み許可形式」にはすべてのクリップボードテキスト形式を含める必要があります。



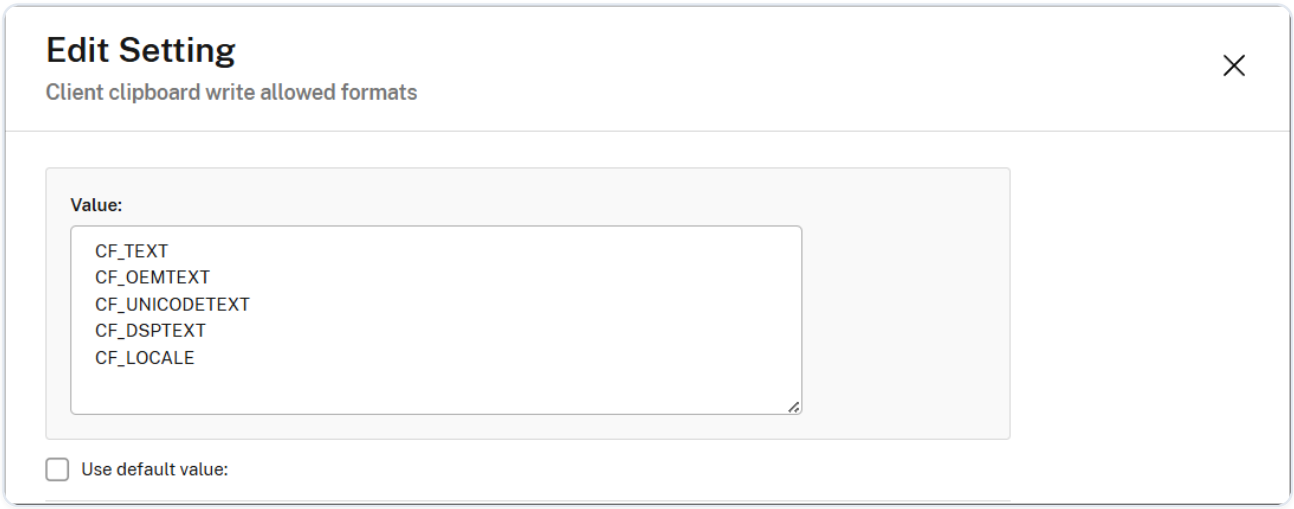
書き込み形式の制限を構成するには、対応するポリシーを編集し、各エントリが別々の行に配置されていることを確認してください。

例として：

CF_TEXT CF_BITMAP

は正しいですが、以下は正しくありません：

CF_TEXT,CF_BITMAP



標準クリップボード形式

以下の表は、標準クリップボード形式について説明しています。

クリップボード形式	タイプ	説明
CF_TEXT	テキスト形式	標準ANSI文字セットのテキスト。各行は復帰/改行（CR-LF）の組み合わせで終わります。
CF_OEMTEXT	テキスト形式	相手先ブランド製造元 (OEM) の文字セットを使用したテキスト。CF_TEXTに似ています。
CF_UNICODETEXT	テキスト形式	Unicode形式のテキスト。NULL終端文字は不要です。
CF_LOCALE	テキスト形式	クリップボードテキストに関連付けられたロケール識別子へのハンドル。これにより、テキストの言語と地域設定を正しく解釈できます。
CF_HTML*	テキスト形式	HTML形式のテキストを表し、リッチテキスト、リンク、画像をサポートするアプリケーション間でコピー＆ペーストできるようにします。

クリップボード形式	タイプ	説明
CF_BITMAP	画像形式	デバイス依存ビットマップ。画像データは特定の出力デバイスに固有です。
CF_DIB	画像形式	デバイス非依存ビットマップ。この形式には色情報と寸法が含まれており、どのデバイスでも正しく表示できます。
CF_DIBV5	画像形式	CF_DIB (デバイス非依存ビットマップ、バージョン5) の拡張で、カラープロファイルや透明度用のアルファチャンネルなどの高度な機能が含まれています。
CF_PALETTE	画像形式	カラーパレットへのハンドル。アプリケーションが他のクリップボードデータ（通常はビットマップ）の色を制御するために使用します。
CF_TIFF	画像形式	タグ付き画像ファイル形式。出版や写真で使われる一般的な高品質画像形式です。
CF_METAFILEPIC	メタファイル形式	メタファイルピクチャ構造へのハンドル。これは、画像を再作成するためのGDI（Graphics Device Interface）関数のコレクションを保存するための古い形式です。
CF_ENHMETAFILE**		拡張メタファイルへのハンドル。これはCF_METAFILEPICTのより現代的で堅牢なバージョンであり、より優れた画質とデバイス非依存性を提供します。

注:

- HTML形式はデフォルトで無効になっています。HTML形式のクリップボードサポートを有効にすると、セキュリティリスクが生じる可能性があります。Webページからコンテンツをコピーすると、埋め込まれたスクリプトもコピーされます。このコンテンツがHTMLをレンダリングするアプリケーションに貼り付けられると、スクリプトが実行される可能性があります。この形式を有効にする際は注意してください。
- 拡張メタファイルのクリップボード転送は、Citrix Virtual Apps and Desktops™ バージョン2511より前では利用できません。 これらの標準形式の他に、Citrix® はデータ交換形式や特殊な形式など、以下の特定のクリップボードデータ形式もサポートしています。

データ交換形式

クリップボードのデータ交換形式は、マルチメディアプログラムやスプレッドシートなどのさまざまなアプリケーション間でのデータ転送を容易にします。

クリップボード形式	説明
CF_SYLK	シンボリックリンク形式。Microsoft Excelのようなスプレッドシートアプリケーション間でデータを交換するためにMicrosoftが作成した古い形式です。
CF_DIF	データ交換形式。スプレッドシートプログラム間でデータを交換するためのテキストベースの形式です。
CF_RIFF	リソース交換ファイル形式。オーディオやビデオなどのマルチメディアデータを保存するためのコンテナ形式です。
CF_WAVE	波形オーディオ形式。オーディオデータを表します。

カスタムクリップボード形式

これらのクリップボード形式に加えて、追加のカスタムクリップボード形式も構成できます。これは、VDA上のオペレーティングシステムに登録されている形式にのみ適用されます。

詳細については、カスタム登録クリップボード形式を参照してください。

変換可能なクリップボード形式

Microsoft Windowsは、さまざまなクリップボード形式をネイティブでサポートしています。クリップボードの内容をコピーして貼り付ける際、Windowsはクリップボードデータを他の互換性のあるクリップボード形式に自動的に変換しようとします。これにより、コンテンツをさまざまなアプリケーションに簡単に貼り付けることができます。

データ形式がクリップボードに投稿されると、Windowsは、他のアプリケーションへの貼り付けが成功する可能性を高めるために、元々投稿された形式のいずれかから変換して取得できる追加の形式を自動的に追加します。

ターゲットアプリケーションが、ソースが直接提供できない形式を要求した場合、Windowsはクリップボードデータをある形式から別の形式に自動的に変換します。

たとえば、ワープロから書式設定されたテキストをコピーする場合、Windowsは、要求元のアプリケーションに対して、元の書式設定されたテキストだけでなく、プレーンテキストなどの他の形式も利用可能にします。

別の例として、クリップボードデータにCF_TEXTクリップボード形式のプレーンテキストデータが含まれており、データを貼り付けるアプリケーションがCF_UNICODETEXT形式のUnicodeテキストを要求した場合、Windowsは貼り付けプロセス中にクリップボードデータを自動的に変換します。

> **注：**
>
> 一部の変換では、たとえばリッチテキストをプレーンテキストに自動変換する場合など、情報が失われる可能性があります。

クリップボード形式	説明
CF_TEXT	CF_TEXT
	CF_OEMTEXT
	CF_UNICODETEXT
	CF_LOCALE
CF_BITMAP	CF_BITMAP

クリップボード形式	説明
	CF_DIB
	CF_DIBV5
CF_METAFILEPICT	CF_METAFILEPICT
	CF_ENHMETAFILE
CF_OEMTEXT	CF_TEXT
	CF_OEMTEXT
	CF_UNICODETEXT
	CF_LOCALE
CF_DIB	CF_BITMAP
	CF_DIB
	CF_DIBV5
CF_UNICODETEXT	CF_TEXT
	CF_OEMTEXT
	CF_UNICODETEXT
	CF_LOCALE
CF_ENHMETAFILE	CF_METAFILEPICT
	CF_ENHMETAFILE
CF_DIBV5	CF_BITMAP
	CF_DIB
	CF_DIBV5

> **注：**
>
> クリップボード形式の変換はWindows OSに依存しており、この表は将来のOSバージョンで変更される可能性があります。
>
> Windowsのクリップボードシステムがすべての形式間で自由に変換するわけではないことを理解することが重要です。自動変換は、主に異なるテキストエンコーディング間やビットマップのバリエーション間など、いくつかの主要なタイプに限定されています。

他のほとんどの形式では、ソースアプリケーションが複数の形式を一度にクリップボードに配置することで互換性が確保されます。たとえば、Excelからグラフをコピーすると、データはOffice描画シェイプ (CFX_OfficeDrawingShape)、拡張メタファイル (CF_ENHMETAFILE)、および単純なビットマップ (CF_DIB) として配置される場合があります。これはクリップボードによる変換ではなく、異なる貼り付けシナリオのためにソースアプリケーションが複数の表現を提供しているものです。
クリップボード形式の制御と変換可能な形式
クリップボード形式制御ポリシーとセッション間クリップボード構成を設計する際には、変換可能な形式を考慮に入れる必要があります。たとえば、クライアントからクリップボードへのテキストベースのコンテンツのみを明示的に許可したい場合は、すべてのテキストベースの形式を「Session Clipboard Write Allowed Formats」ポリシーに追加する必要があります。この例では、以下の形式をポリシーに追加する必要があります。

CF_TEXT

CF_UNICODETEXT

CF_DSPTEXT

CF_LOCALE

CF_OEMTEXT

同様に、あるセッションから別のセッションにそのような種類のデータをコピーする際に、すべてのファイル形式をセッション間で転送したい場合は、すべてのファイルクリップボード形式をCrossSessionFormats構成に追加する必要があります。

CFX_FILES

CFX_HFDROP

クリップボード転送サイズ制限

クリップボード転送サイズ制限を使用すると、1回のコピー＆ペーストのクリップボード操作で転送できるデータのサイズに制限を設定できます。デフォルトでは、これらの設定は無効になっており、クライアントからセッションへ、およびセッションからクライアントへのクリップボード転送に制限はありません。

転送サイズ制限は、帯域幅管理に役立ちます。大規模なクリップボード転送は、特に多数の同時ユーザーがいる環境では、かなりのネットワーク帯域幅を消費する可能性があります。制限を設定することで、管理者はすべてのユーザーに対してよりスムーズなパフォーマンスを確保し、ネットワークの輻輳を防ぐことができます。

無制限のクリップボード転送は、セキュリティリスクをもたらす可能性があります。悪意のあるソフトウェアや不正なユーザーが、大量の機密データをセッションの内外にコピーする可能性があります。転送サイズを制限することは、このようなデータ漏洩に対する予防策となります。

クリップボード転送サイズ制限を構成する際、管理者は以下を考慮する必要があります。

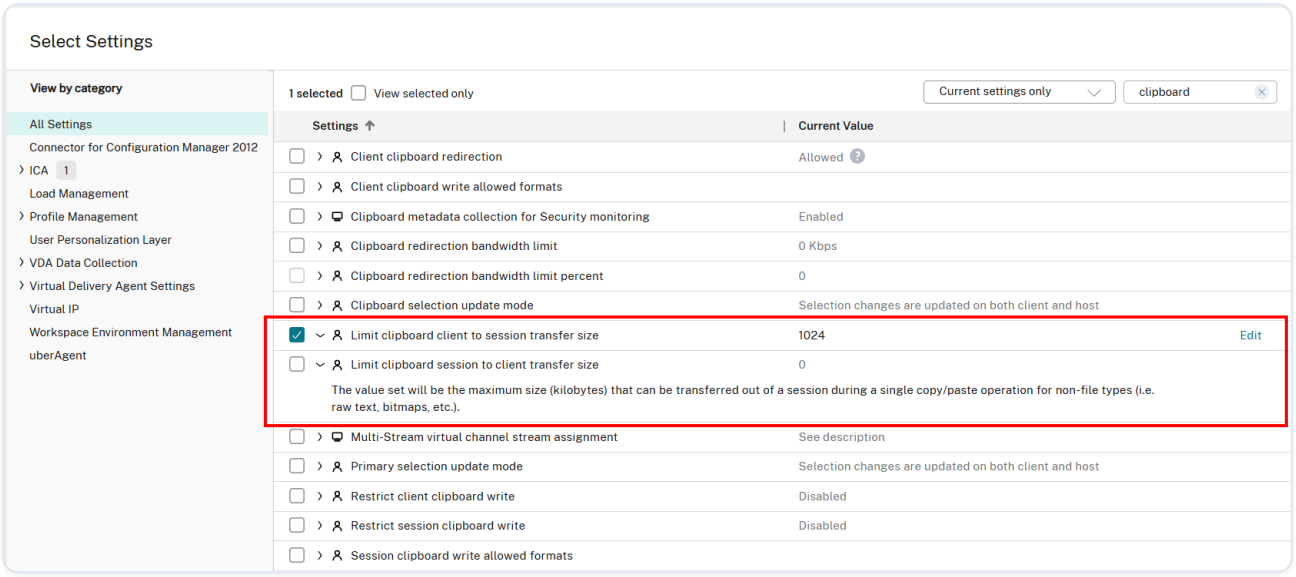
- ユーザーのニーズ: ユーザーの一般的なコピー＆ペースト要件は何ですか？過度に制限的な制限を課すと、生産性が妨げられる可能性があります。
- 帯域幅の使用状況: 利用可能なネットワーク帯域幅はどれくらいで、何人の同時ユーザーが予想されますか？
- 関連するセキュリティポリシー: 組織のデータセキュリティおよびコンプライアンス要件は何ですか？

クリップボードデータ転送をきめ細かく制御するための2つの主要な設定があります。

クリップボードのクライアントからセッションへの転送サイズを制限: この設定は、ユーザーのローカルデバイス（クライアント）からリモートセッション（仮想デスクトップやシームレスアプリケーションなど）にコピーして貼り付けることができるデータの最大サイズをキロバイト単位で構成します。

クリップボードのセッションからクライアントへの転送サイズを制限: 次に、この設定は、リモートセッション内からコピーしてユーザーのローカルデバイスに貼り付けることができるデータの最大サイズをキロバイト単位で制御します。これは、ユーザーが仮想化環境内で機密データを扱っており、クライアントへの大量のデータ流出を防ぐ必要がある場合に特に重要です。

この例では、クライアントからセッションへのクリップボード制限は1024キロバイトに制限されています。



注:

サイズ制限は、固定の文字数ではなく、データサイズ（キロバイト、KB）に基づいています。可変文字エンコーディング（例えばUnicodeなど）のため、コピーできる文字数は異なります。例えば、10 KBの制限では、標準のANSIテキストよりもUnicodeテキストの方が保持できる文字数が少なくなります。

以下の例では、「クライアント転送サイズにクリップボードセッションを制限」ポリシーが1 KBに設定されています。

KBの例(/en-us/citrix-virtual-apps-desktops/2511/media/clipboard-kbexample.png)

このクリップボード転送サイズ制限が適用されている場合、選択されたテキストは、左側のCitrix®セッションから右側のローカルのメモ帳に転送できる最大文字数です。ユーザーがこのCitrixセッションからクライアントにさらに多くの文字をコピーしようとすると、テキストは切り捨てられず、代わりに貼り付け操作全体が失敗します。画像やファイルなどの他のデータ型をコピーしようとすると、コンテンツが設定された最大転送サイズよりも大きい場合も失敗します。

このポリシーを設定する際は、ユーザーが扱うテキストデータの種類を考慮してください。多言語コンテンツやリッチテキストを頻繁に扱う場合、Unicodeテキストのデータサイズが大きいため、より高いキロバイト制限を設定する必要があるかもしれません。

クリップボード転送サイズ制限は、**許可されているすべてのクリップボード形式**に適用されます。

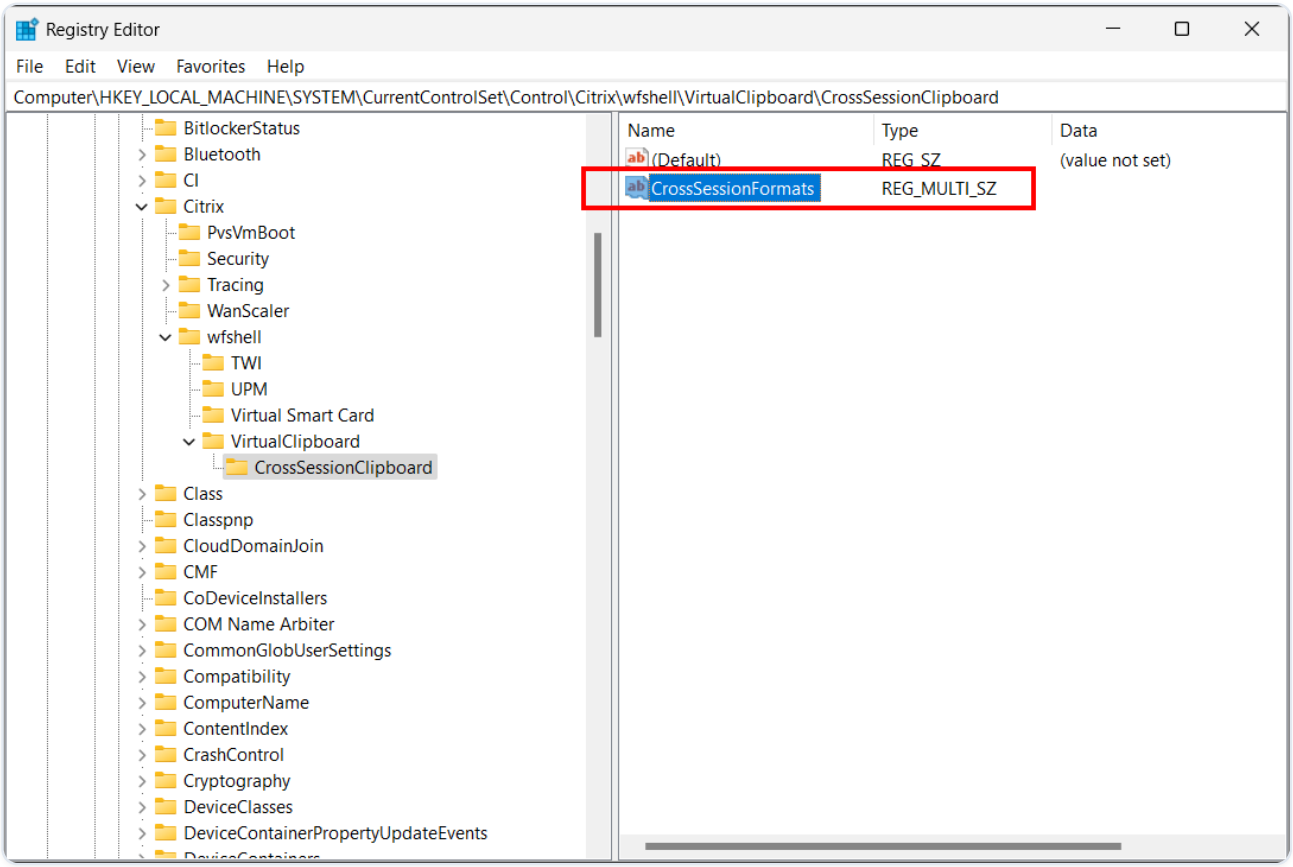
クリップボードのサイズ制限は、許可されているすべてのクリップボード形式で普遍的に適用されます。これは、データ型（テキスト、画像、ファイルなど）に関係なく、転送できるデータの最大量を制限が決定することを意味します。

クロスセッションクリップボード交換 (プレビュー)

構成

クロスセッションクリップボードプレビューは、VDA上で次のレジストリエントリを作成することで有効にできます。

1. regedit.exeを使用してWindowsレジストリエディターを開きます。
2. `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\wfshell\Virtual Clipboard\CrossSessionClipboard\` に移動します。
3. `CrossSessionFormats` という名前のREG_MULTI_SZ値を作成します。



CrossSessionFormatsは、クロスセッションクリップボードを介してトンネルされるクリップボード形式のリストで構成できます。各エントリは別々の行に入力する必要があります。

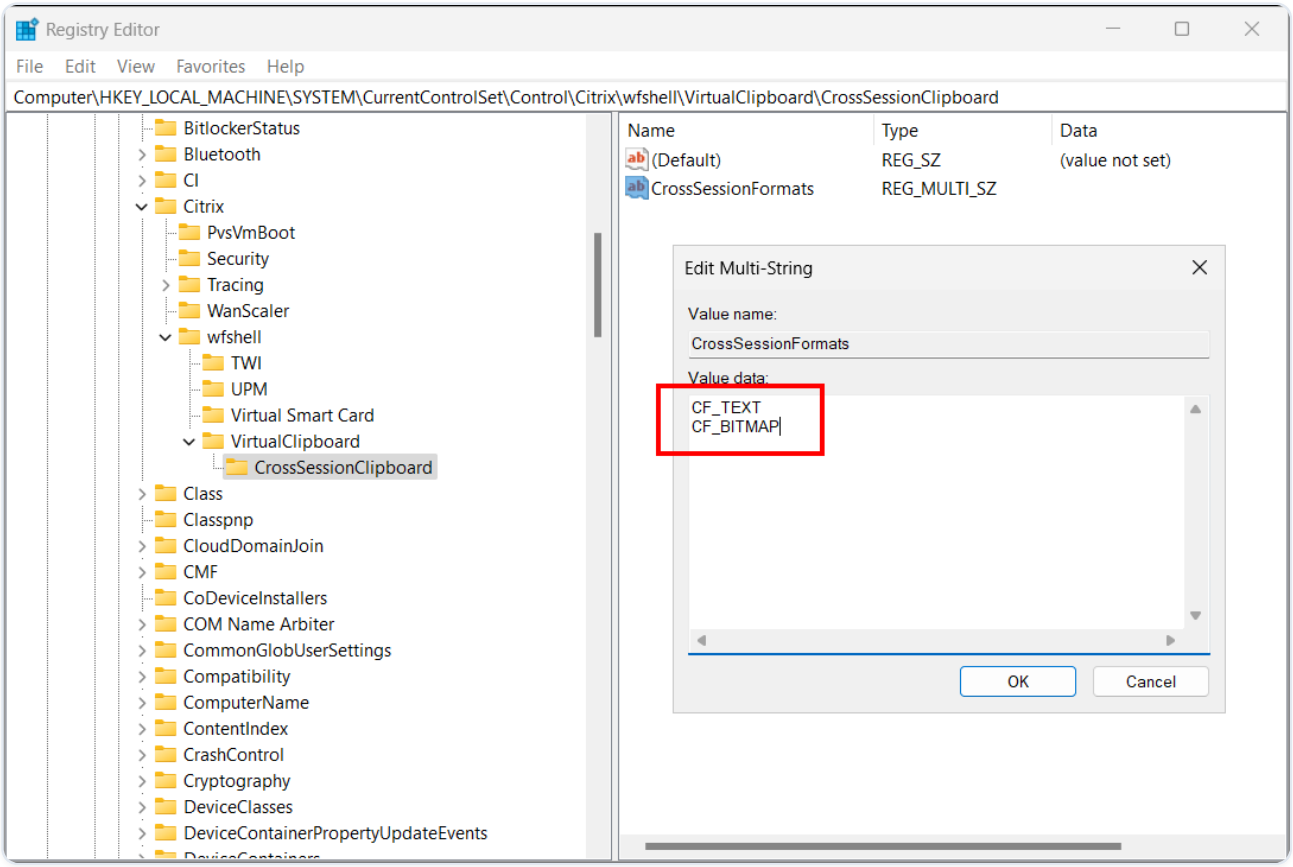
例として:

CF_TEXT

CF_BITMAP

は正しいです。ただし、以下は正しくありません: CF_TEXT,CF_BITMAP

次の例では、CF_TEXTおよびCF_BITMAPクリップボード項目は、これらのデータ形式をあるセッションから別のセッションにコピーするときに、クロスセッションを介してトンネルされて送信されます。



クロスセッションクリップボードが機能するためには、ユーザーがクリップボードデータを共有したいすべてのVDA上で、クロスセッションを目的のクリップボードデータ形式で構成する必要があります。

構成されたクロスセッションクリップボード形式は、クロスセッションをサポートしていないクライアント (CWA for Windows 2507より前のCWAクライアント) からブロックされます。

送信側と受信側の両方のCitrix®セッションで、クロスセッション用に一致するクリップボードデータ形式が設定されている必要があります。

セッション間でコピーされるクリップボードコンテンツは、セッション間でコピーする必要があるクリップボードデータが一致する場合にのみ許可されます。受信側のVDAでクリップボード形式がクロスセッション用に構成されていない場合、クリップボード転送は拒否され、ユーザーは受信側のCitrixセッションにデータを貼り付けることができません。

> **注：**

両方のVDAで、構成されているすべてのクロスセッションクリップボード形式が一致している必要はありませんが、両方のCrossSessionFormats構成に表示される形式のみがセッション間で共有されます。

例えば、

注：

- クロスセッション構成は、セッション間のみを対象としています。構成されている場合、設定された構成に基づいて、セッションからクライアントへの動作が変更される可能性があります。クロスセッションクリップボードは、クライアントからセッションへのクリップボードを変更しません。クライアントからセッションへの構成は、クライアントからセッションに関連するクリップボードポリシーのみを通じて行われます。
- ユーザーがクロスセッションクリップボード用に構成されたCitrixセッションに接続しているが、そのクライアントがクロスセッションをサポートしていない場合（例：2507より前のCitrix Workspaceアプリバージョンを使用している場合、またはCWA LinuxのようなサポートされていないCWAから接続している場合）、クロスセッション構成にリストされている形式のクリップボード転送は、Citrixセッションからクライアントへの転送が拒否されます。

ポリシーとレジストリの優先順位

セッション間クリップボード交換レジストリ構成は、クリップボードポリシーと連携して機能します。

クリップボードリダイレクトが「クライアントクリップボードリダイレクト」ポリシーを禁止に設定することでポリシーによって明示的に禁止されている場合、セッション間クリップボードレジストリ構成は無視され、レジストリがどのように構成されていてもCitrix®セッション間のクリップボード転送も禁止されます。

クリップボードデータ形式が「xxx」ポリシー設定によって明示的に禁止されているが、そのクリップボードデータ形式がセッション間で有効になっている場合、クリップボード形式は禁止されます。セッション間レジストリの構成は無視されます。

セッション間のセッション間クリップボード交換を通じて共有されるクリップボードデータに対しても、クリップボードのサイズ制限が適用されます。
例

例1
すべてデフォルト

ただし：

- CF_TEXT、CF_UNICODETEXT、CF_DSPTEXT、CF_OEMTEXT、CF_LOCALEについて、両方のVDAでセッション間が構成されている

セッション間クリップボード交換レジストリ構成で構成されているデータ形式は、セッション間を通じてトンネルされ、クライアントでは利用できなくなります。この場合、テキスト形式はソースVDAから受信VDAへ共有が許可されます。ポリシーで許可されている他のすべての形式は、引き続きクライアントおよびリモートセッションで許可されます。リモートセッションからコピーされた場合、クライアントクリップボードではテキスト形式のみが禁止されます。

クライアントからセッションへのクリップボードデータ転送は制限されません。
例2
すべてデフォルト

ただし：

- Restrict session clipboard write: 両方のVDAで有効に設定済み
- CF_TEXTに対して両方のVDAでセッション間が設定済み

両方のVDAで「セッションクリップボード書き込みの制限」が有効になっているため、クリップボードデータはセッション間で共有されません。この設定は、セッション間の構成よりも優先されます。

クライアントからセッションへのクリップボードデータの転送も、その同じポリシーによって禁止されます。

CF_TEXTがクロスセッション用に構成されているため、クロスセッション構成によりブロックされるため、CF_TEXTはVDAからクライアントへコピーできないことも意味します。

その他のすべてのクリップボード形式は、セッションからクライアントへ利用可能になります。
例3
すべてデフォルト

例外:

- セッションクリップボード書き込み許可形式は、両方のVDAでCF_TEXTに制限されています
- クロスセッションは、両方のVDAですべてのクリップボードデータ形式に対して構成されています

セッションクリップボード書き込み許可形式は、クロスセッションクリップボード構成よりも優先され、CF_TEXTデータのみがクリップボードを介して受信VDAへコピーを許可されます。

クロスセッションにリストされているすべてのクリップボード形式は、クライアントクリップボードへのコピーが防止されます。
例 4
すべてデフォルト

ただし:

- セッションクリップボード書き込み許可形式がCF_TEXTを除くすべてに設定されている
- セッション間が両方のVDAでCF_TEXT用に構成されている

セッションクリップボード書き込み許可形式は、クロスセッションクリップボード構成よりも優先され、CF_TEXTデータはVDA間でクリップボードを介して共有が許可されません。

クリップボードのシナリオとユースケースの例

クリップボードリダイレクトポリシーを適切に構成することは、ユーザーの生産性と企業セキュリティのバランスを取る上で重要です。最適な構成は、特定のユースケースによって異なります。

一般的なユースケースの例を次に示します。

標準的なナレッジワーカー

ナレッジワーカーや一般的なオフィスユーザーのようなほとんどのユーザーにとって、目標はローカルアプリケーションとリモートアプリケーション間でテキストやシンプルな画像をシームレスにコピー＆ペーストすることです。このシナリオでは、デフォルトのポリシー構成で十分な場合がよくあります。

構成：

- クライアントクリップボードリダイレクト: **許可** (デフォルト)

機密データのユースケース

ユーザーがセキュアなセッションに情報（例：患者データをEHRに）を貼り付ける必要があるが、機密データをローカルデバイスにコピーすることを防ぐ必要がある医療機関や金融機関を考えてみましょう。これは、クリップボードを介した偶発的なデータ流出を防ぐのに役立ちます。

構成：

- クライアントクリップボードリダイレクト: **許可**
- クライアントクリップボード書き込みの制限: **有効** (セッションからクライアントへのコピーをブロック)

- セキュリティを強化するには、「セッションクリップボード書き込みの制限」を有効にし、「セッションクリップボード書き込み許可形式」を使用してプレーンテキスト (CF_TEXT) のみを許可します。

あるいは、お客様は新しいクロスセッションクリップボード機能 (プレビュー) を使用して、セッション間のクリップボードを許可しつつ、セッションからクライアントへのリダイレクトを防ぐことができます。
開発者とIT管理者
これらのユーザーは、スクリプト、ログファイル、インストーラーなどのファイルを、ローカルマシンとVDAの間でコピーする機能を必要とすることがよくあります。これには、より許容的な構成が必要です。

構成:

- クライアントクリップボードリダイレクト: **許可**
- セッションからクライアントへのファイルコピーを有効にするには、クライアントクリップボード書き込みの制限が**無効**になっていることを確認します。または、有効になっている場合は、CFX_FILE形式をクライアントクリップボード書き込み許可形式リストに追加します。
- クライアントからセッションへのファイルコピーを有効にするには、セッションクリップボード書き込みの制限が**無効**になっていることを確認します。または、有効になっている場合は、CFX_FILEをセッションクリップボード書き込み許可形式リストに追加します。

これらのポリシーを構成して、ポリシーに個別にユーザーを追加するのではなく、開発者またはIT管理者が含まれる関連グループをターゲットにします。

グラフィックポリシー設定

「**グラフィック**」セクションには、ユーザーセッションで画像がどのように処理されるかを制御するためのポリシー設定が含まれています。

視覚的にロスレスな圧縮を許可する

この設定により、グラフィックに対して、真のロスレス圧縮の代わりに視覚的にロスレスな圧縮を使用できます。視覚的にロスレスな圧縮は、真のロスレス圧縮よりもパフォーマンスが向上しますが、目視では気づかない程度のわずかな損失があります。この設定は、視覚品質設定の値の使用方法を変更します。

デフォルトでは、この設定は無効になっています。

グラフィックステータスインジケーター

この設定は、グラフィックステータスインジケーターがユーザーセッションで実行されるように構成します。このツールを使用すると、ユーザーはアクティブなグラフィックモードに関する情報を確認できます。

この情報には、ビデオコーデック、ハードウェアエンコード、画質、およびセッションで使用されているモニターに関する詳細が含まれます。グラフィックステータスインジケーターを使用すると、ユーザーはピクセルパーフェクトモードを有効または無効にすることもできます。

Citrix Virtual Apps and Desktops™ 2103以降のリリースには、画質とインタラクティブ性の適切なバランスをユーザーが見つけるのに役立つ画質スライダーが含まれています。

Citrix Virtual Apps™ and Desktops 2109以降のリリースには、グラフィックステータスインジケーターを使用して起動されるユーザーインターフェイスを介して仮想ディスプレイレイアウトを構成する機能が搭載されています。

グラフィックステータスインジケーターは、以前のバージョンのロスレスインジケーターツールに代わるものです。このポリシーは、Citrix Virtual Apps and Desktopsバージョン7.16から1809までのロスレスインジケーターを有効にします。

> **注:**
>
> **グラフィックステータスインジケーター**は、デスクトップセッションでのみ利用可能であり、シームレスアプリケーションセッションでは利用できません。

画面共有

この設定により、ユーザーは画面コンテンツ、キーボード、マウスを含むセッションを他のユーザーと共有できます。

デフォルトでは、この設定は無効になっています。

VDA は、TCP ポート範囲のポートを使用してデータを交換しようとします。最も低いポートから開始し、後続の接続ごとにインクリメントします。このポートは、インバウンドトラフィックとアウトバウンドトラフィックの両方を処理します。

既定では、TCP ポート範囲は 52525～52625 に設定されています。

画面共有に使用されるポートは、ファイアウォールの例外リストに追加する必要があります。このオプションは、VDA のインストール時にチェックボックスとして表示されます。既定では、このオプションはチェックされていません。

表示メモリ制限

この設定は、セッションの最大ビデオバッファサイズをキロバイト単位で指定します。

VDA バージョン 2308 以前の場合、128 から 4,194,303 までのキロバイト単位の量を指定します。指定しない場合、設定は既定で 65,536 キロバイトになります。

VDA バージョン 2311 以降の場合、任意のキロバイト単位の量を指定します。指定しない場合、または 0 を指定した場合、設定は既定で最大値なしになります。

> **注:**
>
> VDA バージョン 2311 以降の場合、Citrix® はこの設定を既定のままにすることをお勧めします。

> 接続に高解像度と複数のモニターを使用すると、より多くのメモリが必要になります。HDX™ は各セッションに必要な表示メモリの量のみを割り当てるため、常に環境内の構成の上位層に基づいて必要なビデオメモリの量を計算してください。したがって、一部のユーザーのみが既定値よりも多く必要とする場合でも、表示メモリ制限を増やしてもスケーラビリティに悪影響はありません。

必要なビデオメモリの量は、次の式を使用して計算されます。

合計ビデオメモリ = ((32 / 8) x Σ)

例 1

次の例では、2 台のモニターを使用するセッションを使用します。1 台は 1920x1080 の解像度、もう 1 台は 1280x720 の解像度です。

1. 解像度の積の合計を計算します。
   - (1080 x 1920) + (720 x 1280)
   - = 2073600 + 921600
   - = 2995200
2. 合計ビデオメモリを計算:
   - ((32 / 8) x 2995200)
   - = (4 x 2995200)
   - = 11,980,800 バイトまたは 11,700 キロバイト

この例では、これら2つのモニター構成を持つセッションをサポートするために、11,700キロバイトのビデオメモリが必要になります。

例2

4Kモニターを4台使用する場合、上記の式を使用すると、これらのセッションには最低129,600キロバイトのビデオメモリが必要になります。

どちらの例でも、VDAバージョン2311以降を使用する場合は、Citrixはディスプレイメモリ制限をデフォルトのままにすることを推奨します。

表示モードの劣化優先順位

> **注：**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> セッションの表示メモリ制限に達した場合、この設定は、色深度と解像度のどちらが先に劣化するかを指定します。

デフォルトでは、カラー深度が最初に低下します。

セッションメモリの制限に達すると、表示される画像の品質を低下させることができます。この品質は、カラー深度と解像度のどちらを最初に低下させるかを選択することで低下させることができます。カラー深度が最初に低下すると、表示される画像はより少ない色を使用します。解像度が最初に低下すると、表示される画像は1インチあたりのピクセル数が少なくなります。

色深度または解像度が劣化した場合にユーザーに通知するには、「表示モードが劣化した場合にユーザーに通知」設定を構成します。

動的ウィンドウプレビュー

この設定は、シームレスウィンドウの表示を有効または無効にします。

- フリップ-
- フリップ 3D
- タスクバープレビュー
- Windows ピーク

WINDOWS AERO プレビューオプション	説明
タスクバープレビュー	ユーザーがウィンドウのタスクバーアイコンにカーソルを合わせると、そのウィンドウの画像がタスクバーの上に表示されます。
Windows ピーク	ユーザーがタスクバーのプレビュー画像にカーソルを合わせると、ウィンドウのフルサイズの画像が画面に表示されます。
フリップ	ユーザーがALT+TABを押すと、開いている各ウィンドウの小さなプレビューアイコンが表示されます。
フリップ3D	ユーザーがTAB+Windowsロゴキーを押すと、開いているウィンドウの大きな画像が画面全体にカスケード表示されます。

デフォルトでは、この設定は有効になっています。

イメージキャッシュ

> **注:**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードのポリシー設定が有効になっている場合にのみ適用されます。

この設定は、セッション内の画像のセクションのキャッシュと取得を有効または無効にします。画像をセクションにキャッシュし、必要に応じてこれらのセクションを取得すると、次のことが可能になります。

- ユーザーデバイスでのスクロールがよりスムーズになる
- ユーザーデバイスでのネットワーク経由で送信されるデータ量を削減する
- ユーザーデバイスで必要となる処理を削減する

デフォルトでは、画像キャッシュ設定は有効になっています。

> **注:**

画像キャッシュ設定は、画像がどのようにキャッシュされ、取得されるかを制御します。この設定は、画像がキャッシュされるかどうかを制御するものではありません。画像は、レガシーグラフィックモード設定が有効になっている場合にキャッシュされます。

レガシーグラフィックモード - サポートされていません。後方互換性のためのみ

重要:

このリリースでは、レガシーグラフィックモードとデスクトップコンポジションリダイレクト (DCR) はサポートされていません。このポリシーは、XenApp 7.15 LTSR、XenDesktop 7.15 LTSR、およびWindows 7とWindows 2008 R2を使用する以前のVDAリリースとの後方互換性のためのみに含まれています。

この設定は、リッチグラフィックエクスペリエンスを無効にします。この設定を使用してレガシーグラフィックエクスペリエンスに戻し、WANまたはモバイル接続での帯域幅消費を削減します。XenAppおよびXenDesktop 7.13で導入された帯域幅削減により、このモードは廃止されました。

デフォルトでは、この設定は無効になっており、ユーザーにはリッチグラフィックエクスペリエンスが提供されます。

レガシーグラフィックモードは以下でサポートされています。

- Windows 7 システム
- ウィンドウズサーバー 2008 R2 VDA 環境。

レガシーグラフィックモードは以下ではサポートされていません。

- Windows 8.xおよび10
- Windows Server 2012、2012 R2、および2016。

XenAppおよびXenDesktop 7.6 FP3以降でのグラフィックモードとポリシーの最適化について詳しくは、CTX202687を参照してください。

最大許容色深度

注:

> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、セッションに許可される最大色深度を指定します。

デフォルトでは、最大許容色深度は32ビット/ピクセルです。

この設定は、Thinwireドライバーと接続にのみ適用されます。プライマリディスプレイドライバーとしてThinWire以外のドライバーを使用するVDAには適用されません。これらのVDAは、Windows Display Driver Model（WDDM）ドライバーをプライマリディスプレイドライバーとして使用するVDAです。Windows 8などのWDDMドライバーをプライマリディスプレイドライバーとして使用するシングルセッションOS VDAの場合、この設定は無効です。Windows Server 2019などのWDDMドライバーを使用するWindowsマルチセッションOS VDAの場合、この設定によりユーザーがVDAに接続できなくなる可能性があります。

高い色深度を設定すると、より多くのメモリが必要になります。メモリ制限に達したときに色深度を低下させるには、**表示モードの低下設定**を構成します。色深度が低下すると、表示される画像はより少ない色を使用します。

表示モードが低下したときにユーザーに通知する

> **注:**

> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、色深度または解像度が低下したときに、ユーザーに簡単な説明を表示します。

デフォルトでは、ユーザーへの通知は無効になっています。

3Dグラフィックワークロード向けに最適化

この設定は、グラフィックを多用するワークロードに最適なデフォルト設定を構成します。グラフィックを多用するアプリケーションに重点を置くユーザーに対して、この設定を有効にします。このポリシーは、セッションでGPUが利用可能な場合にのみ適用してください。このポリシーによって設定されたデフォルト設定を明示的に上書きするその他の設定が優先されます。

デフォルトでは、3Dグラフィックワークロード向け最適化は無効になっています。

キューイングとトッシング

> **注:**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、別の画像に置き換えられたキュー内の画像を破棄します。

デフォルトでは、キューイングとトッシングは有効になっています。

この設定は、グラフィックがユーザーデバイスに送信される際の応答を改善します。この設定を構成すると、フレームがドロップされるため、アニメーションが途切れることがあります。

圧縮にビデオコーデックを使用する

エンドポイントでビデオデコードが利用可能な場合、グラフィックの圧縮にビデオコーデックの使用を許可します。**画面全体**が選択されている場合、ビデオコーデックはすべてのデフォルトコーデックとして適用されます。**アクティブに変更される領域**が選択されている場合、ビデオコーデックは画面上で常に変化する領域に使用され、その他のデータは静止画圧縮とビットマップキャッシュを使用します。エンドポイントでビデオデコードが利用できない場合、または**ビデオコーデックを使用しない**を指定した場合、静止画圧縮とビットマップキャッシュの組み合わせが使用されます。**推奨時に使用**が選択されている場合、システムはさまざまな要因に基づいて選択します。選択方法が強化されるにつれて、結果はバージョン間で異なる場合があります。

現在のシナリオに適切な設定をシステムが最大限に選択できるようにするには、**推奨時に使用**を選択します。

ユーザーエクスペリエンスと帯域幅の向上、特にサーバーレンダリングされたビデオや3Dグラフィックを多用する場合に最適化するには、**画面全体**を選択します。

ビデオパフォーマンスの向上、特に低帯域幅での最適化、および静的コンテンツやゆっくりと変化するコンテンツのスケーラビリティを維持するには、**アクティブに変更される領域**を選択します。この設定は、マルチモニター展開でサポートされています。

サーバーのCPU負荷を最適化し、多数のサーバーレンダリングされたビデオやその他のグラフィックを多用するアプリケーションがない場合に最適化するには、**ビデオコーデックを使用しない**を選択します。

デフォルトは「**推奨時に使用**」です。

ビデオにハードウェアエンコーディングを使用する

この設定により、利用可能な場合、グラフィックハードウェアを使用して画面要素をビデオコーデックで圧縮できます。そのようなハードウェアが利用できない場合、VDAはソフトウェアビデオコーデックを使用したCPUベースのエンコーディングにフォールバックします。

このポリシー設定のデフォルトオプションは「**有効**」です。

複数のモニターがサポートされています。

ビデオデコードをサポートするCitrix Workspace™アプリは、ハードウェアエンコードで使用できます。

NVIDIA

NVIDIA GRID GPUの場合、ハードウェアエンコードはマルチセッションOSおよびシングルセッションOS用のVDAでサポートされています。

NVIDIA GPUはNVENCハードウェアエンコードをサポートしている必要があります。サポートされているGPUのリストについては、NVIDIAビデオコーデックSDKを参照してください。

NVIDIA GRIDにはドライバーバージョン3.1以降が必要です。NVIDIA Quadroにはドライバーバージョン362.56以降が必要です。CitrixはNVIDIA Release R361ブランチのドライバーを推奨しています。

ロスレステキストはNVENCハードウェアエンコードと互換性がありません。ロスレステキストを有効にした場合、ロスレステキストがNVENCハードウェアエンコードよりも優先されます。

アクティブに変化する領域に対するH.264ハードウェアコーデックの選択的な使用がサポートされています。

視覚的にロスレス（YUV 4:4:4）圧縮がサポートされています。視覚的にロスレス（グラフィックポリシー設定、視覚的にロスレスな圧縮を許可）には、Citrix Workspaceアプリ1808以降またはCitrix Receiver for Windows 4.5以降が必要です。

インテル

Intel Iris Proグラフィックプロセッサの場合、ハードウェアエンコードはシングルセッションOSおよびマルチセッションOS用のVDAでサポートされています。

Intel Broadwellプロセッサファミリー以降のIntel Iris Proグラフィックプロセッサがサポートされています。Intel Remote Displays SDKバージョン1.0が必要で、IntelのWebサイトからダウンロードできます: Remote Displays SDK。

ロスレステキストは、ビデオコーデックポリシーが画面全体に設定されており、**3Dグラフィックワークロード用に最適化**ポリシーが無効になっている場合にのみサポートされます。

視覚的にロスレス（YUV 4:4:4）はサポートされていません。

Intelエンコーダーは、最大8つのエンコードセッション（たとえば、1人のユーザーが8台のモニターを使用する場合、または8人のユーザーがそれぞれ1台のモニターを使用する場合）で良好なユーザーエクスペリエンスを提供します。8つ以上のエンコードセッションが必要な場合は、仮想マシンが接続するモニターの数を確認してください。管理者は、良好なユーザーエクスペリエンスを維持するために、このポリシー設定をユーザーごとまたはマシンごとに構成するかどうかを決定します。

AMD

AMDの場合、シングルセッションOS用VDAでハードウェアエンコードがサポートされています。

AMD GPUはRapidFire SDKをサポートしている必要があります。たとえば、AMD Radeon ProまたはFirePro GPUなどです。

エンコードを機能させるには、最新のAMDドライバーをインストールしてください。これらのドライバーは`<https://www.amd.com/en/support>`からダウンロードできます。

ロスレステキストはAMDハードウェアエンコードと互換性がありません。ロスレステキストを有効にした場合、ロスレステキストがAMDハードウェアエンコードよりも優先されます。

活発に変化する領域向けのH.264ハードウェアコーデックの選択的な使用がサポートされています。

キャッシュポリシー設定

このセクションには、クライアント接続の帯域幅が制限されている場合に、ユーザーデバイスで画像データをキャッシュすることを可能にするポリシー設定が含まれています。

永続キャッシュしきい値

注: Virtual Delivery Agent 7.xの場合、このポリシー設定は、**レガシーグラフィックモード**ポリシー設定が有効になっている場合にのみ適用されます。

この設定は、ユーザーデバイスのハードドライブにビットマップをキャッシュし、それにより、以前のセッションからの大きく頻繁に使用される画像の再利用を可能にします。

デフォルトでは、しきい値は1秒あたり3000000ビットです。

しきい値は、永続キャッシュ機能が有効になる下限を表します。たとえば、デフォルト値を使用すると、帯域幅が3000000 bpsを下回った場合、ビットマップはユーザーデバイスのハードドライブにキャッシュされます。

キープアライブ ポリシー設定

Keep Alive セクションには、ICA® キープアライブメッセージを管理するためのポリシー設定が含まれています。

ICA キープアライブ タイムアウト

この設定は、連続するICAキープアライブメッセージ間の秒数を指定します。

デフォルトでは、キープアライブメッセージ間の間隔は60秒です。

ICAキープアライブメッセージを送信する1～3600秒の間隔を指定します。ネットワーク監視ソフトウェアが非アクティブな接続を閉じる役割を担っている場合は、この設定を構成しないでください。

ICA キープアライブメッセージ

この設定は、ICAキープアライブメッセージの定期的な送信を有効または無効にします。

デフォルトでは、キープアライブメッセージは送信されません。

この設定を有効にすると、切断された接続が切断されるのを防ぎます。サーバーがアクティビティを検出しない場合、この設定により、Remote Desktop Services (RDS) がセッションを切断するのを防ぎます。サーバーは数秒ごとにキープアライブメッセージを送信し、セッションがアクティブであるかどうかを検出します。セッションがアクティブでなくなった場合、サーバーはそのセッションを切断済みとしてマークします。

セッションの信頼性を使用している場合、ICAキープアライブは機能しません。セッションの信頼性を使用していない接続に対してのみ、ICAキープアライブを構成してください。

関連するポリシー設定: セッションの信頼性接続。

モバイルエクスペリエンスポリシー設定

「**モバイルエクスペリエンス**」セクションには、Citrix Mobility Packを処理するためのポリシー設定が含まれています。

キーボードの自動表示

この設定は、モバイルデバイスの画面でのキーボードの自動表示を有効または無効にします。

デフォルトでは、キーボードの自動表示は無効になっています。

タッチ最適化デスクトップの起動

この設定は無効になっており、Windows 10またはWindows Server 2016マシンでは使用できません。

この設定は、Citrix Workspace™アプリの全体的なインターフェイス動作を決定します。この設定により、タブレットデバイス向けに最適化されたタッチフレンドリーなインターフェイスを許可または禁止できます。

デフォルトでは、タッチフレンドリーなインターフェイスが使用されます。

Windowsインターフェイスのみを使用するには、このポリシー設定を「禁止」に設定します。

コンボボックスのリモート化

この設定は、モバイルデバイスのセッションで表示できるコンボボックスの種類を決定します。このポリシー設定を「許可」に設定すると、デバイスネイティブのコンボボックスコントロールが表示されます。この設定が許可されている場合、ユーザーはCitrix Workspaceアプリfor iOSのセッション設定を変更してWindowsコンボボックスを使用できます。

デフォルトでは、「**コンボボックスのリモート化**」機能は禁止されています。

マルチメディアポリシー設定

マルチメディアセクションには、ユーザーセッションにおけるストリーミングHTML5およびWindowsオーディオとビデオを管理するためのポリシー設定が含まれています。

> **警告**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になる可能性のある重大な問題を引き起こすことがあります。Citrix®は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。レジストリエディターの使用は自己責任で行ってください。編集する前に必ずレジストリをバックアップしてください。

マルチメディアポリシー

デフォルトでは、Delivery Controller™で設定されたすべてのマルチメディアポリシーは、これらのレジストリに保存されます。

マシンポリシー:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies

ユーザーポリシー:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix{ユーザーセッションID}\User\MultimediaPolicies

現在のユーザーセッションIDを見つけるには、Windowsコマンドラインで**qwinsta**コマンドを発行します。

HTML5ビデオリダイレクト

Citrix Virtual Apps and Desktops™サーバーがHTML5マルチメディアWebコンテンツをユーザーに配信する方法を制御し、最適化します。

デフォルトでは、この設定は無効になっています。

HTML5リダイレクトグラフィックイメージ(/en-us/citrix-virtual-apps-desktops/2511/media/redirection1a.png)

このリリースでは、この機能は制御されたWebページでのみ利用可能です。HTML5マルチメディアコンテンツが利用可能なWebページ（例：社内トレーニングサイトのビデオ）にJavaScriptを追加する必要があります。

HTML5ビデオリダイレクトを構成するには:

1. ファイル **HdxVideo.js** を、VDAインストール先の %Program Files%/Citrix/ICA Service/HTML5 Video Redirection から、社内Webページの場所にコピーします。
2. この行をWebページに挿入します（Webページに他のスクリプトがある場合は、それらのスクリプトの前に **HdxVideo.js** を含めます）。 `<script src="HdxVideo.js" type="text/javascript"\></script>`

注： HdxVideo.js がWebページと同じ場所にない場合は、**src** 属性を使用してその完全なパスを指定します。

JavaScriptが制御されたWebページに追加されておらず、ユーザーがHTML5ビデオを再生する場合を考えてみましょう。この場合、Citrix Virtual Apps™ and Desktops はデフォルトでサーバー側レンダリングに設定されます。

HTML5ビデオのリダイレクトを機能させるには、***Windows Media Redirection***を許可します。このポリシーは、Server Fetch Client Render に必須であり、Client Side Fetching に必要です。Client Side Fetching は、*Windows Media client-side content fetching* も許可されている必要があります。

Microsoft Edgeはこの機能をサポートしていません。

HdxVideo.js は、ブラウザのHTML5プレーヤーコントロールを独自のコントロールに置き換えます。特定のWebサイトでHTML5ビデオリダイレクトポリシーが有効になっていることを確認するには、プレーヤーコントロールを、**HTML5ビデオリダイレクト**ポリシーが禁止されているシナリオと比較します。

（ポリシーが許可されている場合のCitrixカスタムコントロール）



（ポリシーが禁止されているか、構成されていない場合のネイティブWebページコントロール）



以下のビデオコントロールがサポートされています。

- 再生
- 一時停止
- シーク
- 繰り返し
- オーディオ
- 全画面表示

HTML5ビデオリダイレクトテストページを表示できます。

TLS、HTML5ビデオリダイレクト、およびブラウザーコンテンツリダイレクト

HTML5ビデオリダイレクトを使用して、次のことができます。

- HTTPS Webサイトからビデオをリダイレクトする
- または
- ブラウザコンテンツリダイレクトでWebサイト全体をリダイレクトする

これらのWebサイトに挿入されたJavaScriptは、VDA上で実行されているCitrix HDX HTML5ビデオリダイレクトサービス (WebSocketService.exe) へのTLS接続を確立する必要があります。VDA上の証明書ストアにあるCitrix HDX HTML5ビデオリダイレクトサービスは、次の目的で2つのカスタム証明書を生成します。

- ビデオリダイレクトを実現する
- WebページのTLSの整合性を維持する

HdxVideo.jsは、VDA上で実行されているWebSocketService.exeと通信するためにSecure WebSocketsを使用します。このプロセスはローカルシステムアカウントとして実行され、SSL終端とユーザーセッションマッピングを行います。

WebSocketService.exe は 127.0.0.1 ポート 9001 でリッスンしています。

ビデオ品質の制限

この設定は、Windows Mediaにのみ適用され、HTML5には適用されません。**WAN経由のWindows Mediaマルチメディアリダイレクトの最適化**を有効にする必要があります。

この設定は、HDX™接続で許可される最大ビデオ品質レベルを指定します。設定すると、最大ビデオ品質は指定された値に制限され、環境内でマルチメディアのサービス品質 (QoS) が維持されます。

デフォルトでは、この設定は構成されていません。

許可される最大ビデオ品質レベルを制限するには、次のいずれかのオプションを選択します。

- 1080p/8.5Mbps
- 720p/4.0Mbps
- 480p/720Kbps
- 380p/400Kbps
- 240p/200Kbps

同じサーバーで複数のビデオを同時に再生すると、大量のリソースが消費され、サーバーのスケーラビリティに影響を与える可能性があります。

Microsoft Teamsのリダイレクト

この設定は、HDX テクノロジーに基づいた Microsoft Teams の最適化を有効にします。

このポリシーが有効で、サポートされているバージョンのCitrix Workspace™アプリを使用している場合、このレジストリキーはVDAで**1**に設定されます。Microsoft Teamsアプリケーションは、VDIモードでロードするためにこのキーを読み取ります。 レジストリキーを手動で設定する必要はありません。

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

名前: MSTeamsRedirSupport

値: DWORD (1 - オン, 0 - オフ)

> **注:**
>
> Web Studioでポリシーが利用できない古いバージョンのController（バージョン7.15など）で、バージョン1906.2 VDA以降を使用しているとします。この場合、HDX最適化はVDAでデフォルトで有効になっています。Workspaceアプリのバージョンが1907以降の場合、Microsoft Teamsは最適化モードで起動します。7.15 LTSR ControllerとCR VDAを混在させる場合の注意点については、Knowledge Centerの記事CTX205549を参照してください。

> この場合、特定のユーザーに対してこの機能を無効にするには、レジストリ設定を上書きできます。グループポリシーを使用してユーザーの組織単位にログオンスクリプトを適用することで、レジストリ設定を上書きします。

> デフォルトでは、Microsoft Teamsリダイレクトは有効になっています。

マルチメディア会議

この設定では、ビデオ会議アプリケーションによる最適化されたWebカメラリダイレクトテクノロジーの使用を許可または禁止します。

デフォルトでは、ビデオ会議のサポートは許可されています。

この設定をポリシーに追加する場合は、**Windows Mediaリダイレクト**設定が存在し、**許可**（デフォルト）に設定されていることを確認してください。

マルチメディア会議を使用する場合は、次の条件が満たされていることを確認してください。

- マルチメディア会議に使用するWebカメラのメーカー提供ドライバーがクライアントにインストールされていること。
- ビデオ会議セッションを開始する前に、Webカメラをユーザーデバイスに接続してください。サーバーは一度に1つのインストール済みWebカメラのみを使用します。複数のWebカメラがユーザーデバイスにインストールされている場合、サーバーは各Webカメラを順次使用しようとします。この試行は、ビデオ会議セッションが正常に作成されるまで続行されます。

汎用USBリダイレクトを使用してWebカメラをリダイレクトする場合、このポリシーは必要ありません。その場合は、WebカメラドライバーをVDAにインストールしてください。

WAN経由のWindows Mediaマルチメディアリダイレクトの最適化

この設定はWindows Mediaにのみ適用され、HTML5には適用されません。この設定により、以下が可能になります。

- リアルタイムマルチメディアトランスコーディング
- 劣化したネットワーク経由でのモバイルデバイスへのオーディオおよびビデオメディアストリーミングを許可
- WAN経由でWindows Mediaコンテンツが配信される方法を改善することで、ユーザーエクスペリエンスを向上させます。

デフォルトでは、WAN経由でのWindows Mediaコンテンツの配信は最適化されています。

この設定をポリシーに追加する際は、**Windows Media Redirection**設定が存在し、**Allowed**に設定されていることを確認してください。

この設定が有効になっている場合、メディアストリーミングを可能にするために、必要に応じてリアルタイムのマルチメディアトランスコーディングが自動的に展開されます。また、極端なネットワーク条件下でもシームレスなユーザーエクスペリエンスを提供します。

WAN経由でのWindows Mediaマルチメディアリダイレクトの最適化にGPUを使用する

この設定はWindows Mediaにのみ適用され、リアルタイムのマルチメディアトランスコーディングをVirtual Delivery Agent (VDA) のグラフィックス処理ユニット (GPU) で実行できるようにします。これにより、サーバーのスケーラビリティが向上します。GPUトランスコーディングは、VDAがハードウェアアクセラレーションをサポートするGPUを搭載している場合にのみ利用可能です。そうでない場合、トランスコーディングはCPUにフォールバックします。

注: GPUトランスコーディングはNVIDIA GPUでのみサポートされています。

デフォルトでは、WAN経由でのWindows Mediaコンテンツの配信を最適化するためにVDA上のGPUを使用することは禁止されています。

この設定をポリシーに追加する際は、以下の設定が存在し、Allowedに設定されていることを確認してください。

- **Windows Mediaリダイレクト**
- **WAN経由でのWindows Mediaマルチメディアリダイレクト設定の最適化**

Windows Mediaフォールバック防止

この設定は、ブラウザコンテンツリダイレクト、HTML5、およびWindows Mediaに適用されます。HTML5をサポートするには、**HTML5 video redirection**ポリシーを**Allowed**に設定します。

管理者は、**Windows Media fallback prevention**ポリシー設定を使用して、ストリーミングコンテンツをユーザーに配信するために試行される方法を指定できます。

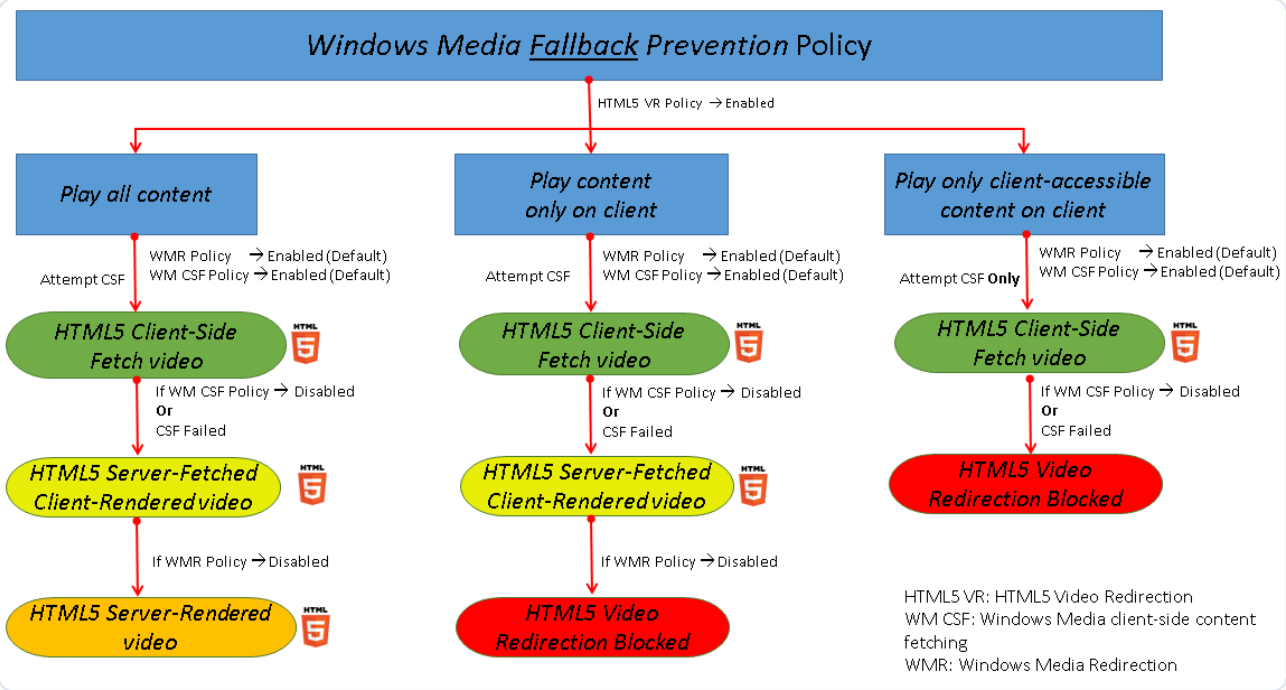
デフォルトでは、この設定は構成されていません。設定が「構成されていません」に設定されている場合、動作は**すべてのコンテンツを再生**と同じになります。

この設定を構成するには、次のいずれかのオプションを選択します。

- **すべてのコンテンツを再生**。クライアント側でのコンテンツ取得を試行し、その後Windows Mediaリダイレクトを試行します。失敗した場合は、サーバーでコンテンツを再生します。
- **すべてのコンテンツをクライアントでのみ再生**。クライアント側での取得を試行し、その後Windows Mediaリダイレクトを試行します。失敗した場合、コンテンツは再生されません。
- **クライアントでクライアントアクセス可能なコンテンツのみを再生**。クライアント側での取得のみを試行します。失敗した場合、コンテンツは再生されません。

コンテンツが再生されない場合、プレーヤーウィンドウに次のエラーメッセージが表示されます（デフォルトの表示時間は5秒）。

「リソース不足のため、会社がビデオをブロックしました」



このエラーメッセージの表示時間は、VDA上の次のレジストリキーでカスタマイズできます。レジストリエントリが存在しない場合、表示時間はデフォルトで5秒になります。

レジストリパスは、VDAのアーキテクチャによって異なります。

`\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream`

または

\HKLM\SOFTWARE\Citrix\HdxMediastream

レジストリキー：

名前: VideoLoadManagementErrDuration

種類: DWORD

範囲: 1 - DWORD制限まで（デフォルト = 5）

単位: 秒

Windows Mediaクライアント側コンテンツ取得

この設定はHTML5とWindows Mediaの両方に適用されます。この設定により、ユーザーデバイスは、XenAppまたはXenDesktop®ホストサーバーを介さずに、インターネットまたはイントラネット上のソースプロバイダーからマルチメディアファイルを直接ストリーミングできるようになります。

デフォルトでは、この設定は**許可**されています。この設定を許可すると、ネットワーク使用量とサーバーのスケーラビリティが向上します。この改善は、メディアに関する処理をホストサーバーからユーザーデバイスに移動することで実現されます。また、Microsoft DirectShowやMedia Foundationなどの高度なマルチメディアフレームワークがユーザーデバイスにインストールされている必要もなくなります。ユーザーデバイスには、URLからファイルを再生する機能のみが必要です。

この設定をポリシーに追加するときは、**Windows Mediaリダイレクト**設定が存在し、**許可**に設定されていることを確認してください。**Windows Mediaリダイレクト**が無効になっている場合、ソースプロバイダーからユーザーデバイスへのマルチメディアファイルの直接ストリーミングも無効になります。

Windows Mediaリダイレクト

この設定はHTML5とWindows Mediaの両方に適用され、サーバーがストリーミングオーディオとビデオをユーザーに配信する方法を制御および最適化します。

デフォルトでは、この設定は**許可**されています。HTML5の場合、ポリシー**HTML5ビデオリダイレクト**が**禁止**されていると、この設定は有効になりません。

この設定が有効になっている場合、サーバーからレンダリングされるオーディオとビデオの品質は、ユーザーデバイスでローカルに再生されるオーディオとビデオに匹敵するレベルに向上します。サーバーは、元の圧縮形式でマルチメディアをクライアントにストリーミングし、ユーザーデバイスがメディアを解凍してレンダリングできるようにします。

Windows Mediaリダイレクトは、Microsoft DirectShow、DirectX Media Objects (DMO)、およびMedia Foundationの標準に準拠するコーデックでエンコードされたマルチメディアファイルを最適化します。特定のマルチメディアファイルを再生するには、そのマルチメディアファイルのエンコード形式と互換性のあるコーデックがユーザーデバイスに存在する必要があります。

デフォルトでは、Citrix Workspaceアプリでオーディオは無効になっています。ユーザーがICA®セッションでマルチメディアアプリケーションを実行できるようにするには、オーディオをオンにするか、Citrix Workspaceアプリのインターフェイスでオーディオをオンにする権限をユーザーに付与します。

Windows Mediaリダイレクトを使用してメディアを再生したときの表示が、基本的なICA圧縮と通常のオーディオを使用してレンダリングした場合よりも悪い場合にのみ、**禁止**を選択します。この状況はまれですが、低帯域幅の条件下、たとえばキーフレームの頻度が低いメディアの場合に発生する可能性があります。

Windows Mediaリダイレクトのバッファサイズ

この設定はレガシーであり、HTML5には適用されません。

この設定では、マルチメディアアクセラレーションのバッファサイズを1～10秒で指定します。

デフォルトでは、バッファサイズは5秒です。

Windows Mediaリダイレクトのバッファサイズの使用

この設定はレガシーであり、HTML5には適用されません。

この設定は、**Windows Media Redirection buffer size** 設定で指定されたバッファサイズの使用を有効または無効にします。

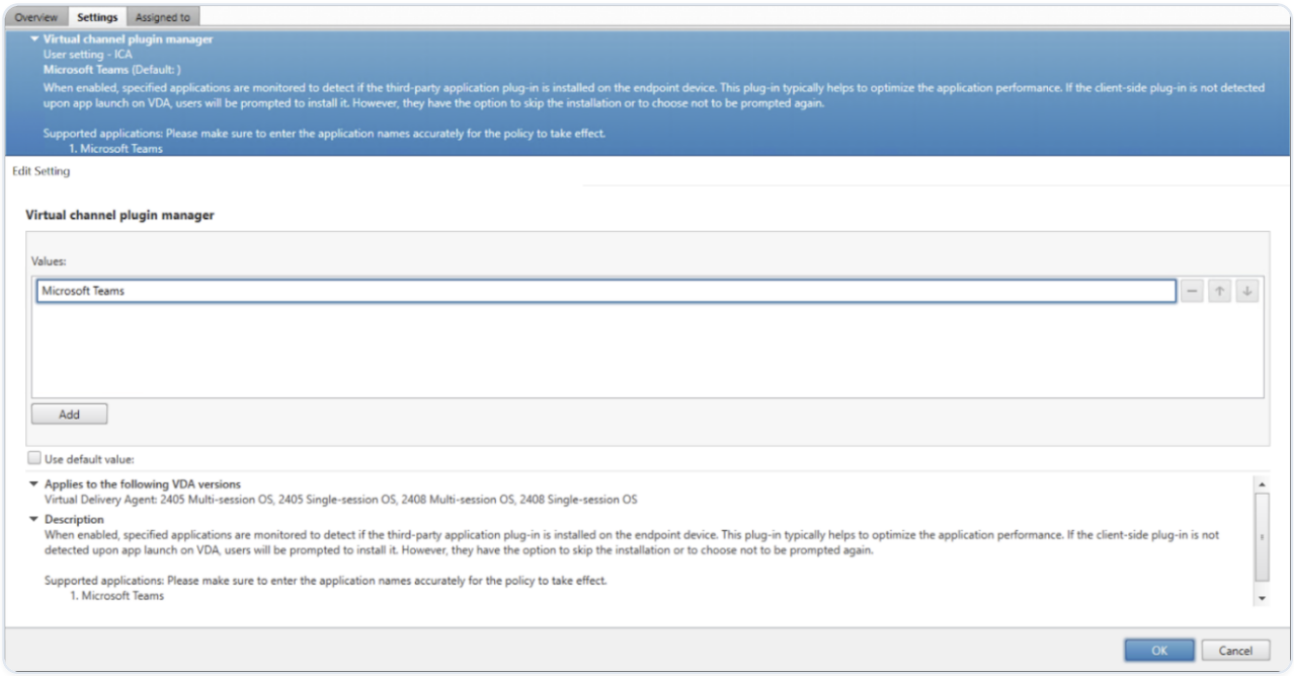
デフォルトでは、指定されたバッファサイズは使用されません。

この設定が無効になっている場合、または**Windows Media Redirection buffer size** 設定が構成されていない場合、サーバーはデフォルトのバッファサイズ値（5秒）を使用します。

仮想チャネルプラグインマネージャーポリシー

仮想チャネルプラグインマネージャーセクションには、この機能を構成するためのポリシー設定が含まれています。

仮想チャネルプラグインマネージャーは、特定の指定されたアプリケーションのクライアントエンドポイント全体にプラグインを展開するように設計されています。プラグインマネージャーは、VDAで実行されている特定のアプリケーションを検出し、アプリケーションの実行時に最高の体験を得るために、エンドポイントにプラグインをインストールするようユーザーに促します。



- 管理者はポリシーを使用して、エンドポイント全体にプラグインをインストールする必要があるアプリケーションを指定できます。
- アプリケーション名は、ポリシーの説明にある「サポートされているアプリケーション」に記載されている名前と同じである必要があります。
- デフォルトでは、ポリシーは無効になっています。
- 現在サポートされているアプリケーション
  - “マイクロソフト チームズ”
- 今後、さらに多くのアプリケーションがサポートされる予定です。

マルチストリーム接続ポリシー設定

マルチストリーム接続セクションには、セッション内の複数のICA®接続のサービス品質の優先順位付けを管理するためのポリシー設定が含まれています。

> **注：**
>
> マルチストリーム接続ポリシーが有効になっている場合、MTU検出はサポートされません。

UDP経由のオーディオ

この設定は、サーバー上でのUDP経由のオーディオを許可または禁止します。

デフォルトでは、サーバー上でのUDP経由のオーディオは許可されています。

有効にすると、この設定はサーバー上でUDPポートを開き、UDP経由のオーディオリアルタイムトランスポートを使用するように構成されたすべての接続をサポートします。

オーディオUDPポート範囲

この設定は、Virtual Delivery Agent (VDA) によって使用されるポート番号の範囲（最小ポート番号、最大ポート番号）を指定します。この指定は、ユーザーデバイスとの間でオーディオパケットデータを交換するのに役立ちます。VDAは、ユーザーデバイスとデータを交換するために各UDPポートペアを使用しようとします。最小値から開始し、その後の試行ごとに2ずつ増やします。各ポートは、インバウンドトラフィックとアウトバウンドトラフィックの両方を処理します。

デフォルトでは、この範囲は16500,16509に設定されています。

マルチポートポリシー

この設定は、ICAトラフィックに使用されるTCPポートを指定し、各ポートのネットワーク優先順位を確立します。

デフォルトでは、プライマリポート (2598) は高優先度です。

ポートを構成するときは、次の優先順位を割り当てることができます。

- **非常に高い:** ウェブカメラ会議などのリアルタイムアクティビティ用
- **高い:** 画面、キーボード、マウスなどのインタラクティブな要素用
- **中:** クライアントドライブマッピングなどのバルクプロセス用
- **低い:** 印刷などのバックグラウンドアクティビティ用

各ポートには一意の優先順位が必要です。たとえば、CGPポート1とCGPポート3の両方に「非常に高」の優先順位を割り当てることはできません。

ポートを優先順位付けから削除するには、ポート番号を0に設定します。プライマリポートを削除したり、その優先順位レベルを変更したりすることはできません。

この設定を構成する際は、サーバーを再起動してください。この設定は、**Multi-Stream computer**設定ポリシー設定が有効になっている場合にのみ適用されます。

マルチストリーム コンピューター設定

この設定は、サーバー上でMulti-Streamを有効または無効にします。

デフォルトでは、Multi-Streamは無効になっています。Citrix SD-WAN™またはサードパーティ製ルーターを使用して目的のQuality of Serviceを実現する場合は、Multi-Stream computerポリシー設定を構成してください。

Multi-Streamが有効になっている場合、Adaptive Transportの機能であるMTU Discoveryはサポートされません。

この設定を構成する際は、変更が適用されるようにサーバーを再起動してください。

> **重要:**
>
> このポリシー設定を、セッション全体の帯域幅制限などの帯域幅制限ポリシー設定と組み合わせて使用すると、予期しない結果が生じる可能性があります。この設定をポリシーに含める場合は、帯域幅制限設定が含まれていないことを確認してください。

マルチストリーム ユーザー設定

この設定は、ユーザーデバイス上でMulti-Streamを有効または無効にします。

デフォルトでは、Multi-Streamはすべてのユーザーに対して無効になっています。Citrix SD-WANまたはサードパーティ製ルーターを使用して目的のQuality of Serviceを実現する場合は、Multi-Stream user設定を構成してください。

この設定は、**Multi-Streamコンピューター**設定ポリシー設定が有効になっているホストでのみ有効になります。

> **重要:**
>
> このポリシー設定を、全体的なセッション帯域幅制限などの帯域幅制限ポリシー設定と併用すると、予期しない結果が生じる可能性があります。この設定をポリシーに含める場合は、帯域幅制限設定を含めないようにしてください。

マルチストリーム仮想チャネル割り当て設定

この設定は、マルチストリームが使用されている場合に仮想チャネルが割り当てられるICAストリームを指定します。

これらの設定を構成しない場合、仮想チャネルはデフォルトのストリームに保持されます。仮想チャネルをICAストリームに割り当てるには、仮想チャネル名の横にある**ストリーム番号**リストから目的のストリーム番号（0、1、2、3）を選択します。

環境でカスタム仮想チャネルが使用されている場合は、**追加**をクリックし、**仮想チャネル**の下のテキストボックスに仮想チャネル名を指定し、その横にある**ストリーム番号**リストから目的のス

トリーム番号を選択します。指定する名前は、フレンドリ名ではなく、実際の仮想チャネル名である必要があります。たとえば、Citrix Browser AccelerationではなくCTXSBRなどです。

これらの設定は、マルチストリームコンピューター設定を有効にした場合にのみ有効になります。

デフォルトでは、仮想チャネルとそのストリーム割り当ては次のとおりです。

- AppFlow®: 2
- オーディオ: 0
- ブラウザコンテンツリダイレクト: 2
- クライアントCOMポートマッピング: 3
- クライアントドライブマッピング: 2
- クライアントプリンターマッピング: 3
- クリップボード: 2
- CTXDND: 1 (**注:** これは、Citrixセッションとローカルエンドポイント間でファイルをドラッグアンドドロップする機能をサポートします。)
- DVCプラグイン (DVCプラグインのフレンドリ名から自動生成された静的VC名、または管理者によって割り当てられたもの): 2
- エンドユーザーエクスペリエンス監視: 1
- ファイル転送 (HTML5 Receiver): 2
- 汎用データ転送: 2
- ICA制御: 1
- 入力メソッドエディター: 1
- レガシー クライアント プリンター マッピング (COM1): 1, 3
- レガシー クライアント プリンター マッピング (COM2): 2, 3
- レガシー クライアント プリンター マッピング (LPT1): 1, 3
- レガシー クライアント プリンター マッピング (LPT2): 2, 3
- ライセンス管理: 1
- Microsoft Teams/WebRTC リダイレクト: 1
- モバイルレシーバー: 1
- MultiTouch: 1
- ポート転送: 2

- リモートオーディオおよびビデオ拡張機能 (RAVE): 2
- シームレス (透過ウィンドウ統合): 1
- センサーと位置情報: 1
- スマートカード: 1
- Thinwire グラフィックス: 1
- 透過UI統合/ログオンステータス: 2
- TWAINリダイレクト: 2
- USB: 2
- ゼロレイテンシーフォントおよびキーボード: 2
- ゼロレイテンシーデータチャネル: 2

仮想チャネルの割り当てと優先順位の詳細については、Knowledge Centerの記事CTX131001を参照してください。

ポートリダイレクトポリシー設定

ポートリダイレクトセクションには、クライアントLPTおよびCOMポートマッピングのポリシー設定が含まれています。

Virtual Delivery Agentのバージョンが**7.0より前**の場合、ポートリダイレクトを構成するには以下のポリシー設定を使用します。VDAバージョン**7.0から7.8**の場合、これらの設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。VDAバージョン**7.9**の場合、以下のポリシー設定を使用します。

クライアントCOMポートの自動接続

この設定は、ユーザーがサイトにログオンしたときに、ユーザーデバイス上のCOMポートの自動接続を有効または無効にします。

デフォルトでは、クライアントCOMポートは自動的に接続されません。

クライアントLPTポートの自動接続

この設定は、ユーザーがサイトにログオンしたときに、ユーザーデバイス上のLPTポートの自動接続を有効または無効にします。

デフォルトでは、クライアントLPTポートは自動的に接続されません。

クライアントCOMポートリダイレクト

この設定は、ユーザーデバイス上のCOMポートへのアクセスを許可または禁止します。

デフォルトでは、COMポートリダイレクトは禁止されています。

関連するポリシー設定は次のとおりです。

- COMポートリダイレクトの帯域幅制限
- COMポートリダイレクトの帯域幅制限（パーセント）

クライアントLPTポートリダイレクト

この設定は、ユーザーデバイス上のLPTポートへのアクセスを許可または禁止します。

デフォルトでは、LPTポートリダイレクトは禁止されています。

LPTポートは、LPTポートに印刷ジョブを送信するレガシーアプリケーションでのみ使用されます。これらのポートは、ユーザーデバイス上の印刷オブジェクトに印刷ジョブを送信するレガシーアプリケーションでは使用されません。現在のほとんどのアプリケーションは、印刷ジョブをプリンターオブジェクトに送信できます。このポリシー設定は、LPTポートに印刷するレガシーアプリケーションをホストするサーバーにのみ必要です。

注：クライアントCOMポートリダイレクトは双方向ですが、LPTポートリダイレクトは出力のみであり、ICAセッション内では\\\client\LPT1および\\\client\LPT2に制限されます。

関連するポリシー設定は次のとおりです。

- LPTポートリダイレクト帯域幅制限
- LPTポートリダイレクト帯域幅制限パーセント

FIDO2 ポリシー設定

この設定は、FIDO2 リダイレクトを有効または無効にします。FIDO2 リダイレクトにより、ユーザーは仮想マシン内のローカルエンドポイントのFIDO2コンポーネントを利用できます。ユーザーは、TPM 2.0とWindows Helloを搭載したデバイスで、FIDO2セキュリティキーまたは統合生体認証を介して仮想セッションを認証できます。

この設定が**許可**されている場合、ユーザーはローカルエンドポイントの機能を使用してFIDO2認証を行うことができます。デフォルトでは、この設定は**許可**されています。

印刷ポリシー設定

印刷セクションには、クライアント印刷を管理するためのポリシー設定が含まれています。

クライアントプリンターリダイレクト

この設定は、ユーザーがセッションにログオンしたときに、クライアントプリンターがサーバーにマップされるかどうかを制御します。

デフォルトでは、クライアントプリンターのマッピングは許可されています。この設定が無効になっている場合、セッション用のPDFプリンターは自動作成されません。

関連するポリシー設定: クライアントプリンターの自動作成

デフォルトプリンター

この設定は、ユーザーデバイス上のデフォルトプリンターがセッションでどのように確立されるかを指定します。

デフォルトでは、ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます。

デフォルトプリンターに現在のRemote Desktop ServicesまたはWindowsユーザープロファイル設定を使用するには、「ユーザーのデフォルトプリンターを調整しない」を選択します。このオプションを選択した場合、デフォルトプリンターはプロファイルに保存されず、他のセッションまたはクライアントのプロパティに応じて変更されません。セッション内のデフォルトプリンターは、セッションで最初に自動作成されたプリンターであり、次のいずれかです。

- **コントロールパネル > デバイス**と**プリンター**でWindowsサーバーにローカルに追加された最初のプリンター。
- サーバーにローカルに追加されたプリンターがない場合、最初に自動作成されたプリンター。

このオプションを使用すると、プロファイル設定を通じてユーザーに最も近いプリンターを提示できます（近接印刷として知られています）。

プリンターの割り当て

この設定は、デフォルトプリンターとセッションプリンターの設定の代替手段を提供します。個別のデフォルトプリンターとセッションプリンターの設定を使用して、サイト、大規模グループ、または組織単位の動作を構成します。**プリンター割り当て**設定を使用して、多数のプリンターを複数のユーザーに割り当てます。

この設定は、リストされたユーザーデバイス上のデフォルトプリンターがセッションでどのように確立されるかを指定します。

デフォルトでは、ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます。

各ユーザーデバイスのセッションで自動作成されるネットワークプリンターも指定します。デフォルトでは、プリンターは指定されていません。

- デフォルトプリンターの値を設定する場合：

  ユーザーデバイスの現在のデフォルトプリンターを使用するには、「Do not adjust」を選択します。

  デフォルトプリンターに現在のRemote Desktop ServicesまたはWindowsユーザープロファイル設定を使用するには、「調整しない」を選択します。このオプションを選択した場合、デフォルトプリンターはプロファイルに保存されず、他のセッションまたはクライアントのプロパティに応じて変更されません。セッション内のデフォルトプリンターは、セッションで自動作成された最初のプリンターであり、それは次のいずれかです。

  - **コントロールパネル > デバイスとプリンター**でWindowsサーバーにローカルに追加された最初のプリンター。
  - サーバーにローカルに追加されたプリンターがない場合、最初に自動作成されたプリンター。

- **セッションプリンターの値: プリンターを追加する**を設定する場合、自動作成したいプリンターのUNCパスを入力します。または、**参照**をクリックして、ネットワーク全体でプリンターを検索します。プリンターサーバーのFQDNまたはNetBIOS名を入力してプリンターを検索することもできます。詳細については、セッションプリンターを参照してください。プリンターを追加した後、ログオンごとに現在のセッションにカスタマイズされた設定を適用できます。

プリンターの自動作成イベントログ設定

この設定は、プリンターの自動作成プロセス中にログに記録されるイベントを指定します。エラーや警告をログに記録しない、エラーのみをログに記録する、またはエラーと警告をログに記録する、のいずれかを選択できます。

デフォルトでは、エラーと警告がログに記録されます。

警告の例としては、プリンターのネイティブドライバーをインストールできず、代わりにUniversal print driverがインストールされるイベントがあります。このシナリオでUniversal print driverを使用するには、Universal print driverの使用設定を「Use universal printing only」または「Use universal printing only if the requested driver is unavailable」に構成します。

セッションプリンター

この設定は、セッションで自動作成されるネットワークプリンターを指定します。ICA/HDXセッション内では、Citrix Print Managerサービス（CpSvc.exe）が、**セッションプリンター**ポリシー設定で指定された各ネットワークプリンターに対して、セッションログオン中にネットワークプリ

ンター接続を作成します。セッションログオフ中にプリンターを削除します。デフォルトでは、プリンターは指定されていません。

「**セッションプリンター**」ポリシー設定では、ネットワークプリンターはWindows Print ServerまたはCitrix Universal™ Print Serverに配置できます。

- **Windows Print Server:** 1つ以上のネットワークプリンターを共有します。また、ネットワークプリンターを使用するために必要なネイティブプリンタードライバーも備えています。
- **Universal Print Server:** Citrix Universal Print Serverソフトウェアがインストールされている Windows Print Serverです。

Windows Print Serverを使用する場合、Citrix Print Managerサービスは、ネイティブプリンタードライバーを使用してネットワークプリンター接続を作成します。Citrix Virtual Apps™サーバーには、ネイティブプリンタードライバーがインストールされている必要があります。

Citrix Universal Print Serverを使用する場合、Citrix Print Managerサービスは、ネイティブプリンタードライバー、Citrix Universal Printer Driver、またはCitrix Universal XPS Printer Driverのいずれかを使用してネットワークプリンター接続を作成します。使用するドライバーは、Universal Print Driverの使用ポリシー設定によって制御されます。

現在、すべてのWindowsプリンタードライバーはv3またはv4ドライバーバージョンのいずれかに分類されます。詳細については、「Microsoft V3およびV4プリンタードライバーアーキテクチャのサポート」を参照してください。

セッションプリンターを追加し、それらがセッションに表示されることを確認するには、次の手順を実行します。

1. Web Studioにサインインし、左ペインで**ポリシー**を選択し、次に**ポリシー**タブをクリックします。
2. ポリシーを選択し、 をクリックします。
3. **設定の編集**ページで、**デフォルト値を使用**チェックボックスをオフにし、次の手順に従ってプリンターを追加するために**追加**をクリックします。

    a. プリンターのUNCパスを次の形式で入力します: `\\<FQDN of the printer server>\<printer name>.` または、**参照**をクリックしてネットワーク全体からプリンターを検索します。プリンターサーバーのFQDNまたはNetBIOS名を入力してプリンターを参照することもできます。

    > **注：**

> **参照**を使用して特定のプリンターを検索できるようにするには、プリンターを構成する際に、**プリンター設定 > プリンターのプロパティ > 共有**の下にある**ディレクトリに一覧表示**オプションが選択されていることを確認してください。

b. デフォルトでは、プリンターサーバーを参照するためにユーザー名とパスワードが使用されます。異なるドメイン資格情報が必要な場合は、**別のドメイン資格情報を使用して参照**を選択し、必要なユーザー名とパスワードを入力し、次に**参照**をクリックします。

c. **完了**をクリックします。

4. ポリシーが設定された後、公開アプリケーションにセッションプリンターが表示されない場合があります。この問題は、Citrix Virtual Appsサーバーにプリンタードライバーがないか、ポリシーが作成されたものの有効になっていないために発生する可能性があります。

> **注:**
>
> セッションプリンターにネイティブプリンタードライバーが必要で、そのネイティブプリンタードライバーが VDA にインストールされていない場合、セッションプリンターはセッションに作成されない可能性があります。

5. 公開されたデスクトップを起動し、 **>** でセッションプリンターを手動で追加します。
6. これが失敗した場合は、Citrix Virtual Apps サーバーとプリントサーバー間の通信を調査します。RDP を使用してテストを実行することを検討してください。

プリンターが作成されるのを待つ

Delivery Controller のポリシーを使用して、Citrix Virtual Desktops でこの機能を有効にします。

プリンターが作成されるまで待機（サーバーデスクトップ）：

この設定により、セッションへの接続を遅延させ、クライアントリダイレクトされたプリンターを自動作成できます。

デフォルトでは、接続遅延は発生しません。

プリンターが作成されるまで待機（Citrix Virtual Apps）：

次の PowerShell コマンドレットを実行すると、マルチセッションホストで実行されている仮想アプリへの接続を遅延させ、アプリケーションが開かれる前にクライアントリダイレクトされたプリンターを自動作成できます。

```
Set-BrokerApplication -Name <VirtualAppName> -WaitForPrinterCreation $true
```

デフォルトでは、接続遅延は発生しません。

クライアントプリンターポリシー設定

クライアントプリンターセクションには、クライアントプリンターの自動作成、プリンタープロパティの保持、プリントサーバーへの接続などのクライアントプリンターのポリシー設定が含まれています。

クライアントプリンターの自動作成

この設定は、自動作成されるクライアントプリンターを指定します。この設定は、デフォルトのクライアントプリンター自動作成設定を上書きします。

デフォルトでは、すべてのクライアントプリンターが自動作成されます。

この設定は、**クライアントプリンターリダイレクト**設定が存在し、**許可**に設定されている場合にのみ有効になります。

この設定をポリシーに追加する際は、オプションを選択してください。

- **すべてのクライアントプリンターを自動作成**すると、ユーザーデバイス上のすべてのプリンターが自動的に作成されます。
- **クライアントのデフォルトプリンターのみを自動作成**すると、ユーザーデバイスでデフォルトプリンターとして選択されているプリンターのみが自動的に作成されます。
- **ローカル（ネットワーク以外）のクライアントプリンターのみを自動作成**すると、LPT、COM、USB、TCP/IP、またはその他のローカルポートを介してユーザーデバイスに直接接続されているプリンターのみが自動的に作成されます。
- **クライアントプリンターを自動作成しない**を選択すると、ユーザーがログオンしたときにすべてのクライアントプリンターの自動作成が無効になります。このオプションを選択すると、クライアントプリンターの自動作成に関するRemote Desktop Services（RDS）の設定が、優先度の低いポリシーのこの設定を上書きします。

汎用ユニバーサルプリンターの自動作成

この設定は、セッション用の汎用Citrix Universal™ Printerオブジェクトの自動作成を有効または無効にします。これらのセッションには、ユニバーサル印刷と互換性のあるユーザーデバイスが使用されているセッションのみが含まれます。

デフォルトでは、汎用ユニバーサルプリンターオブジェクトは自動作成されません。

関連するポリシー設定は次のとおりです。

- ユニバーサルプリントドライバーの使用状況
- ユニバーサルドライバーの優先順位

PDFユニバーサルプリンターの自動作成

この設定は、以下のセッションでCitrix PDFプリンターの自動作成を有効または無効にします。

- Windows向けCitrix Workspaceアプリ (VDA 7.19以降)
- Linux向けCitrix Workspace™アプリ
- macOS向けCitrix Workspaceアプリ
- HTML5向けCitrix Workspaceアプリ
- Chrome向けCitrix Workspaceアプリ

デフォルトでは、Citrix PDFプリンターは自動作成されません。

クライアントプリンター名

この設定は、自動作成されたクライアントプリンターの名前付け規則を選択します。

デフォルトでは、標準のプリンター名が使用されます。

「HPLaserJet 4 from client name in session 3」のようなプリンター名を使用するには、**標準プリンター名**を選択します。

旧式のクライアントプリンター名を使用し、製品のXenDesktopバージョンに存在するレガシープリンター名との下位互換性を維持するには、**レガシープリンター名**を選択します。このオプションは、現在のCitrix Virtual Apps and Desktopsバージョンの製品で使用できます。レガシープリンター名の例は「Client/clientname#/HPLaserJet 4」です。このオプションはセキュリティが低下します。

Citrix Workspace app for HTML5 から起動したセッションで Citrix PDF プリンターを使用する場合、**クライアントプリンター名**設定をデフォルトにするか、**標準プリンター名**を選択します。**レガシープリンター名**を選択した場合、Citrix Workspace app for HTML5 は Citrix PDF プリンターオプションをサポートしません。

印刷サーバーへの直接接続

この設定は、仮想デスクトップまたはサーバーホスティングアプリケーションからクライアントプリンター用の印刷サーバーへの直接接続を有効または無効にします。ここで、クライアントプリンターはアクセス可能なネットワーク共有でホストされます。

デフォルトでは、直接接続が有効になっています。

ネットワークプリントサーバーが仮想デスクトップまたはサーバーホスティングアプリケーションからWANを介していない場合は、直接接続を有効にします。ネットワークプリントサーバーと仮想デスクトップまたはサーバーホスティングアプリケーションが同じLAN上にある場合、直接通信により印刷が高速化されます。

ネットワークがWANを介している場合、または大幅な遅延や帯域幅の制限がある場合は、直接接続を無効にします。印刷ジョブはユーザーデバイスを経由してルーティングされ、そこでネットワークプリントサーバーにリダイレクトされます。ユーザーデバイスに送信されるデータは圧縮されるため、WANを介してデータが転送される際の帯域幅の消費が少なくなります。

2つのネットワークプリンターが同じ名前を持つ場合、ユーザーデバイスと同じネットワーク上のプリンターが使用されます。

プリンタードライバーのマッピングと互換性

この設定は、自動作成されたクライアントプリンターのドライバー置換ルールを指定します。

この設定は、Microsoft OneNote および XPS Document Writer を自動作成されたクライアントプリンターのリストから除外するように構成されています。

ドライバー置換ルールを定義する際、指定されたドライバーでプリンターが作成されることを許可または禁止できます。また、作成されたプリンターがユニバーサルプリントドライバーのみを使用することを許可できます。ドライバー置換は、ユーザーデバイスが提供するプリンタードライバー名を上書きまたはマッピングし、サーバー上の同等のドライバーに置き換えます。これらのルールにより、サーバーアプリケーションは、サーバーと同じドライバーを持つがドライバー名が異なるクライアントプリンターにアクセスできるようになります。

次のことができます。

- ドライバーマッピングを追加する
- 既存のマッピングを編集する
- マッピングのカスタム設定を上書きする
- マッピングを削除
- リスト内のドライバーエントリの順序を変更

マッピングを追加する際は、クライアントプリンタードライバー名を入力し、置き換えたいサーバードライバーを選択します。

プリンタープロパティの保持

この設定は、プリンターのプロパティを保存するかどうか、およびどこに保存するかを指定します。

デフォルトでは、システムはプリンターのプロパティがユーザーデバイスに保存されるか（利用可能な場合）、またはユーザープロファイルに保存されるかを決定します。

この設定をポリシーに追加するときは、オプションを選択してください。

- 「クライアントデバイスのみに保存」は、保存されていない強制プロファイルまたは移動プロファイルを持つユーザーデバイス用です。
- 「ユーザープロファイルのみに保持」は、帯域幅（このオプションはネットワークトラフィックを削減します）とログオン速度によって制約されるユーザーデバイス、またはレガシープラグインを使用するユーザー向けです。このオプションは、プリンタープロパティをサーバー上のユーザープロファイルに保存し、ユーザーデバイスとのプロパティ交換を防ぎます。このオプションは、リモートデスクトップサービス (RDS) の移動プロファイルが使用されている場合にのみ適用されます。
- 「クライアントに保存されていない場合のみプロファイルに保持」は、システムがプリンタープロパティの保存場所を決定できるようにします。プリンタープロパティは、利用可能な場合はユーザーデバイスに、またはユーザープロファイルに保存されます。このオプションは最も柔軟ですが、ログオン時間を遅くしたり、システムチェックのために余分な帯域幅を使用したりする可能性もあります。
- 「プリンタープロパティを保持しない」は、プリンタープロパティの保存を防ぎます。

保持および復元されたクライアントプリンター

この設定は、ユーザーデバイス上のプリンターの保持と再作成を有効または無効にします。デフォルトでは、クライアントプリンターは自動的に保持および復元されます。

保持されたプリンターとは、ユーザーが作成したプリンターで、次回のセッション開始時に再度作成されるか、記憶されているものです。Citrix Virtual Apps™ が保持されたプリンターを再作成する場合、**クライアントプリンターの自動作成**設定を除くすべてのポリシー設定が考慮されます。

復元されたプリンターとは、管理者が完全にカスタマイズし、保存された状態がクライアントポートに永続的に関連付けられているプリンターです。

CITRIX PDF ユニバーサルプリンタードライバー

Citrix PDF ユニバーサルプリンタードライバーを使用すると、Citrix Virtual Apps and Desktopsによって提供されるホスト型アプリケーションまたは仮想デスクトップで実行されているアプリケーションで開かれたドキュメントをユーザーが印刷できるようになります。ユーザーが**Citrix PDF Printer**オプションを選択すると、ドライバーはファイルをPDFに変換し、そのPDFをローカルデバイスに転送します。その後、PDFはローカルに接続されたプリンターから表示および印刷するために開かれます。PDFは、Citrix Universal Printingでサポートされている形式の1つです（EMFおよびXPSに加えて）。 PDFプリンターは、Citrixポリシーを使用して有効化、構成、およ

びデフォルトとして設定できます。**Citrix PDF Printer**オプションは、Windows、Linux、MacOS、Chrome、およびHTML5用のCitrix Workspaceアプリのユーザーが利用できます。

> **注:**
>
> WindowsエンドポイントにはPDFビューアーが必要です。クライアントには、PDFファイルを開くためにWindowsにファイルタイプ関連付けが登録されているアプリケーションが必要です。

ドライバーポリシー設定

「**ドライバー**」セクションには、プリンタードライバーに関連するポリシー設定が含まれています。

インボックスプリンタードライバーの自動インストール

> **注**
>
> このリリースでは、このポリシーはVDAをサポートしていません。

> この設定は、以下の場所からのプリンタードライバーの自動インストールを有効または無効にします。

- Windowsインボックスドライバーセット
- `pnputil.exe /a`を使用してホストにステージングされたドライバーパッケージ

デフォルトでは、これらのドライバーは必要に応じてインストールされます。

ユニバーサルドライバーの優先順位

この設定は、リストの最初のエントリから始まる、ユニバーサルプリンタードライバーが使用される順序を指定します。

デフォルトでは、優先順位は次のとおりです。

- EMF
- XPS
- PCL5c (ピーシーエルファイブシー)
- PCL4

- PS

ドライバーの追加、編集、削除、およびリスト内のドライバーの順序変更が可能です。

ユニバーサルプリントドライバーの使用

この設定は、ユニバーサル印刷を使用するタイミングを指定します。

デフォルトでは、ユニバーサル印刷は、要求されたドライバーが利用できない場合にのみ使用されます。

ユニバーサル印刷は、標準のモデル固有のドライバーではなく汎用プリンタードライバーを使用するため、ホストコンピューターでのドライバー管理の負担が軽減される可能性があります。ユニバーサルプリントドライバーの可用性は、ユーザーデバイス、ホスト、およびプリントサーバーソフトウェアの機能に依存します。特定の構成では、ユニバーサル印刷が利用できない場合があります。

この設定をポリシーに追加するときは、次の表からオプションを選択します。

オプション	説明
プリンターモデル固有のドライバーのみを使用する	クライアントプリンターが、サインイン時に自動作成される標準のモデル固有のドライバーのみを使用することを指定します。要求されたドライバーが利用できない場合、クライアントプリンターは自動作成できません。
ユニバーサル印刷のみを使用する	標準のモデル固有のドライバーは使用されないことを指定します。プリンターの作成にはユニバーサルプリントドライバーのみが使用されます。
要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用する	利用可能な場合、プリンター作成に標準のモデル固有ドライバーを使用します。ドライバーがサーバーで利用できない場合、クライアントプリンターは適切なユニバーサルドライバーで自動的に作成されます。
ユニバーサル印刷が利用できない場合にのみ、プリンターモデル固有のドライバーを使用する	利用可能な場合、ユニバーサルプリントドライバーを使用します。ドライバーがサーバーで利用できない場合、クライアントプリンターは適切なモデル固有のプリンタードライバーで自動的に作成されます。

Universal Print Serverポリシー設定

「**Universal Print Server**」セクションには、Universal Print Serverを処理するためのポリシー設定が含まれています。

SSL暗号スイート

この設定は、暗号化された印刷データストリーム (CGP) 接続のためにUniversal Print Clientで使用されるSSL/TLS暗号スイートのセットを指定します。

暗号化された印刷Webサービス (HTTPS/SOAP) 接続のためにUniversal Print Clientで使用される暗号スイートパッケージを制御するには、を参照してください。

デフォルト値: ALL

この設定には、次の値があります: ALL、COM、またはGOV。

各値に対応する暗号スイートは次のとおりです:

ALL:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

COM:

TLS_ECDHE_RSA_AES128_CBC_SHA

GOV:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

SSL準拠モード

この設定は、暗号化された印刷データストリーム (CGP) 接続にUniversal Print Clientが使用するNIST Special Publication 800-52への準拠レベルを指定します。

デフォルト値: なし。

この設定には、次の値があります。

なし。

暗号化された印刷データストリーム (CGP) 接続は、デフォルトの準拠モードを使用します。

SP800-52。

暗号化された印刷データストリーム (CGP) 接続は、NIST Special Publication 800-52準拠モードを使用します。

SSL有効

この設定は、Universal Print Clientが以下の目的でSSL/TLSを使用するかどうかを指定します。

- 印刷データストリーム (CGP) 接続
- Webサービス (HTTP/SOAP) 接続

Universal Print Serverを有効にするを**Windowsのネイティブリモート印刷へのフォールバックを有効にする**に設定すると、Microsoft Windowsネットワーク印刷プロバイダーによってフォールバック接続が行われます。この設定は、これらのフォールバック接続には影響しません。

既定値: 無効

この設定には、次の値があります。

有効。

Universal Print Client は、SSL/TLS を使用して Universal Print Server に接続します。

無効。

Universal Print Client は、SSL/TLS を使用して Universal Print Server に接続します。

SSL FIPS モード

この設定は、Universal Print Client が印刷データストリーム (CGP) 接続に使用する SSL/TLS 暗号化モジュールが FIPS モードで実行されるかどうかを指定します。

既定値: 無効

この設定には、次の値があります。

有効。

FIPS モードがオンになります。

無効。

FIPS モードがオフになります。

SSL プロトコルバージョン

この設定は、Universal Print Client が使用する SSL/TLS プロトコルバージョンを指定します。

デフォルト値: ALL

この設定には次の値があります。

ALL。

TLS バージョン 1.0、1.1、または 1.2 を使用します。

ティーエルエスv1.

TLS バージョン 1.0 を使用します。

TLSv1.1。

TLS バージョン 1.1 を使用します。

TLSv1.2。

TLS バージョン 1.2 を使用します。

SSL UNIVERSAL PRINT SERVER 暗号化印刷データストリーム (CGP) ポート

この設定は、Universal Print Server 暗号化印刷データストリーム (CGP) ポートの TCP ポート番号を指定します。このポートは、印刷ジョブのデータを受信します。

デフォルト値: 443

SSL UNIVERSAL PRINT SERVER 暗号化 WEB サービス (HTTPS/SOAP) ポート

この設定は、Universal Print Serverの暗号化されたWebサービス（HTTPS/SOAP）ポートのTCPポート番号を指定します。このポートは、印刷コマンドのデータを受信します。

デフォルト値: 8443

UNIVERSAL PRINT SERVERの有効化

このポリシーは、Citrix Universal Print Server (UPS) の使用を有効または無効にします。このポリシー設定は、仮想デスクトップまたはサーバーホスティングアプリケーションを含む組織単位 (OU) に適用します。このポリシー設定には、Citrix UPSコンポーネントが要求されたプリントサーバーにインストールされていないか、利用できない場合に、ネイティブのWindowsリモート印刷サービスを使用してプリントサーバーへの接続を許可するフォールバックオプションが含まれています。このポリシーへの変更は、VDAが再起動された後にのみ適用されます。

デフォルトでは、Universal Print Serverは無効になっています。

この設定をポリシーに追加するときは、次のいずれかのオプションを選択します。

- **Windowsネイティブのリモート印刷へのフォールバックを有効にする**: 可能な場合、Universal Print Serverはネットワークプリンター接続を処理します。Universal Print Serverが利用できない場合、Windows Print Providerが使用されます。Windows Print Providerは、以前にWindows Print Providerで作成されたすべてのプリンターの処理を継続します。
- **Windowsネイティブのリモート印刷へのフォールバックなしで有効にする**: Universal Print Serverは、ネットワークプリンター接続を排他的に処理します。Universal Print Serverが利用できない場合、ネットワークプリンター接続は失敗します。この設定は、Windows Print Providerを介したネットワーク印刷を実質的に無効にします。この設定を含むポリシーがアクティブな間は、以前にWindows Print Providerで作成されたプリンターは作成されません。
- **無効**: Universal Print Server機能は無効になっています。UNC名を持つネットワークプリンターに接続する際、Universal Print Serverへの接続は試行されません。リモートプリンターへの接続は、引き続きWindowsネイティブのリモート印刷機能を使用します。

UNIVERSAL PRINT SERVER印刷データストリーム (CGP) ポート

この設定は、Universal Print Server印刷データストリームのCommon Gateway Protocol (CGP) リスナーが使用するTCPポート番号を指定します。このポリシー設定は、プリントサーバーを含むOUにのみ適用します。

デフォルトでは、ポート番号は7229に設定されています。

有効なポート番号は1～65535の範囲である必要があります。

UNIVERSAL PRINT SERVER印刷ストリーム入力帯域幅制限 (KBPS)

この設定は、印刷データの転送速度の上限（キロビット/秒単位）を指定します。転送速度は、CGPを使用して各印刷ジョブからUniversal Print Serverに配信される印刷データに対して計算されます。このポリシー設定は、仮想デスクトップまたはサーバーホスティングアプリケーションを含むOUに適用します。

デフォルトでは、値は0で、上限がないことを示します。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) ポート

この設定は、Universal Print ServerのWebサービス (HTTP/SOAP) リスナーが使用するTCPポート番号を指定します。Universal Print Serverは、ネットワーク印刷シナリオでCitrixユニバーサル印刷ドライバーの使用を可能にするオプションコンポーネントです。

Universal Print Serverが使用される場合、印刷コマンドはCitrix Virtual Apps and Desktopsホストから SOAP over HTTPを介してUniversal Print Serverに送信されます。この設定は、Universal

Print Serverが受信HTTP/SOAPリクエストをリッスンするデフォルトのTCPポートを変更します。

ホストと印刷サーバーのHTTPポートは両方とも同じように構成する必要があります。ポートを同じように構成しない場合、ホストソフトウェアはUniversal Print Serverに接続しません。この設定はCitrix Virtual Apps and Desktops上のVDAを変更します。さらに、Universal Print Serverのデフォルトポートも変更する必要があります。

デフォルトでは、ポート番号は8080に設定されています。

有効なポート番号は0～65535の範囲である必要があります。

負荷分散用のUNIVERSAL PRINT SERVER

この設定は、他のCitrix®印刷ポリシー設定を評価した後、セッション起動時に確立されたプリンター接続の負荷分散に使用されるUniversal Print Serverを一覧表示します。プリンター作成時間を最適化するために、Citrixはすべての印刷サーバーが同じ共有プリンターのセットを持つことを推奨します。負荷分散のために追加できる印刷サーバーの数に上限はありません。

この設定は、印刷サーバーのフェイルオーバー検出とプリンター接続の回復も実装します。印刷サーバーは定期的に可用性がチェックされます。サーバー障害が検出された場合、そのサーバーは負荷分散スキームから削除されます。また、そのサーバー上のプリンター接続は、他の利用可能な印刷サーバーに再配布されます。障害が発生した印刷サーバーが回復すると、負荷分散スキームに戻されます。

「**Validate Servers**」をクリックして、各サーバーが印刷サーバーであること、サーバーリストに重複するサーバー名が含まれていないこと、およびすべてのサーバーに同一の共有プリンターセットがインストールされていることを確認します。この操作には時間がかかる場合があります。

UNIVERSAL PRINT SERVERのサービス停止しきい値

この設定は、ロードバランサーが利用できない印刷サーバーが回復するのをどれだけ長く待つかを指定します。この時間を過ぎると、サーバーが永続的にオフラインであると判断され、その負荷が他の利用可能な印刷サーバーに再配布されます。

デフォルトでは、しきい値は180（秒）に設定されています。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) 接続タイムアウト

この設定は、Universal Print Client が Universal Print Server Webサービスの connect() 操作がタイムアウトするまで待機する秒数を指定します。この設定には、以下の値があります。これらの値はすべて数値であり、単位（時間）は秒です。

- 最小値は0です。

- 最大値は60です。
- 既定値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Client は、操作が完了するまで指定された時間待機します。この操作は、TCPソケットの接続操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Client は、オペレーティングシステムによって定義された既定のタイムアウトを使用します。この構成は、この変更前のUniversal Print Clientの以前のバージョンで利用可能だった構成です。

Universal Print Clientは、Universal Print Serverと通信するVirtual Delivery Agent (VDA) のコンポーネントです。

> **注:**
>
> このポリシー設定は、VDAバージョン7.35以降に適用されます。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) 受信タイムアウト

この設定は、Universal Print Client が Universal Print Server Webサービスの recv() 操作がタイムアウトするまで待機する秒数を指定します。この設定には以下の値があり、これらの値はすべて数値であり、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- 既定値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Client は、操作が完了するまで指定された時間待機します。この操作は、TCPソケットの受信操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Clientはオペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前のUniversal Print Clientの以前のバージョンで利用可能だった構成です。

Universal Print Clientは、Universal Print Serverと通信するVirtual Delivery Agent (VDA) のコンポーネントです。

> **注:**
>
> このポリシー設定は、VDAバージョン7.35以降に適用されます。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) 送信タイムアウト

この設定は、Universal Print ClientがUniversal Print Server Webサービスのsend()操作がタイムアウトするまで待機する秒数を指定します。この設定には次の値があります。これらの値はすべて数値であり、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- デフォルト値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Clientは操作が完了するまで指定された時間待機します。この操作はTCPソケット送信操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Clientはオペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前のUniversal Print Clientの以前のバージョンで利用可能だった構成です。

Universal Print Clientは、Universal Print Serverと通信するVDAのコンポーネントです。

> **注:**
>
> このポリシー設定は、VDAバージョン7.35以降に適用されます。

ユニバーサル印刷ポリシー設定

「**ユニバーサル印刷**」セクションには、ユニバーサル印刷を管理するためのポリシー設定が含まれています。

ユニバーサル印刷EMF処理モード

この設定は、Windowsユーザーデバイス上のEMFスプールファイルを処理する方法を制御します。

デフォルトでは、EMFレコードはプリンターに直接スプールされます。

この設定をポリシーに追加するときは、オプションを選択します。

- プリンター用のEMFを再処理すると、EMFスプールファイルがユーザーデバイス上のGDIサブシステムを介して再処理および送信されるよう強制されます。この設定は、EMFの再処理を必要とするが、セッションで自動的に選択されない可能性のあるドライバーに使用できます。
- プリンターに直接スプール（Citrix Universal™印刷ドライバーと併用する場合）は、EMFレコードがスプールされ、処理のためにユーザーデバイスに配信されることを保証します。通常、これらのEMFスプールファイルはクライアントのスプールキューに直接挿入されます。EMF形式と互換性のあるプリンターおよびドライバーの場合、これは最速の印刷方法です。

ユニバーサル印刷画像圧縮制限

この設定は以下を指定します:

- Citrix Universal印刷ドライバーで印刷される画像に利用可能な最大品質
- Citrix Universal印刷ドライバーで印刷される画像に利用可能な最小圧縮レベル

デフォルトでは、画像圧縮制限は「最高品質（ロスレス圧縮）」に設定されています。

「圧縮なし」が選択されている場合、圧縮はEMF印刷のみで無効になります。

この設定をポリシーに追加するときは、オプションを選択します。

- 圧縮なし
- 最高品質（ロスレス圧縮）
- 高品質
- 標準品質
- 低品質（最大圧縮）

この設定を、**ユニバーサル印刷最適化のデフォルト**設定を含むポリシーに追加する場合、次の点に注意してください。

- **ユニバーサル印刷画像圧縮制限**設定の圧縮レベルが、**ユニバーサル印刷最適化のデフォルト**設定で定義されているレベルよりも低い場合を考慮してください。この場合、画像はユニバーサル印刷画像圧縮制限設定で定義されているレベルで圧縮されます。
- 圧縮が無効になっている場合、ユニバーサル印刷最適化のデフォルト設定の「希望する画質」と「高負荷圧縮を有効にする」オプションは、ポリシーに影響を与えません。

ユニバーサル印刷最適化のデフォルト

この設定は、セッション用にユニバーサル印刷ドライバーが作成される際の印刷最適化のデフォルト値を指定します。

- 希望する画質は、ユニバーサル印刷に適用されるデフォルトの画像圧縮制限を指定します。デフォルトでは、標準品質が有効になっており、ユーザーは標準または低品質の圧縮を使用してのみ画像を印刷できることを意味します。
- 高負荷圧縮を有効にするは、希望する画質で設定された圧縮レベルを超えて帯域幅を削減するかどうかを有効または無効にします。画質は低下しません。デフォルトでは、高負荷圧縮は無効になっています。
- 画像とフォントのキャッシュ設定は、印刷ストリームに複数回出現する画像とフォントをキャッシュするかどうかを指定します。この設定により、一意の画像またはフォントがプリンターに一度だけ送信されることが保証されます。デフォルトでは、埋め込み画像とフォントはキャッシュされます。これらの設定は、ユーザーデバイスがこの動作をサポートしている場合にのみ適用されます。
- 管理者以外のユーザーがこれらの設定を変更することを許可するは、ユーザーがセッション内でデフォルトの印刷最適化設定を変更できるかどうかを指定します。デフォルトでは、ユーザーはデフォルトの印刷最適化設定を変更できません。

注: これらのオプションはすべてEMF印刷でサポートされています。XPS印刷では、「希望する画質」オプションのみがサポートされています。

この設定を、**ユニバーサル印刷画像圧縮制限**設定を含むポリシーに追加する場合は、以下の点に注意してください。

- **ユニバーサル印刷画像圧縮制限**設定の圧縮レベルが、**ユニバーサル印刷最適化のデフォルト**設定で定義されているレベルよりも低い場合を考えます。この場合、画像はユニバーサル印刷画像圧縮制限設定で定義されているレベルで圧縮されます。
- 圧縮が無効になっている場合、ユニバーサル印刷最適化のデフォルト設定の「希望する画質」および「高負荷圧縮を有効にする」オプションは、ポリシーで効果がありません。

ユニバーサル印刷プレビューの優先設定

この設定は、自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して、印刷プレビュー機能を使用するかどうかを指定します。

デフォルトでは、自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して、印刷プレビューは使用されません。

この設定をポリシーに追加する場合は、オプションを選択します。

- 自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して印刷プレビューを使用しない
- 自動作成されたプリンターに対してのみ印刷プレビューを使用する

- 汎用ユニバーサルプリンターに対してのみ印刷プレビューを使用する
- 自動作成されたプリンターと汎用ユニバーサルプリンターの両方に対して印刷プレビューを使用する

ユニバーサル印刷の印刷品質制限

この設定は、セッションで印刷出力を生成するために利用できる最大ドット/インチ (dpi) を指定します。

デフォルトでは、「制限なし」が有効になっており、これは、ユーザーが接続するプリンターで許可されている最高の印刷品質を選択できることを意味します。

この設定が構成されている場合、出力解像度の観点から、ユーザーが利用できる最高の印刷品質を制限します。印刷品質自体と、ユーザーが接続するプリンターの印刷品質機能の両方が、構成された設定に制限されます。

例えば、中解像度 (600 DPI) に設定されている場合、ユーザーは最大 600 DPI の品質で出力物を印刷できます。また、**Universal Printer** ダイアログボックスの**詳細設定**タブにある**印刷品質**設定には、中品質 (600 DPI) までの解像度設定のみが表示されます。

この設定をポリシーに追加するときは、オプションを選択します。

- ドラフト (150 DPI)
- 低解像度 (300 DPI)
- 中解像度 (600 DPI)
- 高解像度 (1200 DPI)
- 制限なし

セキュリティポリシー設定

セキュリティセクションには、セッション暗号化とログオンデータの暗号化を構成するためのポリシー設定が含まれています。

SecureICAの最小暗号化レベル

この設定は、サーバーとユーザーデバイス間で送信されるセッションデータを暗号化する最小レベルを指定します。

重要: Virtual Delivery Agent 7.xの場合、このポリシー設定は、RC5 128ビット暗号化によるログオンデータの暗号化を有効にするためにのみ使用できます。その他の設定は、Citrix Virtual Apps and Desktopsのレガシーバージョンとの下位互換性のためにのみ提供されています。

VDA 7.xの場合、セッションデータの暗号化はVDAのDelivery Groupの基本設定を使用して行われます。Delivery GroupでEnable Secure ICAが選択されている場合、セッションデータはRC5 (128ビット) 暗号化を使用して暗号化されます。Delivery GroupでEnable Secure ICAが選択されていない場合、セッションデータは基本暗号化で暗号化されます。

この設定をポリシーに追加するときは、オプションを選択してください。

- Basicは、非RC5アルゴリズムを使用してクライアント接続を暗号化します。これにより、データストリームが直接読み取られるのを防ぎますが、復号化は可能です。デフォルトでは、サーバーはクライアントとサーバー間のトラフィックにBasic暗号化を使用します。
- RC5 (128ビット) ログオンのみは、RC5 128ビット暗号化を使用してログオンデータを暗号化し、Basic暗号化を使用してクライアント接続を暗号化します。
- RC5 (40ビット) は、RC5 40ビット暗号化を使用してクライアント接続を暗号化します。
- RC5 (56ビット) は、RC5 56ビット暗号化を使用してクライアント接続を暗号化します。
- RC5 (128ビット) は、RC5 128ビット暗号化を使用してクライアント接続を暗号化します。

クライアントとサーバー間の暗号化に指定する設定は、環境内の他の暗号化設定やWindowsオペレーティングシステムと相互作用する可能性があります。サーバーまたはユーザーデバイスのいずれかでより高い優先度の暗号化レベルが設定されている場合を考慮してください。この場合、公開リソースに指定した設定が上書きされる可能性があります。

特定のユーザーの通信とメッセージの整合性をさらに保護するために、暗号化レベルを上げることができます。ポリシーでより高い暗号化レベルが必要な場合、より低い暗号化レベルを使用しているCitrix Receiversは接続を拒否されます。

SecureICAは認証を実行したり、データの整合性をチェックしたりしません。サイトにエンドツーエンドの暗号化を提供するには、SecureICAをTLS暗号化と組み合わせて使用します。

SecureICA は FIPS 準拠のアルゴリズムを使用しません。この設定が問題となる場合、サーバーと Citrix Receiver を SecureICA を使用しないように構成してください。

SecureICAは、機密保持のためにRFC 2040で説明されているRC5ブロック暗号を使用します。ブロックサイズは64ビット（32ビットワード単位の倍数）です。キー長は128ビットです。ラウンド数は12です。

RC5 ブロック暗号のキーは、セッションが作成されるときにネゴシエートされます。ネゴシエーションは Diffie-Hellman アルゴリズムを使用して実行されます。このネゴシエーションでは、Diffie-Hellman の公開パラメーターが使用されます。これらのパラメーターは、Virtual Delivery Agent がインストールされるときに Windows レジストリに保存されます。公開パラメーターは秘密ではありません。Diffie-Hellman ネゴシエーションの結果は秘密鍵であり、そこから RC5 ブ

ロック暗号のセッションキーが導出されます。ユーザーログオンとデータ転送には、個別のセッションキーが使用されます。また、Virtual Delivery Agent との間でのトラフィックにも個別のセッションキーが使用されます。したがって、各セッションには 4 つのセッションキーがあります。秘密鍵とセッションキーは保存されません。RC5 ブロック暗号の初期化ベクトルも秘密鍵から導出されます。

サーバー制限ポリシー設定

サーバー制限セクションには、アイドル接続を制御するためのポリシー設定が含まれています。

サーバーアイドルタイマー間隔

この設定は、ユーザーからの入力がない場合に、中断されないユーザーセッションがどのくらいの期間維持されるかを決定します。データはミリ秒で計算されます。

デフォルトでは、アイドル接続は切断されません（サーバーアイドルタイマー間隔 = 0）。Citrix®は、この値を最小60000ミリ秒（60秒）に設定することを推奨しています。

ポリシーを表示するには、「**複数のバージョン**」を選択し、シングルセッションOSのバージョンをクリアしてから、「**サーバー制限**」を選択します。

> 「注」
>
> このポリシー設定が使用されている場合、セッションが指定された時間アイドル状態であったときに、「アイドルタイマーの期限切れ」ダイアログボックスがユーザーに表示されることがあります。Citrixポリシー設定は、このMicrosoftダイアログボックスメッセージを制御しません。詳細については、`<http://support.citrix.com/article/CTX118618>`を参照してください。

セッション制限ポリシー設定

セッション制限セクションには、セッションが強制的にログオフされるまでに接続を維持する期間を制御するポリシー設定が含まれています。

切断されたセッションタイマー

この設定は、切断されロックされたデスクトップが、セッションがログオフされるまでにロックされたままになる期間を指定するタイマーを有効または無効にします。

このタイマーが有効になっている場合、タイマーの期限が切れると、切断されたセッションはログオフされます。

デフォルトでは、切断されたセッションはログオフされません。

Remote PC Accessの切断されたセッションタイマー

この設定は、タイマーの期限が切れた後に切断されたユーザーセッションをログオフするタイマーを有効または無効にします。この設定を有効にする場合は、**切断されたセッションタイマー間隔**設定を使用して、ユーザーセッションがログオフされるまでに切断されたデスクトップがロック状態を維持する期間を分単位で指定します。

デフォルトでは、この設定は無効になっています。

切断されたセッションタイマー間隔

この設定は、切断されロックされたデスクトップが、セッションがログオフされるまでにロック状態を維持する期間を分単位で指定します。

デフォルトでは、期間は1,440分（24時間）です。

切断されたセッションタイマー – マルチセッション

この設定は、切断されたRDSセッションがログオフされるまでにどのくらいの期間持続できるかを決定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっており、切断されたセッションはログオフされません。

切断されたセッションタイマー間隔 – マルチセッション

この設定は、切断されたRDSセッションがログオフされるまでに、何分間持続できるかを決定します。デフォルトでは、期間は1440分（24時間）です。

セッション接続タイマー

この設定は、ユーザーデバイスとデスクトップ間の途切れない接続の最大継続時間を指定するタイマーを有効または無効にします。このタイマーが有効になっている場合、タイマーの期限が切れるとセッションは切断されるか、ログオフされます。Microsoft の「**時間制限に達したときにセッションを終了する**」設定が、セッションの次の状態を決定します。

デフォルトでは、このタイマーは無効になっています。

セッション接続タイマー間隔

この設定は、ユーザーデバイスとデスクトップ間の途切れない接続の最大分数（時間）を指定します。

デフォルトでは、最大継続時間は1,440分（24時間）です。

セッション接続タイマー – マルチセッション

この設定は、ユーザーデバイスとターミナルサーバー間の途切れない接続の最大継続時間を指定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっています。

セッション接続タイマー間隔 – マルチセッション

この設定は、ユーザーデバイスとRDSセッション間の途切れない接続の最大分数（時間）を指定します。デフォルトでは、最大継続時間は1440分（24時間）です。

セッションアイドルタイマー

ユーザーが何も入力しない場合、この設定は以下を有効または無効にするために使用されます。

- デスクトップへの途切れないユーザーデバイス接続が維持される期間を指定するタイマー。

このタイマーの期限が切れると、セッションは切断状態になり、「**切断されたセッションタイマー**」が適用されます。「**切断されたセッションタイマー**」が無効になっている場合、セッションはログオフされません。

デフォルトでは、このタイマーは有効になっています。

セッションアイドルタイマー間隔

ユーザーからの入力がない場合、この設定は以下を指定するために使用されます。

- デスクトップへのユーザーデバイスの途切れない接続が維持される分数。

デフォルトでは、アイドル状態の接続は1,440分（24時間）維持されます。

セッションアイドルタイマー – マルチセッション

この設定は、ユーザーデバイスとターミナルサーバー間のアイドル接続の最大期間を決定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっています。

セッションアイドルタイマー間隔 – マルチセッション

この設定は、ユーザーデバイスとRDSセッション間のアイドル接続が何分間続くかを指定します。デフォルトでは、最大期間は1440分（24時間）です。

> **注:**
>
> Citrix®ポリシーを使用して構成されたマルチセッションマシンのタイマー設定は、Microsoftグループポリシーを通じて構成されたタイマー設定を上書きすることが想定されています。予期しない動作を避けるため、いずれかの方法を使用してタイマー設定を構成することをお勧めします。

セッションの信頼性ポリシー設定

セッションの信頼性セクションには、セッションの信頼性接続を管理するためのポリシー設定が含まれています。

セッションの信頼性接続

この設定により、ネットワーク接続が失われたときにセッションを開いたままにするかどうかが決まります。セッションの信頼性は、自動クライアント再接続と連携して、ネットワーク障害から回復した後にユーザーがCitrix Workspace™アプリセッションに自動的に再接続できるようにします。デフォルトでは、セッションの信頼性は許可されています。

Web Studioの設定は、以下のクライアントに適用されます。

- Citrix Workspaceアプリ1808以降
- Windows版 シトリックス レシーバー 4.7 以降。

Web Studioポリシーは、クライアント上のCitrix Receiver™グループポリシーオブジェクトを上書きします。Web Studioでこれらのポリシーを更新すると、セッションの信頼性がサーバーからクライアントに同期されます。

> **注:**
>
> - Citrix Receiver for Windows 4.7以降およびWindows向けCitrix Workspaceアプリ - Web Studioでポリシーを設定します。
> - Citrix Receiver for Windows 4.7より前のバージョン - Web Studioでポリシーを設定します。また、一貫した動作のために、クライアントでCitrix Receiverグループポリシーオブジェクトテンプレートを設定します。

> セッションの信頼性により、ネットワーク接続が中断された場合でも、セッションがアクティブな状態に保たれ、ユーザーの画面に表示されます。ユーザーは、ネットワーク接続が再開されるまで、使用中のアプリケーションを引き続き見ることができます。

セッションの信頼性を使用して、サーバー上でセッションをアクティブな状態に保ちます。接続が失われたことを示すために、ユーザーのディスプレイは不透明になります。ユーザーは中断中にフリーズしたセッションを見る可能性があります。ネットワーク接続が復元されると、ユーザーはア

プリケーションとの対話を再開できます。セッションの信頼性により、再認証のプロンプトなしでユーザーが再接続されます。

セッションの信頼性と自動クライアント再接続の両方を使用する場合、これら2つの機能は順番に動作します。セッションの信頼性は、セッションの信頼性タイムアウト設定で指定された時間の経過後にユーザーセッションを閉じ（または切断し）ます。その後、自動クライアント再接続設定が有効になり、切断されたセッションにユーザーを再接続しようとします。

デフォルトでは、セッションの信頼性は許可されています。

> **注:**
>
> Citrix ADCを使用している場合、ICA接続をプロキシするには、Citrix StoreFront > **Manage Citrix Gateways / Secure Ticket Authority**で**セッションの信頼性を有効にする**を選択する必要があります。

セッションの信頼性ポート番号

この設定は、受信セッションの信頼性接続に使用するTCPポート番号を指定します。

デフォルトでは、ポート番号は2598に設定されています。

セッションの信頼性タイムアウト

この設定は、秒単位で時間の長さを指定します。この時間は、セッションの信頼性プロキシがユーザーの再接続を待機し、セッションが切断されるまでの時間です。

セッションが開いている時間を延長することはできますが、この機能は利便性のためであり、ユーザーに再認証を促すものではありません。セッションが開いている時間が長くなるほど、ユーザーがデバイスを放置し、不正なユーザーがアクセスする可能性が高まります。

デフォルトでは、タイムアウトは180秒（3分）に設定されています。

セッションウォーターマークポリシー設定

「**セッションウォーターマーク**」セクションには、この機能を構成するためのポリシー設定が含まれています。 この機能を有効にすると、VDAマシンのネットワーク帯域幅とCPU使用率が大幅に増加します。利用可能なハードウェアリソースに基づいて、選択したVDAマシンにセッションウォーターマークを設定することをお勧めします。

> **重要**

> 他のウォーターマークポリシー設定を有効にするには、セッションウォーターマークを有効にします。より良いユーザーエクスペリエンスを実現するために、ウォーターマークテキスト項目を2つ以上有効にしないでください。

セッションウォーターマークを有効にする

この設定を有効にすると、セッションディスプレイにはセッション固有の情報を表示する不透明なテキストウォーターマークが表示されます。他のウォーターマーク設定は、この設定が有効になっているかどうかに依存します。

デフォルトでは、セッションウォーターマークは無効になっています。

クライアントIPアドレスを含める

この設定を有効にすると、セッションには現在のクライアントIPアドレスがウォーターマークとして表示されます。

デフォルトでは、クライアントIPアドレスを含めるは無効になっています。

接続時間を含める

この設定を有効にすると、セッションウォーターマークに接続時間が表示されます。形式はyyyy/mm/dd hh:mmです。表示される時刻は、システムクロックとタイムゾーンに基づいています。

デフォルトでは、接続時間を含めるは無効になっています。

ログオンユーザー名を含める

この設定を有効にすると、セッションには現在のログオンユーザー名がウォーターマークとして表示されます。表示形式はUSERNAME@DOMAINNAMEです。ユーザー名は最大20文字にすることをお勧めします。ユーザー名が20文字を超える場合、文字フォントが過度に小さくなったり、切り捨てが発生したりして、ウォーターマークの効果が低下する可能性があります。

デフォルトでは、ログオンユーザー名を含めるが有効になっています。

VDAホスト名を含める

この設定を有効にすると、セッションは現在のICA®セッションのVDAホスト名をウォーターマークとして表示します。

デフォルトでは、VDAホスト名を含めるが有効になっています。

VDA IPアドレスを含める

この設定を有効にすると、セッションは現在のICAセッションのVDA IPアドレスをウォーターマークとして表示します。

デフォルトでは、VDA IPアドレスは無効になっています。

セッションウォーターマークのスタイル

この設定は、単一のウォーターマークテキストラベルを表示するか、複数のラベルを表示するかを制御します。**値**ドロップダウンメニューから**複数**または**単一**を選択します。

複数は、セッションに5つのウォーターマークラベルを表示します。中央に1つ、四隅に4つです。

単一は、セッションの中央に単一のウォーターマークラベルを表示します。

デフォルトでは、セッションウォーターマークスタイルは複数です。

ウォーターマークのカスタムテキスト

この設定により、カスタムテキスト（例：会社名）をセッションウォーターマークに表示できます。空でない文字列を設定すると、ウォーターマークで有効になっている他の情報に追記する形で、新しい行にテキストが表示されます。ウォーターマークのカスタムテキストは25 Unicode文字に制限されています。より長い文字列を設定した場合、25文字に切り詰められます。

デフォルトのテキストはありません。

Citrix Virtual Apps and Desktops™ 7 2206以降、テキストにカスタムタグを使用してさらにカスタマイズを追加できます。その結果、カスタムテキストの最大文字数は1024に増加しました。

ウォーターマーク設定で利用可能なタグは、次の表に記載されています。

タグ	説明	例
`<font=value>`	ウォーターマークテキストのフォントを変更できます。値はVDAで利用可能なフォントの名前です。	`<font=Courier New>`
`<fontzoom=value>`	フォントのズーム率を設定できます。値が200の場合、ウォーターマークテキストは200%にズームされます。	`<fontzoom=200>`
`<position=value>`	ウォーターマークテキストの位置を変更できます。値は `center`、`topleft`、`topright`、`bottomleft`、および `bottomright` で	`<position=topright>`

タグ	説明	例
	す。このタグはシングルスタイルでのみ適用可能です。	
`<rotation=value>`	ウォーターマークのテキストを回転できます。値は度数で指定され、範囲は-360から360です。	`<rotation=45>`
`<style=value>`	表示スタイルを変更できます。このタグは、セッションウォーターマークスタイルポリシーを上書きします。	`<style=single>`

以下のウォーターマークスタイルが利用可能です。

- シングルスタイル - セッションの中央に単一のウォーターマークテキストラベルが表示されます。位置タグを使用して場所を変更できます。
- xスタイルまたは複数 - セッションに5つのウォーターマークラベルが表示されます。中央に1つ、各コーナーに1つずつです。
- タイル - セッションに複数のラベルが表示されます。ウォーターマークテキストは画面全体に均等に配置されます。

ウォーターマークテキストを変更するために利用可能なタグは、以下の表に記載されています。

タグ	説明
`<clientip>`	エンドポイントのIPアドレス。
`<date>`	セッションが確立された日付。
`<domain>`	ログインしているユーザーアカウントのドメイン名。
`<hostname>`	VDA のマシン名。
`<newline>`	追加の行を作成します。
`<serverip>`	VDA の IP アドレス。
`<time>`	セッションが確立された時刻。

タグ	説明
`<username>`	ユーザーの名前。

注:

- **ウォーターマークカスタムテキスト**ポリシーは、**セッションウォーターマークを有効にする**ポリシーが有効になっている場合にのみ適用されます。そのデフォルト値は*無効*です。
- ウォーターマークテキストを変更するためのタグを使用する場合、**セッションウォーターマークを有効にする**を除く他のすべてのセッションウォーターマークポリシーは無視されます。ウォーターマークテキスト設定用のタグを使用する場合、他のすべてのウォーターマークポリシーを使用できます。

透かしの透明度

ウォーターマークの不透明度を0から100まで指定できます。指定する値が大きいほど、ウォーターマークは不透明になります。

デフォルトでは、値は17です。

TWAINデバイスのポリシー設定

TWAINデバイスセクションには、以下のポリシー設定が含まれています。

- デジタルカメラやスキャナーなどのクライアントTWAINデバイスのマッピング
- サーバーからクライアントへの画像転送の最適化

注:

Citrix Receiver for Windows 4.5では、TWAIN 2.0がサポートされています。

クライアントTWAINデバイスのリダイレクト

TWAINデバイスは、TWAINプロトコルを使用して、サーバーでホストされている画像処理アプリケーションと通信します。

この設定は、ユーザーがユーザーデバイス上のTWAINデバイスにアクセスすることを許可または禁止します。デフォルトでは、TWAINデバイスのリダイレクトは許可されています。

以下のポリシー設定が関連しています。

- TWAIN圧縮レベル
- TWAINデバイスリダイレクト帯域幅制限
- TWAINデバイスリダイレクト帯域幅制限パーセント

TWAIN圧縮レベル

この設定は、クライアントからサーバーへの画像転送の圧縮レベルを指定します。最良の画質には「低」、良好な画質には「中」、低い画質には「高」を使用します。デフォルトでは、中程度の圧縮が適用されます。

USBデバイスポリシー設定

USBデバイスセクションには、USBデバイスのファイルリダイレクトを管理するためのポリシー設定が含まれています。

クライアントUSBデバイス最適化ルール

クライアントUSBデバイス最適化ルールは、最適化を無効にするか、最適化モードを変更するためにデバイスに適用できます。

ユーザーがUSB入力デバイスを接続すると、ホストは**USBポリシー**設定がそのデバイスを許可するかどうかを確認します。デバイスが許可されている場合、ホストはデバイスの**クライアントUSBデバイス最適化ルール**を確認します。ルールが指定されていない場合、デバイスは最適化されません。キャプチャモード (04) は、署名デバイスに推奨されるモードです。高遅延によってパフォーマンスが低下する他のデバイスの場合、管理者はインタラクティブモード (02) を有効にできます。この記事の表で利用可能なモードの説明を参照してください。

知っておくと良いこと

- Wacomの署名パッドおよびタブレットを使用する場合は、スクリーンセーバーを無効にすることをお勧めします。スクリーンセーバーを無効にする手順は、このセクションの最後に記載されています。
- Wacom STU署名パッドおよびタブレットシリーズ製品の最適化のサポートは、Citrix Virtual Apps and Desktops™ポリシーのインストール時に事前設定されています。
- 署名デバイスはCitrix Virtual Apps and Desktops全体で機能し、署名デバイスとして使用するためにドライバーを必要としません。Wacomには、デバイスをさらにカスタマイズするために

インストールできる追加ソフトウェアがあります。`<http://www.wacom.com/>`を参照してください。

- 描画タブレット。特定の描画入力デバイスは、PCI/ACPIバス上でHIDデバイスとして表示される場合があり、サポートされていません。これらのデバイスは、Citrix Virtual Desktopsセッション内でリダイレクトされるように、クライアント上のUSBホストコントローラーに接続してください。

ポリシールールは、空白で区切られたtag=value式の形式を取ります。以下のタグがサポートされています。

タグ名	説明
モード	最適化モードは、class=**03**の入力デバイスでサポートされています。サポートされているモードは次のとおりです。最適化なし - 値**01**。インタラクティブモード - 値**02**。ペンタブレットや3D Proマウスなどのデバイスに推奨されます。キャプチャモード - 値**04**。署名パッドなどのデバイスに推奨されます。
VID	デバイス記述子からのベンダーID。4桁の16進数として。
PID	デバイス記述子からの製品ID。4桁の16進数として。
REV	デバイス記述子からのリビジョンID。4桁の16進数として。
クラス	デバイス記述子またはインターフェイス記述子のいずれかからのクラス。
サブクラス	デバイス記述子またはインターフェイス記述子のいずれかからのサブクラス。
プロトコル	デバイス記述子またはインターフェイス記述子のいずれかからのプロトコル。

例

Mode=00000004 VID=067B PID=1230 class=03 #キャプチャモードで動作する入力デバイス

Mode=00000002 VID=067B PID=1230 class=03 #インタラクティブモードで動作する入力デバイス（デフォルト）

Mode=00000001 VID=067B PID=1230 class=03 #最適化なしで動作する入力デバイス

Mode=00000100 VID=067B PID=1230 #デバイスセットアップの最適化が無効（デフォルト）

Mode=00000200 VID=067B PID=1230 #デバイスセットアップの最適化が有効

Wacom署名パッドデバイスのスクリーンセーバーを無効にする

Wacom署名パッドおよびタブレットを使用する場合、Citrix®は、次のようにスクリーンセーバーを無効にすることをお勧めします。

1. デバイスをリダイレクトした後、**Wacom-STU-Driver**をインストールします。
2. 署名パッドのコントロールパネルにアクセスするため、**Wacom-STU-Display MSI**をインストールします。
3. **コントロールパネル > Wacom STU Display > STU430** または **STU530** に移動し、お使いのモデルのタブを選択します。
4. **変更**を選択し、UACセキュリティウィンドウが表示されたら**はい**を選択します。
5. **スライドショーを無効にする**を選択し、**適用**をクリックします。

1つの署名パッドモデルに設定が適用されると、すべてのモデルに適用されます。

クライアントUSBデバイスのリダイレクト

この設定は、ユーザーデバイスとの間でUSBデバイスのリダイレクトを許可または禁止します。

デフォルトでは、USBデバイスはリダイレクトされません。

クライアントUSBデバイスリダイレクト規則

この設定は、USBデバイスのリダイレクトルールを指定します。

デフォルトでは、ルールは指定されていません。

ユーザーがUSBデバイスを接続すると、ホストデバイスは一致が見つかるまで各ポリシー規則と照合します。任意のデバイスに対する最初の一致が決定的なものと見なされます。最初の一致が許可ルールである場合、デバイスは仮想デスクトップにリモート接続されます。最初の一致が拒否ルールである場合、デバイスはローカルデスクトップでのみ利用可能です。一致が見つからない場合、デフォルトのルールが使用されます。

ポリシー規則は{Allow:`|`Deny:}の形式をとり、その後に空白で区切られたtag=value式のセットが続きます。次のタグがサポートされています。

タグ名	説明
VID	デバイス記述子からのベンダーID
PID	デバイス記述子からの製品ID
REL	デバイス記述子からのリリースID
クラス	デバイス記述子またはインターフェイス記述子のいずれかからのクラス
サブクラス	デバイス記述子またはインターフェース記述子のいずれかからのサブクラス
プロトコル	デバイス記述子またはインターフェイス記述子のいずれかからのプロトコル

ポリシー規則を作成する際は、次の点に注意してください。

- ルールでは大文字と小文字は区別されません。
- ルールには、末尾に#で始まるオプションのコメントを付けることができます。
- 空行および純粋なコメント行は無視されます。
- タグは一致演算子=を使用する必要があります（例：VID=067B_）。
- 各ルールは新しい行で開始するか、セミコロン区切りのリストの一部である必要があります。
- USB Implementers Forum, Inc.のWebサイトで入手可能なUSBクラスコードを参照してください。

管理者定義の USB ポリシールールの例:

- 許可: VID=067B PID=0007 # 別の産業、別のフラッシュドライブ
- 拒否: Class=08 subclass=05 # マスストレージ
- すべての USB デバイスを拒否するルールを作成するには、他のタグなしで「DENY:」を使用します。

クライアント USB プラグアンドプレイデバイスのリダイレクト

この設定により、カメラやPOS (point-of-sale) デバイスなどのプラグアンドプレイデバイスをクライアントセッションで使用できるようになります。

デフォルトでは、プラグアンドプレイデバイスのリダイレクトは許可されています。「許可」に設定すると、特定のユーザーまたはグループのすべてのプラグアンドプレイデバイスがリダイレクトされます。「禁止」に設定すると、デバイスはリダイレクトされません。

USB デバイスの自動リダイレクトを構成する

USB サポートが有効になっている場合、USB デバイスは自動的にリダイレクトされます。また、USB ユーザー設定は USB デバイスを自動的に接続するように設定されています。

注:

Receiver for Windows 4.2 では、デスクトップアプライアンスモードで動作している場合も USB デバイスは自動的にリダイレクトされます。また、接続バーは表示されません。以前のバージョンの Citrix Receiver for Windows では、USB デバイスは以下のモードで動作している場合も自動的にリダイレクトされます。

- デスクトップアプライアンスモード
- 仮想マシン (VM) ホスト型アプリケーション

すべてのUSBデバイスをリダイレクトすることが常に最適とは限りません。ユーザーは、自動的にリダイレクトされないUSBデバイスリストからデバイスを明示的にリダイレクトできます。USBデバイスが一覧表示されたりリダイレクトされたりするのを防ぐには、クライアントエンドポイントまたはDDCポリシーでDeviceRulesを使用します。詳細については、管理者ガイドを参照してください。

注意:

レジストリエディターを誤って使用すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤用によって生じた問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

USBデバイスの自動リダイレクトに関するユーザー設定

ポリシー:

1. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrixコンポーネント > Citrix Receiver™ > クライアントデバイスのリモート処理 > 汎用USBリモーティング**に移動します。
2. **新しいUSBデバイス**を開き、**有効**を選択し、**OK**をクリックします。
3. **既存のUSBデバイス**を開き、**有効**を選択し、**OK**をクリックします。

シトリックス レシーバー:

1. **シトリックス レシーバー 環境設定 > 接続** に移動します。
2. 次のオプションが選択されていることを確認します。
   - セッションの開始時にデバイスを自動的に接続する
   - セッションの実行中に新しいデバイスが接続された場合、そのデバイスを自動的に接続する。
3. 「**OK**」をクリックします。

すべてのレジストリキーとポリシーの変更は、Windowsクライアントデバイスに適用されます。

通常のUSBプリンターのリダイレクト

通常のUSBプリンターに最適なソリューションは、専用のユニバーサルプリンタードライバーと仮想チャネルを使用して印刷を実行することです。デフォルトでは、通常のUSBプリンターは自動的にリダイレクトされません。

通常のプリンターはヒューリスティックを使用して検出されます。また、例えばスキャン機能を備えた高度なプリンターは、完全に機能させるにはUSBサポートを使用してリダイレクトする必要がある場合があります。

通常のプリンターが自動的にリダイレクトされるかどうかを構成するには、このレジストリを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectPrinters

種類: DWORD

データ: 00000000

デフォルト値は0です（自動的にリダイレクトしません）。値を0より大きい任意の数値に変更すると、通常のUSBプリンターをリダイレクトするためのUSBサポートが有効になります。

Active Directoryポリシーをこのレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きすることもできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectPrinters

種類: DWORD

データ: 00000000

通常のオーディオデバイスのリダイレクト

通常のプリンターと同様に、通常のオーディオデバイスからオーディオデータを送信するには、ICA®の専用オーディオ仮想チャネルを使用することで最高のユーザーエクスペリエンスが得られます。ただし、USBサポートを使用して一部の特殊なデバイスをリダイレクトする必要がある場合があります。どのデバイスが通常のオーディオデバイスであるかを判断するためにヒューリスティックが使用されます。

クライアントエンドポイントでこのレジストリを使用し、通常のオーディオデバイスが自動的にリダイレクトされるかどうかを構成します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectAudio

種類: DWORD

データ: 00000000

デフォルトは0に設定されています (自動的にリダイレクトしません)。値を0以外に変更すると、USBサポート付きのプレーンなUSBオーディオデバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値をレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectAudio

種類: DWORD

データ: 00000000

プレーンなストレージデバイス (マスストレージデバイス) のリダイレクト

通常のストレージデバイスの場合、最適化も実行するクライアントドライブマッピングなどの専用仮想チャネルを使用することで、最高のユーザーエクスペリエンスを実現できます。単純なファイルの読み書きに加えて、CD/DVDの書き込みや暗号化されたファイルシステムデバイスへのアクセスなどの特定の特殊なタスクを実行するには、汎用USBサポートを使用してデバイスをリダイレクトする必要がある場合があります。

ヒューリスティックを使用して、どのデバイスが通常のストレージデバイスであるかを判断します。通常のストレージデバイスを自動的にリダイレクトするかどうかを設定するには、このレジストリキーを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectStorage

種類: DWORD

データ: 00000000

デフォルトは0に設定されています（自動的にリダイレクトされません）。値を0以外に変更すると、汎用USBサポートを使用して通常のUSBストレージデバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値を以下のレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きすることもできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectStorage

種類: DWORD

データ: 00000000

> **注:**
>
> 汎用USBサポートを使用している場合、プレーンストレージデバイスへの読み取り専用アクセスは構成できませんが、CDMを使用している場合は構成できます。

ハードウェア暗号化USBフラッシュドライブのリダイレクト

ハードウェア暗号化を備えたUSBフラッシュドライブは通常、暗号化されたストレージパーティションと、暗号化されたパーティションのロックを解除するためのユーティリティを含む2番目の

ユーティリティパーティションで構成されています。USBフラッシュドライブデバイスの場合、最適化も実行する専用のクライアントドライブマッピング/ダイナミックサムドライブマッピングHDX仮想チャネルを使用すると、最高のユーザーエクスペリエンスが得られます。

汎用USBリダイレクトは、次の目的で必要です。

- Windows以外のクライアント（Linuxクライアントなど）
- 顧客がクライアント上のローカル機能へのユーザーアクセスを制限（ロックダウン）しているクライアント

汎用USBリダイレクトは、ハードウェア暗号化されていない任意のUSBストレージデバイスを、シングルセッションOSおよびマルチセッションOS VDAセッションの両方にリダイレクトできます。

Citrix Virtual Apps™ and Desktops 7 1808より前は、ハードウェア暗号化を備えたUSBフラッシュドライブを、シングルセッションOSまたはマルチセッションOS VDAセッションに有用な方法でリダイレクトすることはできませんでした。Citrix Virtual Apps and Desktops 7 1808で導入された新機能強化により、ハードウェア暗号化を備えたUSBフラッシュドライブの汎用USBリダイレクトが、シングルセッションOSおよびマルチセッションOS VDAセッションでサポートされます。デバイスがリダイレクトされると、そのドライブはローカルクライアントに表示されません。したがって、ドライブのロック解除が必要な場合は、セッション内で実行します。この機能には、Windows Update KB4074590が必要です。

プレーン静止画像デバイス（スキャナーおよびデジタルカメラ）

プレーン静止画像デバイスの場合、最適化も実行する専用の仮想チャネル（TWAIN仮想チャネルなど）を使用すると、最高のユーザーエクスペリエンスが得られます。これらのデバイスは業界標準に準拠している必要があります。デバイスが非準拠であるか、元の意図に従って使用されていないと見なされる場合があります。この場合、汎用USBリダイレクトがデバイスを使用する唯一の方法である可能性があります。どのデバイスがプレーン静止画像デバイスであるかを判断するためにヒューリスティックが使用されます。

プレーン静止画像デバイスを自動的にリダイレクトするかどうかを構成するには、このレジストリキーを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectImage

種類: DWORD

データ: 00000000

デフォルトは0に設定されています（自動的にリダイレクトされません）。値を0以外に変更すると、汎用USBでプレーンなUSB静止画デバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値をこのレジストリキーに展開することもでき、両方が存在する場合は非ポリシー値を上書きします。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectImage

種類: DWORD

データ: 00000000

デバイス固有の設定

Citrix最適化可能デバイスを選択するために使用されるヒューリスティックは、必ずしもユーザーの希望と一致するとは限りません。Citrix最適化可能デバイスの例としては、プリンター、オーディオ、ビデオ、ストレージ、静止画デバイスなどがあります。上記にリストされていないデバイスの自動リダイレクトを制御したい場合があります。自動リダイレクトは、デバイス固有に制御できます。

例として、DemoTech 2,000バーコードリーダーはUSBサポートを使用してリダイレクトする必要はありません。ベンダー識別子12AB、製品識別子5678を持っています。これらの16進数はデバイスマネージャーで確認できます。

これが自動的にリダイレクトされるのを防ぐには、このデバイス固有のレジストリキーを作成します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名前: AutoRedirect

種類: DWORD

データ: 00000000

値が0の場合、デバイスは自動的にリダイレクトされません。0以外の値は、デバイスが自動リダイレクトの対象となることを示します（ユーザー設定による）。ベンダー識別子と製品識別子の間には単一のスペース文字があります。

Active Directoryポリシーを使用して、この値をこのレジストリキーに展開することもできます。両方が存在する場合、非ポリシー値を上書きします。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名前: AutoRedirect

種類: DWORD

データ: 00000000

デバイス固有のAutoRedirect設定は、上記で説明したより一般的なAutoRedirectXXX値よりも優先されます。Citrix最適化デバイスのデフォルトのヒューリスティックは、デバイスを汎用として誤解する可能性があります。したがって、デバイスを自動的にリダイレクトするには、デバイス固有のAutoRedirect値を1に設定します。

既存のUSBデバイスの自動接続を許可する

この設定は、セッション開始時にエンドポイントに接続されている既存のUSBデバイスのリモートセッションへの自動接続を許可または防止します。

この設定をポリシーに追加する際、次のいずれかのオプションを選択します。

- 利用可能なUSBデバイスをリダイレクトする前に確認する。
- 利用可能なUSBデバイスを自動的にリダイレクトしない。
- 利用可能なUSBデバイスを自動的にリダイレクトします。

デフォルトでは、**利用可能なUSBデバイスをリダイレクトする前に確認する**オプションが選択されています。選択されたポリシーに基づいて、クライアントの**Preferences** > **Devices**セクションで選択されたオプションが上書きされる場合があります。

> **注:**
>
> 現在、**既存のUSBデバイスの自動接続を許可する**ポリシーは、Citrix Workspace™ app for Windowsにのみ適用されます。

新しく接続されたUSBデバイスの自動接続を許可する

この設定は、セッション中にエンドポイントに挿入されたUSBデバイスのリモートセッションへの自動接続を許可または防止します。

この設定をポリシーに追加するときは、次のいずれかのオプションを選択します。

- 利用可能なUSBデバイスをリダイレクトする前に確認します。

- 利用可能なUSBデバイスを自動的にリダイレクトしません。
- 利用可能なUSBデバイスを自動的にリダイレクトします。

デフォルトでは、**利用可能なUSBデバイスをリダイレクトする前に確認する**オプションが選択されています。選択されたポリシーに基づいて、クライアントの**Preferences** > **Devices**セクションで選択されたオプションが上書きされる場合があります。

> **注:**
>
> 現在、**新しく接続されたUSBデバイスの自動接続を許可する**ポリシーは、Citrix Workspace app for Windowsにのみ適用されます。

クライアントUSBデバイスリダイレクトルール (バージョン2)

この設定は、USBデバイスのリモートセッションへのフィルタリング、分割、および自動接続のルールを指定します。

この設定が選択されている場合、ホストは*クライアントUSBデバイスリダイレクト規則*設定を、この設定で構成されたデバイス規則で上書きします。

詳細については、複合USBデバイスリダイレクトの構成を参照してください。

仮想チャネル許可リストポリシー設定

仮想チャネル許可リストポリシー設定は、ICA®セッションで開くことが許可されている仮想チャネルを指定する許可リストの使用を可能にします。

無効にすると、すべての仮想チャネルが許可されます。

有効にすると、Citrix®仮想チャネルのみが許可されます。

カスタムまたはサードパーティの仮想チャネルを使用するには、仮想チャネルをリストに追加します。仮想チャネルをリストに追加するには：

1. 仮想チャネル名の後にコンマを入力します。
2. 仮想チャネルにアクセスするプロセスのパスを入力します。

複数の実行可能パスをリストでき、パスはコンマで区切られます。

例:

```
CTXCVC1,C:\VC1\vchost.exe
```

```
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```

Citrix Virtual Apps and Desktops 7 2109以降、仮想チャネル許可リストはデフォルトで有効になっています。許可リストに仮想チャネルを追加する方法の詳細については、「許可リストへの仮想チャネルの追加」を参照してください。

Skype for Business 用のHDX RealTime Optimization Packを使用している場合は、仮想チャネルを許可リストに追加します。詳細については、「HDX RealTime Optimization Packのドキュメント」を参照してください。

> **重要:**
>
> 設定を有効にするには、VDAマシンを再起動する必要があります。

> 仮想チャネルの詳細については、「ICA 仮想チャネル」を参照してください。

仮想チャネル許可リストのログ記録

このポリシー設定を使用して、仮想チャネル許可リストのログ記録レベルを構成できます。

次のオプションが利用可能です。

オプション	説明
無効	すべてのログイベントを無効にします。
警告のみをログに記録	許可リストに含まれていない、開こうとするカスタム仮想チャネルのイベントのみがログに記録されます。
すべてのイベントをログに記録	すべてのイベントがログに記録されます。

仮想チャネル許可リストのログスロットリング

このポリシー設定を使用して、アクティブなセッションのイベントログ記録の頻度を構成できます。

各仮想チャネルのすべてのイベントは、最初に発生したときにログに記録されます。セッションがアクティブな間、スロットリング期間中は繰り返し発生するイベントは抑制されます。セッションが切断された場合、スロットリング期間はリセットされます。

DVC の仮想チャネル許可リスト

ICAセッションで開くことを許可されている動的仮想チャネルを指定する許可リストの使用を有効にします。

無効にすると、すべての動的仮想チャネルが許可されます。

有効にすると、動的仮想チャネルは許可されません。この機能で動的仮想チャネル (DVC) を使用するには、DVC をリストに追加する必要があります。リストにDVCを追加するには、セッションホストでDVCにアクセスするプロセスのパスを入力し、その後にコンマ、次にクライアント側のプラグイン名、その後にコンマ、そしてプラグインが使用するリスナーの名前を入力します。複数のリスナー名をコンマで区切って追加できます。

プラグインがサポートするすべてのリスナーを許可するために、ワイルドカードを使用できます。

プロセスパス内の単一のディレクトリ名、プロセスパス内のディレクトリ名の一部、実行可能ファイルの名前、または実行可能ファイルの名前の一部を置き換えるために、ワイルドカードを使用することもできます。

この設定への変更は、セッションホストを再起動した後にのみ適用されます。

例: クライアント側プラグイン: `DvcPlugin1.dll`, `DvcPlugin2.dll`, `DvcPlugin3.dll`

許可リストエントリ: `C:\Program Files\App\run1.2.exe,DvcPlugin1,` ListenerName1 `C:\Program Files*\run*.exe,DvcPlugin2,ListenerName1,ListenerName2` `C:\Program Files\App\run1.2.exe,DvcPlugin3,*`

視覚表示ポリシー設定

視覚表示セクションには、仮想デスクトップからユーザーデバイスに送信される画像の品質を制御するためのポリシー設定が含まれています。

シンプルなグラフィックの優先色深度

このポリシー設定は、VDAバージョン7.6 FP3以降で利用可能です。8ビットオプションは、VDAバージョン7.12以降で利用可能です。

この設定により、シンプルなグラフィックがネットワーク経由で送信される際の色深度を下げることができます。ピクセルあたり8ビットまたは16ビットに下げることで、低帯域幅接続での応答性が向上する可能性があります。ただし、この操作は画質のわずかな劣化を招く可能性があります。Use video codec for compressionポリシー設定が「**画面全体**」に設定されている場合、8ビットの色深度はサポートされません。

デフォルトの優先色深度はピクセルあたり24ビットです。

8ビット設定がVDAバージョン7.11以前に適用された場合、VDAは24ビット（デフォルト）の色深度にフォールバックします。

ターゲットフレームレート

この設定は、仮想デスクトップからユーザーデバイスに送信される1秒あたりの最大フレーム数を指定します。

デフォルトでは、最大は1秒あたり30フレームです。

1秒あたりのフレーム数を高く設定する（例：30）と、ユーザーエクスペリエンスは向上しますが、より多くの帯域幅が必要になります。1秒あたりのフレーム数を減らす（例：10）と、ユーザーエクスペリエンスを犠牲にしてサーバーのスケーラビリティを最大化します。CPUが遅いユーザーデバイスの場合、ユーザーエクスペリエンスを向上させるために低い値を指定してください。

1秒あたりの最大サポートフレームレートは60です。

視覚品質

この設定は、ユーザーデバイスに表示される画像の希望する視覚品質を指定します。

デフォルトでは、この設定は「中」です。

画像の品質を指定するには、次のいずれかのオプションを選択します。

- **低** - 視覚的な品質を犠牲にしてでも対話性を優先する、帯域幅が制限されたネットワークに推奨されます。
- **中** - ほとんどのユースケースで最高のパフォーマンスと帯域幅効率を提供します。
- **高** - 視覚的にロスレスな画質が必要な場合に推奨されます。
- **ロスレスにビルド** - ネットワークアクティビティが高い期間はロッシー画像をユーザーデバイスに送信し、ネットワークアクティビティが低下した後はロスレス画像を送信します。この設定により、帯域幅が制限されたネットワーク接続でのパフォーマンスが向上します。
- **常にロスレス** - 画像データの保持が不可欠な場合は、「**常にロスレス**」を選択して、ロッシーデータがユーザーデバイスに送信されないようにします。たとえば、画質の低下が許されないX線画像を表示する場合などです。

動画ポリシー設定

動画セクションには、動的イメージの圧縮を削除または変更できる設定が含まれています。

最小画像品質

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、アダプティブディスプレイで許容される最小画像品質を指定します。使用される圧縮が少ないほど、表示される画像の品質は高くなります。超高、非常に高、高、標準、低のいずれかの圧縮を選択します。

デフォルトでは、これは標準に設定されています。

動画圧縮

この設定は、アダプティブディスプレイが有効になっているかどうかを指定します。アダプティブディスプレイは、利用可能な帯域幅に基づいて、スライドショー内のビデオやトランジションスライドの画質を自動的に調整します。アダプティブディスプレイが有効になっている場合、ユーザーは品質を低下させることなく、スムーズに実行されるプレゼンテーションを見ることができます。

デフォルトでは、アダプティブディスプレイは有効になっています。

VDAバージョン7.0から7.6の場合、この設定はレガシーグラフィックモードが有効になっている場合にのみ適用されます。VDAバージョン7.6 FP1以降の場合、この設定はレガシーグラフィックモードが有効になっている場合、またはレガシーグラフィックモードが無効でビデオコーデックがグラフィックの圧縮に使用されていない場合に適用されます。

レガシーグラフィックモードが有効になっている場合、ポリシーの変更を有効にするにはセッションを再起動する必要があります。アダプティブディスプレイはプログレッシブディスプレイと相互排他的です。アダプティブディスプレイを有効にするとプログレッシブディスプレイが無効になり、その逆も同様です。ただし、プログレッシブディスプレイとアダプティブディスプレイの両方を同時に無効にすることもできます。プログレッシブディスプレイはレガシー機能であるため、XenAppまたはXenDesktopでは推奨されません。プログレッシブしきい値レベルを設定すると、アダプティブディスプレイが無効になります。

プログレッシブ圧縮レベル

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定により、詳細度は劣るものの、より高速な初期画像表示が提供されます。

デフォルトでは、プログレッシブ圧縮は適用されません。

通常の非可逆圧縮設定で定義された、より詳細な画像は、利用可能になったときに表示されます。写真などの帯域幅を多く消費するグラフィックの表示を改善するには、非常に高または超高圧縮を使用します。

プログレッシブ圧縮を有効にするには、その圧縮レベルが「ロッシー圧縮レベル」設定よりも高くする必要があります。

注：プログレッシブ圧縮に関連する圧縮レベルの増加は、クライアント接続を介した動的画像の対話性も向上させます。回転する3Dモデルなどの動的画像の品質は、画像が動きを停止するまで一時的に低下し、その時点で通常のロッシー圧縮設定が適用されます。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮しきい値
- プログレッシブヘビーウェイト圧縮

プログレッシブ圧縮しきい値

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、プログレッシブ圧縮が適用される接続の最大帯域幅を1秒あたりのキロビットで表します。これは、この帯域幅以下のクライアント接続にのみ適用されます。

デフォルトでは、しきい値は1秒あたり2147483647キロビットです。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮しきい値
- プログレッシブヘビーウェイト圧縮

目標最小フレームレート

この設定は、低帯域幅の条件下で、動的画像に対してシステムが維持しようとする1秒あたりの最小フレームレートを指定します。

デフォルトでは、これは10fpsに設定されています。

VDAバージョン7.0から7.6の場合、この設定はレガシーグラフィックモードが有効になっている場合にのみ適用されます。VDAバージョン7.6 FP1以降の場合、この設定はレガシーグラフィックモードが無効または有効になっている場合に適用されます。

> **注:**
>
> ターゲット最小フレームレートポリシーは非推奨となり、10 fpsに設定されています。これは、エンドユーザーがグラフィックステータスインジケーターの品質スライダーを使用して変更できます。

静止画像ポリシー設定

静止画像セクションには、静止画像の圧縮を削除または変更できる設定が含まれています。

追加の色圧縮

この設定は、帯域幅が制限されているクライアント接続を介して配信される画像に対する追加の色圧縮の使用を有効または無効にし、表示される画像の品質を低下させることで応答性を向上させます。

デフォルトでは、追加の色圧縮は無効になっています。

有効にすると、追加の色圧縮は、クライアント接続の帯域幅が「追加の色圧縮しきい値」を下回っている場合にのみ適用されます。クライアント接続の帯域幅がしきい値を超えている場合、または「無効」が選択されている場合、追加の色圧縮は適用されません。

追加の色圧縮しきい値

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、追加の色圧縮が適用される接続の最大帯域幅を1秒あたりのキロビット数で表します。クライアント接続の帯域幅が設定値を下回ると、有効になっている場合、追加の色圧縮が適用されます。

デフォルトでは、しきい値は1秒あたり8192キロビットです。

ヘビーウェイト圧縮

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、より高度でCPU負荷の高いグラフィックアルゴリズムを使用することで、画質を損なうことなくプログレッシブ圧縮を超えて帯域幅を削減することを有効または無効にします。

デフォルトでは、ヘビーウェイト圧縮は無効になっています。

有効にすると、ヘビーウェイト圧縮はすべての非可逆圧縮設定に適用されます。Citrix Workspace™アプリでサポートされていますが、他のプラグインには影響しません。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮レベル
- プログレッシブ圧縮しきい値

非可逆圧縮レベル

注：Virtual Delivery Agent 7.x の場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、帯域幅が制限されているクライアント接続を介して配信される画像に使用される非可逆圧縮の度合いを制御します。このような場合、圧縮せずに画像を表示すると遅くなることがあります。

デフォルトでは、中程度の圧縮が選択されています。

帯域幅を多く消費する画像で応答性を向上させるには、高圧縮を使用します。画質の劣化が許容されないX線画像を表示する場合など、画像データの保持が不可欠な場合は、非可逆圧縮を使用しない方がよい場合があります。

関連するポリシー設定：非可逆圧縮しきい値

非可逆圧縮しきい値

注：Virtual Delivery Agent 7.x の場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、非可逆圧縮が適用される接続の最大帯域幅をキロビット/秒で表します。

デフォルトでは、しきい値は2147483647キロビット/秒です。

ポリシーに非可逆圧縮レベル設定を追加し、しきい値を指定しないことで、LAN経由での写真などの高精細ビットマップの表示速度を向上させることができます。

関連するポリシー設定：非可逆圧縮レベル

WebSocketsポリシー設定

WebSocketsセクションには、HTML5向けCitrix Workspace™アプリを使用して仮想デスクトップおよびホスト型アプリケーションにアクセスするためのポリシー設定が含まれています。WebSockets機能は、ブラウザーベースのアプリケーションとサーバー間の双方向通信を行うことで、セキュリティを強化し、オーバーヘッドを削減します。この機能は、複数のHTTP接続を開くことなくこれを行います。

WebSockets接続

この設定では、WebSockets接続を許可または禁止します。

デフォルトでは、WebSocket接続は禁止されています。

WebSocketsポート番号

この設定では、受信WebSocket接続のポートを識別します。

デフォルトでは、値は8008です。

WebSockets信頼済みオリジンサーバーリスト

この設定は、信頼済みオリジンサーバー（通常はWeb向けCitrix Workspaceアプリ）のコンマ区切りリストをURLとして提供します。サーバーは、これらのアドレスのいずれかから発信されたWebSockets接続のみを受け入れます。

デフォルトでは、ワイルドカード * を使用して、すべてのWeb向けCitrix WorkspaceアプリのURLを信頼します。

リストにアドレスを入力する場合は、次の構文を使用します。

\<protocol>://\<ホストの完全修飾ドメイン名>:

プロトコルはHTTPまたはHTTPSである必要があります。ポートが指定されていない場合、HTTPにはポート80が、HTTPSにはポート443が使用されます。

ワイルドカード `*` は、IPアドレスの一部として（`10.105.*.*`）以外は、URL内で使用できます。

レジストリで管理されるHDX™機能

> **注:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。レジストリエディターの使用は、お客様ご自身の責任において行ってください。編集する前に、必ずレジストリをバックアップしてください。

> レジストリエディターを開くには、サーバーで `regedit.exe` を実行します。次に、設定を追加または編集するレジストリキーに移動します。

デバイス

Bloombergキーボード

Citrix Virtual Apps and Desktops™は、Bloombergモデル4およびモデル3のスターボードキーボードをサポートしています。デフォルトでは、拡張Bloombergキーボードのサポートは無効になっています。

Bloombergキーボードのサポートを有効にするには、接続を開始する前にクライアントマシンで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB`
- **値の名前**: `EnableBloombergHID`
- **値の型**: `DWORD`
- **値のデータ**:
  - `0` - 無効
  - `1` - 有効

詳しくは、「Bloombergキーボード」を参照してください。

マップされたクライアントドライブ

セキュリティ上の予防措置として、ユーザーがCitrix Virtual Apps™ and Desktopsにログオンすると、サーバーはデフォルトで、ユーザーの実行権限なしにクライアントドライブをマップします。マップされたクライアントドライブに存在する実行可能ファイルをユーザーが実行できるようにするには、サーバーのレジストリを編集して、このデフォルト設定を上書きします。

アクセスを許可するには、次のレジストリ値を編集します (**CDMSettings**が存在しない場合は作成します)。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\CDMSettings`
- **値の名前**: `ExecuteFromMappedDrive`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 権限を許可
  - `0` - マップされたドライブでの権限を拒否

この変更は、レジストリを編集した後に接続されたセッションに適用されます。

Citrix Virtual Apps and Desktops 7 2006は、このレジストリの場所を含む最初のバージョンです。以前のバージョンのCitrix Virtual Apps and Desktopsでは、異なるレジストリの場所が使用されていました。

詳しくは、「クライアントドライブマッピング」を参照してください。

マイクロソフト サーフェス プロ および サーフェス ブック ペン

Citrix Virtual Apps and Desktopsは、Windows Inkベースのアプリケーションで標準のペン機能をサポートしています。デフォルトでは、この機能は有効になっています。

この機能を無効または有効にするには、次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent\PenApi`
- **値の名前**: `DisablePen`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 無効
  - `0` - 有効

詳細については、「Microsoft Surface Pro および Surface Book ペン」を参照してください(/ja-jp/citrix-virtual-apps-desktops/2511/devices/mobile-devices.html#microsoft-surface-pro-and-surface-book-pens)。

Windows イメージ取得アプリケーション許可リスト

この設定により、VDA 上のどのアプリケーションが Windows イメージ取得スキャナーリダイレクトにアクセスできるかを制御できます。

デフォルトでは、どのアプリケーションも Windows イメージ取得にアクセスできません。

VDA 上のアプリケーションに対して Windows イメージ取得を調整するには、次のレジストリ設定を作成します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`
- **値の名前**: `WIAAllowedProcesses`

  WIAAllowedProcesses を選択して右クリックします。「**新規 > 複数行文字列値**」を選択し、新しい値の名前を **AllowProcesses** に変更します。
- 値のデータ: Windows イメージ取得にアクセスできる各アプリケーションの完全なパスとプロセス名を入力します。各アプリケーションは新しい行に入力してください。

この設定への変更は、VDAでセッションを次回起動したときに有効になります。

全般

HDX リデューサー

セッションホストで使用するHDX圧縮アルゴリズム（Reducer）のバージョンを構成できます。

シングルセッションVDAでReducer V4を有効にするには、次のレジストリ値を設定します。

キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\WDSettings` **値の名前**: `ReducerOverrideMask` **値の型**: `DWORD` **値のデータ**: `23` (10進数)

マルチセッションVDAでReducer V4を有効にするには、次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **値の名前**: `ReducerOverrideMask`
- **値の型**: `DWORD`
- **値のデータ**: `23` (10進数)

Rendezvousバージョンの構成

使用するRendezvousのバージョンを構成するには、次のレジストリ値を設定します:

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`
- **値の型**: `DWORD`
- **値の名前**: `GctRegistration`
- **値のデータ**:
  - `1` - V2を有効にする
  - `0` - V1を有効にする

VDAへの自動ログオンを構成する

この設定により、Windows 10シングルセッションOSおよびマルチセッションOSのVDAで、Microsoftポリシー設定の**常にパスワードを要求する**を有効または無効にできます。

もし**常にパスワードを要求する**が有効になっている場合、ユーザーはリモートセッションを開始するときにVDAで資格情報を入力する必要があります。この設定が無効になっている場合、ユーザーはVDAで資格情報を提供することなく、自動的にリモートセッションに接続します。

デフォルトでは、Microsoftポリシー設定は無効になっています。**常にパスワードを要求する**設定を有効または無効にするには、VDAで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Portica`
- **値の名前**: `AutoLogon`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - Microsoftポリシー設定を無効にし、ユーザーがリモートセッションに自動的にサインインできるようにします。
  - `0` – Microsoftポリシー設定を有効にし、ユーザーがリモートセッションを起動するときに資格情報の入力を求めます。

タイムアウト警告を無効にする

デフォルトでは、非アクティブまたはアイドル状態のセッションを持つユーザーは、セッションが自動的に切断される2分前に警告メッセージを受け取ります。

この設定は、以下のアイドルセッションタイムアウト制限に達したユーザーに対する警告メッセージを無効にし、削除します。

- ウィンドウズ サーバー 2004
- Windows 10 マルチセッション 2004 またはそれ以降のマルチセッションOS

警告を削除するには、VDAで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\ICA-CGP`
- **値の名前**: `fEnableTimeoutWarning`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 警告メッセージを無効にする
  - `0` - 警告メッセージを有効にする

警告メッセージを表示するには、レジストリ値を削除するか、`0`に設定します。

EDT MTU検出

MTU検出により、EDTはセッション確立時に最大転送単位（MTU）を自動的に決定できます。これにより、パフォーマンスの低下やセッション確立の失敗につながる可能性のあるEDTパケットの断片化を防ぎます。

この設定はデフォルトで有効になっています。EDT MTU検出を無効にするには、次のレジストリ値を構成し、セッションホストを再起動します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **値の名前**: `MtuDiscovery`
- **値の型**: `DWORD`
- **値のデータ**: `0`

MTU Rediscovery を有効にするには、以下のレジストリ値を構成し、セッションホストを再起動します。

- **キー:** `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\MtuRediscovery`
- **値の名前:** `MtuReDiscovery`
- **値の型:** `DWORD`
- **値のデータ:** `1`
- **キー:** `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\MtuRediscovery`
- **値の名前:** `MtuReDiscoveryFrequency`
- **値の型:** `DWORD`
- **値のデータ:** `1`

これらの設定はマシン全体に適用され、サポートされているクライアントから接続するすべてのセッションに影響します。

EDT タイムアウト

VDAのEDTタイムアウトは5秒から25秒の任意の値に設定できます。デフォルトのEDTタイムアウト値は10秒です。

- **キー**: `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\Tds\udp\UDPStackParameters`

- **値の型**: `DWORD`
- **値の名前**: `edtConnectionTimeout`
- **値のデータ**: 5〜25秒（10進数）

Citrix Workspaceアプリ for Windows バージョン2409.10以前の場合、EDTタイムアウトは次のように設定することもできます。

- **キー**: `HKLM\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\EDT`
- **値の型**: `String / REG_SZ`
- **値の名前**: `edtConnectionTimeout`
- **値のデータ**: 5〜25秒（10進数）

> **注:**
>
> バージョン2503以降のCitrix Workspaceアプリでは、VDAからのタイムアウト設定が使用されるため、クライアントデバイスでタイムアウトを設定する必要がなくなります。

一般的なコンテンツリダイレクト

ホストからクライアントへのリダイレクトにURLタイプを追加する

デフォルトでは、HTTP、HTTPS、RTSP、RTSPU、PNM、MMSのURLタイプのリダイレクトをサポートしています。Windowsクライアントで以下のレジストリキーと値を作成することで、URLタイプをリストに追加できます。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA`
- **値の名前**: `ExtraURLProtocols`
- **値の型**: `REG_SZ`
- **値のデータ**: 必要なURLタイプをセミコロンで区切って指定します。URLの権限部分より前のすべてを含めます。例: `ftp://;mailto:;customtype1://;custometype2://`

URLタイプはWindowsクライアントにのみ追加できます。このレジストリ設定がないクライアントは、Citrixセッションへのリダイレクトを拒否します。クライアントには、指定されたURLタイプを処理するようにインストールおよび構成されたアプリケーションが必要です。

詳細については、ホストからクライアントへのリダイレクトを参照してください。

クライアントフォルダーリダイレクト

クライアントフォルダーリダイレクトは、クライアント側のファイルがホスト側のセッションでアクセス可能になる方法を変更します。サーバーでクライアントフォルダーリダイレクトを有効にし、ユーザーがユーザーデバイスでそれを構成するとします。この場合、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

サーバーでクライアントフォルダーリダイレクトを有効にするには、次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection`
- **値の名前**: `CFROnlyModeAvailable`
- **値の型**: `DWORD`
- **値のデータ**: `1`

詳細については、クライアントフォルダーリダイレクトを参照してください。

特定のWebサイトセットに対するホストからクライアントへのリダイレクト

特定のWebサイトセットに対してホストからクライアントへのリダイレクトを有効にするには、サーバーVDAで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- **値の名前**: `ValidSites`
- **値の型**: `REG_MULTI_SZ`
- **値のデータ**: 完全修飾ドメイン名 (FQDN) の任意の組み合わせを指定します。複数のFQDNは別々の行に入力します。プロトコル (`http://` または `https://`) なしでFQDNのみを含めます。FQDNには、ワイルドカード文字としてアスタリスク (`*`) を左端の位置にのみ含めることができます。このワイルドカードは、RFC 6125のルールと一致する単一レベルのドメインに一致します。例:

`www.example.com`

`*.example.com`

詳細については、「ホストからクライアントへのリダイレクト」を参照してください。

ログオフ時および切断時のローカルアプリケーションの動作

デフォルトでは、ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは実行を継続します。再接続後、ローカルアプリケーションが仮想デスクトップで利用可能な場合、それらは再統合されます。ログオフ時および切断時のローカルアプリケーションの動作を構成するには、ホストされているデスクトップで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies`
- **値の名前**: `Session State`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは実行を継続します。再接続後、ローカルアプリケーションが仮想デスクトップで利用可能な場合、それらは再統合されます。
  - `3` - ユーザーが仮想デスクトップからログオフまたは切断すると、ローカルアプリケーションが閉じます。

詳細については、「ローカルアプリアクセスとURLリダイレクト」(/ja-jp/citrix-virtual-apps-desktops/2511/general-content-redirection/laa-url-redirect.html)を参照してください。

ホストからクライアントへのリダイレクトのデフォルトリストからURLタイプを削除する

デフォルトのリダイレクトリストからURLタイプを削除するには、サーバーVDAで以下のレジストリキーと値を作成します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- **値の名前**: `DisableServerFTA`
- **値の型**: `DWORD`
- **値のデータ**: `1`
- **値の名前**: `NoRedirectClasses`
- **値の型**: `REG_MULTI_SZ`
- **値のデータ**: `http`、`https`、`rtsp`、`rtspu`、`pnm`、または`mms`のいずれかの値を組み合わせて指定します。複数の値を入力する場合は、別々の行に入力します。例:

```
http
```

```
https
```

`rtsp`

詳細については、「ホストからクライアントへのリダイレクト」(/ja-jp/citrix-virtual-apps-desktops/2511/general-content-redirection/bidirectional-content-redirection-configuration/host-to-client-redirection.html)を参照してください。

サーバーVDAのデフォルトブラウザ構成

ホストからクライアントへのリダイレクトを有効にすると、Server VDA のデフォルトのブラウザ設定を上書きできます。Web URL がリダイレクトされない場合、Citrix ランチャーは `command_backup` レジストリキーで構成されているブラウザに URL を渡します。このキーはデフォルトで Internet Explorer を指していますが、別のブラウザへのパスを含むように変更できます。

- Internet Explorer (デフォルト)
  - **キー**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"c:\program files\internet explorer\iexplore.exe" "%1"`
  - **キー**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"c:\program files\internet explorer\iexplore.exe" "%1"`
- グーグル クローム
  - **キー**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "%1"`
  - **キー**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "%1"`

- マイクロソフト Edge
  - **キー**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "%1"`
  - **キー**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "%1"`

公開アプリケーションのローカルアプリアクセス

ローカルアプリアクセスは、ローカルにインストールされたWindowsアプリケーションを、デスクトップを切り替えることなくホストされたデスクトップ環境にシームレスに統合します。公開アプリケーションへのアクセスを提供するには、サーバーで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio`
- **値の名前**: `ClientHostedAppsEnabled`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 有効
  - `0` - 無効

詳しくは、「ローカルアプリアクセスとURLリダイレクト」を参照してください。

グラフィック

CUDAまたはOpenCLアプリケーションのGPUアクセラレーション

ユーザーセッションで実行されているCUDAおよびOpenCLアプリケーションのGPUアクセラレーションは、デフォルトで無効になっています。

CUDAアクセラレーションのPOC機能を使用するには、次のレジストリ設定を有効にします。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- **値の名前**: `CUDA`
- **値の型**: `DWORD`
- **値のデータ**: `00000001`

OpenCLアクセラレーションのPOC機能を使用するには、次のレジストリ設定を有効にします。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- **値の名前**: `OpenCL`
- **値の型**: `DWORD`
- **値のデータ**: `00000001`

詳細については、WindowsマルチセッションOSのGPUアクセラレーションを参照してください。

プログレッシブモード

プログレッシブモードはデフォルトで無効になっています。次のレジストリ値でプログレッシブモードの状態を変更できます:

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics`
- **値の型**: `REG_DWORD`
- **値の名前**: `ProgressiveDisplay`
- **値のデータ**:
  - `0` - 常にオフ (プログレッシブモードを無効にします。この値がデフォルトです。)
  - `1` - 自動 (ネットワークの状態に基づいて切り替えます。)
  - 2 = 常にオン

詳細については、プログレッシブモードを参照してください。

> **注:**

> プログレッシブモードは非推奨になりました。Thinwireは、画像の配信を最適化し、キャッシュ効率を維持しながら、プログレッシブモードのほぼすべての利点を提供する代替オプションです。

Windows Presentation Foundation (WPF) レンダリング

HDX 3D Proを使用すると、WindowsマルチセッションOSセッションで実行されているグラフィックを多用するアプリケーションを、サーバーのグラフィック処理ユニット (GPU) でレンダリングできます。Windows Presentation Foundation (WPF) のレンダリングをサーバーのGPUに移行することで、グラフィックレンダリングがサーバーのCPUを遅くすることはありません。

サーバーのGPUを使用してWPFアプリケーションのレンダリングを有効にするには、WindowsマルチセッションOSを実行しているサーバーのレジストリに次の設定を作成します。

1. VDA上でレジストリエディターを開き、次のキーに移動します。

   ```
   HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper
   ```

2. 次のレジストリ値を作成または編集します。

   - AdapterHandle = 0x00000001
   - DevicePath = 0x00000001
   - フラグ = 0x00000412
   - WPF = 0x00000001

3. WPFアプリの実行可能ファイル名でサブキーを作成します。たとえば、アプリが「mywpfapp.exe」という名前の場合、次のキーを作成します。

   ```
   HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper\mywpfapp.exe
   ```

4. 設定を有効にするには、サーバーを再起動します。

詳細については、「WindowsマルチセッションOS向けGPUアクセラレーション」および「WindowsマルチセッションOSでWPFアプリを最大限に活用する」のブログを参照してください。

マルチメディア

マルチメディア会議中のエコーを回避する

Citrix Virtual Apps and Desktopsは、エコーを最小限に抑えるエコーキャンセルオプションを提供します。この機能はデフォルトで有効になっています。エコーキャンセルを無効にするには、次のいずれかのレジストリ設定を変更できます。

- **キー**:
  - 32ビット: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
  - 64ビット: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
- **値の名前**: `EchoCancellation`
- **値の型**: `String/REG_SZ`
- **値のデータ**: `False`

詳細については、オーディオ機能を参照してください。

オーディオの制限

クライアントにオーディオデバイスをインストールし、オーディオリダイレクトを有効にしてRDSセッションを開始した後、オーディオファイルが再生されない場合があります。回避策として、RDSマシンに以下のレジストリキーを追加し、マシンを再起動してください。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig`
- **値の名前**: `EnableSvchostMitigationPolicy`
- **値の型**: `DWORD`
- **値のデータ**: `0`

詳細については、オーディオ機能を参照してください。

高解像度Webカメラの解像度

メディアタイプのネゴシエーションが失敗した場合、HDXはデフォルトのVGA解像度（640 x 480ピクセル）にフォールバックします。クライアント上のレジストリキーを使用して、デフォルトの解像度を構成できます。次のレジストリキーを設定する前に、カメラが指定された解像度をサポートしていることを確認してください。

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- 幅
  - **値の名前**: `DefaultWidth`
  - **値の型**: `DWORD`
  - **値のデータ**: 10進数で指定する希望の幅（例: 1280）
- 高さ

- **値の名前**: `DefaultHeight`
- **値の型**: `DWORD`
- **値のデータ**: 10進数で指定する高さ (例: 720)

Microsoft Teams フォールバックモード

Microsoft Teamsが最適化されたVDIモードでロードに失敗した場合 (Teams/バージョン情報/バージョンで「Citrix HDX Not Connected」と表示される場合)、VDAはウェブカメラのリダイレクトやクライアントのオーディオおよびマイクのリダイレクトなど、レガシーHDXテクノロジーにフォールバックします。Microsoft Teamsの最適化をサポートしないWorkspaceアプリのバージョン/プラットフォームOSを使用している場合、フォールバックレジストリキーは適用されません。

フォールバックメカニズムを制御するには、VDA上で以下のいずれかのレジストリ値を設定します。

- **キー** (いずれか1つのみ必要):
  - **コンピューター設定:** `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams`
  - **ユーザー設定:** `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Teams`
- **値の名前**: `DisableFallback`
- **値の型**: `DWORD`
- 値のデータ:
  - `1` - フォールバックモードを無効にする
  - `2` - オーディオのみを有効にする

値が存在しないか、0に設定されている場合、フォールバックモードが有効になります。この機能には、Microsoft Teamsバージョン1.3.0.13565以降が必要です。詳細については、「Microsoft Teamsの最適化」を参照してください。

Citrix App Layering™ を使用したMicrosoft Teamsの最適化

Citrix App Layeringを使用してVDAとMicrosoft Teamsのインストールを異なるレイヤーで管理している場合は、コマンドラインから`ALLUSER=1`フラグを使用してMicrosoft Teamsをインストールする前に、Windows上に**PortICA**という名前の空のレジストリキーを作成します。デフォルトの値の名前、型、およびデータはそのままにします。

- レジストリエディターの32ビット版のキー:
  `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA`

- レジストリエディターの64ビット版のキー:
  `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

詳細については、「Microsoft Teamsの最適化」を参照してください。

Webカメラのソフトウェア圧縮

Webカメラがハードウェアエンコードをサポートしている場合、HDXビデオ圧縮はデフォルトでハードウェアエンコードを使用します。ハードウェアエンコードは、ソフトウェアエンコードよりも多くの帯域幅を消費する可能性があります。ソフトウェア圧縮を強制するには、クライアントに次の値を追加します。

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HdxRealTime`
- **値の名前**: `DeepCompress_ForceSWEncode`
- **値の型**: `DWORD`
- **値のデータ**: `1`

詳細については、HDX webcam video compressionを参照してください。

Webカメラビデオ圧縮

HDX Webカメラビデオ圧縮は、H.264ビデオを仮想セッションで実行されているビデオ会議アプリケーションに直接送信します。VDAリソースを最適化するために、HDX Webカメラ圧縮はWebカメラビデオのエンコード、トランスコード、デコードを行いません。この機能はデフォルトで有効になっています。

サーバーからビデオ会議アプリへの直接ビデオストリーミングを無効にするには、VDAで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime`
- **値の名前**: `OfferH264ToApp`
- **値の型**: `DWORD`
- **値のデータ**: `0`

詳細については、HDX webcam video compressionを参照してください。

Webカメラビデオ圧縮フレームレート

優先するビデオフレームレートを調整するには、クライアントで次のレジストリ値を編集します。

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- **値の名前**: `FramesPerSecond`

- **値の型**: `DWORD`
- **値のデータ**: `15`

ウェブカメラが指定されたフレームレートをサポートしていない場合、アプリケーションはデフォルトで15 FPSを使用します。

詳細については、HDXウェブカメラビデオ圧縮を参照してください。

負荷管理ポリシー設定

負荷管理セクションには、WindowsマルチセッションOSマシンを提供するサーバー間の負荷管理を有効にし、構成するためのポリシー設定が含まれています。

負荷評価インデックスの計算については、CTX202150を参照してください。

同時ログオン許容数

この設定は、サーバーが受け入れ可能な同時ログオンの最大数を指定します。

デフォルトでは、この値は2に設定されています。

この設定が有効な場合、負荷分散は、指定された数を超えるログオンが同時にサーバーVDAでアクティブにならないように試みます。ただし、この制限は厳密には適用されません。制限を適用し（指定された数を超える同時ログオンを失敗させる）、次のレジストリキーを作成します。

> HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit 種類: DWORD 値: 1

CPU使用率

この設定は、サーバーがフルロードを報告するCPU使用率のレベルをパーセンテージで指定します。有効にすると、サーバーがフルロードを報告するデフォルト値は90%です。

デフォルトでは、この設定は無効になっており、CPU使用率は負荷計算から除外されます。

CPU使用率から除外されるプロセスの優先度

> **注：**

> Workspace Environment Managementがマシンを管理するシナリオでは、この設定をCPU Priority設定と併用すると、予期しない結果が生じる可能性があります。CPU Priority設定を使用することを選択した場合は、この設定を無効にすることをお勧めします。

> この設定は、プロセスのCPU使用率がCPU使用率負荷インデックスから除外される優先度レベルを指定します。

既定では、この値は**通常以下**または**低**に設定されています。

ディスク使用量

この設定は、サーバーが75%のフルロードを報告するディスクキューの長さを指定します。有効にすると、ディスクキューの既定値は8です。

デフォルトでは、この設定は無効になっており、ディスク使用率は負荷計算から除外されます。

セッションの最大数

この設定は、サーバーがホストできるセッションの最大数を指定します。有効にすると、サーバーがホストできるセッションの最大数のデフォルト設定は250になります。

デフォルトでは、この設定は有効になっています。

メモリ使用量

この設定は、サーバーがフルロードを報告するメモリ使用量のレベルをパーセンテージで指定します。有効にすると、サーバーがフルロードを報告する既定値は90%です。

デフォルトでは、この設定は無効になっており、メモリ使用量は負荷計算から除外されます。

メモリ使用量のベースロード

この設定は、ベースオペレーティングシステムのメモリ使用量の近似値を指定します。また、サーバーがゼロ負荷と見なされるメモリ使用量（MB単位）を定義します。

デフォルトでは、この値は768 MBに設定されています。

プロファイル管理ポリシー設定

高度なポリシー設定

ロックされたファイルへのアクセス時の再試行回数

ロックされたファイルへのアクセス時の再試行回数を設定します。

このポリシーが無効になっている場合、デフォルト値の5回の再試行が使用されます。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、デフォルト値が使用されます。

ログオフ時にインターネットCookieファイルを処理する

一部の展開では、`Index.dat`が参照しない余分なインターネットCookieが残されます。継続的なブラウジングの後にファイルシステムに残された余分なCookieは、プロファイルの肥大化につながる可能性があります。このポリシーを使用すると、Profile Managementを有効にしてIndex.datの処理を強制し、余分なCookieを削除できます。このポリシーはログオフ時間を増加させるため、この問題が発生した場合にのみ有効にしてください。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、Index.datの処理は行われません。

自動構成を無効にする

Profile Managementは、Citrix Virtual Desktops™環境（パーソナルvDiskの有無など）を検査し、それに応じてグループポリシーを構成します。「未構成」状態のProfile Managementポリシーのみが調整されるため、行ったカスタマイズはすべて保持されます。

このポリシーにより、展開を高速化し、最適化を簡素化できます。このポリシーを構成する必要はありません。ただし、次のいずれかの操作を行う場合は、自動構成を無効にできます。

- 以前のバージョンからの設定を保持するためにアップグレードする
- トラブルシューティング

自動構成は、実行時に環境に応じてデフォルトのポリシー設定を自動的に構成する動的な構成チェッカーと見なすことができます。これにより、設定を手動で構成する必要がなくなります。実行時環境には以下が含まれます。

- ウィンドウズ OS
- Windows OS のバージョン
- シトリックス バーチャル デスクトップの存在
- パーソナルvDisk の有無

環境が変更された場合、自動構成によって以下のポリシーが変更される可能性があります。

- アクティブライトバック
- 常にキャッシュ
- ログオフ時にローカルにキャッシュされたプロファイルを削除
- キャッシュされたプロファイルを削除するまでの遅延

- プロファイルストリーミング

異なるOSでのポリシーのデフォルトステータスについては、以下の表を参照してください。

	マルチセッションOS	シングルセッションOS
アクティブライトバック	有効	Personal vDisk が使用されている場合は *無効*。それ以外の場合は有効。
常にキャッシュ	無効	Personal vDisk が使用されている場合は *無効*。それ以外の場合は有効。
ログオフ時にローカルにキャッシュされたプロファイルを削除	有効	以下のいずれかの状況が発生した場合は *無効* です: Personal vDisk が使用されている、Citrix Virtual Desktops が割り当てられている、または Citrix Virtual Desktops がインストールされていない。それ以外の場合は有効。
キャッシュされたプロファイルを削除するまでの遅延	0秒	ユーザーの変更が永続的でない場合は60秒。それ以外の場合は0秒。
プロファイルストリーミング	有効	Personal vDisk が使用されている場合は *無効*。それ以外の場合は有効。

ただし、自動構成が無効になっている場合、上記のすべてのポリシーはデフォルトで **無効** になります。

> **重要:**
>
> Personal vDiskは非推奨です。詳細については、PVD、AppDisk、およびサポートされていないホストの削除を参照してください。

> Profile Management 1909以降、Windows 10（バージョン1607以降）のスタートメニューで改善されたエクスペリエンスを得ることができます。この改善は、以下のポリシーの自動構成によって実現されます。

- `Appdata\Local\Microsoft\Windows\Caches`と`Appdata\Local\Packages`を**ミラーリングするフォルダー**に追加します。
- `Appdata\Local\Microsoft\Windows\UsrClass.Dat*`を**同期するファイル**に追加します。

構成の優先順位:

1. この設定がここで構成されていない場合、.iniファイルの値が使用されます。
2. この設定がここでも .ini ファイルでも構成されていない場合、自動構成が有効になります。この場合、環境が変更されると Profile Management の設定も変更される可能性があります。

問題が発生した場合にユーザーをログオフする

問題が発生した場合に Profile Management がユーザーをログオフさせるかどうかを指定できます。

このポリシーが無効になっているか、構成されていない場合、問題が発生すると Profile Management はユーザーに一時プロファイルを提供します。たとえば、ユーザー ストアが利用できない場合などです。

有効になっている場合、エラーメッセージが表示され、ユーザーはログオフされます。この設定により、問題のトラブルシューティングが簡素化されます。

構成の優先順位:

1. この設定がここで構成されていない場合、.ini ファイルの値が使用されます。
2. この設定がここでも .ini ファイルでも構成されていない場合、一時プロファイルが提供されます。

カスタマー エクスペリエンス向上プログラム

デフォルトでは、匿名統計と使用状況データを収集することで、Citrix®製品の品質とパフォーマンスを向上させるために、カスタマーエクスペリエンス向上プログラムが有効になっています。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

Outlookの検索インデックスローミングを有効にする

ユーザープロファイルとともにOutlook検索データを自動的にローミングすることで、ユーザーベースのOutlook検索エクスペリエンスを許可します。この機能には、Outlookの検索インデックスを保存するために、ユーザー ストアに追加のスペースが必要です。

このポリシーを有効にするには、ログオフしてから再度ログオンしてください。

Outlook 検索インデックス データベース – バックアップと復元

「Outlookの検索インデックスローミングを有効にする」ポリシーが有効になっている場合に、ログオン中にProfile Managementが何を行うかを指定できます。

このポリシーが有効になっている場合、Profile Managementは、ログオン時にデータベースが正常にマウントされるたびに検索インデックスデータベースをバックアップします。Profile Managementは、このバックアップを検索インデックスデータベースの良好なコピーとして扱います。データベースの破損により検索インデックスデータベースのマウント試行が失敗した場合、Profile Managementは検索インデックスデータベースを最後に認識された良好なコピーに戻します。

> 注:
>
> 新しいバックアップが正常に保存されると、Profile Managementは以前に保存されたバックアップを削除します。バックアップは利用可能なVHDXストレージを消費します。

OUTLOOK検索データローミングの同時セッションサポートを有効にする

Profile Managementが、同じユーザーの同時セッションでネイティブのOutlook検索エクスペリエンスを提供できるようにします。このポリシーは、「Outlookの検索インデックスローミング」ポリシーと組み合わせて使用します。

このポリシーが有効な場合、各同時セッションは個別のOutlook OSTファイルを使用します。

デフォルトでは、Outlook OSTファイルを保存するために使用できるVHDXディスクは2つのみです（ディスクごとに1ファイル）。ユーザーがさらにセッションを開始すると、Outlook OSTファイルはローカルユーザープロファイルに保存されます。Outlook OSTファイルを保存するためのVHDXディスクの最大数を指定できます。

ONEDRIVEコンテナを有効にする

OneDriveフォルダーをユーザーとともにローミングできるようにします。

OneDriveコンテナは、VHDXベースのフォルダーローミングソリューションです。Profile Managementは、ファイル共有上にユーザーごとにVHDXファイルを作成し、ユーザーのOneDriveフォルダーをVHDXファイルに保存します。VHDXファイルは、ユーザーがログオンするときにアタッチされ、ログオフするときにデタッチされます。

UWPアプリのローミング

UWP (Universal Windows Platform) アプリをユーザーとともにローミングできるようにします。その結果、ユーザーは異なるデバイスから同じUWPアプリにアクセスできます。

このポリシーが有効な場合、Profile ManagementはUWPアプリを個別のVHDXディスクに保存することで、ユーザーとともにローミングできるようにします。これらのディスクは、ユーザーのログオン中にアタッチされ、ログオフ中にデタッチされます。

構成の優先順位:

1. この設定がここで構成されていない場合、.iniファイルの値が使用されます。
2. この設定がここでも.iniファイルでも構成されていない場合、この機能は無効になります。

UWPアプリのロード高速化を有効にする

UWPアプリの読み込み高速化を有効にします。これにより、UWPアプリの読み込みを高速化し、非永続環境での一貫性を向上させることができます。デフォルトでは、WindowsはUWPアプリの登録情報を各マシンにローカルに保存しますが、これは非永続環境での再起動時に失われる可能性があります。このポリシーを有効にすると、Profile Managementは各マシン用にVHDXコンテナを作成してUWPアプリの登録データを保存し、ユーザーログオンを高速化し、再起動時のデータ損失を防ぎます。

構成の優先順位:

1. この設定がGPO、Studio、またはWorkspace Experience Management (WEM) を使用して構成されていない場合、.iniファイルの値が使用されます。
2. この設定がどこにも構成されていない場合、この機能は無効になります。

ログオン時のユーザーグループポリシーの非同期処理を有効にする

Windowsは、ユーザーグループポリシーに同期モードと非同期モードの2つの処理モードを提供します。Windowsは、次回のユーザーログオンの処理モードを決定するためにレジストリ値を使用します。レジストリ値が存在しない場合、同期モードが適用されます。レジストリ値はマシンレベルの設定であり、ユーザーとともにローミングしません。したがって、ユーザーが次の場合、非同期モードは期待どおりに適用されません。

- 異なるマシンにログオンする。

- ログオフ時にローカルにキャッシュされたプロファイルを削除するポリシーが有効になっている同じマシンにログオンする。

このポリシーを有効にすると、レジストリ値はユーザーとともにローミングされます。その結果、ユーザーがログオンするたびに処理モードが適用されます。

VHDディスクの圧縮をトリガーする空き領域の比率

VHDディスクの圧縮を有効にする が有効な場合に適用されます。VHDディスクの圧縮をトリガーする空き領域の比率を指定できます。ユーザーがログオフするときに空き領域の比率が指定された値を超えると、ディスクの圧縮がトリガーされます。

空き領域の比率 = (現在のVHDファイルサイズ – 必要な最小VHDファイルサイズ*) ÷ 現在のVHDファイルサイズ

* Microsoft Windowsオペレーティングシステムの `MSFT_Partition` クラスのGetSupportedSizeメソッドを使用して取得されます。

VHDディスクの圧縮をトリガーするログオフ回数

VHDディスクの圧縮を有効にする が有効な場合に適用されます。VHDディスクの圧縮をトリガーするユーザーログオフの回数を指定できます。

前回の圧縮からのログオフ回数が指定された値に達すると、ディスクの圧縮が再度トリガーされます。

VHDディスクの圧縮のデフラグを無効にする

VHDディスクの圧縮を有効にする が有効な場合に適用されます。VHDディスクの圧縮のファイルデフラグを無効にするかどうかを指定できます。

VHDディスクの圧縮が有効になっている場合、VHDディスクファイルはまずWindowsに組み込まれている `defrag` ツールを使用して自動的にデフラグされ、その後圧縮されます。VHDディスクのデフラグはより良い圧縮結果をもたらしますが、無効にするとシステムリソースを節約できます。

プロファイルコンテナのマルチセッションライトバックを有効にする

マルチセッションシナリオでプロファイルコンテナのライトバックを有効にします。有効にすると、すべてのセッションでの変更がプロファイルコンテナに書き戻されます。そうでない場合、プロファイルコンテナでは最初のセッションのみが読み取り/書き込みモードであるため、最初のセッションでの変更のみが保存されます。Citrix Profile Managementプロファイルコンテナは Citrix Profile Management 2103以降でサポートされています。FSLogix Profile ContainerはCitrix Profile Management 2003以降でサポートされています。

FSLogix Profile Containerでこのポリシーを使用するには、以下の前提条件が満たされていることを確認してください。

- FSLogix Profile Container 機能がインストールされ、有効になっていること。
- FSLogix でプロファイルの種類が **読み取り/書き込みプロファイルを試行し、読み取り専用にフォールバックする** に設定されていること。

ユーザー ストアのレプリケート

リモートユーザープロファイルストアを、ログオンおよびログオフごとに複数のパスにレプリケートできます。これにより、Profile Management はユーザーログオンのプロファイル冗長性を提供できます。

このポリシーを有効にすると、システムI/Oが増加し、ログオフ時間が長くなる可能性があります。

> **注:**
>
> この機能は、ファイルベースとコンテナベースの両方のプロファイルソリューションで利用できます。

ユーザーストアへの資格情報ベースのアクセスを有効にする

デフォルトでは、Citrix Profile Management は現在のユーザーを偽装してユーザー ストアにアクセスします。Profile Management がユーザー ストアにアクセスする際に現在のユーザーを偽装しないようにする場合は、この機能を有効にします。現在のユーザーがアクセス権を持たないストレージリポジトリ（Azure Files など）にユーザー ストアを配置できます。

Profile Management がユーザー ストアにアクセスできるようにするには、プロファイルストレージサーバーの資格情報を Workspace Environment Management™ (WEM) または Windows 資格情報マネージャーに保存します。Profile Management が実行される各マシンで同じ資格情報を構成する必要をなくすために、Workspace Environment Management を使用することをお勧めします。Windows 資格情報マネージャーを使用する場合は、ローカルシステムアカウントを使用して資格情報を安全に保存してください。

> **注:**

> このポリシーは、ファイルベースとVHDXベースの両方のユーザー ストアで利用できます。Profile Management のバージョン2212より前では、このポリシーはVHDXベースのユーザー ストアでのみ利用できます。

> 構成の優先順位：

1. ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。
2. この設定がここまたは.iniファイルで構成されていない場合、デフォルトで無効になります。

VHDXファイルのストレージパスをカスタマイズする

Profile Managementは、以下のVHDXベースのポリシーを提供します: プロファイルコンテナ、Outlookの検索インデックスローミング、およびフォルダミラーリングの高速化。デフォルトでは、VHDXファイルはユーザーストアに保存されます。このポリシーを使用すると、それらを保存するための別のパスを指定できます。

VHDコンテナのデフォルト容量

VHDコンテナのデフォルトのストレージ容量（GB単位）を指定できます。

構成の優先順位:

1. ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。
2. ここで、または .ini ファイルでこの設定が構成されていない場合、デフォルトで無効になります。

VHDX ファイルのストレージ パスをカスタマイズする

Profile Management は、プロファイル コンテナー、Outlook の検索インデックス ローミング、フォルダー ミラーリングの高速化といった VHDX ベースのポリシーを提供します。デフォルトでは、VHDX ファイルはユーザー ストアに保存されます。このポリシーを使用すると、それらを保存する別のパスを指定できます。

VHD コンテナーのデフォルト容量

VHD コンテナーのデフォルトのストレージ容量 (GB 単位) を指定できます。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。
2. ここで、または .ini ファイルでこのポリシーが構成されていない場合、デフォルトは 50 (GB) です。

セッションで VHDX ディスクを自動的に再アタッチする

このポリシーを有効にすると、Profile Management は VHDX ベースのポリシーの高い安定性を確保します。デフォルトでは、このポリシーは有効になっています。

このポリシーが有効になっている場合、Profile Management は VHDX ベースのポリシーで使用されている VHDX ディスクを監視します。いずれかのディスクがデタッチされた場合、Profile Management はそのディスクを自動的に再アタッチします。

プロファイルコンテナの自動拡張しきい値

プロファイルコンテナが自動拡張をトリガーするストレージ容量の使用率を指定できます。

構成の優先順位:

- このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここまたは.iniファイルで構成されていない場合、デフォルトはストレージ容量の90%です。

プロファイルコンテナの自動拡張増分

自動拡張がトリガーされたときに、プロファイルコンテナが自動的に拡張するストレージ容量（GB単位）を指定できます。

構成の優先順位:

- このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここまたは.iniファイルで構成されていない場合、デフォルトは10 GBです。

プロファイルコンテナの自動拡張制限

自動拡張がトリガーされたときに、プロファイルコンテナが自動的に拡張できる最大ストレージ容量（GB単位）を指定できます。

構成の優先順位:

- このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここまたは.iniファイルで構成されていない場合、デフォルトは80 GBです。

ユーザーレベルのポリシー設定を有効にする

このポリシーを有効にすると、マシンレベルのポリシー設定がユーザーレベルで機能し、ユーザーレベルの設定がマシンレベルの設定を上書きします。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
2. ここででも.iniファイルでもこのポリシーが構成されていない場合、無効になります。

ユーザーグループの優先順位を設定する

ユーザーグループの優先順位を指定できます。この順序は、ユーザーが異なるポリシー設定を持つ複数のグループに属している場合に、どのグループが優先されるかを決定します。

ユーザーが競合するポリシー設定を持つ複数のグループに属している場合、以下を考慮してください:

- ユーザーがこのポリシーで定義されている1つ以上のグループに属している場合、最も優先順位の高いグループが優先されます。
- ユーザーがこのポリシーで定義されているどのグループにも属していない場合、アルファベット順で最も早くリストされているSIDを持つグループが優先されます。

ユーザーストアの選択方法

複数のユーザーストアが利用可能な場合のユーザーストア選択方法を指定できます。オプションは次のとおりです。

- **構成順序。** Profile Managementは、最初に構成されたストアを選択します。
- **アクセスパフォーマンス。** Profile Managementは、最もアクセスパフォーマンスの良いストアを選択します。

構成の優先順位:

1. ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。
2. ここでも .ini ファイルでもこの設定が構成されていない場合、**構成順序**が使用されます。

ユーザーストア間でのセッション内プロファイルコンテナフェイルオーバーを有効にする

デフォルトでは、複数のユーザーストアが展開されている場合、プロファイルコンテナのフェイルオーバーはユーザーログオン時にのみ発生します。その結果、プロファイルの冗長性はユーザーログオン時にのみ利用可能です。このポリシーを使用すると、フェイルオーバーの範囲をセッション全体に拡大し、セッション全体でプロファイルの冗長性を確保できます。このポリシーが有効になっている場合、セッション中にProfile Managementがアクティブなプロファイルコンテナへの接続を失うと、自動的に別の利用可能なコンテナに切り替わります。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。

2. ここでも .ini ファイルでもこのポリシーが構成されていない場合、この設定は無効になります。

プロファイル読み込みタイムアウト

プロファイル読み込みタイムアウト機能を有効にし、タイムアウト期間を構成できます。Citrix Profile Management は、一時プロファイルに切り替える前に、ユーザー プロファイルが読み込まれるまで指定されたタイムアウト時間待機します。 デフォルトでは、**プロファイル読み込みタイムアウト**設定は 45 秒で、有効な範囲は 0 ～ 1800 秒です。プロファイルの読み込みをバイパスして一時プロファイルを使用するには、タイムアウトを 0 秒に設定します。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。
2. ここでも .ini ファイルでもこのポリシーが構成されていない場合、このポリシーはデフォルトで無効になります。

ログオフ時のプロファイル同期を制限する

ユーザー ログオフ時に同期されるユーザー ストアの数を指定できます。 デフォルトでは、Citrix Profile Management はログオフ中にすべてのユーザー ストアを同期し、すべてのストアでプロファイルが同期されるまでログオフは完了しません。 同期されるストアの数を減らすと、ログオフが高速化されます。非永続マシンでは、未同期のストアは次回のユーザー セッション中に更新され、永続マシンでは、未同期のストアはバックグラウンドで同期されます。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、ポリシーはデフォルトで無効になります。\n\n注: この設定は、ユーザー ストアのレプリケートポリシーが有効になっている場合にのみ適用されます。

プロファイルサイズがクォータを超過した場合にユーザーに通知する

ユーザープロファイルのクォータを設定し、プロファイルサイズがそれを超過した場合にユーザーに通知できます。

設定の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここまたは.iniファイルで構成されていない場合、設定は無効になります。

プロファイルサイズがクォータを超過した場合の通知メッセージ

プロファイルサイズがクォータを超過した場合にユーザーに通知ポリシーが有効な場合に適用されます。ユーザーが受け取る通知メッセージを設定できます。

設定の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここまたは.iniファイルで構成されていない場合、設定は無効になります。

マシン休止状態のマルチセッションサポートを有効にする

休止状態中にディスクの状態を維持することで、システム休止状態のサポートを有効にできます。これにより、休止状態のセッションで使用されているVHDXディスクが、他の同時セッションに再割り当てされないようにします。その結果、マシンが休止状態から回復した後もユーザープロファイルを再開でき、一貫したセッションの継続性が保証されます。

設定の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここまたは.iniファイルで構成されていない場合、設定は無効になります。

基本的なポリシー設定

このセクションには、Profile Management の基本的な構成に関連するポリシー設定が含まれています。

Profile Management を有効にする

デフォルトでは、展開を容易にするため、Profile Management はログオンまたはログオフを処理しません。Profile Management は、他のすべてのセットアップタスクを実行し、Citrix® ユーザープロファイルが環境でどのように動作するかをテストした後にのみ有効にしてください。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、Profile Management は Windows ユーザープロファイルを一切処理しません。

処理されるグループ

コンピューターローカルグループとドメイングループ（ローカル、グローバル、ユニバーサル）の両方を使用できます。ドメイングループは、DOMAIN NAME\GROUP NAME の形式で指定する必要があります。

このポリシーがここで構成されている場合、Profile Management はこれらのユーザーグループのメンバーのみを処理します。このポリシーが無効になっている場合、Profile Management はすべ

てのユーザーを処理します。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、すべてのユーザーグループのメンバーが処理されます。

除外されるグループ

コンピューターローカルグループとドメイングループ（ローカル、グローバル、ユニバーサル）を使用して、特定のユーザープロファイルが処理されないようにすることができます。ドメイングループは、DOMAIN NAME\ GROUP NAME の形式で指定します。

この設定がここで構成されている場合、Profile Management はこれらのユーザーグループのメンバーを除外します。この設定が無効になっている場合、Profile Management はどのユーザーも除外しません。この設定がここで構成されていない場合、.ini ファイルの値が使用されます。この設定がここでも .ini ファイルでも構成されていない場合、どのグループのメンバーも除外されません。

ローカル管理者のログオンを処理する

BUILTIN\Administrators グループのメンバーのログオンが処理されるかどうかを指定します。Citrix Virtual Apps 環境などのマルチセッションオペレーティングシステムでは、このポリシーが無効になっているか、構成されていないと見なされます。この場合、Profile Management は、ドメインユーザーによるログオンは処理されるが、ローカル管理者によるログオンは処理されないと想定します。シングルセッションオペレーティングシステム（Citrix Virtual Desktops 環境など）では、ローカル管理者のログオンが処理されます。このポリシーにより、ローカル管理者権限を持つドメインユーザー（通常、割り当てられた仮想デスクトップを持つ Citrix Virtual Desktops ユーザー）は、次のことが可能になります。

- 処理をバイパスする
- ログオンする
- Profile Managementでデスクトップに問題が発生した場合のトラブルシューティング

注：ドメインユーザーのログオンは、通常、製品ライセンスへの準拠を確実にするために、グループメンバーシップによって課される制限を受ける場合があります。 このポリシーが無効になっている場合、Profile Managementはローカル管理者によるログオンを処理しません。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここまたは.iniファイルで構成されていない場合、管理者は処理されません。

ユーザーストアへのパス

ユーザー設定（レジストリの変更と同期されたファイル）が保存されるディレクトリ（ユーザーストア）へのパスを設定します。

パスは次のいずれかです。

- 相対パス。ホームディレクトリ（通常、Active Directoryのユーザーの#homeDirectory#属性として構成されます）に対する相対パスである必要があります。
- UNCパス。通常、サーバー共有またはDFS名前空間を指定します。
- 無効または未構成。この場合、#homeDirectory#\Windowsの値が想定されます。

このポリシーでは、次の種類の変数を使用できます。

- パーセント記号で囲まれたシステム環境変数（例：%ProfVer%）。システム環境変数は通常、追加の設定が必要です。
- ハッシュで囲まれたActive Directoryユーザーオブジェクトの属性（例：#sAMAccountName#）。
- Profile Management変数。詳細については、Profile Management変数の製品ドキュメントを参照してください。

`%username%`と`%userdomain%`を除き、ユーザー環境変数は使用できません。場所やユーザーなどを完全に定義するために、カスタム属性を作成することもできます。属性は大文字と小文字を区別します。

例：

- \\server\share#sAMAccountName# は、ユーザー設定をUNCパス \\server\share\JohnSmith に保存します（現在のユーザーに対して #sAMAccountName# が JohnSmith に解決される場合）。
- \\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS! は \\server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64 に展開される場合があります。

重要：使用する属性または変数に関係なく、このポリシーがNTUSER.DATを含むフォルダーの1つ上のフォルダーに展開されることを確認してください。たとえば、このファイルが`\\server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile`に含まれる場合、ユーザー ストアへのパスを`\\server\profiles$\JohnSmith.Finance\Win8x64`に設定します（\UPM_Profileサブフォルダーではありません）。

ユーザー ストアへのパスを指定する際の変数の使用方法について詳しくは、以下のトピックを参照してください。

- 複数のファイルサーバーでCitrixユーザープロファイルを共有する
- OU内およびOU間でプロファイルを管理する

- Profile Managementによる高可用性とディザスターリカバリ

ユーザーストアへのパスが無効になっている場合、ユーザー設定はホームディレクトリのWindowsサブディレクトリに保存されます。

このポリシーが無効になっている場合、ユーザー設定はホームディレクトリのWindowsサブディレクトリに保存されます。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、ホームドライブのWindowsディレクトリが使用されます。

ユーザーストアの移行

ユーザー設定（レジストリの変更と同期されたファイル）が以前に保存されていたフォルダーへのパス（以前使用していたユーザーストアパス）を指定します。

この設定が構成されている場合、以前のユーザー ストアに保存されているユーザー設定は、「ユーザー ストアへのパス」ポリシーで指定された現在のユーザー ストアに移行されます。

パスは、絶対UNCパスまたはホームディレクトリに対する相対パスにすることができます。

どちらの場合も、次の種類の変数を使用できます。

- パーセント記号で囲まれたシステム環境変数
- ハッシュ記号で囲まれたActive Directoryユーザーオブジェクトの属性

例:

- フォルダー `Windows\%ProfileVer%` は、ユーザー設定をユーザーストアの `Windows\W2K3` というサブフォルダーに保存します（%ProfileVer% がW2K3に解決されるシステム環境変数である場合）。
- `\\server\share#SAMAccountName#` は、ユーザー設定をUNCパス `\\server\share\<JohnSmith>` に保存します（`#SAMAccountName#` が現在のユーザーに対してJohnSmithに解決される場合）。

パスでは、`%username%` と `%userdomain%` を除くユーザー環境変数を使用できます。

この設定が無効になっている場合、ユーザー設定は現在のユーザーストアに保存されます。

この設定がここで構成されていない場合、.iniファイルの対応する設定が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、ユーザー設定は現在のユーザーストアに保存されます。

アクティブライトバック

変更されたファイルとフォルダー（レジストリエントリを除く）は、ログオフする前にセッション中にユーザーストアに同期できます。

このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、有効になります。

オフラインプロファイルのサポート

このポリシーにより、プロファイルを可能な限り早くユーザー ストアと同期できます。これは、ローミングするラップトップまたはモバイルデバイスのユーザーを対象としています。ネットワーク接続が切断されても、再起動または休止状態の後でも、プロファイルはラップトップまたはデバイス上でそのまま維持されます。モバイルユーザーが作業すると、プロファイルはローカルで更新されます。また、ネットワーク接続が再確立されると、最終的にユーザー ストアと同期されます。

このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、オフラインプロファイルは無効になります。

アクティブライトバックレジストリ

「アクティブライトバック」と合わせてこのポリシーを使用してください。変更されたレジストリエントリは、セッション中にユーザーストアに同期できます。

ここでこの設定を構成しない場合、.iniファイルの値が使用されます。

ここで、または.iniファイルでこの設定を構成しない場合、アクティブなライトバックレジストリは無効になります。

セッションロックおよび切断時のアクティブなライトバック

このポリシーと**アクティブなライトバック**ポリシーの両方が有効になっている場合、プロファイルファイルとフォルダーは、セッションがロックまたは切断された場合にのみ書き戻されます。

このポリシーと、**アクティブなライトバック**および**アクティブなライトバックレジストリ**の両方のポリシーが有効になっている場合、レジストリエントリは、セッションがロックまたは切断された場合にのみ書き戻されます。

オフラインプロファイルのサポート

オフラインプロファイル機能を有効にします。この機能は、ネットワークから頻繁に切断されるコンピューター向けです。たとえば、サーバーやデスクトップではなく、ラップトップやモバイルデバイスなどです。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定が構成されていない場合、オフラインプロファイルのサポートは無効になります。

クロスプラットフォームポリシー設定

このセクションには、**Profile Management cross-platform** 設定機能の構成に関連するポリシー設定が含まれています。

クロスプラットフォーム設定を有効にする

デフォルトでは、展開を容易にするために、クロスプラットフォーム設定は無効になっています。このポリシーを有効にすることで処理をオンにできますが、この機能の十分な計画とテストを行った後にのみ有効にしてください。

このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、クロスプラットフォーム設定は適用されません。

クロスプラットフォーム設定ユーザーグループ

1つ以上のWindowsユーザーグループを入力します。たとえば、このポリシーを使用して、テストユーザーグループのプロファイルのみを処理できます。このポリシーが構成されている場合、Profile Management のクロスプラットフォーム設定機能は、これらのユーザーグループのメンバーのみを処理します。このポリシーが無効になっている場合、この機能は「処理されたグループ」ポリシーで指定されたすべてのユーザーを処理します。

このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、すべてのユーザーグループが処理されます。

クロスプラットフォーム定義へのパス

ダウンロードパッケージからコピーした定義ファイルのネットワーク上の場所を識別します。このパスはUNCパスである必要があります。ユーザーはこの場所への読み取りアクセス権を持ち、管理者は書き込みアクセス権を持っている必要があります。この場所は、Server Message Block (SMB) または Common Internet File System (CIFS) ファイル共有である必要があります。

このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、クロスプラットフォーム設定は適用されません。

クロスプラットフォーム設定ストアへのパス

クロスプラットフォーム設定ストアへのパスを設定します。これは、ユーザーのクロスプラットフォーム設定が保存されるフォルダーです。ユーザーはこの領域への書き込みアクセス権を持っている必要があります。パスは絶対UNCパスまたはホームディレクトリからの相対パスにすることができます。

この領域は、複数のプラットフォームで共有されるプロファイルデータが配置されるユーザーストアの共通領域です。ユーザーはこの領域への書き込みアクセス権を持っている必要があります。パスは絶対UNCパスまたはホームディレクトリからの相対パスにすることができます。**ユーザーストアへのパス**と同じ変数を使用できます。

このポリシーが無効になっている場合、パス Windows\PM_CP が使用されます。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、デフォルト値が使用されます。

クロスプラットフォーム設定を作成するためのソース

このポリシーがそのプラットフォームのOUで有効になっている場合、プラットフォームをベースプラットフォームとして指定します。このポリシーは、ベースプラットフォームのプロファイルからクロスプラットフォーム設定ストアにデータを移行します。

各プラットフォーム独自のプロファイルセットは、個別のOUに保存されます。クロスプラットフォーム設定ストアをシードするために、どのプラットフォームのプロファイルデータを使用するかを決定する必要があります。これはベースプラットフォームと呼ばれます。クロスプラットフォーム設定ストアにデータのない定義ファイルが含まれている場合、または単一プラットフォームプロファイルのキャッシュデータがストア内の定義データよりも新しい場合を考慮してください。この場合、このポリシーを無効にしない限り、Profile Managementは単一プラットフォームプロファイルからストアにデータを移行します。

> **重要:**
>
> このポリシーが複数のOU、または複数のユーザーオブジェクトやマシンオブジェクトで有効になっている場合、最初にログオンしたユーザーのプラットフォームがベースプロファイルになります。 デフォルトでは、このポリシーは有効になっています。

ファイルシステム ポリシー設定

このセクションには、次の項目を設定するポリシーが含まれています。

- ユーザープロファイル内のどのファイルが、プロファイルがインストールされているシステムとユーザー ストアの間で同期されるか
- ユーザープロファイル内のどのディレクトリが、プロファイルがインストールされているシステムとユーザー ストアの間で同期されるか

除外ポリシー設定

このセクションでは、ユーザープロファイル内のどのファイルとディレクトリを同期プロセスから除外するかを設定するためのポリシー設定について説明します。

除外リスト - ファイル

同期中に無視されるファイルのリスト。ファイル名はユーザープロファイル (%USERPROFILE%) に対する相対パスである必要があります。ファイル名とフォルダー名でワイルドカードがサポートされていますが、ファイル名のワイルドカードのみが再帰的に適用されます。

例:

- `Desktop` フォルダー内の `Desktop.ini` ファイルを `Desktop\Desktop.ini` 無視します。
- プロファイル全体で、拡張子が `.tmp` のすべてのファイルを `%USERPROFILE%*.tmp` 無視します。
- プロファイルの一部で、拡張子が `.tmp` のすべてのファイルを `AppData\Roaming\MyApp*.tmp` 無視します。
- `Downloads` フォルダーの直下のサブフォルダーにある `a.txt` を `Downloads*\a.txt` 無視します。

このポリシーが無効になっている場合、ファイルは除外されません。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ファイルは除外されません。

デフォルトの除外リストを有効にする - ディレクトリ

同期中に無視されるディレクトリのデフォルトリスト。このポリシーを使用して、GPO除外ディレクトリを手動で入力することなく指定できます。

このポリシーを無効にすると、Profile Management はデフォルトでどのディレクトリも除外しません。

このポリシーをここで構成しない場合、Profile Management は .ini ファイルの値を使用します。このポリシーをここでも .ini ファイルでも構成しない場合、Profile Management はデフォルトでどのディレクトリも除外しません。

除外リスト - ディレクトリ

同期中に無視されるフォルダーのリスト。フォルダー名はユーザープロファイル (%USERPROFILE%) に対する相対パスとして指定する必要があります。フォルダー名でのワイルドカードはサポートされていますが、再帰的には適用されません。

例:

- `Desktop` はユーザープロファイル内の `Desktop` フォルダーを無視します

このポリシーが無効になっている場合、フォルダーは除外されません。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、フォルダーは除外されません。

ログオン除外チェック

この設定は、ユーザーストア内のプロファイルに除外されたファイルまたはフォルダーが含まれている場合に、Profile Management が何を行うかを構成します。可能なポリシー設定とそれに対応するアクションを次の表に示します。

ポリシー設定	アクション
設定が無効になっているか、「ログオン時に除外されたファイルまたはフォルダーを同期する」の値がデフォルトに設定されている	ユーザーがログオンすると、Profile Managementはユーザーストアからローカルプロファイルに除外されたファイルまたはフォルダーを同期します。
設定が「ログオン時に除外されたファイルまたはフォルダーを無視する」に設定されている	ユーザーがログオンすると、Profile Managementはユーザーストア内の除外されたファイルまたはフォルダーを無視します。
設定が「ログオン時に除外されたファイルまたはフォルダーを削除する」に設定されている	ユーザーがログオンすると、Profile Managementはユーザーストア内の除外されたファイルまたはフォルダーを削除します。
Web Studioで設定が構成されていない	.iniファイルの値が使用されます
Web Studioまたは.iniファイルで設定が構成されていない	ユーザーがログオンすると、除外されたファイルまたはフォルダーはユーザーストアからローカルプロファイルに同期されます。

大容量ファイルの処理 - シンボリックリンクとして作成されるファイル

ログオンパフォーマンスを向上させ、サイズの大きいファイルを処理するために、Profile Management はこのリスト内のファイルをコピーする代わりにシンボリックリンクを作成します。

ファイルを参照するポリシーではワイルドカードを使用できます。例: `!ctx_localappdata!\Microsoft\Outlook*.OST`。

Microsoft Outlook のオフラインフォルダーファイル (`*.ost`) を処理するには、**Outlook** フォルダーが Profile Management の対象から除外されていないことを確認してください。

これらのファイルは、複数のセッションで同時にアクセスすることはできません。

同期ポリシー設定

同期セクションでは、ユーザープロファイル内のどのファイルとフォルダーを、プロファイルがインストールされているシステムとユーザー ストアの間で同期するかを指定するためのポリシー設定について説明します。

同期するディレクトリ

デフォルトでは、Profile Management は、ユーザープロファイルがインストールされているシステムとユーザー ストアの間でユーザープロファイルを同期します。同期からフォルダーを除外した場合、このポリシーを使用すると、除外されたフォルダーのサブフォルダーを同期に含めることができます。

このリストのパスは、ユーザープロファイルに対する相対パスである必要があります。フォルダー名でのワイルドカードはサポートされていますが、再帰的には適用されません。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ユーザープロファイル内の除外されていないフォルダーのみが同期されます。

同期するファイル

デフォルトでは、Profile Management は、ユーザープロファイルがインストールされているシステムとユーザー ストアの間でユーザープロファイルを同期します。同期からフォルダーを除外した場合、このポリシーを使用すると、除外されたフォルダー内のファイルを同期に含めることができます。

このリストのパスは、ユーザープロファイルに対する相対パスである必要があります。ファイル名とフォルダー名でワイルドカードがサポートされていますが、ファイル名のワイルドカードのみが再帰的に適用されます。ワイルドカードをネストすることはできません。

例:

- `AppData\Local\Microsoft\Office\Access.qat` は、デフォルト構成で除外されているフォルダーの下にあるファイルを指定します。
- `AppData\Local\MyApp*.cfg` は、プロファイルフォルダー `AppData\Local\MyApp` およびそのサブフォルダー内の拡張子 `.cfg` を持つすべてのファイルを指定します。

このポリシーを無効にすると、有効にして空のリストを構成した場合と同じ効果があります。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ユーザープロファイル内の除外されていないファイルのみが同期されます。

ミラーリングするフォルダー

このポリシーを使用すると、トランザクションフォルダー（参照フォルダーとも呼ばれる）に関連する問題を解決できます。このフォルダーには、相互に依存するファイルが含まれており、あるファイルが別のファイルを参照しています。

フォルダーのミラーリングにより、プロファイル管理はトランザクションフォルダーとその内容を単一のエンティティとして処理し、プロファイルの肥大化を防ぐことができます。たとえば、**Internet Explorer の Cookie** フォルダーをミラーリングして、Index.dat がインデックス化する Cookie と同期されるようにすることができます。このような状況では、「最後の書き込みが優先されます」。そのため、複数のセッションで変更されたミラーリングされたフォルダー内のファイルは、最後の更新によって上書きされ、プロファイル変更が失われます。

たとえば、次の表は、ユーザーがインターネットを閲覧しているときに Index.dat が Cookie をどのように参照するかを示しています。

シナリオ	INDEX.DAT が COOKIE を参照する方法	
ユーザーは2つの Internet Explorer セッションを持っており、それぞれ異なるサーバー上で実行され、各セッションで異なるサイトを訪問します。	各サイトからの Cookie は、適切なサーバーに追加されます。	各サイトからの Cookie は、適切なサーバーに追加されます。
ユーザーが最初のセッションからログオフするか、セッションの途中でログオフします (アクティブなライトバッ	2番目のセッションからの Cookie は、最初のセッショ	

シナリオ	INDEX.DAT が COOKIE を参照する方法	
ク機能が構成されている場合)。	ンからの Cookie を置き換える必要があります。	
最初のセッションと2番目のセッションがマージされ、Index.dat 内の Cookie への参照が古くなります。	新しいセッションでのさらなる閲覧は、繰り返しのマージと肥大化した Cookie フォルダーにつながります。	

Cookie フォルダーをミラーリングすることで、この問題は解決されます。この場合、ユーザーがログオフするたびに、Cookie は最後のセッションからの Cookie で上書きされます。そのため、Index.dat は常に最新の状態に保たれます。

ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。ここで、または .ini ファイルでこのポリシーが構成されていない場合、フォルダーはミラーリングされません。

フォルダーのミラーリングを高速化する

このポリシーと**ミラーリングするフォルダー**ポリシーの両方を有効にすると、**Profile Management はミラーリングされた**フォルダーを VHDX ベースの仮想ディスクに保存します。仮想ディスクはログオン時にアタッチされ、ログオフ時にデタッチされます。このポリシーを有効にすると、ユーザー ストアとローカル プロファイルの間でフォルダーをコピーする必要がなくなり、フォルダーのミラーリングが高速化されます。

フォルダーリダイレクトのポリシー設定

このセクションには、プロファイルに一般的に表示されるフォルダーを共有ネットワークの場所にリダイレクトするかどうかを指定するポリシー設定が含まれています。

管理者アクセスの許可

この設定により、管理者はユーザーのリダイレクトされたフォルダーの内容にアクセスできるようになります。

> **注:**
>
> この設定は、ドメインへの完全かつ無制限のアクセス権を持つ管理者に対して権限を付与します。

> デフォルトでは、この設定は無効になっており、ユーザーはリダイレクトされたフォルダーの内容への排他的アクセス権を付与されます。

ドメイン名を含める

この設定により、UNC パスの一部として `%userdomain%` 環境変数を含めることができます。この UNC パスは、リダイレクトされたフォルダーに対して指定されます。

デフォルトでは、この設定は無効になっています。また、リダイレクトされたフォルダーに対して指定された UNC パスの一部として、`%userdomain%` 環境変数は含まれません。

ドキュメントポリシー設定

このセクションには、**ドキュメント**フォルダーの内容を共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ドキュメントパス

この設定は、**ドキュメント**フォルダー内のファイルがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ドキュメントパス設定は、**ドキュメント**フォルダーにファイルをリダイレクトするだけでなく、**ミュージック**、**ピクチャ**、**ビデオ**フォルダーにもファイルをリダイレクトするために有効にする必要があります。

ドキュメントのリダイレクト設定

この設定は、**ドキュメント**フォルダーの内容をリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

ドキュメントフォルダーの内容をリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次の UNC パスにリダイレクトします。ドキュメントパスポリシー設定で指定された UNC パスにコンテンツをリダイレクトします。
- ユーザーのホームディレクトリにリダイレクトします。コンテンツをユーザーのホームディレクトリにリダイレクトします。これは通常、Active Directory のユーザーの #homeDirectory# 属性として構成されます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ダウンロードポリシー設定

このセクションには、**ダウンロード**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ダウンロードパス

この設定は、**ダウンロード**フォルダー内のファイルがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ダウンロードのリダイレクト設定

この設定は、**ダウンロード**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

リンクポリシー設定

このセクションには、**リンク**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

リンクパス

この設定は、**リンク**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

リンクのリダイレクト設定

この設定は、**リンク**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

音楽ポリシー設定

このセクションには、**Music**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

音楽パス

この設定は、**Music**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

この設定がここで構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

音楽のリダイレクト設定

この設定は、**Music**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

Musicフォルダーのコンテンツをリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次のUNCパスにリダイレクトします。Musicパスポリシー設定で指定されたUNCパスにコンテンツをリダイレクトします。
- ドキュメントフォルダーを基準にリダイレクトします。ドキュメントフォルダーを基準としたフォルダーにコンテンツをリダイレクトします。

ドキュメントフォルダーを基準としたフォルダーにコンテンツをリダイレクトするには、**ドキュメントパス**設定を有効にする必要があります。

この設定がここで構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ピクチャのポリシー設定

このセクションには、**画像**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ピクチャのパス

この設定は、**画像**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

画像のリダイレクト設定

この設定は、**画像**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

画像フォルダーのコンテンツをリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次の UNC パスにリダイレクトします。「ピクチャのパス」ポリシー設定で指定された UNC パスにコンテンツをリダイレクトします。
- ドキュメントフォルダーを基準にリダイレクトします。ドキュメントフォルダーを基準としたフォルダーにコンテンツをリダイレクトします。

ドキュメントフォルダーを基準としたフォルダーにコンテンツをリダイレクトするには、「**ドキュメントのパス**」設定を有効にする必要があります。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

Searchesポリシー設定

このセクションには、**検索**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

SEARCHESのリダイレクト設定

この設定は、**検索**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

SEARCHESパス

この設定は、**検索**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

ビデオポリシー設定

このセクションには、**ビデオ**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ビデオのリダイレクト設定

この設定は、**ビデオ**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ビデオフォルダーのコンテンツをリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次のUNCパスにリダイレクトします。コンテンツを、ビデオパスポリシー設定で指定されたUNCパスにリダイレクトします。
- ドキュメントフォルダーを基準にリダイレクトします。コンテンツを、ドキュメントフォルダーを基準としたフォルダーにリダイレクトします。

コンテンツを**ドキュメント**フォルダーを基準としたフォルダーにリダイレクトするには、**ドキュメントパス**設定を有効にする必要があります。

この設定がここで構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

ビデオパス

この設定は、**ビデオ**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

この設定がここで構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

ログポリシー設定

このセクションには、Profile Management のログ記録を構成するポリシー設定が含まれています。

Active Directory のアクション

この設定は、Active Directory で実行されるアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定が Web Studio で構成されていない場合、.ini ファイルの値が使用されます。

この設定が Web Studio または .ini ファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

一般情報

この設定は、一般情報の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

一般的な警告

この設定は、一般的な警告の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログの有効化**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログの有効化

この設定は、デバッグ（詳細ログ）モードでのプロファイル管理ログを有効または無効にします。デバッグモードでは、"%SystemRoot%\System32\Logfiles\UserProfileManager" にあるログファイルに詳細なステータス情報が記録されます。

デフォルトでは、この設定は無効になっており、エラーのみがログに記録されます。

Citrix®は、プロファイル管理のトラブルシューティングを行う場合にのみ、この設定を有効にすることをお勧めします。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、エラーのみがログに記録されます。

ファイルシステムのアクション

この設定は、ファイルシステムで実行されたアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログの有効化**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ファイルシステム通知

この設定は、ファイルシステム通知の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログの有効化**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオフ

この設定は、ユーザーのログオフの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオン

この設定は、ユーザーのログオンの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

Web Studioまたは.iniファイルでこの設定が構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログファイルの最大サイズ

この設定は、Profile Managementログファイルの最大許容サイズをバイト単位で指定します。

デフォルトでは、この値は1048576バイト（1 MB）に設定されています。

十分なディスク容量がある場合、Citrixはこのファイルのサイズを5 MB以上に増やすことを推奨します。ログファイルが最大サイズを超えて増加した場合：

- 既存のファイルのバックアップ（.bak）が削除されます
- ログファイルは.bakに名前が変更されます
- 新しいログファイルが作成されます

ログファイルは`%SystemRoot%\System32\Logfiles\UserProfileManager`に作成されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここで、または.iniファイルでこの設定が構成されていない場合、デフォルト値が使用されます。

ログファイルへのパス

この設定は、Profile Managementログファイルを保存するための代替パスを指定します。

デフォルトでは、この設定は無効になっており、ログファイルはデフォルトの場所である%SystemRoot%\System32\Logfiles\UserProfileManagerに保存されます。

パスはローカルドライブまたはリモートのネットワークベースドライブ（UNCパス）を指すことができます。リモートパスは大規模な分散環境で役立つことがありますが、ログファイルには不適切な大量のネットワークトラフィックを生成する可能性があります。プロビジョニングされた永続的なハードドライブを持つ仮想マシンの場合、そのドライブへのローカルパスを設定します。この設定により、マシンの再起動時にログファイルが保持されます。永続的なハードドライブを持たない仮想マシンの場合、UNCパスを設定することでログファイルを保持できます。ただし、マシンのシステムアカウントはUNC共有への書き込みアクセス権を持っている必要があります。オフラインプロファイル機能によって管理されるラップトップには、ローカルパスを使用してください。

ログファイルにUNCパスを使用する場合、Citrixはログファイルフォルダーに適切なアクセス制御リストを適用することを推奨します。この設定により、承認されたユーザーまたはコンピューターアカウントのみが保存されたファイルにアクセスできるようになります。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

ここまたは .ini ファイルでこの設定が構成されていない場合、デフォルトの場所 %SystemRoot%\System32\Logfiles\UserProfileManager が使用されます。

パーソナライズされたユーザー情報

この設定は、パーソナライズされたユーザー情報の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合、**ログの有効化**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオン時とログオフ時のポリシー値

この設定は、ユーザーがログオンおよびログオフするときのポリシー値の詳細ログ記録を有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合、**ログの有効化**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

レジストリアクション

この設定は、レジストリで実行されたアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオフ時のレジストリの相違点

この設定は、ユーザーがログオフしたときのレジストリの相違点の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー

- 一般情報

プロファイル処理ポリシー設定

このセクションには、Profile Management がユーザープロファイルを処理する方法を指定するポリシー設定が含まれています。

キャッシュされたプロファイルを削除するまでの遅延

この設定は、Profile Management がログオフ時にローカルにキャッシュされたプロファイルを削除するまでの遅延を、分単位で任意に延長する時間を指定します。

値が0の場合、ログオフプロセスの終了時にプロファイルがすぐに削除されます。Profile Management は1分ごとにログオフをチェックします。その結果、値が60の場合、ユーザーがログオフしてから1〜2分以内にプロファイルが削除されることが保証されます。このアクションは、最後のチェックがいつ行われたかによって異なります。ログオフ中にプロセスがファイルまたはユーザーレジストリハイブを開いたままにしていることがわかっている場合、遅延を延長すると便利です。大規模なプロファイルの場合、このプロセスはログオフを高速化することもできます。

デフォルトでは、この値は0に設定されており、Profile Management はローカルにキャッシュされたプロファイルをすぐに削除します。

この設定を有効にする場合は、「ログオフ時にローカルにキャッシュされたプロファイルを削除する」も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、プロファイルはすぐに削除されます。

ログオフ時にローカルにキャッシュされたプロファイルを削除する

この設定は、ユーザーがログオフした後にローカルにキャッシュされたプロファイルが削除されるかどうかを指定します。

この設定が有効になっている場合、ユーザーのローカルプロファイルキャッシュはログオフ後に削除されます。Citrix® は、ターミナルサーバーに対してこの設定を有効にすることを推奨しています。

デフォルトでは、この設定は無効になっており、ユーザーのローカルプロファイルキャッシュはログオフ後も保持されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、キャッシュされたプロファイルは削除されません。

ローカルプロファイルの競合処理

この設定は、ユーザープロファイルが以下の両方に存在する場合のProfile Managementの動作を構成します。

- ユーザーストア
- ローカルWindowsユーザープロファイル（Citrixユーザープロファイルではない）

デフォルトでは、Profile Management はローカルの Windows プロファイルを使用しますが、それを一切変更しません。

Profile Management の動作を制御するには、次のいずれかのオプションを選択します。

- ローカルプロファイルを使用する。Profile Management はローカルプロファイルを使用しますが、それを一切変更しません。
- ローカルプロファイルを削除する。Profile Management はローカルの Windows ユーザープロファイルを削除し、その後ユーザー ストアから Citrix ユーザープロファイルをインポートします。
- ローカルプロファイルの名前を変更する。Profile Management はローカルの Windows ユーザープロファイルの名前を変更し (バックアップ目的)、その後ユーザー ストアから Citrix ユーザープロファイルをインポートします。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がここで、または .ini ファイルで構成されていない場合、既存のローカルプロファイルが使用されます。

既存プロファイルの移行

この設定は、ユーザーがユーザーストアに現在のプロファイルを持っていない場合に、ログオン中にユーザーストアに移行されるプロファイルの種類を指定します。

ユーザーがユーザーストアにプロファイルを持っていない場合、Profile Managementはログオン中に既存のプロファイルを「その場で」移行できます。その後、ユーザーストアプロファイルは、以下の両方でProfile Managementによって使用されます。

- 現在のセッション
- 同じユーザー ストアへのパスで構成されたその他のセッション

デフォルトでは、ログオン時にローカルプロファイルと移動プロファイルの両方がユーザー ストアに移行されます。

ログオン中にユーザー ストアに移行されるプロファイルの種類を指定するには、次のいずれかのオプションを選択します。

- ローカルプロファイルと移動プロファイル
- ローカル
- ローミング
- なし (無効)

なしを選択すると、Profile Managementがインストールされていない環境であるかのように、システムは既存のWindowsメカニズムを使用してプロファイルを作成します。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、既存のローカルプロファイルとローミングプロファイルが移行されます。

既存のアプリケーションプロファイルの自動移行

この設定は、異なるオペレーティングシステム間で既存のアプリケーションプロファイルを自動的に移行するかどうかを有効または無効にします。アプリケーションプロファイルには、`AppData`フォルダー内のアプリケーションデータと、`HKEY_CURRENT_USER\SOFTWARE`の下のレジストリエントリの両方が含まれます。この設定は、異なるオペレーティングシステム間でアプリケーションプロファイルを移行したい場合に役立ちます。

たとえば、オペレーティングシステム（OS）をWindows 10バージョン1803からWindows 10バージョン1809にアップグレードするとします。この設定が有効になっている場合、各ユーザーが最初にログオンするときに、Profile Managementは既存のアプリケーション設定をWindows 10バージョン1809に自動的に移行します。その結果、`AppData`フォルダー内のアプリケーションデータとHKEY_CURRENT_USER\SOFTWAREの下のレジストリエントリが移行されます。

複数の既存のアプリケーションプロファイルがある場合、Profile Managementは次の優先順位で移行を実行します。

1. 同じOSタイプのプロファイル (シングルセッションOSからシングルセッションOS、マルチセッションOSからマルチセッションOS)。
2. 同じWindows OSファミリーのプロファイル。例えば、Windows 10からWindows 10、またはWindows Server 2016からWindows Server 2016。

3. OSの以前のバージョンのプロファイル。例えば、Windows 7からWindows 10、またはWindows Server 2012からWindows 2016。
4. 最も近いOSのプロファイル。

注： ユーザー保存パスに変数「!CTX_OSNAME!」を含めることで、OSの短い名前を指定する必要があります。これにより、Profile Managementは既存のアプリケーションプロファイルを特定できます。

この設定がここで構成されていない場合、.iniファイルの設定が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、デフォルトで無効になります。

テンプレートプロファイルへのパス

この設定は、Profile Managementがユーザープロファイルを作成するためのテンプレートとして使用するプロファイルへのパスを指定します。

指定されたパスは、NTUSER.DATレジストリファイルと、テンプレートプロファイルに必要なその他のフォルダーおよびファイルを含むフォルダーへの完全なパスである必要があります。

注：パスにNTUSER.DATを含めないでください。例えば、ファイルが\\myservername\myprofiles\template\ntuser.datの場合、場所を\\myservername\myprofiles\templateとして設定します。

絶対パスを使用します。これはUNCパスまたはローカルマシン上のパスのいずれかです。後者は、例えばCitrix Provisioning™ Servicesイメージ上にテンプレートプロファイルを永続的に指定するために使用します。相対パスはサポートされていません。

注：この設定は、Active Directory属性、システム環境変数、または`%USERNAME%`および`%USERDOMAIN%`変数の展開をサポートしていません。

デフォルトでは、この設定は無効になっており、新しいユーザープロファイルは、ユーザーが最初にログオンするデバイス上のデフォルトのユーザープロファイルから作成されます。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、テンプレートは使用されません。

テンプレートプロファイルがローカルプロファイルを上書きする

この設定により、ユーザープロファイルの作成時にテンプレートプロファイルがローカルプロファイルを上書きできるようになります。

ユーザーがCitrixユーザープロファイルを持たず、ローカルのWindowsユーザープロファイルを持っているとします。この場合、この値が有効になっていると、デフォルトでローカルプロファイルが使用され、ユーザーストアに移行されます。このポリシー設定を有効にすると、ユーザープロファイルの作成時に使用されるローカルプロファイルをテンプレートプロファイルが上書きできるようになります。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定が構成されていない場合、テンプレートは使用されません。

テンプレートプロファイルが移動プロファイルを上書きする

この設定により、ユーザープロファイルの作成時にテンプレートプロファイルが移動プロファイルを上書きできるようになります。

ユーザーがCitrixユーザープロファイルを持たず、移動Windowsユーザープロファイルを持っているとします。この場合、この値が有効になっていると、デフォルトで移動プロファイルが使用され、ユーザーストアに移行されます。このポリシー設定を有効にすると、ユーザープロファイルの作成時に使用される移動プロファイルをテンプレートプロファイルが上書きできるようになります。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定が構成されていない場合、テンプレートは使用されません。

すべてのログオンでCitrix必須プロファイルとして使用されるテンプレートプロファイル

この設定により、Profile Managementはテンプレートプロファイルをすべてのユーザープロファイルを作成するためのデフォルトプロファイルとして使用できるようになります。

デフォルトでは、この設定は無効になっており、新しいユーザープロファイルは、ユーザーが最初にログオンするデバイス上のデフォルトユーザープロファイルから作成されます。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定が構成されていない場合、テンプレートは使用されません。

ストリーム配信ユーザープロファイルポリシー設定

このセクションには、Profile Management がストリーム配信ユーザープロファイルを処理する方法を指定するポリシー設定が含まれています。

常にキャッシュ

この設定は、ユーザーのログオン後、Profile Management がストリーム配信ファイルをできるだけ早くキャッシュするかどうかを指定します。ユーザーのログオン後にファイルをキャッシュすると、ネットワーク帯域幅が節約され、ユーザーエクスペリエンスが向上します。

この設定は、**プロファイルストリーミング**設定と組み合わせて使用します。

デフォルトでは、この設定は無効になっており、ユーザーのログオン後、ストリーム配信ファイルはできるだけ早くキャッシュされません。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、無効になります。

常にキャッシュするサイズ

この設定は、ストリーム配信されるファイルのサイズの下限を MB 単位で指定します。Profile Management は、このサイズ以上のファイルを、ユーザーのログオン後できるだけ早くキャッシュします。

デフォルトでは、値は 0 (ゼロ) に設定されており、プロファイル全体をキャッシュする機能が使用されます。プロファイル全体をキャッシュする機能が有効になっている場合、Profile Management は、ユーザーのログオン後、ユーザーストア内のすべてのプロファイルコンテンツをバックグラウンドタスクとしてフェッチします。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、無効になります。

プロファイルストリーミング

この設定は、Citrix®ストリーミングユーザープロファイル機能を有効または無効にします。有効にすると、プロファイルファイルとフォルダーは、ユーザーがログオン後にアクセスした場合にのみ、ユーザーストアからローカルコンピューターにフェッチされます。レジストリエントリと保留領域のファイルはすぐにフェッチされます。

デフォルトでは、プロファイルストリーミングは無効になっています。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、無効になります。

ストリーム配信ユーザープロファイルグループ

この設定は、Windows ユーザーグループに基づいて、OU 内のどのユーザープロファイルをストリーム配信するかを指定します。

有効にすると、指定されたユーザーグループ内のユーザープロファイルのみがストリーミングされます。その他のすべてのユーザープロファイルは通常どおり処理されます。

デフォルトでは、この設定は無効になっており、OU内のすべてのユーザープロファイルは通常どおり処理されます。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、すべてのユーザープロファイルが処理されます。

プロファイルストリーミング除外を有効にする

プロファイルストリーミング除外が有効になっている場合：

- Profile Managementは、除外リスト内のフォルダーをストリーミングしません
- ユーザーがログオンすると、すべてのフォルダーがユーザーストアからローカルコンピューターに即座にフェッチされます

詳細については、「ユーザープロファイルのストリーム」を参照してください。

ペンディングエリアロックファイルのタイムアウト

この設定は、ストレージサーバーが応答しなくなったときにユーザー ストアがロックされたままの場合に、保留領域からユーザー ストアにユーザーのファイルが書き戻されるまでの日数を指定します。この動作により、保留領域の肥大化が防止され、ユーザー ストアに常に最新のファイルが含まれるようになります。

デフォルトでは、この設定は1日（1）に設定されています。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、デフォルト値が使用されます。

ペンディングエリアのプロファイルストリーミングを有効にする

保留領域内のファイルとフォルダーのプロファイルストリーミング機能を有効にできます。

保留領域は、プロファイルストリーミングが有効になっている間、プロファイルの一貫性を確保するために使用されます。同時セッションで変更されたプロファイルファイルとフォルダーを一時的に保存します。

デフォルトでは、このポリシーは無効になっており、保留領域内のすべてのファイルとフォルダーはログオン時にローカルプロファイルにフェッチされます。このポリシーを有効にすると、保留領域内のファイルは要求されたときにのみローカルプロファイルにフェッチされます。同時セッションのシナリオで最適なログオンエクスペリエンスを確保するには、このポリシーをプロファイルストリーミングポリシーと組み合わせて使用します。

このポリシーは、フォルダーのプロファイルストリーミングを有効にするポリシーが有効になっている場合に、保留領域内のフォルダーに適用されます。

ユーザーパーソナライゼーションポリシー設定

Virtual Delivery Agent内でユーザーレイヤーのマウントを有効にするには、構成パラメータを使用して以下を指定します。

- ネットワーク上のどこでユーザーレイヤーにアクセスするか。
- 新しいユーザーレイヤーディスクがどのくらい大きくなるか。

そのため、利用可能なポリシーのリストには、次の2つのポリシーが表示されます。

- ユーザーレイヤーリポジトリパス - 「値」フィールドに「\\サーバー名またはアドレス\フォルダー名」の形式でパスを入力します。
- ユーザーレイヤーサイズ (GB) - デフォルトのユーザーレイヤーサイズである10 GBは、Citrix®が推奨する最小値です。ユーザーレイヤーは、スペースが使用されるにつれて設定されたサイズまで拡張するシンプロビジョニングディスクです。ユーザーレイヤーのサイズが小さくなることはありません。

> **注:**
>
> ユーザーレイヤーサイズを増やすと、新しいユーザーレイヤーに影響し、既存のユーザーレイヤーも拡張されます。レイヤーサイズを減らすと、新しいユーザーレイヤーのみに影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

> 詳細については、「ユーザーパーソナライゼーションレイヤー」を参照してください。

Virtual Delivery Agent ポリシー設定

Virtual Delivery Agent (VDA) セクションには、VDA とサイトのコントローラー間の通信を制御するポリシー設定が含まれています。

重要: 自動更新機能を使用しない場合、VDA が Delivery Controller™ に登録するには、これらの設定で提供される情報が必要です。この情報は登録に必要であるため、VDA のインストール中にこの情報を提供しない限り、グループポリシーエディターを使用して次の設定を構成する必要があります。

- コントローラー登録 IPv6 ネットマスク
- コントローラー登録ポート
- コントローラー SID
- コントローラー
- IPv6 コントローラー登録のみを使用する
- サイト GUID

コントローラー登録 IPv6 ネットマスク

このポリシー設定により、管理者は VDA を優先サブネットのみに制限できます（グローバル IP が登録されている場合でも）。この設定は、VDA が登録する IPv6 アドレスとネットワークを指定します。VDA は、指定されたネットマスクに一致する最初のアドレスにのみ登録します。この設定は、「IPv6 コントローラー登録のみを使用する」ポリシー設定が有効になっている場合にのみ有効です。

デフォルトでは、この設定は空白です。

コントローラー登録ポート

この設定は、**コントローラーの自動更新を有効にする** 設定が無効になっている場合にのみ使用してください。

この設定は、レジストリベースの登録を使用する際に、VDA がコントローラーに登録するために使用する TCP/IP ポート番号を指定します。

既定では、ポート番号は80に設定されています。

コントローラーSID

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用します。

この設定は、レジストリベースの登録を使用する場合にVDAがControllerに登録するために使用する、スペース区切りのコントローラーセキュリティ識別子（SID）のリストを指定します。この設定はオプションであり、登録に使用されるControllerのリストを制限するために**コントローラー**設定と組み合わせて使用できます。

既定では、この設定は空白です。

コントローラー

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用します。

この設定は、レジストリベースの登録を使用する場合にVDAがControllerに登録するために使用する、スペース区切りのコントローラー完全修飾ドメイン名（FQDN）のリストを指定します。この設定はオプションであり、**コントローラーSID**設定と組み合わせて使用できます。

既定では、この設定は空白です。

コントローラーの自動更新を有効にする

この設定により、VDAはインストール後にコントローラーに自動的に登録できるようになります。

VDAが登録されると、登録先のControllerは現在のコントローラーFQDNとSIDのリストをVDAに送信します。VDAはこのリストを永続ストレージに書き込みます。各Controllerは、90分ごとにサイトデータベースでController情報を確認します。次のいずれかが発生した場合、Controllerは更新されたリストを登録済みのVDAに送信します。

- 前回の確認以降にControllerが追加または削除された
- ポリシーの変更が発生した

VDAは、受信した最新のリストにあるすべてのコントローラーからの接続を受け入れます。

デフォルトでは、この設定は有効になっています。

IPv6コントローラー登録のみを使用

この設定は、VDAがControllerに登録するために使用するアドレス形式を制御します。

- 有効にすると、VDAはマシンのIPv6アドレスを使用してControllerに登録します。VDAがControllerと通信する場合、次のアドレス順序を使用します：グローバルIPアドレス、ユニークローカルアドレス（ULA）、リンクローカルアドレス（他のIPv6アドレスが利用できない場合）。
- 無効にすると、VDAはマシンのIPv4アドレスを使用してControllerに登録し、通信します。

デフォルトでは、この設定は無効になっています。

サイトGUID

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用してください。

この設定は、Active Directoryベースの登録を使用する際に、VDAがControllerに登録するために使用するサイトのグローバル一意識別子（GUID）を指定します。

デフォルトでは、この設定は空白です。

監視ポリシー設定

「**監視**」セクションには、プロセス、リソース監視、およびアプリケーション障害監視のポリシー設定が含まれています。

これらのポリシーのスコープは、以下に基づいて定義できます。

- サイト
- デリバリーグループ
- デリバリーグループの種類
- 組織単位
- タグ

プロセスおよびリソース監視のポリシー

CPU、メモリ、およびプロセスの各データポイントはVDAから収集され、監視データベースに保存されます。VDAからデータポイントを送信するとネットワーク帯域幅を消費し、それらを保存すると監視データベースの相当なスペースを消費します。特定のスコープ（たとえば、特定のデリバリーグループや組織単位）に対して、リソースデータまたはプロセスデータ、あるいはその両方を監視したくない場合を考慮してください。この場合、ポリシーを無効にすることをお勧めします。

プロセス監視を有効にする

この設定を有効にすると、VDAがインストールされているマシンで実行されているプロセスの監視が可能になります。CPUやメモリ使用量などの統計情報は監視サービスに送信されます。これらの統計情報は、Directorでのリアルタイム通知および履歴レポートに使用されます。

この設定のデフォルトは無効です。

リソース監視を有効にする

この設定を有効にすると、VDAがインストールされているマシンで重要なパフォーマンスカウンターの監視が可能になります。CPUやメモリ使用量、IOPS、ディスク遅延データなどの統計情報

は監視サービスに送信されます。これらの統計情報は、Directorでのリアルタイム通知および履歴レポートに使用されます。

この設定のデフォルトは「有効」です。

スケーラビリティ

CPUおよびメモリデータは、各VDAから5分間隔でデータベースにプッシュされます。プロセスデータ（有効な場合）は10分間隔でデータベースにプッシュされます。IOPSおよびディスク待機時間データは1時間間隔でデータベースにプッシュされます。

CPUとメモリデータ

CPUおよびメモリデータは、デフォルトで**有効**になっています。データ保持期間の値は次のとおりです（Platinumライセンス）：

データ粒度	日数
5分間データ	1日
10分間データ	7日間
1時間データ	30日間
1日データ	90日間

IOPSとディスク遅延データ

IOPSとディスク遅延データは、デフォルトで**有効**です。データ保持値は次のとおりです（Platinumライセンス）。

データ粒度	日数
時間別データ	3日間
日別データ	90日間

データ保持設定では、1つのVDAについて1年間で以下のデータを保存するために、約276 KBのディスク容量が必要です。

- CPU
- メモリ
- IOPS

- ディスク遅延データ

マシンの数	必要なストレージの概算
1	276 KB
1K	270 MB
40K	10.6 GB

プロセスデータ

プロセスデータはデフォルトで**無効**です。必要に応じて、一部のマシンでプロセスデータを有効にすることをお勧めします。プロセスデータのデフォルトのデータ保持設定は次のとおりです。

データ粒度	日数
10分データ	1日
1時間データ	7日

プロセスデータがデフォルトの保持設定で有効になっている場合、プロセスデータは1年間でVDAあたり約1.5 MB、ターミナルサービスVDA (TS VDA) あたり3 MBを消費します。

マシンの数	必要なストレージ容量 (概算) VDA	必要なストレージ容量 (概算) TS VDA
1	1.5 MB	3 MB
1K	1.5 GB	3 GB

注:

前述の数値にはインデックス領域は含まれていません。また、すべての計算は概算であり、展開によって異なります。

オプションの構成

必要に応じて、デフォルトの保持設定を変更できます。ただし、この構成は追加のストレージを消費します。以下の設定を有効にすることで、プロセス使用率データの精度を高めることができます。有効にできる構成は次のとおりです。

ENABLEMINUTELEVELGRANULARITYPROCESSUTILIZATION

ENABLEDAYLEVELGRANULARITYPROCESSUTILIZATION

これらの構成は、監視PowerShellコマンドレットから有効にできます: Set-MonitorConfiguration

アプリケーション障害監視のポリシー

アプリケーション障害タブには、デフォルトでMulti-session OS VDAからのアプリケーション障害のみが表示されます。アプリケーション障害監視の設定は、以下の監視ポリシーで変更できます。

アプリケーション障害の監視を有効にする

この設定を使用して、アプリケーションエラーまたは障害（クラッシュおよび未処理の例外）、あるいはその両方を監視するようにアプリケーション障害監視を構成します。 **値**を**None**に設定すると、アプリケーション障害監視が無効になります。 この設定のデフォルトは「Application faults only」です。

SINGLE-SESSION OS VDAでのアプリケーション障害の監視を有効にする

デフォルトでは、Multi-session OS VDAでホストされているアプリケーションからの障害のみが監視されます。Single-session OS VDAを監視するには、ポリシーを**Allowed**に設定します。 この設定のデフォルトは**Prohibited**です。

障害監視から除外されるアプリケーションのリスト

障害監視の対象としないアプリケーションのリストを指定します。 デフォルトでは、このリストは空です。

Analytics 用データ収集のポリシー

ANALYTICS 用 VDA データ収集

このポリシーを使用して、パフォーマンスおよびセキュリティ分析のためにVDAのパフォーマンスおよびセキュリティ関連メトリックをMonitorサービスが収集することを有効または無効にします。デフォルトでは、このポリシーは**Allowed**です。VDAからのデータ収集を停止するには、ポリシーを**Prohibited**に設定します。

セキュリティ監視のためのクリップボードプレースメタデータ収集

このポリシーを使用して、セキュリティ監視、監査、およびコンプライアンスのためにBrokerサービスによるクリップボードプレースメタデータ収集を有効または無効にします。デフォルトでは、このポリシーは**Enabled**です。VDAからのデータ収集を停止するには、ポリシーを**Disabled**に設定します。

パフォーマンス監視のための診断データ収集

このポリシーを使用して、監視サービスがセッション情報、UPM/EUEM サービスの状態、Microsoft Teams の最適化、接続プロトコルなどの診断データを収集できるようにします。デフォルトでは、このポリシーは**有効**です。VDA からのデータ収集を停止するには、ポリシーを**無効**に設定します。

ストレージ計画のヒント

グループポリシー。リソースデータまたはプロセスデータの監視に関心がない場合は、グループポリシーを使用して、いずれかまたは両方をオフにすることができます。詳細については、ポリシーの作成の**グループポリシー**セクションを参照してください。

データグルーミング。デフォルトのデータ保持設定を変更して、データを早期にグルーミングし、ストレージスペースを解放できます。グルーミング設定の詳細については、APIを使用したデータアクセスの「データの粒度と保持」を参照してください。

ワークスペース エンバイロメント マネジメント™ ポリシー設定

Workspace Environment Management (WEM) セクションには、WEMエージェントの動作を管理するのに役立つポリシー設定が含まれています。

(WEM サービスのみ) エージェントプロキシ構成

現在、DaaS 展開でのみ利用可能です。

WEMエージェントがCitrix Cloudと通信するために使用するプロキシサーバーを指定します。形式: `http://<FQDN or IP address>:<port number>` (例: `<http://10.108.125.51:8080>`)。

(オンプレミス WEM のみ) エージェントサービスポート

現在、DaaS 展開でのみ利用可能です。

WEM エージェントが WEM インフラストラクチャサーバーに接続するために使用するポートを指定します。デフォルトポートは **8286** で、`AgentPort` コマンドライン引数に対応します。

(オンプレミス WEM のみ) キャッシュデータ同期ポート

現在、DaaS 展開でのみ利用可能です。

(WEM 1912 以降に適用) WEM エージェントがローカルキャッシュを WEM インフラストラクチャサーバーと同期するために使用するポートを指定します。デフォルトポートは **8288** で、`CachedDataSyncPort` コマンドライン引数に対応します。

(WEM サービスのみ) Citrix Cloud Connector

WEM エージェントが接続する Citrix Cloud Connector マシンを指定します。高可用性を確保するために、各リソースの場所に少なくとも 2 つの Cloud Connector を展開してください。Cloud Connector とエージェントマシンが同じ AD ドメインにあることを確認してください。

基本展開用のカスタム設定

現在、DaaS 展開でのみ利用可能です。

基本的な展開に使用されるエージェント設定をカスタマイズします。利用可能な設定の詳細については、Workspace Environment Management のドキュメントを参照してください。

(WEMサービスのみ) CVADサービスからCitrix Cloud Connectorを検出する

現在、DaaS展開でのみ利用可能です。

Cloud Connectorが構成されていない場合に、WEMエージェントがCitrix DaaS展開からCloud Connectorを自動的に検出できるようにします。検出が成功すると、エージェントは対応するCloud Connectorマシンに接続します。

重要: この設定は、エージェントのインストール中にCloud Connectorが構成された場合、または**Citrix Cloud Connectors**ポリシー設定がすでに有効になっている場合には適用されません。

(オンプレミスWEMのみ) インフラストラクチャサーバー

現在、DaaS展開でのみ利用可能です。

WEMインフラストラクチャサーバーの完全修飾ドメイン名 (FQDN) またはIPアドレスを指定します。WEMエージェントはこのサーバーに接続して、構成を取得し、ローカルキャッシュを更新し、監視データを報告します。

エージェント展開タイプを上書きする

現在、DaaS展開でのみ利用可能です。

デフォルトのWEMエージェント展開タイプを上書きします。次のいずれかのオプションを選択してください。

- クラウドサービス – エージェントをCitrix CloudのWEMサービスに接続し、WEMの全機能を提供します。
- オンプレミス – エージェントをオンプレミスのWEM展開に接続し、WEMの全機能を提供します。

- 基本的な展開 – WEMインフラストラクチャに接続せずに、限られた機能でWEMをシングルマシンモードで実行します。
- 無効 – エージェントがインストールされているマシン上のすべてのWEM機能を無効にします。

レジストリを使用してCOMポートおよびLPTポートリダイレクト設定を構成する

VDAバージョン7.0から7.8では、**COMポートおよびLPTポート**の設定はレジストリを使用してのみ構成できます。VDAバージョン7.0より前、およびVDAバージョン7.9以降では、これらの設定はWeb Studioで構成できます。詳しくは、「ポートリダイレクトポリシー設定」および「帯域幅ポリシー設定」を参照してください。

COMポートおよびLPTポートリダイレクトのポリシー設定は、VDAイメージまたはマシン上のHKLM\Software\Citrix\GroupPolicy\Defaults\Deprecatedにあります。

COMポートおよびLPTポートリダイレクトを有効にするには、次のようにREG_DWORD型の新しいレジストリキーを追加します。

注意：レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤った使用によって生じた問題が解決できることを保証できません。レジストリエディターは、お客様ご自身の責任において使用してください。編集する前に、必ずレジストリをバックアップしてください。

レジストリキー	説明	許可される値
AllowComPortRedirection	COMポートリダイレクトを許可または禁止する	1 (許可) または 0 (禁止)
LimitComBw	COMポートリダイレクトチャネルの帯域幅制限	数値
LimitComBWPercent	COMポートリダイレクトチャネルの帯域幅制限（セッション全体の帯域幅に対する割合）	0～100の数値
AutoConnectClientComPorts	ユーザーデバイスからCOMポートを自動的に接続する	1（許可）または0（禁止）
AllowLptPortRedirection	LPTポートリダイレクトを許可または禁止する	1（許可）または0（禁止）

レジストリキー	説明	許可される値
LimitLptBw	LPTポートリダイレクトチャネルの帯域幅制限	数値
LimitLptBwPercent	LPTポートリダイレクトチャネルの帯域幅制限（セッション全体の帯域幅に対する割合）	0〜100の数値
AutoConnectClientLptPorts	ユーザーデバイスからLPTポートを自動的に接続する	1 (許可) または 0 (禁止)

これらの設定を構成した後、マシンカタログを新しいマスターイメージまたは更新された物理マシンを使用するように変更します。デスクトップは、ユーザーが次回ログオフしたときに新しい設定で更新されます。

ポリシーの変更

以下の表は、Citrix Virtual Apps and Desktops™ 7 2511におけるポリシーの更新（追加、削除、名前の変更、デフォルト状態の変更を含む）を示しています。

ポリシー設定	変更点
プロファイル管理 > 詳細設定 > マシン休止状態のマルチセッションサポートを有効にする	同時セッション休止状態を有効にするための新しいポリシーです。(/ja-jp/profile-management/current-release/whats-new#support-for-concurrent-session-hibernation-in-virtual-machines)。
クライアントプリンターポリシー設定 > 保持および復元されたクライアントプリンター	2402以降非推奨。

注：

- アップグレードする前に、すべての非推奨設定を削除してください。非推奨設定が使用されたままになっている場合、アップグレードはエラーで失敗する可能性があります。

- すでにアップグレード済みの場合は、アップグレード後に非推奨のポリシー設定を削除する を使用して、非推奨設定がまだ含まれているポリシーとテンプレートをクリーンアップしてください。

管理

Citrix Virtual Apps and Desktops™ サイトの管理には、さまざまな項目とタスクが含まれます。

ライセンス

サイトを作成する際には、Citrix License Serverへの有効な接続が必要です。その後、Studioからライセンスの追加、ライセンスの種類やモデルの変更、ライセンス管理者の管理など、いくつかのライセンス関連タスクを実行できます。StudioからLicense Administration Consoleにアクセスすることも可能です。

アプリケーション

Delivery GroupsおよびオプションでApplication Groups内のアプリケーションを管理します。

ゾーン

地理的に分散した展開では、ゾーンを使用してアプリケーションとデスクトップをエンドユーザーに近づけることで、パフォーマンスを向上させることができます。サイトをインストールして構成すると、すべてのController、マシンカタログ、およびホスト接続は1つのプライマリゾーンに配置されます。その後、Studioを使用して、これらの項目を含むサテライトゾーンを作成できます。サイトに複数のゾーンがある場合、新しく作成されたマシンカタログ、ホスト接続、または追加されたControllerをどのゾーンに配置するかを指定できるようになります。ゾーン間で項目を移動することもできます。

接続とリソース

ハイパーバイザーまたはその他のサービスを使用して、ユーザーにアプリケーションとデスクトップを提供するマシンをホストしている場合、サイトを作成する際に、そのハイパーバイザーまたはその他のサービスへの最初の接続を作成します。その接続のストレージとネットワークの詳細がそのリソースを構成します。その後、その接続とそのリソースを変更したり、さらに多くの接続を作成したりできます。構成された接続を使用するマシンを管理することもできます。

ローカルホストキャッシュ

Local Host Cacheを使用すると、Delivery Controller™とサイトデータベース間の接続が失敗した場合でも、サイト内の接続ブローカー操作を続行できます。

仮想IPと仮想ループバック

Microsoft仮想IPアドレス機能は、公開アプリケーションにセッションごとに一意の動的に割り当てられたIPアドレスを提供します。Citrix仮想ループバック機能を使用すると、localhostとの通信に依存するアプリケーションを、localhost範囲内の一意の仮想ループバックアドレスを使用するように構成できます。

デリバリーコントローラー

この記事では、サイトへのControllerの追加と削除に関する考慮事項と手順について説明します。また、Controllerを別のゾーンまたはサイトに移動する方法、およびVDAを別のサイトに移動する方法についても説明します。

ControllerへのVDA登録

VDAがアプリケーションとデスクトップの配信を支援する前に、Controllerに登録（通信を確立）する必要があります。Controllerのアドレスはいくつかの方法で指定でき、それについてはこの記事で説明します。サイトでControllerが追加、移動、削除される際に、VDAが最新の情報を持っていることが重要です。

セッション

セッションアクティビティを維持することは、最高のユーザーエクスペリエンスを提供するために不可欠です。いくつかの機能により、セッションの信頼性を最適化し、不便、ダウンタイム、生産性の損失を軽減できます。

- セッションの信頼性
- クライアントの自動再接続
- ICA®キープアライブ
- ワークスペースコントロール
- セッションローミング

Studioでの検索の使用

Studioでマシン、セッション、マシンカタログ、アプリケーション、またはデリバリーグループに関する情報を表示したい場合は、柔軟な検索機能を使用します。

タグ

タグを使用して、マシン、アプリケーション、グループ、ポリシーなどの項目を識別します。その後、特定のタグを持つ項目に適用されるように特定の操作を調整できます。

IPv4/IPv6

Citrix Virtual Apps™ and Desktops は、純粋な IPv4、純粋な IPv6、および IPv4 と IPv6 のネットワークが重複するデュアルスタック展開をサポートしています。この記事では、これらの展開について説明し、図解します。また、IPv4 または IPv6 の使用を制御する Citrix ポリシー設定についても説明します。

ユーザープロファイル

デフォルトでは、VDA をインストールすると Citrix Profile Management が自動的にインストールされます。このプロファイルソリューションを使用する場合は、一般的な情報についてこの記事を確認してください。詳細については、Profile Management のドキュメントを参照してください。

Citrix Diagnostic Facility (CDF) トレースの収集

CDFControl ユーティリティは、さまざまな Citrix トレースプロバイダーから表示される Citrix Diagnostic Facility (CDF) トレースメッセージをキャプチャするためのイベントトレースコントローラーまたはコンシューマーです。これは、複雑な Citrix 関連の問題のトラブルシューティング、フィルターサポートの解析、およびパフォーマンスデータの収集のために作成されています。

シトリックス インサイト サービス

Citrix Insight Services (CIS) は、計測、テレメトリ、およびビジネスインサイト生成のための Citrix プラットフォームです。

シトリックス スカウト

Citrix Scout は、診断情報を収集し、ヘルスチェックを実行します。その結果は、Citrix Virtual Apps and Desktops 展開におけるプロアクティブなメンテナンスに利用できます。Citrix は、Citrix Insight Services を通じて、診断コレクションの包括的な自動分析を提供します。また、Scout を使用して、単独で、または Citrix サポートのガイダンスを受けて、問題のトラブルシューティングを行うこともできます。

アプリケーション

> **注:**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™ の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除され

> ました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

展開でデリバリーグループのみを使用している場合（アプリケーショングループを使用していない場合）、アプリケーションをデリバリーグループに追加します。アプリケーショングループも使用している場合は、通常、代わりにアプリケーショングループにアプリケーションを追加します。このガイダンスにより、管理が容易になります。アプリケーションは常に、少なくとも1つのデリバリーグループまたはアプリケーショングループに属している必要があります。

アプリケーションの追加ウィザードでは、1つ以上のデリバリーグループ、または1つ以上のアプリケーショングループを選択できますが、両方は選択できません。後でアプリケーションのグループ関連付けを変更することはできますが（たとえば、アプリケーショングループからデリバリーグループにアプリケーションを移動するなど）、ベストプラクティスでは、そのような複雑さを追加することは推奨されません。アプリケーションは1種類のグループに保持してください。

アプリケーションを複数のグループに関連付けると、それらのすべてのグループでアプリケーションを表示するための十分な権限がない場合、表示の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが関連付けられているすべてのグループを含むようにスコープを拡張してください。

同じ名前の2つのアプリケーション（異なるグループからのものかもしれません）を同じユーザーに公開する場合、Web Studioで `Application name (for user)` プロパティを変更してください。そうしないと、ユーザーはCitrix Workspace™アプリで重複する名前を目にすることになります。

アプリケーションのプロパティ（設定）は、追加時または後で変更できます。アプリケーションが配置されているアプリケーションフォルダーも、アプリケーションの追加時または後で変更できます。

詳細については、以下を参照してください。

- デリバリーグループの作成
- アプリケーショングループの作成
- タグ

アプリケーションの追加

デリバリーグループまたはアプリケーショングループを作成するときに、アプリケーションを追加できます。これらの手順は、デリバリーグループの作成およびアプリケーショングループの作成で詳しく説明されています。次の手順では、グループを作成した後にアプリケーションを追加する方法について説明します。

知っておくと良いこと：

- Remote PC Accessデリバリーグループにアプリケーションを追加することはできません。
- アプリケーションの追加ウィザードを使用して、デリバリーグループまたはアプリケーショングループからアプリケーションを削除することはできません。これは別の操作です。

1つ以上のアプリケーションを追加するには：

1. 左ペインで**アプリケーション**を選択し、アクションバーで**アプリケーションの追加**を選択します。
2. アプリケーションの追加ウィザードが**はじめに**ページとともに起動します。このページは、今後のウィザードの起動時に表示しないように設定できます。
3. ウィザードは、**グループ**、**アプリケーション**、**概要**の各ページを案内します。各ページの作業が完了したら、**概要**ページに到達するまで**次へ**をクリックします。

単一のデリバリーグループまたはアプリケーショングループにアプリケーションを追加する場合の、手順1の代替案：

- **1つのデリバリーグループにのみアプリケーションを追加する場合：** 手順1で、Web Studioの左ペインで**デリバリーグループ**を選択し、中央ペインでデリバリーグループを選択してから、アクションバーで**アプリケーションの追加**を選択します。ウィザードには**グループ**ページは表示されません。
- **1つのアプリケーショングループにのみアプリケーションを追加する場合：** 手順1で、Web Studioの左ペインで**アプリケーション**を選択し、中央ペインでアプリケーショングループを選択してから、アクションバーのアプリケーショングループ名の下にある**アプリケーションの追加**エントリを選択します。ウィザードには**グループ**ページは表示されません。

グループページ

このページには、サイト内のすべてのデリバリーグループが一覧表示されます。アプリケーショングループも作成している場合は、アプリケーショングループとデリバリーグループが一覧表示されます。どちらかのグループを選択できますが、両方のグループを選択することはできません。つまり、アプリケーショングループとデリバリーグループに同時にアプリケーションを追加することは

できません。通常、アプリケーショングループを使用している場合は、デリバリーグループではなくアプリケーショングループにアプリケーションを追加します。

アプリケーションを追加するときは、少なくとも1つのデリバリーグループ（または、利用可能な場合はアプリケーショングループ）の横にあるチェックボックスを選択します。すべてのアプリケーションは、常に少なくとも1つのグループに関連付けられている必要があります。

アプリケーションページ

アプリケーションソースを表示するには、**追加**をクリックします。

- **スタートメニューから:** 選択したデリバリーグループ内のマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、「**OK**」をクリックします。

  このソースは、(1) 関連付けられたデリバリーグループがないアプリケーショングループを選択した場合、(2) 関連付けられたデリバリーグループにマシンが含まれていないアプリケーショングループを選択した場合、または (3) マシンが含まれていないデリバリーグループを選択した場合は選択できません。
- **手動で:** デリバリーグループ内のVDA上、またはネットワーク内の他の場所にあるアプリケーション。このソースを選択すると、アプリケーションを追加する方法を指定する新しいページが開きます。
  - 実行可能ファイルのパス、作業ディレクトリ、オプションのコマンドライン引数、および管理者とユーザーの表示名を入力します。
  - デリバリーグループ内のVDAからアプリケーションを選択します。これを行うには、「**参照**」をクリックし、VDAにアクセスするための資格情報を入力し、VDAに接続されるまで待ってから、VDAからアプリケーションを選択します。選択したアプリケーションのプロパティが、ページのフィールドに自動的に入力されます。
- **既存:** 以前にサイトに追加されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、「**OK**」をクリックします。

  サイトにアプリケーションがない場合、このソースは選択できません。
- **アプリケーションパッケージ:** App-V、MSIX、MSIX app attach、またはFlexAppアプリケーションパッケージ内のアプリケーション。このソースを選択すると、「**パッケージからアプリケーションを追加**」ページが起動します。アプリケーションパッケージのソースを選択し、表

示された結果から追加したいアプリケーションを選択して、「**OK**」を選択します。詳細については、「Appパッケージの展開と配信」を参照してください。

- **アプリケーショングループ:** アプリケーショングループ。このソースを選択すると、アプリケーショングループのリストが表示された新しいページが起動します。（表示には各グループ内のアプリケーションもリストされますが、個々のアプリケーションではなくグループのみを選択できます。）選択したグループ内の現在および将来のすべてのアプリケーションが追加されます。追加するアプリケーショングループのチェックボックスをオンにして、「**OK**」をクリックします。

  このソースは、(1) アプリケーショングループがない場合、または (2) 選択したデリバリーグループがアプリケーショングループをサポートしていない場合（例：静的に割り当てられたマシンを持つデリバリーグループ）は、選択できません。

表に記載されているように、「**追加**」リストの一部のソースは、そのタイプの有効なソースがない場合、選択できません。互換性のないソース（たとえば、アプリケーショングループにアプリケーショングループを追加できないなど）はリストに含まれません。選択したグループに既に追加されているアプリケーションは選択できません。

このページから、または後で、アプリケーションのプロパティ（設定）を変更できます。

デフォルトでは、追加されたアプリケーションは`Applications`という名前のアプリケーションフォルダーに配置されます。このページから、または後でアプリケーションを変更できます。アプリケーションを追加しようとして、同じ名前のアプリケーションが同じフォルダーに存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。提示された新しい名前を受け入れるか、拒否してアプリケーションの名前を変更するか、別のフォルダーを選択できます。たとえば、**Applications**フォルダーに`app`が既に存在し、そのフォルダーに`app`という名前の別のアプリケーションを追加しようとすると、新しい名前`app_1`が提示されます。

概要ページ

10個以下のアプリケーションを追加する場合、それらの名前は「**追加するアプリケーション**」にリストされます。10個を超えるアプリケーションを追加する場合、合計数が指定されます。

概要情報を確認し、**「完了」**をクリックします。

アプリケーションのグループ関連付けを変更する

アプリケーションを追加した後、そのアプリケーションが関連付けられているデリバリーグループとアプリケーショングループを変更できます。

アプリケーションを別のグループにドラッグできます。これは、アクションバーのコマンドを使用する代替手段です。

アプリケーションがアプリケーショングループを使用するか直接的かにかかわらず、複数のデリバリーグループに関連付けられている場合、グループの優先順位を使用して、複数のグループが評価される順序を指定できます。グループは、アクセスポリシー、ユーザーリスト、スマートアクセスタグなどの要因に基づいて考慮対象から除外でき、グループから選択される特定のマシンは、ゾーンの優先順位、起動準備状況、タグの制限などの要因によって影響を受ける可能性があります。デフォルトでは、すべてのグループの優先順位は0（最高）です。デリバリーグループの優先順位が同じ場合、最も負荷の低いデリバリーグループがアプリケーションの起動に選択されます。この場合、垂直ロードバランシングは考慮されません。

アプリケーションは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。(1) デリバリーグループに共有マシンが含まれており、XenDesktop 7.9より前の7.xバージョンで作成された場合、および (2) `Edit delivery group` 権限がある場合、デスクトップのみを配信する共有マシンを含むデリバリーグループも選択できます。プロパティダイアログがコミットされると、デリバリーグループの種類は自動的に `desktops and applications` に変換されます。

1. Web Studioにサインインし、左ペインで**アプリケーション**を選択し、アプリケーションを選択します。
2. アクションバーで**プロパティ**を選択します。
3. **グループ**ページを選択します。

    - グループを追加するには、**追加**をクリックし、**アプリケーショングループ**または**デリバリーグループ**を選択します。（アプリケーショングループを作成していない場合、唯一の項目は**デリバリーグループ**です。）次に、利用可能なグループを1つ以上選択します。アプリケーションと互換性のないグループ、またはすでにアプリケーションに関連付けられているグループは選択できません。
    - グループを削除するには、1つ以上のグループを選択し、**削除**をクリックします。グループの関連付けを削除した結果、アプリケーションがどのグループにも関連付けられなくなる場合、アプリケーションが削除されることを警告されます。
    - グループの優先順位を変更するには、グループを選択し、**優先順位の編集**をクリックします。優先順位の値を選択し、**OK**をクリックします。

4. 完了したら、**適用**をクリックして変更を適用しウィンドウを開いたままにするか、**OK**をクリックして変更を適用しウィンドウを閉じます。

アプリケーションの複製、有効化または無効化、名前変更、または削除

次のアクションが利用可能です。

- **複製：** アプリケーションを複製して、異なるパラメーターやプロパティを持つ別のバージョンを作成したい場合があります。アプリケーションを複製すると、一意のサフィックスで自動的に名前が変更され、元のアプリケーションの隣に配置されます。アプリケーションを複製してから、別のグループに追加したい場合もあります。(複製後、アプリケーションを移動する最も簡単な方法はドラッグすることです。)
- **有効化または無効化：** アプリケーションの有効化と無効化は、デリバリーグループまたはアプリケーショングループの有効化と無効化とは異なるアクションです。
- **名前の変更：** 一度に1つのアプリケーションのみ名前を変更できます。アプリケーションの名前を変更しようとして、同じ名前のアプリケーションが同じフォルダーまたはグループに存在する場合、別の名前を指定するように求められます。
- **削除：** アプリケーションを削除すると、関連付けられていたデリバリーグループおよびアプリケーショングループから削除されますが、元々アプリケーションを追加するために使用されたソースからは削除されません。アプリケーションの削除は、デリバリーグループまたはアプリケーショングループから削除するのとは異なるアクションです。

アプリケーションを複製、有効化、無効化、名前変更、または削除するには：

1. 左ペインで**「アプリケーション」**を選択します。
2. 中央ペインで1つ以上のアプリケーションを選択し、アクションバーで適切なタスクを選択します。
3. プロンプトが表示されたら、アクションを確認します。

デリバリーグループからアプリケーションを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに関連付けられている（属している）必要があります。アプリケーションをデリバリーグループから削除しようとして、そのアプリケーションがどのデリバリーグループまたはアプリケーショングループとも関連付けがなくなる場合、続行するとアプリケーションが削除されることが通知されます。その場合、そのアプリケーションを配信したい場合は、有効なソースから再度追加する必要があります。

1. 左側のペインで、 を選択します。
2. デリバリーグループを選択します。中央下のペインの タブで、削除するアプリケーションを選択します。
3. アクションバーから を選択します。

4. 削除を確認します。

アプリケーショングループからアプリケーションを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに属している必要があります。アプリケーションをアプリケーショングループから削除しようとしたときに、そのアプリケーションがどのグループにも属さなくなる場合、続行するとアプリケーションが削除されるという通知が表示されます。その場合、そのアプリケーションを配信したい場合は、有効なソースから再度追加する必要があります。

1. 左側のペインで、 を選択します。
2. 中央のペインでアプリケーショングループを選択し、1つまたは複数のアプリケーションを選択します。
3. アクションバーで を選択します。
4. 削除を確認します。

アプリケーションのプロパティを変更する

アプリケーションのプロパティは、一度に1つしか変更できません。

アプリケーションのプロパティを変更するには：

1. 左側のペインで を選択します。
2. アプリケーションを選択し、アクションバーで を選択します。
3. 変更するプロパティが含まれるページを選択します。
4. 完了したら、 をクリックして変更を適用し、ウィンドウを開いたままにするか、 をクリックして変更を適用してウィンドウを閉じます。

次のリストでは、ページが括弧内に表示されます。

プロパティ	ページ
アプリケーションがCitrix Workspaceアプリに表示されるカテゴリ/フォルダー	デリバリー
コマンドライン引数。「公開アプリケーションにパラメーターを渡す」を参照してください(#pass-parameters-to-published-applications)	場所

プロパティ	ページ
アプリケーションが利用可能なデリバリーグループとアプリケーショングループ	グループ
説明	識別
ファイル名拡張子とファイルの種類関連付け: アプリケーションが自動的に開く拡張子	ファイルの種類関連付け
アイコン	デリバリー
StoreFront™のキーワード	識別
制限。「アプリケーションの制限を構成する」を参照してください(#configure-application-limits)	配信
名前: ユーザーと管理者が参照する名前	識別
実行可能ファイルへのパス。「公開アプリケーションにパラメーターを渡す」を参照してください(#pass-parameters-to-published-applications)	場所
ユーザーのデスクトップ上のショートカット: 有効または無効	配信
可視性: Citrix Workspaceアプリでアプリケーションを表示できるユーザーを制限します。非表示のアプリケーションでも起動できます。利用不可かつ非表示にするには、別のグループに追加します。	可視性の制限
作業ディレクトリ	場所

アプリケーションの変更は、現在のアプリケーションユーザーがセッションからログオフするまで有効にならない場合があります。

アプリケーション制限を構成する

アプリケーションの使用状況を管理するために、アプリケーション制限を構成します。たとえば、アプリケーション制限を使用して、アプリケーションに同時にアクセスするユーザーの数を管理で

きます。同様に、アプリケーション制限を使用して、リソースを大量に消費するアプリケーションの同時インスタンスの数を管理できます。この制限は、サーバーのパフォーマンスを維持し、サービスの劣化を防ぐのに役立ちます。

この機能は、Controllerによって仲介されるアプリケーション起動の数（Citrix Workspaceアプリや StoreFrontなどから）を制限するものであり、他の方法で起動できる実行中のアプリケーションの数を制限するものではありません。これは、アプリケーション制限が同時使用を管理する際に管理者を支援するものの、すべてのシナリオで強制力を持つわけではないことを意味します。たとえば、Controllerが停止モードの場合、アプリケーション制限は適用できません。

デフォルトでは、同時に実行できるアプリケーションインスタンスの数に制限はありません。アプリケーション制限の設定はいくつかあります。それらのいずれか、またはすべてを構成できます。

- デリバリーグループ内のすべてのユーザーによる、アプリケーションの同時実行インスタンスの最大数。
- デリバリーグループ内のユーザーごとのアプリケーションインスタンス数。
- マシンごとのアプリケーションの同時実行インスタンスの最大数 (PowerShellのみ)。

制限が構成されている場合、ユーザーが構成された制限を超えるアプリケーションインスタンスを起動しようとすると、エラーメッセージが生成されます。複数の制限が構成されている場合、最初に到達した制限でエラーが報告されます。

アプリケーション制限の使用例:

- **同時インスタンス数の上限:** デリバリーグループで、アプリケーション `Alpha` の同時インスタンスの最大数を15に構成します。その後、そのデリバリーグループのユーザーは、そのアプリケーションの15個のインスタンスを同時に実行します。そのデリバリーグループのいずれかのユーザーが `Alpha` を起動しようとすると、エラーメッセージが生成されます。構成された同時アプリケーションインスタンスの制限 (15) を超えるため、`Alpha` は起動されません。
- **ユーザーごとのインスタンス数制限:** 別のデリバリーグループで、アプリケーション `Beta` のユーザーごとのインスタンス数オプションを有効にします。ユーザーのTonyはアプリケーション `Beta` を正常に起動します。その日の後半、そのアプリケーションがTonyのセッションでまだ実行されている間に、彼は `Beta` の別のインスタンスを起動しようとします。エラーメッセージが生成され、ユーザーごとのインスタンス数制限を超えるため、`Beta` は起動されません。
- **同時インスタンス数の上限とユーザーごとのインスタンス数制限:** 別のデリバリーグループで、同時インスタンスの最大数を10に構成し、アプリケーション `Delta` のユーザーごとのインスタンス数オプションを有効にします。その後、そのデリバリーグループの10人のユーザー

がそれぞれ `Delta` のインスタンスを実行しているときに、そのデリバリーグループの他のユーザーが `Delta` を起動しようとすると、エラーメッセージが表示されます。`Delta` は起動されません。現在の10人の `Delta` ユーザーのいずれかがそのアプリケーションの2番目のインスタンスを起動しようとすると、エラーメッセージが表示され、2番目のインスタンスは起動されません。

- **マシンごとの同時インスタンス数の上限とタグ制限の使用:** アプリケーション `Charlie` には、特定のサーバーで同時に実行できるインスタンスの数を規定するライセンスおよびパフォーマンス要件があります。これらの要件は、サイト内のすべてのサーバーで同時に実行できるインスタンスの数も規定します。

  アプリケーションのインスタンス数/マシン制限は、サイト内の任意のサーバーに影響します(特定のデリバリーグループ内のマシンだけでなく)。サイトに3台のサーバーがあるとします。アプリケーション `Charlie` の場合、マシンごとのアプリインスタンス制限を2に構成します。したがって、サイト全体でアプリケーション `Charlie` のインスタンスは6つまでしか起動できません。(これは、3台のサーバーそれぞれでCharlieのインスタンスが2つという制限です。)

  アプリケーションの使用をデリバリーグループ内の特定のコンピューターのみに制限するには(サイト全体のすべてのコンピューターでのインスタンス制限に加えて):

  - それらのマシンにタグ付け機能を使用します。
  - そのアプリケーションのマシンごとの最大インスタンス数を構成します。

アプリケーションがControllerの仲介以外の方法で起動され (たとえば、Controllerが停止モードの場合など)、構成された制限を超過した場合、ユーザーは制限を超過しないように十分なインスタンスを閉じるまで、それ以上のインスタンスを起動できません。制限を超過したインスタンスは強制的にシャットダウンされません。ユーザーがそれらを閉じるまで継続が許可されます。

セッションローミングを無効にする場合は、ユーザーごとのアプリケーションインスタンス数制限を無効にします。ユーザーごとのアプリケーションインスタンス数制限を有効にする場合は、新しいデバイスでの新しいセッションを許可する2つの値のいずれも構成しないでください。ローミングについて詳しくは、「セッション」を参照してください。

デリバリーグループあたりの最大インスタンス数制限と、ユーザーあたりのインスタンス数制限を構成するには：

1. 左側のペインで**アプリケーション**を選択し、アプリケーションを選択します。
2. アクションバーで**アプリケーションプロパティの編集**を選択します。
3. **デリバリー**ページで、次のいずれかのオプションを選択します。

- **アプリケーションの無制限の使用を許可する**。同時に実行されるインスタンスの数に制限はありません。これがデフォルトです。
- **アプリケーションの制限を設定する**。制限の種類は2つあります。いずれかまたは両方を指定します。
  - マシンごとに同時に実行できるインスタンスの最大数を指定します
  - ユーザーあたりのアプリケーションインスタンスを1つに制限する

4. **OK**をクリックして変更を適用し、ダイアログボックスを閉じるか、**適用**をクリックして変更を適用し、ダイアログボックスを開いたままにします。

マシンあたりの最大インスタンス数制限を構成するには（PowerShellのみ）：

- PowerShellで（Citrix Cloud™展開の場合はRemote PowerShell SDKを、オンプレミス展開の場合はPowerShell SDKを使用して）、適切な`BrokerApplication`コマンドレットを`MaxPerMachineInstances`パラメーターとともに実行します。
- ガイダンスについては、`Get-Help`コマンドレットを使用してください。例：

  `Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances`

公開アプリケーションにパラメーターを渡す

アプリケーションのプロパティの**場所**ページを使用して、コマンドラインを入力し、公開アプリケーションにパラメーターを渡します。

公開アプリケーションをファイルの種類に関連付けると、アプリケーションのコマンドラインの末尾に記号 `"%*"` (二重引用符で囲まれたパーセント記号とアスタリスク記号) が追加されます。これらの記号は、ユーザーデバイスに渡されるパラメーターのプレースホルダーとして機能します。

公開アプリケーションが期待どおりに起動しない場合は、そのコマンドラインに正しい記号が含まれていることを確認してください。デフォルトでは、記号 `"%*"` が追加されると、ユーザーデバイスから提供されたパラメーターが検証されます。ユーザーデバイスから提供されたカスタマイズされたパラメーターを使用する公開アプリケーションの場合、コマンドライン検証をバイパスするために、記号 `"%**"` がコマンドラインに追加されます。アプリケーションのコマンドラインにこれらの記号が表示されない場合は、手動で追加してください。

実行可能ファイルへのパスにスペースを含むディレクトリ名が含まれている場合 (`"C:\Program Files"` など)、そのスペースがコマンドラインの一部であることを示すために、アプリケーションのコマンドラインを二重引用符で囲みます。これを行うには、パスを二重引用符で囲み、`%*`

記号を別の二重引用符で囲みます。パスの閉じ引用符と `%*` 記号の開き引用符の間にスペースを含めるようにしてください。

たとえば、公開アプリケーションであるWindows Media Playerのコマンドラインは次のとおりです。

```
"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"
```

> **注：**
>
> 公開アプリケーションを起動するためのコマンドラインの最大文字数 (引数を含む) は203文字です。

公開アプリケーションでのセッションサインアウトの問題のトラブルシューティング

アプリケーションを公開する場合、公開アプリケーションのメインの実行可能ファイルのみが指定されます。ただし、一部のアプリケーションは、バックグラウンドで実行され、メインの公開アプリケーションが閉じられたときに、対応するメインの実行可能ファイルによって閉じられない追加の（子）プロセスを生成する場合があります。追加のプロセスは、実行されるスクリプトや、`Run` や `RunOnceKey` のような特定のレジストリキーから作成されることもあります。これらのアプリケーションは、正常なサインアウトを妨げ、セッションが残存したりハングしたりする原因となり、セッションが閉じられず、ユーザーがサインアウトされない可能性があります。

この場合、Citrix Director を使用してこれらのセッションをリセットまたは終了する必要があります。

セッションが適切にサインアウトされない問題を特定し、トラブルシューティングするために、Citrixは3つのレジストリエントリを提供しています。これらの問題によりセッションが適切にログオフされない場合の特定とトラブルシューティングは、次の3つのステップで行われます。

1. どのセッションの公開アプリケーションが正常なサインアウトを妨げているかを特定する
2. それらの公開アプリケーションが追加の（子）プロセスを生成するかどうかを特定する
3. これらのプロセスを指定されたレジストリエントリに追加して、サインアウトを妨げないようにする

ステップ2: 公開アプリケーションが追加の（子）プロセスを生成するかどうかを特定する

公開アプリケーションが正常なサインアウトを妨げていると特定されたら、次のステップは、このアプリケーションが実行時に追加のプロセスを生成するかどうかを判断することです。

公開アプリケーションが閉じられたときに、どのプロセスが正常なサインアウトをブロックしているかを判断するには、`HKCU\Software\CitrixVolatile\Seamless\Sessions\[ID]\LogoffCheckerBlockingProcess` を参照してください。

以下の例では、キー `LogoffCheckerBlockingProcess` に次のエントリが含まれています。

```
PhoneExperienceHost.exe

SkypeApp.exe

SkypeBackgroundHost.exe
```

これらのプロセスが正常なサインアウトを妨げていました。

> **注:**
>
> 確認したいセッションの正しいセッションIDで を置き換えてください。

ステップ3: これらのプロセスを指定されたレジストリエントリに追加して、サインアウトを妨げないようにする

今後のセッションでこれらのプロセスがサインアウトを妨げないように、以下のレジストリキーに追加できます。

```
Add the process file name to the following registry key:

Caution! Refer to the Disclaimer at the end of this article before using
the Registry Editor.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

Value Name:LogoffCheckSysModules

Type:REG_SZ
```

```
String:MyAppName.exe
```

`LogoffCheckSysModules` の詳細については、公開アプリケーションからの正常なログオフによりセッションがアクティブ状態になる を参照してください。

ステップバイステップのトラブルシューティングガイド

1. テスト対象のVDAでリモートレジストリサービスを開始します。
   a. コントロールパネルで、**管理ツール > サービス** を選択します。
   b. **リモートレジストリサービス** を右クリックし、**プロパティ** を選択します。
   c. **スタートアップの種類** で、ドロップダウンメニューから **自動** を選択します。

   公開アプリケーションレジストリ(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-registry.png)
2. テスト対象VDAのWindowsファイアウォールをオフにするか、ポート455を有効にする受信ファイアウォール規則を作成します。
   a. コントロールパネルで、**Windows Defender ファイアウォール > 詳細設定**を選択します。
   b. **受信の規則**を右クリックし、**新しい規則**を選択します。
   c. **新しい受信の規則ウィザード**で、**ポート**を選択します。
   d. **プロトコルおよびポート**ページで、**TCP および特定のローカルポート**を選択します。ローカルポートとして `445` を入力します。
   e. **操作**ページで、**接続を許可する**を選択します。
   f. 新しい受信規則を適用するファイアウォールプロファイルを選択します。
   g. ファイアウォール規則に名前を付け、**完了**を選択して**新しい受信の規則ウィザード**を終了します。

   公開アプリケーションファイアウォールポート(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-firewall-port.png)
3. 同じドメイン上の別のVM（DC、DDC、または別のVDAでも可）から、`Regedit` を実行し、リモートレジストリに接続します。

   公開アプリケーションレジストリエディター(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-registry-editor.png)
4. テスト対象VDAのIPアドレスを入力し、**OK**をクリックします。`regedit` ツリーには、テスト対象VDAのブランチが表示されるはずです。

公開アプリケーションregedit(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-regedit.png)

5. **コマンドプロンプト**公開アプリケーションを開きます。

   「公開アプリの管理」(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-manage.png)

   コマンドプロンプトアプリがCitrix Workspaceに表示されます。

   「公開アプリのコマンドプロンプト」(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-cmd-prompt.png)

6. クライアントで**Connection Center**を開きます。これは、開いているシームレスアプリを閉じた後、セッションがサインアウトされたときに監視するために使用されます。次の画像で、コマンドプロンプトプロセス`c:\Windows\system32\cmd.exe`がリモートVDIでアクティブになっていることがわかります。

   「公開アプリの接続」(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-citrix-workspace-connection-center.png)

7. **regedit** が実行されている VDA から、次のリモート IP の場所に移動します。
   `HKEY_USERS\S-1-X-XX-XXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXX\SOFTWARE\CitrixVolatile\Seamless\Sessions\X\`

   > **注：**
   >
   > 新しいセッションを開くたびにこのパスは変更されます。

8. ここには読み取るべき2つのキーがあります（ここでは変更しないでください）：**LogoffCheckBlockingProcess**と**LogoffCheckerBlockingVisibleProcess**。これらのキーは、サインアウトをブロックしているプログラムを表示します。最初のキーは、開いていてまだ閉じられていないため、`C:\Windows\System32\cmd.exe`を表示する必要があります。

   > **注：**
   >
   > **LogoffCheckBlockingProcess**と**LogoffCheckerBlockingVisibleProcess**は手動で編集してはいけません。これらのレジストリ値を手動で編集すると、セッションが不安定になる可能性があります。

> 「公開アプリ2」(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-regedit-2.png)

9. 右上隅の **X** をクリックして **Seamless CMD** を終了します。
10. Connection Centerを確認して、セッションが閉じているか確認します。閉じるまでに最大30秒かかる場合があります。閉じている場合、正常なサインアウトを妨げたアプリケーションやプロセスはありませんでした。

    「正常なサインアウト」(/en-us/citrix-virtual-apps-desktops/2511/media/published-app-bwd.png)
11. セッションが閉じなかった場合は、F5 キーで **regedit** の出力を更新します。
12. **LogoffCheckBlockingProcess**と**LogoffCheckerBlockingVisibleProcess**の内容を再度確認します。CMDは存在しないはずですが、別のプロセスがリストされているはずです。現在セッションのサインアウトをブロックしているプロセスがここに表示されているはずです。

    この場合、コマンドプロンプトが閉じられる前に、公開されたコマンドプロンプトから**Notepad.exe**が開かれており、このリモートのメモ帳プロセスが正常なサインアウトを妨げています。

    レジストリエディター(/en-us/citrix-virtual-apps-desktops/2511/media/regedit2.png)
13. この実行可能ファイルのパスと、それが出現したキーをメモし、リモートツリーの下にある以下のレジストリキーに入力します。

    - **LogoffCheckBlockingProcess**に表示される場合：
      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckSysModulesInterna`
    - **LogoffCheckerBlockingVisibleProcess**に表示される場合：
      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckVisibleSysModules`

    > **注：**
    >
    > キーにすでに1つ以上のエントリがある場合は、末尾にコンマを追加し、そのコンマの後に新しいエントリを配置します。

    > レジストリエディター - 最終(/en-us/citrix-virtual-apps-desktops/2511/media/regedit-final.png)
14. クライアントの接続センターからセッションをサインアウトし、リモートアプリケーションを再度開きます。

15. リモートアプリケーションを閉じてから30秒以内にセッションが自動的にサインアウトされるまで、ステップ9〜16を繰り返します。

> **注：**
>
> トラブルシューティング後、必要に応じてリモートレジストリへのアクセスを許可するために、一時的なファイアウォールの変更を元に戻します。

公開アプリケーションを開く際にWindowsの免責事項メッセージをフルサイズで表示するようにLogonUIを変更する方法

認証パススルーが発生しないシナリオでは、**LogonUI** ウィンドウのスケーリングが改善されました。**LogonUI** ウィンドウは、使用されているモニターの解像度とDPI設定に基づいてスケーリングされ、**LogonUI** ウィンドウ全体がクリッピングなしで表示されるようにします。

ウィンドウのサイズは、レジストリで手動でピクセル単位で設定することもできます。

1. **ファイル名を指定して実行**コマンドで `regedit` を使用して、**レジストリエディター**を開きます。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\` にアクセスします。
3. 2つの新しいDWORDキー、**LogonUIWidth**と**LogonUIHeight**を作成します。
4. キーの値を、**LogonUI** ウィンドウに必要な幅と高さ（ピクセル単位）に設定します。

   LogonUI ウィンドウのサイズを手動で設定すると、自動スケーリングは無効になります。

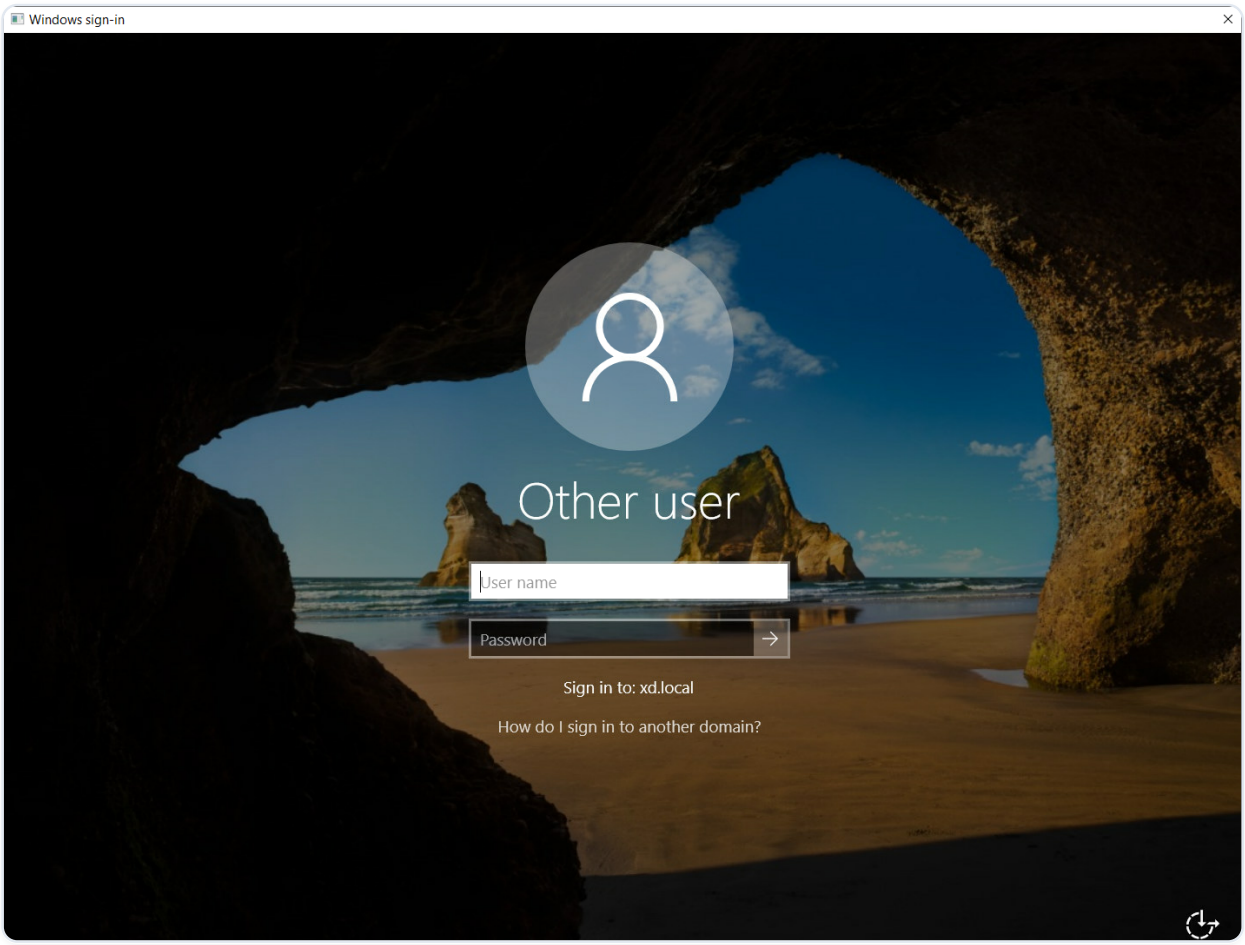
> **注:**
>
> これらのレジストリパスは2407以降変更されました。古いレジストリ値は無視され、非推奨です。

> デフォルトでは、**LogonUI** ウィンドウにはタイトルバーと閉じるボタンが含まれており、必要に応じてエンドユーザーがセッションから切断できるようになっています。

タイトルバーを無効にする

以下のレジストリキーを使用して、**LogonUI** ウィンドウのタイトルバーを無効にできます。

1. **ファイル名を指定して実行**コマンドで`regedit`を使用して、レジストリエディターを開きます。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`にアクセスします。
3. 新しいDWORDキー**LogonUICaption**を作成し、キーの値を`0`に設定します。



アプリケーションフォルダーの管理

デフォルトでは、デリバリーグループに追加する新しいアプリケーションは、**Applications**という名前のフォルダーに配置されます。デリバリーグループの作成時、アプリケーションの追加時、または後で別のフォルダーを指定できます。

知っておくと良いこと:

- Applicationsフォルダーの名前を変更したり削除したりすることはできませんが、その中に含まれるすべてのアプリケーションを、作成した他のフォルダーに移動することはできます。
- フォルダー名には1～64文字を含めることができます。スペースも使用できます。
- フォルダーは最大5レベルまでネストできます。
- フォルダーにアプリケーションを含める必要はありません。空のフォルダーも許可されます。

- フォルダーは、移動したり、作成時に別の場所を指定したりしない限り、Web Studioでアルファベット順に表示されます。
- 親フォルダーが異なる限り、同じ名前のフォルダーを複数持つことができます。同様に、異なるフォルダーにある限り、同じ名前のアプリケーションを複数持つことができます。
- フォルダー内のアプリケーションを表示するには`View Applications`権限が必要です。また、アプリケーションを含むフォルダーを削除、名前変更、または削除するには、そのフォルダー内のすべてのアプリケーションに対して`Edit Application Properties`権限が必要です。
- 以下のほとんどの手順では、Web Studioのアクションバーを使用してアクションを要求します。または、右クリックメニューを使用するか、アイテムをドラッグすることもできます。たとえば、意図しない場所にフォルダーを作成または移動した場合、ドラッグアンドドロップで正しい場所に移動できます。
- Web Studioのすべてのノード（**マシンカタログ**、**デリバリーグループ**、**アプリケーション**、**アプリケーショングループ**など）は、バックエンドで同じフォルダーツリーを共有します。フォルダーの名前変更や移動時に名前の競合を避けるため、異なるノード間で最上位フォルダーに一意の名前を使用してください。

  `New-BrokerAdminFolder` SDK コマンドレットを使用してフォルダーを作成し、それを**アプリケーション**ノードの下に表示させたい場合は、`Set-BrokerAdminFolderMetadata`コマンドレットを使用して`ContainsApplications`メタデータを追加する必要があります。

  例:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsApplications -Value true
  ```

アプリケーションフォルダーを管理するには、左ペインで**アプリケーション**を選択します。以下のリストを参考にしてください。

- **すべてのフォルダーを表示するには（ネストされたフォルダーを除く）：** フォルダーリストの上にある**すべて表示**をクリックします。
- **最上位レベルにフォルダーを作成するには（ネストしない）：** **アプリケーション**フォルダーを選択します。新しいフォルダーを**アプリケーション**以外の既存のフォルダーの下に配置するには、そのフォルダーを選択します。次に、アクションバーで**フォルダーの作成**を選択します。名前を入力します。
- **フォルダーを移動するには：** フォルダーを選択し、アクションバーで**フォルダーの移動**を選択します。フォルダーにネストされたフォルダーが含まれていない限り、一度に1つのフォル

ダーしか移動できません。（フォルダーを移動する最も簡単な方法は、ドラッグすることです。）」

- **フォルダーの名前を変更するには：** フォルダーを選択し、アクションバーで**フォルダー名の変更**を選択します。名前を入力します。
- **フォルダーを削除するには：** フォルダーを選択し、アクションバーで**フォルダーの削除**を選択します。アプリケーションやその他のフォルダーを含むフォルダーを削除すると、それらのオブジェクトも削除されます。アプリケーションを削除すると、デリバリーグループからのアプリケーション割り当てが削除されます。ただし、マシンからは削除されません。
- **アプリケーションをフォルダーに移動するには：** 1つまたは複数のアプリケーションを選択します。次に、アクションバーで**アプリケーションの移動**を選択します。フォルダーを選択します。

デリバリーグループまたはアプリケーショングループを作成する際に、**アプリケーション**ページで追加するアプリケーションをフォルダーに配置することもできます。デフォルトでは、追加されたアプリケーションは**アプリケーション**フォルダーに入ります。**変更**をクリックしてフォルダーを選択または作成します。

公開デスクトップでのアプリケーションのローカル起動を制御する

ユーザーが公開デスクトップ内から公開アプリケーションを起動する際、そのデスクトップセッションでアプリケーションを起動するか、公開アプリケーションとして起動するかを制御できます。Citrix Workspaceアプリは、VDA上のWindowsレジストリでアプリケーションのインストールパスを検索し、存在する場合はアプリケーションのローカルインスタンスを起動します。それ以外の場合は、ホストされたアプリケーションのインスタンスが起動されます。VDAにインストールされていないアプリケーションを起動すると、ホストされたアプリケーションが起動されます。詳細については、「vPrefer起動」を参照してください。

PowerShell（Citrix Cloud展開ではRemote PowerShell SDK、オンプレミス展開ではPowerShell SDKを使用）で、このアクションを変更できます。

`New-Broker`アプリケーションまたは`Set-BrokerApplication`コマンドレットで、`LocalLaunchDisabled`オプションを使用します。例：

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

デフォルトでは、このオプションの値はfalse（`-LocalLaunchDisabled $false`）です。公開デスクトップ内から公開アプリケーションを起動すると、そのデスクトップセッションでアプリケーションが起動されます。

オプションの値をtrue（`-LocalLaunchDisabled $true`）に設定すると、公開アプリケーションが起動されます。これにより、公開デスクトップから（Windows用Citrix Workspaceアプリを使用して）公開アプリケーションへの個別の追加セッションが作成されます。

要件と制限事項:

- アプリケーションの`ApplicationType`値は`HostedOnDesktop`である必要があります。
- このオプションは、適切なPowerShell SDKを介してのみ利用可能です。現在、Web Studioのグラフィカルインターフェイスでは利用できません。
- このオプションには、最低限StoreFront 3.14、Citrix Receiver for Windows 4.11、およびDelivery Controller 7.17が必要です。

アプリケーションパッケージ

アプリケーションパッケージは、Citrix®が管理する事前構成済みのアプリケーション展開です。これにより、アプリケーションを仮想化でき、ユーザーデバイスのオペレーティングシステムやインターフェイスから独立してアプリケーションが実行されることを意味します。

アプリケーションパッケージは、アプリケーション管理を簡素化し、ITオーバーヘッドを削減し、アプリケーションがライフサイクル全体を通じて安全かつ機能的であることを保証します。

Citrix は、ユーザーにアプリケーションを配信するために、以下のパッケージングテクノロジーをサポートしています。

- App-Vアプリケーション
- MSIXおよびMSIX app attachアプリケーション
- FlexAppアプリケーション
- Elastic Appアプリケーション
- Cloudpagingアプリケーション

この記事では、Citrix Virtual Apps and Desktops™ 環境でこれらのパッケージ化されたアプリケーションを展開および配信する方法について説明します。

> **注:**
>
> - バージョン2511以降、Citrix Virtual Apps and Desktops™の唯一の管理コンソールはCitrix Web Studio（Webベース）です。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情

報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

- アプリケーションパッケージの展開と配信にWeb StudioとCitrix Studioを相互に利用することはお勧めしません。それぞれ異なるメカニズムを使用しているため、App-Vサーバー情報が一方では正しく表示されるが、もう一方では表示されないといった不一致が生じる可能性があります。また、Citrix StudioはApp-Vのみをサポートしていることにも注意してください。

App-V アプリケーション

Application Virtualization (App-V) は、エンドユーザーのデバイスにインストールすることなく、アプリケーションをストリーミングしてアクセスできるようにする Microsoft のテクノロジーです。Citrix Virtual Apps and Desktops は App-V を使用してアプリケーションを配信でき、さまざまなクライアントマシン間でアプリケーションを管理するための集中化された効率的な方法を提供します。

App-Vパッケージアプリケーションを配信する際に操作するコンポーネントと概念の詳細については、Microsoftのドキュメント: Windowsクライアント向けApplication Virtualization (App-V) の概要を参照してください。

重要な用語

- **管理サーバー**: App-Vインフラストラクチャを管理するための一元化されたコンソールを提供し、App-Vデスクトップクライアントとリモートデスクトップサービスクライアントの両方に仮想アプリケーションを配信します。App-V管理サーバーは、管理者が要求するセキュリティ、メータリング、監視、データ収集を認証、要求、提供します。このサーバーは、Active Directoryとサポートツールを使用してユーザーとアプリケーションを管理します。
- **公開サーバー**: 特定のユーザー向けにApp-Vクライアントにアプリケーションを提供し、ストリーミング用の仮想アプリケーションパッケージをホストします。管理サーバーからパッケージを取得します。
- **動的構成ファイル**: App-Vパッケージは、動的構成ファイルを使用してカスタマイズできます。これらのファイルは、パッケージに適用されると、その特性を変更するために使用できます。たとえば、追加のアプリケーションショートカットや動作を定義するために使用できます。詳細については、「動的構成ファイル」(#dynamic-configuration-files)を参照してください。

動的構成ファイル

Citrix App-Vは、両方の種類の動的構成ファイルをサポートしています。ファイル設定は、アプリケーションの起動時に適用されます。

- **展開構成ファイル**は、すべてのユーザーに対してマシン全体の構成を提供します。これらのファイルは`<packageFileName>_DeploymentConfig.xml`という名前で、適用されるApp-Vパッケージと同じフォルダーにあることが想定されています。これらのファイルは、シングルおよびデュアル管理管理でサポートされています。
- **ユーザー構成ファイル**は、パッケージに対するユーザーごとのカスタマイズをサポートするユーザー固有の構成を提供します。シングル管理は、`<packageFileName>_[UserSID | Username | GroupSID |GroupName_]UserConfig.xml`という形式で命名され、適用されるApp-Vパッケージと同じフォルダーにあるユーザー構成ファイルをサポートします。

  特定のパッケージに対して複数のユーザー構成ファイルが存在する場合、それらは次の優先順位で適用されます。

  a. ユーザーSID
  b. ユーザー名
  c. ADグループSID（最初に見つかったものが優先）
  d. ADグループ名（最初に見つかったものが優先）
  e. デフォルト

  例:

  ```
  MyAppVPackage_S-1-5-21-000000001-0000000001-000000001-001_UserConfig.xml

  MyAppVPackage_joeblogs_UserConfig.xml

  MyAppVPackage_S-1-5-32-547_UserConfig.xml

  MyAppVPackage_Power Users_UserConfig.xml

  MyAppVPackage_UserConfig.xml
  ```

  注:

  ファイル名のユーザー固有の部分は、オプションで末尾に配置することもできます (例: `MyAppVPackage_UserConfig_joeblogs.xml`)。

> **重要:**
>
> パッケージ内のアプリケーションでユーザーセッションが開いている場合、動的展開構成に変更を適用することはできません。他のユーザー (ただし現在のユーザーではない) がパッケージ内のアプリケーションを開いている場合は、動的ユーザー構成ファイルに変更を適用できます。

動的構成ファイルの場所

単一管理者管理では、Citrix App-Vコンポーネントは、App-Vパッケージと同じフォルダーにある動的構成ファイルのみを処理します。

パッケージ内のアプリケーションが起動されると、対応する動的構成ファイルへの変更が再適用されます。動的構成ファイルがパッケージとは異なる場所にある場合は、マッピングファイルを使用してパッケージを展開構成ファイルにマッピングします。

マッピングファイルを作成するには:

1. 新しいテキストファイルを開きます。
2. 各動的構成ファイルについて、`<PackageGuid> : path`の形式を使用してパッケージへのパスを指定する行を追加します。

   例:

   ```
   F1f4fd78ef044176aad9082073a0c780 : c:\widows\file\packagedeploy.xml
   ```

3. ファイルを`ctxAppVDynamicConfigurations.cfg`として、パッケージと同じフォルダーに保存します。

App-VパッケージとUNC共有上のディレクトリ階層全体が、パッケージ内のアプリケーションが起動されるたびに、このファイルを求めて再帰的に上位検索されます。

方法

App-Vパッケージを配信および管理するには、次の方法を使用できます:

- **デュアル管理者**: この方法では、Citrix Virtual Apps and Desktops と App-V サーバーが連携してパッケージを配信および管理します。この方法では、Citrix Virtual Apps and Desktops が App-V サーバーの状態のスナップショットビューを定期的に更新する必要があります。これには、ハードウェア、インフラストラクチャ、および管理のオーバーヘッドが発生します。Citrix

Virtual Apps and Desktops と App-V サーバーは、特にユーザー権限に関して同期を維持する必要があります。

この方法は、App-VとCitrixが密接に連携する展開で最適に機能します。この方法では:

- **App-V管理サーバー**が動的構成ファイルを処理します。
- **VDAマシンにインストールされているApp Packages Delivery Component**: アプリケーションの起動に必要な適切な公開サーバーの登録を管理します。

これにより、適切なタイミングでユーザーに対して公開サーバーが同期されます。公開サーバーは、構成されている設定を使用して、アプリパッケージのライフサイクル（ログオン時の更新や接続グループなど）の他の側面を維持します。

- **シングル管理者**: アプリケーションパッケージはネットワーク共有に保存されます。Citrix Virtual Apps and Desktops は、パッケージを独立して配信および管理します。

  この方法により、展開においてApp-Vサーバーとデータベースインフラストラクチャが不要になるため、オーバーヘッドが削減されます。

  この方法では、App-Vパッケージをネットワーク共有に保存し、その場所からメタデータを環境にアップロードします。その後、VDAマシンにインストールされているApp Packages Delivery Componentが、次のようにアプリケーションを管理および配信します。

  - アプリケーションが起動されたときに、展開構成ファイルとユーザー構成ファイルを処理します。
  - ホストマシン上のパッケージのライフサイクルのすべての側面を管理します。

注：

- 両方の管理方法を同時に使用できます。つまり、アプリケーションをデリバリーグループに追加する場合、アプリケーションはApp-Vサーバーまたはネットワーク共有にあるApp-Vパッケージから取得できます。
- 両方の管理方法を同時に使用していて、App-Vパッケージが両方の場所に動的構成ファイルを持っている場合、App-Vサーバー（デュアル管理）のファイルが使用されます。
- Web StudioのナビゲーションペインでApp packagesを選択すると、パッケージ名と種類が表示されます。**パッケージの種類**列は、パッケージの配信に使用されるテクノロジーと、**アプリケーションライブラリ**で参照されている場所を示します。パッケージを選択

すると、詳細ペインにパッケージ内のアプリケーションとショートカットが一覧表示されます。

MSIXおよびMSIXアプリアタッチアプリケーション

MSIXは、すべてのWindowsアプリに最新のパッケージングエクスペリエンスを提供するWindowsアプリパッケージ形式です。MSIXは、Win32、.NET、UWPアプリなど、さまざまなWindowsアプリケーションタイプに適しています。

MSIXアプリアタッチは、仮想ハードディスクに事前に展開されたMSIXパッケージを利用します。これにより、パッケージの内容をストリーミングするのではなく、必要に応じてターゲットマシンにマウントできます。展開時間の短縮、ネットワークトラフィックの削減、ターゲットマシンでのIOPSの低減に貢献できますが、アプリアタッチディスクの作成と維持には追加の作業が必要です。

Citrix Virtual Apps and Desktopsは、VDAマシンにインストールされている**App Packages Delivery Component**を介して、MSIXおよびMSIXアプリアタッチアプリケーションをユーザーに提供します。このコンポーネントは、ホストマシン上のパッケージのライフサイクルのあらゆる側面を管理します。

MSIXおよびMSIXアプリアタッチの詳細については、Microsoftのドキュメント: MSIX documentation および App Attach in Azure Virtual Desktop をそれぞれ参照してください。

注記:

- デスクトップおよびサーバーVDA上のネイティブMSIXパッケージと、デスクトップVDAのみで、`.vhd`、`.vhdx`、および`.cim`ディスクイメージ形式のMSIXアプリアタッチをサポートしています。
- MicrosoftはServer 2019向けにAppAttachの実装を提供していません。AppAttachはServer 2022および2025に存在しますが、Microsoftはこれらのバージョンでのサポートを提供していません。したがって、弊社もServer 2022および2025でのAppAttachをサポートしていません。
- Windows Server 2019でサイドローディングを有効にします。
- VDAがパッケージの署名に使用されている証明書を信頼していることを確認してください。

FlexAppアプリケーション

FlexAppは、Liquidwareが開発したアプリケーションレイヤリングソリューションで、従来のアプリケーションインストールプロセスを介して基盤となるベースイメージを変更することなく、任意のアプリケーションをWindowsセッションにアタッチします。

FlexApp Oneアプリケーションは、単一の共有可能なファイルにカプセル化されており、Windowsセッションに追加のアプリケーションレイヤーを必要とせずに動作できます。ユーザーはコンテナファイルをクリックしてアプリケーションを起動でき、これにより1つまたは複数のアプリケーションがWindowsワークスペースに迅速に統合されます。

Citrixは、VDAマシンにインストールされているApp Packages Delivery ComponentとFlexApp配信エージェントを介して、FlexAppアプリケーションをユーザーに提供します。これら2つのコンポーネントは、ホストマシン上のパッケージのライフサイクルのあらゆる側面を管理します。

Elastic Appアプリケーション

Elastic App technology は、Citrix App Layering の機能であり、アプリケーションレイヤーをベースイメージにインストールするのではなく、ログオン時にユーザーに動的に割り当てることができます。Elastic App technology を使用すると、アプリケーションは異なる仮想マシン間でユーザーに追従し、マスターイメージを肥大化させることなく、必要なアプリに常にアクセスできるようにします。

Citrix Virtual Apps and Desktops は、Citrix Personalization コンポーネントと Application Layering Enterprise Layer Manager (ELM) を介して、Elastic App アプリケーションをユーザーに提供します。これら2つのコンポーネントは、ホストマシン上のパッケージのライフサイクルのあらゆる側面を管理します。Application Layering Enterprise Layer Manager の詳細については、Citrix App Layering™ ドキュメントを参照してください。

Cloudpaging アプリケーション

Cloudpaging は、Numecent のアプリケーションストリーミングテクノロジーであり、ベースイメージに変更を加えることなく、Windows セッションにアプリケーションを配信します。

Cloudpaging を使用すると、コードのごく一部（通常は10%未満）のみが最初にストリーミングされるため、アプリケーションはほぼ瞬時に起動します。残りのコンポーネントは、ユーザーがアクセスしたときにバックグラウンドでストリーミングされ、シームレスなエクスペリエンスを提供します。

Citrix 環境では、VDA 上の App Packages Delivery Component が Numecent Cloudpaging Player と連携してアプリケーションのライフサイクルを管理します。Citrix コンポーネントが配信をオー

ケストレーションし、Cloudpaging Player がセッション内でのオンデマンドストリーミングと実行を処理します。

構成要件

次の構成の詳細を考慮してください。

クラウドページング プレイヤー と LOGOFFCHECKSYSMODULES

Cloudpaging コンテナで仮想公開アプリケーションを使用する場合、セッションのログオフを許可するには、次の設定を構成します。

設定	値
レジストリキー	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI`
値の名前	`LogoffCheckSysModules`
値の型	`REG_SZ`
値のデータ	`CoreHelper.exe`

ホワイトリスト登録用のURL

標準のURLホワイトリスト登録要件に加えて、VDAは次のエンドポイントへのアクセスを必要とします。

パラメーター	値
URL	`external-api.cloudpager.net`
ポート	443
クライアント	Cloudpager PoSh モジュール
Webベースのフォワードプロキシ構成	• アウトバウンドアクセスが許可されている • 認証バイパスが必要
説明	Cloudpager PowerShellモジュール

オプションで、Cloudpagerの検出のみを実行するために使用されるVDAを持つ専用のデリバリーグループを作成し、必要なホワイトリスト登録済みURLを制限できます。**VDAバージョン2511以降**と**App packages Delivery Component**がインストールされているマシンでデリバリーグループを作成することをお勧めします。

Cloudpagerクライアントのネットワークおよびファイアウォールの要件の詳細については、Numecentナレッジベースの記事を参照してください。

アプリケーションパッケージの展開と配信

前提条件

App-V、MSIX、MSIX app attach、FlexAppパッケージ、Elastic Appアプリケーション、およびCloudpagingパッケージの配信をサポートするには、まずVDAマシンに**App Packages Delivery Component**をインストールする必要があります。詳細については、VDAマシンにApp Packages Delivery Componentをインストールするを参照してください。

VDAマシンへのAPP PACKAGES DELIVERY COMPONENTのインストール

App Packages Delivery Componentは、App-V、MSIX、MSIX app attach、FlexApp、Elastic App、およびCloudpaging形式のアプリケーションパッケージの公開プロセスを管理します。このコンポーネントは、VDAをインストールする際にデフォルトではインストールされません。コンポーネントは、VDAのインストール中またはインストール後にインストールできます。

VDAのインストール中にコンポーネントをインストールするには、次のいずれかの方法を使用します。

- インストールウィザードで、**追加コンポーネント**ページに移動し、**App Packages Delivery Component**チェックボックスを選択します。
- コマンドラインインターフェースで、`/includeadditional "Citrix Personalization for App-V – VDA"` オプションを使用します。

VDAのインストール後にコンポーネントをインストールするには、次の手順に従います。

1. VDAマシンで、**コントロールパネル > プログラム > プログラムと機能**に移動し、**Citrix Virtual Delivery Agent**を右クリックして、**変更**を選択します。
2. 表示されるウィザードで、**追加コンポーネント**ページに進み、**App Packages Delivery Component**チェックボックスを有効にします。

> **注:**

- Microsoft App-V Desktop Client は、ユーザーデバイスで App-V パッケージから仮想アプリケーションを実行するコンポーネントです。Windows 10 (1607 以降) および Windows Server 2019 以降には、この App-V クライアントソフトウェアがすでに含まれています。VDA マシンでのみ有効にする必要があります。詳細については、この Microsoft ドキュメント記事を参照してください: App-V インボックスクライアントを有効にする。
- FlexApp アプリケーションの場合は、App Packages Delivery Component とともに VDA に FlexApp One Agent をインストールします。
- Elastic App アプリケーションの場合は、App Packages Delivery Component とともに VDA に App Layering 対応イメージをインストールします。
- Cloudpaging アプリケーションの場合は、App Packages Delivery Component とともに VDA に Cloudpaging Playerをインストールします。

FLEXAPP ONE AGENT をインストールする

1. VDA で管理者コマンドプロンプトを起動します。
2. 任意の FlexApp One Package のネットワークパスを見つけます。
3. 次のコマンドを入力します。

```
\\path\to\any\FlexAppOnePackage.exe --install
```

4. 表示されるプロンプトをすべて承認します。

APP LAYERING 対応イメージをインストールする

1. アプリレイヤリングを設定します。 Citrix App Layering ドキュメントの指示に従ってください。プロセスには以下が含まれます。
    a. Enterprise Layer Manager (ELM) を設定します。
    b. ゴールド OS イメージをインポートします。
    c. プラットフォームレイヤーを作成します。
    d. アプリケーションレイヤーを作成します。
    e. ELMで、配信したい各アプリケーションレイヤーに対して、**Studio App Packagesでの使用を有効にする**チェックボックスを選択します。
2. VDAマシンにElastic Layeringコンポーネントを含むイメージをインストールします。以下のいずれかの方法を使用できます。

a. Elastic Layeringが有効な状態でELMからイメージを展開します。
b. マシンにVDAを手動でインストールし、セットアップ中にElastic Layeringコンポーネントを選択します。

CLOUDPAGING PLAYERをインストールする

1. VDAで管理者コマンドプロンプトを開きます。
2. Cloudpaging Playerインストーラーが含まれているフォルダーに移動します。
3. 以下のコマンドを実行して、プレーヤーをサイレントインストールし、SaaSコンソールURLを設定します。必要に応じてプレースホルダーの値を置き換えてください。

```
cloudpaging-player-setup-x64-release.exe /S /v"/qn ADDLOCAL=ALL
REG_BASTOKENPATHORURL=https://your-tenant-url/api/token"
```

4. (オプション) インストール後に、以下のレジストリ値を確認して構成を検証します。
   - **パス:** `HKEY_LOCAL_MACHINE\SOFTWARE\Numecent\StreamingCore\Settings\Launcher`
   - **名前:** `BaseTokenPathOrURL`
   - **データ:** 値は、インストール時に指定したURLと一致する必要があります。

パッケージ化されたアプリケーションを配信する

前提条件のインストールが完了したら、ユーザーにパッケージアプリケーションを配信するには、次の手順を実行します。

1. アプリケーションパッケージをネットワーク共有に保存する。
2. アプリケーションパッケージを環境にアップロードする。
3. デリバリーグループにアプリケーションを追加する。
4. 相互依存するApp-Vパッケージの自動配信を有効にするには、分離グループを作成します。

アプリケーションパッケージをネットワーク共有に保存する

インフラストラクチャをセットアップしたら、アプリケーションパッケージを生成し、UNCまたはSMBネットワーク共有、あるいはAzureファイル共有などのネットワークロケーションに保存します。

詳細な手順は次のとおりです。

1. アプリケーションパッケージを生成します。詳細については、Microsoftのドキュメント「App-V仮想化アプリケーションの作成と管理」を参照してください。
2. アプリケーションパッケージをネットワークロケーションに保存します。

- **App-V Single Admin**の場合: パッケージと対応する動的構成ファイル（App-V）をUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
- **App-V Dual Admin**の場合：UNCパスからApp-V管理サーバーにパッケージを公開します。（HTTP URLからの公開はサポートされていません。）
- **MSIXまたはMSIX app attach**の場合: パッケージをUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
- **FlexApp**の場合: パッケージをUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
- **Elastic App**の場合: パッケージをUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。

3. VDAがパッケージの保存パスに対する読み取り権限を持っていることを確認してください。

   - ADドメイン内のUNCまたはSMBネットワーク共有にパッケージを保存する場合、VDAマシンに保存パスへの読み取り権限を付与します。そのためには、マシンのADアカウントに共有への読み取り権限を明示的に付与するか、その権限を持つADグループにアカウントを含めることができます。
   - Azureファイル共有にパッケージを保存する場合、まずAzureの保存パスに対するユーザーアカウントの読み取り権限を付与します。次に、VDAマシンで実行されている `ctxAppVService` を、そのユーザーアカウントを使用してパッケージ保存パスにアクセスするように構成します。詳細な手順については、ユーザーログオンアカウントの変更を参照してください。

ユーザーログオンアカウントの変更

以下の2つのシナリオでユーザーログオンアカウントを変更します。

- リンクされたADアカウントを使用してAzureファイル共有上のパッケージにアクセスする場合:
  - Microsoft Entra IDはファイル共有上のマシンアカウントに読み取り権限を付与しないため、接続エンティティはマシンアカウントではなくユーザーアカウントである必要があります。
- MSIXおよびMSIX AppAttachパッケージにサービスが含まれている場合:
  - パッケージは、非管理者ユーザーに公開される前に、ローカルマシン上で管理者権限を持つユーザーアカウントを使用して公開される必要があります。これは、パッケージ化されたサービスをインストールするために必要であり、パッケージはマシンではなくユーザーにのみ公開できるため、デフォルトのLocalServiceアカウントは不適切です。

VDAは`ctxAppVService`を呼び出して、パッケージ保存パスにアクセスし、管理者権限を必要とする操作を実行します。デフォルトでは、`ctxAppVService`はマシンのLocalServiceアカウントのコンテキストで実行され、マシンのIDを使用してADに認証するため、上記のシナリオには適していません。

いずれの場合も、サービスは、ローカルで管理者権限を持ち、パッケージの保存場所（SMB共有またはAzureファイル共有）への読み取りアクセス権が付与されているADユーザーアカウントを使用するように再構成する必要があります。手順は次のとおりです。

1. **サービス**を開始し、**ctxAppVService**を右クリックして、**プロパティ**を選択します。
2. 「**ログオン**」タブで、「**このアカウント**」を選択します。
    a. ローカル管理者権限とパッケージストレージパスへの読み取り権限を持つユーザーアカウントを入力します
    b. ユーザーのパスワードを2回入力します。
3. **OK**をクリックします。

環境にアプリケーションパッケージをアップロードする

必要に応じてアプリケーションパッケージをネットワークの場所に保存した後、配信のために環境にアップロードします。必要に応じて、以下のいずれかの方法を使用します。

- 一括アップロード
- 1つずつアップロード

準備

Citrix Virtual Apps and Desktops は、パッケージ検出のためのネットワークロケーションへの接続を設定するために VDA マシンを使用します。したがって、事前にデリバリーグループを作成し、グループ内の少なくとも1つの VDA が次の要件を満たしていることを確認してください。

- VDAバージョン:
    - App-Vパッケージを検出するには: 2203以降
    - MSIXおよびMSIXアプリ添付パッケージを検出するには: 2209以降
    - FlexAppパッケージを検出するには: 2311以降およびFlexApp Agentソフトウェア
    - ElasticAppパッケージを検出するには: 2511以降およびApp Layering対応イメージ
    - Cloudpagingパッケージを検出するには: 2511以降およびCloudpaging Playerソフトウェア
- App Packages Delivery Component: インストール済み

- パッケージの場所に対するアクセス許可: 読み取り (詳細については、Store application packages on network sharesを参照してください。)
- 電源: オン
- 状態: 登録済み

アプリケーションパッケージを一括アップロードする
ネットワーク上の場所にあるパッケージを環境にアップロードします。アップロードする前に、次の項目が準備されていることを確認してください。

- Preparationsの要件を満たすデリバリーグループ
- ネットワークの場所のパス

パッケージを一括でアップロードするには、次の手順に従います。

1. 左側のペインで、**App packages**を選択します。
2. **Packeage discovery**タブで、**Create discovery profile**ボタンをクリックします。**Create discovery profile**ページが表示されます。
3. **Name**フィールドに、プロファイルの説明的な名前を入力します。
4. **Delivery group**フィールドで、**Select a delivery group**をクリックします。次に、Preparationsで述べられている要件を満たすデリバリーグループを選択し、**OK**をクリックします。
5. **Location type**フィールドで、パッケージの保存場所に応じて、**Microsoft App-V server**、**Network share**、または**Numecent Cloudpager**を選択し、対応する設定を完了します。
    - 「**Microsoft App-V サーバー**」を選択した場合は、次の情報を入力します。
        - 管理サーバーのURL。例: `http://appv-server.example.com`
        - 管理サーバー管理者のログイン資格情報。
        - 公開サーバーのURLとポート番号。例: `http://appv-server.example.com:3330`
    - 「**ネットワーク共有**」を選択した場合は、次の情報を指定します。
        - ネットワーク共有のUNCパスを入力します (例: `\\Package-Server\apps\`)。*Elastic App*パッケージの場合は、ELMの**System's Network File Share SMB path**からUNCパスを入力します。
        - アップロードするパッケージの種類を選択します。オプションには、**App-V**、**MSIX**、**MSIX app attach**、**FlexApp**、および**Elastic App**が含まれます。
        - パッケージのサブフォルダーを検索するかどうかを指定します。

> **注:**
>
> `cim`イメージを含むフォルダー構造でMSIX app attachパッケージを検索する場合は、**サブフォルダーを検索**を選択していることを確認してください。そうしないと、ディスクが正しく検出されません。

- 「**Numecent Cloudpager**」を選択した場合は、次の情報を入力します。
  - CloudpagerコンソールのURL。例: `https://cloudpagerconsole.my.org`
  - PowerShell APIキー。
  - AppLauncher MSID。

6. **検出プロファイルの作成**をクリックします。

「**検出プロファイルの作成**」ページが閉じ、新しく追加されたプロファイルがプロファイルリストに表示されます。Citrix Virtual Apps and Desktopsは、デリバリーグループ内のVDAを使用してパッケージを環境にアップロードします。アップロードが完了すると、「ステータス」フィールドに「*インポート成功*」と表示されます。対応するパッケージは「**パッケージ**」タブに表示されます。

> 「**注:**」:
>
> ソースの場所でパッケージの更新を確認し、環境にインポートするには、プロファイルリストで場所を選択し、**更新の確認** をクリックします。

アプリケーションパッケージを1つずつアップロードする
ネットワーク共有からアプリケーションパッケージを環境にアップロードします。アップロードする前に、次の項目を準備してください。

- (#preparations)に記載されている要件を満たすデリバリーグループ
- ネットワークの場所のパス。

パッケージを環境にアップロードするには、次の手順に従います。

1. 左側のペインで、「**アプリパッケージ**」を選択します。
2. 「**パッケージ**」タブで、「**パッケージの追加**」ボタンをクリックします。「**パッケージの追加**」ページが表示されます。

3. 「**デリバリーグループ**」フィールドで、「**デリバリーグループの選択**」をクリックします。次に、(#preparations)に記載されている要件を満たすデリバリーグループを選択し、「**OK**」をクリックします。
4. 「**パッケージのフルパス**」フィールドに、必要に応じてパスを入力します。
   - 複数のパッケージを一度にアップロードするには、セミコロン (`;`) で区切って、それらのフルパスを入力します。例: `\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - ネットワーク共有にあるすべてのパッケージをアップロードするには、ストレージパスを入力します。例: `\\package-Server\apps\`
5. 「**パッケージの追加**」をクリックします。

   アプリケーションパッケージが「**パッケージ**」タブに表示されます。

アプリケーションをデリバリーグループに追加する

アプリケーションパッケージが環境に完全にアップロードされたら、必要に応じてそのアプリケーションを1つ以上のデリバリーグループに追加します。その結果、それらのデリバリーグループに関連付けられているユーザーは、アプリケーションにアクセスできるようになります。

注:

- パッケージ化されたアプリケーションは、デリバリーグループを介してシングルセッションVDAおよびマルチセッションVDAに配信できます。
- デフォルトでは、エンドユーザーは、*シングルセッション*（または*デスクトップ*）VDAに関連付けられているデリバリーグループに割り当てられたすべてのパッケージ化されたアプリケーションにアクセスできます。*デスクトップ*VDA上のパッケージ化されたアプリケーションの可視性を特定のユーザーまたはグループに制限するには、**アプリケーション**ノードに移動し、アプリケーションを選択してから、**アプリケーションプロパティの編集 > 可視性の制限**を選択して変更を加えます。「アプリケーションの可視性を制限する」を参照してください。

パッケージ内の1つ以上のアプリケーションを複数のデリバリーグループに追加するには、次の手順に従います。

1. 左側のペインで、**アプリパッケージ**を選択します。
2. **パッケージ**タブで、必要に応じてパッケージを選択します。

3. アクションバーで、**デリバリーグループの追加**をクリックします。**アプリケーションをデリバリーグループに割り当てる**ページが表示されます。
4. 必要に応じてパッケージ内の1つ以上のアプリケーションを選択し、**次へ**をクリックします。
5. デリバリーグループのリストで、アプリケーションを割り当てるグループを選択し、**次へ**をクリックします。

> **注:**
>
> - MSIXまたはMSIXアプリ添付パッケージを選択した場合、VDAバージョンが2106以降のデリバリーグループのみがリストに表示されます。
> - *FlexApp*パッケージを選択した場合、VDAバージョンが2402以降のデリバリーグループのみがリストに表示されます。
> - *Elastic App* パッケージを選択した場合、VDA バージョンが 2511 以降のデリバリーグループのみがリストに表示されます。
> - *Cloudpaging* パッケージを選択した場合、VDA バージョンが 2511 以降のデリバリーグループのみがリストに表示されます。

6. **完了**をクリックします。

さまざまなパッケージのアプリケーションを複数のデリバリーグループに追加するには、次の手順に従います。

1. 左ペインで、**App Packages**を選択します。
2. **アプリケーション**タブで、**アプリケーションの追加**を選択します。
3. **グループ**ページで、必要に応じて1つ以上のデリバリーグループを選択します。
4. **アプリケーション**ページで、次のように1つ以上のアプリケーションパッケージを選択します。
    a. **追加**をクリックし、**アプリケーションパッケージ**を選択します。
    b. 必要なパッケージプロファイルの種類（例：App-V Single Admin）を選択します。この種類のすべてのパッケージが表示されます。
    c. 必要に応じて1つ以上のパッケージを選択します。
    d. **OK**をクリックし、**次へ**をクリックします。

e. 異なるパッケージタイプのアプリケーションをさらに追加するには、手順aからdを繰り返します。

5. **完了**をクリックします。

次の場合に、パッケージ化されたアプリケーションをデリバリーグループに追加することもできます。

- 配信グループを作成する。詳細については、配信グループの作成を参照してください。
- 既存の配信グループまたはアプリケーショングループを編集する。詳細については、アプリケーションの追加を参照してください。

（オプション）APP-Vパッケージの分離グループを作成する

相互依存するApp-Vパッケージの自動配信を可能にするために、分離グループを作成できます。

> **注:**
>
> 分離グループは、App-Vシングル管理者方式でサポートされています。App-Vデュアル管理者方式を使用している場合は、Microsoft App-Vインフラストラクチャで*接続グループ*を作成することで、同じ目標を達成できます。詳細については、このMicrosoftドキュメント記事を参照してください：接続グループファイルについて。

分離グループについて
分離グループとは、仮想環境を作成するために同じWindows Sandboxで実行する必要がある、相互依存するアプリケーションパッケージの集合です。Citrix App-V分離グループは、App-V接続グループと似ていますが、同じではありません。分離グループには、次の2種類のパッケージが含まれます。

- **明示的なアプリケーションパッケージ**：特定のライセンス要件を持つアプリケーション。これらのアプリケーションを配信グループに追加することで、特定のユーザー範囲に制限できます。
- **自動アプリケーションパッケージ**：配信グループに追加されているかどうかにかかわらず、常にすべてのユーザーが利用できるアプリケーション。

たとえば、アプリケーション`app-a`を実行するにはJRE 1.7が必要です。app-a（*明示的*とマーク）とJRE 1.7（*自動*とマーク）を含む分離グループを作成できます。次に、`app-a`のApp-Vパッケージを1つ以上の配信グループに追加します。ユーザーがapp-aを起動すると、JRE 1.7が自動的に展開されます。

ユーザーが分離グループ内で*明示的*とマークされたApp-Vアプリケーションを起動すると、Citrix Virtual Apps and Desktopsは、配信グループ内のアプリケーションに対するユーザーのアクセス許可を確認します。ユーザーがアプリケーションにアクセスする権限を持っている場合、同じ分離グループ内の*自動*アプリケーションパッケージはすべてユーザーに利用可能になります。

*自動*パッケージをどの配信グループにも追加する必要はありません。分離グループ内に別の*明示的*アプリケーションパッケージがある場合、そのパッケージは同じ配信グループ内にある場合にのみユーザーに利用可能になります。

App-V分離グループを作成する

分離グループを作成し、相互依存するアプリケーションパッケージを追加します。詳細な手順は次のとおりです。

1. 「**分離グループ**」タブで、「**分離グループの追加**」をクリックします。
2. 分離グループの名前と説明を入力します。環境内のすべてのApp-V Single Adminパッケージが「**利用可能なパッケージ**」リストに表示されます。
3. 「**利用可能なパッケージ**」リストから必要に応じてアプリケーションを選択し、右矢印をクリックします。選択したアプリケーションが「**分離グループ内のパッケージ**」リストに表示されます。
4. 「**展開**」フィールドで、アプリケーションに対して「**明示的**」または「**自動**」を選択します。
5. 手順2〜3を繰り返して、さらにパッケージを追加します。
6. リスト内のパッケージの順序を調整するには、上矢印または下矢印をクリックします。
7. 「**保存**」をクリックします。

> **注:**
>
> 分離グループの構成により、VDA上にApp-V接続グループが作成されます。展開シナリオは複雑になる可能性があり、App-Vクライアントは一度に1つのアクティブな接続グループにのみ存在するパッケージをサポートします。同じパッケージを、同じデリバリーグループに追加されている2つの異なる分離グループに追加することは避けることをお勧めします。

ベストプラクティス

- App-Vパッケージを展開するには、PowerShellコマンド `Enable-AppV` を使用してVDAでApp-Vサブシステムを有効にします。
- MSIX（およびAppAttach）パッケージを展開するには、VDAがパッケージの署名に使用されている証明書を信頼する必要があります。

- Windows Server 2019では、MSIXパッケージを展開するためにサイドローディングを有効にします。Windows 10、11、Windows Server 2022、および2025ではサイドローディングは不要です。
- App AttachはWindows Server 2019ではまったく実装されておらず、Windows Server 2022または2025ではMicrosoft（およびCitrix）によって現在サポートされていません。

詳細設定

以下の高度なトピックでは、基本的なアプリパッケージのワークフローを超えて、Citrix Virtual Apps and Desktops でパッケージ化されたアプリケーションがどのように検出、更新、配信されるかを微調整するための追加の構成オプションと制御について説明します。

パッケージ化されたアプリケーションの公開を自動化する

PowerShellコマンドを使用して、パッケージ化されたアプリケーションの公開を自動化できます。

Delivery Controller™上で、以下のPowerShellコマンドを実行します:

1. パッケージ検出モジュールに存在するコマンドをロードするには:

   ```
   Import-Module "D:
   \Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
   ```

   注:

   パッケージ検出モジュールのバージョンは、Citrix Virtual Apps and Desktops ISOの、手順1で述べたパスにあります。

2. パッケージ検出モジュールは、公開するパッケージタイプをサポートするCitrix Virtual Apps and DesktopsバージョンのISOから取得する必要があります。つまり、FlexAppOneアプリケーションには2311以降が必要です。最新の利用可能なものを使用することをお勧めします。
3. 関連するデリバリーグループIDとパッケージ化されたアプリケーションIDを取得するには:

   ```
   Get-BrokerDesktopGroup | Format-Table Uid, Name

   Get-AppLibAppVApplication | Format-Table Uid, Name
   ```

4. パッケージを公開し、適切なBrokerMachineConfigurationsを作成するには:

```
Publish-PackagedApplication -AppLibararyApplicationUid
<AppLibararyApplication.Uid > -DesktopGroupUid <DesktopGroup.Uid>
```

5. Broker構成を同期するには（これらは後でVDA上のBrokerエージェントに送信されます）：

```
Update-DesktopGroupMachineConfigurations -DesktopGroupUid
<DesktopGroup.Uid>
```

注:

PowerShellコマンドラインを介してデリバリーグループからパッケージ化されたアプリケーションを公開または削除した後には、PowerShellコマンド `Update-DesktopGroupMachineConfigurations` を必ず実行してください。そうしないと、公開されたアプリケーションに関する情報がVDAに正しく送信されず、起動に失敗します。

アプリケーションの可視性を制限する

Citrix Virtual Apps and Desktops環境では、パッケージからのアプリケーションがデスクトップに公開されると、システムはそれらのアプリケーションに対するActive Directory (AD) のユーザーおよびグループの可視性設定を尊重します。ただし、ユーザーがパッケージ内の1つのアプリケーションのみに可視性を持っている場合でも、個々のパッケージコンポーネントはVDA上で細分化できないため、パッケージ全体が仮想デスクトップ（またはシームレスアプリ）セッションに展開される必要があります。さらに、VDAバージョン2503より前では、最初の公開後にアプリケーションの可視性を低下させる変更を行っても、その後のデスクトップ起動時に以前公開されたパッケージのクリーンアップは行われません。さらに、デスクトップとワークスペースの可視性など、他の可視性レイヤーはこれらのAD可視性割り当ての上に動作します。

パッケージ化されたアプリケーションがWorkspaceに表示されるべきか、ユーザーのVDIデスクトップセッションに展開されるべきかを制御できます。パッケージ化されたアプリケーションが公開されたら、PowerShellコマンド `Set-BrokerApplication -Name "MyApp" -PackagedApplicationVisibility "Workspace|Desktop|WorkspaceAndDesktop"` を使用して、`BrokerApplictaion` の `PackagedApplicationVisibility` プロパティを更新できます。

`PackagedApplicationVisibility` のデフォルト値は `WorkspaceAndDesktop` です。

値 `Workspace`: アプリはWorkspaceAppにのみ表示され、シームレスなAppLaunchで利用できますが、ユーザーが開始するデスクトップセッションには自動的に公開されません。

値 `Desktop`: アプリのアイコンをWorkspaceAppから非表示にし、シームレスなAppLaunchでは利用できなくなりますが、ユーザーがADグループ設定を通じてアクセスできる場合は、アプリをユーザーのデスクトップセッションに展開できます。

> **注:**
>
> シングルセッション静的デスクトクトップに公開されたパッケージアプリケーションは、この設定で構成された値に関係なく、Workspace Appでは利用できません。

App-Vフルインフラストラクチャからシングル管理者ワークフローへの移行

Microsoft App-Vフルインフラストラクチャ（デュアル管理者）は、サポート終了が近づいています。App-Vパッケージやその他のサポートされているコンテナ形式の提供を継続するには、Citrixシングル管理者モデルに移行してください。

シングル管理者モデルは、App-V管理サーバーと公開サーバーへの依存関係を排除し、Studioでパッケージ管理を一元化します。

シングル管理者モデルの利点

シングル管理者ワークフローに移行することで、アーキテクチャが簡素化され、パッケージ管理が効率化されます。

簡素化されたアーキテクチャ

シングル管理者モデルでは、VDAはファイル共有から直接パッケージを取得します。Citrixはメタデータ、公開、および分離ロジックを管理します。

機能	フルインフラストラクチャ（デュアル管理者）	シングル管理者（CITRIX管理）
管理	App-V 管理コンソール	シトリックス スタジオ または ウェブ スタジオ
データベース	必須 (SQL Server)	なし (メタデータはCitrixサイトデータベースに保存されます)
公開	App-V 公開サーバー	シトリックス VDA (`ctxAppVService`)

機能	フルインフラストラクチャ（デュアル管理者）	シングル管理者（CITRIX管理）
パッケージソース	UNC共有 (管理サーバーと同期)	UNC共有、SMB共有、またはAzure Files
ロジック	接続グループ	Citrix アイソレーション グループ

戦略的利点

Single Adminに移行することで、**同期ラグ**も解消されます。

- Dual Admin モデルでは、App-V 管理サーバーを同期し、その後 Studio を同期する必要があります。
- Single Admin モデルでは、ファイル共有上のパッケージを更新し、Studio で を選択すると、更新されたパッケージは次回のユーザーログオン時に利用可能になります。

移行ワークフロー

既存の App-V フルインフラストラクチャを Citrix Single Admin ワークフローに移行するには、次の手順に従います。

1. ステップ 1: ターゲット環境を準備する
2. ステップ 2: パッケージを Citrix ライブラリにインポートする

ステップ 1: ターゲット環境を準備する

パッケージをインポートする前に、インフラストラクチャと VDA が Single Admin モデルをサポートする準備ができていることを確認してください。

1. **共有リポジトリ**
   a. `.appv` パッケージをホストする UNC 共有を特定します。
   b. VDA マシンアカウント（例: ドメインコンピューター）が、共有と NTFS の両方のアクセス許可に対して **読み取り** アクセス権を持っていることを確認してください。
2. **VDA**

   すべてのVDAに**App Packages Delivery Component**がインストールされていることを確認してください。インストール後にこのコンポーネントを追加するには、次の手順を実行します。

   a. VDA インストーラーを実行します。
   b. で を選択します。

c. 「**App Packages Delivery Component**」を追加します。

3. 「**XML構成ファイル**」

   `_DeploymentConfig.xml`と`_UserConfig.xml`ファイルを、対応する`.appv`ファイルと*同じ*フォルダーに移動します。

   Single Adminモデルでは、VDAは中央のApp-Vデータベースからではなく、ファイル共有上のパッケージフォルダーから構成ファイルを読み取ります。

ステップ2：パッケージをCITRIXライブラリにインポートする

環境を準備したら、既存のApp-VパッケージをCitrixアプリケーションライブラリにインポートします。

1. Citrix Studioで、**構成** > **App Packages**に移動します。
2. 完全に移行する場合は、App-V管理サーバーへの既存の接続をすべて削除します。
3. **パッケージの追加**を選択し、パッケージのUNCパスを指定します。
4. Citrixはフォルダーをスキャンし、パッケージ名、バージョン、およびアプリケーションIDをCitrixアプリケーションライブラリにインポートします。

インポート後、必要に応じてアプリケーションをデリバリーグループに割り当てることができます。

> **注:**
>
> **vPreferポリシー（オプション）**：アプリケーションをリモートサーバーにリダイレクトする代わりにローカルVDAで起動したい場合は、VDAで**vPrefer** GPOを有効にしてください。

App-Vアプリケーションのトラブルシューティング（シングル管理者モデル）

App-Vパッケージ（シングル管理者モデル）が起動しない、またはユーザーセッションに表示されない場合は、以下のガイダンスを使用して一般的な問題を特定し、解決してください。

問題	説明	解決策
パッケージの検出と「カタログ化に失敗しました」エラー	Studioでパッケージを追加すると、ファイルにアクセスできないか、メタデータが無効であることを	1. 権限を確認します。

問題	説明	解決策	
	示すエラーが表示されます。	Delivery Controllerマシンアカウント（例：`DOMAIN\DDC01$`）が、パッケージをホストするUNCパスの共有レベルとNTFSレベルの両方で**読み取り**権限を持っていることを確認してください。 2. XMLの整合性を確認します。`.appv` ファイルと `_DeploymentConfig.xml` ファイルのファイル名プレフィックスが同じで、同じフォルダーにあることを確認してください。	
アプリケーションの起動に失敗する (エラーコード: 0x80070005 または 0x80040154)	ユーザーがアプリケーションアイコンをクリックすると、**Citrix スプラッシュ**画面が表示されますが、アプリケーションは開きません。	1. VDAコンポーネントを確認します。**App Packages Delivery Component** が	

問題	説明	解決策
		VDAにインストールされていることを確認してください。次のファイルが存在することを確認してください: `C:\Program Files\Citrix\AppV\ctxAppVService.exe`。 2. VDAのアクセス許可を確認します。 VDAはファイル共有からパッケージをプルするため、VDAマシンアカウント（例: `DOMAIN\VDA-HR01$`）はUNCパスへの**読み取り**アクセス権を持っている必要があります。 3. App-V クライアントの構成を検証します。 • VDA で次の PowerShell コマンドを実行します: `Get-`

問題	説明	解決策	
		`AppvClientConfiguration`。 • パッケージにスクリプトが必要な場合は、`EnablePackageScripts` が `$True` に設定されていることを確認してください。	
分離グループの競合	Excel アドインなどのプラグインは、その親アプリケーションを認識できません。	1. Studio で、**App Packages** > **Isolation Groups** に移動します。 2. 両方のパッケージが同じ分離グループに追加されていることを確認します。シングル管理者モデルでは、VDA上のApp-Vクライアントが、Delivery Controllerによって配信される構成に基づいて、それらのアプリケーションの仮	

問題	説明	解決策	
		想接続を管理します。	
初回起動が遅い (バッファリング)	AutoCADやArcGISなどの大規模なApp-Vパッケージの初回起動には数分かかります。	1. VDAで、次のレジストリを確認します `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\AppV\Client\Streaming` 2. その後の起動パフォーマンスを向上させるため、`Autoload` を `2` (以前使用したすべてのパッケージを自動ロードする) に設定します。 3. ネットワークパフォーマンスを確認します。ネットワーク共有でのSMB署名またはウイルス対策スキャンが転送速度を制限していないことを確認してください。	

便利なPowerShellコマンド（VDAで実行）

Citrixがパッケージを VDAに正常に配信したかどうかを確認するには、PowerShellウィンドウで次のコマンドを実行します。

コマンド	目的
`Get-AppvClientPackage`	VDAに現在キャッシュされているか、公開されているすべてのApp-Vパッケージを表示します。
`Get-CtxAppvPackage`	Citrixエージェントによって管理されているパッケージを表示します。
`Start-Service ctxAppVService`	Citrix App-Vオーケストレーションサービスを再起動します。

ユニバーサル Windows プラットフォーム アプリ

ユニバーサル Windows プラットフォーム (UWP) アプリの詳細については、以下の Microsoft ドキュメントを参照してください。

- ユニバーサル Windows プラットフォーム (UWP) アプリとは
- Windows パッケージ マネージャー

要件と制限

Citrix Virtual Apps and Desktops™ は、以下の Windows マシン上の VDA で UWP アプリの使用をサポートしています。

- Windows 10 以降のバージョン
- Windows Server 2016 以降のバージョン

VDA はバージョン 7.11 以降である必要があります。

UWPアプリを使用する場合、次のCitrix Virtual Apps™ and Desktopsの機能は、サポートされていないか、制限されています。

- ファイルの種類のアソシエーションはサポートされていません。
- ローカルアプリアクセスはサポートされていません。

- ダイナミックプレビュー: セッションで実行されているアプリが重なっている場合、プレビューにはデフォルトのアイコンが表示されます。ダイナミックプレビューに使用される Win32 API は、UWP アプリではサポートされていません。
- アクションセンターのリモート処理: UWP アプリは、セッション内のメッセージを表示するためにアクションセンターを使用できます。これらのメッセージは現在、ユーザーに表示するためにエンドポイントにリダイレクトされません。

同じサーバーから UWP アプリと非 UWP アプリを起動することはサポートされていません。代わりに、UWP アプリと非 UWP アプリを別々のデリバリーグループまたはアプリケーショングループに配置してください。

マシンにインストールされているすべてのUWPアプリが列挙されるため、Citrix®はWindowsストアへのユーザーアクセスを無効にすることを推奨します。これにより、あるユーザーがインストールしたUWPアプリが別のユーザーによってアクセスされるのを防ぎます。

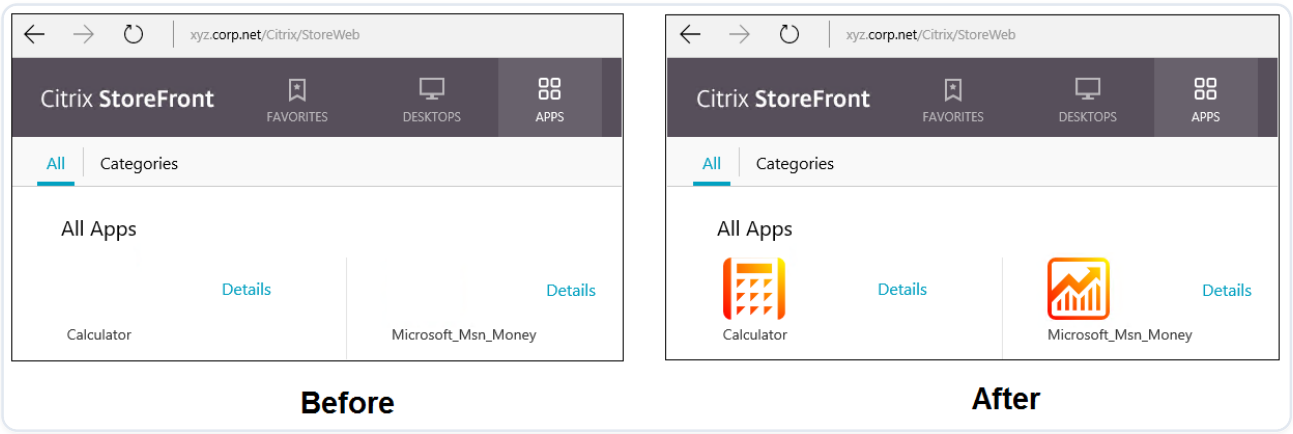
サイドローディング中、UWPアプリはマシンにインストールされ、他のユーザーが使用できるようになります。別のユーザーがアプリを起動すると、アプリがインストールされ、OSはそのAppXデータベースを更新して、そのユーザーによって「インストール済み」であることを示します。

固定ウィンドウまたはシームレスウィンドウで起動された公開UWPアプリから開始された正常なログオフにより、VDAセッションが閉じなくなり、ユーザーが強制的にログオフされる場合があります。この場合、VDAセッションに残っているいくつかのプロセスが、セッションが適切に閉じられるのを妨げます。これを解決するには、VDAセッションが閉じない原因となっているプロセスを特定し、CTX891671のガイダンスに従って、「LogoffCheckSysModules」レジストリキー値に追加します。

UWPアプリのアプリケーション表示名と説明が正しくない場合があります。アプリケーションをデリバリーグループに追加するときに、これらのプロパティを編集して修正してください。

その他の問題については、既知の問題を確認してください。

現在、いくつかのUWPアプリは透明度が有効な白いアイコンを使用しており、StoreFrontの白い背景に対してアイコンが見えなくなることがあります。この問題を回避するには、背景を変更できます。たとえば、StoreFrontマシンでファイル`C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`を編集します。ファイルの最後に`.storeapp-icon {background-image: radial-gradient( circle at top right, yellow, red ); }`を追加します。次の図は、この例の変更前と変更後を示しています。



Windows Server 2016以降のバージョンでは、UWPアプリの起動時にサーバーマネージャーも起動する場合があります。これを防ぐには、`HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon`レジストリキーを使用して、ログオン時にサーバーマネージャーが自動起動しないように無効にできます。詳細については、`<https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/>`を参照してください。

UWPアプリのインストールと公開

UWPアプリのサポートはデフォルトで有効になっています。

VDA（またはマスターイメージ）に1つ以上のUWPアプリをインストールするには、次のいずれかの方法を使用します。

- Windows Store for Businessからオフラインインストールを完了し、Deployment Image Servicing and Management (DISM) などのツールを使用してアプリをデスクトップイメージに展開します。詳細については、Windows Package Managerを参照してください。
- アプリをサイドロードします。詳細については、Windowsクライアントデバイスで基幹業務 (LOB) アプリをサイドロードするを参照してください。
- 各対象ユーザー向けに、Windows Store for Businessから直接UWPアプリをインストールします。

Citrix Virtual AppsまたはCitrix Virtual Desktops™で1つ以上のUWPアプリを追加（公開）するには：

1. UWPアプリがマシンにインストールされた後、UWPアプリをデリバリーグループまたはアプリケーショングループに追加します。これは、グループ作成時または後から実行できます。**アプリケーション**ページで、**追加**メニューから**スタートメニューから**を選択します。
2. アプリケーションリストが表示されたら、公開するUWPアプリを選択します。
3. ウィザードを続行するか、編集ダイアログを閉じます。

VDAでユニバーサルアプリの使用を無効にするには、`HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle`にレジストリ設定**EnableUWASeamlessSupport**を追加し、**0**に設定します。

UWPアプリのアンインストール

`Remove-AppXPackage`のようなコマンドでUWPアプリをアンインストールすると、その項目は管理者に対してのみアンインストールされます。アプリを起動して使用した可能性のあるユーザーのマシンからアプリを削除するには、各マシンで削除コマンドを実行します。1つのコマンドですべてのユーザーのマシンからAppXパッケージをアンインストールすることはできません。

構成のバックアップまたは移行

この機能は、構成のバックアップを取るのに役立ちます。バックアップと復元機能により、オンプレミスからクラウドへ、またはあるクラウドサイトから別のクラウドサイトへのサイト情報の移行が容易になります。また、緊急時にはサイトの即時復旧も可能になります。

バックアップを取るには、以下の方法を使用できます。

1. バックアップ + 復元
    a. Web Studio と統合されています。
2. 自動構成ツール (ACT)
    a. PowerShell ベースのツールです。使用するにはツールをインストールしてください。「Automated Configuration のダウンロード」を参照してください。

バックアップは次の目的で使用できます。

1. 復元
2. 移行

Citrix® は、説明されているシナリオに対して次のツールを推奨します。

バックアップ

環境	ユースケース	推奨ツール	特別な考慮事項	リンク
DaaS とオンプレミス	オンデマンドおよびスケジュールされたバックアップ	バックアップ + 復元	Citrix がバックアップを保持し、必要に応じてユーザーがダ	Web Studio を使用したバックアップと復元

環境	ユースケース	推奨ツール	特別な考慮事項	リンク
			ウンロードできます	
DaaS とオンプレミス	オンデマンドおよびスケジュールされたバックアップ	ACT	ユーザーがバックアップを保持します	Automated Configuration Tool を使用したバックアップと復元

移行

環境	ユースケース	推奨ツール	特別な考慮事項	リンク
オンプレミスからクラウドへ	1つのオンプレミスサイトをDaaSに移行する	ACT		オンプレミスからクラウドへの移行
	複数のオンプレミスサイトを1つのDaaSサイトに統合する	ACT	サイトのマージ	複数のオンプレミスサイトを単一のクラウドサイトにマージする
オンプレミスからオンプレミスへ	1つのオンプレミスサイトを別のオンプレミスサイトに移行する	ACT		「POCガイド：自動構成ツール - オンプレミスからオンプレミスへの移行」(/ja-jp/tech-zone/learn/poc-guides/citrix-automated-configuration-on-premises.html)
	複数のオンプレミスサイトを別のオンプレミス	ACT	サイトのマージ	「POCガイド：自動構成ツール オンプレミスからオンプ

環境	ユースケース	推奨ツール	特別な考慮事項	リンク
	サイトに統合する			レミスへの移行」(/ja-jp/tech-zone/learn/poc-guides/citrix-automated-configuration-on-premises.html)
				「複数のオンプレミスサイトを単一のクラウドサイトにマージする」(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/multi-site-merge)
クラウドからクラウドへ	1つのDaaSサイトを別のDaaSサイトに移行する	ACT		「クラウドからクラウドへの移行」(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/migrate-cloud-to-cloud.html)
複数のDaaSサイトを1つのDaaSサイトに統合する	サイトのマージ	ACT		クラウドからクラウドへの移行
				複数のオンプレミスサイトを単一のクラウドサイトに移行する

構成のバックアップと復元

この機能を使用すると、管理者はクラウド構成のバックアップを作成できます。これにより、Citrix®構成のコピーが常に利用可能になり、すぐに使用できるようになります。バックアップと復元機能により、オンプレミスからクラウドへ、またはあるクラウドサイトから別のクラウドサイトへのサイト情報の移行が容易になります。誤って変更が発生した場合でも、バックアップを選択して復元を選択するだけで、数回のクリックで再び稼働できます。特定のコンポーネントをバックアップおよび復元することもできます。

この機能では、以下をバックアップおよび復元できます。

- タグ
- 管理者ロール
- 管理者スコープ
- ホスト接続

> **注：**
>
> ホスト接続をバックアップできるようになりました。シークレットは毎回入力する必要があります。インポートまたは更新されるホスト接続に対してのみシークレットを要求するために、インポート前チェックモードが実行されます。

- StoreFront™
- デリバリーグループ
- アプリケーショングループ
- アプリケーション
- AppV分離グループ
- AppLibパッケージ検出
- グループポリシー
- ユーザーゾーン設定
- 手動でプロビジョニングされた、またはPVSでプロビジョニングされたマシンカタログ
- 管理者フォルダー
  - アプリケーションフォルダー
  - デリバリーグループフォルダー

    - マシンカタログフォルダー
- サイト設定

> **重要:**
>
> - 異なるコンポーネントを復元するには、リストの順序に従ってください。たとえば、アプリケーション、デリバリーグループ、およびグループポリシーを復元する場合は、次の順序に従う必要があります。
>
>   - デリバリーグループ
>   - アプリケーション
>   - グループポリシー
>
> - MCS マシンカタログをバックアップまたは復元することはできません。

バックアップの種類

要件に応じてバックアップを実行するには、次のオプションを使用します。

- **オンデマンド**: サイト構成をリアルタイムでバックアップします。このアクションは、現在の Citrix Cloud™ サイト構成をバックアップします。
- **スケジュール済み**: スケジュールされた間隔でサイト構成をバックアップします。これは、指定された間隔で繰り返されます。

> **注:**
>
> フル権限を持つ管理者とクラウド管理者のみが、オンデマンドまたはスケジュールされたバックアップと復元を実行できます。

Web Studio を使用したバックアップと復元

この記事では、コンソールの左ペインにある **バックアップと復元** ノードで実行できるアクションについて説明します。

バックアップと復元 を使用すると、管理者は Web Studio からバックアップを取得できます。

ストレージの場所を設定する

バックアップを作成する前に、バックアップを保存するストレージの場所を設定する必要があります。

1. Web Studio から、**管理** をクリックします。
2. 左メニューから、**バックアップ+復元** を選択します。
3. **バックアップと復元** タブ内で、**ストレージのセットアップ** をクリックします。

   バックアップのストレージの場所を設定する (/en-us/citrix-virtual-apps-desktops/2511/media/first-time-backup-storage-1.png)
4. ドロップダウンリストから、**ストレージの種類** を選択します。ストレージの種類は、ファイルストレージまたはAzureストレージにすることができます。

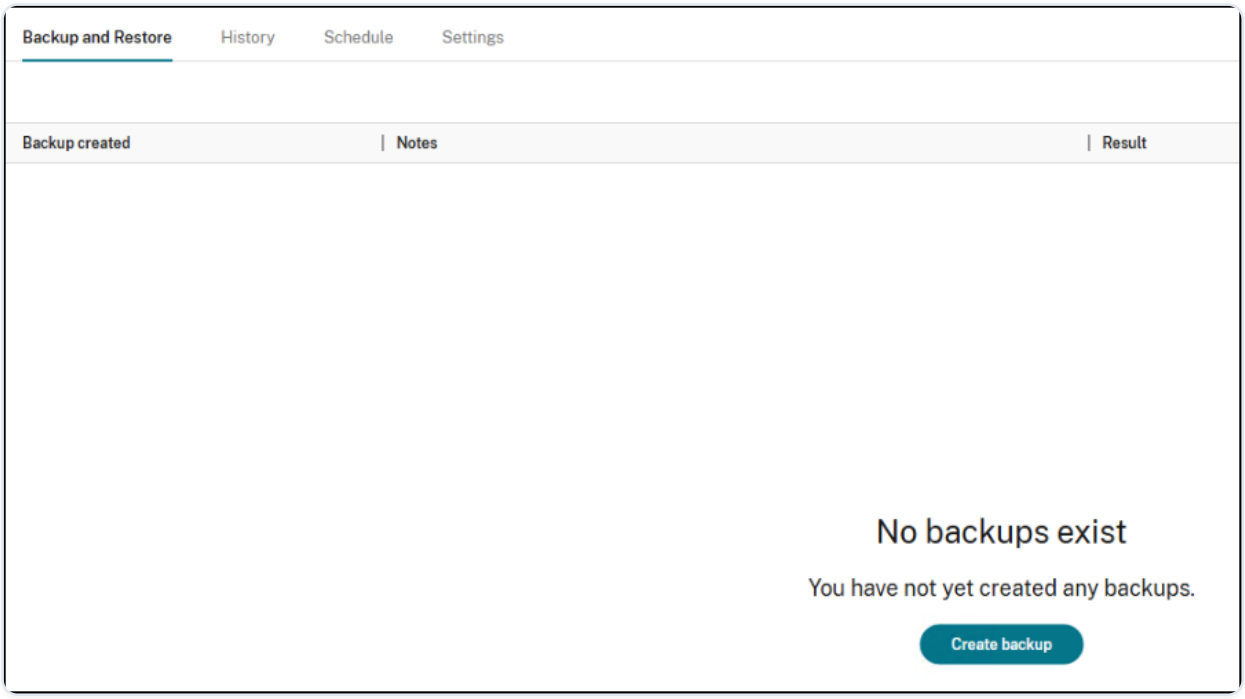
   > **注:**
   >
   > - その場所は、すべてのDelivery Controllerからアクセスできる必要があります。
   > - フォルダーへのアクセスにユーザー名とパスワードが必要な場合は、企業のパスワードポリシーによってパスワードの有効期間が制限されないようにしてください。

5. 以下を選択します。
   - 最大バックアップ数
   - 最大ピン留めバックアップ数
   - 最大自動ピン留めバックアップ数
6. **保存**をクリックしてストレージの場所を保存するか、**保存してバックアップを作成**をクリックしてストレージの場所を保存し、バックアップを作成します。

ストレージの場所を設定したら、バックアップを作成できます。

オンデマンドバックアップの作成

1. Web Studioから、**管理**をクリックします。
2. 左側のメニューから、**バックアップと復元**を選択します。
3. ストレージの場所が設定されているがバックアップが存在しない場合、バックアップを作成するように求められます。



既存のバックアップがある場合は、**バックアップの作成**をクリックできます。

4. **バックアップの作成**ページで、メモを入力し、**バックアップの作成**をクリックします。

   バックアップをトリガーした管理者の名前でバックアップされるバックアップコンポーネントを示す概要アクティビティが表示されます。

5. バックアップが正常に完了すると、**バックアップと復元**タブの下に項目として表示されます。
6. 特定のバックアップを選択すると、**詳細**タブでそのバックアップに関する詳細情報が表示されます。
7. バックアップを削除するには、バックアップを右クリックし、**バックアップの削除**をクリックします。

バックアップをピン留めする

Citrix® は最新の30個のバックアップを保存します。30個を超えるバックアップを作成すると、システムは作成された順序で古いバックアップを削除します。30個のバックアップ制限に加えて新しいバックアップが作成されるたびに、システムは最初に作成されたバックアップを削除します。バックアップのピン留めは、特定のバックアップが自動的に削除されるのを防ぐために使用されます。最大5個のバックアップをピン留めできます。ピン留めされたバックアップがある場合、30個のバックアップに加えてすべてのピン留めされたバックアップを保持します。つまり、最大で35個のバックアップ（ピン留めされていない30個とピン留めされた5個）を保持できます。

1. バックアップをピン留めするには、右クリックします。

スケジュールされたバックアップを作成する

組織の要件に合わせたバックアップスケジュールを作成し、バックアップと復元プロセスを自動化します。バックアップは、選択した頻度（毎日、毎週、毎月、またはその他の適切な頻度）でバックグラウンドで実行されます。

1. 「スケジュール」タブに移動し、**「スケジュールを作成」** を選択します。
2. **「スケジュールを作成」** ページで、以下を入力します。
    - **「このスケジュールを有効にする」**：このバックアップスケジュールを有効にするには、**「はい」** を選択します。
    - **「名前」**：バックアップスケジュールの名前を入力します。
    - **「説明」**：説明を入力します。
    - **「タイムゾーン」**：任意のタイムゾーンを選択します。
    - **「頻度」**：バックアップを実行する頻度を選択します。
    - **「繰り返し間隔」**：スケジュールを繰り返す日数（間隔）を入力します。
    - **「開始日」**：開始日を入力します。
    - **「バックアップ開始時刻」**：バックアップを開始したい時刻を24時間形式で入力します。
3. **完了**を選択します。

スケジュールされたバックアップを制限する

同一のバックアップを避けるため、スケジュールされたバックアップを1日1回に制限できます。

1. **Backup and Restore**ノードの**Settings**タブに移動します。
2. **Scheduled backups**ボックスで「**変更**」をクリックします。
3. トグルを切り替えて、スケジュールされたバックアップを1日1回に制限する機能を有効にします。

スケジュールされたバックアップの自動ピン留め

スケジュールされたバックアップの自動ピン留めは、選択したスケジュールによって作成されたバックアップを自動的にピン留めします。自動ピン留めには1つのスケジュールのみを選択できます。

スケジュールされたバックアップの自動ピン留めを使用すると、最大6つのスケジュールされたバックアップを保持できます。最大制限に達すると、最も古い自動ピン留めされたバックアップが削除されます。

「注：」：

Citrixは最大6つの自動ピン留めされたバックアップを保存します。システムは、6番目のバックアップ以降に作成された古いバックアップを、作成された順序で削除します。6つのバックアップ制限に加えて新しく作成されるバックアップごとに、システムは最初に作成されたバックアップを削除します。

1. **Backup and Restore**ノードの**Settings**タブに移動します。
2. 自動ピン留めするスケジュールされたバックアップを選択します。
3. トグルを切り替えて、自動ピン留めされたスケジュールを有効にします。
4. スケジュールを選択し、**保存**をクリックします。

バックアップストレージの編集

バックアップストレージ設定を編集して、ストレージの種類と場所、最大バックアップ数、最大ピン留めバックアップ数、最大自動ピン留めバックアップ数を変更できます。

1. 「**バックアップと復元**」ノードの「**設定**」タブに移動します。
2. 「**ストレージ**」ボックスで「**変更**」をクリックします。
3. 「**バックアップストレージの編集**」ダイアログでストレージ設定を変更します。

復元

この機能により、管理者はバックアップからサイト構成を復元できます。一度に1つのコンポーネントのみを復元できます。

注：

- 一度に1つのコンポーネントのみを復元することで、コンポーネント間の依存関係による復元中の競合がないことを保証します。
- ホスト接続を復元するワークフローは、ホスト接続を復元しようとするたびにシークレットを入力する必要があるため、他のコンポーネントとは異なります。**Restore Backup**をクリックすると、シークレットを入力するダイアログが表示されます。たとえば、Azureでは、接続の作成に使用した英数字のアプリケーションシークレットを入力します。

1. Web Studioから、「**管理**」をクリックします。
2. 左側のメニューから、「**バックアップと復元**」を選択します。
3. リストから特定のバックアップをクリックします。
4. 「**バックアップの復元**」をクリックします。
5. 「**バックアップの復元**」ウィンドウで、以下を入力します。

    - **コンポーネント**: 復元するコンポーネントを選択します。
    - **フィルター**: 復元するメンバー名をコンマ区切りのリストで指定します。たとえば、*chrome* という単語でフィルターすると、chrome という名前のオブジェクトのみが復元されます。同様に、`chr` というフレーズは、`chr` で始まるオブジェクトを復元します。

      コンポーネントメンバーを表示するには、バックアップを選択し、「**詳細 > コンポーネント**」に移動します。コンポーネントを選択し、「**コンポーネントメンバーの表示**」をクリックします。
    - **チェックモード**: 実際の復元操作が実行されたときに復元する必要があるものを確認するには、**はい**を選択します。このオプションは、実際に復元をトリガーすることなく、復元に必要なすべてを事前に評価します。たとえば、アプリケーションコンポーネントの復元プロセスが実行されたときに復元されるアプリケーションのリストが表示されます。

      > **注:**
      >
      > チェックモードでは、実際の復元は実行されません。このオプションでは、コンポーネント間の依存関係もチェックされません。最適な結果を得るには、一度に1つのコンポーネントでチェックモードを使用することをお勧めします。

    - **復元タイプ**: いずれかを選択します。
        - **不足しているもののみ**: この復元タイプを使用して、コンポーネントとメンバーをサイトに追加します。このオプションは、復元されるバックアップの構成が異なっていても、既存のコンポーネントとメンバーを変更しません。
        - **不足しているものと既存のものを更新**: この復元タイプを使用して、コンポーネントをサイトに追加および更新します。このオプションは、既存のコンポーネントとメンバーを、両方の構成が異なる場合にバックアップの構成で更新します。
    - **メモ**: メモを入力します。
6. **復元**を選択します。

復元アクションが完了すると、復元結果が**復元**ウィンドウに表示されます。すべての復元アクションは、**履歴**タブに一覧表示されます。

履歴

履歴タブで、すべてのバックアップおよび復元アクションを追跡できます。

アクションの下に、削除されたすべてのバックアップとバックアップ履歴が表示されます。

バックアップの詳細を表示するには：

1. **履歴**タブに移動します。
2. バックアップアクションを選択し、**詳細の表示**をクリックします。

バックアップ結果には、次の詳細が表示されます。

- 期間
- 注
- 管理者名
- バックアップされたコンポーネント

「**履歴**」ページの右上にある検索バーを使用して、特定のバックアップを検索します。たとえば、特定の管理者によって実行されたバックアップや、特定の日に実行されたバックアップを検索できます。

自動構成ツールを使用したバックアップと復元

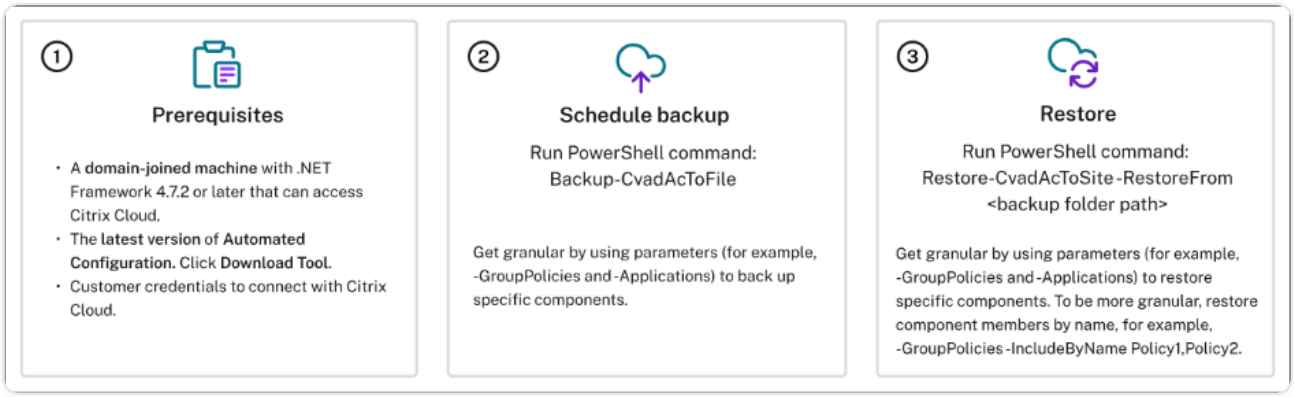
自動構成ツールを使用すると、以下の環境でオンデマンドおよびスケジュールされたバックアップを実行できます。

- シトリックス バーチャルアプリ アンド デスクトップ™
- DaaS

自動構成ツールは、以下の目的で使用できます。

- バックアップと復元（オンデマンドおよびスケジュールされたバックアップ）
- 移行（オンデマンドバックアップ）

移行のための自動構成ツール



シトリックス バーチャルアプリ™ アンド デスクトップ

構成をバックアップするための前提条件

- Citrix Virtual Apps and Desktops のすべてのバージョン。
- Auto Config を実行するマシン。このデバイスは次のいずれかです。
  - デリバリーコントローラー™
  - .NET Framework 4.7.2 以降および Citrix PowerShell SDK がインストールされたドメイン参加済みマシン。Citrix PowerShell の場合、Web Studio をインストールする必要があります。

バックアップ

1. Automated Configuration をインストールします。詳細については、Automated Configuration のダウンロードを参照してください。
2. **Auto-Config** をダブルクリックします。
3. PowerShell ウィンドウで、`Backup-CvadAcToFile` コマンドを実行してすべてのコンポーネントをエクスポートします。オンプレミス構成をエクスポートしても、変更はされません。

初めてコマンドを実行すると、プロセスは次の場所に `.yml` 構成ファイルを含むフォルダーを作成します。 `%HOMEPATH%\Documents\Citrix\AutoConfig` 。

このフォルダーには、最近エクスポートされたバックアップファイルが含まれており、以前の各バックアップはサブフォルダーに保存されます。

復元

1. **Auto-Config** をダブルクリックします。
2. 復元を実行するには、次のコマンドを実行します。

```
Restore-CvadAcToSite -Environment OnPrem -RestoreFolder <folder path of the backup files>
```

3. コマンドを実行した後、エクスポートの状態を確認し、ログフォルダーが次の場所にあることを確認します: `%HOMEPATH%\Documents\Citrix\AutoConfig`。
4. エラーまたは例外がある場合は、ログファイルの「**Fixups**」セクションを参照してください。

DaaS

構成をバックアップするための前提条件

- アクティブなリソースの場所とコネクタがインストールされているDaaS環境。
- Citrix Cloudにアクセスするサイトへの接続。詳細については、システムおよび接続要件を参照してください。

> **注**
>
> Automated Configurationツールを使用して、クラウドからMCSをバックアップすることはできません。

バックアップ

次のファイルをバックアップします。

- お客様ID、クライアントID、およびシークレットキー情報を含む`CustomerInfo.yml`ファイル。お客様ID、クライアントID、およびシークレットキーを取得するプロセスについて詳しくは、お客様ID、クライアントID、およびシークレットキーの生成を参照してください。この情報を`CustomerInfo.yml`ファイルに追加する方法については、顧客情報ファイルの入力を参照してください。
- クラウド内のリソースロケーションをマッピングする情報を含む`ZoneMapping.yml`ファイル。ゾーンをマッピングする方法について詳しくは、ゾーンマッピングファイルの入力を参照してください。
- ホスト接続に関する情報を含む`CvadAcSecurity.yml`ファイル。

1. Automated Configurationをインストールします。詳しくは、Automated Configurationのインストールを参照してください。

> **注**

> DaaSのバックアップの場合、インターネットアクセスがあり、管理者が直接アクセスできるマシンにAutomated Configurationをインストールします。

1. **Auto Config**をダブルクリックします。
2. PowerShellウィンドウで、バックアップを作成するために次のコマンドを実行します: `Export-CvadAcToFile`

初めてコマンドを実行すると、プロセスによって.yml構成ファイルを含むフォルダーが次の場所に作成されます。 `%HOMEPATH%\Documents\Citrix\AutoConfig`

このフォルダーには、最近のエクスポートからのバックアップファイルが含まれており、以前の各バックアップはサブフォルダーに保存されます。

復元

1. 「**Auto Config**」をダブルクリックします。
2. PowerShell ウィンドウで、復元を実行するために次のコマンドを実行します。

```
Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
```

3. コマンドを実行した後、エクスポートの状態を確認し、ログフォルダーは `%HOMEPATH%\Documents\Citrix\AutoConfig` にあります。
4. エラーまたは例外がある場合は、ログファイルの「**Fixups**」セクションを参照してください。

詳細な移行

> **注**
>
> コンポーネントの移行順序の詳細については、「コンポーネントの移行順序」を参照してください。

コンポーネント全体の復元

コンポーネントを復元するには、1つ以上のパラメーターを選択する必要があります。

たとえば、デリバリーグループとマシンカタログのコンポーネント全体を復元するには、次のコマンドを実行します。

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups
-MachineCatalogs
```

コンポーネントメンバーの復元

1つ以上のコンポーネントメンバーを復元するには、`IncludeByName` 機能を使用します。選択したコンポーネントとインクルージョンリストとともに、`Restorefolder` パラメーターを指定して `Restore` コマンドレットを呼び出す必要があります。

たとえば、バックアップから2つのグループポリシーを復元するには、次のコマンドを実行します。

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -GroupPolicies
-IncludeByName Policy1,Policy2
```

クラウドサイト構成全体の復元

すべてのコンポーネントまたはクラウドサイト全体を復元するには、次のコマンドを実行します。

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

バックアップと復元のためのAutomated Configurationツール

自動構成ツールのコマンドは、Web Studio が使用するバックアップおよび復元 API をトリガーします。

`BckRstr` コマンドレットはコンソールにログを記録します。ログ情報を含むフォルダーは `\Documents\Citrix\AutoConfig` に作成されません。

注：

Citrix Virtual Apps and Desktops および Citrix DaaS™ で構成をバックアップするための前提条件は、PowerShell セッションの自動構成ツールと同じです。

バックアップ

Delivery Controller で新しいバックアップアクションを開始するには、PowerShell ウィンドウで `New-BckRstrBackup` を実行します。

復元

既存のバックアップから単一コンポーネントのメンバーを復元するには、PowerShell ウィンドウで `Restore-BckRstrBackups` を実行します。

コマンドの完全なリストについては、「自動構成ツールによるバックアップと復元用のコマンドレット」を参照してください。

バックアップと復元のベストプラクティス

この記事では、バックアップと復元の計画をより適切に行うのに役立ついくつかの推奨事項について説明します。

カテゴリ	ベストプラクティス
バックアップのスケジュール設定	サイト構成の変更頻度に基づいて、毎日、毎週、または毎月の頻度で実行できるデフォルトのバックアップスケジュールを設定します。このデフォルトスケジュールは、アクティビティの少ない時間帯（週末や深夜など）に設定します。スケジュールされたバックアップの詳細については、「スケジュールされたバックアップの作成」を参照してください。
	同じ日に実行される可能性のある複数のバックアップスケジュールが定義されている場合は、**Backup and Restore**ノードの**Settings**タブを使用して、1日あたりのバックアップ制限を1つにリセットします。
バックアップの管理	30個のバックアップ制限に達しても保持されるように、ゴールデンコピーバックアップを常にピン留めしてください。選択したバックアップをピン留めするには、バックアップを右クリックします。

FAQ

カスタム管理者はバックアップと復元を実行できますか?

いいえ。バックアップと復元機能は、フル権限を持つ管理者のみに制限されています。

特定のコンポーネントをバックアップできますか?

いいえ。現在、オンデマンドバックアップとスケジュールされたバックアップは、サイト構成全体をバックアップします。コンポーネントにはいくつかの依存関係と前提条件があります。これらの依存関係が適切に解決されるように、コンポーネント全体をバックアップできます。ただし、選択的なコンポーネントを復元することはできます。

バックアップをダウンロードできますか?

現在、ACTを使用してバックアップをダウンロードします。ACTはAutomated Configuration for Virtual Apps and Desktopsからダウンロードできます。

MCSカタログをバックアップおよび復元できますか?

現在、MCSカタログをバックアップおよび復元することはできません。ACTを使用してMCSカタログをバックアップし、別のサイトにインポートできます。

構成をCitrix Cloud™に移行する

Automated Configuration Tool (ACT) を使用すると、Citrix Virtual Apps and Desktops™ の構成（ポリシー、アプリケーション、カタログ、管理者ロール、スコープなど）を1つ以上のオンプレミスサイトからCitrix Cloudでホストされているサイトに移行できます。また、異なるクラウドリージョンまたはテナント間で情報を移行するためにも使用できます。

このツールは、1つ以上のオンプレミスサイトを構成ファイルのコレクションとして検出し、エクスポートします。これらのファイルはオプションで編集できます。これらのファイルの構成は、Citrix DaaSにインポートできます。 移行は、ツールを複数回実行することで段階的に行われ、目的の構成状態を簡単に実現できます。

ACTは、一度きりの移行ツールではありません。日常のクラウド運用を管理するために使用できます。例えば、次のとおりです。

- テストまたはステージングのクラウドアカウントから本番のクラウドアカウントへの転送を自動化する
- 構成のバックアップと復元
- 1つのクラウド環境を複数のクラウドに分割する

以下の*2分間*のビデオでは、Automated Configurationの概要を簡単に説明しています。

<iframe src="https://www.youtube.com/embed/uyQ9o2L1DXQ" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
Automated Configurationの詳細については、Tech Zoneの概念実証: Automated Configuration Toolを参照してください。

展開の移行とオンプレミス構成の移行準備の詳細については、Tech Zoneの展開ガイド: Citrix Virtual Apps and DesktopsをオンプレミスからCitrix Cloudに移行するを参照してください。

既知の制限事項

- Machine Creation Services™ を介してプロビジョニングされたマシンカタログには、特別な考慮事項があります。MCSの詳細については、Machine Creation Servicesでプロビジョニングされたカタログの移行についてを参照してください。

構成を移行するための前提条件

Citrix Virtual Apps™ and Desktops から構成を*エクスポート*するには、以下が必要です。

- Citrix Virtual Apps and Desktops: 現在のリリースとその直前のリリース、またはCitrix Virtual Apps and Desktops、XenAppおよびXenDesktop® LTSRs: すべてのバージョン
- .NET Framework 4.7.2以降およびCitrix PowerShell SDKがインストールされたドメイン参加済みマシン。これはDelivery Controllerに自動的にインストールされます。(オンプレミスのDelivery Controller以外のマシンで実行するには、Studioが適切なPowerShellスナップインをインストールするため、Citrix Studioをインストールする必要があります。Studioインストーラーはインストールメディアにあります。)

Citrix DaaSに構成を*インポート*するには、以下が必要です。

- Citrix Cloudにアクセスできるマシン。これはDelivery Controller™やドメイン参加済みマシンである必要はありません。
- Citrix DaaSがプロビジョニングされていること。
- Connectorがインストールされ、オンプレミス環境と同じドメインに参加しているアクティブなリソースの場所。
- Citrix Cloudにアクセスするサイトへの接続が許可され、利用可能である必要があります。詳細については、システムおよび接続要件を参照してください。

> **注:**
>
> Automated ConfigurationはCloud Connectorシステムにはインストールできません。

主な手順

1. Automated Configuration Toolをダウンロードし、システム要件を確認します。Automated Configurationのダウンロードを参照してください。
2. Citrix Cloudポータルから生成された`CustomerName`、`CustomerID`、および`SecretKey`の値で`CustomerInfo.yml`ファイルを埋めます。顧客ID、クライアントID、およびシークレットキーの生成と顧客情報ファイルの入力を参照してください。
3. オンプレミスサイトに複数のゾーンが含まれている場合は、ゾーンをCitrix DaaSリソースの場所にマッピングするように`ZoneMapping.yml`ファイルを更新します。ゾーンマッピングファイルの入力を参照してください。
4. サイトに複数のホスティング接続が含まれている場合は、Citrix DaaSに移行する各ホストタイプの接続情報で`CvadAcSecurity.yml`ファイルを更新します。ホスト接続が1つしかない場合は、ホスト接続の接続情報で`CvadACSecurity.yml`ファイルを更新します。ホスト接続のセキュリティファイルの更新を参照してください。
5. ACTを開き、`Export-CvadAcToFile`コマンドを使用してオンプレミスサイトをエクスポートします。移行でサポートされているコンポーネントのリストについては、サポートされている移行オブジェクトを参照してください。エクスポートの手順については、オンプレミス構成のエクスポートを参照してください。
6. `Merge-CvadAcToSite` コマンドを使用して、コンポーネントを段階的にインポートします。または、サイト全体を一度に移行することもできます。コンポーネントの移行順序 に記載されている順序でコンポーネントを移行してください。インポートの手順については、インポートの実行 を参照してください。
7. クラウドサイトをアクティブ化します。サイトのアクティブ化 を参照してください。

Automated Configuration のダウンロード

Citrix DownloadsからAutomated Configurationツールをダウンロードしてインストールします。

Automated Configuration のアップグレード

機能のエラーを防ぐため、常に最新バージョンの ACT を使用してください。

ツールのバージョンを確認するには、次の手順を実行します。

1. **Auto Config**アイコンをダブルクリックします。PowerShellウィンドウが表示されます。
2. バージョン番号を確認するには、次のコマンドを実行します。

```
Get-CvadAcStatus
```

3. Citrix Downloads に記載されているバージョンと、お使いのツールのバージョンを比較してください。ツールの最新バージョンはそこにあります。
4. ツールの最新バージョンをダウンロードしてインストールします。Automated Configuration をアップグレードするために、古いバージョンをアンインストールする*必要はありません*。

> **注:**
>
> Automated Configuration でクラウドにアクセスするコマンドレットを実行すると、新しいバージョンがダウンロード可能になったときにツールが通知します。コマンドレットの詳細については、Automated Configuration ツール コマンドレット を参照してください。

顧客ID、クライアントID、およびシークレットキーを生成する

オンプレミスサイトを Citrix DaaS に移行するには、Citrix Cloud ポータルから顧客 ID、クライアント ID、およびシークレットキーを使用して `CustomerInfo.yml` ファイルに情報を入力します。

顧客IDを取得するには：

1. Citrix Cloudアカウントにサインインし、顧客を選択します。
2. グリッドアイコンをクリックし、**Identity and Access Management**を選択します。
3. **API access > Secure clients**に移動します。顧客IDがページに表示されます。

クライアントIDとシークレットキーを取得するには：

1. **Secure clients**ページで、ボックスに名前を入力します。この名前は、複数のクライアントIDとシークレットキーを区別するために使用されます。
2. 「Create Client」をクリックして、クライアントIDとシークレットキーを作成します。
3. クライアントIDとシークレットキーを安全な場所にコピーし、この情報を含む`.csv`ファイルをダウンロードします。`.csv`ファイルを使用して`CustomerInfo.yml`ファイルを生成します。

> **注:**
>
> - クライアントIDとシークレットキーには有効期限がありません。侵害された場合は、**ゴミ箱**アイコンを使用して直ちに削除し、新しいものを作成してください。

- シークレットキーは、紛失または忘れた場合に取得することはできません。新しいクライアントIDとシークレットキーを作成する必要があります。

顧客情報ファイルを入力する

`CustomerInfo.yml`ファイルを使用すると、コマンドレットを実行するたびに顧客情報パラメーターを指定する必要がなくなります。顧客情報のいずれかは、コマンドレットパラメーターを使用して上書きできます。

`New-CvadAcCustomerInfoFile`コマンドレットを使用して、`CustomerInfo.yml`ファイルを作成します。

重要:

`CustomerInfo.yml` ファイルを手動で編集しないでください。手動で編集すると、意図しない書式設定エラーが発生する可能性があります。

`New-CvadAcCustomerInfoFile` コマンドレットには、次の必須パラメーターがあります。

- CustomerId: 顧客のID。
- ClientId: Citrix Cloud で作成された顧客のクライアントID。
- Secret: Citrix Cloud で作成された顧客のシークレット。

例:

```
New-CvadAcCustomerInfoFile -CustomerId markhof123 -ClientId
6813EEA6-46CC-4F8A-BC71-539F2DAC5984 -Secret TwBLaaaaaaaaaaaaaaaaw==
```

ダウンロードした `security.csv` ファイルを指す `SecurityCsvFileSpec` パラメーターを使用して、`CustomerInfo.yml` を作成することもできます。CustomerId も指定する必要があります。

```
New-CvadAcCustomerInfoFile -SecurityCsvFileSpec C:
\Users\my_user_name\downloads/security.csv -CustomerId markhof123
```

`CustomerInfo.yml` ファイルを更新するには、`Set-CvadAcCustomerInfoFile` コマンドレットを使用します。このコマンドレットはクライアントIDのみを変更します。

```
Set-CvadAcCustomerInfoFile -ClientId C80487EE-7113-49F8-85DD-2CFE30CC398E
```

以下は、CustomerInfo.yml ファイルのサンプルです。

```
# Created/Updated on 2020/01/29 16:46:47

CustomerId: 'markhof123'

ClientId: '6713FEA6-46CC-4F8A-BC71-539F2DDK5384'

Secret: 'TwBLaaabbbaaaaaaaaaaw=='

Environment: Production

AltRootUrl: ''

StopOnError: False

AlternateFolder: ''

Locale: 'en-us'

Editor: 'C:\Program Files\Notepad++\notepad++.exe'

Confirm: True

DisplayLog: True
```

ゾーンマッピングファイルにデータを入力する

オンプレミスゾーンは、クラウドのリソースの場所と同等です。他のサイトコンポーネントとは異なり、オンプレミスゾーンをクラウドに自動的にインポートすることはできません。代わりに、`ZoneMapping.yml` ファイルを使用して手動でマッピングする必要があります。ゾーン名が既存のリソースの場所名に関連付けられていない場合、インポートが失敗する可能性があります。

オンプレミスサイトにゾーンが1つしかなく、クラウドサイトにリソースの場所が1つしかない場合、自動構成ツールが正しい関連付けを行うため、`ZoneMapping.yml` ファイルを手動で管理する必要はありません。

ただし、オンプレミスサイトに複数のゾーンがある場合、またはクラウドサイトに複数のリソースロケーションがある場合は、`ZoneMapping.yml` ファイルを手動で更新して、オンプレミスゾーンとクラウドのリソースロケーションの正しいマッピングを反映させる必要があります。

`ZoneMapping.yml` ファイルは `%HOMEPATH%\Documents\Citrix\AutoConfig` にあります。`.yml` ファイルの内容は、ゾーン名をキー、リソースの場所名を値とする辞書です。

たとえば、プライマリゾーンが「Zone-1」、セカンダリゾーンが「Zone-2」と呼ばれるオンプレミスのCitrix Virtual Apps and Desktopsサイトが、新たに作成された2つのクラウドのリソースロケーション「Cloud-RL-1」と「Cloud-RL-2」を持つCitrix DaaS展開に移行される場合、ZoneMapping.ymlは次のように構成されます。

```
Zone-1: Cloud-RL-1



Zone-2: Cloud-RL-2
```

注:

コロンとリソースロケーション名の間にスペースを追加します。ゾーン名またはリソースロケーション名にスペースが含まれる場合は、名前を引用符で囲みます。

ホスト接続用のセキュリティファイルを更新する

ホスト接続とそれに関連付けられたハイパーバイザーは、ACTを使用してエクスポートおよびインポートできます。

ホスト接続にハイパーバイザーを追加するには、ハイパーバイザーの種類に固有のセキュリティ情報が必要です。この情報は、セキュリティ上の理由からオンプレミスサイトからエクスポートできません。Automated Configurationがホスト接続とハイパーバイザーをクラウドサイトに正常にインポートできるように、この情報を手動で提供する必要があります。

エクスポートプロセスにより、特定のハイパーバイザータイプに必要な各セキュリティ項目のプレースホルダーを含む `%HOMEPATH%\Documents\Citrix\AutoConfig` に `CvadAcSecurity.yml` ファイルが作成されます。クラウドサイトにインポートする前に、`CvadAcSecurity.yml` ファイルを更新する必要があります。管理者による更新は、必要に応じて新しいセキュリティプレースホルダーが追加され、複数のエクスポートにわたって保持されます。セキュリティ項目が削除される

ことはありません。詳細については、「CvadAcSecurity.ymlファイルを更新する」を参照してください。

```
HostConn1:

ConnectionType: XenServer®

UserName: root

PasswordKey: rootPassword

HostCon2:

ConnectionType: AWS

ApiKey: 78AB6083-EF60-4D26-B2L5-BZ35X00DA5CH

SecretKey: TwBLaaaaaaaaaaaaaaaaw==

Region: East
```

ハイパーバイザーごとのセキュリティ情報

各ハイパーバイザータイプに必要なセキュリティ情報を以下に示します。

- ゼノサーバー、ハイパーブイ、ブイエムウェア
  - ユーザー名
  - 平文パスワード
- マイクロソフト アジュール
  - サブスクリプションID
  - アプリケーションID
  - アプリケーションシークレット
- AWS
  - サービスアカウントID
  - アプリケーションシークレット
  - 地域

セキュリティに関する特別な考慮事項

すべてのセキュリティ情報はクリアテキストで入力されます。クリアテキストが推奨されない場合は、ホスト接続と関連するハイパーバイザーを**Studio**を使用して手動で作成できます。ホスト接続を使用するマシンカタログを正常にインポートできるように、ホスト接続とハイパーバイザー名はオンプレミスの対応するものと完全に一致している必要があります。

Citrix Virtual Apps and Desktopsのオンプレミス構成をエクスポートする

`export` PowerShellコマンドを使用して、既存のオンプレミス構成をエクスポートし、必要な`.yml`ファイルを取得できます。これらのファイルは、目的の構成をCitrix Cloudにインポートするために使用されます。

サポートされている移行オブジェクト

自動構成は、以下のコンポーネントの構成の移動をサポートしています。

- タグ
- 委任管理
  - スコープ
  - ロール
- ホスト接続
  - 単一のリソースプール
  - 管理者スコープ
- マシンカタログ
  - 管理者スコープ
  - マシン
  - リモートPCアクセス、物理、プール、プロビジョニング済み、MCS、割り当て済み
- StoreFront™
- デリバリー グループ
  - アクセスポリシー
  - 管理スコープの関連付け
  - アプリケーションアクセスポリシー
  - 割り当てポリシー

    - エンタイトルメント/デスクトップ ポリシー
    - 電源スケジュール
    - セッションの残存
    - セッションプレランチ
    - 再起動スケジュール
    - タグ
- アプリケーション グループ
    - 管理スコープの関連付け
    - デリバリー グループ
    - ユーザーとグループ
- アプリケーション
    - アプリケーション フォルダー
    - アイコン
    - アプリケーション
    - ブローカー構成済みFTA
    - タグ
- グループ ポリシー
- ユーザーゾーンの基本設定

オンプレミス構成のエクスポート

1. **Auto Config**アイコンをダブルクリックします。PowerShellウィンドウが表示されます。
2. すべてのコンポーネントをエクスポートするには、次のコマンドを実行します。オンプレミス構成をエクスポートしても、変更されることは*ありません*。

```
Export-CvadAcToFile
```

初めてコマンドレットを実行すると、`.yml`構成ファイルとログを含むエクスポートフォルダーが作成されます。フォルダーは`%HOMEPATH%\Documents\Citrix\AutoConfig`にあります。エクスポートを繰り返すたびにサブフォルダーが作成されます。親フォルダー`%HOMEPATH%\Documents\Citrix\AutoConfig`には、常に最新のエクスポートからのエクスポートファイルが含まれています。

注:

Automated ConfigurationがDelivery Controllerにインストールされていない場合は、PowerShellを介してツールを使用する前に`import-module Citrix.AutoConfig.Commands`を実行してください。**Auto Config**アイコンを使用してAutomated Configurationを開く場合は、この手順は不要です。

エラーまたは例外が発生した場合は、ログファイルの**Fixups**セクションを参照してください。

Citrix DaaSへの構成のインポート

重要:

- オンプレミス展開をクラウドに移行する際は、Citrix設定を含むドメインおよびOU GPOがクラウドに移行されていることを確認してください。Citrix Web Studio™はGPMCをサポートしていないため、ドメインおよびOU GPOはWeb Studioに表示されません。Citrixポリシーエンジンは、ドメインおよびOU内のVDAとユーザーにドメインおよびOU GPOを適用します。VDAにログインした後、ユーザーはドメインおよびOU GPOからのポリシーがセッションに適用されていることを確認できます。ただし、管理者はこれらのポリシーと設定を確認できないため、混乱を招く可能性があります。

コンポーネントの移行順序

コンポーネントとその依存関係をここに示します。コンポーネントをインポートまたはマージする前に、その依存関係が設定されている必要があります。依存関係が不足している場合、インポートまたはマージコマンドが失敗する可能性があります。インポートまたはマージが失敗した場合、ログファイルの**Fixups**セクションに不足している依存関係が表示されます。

1. タグ
    - 事前依存関係なし
2. 委任管理者
    - 依存関係なし
3. ホスト接続

- CvadAcSecurity.yml のセキュリティ情報

4. マシンカタログ
   - Active Directory に存在するマシン
   - ホスト接続
   - タグ
5. StoreFront
6. デリバリーグループ
   - Active Directory に存在するマシン
   - Active Directory に存在するユーザー
   - マシンカタログ
   - タグ
7. アプリケーショングループ
   - デリバリーグループ
   - タグ
8. アプリケーション
   - デリバリーグループ
   - アプリケーショングループ
   - タグ
9. グループポリシー
   - デリバリーグループ
   - タグ
10. ユーザーゾーン設定

インポートを実行する

1. **Auto Config**アイコンをダブルクリックします。PowerShellウィンドウが表示されます。
2. すべてのコンポーネントをインポートするには、次のコマンドを実行します。

```
Merge-CvadAcToSite
```

新しい現在の状態と期待される状態を検証します。さまざまなインポートオプションにより、インポート結果がオンプレミスサイトと同一であるか、そのサブセットであるかが制御されます。

コマンドレットを実行すると、`.yml`構成ファイルとログを含むエクスポートフォルダーが作成されます。フォルダーは`%HOMEPATH%\Documents\Citrix\AutoConfig`にあります。

エラーまたは例外が発生した場合は、ログファイルの**Fixups**セクションを参照してください。

> **注:**
>
> Delivery ControllerにAutomated Configurationがインストールされていない場合は、PowerShellを介してツールを使用する前に`import-module Citrix.AutoConfig.Commands`を実行します。**Auto Config**アイコンを使用してAutomated Configurationを開く場合は、この手順は不要です。

> 元のCitrix DaaS構成に戻すには、「Citrix DaaS構成のバックアップ」を参照してください。

インポート操作を理解する

インポートプロセスは、更新を正確に実行し、必要な更新のみを実行し、すべての更新が正しく行われたことを確認するように設計されています。すべてのインポート操作で以下の手順が実行されます。

1. エクスポートされた.ymlファイル（期待される状態）を読み取ります。
2. クラウド（現在の状態）を読み取ります。
3. インポート前のクラウドの状態を.ymlファイルにバックアップします（必要に応じて、事前バックアップを復元できます）。
4. 期待される状態と現在の状態の間の違いを評価します。これにより、どの更新を行うかが決定されます。
5. 更新を行います。
6. クラウドを再読み込みします（新しい現在の状態）。
7. インポート後のクラウドの状態を.ymlファイルにバックアップします（必要に応じて、事後バックアップを復元できます）。
8. 新しい現在の状態を期待される状態と比較します。
9. 比較結果を報告します。

詳細な移行

> **重要:**
>
> コンポーネントの移行順序の詳細については、「コンポーネントの移行順序」を参照してください。
>
> コンポーネントのみ、またはコンポーネント名のみを選択的に移行できます。

- サポートされているコンポーネントパラメータには、`MachineCatalogs`、`Tags` などがあります。
- サポートされているコンポーネント名パラメータには、`IncludeByName` および `ExcludeByName` パラメータなどがあります。

パラメータとその使用方法の詳細については、「詳細な移行パラメータ」を参照してください。

サイトをアクティブ化する

オンプレミスサイトとクラウドサイトの両方にあるデリバリーコントローラは、デスクトップ、アプリケーションの仲介、マシンの再起動などのリソースを制御します。2つ以上のサイトによって共通のリソースセットが制御されると問題が発生します。このような状況は、オンプレミスサイトからクラウドサイトへの移行時に発生する可能性があります。オンプレミスとクラウドの両方のデリバリーコントローラが同じリソースセットを管理することが可能です。このような二重管理は、リソースが利用できなくなり、管理不能になる可能性があり、診断が困難になる場合があります。

サイトのアクティブ化により、アクティブなサイトがどこで制御されるかを制御できます。

サイトのアクティブ化は、デリバリーグループのメンテナンスモードを使用して管理されます。サイトが非アクティブの場合、デリバリーグループはメンテナンスモードになります。アクティブなサイトのデリバリーグループからは、メンテナンスモードが解除されます。

サイトのアクティブ化は、VDA登録やマシンカタログに影響を与えたり、管理したりすることはありません。

- `Set-CvadAcSiteActiveStateCloud`
- `Set-CvadAcSiteActiveStateOnPrem`

すべてのコマンドレットは、`IncludeByName` および `ExcludeByName` フィルタリング をサポートしています。このパラメータを使用すると、メンテナンスモードを変更できるデリバリーグループを選択できます。デリバリーグループは必要に応じて選択的に変更できます。

クラウドへのインポートと制御の転送

オンプレミスサイトからクラウドサイトへ制御をインポートおよび転送する方法の概要を以下に示します。

1. オンプレミスサイトをクラウドにエクスポートおよびインポートします。`-SiteActive` パラメーターがインポートコマンドレットのいずれにも存在しないことを確認してください。オンプレミスサイトはアクティブで、クラウドサイトは非アクティブです。デフォルトでは、クラウドサイトのデリバリーグループはメンテナンスモードになっています。
2. クラウドのコンテンツと構成を確認します。
3. 営業時間外に、オンプレミスサイトを非アクティブに設定します。`-SiteActive` パラメーターは存在しない必要があります。すべてのオンプレミスサイトのデリバリーグループはメンテナンスモードになっています。
    - `Set-CvadAcSiteActiveStateOnPrem`
4. クラウドサイトをアクティブに設定します。`-SiteActive` パラメーターは存在する必要があります。クラウドサイトのデリバリーグループはメンテナンスモードではありません。
    - `Set-CvadAcSiteActiveStateCloud -SiteActive`
5. クラウドサイトがアクティブで、オンプレミスサイトが非アクティブであることを確認します。

オンプレミスサイトに制御を戻す

クラウドサイトからオンプレミスサイトに制御を転送するには：

1. 営業時間外に、クラウドサイトを非アクティブに設定します。すべてのクラウドサイトのデリバリーグループはメンテナンスモードになっています。
    - `Set-CvadAcSiteActiveStateCloud`
2. オンプレミスサイトをアクティブに設定します。オンプレミスサイトのデリバリーグループはメンテナンスモードではありません。
    - `Set-CvadAcSiteActiveStateOnPrem -SiteActive`

その他のサイトアクティベーション情報

- マシンが電源管理されておらず、再起動スケジュールもない場合（通常、ホスト接続もないことを意味します）、すべてのクラウドデリバリーグループをアクティブとしてインポートできます。インポート後に`-SiteActive`を`Merge-CvadAcToSite`/`Import-CvadAcToSite`に追加するか、`Set-CvadAcSiteActiveStateCloud -SiteActive`を実行します。
- マシンが電源管理されている場合、または再起動スケジュールがある場合は、別のプロセスが必要です。たとえば、この状況でオンプレミスからクラウドに切り替える場合、`Set-CvadAcSiteActiveStateOnPrem`を使用してオンプレミスサイトを非アクティブに設定します。次に、`Set-CvadAcSiteActiveStateCloud -SiteActive`を使用してクラウドサイトをアクティブに設定します。
- `Set-CvadAcSiteActiveStateCloud`と`Set-CvadAcSiteActiveStateOnPrem`のコマンドレットは、プロセスを元に戻すためにも使用されます。たとえば、`-SiteActive`パラメーターなしで`Set-CvadAcSiteActiveStateCloud`を実行し、次に`-SiteActive`パラメーターを指定して`Set-CvadAcSiteActiveStateOnPrem`を実行します。

Machine Creation Servicesでプロビジョニングされたカタログの移行について理解する

> **注：**
>
> この機能はバージョン3.0以降でのみ利用可能です。Automated Configuration内で`Get-CvadAcStatus`を使用してバージョンを確認してください。

> Machine Creation Services (MCS) カタログは、2種類のカタログを作成します。

- マシンに加えられた変更が失われるか元に戻される場合（一般的にアプリケーションが公開されるサーバーOSの場合） – これはプールされたVDI/マルチセッションのユースケースです
- マシンに加えられた変更が再起動後も保持される場合（一般的に専用ユーザーを持つクライアントOSの場合） – これは静的VDIのユースケースです

カタログの種類は、Citrix Studioのカタログノードでカタログの「User data:」値を確認することで確認できます。

> **注：**

> MCSは、Automated Configurationを使用してクラウドからバックアップすることはできません。

プールされたVDI / マルチセッションカタログ

「User data: Discard」を持つカタログはプールされたVDIカタログであり、メインイメージと構成のみを移行できます。これらのカタログ内の仮想マシンは移行されません。これは、仮想マシンのライフサイクルがインポート元のサイトによって維持されており、マシンが起動されるたびにその状態が変化する可能性があるためです。このため、仮想マシンのインポートデータがすぐに同期されなくなり、インポートは不可能になります。

このツールを使用してこれらのカタログを移行する場合、カタログメタデータが作成され、メインイメージの作成が開始されますが、マシンはインポートされません。

メインイメージのサイズに基づいてこのプロセスの作成には時間がかかる場合があるため、ツール内のインポートコマンドはMCSカタログの作成を開始するだけで、完了を待機しません。インポートが完了したら、クラウド展開のStudioを使用してカタログ作成の進行状況を監視してください。

メインイメージが作成されたら、マシンをプロビジョニングできます。オンプレミスでの使用から容量が消費されるため、容量に関する考慮事項を検討してください。

そのカタログを使用する他のすべてのオブジェクト（デリバリーグループ、アプリケーション、ポリシーなど）はインポートでき、メインイメージの作成を待つ必要はありません。カタログの作成が完了すると、インポートされたカタログにマシンを追加でき、ユーザーはリソースを起動できます。

> **注:**
>
> カタログおよびその他のすべてのオブジェクトを移行するには、ツール内で利用可能な同じコマンドを使用します。

静的VDIカタログ

> **注:**
>
> この操作はデータベースに保存されている低レベルの詳細をインポートするため、このプロセスはデータベースアクセス権を持つマシンから実行する必要があります。

> 静的VDIカタログは、メインイメージ、構成、およびすべての仮想マシンを移行します。プールされたVDIのユースケースとは異なり、イメージを作成する必要はありません。

VDAがクラウドに登録されるように、コネクタを指すように設定する必要があります。

再起動スケジュール、電源管理、その他の項目がクラウドによって制御されるように、クラウドサイトをアクティブにするには、サイトのアクティブ化セクションを参照してください。

移行が完了した後、このカタログをオンプレミスサイトから削除したい場合は、**VMとADアカウントを残す**を選択する必要があります。そうしないと、それらが削除され、クラウドサイトは削除されたVMを指したままになります。

移行後に孤立したリソースを検出するためにMCSタグを更新する

オンプレミス構成からクラウドサイトへ、またはクラウド構成から別のクラウドサイトへ移行した後、永続VMの場合、孤立したリソースが正しく検出されるように、MCSサイトIDタグを更新する必要があります。これを行うには、PowerShellコマンド`Set-ProvResourceTags`を使用します。現在、この機能はAzureに適用されます。

詳細な手順は次のとおりです。

1. 新しいCitrixサイトからPowerShellコマンド `Set-ProvResourceTags` を使用してMCSサイトIDタグを更新します。例:

   ```
   Set-ProvResourceTags -ProvisioningSchemeUid xxxxx  [-VMName <String>]
   [-VMBatchSize XX] [-ResourceType XX]
   ```

   または、,

   ```
   Set-ProvResourceTags -ProvisioningSchemeName xxxxx  [-VMName <String>]
   [-VMBatchSize XX] [-ResourceType XX]
   ```

パラメーターの詳細は次のとおりです。

- `ProvisioningSchemeUid` または `ProvisioningSchemeName` は必須パラメーターです。
- `VMName` はオプションパラメーターです。`VMName` が指定されていない場合、このマシンカタログのすべてのVMのタグが更新されます。

- `VMBatchSize` は、すべてのVMをバッチに分割するためのオプションパラメーターです。`VMBatchSize` が指定されていない場合、デフォルト値 (10) が適用されます。範囲は1から60です。
- `ResourceType` は次のいずれかです。
  - `MachineCatalog`: マシンカタログリソースのタグを更新する場合。
  - `VirtualMachine`: VM関連リソースのタグを更新する場合。
  - `All`: (デフォルトのResourceType): マシンカタログとVM関連リソースの両方のタグを更新する場合。

複数のサイトを単一のサイトに統合する

Automated Configuration のマルチサイトサポートは、複数のオンプレミスサイトを単一のクラウドサイトに統合する方法を提供します。

マルチサイトサポートは、オンプレミスサイトごとにコンポーネント名に一意のプレフィックスとサフィックスを追加し、複数のオンプレミスサイトが単一のクラウドサイトに統合された後も名前の一意性を確保します。

プレフィックスとサフィックスは、オンプレミスサイトごとに以下の各コンポーネントに割り当てることができます。

- `AdminScope`
- `AdminRole`
- `ApplicationAdmin`
- `ApplicationFolder`
- `ApplicationGroup`
- `ApplicationUser`
- `DeliveryGroup`
- `GroupPolicy`
- `HostConnection`
- `MachineCatalog`
- `StoreFront™`
- `Tag`

アプリケーションフォルダーは、プレフィックス、サフィックス、およびルートの再設定をサポートしています。ルートの再設定により、アプリケーションの既存のフォルダー構造に最上位のフォルダーが追加されます。

プレフィックスとサフィックスのルール

1. プレフィックスとサフィックスには、次の特殊文字を含めることはできません。`\ , / ; : # . * ? = < > | ( ) " ' { } [ ]`
2. プレフィックスとサフィックスには末尾のスペースを含めることができますが、先頭のスペースは含めることができません。
3. プレフィックスとサフィックスは、末尾のスペースを含めるために二重引用符で囲む必要があります。
4. プレフィックスとサフィックスは、インポート、マージ、追加時に適用されます。ソースの.ymlファイルは変更されません。
5. プレフィックスとサフィックスのプロセスは、該当する場合、依存するコンポーネント名に自動的にプレフィックスまたはサフィックスを付けます。たとえば、マシンカタログ名に「East」というプレフィックスが付いている場合、それらを参照するデリバリーグループにも「East」というプレフィックスが付けられます。
6. コンポーネント名がすでにプレフィックスまたはサフィックスで始まっている場合、プレフィックスまたはサフィックスは追加されません。コンポーネント名に、同じプレフィックスまたはサフィックスが二重に含まれることはありません。
7. プレフィックスとサフィックスは、個別に、または組み合わせて使用できます。
8. コンポーネントへのプレフィックスまたはサフィックスの使用はオプションです。

> **注:**
>
> Studioはコンポーネントをアルファベット順に表示します。

サイト別にコンポーネントをグループ化する

プレフィックスを使用して、単一サイトのコンポーネントを視覚的にグループ化します。各サイトは独自のグループにリストされ、プレフィックスによって異なるサイトグループの順序がアルファベット順に制御されます。

名前でコンポーネントをグループ化

複数のサイトから同じ名前のコンポーネントを視覚的にグループ化するには、サフィックスを使用します。異なるサイトの同じ名前のコンポーネントは、視覚的に交互に表示されます。

プレフィックスとサフィックスのマッピングファイル

サイトのプレフィックス付けは、1つ以上のオンプレミスサイトのサイトプレフィックスとサフィックスのマッピングを含むSiteMerging.ymlファイルから始まります。SiteMerging.ymlファイルは手動で管理することも、Merging multiple on-premises sites cmdletsセクションに記載されている利用可能なコマンドレットを使用して管理することもできます。

オンプレミスサイトのエクスポート

オンプレミスサイトをエクスポートするまで、マージを開始できません。オンプレミスサイトをエクスポートするには、オンプレミス構成のエクスポートを参照してください。

中央エクスポートターゲットフォルダー

このセクションで説明する方法では、複数のサイトのエクスポートを中央のファイル共有場所に配置します。`SiteMerging.yml` ファイル、`CustomerInfo.yml` ファイル、およびすべてのエクスポートファイルは、そのファイル共有場所に存在するため、オンプレミスサイトとは独立して1つの場所からインポートを実行できます。

クラウドアクセス操作はオンプレミスサイトやActive Directoryを参照しないため、どこからでもクラウドアクセス操作を実行できます。

直接ファイル共有

これを行うには、2つの方法があります。

- 直接ファイル共有: 直接ファイル共有からインポート、マージ、または追加するには、クラウドアクセス操作を実行するマシンを決定する必要があります。
- `SiteMerging.yml`を使用したファイル共有参照: この方法では、サイトのプレフィックスセットの`SiteRootFolder`メンバーを使用し、エクスポート、インポート、マージ、または追加時に誤ったフォルダーをターゲットにする可能性を低減します。

中央ファイル共有方法を使用しない場合は、個々のDelivery Controllerからインポート、結合、または追加を実行します。クラウドに移行される各Delivery Controllerで `SiteMerging.yml` ファイルを作成し、レプリケートします。デフォルトの場所は `%HOMEPATH%\Documents\Citrix\AutoConfig` です。正しいサイトプレフィックスを選択するには、`-SiteName` パラメーターを指定する必要があります。

直接ファイル共有

エクスポート、インポート、マージ、および新規/追加操作では、デフォルトのフォルダーである *%HOMEPATH%\Documents\Citrix\AutoConfig* 以外のフォルダーをターゲットまたはソースとする

パラメーターが提供されます。以下の例では、管理者がすでにアクセス権を持ち、必要に応じて資格情報を提供している、`\\share.central.net` にある中央ファイル共有を使用します。

エクスポートをサイト固有のフォルダーにターゲット設定するには、`-TargetFolder` パラメーターを使用します。

東側のDelivery Controller™から::

```
mkdir \\share.central.net\AutoConfig\SiteEast
```

```
Export-CvadAcToFile -TargetFolder \\share.central.net\AutoConfig\SiteEast
```

西側のDelivery Controllerから::

```
mkdir \\share.central.net\AutoConfig\SiteWest
```

```
Export-CvadAcToFile -TargetFolder \\share.central.net\AutoConfig\SiteWest
```

エクスポートが完了したら、`CustomerInfo.yml` と `SiteMerging.yml` ファイルを作成し、`\\share.central.net\AutoConfig` に配置します。

> **注：**
>
> この直接ファイル共有参照方法を使用する場合、`SitePrefixes.yml` を作成するときに `SiteRootFolder` パラメーターを使用しないでください。

> 直接ファイル共有からインポート、マージ、または追加するには、どのマシンからクラウドアクセス操作を実行するかを決定する必要があります。オプションは次のとおりです。

- ツールがすでにインストールされているオンプレミスの Delivery Controller のいずれか。
- ファイル共有をホストしているマシン。
- 別のマシン。

Automated Configurationは、クラウドにアクセスするマシンにインストールする必要があります。オンプレミスのPowerShell SDK、Delivery Controller、Active Directoryは使用されないため、クラウドアクセス実行要件はエクスポート要件よりもシンプルです。

East Delivery Controllerをクラウドにマージするには：

```
Merge-CvadAcToSite –SiteName East –SourceFolder \
\share.central.net\AutoConfig\SiteEast -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

West Delivery Controllerをクラウドにマージするには：

```
Merge-CvadAcToSite –SiteName West –SourceFolder \
\share.central.net\AutoConfig\SiteWest -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

以下は、前の例で使用された `SitePrefixes.yml` ファイルのサンプルです。

```
East:

  SiteRootFolder: "" # Important: leave this empty

  AdminScopePrefix: "East_"

  AdminRolePrefix: "East_"

  ApplicationAdminPrefix: "East_"

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "East"

  ApplicationGroupPrefix: "East_"

  ApplicationUserPrefix: "East_"

  DeliveryGroupPrefix: "East_"

  GroupPolicyPrefix: "East_"

  HostConnectionPrefix: "East_"

  MachineCatalogPrefix: "East_"

  StoreFrontPrefix: "East_"

  TagPrefix: "East_"
```

```
  AdminScopeSuffix: "_east"

  AdminRoleSuffix: "_east"

  ApplicationAdminSuffix: "_east"

  ApplicationFolderSuffix: "_east"

  ApplicationGroupSuffix: "_east"

  ApplicationUserSuffix: "_east"

  DeliveryGroupSuffix: "_east"

  GroupPolicySuffix: "_east"

  HostConnectionSuffix: "_east"

  MachineCatalogSuffix: "_east"

  StoreFrontSuffix: "_east"

  TagSuffix: "_east"

West:

  SiteRootFolder: "" # Important: leave this empty

  AdminScopePrefix: "Western "

  AdminRolePrefix: "Western "

  ApplicationAdminPrefix: "Western "

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "Western"

  ApplicationGroupPrefix: "Western "

  ApplicationUserPrefix: "Western "
```

```
DeliveryGroupPrefix: "Western "

GroupPolicyPrefix: "Western "

HostConnectionPrefix: "Western "

MachineCatalogPrefix: "Western "

StoreFrontPrefix: "Western "

TagPrefix: "Western "

AdminScopeSuffix: ""

AdminRoleSuffix: ""

ApplicationAdminSuffix: ""

ApplicationFolderSuffix: ""

ApplicationGroupSuffix: ""

ApplicationUserSuffix: ""

DeliveryGroupSuffix: ""

GroupPolicySuffix: ""

HostConnectionSuffix: ""

MachineCatalogSuffix: ""

StoreFrontSuffix: ""

TagSuffix: ""
```

SiteMerging.ymlを使用したファイル共有参照

この方法では、サイトのプレフィックスセットの`SiteRootFolder`メンバーを使用します。直接ファイル共有方法よりも複雑ですが、この方法を使用すると、エクスポート、インポート、マージ、または追加時に誤ったフォルダーをターゲットにする可能性が低減されます。

まず、SiteMerging.ymlファイルで各サイトの`SiteRootFolder`を設定します。これは共有場所で行う必要があります。

```
New-CvadAcSiteMergingInfo –SiteName East –SiteRootFolder \
\share.central.net\AutoConfig\SiteEast -SitePrefixesFolder \
\share.central.net\AutoConfig
```

```
New-CvadAcSiteMergingInfo –SiteName West –SiteRootFolder SiteWest
-SitePrefixesFolder \\share.central.net\AutoConfig
```

この例では、Eastは完全修飾フォルダー指定であり、Westは相対フォルダー指定です。

SiteMerging.ymlファイルを使用して、エクスポートをサイト固有のフォルダーにターゲット設定するには：

東デリバリーコントローラーから：

```
mkdir \\share.central.net\AutoConfig\SiteEast
```

```
Export-CvadAcToFile -SiteName East -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

西デリバリーコントローラーから:

```
mkdir \\share.central.net\AutoConfig\SiteWest
```

```
Export-CvadAcToFile -SiteName West -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

エクスポートコマンドレットは、`CustomerInfo.yml`フォルダーの場所を使用して`SiteMerging.yml`ファイルを特定します。Eastの場合、`SiteRootFolder`は完全修飾されています。これはそのまま使用されます。Westの場合、`SiteRootFolder`は完全修飾されていません。これは`CustomerInfo.yml`フォルダーの場所と組み合わされて、Westの完全修飾フォルダーの場所が取得されます。

East Delivery Controllerをクラウドにマージするには:

```
Merge-CvadAcToSite –SiteName East -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

West Delivery Controllerをクラウドにマージするには:

`Merge-CvadAcToSite –SiteName West -CustomerInfoFileSpec \ \\share.central.net\AutoConfig\CustomerInfo.yml`

以下は、前の例で使用された`SitePrefixes.yml`ファイルのサンプルです。

```
  East:

  SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteEast"

  AdminScopePrefix: "East_"

  AdminRolePrefix: "East_"

  ApplicationAdminPrefix: "East_"

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "East"

  ApplicationGroupPrefix: "East_"

  ApplicationUserPrefix: "East_"

  DeliveryGroupPrefix: "East_"

  GroupPolicyPrefix: "East_"

  HostConnectionPrefix: "East_"

  MachineCatalogPrefix: "East_"

  StoreFrontPrefix: "East_"

  TagPrefix: "East_"

  AdminScopeSuffix: "_east"

  AdminRoleSuffix: "_east"

  ApplicationAdminSuffix: "_east"

  ApplicationFolderSuffix: "_east"
```

```
  ApplicationGroupSuffix: "_east"

  ApplicationUserSuffix: "_east"

  DeliveryGroupSuffix: "_east"

  GroupPolicySuffix: "_east"

  HostConnectionSuffix: "_east"

  MachineCatalogSuffix: "_east"

  StoreFrontSuffix: "_east"

  TagSuffix: "_east"

West:

  SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteWest"

  AdminScopePrefix: "Western "

  AdminRolePrefix: "Western "

  ApplicationAdminPrefix: "Western "

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "Western"

  ApplicationGroupPrefix: "Western "

  ApplicationUserPrefix: "Western "

  DeliveryGroupPrefix: "Western "

  GroupPolicyPrefix: "Western "

  HostConnectionPrefix: "Western "

  MachineCatalogPrefix: "Western "
```

```
StoreFrontPrefix: "Western "

TagPrefix: "Western "

AdminScopeSuffix: ""

AdminRoleSuffix: ""

ApplicationAdminSuffix: ""

ApplicationFolderSuffix: ""

ApplicationGroupSuffix: ""

ApplicationUserSuffix: ""

DeliveryGroupSuffix: ""

GroupPolicySuffix: ""

HostConnectionSuffix: ""

MachineCatalogSuffix: ""

StoreFrontSuffix: ""

TagSuffix: ""
```

中央ファイル共有方法が使用されておらず、個々のDelivery Controllerからインポート、マージ、または追加が行われる場合は、クラウドに移行される各Delivery Controllerで`SiteMerging.yml`ファイルを作成して複製します。デフォルトの場所は *%HOMEPATH%\Documents\Citrix\AutoConfig* です。正しいサイトプレフィックスを選択するには、`-SiteName`パラメーターを指定する必要があります。

サイトをマージする

Citrix®は、クラウド操作を段階的に実行し、次のクラウド操作を行う前に各結果を完全にレビューすることを推奨しています。たとえば、3つのサイトを単一のクラウドサイトにマージする場合：

1. 適切な`SiteName`値を使用して、最初のサイトをクラウドにマージします。

2. Studioで結果を確認します。
3. 結果が正しくない場合は、問題とその原因を特定し、修正してからマージを再実行します。必要に応じて、クラウドコンポーネントを削除し、選択したコンポーネントとメンバーに`Remove-CvadAcFromSite`を使用して最初からやり直します。結果が正しい場合は、続行します。
4. 最初のマージが正しい場合は、2番目のサイトを単一のクラウドサイトにマージします。
5. 手順2と3を繰り返します。
6. 2番目のマージが正しければ、3番目のサイトを単一のクラウドサイトにマージします。
7. 手順2と3を繰り返します。
8. ユーザーの視点からリソースを確認し、ビューが目的の状態であることを確認します。

サイトプレフィックスを使用してコンポーネントを削除する

`Remove-CvadAcFromSite`コマンドレットの`-IncludeByName`パラメーターにプレフィックスを使用することで、単一サイトのコンポーネントを選択的に削除できます。次の例では、West Delivery Controllerのデリバリーグループが正しくありません。Westサイトのみのデリバリーグループを削除するには：

```
Remove-CvadAcFromSite -DeliveryGroups -IncludeByName "Western *"
```

すべてのWestコンポーネントを削除するには、次のコマンドレットを順番に実行します。

1. `Remove-CvadAcFromSite -GroupPolicies -IncludeByName "Western *"`
2. `Remove-CvadAcFromSite -Applications -IncludeByName "Western *"`
3. `Remove-CvadAcFromSite - ApplicationGroups -IncludeByName "Western *"`
4. `Remove-CvadAcFromSite -DeliveryGroups -IncludeByName "Western *"`
5. `Remove-CvadAcFromSite -MachineCatalogs -IncludeByName "Western *"`
6. `Remove-CvadAcFromSite -HostConnections -IncludeByName "Western *"`
7. `Remove-CvadAcFromSite -Tags -IncludeByName "Western *"`

東コンポーネントのグループポリシーを削除するには、次のサフィックスを使用します。

```
Remove-CvadAcFromSite -GroupPolicies -IncludeByName "*_east"
```

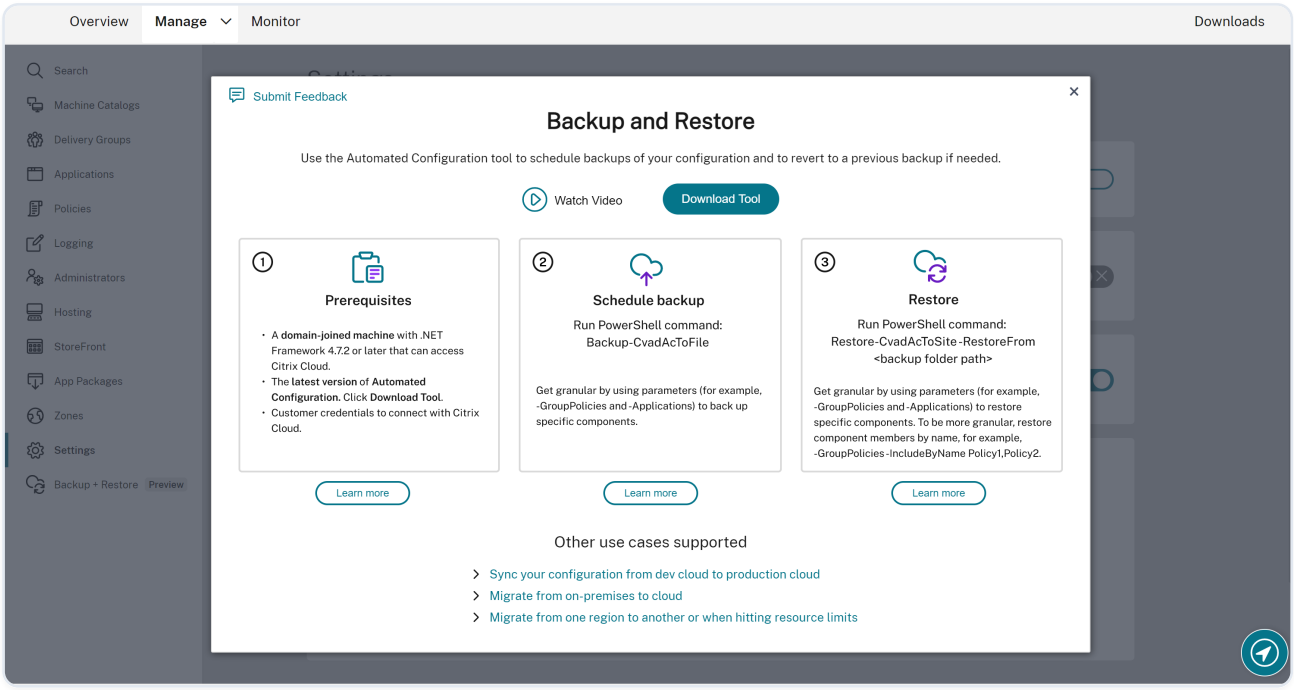
クラウドからクラウドへの移行

Automated Configurationを使用すると、クラウド構成を別のクラウドサイトに移動したり、独自のクラウドサイトを復元したりするプロセスを自動化できます。

Automated Configurationを使用すると、多くのユースケースを解決できます。

- テスト環境またはステージング環境から本番環境へのサイトの同期
- 構成のバックアップと復元
- リソース制限への到達
- あるリージョンから別のリージョンへの移行

Citrix Cloud™のStudioで、Automated Configurationと、それを使用して構成をクラウドからクラウドに移行する方法については、ノードを参照してください。



構成を移行するための前提条件

構成をバックアップおよび復元するには、以下が必要です。

- Citrix DaaS™がプロビジョニングされていること。
- Connectorがインストールされたアクティブなリソースの場所。
- Citrix Cloudにアクセスするサイトへの接続が許可され、利用可能である必要があります。詳しくは、「システムおよび接続要件」を参照してください。

> **注:**
>
> MCSは、Automated Configurationを使用してクラウドからバックアップすることはできません。

Citrix DaaS の構成をバックアップする

要件

Citrix DaaS の構成をバックアップする前に、次の操作を実行します。

1. `CustomerInfo.yml`ファイルに、顧客ID、クライアントID、および含まれているシークレットキー情報を入力します。顧客ID、クライアントID、およびシークレットキーの取得方法の詳細については、「顧客ID、クライアントID、およびシークレットキーを生成する」を参照してください。この情報を`CustomerInfo.yml`ファイルに追加する方法については、「顧客情報ファイルに入力する」を参照してください。

バックアップ コマンドを実行するときは、`CustomerInfo.yml` に、バックアップ元となるソース サイトの顧客の詳細が含まれている必要があります。

復元コマンドを実行するときは、`CustomerInfo.yml`に構成を復元する先の宛先サイト顧客の詳細が含まれている必要があります。

1. `ZoneMapping.yml`ファイルに、クラウド内のリソースロケーションをマッピングする情報を入力します。ゾーンのマッピング方法の詳細については、「ゾーンマッピングファイルに入力する」を参照してください。
2. ホスト接続がある場合は、対応する情報を`CvadAcSecurity.yml`ファイルに入力する必要があります。「ホスト接続のセキュリティファイルを更新する」を参照してください。

Citrix DaaS 構成をバックアップする手順

1. Automated Configurationをインストールする。

> **注：**
>
> クラウド間移行の場合、Automated Configurationは、管理者が直接アクセスできるインターネットに接続されたマシンにインストールできます。

2. **Auto Config**アイコンをダブルクリックします。PowerShellウィンドウが表示されます。
3. バックアップを実行するには、次のコマンドを実行します。

```
Backup-CvadAcToFile
```

初めて任意のコマンドレットを実行すると、`.yml`構成ファイルとログを含むエクスポートフォルダが作成されます。フォルダは`%HOMEPATH%\Documents\Citrix\AutoConfig`にあります。

エラーや例外が発生した場合は、ログファイルの**Fixups**セクションを参照してください。

Citrix DaaSへの構成の復元

1. **Auto Config**アイコンをダブルクリックします。PowerShellウィンドウが表示されます。
2. 復元を実行するには、次のコマンドを実行します。

```
Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
```

新しい現在の状態と期待される状態を検証します。

コマンドレットを実行すると、`.yml`構成ファイルとログを含むエクスポートフォルダが作成されます。フォルダは*%HOMEPATH%\Documents\Citrix\AutoConfig*にあります。

エラーや例外が発生した場合は、ログファイルの**Fixups**セクションを参照してください。

バックアップと復元プロセスは、意図しないクラウドサイト構成の変更や破損から保護します。自動構成は変更が行われるたびにバックアップを作成しますが、このバックアップは変更前のクラウドサイト構成の状態を反映しています。自身を保護するには、クラウドサイト構成を定期的にバックアップし、安全な場所に保存する必要があります。望ましくない変更や破損が発生した場合、バックアップを使用して、きめ細かいレベルまたはサイト構成全体レベルで変更や破損を修正できます。

詳細な移行

> **重要:**
>
> コンポーネントの移行順序の詳細については、「コンポーネントの移行順序」を参照してください。

すべてのコンポーネントを復元する

1つのコンポーネントを復元するには、1つ以上のコンポーネントパラメータを選択します。

復元するには:

- デリバリーグループ全体とマシンカタログコンポーネント
- 完全なクラウドサイト構成

次の例に従ってください:

```
Restore-CvadAcToSite   -RestoreFolder   %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

コンポーネントメンバーを復元する

1つ以上のコンポーネントメンバーを復元するには、`IncludeByName` 機能を使用します。`Restore` コマンドレットは、選択した単一のコンポーネントとインクルージョンリストとともに、`RestoreFolder` パラメーターを指定して呼び出されます。

バックアップから2つのグループポリシーを復元するには、次の例に従ってください:

```
Restore-CvadAcToSite   -RestoreFolder   %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss



-GroupPolicies -IncludeByName   Policy1,Policy2



-DeliveryGroups -MachineCatalogs
```

サイトをアクティブ化する

サイトのアクティブ化により、アクティブなサイトを制御し、リソースを管理できます。詳しくは、「」(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/migrate.html#activate-sites)を参照してください。

クラウド構成をオンプレミスに移行する

この記事では、クラウド構成をバックアップし、オンプレミスサイトに移行する方法について説明します。

構成を移行するための前提条件

- 少なくとも1つの登録済みVDAを持つCitrix Virtual Apps and Desktops™オンプレミス環境。
- 次のいずれかのバージョンで実行されているCitrix Virtual Apps™ and Desktopsオンプレミス環境:
    - 最新の長期サービスリリース (LTSR) バージョン - 2402。
    - いずれかの現行リリース (CR) バージョン - 2308、2311。

- .Net 4.7.2以降のバージョンがインストールされたドメイン参加済みマシンで、自動構成ツール (ACT) コマンドを実行します。
- Citrix PowerShell SDKがインストールされたマシン。PowerShell SDKは、Citrix Delivery Controller™のインストール可能ファイル内にあります。

注:

- 別のマシンでACTを実行している場合は、そのマシンはドメインに参加している必要があり、Studioには適切なPowerShellスナップインがインストールされている必要があります。インストーラーを入手するには、Citrix Virtual Apps and Desktopsダウンロード Webサイトにアクセスしてください。
- オンプレミスサイトでは、ACTをDelivery Controllerにインストールすることをお勧めします。ACTはデスクトップアイコンから起動できます。
- ACTを標準のPowershellウィンドウから使用する場合は、次のコマンドを実行する必要があります: `Import-Module Citrix.AutoConfig.Commands`

ACTはシステムPowerShellパスの一部ではないため、明示的にインポートする必要があります

主な手順

クラウド構成をオンプレミスに移行する手順は次のとおりです。

1. クラウド構成のバックアップ
2. YML ファイルの変更
3. 構成をオンプレミスにインポート

クラウド構成のバックアップ

1. **Automated Configuration** をインストールします。
2. **CustomerInfo.yml** ファイルを作成するには、`New-CvadAcCustomerInfoFile`を実行します。詳細については、(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/migrate.html#populate-customer-info-file)を参照してください。
3. クラウド構成のバックアップを作成するには、コマンド`Backup-CvadAcToFile`を実行します。

注：

- 任意のコマンドレットを初めて実行すると、.yml 構成ファイルとログを含むエクスポートフォルダーが作成されます。フォルダーは `%HOMEPATH%\Documents\Citrix\AutoConfig` にあります。
- エラーまたは例外が発生した場合は、ログファイルの**Fixups**セクションを参照してください。
- Backup-CvadToFile は、パラメーター `IncludeByName` または `ExcludeByName` をサポートしていません。

重要:

Citrix は、すべてのコンポーネントをまとめてバックアップすることをお勧めします。

YML ファイルの変更

次の表に示すように、`%HOMEPATH%\Documents\Citrix\AutoConfig` にある `.yml` ファイルを変更して、オンプレミスの詳細を含めます。

YMLファイル	パラメーター	説明	例
CustomerInfo.yml	環境	Environmentを OnPremに変更します。環境パラメーターの値は大文字と小文字を区別します。	
ZoneMapping.yml	DaaS:CVAD	クラウドのリソースの場所をオンプレミスゾーンにマッピングします。	それはold:newゾーンである必要があります。
CvadAcSecurity.yml	ハイパーバイザー: 接続タイプ: ‘ ‘ ユーザー名: ‘ ’ パスワード: ‘ ‘	ハイパーバイザーのユーザー名とパスワードを追加します。	ハイパーバイザーがXenServerの場合、XenServer: ConnectionType: ‘XenServer’

YMLファイル	パラメーター	説明	例
			Username: ‘root’ Password: ‘ ‘

オンプレミスに構成をインポートする

1. 要件に応じて、オンプレミスサイトで以下のいずれかのコマンドを実行します。
   a. `Merge-CvadAcToSite` - オンプレミスサイトが稼働しており、クラウド構成をそれにマージしたい場合。
   b. `Import-CvadAcToSite -Environment OnPrem` - オンプレミス構成が利用できず、クラウド構成をインポートして新しいものを作成する場合。

> **重要:**
>
> 競合を避けるため、Citrixはコンポーネントを一度に1つずつインポートすることを推奨します。

オンプレミス構成をオンプレミスサイトに移行する

この記事では、Automated Configuration Tool (ACT) を使用して、オンプレミス構成をあるオンプレミスサイトから別のオンプレミスサイトに移行する手順について説明します。

要件

- 両方のオンプレミスサイトは、同じドメインにドメイン参加している必要があります。
- Citrix Virtual Apps and Desktops™ バージョン 2305 以降を使用してください。

手順

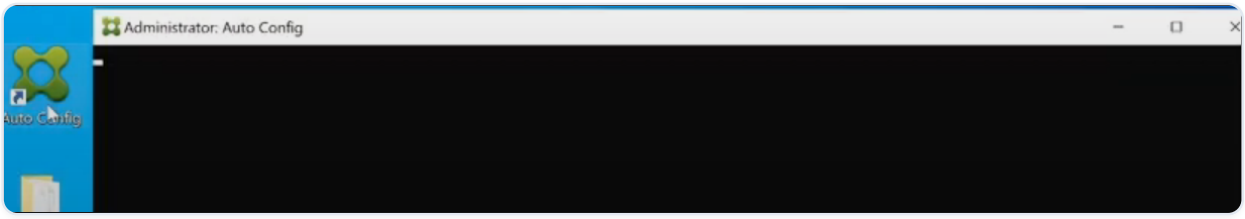
1. Automated Configuration Tool をダウンロードし、システム要件を確認してください。Automated Configuration のダウンロードを参照してください。
2. ACT を開き、次のコマンドを使用してオンプレミスサイトをエクスポートします。

   ```
   Export-CvadAcToFile
   ```

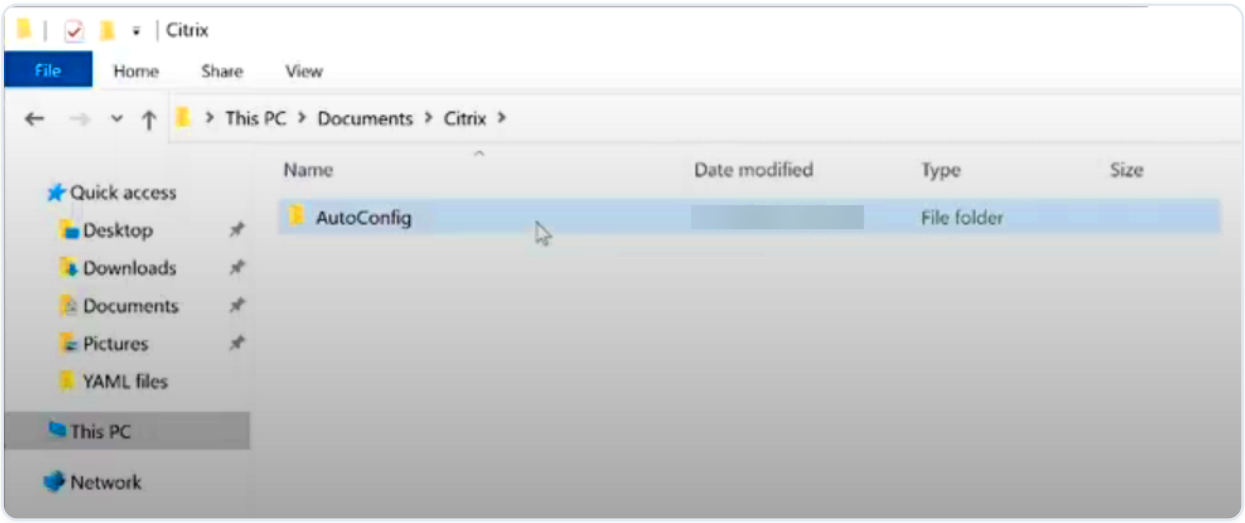
   移行でサポートされているコンポーネントのリストについては、サポートされている移行オブジェクトを参照してください。エクスポートの手順については、オンプレミス構成のエクス

ポートを参照してください。親フォルダー `%HOMEPATH%\\Documents\\Citrix\\AutoConfig` には、常に最新のエクスポートからのエクスポートファイルが含まれています。

3. ターゲットサイトで ACT を起動します。`%HOMEPATH%\\Documents\\Citrix` に `AutoConfig` フォルダーが作成されていることを確認してください。



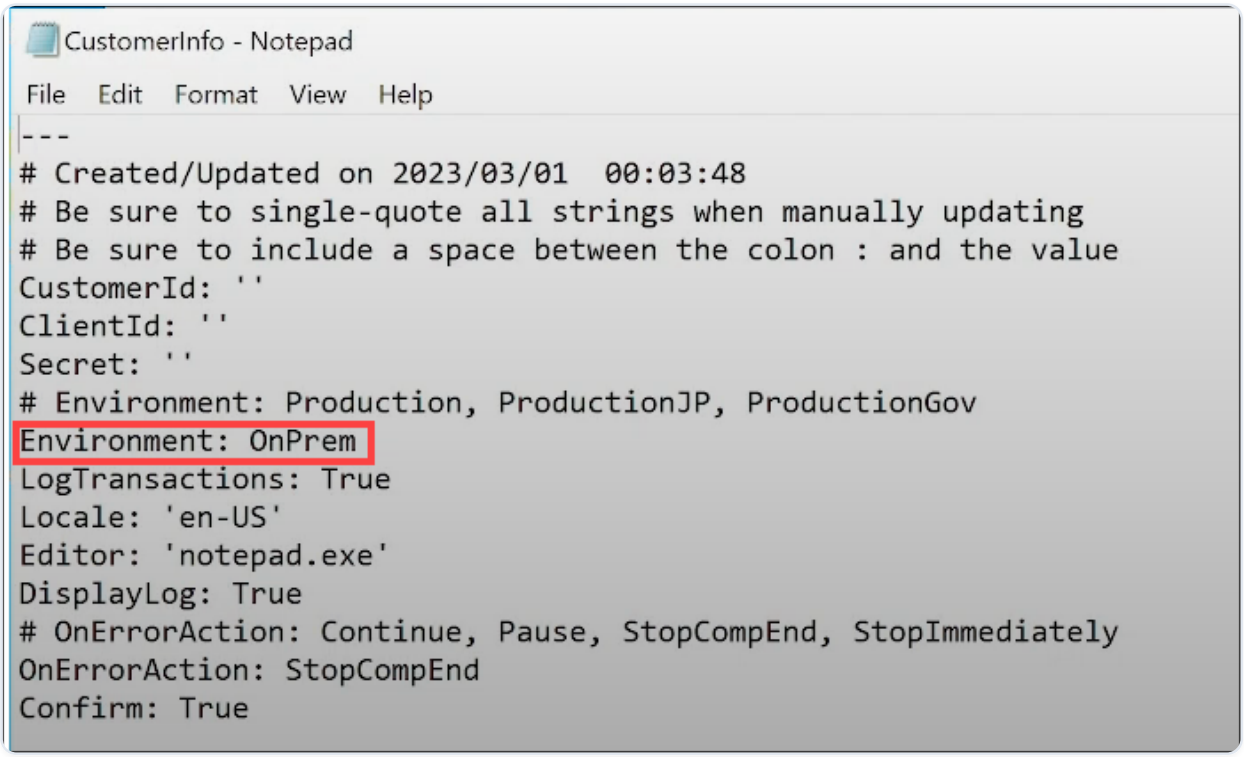
4. ソースサイトの **Export** フォルダーから `.yml` ファイルをターゲットサイトの `%HOMEPATH%\\Documents\\Citrix\\AutoConfig` フォルダーにコピーします。



5. `Set-CvadAcCustomerInfoFile` コマンドを使用して、作業している環境を指定します。例:

```
Set-CvadAcCustomerInfoFile -Environment OnPrem
```

このコマンドは、環境で **CustomerInfo** ファイルを更新します。



6. 次のコマンドを使用して構成ファイルを移行します。

```
Import-CvadAcToFile
```

`AutoConfig` フォルダー以外のフォルダーからインポートする場合は、次を実行します。

```
Import-CvadAcToFile -Sourcefolder PATH
```

注:

ホスト接続を移行する場合は、各ホストタイプの接続情報で `CvadAcSecurity.yml` ファイルを更新します。ホスト接続のセキュリティファイルを更新するを参照してください。

エラーまたは例外が発生した場合は、ログファイルの「Fixups」セクションを参照してください。

7. Web Studioを使用して、構成がターゲットサイトに移行されていることを確認します。

移行用自動構成ツール コマンドレット

このページでは、移行のユースケースでツールがサポートするすべてのコマンドレットとパラメーターを一覧表示します。

すべてのコマンドレットは、次のいずれかの型のパラメーターを受け取ります。

- 文字列
- 文字列のリスト
- ブール値: `$true` または `$false`
- SwitchParameter: パラメータが存在する場合は `$true` を意味し、パラメータが存在しない場合は `$false` を意味します。

> **注:**
>
> SwitchParameter は真偽の選択に推奨される方法ですが、レガシーの問題により、ツールでは引き続きブール値が使用されます。

次の表は、すべてのコマンドレットの概要です。各コマンドレットがサポートするパラメータについては、各セクションを参照してください。

カテゴリ	コマンドレット	説明
オンプレミスからクラウドへの移行	`Export-CvadAcToFile`	オンプレミスファイルをYAMLファイルにエクスポートします。
	`Import-CvadAcToSite`	YAMLファイルをクラウドにインポートします。作成、更新、削除の操作をサポートします。
	`Merge-CvadAcToSite`	YAMLファイルをクラウドにインポートします。作成および更新の操作をサポートします。
	`New-CvadAcToSite`	YAMLファイルをクラウドにインポートします。作成およ

カテゴリ	コマンドレット	説明
		び更新の操作をサポートします。
	`Sync-CvadAcToSite`	エクスポートとインポートを1ステップで実行します。
	きめ細かな移行 コンポーネントの場合は、上記のコマンドでパラメータを使用します。例: `MachineCatalogs`、`Tags`。コンポーネント名の場合は、上記のコマンドでパラメータを使用します。例: `IncludeByName`、`ExcludeByName`。	コンポーネントまたはコンポーネント名のみを選択的に移行する
クラウドからクラウドへのコマンドレット	`Backup-CvadAcToFile`	クラウドサイトからすべての構成をバックアップします。
	`Restore-CvadAcToSite`	バックアップYAMLファイルをクラウドサイトに復元します。このクラウドサイトは、ソースクラウドサイトと同じでも異なっていてもかまいません。
	`Remove-CvadAcFromSite`	クラウドからコンポーネントメンバーを削除します。
	きめ細かい移行 コンポーネントの場合は、上記のコマンドでパラメータを使用します。例: `MachineCatalogs`、`Tags`。コンポーネント名の場合は、上記のコマンドでパラメータを使用します。例: `IncludeByName`、`ExcludeByName`。	コンポーネントまたはコンポーネント名のみを選択的に移行する

カテゴリ	コマンドレット	説明
その他の基本コマンドレット	`Compare-CvadAcToSite`	オンプレミスの.ymlファイルをクラウド構成と比較します。
前提条件関連のコマンドレット	`New-CvadAcCustomerInfoFile`	顧客情報ファイルを作成します。
	`Set-CvadAcCustomerInfoFile`	既存の顧客情報ファイルを更新します。
サポートおよびトラブルシューティングのコマンドレット	`New-CvadAcZipInfoForSupport`	すべてのログファイルと.ymlファイルを単一のzipファイルに圧縮し、サポートのためにCitrix®に送信します。
	`Get-CvadAcStatus`	接続をテストし、すべての前提条件が満たされていることを確認するために使用します。ツールに関する情報（バージョン番号、クラウドとの接続、コネクタの状態など）を返します。
	`Test-CvadAcConnectionWithSite`	クラウドサイトとの接続をテストします。
	`Find-CvadAcConnector`	既存のコネクタを特定し、その実行状態を判断します。
	`Get-CvadAcCustomerSites`	すべての顧客サイトのリストを返します。
	`New-CvadAcTemplateToFile`	選択したコンポーネントのテンプレートファイルを作成します。
	`Show-CvadAcDocument`	このドキュメントをデフォルトのブラウザに表示します。
	`Find-CvadAcInFile`	ファイル内検索は、ワイルドカードを含む可能性のある1つ以上の名前に一致するメン

カテゴリ	コマンドレット	説明
		バーを探して、コンポーネントのYAMLファイルを検索します。
サイトアクティベーションコマンドレット(#site-activation-cmdlets)	`Set-CvadAcSiteActiveStateOnPrem`	オンプレミスサイトの状態をアクティブまたは非アクティブのいずれかに設定します。
	`Set-CvadAcSiteActiveStateCloud`	クラウドサイトの状態をアクティブまたは非アクティブのいずれかに設定します。
複数のオンプレミスサイトをマージするコマンドレット(#merging-multiple-on-premises-sites-cmdlets)	`New-CvadAcSiteMergingInfo`	サイトマージのプレフィックス/サフィックス情報セットを作成します。
	`Set-CvadAcSiteMergingInfo`	既存のサイトマージのプレフィックス/サフィックス情報セットを更新します。
	`Remove-CvadAcSiteMergingInfo`	既存のサイトマージのプレフィックス/サフィックス情報セットを削除します。

パラメーターとその使用方法の詳細については、「きめ細かな移行パラメーター」を参照してください。

基本的なコマンドレット

オンプレミスからクラウドへのコマンドレット

- `Export-CvadAcToFile` - オンプレミスファイルをYAMLファイルにエクスポートします。

  オンプレミス設定から構成をエクスポートします。これは、自動構成のデフォルトのエクスポート操作です。オンプレミスサイト構成には変更は加えられません。エクスポートされたファイルは、一意の名前が付けられた**Export**サブフォルダー内のディレクトリ *%HOMEPATH%\Documents\Citrix\AutoConfig* に配置されます。フォルダー *%HOMEPATH%\Documents\Citrix\AutoConfig* には、常に最新のエクスポートされたオンプレミスサイト構成が含まれています。

  パラメーター:

名前	説明	必須ですか?	タイプ
コンポーネントによる移行	を参照してください(#migrate-by-components)		SwitchParameters
オブジェクト名によるフィルタリング	「オブジェクト名によるフィルタリング」を参照してください(#filtering-by-object-names)		文字列のリスト
`TargetFolder`	エクスポート先のフォルダーを指定します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`AdminAddress`	エクスポートがDelivery Controllerで実行されていない場合に、Delivery ControllerのDNSまたはIPアドレスを指定します。		文字列
`CheckUserAndMachines`	ユーザーとマシンがActive Directoryに存在するかどうかを確認します。Active Directoryに存在しないユーザーとマシンは、インポートの失敗につながる可能性があります。		`$true` または `$false`

名前	説明	必須ですか?	タイプ
`ZipResults`	バックアップされたYAMLファイルを単一のzipファイルに圧縮します。このファイルは、バックアップされたYAMLファイルと同じフォルダーにあり、フォルダーと同じ名前を持ちます。		SwitchParameter

戻り値:

- Cmdlet の戻り値を参照してください。

データをクラウドにインポートする方法は3つあります。特定のコマンドレットを実行すると、クラウドサイトで次の3つのアクションの組み合わせのいずれかが実行されます。

- 追加、更新、および削除
- 追加と更新のみ
- 追加のみ

コマンドレット	追加	更新	削除
インポート	X	X	X
マージ	X	X	
新規	X		

- `Import-CvadAcToSite` - YAMLファイルをクラウドにインポートします。作成、更新、削除操作をサポートします。

  すべてのオンプレミスファイルをクラウドにインポートします。このコマンドは、クラウドの最終状態がオンプレミスの状態と同一であることを保証します。このオプションは、クラウドに存在する変更をすべて削除します。インポートされたサイト構成ファイルは、*%HOMEPATH%\Documents\Citrix\AutoConfig* から取得されます。*注意して使用してください。*

パラメーター:

名前	説明	必須ですか?	タイプ
コンポーネントによる移行	コンポーネントによる移行を参照してください。		SwitchParameters
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリングを参照してください。		文字列のリスト
クラウドアクセスパラメータ	クラウドアクセスパラメーターを参照してください。		SwitchParameters
`SourceFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代替ルートフォルダーを識別します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true` または `$false`
`Merge`	`$true` に設定すると、クラウドサイトにコンポーネントのみを追加します。コンポーネントは削除されません。コン		`$true` または `$false`

名前	説明	必須ですか?	タイプ
	ポーネントを削除するには、`$false`に設定します。		
`AddOnly`	`$true`に設定すると、新しいコンポーネントのみを追加し、既存のコンポーネントを更新または削除しません。更新と削除を許可するには、`$false`に設定します。このパラメーターが`$true`の場合、`Merge`は無視されます。		`$true`または`$false`
`MergePolicies`	ポリシー設定とフィルターをマージします。マージは、インポートされるポリシーがクラウドDDCに既に存在する場合にのみ行われます。ポリシーをマージした結果、クラウドDDCポリシーには、既存の設定とフィルターに加えて、インポートされる新しい設定とフィルターが含まれます。設定とフィルターの競合が発生した場合、インポートされた値が優先されることに注意してください。		スイッチパラメーター
`OnErrorAction`	「OnErrorAction パラメーター」を参照		文字列

名前	説明	必須ですか?	タイプ
	してください(/ja-jp/citrix-virtual-apps-desktops/2511/upgrade-migrate/auto-config-troubleshoot#onerroraction-parameter)。		

戻り値：

- 「Cmdlet の戻り値」を参照してください(#cmdlet-return-values)

- `Merge-CvadAcToSite` - YAMLファイルをクラウドにインポートします。作成および更新操作をサポートします。

  オンプレミスファイルをクラウドにマージしますが、クラウドまたはオンプレミスサイトのコンポーネントを削除することは*ありません*。これにより、クラウドで既に行われた変更が保持されます。Citrix Cloud に同じ名前のコンポーネントが存在する場合、このコマンドはそのコンポーネントを変更できます。これは、自動構成のデフォルトのインポート操作です。マージされたサイト構成ファイルは、*%HOMEPATH%\Documents\Citrix\AutoConfig* から取得されます。

  パラメーター：

名前	説明	必須？	タイプ
コンポーネントによる移行	「コンポーネントによる移行」を参照してください(#migrate-by-components)。		SwitchParameters
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリングを参照してください。		文字列のリスト
クラウドアクセスパラメータ	クラウドアクセスパラメーターを参照してください。		SwitchParameters

名前	説明	必須？	タイプ
`SourceFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代替ルートフォルダーを識別します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true` または `$false`
`Merge`	`$true` に設定すると、クラウドサイトにコンポーネントのみを追加します。コンポーネントは削除されません。コンポーネントを削除するには、`$false` に設定します。		`$true` または `$false`
`AddOnly`	`$true` に設定すると、新しいコンポーネントのみを追加し、既存のコンポーネントを更新または削除しません。更新と削除を許可するには、`$false` に設定します。このパラメーターが `$true`		`$true` または `$false`

名前	説明	必須？	タイプ
	の場合、`Merge` は無視されます。		
`MergePolicies`	ポリシー設定とフィルターをマージします。マージは、インポートされるポリシーがクラウドDDCに既に存在する場合にのみ行われます。ポリシーをマージした結果、クラウドDDCポリシーには、既存の設定とフィルターに加えて、インポートされる新しい設定とフィルターが含まれます。設定とフィルターの競合が発生した場合、インポートされた値が優先されることに注意してください。		SwitchParameter
`OnErrorAction`	OnErrorAction パラメーター を参照してください。		文字列

戻り値:

- Cmdlet の戻り値 を参照してください。

- `New-CvadAcToSite` - YAMLファイルをクラウドにインポートします。作成および更新操作をサポートします。

  オンプレミスサイト構成をクラウドにインポートしますが、新しいコンポーネントのみを追加します。既存のクラウドサイトコンポーネントは更新も削除もされません。既存のクラウドサイトコンポーネントを変更しないままにする必要がある場合は、このコマンドを使用してください。

パラメーター:

名前	説明	必須?	型
コンポーネントによる移行	コンポーネントによる移行 を参照してください。		SwitchParameters
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリング を参照してください。		文字列のリスト
クラウドアクセスパラメーター	クラウドアクセスパラメーターを参照してください。		SwitchParameters
`SourceFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代替ルートフォルダーを識別します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true` または `$false`
`OnErrorAction`	OnErrorAction parameterを参照してください。		文字列

戻り値:

    - Cmdlet return valuesを参照してください

- `Sync-CvadAcToSite` - 1つのステップでエクスポートとインポートを実行します。

  同期は、1つのステップでエクスポートとインポートの両方を実行します。`SourceTargetFolder`パラメーターを使用して、エクスポート/インポートの宛先フォルダーを指定します。

  パラメーター:

名前	説明	必須?	種類
コンポーネント別に移行	Migrate by componentsを参照してください		SwitchParameters
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリングを参照		文字列のリスト
クラウドアクセスパラメーター	クラウドアクセスパラメーターを参照		SwitchParameters
`SourceTargetFolder`	エクスポート/インポートの保存先フォルダーを指定します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`AdminAddress`	エクスポートがデリバリーコントローラーで実行されていない場合に、デリバリーコントローラーのDNSまたはIPアドレスを指定します。		文字列

名前	説明	必須?	種類
`Quiet`	コンソールへのログ出力を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。`$false` に設定すると、ログ表示を抑制します。		`$true` または `$false`
`Merge`	`$true` に設定すると、クラウドサイトにコンポーネントを追加するだけです。コンポーネントは削除されません。コンポーネントを削除するには `$false` に設定します。		`$true` または `$false`
`AddOnly`	`$true` に設定すると、新しいコンポーネントのみを追加し、既存のコンポーネントを更新または削除しません。更新と削除を許可するには `$false` に設定します。このパラメーターが `$true` の場合、`Merge` は無視されます。		`$true` または `$false`
`MergePolicies`	ポリシー設定とフィルターをマージします。マージは、インポートされるポリシーがクラウドDDCに既に存在する場合にのみ行われます。ポリシーを		スイッチパラメーター

名前	説明	必須?	種類
	マージした結果、クラウドDDCポリシーには、既存の設定とフィルターに加えて、インポートされる新しい設定とフィルターが含まれます。設定とフィルターの競合が発生した場合、インポートされた値が優先されることに注意してください。		

戻り値:

- 「Cmdlet の戻り値」を参照してください(#cmdlet-return-values)

クラウド間コマンドレット

- `Backup-CvadAcToFile` - クラウドサイトからすべての構成をバックアップします。

  クラウド構成を.ymlファイルにエクスポートします。このバックアップは、バックアップおよび復元プロセスで失われたコンポーネントを復元するために使用できます。

  パラメーター:

名前	説明	必須？	型
コンポーネントによる移行	「コンポーネントによる移行」を参照してください(#migrate-by-components)		スイッチパラメーター
クラウドアクセスパラメーター	クラウドアクセスパラメータを参照してください		SwitchParameters

名前	説明	必須？	型
`TargetFolder`	エクスポート先のフォルダーを指定します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false`に設定します。		`$true` または `$false`
`ZipResults`	バックアップされたYAMLファイルを単一のzipファイルに圧縮します。ファイルはバックアップされたYAMLファイルと同じフォルダーにあり、フォルダーと同じ名前です。		SwitchParameter

戻り値:

- コマンドレットの戻り値を参照してください。

- `Restore-CvadAcToSite` - バックアップされたYAMLファイルをクラウドサイトに復元します。このクラウドサイトは、ソースクラウドサイトと同じでも異なっていてもかまいません。

  クラウドサイトを以前の構成に復元します。インポートされたファイルは、`-RestoreFolder`パラメーターを使用して指定されたフォルダーから取得されます。このパラメーターは、クラウドサイトに復元する.ymlファイルを含むフォルダーを識別します。これは、完全修飾フォルダー指定である必要があります。このコマンドレットは、以前の構成

に戻すため、またはクラウドサイトをバックアップおよび復元するために使用できます。このコマンドは、クラウドサイトの追加、削除、更新を行うことができます。

パラメーター:

名前	説明	必須ですか?	タイプ
コンポーネントによる移行	コンポーネントによる移行を参照してください。		SwitchParameters
オブジェクト名によるフィルタリング	を参照してください (#filtering-by-object-names)。		文字列のリスト
クラウドアクセスパラメーター	を参照してください (#cloud-accessing-parameters)。		SwitchParameters
`RestoreFolder`	.ymlファイルをクラウドサイトに復元するためのフォルダーを識別します。これは完全修飾フォルダー指定である必要があります。		文字列
`Locale`	エクスポートできる人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true` または `$false`

名前	説明	必須ですか?	タイプ
`Merge`	`$true` に設定すると、クラウドサイトにコンポーネントのみを追加します。コンポーネントは削除されません。コンポーネントを削除するには、`$false` に設定します。		`$true` または `$false`
`AddOnly`	`$true` に設定すると、新しいコンポーネントのみを追加し、既存のコンポーネントを更新または削除しません。更新と削除を許可するには、`$false` に設定します。このパラメーターが `$true` の場合、`Merge` は無視されます。		`$true` または `$false`
`MergePolicies`	ポリシー設定とフィルターをマージします。マージは、インポートされるポリシーがクラウドDDCにすでに存在する場合にのみ行われます。ポリシーをマージした結果、クラウドDDCポリシーには、既存の設定とフィルターに加えて、インポートされる新しい設定とフィルターが含まれます。設定とフィルターの競合が発生した場合、インポート		SwitchParameter

名前	説明	必須ですか?	タイプ
	された値が優先されることに注意してください。		
`OnErrorAction`	「」を参照してください(/ja-jp/citrix-virtual-apps-desktops/2511/upgrade-migrate/auto-config-troubleshoot#onerroraction-parameter)。		文字列

戻り値:

- Cmdlet の戻り値を参照してください。

- `Remove-CvadAcFromSite` – クラウドからコンポーネントメンバーを削除します。

  サイト全体をリセットしたり、コンポーネントからメンバーアイテムを削除したりできます(例: カタログのリストから1つのマシンカタログを削除する)。これは、`IncludeByName` パラメーターと組み合わせて使用することで、特定のメンバーを選択的に削除できます。

  パラメーター:

名前	説明	必須ですか？	種類
コンポーネントによる移行	コンポーネントによる移行を参照してください。		SwitchParameters
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリングを参照してください。		文字列のリスト
クラウドアクセスパラメーター	「クラウドアクセスパラメータ」を参照してください(#cloud-accessing-parameters)		スイッチパラメータ

名前	説明	必須ですか？	種類
`Quiet`	コンソールへのログ出力を抑制します。		スイッチパラメータ
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false`に設定します。		`$true` または `$false`

戻り値:

- コマンドレットの戻り値を参照してください

その他の基本コマンドレット

- `Compare-CvadAcToSite` - オンプレミスの.ymlファイルをクラウド構成と比較し、`Import`、`Merge`、または`Restore`コマンドレットによって行われた変更のレポートを生成します。

  パラメーター:

名前	説明	必須ですか？	タイプ
コンポーネントによる移行	コンポーネントによる移行を参照してください。		SwitchParameters
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリングを参照してください。		文字列のリスト
クラウドアクセスパラメーター	クラウドアクセスパラメーターを参照してください。		SwitchParameters
`SourceFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代替ルートフォルダーを識別します。		文字列

名前	説明	必須ですか？	タイプ
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true` または `$false`
`Merge`	`$true` に設定すると、クラウドサイトにコンポーネントのみを追加します。コンポーネントは削除されません。コンポーネントを削除するには、`$false` に設定します。		`$true` または `$false`
`AddOnly`	`$true` に設定すると、新しいコンポーネントのみを追加し、既存のコンポーネントを更新または削除しません。更新と削除を許可するには、`$false` に設定します。このパラメーターが `$true` の場合、`Merge` は無視されます。		`$true` または `$false`
`OnErrorAction`	「OnErrorAction parameter」を参照してください(/ja-jp/		文字列

名前	説明	必須ですか？	タイプ
	citrix-virtual-apps-desktops/2511/upgrade-migrate/auto-config-troubleshoot#onerroraction-parameter)。		

戻り値:

- 「Cmdlet return values」を参照してください(#cmdlet-return-values)

詳細な移行パラメータ

コンポーネントによる移行

サポートするコマンドレットで、以下のコンポーネントを指定できます。コンポーネントパラメータが指定されていない場合、`All`オプションが自動的に選択されます。エラーを避けるため、コンポーネントを以下の順序で移行することをお勧めします。

- `All`
- `Tags`
- `AdminRoles`
- `AdminScopes`
- `HostConnections`
- `MachineCatalogs`
- `StoreFronts`
- `DeliveryGroups`
- `ApplicationGroups`
- `ApplicationFolders`
- `Applications`
- `GroupPolicies`
- `UserZonePreference`

オブジェクト名によるフィルタリング

コンポーネント名による移行

`IncludeByName` と `ExcludeByName` パラメーターを使用すると、名前でコンポーネントメンバーをコマンドレットに含めたり除外したりできます。サポートされているコマンドレットでは、一度に1つのコンポーネント（例：デリバリーグループ）のみを選択できます。コンポーネントメンバーが両方の領域にある場合、除外は他のすべてのパラメーターを上書きし、除外されたコンポーネントとメンバー名を特定するエントリがログ修正リストに作成されます。

`IncludeByName`と`ExcludeByName`は、コンポーネントメンバー名のリストを受け取ります。任意の名前には、1つ以上のワイルドカードを含めることができます。2種類のワイルドカードがサポートされています。メンバー名に特殊文字が含まれている場合、コンポーネントメンバー名のリストは単一引用符で囲む必要があります。

- * 任意の数の文字に一致します
- ？1文字に一致します

`IncludeByName` と `ExcludeByName` は、各メンバーが明示的であるかワイルドカードを含むことができるメンバーのリストを含むファイルも受け取ることができます。ファイルの各行には1つのメンバーを含めることができます。メンバー名から先頭と末尾のスペースはトリミングされます。ファイル名の前には @ 記号を付け、単一引用符で囲む必要があります（@ が再解釈されないようにするためのPowerShellの要件です）。メンバー名と混在させることに加えて、複数のファイルをリストすることもできます。

名前が `DgSite1` で始まり、`Home2` を含むすべてのデリバリーグループをマージする例は、次のように記述されます。

```
Merge-CvadAcToSite –DeliveryGroups –IncludeByName DgSite1*,*Home2*
```

デリバリーグループ名別

`ByDeliveryGroupName` は、アプリケーションおよびアプリケーション グループのデリバリー グループ名でフィルター処理します。このパラメーターは常に、デリバリー グループの関連付けに基づいて含めるメンバーを識別するインクルージョン リストです。

`ByDeliveryGroupName` は、デリバリー グループ名のリストを受け取ります。任意の名前には、1 つ以上のワイルドカードを含めることができます。2 種類のワイルドカードがサポートされています。

- * は任意の数の文字に一致します
- ？は単一の文字に一致します

次の例では、`EastDg` で始まるすべてのデリバリー グループ名を参照するすべてのアプリケーションをマージします。

```
Merge-CvadAcToSite –Applications –ByDeliveryGroupName EastDg*
```

無効なものを除外

`ExcludeDisabled` は、無効になっているすべてのアプリケーションおよびアプリケーション グループをインポート操作から除外します。`ExcludeDisabled` の既定値は `false` であり、これはすべてのアプリケーションおよびアプリケーション グループが有効状態に関係なくインポートされることを意味します。

マシン名別

`ByMachineName` は、マシン カタログおよびデリバリー グループのマシン名でフィルター処理します。このパラメーターは常に、マシン名の関連付けに基づいて含めるメンバーを識別するインクルージョン リストです。

`ByMachineName` は、マシン名のリストを受け取ります。任意の名前には、1 つ以上のワイルドカードを含めることができます。2 種類のワイルドカードがサポートされています。

- * は任意の数の文字に一致します
- ? は単一の文字に一致します

エクスポートまたはインポート時に `ByMachineName` を使用し、マシン名フィルターによってマシン カタログまたはデリバリー グループにマシンが存在しない場合、そのマシン カタログまたはデリバリー グループはエクスポートまたはインポートから除外されます。

> **注:**
>
> 任意のインポート型コマンドレットで `ByMachineName` を使用すると、`MergeMachines` が `$true` に設定されます。

マシンのマージ

`MergeMachines` が `$true` に設定されている場合、インポート操作はマシンをマシンカタログまたはデリバリーグループにのみ追加するように指示します。マシンは削除されないため、増分追加操作が可能です。

`MergeMachines` のデフォルトはfalseであり、マシンカタログまたはデリバリーグループの.ymlファイルに存在しないマシンは削除されます。`ByMachineName` が使用されると `MergeMachines` は `$true` に設定されますが、`MergeMachines` をfalseに設定することで上書きできます。

前提条件関連のコマンドレット

- `New-CvadAcCustomerInfoFile` - 顧客情報ファイルを作成します。デフォルトでは、顧客情報ファイルは *%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。

  パラメーター:

名前	説明	必須？	タイプ
`CustomerId`	顧客ID。	x	文字列
`ClientId`	Citrix Cloudで作成された顧客のクライアントID。このパラメーターを使用する場合は、CustomerIdとSecretを指定する必要があります。	条件付き	文字列
`Secret`	Citrix Cloudで作成された顧客のシークレットキー。このパラメーターを使用する場合は、CustomerIdとClientIdを指定する必要があります。	条件付き	文字列
`Environment`	Production、ProductionGov、またはProductionJP環境。		列挙
`LogFileName`	ログファイルプレフィックスをCitrixLogから別のものに変更します。		文字列
`AltRootUrl`	Citrixの指示の下でのみ使用してください。		文字列

名前	説明	必須？	タイプ
`StopOnError`	最初のエラーで操作を停止します。		`$true` または `$false`
`TargetFolder`	ルートフォルダとして、*%HOMEPATH%\Documents\Citrix\AutoConfig* の代わりに指定されたフォルダを使用します。		文字列
`Locale`	ツールが実行されているシステムから派生したロケールの代わりに、指定されたロケールを使用します。		文字列
`Editor`	各コマンドレットの完了時にログを表示するために、指定されたエディターを使用します。Notepad.exe が既定のエディターです。このパラメーターには、エディターへの完全修飾ファイル指定を含める必要があり、エディターはログファイル指定を唯一のパラメーターとして受け取る必要があります。		文字列
`SecurityCsvFileSpec`	Citrix Identity and Access Managementからダウンロードされた SecurityClient.csv ファイルを指す完全		文字列

名前	説明	必須？	タイプ
	修飾ファイル指定。このパラメーターを使用する場合は、CustomerIdを指定する必要があります。		

戻り値:

- Cmdletの戻り値を参照

- `Set-CvadAcCustomerInfoFile` - 既存の顧客情報ファイルを更新します。コマンドレットで指定されたパラメーターのみが変更されます。CustomerInfo.ymlファイル内の指定されていないすべてのパラメーター値は変更されません。

  パラメーター:

名前	説明	必須?	種類
`CustomerId`	顧客のID。		文字列
`ClientId`	Citrix Cloudで作成された顧客のクライアントID。		文字列
`Secret`	Citrix Cloudで作成された顧客のシークレットキー。		文字列
`Environment`	Production、ProductionGov、またはProductionJP環境。		列挙型
`LogFileName`	ログファイルプレフィックスをCitrixLogから別のものに変更します。		文字列
`StopOnError`	最初のエラーで操作を停止します。		`$true` または `$false`

名前	説明	必須?	種類
`TargetFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代わりに、指定されたフォルダーをルートフォルダーとして使用します。		文字列
`Locale`	ツールが実行されているシステムから派生したロケールの代わりに、指定されたローカルを使用します。		文字列
`Editor`	各コマンドレットの完了時にログを表示するために、指定されたエディターを使用します。Notepad.exeがデフォルトのエディターです。このパラメーターには、エディターへの完全修飾ファイル指定を含める必要があり、エディターはログファイル指定を唯一のパラメーターとして受け取る必要があります。		文字列
`SecurityCsvFileSpec`	Citrix Identity and Access Managementからダウンロードされた SecurityClient.csv ファイルを指す完全修飾ファイル指定。このパラメーターを		文字列

名前	説明	必須?	種類
	使用する場合、CustomerIdを指定する必要があります。		

戻り値:

- コマンドレットの戻り値を参照してください

前提条件関連のパラメーター

クラウドアクセスパラメーターに加えて、前提条件関連のコマンドレットで以下のパラメーターを使用できます。

- `Environment` – ProductionまたはProductionGov環境。
- `LogFileName` – ログファイルプレフィックスをCitrixLogから別のものに変更します。
- `StopOnError` – 最初のエラーで操作を停止します。
- `AlternateRootFolder` – *%HOMEPATH%\Documents\Citrix\AutoConfig*の代わりに、指定されたフォルダーをルートフォルダーとして使用します。
- `Locale` – ツールが実行されているシステムから派生したロケールの代わりに、指定されたロケールを使用します。
- `Editor` – 各コマンドレットの完了時にログを表示するために指定されたエディターを使用します。Notepad.exeがデフォルトのエディターです。このパラメーターには、エディターへの完全修飾ファイル指定を含める必要があり、エディターはログファイル指定を唯一のパラメーターとして受け取る必要があります。

サポートおよびトラブルシューティングのコマンドレット

- `New-CvadAcZipInfoForSupport` - すべてのログファイルと.ymlファイルを単一のzipファイルに圧縮し、サポートのためにCitrixに送信します。顧客の機密情報（CustomerInfo.ymlおよびCvadAcSecurity.yml）はzipに含まれません。Icon.ymlファイルもサイズが大きいため除外されます。zipファイルは、日付とタイムスタンプに基づいて、*%HOMEPATH%\Documents\Citrix\AutoConfig*に配置され、*CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip*という名前が付けられます。このzipファイルはバックアップとしても機能します。

  パラメーター:

名前	説明	必須?	タイプ
`TargetFolder`	zipファイルを作成して保存するターゲットフォルダーを指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter

戻り値:

- zipファイル名と場所を含むzipファイルがコマンドプロンプトに表示されます。

- `Get-CvadAcStatus` - 接続をテストし、すべての前提条件が満たされていることを確認するために使用します。バージョン番号、クラウドとの接続、コネクタの状態など、ツールに関する情報を返します。

  パラメーター:

名前	説明	必須?	タイプ
クラウドアクセスパラメータ	クラウドアクセスパラメータを参照してください。		SwitchParameters
`SiteId`	接続先のサイトを識別します。		文字列
`AdminAddress`	これは、管理者のアクセスレベルを確認するために使用されるオンプレミスのDelivery ControllerのDNSまたはIPアドレスです。ツールがDelivery Controllerで実行されていない場合に必要です。		文字列

  戻り値:

◦ 各項目の結果を表示します。

- `Test-CvadAcConnectionWithSite` – クラウドサイトとの接続をテストし、通信接続が機能していることを確認します。このコマンドレットは、クラウドアクセスパラメータまたはCustomerInfo.ymlファイルを使用して、顧客の接続情報を指定します。

  パラメータ:

名前	説明	必須?	タイプ
クラウドアクセスパラメータ	クラウドアクセスパラメータを参照してください。		SwitchParameters
`Quiet`	コンソールへのログ出力を抑制します。		SwitchParameter

  戻り値:

  ◦ テスト結果はコマンドラインに表示されます。

- `Find-CvadAcConnector` - 既存のコネクタを特定し、その実行状態を判断します。このコマンドレットは、CustomerInfo.yml ファイルまたは顧客IDパラメータからの情報を使用して、顧客のコネクタを特定します。

  パラメータ:

名前	説明	必須ですか?	型
`CustomerInfoFileSpec`	デフォルトの場所と名前を上書きするための、顧客情報ファイルを指すファイル指定。`CustomerId` パラメータが指定されている場合、このパラメータは無視されます。		文字列
`CustomerId`	顧客のID。このパラメーターは、CustomerInfo.yml		文字列

名前	説明	必須ですか?	型
	ファイル内の同じ値を上書きします。		

戻り値:

- 結果はコマンドラインに表示されます。

- `Get-CvadAcCustomerSites` - すべての顧客サイトのリストを返します。このコマンドレットは、クラウドアクセスパラメーターまたはCustomerInfo.ymlファイルを使用して、顧客の接続情報を指定します。

  パラメーター:

  - クラウドアクセスパラメーターを参照してください

  戻り値:

  - 見つかった顧客サイトIDのリストを表示します。

- `New-CvadAcTemplateToFile` – 選択したコンポーネントのテンプレートファイルを作成し、インポートファイルを手動で作成できるようにします。

  パラメーター:

名前	説明	必須?	タイプ
コンポーネントによる移行	を参照してください(#migrate-by-components)		SwitchParameters
`TargetFolder`	エクスポート先のフォルダーを指定します。		文字列

  戻り値:

  - を参照してください(#cmdlet-return-values)

- `Show-CvadAcDocument` - 既定のブラウザーでこのドキュメントを表示します。

  パラメーター:

- なし。

戻り値:

- 既定のWebブラウザーでこのWebページを表示します。

- `Find-CvadAcInFile` - ファイル内検索は、ワイルドカードを含む1つ以上の名前に一致するメンバーをコンポーネントのYAMLファイルで検索します。結果は、見つかったメンバーのレポートです。ファイル内検索は、一度に1つのコンポーネントしか検索できません。ファイル内検索は、現在のフォルダーとすべてのサブフォルダー内のすべてのYAMLファイルを検索します。検索するファイルの数を制限するには、`FindSourceFolder`を使用します。

  パラメーター:

名前	説明	必須?	種類
コンポーネントによる移行	を参照してください (#migrate-by-components)。注: `-All` の値は無効です。		SwitchParameters
`IncludeByName`	サイトのアクティブ状態をアクティブに設定する際に含めるデリバリーグループの名前を指定するリスト。名前に「*」と「?」のワイルドカードがサポートされています。		文字列のリスト
`Unique`	一意に見つかったメンバーのみを報告します。		SwitchParameter
`IncludeYaml`	メンバー固有のYAMLを含めます。		SwitchParameter
`FindSourceFolder`	検索を開始するフォルダー。		文字列

名前	説明	必須?	種類
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		SwitchParameter
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter

戻り値:

- 指定されたコンポーネントについて、検出されたメンバーを含むレポートを作成します。

サイトアクティベーションコマンドレット

サイトのアクティベーションとこれらのコマンドレットの使用方法の詳細については、「サイトのアクティベーション」を参照してください。

- `Set-CvadAcSiteActiveStateOnPrem` - オンプレミスサイトの状態をアクティブまたは非アクティブに設定します。

  パラメーター:

名前	説明	必須ですか？	タイプ
クラウドアクセスパラメータ	クラウドアクセスパラメータを参照		SwitchParameters
`SiteActive`	存在する場合、オンプレミスサイトをアクティブに設定し、すべてのデリバリーグループからメンテナンスモードを削除します。このパラメータが存在しない場合、すべてのデリバリーグループにメンテナンスモードが設定されます。		SwitchParameter

名前	説明	必須ですか？	タイプ
`IncludeByName`	サイトのアクティブ状態をアクティブに設定する際に含めるデリバリーグループの名前を指定するリスト。名前に「*」と「?」のワイルドカードがサポートされています。		文字列のリスト
`ExcludeByName`	サイトのアクティブ状態をアクティブに設定する際に除外するデリバリーグループの名前を指定するリストです。名前に「*」と「?」のワイルドカードがサポートされています。		文字列のリスト
`Quiet`	コンソールへのログ出力を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには `$false` に設定します。		`$true or $false`

戻り値:

- Cmdlet の戻り値 を参照してください。

- `Set-CvadAcSiteActiveStateCloud` - クラウドサイトの状態をアクティブまたは非アクティブに設定します。

  パラメータ:

名前	説明	必須ですか？	タイプ
クラウドアクセスパラメータ	クラウドアクセスパラメータを参照してください		SwitchParameters
`SiteActive`	存在する場合、クラウドサイトをアクティブに設定し、すべてのデリバリーグループからメンテナンスモードを削除します。このパラメータが存在しない場合、すべてのデリバリーグループでメンテナンスモードが設定されます。		SwitchParameter
`IncludeByName`	サイトのアクティブ状態をアクティブに設定する際に含めるデリバリーグループの名前を指定するリスト。名前に「*」と「?」のワイルドカードがサポートされています。		文字列のリスト
`ExcludeByName`	サイトのアクティブ状態をアクティブに設定する際に除外するデリバリーグループの名前を指定するリスト。名前に「*」と「?」のワイルドカードがサポートされています。		文字列のリスト
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter

名前	説明	必須ですか？	タイプ
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true or $false`

戻り値:

- コマンドレットの戻り値を参照してください。

複数のオンプレミスサイトをマージするコマンドレット

サイトのマージとこれらのコマンドレットの使用方法の詳細については、複数のサイトを単一のサイトにマージするを参照してください。

- `New-CvadAcSiteMergingInfo` - サイトマージのプレフィックス/サフィックス情報セットを作成します。最初からすべてのプレフィックスまたはサフィックスを知っている必要はありません。これらは `Set-CvadAcSiteMergingInfo` で、または SiteMerging.yml ファイルを手動で編集することで更新できます。 パラメーター:

名前	説明	必須ですか？	型
`SiteName`	特定のサイトのプレフィックス/サフィックスのセットを識別するために使用される名前。実際のサイト名と一致してもよいが、一致する必要はない。	x	文字列
サイト統合パラメーター	サイト統合パラメーターを参照してください		SwitchParameters
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter

戻り値:

- なし

- `Set-CvadAcSiteMergingInfo` - 既存のサイト統合プレフィックス/サフィックス情報セットを更新します。

  パラメーター:

名前	説明	必須ですか？	タイプ
`SiteName`	特定のサイトのプレフィックス/サフィックスのセットを識別するために使用される名前。実際のサイト名と一致してもよいが、その必要はない。	x	文字列
サイト統合パラメーター	サイト統合パラメーターを参照		SwitchParameters
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter

  戻り値:

  - なし

- `Remove-CvadAcSiteMergingInfo` - 既存のサイト統合プレフィックス/サフィックス情報セットを削除します。

  パラメーター:

  - `SiteName` – サイトのプレフィックスとサフィックスのセットを識別します。これは文字列であり、必須です。

  戻り値:

  - なし

サイト統合パラメーター

サイト統合コマンドレットの実行時に、以下のパラメーターを使用できます。リストされているすべてのパラメーターは文字列です。

- `SiteName` – 特定のサイトのプレフィックス/サフィックスのセットを識別するために使用される名前。実際のサイト名と一致してもよいが、必須ではない。SiteName は必須パラメーターです。
- `AdminScopedPrefix` – 管理者スコープに適用するプレフィックス。
- `ApplicationPrefix` – アプリケーションに適用するプレフィックス。
- `ApplicationFolderPrefix` – アプリケーションフォルダーに適用するプレフィックス。`ApplicationFolderPrefix` は `ApplicationFolderRoot` と組み合わせることができます。
- `ApplicationFolderRoot` – アプリケーションフォルダーの新しいルートフォルダー。これにより、追加のフォルダー階層が作成されます。`ApplicationFolderRoot` は `ApplicationFolderPrefix` と組み合わせることができます。
- `ApplicationGroupPrefix` – アプリケーショングループのプレフィックス。
- `ApplicationUserPrefix` – ユーザーに表示されるアプリケーション名に適用するプレフィックス。
- `ApplicationAdminPrefix` – 管理者に表示されるアプリケーション名に適用するプレフィックス。
- `DeliveryGroupPrefix` – デリバリーグループに適用するプレフィックス。
- `GroupPolicyPrefix` – ポリシー名に適用するプレフィックス。
- `HostConnectionPrefix` – ホスト接続に適用するプレフィックス。
- `MachineCatalogPrefix` – マシンカタログに適用するプレフィックス。
- `StoreFrontPrefix` – StoreFront™ 名に適用するプレフィックス。
- `TagPrefix` – タグに適用するプレフィックス。
- `AdminScopedSuffix` – 管理者スコープに適用するサフィックス。
- `ApplicationSuffix` - アプリケーションに適用するサフィックス。
- `ApplicationFolderSuffix` – アプリケーションフォルダーに適用するサフィックス。`ApplicationFolderSuffix` は `ApplicationFolderRoot` と組み合わせることができます。
- `ApplicationGroupSuffix` – アプリケーショングループのサフィックス。
- `ApplicationUserSuffix` – ユーザーに表示されるアプリケーション名に適用するサフィックス。
- `ApplicationAdminSuffix` – 管理者に表示されるアプリケーション名に適用するサフィックス。
- `DeliveryGroupSuffix` – デリバリーグループに適用するサフィックス。

- `GroupPolicySuffix` – ポリシー名に適用するサフィックス。
- `HostConnectionSuffix` – ホスト接続に適用するサフィックス。
- `MachineCatalogSuffix` – マシンカタログに適用するサフィックス。
- `StoreFrontSuffix` – StoreFront名に適用するサフィックス。
- `TagSuffix` – タグに適用するサフィックス。
- `SiteRootFolder` – エクスポートおよびインポートに使用する完全修飾フォルダー名。ローカルフォルダーまたはファイル共有にすることができます。

汎用パラメーター

クラウドアクセスパラメーター

クラウドにアクセスするすべてのコマンドレットは、次の追加パラメーターをサポートしています。

> **注:**
>
> CustomerId、ClientId、および Secret は、CustomerInfo.yml ファイルに配置するか、次のパラメーターを使用してコマンドレットで指定できます。両方の場所で指定されている場合、コマンドレットパラメーターが優先されます。

- `CustomerId` – Rest API で使用される顧客 ID であり、すべての Rest API にアクセスするために必要です。顧客 ID は Citrix Cloud にあります。
- `ClientId` – Citrix Cloud Identity and Access Management Web サイトで作成された clientID。これは、すべての Rest API の認証に必要なベアラートークンを取得するために必要です。
- `Secret` – Citrix Cloud Identity and Access Management Web サイトで作成された秘密鍵。これは、すべての Rest API の認証に必要なベアラートークンを取得するために必要です。
- `CustomerInfoFileSpec` – デフォルトの場所と名前を上書きするための顧客情報ファイルを指すファイル指定。

移行モードパラメーター

クラウドサイト構成を変更するコマンドレット (`Import`、`Restore`、`Merge`、`New`、および `Sync`) は、さらなる柔軟性を提供するために、以下の追加パラメーターをサポートします。

- `CheckMode` – インポート操作を実行しますが、*変更は行いません*。予想されるすべての変更は、インポートが完了する前に報告されます。このコマンドを使用して、インポートが実行される前にテストできます。
- `BackupFirst` – クラウド構成を変更する前に、クラウドコンテンツを.ymlファイルにバックアップします。これはデフォルトで有効になっています。
- `Confirm` – trueの場合、クラウドサイト構成に変更を加えることをユーザーに確認するよう促します。`Remove` コマンドレットは、その破壊的な性質のため、プロンプトを表示します。自動スクリプト内で実行する場合など、プロンプトが不要な場合はfalseに設定します。`Confirm` はデフォルトでtrueです。
- `SecurityFileFolder` – これは、CustomerInfo.ymlファイルを含む完全修飾フォルダーであり、ローカルフォルダーまたは認証制御下にある可能性のあるネットワーク共有フォルダーを指す場合があります。ツールは資格情報を要求しません。ツールを実行する前に、制御されたリソースへのアクセスを取得する必要があります。
- `SiteName` – インポート時に使用するサイトマージのプレフィックスとサフィックスのセットを指定します。
- `SiteActive` – インポートされたサイトがアクティブか非アクティブかを指定します。デフォルトでは、このパラメーターは `$false` に設定されており、インポートされたサイトは非アクティブであることを意味します。

ログ表示パラメーター

`Export`、`Import`、`Sync`、`Restore`、`Backup`、`Compare`、および `Remove` コマンドレットは、操作が完了するとログファイルを表示します。`-DisplayLog` パラメーターを `$false` に設定することで、表示を抑制できます。ログファイルの表示には、デフォルトでNotepad.exeが使用されます。CustomerInfo.ymlファイルで別のエディターを指定できます。

```
Editor: C:\Program Files\Notepad++\notepad++.exe
```

コマンドレットの戻り値

ActionResult

すべてのコマンドレットは次の値を返します。

```
public class ActionResult

{

    public bool                         Overall_Success;
```

```
    public Dictionary&lt;string, string>   Individual_Success;

    public object                        CustomResult;

}
```

`Overall_Success` は、選択されたすべてのコンポーネントにおけるコマンドレット全体の成功を示す単一のブール値を返します。trueは成功、falseは失敗を意味します。

`Individual_Success` は、各主要コンポーネントに対して1つまたは3つの値を返します。コンポーネントの結果は、Success、Failure、またはSkippedのいずれかになります。Skippedは、そのコンポーネントがコマンドレットによる実行のために選択されなかったことを示します。

`CustomResult` はコマンドレット固有です。

CustomResult

`Import`、`Merge`、`Restore`、`Sync`、`Compare`、`Compare File`、および`Remove`は、`EvaluationResultData`の単一インスタンスに以下のカスタム結果情報を返します。

注：

`Export`および`Template`のコマンドレットは、カスタム結果を返しません。

```
 public class EvaluationResultData

 {

     public Dictionary&lt;string, Dictionary&lt;string, ActionResultValues
>> EvaluationResults;

     public int                 Added;

     public int                 Updated;

     public int                 Deleted;

     public int                 NoChange;

     public int                 TotalChanged;
```

```
    public EvaluationResults     OverallResult;

    public string               CloudBackupFolder;

    public string               SourceBackupFolder;

 }

 Where:

 public enum ActionResultValues

{

    Add,

    Update,

    Delete,

    Identical,

    DoNothing

 }

 public enum EvaluationResults

 {

    Success,

    Failure,

    Skipped

 }
```

`EvaluationResults`は、選択されたコンポーネントごとに1つのエントリを持つリストを表示します。キーはコンポーネント名であり、値は各コンポーネントメンバーのリストと、そのコンポー

ネントメンバーに対して実行されたアクションです。アクションは、`ActionResultValues`の値のいずれかになります。

`Added`、`Updated`、`Deleted`、および`NoChange`は、追加、更新、削除、またはアクションなしのコンポーネントメンバーの総数をこの順序で示します。

`TotalChanged`は、`Added`、`Updated`、および`Deleted`の合計です。

`OverallResult`は、コマンドレットの結果を示す単一のブール値です。Trueはすべてのコンポーネントで完全な成功を示し、falseは1つ以上のコンポーネントの処理における失敗を示します。

`CloudBackupFolder`は、コマンドレットがクラウドを変更するアクションを実行する前の、クラウドサイト構成バックアップの完全修飾ファイル指定です。

`SourceBackupFolder`は、コマンドレットの完了後に作成されたソースファイルバックアップの完全修飾ファイル指定です。デフォルトでは、これらのファイルは *%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。

PowerShell ヘルプ

PowerShell ヘルプは各コマンドレットで利用できます。すべてのパラメーターは、コマンドレットの簡単な説明とともに各コマンドレットで文書化されています。任意のコマンドレットのヘルプにアクセスするには、コマンドレットの前に`Get-Help`と入力します。

```
Get-Help Import-CvadAcToSite
```

バックアップと復元のための自動構成ツール コマンドレット

このページでは、Web Studio が使用するバックアップおよび復元 API をトリガーするためにツールがサポートするすべてのコマンドレットとパラメーターを一覧表示します。

バックアップストレージ コマンドレット

Get-BckRstrStorage

このコマンドレットはオンプレミスのみに適用されます。バックアップが保存されるストレージの詳細を取得します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。

パラメーター	説明
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティ情報と環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。

Set-BckRstrStorage

このコマンドレットはオンプレミスのみに適用されます。バックアップが保存される新しいストレージを設定します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。

パラメーター	説明
`CustomerInforFileSpec`	セキュリティ情報と環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`MaximumBackups`	新しいバックアップが作成されたときに、バックアップクリーンアッププロセスが最も古いバックアップを削除するまで保持される、ピン留めされていないバックアップの最大数。
`MaximumPinnedBackups`	保持されるピン留めされたバックアップの最大数。これらのバックアップはクリーンアッププロセスによって削除されません。
`BlobStorageType`	ストレージの種類: `FileStorage` または `CustomerAzureStorage`。

パラメーター	説明
`FileStoragefolder`	`BlobStorageType` `FileStorage` オプションの完全修飾フォルダー指定。
`Info1`	`FileStorage` の場合、オプションの `UserName` `CustomerAzureStorage` の場合、Azure SAS URL
`Info2`	`FileStorage` の場合、オプションのパスワード
`Info3` と `Info4`	使用されていません

テスト-バックアップリストアストレージ

このコマンドレットはオンプレミスのみに適用されます。定義されたストレージが有効であることを確認するためのテストです。

`FileStorage` の場合、テストはフォルダーが存在し、書き込み可能であることを確認します。

`CustomerAzureStorage`の場合、テストは、SAS URLが正しい権限を持ち、現在の日付がURLの開始日と終了日の間にあることを確認します。

有効な場合は`true`を、無効な場合は`false`を返します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。

パラメーター	説明
`ProfileName`	以前のパラメーターの代わりに使用される、既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	コンソールへの出力を抑制するパラメーター。

バックアップコマンドレット

Get-BckRstrBackups

バックアップまたは復元BLOBストレージの場所に保存されているバックアップを列挙します。Citrix Virtual Apps and Desktops™の場合、この場所は管理者がWebStudioを通じて設定します。DaaSの場合、これは既存の顧客Azureストレージです。各バックアップに関する完全な情報については、`Get-BckRstrBackupsWithDetiails`を使用してください。バックアップの詳細には、次のものが含まれます。

- バックアップ名
- メモ
- ピン留め済み (true または false)
- バックアップの日時
- 履歴UID
- 関連UID (最後の復元履歴レコードのUID)
- 関連日時
- チェックモードで実行された場合に関連
- 期間（秒単位）
- 管理者名
- 各コンポーネントと各コンポーネントのメンバー数を列挙した詳細。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメータの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメータ。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメータ。

Get-BckRstrBackupsMembers

選択したバックアップに保存されている単一コンポーネントのメンバーを列挙します。メンバー名は単純なリストで返されます。

コンポーネントは次のとおりです。

- タグ
- AdminScopes
- AdminRoles
- AdminAdministrators (オンプレミスのみ)
- HostConnections
- アイコン
- AdminFolders

- MachineCatalogs
- StoreFronts
- DeliveryGroups
- ApplicationGroups
- ApplicationFolders
- アプリケーション
- AppVServers
- AppLibPackageDiscovery
- AppVIsolationGroups
- グループポリシー
- ユーザーゾーン設定
- サイトデータ
- ゾーン (オンプレミスのみ)

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud を参照してください。

パラメーター	説明
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip` 拡張子はオプションです。
`Component`	バックアップに含めるコンポーネント。

New-BckRstrBackup

Delivery Controllerで新しいバックアップアクションを開始します。このアクションは、`New-BckRstrBackup` コマンドレットに対して非同期です。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。

パラメーター	説明
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`Notes`	バックアップに関するメモ。
`PollForCompletion`	アクションが完了するまで、Delivery Controllerで実行中のアクションをポーリングするためのパラメーター。`Quite`パラメーターが指定されていない限り、ポーリングは進行状況と完了結果をコンソールにログ記録します。

バックアップをピン留めするコマンドレット

Set-BckRstrPinBackups

Delivery Controllerのバックアップクリーンアッププロセスの一部として削除されないように、バックアップをピン留めします。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される、既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。

パラメーター	説明
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip` 拡張子はオプションです。

Set-BckRstrUnpinBackups

バックアップのピン留めを解除し、Delivery Controller のバックアップクリーンアッププロセスで削除できるようにします。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティと環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud を参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。

パラメーター	説明
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip` 拡張子はオプションです。

バックアップ コマンドレットの削除

リムーブ-バックアップリストアバックアップ

1つ以上のバックアップを削除します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される、既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。

パラメーター	説明
`IncludeByName`	復元対象とするコンポーネントメンバーを指定するフィルター。これは、コンマ区切りのフィルター値のリストであり、ワイルドカード文字 `*` および `?` を使用できます。

スケジュールされたバックアップコマンドレット

Get-BckRstrSchedules

バックアップスケジュールのリストを取得します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。

パラメーター	説明
`BackupName`	バックアップの名前。`.zip`拡張子はオプションです。
`Notes`	設定または変更するメモ。

New-BckRstrSchedule

新しいバックアップスケジュールを作成します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	既存のセキュリティプロファイルを識別するためのパラメーターで、以前のパラメーターの代わりに使用されます。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境の種類: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`Name`	スケジュール名。
`Frequency`	頻度の種類: 毎日、毎週、または毎月。

パラメーター	説明
`Day`	頻度が毎日の場合。
`DaysInWeek`	頻度が毎週の場合。
`DayInMonth`	頻度が毎月の場合。
`WeekInMonth`	頻度が毎月の場合。
`StartDate`	形式は `M/d/yy` です
`StartTime`	24時間形式で指定された開始時刻。
`FrequencyFactor`	毎日（値 = 1）または隔日（値 = 2）のように、n回ごとに実行します。
`Description`	スケジュールされたバックアップの説明
`Enabled`	このバックアップスケジュールを有効にするためのパラメーター。有効な場合は `True`、無効な場合は `false`。
`TimeZoneId`	WindowsタイムゾーンID

Set-BckRstrSchedule

既存のバックアップスケジュールを変更します。変更するスケジュールを選択するために、名前またはUidを指定します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。

パラメーター	説明
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production, ProductionGov, ProductionJP, OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`Name`	スケジュール名。
`Uid`	スケジュール名を変更する場合。
`Frequency`	頻度の種類: 日次、週次、または月次。
`Day`	頻度が日次の場合。
`DaysInWeek`	頻度が週次の場合。
`DayInMonth`	頻度が月次の場合。
`WeekInMonth`	頻度が月次の場合。
`StartDate`	形式は `M/d/yy` です
`StartTime`	24時間形式で指定された開始時刻。
`FrequencyFactor`	毎日 (値 = 1) または隔日 (値 = 2) のように、n 回ごとに実行します。
`Description`	スケジュールされたバックアップの説明

パラメーター	説明
`Enabled`	このバックアップスケジュールを有効にするパラメーター。有効な場合は `True`、無効な場合は `false`。
`TimeZoneId`	Windows タイムゾーン ID

Set-BckRstrScheduleEnabled

既存のバックアップスケジュールを有効にします。有効にするスケジュールを選択するには、名前または Uid を指定します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客 ID。
`CientId`	ベアラートークンを取得するために必要なクライアント ID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud を参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するパラメーター。
`Name`	スケジュール名。

パラメーター	説明
`Uid`	スケジュール名を変更する場合。

Set-BckRstrScheduleDisabled

既存のバックアップスケジュールを無効にします。無効にするスケジュールを選択するには、名前またはUidを指定します。

パラメーター:

パラメータ	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメータの代わりに使用される、既存のセキュリティプロファイルを識別するためのパラメータ。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するパラメータ。
`Name`	スケジュール名。
`Uid`	スケジュール名を変更する場合。

バックアップを制限するコマンドレット

Set-BckRstrOptions

スケジュールされたバックアップを1日1回に制限し、同一のバックアップを回避します。

パラメータ:

パラメータ	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud を参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`OneScheduledBackupPerDay`	同一のバックアップを避けるため、スケジュールされたバックアップを1日1回に制限するパラメーター。

復元コマンドレット

リストア-バックリストアバックアップス

既存のバックアップから単一コンポーネントのメンバーを復元します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、「XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud」を参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip` 拡張子はオプションです。
`Component`	バックアップに含めるコンポーネント。
`Notes`	バックアップに関するメモ。
`CheckMode`	復元されるコンポーネントメンバーを識別するパラメーターですが、実際の復元は実行しません。
`RestoreType`	復元タイプ: MissingOnly または MissingUpdateExisting

パラメーター	説明
`IncludeByName`	復元対象とするコンポーネントメンバーを指定するフィルター。これは、フィルター値のコンマ区切りリストであり、ワイルドカード文字 `*` および `?` を含めることができます。

バックアップの制限コマンドレット

Set-BckRstrOptions

同一のバックアップを避けるため、スケジュールされたバックアップを1日1回に制限します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。

パラメーター	説明
`OneScheduledBackupPerDay`	同一のバックアップを避けるため、スケジュールされたバックアップを1日1回に制限するパラメーター。

復元コマンドレット

レストア-バックリストアバックアップス

既存のバックアップから単一コンポーネントのメンバーを復元します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される、既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip`拡張子はオプションです。

パラメーター	説明
`Component`	バックアップに含めるコンポーネント。
`Notes`	バックアップに関するメモ。
`CheckMode`	復元されるはずのコンポーネントメンバーを識別するためのパラメーターですが、実際の復元は実行しません。
`RestoreType`	復元タイプ: MissingOnly または MissingUpdateExisting
`IncludeByName`	復元対象とするコンポーネントメンバーを指定するためのフィルター。これは、フィルター値のコンマ区切りリストであり、ワイルドカード文字 `*` および `?` を含めることができます。

履歴コマンドレット

Get-BckRstrHistory

すべてのアクションの履歴詳細のリストを取得します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイル

パラメーター	説明
	の設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production, ProductionGov, ProductionJP, OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。

Get-BckRstrSpecificBackupHistory

特定のバックアップの履歴詳細のリストを取得します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud を参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。

パラメーター	説明
`BackupName`	バックアップの名前。`.zip`拡張子はオプションです。

Set-BckRstrNotes

履歴レコード内のメモを設定または変更します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するパラメーター。
`BackupName`	バックアップの名前。`.zip`拡張子はオプションです。
`Notes`	設定または変更するメモ。

自動構成のトラブルシューティングと追加情報

重要:

自動構成でよく発生するエラーメッセージと対応する解決策については、Knowledge Centerの記事CTX277730の*トラブルシューティングFAQ*を参照してください。

自動構成ツールのエラー

自動構成ツールの操作中にエラーが発生することがあります。たとえば、マシンカタログ、デリバリーグループ、グループポリシーなどのコンポーネントを処理する際に障害が発生する可能性があります。`OnErrorAction`と継続パラメーターを使用すると、処理中にエラーを捕捉し、解決して、中断したところから再開できます。

デフォルトの`OnErrorAction`値は`StopCompEnd`です。エラーが発生すると、ツールは現在のコンポーネントの処理を完了します。追加のコンポーネントは処理されず、エラーは下流の依存コンポーネントに引き継がれません。エラーを解決した後、継続パラメーターを適用してコマンドレットを再実行できます。

OnErrorActionパラメーター

コンポーネントの処理中にツールが検出したエラーへの応答方法を制御するために、移行コマンドで`OnErrorAction`パラメーター値を定義できます。

この表は、パラメーター値とその説明を示しています。

値	説明
`Continue`	すべてのコンポーネントを可能な限り多く処理しようとします。
`Pause`	処理の最後に一時停止し、続行するか停止するかを尋ねます。
`StopCompEnd`	コンポーネントを可能な限り多く処理しようとします。コンポーネントの完了後に停止します。(デフォルト)
`StopImmediately`	エラーが検出されると処理が停止します。

移行cmdlet

次の移行コマンドに `OnErrorAction` パラメーターを適用できます。

- `Compare-CvadAcToSite`
- `Import-CvadAcToSite`
- `Merge-CvadAcToSite`
- `New-CvadAcToSite`
- `Restore-CvadAcToSite`

例: `Merge-CvadAcToSite -OnErrorAction StopImmediately`

再開パラメーター

これらのパラメーターは、エラーのために操作が一時停止または停止した後にツールがどのように再開するかを定義します。

次の `OnErrorAction` パラメーター値のいずれかを含む移行コマンドレットに、再開パラメーターを適用できます。

- `Pause`
- `StopCompEnd`
- `StopImmediately`

この表は、パラメーターの値とその説明を示しています。

値	説明
`-AllRemaining`	開始コンポーネントが必要です。処理は開始コンポーネントから始まり、残りのすべてのコンポーネントを処理します。複数のコンポーネントが処理されます。
`-Resume`	`CurrentComponent.txt` のコンポーネントを開始点として使用します。残りのすべてが true に設定されます。複数のコンポーネントが処理されます。
`-Repeat`	`CurrentComponent.txt` のコンポーネントを開始点として使用します。残りのすべてが false に設定されます。1つのコンポーネントのみが処理されます。

最後に処理されたコンポーネントは、AutoConfigフォルダー内の `CurrentComponent.txt` ファイルに保存されます。このファイルの編集は推奨されません。 `-Resume` または `-Repeat` を指定し、`CurrentComponent.txt` が見つからないか無効な場合、処理は停止し、コンポーネントを選択するように求められます。

CustomerInfo.ymlファイルでのOnErrorActionの設定

`CustomerInfo.yml` ファイルで `OnErrorAction` の値を設定することもできます。次のコマンドレットを使用して値を設定します。

- 新しいファイルの場合: `New-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`
- 既存のファイルの場合: `Set-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`

ログ

いずれかのコマンドレットを実行すると、ログファイルが作成され、メインの履歴ログファイルにエントリが追加されます。すべての操作ログファイルはバックアップフォルダーに配置されます。すべてのログファイル名は `CitrixLog` で始まり、その後に自動構成操作とコマンドレット実行の日付とタイムスタンプが表示されます。ログは自動削除されません。

メインの履歴ログは、`*%HOMEPATH%\Documents\Citrix\AutoConfig*` にある **History.Log** という名前のファイルにあります。各コマンドレットの実行により、実行の日付、操作、結果、バックアップ、およびログファイルの場所を含むメインログエントリが生成されます。

また、`New-CvadAcZipInfoForSupport` コマンドレットを使用して、Citrix にサポートのために送信するログを収集することもできます。このコマンドレットは、すべてのログファイルと .yml ファイルを単一の zip ファイルに圧縮します。顧客の機密情報 (CustomerInfo.yml および CvadAcSecurity.yml) は zip に含まれません。Icon.yml ファイルもサイズが大きいため除外されます。zip ファイルは *%HOMEPATH%\Documents\Citrix\AutoConfig* に配置され、日付とタイムスタンプに基づいて *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip* という名前が付けられます。この zip ファイルはバックアップとしても機能します。

各ログファイルには以下が含まれます。

- 操作の名前と、チェックモードが有効になっているかどうか
- 開始日時と終了日時
- 各コンポーネントのアクションと成功/失敗の通知に関する複数のエントリ
- 実行されたアクションの概要（作成されたオブジェクトのさまざまな数を含む）

- 該当する場合の推奨される修正
- 該当する場合のバックアップフォルダーの場所
- メインログの場所
- 期間

診断ファイル

診断ファイルは、問題の特定と解決に役立ちます。操作が実行されると、次のファイルが作成されます。これらは、*%HOMEPATH%\Documents\Citrix\AutoConfig* の下にあるアクション固有のサブフォルダーにあります。問題解決のサポート情報を提供する際には、これらのファイルを含めてください。

エクスポート

`PoshSdk_yyyy_mm_dd_hh_mm_ss.ps1`

このファイルは、サイト構成をファイルにエクスポートするために行われたすべてのBroker PowerShell SDK呼び出しをカウントします。

インポート、マージ、復元、同期、バックアップ、比較

`Transaction_yyyy_mm_dd_hh_mm_ss.txt`

このファイルは、各Rest API呼び出しと関連情報を記録します。

`RestApiContent_yyyy_mm_dd_hh_mm_ss.txt`

このファイルには、すべての `Add`、`Update`、および `Delete` Rest APIコンテンツが含まれています。

依存関係に起因する問題

インポートとマージは、依存関係の欠落が原因で失敗する可能性があります。一般的な問題は次のとおりです。

1. グループポリシーにデリバリーグループフィルターがありません。通常の原因は、インポートされていないデリバリーグループです。
2. アプリケーションのインポートまたはマージが失敗します。通常の原因は、インポートされていないデリバリーグループまたはアプリケーショングループの欠落です。
3. アプリケーショングループにRestrictToTagがありません。通常の原因は、インポートされていないタグです。

4. ホスト接続が失敗します。通常の原因は、CvadAcSecurity.ymlファイルにセキュリティ情報がないことです。
5. マシンカタログが失敗します。通常の原因は、インポートされなかったホスト接続です。
6. マシンカタログとデリバリーグループからマシンが欠落しています。通常の原因は、Active Directoryで見つからなかったマシンです。
7. デリバリーグループからユーザーが欠落しています。通常の原因は、Active Directoryで見つからなかったユーザーです。

推奨事項

- 自動構成の複数のインスタンスを同時に実行しないでください。複数のインスタンスを同時に実行すると、クラウドサイトで予期しない結果が生じます。この問題が発生した場合は、自動構成の1つのインスタンスを再実行して、サイトを目的の状態に戻してください。
- 自動構成の実行中にStudioで作業したり、データを変更したりしないでください。
- クラウドサイトが期待どおりであることを確認するために、Studioでマージ、インポート、または復元の結果を常に視覚的に確認してください。

フォルダー

デフォルトのフォルダーのルート場所

すべての自動構成ツール操作は、ルートフォルダーまたはその中のサブフォルダーで行われます。ルートフォルダーは、*%HOMEPATH%\Documents\Citrix\AutoConfig*にあります。

エクスポート

すべてのエクスポートされたファイルは、使いやすさとエクスポート履歴を提供するために、2つのフォルダーの場所に配置されます。エクスポートは常にルートフォルダーに配置されます。コピーは、エクスポートの日時とともに**Export**という名前のサブフォルダーに配置されます。

ルートフォルダーには常に、最新のエクスポートされたオンプレミスサイト構成が含まれています。各**Export**サブフォルダーには、指定された日時に行われたエクスポートが含まれており、エクスポートの履歴が保持されます。任意の**Export**サブフォルダーを使用して、クラウドサイトを構成できます。自動構成は、既存のエクスポートサブフォルダーを削除または変更しません。

インポート/マージ/同期/比較

`Import`、`Merge`、および`Compare`操作は、常にルートフォルダーにあるファイルから取得されます。各操作によりサブフォルダーが作成され、ルートフォルダー内のファイルがそこにコピーされ、クラウドサイトの変更元ファイルの履歴が提供されます。

復元

`Restore`操作は、既存のサブフォルダーを使用してクラウドサイトを構成します。ソースフォルダーは、必須の`-RestoreFolder`パラメーターで指定されます。他のコマンドとは異なり、`Restore`操作は既存のサブフォルダーを使用するため、新しいサブフォルダーは作成されません。復元フォルダーはルートフォルダーにすることもできますが、それでも`-RestoreFolder`パラメーターで指定する必要があります。

バックアップ

Automated Configurationは、クラウドサイトの構成を初期化、更新、およびバックアップします。長期間使用すると、クラウドサイトでさまざまな構成が変更される可能性があります。長期的な使用を容易にし、履歴の変更を保持するために、Automated Configurationは保存スキームを使用してこの変更履歴を保存し、以前の状態を復元する方法を提供します。

クラウドサイト構成のバックアップは、常にバックアップの日時を含む**Backup**という名前のサブフォルダーに作成されます。Automated Configurationは、既存のエクスポートサブフォルダーを削除または変更しません。

バックアップを使用して、特定のコンポーネントまたは構成全体を復元できます。デリバリーグループとマシンカタログコンポーネント全体を復元するには、次のコマンドレットを使用します。

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig\Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups -MachineCatalogs
```

> **注:**
>
> 前述のコマンドレットのバックアップファイル情報は、独自のバックアップに基づいています。

クラウドサイト構成全体を復元するには、次のコマンドレットを使用します。

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig\Backup_yyyy_mm_dd_hh_mm_ss
```

> **注:**

> 前述のコマンドレットのバックアップファイル情報は、独自のバックアップに基づいています。

デフォルトのルートフォルダーの変更

`Export`、`Import`、`Merge`、`Sync`、および`Compare`の各操作は、`-AlternateFolder`パラメーターを使用してデフォルトのルートフォルダーを変更できます。操作ごとのサブフォルダーの作成と管理は、前述のとおり変更ありません。

サブフォルダーにコピーされるファイル

以下のファイルを除き、拡張子が「.yml」のすべてのファイルは操作サブフォルダーにコピーされます。

- CustomerInfo.yml
- ZoneMapping.yml
- CvadAcSecurity.yml

自動フェイルセーフクラウドサイトバックアップ

現在のクラウドサイト構成のバックアップは、構成を変更する操作を実行する前に作成されます。これには、`Import`、`Merge`、`Sync`、および`Restore`パラメーターが含まれます。バックアップは常に、運用サブフォルダーの下のサブフォルダーに保存されます。

`Restore`の場合、バックアップフォルダーは`-RestoreFolder`パラメーターで指定されたフォルダーのサブフォルダーです。

自動化

自動構成ツールコマンドレットは、プロンプトとコマンドレット完了時のログ結果の表示を抑制することで、管理者による介入なしに自動化スクリプトで実行できます。CustomerInfo.ymlファイルを使用して、同じことを行うようにパラメーターを設定することもできます。

プロンプトの表示を抑制するには、クラウド変更コマンドレットに次のパラメーターを追加します。

```
-Confirm $false
```

コマンドレットの完了時にログの表示を抑制するには、コマンドレットに次のパラメーターを追加します。

```
-DisplayLog $false
```

PowerShellコマンドウィンドウへのログ記録を抑制するために、次のパラメーターをコマンドレットに追加します。

`-Quiet`

別の方法として、次のパラメーターをCustomerInfo.ymlファイルに配置できます。

`Confirm: False`

`DisplayLog: False`

Delivery Controller™以外のPCからのエクスポート

Automated configurationツールは、複数のCitrix PowerShell SDKを使用して、オンプレミスサイト構成をファイルにエクスポートします。これらのSDKはDelivery Controllerに自動的にインストールされるため、追加の操作なしでツールをDelivery Controllerで実行できます。Delivery Controller以外のマシンで実行する場合は、ツールに必要なCitrix PowerShell SDKのセットをインストールする必要があります。このSDKセットはCitrix Studioの一部であり、Citrix Virtual Apps and Desktops™インストールメディアからインストールできます。

> **注:**
>
> Automated configurationはCloud Connectorでは実行できません。

Citrix Cloud™ GovernmentおよびJapan Control Planeへの移行

Citrix Cloud GovernmentおよびJapan Control Plane環境では、認証およびアクセストークンの割り当てに異なるアクセスポイントを使用します。この固有の要件は、クラウドにアクセスするすべてのAutomated configurationツールに適用されます。これらの環境でAutomated configurationを使用するには、次の手順を実行します。

1. *%HOMEPATH%\Documents\Citrix\AutoConfig*フォルダーで、CustomerInfo.ymlを編集します。
2. 接続する環境に応じて、次のいずれかの行をCustomerInfo.ymlに追加します（または、既に存在する場合は変更します）。

   `Environment: 'ProductionGov'`

   または

   `Environment: 'ProductionJP'`

自動構成は、これらの環境で使用できるようになりました。

Citrix Cloud のデータ収集

Citrix Cloud が収集する情報については、「Citrix Cloud Services Customer Content and Log Handling」を参照してください。

その他のリソース

ディスカッションフォーラム

Citrix Discussion forum for Automated Configurationにアクセスしてください。

ビデオ

Citrix Virtual Apps and Desktops 用自動構成ツールの詳細 を YouTube でご覧ください。

トレーニング

Cloud Learning Centerには、サービス展開を構築するためのステップバイステップのビデオガイドが含まれており、この記事で説明されているタスクも含まれています。「Migrating Citrix Virtual Apps and Desktops to Citrix Cloud Learning Path」を参照してください。

オートスケール™

> **注:**
>
> この機能はWeb Studioでのみ利用可能です。

> Autoscaleは、マシンを積極的に電源管理するための、一貫性のある高性能なソリューションを提供する機能です。コストとユーザーエクスペリエンスのバランスを取ることを目的としています。

Autoscaleは、デリバリーグループ内の登録されているすべてのシングルセッションおよびマルチセッションOSマシンの積極的な電源管理を可能にします。

Autoscaleの機能は次のとおりです。

- スケジュールベースおよび負荷ベースの設定(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/autoscale/schedule-based-and-load-based-settings.html)
- 動的セッションタイムアウト(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/autoscale/dynamic-session-timeout.html)

- Autoscaleタグ付きマシン（クラウドバースト）(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/autoscale/autoscale-tagged-machines.html)
- ユーザーログオフ通知(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/autoscale/force-user-logoff.html)

一般的なユースケース

以下は、Autoscaleが一般的に使用されるシナリオです。

- 予想されるワークロードに対応するためのスケジュールベースのマシンの電源投入

  Autoscaleを使用すると、管理者は電源投入済み容量を30分単位で調整でき、異なる日に異なるスケジュールを設定できます。変動の激しいワークロードが予想される場合は、ユーザーがマシンの電源投入を待つ必要がないように、容量バッファを設定することをお勧めします。

- クラウドバーストのユースケース

  Autoscale は、デリバリーグループ内のマシンの一部のみを電源管理する柔軟性を提供します。これを実現するには、1つ以上のマシンにタグを適用し、Autoscale を構成してタグ付けされたマシンのみを電源管理するようにします。

  この機能は、クラウドベースのリソースが追加の需要（つまり、バーストワークロード）に対応する前に、オンプレミスリソース（または予約済みのパブリッククラウドインスタンス）を使用してワークロードを処理したいクラウドバーストのユースケースで役立ちます。

- 徐々に利用を開始するユーザーまたは季節的なユーザー

  組織がユーザーを徐々にオンボーディングしており、事前にすべての容量をプロビジョニングしたくない場合、動的プロビジョニング機能が役立ちます。この機能は、デリバリーグループの負荷を常に評価し、現在の負荷状況に基づいてデリバリーグループ内のマシンの数を動的にスケールアップまたはスケールダウンします。管理者は、マシンを作成するためにデリバリーグループの負荷に対する高および低ウォーターマークを定義する必要があります。管理者は、プロビジョニングするマシンの最大数と、これらのマシンに適用するタグをオプションで定義できます。

サポートされているVDAホスティングプラットフォーム

Autoscale は、Citrix Virtual Apps and Desktops がサポートするすべてのプラットフォームをサポートしています。これには、XenServer、Amazon Web Services、Google Cloud Platform、Microsoft Azure Resource Manager、VMware vSphere など、さまざまなインフラストラクチャプラットフォームが含まれます。サポートされているプラットフォームの完全なリストについては、Citrix Virtual Apps and Desktops の システム要件 を参照してください。

注:

展開にパブリッククラウドホスト接続を追加する場合、ハイブリッド権限ライセンスが必要です。ハイブリッド権限ライセンスについては、ハイブリッド権限による移行とアップグレード（TTU） を参照してください。ライセンスの追加については、サイトの作成 を参照してください。

サポートされているワークロード

Autoscale は、マルチセッションOSとシングルセッションOSの両方のデリバリーグループをサポートしています。注意すべきユーザーインターフェイスは3つあります。

- マルチセッションOSデリバリーグループ（旧RDSデリバリーグループ）用のAutoscaleユーザーインターフェイス
- シングルセッションOSランダム（プールされた）デリバリーグループ（旧プールされたVDIデリバリーグループ）用のAutoscaleユーザーインターフェイス
- シングルセッションOS静的デリバリーグループ（旧静的VDIデリバリーグループ）用のAutoscaleユーザーインターフェイス

異なるデリバリーグループのユーザーインターフェイスの詳細については、Autoscaleユーザーインターフェイス を参照してください。

利点

Autoscale機能は以下の利点を提供します:

- デリバリーグループ内のマシンを電源管理するための、単一で一貫したメカニズムを提供します。
- 負荷ベースまたはスケジュールベースの電源管理、あるいはその両方の組み合わせでマシンに電源を供給することで、可用性を確保し、コストを制御します。
- コスト削減やキャパシティ利用率などのメトリックを監視し、通知を有効にするには、Directorを使用します。

2分間のビデオを見る

以下のビデオでは、Autoscaleの簡単なツアーを提供します。

<iframe src="https://www.youtube.com/embed/5yxERrFZQ68" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

Autoscale™ の使用を開始する

Autoscale は、構成されたスケジュールまたは負荷の要求に基づいてデリバリーグループをプロアクティブにスケーリングするための、一貫性のある高性能な電源管理ソリューションを提供する機能です。

Autoscale は、次のすべての種類のデリバリーグループに適用されます。

- シングルセッション静的 OS
- シングルセッションランダム OS
- マルチセッションランダム OS

この記事では、Autoscale に関連する基本的な概念について説明し、デリバリーグループで Autoscale を有効にして構成する方法に関するガイダンスを提供します。

基本的な概念

開始する前に、Autoscale の次の基本的な概念について学習してください。

- 容量とマシンの登録
- 複数のマシンカタログにわたるスケーリング
- マシンのプロビジョニングとセッションの需要
- インスタンスサイズの考慮事項
- スケジュール
- ピーク時とオフピーク時
- 「電源オフ遅延」(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/autoscale/get-started#power-off-delay)
- 「プールサイズ」(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/autoscale/get-started#pool-size)
- 「容量バッファ」(#capacity-buffer)
- 「負荷インデックス」(#load-index)
- 「Autoscaleとメンテナンスモード」(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/autoscale/get-started#autoscale-and-maintenance-mode)
- 「マシンコスト」(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/autoscale/get-started#machine-cost)
- 「デリバリーグループのスケールアップ」(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/autoscale/get-started#scale-up-a-delivery-group)

- 「デリバリーグループのスケールダウン」(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/autoscale/get-started#scale-down-a-delivery-group)
- 「ドレイン状態」(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/autoscale/get-started#drain-state)

容量とマシンの登録

Autoscaleは、容量を決定する際に、サイトに登録されているマシンのみを含めます。登録されていない電源オンのマシンはセッション要求を受け入れることができません。その結果、それらはデリバリーグループの全体的な容量には含まれません。

複数のマシンカタログにわたるスケール

一部のサイトでは、複数のマシンカタログが単一のデリバリーグループに関連付けられている場合があります。Autoscaleは、スケジュールまたはセッションの需要要件を満たすために、各カタログからマシンをランダムに電源オンにします。

たとえば、あるデリバリーグループには2つのマシンカタログがあります。カタログAには3台のマシンが電源オンになっており、カタログBには1台のマシンが電源オンになっています。Autoscaleが追加のマシンを電源オンにする必要がある場合、カタログAまたはカタログBのいずれかのマシンを電源オンにする可能性があります。

マシンのプロビジョニングとセッションの需要

デリバリーグループに関連付けられているマシンカタログには、需要の増減に応じて電源をオン/オフできる十分なマシンが必要です。セッション需要がデリバリーグループ内の登録済みマシンの総数を超えた場合、Autoscaleはすべての登録済みマシンが電源オン状態であることを保証します。ただし、**Autoscaleは追加のマシンをプロビジョニングしません。**

> **注:**
>
> デリバリーグループに63台のマシンがあり、営業時間外に10%のバッファ容量が設定されている場合、Autoscaleの計算によると、営業時間外には6.3台のマシンが電源オンになっている必要があります。小数点以下の値を処理するためのルールは次のとおりです。
>
> - 最も近い値に丸める：たとえば、値が6.4の場合、6台のマシンがオンになります。値が6.7の場合、7台のマシンがオンになります。
> - 1未満のゼロ以外の値はすべて1に丸める：たとえば、値が0.2または0.9の場合、1台のマシンがオンになります。

インスタンスサイズの考慮事項

パブリッククラウドでインスタンスのサイズを適切に設定すると、コストを最適化できます。ワークロードのパフォーマンスと容量要件に合致する限り、より小さいインスタンスをプロビジョニングすることをお勧めします。

小さいインスタンスは、大きいインスタンスよりも少ないユーザーセッションをホストします。そのため、最後のユーザーセッションがログオフされるまでの時間が短いため、Autoscaleはマシンをより速くドレイン状態にします。結果として、Autoscaleは小さいインスタンスの電源をより早くオフにし、コストを削減します。

スケジュール

Autoscaleは、設定したスケジュールに基づいて、デリバリーグループ内のマシンの電源をオン/オフします。

スケジュールには、ピーク時とオフピーク時が定義された、各時間帯のアクティブなマシンの数が含まれます。

スケジュールの設定は、デリバリーグループの種類によって異なります。詳細については、以下を参照してください。

- マルチセッションOSデリバリーグループ
- シングルセッションOSランダムデリバリーグループ
- シングルセッションOS静的デリバリーグループ

ピーク時とオフピーク時

ピーク時とオフピーク時は、1日の特定の期間にどのキャパシティバッファ値を使用するかを示すために使用されます。ピーク時間を定義し、残りの未定義の時間をオフピーク時間として残すことができます。

電源オフ遅延

電源オフ遅延とは、Autoscale がマシンを電源オフにする前に、マシンが電源オンになってから経過しなければならない最小分数です。これにより、セッション需要が不安定なときにマシンがオンとオフを繰り返すのを防ぎます。デフォルトでは、電源オフ遅延は30分です。0〜60分の範囲で設定できます。

プールサイズ

プールサイズとは、1日の特定の期間に電源オンの状態を維持する必要があるマシンの数です。

キャパシティバッファ

キャパシティバッファは、動的な負荷増加に対応するために、現在の需要に予備のキャパシティを追加するために使用されます。注意すべき2つのシナリオがあります。

- マルチセッションOSデリバリーグループの場合、キャパシティバッファは、ロードインデックスの観点から、デリバリーグループの総キャパシティの割合として定義されます。
- シングルセッションOSデリバリーグループの場合、キャパシティバッファは、デリバリーグループ内のマシンの総数の割合として定義されます。

キャパシティバッファはローリングバッファであり、設定されたプールサイズに加えて計算および適用されるのではなく、現在の使用状況に基づいて計算および適用されます。

例えば、10台のマシンを持つデリバリーグループがあり、現在の期間のプールサイズが1台、キャパシティバッファが10%であるとします。スケジュールで定義された1台の電源オンマシンが、10%のキャパシティバッファが満たされなくなるまで負荷がかかった場合、追加のマシンが電源オンになります。2台目のマシンを電源オンにした後で負荷が減少し、10%のキャパシティバッファを満たすのに十分な空き負荷キャパシティがある場合、Autoscaleは1台のマシンを電源オフの準備をします。

ロードインデックス

> **重要:**
>
> ロードインデックスは、マルチセッションデリバリーグループにのみ適用されます。

> ロードインデックスメトリックは、マシンがユーザーログオン要求を受信する可能性を決定します。これは、同時ログオン、セッション、CPU、ディスク、メモリ使用量に対して構成された**Citrix Load Management policy**設定を使用して計算されます。

ロードインデックスは0から10,000の範囲です。デフォルトでは、マシンが250セッションをホストしている場合、完全にロードされていると見なされます。

- 「0」はアンロードされたマシンを示します。ロードインデックス値が0のマシンは、ベースライン負荷状態です。
- 「10,000」は、これ以上セッションを実行できない完全にロードされたマシンを示します。

Autoscaleとメンテナンスモード

メンテナンスモードのマシンは、その可用性ステータスに関係なく、全体のプールサイズの計算の一部と見なされます。したがって、プール内のすべてのマシンがメンテナンスモードになっている可能性があります。ただし、これらのマシンは容量バッファの計算から除外され、即座に利用可能であることが保証されます。ユーザー接続のために特定の割合のマシンがアクセス可能であることを保証するには、プールサイズとバッファ値をそれに応じて調整してください。

マシンコスト

1時間あたりのマシンインスタンスコストは、使用されているコンピューティング容量の1時間あたりのコスト（米ドル）です。この設定は、Autoscale設定によるコスト削減を計算するために使用されます。節約額を表示するには、 **> >** に移動します。

デリバリーグループのスケールアップ

Autoscaleは、Autoscaleが有効なデリバリーグループで、次の場合に追加のマシンの電源をオンにします。

1. デリバリーグループのAutoscaleスケジュールが、現在の期間により多くのマシンの電源をオンにする必要があることを示している場合。
2. デリバリーグループの現在の負荷が容量バッファを超えている場合。

マシンの電源をオンにする条件：

1. メンテナンスモードではないこと。
2. ハイパーバイザーはメンテナンスモードではありません。
3. 電源がオフで、登録されていません。
4. スケールアップが必要なデリバリーグループに属している
5. 保留中の電源操作はありません。

デリバリーグループをスケールダウンする

Autoscale は、Autoscale が有効なデリバリーグループ内のマシンを、次の場合に電源オフにします。

1. Autoscale スケジュールで、現在の期間に設定されたマシン数に合わせるために、マシンの電源をオフにする必要があると指定されている場合。
2. デリバリーグループの現在の負荷が減少し、プールサイズと容量バッファを満たすために必要な数よりも多くの電源オン状態のマシンが存在する場合。

Autoscale は、プールサイズと容量バッファを満たすために必要な数を超える余分なマシンの電源をオフにすることで、デリバリーグループをスケールダウンします。

スケールダウンプロセスには、次の2つのステップがあります。

1. 必要な数のマシンをドレイン状態にする。
2. ドレイン状態のすべてのマシンを電源オフのために選択する。

電源オフの対象となるマシンは、次の基準を満たしている必要があります。

1. メンテナンスモードではない
2. ハイパーバイザーがメンテナンスモードではない
3. 現在電源オンの状態である
4. 利用可能として登録されているか、起動後に登録を待機している
5. ドレイン状態であり、アクティブなセッションがない
6. 保留中の電源操作がない
7. 電源オフ遅延を満たしている

ドレイン状態

Autoscaleは、デリバリーグループ内の電源オン状態のマシンの数を、構成されたプールサイズと容量バッファにまでスケールダウンしようとします。

この目標を達成するために、Autoscaleはセッション数が最も少ない余剰マシンを「ドレイン状態」にし、すべてのセッションがログオフされたときにそれらの電源をオフにします。この動作は、セッションの需要が減少し、スケジュールで電源オン状態のマシンよりも少ないマシンが必要とされる場合に発生します。

マシンがドレイン状態になる条件:

1. 電源オンである
2. メンテナンスモードではない
3. ハイパーバイザーがメンテナンスモードではない
4. スケールダウンが必要なデリバリーグループに属している
5. 現在のアクティブセッション数が最も少ない

> **注:**
>
> - 電源オフ遅延で指定された時間以上電源オン状態であったマシンが、ドレインの対象として優先されます。

- ドレイン状態のマシンは、新しいセッションの起動をホストしなくなり、既存のセッションがログオフされるのを待機します。マシンは、すべてのセッションがログオフされた場合にのみシャットダウンされます。ただし、セッション起動にすぐに利用できるマシンがない場合、Autoscale は、マシンの電源をオンにするよりも、ドレイン状態のマシンにセッション起動を誘導することを優先します。

Autoscale は、過剰なマシンを1台ずつ「ドレイン状態」にします。

- 2台以上のマシンが同じ数のアクティブセッションを持っている場合、Autoscale は、指定された電源オフ遅延時間の間電源がオンになっていたマシンをドレインします。

  そうすることで、最近電源がオンになったマシンがドレイン状態になるのを回避します。それらのマシンはセッション数が最も少ない可能性が高いからです。
- 2台以上のマシンが指定された電源オフ遅延時間の間電源がオンになっていた場合、Autoscale はそれらのマシンをランダムに1台ずつドレインします。

ドレイン状態のマシンは、新しいセッションの起動をホストしなくなり、既存のセッションがログオフされるのを待機しています。マシンは、すべてのセッションがログオフされた場合にのみシャットダウンの候補になります。ただし、セッション起動にすぐに利用できるマシンがない場合、Autoscale は、マシンの電源をオンにするよりも、ドレイン状態のマシンにセッション起動を誘導することを優先します。

マシンは、次のいずれかの条件が満たされた場合にドレイン状態から解除されます。

- マシンの電源がオフになる。
- マシンが属するデリバリーグループに対して Autoscale が無効になっている。
- Autoscale は、スケジュールまたは負荷需要の要件を満たすためにマシンを使用します。このケースは、スケジュール (スケジュールベースのスケーリング) または現在の需要 (負荷ベースのスケーリング) が、現在電源がオンになっているマシンの数よりも多くのマシンを必要とする場合に発生します。

重要:

セッション起動にすぐに利用できるマシンがない場合、Autoscale は、マシンの電源をオンにするよりも、ドレイン状態のマシンにセッション起動を誘導することを優先します。セッション起動をホストするドレイン状態のマシンは、ドレイン状態のままになります。

ドレイン状態の表示

PowerShell または Web Studio を使用して、どのマシンがドレイン状態にあるかを判断できます。

PowerShell の使用

`Get-BrokerMachineV2` PowerShellコマンドレットを実行して、マシンの**IsDraining**および**DrainingReason**プロパティを表示します。

例えば: `Get-BrokerMachineV2 -Property IsDraining,DrainingReason,MachineName | Format-Table MachineName,IsDraining,DrainingReason`

- **IsDraining:** このブール値プロパティは、マシンがドレイン状態の場合に `True` になり、そうでない場合は `False` になります。
- **DrainingReason:** このプロパティは、マシンがドレイン状態にある特定の理由を示します。そのデフォルト値は `NotDraining` です。マシンがドレイン中の場合、**DrainingReason** は次のいずれかの値を表示します。
  - **AutoscaleScaleDown:** Autoscaleは、構成されたプールサイズと容量バッファの要件を満たすために、デリバリーグループ内の電源オン状態のマシン数をスケールダウンするためにドレイン状態を開始しました。これは、セッション需要が減少した場合、またはスケジュールで必要なマシン数が少ない場合に発生します。
  - **NaturalRebootCycle:** マシンは、「セッション終了を待機」再起動モードでのスケジュールされた再起動サイクルの一部としてドレイン中です。マシンは、再起動する前にアクティブなセッションが終了するのを待機します。
  - **RebootCycle:** マシンは、「強制ログオフ」再起動モードでのスケジュールされた再起動サイクルの一部としてドレイン中です。マシンが再起動する前に、アクティブなセッションは強制的にログオフされます。
  - **MaintenanceMode:** 管理者がマシンをメンテナンスモードにしました。
  - **HypervisorInMaintenanceMode:** マシンをホストしているハイパーバイザー接続がメンテナンスモードになっています。
  - **MaintenanceCycle:** マシンは、OSディスクのリセットなど、VUSメンテナンスサイクル操作の一部としてドレイン中です。
  - **GuestOSDraining:** ゲストオペレーティングシステムが明示的に自身をドレインモードに設定します（たとえば、レジストリ設定を介して）。この理由は、マルチセッションマシンにのみ適用されます。

- **GuestOSDrainingUntilRestart:** ゲストオペレーティングシステムは、次回の再起動まで持続するドレインモードに自身を設定します。この理由は、マルチセッションマシンにのみ適用されます。

Web Studio を使用する

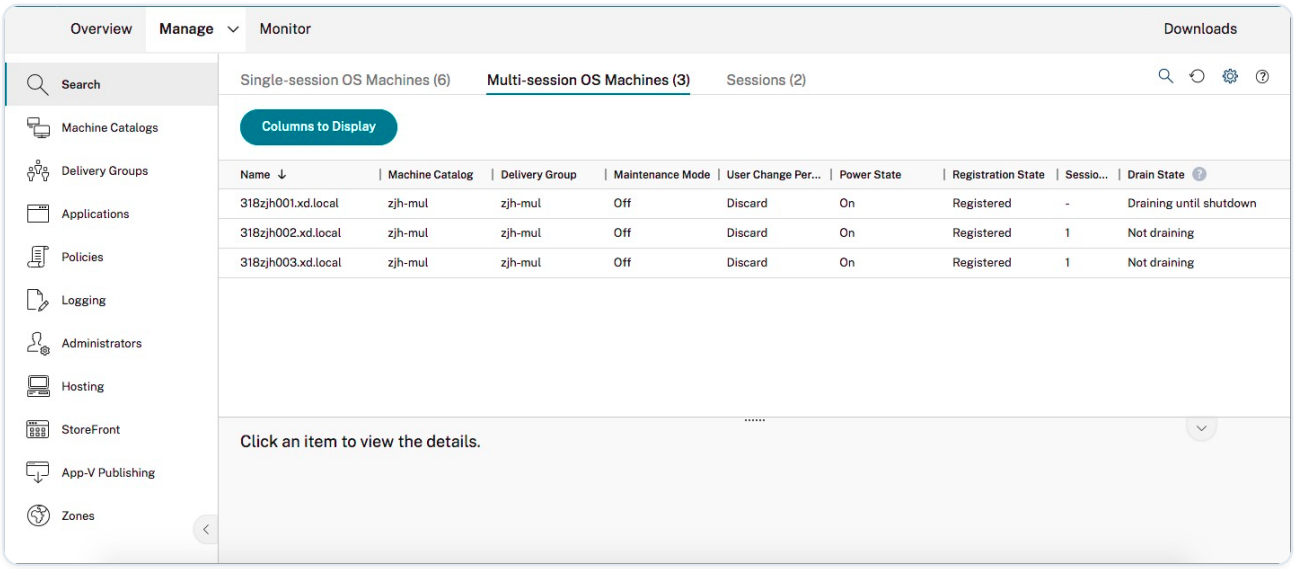
> **注:**
>
> `IsDraining` および `DrainingReason` プロパティは、シングルセッションマシンとマルチセッションマシンの両方に適用されますが（`GuestOSDraining` の理由はマルチセッション固有です）、Web Studio の **ドレイン状態** 列は、これらの状態を表示するために、歴史的にマルチセッションマシンにのみ適用されます。

Web Studio でドレイン状態のマシンを表示するには:

1. **検索**ノードに移動し、**表示する列**をクリックします。
2. **表示する列**ウィンドウで、**ドレイン状態**の横にあるチェックボックスを選択します。
3. **保存**をクリックして、**表示する列**ウィンドウを閉じます。

ドレイン状態列には、次の情報が表示されます。

- **シャットダウンまでドレイン中。** マシンがシャットダウンされるまでドレイン状態にある場合に表示されます。
- **ドレイン中ではありません。** マシンがまだドレイン状態にない場合に表示されます。

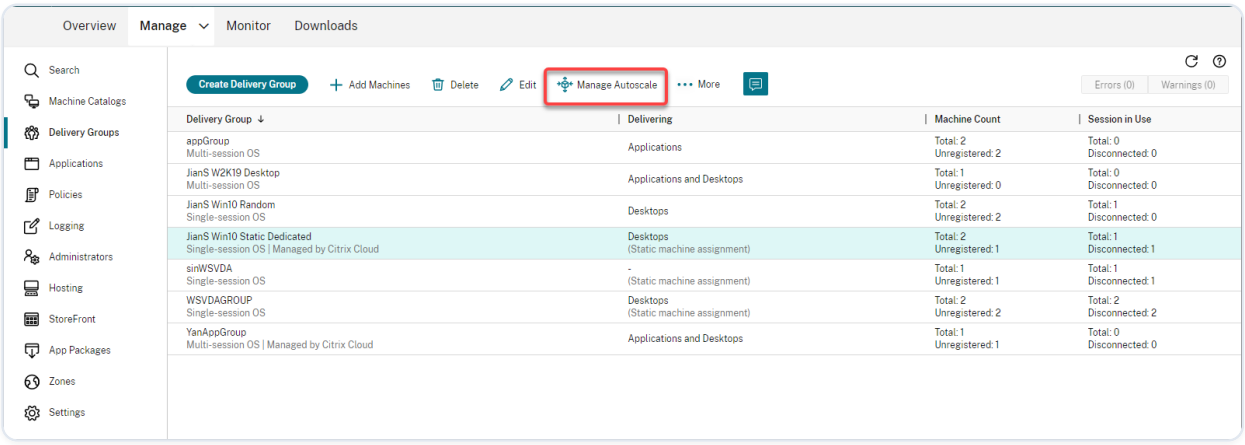


デリバリーグループのAutoscaleを有効にする

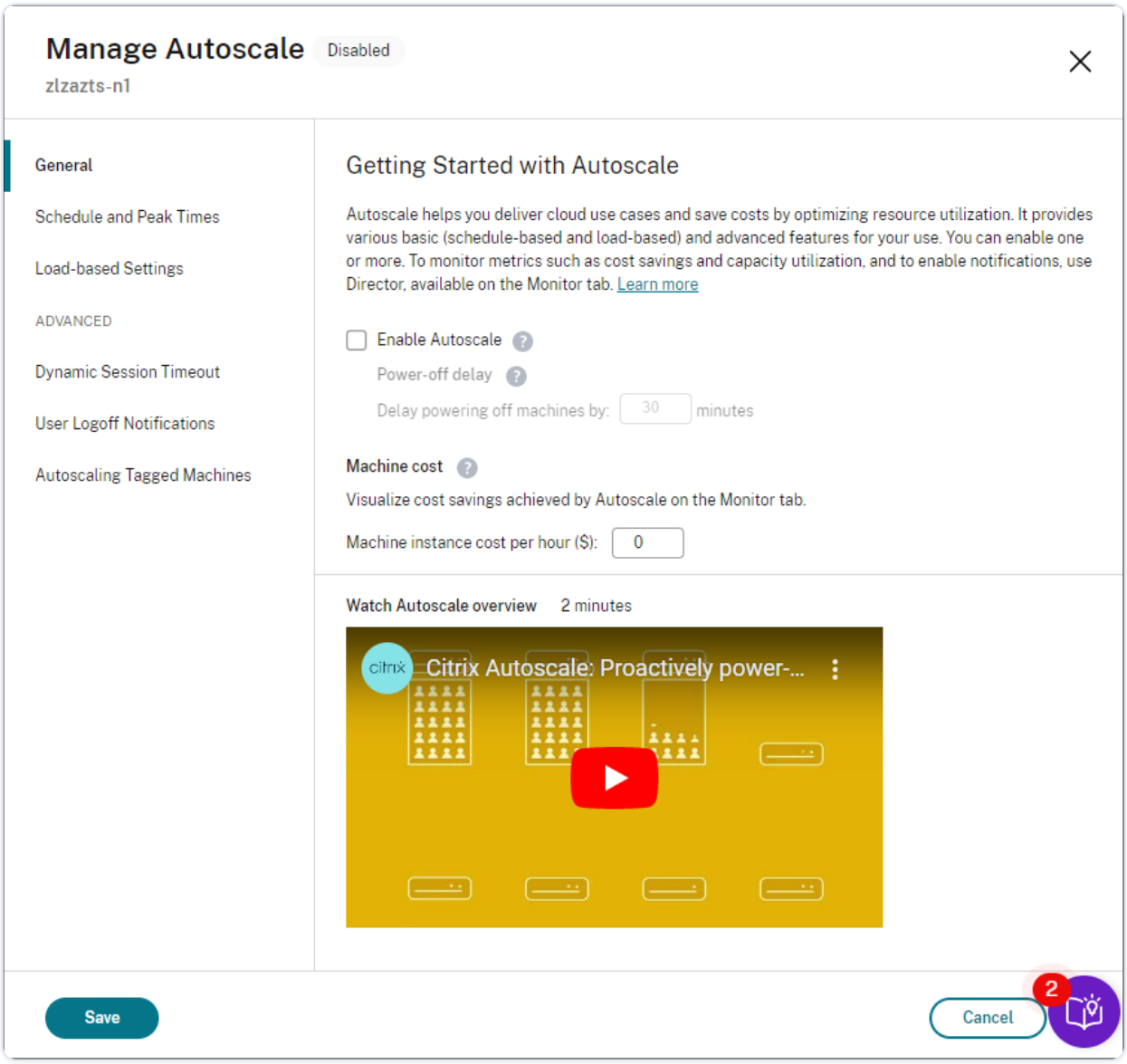
デリバリーグループを作成すると、Autoscaleはデフォルトで無効になります。Web Studioを使用してデリバリーグループのAutoscaleを有効にして構成するには、次の手順に従います。

PowerShellコマンドを使用して、デリバリーグループのAutoscaleを有効にして構成することもできます。詳細については、「Broker PowerShell SDKコマンド」を参照してください。

1. 左側のペインで を選択します。
2. 管理するデリバリーグループを選択し、**Autoscaleの管理**をクリックします。



3. **Autoscaleの管理**ページで、**Autoscaleを有効にする**チェックボックスを選択してAutoscaleを有効にします。Autoscaleを有効にすると、ページ上のオプションが有効になります。



4. 組織のニーズに基づいてデフォルト設定を変更するには、次の設定を完了します。

   - スケジュールを設定する
   - 非アクティブなマシンをより効率的に電源オフするには、動的セッションタイムアウトとユーザーログオフ通知を使用します。
   - デリバリーグループ内のマシンの一部を電源管理するには、タグ付けされたマシンの自動スケーリングを使用します。

Autoscaleを無効にするには、 チェックボックスをオフにします。ページ上のオプションがグレー表示され、選択したデリバリーグループでAutoscaleが無効になっていることを示します。

> **重要：**

- Autoscaleを無効にすると、Autoscaleによって管理されているすべてのマシンは、無効化時の状態のままになります。
- Autoscaleを無効にすると、ドレイン状態のマシンはドレイン状態から解除されます。ドレイン状態の詳細については、ドレイン状態を参照してください。
- **負荷ベースの設定**ページにあるシングルセッションOS静的デリバリーグループおよびシングルセッションOSランダムデリバリーグループの**電源ポリシー**アクションは、Autoscaleの設定（有効または無効）とは独立しています。

ドレイン中のマシンを自動スケール計算から除外する

この機能により、再起動スケジュールによりドレイン中のマシンがAutoscaleの容量ターゲットにカウントされるのを防ぐことができます。これらのマシンを除外することで、リソースプロビジョニングを最適化し、過剰なプロビジョニングを回避できます。

例：Autoscaleと定期的な再起動スケジュールで構成されたマルチセッションOSマシンのデリバリーグループがあるとします。マシンが再起動のためにドレイン状態に入ると、通常、Autoscaleはそれらを利用可能な容量としてカウントします。これにより、不必要に追加のマシンがプロビジョニングされる可能性があります。この機能を有効にすることで、Autoscaleに容量計算時にこれらのドレイン中のマシンを無視するように指示します。これにより、アクティブに利用可能なマシンのみがターゲットに貢献し、より効率的なリソース利用と運用コストの削減につながります。

適用範囲

この機能は、**マルチセッション OS マシン (RDS)** を含むデリバリーグループに適用されます。

制限事項

- この機能はシングルセッション OS マシンには適用されません。
- Autoscale を「マシンの数」（「割合」ではなく）に基づいて構成する場合、システムはドレイン状態のマシンを Autoscale の計算から除外しません。

重要な考慮事項

- プロパティ `ExcludeNaturalRebootDrainingFromAutoscale` はデリバリーグループで構成されます。
- プロパティ `ExcludeNaturalRebootDrainingFromAutoscale` のデフォルト値は `False` です。これは、ドレイン状態のマシンがデフォルトでAutoscaleの計算に含まれることを意味します。

前提条件

- マルチセッションOSデリバリーグループを構成します。
- ターゲットデリバリーグループに対してAutoscaleを有効にして構成します。スケーリングには「マシンの割合」を使用することをお勧めします。
- デリバリーグループの再起動スケジュールを構成して、マシンをドレイン状態にします。

構成方法

この機能は、PowerShellコマンドを使用してデリバリーグループレベルで構成します。

1. 機能トグル `ExcludeNaturalRebootDrainingFromAutoscale` が有効になっていることを確認します。これは、PowerShellで `Get-ConfigEnabledFeature` を実行し、出力リストでトグルを確認することで検証できます。

   > **注:**
   >
   > トグルが無効になっている場合、デリバリーグループのプロパティを変更することはできません。

2. ドレイン中のマシンを除外するようにデリバリーグループのプロパティを設定します。

   a. 管理者権限でPowerShellを開きます。

   b. マルチセッションOSデリバリーグループを特定します。

   c. `Set-BrokerDesktopGroup` コマンドレットを使用して、デリバリーグループの `ExcludeNaturalRebootDrainingFromAutoscale` プロパティを `$True` に設定します。

   ```
   Set-BrokerDesktopGroup -Name "<YourDeliveryGroupName>"
   -ExcludeNaturalRebootDrainingFromAutoscale $True
   ```

   `<YourDeliveryGroupName>` をデリバリーグループの実際の名前で置き換えます。

   d. 実行して、プロパティが `True` に設定されていることを確認します。

   ```
   Get-BrokerDesktopGroup -Name "<YourDeliveryGroupName>" | Select
   Name, ExcludeNaturalRebootDrainingFromAutoscale
   ```

   出力には `ExcludeNaturalRebootDrainingFromAutoscale : True` が表示されるはずです。

3. Autoscaleと再起動スケジュールを設定します（まだ設定されていない場合）。

   デリバリーグループでAutoscaleが有効になっており、マシンがドレイン状態になるように再起動スケジュールが構成されていることを確認します。

   a. Web Studioで、デリバリーグループを編集します。
   b. **Autoscaleの管理** に移動し、ピーク/オフピークスケジュールを設定して、Autoscaleが有効になっていることを確認します。ドレイン中のマシンを除外する場合は、「マシンの割合」に基づいてスケジュールを設定します。
   c. **再起動スケジュール** に移動し、マシンがドレイン状態になるスケジュールを作成または編集します（例：Cloudの場合は **Graceful restart**、オンプレミス展開の場合は **Re-start all machines after draining session** を使用します）。

監視とトラブルシューティング

問題: この機能を有効にしても、セッションがドレイン中のマシンで起動することがあります。

原因: これは予期される動作です。ドレイン状態のマシンは、他の適切なドレイン状態ではないマシンが利用できない場合の「最終手段」として、セッション起動に引き続き利用できます。この機能は主に、プロビジョニング/デプロビジョニングのAutoscale計算に影響を与えます。ブローカーのセッション起動ロジック自体には影響しません。

解決策：これは問題ではなく、意図された設計です。ドレイン中のマシンにセッションが移行するのを最小限に抑えるには、Autoscaleのバッファと容量が、需要を満たすのに十分な非ドレイン中のマシンを維持できることを確認してください。

ユーザーセッションを持つVMのAutoscaleオプション

Autoscaleは、割り当て済みマシンとプールされたマシンの両方を管理し、それらの電源と可用性を最適化できます。以下のコンテンツでは、割り当て済みマシンとプールされたマシン向けに、ピーク時とオフピーク時、およびユーザーセッションに基づいてマシンの電源状態を制御するためのPowerShellコマンドとUI設定を提供します。

割り当てられたマシンは単一ユーザー専用ですが、プールされたマシンは複数のユーザー間で共有されます。

> **注:**
>
> - Citrix Studioのセッション制限ポリシー、特に*切断されたセッションタイマー*と*セッションアイドルタイマー*は、Citrix Autoscaleが有効になっていない場合でも、ユーザーセッ

ションを管理するために重要です。これらのポリシーは、セッションが終了するまでに切断またはアイドル状態を維持できる期間を定義し、リソースの利用を確保し、ロックアウトされたセッションを防ぎます。このポリシー設定は、割り当て済みマシンとプールされたマシンの両方、特にマルチセッションVDAを実行しているマシンで使用できます。詳細については、「セッション制限ポリシー設定」を参照してください。

- `Get-BrokerMachine` PowerShellコマンドは非推奨です。代替として`Get-BrokerMachineV2`を使用してください。

割り当てられたマシンについて

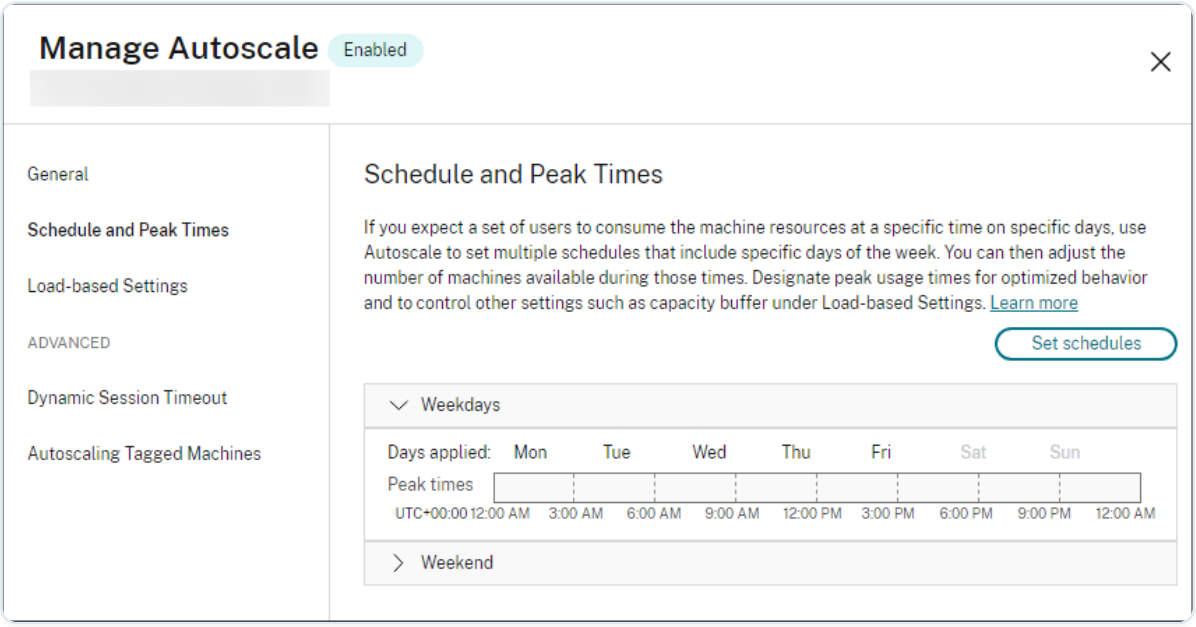
- ピーク時間の開始時に、静的デリバリーグループ内の割り当てられたシングルセッションマシンを自動的に電源オンにするには、PowerShellコマンドを使用します。

```
Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssigned $True
```

- ピーク時間中にオフになっていることが判明した割り当てられたマシンが再起動されるようにするには、`AutomaticPowerOnForAssignedDuringPeak`も有効にします。

```
Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssigned $True
-AutomaticPowerOnForAssignedDuringPeak $True
```

- ユーザーがセッションを起動したときにのみVMをオンにしたい場合は、次のいずれかを実行します。
  - `AutomaticPowerOnForAssigned`と`AutomaticPowerOnForAssignedDuringPeak`を`False`に設定します。
  - UIインターフェイスを使用して、すべての時間をオフピークとして定義し、ピーク時間をまったく設定しないようにします。「スケジュールベースの設定」を参照してください。オフピーク時には、Autoscaleによって管理されている割り当て済みマシンは、ユーザーセッションがない場合にシャットダウンされます。



- ピーク時にAutoscaleによってすべてのマシンがオンになる場合、UIインターフェイスを使用して、待機時間（分）と、Autoscaleによってマシンが電源オンになった後にユーザーがログオンしない場合の「アクションなし」、「一時停止」、または「シャットダウン」などのアクションを設定します。「電源ポリシー」を参照してください。

プールされたマシンについて

セッションログオフ後にプールされたマシンを自動的にシャットダウンするには、デリバリーグループに対してPowerShellコマンド`ShutdownAfterUse`を`True`に設定します。例:

```
Set-BrokerDesktopGroup -Name “DesktopGroupName” -ShutdownDesktopsAfterUse $true
```

メトリックを監視する

デリバリーグループでAutoscaleを有効にすると、DirectorからAutoscaleで管理されているマシンの以下のメトリックを監視できます。

- マシンの使用状況
- 推定節約額
- マシンとセッションのアラート通知
- マシンのステータス
- 負荷評価の傾向

注:

> デリバリーグループでAutoscaleを最初に有効にした場合、そのデリバリーグループの監視データが表示されるまでに数分かかることがあります。 Autoscaleが有効になり、その後デリバリーグループで無効になった場合でも、監視データは引き続き利用可能です。Autoscaleは5分間隔で監視データを収集します。

> メトリックの詳細については、「Autoscaleで管理されるマシンの監視」を参照してください。

休止状態のVMでのAutoscale

Autoscaleの設定可能な設定を通じてVMを休止状態にできます。PowerShellコマンド `Get-BrokerDesktopGroups`、`New-BrokerDesktopGroups`、または `Set-BrokerDesktopGroups` を使用して、パラメーター `AutoscaleScaleDownActionDuringPeak` (ピーク時) または `AutoscaleScaleDownActionDuringOffPeak` (オフピーク時) に以下の正の値を設定し、電源アクションを定義します。

- 0：スケールダウン時にVMをシャットダウンする
- 1：スケールダウン時に一時停止（VMを休止状態にする）

休止状態にできないVMはシャットダウンされます。

Delivery Groupで休止状態が有効になっている場合、休止状態のVMの再起動スケジュールを構成できます。再起動サイクルでは、VMは再開され、その後シャットダウンされます。再起動スケジュールは、毎週、毎日、毎月、および1回に設定できます。複数のスケジュールを構成できます。ただし、休止状態から再開するVMには数分かかる場合があります。

Autoscaleは、ピーク時にセッションがない休止状態のマルチセッションRemote Desktop Services (RDS)および共有シングルセッションVMの電源をオンにすることもできます。VMはMCSおよび非MCSマシンカタログのものである可能性があります。

詳細情報

Autoscaleの詳細については、Tech ZoneのCitrix Autoscaleを参照してください。

スケジュールベースおよび負荷ベースの設定

Autoscale™ がマシンを電源管理する方法

Autoscale は、選択されたスケジュールに基づいてマシンの電源をオン/オフします。Autoscale を使用すると、特定の曜日を含む複数のスケジュールを設定し、その時間帯に利用可能なマシンの数を調整できます。特定の曜日の特定の時間に一連のユーザーがマシンリソースを消費すると予想

される場合、Autoscale は最適化されたエクスペリエンスを提供するのに役立ちます。これらのマシンは、セッションが実行されているかどうかにかかわらず、スケジュール中に電源がオンになることに注意してください。

> **注：**
>
> Autoscale は、電源管理されているすべてのマシンをサポートします。
>
> スケジュールは、デリバリーグループの**タイムゾーン**に基づいています。タイムゾーンを変更するには、デリバリーグループのユーザー設定を変更します。詳細については、「デリバリーグループの管理」を参照してください。

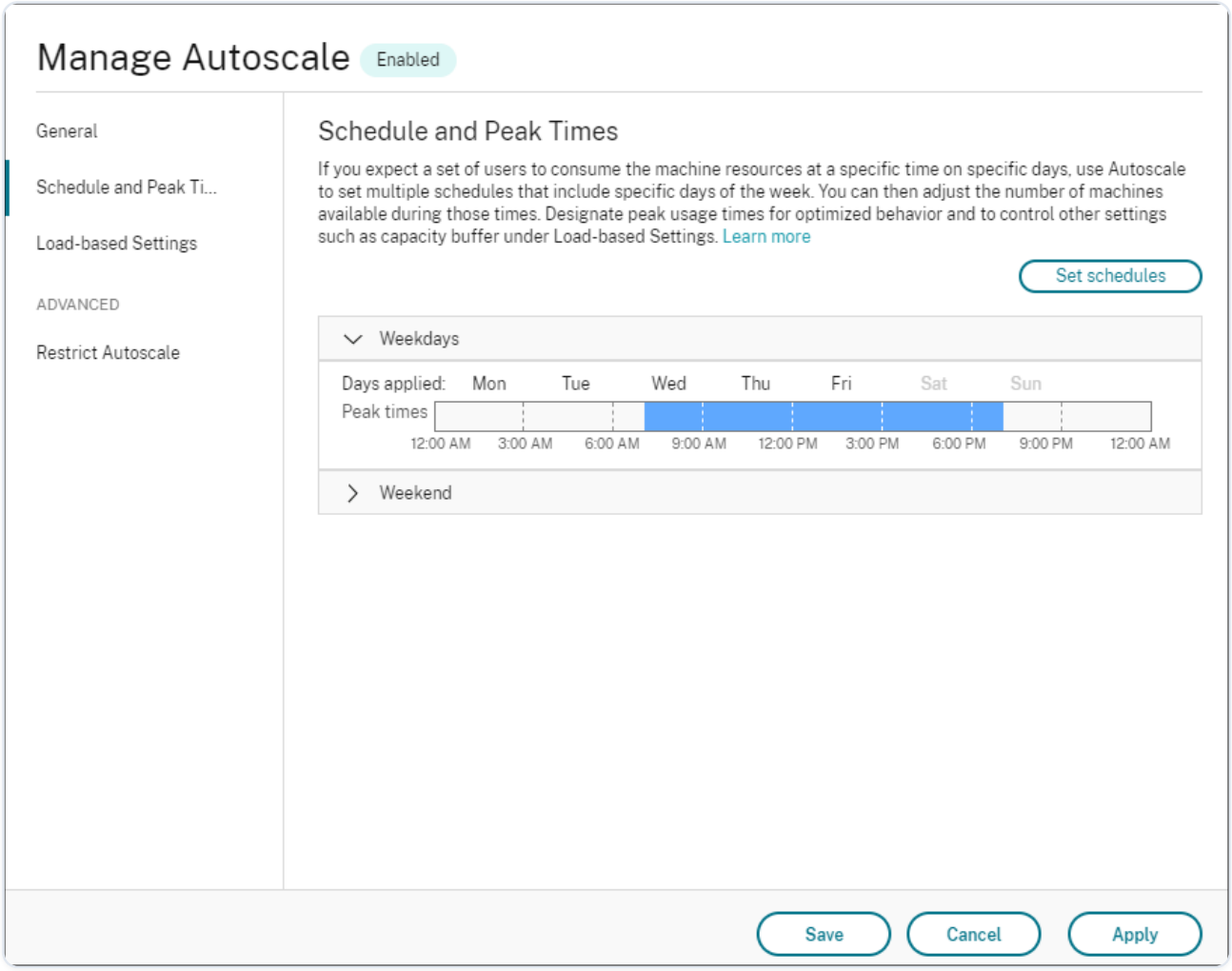
Autoscale には、*平日*（月曜日から金曜日）と*週末*（土曜日と日曜日）の2つのデフォルトスケジュールがあります。デフォルトでは、**平日**スケジュールでは、ピーク時に午前7時から午後6時30分まで1台のマシンの電源がオンになり、オフピーク時には電源がオンになりません。デフォルトの容量バッファは、ピーク時とオフピーク時ともに10%に設定されています。デフォルトでは、**週末**スケジュールでは、マシンの電源はオンになりません。

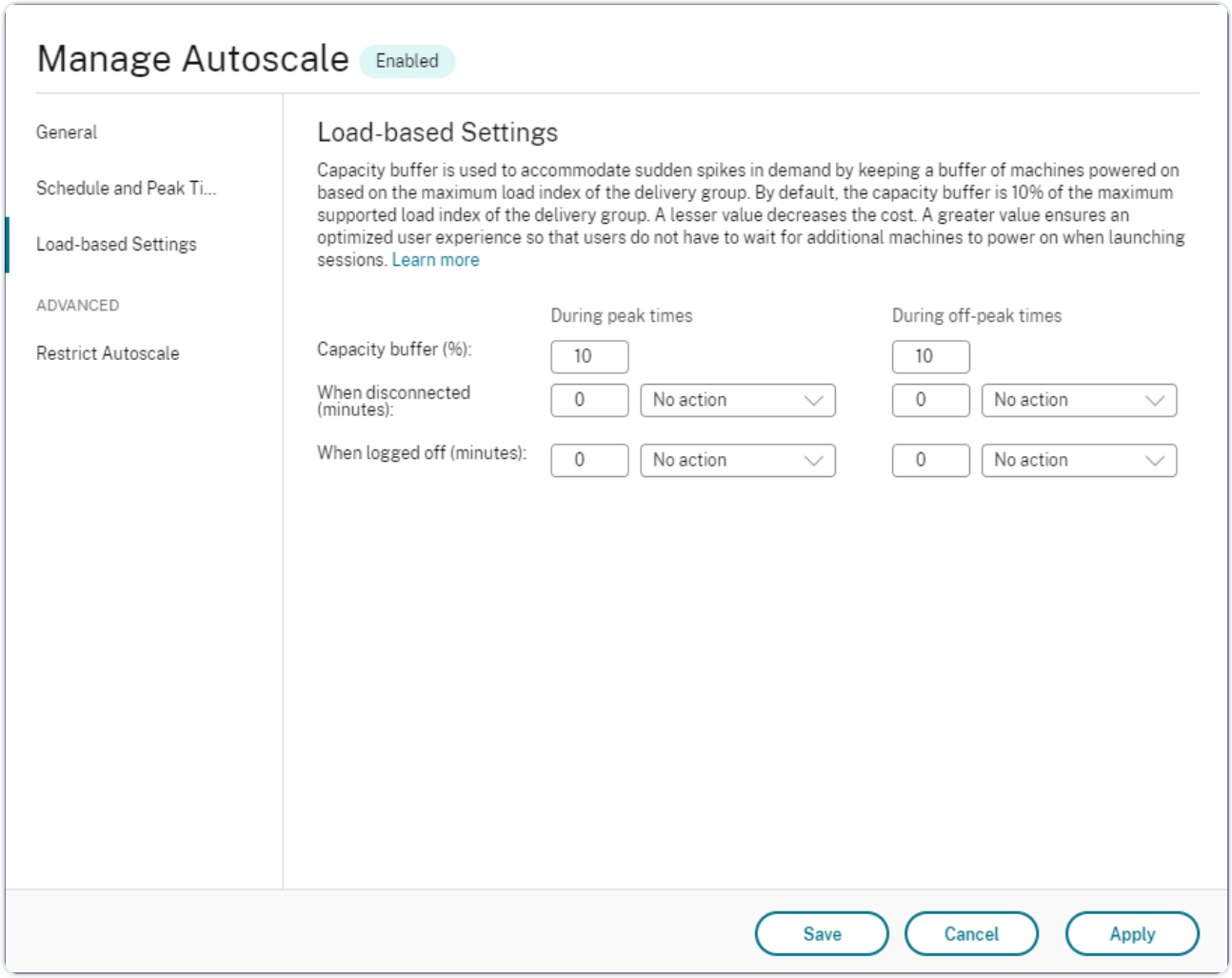
> **注：**
>
> Autoscale は、サイトに登録されているマシンのみを、計算における利用可能な容量の一部として扱います。「登録済み」とは、マシンが使用可能であるか、すでに使用中であることを意味します。これにより、ユーザーセッションを受け入れられるマシンのみがデリバリーグループの容量に含まれるようになります。

ユーザーインターフェイス

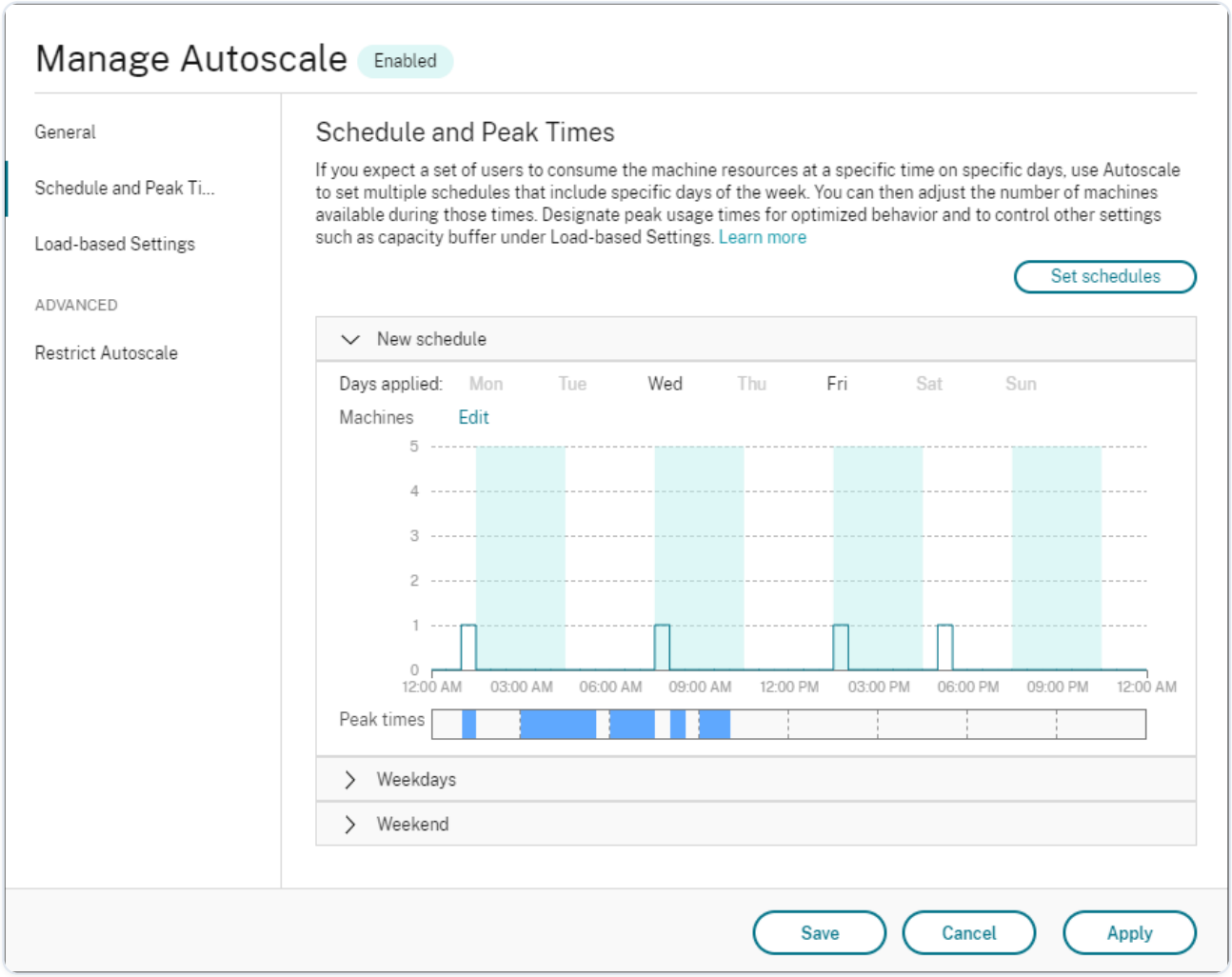
留意すべきユーザーインターフェイスは3種類あります。

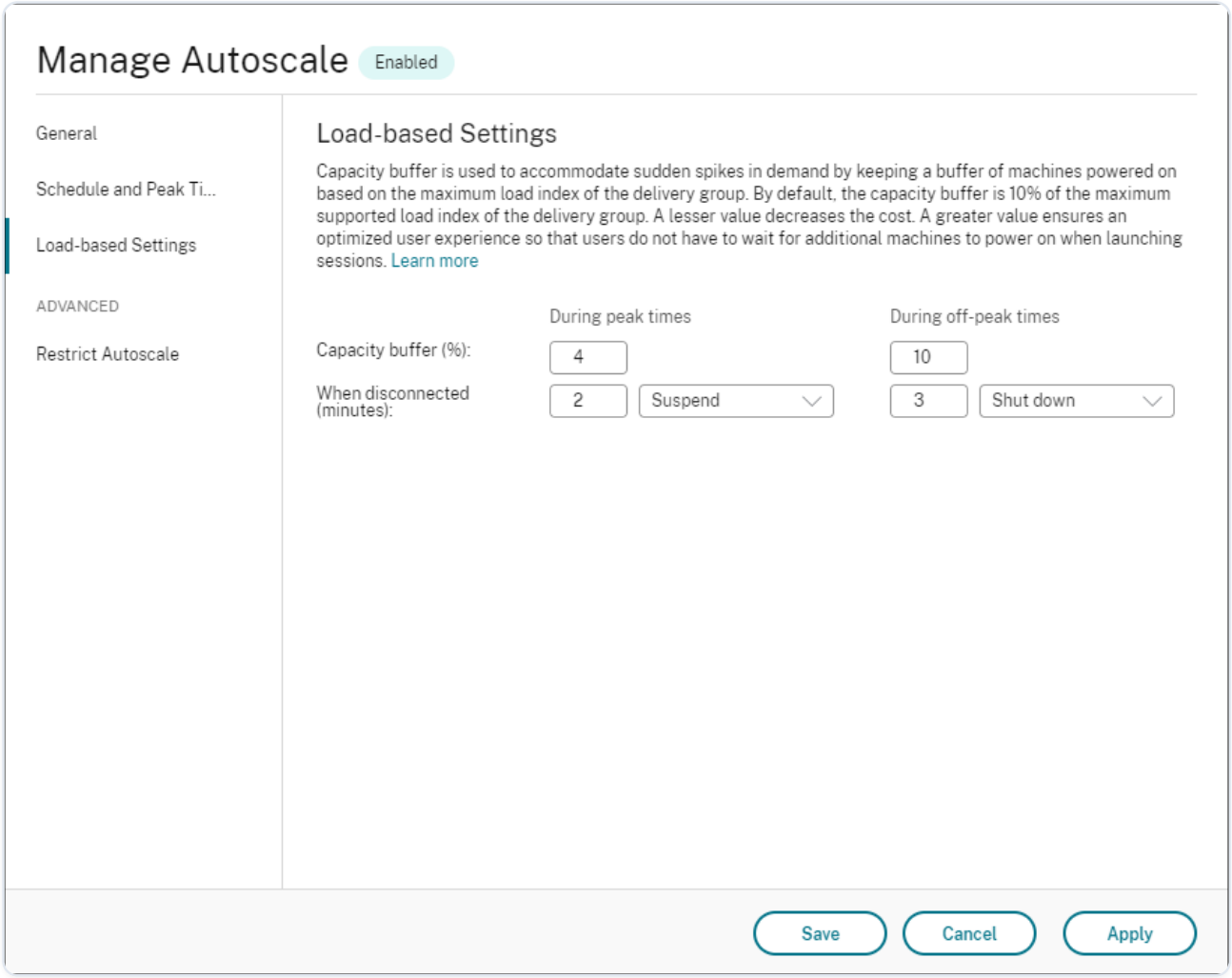
*シングルセッションOS静的デリバリーグループ*のユーザーインターフェイス：


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
Weekdays
Days applied: Mon Tue Wed Thu Fri Sat Sun
Peak times
12:00 AM 3:00 AM 6:00 AM 9:00 AM 12:00 PM 3:00 PM 6:00 PM 9:00 PM 12:00 AM
Weekend
Save
Cancel
Apply

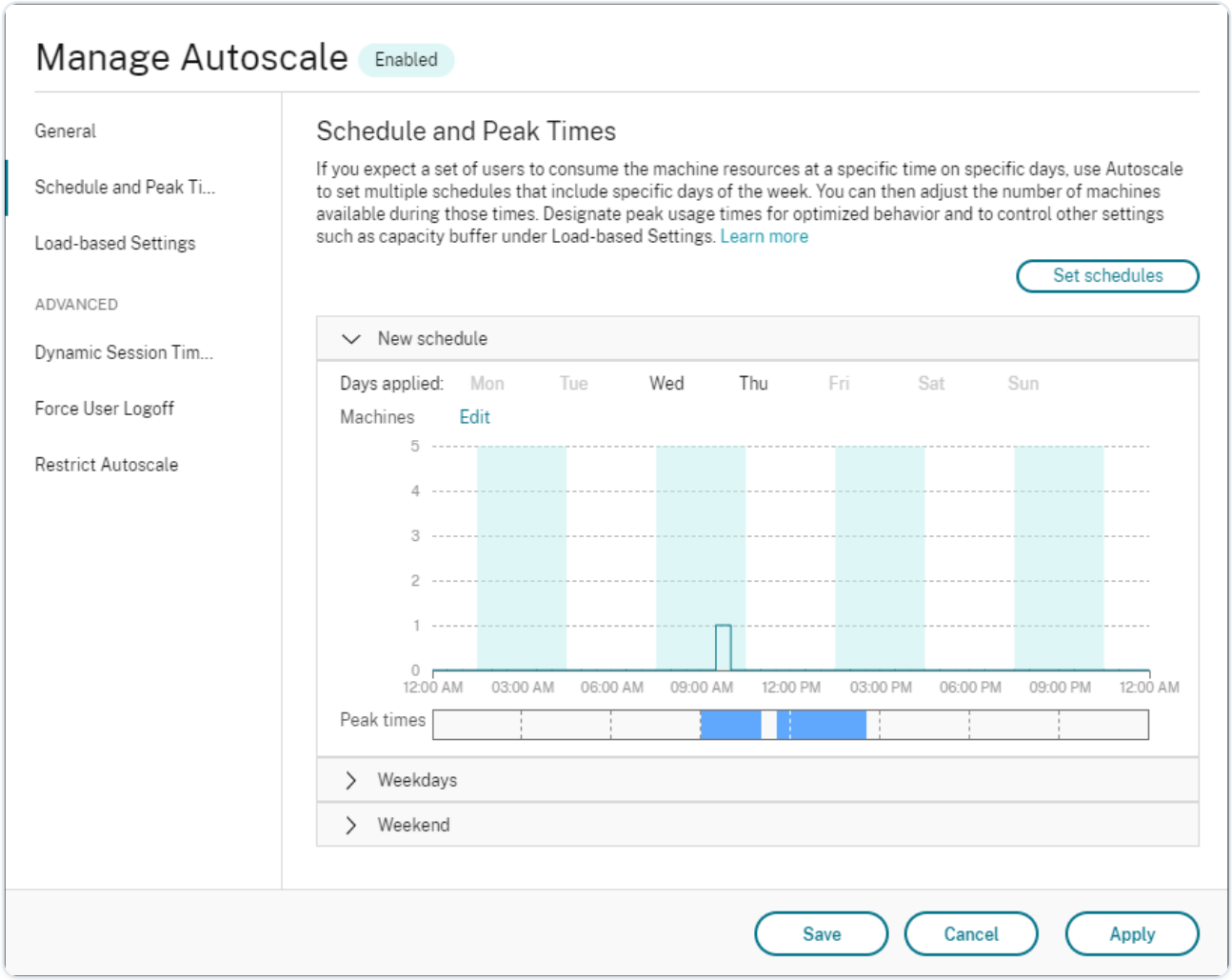


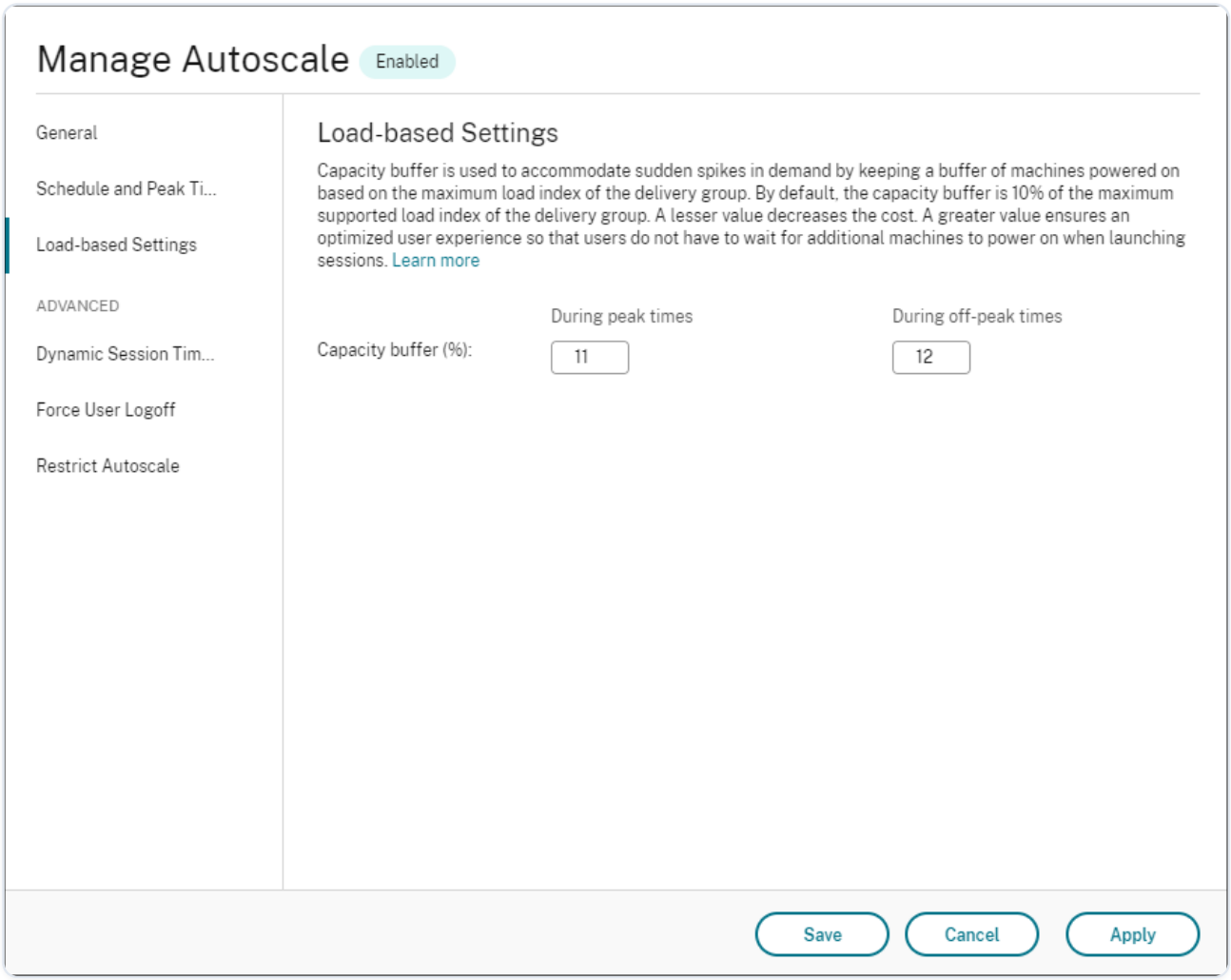
*シングルセッションOSランダムデリバリーグループ*のAutoscaleユーザーインターフェイス：


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
New schedule
Days applied: Mon Tue Wed Thu Fri Sat Sun
Machines Edit
5
4
3
2
1
0
12:00 AM 03:00 AM 06:00 AM 09:00 AM 12:00 PM 03:00 PM 06:00 PM 09:00 PM 12:00 AM
Peak times
Weekdays
Weekend
Save
Cancel
Apply



Autoscale のユーザーインターフェイス (マルチセッションOSデリバリーグループ):


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Dynamic Session Tim...
Force User Logoff
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
New schedule
Days applied: Mon Tue Wed Thu Fri Sat Sun
Machines Edit
5
4
3
2
1
0
12:00 AM 03:00 AM 06:00 AM 09:00 AM 12:00 PM 03:00 PM 06:00 PM 09:00 PM 12:00 AM
Peak times
Weekdays
Weekend
Save
Cancel
Apply



スケジュールベースの設定

Autoscaleスケジュール。スケジュールの追加、編集、選択、削除が可能です。

適用された日数。選択したスケジュールに適用した日を強調表示します。残りの日はグレー表示されます。

編集。マシンを1時間ごとまたは30分ごとに割り当てることができます。マシンは数値またはパーセンテージで割り当てることができます。

> **注:**
>
> - このオプションは、Autoscale のユーザーインターフェイスで、マルチセッションOSおよびシングルセッションOSランダムデリバリーグループにのみ使用できます。
> - **編集**の横にあるヒストグラムは、異なるタイムスロットで実行されているマシンの数または割合を示します。

- **ピーク時間**の上にある**編集**をクリックして、各タイムスロットに**マシンを割り当てる**ことができます。**起動するマシン**ウィンドウのメニューから選択したオプションに応じて、マシンを数値またはパーセンテージで割り当てることができます。
- マルチセッションOSデリバリーグループの場合、各日において30分単位で実行中のマシンの最小数を個別に設定できます。シングルセッションOSランダムデリバリーグループの場合、各日において60分単位で実行中のマシンの最小数を個別に設定できます。

独自のスケジュールを定義するには、次の手順に従います。

1. **Autoscaleの管理**ウィンドウの**スケジュールとピーク時間**ページで、**スケジュールの設定**をクリックします。
2. **Autoscaleスケジュールの編集**ウィンドウで、各スケジュールに適用する曜日を選択します。必要に応じてスケジュールを削除することもできます。
3. **完了**をクリックしてスケジュールを保存し、**スケジュールとピーク時間**ページに戻ります。
4. 該当するスケジュールを選択し、必要に応じて構成します。
5. **適用**をクリックして**Autoscaleの管理**ウィンドウを終了するか、他のページで設定を構成します。

重要:

- Autoscaleでは、異なるスケジュールで同じ曜日が重複することはできません。たとえば、schedule1で月曜日を選択した後、schedule2で月曜日を選択すると、schedule1の月曜日は自動的にクリアされます。
- スケジュール名は大文字と小文字を区別しません。
- スケジュール名は空白にしたり、スペースのみを含めたりすることはできません。
- Autoscaleでは、文字間に空白スペースを使用できます。
- スケジュール名には、次の文字を含めることはできません: \ / ; : # . * ? = < > \| ( ) { } " ' `。
- Autoscaleは重複するスケジュール名をサポートしていません。各スケジュールに異なる名前を入力してください。
- Autoscaleは空のスケジュールをサポートしていません。つまり、曜日が選択されていないスケジュールは保存されません。

注:

選択したスケジュールに含まれる曜日は強調表示され、含まれない曜日はグレー表示されます。

負荷ベースの設定

ピーク時間。選択したスケジュールに適用した日のピーク時間を定義できます。これを行うには、横棒グラフを右クリックします。ピーク時間を定義すると、残りの未定義の時間はデフォルトでオフピーク時間になります。**デフォルト**では、選択したスケジュールに含まれる日のピーク時間として、午前7時から午後7時までの時間帯が定義されています。

重要:

- マルチセッションOSデリバリーグループの場合、ピーク時間の棒グラフは容量バッファに使用されます。
- シングルセッションOSデリバリーグループの場合、ピーク時間の棒グラフは容量バッファに使用され、ログオフ後および/または切断後にトリガーされるアクションを制御します。
- マルチセッションOSおよびシングルセッションOSデリバリーグループの両方で、スケジュールに含まれる日のピーク時間を30分単位で細かく定義できます。または、代わりに`New-BrokerPowerTimeScheme PowerShell`コマンドを使用することもできます。詳しくは、「Broker PowerShell SDKコマンド」を参照してください。

容量バッファ。電源がオンになっているマシンのバッファを維持できます。値が小さいほどコストが削減されます。値が大きいほど、セッション起動時にユーザーが追加のマシンの電源がオンになるのを待つ必要がなくなり、最適化されたユーザーエクスペリエンスが保証されます。デフォルトでは、容量バッファはピーク時間とオフピーク時間で10%です。容量バッファを0に設定すると、セッション起動時にユーザーが追加のマシンの電源がオンになるのを待つ必要がある場合があります。Autoscaleでは、ピーク時間とオフピーク時間で容量バッファを個別に決定できます。

その他の設定

ヒント:

- Broker PowerShell SDKを使用してその他の設定を構成することもできます。詳しくは、「Broker PowerShell SDKコマンド」を参照してください。
- 切断時およびログオフ時の設定に関連するSDKコマンドについては、`<https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy>`を参照してください。

切断時。セッション切断後、切断されロックされたマシンが、一時停止またはシャットダウンされるまでに電源がオンのままになる時間を指定できます。時間値を指定すると、構成したアクションに応じて、指定された切断時間が経過したときにマシンが一時停止またはシャットダウンされます。デフォルトでは、切断されたマシンにはアクションが割り当てられません。ピーク時間とオフピーク時間でアクションを個別に定義できます。そのためには、下矢印をクリックし、メニューから次のいずれかのオプションを選択します。

- **アクションなし**。選択した場合、セッション切断後もマシンは電源がオンのままになります。Autoscaleはそれに対してアクションを実行しません。
- **一時停止**。選択した場合、指定された切断時間が経過すると、Autoscaleはマシンをシャットダウンせずに一時停止します。**一時停止**を選択すると、次のオプションが使用可能になります。
  - **再接続がない場合（分）**。一時停止されたマシンは、切断されたユーザーが再接続したときに利用可能ですが、新しいユーザーには利用できません。すべてのワークロードを処理するためにマシンを再度利用可能にするには、シャットダウンします。Autoscaleがシャットダウンするまでのタイムアウトを分単位で指定します。
- **シャットダウン**。選択すると、指定された切断時間が経過したときに、Autoscaleはマシンをシャットダウンします。

注:

このオプションは、シングルセッションOSのランダムおよび静的デリバリーグループ用のAutoscaleユーザーインターフェイスでのみ利用可能です。

ログオフ時。セッションログオフ後、マシンが一時停止またはシャットダウンされるまでに、どのくらいの時間電源がオンのままになるかを指定できます。時間値を指定した場合、設定したアクションに応じて、指定されたログオフ時間が経過するとマシンは一時停止また

はシャットダウンされます。デフォルトでは、ログオフされたマシンにはアクションが割り当てられません。ピーク時とオフピーク時でアクションを個別に定義できます。そのためには、下矢印をクリックし、メニューから以下のいずれかのオプションを選択します。

- **アクションなし**。選択した場合、セッションログオフ後もマシンは電源がオンのままになります。Autoscale はそのマシンに対して何もアクションを実行しません。
- **一時停止**。選択した場合、指定されたログオフ時間が経過すると、Autoscale はマシンをシャットダウンせずに一時停止します。
- **シャットダウン**。選択した場合、指定されたログオフ時間が経過すると、Autoscale はマシンをシャットダウンします。

注:

このオプションは、シングルセッションOSの静的デリバリーグループ用のAutoscaleユーザーインターフェイスでのみ利用可能です。

切断されたセッションを持つシングルセッションOSマシンが異なる時間帯に移行する際の電源管理

重要:

- この機能強化は、切断されたセッションを持つシングルセッションOSマシンにのみ適用されます。ログオフされたセッションを持つシングルセッションOSマシンには適用されません。
- この機能強化を有効にするには、該当するデリバリーグループでAutoscaleを有効にする必要があります。そうしないと、期間移行時に切断電源ポリシーアクションはトリガーされません。

以前のリリースでは、アクション（切断アクション = 「**一時停止**」または「**シャットダウン**」）が必要な時間帯に移行するシングルセッションOSマシンは、電源がオンのままでした。このシナリオは、アクション（切断アクション = 「**何もしない**」）が不要な時間帯（ピーク時またはオフピーク時）にマシンが切断された場合に発生しました。

このリリース以降、Autoscale は、指定された切断時間が経過すると、移行先の時間帯に設定された切断アクションに応じて、マシンを一時停止または電源オフにします。

例えば、シングルセッションOSデリバリーグループに対して、以下の電源ポリシーを設定します。

- `PeakDisconnectAction` を「何もしない」に設定します。
- `OffPeakDisconnectAction` を「シャットダウン」に設定します。
- 'OffPeakDisconnectTimeout' を「10」に設定します。

注:

切断アクション電源ポリシーの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy>` および `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>` を参照してください。

以前のリリースでは、ピーク時にセッションが切断されたシングルセッションOSマシンは、ピークからオフピークに移行しても電源がオンのままでした。このリリース以降、`OffPeakDisconnectAction` および `OffPeakDisconnectTimeout` ポリシーアクションは、期間移行時にシングルセッションOSマシンに適用されます。その結果、マシンはオフピークに移行してから10分後に電源がオフになります。

以前の動作に戻したい場合（つまり、切断されたセッションでピークからオフピーク、またはオフピークからピークに移行するマシンに対して何もしない場合）は、次のいずれかを実行します。

- 「LegacyPeakTransitionDisconnectedBehaviour」レジストリ値を1（true; 以前の動作を有効にする）に設定します。デフォルトでは、値は0（false; 期間移行時に切断電源ポリシーアクションをトリガーする）です。
  - パス: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - 名前: LegacyPeakTransitionDisconnectedBehaviour
  - 種類: REG_DWORD
  - データ: 0x00000001 (1)
- `Set-BrokerServiceConfigurationData` PowerShellコマンドを使用して設定を構成します。例:

- `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

期間移行時に電源ポリシーアクションが適用される前に、マシンは以下の条件を満たしている必要があります。

- 切断されたセッションがある。
- 保留中の電源アクションがない。
- 異なる期間に移行するシングルセッションOSデリバリーグループに属している。
- 特定の期間（ピーク時またはオフピーク時）に切断されるセッションがあり、電源アクションが割り当てられている期間に移行する。

キャパシティバッファの仕組み

キャパシティバッファは、動的な負荷増加に対応するため、現在の需要に予備容量を追加するために使用されます。留意すべき2つのシナリオがあります。

- マルチセッションOSデリバリーグループの場合、キャパシティバッファは、ロードインデックスの観点から、デリバリーグループの総容量のパーセンテージとして定義されます。ロードインデックスの詳細については、「ロードインデックス」を参照してください。
- シングルセッションOSデリバリーグループの場合、キャパシティバッファは、マシンの数の観点から、デリバリーグループの総容量のパーセンテージとして定義されます。

> **注:**
>
> Autoscaleをタグ付きマシンに制限するシナリオでは、キャパシティバッファは、ロードインデックスの観点から、デリバリーグループ内のタグ付きマシンの総容量のパーセンテージとして定義されます。

> Autoscaleでは、ピーク時とオフピーク時でキャパシティバッファを個別に設定できます。キャパシティバッファフィールドの値が小さいほど、Autoscaleが起動する予備容量が少なくなるため、コストが削減されます。値が大きいほど、ユーザーがセッションを起動する際に追加のマシンが起動するのを待つ必要がなくなり、最適化されたユーザーエクスペリエンスが保証されます。デフォルトでは、キャパシティバッファは10%です。

> **重要:**

キャパシティバッファにより、総予備容量がデリバリーグループの総容量の「X」パーセントを下回った場合にマシンが起動されます。これにより、必要な割合の予備容量が確保されます。

マルチセッションOSデリバリーグループ

マシンはいつ起動されますか?

重要:

スケジュールが選択されている場合、Autoscaleはスケジュールで電源オンになるように構成されているすべてのマシンの電源をオンにします。Autoscaleは、負荷に関係なく、スケジュール中に指定された数のマシンの電源をオンに保ちます。

デリバリーグループ内の電源オン状態のマシン数が、負荷インデックスの観点からバッファ容量を維持するために必要なバッファを満たせなくなった場合、Autoscaleは追加のマシンの電源をオンにします。たとえば、デリバリーグループに20台のマシンがあり、スケジュールベースのスケーリングの一部として、容量バッファ20%で3台のマシンの電源がオンになるようにスケジュールされているとします。最終的に、負荷がない場合でも4台のマシンの電源がオンになります。これは、バッファとして4 x 10kの負荷インデックスが必要であるため、少なくとも4台のマシンの電源がオンになっている必要があるためです。このケースは、ピーク時、マシンの負荷増加、新しいセッションの起動、およびデリバリーグループに新しいマシンを追加する際に発生する可能性があります。Autoscaleは、次の条件を満たすマシンのみの電源をオンにします。

- マシンがメンテナンスモードではない。
- マシンが実行されているハイパーバイザーがメンテナンスモードではない。
- マシンが現在電源オフ状態である。
- マシンに保留中の電源操作はありません。

マシンはいつ電源オフになりますか?

重要:

- スケジュールが選択されている場合、Autoscaleはスケジュールに基づいてマシンの電源をオフにします。
- Autoscaleは、スケジュール中に電源オンになるようにスケジュールで構成されているマシンの電源をオフにしません。

デリバリーグループの目標とする電源オン状態のマシン数（バッファを含む）をサポートするのに十分なマシン数を超えている場合、Autoscaleは余分なマシンの電源をオフにします。このケースは、オフピーク時、マシンの負荷減少、セッションログオフ、およびデリバリーグループからマシンを削除する際に発生する可能性があります。Autoscaleは、次の条件を満たすマシンのみの電源をオフにします。

- マシンと、マシンが実行されているハイパーバイザーがメンテナンスモードではありません。
- マシンが現在電源オン状態である。
- マシンは起動後に利用可能として登録されるか、登録待ちの状態です。
- マシンにアクティブなセッションはありません。
- マシンに保留中の電源操作はありません。
- マシンは指定された電源オフ遅延を満たしています。これは、マシンが少なくとも「X」分間電源オンの状態であったことを意味します。「X」はデリバリーグループに指定された電源オフ遅延です。

例のシナリオ

次のシナリオを想定します。

- **デリバリーグループの構成**。Autoscale で電源管理するデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscaleの構成**
  - 容量バッファは10%に設定されています。
  - 選択したスケジュールにマシンは含まれていません。

シナリオは次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. さらにユーザーセッションが開始されます。
4. セッション終了により、ユーザーセッションの負荷が減少します。

5. ユーザーセッションの負荷は、セッションの負荷がオンプレミスリソースのみで処理されるまでさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかの詳細については、以下を参照してください。

- ユーザー負荷なし (初期状態)
  - 1台のマシン (例: M1) が電源オンになります。マシンは、構成されたキャパシティバッファのために電源オンになります。この場合、10 (マシン数) x 10,000 (負荷インデックス) x 10% (構成されたキャパシティバッファ) は10,000に等しくなります。したがって、1台のマシンが電源オンになります。
  - 電源オンになっているマシン (M1) の負荷インデックス値はベースライン負荷にあります (負荷インデックスは0に等しい)。
- 最初のユーザーがログオンします
  - セッションはマシンM1でホストされるように指示されます。
  - 電源オンになっているマシンM1の負荷インデックスが増加し、マシンM1はもはやベースライン負荷ではありません。
  - Autoscaleは、構成されたキャパシティバッファのために需要を満たすために、追加のマシン (M2) の電源をオンにし始めます。
  - マシンM2の負荷インデックス値はベースライン負荷にあります。
- ユーザーが負荷を増加させます
  - セッションはマシンM1とM2の間で負荷分散されます。その結果、電源オンになっているマシン (M1とM2) の負荷インデックスが増加します。
  - 総予備容量は、負荷インデックスの観点からまだ10,000を超えるレベルにあります。
  - マシンM2の負荷インデックス値はもはやベースライン負荷ではありません。
- より多くのユーザーセッションが開始されます
  - セッションはマシン（M1およびM2）間で負荷分散されます。その結果、電源がオンになっているマシン（M1およびM2）の負荷インデックスがさらに増加します。
  - 負荷インデックスの観点から、合計予備容量が10,000を下回るレベルに低下すると、Autoscaleは、構成された容量バッファにより、需要を満たすため追加のマシン（M3）の電源をオンにし始めます。
  - マシンM3の負荷インデックス値はベースライン負荷にあります。

- さらに多くのユーザーセッションが開始されます
  - セッションはマシン（M1からM3）間で負荷分散されます。その結果、電源がオンになっているマシン（M1からM3）の負荷インデックスが増加します。
  - 負荷インデックスの観点から、合計予備容量は10,000を超えるレベルにあります。
  - マシンM3の負荷インデックス値はもはやベースライン負荷ではありません。
- セッション終了によりユーザーセッション負荷が減少します
  - ユーザーがセッションからログオフするか、アイドルセッションがタイムアウトすると、マシンM1からM3で解放された容量は、他のユーザーが開始したセッションをホストするために再利用されます。
  - 負荷インデックスの観点から、合計予備容量が10,000を超えるレベルに増加すると、Autoscaleは、いずれかのマシン（たとえばM3）をドレイン状態にします。その結果、新しい変更が発生しない限り、他のユーザーが開始したセッションはそのマシンに転送されなくなります。たとえば、エンドユーザーの負荷が再び増加したり、他のマシンの負荷が最も低くなったりする場合です。
- ユーザーセッション負荷は減少し続けます
  - マシンM3上のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、Autoscaleはマシン M3の電源をオフにします。
  - さらに多くのユーザーがセッションを終了すると、電源がオンになっているマシン（M1およびM2）で解放された容量は、他のユーザーが開始したセッションをホストするために再利用されます。
  - 負荷インデックスの観点から、合計予備容量が10,000を超えるレベルに増加すると、Autoscaleは、いずれかのマシン（たとえばM2）をドレイン状態にします。その結果、他のユーザーが開始したセッションはそのマシンに転送されなくなります。
- セッションがなくなるまでユーザーセッション負荷は減少し続けます
  - M2上のすべてのセッションが終了し、指定された電源オフ遅延時間が経過すると、AutoscaleはM2の電源をオフにします。
  - 電源がオンになっているマシン（M1）の負荷インデックス値は、ベースライン負荷にあります。Autoscaleは、構成されたキャパシティバッファのため、マシンM1をドレイン状態にしません。

> **注:**

> マルチセッションOSデリバリーグループの場合、ユーザーがセッションからログオフすると、デスクトップへのすべての変更は失われます。ただし、構成されている場合、ユーザー固有の設定はユーザープロファイルとともにローミングされます。

シングルセッションOSランダムデリバリーグループ

キャパシティバッファは、デリバリーグループ内のマシンの総数に基づいて、電源がオンになっているマシンのバッファを維持することで、需要の急増に対応するために使用されます。デフォルトでは、キャパシティバッファはデリバリーグループ内のマシンの総数の10%です。

マシンの数（キャパシティバッファを含む）が現在電源がオンになっているマシンの総数を超える場合、需要を満たすために追加のマシンの電源がオンになります。マシンの数（キャパシティバッファを含む）が現在電源がオンになっているマシンの総数よりも少ない場合、余分なマシンは、構成したアクションに応じてシャットダウンまたは一時停止されます。

電源ポリシー

さまざまなシナリオに合わせてマシンの電源を管理するポリシーを構成します。各シナリオについて、待機時間（分単位）と、指定された時間が終了した後に実行するアクションを指定できます。電源ポリシーは、シングルセッションOSランダムデリバリーグループおよびシングルセッションOSスタティックデリバリーグループに適用されます。

電源ポリシーのアクション(/en-us/citrix-virtual-apps-desktops/2511/media/power-policies-actions.png)

切断後、ピーク時とオフピーク時の両方で以下の設定が適用されます。

- ドロップダウンから、待機時間（分単位）と、アクション（アクションなし、一時停止、シャットダウンなど）を設定できます。
- 一時停止アクションを選択した場合、マシンをシャットダウンするための追加の待機時間を構成します。

> **注:**
>
> - ピーク時とオフピーク時では、シャットダウンアクションの待機時間は、一時停止の待機時間よりも長くする必要があります。
> - サスペンドされたマシンは、再接続時に切断されたユーザーのみがアクセスできます。新しいユーザーがサスペンドされたマシンを利用できるようにするには、それらをシャットダウンします。

- サスペンドおよびシャットダウンフィールドの時刻設定が正しく構成されていない場合、**保存**オプションは無効になり、設定エラーを示す赤い点もナビゲーション項目の横に表示されます。

シングルセッションOSランダムDG電源ポリシー設定(/en-us/citrix-virtual-apps-desktops/2511/media/single-session-os-random-dg-power-policies-settings.png)

例

- 待機時間を12分に設定し、最初の操作を「操作なし」に選択した場合、12分が経過した後もマシンは電源オンの状態を維持します。
- 待機時間を15分に設定し、最初の操作を「サスペンド」に選択し、2番目の待機時間を20分に設定した場合、15分が経過した後、マシンはサスペンドされます。2番目の待機時間が経過した後、マシンはシャットダウンされます。
- 待機時間を18分に設定し、最初の操作を「シャットダウン」に選択した場合、18分が経過した後、マシンはシャットダウンされます。

シナリオ例

次のシナリオを想定します。

- **デリバリーグループの構成**。Autoscaleで電源管理するデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscaleの構成**
  - 容量バッファは10%に設定されています。
  - 選択されたスケジュールにはマシンが含まれていません。

シナリオは次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. さらに多くのユーザーセッションが開始されます。
4. セッション終了により、ユーザーセッションの負荷が減少します。
5. セッション負荷がオンプレミスリソースのみで処理されるようになるまで、ユーザーセッションの負荷はさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかの詳細については、以下を参照してください。

- ユーザー負荷なし（初期状態）
  - 1台のマシン（M1）が電源オンになります。このマシンは、構成された容量バッファのために電源オンになります。この場合、10（マシンの数）x 10%（構成された容量バッファ）は1になります。したがって、1台のマシンが電源オンになります。
- 最初のユーザーがログオンします
  - ユーザーがデスクトップを使用するために初めてログオンすると、電源オンになっているマシンでホストされているデスクトップのプールからデスクトップが割り当てられます。この場合、ユーザーにはマシンM1からデスクトップが割り当てられます。
  - 構成された容量バッファのため、Autoscaleは需要を満たすために追加のマシン（M2）の電源をオンにし始めます。
- ユーザーが負荷を増加させます
  - セッションはマシン M1 と M2 の間で負荷分散されます。その結果、起動中のマシン (M1 と M2) の負荷インデックスが増加します。
  - 総予備容量は、負荷インデックスの観点から依然として 10,000 を超えるレベルにあります。
  - マシン M2 の負荷インデックス値はもはやベースライン負荷ではありません。
- 3番目のユーザーがログオンします
  - ユーザーにはマシンM3からデスクトップが割り当てられます。
  - Autoscale は、設定されたキャパシティバッファのために、需要を満たすため追加のマシン (M4) の電源をオンにし始めます。
- ユーザーがログオフします
  - ユーザーがログオフするか、ユーザーのデスクトップがタイムアウトすると、解放されたキャパシティ (例: M3) がバッファとして利用可能になります。その結果、キャパシティバッファが10%に設定されているため、Autoscale はマシン M4 の電源をオフにし始めます。
- ユーザーがいなくなるまで、さらに多くのユーザーがログオフします
  - さらに多くのユーザーがログオフした後、Autoscale はマシン (例: M2 または M3) の電源をオフにします。
  - ユーザーが残っていなくても、Autoscale は残りの1台のマシン (例: M1) の電源をオフにしません。そのマシンは予備のキャパシティとして予約されているためです。

> **注:**
>
> シングルセッションOSのランダムデリバリーグループの場合、ユーザーがセッションをログオフすると、デスクトップへのすべての変更は失われます。ただし、設定されている場合、ユーザー固有の設定はユーザープロファイルとともにローミングされます。

シングルセッションOSランダムデリバリーグループ

キャパシティバッファは、デリバリーグループ内の未割り当てマシンの総数に基づいて、未割り当てマシンのバッファの電源をオンに保つことで、急激な需要の急増に対応するために使用されます。デフォルトでは、キャパシティバッファはデリバリーグループ内の未割り当てマシンの総数の10%です。

> **重要:**
>
> デリバリーグループ内のすべてのマシンが割り当てられた後、キャパシティバッファはマシンの電源のオン/オフには関与しません。

> マシンの数 (キャパシティバッファを含む) が現在電源がオンになっているマシンの総数を超える場合、需要を満たすために追加の未割り当てマシンが電源オンになります。マシンの数 (キャパシティバッファを含む) が現在電源がオンになっているマシンの総数よりも少ない場合、設定したアクションに応じて、余分なマシンは電源オフまたは一時停止されます。

シングルセッションOSの静的デリバリーグループの場合、Autoscale は次のようになります。

- 該当するシングルセッションOSデリバリーグループの `AutomaticPowerOnForAssigned` プロパティが true に設定されている場合にのみ、ピーク時に割り当てられたマシンの電源をオンにし、オフピーク時に電源をオフにします。
- ピーク時に電源がオフになっているマシンを自動的に電源オンにします。ただし、そのマシンが属するデリバリーグループの`AutomaticPowerOnForAssignedDuringPeak`プロパティがtrueに設定されている場合に限ります。

割り当てられたマシンで容量バッファがどのように機能するかを理解するには、以下を考慮してください。

- 容量バッファは、デリバリーグループに1つ以上の未割り当てマシンがある場合にのみ機能します。

- デリバリーグループに未割り当てマシンがない場合 (デリバリーグループ内のすべてのマシンが割り当てられている場合)、容量バッファはマシンの電源オン/オフに影響しません。
- `AutomaticPowerOnForAssignedDuringPeak`プロパティは、ピーク時に割り当てられたマシンが電源オンになるかどうかを決定します。trueに設定されている場合、Autoscaleはピーク時にマシンの電源をオンに保ちます。また、電源がオフになっている場合でも、Autoscaleはそれらを電源オンにします。

電源ポリシー

さまざまなシナリオでマシンの電源を管理するポリシーを構成します。各シナリオについて、待機時間（分単位）と、指定された時間が終了した後に実行するアクションを指定できます。電源ポリシーは、シングルセッションOSランダムデリバリーグループおよびシングルセッションOS静的デリバリーグループに適用されます。

電源ポリシーのアクション(/en-us/citrix-virtual-apps-desktops/2511/media/power-policies-actions.png)

切断後および**ログオフ後**の場合、以下の設定は、ピーク時とオフピーク時の両方に適用されます。ドロップダウンから、待機時間 (分単位) と、アクション (アクションなし、一時停止、シャットダウンなど) を設定できます。

Autoscaleによってマシンが電源オンにされた後、ユーザーがログオンしない場合、以下の設定はピーク時にのみ適用されます。ピーク時に、ドロップダウンから待機時間 (分単位) と、アクション (アクションなし、一時停止、シャットダウンなど) を設定できます。

> **注:**
>
> - ピーク時およびオフピーク時において、シャットダウンアクションの待機時間は、一時停止の待機時間よりも長くする必要があります。
> - 一時停止されたマシンは、切断されたユーザーが再接続した場合にのみアクセス可能です。一時停止されたマシンを新規ユーザーが利用できるようにするには、シャットダウンしてください。
> - 一時停止フィールドとシャットダウンフィールドの時刻設定が正しく構成されていない場合、**保存**オプションが無効になり、設定エラーを示す赤い点もナビゲーション項目の横に表示されます。

> シングルセッションOSランダムDG電源ポリシー設定(/en-us/citrix-virtual-apps-desktops/2511/media/single-session-os-random-dg-power-policies-settings.png)

- **デリバリーグループの構成**。Autoscaleで電源管理するデリバリーグループには、10台のマシン (M1～M10) が含まれています。
- **Autoscaleの構成**
  - マシンM1～M3は割り当て済みで、マシンM4～M10は未割り当てです。
  - ピーク時とオフピーク時のキャパシティバッファは10%に設定されています。
  - 選択されたスケジュールに従って、Autoscaleは午前9時から午後6時の間、マシンを電源管理します。

上記のシナリオでAutoscaleがどのように機能するかについての詳細は、以下を参照してください。

- スケジュールの開始 – 午前9時
  - AutoscaleはマシンM1からM3を起動します。
  - 設定されたキャパシティバッファのため、Autoscaleは追加のマシン（例: M4）を起動します。マシンM4は割り当てられていません。
- 最初のユーザーがログオンします
  - ユーザーがデスクトップを使用するために初めてログオンすると、ユーザーは、割り当てられていない電源オン状態のマシンでホストされているデスクトップのプールからデスクトップを割り当てられます。この場合、ユーザーはマシンM4からデスクトップを割り当てられます。そのユーザーによるその後のログオンは、初回使用時に割り当てられた同じデスクトップに接続します。
  - 設定されたキャパシティバッファのため、Autoscaleは需要を満たすために追加のマシン（例: M5）を起動し始めます。
- 2番目のユーザーがログオンします
  - ユーザーは、割り当てられていない電源オン状態のマシンからデスクトップを割り当てられます。この場合、ユーザーはマシンM5からデスクトップを割り当てられます。そのユーザーによるその後のログオンは、初回使用時に割り当てられた同じデスクトップに接続します。
  - 設定されたキャパシティバッファのため、Autoscaleは需要を満たすために追加のマシン（例: M6）を起動し始めます。

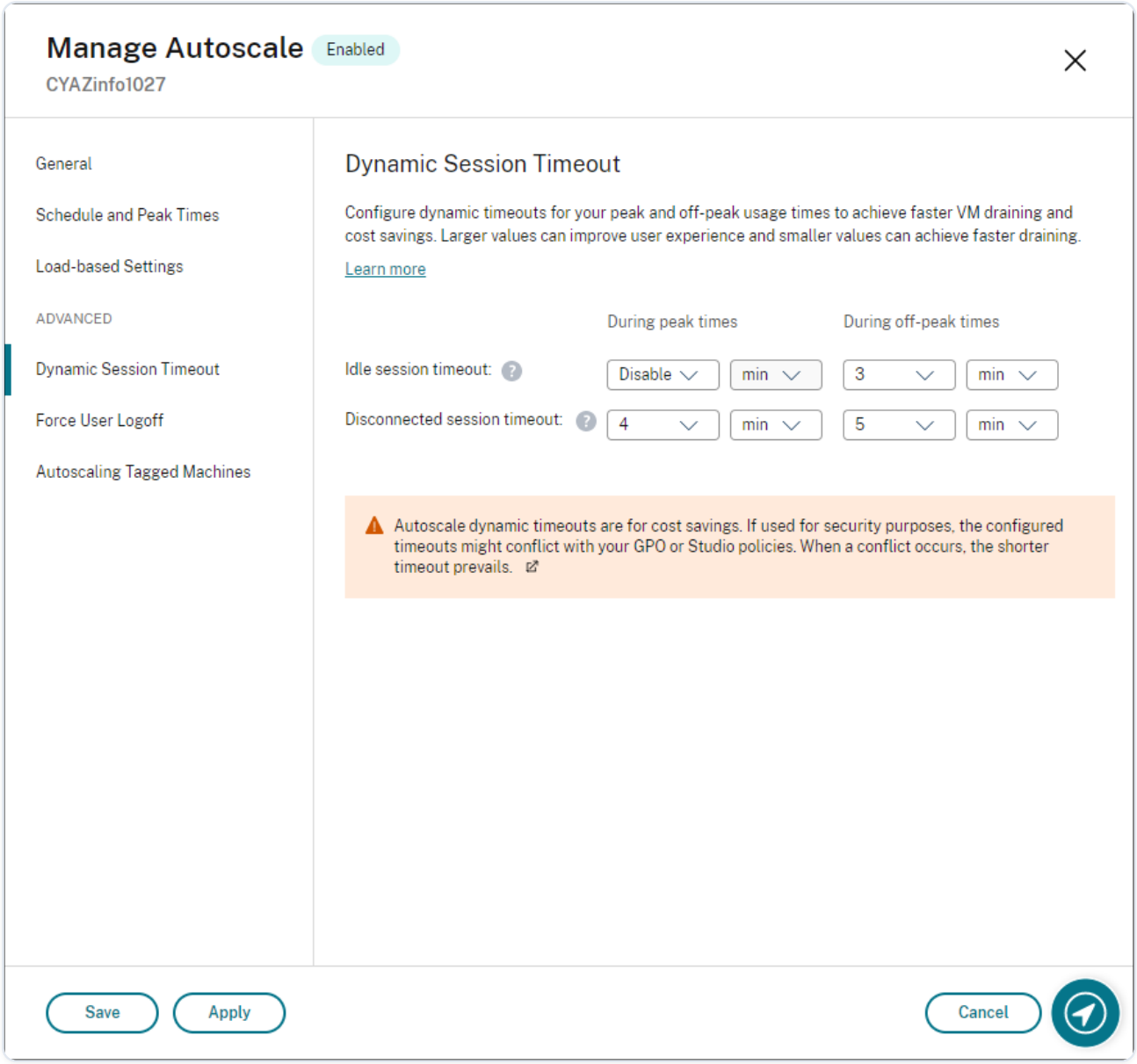
- ユーザーがログオフします
  - ユーザーがデスクトップからログオフするか、デスクトップがタイムアウトすると、Autoscaleは午前9時から午後6時の間、マシンM1からM5を電源オン状態に保ちます。それらのユーザーが次回ログオンするとき、初回使用時に割り当てられた同じデスクトップに接続します。
  - 割り当てられていないマシンM6は、新しく割り当てられるユーザーにデスクトップを提供するのを待機しています。
- スケジュールの終了 – 午後 6 時
  - 午後 6 時、Autoscale はマシン M1 から M5 の電源をオフにします。
  - Autoscale は、構成された容量バッファのため、未割り当てのマシン M6 の電源をオンのままにします。そのマシンは、受信する未割り当てユーザーにデスクトップを提供するのを待機しています。
  - デリバリーグループでは、マシン M6 から M10 が未割り当てのマシンです。

動的セッションタイムアウト

この機能を使用すると、ピーク時とオフピーク時の使用時間に合わせて切断されたセッションとアイドルセッションのタイムアウトを設定し、マシンのドレインを高速化してコストを削減できます。この機能は以下に適用されます。

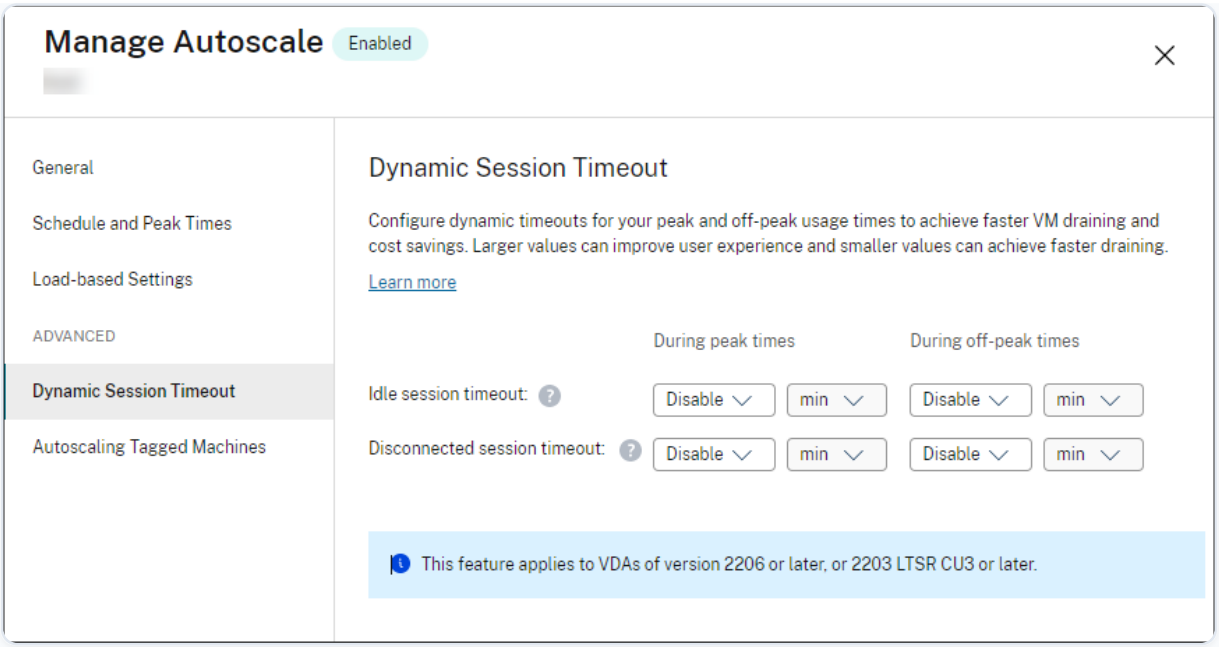
- シングルセッションおよびマルチセッションOSマシン。
- オートスケール用にタグ付けされているかどうかにかかわらず、デリバリーグループ内のすべてのマシン。

VDAは、10分以上アイドル状態のセッションのアイドル時間を報告するため、動的セッションタイムアウトでは、アイドル状態になってから10分以内にアイドルセッションを切断することはできません。より短い値を設定すると、残存するセッションがより早く削除され、コストが削減されます。



注:

- この機能は、マルチセッションOSデリバリーグループで常に利用できます。
- シングルセッションOSデリバリーグループの場合、この機能はバージョン2206 CR以降、または2203 LTSR CU3以降のVDAに適用されます。これらのVDAがCitrix Cloud™に少なくとも1回登録されていることを確認してください。利用できない場合、次のユーザーインターフェイスが表示されます。



- Autoscale™ の動的タイムアウトはコスト削減を目的としています。セキュリティ目的で使用する場合、構成されたタイムアウトがGPOまたは管理コンソールポリシーと競合する可能性があります。競合が発生した場合、短い方のタイムアウトが優先されます。

アイドルセッションタイムアウト。ユーザー入力がない場合に、中断されていないユーザー接続が維持される時間を指定するタイマーを有効または無効にします。タイマーが期限切れになると、セッションは切断状態になり、**切断セッションタイムアウト**が適用されます。**切断セッションタイムアウト**が無効になっている場合、セッションはログオフされません。

重要:

- 10分（600秒）以下の値を指定した場合、Autoscale は、関連するセッションが10分間アイドル状態になった後に切断します。これは、Autoscale がVDAが報告するセッションのアイドル時間に依存しているためです。VDAは、10分以上アイドル状態のセッションに対してのみアイドル時間を報告します。
- アイドルセッションタイムアウトに達するまでの最後の5分間にユーザーが操作した場合でも、アイドルセッションは切断状態になることがあります。

> **切断されたセッションのタイムアウト**。切断されたデスクトップがセッションのログオフ前にロックされたままになる時間を指定するタイマーを有効または無効にします。有効にすると、タイマーの期限が切れたときに切断されたセッションがログオフされます。

よくある質問

動的セッションタイムアウト機能は、オートスケール用にタグ付けされたマシンにのみ適用されます?

動的セッションタイムアウト機能は、オートスケール用にタグ付けされているかどうかにかかわらず、デリバリーグループ内のすべてのマシンに適用されます。

動的セッションタイムアウトによりセッションがログオフされた場合、タグ付けされていないマシンも、タグ付けされたマシンのオートスケールターゲットに含まれます?

動的セッションタイムアウト機能は、オートスケールタグ付け機能とは関係ありません。動的セッションタイムアウトによってセッションが終了した場合、マシンがシャットダウンされるまでドレイン状態になっている場合に限り、タグ付けされていないマシンもそのプロセス中にシャットダウンされる可能性があります。

タグ付けされたマシンのオートスケール (クラウドバースト)

> **注:**
>
> この機能は以前、「オートスケールの制限」という名称でした。

はじめに

Autoscaleは、デリバリーグループ内のマシンの一部のみを電源管理する柔軟性を提供します。これを実現するには、1つ以上のマシンにタグを適用し、Autoscaleがタグ付けされたマシンのみを電源管理するように構成します。

この機能は、クラウドベースのリソースが追加の需要（つまり、バーストワークロード）に対応する前に、オンプレミスリソース（または予約済みのパブリッククラウドインスタンス）を使用してワークロードを処理したいクラウドバーストのユースケースで役立ちます。オンプレミスのマシン（または予約済みインスタンス）に最初にワークロードを処理させるには、タグ制限とゾーン優先度を併用する必要があります。

タグ制限は、Autoscaleによって電源管理されるマシンを指定します。ゾーン優先度は、ユーザーの起動要求を処理する優先ゾーン内のマシンを指定します。詳細については、タグおよびゾーン優先度を参照してください。

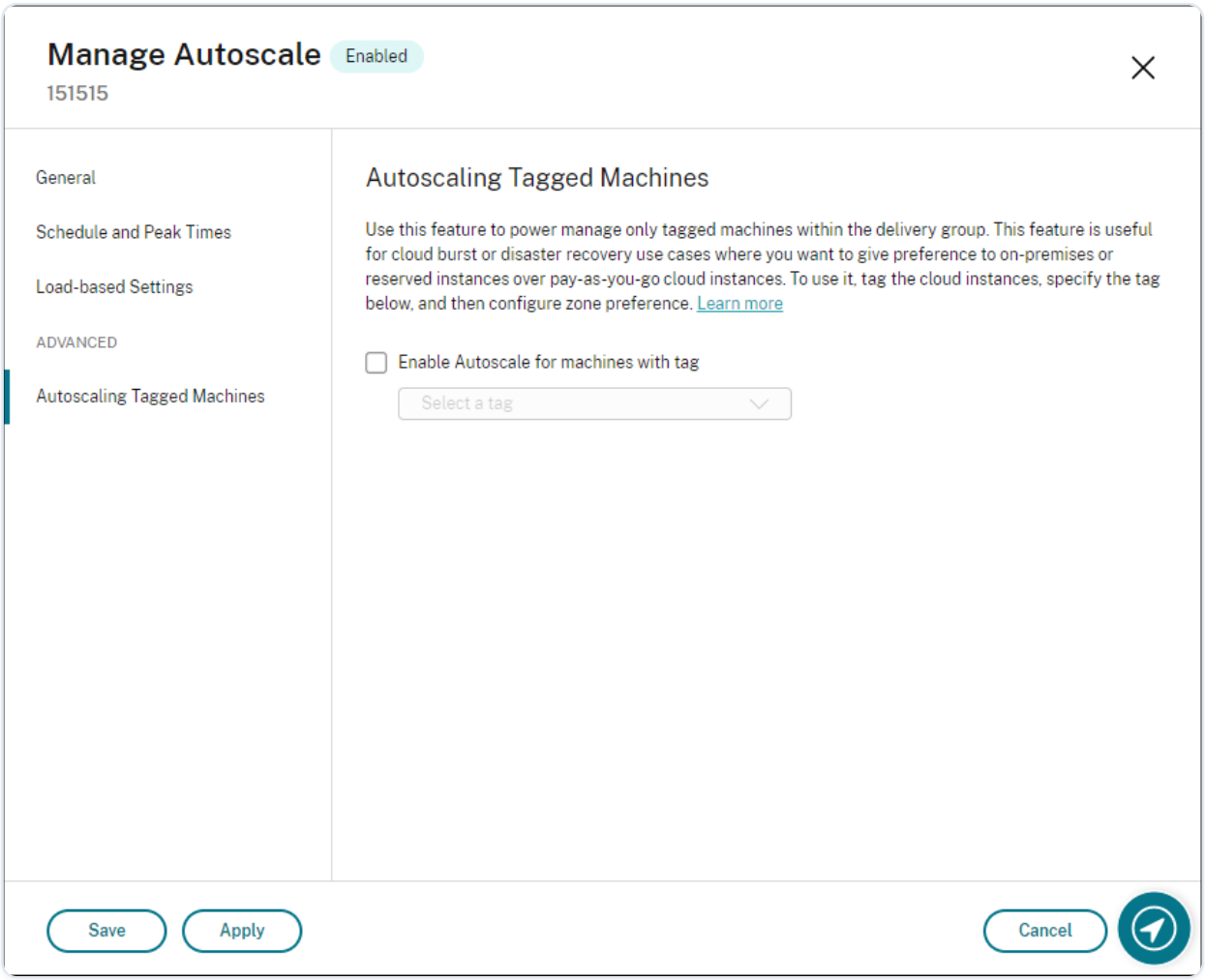
特定のタグ付けされたマシンをオートスケールするには、ManageコンソールまたはPowerShellを使用できます。

Manageコンソールを使用して特定のタグ付けされたマシンをオートスケールする

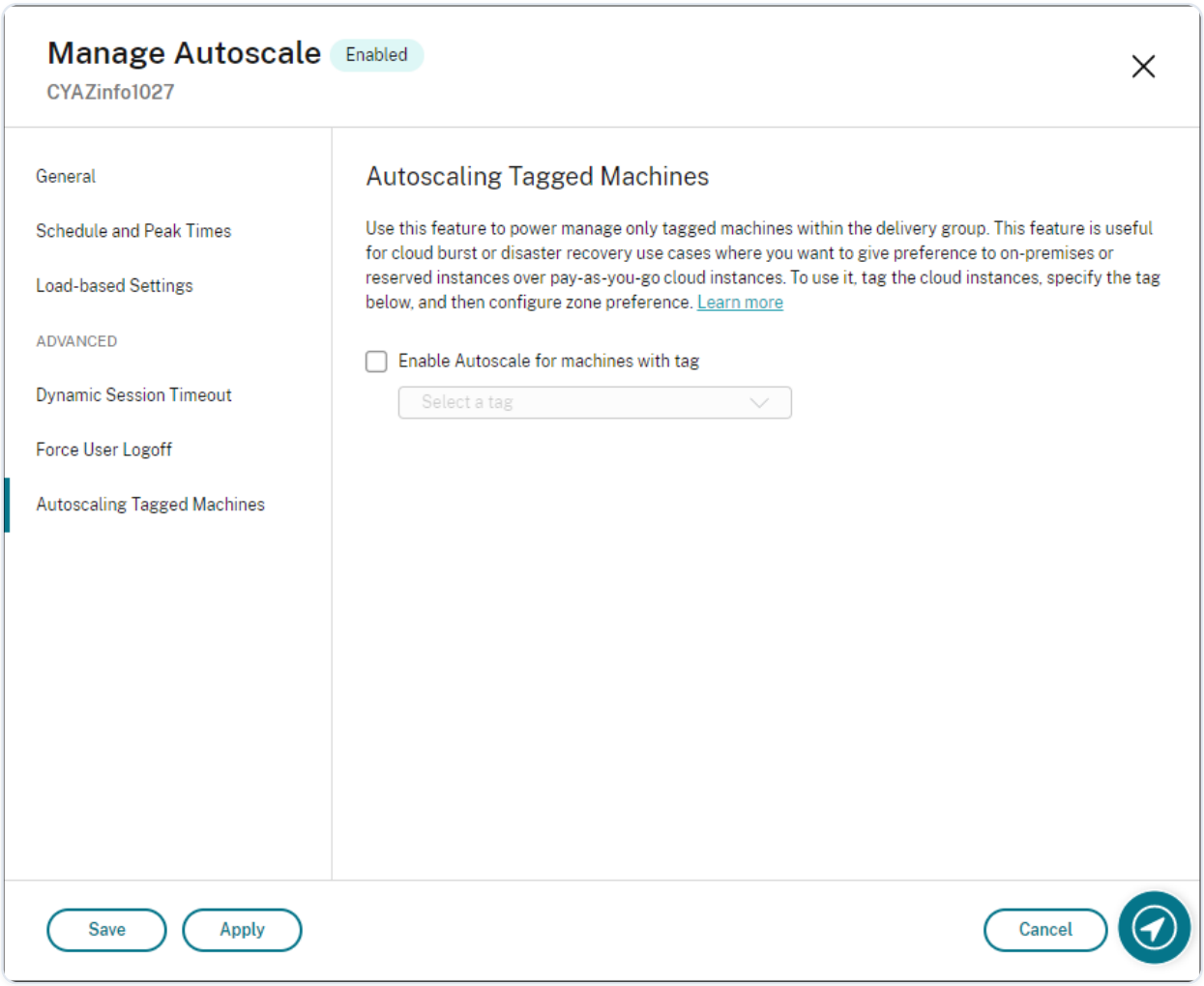
特定のタグ付けされたマシンをオートスケールするには、次の手順を実行します。

1. タグを作成し、そのタグをデリバリーグループ内の該当するマシンに適用します。詳細については、タグとタグ制限の管理を参照してください。
2. デリバリーグループを選択し、**Autoscaleの管理**ウィザードを開きます。
3. **タグ付けされたマシンのオートスケール**ページで、**タグ付きマシンのAutoscaleを有効にする**を選択し、リストからタグを選択して、**適用**をクリックして変更を保存します。

   シングルセッションOSの*静的*および*ランダム*なデリバリーグループのユーザーインターフェイス:



マルチセッションOSデリバリーグループのユーザーインターフェイス:



警告:

- 特定のタグを持つマシンのAutoscaleにより、タグごとのマシン数を反映するようにヒストグラムが自動的に更新される場合があります。**スケジュールとピーク時間**ページで、必要に応じて各時間帯にマシンを手動で割り当てることができます。
- タグ付きマシンで使用されているタグは削除できません。タグを削除するには、まずタグの制限を解除する必要があります。

タグの制限を適用した後、後でデリバリーグループから削除したい場合があります。そのためには、**Autoscaleの管理 > タグ付けされたマシンのAutoscale**ページに移動し、**タグ付きマシンのAutoscaleを有効にする**のチェックを外します。

警告:

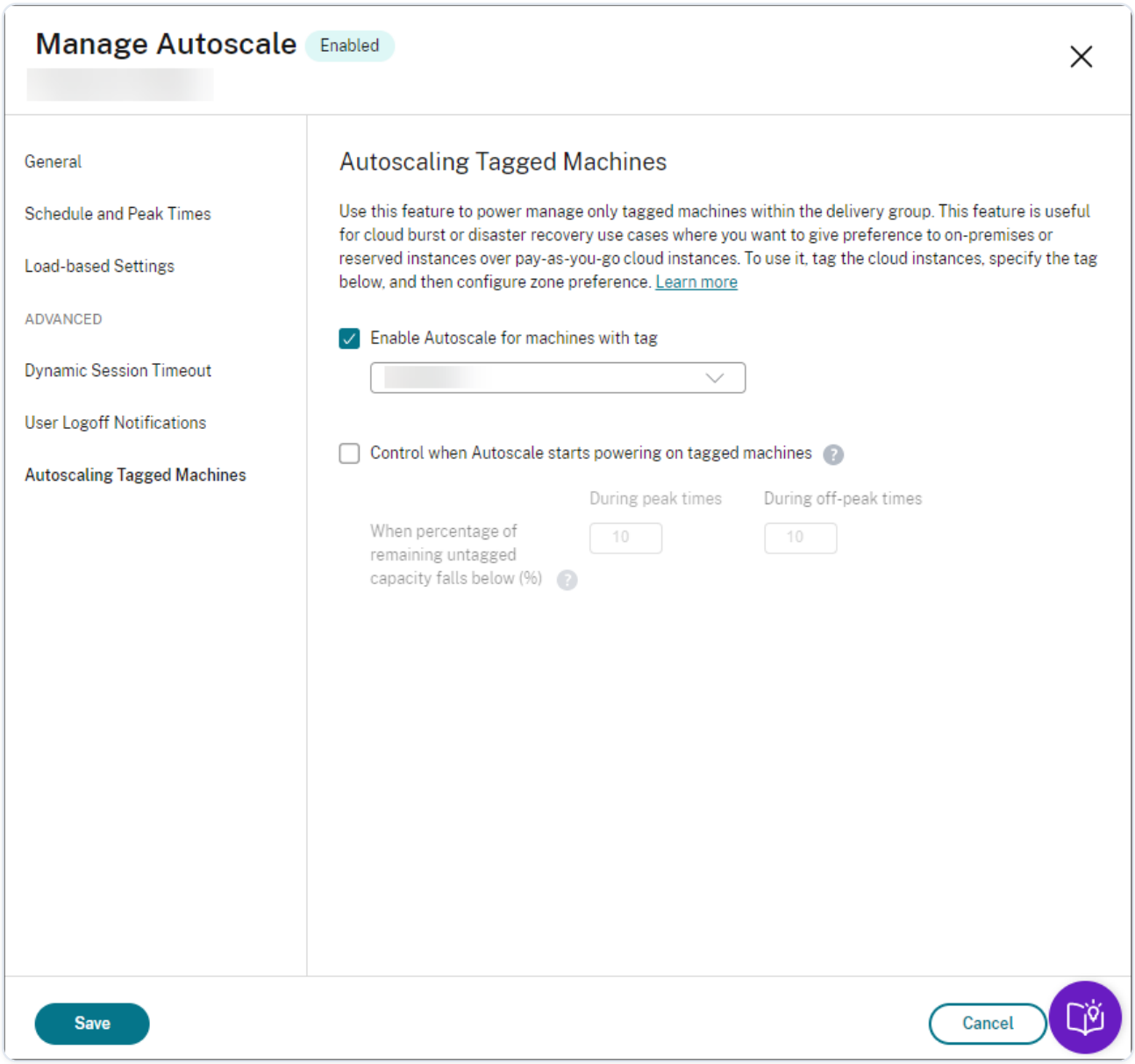
- **タグ付きマシンのAutoscaleを有効にする**のチェックを外さずに、該当するマシンからタグを削除すると、**Autoscaleの管理**ウィザードを開いたときに警告が表示される場合があります。マシンからタグを削除すると、Autoscaleで指定したタグが無効になるため、Autoscaleが管理するマシンがなくなる可能性があります。この警告を解決するには、**タグ付きマシンのAutoscale**ページに移動し、無効なタグを削除して、**適用**をクリックして変更を保存します。

Autoscaleがリソースの電源をオンにするタイミングを制御する

タグ付けされていないマシンの使用状況に基づいて、Autoscaleがタグ付けされたマシンの電源をオンにし始めるタイミングを制御することもできます。これにより、タグ付けされたワークロードまたはパブリッククラウドワークロードの消費をさらに最適化できます。

これを行うには、次の手順を実行します:

1. **タグ付きマシンのAutoscale**ページで、**Autoscaleがタグ付きマシンの電源をオンにし始めるタイミングを制御する**を選択します。
2. ピーク時間とオフピーク時間の両方で到達させたいタグなしマシンの使用率を入力し、**適用**をクリックします。サポートされる値: 0〜100。



ヒント:

この割合は、Autoscaleがタグ付けされたマシンの電源をオンにし始めるタイミングを制御します。割合がしきい値（デフォルトは10%）を下回ると、Autoscaleはタグ付けされたマシンの電源をオンにし始めます。割合がしきい値を超えると、Autoscaleは電源オフモードに入ります。割合を入力する際は、次の2つのシナリオを考慮してください。

- シングルセッションOSデリバリーグループの場合: この値は、アイドル状態のタグなしマシンの総数に対する割合として定義されます。例: タグなしのシングルセッションOSマシンが10台あります。セッションなしで1台だけになった場合、Autoscaleはタグ付けされたマシンの電源をオンにし始めます。

- マルチセッションOSデリバリーグループの場合: この値は、利用可能なタグなしマシンの総容量（ロードインデックスの観点から）に対する割合として定義されます。例: タグなしのマルチセッションOSマシンが10台あります。90%の負荷になった場合、Autoscaleはタグ付けされたマシンの電源をオンにし始めます。

PowerShellを使用して特定のタグ付けされたマシンを自動スケーリングする

注:

`Get-BrokerMachine` PowerShellコマンドは非推奨です。代わりに`Get-BrokerMachineV2`を使用してください。

PowerShell SDKを直接使用するには、次の手順を完了してください。

1. **タグを作成します。** New-Brokertag PowerShellコマンドを使用してタグを作成します。
   - 例: `$managed = New-BrokerTag Managed`。この場合、タグは「Managed」と名付けられています。New-Brokertag PowerShellコマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/>`を参照してください。
2. **マシンにタグを適用します。** Get-Brokermachine PowerShellコマンドを使用して、Autoscaleで電源管理するカタログ内のマシンにタグを適用します。
   - 例: `Get-BrokerMachine -CatalogName "cloud" | Add-BrokerTag $managed.Name`。この場合、カタログは「cloud」と名付けられています。
   - Get-Brokermachine PowerShellコマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/>`を参照してください。

   注:

   タグを適用した後で、カタログに新しいマシンを追加する場合があります。そのタグは、それらの新しいマシンには*自動的に*適用されません。

3. **Autoscaleで電源管理するデリバリーグループにタグ付けされたマシンを追加します。** Get-BrokerDesktopGroup PowerShellコマンドを使用して、マシンを含むデリバリーグループにタグ制限を追加します（つまり、「タグXを持つマシンへの起動を制限する」）。

    - 例えば: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`。この場合、デリバリーグループのUIDは1です。
    - Get-BrokerDesktopGroup PowerShellコマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>`を参照してください。

タグ制限を適用した後、後でデリバリーグループから削除したい場合があります。その場合は、Get-BrokerDesktopGroup PowerShellコマンドを使用します。

例: `Get-BrokerDesktopGroup –Uid 1 | Set-BrokerDesktopGroup –RestrictAutoscaleTagUid $null`。この場合、デリバリーグループのUIDは1です。

> **注:**
>
> タグ付けされていないマシンは、ユーザーが電源を切った後に自動的に再起動します。この動作により、ワークロードをより早く処理できるようになります。これは、`Set-BrokerDesktopGroup`の`AutomaticRestartForUntaggedMachines`プロパティを使用して、デスクトップグループごとに有効または無効にできます。詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`を参照してください。

例のシナリオ

次のシナリオを想定します。

- **マシンカタログの構成**。2つのマシンカタログ（C1とC2）があります。
    - カタログC1には、オンプレミス展開にローカルな5台のマシン（M1からM5）が含まれています。
    - カタログC2には、クラウド展開にリモートな5台のマシン（M6からM10）が含まれています。
- **タグ制限**。「Cloud」という名前のタグが作成され、カタログC2のマシンM6からM10に適用されます。

- **ゾーン構成**。2つのゾーン（Z1とZ2）が作成されます。
  - カタログC1を含むゾーンZ1は、オンプレミス展開に対応します。
  - カタログC2を含むゾーンZ2は、クラウド展開に対応します。
- **デリバリーグループの構成**
  - デリバリーグループには10台のマシン（M1～M10）が含まれており、そのうち5台はカタログC1（M1～M5）から、残りの5台はカタログC2（M6～M10）からのものです。
  - マシンM1～M5は手動で電源がオンにされ、スケジュール期間中ずっと電源がオンのままになります。
- **Autoscale構成**
  - 容量バッファは10%に設定されています。
  - Autoscaleは、「Cloud」タグが付いたマシンのみを電源管理します。この場合、Autoscaleはクラウドマシン M6からM10を電源管理します。
- **公開アプリケーションまたはデスクトップの構成**。公開デスクトップ（例）にはゾーン設定が構成されており、ユーザーの起動要求に対してゾーンZ2よりもゾーンZ1が優先されます。
  - ゾーンZ1は、公開デスクトップの優先ゾーン（ホームゾーン）として構成されています。

このシナリオは、次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. 利用可能なすべてのオンプレミス マシンが消費されるまで、ユーザーセッションはさらに増加します。
4. さらに多くのユーザーセッションが開始されます。
5. セッション終了により、ユーザーセッションが減少します。
6. セッション負荷がオンプレミス マシンのみで処理されるまで、ユーザーセッションはさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期状態）
  - オンプレミス環境のマシンM1からM5はすべて電源がオンになっています。

    - クラウド内のマシン1台（例：M6）は電源がオンになっています。このマシンは、構成された容量バッファのために電源がオンになっています。この場合、10（マシン数）x 10,000（負荷インデックス）x 10%（構成された容量バッファ）は10,000に等しくなります。したがって、マシン1台が電源オンになります。
    - 電源がオンになっているすべてのマシン（M1からM6）の負荷インデックス値は、ベースライン負荷（負荷インデックスは0）です。

- ユーザーがログオンします
    - セッションは、構成されたゾーン優先度を通じてマシンM1からM5でホストされるように指示され、これらのオンプレミス環境のマシン間で負荷分散されます。
    - 電源がオンになっているマシン（M1からM5）の負荷インデックス値が増加します。
    - 電源がオンになっているマシンM6の負荷インデックス値は、ベースライン負荷です。
- ユーザーが負荷を増やし、すべてのオンプレミスリソースを消費します
    - セッションは、構成されたゾーン優先度を通じてマシンM1からM5でホストされるように指示され、これらのオンプレミス環境のマシン間で負荷分散されます。
    - 電源がオンになっているすべてのマシン（M1からM5）の負荷インデックス値は10,000に達しました。
    - 電源がオンになっているマシンM6の負荷インデックス値は、ベースライン負荷のままです。
- もう1人のユーザーがログオンします
    - セッションはゾーン優先度を超過し、クラウドマシンM6でホストされるように指示されます。
    - 起動中のすべてのマシン (M1～M5) のロードインデックス値が10,000に達しました。
    - 起動中のマシンM6のロードインデックス値が増加し、ベースライン負荷ではなくなります。総予備容量がロードインデックスに関して10,000を下回るレベルに低下すると、構成された容量バッファのため、Autoscaleは需要を満たすために追加のマシン (M7) の電源をオンにし始めます。マシンM7の電源をオンにするには時間がかかる場合があることに注意してください。そのため、マシンM7が準備できるまでに遅延が発生する可能性があります。
- さらに多くのユーザーがログオンします
    - セッションはマシンM6でホストされるように指示されます。
    - 起動中のすべてのマシン (M1～M5) のロードインデックス値が10,000に達しました。

    - 起動中のマシンM6のロードインデックス値はさらに増加しますが、総予備容量はロードインデックスに関して10,000を上回るレベルです。
    - 起動中のマシンM7のロードインデックス値はベースライン負荷のままです。
- さらに多くのユーザーがログオンします
    - マシンM7の準備ができた後、セッションはマシンM6とM7でホストされるように指示され、これらのマシン間で負荷分散されます。
    - 起動中のすべてのマシン (M1～M5) のロードインデックス値が10,000に達しました。
    - マシンM7のロードインデックス値はベースライン負荷ではなくなります。
    - 起動中のマシン (M6とM7) のロードインデックス値が増加します。
    - 総予備容量は、ロードインデックスに関してまだ10,000を上回るレベルです。
- セッション終了のためユーザーセッション負荷が減少します
    - ユーザーがセッションからログオフした後、またはアイドルセッションがタイムアウトした後、マシンM1からM7で解放された容量は、他のユーザーによって開始されたセッションをホストするために再利用されます。
    - 負荷インデックスの観点から総予備容量が10,000を超えるレベルに増加すると、Autoscaleはクラウドマシン（M6からM7）の1つをドレイン状態にします。その結果、新しい変更（例えば、ユーザー負荷が再び増加したり、他のクラウドマシンが最も負荷が低くなったりする）が発生しない限り、他のユーザーによって開始されたセッションはそのマシン（例えばM7）に転送されなくなります。
- 1つ以上のクラウドマシンが不要になるまで、ユーザーセッションの負荷はさらに減少します。
    - マシンM7上のすべてのセッションが終了し、指定された電源オフ遅延時間が経過すると、AutoscaleはマシンM7の電源をオフにします。
    - 電源がオンになっているすべてのマシン（M1からM5）の負荷インデックス値は、10,000を下回るレベルに低下する可能性があります。
    - 電源がオンになっているマシン（M6）の負荷インデックス値は減少します。
- クラウドマシンが不要になるまで、ユーザーセッションはさらに減少します。
    - マシンM6にユーザーセッションがない場合でも、Autoscaleはそれを予備容量として予約しているため、電源をオフにしません。

- Autoscaleは、構成された容量バッファのため、残りのクラウドマシンM6の電源をオンのままにします。そのマシンは、着信するユーザーにデスクトップを提供するのを待機しています。
- オンプレミス環境のマシンに利用可能な容量がある限り、セッションはマシンM6でホストされるようには転送されません。

Autoscale™ プラグイン

Autoscale プラグインは、VM の電源管理に直接アクションを実行できるプラグインモデルです。VM の電源管理に関連する標準の Autoscale 設定から逸脱し、さまざまなシナリオで異なる設定を持つことができます。現在、使用できるプラグインは次のとおりです。

- Autoscale ホリデープラグイン
- インテリジェント Autoscale スケジュールプラグイン

Autoscale ホリデープラグイン

Autoscale ホリデープラグインを使用して、休日ごとに異なる設定を処理できます。たとえば、平日にはほとんどの VM を電源オンにしたいとします。ただし、デフォルトでは（プラグインなしでは）、祝日にも平日のスケジュールが適用されます。このシナリオを処理するために、プラグインを使用すると、指定された休日に VM の電源をオフにできます。

Studio を使用してカスタムの休日スケジュールを作成する

Studio を使用してカスタムスケジュールを作成し、休日などの特定の日にデリバリーグループ内の未使用の VM の電源をオフにして、不要なリソース消費を削減します。

> **注:**
>
> - カスタムスケジュールは作成の翌日から有効になります。
> - タグ付けされたマシンの場合、この機能はデリバリーグループ内のタグ付けされたマシンにのみ適用されます。

カスタムスケジュールを作成するには:

1. Studio で、**デリバリーグループ**に移動します。デリバリーグループを右クリックし、**Autoscale の管理**を選択します。
2. **全般**ページで、**Autoscale を有効にする**を選択します。

3. **スケジュール**ページで、**スケジュールを作成**をクリックします。
4. スケジュールの名前を入力します。
5. デリバリーグループ内の VM を電源オフにする日付を1つまたは複数選択します。

   このスケジュールを他のデリバリーグループで使用するためのテンプレートとして保存する場合は、**Save as template** をクリックします。
6. カスタムスケジュールを作成するには、**完了**をクリックします。

   これで、**スケジュール**ページの**カスタム**の下に作成されたカスタムスケジュールが表示されるはずです。

カスタムスケジュールを編集するには:

1. 編集したいスケジュールについて、**アクション**の下にある鉛筆アイコンをクリックします。次の編集が可能です:
   - カスタムスケジュールを無効にする: **有効**トグルボタンをオフにします。
   - テンプレートを変更または適用します。
   - スケジュールの名前を変更します。
   - スケジュールの日付を変更します。
2. 変更を適用するには、**完了**をクリックします。

カスタムスケジュールを削除することもできます。

> **注:**
>
> デリバリーグループを削除すると、そのカスタムスケジュールも削除されます。保存されたテンプレートは削除されません。

PowerShell を使用して休日の日付を構成する

Autoscale ホリデープラグインをデリバリーグループに関連付け、プラグインが設定された日付にVMの電源をオフにできるように、休日の日付を設定します。これを行うには、次のコマンドを実行します。

1. `Get-BrokerAutoscalePlugin` を実行して、ホリデープラグインのUIDを取得します。

```
(Get-BrokerAutoscalePlugin -Name
Citrix.AutoscalePlugin.HolidaySchedule).Uid
```

`HolidaySchedule` プラグインのUID値をメモします。`HolidaySchedule` プラグインのUIDが1であると仮定します。

2. プラグインを関連付けたいデリバリーグループのUIDを取得します。例:

```
$dgUid = (Get-BrokerDesktopGroup 'My Group Name').Uid
```

3. `HolidaySchedule` プラグインをデリバリーグループ `(-AutoscalePluginUid “<HolidaySchedule plugin UID>”)` に関連付け、必要な休日の日付を指定します。例:

```
New-BrokerAutoscaleGroupPlugin -Name "Company Holidays"
-DesktopGroupUid $dgUid -AutoscalePluginUid 1 -Configuration
'{"Holidays":["2024-11-28","2024-11-29","2024-12-25"]}'
```

作成された `AutoscaleGroupPlugin` (プラグインとデリバリーグループ間の関連付け) のUIDをメモします。

注:

関連付けの名前は、特定のデリバリーグループの関連付けの中で一意である必要があります。たとえば、1つのデリバリーグループに対して「Company Holidays」という名前の関連付けは1つしか存在できませんが、1つ以上の他のデリバリーグループも「Company Holidays」という名前の関連付けを持つことができます。

休日の日付を変更する

`Set-BrokerAutoscaleGroupPlugin` PowerShell コマンドを使用して、指定された休日の日付を変更し、`AutoscaleGroupPlugin` のUIDを指定できます。たとえば、`AutoscaleGroupPlugin` のUIDが2であると仮定します。

```
Set-BrokerAutoscaleGroupPlugin 2 -Configuration '{"Holidays":
["2024-11-28","2024-11-29"]}'
```

重要な考慮事項

Autoscaleホリデープラグインを使用する際は、次の点を考慮してください。

- Autoscale ホリデープラグインがアクティブな場合、すべてのVDAはオフになり、システムは容量を削減して動作しません。新しい起動要求は処理されますが、VDAの起動準備のため、ユーザーは遅延を経験する可能性があります。
- デリバリーグループにはタイムゾーンが指定されている必要があります。
- 日付形式は「yyyy-mm-dd」である必要があります。
- スケジュールの上書き（標準のAutoscale設定を上書きするもの）は、前日の22:00に1日前に生成されます。22:00以降は、翌日のスケジュールの上書きを追加、削除、または変更することはできません。
- 同じAutoscaleプラグインを複数のデリバリーグループに関連付けることができます。各デリバリーグループに対して`New-BrokerAutoscaleGroupPlugin`を実行し、そのグループに必要な休日を設定します。
- 最新の`Set-BrokerAutoscalePlugin -Configuration`コマンドは、指定された新しい休日で既存のすべての休日を上書きします。

Intelligent Autoscale スケジュールプラグイン

Intelligent Autoscaleは、最小限の管理設定でデリバリーグループのパフォーマンスターゲットを構成できる、データ駆動型のAutoscale機能です。パフォーマンスターゲット値は1から99の範囲で、この値はユーザーエクスペリエンスとコストの間の目標バランスを指定します。

- 値が低いほどコスト削減を優先します。
- 値が高いほどユーザーエクスペリエンスを優先します。

パフォーマンスターゲットは、過去の使用状況データと組み合わされて、1日の30分ごとのブロックごとに最適なバッファ容量（電源をオンにするVMの数）を計算します。したがって、毎日開始時に48の最適なバッファ容量が計算されます。

最適なバッファ容量は、利用可能なマシンを管理するために、ピーク時/オフピーク時のバッファ容量とプールサイズを置き換えます。

最適なバッファ容量を計算するために使用される過去の使用状況データは次のとおりです。

- 顧客のログオン率（1分あたりのユーザー数）
- 平均VM電源オン時間（分）
- 平均VM密度（VMあたりのユーザー数）.

前提条件

Intelligent Autoscaleを有効にするための要件は次のとおりです。

- デリバリーグループは共有デリバリーグループである必要があります。
- デリバリーグループは Autoscale が有効になっている必要があります。
- デスクトップグループにインテリジェント Autoscale を構成する前に、デリバリーグループには少なくとも90日分の履歴データが必要です。コマンドを使用して、`ConnectionLogLifetimeHours` を48時間から90日に増やすことができます。

```
Set-BrokerServiceConfigurationData Logging.ConnectionLogLifetimeHours
-SettingValue 2160.
```

重要な考慮事項

- デリバリーグループにはタイムゾーンが指定されている必要があります。
- スケジュールの上書きは、前日の22:00に1日前に生成されます。22:00以降は、翌日のスケジュールの上書きを追加、削除、または変更することはできません。
- 同じ Autoscale プラグインを複数のデリバリーグループに関連付けることができます。各デリバリーグループに対して `New-BrokerAutoscaleGroupPlugin` を実行し、そのグループに必要なパフォーマンスターゲットを構成します。
- 最新の `Set-BrokerAutoscalePlugin -Configuration` コマンドは、既存のすべての休日を、指定された新しい休日で上書きします。

パフォーマンスターゲットの構成

`IntelligentAutoscaleSchedules` プラグインをデリバリーグループに関連付け、パフォーマンスターゲットを構成します。これにより、パフォーマンスターゲットと履歴使用量データを組み合わせて、1日の30分ごとのブロックに最適なバッファ容量を計算できます。これを実現するには、次のコマンドを実行します。

1. `Get-BrokerAutoscalePlugi` を実行して、Intelligent Autoscale プラグインの UID を取得します。`IntelligentAutoscaleSchedules` プラグインの UID 値をメモします。

   ```
   (Get-BrokerAutoscalePlugin -Name
   Citrix.AutoscalePlugin.IntelligentAutoscaleSchedules).Uid
   ```

   `IntelligentAutoscaleSchedules`プラグインのUIDが2であると仮定します。
2. プラグインを関連付けたいデリバリーグループのUIDを取得します。例:

   ```
   $dgUid = (Get-BrokerDesktopGroup 'My Group Name').Uid
   ```

3. `IntelligentAutoscaleSchedules`プラグインをデリバリーグループ(`-AutoscalePluginUid “<IntelligentAutoscaleSchedules value>”`)に関連付け、パフォーマンスターゲット値を指定します。

```
New-BrokerAutoscaleGroupPlugin -DesktopGroupUid $dgUid
-AutoscalePluginUid 2 -Configuration '{"PerformanceTarget":70}'
```

4. 作成された`AutoscaleGroupPlugin`のUIDをメモします (プラグインとデリバリーグループ間の関連付け)。

パフォーマンスターゲット値の更新

`Set-BrokerAutoscaleGroupPlugin` PowerShellコマンドを使用し、`AutoscaleGroupPlugin`のUIDを指定することで、指定されたパフォーマンスターゲット値を更新できます。例えば、AutoscaleGroupPluginのUIDが2であると仮定します。

```
Set-BrokerAutoscaleGroupPlugin 2 -Configuration '{"PerformanceTarget":70}'
```

Autoscaleグループプラグインの自動承認を構成する

スケジュールの上書き (標準のAutoscale設定を上書きする) を許可するには、`BrokerAutoscaleGroupPlugin`で以下の2つのプロパティを構成します。

- `AutoApprove`
  - `True`の場合: プラグインによって生成されたスケジュールの上書きが自動的に承認されることを示します。
  - `False`の場合: スケジュールは、ターゲット日付がApprovedUntilプロパティで指定された日付以前である場合にのみ承認されます。

  `AutoApprove`が`False`で、`ApprovedUntil`の日付が設定されていないか、過去のものである場合、生成されたスケジュールの上書きは使用されずに破棄されます。
- `ApprovedUntil`:
  - `AutoApprove`が`False`で、`ApprovedUntil`の日付を指定した場合、プラグインによって生成されたスケジュールの上書きは、ターゲット日付のスケジュールとして自動的に承認されます。

例えば、`AutoscaleGroupPlugin`のUIDが2であると仮定します。

- そのデスクトップグループの自動承認を有効にするには:

```
Set-BrokerAutoscaleGroupPlugin 2 -AutoApprove $true
```

- 将来の特定の日付まで自動承認を有効にするには:

```
Set-BrokerAutoscaleGroupPlugin 2 -ApprovedUntil "2025-01-01"
```

ユーザーログオフ通知

重要:

この機能は、マルチセッションアプリベースのデリバリーグループのAutoscale™ユーザーインターフェイスでのみ利用可能です。

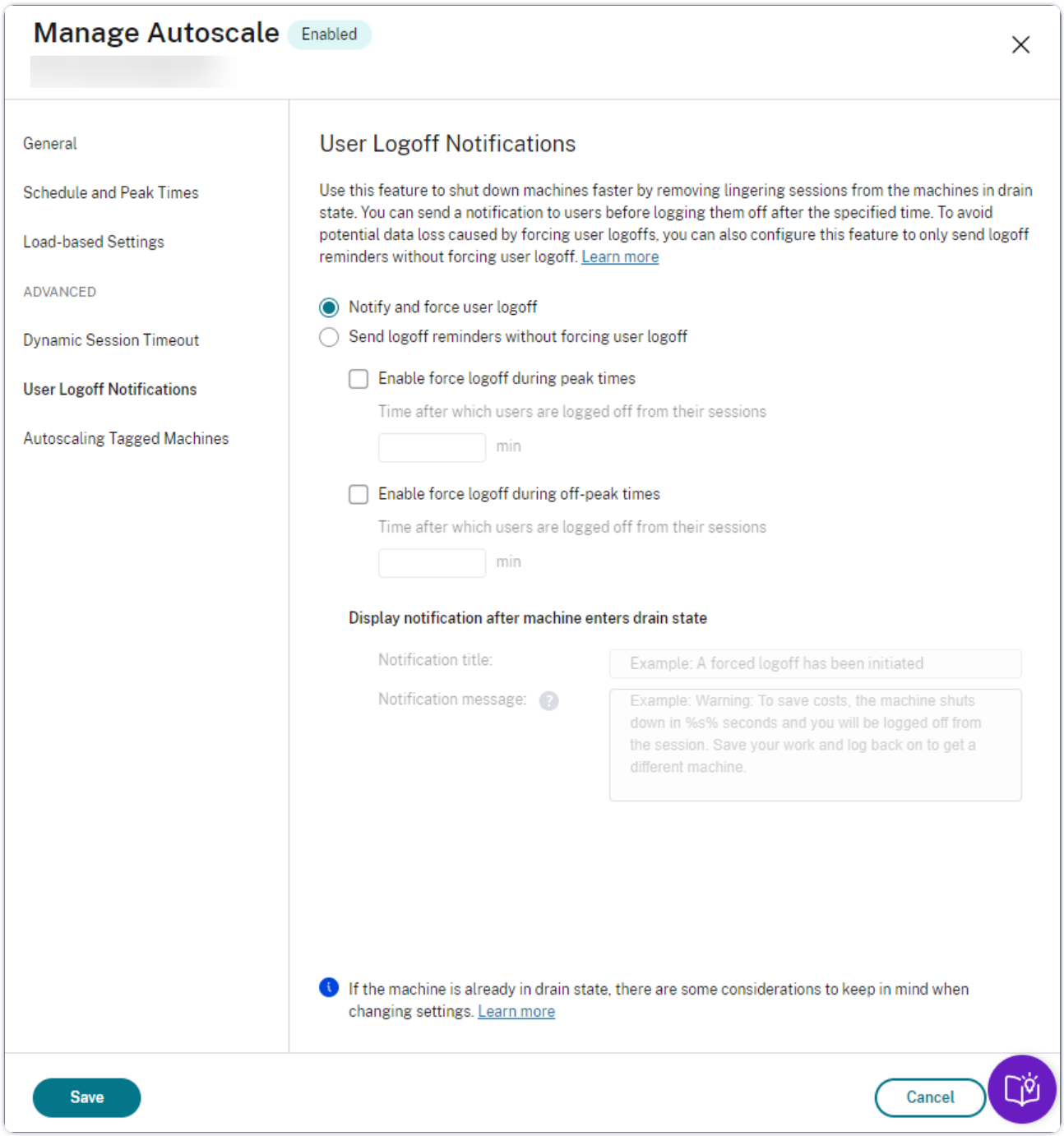
コスト削減をより効果的に実現するために、Autoscaleでは、残存セッションを強制的にログオフできます。これは、ユーザーにカスタム通知を送信し、セッションが強制的にログオフされるまでの猶予期間を指定することで行われます。これは、ドレイン状態のマシンに対してのみ行われ、すべての電源オンのマシンに対して行われるわけではありません。ユーザーの強制ログオフによって引き起こされる可能性のあるデータ損失を回避するために、この機能をユーザーの強制ログオフなしでログオフリマインダーのみを送信するように構成することもできます。

以下の2つのオプションがあります。

- **通知してユーザーを強制ログオフする**
- **ユーザーを強制ログオフせずにログオフリマインダーを送信する**

ユーザーに通知してログオフを強制する

これを選択すると、Autoscaleは、以下で指定された時間が経過した後、ユーザーをセッションからログオフします。



ピーク時の強制ログオフを有効にする。選択した場合、指定された時間が経過すると、Autoscaleはピーク時にそれらのユーザーをセッションからログオフします。

オフピーク時の強制ログオフを有効にする。選択した場合、指定された時間が経過すると、Autoscaleはオフピーク時にそれらのユーザーをセッションからログオフします。

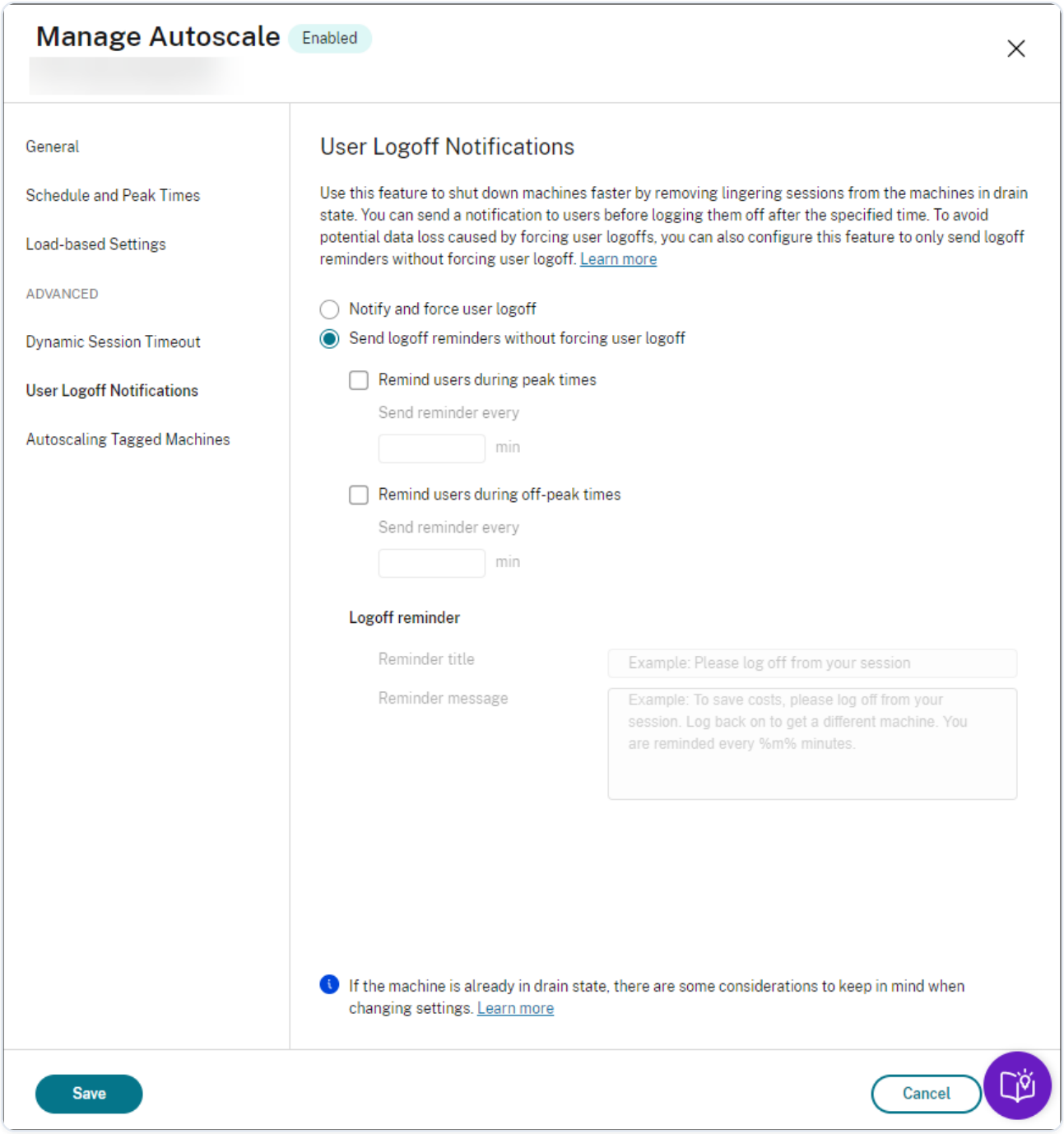
マシンがドレイン状態になった後に通知を表示する。マシンがドレイン状態になった後、ユーザーに通知を送信できます。

- **通知のタイトル。**ユーザーに送信する通知のタイトルを指定できます。例: `A forced logoff has been initiated.`.

- **通知メッセージ**。ユーザーに送信する通知の内容を指定できます。メッセージで指定された時間を示す変数として、%s% または %m% を使用できます。時間を秒で表すには %s% を使用します。時間を分で表すには %m% を使用します。例: `Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine.`.

ユーザーのログオフを強制せずにログオフリマインダーを送信する

選択すると、マシンがドレイン状態になった後、ユーザーはログオフを促すリマインダーを受け取ります。このリマインダーは、以下で指定された間隔で送信されるように構成できます。



ピーク時にユーザーにリマインダーを送信する。選択した場合、ユーザーはピーク時にX分ごとにセッションからログオフするようリマインダーを受け取ります（Xは指定された時間を示します）。

オフピーク時にユーザーにリマインダーを送信する。選択した場合、ユーザーはオフピーク時にX分ごとにセッションからログオフするようリマインダーを受け取ります（Xは指定された時間を示します）。

ログオフリマインダー。マシンがドレイン状態になった後、ユーザーに送信されるリマインダーを構成できます。

- **リマインダーのタイトル**。ユーザーに送信するリマインダーのタイトルを指定できます。例: `Please log off from your session`。
- **リマインダーメッセージ**。ユーザーに送信するメッセージを指定できます。例: `Please log off from your session and log back on to save costs`。

考慮事項

マシンがすでにドレイン状態にある場合、設定を変更する際には以下の点を考慮してください。

- 設定を**ユーザーのログオフを強制せずにログオフリマインダーを送信する**から**通知してユーザーのログオフを強制する**に変更した場合、新しい設定はすぐに有効になります。
- 設定を**通知してユーザーのログオフを強制する**から**ユーザーのログオフを強制せずにログオフリマインダーを送信する**に変更した場合、新しい設定はマシンが次にドレイン状態になるまで有効になりません。ユーザーは引き続きログオフを強制されます。

Autoscale™ 設定の有効性を分析する

この記事では、前週のマシン使用状況に基づいてAutoscale設定の有効性を分析する方法について説明します。この分析を通じて、Autoscale設定の有効性に関する以下のインサイトを得ることができます。

- 過剰プロビジョニングに起因する財務上の無駄を特定します。
- プロビジョニング不足によりユーザーエクスペリエンスがマイナスの影響を受けているかどうかを判断します。
- プロビジョニングされた容量がマシン使用状況と適切に一致していることを確認します。

この目標を達成するには、次の手順に従います。

1. Autoscaleが有効なデリバリーグループを選択します。
2. 下部のペインで、**Autoscale Insights**タブをクリックします。

次のグラフが表示され、前週のマシン使用状況データとAutoscale設定に基づいて電源がオンになるマシンの数の比較が示されます。

Autoscaleインサイト(/en-us/citrix-virtual-apps-desktops/2511/media/autoscale-insights.png)

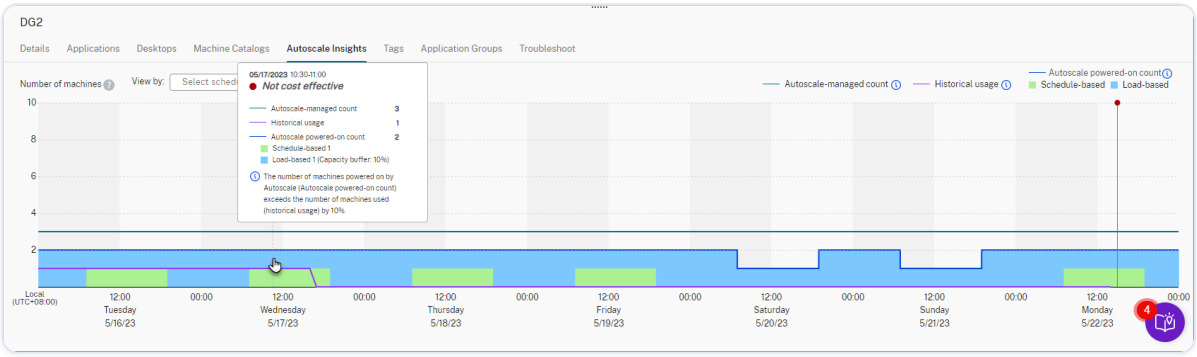
* 赤い垂直線は現在時刻を示します。

次の表は、このグラフに表示されるメトリックの説明を提供します。

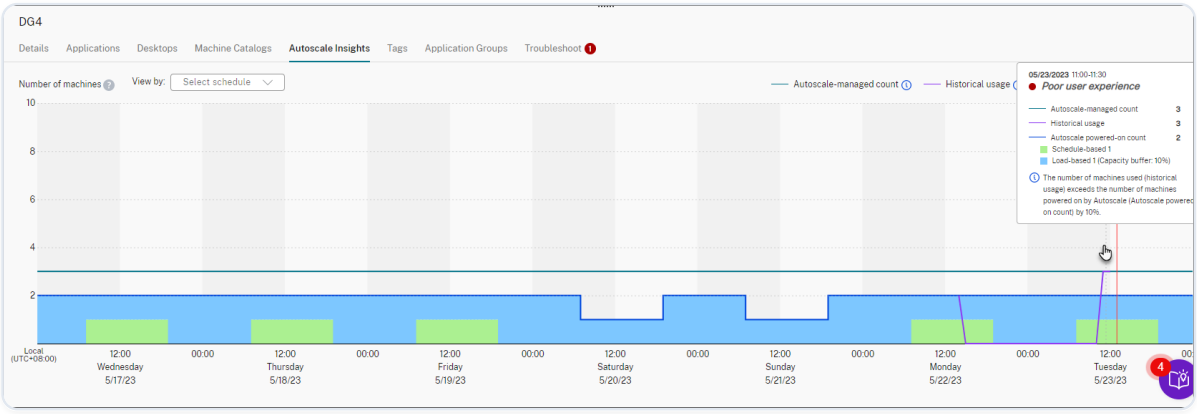
メトリック	説明
Autoscale管理対象数	Autoscaleによって管理されるマシンの総数。Autoscale管理数 = デリバリーグループ内のマシンの総数 – メンテナンスモードのマシンの数 – Autoscale用にタグ付けされていないマシンの数（タグ付けされたAutoscale機能が有効な場合）。
Autoscaleによる電源オン数	Autoscaleによって電源がオンにされたマシンの総数。Autoscaleによる電源オン数 = スケジュールベースのマシン数 + 負荷ベースのマシン数。
履歴使用状況	ユーザーに提供されたマシンの数。
スケジュールベース	Autoscaleのスケジュールベース設定に基づいて電源がオンにされるマシンの数（**注：**スケジュールベース設定は、静的シングルセッションOSタイプのデリバリーグループには適用されません）。
負荷ベース	Autoscaleの負荷ベース設定に基づいて電源がオンにされるマシンの数。

3. 特定の時間帯におけるAutoscale設定の有効性を確認するには、グラフ上のその時間帯にマウスを合わせます。比較結果と詳細なマシン数が表示された情報ボックスが表示されます。

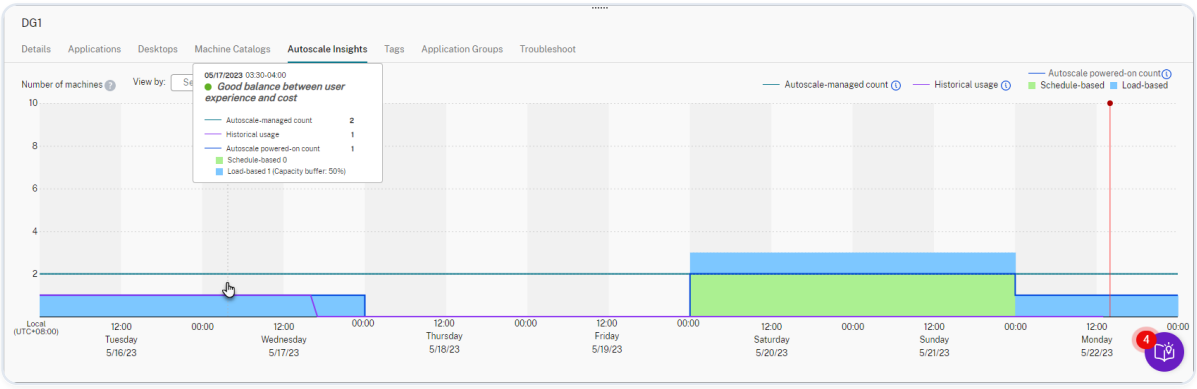
    - **費用対効果が低い**。履歴使用状況がAutoscale設定（Autoscaleによる電源オン数）の90%未満です。その結果、無駄な容量が存在する可能性があります。



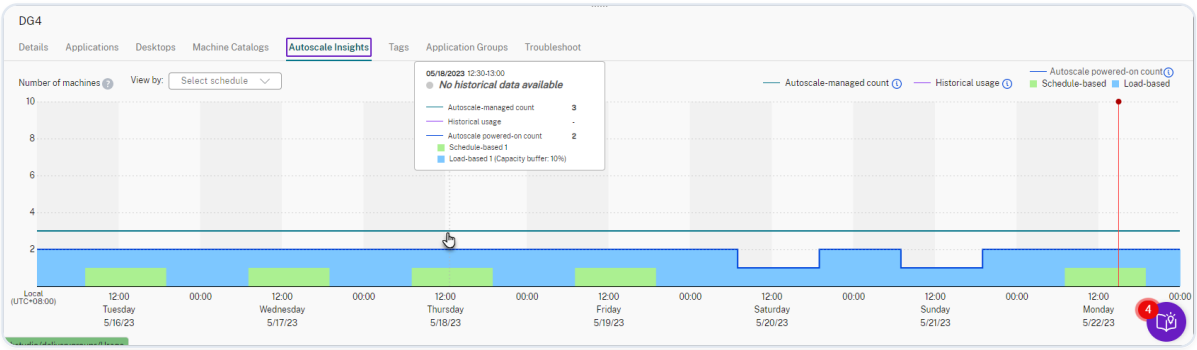
- **ユーザーエクスペリエンスが悪い。**履歴使用状況がAutoscale設定（Autoscaleによる電源オン数）の110%を超えています。その結果、ユーザーはマシンの電源がオンになるまでの待ち時間が長くなる可能性があります。



- **ユーザーエクスペリエンスとコストの良好なバランス。**履歴使用状況とAutoscale設定（Autoscaleによる電源オン数）の差が10%未満です。Autoscale設定は履歴使用状況と一致しています。



- **履歴データがありません。**履歴データがありません。考えられる原因としては、デリバリーグループでAutoscaleが有効になってから1週間未満であることなどが挙げられます。



4. Autoscaleスケジュールに基づいて日付範囲を強調表示するには、「**表示方法**」フィールドからスケジュールを選択します。
5. 分析に基づいて、Autoscale設定を調整します。詳細については、「スケジュールベースおよび負荷ベースの設定」を参照してください。

Broker PowerShell SDKコマンド

Broker PowerShell SDKを使用して、デリバリーグループのAutoscaleを構成できます。PowerShellコマンドを使用してAutoscaleを構成するには、PowerShell SDKバージョン7.21.0.12以降を使用する必要があります。PowerShell SDKの詳細については、「SDKとAPI」(/ja-jp/citrix-virtual-apps-desktops/2511/sdk-api.html)を参照してください。

Set-BrokerDesktopGroup

既存のBrokerDesktopGroupを無効または有効にするか、その設定を変更します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`を参照してください。

例

PowerShellコマンドレットの使用方法の詳細については、以下の例を参照してください。

Autoscale™を有効にする

- 名前が「MyDesktop」であるデリバリーグループに対してAutoscaleを有効にしたいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -AutoscalingEnabled $true`

容量バッファをピーク時とオフピーク時で個別に構成する

- 名前が「MyDesktop」であるデリバリーグループに対して、容量バッファをピーク時は20%、オフピーク時は10%に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:

    - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakBufferSizePercent 20 -OffPeakBufferSizePercent 10`

切断時のタイムアウト設定を構成する

- 名前が「MyDesktop」であるデリバリーグループに対して、**切断時のタイムアウト**値をピーク時は60分、オフピーク時は30分に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:

    - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakDisconnectTimeout 60 -OffPeakDisconnectTimeout 30`

ログオフ時のタイムアウト設定を構成する

- 「MyDesktop」という名前のデリバリーグループについて、ピーク時の**ログオフ時のタイムアウト**値を60分に、オフピーク時の値を30分に設定するとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:

    - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakLogOffTimeout 60 -OffPeakLogOffTimeout 30`

電源オフ遅延設定を構成する

- 「MyDesktop」という名前のデリバリーグループについて、電源オフ遅延を15分に設定するとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:

    - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PowerOffDelay 15`

電源オフ遅延が適用されない期間を構成する

- 「MyDesktop」という名前のデリバリーグループについて、30分経過するまで電源オフ遅延を適用するとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:

    - `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -SettlementPeriodBeforeAutoShutdown 30`。

マシンインスタンスコスト設定を構成する

- 「MyDesktop」という名前のデリバリーグループについて、1時間あたりのマシンインスタンスコストを0.2ドルに設定するとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:

    - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -MachineCost 0.2`

メンテナンスモードのVMをオートスケールプールから除外する

- 10台のマシンを持つデリバリーグループがあり、そのうち2台のマシンがメンテナンスモードであるとします。オートスケールのバッファ容量は50%に設定されています。メンテナンスモードのVMをオートスケールプールから除外したい場合は、`PoolSizeExcludesMaintenanceMode`を`True`に設定します。メンテナンスモードの2台のマシンはマシンプールに含まれないため、オートスケールは4台のマシンを起動します。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup -PoolSizeExcludesMaintenanceMode $true`

  シングルセッションのデリバリーグループの`PoolSizeExcludesMaintenanceMode`のデフォルト値は`False`です。

  マルチセッションのデリバリーグループの`PoolSizeExcludesMaintenanceMode`のデフォルト値は`True`です。

New-BrokerPowerTimeScheme

デリバリーグループのBrokerPowerTimeSchemeを作成します。詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/>`を参照してください。

例

UID値が3のデリバリーグループに対して電源時間スキームを作成するとします。新しいスキームは、週末、月曜日、火曜日を対象とします。午前8時から午後6時30分までの時間帯は、スキームに含まれる日のピーク時間として定義されます。ピーク時間の場合、プールサイズ（電源がオンのまま維持されるマシンの数）は20です。オフピーク時間の場合、5です。`Set-BrokerDesktopGroup` PowerShellコマンドを使用できます。例：

- `PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { 5 } else { 20 } } )`
- `PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { $false } else { $true } } )`
- `PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week' -DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48`

動的セッションタイムアウトのパラメーター

以下のBroker PowerShell SDKコマンドレットは、複数の新しいパラメーターをサポートすることで、動的セッションタイムアウトに対応するように拡張されました。

- Get-BrokerDesktopGroup
- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

これらのパラメーターには以下が含まれます。

- **DisconnectPeakIdleSessionAfterSeconds** – ピーク時にアイドル状態のセッションが切断されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、ピーク時の関連動作が無効になっていることを示します。0より大きい値は、ピーク時のみデリバリーグループの動作を有効にします。
- **DisconnectOffPeakIdleSessionAfterSeconds** - オフピーク時にアイドル状態のセッションが切断されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、オフピーク時の関連動作が無効になっていることを示します。0より大きい値は、オフピーク時のみデリバリーグループの関連動作を有効にします。
- **LogoffPeakDisconnectedSessionAfterSeconds** - ピーク時に切断されたセッションが終了されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、ピーク時の関連動作が無効になっていることを示します。0より大きい値は、ピーク時のみデリバリーグループの関連動作を有効にします。
- **LogoffOffPeakDisconnectedSessionAfterSeconds** - オフピーク時に切断されたセッションが終了されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、オフピーク時の関連動作が無効になっていることを示します。0より大きい値は、オフピーク時のみデリバリーグループの関連動作を有効にします。

例

名前が「MyDesktop」であるデリバリーグループのピーク時のアイドルセッションタイムアウトを3,600秒に設定するとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例：

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -DisconnectOffPeakIdleSessionAfterSeconds 3600`

これにより、名前が「MyDesktop」であるデスクトップグループのオフピーク時に1時間以上アイドル状態だったセッションが切断されます。

Citrix インサイトサービス

Citrix Insight Services (CIS) は、計測、テレメトリー、ビジネスインサイト生成のための Citrix プラットフォームです。その計測およびテレメトリー機能により、技術ユーザー（顧客、パート

ナー、エンジニア）は、問題を自己診断して修正し、環境を最適化できます。CIS の詳細および最新情報については、`<https://cis.citrix.com>` を参照してください（Citrix アカウントの資格情報が必要です）。

Citrixにアップロードされるすべての情報は、トラブルシューティングと診断の目的、および製品の品質、信頼性、パフォーマンスの向上のために使用されます。ただし、以下に従います。

- シトリックス インサイト サービス ポリシー (https://cis.citrix.com/legal)
- Citrixプライバシーポリシー（`<https://www.cloud.com/privacy-policy>`）

このCitrix Virtual Apps and Desktops™リリースは、以下のテクノロジーをサポートしています。

- Citrix Virtual Apps™ and Desktops のインストールおよびアップグレード分析
- Citrix カスタマーエクスペリエンス向上プログラム (CEIP)
- Citrix コールホーム
- Citrix スカウト

インストールおよびアップグレード分析

Citrix Virtual Apps and Desktops コンポーネントを展開またはアップグレードするためにフルプロダクトインストーラーを使用すると、インストールプロセスに関する匿名情報が収集され、コンポーネントをインストール/アップグレードしているマシンに保存されます。このデータは、Citrix が顧客のインストールエクスペリエンスを向上させるのに役立てられます。

この情報は、%ProgramData%\\Citrix\\CTQs の下にローカルに保存されます。

このデータの自動アップロードは、フルプロダクトインストーラーのグラフィカルインターフェイスとコマンドラインインターフェイスの両方で、デフォルトで有効になっています。

- レジストリ設定のデフォルト値を変更できます。インストール/アップグレード前にレジストリ設定を変更した場合、フルプロダクトインストーラーを使用する際にその値が使用されます。
- コマンドでオプションを指定することにより、コマンドラインインターフェイスでインストール/アップグレードする際にデフォルト設定を上書きできます。

自動アップロードの制御:

- インストール/アップグレード分析の自動アップロードを制御するレジストリ設定 (デフォルト = 1):
  - 場所: `HKLM:\Software\Citrix\MetaInstall`
  - 名前: SendExperienceMetrics

  - 値: 0 = 無効、1 = 有効

- PowerShell を使用すると、次のコマンドレットでインストール/アップグレード分析の自動アップロードが無効になります:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
SendExperienceMetrics -PropertyType DWORD -Value 0
```

- XenDesktopServerSetup.exe または XenDesktopVDASetup.exe コマンドで自動アップロードを無効にするには、`/disableexperiencemetrics` オプションを含めます。

  XenDesktopServerSetup.exe または XenDesktopVDASetup.exe コマンドで自動アップロードを有効にするには、`/sendexperiencemetrics` オプションを含めます。

Citrix カスタマーエクスペリエンス向上プログラム

Citrixカスタマーエクスペリエンス向上プログラム (CEIP) に参加すると、匿名の統計情報と使用状況情報がCitrixに送信され、Citrix製品の品質とパフォーマンスの向上に役立てられます。詳細については、https://more.citrix.com/XD-CEIP を参照してください。

サイト作成時またはアップグレード時の登録

サイトを作成すると (最初のDelivery Controller™をインストールした後)、CEIPに自動的に登録されます。最初のデータアップロードは、サイト作成後約7日で行われます。

サイト作成後、いつでも参加を停止できます。Studioの左ペインで**設定**ノードを選択し、**Citrixカスタマーエクスペリエンス向上プログラム**設定をオフにしてください。

Citrix Virtual Apps and Desktops展開をアップグレードする場合:

- CEIP をサポートしていないバージョンからアップグレードする場合、参加するかどうかを尋ねられます。
- CEIPをサポートしていたバージョンからアップグレードし、参加が有効になっていた場合、アップグレードされたサイトでCEIPが有効になります。
- CEIPをサポートしていたバージョンからアップグレードし、参加が無効になっていた場合、アップグレードされたサイトでCEIPが無効になります。
- CEIPをサポートしていたバージョンからアップグレードし、参加状況が不明な場合、参加を希望するかどうか尋ねられます。

収集された情報は匿名であるため、Citrix Insight Servicesにアップロードされた後は閲覧できません。

VDAインストール時の登録

デフォルトでは、Windows VDAをインストールすると、CEIPに自動的に登録されます。このデフォルト設定はレジストリ設定で変更できます。VDAをインストールする前にレジストリ設定を変更した場合、その値が使用されます。

CEIPへの自動登録を制御するレジストリ設定（デフォルト = 1）：

場所: HKLM: `\\Software\Citrix\Telemetry\CEIP` 名前: Enabled 値: 0 = 無効, 1 = 有効

デフォルトでは、`Enabled` プロパティはレジストリに隠されています。指定されていない場合、自動アップロード機能は有効になります。

PowerShellを使用すると、次のコマンドレットでCEIPへの登録を無効にできます。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled
-PropertyType DWORD -Value 0
```

収集されたランタイムデータポイントは、定期的にファイルとして出力フォルダー（デフォルト %programdata%/Citrix/VdaCeip）に書き込まれます。

データの初回アップロードは、VDAのインストール後約7日で行われます。

その他の製品およびコンポーネントのインストール時の登録

関連するCitrix製品、コンポーネント、テクノロジー（Citrix Provisioning™、AppDNA、Citrix License Server、Windows向けCitrix Workspace™アプリ、Universal Print Server、Session Recordingなど）をインストールする際にも、CEIPに参加できます。インストールと参加のデフォルト値の詳細については、それぞれのドキュメントを参照してください。

シトリックス Call Home

Citrix Virtual Apps and Desktopsで特定のコンポーネントや機能をインストールする際、Citrix Call Homeへの参加を求められます。Call Homeは診断データを収集し、そのデータを含むテレメトリパッケージを、分析とトラブルシューティングのためにCitrix Insight Servicesに直接（デフォルトポート443のHTTPS経由で）定期的にアップロードします。

Citrix Virtual Apps and Desktopsでは、Call HomeはCitrix Telemetry Serviceという名前のバックグラウンドサービスとして実行されます。

Call Homeのスケジュール機能はCitrix Scoutでも利用できます。詳細については、Citrix Scoutを参照してください。

収集される情報

Citrix Diagnostic Facility (CDF) トレースは、トラブルシューティングに役立つ情報をログに記録します。Call Homeは、VDA登録やアプリケーション/デスクトップの起動など、一般的な障害のトラブルシューティングに役立つCDFトレースのサブセットを収集します。このテクノロジーは、常時オンのトレース (AOT) として知られています。AOTログは、C:\ProgramData\Citrix\TelemetryService\CitrixAOTにディスクに保存されます。

> **注:**
>
> `ProgramData`フォルダーは非表示になっています。表示するには、**表示** > **表示/非表示** > **隠しファイル**をクリックします。

> Call Homeは、その他のEvent Tracing for Windows (ETW) 情報を収集せず、またそのように構成することもできません。

Call Homeは、次のようなその他の情報も収集します。

- `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`の下にCitrix Virtual Apps and Desktopsによって作成されたレジストリ。
- Citrix名前空間下のWindows Management Instrumentation (WMI) 情報。
- 実行中のプロセスの一覧。
- %PROGRAM DATA%\\Citrix\\CDFに保存されているCitrixプロセスのクラッシュダンプ。
- インストールおよびアップグレード情報。これには、製品の完全なメタインストーラーログ、失敗したMSIログ、MSIログアナライザーからの出力、StoreFront™ログ、ライセンス互換性チェックログ、およびサイトアップグレードの事前テスト結果が含まれます。

トレース情報は収集時に圧縮されます。Citrix Telemetry Service は、最大 10 MB の圧縮された最新のトレース情報を、最長 8 日間保持します。

- データを圧縮することで、Call Home は VDA 上で小さなフットプリントを維持できます。
- プロビジョニングされたマシンでの IOP を回避するため、トレースはメモリに保持されます。
- トレースバッファは、メモリ内のトレースを保持するために循環メカニズムを使用します。

Call Home は、Call Home の主要なデータポイントに記載されている主要なデータポイントを収集します。

構成と管理の概要

Call Home には、製品版インストールウィザードの使用時、または後で PowerShell コマンドレットを使用して登録できます。登録すると、既定では、診断情報が毎週日曜日の現地時間午前 3 時頃に収集され、Citrix にアップロードされます。アップロードは、指定された時刻から 2 時間の範囲でランダム化されます。つまり、既定のスケジュールを使用するアップロードは、午前 3 時から午前 5 時の間に行われます。

診断情報をスケジュールに基づいてアップロードしたくない場合（またはスケジュールを変更したい場合）は、PowerShell コマンドレットを使用して、診断情報を手動で収集してアップロードするか、ローカルに保存できます。

スケジュールされた Call Home アップロードに登録する場合、および診断情報を手動で Citrix にアップロードする場合、Citrix アカウントまたは Citrix Cloud™ の資格情報を入力します。Citrix は、資格情報をアップロードトークンと交換します。このトークンは、顧客を識別し、データをアップロードするために使用されます。資格情報は保存されません。

アップロードが発生すると、Citrix アカウントに関連付けられているアドレスに通知メールが送信されます。

コンポーネントのインストール時に Call Home を有効にした場合、後で無効にできます。

前提条件

- マシンで PowerShell 3.0 以降が実行されている必要があります。
- マシンで Citrix Telemetry Service が実行されている必要があります。
- システム変数 `PSModulePath` は、Telemetry のインストールパス (例えば、C:\\Program Files\\Citrix\\Telemetry Service\\.) に設定する必要があります。

コンポーネントのインストール中に Call Home を有効にする

VDA のインストールまたはアップグレード中: 製品版インストーラーのグラフィカルインターフェイスを使用して Virtual Delivery Agent をインストールまたはアップグレードする際に、Call Home に参加するかどうかを尋ねられます。次の 2 つのオプションがあります。

- Call Home に参加する。
- Call Home に参加しない。

VDAをアップグレードしていて、以前にCall Homeに登録していた場合、そのウィザードページは表示されません。

Controllerのインストールまたはアップグレード中: グラフィカルインターフェイスを使用してDelivery Controllerをインストールまたはアップグレードすると、Call Homeに参加するかどうかを尋ねられます。3つのオプションがあります。

Controllerをインストールする際、そのサーバーに「サービスとしてログオン」ポリシー設定が適用されたActive Directory GPOがある場合、インストールウィザードのCall Homeページで情報を構成することはできません。詳細については、CTX218094を参照してください。

Controllerをアップグレードしていて、以前にCall Homeに登録していた場合、参加について尋ねられることはありません。

PowerShellコマンドレット

PowerShellヘルプには、これらの一般的なユースケースでは使用されないコマンドレットとパラメーターの説明を含む、包括的な構文が記載されています。

アップロードにプロキシサーバーを使用するには、「プロキシサーバーの構成」を参照してください。

- **スケジュールされたアップロードを有効にする:** 診断コレクションはCitrixに自動的にアップロードされます。カスタムスケジュール用の追加のコマンドレットを入力しない場合、デフォルトのスケジュールが使用されます。

  ```
  $cred = Get-Credential

  Enable-CitrixCallHome -Credential $cred
  ```

  スケジュールされたアップロードが有効になっていることを確認するには、`Get-CitrixCallHome`と入力します。有効になっている場合、戻り値は`IsEnabled=True`と`IsMasterImage=False`です。

- **マスターイメージから作成されたマシンに対するスケジュールされたアップロードを有効にする:** マスターイメージでスケジュールされたアップロードを有効にすると、マシンカタログで作成される各マシンを構成する必要がなくなります。

  `Enable-CitrixCallHome -Credential $cred -MasterImage`

  スケジュールされたアップロードが有効になっていることを確認するには、**Get-CitrixCallHome** と入力します。有効になっている場合、戻り値は `IsEnabled=True` および `IsMasterImage=True` です。

- **カスタムスケジュールを作成する:** 診断コレクションとアップロードの毎日または毎週のスケジュールを作成します。

```
$timespan = New-TimeSpan –Hours hours -Minutes minutes

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek day
-UploadFrequency {Daily|Weekly}
```

例:

次のコマンドレットは、毎晩22:20にデータをバンドルしてアップロードするスケジュールを作成します。Hoursパラメーターは24時間形式を使用します。`UploadFrequency`パラメーターの値がDailyの場合、`DayOfWeek`パラメーターは指定されていても無視されます。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

スケジュールを確認するには、`Get-CitrixCallHomeSchedule`と入力します。上記の例では、`StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily`が返されます。

次のコマンドレットは、毎週水曜日の夜10時20分にデータをバンドルしてアップロードするスケジュールを作成します。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed
-UploadFrequency Weekly
```

スケジュールを確認するには、`Get-CitrixCallHomeSchedule`と入力します。上記の例では、`StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly`が返されます。

Call Homeを無効にする

PowerShellコマンドレットを使用するか、Citrix Scoutを介してCall Homeを無効にできます。

Call Homeのスケジュールされたアップロードが無効になっている場合でも、AOTログは収集され、ディスクに保存されます。(スケジュールされたアップロードが無効になっている場合、AOT

ログはCitrixに自動的にアップロードされません。) AOTログの収集とローカルストレージを無効にすることができます。

PowerShellでCall Homeを無効にする

次のコマンドレットを実行すると、診断データはCitrixに自動的にアップロードされません。(Citrix ScoutまたはテレメトリPowerShellコマンドレットを使用して診断データをアップロードすることは引き続き可能です。)

```
Disable-CitrixCallHome
```

Call Homeが無効になっていることを確認するには、`Get-CitrixCallHome` と入力します。無効になっている場合、戻り値は `IsEnabled=False` および `IsMasterImage=False` です。

Citrix Scoutを使用して収集スケジュールを無効にする

Citrix Scout を使用して診断収集スケジュールを無効にするには、スケジュール収集 のガイダンスに従ってください。ステップ 3 で、**オフ** をクリックして、選択したマシンのスケジュールをキャンセルします。

AOTログの収集を無効にする

次のコマンドレットを実行すると(`Enabled`フィールドを`false`に設定すると)、AOTログは収集されなくなります。

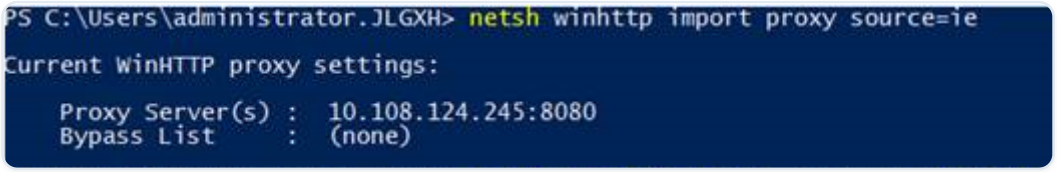
```
Enable-CitrixTrace -Listen'{"trace":{"enabled":false,"persistDirectory":"C:\Users\Public","maxSizeBytes":1000000, "sliceDurationSeconds":300}}'
```

`Listen`パラメーターには、JSON形式の引数が含まれています。

Call Homeアップロード用のプロキシサーバーを構成する

Call Home が有効になっているマシンで、次のタスクを完了します。以下の手順の例の図には、サーバーアドレスとポート 10.158.139.37:3128 が含まれています。お使いの情報とは異なります。

1. ブラウザにプロキシサーバー情報を追加します。Internet Explorer で、**インターネットオプション \> 接続 \> LAN の設定** を選択します。「**LAN にプロキシサーバーを使用する**」を選択し、プロキシサーバーのアドレスとポート番号を入力します。
2. PowerShell で `netsh winhttp import proxy source=ie` を実行します。



3. テキストエディターを使用して、C:\\Program Files\\Citrix\\Telemetry Service にある TelemetryService.exe 構成ファイルを編集します。赤いボックスに示されている情報を追加します。

   TelemetryService.exe ファイルにプロキシ情報を追加(/en-us/citrix-virtual-apps-desktops/2511/media/call-home-proxy-config.png)

4. テレメトリサービスを再起動します。

PowerShell で Call Home コマンドレットを実行します。

診断情報を手動で収集してアップロードする

CISウェブサイトを使用して、診断情報バンドルをCISにアップロードできます。PowerShellコマンドレットを使用して、診断情報を収集し、CISにアップロードすることもできます。

CISウェブサイトを使用してバンドルをアップロードするには:

1. Citrixアカウントの資格情報を使用して、Citrix Insight Servicesにログオンします。
2. を選択します。
3. を選択し、データの場所に移動します。

CISは、データアップロードを管理するいくつかのPowerShellコマンドレットをサポートしています。このドキュメントでは、2つの一般的なケースのコマンドレットについて説明します。

- `Start-CitrixCallHomeUpload` コマンドレットを使用して、診断情報バンドルを手動で収集し、CISにアップロードします。(バンドルはローカルに保存されません。)
- `Start-CitrixCallHomeUpload` コマンドレットを使用して、データを手動で収集し、診断情報バンドルをローカルに保存します。これにより、データをプレビューできます。後で、`Send-CitrixCallHomeBundle` コマンドレットを使用して、そのバンドルのコピーを手動でCISにアップロードします。(最初に保存したデータはローカルに残ります。)

PowerShellヘルプには、これらの一般的なユースケースでは使用されないコマンドレットとパラメーターの説明を含め、包括的な構文が記載されています。

CISにデータをアップロードするコマンドレットを入力すると、アップロードの確認を求められます。アップロードが完了する前にコマンドレットがタイムアウトした場合は、システムイベントログでアップロードのステータスを確認してください。サービスがすでにアップロードを実行している場合、アップロード要求は拒否される可能性があります。

データを収集し、バンドルをCISにアップロードする:

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath string]
[-Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploadHeader string] [-AppendHeaders string] [-Collect string]
[<CommonParameters>]
```

データを収集し、ローカルに保存する:

```
Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
strings] [<CommonParameters>]
```

次のパラメーターが有効です:

- **Credential:** CISへのアップロードを指示します。
- **InputPath:** バンドルに含めるzipファイルの場所。これは、Citrixサポートが要求する追加ファイルである可能性があります。.zip拡張子を含めるようにしてください。
- **OutputPath:** 診断情報が保存される場所。このパラメーターは、Call Homeデータをローカルに保存する場合に必須です。
- **Description and Incident Time:** アップロードに関する自由形式の情報。
- **SRNumber:** Citrixテクニカルサポートのインシデント番号。
- **Name:** バンドルを識別する名前。
- **UploadHeader:** CISにアップロードされるアップロードヘッダーを指定するJSON形式の文字列。
- **AppendHeaders:** CISにアップロードされる追加ヘッダーを指定するJSON形式の文字列。
- **Collect:** 収集または除外するデータを指定するJSON形式の文字列。形式は{'collector':{'enabled':Boolean}}で、Booleanはtrueまたはfalseです。 有効なコレクター値は次のとおりです。
  - WMI
  - プロセス
  - レジストリ
  - クラッシュレポート
  - トレース
  - ファイル

- MSI
- ローカルデータ
- 'サイトデータ'
- 'SFB'

デフォルトでは、「sfb」を除くすべてのコレクターが有効になっています。

「sfb」コレクターは、Skype for Businessの問題を診断するためにオンデマンドで使用されるように設計されています。「enabled」パラメーターに加えて、「sfb」コレクターはターゲットユーザーを指定するための「account」および「accounts」パラメーターをサポートしています。次のいずれかの形式を使用します。

- "-コレクト "{'sfb':{'account':'domain\\\user1'}}"
- "-コレクト "{'sfb':{'accounts':}}"

- **共通パラメーター:** PowerShellのヘルプを参照してください。

以前にローカルに保存されたデータをアップロードする:

`Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string [<CommonParameters>]`

`Path` パラメーターは、以前に保存されたバンドルの場所を指定します。

例:

次のコマンドレットは、Call Homeデータ（WMIコレクターからのデータを除く）をCISにアップロードするよう要求します。このデータは、Citrix Provisioning VDAの登録失敗に関連しており、Citrixサポートケース123456について午後2時30分に記録されました。Call Homeデータに加えて、ファイル「c:\\Diagnostics\\ExtraData.zip」がアップロードされたバンドルに組み込まれます。

```
C:\PS\>Start-CitrixCallHomeUpload -InputPath "c:
\Diagnostics\ExtraData.zip" -Description "Registration failures with
Citrix Provisioning VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name
"RegistrationFailure-021812016" -Collect "{'wmi':{'enabled':false}}"
-UploadHeader "{'key1':'value1'}" -AppendHeaders "{'key2':'value2'}"
```

次のコマンドレットは、午前8時15分に記録されたCitrixサポートケース223344に関連するCall Homeデータを保存します。データはネットワーク共有上のファイルmydata.zipに保存されます。

Call Homeデータに加えて、ファイル「c:\\Diagnostics\\ExtraData.zip」が保存されたバンドルに組み込まれます。

```
C:\PS\>Start-CitrixCallHomeUpload -OutputPath \
\mynetwork\myshare\mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip"
-Description "Diagnostics for incident number 223344" -IncidentTime "8:15"
-SRNumber 223344
```

以下のコマンドレットは、以前に保存したデータバンドルをアップロードします。

```
$cred=Get-Credential

C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \
\mynetwork\myshare\mydata.zip
```

シトリックス スカウト

はじめに

Citrix Scout は診断情報を収集し、ヘルスチェックを実行します。その結果を使用して、Citrix Virtual Apps and Desktops™ の展開を維持できます。Citrix は、Citrix Insight Services を通じて、診断情報収集の包括的で自動化された分析を提供します。また、Scout を使用して、ご自身で、または Citrix サポートのガイダンスを受けて、問題をトラブルシューティングすることもできます。

収集ファイルを Citrix にアップロードして、Citrix サポートからの分析とガイダンスを受けることができます。または、収集したファイルをローカルに保存してご自身で確認し、後でその収集ファイルを Citrix にアップロードして分析することもできます。

Scout は次の手順を提供します。

- **収集:** サイトで選択したマシンに対して、一度限りの診断情報収集を実行します。その後、ファイルを Citrix にアップロードするか、ローカルに保存することができます。
- **トレースと再現:** 選択したマシンで手動トレースを開始します。その後、それらのマシンで問題を再現します。問題を再現した後、トレースは停止されます。その後、Scout は他の診断情報を収集し、ファイルを Citrix にアップロードするか、ローカルに保存します。
- **スケジュール:** 選択したマシンで、指定した時間に毎日または毎週診断情報収集が実行されるようにスケジュールします。ファイルは自動的に Citrix にアップロードされます。
- **ヘルスチェック:** サイトとそのコンポーネントの健全性と可用性を測定するチェックを実行します。Delivery Controller、Virtual Delivery Agent (VDA)、StoreFront™ サーバー、Citrix

License Server のヘルスチェックを実行できます。チェック中に問題が検出された場合、Scout は詳細なレポートを提供します。Scout が起動するたびに、更新されたヘルスチェックスクリプトがないか確認します。新しいバージョンが利用可能な場合、Scout はそれらを自動的にダウンロードし、次回のヘルスチェック実行時に使用します。

> **注:**
>
> **トレースと再現、スケジュール、ヘルスチェック**の手順は、現在 Linux VDA では利用できません。

> この記事で説明されているグラフィカルインターフェイスは、Scout を使用する主要な方法です。あるいは、PowerShell を使用して、一度限りの診断情報収集またはスケジュールされた診断情報収集とアップロードを構成することもできます。「Call Home」(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/cis.html#citrix-call-home) を参照してください。

Scout の実行場所:

- オンプレミス展開では、Delivery Controller™ から Scout を実行して、1つ以上のVirtual Delivery Agent (VDA)、Delivery Controller、StoreFront サーバー、Federated Authentication Service (FAS) サーバー、および License Server の診断情報を取得したり、チェックを実行したりできます。また、VDA から Scout を実行してローカル診断情報を収集することもできます。

  > **注:**
  >
  > 現在、FASサーバー上のScoutでは、FAS構成の問題を診断するためのヘルスチェックはサポートされていません。

- Citrix DaaS（旧称Citrix Virtual Apps™ and Desktopsサービス）を使用するCitrix Cloud環境では、VDAからScoutを実行してローカル診断を収集します。

Scout アプリケーションのログは `C:\ProgramData\Citrix\TelemetryService\ScoutUI.log` に保存されます。このファイルはトラブルシューティングに使用できます。

収集される情報

Scoutによって収集される診断情報には、Citrix Diagnostic Facility（CDF）トレースログファイルが含まれます。Always-on Tracing（AOT）と呼ばれるCDFトレースのサブセットも含まれます。AOT情報は、VDA登録やアプリケーション/デスクトップの起動などの一般的な問題のトラブルシューティングに役立ちます。その他のEvent Tracing for Windows（ETW）情報は収集されません。

収集される情報には以下が含まれます。

- `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`の下にCitrix Virtual Apps and Desktopsによって作成されたレジストリエントリ。
- **Citrix名前空間**下のWindows Management Instrumentation (WMI) 情報。
- 実行中のプロセス。
- `%PROGRAMDATA%\Citrix\CDF`に保存されているCitrixプロセスのクラッシュダンプ。
- Citrixポリシー情報（CSV形式）。
- インストールおよびアップグレード情報。収集される情報には、製品の完全なメタインストーラーログ、失敗したMSIログ、MSIログアナライザーからの出力、StoreFrontログ、ライセンス互換性チェックログ、および予備的なサイトアップグレードテストの結果が含まれる場合があります。

トレース情報について：

- トレース情報は収集時に圧縮され、マシン上のフットプリントを小さく保ちます。
- 各マシンで、Citrix Telemetry Serviceは圧縮された最新のトレース情報を最大8日間保持します。
- Citrix Virtual Apps and Desktops 7 1808以降、AOTトレースはデフォルトでローカルディスクに保存されます。（以前のバージョンでは、トレースはメモリに保持されていました。）デフォルトパス = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`。
- Citrix Virtual Apps and Desktops 7 1811以降、ネットワーク共有に保存されたAOTトレースは、他の診断情報とともに収集されます。
- `Enable-CitrixTrace` cmdletまたは`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen`レジストリ文字列を使用して、最大サイズ（デフォルト = 10 MB）とスライス期間を変更できます。
- トレースは、ファイルが`MaxSize`の10%に達するまでファイルに追加されます。

Scoutが収集するデータポイントのリストについては、「Call Home key datapoints」を参照してください。

Scoutの構成

ScoutはLinux VDAで動作するように構成できます。Linux VDAとテレメトリの詳細については、「Citrix Telemetry Serviceとの統合」を参照してください。

Linux VDAは、`ctxtelemetry`ソケットポートまたはテレメトリサービス用のポートを自動的に変更する場合があります。その場合は、ポートを手動で構成する必要があります。

1. C:\Program Files\Citrix\Telemetry Serviceに移動します。
2. ScoutUI.exe.configファイルを開きます。
3. LinuxVDATelemetryServicePortまたはLinuxVDATelemetryWakeupPortの値を、Linux VDAで構成された値に変更します。

- `<add key="LinuxVDATelemetryServicePort" value="7502"/>`
- `<add key="LinuxVDATelemetryWakeupPort" value="7503"/>`

1. 変更を保存してファイルを閉じます。
2. 最新の構成が読み込まれていることを確認するために、Scoutを再度開きます。

ヘルスチェックについて

ヘルスチェックデータは、`C:\ProgramData\Citrix\TelemetryService\`の下のフォルダーに保存されます。

サイトのヘルスチェック

サイトヘルスチェックは、FlexCast Management Architecture (FMA) サービスの包括的な評価を提供する環境テストサービスに含まれています。これらのチェックでは、サービスの可用性を確認するだけでなく、データベース接続などの他のヘルスインジケーターも確認します。

サイトヘルスチェックはDelivery Controllerで実行されます。サイトの規模によっては、これらのチェックの完了に最大1時間かかる場合があります。

DELIVERY CONTROLLER構成チェック

サイトヘルスチェックの一環として、Delivery Controller構成チェックは、Virtual Apps and Desktopsサイトに関するCitrixの推奨事項に基づいて、以下の問題が存在するかどうかを確認します。

- 1つ以上のDelivery Controllerが失敗状態にある。
- サイトにDelivery Controllerが1つしかない。
- Delivery Controllerのバージョンが異なる。

ヘルスチェックの権限と要件を満たすことに加えて、Delivery Controller構成チェックには以下が必要です。

- 少なくとも 1 つの Controller の電源がオンになっていること。
- Controller 上で Broker Service が実行されていること。
- Controller からサイトデータベースへの接続が機能していること。

VDA の健全性チェック

VDA の健全性チェックは、一般的な VDA 登録、セッション起動、およびタイムゾーンリダイレクトの問題の考えられる原因を特定します。

VDAでの登録について、Scoutは以下をチェックします:

- VDA ソフトウェアのインストール
- VDA マシンのドメインメンバーシップ
- VDA 通信ポートの可用性
- VDA サービスステータス
- Windows ファイアウォール構成
- Controller との通信
- Controller との時刻同期
- VDA 登録ステータス

VDAでのセッション起動について、Scoutは以下をチェックします:

- セッション起動通信ポートの可用性
- セッション起動サービスのステータス
- セッション起動 Windows ファイアウォール構成
- VDA リモートデスクトップサービス クライアントアクセスライセンス
- VDA アプリケーション起動パス
- セッション起動レジストリ設定

VDA でのタイムゾーンリダイレクトについて、Scout は以下をチェックします。

- Windows ホットフィックスのインストール
- Citrix ホットフィックスのインストール
- Microsoft グループポリシー設定

- Citrix グループポリシー設定

VDA 上の Profile Management について、Scout は以下をチェックします。

- ハイパーバイザーの検出
- プロビジョニングの検出
- Citrix 仮想アプリおよびデスクトップ
- Personal vDisk の構成
- ユーザー ストア
- Profile Management Service のステータス検出
- Winlogon.exe フッキングテスト

Profile Managementでチェックを実行するには、VDAにProfile Managementをインストールして有効にする必要があります。Profile Managementの構成チェックの詳細については、Knowledge Centerの記事CTX132805を参照してください。

StoreFrontのヘルスチェック

StoreFrontのチェックでは、以下を確認します。

- Citrix Default Domain サービスが実行中であること
- Citrix Credential Wallet サービスが実行中であること
- StoreFront サーバーから Active Directory ポート 88 への接続
- StoreFrontサーバーからActive Directoryポート389への接続
- ベースURLに有効なFQDNがあること
- ベースURLから正しいIPアドレスを取得できること
- IISアプリケーションプールが.NET 4.0を使用していること
- 証明書がホストURLのSSLポートにバインドされているかどうか
- 証明書チェーンが完全であるかどうか
- 証明書の有効期限が切れているかどうか
- 証明書の有効期限が間もなく切れるかどうか（30日以内）

ライセンスサーバーのチェック

ライセンスサーバーのチェックでは、以下を確認します。

- Delivery Controller からのライセンスサーバー接続
- ライセンスサーバーのファイアウォールリモートアクセスステータス

- Citrix Licensing サービスのステータス
- ライセンスサーバーのライセンスキャッシュモードの状態
- ライセンスサーバーのポート接続
- Citrix ベンダーデーモン (CITRIX) が実行されているかどうか
- システムクロックが同期されているかどうか
- Citrix Licensing サービスがローカルサービスアカウントで実行されているかどうか
- `CITRIX.opt` ファイルの存在
- Customer Success Services の利用資格日
- Citrix ライセンスサーバーの更新
- ライセンスサーバー証明書が Delivery Controller の信頼されたルートストアにあるかどうか

ヘルスチェックの 権限と要件 を満たすことに加えて、ライセンスサーバーはドメインに参加している必要があります。そうでない場合、ライセンスサーバーは検出されません。

ヘルスチェックの実行

ヘルスチェック手順は、マシンの選択、チェックの開始、および結果レポートの確認で構成されます。

1. Scoutを起動します。マシンの**スタート**メニューから、**Citrix > Citrix Scout**を選択します。開いたページで、**Health Check**をクリックします。
2. マシンを選択します。**Find machine**をクリックしてマシンを検出します。**Select machines**ページには、サイトで検出されたすべてのVDA、Delivery Controller、およびライセンスサーバーが一覧表示されます。マシン名で表示をフィルターできます。診断情報を収集する各マシンの横にあるチェックボックスをオンにして、**Continue**をクリックします。

   その他のコンポーネントの種類（StoreFrontサーバーやVDAマシンなど）を追加するには、「Add machines manually」および「Import VDA machines」を参照してください。Citrix Provisioning™サーバーまたはライセンスサーバーを手動で追加することはできません。

   Scoutは、選択された各マシンで検証テストを自動的に起動し、検証テストに記載されている基準を満たしていることを確認します。検証に失敗した場合、**Status**列にメッセージが表示され、そのマシンのチェックボックスがオフになります。次のいずれかを実行できます。

   - 問題を解決し、そのマシンのチェックボックスを再度選択します。これにより、検証テストが再試行されます。
   - そのマシンをスキップします（チェックボックスは選択解除のままにします）。そのマシンではヘルスチェックは実行されません。

検証テストが完了したら、**続行**をクリックします。

3. 選択したマシンでヘルスチェックを実行します。概要には、テストが実行されたマシン（検証テストに合格した選択済みのマシン）が一覧表示されます。**チェック開始**をクリックします。

   チェック中およびチェック後：

   - **Status**列は、マシンの現在のチェック状態を示します。
   - 進行中のすべてのチェックを停止するには、ページ右下隅にある**Stop Checking**をクリックします。（単一のマシンのヘルスチェックをキャンセルすることはできず、選択したすべてのマシンのみをキャンセルできます。チェックが完了したマシンからの情報は保持されます。
   - 選択したすべてのマシンのチェックが完了すると、右下隅の**Stop Checking**ボタンが**Done**に変わります。
   - チェックが失敗した場合は、**Action**列の**Retry**をクリックできます。
   - チェックが完了し、問題が見つからなかった場合、**Action**列は空になります。
   - チェックで問題が見つかった場合は、**詳細の表示**をクリックして結果を表示します。
   - 選択したすべてのマシンでチェックが完了したら、**戻る**をクリックしないでください。（クリックすると、チェック結果が失われます。）

4. チェックが完了したら、**完了**をクリックしてScoutの開始ページに戻ります。

ヘルスチェックの結果

レポートを生成するCitrixチェックの場合、レポートには以下が含まれます。

- 結果レポートが生成された日時
- チェックされたマシン
- チェックが対象マシンで探した条件

権限と要件

権限:

- 診断情報を収集するには:
  - 診断情報を収集する各マシンで、ローカル管理者およびドメインユーザーである必要があります。
  - 各マシン上のLocalAppDataディレクトリに書き込む権限が必要です。
- ヘルスチェックを実行するには:

    - ドメインユーザーグループのメンバーである必要があります。
    - サイトに対して、フル管理者であるか、または読み取り専用と「**環境テストの実行**」権限を持つカスタムロールを持っている必要があります。
    - スクリプトの実行を許可するには、スクリプト実行ポリシーを少なくとも `RemoteSigned` に設定します。例: `Set-ExecutionPolicy RemoteSigned`。**注:** 他のスクリプト実行権限でも機能する場合があります。

- Scout の起動時には、**管理者として実行**を使用します。

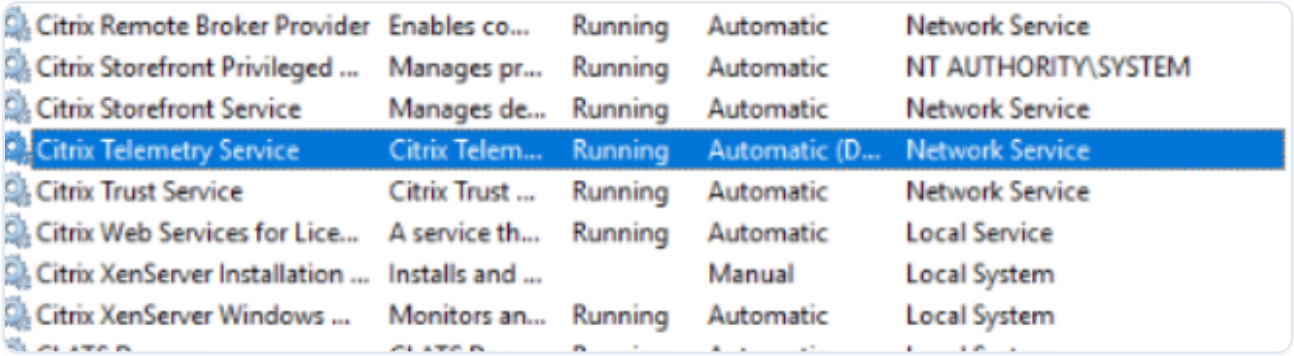
診断情報を収集したり、ヘルスチェックを実行したりする各マシンについて:

- Scout がそのマシンと通信できる必要があります。
- ファイルとプリンターの共有が有効になっている必要があります。
- PSRemoting と WinRM が有効になっている必要があります。マシンでは PowerShell 3.0 以降が実行されている必要もあります。
- Citrix Telemetry Service がマシンで実行されている必要があります。
- マシンで Windows Management Infrastructure (WMI) アクセスが有効になっている必要があります。
- 診断情報収集のスケジュールを設定するには、マシンで互換性のあるScoutバージョンが実行されている必要があります。

パス名で指定するユーザー名にドル記号 ($) を使用しないでください。診断情報の収集が妨げられます。

Scout は、選択したマシンに対して検証テストを実行し、これらの要件が満たされていることを確認します。

Windows用Telemetry Serviceは、ネットワークサービスで実行されます。



AOTトレースフォルダーは `C:\ProgramData\Citrix\TelemetryService\CitrixAOT` に保存されます。

管理者グループ、システム、およびテレメトリサービスSIDのユーザーのみが、`HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry`レジストリにアクセスする権限を持っています。

Scoutのデータ使用量2(/en-us/citrix-virtual-apps-desktops/2511/media/scout-data2.png)

テレメトリサービスをアンインストールした後も、テレメトリサービスSIDはパフォーマンスログユーザーグループに残りますが、手動で削除できます。

Scoutのデータ使用量3(/en-us/citrix-virtual-apps-desktops/2511/media/scout-data3.png)

検証テスト

診断コレクションまたはヘルスチェックが開始される前に、選択された各マシンに対して検証テストが自動的に実行されます。これらのテストは、要件が満たされていることを確認します。マシンのテストが失敗した場合、Scoutは推奨される是正措置を含むメッセージを表示します。

- **Scoutはこのマシンに到達できません** - 以下を確認してください。
  - マシンが電源オンになっていること。
  - ネットワーク接続が正常に機能していること。（これには、ファイアウォールが適切に構成されていることの確認も含まれます。）」
  - ファイルとプリンターの共有がオンになっていること。手順については、Microsoftのドキュメントを参照してください。
- **PSRemotingとWinRMを有効にする** - PowerShellリモート処理とWinRMを同時に有効にできます。**管理者として実行**を使用して、`Enable-PSRemoting`コマンドレットを実行します。詳細については、コマンドレットに関するMicrosoftのヘルプを参照してください。
- **ScoutにはPowerShell 3.0（最小）が必要です** - マシンにPowerShell 3.0（またはそれ以降）をインストールし、PowerShellリモート処理を有効にします。
- **このマシン上のLocalAppDataディレクトリにアクセスできません** - アカウントがマシン上のLocalAppDataディレクトリへの書き込み権限を持っていることを確認してください。
- **Citrix Telemetry Serviceが見つかりません** - Citrix Telemetry Serviceがマシンにインストールされ、開始されていることを確認してください。
- **スケジュールを取得できません** - マシンを（最小で）XenAppおよびXenDesktop 7.14にアップグレードしてください。
- **WMIがマシンで実行されていません** - Windows Management Instrumentation (WMI) アクセスが有効になっていることを確認してください。
- **WMI接続がブロックされています** - Windows FirewallサービスでWMIを有効にしてください。

- **Citrix Telemetry Serviceの新しいバージョンが必要です** - (バージョンは、収集とトレース＆再現の場合にのみチェックされます。) マシン上のTelemetry Serviceのバージョンをアップグレードしてください (インストールとアップグレードを参照)。サービスをアップグレードしない場合、そのマシンは**収集**または**トレース＆再現**アクションに含まれません。
- **Scoutがこのマシン上のsystemdソケットに接続できません** - 以下を確認してください。
  - ポート7503が開いています。`systemd ctxtelemetry.socket`がマシン上のポート7503でリッスンしていることを確認してください。`ctxtelemetry.socket`ポートが変更されている場合、ポートが異なる可能性があります。ポートを調整するには、Scout構成を参照してください。
  - ネットワーク接続が正常に機能していることを確認してください。(これには、ファイアウォールが適切に構成されていることの確認が含まれる場合があります。)
- **Linux VDA Telemetry Serviceがこのマシンで開始されていません** - 以下を確認してください。
  - ポート7502が開いています。Linux VDA Telemetry Serviceがマシンにインストールされ、開始されていることを確認してください。テレメトリサービスポートが変更されている場合、ポートが異なる可能性があります。ポートを調整するには、Scout構成を参照してください。
  - ネットワーク接続が正常に機能していることを確認してください。(これには、ファイアウォールが適切に構成されていることの確認が含まれる場合があります。)

バージョン互換性

このバージョンのScout (3.x) は、Citrix Virtual Apps and Desktops (または最低限XenApp and XenDesktop 7.14) のコントローラーおよびVDAで実行することを目的としています。

| 機能 | スカウト 2.23 | スカウト 3.0 | --- | --- | ---| -- | Citrix Virtual Apps and Desktops (および XenApp and XenDesktop 7.14から7.18) をサポート | はい | はい XenDesktop 5.x、7.1〜7.13をサポート | はい | いいえ XenApp 6.x、7.5〜7.13をサポート | はい | いいえ 製品に同梱 | 7.1〜7.13 | 7.14以降 CTX記事からダウンロード可能 | はい | いいえ CDFトレースをキャプチャ | はい | はい Always-on-Traces (AOT) をキャプチャ | いいえ | はい 診断データの収集を許可 | 一度に最大10台のマシン（デフォルト） | 無制限（リソースの可用性による） 診断データをCitrixに送信することを許可 | はい | はい 診断データをローカルに保存することを許可 | はい | はい Citrix Cloud™ 資格情報をサポート | いいえ | はい Citrix資格情報のサポート | はい | はい アップロード用プロキシサーバーのサポート | はい | はい スケジュールの調整 | 該当なし | はい スクリプトのサポート | コマンドライン（ローカルコントローラーのみ） | Call Homeコマンドレットを使用したPowerShell

（Telemetry Serviceがインストールされている任意のコンピューター） ヘルスチェック | いいえ | はい データマスキング | いいえ | 3.17以降

インストールとアップグレード

デフォルトでは、VDAまたはControllerをインストールまたはアップグレードすると、Citrix Telemetry Serviceの一部としてScoutが自動的にインストールまたはアップグレードされます。

VDAのインストール時にCitrix Telemetry Serviceを省略した場合、または後でサービスを削除した場合は、Citrix Virtual Apps and Desktopsのインストールメディアにある`x64\Virtual Desktop Components`または`x86\Virtual Desktop Components`フォルダーから`TelemetryServiceInstaller_xx.msi`を実行してください。

Collectまたは**Trace & Reproduce**アクションを選択すると、マシンで古いバージョンのCitrix Telemetry Serviceが実行されている場合に通知されます。Citrixでは、サポートされている最新バージョンを使用することをお勧めします。そのマシンでTelemetry Serviceをアップグレードしない場合、そのマシンは**Collect**または**Trace & Reproduce**アクションに含まれません。Telemetry Serviceをアップグレードするには、インストールと同じ手順を使用します。

アップロードの承認

診断コレクションをCitrixにアップロードする予定がある場合は、CitrixアカウントまたはCitrix Cloudアカウントが必要です。（これらは、Citrixダウンロードにアクセスしたり、Citrix Cloud Control Centerにアクセスしたりするために使用する資格情報です。）アカウントの資格情報が検証されると、トークンが発行されます。

CitrixアカウントまたはCitrix Cloudアカウントで認証する場合は、リンクをクリックして、デフォルトのブラウザーでHTTPSを使用してCitrix Cloudにアクセスします。Citrix Cloudの資格情報を入力すると、トークンが表示されます。トークンをコピーしてScoutに貼り付けます。その後、Scoutウィザードを続行できます。

トークンは、Scoutを実行しているマシンにローカルに保存されます。次回**Collect**または**Trace & Reproduce**を実行するときにそのトークンを使用できるようにするには、**Store token and skip this step in the future**チェックボックスをオンにします。

Scoutの開始ページで**Schedule**を選択するたびに、再認証する必要があります。スケジュールを作成または変更する際に、保存されたトークンを使用することはできません。

アップロードにプロキシを使用する

Citrixにコレクションをアップロードするためにプロキシサーバーを使用したい場合、Scoutにブラウザのインターネットプロパティで設定されたプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を指定することもできます。

マシンの検索

収集、トレースと再現、スケジュールの手順では、Scoutは自動的に検出したコントローラーとVDAを一覧表示します。

Delivery ControllerからScout Health Checkを実行する場合、**マシンの検索**をクリックして、デリバリーコントローラー、VDA、ライセンスサーバー、StoreFrontサーバーなどのマシンを検出します。

Delivery Controllerではないドメイン参加済みマシンからScout Health Checkを実行する場合、Scoutはマシンを自動的に検出できません。マシンを手動で追加するか、VDAマシンをインポートする必要があります。

マシンを手動で追加する

Scout が検出したコントローラーと VDA を一覧表示した後、StoreFront サーバー、ライセンスサーバー、Citrix Provisioning サーバーなど、展開内の他のマシンを手動で追加できます。

ヘルスチェックの実行時：

- ドメイン内の Citrix ライセンスサーバーは自動的に検出されます。ライセンスサーバーを手動で追加することはできません。
- ヘルスチェックは現在、Citrix Provisioning サーバーをサポートしていません。

検出されたマシンを一覧表示するScoutの任意のページで、**+ マシンの追加**をクリックします。追加するマシンのFQDNを入力し、**続行**をクリックします。必要に応じて、他のマシンを追加するために繰り返します。（FQDNの代わりにDNSエイリアスを入力しても有効に見える場合がありますが、ヘルスチェックが失敗する可能性があります。）

手動で追加されたマシンは、常に検出されたマシンよりも上の、マシンリストの先頭に表示されます。

手動で追加されたマシンを識別する簡単な方法は、行の右端にある赤い削除ボタンです。このボタンがあるのは手動で追加されたマシンのみです。検出されたマシンにはありません。

手動で追加されたマシンを削除するには、行の右端にある赤いボタンをクリックします。削除を確認します。他の手動で追加されたマシンを削除するために繰り返します。

Scout は、手動で追加されたマシンを削除するまで記憶しています。Scout を閉じてから再度開くと、手動で追加されたマシンは引き続きリストの先頭に表示されます。

StoreFront サーバーで **Trace & Reproduce** を使用する場合、CDF トレースは収集されません。ただし、その他のすべてのトレース情報は収集されます。

ヒント：

Scoutは、Citrix Virtual Apps and Desktops LTSR 2507バージョン以降のStoreFrontタイプのマシンで実行されている場合、**Collect**ページに**+ Add machine**ボタンを表示することをサポートしています。このオプションにより、ユーザーは同じクラスター内の複数のStoreFrontサーバーマシンを手動で追加し、同時に収集をトリガーできます。*TelemetryService*の古いバージョンでは、この機能はサポートされていません。

VDAマシンのインポート

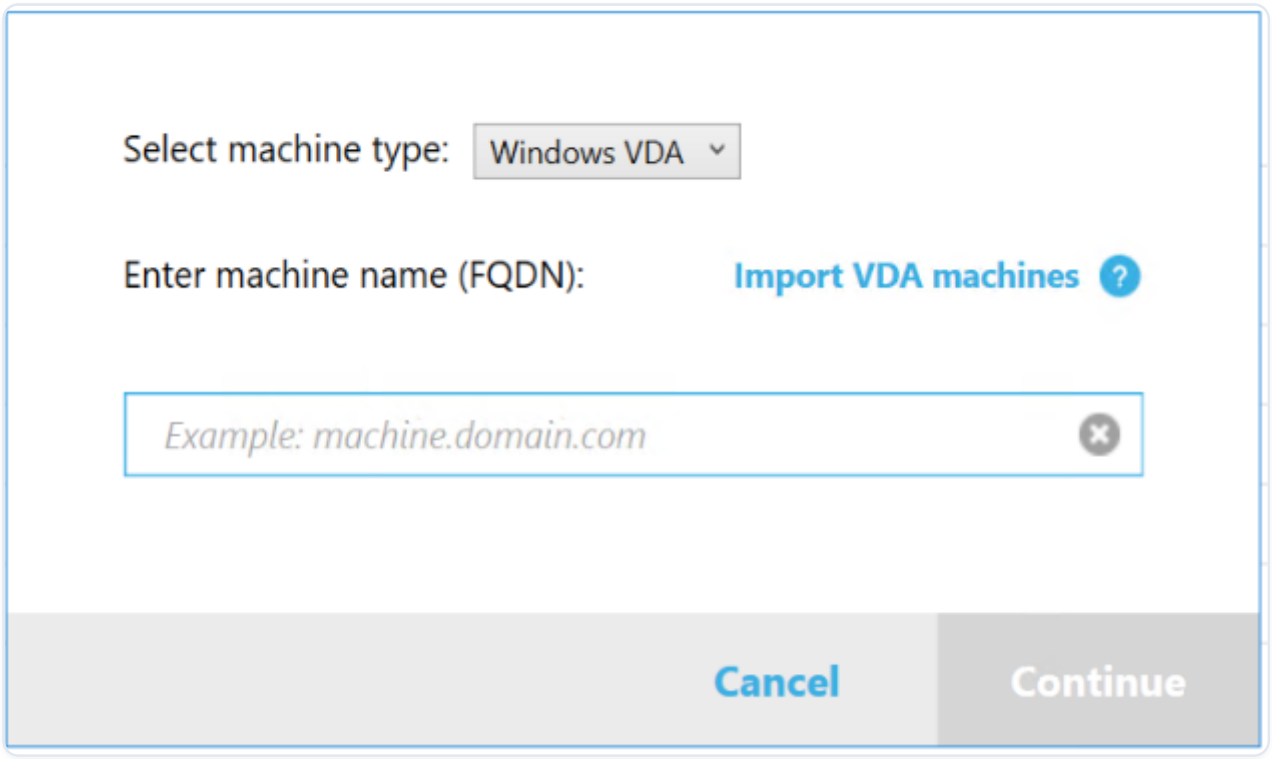
ヘルスチェックを実行する際に、展開環境でVDAマシンをインポートできます。

1. Delivery Controller または Connector で、PowerShell コマンドを使用してマシンリストファイルを生成します。Connector では、Citrix 資格情報を入力し、ポップアップダイアログで顧客を選択する必要があります。

   ```
   Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList.txt
   ```

2. machineList.txtファイルを、Scout Health Checkを起動するドメイン参加済みマシンにコピーします。
3. Scout Health Check ページで、 をクリックします。
4. マシンタイプを選択します。
5. をクリックします。
6. machineList.txt ファイルを選択します。
7. をクリックします。

インポートされた VDA マシンが Scout Health Check ページに一覧表示されます。



診断情報の収集

収集手順は、マシンを選択し、診断情報の収集を開始し、収集を含むファイルをCitrixにアップロードするか、ローカルに保存することで構成されます。

1. Scout を起動します。マシンの メニューから、 > を選択します。開いたページで、 をクリックします。
2. マシンを選択します。

   - Controllerでは、**マシンの選択**ページにサイト内のすべてのVDAとControllerが一覧表示されます。マシン名で表示をフィルタリングできます。他のマシン（StoreFrontやCitrix Provisioningサーバーなど）を手動で追加するには、マシンを手動で追加するを参照してください。
   - StoreFrontでは、**マシンの選択**ページにローカルマシンのみが一覧表示されます。同じクラスター内の他のStoreFrontマシンを追加するには、マシンを手動で追加するを参照してください。
   - その他のコンポーネント（VDAサーバーなど）では、**マシンの選択**ページにローカルマシンのみが一覧表示されます。マシンの手動追加はサポートされていません。

   診断情報を収集する各マシンの横にあるチェックボックスをオンにし、「**続行**」をクリックします。

Scoutは、選択された各マシンで検証テストを自動的に起動し、検証テストに記載されている基準を満たしていることを確認します。検証に失敗した場合、**ステータス**列にメッセージが表示され、そのマシンのチェックボックスは選択解除されます。次のいずれかを実行できます。

- 問題を解決し、そのマシンのチェックボックスを再度選択します。これにより、検証テストが再試行されます。
- そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンからは診断情報は収集されません。

検証テストが完了したら、**続行**をクリックします。

3. 診断情報を収集します。概要には、診断情報が収集されるすべてのマシン（検証テストに合格した選択済みのマシン）が一覧表示されます。**収集開始**をクリックします。

   収集中:

   - **ステータス**列には、マシンの現在の収集状態が表示されます。
   - 1台のマシンで進行中の収集を停止するには、そのマシンの**アクション**列にある**キャンセル**をクリックします。
   - 進行中のすべての収集を停止するには、ページの右下隅にある**収集の停止**をクリックします。収集が完了したマシンからの診断は保持されます。収集を再開するには、各マシンの**アクション**列にある**再試行**をクリックします。
   - 選択したすべてのマシンで収集が完了すると、右下隅にある**収集の停止**ボタンが**続行**に変わります。
   - 診断を再度収集するには、そのマシンの**アクション**列にある**再度収集**をクリックします。新しい収集は以前のものを上書きします。
   - 収集が失敗した場合は、**アクション**列にある**再試行**をクリックできます。成功した収集のみがアップロードまたは保存されます。
   - 選択したすべてのマシンで収集が完了したら、**戻る**をクリックしないでください。(クリックすると、収集は失われます。)

   収集が完了したら、**続行**をクリックします。

4. 収集を保存またはアップロードします。ファイルをCitrixにアップロードするか、ローカルマシンに保存するかを選択します。

   今すぐファイルをアップロードする場合は、手順5に進みます。

   ファイルをローカルに保存することを選択した場合:

   - Windowsの**保存**ダイアログボックスが表示されます。目的の場所に移動します。

- ローカル保存が完了すると、ファイルのパス名が表示され、リンクされます。ファイルを表示できます。後でファイルをCitrixにアップロードできます。CTX136396を参照してください。

完了をクリックしてScoutの開始ページに戻ります。この手順でこれ以上ステップを完了する必要はありません。

5. アップロードの認証を行い、必要に応じてプロキシを指定します。詳細については、(#upload-authorization)を参照してください。

   - Scoutを通じて認証していない場合は、この手順に進みます。
   - Scout経由で認証済みの場合、保存されている認証トークンがデフォルトで使用されます。これでよろしければ、このオプションを選択し、**続行**をクリックします。この収集では資格情報の入力を求められません。ステップ6に進みます。
   - 以前に認証済みであっても、再認証して新しいトークンを取得したい場合は、**変更/再認証**をクリックして、この手順に進みます。

   アップロードを認証するために、Citrix資格情報を使用するかCitrix Cloud資格情報を使用するかを選択します。**続行**をクリックします。資格情報ページは、保存されたトークンを使用していない場合にのみ表示されます。

   資格情報ページで:

   - ファイルのアップロードにプロキシサーバーを使用したい場合は、**プロキシの構成**をクリックします。Scoutに、ブラウザのインターネットプロパティ用に構成されたプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
   - Citrix Cloudアカウントの場合は、**トークンの生成**をクリックします。デフォルトのブラウザがCitrix Cloudページを起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
   - Citrixアカウントの場合は、資格情報を入力します。

   完了したら、**続行**をクリックします。

6. アップロードに関する情報を入力します。

   - 名前フィールドには、収集された診断ファイルのデフォルト名が含まれています。ほとんどの収集ではこれで十分ですが、名前を変更することもできます。(デフォルト名を削除して名前フィールドを空にした場合、デフォルト名が使用されます。)
   - オプションで、8桁のCitrixサポートケース番号を指定します。

- オプションの**説明**フィールドに、問題を説明し、該当する場合は問題が発生した時期を示します。

完了したら、**アップロードの開始**をクリックします。

アップロード中、ページの左下部分にアップロードの完了パーセンテージが概算で表示されます。進行中のアップロードをキャンセルするには、**アップロードの停止**をクリックします。

アップロードが完了すると、その場所のURLが表示され、リンクされます。リンクをたどってCitrixの場所に移動し、アップロードの分析を表示することも、リンクをコピーすることもできます。

「**完了**」をクリックして、Scoutの開始ページに戻ります。

トレースと再現

トレースと再現の手順は、マシンの選択、トレースの開始、問題の再現、診断情報の収集の完了、そしてファイルをCitrixにアップロードするかローカルに保存することから構成されます。

この手順は標準の**収集**手順に似ています。ただし、マシン上でトレースを開始し、それらのマシンで問題を再現することができます。すべての診断情報収集にはAOTトレース情報が含まれます。この手順では、トラブルシューティングに役立つCDFトレースが追加されます。

1. Scoutを起動します。マシンの「**スタート**」メニューから「**Citrix > Citrix Scout**」を選択します。開始ページで、「**トレースと再現**」をクリックします。
2. マシンを選択します。「**マシンの選択**」ページには、サイト内のすべてのVDAとControllerが一覧表示されます。マシン名で表示をフィルターできます。トレースと診断情報を収集する各マシンの横にあるチェックボックスをオンにします。次に、**続行**をクリックします。

   その他のマシンを手動で追加するには (StoreFrontまたはCitrix Provisioningサーバーなど)、マシンを手動で追加するを参照してください。

   Scoutは、選択した各マシンで検証テストを自動的に起動し、検証テストに記載されている基準を満たしていることを確認します。マシンの検証が失敗した場合、**ステータス**列にメッセージが表示され、そのマシンのチェックボックスはオフになります。次のいずれかを実行できます。

   - 問題を解決してから、そのマシンのチェックボックスを再度オンにします。これにより、検証テストが再試行されます。
   - そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンからは診断情報とトレースは収集されません。

検証テストが完了したら、**Continue** をクリックします。

3. トレースを開始します。概要には、トレースが収集されるすべてのマシンが一覧表示されます。「**トレースの開始**」をクリックします。

   選択した1つ以上のマシンで、発生した問題を再現します。その間もトレースの収集は続行されます。問題の再現が完了したら、Scoutで「**続行**」をクリックします。これによりトレースが停止します。

   トレースを停止した後、トレース中に問題を再現したかどうかを示します。

4. マシンから診断情報を収集します。「**収集の開始**」をクリックします。収集中：

   - 「**ステータス**」列は、マシンの現在の収集状態を示します。
   - 単一マシンで進行中の収集を停止するには、そのマシンの「**アクション**」列にある「**キャンセル**」をクリックします。
   - 進行中のすべての収集を停止するには、ページの右下隅にある「**収集の停止**」をクリックします。収集が完了したマシンからの診断は保持されます。収集を再開するには、各マシンの「**アクション**」列にある「**再試行**」をクリックします。
   - 選択したすべてのマシンで収集が完了すると、右下隅にある「**収集の停止**」ボタンが「**続行**」に変わります。
   - マシンから診断を再度収集するには、そのマシンの「**アクション**」列にある「**再収集**」をクリックします。新しい収集は以前のものを上書きします。
   - 収集が失敗した場合、「**アクション**」列にある「**再試行**」をクリックできます。成功した収集のみがアップロードまたは保存されます。
   - 選択したすべてのマシンで収集が完了したら、「**戻る**」をクリックしないでください。(クリックすると、収集は失われます。)

   収集が完了したら、**続行**をクリックします。

5. コレクションを保存またはアップロードします。ファイルをCitrixにアップロードするか、ローカルに保存するかを選択します。

   今すぐファイルをアップロードすることを選択した場合、手順6に進みます。

   ファイルをローカルに保存する場合:

   - Windowsの保存ダイアログボックスが表示されます。目的の場所を選択します。
   - ローカル保存が完了すると、ファイルのパス名が表示され、リンクされます。ファイルを表示できます。注意: ファイルは後でCitrixからアップロードできます。Citrix Insight Servicesについては、CTX136396を参照してください。

完了をクリックしてScoutの開始ページに戻ります。この手順でこれ以上完了する必要のある手順はありません。

6. アップロードのために認証し、必要に応じてプロキシを指定します。このプロセスの詳細については、アップロード認証を参照してください。

   - Scout経由で認証していない場合は、この手順に進んでください。
   - Scout経由で認証済みの場合、保存されている認証トークンがデフォルトで使用されます。これを実行したい場合は、このオプションを選択し、**続行**をクリックします。このコレクションの資格情報は要求されません。手順7に進んでください。
   - 以前に認証済みであっても、再認証して新しいトークンを取得したい場合は、**変更/再認証**をクリックしてこの手順に進んでください。

   アップロードを認証するために、Citrix資格情報を使用するか、Citrix Cloud資格情報を使用するかを選択します。**続行**をクリックします。資格情報ページは、保存されたトークンを使用していない場合にのみ表示されます。

   資格情報ページで:

   - ファイルのアップロードにプロキシサーバーを使用したい場合は、**プロキシの構成**をクリックします。Scoutにブラウザのインターネットプロパティで構成されているプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
   - Citrix Cloudアカウントの場合は、**トークンを生成**をクリックします。デフォルトのブラウザがCitrix Cloudページを起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
   - Citrixアカウントの場合は、資格情報を入力します。

   完了したら、**続行**をクリックします。

7. アップロードに関する情報を提供します。

   アップロードの詳細を入力します。

   - 名前フィールドには、収集された診断ファイルのデフォルト名が含まれています。ほとんどの収集ではこれで十分ですが、名前を変更することもできます。(デフォルト名を削除して名前フィールドを空のままにした場合、デフォルト名が使用されます。)
   - オプションで、8桁のCitrixサポートケース番号を指定します。
   - オプションの「説明」フィールドに、問題について説明し、該当する場合は問題が発生した時期を示します。

完了したら、**アップロードを開始**をクリックします。

アップロード中、ページの左下部分にアップロードの完了率の概算が表示されます。進行中のアップロードをキャンセルするには、「**Stop Upload**」をクリックします。

アップロードが完了すると、その場所のURLが表示され、リンクされます。リンクをたどってCitrixの場所に移動し、アップロードの分析を表示することも、リンクをコピーすることもできます。

「**Done**」をクリックしてScoutの開始ページに戻ります。

ScoutはTraceLoggingプロバイダーをサポート

以前は、ScoutはWindowsパフォーマンスプロバイダーのみをサポートしており、これには追加のデコードファイルが必要で、同じプロバイダーの単一セッションからのセッションとイベントのみをトレースしていました。

Citrix Virtual Apps and Desktopsバージョン2411以降、ScoutはTraceLoggingプロバイダーをサポートしています。このプロバイダーは追加のデコードファイルを必要とせず、同じプロバイダーに対して最大8つのトレースセッションからのイベントを有効にして受信できます。この機能はデフォルトで有効になっています。

追加のログ収集を有効にする

「**Enable additional log collection**」機能を使用すると、perfmon、Netsh、DebugView、Wiresharkなどのより多くのツールでトレースおよび再現機能を使用できます。

2407リリース以降、追加のログ収集を有効にすると、ScoutはマシンにインストールされているCDC関連ツールを自動的に検出し、CDCツール関連のトレースログをzipパッケージに自動収集します。これらのzipファイルをカスタマイズしてScoutに添付できます。この自動化により、Citrix Scoutをより効果的に使用でき、問題の迅速な診断に役立ちます。

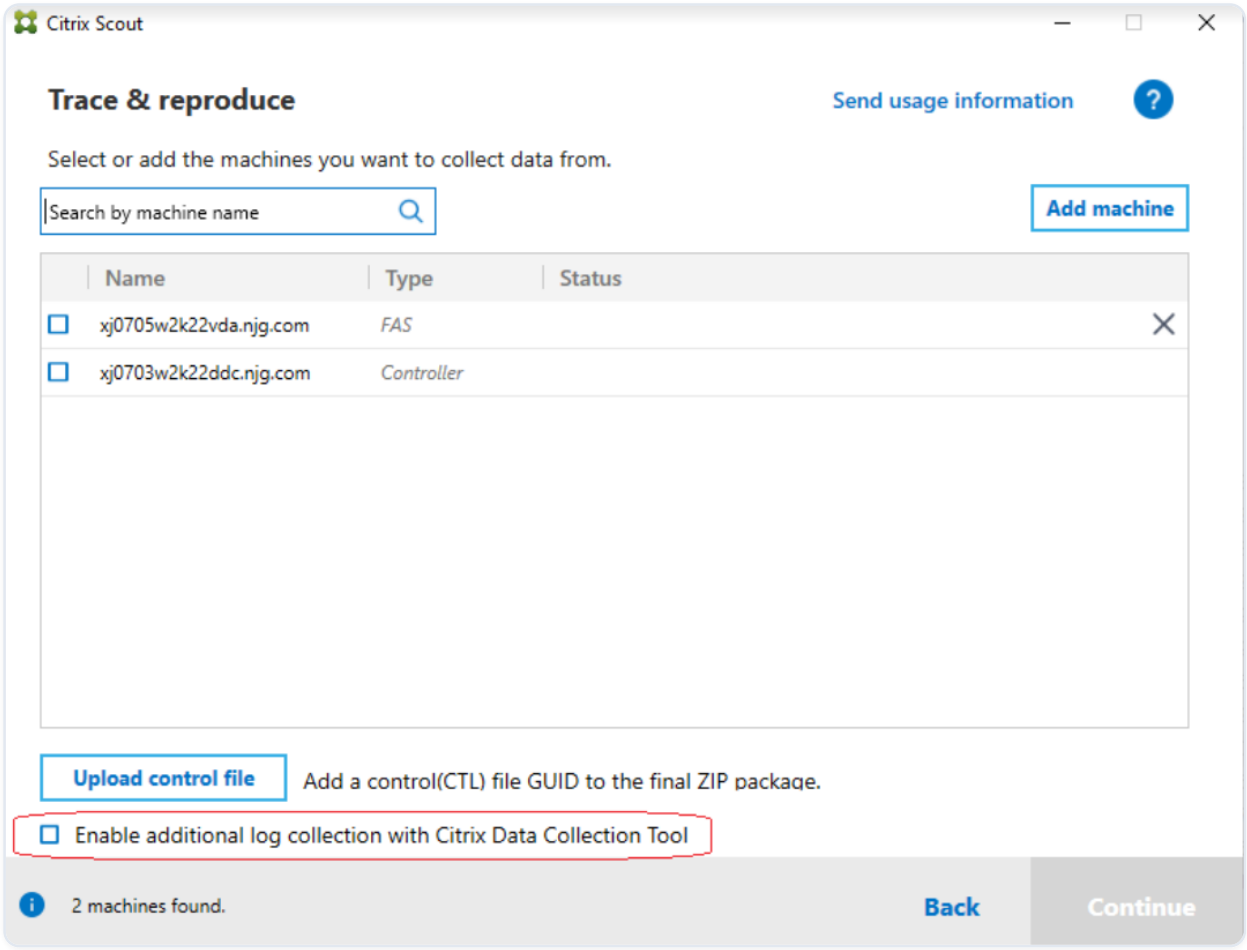
> **注:**
>
> これはローカルマシンにのみ適用されます。
>
> 追加のログ収集を有効にするには、次の必要なツールがインストールされており、指定された場所にディレクトリが手動で作成されていることを確認してください。

ツールのインストール場所:

- **Procdump**ログ: **Procdump**をダウンロードし、%ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\Procdump\procdump.exeに配置します。
- **StoreFront**ログ: **DbgView**をダウンロードし、%ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\DebugView\Dbgview.exeに配置します。
- **Procmon** ログ: **Process Monitor** をダウンロードし、%ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\ProcessMonitor\Procmon.exe に配置します。
- **Wireshark** ログ: システムに **Wireshark** を手動でインストールします。

追加のログを収集するには：

1. Scoutのホームページで、**Trace & Reproduce**をクリックします。
2. データ収集元の**Select or add machines**ページで、ローカルマシンのチェックボックスをオンにします。ステータスは*Verified*と表示されている必要があります。
3. **Enable additional log collection with Citrix Data Collection Tool**チェックボックスをオンにして、追加のログ収集を有効にします。
4. **Upload control file**ボタンをクリックして、1つのCTLファイルをロードします。このボタンを使用すると、ScoutでのAOT収集のために、AOT収集リストに追加のGUIDを追加できます。
5. 「**続行**」をクリックし、トレースと再現の手順に従います。
6. 完了後、zip ファイル内のログを確認します。ログは *CDCLogs* フォルダーに圧縮されています。



注:

トレースにProcmonツールが選択されている場合、Process Monitorログはすぐに大きくなる可能性があります。必要なツールのみを選択するようにしてください。ログのサイズは*%temp%\Scout-CDC-Log*で監視することもできます。

コレクションのスケジュール

注:

現在、コレクションをスケジュールできますが、ヘルスチェックはできません。

スケジュール プロシージャは、マシンを選択し、スケジュールを設定またはキャンセルすることで構成されます。スケジュールされたコレクションは自動的にCitrixにアップロードされ

> ます。(PowerShellインターフェースを使用して、スケジュールされたコレクションをローカルに保存できます。Citrix Call Homeを参照してください。)

1. Scoutを起動します。マシンのスタートメニューから、**Citrix > Citrix Scout**を選択します。開いたページで、**Schedule**をクリックします。
2. マシンを選択します。サイト内のすべてのVDAとコントローラーが一覧表示されます。マシン名で表示をフィルターできます。

   グラフィカルインターフェースを使用してVDAとコントローラーをインストールしたときに、Call Homeスケジュールを設定した場合（Citrix Call Homeを参照）、Scoutはデフォルトでそれらの設定を表示します。このバージョンのScoutを使用して、スケジュールされたコレクションを初めて開始したり、以前に構成したスケジュールを変更したりできます。

   コンポーネントのインストール中にマシンごとにCall Homeを有効/無効にした場合でも、Scoutで構成されたスケジュールは、選択したすべてのマシンに影響します。

   診断情報を収集する各マシンの横にあるチェックボックスをオンにして、「**続行**」をクリックします。

   その他のマシン（StoreFrontサーバーやCitrix Provisioningサーバーなど）を手動で追加するには、Add machines manuallyを参照してください。

   Scoutは、選択した各マシンで検証テストを自動的に起動し、Verification testsの基準を満たしていることを確認します。マシンの検証が失敗した場合、**Status**列にメッセージが表示され、そのマシンのチェックボックスはオフになります。次のいずれかを実行できます。

   - 問題を解決してから、マシンのチェックボックスをもう一度選択します。これにより、検証テストが再試行されます。
   - そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンからは診断（またはトレース）は収集されません。

   検証テストが完了したら、**Continue**をクリックします。

   概要ページには、スケジュールが適用されるマシンが一覧表示されます。**Continue**をクリックします。
3. スケジュールを設定します。診断情報を収集するタイミングを指定します。注意：スケジュールは、選択したすべてのマシンに影響します。

   - 選択したマシンに週次スケジュールを構成するには、**Weekly**をクリックします。曜日を選択します。収集を開始する時刻（24時間形式）を入力します。

- 選択したマシンに日次スケジュールを構成するには、**Daily**をクリックします。収集を開始する時刻（24時間形式）を入力します。
- 選択したマシンに対して既存のスケジュールをキャンセルし（別のスケジュールに置き換えない）、**オフ**をクリックします。これにより、それらのマシンに対して以前に構成されていたスケジュールがすべてキャンセルされます。

続行をクリックします。

4. アップロードの認証を行い、必要に応じてプロキシを指定します。このプロセスの詳細については、アップロード認証を参照してください。注意：Scoutスケジュールを使用している場合、保存されたトークンを使用して認証することはできません。

   アップロードを認証するために、Citrix資格情報を使用するか、Citrix Cloud資格情報を使用するかを選択します。**続行**をクリックします。

   資格情報ページで：

   - ファイルをアップロードするためにプロキシサーバーを使用したい場合は、**プロキシの構成**をクリックします。Scoutに、ブラウザのインターネットプロパティで構成されているプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
   - Citrix Cloudアカウントの場合は、**トークンを生成**をクリックします。デフォルトのブラウザがCitrix Cloudページに起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
   - Citrixアカウントの場合は、資格情報を入力します。

   完了したら、 をクリックします。

   構成されたスケジュールを確認します。**完了**をクリックしてScoutの開始ページに戻ります。

   収集中、選択された各マシンのWindowsアプリケーションログには、収集とアップロードに関するエントリが含まれます。

データマスキング

Citrix Scout を使用して収集された診断情報には、セキュリティ上機密性の高い情報が含まれる場合があります。Citrix Scout のデータマスキング機能を使用すると、診断ファイルを Citrix にアップロードする前に、機密データをマスクできます。

Scout のデータマスキングは、IP アドレス、マシン名、ドメイン名、ユーザー名、ハイパーバイザー名、デリバリーグループ名、カタログ名、アプリケーション名、および SID をマスクするように構成されています。

> **注：**
>
> CDF トレースは暗号化されており、マスクできません。
>
> Linux VDAログは`.tar.gz2`形式に圧縮されているため、マスクできません。

新しい診断情報を収集し、データマスキングを実行する

Citrix Scoutのデータマスキング機能を使用するには、コマンドラインからScoutを起動します。

1. Windowsで、コマンドプロンプトを管理者として開きます。
2. Scoutがインストールされているディレクトリに移動します: `cd C:\Program Files\Citrix\Telemetry Service`。
3. Scoutを起動します: `ScoutUI.exe datamasking`。
4. 診断情報を収集するには、**Collect**または**Trace & Reproduce**をクリックします。
5. 収集が完了したら、**Enable data masking**を選択します。このオプションはデフォルトで有効になっています。
6. データマスクを設定します。デフォルトのルールを使用することも、ルールをカスタマイズすることもできます。
7. 診断情報の収集をアップロードするか保存するかを選択します。
   - **Upload the diagnostics collection to Citrix**を選択した場合、マスクされた診断ファイルはCitrixにアップロードされます。
   - **Save the diagnostics collection on your local machine**を選択した場合、元の診断情報とマスクされた診断情報の両方が指定された場所に保存されます。

既存の診断情報に対してデータマスキングを実行する

1. Windowsで、コマンドプロンプトを管理者として開きます。
2. Scoutがインストールされているディレクトリに移動します: `cd C:\Program Files\Citrix\Telemetry Service`。
3. データマスキングモードでScoutを直接起動します: `ScoutUI.exe datamasking filePath`。
4. 続行するには「データマスキングを有効にする」を選択します。このオプションはデフォルトで有効になっています。

5. データマスクを設定します。デフォルトのルールでデータマスキングを実行することも、ルールをカスタマイズすることもできます。
6. 診断コレクションをアップロードするか保存するかを選択します。

    - **診断コレクションをCitrixにアップロード**を選択した場合、マスクされた診断ファイルはCitrixにアップロードされます。
    - **診断コレクションをローカルマシンに保存**を選択した場合、元の診断とマスクされた診断の両方が指定された場所に保存されます。

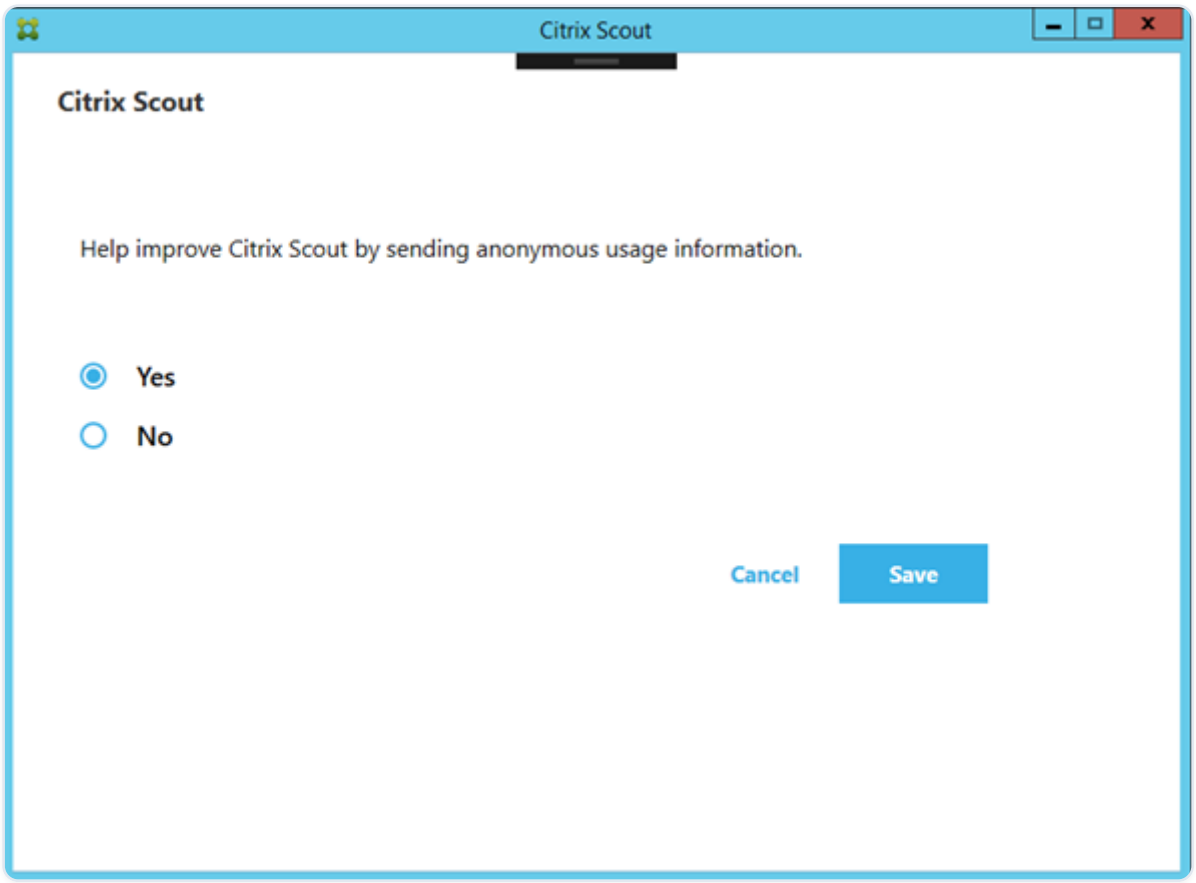
マスクされたデータファイルとマッピングファイルの場所

診断コレクションをアップロードまたは保存した後、リンクをクリックして元の診断とマスクされた診断を開き、マッピング情報ファイルを開きます。

使用状況データ収集

Scoutを使用すると、CitrixはGoogle Analyticsを使用して匿名使用状況データを収集し、将来の製品機能や改善に役立てます。データ収集はデフォルトで有効になっています。

使用状況データの収集とアップロードを変更するには、Scout UIの**設定**ギアをクリックします。その後、**はい**または**いいえ**を選択し、**保存**をクリックして情報を送信するかどうかを選択できます。



Scout 機能のコマンドラインインターフェイス

Scout 機能のコマンドラインインターフェイスを使用できるようになり、Scout UI を開かずに必要なログとデータを収集できます。この機能は、上級ユーザーがターゲットマシンまたはサイトのログまたはトレースプロセスをローカルまたはリモートで自動化するのに便利です。この機能はデフォルトで有効になっています。

以下の機能にコマンドが追加されました。

- ヘルプ
- 診断情報の収集
- トレースの開始
- トレースの停止
- 進行中のトレースセッションのリスト表示
- CDCの開始と停止

> **注:**
>
> リモートトレースセッションを実行する場合、新しいテレメトリバージョンがVDAとDDCの両方にインストールされている必要があります。ScoutコマンドラインはCitrix Virtual Apps and Desktopsバージョン2411からサポートされており、`TelemetryService`の古いバージョンはこの機能をサポートしていないため、このインストールが必要です。

次の表は、新しく追加されたコマンドについて説明しています。

ヘルプ

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe -h`	コンテキストに応じたヘルプを表示します。	`ScoutCLI.exe -h` `ScoutCLI.exe -help`

診断情報を収集するためのコマンド

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe Collect -exclude <collector>`	指定されたコレクター（Windows Management Instrumentation (WMI) プロセス、レジストリ、クラッシュレポート、ヘッダー、トレース、`msi`、`vcu`、ツールテレメトリ、ローカルデータ）からの診断を除外します。	`ScoutCLI.exe collect -exclude wmi, localdata -output "C:/Logs/mydata.zip"`
`ScoutCLI.exe Collect -output <filename>`	出力ログファイルを、`.zip` をサフィックスとして保存する場所を指定します。	
`ScoutCLI.exe Collect -fqdn <hostname>`	サイト内の指定されたマシンで診断情報を収集します。	`ScoutCLI.exe collect -fqdn hostname -exclude wmi, localdata -output "C:/Logs/mydata.zip"`

トレースの開始

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe StartTrace -guids <filename (xxx.ctl)>`	指定されたGUIDのターゲットモジュールのログを収集します。	ローカルマシンのトレース開始例 - `ScoutCLI.exe StartTrace -guids C:\Logs\provider1.ctl -output C:\Logs\xxx.etl -name session1 -level 16 -max 50`; リモートマシンのトレース開始例 - `ScoutCLI.exe StartTrace -fqdn hostname -guids C:\Logs\provider1.ctl -output C:\Logs\xxx.etl -name session1 -level 16 -max 50`
`ScoutCLI.exe StartTrace -output <filename>`	出力ログファイルをサフィックスとして.etlで保存する場所を指定します。	
`ScoutCLI.exe StartTrace -name <session name>`	トレースセッションの名前を定義します。	
`ScoutCLI.exe StartTrace -level <value>`	ターゲット診断の詳細をログに記録するログレベルを選択します。デフォルト値は16です。	

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe StartTrace -max <value>`	最大ログファイルサイズをMB単位で指定します。デフォルト値は50です。	
`ScoutCLI.exe StartTrace -fqdn <hostname>`	サイト内の指定されたマシンでトレースを開始します。	

トレースの停止

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe StopTrace -name <session name>`	指定されたトレースセッションを停止します。	`ScoutCLI.exe StopTrace -name session1`
`ScoutCLI.exe StopTrace -fqdn <hostname>`	サイト内の指定されたマシンでのトレースを停止します。リモートの `.etl` がコピーされるローカルパスを割り当てるには、-o オプションが必要です。	`ScoutCLI.exe StopTrace -fqdn hostname -name session1 -output C:\Logs\xxx.etl`
`ScoutCLI.exe StopTrace -output <filename>`	出力ログファイルを .etl をサフィックスとしてどこに保存するかを指定します。	

進行中のトレースセッションを一覧表示する

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe ListSession -name <session name>`	指定されたトレースセッションの詳細を表示します。名前が指定されていない場合は、実行中のすべてのトレースセッションの詳細を表示します。	`ScoutCLI.exe ListSession -name session1`

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe ListSession -fqdn <hostname>`	サイト内の指定されたマシンでトレースの詳細を表示します。	`ScoutCLI.exe ListSession -fqdn hostname -name session1`

CDC の開始と停止

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe StartCDC -config <filename>`	Citrix Diagnostic Collectors (CDC) ツールのパラメーターの JSON 構成ファイルを指定します。	`ScoutCLI.exe StartCDC -config xxx.json -path C:\Logs`
`ScoutCLI.exe StartCDC -path <folder>`	出力ログファイルの保存場所を指定します。	
`ScoutCLI.exe StopCDC`	CDC ツールの収集を停止します。	`ScoutCLI.exe StopCDC`

委任管理

注:

バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

委任管理モデルは、ロールベースおよびオブジェクトベースの制御を使用して、組織が管理アクティビティを委任する方法に合わせる柔軟性を提供します。委任管理はあらゆる規模の展開に対応し、展開の複雑さが増すにつれて、より詳細な権限の粒度を構成できます。委任管理では、管理者、ロール、スコープの3つの概念を使用します。

- **管理者:** 管理者は、Active Directoryアカウントによって識別される個人またはグループを表します。各管理者は、1つ以上のロールとスコープのペアに関連付けられています。

- **ロール:** ロールは職務を表し、それに関連付けられた定義済みの権限を持ちます。たとえば、Delivery Group Administratorロールには、「Delivery Groupの作成」や「Delivery Groupからのデスクトップの削除」などの権限があります。管理者はサイトに対して複数のロールを持つことができるため、ある人物がDelivery Group AdministratorとMachine Catalog Administratorの両方になることができます。ロールは組み込みまたはカスタムにすることができます。

  組み込みロールは次のとおりです。

ロール	権限
フル管理者	すべてのタスクと操作を実行できます。フル管理者は常に「すべて」のスコープと組み合わされます。
読み取り専用管理者	グローバル情報に加えて、指定されたスコープ内のすべてのオブジェクトを表示できますが、何も変更できません。たとえば、Scope=London の読み取り専用管理者は、すべてのグローバルオブジェクト（構成ログなど）とロンドンにスコープ設定されたオブジェクト（ロンドンデリバリーグループなど）を表示できます。ただし、その管理者はニューヨークスコープ内のオブジェクトを表示できません（ロンドンとニューヨークのスコープが重複しないと仮定した場合）。
ヘルプデスク管理者	デリバリーグループを表示し、それらのグループに関連付けられたセッションとマシンを管理できます。監視対象のデリバリーグループのマシンカタログとホスト情報を表示できます。また、それらのデリバリーグループ内のマシンに対して、セッション管理およびマシンの電源管理操作を実行できます。
マシンカタログ管理者	マシンカタログを作成および管理し、それらにマシンをプロビジョニングできます。仮想化インフラストラクチャ、Provisioning Services、および物理マシンからマシンカタログを構築できます。この役割は、ベースイメージの管理とソフトウェアのインストールはできますが、アプリケーションやデスク

ロール	権限
	トップをユーザーに割り当てることはできません。
デリバリーグループ管理者	アプリケーション、デスクトップ、およびマシンを配信できます。関連するセッションも管理できます。ポリシーや電源管理設定など、アプリケーションとデスクトップの構成も管理できます。
ホスト管理者	ホスト接続とそれに関連するリソース設定を管理できます。マシン、アプリケーション、またはデスクトップをユーザーに配信することはできません。
コスト管理者	Azure MCSカタログのコスト詳細を監視および表示できます。具体的には、過去30日間に発生した総コストと、現在および以前の30日間期間の比較を確認できます。

特定の製品エディションでは、組織の要件に合わせてカスタムロールを作成し、より詳細な権限を委任できます。カスタムロールを使用して、コンソール内のアクションまたはタスクの粒度で権限を割り当てることができます。

- **スコープ:** スコープはオブジェクトのコレクションを表します。スコープは、組織に関連する方法でオブジェクトをグループ化するために使用されます（たとえば、営業チームが使用するデリバリーグループのセット）。オブジェクトは複数のスコープに属することができます。オブジェクトには1つ以上のスコープがラベル付けされていると考えることができます。組み込みスコープは1つだけあり、それはすべてのオブジェクトを含む「すべて」です。フル管理者ロールは常に**すべて**スコープとペアになります。

例

XYZ社は、部門（経理、営業、倉庫）とデスクトップオペレーティングシステム（Windows 7またはWindows 8）に基づいてアプリケーションとデスクトップを管理することにしました。管理者は5つのスコープを作成し、各デリバリーグループに2つのスコープをラベル付けしました。1つは使用される部門用、もう1つは使用されるオペレーティングシステム用です。

次の管理者が作成されました。

管理者	ロール	スコープ
domain/fred	フル管理者	すべて (フル管理者ロールは常に「すべて」スコープを持ちます)
domain/rob	読み取り専用管理者	すべて
domain/heidi	読み取り専用管理者、ヘルプデスク管理者	すべての営業
domain/warehouseadmin	ヘルプデスク管理者	倉庫
domain/peter	デリバリーグループ管理者、マシンカタログ管理者	Win7

- Fredはフル管理者であり、システム内のすべてのオブジェクトを表示、編集、削除できます。
- Robはサイト内のすべてのオブジェクトを表示できますが、編集または削除はできません。
- Heidiはすべてのオブジェクトを表示でき、Salesスコープ内のデリバリーグループでヘルプデスクタスクを実行できます。これにより、彼女はそれらのグループに関連付けられたセッションとマシンを管理できますが、マシンの追加や削除など、デリバリーグループに変更を加えることはできません。
- warehouseadmin Active Directoryセキュリティグループのメンバーであれば誰でも、Warehouseスコープ内のマシンを表示し、ヘルプデスクタスクを実行できます。
- PeterはWindows 7のスペシャリストであり、すべてのWindows 7マシンカタログを管理でき、どの部門スコープに属していてもWindows 7アプリケーション、デスクトップ、およびマシンを提供できます。管理者はPeterをWin7スコープのフル管理者にすることを検討しました。しかし、フル管理者は「サイト」や「管理者」など、スコープが設定されていないすべてのオブジェクトに対しても完全な権限を持つため、彼女はこれに反対しました。

委任管理の使用方法

一般に、管理者の数とその権限の粒度は、展開の規模と複雑さによって異なります。

- 小規模な展開や概念実証の展開では、1人または数人の管理者がすべての作業を行います。委任はありません。この場合、各管理者を、すべてのスコープを持つ組み込みのフル管理者ロールで作成します。
- より多くのマシン、アプリケーション、デスクトップを持つ大規模な展開では、より多くの委任が必要です。複数の管理者が、より具体的な機能的責任（ロール）を持つ場合があります。

たとえば、2人がフル管理者で、他の管理者がヘルプデスク管理者である場合があります。また、管理者はマシンカタログなど、特定のオブジェクトグループ（スコープ）のみを管理する場合があります。この場合、新しいスコープを作成し、組み込みロールのいずれかと適切なスコープを持つ管理者を作成します。

- さらに大規模な展開では、より多くの（またはより具体的な）スコープ、および型にはまらないロールを持つ異なる管理者が必要になる場合があります。この場合、より多くのスコープを編集または作成し、カスタムロールを作成し、既存および新しいスコープに加えて、組み込みまたはカスタムロールを持つ各管理者を作成します。

柔軟性と構成の容易さのために、管理者を作成するときにスコープを作成できます。マシンカタログまたは接続を作成または編集するときにスコープを指定することもできます。

管理者の作成と管理

ローカル管理者としてサイトを作成すると、ユーザーアカウントは自動的にすべてのオブジェクトに対する完全な権限を持つフル管理者になります。サイトが作成された後、ローカル管理者には特別な権限はありません。

フル管理者ロールは常にすべてのスコープを持ちます。これは変更できません。

デフォルトでは、管理者は有効になっています。管理者を今作成しても、その人が後で管理業務を開始しない場合は、管理者を無効にする必要があるかもしれません。既存の有効な管理者については、オブジェクト/スコープを再編成している間は複数人を無効にし、更新された構成で運用を開始する準備ができたときに再度有効にしたい場合があります。有効なフル管理者がいなくなる場合、フル管理者を無効にすることはできません。管理者を作成、コピー、または編集するときに、有効/無効のチェックボックスを利用できます。

管理者をコピー、編集、または削除する際にロール/スコープのペアを削除すると、その管理者に対するロールとスコープ間の関連付けのみが削除されます。ロールまたはスコープ自体は削除されません。また、そのロール/スコープのペアで構成されている他の管理者には影響しません。

管理者を作成および管理するには、次の手順に従います。

1. Web Studioにサインインし、左側のペインで**管理者**をクリックし、次に**管理者**タブをクリックします。
2. 実行するタスクの手順に従います。

    - **管理者を作成する:** アクションバーで**管理者を作成**をクリックします。ユーザーアカウント名を入力または参照し、スコープを選択または作成し、ロールを選択します。新しい管理者は既定で有効になっています。これは変更できます。

- **管理者をコピーする:** 管理者を選択し、アクションバーで**管理者をコピー**をクリックします。ユーザーアカウント名を入力または参照します。ロール/スコープのペアを選択して編集または削除したり、新しいペアを追加したりできます。新しい管理者は既定で有効になっています。これは変更できます。
- **管理者を編集する:** 管理者を選択し、アクションバーで**管理者を編集**をクリックします。ロール/スコープのペアを編集または削除したり、新しいペアを追加したりできます。
- **管理者を削除する:** 管理者を選択し、アクションバーで**管理者を削除**をクリックします。有効なフル管理者がいなくなる場合、フル管理者を削除することはできません。

上部のペインには、作成した管理者が表示されます。管理者を選択すると、下部のペインにその詳細が表示されます。**警告**列は、管理者に関連付けられているロールとスコープのペアに、使用できないロールまたはスコープが含まれているかどうかを示します。関連付けられているロールとスコープのペアに、使用できないロールまたはスコープが含まれている場合、次の警告メッセージが表示されます。

- 関連付けられているロールまたはスコープが使用できません

> **重要:**

> 警告メッセージは、関連付けられているロールとスコープのペアに、使用できないロール、スコープ、またはその両方が含まれている場合にのみ表示されます。

> 管理者からロールとスコープのペアを削除するには、次のいずれかの手順を実行します。

- ロールとスコープのペアを削除します。
  a. アクションバーで、**管理者編集**をクリックします。
  b. **管理者名と詳細**ウィンドウで、役割とスコープのペアを選択し、**削除**をクリックします。
  c. **保存**をクリックして終了します。
- 管理者を削除します。
  a. アクションバーで、**管理者削除**をクリックします。
  b. 確認ウィンドウで、**削除**をクリックします。

役割の作成と管理

管理者が役割を作成または編集する場合、自分自身が持っている権限のみを有効にできます。これにより、管理者が現在持っている権限よりも多くの権限を持つ役割を作成し、それを自分自身に割り当てたり（または既に割り当てられている役割を編集したりする）ことを防ぎます。

役割名には最大64個のUnicode文字を含めることができます。ただし、バックスラッシュ、スラッシュ、セミコロン、コロン、ポンド記号、コンマ、アスタリスク、疑問符、等号、左右の矢印、パイプ、左右の角括弧、左右の丸括弧、引用符、アポストロフィは含めることができません。説明には最大256個のUnicode文字を含めることができます。

組み込みの役割を編集または削除することはできません。カスタム役割が管理者によって使用されている場合、その役割を削除することはできません。

> **注:**
>
> 特定の製品エディションのみがカスタム役割をサポートしています。カスタム役割をサポートするエディションのみが、アクションバーに関連エントリを持っています。

役割を作成および管理するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**管理者**をクリックし、**役割**タブをクリックします。
2. 完了したいタスクの手順に従います。

   - **役割の詳細を表示:** 役割を選択します。下部のペインに、役割のオブジェクトの種類と関連する権限が表示されます。下部のペインにある**管理者**タブをクリックすると、現在この役割を持つ管理者の一覧が表示されます。
   - **カスタム役割を作成:** アクションペインで**役割の作成**をクリックします。名前と説明を入力します。オブジェクトの種類と権限を選択します。
   - **役割をコピー:** 役割を選択し、アクションバーで**役割のコピー**をクリックします。必要に応じて、名前、説明、オブジェクトの種類、および権限を変更します。
   - **カスタム役割を編集:** 役割を選択し、アクションバーで**役割の編集**をクリックします。必要に応じて、名前、説明、オブジェクトの種類、および権限を変更します。
   - **カスタム役割を削除:** 役割を選択し、アクションバーで**役割の削除**をクリックします。プロンプトが表示されたら、削除を確定します。

スコープの作成と管理

サイトを作成するときに利用できるスコープは「すべて」スコープのみであり、これは削除できません。

次の手順でスコープを作成できます。管理者を作成するときにもスコープを作成できます。各管理者は、少なくとも1つのロールとスコープのペアに関連付けられている必要があります。デスクトップ、マシンカタログ、アプリケーション、またはホストを作成または編集するときに、それらを既存のスコープに追加できます。スコープに追加しない場合、それらは「すべて」スコープの一部として残ります。

サイトの作成はスコープ化できず、委任された管理オブジェクト（スコープと役割）もスコープ化できません。ただし、スコープ化できないオブジェクトは「すべて」スコープに含まれます。（フル管理者は常に「すべて」スコープを持ちます。）マシン、電源アクション、デスクトップ、およびセッションは直接スコープ化されません。管理者は、関連するマシンカタログまたはデリバリーグループを通じて、これらのオブジェクトに対する権限を割り当てることができます。

スコープの作成と管理に関するルール：

- スコープ名には最大64個のUnicode文字を含めることができます。スコープ名には、バックスラッシュ、スラッシュ、セミコロン、コロン、ポンド記号、コンマ、アスタリスク、疑問符、等号、左矢印、右矢印、パイプ、左右の角かっこ、左右の丸かっこ、引用符、アポストロフィを含めることはできません。
- スコープの説明には、最大256個のUnicode文字を含めることができます。
- スコープをコピーまたは編集する際、スコープからオブジェクトを削除すると、それらのオブジェクトが管理者からアクセスできなくなる可能性があることに注意してください。編集されたスコープが1つ以上の役割とペアになっている場合、スコープの更新によって役割/スコープのペアが使用できなくならないようにしてください。

スコープを作成および管理するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**管理者**をクリックしてから、**スコープ**タブをクリックします。
2. 完了したいタスクの手順に従ってください。

    - **スコープの作成:** アクションバーで**Create new Scope**をクリックします。名前と説明を入力します。特定の種類のすべてのオブジェクト（例: デリバリーグループ）を含めるには、オブジェクトの種類を選択します。特定のオブジェクトを含めるには、種類を展開してから個々のオブジェクト（例: 営業チームが使用するデリバリーグループ）を選択します。

- **スコープのコピー:** スコープを選択し、アクションバーで**Copy Scope**をクリックします。名前と説明を入力します。必要に応じて、オブジェクトの種類とオブジェクトを変更します。
- **スコープの編集:** スコープを選択し、アクションバーで**Edit Scope**をクリックします。必要に応じて、名前、説明、オブジェクトの種類、およびオブジェクトを変更します。
- **スコープの削除:** スコープを選択し、アクションバーで**Delete Scope**をクリックします。プロンプトが表示されたら、削除を確定します。

テナント管理をセットアップする

単一のCitrix Virtual Apps™ and Desktopsサイト内で管理パーティションを作成するために、テナント管理をセットアップします。各テナントには、マシンカタログやデリバリーグループなどの分離されたリソースと構成があります。特定のテナントへのアクセス権を持つ管理者は、そのテナントに関連付けられたリソースと構成のみを管理できます。使用例としては、単一サイト内に異なるビジネスサイロ（独立した部門または個別のIT管理チーム）を持つ企業が挙げられます。

大まかに言えば、テナント管理をセットアップするためのワークフローには以下が含まれます。

1. テナントを作成する
2. テナントの管理者を追加する

テナントを作成する

テナントスコープを作成してテナントを作成します。詳細な手順は次のとおりです。

1. Web Studioにサインインし、左ペインで**Administrators**をクリックし、**Scopes**タブをクリックします。
2. *Create Scope** をクリックして、テナントの作成を開始します。
3. テナントスコープの以下の詳細を入力します。
    a. スコープのわかりやすい名前を入力します。この名前はテナントの識別子としても機能します。
    b. （オプション）簡単な説明を入力します。
    c. **テナントスコープ**を選択します。
    d. 必要に応じて、テナントに関連付けられているオブジェクトを選択します。オブジェクトの作成時または管理時に、テナントスコープにオブジェクトを追加することもできます。
    e. **OK**をクリックして作成を完了します。

完了後、以下を確認できます。

- 新しいテナントスコープレコードがスコープリストに表示され、**種類**列で**テナント**として識別されます。
- スコープ名は、Web Studioの右上隅にある**すべてのテナント**ドロップダウンリストに表示されます。

テナントスコープを操作する際は、次の考慮事項に留意してください。

- テナントプロパティは、ホスティング > マシンカタログ > デリバリーグループ > アプリケーションという階層的な割り当て順序に従います。下位レベルのオブジェクトは、上位レベルのオブジェクトからテナントプロパティを継承します。たとえば、テナントスコープのデリバリーグループを選択する場合は、関連するホスティングとマシンカタログも選択していることを確認してください。そうしないと、デリバリーグループはテナントのプロパティを継承できません。
- テナントスコープを作成した後、オブジェクトを変更することでテナントの割り当てを編集できます。テナントの割り当てが変更された場合でも、同じテナントまたはそれらのテナントのサブセットに割り当てる必要があるという制約が適用されます。ただし、テナントの割り当てが変更されても、下位レベルのオブジェクトは再評価されません。テナントの割り当てを変更する際は、オブジェクトが適切に制限されていることを確認してください。たとえば、マシンカタログが `TenantA` と `TenantB` で利用可能な場合、`TenantA` 用と `TenantB` 用のデリバリーグループを作成できます。(`TenantA` と `TenantB` はどちらもそのマシンカタログに関連付けられています。) その後、マシンカタログを `TenantA` のみに関連付けられるように変更できます。その結果、`TenantB` に関連付けられているデリバリーグループは無効になります。

テナントの管理者を追加する

管理者ロールとテナントを持つユーザーアカウントを割り当てることで、テナントの管理者を追加します。

テナントの管理者を追加するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**管理者**をクリックし、次に**管理者**タブをクリックします。
2. **管理者を追加**をクリックし、以下の手順に従って完了します。
    a. ユーザーアカウント名を入力または参照し、**次へ**をクリックします。
    b. **カスタムアクセス**を選択し、必要に応じて1つ以上の役割（例: マシンカタログ管理者）を選択します。
    c. 各役割の横にある**スコープの編集**をクリックし、スコープを**すべて**から目的のテナントスコープに変更して、**保存**をクリックします。

3. **次へ**をクリックします。
4. **確認と確定**ページで、**招待状を送信**をクリックします。

レポートの作成

委任管理レポートには、次の2種類を作成できます。

- 管理者に関連付けられている役割/スコープのペアと、各オブジェクトタイプ（例: デリバリーグループとマシンカタログ）の個々の権限を一覧表示するHTMLレポート。このレポートはWeb Studioから生成します。

  このレポートを作成するには、次の手順に従います。

  a. Web Studioにサインインし、左ペインで「**管理者**」をクリックします。

  b. 管理者を選択し、アクションバーで「**レポートの作成**」をクリックします。

  管理者の作成、コピー、または編集時に、このレポートを要求することもできます。
- すべての組み込み役割とカスタム役割を権限にマッピングするHTMLまたはCSVレポート。このレポートは、OutputPermissionMapping.ps1という名前のPowerShellスクリプトを実行して生成します。

  このスクリプトを実行するには、フル管理者、読み取り専用管理者、または役割を読み取る権限を持つカスタム管理者である必要があります。スクリプトは、Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scriptsにあります。

  構文：

  `OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path string] [-AdminAddress string] [-Show] [CommonParameters]`

パラメーター	説明
`-Help`	スクリプトのヘルプを表示します。
`-Csv`	CSV 出力を指定します。デフォルト = HTML
`-Path string`	出力の書き込み先。デフォルト = stdout
`-AdminAddress string`	接続先のDelivery Controller™のIPアドレスまたはホスト名。デフォルト = localhost

パラメーター	説明
`-Show`	(`-Path` パラメーターも指定されている場合にのみ有効です) 出力をファイルに書き込むと、`-Show` によって、Web ブラウザーなどの適切なプログラムで出力が開かれます。
共通パラメーター	`Verbose`、`Debug`、`ErrorAction`、`ErrorVariable`、`WarningAction`、`WarningVariable`、`OutBuffer`、および `OutVariable`。詳細については、Microsoft のドキュメントを参照してください。

次の例では、HTMLテーブルをRoles.htmlという名前のファイルに書き込み、そのテーブルをWebブラウザで開きます。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

-Path Roles.html –Show
```

次の例では、CSVテーブルをRoles.csvという名前のファイルに書き込みます。このテーブルは表示されません。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

–CSV -Path Roles.csv
```

Windowsのコマンドプロンプトから、上記の例のコマンドは次のとおりです。

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'

-CSV -Path Roles.csv"
```

デリバリーコントローラー

注：

バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

デリバリーコントローラーは、ユーザーアクセス管理、接続の仲介と最適化を担当するサーバー側コンポーネントです。コントローラーは、デスクトップおよびサーバーイメージを作成するMachine Creation Services™も提供します。

サイトには少なくとも1つのコントローラーが必要です。最初のコントローラーをインストールした後、サイトの作成時または後でコントローラーを追加できます。サイトに複数のコントローラーを配置することには、主に2つの利点があります。

- **冗長性：** ベストプラクティスとして、本番サイトでは常に異なる物理サーバー上に少なくとも2つのコントローラーを配置してください。1つのコントローラーが故障した場合でも、他のコントローラーが接続を管理し、サイトを管理できます。
- **スケーラビリティ：** サイトのアクティビティが増加すると、コントローラーのCPU使用率とデータベースのアクティビティも増加します。コントローラーを追加することで、より多くのユーザー、アプリケーション、デスクトップ要求を処理できるようになり、全体的な応答性を向上させることができます。

各コントローラーはサイトデータベースと直接通信します。複数のゾーンがあるサイトでは、すべてのゾーンのコントローラーがプライマリゾーンのサイトデータベースと通信します。

重要：

サイトが構成された後で、コントローラーのコンピューター名またはドメインメンバーシップを変更しないでください。

VDAがコントローラーに登録する方法

VDAを使用する前に、サイト内のデリバリーコントローラーに登録（通信を確立）する必要があります。VDA登録の詳細については、「コントローラーへのVDA登録」を参照してください。

コントローラーの追加、削除、または移動

コントローラーを追加、削除、または移動するには、「データベース」の記事に記載されているサーバーロールおよびデータベースロールの権限が必要です。

SQLクラスタリングまたはSQLミラーリングのインストールにおけるノードへのコントローラーのインストールはサポートされていません。

サイトにDelivery Controller™を追加する際は、高可用性のために使用するレプリカSQL Serverに、そのマシンのログオン資格情報を必ず追加してください。

展開でデータベースミラーリングを使用している場合:

- Controllerを追加、削除、または移動する前に、プリンシパルデータベースとミラーデータベースの両方が実行されていることを確認してください。さらに、SQL Server Management Studioでスクリプトを使用している場合は、スクリプトを実行する前にSQLCMDモードを有効にしてください。
- Controllerを追加、削除、または移動した後にミラーリングを確認するには、PowerShell `Get-configdbconnection` コマンドレットを実行します。このコマンドレットは、接続文字列でミラーへのフェールオーバーパートナーが設定されていることを確認します。

Controller を追加、削除、または移動した後:

- 自動更新が有効になっている場合、VDAは90分以内に更新されたControllerのリストを受け取ります。
- 自動更新が有効になっていない場合は、すべてのVDAに対してControllerポリシー設定またはListOfDDCsレジストリキーが更新されていることを確認してください。Controllerを別のサイトに移動した後は、両方のサイトでポリシー設定またはレジストリキーを更新してください。

Controller を追加する

Controllerは、サイトの作成時および後で追加できます。このソフトウェアの以前のバージョンでインストールされたControllerを、このバージョンで作成されたサイトに追加することはできません。

1. サポートされているオペレーティングシステムを含むサーバーでインストーラーを実行します。Delivery Controllerコンポーネントと、必要なその他のコアコンポーネントをインストールします。インストールウィザードを完了します。
2. まだサイトを作成していない場合は、このControllerでCitrix Site Managerを実行してサイトを作成します。このControllerのIPアドレスは、新しいサイトに自動的に追加されます。

データベースを初期化するスクリプトを生成する予定がある場合は、スクリプトを生成する前に Controller を追加してください。

3. 既にサイトを作成している場合は、次の手順に従ってください。

   a. このControllerでCitrix Site Managerを実行し、 をクリックして、参加するサイト内のControllerのアドレスを入力します。

   b. Studio構成ツールを実行して、ControllerをWeb Studioに追加します。

Controller を削除する

サイトからコントローラーを削除しても、Citrixソフトウェアやその他のコンポーネントはアンインストールされません。この操作により、コントローラーはデータベースから削除され、接続の仲介やその他のタスクを実行できなくなります。コントローラーを削除しても、後で同じサイトまたは別のサイトに再度追加できます。サイトには少なくとも1つのコントローラーが必要なため、Web Studioに表示されている最後のコントローラーを削除することはできません。

サイトからコントローラーを削除しても、データベースサーバーへのコントローラーのログオンは削除されません。これにより、同じマシン上の他の製品のサービスで使用されているログオンが誤って削除されるのを防ぎます。ログオンが不要になった場合は、手動で削除する必要があります。ログオンを削除するには、`securityadmin`サーバーロールの権限が必要です。

Controller を削除した後:

- 自動更新を使用しているVDAは、他の利用可能なコントローラーに再登録されます。この再登録は、自動更新メカニズムが有効になっており、VDAが他のコントローラー（削除されたコントローラーと同じセカンダリゾーン、またはオンプレミス展開のプライマリゾーン）に到達できる場合にのみ発生します。
- Citrix StoreFrontでコントローラー情報を更新します。詳細については、「コントローラーの管理」を参照してください。
- Citrix StoreFrontで、Citrix Gatewayを介したリモートアクセス用のSecure Ticket Authority (STA) URLを更新します。詳細については、「Secure Ticket Authorityの管理」を参照してください。
- Citrix Gatewayで、仮想サーバーのSTA URLを更新します。詳細については、「Citrix Gateway」を参照してください。

> **重要:**

> サイトからコントローラーを削除するまでは、Active Directoryからコントローラーを削除しないでください。

1. Web Studioがロードされ、削除したいコントローラーが表示されるように、コントローラーの電源がオンになっていることを確認してください。
2. Web Studioがコントローラーを完全にロードした後、コントローラー上のすべてのサービスが実行されており、コントローラーの電源がオンのままであることを確認してください。
3. Web Studioにサインインし、左ペインで**設定**を選択します。
4. **Delivery Controller**タイルを見つけて、**編集**をクリックします。
5. **Delivery Controllerの管理**ページで、削除したいコントローラーを選択します。
6. **Controllerの削除**を選択します。適切なデータベースロールと権限がない場合、データベース管理者がControllerを削除できるようにするスクリプトを生成するオプションが提示されます。

   Web Studioは、Controllerを削除する前に事前チェックを実行します。Controllerが電源オフになっており、以下のサービスステータスにない場合は、安全に削除できます。

   - 不明
   - 障害保留中
   - 古いバージョン
   - 新しいバージョン
   - バージョン変更が進行中
   - 必須機能が不足しています

   Controller の電源がオフになっておらず、上記のいずれかのサービスステータスである場合、Web Studio は Controller の電源をオフにするよう求めます。
7. データベースサーバーから Controller のマシンアカウントを削除する必要があります。削除する前に、別サービスがそのアカウントを使用していないことを確認してください。

Web Studio を使用して Controller を削除した後、現在のタスクが適切に完了するように、その Controller へのトラフィックがしばらく残る場合があります。短時間で Controller の削除を強制したい場合は、Citrix は、インストールされていたサーバーをシャットダウンするか、そのサーバーを Active Directory から削除することを推奨します。その後、サイト上の他の Controller を再起動して、削除された Controller とのそれ以上の通信がないことを確認してください。

Controller を別のゾーンに移動する

サイトに複数のゾーンが含まれている場合、Controller を別のゾーンに移動できます。この移動が VDA 登録やその他の操作にどのように影響するかについては、「ゾーン」を参照してください。

1. 左ペインで**ゾーン**を選択します。
2. 中央ペインでゾーンを選択し、Controllerを選択します。
3. アクションバーで を選択します。
4. 表示される ページで、Controller を移動するゾーンを選択します。
5. をクリックします。

VDA を別のサイトに移動する

Citrix Provisioning™ を使用してプロビジョニングされた VDA、または既存のイメージである VDA は、アップグレード時、またはテストサイトで作成された VDA イメージを本番サイトに移動する際に、別のサイト（サイト1からサイト2へ）に移動できます。Machine Creation Services (MCS) を使用してプロビジョニングされた VDA は、あるサイトから別のサイトに移動できません。MCS は、VDA が Controller に登録するためにチェックする ListOfDDCs の変更をサポートしていません。MCS を使用してプロビジョニングされた VDA は、常に作成されたサイトに関連付けられている ListOfDDCs をチェックします。

VDA を別のサイトに移動するには、インストーラーを使用する方法と Citrix ポリシーを使用する方法の2つがあります。

インストーラー

インストーラーを実行して Controller を追加し、サイト2の Controller の FQDN（DNSエントリ）を指定します。

Controller ポリシー設定が使用されていない場合にのみ、インストーラーで Controller を指定します。

グループポリシーエディター

次の例では、複数の VDA をサイト間で移動します。

1. サイト1で次の設定を含むポリシーを作成し、そのポリシーをデリバリーグループレベルにフィルター処理して、サイト間の段階的な VDA 移行を開始します。
    - Controller：サイト2の1つ以上の Controller の FQDN（DNSエントリ）を含む。
    - Controller の自動更新を有効にする：無効に設定。

2. デリバリーグループ内の各 VDA は、新しいポリシーが適用されてから90分以内に通知を受け取ります。VDA は受信した Controller のリストを無視し（自動更新が無効になっているため）、ポリシーで指定された Controller のいずれかを選択します。このポリシーにはサイト2の Controller がリストされています。
3. VDAがサイト2のControllerに正常に登録されると、サイト2のListOfDDCsとポリシー情報を受け取ります。これらはデフォルトで自動更新が有効になっています。VDAがサイト1で登録されていたControllerは、サイト2のControllerから送信されたリストには含まれていません。そのため、VDAはサイト2のリストにあるControllerの中から選択して再登録します。それ以降、VDAはサイト2からの情報で自動的に更新されます。

グループポリシーエディターの使用方法については、Citrixポリシーのドキュメントを参照してください。

ホーム

Web Studio のホームページには、Citrix Virtual Apps and Desktops™ の展開とワークロードの概要、およびサブスクリプションを最大限に活用するのに役立つ情報が表示されます。この記事では、このページで利用できるウィジェットを紹介します。

- サイトの詳細
- リソース
- セッション
- 最近
- エラーと警告
- 開始する

ニーズに合わせてウィジェットを追加、削除、または再配置することで、このホームページをカスタマイズできます。

サイトの詳細

このウィジェットは、Citrix Virtual Apps and Desktops サイトの概要を一目で確認できるようにします。ライセンスの種類、Studio のバージョン、Delivery Controller のバージョンとステータスなどの主要情報が表示されます。

サイトの問題を診断するには、 を選択して、データベースの正常性、接続、委任管理、VDA 更新の準備状況、登録状態などのチェックを実行します。このアクションは、アップグレード中に特に役立ち、展開の前後でサイトが安定して準備ができていることを確認するのに役立ちます。

リソース

このウィジェットは、Citrix Virtual Apps and Desktops展開の概要を提供します。

- **リソース**。展開されたリソースの数と、カテゴリごとのカウントを表示します。

リソース	カテゴリ別にカウントを表示するには
マシン	**マシン**をクリックし、状態を選択して、ドーナツグラフにカーソルを合わせると詳細が表示されます。利用可能なオプション: **可用性状態** (利用可能、使用中、オフ、利用不可)、**登録状態** (登録済み、未登録)、**メンテナンス状態** (メンテナンス中、メンテナンス中ではない)。可用性状態別にマシンの数を表示する場合、状態をクリックすると対応するマシンの詳細を表示できます。
アプリケーション	**アプリケーション**をクリックし、ドーナツグラフにカーソルを合わせると詳細が表示されます。
デリバリーグループ	**デリバリーグループ**をクリックし、ドーナツグラフにカーソルを合わせると詳細が表示されます。
マシンカタログ	**マシンカタログ**をクリックし、ドーナツグラフにカーソルを合わせると詳細が表示されます。

- **過去7日間に起動されたセッション**。過去7日間に毎日起動されたデスクトップおよびアプリセッションの数を表示します。詳細を確認するには、Directorに移動をクリックします。

セッション

このウィジェットは、過去7日間のCitrix Virtual Apps and Desktopsワークロードの概要を提供します。過去7日間に毎日起動されたデスクトップおよびアプリセッションの数を表示します。

最近

このウィジェットには、Web Studioで最近アクセスしたオブジェクトの履歴が表示されます。これにより、オブジェクトのアクセス履歴をすばやく確認できます。リスト内のオブジェクト名をクリックすると、そのオブジェクトがそれぞれのノード内で直接開きます。

以下に留意してください。

- リストはブラウザのキャッシュにローカルに保存されます。キャッシュをクリアしたり、ブラウザを切り替えたり、シークレットモードを使用したりすると、リストはリセットされます。
- リストは、過去30日間にアクセスした最新の100個のオブジェクトに限定されます。
- このリストには、個々のオブジェクトの表示または操作のみが記録されます。一度に*複数*のオブジェクトを選択しても、リストには記録*されません*。
- 以下のオブジェクトは追跡*されません*。
  - **設定**、**ライセンス**、**ログ**ノード内のオブジェクト。
  - **ポリシー**ノードの**比較**タブと**モデリング**タブ内のオブジェクト。
  - **バックアップと復元**ノードの**履歴**タブと**設定**タブ内のオブジェクト。

開始する

このウィジェットは、Citrix Virtual Apps and Desktopsの展開をセットアップするのに役立つ一連の質問に答えるようにガイドします。これらの質問に答えることで、展開を迅速に構成できます。

エラーと警告

展開からのエラーと警告を一元的に表示します。

- 以下の構成ノードに存在するエラー数と警告数を一覧表示します: ゾーン、マシン、マシンカタログ、デリバリーグループ、ホスティング、およびイメージ。数字をクリックすると、対応するノードのUIにリンクされます。
- サイト内の優先度の高いエラーを一覧表示し、推奨されるアクションも示します。

ホームページのカスタマイズ

「ホーム」ページをカスタマイズするには、次の手順に従います。

1. Web Studioにサインインします。

   ホームページが表示されます。
2. 「ホーム」ページの右上隅にある**編集**アイコンをクリックします。
3. ウィジェットを再配置するには、目的の位置にドラッグします。
4. 「ホーム」ページからウィジェットを削除するには、ウィジェットの右上にある**削除**アイコンをクリックします。

5. 「ホーム」ページにウィジェットを再度追加するには、「ホーム」ページの右上隅にある**ウィジェットの追加**アイコンをクリックします。
6. 変更を保存するには、**完了**をクリックします。

IPv4/IPv6 のサポート

このリリースでは、純粋なIPv4、純粋なIPv6、およびIPv4とIPv6のネットワークが重複するデュアルスタック展開をサポートしています。

次のコンポーネントはIPv4のみをサポートします。その他のすべてのコンポーネントはIPv4とIPv6をサポートします。

- XenServer®
- **IPv6 Controller登録のみを使用**ポリシー設定によって制御されていないVirtual Delivery Agent (VDA)

IPv6通信は、VDA接続に関連する2つのCitrix®ポリシー設定で制御されます。

- **IPv6 の使用を強制する主要な設定:** IPv6 Controller 登録のみを使用。

  このポリシー設定は、VDA が Delivery Controller に登録するために使用するアドレス形式を制御します。

  有効にすると、VDAは次の優先順位で選択された単一のIPv6アドレスを使用してControllerに登録し、通信します: グローバルIPアドレス、ユニークローカルアドレス (ULA)、リンクローカルアドレス (他のIPv6アドレスが利用できない場合のみ)。

  無効にすると、VDAはマシンのIPv4アドレスを使用してControllerに登録し、通信します。これがデフォルト値です。

  チームが頻繁にIPv6ネットワークを使用する場合は、**IPv6 Controller登録のみを使用**ポリシー設定が有効になっているイメージまたは組織単位 (OU) に基づいて、それらのユーザー向けにデスクトップとアプリケーションを公開します。

  チームが頻繁にIPv4ネットワークを使用する場合は、**IPv6 Controller登録のみを使用**ポリシー設定が無効になっているイメージまたはOUに基づいて、それらのユーザー向けにデスクトップとアプリケーションを公開します。
- **IPv6 ネットマスクを定義する依存設定:** Controller 登録 IPv6 ネットマスク。

  マシンは複数のIPv6アドレスを持つことができます。このポリシー設定により、管理者は、登録されている場合に、VDAをグローバルIPではなく優先サブネットのみに制限できます。この

設定は、VDAが登録するネットワークを指定します。VDAは、指定されたネットマスクに一致する最初のアドレスでのみ登録します。

この設定は、**IPv6 Controller登録のみを使用ポリシー**設定が有効になっている場合にのみ有効です。デフォルト = 空の文字列

展開に関する考慮事項

環境にIPv4とIPv6の両方のネットワークが含まれている場合、IPv4のみのクライアントと、IPv6ネットワークにアクセスできるクライアント向けに、個別のデリバリーグループ構成を作成します。ユーザーを区別するために、命名規則、手動のActive Directoryグループ割り当て、またはSmartAccessフィルターの使用を検討してください。 接続がIPv6ネットワークで開始され、その後、IPv4アクセスのみを持つクライアントから再接続しようとすると、セッションの再接続が失敗する可能性があります。

注記 - DNS解決が有効になっている場合、これらの考慮事項は適用されません。

Web Studio を使用した Citrix Virtual Apps and Desktops™ のライセンス

注:

- バージョン2511以降、Citrix Web Studio (Webベース) はCitrix Virtual Apps and Desktops™ の唯一の管理コンソールです。Citrix Studio (MMCベース) はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。
- License Activation Service (LAS) は、従来のCitrix®レガシーライセンスに代わる新しいクラウドベースのライセンスソリューションです。LASはアクティベーション用の新しいモジュールを導入し、ライセンス管理へのシームレスで最新のアプローチを保証します。詳細については、License Activation Serviceを参照してください。

Web Studioから、ライセンスサーバーがWeb Studioと同じドメイン内にあるか、または信頼されたドメイン内にある場合、ライセンスを管理および追跡できます。ライセンスタスクの詳細については、ライセンスドキュメントおよび複数タイプのライセンスを参照してください。

次の表に、サポートされているエディションとライセンスモデルを示します。

製品	エディション	ライセンスモデル
シトリックス バーチャル アプリケーションズ	プレミアム、アドバンスト、スタンダード	同時接続
シトリックス バーチャル デスクトップ	プレミアム、アドバンスト、スタンダード	ユーザー/デバイスおよび同時接続

詳細については、「同時使用ライセンス」および「ユーザー/デバイスライセンス」を参照してください。

サポートされているCurrent Release (CR)およびLong Term Service Release (LTSR)バージョン

Citrixは、機能やセキュリティの改善の恩恵を受けるために、常にCitrix License Serverの最新バージョンを使用することを強く推奨します。

> **注:**
>
> License Server VPXは非推奨となり、今後のメンテナンスやセキュリティ修正は提供されません。License Server VPXのバージョン11.16.6以前を使用しているお客様は、できるだけ早くWindows用License Serverの最新バージョンに移行することをお勧めします。

> Citrix製品のライフサイクル日付の詳細については、製品マトリックスを参照してください。

レガシー製品および製品バージョンについては、「レガシー製品マトリックス」を参照してください。

以下のタスクを完了するには、完全なライセンス管理者である必要があります。Web Studioでライセンス情報を表示するには、管理者は少なくとも「ライセンスの読み取り」委任管理権限を持っている必要があります。組み込みの「完全管理者」および「読み取り専用管理者」の役割には、その権限があります。

Web Studioを使用してCitrixからライセンスをダウンロードしてインストールする

1. Web Studioにサインインし、左側のペインで**ライセンス**を選択します。

2. アクションバーで**ライセンスの割り当て**を選択します。
3. ライセンスアクセスコードを入力します。これは、ライセンスの購入または更新後にCitrixから電子メールで受け取ったものです。
4. 製品を選択し、**ライセンスの割り当て**を選択します。その製品で利用可能なライセンスが割り当てられ、ダウンロードされます。特定のライセンスアクセスコードのすべてのライセンスを割り当ててダウンロードすると、そのライセンスアクセスコードを再利用することはできません。同じコードで他のトランザクションを行うには、マイアカウントにログオンしてください。

ローカルコンピューターまたはネットワークに保存されているライセンスを追加する

1. Web Studioにサインインし、左側のペインで**ライセンス**を選択します。
2. アクションバーで**ライセンスの追加**を選択します。
3. ライセンスファイルを参照して、ライセンスサーバーに追加します。

ライセンスサーバーを変更する

1. Web Studioにサインインし、左ペインで**Licensing**を選択します。
2. アクションバーで**Change License Server**を選択します。
3. ライセンスサーバーのアドレスを*name:port*の形式で入力します。ここで、nameはDNS、NetBIOS、またはIPアドレスです。ポート番号を指定しない場合、デフォルトポート（27000）が使用されます。

使用するライセンスの種類を選択する

- サイトを構成する際、ライセンスサーバーを指定した後、使用するライセンスの種類を選択するよう求められます。サーバーにライセンスがない場合、ライセンスなしで製品を30日間試用するオプションが自動的に選択されます。
- サーバーにライセンスがある場合、その詳細が表示され、そのうちの1つを選択できます。または、ライセンスファイルをサーバーに追加してから、そのファイルを選択することもできます。

製品エディションとライセンスモデルを変更する

1. Web Studioにサインインし、左側のペインで**［ライセンス］**を選択します。
2. アクションバーで**［製品エディションの編集］**を選択します。
3. 適切なオプションを更新します。

License Administration Consoleにアクセスするには、アクションバーで**License Administration Console**を選択します。コンソールはすぐに表示されるか、ダッシュボードがパスワードで保護されている場合は、License Administration Consoleの資格情報の入力を求められます。コンソールの使用方法の詳細については、ライセンスドキュメントを参照してください。

> **注：**
>
> Web Studioでライセンスを切り替えると、その変更がCitrix Directorに反映されるまでに最大5分かかります。たとえば、AdvancedとPremiumを切り替える場合などです。

ライセンス管理者を追加する

1. Web Studioにサインインし、左ペインで**［Licensing］**を選択します。
2. **［Licensing Administrators］**タブを選択します。
3. アクションバーで**［Add licensing administrator］**を選択します。
4. 管理者として追加するユーザーを参照し、権限を選択します。

ライセンス管理者のアクセス許可を変更またはライセンス管理者を削除する

1. Web Studioにサインインし、左ペインで**［Licensing］**を選択します。
2. **［Licensing Administrators］**タブを選択し、管理者を選択します。
3. アクションバーで**［Edit licensing administrator］または［Delete licensing administrator］**のいずれかを選択します。

ライセンス管理者グループを追加する

1. Web Studioにサインインし、左ペインで**［Licensing］**を選択します。
2. **［Licensing Administrators］**タブを選択します。
3. アクションバーで**［Add licensing administrator group］**を選択します。
4. ライセンス管理者として機能させるグループを参照し、権限を選択します。Active Directoryグループを追加すると、そのグループ内のユーザーにライセンス管理者権限が付与されます。

ライセンス管理者グループの権限を変更または削除する

1. Web Studioにサインインし、左ペインで**Licensing**を選択します。
2. **Licensing Administrators**タブを選択し、次に管理者グループを選択します。

3. アクションバーで、**Edit licensing administrator group**または**Delete licensing administrator group**のいずれかを選択します。

ライセンス情報を表示する

Web Studioにサインインし、左ペインで**Licensing**を選択します。サイトのライセンス使用状況と設定の概要が、指定されたライセンスサーバーに現在インストールされているすべてのライセンスのリストとともに表示されます。

サイトのライセンス設定（製品タイプ、ライセンスエディション、ライセンスモデルを含む）が、構成済みのライセンスサーバーが使用するライセンスと一致していることを確認してください。一致しない場合は、サイトのライセンス設定に一致させるために、既存のライセンスをダウンロードまたは割り当てる必要がある場合があります。

`Get-Brokersite`コマンドを実行して、以下のライセンス情報を取得します。

- TotalUniqueLicenseUsers
- PeakConcurrentLicenseUsers
- PeakConcurrentLicensedDevice

> **注:**
>
> Citrix DaaSの情報を取得するには、クラウドライセンスAPIを使用します。クラウドライセンスAPIの詳細については、APIs to manage Citrix Cloud licensingを参照してください。

ライセンス有効期限アラートを表示する

Web Studioは、Citrix License Serverからライセンスファイルの有効期限を照会します。ライセンスファイルの有効期限が近づいているか、すでに期限切れになっている場合、Web Studioは概要タブで管理者にアラートを表示します。

関連リンク

- 「Citrix オンプレミス年間および期間ベースのリテールライセンスのサブスクリプション」を参照してください。(/ja-jp/licensing/current-release/license-types.html#citrix-on-premises-subscription-for-annual-and-term-based-retail-licenses).
- 「ハイブリッド権限による移行とアップグレード (TTU)」を参照してください。(/ja-jp/licensing/current-release/hybrid-rights-ttu.html).

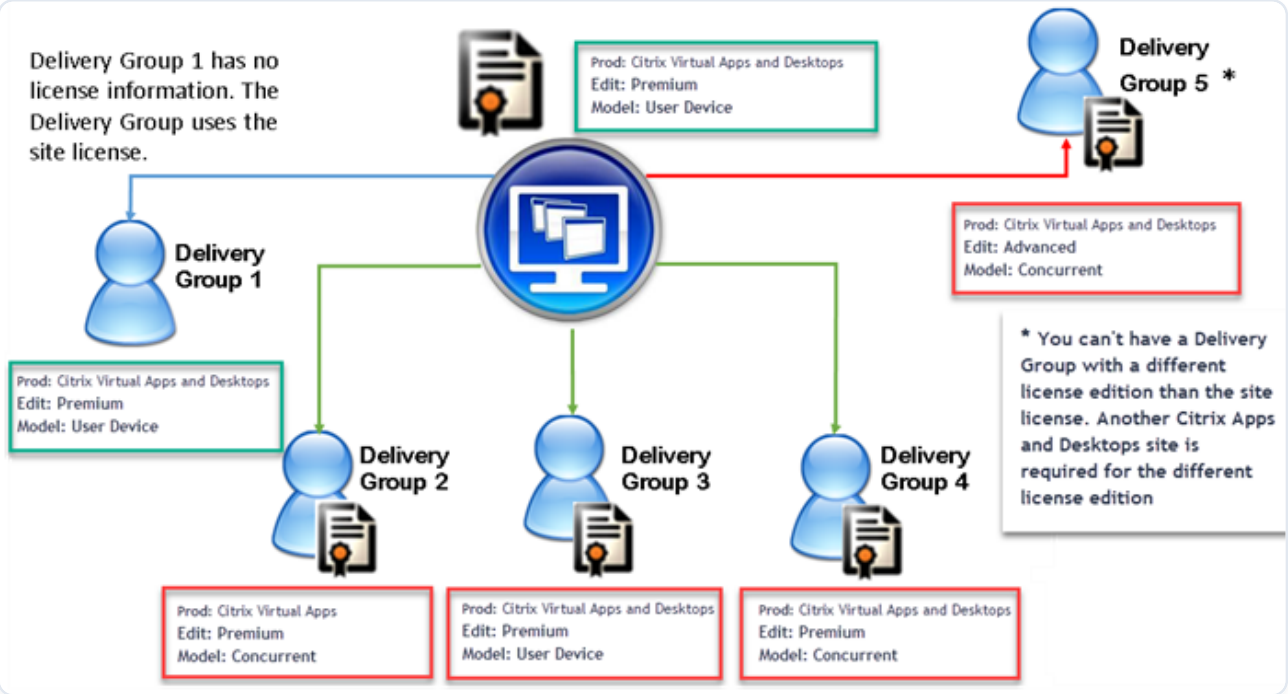
マルチタイプライセンス

注:

ライセンスアクティベーションサービス は、マルチタイプライセンスをサポートしていません。

マルチタイプライセンスは、単一のCitrix Virtual Apps and Desktopsサイト上のデリバリーグループに対して、異なるライセンスタイプの消費をサポートします。**タイプ**は、製品ID（XDTまたはMPS）とモデル（UserDeviceまたはConcurrent）の単一の組み合わせです。デリバリーグループは、サイトレベルで構成されているものと同じ製品エディション（PLT/PremiumまたはENT/Advanced）を使用する必要があります。Citrix Virtual Apps and Desktops展開でマルチタイプライセンスを構成する際には、この記事の最後にある特別な考慮事項 に注意してください。

マルチタイプライセンスが構成されていない場合、異なるライセンスタイプは、個別のサイト用に構成されている場合にのみ使用できます。デリバリーグループはサイトライセンスを使用します。マルチタイプライセンスが構成されている場合の重要な通知制限については、特別な考慮事項を参照してください。



異なる種類のライセンスを消費するデリバリーグループを特定するには、以下のBroker PowerShellコマンドレットを使用します。

- New-BrokerDesktopGroup

- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

ライセンスをインストールするには、以下を使用します。

- シトリックス スタジオ
- シトリックス ライセンシング マネージャー
- citrix.com

Customer Success Services の日付は、各ライセンスファイル、各製品、およびモデルに固有です。異なる設定のデリバリーグループは、互いに異なる Customer Success Services の日付を持つ場合があります。

特別な考慮事項

マルチタイプライセンスは、通常のCitrix Virtual Apps and Desktops™ライセンスとは異なる機能を持ちます。

サイト構成とは異なるタイプを使用するように構成されたデリバリーグループの場合、DirectorまたはStudioからのアラートや通知はありません。

- ライセンス制限に近づいている場合、またはライセンスバーストモードのトリガーや有効期限切れの場合でも、情報はありません。
- 特定のグループに問題が発生した場合でも、通知はありません。

マルチタイプライセンス用に構成されたデリバリーグループは、そのライセンスタイプのみを消費し、完全に消費されてもサイト構成にフォールバックしません。

Citrix Virtual Apps StandardとCitrix Virtual Desktops™ Standardのライセンスエディション名はどちらもStandardであることを示していますが、これらは同じエディションではありません。マルチタイプライセンスは、Citrix Virtual Apps StandardおよびCitrix Virtual Desktop Standardライセンスでは利用できません。

ライセンス互換性マトリックス

この表は、古い製品名、新しい製品名、および関連する機能名を詳述しています。4つの互換性列は、どの製品とライセンスモデルの組み合わせがマルチタイプライセンスと互換性があるかを指定します。CCUとCCSは同時接続ライセンスを表し、UDはユーザー/デバイスライセンスを表します。

ライセンス互換性マトリックスと旧名および新名(/en-us/citrix-virtual-apps-desktops/2511/media/multi-type-compatibility-names.png)

ブローカー PowerShell SDK

DesktopGroup オブジェクトには、関連するNew-BrokerDesktopGroupおよびSet-BrokerDesktopGroupコマンドレットを使用して操作できる次の2つのプロパティがあります。

名前	値	制限
LicenseModel	グループのライセンスモデルを指定するパラメーター (Concurrent または UserDevice)。指定されていない場合、サイト全体のライセンスモデルが使用されます。	機能トグルが無効になっている場合、プロパティを設定しようとすると失敗します。
ProductCode	XDT (Citrix Virtual Desktops用) またはMPS (Citrix Virtual Apps™用) のテキスト文字列で、グループのライセンス製品IDを指定します。指定されていない場合、サイト全体の製品コードが使用されます。	機能トグルが無効になっている場合、プロパティを設定しようとすると失敗します。

LicenseModelおよびProductCodeの詳細については、about_Broker_Licensingを参照してください。

New-BrokerDesktopGroup

デスクトップグループのブローカーを管理するためのデスクトップグループを作成します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/>`を参照してください。

Set-BrokerDesktopGroup

既存のブローカーデスクトップグループを無効または有効にするか、その設定を変更します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`を参照してください。

Get-BrokerDesktopGroup

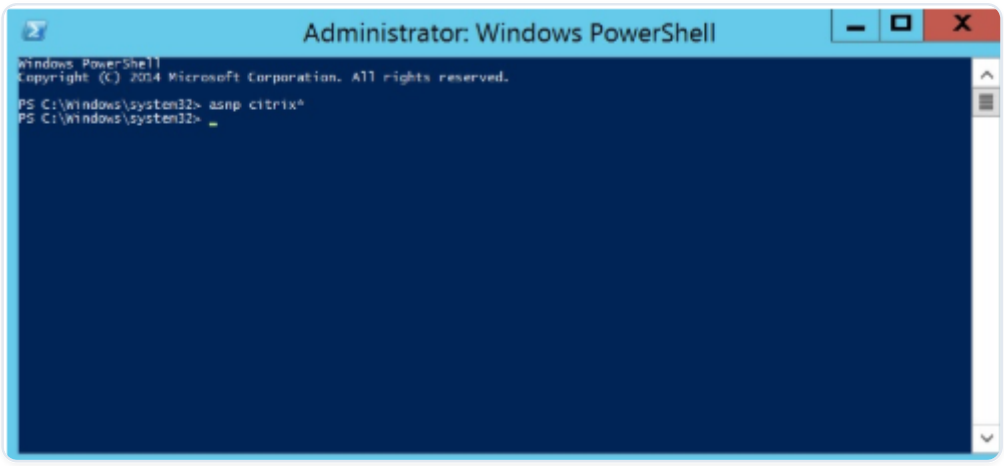
指定された基準に一致するデスクトップグループを取得します。Get-BrokerDesktopGroupコマンドレットの出力には、グループの**ProductCode**および**LicenseModel**プロパティが含まれます。New-BrokerDesktopGroupまたはSet-BrokerDesktopGroupを使用してプロパティが設定されていない場合、null値が返されます。nullの場合、サイト全体のライセンスモデルと製品コードが使用さ

れます。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/>`を参照してください。

デリバリーグループごとに異なるライセンス製品とモデルを構成する

> **注:**
>
> 1つのデリバリーグループに、2つ以上の異なる種類の製品、エディション、またはライセンスモデルを構成することはできません。異なる種類の製品、エディション、またはライセンスモデルがある場合は、それらを別々のデリバリーグループで構成してください。

1. 管理者権限でPowerShellを開き、Citrixスナップインを追加します。

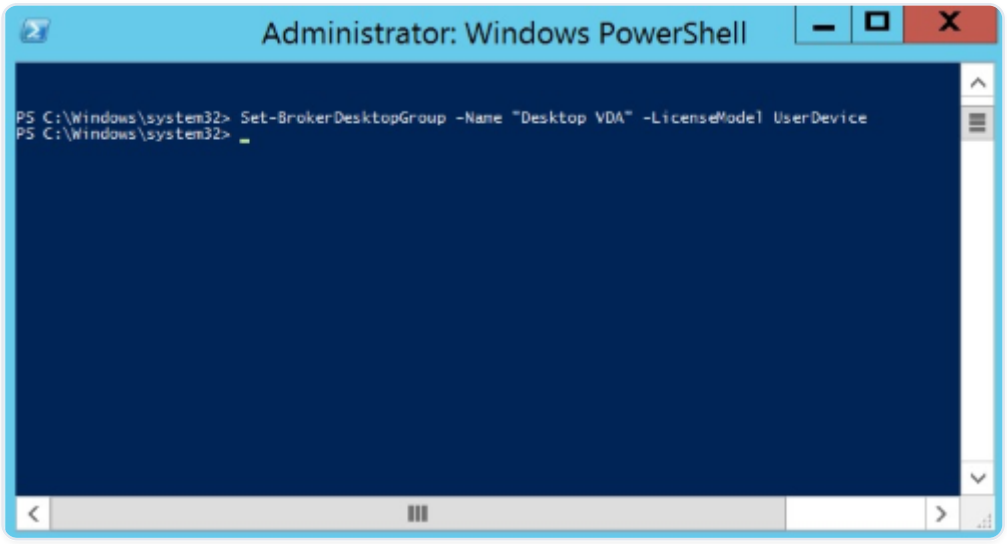


2. コマンド **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** を実行して、現在のライセンス構成を表示します。パラメーター **LicenseModel** と **ProductCode** を見つけます。これらのパラメーターを以前に構成していない場合、空白になっている可能性があります。

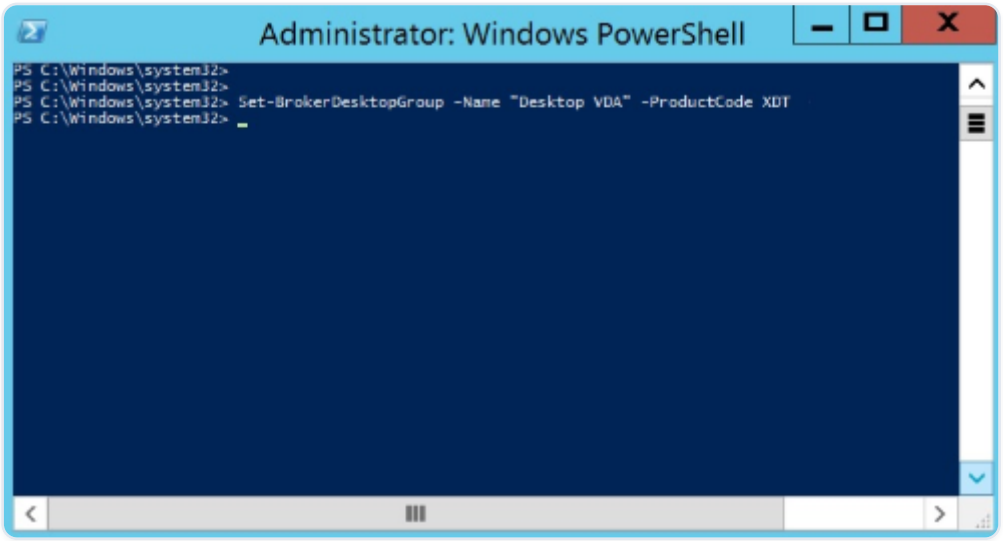
> **注:**
>
> デリバリーグループにライセンス情報が設定されていない場合、デフォルトで **Site level Site license** が適用されます。

> PowerShellコマンド(/en-us/citrix-virtual-apps-desktops/2511/media/license-configuration-2.png)

3. コマンド **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –LicenseModel LicenseModel** を実行して、ライセンスモデルを変更します。



4. コマンドを実行してライセンス製品を変更します: **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –ProductCode ProductCode**。



5. 変更を検証するには、コマンド **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** を入力します。

> **注:**
>
> 同じサイト内でエディションを混在させることはできません。たとえば、Premiumライセンスとライセンスなどです。異なるエディションのライセンスがある場合は、複数のサイトが必要です。

> PowerShellコマンド(/en-us/citrix-virtual-apps-desktops/2511/media/license-configuration-5.png)

6. 前の手順で説明したのと同じ **Set-BrokerDesktopGroup** コマンドを実行し、値を **$null** に設定して、ライセンス構成を削除します。

> **注:**
>
> Studioでは、各デリバリーグループのライセンス構成は表示されません。現在の構成を表示するには、PowerShellを使用します。
>
> PowerShell コマンド(/en-us/citrix-virtual-apps-desktops/2511/media/license-configuration-6.png)

例

この PowerShell コマンドレットの例は、既存の2つのデリバリーグループに対するマルチタイプライセンスの設定方法を示し、さらに3つ目のデリバリーグループを作成して設定します。

デリバリーグループに関連付けられているライセンス製品とライセンスモデルを確認するには、**Get-BrokerDesktopGroup** PowerShell コマンドレットを使用します。

1. 最初のデリバリーグループを XenApp® と Concurrent 用に設定します。

   Set-BrokerDesktopGroup -Name "Citrix Virtual Apps Premium Concurrent 用のデリバリーグループ" -ProductCode MPS -LicenseModel Concurrent

2. 2番目のデリバリーグループを XenDesktop® と Concurrent 用に設定します。

   Set-BrokerDesktopGroup -Name "シトリックス バーチャルデスクトップ プレミアム コンカレント のデリバリーグループ" -ProductCode XDT -LicenseModel Concurrent

3. 3番目のデリバリーグループを XenDesktop と UserDevice 用に作成して設定します。

   New-BrokerDesktopGroup -Name "Citrix Virtual Desktops Premium UserDevice 用のデリバリーグループ" -PublishedName "MyDesktop" -DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

ライセンスアクティベーションサービス

ライセンスアクティベーションサービス (LAS) は、従来のCitrix®レガシーライセンスに代わる、新しいクラウドベースのライセンスソリューションです。LASはアクティベーション用の新しいモジュールを導入し、ライセンス管理へのシームレスで最新のアプローチを保証します。

LASはCitrixライセンスのエクスペリエンスを簡素化します。ライセンスサーバーで生成、ダウンロード、またはインストールするライセンスアクセスコードやファイルは不要になりました。ライセンスサーバーをアップグレードし、Citrix Cloudに登録するだけです。互換性のある製品がライセンスサーバーを指すように設定されると、自動的にアクティベートされます。

アクティベーション後、ライセンスサーバーはライセンスアクティベーションサービスと定期的に通信し、アクティベーションを最新の状態に保ちます。LASはクラウドテクノロジーで構築されており、パフォーマンスを向上させ、ダウンタイムがないことを保証します。何らかの理由でライセンスサーバーまたはLASに到達できない場合、システムはライセンスキャッシュモードに入ります。これは、システムのライセンスが失われるのを防ぎ、停止を回避するように設計されています。詳細については、「ライセンスキャッシュモード」を参照してください。

LASの詳細については、ライセンスドキュメントの「ライセンスアクティベーションサービス」を参照してください。

前提条件

- ライセンスサーバーをバージョン11.17.2ビルド53100以降にインストールまたは更新します。
- ライセンスサーバー用の信頼性の高い継続的なインターネット接続。

考慮事項

- Studioがアクティベーションを促す前に、すべてのDelivery ControllerがLASと互換性がある必要があります。1つのサイトでは、レガシーライセンスまたはLASのいずれかを使用できます。
- 同じCitrix Cloud ID (CCID) またはOrgIDに複数のライセンスサーバーを登録できます。ただし、サイトは1つのライセンスサーバーのみを指すように構成できます。

制限事項

- LASへの移行により、製品エディションは**Premium**に、ライセンスモデルは**Concurrent**に設定されますが、これは将来変更される可能性があります。PowerShellを使用してライセンス構成を変更しないでください。登録とセッション起動に影響を与える可能性があります。
- 既存のレガシーライセンスからLASへのCitrix Virtual Apps and Desktops™サイトの移行は、Studioのみを使用して行うことができます。

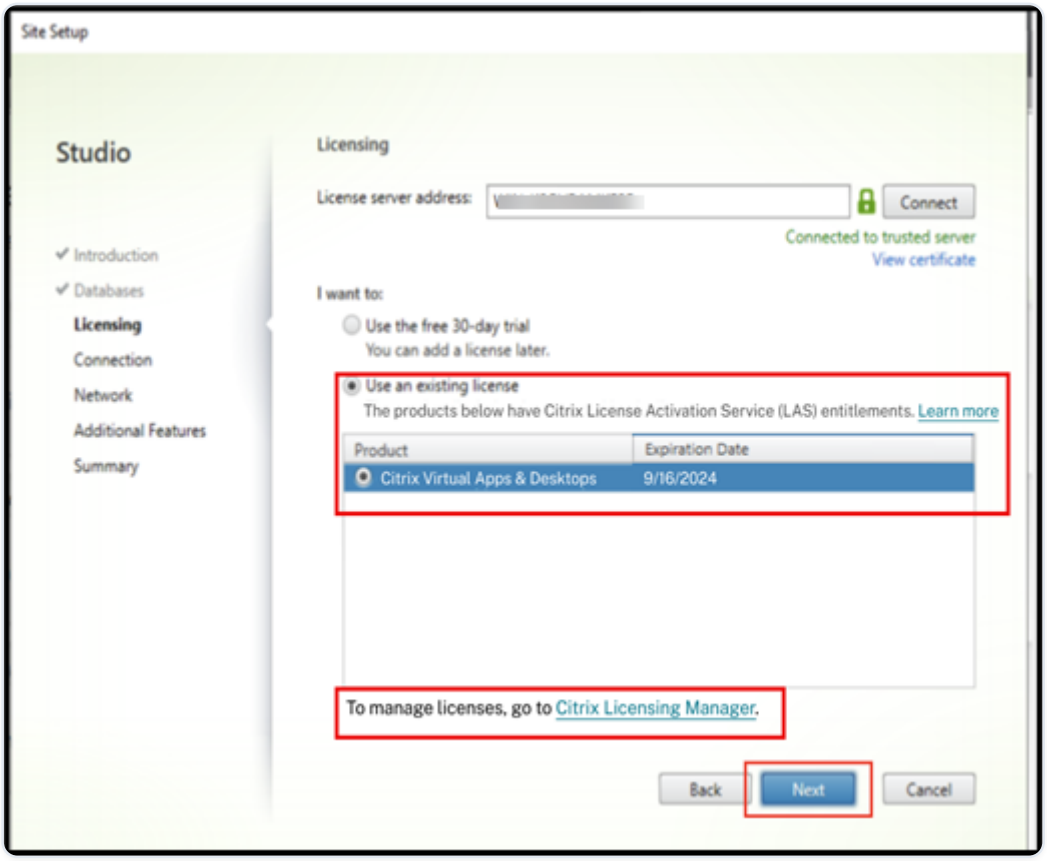
主な手順

1. License Serverをバージョン11.17.2ビルド53100以降にインストールまたはアップグレードし、(/ja-jp/licensing/current-release/license-activation-service#how-to-configure-license-server-for-license-activation-service)に記載されている手順に従ってLASを構成します。

2. Citrix Virtual Apps™ and Desktopsバージョン2411以降をインストールします。Citrix Delivery Controller、Studio、Citrix Directorなどのコアコンポーネントをインストールします。

> **注:**
>
> Citrix Virtual Apps and Desktopsサイト内のすべてのDelivery Controllerは、LASと互換性がある必要があります。

3. 必要なコンポーネントをインストールしたら、Citrix Site Managerを使用してサイトを作成します。サイトの作成については、(/ja-jp/citrix-virtual-apps-desktops/2511/install-configure/site-create)を参照してください。License ServerがLASを使用するように構成されている場合、Metainstallerはエンタイトルメントを表示します。エンタイトルメントは、対応するライセンス有効期限とともに提供されます。



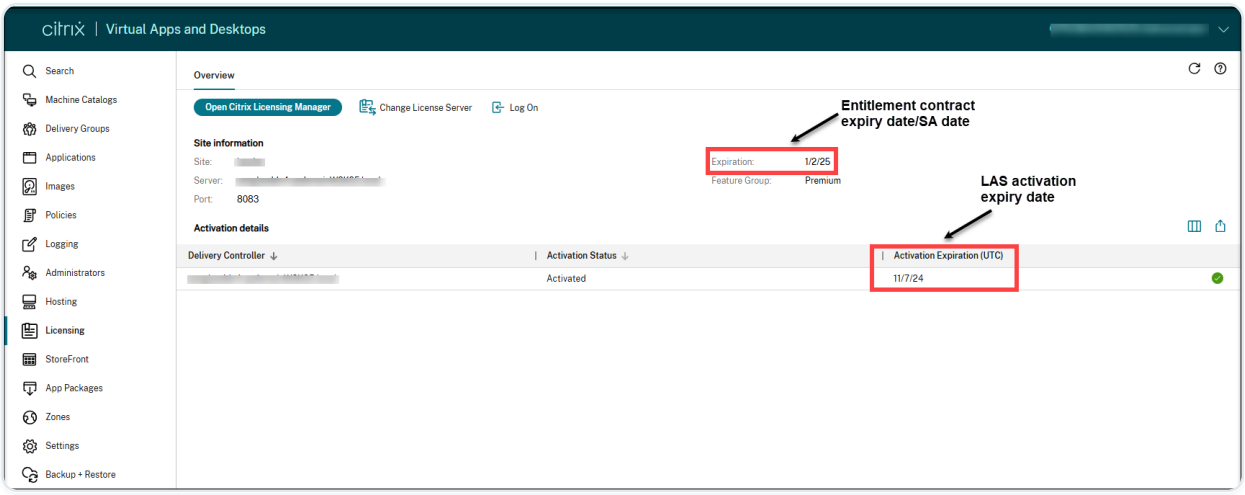
> **注:**
>
> License Serverが最新のLicense Serverバージョンにアップグレードされていない場合、エラーメッセージが表示されます。

4. ライセンスの詳細を確認。
5. レガシーライセンスをLASに移行。

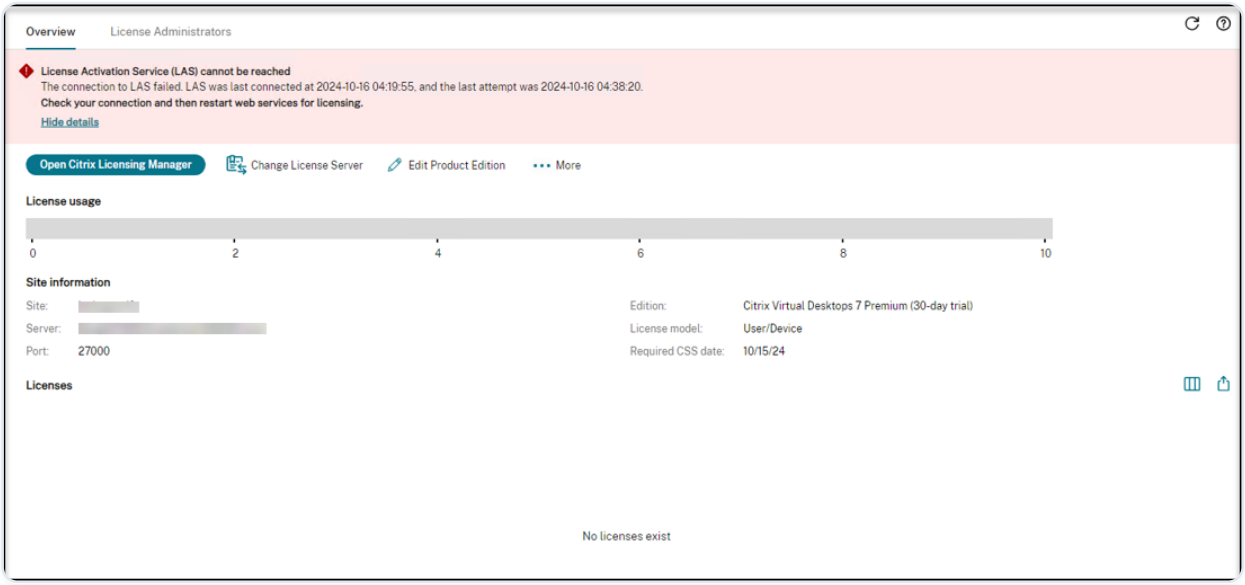
ライセンスの詳細を確認する

サイトを作成したら、Studioを使用してライセンスの詳細を確認します。

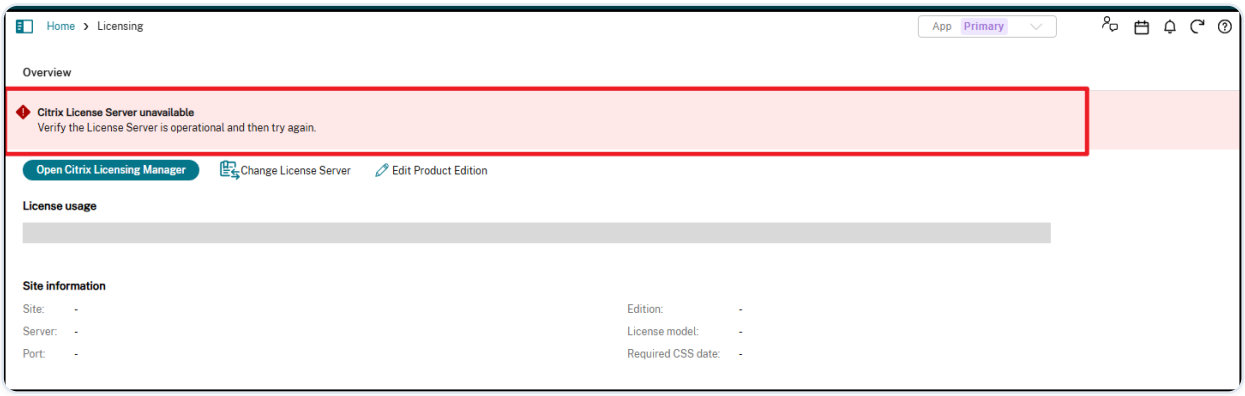
1. Studioで、**Licensing**ノードを選択します。
2. **概要**タブで、Citrix Virtual Apps and Desktopsサイトに適切なライセンスがあるか、またはLAS機能の使用中にライセンスが期限切れになっていないかを確認します。



LAS に到達できない場合、次のようなエラーメッセージが表示されることがあります。



ライセンスサーバーが利用できない場合、次のようなエラーメッセージが表示されることがあります。



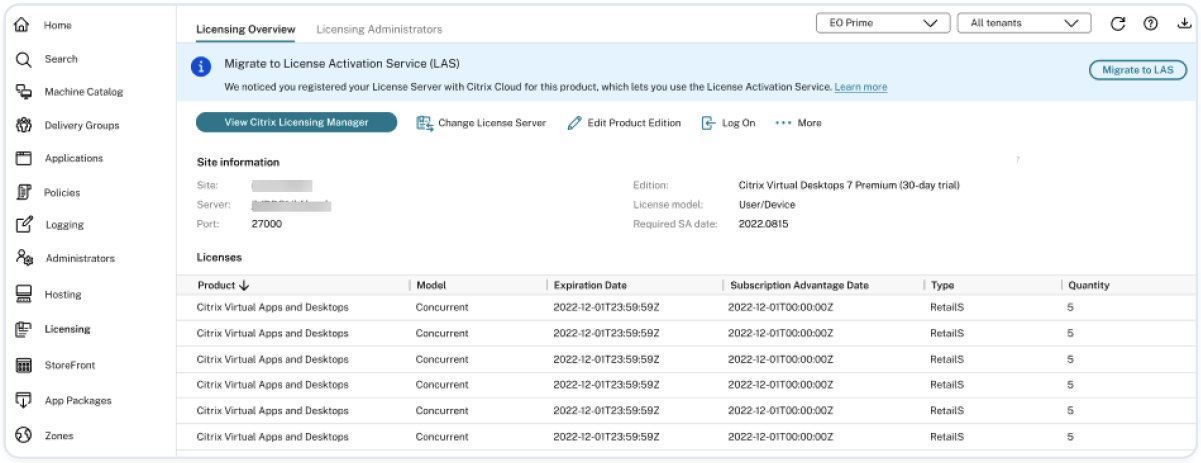
ライセンスサーバーが古いレガシーライセンスをまだ使用しており、Citrix Virtual Apps and Desktops サイトが LAS 対応である場合、Studio はライセンスサーバーを Citrix Cloud に登録するよう促します。

LASを使用するためにライセンスサーバーを登録する(/en-us/citrix-virtual-apps-desktops/2511/media/register-license-server.png)

レガシーライセンスをLASに移行する

ライセンスサーバーを Citrix Cloud に登録済みで、必要なエンタイトルメントがある場合は、ユーザーセッションに影響を与えることなく、既存の Citrix Virtual Apps and Desktops サイトをレガシーライセンスから LAS に移行するために、以下の特定の順序に従う必要があります。

1. **ライセンスサーバーのアップグレード:** ライセンスサーバーをサポートされている最小バージョンにアップグレードします。
2. **Delivery Controller のアップグレード:** サイト内のすべての Delivery Controller を LAS 対応バージョンにアップグレードします。
3. **デリバリーグループのライセンス割り当ての削除:**
   - **Migrate to LAS** をクリックする前に、サイトレベルより下で設定されているライセンス割り当て（つまり、デリバリーグループレベルのライセンス割り当て）を手動で削除します。
4. **割り当ての確認:** LAS の割り当てが正確であることを確認します。
5. **Migrate to LAS をクリック:**
   - 前の手順が完了したら、**Migrate to LAS**をクリックします。



- LASに移行すると、Citrix Virtual Apps and Desktopsサイトの**ライセンスエディション**は**Citrix Virtual Apps and Desktops Premium**に設定され、**ライセンスモデル**は**Concurrent**に構成されます。

LASからレガシーライセンスへのロールバック

LASからレガシーライセンスにロールバックするには、以下を実行します。

1. 次のPowerShellコマンドを実行します。

   ```
   Set-ConfigSite -UseLicenseActivationService $false
   ```

2. Studioでレガシーライセンスを構成します。

注：

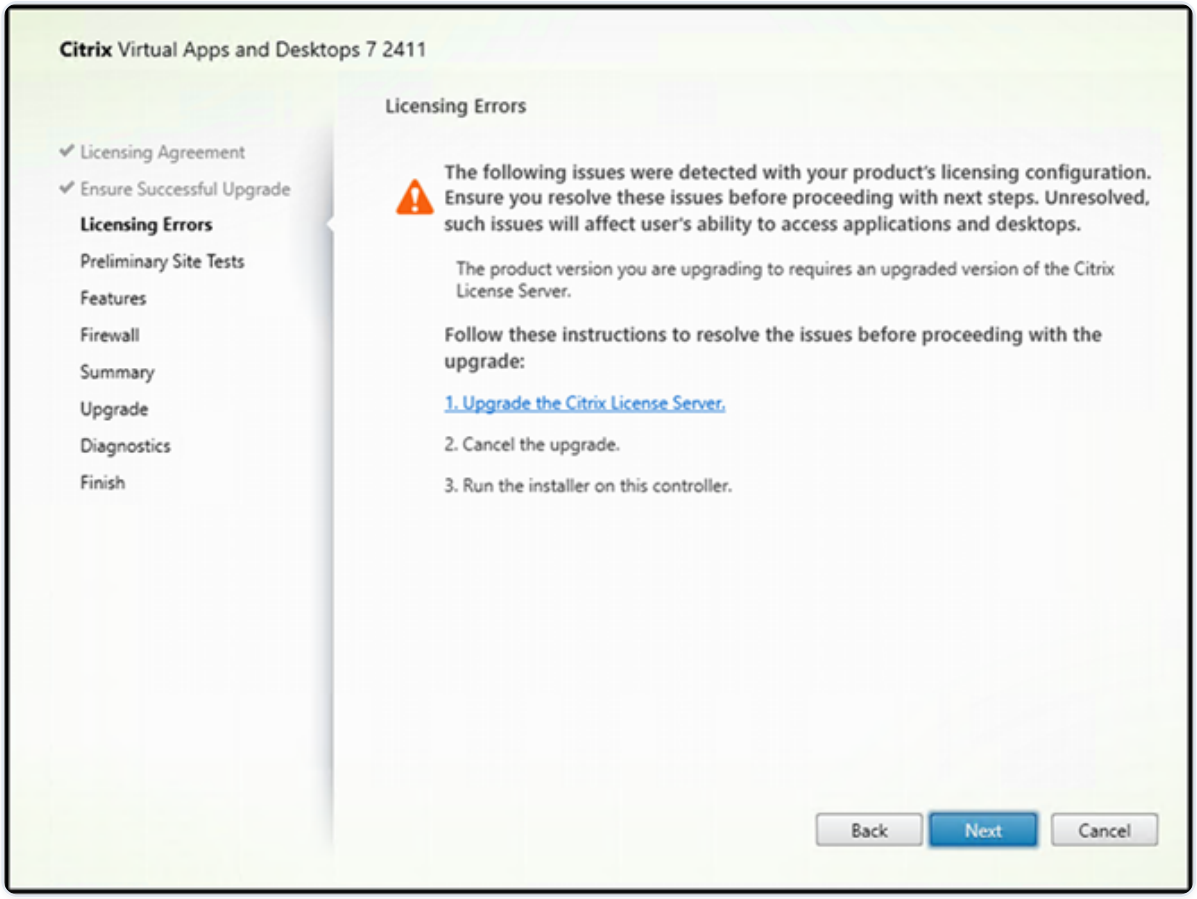
これらの手順は、一時的なトラブルシューティングのみを目的としています。レガシーライセンスファイルは、サポート終了（EOL）が近づいており、April 15, 2026以降は機能しません。中断のないサービスを確保するため、License Activation Service (LAS) への移行をお勧めします。詳細については、お知らせを参照してください。

アップグレードに関する重要な考慮事項

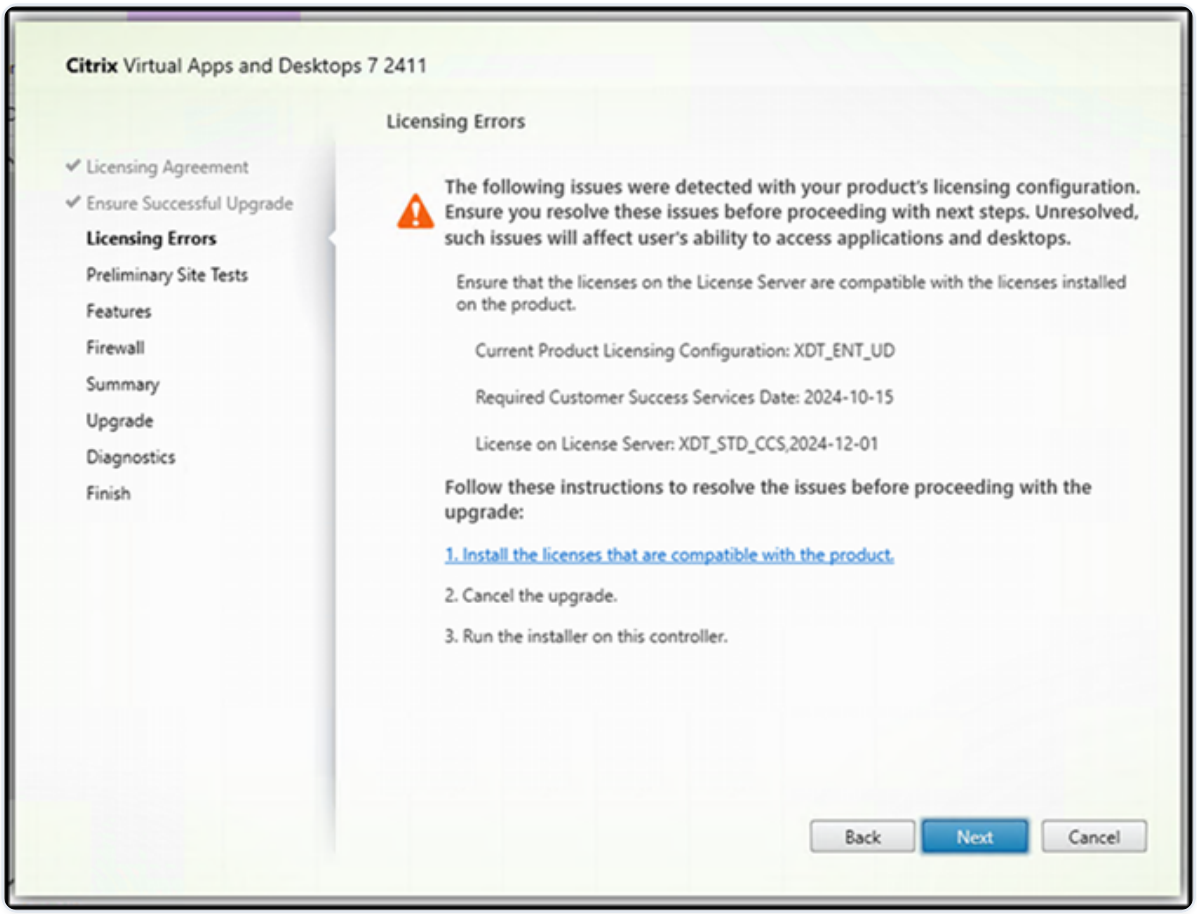
以前のCitrix Virtual Apps and Desktopsバージョンから2411以降にアップグレードする場合は、License Serverを最新バージョン（バージョン11.2.17ビルド53100以降）にアップグレードしてください。

- メタインストーラーUIを使用してアップグレード中に、ライセンスエラーページに次のエラーが表示されます。

- 最新のLicense Serverバージョンにアップグレードしない場合：



- License Serverが古い場合やライセンスが利用できない場合など、互換性のない点がある場合：



- コマンドラインを使用してアップグレードする場合、アップグレードの失敗を避けるために次のコマンドを実行します (マウントされたISOの\x64フォルダー内にいると仮定して)：

1. 次を実行します：

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet
   ```

   ライセンスバイナリをローカルドライブのいずれかにコピーしている場合、次のコマンドを実行します：

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet /l install.log
   ```

2. 次を実行します：

   ```
   \x64\XenDesktop Setup\XenDesktopServerSetup.exe  /components
   "CONTROLLER,WEBSTUDIO,DESKTOPDIRECTOR" /CONFIGURE_FIREWALL
   ```

コアコンポーネントのアンインストール

アップグレード中に、`\x64\Licensing\CitrixLicensing.exe /quiet` または `\x64\Licensing\CitrixLicensing.exe /quiet /l install.log` コマンドを使用して最初にライセンスサーバーをインストールし、その後コアコンポーネントをインストールした場合は、アンインストールも同じ順序で行ってください。

1. コマンドラインを使用してライセンスサーバーをアンインストールします。

   ```
   CitrixLicensing.exe /quiet /uninstall /l uninstall.log
   ```

2. GUIまたはコマンドラインを使用してコンポーネントをアンインストールします。詳細については、コンポーネントの削除を参照してください。

コマンドライン `XenDesktopServerSetup.exe` または `removeall` を使用してライセンスサーバーとコンポーネントをアンインストールする場合は、レジストリエントリと残りのファイルをクリーンアップしてください。

レジストリエントリをクリーンアップするには：

1. レジストリキー `Citrix Licensing` を検索し、そのエントリを削除します。ほとんどの場合、エントリは次の場所で見つかります。

   ```
   "Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Cur
   rentVersion\Uninstall\
   ```

2. レジストリキーの**Uninstall String**が指すフォルダーを削除します。

トラブルシューティング

Citrix Cloudでライセンスサーバーのステータスが緑色以外で表示されている場合は、問題が発生している可能性のあるアクティベーションの詳細を把握するために、次の手順を実行してください。

1. Citrix Cloudで、**ライセンス > ライセンス済み展開 > ライセンスサーバー**に移動します。
2. Citrix Virtual Apps and Desktops の横にある展開ボタン **>** をクリックして、アクティベートされた Delivery Controller のリストを表示します。

   アクティベートされた Delivery Controller のリスト (/en-us/citrix-virtual-apps-desktops/2511/media/las-product-activation1.png)
3. アクティベーションの横にある **View details** をクリックして、詳細情報を表示します。

ID は、アクティベーションを識別するための固有の識別子です。

次の詳細が提供されます。

トラブルシューティングの詳細を表示 (/en-us/citrix-virtual-apps-desktops/2511/media/las-product-activation3.png)

- **製品とバージョン**: LAS でアクティベートする際に製品が使用するように構成されている Product_Edition_Model と Burn In Date。BurnInDate は通常、製品のリリース日です。
- **BrokerServiceGroupUid**: ブローカーサービスグループの UID。
- **Controller UUID**: デリバリーコントローラーの UUID。
- **LasUniqueEnvId**: アクティベーションのために LAS によって提供されるインスタンスの固有 ID。
- **HA-Broker**: HA ブローカーかメインブローカーかを示す True または False。

アクティベートされたホストの詳細を実際のホストにマッピングするには、ホストで次のコマンドを実行します。

- `Get-BrokerSite`: 画面に表示される **BrokerServiceGroupUid** の値を、コマンドの `BrokerServiceGroupId` 出力と比較します。
- `Get-BrokerController`: 画面に表示される **Controller UUID** の値を、コマンドの UUID 出力と比較します。

ライセンスイベントに関連するイベントビューアーログ

イベントID	説明
1112	Citrix Broker Service は、ユーザーからリソースへの接続を仲介できませんでした。このサイトの製品およびエディションのライセンス構成では、このタイプのリソースは許可されていません。このサイトに正しいライセンスが選択されていることを確認してください。
1150	Citrix Broker Service はライセンスサーバーへの接続に成功しました。
1151	Citrix Broker Service はライセンスサーバーに接続できません。ライセンスサーバーが正しく機能していること、およびXenDesktop構成

イベントID	説明
	でライセンスサーバーを識別する詳細が正しいことを確認してください。
1152	このXenDesktopサイトには、ライセンスサーバーに必要な製品ライセンスがありません。ライセンス管理コンソールを使用して、関連する製品ライセンスをライセンスサーバーに追加してください。
1153	このXenDesktopサイトのライセンスの有効期限が切れました。Citrix Broker Service はライセンスサーバーに新しいライセンスを要求します。
1154	このコントローラーは、ライセンスサーバーに接続できなかったため、ライセンスキャッシュモードに入りました。このコントローラーがデスクトップおよびアプリケーションセッションの提供を停止するまで、残り2時間です。
1155	Citrix Broker Service は、デスクトップおよびアプリケーションセッションの提供を停止します。このコントローラーは、ライセンスサーバーとの通信が継続的に失敗したため、ライセンスキャッシュモードではなくなったか、ライセンスキャッシュモードに入ることができませんでした。ライセンスサーバーが機能していることを確認し、必要に応じて、ライセンス管理コンソールを使用して関連するライセンスをライセンスサーバーに追加してください。
1156	Citrix Broker Service はライセンスサーバーと正常に通信しています。このコントローラーはライセンスキャッシュモードではなくなりました。
1157	実行中のライセンスサーバーのバージョンは、Citrix Broker Service のバージョンよりも古いため、互換性がありません。ライセンスサーバーをアップグレードするか、

イベントID	説明
	XenDesktop 構成で正しいバージョンのライセンスサーバーの場所を指定してください。
1158	Citrix Broker Service は、このエディションのこのサイトでライセンスサーバーが利用できるライセンス数を超過していることを検出しました。ライセンスサーバーは、オーバードラフトライセンスを付与しました。
1159	このサイトにインストールされているライセンスの最大数を超過したため、Citrix Broker Service はデスクトップ接続を拒否しました。このエディションには3つのライセンスがインストールされていますが、このエディションで許可されているライセンスの最大数は2つです。ライセンス制限に準拠するために、ライセンスサーバーから関連するライセンスを削除してください。
1160	Citrix Broker Service は、ライセンスの管理中に内部エラーを検出しました。ライセンスサーバーが正しく機能していること、およびXenDesktop構成でライセンスサーバーを識別する詳細が正しいことを確認してください。Citrix Broker Service を再起動すると、問題が解決する場合もあります。この問題が解決しない場合は、Citrix XenDesktop Controller を再インストールしてください。Citrix Knowledge Base の記事 CTX126990 を参照してください。
1161	ライセンスの初期化エラー。ライセンスサーバーの接続を確認してください。
1162	ライセンスの停止エラー。ライセンスサーバーの接続を確認してください。
1163	接続ライセンスがありません。解決するには、不要なセッションを閉じてライセンスを解放するか、ライセンスを追加してください。

イベントID	説明
1164	接続ライセンスのチェックアウト中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1165	接続ライセンスのチェックイン中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1166	ライセンスの可用性確認中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1167	ライセンスの開始に失敗しました。ライセンスサーバーの接続を確認してください。
1168	ライセンスユーザー通知設定の読み取り中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1169	ライセンスサーバーで適切なライセンスが見つからなかったため、このコントローラーは初期設定のライセンスキャッシュモードに入りました。このコントローラーがデスクトップおよびアプリケーションセッションの提供を停止するまで、残り2時間です。
1170	Citrix Broker Serviceは、ライセンスサーバーで適切なライセンスを正常に検出しました。このコントローラーは、初期設定のライセンスキャッシュモードではなくなりました。
1171	ライセンスサーバーが指定されていません。有効なライセンスサーバーが指定されるまで、Citrix Broker Serviceはユーザーにデスクトップとアプリケーションを提供できません。Citrix StudioまたはCitrix PowerShell SDKのSet-ConfigSiteコマンドレットを使用して、ライセンスサーバーを指定できます。
1172	ライセンスサーバーの適合性チェック中にエラーが発生しました。Citrix Broker Service

イベントID	説明
	は、マシンがライセンスサーバーとして使用するのに適しているかどうかを確認する際に、予期しない応答を受け取りました。コントローラーからそのマシンに接続できること、およびそのマシン上のファイアウォールがコントローラーからの接続を許可していることを確認してください。マシンにライセンスサーバーがインストールされている場合は、それが正しく構成され、動作していることを確認してください。
1173	このXenDesktopサイトには、ライセンスサーバーに必要な起動ライセンスがありません。License Administration Consoleを使用して、関連するライセンスをライセンスサーバーに追加してください。
1174	このXenDesktopサイト用に構成された製品エディションはアプリケーションをサポートしていません。アプリケーションリソースは利用できません。
1176	構成された製品エディションは、マルチセッションマシンをサポートしていません。登録は拒否されました。
1177	構成された製品エディションは、シングルセッションマシンをサポートしていません。登録は拒否されました。
1178	構成された製品エディションはRemotePCをサポートしていません。登録は拒否されました。
1179	設定された製品エディションは、クラウドシステムにプロビジョニングされたマシンをサポートしていません。登録は拒否されました。
1180	このXenDesktopサイト用に設定された製品エディションは、シングルセッション（ワークステーションOS）マシン上のアプリケーション

イベントID	説明
	をサポートしていません。アプリケーションリソースの起動は拒否されました。
1181	このXenDesktopサイト用に設定された製品エディションは、マルチセッション（サーバーOS）マシン上のアプリケーションをサポートしていません。アプリケーションリソースの起動は拒否されました。
1182	このXenDesktopサイト用に設定された製品エディションは、シングルセッション（ワークステーションOS）マシン上のデスクトップをサポートしていません。デスクトップリソースの起動は拒否されました。
1183	このXenDesktopサイト用に設定された製品エディションは、マルチセッション（サーバーOS）マシン上のデスクトップをサポートしていません。デスクトップリソースの起動は拒否されました。
1196	このコントローラーは、ライセンスサーバー上の利用可能なすべてのライセンスを使い果たしたため、ライセンスバーストモードに入りました。これを解決するには、さらにライセンスを追加してください。このコントローラーがデスクトップおよびアプリケーションセッションの提供を停止するまで、残り2時間です。
1197	Citrix Broker Serviceは、デスクトップおよびアプリケーションセッションの提供を停止します。このコントローラーは、ライセンスサーバー上のライセンスが不足しているため、ライセンスバーストモードではなくなったか、ライセンスバーストモードに入ることができませんでした。ライセンス管理コンソールを使用して、関連するライセンスをライセンスサーバーに追加してください。

イベントID	説明
1198	Citrix Broker Serviceは、ライセンスサーバーからライセンスを正常に消費しています。現在の需要を満たすのに十分なライセンスがサーバーにあります。このコントローラーは、ライセンス枯渇によって引き起こされたライセンスバーストモードではなくなりました。
1199	Citrix Broker Serviceは、デスクトップおよびアプリケーションセッションの提供を停止します。ライセンスサーバーにライセンスがインストールされていないため、このコントローラーはライセンスキャッシュモードではなくなったか、ライセンスキャッシュモードに入ることができませんでした。ライセンス管理コンソールを使用して、関連するライセンスをライセンスサーバーに追加してください。
1205	ソフトウェアメンテナンスの有効期限が切れました。現在、Citrix環境はサポートされていません。ライセンスサーバーで期限切れのライセンスを確認し、削除してください。ユーザーが警告メッセージを受け取り始める前に、30日間のライセンスキャッシュモードがあります。
1206	ライセンス証明書のハッシュが無効です。Citrixライセンス証明書のハッシュが無効です。
1300	Citrix Broker Serviceは、デスクトップおよびアプリケーションセッションの提供を停止します。ライセンスサーバーのシステムクロックに問題があります。
1301	ライセンスサーバーのシステムクロックに関する問題が修正されました。Citrix Broker Serviceは通常の操作を再開します。
1302	このコントローラーは、接続ライセンスのチェックインまたはチェックアウトに再度失敗しました。以前に検出された障害はまだ存

イベントID	説明
	在します。過剰なイベントログを避けるため、問題が解決されるまで、サービスは関連メッセージ（イベントID 1163、1164、1165）を抑制しています。ライセンス取得の試行は継続されます。
1303	このコントローラーは、関連メッセージ（イベントID 1163、1164、1165）の抑制を停止しました。
1304	Citrix Broker Service は LAS に正常に接続しました。
1305	Citrix Broker Service は LAS に接続できません。LAS が正常に機能していること、および XenDesktop 構成で LAS を識別する詳細が正しいことを確認してください。

詳細情報

サイトのLAS状態の確認、またはサイトがライセンスキャッシュモードであるかどうかの確認については、以下を参照してください。

- サイトの LAS 状態を確認するにはどうすればよいですか？
- サイトがライセンスキャッシュモードであるかどうかを確認するにはどうすればよいですか？

コマンドの詳細については、以下を参照してください。

- Get-BrokerController
- Get-ConfigSite

Citrix Virtual Apps and Desktops™ テレメトリデータ要素

ブローカー

使用方法

ヘッダー

キー	説明	例
バージョン	テレメトリイベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	SendBrokerTelemetryData
st	Brokerでイベントが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
製品	使用イベントの発生元となる製品と展開を識別します。	XenDesktop.Broker (クラウド) OnPrem.Broker (On Prem)
prodVer	Citrix DaaS/Citrix Virtual Apps and Desktops の製品バージョンを示します。	7.25.0.0

ペイロード

フィールド	説明	例
TotalPublishedApps	公開されているアプリケーションの総数を示します。	10
TotalPublishedDesktops	公開されているデスクトップの総数を示します。	10
VDAs.Total	VDAの総数を示します。	10
VDAs.OSTypes	Windows、Linux、MacなどのOSタイプ別のVDAの総数を示します。	10
VDAs.OSVersions	Windows 10、11、2022、2019などのOSバージョン別の総数を示します。	10
VDAs.HostingLocations.Azure	Azure、AWS、GCP、Nutanix、VMWare、XenServer、HyperVなど、サポートされている各ホスティングロケーションのVDA数を示します。	10
VDAs.HostingLocations.AWS		
VDAs.HostingLocations.Nutanix		
VDAs.HostingLocations.VMWare		
VDAs.HostingLocations.XenServer		
VDAs.HostingLocations.HyperV		
VDAs.ProvisionedMethod.MCS	Machine Creation Service (MCS) によってプロビジョニングされたマシンの数を示します。	10

フィールド	説明	例
VDAs.ProvisionedMethod.ManualOr3P	手動または3Pでプロビジョニングされたマシンの数を示します。	10
VDAs.SessionSupport.StaticSingle	静的に割り当てられたシングルセッションのマシンの数を示します。	10
VDAs.SessionSupport.DynamicSingle	動的に割り当てられたシングルセッションのマシンの数を示します。	10
VDAs.SessionSupport.Multi	マルチセッションマシンの総数を示します。	10
VDAs.RemotePCAccess.Windows	OSタイプ別 (Windows、Mac、Linux) のRemote PC Access マシンの数を示します。	10
VDAs.RemotePCAccess.Linux		
VDAs.RemotePCAccess.MacOS		
VDAs.ActiveSessionRecordingAgents	アクティブなセッション記録エージェントを持つVDAの数を示します。	5
VDAs.Subscriptions	VDAのパブリッククラウドサブスクリプションの数を示します。	2
VDAs.LocationTypes	VDAのロケーションタイプの数を示します。	2
AutoScale.DGWithAutoscaleEnabled	**Autoscale** が有効になっているデリバリーグループの数を示します。	2
AutoScale.TotalMachinesCtrlByAutoscale	Autoscaleによって制御されるマシンの数を示します。	5

フィールド	説明	例
AutoScale.VerticalAutoscaleEnabledByDGandSite	DGとサイトによって**Vertical Autoscale**が有効になっているマシンの数を示します。	2
AutoScale.TaggedBasedAutoscaledDG	タグベースのAutoscaleが適用されたデリバリーグループの数を示します。	2
DeliveryGroup.TotalRebootSchedulesEnabled	**再起動スケジュール**が有効になっているデリバリーグループの数を示します。	2
DeliveryGroup.Total	デリバリーグループの総数を示します。	10
Policy.TotalPolicySets	ポリシーセットの数を示します。	3
Policy.TotalPolicies	グループポリシーの数を示します。	2
Policy.TotalPolicySettings	グループ設定の数を示します。	2
PublishedPackageApps.AppVSingleAdmin	AppVシングルアドミンモードで公開されているパッケージアプリの総数を示します。	2
PublishedPackageApps.AppVDualAdmin	AppVデュアルアドミンモードで公開されているパッケージアプリの総数を示します。	2
PublishedPackageApps.Msix	MSIXモードで公開されているパッケージアプリの総数を示します。	2
PublishedPackageApps.AppAttach	AppAttachモードで公開されたパッケージ化されたアプリの総数を示します。	2

フィールド	説明	例
PublishedPackageApps.FlexApp	FlexAppモードで公開されたパッケージ化されたアプリの総数を示します。	2

セッション

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	Citrix Analytic Serviceがクラウド使用状況イベントを識別するために使用するイベントの種類を示します。	Cloud.Licensing
st	イベントがBrokerで生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
製品	使用状況イベントの元の製品と展開を識別します。	XenDesktop.Broker (クラウド) OnPrem.Broker (OnPrem)
prodVer	Citrix DaaSまたはCitrix Virtual Apps and Desktopsの製品バージョンを示します。	7.25.0.0

フィールド	説明	例
ユーザー	セッション起動を開始するユーザーを一意に識別するユーザーIDを特定します。**値はスクランブルされます。**	fullName: C648FE671A44B3F7 **(常にスクランブルされます)** samName:C758LH671A44B3F7 **(常にスクランブルされます)** upn: C7948FE671A44B3F7 **(常にスクランブルされます)** userLicenseId:C265FE671A44B3F7 **(常にスクランブルされます)** userSid: C097FE671A44B3F7 **(常にスクランブル化されています)**
テナント -> ID	Citrix Cloud™ アカウントの顧客IDを示します。オンプレミス展開の場合、このフィールドは適用されず、値はありません。	ジョジイチエムゼロゴキュウハチティージェイ
dvc から dvcId	セッション起動が開始されたデバイスを一意に識別するためのデバイスIDを示します。	AE18C4D5

フィールド	説明	例
dvc から dvcName	デバイスのフレンドリ名を示します。**値はスクランブル化されています。**	C758LH671A44B3F7 **(常にスクランブル化されています)**

ペイロード

フィールド	説明	例
appProtectionKeyLoggingRequired	セッションがキーロギング保護を有効にして起動されたかどうかを示します。	偽
appProtectionScreenCaptureRequired	セッションが画面キャプチャ保護を有効にして起動されたかどうかを示します。	偽
cspTenantCustomerId	CSPテナントのCitrix Cloudアカウントの顧客IDを示します。オンプレミス展開の場合、このフィールドは適用されず、値はありません。	ロクシーツーブイティーエックスジーエックスワイエフティーティー
isAnonymousUser	認証されていないセッションが起動されたかどうかを示します。	偽
licenseActivityTimeStamp	ペイロードが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
licenseActivityType	ライセンスイベントの種類を示します。このフィールドは、ライセンスイベント	接続

フィールド	説明	例
	の種類が割り当てアクションか解放アクションかを示します。	
licenseModel	展開のライセンスモデルを示します。	UserDevice
productEdition	展開の製品エディションを示します。	プレミアム
productId	展開内の製品の製品IDを示します。	CAVDS
プロトコル	セッションの起動に使用されたプロトコルを示します。	HDX™
sessionKey	セッションの一意の識別子を示します。	uq390c5fc3-86eb-4df3-bd9a-f4a8fed2c9e2
sessionSupport	セッションサポートの種類を示します。	SingleSession
sessionType	セッションの種類を示します。	アプリケーション
バージョン	ペイロードのバージョンを示します。	1.3
workerSid	セッションに使用されるVDAの一意の識別子を示します。**値はスクランブル化されています。**	1E5LH671A44B3F7 **(常にスクランブル化されています)**
isWindows365	セッションがWindows 365向けに起動されたかどうかを示します。	はい

フィールド	説明	例
entitlementType	お客様のライセンスエンタイトルメントタイプを示します。	本番
siteId	サイトの一意の識別子を示します。	a35647d0-901c-4477-87e0-dcd781d455f4
desktopGroupId	デスクトップまたはデリバリーグループの一意の識別子を示します。	e9d859dc-1bfc-4b3e-bad3-41806bb4e694
clientType	Citrix Workspace™ アプリのタイプを示します。	ウィンドウズ
clientVersion	Citrix Workspaceアプリのバージョンを示します。	23.5.1.83
workerCloudType	VDAプロビジョニングに使用されるパブリッククラウドの種類を示します。	アジュール
enabledFeatures	セッションで有効になっている機能を示します。たとえば、`AppProtectionScreenCaptureRequired` と `SessionRecording` が有効になっているセッションでは、このフィールドの値は66です。	66
launchRequestSource	起動を要求するために使用された製品を記録します。オンプ	0 (StoreFrontまたは3P)

フィールド	説明	例
	レミスStoreFront™またはCloud StoreFrontのいずれかです。	1 (ワークスペース)
isEvents	{{page.lic}}における重大な障害を示します。	STデータベースを作成できません。
heartBeatTime	CISまたはCitrix Analytic Serviceへのライセンスサーバーのハートビート時間を示します。	1689058813
vdaTelemetry	App Layering、ユーザーパーソナライゼーションレイヤー、ユーザープロファイル管理、Workspace Environment Management™、およびHDX機能のためにキャプチャされたペイロードを示します。	vdaTelemetry SessionTelemetry CPM機能: 32 HDX1: 66 HDX2: 0 MachineTelemetry AL_productVersion: 23.12.0.1001 UPL_isEnabled: 1 CPM_version: 22.3.4000 wem_enableMethod: 1 wem_agentVersion: 2402.1

スタジオ

使用方法

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	8c2e20a5-ca3f-4401-ad69-d037933c40a0
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	Studio.Usage
st	Studio でイベントが生成されたときのタイムスタンプを示します。	2024-03-22T01:32:23.4056195Z
製品	使用状況イベントの発生元製品と展開を識別します。	XenDesktop.Studio
prodVer	Citrix DaaS/Citrix Virtual Apps and Desktops の製品バージョンを示します	7.42.0.0

ペイロード

フィールド	説明	例
AdminLoginList	一意の管理者SamAccountNameのリストを示します。**値はスクランブルされています。**	{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw= =]}**(常にスクランブルされます)**
TotalApiRequests	オーケストレーションサービスのAPIリクエストを示します。	{TotalApiRequests: 1000}

フィールド	説明	例
BackupCount	Studio管理者によって操作されたバックアップの数を示します。	{BackupCount: 200}
RestoreCount	Studio管理者によって実行されたリストアの回数を示します。	{RestoreCount: 20}

ディレクター

使用状況レポート

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	8c2e20a5-ca3f-4401-ad69-d037933c40a0
タイプ	Citrix Analytic Serviceがクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	テレメトリ
st	Studioでイベントが生成されたときのタイムスタンプを示します。	2024-03-22T01:32:23.4056195Z
製品	使用状況イベントの発信元の製品と展開を識別します。	XenApp.Monitor
prodVer	Director製品バージョンを示します。	7.42.0.0
dvcName	サーバーの名前	C758LH671A44B3F7

ペイロード

フィールド	説明	例
AdminLoginCount	これは、管理者ログインの数を提供するペイロードのセクションです。	type: 管理者ログイン統計 0: 1 1: 7
FeatureUsageCount	このペイロードのセクションには、Directorで使用されている主要な機能の数が含まれています。	タイプ: FeatureUsage 統計 0: 15 1: 20 5: 10
OdataUsageCount	ペイロードのこのセクションには、Odata API の使用状況のカウントが含まれています。	タイプ: OData_v3 統計情報 0: 1 2: 7 5: 9 タイプ: OData_v4 統計 0: 1 2: 8 6: 7
AppUsage	公開されたアプリケーションの週ごとの使用状況メトリックを示します。	タイプ: AppUsage ヘッダー: applicationName,pr

フィールド	説明	例
		ocessName,totalDurationInMinutes 期間: 01/05/24-07/05/24 値: [Calc_AWTSVDA-1907R,calc.exe,0.13, Notepad_AWTSVDA-1907R,notepad.exe,4]
UniqueAppUsers	公開されたアプリケーションについて、1か月あたりのユニークユーザー数とアプリケーションの合計起動回数を表します。	タイプ: UniqueAppUsers ヘッダー: applicationName,totalLaunches,totalUniqueUsers 期間: 04/24 値: [Calc_AWTSVDA-1907R,100,10, Notepad_AWTSVDA-1907R,200,20]
DesktopUsage	公開されたデスクトップの週ごとの使用状況メトリックを示します。	タイプ: デスクトップ使用状況 ヘッダー: デスクトップグループ名,セッションサポート,合計継続時間（分）

フィールド	説明	例
		期間: 01/05/24-07/05/24 値: [RdsDesktopAndAppGroup,1,10]
UniqueDesktopUsers	公開デスクトップについて、1か月あたりの総起動回数とともにユニークユーザーの数を表します。	種類: UniqueDesktopUsers ヘッダー: desktopGroupName,totalLaunches,totalUniqueUsers 期間: 04/24 値: [RdsDesktopAndAppGroup,10,5]
AvgLogonDuration	平均ログオン時間を示します。	タイプ: AvgLogonDuration ヘッダー: totalUserLogons, avgLogonDurationInSeconds 期間: 01/05/24-07/05/24 値: [200,4]
CostSaved	顧客が1ヶ月間に節約したコストを示します。	タイプ: CostSaved

フィールド	説明	例	
		ヘッダー: ハイパーバイザー,コストセーブ,通貨 期間: 04/24 値: [1,221.02,1 2,301.02,2]	

Storefront の構成

使用方法

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1.0
id	使用イベントの一意の識別子を示します。	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	CAS がクラウド使用状況イベントを識別するために使用するイベントの種類を示します。	構成
st	StoreFront でイベントが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
本番	使用イベントの発生元の製品と展開を識別します。	OnPrem.StoreFront
prodVer	StoreFront のバージョン (内部) を示します。	3.30.0.0

ペイロード

フィールド	説明	例
serverName	StoreFrontが稼働しているサービスのホスト名を示します	storefront-01.storefront.local
deploymentId	StoreFrontの展開の一意の識別子を示します	f47ac10b-58cc-4372-a567-0e02b2c3d479
installedWithCVAD	StoreFrontがCVADと同時にインストールされたかどうかを示します。	偽
cpuCores	CPUコアの総数を示します。	4
cpuModel	StoreFrontを実行しているCPUを示します。	第12世代 Intel(R) Core(TM) i7-1255U 1.70 GHz
ramGb	RAMの総容量（GB単位）を示します。	16
numServersInGroup	サーバーグループ内のサーバー数を示します。	3
ストア	StoreFrontストア構成JSONブロブを示します。Storeオブジェクトの配列です。**一部の値はスクランブルされています**	例
rfWebSites	StoreFront RFWeb構成JSONブロブを示します。RFWeb Configオブジェクトの配列です。	例
ゲートウェイ	ゲートウェイ構成オブジェクトをJSONブロブとして示します。ゲートウェイオブジェクトの配列です。	例
authServices	認証サービス構成オブジェクトをJSONブロブとして示し	例

フィールド	説明	例
	ます。認証サービスオブジェクトの配列です。	
IsPiiScrambled	真	

フィールド STORES の例

```
[{
            "BaseUrl": "baseUrl",
            "StorePath": "/",
            "EnabledFeatures": 21 bit bitmap,
            "ResourceTypeFilteringEnabled": "disabled|
Citrix.MPS.Application;Citrix.MPS.Desktop",
            "DefaultRfWebSite": "/Citrix/StoreWeb",
            "GatewaysUsed": [
                "gatewayId"
            ],
            "VdaLogonDataProvider": "",
            "ResourceFeeds": [
                {
                    "FeedName": "<resourceFeedName>|scrambled",
                    "Type": "CVAD",
                    "LoadBalancingEnabled": true,
                }
            ],
```

```
            "AdvancedAggregation": {
                "Enabled": true,
                "GroupingCount": 1,
                "ControllersPushIdenticalResources": true,
                "LoadBalanced": true,
                "AnyPrimaryFarms": true,
                "AnyBackupFarms": true,
            }
}]
```

ストアが見つからない場合、それは空の配列になります 。

フィールド RFWEBSITES の例

```
[{
    "SiteId": "siteId",
    "BaseUrl": "baseUrl",
    "StorePath": "storePath",
    "UiExperienced": 0,
    "EnabledFeatures": 9 bit,
    "AuthMethodsEnabled": [
        "ad"
    ],
    "CanUsersDownloadApps": {
        "Enabled": true,
```

```
        "Windows": "exe",
        "MacOS": "dmg"
    },
    "WorkspaceControl": {
        "Enabled": true,
        "LogoffAction": 0,
        "AutoReconnectAtLogon": true,
        "ShowReconnectButton": true,
        "ShowDisconnectButton": true
    },
    "MultiClickTimeout": 1,
    "UiViews": [
        "apps",
        "desktops"
    ],
    "DefaultTab": 0,
}]
```

rfWebサイトが見つからない場合、それは空の配列になります 。

フィールド GATEWAYS の例

```
[{
            "GatewayId": "gatewayId",
            "IsCloudGateway": true,
```

```
            "LoadBalancingSTAEnabled": true,

            "SessionReliabilityEnabled": true,

            "RequestTicketsFromTwoSTA": true,

            "Version": "1234",

            "LogonType": "domain",

            "SmartCardFallbackEnabled": true

}]
```

ゲートウェイが見つからない場合、それは空の配列になります 。

フィールド AUTHSERVICES の例

```
[{

    "SiteId": "SiteId",

    "Store": "StoreAuth",

    "AuthMethodsEnabled": [

        "ad"

    ],

    "PasswordChangeWhenExpired": 0,

    "PasswordRemindersForm": 1,

    "DelegateCredentialValidationToCitrix": true,

    "ValidatePasswordsOnDeliveryControllers": true

}]
```

認証サービスが見つからない場合、それは空の配列になります 。

ストアフロントログイン

使用方法

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します	1.0
ID	使用イベントの一意の識別子を示します	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	CASがクラウド使用イベントを識別するために使用するイベントタイプを示します	ログイン
st	Brokerでイベントが生成されたときのタイムスタンプを示します	2011-08-12T20:17:46.384Z
製品	使用イベントの発生元となる製品と展開を識別します	OnPrem.StoreFront
prodVer	StoreFrontバージョン (内部)	3.30.0.0

ペイロード

フィールド	説明	例
ユーザー	起動を開始したユーザー。**値はスクランブル化されています**	fullName: C648FE671A44B3F7 **(常にスクランブル化されています)** samName:C758LH671A44B3F7 **(常にスクランブル化されています)** upn: C7948FE671A44B3

フィールド	説明	例
		F7 **(常にスクランブル化されています)** userLicenseId:C265FE671A44B3F7 **(常にスクランブル化されます)** userSid:C097FE671A44B3F7 **(常にスクランブル化されます)**
serverName	StoreFrontが実行されているサービスのホスト名を示します	ストアフロント-01.ストアフロント.ローカル
loginMethodRfWeb	ユーザーがRFWebからStoreFrontにログインするために使用した方法を示します	0
loginMethodAuth	ユーザーがAuthサービスからStoreFrontにログインするために使用した方法を示します	0
gatewayURL	ログイン時に使用されたNetscaler Gatewayを示します	ネットスケーラー-ゲートウェイ.コム
enabledFeatures	有効な機能のビットマスクを示します	12
userAgent	ログインに使用されたクライアントのUserAgentを示します	CitrixReceiver/22.11.0.19 リナックス/5.17.15 X1クラスCWA対応 CWA/22.11.0.19

フィールド	説明	例
baseUrl	ユーザーがログインしたストアを示します	storefront-dev.storefront.dev
storePath	ユーザーがログインしたストアを示します	/Citirx/StoreWeb
apiUsed	クライアントがStore APIまたはPNAgent APIを使用しているかどうかを示します	0
deviceId	StoreFrontへのログインに使用されるデバイスを示します。**値はスクランブルされています**	ジョン・ドウ
transactionId	単一のトランザクション中に送信/生成されるトランザクションIDを示します	773aba9e-5b91-4ef9-8782-c4afb75698e7

委任管理

使用方法

ヘッダー

キー	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	8c2e20a5-ca3f-4401-ad69-d037933c40a0
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別	DelegatedAdmin.Usage

キー	説明	例
	するために使用するイベントタイプを示します。	
st	Delegated Admin でイベントが生成されたときのタイムスタンプを示します。	2024-03-22T01:32:23.4056195Z
製品	使用状況イベントの発生元となる製品と展開を識別します。	XenDesktop.DelegatedAdmin (クラウド) OnPrem.DelegatedAdmin (OnPrem)
prodVer	Citrix DaaSまたはCitrix Virtual Apps and Desktopsの製品バージョンを示します。	7.42.0.0

ペイロード

キー	説明	例
TotalCustomScopes	カスタムスコープの合計数を示します。	2
TotalCustomRoles	カスタムロールの合計数を示します。	4

ライセンステレメトリデータをスクランブルする

ライセンス テレメトリで送信される情報の機密性を考慮し、Citrix はデータのスクランブルを行うオプションを提供します。

次の表に、スクランブル可能なデータを示します。

フィールド	説明	例
ユーザー	セッション起動を開始するユーザーを一意に識別するためのユーザー ID を示します。	• fullName: `C648FE671A44B3F7`

フィールド	説明	例
		• samName: `C758LH671A44B3F7` • ユーザープリンシパル名: `C7948FE671A44B3F7` • userLicenseId: `C265FE671A44B3F7` • userSid: `C097FE671A44B3F7`
デバイス -> デバイス名	デバイスのフレンドリ名を示します。	`C758LH671A44B3F7`
workerSid	セッションに使用されるVDAの一意の識別子を示します。	`1E5LH671A44B3F7`
AdminLoginList	一意の管理者SamAccountNameのリストを示します	`{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw= =]}`
ストア	StoreFrontストア構成のJSONブロブを示します。ストアオブジェクトの配列です。**一部の値はスクランブルされています**	例
deviceId	StoreFrontへのログインに使用されるデバイスを示します。	ジョン・ドウ

スクランブルを有効または無効にするには、Delivery Controllerで次のPowerShellコマンドを実行します。

注:

Citrix Service Provider™ (CSP) のお客様の場合、スクランブルは常に無効になっています。CSP のお客様は、PowerShell コマンドを使用してスクランブルを有効にすることはできません。

1. Delivery ControllerホストからPowerShellウィンドウを開きます。
2. コマンド `asnp citrix` を実行して、Citrix固有のPowerShellモジュールをロードします。
3. スクランブルを有効または無効にするには、次のコマンドを実行します。

   デフォルトでは、値は`1`または`true`であり、ライセンステレメトリデータのスクランブルを有効にします。

   無効にするには:

   ```
   Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
   -SettingValue $false
   ```

   スクランブルを無効にした後、次のコマンドを使用して有効にできます。

   ```
   Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
   -SettingValue $true
   ```

ライセンスに関するFAQ

注記:

- COVID-19パンデミックに関連する事業継続リソースについては、CTX27055を参照してください。
- 事業継続の維持に関する一般情報については、Business continuity — on demandを参照してください。

- 現在のCitrix License Serverの詳細については、Licensingを参照してください。

Citrix® ライセンス

License Activation Service とは何ですか?

License Activation Service (LAS) は、オンプレミスのCitrix License Server向けの最新のクラウドベースのライセンスソリューションです。これは、従来のファイルベースのライセンス方式に代わる合理化された方法を提供します。

ライセンスファイルを手動でアップロードする代わりに、ライセンスサーバーをCitrix Cloud™に接続してオンラインアクティベーションを行うことができます。これにより、ライセンスが自動的にライセンスサーバーに配信され、ライセンスファイルのライフサイクル管理が不要になります。

クラウドに接続できないライセンスサーバー向けに、LASはオフラインアクティベーションオプションも提供しており、さまざまなネットワーク環境に柔軟に対応できます。このサービスは、Citrix製品ライセンスを管理するためのシームレスで最新のアプローチを導入します。

詳細については、License Activation Serviceを参照してください。

ライセンスファイルはどのように入手できますか?

ライセンスアクセスコードは電子メールで送信されます。ライセンスアクセスコードを使用してライセンスファイルを生成する方法は3つあります。

- `citrix.com` のMyAccountページにある**Manage Licenses**。詳細については、Manage licenses on citrix.comを参照してください。
- Web Studioでご購入を割り当てると、ライセンスファイルがCitrix License Serverに自動的にインストールされます。
- Citrix License Server内のCitrix Licensing Managerを使用して、購入を割り当て、ライセンスファイルをインストールします。詳細については、ライセンスのインストールを参照してください。

myaccountでライセンスを割り当てる方法?

ライセンスの割り当てを参照してください。

割り当てられたライセンスをライセンスサーバーに追加する方法?

ライセンスの変更を参照してください。

Citrixライセンスはどのポートを使用しますか?

- ライセンスサーバーのポート番号は27000です
- ベンダーデーモンのポート番号は7279です
- ライセンス用Webサービスのポートは8083です

Citrix License Serverとは何ですか?

Citrix License Serverは、ネットワーク全体でライセンスを共有できるシステムです。詳細については、ライセンス操作の概要を参照してください。

Citrix License Serverを仮想化またはクラスター化できますか?

はい。Citrix License Serverを仮想化またはクラスター化できます。詳細については、クラスター化されたライセンスサーバーを参照してください。

Citrix License Serverを仮想化した場合、どのような利点がありますか?

Citrix License Serverを仮想化すると、冗長なソリューションが提供されます。そのソリューションにより、ダウンタイムなしで複数の物理サーバー間を移動できます。

Citrix License Serverを仮想化する場合に考慮すべき制限はありますか?

いいえ。

Citrix License Serverは、Citrix Virtual Apps and Desktops™展開のすべてのライセンスを管理しますか?

Citrix License Serverは、Citrix Virtual Apps™ and Desktop用に受け取るすべてのライセンスを管理しますが、Citrix Gatewayで使用されるPremium Editionのライセンスは除きます。これらのセキュリティ指向のネットワークデバイスに必要な、ネットワークアプライアンスに組み込まれたライセンスサーバーが、それらのライセンスを管理します。

Citrix Licensing Managerとは何ですか?

Citrix Licensing Managerを使用すると、Citrix Licensing ManagerをインストールしたLicense Serverからライセンスファイルをダウンロードして割り当てることができます。Citrix Licensing Managerは、推奨されるLicense Server管理方法であり、次のことを可能にします。

- License ServerのCitrix Cloudへのショートコード登録と、登録の簡単な削除。
- ユーザーアカウントとグループアカウントの構成。
- ダッシュボードを使用して、インストール済み、使用中、期限切れ、利用可能なライセンス、およびCustomer Success Servicesの日付を表示する。
- レポート作成のためにライセンス使用状況データをエクスポートする。

- 履歴使用状況データの保持期間を構成する。デフォルトのデータ保持期間は180日です。
- ライセンスアクセスコードまたはダウンロードしたファイルを使用して、License Serverにライセンスファイルを簡単にインストールする。
- ライセンスバーストモードを有効または無効にする。
- カスタマーエクスペリエンス向上プログラム (CEIP) とコールホームを構成する。
- Customer Success Servicesの更新ライセンスを自動または手動で確認し、見つかった場合は通知またはインストールする。
- ライセンスサーバーの状態（起動ライセンスの不足、時間に関する問題、アップローダーの失敗）を通知します。
- 次のポートを変更します。
  - ライセンスサーバー（デフォルト 27000）
  - ベンダーデーモン（デフォルト 7279）
  - ライセンス用Webサービス（デフォルト 8083）

詳細については、Citrix Licensing Managerを参照してください。

Citrix License Administration Consoleはどこにありますか?

License Administration Consoleはサポートされなくなり、License Serverバージョン11.16.6から削除されました。Citrix Licensing Managerの使用をお勧めします。

ライセンスサーバーがStudioと同じドメイン内、または信頼されたドメイン内にある場合、Studioを使用してライセンスを管理および追跡できます。

詳細については、Citrix Licensing Managerを参照してください。

ライセンス割り当て期間?

ライセンス割り当て期間とは、Citrix Virtual Apps and Desktopsライセンスがユーザーまたはデバイスに割り当てられる期間のことです。デフォルトのライセンス割り当て期間は90日間です。

組織が購入したライセンス数の確認方法?

購入したすべてのライセンスは、`<https://www.citrix.com>`の**My Account**ページにある安全な**Manage Licenses**ツールボックスから、いつでも（24時間365日）確認およびアクセスできます。

現在使用中のライセンス数を確認する方法?

Citrix Licensing ManagerとStudioは、リアルタイムのライセンス使用状況に関する詳細情報を提供します。

ライセンスサーバーのディザスターリカバリとメンテナンス

ライセンスサーバーのディザスターリカバリとメンテナンスについては、Citrix Licensingのドキュメントの「ディザスターリカバリとメンテナンス」を参照してください。

Citrix Virtual Apps and Desktopsのライセンス

Citrix Virtual Apps and Desktopsはどのようにライセンスされますか?

Citrix Virtual Apps and Desktops のライセンスには、ユーザー単位およびデバイス単位のモデルと、同時接続モデルがあります。

ユーザー/デバイス:

柔軟なユーザー/デバイスモデルは、以下と連携します。

- 全社的なデスクトップ利用。
- 基盤となるMicrosoftデスクトップ仮想化ライセンス。
- 仮想デスクトップとアプリへのアクセスが時々しか必要ないユーザーを持つ顧客向けの同時使用ライセンス。

ユーザー/デバイスライセンスにより、ユーザーは無制限のデバイスから仮想デスクトップとアプリにアクセスできます。デバイスライセンスにより、無制限のユーザーが単一のデバイスから仮想デスクトップとアプリにアクセスできます。このアプローチは、最大限の柔軟性を提供し、Microsoftデスクトップ仮想化ライセンスとの整合性を向上させます。

> **重要:**

> ライセンスをユーザーまたはデバイスに手動で割り当てることはできません。ライセンスサーバーまたはクラウドサービスがライセンスを割り当てます。ユーザー/デバイスライセンスでは、一度割り当てられたライセンスは、90日間非アクティブになるまで別のユーザーに割り当てることはできません。

> **同時使用:**

同時使用ライセンスは、任意のユーザーおよび任意のデバイスに対して、無制限の数の仮想アプリおよびデスクトップへの1つの接続を許可します。ライセンスはアクティブなセッション中にのみ消費されます。セッションが切断または終了した場合、ライセンスはプールに戻されます。

ユーザー/デバイスライセンスの詳細については、ユーザー/デバイスライセンス を参照してください。同時使用ライセンスについては、同時使用ライセンス を参照してください。

ライセンスを購入する前にCitrix Virtual Apps and Desktopsを試用することはできますか?

はい。Citrix Virtual Apps and Desktopsソフトウェアをダウンロードし、試用モードで実行できます。試用モードでは、ライセンスなしで、30日間、10接続までCitrix Virtual Apps and Desktopsをオンプレミスで使用できます。詳細については、「評価版ライセンス」を参照してください。

Citrix Cloud向けのCitrix DaaS™（旧Citrix Virtual Apps and Desktopsサービス）は、承認に基づき試用サービスとして利用できます。詳細については、Citrix担当者にお問い合わせください。

CitrixはCitrix Virtual Apps and Desktopsの同時使用をどのように定義していますか?

Citrix Virtual Apps and Desktopsの同時使用モデルでは、任意のユーザーおよび任意のデバイスに対して、無制限の数の仮想アプリとデスクトップへの接続を1つ許可します。ライセンスはアクティブなセッション中にのみ消費されます。セッションが切断または終了すると、ライセンスは再発行のためにプールに返却されます。詳細については、「同時使用ライセンス」を参照してください。

共通のライセンスサーバーにCitrix Virtual Apps and Desktopsライセンスの複数のエディションを展開できますか?

はい。ライセンスサーバーは、Citrix Virtual AppsとCitrix Virtual Apps and Desktopsの両方のライセンスを同時に管理します。最新のライセンスサーバーバージョンをインストールすることをお勧めします。お使いのライセンスサーバーバージョンが最新であるか不明な場合は、Citrixダウンロードサイトの番号と比較して確認してください。

単一のサイトでCitrix Virtual AppsとCitrix Virtual Apps and Desktopsの両方のライセンスを使用できます?

バージョンによっては、単一のCitrix Virtual AppsまたはCitrix Virtual Apps and Desktopsサイトで、ユーザー/デバイスまたは同時使用の両方のライセンスモデルをサポートできます。単一のCitrix Virtual AppsまたはCitrix Virtual Apps and Desktopsサイトでサポートできるエディションは1つだけです。詳細については、「複数タイプのライセンス」を参照してください。

複数タイプのライセンスをサポートする最小バージョンは、XenApp and XenDesktop 7.15 Long Term Service Release (LTSR) および Citrix Virtual Apps and Desktops 7 1808 です。

ライセンスサーバーにCitrix Virtual Apps and Desktopsユーザー/デバイスまたはCitrix Virtual Apps and Desktops同時接続ライセンスがインストールされている場合、製品モデルとしてCitrix Virtual Apps同時接続を選択できます?

Citrix Virtual AppsをCitrix Virtual Apps and Desktops AdvancedまたはPremium Editionの機能として使用する場合、Citrix Virtual Appsのライセンスモデルは、Citrix Virtual Apps and DesktopsのAdvancedまたはPremium Editionと同じになります。Citrix Virtual Apps and Desktopsを購入した場合、Citrix Virtual Appsの機能のみを使用する予定であっても、ライセンスをCitrix Virtual Apps

and Desktopsとして構成してください。製品モデルとしてCitrix Virtual Appsを選択するのは、ライセンスサーバーにCitrix Virtual Appsの同時使用スタンドアロンライセンスがインストールされている場合のみです。

各Citrix Virtual AppsおよびCitrix Virtual Apps and Desktopsエディションには、どのような製品コンポーネントが含まれていますか?

エディションごとの全機能マトリックスについては、Citrix Virtual Apps and Desktops featuresを参照してください。

Citrix Virtual Apps and Desktops EULAに準拠して、Citrix Virtual Desktops™環境のライセンスを付与するにはどうすればよいですか?

Citrix Virtual Apps and Desktops EULAに準拠して、ユーザー/デバイスまたは同時接続ライセンスモデルでCitrix Virtual Apps and Desktopsを展開するには、ライセンスファイルをライセンスサーバーに適用します。ライセンスサーバーは、ライセンスコンプライアンスを制御および監視します。購入した製品に基づいて製品を構成することをお勧めします。たとえば、Citrix Virtual Apps and Desktops Premiumを購入したが、Citrix Virtual Apps機能のみを使用したい場合は、コンプライアンスを満たすために製品をCitrix Virtual Apps and Desktopsに構成します。詳細については、Product License Compliance Centerを参照してください。

Citrix Virtual Apps EULAに準拠して、Citrix Virtual Apps環境のライセンスを付与するにはどうすればよいですか?

Citrix Virtual Apps EULAに準拠して同時接続ライセンスモデルでCitrix Virtual Appsを展開するには、ライセンスファイルをライセンスサーバーに適用します。ライセンスサーバーは、ライセンスコンプライアンスを制御および監視します。

Citrix Virtual Apps and Desktopsのサービスオプション（Long Term Service Release (LTSR)またはCurrent Release (CR)）にライセンス要件はありますか?

Long-Term Service ReleaseなどのCitrix Virtual Apps and Desktops Servicing Optionsは、Customer Success Servicesプログラムの特典です。LTSRの特典を受けるには、アクティブなCustomer Success Servicesが必要です。詳細については、[Citrix Virtual Apps, Citrix Virtual Apps and Desktops, and XenServer Servicing Optionsを参照してください。

Remote Browser Isolation (RBI) Serviceのプールされた時間はどのように機能しますか?

サービスを最低25ユーザー購入すると、すべてのユーザーでプールされた5000時間のサービス利用権が付与されます。その後のユーザー権限の購入では、プールされた時間の権利は増加しません。サービス時間の権利を増やすには、アドオンパックを購入してください。

CCUライセンスでRemote PC Accessを使用できますか?

はい。

Remote PC Accessの詳細については、Remote PC Accessを参照してください。

Citrix環境のソフトウェアメンテナンスの有効期限が切れるとどうなりますか?

ソフトウェアメンテナンス (SWM) またはサブスクリプションの有効期限が切れると、ソフトウェアアップグレードとテクニカルサポートへのアクセスが一時停止されます。また、ライセンスの種類と製品バージョンによっては、エンドユーザーと管理者に、環境がサポートされていないことを示す特定の警告通知が届きます。

これらの通知は、サーバー上のすべてのライセンスの有効期限が切れた場合にのみトリガーされます。

エンドユーザーエクスペリエンス

ユーザーはセッション起動後に警告メッセージを受け取ります。メッセージには次のように表示されます。

```
Citrix Virtual Apps and Desktops warning: Your corporate Citrix
environment is currently unsupported. Please contact your IT department to
resolve.
```

管理者エクスペリエンス

管理者は、Citrix Studioコンソール内で、間近に迫った、または現在有効な有効期限を警告するアラートを確認できます。

ライセンスの種類による有効期限の動作

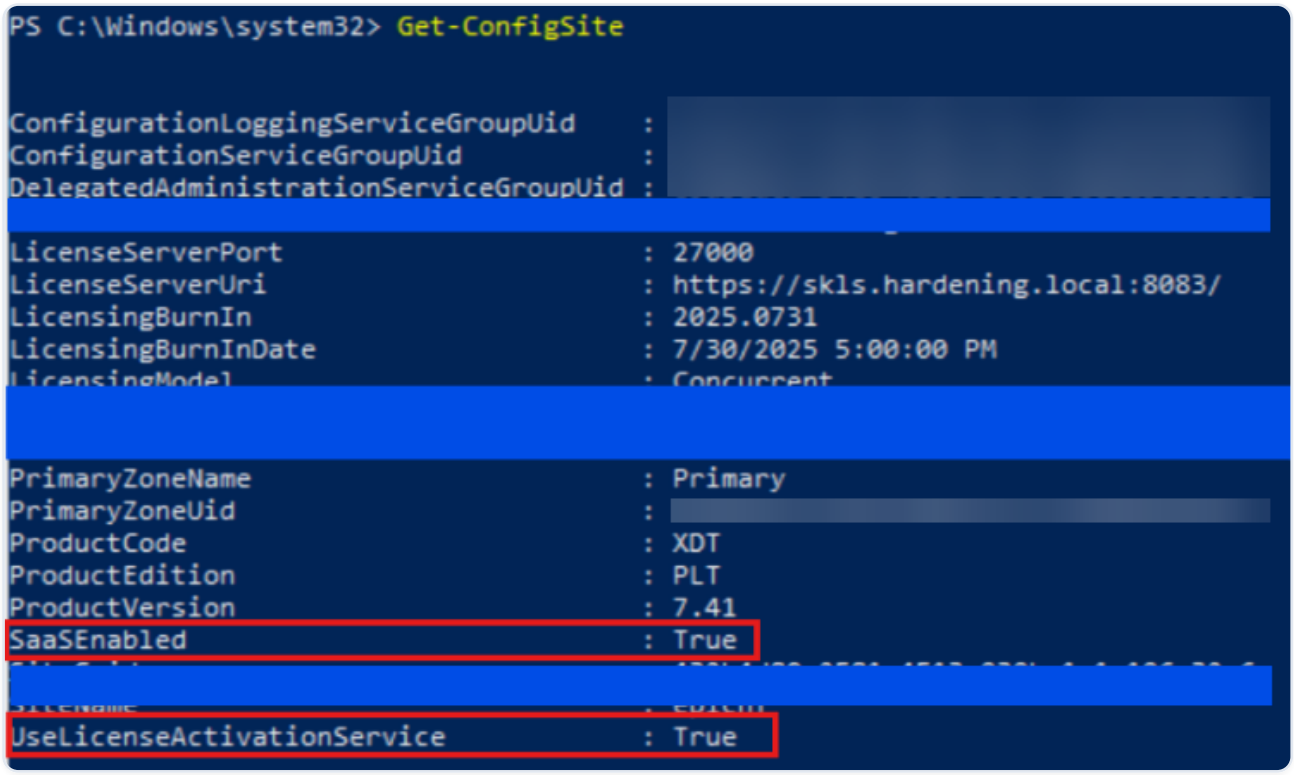
これらのメッセージの表示タイミングは、ライセンスの種類とインストールされているCitrix Virtual Apps and Desktopsのバージョンによって異なります。

オンプレミスサブスクリプションライセンス

- エンドユーザー警告: サブスクリプションの有効期限が切れた後、猶予期間中に表示されます。
- 管理者警告: サブスクリプションの有効期限が切れる30日前にStudioに表示されます。
- サポートされているバージョン:
  - 現在のリリース: Citrix Virtual Apps and Desktops 2411以降。
  - LTSR: 2203 CU6、2402 CU1、およびそれ以降のLTSRリリース

サイトのLAS状態を確認するにはどうすればよいですか?

LASアクティベーションの状態とSaaSビットのステータスを確認するには、`Get-configsite`を実行します。



サイトがライセンスキャッシュモードになっているか確認するにはどうすればよいですか?

キャッシュモードと残り時間の詳細を取得するには、`Get-Brokercontroller`と`Get-brokersite`を実行します。

- `Get-Brokercontroller`出力：

  Get-Brokercontroller コマンドの画像(/en-us/citrix-virtual-apps-desktops/2511/media/get-broker-controller-brk-cmnd.png)

- `Get-brokersite`出力：

  Get-brokersite コマンドの画像(/en-us/citrix-virtual-apps-desktops/2511/media/get-brk-site-brk-cmnd.png)

コマンドの詳細については、以下を参照してください。

- Get-BrokerController
- Get-ConfigSite

ライセンスに関するDelivery Controllerのイベントビューアーログについては、ライセンスイベントに関連するイベントビューアーログ を参照してください。

ユーザーまたはデバイスライセンス

Citrixは、ユーザー/デバイスライセンスモデルでユーザーにライセンスをどのように割り当てますか?

ユーザー/デバイスライセンスモデルでは、ライセンスサーバーはライセンスを一意のユーザーIDに割り当てます。これにより、その単一ユーザーは無制限のデバイスから無制限の接続を行うことができます。ユーザーがデスクトップまたはデバイスに接続する場合、仮想デスクトップまたはアプリケーションにアクセスするには、そのユーザーに割り当てられた1つのライセンスが必要です。ライセンスサーバーまたはクラウドサービスがライセンスを割り当てます。これらのライセンスを手動で割り当てることはできません。ライセンスは共有デバイスではなく、ユーザーに割り当てられます。一度ライセンスが割り当てられると、90日間の非アクティブ期間が経過するまで、別のユーザーに割り当てることはできません。詳細については、ユーザー/デバイスライセンス を参照してください。

Citrixは、ユーザー/デバイスライセンスモデルでライセンスデバイスをどのように定義しますか?

ライセンスデバイスには、一意のエンドポイントデバイスIDが必要です。ユーザー/デバイスモデルでは、デバイスとは、Citrix Virtual Apps and Desktopsのインスタンスにアクセスするために、個人が使用することを許可したあらゆる機器を指します。共有デバイスの場合、単一のCitrix Virtual Apps and Desktopsユーザー/デバイスライセンスで、そのデバイスを共有する複数のユーザーをサポートできます。たとえば、共有デバイスは、教室のワークステーションや病院の臨床ワークステーションなどです。

Citrix Virtual Desktops Standard Edition の同時接続ライセンスを、ユーザー/デバイスモデルに変換できますか？

Citrix Virtual Desktops Standard Editionの同時使用ライセンスをCitrix Virtual Desktops Standard Editionのユーザー/デバイスライセンスに変換することはできません。同様に、Citrix Virtual Desktops Standard Editionのユーザー/デバイスライセンスをCitrix Virtual Desktops Standard Editionの同時使用ライセンスに変換することもできません。

Citrix Virtual Desktops Standard Editionの同時使用ライセンスをお持ちで、ユーザー/デバイスライセンスモデルをご希望の場合は、Citrix Virtual Apps and Desktops AdvancedまたはPremium Editionにアップグレードしてください。

元	STANDARD 同時接続へ	スタンダードユーザー/デバイスへ	アドバンストユーザー/デバイスへ	プレミアムユーザー/デバイスへ
Citrix Virtual Desktops Standard	該当なし	同時接続からユーザー/デバイスへの変換は	ライセンスモデルを変換することはできません	ライセンスモデルを変換することはできません

元	STANDARD 同時接続へ	スタンダードユーザー/デバイスへ	アドバンストユーザー/デバイスへ	プレミアムユーザー/デバイスへ
Edition 同時接続ライセンス		許可されていません	が、Citrix Virtual Apps and Desktops Advanced または Premium Edition にアップグレードすることはできます。	が、Citrix Virtual Apps and Desktops Advanced または Premium Edition にアップグレードすることはできます。
Citrix Virtual Desktops スタンダードエディション ユーザー/デバイスライセンス	ユーザー/デバイスから同時接続への変換は許可されていません	該当なし	該当なし	該当なし

同時使用ライセンスは、ユーザー/デバイスライセンスとどのように異なりますか?

同時使用ライセンスは、デバイスの同時接続数に基づいています。同時使用ライセンスは、デバイスがアクティブな接続を確立している場合にのみ使用されます。接続が終了すると、同時使用ライセンスはすぐに使用できるライセンスプールに戻ります。このライセンスモデルは、一時的な使用におすすめです。ユーザー/デバイスライセンスは一定期間リースされ、リース期間が終了するまで他のユーザーは利用できません。

ユーザー/デバイスモデルにおける、同じ企業内でのユーザーとデバイスへのライセンス割り当て?

はい。両方のタイプを同じ企業内で使用できます。ライセンスサーバーは、使用状況に基づいてユーザーまたはデバイスにライセンスを最適に割り当てます。これらのライセンスを手動で割り当てることはできません。

ライセンスを付与するユーザーまたはデバイスの数をどのように決定すればよいですか?

適切なライセンス数を決定するために、ユースケースの要件を評価してください。ユーザー/デバイスライセンスは、無制限のデバイスから無制限の仮想デスクトップと仮想アプリへの無制限のアクセスを可能にします。同時使用ライセンスは、無制限のユーザーが使用できる単一のデバイスから、無制限の仮想デスクトップと仮想アプリへの無制限のアクセスを可能にします。次の式を考慮してください。

```
(Number of total users) – (number of users that only access exclusively

 with shared devices) + (number shared devices) = total number

 of licenses to buy.



For example, there are 1000 total users at the hospital. If 700 of them
access only

Citrix Virtual Desktops from 300 shared devices in the hospital, the
number of

licenses to purchase is 1000 – 700 + 300 = 600 licenses.
```

ユーザー/デバイスモデルでは、ライセンスを持つユーザーが私の環境に接続するために使用できるデバイスの最大数はいくつですか?

各ライセンスユーザーは、接続されているデバイスまたはオフラインのデバイスを無制限に使用できます。

ユーザー/デバイスモデルでは、ライセンスを持つデバイスにアクセスできるユーザーの最大数?

各ライセンスデバイスは、組織内で無制限のユーザーにサービスを提供できます。

ユーザー/デバイスモデルでは、ライセンスを持つユーザーが一度に消費できる仮想デスクトップまたはRBI Webアプリケーションの最大数?

各ライセンスユーザーは、無制限の仮想デスクトップまたはWebアプリケーションに接続できます。

既存のCitrix Virtual Apps and Desktops環境で、ライセンスユーザー/デバイスの数を増やすためにCitrix Virtual Apps and Desktopsライセンスを購入できますか?

はい。既存のCitrix Virtual Apps and Desktops環境で、ライセンスユーザー/デバイスの数を増やすためにCitrix Virtual Apps and Desktopsライセンスを購入できます。

承認されたユーザー/デバイスライセンスを解放するにはどうすればよいですか?

承認されたユーザー/デバイスの割り当てを解放するには、EULAの条項に従って`udadmin`ユーティリティを使用します。その後、ライセンスサーバーは次の適切なユーザー/デバイスにライセンスを割り当てます。詳細については、「ユーザーまたはデバイスのライセンスを表示または解放する」を参照してください。

購入したユーザー/デバイスライセンス数を超過した場合、どうなりますか?

ユーザー/デバイスライセンスには10%のオーバードラフトが含まれており、これはライセンス生成時に含まれます。オーバードラフトは、インストールされているライセンス数にも含まれます。使用量の急増がオーバードラフトを含むインストール済み数を超えた場合、追加ユーザーのアクセスは拒否されます。追加ユーザーのアクセスを有効にするには、新しいライセンスを購入して展開してください。

ライセンスオーバードラフトを含むすべてのライセンスが使用中の場合、ライセンスバーストモードにより、製品への無制限の接続が可能になります。ライセンスバーストモードは、最大ライセンス数を超過した理由を特定し、ユーザーを中断することなく追加ライセンスを購入するための時間を提供します。この期間は、15日が経過するか、追加の小売ライセンスをインストールするかのいずれか早い方まで続きます。詳細については、「ライセンスバーストモード」を参照してください。

Director はライセンスキャッシュモードの状態を表示します。詳細については、「Director ダッシュボードのパネル」(/ja-jp/citrix-virtual-apps-desktops/2511/director/site-analytics.html#panels-on-the-director-dashboard)を参照してください。

ライセンスユーザーが一度に消費できる仮想アプリケーションの最大数はいくつですか?

各ライセンスユーザーは、無制限の仮想アプリケーションに接続できます。

ライセンスユーザーが組織を離れた場合、どうなりますか?

既存のライセンスユーザーが組織を離れる場合、Citrixに通知することなく、そのユーザーのライセンスを解放できます。ライセンスを解放するには、`udadmin`ユーティリティを使用します。ライセンスを解放しない場合、ライセンスサーバーは90日間の非アクティブ状態の後、自動的にライセンスを解放します。この情報は、EULAに指定された条項に従います。

ライセンスユーザーが長期間不在の場合、どうなりますか?

既存のライセンスユーザーが長期間不在の場合、Citrix に通知することなくライセンスを解放し、再割り当てできるようにすることができます。ライセンスを解放するには、`udadmin` ユーティリティを使用します。

組織内のライセンスデバイスを交換した場合、どうなりますか?

既存のライセンスデバイスを交換する場合、Citrixに通知することなくライセンスを解放し、再割り当てできるようにすることができます。ライセンスを解放するには、`udadmin`ユーティリティを使用します。

ライセンスされたデバイスが長期間サービス停止した場合、どうなりますか?

既存のライセンスデバイスが長期間サービス停止した場合、Citrixに通知することなくライセンスを解放し、再割り当てできるようにすることができます。ライセンスを解放するには、`udadmin`ユーティリティを使用します。ライセンスを解放しない場合、ライセンスサーバーは90日間アクティビティがないと自動的にライセンスを解放します。この情報は、EULAに指定された条件に従います。

デバイスまたはユーザーにライセンスを割り当てた後で、ユーザーライセンスをデバイスライセンスに、またはその逆に切り替えることはできますか?

はい、できます。この変更は自動的に行われます。ライセンスサーバーは、使用パターンに基づいてユーザーまたはデバイスのいずれかにライセンスを割り当てます。使用パターンが変更された場合、ライセンスサーバーは新しい使用状況に基づいて割り当てを切り替えることがあります。ライセンスサーバーは常に、顧客にとって最も経済的な方法でライセンスを割り当てます。また、ライセンスサーバーは、90日間の割り当て期間後に**未使用**のライセンスを特定するためにライセンスを監視します。90日間の割り当て期間後に未使用と識別されたライセンスは、他のユーザーまたはデバイスに再割り当てできます。

同時使用ライセンス

同時使用モデルでは、Citrix Virtual Apps and Desktops のライセンスユーザーが一度に消費できる仮想デスクトップの最大数はいくつですか?

エンドポイントは多数のユーザーにサービスを提供でき、無制限の接続を許可します。

以前のバージョンのCitrix Virtual Apps and Desktopsの同時接続ライセンスと、新しいユーザー/デバイスまたは同時接続ライセンスを単一のライセンスサーバーに展開できます?

はい。同じライセンスサーバーを使用して、ユーザー/デバイスまたは同時使用ライセンスの展開をサポートし続けることができます。

同時接続ライセンスとユーザー/デバイスまたは同時接続ライセンスを単一のライセンスサーバーに展開できます?

はい。引き続き同じライセンスサーバーを使用して、同時使用ライセンスとユーザー/デバイスライセンス、または同時使用ライセンスの展開をサポートできます。

Citrix Virtual Apps and Desktops AdvancedおよびPremiumエディションには、Citrix Virtual Appsの同時使用ライセンスが含まれていますか?

Citrix Virtual Apps and Desktops AdvancedおよびPremiumのユーザー/デバイスライセンスには、互換性のためだけにCitrix Virtual Appsの同時接続ライセンスが含まれています。これらの同時接続ライセンスは、ユーザー/デバイスライセンスと互換性のない以前の製品バージョンでのみ使用で

きます。ユーザー/デバイスライセンスに含まれる同時接続互換性ライセンスの使用は、これらのバージョン（XenApp 6.5より前のバージョンおよびXenDesktop 5.0 Service Pack 1より前のバージョン）でのみ許可されます。

購入した同時使用ライセンス数を超過した場合、どうなりますか?

すべてのライセンスが使用中の場合、ライセンスバーストモードにより、製品への無制限の接続が可能になります。ライセンスバーストモードは、最大ライセンス数を超過した理由を特定し、ユーザーに中断を与えることなく追加のライセンスを購入するための時間を提供します。この期間は、15日が経過するか、追加の小売ライセンスをインストールするかのいずれか早い方まで続きます。詳細については、「ライセンスバーストモード」を参照してください。

Directorは猶予期間の状態を表示します。詳細については、「Directorダッシュボードのパネル」を参照してください。

超過ライセンス

超過ライセンスはどのように入手できますか?

ユーザー/デバイス、ユーザー、またはデバイスライセンスモデルをサポートする製品（Citrix Cloudを除く）には、アクセス拒否を防ぐために限られた数の追加ライセンスを使用できるライセンス超過機能が含まれています。当社は、便宜のために超過機能を提供しており、ライセンスの権利としてではありません。同時接続ライセンスおよびサーバーライセンスには超過機能は含まれていません。使用された超過ライセンスは、初回使用から30日以内に購入する必要がありますが、使用期間は30日に限定されません。Citrixは、新しい製品リリースで超過機能を削除する権利を留保します。詳細については、「ライセンス超過」を参照してください。

ライセンス超過をどのように識別できますか?

Citrix Licensing Managerで、超過しているライセンス数を含む使用状況情報を表示できます。Studioにも超過使用状況情報が含まれています。

超過ライセンスが消費されるとどうなりますか?

Citrix Virtual Apps and Desktops環境へのアクセスを有効にするために、インストールされているライセンスからライセンスが割り当てられます。この超過ライセンスは、他のライセンスと同等のアクセスと機能を提供します。

超過ライセンスが消費されたときにアラートを受け取ることはできますか?

現在、オーバードラフトライセンスが消費されたときに提供される特定の警告はありません。

超過ライセンスはどのくらいの期間消費可能か?

最初に使用してから30日以内に使用されたオーバードラフトライセンスを購入してください。

その他の製品固有のライセンス情報

- シトリックス ADC
- シトリックス クラウド
- シトリックス エンドポイント マネジメント
- シトリックス ゲートウェイ
- XenServer
- シトリックス ライセンシング

ローカルホストキャッシュ

Citrix Virtual Apps and Desktopsサイトデータベースが常に利用可能であることを保証するため、CitrixはMicrosoftの高可用性ベストプラクティスに従って、フォールトトレラントなSQL Server展開から始めることを推奨します。(サポートされているSQL Serverの高可用性機能については、データベースを参照してください。)しかし、ネットワークの問題や中断により、ユーザーがアプリケーションやデスクトップに接続できなくなる可能性があります。

ローカルホストキャッシュ機能により、障害発生時にサイト内の接続仲介操作を継続できます。障害は、オンプレミスのCitrix®環境でDelivery Controller™とサイトデータベース間の接続が失敗したときに発生します。サイトデータベースに90秒間アクセスできない場合、ローカルホストキャッシュが有効になります。

XenAppおよびXenDesktop 7.16以降、接続リース機能（以前のリリースにおける先行の高可用性機能）は製品から削除され、利用できなくなりました。

データコンテンツ

ローカルホストキャッシュには、メインデータベースの情報の一部である以下の情報が含まれます。

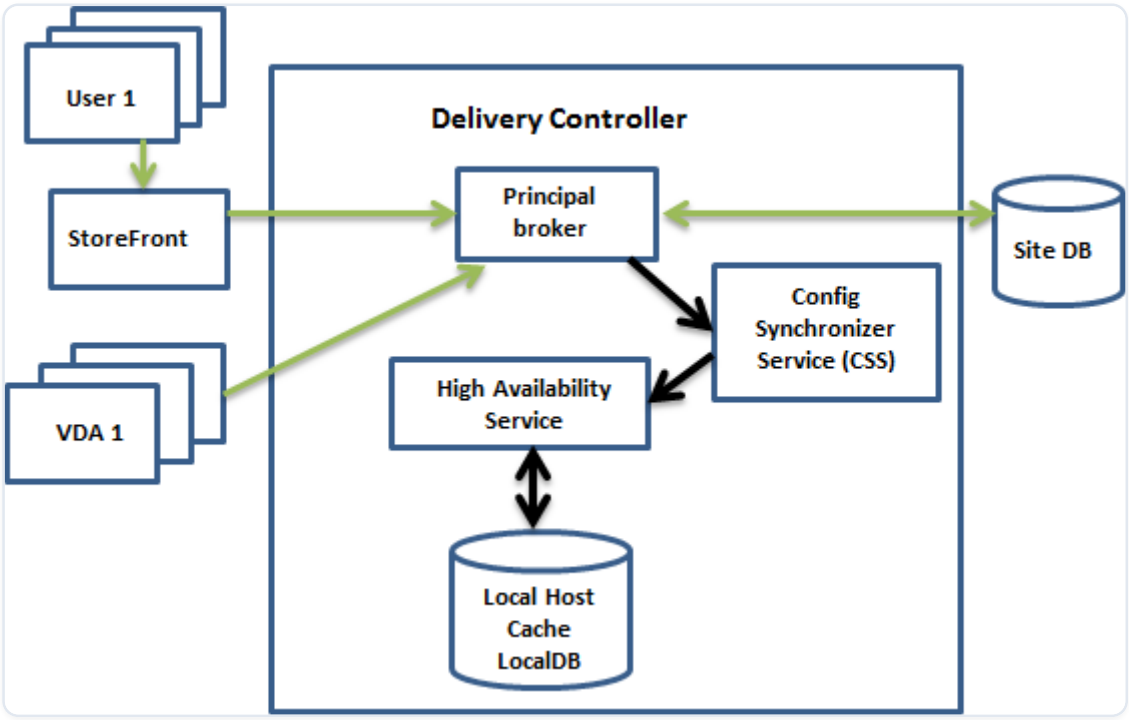
- サイトから公開されたリソースへの権限が割り当てられているユーザーとグループのID。
- サイトから公開されたリソースを現在使用している、または最近使用したユーザーのID。
- サイトで構成されているVDAマシン（リモートPCアクセス マシンを含む）のID。
- 公開されたリソースへの接続に積極的に使用されているクライアントCitrix Receiver™マシンのID（名前とIPアドレス）。

また、メインデータベースが利用できなかった間に確立された、現在アクティブな接続に関する情報も含まれています。

- Citrix Receiverによって実行されたクライアントマシンのエンドポイント分析の結果。
- サイトに関与しているインフラストラクチャマシン（NetScaler GatewayやStoreFront™サーバーなど）のID。
- ユーザーによる最近のアクティビティの日時と種類。

動作の仕組み

次の図は、通常動作時のローカルホストキャッシュのコンポーネントと通信パスを示しています。



通常動作時

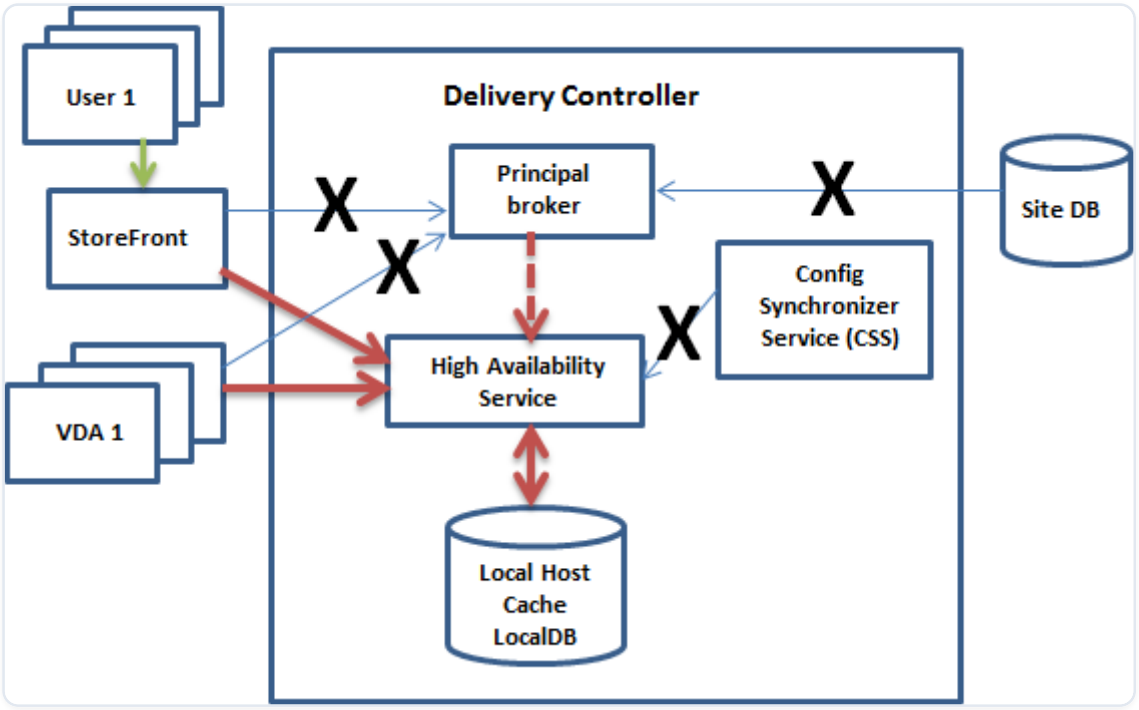
- Controller上の *プライマリブローカー*（Citrix Broker Service）は、StoreFrontからの接続要求を受け入れます。ブローカーはサイトデータベースと通信し、Controllerに登録されているVDAにユーザーを接続します。
- Citrix Config Synchronizer Service（CSS）は、約5分ごとにブローカーに問い合わせて、変更が行われたかどうかを確認します。これらの変更は、管理者によって開始されたもの（デリバリーグループのプロパティの変更など）またはシステムアクション（マシン割り当てなど）である可能性があります。
- 前回のチェック以降に構成変更があった場合、CSSは情報をController上のセカンダリブローカーに同期（コピー）します。（セカンダリブローカーは高可用性サービスとも呼ばれます。）

前回のチェック以降に変更された項目だけでなく、すべての構成データがコピーされます。CSSは、構成データをController上のMicrosoft SQL Server Express LocalDBデータベースにインポートします。このデータベースは、ローカルホストキャッシュデータベースと呼ばれます。CSSは、ローカルホストキャッシュデータベースの情報がサイトデータベースの情報と一致することを確認します。ローカルホストキャッシュデータベースは、同期が行われるたびに再作成されます。

Microsoft SQL Server Express LocalDB（ローカルホストキャッシュデータベースで使用）は、Controllerをインストールすると自動的にインストールされます。（コマンドラインからControllerをインストールする際に、このインストールを禁止できます。）ローカルホストキャッシュデータベースは、複数のController間で共有できません。ローカルホストキャッシュデータベースをバックアップする必要はありません。構成変更が検出されるたびに再作成されます。

- 前回のチェック以降に変更がない場合、データはコピーされません。

次の図は、プライマリブローカーがサイトデータベースとの接続を失った場合（停止が開始された場合）の通信パスの変更を示しています。



停止中

停止が開始されると、次のようになります。

- セカンダリブローカーは、接続要求のリッスンと処理を開始します。

- 停止が開始されると、セカンダリブローカーは最新のVDA登録データを持っていませんが、VDAがセカンダリブローカーと通信すると、登録プロセスがトリガーされます。そのプロセス中に、セカンダリブローカーは当該VDAに関する最新のセッション情報も取得します。
- セカンダリブローカーが接続を処理している間、ブローカリングプリンシパルは接続を監視し続けます。接続が復元されると、ブローカリングプリンシパルはセカンダリブローカーに接続情報のリスニングを停止するよう指示し、ブローカリングプリンシパルはブローカリング操作を再開します。次にVDAがブローカリングプリンシパルと通信するときに、登録プロセスがトリガーされます。セカンダリブローカーは、以前の停止から残っているVDA登録をすべて削除します。CSSは、展開で構成変更が発生したことを認識すると、情報の同期を再開します。

同期中に停止が発生する万が一の事態では、現在のインポートは破棄され、最後に認識された構成が使用されます。

イベントログは、同期と停止に関する情報を提供します。

停止モードでの運用に時間制限はありません。

通常モードと停止モード間の移行は、既存のセッションには影響しません。新しいセッションの起動のみに影響します。

意図的に停止をトリガーすることもできます。その理由と方法の詳細については、停止の強制を参照してください。

複数のコントローラーがあるサイト

CSSは、他のタスクの中でも、ゾーン内のすべてのコントローラーに関する情報をセカンダリブローカーに定期的に提供します。(展開に複数のゾーンが含まれていない場合、このアクションはサイト内のすべてのコントローラーに影響します。)その情報を持つことで、各セカンダリブローカーは、ゾーン内の他のコントローラーで実行されているすべてのピアセカンダリブローカーについて認識します。

セカンダリブローカーは、別のチャネルで互いに通信します。これらのブローカーは、実行されているマシンのFQDN名のアルファベット順リストを使用して、停止が発生した場合にゾーン内でブローカー操作を行うセカンダリブローカーを決定（選出）します。停止中、すべてのVDAは選出されたセカンダリブローカーに登録します。ゾーン内の選出されていないセカンダリブローカーは、受信接続およびVDA登録要求を積極的に拒否します。

停止中に選出されたセカンダリブローカーが失敗した場合、別のセカンダリブローカーが引き継ぐために選出され、VDAは新しく選出されたセカンダリブローカーに登録します。

停止中にコントローラーが再起動された場合：

- そのコントローラーが選出されたブローカーでない場合、再起動による影響はありません。
- そのコントローラーが選出されたブローカーである場合、別のコントローラーが選出され、VDAが登録されます。再起動されたコントローラーが電源オンになると、自動的にブローカリングを引き継ぎ、VDAが再度登録されます。このシナリオでは、登録中にパフォーマンスが影響を受ける可能性があります。

通常操作中にコントローラーの電源をオフにし、停止中に電源をオンにした場合、そのコントローラーがブローカーとして選出されると、そのコントローラーではローカルホストキャッシュを使用できません。

イベントログは、選出に関する情報を提供します。

停止中に利用できないもの、およびその他の違い

停止モードでの運用に時間制限はありません。ただし、Citrixは可能な限り迅速に接続を復元することを推奨しています。

停止中：

- Studioを使用できません。
- PowerShell SDKへのアクセスは制限されます。
    - まず、次の操作を行う必要があります。
        - 値が1のレジストリキー `EnableCssTestMode` を追加します: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
        - ポート89を使用します: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ControllerDNSName, DesktopGroupName, RegistrationState`
    - これらのコマンドを実行すると、以下にアクセスできます。
        - すべての `Get-Broker*` コマレット。
- ハイパーバイザーの資格情報はホストサービスから取得できません。すべてのマシンは不明な電源状態になり、電源操作を発行できません。ただし、電源がオンになっているホスト上のVM は、接続要求に使用できます。
- 割り当てられたマシンは、通常の操作中に割り当てが行われた場合にのみ使用できます。停止中に新しい割り当てを行うことはできません。

- リモート PC アクセス マシンの自動登録と構成はできません。ただし、通常の操作中に登録および構成されたマシンは使用できます。
- サーバーでホストされているアプリケーションおよびデスクトップのユーザーは、リソースが異なるゾーンにある場合、構成されたセッション制限よりも多くのセッションを使用する可能性があります。
- ユーザーは、現在アクティブ/選出されているセカンダリブローカーを含むゾーン内の登録済みVDA からのみアプリケーションとデスクトップを起動できます。ゾーンをまたぐ起動（あるゾーンのセカンダリブローカーから別のゾーンの VDA への起動）は、停止中はサポートされません。
- 配信グループ内のVDAのスケジュールされた再起動が開始される前にサイトデータベースの停止が発生した場合、停止が終了したときに再起動が開始されます。これにより、意図しない結果が生じる可能性があります。詳細については、「データベースの停止により遅延するスケジュールされた再起動」を参照してください。
- ゾーンの優先順位は構成できません。構成されている場合、セッション起動時に優先順位は考慮されません。
- タグがゾーンの指定に使用されるタグ制限は、セッション起動ではサポートされていません。このようなタグ制限が構成されており、StoreFrontストアの高度なヘルスチェックオプションが有効になっている場合、セッションの起動が断続的に失敗する可能性があります。

アプリケーションとデスクトップのサポート

LHCは、次の種類のVDAと配信モデルをサポートしています。

VDAの種類	配信モデル	LHCイベント中のVDAの可用性
マルチセッションOS	アプリケーションとデスクトップ	常に利用可能。
シングルセッションOS静的（割り当て済み）	デスクトップ	常に利用可能。
電源管理されたシングルセッションOSランダム（プール済み）	デスクトップ	デフォルトでは利用できません。プールされたデリバリーグループ内の電源管理されたVDAへのすべてのセッション起動

VDAの種類	配信モデル	LHCイベント中のVDAの可用性	
		試行は、デフォルトで失敗します。LHCイベント中に新しい接続で利用できるようにすることができます。詳細については、「Web Studio を使用して有効にする」および「PowerShell を使用して有効にする」を参照してください。 **重要:** 電源管理されたシングルセッションのプールされたマシンへのアクセスを有効にすると、以前のユーザーセッションのデータと変更が後続のセッションに存在する可能性があります。	

注:

プールされたデリバリーグループ内の電源管理されたデスクトップVDAへのアクセスを有効にしても、通常の操作中に構成された`ShutdownDesktopsAfterUse`プロパティがどのように機能するかには影響しません。LHC中にこれらのデスクトップへのアクセスが有効になっている場合、LHCイベントが完了してもVDAは自動的に再起動しません。プールされたデリバリーグループ内の電源管理されたデスクトップVDAは、VDAが再起動するまで以前のセッションのデータを保持できます。VDAの再起動は、非LHC操作中にユーザーがVDAからログオフした場合、または管理者がVDAを再起動した場合に発生する可能性があります。

Web Studio を使用して、電源管理されたシングルセッションOSのプールされたVDAでLHCを有効にする

Web Studio を使用して、デリバリーグループごとにLHCイベント中に新しい接続でこれらのマシンを利用できるようにすることができます。

- デリバリーグループの作成中にこの機能を有効にするには、「デリバリーグループの作成」を参照してください。
- 既存のデリバリーグループでこの機能を有効にするには、「デリバリーグループの管理」を参照してください。

> **注:**
>
> この設定は、電源管理されたVDAを提供するプールされたデスクトップデリバリーグループの場合にのみ、Web Studio で利用できます。

PowerShellを使用して、電源管理されたシングルセッションOSのプールされたVDAに対してLHCを有効にする

特定のデリバリーグループ内のVDAに対してLHCを有効にするには、以下の手順に従います。

1. 次のコマンドを実行して、サイトレベルでこの機能を有効にします。

   ```
   Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
   ```

2. デリバリーグループ名を指定して次のコマンドを実行し、デリバリーグループのLHCを有効にします。

   ```
   Set-BrokerDesktopGroup -Name "name" -ReuseMachinesWithoutShutdownInOutage $true
   ```

電源管理されたVDAを持つ新しく作成されたプールデリバリーグループのデフォルトのLHC可用性を変更するには、次のコマンドを実行します。

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

RAM サイズに関する考慮事項

LocalDBサービスは、約1.2 GBのRAM（データベースキャッシュに最大1 GB、SQL Server Express LocalDBの実行に200 MB）を使用できます。セカンダリブローカーは、多くのログオンが発生する長時間の停止（たとえば、10Kユーザーで12時間）の場合、最大1 GBのRAMを使用で

きます。これらのメモリ要件は、Controllerの通常のRAM要件に追加されるため、RAM容量の合計を増やす必要がある場合があります。

サイトデータベースにSQL Server Expressインストールを使用している場合、サーバーには2つのsqlserver.exeプロセスがあります。

CPU コアとソケット構成に関する考慮事項

ControllerのCPU構成、特にSQL Server Express LocalDBで利用可能なコアの数は、メモリ割り当てよりもさらに、ローカルホストキャッシュのパフォーマンスに直接影響します。このCPUオーバーヘッドは、データベースに到達できず、セカンダリブローカーがアクティブな停止期間中にのみ観察されます。

LocalDBは複数のコア（最大4つ）を使用できますが、単一のソケットに制限されています。ソケットを追加してもパフォーマンスは向上しません（たとえば、1コアずつ4つのソケットがある場合）。代わりに、Citrixは複数のソケットと複数のコアを使用することを推奨しています。Citrixのテストでは、2x3（2ソケット、3コア）構成は4x1および6x1構成よりも優れたパフォーマンスを提供しました。

ストレージに関する考慮事項

ユーザーが障害中にリソースにアクセスすると、LocalDB は増大します。たとえば、1 秒あたり 10 回のログオンで実行されるログオン/ログオフ テスト中に、データベースは 2 ～ 3 分ごとに 1 MB 増加しました。通常の操作が再開されると、ローカル データベースが再作成され、スペースが返されます。ただし、障害中のデータベースの増大を許容するために、LocalDB がインストールされているドライブには十分な空き容量が必要です。ローカル ホスト キャッシュは、障害中にさらに多くの I/O を発生させます。具体的には、1 秒あたり約 3 MB の書き込みと、数十万回の読み取りが発生します。

パフォーマンスに関する考慮事項

障害発生中は、1 つのセカンダリ ブローカーがすべての接続を処理するため、通常の操作中に複数のコントローラー間で負荷分散を行うサイト（またはゾーン）では、選出されたセカンダリ ブローカーが障害中に通常よりもはるかに多くの要求を処理する必要がある場合があります。したがって、CPU の要求は高くなります。障害中に選出されるセカンダリ ブローカーは変更される可能性があるため、サイト（ゾーン）内のすべてのセカンダリ ブローカーは、ローカル ホスト キャッシュ データベースと影響を受けるすべての VDA によって課される追加の負荷を処理できる必要があります。

VDI の制限:

- 単一ゾーンの VDI 展開では、障害発生時に最大 10,000 台の VDA を効果的に処理できます。

- マルチゾーン VDI 展開では、障害発生時に各ゾーンで最大 10,000 台の VDA を効果的に処理でき、サイト全体では最大 40,000 台の VDA を処理できます。たとえば、以下の各サイトは障害発生時に効果的に処理できます。
  - 4 つのゾーンがあり、それぞれに 10,000 台の VDA が含まれるサイト。
  - 7 つのゾーンがあり、1 つのゾーンに 10,000 台の VDA、残りの 6 つのゾーンにそれぞれ 5,000 台の VDA が含まれるサイト。

障害発生中は、サイト内の負荷管理が影響を受ける可能性があります。負荷評価機能（特にセッション数ルール）が超過する可能性があります。

すべての VDA がセカンダリ ブローカーに登録されるまでの間、そのサービスは現在のセッションに関する完全な情報を持っていない可能性があります。そのため、その期間中のユーザー接続要求は、既存のセッションへの再接続が可能であったとしても、新しいセッションが起動される結果となる可能性があります。この間隔（「新しい」セカンダリ ブローカーが再登録中にすべての VDA からセッション情報を取得する間）は避けられません。障害発生時に接続されているセッションは、移行期間中に影響を受けませんが、新しいセッションやセッションの再接続は影響を受ける可能性があります。

この間隔は、VDA が登録する必要がある場合に発生します。

- 障害の開始: プリンシパル ブローカーからセカンダリ ブローカーに移行する場合。
- 障害中のセカンダリ ブローカーの障害: 障害が発生したセカンダリ ブローカーから新しく選出されたセカンダリ ブローカーに移行する場合。
- 障害からの復旧: 通常の操作が再開され、プリンシパル ブローカーが制御を再開する場合。

Citrix Broker Protocolの`HeartbeatPeriodMs`レジストリ値を下げることで、間隔を短縮できます(デフォルト = 600000ミリ秒、つまり10分)。このハートビート値は、VDAがpingに使用する間隔の2倍であるため、デフォルト値では5分ごとにpingが実行されます。

たとえば、次のコマンドはハートビートを5分（300000ミリ秒）に変更します。これにより、2.5分ごとにpingが実行されます。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name HeartbeatPeriodMs -PropertyType DWORD –Value 300000
```

ハートビート値を変更する際は注意してください。頻度を上げると、通常モードと障害モードの両方でControllerへの負荷が増大します。

VDAがどれだけ迅速に登録されても、この間隔を完全に排除することはできません。

セカンダリブローカー間で同期にかかる時間は、オブジェクト（VDA、アプリケーション、グループなど）の数が増えるにつれて長くなります。たとえば、5000台のVDAを同期するには、完了までに10分以上かかる場合があります。

XenApp 6.xリリースとの違い

このローカルホストキャッシュの実装は、XenApp 6.xおよびそれ以前のXenAppリリースにおけるローカルホストキャッシュ機能と同じ名前を共有していますが、重要な改善点があります。この実装は、より堅牢で破損しにくいものです。定期的な`dsmaint`コマンドの必要性を排除するなど、メンテナンス要件が最小限に抑えられています。このローカルホストキャッシュは、技術的にはまったく異なる実装です。

ローカルホストキャッシュの管理

ローカルホストキャッシュが正しく機能するためには、各ControllerのPowerShell実行ポリシーをRemoteSigned、Unrestricted、またはBypassに設定する必要があります。

SQL Server エクスプレス ローカルDB

ローカルホストキャッシュが使用するMicrosoft SQL Server Express LocalDBソフトウェアは、Controllerをインストールするか、バージョン7.9より前のControllerをアップグレードする際に自動的にインストールされます。セカンダリブローカーのみがこのデータベースと通信します。PowerShellコマンドレットを使用して、このデータベースに関する何も変更することはできません。LocalDBはController間で共有できません。

SQL Server Express LocalDBデータベースソフトウェアは、ローカルホストキャッシュが有効になっているかどうかにかかわらずインストールされます。

そのインストールを防ぐには、`XenDesktopServerSetup.exe`コマンドを使用してControllerをインストールまたはアップグレードし、`/exclude "Local Host Cache Storage (LocalDB)"`オプションを含めます。ただし、ローカルホストキャッシュ機能はデータベースなしでは機能せず、セカンダリブローカーで別のデータベースを使用することはできないことに注意してください。

このLocalDBデータベースのインストールは、サイトデータベースとして使用するためにSQL Server Expressをインストールするかどうかには影響しません。

以前のSQL Server Express LocalDBバージョンを新しいバージョンに置き換える方法については、「SQL Server Express LocalDBの置き換え」を参照してください。

製品のインストールとアップグレード後のデフォルト設定

Citrix Virtual Apps and Desktops (最小バージョン7.16) の新規インストール中、ローカルホストキャッシュは有効になります。

アップグレード後 (バージョン7.16以降)、展開全体でVDAが10,000未満の場合、ローカルホストキャッシュは有効になります。

ローカルホストキャッシュの有効化と無効化

- ローカルホストキャッシュを有効にするには、次のように入力します。

  ```
  Set-BrokerSite -LocalHostCacheEnabled $true
  ```

  ローカルホストキャッシュが有効になっているかどうかを確認するには、`Get-BrokerSite` と入力します。`LocalHostCacheEnabled` プロパティが `True` であることを確認します。
- ローカルホストキャッシュを無効にするには、次のように入力します。

  ```
  Set-BrokerSite -LocalHostCacheEnabled $false
  ```

注意: XenAppおよびXenDesktop 7.16以降、接続リース (バージョン7.6からローカルホストキャッシュに先行していた機能) は製品から削除され、利用できなくなりました。

ローカルホストキャッシュが機能していることを確認する

ローカルホストキャッシュが正しく設定され、機能していることを確認するには:

- 同期インポートが正常に完了していることを確認します。イベントログ を確認してください。
- 各Delivery ControllerにSQL Server Express LocalDBデータベースが作成されていることを確認します。これにより、必要に応じてセカンダリブローカーが引き継ぐことができることが確認されます。
  - Delivery Controllerサーバーで、`C:\Windows\ServiceProfiles\NetworkService` に移動します。
  - `HaDatabaseName.mdf` と `HaDatabaseName_log.ldf` が作成されていることを確認します。
- Delivery Controllerで障害を強制発生させます。ローカルホストキャッシュが機能することを確認したら、すべてのControllerを通常モードに戻すことを忘れないでください。これには約15分かかる場合があります。

イベントログ

イベントログは、同期と障害が発生した時期を示します。イベントビューアログでは、障害モードは*HA モード*と呼ばれます*。

構成同期サービス:

通常の操作中、CSSがローカルホストキャッシュブローカーを使用して構成データをローカルホストキャッシュデータベースにインポートする際に、次のイベントが発生する可能性があります。

- 503: Citrix Config Sync Serviceが更新された構成を受信しました。このイベントは、同期プロセスの開始を示します。
- 504: Citrix Config Sync Serviceが更新された構成をインポートしました。構成のインポートは正常に完了しました。
- 505: Citrix Config Sync Serviceがインポートに失敗しました。構成のインポートは正常に完了しませんでした。以前に正常な構成が利用可能な場合、障害が発生するとそれが使用されます。ただし、それは現在の構成から古くなります。以前の構成が利用できない場合、サービスは障害発生時にセッションブローカーに参加できません。この場合、トラブルシューティングセクションを参照し、Citrixサポートに連絡してください。
- 507: システムが障害モードであり、ローカルホストキャッシュブローカーがブローカー処理に使用されているため、Citrix Config Sync Serviceはインポートを中止しました。サービスは新しい構成を受信しましたが、障害が発生したためインポートは中止されました。これは予期される動作です。
- 510: プライマリ構成サービスから構成サービス構成データが受信されませんでした。
- 517: プライマリブローカーとの通信中に問題が発生しました。
- 518: セカンダリブローカー（高可用性サービス）が実行されていないため、構成同期スクリプトが中止されました。

高可用性サービス:

このサービスは、ローカルホストキャッシュブローカーとも呼ばれます。

- 3502: 停止が発生し、ローカルホストキャッシュブローカーがブローカー操作を実行しています。
- 3503: 停止が解決され、通常の操作が再開されました。
- 3504: どのローカルホストキャッシュブローカーが選出されたか、および選出に関与した他のローカルホストキャッシュブローカーを示します。
- 3507: 2分ごとにローカルホストキャッシュのステータス更新を提供し、選出されたブローカーでローカルホストキャッシュモードがアクティブであることを示します。停止期間、VDA登録、セッション情報を含む停止の概要が含まれます。
- 3508: 選出されたブローカーでローカルホストキャッシュがアクティブでなくなり、通常の操作が復元されたことを通知します。停止期間、ローカルホストキャッシュイベント中に登録されたマシンの数、LHCイベント中の正常な起動の数を含む停止の概要が含まれます。

- 3509: 非選出ブローカーでローカルホストキャッシュがアクティブであることを通知します。2分ごとの停止期間が含まれ、選出されたブローカーを示します。
- 3510: 非選出ブローカーでローカルホストキャッシュがアクティブでなくなったことを通知します。停止期間が含まれ、選出されたブローカーを示します。

停止を強制する

意図的に停止を強制したい場合があります。

- ネットワークが繰り返し停止したり起動したりする場合。ネットワークの問題が解決されるまで停止を強制することで、通常モードと停止モード間の継続的な移行（およびそれに伴う頻繁なVDA登録ストーム）を防ぎます。
- ディザスタリカバリ計画をテストするため。
- ローカルホストキャッシュが正しく機能していることを確認するため。
- サイトデータベースサーバーの交換または保守中。

停止を強制するには、Delivery Controllerを含む各サーバーのレジストリを編集します。`HKLM\Software\Citrix\DesktopServer\LHC`で、`OutageModeForced`を`REG_DWORD`として`1`に作成して設定します。この設定により、データベースの状態に関係なく、ローカルホストキャッシュブローカーは停止モードに入ります。値を`0`に設定すると、ローカルホストキャッシュブローカーは停止モードを終了します。

イベントを確認するには、`C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityService`の`Current_HighAvailabilityService`ログファイルを監視します。

トラブルシューティング

ローカルホストキャッシュデータベースへの同期インポートが失敗し、505イベントが投稿された場合、いくつかのトラブルシューティングツールが利用可能です。

CDFトレース: `ConfigSyncServer`および`BrokerLHC`モジュールのオプションが含まれています。これらのオプションは、他のブローカーモジュールとともに、問題を特定するのに役立つでしょう。

レポート: 同期インポートが失敗した場合、レポートを生成できます。このレポートは、エラーの原因となっているオブジェクトで停止します。このレポート機能は同期速度に影響するため、Citrixは使用しないときは無効にすることを推奨します。

CSSトレースレポートを有効にして生成するには、次のコマンドを入力します。

`New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1`

HTMLレポートは `C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.htm` に投稿されます。

レポートが生成されたら、レポート機能を無効にするには次のコマンドを入力します。

`Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0`

ブローカー構成のエクスポート: デバッグ目的で正確な構成を提供します。

`Export-BrokerConfiguration | Out-File <file-pathname>`

例: `Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`。

ローカルホストキャッシュのPowerShellコマンド

PowerShellコマンドを使用して、Delivery Controllerでローカルホストキャッシュ (LHC) を管理できます。

PowerShellモジュールは、Delivery Controllerの次の場所にあります。

`C:\Program Files\Citrix\Broker\Service\ControlScripts`

> **重要:**
>
> このモジュールは、Delivery Controllerでのみ実行してください。

PowerShell モジュールのインポート

モジュールをインポートするには、Delivery Controllerで次を実行します。

`cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-Module .\HighAvailabilityServiceControl.psm1`

LHC を管理するための PowerShell コマンド

以下のコマンドは、Delivery Controller で LHC モードをアクティブ化および管理するのに役立ちます。

コマンドレット	機能
`Enable-LhcForcedOutageMode`	ブローカーをLHCモードにします。`Enable-LhcForcedOutageMode`が適切に機能するには、ConfigSyncサービスによってLHCデータベースファイルが正常に作成されている必要があります。このコマンドレットは、実行されたDelivery ControllerでのみLHCを強制します。LHCをアクティブにするには、ゾーン内のすべてのDelivery Controllerでこのコマンドを実行する必要があります。
`Disable-LhcForcedOutageMode`	ブローカーをLHCモードから外します。このコマンドレットは、実行されたDelivery ControllerでのみLHCモードを無効にします。`Disable-LhcForcedOutageMode`は、ゾーン内のすべてのDelivery Controllerで実行する必要があります。
`Set-LhcConfigSyncIntervalOverride`	Citrix Config Synchronizer Service (CSS) がサイト内の構成変更をチェックする間隔を設定します。時間間隔は60秒（1分）から3600秒（1時間）まで設定できます。この設定は、実行されたDelivery Controllerにのみ適用されます。Delivery Controller間の一貫性を保つため、このコマンドレットを各Delivery Controllerで実行することを検討してください。例: `Set-LhcConfigSyncIntervalOverride -Seconds 1200`
`Clear-LhcConfigSyncIntervalOverride`	Citrix Config Synchronizer Service (CSS) がサイト内の構成変更をチェックする間隔を、デフォルト値の300秒（5分）に設定します。この設定は、実行されたDelivery Controllerにのみ適用されます。Delivery Controller間の一貫性を保つため、このコマンドレットを各Delivery Controllerで実行することを検討してください。

コマンドレット	機能
`Enable-LhcHighAvailabilitySDK`	実行されたDelivery Controller内のすべての `Get-Broker*` コマンドレットへのアクセスを有効にします。
`Disable-LhcHighAvailabilitySDK`	実行されたDelivery Controller内のBrokerコマンドレットへのアクセスを無効にします。

注:

- Delivery Controllerで `Get-Broker*` コマンドレットを実行する際は、ポート89を使用します。例:
  - `Get-BrokerMachine -AdminAddress localhost:89`
- LHCモードでない場合、Delivery Controller上のLHC Brokerは構成情報のみを保持します。
- LHCモード中、選出されたDelivery Controller上のLHC Brokerは次の情報を保持します。
  - リソースの状態
  - セッションの詳細
  - VDA登録
  - 構成情報

検索 > デフォルトビューでマシンとセッションを監視および管理する

注:

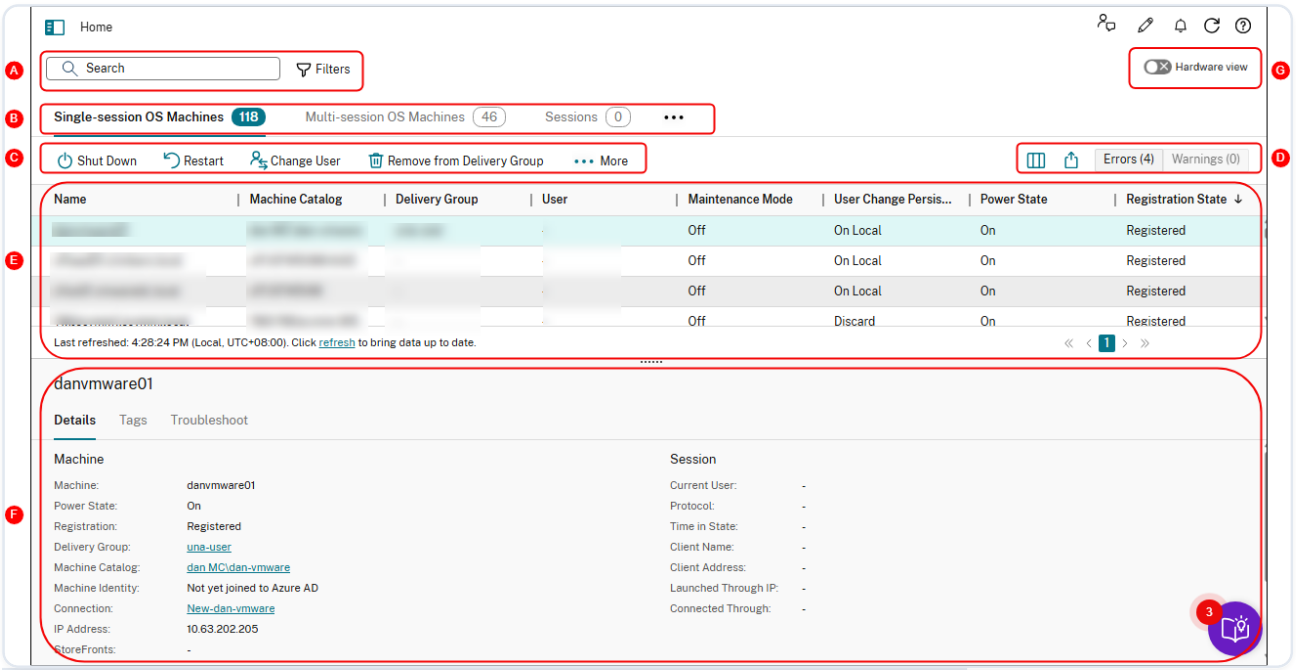
バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

この記事では、**検索**ノード内のデフォルトビューを使用してマシンとセッションを監視および管理する方法について説明します。以下のトピックが含まれています。

- デフォルトビューについて
- マシンとセッションの検索
- 表示する列のカスタマイズ
- マシンとセッションの管理
- マシンまたはセッションデータをCSVファイルにエクスポート

デフォルトビューについて

検索ノード内のデフォルトビューは、マシンとユーザーセッションを監視および管理するための一元的な場所を提供します。



コールアウト	領域	説明
A	検索バー	クイック検索と、複雑な検索条件を定義できるフィルターベースの検索を提供します。詳しくは、「インスタンスの検索」を参照してください。

コールアウト	領域	説明
B	種類タブ	種類別にマシンを一覧表示したり、すべてのセッションを一覧表示したりするためのタブを表示します。インスタンスの数はタブ名に表示されます。
C	インスタンスレベルのアクション	*選択したインスタンス*（マシンまたはセッション）に対して実行できるアクションを表示します。詳しくは、「マシンアクション」および「セッションアクション」を参照してください。
D	リストレベルのアクション	現在の*リスト*に対して実行できるアクションを表示します。 • **エクスポート**アイコン：メインビューに表示されているインスタンスのリストをCSVファイルにエクスポートします。 • 「**表示する列**」アイコン: リストのメイン

コールアウト	領域	説明	
		ビューをカスタマイズします。 • 「**エラー**」ラベル: このラベルを有効にすると、メインビューにエラーのある未登録のマシンのみが表示されます。問題の詳細を表示するには、「**詳細**」ペインの「**トラブルシューティング**」タブに移動します。 • 「**警告**」ラベル: このラベルを有効にすると、メインビューに警告のある未登録のマシンのみが表示されます。問題の詳細を表示するには、「**詳細**」ペインの「**トラブルシューティング**」タブに移動します。	
E	メインビュー	インスタンスとそのプロパティを表示します。「**表示する列**」アイコンを選択して、メインビューを	

コールアウト	領域	説明
		カスタマイズできます。利用可能な列の詳細については、「マシン列」および「セッション列」を参照してください。
F	詳細ペイン	以下の詳細が表示されます • 選択したインスタンス（マシンまたはセッション）の詳細 • 選択したマシンに適用されているタグ • 選択したマシンに関するエラーまたは警告の詳細（問題、考えられる原因、推奨される解決策を含む）
G	ハードウェアビューに切り替える	クリックして、デフォルトビューからハードウェアビューに切り替えます。

インスタンスの検索

検索機能を使用して、特定のマシンとセッションを検索します。

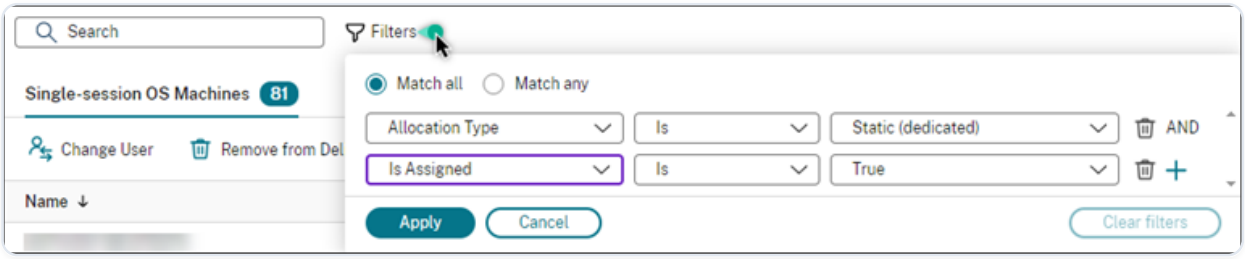
- フィルターを使用した検索
- クイック検索用に現在のフィルターセットを保存する(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/studio-search.html#save-the-current-filter-set-for-a-quick-search)

- 検索バーにフィルターフィールドをピン留めする(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/studio-search.html#pin-a-filter-field-in-the-search-bar)
- クイック検索ボックスを使用して検索する(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/studio-search.html#search-using-the-quick-search-box)
- 検索を強化するためのヒント(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/studio-search.html#tips-to-enhance-a-search)

フィルターを使用した検索

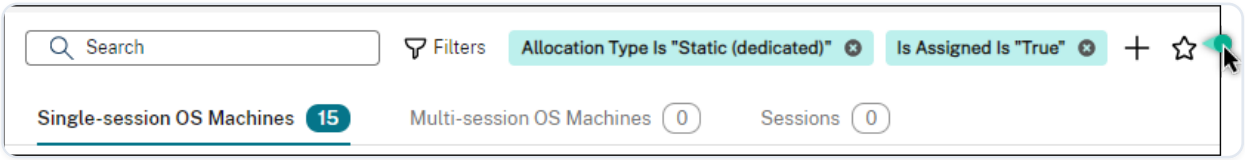
たとえば、*静的でユーザーに割り当てられている*すべてのシングルセッションOSマシンを見つけるには、次の手順に従います。

1. **シングルセッションOSマシン**タブで、**フィルター**アイコンをクリックします。フィルターパネルが表示されます。
2. 必要なフィルター条件を追加します。



3. すべてのフィルター条件に一致する結果を検索で返す場合は、**すべて一致**（AND演算子）を選択します。いずれかのフィルター条件に一致する結果を検索で返す場合は、**いずれか一致**（OR演算子）を選択します。
4. **適用**をクリックします。

   フィルターされたリストには、静的でユーザーに割り当てられているすべてのシングルセッションOSマシンが表示されます。



クイック検索用に現在のフィルターセットを保存する

たとえば、静的でユーザーに割り当てられているシングルセッションOSマシンのフィルターセットを将来使用するために保存するには、次の手順に従います。

1. フィルターベースの検索を実行した後、前の図に示すように、検索バーの**星**アイコンをクリックします。

2. 表示されるページで、このフィルターセットの名前を入力します（例：*静的および割り当て済みマシン*）。
3. **保存**をクリックします。

   検索ボックスをクリックすると、保存されたフィルターセットが検索履歴リストに表示されます。

   検索フィルターセット(/en-us/citrix-virtual-apps-desktops/2511/media/search-filter-set.png)

> **注：**
>
> フィルターセットはユーザーアカウントごとに保存されます。保存されたフィルターセットを管理するには、**管理**を選択します。

> 特定のコンピューター、セッション、マシンカタログ、アプリケーション、またはデリバリーグループに関する情報を表示するには、検索機能を使用します。Web Studioで**検索**を選択すると、いくつかのオプションが表示されます。

頻繁に使用するフィルター*フィールド*を検索バーにピン留めすると、簡単にアクセスできます。たとえば、フィルターベースの検索を実行した後、**割り当てタイプ**を検索バーにピン留めしたいとします。次の手順に従います。

> - デフォルトでは、**名前**、**セッション状態**、**障害状態**のフィルターがビューにピン留めされています。フィルターを選択して式を作成します。フィルターをカスタマイズするには、省略記号をクリックします。表示されるウィンドウで、次の操作を実行できます。
>
> - フィルターをピン留めまたはピン留め解除します。ピン留め解除されたフィルターは一度限りの使用であり、保存されません。
>
> - フィルターをクリックしてビューに追加します。
>
> - フィルターをクリアして、現在のフィルター検索をクリアし、ピン留め解除されたフィルターを削除します。
>
> - 演算子をクリックして、**すべて一致**（**AND**演算子）または**いずれか一致**（**OR**演算子）を切り替えます。**すべて一致**に設定すると、すべてのフィルター条件に一致

する結果が検索で返されます。いずれか一致に設定すると、いずれかのフィルター条件に一致する結果が検索で返されます。

- 星の記号をクリックして、使用中のフィルターを保存します。保存された項目はフィルターセットとして知られています。保存された項目は「保存済みフィルターセット」リストに表示されます。（リストにアクセスするには、検索ボックスを選択します。）保存されたフィルターセットをクリックして、検索にフィルターを適用できます。保存されたフィルターセットを管理するには、検索ボックスを選択し、**管理**を選択します。

フィルターセットを管理(/en-us/citrix-virtual-apps-desktops/2511/media/manage-filter-sets.png)

1. 検索ボックスをクリックします。最近の検索と保存されたフィルターセットがドロップダウンリストに表示されます。以前の検索またはフィルターセットをクリックすると、クイック検索を実行できます。

検索ボックスに入力すると、プロンプト付きのメニューが表示され、検索をすばやく絞り込むのに役立つさまざまな検索オプションが提供されます。入力したコンテンツが*VM01*であるとします。次のいずれかのプロンプトを選択します。

- マシン名またはDNS名
- マシンカタログ名
- デリバリーグループ名
- セッションユーザー名
- セッションクライアント名
- セッションをホストしているVMのフレンドリ名（ハイパーバイザーで使用されているもの）
- ホストサーバー名

一般的な検索を実行すると、Citrix Virtual Apps and Desktops は以下の条件で一致するものを検索し、関連する結果を提供します。

- **名前**。マシン名またはDNS名で検索します。
- **マシンカタログ**。マシンカタログ名で検索します。
- **デリバリーグループ**。デリバリーグループ名で検索します。
- **ユーザー**。セッションユーザー名で検索します。

- **クライアント**。セッションクライアント名で検索します。
- **VM**。ホストされているマシン名で検索します。これは、ハイパーバイザーが使用するホストされているマシンのフレンドリ名です。
- **ホスティングサーバー名**。ホスティングサーバー名で検索します。

ユーザー、デスクトップグループ、カタログ、マシンなどの特定の項目を検索する場合、一般的な検索は必要な情報を見つける便利な方法を提供します。

マシンカタログまたはデリバリーグループを検索する

マシンカタログノードとデリバリーグループノード内でリソースを検索および特定できます。これらのノードの検索機能は、検索ノードと同じインターフェイスを提供し、Citrix Virtual Apps and Desktops 全体でシームレスな検索エクスペリエンスを提供します。

一般的な検索とフィルターベースの検索を実行できます。マシンカタログでは、次のフィルターが利用可能です。

- **カタログ名**。マシンカタログの名前で検索します。
- **割り当ての種類**。静的（専用）またはランダム（プール）割り当て、あるいはその両方でフィルターします。
- **プロビジョニングの種類**。手動またはMCSプロビジョニング方法、あるいはその両方でフィルタリングします。
- **セッションサポート**。シングルセッションまたはマルチセッションマシン、あるいはその両方でフィルタリングします。
- **割り当て済み数**。割り当て済みマシンの数でフィルタリングします。
- **永続性**。非永続的（破棄）または永続的（ローカルディスク上）なマシンの変更、あるいはその両方でフィルタリングします。
- **マシンの種類**。物理マシンまたは仮想マシンの種類、あるいはその両方でフィルタリングします。

デリバリーグループでは、次のフィルターが利用可能です。

- **グループ名**。デリバリーグループの名前で検索します。
- **説明**。デリバリーグループ作成時に指定されたデリバリーグループの説明でフィルタリングします。
- **セッションサポート**。シングルセッションまたはマルチセッションマシン、あるいはその両方でフィルタリングします。

- **マシンID**。マシンのIDでフィルタリングします。
- **Remote PCアクセス**。Remote PCアクセス マシンでフィルタリングします。
- **メンテナンスモード**。メンテナンスモードのマシン（オン、オフ、またはその両方）でフィルタリングします。
- **グループの状態**。グループの状態によってフィルタリングします。（> の オプションは、アプリケーションとデスクトップの配信を停止するかどうかを制御します。）
- **割り当ての種類**。静的（専用）またはランダム（プール）の種類、あるいはその両方でフィルタリングします。

一般検索を実行すると、Citrix Virtual Apps and Desktopsは以下の条件で項目を検索し、関連する結果を提供します。

- マシンカタログ:
  - 名前: フォルダーパスを含む名前でマシンカタログを検索します。
  - マシンカタログ: 名前でマシンカタログを検索します。
  - 説明。カタログ作成時に指定されたマシンカタログの説明で検索します。
- デリバリーグループ:
  - デリバリーグループ名: 名前でデリバリーグループを検索します。
  - 説明: デリバリーグループ作成時に指定されたデリバリーグループの説明で検索します。

アプリケーショングループの検索

アプリケーショングループの一般的な検索とフィルターベースの検索を実行できます。アプリケーショングループでは、次のフィルターを使用できます。

- **名前**。アプリケーショングループの名前でフィルターします。
- **タグ**。アプリケーショングループのタグでフィルターします。
- **説明**。アプリケーショングループ作成時に指定されたアプリケーショングループの説明でフィルターします。
- **デリバリーグループ**。アプリケーショングループのデリバリーグループでフィルターします。
- **状態**。アプリケーショングループの状態によってフィルターします。

表示する列をカスタマイズする

列をカスタマイズする際、**パフォーマンスが低下します**というラベルが付いた列が表示されます。これらの列を選択すると、コンソールのパフォーマンスが低下する可能性があります。カスタマイズが完了すると、選択した列を表示するようにテーブルが更新されます。これらの列が存在すると、テーブルを更新する際に遅延が発生する可能性があります。

カスタマイズにパフォーマンスを低下させる列が含まれている場合、それらを保持するかどうかを決定するよう求められます。プロンプトは、ブラウザウィンドウを更新するか、コンソールからサインアウトして再度サインインした後に表示されます。列を保持することにした場合は、次の考慮事項に注意してください。

- コンソールのパフォーマンスを確保するため、テーブルを1分間に1回以上更新することはできません。この制限は、**シングルセッションOSマシン**、**マルチセッションOSマシン**、**セッション**のすべてのタブに適用されます。より頻繁な更新が必要な場合は、パフォーマンスを低下させるすべての列を削除してください。

検索結果をCSVファイルにエクスポートする

検索結果（最大10,000項目）をCSVファイルにエクスポートできます。ファイルはブラウザのデフォルトのダウンロード場所に保存されます。

この機能は、マシンとセッションの両方で利用できます。検索結果をエクスポートするには、右上隅のエクスポートアイコンをクリックします。エクスポートには最大1分かかる場合があります。

検索ノードの各タブでは、エクスポートの実行中に別のエクスポートを実行することはできません。

検索を強化するためのヒント

検索機能を使用する際は、以下のヒントを参考にしてください。

- **検索**ノードで、任意の列を選択して項目を並べ替えます。
- 検索および並べ替えが可能な表示に含める特性をさらに表示するには、**表示する列**を選択するか、任意の列をクリックして**表示する列**を選択します。**表示する列**ウィンドウで、表示したい項目の横にあるチェックボックスをオンにし、**保存**を選択して終了します。

> **注:**

> パフォーマンスを低下させる列には、**パフォーマンスを低下させる**というラベルが付けられています。

- マシンに接続されているユーザーデバイスを見つけるには、**クライアント (IP)** と **Is** を使用し、デバイスのIPアドレスを入力します。
- アクティブなセッションを見つけるには、**セッション状態**、**Is**、および **接続済み**を使用します。
- デリバリーグループ内のすべてのマシンを一覧表示するには、左側のペインで**デリバリーグループ**を選択します。グループを選択し、アクションバーまたはコンテキストメニューから**マシンの表示**を選択します。
- MCSプロビジョニングされたマシンを特定のプロパティですばやく絞り込むには、ハードウェアビューで利用可能な**検索**バーを使用します。

ソート操作を実行する際は、以下の考慮事項に留意してください。

- アイテム数が5,000を超えない限り、任意の列をクリックしてアイテムをソートできます。数が5,000を超えると、名前または現在のユーザーでのみソートできます（現在表示しているタブによって異なります）。ソートを有効にするには、フィルターを使用してアイテム数を5,000以下に減らしてください。
- アイテム数が500より多く、5,000以下の場合は、次のようになります。
  - ソートパフォーマンスを向上させるため、すべてのデータをローカルにキャッシュします。**シングルセッションOSマシン**タブと**マルチセッションOSマシン**タブでは、列（**名前**列を除く任意の列）を初めてクリックしてソートするときにデータをキャッシュします。**セッション**タブでは、列（**現在のユーザー**列を除く任意の列）を初めてクリックしてソートするときにデータをキャッシュします。その結果、ソートの完了に時間がかかります。パフォーマンスを向上させるには、名前または現在のユーザーでソートするか、フィルターを使用してアイテム数を減らしてください。
  - テーブルの下に表示される次のメッセージは、データがキャッシュされていることを示します: 最終更新: `<the time when you refreshed the table>`。この場合、ソート操作は以前にロードされたアイテムに基づいています。これらのアイテムは最新ではない可能性があります。最新の状態にするには、更新アイコンをクリックしてください。

表示する列をカスタマイズする

日常業務に不可欠なプロパティとステータスを表示するために、パーソナライズされたメインビューを作成します。詳細な手順は次のとおりです。

1. **検索**ノードで、必要に応じて、**マルチセッションOSマシン**、**シングルセッションOSマシン**、または**セッション**タブを選択します。
2. アクションバーの**表示する列**アイコンをクリックし、列を選択します。

   利用可能な列とその説明の詳細については、マシン列とセッション列を参照してください。

列を選択する際、**パフォーマンスを低下させる**というラベルが付いた列が表示されることがあります。これらの列を選択すると、コンソールのパフォーマンスが低下する可能性があります。以下の考慮事項に留意してください。

- カスタマイズが完了すると、選択した列を表示するためにテーブルが更新されます。これらの列が存在すると、テーブルを更新する際に遅延が発生する可能性があります。
- ブラウザを更新するか、コンソールからサインアウトして再度サインインすると、それらの列を保持するかどうかを尋ねるメッセージが表示されます。保持することを選択した場合、最適なコンソールパフォーマンスを維持するため、テーブルの更新は1分間に1回までに制限されます。より頻繁に更新するには、パフォーマンスを低下させる列を削除してください。

マシンとセッションの管理

「Search」ノードのアクションを使用して、マシンとセッションの問題をトラブルシューティングしたり、ユーザー要求を処理したりします。

知っておくと良いこと

マシンはさまざまなレベルで管理できます。

- 個々のマシンレベル。**Search** ノードを使用して、ターゲットマシンを特定し、アクションを実行します。
- マシンカタログレベル。カタログのマスターイメージの変更、カタログからのマシンの削除、カタログへのマシンの追加など。詳細については、「マシンカタログの管理」を参照してください。
- デリバリーグループレベル。グループ内のマシンのメンテナンスモードのオン/オフなど。詳細については、「デリバリーグループの管理」を参照してください。

個々のセッションレベルに加えて、デリバリーグループレベルでもセッションを管理できます。たとえば、デリバリーグループのセッションの事前起動と維持を構成するなどです。詳細については、「デリバリーグループの管理」を参照してください。

マシンまたはセッションでアクションを実行する

個々のインスタンスレベルでマシンまたはセッションを管理するには、次の手順に従います。

1. **Search** ノードで、**Multi-session OS Machines**、**Single-session OS Machines**、または **Sessions** タブを選択します。
2. 必要に応じて、1つ以上のインスタンスを選択します。
3. アクションバーまたは右クリックメニューから、それらのインスタンスで発生した問題やユーザー要求に基づいてアクションを選択します。

   利用可能なアクションとその説明の詳細については、「マシンアクション」および「セッションアクション」を参照してください。

> **注：**
>
> 2つ以上のインスタンスを選択した場合、それらすべてに適用されるアクションのみが利用可能です。

マシンまたはセッションデータをCSVファイルにエクスポートする

タブに表示されているインスタンス（マシンまたはセッション）のリスト（最大30,000項目）をCSVファイルにエクスポートします。詳細な手順は次のとおりです。

1. **検索**ノードで、必要に応じて**マルチセッションOSマシン**、**シングルセッションOSマシン**、または**セッション**タブを選択します。
2. 右上隅にある**エクスポート**アイコンをクリックします。
3. 表示されるダイアログボックスで、**続行**をクリックします。

   エクスポートが完了するまでに数分かかる場合があります。ファイルはブラウザのデフォルトのダウンロードフォルダにあります。

> **注：**
>
> **検索**ノードの各タブで、エクスポートの実行中は、別のエクスポートを実行できません。

マシンのアクションと列

この記事では、マシンのアクションと列を説明とともに一覧表示します。

アクション

マシンで実行できるアクションとその説明を表示します。

アクション	説明	適用対象
デリバリーグループから削除	デリバリーグループからマシンを削除します。	シングルセッションおよびマルチセッション
デリバリーグループに追加	マシンをデリバリーグループに追加します。	シングルセッションおよびマルチセッション
セッションの表示	マシンで実行中のセッションを表示します	シングルセッションおよびマルチセッション
タグの管理	マシンにタグを追加して管理します。タグの一般的な使用例について詳しくは、「タグ」を参照してください。	シングルセッションおよびマルチセッション
メンテナンスモードをオンにする	パッチを適用する前、またはトラブルシューティングのために、マシンをメンテナンスモードにします。 このモードでは、そのマシンへの新しい接続が防止されます。ユーザーはそのマシン上の既存のセッションに接続できますが、そのマシン上で新しいセッションを開始することはできません。	シングルセッションおよびマルチセッション
メンテナンスモードをオフにする	マシンのメンテナンスモードをオフにします。	シングルセッションおよびマルチセッション
VDAのアップグレード	マシンのVDAをアップグレードします。	特定の要件を満たすシングルセッションまたはマルチセッションOSマシン: 詳細はこちら。
ログオフ	マシンを強制的にログオフする	シングルセッションおよびマルチセッション
削除	マシンカタログからVMを削除しますが、ハイパーバイ	シングルセッションおよびマルチセッション

アクション	説明	適用対象
	ザーまたはクラウドサービス上ではそのまま残します。	
ユーザーの変更	特定のユーザーにマシンを割り当てる。	シングルセッションの*静的*マシン。
起動	マシンを起動する。	シングルセッションおよびマルチセッション
シャットダウン	マシンをシャットダウンする。	シングルセッションおよびマルチセッション
再起動	マシンを再起動します	シングルセッションおよびマルチセッション
サスペンド	マシンを休止状態またはサスペンド状態にします。マシンをサスペンドすると、Delivery Controller はマシンのメモリ内容をファイルに保存し、マシンをシャットダウンします。	シングルセッションOSマシン
再開	サスペンドされたマシンを再開します。サスペンドされたマシンを再開すると、Delivery Controller はマシンを起動し、以前の状態に復元します。	シングルセッションOSマシン
強制再起動	マシンを強制的に再起動します。	シングルセッションOSマシン
強制シャットダウン	マシンを強制的にシャットダウンします。	シングルセッションOSマシン

列

タイプ別にすべてのマシン列とその説明を表示します。

- マシン
- マシンの詳細

- アプリケーション
- ホスティング
- 接続
- 登録
- セッションの詳細
- セッション

マシン

マシンカテゴリの列。

列	説明	適用対象
名前	マシンのDNSホスト名。	シングルセッションおよびマルチセッション
マシンカタログ	マシンが属するカタログの名前。	シングルセッションおよびマルチセッション
デリバリーグループ	マシンが属するデリバリーグループの名前。	シングルセッションおよびマルチセッション
ユーザー表示名	マシンに関連付けられているユーザーのフルネーム（通常、`Firstname Lastname`の形式）。関連付けられているユーザーとは、共有マシンの現在のユーザーと、専用マシンの割り当て済みユーザーを指します。	シングルセッションおよびマルチセッション
ユーザー	マシンに関連付けられているユーザーのユーザー名（「domain\user」	シングルセッションおよびマルチセッション

列	説明	適用対象
	の形式）。関連付けられているユーザーとは、共有マシンの現在のユーザーと、専用マシンの割り当て済みユーザーを指します。	
ユーザープリンシパル名	マシンに関連付けられているユーザーのユーザープリンシパル名（「user@domain」の形式）。関連付けられているユーザーとは、共有マシンの現在のユーザーと、専用マシンに割り当てられているユーザーです。	シングルセッションおよびマルチセッション
デスクトップ表示名	セッションの起動に元々使用されたマシンの公開名。Citrix Workspace™アプリまたはStoreFrontに表示される名前です。	シングルセッションのみ
	注： デスクトップの表示を変更するには、表示名の変更にマシンプロパティの更新が含まれるため、**Perform Machine Update** 権限が必要です。	
デスクトップの状態	マシンに対する未解決のデスクトップ状態のリスト。可能な	シングルセッションおよびマルチセッション

列	説明	適用対象
	値：Unknown、CPU、ICALatency、UPMLogonTime。	
割り当てタイプ	マシンの割り当てタイプ：ユーザーに永続的に割り当てられる場合は **Permanent**。ランダムに割り当てられる場合は **Random**。	シングルセッションおよびマルチセッション
メンテナンスモード	マシンがメンテナンスモードであるかどうかを示します。	シングルセッションおよびマルチセッション
Windows接続設定	Windowsによって報告されたログオンモード。	マルチセッションのみ
	指定できる値: LogonEnabled、Draining、DrainingUntilRestart、および LogonDisabled。	
割り当て済み	専用デスクトップがユーザーまたはクライアント（名前/アドレス）に割り当てられているかどうかを示します。ユーザーは明示的に割り当てることも、マシンの初回使用時に割り当てることもできます。	シングルセッションおよびマルチセッション
物理マシン	マシンが物理マシンであるかどうかを示します。`True` はマ	シングルセッションおよびマルチセッション

列	説明	適用対象	
	シンが物理マシンであることを示し、Delivery Controllerによって電源管理されていないことを意味します。`False` はその逆を示します。		
プロビジョニングの種類	マシンがプロビジョニングされた方法。指定可能な値 • 手動: PVSまたはMCSを使用してプロビジョニングされていません。 • PVS: PVSを使用してプロビジョニングされています (物理マシン、ブレードマシン、仮想マシン)。 • MCS: MCSを使用してプロビジョニングされています (VMのみ)。	シングルセッションおよびマルチセッション	
スケジュールされた再起動	マシンのスケジュールされた再起動操作の状態。指定可能な値	シングルセッションおよびマルチセッション	

列	説明	適用対象	
	• なし: 再起動はスケジュールされていません。 • 保留中: 再起動を待機中ですが、使用可能です。 • ドレイン中: 再起動を待機中で、新しいセッションには使用できません。ただし、既存の接続への再接続は引き続き許可されます。 • 進行中: スケジュールされた再起動がアクティブに実行されています。 • 自然: 自然な再起動が進行中です。マシンは再起動を待機しています。		
ゾーン	マシンが配置されているゾーンの名前です。	シングルセッションおよびマルチセッション	
状態	セッション状態、登録状態、電源状態など、さまざまな特定の状態から導き出さ	シングルセッションおよびマルチセッション	

列	説明	適用対象
	れる、マシンに関連付けられたデスクトップの全体的な状態です。	
	可能な状態: オフ、未登録、利用可能、切断済み、使用中、準備中。	
タグ	マシンに関連付けられているタグのリストです。	シングルセッションおよびマルチセッション
VDAアップグレード	VDAパッケージアップグレードアクションのマシン状態です。	シングルセッションおよびマルチセッション
	指定可能な値: MissingUpgradeType、UpgradeScheduled、UpgradeAvailable、UpToDate、および Unknown。	
サスペンド可能	マシンが電源アクション（サスペンドと再開）をサポートしているかどうかを示します。	シングルセッションおよびマルチセッション
ロード評価インデックス	マシンの全体的な実効負荷インデックス（パーセンテージ）。詳細については、「CTX202150」を参照してください。	マルチセッションのみ

列	説明	適用対象
ロードインデックス	現在のロードインデックス。詳細については、「詳細はこちら」を参照してください。	マルチセッションのみ
ドレイン状態	マシンがドレイン中で、マシン上のすべてのセッションが終了した後にシャットダウンするかどうかを示します。Trueは、電源管理されたマルチセッションマシンにのみ表示されます。	マルチセッションのみ
	注: マシンがメンテナンスモードの場合、シャットダウンしません。メンテナンスモードが解除された後にのみシャットダウンします。	

マシンの詳細

マシンの詳細カテゴリの列。

列	説明	適用対象
エージェントバージョン	マシンにインストールされているCitrix Virtual Delivery Agent (VDA) のバージョン。	シングルセッションおよびマルチセッション
IPアドレス	マシンのIPアドレス。	シングルセッションおよびマルチセッション
割り当て済み	専用デスクトップがユーザーまたはクライアント（名前/アドレス）に割り当てられてい	シングルセッションおよびマルチセッション

列	説明	適用対象
	るかどうかを示します。ユーザーは明示的に割り当てられるか、マシンの初回使用時に割り当てられます。	
OSの種類	マシンで実行されているオペレーティングシステムの種類。	シングルセッションのみ

アプリケーション

アプリケーションカテゴリの列。

列	説明	適用対象
使用中のアプリケーション	マシンで使用中のアプリケーションのリスト（ブラウザ名として表示されます）。	シングルセッションおよびマルチセッション
公開済みアプリケーション	マシンによって公開されたアプリケーションのリスト（ブラウザ名として表示されます）。	シングルセッションおよびマルチセッション

接続

接続カテゴリの列。

列	説明	適用対象
クライアント (IP)	マシンに接続されているクライアントのIPアドレス。	シングルセッションのみ
クライアント	マシンに接続されているクライアントのホスト名。	シングルセッションのみ
プラグインバージョン	接続されているクライアント上のCitrix Workspaceアプリのバージョン。	シングルセッションのみ

列	説明	適用対象
接続元	受信接続のホスト名。通常、ゲートウェイ、ルーター、またはクライアントです。	シングルセッションのみ
接続元 (IP)	受信接続のIPアドレス。通常、ゲートウェイ、ルーター、またはクライアントです。	シングルセッションのみ
接続タイプ	セッションに使用されるプロトコル。可能な値：HDX、RDP、およびConsole。注：XenDesktop® 5 VDA上のコンソールセッションの場合、このフィールドは空白になります。	シングルセッションのみ
最終接続時刻 (UTC)	失敗または成功した、最後に検出された接続試行の時刻。	シングルセッションおよびマルチセッション
最終接続ユーザー	最後にマシンへの接続を試行したユーザーのSAM名（「DOMAIN\user」の形式）。SAM名が利用できない場合は、SIDが使用されます。	シングルセッションおよびマルチセッション
Secure ICA® アクティブ	現在のセッションでSecureICAがアクティブであるかどうかを示します。マルチセッションマシンでは常にnullです。	シングルセッションおよびマルチセッション

ホスティング

ホスティングカテゴリの列。

列	説明	適用対象
VM	セッションを実行しているホストされたマシンのフレンドリ名で、そのハイパーバイザーによって使用されます。マシンの DNS 名または AD 名と必ずしも一致するとは限りません。	シングルセッションおよびマルチセッション
ホスティングサーバー名	管理対象の場合、マシンをホストしているハイパーバイザーの DNS 名。	シングルセッションおよびマルチセッション
接続	セッションをホストしているマシンに割り当てられているホスト接続の名前。	シングルセッションおよびマルチセッション
保留中の更新	ホストされているマシンのVMイメージが古くなっており、次回の再起動時に新しいイメージに更新される必要があるかどうかを示します。	シングルセッションおよびマルチセッション
ユーザー変更の永続性	ユーザーの変更がどのように処理されるかを示し、変更が永続的であるかどうかを示します: • OnLocal: 永続的。ユーザーの変更はローカルに保存されます。	シングルセッションおよびマルチセッション

列	説明	適用対象	
	• Discard: 非永続的。ユーザーの変更は破棄されます。		
保留中の電源操作	マシンに保留中の電源操作があるかどうかを示します。	シングルセッションおよびマルチセッション	
電源状態	マシンの電源状態。可能な値: Unmanaged、Unknown、Unavailable、Off、On、Suspended、TurningOn、TurningOff、Suspending、Resuming。	シングルセッションおよびマルチセッション	
使用後にシャットダウンします	電源管理されたシングルセッションマシンにのみ適用されます。マシンが汚染されており、すべてのセッションが終了した後にシャットダウンするかどうかを示します。	シングルセッションのみ	
	注: マシンがメンテナンスモードの場合、シャットダウンしません。メンテナンスモードから解除された後にのみシャットダウンします。		

登録

登録カテゴリの列。

列	説明	適用対象
最終登録失敗	ブローカーへのマシンの最終登録解除の理由。 指定できる値は、AgentShutdown、AgentSuspended、AgentRequested、IncompatibleVersion、AgentAddressResolutionFailed、AgentNotContactable、AgentWrongActiveDirectoryOU、EmptyRegistrationRequest、MissingRegistrationCapabilities、MissingAgentVersion、InconsistentRegistrationCapabilities、NotLicensedForFeature、UnsupportedCredentialSecurityVersion、InvalidRegistrationRequest、SingleMultiSessionMismatch、FunctionalLevelTooLowForCatalog、FunctionalLevelTooLowForDesktopGroup、PowerOff、DesktopRestart、	シングルセッションおよびマルチセッション

列	説明	適用対象
	DesktopRemoved、AgentRejectedSettingsUpdate、SendSettingsFailure、SessionAuditFailure、SessionPrepareFailure、ContactLost、SettingsCreationFailure、UnknownError、およびBrokerRegistrationLimitReachedです。	
最終登録失敗時刻 (UTC)	マシンの最終登録解除時刻。	シングルセッションおよびマルチセッション
登録状態	マシンの登録状態。指定できる値は、Unregistered、Initializing、Registered、およびAgentErrorです。	シングルセッションおよびマルチセッション
障害状態	マシンの現在の障害状態の概要。可能な値 • None: 障害なし。マシンは正常です。 • FailedToStart: マシンの最後の電源投入操作が失敗しました。	シングルセッションおよびマルチセッション

列	説明	適用対象	
	• StuckOnBoot: 電源投入後、マシンが起動できませんでした。 • Unregistered: マシンが予期された期間内に登録できませんでした、または登録が拒否されました。		
	MaxCapacity。マシンが最大容量に達していることを報告しています。		

セッションの詳細

セッションの詳細カテゴリの列。

列	説明	適用対象
起動元	現在ブローカーされているセッションの起動に使用されたStoreFrontサーバーのホスト名。マルチセッションマシンでは常にnullです。	シングルセッションおよびマルチセッション
起動元 (IP)	現在ブローカーされているセッションの起動に使用されたStoreFrontサーバーのIPアドレス。マルチセッションマシンでは常にnullです。	シングルセッションおよびマルチセッション
セッション変更時刻 (UTC)	現在のセッションの最終状態変更時刻。	シングルセッションのみ

列	説明	適用対象
SmartAccessフィルター	現在のセッションのSmart Accessタグ。マルチセッションマシンでは常にnullです。	シングルセッションおよびマルチセッション

セッション

セッションカテゴリの列。

列	説明	適用対象
セッション状態	現在のセッションの状態。可能な値: Other、PreparingSession、Connected、Active、Disconnected、Reconnecting、NonBrokeredSession、およびUnknown。	シングルセッションのみ
現在のユーザー	現在のセッションのユーザー名（「DOMAIN\user」の形式）。	シングルセッションのみ
開始時刻 (UTC)	現在のセッションの開始時刻。	シングルセッションのみ
セッション数	マシン上のセッション数。	マルチセッションのみ

セッションのアクションと列

この記事では、参照用にマシンのアクションと列を説明とともに一覧表示します。

アクション

セッションで実行できるアクションとその説明を表示します。

アクション	説明	適用対象セッション
ログオフ	セッションからユーザーをログオフします。	シングルセッションOSマシンまたはマルチセッションOSマシン

アクション	説明	適用対象セッション
メッセージを送信	セッションのユーザーにメッセージを送信します。	シングルセッションOSマシンまたはマルチセッションOSマシン
マシンの表示	セッションのホストマシンを表示します。	シングルセッションOSマシンまたはマルチセッションOSマシン
切断	セッションを切断します。セッションが切断されても、セッションはアクティブなままでアプリケーションは実行され続けますが、ユーザーデバイスはDelivery Controllerと通信しなくなります。	シングルセッションOSマシンまたはマルチセッションOSマシン
マシンのシャットダウン	セッションに関連付けられているマシンをシャットダウンします。	シングルセッションOSマシン
マシンの再起動	セッションに関連付けられているマシンを再起動します。	シングルセッションOSマシン

列

セッションの列とその説明を表示します。

列	説明
現在のユーザー	ユーザーの名前。ユーザーのユーザープリンシパル名(UPN)。
名前	セッションをホストしているマシンのDNSホスト名。
デリバリーグループ	セッションをホストしているマシンを含むデリバリーグループの名前。

列	説明
マシンカタログ	セッションをホストしているマシンを含むマシンカタログの名前。
エージェントバージョン	セッションをホストしているマシンにインストールされているCitrix Virtual Delivery Agent (VDA) のバージョン。
使用中のアプリケーション	セッションで使用されているアプリケーションのリスト。管理名で識別されます。
自律的に仲介済み	これは、仲介されずに直接接続によって確立されたHDX™セッションであるかどうか。
仲介時間 (UTC)	セッションが仲介された時刻。
仲介ユーザー名	ブローカーユーザーの名前。
クライアント (IP)	セッションに接続されているクライアントのIPアドレス。
クライアント	セッションに接続されているクライアントのホスト名。
プラグインバージョン	セッションに接続されているクライアントで実行されているCitrix Workspace™アプリのバージョン。
接続元	受信接続のホスト名。通常はゲートウェイ、ルーター、またはクライアントです。
接続元 (IP)	受信接続のIPアドレス。通常はゲートウェイ、ルーター、またはクライアントです。

列	説明
割り当てタイプ	セッションが共有か専用か。
非表示	セッションがユーザーから非表示になっているか、再接続できない状態であるか。
VM	セッションをホストしているVMの、ハイパーバイザーで使用されるフレンドリ名。マシンのDNS名またはAD名と必ずしも一致するとは限りません。
ホスティングサーバー名	セッションのホスティングマシンをホストしているハイパーバイザーのDNS名。
接続	セッションをホストしているマシンに割り当てられているホスト接続の名前。
更新保留中	ホストされているマシンのVMイメージが古くなっているか、次回のマシンの再起動時に新しいイメージに更新される予定であるか。
メンテナンスモード	セッションをホストしているマシンがメンテナンスモードであるか。
IPアドレス	セッションをホストしているマシンのIPアドレス。
物理であるか	セッションをホストしているマシンが物理であるか否か。`True` はマシンが物理であることを示し、Delivery Controllerによって電源管理されていないことを意味しま

列	説明
	す。`False` はそれ以外を示します。
起動元	セッションの起動に使用されたStoreFront™サーバーのホスト名。セッションがWorkspace経由で起動された場合は空白。
起動元 (IP)	セッションの起動に使用されたStoreFrontサーバーのIPアドレス。セッションがWorkspace経由で起動された場合は空白。
OSの種類	セッションをホストしているオペレーティングシステムの識別文字列。
ユーザー変更の永続性	ユーザーの変更がどのように処理されるかを示し、変更が永続的であるかどうかを示します: • OnLocal: 永続的。ユーザーの変更はローカルに保存されます。 • Discard: 非永続的。ユーザーの変更は破棄されます。
接続の種類	HDX、RDP、Consoleなど、セッションに使用されるプロトコル。 **注：** XenDesktop® 5 VDA上のコンソールセッションの場合、このフィールドは空白です。

列	説明
プロビジョニングの種類	セッションをホストしているマシンがどのようにプロビジョニングされたか： • 手動：PVSまたはMCSを使用してプロビジョニングされていません。 • PVS：PVSによってプロビジョニングされています（物理マシン、ブレードマシン、仮想マシン）。 • MCS：MCSによってプロビジョニングされています（VMのみ）。
Secure ICA® アクティブ	セッションでSecureICAがアクティブであるかどうか。
セッションの状態	セッションの状態。可能な値：Connected、Active、またはDisconnected。L7より前の機能レベルのマシン上のセッションでは、PreparingSession、Reconnecting、NonBrokeredSession、Other、Unknownなどの他の状態が発生する可能性があります。
セッション変更時刻	セッションの最新の状態変更時刻。
アプリケーションの状態	セッション内のアプリケーションの状態。可能な値: PreLogon、PreLaunched、

列	説明
	Active、Desktop、Lingering、NoApps。
セッションサポート	セッションをホストしているマシンが、複数セッションをサポートするか、単一セッションをサポートするか。
ゾーン	セッションをホストしているマシンが配置されているゾーンの名前。
SmartAccessフィルター	セッションのSmart Accessタグ。
開始時刻 (UTC)	セッションが開始された時刻。
状態	マシンの概要状態。可能な値 : Unregistered、Disconnected、InUse。
状態継続時間 (UTC)	セッションが現在の状態になってからの時間。
デリバリーコントローラー™	セッションのホストマシンが登録されているコントローラーのDNSホスト名。
ユーザー表示名	ユーザーのフルネーム。
デスクトップ表示名	セッションの起動に元々使用されたマシンの公開名。Citrix Workspaceアプリまたはストアフロントに表示される名前です。アプリケーションセッションの場合、そのアプリケーションが終了していても、セッションに起動された最初のアプリケーションの名前です。リソースが後で名前

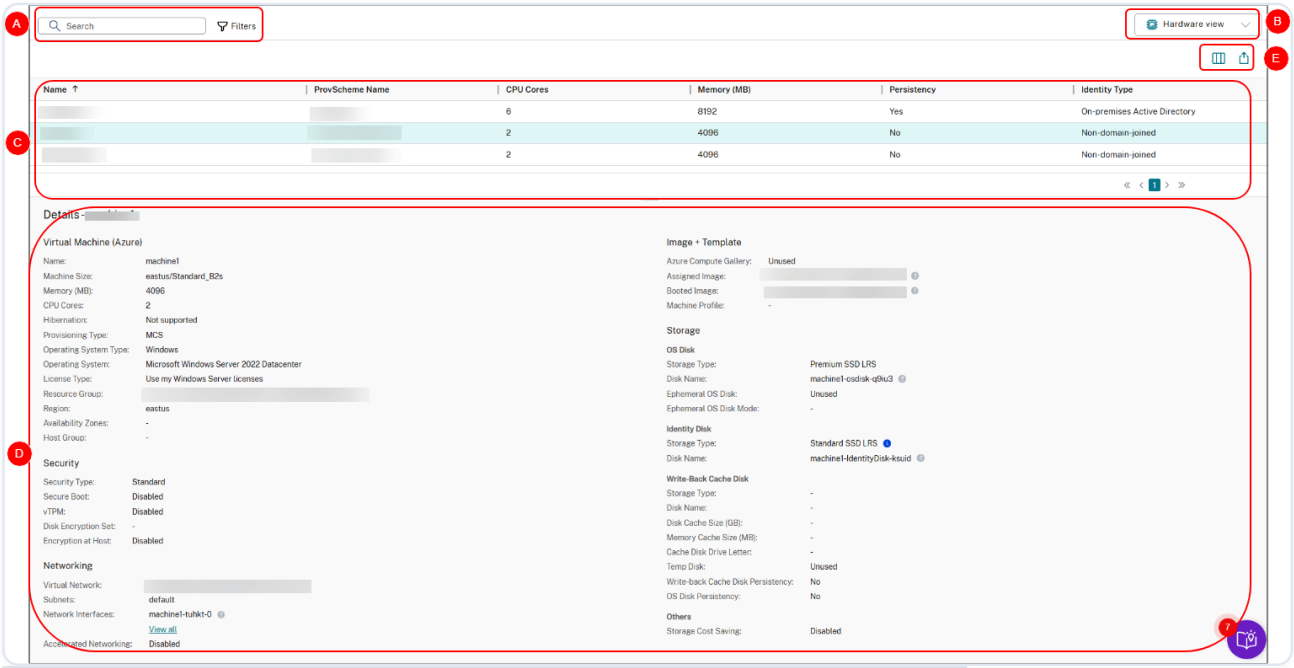
列	説明
	変更または削除されても、名前は変更されません。

MCSプロビジョニング済みマシン (検索 > ハードウェアビュー)

この記事では、**検索**ノード内の**ハードウェアビュー**を使用して、MCSプロビジョニングされたマシンとそのプロパティを表示する方法を説明します。

ハードウェアビューについて学ぶ

「**検索**」ノード内のハードウェアビューには、MCSプロビジョニングされたマシンと、マシンのセキュリティ設定、ネットワークの詳細、イメージ、マシンプロファイルの詳細を含む重要なプロパティが表示されます。



コールアウト	領域	説明
A	検索バー	クイック検索と、複雑な検索条件を定義できるフィルターベースの検索を提供します。詳細については、「マシンの検索」を参照してください。

コールアウト	領域	説明
		ヒント: 特定のプロパティでマシンをすばやく絞り込むには、フィルターを使用します。たとえば、**保留中のイメージ更新 = はい**と**IDタイプ = ActiveDirectory**を組み合わせて、イメージ更新が保留中のすべてのActive Directoryマシンを表示します。
B	デフォルトビューに切り替える	ハードウェアビューからデフォルトビューに切り替える。
C	メインビュー	MCSプロビジョニングされたマシンとその重要なプロパティを表示します。「**表示する列**」アイコンを選択して、ビューをカスタマイズできます。利用可能な列の詳細については、「マシン列」を参照してください。
D	詳細ペイン	選択したマシンの詳細情報を表示します。
E	リストレベルのアクション	表示されているリスト全体に対して実行

コールアウト	領域	説明	
		できるアクションを表示します。 • **エクスポート**アイコン: メインビューに表示されているマシンの一覧をCSVファイルにエクスポートします。 • **表示する列**アイコン: リストのメインビューをカスタマイズします。	

参照: マシン列

この表は、ハードウェアビューのすべての列とその説明を一覧表示します。

列	説明
名前	マシンのDNSホスト名。
プロビジョニングスキーム名	マシンをプロビジョニングするために使用されたプロビジョニングスキームの名前。
CPUコア	マシンに割り当てられたCPUコアの数。
メモリ (MB)	マシンに割り当てられたメモリ量 (MB単位)。
永続性	マシンのディスクとデータが再起動後も保持されるかどうかを示します。
IDタイプ	マシンのIDタイプです。

列	説明
保留中のイメージ更新	マシンのVMイメージが古くなっており、次回の再起動時に新しいイメージに更新される予定であるかどうかを示します。
最終起動時刻 (UTC)	マシンが最後に起動された日時 (UTC) です。
WBCを使用	マシンがWBC (MCSIOとも呼ばれる) で構成されているかどうかを示します。
WBCディスクサイズ (GB)	マシンのMCSIOディスクキャッシュサイズです。
WBCメモリサイズ (MB)	マシンのMCSIOメモリキャッシュサイズです。
IDプロバイダー	マシンのIDプロバイダーです。
アクティベーションの種類	Windows VDAのみ有効です。マシンのWindowsライセンスのアクティベーションの種類。値は次のとおりです: サポートされていないVDA、キー管理サービス、複数ライセンス認証キー、および無効です。

セキュリティキー

重要:

- この機能は、StoreFront™ 1912 LTSR CU2以降と組み合わせて使用する必要があります。
- Secure XML機能は、Citrix ADCおよびCitrix Gatewayリリース12.1以降でのみサポートされています。

注:

バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除され

> ました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> この機能を使用すると、承認されたStoreFrontおよびCitrix Gatewayマシンのみがデリバリーコントローラーと通信できるようになります。この機能を有効にすると、キーを含まないすべての要求はブロックされます。この機能を使用して、内部ネットワークからの攻撃から保護するための追加のセキュリティ層を追加します。

この機能を使用するための一般的なワークフローは次のとおりです。

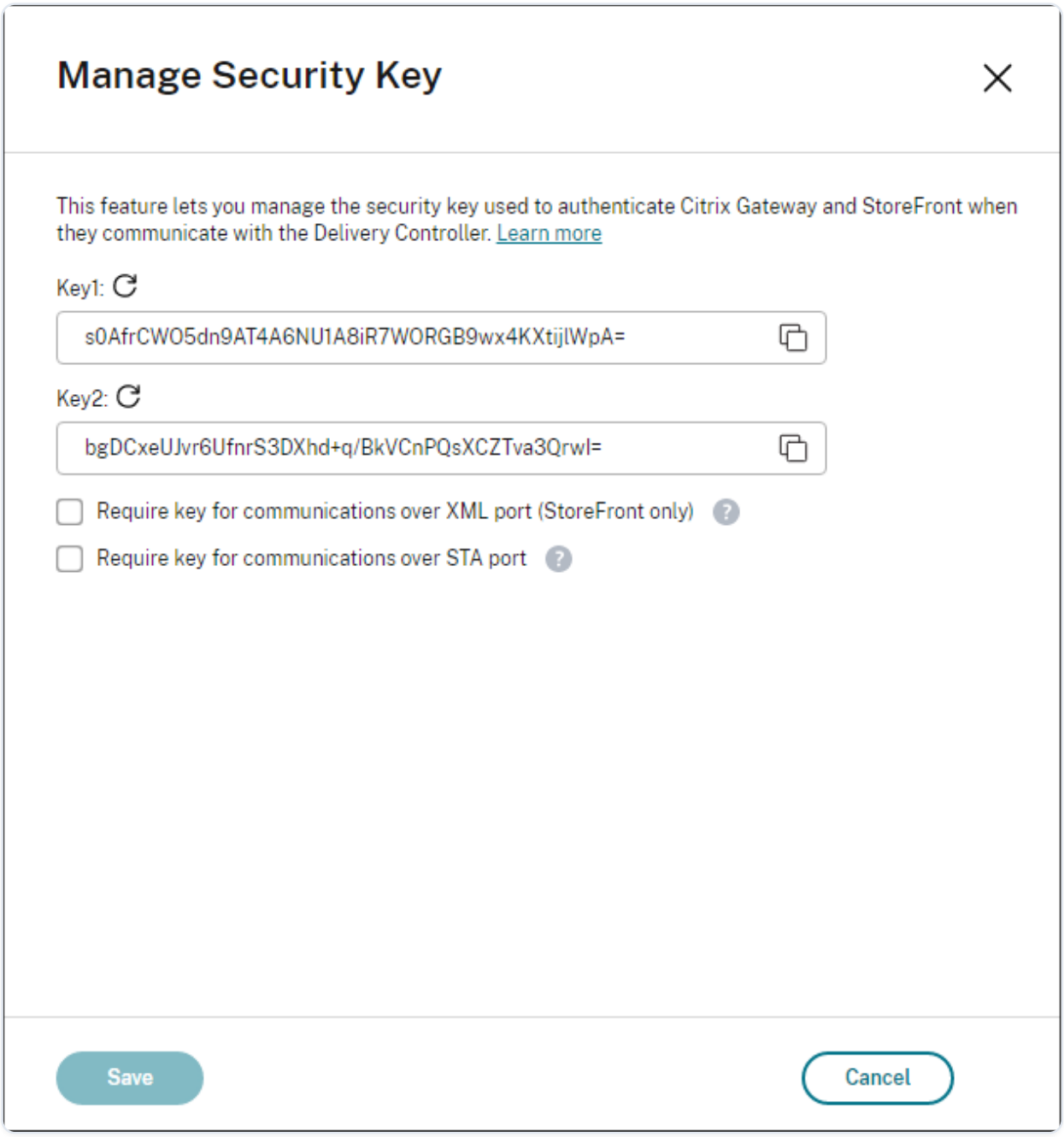
1. Web Studioを有効にして、機能設定を表示します。
2. サイトの設定を構成します。
3. StoreFrontの設定を構成します。
4. Citrix ADCの設定を構成します。

サイトの設定を構成する

Web StudioまたはPowerShellを使用して、サイトのセキュリティキー設定を構成できます。

Web Studioを使用する

1. Web Studio にサインインし、左側のペインで を選択します。
2. タイルを見つけて をクリックします。 ページが表示されます。



3. 更新アイコンをクリックしてキーを生成します。

重要:

- 使用可能なキーは2つあります。XMLポートおよびSTAポートを介した通信には、同じキーまたは異なるキーを使用できます。一度に1つのキーのみを使用することをお勧めします。未使用のキーは、キーのローテーションにのみ使用されます。
- 使用中のキーを更新するために更新アイコンをクリックしないでください。クリックすると、サービスが中断されます。

4. 通信にキーが必要な場所を選択します。

   - **XMLポートを介した通信にキーを要求する（StoreFrontのみ）**。選択した場合、XMLポートを介した通信を認証するためにキーが必要になります。StoreFrontは、このポートを介してCitrix Cloudと通信します。XMLポートの変更については、Knowledge Centerの記事CTX127945を参照してください。
   - **STAポートを介した通信にキーを要求する**。選択した場合、STAポートを介した通信を認証するためにキーが必要になります。Citrix GatewayとStoreFrontは、このポートを介してCitrix Cloudと通信します。STAポートの変更については、Knowledge Centerの記事CTX101988を参照してください。

5. をクリックして変更を適用し、ウィンドウを閉じます。

PowerShell を使用する

以下は、Web Studioの操作に相当するPowerShellの手順です。

1. シトリックス バーチャル アプリ™ アンド デスクトップ リモート パワーシェル SDK を実行します。
2. コマンドウィンドウで、次のコマンドを実行します。

   - `Add-PSSnapIn Citrix*`

3. 次のコマンドを実行して、キーを生成し、Key1 をセットアップします。

   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`

4. 次のコマンドを実行して、キーを生成し、Key2 をセットアップします。

   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`

5. 通信の認証でキーの使用を有効にするには、次のコマンドのいずれか、または両方を実行します。

   - XML ポート経由で通信を認証するには:
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - STAポート経由の通信を認証するには:
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

ガイダンスと構文については、PowerShellコマンドのヘルプを参照してください。

StoreFrontの設定を構成する

サイトの構成が完了したら、PowerShellを使用してStoreFrontの関連設定を構成する必要があります。

StoreFront サーバーで、以下の PowerShell コマンドを実行します。

XMLポート経由の通信用にキーを構成するには、コマンドを使用します。例：

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [secret]
```

次のパラメータに適切な値を入力します。

- `Path to store`
- `Resource feed name`
- `secret`

STAポート経由の通信用にキーを構成するには、`New-STFSecureTicketAuthority`および`Set-STFRoamingGateway`コマンドを使用します。例：

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

次のパラメータに適切な値を入力します。

- `Gateway name`

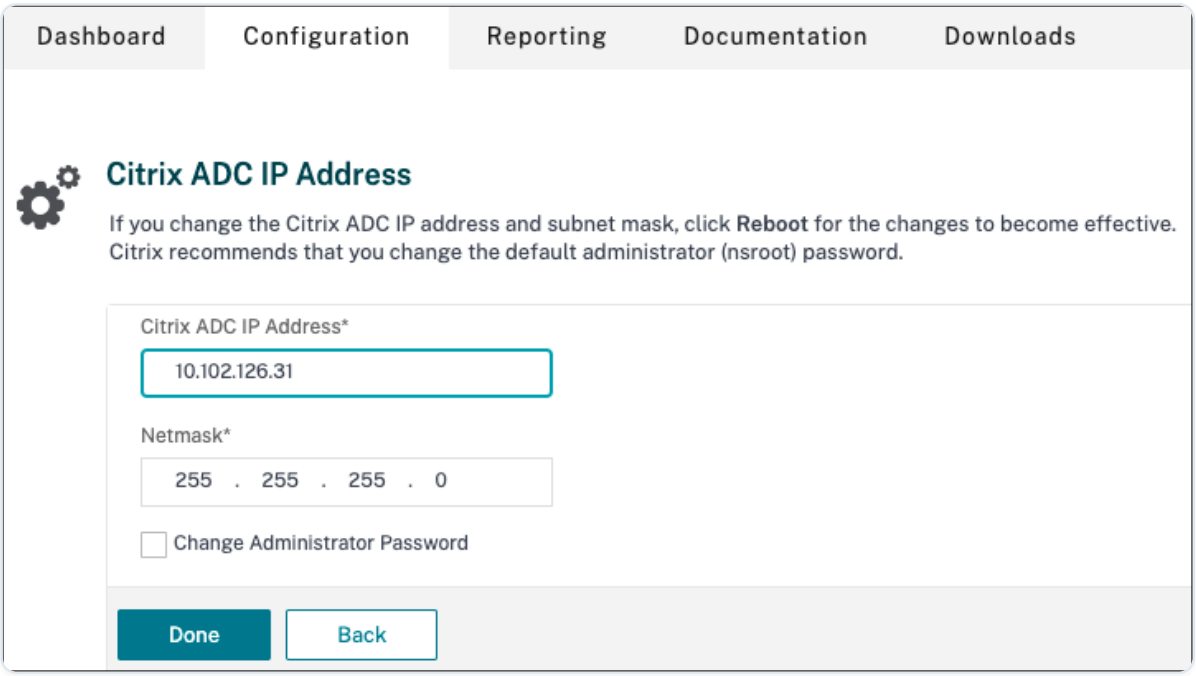
- `STA URL`
- `Secret`

ガイダンスと構文については、PowerShellコマンドのヘルプを参照してください。

Citrix ADCの設定を構成する

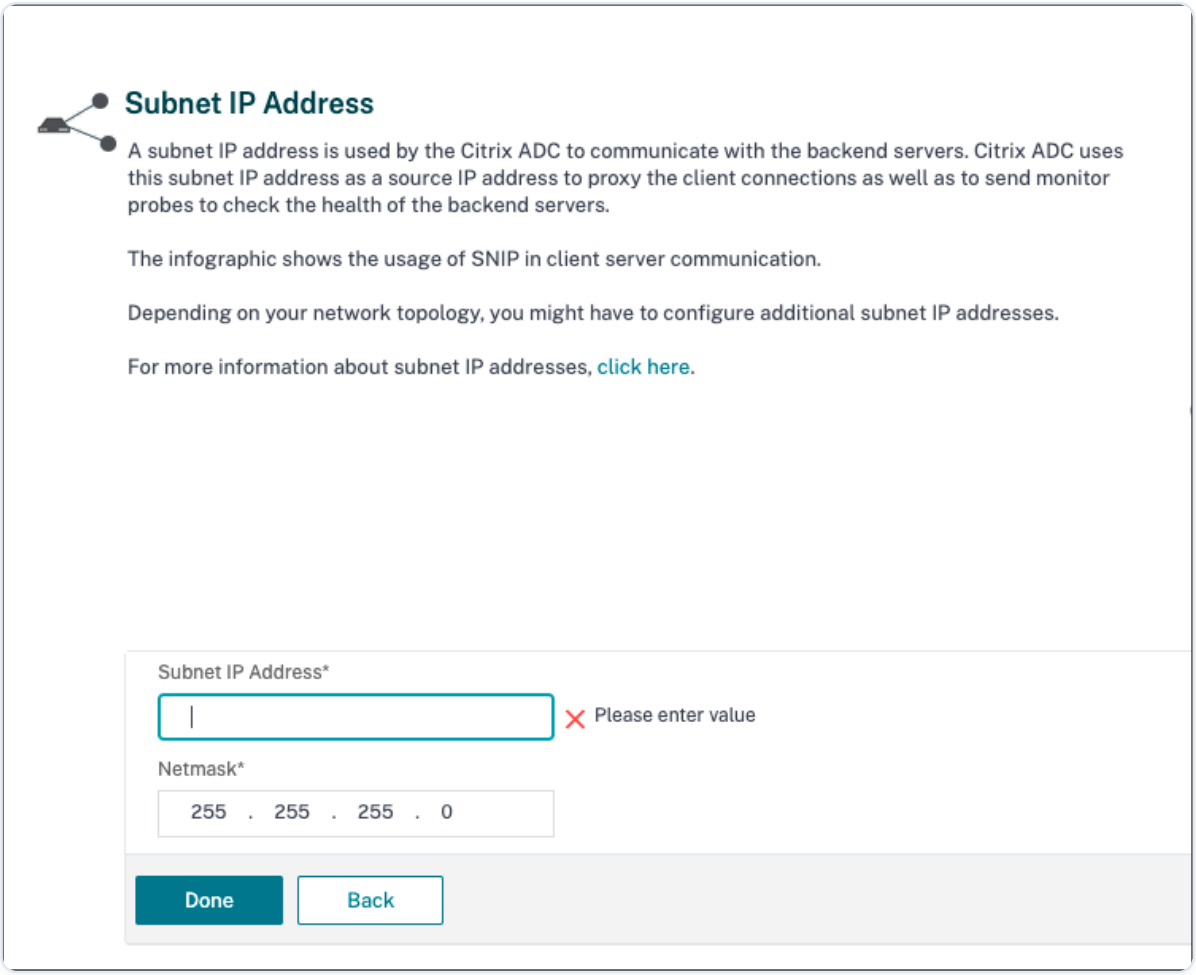
> **注:**
>
> Citrix ADCをゲートウェイとして使用しない限り、Citrix ADCでこの機能を構成する必要はありません。Citrix ADCを使用する場合は、次の手順に従ってください。

1. 以下の前提条件となる構成がすでに整っていることを確認してください。
   - 次のCitrix ADC関連のIPアドレスが構成されています。
     - Citrix ADCコンソールにアクセスするための Citrix ADC管理IP (NSIP) アドレス。詳細については、「NSIPアドレスの構成」を参照してください。

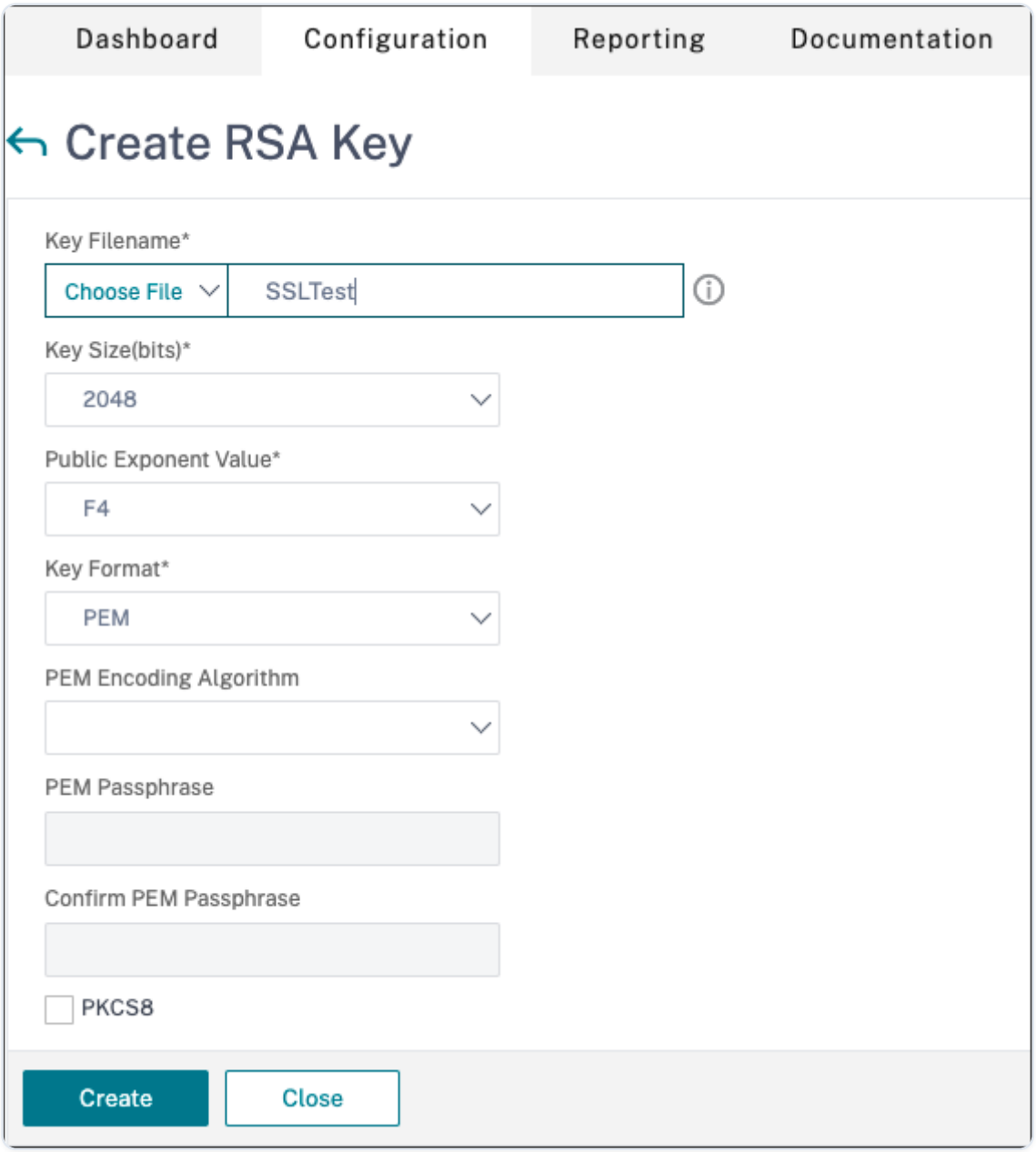


     - Citrix ADCアプライアンスとバックエンドサーバー間の通信を有効にするためのサブネットIP（SNIP）アドレス。詳細については、「サブネットIPアドレスの構成」を参照してください。

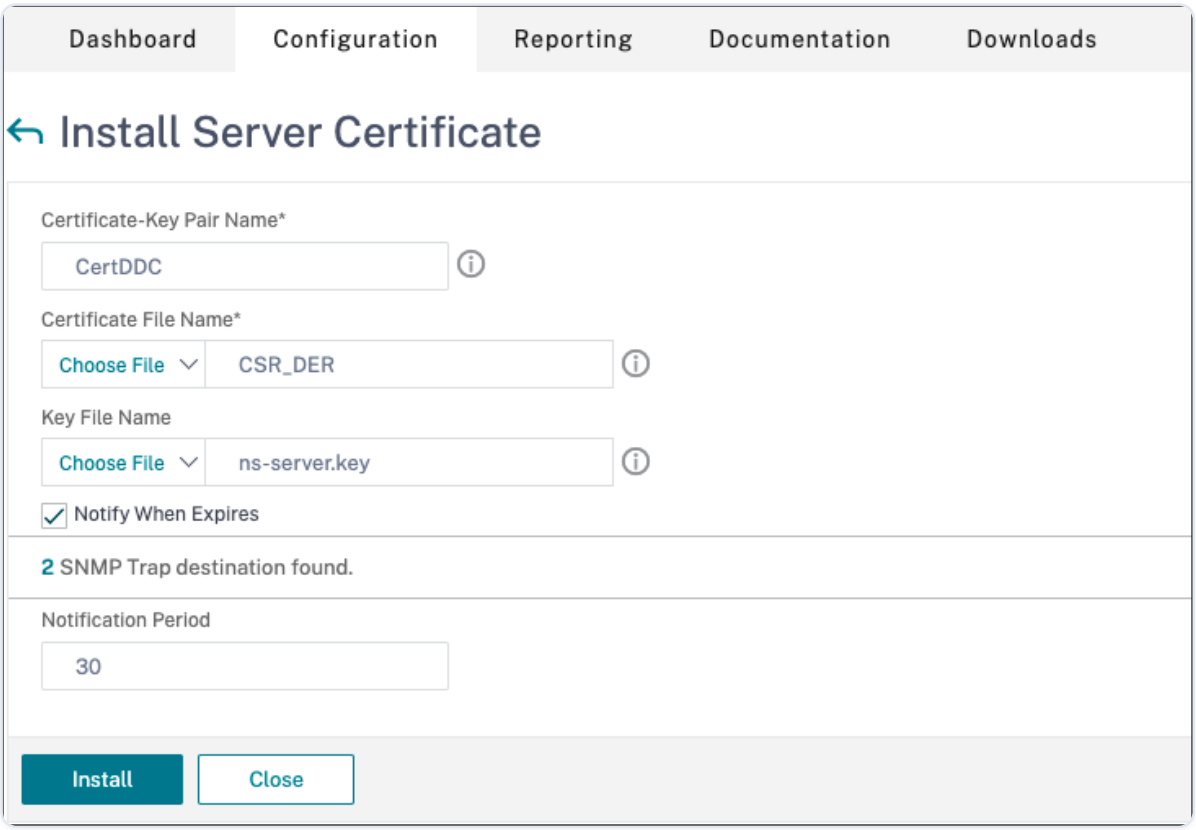
- セッション起動のためにADCアプライアンスにログインするためのCitrix Gateway仮想IPアドレスとロードバランサー仮想IPアドレス。詳細については、「仮想サーバーの作成」を参照してください。



- Citrix ADCアプライアンスで必要なモードと機能が有効になっています。
  - モードを有効にするには、Citrix ADC GUIで **System > Settings > Configure Mode** に移動します。
  - 機能を有効にするには、Citrix ADC GUIで **System > Settings > Configure Basic Features** に移動します。
- 証明書関連の構成が完了しています。
  - 証明書署名要求 (CSR) が作成されています。詳細については、「証明書の作成」を参照してください。



- サーバー証明書、CA証明書、およびルート証明書がインストールされています。詳細については、「インストール、リンク、および更新」を参照してください。



CA証明書をインストール(/en-us/citrix-virtual-apps-desktops/2511/media/adc-install-ca-certificate.png)

- Citrix Virtual Desktops用にCitrix Gatewayが作成されました。仮想サーバーがオンラインであることを確認するには、**Test STA Connectivity**ボタンをクリックして接続をテストします。詳細については、「Citrix Virtual Apps and Desktops向けCitrix ADCのセットアップ」(/ja-jp/citrix-adc/current-release/solutions/deploy-xa-xd.html)を参照してください。

仮想デスクトップ用ゲートウェイ(/en-us/citrix-virtual-apps-desktops/2511/media/xenapp-xendesktop-wizard.gif)

2. リライトアクションを追加します。詳細については、「リライトアクションの構成」(/ja-jp/citrix-adc/current-release/appexpert/rewrite.html#configuring-a-rewrite-action)を参照してください。

   a. **AppExpert > Rewrite > Actions**に移動します。
   b. **Add**をクリックして、新しいリライトアクションを追加します。アクションの名前は「set Type to INSERT_HTTP_HEADER」とすることができます。

   リライトアクションの追加(/en-us/citrix-virtual-apps-desktops/2511/media/adc-appexpert-rewrite-action.png)

   a. **タイプ**で、**INSERT_HTTP_HEADER**を選択します。

b. **ヘッダー名**に「X-Citrix-XmlServiceKey」と入力します。
c. **式**に、引用符付きで`<XmlServiceKey1 value>`を追加します。XmlServiceKey1 の値は、Desktop Delivery Controller™ の構成からコピーできます。

XMLサービスキーの値(/en-us/citrix-virtual-apps-desktops/2511/media/xml-service-key-values.png)

3. リライトポリシーを追加します。詳細については、「リライトポリシーの構成」(/ja-jp/citrix-adc/current-release/appexpert/rewrite.html#configure-rewrite-policy)を参照してください。

a. **AppExpert > Rewrite > Policies**に移動します。
b. 新しいポリシーを追加するには、**追加**をクリックします。

リライトポリシーの追加(/en-us/citrix-virtual-apps-desktops/2511/media/adc-appexpert-rewrite-policy.png)

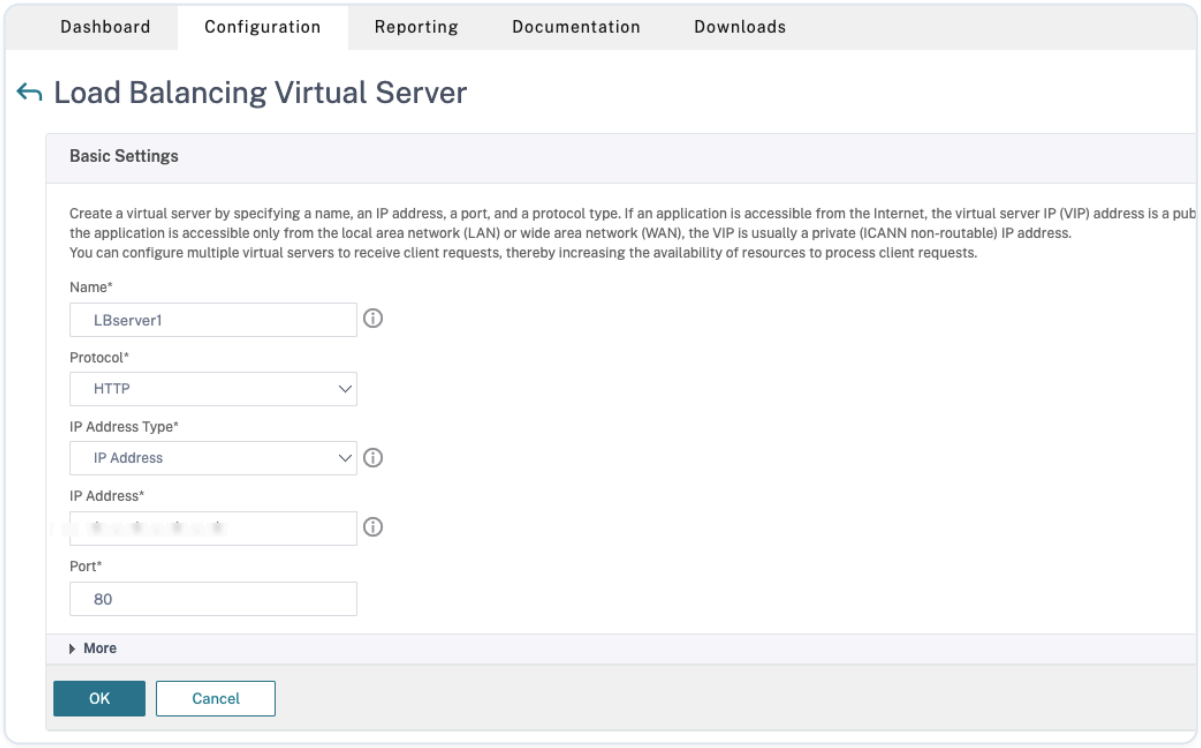
a. **アクション**で、前の手順で作成したアクションを選択します。
b. **式**に「HTTP.REQ.IS_VALID」を追加します。
c. **OK**をクリックします。

4. 負荷分散を設定します。STAサーバーごとに1つの負荷分散仮想サーバーを構成する必要があります。構成しない場合、セッションの起動に失敗します。

詳細については、基本的な負荷分散のセットアップを参照してください。

a. 負荷分散仮想サーバーを作成します。

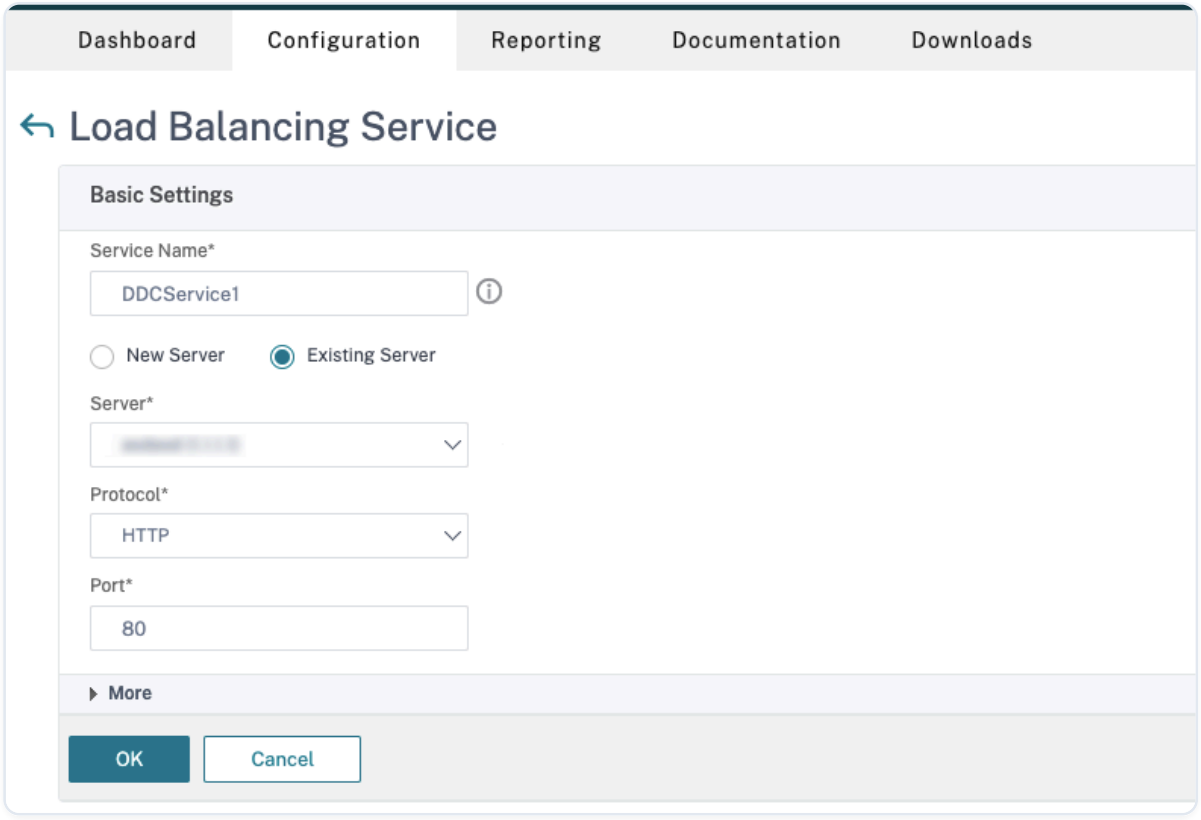
- **トラフィック管理 > ロードバランシング > サーバー**に移動します。
- **Virtual Servers**ページで、**Add**をクリックします。



- **Protocol**で、**HTTP**を選択します。
- 負荷分散仮想IPアドレスを追加し、**Port**で**80**を選択します。
- **OK**をクリックします。

b. 負荷分散サービスを作成します。

- **トラフィック管理 > ロードバランシング > サービス**に移動します。



- 「**Existing Server**」で、前の手順で作成した仮想サーバーを選択します。
- 「**Protocol**」で「**HTTP**」を選択し、「**Port**」で「**80**」を選択します。
- 「**OK**」をクリックし、次に「**Done**」をクリックします。

c. サービスを仮想サーバーにバインドします。

- 以前に作成した仮想サーバーを選択し、「**Edit**」をクリックします。
- 「**サービスとサービスグループ**」で、「**ロードバランシング仮想サーバーサービスバインディングなし**」をクリックします。

サービスを仮想サーバーにバインドします(/en-us/citrix-virtual-apps-desktops/2511/media/adc-bind-service-to-lbvserver.png)

- 「**Service Binding**」で、以前に作成したサービスを選択します。
- 「**Bind**」をクリックします。

d. 以前に作成した書き換えポリシーを仮想サーバーにバインドします。

- 以前に作成した仮想サーバーを選択し、「**Edit**」をクリックします。
- 「**Advanced Settings**」で「**Policies**」をクリックし、次に「**Policies**」セクションで「**+**」をクリックします。

書き換えポリシーをバインドします(/en-us/citrix-virtual-apps-desktops/2511/media/adc-bind-rewrite-policy.png)

- 「**Choose Policy**」で「**Rewrite**」を選択し、「**Choose Type**」で「**Request**」を選択します。
- 「**Continue**」をクリックします。
- 「**ポリシーの選択**」で、以前に作成した書き換えポリシーを選択します。
- 「**バインド**」をクリックします。
- 「**完了**」をクリックします。

e. 必要に応じて、仮想サーバーの永続性を設定します。

- 以前に作成した仮想サーバーを選択し、**編集**をクリックします。
- **詳細設定**で、**永続性**をクリックします。

永続性の設定(/en-us/citrix-virtual-apps-desktops/2511/media/adc-lb-vserver-persistence.png)

- 永続性の種類として「**その他**」を選択します。
- 仮想サーバーによって選択されたサービスのIPアドレス (宛先IPアドレス) に基づいて永続セッションを作成するには、「**DESTIP**」を選択します。
- 「**IPv4ネットマスク**」で、DDCと同じネットワークマスクを追加します。
- 「**OK**」をクリックします。

f. 他の仮想サーバーについても、これらの手順を繰り返します。

Citrix ADCアプライアンスがCitrix Virtual Desktops™で既に構成されている場合の構成の変更点

Citrix ADCアプライアンスをCitrix Virtual Desktopsで既に構成している場合、Secure XML機能を使用するには、以下の構成変更を行う必要があります。

- セッション起動前に、ゲートウェイの「**セキュリティチケット機関のURL**」を変更して、負荷分散仮想サーバーのFQDNを使用するようにします。
- `TrustRequestsSentToTheXmlServicePort`パラメーターがFalseに設定されていることを確認します。デフォルトでは、`TrustRequestsSentToTheXmlServicePort`パラメーターはFalseに設定されています。ただし、顧客がCitrix Virtual Desktops用にCitrix ADCをすでに構成している場合、`TrustRequestsSentToTheXmlServicePort`はTrueに設定されます。

1. Citrix ADC GUIで、**［Configuration］>［Integrate with Citrix Products］**の順に選択し、**［XenApp and XenDesktop®］**をクリックします。
2. ゲートウェイインスタンスを選択し、編集アイコンをクリックします。

   既存のゲートウェイ構成を編集(/en-us/citrix-virtual-apps-desktops/2511/media/edit-gateway-instance.png)
3. StoreFrontペインで、編集アイコンをクリックします。

   StoreFrontの詳細を編集(/en-us/citrix-virtual-apps-desktops/2511/media/edit-storefront-details.png)
4. **Secure Ticket Authority URL**を追加します。
   - Secure XML機能が有効になっている場合、STA URLはロードバランシングサービスのURLである必要があります。
   - Secure XML機能が無効になっている場合、STA URLはSTAのURL（DDCのアドレス）である必要があり、DDC上の`TrustRequestsSentToTheXmlServicePort`パラメーターはTrueに設定する必要があります。

STA URLを追加(/en-us/citrix-virtual-apps-desktops/2511/media/add-sta-urls.png)

セッションの回復性設定

セッションアクティビティを維持することは、最高のユーザーエクスペリエンスを提供するために不可欠です。信頼性の低いネットワーク、非常に変動するネットワーク遅延、ワイヤレスデバイスの範囲制限による接続の喪失は、ユーザーの不満につながる可能性があります。デバイス間を素早く移動し、ログオンするたびに同じアプリケーションにアクセスすることは、医療従事者などの多くのモバイルワーカーにとって優先事項です。

この記事で説明する機能は、セッションの信頼性を最適化し、不便さ、ダウンタイム、生産性の損失を軽減します。これらの機能を使用することで、モバイルユーザーはデバイス間を迅速かつ簡単に移動できます。

セッションの信頼性

セッションの信頼性により、ネットワーク接続が中断された場合でも、セッションはアクティブな状態を維持し、ユーザーの画面に表示されます。ユーザーは、ネットワーク接続が再開されるまで、使用中のアプリケーションを引き続き見ることができます。

この機能は、ワイヤレス接続を使用するモバイルユーザーにとって特に便利です。たとえば、ワイヤレス接続を使用しているユーザーが鉄道トンネルに入り、一時的に接続が失われたとします。通常、セッションは切断されてユーザーの画面から消え、ユーザーは切断されたセッションに再接続する必要があります。セッションの信頼性を使用すると、セッションはマシン上でアクティブなままになります。接続が失われたことを示すために、ユーザーのディスプレイはフリーズし、カーソルはトンネルの反対側で接続が再開されるまで回転する砂時計に変わります。ユーザーは中断中もディスプレイにアクセスし続け、ネットワーク接続が復元されたときにアプリケーションとの対話を再開できます。セッションの信頼性により、再認証のプロンプトなしでユーザーが再接続されます。

Citrix Workspace™アプリのユーザーは、Controllerの設定を上書きできません。

セッションの信頼性は、Transport Layer Security (TLS) とともに使用できます。TLSは、ユーザーデバイスとCitrix Gatewayの間で送信されるデータのみを暗号化します。

次のポリシー設定でセッションの信頼性を有効にして構成します。

- セッションの信頼性接続ポリシー設定は、セッションの信頼性を許可または禁止します。
- セッションの信頼性タイムアウトポリシー設定のデフォルトは180秒、つまり3分です。セッションの信頼性がセッションを開いたままにする時間を延長することはできますが、この機能はユーザーの利便性のために設計されています。そのため、ユーザーに再認証を促すことはあ

りません。セッションを開いたままにする時間を延長すると、ユーザーが注意散漫になり、ユーザーデバイスから離れてしまう可能性が高まります。これらの行動は、セッションを不正なユーザーがアクセスできる状態にする可能性があります。

- 受信セッションの信頼性接続は、セッションの信頼性ポート番号ポリシー設定でポート番号を変更しない限り、ポート2598を使用します。
- ユーザーが再認証なしで中断されたセッションに再接続するのを防ぐには、自動クライアント再接続機能を使用します。自動クライアント再接続認証ポリシー設定を構成して、中断されたセッションに再接続する際にユーザーに再認証を促すことができます。

セッションの信頼性と自動クライアント再接続の両方を使用する場合、これら2つの機能は順次動作します。セッションの信頼性は、セッションの信頼性タイムアウトポリシー設定で指定した時間の経過後にユーザーセッションを閉じ、または切断します。その後、自動クライアント再接続ポリシー設定が有効になり、切断されたセッションにユーザーを再接続しようとします。

クライアントの自動再接続

Auto Client Reconnect機能を使用すると、Citrix Workspaceアプリは意図しないICA®セッションの切断を検出し、影響を受けるセッションにユーザーを自動的に再接続できます。この機能がサーバーで有効になっている場合、ユーザーは手動で再接続することなく作業を続行できます。

アプリケーションセッションの場合、Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルするまで、セッションへの再接続を試みます。

デスクトップセッションの場合、Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルしない限り、指定された期間、セッションへの再接続を試行します。デフォルトでは、この期間は5分です。この期間を変更するには、ユーザーデバイスで以下のレジストリ設定を編集します（`seconds` は、セッションの再接続がそれ以上試行されなくなるまでの秒数です）。

`HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>`

次のポリシー設定を使用して、Auto Client Reconnectを有効にして構成します。

- **Auto Client Reconnect:** 接続が中断された後、Citrix Workspaceアプリによる自動再接続を有効または無効にします。
- **Auto Client Reconnect authentication:** 自動再接続後のユーザー認証の要件を有効または無効にします。
- **Auto Client Reconnect logging:** イベントログへの再接続イベントのログ記録を有効または無効にします。ログ記録はデフォルトで無効になっています。有効にすると、サーバーのシス

テムログは、成功および失敗した自動再接続イベントに関する情報をキャプチャします。各サーバーは、再接続イベントに関する情報を独自のシステムログに保存します。サイトは、すべてのサーバーの再接続イベントの統合ログを提供しません。

注：

再認証なしのAuto Client Reconnectは、パスワード認証のみでサポートされています。フェデレーション認証サービスまたはスマートカード認証を使用している場合、再認証なしのAuto Client Reconnectはサポートされません。そのような場合、ユーザーはログイン画面にリダイレクトされます。

Auto Client Reconnectは、暗号化されたユーザー資格情報に基づく認証メカニズムを組み込んでいます。ユーザーが最初にログオンすると、サーバーはユーザー資格情報を暗号化してメモリに保存します。サーバーはまた、暗号化キーを含むCookieを作成し、Citrix Workspaceアプリに送信します。Citrix Workspaceアプリは、再接続のためにキーをサーバーに送信します。サーバーは資格情報を復号化し、認証のためにWindowsログオンに送信します。Cookieの有効期限が切れると、ユーザーはセッションに再接続するために再認証する必要があります。

Auto Client Reconnect認証設定を有効にしている場合、Cookieは使用されません。代わりに、Citrix Workspaceアプリが自動的に再接続を試みるときに、資格情報を要求するダイアログボックスがユーザーに表示されます。

ユーザー資格情報とセッションを最大限に保護するために、クライアントとサイト間のすべての通信に暗号化を使用してください。

icaclient.admファイルを使用して、Windows版Citrix WorkspaceアプリでAuto Client Reconnectを無効にします。詳細については、お使いのWindows版Citrix Workspaceアプリのドキュメントを参照してください。

接続の設定もAuto Client Reconnectに影響します。

- デフォルトでは、前述のとおり、サイトレベルのポリシー設定により自動クライアント再接続が有効になっています。ユーザーの再認証は不要です。ただし、サーバーのICA TCP接続が、切断された通信リンクでセッションをリセットするように構成されている場合、自動再接続は行われません。自動クライアント再接続は、サーバーが切断された接続またはタイムアウトした接続がある場合にのみセッションを切断する場合に機能します。このコンテキストでは、

ICA TCP接続とは、TCP/IPネットワーク上のセッションに使用されるサーバーの仮想ポート（実際のネットワーク接続ではなく）を指します。

- デフォルトでは、サーバー上のICA TCP接続は、切断された接続またはタイムアウトした接続でセッションを切断するように設定されています。切断されたセッションはシステムメモリにそのまま保持され、Citrix Workspaceアプリによる再接続が可能です。
- 接続は、切断された接続またはタイムアウトした接続でセッションをリセットまたはログオフするように構成できます。セッションがリセットされると、再接続を試みると新しいセッションが開始されます。ユーザーを使用中のアプリケーションの同じ場所に戻すのではなく、アプリケーションが再起動されます。
- サーバーがセッションをリセットするように構成されている場合、自動クライアント再接続は新しいセッションを作成します。このプロセスでは、ユーザーがサーバーにログオンするために資格情報を入力する必要があります。
- Citrix Workspaceアプリまたはプラグインが誤った認証情報を送信した場合、自動再接続が失敗することがあります。これは、攻撃中に発生したり、サーバーが切断された接続を検出してから時間が経ちすぎたと判断した場合に発生する可能性があります。

ICA キープアライブ

ICAキープアライブ機能を有効にすると、切断された接続が切断されるのを防ぎます。有効にすると、サーバーがアクティビティを検出しない場合、この機能によりリモートデスクトップサービスがそのセッションを切断するのを防ぎます。アクティビティがない例としては、時計の変更がない、マウスの動きがない、画面の更新がないなどが挙げられます。サーバーは数秒ごとにキープアライブパケットを送信し、セッションがアクティブであるかどうかを検出します。セッションがアクティブでなくなった場合、サーバーはセッションを切断済みとしてマークします。

> **重要：**
>
> ICA Keep-Aliveは、セッションの信頼性を使用していない場合にのみ機能します。セッションの信頼性には、途切れた接続が切断されるのを防ぐ独自のメカニズムがあります。ICA Keep-Aliveは、セッションの信頼性を使用しない接続に対してのみ構成してください。

> ICA Keep-Alive設定は、Windowsグループポリシーで構成されているキープアライブ設定を上書きします。

以下のポリシー設定でICAキープアライブを有効にして構成します。

- **ICAキープアライブタイムアウト:** ICAキープアライブメッセージの送信に使用する間隔（1〜3600秒）を指定します。切断された接続が非常にまれで、ユーザーがセッションに再接続できることが問題にならない環境で、ネットワーク監視ソフトウェアに非アクティブな接続を閉じさせたい場合は、このオプションを構成しないでください。

  デフォルトの間隔は60秒です。ICAキープアライブパケットは60秒ごとにユーザーデバイスに送信されます。ユーザーデバイスが60秒以内に応答しない場合、ICAセッションのステータスは切断済みに変わります。

- **ICAキープアライブ:** ICAキープアライブメッセージの送信を許可または禁止します。

ワークスペースコントロール

ワークスペースコントロールを使用すると、デスクトップとアプリケーションがユーザーをあるデバイスから別のデバイスへと追跡できます。このローミング機能により、ユーザーはログオンするだけで、各デバイスでデスクトップやアプリケーションを再起動することなく、どこからでもすべてのデスクトップや開いているアプリケーションにアクセスできます。たとえば、ワークスペースコントロールは、病院でさまざまなワークステーション間を迅速に移動し、ログオンするたびに同じアプリケーションセットにアクセスする必要がある医療従事者を支援できます。ワークスペースコントロールオプションを許可するように構成すると、これらの従業員は1つのクライアントデバイスで複数のアプリケーションから切断し、別のクライアントデバイスで同じアプリケーションを開くために再接続できます。

ワークスペースコントロールは、次のアクティビティに影響します。

- **ログオン:** デフォルトでは、ワークスペースコントロールにより、ユーザーはログオン時に実行中のすべてのデスクトップとアプリケーションに自動的に再接続でき、手動で再開する必要がなくなります。ワークスペースコントロールを介して、ユーザーは切断されたデスクトップまたはアプリケーション、および別のクライアントデバイスでアクティブになっているものを開くことができます。デスクトップまたはアプリケーションから切断すると、それはサーバー上で実行されたままになります。一部のデスクトップまたはアプリケーションを1つのクライアントデバイスで実行したまま、別のクライアントデバイスでデスクトップまたはアプリケーションのサブセットに再接続する必要があるローミングユーザーがいる場合、ログオン再接続動作を構成して、ユーザーが以前に切断したデスクトップまたはアプリケーションのみを開くようにすることができます。
- **再接続:** サーバーにログオンした後、ユーザーはいつでも「再接続」をクリックして、すべてのデスクトップまたはアプリケーションに再接続できます。デフォルトでは、「再接続」は切断されたデスクトップまたはアプリケーション、および現在別のクライアントデバイスで実行されているものを開きます。「再接続」を構成して、ユーザーが以前に切断したデスクトップまたはアプリケーションのみを開くようにすることができます。

- **ログオフ:** StoreFront™ を介してデスクトップまたはアプリケーションを開くユーザーの場合、**ログオフ**コマンドを構成して、StoreFrontとすべてのアクティブなセッションからユーザーをログオフするか、StoreFrontからのみログオフすることができます。
- **切断:** ユーザーは、実行中のすべてのデスクトップとアプリケーションから一度に切断でき、個別に切断する必要はありません。

ワークスペースコントロールは、Citrix StoreFront接続を介してデスクトップおよびアプリケーションにアクセスするCitrix Workspaceアプリユーザーのみが利用できます。デフォルトでは、ワークスペースコントロールは仮想デスクトップセッションでは無効になっていますが、ホスト型アプリケーションでは有効になっています。公開されたデスクトップと、それらのデスクトップ内で実行されている公開されたアプリケーションとの間で、セッション共有はデフォルトでは行われません。

ユーザーが新しいクライアントデバイスに移動すると、ユーザーポリシー、クライアントドライブマッピング、およびプリンター構成が適切に変更されます。ポリシーとマッピングは、ユーザーがセッションにログオンしているクライアントデバイスに従って適用されます。たとえば、医療従事者が救急治療室のデバイスからログオフし、X線検査室のワークステーションにログオンするとします。X線検査室でのセッションに適したポリシー、プリンターマッピング、およびクライアントドライブマッピングは、セッション開始時に有効になります。

ユーザーが場所を変更したときに表示されるプリンターをカスタマイズできます。また、ユーザーがローカルプリンターに印刷できるかどうか、ユーザーがリモートで接続したときに消費される帯域幅の量、およびその他の印刷エクスペリエンスの側面を制御することもできます。

ユーザー向けにワークスペースコントロールを有効にして構成する方法については、StoreFrontのドキュメントを参照してください。

セッションローミング

> **注:**
>
> 次の情報は、PowerShellを使用してセッションローミングを構成する方法を説明しています。代わりにWeb Studioを使用することもできます。詳細については、「デリバリーグループの管理」を参照してください。

> デフォルトでは、セッションはユーザーとともにクライアントデバイス間をローミングします。ユーザーがセッションを起動し、別のデバイスに移動すると、同じセッションが使用され、両方のデバイスでアプリケーションが利用可能になります。アプリケーションは、デバ

> イスや現在のセッションの有無にかかわらず追跡されます。多くの場合、アプリケーションに割り当てられたプリンターやその他のリソースも追跡されます。

このデフォルトの動作には多くの利点がありますが、すべての場合に理想的であるとは限りません。PowerShell SDKを使用してセッションローミングを防止できます。

例1：医療従事者が2台のデバイスを使用しており、デスクトップPCで保険フォームを記入し、タブレットで患者情報を閲覧しています。

- セッションローミングが有効になっている場合、両方のアプリケーションが両方のデバイスに表示されます（1つのデバイスで起動されたアプリケーションは、使用中のすべてのデバイスで表示されます）。これはセキュリティ要件を満たさない可能性があります。
- セッションローミングが無効になっている場合、患者記録はデスクトップPCに表示されず、保険フォームはタブレットに表示されません。

例2：生産管理者がオフィスにあるPCでアプリケーションを起動します。デバイス名と場所によって、そのセッションで利用できるプリンターやその他のリソースが決まります。その日の後半、彼はプリンターの使用が必要な会議のため、隣の建物のオフィスに行きます。

- セッションローミングが有効になっている場合、生産管理者は会議室近くのプリンターにアクセスできない可能性があります。なぜなら、彼がオフィスで以前に起動したアプリケーションによって、その場所に近いプリンターやその他のリソースが割り当てられているためです。
- セッションローミングが無効になっている場合、彼が別のマシンに（同じ資格情報を使用して）ログオンすると、新しいセッションが開始され、近くのプリンターやリソースが利用可能になります。

セッションローミングの構成

セッションローミングを構成するには、「SessionReconnection」プロパティを指定して、以下のエンタイトルメントポリシー規則のコマンドレットを使用します。オプションで、「LeasingBehavior」プロパティも指定できます。

デスクトップセッションの場合：

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

アプリケーションセッションの場合：

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

ここで、`value` は次のいずれかになります。

- **Always:** クライアントデバイスやセッションが接続されているか切断されているかに関係なく、セッションは常にローミングします。これがデフォルト値です。
- **DisconnectedOnly:** 既に切断されているセッションにのみ再接続します。それ以外の場合は、新しいセッションを起動します。（セッションは、最初に切断するか、Workspace Controlを使用して明示的にローミングすることで、クライアントデバイス間をローミングできます。）別のクライアントデバイスからのアクティブな接続済みセッションは使用されません。代わりに、新しいセッションが起動されます。
- **SameEndpointOnly:** ユーザーは使用するクライアントデバイスごとに一意のセッションを取得します。これにより、ローミングが完全に無効になります。ユーザーは、以前セッションで使用したのと同じデバイスにのみ再接続できます。

「LeasingBehavior」プロパティについては、以下で説明します。

その他の設定による影響：

セッションローミングの無効化は、デリバリーグループのアプリケーションプロパティにあるアプリケーション制限 **ユーザーごとにアプリケーションのインスタンスを1つのみ許可** の影響を受けます。

- セッションローミングを無効にする場合は、「ユーザーごとにアプリケーションのインスタンスを1つのみ許可」アプリケーション制限も無効にしてください。
- 「ユーザーごとにアプリケーションのインスタンスを1つのみ許可」アプリケーション制限を有効にする場合は、新しいデバイスでの新しいセッションを許可する2つの値のいずれも構成しないでください。

ログオン間隔

デスクトップVDAを含む仮想マシンがログオンプロセス完了前に閉じられた場合、そのプロセスにより多くの時間を割り当てることができます。バージョン7.6以降のデフォルトは180秒です（バージョン7.0～7.5のデフォルトは90秒です）。

マシン（またはマシンカタログで使用されるマスターイメージ）で、次のレジストリキーを設定します。

キー: `HKLM\SOFTWARE\Citrix\PortICA`

- 値: `AutoLogonTimeout`
- 種類: `DWORD`

- 0〜3600の範囲で、10進数の時間を秒単位で指定します。

マスターイメージを変更する場合は、カタログを更新してください。

この設定は、デスクトップVDAを搭載したVMにのみ適用されます。サーバーVDAを搭載したマシンのログオンタイムアウトはMicrosoftが制御します。

設定

> **注:**

> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> Web Studioを使用して、以下の設定を管理できます。

- 認証の管理
- Studioログインページのデフォルトドメイン名を設定する
- Citrixカスタマーエクスペリエンス向上プログラム
- Delivery Controllerを削除する
- データベースの場所を変更する
- Studioで個人設定を管理する
- サイト管理を一元化する
- Remote PC Accessの複数ユーザーの自動割り当てを有効にする
- DNS解決の有効化
- XML信頼を有効にする
- セキュリティキーを管理する
- Studioコンソールの非アクティブタイムアウトの設定
- サイト管理の一元化
- Studioログインページにカスタム通知を設定する(#set-a-custom-notice-on-the-studio-login-page)

- Studioログインページにアクティブなデフォルト DDC の FQDN を表示する(#display-the-fqdn-of-active-ddc-on-the-studio-login-page)
- ログサーバーの構成

認証の管理

デフォルトでは、ユーザーはドメインのユーザー名とパスワードを使用してWeb Studioにログオンします。スマートカード認証や統合Windows認証など、ユーザーに対して別の認証方法を選択することもできます。

Studio を使用して管理

ユーザーの認証方法を選択するには、次の手順に従います。

1. Web Studio にサインインし、左ペインで を選択します。
2. タイルを見つけて をクリックし、オプションを選択します。

   - **ドメイン資格情報**
   - **ドメイン資格情報または統合 Windows 認証**

     統合 Windows 認証が有効になっている場合、ユーザーは Windows 資格情報 (Kerberos/NTLM) またはクライアント証明書を使用して Web Studio にアクセスできます。

     Web Studio と Delivery Controller™ が異なるマシンにインストールされている場合、統合 Windows 認証を機能させるには、クロスオリジンアクセスを許可し、Web Studio サーバーの URL を許可リストに追加します。

     > **重要**
     >
     > Web Studio が Delivery Controller のプロキシとして構成されている場合、統合 Windows 認証は機能しません。

   - **スマートカード認証**
   - **ドメイン資格情報またはスマートカード認証**

     スマートカード認証を有効にするには、追加の構成が必要です。詳細については、「Web Studio のスマートカード認証をセットアップする」を参照してください。

PowerShell スクリプトを使用した管理

認証方法は Delivery Controller データベースで構成されます。認証方法を設定するには、次の PowerShell スクリプトを使用できます。

1. Delivery Controller で次のコマンドを実行して、現在のサイト ID を取得します。

   `Get-ConfigSite | Select SiteGuid`

2. 以下のスクリプトを実行して認証方法を設定します。

```
# Generate a new bearer token

$bearerData = New-TrustBearerToken

# Define the Delivery Controller DNS name and Site ID

$ddc = "ddc.dc.com" # replace this with the Delivery Controller's DNS
name

$siteid = "c68a8f89-42af-4bea-a6e9-c8c936353f49" # replace this with
the site ID you get from step #1

# Define the URL and headers

$url = "https://$ddc/citrix/orchestration/api/CitrixOnPremises/Sites/
$siteid/Settings"

$headers = @{

"Content-Type" = "application/json"

"Authorization" = "Bearer $($bearerData.Token)"

}

# Define the JSON body

$body = @{

SupportedAuthenticators = "BasicAndSmartCard" # replace this with a
required authentication method: "Basic" for "Domain credentials";
"BasicAndIntegratedWindowsAuthentication" for "Domain credentials or
integrated Windows authentication"; "BasicAndSmartCard" for "Domain
```

```
credentials or smart card authentication"; "SmartCard" for "Smart card
authentication"

} | ConvertTo-Json -Depth 10

# Send the PATCH request

Invoke-RestMethod -Uri $url -Method Patch -Headers $headers -Body $body
```

統合 Windows 認証のためにブラウザを構成する

ドメイン資格情報または統合 Windows 認証を使用して *統合 Windows 認証* を有効にすると、ユーザーが次回サインインするときに、自動的にサインインされます。ユーザーとして自動的にサインインできない場合は、次の手順に従って、統合 Windows 認証を許可するように Web ブラウザを構成してください。

Google Chrome の場合:

1. コントロールパネルから、「**インターネットオプション**」を選択します。
2. 「**詳細設定**」タブを選択します。
3. **統合Windows認証を有効にする**を選択します。
4. **セキュリティ**タブを選択します。
5. **ローカルイントラネット > サイト > 詳細設定**を選択します。
6. **このWebサイトをゾーンに追加する**ボックスで：
   - Web StudioとDelivery Controllerが同じサーバー上にある場合は、Web Studioを実行しているホストのURLを入力します。
   - そうでない場合は、ワイルドカードドメインを入力します。例：Delivery Controllerが `ddc.domain.com` にある場合、`*.domain.com` と入力します。
7. **追加 > 閉じる**をクリックします。

Mozilla Firefoxの場合：

1. ブラウザーから、URLボックスに`about:config`と入力します。
2. 「**検索**」ボックスに「`network negotiate`」と入力します。
3. **network.negotiate-auth.trusted-uris** を右クリックし、「**変更**」を選択します。
4. 「**文字列値を入力**」ボックスで、次のようにします。

- Web Studio と Delivery Controller が同じサーバー上にある場合は、Web Studio をホストしているサーバー名を参照する URL および/またはエイリアスのコンマ区切りリストを追加します。
- そうでない場合は、次のように URL を追加します。例: Delivery Controller が `ddc.domain.com` にある場合、「`*.domain.com`」と入力します。

ブラウザーを設定したら、サインインページで「**Windows 統合サインイン**」をクリックして再試行できます。

Web Studio と Delivery Controller が異なるマシンにインストールされている場合、統合 Windows 認証を機能させるには、**Allow cross-origin access** を有効にする必要があります。

Allow cross-origin access を有効にするには、次の手順に従います。

1. **Allow cross-origin access** チェックボックスをオンにします。
2. Web Studio サーバーの URL を許可リストに追加します。
3. **Enter URL** フィールドに URL を入力します。必要に応じて、**Add** をクリックしてさらに追加します。

> **注**
>
> - URL は正しい形式 `<scheme>://<hostname>` に従う必要があります。パスや末尾のスラッシュを含まないようにしてください。
> - IP アドレスと FQDN がサポートされています。URL を追加するときは、Web Studio へのアクセス方法と一致していることを確認してください。たとえば、IP アドレスを使用して Web Studio にアクセスする場合は、IP アドレスベースの URL をリストに追加します。
> - デフォルト以外のポートを使用する場合は、ポート番号を含めるようにしてください。

4. 必要に応じて、**Add** をクリックしてさらに追加します。
5. 完了したら、**Done** をクリックして保存し、終了します。

Studioログインページのデフォルトドメイン名を設定する

Studio ログインページの **Domain** フィールドにドメイン名を自動入力するには、次の手順に従います。

1. Web Studio にサインインし、左ペインで設定を選択します。
2. **Configure domain name** タイルで、必要に応じてドメイン名を入力します。
3. 「**適用**」をクリックします。

   管理者がStudioのログインページにアクセスすると、設定したドメイン名が *ドメイン*フィールドに自動的に入力されます。

Studio で個人設定を管理する

設定ノードの下にある**マイ設定**タブを使用して、Studioでの個人の表示設定と操作設定を管理します。これらの設定はご自身のアカウントにのみ適用され、他の管理者には影響しません。利用可能なオプションは次のとおりです。

- **日付と時刻**: デフォルトのタイムゾーン、日付形式、時刻形式を設定します。これらの設定は、スケジュールされた再起動や自動スケーリングなど、時刻に関連する表示のためにStudio全体で使用されます。
- **フォルダービュー**: **マシンカタログ**、**デリバリーグループ**、および**アプリケーション**ノードでフォルダービューを表示するか非表示にするかを選択します。
- **検索でのタブ順序**: **検索**ノード内のタブ順序をカスタマイズします。

Studioで優先表示を設定するには、次の手順に従います。

1. Studio で、**設定 > 個人設定**に移動します。
2. 「**編集**」をクリックします。
3. 「**日付と時刻**」タイルで、次の形式設定を構成します。

   - **日付形式**: 日付の表示方法を選択します（例: yyyy/MM/dd）。Studio用に選択した言語に関連付けられた日付形式を使用するには、「**コンソール言語に合わせる**」を選択します。
   - **時刻形式**: 12時間形式（例: 午後09:00）または24時間形式（例: 21:00）を選択します。Studio用に選択した言語に関連付けられた時刻形式を使用するには、「**コンソール言語に合わせる**」を選択します。
   - **タイムゾーン**: 優先するタイムゾーンを選択します。コンピューターのタイムゾーンを使用するには、「**コンソール言語に合わせる**」を選択します。

   > **注:**

- コンピューターの地域設定を日付、時刻、またはタイムゾーンに使用するには、**コンソール言語に合わせる**を選択します。
- Studioでは、表示されている時刻にカーソルを合わせると、ローカルタイムゾーンでの同等の時刻を表示できます。

4. **フォルダービュー**タイルで、**マシンカタログ**、**デリバリーグループ**、および**アプリケーション**ノードでフォルダービューを表示するか非表示にするかを選択します。
5. **検索でのタブ順序**タイルで、**検索**ノード内のタブをドラッグして並べ替えます。
6. 変更をすぐに保存して適用するには、**適用**をクリックします。

DNS解決を有効にする

ICA®ファイルでIPアドレスの代わりにDNS名を表示するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**設定**を選択します。
2. **DNS解決を有効にする**設定をオンにします。

Studioコンソールの非アクティビティタイムアウトを設定する

管理者がStudioコンソールから自動的にサインアウトされるまでの非アクティブ期間を設定できます。

1. Web Studioにサインインし、左ペインで**設定**を選択します。
2. 10分から24時間の範囲で期間を入力します。
3. この設定を適用するには、ページを更新するか、サインアウトしてから再度サインインします。

サイト管理の一元化

この機能を使用すると、1つのWeb Studioコンソールで複数のCitrix Virtual Apps and Desktopsサイトを管理できます。詳細については、「複数サイト管理の有効化」を参照してください。

Studioログインページにカスタム通知を設定する

サインインページの通知を設定するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**［設定］**を選択します。
2. **［ログインページの通知］タイルを見つけて、［ログインページに通知を表示］**チェックボックスをオンにします。

3. **［編集］をクリックして［ログインページの通知］**ページを開き、必要に応じてログインページの通知を入力します。
4. **［保存］**をクリックします。

StudioログインページにアクティブなDDCのFQDNを表示する

現在のセッションで使用されているDDCのFQDNをStudioサインインページに表示するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**［設定］**を選択します。
2. **［接続されているDelivery Controllerを表示］**をオンにします。

ログサーバーを構成する

AOT（Always-on Tracing）ログサーバーを構成し、ログ記録の範囲を定義します。**Director**はログサーバーに接続して、監視およびトラブルシューティング用のログを取得します。

ログサーバーを構成し、ログ記録の範囲を定義するには、次の手順に従います。

1. **Web Studio**にサインインし、左ペインで**［設定］**を選択します。
2. ログサーバーが構成されていない場合は、「**Log server**」タイルで「**Add**」をクリックします。
3. 表示される「**Log server**」ページで、「**Enable log forwarding to log server**」を選択します。
4. どのコンポーネントがログをログサーバーに転送するかを選択します:
    - 「**Delivery Controllerを含める**」: すべてのDelivery Controllerからのログをログサーバーに転送します。
    - 「**デリバリーグループを選択**」: 特定のデリバリーグループ内のVDAからのログをログサーバーに転送します。デフォルトでは、「**すべてのデリバリーグループ**」が選択されており、すべてのデリバリーグループ内のVDAからのログが転送されます。特定のデリバリーグループ内のVDAからのみログを転送するには、「**特定のデリバリーグループを選択**」を選択し、含めるグループを選択します。
5. ログサーバーによって生成された**Authkey**を入力します。**Director**はこのキーを使用してログサーバーにアクセスします。
6. 「**Save**」をクリックして構成を適用します。

ログサーバーを更新するか、ログ記録の範囲を変更するには、「**設定 > ログサーバー**」タイルで「**編集**」をクリックします。

タグ

> **注:**
>
> バージョン2511以降、Citrix Web Studio (Webベース) は、Citrix Virtual Apps and Desktops™ の唯一の管理コンソールです。Citrix Studio (MMCベース) はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

タグは、マシン、アプリケーション、デスクトップ、デリバリーグループ、アプリケーショングループ、ポリシーなどの項目を識別する文字列です。タグを作成して項目に追加すると、特定の操作を、指定されたタグを持つ項目にのみ適用するように調整できます。

- Web Studioでの検索表示を調整します。

  たとえば、テスター向けに最適化されたアプリケーションのみを表示するには、「test」という名前のタグを作成し、それらのアプリケーションに追加（適用）します。これで、Web Studioの検索を「test」タグでフィルタリングできます。
- アプリケーショングループからアプリケーションを公開したり、デリバリーグループから特定のデスクトップを公開したりする際に、選択したデリバリーグループ内のマシンの一部のみを考慮します。これは*タグ制限*と呼ばれます。

  タグ制限を使用すると、既存のマシンを複数の公開タスクに使用できるため、より多くのマシンを展開および管理するコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）するものと考えることができます。その機能は、XenApp 7.xより前のリリースにおけるワーカーグループと似ていますが、同一ではありません。

  タグ制限付きのアプリケーショングループまたはデスクトップを使用すると、デリバリーグループ内のマシンの一部を分離してトラブルシューティングする際に役立ちます。
- デリバリーグループ内のマシンの一部に対して定期的な再起動をスケジュールします。

  マシンにタグ制限を使用すると、新しいPowerShellコマンドレットを使用して、デリバリーグループ内のマシンの一部に対して複数の再起動スケジュールを構成できます。例と詳細については、「デリバリーグループの管理」を参照してください。

- 指定されたタグを持つ（または持たない）デリバリーグループ、デリバリーグループの種類、またはOU内のマシンの一部にCitrixポリシーの適用（割り当て）を調整します。

  たとえば、より強力なワークステーションにのみCitrixポリシーを適用したい場合は、それらのマシンに「high power」という名前のタグを追加します。次に、ポリシー作成ウィザードの**ポリシーの割り当て**ページで、そのタグと**有効にする**チェックボックスを選択します。デリバリーグループにタグを追加し、そのグループにCitrixポリシーを適用することもできます。詳細については、「ポリシーの作成」を参照してください。

タグを適用できる対象:

- マシン
- アプリケーション
- マシンカタログ（PowerShellのみ。詳細については、「マシンカタログのタグ」を参照してください）
- デリバリーグループ
- アプリケーショングループ

Web Studioで以下を作成または編集する際に、タグ制限を構成できます。

- 共有デリバリーグループ内のデスクトップ
- アプリケーショングループ

> **重要:**
>
> タグは、マシンに明示的に適用することも、マシンカタログまたはデリバリーグループレベルで明示的に適用することもできます。タグがマシンカタログまたはデリバリーグループレベルで適用されると、そのカタログまたはデリバリーグループ内のすべてのマシンが暗黙的にタグを継承します。これらの継承されたタグは、マシンレベルで削除することはできません。タグの効果を削除するには、マシンカタログまたはデリバリーグループレベルからタグを削除する必要があります。

デスクトップまたはアプリケーショングループのタグ制限

タグ制限にはいくつかの手順があります。

- タグを作成し、マシンに追加（適用）します。

- タグ制限付きのグループを作成または編集します（つまり、「タグxを持つマシンへの起動を制限する」）。

タグ制限は、ブローカーのマシン選択プロセスを拡張します。ブローカーは、アクセスポリシー、構成されたユーザーリスト、ゾーン設定、起動準備、およびタグ制限（存在する場合）に従って、関連付けられたデリバリーグループからマシンを選択します。アプリケーションの場合、ブローカーは優先順位に従って他のデリバリーグループにフォールバックし、検討対象の各デリバリーグループに同じマシン選択ルールを適用します。

例1：シンプルなレイアウト

この例では、タグ制限を使用して、特定のデスクトップおよびアプリケーションの起動にどのマシンが考慮されるかを制限するシンプルなレイアウトを紹介します。このサイトには、1つの共有デリバリーグループ、1つの公開デスクトップ、および2つのアプリケーションで構成された1つのアプリケーショングループがあります。

シンプルなレイアウトでタグ制限を使用する例。(/en-us/citrix-virtual-apps-desktops/2511/media/tags-example.png)

- 3台のマシン（VDA 101～103）のそれぞれにタグが追加されています。
- 共有デリバリーグループ内のデスクトップは、「Red」という名前のタグ制限付きで作成されました。デスクトップは、そのデリバリーグループ内で「Red」タグを持つマシン（VDA 101および102）でのみ起動できます。
- アプリケーショングループは「Orange」タグ制限付きで作成されたため、そのアプリケーション（CalculatorとNotepad）はそれぞれ、「Orange」タグを持つデリバリーグループ内のマシン（VDA 102および103）でのみ起動できます。

マシンVDA 102は両方のタグ（RedとOrange）を持っているため、アプリケーションとデスクトップの起動に考慮されます。

例2：より複雑なレイアウト

この例には、タグ制限付きで作成された複数のアプリケーショングループが含まれています。これにより、デリバリーグループのみを使用した場合に必要となるよりも少ないマシンで、より多くのアプリケーションを配信できるようになります。

例2の構成方法は、この例でタグを作成および適用し、タグ制限を構成するために使用される手順を示しています。

複雑なレイアウトでタグ制限を使用する例。(/en-us/citrix-virtual-apps-desktops/2511/media/tags-example2.png)

この例では、10台のマシン（VDA 101〜110）、1つのデリバリーグループ（D01）、および3つのアプリケーショングループ（A100、A200、A300）を使用します。各マシンにタグを適用し、各アプリケーショングループの作成時にタグ制限を指定することで、次のことが可能になります。

- グループ内の経理ユーザーは、5台のマシン（VDA 101〜105）で必要なアプリにアクセスできます
- グループ内のCAD設計者は、5台のマシン（VDA 106-110）で必要なアプリにアクセスできます
- グループ内でOfficeアプリケーションを必要とするユーザーは、10台のマシン（VDA 101〜110）でOfficeアプリにアクセスできます

10台のマシンのみが使用され、デリバリーグループは1つだけです。デリバリーグループのみを使用する場合（アプリケーショングループなし）、1台のマシンは1つのデリバリーグループにしか属せないため、2倍のマシンが必要になります。

タグとタグ制限の管理

タグは、Web Studioの**タグの管理**アクションを通じて、選択したアイテムに対して作成、追加（適用）、編集、削除されます。

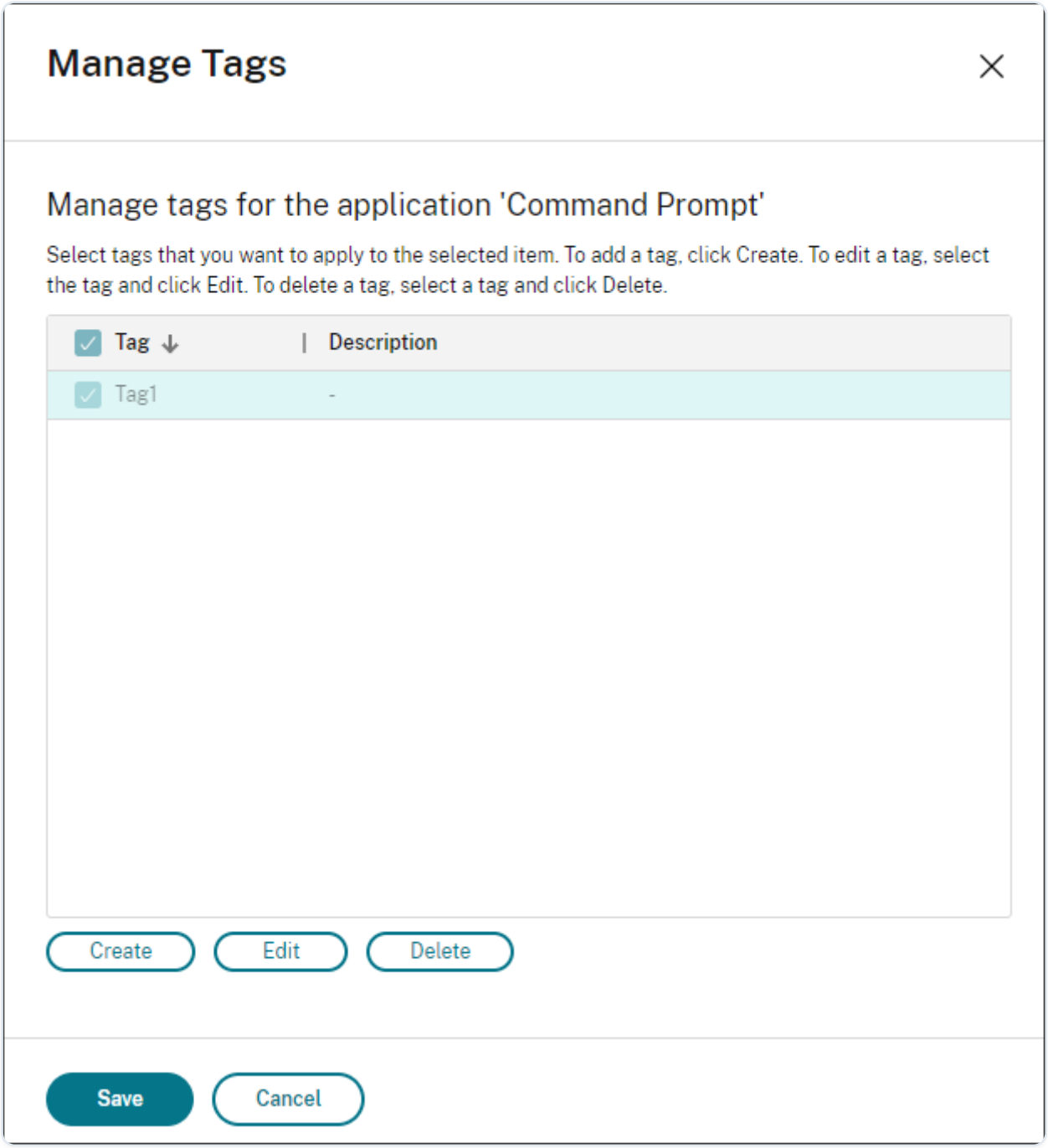
（例外：ポリシー割り当てに使用されるタグは、Web Studioの**タグの管理**アクションを通じて作成、編集、削除されます。ただし、タグはポリシーの作成時に適用（割り当て）されます。詳細については、「ポリシーの作成」を参照してください。）

タグ制限は、デリバリーグループでデスクトップを作成または編集するとき、およびアプリケーショングループを作成および編集するときに構成されます。

Web Studioで［タグの管理］ダイアログを使用する

Web Studioで、タグを適用するアイテム（1つ以上のマシン、アプリケーション、デスクトップ、デリバリーグループ、またはアプリケーショングループ）を選択し、アクションバーで**タグの管理**を選択します。ダイアログボックスには、選択したアイテムだけでなく、サイトで作成されたすべてのタグが一覧表示されます。

- チェックマークが付いたチェックボックスは、そのタグが選択したアイテムに既に追加されていることを示します。（以下のスクリーンショットでは、選択したマシンに「Tag1」という名前のタグが適用されています。）
- 複数のアイテムを選択した場合、ハイフンが付いたチェックボックスは、選択したアイテムの一部にのみそのタグが追加されていることを示します。



タグの管理ダイアログボックスから、次のアクションを実行できます。「タグを使用する際の注意点」を必ず確認してください。

- **タグを作成するには:**

  作成をクリックします。名前と説明を入力します。タグ名は一意である必要があり、大文字と小文字は区別されません。次に、**OK**をクリックします。（タグを作成しても、選択したアイテムに自動的に適用されるわけではありません。チェックボックスを使用してタグを適用します。）

- **1つ以上のタグを追加（適用）するには:**

タグ名の横にあるチェックボックスを有効にします。複数のアイテムを選択していて、タグの横にあるチェックボックスにハイフンが含まれている場合（選択したアイテムの一部にのみタグが既に適用されていることを示す）、それをチェックマークに変更すると、選択したすべてのマシンに影響します。

1つ以上のマシンにタグを追加しようとして、そのタグがアプリケーショングループで制限として使用されている場合、その操作によってそれらのマシンが起動可能になる可能性があるという警告が表示されます。それが意図したとおりであれば、続行してください。

- **1つ以上のタグを削除するには:**

  タグ名の横にあるチェックボックスをオフにします。複数の項目を選択していて、タグの横にあるチェックボックスにハイフンが含まれている場合（選択された項目の一部にのみタグが適用されていることを示す）、チェックボックスをオフにすると、選択されたすべてのマシンからタグが削除されます。

  制限としてタグを使用しているマシンからタグを削除しようとすると、その操作によって起動対象となるマシンに影響が出る可能性があるという警告が表示されます。それが意図した動作であれば、続行してください。

- **タグを編集するには:**

  タグを選択し、**編集**をクリックします。新しい名前、説明、またはその両方を入力します。一度に編集できるタグは1つだけです。

- **1つ以上のタグを削除するには:**

  タグを選択し、**削除**をクリックします。「タグの削除」ダイアログボックスには、現在選択されているタグを使用している項目の数が表示されます（例：「2台のマシン」）。項目をクリックすると、詳細情報が表示されます。たとえば、「2台のマシン」項目をクリックすると、そのタグが適用されている2台のマシンの名前が表示されます。タグを削除するかどうかを確認します。

  制限として使用されているタグをWeb Studioで削除することはできません。まず、アプリケーショングループを編集し、タグ制限を削除するか、別のタグを選択してください。

タグの管理ダイアログボックスでの作業が完了したら、**保存**をクリックします。

マシンにタグが適用されているかどうかを確認するには、左ペインで**デリバリーグループ**を選択します。中央ペインでデリバリーグループを選択し、アクションバーで**マシンの表示**を選択します。中央ペインでマシンを選択し、**詳細**ペインで**タグ**タブを選択します。

タグ制限の管理

タグ制限の構成は多段階のプロセスです。まずタグを作成し、それをマシンに追加/適用します。次に、アプリケーショングループまたはデスクトップに制限を追加します。

- **タグの作成と適用：**

  タグを作成し、前述の**タグの管理**アクションを使用して、タグ制限の影響を受けるマシンにタグを追加（適用）します。

- **アプリケーショングループにタグ制限を追加するには:**

  アプリケーショングループを作成または編集します。**デリバリーグループ**ページで、**タグを持つマシンへの起動を制限する**を選択し、リストからタグを選択します。

- **アプリケーショングループのタグ制限を変更または削除するには:**

  グループを編集します。**デリバリーグループ**ページで、リストから別のタグを選択するか、**タグを持つマシンへの起動を制限する**のチェックを外してタグ制限を完全に削除します。

- **デスクトップにタグ制限を追加するには:**

  デリバリーグループを作成または編集します。**デスクトップ**ページで、**追加**または**編集**をクリックします。「デスクトップの追加」ダイアログボックスで、**タグを持つマシンへの起動を制限する**を選択し、メニューからタグを選択します。

- **デリバリーグループのタグ制限を変更または削除するには:**

  グループを編集します。デスクトップページで、**編集**をクリックします。ダイアログボックスで、リストから別のタグを選択するか、**タグを持つマシンへの起動を制限する**のチェックを外してタグ制限を完全に削除します。

タグを使用する際の注意点

アイテムに適用されたタグはさまざまな目的に使用できるため、タグの追加、削除、および削除が意図しない影響を与える可能性があることに留意してください。Web Studioの検索フィールドでマシンの表示を並べ替えるためにタグを使用できます。アプリケーショングループまたはデスクトップを構成する際に、同じタグを制限として使用できます。タグは、そのタグを持つ指定されたデリバリーグループ内のマシンのみに起動の考慮を制限します。

デスクトップまたはアプリケーショングループのタグ制限としてタグが構成された後で、マシンにそのタグを追加しようとすると、警告が表示されます。そのタグを追加すると、マシンが追加のアプリケーションまたはデスクトップの起動に利用可能になる可能性があります。それが意図したことであれば、続行してください。そうでない場合は、操作をキャンセルできます。

たとえば、「Red」タグ制限を持つアプリケーショングループを作成したとします。その後、そのアプリケーショングループで使用されている同じデリバリーグループに他のマシンをいくつか追加します。そのマシンに「Red」タグを追加しようとすると、Web Studioは次のようなメッセージを表示します。「タグ「Red」は以下のアプリケーショングループの制限として使用されています。このタグを追加すると、選択したマシンがこのアプリケーショングループ内のアプリケーションを起動できるようになる可能性があります。」その後、それらの追加のマシンにそのタグを追加することを確認またはキャンセルできます。

同様に、アプリケーショングループが起動を制限するためにタグを使用している場合、Web Studioは、制限として削除するためにグループを編集するまでタグを削除できないことを警告します。（アプリケーショングループで制限として使用されているタグを削除することが許可された場合、その結果、アプリケーショングループに関連付けられたデリバリーグループ内のすべてのマシンでアプリケーションの起動が許可される可能性があります。）デスクトップの起動の制限としてタグが使用されている場合も、タグの削除に対する同じ禁止が適用されます。そのタグ制限を削除するためにアプリケーショングループまたはデリバリーグループ内のデスクトップを編集した後、タグを削除できます。

すべてのマシンが同じアプリケーションセットを持っているとは限りません。ユーザーは複数のアプリケーショングループに属することができ、それぞれが異なるタグ制限と、デリバリーグループからの異なるまたは重複するマシンセットを持っています。以下の表は、マシンの考慮事項がどのように決定されるかを示しています。

アプリケーションが追加された場合	選択されたデリバリーグループ内のこれらのマシンが起動対象と見なされます
タグ制限のない1つのアプリケーショングループ	任意のマシン。
タグ制限Aのある1つのアプリケーショングループ	タグAが適用されているマシン。
2つのアプリケーショングループ（1つはタグ制限A、もう1つはタグ制限B）	タグAとタグBを持つマシン。利用可能なマシンがない場合は、タグAまたはタグBを持つマシン。
2つのアプリケーショングループ（1つはタグ制限A、もう1つはタグ制限なし）	タグAを持つマシン。利用可能なマシンがない場合は、任意のマシン。

マシン再起動スケジュールでタグ制限を使用した場合、タグの適用または制限に影響を与える変更は、次のマシン再起動サイクルに影響します。変更が行われている間に進行中の再起動サイクルには影響しません。

例2の構成方法

以下の手順では、タグを作成して適用し、2番目の例で示されているアプリケーショングループのタグ制限を構成する手順を示します。

VDAとアプリケーションはすでにマシンにインストールされており、デリバリーグループも作成されています。

マシンにタグを作成して適用します。

1. Web Studioで、デリバリーグループD01を選択し、アクションバーで**View Machines**を選択します。
2. マシン VDA 101～105 を選択し、アクションバーで**タグの管理**を選択します。
3. タグの管理ダイアログボックスで、**作成**をクリックし、`CADApps`という名前のタグを作成します。**OK**をクリックします。
4. もう一度**作成**をクリックし、OfficeAppsという名前のタグを作成します。**OK**をクリックします。
5. **タグの管理**ダイアログボックスを開いたまま、各タグの名前（`CADApps`と`OfficeApps`）の横にあるチェックボックスを有効にして、新しく作成したタグを選択したマシンに追加（適用）します。完了したら、ダイアログボックスを閉じます。
6. デリバリーグループ D01 を選択し、アクションバーで**マシンの表示**を選択します。
7. マシン VDA 106～110 を選択し、アクションバーで**タグの管理**を選択します。
8. **タグの管理**ダイアログボックスで、**作成**をクリックします。`AcctgApps`という名前のタグを作成します。**OK**をクリックします。
9. 新しく作成した`AcctgApps`タグと`OfficeApps`タグを、各タグ名の横にあるチェックボックスをクリックして選択したマシンに適用し、ダイアログボックスを閉じます。

タグ制限付きのアプリケーショングループを作成します。

1. Web Studioで、左ペインの**アプリケーション**を選択し、**アプリケーショングループ**タブを選択してから、アクションバーの**アプリケーショングループの作成**を選択します。アプリケーショングループ作成ウィザードが起動します。
2. ウィザードの**デリバリーグループ**ページで、デリバリーグループ D01 を選択します。**タグ付きマシンへの起動を制限する**を選択し、リストから`AcctgApps`タグを選択します。
3. 会計ユーザーと会計アプリケーションを指定してウィザードを完了します。（アプリケーションを追加するときは、`AcctgApps`タグを持つマシンでアプリケーションを検索する**スタート**

メニューからソースを選択します。）**概要**ページで、グループに`A100`という名前を付けます。

4. 前の手順を繰り返して、`CADApps`タグを持つマシンと、適切なユーザーおよびアプリケーションを指定して、アプリケーショングループ`A200`を作成します。
5. 手順を繰り返して、`OfficeApps`タグを持つマシンと、適切なユーザーおよびアプリケーションを指定して、アプリケーショングループ`A300`を作成します。

マシンカタログのタグ

マシンカタログでタグを使用できます。タグを作成してカタログに適用する全体的な手順は、前述のとおりです。ただし、カタログへのタグの適用は、PowerShellインターフェースを介してのみサポートされています。Web Studioを使用してカタログにタグを適用したり、カタログからタグを削除したりすることはできません。Web Studioのカタログ表示では、タグが適用されているかどうかは示されません。

概要: Web StudioまたはPowerShellを使用して、カタログで使用するタグを作成または削除できます。PowerShellを使用して、タグをカタログに適用します。

カタログでタグを使用する例をいくつか示します。

- デリバリーグループには複数のカタログのマシンが含まれていますが、操作（再起動スケジュールなど）を特定のカタログのマシンのみに影響させたい場合。そのカタログにタグを適用することで、それが実現できます。
- アプリケーショングループで、アプリケーションセッションを特定のカタログのマシンに制限したい場合。そのカタログにタグを適用することで、それが実現できます。

影響を受けるPowerShellコマンドレット:

- `Add-BrokerTag`や`Remove-BrokerTag`などのコマンドレットにカタログオブジェクトを渡すことができます。
- `Get-BrokerTagUsage`は、タグを含むカタログの数を示します。
- `Get-BrokerCatalog`には、`Tags`という名前のプロパティがあります。

例えば、次のコマンドレットは、`acctg`という名前のカタログに`fy2018`という名前のタグを追加します。`Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`。（タグは以前にWeb StudioまたはPowerShellのいずれかを使用して作成されています。）

詳細なガイダンスと構文については、PowerShellコマンドレットのヘルプを参照してください。

自動タグ

自動タグを使用すると、マシン、アプリケーショングループ、アプリケーション、デスクトップグループ、またはデスクトップに対するタグの自動追加および削除のルールを定義できます。定義されたルールを満たさない場合、タグは自動的に削除されます。この機能強化により、環境最適化のために定期的に実行されるさまざまなスクリプトを維持する必要がなくなります。

ユースケース

自動タグ付けを使用すると、コスト削減、インフラストラクチャの最適化、消費の促進など、ビジネスドライバーに関連するルールを実装できます。以下にいくつかのユースケースを示します。

- **未使用VDIの再利用** - 事前設定された日数以上使用されていない専用ワークロードを、利用可能なプールに解放するため。
- **アプリケーションの煩雑さを解消** - 事前設定された日数以上使用されていないアプリケーションを特定することで、アプリケーションの煩雑さを軽減するため。
- **X未満の機能レベルを持つDG** - 特定の機能レベル未満のデリバリーグループを見つけるため。
- **非アクティブユーザー** - 事前設定された日数以上ログオンしていないユーザーのリソースを再利用するため。

> **注:**
>
> 30日以上使用されていないマシンに付与されたタグは、ユーザーが30日後にそのマシンにログインした場合、次回実行時にそのマシンから削除されます。

PowerShellコマンド

PowerShellコマンドを使用してオートタグを作成できます。オートタグルールが作成されると、3600秒の頻度で評価されます。詳細については、New-BrokerAutoTagRuleを参照してください。

`New-BrokerAutoTagRule` のパラメーターは次のとおりです。

- 名前: ルールの汎用名
- オブジェクトタイプ: マシン
- ルールテキスト: ルールを定義するフィルター。
- タグUid: 関連付けたいタグID。

例

1. 30日以上使用されていない専用VDIにタグを付けるには:

```
New-BrokerAutoTagRule -Name ‘UnusedVdi’ -ObjectType ‘Machine’ -RuleText
“-AllocationType Static -IsAssigned $true -Filter { SummaryState -ne
`”InUse`” -and ( LastConnectionTime -lt ‘-30’ -or LastConnectionTime
-eq `$null ) }” -TagUid 123
```

ルールが構成されると、**unused-VDI** タグを持つマシンが解放されます。

2. 機能レベルがX未満のデリバリーグループにタグを付けるには（しきい値機能レベルとして **L7_20** を使用）：

```
New-BrokerAutoTagRule -Name 'LowFL' -ObjectType 'DesktopGroup'
-RuleText " -Filter { MinimumFunctionalLevel -lt 'L7_20' } " -TagUid
143
```

3. フォルダーなしで公開されたユーザーに表示されるアプリにタグを付けるには：

```
New-BrokerAutoTagRule -Name 'NoFolder' -ObjectType 'Application'
-RuleText "-Enabled $true -Filter { ClientFolder -eq $null } " -TagUid
153`
```

詳細情報

ブログ投稿：特定のサーバーにデスクトップを割り当てる方法。

ユーザープロファイル

デフォルトでは、Virtual Delivery Agentをインストールするとと Citrix Profile Managementがマスターイメージにサイレントインストールされますが、プロファイルソリューションとしてProfile Managementを使用する必要はありません。

ユーザーのさまざまなニーズに合わせて、Citrix Virtual Apps and Desktops™ポリシーを使用して、各デリバリーグループ内のマシンに異なるプロファイル動作を適用できます。たとえば、あるデリバリーグループでは、テンプレートが1つのネットワーク場所に保存されているCitrix強制プロファイルが必要になる場合があります。一方、別のデリバリーグループでは、複数のリダイレクトされたフォルダーとともに別の場所に保存されているCitrixローミングプロファイルが必要になります。

- 組織内の他の管理者がCitrix Virtual Apps™ and Desktopsポリシーを担当している場合は、彼らと協力して、デリバリーグループ全体でプロファイル関連のポリシーが設定されていることを確認してください。

- Profile Managementポリシーは、グループポリシー、Profile Management .iniファイル、および個々の仮想マシン上でローカルに設定することもできます。プロファイル動作を定義するこれらの複数の方法は、次の順序で読み取られます。

  a. グループポリシー (.admまたは.admxファイル)

  b. ポリシーノード内のCitrix Virtual Apps and Desktopsポリシー

  c. ユーザーが接続する仮想マシン上のローカルポリシー

  d. Profile Management .iniファイル

  たとえば、グループポリシーとポリシーノードの両方で同じポリシーを構成した場合、システムはグループポリシーのポリシー設定を読み取り、Citrix Virtual Apps and Desktopsポリシー設定を無視します。

どのプロファイルソリューションを選択しても、Director管理者は診断情報にアクセスし、ユーザープロファイルのトラブルシューティングを行うことができます。詳しくは、Directorのドキュメントを参照してください。

自動構成

デスクトップの種類は、Virtual Delivery Agentのインストールに基づいて自動的に検出され、Studioで行う構成の選択に加えて、それに応じてProfile Managementのデフォルトを設定します。

Profile Managementが調整するポリシーを次の表に示します。デフォルト以外のポリシー設定は保持され、この機能によって上書きされることはありません。各ポリシーの詳細については、Profile Managementのドキュメントを参照してください。プロファイルを作成するマシンの種類は、調整されるポリシーに影響します。主な要因は、マシンが永続的かプロビジョニング済みか、および複数のユーザーで共有されるか、1人のユーザー専用であるかです。

永続システムには何らかのローカルストレージがあり、システムがシャットダウンしてもその内容は永続すると予想されます。永続システムは、SANなどのストレージテクノロジーを使用して、ローカルディスクのエミュレーションを提供する場合があります。対照的に、プロビジョニングされたシステムは、ベースディスクと何らかのIDディスクから「オンザフライ」で作成されます。ローカルストレージは通常、RAMディスクまたはネットワークディスクによってエミュレートされますが、後者は高速リンクを備えたSANによって提供されることがよくあります。プロビジョニングテクノロジーは、一般的にCitrix ProvisioningまたはMachine Creation Services™（あるいはサードパーティ製の同等品）です。プロビジョニングされたシステムが永続的なローカルストレージを持つこともあります。これらは永続的として分類されます。

これら2つの要素を合わせると、以下のマシンタイプが定義されます。

- **永続的かつ専用**。例としては、Machine Creation Servicesで作成された静的割り当てと永続的なローカルストレージを持つシングルセッションOSマシン、物理ワークステーション、ラップトップなどがあります。
- **永続的かつ共有**。例としては、Machine Creation Servicesで作成されたマルチセッションOSマシン、およびCitrix Virtual Appsサーバーなどがあります。
- **プロビジョニング済みかつ専用**。例としては、静的割り当てを持つが永続ストレージを持たないシングルセッションOSマシンで、Citrix Provisioning Service (Citrix Virtual Desktops™内) で作成されたものなどがあります。
- **プロビジョニング済みかつ共有**。例としては、ランダム割り当てを持つシングルセッションOSマシンで、Citrix Provisioning™ Service (Citrix Virtual Desktops内) で作成されたもの、およびCitrix Virtual Appsサーバーなどがあります。

以下のプロファイル管理ポリシー設定は、異なるマシンタイプに対する推奨ガイドラインです。ほとんどの場合にうまく機能しますが、展開の要件に応じてこれらから逸脱することもできます。

> **重要:**
>
> **ログオフ時にローカルにキャッシュされたプロファイルを削除**、**プロファイルストリーミング**、および**常にキャッシュ**は、自動構成機能によって適用されます。その他のポリシーは手動で調整してください。

永続マシン

ポリシー	永続的かつ専用	永続的かつ共有
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効	有効
プロファイルストリーミング	無効	有効
常にキャッシュ	有効 (注1)	無効 (注2)
アクティブライトバック	無効	無効 (注3)
ローカル管理者によるログオンの処理	有効	無効 (注4)

プロビジョニング済みマシン

ポリシー	プロビジョニング済みと専用の両方	プロビジョニング済みと共有の両方
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効 (注5)	有効
プロファイルストリーミング	有効	有効
常にキャッシュ	無効 (注6)	無効
アクティブライトバック	有効	有効
ローカル管理者によるログオンの処理	有効	有効 (注7)

1. このマシンタイプでは**プロファイルストリーミング**が無効になっているため、**常にキャッシュ**設定は常に無視されます。
2. **常にキャッシュ**を無効にします。ただし、このポリシーを有効にし、ファイルサイズ制限 (MB単位) を定義することで、ログオン後できるだけ早く大きなファイルがプロファイルにロードされるようにすることができます。このサイズ以上のファイルは、できるだけ早くローカルにキャッシュされます。
3. Citrix Virtual Appsサーバー間をローミングするユーザーのプロファイルへの変更を保存する場合を除き、**アクティブライトバック**を無効にします。この場合は、このポリシーを有効にします。
4. ホスト型共有デスクトップの場合を除き、**ローカル管理者のログオンを処理**を無効にします。この場合は、このポリシーを有効にします。
5. **ログオフ時にローカルにキャッシュされたプロファイルを削除**を無効にします。この設定は、ローカルにキャッシュされたプロファイルを保持します。マシンはログオフ時にリセットされますが、個々のユーザーに割り当てられるため、プロファイルがキャッシュされている場合はログオンが高速になります。
6. **常にキャッシュ**を無効にします。ただし、このポリシーを有効にし、ファイルサイズ制限 (MB単位) を定義することで、ログオン後できるだけ早く大きなファイルがプロファイルにロードされるようにすることができます。このサイズ以上のファイルは、できるだけ早くローカルにキャッシュされます。

7. Citrix Virtual Apps and Desktopsサーバー間をローミングするユーザーのプロファイルの場合を除き、**ローカル管理者のログオンを処理**を有効にします。この場合は、このポリシーを無効にします。

フォルダーリダイレクト

フォルダーリダイレクトを使用すると、プロファイルが保存されている場所とは異なるネットワーク共有にユーザーデータを保存できます。フォルダーリダイレクトはプロファイルサイズとロード時間を削減しますが、ネットワーク帯域幅に影響を与える可能性があります。フォルダーリダイレクトは、Citrixユーザープロファイルが使用されていることを必要としません。ユーザープロファイルを独自に管理し、フォルダーをリダイレクトすることもできます。

StudioでCitrixポリシーを使用してフォルダーリダイレクトを構成します。

- リダイレクトされたフォルダーのコンテンツを保存するために使用されるネットワークの場所が利用可能であり、適切な権限を持っていることを確認してください。場所のプロパティは検証されます。
- リダイレクトされたフォルダーはネットワーク上に設定され、そのコンテンツはログオン時にユーザーの仮想デスクトップから入力されます。

フォルダーリダイレクトは、CitrixポリシーまたはActive Directoryグループポリシーオブジェクトのいずれか一方のみを使用して構成し、両方は使用しないでください。両方のポリシーエンジンを使用してフォルダーリダイレクトを構成すると、予期しない動作が発生する可能性があります。

高度なフォルダーリダイレクト

複数のオペレーティングシステム (OS) を使用する展開では、ユーザープロファイルの一部を各OSで共有したい場合があります。プロファイルの残りの部分は共有されず、1つのOSでのみ使用されます。OS間で一貫したユーザーエクスペリエンスを確保するには、各OSで異なる構成、つまり高度なフォルダーリダイレクトが必要です。たとえば、2つのOSで実行されているアプリケーションの異なるバージョンが共有ファイルを読み書きする必要がある場合、両方のバージョンがアクセスできる単一のネットワーク場所にリダイレクトすることを決定します。あるいは、2つのOSで**スタートメニュー**フォルダーの内容の構造が異なるため、両方ではなく、いずれか1つのフォルダーのみをリダイレクトすることを決定します。このアプローチにより、各OSで**スタートメニュー**フォルダーとその内容が分離され、ユーザーに一貫したエクスペリエンスが保証されます。

展開で高度なフォルダーリダイレクトが必要な場合は、ユーザーのプロファイルデータの構造を理解し、そのどの部分をOS間で共有できるかを判断する必要があります。フォルダーリダイレクトが正しく使用されないと、予期しない動作が発生する可能性があります。

高度な展開でフォルダーをリダイレクトするには：

- 各OSに個別のデリバリーグループを使用します。
- 仮想デスクトップ上のものを含む仮想アプリケーションがユーザーデータと設定をどこに保存するかを理解し、データの構造を理解します。
- 安全にローミングできる共有プロファイルデータ（各OSで同じ構造であるため）については、各デリバリーグループ内のコンテナフォルダーをリダイレクトします。
- ローミングできない非共有プロファイルデータについては、デスクトップグループのいずれか1つ（通常は最も使用されているOSまたはデータが最も関連性の高いOS）のコンテナフォルダーをリダイレクトします。あるいは、OS間でローミングできない非共有データについては、両方のシステムのコンテナフォルダーを別々のネットワーク場所にリダイレクトします。

高度な展開の例

この展開には、Windows 10デスクトップで実行されるMicrosoft OutlookおよびInternet Explorerのバージョンを含むアプリケーションと、Windows Server 2019によって配信されるOutlookおよびInternet Explorerの他のバージョンを含むアプリケーションがあります。2つのOS用に2つのデリバリーグループを既に設定しています。ユーザーは、両方のアプリケーションのバージョンで同じ**連絡先**と**お気に入り**のセットにアクセスしたいと考えています。

重要: 以下の決定とアドバイスは、説明されているOSと展開に有効です。組織では、リダイレクトするフォルダーとそれらを共有するかどうかの決定は、特定の展開に固有のさまざまな要因によって異なります。

- デリバリーグループに適用されるポリシーを使用して、次のフォルダーをリダイレクトするように選択します。

フォルダ	WINDOWS 10でリダイレクトされますか？	WINDOWS SERVER 2019でリダイレクトされますか？
マイドキュメント	はい	はい
アプリケーションデータ	いいえ	いいえ
連絡先	はい	はい
デスクトップ	はい	いいえ
ダウンロード	いいえ	いいえ
お気に入り	はい	はい

フォルダ	WINDOWS 10でリダイレクトされますか？	WINDOWS SERVER 2019でリダイレクトされますか？
リンク	はい	いいえ
マイミュージック	はい	はい
マイピクチャ	はい	はい
マイビデオ	はい	はい
検索	はい	いいえ
保存されたゲーム	いいえ	いいえ
スタートメニュー	はい	いいえ

- 共有され、リダイレクトされたフォルダーの場合:
  - OutlookおよびInternet Explorerの異なるバージョンによって保存されたデータの構造を分析した結果、**連絡先**フォルダーと**お気に入り**フォルダーを共有しても安全であると判断しました。
  - **マイ ドキュメント**、**マイ ミュージック**、**マイ ピクチャ**、**マイ ビデオ**フォルダーの構造は、OS間で標準であることがわかっています。そのため、これらのフォルダーを各デリバリーグループの同じネットワーク場所に保存しても安全です。
- 共有されていない、リダイレクトされたフォルダーの場合:
  - Windows Serverデリバリーグループでは、デスクトップ、リンク、検索、または**スタートメニュー**フォルダーをリダイレクトしません。これらのフォルダーのデータは2つのOSで異なる方法で整理されているためです。したがって、共有することはできません。
  - この共有されていないデータの予測可能な動作を保証するために、Windows 10デリバリーグループでのみリダイレクトします。Windows 10は、ユーザーが日常業務でより頻繁に使用します。ユーザーは、Windows Serverによって提供されるアプリケーションにたまにしかアクセスしません。また、この場合、共有されていないデータは、アプリケーション環境よりもデスクトップ環境により関連性があります。たとえば、デスクトップショートカットは**デスクトップ**フォルダーに保存され、Windows 10マシンから発生した場合は役立つ可能性がありますが、Windows Serverマシンから発生した場合は役立ちません。
- リダイレクトされていないフォルダーの場合:

- ユーザーがダウンロードしたファイルでサーバーを散らかしたくないため、ダウンロードフォルダーをリダイレクトしないことを選択します。
- 個々のアプリケーションからのデータは互換性およびパフォーマンスの問題を引き起こす可能性があるため、アプリケーションデータフォルダーをリダイレクトしないことを決定します。

フォルダーリダイレクトの詳細については、「フォルダーリダイレクト、オフラインファイル、および移動ユーザープロファイルの概要」を参照してください。

フォルダーリダイレクトと除外

Citrix Profile Managementでは（Studioでは不可）、パフォーマンス強化により、除外を使用してフォルダーが処理されるのを防ぐことができます。この機能を使用する場合、リダイレクトされたフォルダーを除外しないでください。フォルダーリダイレクトと除外機能は連携して動作します。リダイレクトされたフォルダーが除外されないようにすることで、Profile Managementはそれらをプロファイルフォルダー構造に戻し、後でリダイレクトしないと決定した場合でもデータ整合性を維持できます。除外の詳細については、「項目の含める/除外」を参照してください。

VDA登録

はじめに

> **注:**
>
> オンプレミス環境では、VDAはDelivery Controllerに登録します。Citrix Cloudサービス環境では、VDAはCloud Connectorに登録します。ハイブリッド環境では、一部のVDAはDelivery Controllerに登録し、他のVDAはCloud Connectorに登録します。

> VDAを使用する前に、サイト上の1つ以上のControllerまたはCloud Connectorに登録（通信を確立）する必要があります。VDAは、`ListofDDCs`と呼ばれるリストをチェックしてControllerまたはConnectorを見つけます。VDA上の`ListOfDDCs`には、そのVDAをサイト上のControllerまたはCloud Connectorにポイントするエントリが含まれています。負荷分散のため、VDAはリスト内のすべてのControllerまたはCloud Connectorに接続を自動的に分散します。

VDA登録がこれほど重要なのはなぜですか？

- セキュリティの観点から見ると、登録は機密性の高い操作です。ControllerまたはCloud ConnectorとVDA間の接続を確立しています。このような機密性の高い操作では、すべてが完璧な状態でない場合、接続を拒否するのが期待される動作です。事実上、VDAからControllerまたはCloud Connectorへ、およびControllerまたはCloud ConnectorからVDAへの2つの別々の通信チャネルを確立しています。接続にはKerberosが使用されるため、時刻同期やドメインメンバーシップの問題は許容されません。Kerberosはサービスプリンシパル名（SPN）を使用するため、負荷分散されたIP\\ホスト名を使用することはできません。
- Controller（またはCloud Connector）を追加および削除する際に、VDAが正確で最新のControllerまたはCloud Connector情報を持っていない場合、VDAはリストにないControllerまたはCloud Connectorによって仲介されるセッション起動を拒否する可能性があります。無効なエントリは、仮想デスクトップシステムソフトウェアの起動を遅らせる可能性があります。VDAは、不明で信頼できないControllerまたはCloud Connectorからの接続を受け入れません。

`ListofDDCs`に加えて、`ListOfSIDs`（セキュリティID）は、`ListofDDCs`内のどのマシンが信頼されているかを示します。`ListofSIDs`は、Active Directoryの負荷を軽減したり、侵害されたDNSサーバーからの潜在的なセキュリティ脅威を回避したりするために使用できます。詳細については、ListOfSIDsを参照してください。

`ListofDDCs`が複数のControllerまたはCloud Connectorを指定している場合、VDAはランダムな順序でそれらに接続しようとします。オンプレミス展開では、`ListofDDCs`にはControllerグループも含まれる場合があります。VDAは、`ListofDDCs`内の他のエントリに移動する前に、グループ内の各Controllerに接続しようとします。

Citrix Virtual Apps and Desktops™は、VDAのインストール中に、構成されたControllerまたはCloud Connectorへの接続を自動的にテストします。ControllerまたはCloud Connectorに到達できない場合、エラーが表示されます。ControllerまたはCloud Connectorに連絡できないという警告を無視した場合（またはVDAのインストール中にControllerまたはCloud Connectorのアドレスを指定しなかった場合）、メッセージが表示されて通知されます。

ControllerまたはCloud Connectorアドレスを構成する方法

管理者は、VDAが初めて登録するとき（初回登録）に使用する構成方法を選択します。初回登録時に、VDA上に永続的なキャッシュが作成されます。その後の登録では、構成の変更が検出されない限り、VDAはこのローカルキャッシュからControllerまたはCloud Connectorのリストを取得します。

その後の登録でそのリストを取得する最も簡単な方法は、自動更新機能を使用することです。自動更新はデフォルトで有効になっています。詳細については、「自動更新」を参照してください。

VDA上でControllerまたはCloud Connectorアドレスを構成する方法はいくつかあります。

- ポリシーベース（LGPOまたはGPO）
- レジストリベース（手動、グループポリシー設定（GPP）、VDAインストール時に指定）
- Active Directory OUベース（レガシーOU検出）
- MCSベース (personality.ini)

VDAをインストールする際に、初期登録方法を指定します。(自動更新を無効にした場合、VDAインストール時に選択した方法がその後の登録に使用されます。)

次の図は、VDAインストールウィザードの**Delivery Controller**ページを示しています。

VDAインストールウィザードのDelivery Controllerページ(/en-us/citrix-virtual-apps-desktops/2511/media/vda-install-controllers-all.png)

ポリシーベース (LGPO\\GPO)

Citrix®は、初期VDA登録にGPOを使用することを推奨します。これは最も高い優先順位を持ちます。(自動更新が最も高い優先順位としてリストされていますが、自動更新は初期登録後にのみ使用されます。) ポリシーベースの登録は、構成にグループポリシーを使用することによる一元化の利点を提供します。

この方法を指定するには、以下の両方の手順を完了します。

- VDAインストールウィザードの**Delivery Controller**ページで、**後で実行 (詳細)** を選択します。ウィザードは、VDAインストール中にControllerアドレスを指定しない場合でも、Controllerアドレスを指定するよう何度も通知します。(VDA登録はそれほど重要です。)
- Citrixポリシーを介してポリシーベースのVDA登録を有効または無効にします。`Virtual Delivery Agent Settings > Controllers`設定を使用します。(セキュリティが最優先事項である場合は、`Virtual Delivery Agent Settings > Controller SIDs`設定を使用します。)

この設定は`HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)`の下に保存されます。

レジストリベース

この方法を指定するには、以下のいずれかの手順を完了します。

- VDAインストールウィザードの**Delivery Controller**ページで、**手動で実行** を選択します。次に、インストールされているControllerのFQDNを入力し、**追加** をクリックします。複数のControllerをインストールしている場合は、それらのアドレスを追加します。

- コマンドラインVDAインストールの場合、/controllersオプションを使用し、インストールされているControllerまたはCloud ConnectorのFQDNを指定します。

この情報は、レジストリキー`HKLM\Software\Citrix\VirtualDesktopAgent`または`HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent`の下のレジストリ値`ListOfDDCs`に保存されます。

このレジストリキーは、手動で構成することも、グループポリシー設定 (GPP) を使用することもできます。この方法は、ポリシーベースの方法よりも推奨される場合があります（たとえば、異なるControllerまたはCloud Connectorの条件付き処理が必要な場合など。例：XDW-001-で始まるコンピューター名にはXDC-001を使用する）。

`ListOfDDCs`レジストリキーを更新します。このキーには、サイト内のすべてのControllerまたはCloud ConnectorのFQDNが一覧表示されます。(このキーはActive Directoryサイト OUに相当します。)

```
HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)
```

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`レジストリの場所に`ListOfDDCs`と`FarmGUID`の両方のキーが含まれている場合、ControllerまたはCloud Connectorの検出には`ListOfDDCs`が使用されます。VDAのインストール中にサイトOUが指定された場合、`FarmGUID`が存在します。(これはレガシー展開で使用される場合があります。)

オプションで、`ListOfSIDs`レジストリキーを更新します（詳細については、ListOfSIDsを参照してください）。

```
HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)
```

注意：Citrixポリシーを介してポリシーベースのVDA登録も有効にすると、それはより優先度の高い方法であるため、VDAインストール中に指定した設定が上書きされます。

Active Directory OUベース (レガシー)

この方法は、主に下位互換性のためにサポートされており、推奨されません。まだ使用している場合は、Citrixは別の方法に変更することを推奨します。

この方法を指定するには、以下の両方の手順を完了します。

- VDAインストールウィザードの**Delivery Controller**ページで、**Active Directoryから場所を選択**を選択します。

- `Set-ADControllerDiscovery.ps1`スクリプト（すべてのControllerで利用可能）を使用します。また、各VDAで`FarmGuid`レジストリエントリを構成して、適切なOUを指すようにします。この設定は、グループポリシーを使用して構成できます。

MCSベース

MCSを使用してVMをプロビジョニングする場合、MCSはControllerまたはCloud Connectorのリストを設定します。この機能は自動更新と連携します。カタログの作成時、MCSは初期プロビジョニング中にControllerまたはCloud Connectorのリストを`Personality.ini`ファイルに挿入します。自動更新により、リストは最新の状態に保たれます。

この方法を指定するには、VDAインストールウィザードの **Delivery Controller** ページで、**Machine Creation Services™に任せる** を選択します。

レビューと推奨事項

ベストプラクティスとして:

- 初期登録にはグループポリシー登録方法を使用します。
- Controllerのリストを最新の状態に保つには、自動更新（デフォルトで有効）を使用します。
- マルチゾーン展開では、初期構成にはグループポリシーを使用します（ControllerまたはCloud Connectorを2つ以上使用）。VDAを、そのゾーン内のローカルなControllerまたはCloud Connectorに向けます。自動更新を使用して、それらを最新の状態に保ちます。自動更新は、サテライトゾーンのVDAに対して`ListofDDCs`を自動的に最適化します。
- Controllerが利用できない場合の登録の問題を防ぐため、`ListOfDDCs`レジストリキーに複数のControllerをスペースで区切ってリストします。例:

```
DDC7x.xd.local DDC7xHA.xd.local



32-bit: HKEY_LOCAL_MACHINE
\Software\Citrix\VirtualDesktopAgent\ListOfDDCs



HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\ListOfDDCs
(REG_SZ)
```

- 起動時の登録遅延を防ぐため、`ListofDDCs`の下にリストされているすべての値が、有効な完全修飾ドメイン名にマップされていることを確認します。

自動更新

自動更新（XenAppおよびXenDesktop 7.6で導入）は、デフォルトで有効になっています。これは、VDA登録を最新の状態に保つための最も効率的な方法です。初期登録には使用されませんが、初期登録時に、自動更新ソフトウェアは`ListofDDCs`をダウンロードし、VDA上の永続キャッシュに保存します。このプロセスは各VDAに対して実行されます。キャッシュにはマシンポリシー情報も保持され、これによりポリシー設定が再起動後も保持されます。

自動更新は、MCSまたはCitrix Provisioning™を使用してマシンをプロビジョニングする場合にサポートされますが、Citrix Provisioningのサーバー側キャッシュは除きます。サーバー側キャッシュは、自動更新キャッシュ用の永続ストレージがないため、一般的なシナリオではありません。

この方法を指定するには:

- 設定`Virtual Delivery Agent Settings > Enable auto update of Controllers`を含むCitrixポリシーを介して自動更新を有効または無効にします。この設定はデフォルトで有効になっています。

仕組み：

- VDAが再登録されるたび（たとえば、マシンの再起動後）に、キャッシュが更新されます。各ControllerまたはCloud Connectorも、90分ごとにサイトデータベースをチェックします。前回のチェック以降にControllerまたはCloud Connectorが追加または削除された場合、あるいはVDA登録に影響するポリシー変更が発生した場合、ControllerまたはCloud Connectorは登録済みのVDAに更新されたリストを送信し、キャッシュが更新されます。VDAは、最新のキャッシュ済みリストにあるすべてのControllerまたはCloud Connectorからの接続を受け入れます。
- VDAが、自身が登録されているControllerまたはCloud Connectorが含まれていないリストを受け取った場合（つまり、そのControllerまたはCloud Connectorがサイトから削除された場合）、VDAは、`ListofDDCs`にあるControllerまたはCloud Connectorの中から選択して再登録します。

例：

- ある展開には、3つのController（A、B、C）があります。VDAはController Bに登録されます（これはVDAのインストール時に指定されました）。
- その後、2つのController（DとE）がサイトに追加されます。90分以内に、VDAは更新されたリストを受け取り、Controller A、B、C、D、Eからの接続を受け入れます。（VDAが再起動されるまで、負荷はすべてのControllerに均等に分散されません。）

- さらにその後、Controller Bが別のサイトに移動されます。90分以内に、元のサイトのVDAは、前回のチェック以降にControllerの変更があったため、更新されたリストを受け取ります。元々Controller Bに登録されていたVDA（リストにはもうありません）は、現在のリスト（A、C、D、E）にあるControllerの中から選択して再登録します。

マルチゾーン展開では、サテライトゾーンの自動更新機能が、まずすべてのローカルControllerを自動的にキャッシュします。プライマリゾーンのすべてのControllerは、バックアップグループにキャッシュされます。サテライトゾーンにローカルControllerが利用できない場合、プライマリゾーンのControllerで登録が試行されます。

次の例に示すように、キャッシュファイルにはホスト名とセキュリティIDのリスト（`ListofSIDs`）が含まれています。VDAはSIDを照会しないため、Active Directoryの負荷を軽減します。



```
<?xml version="1.0"?>
<ListOfDDcsListIfSids xmlns="http://schemas.datacontract.org/2004/07/Citrix.Cds.BrokerAgent" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
 - <_x003C_GroupsOfDDCs_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
    - <d2p1:ArrayOfstring>
        <d2p1:string>CTX-XDC-002.zugec.lan</d2p1:string>
        <d2p1:string>CTX-XDC-001.zugec.lan</d2p1:string>
      </d2p1:ArrayOfstring>
   </_x003C_GroupsOfDDCs_x003E_k__BackingField>
 - <_x003C_ListOfDDCs_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
      <d2p1:string>CTX-XDC-002.zugec.lan</d2p1:string>
      <d2p1:string>CTX-XDC-001.zugec.lan</d2p1:string>
   </_x003C_ListOfDDCs_x003E_k__BackingField>
 - <_x003C_ListOfSids_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
      <d2p1:string>S-1-5-21-726903571-3621260514-849154371-1119</d2p1:string>
      <d2p1:string>S-1-5-21-726903571-3621260514-849154371-1126</d2p1:string>
   </_x003C_ListOfSids_x003E_k__BackingField>
   <_x003C_NonAutoListOfDDCsMethod_x003E_k__BackingField>RegistryBasedFarm</_x003C_NonAutoListOfDDCsMethod_x003E_k__BackingField>
   <_x003C_NonAutoListOfDDCsOrOu_x003E_k__BackingField>CTX-XDC-002.zugec.lan</_x003C_NonAutoListOfDDCsOrOu_x003E_k__BackingField>
</ListOfDDcsListIfSids>
```


WMI呼び出しでキャッシュファイルを取得できます。ただし、SYSTEMアカウントのみが読み取り可能な場所に保存されています。

> **重要：**
>
> この情報は、情報提供のみを目的としています。このファイルを変更しないでください。このファイルまたはフォルダーに対するいかなる変更も、サポートされていない構成となります。

```
Get-WmiObject -Namespace "Root\Citrix\DesktopInformation" -Class "Citrix_VirtualDesktopInfo" -Property "PersistentDataLocation"
```

セキュリティ上の理由から（Active Directoryの負荷軽減とは別に）`ListofSIDs`を手動で構成する必要がある場合、自動更新機能を使用することはできません。詳細については、「ListOfSIDs」を参照してください。

自動更新の優先順位の例外

自動更新は通常、すべてのVDA登録方法の中で最も高い優先順位を持ち、他の方法の設定を上書きしますが、例外があります。キャッシュ内の `NonAutoListOfDDCs` 要素は、初期VDA構成方法を指定します。自動更新はこの情報を監視します。初期登録方法が変更された場合、登録プロセスは自動更新をスキップし、次に高い優先順位で構成された方法を使用します。このプロセスは、VDAを別のサイトに移動する場合 (たとえば、ディザスターリカバリー中) に役立ちます。

構成に関する考慮事項

一般的なVDA登録構成を表示します。

<iframe src="https://www.youtube.com/embed/MgGMZp4SnZgEq9ieibQc9j" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
VDA登録手順を表示します。

<iframe src="https://www.youtube.com/embed/iwsbajSVY5QvoUTh6m7AjG" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
VDA登録に影響を与える可能性のある項目を構成する際は、次の点を考慮してください。

ControllerまたはCloud Connectorのアドレス

ControllerまたはCloud Connectorを指定するためにどの方法を使用するかにかかわらず、CitrixはFQDNアドレスを使用することを推奨します。IPアドレスは、DNSレコードよりもIPを侵害する方が容易であるため、信頼できる構成とは見なされません。`ListofSIDs` を手動で入力する場合、`ListofDDCs` でIPを使用できます。ただし、FQDNが引き続き推奨されます。

負荷分散

前述のとおり、VDAは `ListofDDCs` 内のすべてのControllerまたはCloud Connectorに接続を自動的に分散します。フェールオーバーおよび負荷分散機能は、Citrix Brokering Protocol (CBP) に組み込まれています。構成で複数のControllerまたはCloud Connectorを指定した場合、必要に応じて登録はそれらの間で自動的にフェールオーバーします。自動更新では、すべてのVDAに対して自動フェールオーバーが自動的に発生します。

セキュリティ上の理由から、Citrix ADCなどのネットワークロードバランサーを使用することはできません。VDA登録ではKerberos相互認証が使用され、クライアント（VDA）はサービス（Controller）に対して自身のIDを証明する必要があります。ただし、ControllerまたはCloud ConnectorもVDAに対して自身のIDを証明する必要があります。これは、VDAとControllerまたはCloud Connectorが同時にサーバーとクライアントとして機能することを意味します。この記事の

冒頭で述べたように、VDAからController/Cloud Connectorへ、およびController/Cloud ConnectorからVDAへの2つの通信チャネルがあります。

このプロセスにおけるコンポーネントの1つは、Active Directoryコンピューターオブジェクトのプロパティとして保存されるサービスプリンシパル名（SPN）と呼ばれます。VDAがControllerまたはCloud Connectorに接続するときは、通信相手を指定する必要があります。このアドレスがSPNです。負荷分散されたIPを使用すると、Kerberos相互認証は、そのIPが予期されるControllerまたはCloud Connectorに属していないことを正しく認識します。

詳細については、以下を参照してください。

- Kerberosの概要
- Kerberosを使用した相互認証

自動更新による CNAME の置き換え

自動更新機能は、XenApp および XenDesktop 7.x より前のバージョンにおける CNAME (DNS エイリアス) 機能を置き換えます。CNAME 機能は、XenApp および XenDesktop 7 以降では無効になっています。CNAME の代わりに自動更新を使用してください。(CNAME を使用する必要がある場合は、「CTX137960」を参照してください。DNS エイリアスを常に機能させるには、自動更新と CNAME の両方を同時に使用しないでください。)

Controller/Cloud Connector グループ

特定のシナリオでは、Controller または Cloud Connector をグループで処理し、一方のグループを優先し、すべての Controller/Cloud Connector が失敗した場合に他方のグループをフェイルオーバーに使用したい場合があります。Controller または Cloud Connector はリストからランダムに選択されるため、グループ化することで優先的な使用を強制するのに役立ちます。

これらのグループは、単一のサイト内での使用を目的としています (複数のサイトではありません)。

Controller/Cloud Connector のグループを指定するには、かっこを使用します。たとえば、4 つの Controller (プライマリ 2 つとバックアップ 2 つ) の場合、グループ化は次のようになります。

```
(XDC-001.cdz.lan XDC-002.cdz.lan) (XDC-003.cdz.lan XDC-004.cdz.lan)
```

この例では、最初のグループの Controller (001 と 002) が最初に処理されます。両方が失敗した場合、2 番目のグループの Controller (003 と 004) が処理されます。

XenDesktop 7.0 以降の場合、**登録グループ**機能を使用するには、追加の手順を実行する必要があります。Studio から**Controller の自動更新を有効にする**ポリシーを**禁止**する必要があります。

ListOfSIDs

VDA が登録のために接続できる Controller のリストは `ListofDDCs` です。VDA は、`ListofDDCs` の Controller を自動的に信頼しないため、どの Controller を信頼すべきかも知っている必要があります。`ListofSIDs` (セキュリティ ID) は、信頼された Controller を識別します。VDA は、信頼された Controller にのみ登録を試みます。

ほとんどの環境では、`ListofSIDs` は `ListofDDCs` から自動的に生成されます。CDF トレースを使用して `ListofSIDs` を読み取ることができます。

通常、`ListofSIDs` を手動で変更する必要はありません。いくつかの例外があります。最初の 2 つの例外は、新しいテクノロジーが利用可能になったため、もはや有効ではありません。

- **Controllerの役割の分離:** XenAppおよびXenDesktop 7.7でゾーンが導入される前は、登録にControllerのサブセットのみが使用される場合、`ListofSIDs`は手動で構成されていました。たとえば、XDC-001とXDC-002をXMLブローカーとして使用し、XDC-003とXDC-004をVDA登録に使用する場合、すべてのControllerを`ListofSIDs`に、XDC-003とXDC-004を`ListofDDCs`に指定していました。これは一般的な構成でも推奨される構成でもありません。新しい環境では使用しないでください。代わりにゾーンを使用してください。
- **Active Directoryの負荷軽減:** XenAppおよびXenDesktop 7.6で自動更新機能が導入される前は、`ListofSIDs`がドメインコントローラーの負荷を軽減するために使用されていました。`ListofSIDs`を事前に入力することで、DNS名からSIDへの解決をスキップできます。ただし、この永続キャッシュにはSIDが含まれているため、自動更新機能によりこの作業は不要になります。Citrixは自動更新機能を有効にしておくことを推奨します。
- **セキュリティ:** 一部の高度に保護された環境では、侵害されたDNSサーバーからの潜在的なセキュリティ脅威を回避するために、信頼されたControllerのSIDが手動で構成されていました。ただし、これを行う場合は、自動更新機能も無効にする必要があります。そうしないと、永続キャッシュからの構成が使用されます。

したがって、特別な理由がない限り、`ListofSIDs` を変更しないでください。

`ListofSIDs`を変更する必要がある場合は、`HKLM\Software\Citrix\VirtualDesktopAgent`の下に`ListOfSIDs (REG_SZ)`という名前のレジストリキーを作成します。値は信頼されたSIDのリストで、複数ある場合はスペースで区切ります。

次の例では、1 つの Controller が VDA 登録 (`ListofDDCs`) に使用されていますが、2 つの Controller がブローカー処理 (List OfSIDs) に使用されています。

登録とブローカー処理に使用される異なる Controller の例(/en-us/citrix-virtual-apps-desktops/2511/media/vda-registration-listofsids.png)

VDA 登録中の Controller 検索

VDAが登録を試みるとき、Broker Agentはまずローカルドメインで DNSルックアップを実行し、指定されたControllerに到達できることを確認します。

その最初のルックアップでControllerが見つからない場合、Broker AgentはADでフォールバックのトップダウンクエリを開始できます。そのクエリはすべてのドメインを検索し、頻繁に繰り返されます。Controllerアドレスが無効な場合（たとえば、管理者がVDAのインストール時に誤ったFQDNを入力した場合）、そのクエリのアクティビティは、ドメインコントローラー上で分散型サービス拒否（DDoS）状態を引き起こす可能性があります。

以下のレジストリキーは、Broker Agentが最初の検索中にControllerを見つけられない場合に、フォールバックのトップダウンクエリを使用するかどうかを制御します。

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`

- 名前: `DisableDdcWildcardNameLookup`
- 種類: `DWORD`
- 値: `0` (デフォルト) または任意のゼロ以外の値

`0`に設定すると、フォールバック検索が有効になります。コントローラーの初期検索が失敗した場合、フォールバックのトップダウン検索が開始されます。これはデフォルトの動作です。ただし、ゼロ以外の値に設定すると、フォールバック検索は無効になります。コントローラーの初期検索が失敗した場合、ブローカーエージェントは検索を停止します。

読み取り専用ドメインコントローラーを使用した VDA 登録中の LDAP バインディングシーケンス

VDAが読み取り専用ドメインコントローラー (RODC) に登録する場合、ブローカーエージェントは無視するLight Directory Access Protocol (LDAP) バインディングを選択する必要があります。この選択を行うには、ブローカーエージェントに適切なレジストリキーが必要です。

レジストリキーが提供されていない場合、またはレジストリキーフィールドが空の場合、元のLDAPバインディングシーケンスを通過する必要があるため、RODCへのVDA登録に時間がかかります。

LDAPバインディングシーケンスを変更するために、レジストリキー`ListofIgnoredBindings`が`HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`に追加されました。`ListofIgnoredBindings`を使用すると、必要に応じてLDAPバインディングシーケンスを変更でき、それによってRODCへのVDA登録を高速化できます。

- 名前: `ListofIgnoredBindings`
- 種類: `REG_SZ`
- 値: `DefaultPath`、`DomainPath`、`PDCPath`

この値は、コンマで区切られたバインディングパスオプションのリストです。レジストリキーは、有効と認識しない値を無視します。

VDA登録の問題のトラブルシューティング

前述のとおり、VDAは、ブローカーセッションの起動時に考慮されるように、Delivery ControllerまたはCloud Connectorに登録されている必要があります。未登録のVDAは、利用可能なリソースの活用不足につながる可能性があります。VDAが登録されない理由はさまざまあり、その多くは管理者がトラブルシューティングできます。Studioは、カタログ作成ウィザードで、およびデリバリーグループの作成後にトラブルシューティング情報を提供します。

- **マシンカタログ作成中の問題の特定:** カタログ作成ウィザードで、既存のマシンを追加した後、コンピューターアカウント名のリストは、各マシンがカタログに追加するのに適しているかどうかを示します。各マシンの横にあるアイコンにカーソルを合わせると、そのマシンに関する情報メッセージが表示されます。

  メッセージが問題のあるマシンを特定した場合、そのマシンを削除する（**削除**ボタンを使用）か、マシンを追加することができます。たとえば、メッセージがマシンに関する情報が取得されなかったことを示している場合（おそらく登録されたことがないため）、とにかくマシンを追加することを選択できます。

  カタログの機能レベルは、カタログ内のマシンで利用できる製品機能を制御します。新しい製品バージョンで導入された機能を使用するには、新しいVDAが必要になる場合があります。機能レベルを設定すると、そのバージョンで導入されたすべての機能（および機能レベルが変更されない場合はそれ以降の機能）がカタログ内のマシンで利用できるようになります。ただし、そのカタログ内の以前のVDAバージョンのマシンは登録できません。
- **デリバリーグループ作成後の問題の特定:** デリバリーグループを作成した後、Studioはそのグループに関連付けられたマシンの詳細を表示します。

  デリバリーグループの詳細ペインには、登録が必要だが登録されていないマシンの数が表示されます。つまり、電源が入っていてメンテナンスモードではないが、現在コントローラーに登録されていないマシンが1台以上存在する可能性があります。「登録されていないが、登録が必要な」マシンを表示している場合は、詳細ペインの**トラブルシューティング**タブで、考えられる原因と推奨される是正措置を確認してください。

VDA登録のトラブルシューティングに関する詳細情報

- 機能レベルの詳細については、「VDAのバージョンと機能レベル」を参照してください。
- VDA登録のトラブルシューティングについて詳しくは、「CTX136668」を参照してください。
- VDA登録とセッション起動のトラブルシューティングには、Citrix Scoutのヘルスチェックも使用できます。詳細については、「ヘルスチェックについて」を参照してください。

仮想IPおよび仮想ループバック

重要:

- Windows 10 Enterprise マルチセッションは、リモートデスクトップIP仮想化（仮想IP）をサポートしていません。また、Windows 10 Enterprise マルチセッションでは、リモートデスクトップIP仮想化または仮想ループバックをサポートしていません。
- リモートデスクトップIP仮想化（仮想IP）は、クラウドホスト型マシンではサポートされていません。 詳しくは、Microsoftのドキュメントを参照してください。

リモートデスクトップIP仮想化および仮想ループバック機能は、Windows Server 2016、Windows Server 2019、およびWindows Server 2022マシンでサポートされています。これらの機能は、WindowsデスクトップOSマシンには適用されません。

Microsoftのリモートデスクトップ IP仮想化アドレス機能は、公開アプリケーションにセッションごとに一意の動的に割り当てられたIPアドレスを提供します。Citrixの仮想ループバック機能を使用すると、localhost（デフォルトでは127.0.0.1）との通信に依存するアプリケーションを、localhost範囲（127.*）内の一意の仮想ループバックアドレスを使用するように構成できます。

CRMやCTI（Computer Telephony Integration）などの特定のアプリケーションは、アドレス指定、ライセンス、識別、または一意のIPアドレスやループバックアドレスを必要とするその他の目的でIPアドレスを使用します。他のアプリケーションは静的ポートにバインドする可能性があり、その場合、マルチユーザー環境でアプリケーションの追加インスタンスを起動しようとすると、ポートが使用中のため失敗します。このようなアプリケーションがCitrix Virtual Apps™環境で正しく機能するには、デバイスごとに一意のIPアドレスが必要です。

Remote Desktop IP Virtualization と仮想ループバックは、互いに独立した機能です。どちらか一方、または両方を使用できます。

管理者の操作の概要:

- MicrosoftのリモートデスクトップIP仮想化を使用するには、Windowsサーバーでそれを有効にして構成します。（Citrix®ポリシー設定は不要です。）
- Citrix仮想ループバックを使用するには、Citrixポリシーで2つの設定を構成します。

リモートデスクトップIP仮想化 (仮想IP)

Windowsサーバーでリモートデスクトップ IP仮想化が有効になり構成されると、セッションで実行されている構成済みの各アプリケーションは、一意のアドレスを持っているように見えます。ユーザーは、他の公開アプリケーションにアクセスするのと同じ方法で、Citrix Virtual Appsサーバー上のこれらのアプリケーションにアクセスします。プロセスがリモートデスクトップIP仮想化を必要とするのは、次のいずれかのケースです。

- プロセスがハードコードされたTCPポート番号を使用している
- プロセスがWindowsソケットを使用しており、一意のIPアドレスまたは指定されたTCPポート番号を必要としている

アプリケーションが Remote Desktop IP Virtualization アドレスを使用する必要があるかどうかを判断するには：

1. Microsoft から **TCPView** ツールを入手します。このツールは、特定の IP アドレスとポートをバインドするすべてのアプリケーションを一覧表示します。TCPView の詳細については、Microsoft ドキュメント を参照してください。
2. **IP アドレスの解決**機能を無効にして、ホスト名ではなくアドレスが表示されるようにします。
3. アプリケーションを起動し、**TCPView** を使用して、アプリケーションが開いている IP アドレスとポート、およびこれらのポートを開いているプロセス名を確認します。
4. サーバーのIPアドレス、0.0.0.0、または127.0.0.1を開くプロセスを構成します。
5. アプリケーションが異なるポートで同じ IP アドレスを開かないようにするには、アプリケーションの別のインスタンスを起動します。

Microsoft Remote Desktop (RD) IP仮想化の仕組み

- Microsoftサーバーで仮想IPアドレス指定を有効にする必要があります。

  たとえば、Windows Server 2016 環境では、サーバーマネージャーから **Remote Desktop Services > RD Session Host Connections** を展開して、RD IP Virtualization 機能を有効にし、セッションごとまたはプログラムごとに動的ホスト構成プロトコル (DHCP) サーバーを使用して IP アドレスを動的に割り当てる設定を構成します。Remote Desktop IP Virtualization の構成の詳細については、Microsoft ドキュメント を参照してください。

- この機能を有効にすると、セッションの開始時に、サーバーはDHCPサーバーから動的に割り当てられたIPアドレスを要求します。
- **RD IP仮想化**機能は、セッションごとまたはプログラムごとにリモートデスクトップ接続にIPアドレスを割り当てます。複数のプログラムにIPアドレスを割り当てる場合、それらはセッションごとのIPアドレスを共有します。
- セッションにアドレスが割り当てられると、以下の呼び出しが行われるたびに、セッションはシステムのプライマリIPアドレスではなく仮想アドレスを使用します: `bind`、`closesocket`、`connect`、`WSAConnect`、`WSAAccept`、`getpeername`、`getsockname`、`sendto`、`WSASendTo`、`WSASocketW`、`gethostbyaddr`、`getnameinfo`、`getaddrinfo`。

リモートデスクトップセッションホスティング構成内でMicrosoft IP仮想化機能を使用する場合、アプリケーションとWinsock関数呼び出しの間に「フィルター」コンポーネントを挿入することで、アプリケーションは特定のIPアドレスにバインドされます。その後、アプリケーションは使用する正しいIPアドレスのみを認識します。アプリケーションがTCPまたはUDP通信をリッスンしようとすると、割り当てられた仮想IPアドレス（またはループバックアドレス）に自動的にバインドされます。アプリケーションによって開かれた発信接続は、アプリケーションにバインドされたIPアドレスから発信されます。

アドレスを返す関数（Windowsポリシーが制御する`GetAddrInfo()`など）で、ローカルホストIPアドレスが要求された場合、リモートデスクトップIP仮想化は返されたIPアドレスを調べ、それをセッションのリモートデスクトップIP仮想化アドレスに変更します。そのような名前関数を介してローカルサーバーのIPアドレスを取得しようとするアプリケーションは、そのセッションに割り当てられた一意のリモートデスクトップIP仮想化アドレスのみを認識します。このIPアドレスは、bindやconnectなどの後続のソケット呼び出しでよく使用されます。Windowsポリシーの詳細については、Windows ServerでのRDS IP仮想化を参照してください。

多くの場合、アプリケーションはアドレス0.0.0.0でリッスンするためにポートへのバインドを要求します。アプリケーションがこれを行い、静的ポートを使用する場合、アプリケーションの複数のインスタンスを起動することはできません。リモートデスクトップIP仮想化アドレス機能は、これらの呼び出しタイプで0.0.0.0も検索します。これは、呼び出しを特定のリモートデスクトップIP仮想化アドレスでリッスンするように変更します。これにより、複数のアプリケーションが同じコンピューター上の同じポートでリッスンできるようになります。これは、それらがすべて異なるアドレスでリッスンしているためです。呼び出しは、ICAセッション内であり、リモートデスクトップIP仮想化アドレス機能が有効になっている場合にのみ変更されます。たとえば、異なるセッションで実行されているアプリケーションの2つのインスタンスが、すべてのインターフェース（0.0.0.0）と特定のポート（9000など）にバインドしようとすると、それらはVIPAddress1:9000とVIPAddress2:9000にバインドされ、競合は発生しません。

仮想ループバック

Citrix Remote Desktop IP Virtualization loopback policy設定を有効にすると、各セッションが通信用に独自のループバックアドレスを持つことができます。アプリケーションがWinsock呼び出しでlocalhostアドレス（デフォルト = 127.0.0.1）を使用する場合、仮想ループバック機能は127.0.0.1を127.X.X.Xに置き換えます。ここで、X.X.Xはセッション ID + 1を表します。たとえば、セッションIDが7の場合、アドレスは127.0.0.8になります。セッションIDが第4オクテット（255を超える）を超過する可能性は低いですが、その場合、アドレスは次のオクテット（127.0.1.0）に繰り上がり、最大127.255.255.255までとなります。

プロセスが仮想ループバックを必要とするのは、次のいずれかのケースです。

- プロセスがWindowsソケットループバック（localhost）アドレス（127.0.0.1）を使用している場合
- プロセスがハードコードされたTCPポート番号を使用している場合

プロセス間通信にループバックアドレスを使用するアプリケーションには、仮想ループバックポリシー設定を使用します。追加の設定は不要です。仮想ループバックは仮想IPに依存しないため、Microsoftサーバーを設定する必要はありません。

- 仮想IPループバックサポート。このポリシー設定を有効にすると、各セッションが独自の仮想ループバックアドレスを持つことができます。この設定はデフォルトで無効になっています。この機能は、仮想IP仮想ループバックプログラムリストポリシー設定で指定されたアプリケーションにのみ適用されます。
- 仮想IP仮想ループバックプログラムリスト。このポリシー設定は、仮想IPループバック機能を使用するアプリケーションを指定します。この設定は、仮想IPループバックサポートポリシー設定が有効になっている場合にのみ適用されます。
- 仮想IPループバックポート除外。アプリケーションがこの設定で指定されたポートでループバックアドレスを呼び出す場合、仮想ループバックは呼び出しをセッション固有のループバックアドレスに変更しません。

関連機能

仮想IPよりも仮想ループバックが優先されるように、以下のレジストリ設定を使用できます。この機能は「優先ループバック」と呼ばれます。ただし、注意して進めてください。

- 優先ループバックは、仮想IPと仮想ループバックの両方が有効になっている場合にのみ使用してください。そうしないと、予期しない結果が生じる可能性があります。
- レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用に

よって生じる問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

アプリケーションが常駐するサーバーでregeditを実行します。

- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP`
- 名前: PreferLoopback, 種類: REG_DWORD, データ: 1
- 名前: PreferLoopbackProcesses, 種類: REG_MULTI_SZ, データ: \<list of processes\>

ゾーン

注：

バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

WANで接続された広範囲に分散した場所にまたがる展開では、ネットワークの遅延と信頼性により課題が生じる可能性があります。これらの課題を軽減する2つのオプションがあります。

- 複数のサイトを展開し、それぞれに独自のSQL Serverサイトデータベースを配置します。

  このオプションは、大規模なエンタープライズ展開に推奨されます。複数のサイトは個別に管理され、それぞれに独自のSQL Serverサイトデータベースが必要です。各サイトは独立したCitrix Virtual Apps™展開です。

- 単一サイト内に複数のゾーンを構成します。

  ゾーンを構成することで、リモート地域のユーザーがWANの大部分を通過することなくリソースに接続できるようになります。ゾーンを使用すると、単一のWeb Studioコンソール、Citrix Director、およびサイトデータベースから効果的なサイト管理が可能になります。これにより、リモートロケーションに個別のデータベースを含むサイトをさらに展開、人員配置、ライセンス供与、運用するコストを節約できます。

  ゾーンは、あらゆる規模の展開で役立ちます。ゾーンを使用して、アプリケーションとデスクトップをエンドユーザーに近づけることで、パフォーマンスを向上させることができます。

ゾーンには、冗長性と回復性のために1つ以上のControllerをローカルにインストールできますが、必須ではありません。

サイトに構成されているControllerの数は、サイト自体に新しいControllerを追加するなどの一部の操作のパフォーマンスに影響を与える可能性があります。これを避けるため、Citrix Virtual AppsまたはCitrix Virtual Desktops™サイトのゾーン数を50以下に制限することをお勧めします。

ゾーンのネットワーク遅延が250ミリ秒RTTを超える場合は、ゾーンではなく複数のサイトを展開することをお勧めします。

この記事全体を通して、「ローカル」という用語は、議論されているゾーンを指します。たとえば、「VDAがローカルControllerに登録する」とは、VDAがVDAが配置されているゾーン内のControllerに登録することを意味します。

このリリースでのゾーンは、XenAppバージョン6.5以前のゾーンと似ていますが、同一ではありません。たとえば、このゾーンの実装では、データコレクターはありません。サイト内のすべてのControllerは、プライマリゾーンの1つのサイトデータベースと通信します。また、このリリースでは、フェールオーバーゾーンと優先ゾーンの動作が異なります。

ゾーンの種類

サイトには常に1つのプライマリゾーンがあります。オプションで、1つ以上のサテライトゾーンを持つこともできます。サテライトゾーンは、災害復旧、地理的に離れたデータセンター、支社、クラウド、またはクラウド内のアベイラビリティゾーンに使用できます。

プライマリゾーン:

プライマリゾーンのデフォルト名は「Primary」です。このゾーンには、SQL Serverサイトデータベース（高可用性SQLサーバーを使用している場合）、Web Studio、Director、Citrix StoreFront™、Citrix License Server、およびCitrix Gatewayが含まれます。サイトデータベースは常にプライマリゾーンに配置してください。

プライマリゾーンには、冗長性のために少なくとも2つのControllerが必要です。プライマリゾーンには、データベースおよびインフラストラクチャと密接に連携するアプリケーションを持つVDAを配置できます。

サテライトゾーン:

サテライトゾーンには、1つ以上のVDA、Controller、StoreFrontサーバー、およびCitrix Gatewayサーバーが含まれます。通常の運用では、サテライトゾーンのControllerはプライマリゾーンのデータベースと直接通信します。

サテライトゾーン、特に大規模なものは、そのゾーンのマシンをプロビジョニングおよび保存するために使用されるハイパーバイザーを含む場合もあります。サテライトゾーンを構成する際、ハイパーバイザーまたはその他のサービス接続を関連付けることができます。（その接続を使用するカタログが同じゾーンにあることを確認してください。）

サイトには、独自のニーズと環境に基づいて、さまざまな構成のサテライトゾーンを含めることができます。次の図は、プライマリゾーンとサテライトゾーンの例を示しています。

プライマリゾーンとサテライトゾーンの図(/en-us/citrix-virtual-apps-desktops/2511/media/zones1.png)

図では次のようになります。

- **プライマリゾーン:** 2つのController、Web Studio、Director、StoreFront、License Server、およびサイトデータベース（高可用性SQL Server展開を含む）が含まれます。プライマリゾーンには、複数のVDAとCitrix Gatewayも含まれます。
- **サテライトゾーン1: Controllerを持つVDA:** サテライトゾーン1には、Controller、VDA、およびStoreFrontサーバーが含まれます。このサテライトゾーンのVDAは、ローカルのControllerに登録されます。ローカルのControllerは、プライマリゾーンのサイトデータベースおよびライセンスサーバーと通信します。

  WANが失敗した場合、ローカルホストキャッシュ機能により、サテライトゾーンのControllerはそのゾーンのVDAへの接続の仲介を継続できます。このような展開は、従業員がローカルのStoreFrontサイトとローカルのControllerを使用してローカルリソースにアクセスするオフィスで効果的です。
- **サテライトゾーン2: 冗長なControllerを持つVDA:** サテライトゾーン2には、2つのController、VDA、およびStoreFrontサーバーが含まれます。これは最も回復力のあるゾーンタイプであり、WANとローカルのControllerの1つが同時に障害を起こした場合でも保護を提供します。

VDAの登録場所とControllerのフェールオーバー場所

プライマリゾーンとサテライトゾーンを含むサイトで、VDAの最小バージョンが7.7の場合：

- Primary zone の VDA は、Primary zone の Controller に登録します。Primary zone の VDA は、Satellite zone の Controller に登録しようとすることはありません。
- Satellite zone の VDA は、可能であればローカルの Controller に登録します。(これは優先 Controller と見なされます。) ローカルの Controller が利用できない場合 (たとえば、VDA 登録をこれ以上受け入れられない、または障害が発生した場合など)、VDA は Primary zone の Controller に登録しようとします。この場合、Satellite zone の Controller が再び利用可能に

なったとしても、VDA は Primary zone に登録されたままになります。Satellite zone の VDA は、別の Satellite zone の Controller に登録しようとすることはありません。

- Controller の VDA 検出で自動更新が有効になっており、VDA のインストール中に Controller アドレスのリストを指定した場合、最初の登録にはそのリストから Controller がランダムに選択されます (Controller がどのゾーンにあるかに関係なく)。その VDA を持つマシンが再起動されると、VDA はローカルゾーンの Controller への登録を優先するようになります。
- Satellite zone の Controller が障害を起こした場合、可能であれば別のローカル Controller にフェールオーバーします。ローカルの Controller が利用できない場合は、Primary zone の Controller にフェールオーバーします。
- Controller をゾーンの内外に移動し、自動更新が有効になっている場合、両方のゾーンの VDA は、どの Controller がローカルで、どの Controller が Primary zone にあるかを示す更新されたリストを受け取ります。これにより、VDA はどの Controller に登録し、接続を受け入れることができるかを知ることができます。
- カタログを別のゾーンに移動すると、そのカタログ内の VDA は、カタログを移動したゾーンの Controller に再登録します。(カタログを別のゾーンに移動するときは、このゾーンと関連するホスト接続があるゾーンが適切に接続されていることを確認してください。帯域幅が制限されている場合や、待機時間が長い場合は、ホスト接続を関連するマシンカタログを含む同じゾーンに移動してください。)

Primary zone のすべての Controller が障害を起こした場合:

- Web Studio はサイトに接続できません。
- Primary zone の VDA への接続はできません。
- Primary zone の Controller が利用可能になるまで、サイトのパフォーマンスが低下します。

VDA バージョン 7.7 より前のサイトの場合:

- Satellite zone の VDA は、ローカルゾーンおよび Primary zone の Controller からの要求を受け入れます。(最小バージョン 7.7 の VDA は、他の Satellite zone の Controller 要求を受け入れることができます。)
- Satellite zone の VDA は、Primary zone またはローカルゾーンの Controller にランダムに登録します。(最小バージョン 7.7 の VDA はローカルゾーンを優先します。)

ゾーンの優先順位

ゾーンの優先順位機能を使用するには、StoreFront 3.7 および Citrix Gateway 11.0-65.x 以降を使用している必要があります。

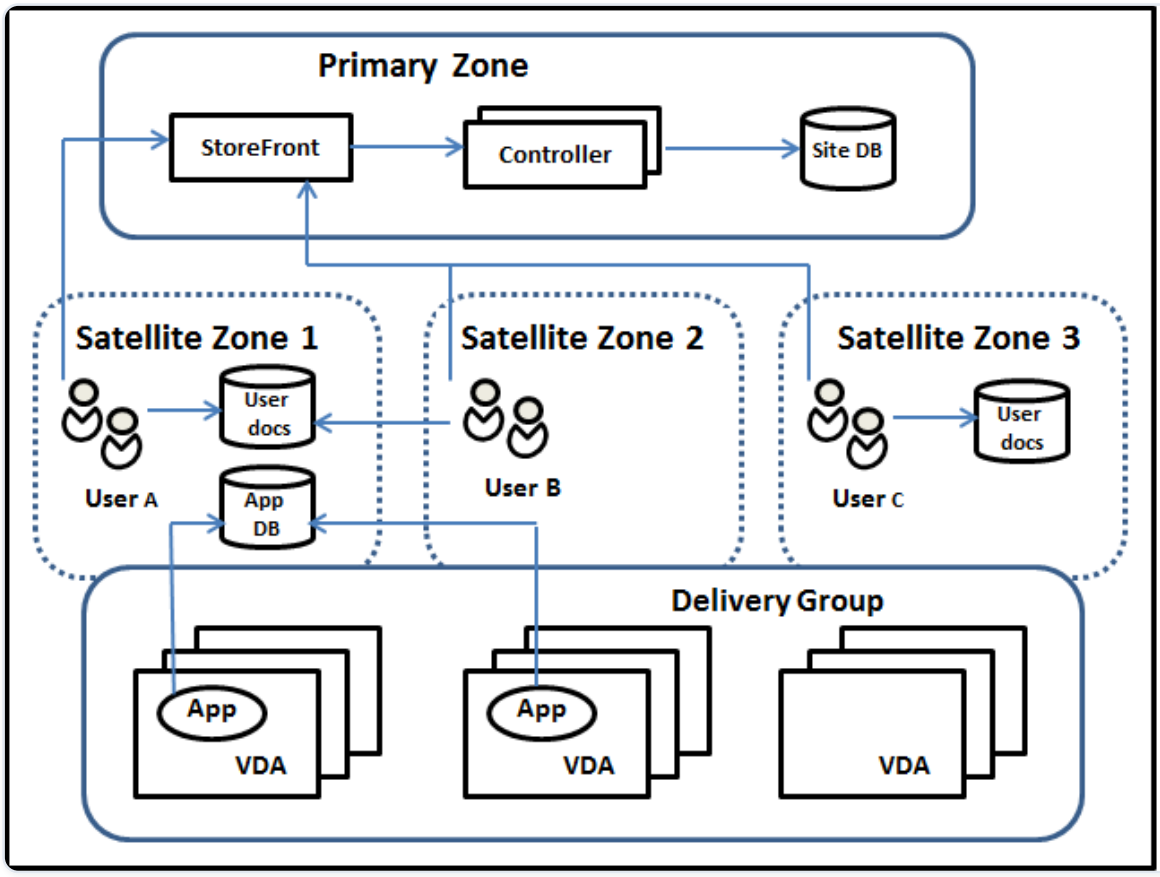
マルチゾーンサイトでは、ゾーン優先機能により、管理者はアプリケーションまたはデスクトップの起動に使用されるVDAをより柔軟に制御できます。

ゾーンの優先順位の仕組み

ゾーンの優先順位には3つの形式があります。特定のゾーンのVDAを使用することを優先する場合があります。その理由は次のとおりです。

- アプリケーションのデータが保存されている場所。これはアプリケーションホームと呼ばれます。
- ユーザーのホームデータ（プロファイルやホーム共有など）の場所。これはユーザーホームと呼ばれます。
- ユーザーの現在の場所（Citrix Workspace™アプリが実行されている場所）。これはユーザーの場所と呼ばれます。

次の図は、マルチゾーン構成の例を示しています。



この例では、VDAは3つのサテライトゾーンに分散していますが、すべて同じデリバリーグループに属しています。そのため、ブローカーはユーザーの起動要求に対してどのVDAを使用するかを選択できる場合があります。この例は、ユーザーがCitrix Workspaceアプリのエンドポイントを実行できる場所がいくつかあることを示しています。

- ユーザーAは、サテライトゾーン1でCitrix Workspaceアプリがインストールされたデバイスを使用しています。
- ユーザーBは、サテライトゾーン2でデバイスを使用しています。
- ユーザーのドキュメントはさまざまな場所に保存できます。
  - ユーザーAとBは、サテライトゾーン1にある共有を使用します。
  - ユーザーCは、サテライトゾーンCの共有を使用します。
  - 公開されているアプリケーションの1つは、サテライトゾーン1にあるデータベースを使用します。

ユーザーまたはアプリケーションにホームゾーンを設定することで、ユーザーまたはアプリケーションをゾーンに関連付けます。その後、Delivery Controller™ のブローカーは、リソースが利用可能な場合、これらの関連付けを使用してセッションが起動されるゾーンの選択を支援します。次のことができます。

- ユーザーをゾーンに追加して、ユーザーのホームゾーンを構成します。
- アプリケーションのプロパティを編集して、アプリケーションのホームゾーンを構成します。

ユーザーまたはアプリケーションは、一度に1つのホームゾーンしか持つことができません。（ユーザーグループのメンバーシップにより複数のゾーンメンバーシップが発生する場合、ユーザーには例外が発生する可能性があります。「その他の考慮事項」セクションを参照してください。ただし、この場合でも、ブローカーは1つのホームゾーンのみを使用します。）

ユーザーおよびアプリケーションのゾーン設定を構成できますが、ブローカーは起動に対して1つの優先ゾーンのみを選択します。優先ゾーンを選択するためのデフォルトの優先順位は、アプリケーションホーム \> ユーザーホーム \> ユーザーロケーションです。この順序を制限できます。詳細については、「ゾーン設定の調整」を参照してください。ユーザーがアプリケーションを起動すると、次のようになります。

- そのアプリケーションに構成済みのゾーン関連付け（アプリケーションホーム）がある場合、優先ゾーンはそのアプリケーションのホームゾーンになります。
- アプリケーションに構成済みのゾーン関連付けがないが、ユーザーに構成済みのゾーン関連付け（ユーザーホーム）がある場合、優先ゾーンはそのユーザーのホームゾーンになります。
- アプリケーションとユーザーのどちらにも構成済みのゾーン関連付けがない場合、優先ゾーンはユーザーがCitrix Workspaceアプリインスタンスを実行しているゾーン（ユーザーロケーション）になります。そのゾーンが定義されていない場合、ランダムなVDAとゾーン選択が使用されます。優先ゾーン内のすべてのVDAに負荷分散が適用されます。優先ゾーンがない場合、Delivery Group内のすべてのVDAに負荷分散が適用されます。

ゾーン設定の調整

ユーザーまたはアプリケーションのホームゾーンを構成（または削除）する際に、ゾーン設定の使用方法をさらに制限することもできます。

- **必須のユーザーホームゾーンの使用:** Delivery Groupでは、ユーザーのホームゾーン（構成されている場合）でセッションを起動するように指定できます。ホームゾーンに利用可能なリソースがない場合でも、他のゾーンへのフェイルオーバーは行われません。この制限は、ゾーン間で大きなプロファイルやデータファイルをコピーするリスクを回避する必要がある場合に役立ちます。つまり、別のゾーンでセッションを起動するよりも、セッションの起動を拒否する方が望ましいということです。
- **必須のアプリケーションホームゾーンの使用:** 同様に、アプリケーションのホームゾーンを構成する際、アプリケーションのホームゾーンにリソースがない場合でも、そのゾーンでのみアプリケーションを起動し、別のゾーンへのフェイルオーバーを行わないように指定できます。
- **アプリケーションホームゾーンなし、および構成済みのユーザーホームゾーンを無視:** アプリケーションのホームゾーンを指定しない場合、そのアプリケーションを起動する際に、構成済みのユーザーゾーンを考慮しないように指定することもできます。たとえば、一部のユーザーが異なるホームゾーンを持っている場合でも、ユーザーロケーションゾーン設定を使用して、ユーザーが自分のデバイスに近いVDAでアプリケーションを実行することを優先する場合があります。

優先ゾーンがセッションの使用に与える影響

ユーザーがアプリケーションまたはデスクトップを起動すると、ブローカーは既存のセッションを使用するよりも優先ゾーンを使用することを優先します。

アプリケーションまたはデスクトップを起動するユーザーが、起動されるリソースに適したセッション（たとえば、アプリケーションのセッション共有を使用できるセッション、または起動されるリソースがすでに実行されているセッション）をすでに持っている場合でも、そのセッションがユーザー/アプリケーションの優先ゾーン以外のゾーンにあるVDAで実行されている場合、システムは新しいセッションを作成する可能性があります。これにより、そのユーザーのセッション要件に対して優先度の低いゾーンのセッションに再接続するよりも、正しいゾーンでの起動が満たされます（利用可能な容量がある場合）。

到達不能になった孤立したセッションを防ぐため、既存の切断されたセッションへの再接続は、たとえそれらが優先されないゾーンにあったとしても許可されます。

起動を満たすためのセッションの望ましさの順序は次のとおりです。

1. 優先ゾーン内の既存のセッションに再接続する。

2. 優先ゾーン以外のゾーンにある既存の切断されたセッションに再接続する。
3. 優先ゾーンで新しいセッションを開始する。
4. 優先ゾーン以外のゾーンにある接続されている既存のセッションに再接続する。
5. 優先ゾーン以外のゾーンで新しいセッションを開始する。

その他のゾーン優先度に関する考慮事項

- ユーザーグループ（セキュリティグループなど）にホームゾーンを構成すると、そのグループのユーザー（直接的または間接的なメンバーシップを通じて）は指定されたゾーンに関連付けられます。ただし、ユーザーは複数のセキュリティグループのメンバーになることができ、その結果、他のグループメンバーシップを通じて異なるホームゾーンが構成される可能性があります。このような場合、そのユーザーのホームゾーンの決定は曖昧になる可能性があります。

ユーザーがグループメンバーシップを通じて取得したものではない構成済みのホームゾーンを持っている場合、そのゾーンがゾーン優先度に使用されます。グループメンバーシップを通じて取得されたゾーン関連付けはすべて無視されます。

ユーザーがグループメンバーシップのみを通じて取得された複数の異なるゾーン関連付けを持っている場合、ブローカーはゾーンの中からランダムに選択します。ブローカーがこの選択を行うと、そのゾーンはユーザーのグループメンバーシップが変更されるまで、その後のセッション起動に使用されます。

- ユーザーロケーションゾーン優先度では、デバイスが接続しているCitrix Gatewayによってエンドポイントデバイス上のCitrix Workspaceアプリが検出される必要があります。Citrix Gatewayは、IPアドレスの範囲を特定のゾーンに関連付けるように構成されている必要があり、検出されたゾーンIDはStoreFrontを介してControllerに渡される必要があります。

ゾーン優先度に関する詳細については、「ゾーン優先度の内部動作」を参照してください。

考慮事項、要件、およびベストプラクティス

- ゾーンには、コントローラー、マシンカタログ、ホスト接続、ユーザー、アプリケーションを配置できます。カタログがホスト接続を使用する場合は、カタログと接続が同じゾーンにあることを確認してください。(ただし、低遅延で高帯域幅の接続が利用できる場合は、異なるゾーンに配置することもできます。)
- サテライトゾーンにアイテムを配置すると、サイトがそれらやそれらに関連する他のオブジェクトとどのようにやり取りするかに影響します。
    - コントローラーがサテライトゾーンに配置されると、それらのマシンは同じゾーン内のハイパーバイザーおよびVDAに対して良好な（ローカル）接続性を持つと想定されます。そ

のサテライトゾーン内のコントローラーは、それらのハイパーバイザーおよびVDAマシンを処理するために、プライマリゾーン内のコントローラーよりも優先的に使用されます。

- ハイパーバイザー接続がサテライトゾーンに配置されると、そのハイパーバイザー接続を介して管理されるすべてのハイパーバイザーもそのサテライトゾーンに存在すると想定されます。そのサテライトゾーン内のコントローラーは、そのハイパーバイザー接続と通信する際に、プライマリゾーン内のコントローラーよりも優先的に使用されます。
- マシンカタログがサテライトゾーンに配置されると、そのカタログ内のすべてのVDAマシンがサテライトゾーンにあると想定されます。各VDAの初回登録後にコントローラーリストの自動更新メカニズムがアクティブになった後、サイトへの登録を試みる際には、プライマリゾーン内のコントローラーよりもローカルコントローラーが優先的に使用されます。
- Citrix Gatewayインスタンスもゾーンに関連付けることができます。これは、ここで説明する他の要素のようにサイト構成の一部としてではなく、StoreFront Optimal HDX™ Routing構成の一部として行われます。Citrix Gatewayがゾーンに関連付けられている場合、そのゾーン内のVDAマシンへのHDX接続が使用されるときに優先的に使用されます。

- 実稼働サイトを作成し、最初のカタログとデリバリーグループを作成すると、すべてのアイテムはプライマリゾーンに配置されます。この初期設定が完了するまで、サテライトゾーンを作成することはできません。(空のサイトを作成した場合、プライマリゾーンには最初はコントローラーのみが含まれます。カタログとデリバリーグループを作成する前または後にサテライトゾーンを作成できます。)
- 1つ以上のアイテムを含む最初のサテライトゾーンを作成すると、サイト内の他のすべてのアイテムはプライマリゾーンに残ります。
- プライマリゾーンはデフォルトで「Primary」という名前ですが、この名前は変更できます。Web Studioはどのゾーンがプライマリゾーンであるかを示しますが、プライマリゾーンには識別しやすい名前を使用するのがベストプラクティスです。プライマリゾーンを再割り当て（つまり、別のゾーンをプライマリゾーンにする）できますが、常にサイトデータベースと高可用性サーバーが含まれている必要があります。
- サイトデータベースは常にプライマリゾーンに保持してください。
- ゾーンを作成した後、後でアイテムをあるゾーンから別のゾーンに移動できます。この柔軟性により、近接して最も効果的に機能するアイテムを分離できる可能性があります。たとえば、カタログ内のマシンを作成する接続（ホスト）とは異なるゾーンにカタログを移動すると、パフォーマンスに影響を与える可能性があります。ゾーン間でアイテムを移動する前に、予期しない潜在的な影響を考慮してください。カタログとそれが使用するホスト接続は同じゾーンに、または適切に接続されたゾーン（たとえば、低遅延で高帯域幅のネットワークを介して）に保持してください。

- 最適なパフォーマンスを得るには、Web StudioとDirectorはプライマリゾーンにのみインストールしてください。Web StudioとDirectorはWebアプリケーションであるため、サテライトゾーン（たとえば、プライマリゾーンがアクセス不能になった場合のフェイルオーバーとして使用するコントローラーを含むサテライトゾーン）からアクセスできます。
- 理想的には、サテライトゾーンのCitrix Gatewayは、他のゾーンまたは外部の場所からそのゾーンに入ってくるユーザー接続に使用されますが、ゾーン内の接続にも使用できます。
- 注意：ゾーン優先機能を使用するには、StoreFront 3.7およびCitrix Gateway 11.0-65.x以降を使用している必要があります。

接続品質の制限

サテライトゾーンのControllerは、サイトデータベースと直接SQLインタラクションを実行します。これにより、サテライトゾーンとサイトデータベースを含むプライマリゾーン間のリンク品質にいくつかの制限が課されます。具体的な制限は、サテライトゾーンに展開されているVDAの数と、それらのVDA上のユーザーセッションの数に比例します。したがって、VDAとセッションが少ないサテライトゾーンは、VDAとセッションが多いサテライトゾーンよりも、データベースへの接続品質が低い状態でも機能できます。

詳細については、「Latency and SQL Blocking Query Improvements」を参照してください。

ブローカーパフォーマンスに対する待機時間の影響

ゾーンによってユーザーは待機時間の長いリンクを使用できますが、ローカルブローカーが存在する場合でも、追加の待機時間はエンドユーザーエクスペリエンスに必然的に影響を与えます。ユーザーが行うほとんどの作業において、サテライトゾーンのControllerとサイトデータベース間のラウンドトリップによって引き起こされる遅延が発生します。

アプリケーションを起動する場合、セッションブローカープロセスがセッション起動要求を送信するのに適したVDAを特定する際に、追加の遅延が発生します。

ゾーンの作成と管理

フル管理者であれば、すべてのゾーン作成および管理タスクを実行できます。ただし、ゾーンの作成、編集、削除を許可するカスタムロールを作成することもできます。ゾーン間でアイテムを移動する場合、ゾーン関連の権限（ゾーン読み取り権限を除く）は必要ありませんが、移動するアイテムに対する編集権限が必要です。たとえば、カタログをあるゾーンから別のゾーンに移動するには、そのカタログに対する編集権限が必要です。詳細については、「委任管理」を参照してください。

Citrix Provisioning™を使用する場合： Citrix Provisioningコンソールはゾーンを認識しないため、サテライトゾーンのカタログを作成するにはWeb Studioを使用することをお勧めします。

Web Studioでカタログを作成し、正しいサテライトゾーンを指定します。その後、Citrix Provisioningコンソールを使用して、そのカタログ内のマシンをプロビジョニングします。（Citrix Provisioningウィザードを使用してカタログを作成した場合、カタログはプライマリゾーンに配置されます。後でWeb Studioを使用してサテライトゾーンに移動する必要があります。）

ゾーンの作成

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. アクションバーで を選択します。
4. ゾーンの名前と説明（オプション）を入力します。名前はサイト内で一意である必要があります。
5. 新しいゾーンに配置するアイテムを選択します。選択可能なアイテムのリストをフィルター処理したり、検索したりできます。空のゾーンを作成することもできます。その場合は、どのアイテムも選択しないでください。
6. 「**保存**」をクリックします。

この方法の代わりに、Web Studioで1つ以上の項目を選択し、アクションバーで**ゾーンの作成**を選択することもできます。

ゾーン名または説明の変更

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. 中央のペインでゾーンを選択し、アクションバーで**ゾーンの編集**を選択します。
4. ゾーン名、説明、またはその両方を変更します。プライマリゾーンの名前を変更する場合は、そのゾーンがプライマリゾーンとして容易に識別できることを確認してください。
5. または をクリックします。

ゾーン間でアイテムを移動する

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. 中央ペインでゾーンを選択し、1つ以上の項目を選択します。
4. アイテムを移動先のゾーンにドラッグするか、アクションバーで を選択し、移動先のゾーンを指定します。

確認メッセージには、選択したアイテムが一覧表示され、それらすべてを移動してもよろしいかどうかが尋ねられます。

注意: カタログがハイパーバイザーまたはその他のサービスへのホスト接続を使用する場合、カタログと接続の両方を同じゾーンに配置してください。そうしないと、パフォーマンスに影響が出る可能性があります。一方を移動する場合は、もう一方も移動してください。

ゾーンを削除する

ゾーンは、削除する前に空である必要があります。プライマリゾーンは削除できません。

1. Web Studio にサインインします。
2. 左側のペインで を選択します。
3. 中央のペインでゾーンを選択します。
4. アクションバーから を選択します。ゾーンが空でない場合（アイテムが含まれている場合）、それらのアイテムを移動するゾーンを選択するよう求められます。
5. 削除を確認します。

ユーザーのホームゾーンを追加する

ユーザーのホームゾーンを構成することは、*ユーザーをゾーンに追加する*とも呼ばれます。

1. Web Studio にサインインします。
2. 左側のペインで を選択し、中央のペインでゾーンを選択します。
3. アクションバーで を選択します。
4. ダイアログボックスで、 をクリックし、ゾーンに追加するユーザーとユーザーグループを選択します。すでにホームゾーンを持つユーザーを指定した場合、メッセージが表示され、2つの選択肢が提示されます: = ホームゾーンを持たない指定したユーザーのみを追加します。 = ユーザー選択ダイアログに戻ります。
5. をクリックします。

ホームゾーンが構成されているユーザーの場合、セッションをそのホームゾーンからのみ起動するように要求できます。

1. デリバリーグループを作成または編集します。
2. 「**ユーザー**」ページで、「**セッションをユーザーのホームゾーンで起動するよう要求する（構成されている場合）**」チェックボックスをオンにします。

そのデリバリーグループのユーザーが起動するすべてのセッションは、そのユーザーのホームゾーン内のマシンから起動する必要があります。デリバリーグループ内のユーザーにホームゾーンが構成されていない場合、この設定は無効です。

ユーザーのホームゾーンを削除する

この手順は、ゾーンからユーザーを削除することとも呼ばれます。

1. Web Studioにサインインします。
2. 左ペインで**ゾーン**を選択し、中央ペインでゾーンを選択します。
3. アクションバーで**ゾーンからユーザーを削除**を選択します。
4. 「**ゾーンにユーザーを追加**」ダイアログボックスで、**削除**をクリックし、ゾーンから削除するユーザーとグループを選択します。この操作では、ユーザーはゾーンからのみ削除されます。それらのユーザーは、所属するデリバリーグループおよびアプリケーショングループに残ります。
5. プロンプトが表示されたら削除を確定します。

アプリケーションのホームゾーンを管理する

アプリケーションのホームゾーンを構成することは、アプリケーションをゾーンに追加することとも呼ばれます。デフォルトでは、マルチゾーン環境では、アプリケーションにホームゾーンはありません。

アプリケーションのホームゾーンは、アプリケーションのプロパティで指定されます。アプリケーションのプロパティは、アプリケーションをグループに追加するとき、または後で構成できます。

- デリバリーグループを作成する、アプリケーショングループを作成する、または既存のグループにアプリケーションを追加するときに、ウィザードの「**アプリケーション**」ページで**プロパティ**を選択します。
- アプリケーションの追加後にアプリケーションのプロパティを変更するには、左ペインで**アプリケーション**を選択します。アプリケーションを選択し、アクションバーで**アプリケーションプロパティの編集**を選択します。

アプリケーションのプロパティ/設定の ページで、次の操作を行います。

- アプリケーションにホームゾーンを設定する場合：
  - **選択したゾーンを使用して決定する**ラジオボタンを選択し、ゾーンを選択します。
  - アプリケーションを（他のゾーンからではなく）選択したゾーンからのみ起動する場合は、ゾーン選択の下にあるチェックボックスをオンにします。

- アプリケーションにホームゾーンを設定しない場合：
  - **ホームゾーンを構成しない**ラジオボタンを選択します。
  - このアプリケーションを起動する際に、ブローカーが構成済みのユーザーゾーンを考慮しないようにする場合は、ラジオボタンの下にあるチェックボックスをオンにします。この場合、アプリケーションまたはユーザーのホームゾーンのいずれも、このアプリケーションを起動する場所を決定するために使用されません。

ゾーンの指定を含むその他のアクション

少なくとも1つのサテライトゾーンを作成した後、ホスト接続を追加するか、カタログを作成する際にゾーンを指定できます。

通常、プライマリゾーンがデフォルトです。Machine Creation Services™を使用してカタログを作成する場合、ホスト接続用に構成されたゾーンが自動的に選択されます。

サイトにサテライトゾーンが含まれていない場合、プライマリゾーンが想定され、ゾーン選択ボックスは表示されません。

キャッシュからブローカーユーザーを削除する

管理者がキャッシュからブローカーユーザーを削除できない場合や、`Get-BrokerUser` の実行時にユーザーが AD から誤った SID を表示する場合があります。

これは、ユーザーが AD から削除され再作成されたにもかかわらず、ブローカーキャッシュに以前のユーザー SID が残っている場合に発生します。

これを解決するには、次の手順を実行します。

1. Active Directory からユーザーを削除します。
2. 削除された各アカウントに対して `Get-BrokerUser` を実行します。どこからも参照されていないアカウントは、結果を返しません。参照されているユーザーの場合、`Get-BrokerUser` の実行後に値が返されます。次に、ユーザーが割り当てられているリソースを特定し、それらのリソースからユーザーを手動で削除する必要があります。

   例:

   - ユーザーがアプリケーションに割り当てられているかを確認します: `Get-BrokerApplication`
   - ユーザーがアプリケーショングループに割り当てられているかを確認します: `Get-BrokerApplicationGroup`

- ユーザーがアクセスポリシーに割り当てられているかを確認します: `Get-BrokerAccessPolicyRule`
- ユーザーがアプリケーションエンタイトルメントポリシーに割り当てられているかを確認します: `Get-BrokerAppEntitlementPolicyRule`
- ユーザーがデスクトップエンタイトルメントポリシーに割り当てられているかを確認します: `Get-BrokerEntitlementPolicyRule`
- ユーザーがデスクトップグループセッションリンガーに割り当てられているかを確認します: `Get-BrokerSessionLinger`
- ユーザーが VDA でセッションを実行しているかを確認します: `Get-BrokerSession`
- ユーザーが結合されたグループのリソースに割り当てられているかを確認します: `Get-BrokerMergedResource`
- ユーザーがリソースグループに割り当てられているかを確認します: `Get-BrokerMergeGroup`
- ユーザーのコマンドがキューに入っているかを確認します: `Get-BrokerMachineCommand`
- ユーザーがプライベートデスクトップに割り当てられているかを確認します: `Get-BrokerMachineV2`
- ユーザーがゾーン設定に割り当てられているかを確認します: `Get-BrokerUserZonePreference`

3. リソースからユーザーを手動で削除します。
4. ユーザーがすべてのリソースから削除されたことを確認するために、`Get-BrokerUser` コマンドを実行します。
5. ユーザーがすべてのリソースから削除されたら、以下を実行してキャッシュからユーザーを削除します。

```
Update-BrokerNameCache -Users -Purge -UnusedFor 0
```

Citrix Virtual Desktop Assistantアプリケーション

Citrix Virtual Desktop Assistantアプリは、エンドユーザーがCPU、メモリ、ネットワーク、HDX™、その他のパフォーマンス要因全体でセッションを最適化できるように設計されたGUIツールです。シンプルで便利なエクスペリエンスを提供し、多くの場合、ワンクリックでセッションパフォーマンスを大幅に向上させたり、トラブルシューティングを行ったりできます。

現在、セッションは次の領域で最適化できます。

- システムリソース：CPUとメモリの最適化。
- ネットワーク：ネットワークステータスの確認とパーソナライズされた推奨事項。
- アプリケーション：応答しないアプリケーションの表示と終了オプション。
- ストレージ：一時ファイルをクリーンアップし、100 MBを超えるファイルをユーザーインターフェイスから直接削除するために特定します。
- ハードウェアの診断とトラブルシューティング：
  - オーディオの診断とトラブルシューティング。
  - カメラデバイスのテスト。
  - キーボード診断
  - USB診断

インストールと実行

ワークステーションVDAの場合： Citrix Virtual Desktop Assistantアプリはデフォルトでダウンロードされ、最小限の操作モードで実行されます。インストール後、VDAを再起動して、システムトレイにCitrix Virtual Desktop Assistantアプリのアイコンを表示します。次に、システムトレイのCitrix Virtual Desktop Assistantアプリのアイコンをクリックして、グラフィカルユーザーインターフェイス（GUI）を起動します。

Citrix Virtual Desktop Assistant Studioポリシー設定を通じてアプリケーションを無効にできます。無効にすると、アイコンがシステムトレイから削除され、ユーザーはアプリケーションを起動できなくなります。これを行うには：

1. Studioから、**ポリシー**に移動します。
2. Assistantアプリを右クリックし、**設定の編集**を選択して**無効**をクリックします。

サーバーVDAの場合: Citrix Virtual Desktop Assistantアプリは、Citrix Virtual Apps and Desktops ISOファイルに含まれています。インストールするには、ISOをダウンロードし、**Support > CitrixAssistantApp folder**に移動します。このフォルダーを開き、`CitrixAssistant.exe`を実行して、画面の指示に従ってインストールを完了します。

ログファイル

Citrix Virtual Desktop Assistantアプリのログファイルは`USERPROFILE%\AppData\Local\Temp\citrix\AssistantApp\ctxasst.log`に保存されます。トラブルシューティングにはログファイルを使用してください。

これらのログを手動で添付し、`CitrixVDAssistantFeedback@citrix.com`にメールで送信していただくことで、Citrix Virtual Desktop Assistantアプリケーションの改善にご協力いただけます。

UIを探索する

アプリはオペレーティングシステムの言語バリアントを自動的に検出し、その言語でアプリを表示します。

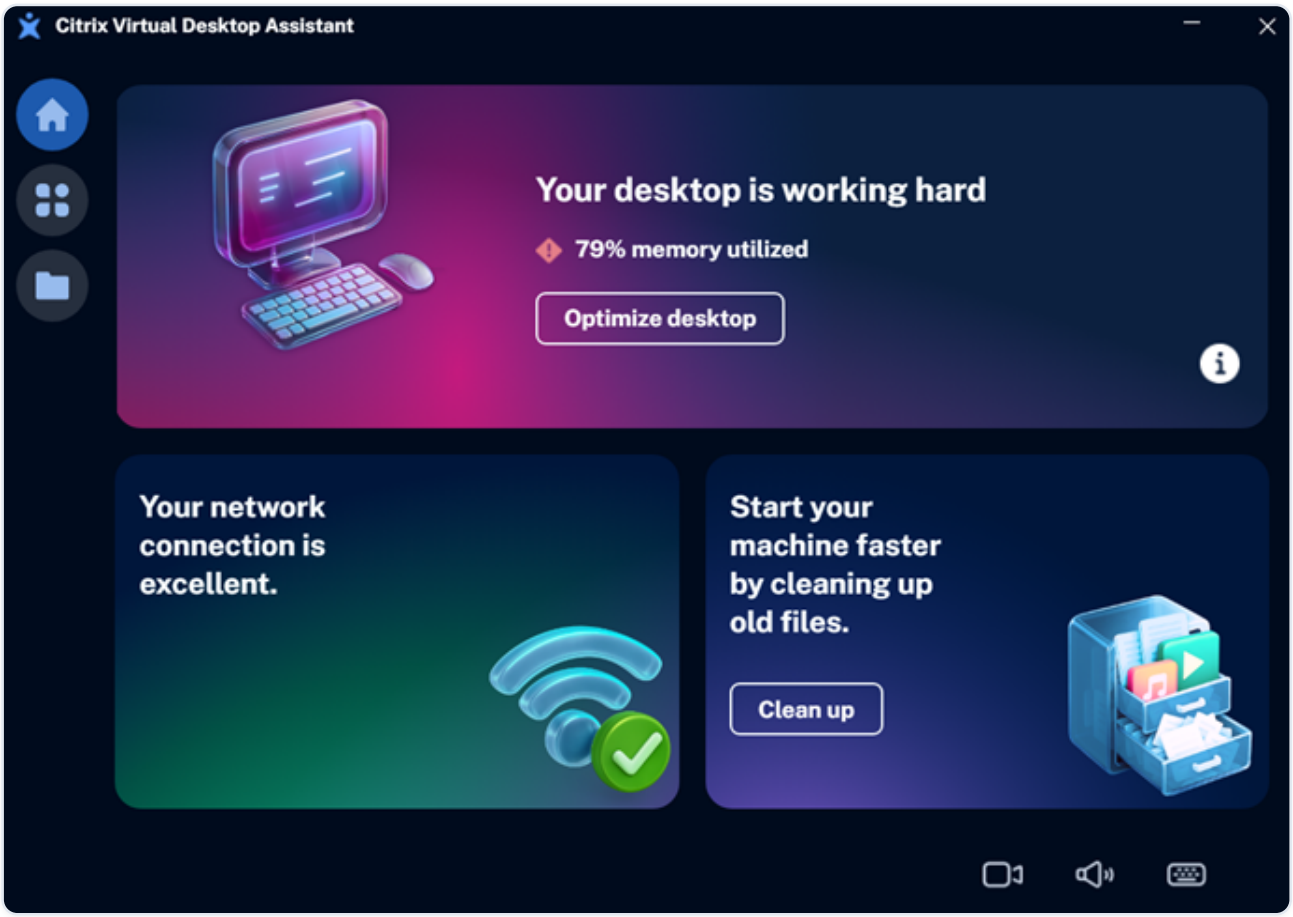
アプリには、左ペインからアクセスできる3つの主要なページがあります。

- ホーム
- アプリ
- ファイル

カメラ、サウンド、キーボード、USBの設定は、右下隅で利用できます。

ホーム

ホームページでは、次の機能が提供されます。



- *デスクトップの最適化*: 最適化機能は、CPU使用率が高い期間にリソースを大量に消費するアプリケーションのCPU優先度を調整することで、システム全体のパフォーマンスを向上させま

す。また、非アクティブなアプリケーションからメモリを解放し、システムリソースを効率的に使用できるようにします。**デスクトップの最適化**をクリックすると、システムパフォーマンスの向上と、メモリ解放によって最適化されたアプリケーションに気づくかもしれません。

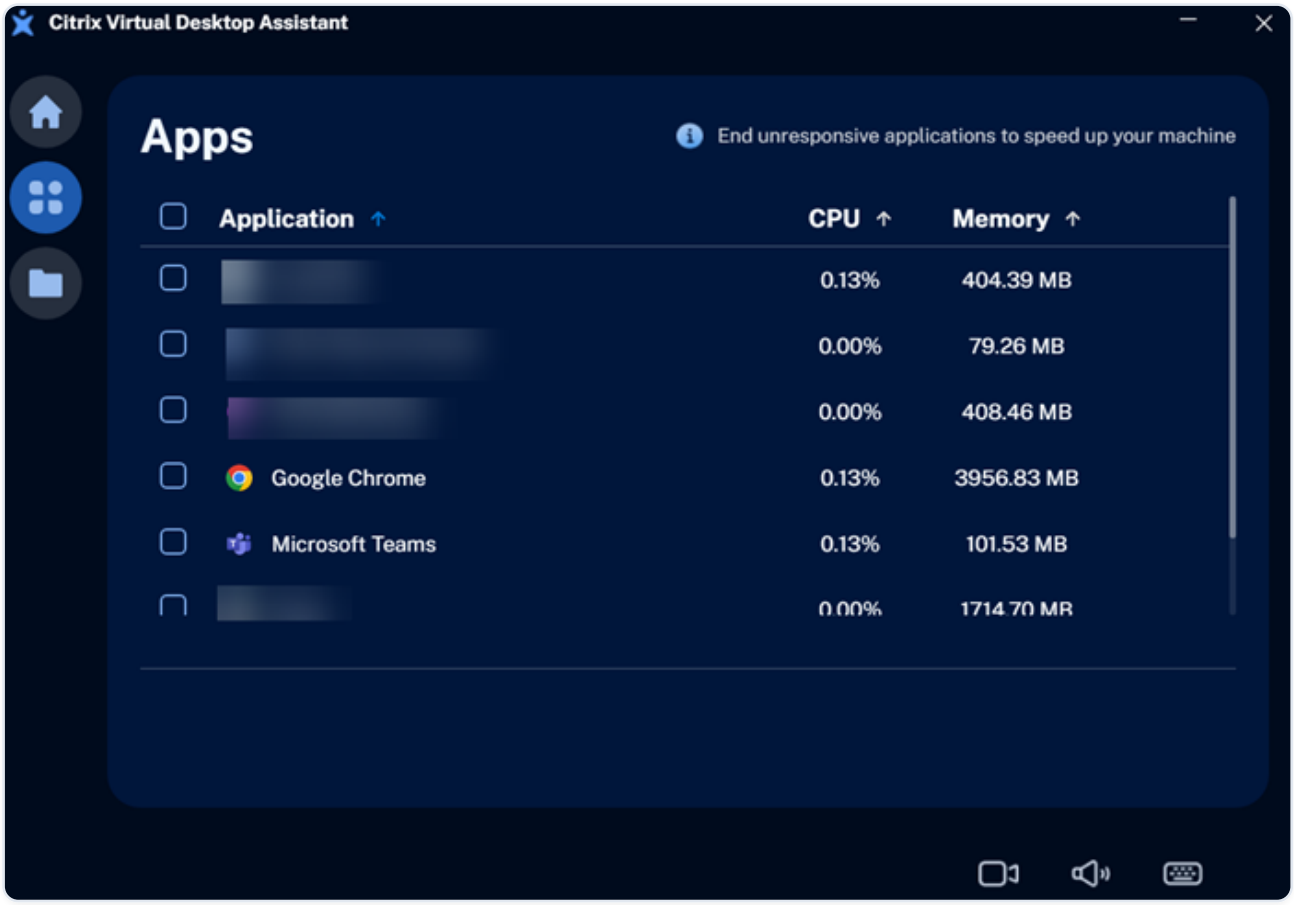
- *ネットワークステータス*: このタイルには、VDAネットワーク接続ステータスが表示されます。帯域幅と遅延データに基づいて、ネットワーク接続結果が表示されます。接続ステータスは、良好、普通、または不良に分類されます。ステータスが普通または不良の場合、**どうすればよいですか？**をクリックすると、改善のための推奨事項が提供されます。

  > **注:**
  >
  > 接続が不良の場合、ファイルをクリーンアップするオプションは利用できません。

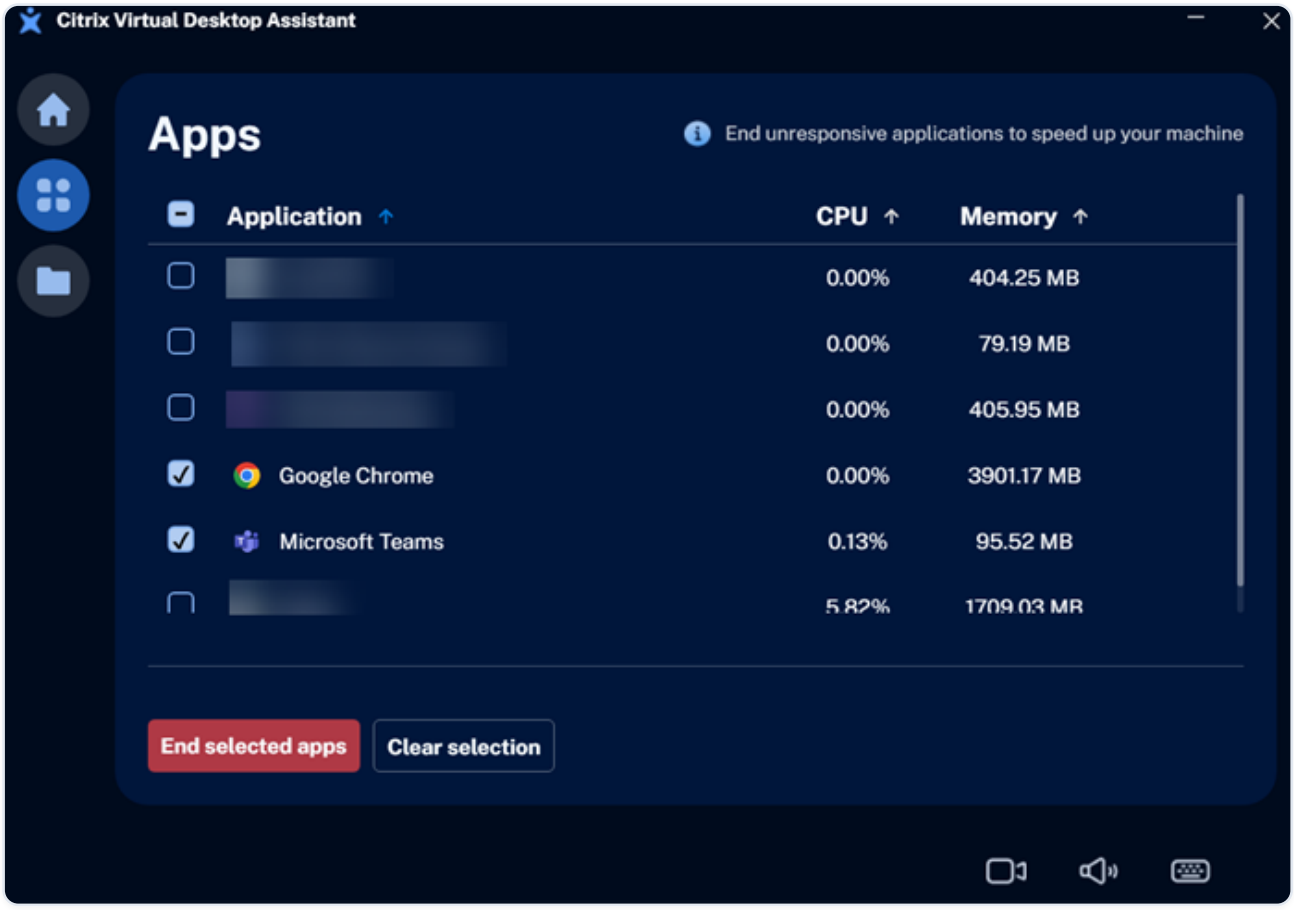
- *クリーンアップ*: このオプションは、ユーザープロファイルに関する情報を提供し、一時ファイルや大きなファイル（100 MBを超えるファイル）のクリーンアップに役立ちます。この操作により、マシンのログオン時間を大幅に改善できます。一時ファイルには、クラッシュダンプレポート、アプリケーションキャッシュ、および肥大化したプロファイルの原因となる隠しファイルが含まれます。左ペインのファイルページにアクセスして、ファイルをクリーンアップすることもできます。詳細については、ファイルページを参照してください。

アプリページ

「**アプリ**」ページには、VDAセッション内の応答しないすべてのアプリケーションと、それらを終了するオプションが表示されます。このインターフェイスから、単一または複数のアプリケーションを終了できます。

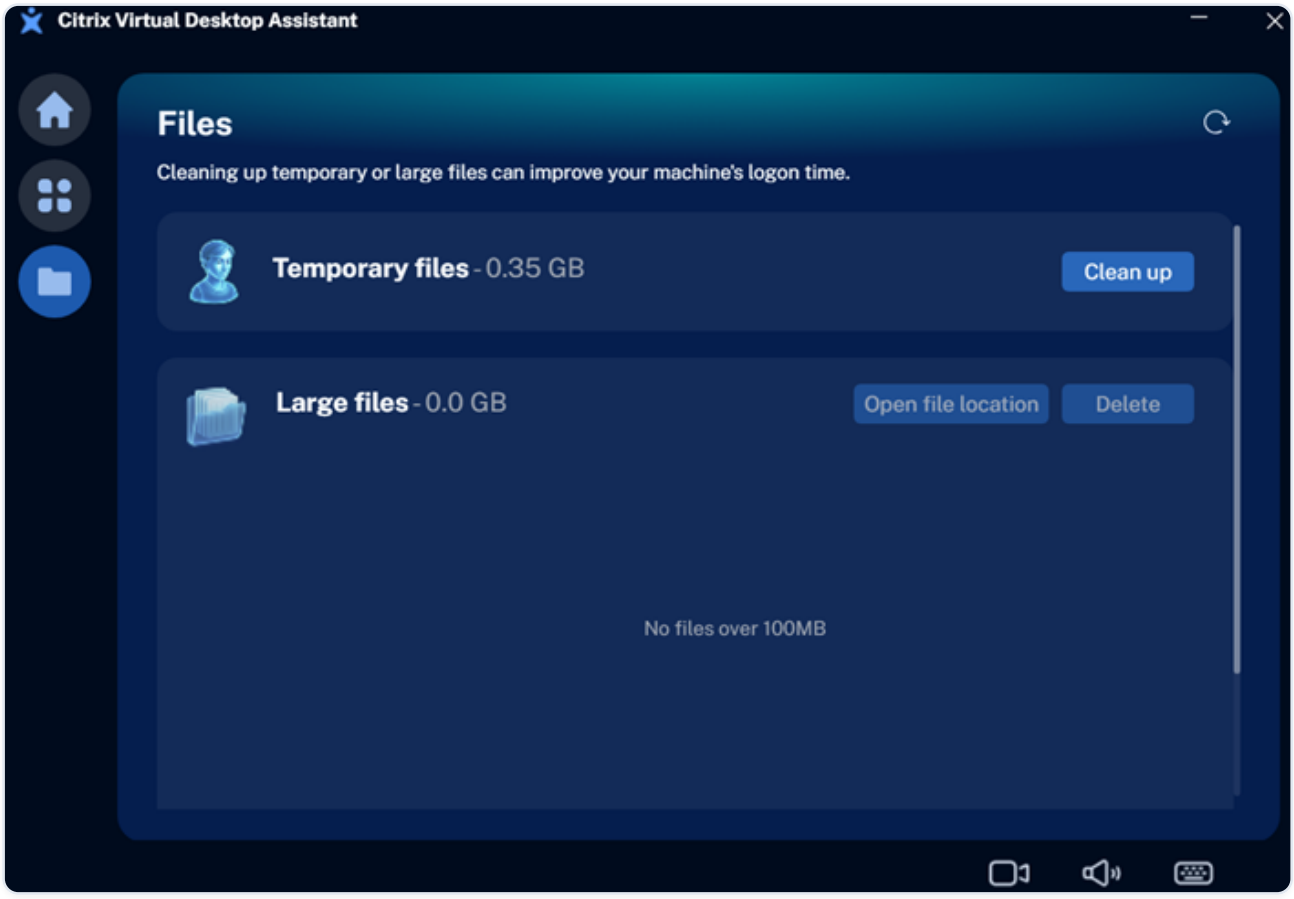


- 単一のアプリを終了する: アプリの行にカーソルを合わせると ボタンが表示されるか、チェックボックスを選択して をクリックします。プロンプトが表示されたら、操作を確定します。
- 複数のアプリを終了する: 複数のアプリケーションを一度に選択し、 をクリックします。プロンプトが表示されたら、操作を確定します。



ファイルページ

ファイルページには、ユーザープロファイルに関する情報が表示され、一時ファイルや大きなファイル（100 MBを超えるファイル）のクリーンアップに役立ちます。この操作により、マシンのログオン時間を大幅に改善できます。一時ファイルには、クラッシュダンプレポート、アプリケーションキャッシュ、および肥大化したプロファイルの原因となる隠しファイルが含まれます。



- 一時ファイル: **クリーンアップ**をクリックして一時ファイルをクリーンアップします。
- 大容量ファイル: **削除**をクリックして大容量ファイルを削除するか、**ファイルの場所を開く**をクリックしてその場所に移動し、適切なアクションを決定できます。**Ctrl**キーを使用して、複数のファイルを同時に選択できます。
- ダウンロードとごみ箱フォルダー: **開く**をクリックしてその場所に移動し、適切なアクションを決定します。

ファイルページでデータを再計算するには、アプリの右上隅にある**更新**アイコンをクリックします。

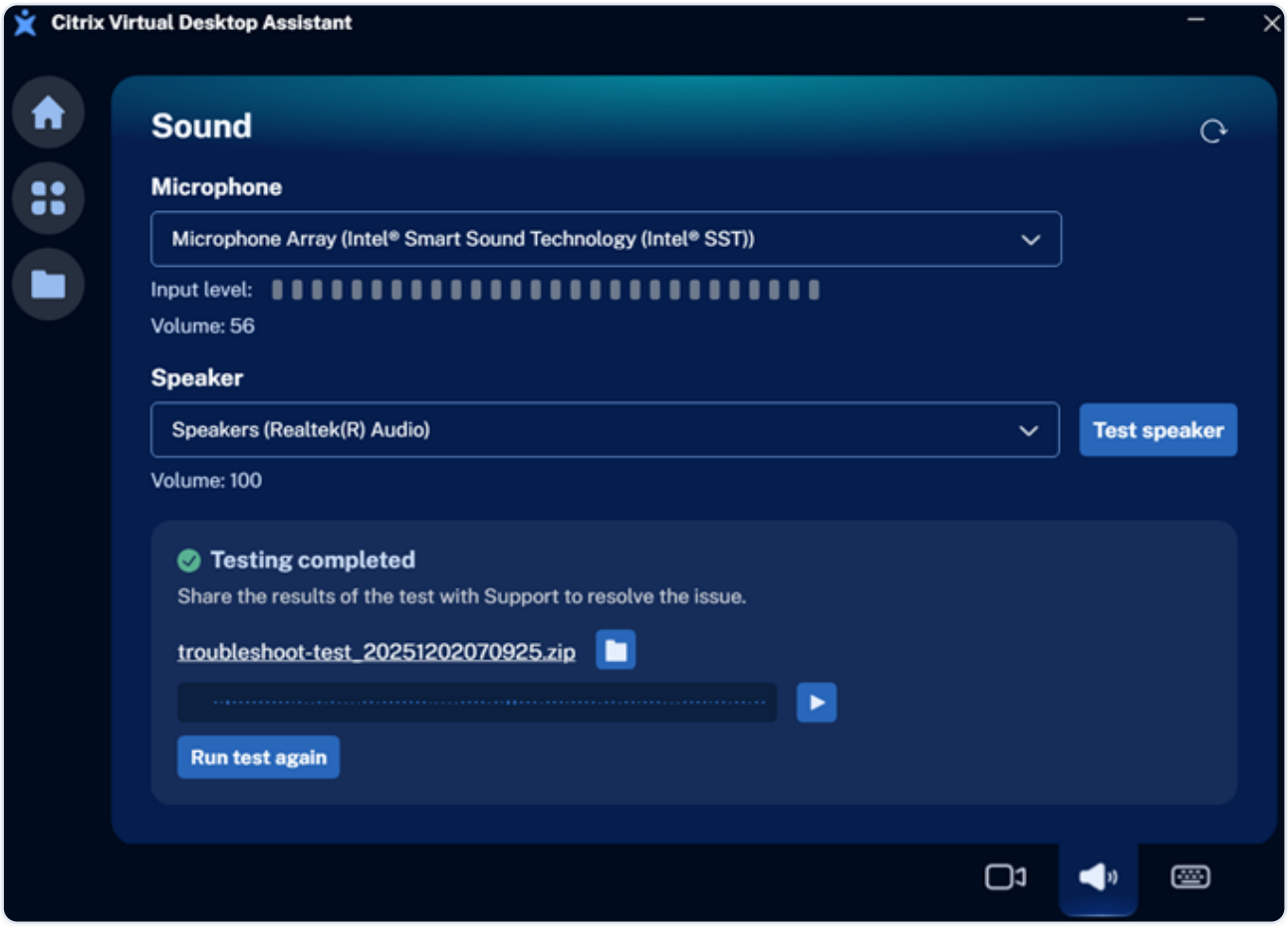
サウンドページ

Citrix Virtual Desktop Assistantアプリのサウンドページは、VDAセッション内のオーディオ設定の診断とトラブルシューティングに役立ちます。

Citrix Assistantアプリのサウンドページ(/en-us/citrix-virtual-apps-desktops/2511/media/new-assistant-sounds-page.png)

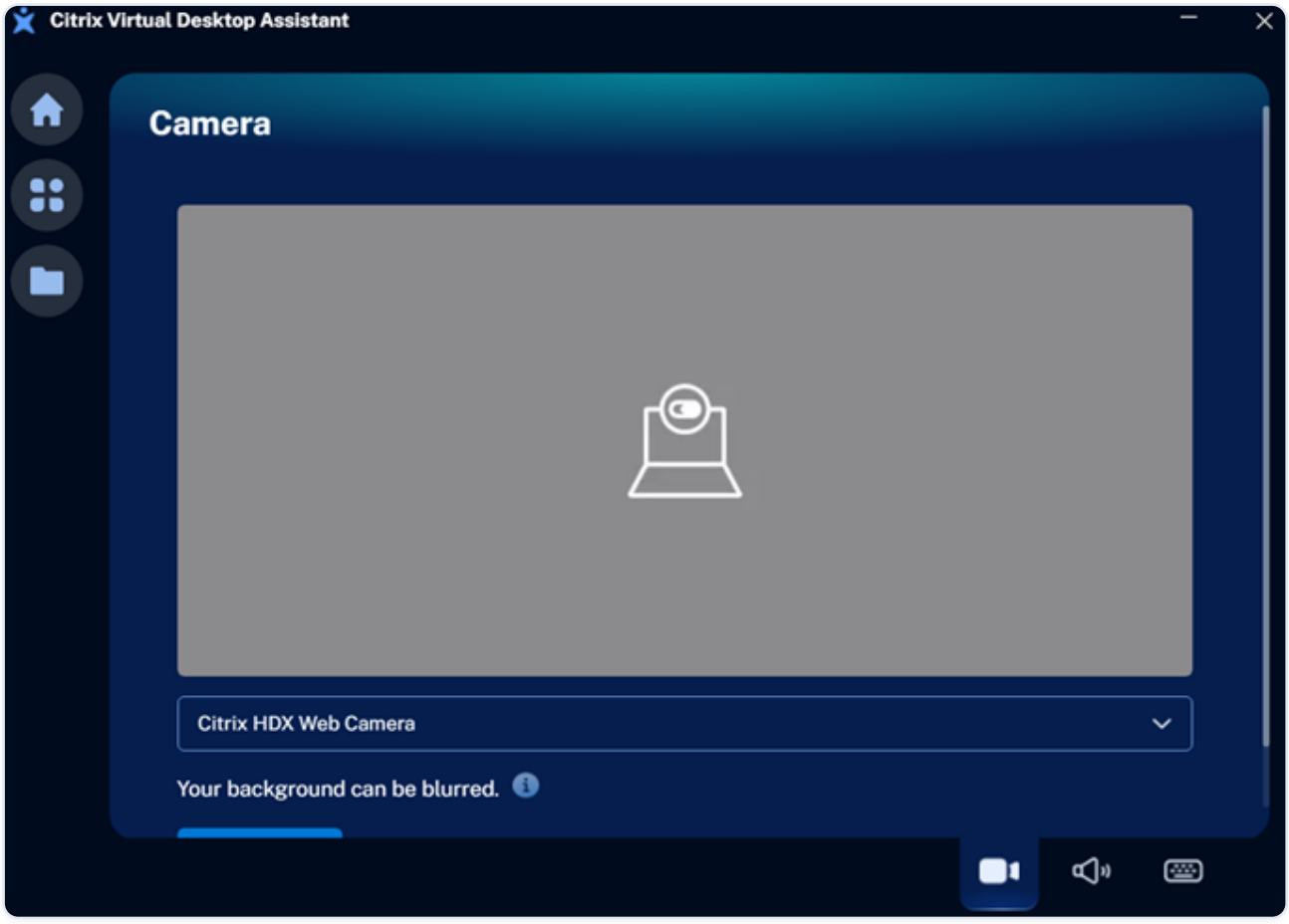
- 複数のオーディオデバイスが接続されている場合は、ドロップダウンリストからマイクとスピーカーを選択できます。

- デモオーディオを再生して選択したスピーカーデバイスをテストするには、**スピーカーのテスト**をクリックします。
- VDAセッション内でオーディオデバイスの問題をトラブルシューティングする場合、**テストの実行**をクリックすると、アプリケーションがサウンド入力を記録します。この記録はzipファイルにエクスポートされます。このzipファイルをITまたはCitrix管理者チームと共有してサポートを受けることができます。また、オーディオを再生してサウンドの再生を確認することもできます。



カメラページ

Citrix Virtual Desktop Assistant アプリのカメラページは、VDAセッション内のビデオ設定を構成するのに役立ちます。



- 複数のカメラが接続されている場合は、ドロップダウンリストからカメラを選択できます。

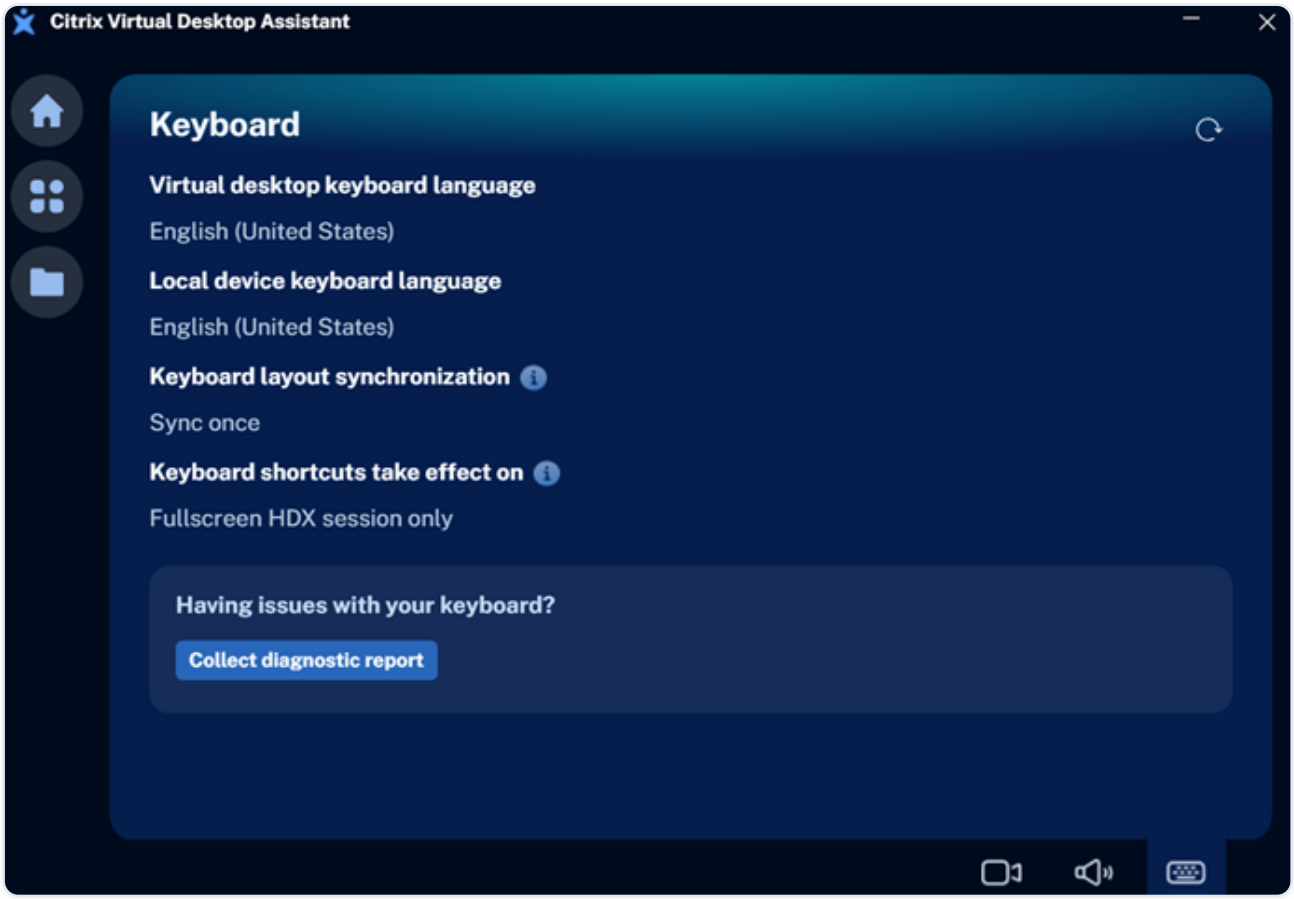
> **注：**
>
> CWAクライアントに複数のカメラデバイスが接続されているにもかかわらず、**Citrix HDX Web Camera**のみが表示される場合は、VDAマシンを再起動して、接続されているすべてのカメラデバイスのリストを確認してください。再起動は、Citrix Virtual Desktop Assistantアプリをインストールした後に行ってください。

- 背景をぼかすことができます。背景をぼかすには、**Citrix Workspace™アプリ > 環境設定 > デフォルトのWebカメラ > 背景のぼかしを有効にする**に移動します。
- カメラ設定を調整するには、**カメラを再試行**をクリックします。ただし、カメラが他のビデオ会議ツールで使用されていないことを確認してください。

キーボードページ

「**キーボード**」ページには、クライアントキーボード、VDAキーボード、同期設定、およびキーボードショートカット設定が1つのビューに表示されます。これらの設定は、Citrix Workspaceアプリ (CWA) の環境設定ツールバーから更新でき、変更はAssistantアプリに反映されます。

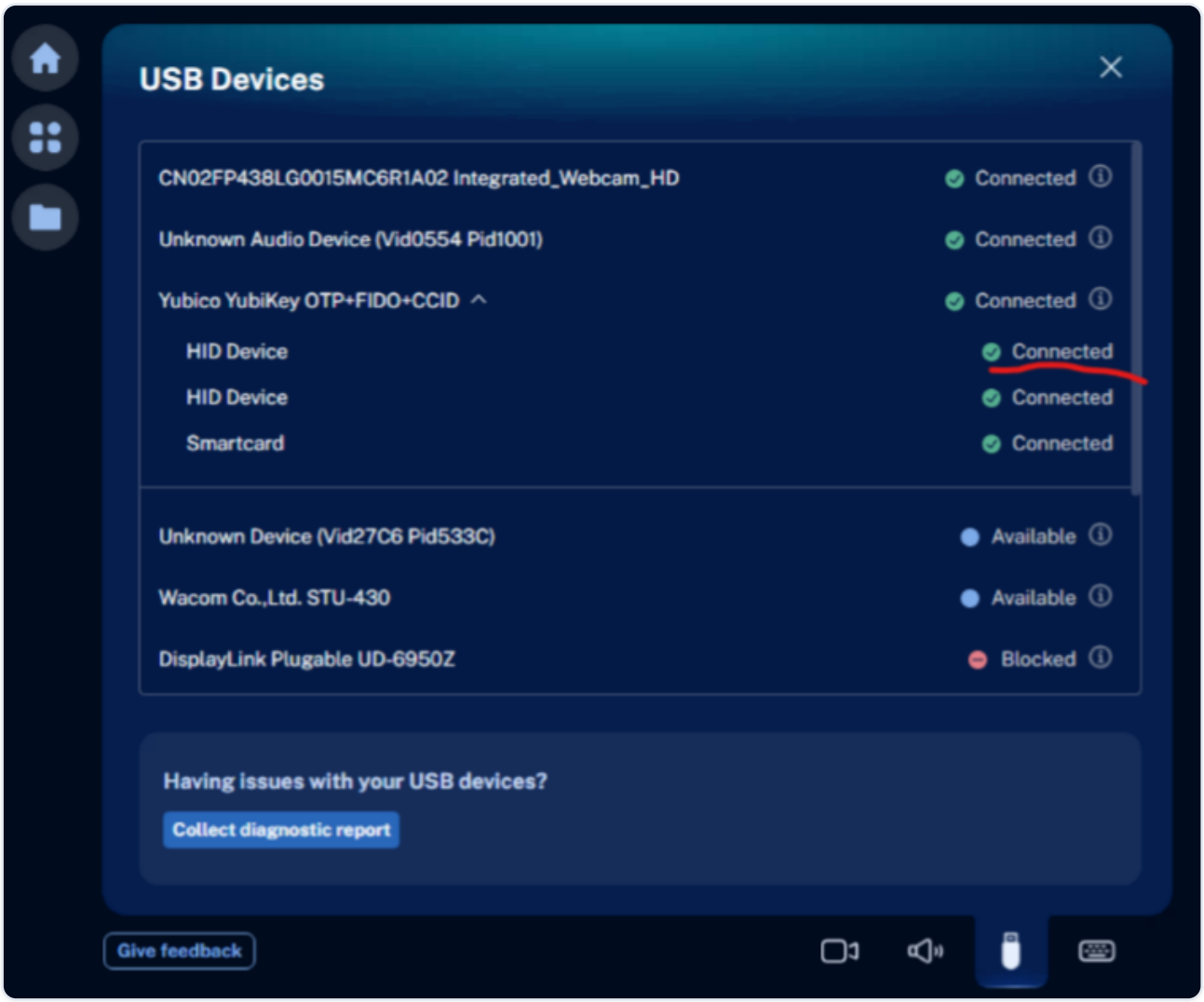
VDAセッション内のキーボードまたはIMEの問題をトラブルシューティングするには、ページ下部にある**診断レポートの収集**をクリックします。



> **注：**
>
> 情報アイコンにカーソルを合わせると、キーボード設定値について確認できます。

USBページ

「**USB**」ページでは、USBデバイスを表示できます。



Citrix AssistantでUSB画面が表示されない場合は、以下を確認してください。

- Citrix Workspaceアプリ (CWA) のバージョンが2511以降であること。
- 「USBリダイレクトポリシー」は無効になっています。
- 環境設定ツールバーで、以下のチェックボックスが選択されています

  「Citrix AssistantアプリのUSBページチェック」(/en-us/citrix-virtual-apps-desktops/2511/media/assisstant-app-usb-checks.png)

USBデバイスには、次の5つの異なるステータス値があります。

- **接続済み**: これらのデバイスは正常にリダイレクトされ、仮想チャネルを使用し、クライアントとVDAの両方で使用できます。
- **情報付きで接続済み**: これらのUSBデバイスは正常にリダイレクトされ、VDAで使用できます。Citrix Workspaceアプリ（CWA）ツールバーから**デバイス**ツールバーにアクセスして、これらを無効にすることができます。

- **ドライバーが見つかりません**: これらのデバイスはVDAにドライバーをインストールする必要がありますが、現在そのドライバーが見つかりません。
- **ブロック済み**: これらのデバイスは、デバイスルールによって管理者にブロックされています。これらのデバイスを使用するには、管理者にお問い合わせください。
- **利用可能**: **デバイス**ツールバーからこれらのデバイスを有効にします。有効にすると、接続され、VDAで使用できるようになります。

VDAセッション内でUSBの問題をトラブルシューティングするには、ページ下部にある**診断レポートの収集**をクリックします。

バージョン情報ページ

システムトレイからアプリのアイコンを右クリックして、**バージョン情報**ページを開きます。Citrix Virtual Desktop Assistantアプリのバージョン情報とサードパーティライセンスエントリは、**バージョン情報**ページに表示されます。

制限事項

- **デスクトップの最適化の動作**: **デスクトップの最適化**ボタンは、最適化後すぐに元の状態に戻ります。今後のバージョンでは、最適化プロセスに関する詳細情報が提供され、最適化された状態がより長く維持されます。
- **カメラとマイクへのアクセス**: Citrix Virtual Desktop Assistantアプリは、デフォルトのフレームワーク通知を使用して、カメラとマイクへのアクセスを時折要求します。
- **一時ファイルのクリーンアップの制限**: 読み取り専用、破損している、または現在使用中のため、一時ファイルをクリーンアップできません。
- **削除できない大きなファイル**: 読み取り専用の一部の大きなファイルは削除できません。今後のバージョンでは、この制限をユーザーに通知する警告メッセージが含まれる予定です。
- **大きなファイルのレンダリング時間**: **大きなファイル**セクションでファイルが表示されるまでにかなりの時間がかかる場合があります。これらのファイルのリスト表示時間を短縮するための取り組みが進行中です。
- **アプリケーションのリスト表示**: メモリが解放され、優先度が低下したアプリケーションがリスト表示されます。これには、バックグラウンドアプリやCitrix Virtual Desktop Assistantアプリ自体が含まれる場合があります。

モニター

管理者とヘルプデスク担当者は、さまざまな機能とツールを使用してCitrix Virtual Apps and Desktops™サイトを監視できます。これらのツールを使用すると、以下を監視できます。

- ユーザーセッションとセッションの使用状況
- ログオンパフォーマンス
- 接続とマシン（障害を含む）
- 負荷評価
- 履歴トレンド
- インフラストラクチャ

Citrix Director (シトリックス ディレクター)

Directorは、監視とトラブルシューティング、およびエンドユーザーのサポートタスクの実行に使用できるリアルタイムのWebツールです。

詳細については、Director の記事を参照してください。

構成ログ

構成ログを使用すると、管理者はサイトに対する管理上の変更を追跡できます。構成ログは、構成変更が行われた後の問題の診断とトラブルシューティング、変更管理と構成の追跡の支援、および管理アクティビティの報告に役立ちます。

Studioからログに記録された情報を表示し、レポートを生成できます。また、Directorのトレンドビューでログに記録された項目を表示して、構成変更の通知を提供することもできます。この機能は、Studioにアクセスできない管理者にとって役立ちます。

トレンドビューは、一定期間にわたる構成変更の履歴データを提供するため、管理者は、サイトに対してどのような変更がいつ誰によって行われたかを評価し、問題の原因を特定できます。このビューは、構成情報を次の3つのカテゴリに分類します。

- 接続障害
- 失敗したシングルセッションマシン

- 失敗したマルチセッションマシン

構成ログを有効にして構成する方法の詳細については、構成ログを参照してください。Directorの記事では、そのツールからログに記録された情報を表示する方法について説明しています。

イベントログ

Citrix Virtual Apps™ and Desktops 内のサービスは、発生したイベントをログに記録します。イベントログは、操作の監視とトラブルシューティングに使用されます。

詳細については、イベントログ を参照してください。個々の機能の記事にもイベント情報が含まれている場合があります。

構成ログ

構成ログは、サイト構成の変更と管理アクティビティをデータベースに記録する機能です。この機能はデフォルトで有効になっています。記録されたコンテンツを使用して、次のことができます。

- 構成変更が行われた後の問題を診断し、トラブルシューティングします。ログは追跡記録を提供します。
- 変更管理を支援し、構成を追跡します。
- 管理アクティビティを報告します。

Citrix Studioから、構成ログ設定を行い、構成ログを表示し、HTMLおよびCSVレポートを生成できます。構成ログの表示は、日付範囲と全文検索結果でフィルタリングできます。強制ログが有効になっている場合、ログに記録できない構成変更は行われません。適切な権限があれば、構成ログからエントリを削除できます。構成ログ機能を使用してログコンテンツを編集することはできません。

構成ログは、PowerShell SDKと構成ログサービスを使用します。構成ログサービスは、サイト内のすべてのControllerで実行されます。いずれかのControllerが失敗した場合、別のController上のサービスがログ要求を自動的に処理します。

デフォルトでは、構成ログ機能は有効になっており、サイト作成時に作成されるデータベース（サイト構成データベース）を使用します。データベースの別の場所を指定できます。構成ログデータベースは、サイト構成データベースと同じ高可用性機能をサポートします。

構成ログへのアクセスは、委任管理によって、「ログ設定の編集」および「構成ログの表示」権限を使用して制御されます。

構成ログは、作成時にローカライズされます。たとえば、英語で作成されたログは、読み手のロケールに関係なく、英語で読み取られます。

ログに記録される内容

Studio、Director、およびPowerShellスクリプトから開始された構成変更と管理アクティビティがログに記録されます。ログに記録される構成変更の例には、次のもの（作成、編集、削除、割り当て）の操作が含まれます。

- マシンカタログ
- デリバリーグループ（電源管理設定の変更を含む）
- 管理者ロールとスコープ
- ホストリソースと接続
- Studio を介した Citrix ポリシー

ログに記録される管理上の変更の例を次に示します。

- 仮想マシンまたはユーザーデスクトップの電源管理
- Studio または Director がユーザーにメッセージを送信する

次の操作はログに記録されません。

- プール管理による仮想マシンの電源投入などの自律的な操作。
- グループポリシー管理コンソール (GPMC) を介して実装されたポリシーアクション。これらのアクションのログを表示するには、Microsoft ツールを使用します。
- レジストリ、データベースへの直接アクセス、または Studio、Director、PowerShell 以外のソースを介して行われた変更。
- 展開が初期化されると、最初の構成ログサービスインスタンスが構成サービスに登録されたときに構成ログが利用可能になります。したがって、構成の初期段階はログに記録されません（たとえば、データベーススキーマが取得されて適用されたとき、ハイパーバイザーが初期化されたときなど）。

構成ログの管理

デフォルトでは、構成ログはサイトの作成時に作成されるデータベース（サイト構成データベースとも呼ばれます）を使用します。Citrix は、次の理由により、構成ログデータベース（および監視データベース）に別の場所を使用することをお勧めします。

- 構成ログデータベースのバックアップ戦略は、サイト構成データベースのバックアップ戦略とは異なる可能性があります。
- 構成ログ（および監視サービス）のために収集されるデータ量によって、サイト構成データベースで利用可能な領域に悪影響が及ぶ可能性があります。
- これにより、3つのデータベースの単一障害点が分割されます。

構成ログをサポートしない製品エディションには、Studioにログノードがありません。

構成ログと強制ログの有効化と無効化

デフォルトでは、構成ログは有効になっており、強制ログは無効になっています。

1. Web Studio にサインインし、左側のペインで **Logging** を選択します。
2. アクションバーで **Preferences** を選択します。構成ログのダイアログボックスには、データベース情報が含まれており、構成ログと強制ログが有効か無効かを示します。
3. 希望するアクションを選択します。

   構成ログを有効にするには、**有効にする**を選択します。これがデフォルト設定です。データベースに書き込めない場合、ログ情報は破棄されますが、操作は続行されます。

   構成ログを無効にするには、**Disable** を選択します。以前にログが有効になっていた場合、既存のログはPowerShell SDKで読み取り可能です。

   強制ログを有効にするには、**Prevent changes to the site configuration when the database is not available** を選択します。通常ログに記録される構成変更や管理アクティビティは、構成ログデータベースに書き込みが可能な場合にのみ許可されます。強制ログは、構成ログが有効になっている場合（**Enable** が選択されている場合）にのみ有効にできます。構成ログサービスが失敗し、高可用性が使用されていない場合、強制ログが有効であると見なされます。そのような場合、通常ログに記録される操作は実行されません。

   強制ログを無効にするには、**データベースが利用できない場合にサイト構成の変更を許可する**を選択します。構成ログデータベースにアクセスできない場合でも、構成変更と管理アクティビティが許可されます。これがデフォルト設定です。

構成ログデータベースの場所を変更する

強制ログが有効になっている場合、データベースの場所を変更することはできません。場所の変更には、ログに記録できない短い切断間隔が含まれるためです。

1. サポートされているSQL Serverバージョンを使用して、データベースサーバーを作成します。
2. Web Studioにサインインし、左ペインで**ログ**を選択します。

3. アクションバーで**設定**を選択します。
4. 「ログ設定」ダイアログボックスで、「**ログデータベースの変更**」を選択します。
5. 「ログデータベースの変更」ダイアログボックスで、新しいデータベースサーバーを含むサーバーの場所を指定します。有効な形式については、「データベースアドレス形式」を参照してください。
6. Studioでデータベースを作成するには、「**OK**」をクリックします。プロンプトが表示されたら「**OK**」をクリックすると、データベースが自動的に作成されます。Studioは、現在のStudioユーザーの資格情報を使用してデータベースへのアクセスを試行します。失敗した場合は、データベースユーザーの資格情報の入力を求められます。その後、Studioはデータベーススキーマをデータベースにアップロードします。(資格情報はデータベース作成中のみ保持されます。)
7. データベースを手動で作成するには、「**データベーススクリプトの生成**」をクリックします。生成されたスクリプトには、データベースを手動で作成するための手順が含まれています。スキーマをアップロードする前に、データベースが空であり、少なくとも1人のユーザーがデータベースにアクセスして変更する権限を持っていることを確認してください。

以前のデータベースの構成ログデータは、新しいデータベースにはインポートされません。ログを取得する際に、両方のデータベースからログを集約することはできません。新しい構成ログデータベースの最初のログエントリは、データベースの変更が発生したことを示しますが、以前のデータベースを特定するものではありません。

構成ログコンテンツの表示

構成ログコンテンツを表示するには、左側のペインで「**ログ**」を選択し、「**イベント**」タブを選択します。

デフォルトでは、イベントログは管理者名で一覧表示されます。必要に応じて、次のタスクを実行できます。

- **ログの詳細を表示**。高レベルの操作は、1つ以上のサービスおよびSDK呼び出し（低レベルの操作）をもたらします。上部のペインで高レベルの操作を選択すると、下部のペインに低レベルの操作が表示されます。
- **表示の並べ替え**。列ヘッダーをクリックして表示を並べ替えます。
- **ログのフィルター**。日付間隔やカスタム期間などのフィルター条件を設定するか、検索ボックスにメインタスクの完全な名前または部分的な名前を入力して、表示を絞り込みます。検索を使用した後に標準表示に戻るには、検索ボックスのテキストをクリアします。
- **ログのエクスポート**。選択したログまたはすべてのログをCSVファイルにエクスポートして、アーカイブまたは詳細な分析を行います。

- **列のカスタマイズ**。クライアントIPやラベルなどのデフォルト以外の列を追加して、表示をニーズに合わせて調整します。
- **ラベルの管理**。イベントログのラベルを追加、編集、削除して、ログの整理と追跡を強化します。

表示の特性：

- 操作が完了する前に失敗した場合、ログ操作がデータベースで完了しない可能性があります。たとえば、開始レコードに対応する停止レコードがない場合などです。このような場合、ログには情報が不足していることが示されます。時間範囲に基づいてログを表示すると、データが条件に一致する場合、不完全なログが表示されます。

  たとえば、過去5日間のログを要求し、過去5日間に開始時刻があり終了時刻がないログがある場合、それも含まれます。
- PowerShell コマンドレットを呼び出すスクリプトを使用する場合、親の上位レベル操作を指定せずに下位レベル操作を作成すると、構成ログは代替の上位レベル操作を作成します。

レポートを生成する

構成ログデータを含むCSVおよびHTMLレポートを生成できます。

- CSVレポートには、指定された時間間隔のすべてのログデータが含まれます。データベース内の階層データは、単一のCSVテーブルにフラット化されます。ファイル内のデータのどの側面も優先されません。書式設定は使用されず、人間が読めることは想定されていません。ファイル（MyReportという名前）には、普遍的に利用可能な形式でデータが含まれています。CSVファイルは、データのアーカイブや、Microsoft Excelなどのレポート作成ツールやデータ操作ツールのデータソースとしてよく使用されます。
- HTMLレポートは、指定された時間間隔のログデータを人間が読める形式で提供します。変更を確認するための構造化されたナビゲート可能なビューを提供します。HTMLレポートは、SummaryとDetailsという2つのファイルで構成されます。Summaryには、上位レベルの操作（各操作がいつ、誰によって行われたか、およびその結果）が一覧表示されます。各操作の横にある**Details**リンクをクリックすると、Detailsファイル内の下位レベルの操作に移動し、追加情報が表示されます。

構成ログレポートを生成するには、Studioナビゲーションペインで**Logging**を選択し、アクションバーで**Create custom report**を選択します。

- レポートの日付範囲を選択します。
- レポート形式（CSV、HTML、またはその両方）を選択します。

- レポートを保存する場所を参照します。

構成ログコンテンツを削除する

構成ログを削除するには、特定の委任管理権限とSQL Serverデータベース権限が必要です。

- **委任管理:** 展開構成の読み取りを許可する委任管理ロールが必要です。完全管理者ロールにはこの権限があります。カスタムロールには、 カテゴリで または が選択されている必要があります。

  構成ログデータを削除する前にバックアップを作成するには、カスタムロールに カテゴリで または が選択されている必要もあります。

- **SQL Server データベース:** データベースからレコードを削除する権限を持つ SQL Server ログインが必要です。これには2つの方法があります。

  - sysadmin サーバーロールを持つ SQL Server データベースログインを使用します。これにより、データベースサーバー上のあらゆるアクティビティを実行できます。あるいは、`serveradmin` または `setupadmin` サーバーロールを使用すると、削除操作を実行できます。
  - 展開でより高いセキュリティが必要な場合は、データベースからレコードを削除する権限を持つデータベースユーザーにマッピングされた非sysadminデータベースログインを使用します。

    a. SQL Server Management Studio で、「sysadmin」以外のサーバーロールを持つ SQL Server ログインを作成します。

    b. ログインをデータベース内のユーザーにマッピングします。SQL Server は、ログインと同じ名前のユーザーをデータベース内に自動的に作成します。

    c. データベースロールメンバーシップで、データベースユーザーのロールメンバーの少なくとも1つを指定します: `ConfigurationLoggingSchema_ROLE` または `dbowner`。

  詳細については、SQL Server Management Studioのドキュメントを参照してください。

構成ログを削除するには:

1. Web Studioにサインインし、左ペインで**ログ**を選択します。
2. アクションバーで**ログの削除**を選択します。
3. ログを削除する前にバックアップを作成するかどうかを尋ねられます。バックアップを作成することを選択した場合、バックアップアーカイブが保存される場所を参照します。バックアップはCSVファイルとして作成されます。

構成ログがクリアされた後、ログの削除は空のログに投稿される最初のアクティビティです。そのエントリには、誰がいつログを削除したかに関する詳細が記載されています。

API および PowerShell ログの表示

現在のセッション中に作成されたAPIリクエストを監視するには、**API**タブをクリックします。APIログは、Web Studioからサインアウトするとクリアされます。

その日に行ったUIアクションに対応するPowerShellコマンドを表示するには、**PowerShell**タブをクリックします。

構成ログにメタデータを関連付ける

構成ログにメタデータを添付するには、`MetadataMap` と呼ばれる `name-value` ペアをログレコードに関連付けます。

> **注:**
>
> - メタデータは、高レベルの操作オブジェクトにのみ添付できます。
> - メタデータは、実行時に既存のレコードに関連付けられます。

メタデータを設定する

ログレコードを `MetadataMap` に関連付けるには、PowerShell コマンド `Set-LogHighLevelOperationMetadata` を実行します。 `Set-LogHighLevelOperationMetadata` は次のパラメーターを受け取ります。

- **Id**: 高レベル操作のID。
- **InputObject**: メタデータを追加する高レベル操作。これは、高レベル操作オブジェクトまたはオブジェクトのリストが PowerShell コマンドに渡される `Id` パラメーターの代替です。
- **Name**: 追加するメタデータのプロパティ名。指定された高レベル操作に対して、プロパティは一意である必要があります。プロパティには、次の文字 ()\/;:#.*?=<>|'" を含めることはできません。
- **Value**: プロパティの値。
- **Map**: プロパティの (名前、値) ペアの辞書。これは、`-Name` および `-Value` パラメーターを使用してメタデータを設定する代替手段です。

例えば、ID 40 のすべての高レベルログレコードにメタデータを添付するには、次の PowerShell コマンドを実行します。

```
Get-LogHighLevelOperation – Id 40 | Set-LogHighLevelOperationMetadata -Name A -Value B
```

ユーザー `abc@example.com` を持つ高レベルレコードにメタデータを添付するには、次の PowerShell コマンドを実行します。

```
Get-LogHighLevelOperation – User `abc@example.com` | Set-LogHighLevelOperationMetadata -Name C -Value D
```

メタデータを使用して取得する

関連付けられたメタデータを使用してログレコードを取得するには、次のPowerShellコマンドを実行します。

- キーと値で検索:

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- 値で任意のキーを検索:

  ```
  Get-LogHighLevelOperation -Metadata "*:Value"
  ```

- キーと任意の値で検索:

  ```
  Get-LogHighLevelOperation -Metadata "Key:*"
  ```

メタデータを削除する

関連付けられたメタデータを削除するには、PowerShellコマンド `Remove-LogHighLevelOperationMetadata` を実行します。 `Remove-LogHighLevelOperationMetadata` は次のパラメーターを受け取ります:

- **Id**: 高レベル操作のID。
- **InputObject**: メタデータを追加する高レベル操作。これは、高レベル操作オブジェクトまたはオブジェクトのリストがPowerShellコマンドに渡される `Id`` パラメーターの代替です。
- **Name**: 削除するメタデータのプロパティ名。指定されたオブジェクトのすべてのメタデータを削除するには、$null に設定します。
- **Map**: プロパティの (名前、値) ペアの辞書。これはハッシュテーブル (@{"name1" = "val1"; "name2" = "val2"} で作成) または文字列辞書 (new-object

"System.Collections.Generic.Dictionary" で作成) のいずれかです。マップ内のキーと名前が一致するプロパティは削除されます。

イベントログ

以下の記事では、Citrix Virtual Apps and Desktops 内のサービスによってログに記録される可能性のあるイベントを一覧表示し、説明します。

この情報は網羅的ではありません。読者は、追加のイベント情報について、個々の機能記事を確認してください。

- Citrix Broker Service イベント
- Citrix FMA Service SDK イベント
- シトリックス コンフィギュレーション サービス イベント
- Citrix 委任管理サービス イベント

ディレクター

Director は、Citrix Virtual Apps and Desktops 用の監視およびトラブルシューティングコンソールです。

Director のアーキテクチャ(/en-us/citrix-virtual-apps-desktops/2511/media/director-architecture.png)

Director は以下にアクセスできます。

- Analytics、Performance Manager、および Network Inspector と統合された統合コンソールを使用して、Broker Agent からのリアルタイムデータ。以下の分析は、Citrix ADM によって提供され、Citrix Virtual Apps™ または Desktops 環境におけるネットワークに起因するボトルネックを特定します。
    - 健全性と容量の保証のためのパフォーマンス管理
    - 履歴トレンドとネットワーク分析
- Configuration Logging データベースにアクセスするために Monitor データベースに保存されている履歴データ。
- Citrix ADM を使用した Citrix Gateway からの ICA® データ。
    - Citrix Virtual Apps または Desktops の仮想アプリケーション、デスクトップ、およびユーザーのエンドユーザーエクスペリエンスに対する可視性を得る。
    - 効果的なトラブルシューティングのために、ネットワークデータをアプリケーションデータおよびリアルタイムメトリックと関連付ける。
    - Citrix Virtual Desktop 7 Director 監視ツールと統合する。

Director は、Citrix Virtual Apps または Desktops Site のリアルタイムおよび履歴の健全性監視を提供するトラブルシューティングダッシュボードを使用します。この機能により、リアルタイムで障害を確認でき、エンドユーザーが何を経験しているかをよりよく把握できます。

Director の機能と Delivery Controller (DC)、VDA、およびその他の依存コンポーネントとの互換性に関する詳細については、「機能互換性マトリックス」を参照してください。

> **注:**

MeltdownおよびSpectreの投機的実行サイドチャネル脆弱性が開示されたため、Citrixは関連する緩和パッチをインストールすることを推奨します。これらのパッチはSQL Serverのパフォーマンスに影響を与える可能性があります。詳細については、Microsoftサポート記事「Protect SQL Server from attacks on Spectre and Meltdown side-channel vulnerabilities」を参照してください。Citrixは、実稼働環境にパッチを展開する前に、規模をテストし、ワークロードを計画することを推奨します。

Directorは、デフォルトでDelivery Controller上のWebサイトとしてインストールされます。前提条件およびその他の詳細については、このリリースのシステム要件ドキュメントを参照してください。Directorのインストールと構成に関する具体的な情報については、「Directorのインストールと構成」を参照してください。

Directorへのログオン

Director の Web サイトは、https または `http://<Server FQDN>/Director` にあります。

マルチサイト展開でいずれかのサイトがダウンしている場合、ダウンしているサイトへの接続を試みるため、ログオンに少し時間がかかります。

PIV スマートカード認証での Director の使用

Directorは、ログオンに個人識別検証（PIV）ベースのスマートカード認証をサポートするようになりました。この機能は、アクセス制御にスマートカードベースの認証を使用する組織や政府機関にとって役立ちます。 スマートカード認証には、DirectorサーバーとActive Directoryでの特定の構成が必要です。構成手順の詳細については、「PIVスマートカード認証の構成」を参照してください。

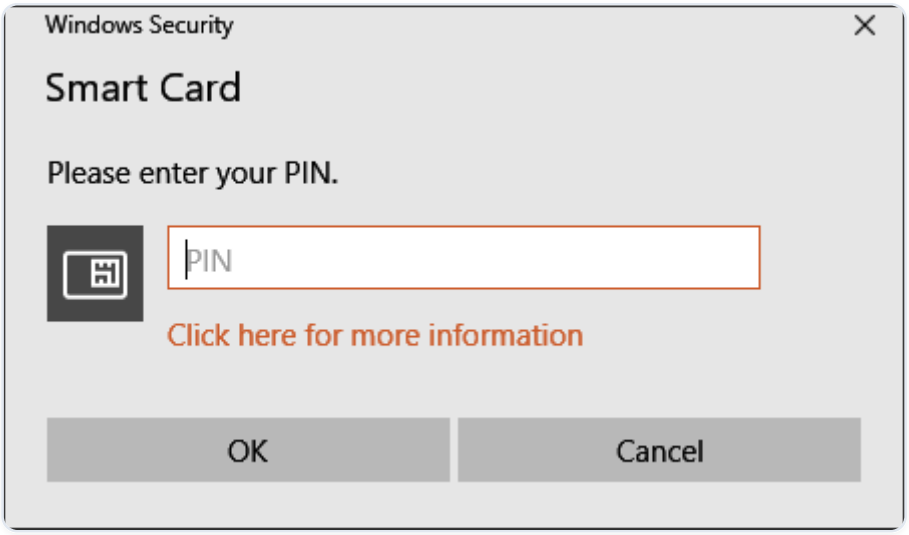
注:

スマートカード認証は、同じ Active Directory ドメインのユーザーのみがサポートされます。

必要な構成を実行した後、スマートカードを使用して Director にログオンできます。

1. スマートカードをスマートカードリーダーに挿入します。

2. ブラウザーを開き、Director の URL `https://<directorfqdn>/Director` にアクセスします。
3. 表示されたリストから有効なユーザー証明書を選択します。
4. スマートカードトークンを入力します。



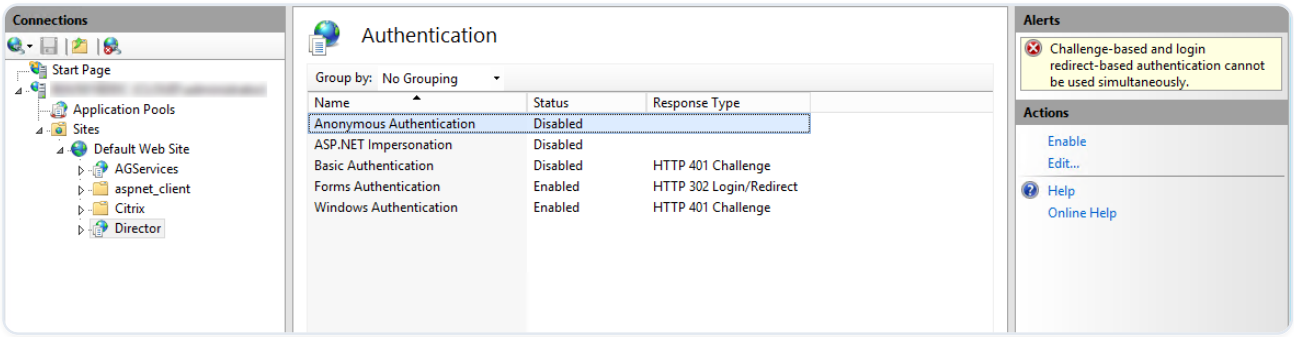
5. 認証されると、Director ログオンページで追加の資格情報を入力することなく Director にアクセスできます。

統合 Windows 認証での Director の使用

統合Windows認証（IWA）を使用すると、ドメイン参加ユーザーはDirectorログオンページで資格情報を再入力することなく、Directorに直接アクセスできます。統合Windows認証とDirectorを使用するための前提条件は次のとおりです。

- Director をホストする IIS Web サイトで統合 Windows 認証を有効にします。Director をインストールすると、匿名認証とフォーム認証が有効になります。統合 Windows 認証と Director をサポートするには、匿名認証を無効にし、Windows 認証を有効にします。非ドメインユーザーの認証には、フォーム認証を有効のままにしておく必要があります。

  a. IIS マネージャーを起動します。
  b. **サイト** \> **Default Web Site** \> **Director** に移動します。
  c. **認証**を選択します。
  d. **匿名認証**を右クリックし、**無効**を選択します。
  e. **Windows 認証**を右クリックし、**有効**を選択します。



- Director マシンに対する Active Directory 委任権限を構成します。構成は、Director と Delivery Controller™ が別々のマシンにインストールされている場合にのみ必要です。

  a. Active Directory マシンで、Active Directory 管理コンソールを開きます。

  b. Active Directory 管理コンソールで、**ドメイン名** \> **コンピューター**に移動します。Director マシンを選択します。

  c. 右クリックして**プロパティ**を選択します。

  d. プロパティで、**委任**タブを選択します。

  e. オプション、**このコンピューターを任意のサービスへの委任に信頼する (Kerberos のみ)** を選択します。

- Director へのアクセスに使用するブラウザーは、統合 Windows 認証をサポートしている必要があります。Firefox および Chrome では、追加の構成手順が必要になる場合があります。詳細については、ブラウザーのドキュメントを参照してください。
- Monitoring Service は、Microsoft .NET Framework 4.5.1 以降の、Director のシステム要件に記載されているサポート対象バージョンを実行している必要があります。詳細については、システム要件を参照してください。

ユーザーが Director からログオフするか、セッションがタイムアウトすると、ログオンページが表示されます。ログオンページから、ユーザーは認証の種類を**自動ログオン**または**ユーザー資格情報**に設定できます。

インターフェイスビュー

Directorは、特定の管理者向けに調整されたさまざまなインターフェイスビューを提供します。製品の権限によって、表示される内容と利用可能なコマンドが決まります。

たとえば、ヘルプデスク管理者は、ヘルプデスクタスクに合わせて調整されたインターフェイスを参照します。Director を使用すると、ヘルプデスク管理者は問題を報告しているユーザーを検索し、そのユーザーに関連付けられたアクティビティを表示できます。たとえば、ユーザーのアプリケーションとプロセスのステータスなどです。応答しないアプリケーションやプロセスを終了す

る、ユーザーのマシンで操作をシャドウする、マシンを再起動する、ユーザープロファイルをリセットするなどのアクションを実行することで、問題を迅速に解決できます。

対照的に、完全な管理者はサイト全体を参照および管理し、複数のユーザーおよびマシンに対してコマンドを実行できます。ダッシュボードには、セッションのステータス、ユーザーログオン、サイトインフラストラクチャなど、展開の主要な側面に関する概要が表示されます。情報は毎分更新されます。問題が発生した場合、発生した障害の数と種類に関する詳細が自動的に表示されます。

Director におけるさまざまな役割とその権限の詳細については、委任管理とDirectorを参照してください。

Pendo による使用状況データ収集

Director のインストール後、Director Service は Pendo を使用して使用状況データの収集を開始します。トレンドページの使用状況と OData API 呼び出し分析に関する統計が収集されます。分析データの収集は、Citrix プライバシーポリシーに準拠しています。Director をインストールすると、データ収集はデフォルトで有効になります。

Pendo のデータ収集をオプトアウトするには、Director がインストールされているマシンでレジストリキーを編集します。レジストリキーが存在しない場合は、作成して目的の値に設定します。レジストリキーの値を変更した後、Director インスタンスを更新します。

注意: レジストリエディターを誤って使用すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix は、レジストリエディターの誤った使用によって発生した問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。Citrix は、Windows レジストリを変更する前にバックアップすることをお勧めします。

場所：HKEY_LOCAL_MACHINE\Software\Citrix\Director

名前：DisableGoogleAnalytics

> **注:**
>
> 以前は、DirectorサービスはGoogle Analyticsを使用してデータを収集していました。現在、同じレジストリキーがPendoに使用されています。

> 値：0 = 有効（デフォルト）、1 = 無効

Pendoによるデータ収集を無効にするには、次のPowerShellコマンドレットを使用します。

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

新機能ガイド

Directorには、Pendoを使用して、Directorの現在のバージョンでリリースされた新機能に関する洞察を提供する製品内ガイドがあります。適切な製品内メッセージと組み合わせた簡単な概要は、製品の新機能を理解するのに役立ちます。

この機能をオプトアウトするには、Directorがインストールされているマシンで、以下に説明するようにレジストリキーを編集します。レジストリキーが存在しない場合は、作成して目的の値に設定します。レジストリキーの値を変更した後、Directorインスタンスを更新します。

注意:

レジストリエディターを誤って使用すると、オペレーティングシステムの再インストールが必要になるような重大な問題を引き起こす可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。Citrixは、Windowsレジストリを変更する前にバックアップすることをお勧めします。

場所: HKEY_LOCAL_MACHINE\Software\Citrix\Director

名前: DisableGuidedHelp

値: 0 = 有効（デフォルト）、1 = 無効

製品内ガイドを無効にするには、次のPowerShellコマンドレットを使用します。

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director
```

```
New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
-PropertyType DWORD -Value 1
```

参照記事

- Citrix DirectorからのMTTRの削減
- Citrix Director - PowerShell を使用してアラートと通知を管理および構成する
- Citrix Virtual Apps and Desktops 開発者向けドキュメント

関連製品の新機能

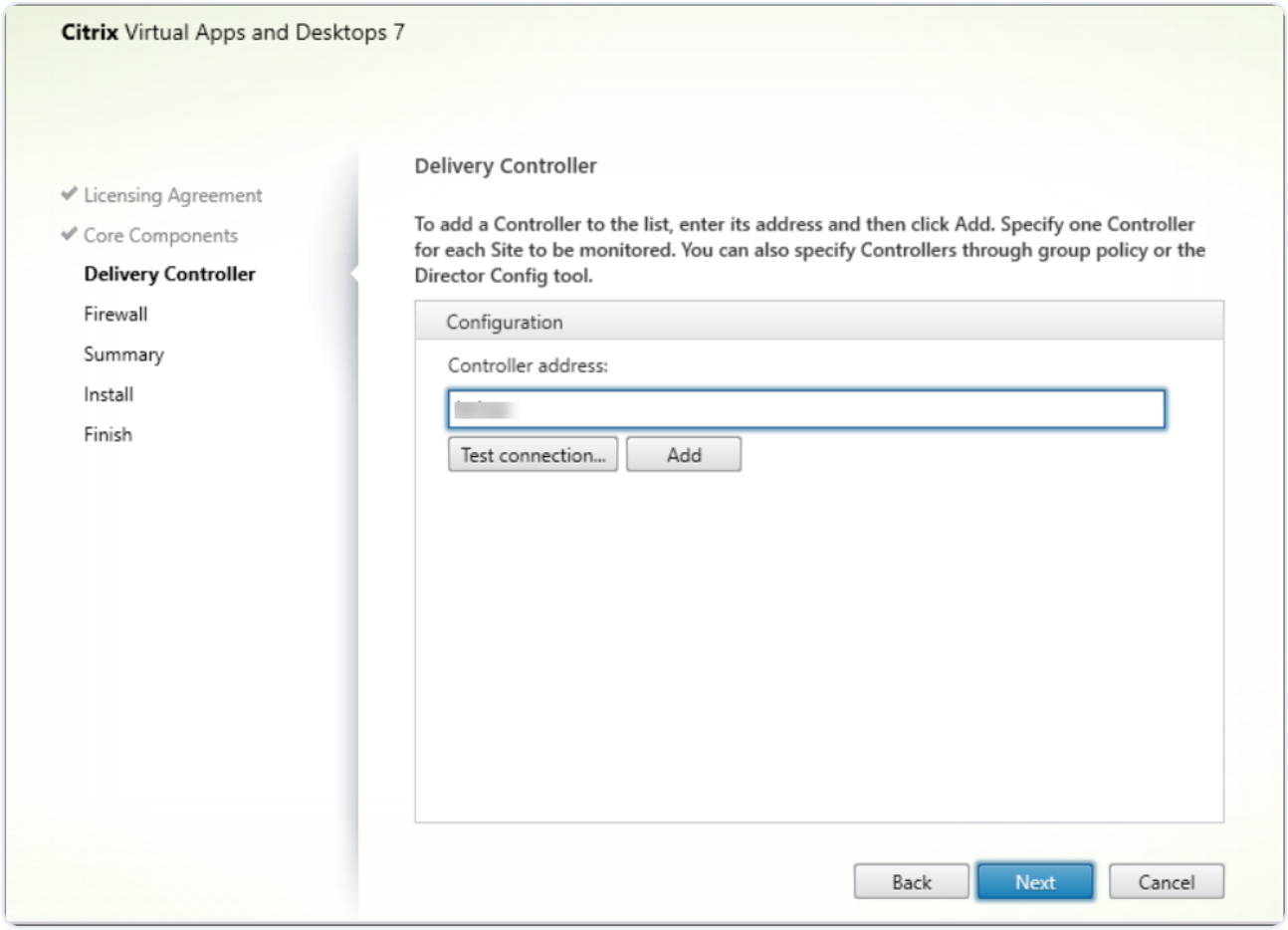
- シトリックス DaaS
- StoreFront
- セキュアプライベートアクセス
- シトリックス エンタープライズ ブラウザ
- Citrix Workspace (シトリックス ワークスペース)
- プロビジョニング

インストールと構成

Directorのインストール

Citrix Virtual Apps and Desktops 用のフル製品ISOインストーラーを使用してDirectorをインストールします。これにより、前提条件の確認、不足しているコンポーネントのインストール、Director Webサイトのセットアップ、および基本的な構成が実行されます。前提条件およびその他の詳細については、本リリースのシステム要件ドキュメントを参照してください。このリリースのDirectorは、Virtual Apps 6.5以前の展開、またはVirtual Desktops 7以前の展開とは互換性がありません。 ISOインストーラーによって提供されるデフォルト構成は、一般的な展開に対応します。インストール時にDirectorが含まれていなかった場合は、ISOインストーラーを使用してDirectorを追加します。追加のコンポーネントを追加するには、ISOインストーラーを再実行し、インストールするコンポーネントを選択します。ISOインストーラーの使用方法については、インストールドキュメントのコアコンポーネントのインストールを参照してください。Citrixでは、.MSIファイルではなく、フル製品ISOインストーラーのみを使用してインストールすることをお勧めします。

DirectorがControllerにインストールされている場合、サーバーアドレスとしてlocalhostが自動的に構成され、Directorはデフォルトでローカルの Controllerと通信します。Controllerから離れた専用サーバーにDirectorをインストールする場合は、ControllerのFQDNまたはIPアドレスの入力を求められます。



注:

追加をクリックして、監視するControllerを追加します。

Directorはデフォルトで、指定されたControllerと通信します。監視するサイトごとにControllerアドレスを1つだけ指定してください。指定したControllerが失敗した場合、Directorは同じサイト内の他のすべてのControllerを自動的に検出し、それらのControllerにフォールバックします。

注:

DirectorはController間で負荷分散を行いません。

ブラウザーとWebサーバー間の通信を保護するために、Citrix®は、DirectorをホストするIIS WebサイトでTLSを実装することをお勧めします。手順については、Microsoft IISのドキュメントを参照してください。TLSを有効にするためにDirectorの構成は必要ありません。

Directorの展開と構成

Directorが複数のサイトを含む環境で使用される場合、Controller、Director、およびその他のコアコンポーネントがインストールされているすべてのサーバーでシステムクロックを同期してください。そうしないと、Directorでサイトが正しく表示されない可能性があります。

重要:

ネットワーク経由でプレーンテキストで送信されるユーザー名とパスワードのセキュリティを保護するため、Director接続にはHTTPではなくHTTPSのみを使用してください。特定のツールは、HTTP（暗号化されていない）ネットワークパケット内のプレーンテキストのユーザー名とパスワードを読み取ることができ、ユーザーにとって潜在的なセキュリティリスクを生み出す可能性があります。

権限を構成する

Directorにログオンするには、Directorの権限を持つ管理者はActive Directoryドメインユーザーであり、以下の権限を持っている必要があります。

- 検索対象となるすべてのActive Directoryフォレストでの読み取り権限（高度な構成を参照）。
- 構成済みの委任管理者ロール（委任管理とDirectorを参照）。
- ユーザーをシャドウするには、管理者はWindowsリモートアシスタンス用のMicrosoftグループポリシーを使用して構成する必要があります。さらに：
  - VDAをインストールする際は、すべてのユーザーデバイスでWindowsリモートアシスタンス機能が有効になっていることを確認してください（デフォルトで選択されています）。
  - サーバーにDirectorをインストールする際は、Windowsリモートアシスタンスがインストールされていることを確認してください（デフォルトで選択されています）。ただし、サーバーではデフォルトで無効になっています。Directorがエンドユーザーにアシスタンスを提供するために、この機能を有効にする必要はありません。Citrixは、サーバーのセキュリティを向上させるために、この機能を無効のままにしておくことを推奨します。

- 管理者がWindowsリモートアシスタンスを開始できるようにするには、リモートアシスタンス用の適切なMicrosoftグループポリシー設定を使用して、必要な権限を付与します。詳細については、CTX239706: 最新のDirectorバージョンでシャドウ機能を構成する方法を参照してください。

DirectorとのCitrix uberAgent®統合

Citrix uberAgentは、Citrix Virtual Apps and Desktops™のインストールにデフォルトで含まれるようになり、強化された監視機能とCitrix Directorとのシームレスな統合を提供します。管理者は、Virtual Delivery Agentのセットアップ中に**オプションソフトウェア**画面で選択を解除することで、インストールから除外できます。

Citrix Virtual Apps and Desktopsのインストールの一部としてuberAgentをインストールする方法の詳細については、uberAgentのドキュメントを参照してください。

主な機能：

ローカルアプリケーション使用状況の監視: Citrix uberAgentを使用すると、仮想デスクトップセッション内で起動されたアプリケーション（ローカルアプリケーションとも呼ばれます）の使用状況を監視でき、Directorとの統合により、データはDirectorダッシュボードで直接利用できます（Platinumライセンスで利用可能）。

DirectorとのCitrix uberAgent統合の構成

Citrix uberAgentのインストール後、DirectorとuberAgentを完全に統合して使用するには、Citrix Web Studio™で以下のポリシーを構成します。

- **uberAgentデータ収集ポリシーを有効にする**：有効にすると、uberAgentはアプリケーションの使用状況とパフォーマンス、システムヘルス、ネットワークメトリック、セキュリティ分析に関するインサイトを提供します。このポリシーはデフォルトで無効になっています。
- **uberAgentデータポリシーでDirectorを強化する**：このポリシーは、DirectorとuberAgentの統合を可能にします。これにより、DirectorはuberAgentが提供するデータを処理し、ローカルアプリケーションの使用状況の監視を含む監視機能を強化できます。このポリシーはデフォルトで有効になっています。

設定が完了すると、データはCitrix Directorのアプリケーション使用状況の監視セクションで利用可能になります。

> **注:**

> uberAgentのローカルアプリケーション使用状況データがDirectorで集計され表示されるまでには、少なくとも1日かかります。

詳細設定

Directorは、ユーザー、Delivery Controller (DC)、VDA、およびDirectorが異なるフォレストに配置されているフォレスト構成にまたがるマルチフォレスト環境をサポートできます。これには、フォレスト間の信頼関係と構成設定の適切なセットアップが必要です。

マルチフォレスト環境における推奨構成

推奨構成では、ドメイン全体の認証を伴うフォレスト間の送信および受信フォレスト信頼関係の作成が必要です。

マルチフォレストサイト構成(/en-us/citrix-virtual-apps-desktops/2511/media/multiforest-config.png)

Directorからの信頼関係により、異なるフォレストに配置されているユーザーセッション、VDA、およびDelivery Controllerにおける問題のトラブルシューティングが可能になります。

Directorが複数のフォレストをサポートするために必要な詳細設定は、Internet Information Services (IIS) マネージャーで定義された設定によって制御されます。

> **重要:**

> IISで設定を変更すると、Directorサービスは自動的に再起動し、ユーザーをログオフします。

> IISを使用して詳細設定を構成するには：

1. Internet Information Services (IIS) マネージャーコンソールを開きます。
2. デフォルトWebサイトの下にあるDirector Webサイトに移動します。
3. 「**アプリケーション設定**」をダブルクリックします。
4. 設定をダブルクリックして編集します。
5. 「**追加**」をクリックして、新しい設定を追加します。

Directorは、ユーザーの検索や、より詳細なユーザーおよびマシン情報の参照にActive Directoryを使用します。デフォルトでは、Directorは以下のドメインまたはフォレストを検索します。

- 管理者アカウントがメンバーです。
- Director Webサーバーがメンバーです（異なる場合）。

Directorは、Active Directoryグローバルカタログを使用してフォレストレベルで検索を実行しようとします。フォレストレベルで検索する権限がない場合、ドメインのみが検索されます。

別のActive Directoryドメインまたはフォレストからデータを検索または参照するには、検索するドメインまたはフォレストを明示的に設定する必要があります。IIS ManagerでDirector Webサイトに以下のアプリケーション設定を構成します。

```
Connector.ActiveDirectory.Domains = (user),(server)
```

値属性のuserとserverは、それぞれDirectorユーザー（管理者）とDirectorサーバーのドメインを表します。

追加のドメインまたはフォレストからの検索を有効にするには、この例に示すように、ドメイン名をリストに追加します。

```
Connector.ActiveDirectory.Domains = (user),(server),\&lt;domain1\>,
\&lt;domain2\>
```

リスト内の各ドメインについて、Directorはフォレストレベルで検索を実行しようとします。フォレストレベルで検索する権限がない場合、ドメインのみが検索されます。

ドメインローカルグループの構成

ほとんどのCitrix Service Provider（CSP）は、インフラストラクチャフォレストにVDA、DC、およびDirectorで構成される同様の環境設定を持っています。ユーザーまたはユーザーグループのレコードはカスタマーフォレストに属します。インフラストラクチャフォレストからカスタマーフォレストへの一方向の送信信頼が存在します。

CSP管理者は通常、インフラストラクチャフォレストにドメインローカルグループを作成し、カスタマーフォレスト内のユーザーまたはユーザーグループをこのドメインローカルグループに追加します。

推奨されるマルチフォレストサイト構成(/en-us/citrix-virtual-apps-desktops/2511/media/domainlocalgroup-config.png)

Directorはこのようなマルチフォレスト設定をサポートし、ドメインローカルグループを使用して構成されたユーザーのセッションを監視できます。

1. IIS ManagerでDirector Webサイトに以下のアプリケーション設定を追加します。

   ```
   Connector.ActiveDirectory.DomainLocalGroupSearch= true



   DomainLocalGroupSearchDomains= \&lt;domain1\>,\&lt;domain2\>
   ```

   \<domain1\>\<domain2\> は、ドメインローカルグループが存在するフォレストの名前です。

2. Web Studioでドメインローカルグループをデリバリーグループに割り当てます。
3. 変更を有効にするには、IISを再起動し、Directorに再度ログオンします。これで、Directorはこれらのユーザーのセッションを監視および表示できます。

Directorにサイトを追加する

Directorがすでにインストールされている場合は、複数のサイトで動作するように構成します。構成するには、各DirectorサーバーでIISマネージャーコンソールを使用して、アプリケーション設定のサーバーアドレスリストを更新します。

各サイトのControllerのアドレスを次の設定に追加します。

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
```

SiteAControllerとSiteBControllerは、2つの異なるサイトのDelivery Controllerのアドレスです。

アクティビティマネージャーで実行中のアプリケーションの可視性を無効にする

デフォルトでは、Directorのアクティビティマネージャーには、ユーザーセッションのすべての実行中アプリケーションのリストが表示されます。この情報は、Directorのアクティビティマネージャー機能にアクセスできるすべての管理者が表示できます。委任された管理者ロールの場合、これにはフル管理者、デリバリーグループ管理者、ヘルプデスク管理者が含まれます。

ユーザーのプライバシーと実行中のアプリケーションを保護するために、**アプリケーション**タブを無効にして、実行中のアプリケーションを一覧表示しないようにすることができます。

> **警告:**

> レジストリを誤って編集すると、オペレーティングシステムを再インストールする必要があるような深刻な問題が発生する可能性があります。Citrix® は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証しません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

1. VDAで、HKEY_LOCAL_MACHINE\\Software\\Citrix\\Director\\TaskManagerDataDisplayedのレジストリキーを変更します。デフォルトでは、このキーは1に設定されています。値を0に変更すると、VDAから情報が収集されなくなり、アクティビティマネージャーに表示されなくなります。
2. Directorがインストールされているサーバーで、実行中のアプリケーションの表示を制御する設定を変更します。デフォルトでは、値は「true」であり、アプリケーションタブで実行中のアプリケーションの表示が許可されます。値を「false」に変更すると、表示が無効になります。このオプションは、Directorのアクティビティマネージャーのみに影響し、VDAには影響しません。 次の設定の値を変更します。 UI.TaskManager.EnableApplications = false

> **重要:**
>
> 実行中のアプリケーションの表示を無効にするには、Activity Managerにデータが表示されないように両方の変更を行います。

PIVスマートカード認証を構成する

この記事では、スマートカード認証機能を有効にするためにDirectorサーバーとActive Directoryで必要な構成を一覧表示します。

> **注:**
>
> スマートカード認証は、同じActive Directoryドメインのユーザーのみがサポートされます。

Directorサーバーの構成

Directorサーバーで以下の構成手順を実行します。

1. クライアント証明書マッピング認証をインストールして有効にします。Microsoftドキュメントのクライアント証明書マッピング認証にある**Active Directoryを使用したクライアント証明書マッピング認証**の手順に従います。

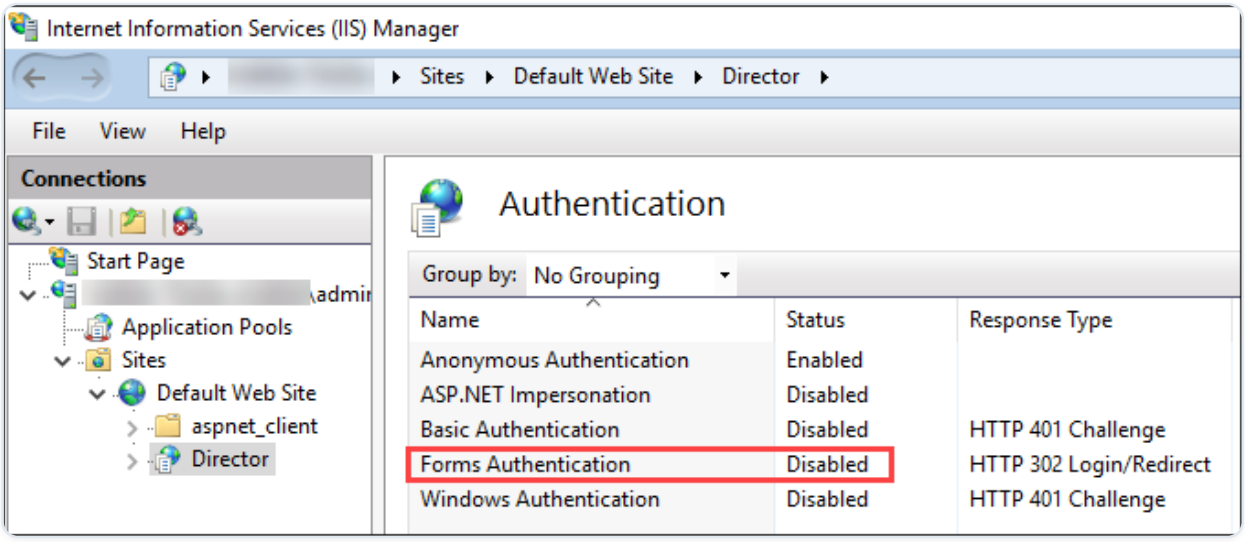
2. Directorサイトでフォーム認証を無効にします。

   IISマネージャーを起動します。

   サイト \> **既定のWebサイト** \> **Director** に移動します。

   認証 を選択します。

   フォーム認証 を右クリックして、**無効** を選択します。



3. クライアント証明書認証のために、DirectorのURLをより安全なhttpsプロトコル (HTTPではなく) に構成します。

   a. IISマネージャーを起動します。

   b. 「**サイト**」>「**既定のWebサイト**」>「**Director**」に移動します。

   c. 「**SSL Settings**」を選択します。

   d. 「**SSLを要求**」と「**クライアント証明書**」\>「**要求**」を選択します。

   SSL設定(/en-us/citrix-virtual-apps-desktops/2511/media/dir-smartcard-config2.png)

4. web.configを更新します。テキストエディターを使用して、web.configファイル（c:\\inetpub\\wwwroot\\Director にあります）を開きます。

`<system.webServer>` 親要素の下に、次のスニペットを最初の子要素として追加します。

```
&lt;defaultDocument&gt;

   &lt;files&gt;

      &lt;add value="LogOn.aspx"/&gt;
```

```
    &lt;/files>

&lt;/defaultDocument>
```

Active Directory の構成

デフォルトでは、Directorアプリケーションは**アプリケーションプール**のIDプロパティで実行されます。スマートカード認証には委任が必要であり、そのためにはDirectorアプリケーションのIDがサービスホスト上でTrusted Computing Base (TCB)権限を持っている必要があります。

Citrixでは、アプリケーションプールID用に個別のサービスアカウントを作成することをお勧めします。Microsoft MSDNの記事「Protocol Transition with Constrained Delegation Technical Supplement」の手順に従って、サービスアカウントを作成し、TCB権限を割り当ててください。

新しく作成したサービスアカウントを Director アプリケーションプールに割り当てます。次の図は、サンプルサービスアカウント「Domain Pool」のプロパティダイアログを示しています。

サンプルサービスアカウント(/en-us/citrix-virtual-apps-desktops/2511/media/dir-smartcard-config3.png)

このアカウントに対して、次のサービスを構成します。

- デリバリーコントローラー™: HOST、HTTP
- ディレクター: HOST、HTTP
- アクティブディレクトリ: GC、LDAP

構成するには、,

1. 「ユーザーアカウントのプロパティ」ダイアログで、「**追加**」をクリックします。
2. **サービスの追加**ダイアログで、ユーザーまたはコンピューターをクリックします。
3. Delivery Controllerのホスト名を選択します。
4. 「**利用可能なサービス**」リストから、HOSTとHTTPの「**サービスの種類**」を選択します。

サービスを構成する(/en-us/citrix-virtual-apps-desktops/2511/media/dir-smartcard-config4.png)

同様に、**Director**および**Active Directory**ホストのサービスの種類を追加します。

サービスプリンシパル名レコードを作成する

各Directorサーバーと、Directorサーバーのプールへのアクセスに使用される負荷分散された仮想IP（VIP）ごとにサービスアカウントを作成する必要があります。新しく作成されたサービスアカウントへの委任を構成するには、サービスプリンシパル名（SPN）レコードを作成する必要があります。

- DirectorサーバーのSPNレコードを作成するには、次のコマンドを使用します。

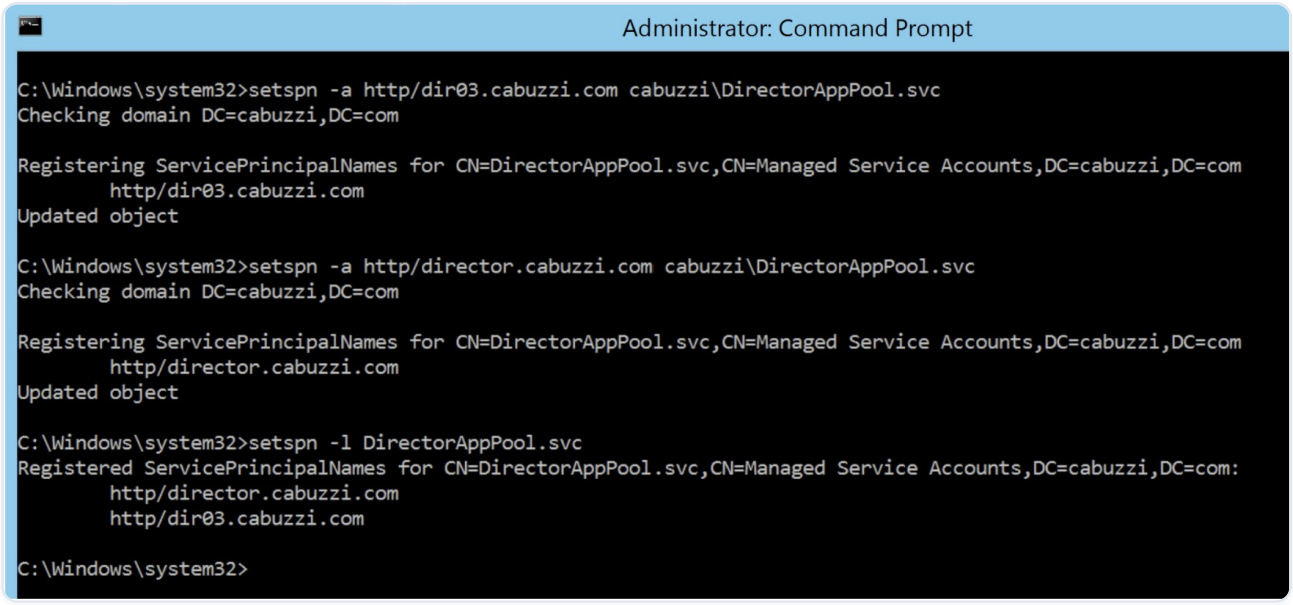
```
  setspn -a http/<directorServer>.<domain_fqdn>
<domain>\<DirectorAppPoolServiceAcct>
```

- 負荷分散されたVIPのSPNレコードを作成するには、次のコマンドを使用します。

```
  setspn -S http/<DirectorFQDN> <domain>\<DirectorAppPoolServiceAcct>
```

- 作成されたSPNを表示またはテストするには、次のコマンドを使用します。

```
  setspn –l <DirectorAppPoolServiceAcct>
```



- 左ペインでDirector仮想ディレクトリを選択し、 をダブルクリックします。 ウィンドウで をクリックし、**AllowKerberosConstrainedDelegation** が1に設定されていることを確認します。

ケルベロス(/en-us/citrix-virtual-apps-desktops/2511/media/dir-smart-card-auth-3.png)

- 左側のペインで を選択し、Directorアプリケーションプールを右クリックして を選択します。
- 「**ID**」を選択し、省略記号（「…」）をクリックして、サービスアカウントのドメイン\ログオンとパスワードの資格情報を入力します。IISコンソールを閉じます。

ID(/en-us/citrix-virtual-apps-desktops/2511/media/dir-smart-card-auth-4.png)

- 管理者として実行したコマンドプロンプトから、ディレクトリを C:\Windows\System32\inetsrv に変更し、次のコマンドを入力します。

```
   appcmd.exe set config “Default Web Site” -section:system.webServer/
security/authentication/clientCertificateMappingAuthentication /
enabled:”True” /commit:apphost
```

```
    appcmd.exe set config “Default Web Site” -section:system.webServer/
security/access /sslFlags:”Ssl, SslNegotiateCert” /commit:apphost
```

コマンドプロンプト(/en-us/citrix-virtual-apps-desktops/2511/media/dir-smart-card-auth-5-scaled.png)

Firefoxブラウザーの構成

Firefoxブラウザーを使用するには、OpenSC 0.17.0で入手可能なPIVドライバーをインストールします。インストールと構成の手順については、FirefoxでのOpenSC PKCS#11モジュールのインストール、ステップバイステップを参照してください。 Directorでのスマートカード認証機能の使用方法については、Directorの記事の「PIVベースのスマートカード認証でDirectorを使用する」セクションを参照してください。

ネットワーク分析の構成

注:

この機能の利用可否は、組織のライセンスと管理者権限によって異なります。

DirectorはCitrix ADMと統合され、ネットワーク分析とパフォーマンス管理を提供します。

- ネットワーク分析は、Citrix ADMのHDX™ Insightレポートを使用して、ネットワークのアプリケーションおよびデスクトップのコンテキストビューを提供します。この機能により、Directorは展開環境におけるICAトラフィックの詳細な分析を提供します。
- パフォーマンス管理は、履歴データの保持と傾向レポートを提供します。リアルタイム評価と比較して履歴データを保持することで、容量や健全性の傾向を含むトレンドレポートを作成できます。

Directorでこの機能を有効にすると、HDX InsightレポートはDirectorに追加情報を提供します。

- 「トレンド」ページの「ネットワーク」タブには、展開環境全体のアプリケーション、デスクトップ、およびユーザーに対する遅延と帯域幅の影響が表示されます。
- 「ユーザー詳細」ページには、特定のユーザーセッションに固有の遅延と帯域幅の情報が表示されます。

制限事項:

- トレンドビューでは、バージョン7より前のVDAのHDX接続ログオンデータは収集されません。それより前のVDAの場合、グラフデータは0と表示されます。

ネットワーク分析を有効にするには、DirectorにCitrix ADMをインストールして構成する必要があります。Directorには、Citrix ADMバージョン11.1ビルド49.16以降が必要です。MASはXenServer上で動作する仮想アプライアンスです。ネットワーク分析を使用すると、Directorは展開環境に関連する情報を通信し、収集します。

詳しくは、Citrix ADMドキュメントを参照してください。

> **注：**
>
> Citrix NetScaler Insight Center は、15 May 2018 をもってメンテナンス終了日を迎えました。Citrix Product Matrixを参照してください。ネットワーク分析には、Director を Citrix ADM と統合してください。NetScaler Insight Center から Citrix ADM への移行については、「Migrate from NetScaler Insight Center to Citrix ADM」を参照してください。

1. Directorがインストールされているサーバーで、C:\\inetpub\\wwwroot\\Director\\toolsにあるDirectorConfigコマンドラインツールを見つけ、コマンドプロンプトからパラメータ/confignetscalerを指定して実行します。

2. プロンプトが表示されたら、Citrix ADMマシン名（FQDNまたはIPアドレス）、ユーザー名、パスワード、HTTPS接続タイプ（HTTPよりも推奨）を入力し、Citrix ADM統合を選択します。
3. 変更を検証するには、ログオフして再度ログオンします。

> **注：**
>
> Citrix NetScaler Insight Centerは、15 May 2018をもってメンテナンス終了日を迎えました。Citrix製品マトリックス を参照してください。ネットワーク分析のためにDirectorをCitrix ADMと統合してください。NetScaler Insight CenterをCitrix ADMに移行するには、「NetScaler Insight CenterからCitrix ADMへの移行」を参照してください。

1. Directorがインストールされているサーバーで、`C:\inetpub\wwwroot\Director\tools`にあるDirectorConfigコマンドラインツールを見つけ、コマンドプロンプトからパラメーター/confignetscalerを指定して実行します。
2. プロンプトが表示されたら、Citrix ADMマシン名（FQDNまたはIPアドレス）、ユーザー名、パスワード、HTTPS接続タイプ（HTTPよりも推奨）、およびCitrix ADM統合を選択します。
3. 変更を確認するには、ログオフして再度ログオンします。

> **注:**
>
> ADM Director統合のユーザーロール(/en-us//citrix-virtual-apps-desktops/media/dir-adm-user-role.png)

> 詳細については、アクセスポリシーの構成を参照してください。

委任管理とDirector

委任管理では、管理者、役割、スコープという3つの概念を使用します。権限は、管理者の役割と、その役割のスコープに基づいています。たとえば、管理者は、スコープが1つのサイトのエンドユーザーに対する責任のみを含むヘルプデスク管理者ロールを割り当てられる場合があります。

委任管理者の作成については、メインの委任管理の記事を参照してください。

管理権限は、管理者に提示されるDirectorインターフェイスと、管理者が実行できるタスクを決定します。権限は以下を決定します。

- 管理者がアクセスできるビュー（総称してビューと呼ばれます）。
- 管理者が表示および操作できるデスクトップ、マシン、およびセッション。
- ユーザーセッションのシャドウイングやメンテナンスモードの有効化など、管理者が実行できるコマンド。

組み込みの役割と権限は、管理者がDirectorをどのように使用するかを決定します。

管理者ロール	DIRECTORでの権限
フル管理者	すべてのビューへのフルアクセス権を持ち、ユーザーセッションのシャドウイング、メンテナンスモードの有効化、トレンドデータのエクスポートなど、すべてのコマンドを実行できます。
デリバリーグループ管理者	すべてのビューへのフルアクセス権を持ち、ユーザーセッションのシャドウイング、電源管理とセッション管理、メンテナンスモードの有効化、トレンドデータのエクスポートなど、すべてのコマンドを実行できます。
読み取り専用管理者	指定されたスコープ内のすべてのビューにアクセスし、すべてのオブジェクトとグローバル情報を表示できます。HDX™チャネルからレポートをダウンロードし、トレンドビューの「エクスポート」オプションを使用してトレンドデータをエクスポートできます。その他のコマンドを実行したり、ビュー内の何かを変更したりすることはできません。
ヘルプデスク管理者	ヘルプデスクビューとユーザー詳細ビューのみにアクセスでき、管理者が管理を委任されているオブジェクトのみを表示できます。ユーザーのセッションをシャドウし、そのユーザーのコマンドを実行できます。メンテナンスモード操作を実行できます。シングルセッションOSマシンに対して電源制御オプションを使用できます。ダッシュボード、トレンド、アラート、またはフィルタービューにはアクセ

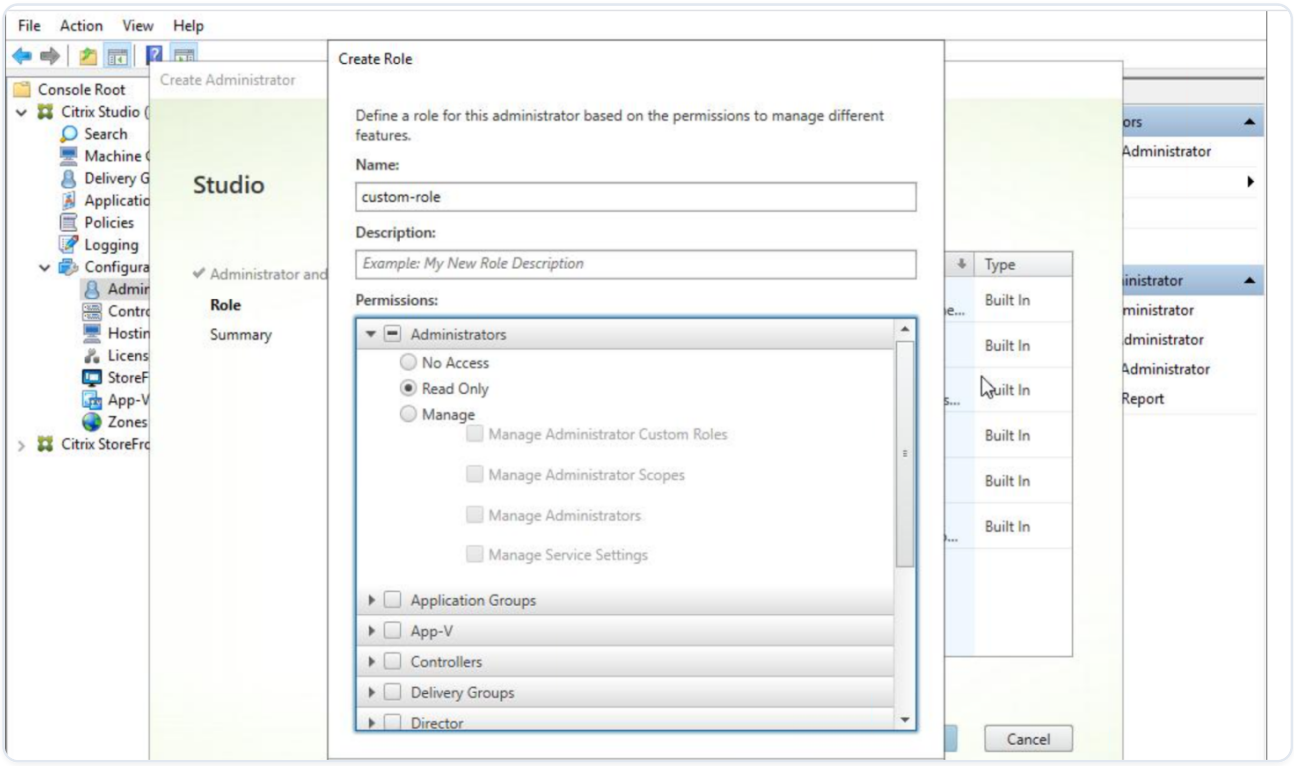
管理者ロール	DIRECTORでの権限
	スできません。マルチセッションOSマシンに対して電源制御オプションを使用できません。
マシンカタログ管理者	マシン詳細ページ（マシンベース検索）のみにアクセスできます。
ホスト管理者	アクセスできません。この管理者はDirectorではサポートされておらず、データを表示できません。

Director管理者用のカスタム役割を構成する

Studioでは、組織の要件により厳密に一致させ、権限をより柔軟に委任するために、Director固有のカスタムロールを構成することもできます。たとえば、組み込みのヘルプデスク管理者ロールを制限して、この管理者がセッションをログオフできないようにすることができます。

Director権限を持つカスタム役割を作成する場合、その役割に他の一般的な権限も付与する必要があります。

- DirectorにログオンするためのDelivery Controller™権限 - 管理者ノードで少なくとも読み取り専用アクセス
- Directorで配信グループに関連するデータを表示するための配信グループへの権限 - 少なくとも読み取り専用アクセス

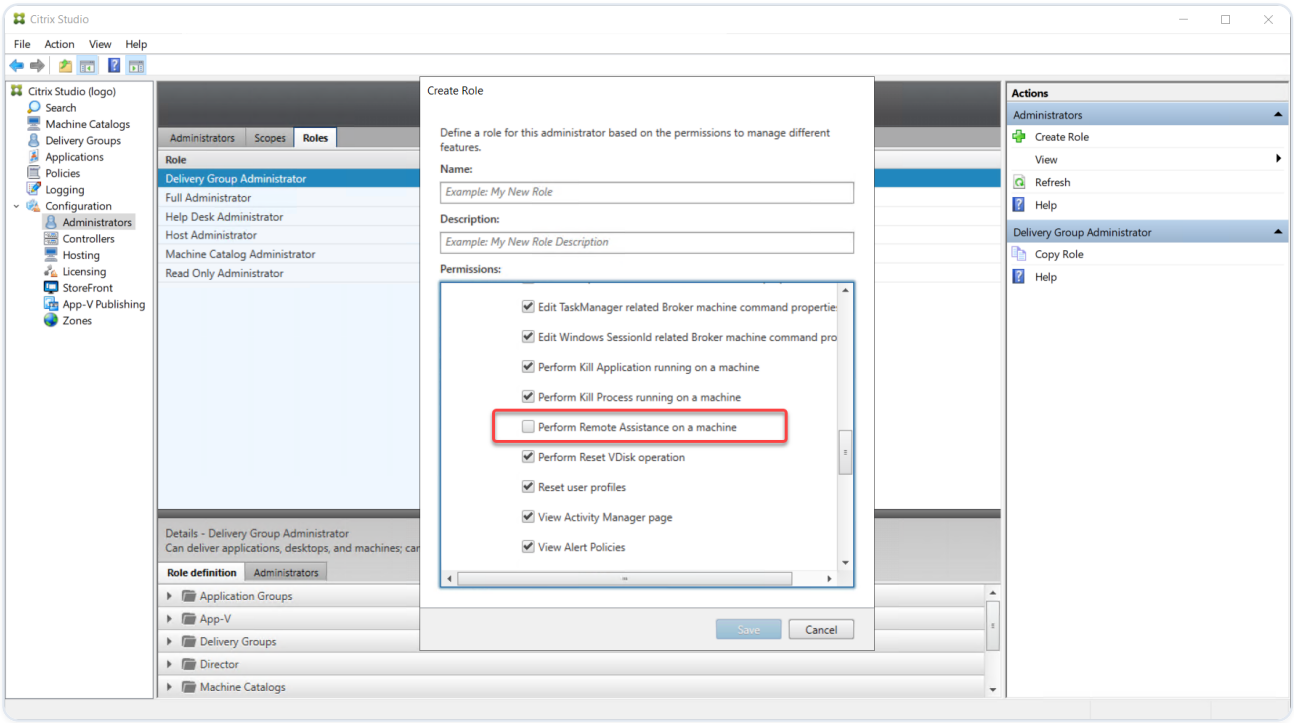


または、既存のロールをコピーして、異なるビューの追加権限を含めることで、カスタムロールを作成できます。たとえば、ヘルプデスクロールをコピーして、ダッシュボードまたはフィルターページを表示する権限を含めることができます。

カスタムロールのDirector権限を選択します。これには以下が含まれます。

- マシン上で実行中のアプリケーションの強制終了を実行する
- マシン上で実行中のプロセスの強制終了を実行する
- マシン上でリモートアシスタンスを実行する
- ユーザープロファイルをリセットする
- クライアント詳細ページを表示
- ダッシュボードページの表示
- フィルターページを表示する
- マシン詳細ページを表示
- トレンドページの表示
- ユーザー詳細ページを表示

この例では、シャドウイング（マシン上でリモートアシスタンスを実行する）が無効になっています。



権限は、UIで適用可能になるために他の権限に依存する場合があります。たとえば、**マシン上で実行中のアプリケーションの強制終了を実行する**権限を選択すると、ロールに権限があるパネルでのみ**アプリケーションの終了**機能が有効になります。次のパネル権限を選択できます。

- フィルターページを表示する
- ユーザー詳細ページを表示する
- 「マシンの詳細」ページを表示
- 「クライアントの詳細」ページを表示

さらに、他のコンポーネントの権限リストから、デリバリーグループの以下の権限を検討してください。

- デリバリーグループのメンバーシップを使用して、マシンのメンテナンスモードを有効/無効にする。
- デリバリーグループのメンバーシップを使用して、Windowsデスクトップマシンで電源操作を実行する。
- デリバリーグループのメンバーシップを使用して、マシンでセッション管理を実行する。

Directorのセキュアな展開

この記事では、Directorの展開および構成時にシステムセキュリティに影響を与える可能性のある領域について説明します。

Directorの通信

本番環境では、Directorとサーバー間でやり取りされるデータを保護するためにHTTPSプロトコルを使用します。HTTPSは、強力なデータ暗号化を提供するためにトランスポート層セキュリティ（TLS）プロトコルを使用します。

> **注：**
>
> - Citrix®は、イントラネットネットワーク内でのDirectorコンソールへのアクセスを制限することを強く推奨します。
> - Citrixは、本番環境でDirectorへの保護されていない接続を有効にしないことを強く推奨します。
> - TLS 1.2以降を使用してください。レガシーTLSまたはSSLは使用しないでください。

> ユーザーのWebブラウザーとDirector間の通信を保護するには、Web StudioおよびDirectorでTLSを有効にするを参照してください。

DirectorとCitrix Virtual Apps and Desktopsサーバー間の通信（監視およびレポート用）を保護するには、「オンプレミスMonitor OData APIアクセスを保護する」を参照してください。

DirectorとCitrix ADC間の通信（Citrix Insight用）を保護するには、「ネットワーク分析を構成する」ときに、接続の種類としてHTTPSを選択します。

Microsoft Internet Information Services (IIS) を構成する

Directorを制限されたIIS構成で構成できます。

アプリケーションプールのリサイクル制限

Directorは、**Director**という名前のアプリケーションプールを使用します。アプリケーションプールで次のアプリケーションプールのリサイクル制限を設定できます。

- 仮想メモリ制限: 4,294,967,295
- プライベートメモリ制限: StoreFront™サーバーの物理メモリのサイズ
- 要求制限: 4,000,000,000

ファイル名拡張子

インストール中、Directorは次の拡張子のみを許可するように要求フィルタリングを構成します。

- .

- .aspx
- ．css
- ．eot
- .html ファイル
- ．ico
- .js
- ．png
- ．svc
- ．svg
- 「.gif」
- .json ファイル
- .woff 拡張子
- .woff2 拡張子
- 「.ttf」

HTTP動詞

インストール中、Director は以下の動詞のみを許可するように要求フィルタリングを構成します。

- GET
- POST
- HEAD

IIS機能

Directorは以下のIISコンポーネントを必要としません。

- ISAPI拡張機能
- CGIプログラム
- FastCGIプログラム

これらのコンポーネントは削除できます。

.NET 信頼レベル

Director では、**.NET 信頼レベル**を**完全信頼**に設定する必要があります。.NET 信頼レベルを他の値に設定しないでください。

ユーザー権限の構成

Director のインストール時に、そのアプリケーションプールには次の権限が付与されます。

- **サービスとしてログオン**のログオン権限
- **プロセスに対するメモリクォータの調整**、**セキュリティ監査の生成**、および**プロセスレベルトークンの置き換え**の特権

上記の権限と特権は、アプリケーションプールが作成される際の通常のインストール動作です。

これらのユーザー権限を変更する必要はありません。これらの特権は Director では使用されず、自動的に無効になります。

Director のセキュリティ分離

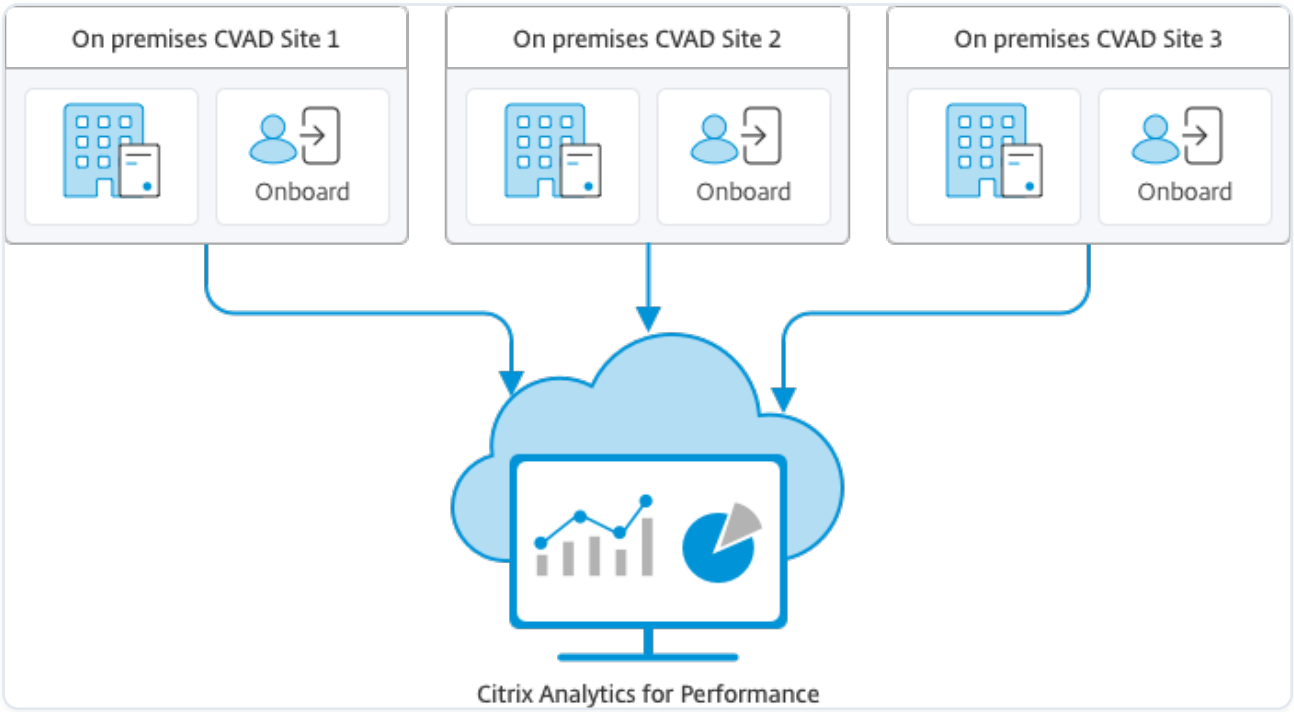
Director と同じ Web ドメイン（ドメイン名とポート）に任意の Web アプリケーションを展開できます。ただし、それらの Web アプリケーションのセキュリティリスクは、Director 展開のセキュリティを低下させる可能性があります。より高度なセキュリティ分離が必要な場合は、Citrix では Director を別の Web ドメインに展開することをお勧めします。

Citrix Analytics for Performance™ を使用したオンプレミスサイトの構成

Citrix Analytics for Performance (Performance Analytics) は、Citrix Analytics Cloud Service が提供する包括的なパフォーマンス監視ソリューションです。Performance Analytics は、パフォーマンスメトリックに基づいて構築された高度なインサイトと分析を提供します。Performance Analytics を使用すると、組織内の1つ以上のCitrix Virtual Apps and Desktops™サイトの使用状況とパフォーマンスメトリックを監視および表示できます。

Performance Analyticsの詳細については、Performance Analyticsの記事を参照してください。

サイトから Citrix Cloud™ 上の Citrix Analytics for Performance にパフォーマンスデータを送信して、その高度なパフォーマンス分析機能を活用できます。Performance Analytics を表示および使用するには、まず **Director** の **Analytics** タブからオンプレミスサイトを Citrix Analytics for Performance で構成する必要があります。



Performance Analyticsは安全な方法でデータにアクセスし、Citrix Cloudからオンプレミス環境にデータが転送されることはありません。

前提条件

Director から Citrix Analytics for Performance を構成するために、新しいコンポーネントをインストールする必要はありません。以下の要件が満たされていることを確認してください。

- Delivery Controller と Director がバージョン 1912 CU2 以降であること。詳細については、機能互換性マトリックスを参照してください。

注:

- Delivery Controller が Microsoft .NET Framework バージョン 4.8 より前のバージョンを実行している場合、Director からオンプレミスサイトを Citrix Analytics for Performance で構成すると失敗する可能性があります。回避策として、Delivery Controller の .NET Framework をバージョン 4.8 にアップグレードしてください。LCM-9255。
- Citrix Virtual Apps and Desktops バージョン 2012 を実行しているオンプレミスサイトを Director から Citrix Analytics for Performance で構成すると、数時間後または Delivery Controller の Citrix Monitor Service の再起動後に構成が失敗する可能性があります。この場合、Analytics タブには「未接続」ステータスが表示されます。回避策として、Delivery Controller のレジストリに Encryption フォルダーを作成します。場所: HKEY_LOCAL_MACHINE\Software\Citrix\XDservices\Monitor、フォルダー名:

> Encryption。CitrixMonitor アカウントが Encryption フォルダーに対してフルコントロールアクセス権を持っていることを確認します。Citrix Monitor Service を再起動します。DIR-14324。

- この構成を実行するための **Analytics** タブへのアクセスは、フル管理者のみが利用できます。
- Performance Analytics がパフォーマンスメトリックにアクセスするには、すべての Delivery Controller および Director がインストールされているマシンでアウトバウンドインターネットアクセスが利用可能である必要があります。具体的には、次の URL へのアクセス可能性を確認してください。
  - Citrix キー登録: `https://*.citrixnetworkapi.net/`
  - シトリックスクラウド: `https://*.citrixworkspacesapi.net/`
  - シトリックスアナリティクス: `https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/` Delivery ControllerとDirectorマシンがイントラネット内にあり、アウトバウンドインターネットアクセスがプロキシサーバー経由である場合、以下を確認してください。
- プロキシサーバーは、上記のURLリストを許可する必要があります。
- Director web.config および citrix.monitor.exe.config ファイルに次の構成を追加します。この構成は **configuration** タグ内に追加してください。

```
&lt;system.net>

    &lt;defaultProxy>

        &lt;proxy  usesystemdefault = "false"  proxyaddress = "http://
&lt;your_proxyserver_address>:80" bypassonlocal = "true"  />

    &lt;/defaultProxy>

&lt;/system.net>
```

  - Director web.config は、Director がインストールされているマシンの `C:\inetpub\wwwroot\Director\web.config` にあります。
  - citrix.monitor.exe.config は、Delivery Controller がインストールされているマシンの `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` にあります。

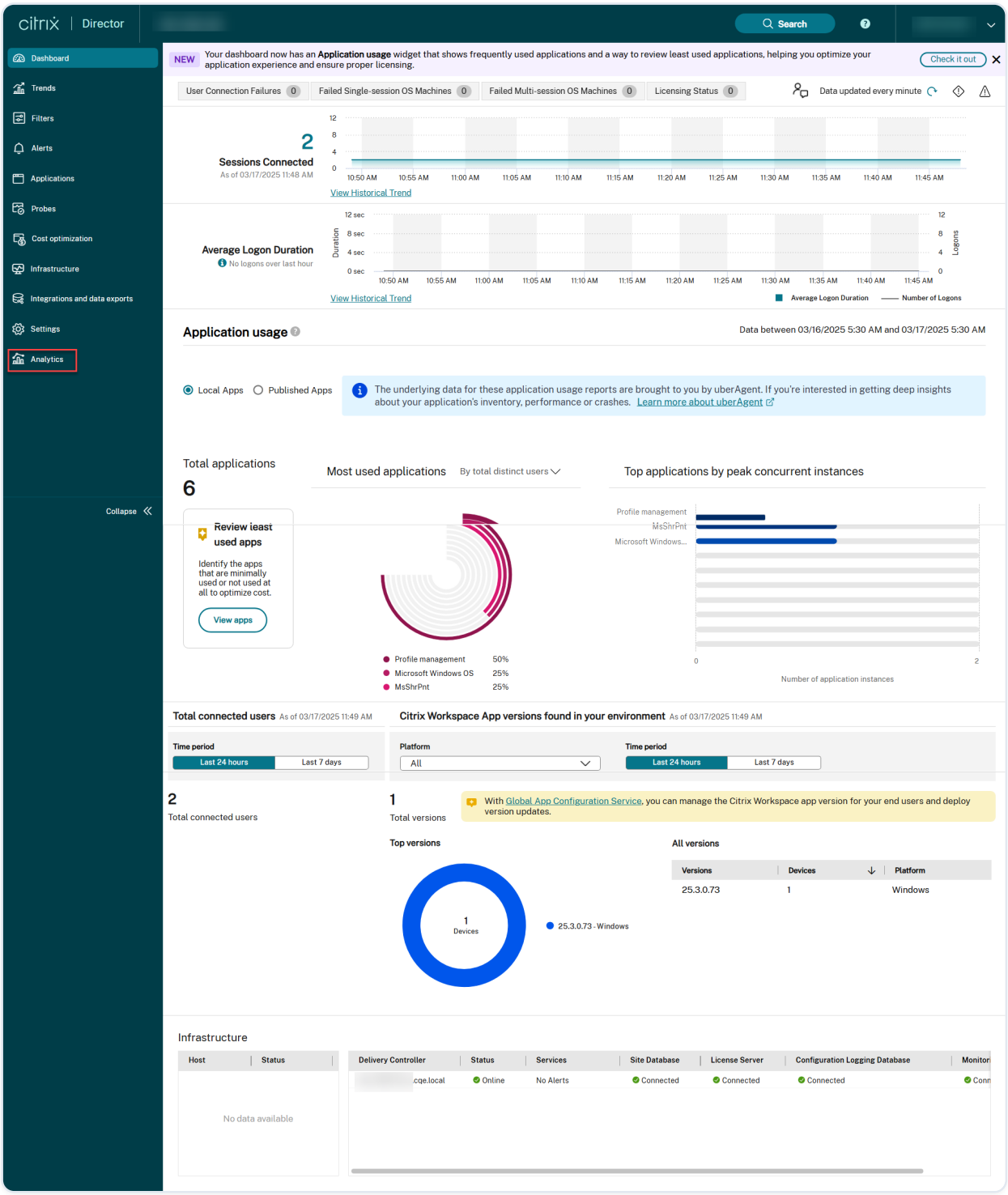
この設定は、IIS上のMicrosoftによって提供されます。詳細については、`https://docs.microsoft.com/ja-jp/dotnet/framework/network-programming/proxy-configuration`を参照してください。 構成ファイルの**defaultproxy**フィールドは、DirectorおよびMonitor Serviceのアウトバウンドアクセスを制御します。Performance Analyticsとの構成および通信には、**defaultproxy**フィールドを**true**に設定する必要があります。有効なポリシーによってこのフィールドがfalseに設定されている可能性があります。この場合、手動でフィールドをtrueに設定する必要があります。変更を行う前に構成ファイルのバックアップを取ってください。変更を適用するには、Delivery Controller™上の監視サービスを再起動してください。

- Citrix Analytics for PerformanceのCitrix Cloudエンタイトルメントがアクティブであること。
- Citrix Cloudアカウントが、製品登録エクスペリエンスに対する権限を持つ管理者アカウントであること。管理者権限の詳細については、管理者権限の変更を参照してください。

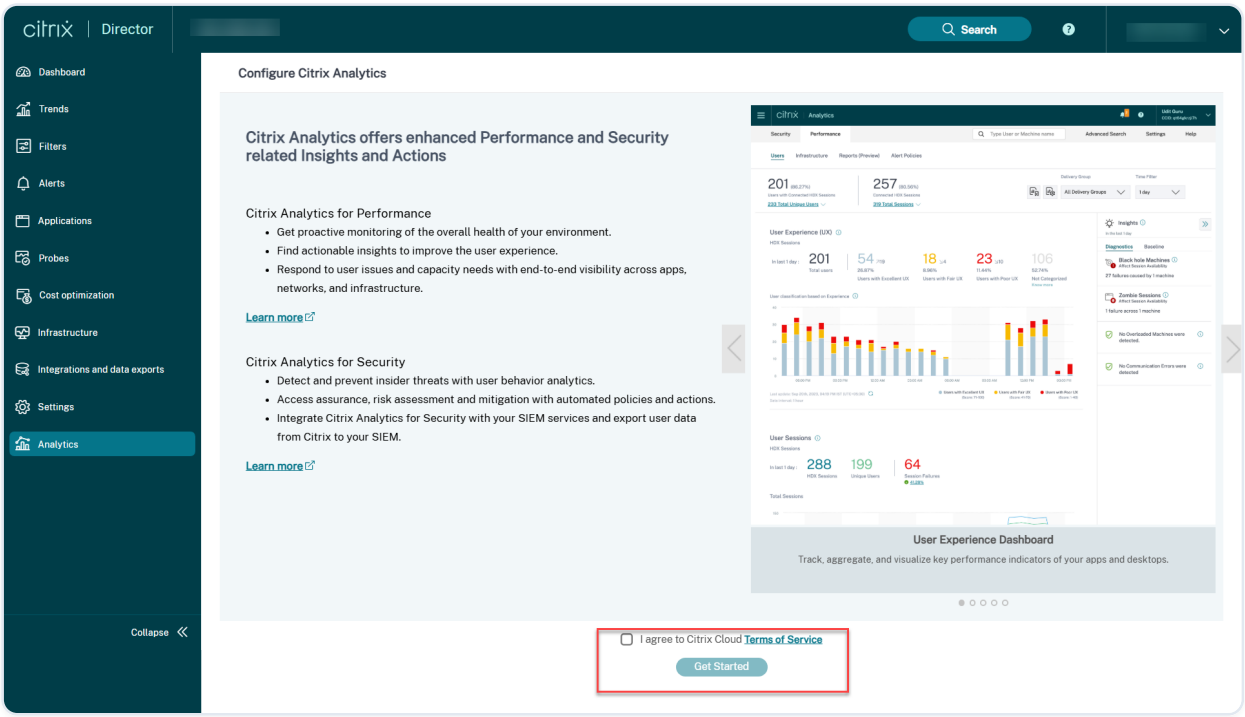
構成手順

前提条件を確認したら、次の手順を実行します。

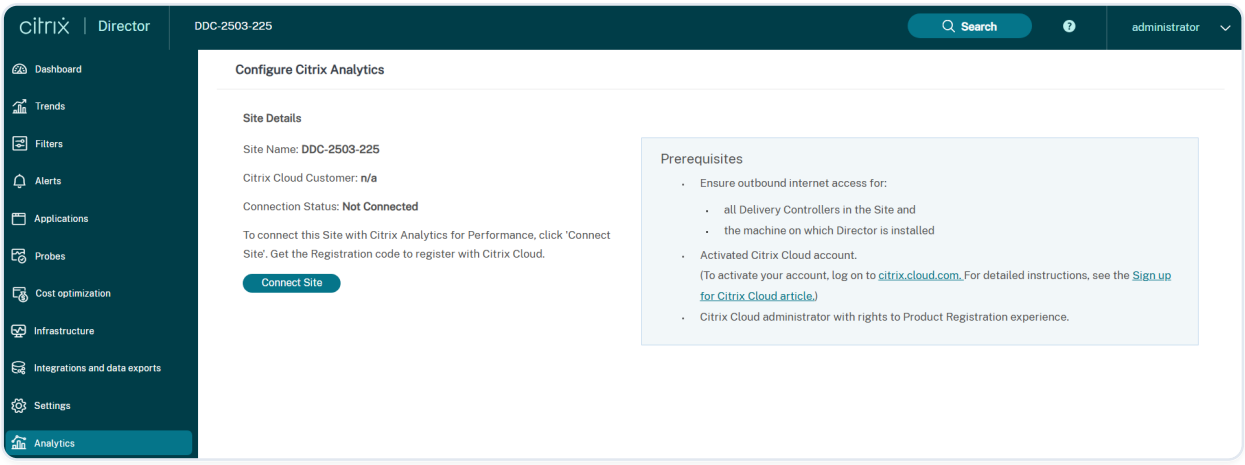
1. Director にフル管理者としてサインインし、Performance Analytics で構成するサイトを選択します。Director ダッシュボードページが表示されます。



2. **Analytics**タブをクリックします。**Citrix Analyticsの構成**ページが表示されます。

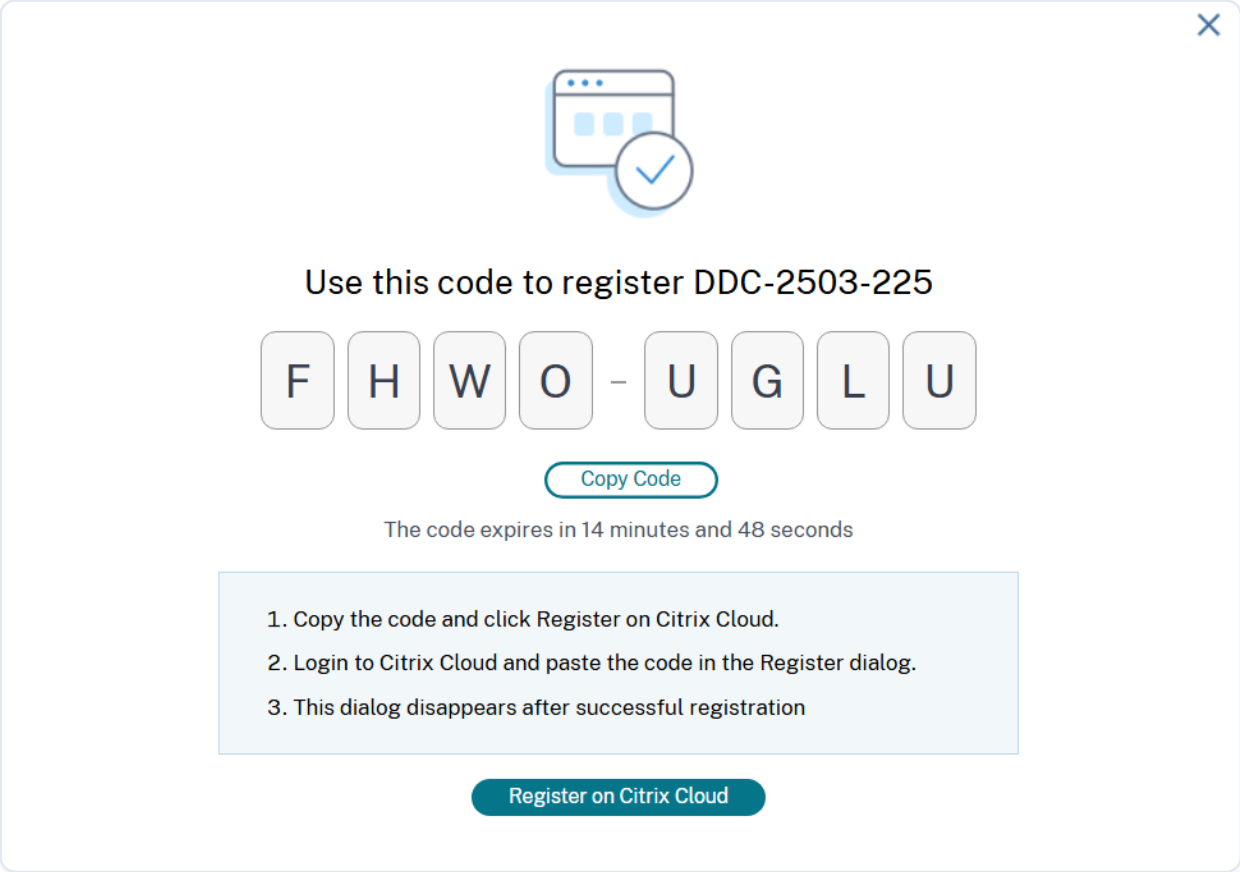


3. 手順を確認し、サービス利用規約を選択してから、**開始する**をクリックします。**サイトの詳細**ページが表示されます。



4. 前提条件を確認し、それらが満たされていることを確認します。サイトの詳細を確認します。
5. 構成プロセスを開始するには、**サイトを接続**をクリックします。

   このサイトをCitrix Cloudに登録するために使用する、一意の8桁の登録コードが生成されます。



6. **コードをコピー**をクリックしてコードをコピーし、**Citrix Cloudに登録**をクリックします。Citrix Cloudの登録URLにリダイレクトされます。
7. Citrix Cloudの資格情報でサインインし、顧客を選択します。
8. コピーした登録コードをCitrix Cloudの製品登録ページに貼り付けます。登録するには**続行**をクリックします。登録の詳細を確認し、**登録**をクリックします。

   「Citrix Cloudに登録」(/en-us/citrix-virtual-apps-desktops/2511/media/dir-onboarding6.png)

   オンプレミスサイトがCitrix Cloudに登録されます。
9. **Director**の**Analytics**タブで、**Analyticsに移動**をクリックします。

   「Analyticsに移動」(/en-us/citrix-virtual-apps-desktops/2511/media/dir-onboarding7.png)

   Performance Analyticsがブラウザの新しいタブで開きます。 (/en-us/citrix-virtual-apps-desktops/2511/media/dir-onboarding-pa-dashboard.png)

   Citrix Cloudセッションの有効期限が切れている場合、Citrix.comまたはMy Citrixアカウントのログオンページにリダイレクトされることがあります。
10. Performance Analyticsに複数のサイトを登録するには、Directorから各サイトについて、前述の構成手順を繰り返します。構成されたすべてのサイトのメトリックは、Performance Analyticsダッシュボードに表示されます。

サイトごとに複数のDirectorインスタンスが実行されている場合は、いずれか1つのDirectorインスタンスから構成します。サイトに接続されている他のすべてのDirectorインスタンスは、構成プロセスの後、次回の更新時に更新されます。

11. Citrix Cloudからサイトを切断するには、 をクリックします。このオプションは、既存の構成を削除します。

> **注:**
>
> サイトを初めて構成する場合、サイトからのイベントの処理には時間がかかる場合があります（約1時間）。そのため、Performance Analyticsダッシュボードにメトリックが表示されるまでに遅延が生じます。その後、イベントは定期的に更新されます。
>
> 切断後、新しいアカウントからのイベントが送信されるまで、古いアカウントからのデータ送信はしばらく継続されます。データ送信が停止してから約1時間、古いアカウントに関連する分析は、Performance Analyticsダッシュボードに表示されたままになります。
>
> Citrix Analyticsサービスへのエンタイトルメントの有効期限が切れると、サイトメトリックがPerformance Analyticsへの送信を停止するまでに最大1日かかります。

LTSR展開用のDirectorの独立リリース

LTSR展開用のDirectorの独立リリースにより、互換性のあるLTSR環境でCitrix®環境におけるトラブルシューティングと監視を強化するための最新のDirector機能にアクセスするオプションが提供されるようになりました。この機能により、2402 LTSR展開で最新のDirectorバージョンを使用できます。また、LTSR発表後にリリースされた機能に、アプリケーション配信インフラストラクチャに影響を与えることなくアクセスできます。

スタンドアロンインストーラーには、モニターサービス、Directorサービス、およびモニターSnap-inの最新の.msiが含まれています。これらの新しい.msiファイルを使用すると、2402 LTSR CU1を現在のリリース機能でアップグレードできます。

2402 LTSRリリース以降の現在のリリースに含まれるDirector機能については、以下を参照してください。

- シトリックス バーチャル アプリケーションズ アンド デスクトップス 2407 リリース
- シトリックス バーチャル アプリケーションズ アンド デスクトップス 2411 リリース

最小バージョンのVDAでのDirectorの特定の機能の詳細については、Directorバージョンマトリックスを参照してください。

利点

- **新機能へのアクセス**: 2402 LTSR発表後にリリースされたDirector機能（Citrix Virtual Apps and Desktops™ 2407および2411累積リリース（CR）の機能を含む）にアクセスできます。
- **ターゲットを絞ったアップグレード**: LTSRインフラストラクチャの残りの部分に影響を与えることなく、Directorおよび監視サービスコンポーネントのみをアップグレードします。
- **LTSR互換性**: 最新のDirector機能強化の恩恵を受けながら、LTSR環境を維持します。
- **ロールバックオプション:** 必要に応じて、以前のDirectorバージョンにロールバックする柔軟性があります。

重要な考慮事項

アップグレードされたDirectorコンポーネントはLTSR互換ですが、LTSRコアコンポーネントのサポート対象ではありません。ただし、LTSRインフラストラクチャの残りの部分は、既存のサポートを維持します。

前提条件

1. `Director2411.zip`ファイルをCitrixダウンロードページからダウンロードします。
2. インストーラーファイルを解凍すると、次のインストーラーが見つかります。
    - DesktopDirector.msi
    - Monitor_PowerShellSnapIn.msi
    - Monitor_Service_x64.msi
3. Citrix Virtual Apps™ and Desktops 2402 LTSR または 2402 LTSR CU1 サイトを使用していることを確認してください。

概要

Citrix Virtual Apps and Desktops 2402 LTSR CU1 サイトを最新のCurrent Releaseの機能でアップグレードするには、次の手順に従います。

1. **データベースをバックアップする**: アップグレードする前に、監視データベースをバックアップしてください。アップグレードプロセスではデータベースも更新されるため、この手順は非常に重要です。
2. **サイトをアップグレードする**: 現在のリリースで新しい機能を取り込むために、サイトのアップグレードを進めます。

3. **ロールバックオプション**: アップグレードされたサイトの使用を継続しないと決定した場合、ロールバック手順を使用して以前のサイトに戻すことができます。

アップグレード手順

1. 監視データベースのバックアップを取ります。
2. `Director2411.zip`ファイルをCitrixダウンロードページからダウンロードします。
3. インストーラーファイルを解凍すると、次のインストーラーが見つかります。
   - DesktopDirector.msi
   - Monitor_PowerShellSnapIn.msi
   - Monitor_Service_x64.msi
4. .msiファイルのある場所に移動します。
5. コマンドラインを使用してMonitorサービスをインストールします。

```
msiexec /i Monitor_service_x64 REINSTALLMODE=amus /l*v <logfile path
and name>
```

6. 画面の指示に従ってウィザードを完了します。
7. コマンドラインを使用してDirectorサービスをインストールします。

```
msiexec /i DesktopDirector /l*v <logfile path and name>
```

8. 画面の指示に従ってウィザードを完了します。
9. コマンドラインを使用して次のコマンドを実行します。

```
DirectorConfig.exe /UPGRADE
```

10. コマンドラインを使用してモニター スナップインをインストールします。

```
msiexec /i Monitor_PowershellSnapin_x64.msi
```

11. すべての.msiインストールが完了したら、Program Files内のモニターサービスに移動し、コマンドを実行します。

```
Citrix.Monitor.exe /upgrade /enablefeatures
```

12. Citrix Site Managerを開き、**自動サイトアップグレード**オプションを選択して、アップグレードワークフローを完了します。
13. Directorにサインインして、新機能が利用可能であることを確認します。

ロールバック手順

1. 監視データベースのバックアップを必ず取得してください。
2. 「dbollback.zip」という名前のデータベースロールバックスクリプトをダウンロードして実行します。
3. コントロールパネルから以下をアンインストールします。
   - **Citrix Monitor Service PowerShell Snap-in- x64**を選択し、**アンインストール**をクリックします。
   - **Citrix Monitor Service - x64**を選択し、**アンインストール**をクリックします。
   - **Citrix Director**を選択し、**アンインストール**をクリックします。
4. すでに取得済みのバックアップから監視データベースを復元します。詳細については、ナレッジ共有記事CTX135207を参照してください。
5. Citrix Virtual Apps and Desktopsインストーラーを使用して、Delivery ControllerとDirectorを再インストールします。詳細については、install core componentsを参照してください。

   または、,

次のコマンドを使用してコンポーネントを再インストールすることもできます。

```
XenDesktopServerSetup.exe /components controller,director /
configure_firewall /quiet
```

1. インストールが完了したら、**Open Citrix Site Manager**チェックボックスをオンにします。
2. Citrix Site Managerで推奨されている場合は、サイトのアップグレードを実行します。

サポートとコンプライアンス

サポート

- Directorの累積リリース（CR）バージョンはLTSR互換ですが、LTSR準拠ではありません。

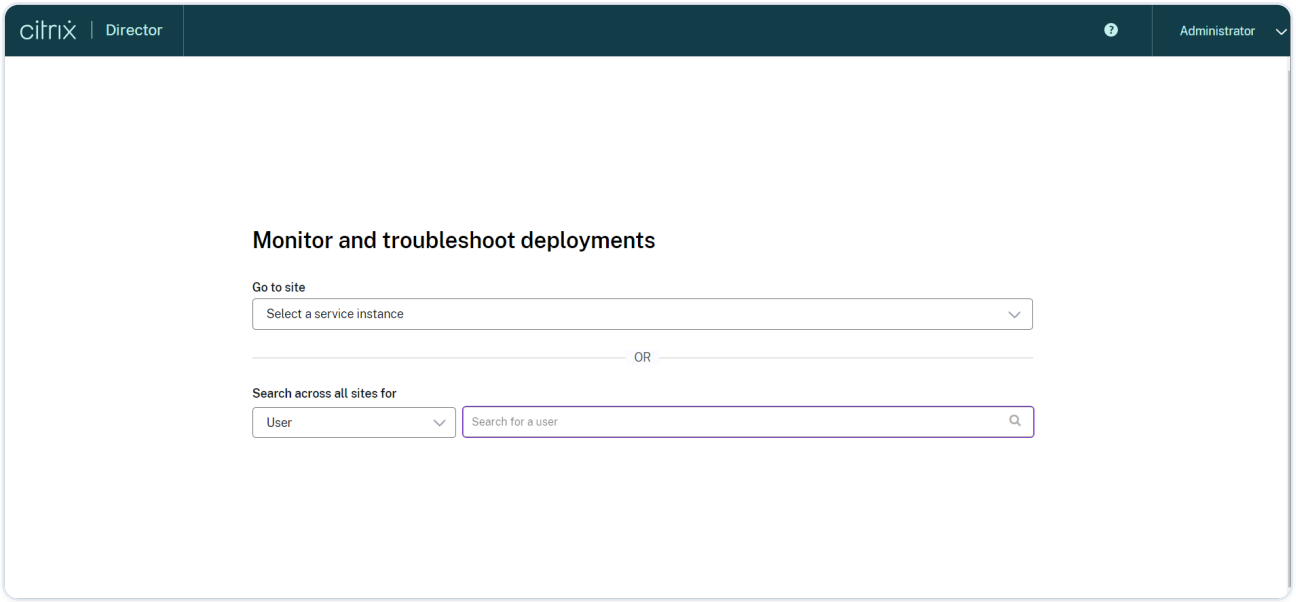
- アップグレード後、必要なすべてのサポートチケットとバグ修正は、Directorの次の累積リリース（CR）に追加されます。
- 変更または修正を含むCRは、以下の累積更新プログラム（CU）で利用可能です。

508/WCAG 2.1

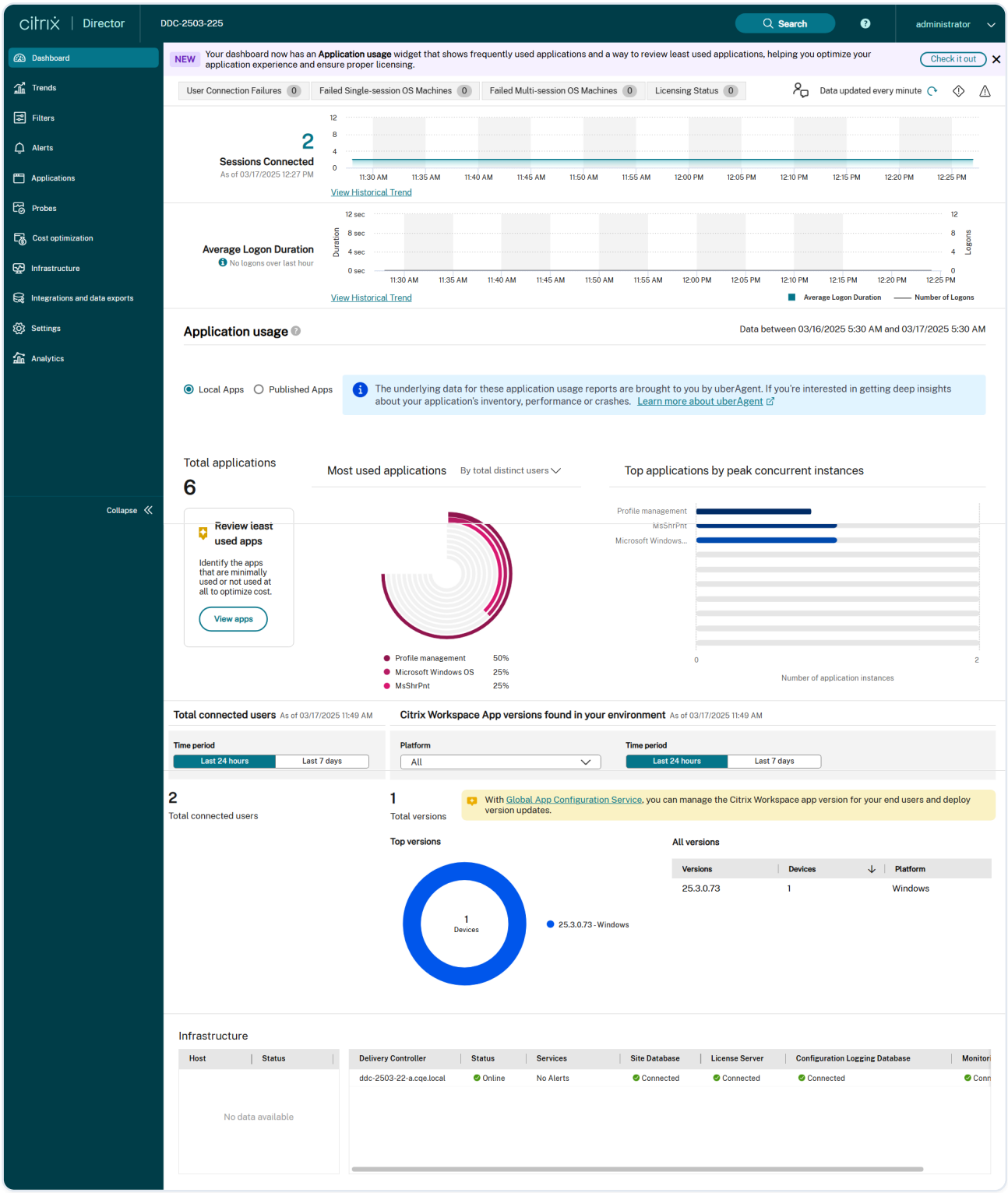
- 508/WCAG 2.1準拠義務のあるお客様には、すべてのコアコンポーネントのLTSRバージョンを引き続き使用することをお勧めします。

サイト分析

Director を使用して、展開の健全性を監視できます。オンボードされたすべてのサイトでユーザー、エンドポイント、またはマシンを検索することで、パフォーマンスの問題をトラブルシューティングできます。



完全な管理者権限を持つユーザーがDirectorを開くと、ダッシュボードにはサイトの健全性と使用状況を監視するための一元的な場所が提供されます。



現在障害がなく、過去60分間に障害が発生していない場合、パネルは折りたたまれたままになります。障害が発生すると、特定の障害パネルが自動的に表示されます。

> **注:**
>
> 組織のライセンスと管理者権限によっては、一部のオプションまたは機能が利用できない場合があります。

Director ダッシュボードのパネル

ユーザー接続障害

過去60分間の接続障害。合計数の横にあるカテゴリをクリックすると、その種類の障害のメトリックが表示されます。隣接するテーブルでは、その数がデリバリーグループ別に分類されています。接続障害には、アプリケーション制限に達したことによる障害が含まれます。アプリケーション制限の詳細については、「アプリケーション」を参照してください。

失敗したシングルセッションOSマシンまたは失敗したマルチセッションOSマシン

過去60分間の合計障害数（デリバリーグループ別）。障害は、起動失敗、起動中に停止、未登録などの種類別に分類されます。マルチセッションOSマシンでは、障害には最大負荷に達したマシンも含まれます。

ライセンスステータス

ライセンスサーバーアラートには、ライセンスサーバーから送信されたアラートと、アラートを解決するために必要なアクションが表示されます。これにはライセンスサーバーバージョン11.12.1以降が必要です。デリバリーコントローラーアラートには、コントローラーから見たライセンス状態の詳細が表示され、コントローラーによって送信されます。これにはXenApp 7.6またはXenDesktop 7.6以降のコントローラーが必要です。アラートのしきい値はStudioで設定できます。**Delivery Controllers** > **Details** > **Product Editions** > **PLT**に表示されるライセンスステータスは、**Premium**を示し、**Platinum**ではありません。

猶予状態

Directorは、以下のいずれかの猶予状態を表示します。この情報は、Delivery Controllerから取得されます。

1. **非アクティブ:** いずれのライセンスキャッシュモードでもありません。通常のライセンス制限が適用されます。
2. **緊急猶予:** ライセンスサーバーに到達できない場合、または接続を仲介している間にライセンス情報を取得できない場合に有効になります。ユーザーには影響ありません。Directorに表示されるエラーは、ライセンスサーバーに到達可能になるまで解除できません。
3. **猶予期限切れ:** 緊急ライセンスキャッシュモードの有効期限が切れました。

詳細については、ライセンスの超過 および ライセンスバーストモード を参照してください。

接続されたセッション

過去60分間のすべてのデリバリーグループにわたる接続セッション。

平均ログオン時間

過去60分間のログオンデータ。左側の大きな数字は、1時間あたりの平均ログオン時間です。XenDesktop 7.0より前のVDAのログオンデータは、この平均には含まれません。詳しくは、「ユーザーログオンの問題の診断」を参照してください。

インフラストラクチャ

サイトのインフラストラクチャ（ホストとController）を一覧表示します。XenServerまたはVMwareのインフラストラクチャの場合、パフォーマンスアラートを表示できます。たとえば、XenCenterを構成して、管理対象サーバーまたは仮想マシンでCPU、ネットワークI/O、またはディスクI/Oの使用率が指定されたしきい値を超えたときにパフォーマンスアラートを生成できます。デフォルトでは、アラートの繰り返し間隔は60分ですが、これも構成できます。詳細については、「XenServer製品ドキュメント」のXenCenterパフォーマンスアラートのセクションを参照してください。

> **注:**
>
> 特定のメトリックのアイコンが表示されない場合、そのメトリックが使用しているホストの種類でサポートされていないことを示します。たとえば、System Center Virtual Machine Manager（SCVMM）ホスト、AWS、CloudStackでは、正常性情報は利用できません。

> 以下のオプション（次のセクションで説明）を使用して、問題のトラブルシューティングを続行します。

- ユーザーマシンの電源を制御する
- マシンへの接続を防止する

接続ユーザーの合計数

過去24時間または過去7日間に少なくとも1つの接続があったユーザーの数を表示します。このパネルは、管理者が導入傾向を経営陣に示すのに役立ちます。

環境内で検出されたCitrix Workspace™アプリのバージョン

組織全体で使用されているCitrix Workspaceアプリのバージョン概要を提供します。これにより、異なるバージョンを使用しているデバイスの数を示すことで、バージョンを統一するのに役立ちま

す。デフォルトでは、すべてのOSプラットフォームのCitrix Workspaceアプリのバージョンデータが表示されます。「**Platform drop-down**」リストから対応するOSを選択することで、特定のOSプラットフォームのバージョンデータを表示できます。

セッションの監視

セッションが切断されても、セッションはアクティブなままでアプリケーションは実行され続けますが、ユーザーデバイスはサーバーと通信しなくなります。

アクション	説明
ユーザーの現在接続されているマシンまたはセッションを表示する	アクティビティマネージャーとユーザー詳細ビューから、ユーザーの現在接続されているマシンまたはセッション、およびこのユーザーがアクセスできるすべてのマシンとセッションのリストを表示します。このリストにアクセスするには、ユーザータイトルバーのセッションスイッチャーアイコンをクリックします。詳細については、「セッションの復元」を参照してください。
すべてのデリバリーグループにわたる接続セッションの総数を表示する	ダッシュボードの「**Sessions Connected**」ペインで、過去60分間のすべてのデリバリーグループにわたる接続セッションの総数を表示します。次に、大きな合計数をクリックすると、フィルタービューが開き、選択したデリバリーグループと範囲、およびデリバリーグループ全体の使用状況に基づいてグラフィカルなセッションデータを表示できます。
アイドル状態のセッションを終了する	「セッションフィルター」ビューには、すべてのアクティブなセッションに関連するデータが表示されます。関連ユーザー、デリバリーグループ、セッション状態、およびしきい値時間より長いアイドル時間に基づいてセッションをフィルターします。フィルターされたリストから、ログオフまたは切断するセッションを選択します。詳しくは、「アプリケーションのトラブルシューティング」を参照してください。

アクション	説明
より長期間のデータを表示する	「傾向」ビューで、**［セッション］**タブを選択すると、より長期間にわたる接続済みセッションと切断済みセッションのより具体的な使用状況データ（つまり、過去60分より前のセッション合計）をドリルダウンして表示できます。この情報を表示するには、**［履歴傾向の表示］**をクリックします。

注:

ユーザーデバイスが、バージョン7より前のVDAやLinux VDAなどのレガシーVirtual Delivery Agent（VDA）を実行している場合、Directorはセッションに関する完全な情報を表示できません。代わりに、情報が利用できないことを示すメッセージが表示されます。

デスクトップ割り当て規則の制限: Web Studioでは、異なるユーザーまたはユーザーグループに対して複数のデスクトップ割り当て規則（DAR）をデリバリーグループ内の単一のVDAに割り当てることができます。StoreFront™は、ログインユーザーのDARに従って、対応する**表示名**で割り当てられたデスクトップを表示します。ただし、DirectorはDARをサポートしておらず、ログインユーザーに関係なく、デリバリーグループ名を使用して割り当てられたデスクトップを表示します。その結果、Directorで特定のデスクトップをマシンにマッピングすることはできません。 StoreFrontに表示される割り当てられたデスクトップを、Directorに表示されるデリバリーグループ名にマッピングするには、次のPowerShellコマンドを使用します。

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq
"\&lt;Name on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property
Name, Uid
```

セッション転送プロトコル

［セッションの詳細］パネルで、現在のセッションのHDX接続タイプで使用されている転送プロトコルを表示します。この情報は、VDAバージョン7.13以降で起動されたセッションで利用できます。

転送プロトコル (/en-us/citrix-virtual-apps-desktops/2511/media/sessions-transport-protocol.png)

- **HDX™** 接続タイプの場合、,
  - HDX接続にEDTが使用されている場合、プロトコルは **UDP** と表示されます。
  - HDX接続にTCPが使用されている場合、プロトコルは **TCP** と表示されます。
- **RDP**接続タイプの場合、プロトコルは**n/a**と表示されます。

アダプティブトランスポートが構成されている場合、セッション転送プロトコルは、ネットワークの状態に基づいてEDT（UDP経由）とTCPの間で動的に切り替わります。EDTを使用してHDXセッションを確立できない場合、TCPプロトコルにフォールバックします。

アダプティブトランスポートの構成について詳しくは、「アダプティブトランスポート」を参照してください。

レポートのエクスポート

定期的な使用状況および容量管理レポートを生成するために、トレンドデータをエクスポートできます。エクスポートは、PDF、Excel、およびCSVレポート形式をサポートしています。PDFおよびExcel形式のレポートには、グラフと表として表現されたトレンドが含まれます。CSV形式のレポートには、ビューを生成するために処理できる、またはアーカイブできる表形式のデータが含まれます。

レポートをエクスポートするには：

1. **トレンド**タブに移動します。
2. フィルター条件と期間を設定し、**適用**をクリックします。傾向グラフと表にデータが入力されます。
3. **エクスポート**をクリックし、レポートの名前と形式を入力します。

Directorは、選択したフィルター条件に基づいてレポートを生成します。フィルター条件を変更する場合は、**エクスポート**をクリックする前に**適用**をクリックしてください。

> **注:**
>
> 大量のデータをエクスポートすると、Directorサーバー、Delivery Controller、およびSQLサーバーのメモリとCPU消費量が大幅に増加します。最適なエクスポートパフォーマンスを達成するために、サポートされる同時エクスポート操作の数とエクスポートできるデータ量は、デフォルトの制限に設定されています。

サポートされるエクスポート制限

エクスポートされたPDFおよびExcelレポートには、選択されたフィルター条件に対する完全なグラフィカルチャートが含まれます。ただし、すべてのレポート形式の表形式データは、テーブル内の行数またはレコード数のデフォルト制限を超えると切り捨てられます。サポートされるレコードのデフォルト数は、レポート形式に基づいて定義されます。

Internet Information Services (IIS) のDirectorアプリケーション設定を構成することで、デフォルトの制限を変更できます。

レポート形式	サポートされるレコードのデフォルト数	DIRECTORアプリケーション設定のフィールド	サポートされるレコードの最大数
PDF	500	UI.ExportPdfDrilldownLimit	5000
エクセル	100,000	UI.ExportExcelDrilldownLimit	100,000
CSV	100,000 (「**セッション**」タブでは 10,000,000)	UI.ExportCsvDrilldownLimit	100,000

エクスポートできるレコード数の制限を変更するには：

1. IIS Managerコンソールを開きます。
2. Default website の下の Director ウェブサイトに移動します。
3. をダブルクリックします。
4. 必要に応じて、UI.ExportPdfDrilldownLimit、UI.ExportExcelDrilldownLimit、または UI.ExportCsvDrilldownLimit フィールドの設定を編集または追加します。

これらのフィールド値を に追加すると、デフォルト値が上書きされます。

> **警告:**
>
> サポートされている最大レコード数を超えるフィールド値を設定すると、エクスポートのパフォーマンスに影響を与える可能性があり、サポートされていません。

エラー処理

このセクションでは、エクスポート操作中に発生する可能性のあるエラーの対処方法について説明します。

- **Director がタイムアウトしました**

このエラーは、ネットワークの問題、Director サーバーまたは Monitor Service でのリソース使用量の増加が原因で発生する可能性があります。

デフォルトのタイムアウト期間は 100 秒です。Director Service のタイムアウト期間を長くするには、Internet Information Services (IIS) の Director Application Settings で **Connector.DataServiceContext.Timeout** フィールドの値を設定します。

1. IIS マネージャーコンソールを開きます。
2. Default website の下の Director ウェブサイトに移動します。
3. をダブルクリックします。
4. **Connector.DataServiceContext.Timeout** の値を編集します。

- **Monitorがタイムアウトしました**

このエラーは、ネットワークの問題、またはモニターサービスやSQLサーバーでのリソース使用率の高さが原因で発生する可能性があります。

モニターサービスのタイムアウト期間を延長するには、デリバリーコントローラーで次のPowerShellコマンドを実行します。

```
asnp Citrix.*

Get-MonitorConfiguration

Set-MonitorConfiguration -MonitorQueryTimeoutSeconds &lt;timeout value>
```

- **最大同時エクスポートまたはプレビュー操作が進行中**

Directorは、エクスポートまたはプレビューの1つのインスタンスをサポートします。「**最大同時エクスポートまたはプレビュー操作が進行中**」エラーが発生した場合は、次のエクスポート操作を後でもう一度試してください。

同時エクスポートまたはプレビュー操作の数を増やすことは可能ですが、これはDirectorのパフォーマンスに影響を与える可能性があり、サポートされていません。

1. IISマネージャーコンソールを開きます。
2. デフォルトのWebサイトの下にあるDirector Webサイトに移動します。
3. **アプリケーション設定**をダブルクリックします。
4. 値**UI.ConcurrentExportLimit**を編集します。

- **Directorのディスク容量不足**

各エクスポート操作には、Windows Tempフォルダーに最大2 GBのハードディスク容量が必要です。Directorサーバーで空き容量を確保するか、ハードディスク容量を追加してから、エクスポートを再試行してください。

モニターのホットフィックス

特定のVDAマシン（物理またはVM）にインストールされているホットフィックスを表示するには、**マシン詳細**ビューを選択します。

ユーザーマシンの電源状態を制御する

Directorで選択したマシンの状態を制御するには、電源制御オプションを使用します。これらのオプションは、シングルセッションOSマシンで利用できますが、マルチセッションOSマシンでは利用できない場合があります。

> **注:**
>
> この機能は、物理マシンまたはリモートPCアクセスを使用するマシンでは利用できません。

コマンド	機能
再起動	VMの順序だった（ソフト）シャットダウンを実行し、VMを再起動する前に実行中のすべてのプロセスを個別に停止します。たとえば、Directorで「起動に失敗しました」と表示されるマシンを選択し、このコマンドを使用してそれらを再起動します。
強制再起動	シャットダウン手順を最初に実行せずにVMを再起動します。このコマンドは、物理

コマンド	機能
	サーバーのプラグを抜き、再度差し込んで電源を入れるのと同じように機能します。
シャットダウン	VMの順序だった（ソフト）シャットダウンを実行します。実行中のすべてのプロセスが個別に停止されます。
強制シャットダウン	シャットダウン手順を最初に実行せずにVMをシャットダウンします。このコマンドは、物理サーバーのプラグを抜くのと同じように機能します。これにより、実行中のすべてのプロセスが常にシャットダウンされるとは限らず、この方法でVMをシャットダウンするとデータが失われるリスクがあります。
サスペンド	実行中のVMを現在の状態で一時停止し、その状態をデフォルトのストレージリポジトリ上のファイルに保存します。このオプションを使用すると、VMのホストサーバーをシャットダウンし、その後、再起動してからVMを再開し、元の実行状態に戻すことができます。
再開	中断されたVMを再開し、元の実行状態に戻します。
開始	VMがオフのときに起動します（コールドスタートとも呼ばれます）。

電源制御アクションが失敗した場合、アラートにマウスを重ねると、失敗の詳細を示すポップアップメッセージが表示されます。

マシンへの接続を防止する

適切な管理者がイメージのメンテナンス作業を行っている間、一時的に新しい接続を防止するためにメンテナンスモードを使用します。

マシンでメンテナンスモードを有効にすると、無効にするまで新しい接続は許可されません。ユーザーが現在ログオンしている場合、すべてのユーザーがログオフするとすぐにメンテナンスモードが有効になります。ログオフしないユーザーには、マシンが特定の時間にシャットダウン

されることを通知するメッセージを送信し、電源制御を使用してマシンを強制的にシャットダウンします。

1. ユーザー詳細ビューから、またはフィルタービューでマシンのグループから、マシンを選択します。
2. **メンテナンスモード**を選択し、オプションをオンにします。

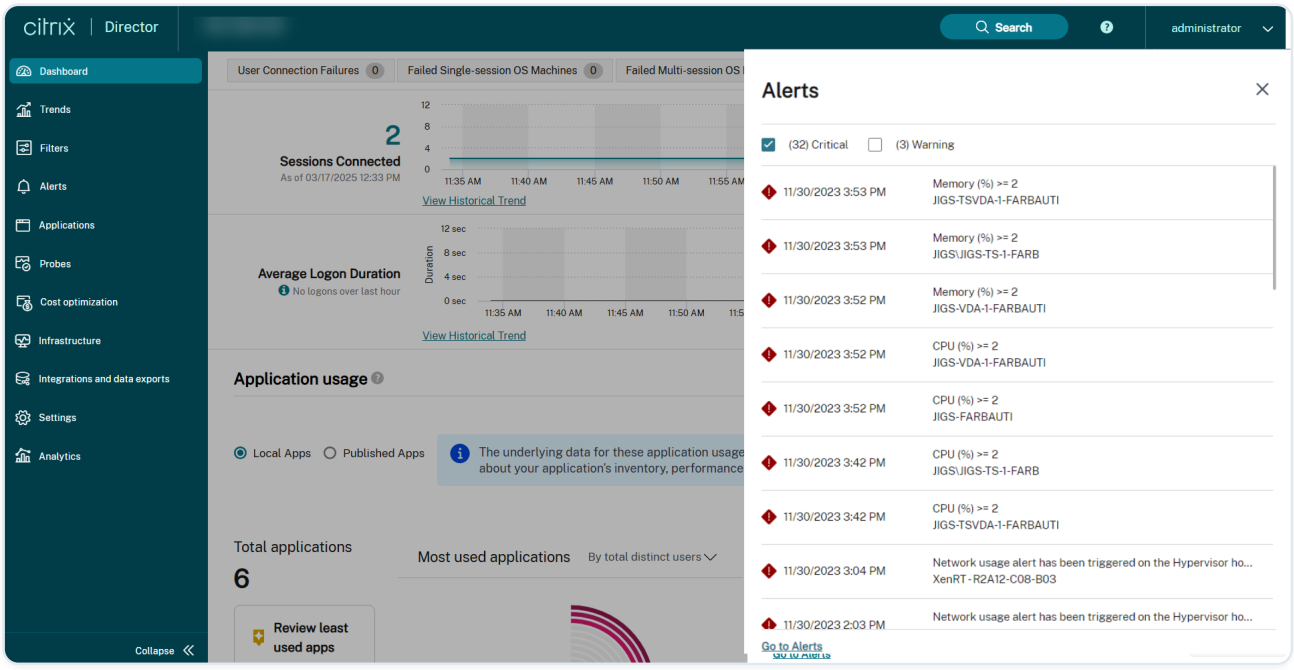
ユーザーがメンテナンスモード中の割り当てられたデスクトップに接続しようとすると、デスクトップが利用できないことを示すメッセージが表示されます。メンテナンスモードを無効にするまで、新しい接続は確立できません。

アプリケーション分析

アプリケーションタブには、アプリケーションベースの分析が単一の統合ビューで表示され、アプリケーションのパフォーマンスを効率的に分析および管理するのに役立ちます。サイトで公開されているすべてのアプリケーションの健全性および使用状況に関する貴重な洞察を得ることができます。プローブ結果、アプリケーションごとのインスタンス数、公開されたアプリケーションに関連する障害やエラーなどのメトリックが表示されます。詳細については、**アプリケーションのトラブルシューティング**のアプリケーション分析セクションを参照してください。

アラートと通知

アラートは、Directorのダッシュボードやその他の上位レベルのビューに、警告および重大なアラートシンボルとともに表示されます。アラートは、**Premium**ライセンスサイトで利用できます。アラートは1分ごとに自動的に更新されます。また、オンデマンドでアラートを更新することもできます。

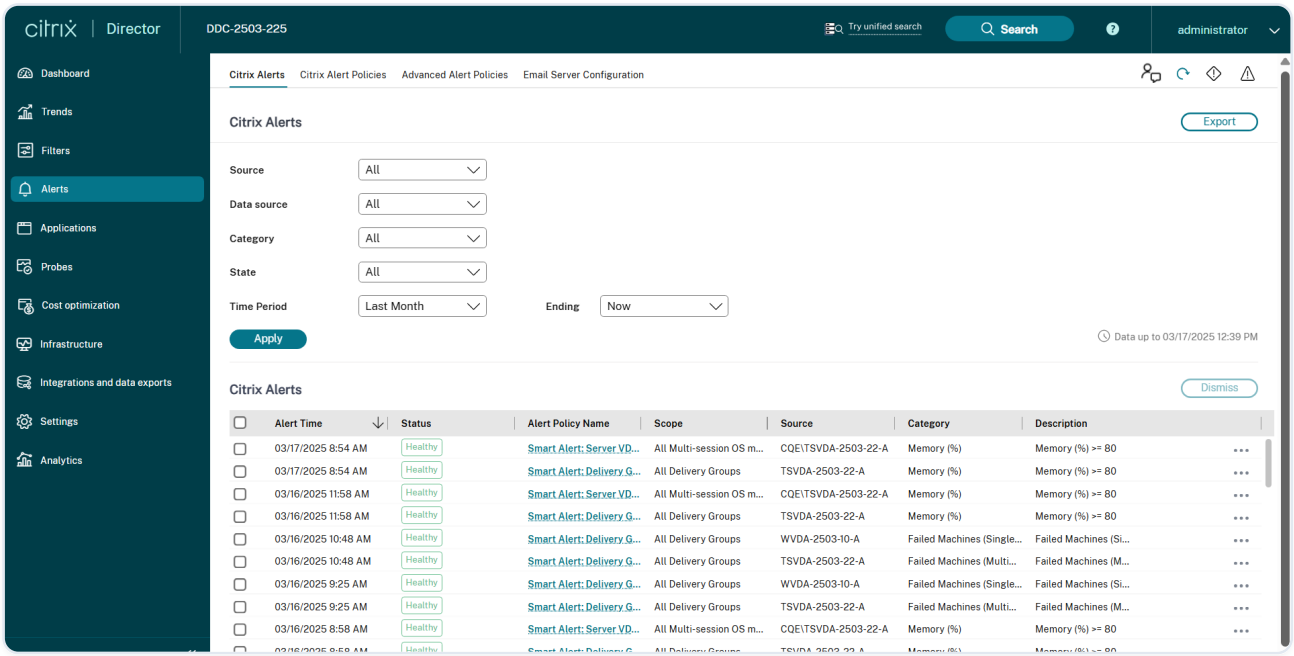


警告アラート（琥珀色の三角形）は、条件の警告しきい値に達したか、それを超えたことを示します。

重大なアラート（赤い円）は、条件の重大なしきい値に達したか、それを超えたことを示します。

アラートの詳細情報を表示するには、サイドバーからアラートを選択するか、サイドバーの下部にある**Go to Alerts**リンクをクリックするか、Directorページの上部から**Alerts**を選択します。

アラートビューでは、アラートをフィルター処理してエクスポートできます。たとえば、特定のデリバリーグループの過去1か月間の失敗したマルチセッションOSマシン、または特定のユーザーのすべてのアラートなどです。詳細については、「レポートのエクスポート」を参照してください。



Citrix®アラート

Citrixアラートは、Citrixコンポーネントから発生し、Directorで監視されるアラートです。Directorの**アラート** \> **Citrixアラートポリシー**でCitrixアラートを構成できます。構成の一部として、アラートが設定したしきい値を超えたときに、個人やグループに電子メールで通知を送信するように設定できます。Citrixアラートの設定の詳細については、「アラートポリシーの作成」を参照してください。

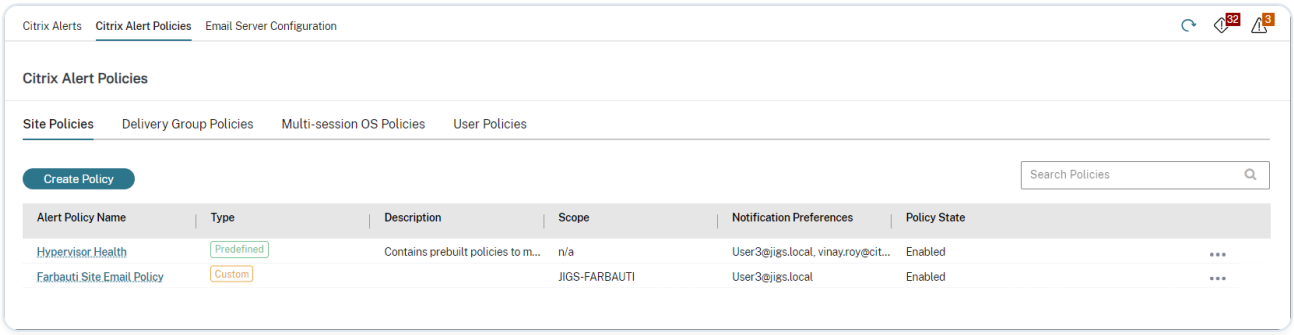
> **注:**
>
> ファイアウォール、プロキシ、またはMicrosoft Exchange Serverが電子メールアラートをブロックしないようにしてください。

スマートアラートポリシー

定義済みのしきい値を持つ一連の組み込みアラートポリシーは、デリバリーグループおよびマルチセッションOS VDAスコープで利用できます。この機能には、Delivery Controllerバージョン7.18以降が必要です。組み込みアラートポリシーのしきい値パラメーターは、**アラート** \> **Citrixアラートポリシー**で変更できます。 これらのポリシーは、サイトに少なくとも1つのアラートターゲット（デリバリーグループまたはマルチセッションOS VDA）が定義されている場合に作成されます。さらに、これらの組み込みアラートは、新しいデリバリーグループまたはマルチセッションOS VDAに自動的に追加されます。

Directorとサイトをアップグレードする場合、以前のDirectorインスタンスのアラートポリシーが引き継がれます。組み込みアラートポリシーは、Monitorデータベースに対応するアラートルールが存在しない場合にのみ作成されます。

組み込みアラートポリシーのしきい値については、「アラートポリシーの条件」セクションを参照してください。



高度なアラートポリシー

Directorのプロアクティブ通知およびアラート機能は、**高度なアラートポリシー**という新しいアラートフレームワークを含むように強化されています。この機能を使用すると、各要素または条件に詳細な情報を含めることでアラートを作成でき、アラートの範囲に対する制御が強化されます。現在、これらのポリシーには、コスト削減とインフラストラクチャに関するアラートが含まれています。

データソース駆動型アラートである高度なアラートポリシーの導入により、複数条件のスコープフィルタリングを使用できます。

この機能は、重要な問題への対応の迅速性や有効性の低下につながる可能性のある過剰なアラートを減らすのに役立ちます。このポリシーは、アラートポリシーの有効性と管理者からのエンゲージメントを測定するのに役立ちます。

高度なアラートポリシーは、**アラート** > **高度なアラートポリシー** > **ポリシーの作成**セクションから作成できます。

次のデータソースのいずれかを選択できます。

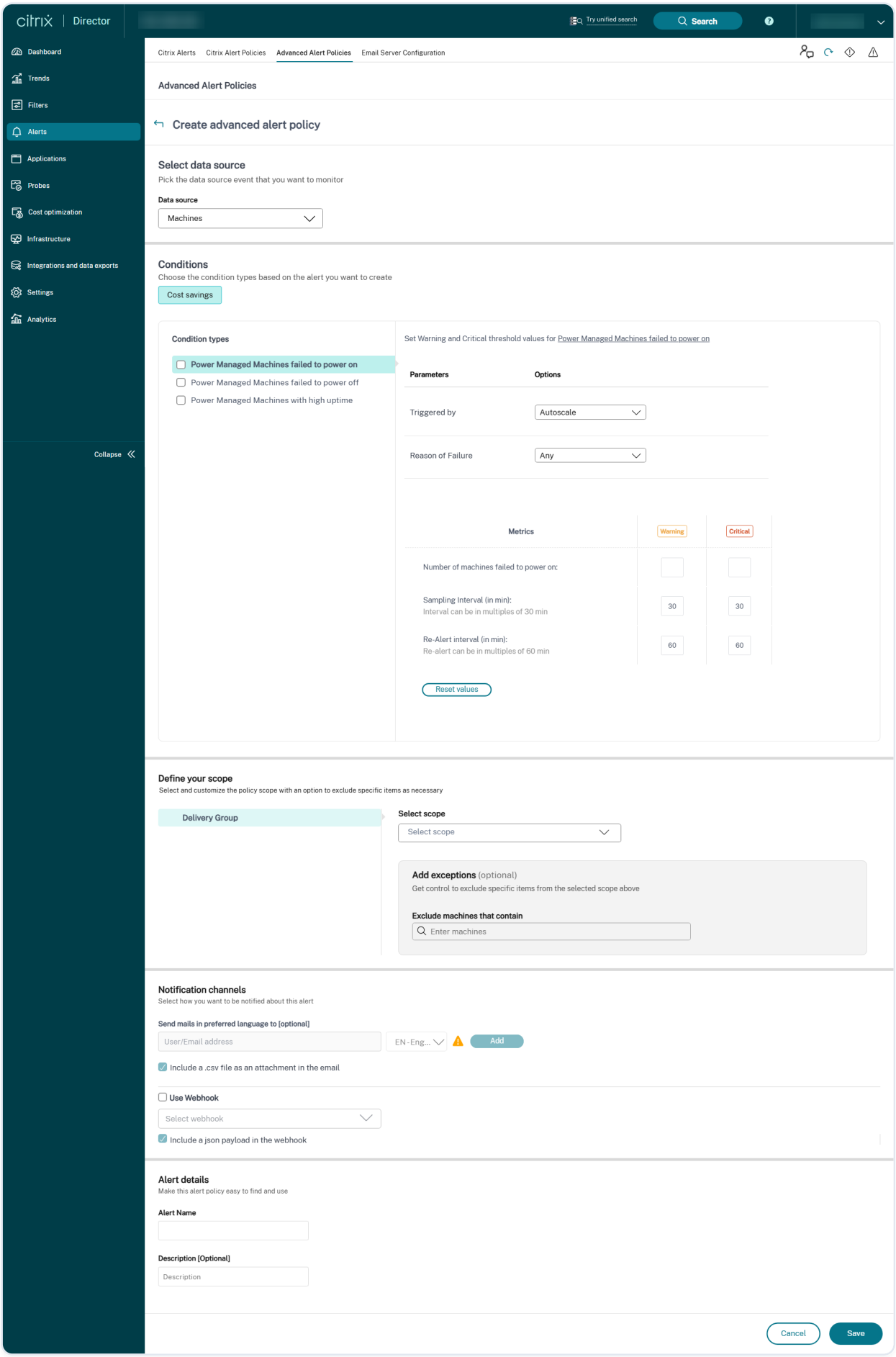
- マシン
- プロビジョニングサービス
- StoreFront™
- デリバリーコントローラー™

コスト削減に関するアラート

コストを最適化するのに役立つコスト削減に関するアラートを作成できます。現在、マシンに関するアラートを作成できます。

マシンに関するアラートを作成するには、次の手順を実行します。

1. 「**アラート**」タブ > 「**高度なアラートポリシー**」の順にクリックします。「**高度なアラートポリシー**」ページが表示されます。
2. 「**ポリシーの作成**」をクリックします。「**高度なアラートポリシーの作成**」セクションが表示されます。
3. データソースドロップダウンリストから「**マシン**」を選択します。コスト削減条件とそれに対応する条件タイプが表示されます。


citrix | Director
Try unified search
Search
Dashboard
Trends
Filters
Alerts
Applications
Probes
Cost optimization
Infrastructure
Integrations and data exports
Settings
Analytics
Collapse
Citrix Alerts
Citrix Alert Policies
Advanced Alert Policies
Email Server Configuration
Advanced Alert Policies
Create advanced alert policy
Select data source
Pick the data source event that you want to monitor
Data source
Machines
Conditions
Choose the condition types based on the alert you want to create
Cost savings
Condition types
Power Managed Machines failed to power on
Power Managed Machines failed to power off
Power Managed Machines with high uptime
Set Warning and Critical threshold values for Power Managed Machines failed to power on
Parameters
Options
Triggered by
Autoscale
Reason of Failure
Any
Metrics
Warning
Critical
Number of machines failed to power on:
Sampling Interval (in min):
Interval can be in multiples of 30 min
30
30
Re-Alert interval (in min):
Re-alert can be in multiples of 60 min
60
60
Reset values
Define your scope
Select and customize the policy scope with an option to exclude specific items as necessary
Delivery Group
Select scope
Select scope
Add exceptions (optional)
Get control to exclude specific items from the selected scope above
Exclude machines that contain
Enter machines
Notification channels
Select how you want to be notified about this alert
Send mails in preferred language to [optional]
User/Email address
EN - Eng...
Add
Include a .csv file as an attachment in the email
Use Webhook
Select webhook
Include a json payload in the webhook
Alert details
Make this alert policy easy to find and use
Alert Name
Description [Optional]
Description
Cancel
Save

4. 必要な条件タイプを以下から選択します。
    - 電源管理されたマシンの電源オンに失敗しました
    - 電源管理されたマシンの電源オフに失敗しました
    - 高い稼働時間の電源管理マシン
5. 選択した各条件について、特定のパラメーターと対応するオプションを選択します。
6. 選択した条件タイプに対して、警告およびクリティカルのメトリックを設定します。
    - 高い稼働時間の電源管理マシンについて:
        - アップタイムのしきい値を超えているマシンの数
        - 再アラート間隔（分）。間隔は最低60分です。
    - 電源オンに失敗した電源管理マシンおよび電源オフに失敗した電源管理マシンについて:
        - アップタイムのしきい値を超えているマシンの数
        - サンプリング間隔（分）は30分の倍数にできます
        - 再アラート間隔（分）は60分の倍数にできます
7. 必要に応じて、選択したアラートの再アラート間隔をスケジュールします。
8. アラートのスコープを定義します。
9. 通知チャネルを設定します。これはメールまたはWebhookにすることができます。
    a. 次のチェックボックスを選択できます。
        - WebhookにJSONペイロードを添付として含める
        - メールにCSVファイルを添付として含める

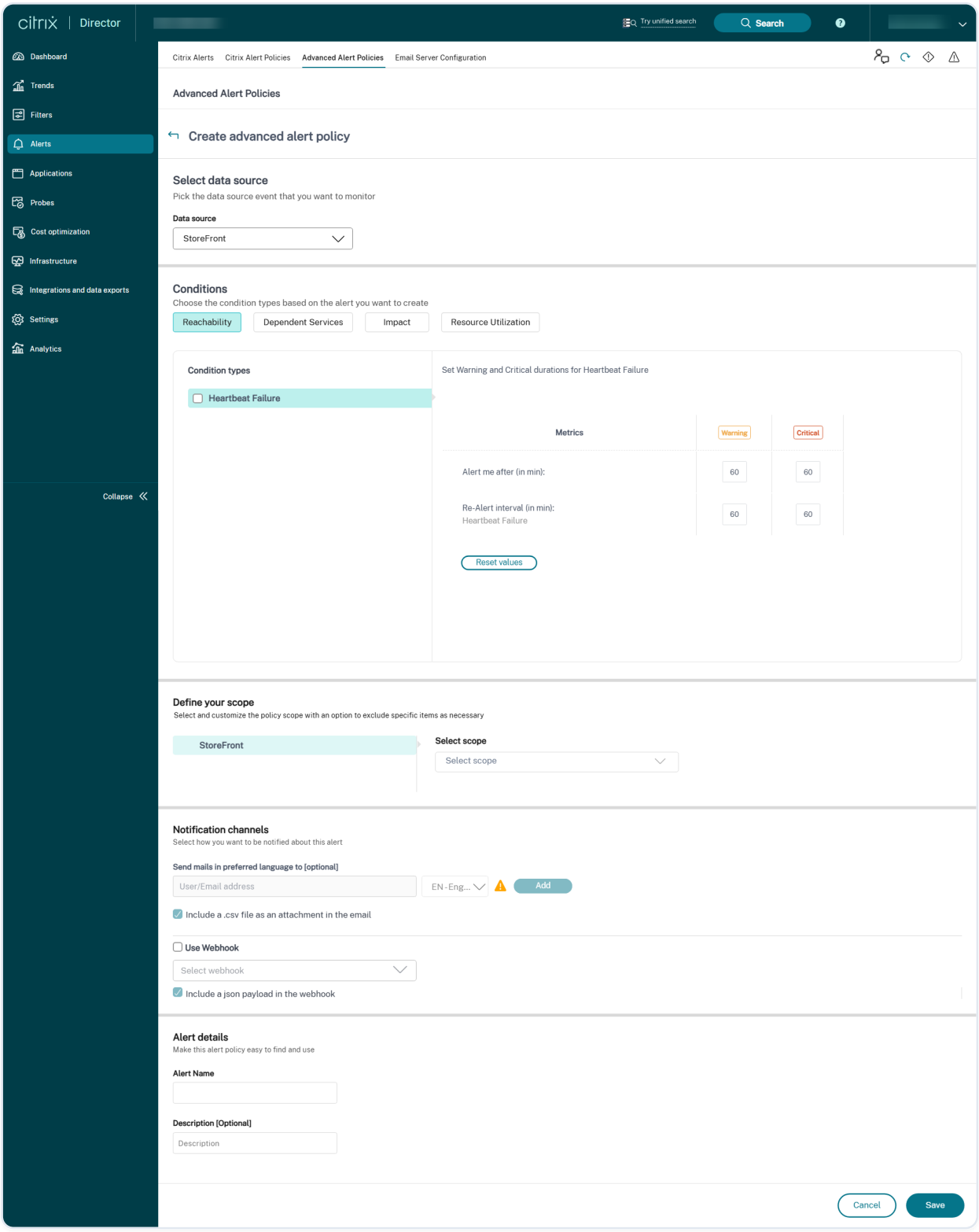
    詳細については、アラートコンテンツの機能強化を参照してください。
10. **アラート名**や**説明**（オプション）などの**アラートの詳細**を入力します。
11. **保存**をクリックします。アラートが作成されます。

インフラストラクチャ監視のアラート

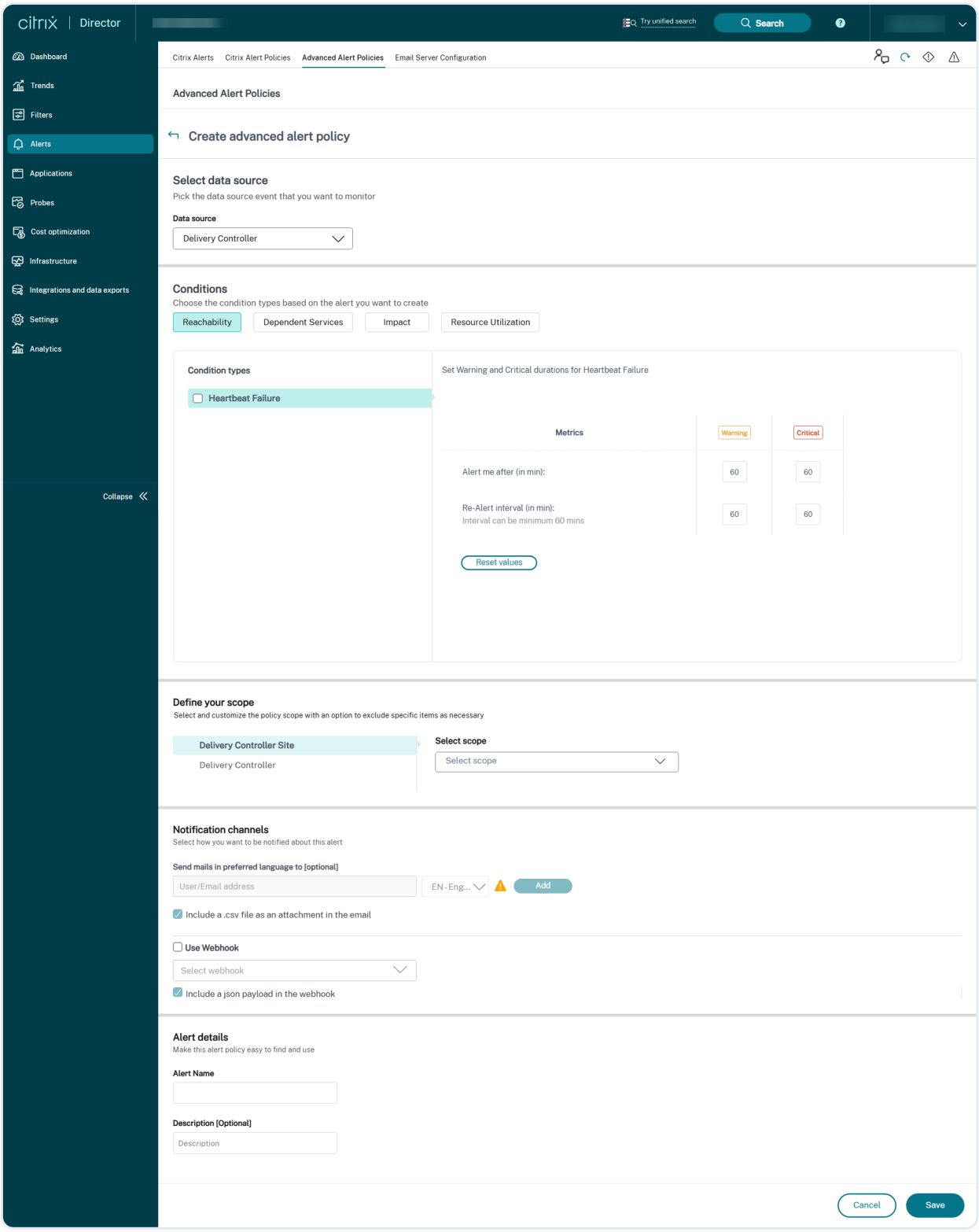
次のサポートされているCitrix Virtual Apps and Desktops™コンポーネントの正常性を監視するためのアラートを作成できます。

- プロビジョニングサービス

- StoreFront



- デリバリーコントローラー



インフラストラクチャ監視のセットアップが完了すると、Directorで利用可能なヘルスデータを使用して、必要なコンポーネントのアラートを設定できます。管理者は、条件、スコープ、通知媒体を設定して、電子メールまたはWebhook経由のJSONペイロードで重要なアラートを受信できます。Provisioning ServiceおよびDelivery Controllerの場合、アラートのスコープをサイトレベルまたは個々のサーバーレベルのいずれかとして選択できます。例えば、Provisioning Serviceの場合、「すべてのProvisioning Service」を選択すると、サイトに2台のサーバーがあっても、サイト

全体に対して1つのアラートのみを受信します。これはサイトレベルのアラートと見なされます。発生したアラートは、分析および管理のために**Citrix Alerts**セクションでも利用できます。

新しく導入されたインフラストラクチャポリシーの一部として、アラート条件は以下の4つのセクションに分類されます。

- 到達可能性
- 依存サービス
- 影響
- リソース使用率

各カテゴリ内の条件は、組織の優先順位に基づいて、**重大**および**警告**の重大度で設定できます。これらのアラートの再アラート間隔をスケジュールすることもできます。

アラート > **Citrixアラートポリシー**セクションからインフラストラクチャポリシーを作成できます。必要なカテゴリを選択し、ポリシーに必要な条件を選択できます。ポリシーの作成方法の詳細については、「アラートポリシーの作成」を参照してください。ポリシーが作成された後、Citrix Alertsページでポリシーを編集、削除、または無効にすることができます。

各カテゴリとコンポーネントでサポートされている条件の詳細については、以下を参照してください。

- Provisioning Serviceのヘルス指標
- StoreFrontのヘルス指標
- デリバリーコントローラーの健全性メトリック

次のデータは、電子メールまたは Citrix Alert ページでアラートとして受信されます。

フィールド	説明
顧客ID	サイトの顧客ID。
アラートレベル	指定できる値は、致命的および警告です。
ターゲット	アラートがトリガーされたマシンの名前。
時間	アラートがトリガーされた時刻。
スコープ	ポリシーのスコープ。
ポリシー	ポリシーの名前。

フィールド	説明
説明	アラートがトリガーされる問題の説明。

ポリシーのスコープを定義する

アラートのスコープを定義し、例外を追加できます。アラートは選択したスコープに対してのみ生成され、例外の追加を使用して除外されたサブスコープはアラート生成に含まれません。この機能は、詳細なレベルでアラートを作成するのに役立ちます。

メールまたはWebhook URLを介して通知を作成できます。アラートを受信する希望の言語を選択することもできます。また、メールの場合は.CSVファイル添付で、Webhook URLを介してはJSONペイロードでアラートパラメータを受信するオプションを選択することもできます。添付ファイルには、必要なパラメータの詳細が含まれています。詳細については、「アラートコンテンツの機能強化」を参照してください。

次のデータは、メールまたは**Citrix Alerts**ページでアラートとして受信されます。

フィールド	説明
顧客ID	サイトの顧客ID。
アラートレベル	この値は、各アラート条件に設定された事前定義値です。可能な値は、CriticalとWarningです。
条件	この値は、ポリシー作成時に設定された条件です。たとえば、未登録のマシンの数が20以上である場合などです。
ターゲット	アラートがトリガーされるデリバリーグループまたはサイトの名前。
サイト	サイトの名前。
スコープ	ポリシーのスコープ。この値にはサブスコープも含まれます。
ポリシー	ポリシーの名前。
説明	アラートがトリガーされる問題の説明。

PowerShellスクリプトを使用して高度なアラートポリシーを作成する方法?

アラートポリシーを作成するためのPowerShellスクリプト:

```
asnp Citrix.Monitor.*

# Add Parameters

$timeSpan = New-TimeSpan -Seconds 30

$alertThreshold = 1

$alarmThreshold = 2

# Add Target UID's

$targetIds = @()

$targetIds += "e9a211b4-a1f3-4f74-b6c7-85225902e997"

# Add email addresses

$emailaddress = @()

$emailaddress += "loki@abc.com"

# Create new policy

$policy = New-MonitorNotificationPolicy -Name
"FailedMachinePercentageAlertCreationViaPowershell" -Description "Policy
created to test urm" -Enabled $true
```

次の行をFAILEDMACHINEPERCENTAGEの正しい条件に置き換えます

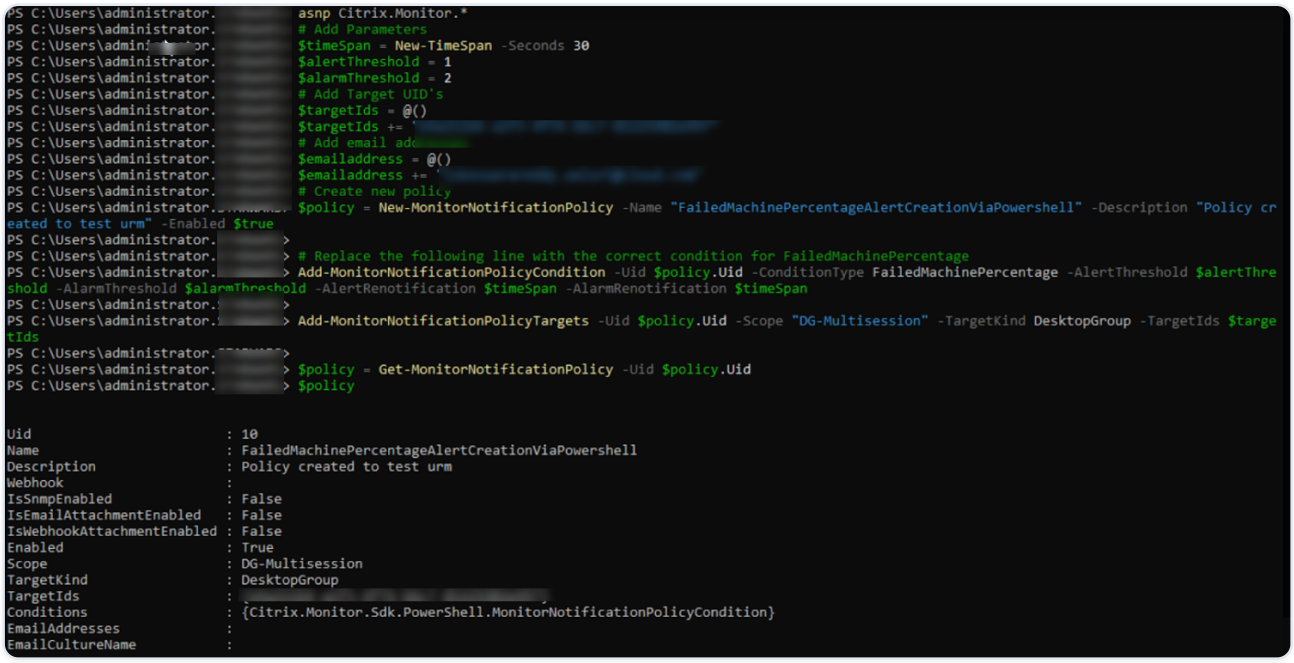
```
Add-MonitorNotificationPolicyCondition -Uid $policy.Uid -ConditionType
FailedMachinePercentage -AlertThreshold $alertThreshold -AlarmThreshold
$alarmThreshold -AlertRenotification $timeSpan -AlarmRenotification
$timeSpan



Add-MonitorNotificationPolicyTargets -Uid $policy.Uid -Scope "DG-
Multisession" -TargetKind DesktopGroup -TargetIds $targetIds
```

```
$policy = Get-MonitorNotificationPolicy -Uid $policy.Uid

$policy
```



上記の画像から、ポリシーが作成され、Uidが10であることがわかります。

構成にメールを追加するには

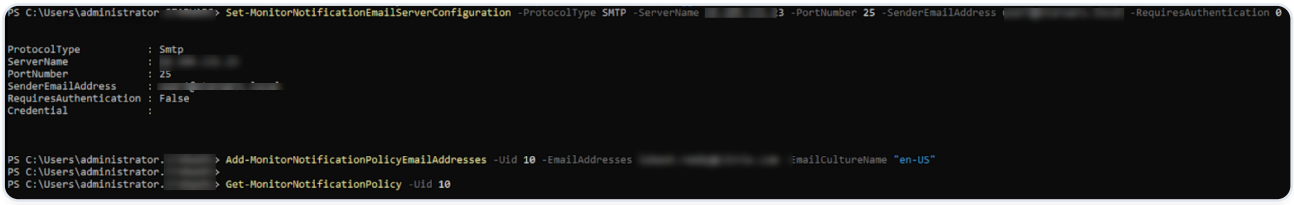
```
Set-MonitorNotificationEmailServerConfiguration -ProtocolType SMTP
-ServerName NameOfTheSMTPServerOrIPAddress -PortNumber 80
-SenderEmailAddress loki@abc.com -RequiresAuthentication 0
```

ポリシーにメールを追加するには

```
Add-MonitorNotificationPolicyEmailAddresses -Uid $policy.Uid
-EmailAddresses $emailaddress -EmailCultureName "en-US"
```

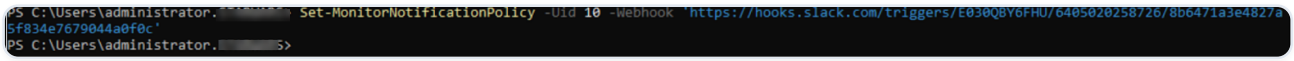
メールを追加するためのサンプルスクリプト:

```
Add-MonitorNotificationPolicyEmailAddresses -Uid 10 -EmailAddresses
$emailaddress -EmailCultureName "en-US"
```



ポリシーにWEBHOOK URLを追加するには

```
Set-MonitorNotificationPolicy –Uid $polcy.Uid –Webhook 'URL'
```

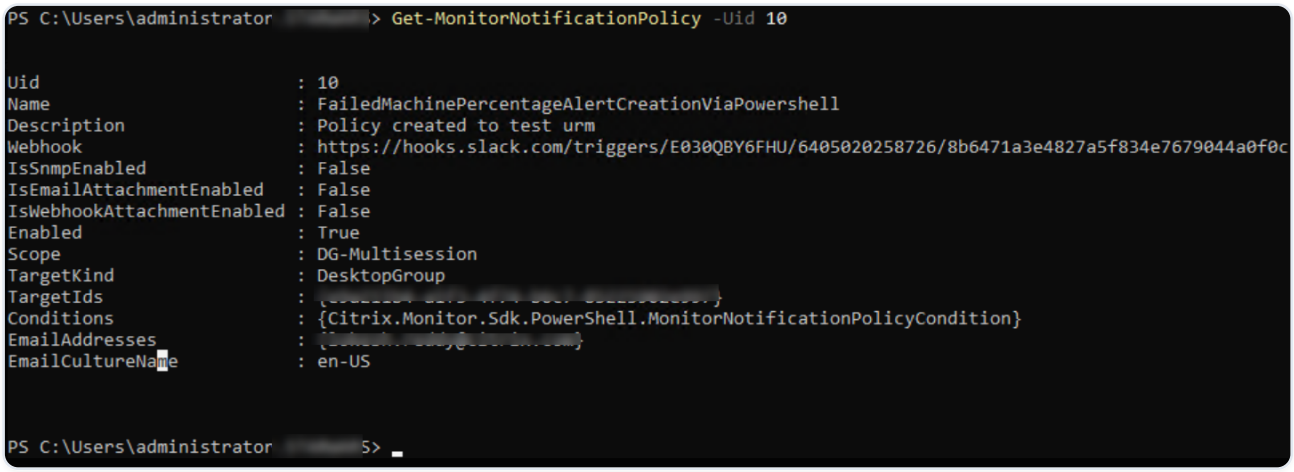


Webhook URLを追加するためのサンプルスクリプト:

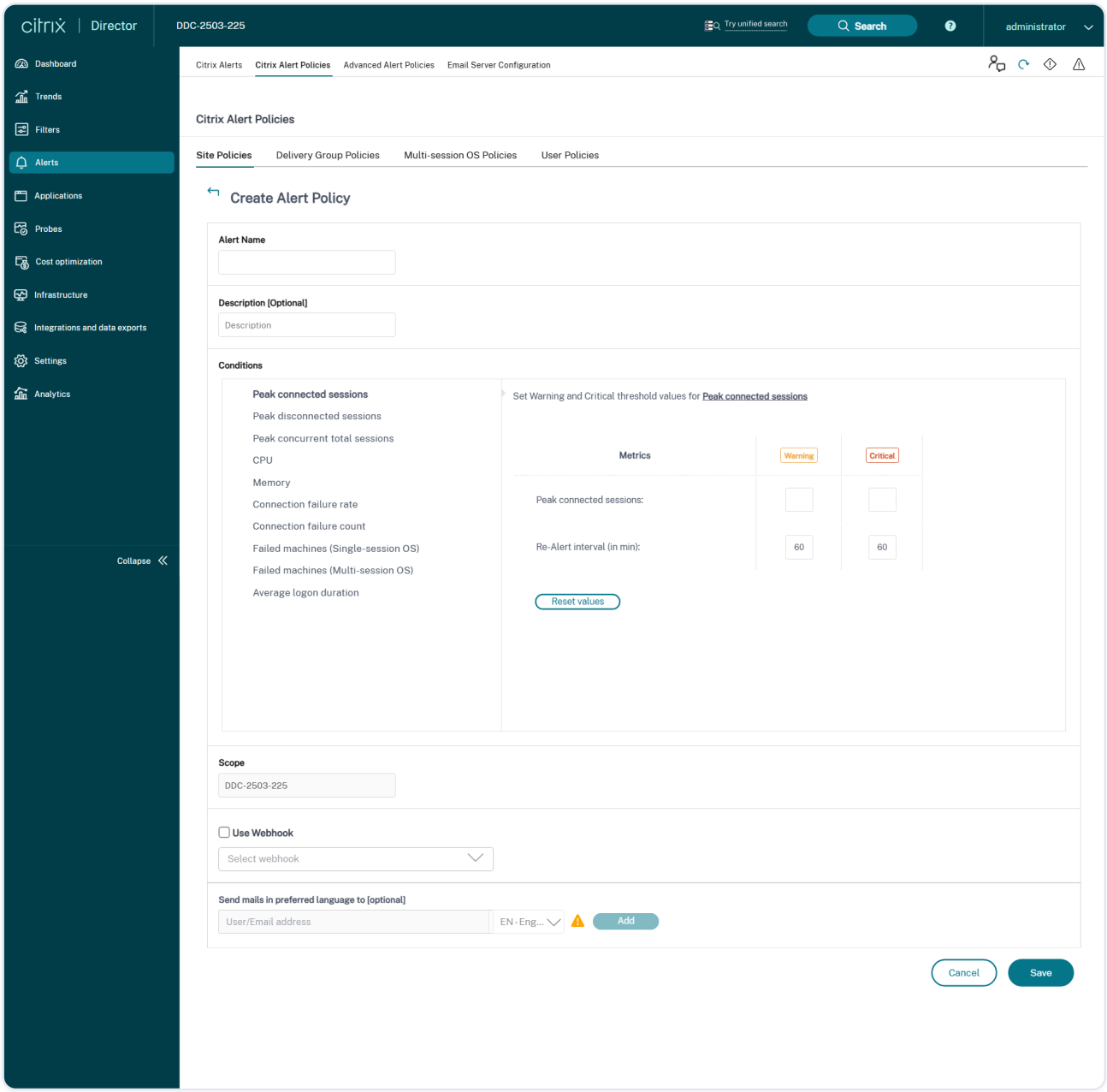
```
Set-MonitorNotificationPolicy –Uid 10  –Webhook  'https://hooks.slack.com/
triggers/E030QBY6FHU/6405020258726/8b6471a3e4827a5f834e7679022a1f1c'
```

作成されたポリシーの詳細を取得する

```
Get-MonitorNotificationPolicy -Uid 10
```



アラートポリシーを作成する



アラートポリシーを作成するには、たとえば、特定のセッション数条件が満たされたときにアラートを生成するには、次の手順を実行します。

1. **アラート** > **Citrixアラートポリシー** に移動し、たとえば、マルチセッションOSポリシーを選択します。
2. **作成** をクリックします。
3. ポリシーに名前を付けて説明し、アラートがトリガーされるために満たす必要がある条件を設定します。たとえば、ピーク接続セッション、ピーク切断セッション、およびピーク同時合計セッションの警告値と重大値を指定します。警告値は重大値より大きくしてはいけません。詳細については、アラートポリシーの条件を参照してください。

4. 再アラート間隔を設定します。アラートの条件が引き続き満たされている場合、この時間間隔でアラートが再度トリガーされ、アラートポリシーで設定されている場合は、メール通知が生成されます。却下されたアラートは、再アラート間隔でメール通知を生成しません。
5. スコープを設定します。たとえば、特定のデリバリーグループに設定します。
6. 通知設定で、アラートがトリガーされたときにメールで通知する必要があるユーザーを指定します。アラートポリシーでメール通知設定を行うには、**メールサーバー構成**タブでメールサーバーを指定する必要があります。

    a. アラートコンテンツを.CSV添付ファイルまたはJSONペイロードで受信することもできます。これを行うには、次のチェックボックスをオンにします。

    - **Webhookにjsonペイロードを添付として含める**
    - **メールにcsvファイルを添付として含める**

> **注:**
>
> .CSV添付ファイルおよびJSONペイロードオプションによるアラートコンテンツの受信は、現在、一部のアラートでのみ利用可能です。詳細については、「アラートコンテンツの機能強化」を参照してください。

7. 「**保存**」をクリックします。

スコープで20以上のデリバリーグループが定義されたポリシーを作成すると、構成の完了に約30秒かかる場合があります。この間、スピナーが表示されます。

最大20の固有のデリバリーグループ（合計1000のデリバリーグループターゲット）に対して50を超えるポリシーを作成すると、応答時間が増加する可能性があります（5秒以上）。

アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、マシンパラメーターを使用して定義された誤ったデリバリーグループアラートがトリガーされる可能性があります。

> **注:**
>
> アラートポリシーを削除した後、そのポリシーによって生成されたアラート通知が停止するまでに最大30分かかる場合があります。

アラートコンテンツの機能強化

Directorのアラート機能が強化され、CSV添付ファイルとJSONペイロードが含まれるようになりました。この機能強化により、メールでCSV添付ファイルとして、またはWebhookがある場合はJSONペイロードとしてアラートの詳細を取得できます。このCSV添付ファイルまたはJSONペイロードを使用すると、詳細レベルで豊富なコンテンツを受信でき、問題の迅速な特定と解決に役立ちます。

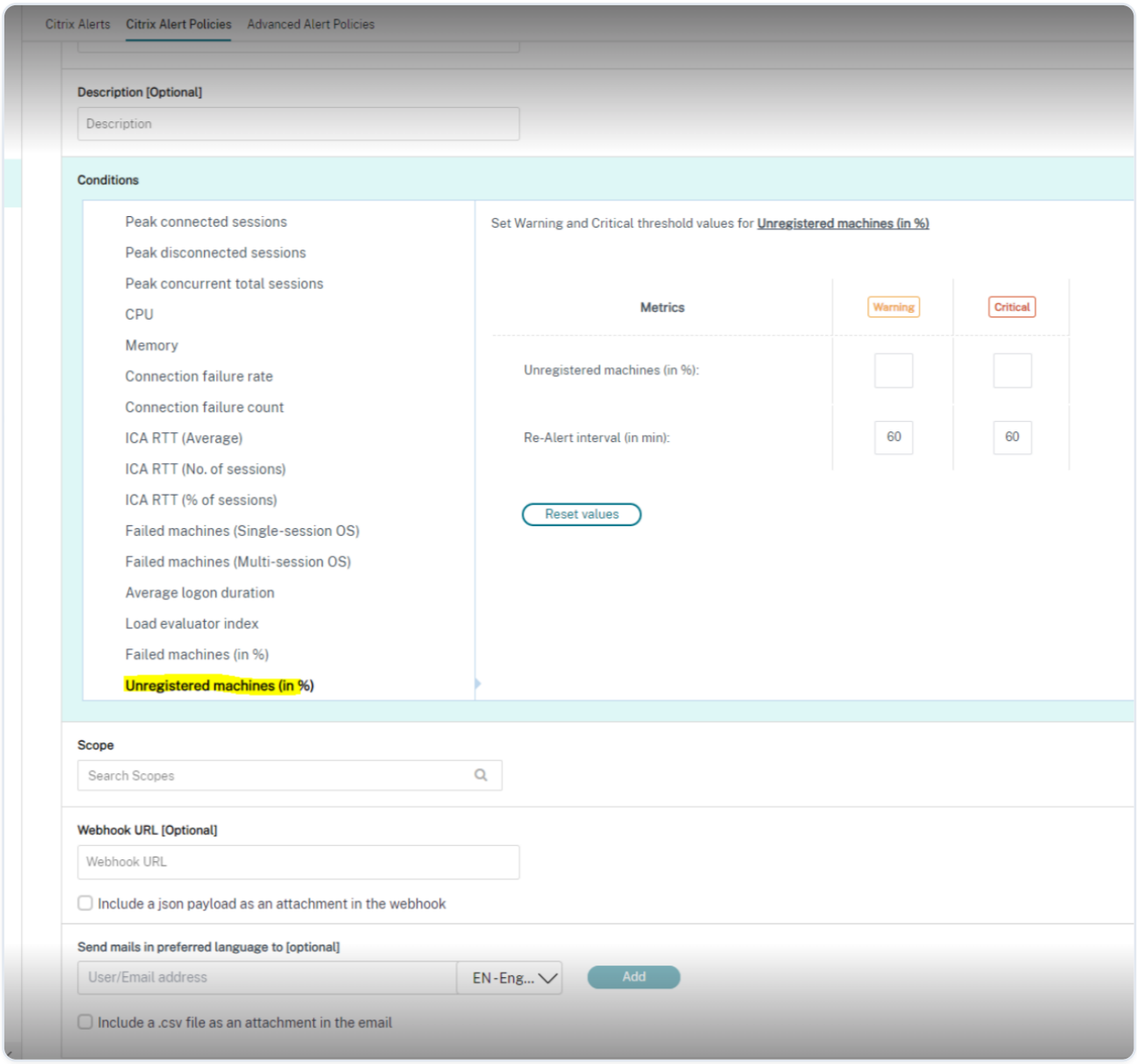
現在、この機能強化は次のアラートでのみ利用可能です。

- マシンの稼働時間
- 電源オンアクションの失敗
- 電源オフアクションの失敗
- 未登録マシン (%)

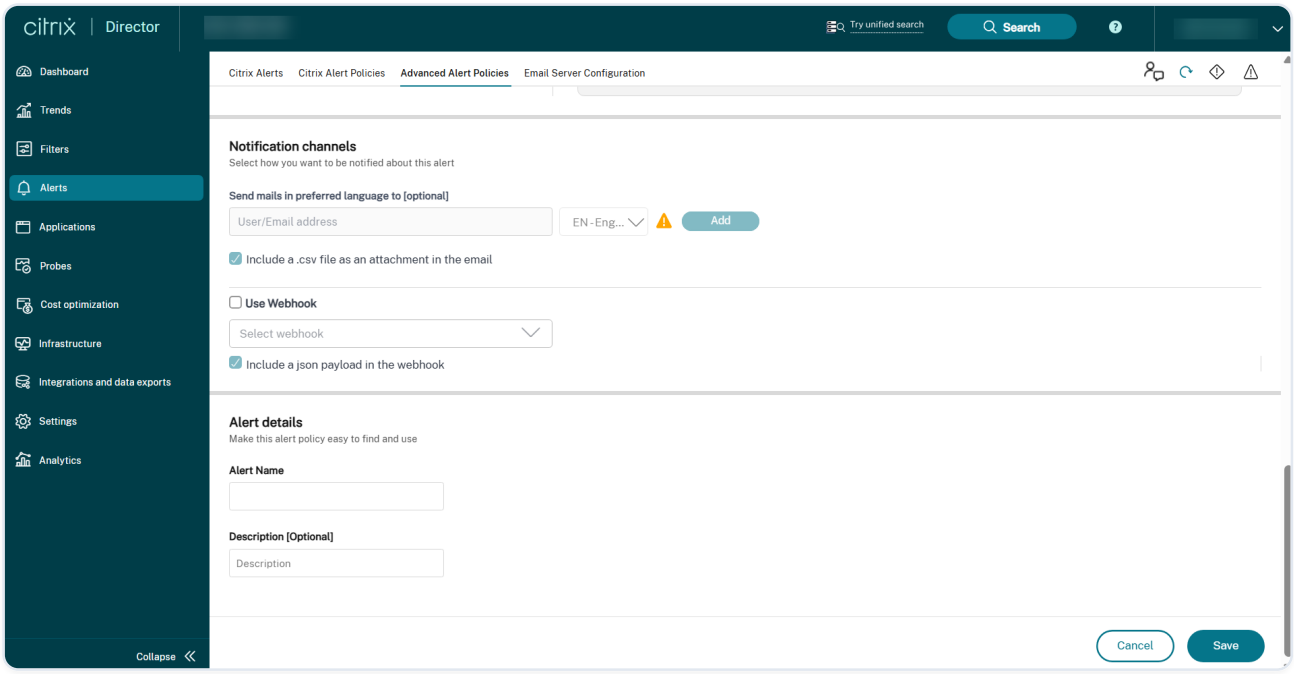
この機能を使用するには、アラートに移動し、次のチェックボックスを選択します。

- **WebhookにJSONペイロードを添付ファイルとして含める**
- **メールにCSVファイルを添付ファイルとして含める**

以下は、**Citrixアラートポリシー**セクションのスクリーンショットです。



以下は、**高度なアラートポリシー**セクションのスクリーンショットです。



CSV添付ファイル

次の表は、サポートされているすべてのアラートの.CSV添付ファイルの列を示しています。

列	適用されるアラート
マシン名、IPアドレス、およびデリバリーグループ名	マシンの稼働時間、電源オフ失敗アクションと電源オン失敗アクション、および未登録マシン（%）
現在の登録状態、失敗日、障害状態、およびライフサイクル状態	未登録マシン（%）
最終電源アクション失敗理由、最終電源アクショントリガー元、最終電源アクションタイプ、および最終電源アクション完了日	電源オフ失敗アクションと電源オン失敗アクション
電源状態、電源オン日時、総稼働時間（分）	マシンの稼働時間

WEBHOOKペイロード

未登録マシンの割合アラート

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Unregistered machines (in %)\",\"Value\":\"<Value Set as
```

```
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"CurrentRegistrationState\":\"Unregistered\",
\"FailureDate\":\"<Date of Failure>\",\"FaultState\":\"<Fault State of the
Machine>\",\"LifecycleState\":\"<Lifecycle state of the Machine>\"},
{\"MachineName\":\"<Name of the Machine>\",\"IPAddress\":\"<IP Address>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",
\"CurrentRegistrationState\":\"Unregistered\",\"FailureDate\":\"<Date of
Failure>\",\"FaultState\":\"<Fault State of the Machine>\",
\"LifecycleState\":\"<Lifecycle state of the Machine>\"}]}"

}
```

電源オン失敗アクションアラート

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Failure To PowerOn Action\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure, HypervisorRateLimitExceeded, UnknownError,
Power Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-User,
Administrator, Auto-Scale, Schedule>\",\"LastPowerActionType\":\"<PowerOn/
PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"},{\"MachineName\":\"<Name of the Machine>\",
\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of the
DeliveryGroup>\",\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure, HypervisorRateLimitExceeded, UnknownError,
Power Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-User,
Administrator, Auto-Scale, Schedule>\",\"LastPowerActionType\":\"<PowerOn/
PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"}]}"
```

```
}
```

電源オフ失敗アクションアラート

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Failure To PowerOff Action\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IPV4 Address of the Machine>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",
\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Powe
r Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-
User,Administrator,Auto-Scale,Schedule>\",\"LastPowerActionType\":
\"<PowerOn/PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"},{\"MachineName\":\"<Name of the Machine>\",
\"IPAddress\":\"<IPV4 Address of the Machine>\",\"DeliveryGroupName\":
\"<Name of the DeliveryGroup>\",\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Powe
r Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-
User,Administrator,Auto-Scale,Schedule>\",\"LastPowerActionType\":
\"<PowerOn/PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"}]}"

}
```

マシンの稼働時間アラート

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Machine Uptime Alert\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
```

```
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"PowerState\":\"<On/Off>\",\"PoweredOnDate\":
\"2024-05-15T15:04:27.723\",\"TotalUptimeInMinutes\":180},
{\"MachineName\":\"<Name of the Machine>\",\"IPAddress\":\"<IP Address>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",\"PowerState\":
\"<ON/OFF>\",\"PoweredOnDate\":\"2024-05-15T15:04:27.723\",
\"TotalUptimeInMinutes\":\"<Uptime Duration>\"}]}"

}
```

アラートポリシーの条件

以下に、アラートカテゴリ、アラートを軽減するための推奨アクション、および定義されている場合は組み込みポリシー条件を示します。組み込みのアラートポリシーは、アラートおよび再アラートの間隔が60分に設定されています。

ピーク時の接続済みセッション

- Directorのセッショントレンドビューで、ピーク時の接続済みセッションを確認します。
- セッション負荷に対応するのに十分な容量があることを確認します。
- 必要に応じて新しいマシンを追加します

ピーク時の切断済みセッション

- Directorのセッショントレンドビューで、ピーク時の切断済みセッションを確認します。
- セッション負荷に対応するのに十分な容量があることを確認します。
- 必要に応じて新しいマシンを追加します。
- 必要に応じて切断されたセッションをログオフします

ピーク時の同時合計セッション

- Directorのセッショントレンドビューで、ピーク時の同時セッションを確認します。
- セッション負荷に対応するのに十分な容量があることを確認します。
- 必要に応じて新しいマシンを追加します。
- 必要に応じて、切断されたセッションをログオフします。

CPU

CPU 使用率の割合は、プロセスを含む VDA 上の全体的な CPU 消費量を示します。個々のプロセスによる CPU 使用率の詳細については、対応する VDA の ページで確認できます。

- **マシン詳細 > 履歴使用率の表示 > 上位10プロセス**に移動し、CPUを消費しているプロセスを特定します。プロセスレベルのリソース使用状況統計の収集を開始するには、プロセス監視ポリシーが有効になっていることを確認してください。
- 必要に応じてプロセスを終了します。
- プロセスを終了すると、保存されていないデータが失われます。
- すべてが期待どおりに機能している場合は、将来的に追加のCPUリソースを追加します。

> **注：**
>
> **リソース監視を有効にする**ポリシー設定は、VDAがインストールされているマシンでのCPUおよびメモリパフォーマンスカウンターの監視に対して、デフォルトで許可されています。このポリシー設定が無効になっている場合、CPUおよびメモリの状態に関するアラートはトリガーされません。詳細については、監視ポリシー設定を参照してください。
>
> **スマートポリシー条件：**
>
> - **スコープ：** デリバリーグループ、マルチセッションOSスコープ
> - **しきい値：** 警告 - 80%、クリティカル - 90%

メモリ

メモリ使用率の割合は、プロセスを含むVDA全体のメモリ消費量を示します。個々のプロセスによるメモリ使用量の詳細については、対応するVDAの**マシン詳細**ページで確認できます。

- **マシン詳細 > 履歴使用率の表示 > 上位10プロセス**に移動し、メモリを消費しているプロセスを特定します。プロセスレベルのリソース使用状況統計の収集を開始するには、プロセス監視ポリシーが有効になっていることを確認してください。
- 必要に応じてプロセスを終了します。
- プロセスを終了すると、保存されていないデータが失われます。
- すべてが期待どおりに動作している場合は、今後、追加のメモリを増設してください。

> **注:**
>
> **リソース監視を有効にする**ポリシー設定は、VDAがインストールされたマシン上のCPUおよびメモリのパフォーマンスカウンターを監視するために、デフォルトで許可されています。このポリシー設定が無効になっている場合、CPUおよびメモリの状態に関するアラートはトリガーされません。詳細については、「監視ポリシー設定」を参照してください。

> **スマートポリシー条件:**

- **スコープ:** デリバリーグループ、マルチセッションOSスコープ
- **しきい値:** 警告 - 80%、重大 - 90%

接続失敗率

過去1時間の接続失敗の割合。

- 試行された接続の総数に対する総失敗数に基づいて計算されます。
- Directorの接続失敗トレンドビューで、構成ログから記録されたイベントを確認します。
- アプリケーションまたはデスクトップが到達可能であるかどうかを判断します。

接続失敗数

過去1時間の接続失敗数。

- Director の ビューで、構成ログから記録されたイベントを確認します。
- アプリケーションまたはデスクトップに到達可能かどうかを判断します。

ICA® RTT (平均)

平均 ICA ラウンドトリップ時間。

- ICA RTT の内訳について Citrix ADM を確認し、根本原因を特定します。詳細については、Citrix ADM ドキュメントを参照してください。
- Citrix ADM が利用できない場合は、Director の ビューで ICA RTT と遅延を確認し、ネットワークの問題か、アプリケーションまたはデスクトップの問題かを判断します。

ICA RTT (セッション数)

しきい値の ICA ラウンドトリップ時間を超えるセッションの数。

- 高い ICA RTT を持つセッションの数について Citrix ADM を確認します。詳細については、Citrix ADM ドキュメントを参照してください。
- Citrix ADM が利用できない場合は、ネットワークチームと協力して根本原因を特定します。

  スマートポリシーの条件:

  - **スコープ:** デリバリーグループ、マルチセッション OS スコープ
  - **しきい値:** 警告 - 5 セッション以上で 300 ミリ秒、重大 - 10 セッション以上で 400 ミリ秒

ICA RTT (セッションの割合)

平均 ICA ラウンドトリップ時間を超えるセッションの割合。

- ICA RTTが高いセッションの数についてCitrix ADMを確認します。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、ネットワークチームと協力して根本原因を特定してください。

ICA RTT (ユーザー)

指定されたユーザーによって起動されたセッションに適用されるICAラウンドトリップ時間。少なくとも1つのセッションでICA RTTがしきい値を超えた場合、アラートがトリガーされます。

失敗したマシン（シングルセッションOS）

失敗したシングルセッションOSマシンの数。失敗の原因は、Directorのダッシュボードビューとフィルタービューに示されているように、さまざまです。

- 根本原因を特定するためにCitrix Scout診断を実行します。

  スマートポリシー条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 1、重大 - 2

失敗したマシン (マルチセッションOS)

失敗したマルチセッションOSマシンの数。失敗の原因は、Directorのダッシュボードビューとフィルタービューに示されているように、さまざまです。

- 根本原因を特定するためにCitrix Scout診断を実行します。

  スマートポリシーの条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ

- **しきい値:** 警告 - 1、重大 - 2

失敗したマシン（%）

デリバリーグループ内の失敗したシングルセッションおよびマルチセッションOSマシンの割合で、失敗したマシンの数に基づいて計算されます。このアラート条件により、デリバリーグループ内の失敗したマシンの割合としてアラートしきい値を構成でき、30秒ごとに計算されます。Directorのダッシュボードおよびフィルタービューに示されているように、さまざまな理由で障害が発生する可能性があります。Citrix Scout診断を実行して、根本原因を特定してください。詳細については、「ユーザーの問題のトラブルシューティング」を参照してください。

失敗した電源オンアクションと失敗した電源オフアクション

デリバリーグループ内の失敗した電源オンアクションの数と失敗した電源オフアクションの数で、電源オンまたはオフに失敗した**電源管理対象マシン**の数に基づいて計算されます。このアラート条件により、デリバリーグループ内で電源オンまたはオフに失敗した**電源管理対象マシン**の数としてアラートしきい値を構成でき、30分ごとに計算されます。

管理者は、高度なアラートポリシーでこれらのアラートに対して次のパラメーターを構成できます。

- トリガー元: 電源アクションをトリガーしたもの
- 失敗の理由: アクションが失敗した理由
- しきい値: ポリシーをトリガーするために電源アクションに失敗したマシンのしきい値
- サンプリング間隔: 失敗した電源アクションを確認する必要がある間隔
- 再アラート間隔: アラートを再送信する必要がある時間

Directorのダッシュボードおよびフィルタービューに示されているように、さまざまな理由で障害が発生する可能性があります。Citrix Scout診断を実行して、根本原因を特定してください。詳細については、「ユーザーの問題のトラブルシューティング」を参照してください。

未登録のマシン（%）

マシンが再起動によって不安定になった場合、またはデリバリーコントローラーと仮想マシン間で通信の問題が発生した場合、マシンは未登録と見なされます。**未登録のマシン（%）**は、未登録のシングルセッションおよびマルチセッションOSマシンの割合で、未登録のマシンの数に基づいて計算されます。このアラート条件により、デリバリーグループ内の未登録のマシンの割合として警告および重大なしきい値を構成できます。再アラートの間隔を設定できます。また、**未登録のマシン（%）の条件が満たされたときに通知を受け取るためにメールを追加することもできます。重大または警告のしきい値を超えると、アラートとメールが生成されます。アラートはCitrix**

Alertsで確認できます。**未登録のマシン（%）**カテゴリと、必要な状態および時間でフィルターできます。

メールがある場合はCSV添付ファイルで、Webhookがある場合はJSONペイロードを介してアラートの詳細を受け取ることもできます。

> **注:**
>
> 危険値は警告値よりも大きくなければなりません。

> **ポリシー条件:**

- **範囲**: シングルセッションOS、およびマルチセッションOSデリバリーグループ
- **しきい値**: 警告および危険

マシン稼働時間アラート

デリバリーグループ内のマシンの稼働時間は、デリバリーグループで電源がオンになっているマシンについて、1日あたりの時間、1週間あたりの時間、または1か月あたりの時間に基づいて計算されます。このアラート条件により、デリバリーグループでマシンがオンになっている時間をアラートしきい値として構成できます。マシンの稼働時間アラートは、次の場合に次のように機能します。

- 1日あたりの時間 - 1日あたりにマシンがオンになっている時間を指定でき、30分ごとに計算されます。設定できる1日あたりの最大時間は24時間です。
- 1週間あたりの時間 - 1週間あたりにマシンがオンになっている時間を指定でき、6時間ごとに計算されます。設定できる1週間あたりの最大時間は168時間です。
- 1か月あたりの時間 - 1か月あたりにマシンがオンになっている時間を指定でき、毎日1回計算されます。1か月あたりの最大時間は720時間です。 設定できる再アラート間隔の最小値は60分です。警告および危険アラートセクションで、マシンの稼働時間しきい値を超過するマシンの数を入力できます。また、任意のマシンに対して例外を追加することもできます。

たとえば、このアラートに5つのデリバリーグループが追加されており、最初のデリバリーグループと4番目のデリバリーグループで、マシンの数が警告または危険のしきい値を超えた場合、アラートは最初のデリバリーグループと4番目のデリバリーグループに対して個別にトリガーされます。

このアラートは、管理者がマシンの稼働時間を分析するのに役立ち、この分析に基づいて、管理者はコストの最適化に貢献できます。メールがある場合はCSV添付ファイルで、またはWebhookがある場合はJSONペイロードを介してアラートの詳細を受け取ることもできます。

平均ログオン時間

過去1時間に発生したログオンの平均ログオン時間。

- Directorダッシュボードを確認して、ログオン時間に関する最新のメトリックを取得してください。短期間に多くのユーザーがログインすると、ログオン時間が増加する可能性があります。
- 原因を絞り込むために、ログオンのベースラインと内訳を確認します。詳細については、「ユーザーログオンの問題の診断」(/ja-jp/citrix-virtual-apps-desktops/2511/director/troubleshoot-deployments/user-issues/user-logon.html)を参照してください。

  スマートポリシー条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 45秒、危険 - 60秒

ログオン時間（ユーザー）

過去1時間に発生した、指定されたユーザーのログオン期間。

ロード評価インデックス

過去5分間のロード評価インデックスの値。

- ピーク負荷（最大負荷）がかかっている可能性のあるマルチセッションOSマシンについてDirectorを確認します。ダッシュボード（障害）とトレンドのロード評価インデックスレポートの両方を確認します。

  スマートポリシーの条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 80%、危険 - 90%

Webhook を使用してアラートポリシーを構成する

電子メール通知とは別に、Webhook を使用してアラートポリシーを構成できます。

注: この機能には、Delivery Controller バージョン 7.11 以降が必要です。

PowerShell コマンドレットを使用して、HTTP コールバックまたは HTTP POST でアラートポリシーを構成できます。これらは Webhook をサポートするように拡張されています。

新しい Octoblu ワークフローの作成と、対応する Webhook URL の取得については、Octoblu Developer Hub を参照してください。

新しいアラートポリシーまたは既存のポリシーのWebhook URLを構成するには、次のPowerShellコマンドレットを使用します。

Webhook URLを使用して新しいアラートポリシーを作成します:

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -Description
<Policy description> -Enabled $true -Webhook <Webhook URL>
```

既存のアラートポリシーに Webhook URL を追加する:

```
Set-MonitorNotificationPolicy - Uid <Policy id> -Webhook <Webhook URL>
```

PowerShellコマンドのヘルプについては、PowerShellヘルプを使用してください。例:

```
Get-Help  <Set-MonitorNotificationPolicy>
```

アラートポリシーから生成された通知は、Webhook URL への POST 呼び出しで Webhook をトリガーします。POST メッセージには、JSON 形式の通知情報が含まれています。

```
{"NotificationId" : \<Notification Id\>,



"Target" : \<Notification Target Id\>,



"Condition" : \<Condition that was violated\>,



"Value" : \<Threshold value for the Condition\>,



"Timestamp": \<Time in UTC when notification was generated\>,
```

```
"PolicyName": \<Name of the Alert policy\>,


"Description": \<Description of the Alert policy\>,


"Scope" : \<Scope of the Alert policy\>,


"NotificationState": \<Notification state critical, warning, healthy or
dismissed\>,


"Site" : \<Site name\>}
```

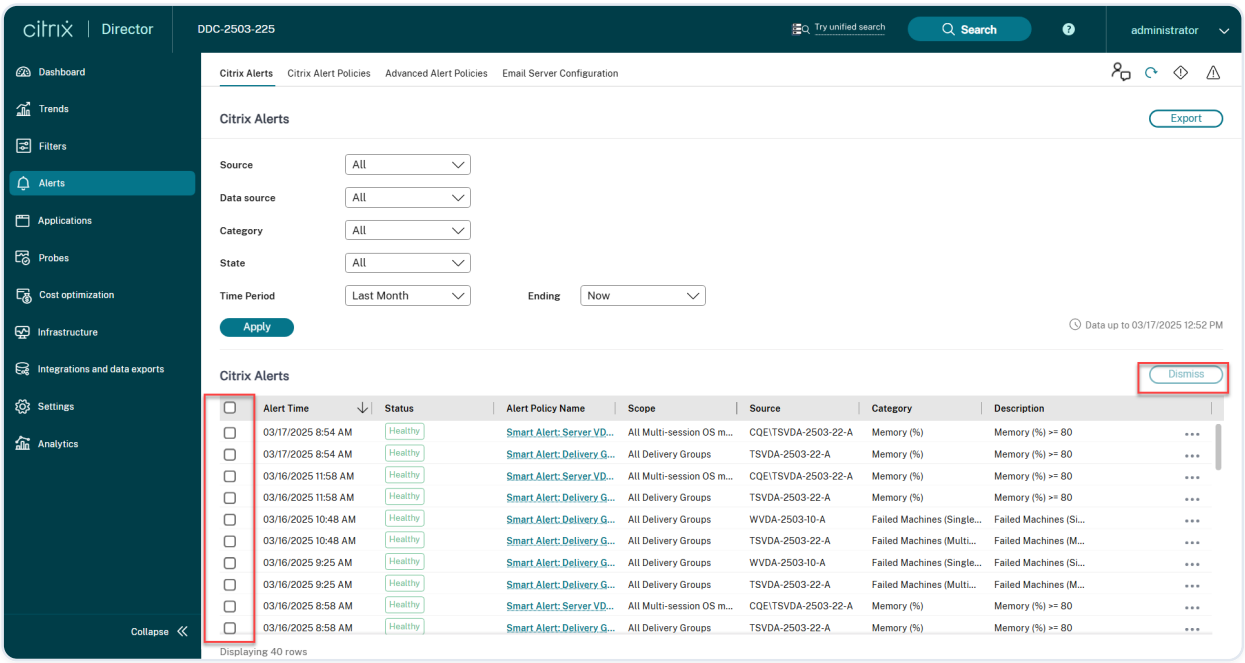
アラートの一括解除

この機能は、管理者のアラート管理プロセスを最適化し、柔軟性を提供し、アラート疲労を軽減します。管理者は、時間、種類、またはカテゴリに基づいてアラートを一括解除でき、メンテナンス中やハイパーバイザーおよびその他の環境を扱う際のアラート管理を簡素化します。

アラートの一括解除は、管理者がワークロードを効率的に管理し、大量のアラートに圧倒されるのを防ぐのに役立ちます。

アラートを一括解除する手順

1. **アラート** > **Citrixアラート**タブに移動します。アラートが表示されます。



2. **ソース**、**カテゴリ**、**状態**、または**期間**からオプションを選択して、解除したいアラートをフィルターします。特定のアラートが表示されます。
3. 特定のアラートの横にあるチェックボックスを選択するか、上部にあるチェックボックスを選択してすべてのアラートを選択します。
4. **解除**をクリックします。アラートの解除を確認する通知が表示されます。
5. **はい**をクリックします。選択されたアラートは*解除済み*としてマークされ、アラートのステータスがそれに応じて更新されます。

PowerShell SDKを使用したWebhook構成

PowerShell SDKを使用したWebhook構成機能により、管理者はWebhookプロファイルを作成、変更、削除、および一覧表示できます。この機能は、ヘッダー、認証タイプ、コンテンツタイプ、ペイロード、およびWebhook URLの指定を可能にすることで、Webhookの構成に柔軟性を提供します。

> **注:**
>
> サポートされているペイロード形式はテキストであり、エンドユーザーはWebhookでテキストを有効にする必要があります。

最新のペイロード形式は次のとおりです。

```
{"text": "This is a message from a Webex incoming webhook."}
```

Webhookを作成する

次のPowerShellサンプルコマンドを使用して、Webhookプロファイルを作成できます。

認証ヘッダーなしでWebhookを作成するには:

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")


$payloads = '{ "text": "$PAYLOAD" }'


$url = "<Fill this field with the required URL>"


Add-MonitorWebhookProfile -Name "profile_slack" -Description "webhook
profile for slack" -Url $url -Headers $headers -PayloadFormat $payloads
```

認証ヘッダー付きでWebhookを作成するには:

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")


$headers.Add("Authorization", "Basic <Fill this field with the
authorization token>")

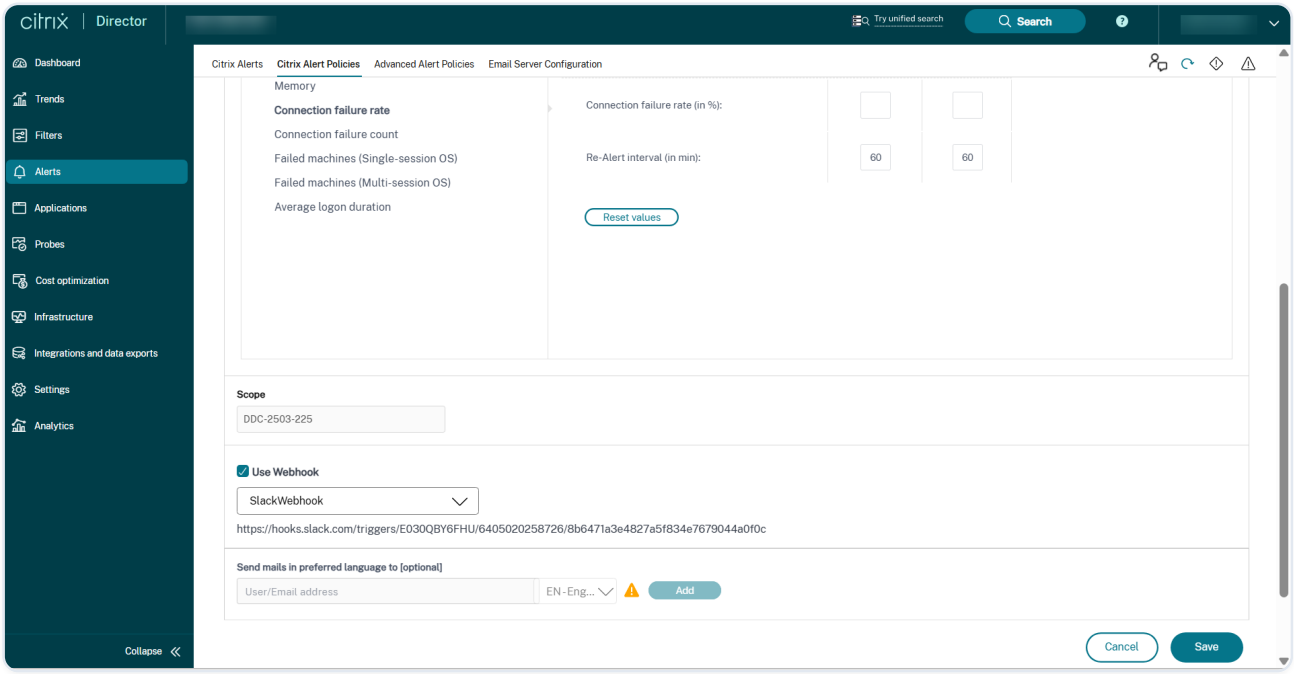

$payloads = '{ "text": "$PAYLOAD" }'
```

```
$url = "<Fill this field with the required URL>"



Add-MonitorWebhookProfile -Name "profile_azure" -Description "webhook
profile for azure function with Authentication" -Url $url -Headers
$headers -PayloadFormat $payloads
```

プロファイルが作成されたら、データベースで確認できます。また、新しく作成されたWebhookプロファイルは、**Citrix Alerts**ページで見つけることができます。



Webhookプロファイルを更新する

次のPowerShellサンプルコマンドを使用して、Webhookプロファイルを更新できます。

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()



$headers.Add("Content-Type", "application/json")



$payloads = '{ "text": "$PAYLOAD" }'
```

```
$url =  "<Fill this field with the required URL>"



Set-MonitorWebhookProfile -Uid 1  -Name "profile_slack_citrix"
-Description "webhook profile for citrix slack" -Url $url -Headers
$headers -PayloadFormat $payloads
```

すべてのWebhookプロファイルの一覧を取得する

利用可能なすべてのWebhookプロファイルの一覧を取得するには、次のPowerShellコマンドの例を使用できます。

```
Get-MonitorWebhookProfile



Get-MonitorWebhookProfile -Name 'profile_msteams'



Get-MonitorWebhookProfile -Uid 1
```

Webhookプロファイルを削除する

Webhookプロファイルを削除するには、次のPowerShellコマンドの例を使用できます。

```
Remove-MonitorWebhookProfile -Uid 1
```

注:

Webhookプロファイルがいずれかのポリシーにマッピングされている場合、削除できません。回避策として、まずポリシーからWebhookマッピングを削除する必要があります。

Webhookプロファイルを使用してポリシーを作成する

Webhookプロファイルを使用してポリシーを作成するには、次のPowerShellコマンドの例を使用できます。

```
New-MonitorNotificationPolicy -Name "Policy1" -Description "Policy
Description" -Enabled $true -WebhookProfileId 1
```

Webhookプロファイルを使用してポリシーを更新する

Webhookプロファイルを使用してポリシーを更新するには、次のPowerShellコマンドの例を使用できます。

```
$Policy = Set-MonitorNotificationPolicy -Uid 1 -WebhookProfileId 1
```

ポリシーからWebhookマッピングを削除する

ポリシーからWebhookプロファイルを削除するには、次のPowerShellコマンドの例を使用できます。

```
$Policy = Set-MonitorNotificationPolicy -Uid 1 -WebhookProfileId 0
```

Webhookプロファイルをテストする

Webhookプロファイルをテストするには、次のPowerShellコマンドの例を使用できます。

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()



$headers.Add("Content-Type", "application/json")



$headers.Add("Authorization", "Basic <Fill this with authorization
token>")



$payloads = '{ "text": "$PAYLOAD" }'

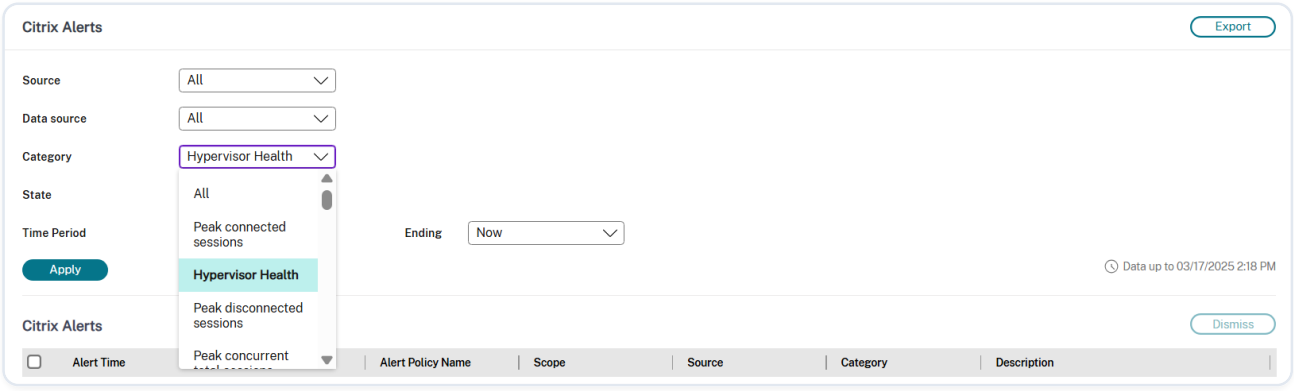


$url ="<Fill this field with the required URL>"
```

```
Test-MonitorWebhookProfile -Url $url -Headers $headers -PayloadFormat
$payloads
```

ハイパーバイザーアラートの監視

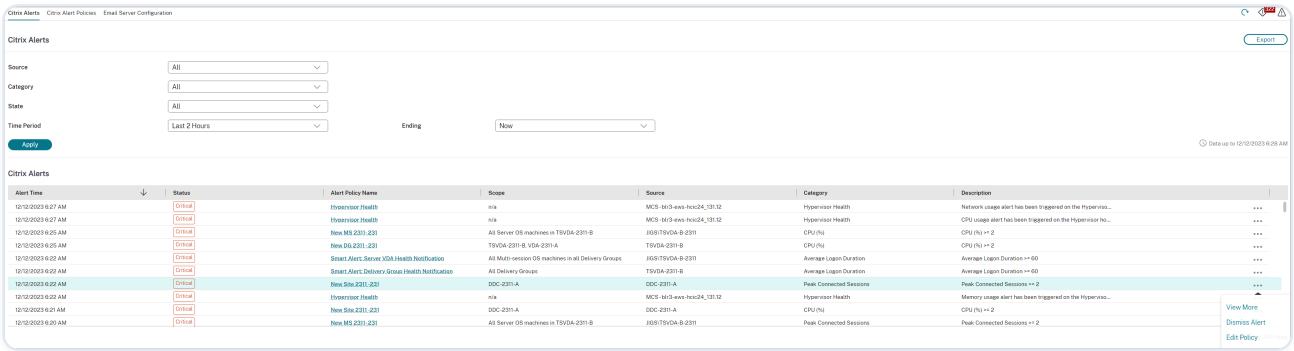
Directorは、ハイパーバイザーの健全性を監視するためのアラートを表示します。XenServer®およびVMware vSphereからのアラートは、ハイパーバイザーのパラメーターと状態の監視に役立ちます。ハイパーバイザーへの接続ステータスも監視され、ホストのクラスターまたはプールが再起動されたり、利用できなくなったりした場合にアラートが提供されます。



ハイパーバイザーアラートを受信するには、Web Studio でホスティング接続が作成されていることを確認してください。詳しくは、「接続とリソース」を参照してください。ハイパーバイザーアラートの監視対象となるのは、これらの接続のみです。

これらのアラートは、しきい値に達するか、それを超えると表示されます。ハイパーバイザーアラートには次のものがあります。

- 重大 — ハイパーバイザーアラームポリシーの重大なしきい値に達したか、超えた場合
- 警告 — ハイパーバイザーアラームポリシーの警告しきい値に達したか、超えた場合
- 却下済み — アクティブなアラートとして表示されなくなったアラート



この機能には、Delivery Controller バージョン 7 1811 以降が必要です。Director の古いバージョンをサイト 7 1811 以降で使用している場合、ハイパーバイザーアラートの数のみが表示されます。アラートを表示するには、Director をアップグレードする必要があります。

次の表は、ハイパーバイザーアラートのさまざまなパラメーターと状態について説明しています。

アラート	サポートされているハイパーバイザー	トリガー元	条件	構成
CPU使用率	ゼノサーバー、ヴイエムウェアvSphere	ハイパーバイザー	CPU使用率アラートのしきい値に達したか、超えた場合	アラートのしきい値はハイパーバイザーで構成する必要があります。
メモリ使用率	ゼノサーバー、ヴイエムウェアvSphere	ハイパーバイザー	メモリ使用率アラートのしきい値に達したか、超えた場合	アラートのしきい値はハイパーバイザーで構成する必要があります。
ネットワーク使用率	ゼノサーバー、ブイエムウェアブイスフィア	ハイパーバイザー	ネットワーク使用率アラートのしきい値に達したか、超えた場合	アラートのしきい値はハイパーバイザーで構成する必要があります。
ディスク使用量	ヴイエムウェアブイスフィア	ハイパーバイザー	ディスク使用量アラートのしきい値に達したか、超過しました	アラートのしきい値はハイパーバイザーで構成する必要があります。
ホスト接続または電源状態	ヴイエムウェアブイスフィア	ハイパーバイザー	ハイパーバイザーホストが再起動されたか、利用できません	アラートはVMware vSphereに組み込まれています。追加の構成は不要です。
ハイパーバイザー接続が利用できません	ゼンサーバー、ヴイエムウェアブイスフィア	デリバリーコントローラー	ハイパーバイザー（プールまたはクラスター）への接続が失われたか、電源が切られたか、再起動され	アラートはDelivery Controllerに組み込まれています。追加の構成は不要です。

アラート	サポートされているハイパーバイザー	トリガー元	条件	構成
			ました。このアラートは、接続が利用できない間、1時間ごとに生成されます。	

注:

アラートの設定に関する詳細については、Citrix XenCenter Alertsを参照するか、VMware vCenter Alertsのドキュメントを確認してください。

メール通知設定は、**Citrix Alerts Policy > Site Policy > Hypervisor Health**で構成できます。ハイパーバイザーアラートポリシーのしきい値条件は、Directorからではなく、ハイパーバイザーからのみ構成、編集、無効化、または削除できます。ただし、メール設定の変更とアラートの解除はDirectorで行うことができます。インフラストラクチャ監視が役割に含まれていない場合は、アラートを無効にできます。

重要:

- ハイパーバイザーによってトリガーされたアラートは、Directorで取得および表示されます。ただし、ハイパーバイザーアラートのライフサイクル/状態の変更はDirectorには反映されません。
- ハイパーバイザーコンソールで正常、解除、または無効化されたアラートは、Directorに表示され続け、明示的に解除する必要があります。
- Directorで解除されたアラートは、ハイパーバイザーコンソールでは自動的に解除されません。

垂直および水平ロードバランシングアラートの処理の改善

以前は、`UseVerticalScalingForRdsLaunches`をtrueに設定し、Studioで「最大セッション数」ポリシーを構成すると、マシンは「最大容量」状態に移行していました。Directorは、垂直ロードバランシングまたは水平ロードバランシングのいずれによって制限に達したかに関わらず、「最大容量」のアラートをトリガーしていました。「最大負荷に到達」などの特定のエラーが発生した場合、垂直ロードバランシングと水平ロードバランシングを区別する方法はありませんでした。これにより、垂直スケーリングシナリオにおける予期される動作に対して不要なアラートが発生し、時間と混乱を招いていました。

現在、垂直ロードバランシングがアクティブで、マシンがセッション制限に達すると、新しい状態である「垂直スケーリングの最大容量」に移行します。Directorは、この新しい状態に対してアラートを生成しなくなりました。アラートは、水平スケーリングシナリオにおける「最大容量」に対してのみトリガーされます。フィルターおよびカスタムレポートページで新しい状態を表示できるため、予期される条件と例外的な条件を区別しやすくなります。この機能強化により、不要なアラートを回避し、実際の問題に集中できるようになり、監視とトラブルシューティングが効率化されます。これは、Set-BrokerSiteを使用して`UseVerticalScalingForRdsLaunches`を構成し、Studioで「最大セッション数」ポリシーを設定した場合に適用されます。

アプリケーション使用状況の監視

Citrix Directorは、以下の使用状況を監視するのに役立ちます。

- 仮想デスクトップセッション内で起動されたアプリケーション（ローカルアプリケーションとも呼ばれます）
- Citrix Workspace™アプリセッションから直接起動されたアプリケーション（公開アプリケーションとも呼ばれます）

アプリケーション使用状況レポートは、最も使用されているアプリケーション、ほとんど使用されていないアプリケーション、および使用されていないアプリケーションを可視化します。最も使用されているアプリケーションはダッシュボードに表示され、厳選されたグラフが含まれています。これらのグラフは、IT管理者またはアプリケーション管理者が、どのアプリケーションが頻繁に使用されているか、およびその使用状況の程度を把握するのに役立ちます。

> **注:**
>
> - この機能は、プラチナライセンスサイトでのみ利用できます。

- ローカルアプリケーションの使用状況を監視するには、uberAgentをDirectorと統合する必要があります。詳しくは、「Citrix uberAgentとDirectorの統合」を参照してください。
- 環境で同じアプリケーションが公開アプリとデスクトップ内にインストールされたアプリ（ローカルアプリ）の両方として提供されている場合、そのアプリが公開アプリレポートとローカルアプリレポートの両方に表示されることがあります。

この機能により、管理者はどのローカルアプリケーションと公開アプリケーションが最も使用されているかを確認できます。このデータを使用して、管理者は使用状況の範囲をさらに深く掘り下げることができます。管理者は、過去24時間の人気アプリの詳細を以下のデータポイントで分析できます。

- アプリケーションの総数 - 企業のサイトのすべてのユーザーが使用しているアプリケーションの総数を特定します。
- 個別のユーザー総数による最も使用されているアプリケーション - ユニークユーザーの総数に基づいて上位10のアプリを特定します。
- アプリケーション起動総数による最も使用されているアプリケーション - アプリケーション起動総数に基づいて上位10のアプリを特定します。
- 同時実行アプリインスタンスのピーク上位 - 各アプリケーションの使用状況の同時インスタンスの最大数に基づいて上位10のアプリを特定します。この情報は、リストされているアプリケーションの最大需要を提供します。

このグラフはダッシュボードページの下部に表示されます。ただし、画面上部の をクリックすると、グラフに直接アクセスできます。

アプリケーション監視(/en-us/citrix-virtual-apps-desktops/2511/media/application-monitoring.png)

をクリックして、単一のアプリの詳細を表示することもできます。このリンクをクリックすると、> > ページが開きます。

このグラフは、アプリの使用状況を視覚的に表現したものです。また、グラフにカーソルを合わせると、選択したデータポイントの絶対数が表示されます。グラフ上の任意のデータポイントをクリックすると、特定のアプリ名が選択された状態で、**トレンド** > **キャパシティ管理** > **ホストされたアプリケーションの使用状況**ページが開きます。このデータは、企業のシステムに存在するすべてのアプリに対する比較値を示すものです。データポイントの絶対値も、同じホバー内に別途記載されています。

最も使用頻度の低いアプリと未使用のアプリのレポート

大規模なCitrix Virtual Apps and Desktops™環境では、利用率の低いアプリケーションが多数存在することがよくあります。環境を最適化するために、**アプリケーション**ページでは、組織内のアプリケーション使用パターンを理解し、リソース割り当てとコスト削減を改善するためのデータに基づいた意思決定を行うのに役立つ追加のメトリックが提供されるようになりました。

主な機能

- **詳細な使用状況情報:** 各アプリケーションについて、個別のユーザー数（過去30日間）、合計起動回数、ピーク時の同時インスタンス数、および経時的な個別のユーザー数のトレンドチャートを表示します。
- **データフォーカス:** 過去7日間、30日間、または90日間のアプリケーション使用パターンを分析し、アプリケーションの必要性を評価します。90日間のデータを表示することをお勧めします。これは、四半期分のデータが提供され、アプリケーションの使用状況が変動するか、一貫しているかを観察できるためです。X軸の日付は、組織のイベントと使用状況の傾向を関連付け、低下が予想されたものかどうかを判断するのに役立ちます。このデータにより、管理者は不要なアプリケーションを排除することで、効率的な環境を維持できます。
- **最適化:** 公開されているアプリの総数、最も使用頻度の低いアプリ、未使用のアプリを特定し、Citrix展開を最適化します。
- **実用的なデータ:** アプリケーション管理を支援するデータに基づいた意思決定を行い、リソース割り当てとライセンス管理を最適化します。
- **データのエクスポート:** 詳細な分析のために、データをPDFまたはCSV形式でエクスポートします。Power BI統合またはアプリケーション使用状況を使用したODATAクエリを使用してデータをエクスポートすることもできます。

要件

- デリバリーコントローラー バージョン 7.16 以降
- VDA バージョン 7.15 以降

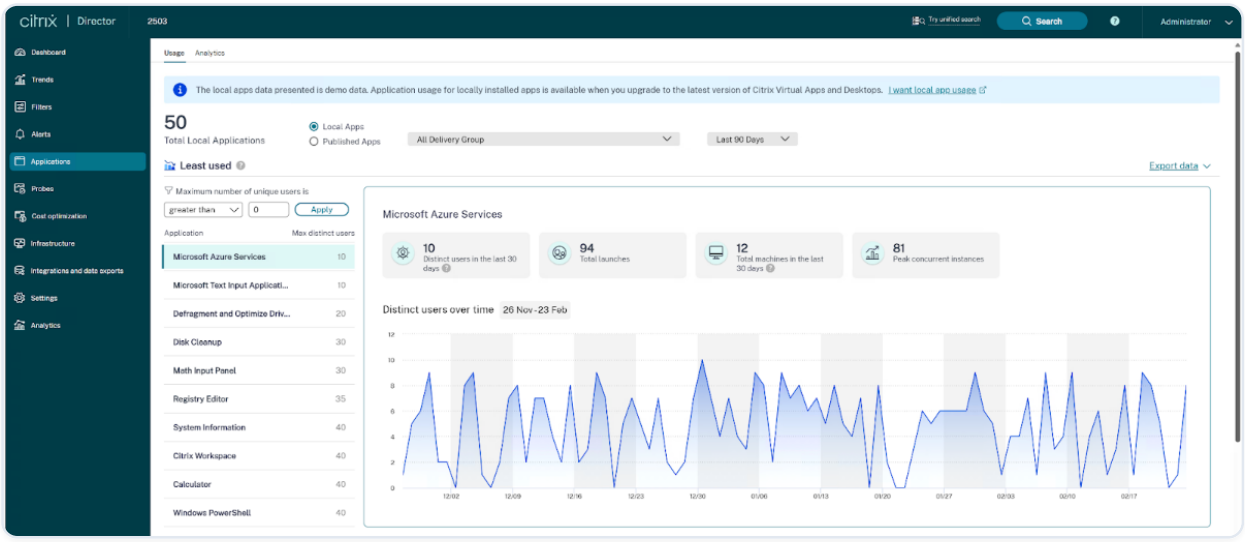
アプリケーション使用状況の詳細の表示

1. ダッシュボードの「**使用頻度の低いアプリの確認**」セクションで、「**アプリの表示**」リンクをクリックします。

   または、,

   「**アプリケーション**」タブをクリックします。次のページが表示されます。

   「**ローカルアプリ**」オプションが選択されている場合:



「**公開済みアプリ**」オプションが選択されている場合:

「アプリケーション」タブ(/en-us/citrix-virtual-apps-desktops/2511/media/dir-app-analytics-published.png)

2. 目的のデリバリーグループを選択します。
3. 必要な期間を選択します。(注: 最適な分析のため、デフォルトは過去90日間です。)

   次の情報が表示されます。

   - **ローカルおよび公開済みアプリケーションの合計:** ローカルおよび公開済みアプリケーションの合計数を表示します。
   - **使用頻度の低いもの:** 選択した期間で、一意のユーザーが最も少ないアプリを表示します。計算は次のように行われます。

     a. **1日のユーザー数:** 各アプリの一意のユーザー数が毎日カウントされます。

     b. **1日のピーク使用量:** 各アプリの1日のユーザー数の最高値が特定されます。

     c. **全体で最も高い使用量:** 選択した期間における各アプリのユーザー数の最高値が決定されます。

     d. **昇順:** アプリは、最も低いユーザー数のアプリから始まり、全体で最も高いユーザー数に基づいて昇順で一覧表示されます。

> **注:**
>
> 分析期間として過去90日間を選択することをお勧めします。この期間は四半期分のデータを提供し、アプリの使用パターンを包括的に把握できます。ただし、7日間および1か月でフィルタリングするオプションも利用できます。

- **未使用:** 過去90日間で一度も起動されていないアプリケーションが表示されます。それらが配信されたデリバリーグループ、アプリのバージョン、および最終使用の正確なタイムスタンプが提供されます。この情報は、管理者が仮想デスクトップからアプリケーションを削除する前に、情報に基づいた意思決定を行うのに役立ちます。

  「アプリケーション」タブ - 未使用(/en-us/citrix-virtual-apps-desktops/2511/media/dir-app-analytics-not-used.png)

4. **使用頻度の低い**カテゴリからアプリを選択して、以下の詳細な使用情報を表示します。

   - **過去30日間のユニークユーザー数:** 過去30日間にアプリにアクセスしたユニークユーザーの数を表示します。7日間でフィルタリングした場合、このメトリックは選択したアプリのその7日間のユニークユーザー数を表示します。

   > **注:**
   >
   > 90日を選択した場合でも、このメトリックは過去30日間のデータのみを表示します。

   - **合計起動回数:** アプリが起動された回数を表示します。
   - **過去30日間の合計マシン数**: 過去30日間にインストールされたマシンの数を表示します。このメトリックは、ローカルアプリの詳細を表示している場合にのみ表示されます。
   - **ピーク同時実行インスタンス数:** 同時に実行されているインスタンスの最大数を表示します。
   - **トレンドグラフ:** 選択したアプリの経時的なユニークユーザー数を示すトレンドグラフを表示します。**詳細の表示**をクリックすると、**キャパシティ管理 > ホストされたアプリケーションの使用状況**セクションで詳細情報が表示されます。

トレンドグラフの使用方法

トレンドグラフは使用パターンを示し、選択した期間における傾向や使用量の低い期間または高い期間を特定するのに役立ちます。X軸は日数を表し、Y軸は経時的なユニークユーザー数を表します。これらのメトリックと使用パターングラフを分析することで、管理者は自信を持ってCitrix Virtual Apps™ and Desktops環境を最適化できます。

トレンドチャートは、以下の方法で使用できます。

- **データポイントにカーソルを合わせる:** 選択した期間の個別のユーザー数を表示します。
- **トレンドを表示する:** 使用パターンを特定し、アプリの使用状況が一貫しているか、一時的な急増に過ぎないかを判断します。このチャートは、管理者が従業員の活動を監視し、潜在的な

問題や改善領域を特定するのに役立ちます。たとえば、従業員が休暇を取った場合、その期間はアプリケーションの使用がない可能性があります。従業員が戻ると、アプリケーションの使用が増加します。期間のデフォルトフィルターは90日間であり、管理者がこれらの計算を行うのに役立ちます。

- **詳細を表示する:** 日付と対応する個別のユーザー数を表示します。
- **フィルターオプション:** 異なる「期間」フィルターオプションを選択して、対応するデータを表示します。

障害のトラブルシューティングのためにデータをフィルタリングする

ダッシュボードの数字をクリックするか、フィルターメニューから定義済みフィルターを選択すると、フィルタービューが開き、選択したマシンまたは障害タイプに基づいてデータが表示されます。

定義済みフィルターは編集できませんが、定義済みフィルターをカスタムフィルターとして保存し、その後変更できます。また、すべてのデリバリーグループにわたるマシン、接続、セッション、およびアプリケーションインスタンスのカスタムフィルタービューを作成できます。

1. ビューを選択します:

    - **マシン**。シングルセッションOSマシンまたはマルチセッションOSマシンを選択します。これらのビューには、構成されたマシンの数が表示されます。マルチセッションOSマシンタブには、パフォーマンスカウンターの分布を示すロード評価インデックスと、リンクにカーソルを合わせると表示されるセッション数のツールヒントも含まれます。
    - **セッション**。過去60分、過去24時間、過去7日間、またはカスタム期間など、異なる期間でセッションをフィルターします。セッションビューからセッション数を確認することもできます。アイドル時間の測定値を使用して、しきい値期間を超えてアイドル状態になっているセッションを特定します。**関連ユーザー**をクリックすると、そのユーザーのアクティビティマネージャーが開きます。**エンドポイント**名をクリックすると、そのエンドポイントのアクティビティマネージャーが開きます。**詳細表示**をクリックすると、それぞれ**ユーザーの詳細**ページまたは**エンドポイントの詳細**ページが開きます。詳細については、「ユーザーの詳細」を参照してください。
    - **接続**。過去60分、過去24時間、過去7日間、またはカスタム期間など、異なる期間で接続をフィルターします。
    - **アプリケーションインスタンス**。過去60分、過去24時間、過去7日間、またはカスタム期間など、異なる期間でアプリケーションインスタンスをフィルターします。このビューには、サーバーおよびシングルセッションOSのVDA上のすべてのアプリケーションインスタ

ンスのプロパティが表示されます。マルチセッションOSのVDA上のアプリケーションインスタンスでは、セッションアイドル時間の測定値が利用可能です。

> **注:**
>
> Windows 10 1809コンピューターにインストールされたVDAでデスクトップセッションを起動した場合、Directorのアクティビティマネージャーは、Microsoft EdgeとOfficeがアクティブに実行されているアプリケーションとして表示されることがありますが、実際にはバックグラウンドでのみ実行されています。

2. **フィルター条件**で、基準を選択します。
3. 必要に応じて、各ビューの追加タブを使用してフィルターを完了します。
4. 必要に応じて、追加の列を選択して、さらにトラブルシューティングを行います。
5. フィルターを保存して名前を付けます。
6. 複数のDirectorサーバーからフィルターにアクセスするには、それらのサーバーからアクセス可能な共有フォルダーにフィルターを保存します:
   - 共有フォルダーは、Directorサーバー上のアカウントに対して変更権限を持っている必要があります。
   - Directorサーバーは、共有フォルダーにアクセスできるように構成する必要があります。構成するには、**IIS Manager**を実行します。**Sites > Default Web Site > Director > Application Settings**で、**Service.UserSettingsPath**設定を共有フォルダーのUNCパスを反映するように変更します。
7. 後でフィルターを開くには、**Filters**メニューからフィルターの種類（Machines、Sessions、Connections、またはApplication Instances）を選択し、保存されたフィルターを選択します。
8. **Export**をクリックして、データをCSV形式ファイルにエクスポートします。最大100,000レコードのデータをエクスポートできます。この機能は、Delivery Controller™バージョン1808以降で利用可能です。
9. 必要に応じて、**Machines**または**Connections**ビューでは、フィルターされたリストで選択したすべてのマシンに対して電源制御を使用します。Sessionsビューでは、セッション制御またはメッセージ送信オプションを使用します。
10. 必要に応じて、複数のアクションを使用できます。アクションの進行状況を示すプログレスバーが表示されます。また、アクションが完了するとメッセージが表示されます。

11. **Machines**および**Connections**ビューで、失敗したマシンまたは接続の**Failure Reason**をクリックすると、障害の詳細な説明と、障害のトラブルシューティングに推奨されるアクションが表示されます。マシンおよび接続の障害理由と推奨されるアクションは、Citrix Director failure reasons and troubleshootingで確認できます。
12. **Machines**ビューで、マシン名リンクをクリックすると、対応する**Machine Details**ページに移動します。このページには、マシンの詳細が表示され、電源制御が提供され、CPU、メモリ、ディスク監視、およびGPU監視グラフが表示されます。また、**View Historical Utilization**をクリックすると、マシンのリソース使用率の傾向を確認できます。詳細については、Troubleshoot machinesを参照してください。
13. **Application Instances**ビューで、しきい値期間を超える**Idle Time**に基づいて並べ替えまたはフィルター処理を行います。終了するアイドル状態のアプリケーションインスタンスを選択します。アプリケーションインスタンスのログオフまたは切断は、同じセッション内のすべてのアクティブなアプリケーションインスタンスを終了します。詳細については、Troubleshoot applicationsを参照してください。Director、Delivery Controllers、およびVDAがバージョン7.13以降の場合、Application InstancesフィルターページとSessionsフィルターページでのアイドル時間測定が利用可能です。

注:

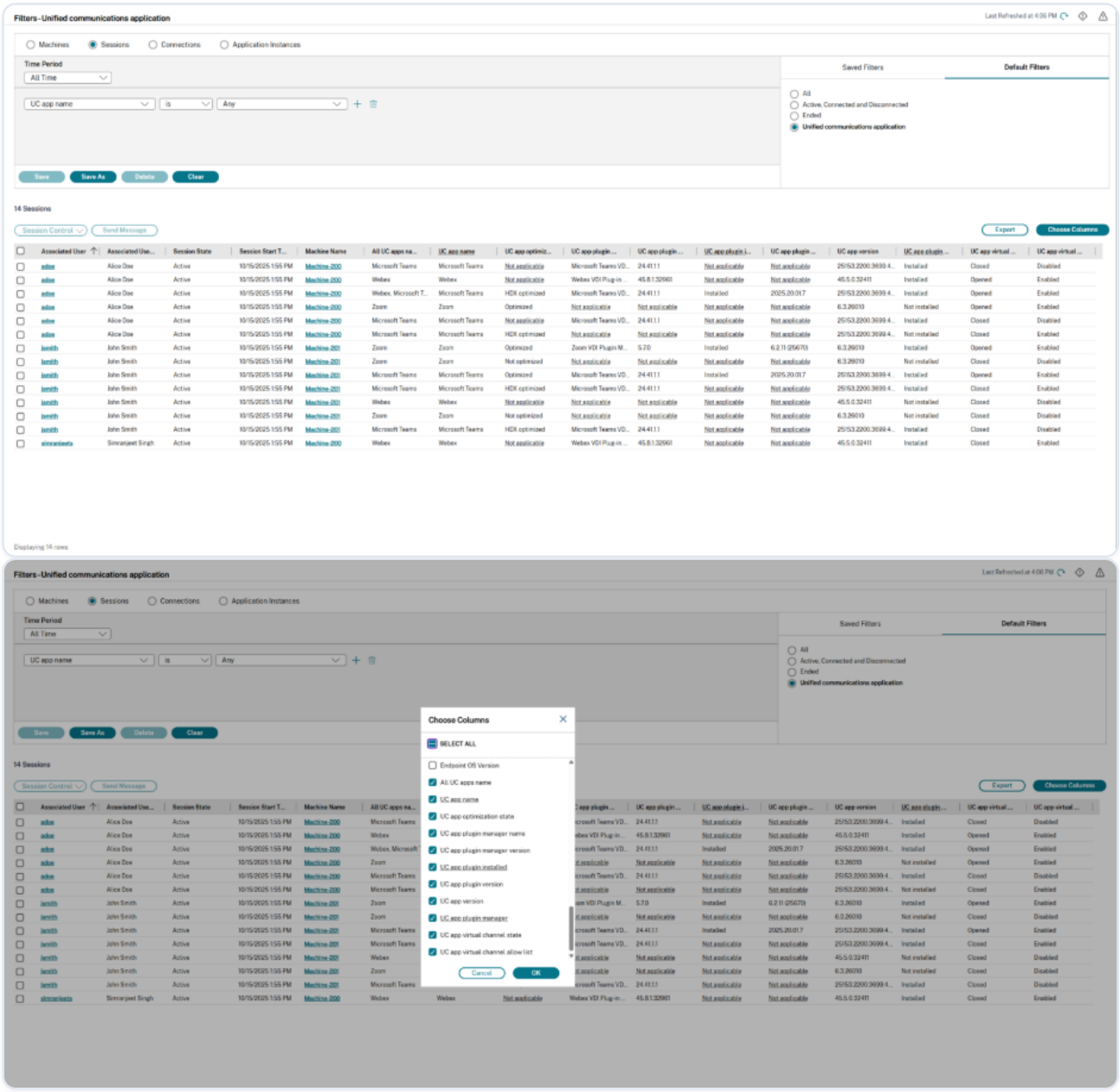
Web Studioでは、デリバリーグループ内の単一のVDAに、異なるユーザーまたはユーザーグループに対して複数のデスクトップ割り当てルール（DAR）を割り当てることができます。StoreFront™は、ログインしているユーザーに対して、DARに従って対応する表示名で割り当てられたデスクトップを表示します。しかし、DirectorはDARをサポートしておらず、ログインしているユーザーに関係なく、デリバリーグループ名を使用して割り当てられたデスクトップを表示します。その結果、Directorで特定のデスクトップをマシンにマッピングすることはできません。StoreFrontに表示される割り当てられたデスクトップをDirectorに表示されるデリバリーグループ名にマッピングするには、次のPowerShellコマンドを使用します。

```
Get-BrokerDesktopGroup | Where-Object { $_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $_.PublishedName -eq "<Name on
StoreFront>" }).DesktopGroupUid } | Select-Object -Property Name, Uid
```

ユニファイドコミュニケーションアプリのメトリック

セッションビューには、ユーザーセッションにおけるユニファイドコミュニケーション（UC）アプリケーションの使用状況に関する詳細な洞察を提供するいくつかの新しい表示列が含まれるようになりました。これらのメトリックは、セッションのリストを絞り込むためのフィルターで利用でき、メインのセッションテーブルビューに表示するために**「列の選択」**オプションを介して選択することもできます。

- **すべてのUCアプリ名（列のみ）：** セッションで同時に実行されていたすべての複数のUCアプリケーションのデータリストが含まれます。これは表示列であり、フィルターオプションではありません。
- **UCアプリ名：** 特定のユニファイドコミュニケーションアプリケーションの名前（例：Microsoft Teams、Webex、Zoom）。
- **UCアプリの最適化状態:** セッション内のUCアプリケーションの最適化状態 (例: 最適化済み、HDX最適化済み、最適化されていません、該当なし)。
- **UCアプリプラグインマネージャー名:** UCアプリケーションに使用されるプラグインマネージャーの名前。
- **UCアプリプラグインマネージャーのバージョン:** 使用されているプラグインマネージャーのバージョン。
- **UCアプリプラグインのインストール状況:** UCアプリケーションに必要なアプリケーションプラグインがインストールされているか、インストールされていないかを示します。
- **UCアプリプラグインのバージョン:** 特定のUCアプリケーションプラグインのバージョン。
- **UCアプリのバージョン:** ユニファイドコミュニケーションアプリケーション全体のバージョン。
- **UCアプリプラグインマネージャー:** UCアプリケーションに必要なアプリケーションプラグインマネージャーがエンドポイントにインストールされているか、インストールされていないかを示します。
- **UCアプリ仮想チャネルの状態:** UCアプリケーション用に確立された仮想チャネルの状態 (例: 開いています、閉じています)。
- **UCアプリ仮想チャネルの許可リスト:** アプリケーションの仮想チャネルが許可リストにあるかどうかを示します。



サイト全体の履歴トレンドを監視する

トレンドビューでは、各サイトの履歴トレンド情報に次のパラメーターでアクセスできます。

- セッション
- 接続障害
- マシンの障害
- ログオンパフォーマンス
- 負荷評価
- キャパシティ管理
- マシン使用状況

- リソース使用率
- 各サイトのネットワーク分析。

この情報を見つけるには、**トレンド**メニューをクリックします。

ズームインしてドリルダウンする機能を使用すると、期間を拡大（グラフのデータポイントをクリック）し、トレンドに関連付けられた詳細を表示するためにドリルダウンすることで、トレンドグラフをナビゲートできます。この機能により、誰が、または何が影響を受けているかの詳細をよりよく理解できます。

各グラフのデフォルトのスコープを変更するには、データに別のフィルターを適用します。

履歴トレンド情報が必要な期間を選択します。期間の可用性は、Directorの展開によって次のように異なります。

- Premiumライセンスサイトでは、最大「昨年」（365日間）までのトレンドレポートが利用できます。
- Advancedライセンスサイトでは、最大「先月」（31日間）までのトレンドレポートが利用できます。
- PremiumおよびAdvanced以外のライセンスサイトでは、最大「過去7日間」までのトレンドレポートが利用できます。

注:

- すべてのDirector展開において、期間が「先月」（**現在まで**）またはそれより短い期間に設定されている場合、セッション、障害、ログオンパフォーマンスのトレンド情報はグラフおよびテーブルとして利用できます。カスタム終了日を指定した「先月」または「昨年」として選択された期間の場合、トレンド情報はグラフとしてのみ利用でき、テーブルとしては利用できません。
- Monitor Serviceのグルーミング保持値によって、トレンドデータの可用性が制御されます。デフォルト値については、データ粒度と保持を参照してください。Premiumライセンスサイトのお客様は、グルーミング保持を希望する保持日数に変更できます。
- IISマネージャーの以下のパラメーターは、選択可能なカスタム終了日の範囲を制御します。ただし、選択された日付のデータ可用性は、測定対象の特定のメトリックに対するグルーミング保持設定によって異なります。

パラメーター	デフォルト値
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

利用可能なトレンド

セッションのトレンドを表示: セッションタブから、デリバリーグループと期間を選択して、同時セッション数に関する詳細情報を表示します。

セッションの自動再接続列には、セッション内の自動再接続の数が表示されます。自動再接続は、セッションの信頼性ポリシーまたはクライアントの自動再接続ポリシーが有効な場合に有効になります。エンドポイントでネットワークが中断されると、次のポリシーが有効になります。

- セッションの信頼性が有効になり（デフォルトで3分間）、Citrix Receiver™またはCitrix Workspace™アプリがVDAへの接続を試行します。
- クライアントの自動再接続が3分から5分の間に有効になり、クライアントがVDAへの接続を試行します。

両方の再接続がキャプチャされ、ユーザーに表示されます。この情報は、再接続が発生してからDirector UIに表示されるまでに最大5分かかる場合があります。

自動再接続情報は、中断のあるネットワーク接続の表示とトラブルシューティングに役立ちます。また、シームレスなエクスペリエンスを持つネットワークも分析します。フィルターで選択した特定のデリバリーグループまたは期間の再接続数を表示できます。ドリルダウンでは、セッションの信頼性やクライアントの自動再接続、タイムスタンプ、エンドポイントIP、Workspaceアプリがインストールされているマシンのエンドポイント名などの追加情報が提供されます。

デフォルトでは、ログはイベントのタイムスタンプの降順でソートされます。この機能は、Windows用Citrix Workspaceアプリ、Mac用Citrix Workspaceアプリ、Windows用Citrix Receiver、およびMac用Citrix Receiverで利用できます。この機能には、Delivery Controller™バージョン7 1906以降、およびVDA 1906以降が必要です。

セッションの再接続の詳細については、「セッション」を参照してください。

ポリシーの詳細については、クライアントの自動再接続ポリシー設定およびセッションの信頼性ポリシー設定を参照してください。

自動再接続データがDirectorに表示されない場合があります。その理由は次のとおりです。

- Workspaceアプリが自動再接続データをVDAに送信していません。
- VDAがモニターサービスにデータを送信していません。
- デリバリーコントローラーは、対応するセッションがない可能性があるため、VDAペイロードを破棄します。

> **注:**
>
> 場合によっては、特定のCitrix Gatewayポリシーが設定されていると、クライアントIPアドレスが正しく取得されないことがあります。

> **接続障害の傾向を表示:** タブから、接続、マシンタイプ、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のユーザー接続障害に関する詳細情報を含むグラフを表示します。

マシン障害の傾向を表示: シングルセッションOSマシン障害タブまたはマルチセッションOSマシンタブから、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のマシン障害に関する詳細情報を含むグラフを表示します。

ログオンと再接続のパフォーマンスの傾向を表示: タブから、デリバリーグループと期間を選択して、サイト全体のユーザーログオンおよび再接続の期間に関する詳細情報を含むグラフを表示します。このビューは、ログオンまたは再接続の数と全体的なパフォーマンスを把握するのに役立ちます。

グラフには以下が含まれます。

- **ログオンイベント、ログオン期間、およびフェーズ**(ブローカリング、対話型セッションなど)は、新しいセッションを起動する際のユーザーエクスペリエンスに関する洞察を提供します。
- **再接続イベントと再接続期間**。切断されたセッションから再接続する際のユーザーエクスペリエンスに関する洞察を提供します。

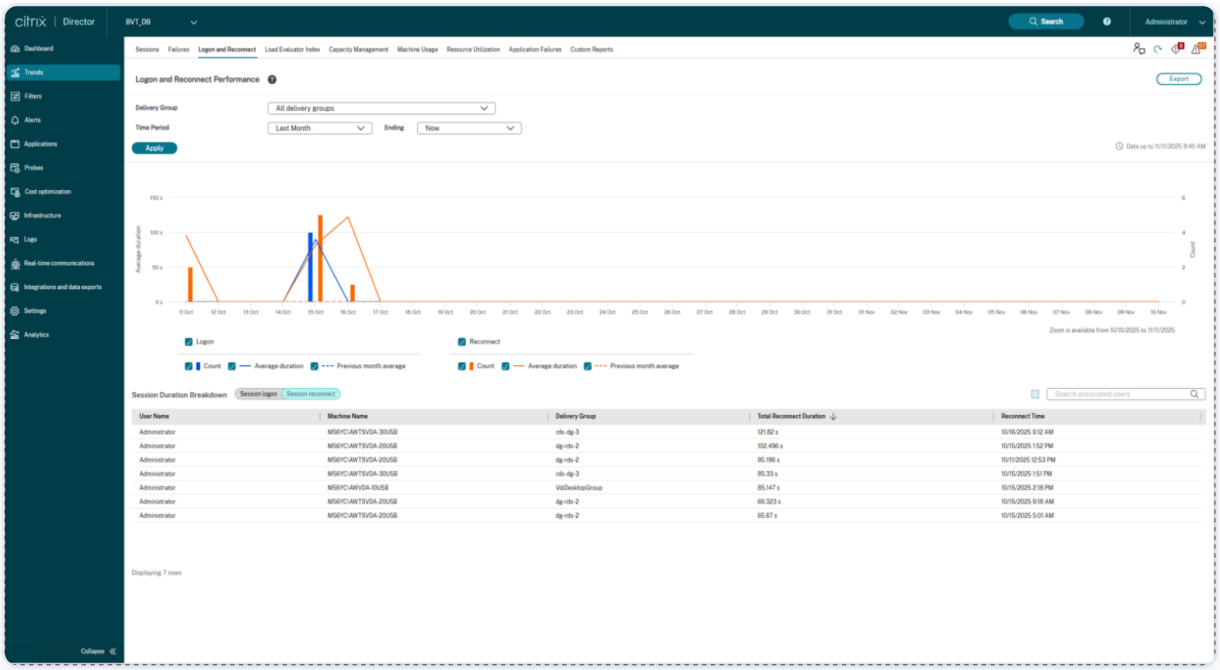
凡例を使用して、分析されている傾向に基づいて必要なメトリックを選択します。

- カウント
- 平均期間

- 以前の（期間）平均

グラフの下のテーブルには、ユーザーセッションまたは接続ごとの**セッションログオン**と**セッション再接続**の詳細が表示されます。テーブルの上の選択肢を使用してメトリックを切り替えたり、表示する列を選択したり、任意の列で並べ替えたり、レポートをPDF、Excel、またはCSV形式でエクスポートしたりできます。

> **注:**
>
> セッション再接続時間は、**DirectorおよびVDAバージョン2511 CR以降**でサポートされています。



負荷評価の傾向を表示: 負荷評価インデックスタブから、マルチセッションOSマシン間に分散されている負荷に関する詳細情報を含むグラフを表示します。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のマルチセッションOSマシン、マルチセッションOSマシン（デリバリーグループ内のマルチセッションOSマシンが選択されている場合にのみ利用可能）、および範囲が含まれます。

ホストされているアプリケーションの使用状況を表示: この機能の利用可否は、組織のライセンスによって異なります。 **キャパシティ管理**タブから、**ホストされているアプリケーションの使用状況**タブを選択します。デリバリーグループと期間を選択して、ピーク時の同時使用状況を示すグラフと、アプリケーションベースの使用状況を示すテーブルを表示します。アプリケーションベースの使用状況テーブルから、特定のアプリケーションを選択して詳細を表示したり、そのアプリケーションを使用している、または使用したユーザーのリストを表示したりできます。

Single-sessionおよびMulti-session OSの使用状況を表示: トレンドビューには、サイト別およびデリバリーグループ別のSingle-session OSの使用状況が表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、ユーザーごとの使用状況が表示されます。 トレンドビューには、サイト別、デリバリーグループ別、およびマシン別のMulti-session OSの使用状況も表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、マシンごとおよびユーザーごとの使用状況が表示されます。マシンが選択されている場合は、ユーザーごとの使用状況が表示されます。

仮想マシンの使用状況を表示: マシン使用状況タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択すると、VM使用状況のリアルタイムビューが表示され、サイトのキャパシティニーズを迅速に評価できます。 シングルセッションOSの可用性 - サイト全体または特定のデリバリーグループの可用性別に、シングルセッションOSマシン（VDI）の現在の状態を表示します。 マルチセッションOSの可用性 - サイト全体または特定のデリバリーグループの可用性別に、マルチセッションOSマシンの現在の状態を表示します。

表示されるバナーの以下のリンクをクリックすると、**コスト最適化**によるマシン使用状況の可視性を高めることができます。

- 推定節約額 - このリンクをクリックすると、**コスト最適化**ページの**推定節約額**セクションに移動し、すべてのデリバリーグループの詳細が表示されます。
- 節約レポート - このリンクをクリックすると、**コスト最適化**ページの**節約レポート**セクションに移動し、すべてのデリバリーグループの詳細が表示されます。

> **注:**
>
> 利用可能カウンターに表示されるマシンの数には、メンテナンスモードのマシンが含まれます。

> **リソース使用率を表示: リソース使用率**タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択すると、各VDIマシンのCPUおよびメモリ使用量、IOPS、ディスク遅延に関する履歴傾向データが把握でき、より適切なキャパシティプランニングが可能になります。 この機能には、Delivery ControllerおよびVDAの**バージョン7.11**以降が必要です。 グラフには、平均CPU、平均メモリ、平均IOPS、ディスク遅延、およびピーク時の同時セッションのデータが表示されます。マシンにドリルダウンして、CPUを消費している上位10個のプロセスのデータとグラフを表示できます。

デリバリーグループと期間でフィルターします。CPU、メモリ使用量、およびピーク時の同時セッションのグラフは、過去2時間、24時間、7日間、1か月、1年間で利用できます。平均IOPSとディスク遅延のグラフは、過去24時間、1か月、1年間で利用できます。バナーの**チェックアウト**リンクをクリックすると、コスト最適化によるマシン使用状況の可視性を高めることができます。このリンクをクリックすると、**コスト最適化**ページの**ワークロードの適正化**タブに移動し、**リソース使用率**タブから選択されたデリバリーグループの詳細が表示されます。

注:

- 履歴マシン使用率ページの「上位10プロセス」テーブルでデータを収集して表示するには、監視ポリシー設定の**プロセス監視を有効にする**を**許可**に設定する必要があります。このポリシーは、デフォルトで**禁止**に設定されています。すべてのリソース使用率データはデフォルトで収集されます。これは、**リソース監視を有効にする**ポリシー設定を使用して無効にできます。グラフの下のテーブルには、マシンごとのリソース使用率データが表示されます。詳細については、「監視ポリシー設定」を参照してください。
- 平均IOPSは日次平均を表示します。ピークIOPSは、選択した時間範囲におけるIOPS平均の最高値として計算されます。(IOPS平均とは、VDAで1時間内に収集されたIOPSの時間平均です)。
- マシンのドリルダウンは、平均CPU使用率または平均メモリ使用率が1%を超えるプロセスを一覧表示します。これは、場合によっては10未満のプロセスしか表示されない可能性があることを意味します。

ネットワーク分析データの表示: この機能の可用性は、組織のライセンスと管理者権限によって異なります。この機能には、Delivery Controllerの**バージョン7.11**以降が必要です。

ネットワークタブから、ネットワーク分析を監視します。これにより、ネットワークのユーザー、アプリケーション、デスクトップのコンテキストビューが提供されます。この機能により、DirectorはCitrix ADMからのHDX Insightレポートを通じて、展開におけるICAトラフィックの高度な分析を提供します。詳細については、「ネットワーク分析の構成」を参照してください。

アプリケーション障害の表示: アプリケーション障害タブは、VDA上の公開アプリケーションに関連する障害を表示します。

この機能には、Delivery ControllerおよびVDA **バージョン7.15**以降が必要です。Windows Vista以降を実行するシングルセッションOS VDA、およびWindows Server 2008以降を実行するマルチ

セッションOS VDAがサポートされています。 詳しくは、「履歴アプリケーション障害監視」を参照してください。

デフォルトでは、マルチセッションOS VDAからのアプリケーション障害のみが表示されます。監視ポリシーを使用して、アプリケーション障害の監視を設定できます。詳細については、「監視ポリシー設定」を参照してください。

プローブ結果の表示: プローブ結果タブは、構成ページでプローブ用に構成されたアプリケーションおよびデスクトップのプローブ結果を表示します。ここには、障害が発生した起動の段階が記録されます。

詳しくは、「アプリケーションおよびデスクトップのプローブ」を参照してください。

カスタマイズされたレポートの作成: カスタムレポートタブは、監視データベースからのリアルタイムデータと履歴データを含むカスタムレポートを表形式で生成するためのユーザーインターフェイスを提供します。

この機能には、Delivery Controllers **バージョン7.12**以降が必要です。

以前に保存したカスタムレポートクエリのリストから、**実行してダウンロード**をクリックしてレポートをCSV形式でエクスポートしたり、**ODataをコピー**をクリックして対応するODataクエリをコピーして共有したり、**編集**をクリックしてクエリを編集したりできます。 マシン、接続、セッション、またはアプリケーションインスタンスに基づいてカスタムレポートクエリを作成できます。マシン、デリバリーグループ、期間などのフィールドに基づいてフィルター条件を指定します。カスタムレポートに必要な追加の列を指定します。プレビューには、レポートデータのサンプルが表示されます。カスタムレポートクエリを保存すると、保存されたクエリのリストに追加されます。

コピーしたODataクエリに基づいてカスタムレポートクエリを作成できます。これを行うには、ODataクエリオプションを選択し、コピーしたODataクエリを貼り付けます。結果のクエリは後で実行するために保存できます。

> **注:**
>
> ODataクエリを使用して生成されたプレビューおよびエクスポートレポートの列名はローカライズされておらず、英語で表示されます。

グラフ上のフラグアイコンは、特定の期間における重要なイベントまたはアクションを示します。フラグにマウスを合わせ、クリックしてイベントまたはアクションを一覧表示します。

注:

- HDX™接続ログオンデータは、7より前のVDAでは収集されません。それより前のVDAの場合、グラフデータは0と表示されます。
- Citrix Studioで削除されたデリバリーグループは、関連データが整理されるまで、Director Trendsフィルターで選択可能です。削除されたデリバリーグループを選択すると、保持期間までの利用可能なデータのグラフが表示されます。ただし、テーブルにはデータは表示されません。
- アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、新しいデリバリーグループの**リソース使用率と負荷評価インデックス**テーブルに、古いデリバリーグループと新しいデリバリーグループから統合されたメトリックが表示されます。

Autoscale管理マシンの監視

Autoscaleは、デリバリーグループ内の登録済みすべてのマルチセッションおよびシングルセッションOSマシンのプロアクティブな電源管理を可能にする電源管理機能です。Web Studioで、選択したデリバリーグループに対してAutoscaleを構成できます。詳細については、「Autoscale」(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/autoscale.html)を参照してください。Directorを使用して、Autoscaleが有効なマシンの主要なメトリックを監視できます。

マシン使用状況

マシンの使用状況ページには、選択したデリバリーグループと期間において電源がオンになっているAutoscaleが有効なマルチセッションおよびシングルセッションOSマシンの合計数が表示されます。このメトリックは、デリバリーグループ内のマシンの実際の使用状況を示します。 **シングルセッションOSマシン**タブまたは**マルチセッションOSマシン**タブから、デリバリーグループと期間を選択します。

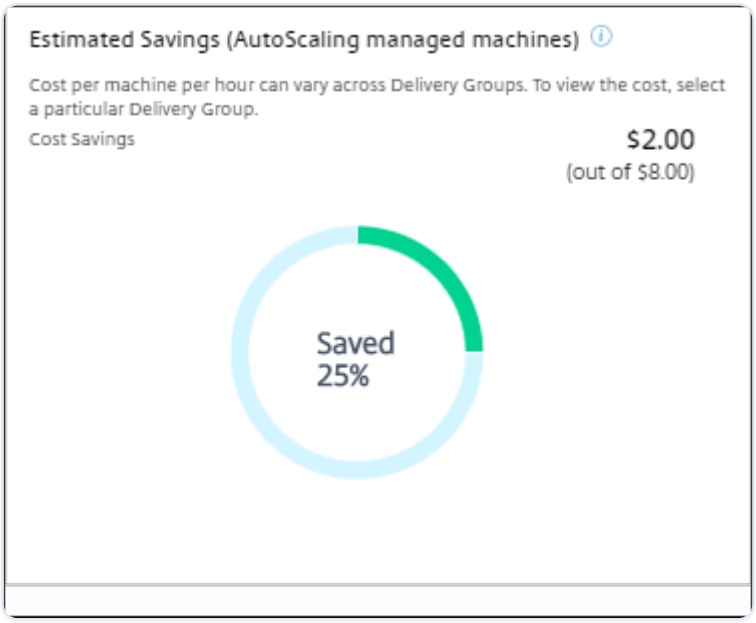
このグラフには、次のメトリックが表示されます:

- **電源オンのマシン** - 電源がオンになっているAutoscaleが有効なマシンの数
- **登録済みマシン** - 登録済みのマルチセッションまたはシングルセッションOSマシンの数

- **メンテナンス中のマシン** - メンテナンスモードがオンになっているマルチセッションまたはシングルセッションOSマシンの数

推定節約額

マシン使用状況ページには、選択したデリバリーグループでAutoscaleを有効にすることによって達成された推定コスト削減額も表示されます。



推定節約額は、**デリバリーグループの編集** > **Autoscale**で構成されている、1時間あたりのマシンごとの節約率（米ドル）として計算されます。マシンごとの節約額の構成について詳しくは、「Autoscale」(/ja-jp/citrix-virtual-apps-desktops/2511/manage-deployment/autoscale.html)を参照してください。

すべてのデリバリーグループを選択すると、すべてのデリバリーグループにおける推定節約額の平均値が表示されます。

推定節約額は、管理者が既存のインフラストラクチャを統合し、最大の節約と利用率を達成するための容量を計画するのに役立ちます。

マシンとセッションのアラート通知

Directorダッシュボードには、アラート通知が表示されます。これらの通知はさらにドリルダウンできます。アラートの詳細は、**アラート**ページに表示されます。

- デリバリーグループでアラートポリシーを作成するには、**アラート** > **Citrixアラートポリシー** > **デリバリーグループポリシー**に移動します。
- ここで、次の警告および重大なしきい値を設定できます。

    - 失敗したマシン（シングルセッションOS）および失敗したマシン（マルチセッションOS）、,
    - デリバリーグループ内のピーク接続セッション、ピーク切断セッション、およびピーク同時合計セッション。

- デリバリーグループ内の対応するメトリックがしきい値に達すると、アラートが生成されます。

アラートポリシーの条件と新しいアラートポリシーの作成に関する詳細については、「アラートと通知」を参照してください。

マシンのステータス

- **フィルター** > **マシン**には、すべてのマシンの電源状態が表形式で表示されます。特定のデリバリーグループでフィルターできます。
- **フィルター** > **セッション**には、マシン名でフィルターして、関連するセッションとそのリアルタイムステータスが表示されます。
- **トレンド** > **セッション**で、デリバリーグループと期間を選択して、セッションとその関連メトリックの傾向を確認します。

詳細については、「障害のトラブルシューティングのためにデータをフィルターする」を参照してください。

負荷評価のトレンド

トレンド > **負荷評価インデックス**ページには、マルチセッションOSマシン間で分散される負荷に関する詳細情報を示すグラフが表示されます。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のマルチセッションOSマシン、マルチセッションOSマシン（デリバリーグループ内のマルチセッションOSマシンが選択されている場合にのみ利用可能）、および範囲が含まれます。負荷評価インデックスは、合計CPU、メモリ、ディスク、またはセッションの割合として表示され、最後の間隔での接続ユーザー数と比較して示されます。

展開のトラブルシューティング

アプリケーションのトラブルシューティング

リアルタイムアプリケーション監視

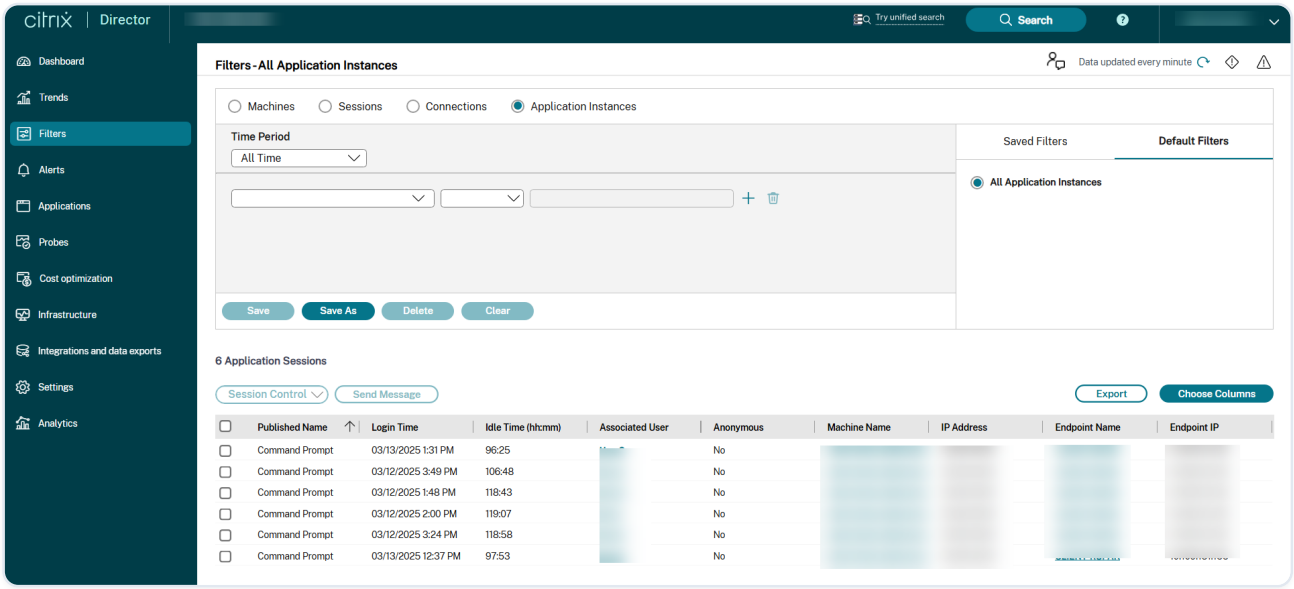
アイドル時間メトリックを使用して、特定の時間制限を超えてアイドル状態になっているインスタンスを特定することで、アプリケーションとセッションのトラブルシューティングを行うことができます。

アプリケーションベースのトラブルシューティングの典型的なユースケースは、従業員がアプリケーションライセンスを共有する医療分野です。そこでは、アイドル状態のセッションとアプリケーションインスタンスを終了して、Citrix Virtual Apps and Desktops™環境をパージしたり、パフォーマンスの低いサーバーを再構成したり、アプリケーションを保守およびアップグレードしたりする必要があります。

「**アプリケーションインスタンス**」フィルターページには、サーバーおよびシングルセッションOSのVDA上のすべてのアプリケーションインスタンスが一覧表示されます。関連するアイドル時間測定値は、マルチセッションOSのVDA上で10分以上アイドル状態になっているアプリケーションインスタンスに対して表示されます。

> **注:**
>
> アプリケーションインスタンスのメトリックは、すべてのライセンスエディションのサイトで利用できます。

この情報を使用して、特定の期間を超えてアイドル状態になっているアプリケーションインスタンスを特定し、必要に応じてログオフまたは切断します。これを行うには、**フィルター \> アプリケーションインスタンス** を選択し、事前に保存されたフィルターを選択するか、**すべてのアプリケーションインスタンス** を選択して独自のフィルターを作成します。



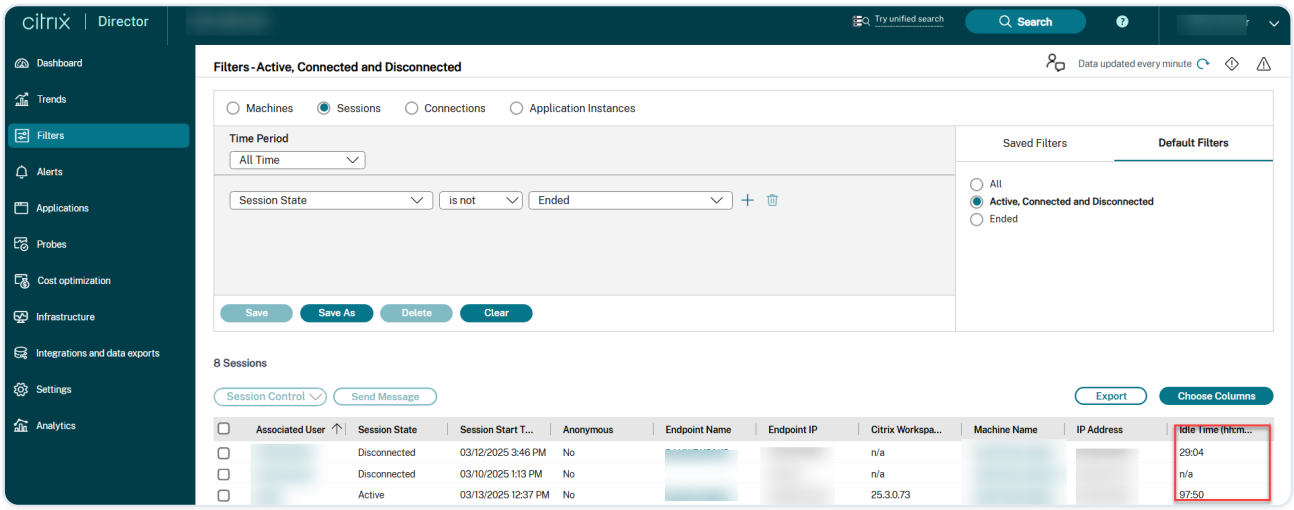
フィルターの例は次のとおりです。**フィルター条件**として、**公開名**（アプリケーションの）と**アイドル時間**を選択します。次に、**アイドル時間**を特定の時間制限の**以上**に設定し、再利用のためにフィルターを保存します。フィルターされたリストから、アプリケーションインスタンスを選択し

ます。メッセージを送信するオプションを選択するか、**セッション制御**ドロップダウンから**ログオフ**または**切断**を選択してインスタンスを終了します。

注:

アプリケーションインスタンスをログオフまたは切断すると、現在のセッションがログオフまたは切断され、同じセッションに属するすべてのアプリケーションインスタンスが終了します。

「**セッション**」フィルターページから、セッションの状態とセッションアイドル時間メトリックを使用して、アイドル状態のセッションを特定できます。**アイドル時間**列で並べ替えるか、フィルターを定義して、特定の時間制限を超えてアイドル状態になっているセッションを特定します。アイドル時間は、マルチセッションOSのVDA上で10分以上アイドル状態になっているセッションに対して表示されます。



セッションまたはアプリケーションインスタンスが次の条件の場合、**アイドル時間**は**N/A**と表示されます。

- 10分以上アイドル状態になっていない、,
- シングルセッションOSのVDAで起動されている、または
- バージョン7.12以前を実行しているVDAで起動されている。

アプリケーション障害の履歴監視

「**トレンド**」-\>「**アプリケーション障害**」タブには、VDA上の公開アプリケーションに関連する障害が表示されます。

アプリケーション障害の傾向は、PremiumおよびAdvancedライセンスサイトの場合、過去2時間、24時間、7日間、および1か月間利用できます。その他のライセンスタイプの場合、過去2時間、24時間、および7日間利用できます。「Application Errors」をソースとしてイベントビューアにログ記録されたアプリケーション障害が監視されます。**エクスポート**をクリックすると、CSV、Excel、またはPDF形式でレポートが生成されます。

アプリケーション障害監視のグルーミング保持設定であるGroomApplicationErrorsRetentionDaysとGroomApplicationFaultsRetentionDaysは、Premiumおよび非Premiumライセンスサイトの両方で、デフォルトで1日に設定されています。この設定は、PowerShellコマンドを使用して変更できます。

```
Set-MonitorConfiguration -\<setting name\> \<value\>
```

アプリケーション障害の傾向(/en-us/citrix-virtual-apps-desktops/2511/media/dir_application_faults.png)

障害は、その重大度に基づいて**アプリケーションフォールト**または**アプリケーションエラー**として表示されます。アプリケーションフォールトタブには、機能またはデータの損失に関連する障害が表示されます。アプリケーションエラーは、すぐには関連しない問題を示し、将来問題を引き起こす可能性のある状態を示します。

障害は、**公開アプリケーション名**、**プロセス名**、**デリバリーグループ**、および**期間**に基づいてフィルタリングできます。テーブルには、フォールトまたはエラーコードと障害の簡単な説明が表示されます。詳細な障害の説明はツールチップとして表示されます。

注:

対応するアプリケーション名を導出できない場合、公開アプリケーション名は「Unknown」と表示されます。これは通常、起動されたアプリケーションがデスクトップセッションで失敗した場合、または依存する実行可能ファイルによって引き起こされた未処理の例外が原因で失敗した場合に発生します。

デフォルトでは、マルチセッションOS VDAでホストされているアプリケーションのフォールトのみが監視されます。監視グループポリシー（アプリケーション障害の監視を有効にする、シングルセッションOS VDAでのアプリケーション障害の監視を有効にする、障害監視から除外されるアプリケーションのリスト）を通じて監視設定を変更できます。詳細については、監視ポリシー設定のアプリケーション障害監視のポリシーを参照してください。

「**トレンド**」\>「**アプリケーションプローブ結果**」ページには、過去24時間および7日間にサイトで実行されたアプリケーションプローブの結果が表示されます。アプリケーションプローブの構成方法の詳細については、アプリケーションプローブを参照してください。

マシンのトラブルシューティング

> **注:**
>
> **Citrix Health Assistant**は、未登録VDAの構成に関する問題をトラブルシューティングするためのツールです。このツールは、VDA登録の失敗、セッション起動、およびタイムゾーンリダイレクト構成における問題の根本原因を特定するために、いくつかのヘルスチェックを自動化します。ナレッジセンターの記事「Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch」には、**Citrix Health Assistant**ツールのダウンロードと使用方法が記載されています。

> Directorコンソールの**フィルター > マシン**ビューには、サイトで構成されているマシンが表示されます。マルチセッションOSマシンタブには、パフォーマンスカウンターの分布を示す負荷評価インデックスと、リンクにカーソルを合わせるとセッション数のツールヒントが表示されます。

失敗したマシンの**失敗理由**列をクリックすると、失敗の詳細な説明と、その失敗をトラブルシューティングするために推奨されるアクションが表示されます。マシンおよび接続の失敗の理由と推奨されるアクションについては、「Citrix Directorの失敗理由とトラブルシューティング」を参照してください。

マシン名リンクをクリックすると、**マシン詳細**ページに移動します。

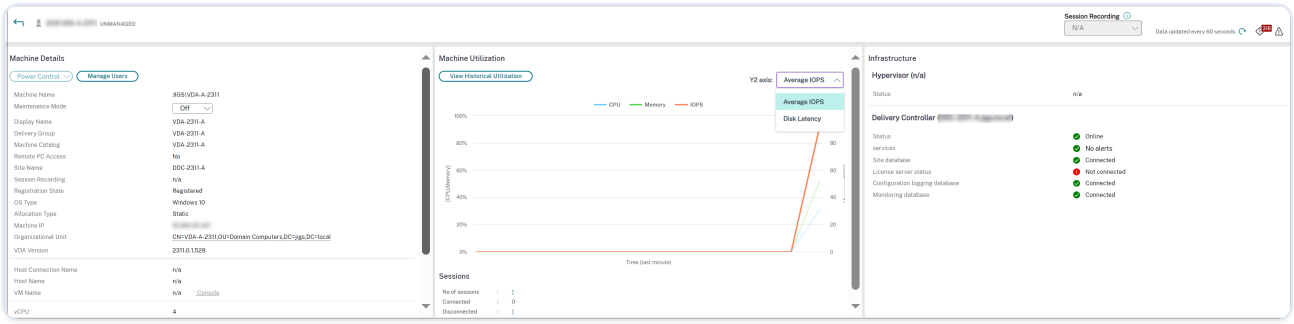
マシン詳細ページには、マシンの詳細、インフラストラクチャの詳細、およびマシンに適用されている修正プログラムの詳細が一覧表示されます。

マシンベースのリアルタイムリソース使用率

マシン使用率パネルには、CPUとメモリのリアルタイム使用率を示すグラフが表示されます。さらに、Delivery ControllerとVDAのバージョンが**7.14**以降のサイトでは、ディスクとGPUの監視グラフを利用できます。

ディスク監視グラフ、平均IOPS、ディスク遅延は、VDAディスクに関連する問題を監視およびトラブルシューティングするのに役立つ重要なパフォーマンス測定値です。平均IOPSグラフは、

ディスクへの読み取りと書き込みの平均数を表示します。**ディスク遅延**を選択すると、データ要求からディスクからの応答までの遅延をミリ秒単位で測定したグラフが表示されます。



GPU使用率

GPU使用率を選択すると、GPU、GPUメモリ、エンコーダー、デコーダーのパーセンテージ使用率が表示され、マルチセッションおよびシングルセッションOS VDAでのGPU関連の問題をトラブルシューティングできます。

サポートされているGPUバージョン：

- ディスプレイドライバーバージョン369.17以降を実行しているNVIDIA Tesla M60 GPU。詳細については、「NVIDIA vGPU Software」を参照してください。
- AMD Radeon Instinct MI25 GPU および AMD EPYC 7V12(Rome) CPU。詳細については、AMD Drivers and Support を参照してください。

ドライバー:

適切なドライバーまたは拡張機能をVDAにインストールする必要があります。

- NVIDIA GPU の場合は、GRID ドライバーを手動または拡張機能経由でインストールします。詳細については、NVIDIA vGPU Software を参照してください。
  - NVIDIA の場合、GRID ドライバーのみがサポートされます。CUDA ドライバーは NVadsA10 v5 シリーズでは動作せず、サポートされていません。
  - Azure ベースのマシンに拡張機能経由で NVIDIA Grid GPU ドライバーをインストールする手順の例については、NVIDIA GRID drivers. NVIDIA GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines を参照してください。
  - NVIDIA Grid GPU ドライバーを手動でインストールする手順の例については、Azure N-series NVIDIA GPU driver setup for Windows - Azure Virtual Machines を参照してください。
- AMD GPU の場合は、AMD グラフィックドライバーを手動または拡張機能経由でインストールします。詳細については、AMD Drivers and Support を参照してください。

  - Azure ベースのマシンに拡張機能経由で AMD GPU ドライバーをインストールする手順の例については、AMD GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines を参照してください。
  - Azure マシンに AMD GPU ドライバーを手動でインストールする手順の例については、Install AMD GPU drivers on N-series VMs running Windows を参照してください。

使用上の注意:

- GPU 使用率グラフは、64 ビット Windows を実行している VDA でのみ利用できます。
- GPU アクセラレーションを提供するには、VDA で HDX 3D Pro を有効にする必要があります。詳細については、GPU acceleration for Windows Single-session OS および GPU acceleration for Windows Multi-session OS を参照してください。
- VDA が複数の GPU にアクセスする場合、使用率グラフには個々の GPU から収集された GPU メトリックの平均が表示されます。GPU メトリックは VDA 全体に対して収集され、個々のプロセスに対しては収集されません。
- AMD の場合、エンコーダーとデコーダーの使用状況は個別にサポートされていません。GPU を使用するエンコード/デコードのワークロードはすべて、GPU 使用率における一般的な 3D 負荷として報告されます。
- インストール中にNVIDIA WMIをインストールするようにしてください。このウィンドウは手動インストール時にのみ利用可能です。
- ドライバーがインストールされているにもかかわらず、DirectorがGPUを検出しない場合
  - タスクマネージャーを確認してください。ドライバーが適切にインストールされていれば、GPUはタスクマネージャーに表示されるはずです。
  - マシンが登録されているか確認してください。マシンがオンラインとして検出されるまでに時間がかかる場合があります。
- DirectorでGPU使用率にアクティビティが表示されない場合は、実行しているワークロードがGPUを使用していることを確認してください。グラフィックワークロードの場合、これは > > > > から有効にできます。必ずをオンにしてください。場合によっては、他の設定に基づいて、これがシステムデフォルトまたは省電力に設定されていると、Windowsはグラフィックワークロードにcpuを使用するようデフォルトで設定されます。
- データは毎分更新され、**GPU使用率**を選択してから1分以内にデータの視覚化が開始されます。

マシンベースの履歴リソース使用率

マシン使用率パネルで、**履歴使用率の表示**をクリックして、選択したマシン上のリソースの履歴使用状況を表示します。 使用率グラフには、CPU、メモリ、ピーク時の同時セッション、平均IOPS、ディスク遅延の重要なパフォーマンスカウンターが含まれます。

> **注:**
>
> 監視ポリシー設定の**プロセス監視を有効にする**は、履歴マシン使用率ページのトップ10プロセス表でデータを収集および表示するために、Allowedに設定する必要があります。収集はデフォルトで禁止されています。

> CPUとメモリの使用率、平均IOPS、およびディスク遅延データはデフォルトで収集されます。**リソース監視を有効にする**ポリシー設定を使用して、収集を無効にできます。

履歴マシン使用率(/en-us/citrix-virtual-apps-desktops/2511/media/dir-machine-util-historical.png)

1. **マシン詳細**ビューの**マシン使用率**パネルから、**履歴使用率の表示**を選択します。
2. **履歴マシン使用率**ページで、**期間**を「過去2時間」、「過去24時間」、「過去7日間」、「月」、「年」に設定して使用状況を表示します。

   > **注:**
   >
   > 平均IOPSとディスク遅延の使用状況データは、現在までの過去24時間、月、年についてのみ利用可能です。カスタム終了時刻はサポートされていません。

3. **適用**をクリックし、必要なグラフを選択します。
4. グラフの異なるセクションにカーソルを合わせると、選択した期間の詳細情報が表示されます。



例えば、**過去2時間**を選択した場合、ベースライン期間は選択した時間範囲の前の2時間です。過去2時間およびベースライン期間のCPU、メモリ、セッションの傾向を表示します。**先月**を選択した場合、ベースライン期間は前月です。先月およびベースライン期間の平均IOPSとディスク遅延を表示するように選択します。

1. **エクスポート**をクリックして、選択した期間のリソース使用状況データをエクスポートします。詳細については、展開の監視のレポートのエクスポートセクションを参照してください。
2. グラフの下の表には、CPUまたはメモリ使用率に基づいて上位10個のプロセスが一覧表示されます。選択した時間範囲でのアプリケーション名、ユーザー名、セッションID、平均CPU、ピークCPU、平均メモリ、ピークメモリを示す任意の列で並べ替えることができます。IOPSとディスク遅延の列は並べ替えることができません。

   > **注:**
   >
   > システムプロセスのセッションIDは「0000」と表示されます。

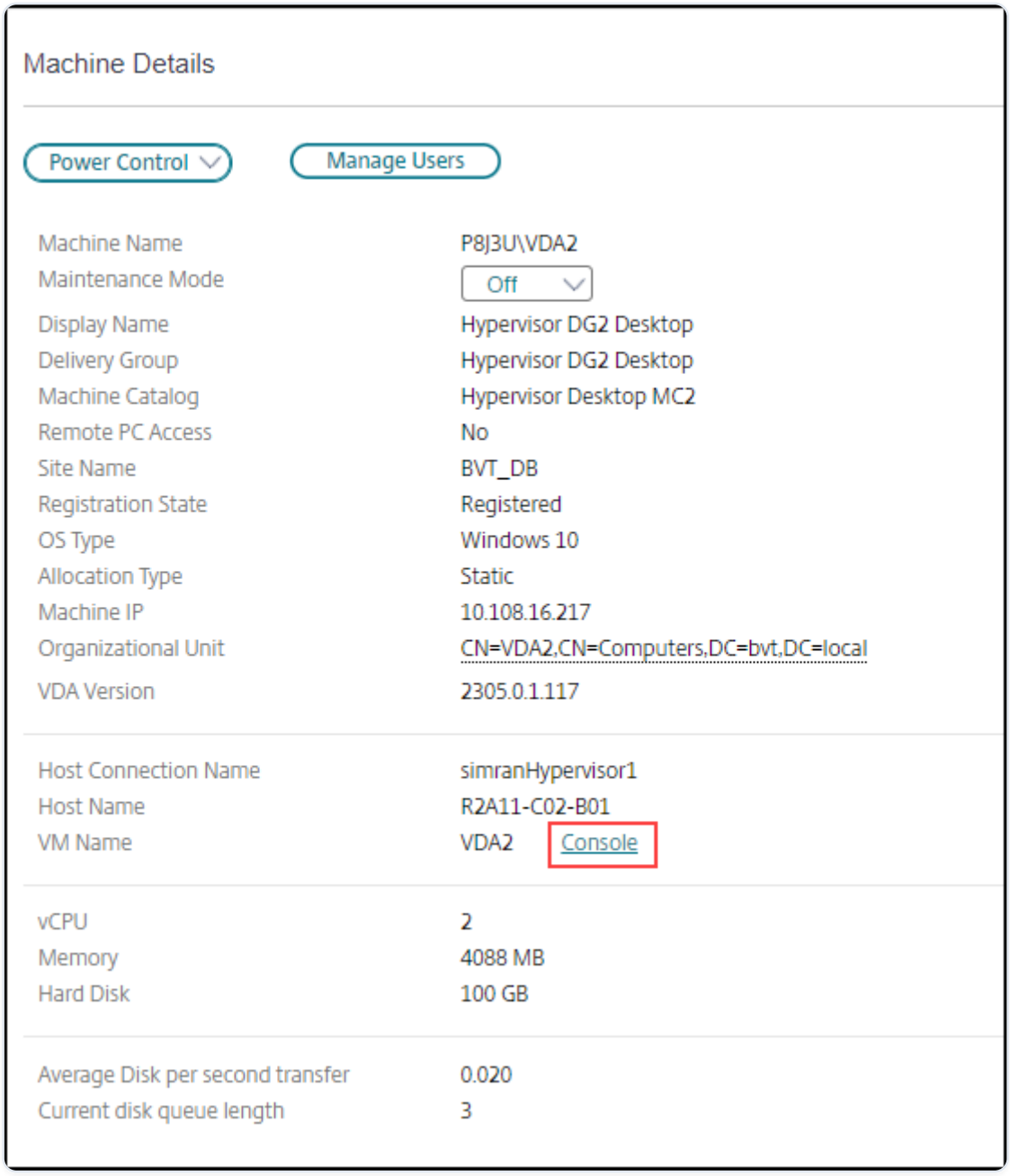
3. 特定のプロセスのリソース消費の履歴傾向を表示するには、上位10個のプロセスのいずれかをドリルダウンします。

マシンコンソールへのアクセス

XenServerバージョン7.3以降でホストされているシングルセッションおよびマルチセッションOSマシンのコンソールには、Directorから直接アクセスできます。これにより、XenServerでホストされているVDAの問題をトラブルシューティングするためにXenCenterは必要ありません。この機能を利用するには：

- バージョン7.16以降のDelivery Controllerが必要です。

- マシンをホストしているXenServerはバージョン7.3以降である必要があり、Director UIからアクセスできる必要があります。



マシンをトラブルシューティングするには、対応するマシン詳細パネルの リンクをクリックします。指定したホスト資格情報が認証されると、WebベースのVNCクライアントであるnoVNCを使用して、マシンのコンソールが別のタブで開きます。これで、コンソールにキーボードとマウスでアクセスできるようになります。

> **注:**
>
> - この機能はInternet Explorer 11ではサポートされていません。

- マシンコンソールのマウス ポインターがずれている場合は、問題を解決する手順についてCTX230727を参照してください。
- Directorは新しいタブでコンソールアクセスを起動します。ブラウザーの設定でポップアップが許可されていることを確認してください。
- セキュリティ上の理由から、Citrix®はブラウザーにSSL証明書をインストールすることをお勧めします。

最近の電源操作があるマシンを検査する

電源操作の成功および失敗のステータスを持つマシンを検査できるようになりました。この機能は、次の分析に役立ちます。

- ユーザーの問題を引き起こす電源オンの失敗
- コストを増加させる電源オフの失敗

注:

データは、電源管理されているマシンでのみ利用可能です。この機能がサポートされる前に行われた電源操作のデータは利用できません。

次の方法で、マシンの電源操作ステータスを表示できます。

-> タブから。この場合、デフォルトで 列と 列が表示されます。表示したい列を選択することもできます。

タブから。この場合、デフォルトのフィルターは が *Autoscale*™ に設定され、 が *失敗* に設定されています。

この機能を使用すると、電源操作コントロールの詳細を表示できます。たとえば、誰がアクションをトリガーしたか、どのアクションが電源状態を変更したか、失敗の理由、およびアクションが完了した時刻を表示できます。これらの詳細をエクスポートすることもできます。

電源操作のステータスを表示するために、以下のフィルターが追加されました。

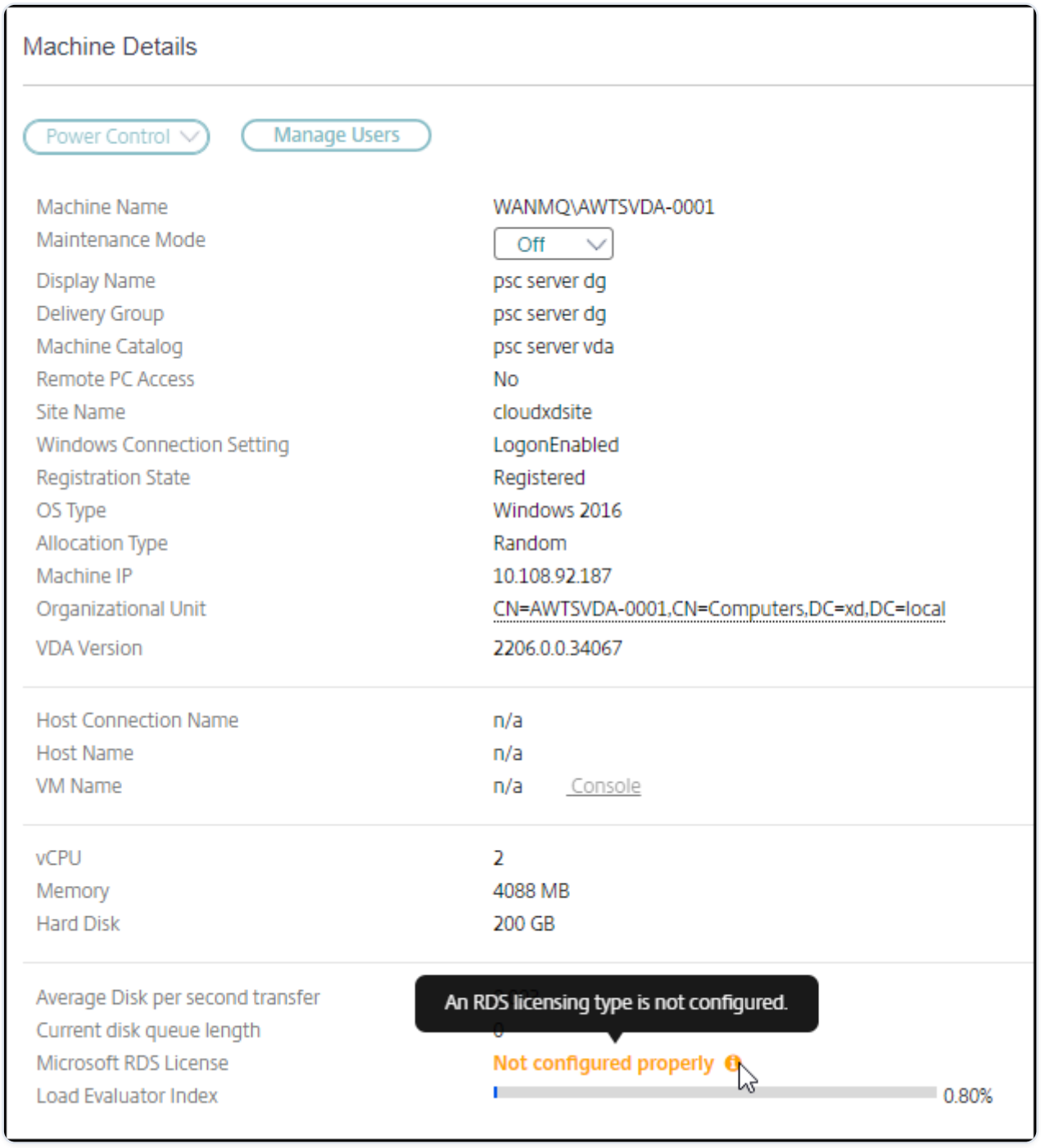
フィルター	説明
電源操作結果	電源操作の結果を表示します。可能なフィルター値は「成功」と「失敗」です。

フィルター	説明
電源操作のトリガー元	電源操作をトリガーしたユーザーまたは内容を表示します。可能なフィルター値は次のとおりです。 • オートスケール - この値は、電源操作が以下によってトリガーされた場合に表示されます。 • 管理者がVMのOSディスクを初期状態に戻すためにVMをシャットダウンした場合 • 設定されたポリシーに基づいてVMがシャットダウンまたは中断された場合 • プールサイズまたはバッファサイズの構成に基づいてVMが利用可能になった場合 • 管理者 - この値は、管理者が電源操作をトリガーしたときに表示されます。考えられる例としては、管理者がVMのシャットダウン、起動、一時停止、再開、再起動、またはリブートを要求した場合などがあります。 • ユーザー - この値は、ユーザーが電源操作をトリガーしたときに表示されます。例としては、ユーザーがVMをリセット、起動、または作業を再開した場合などがあります。

フィルター	説明
	• その他 - この値は、スケジュールされた理由または不明な理由によって電源操作がトリガーされたときに表示されます。
最終電源操作	マシンで発生した正確な電源操作（電源オン、電源オフ、シャットダウン、再起動、リセット、再開など）を表示します。
電源操作時刻	電源操作が完了した時刻。可能なフィルター値は、過去1分、過去5分、過去30分、過去1時間、今日、過去24時間、昨日です。
電源操作失敗理由	失敗の理由を表示します。可能なフィルター値は、ハイパーバイザー報告の失敗、ハイパーバイザーのレート制限超過、不明なエラー、なしです。操作が成功した場合は、「なし」と表示されます。

Microsoft RDSライセンスの健全性

マルチセッションOSマシンの**マシン詳細**ページと**ユーザー詳細**ページの**マシン詳細**パネルで、Microsoft RDSライセンスのステータスを表示できます。



次のいずれかのメッセージが表示されます:

- ライセンスが利用可能です
- 適切に構成されていません (警告)
- ライセンスエラー (エラー)
- 互換性のないVDAバージョン (エラー)

> **注:**

有効なライセンスを持つ猶予期間中のマシンでは、Microsoft RDSライセンスの状態が緑色で「**ライセンスが利用可能です**」というメッセージを表示します。ライセンスの有効期限が切れる前に更新してください。

警告メッセージおよびエラーメッセージについては、情報アイコンにカーソルを合わせると、次の表に示す追加情報を表示できます。

メッセージの種類	DIRECTOR内のメッセージ
エラー	VDAバージョン7.16以降で利用可能です。
エラー	新しいRDS接続は許可されていません。
エラー	Microsoft RDSライセンスの猶予期間が過ぎました。
エラー	必要なOSレベルに対して、デバイスごとのクライアントアクセスライセンスの種類でライセンスサーバーが構成されていません。
エラー	構成されているライセンスサーバーは、デバイスごとのクライアントアクセスライセンスの種類でRDSホストOSレベルと互換性がありません。
警告	パーソナルターミナルサーバーは、Citrix Virtual Apps and Desktops™展開では有効なRDSライセンスの種類ではありません。
警告	管理用リモートデスクトップは、Citrix Virtual Apps™ and Desktops展開では有効なライセンスの種類ではありません。
警告	RDSライセンスの種類が構成されていません。
警告	ユーザーごとのクライアントアクセスRDSライセンスの種類では、ドメインコントローラーまたはライセンスサーバーに到達できません。

メッセージの種類	DIRECTOR内のメッセージ
警告	「デバイスごとのクライアントアクセス」ライセンスの種類の場合、必要なOSレベルのライセンスサーバーに到達できないため、クライアントデバイスライセンスを特定できません。

注意：

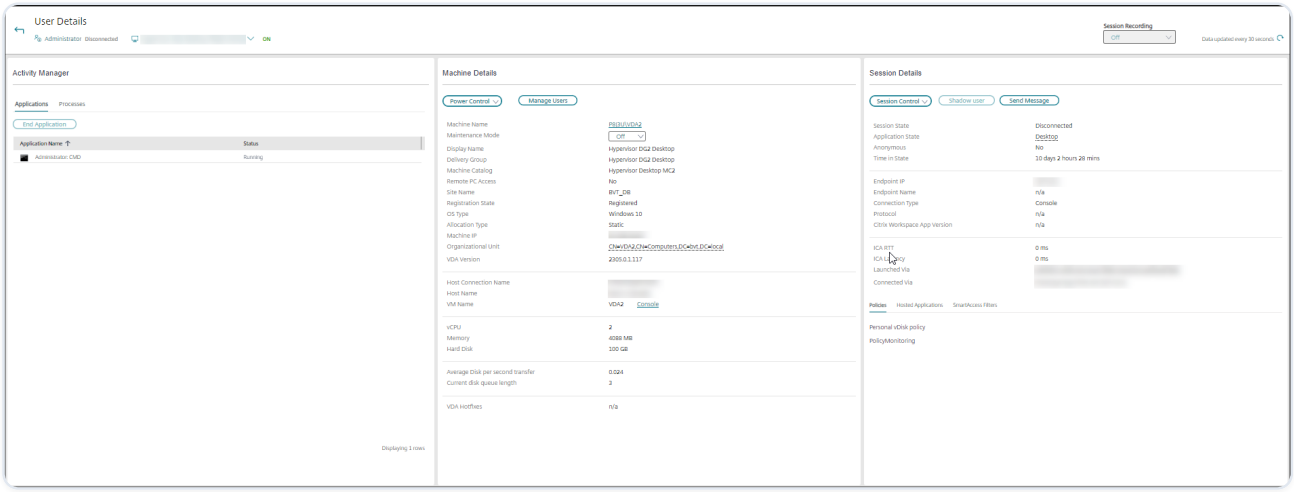
この機能は、Microsoft RDS CAL (クライアントアクセスライセンス) にのみ適用されます。

ユーザーの問題のトラブルシューティング

Directorの**ヘルプデスク**ビュー（**アクティビティマネージャー**ページ）を使用して、ユーザーまたはセッションに関する情報を表示します。

ユーザーの詳細(/en-us/citrix-virtual-apps-desktops/2511/media/dir-user-details-summary.png)

アクティビティマネージャーからユーザーに対して**詳細の表示**をクリックすると、**ユーザーの詳細**ページが開きます。 アクティビティマネージャーからエンドポイントに対して**詳細の表示**をクリックすると、**エンドポイントの詳細**ページが開きます。



セッションセレクター

ユーザーが複数のセッションを開始している場合、セッションセレクターはセッションの選択に役立ちます。

セッションセレクター(/en-us/citrix-virtual-apps-desktops/2511/media/dir-session-selector.png)

詳細を表示するセッションを選択します。

- セッション、ユーザーのサインインエクスペリエンス、セッションの起動、接続、およびアプリケーションに関する詳細を確認します。
- ユーザーのマシンをシャドウできます。
- ICA®セッションを記録します。

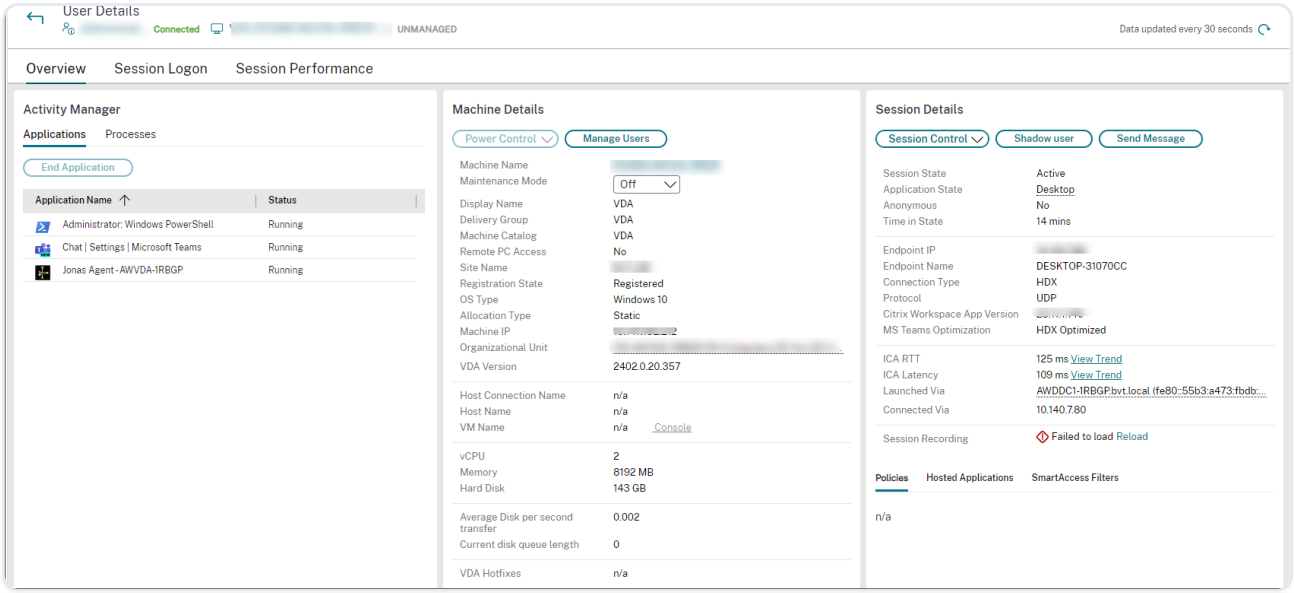
Microsoft Teamsの最適化ステータス

Directorは、**ユーザーの詳細**ページ > **セッションの詳細**パネル > **MS Teamsの最適化**フィールドに、HDX™セッションのMicrosoft Teamsの最適化ステータスを表示します。Microsoft Teamsが最適化されていることは、クリアなオーディオとビデオなど、より良いユーザーエクスペリエンスにとって重要です。Microsoft Teamsの最適化ステータスの可視性は、チケット解決にかかる時間を短縮し、管理者がトラブルシューティング中に重要なメトリックを特定するのに役立ちます。

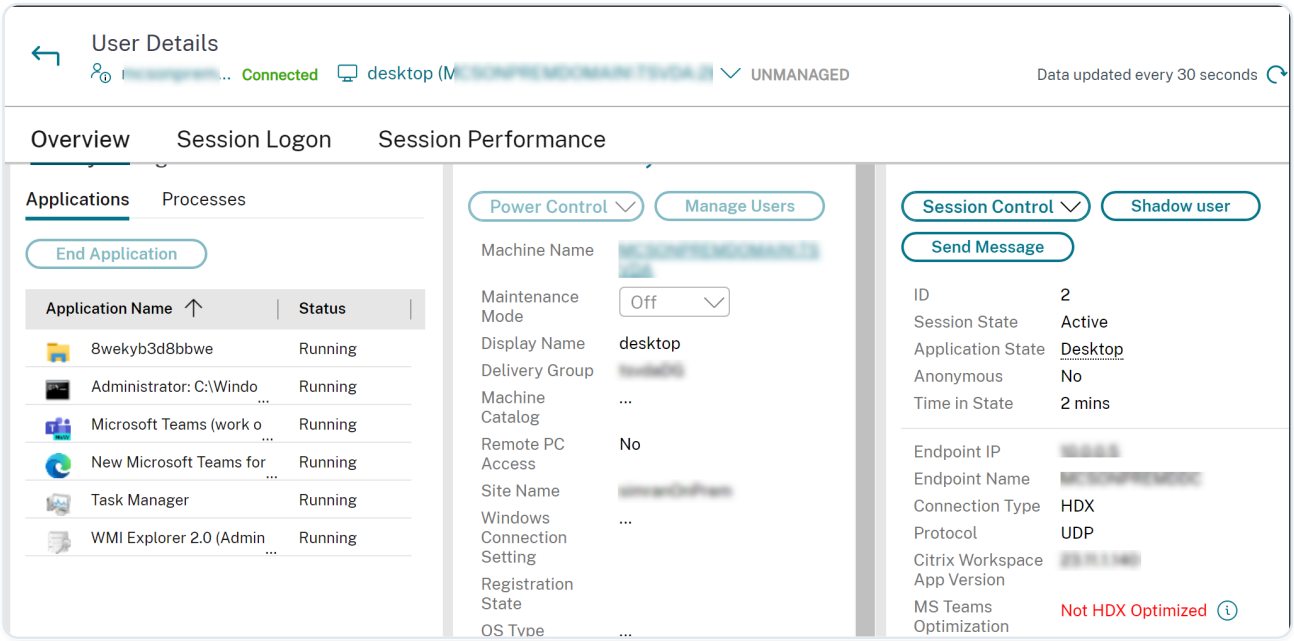
> **注：**
>
> Citrix Directorは、Microsoft Teamsバージョン2.1以前をサポートしています。

> 前提条件:

- VDA はバージョン 2311 以降を実行しています。
- サポートされている Citrix Workspace アプリのバージョンは、Microsoft Teams の最適化 に記載されています。
- Microsoft Teams は、公開アプリケーションとして、または公開デスクトップ内で実行されます。
- Citrix HDX HTML5 Video Redirection Service などの重要なサービスが実行されています。



Microsoft Teams が最適化されていない場合、ツールチップには、Microsoft Teams を最適化するためのヒントを含む HDX からの外部トラブルシューティングライブ記事へのリンクが表示されます。HDX 最適化のトラブルシューティング。



トラブルシューティングのヒント

次の表に記載されている推奨されるアクションで問題をトラブルシューティングし、必要に応じて適切な管理者に問題をエスカレートしてください。

ユーザーの問題	提案
ログオンに時間がかかる、または断続的または繰り返し失敗する	ユーザーログオンの問題を診断する

ユーザーの問題	提案
セッションの起動に時間がかかる、または断続的/繰り返し失敗する	セッション起動の問題を診断する
セッションの応答が遅い、または応答しない	セッションパフォーマンスの問題を診断する
アプリケーションの動作が遅い、または応答しない	アプリケーションの障害を解決する
接続に失敗しました	デスクトップ接続を復元する
セッションの動作が遅い、または応答しない	セッションを復元する
セッションを記録する	セッションを記録する
ビデオの動作が遅い、または品質が悪い	HDXチャネルシステムレポートを実行する

注:

マシンがメンテナンスモードでないことを確認するには、ユーザー詳細ビューからマシン詳細パネルを確認します。

セッションログオン

ユーザー詳細ビュー > **セッションログオン**タブには、セッションログオンプロセスの包括的なビューが表示されます。このタブには、合計ログオン時間、クライアントとコントローラーの時間、およびVDAの時間が表示されます。**セッションログオン**タブには、さまざまなログオンフェーズがプロットされたログオン時間フェーズチャートが含まれています。このデータを使用して、ユーザーログオンの問題をトラブルシューティングします。詳細については、「ユーザーログオンの問題の診断」を参照してください。

セッションパフォーマンス

セッションパフォーマンスタブには、ユーザーセッション内の問題を特定するためにリアルタイムメトリックを関連付ける機能から始まる、強化されたトラブルシューティングワークフローがあります。**セッショントポロジ**パネルは、接続されたHDXセッションのセッション内パスを視覚的に表現します。**パフォーマンスメトリック**パネルは、ICARTT、ICA待機時間、1秒あたりのフレーム数、利用可能な出力帯域幅、消費された出力帯域幅などのセッションメトリックの傾向を

提供し、これらのメトリックが時間の経過とともにどのようにパフォーマンスしたかを示します。詳細については、「セッションパフォーマンスの問題の診断」を参照してください。

検索のヒント

検索フィールドにユーザー名を入力すると、Director は Director をサポートするように構成されているすべてのサイトのユーザーについて、Active Directory でユーザーを検索します。

検索フィールドにマルチユーザーマシンの名前を入力すると、Director は指定されたマシンのマシン詳細を表示します。

検索フィールドにエンドポイント名を入力すると、Director は特定のEndpointに接続されている認証されていない（匿名）セッションと認証済みセッションを使用します。この検索により、認証されていないセッションのトラブルシューティングが可能になります。認証されていないセッションのトラブルシューティングを可能にするには、エンドポイント名が一意であることを確認してください。

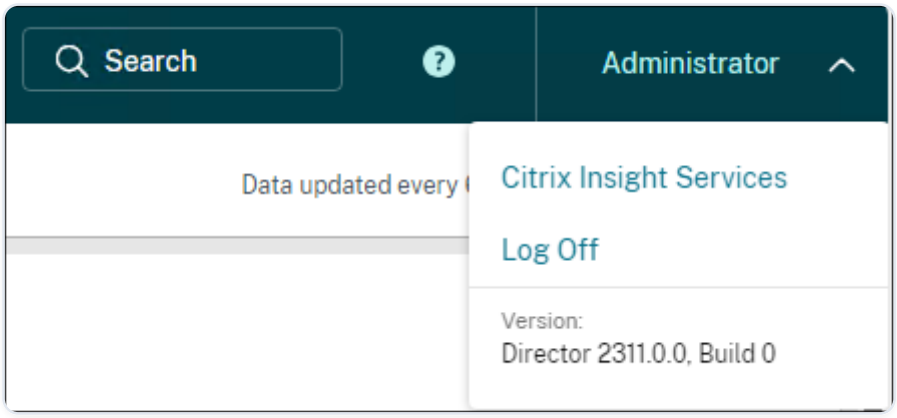
検索結果には、現在マシンを使用していない、またはマシンに割り当てられていないユーザーも含まれます。

- 検索では大文字と小文字は区別されません。
- 部分的な入力では、一致する可能性のあるリストが生成されます。
- スペースで区切られた2つの部分からなる名前の数文字を入力すると、結果には両方の文字列の一致が含まれます。2つの部分からなる名前の例としては、ユーザー名、姓と名、または表示名があります。たとえば、「jo rob」と入力すると、結果には「John Robertson」や「Robert Jones」などの文字列が含まれる場合があります。

ランディングページに戻るには、**Director ロゴ**をクリックします。

Citrix Insight Servicesへのアクセス

Directorの**ユーザー**ドロップダウンリストからCitrix Insight Services (CIS) にアクセスして、追加の診断情報を取得できます。CISで利用可能なデータは、Call HomeやCitrix Scoutなどのソースから提供されます。



トラブルシューティング情報をCitrixテクニカルサポートにアップロードする

単一のDelivery Controller™またはVDAからCitrix Scoutを実行し、主要なデータポイントとCitrix Diagnostics Facility (CDF) トレースをキャプチャして、選択したコンピューターのトラブルシューティングを行います。Scoutは、データをCISプラットフォームに安全にアップロードする機能を提供し、Citrixテクニカルサポートのトラブルシューティングを支援します。Citrixテクニカルサポートは、CISプラットフォームを使用して、顧客から報告された問題の解決にかかる時間を短縮します。

Scoutは、Citrix Virtual Apps and Desktops™コンポーネントとともにインストールされます。Windowsのバージョンに応じて、Citrix Virtual Apps and Desktopsをインストールまたはアップグレードすると、Scoutは**Windowsのスタート**メニューまたはスタート画面に表示されます。

Scoutを起動するには、スタートメニューまたはスタート画面から **\>** を選択します。

Scoutの使用方法と構成、およびFAQについては、CTX130147を参照してください。

セッション起動の問題を診断する

ユーザーログオンの問題の診断セクションで述べられているログオンプロセスフェーズに加えて、Directorはセッション起動時間を表示します。これは、**ユーザー詳細**ページと**マシン詳細**ページで、Workspace Appセッション起動時間とVDAセッション起動時間に分けられます。これらの2つの期間は、さらに個々のフェーズを含み、その起動時間も表示されます。このデータは、セッション起動時間の長さの理解とトラブルシューティングに役立ちます。さらに、セッション起動に関わる各フェーズの所要時間は、個々のフェーズに関連する問題のトラブルシューティングに役立ちます。たとえば、ドライブマッピング時間が長い場合、GPOまたはスクリプトですべての有効なドライブが正しくマッピングされているかを確認できます。この機能は、Delivery Controllerバージョン7 1906以降およびVDA 1903以降で利用可能です。

前提条件

セッション起動時間データが表示されるように、以下の前提条件が満たされていることを確認してください。

- Delivery Controller™ のバージョン 7 1906 以降。
- VDA 1903以降。
- Citrix End User Experience Monitoring (EUEM)サービスがVDA上で実行されている必要があります。

制限事項

Directorがセッション起動時間データを表示する場合、以下の制限事項が適用されます。

- セッション起動時間はHDX™セッションでのみ利用可能です。
- iOSおよびAndroid OSからのセッション起動の場合、VDA起動時間のみ利用可能です。
- ICA®ファイルダウンロード時間 (IFDCD) は、ブラウザから起動する際にWorkspace Appが検出された場合にのみ利用可能です。
- Mac OSからのセッション起動の場合、IFDCDはWorkspace App 1902以降でのみ利用可能です。
- Windows OSからのセッション起動の場合、IFDCDはWorkspace app 1902以降で利用可能です。それ以前のバージョンでは、IFDCDはWorkspace appが検出されたブラウザからのアプリ起動の場合にのみ表示されます。

> **注記:**
>
> - 前提条件が満たされた後もセッション起動時間の表示に問題がある場合は、CTX130320に記載されているDirectorサーバーおよびVDAログを確認してください。 共有セッション（同じセッションで複数のアプリケーションが起動された場合）の場合、Workspace Appの起動メトリックは、最新の接続または最新のアプリケーション起動に対して表示されます。
> - VDAセッション起動の一部のメトリックは、再接続時には適用されません。そのような場合、メッセージが表示されます。

セッション起動(/en-us/citrix-virtual-apps-desktops/2511/media/session_startup.png)

Workspace App セッション起動フェーズ

セッション起動クライアント期間 (SSCD)

このメトリックが高い場合、起動時間が長くなる原因となっているクライアント側の問題を示しています。問題の根本原因を特定するために、後続のメトリックを確認してください。SSCDは、

要求（マウスクリック）の時刻にできるだけ近い時点から開始されます。クライアントデバイスとVDA間のICA接続が確立されたときに終了します。共有セッションの場合、サーバーへの新しい接続の作成に関連するセットアップコストの多くが発生しないため、この期間ははるかに短くなります。次のレベルでは、いくつかの詳細なメトリックが利用可能です。

ICA ファイルダウンロード期間

これは、クライアントがサーバーからICAファイルをダウンロードするのにかかる時間です。全体的なプロセスは次のとおりです。

1. ユーザーはWorkspaceアプリケーションでリソース（アプリケーションまたはデスクトップ）をクリックします。
2. ユーザーからの要求は、Citrix Gateway（構成されている場合）を介してStoreFront™に送信され、StoreFront™は要求をDelivery Controllerに送信します。
3. Delivery Controllerは要求に利用可能なマシンを見つけ、マシン情報とその他の詳細をStoreFrontに送信します。また、StoreFrontはSecure Ticket Authorityからワンタイムチケットを要求し、受け取ります。
4. StoreFrontはICAファイルを生成し、Citrix Gateway（構成されている場合）を介してユーザーに送信します。

IFDCDは、完全なプロセス（ステップ1〜4）にかかる時間を表します。IFDCDのカウントは、クライアントがICAファイルを受信したときに停止します。

LPWD は、プロセスの StoreFront コンポーネントです。

IFDCD が高い (ただし LPWD が正常である) 場合、起動のサーバー側処理は成功しましたが、クライアントデバイスと StoreFront の間に通信の問題がありました。これは、2つのマシン間のネットワークの問題に起因します。したがって、まず潜在的なネットワークの問題をトラブルシューティングできます。

起動ページ WEB サーバー期間 (LPWD)

これは、StoreFrontで起動ページ (launch.aspx) を処理するのにかかった時間です。LPWDが高い場合、StoreFrontでボトルネックが発生している可能性があります。

考えられる原因は次のとおりです。

- StoreFrontの負荷が高い。Internet Information Services (IIS) ログ、監視ツール、タスクマネージャー、パフォーマンスモニターなどを確認して、速度低下の原因を特定してください。
- StoreFrontがDelivery Controllerなどの他のコンポーネントとの通信に問題がある。StoreFrontとDelivery Controller間のネットワーク接続が遅いか、一部のDelivery Controllerがダウンしているか、過負荷状態になっていないかを確認してください。

名前解決WEBサーバー期間 (NRWD)

これは、Delivery Controllerが公開アプリケーション/デスクトップの名前をVDAマシンのIPアドレスに解決するのにかかる時間です。

このメトリックが高い場合、Delivery Controllerが公開アプリケーションの名前をIPアドレスに解決するのに時間がかかっていることを示します。

可能性のある原因としては、クライアント側の問題、Delivery Controllerの過負荷などのDelivery Controllerの問題、またはそれらの間のネットワークリンクの問題が挙げられます。

チケット応答WEBサーバー期間 (TRWD)

この期間は、Secure Ticket Authority (STA) サーバーまたはDelivery Controllerからチケットを取得するのにかかる時間を示します（必要な場合）。この期間が高い場合、STAサーバーまたはDelivery Controllerが過負荷状態であることを示します。

セッション検索クライアント期間 (SLCD)

この期間は、要求された公開アプリケーションをホストするためにすべてのセッションを照会するのにかかる時間を示します。既存のセッションがアプリケーション起動要求を処理できるかどうかを判断するために、クライアントでチェックが実行されます。使用される方法は、セッションが新規か共有かによって異なります。

セッション作成クライアント期間 (SCCD)

この期間は、wfica32.exe（または同様の同等ファイル）が起動されてから接続が確立されるまでの、セッション作成にかかる時間を示します。

VDAセッション起動フェーズ

セッション起動VDA期間 (SSVD)

この期間は、VDAが起動操作全体を実行するのにかかる時間を含む、高レベルのサーバー側接続起動メトリックです。このメトリックが高い場合、セッション起動時間を増加させるVDAの問題があることを示します。これには、VDAが起動操作全体を実行するのに費やされた時間が含まれます。

資格情報取得VDA期間 (COVD)

VDAがユーザー資格情報を取得するのにかかる時間。

ユーザーがタイムリーに資格情報を提供できない場合、この期間は人為的に増加する可能性があります。そのため、VDA起動期間には含まれません。この時間は、手動ログインが使用され、サーバー側の資格情報ダイアログが表示される場合（またはログイン開始前に法的通知が表示される場合）にのみ重要となる可能性があります。

資格情報認証VDA期間 (CAVD)

これは、VDAが認証プロバイダーに対してユーザーの資格情報を認証するのにかかる時間です。認証プロバイダーは、Kerberos、Active Directory、またはセキュリティサポートプロバイダーインターフェース (SSPI) のいずれかです。

グループポリシーVDA期間 (GPVD)

この期間は、ログオン中にグループポリシーオブジェクトを適用するのにかかる時間です。

ログオンスクリプト実行VDA期間 (LSVD)

これは、VDAがユーザーのログオンスクリプトを実行するのにかかる時間です。

ユーザーまたはグループのログオンスクリプトを非同期にすることを検討してください。アプリケーション互換性スクリプトを最適化するか、代わりに環境変数を使用することを検討してください。

プロファイルロードVDA期間 (PLVD)

これは、VDAがユーザープロファイルをロードするのにかかる時間です。

この期間が長い場合は、ユーザープロファイル構成を検討してください。ローミングプロファイルのサイズと場所は、セッションの起動が遅くなる原因となります。ユーザーがターミナルサービスローミングプロファイルとホームフォルダーが有効になっているセッションにログオンすると、ローミングプロファイルの内容と当該フォルダーへのアクセスがログオン中にマッピングされます。これには追加のリソースが必要です。場合によっては、CPU使用率を大幅に消費することがあります。この問題を軽減するために、リダイレクトされた個人フォルダーとともに**ターミナルサービスホーム**フォルダーを使用することを検討してください。一般に、Citrix環境でユーザープロファイルを管理するには、Citrix Profile Managementの使用を検討してください。Citrix Profile Managementを使用しており、ログオン時間が遅い場合は、アンチウイルスソフトウェアがCitrix Profile Managementツールをブロックしていないか確認してください。

プリンター作成VDA期間 (PCVD)

これは、VDAがユーザーのクライアントプリンターを同期的にマッピングするのにかかる時間です。プリンター作成が非同期で実行されるように構成されている場合、セッション起動の完了に影響しないため、PCVDの値は記録されません。

プリンターのマッピングに過剰な時間が費やされるのは、多くの場合、プリンターの自動作成ポリシー設定が原因です。ユーザーのクライアントデバイスにローカルで追加されたプリンターの数と、印刷構成がセッションの開始時間に直接影響を与える可能性があります。セッションが開始されると、Citrix Virtual Apps and Desktops™ は、クライアントデバイス上のローカルにマップされたすべてのプリンターを作成する必要があります。特にユーザーが多数のローカルプリンターを持っている場合は、作成されるプリンターの数を減らすために、印刷ポリシーを再構成すること

を検討してください。これを行うには、Delivery Controller および Citrix Virtual Apps and Desktops でプリンターの自動作成ポリシーを編集します。

ドライブマッピングVDA期間 (DMVD)

これは、VDAがユーザーのクライアントドライブ、デバイス、ポートをマッピングするのにかかる時間です。

ベースポリシーに、未使用の仮想チャネルを無効にする設定が含まれていることを確認してください。たとえば、オーディオやCOMポートのマッピングを無効にすることで、ICAプロトコルを最適化し、セッション全体のパフォーマンスを向上させることができます。

アプリケーション/デスクトップ起動VDA期間 (ALVD/DLVD)

このフェーズは、UserinitとShellの期間の組み合わせです。ユーザーがWindowsマシンにログオンすると、winlogonがuserinit.exeを実行します。Userinit.exeはログオンスクリプトを実行し、ネットワーク接続を再確立してからExplorer.exeを起動します。Userinitは、userinit.exeの開始から仮想デスクトップまたはアプリケーションのユーザーインターフェイスの開始までの期間を表します。Shell期間は、ユーザーインターフェイスの初期化からユーザーがキーボードとマウスの制御を受け取るまでの時間です。

セッション作成VDA期間 (SCVD)

この時間には、VDAでのセッション作成時間におけるその他の遅延が含まれます。

ユーザーログオンの問題を診断する

ユーザー詳細ビュー > **セッションログオン**タブには、セッションログオンプロセスの包括的なビューが表示されます。このタブには、合計ログオン時間、クライアントとコントローラーの時間、およびVDAの時間が表示されます。このデータを使用して、ユーザーログオンの問題をトラブルシューティングします。

ログオン時間は、HDXを使用してデスクトップまたはアプリに初回接続する場合にのみ測定されます。このデータには、リモートデスクトッププロトコルで接続しようとしているユーザーや、切断されたセッションから再接続しているユーザーは含まれません。具体的には、ユーザーが最初に非HDXプロトコルを使用して接続し、HDXを使用して再接続する場合、ログオン時間は測定されません。

ユーザーがCitrix Virtual Apps and Desktops™にログオンすると、Monitor Serviceはログオンプロセスのフェーズを追跡します。フェーズは、ユーザーがCitrix Workspace™アプリから接続した時点から、アプリまたはデスクトップが使用可能になるまでの時間で始まります。

セッションログオンタブには、さまざまなログオンフェーズがプロットされたログオン時間フェーズチャートが含まれています。ログオン時間は、Delivery Controller™から接続を確立して

アプリまたはデスクトップを取得するのに費やされた時間と、仮想アプリまたはデスクトップに認証してログオンするのに費やされた時間を表します。時間の情報は秒（または秒の端数）で表示されます。

ログオン時間 - GPOドリルダウン(/en-us/citrix-virtual-apps-desktops/2511/media/dir-logon-duration.png)

ログオン時間フェーズチャートは、さまざまなログオンフェーズとその開始時刻および終了時刻を明確に示します。このチャートは、個々のログオンフェーズの重複を示しています。合計ログオン時間は、個々のログオンフェーズの合計時間ではない場合があります。これは、個々のフェーズが重複する可能性があり、すべてのログオンフェーズがこの表現の一部ではないためです。また、特定のフェーズは、ユーザーが仮想アプリまたはデスクトップとの対話を開始した後も延長される可能性があり、この期間は全体のログオン時間の一部として測定されません。

このビューを使用して、セッション起動の遅延を引き起こしている特定のログオンフェーズを特定します。各ログオンフェーズの定義と、情報を追跡できるイベントソースは、さらなるトラブルシューティングに役立ちます。チャートにカーソルを合わせると、現在のセッションのフェーズ期間、ユーザーの7日間平均、およびデリバリーグループの7日間平均を含むツールチップが表示されます。この情報は、現在のセッションログオン期間を7日間平均値と比較するのに役立ちます。GPOおよびプロファイル詳細の場合、サブフェーズの測定値にさらにドリルダウンできます。この視覚化は、ログオン時間に関連する問題を簡単に理解し、トラブルシューティングするのに役立ちます。

前提条件

ログオン時間のデータとドリルダウンが表示されるように、以下の前提条件が満たされていることを確認してください。

1. VDAに**Citrix User Profile Manager**と**Citrix User Profile Manager WMI Plugin**をインストールします。
2. Citrix Profile Management Serviceが実行されていることを確認します。
3. XenAppおよびXenDesktopサイト7.15以前の場合、GPO設定**レガシー実行リストを処理しない**を無効にします。
4. 対話型セッションのドリルダウンには、監査プロセス追跡を有効にする必要があります。
5. GPOドリルダウンの場合、グループポリシーの運用ログのサイズを増やします。

> **注:**

- ログオン時間は、デフォルトのWindowsシェル (explorer.exe) でのみサポートされ、カスタムシェルではサポートされません。
- Remote PC Accessのログオン時間は、Remote PC Accessのインストール中に**Citrix User Profile Manager**と**Citrix User Profile Manager WMI Plugin**が追加コンポーネントとしてインストールされている場合にのみ利用可能です。詳細については、「Remote PC Accessの構成とシーケンスに関する考慮事項」のステップ4を参照してください。

ユーザーログオンの問題をトラブルシューティングする手順

1. 「**ユーザー詳細**」ビュー > 「**セッションログオン**」タブから、ログオン時間チャートを使用してログオン状態をトラブルシューティングします。
   - ユーザーがログオン中の場合、ビューにはログオンのプロセスが反映されます。
   - ユーザーがログオンしている場合、ログオン期間パネルには、ユーザーが現在のセッションにログオンするのにかかった時間が表示されます。
2. ログオンプロセスのフェーズを調べます。

ログオンプロセスのフェーズ

クライアントとコントローラーの時間
ユーザーがアプリまたはデスクトップアイコンをクリックしてから、セッションを操作するためのキーボードとマウスの制御がエンドユーザーに引き渡されるまでにかかった時間。
ブローカリング
ユーザーに割り当てるデスクトップを決定するのにかかった時間。
マシンの起動
セッションでマシンの起動が必要な場合、これは仮想マシンを起動するのにかかった時間です。以下のサブセクションでは、異なるフェーズで仮想マシンを起動するのにかかった時間の内訳を示します。

- **電源投入** - 仮想マシンの電源投入にかかった時間を表示します
- **起動と登録** - 仮想マシンの起動と登録にかかった時間を表示します

マシンの起動の下にあるオプションを折りたたんだり展開したりするには、折りたたみボタンを使用します。
HDX接続
クライアントから仮想マシンへのHDX接続をセットアップする際に必要な手順を完了するのにかかった時間。

VDAの時間

セッションを作成するためにVDA上でかかった時間。
認証
リモートセッションへの認証を完了するのにかかった時間。
プロファイル読み込み
ユーザーまたは仮想マシンにプロファイル設定が構成されている場合、これはプロファイルの読み込みにかかる時間です。

Citrix Profile ManagementとFSLogixが構成されている場合、プロファイルロードバーには、Citrix Profile ManagementとFSLogixがユーザープロファイルを処理するのにかかった時間が含まれます。この情報は、管理者が高いプロファイル処理時間の問題をトラブルシューティングするのに役立ちます。Profile ManagementとFSLogixが構成されている場合、プロファイルロードバーは増加した時間を表示します。この増加はこの機能強化によって引き起こされるものであり、パフォーマンスの低下を反映するものではありません。この機能強化は、VDAバージョン2407以降で利用可能です。

プロファイルロードバーにカーソルを合わせると、現在のセッションのユーザープロファイルの詳細を示すツールチップが表示されます。

プロファイルのドリルダウン(/en-us/citrix-virtual-apps-desktops/2511/media/profile_drilldown_1.png)

詳細をクリックして、プロファイルルートフォルダー内の各個別のフォルダー（例: C:/Users/username）、そのサイズ、およびファイル数（ネストされたフォルダー内のファイルを含む）にさらにドリルダウンします。

詳細なドリルダウン(/en-us/citrix-virtual-apps-desktops/2511/media/profile_drilldown_2.png)

プロファイルドリルダウンは、Delivery Controllerバージョン7 1811以降およびVDA 1811以降で利用できます。プロファイルドリルダウン情報を使用すると、プロファイルの読み込み時間が長いことに関する問題を解決できます。次のことができます。

- ユーザープロファイルをリセットする
- 不要な大きなファイルを削除してプロファイルを最適化する
- ネットワーク負荷を軽減するためにファイル数を減らす
- プロファイルストリーミングを使用する

デフォルトでは、プロファイルルート内のすべてのフォルダーがドリルダウンに表示されます。フォルダーの表示を非表示にするには、VDAマシンで次のレジストリ値を編集します。

警告:

レジストリを誤って追加および編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決されることを保証しません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

1. VDAで、HKEY_LOCAL_MACHINE\Software\Citrix\Director\に新しいレジストリ値 **ProfileFoldersNameHidden** を追加します。
2. 値を1に設定します。この値はDWORD (32ビット) 値である必要があります。フォルダー名の表示が無効になります。
3. フォルダー名を再度表示するには、値を0に設定します。

注:

GPOまたはPowerShellコマンドを使用して、複数のマシンにレジストリ値の変更を適用できます。GPOを使用してレジストリの変更を展開する方法の詳細については、ブログを参照してください。

追加情報

- プロファイルドリルダウンは、リダイレクトされたフォルダーを考慮しません。
- ルートフォルダー内のNTUser.datファイルは、エンドユーザーには表示されない場合があります。ただし、それらはプロファイルドリルダウンに含まれ、**ルートフォルダー**のファイルリストに表示されます。
- AppDataフォルダー内の一部の隠しファイルは、プロファイルドリルダウンには含まれません。
- 特定のWindowsの制限により、ファイル数とプロファイルサイズデータがパーソナライズパネルのデータと一致しない場合があります。

インタラクティブセッション

インタラクティブセッションとは、ユーザープロファイルがロードされた後、キーボードとマウスの制御をユーザーに「引き渡す」のにかかる時間です。これは通常、ログオンプロセスのすべてのフェーズの中で最も長い期間であり、**インタラクティブセッションの期間 = デスクトップ準備完了イベントのタイムスタンプ (VDA上のEventId 1000) - ユーザープロファイルロード完了イベ**

ントのタイムスタンプ (VDA上のEventId 2) として計算されます。インタラクティブセッションには、Pre-userinit、Userinit、Shellの3つのサブフェーズがあります。インタラクティブセッションにカーソルを合わせると、次の情報を示すツールヒントが表示されます。

- サブフェーズ
- 各サブフェーズにかかった時間
- これらのサブフェーズ間の合計累積時間遅延

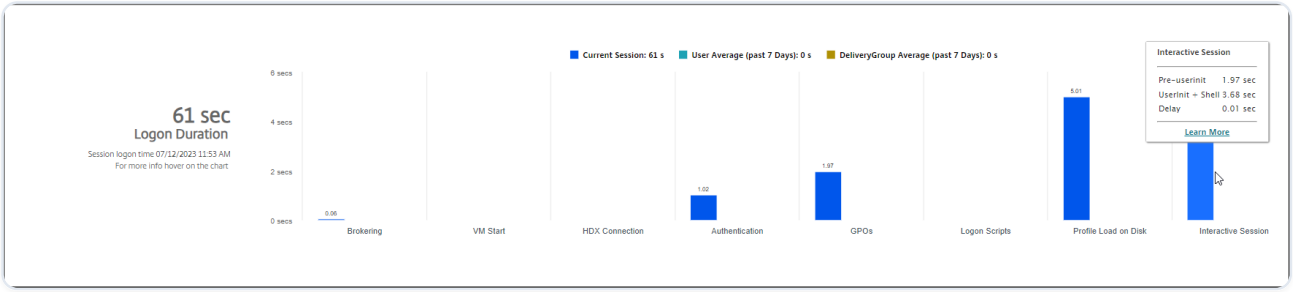
折りたたみボタンを使用して、**インタラクティブセッション**の下のオプションを折りたたんだり展開したりできます。

> **注:**
>
> この機能は、VDA 1811以降で利用できます。7.18より前のサイトでセッションを起動し、その後7.18以降にアップグレードした場合、「サーバーエラーのためドリルダウンを利用できません」というメッセージが表示されます。ただし、アップグレード後にセッションを起動した場合は、エラーメッセージは表示されません。

> 各サブフェーズの期間を表示するには、VM (VDA) で監査プロセス追跡を有効にします。監査プロセス追跡が無効になっている場合 (デフォルト)、Pre-userinitの期間と、UserinitおよびShellの合計期間が表示されます。グループポリシーオブジェクト (GPO) を使用して、次のように監査プロセス追跡を有効にできます。

1. GPOを作成し、GPOエディターを使用して編集します。
2. **コンピューターの構成 > Windows の設定 > セキュリティの設定 > ローカル ポリシー > 監査ポリシー**に移動します。
3. 右側のペインで、**監査プロセス追跡**をダブルクリックします。
4. **成功**を選択し、OKをクリックします。
5. このGPOを必要なVDAまたはグループに適用します。

監査プロセス追跡とその有効化または無効化の詳細については、Microsoftのドキュメントの監査プロセス追跡を参照してください。



ユーザー詳細ビューのログオン期間パネル。

- **対話型セッション – Pre-userinit:** グループポリシーオブジェクトとスクリプトと重複する対話型セッションのセグメントです。このサブフェーズは、GPOとスクリプトを最適化することで短縮できます。
- **対話型セッション – Userinit:** ユーザーがWindowsマシンにログオンすると、Winlogonはuserinit.exeを実行します。Userinit.exeはログオンスクリプトを実行し、ネットワーク接続を再確立してから、WindowsユーザーインターフェイスであるExplorer.exeを起動します。対話型セッションのこのサブフェーズは、Userinit.exeの開始から仮想デスクトップまたはアプリケーションのユーザーインターフェイスの開始までの期間を表します。
- **対話型セッション – シェル:** 前のフェーズでは、UserinitがWindowsユーザーインターフェイスの初期化を開始します。シェルサブフェーズは、ユーザーインターフェイスの初期化からユーザーがキーボードとマウスの制御を受け取るまでの期間を捕捉します。
- **遅延:** これは、**Pre-userinitとUserinit**サブフェーズと**Userinitとシェル**サブフェーズ間の累積時間遅延です。

合計ログオン時間は、これらのフェーズの正確な合計ではありません。たとえば、一部のフェーズは並行して発生し、一部のフェーズでは、合計よりも長いログオン期間になる可能性のあるより多くの処理が発生します。 合計ログオン時間には、ICAファイルのダウンロードとアプリケーションのICAファイルの起動の間の時間であるICA®アイドル時間は含まれません。 アプリケーション起動時にICAファイルを自動的に開くには、ICAファイルのダウンロード時にICAファイルを自動的に起動するようにブラウザーを設定します。詳細については、CTX804493を参照してください。

> **注:**
>
> ログオン期間グラフは、ログオンフェーズを秒単位で表示します。1秒未満の期間値は、サブ秒値として表示されます。1秒を超える値は、最も近い0.5秒に丸められます。グラフは、Y軸の最大値が200秒になるように設計されています。200秒を超える値は、バーの上に実際の値が表示されます。

ログオンスクリプト
セッションにログオンスクリプトが構成されている場合、これはログオンスクリプトの実行にかかる時間です。
GPO
仮想マシンでグループポリシー設定が有効になっている場合、これはログオン中にグループポリシーオブジェクトを適用するのにかかる時間です。CSE（クライアント側拡張）ごとの各ポリシーの適用にかかる時間のドリルダウンは、GPOバーにカーソルを合わせるとツールチップとして表示されます。



詳細をクリックすると、ポリシーのステータスと対応するGPO名が記載されたテーブルが表示されます。ドリルダウンの時間間隔はCSEの処理時間のみを表し、GPOの合計時間には加算されません。ドリルダウンテーブルは、さらなるトラブルシューティングやレポートでの使用のためにコピーできます。ポリシーのGPO時間は、イベントビューアーのログから取得されます。ログは、運用ログに割り当てられたメモリ（デフォルトサイズは4 MB）に応じて上書きされる可能性があります。運用ログのログサイズを増やす方法の詳細については、Microsoft TechNetの記事イベントログの構成を参照してください。
ユーザー初期化
ユーザーがWindowsマシンにログオンすると、Winlogonはuserinit.exeを実行します。Userinit.exeはログオンスクリプトを実行し、ネットワーク接続を再確立してから、Windowsユーザーインターフェイスであるexplorer.exeを起動します。インタラクティブセッションのこのサブフェーズは、Userinit.exeの開始から仮想デスクトップまたはアプリケーションのユーザーインターフェイスの開始までの期間を表します

シェル

シェルサブフェーズは、ユーザーインターフェイスの初期化からユーザーがキーボードとマウスの制御を受け取るまでの期間を捕捉します。
AppXファイルの関連付け
新しいVDAセッション中にAppXファイルを関連付けるのにかかった時間。

AppXパッケージの読み込み
新しいVDAセッション中にAppXパッケージを読み込むのにかかった時間。

> **注:**
>
> 新しいVDAセッション中のAppXパッケージの読み込み時間を収集するには、uberAgentをDirectorと統合する必要があります。詳細については、「Citrix uberAgentとDirectorの統合」を参照してください。

データのエクスポート

デフォルトのログオン時間フェーズテーブルオプション（セッションログオンフェーズと期間）に加えて、セッションログオンページで次の列を選択することもできます。

- 開始時刻
- 終了時刻
- デリバリーグループ - 7日間平均 (秒)
- ユーザー - 7日間平均 (秒)

以前のデータを.CSVファイルにエクスポートすることもできます。

トラブルシューティングのヒント

グラフ内の異常な値や予期しない値を特定するには、現在のセッションの各フェーズにかかった時間と、このユーザーの過去7日間の平均所要時間、およびこのデリバリーグループのすべてのユーザーの過去7日間の平均所要時間を比較します。

必要に応じてエスカレートします。たとえば、**マシンの起動**が遅い場合、問題はハイパーバイザーにある可能性があるため、ハイパーバイザー管理者にエスカレートできます。

以下を含む異常な相違点を調べます。

- 欠落している（現在の）ログオンバー
- 現在の所要時間とこのユーザーの平均所要時間の間に大きな相違がある。原因は次のとおりです。
  - 新しいアプリケーションがインストールされた。
  - オペレーティングシステムのアップデートが行われた。
  - 構成変更が行われた。

    - ユーザーのプロファイルサイズが大きい。この場合、プロファイルロードが高くなります。

- ユーザーのログオン数（現在および平均所要時間）とデリバリーグループの平均所要時間の間に大きな相違がある。

必要に応じて、「**再起動**」をクリックしてユーザーのログオンプロセスを監視し、「**マシンの起動**」や「**ブローカリング**」などの問題をトラブルシューティングします。

セッションパフォーマンスの問題を診断する

ユーザー詳細ページの**セッションパフォーマンス**タブには、HDX™ユーザーセッション内の問題を特定するのに役立つ強化されたトラブルシューティングワークフローがあります。**セッションのトポロジとパフォーマンスメトリック**パネルは、セッションのコンポーネントビューと複数のパフォーマンスメトリックを単一のビューで関連付け、セッションエクスペリエンスの問題解決にかかる平均時間を短縮するのに役立ちます。

セッションパフォーマンスビュー(/en-us/citrix-virtual-apps-desktops/2511/media/dir-session-performance.png)

エンドツーエンドのネットワークホップビュー

エンドツーエンドのネットワークホップビューは、完全なセッションパスを視覚的に表現し、トラブルシューティングに大きく役立ちます。このビューには、**ユーザー詳細** > **セッションパフォーマンス** > **セッションのトポロジ**からアクセスできます。エンドツーエンドのネットワークホップビューには、接続されたHDXセッションのコンポーネント、メタデータ、リンク、および公開アプリケーションが表示されます。

このビューは、管理者が次のことを行うのに役立ちます。

- セッションのデータフローを理解する。
- 特定のホップにおけるパフォーマンスのボトルネックを特定する。

セッションパフォーマンスメトリック

管理者が特定のセッションのパフォーマンスを理解するのに役立つ、以下のメトリックがコンテキストに応じて利用可能です。エンドツーエンドのネットワークホップビューに表示されるメトリックは、ほぼリアルタイムで利用可能であり、UIに表示される間隔に基づいて定期的に更新されます。
エンドポイントメトリック
エンドポイントメトリックは、ユーザーエクスペリエンスの「ラストマイル」に関する洞察を提供し、ユーザーの即時環境に関する詳細を明らかにするため、Citrix®セッションパフォーマンスのトラブルシューティングに不可欠です。これらのメトリックは、貧弱なWi-Fi、低いネットワー

クスループット、エンドポイントデバイスの制限などのローカルなボトルネックを特定し、サーバー側とクライアント側の問題を区別するのに役立ちます。セッションのトポロジのメトリックと組み合わせることで、エンドポイントデータは全体的なビューを提供し、パフォーマンス問題の根本原因の特定を迅速化し、解決を早め、ユーザーエクスペリエンスを向上させます。

Citrix Studioのポリシーを使用して、要件に基づいてリストされているエンドポイントメトリックの収集を有効または無効にします。これらのポリシーは、Citrix管理者がコンプライアンス要件に準拠してメトリックを報告するための詳細な制御を提供します。

ポリシー名	ポリシーの説明	UIメトリック	デフォルト値	値のオプション	VIRTUAL DELIVERY AGENTのバージョン
エンドポイント統計間隔	ユーザーエンドポイントからエンドポイントネットワーク詳細の収集を許可します。このポリシーを有効にすることは、他のエンドポイント関連ポリシーが有効になるための前提条件です。	Wi-Fi信号強度、ネットワークインターフェースタイプ、スループット（受信または送信）、リンク速度、ワークスペースタイプ、エンドポイントCPU、エンドポイントメモリ、エンドポイントGPU	有効	有効または無効。頻度を60秒～3600秒の間で変更するオプション。60秒が推奨値です。	2407以降
エンドポイント位置情報データ収集	Locusサービス (https://locus.analytics.cloud.com) を使用して、ユーザーエンドポイントからエンドポ	パブリックIPアドレス、国、都市、インターネットサービスプロバイダー。	無効	有効または無効	2411 以降

ポリシー名	ポリシーの説明	UIメトリック	デフォルト値	値のオプション	VIRTUAL DELIVERY AGENTのバージョン
	イントの位置情報とISPの詳細の収集を許可します。				
エンドポイントネットワーク遅延測定間隔	エンドポイントとビーコンホスト間のネットワーク遅延の測定と収集を可能にします - `<https://downloadplugins.citrix.com>`	ネットワーク遅延（エンドポイントネットワーク詳細内）	無効	有効または無効。頻度を60秒～3600秒の間で変更するオプション。60秒が推奨値です。	2411 以降

注:

Citrix Virtual Apps and Desktops™ 2507 以降では、**エンドポイント位置情報データ収集**ポリシーと**エンドポイントネットワーク遅延測定間隔**ポリシーはデフォルトで無効になっています。そのため、これらのポリシーがStudioで手動で有効にされない限り、関連データはDirectorで利用できません。

すぐに利用できるエンドポイントメトリックは以下のとおりです。

- エンドポイント名
- エンドポイントIP
- エンドポイントOS
- Citrix Workspace™ アプリバージョン

次の表に、サポートされている製品バージョンに依存するメトリックを示します。

機能名	UIパラメーター	VDA WINDOWSバージョン	VDA MACバージョン	VDA LINUXバージョン	CITRIX WORKSPACE APP FOR WINDOWSのバージョン	CITRIX WORKSPACE APP FOR MACのバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5バージョン	CITRIX WORKSPACE APP FOR CHROME OSバージョン
エンドポイントネットワークの詳細	ネットワークインターフェースの種類	2407以降	NA	NA	2405.10以降	2409以降	2408以降	2411以降	2411以降
	信号強度	2407以降	該当なし	該当なし	2405.10以降	2409以降	2408以降	該当なし	該当なし
	エンドポイントスループット(受信、送信)	2407以降	該当なし	該当なし	2405.10以降	2409以降	2408以降	該当なし	該当なし
	リンク速度	2407以降	該当なし	該当なし	2405.10以降	2409以降	2408以降	2411以降	2411以降

機能名	UIパラメーター	VDA WINDOWS バージョン	VDA MAC バージョン	VDA LINUX バージョン	CITRIX WORKSPACE APP FOR WINDOWS のバージョン	CITRIX WORKSPACE APP FOR MAC のバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5 バージョン	CITRIX WORKSPACE APP FOR CHROME OS バージョン
	エンドポイントのパブリックIPアドレス	2411 以降	NA	NA	2409 以降	2409 以降	2408 以降	2411 以降	2411 以降
	エンドポイントの都市、エンドポイントの国	2411 以降	NA	NA	2409 以降	2409 以降	2408 以降	2411 以降	2411 以降
	インターネットサービスプロ	2411 以降	該当なし	該当なし	2409 以降	2409 以降	2408 以降	2411 以降	2411 以降

機能名	UIパラメーター	VDA WINDOWSバージョン	VDA MACバージョン	VDA LINUXバージョン	CITRIX WORKSPACE APP FOR WINDOWSのバージョン	CITRIX WORKSPACE APP FOR MACのバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5バージョン	CITRIX WORKSPACE APP FOR CHROME OSバージョン
	バイダー								
	ワークスペースの種類	2411以降	該当なし	該当なし	2409以降	2409以降	2408以降	2411以降	2411以降
	アクセスタイプ(Workspace / StoreFront経由)	2411以降	該当なし	該当なし	2409以降	2409以降	2408以降	2411以降	2411以降
	エンドポイントCPU	2411以降	NA	NA	2409以降	2409以降	2408以降	該当なし	2411以降
	エンドポイン	2411以降	NA	NA	2409以降	2409以降	2408以降	該当なし	2411以降

機能名	UIパラメーター	VDA WINDOWSバージョン	VDA MACバージョン	VDA LINUXバージョン	CITRIX WORKSPACE APP FOR WINDOWSのバージョン	CITRIX WORKSPACE APP FOR MACのバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5バージョン	CITRIX WORKSPACE APP FOR CHROME OSバージョン
	トメモリ								
	エンドポイントGPU	2411以降	該当なし	該当なし	2409以降	2409以降	2408以降	該当なし	該当なし
	ネットワーク遅延	2411以降	NA	NA	2409以降	2409以降	2408以降	2411以降	2411以降

データ定義:

UIパラメーター	説明
エンドポイント名	セッションに使用されるユーザーのエンドポイントデバイスの名前。
エンドポイントIP	Virtual Delivery Agent (VDA) で利用可能なエンドポイントのIPアドレス。エンドポイントデバイスのプライベートIPアドレスまたはパブリックIPアドレスが含まれる場合があります。
エンドポイントOS	エンドポイントデバイスのオペレーティングシステム

UIパラメーター	説明
Citrix Workspaceアプリのバージョン	インストールされているCitrix Workspaceアプリのバージョン
信号強度	ワイヤレス信号の品質と強度を表示します。
エンドポイントスループット (受信、送信)	ネットワークインターフェイスへのデータ転送速度と、ネットワークインターフェイスからのデータ転送速度を示します。エンドポイントで観測されるアップロードおよびダウンロードのインターネット速度に類似しています。
リンク速度	イーサネット、Wi-Fi、セルラーなどのネットワーク接続の種類を指定します。
ネットワークインターフェイスの種類	ネットワーク接続の最大データ転送速度を表します。
エンドポイントのパブリックIPアドレス	インターネットサービスプロバイダーによってデバイスに割り当てられた外部IPアドレス。
エンドポイントの都市、エンドポイントの国	デバイスの地理的な場所（国と都市を含む）。
インターネットサービスプロバイダー	エンドユーザーデバイスにインターネットアクセスを提供する会社の名前。
ワークスペースの種類	使用されているワークスペースの種類（Citrix WorkspaceアプリまたはWebブラウザー）。
アクセスタイプ（Workspace / StoreFront経由）	リソースにアクセスする方法（Citrix WorkspaceまたはStoreFront経由）。
エンドポイントCPU	現在使用されているCPUリソースの割合。
エンドポイントメモリ	現在使用されているメモリリソースの割合。
エンドポイントGPU	現在使用されているGPUリソースの割合。
ネットワーク遅延テスト	ネットワークで発生する時間遅延（ミリ秒単位で測定）。

ネットワークメトリック

Citrixセッションのパフォーマンスと安定性は基盤となるネットワークの状態に大きく依存しているため、ネットワークメトリックはCitrixセッションのトラブルシューティングにとって重要です。ローカルアプリケーションとは異なり、Citrixセッションではインタラクティブなデスクトップまたはアプリケーションのエクスペリエンスがネットワーク経由でストリーミングされるため、ネットワークの不安定性やボトルネックはユーザーのパフォーマンス認識に直接影響します。

Citrix Studioのポリシーを使用して、要件に基づいてリストされているネットワークメトリックの収集を有効または無効にします。これらのポリシーは、Citrix管理者に、コンプライアンス要件に従ってメトリックを報告するためのきめ細かな制御を提供します。

ポリシー名	ポリシーの説明	UIメトリック	デフォルト値	値のオプション	VIRTUAL DELIVERY AGENTバージョン
ネットワークテレメトリ	ユーザーエンドポイントとバックエンドコンポーネント間のネットワーク詳細の収集を許可します。	Citrix GatewayおよびCitrix Gatewayサービスに関するすべてのHDX Insightsメトリック	無効	有効または無効。頻度を60秒～3600秒の間で変更するオプション。60秒が推奨値です。	Gatewayサービスの場合は2411以降。Citrix Gatewayの場合は2503以降。

Citrix Gatewayサービス
次の表は、サポートされている製品バージョンに依存するメトリックを示しています。

機能名	UIパラメーター	WINDOWS VDA バージョン	MAC VDA バージョン	LINUX VDA バージョン	CITRIX WORKSPACE アプリ FOR WINDOWS バージョン	CITRIX WORKSPACE アプリ FOR MAC バージョン	CITRIX WORKSPACE アプリ FOR LINUX バージョン	CITRIX WORKSPACE アプリ FOR HTML5 バージョン	CITRIX WORKSPACE アプリ FOR CHROME OS バージョン
ネットワークメトリック	L7 サーバー遅延	2411 以降	2507 以降	2507 以降	2409 以降	2505 以降	2505 以降	該当なし	該当なし
	L7 クライアント遅延	2411 以降	2507 以降	2507 以降	2409 以降	2505 以降	2505 以降	該当なし	該当なし
	クライアント側の再送信 注: TCP セッションでのみ利用可能です	2411 以降	2507 以降	2507 以降	2409 以降	2505 以降	2505 以降	該当なし	該当なし
	スルー	2411 以降	N/A	N/A	2409 以降	2505 以降	2505 以降	N/A	N/A

機能名	UIパラメーター	WINDOWS VDAバージョン	MAC VDAバージョン	LINUX VDAバージョン	CITRIX WORKSPACE アプリ FOR WINDOWS バージョン	CITRIX WORKSPACE アプリ FOR MAC バージョン	CITRIX WORKSPACE アプリ FOR LINUXバージョン	CITRIX WORKSPACE アプリ FOR HTML5 バージョン	CITRIX WORKSPACE アプリ FOR CHROME OS バージョン
	プット								

シトリックス ゲートウェイ

次の表に、サポートされている製品バージョンに依存するメトリックを示します。

機能名	UIパラメーター	CITRIX GATEWAY バージョン	WINDOWS VDAバージョン	MACバージョン	LINUXバージョン	WINDOWS版 CITRIX WORKSPACE アプリのバージョン	MAC版 CITRIX WORKSPACE アプリのバージョン	LINUX版 CITRIX WORKSPACE アプリのバージョン	HTML5版 CITRIX WORKSPACE アプリのバージョン	CHROMEOS版 CITRIX WORKSPACE アプリのバージョン
ネットワークメトリック	WAN遅延	Netscaler 14.1-47.46 以降	2503 以降	2507 以降	2507 以降	2503 以降	2505 以降	2505 以降	該当なし	NA

機能名	UIパラメーター	CITRIX GATEWAY バージョン	WINDOWS VDA バージョン	MAC バージョン	LINUX バージョン	WINDOWS 版 CITRIX WORKSPACE アプリのバージョン	MAC版 CITRIX WORKSPACE アプリのバージョン	LINUX 版 CITRIX WORKSPACE アプリのバージョン	HTML5版 CITRIX WORKSPACE アプリのバージョン	CHROMEOS 版 CITRIX WORKSPACE アプリのバージョン
	DC 遅延	Netscaler 14.1-47.46 以降	2503 以降	2507 以降	2507 以降	2503 以降	2505 以降	2505 以降	NA	NA
	サーバー側再送信	Netscaler 14.1-47.46 以降	2503 以降	2507 以降	2507 以降	2503 以降	2505 以降	2505 以降	NA	NA
	クライアント側の再送信	Netscaler 14.1-47.46 以降	2503 以降	2507 以降	2507 以降	2503 以降	2505 以降	2505 以降	NA	NA
	L7 サーバー遅延	Netscaler 14.1	2503 以降	2507 以降	2507 以降	2503 以降	2505 以降	2505 以降	NA	NA

機能名	UIパラメーター	CITRIX GATEWAY バージョン	WINDOWS VDA バージョン	MAC バージョン	LINUX バージョン	WINDOWS 版 CITRIX WORKSPACE アプリのバージョン	MAC版 CITRIX WORKSPACE アプリのバージョン	LINUX 版 CITRIX WORKSPACE アプリのバージョン	HTML5版 CITRIX WORKSPACE アプリのバージョン	CHROMEOS 版 CITRIX WORKSPACE アプリのバージョン
		-47.46 以降								
	L7 クライアント遅延	Netscaler 14.1-47.46 以降	2503 以降	2507 以降	2507 以降	2503 以降	2505 以降	2505 以降	NA	NA
	クライアント側のゼロウィンドウサイズイベント	Netscaler 14.1-47.46 以降	2503 以降	2507 以降	2507 以降	2503 以降	2505 以降	2505 以降	NA	NA
	クライアント側の	Netscaler 14.1-47.	2503 以降	2507 以降	2507 以降	2503 以降	2505 以降	2505 以降	NA	NA

機能名	UIパラメーター	CITRIX GATEWAY バージョン	WINDOWS VDA バージョン	MAC バージョン	LINUX バージョン	WINDOWS 版 CITRIX WORKSPACE アプリのバージョン	MAC版 CITRIX WORKSPACE アプリのバージョン	LINUX 版 CITRIX WORKSPACE アプリのバージョン	HTML5版 CITRIX WORKSPACE アプリのバージョン	CHROMEOS 版 CITRIX WORKSPACE アプリのバージョン
	高速 RTO	46 以降								
	サーバー側ゼロウィンドウサイズイベント	Netscaler 14.1-47.46 以降	2503 以降	2507 以降	2507 以降	2503 以降	2505 以降	2505 以降	NA	NA
	サーバー側高速 RTO	Netscaler 14.1-47.46 以降	2503 以降	2507 以降	2507 以降	2503 以降	2505 以降	2505 以降	該当なし	該当なし

データ定義:

UIパラメーター	説明
WAN遅延	NetScaler®からエンドユーザーまでの、ネットワークのクライアント側によって引き起こされる遅延。
DC レイテンシー	NetScalerからバックエンドサーバーまでの、ネットワークのサーバー側によって引き起こされる遅延。
L7 クライアントレイテンシー	ICA®クライアントとNetScalerインスタンス間で観測された平均L7レイテンシー。このメトリックは、配信パスに存在するCitrix以外のデバイスで役立ちます。
L7 サーバーレイテンシー	NetScalerデバイスとCitrix Virtual App間で観測された平均L7レイテンシー。このメトリックは、配信パスにCitrix以外のデバイスが存在する場合に役立ちます。
クライアント再送信	NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高い場合、再送信による高い帯域幅使用率を示しますが、必ずしもユーザーエクスペリエンスが悪いことを意味するわけではありません。注：Gatewayサービスを使用するセッションの場合、クライアント再送信はTCPセッションでのみ利用可能です。
サーバー側再送信	NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。
クライアント側ゼロウィンドウ数	クライアントがゼロTCPウィンドウをアドバタイズした回数。
サーバー側ゼロウィンドウ数	サーバーがゼロTCPウィンドウをアドバタイズした回数。

VDAメトリック

機能名	UIパラメーター	WINDOWS VDAのバージョン	MACのバージョン	LINUXのバージョン	CITRIX WORKSPACE APP FOR WINDOWSのバージョン	CITRIX WORKSPACE APP FOR MACのバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5バージョン	CITRIX WORKSPACE APP FOR CHROME OSバージョン
VDAメトリック	VDA CPU	2511以降	NA	NA	2503以降	2503以降	2503以降	NA	NA
	VDAメモリ	2511以降	NA	NA	2503以降	2503以降	2503以降	NA	NA
	VDAディスクIOPS	2511以降	NA	NA	2503以降	2503以降	2503以降	NA	NA
	VDAディスク待機時間	2511以降	NA	NA	2503以降	2503以降	2503以降	該当なし	該当なし

HDXメトリック

HDXメトリックは、ユーザーの仮想エクスペリエンスの品質を理解し、トラブルシューティングを行う上で不可欠です。これらのメトリックは、仮想セッションを提供するICA/HDXプロトコルのパフォーマンスを直接測定します。

> **注:**
>
> ICAメトリックは、Citrix Workspaceアプリ for Windowsバージョン2405.10以降、およびCitrix Virtual Apps and Desktops 2407以降で利用可能です。ただし、データの更新と修正は

最新バージョンで提供されます。各データポイントの推奨バージョンについては、以下の表を参照してください。

機能名	UIパラメーター	WINDOWS VDA バージョン	MAC VDA バージョン	LINUX VDA バージョン	CITRIX WORKSPACEアプリ FOR WINDOWS バージョン	MAC版 CITRIX WORKSPACEアプリのバージョン	LINUX版 CITRIX WORKSPACEアプリのバージョン	HTML5版 CITRIX WORKSPACEアプリのバージョン
ICAメトリック	ICA RTT	2507以降	NA	NA	2503以降	2503以降	2503以降	2503以降
	ネットワーク待機時間	2507以降	該当なし	該当なし	2503以降	2503以降	2503以降	2503以降
	HDX接続タイプ	2411以降	該当なし	該当なし	2411以降	2411以降	2411以降	2411以降
	プロトコル	2411以降	NA	NA	2411以降	2411以降	2411以降	2411以降
	EDT MTU	2411以降	NA	NA	2411以降	2411以降	2411以降	2411以降

データ定義:

UI パラメーター	説明
ICA RTT	ユーザー操作から画面応答までの時間を測定します。Thinwire RTT カウンターは、Citrix Virtual Apps and Desktops バージョン 2507 以降、このメトリックを表します。以前のバージョンでは、引き続き EUEM RTT を使用します。
ネットワーク遅延	ネットワーク遅延と潜在的な速度低下を示します。Citrix Virtual Apps and Desktops バージョン 2503 以降、クライアント側とサーバー側の遅延の合計として定義されます。以前のバージョンでは、VDA で報告される HDX 遅延を継続して使用します。
HDX 接続タイプ	ユーザーセッションの HDX 接続の種類。
プロトコル	ユーザーセッションに使用される基盤となるプロトコル。値は *TCP* または *EDT* です。
EDT MTU	MTU（最大転送単位）は、ネットワークインターフェイスがフラグメント化せずに送信できるパケットの最大サイズ（バイト単位）です。EDT MTUは、ユーザーのEDTセッション用に確立されたMTUを表します。

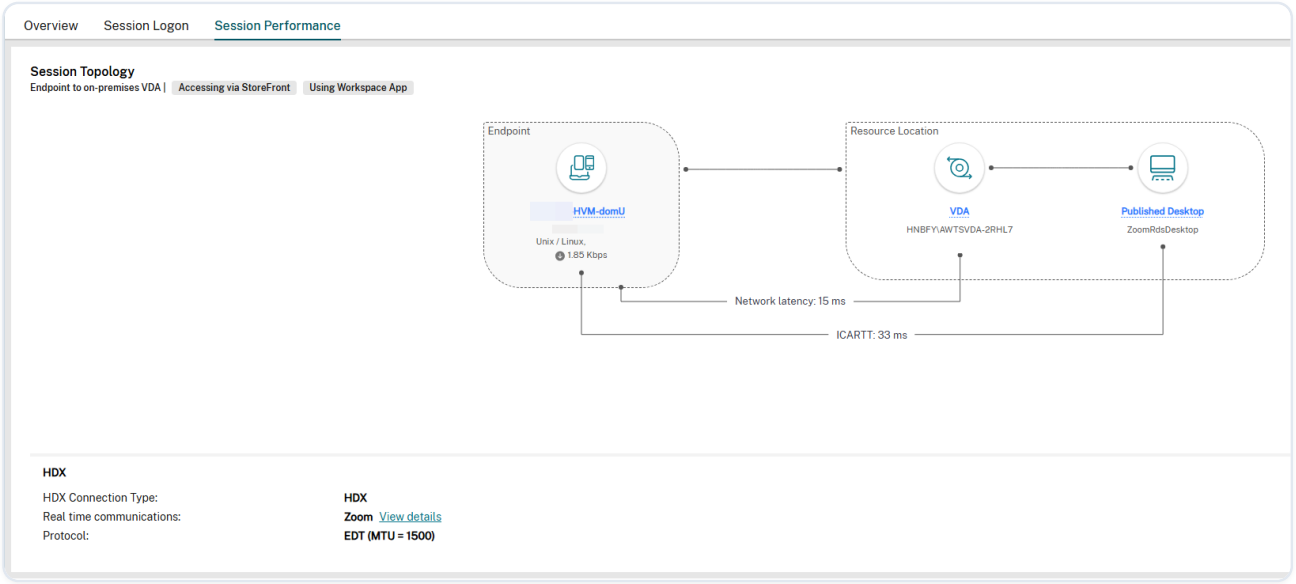
リアルタイム通信の最適化の可視性
セッショントポロジは、Citrixセッション内のMicrosoft Teams、Zoom、WebExなどのリアルタイム通信（RTC）アプリケーションの最適化ステータスに関する包括的な可視性を提供します。アプリケーションが最適化されているかどうかを特定し、最適なパフォーマンスを妨げる不足しているコンポーネント（必要なプラグイン、プラグイン管理、プラットフォーム固有の制限など）を識別します。

利点:

- 顧客はRTCアプリケーションの最適化に関して明確な保証を得ることができ、セッションが本当に最適化されているかどうかについての推測を排除できます。
- 不足しているコンポーネントを直接把握することで、問題を事前に解決し、完全な最適化を実現できます。

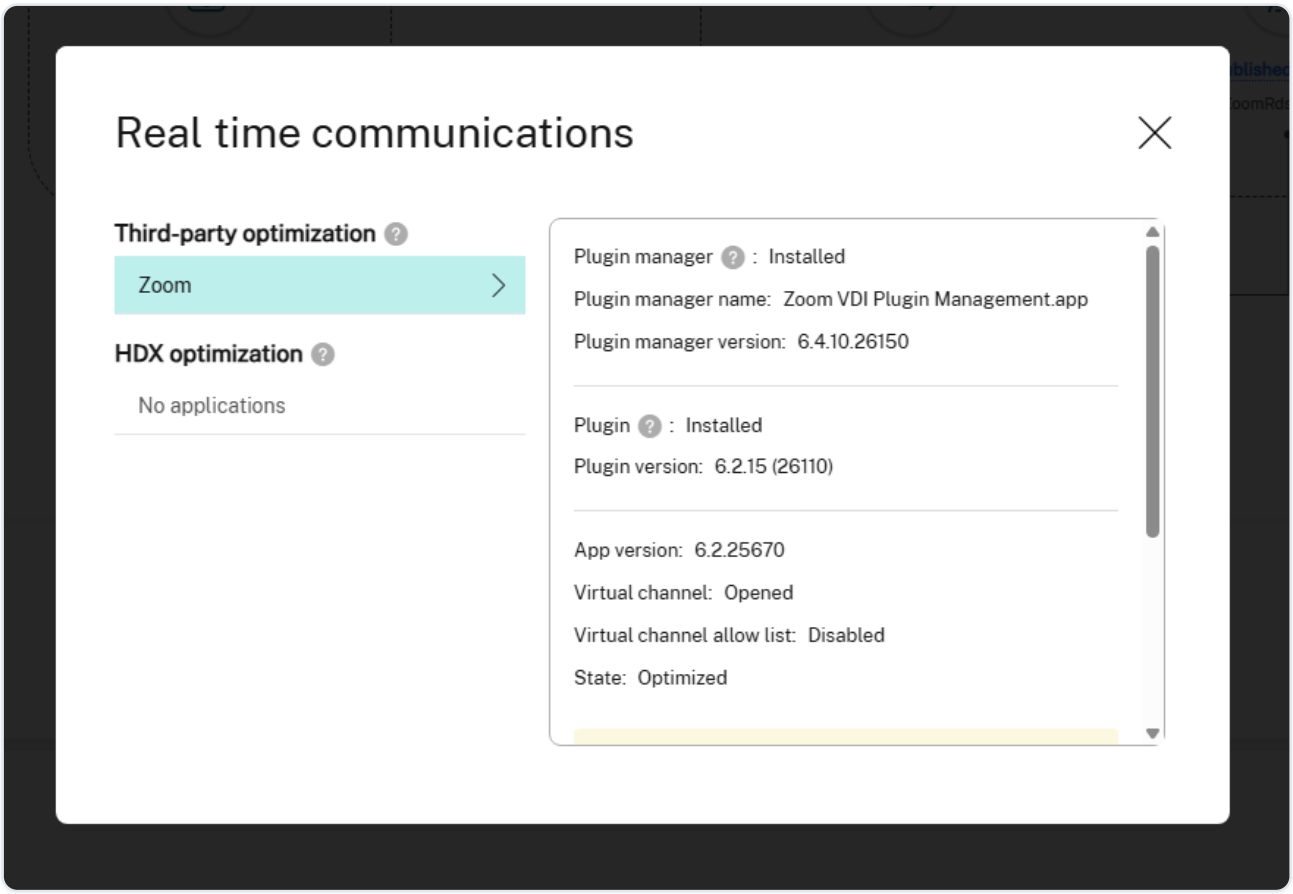
- トラブルシューティングの高速化により、重要な通信ツールのユーザーエクスペリエンスが向上します。

セッショントポロジの**リアルタイム通信**フィールドを使用して、各アプリケーションの最適化の詳細を表示します。



サードパーティ製の最適化されたアプリケーションは、Citrixテクノロジを使用して仮想チャネルを作成しますが、その他の構成と設定はアプリケーションベンダーが管理します。最適化はベンダーが所有するソリューションに依存します。

セッショントポロジ画面の**リアルタイム通信**フィールドの横にある**詳細を表示**リンクをクリックします。次の画面が表示されます。



HDX最適化アプリケーションはCitrix仮想チャネルを使用し、Citrixの構成と設定によって直接影響を受けます。

リアルタイム通信画面の**HDX最適化**セクションをクリックします。次の画像が表示されます。

MS Teamsリアルタイム通信(/en-us/citrix-daas/media/msteams-real-time-opt.png)

リアルタイム通信の詳細は5分ごとに更新されます。次の表は、サードパーティの最適化に依存するアプリケーションで利用可能な詳細を示しています。完全な可視性を得るには、サポートされている製品バージョンを使用していることを確認してください。

注:

- Microsoft Teams Slimcore最適化は、公開されたデスクトップと、ベンダーサポートに従ってNew Teamsでのみ利用可能です。
- Zoomの場合、プラグインの詳細と最適化の状態を取得するためのベンダー変更はバージョン6.3.10以降で利用可能です。詳細については、Zoomドキュメントを参照してください。

次の表に、Citrix HDX最適化に依存するアプリケーションで利用可能な詳細を示します。完全な可視性を得るには、サポートされている製品バージョンを使用していることを確認してください。

機能名	UIパラメーター	VIRTUAL DELIVERY AGENTバージョン	CITRIX WORKSPACE APP FOR WINDOWS のバージョン	CITRIX WORKSPACE APP FOR MAC のバージョン	CITRIX WORKSPACE APP LINUX版 バージョン
Microsoft Teams スリムコア	プラグインマネージャー、プラグインマネージャー名、プラグインマネージャーバージョン	2503	2503	ベンダーによってサポートされていません	ベンダーによってサポートされていません
	アプリバージョン、仮想チャネル、仮想チャネル許可リスト	2503	2402	ベンダーによってサポートされていません	ベンダーによってサポートされていません
	プラグイン、プラグインバージョン、状態	2507	2503	ベンダーによってサポートされていません	ベンダーによってサポートされていません
ズーム	プラグインマネージャー、プラグインマネージャー名、プラグインマネージャーバージョン	2507	2503	2505	プラグインが利用できません

機能名	UIパラメーター	VIRTUAL DELIVERY AGENTバージョン	CITRIX WORKSPACE APP FOR WINDOWS のバージョン	CITRIX WORKSPACE APP FOR MAC のバージョン	CITRIX WORKSPACE APP LINUX版 バージョン
	アプリバージョン、仮想チャネル、仮想チャネル許可リスト	2507	2402	2402	2402
	プラグイン、プラグインバージョン、状態	2507	2503	2505	プラグイン利用不可
ウェブエックス	プラグインマネージャー、プラグインマネージャー名、プラグインマネージャーバージョン	2507	2503	プラグイン利用不可	プラグイン利用不可
	アプリバージョン、仮想チャネル、仮想チャネル許可リスト	2507	2402	2402	2402

次の表に、Citrix HDX最適化に依存するアプリケーションで利用可能な詳細を示します。完全な可視性を得るには、サポートされている製品バージョンを使用していることを確認してください。

機能名	UIパラメーター	VIRTUAL DELIVERY AGENTバージョン	CITRIX WORKSPACE APP FOR WINDOWS のバージョン	CITRIX WORKSPACE APP FOR MAC のバージョン	CITRIX WORKSPACE APP LINUX版 バージョン
マイクロソフト チームズ	状態	1906.2	2112	2203	2203

データ定義:

UIパラメーター	説明
プラグインマネージャー	プラグインマネージャーがインストールされているかどうかを示します。プラグインマネージャーは、仮想チャネルを開き、最適化に必要なメディアエンジン（プラグイン）をダウンロードする小さな管理コンポーネントです。注：機能はベンダーによって異なる場合があります。
プラグインマネージャー名	インストールされているプラグインマネージャーの名前です。
プラグインマネージャーのバージョン	インストールされているプラグインマネージャーのバージョンです。
プラグイン	プラグインがインストールされているかどうかを示します。プラグインは、最適化に必要なメディアエンジンです。注：機能はベンダーによって異なる場合があります。
プラグインのバージョン	エンドポイントにインストールされているプラグインのバージョン。
アプリケーションのバージョン	仮想配信エージェント（VDA）上のアプリケーションのバージョンを表します。
仮想チャネル	リアルタイム通信アプリの仮想チャネルが開いているか閉じているかを表します。

UIパラメーター	説明
仮想チャネル許可リスト	仮想チャネルのステータスを表示します。値は *Enabled* または *Disabled* です。
状態	特定のユーザーセッションにおけるアプリケーションの最適化状態を表示します

セッショントポロジのシナリオ

セッショントポロジはアクティブなセッションで利用可能で、リアルタイムで更新されます。切断されたセッションや終了したセッションでは、包括的なセッション後分析のために、最後に認識された状態のトポロジが表示されます。

サイトの展開シナリオに応じて、セッションに関与するコンポーネントは以下のすべてまたは一部です。

- エンドポイント上のCitrix Workspaceアプリ
- Gatewayサービス/オンプレミスGateway
- Cloud Connector – ハイブリッド接続の場合、GatewayはCloud Connectorを介してDaaSに接続されます。
- VDA

したがって、可能なネットワークトポロジは次のとおりです。

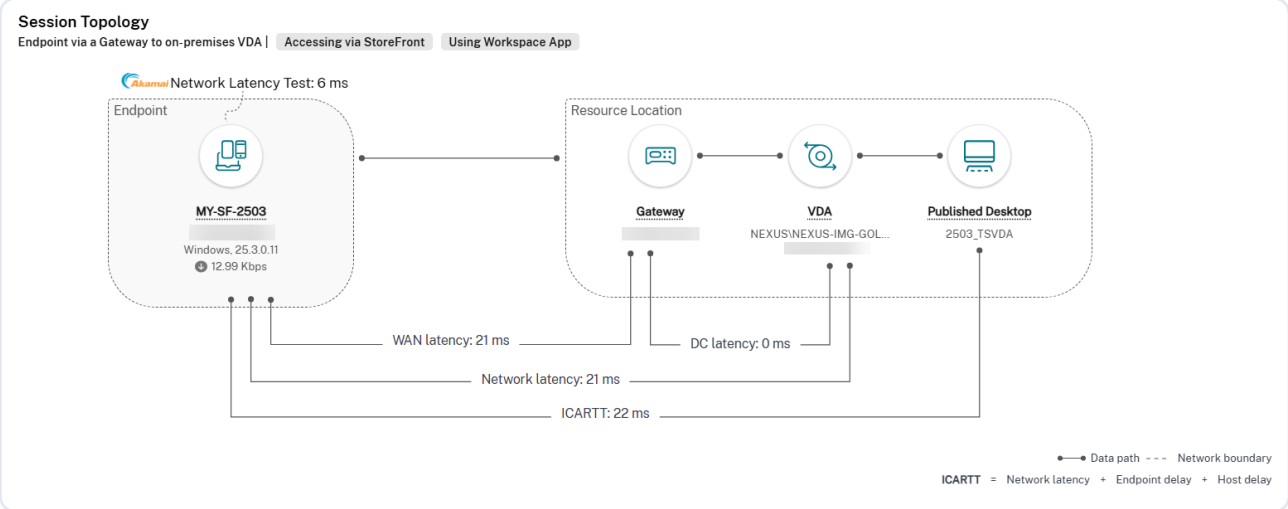
- エンドポイント上のCitrix Workspaceアプリは、Citrix WorkspaceおよびGateway Serviceを介してオンプレミスのVDAに接続します。VDAへの接続にCloud Connectorは使用されません。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/2511/media/dir-session-topology1.png)

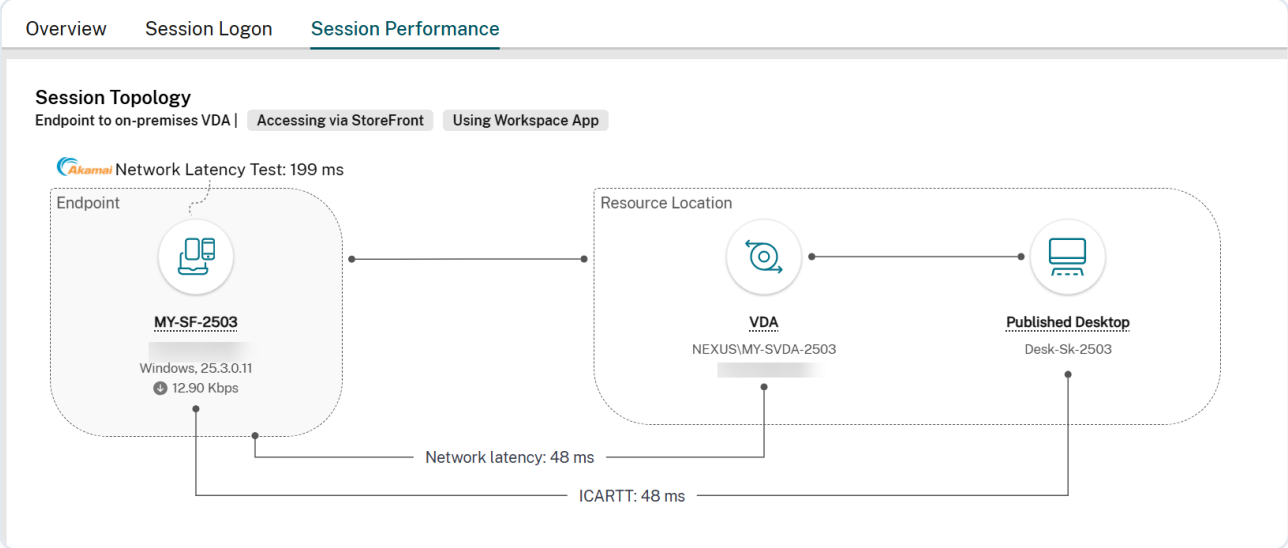
- エンドポイント上のCitrix Workspaceアプリは、Citrix WorkspaceおよびGateway Serviceを介して、Cloud Connector経由でオンプレミスのVDAに接続します。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/2511/media/dir-session-topology2.png)

- エンドポイント上のCitrix Workspaceアプリは、StoreFront™およびオンプレミスGatewayを介してオンプレミスVDAに接続します。

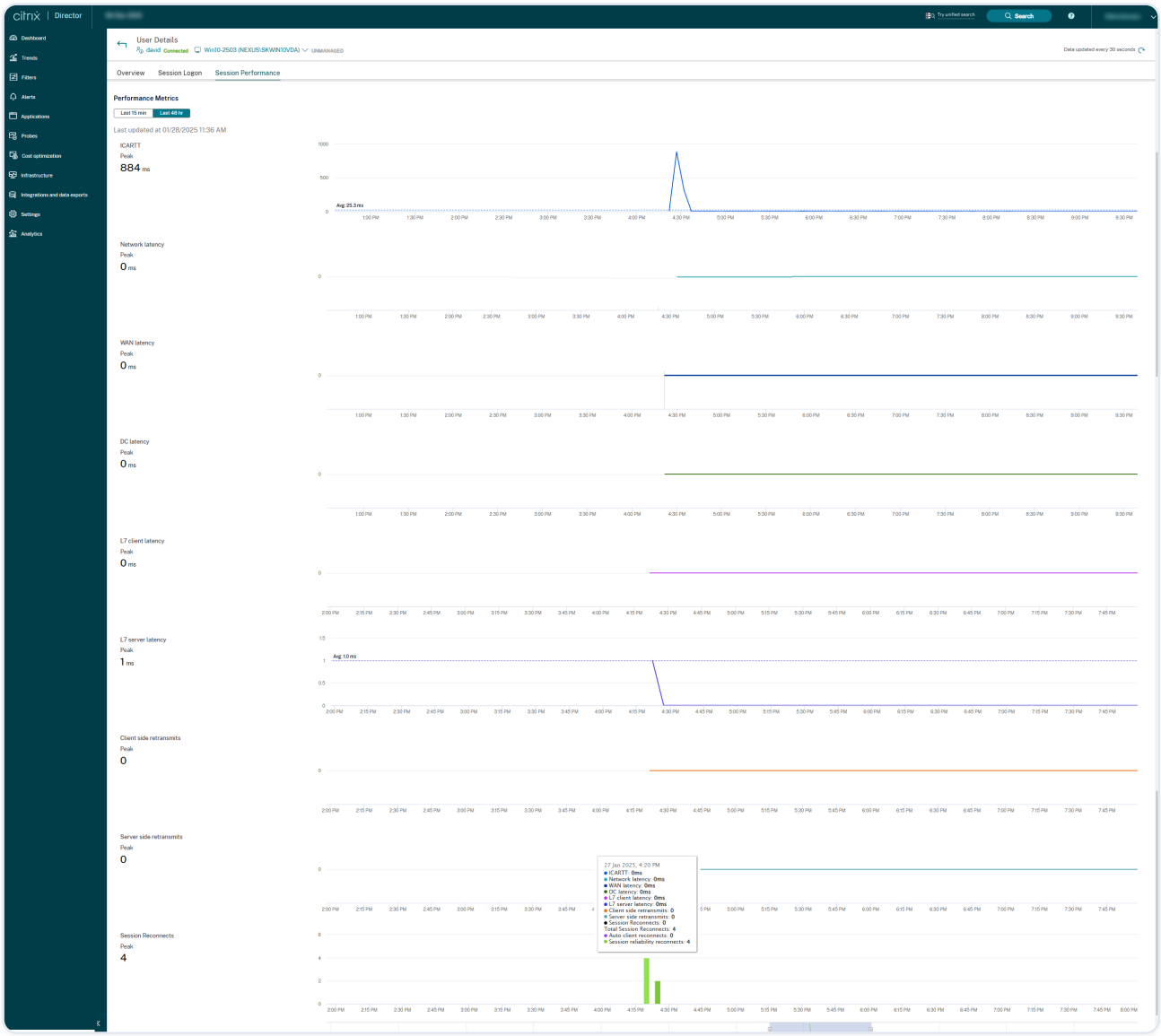


- エンドポイント上のCitrix Workspaceアプリは、StoreFrontを介してオンプレミスVDAに接続します。



パフォーマンスメトリック

パフォーマンスメトリックパネルでは、リアルタイムメトリックを関連付けて、ユーザーセッション内の問題を特定できます。セッションメトリックの傾向は、これらのメトリックが時間の経過とともにどのようにパフォーマンスを発揮したかを示すのに役立ちます。**セッションパフォーマンス**タブをクリックすると、リアルタイムデータとともに、過去15分間および48時間のデータを表示できます。プロットは、複数のコンポーネントのパフォーマンスメトリックを単一のビューで関連付けるのに役立ちます。



注：

- 過去15分間のメトリックサポートにより、グラフはセッションが接続および切断された期間についてプロットされます。切断されたセッションのメトリックは、値ゼロで表示されます。
- 過去48時間のメトリックサポートにより、ICARTT、ICA Latency、およびセッション再接続のプロットが履歴データメトリックで更新されます。セッション再接続情報は、中断のあるネットワーク接続を表示およびトラブルシューティングするのに役立ちます。また、シームレスなエクスペリエンスを持つネットワークも分析します。セッション再接続数、合計セッション再接続数、自動クライアント再接続、およびセッション信頼性再接続の数を確認するためのグラフです。

> ICARTTとICA Latencyの他に、リアルタイムおよび過去15分間のメトリックとして、次のメトリックが利用可能です。

- 1秒あたりのフレーム数 - 1秒あたりのフレーム数は、セッションの応答性を示す重要なメトリックです。
- 利用可能な出力帯域幅 - 利用可能な出力帯域幅は、VDAからエンドポイントにデータを送信するために利用可能な総帯域幅の測定値です。
- 消費された出力帯域幅 - 消費された出力帯域幅は、ユーザーにセッションを表示するためにVDAからエンドポイントに送信された実際のデータ量を示します。

利用可能な出力帯域幅と消費された出力帯域幅を分析することで、セッションを提供するために十分な帯域幅が利用可能であるか、およびセッションが帯域幅不足の影響を受けているかどうかを確認できます。

ICA RTTまたはセッションログオン期間のデータが入力されない場合のトラブルシューティング

以前は、EUEMサービスまたはプロファイル管理サービスが実行に失敗した場合、ICA RTTまたはセッションログオン期間に関連するデータ取得の失敗理由が表示されませんでした。この新機能により、失敗の理由と、その失敗に対する対応する解決策を取得できます。**詳細はこちら**のリンクには、以下の表に示すように、ICA RTTおよびセッションログオン期間のエラー、失敗の理由、および解決策が記載されています。

エラーの種類	エラー	エラーメッセージ	解決策
ICA RTTエラー	ICA RTT値が表示されません。	**Citrix End User Experience Monitoringが実行されていません。**	1. サービスコンソールを開きます。このコンソールを開くには、**スタート**をクリックし、**サービス**と入力します。
			2. Citrix End User Experience Monitoring Serviceが実行されていることを確認します。
			3. デスクトップセッションを再度開き、試してくださ

エラーの種類	エラー	エラーメッセージ	解決策
			い。ICA RTT値が表示されるはずです。
			4. 問題が解決しない場合は、Citrix管理者に連絡してください。
ICA RTTエラー	ICA RTT値が表示されません。	**Citrix End User Experience Monitoringがインストールされていません。**	1. VDAを再インストールしてください。
			2. サービスコンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サービス」と入力します。
			3. Citrix End User Experience Monitoring Serviceが実行されていることを確認してください。
			4. デスクトップセッションを再度開き、試してください。ICA RTT値が現在表示されているはずです。
			5. 問題が解決しない場合は、Citrix管理者に連絡してください。
ICA RTTエラー	ICA RTT値が表示されません。	**データの取得エラー。**	1. 「サービス」コンソールを開きます。このコンソール

エラーの種類	エラー	エラーメッセージ	解決策
			を開くには、**スタート**をクリックし、「サービス」と入力します。
			`2.` **Windows Management Instrumentation Service**が実行されていることを確認します。
			`3.` また、**アクティビティマネージャー** > **プロセス**タブでWfShell.exe/PicaShell.exeプロセスが実行されていることを確認します。実行されていない場合は、デスクトップセッションを再度開きます。
			`4.` 前述の手順で解決しない場合は、Citrix_Euem_RoundTripインスタンスが存在することを確認するために、次のコマンドを実行します。`Get-CimInstance -Namespace 'ROOT\Citrix\Euem' -Query "select * from Citrix_Euem_RoundTrip"`

エラーの種類	エラー	エラーメッセージ	解決策
			5. Citrix_Euem_RoundTripインスタンスが存在する場合は、デスクトップセッションを再度開きます。
			6. 問題が解決しない場合は、Citrix管理者に連絡してください。
セッションログオン期間エラー	グラフが読み込まれていません。	**Citrix Profile Managementが実行されていません**	1. サービスコンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サービス」と入力します。
			2. **Citrix Profile Management Service**が実行されていることを確認してください。
			3. デスクトップセッションを再度開き、試してください。グラフが表示されるはずです。
			4. 問題が解決しない場合は、Citrix管理者に連絡してください。
セッションログオン期間エラー	グラフが読み込まれていません。	**Citrix Profile Management がインストールされていません。**	1. Citrix Profile Management Service をインストールしてください。

エラーの種類	エラー	エラーメッセージ	解決策
			2. サービスコンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サービス」と入力します。
			3. **Citrix Profile Management Service** が実行されていることを確認します。
			4. デスクトップセッションを再度開き、試してください。グラフが表示されるはずです。
			5. 問題が解決しない場合は、Citrix 管理者に連絡してください。
セッションログオン期間エラー	グラフが読み込まれていません。	**データの取得中にエラーが発生しました。**	1. 「**サービス**」コンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サービス」と入力します。
			2. **Windows Management Instrumentation Service**が実行中であることを確認します。

エラーの種類	エラー	エラーメッセージ	解決策
			`3.` 前述のサービスがすでに実行中の場合は、`LogonTimings instance is present`であることを確認するために、次のコマンドを実行します: `Get-CimInstance -Namespace 'ROOT\Citrix\Profile\Metrics' -Query "select * from LogonTimings"`
			`4.` 問題が解決しない場合は、Citrix管理者に連絡してください。
ICA RTTエラー	ICA RTT値が表示されません。	コンソールはサポートされていません。	HDXを使用してセッションを開始します。
ICA RTTエラー	ICA RTT値が表示されません。	リモートデスクトッププロトコル (RDP) はサポートされていません。	HDXを使用してセッションを開始します。
ICA RTTエラー	ICA RTT値が表示されません。	詳細なエラー検出とすべての機能へのアクセスを得るには、VDAをバージョン2402以降にアップグレードしてください。	VDAを2402以降にアップグレードしてください。

エラーの種類	エラー	エラーメッセージ	解決策
セッションログオン期間エラー	グラフが読み込まれていません。	Citrix Profile Management WMIプラグインがインストールされていません。	Citrix Profile Management WMIプラグインをインストールしてください。

終了したユーザーセッションの診断

Citrix Director は、アクティブ、切断、または終了状態のセッションの詳細を表示するようになりました。以前は、アクティブなセッションの詳細のみを表示できました。この機能により、ヘルプデスク管理者は、終了したセッションまたは終了状態のセッションに関する問題をトラブルシューティングできます。終了したセッションの詳細は、過去24時間および過去2日間利用できます。終了したセッションまたは終了状態のセッションについて、以下の詳細を表示できます。

- マシン詳細パネル - 選択したセッションが起動されたマシンの利用可能な詳細を表示します。
- セッション詳細パネル - 選択したセッションの利用可能な詳細を表示します。
- セッションログオン期間 - 選択したセッションにかかったログオン期間に関する情報を表示します。以下の項目にかかった時間のグラフを表示できます。
    - ブローカリング
    - マシンの起動
    - HDX™接続
    - 認証
    - GPO
    - ログオンスクリプト
    - ディスク上のプロファイル読み込み
    - 対話型セッション

過去のユーザーセッションを表示するには、次の手順を実行します。

1. **フィルター** > **セッション**ビューをクリックします。
2. 「**関連ユーザー**」をクリックして、ユーザーのActivity Managerを開きます。

    過去のユーザーセッションのアクティビティマネージャー(/en-us/citrix-virtual-apps-desktops/2511/media/dir-his-user-sessions-am.png)
3. 「**終了したセッション**」セクションから必要なセッションを選択します。

4. 「**マシン詳細**」パネルと「**セッション詳細**」パネルを表示します。

   過去のユーザーセッションの詳細(/en-us/citrix-virtual-apps-desktops/2511/media/dir-his-user-sessions-details.png)

5. 下にスクロールして、終了したセッションの「**セッションログオン期間**」を表示します。

   過去のユーザーセッションの期間(/en-us/citrix-virtual-apps-desktops/2511/media/dir-his-user-sessions-duration.png)

6. 「**セッションログオン**」タブをクリックして、詳細を表示します。

   終了したユーザーセッションのログオン期間(/en-us/citrix-virtual-apps-desktops/2511/media/session-logon-ended.png)

7. 「**セッションパフォーマンス**」タブをクリックして、詳細を表示します。

   終了したユーザーセッションのパフォーマンス(/en-us/citrix-virtual-apps-desktops/2511/media/session-performance-ended.png)

ユーザーのシャドウイング

Directorから、シャドウユーザー機能を使用して、ユーザーの仮想マシンまたはセッションを直接表示したり操作したりできます。Windows VDAとLinux VDAの両方をシャドウできます。シャドウしたいマシンにユーザーが接続している必要があります。これは、ユーザーのタイトルバーに表示されているマシン名を確認することで検証できます。

Directorは新しいタブでシャドウイングを起動します。DirectorのURLからのポップアップを許可するようにブラウザ設定を更新してください。

シャドウ機能は、**ユーザーの詳細**ビューからアクセスします。ユーザーセッションを選択し、アクティビティマネージャービューまたはセッション詳細パネルで**シャドウ**をクリックします。

リモートアシストの使用

LINUX VDAのシャドウ

シャドウイングは、RHEL7.3またはUbuntuバージョン16.04のLinuxディストリビューションを実行しているLinux VDAバージョン7.16以降で利用できます。

> **注:**

- シャドウイングが機能するには、VDAがDirector UIからアクセス可能である必要があります。したがって、シャドウイングはDirectorクライアントと同じイントラネット内のLinux VDAでのみ可能です。
- DirectorはFQDNを使用してターゲットのLinux VDAに接続します。Directorクライアントがlinux VDAのFQDNを解決できることを確認してください。
- VDAには、python websockifyおよびx11vncパッケージがインストールされている必要があります。
- VDAへのnoVNC接続はWebSocketプロトコルを使用します。デフォルトでは、**ws://** WebSocketプロトコルが使用されます。セキュリティ上の理由から、Citrixは安全な **wss://** プロトコルを使用することを推奨します。各DirectorクライアントとLinux VDAにSSL証明書をインストールしてください。

セッションシャドウ の手順に従って、シャドウ用にVDAを構成してください。

1. **シャドウ**をクリックすると、シャドウ接続が初期化され、ユーザーデバイスに確認プロンプトが表示されます。
2. ユーザーに**はい**をクリックするよう指示して、マシンまたはセッションの共有を開始します。
3. 管理者はシャドウされたセッションを表示することのみ可能です。

WINDOWS VDA のシャドウイング

Windows VDAセッションは、Windowsリモートアシスタンスを使用してシャドウされます。VDAのインストール中に、**ユーザーWindowsリモートアシスタンス**機能を有効にします。詳細については、「機能の有効化または無効化」を参照してください。

1. **Shadow**をクリックすると、シャドウ接続が初期化され、.msrcインシデントファイルを開くか保存するかを促すダイアログボックスが表示されます。
2. デフォルトで選択されていない場合は、リモートアシスタンスビューアでインシデントファイルを開きます。ユーザーデバイスに確認プロンプトが表示されます。
3. マシンまたはセッションの共有を開始するには、ユーザーに**はい**をクリックするよう指示します。
4. より詳細な制御を行うには、ユーザーにキーボードとマウスの制御を共有するよう依頼します。

シャドウイングのためのMICROSOFT INTERNET EXPLORERブラウザーの合理化

ダウンロードしたMicrosoft Remote Assistance (.msra) ファイルをリモートアシスタンスクライアントで自動的に開くように、Microsoft Internet Explorerブラウザーを構成します。

これを行うには、グループポリシーエディターで 設定を有効にする必要があります。

コンピューターの構成 \> 管理用テンプレート \> Windows コンポーネント \> Internet Explorer \> インターネットコントロールパネル \> セキュリティページ \> インターネットゾーン \> ファイルのダウンロード時に自動的に確認する。

デフォルトでは、このオプションはローカルイントラネットゾーンのサイトで有効になっています。Director サイトがローカルイントラネットゾーンにない場合は、このゾーンにサイトを手動で追加することを検討してください。

HDX Screen Share の使用

Directorは、IT管理者とヘルプデスク担当者がHDX画面共有テクノロジーを通じてエンドユーザーにリモートサポートを提供できるようにするリモートアシスタンスをサポートしています。この機能は、CitrixのネイティブHDXプロトコルを活用して、トラブルシューティングとユーザー支援のシナリオ向けに安全で高性能な画面共有機能を提供します。

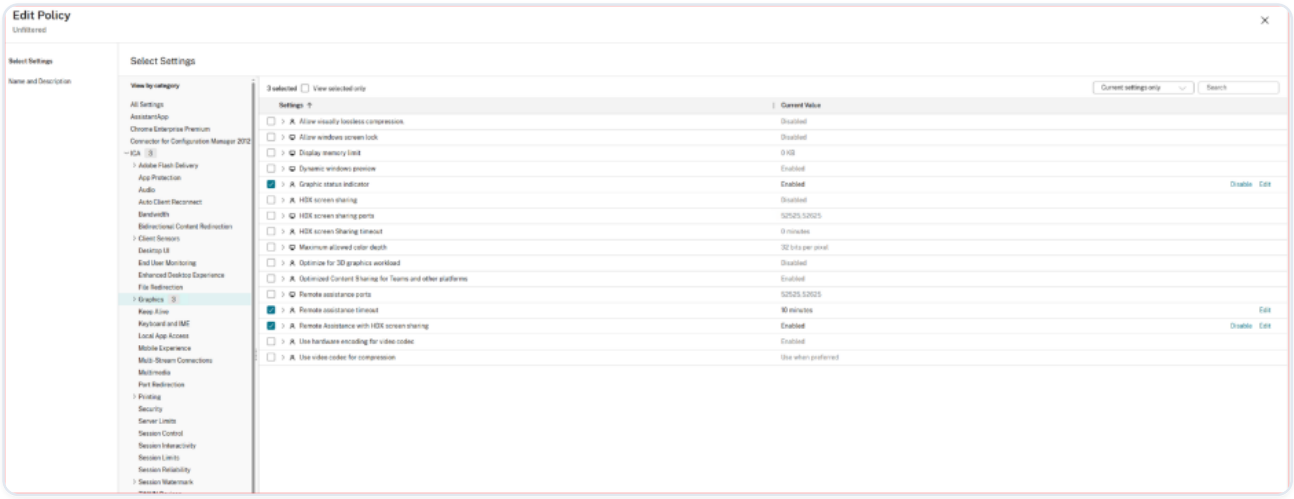
前提条件

コンポーネント	サポートされる環境またはバージョン
オペレーティングシステム	シングルセッションOS**またはマルチセッションOS**用のWindows、Linux
仮想デリバリーエージェント (VDA)	CR 2511以降
ディレクター	CR 2511以降
デリバリーコントローラー	CR 2511以降
TWPlayer (シンワイヤープレイヤー)	シャドウセッションを開始すると、Director UIでプレーヤーをダウンロードするためのリンクが利用可能になります

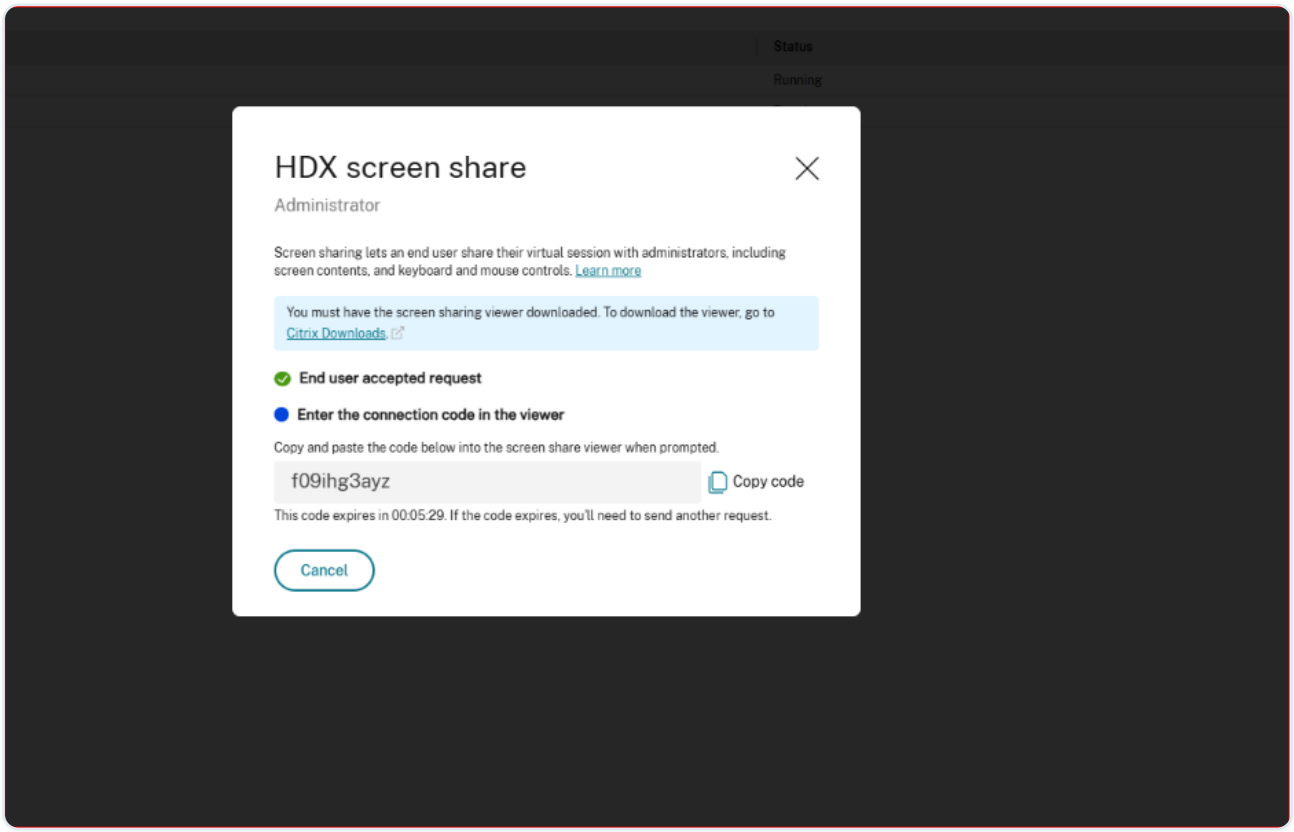
グループポリシーの構成

DirectorとHDX Screen Shareを使用してリモートアシスタンスを有効にするには、VDA上で次のグループポリシーを構成します。

- HDX画面共有によるリモートアシスタンス
- リモートアシスタンスのタイムアウト
- グラフィックステータスインジケーター



TWPlayer (ThinWire Player) は、HDXスクリーン共有機能を有効にするために一度ダウンロードする必要がある必須コンポーネントです。プレイヤーをダウンロードするためのリンクは、シャドウセッションを開始する際にDirector UIで利用できます。



制限事項

- 公開アプリケーション（アプリセッション）はシャドウできません – デスクトップセッションのみです。

DirectorとHDXスクリーン共有を使用したワークフロー
以下に示す手順は、管理者がHDXスクリーン共有セッションを開始するプロセスを概説しています。

1. **シャドウセッションの開始**

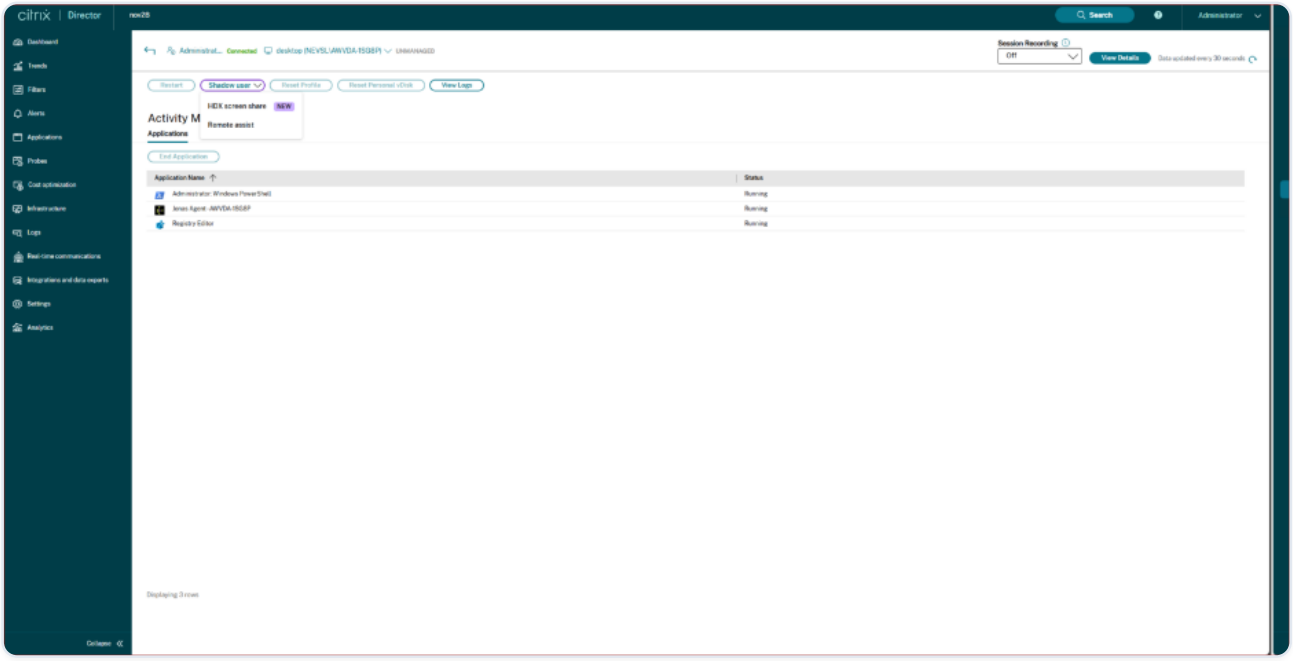
a. Citrix Directorにログインします
b. サポートが必要なユーザーセッションに移動します
c. 「シャドウ」ボタンをクリックします
d. HDXスクリーン共有を選択します

2. **ビューアを起動**

a. 生成されたインシデントファイルを TWPlayer/リモートアシスタンスビューアーで開きます
b. ユーザーが接続要求を承諾するのを待ちます

3. **セッションの表示**

a. セッション画面がビューアーウィンドウに表示されます
b. 管理者はユーザーの操作をリアルタイムで監視できます



ユーザーにメッセージを送信する

Directorから、1台以上のマシンに接続しているユーザーにメッセージを送信します。この機能を使用して、デスクトップのメンテナンス、マシンのログオフと再起動、プロファイルのリセットなど、管理アクションに関する即時通知を送信できます。

1. アクティビティマネージャービューで、ユーザーを選択し、をクリックします。
2. ユーザー詳細ビューで、パネルを見つけてをクリックします。
3. フィールドとフィールドにメッセージ情報を入力し、をクリックします。

メッセージが正常に送信されると、Directorに確認メッセージが表示されます。メッセージはユーザーのマシンに表示されます。

メッセージが正常に送信されなかった場合、Directorにエラーメッセージが表示されます。エラーメッセージに従って問題をトラブルシューティングします。完了したら、件名とメッセージテキストを再度入力し、もう一度 をクリックします。

アプリケーションの障害を解決する

「**アクティビティマネージャー**」ビューで、アプリケーションタブをクリックします。このユーザーがアクセスできるすべてのマシンのすべてのアプリケーション（現在接続されているマシンのローカルアプリケーションとホストされているアプリケーションを含む）と、それぞれのステータスを表示できます。

> **注:**
>
> アプリケーションタブがグレー表示されている場合は、そのタブを有効にする権限を持つ管理者に連絡してください。

> このリストには、セッション内で起動されたアプリケーションのみが含まれます。

マルチセッションOSマシンおよびシングルセッションOSマシンでは、切断されたセッションごとにアプリケーションが一覧表示されます。ユーザーが接続されていない場合、アプリケーションは表示されません。

アクション	説明
応答しないアプリケーションを終了する	応答しないアプリケーションを選択し、「アプリケーションの終了」をクリックします。アプリケーションが終了したら、ユーザーに再度起動するよう依頼します。
応答しないプロセスを終了する	必要な権限がある場合は、プロセスタブをクリックします。アプリケーションに関連する、または大量のCPUリソースやメモリを使用しているプロセスを選択し、「プロセスの終了」をクリックします。ただし、プロセスを終了するための必要な権限がない場合、プロセスを終了しようとしても失敗します。

アクション	説明
ユーザーのマシンを再起動する	シングルセッションOSマシンのみ、選択したセッションで「再起動」をクリックします。または、「マシン詳細」ビューから、電源コントロールを使用してマシンを再起動またはシャットダウンします。アプリケーションを再確認できるように、ユーザーに再度ログオンするよう指示します。マルチセッションOSマシンでは、再起動オプションは利用できません。代わりに、ユーザーからログオフし、ユーザーに再度ログオンさせます。
マシンをメンテナンスモードにする	マシンのイメージにパッチやその他の更新などのメンテナンスが必要な場合は、マシンをメンテナンスモードにします。[マシンの詳細] ビューから、[詳細] をクリックし、メンテナンスモードオプションをオンにします。適切な管理者にエスカレートしてください。

セッションを復元する

セッションが切断されても、セッションはアクティブなままでアプリケーションは引き続き実行されますが、ユーザーデバイスはサーバーと通信しなくなります。

ユーザー詳細ビューで、**セッションの詳細**パネルのセッション障害をトラブルシューティングします。セッションIDで示される現在のセッションの詳細を表示できます。

アクション	説明
応答しないアプリケーションまたはプロセスを終了する	**アプリケーション**タブをクリックします。応答しないアプリケーションを選択し、**アプリケーションの終了**をクリックします。同様に、応答しない対応するプロセスを選択し、**プロセスの終了**をクリックします。また、CPUを使い物にならなくする可能性のある、異常に大量のメモリまたはCPUリソースを消費しているプロセスも終了します。
Windowsセッションを切断する	**セッション制御**をクリックし、**切断**を選択します。このオプションは、ブローカーされたマルチセッションOSマシンでのみ使用できま

アクション	説明
	す。ブローカーされていないセッションの場合、このオプションは無効になります。
ユーザーのセッションからログオフする	**セッション制御**をクリックし、**ログオフ**を選択します。

セッションをテストするには、ユーザーはセッションに再度ログオンを試みることができます。また、ユーザーをシャドウして、このセッションをより詳細に監視することもできます。

HDX™ チャネルシステムレポートを実行する

「**ユーザー詳細**」ビューで、「**HDX**」パネルにあるユーザーのマシン上のHDXチャネルのステータスを確認します。このパネルは、ユーザーマシンがHDXを使用して接続されている場合にのみ利用可能です。

情報が現在利用できないことを示すメッセージが表示された場合は、ページが更新されるまで1分間待つか、「**更新**」ボタンを選択してください。HDXデータは、他のデータよりも更新に少し時間がかかります。

詳細については、エラーまたは警告アイコンをクリックしてください。

> ヒント:
>
> タイトルバーの左隅にある左右の矢印をクリックすると、同じダイアログボックスで他のチャネルに関する情報を表示できます。
>
> HDXチャネルシステムレポートは、主にCitrixサポートによって、さらなるトラブルシューティングのために使用されます。

1. HDXパネルで、をクリックします。
2. .xmlレポートファイルを表示または保存できます。
    - .xmlファイルを表示するには、をクリックします。.xmlファイルは、Directorアプリケーションと同じウィンドウに表示されます。
    - .xmlファイルを保存するには、をクリックします。ウィンドウが表示され、Directorマシン上のファイルのダウンロード先を尋ねられます。

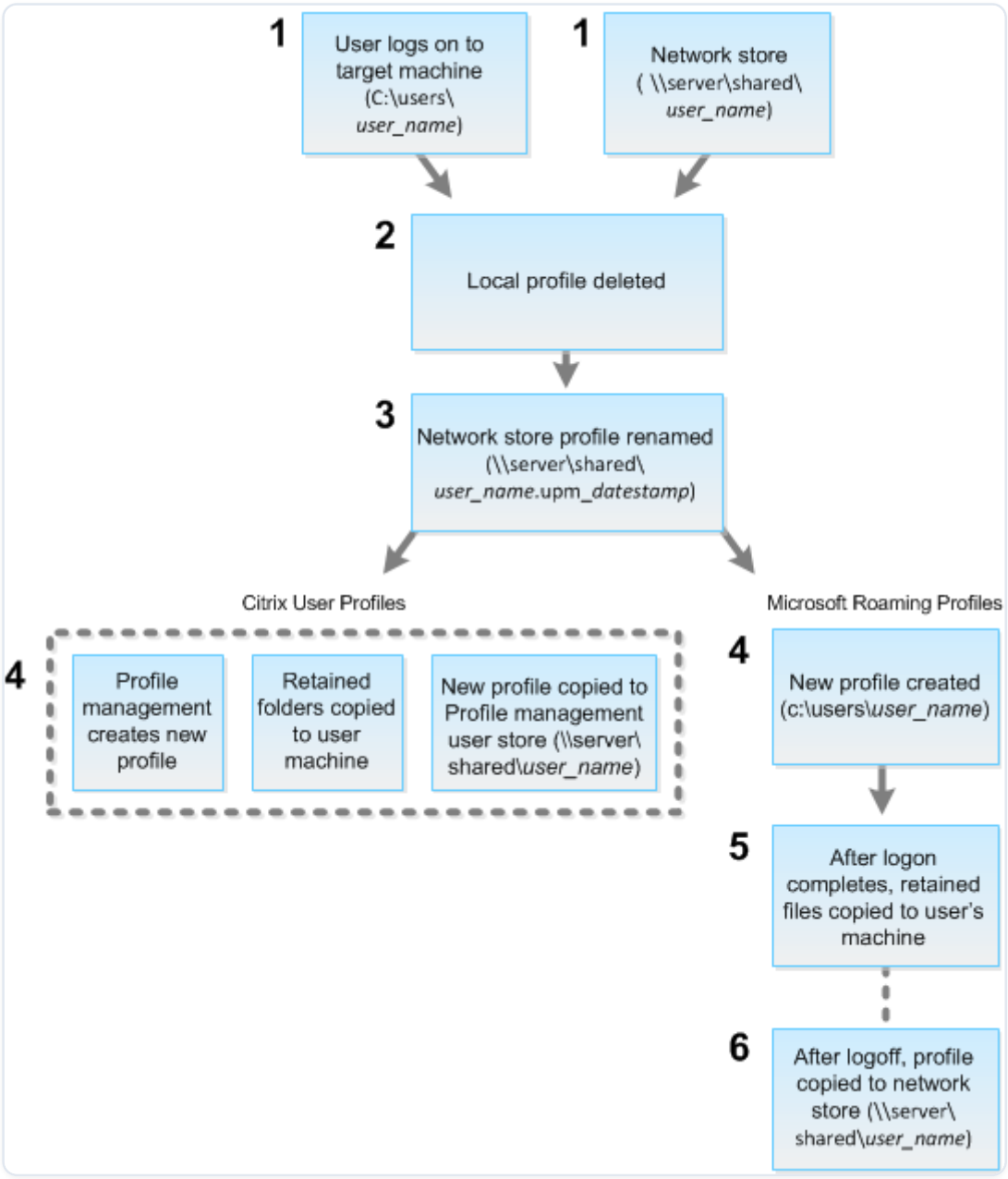
ユーザープロファイルをリセットする

> **注意:**
>
> プロファイルがリセットされると、ユーザーのフォルダーとファイルは保存され、新しいプロファイルにコピーされます。ただし、ほとんどのユーザープロファイルデータは失われます（たとえば、レジストリがリセットされ、アプリケーション設定が削除される可能性があります）。
>
> リセット機能は、ファイルベースとコンテナベースの両方のプロファイルソリューションに適用されます。

リセットされたプロファイルの処理方法

任意のCitrix®ユーザープロファイルまたはMicrosoftローミングプロファイルをリセットできます。ユーザーがログオフし、リセットコマンド（DirectorまたはPowerShell SDKを使用）を選択すると、Directorはまず使用中のユーザープロファイルを識別し、適切なリセットコマンドを発行します。Directorは、プロファイルサイズ、種類、ログオン時間などの情報をProfile Managementを通じて受け取ります。

この図は、ユーザープロファイルがリセットされた後のユーザーログオンプロセスを示しています。



Directorによって発行されたリセットコマンドは、プロファイルの種類を指定します。その後、Profile Managementサービスはその種類のプロファイルをリセットしようとし、適切なネットワーク共有（ユーザーストア）を探します。ユーザーがProfile Managementによって処理されているにもかかわらず、ローミングプロファイルコマンドを受け取った場合、それは拒否されます（またはその逆も同様です）。

1. ローカルプロファイルが存在する場合、それは削除されます。
2. ネットワークプロファイルの名前が変更されます。
3. 次のアクションは、リセットされるプロファイルがCitrixユーザープロファイルかMicrosoftローミングプロファイルかによって異なります。

Citrixユーザープロファイルの場合、新しいプロファイルはProfile Managementのインポートルールを使用して作成されます。フォルダーはネットワークプロファイルにコピーされ、ユーザーは通常どおりログオンできます。リセットにローミングプロファイルが使用される場合、ローミングプロファイル内のレジストリ設定はリセットされたプロファイルに保持されます。必要に応じて、テンプレートプロファイルがローミングプロファイルを上書きするようにProfile Managementを構成できます。

Microsoftローミングプロファイルの場合、Windowsはプロファイルを作成し、ユーザーがログオンすると、フォルダーはユーザーデバイスにコピーされます。ユーザーが再度ログオフすると、新しいプロファイルはネットワークストアにコピーされます。

Directorでユーザープロファイルをリセットするには

Citrix Virtual Desktops™ (Desktop VDA) を使用している場合は、次の操作を行います。

1. **Director** で、プロファイルをリセットするユーザーを検索し、そのユーザーのセッションを選択します。
2. をクリックします。
3. ユーザーにすべてのセッションからログオフするよう指示します。
4. ユーザーに再度ログオンするよう指示します。 ユーザーのプロファイルから保存されたフォルダーとファイルは、新しいプロファイルにコピーされます。

Citrix Virtual Desktops (Server VDA) を使用している場合、プロファイルのリセットを実行するにはログオンしている必要があります。その後、ユーザーはログオフし、再度ログオンしてプロファイルのリセットを完了する必要があります。

重要:

ユーザーが複数のプラットフォーム（Windows 8 や Windows 7 など）でプロファイルを持っている場合は、ユーザーが問題として報告したのと同じデスクトップまたはアプリに最初に再度ログオンするよう指示します。このログオン操作により、正しいプロファイルがリセットされます。プロファイルがCitrixユーザープロファイルである場合、ユーザーのデスクトップが表示されるまでにプロファイルはすでにリセットされています。プロファイルがMicrosoftローミングプロファイルである場合、フォルダーの復元が短時間進行中の可能性があります。ユーザーは、復元が完了するまでログオンしたままにする必要があります。

> プロファイルが正常にリセットされない場合（たとえば、ユーザーがマシンに正常に再度ログオンできない、または一部のファイルが欠落している場合）、元のプロファイルを手動で復元する必要があります。

次の点に注意してください。

- ユーザープロファイルソリューションとしてユーザーストアが有効になっている場合、新しいプロファイルには元のユーザープロファイルから次の個人用フォルダーが含まれます。
  - デスクトップ
  - クッキー
  - お気に入り
  - ドキュメント
  - ピクチャ
  - ミュージック
  - ビデオ
- Citrix Profile Managementバージョン2407以降では、プロファイルコンテナがユーザープロファイルソリューション全体として有効になっている場合、新しいプロファイルは以前の個人用フォルダーを保持します。
- Windows 8以降では、プロファイルがリセットされると、Cookieは新しいプロファイルにコピーされません。

リセットに失敗したプロファイルを手動で復元するには

1. ユーザーにすべてのセッションからログオフするよう指示します。
2. ローカルプロファイルが存在する場合は削除します。
3. ネットワーク共有上で、フォルダー名に日付と時刻が付加されたアーカイブフォルダー（.upm_datestamp拡張子を持つフォルダー）を見つけます。
4. 現在のプロファイル名（upm_datestamp拡張子のないもの）を削除します。
5. アーカイブされたフォルダーを元のプロファイル名にリネームします。つまり、日付と時刻の拡張子を削除します。これにより、プロファイルはリセット前の元の状態に戻ります。

PowerShell SDKを使用してプロファイルをリセットするには

Broker PowerShell SDKを使用してプロファイルをリセットできます。

NEW-BROKERMACHINECOMMAND

特定のユーザー、セッション、またはマシンへの配信のためにキューに入れられたコマンドを作成します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerMachineCommand/>`を参照してください。

例

プロファイルをリセットするためのPowerShellコマンドレットの使用方法の詳細については、以下の例を参照してください。

Profile Managementプロファイルをリセットする

- user1のプロファイルをリセットするとします。New-BrokerMachineCommand PowerShellコマンドを使用します。例：
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetUpmProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

> **重要：**
>
> `CommandData $byteArray`は次の形式である必要があります：`<SID>[,<backup path>]`。バックアップパスを指定しない場合、Profile Managementは現在の日時で名前が付けられたバックアップフォルダーを生成します。

Windowsローミングプロファイルをリセットする

- user1のローミングプロファイルをリセットするとします。New-BrokerMachineCommand PowerShellコマンドを使用します。例：
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetRoamingProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

セッションの録画

Directorの**ユーザー詳細**画面と**マシン詳細**画面にあるセッション録画コントロールを使用して、ICA®セッションを録画できます。この機能は、**Premium**サイトのお客様にご利用いただけます。

動的セッション録画

ユーザー詳細画面にあるセッション録画コントロールを使用して、現在アクティブなセッションを録画できます。動的セッション録画について詳しくは、セッション録画サービスの記事を参照してください。

ポリシーベースのセッション録画

DirectorConfigツールを使用してDirectorでポリシーベースのセッション録画を構成するには、セッション録画ポリシーの構成の「**Directorでセッション録画サーバーを使用するように構成する**」セクションを参照してください。 セッション録画コントロールは、ログインしているユーザーがセッション録画ポリシーを変更する権限を持っている場合にのみDirectorで利用できます。この権限は、ユーザーの承認で説明されているように、セッション録画承認コンソールで設定できます。

> **注:**
>
> Directorまたはセッション録画ポリシーコンソールを通じてセッション録画設定に加えられた変更は、以降のICAセッションから有効になります。

Directorのセッション録画コントロール

ユーザー詳細 > **セッション録画**アクションを使用して、現在または以降のセッションを録画できます。

- 動的セッション録画をオンにする - 現在のセッションが録画されます。
- オンにする（通知あり） - 以降のセッションが録画され、ICAセッションにログオンする際に、セッションが録画されていることがユーザーに通知されます。
- オンにする（通知なし） - 以降のセッションが録画され、ユーザーに通知することなく、セッションがサイレントで録画されます。
- オフにする - ユーザーのセッション録画を無効にします。

ポリシーパネルには、アクティブなセッション録画ポリシーの名前が表示されます。

「ユーザーの詳細 - セッション録画」(/en-us/citrix-virtual-apps-desktops/2511/media/dir-session-recording-userdetails.png)

「**マシン詳細**」パネルには、そのマシンに対するセッション録画ポリシーのステータスが表示されます。

ライブセッションと録画済みセッションを再生する

録画済みおよびライブのユーザーセッションを再生して、ユーザーが遭遇した問題を理解できます。Directorコンソール内で録画とセッション関連のメトリックにすぐにアクセスできるため、複数のセッション録画サーバーで録画を検索したり、録画を表示するためのサードパーティ製アプリを探したりする必要がなくなります。これにより、録画で発見された問題とパフォーマンスメトリックを関連付けるのに役立ちます。

この機能には、以下が必要です。

- VDAとセッション録画サーバーはバージョン2308以降であること。
- Delivery Controller™とDirectorはバージョン2311以降であること。

Directorはセッション録画を一元的なリポジトリに保存します。ユーザーに属する録画のリストは、「**セッションセレクター**」モーダル > 「**録画のあるセッション**」リンクをクリックすると表示されます。

「セッション録画 - 再生」(/en-us/citrix-virtual-apps-desktops/2511/media/dir-sr-playback1.png)

過去24時間または過去2日間にアクティブだったセッションの録画を表示することを選択できます。現在アクティブなセッションのライブ録画は、**セッション終了時刻**が「**実行中**」と表示されます。

「セッション録画 - 再生」(/en-us/citrix-virtual-apps-desktops/2511/media/dir-sr-playback2.png)

「**表示**」リンクをクリックすると、Citrix Session Recording再生サーバーを使用して新しいタブで録画を再生できます。

ハイブリッドマルチクラウド展開のための統合検索

以前は、トリアージ中にDirectorでユーザーを検索すると、そのユーザーがオンプレミスサイトからのものである場合にのみ、ユーザーの詳細が表示されました。ユーザーがクラウドサイトからのものである場合は、Monitorに移動して再度検索する必要がありました。

この強化された検索機能により、Directorの**検索**オプションを使用して、クラウドサイトまたはオンプレミスサイトのユーザーを検索できます。この機能は、ハイブリッド展開（クラウドサイトとオンプレミスサイトの両方）を使用している場合や、トリアージ目的でDirectorを使用している場合に利用できます。オンプレミスサイトかクラウドサイトかに関わらず、ユーザーの詳細を取得できます。サイトがDirectorに存在する場合、選択したセッションのActivity ManagerにDirector内で直接移動できます。サイトがDirectorに存在しない場合、選択したセッションのActivity ManagerにMonitor内で直接移動できます。その後、トリアージを続行できます。

> **注:**
>
> Citrix Directorを介して統合検索コンソールを使用できます。
>
> この機能により、問題解決までの平均時間が短縮され、クラウドユーザーとオンプレミスユーザーの両方に単一のコンソールでシームレスなエクスペリエンスを提供します。追加の利点として、Directorにはクラウドサイトの詳細のみが追加されるため、データベースのサイズが急速に増大することはありません。ユーザーの詳細はクラウド自体に保存されます。

> **注:**
>
> 最大6つ以下のクラウドサイトの場合、3秒以内に検索結果を取得できます。
>
> この機能を有効にするには、クラウドサイトをDirectorに接続する必要があります。

Directorへのクラウドサイトの接続

前提条件

Citrix Directorで統合検索を構成するために、新しいコンポーネントをインストールする必要はありません。次の要件が満たされていることを確認してください。

- 統合検索の場合、すべてのDelivery ControllerおよびDirectorがインストールされているマシンで、アウトバウンドインターネットアクセスが利用可能であること。具体的には、次のURLへのアクセスが可能であることを確認してください。
  - Citrix キー登録: `<https://*.citrixnetworkapi.net/>`
  - シトリックスクラウド: `<https://*.citrixworkspacesapi.net/>`
  - シトリックス DaaS: `<https://*.cloud.com/>`
  - マイクロソフト Azure: `<https://*.windows.net/>`
- Delivery ControllerとDirectorマシンがイントラネット内にあり、アウトバウンドインターネットアクセスがプロキシサーバー経由である場合は、以下を確認してください。
  - プロキシサーバーは、上記のURLリストを許可する必要があります。

- Directorの**web.config**ファイルと**citrix.monitor.exe.config**ファイルに以下の構成を追加します。この構成は**configuration**タグ内に必ず追加してください。

```
<system.net>

    <defaultProxy>

        <proxy usesystemdefault="false" proxyaddress="http://
<your_proxyserver_address>:80" bypassonlocal="true" />

    </defaultProxy>

</system.net>
```

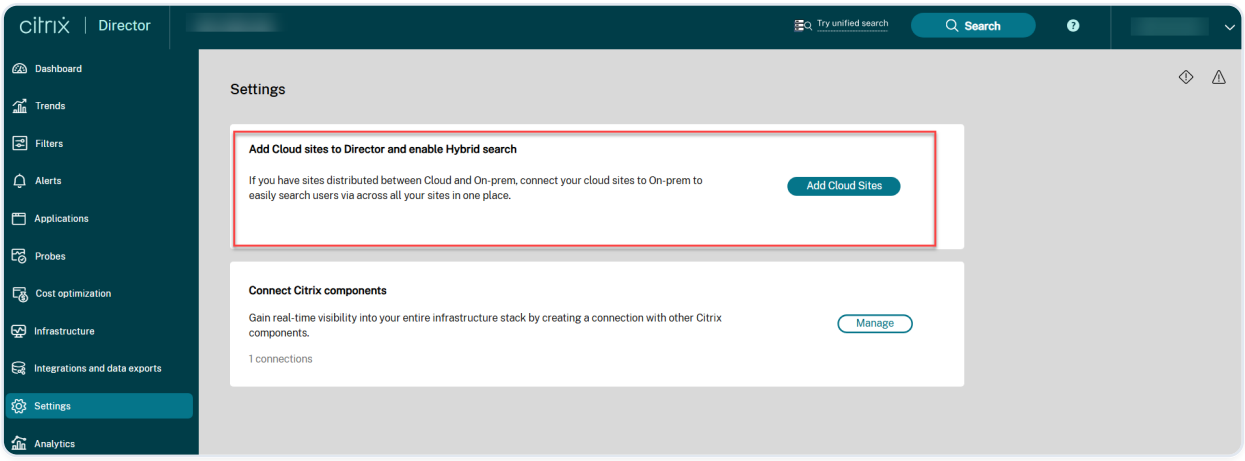
- Directorの**web.config**は、Directorがインストールされているマシンの`C:\inetpub\wwwroot\Director\web.config`にあります。
- **citrix.monitor.exe.config**は、Delivery Controllerがインストールされているマシンの`C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config`にあります。

この設定は、IIS上のMicrosoftによって提供されます。詳細については、「プロキシ構成」を参照してください。構成ファイルの**defaultproxy**フィールドは、Directorおよび監視サービスのアウトバウンドアクセスを制御します。Citrix DaaSとの構成および通信には、**defaultproxy**フィールドをtrueに設定する必要があります。有効なポリシーによってこのフィールドがfalseに設定されている可能性があります。この場合、手動でフィールドをtrueに設定する必要があります。変更を行う前に、構成ファイルのバックアップを取ってください。変更を反映させるには、Delivery Controllerで監視サービスを再起動してください。

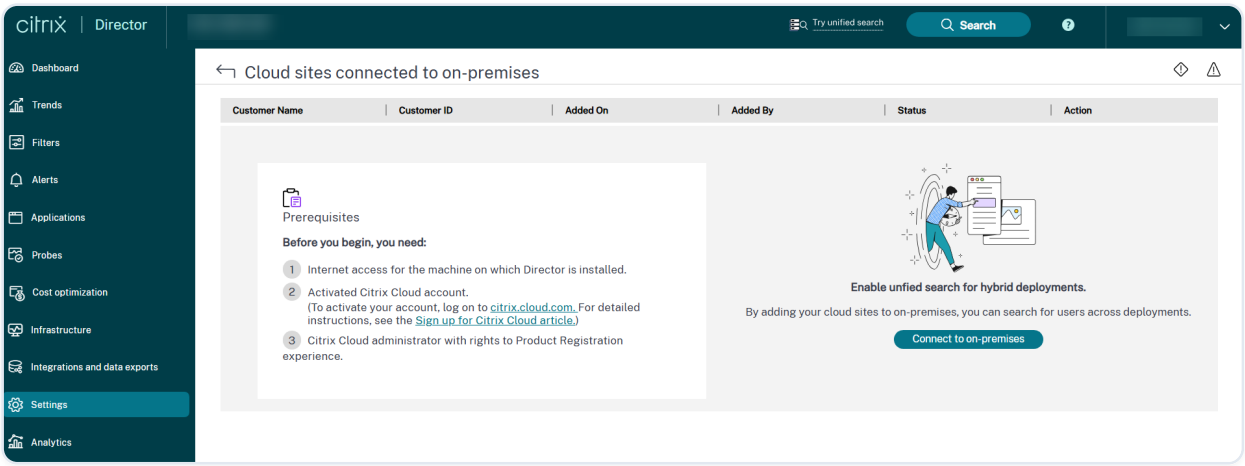
- DaaSのCitrix Cloud™エンタイトルメントがアクティブであること。
- Citrix Cloudアカウントが、製品登録エクスペリエンスに対する権限を持つ管理者アカウントであること。管理者権限の詳細については、「管理者権限の変更」を参照してください。
- Citrix Directorがインストールされているマシンにインターネットアクセスがあることを確認してください。
- Citrix Cloudサービスを使用するには、HTTPSポート443を介して必要なCitrixアドレスに接続できる必要があります。詳細については、「インターネット接続要件」を参照してください。
- 製品登録を実行するための完全な管理者アクセス権があることを確認してください。

構成手順

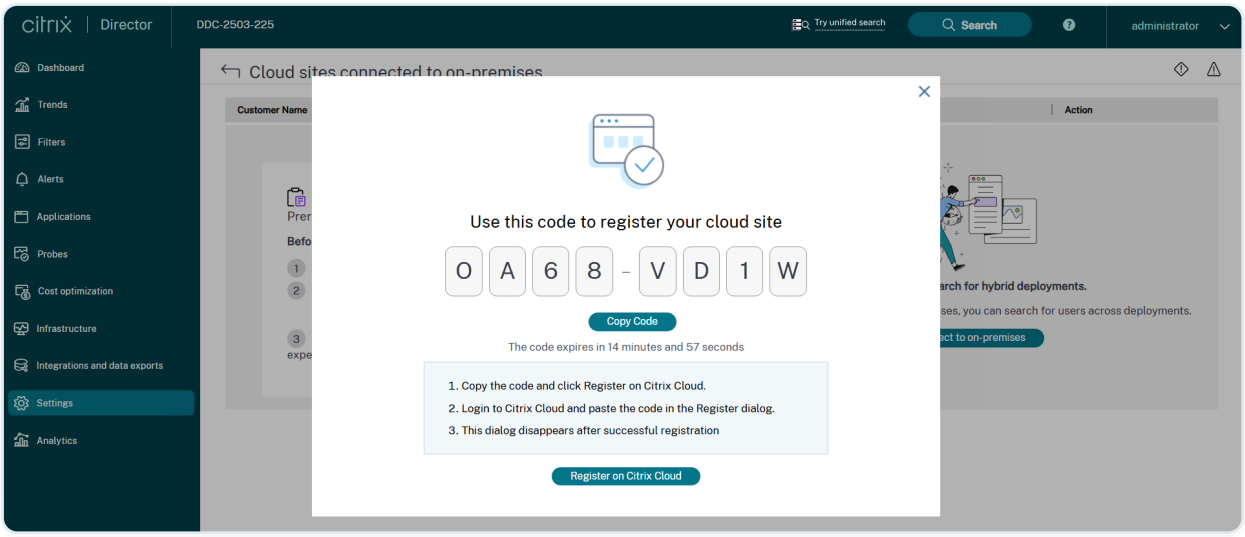
1. Directorにフル管理者としてサインインします。Directorダッシュボードページが表示されます。
2. 「**設定**」タブをクリックします。「**設定**」ページが表示されます。



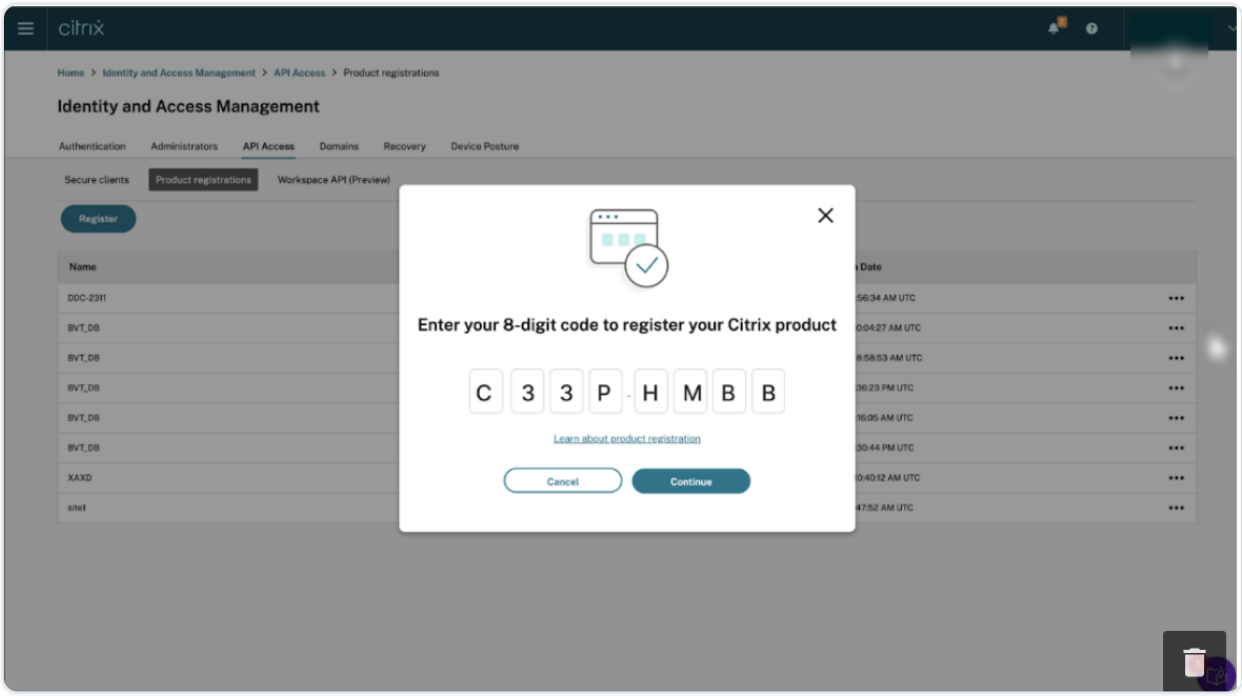
3. **クラウドサイトの追加**をクリックします。次のページが表示されます。



4. 前提条件を確認し、「**クラウドサイトの接続**」をクリックして構成プロセスを開始します。Citrix Cloudにこのサイトを登録するために、一意の8桁の登録コードが生成されます。



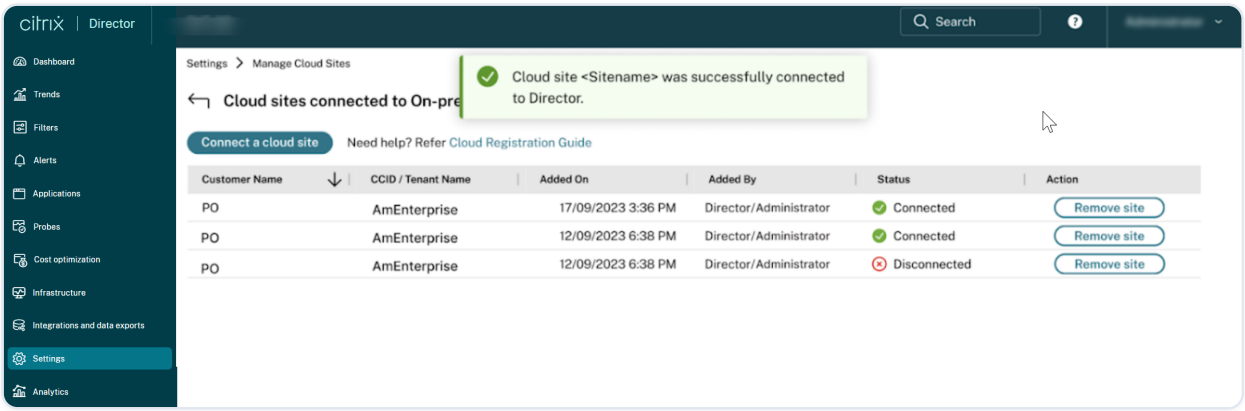
5. 「**コードのコピー**」をクリックしてコードをコピーし、「**Citrix Cloudで登録**」をクリックします。Citrix Cloudの登録URLにリダイレクトされます。
6. Citrix Cloudの資格情報でサインインし、顧客を選択します。
7. コピーした登録コードをCitrix Cloudの **Product Registrations** ページに貼り付けます。**Continue** をクリックしてサイトを登録します。



8. **Continue** をクリックします。クラウドサイトがCitrix Directorに登録され、次のメッセージが表示されます。

   統合検索登録の成功(/en-us/citrix-virtual-apps-desktops/2511/media/unified-search-reg-success.png)

9. **Close** をクリックします。次の画面が表示されます。



10. Directorで複数のクラウドサイトを構成するには、Directorから各サイトに対して前述の構成手順を繰り返します。

    サイトごとに複数のDirectorインスタンスが実行されている場合は、いずれか1つのDirectorインスタンスから構成します。サイトに接続されている他のすべてのDirectorインスタンスは、構成プロセス後の次回の更新時に更新されます。

> **注:**
>
> サイトをCitrix Directorから切断するには、**Remove site** をクリックします。このオプションは既存の構成を削除します。

ハイブリッド展開からのユーザー検索

ユーザーを検索するには、次の手順を実行します。

1. 上部のナビゲーションバーで「**検索**」をクリックします。「**展開の監視とトラブルシューティング**」ページが表示されます。

   統合検索サイト(/en-us/citrix-virtual-apps-desktops/2511/media/unified-search-site.png)

2. ドロップダウンリストから「**ユーザー**」を選択し、ユーザー名を入力します。オンプレミスおよびクラウド展開からのアクティブなセッションと失敗したセッションのリストが表示されます。

   統合検索 - 完了(/en-us/citrix-virtual-apps-desktops/2511/media/unified-search-done.png)

3. 検査するセッションを選択します。

- クラウド展開を使用しているセッションの場合、ユーザーコンテキストを含む関連するDaaS Monitor URLが「**アクティビティマネージャー**」ページに開き、すばやくトラブルシューティングを開始できます。

- オンプレミス展開を使用しているセッションの場合、アクティビティマネージャーページがすぐに開き、トラブルシューティングを開始できます。

インフラストラクチャ監視

Directorは、Citrix Virtual Apps and Desktops™コンポーネントの稼働状況を可視化する機能を提供するようになりました。この機能は、インフラストラクチャに関連する問題を簡単に特定し、トラブルシューティングし、解決するのに役立ちます。現在、以下のコンポーネントの健全性が監視されています。

- デリバリーコントローラー™
- シトリックス プロビジョニング™ サービス
- StoreFront™

この機能をサポートするために、Citrixコンポーネント向けに`citrixinframonitor.msi`という新しいWindows実行可能ファイルが導入されました。これにより、Provisioning ServiceまたはStoreFrontサーバーからDirectorへの関連する健全性メトリックの収集と送信が容易になります。ただし、Delivery Controllerの監視には`CitrixInfraMonitor.msi`は必要ありません。Delivery Controllerコンポーネントは、Citrix Virtual Apps and Desktopsサイトに接続されると、監視のために自動的にオンボーディングされます。

この機能は、Directorの単一ダッシュボードで、Delivery Controller、Provisioning Service、およびStoreFrontサーバーに関する重要な監視データセットとプロアクティブなアラートを取得するのに役立ちます。最新の情報を確保するため、監視対象コンポーネントから5分ごとにデータが収集されます。

この機能は、プロアクティブな監視、詳細なメトリック、および自動アラートを提供することで運用効率を向上させ、Citrix®インフラストラクチャがスムーズかつ効率的に稼働することを保証することを目的としています。

主な機能

リアルタイム監視:

- Delivery Controller、Citrix Provisioning (Provisioning Service) サーバー、StoreFront などのCitrix インフラストラクチャコンポーネントの継続的な監視。
- システムの健全性、リソース使用率、および関連するパフォーマンスメトリックを表示するダッシュボードビュー。

詳細な分析:

- 各コンポーネントの接続ステータス、サービスまたはプロセスステータスなどのシステム健全性メトリックに関する詳細な分析を提供します。
- CPU、メモリ、ディスク使用率などのリソース使用率メトリックの詳細。

自動アラートと通知:

- さまざまなメトリックと状態に対して、きめ細かなスコープでカスタマイズ可能なアラートしきい値。
- メールとWebhookによるリアルタイム通知。

ユースケース

運用効率:

Citrix管理チームがCitrixサーバーとサービスの高可用性とパフォーマンスを維持できるようにします。この機能は、重大なユーザーグループに影響を与える前に問題をプロアクティブに特定して管理者に警告することで、ダウンタイムを最小限に抑えるのにも役立ちます。

チケット解決の高速化:

サーバーの健全性とパフォーマンスに関する主要なメトリックを監視し、仮想アプリケーションとデスクトップのユーザーへの最適な配信を評価します。これらのメトリックを使用して、関連するコンポーネントを分析することで、パフォーマンスに関連するユーザーの苦情を診断し、解決します。

前提条件

- Citrix Virtual Apps™ and Desktopsバージョン2407以降
- Provisioning Serviceの前提条件またはStoreFrontの前提条件が満たされていることを確認してください。
- Citrix Provisioningの監視の場合：
  - **DB接続**と**ライセンスサーバー到達可能性**を監視するために必要な最小バージョンはCitrix Provisioning 2407です。
  - **PXEサービス**、**TFTPサービス**、および**合計再接続数**を監視するために必要な最小バージョンはCitrix Infra Monitor 2411です。
- Citrix Infrastructure Monitorを実行するために必要なユーザーアカウントまたは権限：
  - エンドポイントマシンにCitrix Infrastructure Monitorをインストールするための Windows管理者権限を持つユーザーアカウント。

- 次のDirector権限を持つフル管理者ユーザーアカウントまたはカスタムロール:
  - アラートポリシーの作成\編集\有効化\削除
  - アラートメールサーバー構成の作成\編集\削除
  - Citrixコンポーネントへの接続の作成\編集\管理 (インフラ監視)
  - アラートの解除
  - アラートポリシーの表示
  - アラートの表示
  - ダッシュボードページの表示
  - Infrastructure Monitorページの表示

注:

- 前述の前提条件は、Provisioning ServiceおよびStoreFrontコンポーネントの監視にのみ有効です。
- **アラート**ページにアクセスする権限がない場合、**インフラストラクチャ監視**ページで**アラートの管理**オプションが無効になります。

詳細については、以下を参照してください。

- インフラストラクチャ監視の概要
- 接続の管理
- インフラストラクチャダッシュボード
- 高度なアラートポリシー
- インフラストラクチャポリシー

インフラストラクチャ監視の概要

Citrix Infrastructure Monitorには、次の方法で接続できます。

- 手動接続 - Citrix Infrastructure Monitorサービスを手動でダウンロードしてインストールします。
- 自動接続 - UIがダウンロードとインストールを自動的に処理します。

手動接続と自動接続の両方を行った後、Citrix Infrastructure MonitorのHTTPSをオプションで構成できます。

詳細については、以下を参照してください。

- 手動接続
- 自動接続
- Citrix Infrastructure Monitor の HTTPS を構成する

接続の管理

「**Citrixコンポーネントの接続**」ページで、接続の表示、削除、または編集ができます。

接続の表示

このビューで利用可能な、接続済みおよび切断済みのすべてのコンポーネントの詳細を表示できます。次の表は、「**接続の作成**」ページのさまざまな列について説明しています。

列	説明
ホスト名	サーバーの名前。
種類	接続の種類。Delivery Controller™、Provisioning Service、およびStoreFrontです。
バージョン	コンポーネントにインストールされている `CitrixInfraMonitor.msi` のバージョン。このフィールドはDelivery Controllerには適用されません。
作成者	接続を作成したユーザーの名前。
作成日	接続が確立された日付。
最終更新	接続が最後に更新された日付。
状態	異なる状態は、接続中、接続済み、切断済みです。
	接続中: この状態は、新しいコンポーネントのデータが表示されるまでに約5分、リソース使用率データが利用可能になるまでに約10分かかることを示します。

列	説明
	接続済み: この状態は、コンポーネントとサイト間の接続が稼働中であることを示します。
	切断済み: この状態は、コンポーネントとサイト間の接続が切断されていることを示します。切断状態の考えられる理由としては、サーバーのダウンタイムや、サイトがCitrix Infrastructure Monitorに接続できないことなどが挙げられます。

> **注:**
>
> オンプレミスのCitrix Virtual Apps and Desktops™サイトに接続されている場合、Delivery Controllerの接続はこのビューに自動的に入力されます。

接続の編集

Provisioning ServiceまたはStoreFront™接続を確立するために使用される管理者資格情報を更新するには、接続の編集が必要になる場合があります。

既存の接続を編集するには、次の手順を実行します。

1. **設定**タブまたは**インフラストラクチャ**タブから「**Citrixコンポーネントの接続**」ページに移動します。
2. 接続リストテーブルで、目的のコンポーネントの行の末尾にある3つの点をクリックします。
3. **編集**をクリックし、必要に応じて詳細を更新します。

コンポーネントを削除する

Director UIから、またはPowerShellコマンドを使用して、コンポーネントを削除できます。

Director UIの使用

コンポーネントの削除とは、DirectorからProvisioning ServiceまたはStoreFront接続を登録解除するプロセスです。登録解除プロセスが完了すると、選択したコンポーネントの新しいデータ収集は停止します。既存の接続を削除するには：

1. **設定**タブまたは**インフラストラクチャ**タブから「**Citrixコンポーネントの接続**」ページに移動します。

2. 接続リストテーブルで、目的のコンポーネントの行の末尾にある3つの点をクリックします。
3. 「**削除**」をクリックします。接続は登録解除され、Director から削除されます。

PowerShell SDK の使用

特定のコンポーネントの登録を解除する必要がある場合は、Delivery Controller で次の PowerShell コマンドを実行します。

```
Remove-MonitorDirectorAgent -Fqdn <FQDN of component> -Component
<component>
```

Citrix Infrastructure Monitorの登録を削除するコマンドの例を次に示します。

```
Remove-MonitorDirectorAgent -Component PVS -Fqdn [redacted]
```

> **注：**
>
> コンポーネントの登録を解除すると、特定のコンポーネントからDirectorへのデータフローが停止するだけです。Citrix Infrastructure Monitorをアンインストールする必要がある場合は、**コントロールパネル**からアンインストールしてください。

インフラストラクチャダッシュボード

コンポーネントの正常性値は、**Infrastructure Monitoring**ページで確認できます。これらの結果は、インフラストラクチャに関する問題をプロアクティブに分析し、トラブルシューティングするのに役立ちます。

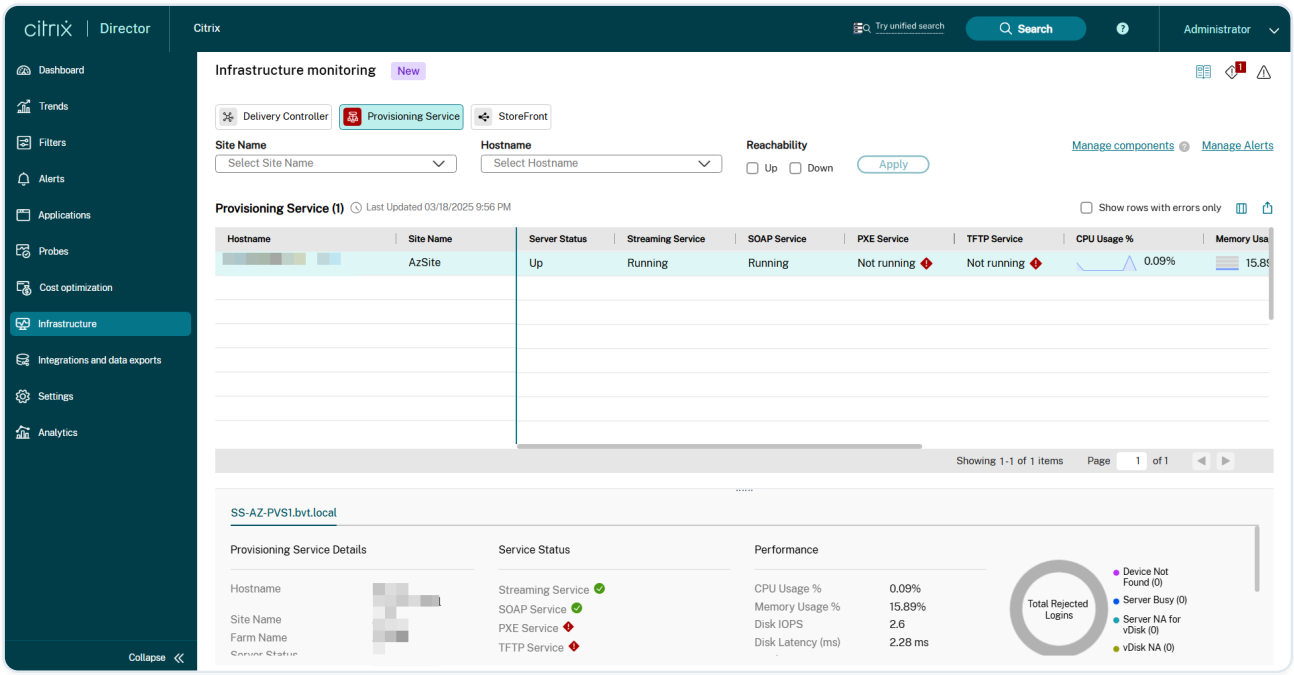
Infrastructure Monitoringページは、以下でフィルタリングできます。

- ホスト名 - ホスト名を選択します
- 到達可能性 - **Up**（サーバーに到達可能）または**Down**（サーバーに到達不能）チェックボックスを選択します
- エラー - 「Show rows with errors only」チェックボックスを選択します。

Manage columnsオプションを使用して、ダッシュボードに表示するデータを選択します。

Provisioning Serviceの正常性メトリック

Infrastructureタブをクリックし、**Provisioning Service**を選択します。Provisioning Serviceのインフラストラクチャダッシュボードが表示されます。



Provisioning Serviceサーバーについては、以下の詳細が監視されます。

カテゴリ	メトリック	説明
到達可能性	ホスト名	Citrix Infrastructure Monitor がインストールされている Provisioning Service マシンの名前。このメトリックは文字列値です。
	Provisioning Service サイト名	Provisioning Service サイトの名前。このメトリックは文字列値です。
	Provisioning Service ファーム名	Provisioning Service ファームの名前。このメトリックは文字列値です。
	プロビジョニングサービス サイト ID	Provisioning Service サーバーのサイト ID を表示します。このメトリックは文字列値です。
	プロビジョニングサービス ファーム ID	Provisioning Service サーバーのファーム ID を表示します。このメトリックは文字列値です。

カテゴリ	メトリック	説明
	サーバーの状態	指定されたサーバーの到達可能性の状態を表示します。可能な値は、*Up*、*Down*、*Unknown* です。
	最終起動時刻	Provisioning Service サーバーが最後に起動された時刻を表示します。
	最終更新	Provisioning Service サーバーからデータが収集された時刻を表示します。
依存サービス	ストリーミングサービス	ストリーミングサービスのステータスを表示します。このメトリックは、Windows サービスのステータスを示します。可能な値は、*Not running*、*Running*、*Not Installed*、*n/a* (ヘルプアイコン付き) です。
	SOAP サービス	Simple Object Access Protocol (SOAP) サービスのステータスを表示します。このメトリックは、Windows サービスのステータスを示します。可能な値は、*Not running*、*Running*、*Not Installed*、*n/a* (ヘルプアイコン付き) です。
	DB接続	データベース接続のステータスを表示します。Citrix Provisioningサーバーバージョン2402以前を使用している場合、不明なエラーが発生する可能性があります。可能な値は、*未接続*、*接続済み*、*不明*、および*該当なし*（ヘルプアイコン付き）です。

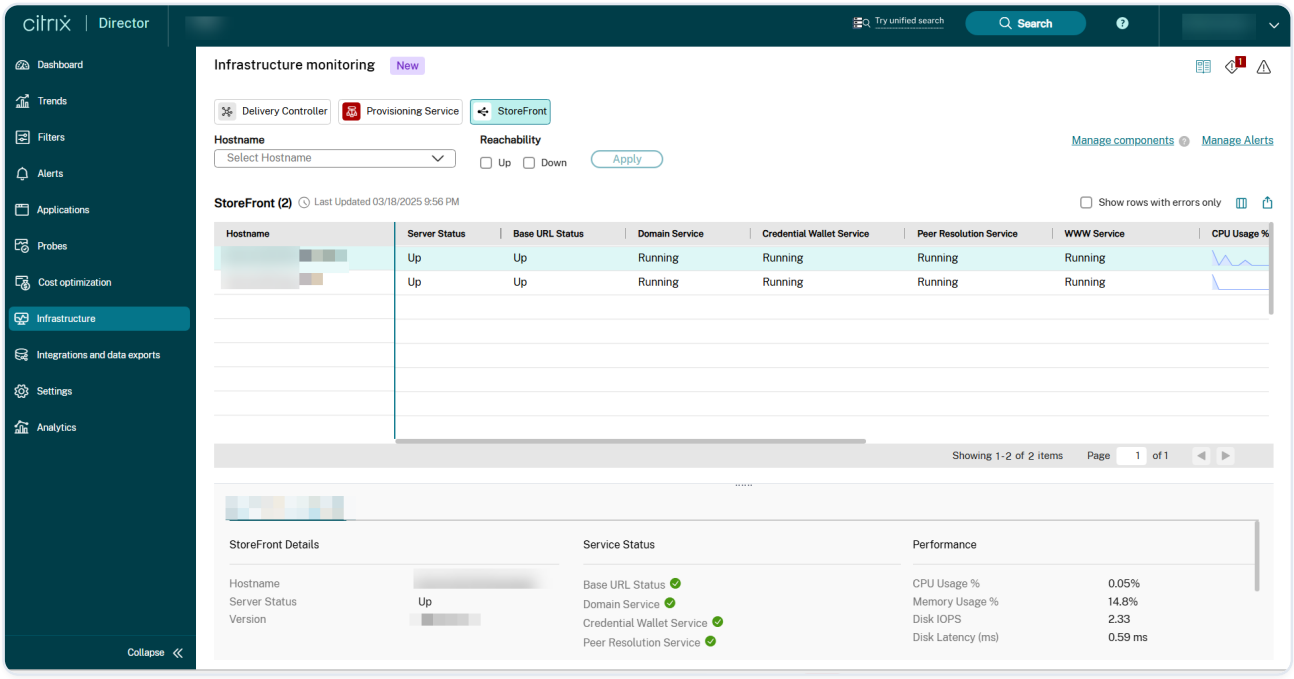
カテゴリ	メトリック	説明
	ライセンスサーバー到達可能性	ライセンスサーバーが到達可能かどうかを表示します。Citrix Provisioningサーバーバージョン2402以前を使用している場合、不明なエラーが発生する可能性があります。可能な値は、*未接続*、*接続済み*、*不明*、および*該当なし*（ヘルプアイコン付き）です。
	再接続合計回数	セッションが再接続された回数を表示します。
	PXEサービス	Preboot Execution Environmentサービスのステータスを表示します。このメトリックはWindowsサービスのステータスを示します。可能な値は、*実行中ではない*、*実行中*、*インストールされていない*、および*該当なし*（ヘルプアイコン付き）です。
	TFTPサービス	Trivial File Transfer Protocolサービスのステータスを表示します。このメトリックはWindowsサービスのステータスを示します。可能な値は、*実行中ではない*、*実行中*、*インストールされていない*、および*該当なし*（ヘルプアイコン付き）です。
リソース使用率	CPU使用率 %	CPU使用率を折れ線グラフで表示します。表示される値は、過去5分間の終わりの最新の値です。

カテゴリ	メトリック	説明
	平均CPU使用率 %	過去10分間に集計されたProvisioning Serviceサーバーの平均CPU使用率を表示します。
	ピークCPU使用率 %	過去5分間のProvisioning Serviceサーバーのピーク CPU使用率を表示します。
	メモリ使用率 %	メモリ使用率を積み上げグラフで表示します。表示される値は、過去5分間の終わりの最新の値です。
	平均メモリ使用率 %	過去10分間に集計されたProvisioning Serviceサーバーの平均メモリ使用率を表示します。
	ピークメモリ %	過去5分間のProvisioning Serviceサーバーのピークメモリ使用率を表示します。
	ディスク IOPS	ディスクの入出力値を折れ線グラフで表示します。
	平均ディスク IOPS %	過去10分間に集計されたProvisioning Serviceサーバーの平均ディスクIOPSを表示します。
	ピークディスク IOPS %	過去10分間のProvisioning Serviceサーバーのピークディスク IOPS 使用率を表示します。
	ディスクレイテンシー (ミリ秒)	ディスクのレイテンシー値を折れ線グラフで表示します。
	平均ディスク待機時間 %	過去10分間に集計されたProvisioning Serviceサーバー

カテゴリ	メトリック	説明
		の平均ディスク待機時間を表示します。
	ピークディスク待機時間 %	過去5分間のProvisioning Serviceサーバーのピークディスク待機時間の割合を表示します。
影響	拒否されたログインの合計	失敗したログインの合計数を、ログイン試行の合計数で割った値。
	アクティブなデバイス数	Provisioning Serviceサーバー内のアクティブなデバイスの総数を表示します。このメトリックは整数値です。

StoreFront™の健全性メトリック

インフラストラクチャタブをクリックし、**StoreFront**を選択します。StoreFrontのインフラストラクチャダッシュボードが表示されます。



StoreFrontサーバーについては、以下の詳細が監視されます。

カテゴリ	メトリック	説明
到達可能性	ホスト名	StoreFrontサーバーの名前を表示します。このメトリックは文字列値です。
	サーバーの状態	StoreFrontサーバーの状態を表示します。このメトリックはWindowsサービスのステータスを示します。可能な値は、*実行中ではない*、*実行中*、*インストールされていない*、および*該当なし*（ヘルプアイコン付き）です。
	ベースURLの状態	ベースURLの健全性を表示します。HTTPステータスコードが200の場合、ステータスはUPです。それ以外の場合、値はDownです。
	最終起動時刻	StoreFrontサーバーが最後に起動された時刻を表示します。
	最終更新	StoreFrontサーバーからデータが収集された時刻を表示します。
依存サービス	ドメインサービス	ドメインサービスという名前のWindowsサービスの正常性。このメトリックは、Windowsサービスのステータスを示します。可能な値は、*実行していません*、*実行中*、*インストールされていません*、および *n/a* (ヘルプアイコン付き) です。
	資格情報ウォレットサービス	このサービスは、暗号化されたパスワードを保存するために使用されるWindowsサービスです。可能な値は、*実行し*

カテゴリ	メトリック	説明
		ていません、*実行中*、*インストールされていません*、および *n/a* (ヘルプアイコン付き) です。
	ピア解決サービス	このサービスは、StoreFrontサーバーのピアメッシュを形成するサーバー間グループネットワーク通信を担当するWindowsサービスです。可能な値は、*実行していません*、*実行中*、*インストールされていません*、および *n/a* (ヘルプアイコン付き) です。
	WWWサービス	このメトリックは、StoreFrontサーバーのWebサービスです。このメトリックは、Windowsサービスのステータスを示します。可能な値は、*実行していません*、*実行中*、*インストールされていません*、および *n/a* (ヘルプアイコン付き) です。
リソース使用率	CPU使用率 %	CPUの使用率を折れ線グラフでパーセンテージ表示します。表示される値は、過去5分間の終わり時点での最新の値です。
	平均CPU使用率 %	過去10分間にわたって集計されたStoreFrontサーバーの平均CPU使用率をパーセンテージで表示します。
	ピークCPU使用率 %	過去5分間のStoreFrontサーバーのピークCPU使用率をパーセンテージで表示します。この値は、CPUに必要な

カテゴリ	メトリック	説明
		最大容量を決定するのに役立ちます。
	メモリ使用率 %	メモリの使用率をスタックチャートでパーセンテージ表示します。表示される値は、過去5分間の終わり時点での最新の値です。
	平均メモリ使用率 %	過去10分間にわたって集計されたStoreFrontサーバーの平均メモリ使用率をパーセンテージで表示します。
	ピークメモリ使用率	過去5分間のStoreFrontサーバーのピークメモリ使用率を表示します。
	ディスクIOPS	折れ線グラフを使用して、ディスクの入出力値を表示します。
	平均ディスクIOPS %	浮動小数点数を使用して、StoreFrontサーバーの平均ディスクIOPSを表示します。
	ピークディスクIOPS %	過去10分間に集計されたStoreFrontサーバーのピークディスクIOPS使用率を表示します。
	ディスク待機時間 (ミリ秒)	折れ線グラフを使用して、ディスクの待機時間値を表示します。
	平均ディスク待機時間 %	過去10分間のStoreFrontサーバーの平均ディスク待機時間を表示します。

カテゴリ	メトリック	説明
	ピークディスク待機時間 %	過去5分間のStoreFrontサーバーのピークディスク待機時間の割合を表示します。
影響	ICA® 証明書の有効性	ICA証明書の有効性を表示します。可能な値は、*期限切れ*、*期限切れ間近*、*有効*、*見つかりません*です。
	ICA証明書チェーンの有効性	StoreFront ICA証明書チェーンが有効であるかどうかを表示します。可能な値は、*はい*または*いいえ*です。
	IIS証明書の有効性	IIS証明書の有効性を表示します。可能な値は、*期限切れ*、*期限切れ間近*、*有効*、*見つかりません*です。
	IIS証明書チェーンの有効性	StoreFront IIS証明書チェーンが有効かどうかを表示します。可能な値は *Yes* または *No* です。

Delivery Controller™のヘルス指標

Delivery Controllerコンポーネントは、インフラストラクチャ監視の一部としてデフォルトで追加されます。Citrix Virtual Apps and Desktops™サイトに接続されているDelivery Controllerコンポーネントは、監視のために自動的にオンボードされます。

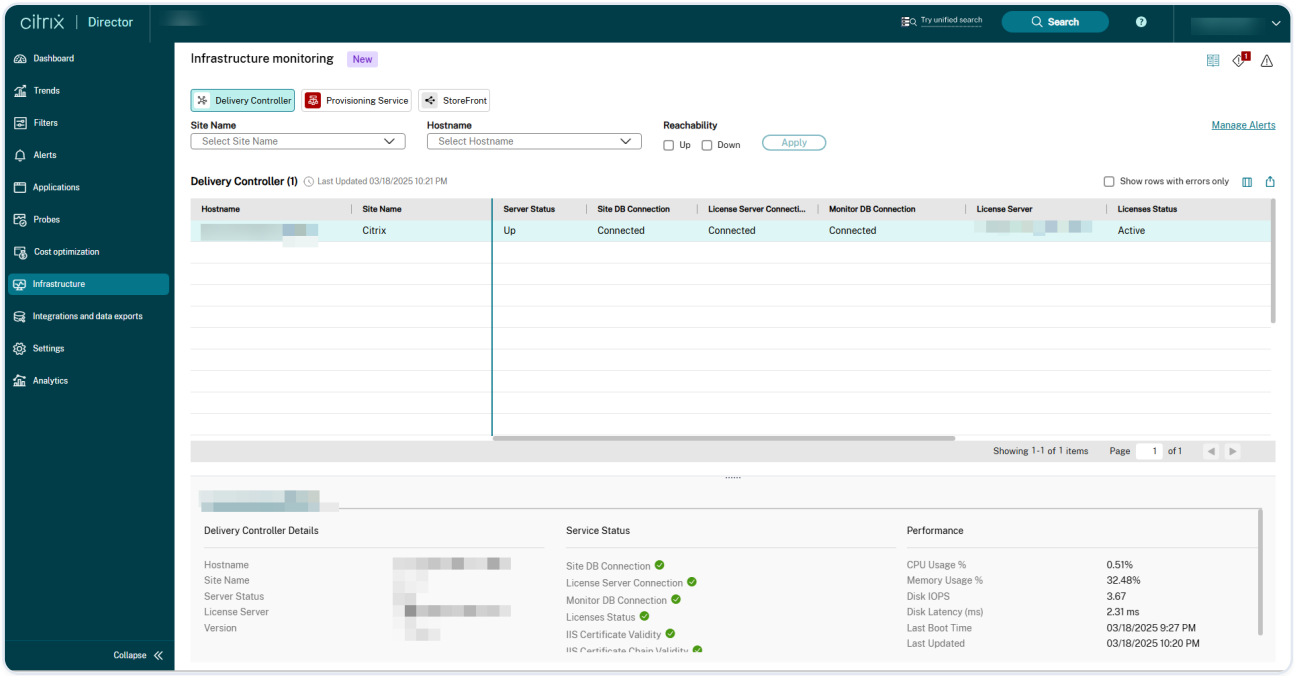
この機能により、お客様はインフラストラクチャ監視ダッシュボードでコントローラーの健全性を監視し、アラートを設定できます。アラート機能により、デリバリーコントローラー用に作成されたポリシーのいずれかがクリティカルまたは警告段階にある場合、顧客管理者にアラートが送信されます。

必要なサイト名を選択すると、選択したサイト名に応じて詳細が表示されます。*Up* または *Down* などの**到達可能性ステータス**も選択できます。

注： Delivery Controllerの監視には`CitrixInfraMonitor.msi`ファイルは不要です。

インフラストラクチャの詳細について、シングルサイトとマルチサイトの両方の詳細を監視できます。

インフラストラクチャタブをクリックし、**Delivery Controller**を選択します。Delivery Controllerのインフラストラクチャダッシュボードが表示されます。



Delivery Controllerでは、以下の詳細が監視されます。

カテゴリ	メトリック	説明
到達可能性	サーバーの状態	指定されたDelivery Controllerの到達可能性の状態を表示します。可能な値は*Up*と*Down*です。
	バージョン	Delivery Controllerのバージョン。
	最終起動時刻	Delivery Controllerが最後に起動された時刻を表示します。
	最終更新日時	Delivery Controllerからデータが収集された時刻を表示します。
依存サービス	サイトDB接続	サイトデータベース接続のステータスを表示します。可能な値は、*Not Connected*、

カテゴリ	メトリック	説明
		Connected、*Unknown*、および*n/a*（ヘルプアイコン付き）です。**Unknown:** この値は、メトリックが収集されていないか、利用できない場合に表示されます。**n/a:** 該当なし。この値は、サーバーのステータスがダウンしている場合に表示されます。
	ライセンスサーバー接続	ライセンスサーバー接続のステータスを表示します。可能な値は、*未接続*、*接続済み*、*不明*、および *n/a* (ヘルプアイコン付き) です。
	モニターDB接続	モニターデータベース接続のステータスを表示します。可能な値は、*未接続*、*接続済み*、*不明*、および *n/a* (ヘルプアイコン付き) です。
	ライセンスサーバー	ライセンスサーバーに到達可能かどうかを表示します。
	ライセンスステータス	ライセンスのステータスを表示します。
リソース使用率	CPU使用率 %	CPU使用率を折れ線グラフでパーセンテージ表示します。表示される値は、過去5分間の終わり時点での最新の値です。
	平均CPU使用率	Delivery Controllerサーバーの過去10分間の平均CPU使用率を表示します。
	ピークCPU使用率	Delivery Controllerサーバーの過去5分間のピークCPU使用率を表示します。

カテゴリ	メトリック	説明
	メモリ使用率	スタックチャートを使用してメモリ使用率をパーセンテージで表示します。表示される値は、過去5分間の終わりにおける最新の値です。
	平均メモリ使用率	Delivery Controllerサーバーの過去10分間の平均メモリ使用率を表示します。
	ピークメモリ使用率	Delivery Controllerサーバーの過去5分間のピークメモリ使用率を表示します。
	ディスク IOPS	ディスクの入出力値を折れ線グラフで表示します。
	平均ディスク IOPS %	過去10分間のDelivery Controllerサーバーの平均ディスクIOPSを集計して表示します。
	ピークディスク IOPS %	過去10分間のDelivery Controllerサーバーのピークディスクパーセンテージを表示します。
	ディスク待機時間 (ミリ秒)	ディスクの待機時間値を折れ線グラフで表示します。
	平均ディスク待機時間 %	過去10分間のDelivery Controllerサーバーの平均ディスク待機時間を集計して表示します。
	ピークディスク待機時間 %	過去5分間のDelivery Controllerサーバーのピークディスク待機時間の割合を表示します。

カテゴリ	メトリック	説明
影響	IIS証明書の有効性	IIS証明書の有効性を表示します。可能な値は、*期限切れ*、*期限切れ間近*、*有効*、*見つかりません*です。
	IIS証明書チェーンの有効性	StoreFront IIS証明書チェーンが有効であるかどうかを表示します。可能な値は、*はい*または*いいえ*です。

アラートの作成と管理

関心のある条件とスコープをプロアクティブに監視し、アラート疲労を軽減するためにアラートを設定できます。アラートは、重要度、再アラート間隔、通知媒体で構成でき、製品でサポートされているアラートライフサイクルに従います。インフラストラクチャに関連するアラートは、**高度なアラートポリシー**セクションから作成できます。

詳細については、高度なアラートポリシーページを参照してください。

アプリケーションおよびデスクトップのプロービング

アプリケーションおよびデスクトップのプロービングは、StoreFrontを使用してサイトで公開されているアプリケーションとデスクトップを順次テスト起動することで、それらの健全性をチェックするプロセスを自動化します。プロービングの結果はDirectorで利用できます。

要件

- Delivery Controllerは、アプリケーションプロービングの場合はバージョン7.18以降、デスクトッププロービングの場合はバージョン1906以降を実行している必要があります。
- プローブエージェントを実行しているエンドポイントマシンはWindowsマシンであり、アプリケーションプロービングの場合はWindows版Citrix Workspace™アプリバージョン1808以降、デスクトッププロービングの場合はバージョン1906以降がインストールされている必要があります。Unified Windows Platform (UWP) 用Workspaceアプリはサポートされていません。
- Citrix Probe Agentは、Active Directory資格情報を使用したStoreFrontおよびCitrix Workspace経由の認証をサポートしています。エンドポイントデバイスがCitrix Gateway経由でStoreFront / Workspaceに接続されている場合、Citrix Gatewayドメイン資格情報または多要素認証 (MFA) を使用して認証できます。Citrix Probe Agentは、シングルサインオン (SSO) などの他の認証方法をサポートしていません。

> **注:**
>
> - ユーザーがCitrix Cloud™でサインインポリシーまたは条件付き認証を有効にしている場合、プローブエージェントはStoreFrontまたはCitrix Workspaceアプリにサインインできません。
> - Probe Agentは、Citrix Workspaceアプリへの認証にActive Directory認証のみをサポートしています。

- Citrix Probe Agentは、Citrix GatewayやCitrix ADCのようなプロキシサーバーやロードバランサーが展開されていない場合にのみ機能します。
- プローブエージェントをインストールするエンドポイントマシンに、Microsoft .NET Frameworkバージョン4.7.2以降がインストールされていることを確認してください。

プロービングの実行に必要なユーザーアカウントまたは権限：

- 各エンドポイントマシンでプローブする一意の StoreFront ユーザー。StoreFront ユーザーは管理者である必要はありません。プローブは非管理者コンテキストで実行できます。
- エンドポイントマシンにCitrix Probe Agentをインストールおよび構成するためのWindows管理者権限を持つユーザーアカウント。
- ユーザーは、アプリケーションまたはデスクトップの起動に使用されるVDAと同じドメインのメンバーである必要があります。プローブエージェントは現在、複数のドメインをサポートしていません。
- プロービングのために既存のユーザーアカウントを再利用すると、ユーザーのアクティブなセッションからログオフされる可能性があります。フル管理者ユーザーアカウント、または以下の権限を持つカスタムロールが必要です。
  - デリバリーグループの権限:
    - 読み取り専用
  - Directorの権限:
    - アラートメールサーバー構成の作成\\編集\\削除 - (メールサーバーがまだ構成されていない場合)
    - プローブ構成の作成\\編集\\削除
    - 構成ページの表示

- トレンドページの表示

構成

複数の地域で、ピーク時間外にプローブを実行するようにスケジュールできます。包括的なプローブ結果は、ユーザーが問題に遭遇する前に、アプリケーション、ホストマシン、または接続に関連する問題をトラブルシューティングするのに役立ちます。

Citrix Probe Agentバージョン2103以降は、サイト集約をサポートしています。Citrix Probe Agentを構成する際、「Workspace (StoreFront) Site Aggregation Enabled」オプションを選択して、集約されたサイトからのアプリケーションとデスクトップの列挙を有効にします。以下のサイトの組み合わせがサポートされています。

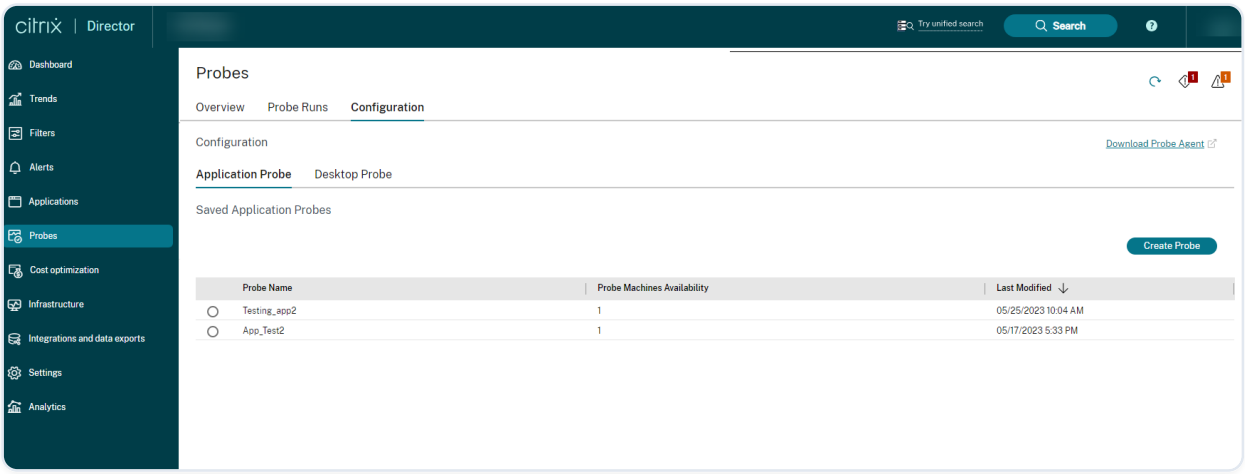
- 1つのStoreFront URLを持つ複数のオンプレミスサイト。
- StoreFrontまたはWorkspace URLを持つオンプレミスサイトとクラウドサイト。
- 1つのWorkspace URLを持つ複数のクラウドサイト。
- Citrix Gateway経由でStoreFrontまたはWorkspaceに接続されたオンプレミスサイト。

> **注:**
>
> 1つのサイトにのみアクセスできるプローブを構成するには、個別の管理者またはユーザーを作成する必要があります。

ステップ1: Citrix Probe Agentのインストールと構成

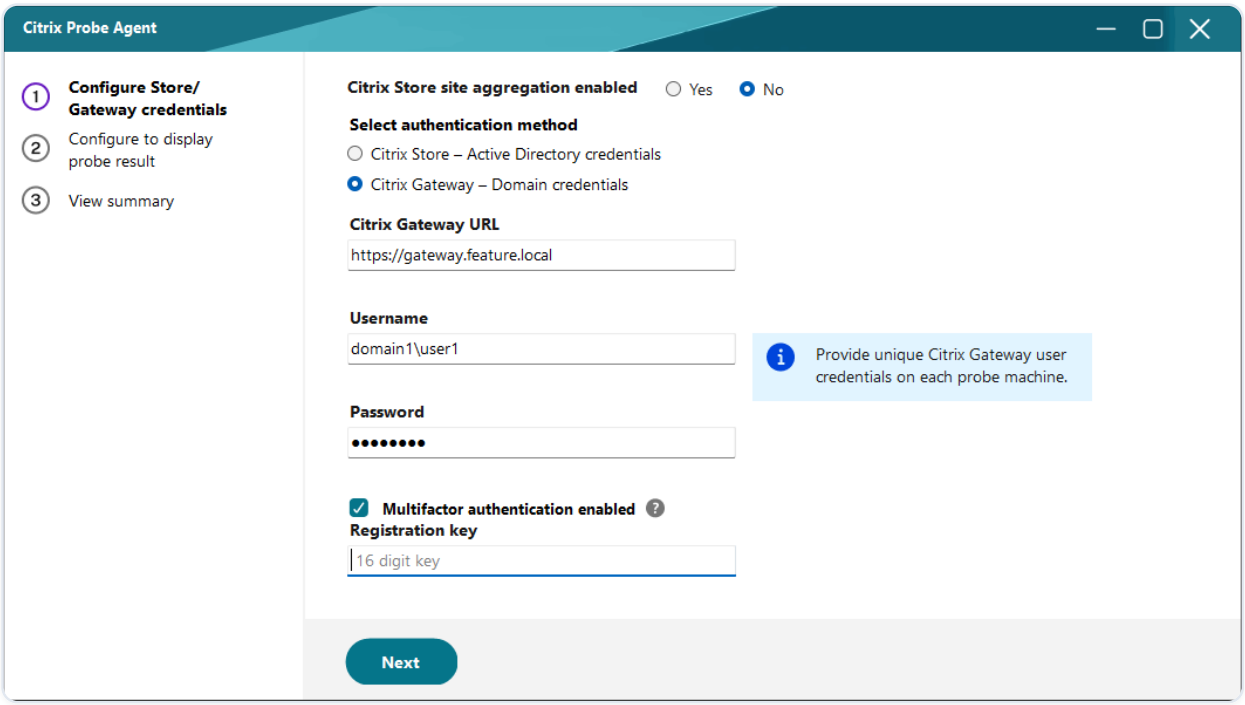
Citrix Probe Agentは、StoreFrontを介したユーザーによる実際のアプリケーションまたはデスクトップの起動をシミュレートするWindows実行可能ファイルです。これは、Directorで構成された起動をテストし、その結果をDirectorに報告します。

1. プロービングを実行するエンドポイントマシンを特定します。
2. 管理者権限を持つユーザーは、エンドポイントマシンにCitrix Probe Agentをインストールして構成できます。Citrix downloadsページで入手できるCitrix Probe Agentの実行可能ファイルをダウンロードしてください。ダウンロードリンクは、Directorの**Probes**タブでも利用できます。



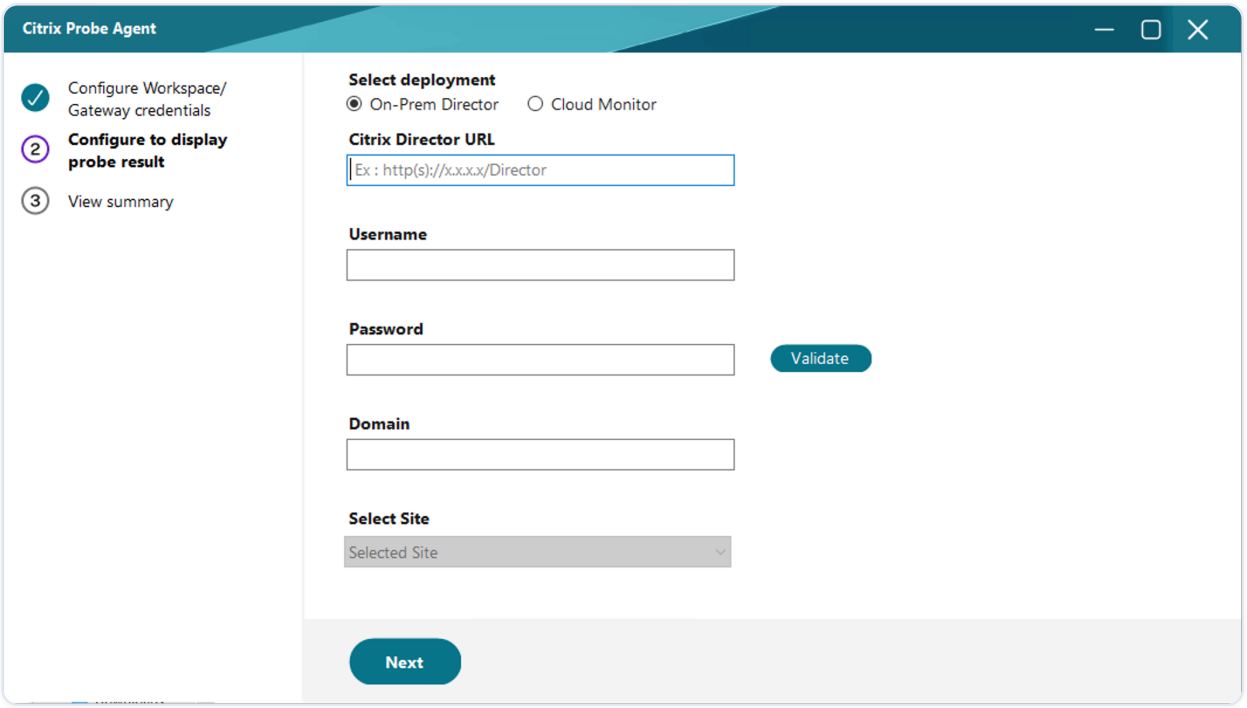
。

3. 集約されたサイトがある場合は、集約されたサイトからのアプリケーションとデスクトップの列挙を有効にするために、Workspace (StoreFront) Site Aggregation Enabledオプションを選択します。
4. 認証方法を選択し、関連する資格情報を入力します。資格情報は暗号化され、安全に保存されます。
5. StoreFront Active Directoryの資格情報で構成します。各エンドポイントマシンで一意のWorkspace (StoreFront)ユーザーを構成します。
6. エンドポイントがCitrix Gatewayを介してStoreFrontに接続されている場合は、Citrix Gatewayオプションを選択し、Citrix Gatewayドメインの資格情報で構成します。



7. ゲートウェイが多要素認証をサポートしている場合は、多要素認証オプションを選択し、16桁の認証キーを入力します。これは、シングルログインスキーマを使用してLDAPとネイティブOTPで構成されているCitrix Gatewayでのみ利用できます。

8. タブで、Director の資格情報を入力し、 をクリックします。



9. サイトを選択し、**次へ**をクリックします。
10. **概要の表示**タブで、設定された詳細が正確であることを確認します。変更が必要な場合は、該当するタブに移動して更新します。

> **注:**
>
> Automating Citrix Probe Agent Installation and Configuration に含まれるPowerShellスクリプトを使用して、Citrix Probe Agentのインストールと構成を自動化できます。

ステップ 2: Director でプロービングを構成する

> **制限事項:**
>
> 対話型ログオンメッセージバナーが有効になっている Windows VDA からアプリケーションまたはデスクトップがテスト起動されると、プロービングは失敗します。これは、対話型ログオンメッセージの承認を待機しているためにタイムアウトが発生するためです。 サーバー VDA でログオンメッセージを無効にするには、コンピューターの構成 > Windows の設定 > セキュリティの設定 > ローカルポリシー > セキュリティオプションに移動します。

以下のフィールドのテキストを削除し、Microsoftポリシーを更新します。

- 対話型ログオン: ログオンしようとするユーザーへのメッセージテキスト
- 対話型ログオン: ログオンしようとするユーザーへのメッセージタイトル

対話型ログオンメッセージバナーが無効になっているこの特定のサーバー VDA にプローブユーザーを割り当てて、プローブがアプリケーションまたはデスクトップの起動状態を通過できるようにします。

詳細については、`<https://learn.microsoft.com/ja-jp/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>`を参照してください。

1. **プローブ** \> **アプリケーションプローブ**または**デスクトッププローブ**に移動し、**プローブの作成**をクリックします。
2. 「**プローブの作成**」ページで、プローブの名前を入力します。
3. スケジュールを選択します。
    a. プローブを実行する曜日を選択します。
    b. プローブを実行する開始時刻を入力します。
    c. さらに、**1日あたりの繰り返し**オプションを選択できます。プローブを1日の中で繰り返す終了時刻と間隔を入力します。たとえば、以下の構成では、月曜日、水曜日、木曜日、日曜日のそれぞれで、12時08分から16時34分まで30分ごとにアプリケーションプローブを実行できます。
4. 間隔に応じて、プローブするアプリケーションまたはデスクトップの推奨数を選択します。
5. プローブを実行する必要があるエンドポイントマシンを選択します。
6. 失敗したプローブの結果を送信する管理者のメールアドレスを入力します。メールサーバーは、**アラート** > **メールサーバーの構成**で構成します。

Directorの構成(/en-us/citrix-virtual-apps-desktops/2511/media/dir-probe-config.png)

この構成では、アプリケーションセッションは月曜日、水曜日、木曜日、日曜日のそれぞれで、12時08分、12時38分、13時08分といった具合に、16時08分まで起動します。

注:

- 構成後、エージェントは次の時間から構成されたプローブを実行します。
- **1日あたりの繰り返し**オプションが導入される前に設定されたプローブは、スケジュールされた時間に引き続き実行されます。これらのプローブでは、**1日あたりの繰り返し**オプションはデフォルトで無効になっています。
- 重複を防ぐため、各実行に5分間の期間が設けられるようにプローブを構成することをお勧めします。

ステップ3：プローブの実行

エージェントは、Directorから定期的にフェッチするプローブ構成に従ってプローブを実行します。

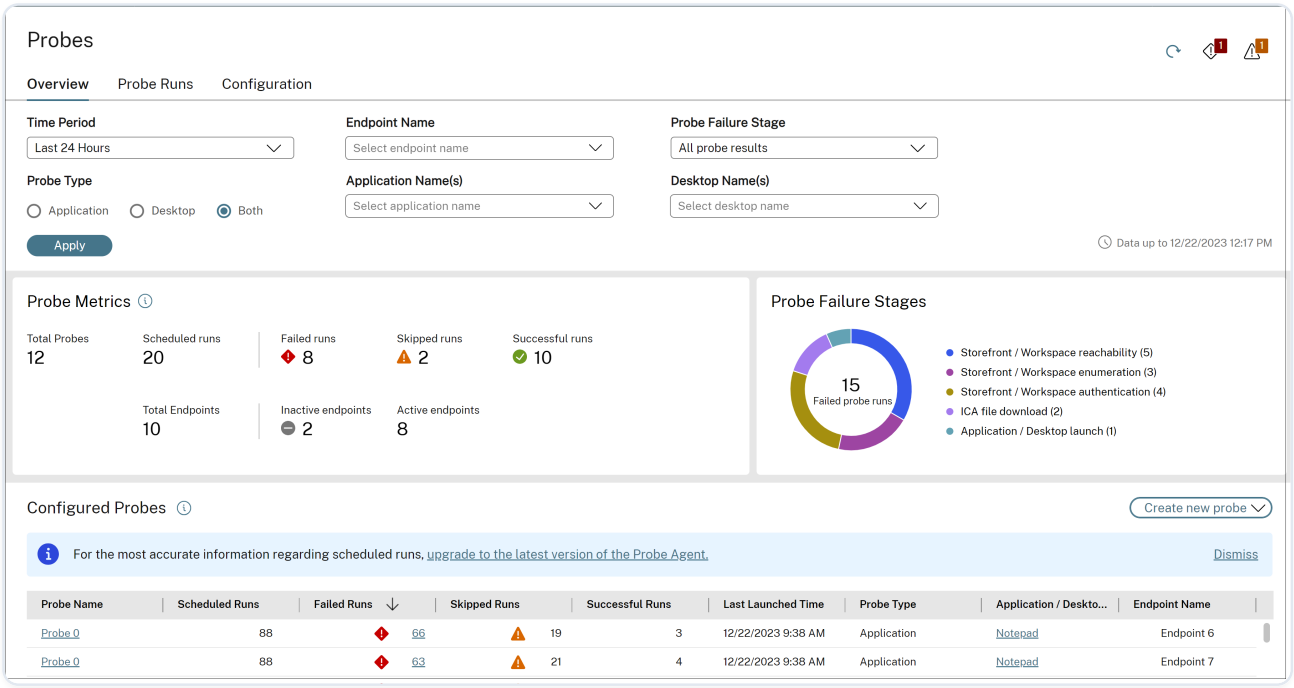
StoreFrontを使用して、選択されたアプリケーションを順次起動します。エージェントは、Monitorデータベースを介して結果をDirectorに報告します。障害は5つの特定の段階で報告されます。

- **StoreFront到達可能性** - 設定されたStoreFront URLに到達できません。
- **StoreFront認証** - 設定されたStoreFront資格情報が無効です。
- **StoreFront列挙** - StoreFrontのアプリケーション列挙リストに、プローブ対象のアプリケーションまたはデスクトップが含まれていません。
- **ICA®ダウンロード** - ICAファイルが利用できません。
- **アプリケーション/デスクトップ起動** – アプリケーションまたはデスクトップを起動できませんでした。

ステップ4：プローブ結果の表示

プローブでプローブ結果を確認できます。プローブビューでは、プローブ結果の包括的な概要が表示されます。これらの結果は、問題を事前に分析してトラブルシューティングするのに役立ち、ユーザーのセッション起動エクスペリエンスをよりスムーズにします。

概要タブには、設定されているすべてのプローブの概要が1つのビューに表示されます。



プローブは、期間、プローブの種類、エンドポイント名、アプリケーション名、デスクトップ名、およびプローブ結果の種類に基づいてフィルタリングできます。フィルタ条件に一致するプローブは、プローブ、アプリケーション/デスクトップ、およびエンドポイントごとに次の詳細とともに表示されます。

プローブメトリックには、スケジュール済み、計画済み、スキップ済み、成功、失敗した実行の数が表示されます。

- 完了した実行 – 完了まで実行されたプローブ実行の数。
- 失敗した実行 – 失敗したプローブ実行の数。
- スキップされた実行 – エンドポイントが非アクティブであるか、サービスが利用できないために完了まで実行されなかった実行の数。
- 成功した実行 – アプリ/デスクトップの起動中にどの段階でも失敗することなく正常に完了したプローブの数。

エンドポイントマシンの総数も、アクティブなマシンと非アクティブなマシンの数とともに表示されます。

「**プローブ失敗ステージ**」は、各障害グループの障害分布を視覚的に内訳表示します。ほとんどの障害が発生したステージを分析することで、プローブ結果の解釈と問題のトラブルシューティングが容易になります。グラフィカル表示には、アプリケーション/デスクトップの起動、ICAファイルのダウンロード、Storefront/Workspaceの列挙、Storefront/Workspaceの到達可能性、Storefront/Workspaceの認証における失敗したプローブ実行の数が示されます。

これにより、ほとんどの障害が発生したステージを分析するのに役立ちます。この情報は、プローブ結果を迅速に理解し、トラブルシューティングを行うのに役立ちます。

エンドポイントが非アクティブであるか、サービスが利用できないために、一部のプローブ実行が完了しない場合があります。

「**プローブ実行**」タブには、完了したプローブ実行の結果が詳細に表示されます。選択したプローブの個々の実行の詳細を表示するためにドリルダウンできます。重要なピボットポイントに基づいて、さらにフィルタリングおよび分析できます。

Directorプローブ実行(/en-us/citrix-virtual-apps-desktops/2511/media/dir-probe-runs.png)

プローブ実行は、期間、プローブタイプ、エンドポイント名、アプリケーション名、デスクトップ名、プローブ失敗ステージに基づいてフィルタリングできます。プローブ失敗ステージは、プローブが失敗したステージを表示します。プローブ名、スケジュールされた実行、失敗した実行、アプリケーション/デスクトップ名のリンクをクリックすると、フィルタ条件に一致するプローブ実行のリストが表示されたプローブ実行ページに移動します。

コスト最適化

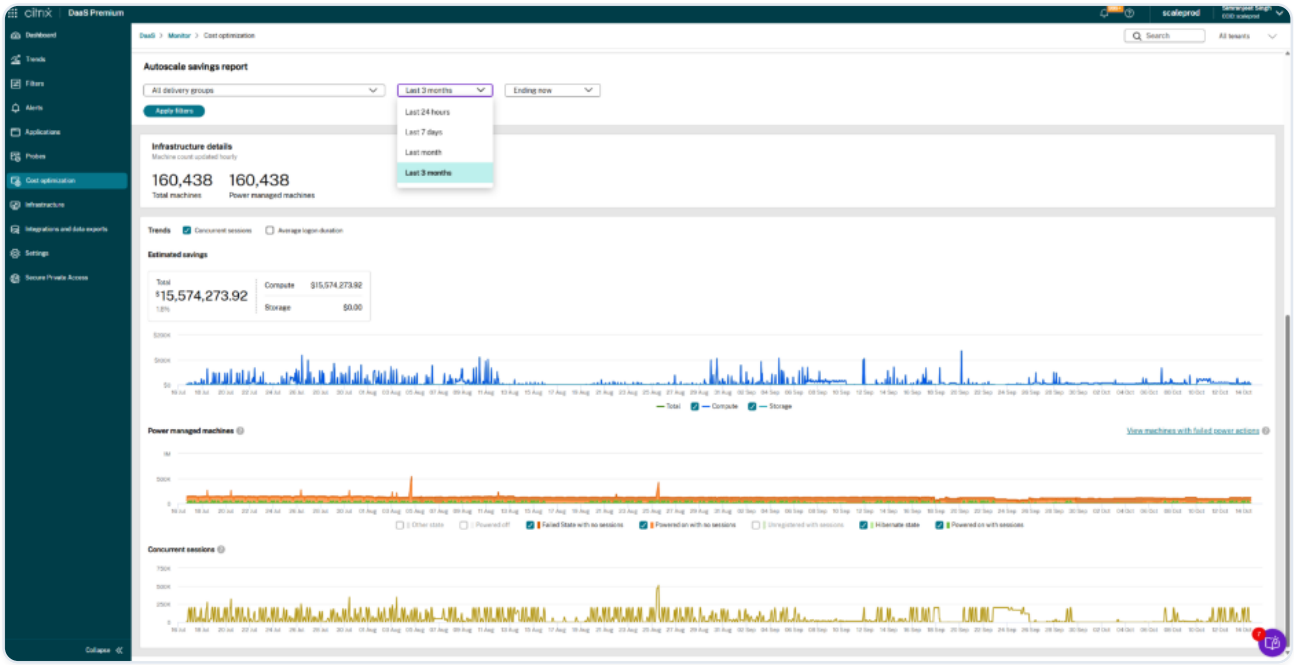
Citrix Director に、仮想マシンとセッションの使用状況を効果的に分析するのに役立つ「コスト最適化」という新機能が導入されました。この機能は、コストを最適化する方法について洞察に満ちた視覚的な表現を提供します。また、不要なマシンを排除し、それによってコストを削減するのにも役立ちます。

コスト最適化をサポートするために、次のアラートも導入されました。

- 電源オンアクションの失敗と電源オフアクションの失敗
- マシンの稼働時間アラート

最近の電源アクションを持つマシンを検査して、ユーザーの問題を引き起こす電源オンの失敗や、コストを増加させる電源オフの失敗を分析することもできます。詳細については、「最近の電源アクションを持つマシンを検査する」セクションを参照してください。

ホームページの左メニューから**コスト最適化**タブをクリックして、**コスト最適化**ページにアクセスします。



コスト最適化ホームでは、次のことができます。

- 開始リンク - このリンクにアクセスして、コスト最適化機能の詳細を確認します。
- コスト最適化ページを確認する - **コスト最適化**ページに関するフィードバックを提供できます。
- データを更新します。
- アラートを表示する - 重大なアラートと警告アラートの両方を表示できます。

コスト最適化ページには、次の機能が含まれています。

- コスト削減
- インフラストラクチャの適正化

コスト最適化のコストの計算方法?

マシンあたりの時間あたりのコストは、ハイパーバイザーがサポートする通貨で表示されます。このセクションでは、Azure マシンおよびその他のマシンのコストがどのように計算されるかについて説明します。

Azure マシンのコスト

コスト計算の優先順位は次のとおりです:

1. 「Microsoft.Consumption/pricesheets/read」 権限が利用可能な場合、実効価格は Azure サブスクリプションで構成されている通貨で表示されます。
2. 権限が利用できない場合、Azure の小売価格が表示されます。詳細については、Azure 小売価格の概要 を参照してください。

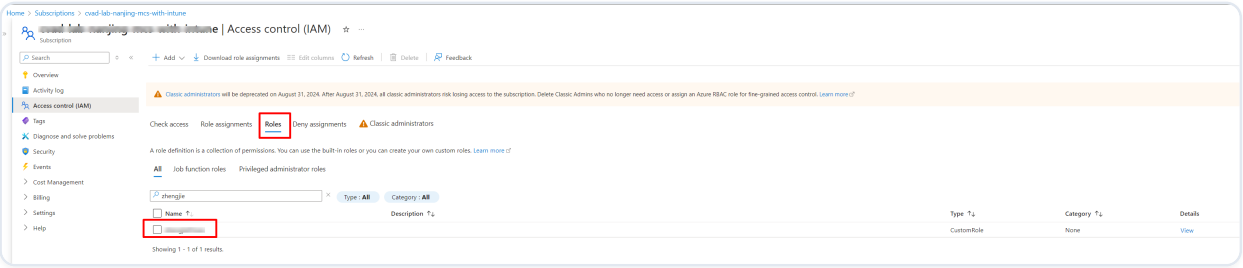
3. 実効価格または小売価格が利用できない場合、コストは管理者が Web Studio で入力したコストに基づいて表示されます。
4. Web Studio でコストが指定されていない場合、デフォルトのコスト $1 が考慮されます。

Azure のアカウント詳細を確認し、実効価格を見つけるために必要な権限を追加するには、次の手順を実行します。

1. Citrix DaaS に移動します。
2. タブをクリックして、ホスティング接続アカウントを見つけます。
3. タブに記載されている を探します。

   ホスティングタブ(/en-us/citrix-virtual-apps-desktops/2511/media/daas-azure-hosting.png)
4. Microsoft Entra ID に移動し、手順 3 でメモした を探します。
5. **サブスクリプション** > **アクセス制御 (IAM)** に移動し、ホスティング接続SPN用に構成されたカスタマイズされた役割を選択します。

   Azure ポータル(/en-us/citrix-virtual-apps-desktops/2511/media/azure-portal.png)



6. その役割に *Microsoft.Consumption/pricesheets/read* 権限を追加します。

Azureの小売価格を確認する方法?

`Microsoft.Consumption/pricesheets/read` が利用できない場合、Azure の小売価格が表示されます。これで、Retail Rates Prices API を使用して、すべての Azure サービスの小売価格を取得できます。以前は、Azure サービスの価格を取得する唯一の方法は、Azure 料金計算ツールを使用するか、Azure ポータルを使用することでした。詳細については、Azure の小売価格の概要を参照してください。

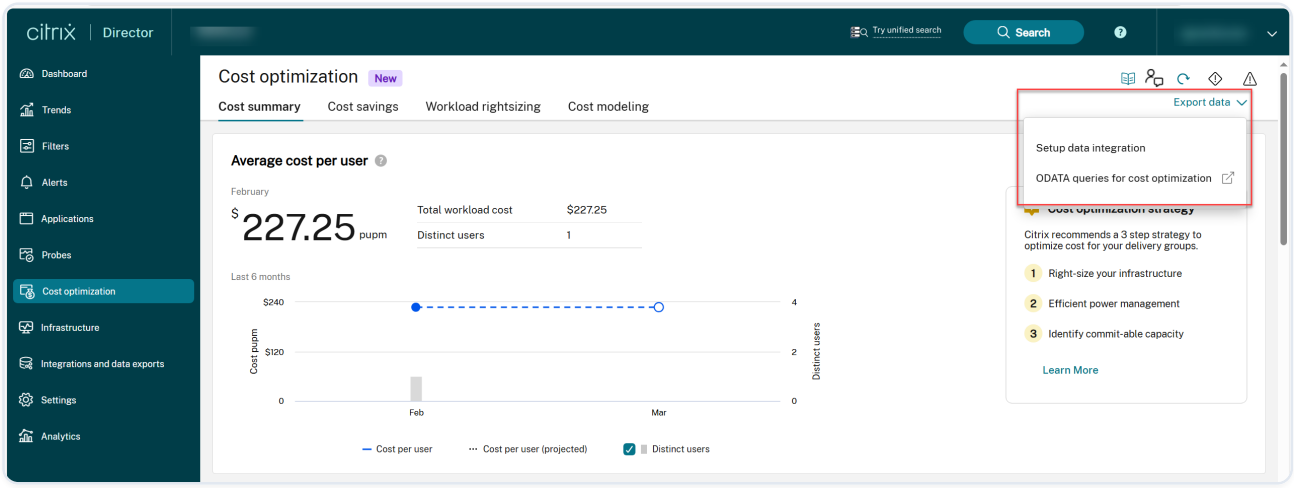
Azure 以外のマシンのコスト計算

その他のマシンについては、Web Studio で管理者が入力したコストに基づいてコストが表示されます。Web Studio でコストが指定されていない場合、デフォルトのコストである 1 ドルが考慮されます。

データのエクスポート

データ統合と ODATA クエリを使用して、「**コスト最適化**」ページのデータをエクスポートできます。データをエクスポートするには、「**コスト最適化**」ページで「**データのエクスポート**」をクリックすると、次のオプションが表示されます。

- データ統合のセットアップ
- コスト最適化のための ODATA クエリ



データ統合のセットアップ

コスト最適化データをMonitor Service APIと統合することで、トラブルシューティングや問題のトリアージのためのデータを収集できます。詳細については、統合とデータのエクスポートページを参照してください。

コスト最適化のためのODATAクエリ

コスト最適化ページで利用可能なサンプルODATAクエリを使用して、データをエクスポートできます。

ODATAの利用を開始する

以下のリンクは、ODATAの利用を開始するのに役立ちます。

- ODATAの概要
- Citrix CloudのOData v4エンドポイントを使用してCitrix Monitor Serviceデータにアクセスするためのさまざまな方法
- Citrix Monitor ServiceデータでOData V4集計クエリを使用する
- ODataおよびAPIクライアントを使用してPowerBIとDaaS Monitorを接続する方法
- Postmanを使用してログオン時間が長いユーザーの詳細を取得する
- Monitor Serviceデータにアクセスする方法

- データアクセスプロトコル
- モニターモデル
- モニター通知

サンプルODATAクエリ

未使用のVDAを検索する

未使用のVDAを特定するには、デスクトップグループID、VDAの開始日、および終了日を指定する必要があります。

未使用リソースの費用削減に関する詳細については、「ワークロードの適正化」を参照してください。

クエリの例:

```
https://<DDC URL>/monitorodata/ResourceUtilizationSummary?
$apply=filter(DesktopGroupId eq desktop-group-id and granularity eq 1440
and SummaryDate ge startdate and SummaryDate lt enddate)/
groupby((MachineId), aggregate(cast(TotalSessionCount, Edm.Int32) with
average as AvgTotalSessionCount))/filter(AvgTotalSessionCount eq 0.0)/
aggregate($count as UnusedVDACount)
```

1日の平均稼働時間（分）を検索する

1日の平均稼働時間（分）を検索するには、以下を指定する必要があります。

- デスクトップグループID
- 開始日
- 終了日
- 終了日と開始日の間の日数差.

未使用リソースの費用削減に関する詳細については、「ワークロードの適正化」を参照してください。

クエリの例:

```
https://[<DDC URL>|https://api-us.cloud.com/monitorodata/
ResourceUtilizationSummary?$apply=filter(DesktopGroupId] /monitorodata/
ResourceUtilizationSummary?$apply=filter(desktopGroupId eq desktop-group-
id and granularity eq 1440 and SummaryDate ge startdate and SummaryDate lt
enddate)/groupby((MachineId), aggregate(cast(UptimeInMinutes, Edm.Int32)
```

```
div day-difference with sum as TotalUptimeInMinutes))/
aggregate(TotalUptimeInMinutes with average as
DailyAverageUptimeInMinutes)
```

失敗したマシンの電源アクションを検索する

失敗したマシンの電源操作の詳細については、「電源オン操作の失敗と電源オフ操作の失敗」を参照してください。

クエリの例:

```
https:// <DDC URL> /monitorodata/Machines?$filter=LifecycleState eq 0 and
DesktopGroup/SessionSupport eq 1 and
(cast(LastPowerActionReason,'Edm.Int32') eq 6 or
cast(LastPowerActionReason,'Edm.Int32') eq 7 or
cast(LastPowerActionReason,'Edm.Int32') eq 8) and
(cast(LastPowerActionFailureReason,'Edm.Int32') eq 300 or
cast(LastPowerActionFailureReason,'Edm.Int32') eq 402 or
cast(LastPowerActionFailureReason,'Edm.Int32') eq 401) and MachineRole eq
0&$orderby=Name&$skip=0&$top=50&$expand=DesktopGroup($select=Name)&$select
=Sid,Id,Name,IsAssigned,IPAddress,FaultState,LastDeregisteredCode,FailureD
ate,CurrentPowerState,CurrentSessionCount,IsInMaintenanceMode,LastPowerAct
ionFailureReason,LastPowerActionCompletedDate
```

総節約額を特定する

コスト削減の詳細については、コスト削減ページを参照してください。

サンプルクエリ:

```
https://[<DDC URL>|https://api-us.cloud.com/monitorodata/
ResourceUtilizationSummary?$apply=filter(DesktopGroupId] /monitorodata/
MachineCostSavingsSummaries?$apply=aggregate(TotalAmountSaved with sum as
TotalAmountSavedSum)
```

マシンの状態を確認する

コスト削減の詳細については、コスト削減ページを参照してください。

サンプルクエリ:

```
https:// <DDC URL> /monitorodata/MachineCostSavingsSummaries?
$filter=SummaryDate eq
2024-08-09T06:00:00Z&$select=TotalMachinesCount,PowerManagedMachinesOff,Po
```

```
werManagedMachinesInHibernate,PowerManagedMachinesOnWithSessions,PowerMana
gedMachinesOnWithoutSessions
```

コスト削減

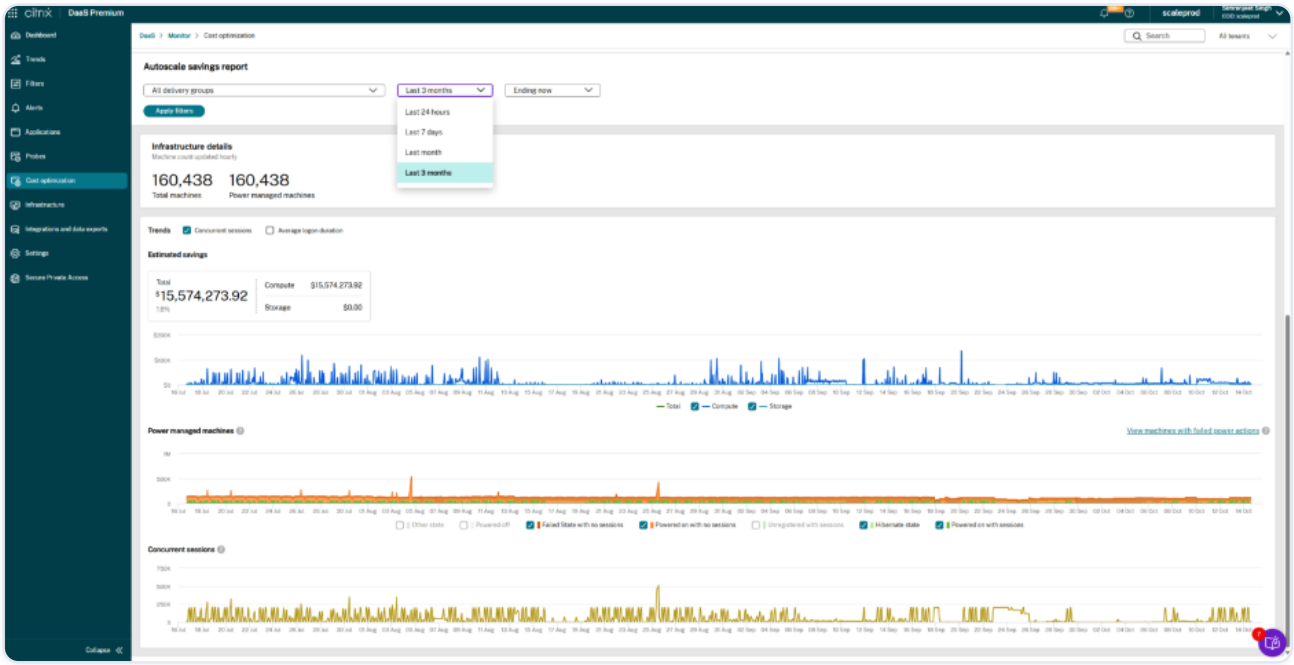
コスト削減ページでは、選択した期間にわたって蓄積されたインフラストラクチャの節約額を視覚的に表示し、残りの日数で予想される節約額を予測します。このページは、マシンの使用状況とセッションを分析することで、達成された節約とコスト削減の機会を特定するのに役立ちます。このページでは以下を提供します。

- インフラストラクチャコストの最適化に関する洞察
- 節約された金額
- 予測コストを超える可能性のあるさまざまなシナリオに関する情報
- インフラストラクチャコストの節約を実現するための特定と戦略的計画の潜在的な機会

マシンの使用状況は通常、ピーク時に増加し、リソースの増加を要求します。Autoscale™ 機能は、需要の低い期間中に未使用のマシンを自動的に電源オフにすることで、コストを削減するのに役立ちます。予測される節約額は、この使用パターンに依存します。ただし、未使用のマシンが存在する場合や、Autoscaleの電源アクションに障害がある場合など、特定の状況下ではコストが予想を超える可能性があります。これらの発生の背後にある理由を特定することは、以前は困難でした。

コスト最適化ページでは、予想コストを超える原因となる可能性のあるさまざまなシナリオに関する詳細情報が提供されます。同様に、たとえば、セッションのないマシンがある場合、さらなるコスト削減の機会が示されます。

ホームページの左側のメニューから**コスト最適化**タブをクリックして、**コスト最適化**ページにアクセスします。



上部のドロップダウンリストから、サイトにクラウドとオンプレミスの両方のプロバイダーがある場合、すべてのクラウドプロバイダー、すべてのオンプレミスプロバイダー、または個々のプロバイダーでフィルタリングできるようになりました。

注:

> フィルターは、適用ボタンなしで選択するとすぐに適用されます。

> **コスト最適化**ページには、**推定節約額**と**Autoscale節約レポート**が含まれています。コスト削減は、ハイパーバイザーの通貨または発生したコストのパーセンテージとして表示できます。

推定節約額: このグラフ表示は、インフラストラクチャリソースの効率的な利用を評価するのに役立ちます。コスト削減は、ハイパーバイザーの通貨または発生したコストのパーセンテージとして表示されます。このグラフは、コンピューティング関連の節約とストレージの節約から達成された節約を示しています。

注:

> ストレージからの節約を表示するには:

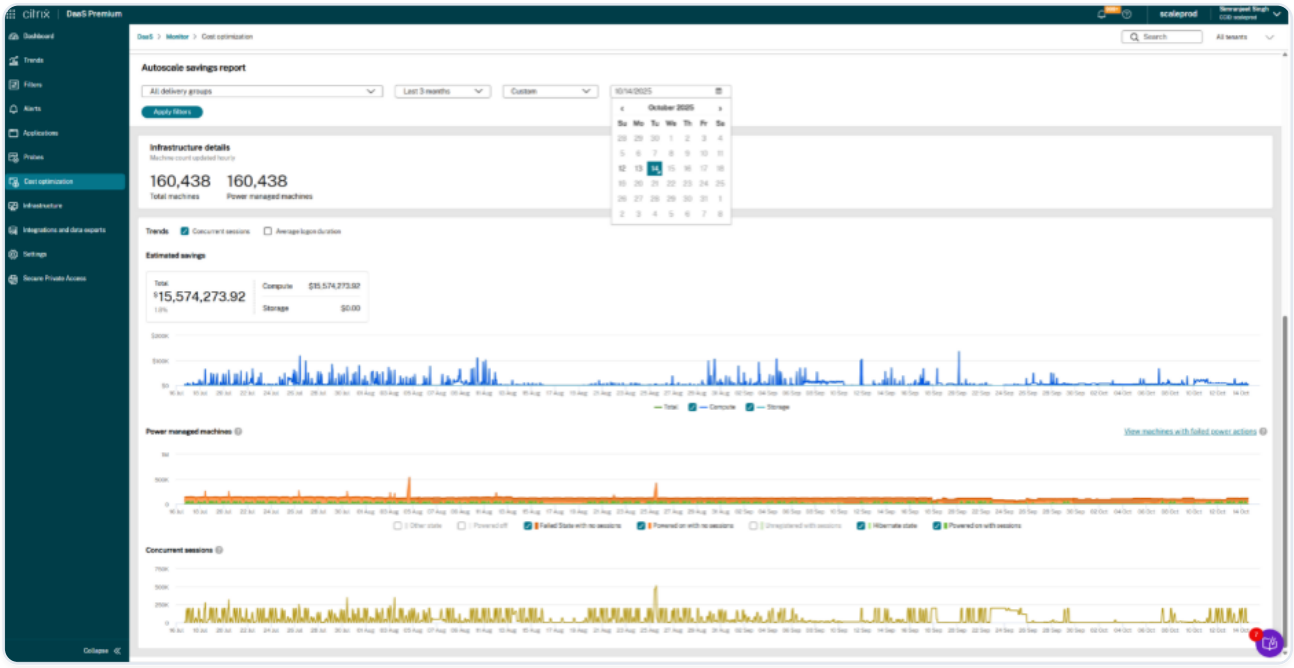
> - コンピューティングコストを最適化するには、Autoscaleを有効にする必要があります。詳細については、「Autoscaleの概要」を参照してください。

- ストレージコストを最適化するには、VMのシャットダウン時にストレージタイプを下位層に変更します。詳細については、「VMのシャットダウン時にストレージタイプを下位層に変更する」ドキュメントを参照してください。
- この機能は現在、Azureマシンにのみ適用されます。

次の期間の結果を表示できます:

- 7日間
- 30日間
- 3か月
- 6か月
- 12か月

次の図は、「推定インフラストラクチャの節約」セクションを示しています:



次の表は、「推定インフラストラクチャの節約」グラフの要素を示しています:

要素	説明
合計節約額	選択した期間にインフラストラクチャで達成された合計節約額を表示します。節約額はさらにストレージコストとコンピューティングコストに分類され、表形式で利用できます。

要素	説明
推定節約額	選択した期間にインフラストラクチャで達成された節約額を表示します。
電源管理されたマシン	電源管理されたマシンの合計数を表示します。
予測節約額	残りの期間でどれだけのインフラストラクチャの節約が可能かを表示します。
コンピューティング - 合計	コンピューティング関連の節約から達成された合計節約額を表示します。
コンピューティング - オートスケール	Autoscale機能を使用しているコンピューティング関連の節約から達成された合計節約額を表示します。
コンピューティング - ユーザーアクション	ユーザーアクションによるコンピューティング関連の節約から達成された合計節約額を表示します。
ストレージ - 合計	ストレージの節約から達成された合計節約額を表示します。
ストレージ - Autoscale	Autoscale機能を使用しているストレージの節約から達成された合計節約額を表示します。
ストレージ - ユーザーアクション	ユーザーアクションによるストレージ節約から達成された合計節約額を表示します。

Autoscale節約レポート: このグラフィカルな表示は、Autoscale機能が構成および有効化されているデリバリーグループの節約レポートを提供します。このレポートは、電源管理されているマシンにのみ適用されます。デリバリーグループを選択し、今日、昨日、先週、来週、今月、または来月のデータを選択できます。グラフにカーソルを合わせると、特定のグラフ値を取得できます。

> **注:**
>
> デリバリーグループが削除された場合、オートスケール節約レポートでデータは取得できません。

> デリバリーグループのドロップダウンリストから、以下のオプションにドリルダウンできます。

- **すべてのデリバリーグループ**: インフラストラクチャの詳細には、すべてのデリバリーグループ情報が表示されます。
- **すべてのシングルセッション**: シングルセッションマシンであるすべてのデリバリーグループのインフラストラクチャの詳細と、グラフにカーソルを合わせたときの、マシンの電源状態、成功したAutoscale電源アクション、およびセッションのグラフィカルな表示。
- **すべてのマルチセッション**: マルチセッションマシンであるすべてのデリバリーグループのインフラストラクチャの詳細と、グラフィカルな表示。
- **最大15個を選択** - インフラストラクチャの詳細には、選択されたすべてのデリバリーグループ（最大15個）とグラフィカルな表示が表示されます。
- **最大15個を除外** - インフラストラクチャの詳細には、選択されたデリバリーグループ（最大15個）を除いたすべてのデリバリーグループとグラフィカルな表示が表示されます。

選択した期間のデータが表示されます。**推定節約額**のグラフ表示は、ドロップダウンメニューから選択された実際の節約額です。ピークポイントにカーソルを合わせると、マシンの電源状態、Autoscaleの成功した電源アクション、およびセッションに関する情報が表示されます。

選択したデリバリーグループに基づいて、次の詳細を表示できます。

- **インフラストラクチャの詳細**
  - 合計マシン数と電源管理されているマシン数 - マシンの総数と、そのうち電源管理されているマシンの数を表示します。このデータは、残りの電源管理されていないマシンを電源管理されているマシンに変換し、Autoscale機能を有効にしてより包括的なカバレッジを実現する機会を提供します。インフラストラクチャの詳細セクションのデータは、1時間ごとに更新される最新の既知の情報を表示します。
- **カタログの詳細**

  ハイパーバイザー（サービスプロバイダー）の名前を表示します。詳細については、サポートされているVDAホスティングプラットフォームを参照してください。カタログの詳細のデータは、現在の時点で利用可能な最新のデータ（ライブデータ）を表示します。

  次の詳細を取得できます。

  - **ハイパーバイザー名** - サイトが接続されているハイパーバイザーの名前を表示します。複数のハイパーバイザーが存在する場合は、利用可能なすべてのハイパーバイザーを表示します。

- **インスタンス** - インスタンスの名前を表示します。
- **1時間あたりの総コスト** - ハイパーバイザーがサポートする通貨で、マシンあたりの1時間あたりのコストを表示します。Azureマシンでは、Microsoft.Consumption/pricesheets/read権限が利用可能な場合、Azureサブスクリプションで構成されている通貨で実効価格が表示されます。権限が利用できない場合は、Azureの小売価格が表示されます。詳細については、Azure小売価格の概要を参照してください。その他のマシンについては、Web Studioで管理者が入力したコストに基づいてコストが表示されます。Web Studioでコストが記載されていない場合、デフォルトのコストは1ドルです。詳細については、？
- **1時間あたりのコンピューティングコスト** - コンピューティング関連の節約によるコスト削減額を表示します。
- **1時間あたりのストレージコスト** - ストレージの節約によるコスト削減額を表示します。
- **マシン** - 選択したインスタンスのマシン数を表示します。

- **Autoscale構成（最終既知）**

  使用中のタグ - WebStudioのAutoscale設定で構成されているマシンのタグを表示します。タグ付けされたマシンに基づいてデータをフィルタリングすることもできます。この場合、タグ付けされたマシンの概要のみが表示されます。

  「キャパシティバッファ (ピーク時)」および**「キャパシティバッファ (オフピーク時)」**

  ピーク時とオフピーク時におけるデリバリーグループの最大要件に基づいて、電源がオンになっているマシンのバッファの割合を表示します。

- **推定節約額**

  選択した期間にインフラストラクチャで達成された節約額を表示します。Autoscale機能が有効になっているAzureマシンについては、コンピューティング関連の節約とストレージ関連の節約から節約額を確認できます。

- **「電源管理されたマシン」**

  Autoscaleが有効になっている場合、電源管理されたマシンは使用されていないときにオフにされ、コストを最適化します。次の詳細を取得できます。

  - 電源がオフになったマシンの数 - このデータは、電源がオフになり、コスト削減に貢献したマシンの数を分析するのに役立ちます。
  - 休止状態 - このデータは、休止状態にあるマシンの数を分析するのに役立ちます。

- セッションなしでオンになっているマシン - このデータは、なぜマシンがセッションなしでアクティブだったのかを分析する機会を提供します。このデータは、より効果的なインフラストラクチャ節約戦略を計画する機会を提供します。
- セッションありでオンになっているマシン - このデータは、電源がオンになっていてアクティブなセッションがあるマシンの数を分析するのに役立ちます。
- 電源オフ - このデータは、電源がオフまたは中断されたマシンの数と、このアクションがいつ実行されたかを分析するのに役立ちます。このデータを確認し、さらに変更を加えることで、コスト削減に貢献できます。
- 電源オン - このデータは、電源がオンになったマシンの数と、このアクションがいつ実行されたかを分析するのに役立ちます。このデータを確認し、さらに変更を加えることで、コスト削減に役立てることができます。
- セッションなしの失敗状態: このフィールドには、失敗状態にあり、アクティブなセッションがないマシンの数が表示されます。
- セッションありの未登録: このフィールドには、未登録状態にあるがセッションを提供しているマシンの数が表示されます。

> **注:**
>
> セッションなしで「失敗」状態のマシンと、電源アクションが失敗した状態のマシンの数を表示し、失敗の理由、時間、デリバリーグループに基づいてアクションを実行できます。これらの数はクリック可能なリンクであり、さらなるアクションのためにフィルターページに移動します。この数には、シングルセッションマシンとマルチセッションマシンの両方が含まれます。

- **同時セッション**

  選択した時点でのセッションの合計数を表示します。このデータは、コスト最適化のためにマシンをいつ電源オフにするかを決定するのに役立ちます。

- **平均ログオン時間**

  選択した期間におけるユーザーの平均ログオン時間を表示します。

ワークロードの適正化

強化されたワークロードの適正化ページは、デリバリーグループの使用状況とサイジングの側面を分析するのに役立ちます。これにより、デリバリーグループはマシンまたはユーザーのアクティビティに基づいて分析できます。

マシンベースの分析により、次のことが可能になります。

- 使用状況に基づいて仮想デスクトップを分類し、アクティビティがない、または低いマシンを特定して、未使用のリソースへの支出を削減します。使用状況分析
- 仮想デスクトップのリソース使用率を分析し、コスト削減またはユーザーエクスペリエンス向上のために適正化する必要があるマシンを特定します。サイジング分析

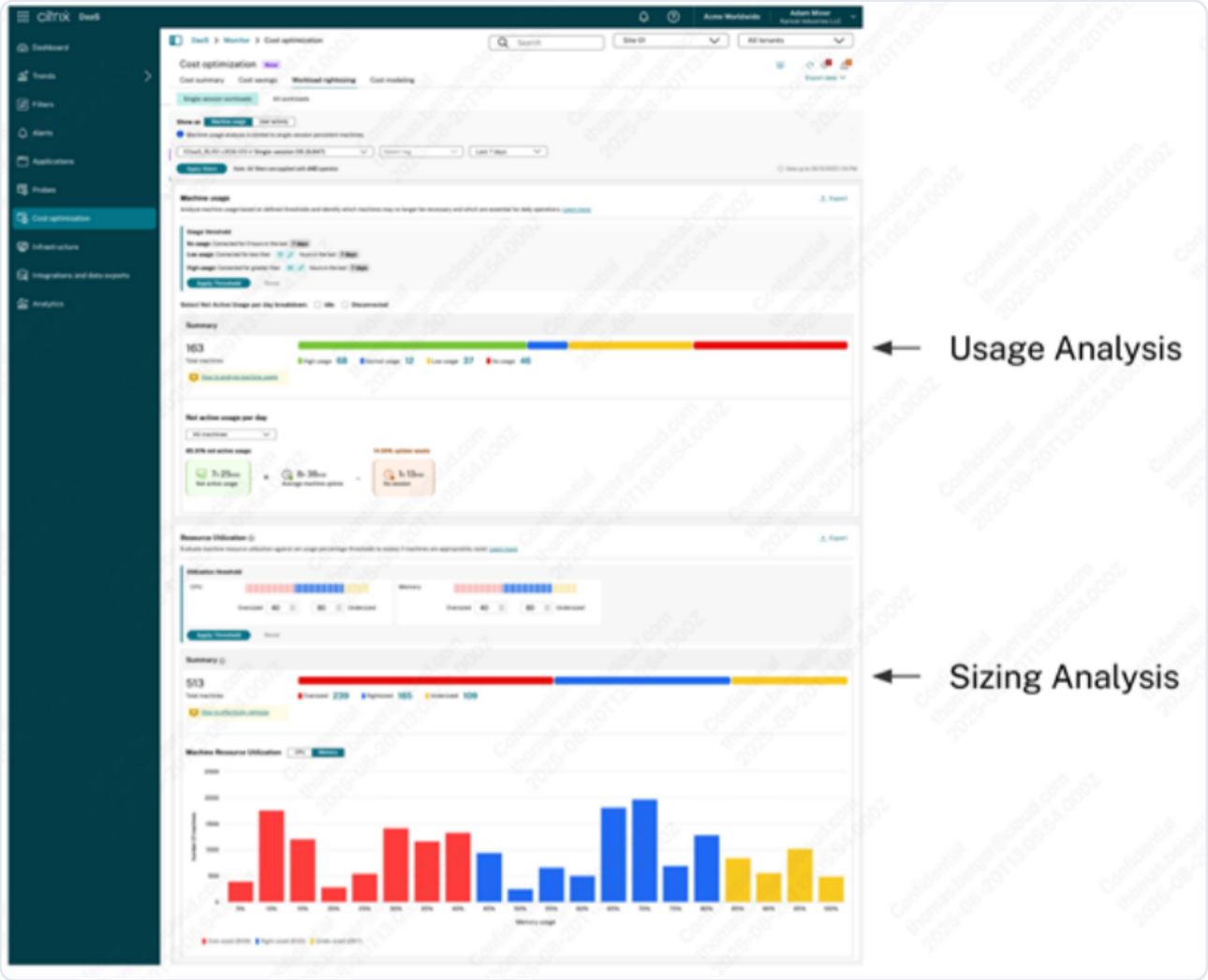
ユーザーベースの分析により、次のことが可能になります。

- アクティビティに基づいてユーザーを分類します。IT衛生上の理由から、アクティビティがないユーザーのアクセス権を削除することを検討してください。使用率の低いユーザーは、より効率的なリソース使用のために共有リソースに移動できます。
- ユーザーのリソース消費量を分析して、平均よりも高いまたは低いリソース消費量を持つコホートを特定し、ユーザーをより効果的に分散させます。

ホームページの左メニューから**コスト最適化**タブをクリックします。次に、**ワークロードの適正化**タブをクリックして、**ワークロードの適正化**ページにアクセスします。

> **注:**
>
> ページの上部で、マシンベースとユーザーベースの分析を切り替えることができます。

> **コスト最適化タブ > コスト削減**の**インフラストラクチャの詳細**セクションにある**このデリバリーグループを適正化するリンク**をクリックして、**ワークロードの適正化**ページにアクセスすることもできます。



マシン分析は、Windows 365 EnterpriseやFrontline専用など、ユーザーに静的に割り当てられた仮想デスクトップのシナリオに最適です。ユーザー分析は、ランダムに割り当てられた仮想デスクトップを持つデリバリーグループの分析に役立ちます。現在、どちらの分析もシングルセッションマシンに限定されています。

> **注:**
>
> ページ上部の「すべてのワークロード」ボタンからアクセスできる従来のライトサイジング分析は、今後のリリースで非推奨になります。

使用状況分析

使用状況分析を使用すると、仮想デスクトップのアクティビティレベルに基づいて、次のように分類できます。

- **使用率が低い、または使用されていないマシン（専用マシン）**：このカテゴリのマシンは不要になっている可能性があり、コスト削減のために削除できる場合があります。

- **使用率が高いマシン（専用マシン）**：このカテゴリは日常業務にとって重要であり、追加のサービス継続性対策が必要になる場合があります。
- **使用率が低い、または使用されていないユーザー（プールされたマシン）**：選択した期間内にアクティビティがないユーザーは、デリバリーグループに割り当てる必要がなくなる場合があります。それらを削除することで、環境のコストを削減できます。アクティビティの低いユーザーは、再割り当ての恩恵を受ける可能性があります。使用状況を統合し、コストを削減するには、専用デスクトップを持つアクティビティの低いユーザーをプールされたデスクトップに移動することを検討してください。

使用状況分析を実行するには：

1. デリバリーグループまたはタグに基づいてマシンを選択します
2. 分析の期間を選択します。
3. 低使用率および高使用率のパターンを定義するしきい値を確認および構成します。
4. 構成されたしきい値に基づいて仮想デスクトップの分類を示す概要セクションを調べます。
5. 各マシンの使用状況の詳細を表示する正味アクティブ使用状況セクションを確認します。アイドル時間と切断時間は、正味アクティブ使用状況分析に含めることも除外することもできます。
6. ドロップダウンを使用して、特定のカテゴリに焦点を当てます。
7. エクスポート機能を使用してマシン名と関連ユーザーをエクスポートし、マシン名と関連ユーザーを確認します。

> **注:**
>
> 提供された例はマシンベースの使用状況分析を示していますが、ユーザーベースの分析の手順は同等であり、個別に説明されていません。



サイジング分析

サイジング分析は、リソース使用率に基づいて仮想デスクトップまたはユーザーを以下のように分類します。

- 過剰なサイズのマシン：必要以上のリソースを持っています。リソース割り当てを減らすことで、ユーザーエクスペリエンスに影響を与えることなくコストを削減できます。
- 不十分なサイズのマシン：十分なリソースがありません。より多くのリソースを割り当てることで、ユーザーエクスペリエンスを向上させることができます。
- 適切なサイズのマシン：過剰なサイズと不十分なサイズのしきい値の間に収まります。
- ライトユーザー：これらのユーザーは再割り当ての恩恵を受ける可能性があります。コストを統合し削減するために、専用デスクトップを持つライトユーザーを共有プールデスクトップに移動することを検討してください。
- 中程度のユーザー：中程度のユーザーはデリバリーグループ内のマシンに適切に割り当てられており、最適なユーザーエクスペリエンスを期待できます。
- パワーユーザー：パワーユーザーは大量のリソースを消費し、プールされたデスクトップを共有する場合、その高い使用率がそのマシン上の他のユーザーの全体的なエクスペリエンスに悪影響を与える可能性があります。すべてのユーザーのエクスペリエンスを向上させ、パワーユーザーがデスクトップに一貫してアクセスできるようにするために、これらのユーザーを専用デスクトップに移動するか、個別のデリバリーグループに割り当てることを検討してください。

サイジング分析を実行するには：

1. デリバリーグループまたはタグに基づいてマシンを選択します
2. 分析の期間を選択します。
3. CPUとメモリ使用率のしきい値を個別に構成します。
4. 仮想デスクトップの分類を示す概要セクションを確認します
5. マシンのリソース使用率チャート（CPUとメモリの分布を示す）を分析する
6. リソースタイプに基づいてマシン構成を微調整し、外れ値を特定する
7. エクスポート機能を使用してマシン名と関連ユーザーをエクスポートし、マシン名と関連ユーザーを確認する

> **注:**
>
> 提示された例はマシンベースのリソース消費分析を示していますが、ユーザーベースの分析の手順も同等であり、別途説明はしません。

> リソース使用率(/en-us/citrix-daas/media/resource-utilization.png)

> **注:**
>
> 使用率分析では、選択した期間におけるデリバリーグループの95パーセンタイル使用率を使用します。これは、CPUまたはメモリ使用率の95%が設定値以下であることを示します。

ベストプラクティス

- 使用状況分析を使用して、利用率の低いマシンを削除することでコスト削減の機会を特定します。
- サイジング分析を適用して、リソース割り当てを最適化し、ユーザーエクスペリエンスを向上させます。
- 静的に割り当てられた仮想デスクトップシナリオでは、正確な分析のためにマシン分析を使用します。
- プールされた仮想デスクトップシナリオでは、正確な分析のためにユーザーアクティビティを使用します。
- ランダムに割り当てられた仮想デスクトップを分析する際は、ローミングパターンを考慮してください。

- 詳細なレポートをエクスポートして、さらなる分析とドキュメント作成に役立てます。

主要な用語とグラフ

マシンの正味アクティブ使用量: 正味アクティブ使用量は、平均マシン稼働時間から合計稼働時間の無駄を差し引いて計算されます。すべての時間は分単位です。

正味アクティブ使用量の割合: ユーザーがマシンをアクティブに使用した実際の時間。これは、マシンが電源オンの状態で、少なくとも1つのセッションがアクティブであった期間です。

平均マシン稼働時間: マシンの電源がオンになっていた合計時間。

セッションなし: アクティブなセッションがないことによる稼働時間の無駄。

アイドル時間: アイドル状態のセッションによる稼働時間の無駄。これは、マシン上のすべてのセッションがアイドル状態である時間です。

切断時間: 切断されたセッションによる稼働時間の無駄。これは、マシン上のすべてのセッションが切断されている時間です。

合計マシン数 - マシンの総数を表示します。これには、選択した期間中に電源がオンになっていたすべてのマシンが含まれます。

平均セッション密度 - これは、マシン数と選択した期間にわたる平均です。セッションに利用可能なリソースに影響を与える、マシン上のセッション負荷の量を指します。

未使用のマシン - 選択した期間中にセッションがなかったが、電源がオンになっていたマシンの数を表示します。

CPU使用率:

マシンコホート - CPU使用率に基づいて、トップ、ミドル、ボトムに分類されたマシングループに関する情報を提供します。しきい値の制限は管理者が構成できます。

CPUピークの範囲 - マシンコホートに対応するCPU使用率に基づいて、CPUピークの範囲を表示します。

マシン - マシンコホートに対応するマシンの数を表示します。

セッション密度 - マシンコホートに対応するセッション密度を表示します。

リソース使用率の傾向:

CPUピークの範囲 - バンド内のCPUピークの範囲を表示します。バンド内の任意のポイントにカーソルを合わせると、バンドの上下の値が表示されます。

ピークメモリ使用率 - グラフ上に、選択したマシンおよび選択した時間の最大メモリ使用率を表示します。

平均セッション密度 - グラフ上に、選択したマシンおよび選択した時間の平均セッション密度を表示します。

平均ICA RTT - セッションの平均ラウンドトリップ時間を表示します。このグラフは、アクティブなセッションがない場合やセッションが切断されている場合に中断を示します。

平均ログオン時間 - グラフ上に、選択したマシンおよび選択した期間の平均ログオン時間を表示します。このグラフは、選択した時間に新しいログオンが開始された場合にデータを表示します。

コスト概要

「**コスト概要**」ページでは、Citrix® 環境の実行に関連する費用の包括的な概要が提供されます。この機能強化により、次の項目を可視化できます。

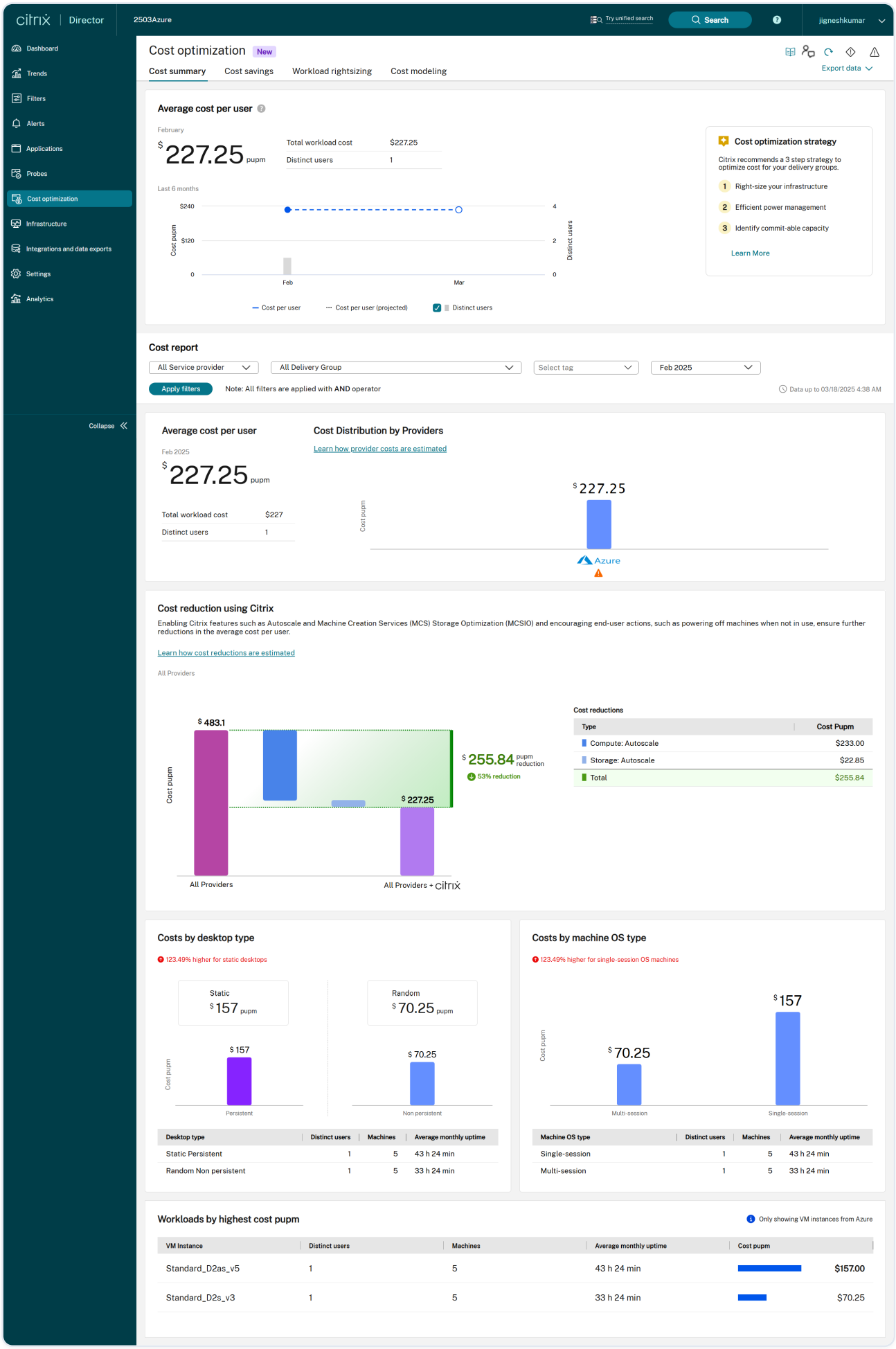
- ユーザーあたりの総コスト
- 選択したワークロードプロバイダー、デスクトップタイプ、およびVMシリーズセットによる仮想化提供のコスト

このページでは、次の情報が提供されます。

- 仮想化されたアプリまたはデスクトップをユーザーに提供するコストに関するインサイト
- 節約された金額
- 次のカテゴリに分類されたコストと節約に関する情報:
  - プラットフォームプロバイダー
  - OSタイプ
  - デスクトップタイプ
  - VMシリーズ

> **注:**
>
> 「**コスト概要**」ページは、サイトが1か月に少なくとも15日間稼働している場合にのみ利用できます。

> 「**コスト概要**」ページにアクセスするには、「**Director**」>「**コスト最適化**」>「**コスト概要**」をクリックします。「**コスト概要**」ページが表示されます。


citrix | Director
2503Azure
Try unified search
Search
jigneshkumar
Dashboard
Trends
Filters
Alerts
Applications
Probes
Cost optimization
Infrastructure
Integrations and data exports
Settings
Analytics
Collapse
Cost optimization
New
Cost summary
Cost savings
Workload rightsizing
Cost modeling
Export data
Average cost per user
February
$ 227.25 pupm
Total workload cost $227.25
Distinct users 1
Last 6 months
$240
$120
0
Cost pupm
4
2
0
Distinct users
Feb
Mar
Cost per user
Cost per user (projected)
Distinct users
Cost optimization strategy
Citrix recommends a 3 step strategy to optimize cost for your delivery groups.
1 Right-size your infrastructure
2 Efficient power management
3 Identify commit-able capacity
Learn More
Cost report
All Service provider
All Delivery Group
Select tag
Feb 2025
Apply filters
Note: All filters are applied with AND operator
Data up to 03/18/2025 4:38 AM
Average cost per user
Feb 2025
$ 227.25 pupm
Total workload cost $227
Distinct users 1
Cost Distribution by Providers
Learn how provider costs are estimated
$ 227.25
Cost pupm
Azure
Cost reduction using Citrix
Enabling Citrix features such as Autoscale and Machine Creation Services (MCS) Storage Optimization (MCSIO) and encouraging end-user actions, such as powering off machines when not in use, ensure further reductions in the average cost per user.
Learn how cost reductions are estimated
All Providers
$ 483.1
Cost pupm
$ 255.84 pupm reduction
53% reduction
$ 227.25
All Providers
All Providers + citrix
Cost reductions
Type
Cost Pupm
Compute: Autoscale $233.00
Storage: Autoscale $22.85
Total $255.84
Costs by desktop type
123.49% higher for static desktops
Static
$ 157 pupm
Random
$ 70.25 pupm
$ 157
$ 70.25
Cost pupm
Persistent
Non persistent
Desktop type
Distinct users
Machines
Average monthly uptime
Static Persistent 1 5 43 h 24 min
Random Non persistent 1 5 33 h 24 min
Costs by machine OS type
123.49% higher for single-session OS machines
$ 157
$ 70.25
Cost pupm
Multi-session
Single-session
Machine OS type
Distinct users
Machines
Average monthly uptime
Single-session 1 5 43 h 24 min
Multi-session 1 5 33 h 24 min
Workloads by highest cost pupm
Only showing VM instances from Azure
VM Instance
Distinct users
Machines
Average monthly uptime
Cost pupm
Standard_D2as_v5 1 5 43 h 24 min $157.00
Standard_D2s_v3 1 5 33 h 24 min $70.25

コスト概要ページには、以下が含まれます。

- **ユーザーあたりの平均コスト**

  過去6か月間のユーザーあたりの実際の月額コストと、今月の予測コストを表示できます。さらに、ワークロードの総コストとサイト上のユニークユーザー数を確認できます。複数の通貨が関係している場合、USDが含まれていればコストはUSDで表示されます。それ以外の場合は、リストからランダムに選択された通貨でコストが表示されます。先月および先々月と比較したコスト削減額がパーセンテージで表示されます。また、ユニークユーザー数の変化も表示されます。グラフ表示には毎月の傾向が示されます。

  ユーザーあたりの平均コストを使用して、使用状況を最適化できます。

- **コストレポート**

  選択したサービスプロバイダー、選択したデリバリーグループ、および選択したタグのコストレポートを表示できます。過去3か月分のレポートを個別に表示することも、過去3か月分のデータを統合して表示することもできます。

- **Citrix を使用したコスト削減**

  AutoscaleやMachine Creation Services™ (MCS)、Storage Optimization (MCSIO) などのCitrix機能を有効にすることで、ユーザーあたりの平均コストをさらに削減できます。また、使用していないときにマシンをシャットダウンするなど、エンドユーザーの行動を促します。

  このデータは、Citrix機能が適用された場合の合計削減額を表示します。また、エンドユーザーの行動による削減額も表示します。

- **デスクトップタイプ別のコスト**

  次の種類のデスクトップのコストを表示できます。

  - **静的永続:** ユーザーは毎回同じ仮想デスクトップにサインオンし、デスクトップに加えられた変更は保存されます。
  - **静的非永続:** ユーザーは毎回同じ仮想デスクトップにサインオンし、デスクトップに加えられた変更は保存されません。
  - **ランダム永続:** ユーザーにはデスクトッププールから仮想デスクトップが割り当てられ、デスクトップに加えられた変更は保存されます。
  - **ランダム非永続型:** ユーザーにはデスクトッププールから仮想デスクトップが割り当てられ、デスクトップに加えられた変更は保存されません。

  各マシンタイプについて、個別のユーザー数、マシン数、および月間平均稼働時間を表示できます。

このデータを使用して、ユーザーを異なる種類のデスクトップに移動することでコスト削減を計画できます。たとえば、静的永続デスクトップタイプは、ランダム非永続デスクトップと比較して、より多くのリソース使用量が必要です。そのため、一部のユーザーを静的永続デスクトップタイプからランダム非永続デスクトップタイプに移動することを計画できます。

- **OSタイプ別のコスト**

  シングルセッションおよびマルチセッションOSタイプのコストを表示できます。マシンのOSタイプ、個別のユーザー数、マシン数、および月間平均稼働時間を表示できます。このデータを使用して、ユーザーを異なる種類のOSに移動することでコストを節約する計画を立てることができます。

- **ユーザーあたりの月間最高コストによるワークロード**

  仮想マシンインスタンス、個別のユーザー数、マシンの平均稼働時間など、ユーザーあたりの月間最高コストの詳細を表示できます。また、マシン数とユーザーあたりのコストも確認できます。

  このデータを使用して、各VM構成タイプのコストを表示し、どの構成をユーザーに割り当てるかを決定します。

機能互換性マトリックス

Citrix Director 7 2503 は以下と互換性があります:

- シトリックス バーチャル アプリケーションズ アンド デスクトップス™ 7 2112 以降
- シトリックス バーチャル アプリケーションズ™ アンド デスクトップス 7 1912 LTSR

各サイト内で、Director を以前のバージョンの Delivery Controller™ とともに使用できますが、Director の最新バージョンのすべての機能が利用できるとは限りません。Citrix は、Director、Delivery Controller、および VDA を同じバージョンにすることを推奨しています。

> **注：**
>
> Delivery Controller をアップグレードした後、Studio を開くとサイトのアップグレードを促されます。詳細については、展開のアップグレード の「**アップグレードシーケンス**」セクションを参照してください。

Director のアップグレード後に初めてログインすると、構成済みのサイトでバージョンチェックが実行されます。いずれかのサイトが Director より古いバージョンの Controller を実行している場合、Director コンソールにサイトのアップグレードを推奨するメッセージが表示されます。さらに、サイトのバージョンが Director のバージョンよりも古い間は、この不一致を示すメモが Director ダッシュボードに表示され続けます。

注：

以前のバージョンの Citrix Director では、最近の VDA バージョンで実行されているユーザーセッションに適用されたポリシーは表示されません。Citrix Director 1912 およびそれ以前のバージョンでは、VDA バージョン 2003 以降で実行されているユーザーセッションに適用されたポリシーは表示されません。これらのポリシーを表示するには、Citrix Director バージョン 2003 以降を使用してください。

必要な Delivery Controller (DC)、VDA、およびその他の依存コンポーネントの最小バージョンとライセンスエディションを含む、特定の Director 機能は以下のとおりです。

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2507	監視とトラブルシューティングのためのMicrosoft通話品質ダッシュボード(/ja-jp/citrix-virtual-apps-desktops/2511/director/real-time-communication-dashboard/microsoft-teams.html)	なし	すべて
2507	垂直および水平ロードバランシングアラートの処理の改善(/ja-jp/citrix-virtual-apps-desktops/2511/whats-new#citrix-director.html)	なし	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2507	セッショントポロジで使用されるエンドポイントデータ収集のデフォルトポリシー動作の変更(/ja-jp/citrix-virtual-apps-desktops/2511/director/troubleshoot-deployments/user-issues/session-performance#end-to-end-network-hop-view.html)	なし	すべて
2507	DirectorにおけるICA RTTおよびネットワーク遅延測定の定義の強化(/ja-jp/citrix-virtual-apps-desktops/2511/director/troubleshoot-deployments/user-issues/session-performance#hdx-metrics.html)	なし	すべて
2507	リアルタイム通信アプリケーションのプラグインマネージャーと最適化状態の可視性の向上(/ja-jp/citrix-virtual-apps-desktops/2511/director/troubleshoot-deployments/user-issues/session-performance#real-time-communications-	なし	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	optimization-visibility.html)		
2503	Azureワークロードのコストモデリング(/ja-jp/citrix-virtual-apps-desktops/2511/director/cost-optimization/cost-modeling.html)	なし	すべて
2503	コスト削減ページの機能強化(/ja-jp/citrix-virtual-apps-desktops/2511/director/cost-optimization/cost-savings.html)	なし	すべて
2503	uberAgentとのDirector統合(/ja-jp/citrix-virtual-apps-desktops/2511/director/install-and-configure#citrix-uberagent-integration-with-director)	VDA 2503 (uberAgent インストール済み)	すべて
2503	ローカルアプリケーション使用状況レポート	VDA 2503	Platinumライセンスサイト
2503	VDAログオン期間の詳細の監視	VDA 2503	すべて
2503	Provisioning Serviceの追加メトリック収集	VDA 2503	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2503	Microsoft Teams以外のHDX最適化の監視を拡張するオプション](/ja-jp/citrix-virtual-apps-desktops/2511/director/troubleshoot-deployments/user-issues/session-performance#hdx-optimization-details)	VDA 2503	すべて
2503	フィルタービューとセッションパフォーマンスタブでのセッション自動再接続の詳細](/ja-jp/citrix-virtual-apps-desktops/2511/director/site-analytics/trends)	VDA 2503	すべて
2503	Citrix Directorの統合プラットフォームエクスペリエンス	なし	すべて
2503	ユーザーアクションの一括アクションオプションを制限するカスタムロール](/ja-jp/citrix-virtual-apps-desktops/2511/director/troubleshoot-deployments/user-issues/custom-role-to-limit-bulk-action)	なし	すべて
2503	Provisioning Service および Delivery Controller のサイト	VDA 2503	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	レベルのアラートを設定する機能		
2503	Webhook との統合	なし	すべて
2411	「アプリケーション」ページでの使用頻度の低い公開済みアプリと未使用の公開済みアプリのレポート	DDC 7.16 および VDAs 7.15	Platinum ライセンスサイト
2411	アクティビティマネージャーでの TCP または UDP アプリケーション向けアプリケーション詳細の列挙	VDA 2411 および DDC 2411	すべて
2411	PowerShell SDK を使用した Webhook 構成	VDA 2411 および DDC 2411	すべて
2411	一括アラート解除	VDA 2411 および DDC 2411	すべて
2411	ワークロードの適正化ページでのマシンの純アクティブ使用量	なし	すべて
2411	ストレージ使用量の最適化によるコスト削減 (プレビュー)	なし	すべて
2411	コスト概要 (プレビュー)	なし	すべて
2411	Delivery Controller の監視 (プレビュー)	VDA 2411	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2411	UI から Citrix コンポーネントを接続 (プレビュー)	VDA 2411	すべて
2407	コスト最適化	なし	すべて
2407	統合とデータエクスポート	VDA 2407	すべて
2407	過去のユーザーセッションの診断 (プレビュー)	VDA 2407	すべて
2407	Secure Private Accessセッション用アクティビティマネージャー (プレビュー)	VDA 2407	すべて
2407	Director を使用した TCP および UDP アプリの Secure Private Access 統合 (プレビュー)	VDA 2407	すべて
2407	インフラストラクチャ監視 (プレビュー)	VDA 2407	すべて
2407	未登録マシンアラート	VDA 2407 および DDC 2407	すべて
2407	マシン稼働時間アラート	VDA 2407 および DDC 2407	すべて
2407	電源オンアクションの失敗と電源オフアクションの失敗アラート	VDA 2407 および DDC 2407	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2407	アラートメールにCSV添付ファイルを含める機能とアラートWebhookにJSONペイロードを含める機能	VDA 2407 および DDC 2407	すべて
2407	最近の電源アクションを持つマシンを検査	VDA 2407	すべて
2407	高度なアラートポリシー	VDA 2407 および DDC 2407	すべて
2407	クラウドおよびオンプレミスユーザー向け統合検索	DDC 2407	すべて
2407	ダッシュボード上の公開アプリケーション使用状況監視グラフ	VDA 2407 および DDC 2407	Platinumライセンスサイト
2402 LTSR	Director を使用した Web および SaaS アプリの Secure Private Access 統合 (プレビュー)	VDA 2402 LTSR	すべて
2402 LTSR	Microsoft Teams バージョン 2.1 以前のサポート(/ja-jp/citrix-virtual-apps-desktops/2511/2402-ltsr/director/troubleshoot-deployments/user-issues#microsoft-teams-optimization-status)	VDA 2402 LTSR	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2311	ライブセッションと録画セッションの再生(/ja-jp/citrix-virtual-apps-desktops/2511/director/troubleshoot-deployments/user-issues/record-sessions#play-back-live-and-recorded-sessions)	VDA 2308 および DDC 2311	すべて
2311	セッショントポロジとパフォーマンスメトリック(/ja-jp/citrix-virtual-apps-desktops/2511/director/troubleshoot-deployments/user-issues/session-performance#session-topology)	複数のバージョン - リンク(/ja-jp/citrix-daas/monitor/troubleshoot-deployments/user-issues/session-performance#session-performance-metrics)	すべて
2311	最適な画面解像度(/ja-jp/citrix-virtual-apps-desktops/2511/system-requirements#citrix-director)	なし	すべて
2311	MS Teams の最適化	VDA 2311および DDC最新版	すべて
2311	プローブ概要の機能強化	なし	すべて
2311	セッションログオン期間ビューの刷新	なし	すべて
2308	プローブの概要とドリルダウン	なし	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2308	Citrix Gateway 多要素認証に対するCitrix Probe Agentのサポート	Citrix ゲートウェイ	すべて
2308	ハイパーバイザーアラートの無効化	なし	すべて
2308	セッションエクスペリエンスメトリックの傾向	なし	すべて
2305	Citrix Gatewayを介した認証のサポート	なし	すべて
2305	DirectorでのAutoscale管理	なし	すべて
2303	失敗したマシンのアラート	DC 7 2303	プレミアム
2203	TLS 1.3のサポート	-	すべて
2212	AMD GPUで利用可能なリアルタイムGPU使用率(/ja-jp/citrix-virtual-apps-desktops/2511/2212/director/troubleshoot-deployments/machines.html#gpu-utilization)	DC 7.14およびVDA 7.14（64ビットWindowsおよびHDX 3D Proが有効な環境で実行）	すべて
2212	高度なプローブスケジューリング(/ja-jp/citrix-virtual-apps-desktops/2511/director/probes.html)	DC 7 1906 および シトリックス プローブ エージェント 2209	プレミアム

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
1909	Citrix Analytics for Performanceでオンプレミスサイトを構成(/ja-jp/citrix-virtual-apps-desktops/2511/director/install-and-configure/onboarding.html)	DC 7 1906およびVDA 1906	すべて
1906	セッションの自動再接続(/ja-jp/citrix-virtual-apps-desktops/2511/director/site-analytics/trends.html#available-trends)	DC 7 1906およびVDA 1906	すべて
1906	セッション起動時間	DC 7 1906およびVDA 1903	すべて
1906	デスクトッププロービング	DC 7 1906 と Citrix プローブエージェント 1903	プレミアム
7.9以降	プロファイルロードにおけるCitrix Profile Managementの期間	VDA 1903	すべて
1811	プロファイルドリルダウン	DC 7 1811およびVDA 1811	すべて
1811	ハイパーバイザーアラートの監視	DC 7 1811	プレミアム
1811	アプリケーションプロービング	DC 7 1811 と Citrix アプリケーションプローブエージェント 1811	プレミアム

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
1811	Microsoft RDSライセンスの状態	DC 7 1811およびVDA 7.16	すべて
1811	主要なRTOPデータの表示	DC 7 1811 およびVDA 1808	プレミアム
1808	フィルターデータの書き出し	DC 7 1808	すべて
1808	対話型セッションのドリルダウン	DC 7 1808 およびVDA 1808	すべて
1808	GPOのドリルダウン	DC 7 1808 およびVDA 1808	すべて
1808	OData APIを使用して利用可能なマシンの履歴データ(https://developer-docs.citrix.com/projects/monitor-service-odata-api/en/)	DC 7 1808	すべて
7.18	アプリケーションプロービング(/ja-jp/citrix-virtual-apps-desktops/2511/director/probes.html)	DC 7.18	プレミアム (旧称 プラチナ)
7.18	スマートアラートポリシー(/ja-jp/citrix-virtual-apps-desktops/2511/director/site-analytics/alerts-notifications.html#smart-alert-policies)	DC 7.18	プレミアム (旧称 プラチナ)

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.18	ヘルスアシスタントリンク(/ja-jp/citrix-virtual-apps-desktops/2511/director/troubleshoot-deployments/machines.html)	なし	すべて
7.18	インタラクティブセッションのドリルダウン	なし	すべて
7.17	PIVスマートカード認証	なし	すべて
7.16	アプリケーション分析	DC 7.16およびVDA 7.15	すべて
7.16	OData API バージョン4	DC 7.16	すべて
7.16	Shadow Linux VDA ユーザー	VDA 7.16	すべて
7.16	ドメインローカルグループのサポート	なし	すべて
7.16	マシンコンソールアクセス	DC 7.16	すべて
7.15	アプリケーション障害監視	DC 7.15およびVDA 7.15	すべて
7.14	アプリケーション中心のトラブルシューティング	DC 7.13およびVDA 7.13	すべて
7.14	ディスク監視	DC 7.14およびVDA 7.14	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.14	GPU監視	DC 7.14およびVDA 7.14	すべて
7.13	セッション詳細パネルの転送プロトコル(/ja-jp/citrix-virtual-apps-desktops/2511/director/site-analytics.html#session-transport-protocol)	DC 7.x および VDA 7.13	すべて
7.12	ユーザーフレンドリーな接続およびマシンの障害の説明(/ja-jp/citrix-virtual-apps-desktops/2511/director/site-analytics/filters-data.html)	DC 7.12 および VDA 7.x	すべて
7.12	Enterpriseエディションでの履歴データの可用性の増加(/ja-jp/citrix-virtual-apps-desktops/2511/director/site-analytics/trends.html)	DC 7.12 および VDA 7.x	エンタープライズ
7.12	カスタムレポート(/ja-jp/citrix-virtual-apps-desktops/2511/director/site-analytics/trends.html)	DC 7.12 および VDA 7.x	プレミアム (旧プラチナ)
7.11	リソース使用率レポート(/ja-jp/citrix-virtual-apps-desktops/2511/director/site-analytics/trends.html)	DC 7.11およびVDA 7.11	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.11	CPU、メモリ、ICA RTT条件に対するアラート機能の拡張(/ja-jp/citrix-virtual-apps-desktops/2511/director/site-analytics/alerts-notifications.html)	DC 7.11およびVDA 7.11	プレミアム (旧 Platinum)
7.11	レポートのエクスポート機能の改善(/ja-jp/citrix-virtual-apps-desktops/2511/director/site-analytics.html#export-reports)	DC 7.11およびVDA 7.x	すべて
7.11	Citrix ADMとの統合(/ja-jp/citrix-virtual-apps-desktops/2511/director/install-and-configure/hdx-insight.html)	DC 7.11、VDA 7.x、およびMASバージョン11.1ビルド49.16	プレミアム (旧プラチナ)
7.9	ログオン期間の内訳	DC 7.9 および VDA 7.x	すべて
7.7	プロアクティブな監視とアラート	DC 7.7 および VDA 7.x	プレミアム (旧プラチナ)
7.7	Windows 認証統合	DC 7.x および VDA 7.x	すべて
7.7	シングルセッションおよびマルチセッション OS の使用状況	DC 7.7 および VDA 7.x	プレミアム (旧 プラチナ)
7.6.300	Framehawk仮想チャネルのサポート	DC 7.6 および VDA 7.6	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.6.200	セッション記録の統合	DC 7.6 および VDA 7.x	プレミアム (旧 プラチナ)
7	HDX Insightの統合	DC 7.6、VDA 7.x、およびCitrix ADM	プレミアム (旧 プラチナ)

データ粒度と保持

データ値の集計

Monitor Serviceは、ユーザーセッションの使用状況、ユーザーログオンパフォーマンスの詳細、セッション負荷分散の詳細、接続およびマシン障害情報など、さまざまなデータを収集します。データはカテゴリに応じて異なる方法で集計されます。OData Method APIを使用して提示されるデータ値の集計を理解することは、データを解釈するために不可欠です。例:

- 接続されたセッションとマシン障害は一定期間に発生します。したがって、それらは期間中の最大値として公開されます。
- ログオン期間は時間の長さを測定するものであるため、期間中の平均値として公開されます。
- ログオン数と接続障害は一定期間に発生した回数であるため、期間中の合計値として公開されます。

同時データ評価

セッションは、同時と見なされるためには重複している必要があります。ただし、時間間隔が1分の場合、その1分間のすべてのセッション（重複しているかどうかに関わらず）は同時と見なされます。間隔のサイズが非常に小さいため、精度を計算するのに伴うパフォーマンスオーバーヘッドは、追加される価値に見合いません。セッションが同じ時間内に発生しても、同じ分内に発生しない場合、それらは重複しているとは見なされません。

サマリーテーブルと生データの相関

データモデルは、メトリックを2つの異なる方法で表します。

- サマリーテーブルは、分、時間、日ごとの時間粒度でメトリックの集計ビューを表します。
- 生データは、セッション、接続、アプリケーション、およびその他のオブジェクトで追跡される個々のイベントまたは現在の状態を表します。

API呼び出し間またはデータモデル自体内でデータを関連付けようとする場合、以下の概念と制限を理解することが重要です。

- **部分的な間隔のサマリーデータはありません。** メトリックのサマリーは、長期間にわたる履歴トレンドのニーズを満たすように設計されています。これらのメトリックは、完全な間隔についてサマリーテーブルに集計されます。データ収集の開始時（利用可能な最も古いデータ）にも終了時にも、部分的な間隔のサマリーデータはありません。1日の集計（Interval=1440）を表示する場合、これは最初と最新の不完全な日にはデータがないことを意味します。これらの部分的な間隔に生データが存在する可能性はありますが、それは決して要約されません。特定のデータ粒度について、特定のサマリーテーブルから最小および最大のSummaryDateを抽出することで、最も早いおよび最も遅い集計間隔を決定できます。SummaryDate列は間隔の開始を表します。Granularity列は、集計データの期間の長さを表します。
- **時間による相関。** メトリックは、前述のセクションで説明されているように、完全な間隔についてサマリーテーブルに集計されます。これらは履歴トレンドに使用できますが、生イベントはトレンド分析のために要約されたものよりも現在の状態をより正確に反映している可能性があります。サマリーと生データの時間ベースの比較では、発生する可能性のある部分的な間隔や期間の開始と終了にはサマリーデータがないことを考慮する必要があります。
- **見逃されたイベントと潜在イベント。** イベントが見逃されたり、集計期間に対して潜在的であったりすると、サマリーテーブルに集計されるメトリックがわずかに不正確になる可能性があります。モニターサービスは正確な現在の状態を維持しようとしますが、見逃されたイベントや潜在イベントのためにサマリーテーブルの集計を再計算するために過去に戻ることはありません。
- **接続の高可用性。** 接続の高可用性中、現在の接続のサマリーデータカウントにギャップが生じますが、セッションインスタンスは引き続き生データで実行されます。
- **データ保持期間。** サマリーテーブルのデータは、生イベントデータのスケジュールとは異なるグルーミングスケジュールで保持されます。データがサマリーテーブルまたは生テーブルからグルーミングされたために、データが欠落している可能性があります。保持期間は、サマリーデータの粒度によって異なる場合もあります。粒度の低いデータ（分単位）は、粒度の高いデータ（日単位）よりも早くグルーミングされます。グルーミングによってある粒度からデータが欠落している場合でも、より高い粒度で見つかる可能性があります。API呼び出しは要求された特定の粒度のみを返すため、ある粒度でデータが受信されないからといって、同じ期間のより高い粒度でデータが存在しないという意味ではありません。
- **タイムゾーン。** メトリックはUTCタイムスタンプで保存されます。サマリーテーブルは、時間単位のタイムゾーン境界で集計されます。時間単位の境界に該当しないタイムゾーンの場合、データが集計される場所に関して多少の不一致が生じる可能性があります。

粒度と保持

Directorによって取得される集計データの粒度は、要求された時間 (T) スパンの関数です。ルールは次のとおりです。

- 0 \< T \<= 1 時間 - 分単位の粒度を使用
- 0 \< T \<= 30 日 - 時間単位の粒度を使用
- T \> 31 日 - 日単位の粒度を使用

集計データから取得されない要求データは、生のセッションおよび接続情報から取得されます。このデータは急速に増加する傾向があるため、独自のグルーミング設定があります。グルーミングにより、関連データのみが長期的に保持されます。グルーミングは、レポートに必要な粒度を維持しながら、パフォーマンスを向上させます。Premiumライセンスサイトのお客様は、グルーミング保持を希望する保持日数に変更できます。変更しない場合は、デフォルトが使用されます。サイトデータベースとの接続が失われた場合、モニターサービスは以下の表で指定されているPremiumエンタイトルメントのデフォルトの保持日数を使用します。

設定にアクセスするには、Delivery Controller™で次のPowerShellコマンドを実行します。

```
asnp Citrix.*

 Get-MonitorConfiguration

 Set-MonitorConfiguration -<setting name> <value>
```

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	プレミアムの保持日数	アドバンストの保持日数
1	GroomSessionsRetentionDays	MonitorData.SessionおよびMonitordata.Connectionテーブル	この設定は、セッションの詳細、ユーザーセッションごとのログオン期間、トレンドページ上のアプリケーション	90	31

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	プレミアムの保持日数	アドバンストの保持日数
			ベースの使用状況テーブルに影響します。		
2	GroomFailuresRetentionDays	MonitorData.MachineFailureLogおよびMonitorData.ConnectionFailureLog	トレンドページ: この設定は、障害タブ上のチャートとテーブルに影響します。	90	31
3	GroomLoadIndexesRetentionDays	MonitorData.LoadIndex	この設定は、Trendsページの「Load Evaluator Index」タブに表示されるデータに影響します。	3	3
4	GroomDeletedRetentionDays	LifecycleStateが「Deleted」であるMonitorData.Machine、MonitorData.Catalog、MonitorData.DesktopGroup、およびMonitorData.Hypervisorエンティ	LifecycleStateが「Deleted」であるMachine、Catalog、DesktopGroup、およびHypervisorエンティティ。この設定は、関連するSession、	90	31

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	プレミアムの保持日数	アドバンストの保持日数
		ティ。この設定は、関連するSession、SessionDetail、Summary、Failure、またはLoadIndexレコードも削除します。	SessionDetail、Summary、Failure、またはLoadIndexレコードも削除します。		
5	GroomSummariesRetentionDays	MonitorData.DesktopGroupSummary、MonitorData.FailureLogSummary、およびMonitorData.LoadIndexSummary	この設定は、Trendsページのすべてのグラフデータに影響します。	365	31
6	GroomMachineHotfixLogRetentionDays	MonitorData.Hotfix	この設定は、マシン詳細ページに表示されるVDAホットフィックスデータに影響します。	90	31

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	プレミアムの保持日数	アドバンストの保持日数
7	GroomMinuteRetentionDays	すべての概要テーブル	この設定は、トレンドページに表示される「過去2時間」の時間期間のグラフに影響します。	3	3
8	GroomHourlyRetentionDays	すべての概要テーブル	これは、トレンドページに表示される週次グラフに影響します。	32	31
9	GroomApplicationInstanceRetentionDays	MonitorData.ApplicationInstance	この設定は、キャパシティ管理タブのグラフとテーブル、およびトレンドページのアプリケーション使用状況テーブルに影響します。	90	該当なし
10	GroomNotificationLogRetentionDays	MonitorData.NotificationLog	この設定は、Monitorに表示されるアラートに影響します。	90	該当なし

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	プレミアムの保持日数	アドバンストの保持日数
11	GroomResourceUsageRawDataRetentionDays	MonitorData.Resourceutilization	この設定は、「Historical Machine Utilization」マシン詳細ページに表示されるCPUおよびメモリチャートと、コスト最適化領域の「Workload rightsizing tab」でのデータ計算に影響します。	3	3
12	GroomResourceUsageMinuteDataRetentionDays	MonitorData.ResourceUtilizationSummary	この設定は、「Historical Machine Utilization」マシン詳細ページに表示される「Last 2 Hours」期間のCPUおよびメモリチャートと、コスト最適化領域の「Workload	7	7

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	プレミアムの保持日数	アドバンストの保持日数
			rightsizing tab」でのデータ計算に影響します。		
13	GroomResourceUsageHourDataRetentionDays	MonitorData.Resourceutilizationsummary	この設定は、「履歴マシン使用率」のマシン詳細ページに表示されるCPUおよびメモリチャートと、コスト最適化領域の「ワークロードの適正化タブ」でのデータ計算に影響します。	30	30
14	GroomResourceUsageDayDataRetentionDays	MonitorData.Resourceutilizationsummary	この設定は、トレンドページの「リソース使用率」のマシンに表示されるCPUおよびメモリチャートと、特定のマシンの「マシン使用率」ペー	365	31

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	プレミアムの保持日数	アドバンストの保持日数
			ジに影響します。		
15	GroomProcessUsageRawDataRetentionDays	MonitorData.ProcessUtilization	この設定は、マシンの履歴使用状況ページに表示されるプロセスごとのリソーストレンド情報に影響します。	1	1
16	GroomProcessUsageMinuteDataRetentionDays	MonitorData.ProcessUtilizationMinuteSummary	この設定は、履歴マシン使用率ページに表示される「過去2時間」のプロセスごとのCPUおよびメモリ使用量チャートに影響します。	3	3
17	GroomProcessUsageHourDataRetentionDays	MonitorData.ProcessUtilizationHourSummary	この設定は、マシン履歴使用状況ページに表示されるプロセスごとのCPUおよびメモリ使用量の傾	7	7

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	プレミアムの保持日数	アドバンストの保持日数
			向に影響します。		
18	GroomProcessUsageDayDataRetentionDays	MonitorData.ProcessUtilizationDaySummary	この設定は、マシンの履歴使用状況ページに表示されるプロセスごとのCPUおよびメモリ使用量の傾向に影響します。	30	30
19	GroomSessionMetricsDataRetentionDays	MonitorData.Sessionmetrics	この設定は、ユーザー詳細ページの「セッションパフォーマンス」タブに表示されるすべてのグラフに影響します。	1	1
20	GroomMachineMetricDataRetentionDays	MonitorData.Machinemetrics	この設定は、トレンドページの「リソース使用率」タブにあるグラフと表に影響します。	3	3

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	プレミアムの保持日数	アドバンストの保持日数
21	GroomMachineMetricDaySummaryDataRetentionDays	MonitorData.MachineMetricDaySummary	この設定は、トレンドページの「リソース使用率」タブにあるグラフと表に影響します。	365	31
22	GroomApplicationErrorsRetentionDays	MonitorData.ApplicationError	この設定は、アプリケーションページの「アプリケーションエラー」列に表示されるエラーの詳細に影響します。	1	1
23	GroomApplicationFaultsRetentionDays	MonitorData.Applicationfailure	この設定は、アプリケーションページ上の「アプリケーション障害」列に影響します。	1	1

注意:

> Monitor Serviceデータベースの値を変更した場合、新しい値を有効にするにはサービスを再起動する必要があります。Monitor Serviceデータベースへの変更は、Citrixサポートの指示の下でのみ行うことをお勧めします。

> 設定GroomProcessUsageRawDataRetentionDays、GroomResourceUsageRawDataRetentionDays、およびGroomSessionMetricsDataRetentionDaysはデフォルト値の1に制限されており、GroomProcessUsageMinuteDataRetentionDaysはデフォルト値の3に制限されています。プロセス使用状況データは急速に増加する傾向があるため、これらの値を設定するPowerShellコマンドは無効になっています。 また、ライセンスベースの保持設定は次のとおりです。

- **Premiumライセンスサイト -** すべての設定のグルーミング保持期間は1000日（Citrixは365日を推奨）に制限されています。
- **Advancedライセンスサイト -** すべての設定のグルーミング保持期間は31日に制限されています。
- **その他のすべてのサイト -** すべての設定のグルーミング保持期間は7日に制限されています。

例外:

- GroomApplicationInstanceRetentionDaysはPremiumライセンスサイトでのみ設定できます。
- Premiumライセンスサイトでは、GroomApplicationErrorsRetentionDaysとGroomApplicationFaultsRetentionDaysは31日に制限されています。

長期間データを保持すると、テーブルサイズに以下の影響があります:

- **時間単位のデータ。** 時間単位のデータがデータベースに最大2年間保持される場合、1000のデリバリーグループを持つサイトでは、データベースが次のように増加する可能性があります。

  1000のデリバリーグループ x 24時間/日 x 365日/年 x 2年 = 17,520,000行のデータ。集計テーブルにこれほど大量のデータがあると、パフォーマンスへの影響は甚大です。ダッシュボードのデータはこのテーブルから取得されるため、データベースサーバーへの要件は大きくなる可能性があります。過度に大量のデータは、パフォーマンスに劇的な影響を与える可能性があります。
- **セッションおよびイベントデータ。** セッションが開始され、接続/再接続が行われるたびに収集されるデータです。大規模なサイト（10万ユーザー）では、このデータは急速に増加します。例えば、これらのテーブルの2年分のデータは1TBを超え、ハイエンドのエンタープライズレベルのデータベースが必要になります。

Citrix Director の障害理由とトラブルシューティング

以下の表は、さまざまな障害カテゴリ、その理由、および問題を解決するために必要なアクションについて説明しています。詳細については、「列挙型、エラーコード、および説明」を参照してください。

接続障害エラー

カテゴリ	理由	問題	アクション
該当なし	[0] 不明。このエラーコードはマッピングされていません。	監視サービスは、ブローカリングサービスから共有された情報から、報告された起動または接続障害の理由を特定できません。	コントローラでCDFログを収集し、Citrixサポートに連絡してください。
[0] なし	[1] なし	なし	該当なし
[2] MachineFailure	[2] SessionPreparation	デリバリーコントローラーからVDAへのセッション準備要求が失敗しました。考えられる原因: コントローラーとVDA間の通信の問題、Broker Serviceが準備要求の作成中に発生した問題、またはVDAが要求を受け入れない原因となるネットワークの問題です。	コントローラーとVDA間の通信の問題を引き起こす一般的な問題については、ナレッジセンターの記事、Citrix Virtual Apps and Desktopsにおけるデリバリーコントローラーへの Virtual Delivery Agent登録のトラブルシューティングに記載されているトラブルシューティング手順を参照してください。
[2] MachineFailure	[3] RegistrationTimeout	VDAは電源がオンになっていましたが、デリバリーコントローラーへの登録を試行中にタイムアウトが発生しました。	デリバリーコントローラーでCitrix Broker Serviceが実行されていること、およびVDAでDesktopサービスが

カテゴリ	理由	問題	アクション
			実行されていることを確認してください。停止している場合は、それぞれを開始してください。
[1] ClientConnectionFailure	[4] ConnectionTimeout	VDAがセッション起動のために準備された後、クライアントがVDAに接続しませんでした。セッションは正常に仲介されましたが、クライアントがVDAに接続するのを待っている間にタイムアウトが発生しました。考えられる原因: ファイアウォール設定、ネットワークの中断、またはリモート接続を妨げる設定です。	Directorコンソールで、クライアントが現在アクティブな接続を持っているかどうかを確認してください。これは、ユーザーに影響がないことを意味します。セッションが存在しない場合は、クライアントとVDAのイベントログでエラーがないか確認してください。クライアントとVDA間のネットワーク接続に関する問題を解決してください。
[4] NoLicensesAvailable	[5] ライセンス	ライセンス要求が失敗しました。考えられる原因: ライセンス数が不足しているか、ライセンスサーバーが30日以上ダウンしていることです。	ライセンスサーバーがオンラインで到達可能であることを確認します。ライセンスサーバーへのネットワーク接続の問題を解決するか、ライセンスサーバーが誤動作しているように見える場合は再起動します。環境内に十分なライセンスがあることを確認し、必要に応じて追加で割り当てます。

カテゴリ	理由	問題	アクション
[1] ClientConnectionFailure	[6] チケット発行	チケット発行中にエラーが発生しました。これは、VDAへのクライアント接続が仲介された要求と一致しないことを示しています。起動要求チケットはBrokerによって準備され、ICA®ファイルで配信されます。ユーザーがセッションを起動しようとすると、VDAはICAファイル内の起動チケットをBrokerと照合して検証します。考えられる原因：ICAファイルが破損しているか、ユーザーが不正な接続を試みている。	デリバリーグループで定義されているユーザーグループに基づいて、ユーザーがアプリケーションまたはデスクトップにアクセスできることを確認します。これが一時的な問題であるかどうかを判断するために、ユーザーにアプリケーションまたはデスクトップを再起動するように指示します。問題が再度発生する場合は、クライアントデバイスのイベントログでエラーを確認します。ユーザーが接続しようとしているVDAが登録されていることを確認します。登録されていない場合は、VDAのイベントログを確認し、登録に関する問題を解決します。
[1] ClientConnectionFailure	[7] その他	クライアントが最初にVDAに接続した後、接続シーケンスを完了する前に、セッションがVDAから終了したと報告されました。	起動前にユーザーによってセッションが終了されなかったことを確認します。セッションを再起動してみてください。問題が解決しない場合は、CDFログを収集してCitrixサポートに連絡してください。

カテゴリ	理由	問題	アクション
[1] ClientConnectionFailure	[8] GeneralFail	セッションの起動に失敗しました。考えられる原因：Brokerがまだ起動中または初期化中に仲介された起動が要求された、または起動の仲介フェーズ中に内部エラーが発生した。	Citrix Broker Serviceが実行されていることを確認し、セッションの起動を再試行します。
[5] 構成	[9] MaintenanceMode	VDA、またはVDAが属するデリバリーグループがメンテナンスモードに設定されています。	メンテナンスモードが必要かどうかを判断します。不要な場合は、該当するデリバリーグループまたはマシンでメンテナンスモードを無効にし、ユーザーに再接続を試みるよう指示します。
[5] 構成	[10] アプリケーション無効	アプリケーションは管理者によって無効にされているため、エンドユーザーはアクセスできません。	アプリケーションが本番環境で使用されることを意図している場合は、アプリケーションを有効にし、ユーザーに再接続するよう指示します。
[4] 利用可能なライセンスなし	[11] ライセンス機能拒否	使用されている機能は、既存のライセンスではカバーされていません。	既存のCitrix Virtual Apps and Desktops™ライセンスのエディションとタイプでカバーされている機能を確認するには、Citrixの営業担当者にお問い合わせください。

カテゴリ	理由	問題	アクション
[3] 利用可能な容量なし	[13] セッション制限に到達	すべてのVDAが使用中であり、これ以上セッションをホストする容量がありません。考えられる原因：すべてのVDAが使用中である（シングルセッションOS VDAの場合）、またはすべてのVDAが設定された最大同時セッション数に達している（マルチセッションOS VDAの場合）。	メンテナンスモードのVDAがないか確認します。容量を増やすために不要な場合は、メンテナンスモードを無効にします。サーバーVDAあたりのセッション数を増やすには、Citrixポリシー設定の**最大セッション数**の値を増やすことを検討してください。マルチセッションOS VDAを追加することを検討してください。シングルセッションOS VDAを追加することを検討してください。
[5] 構成	[14] DisallowedProtocol	ICAおよびRDPプロトコルは許可されていません。	デリバリーコントローラーで **Get-BrokerAccessPolicyRule** PowerShellコマンドを実行し、**AllowedProtocols** の値に目的のプロトコルがすべてリストされていることを確認します。この問題は、構成が誤っている場合にのみ発生します。
[5] 構成	[15] ResourceUnavailable	ユーザーが接続しようとしているアプリケーションまたはデスクトップは利用できません。このアプリケーションまたは	アプリケーションまたはデスクトップがまだ公開されており、VDAがメンテナンスモードではないことを確認します。

カテゴリ	理由	問題	アクション
		デスクトップが存在しないか、それを実行できるVDAがありません。考えられる原因: アプリケーションまたはデスクトップが非公開になっている、またはアプリケーションまたはデスクトップをホストしているVDAが最大負荷に達している、またはアプリケーションまたはデスクトップがメンテナンスモードに設定されている。	マルチセッションOS VDAがフルロード状態であるかどうかを判断します。その場合は、マルチセッションOS VDAをさらにプロビジョニングします。接続に利用できるシングルセッションOS VDAがあることを確認します。必要に応じて、シングルセッションOS VDAをさらにプロビジョニングします。
[5] 構成	[16] ActiveSessionReconnectDisabled	ICAセッションはアクティブで、別のエンドポイントに接続されています。しかし、**Active Session Reconnection** が無効になっているため、クライアントはアクティブなセッションに接続できません。	デリバリーコントローラーで、**Active Session Reconnection** が有効になっていることを確認します。レジストリの **HKEY_LOCAL_MACHINE\Software\Citrix\Desktop\Server** にある **DisableActiveSessionReconnect** の値が0に設定されていることを確認します。
[2] MachineFailure	[17] NoSessionToReconnect	クライアントは特定のセッションに再接続しようとしましたが、そのセッションは終了していました。	ワークスペースコントロールの再接続を再試行してください。

カテゴリ	理由	問題	アクション
[2] MachineFailure	[18] SpinUpFailed	VDAをセッション起動のために電源オンにできません。これはハイパーバイザーが報告した問題です。	マシンがまだ電源オフの状態である場合は、Citrix Studioからマシンの起動を試みてください。これが失敗した場合は、ハイパーバイザーの接続と権限を確認してください。VDAがPVSプロビジョニングされたマシンである場合は、PVSコンソールでマシンが実行中であることを確認してください。そうでない場合は、マシンにPersonal vDiskが割り当てられていることを確認し、ハイパーバイザーにログインしてVMをリセットしてください。
[2] MachineFailure	[19] 拒否	デリバリーコントローラーは、エンドユーザーからの接続に備えるようVDAに要求を送信しますが、VDAはこの要求を積極的に拒否します。	pingを使用して、デリバリーコントローラーとVDAが正常に通信できることを確認してください。通信できない場合は、ファイアウォールまたはネットワークルーティングの問題を解決してください。
[2] MachineFailure	[20] 構成セットの失敗	デリバリーコントローラーは、セッション起動中にポリシー設定やセッション情報などの必要な	-

カテゴリ	理由	問題	アクション
		構成データをVDAに送信しませんでした。考えられる原因：コントローラーとVDA間の通信の問題、構成セット要求の作成中にBroker Serviceで発生した問題、またはVDAが要求を受け入れない原因となるネットワークの問題。	
[3] NoCapacityAvailable	[21] MaxTotalInstancesExceeded	アプリケーションの最大インスタンス数に達しました。VDA上でアプリケーションの追加インスタンスを開くことはできません。この問題は、アプリケーション制限機能に関連しています。	ライセンスが許す場合、アプリケーション設定の「**同時に実行するインスタンスの数を制限する**」の値をより高い値に増やすことを検討してください。
[3] NoCapacityAvailable	[22] MaxPerUserInstancesExceeded	ユーザーがアプリケーションの複数のインスタンスを開こうとしていますが、アプリケーションはユーザーごとに単一のインスタンスのみを許可するように構成されています。この問題は、アプリケーション制限機能に関連しています。	デフォルトでは、ユーザーごとにアプリケーションのインスタンスは1つのみ許可されています。ユーザーごとに複数のインスタンスが必要な場合は、アプリケーション設定の「**ユーザーごとに1つのインスタンスに制限する**」設定をクリアすることを検討してください。

カテゴリ	理由	問題	アクション
[1] ClientConnectionFailure	[23] 通信エラー	デリバリーコントローラーがVDAに接続準備のリクエストなどの情報を送信しようとしましたが、通信中にエラーが発生しました。これはネットワーク障害が原因である可能性があります。	既に開始されている場合は、VDA上のDesktopサービスを再起動して登録プロセスを再開し、VDAが正常に登録されることを確認します。アプリケーションイベントログの詳細を通じて、VDA用に構成されたデリバリーコントローラーが正確であることを確認します。
[3] NoCapacityAvailable	[100] NoMachineAvailable 監視サービスは[12] NoDesktopAvailable をこのエラーコードに変換します。	セッションの起動に割り当てられたVDAが無効な状態であるか、利用できません。考えられる原因：VDAの電源状態が不明または利用できない、最後のユーザーセッション以降VDAが再起動されていない、現在のセッションで有効にする必要があるにもかかわらずセッション共有が無効になっている、またはVDAがデリバリーグループまたはサイトから削除された。	VDAがデリバリーグループ内にあることを確認します。そうでない場合は、適切なデリバリーグループに追加します。ユーザーが要求した公開共有デスクトップまたはアプリケーションを起動できるように、十分なVDAが登録され、準備状態にあることを確認します。VDAをホストしているハイパーバイザーがメンテナンスモードではないことを確認します。
[2] MachineFailure	[101] MachineNotFunctional. 監視サービスは [12] NoDesktopAvailable	VDAが動作していません。考えられる原因：VDAがデリバリーグループから削除された、VDAが登録解除されている、	VDAがデリバリーグループに属していることを確認します。属していない場合は、適切なデリバリーグループに追加

	をこのエラーコードに変換します。	VDAの電源状態が利用できない、またはVDAが内部的な問題を抱えている。	します。Citrix StudioでVDAが電源オンとして表示されていることを確認します。複数のマシンの電源状態が不明な場合は、ハイパーバイザーへの接続に関する問題またはホストの障害を解決します。VDAをホストしているハイパーバイザーがメンテナンスモードではないことを確認します。これらの問題が解決されたら、VDAを再起動します。

マシン障害の種類

エラーコード	エラーコードID	問題	アクション
不明	-	-	-
未登録	3	-	-
MaxCapacity（Director上では最大負荷として表示）	4	マシンが最大容量、つまりMax Load Indexに達していると報告しています。	すべてのハイパーバイザーの電源がオンになっていることを確認してください。ハイパーバイザーの容量を増やすか、ハイパーバイザーを追加することで、影響を受けるデリバリーグループにマシンを追加してください。
StuckOnBoot	2	仮想マシンが起動シーケンスを完了せず、ハイパーバイ	仮想マシンがハイパーバイザー上で正常に起動したことを確認してください。

エラーコード	エラーコードID	問題	アクション
		ザーと通信していません。	OSの問題など、仮想マシン上の他のメッセージを確認してください。ハイパーバイザーツールが仮想マシンにインストールされていることを確認してください。VDAが仮想マシンにインストールされていることを確認してください。
FailedToStart	1	仮想マシンがハイパーバイザー上で起動しようとしたときに問題が発生しました。	ハイパーバイザーログを確認してください。
なし	0	-	-

マシンの登録解除理由 (障害の種類が「未登録」または「不明」の場合に適用)

エラーコード	エラーコードID	問題	アクション
AgentShutdown	0	VDAが正常にシャットダウンされました。	既存の電源管理ポリシーに基づいてVDAがオフになっていると想定されない場合は、VDAの電源をオンにします。イベントログでエラーを確認してください。
AgentSuspended	1	VDAは休止状態またはスリープモードです。	VDAを休止モードから解除します。電源設定を通じて、Citrix Virtual Apps™および

エラーコード	エラーコードID	問題	アクション
			Desktops VDAの休止状態を無効にすることを検討してください。
IncompatibleVersion	100	Citrixプロトコルバージョンの不一致により、VDAはデリバリーコントローラーと通信できません。	VDAとデリバリーコントローラーのバージョンを合わせます。
AgentAddressResolutionFailed	101	デリバリーコントローラーがVDAのIPアドレスを解決できませんでした。	VDAマシンアカウントがADに存在することを確認します。存在しない場合は、作成します。DNS内のVDAの名前とIPアドレスが正確であることを確認します。正確でない場合は、修正します。広範囲にわたる場合は、デリバリーコントローラーのDNS設定を検証します。`nslookup`コマンドを実行して、コントローラーからのDNS解決を確認します。
[Cloud]:AgentAddressResolutionFailed	101	デリバリーコントローラーがVDAのIPアドレスを解決できませんでした。	VDAマシンアカウントがADに存在することを確認します。存在しない場合は、作成します。DNS内のVDAの名前とIPアドレスが正確であることを確認します。正確でない場合は、修正します。

エラーコード	エラーコードID	問題	アクション
AgentNotContactable	102	デリバリーコントローラーとVDA間で通信の問題が発生しました。	pingを使用して、デリバリーコントローラーとVDAが正常に通信できることを確認します。通信できない場合は、ファイアウォールまたはネットワークの問題を解決します。コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。
[Cloud]: エージェントに接続できません	102	デリバリーコントローラーとVDA間で通信の問題が発生しました。	コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Citrix Virtual Apps and Desktops でのデリバリーコントローラーへの Virtual Delivery Agent登録のトラブルシューティング (CTX136668)」に記

エラーコード	エラーコードID	問題	アクション
			載されているトラブルシューティング手順を参照してください。Citrixサポートにお問い合わせください。
エージェントのActive Directory OUが間違っています	103	Active Directoryの検出設定が誤っています。VDAレジストリで構成されているサイト固有のOU（サイトコントローラー情報がADに保存されている場所）が、別のサイト用です。	Active Directoryの構成が正しいことを確認するか、レジストリ設定を確認してください。
空の登録要求	104	VDAからデリバリーコントローラーに送信された登録要求が空でした。これは、VDAソフトウェアのインストールが破損していることが原因である可能性があります。	VDA上のDesktopサービスを再起動して登録プロセスを再開し、アプリケーションイベントログを介してVDAが正しく登録されていることを確認してください。
登録機能が不足しています	105	VDAのバージョンがデリバリーコントローラーと互換性がありません。	VDAをアップグレードするか、VDAを削除してから再インストールします。
MissingAgentVersion	106	VDAのバージョンがデリバリーコントローラーと互換性がありません。	問題がすべてのマシンに影響している場合は、VDAソフトウェアを再インストールします。
InconsistentRegistrationCapabilities	107	VDAは、その機能をブローカーに伝えることができません。これは、VDAとデリ	VDAとデリバリーコントローラーのバー

エラーコード	エラーコードID	問題	アクション
		バリーコントローラーのバージョン間の非互換性が原因である可能性があります。バージョンごとに変更される登録機能は、登録要求と一致しない形式で表現されています。	ジョンを合わせます。
NotLicensedForFeature	108	使用しようとしている機能はライセンスされていません。	Citrixライセンスエディションを確認するか、VDAを削除してから再インストールします。
[Cloud]: NotLicensedForFeature	108	使用しようとしている機能はライセンスされていません。	Citrixサポートにお問い合わせください。
サポートされていないCredentialSecurityバージョン	109	VDAとデリバリーコントローラーが同じ暗号化メカニズムを使用していません。	VDAとデリバリーコントローラーのバージョンを合わせてください。
無効な登録リクエスト	110	VDAがBrokerに登録リクエストを行いましたが、リクエストの内容が破損しているか無効です。	コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手

エラーコード	エラーコードID	問題	アクション
			順を参照してください。
シングル/マルチセッションの不一致	111	VDAのオペレーティングシステムタイプは、マシンカタログまたはデリバリーグループと互換性がありません。	VDAを、同じオペレーティングシステムを持つマシンを含む正しいマシンカタログタイプまたはデリバリーグループに追加してください。
カタログに対して機能レベルが低すぎます	112	マシンカタログが、インストールされているVDAバージョンよりも高いVDA機能レベルに設定されています。	VDAのマシンカタログ機能レベルがVDAの機能レベルと一致していることを確認します。VDAの機能レベルと一致するようにマシンカタログをアップグレードまたはダウングレードします。
FunctionalLevelTooLowForDesktopGroup	113	デリバリーグループが、インストールされているVDAバージョンよりも高いVDA機能レベルに設定されています。	VDAのデリバリーグループ機能レベルがVDAの機能レベルと一致していることを確認します。VDAの機能レベルと一致するようにマシンカタログをアップグレードまたはダウングレードします。
PowerOff	200	VDAが正常にシャットダウンされませんでした。	VDAが電源オン状態であるべき場合は、Citrix StudioからVDAを起動し、正常に起動して登録されることを確認してください。起動または登録に関する問題をトラ

エラーコード	エラーコードID	問題	アクション
			ブルシューティングします。VDAが再び稼働したら、イベントログを確認してシャットダウンの根本原因を特定するのに役立ててください。
AgentRejectedSettingsUpdate	203	Citrixポリシーなどの設定が変更または更新されましたが、VDAへの更新の送信中にエラーが発生しました。これは、更新がインストールされているVDAバージョンと互換性がない場合に発生する可能性があります。	必要に応じてVDAをアップグレードします。適用された更新がVDAバージョンでサポートされているかどうかを確認します。
SessionPrepareFailure	206	BrokerはVDAで実行されているセッションの監査を完了しませんでした。	広範囲にわたる場合は、デリバリーコントローラーでCitrix Broker Serviceを再起動してください。
[Cloud]: SessionPrepareFailure	206	BrokerはVDAで実行されているセッションの監査を完了しませんでした。	Citrixサポートにお問い合わせください。
ContactLost	207	デリバリーコントローラーがVDAとの接続を失いました。これはネットワーク障害が原因である可能性があります。	デリバリーコントローラーでCitrix Broker Serviceが実行されており、VDAでDesktopサービスが実行されていることを確認してください。停止している場合はそれぞれを起動

エラーコード	エラーコードID	問題	アクション
			してください。すでに起動している場合は、VDAでDesktopサービスを再起動して登録プロセスを再開し、VDAが正常に登録されることを確認してください。アプリケーションイベントログの詳細を通じて、VDA用に構成されたデリバリーコントローラーが正確であることを確認してください。pingを使用して、デリバリーコントローラーとVDAが正常に通信できることを確認してください。通信できない場合は、ファイアウォールまたはネットワークの問題を解決してください。
[Cloud]: ContactLost	207	デリバリーコントローラーがVDAとの接続を失いました。これはネットワーク障害が原因である可能性があります。	VDAでDesktopサービスが実行されていることを確認します。停止している場合は開始します。
BrokerRegistrationLimitReached	301	デリバリーコントローラーは、同時に登録できるVDAの構成済み最大数に達しました。デフォルトでは、デリバリーコントローラーは	サイトにデリバリーコントローラーを追加するか、サイトを作成することを検討してください。また、**HKEY_LOCAL_MACHINE\Software\Cit**

エラーコード	エラーコードID	問題	アクション
		10,000の同時VDA登録を許可します。	**rix\DesktopServer\MaxWorkers**レジストリキーを介して、デリバリーコントローラーに同時に登録できるVDAの数を増やすこともできます。詳細については、Knowledge Centerの記事「Citrix Virtual Apps and Desktopsで使用されるレジストリキーエントリ (CTX117446)」を参照してください。この数を増やすと、コントローラーにより多くのCPUおよびメモリリソースが必要になる場合があります。
SettingsCreationFailure	208	Brokerは、VDAに送信する設定と構成のセットを構築しませんでした。Brokerがデータを収集できない場合、登録は失敗し、VDAは登録解除されます。	デリバリーコントローラーのイベントログでエラーがないか確認します。ログに特定の問題が明らかでない場合は、Broker Serviceを再起動します。Broker Serviceが再起動されたら、影響を受けるVDAでDesktopサービスを再起動し、それらが正常に登録されることを確認します。
[Cloud]: SettingsCreationFailure	208	Brokerは、VDAに送信する設定と構成のセットを構築しませ	影響を受けるVDAでDesktopサービスを再起動し、それらが

エラーコード	エラーコードID	問題	アクション
		んでした。Brokerがデータを収集できない場合、登録は失敗し、VDAは登録解除されます。	正常に登録されることを確認します。Citrixサポートに連絡してください。
SendSettingsFailure	204	BrokerがVDAに設定および構成データを送信しませんでした。Brokerがデータを収集できても送信できない場合、登録は失敗します。	単一のVDAに限定される場合、VDA上のDesktopサービスを再起動して再登録を強制し、アプリケーションイベントログを介してVDAが正常に登録されることを確認します。発生したエラーをトラブルシューティングします。コントローラーとVDA間の通信問題を引き起こす一般的な問題については、ナレッジセンターの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。
AgentRequested	2	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
DesktopRestart	201	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。

エラーコード	エラーコードID	問題	アクション
DesktopRemoved	202	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
SessionAuditFailure	205	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
UnknownError	300	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
RegistrationStateMismatch	302	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
不明	-	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。

Secure Private Access と Director の統合 (プレビュー)

Secure Private Access と Director の統合により、ヘルプデスク管理者または完全な管理者は、Director 内のすべての Secure Private Access セッションを監視およびトラブルシューティングできます。この機能をサポートするには、Director、Secure Private Access、Citrix Workspace™ app、および VDA のバージョン 2402 以降を使用する必要があります。

利用可能なアクションには、以下の詳細の表示が含まれます。

- **セッションの選択**ポップアップ > **セッション**タブ > **Web SaaS およびクライアント/サーバーアプリ**の下にあるユーザーの Secure Private Access アクティブセッション
- **セッションの選択**ポップアップ > **アクセス拒否**タブの下にある Secure Private Access の失敗またはブロックされた列挙、および失敗したアプリ起動
- アクティブおよび失敗したアプリ起動のセッションとアプリケーションの詳細表示
- 失敗およびブロックされた列挙のセッションとアプリケーションの詳細表示

注:

Director との Secure Private Access 統合は、Director のフォームベース認証のみをサポートしており、統合 Windows 認証またはスマートカードベース認証はサポートしていません。

前提条件

1. この機能をサポートするには、以下を使用する必要があります。
   - Director 2402 以降のバージョン
   - Secure Private Access 2402 以降のバージョン
   - Citrix Workspace app 2402 以降のバージョン
2. Director に少なくとも1つの Citrix Virtual Apps and Desktops™ サイトが構成されていることを確認してください。
3. Secure Private Access をセットアップする](/ja-jp/citrix-secure-private-access/current-release/spa-onprem-setup-spa.html)。
4. Director サーバーが Secure Private Access サーバーへのネットワーク接続を持っていることを確認してください。

   > **注:**
   >
   > Citrix Director への接続を正常に確立するには、Secure Private Access サーバーに信頼された証明書がインストールされている必要があります。

5. Director 管理者ユーザーが次の権限を持っていることを確認します。
   a. Secure Private Access 管理コンソールで Secure Private Access のフル管理者または読み取り専用管理者。
   b. Citrix Studio コンソールで Citrix Virtual Apps™ または Desktops のヘルプデスク、フル管理者、または読み取り専用管理者。

Director を Secure Private Access で構成する

1. Directorがインストールされているマシンで、管理者としてコマンドプロンプトを開きます。
2. 次のコマンドを実行して、`DirectorConfig` ツールのパスに移動します。

```
cd c:\inetpub\wwwroot\Director\tools
```

3. Secure Private Access を構成するには、次のコマンドを実行します。

```
DirectorConfig.exe /configspa
```

4. Secure Private Access がインストールされているマシンの FQDN とポート番号を入力します。
5. Secure Private Access (サーバーまたはロードバランサー) への接続が安全であり、信頼された証明書が適用されていることを確認してください。

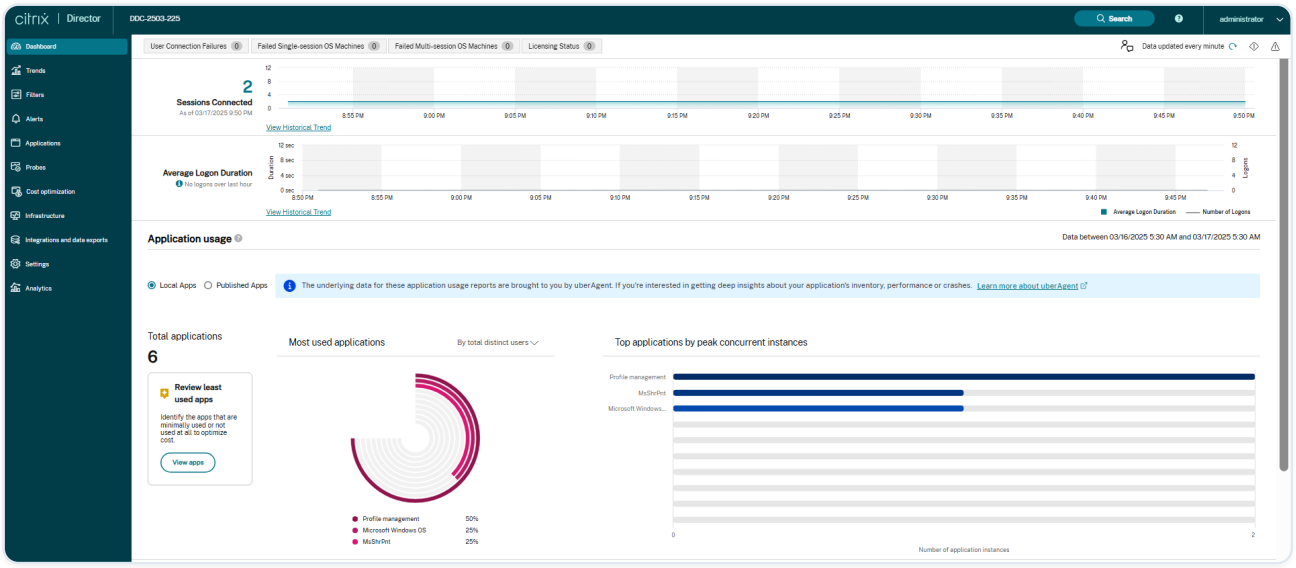


> **注:**
>
> Director で Secure Private Access セッションの詳細を表示するには、管理者を Secure Private Access コンソールに追加する必要があります。詳細については、「管理者の管理」を参照してください。

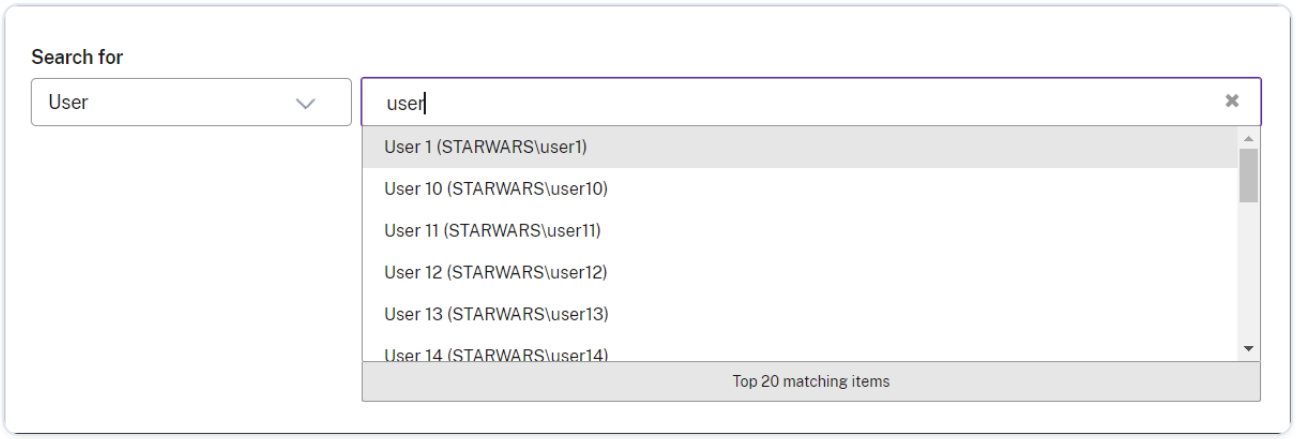
ユーザー別にSecure Private Accessセッションを表示する

Director ダッシュボードで、**「検索」をクリックし、ユーザー名を入力します。**「セッションの選択」**画面が表示されます。

フル管理者:



ヘルプデスク管理者:



Secure Private Accessセッションのアクティビティマネージャーを表示する

Citrix Directorは、Secure Private Accessセッションのアクティビティマネージャービューを提供し、セッションアクティビティの全体像を把握できます。アクティビティマネージャーは、正常に開かれた、開くのに失敗したすべてのアプリとデスクトップ、およびSecure Private Accessアプリで設定されたポリシーの結果を包括的に表示します。この機能は、Citrix Virtual Apps and Desktopsバージョン2407以降で利用できます。

前提条件:

- Director 2407以降のバージョン
- Secure Private Access 2407以降のバージョン

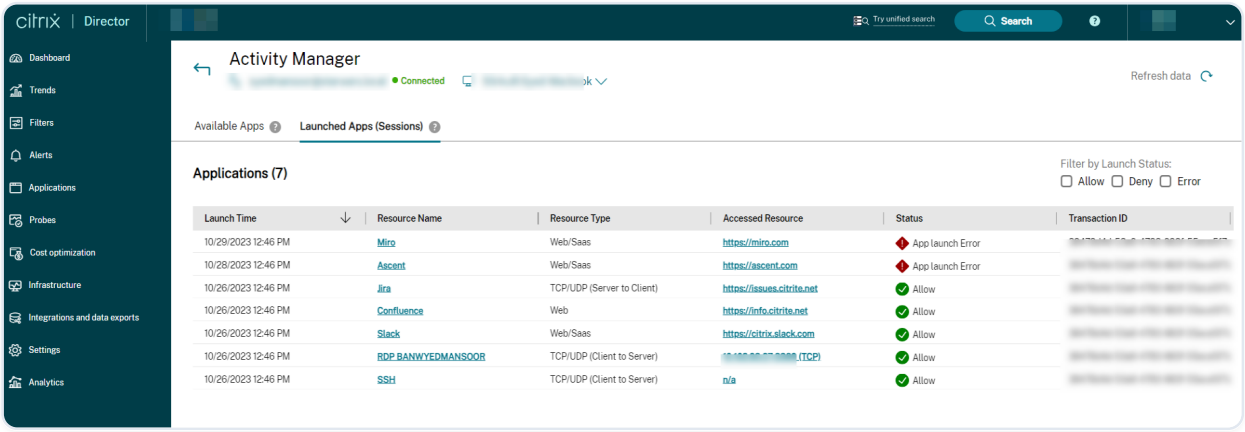
アクティビティマネージャーには、「**利用可能なアプリ**」と「**起動されたアプリ**」の詳細が表示されます。以下のセッション詳細を確認できます。

- 起動時間

- リソース名
- リソースの種類
- アクセスされたリソース
- ステータス
- トランザクションID

Activity Managerを表示するには、次の手順を実行します。

1. Directorダッシュボードで、**［検索］**をクリックし、ユーザー名を入力します。**［セッションの選択］**画面が表示されます。
2. Secure Private Accessセッションを使用して開かれたセッションを選択します。選択したセッションのアクティビティマネージャーが表示されます。



3. **［利用可能なアプリ］**をクリックして、Citrix Workspaceアプリで利用可能なアプリを表示します。

または、,

［起動されたアプリ（セッション）］をクリックして、Citrix Workspaceアプリで開かれているアプリを表示します。

Secure Private Accessアプリで設定されたリソースのステータスでリソースをフィルタリングできます。

- 許可 - ユーザーがアクセスを許可されているリソース。このステータスは、Secure Private Accessアプリのポリシーを使用して設定されます。このリソースは、Citrix Workspaceアプリでユーザーに表示されます。
- 拒否 - ユーザーがアクセスを拒否されているリソース。このステータスは、Secure Private Accessアプリのポリシーを使用して設定されます。このリソースは、Citrix Workspaceアプリでユーザーに表示されます。

- エラー - Secure Private Accessアプリでユーザーがアクセスを許可されているリソース。ただし、何らかのエラーにより、Citrix Workspaceアプリでリソースが利用できません。列挙エラーとセッションエラーの2種類のエラーがあります。

利用可能なアプリを表示

Citrix Workspaceアプリで利用可能なWebおよびSaaSアプリは、**利用可能なアプリ**セクションに表示されます。このセクションには、アプリの最後の列挙試行と、その列挙試行のステータスが表示されます。

以下の詳細を表示できます。

- リソース名
- ステータス
- トランザクションID

上記詳細を、**許可**、**拒否**、**エラー**などのアプリケーションステータスでフィルタリングすることもできます。また、上下矢印を使用して詳細を並べ替えることもできます。

> **注:**
>
> TCP/UDPアプリは、**利用可能なアプリ**セクションには表示されません。

起動されたアプリを表示

Citrix Workspaceアプリで開かれたアプリは、**起動されたアプリ (セッション)** セクションに表示されます。以下の詳細を表示できます。

- 起動時間
- リソース名
- リソースの種類
- アクセスされたリソース
- ステータス
- トランザクションID

また、**許可**、**拒否**、**エラー**などのアプリケーションステータスで、上記の詳細をフィルタリングすることもできます。上下の矢印を使用して詳細を並べ替えることもできます。

Secure Private Accessアプリのセッショントポロジビュー

Secure Private Accessを使用して開かれたアプリのセッショントポロジを表示できます。選択したアプリのセッショントポロジを表示するには、**アクティビティマネージャー**から目的のアプリをクリックします。

Web/SaaSアプリ:

WebまたはSaaSのセッショントポロジ(/en-us/citrix-virtual-apps-desktops/2511/media/spa-session-topology-web.png)

TCP/UDPアプリ:

アクティビティマネージャー(/en-us/citrix-virtual-apps-desktops/2511/media/spa-session-topology.png)

セッショントポロジビューは、アプリの起動プロセスのフローを提供します。エンドポイントはCitrix Gatewayに接続し、Citrix GatewayはSecure Private Accessプラグインに接続します。Secure Private Accessプラグインからの情報を使用して、アプリが起動されます。この機能は、Citrix Virtual Apps and Desktopsバージョン2407以降で利用できます。

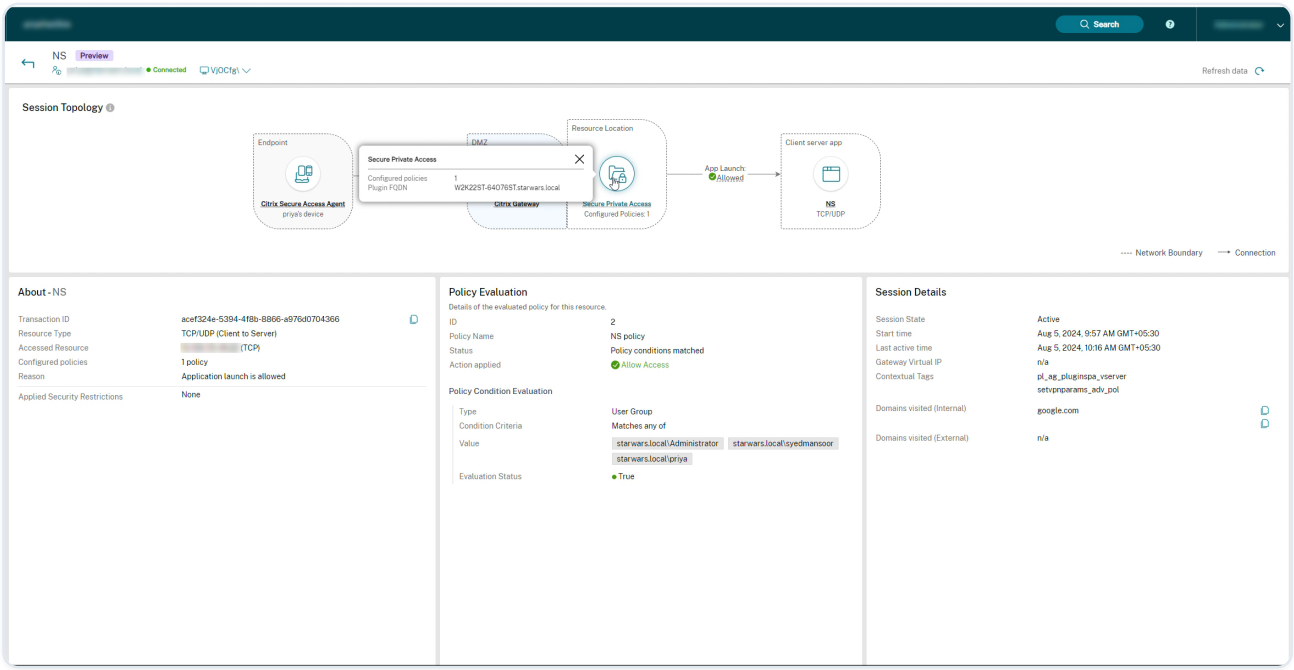
前提条件:

- Director 2407以降のバージョン
- Secure Private Access 2407以降のバージョン
- Citrix Secure Access 24.8.1.x以降のバージョン

以下を表示できます。

- エンドポイント - アプリが開かれているエンドポイントを表示します。選択肢はCitrix WorkspaceアプリとCitrix Secure Agentです。デバイスIDが表示されます。
- 内部ネットワーク - 列挙されたアプリの数と構成されたポリシーの数を表示します。
- ポリシー評価 - Secure Private Accessアプリに設定されているポリシーの結果を表示します。異なる値は、**許可**、**拒否**、**制限付きアクセス許可**、および**エラー**です。これはWebまたはSaaSアプリにのみ適用されます。
- アプリ起動 - アプリの種類とアプリ起動のステータスを表示します。アプリの種類として可能な値は、Web/SaaSアプリまたはTCP/UDPアプリです。同様に、アプリ起動ステータスとして可能な値は、**許可**、**拒否**、**制限付きアクセス許可**、および**エラー**です。

Secure Private Accessアプリの**セッション トポロジ**ビューで、以下の追加の詳細を表示できるようになりました。この変更は、TCP/UDPアプリに加えて、WebアプリとSaaSアプリの両方に適用されます。



エンドポイント:

エンドポイント内のリンクをクリックすると、以下が表示されます。

- **エンドポイントの種類:** これはSecure Access AgentまたはCitrix Workspaceアプリのいずれかです。
- **アクセス詳細:** エンドポイントがStoreFront™またはCitrix Workspaceアプリのどちらを介してアクセスされたかを表示します。
- **エンドポイントOS:** 例: Windows。
- **場所の種類:** 場所が内部か外部かを示します。

リソースの場所:

リソースの場所内のリンクをクリックすると、以下が表示されます。

> **注:** これは Web アプリと SaaS アプリにのみ適用されます。

- **列挙されたアプリケーションの数:** 列挙されたアプリケーションの数とストアURLを表示します。
- **アクセス方法:** エンドポイントがStoreFrontまたはCitrix Workspaceアプリを介してアクセスされるかどうかを示します。

セキュア プライベート アクセス:

- **構成済みポリシー:** 構成済みポリシーの数を表示します。
- **FQDN プラグイン:** リクエストを処理したエージェントの FQDN を表示します。

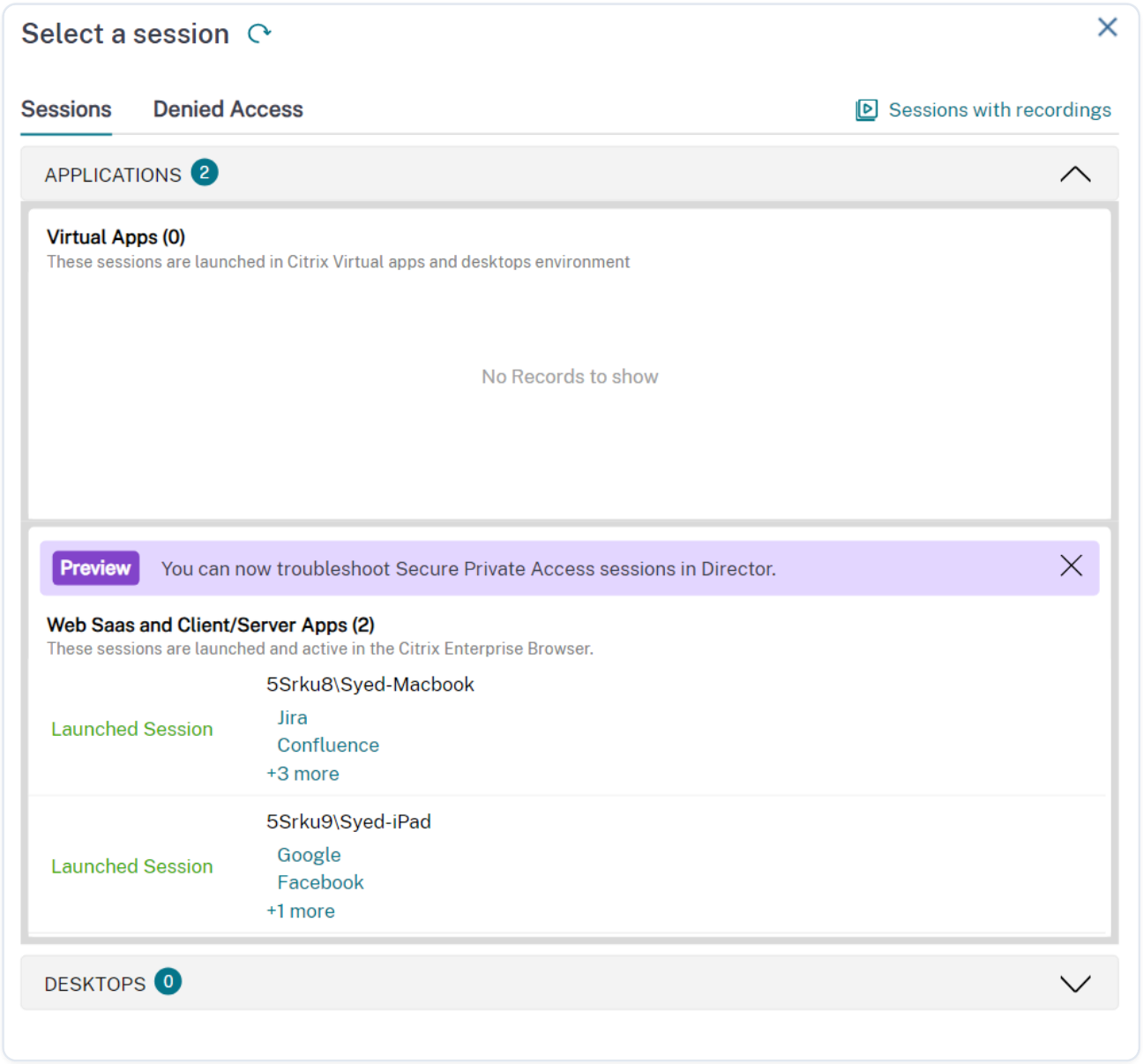
WebおよびSaaSアプリ / クライアントサーバーアプリ (TCP/UDP):

WebおよびSaaSアプリ / クライアントサーバーアプリ内のリンクをクリックすると、以下が表示されます。

- **アプリ名:** アプリの名前。
- **トップレベルURL:** WebまたはSaaSアプリの場合、公開されたアプリのURLが表示されます。TCP/UDPアプリの場合、アプリのプロトコルIPアドレスが表示されます。
- **アプリの種類:** アプリがWebまたはSaaSアプリであるか、TCP/UDPアプリであるかを示します。
- **アプリの公開タイプ:** アプリが外部公開されているか内部公開されているかを示します。

正常に起動されたWebアプリとSaaSアプリを表示する

正常に起動されたアプリは、**Web SaaSおよびクライアント/サーバーアプリ**セクションに表示されます。



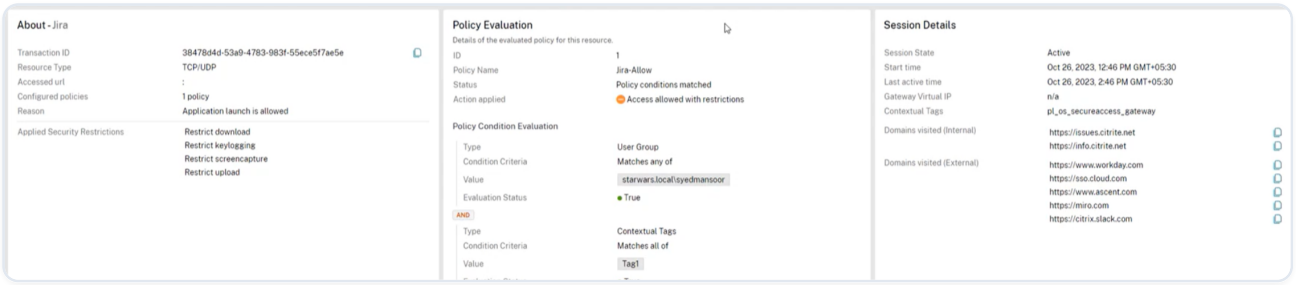
Web SaaSおよびクライアント/サーバーアプリセクションからアプリをクリックして詳細を表示します。

Director SPA の起動成功(/en-us/citrix-virtual-apps-desktops/2511/media/director-spa-successful-app.png)

成功コードの詳細については、「Citrix Director関連コード」を参照してください。

アクセスが拒否されたアプリの詳細を表示する

セッションの選択画面で**アクセス詳細の確認**をクリックします。



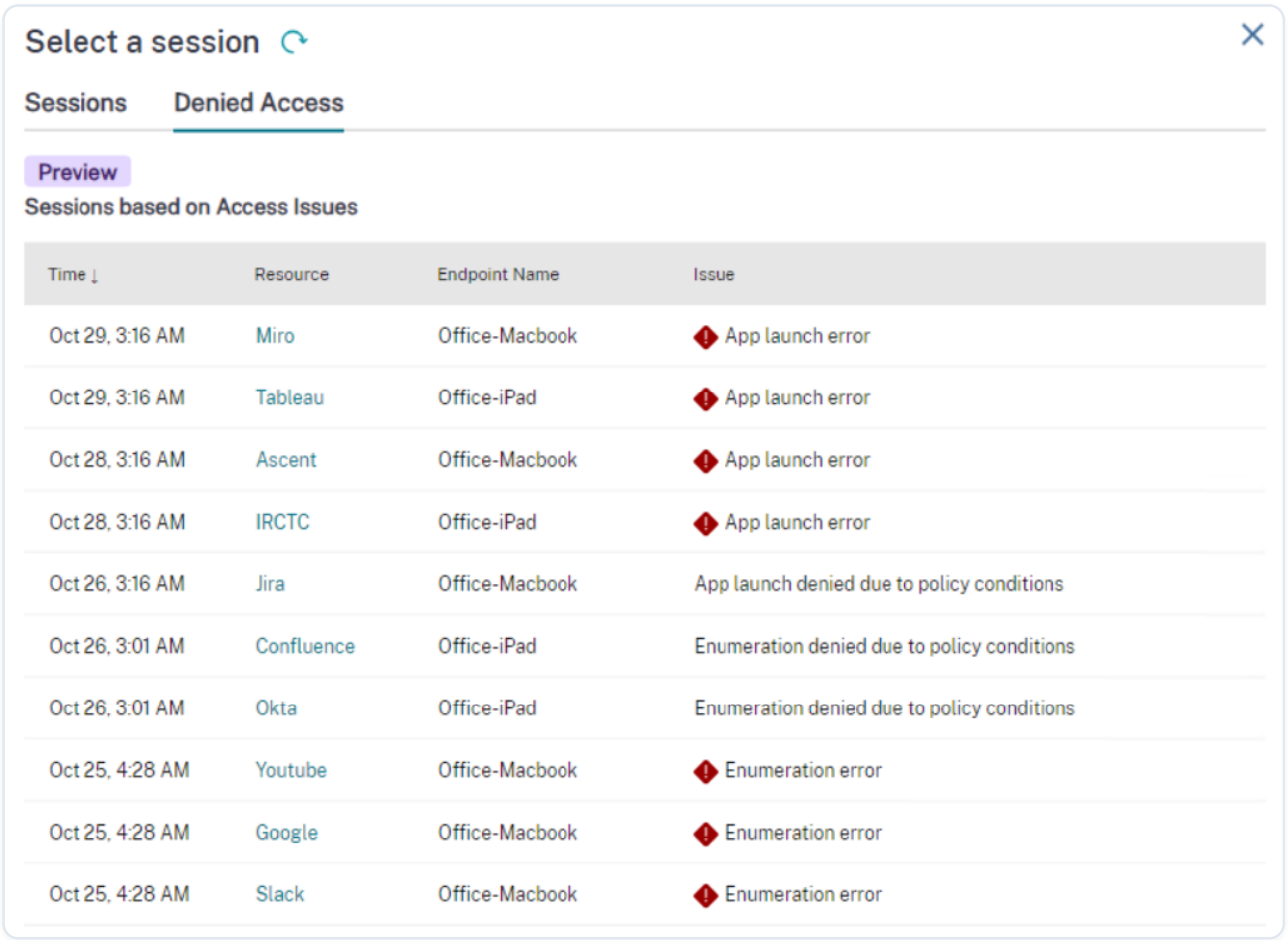
注：

アクティブなセッションがない場合、**アクセス詳細の確認**ボタンが表示されます。

または、,

アクセスが拒否されたアプリを表示するには、**アクセス拒否**タブをクリックします。

アクセス拒否タブが開きます。



時間、リソース、エンドポイント名、失敗の理由などのセッション詳細が表示されます。エラーコードの詳細については、「Citrix Director関連コード」を参照してください。

現在、以下の問題が確認されています。

- ポリシー条件により列挙が拒否されました
- アプリの起動エラー
- 列挙エラー
- ポリシー条件によりアプリの起動が拒否されました

詳細を表示するには、**Denied Access**タブ > **Resource**列からアプリを選択します。

Director SPAが詳細へのアクセスに失敗しました(/en-us/citrix-virtual-apps-desktops/2511/media/director-spa-failed-app.png)

成功または失敗したセッションについて、以下の詳細が表示されます。

- アプリについて
- ポリシー評価
- セッションの詳細

アプリについて

成功、失敗、または拒否されたアプリの名前が表示されます。それに加えて、成功または失敗したアプリの以下の詳細が表示されます。

フィールド	説明
トランザクションID	セッションまたは列挙中のCitrixトランザクションID。
リソースの種類	リソースのタイプを表示します。指定可能な値は、Web、SaaS、TCP/UDP (サーバーからクライアント)、およびTCP/UDP (クライアントからサーバー) です。
アクセスされたリソース	セッションまたは列挙中にアクセスされたリソースのURL。TCPまたはUDPアプリの場合、アクセスされたリソースのタイプがTCPかUDPかを示します。
構成済みポリシー	セッションまたは列挙内で使用されるポリシーの数。
理由	セッションまたは列挙アクティビティの分析。

フィールド	説明
適用されたセキュリティ制限	Secure Private Accessアプリに適用されているセキュリティ制限を表示します。

ポリシー評価

正常なセッションの評価中に問題が検出されなかったことを示します。失敗したセッションまたは列挙の場合、評価されたポリシーの次の詳細が表示されます。

フィールド	説明
ID	Citrix トランザクション ID。
ポリシー名	ポリシーの名前。複数のポリシーがある場合、設定された条件に一致する最初のポリシーが表示されます。
ステータス	ポリシーのステータス。
適用されたアクション	ポリシーに適用されたアクション。たとえば、アクセス拒否。
ポリシー条件の評価	
種類	ポリシー条件の種類。
条件基準	失敗したセッションまたは列挙に適用されたポリシーの条件基準。
値	ポリシーの値。
評価ステータス	ポリシーの評価ステータス。異なる値は、**許可**、**拒否**、**制限付きアクセス許可**、**エラー**です。

セッションの詳細

失敗したセッションの場合、セッション失敗の理由が表示されます。成功したセッションの場合、次の詳細が表示されます。

フィールド	説明
セッションの状態	セッションがアクティブか非アクティブか、その状態を表示します。
開始時刻	セッションの開始時刻を表示します。
最終アクティブ時刻	成功したセッションの最終アクティブ時刻を表示します。
ゲートウェイ仮想IP	正常に接続されたセッションが接続されているゲートウェイの仮想IPアドレスを表示します。
コンテキストタグ	コンテキストタグを表示します。Secure Private Accessプラグインのコンテキストタグは、認証済みユーザーのセッションに適用されるNetScaler® Gatewayポリシー（セッション、事前認証、EPA）の名前です。
アクセス済みドメイン (内部)	成功したセッションを使用してアクセスされた内部ドメインを表示します。
アクセス済みドメイン (外部)	成功したセッションを使用してアクセスされた外部ドメインを表示します。

VDA アップグレードサービス (VUS)

テクニカルプレビューの機能

テクニカルプレビューの機能は、非本番環境または限定的な本番環境で使用でき、お客様がフィードバックを共有する機会を提供します。Citrix はテクニカルプレビューの機能に関するサポートケースを受け付けていませんが、改善のためのフィードバックを歓迎します。Citrix は、フィードバックの重大度、重要度、および重要性に基づいて対応する場合があります。

これは、いかなる資料、コード、または機能を提供するというコミットメント、約束、または法的義務ではなく、Citrix製品の購入決定において依拠すべきではありません。いかなる機能の開発、リリース、および時期は、当社の単独の裁量に委ねられており、通知または協議なしに変更される場合があります。

Citrix VDA アップグレードサービスの概要

Citrix VDA アップグレードサービス (VUS) は、Citrix Virtual Apps and Desktops™ (CVAD) のコンポーネントであり、Citrix 環境内の永続的な Virtual Delivery Agent (VDA) のアップグレードプロセスを効率化します。このサービスは、環境を最新の VDA バージョンに保ち、パフォーマンスとセキュリティを強化し、新しい Citrix DaaS 機能を有効にするのに役立ちます。

管理者はVUSを活用して、更新の確認、アップグレードのスケジュール設定、アップグレードの進行状況の監視を行うことができます。アップグレードはすぐに開始することも、特定の日時にスケジュールすることもでき、これにより、アップグレードに最適な時間を選択できます。

VDAのアップグレードがこれまでになく簡単になりました。VDAまたはイメージにVDAアップグレードエージェントをインストールし、Web Studioでマシンまたはマシンカタログを右クリックして「Upgrade VDAs」を選択し、環境に最適なオプションを選択します。

アップグレードする前に、アップグレードサイクルオプションを確認してください。VDAには2つのアップグレードトラックがあります。Long-Term Service Release (LTSR) と Current Release (CR) です。LTSRはサポートライフサイクルが長く、より高い安定性とアップグレード頻度の低減を提供します。CRバージョンはより頻繁にリリースされ、最新かつ最高の機能を提供します。詳細については、 ライフサイクルマイルストーンを参照してください。

VUSを使用したVDAアップグレードの前提条件

VUSを使用してVDAアップグレードを実行するには、以下の前提条件を満たす必要があります。

サイトのVDAアップグレードサービスを有効にする

2503サイトでVUSを有効にするには、以下のPowerShellコマンドレットを実行します。

```
Set-VusSite -Enabled $true
```

有効にしたら、以下のPowerShellコマンドレットを実行して、最新のVDAバージョンをCVADサイトにインポートします。

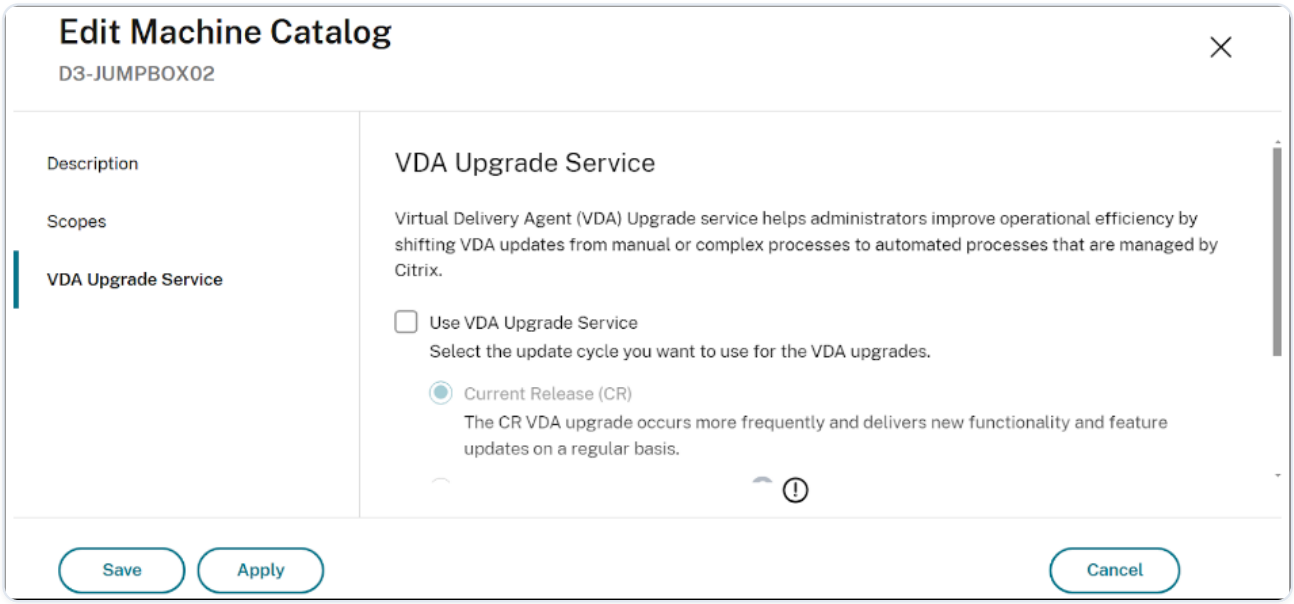
```
Import-VusVdaReleasesMetadata -Path '[<CVAD-2503-ISO>\Support\VdaUpdateServiceMetadata\vda_releases.xml]'
```

VDAアップグレードサービスを有効にする

VDAアップグレードサービス機能を有効にするには、マシンカタログの作成または編集時にVDAアップグレードオプションを使用します。管理者はVUSを有効にする際に、以下のアップグレードサイクルから選択する必要があります。

- LTSR
- CR
- LTSR 早期アクセスリリース (EAR)
- CR EAR

Web Studioからマシンカタログの VDAアップグレードサービスを有効にするには、カタログを右クリックし、「カタログの編集」をクリックし、「VDAアップグレードサービス」タブを選択し、「VDAアップグレードサービスを使用」チェックボックスをオンにし、アップグレードトラックを選択します。



PowerShell を使用してマシンカタログの VDA アップグレードサービスを有効にするには、`Set-VusCatalogUpgradeType` コマンドレットを使用します。

アップグレードタイプは、「LTSR」、「CR」、「EAR_CR」、または「EAR_LTSR」として設定できます。

例: `Set-VusCatalogUpgradeType -CatalogName "Workstation catalog" -UpgradeType LTSR`

> **注:**
>
> VDA アップグレードオプションを有効にしても、VDA の自動アップグレードは行われません。VUS を介したすべての VDA アップグレードは、管理者によって明示的に実行される個別のタスクとして開始する必要があります。

VDAの要件

VDAのバージョン

- MCS を使用して作成されたマシンの場合:
  - 2311 以降
- Websocket VDA Enrollment を使用して追加されたマシンの場合
  - 2311 以降
- 手動でプロビジョニングされたマシンの場合

- 2411 以降

プロビジョニングタイプ

- Citrix 以外のプロビジョニング™サービスまたは を使用してプロビジョニングされたシングルセッションまたはマルチセッションの永続マシン。
- シングルセッションのMCSプロビジョニングされた永続マシン (AD参加済み、Microsoft Entra参加済み、およびドメイン非参加)。
- リモートPCアクセス マシン。

VDAアップグレードエージェント

- VDAアップグレードエージェント バージョン7.44以降がVDAにインストールされ、アクティブになっている必要があります。エージェントは、次の方法でインストールできます。
  - VDAをアップグレードするとき、またはVDAのインストールを変更するときに、追加コンポーネントとして。
  - Citrix Virtual Apps and Desktops™ ISOで利用可能なスタンドアロンMSIを使用して。
    - MSI名: CitrixUpgradeAgent_x64.msi
    - パス: x64\仮想デスクトップコンポーネント

権限

CVADで、フル管理者またはマシンカタログ管理者役割が必要です。

VDAの状態

VUSを介してスケジュールされたアップグレードが意図どおりに進行するには、アップグレード対象のVDAは次の前提条件を満たしている必要があります。

- VDAは手動でメンテナンスモードに設定されていない必要があります。
- VDAアップグレードを正常に実行するには、ユーザーがログオンしていない必要があります。
  - アップグレードプロセスがアップグレード期間中にユーザーセッションのドレインを開始すると、VDAはメンテナンスモードに設定されます。アップグレードが正常に完了すると、メンテナンスモードから解除されます。
  - アップグレードウィンドウの期間中、ユーザーがアクティブまたは切断されたセッションを持っている場合、アップグレードはアップグレードウィンドウの終了時にキャンセルされます。

> **注:**
>
> アクティブおよび切断されたセッションは、VUS の強制ログオフオプションを使用して終了できます。

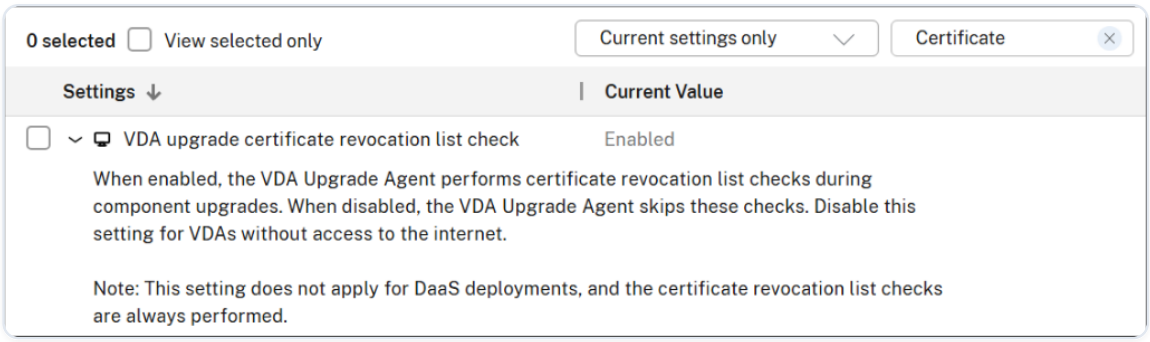
- MCS を介してプロビジョニングされていない VDA (手動でプロビジョニングされたもの) は、VUS を介してアップグレードを実行する前に、デリバリーグループに追加する必要があります。
- VDA は電源がオンになっている必要があります。

> **注:**
>
> VDA のアップグレードがスケジュールされている場合でも、AutoScale™ はマシンの電源管理を停止しません。アップグレードの進行中は、デリバリーグループの AutoScale スケジュールを無効にすることを検討してください。

接続

- VDA のアップグレードには、VDA が HTTPS 経由でデリバリーコントローラーと通信できる必要があります。
  - VDA インストーラーが有効な証明書で署名されていることを確認するには、VDA は次の URL と通信できる必要があります。
    - `<http://crl3.digicert.com/>` *
    - `<http://crl4.digicert.com/>` *
    - `<http://ocsp.digicert.com/>` *
    - `<http://cacerts.digicert.com/>` *
- VDA がインターネットにアクセスできない場合は、証明書失効リスト (CRL) をバイパスするように VDA を構成します。
  - 「VDAアップグレード証明書失効リストチェック」Citrix®ポリシー設定を無効にし、デリバリーグループに割り当てます。
    - ポリシーの説明:

- 有効にすると、VDAアップグレードエージェントはコンポーネントのアップグレード中に証明書失効リストチェックを実行します。
- 無効にすると、VDAアップグレードエージェントはこれらのチェックをスキップします。インターネットにアクセスできないVDAの場合は、この設定を無効にします。



プロキシ構成を持つVDA

- ホスト名:ポート (IP:ポート) およびPACファイルの形式のプロキシのみがサポートされています。SOCKS5プロキシはサポートされていません。
- VDAアップグレードエージェントは、Web Studioまたはレジストリを使用してプロキシを使用するように構成する必要があります。
  - Web Studioを使用したVDAアップグレードエージェントのプロキシ構成。
    - プロキシを使用するVDAに対して、「VDAアップグレードプロキシ構成」Citrixポリシー設定を有効にします。
    - 設定でプロキシアドレスまたはPACファイルへのパスを入力します。
  - レジストリを使用したVDAアップグレードエージェントのプロキシ構成
    - **キー:** `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`
      - **値の型:** `String`
      - **値の名前:** `ProxySettings`
      - **値のデータ:** プロキシアドレスまたはPACファイルへのパス。
        - 例:
          - **プロキシアドレス:** `http://<URL or IP>:\<port>`
          - **PACファイル:** `http://<URL or IP>/\<path/\<filename>.pac`

VDAWorkstationCoreSetup.exe を使用してインストールされた VDA

VDA が VDAWorkstationCoreSetup.exe を使用して最初にインストールされた場合でも、`VDAWorkstationSetup.exe` を利用する VUS を使用してアップグレードできます。

VUS を使用して `VDAWorkstationCoreSetup.exe` でインストールされた VDA をアップグレードする場合、インストールオプションを確認して、必要な機能のみが有効になっていることを確認する必要があります。特に、最小限のコアインストールから移行する場合は注意が必要です。

VUS を使用して VDA をアップグレードする

ターゲットのマシンカタログ、個々のマシン、またはマシンのグループを選択し、「VDAのアップグレード」を選択することで、VDAアップグレードサービスを通じてVDAアップグレードを開始できます。

> **注:**
>
> Citrix® は、可能な場合はアップグレードを実行する前に VDA をバックアップすることを推奨します。

アップグレードのスケジュール設定

Citrix の VDA アップグレードプロセスは、要件に応じて、カタログレベル、マシンのグループレベル、または個々のマシンレベルで実行できます。アップグレードはすぐに開始するように設定することも、最大 7 日前までに日時を指定してスケジュールすることもできます。

考慮事項

- **カタログ vs. マシンのグループ vs. マシンのスコープ:** カタログのアップグレードは一括更新に最適ですが、個別にまたはグループでマシンをアップグレードすると、よりきめ細かな制御が可能になります。
- **スケジュール設定:** アップグレードは最大7日前までにスケジュールできます。マシンカタログレベルのアップグレードを使用する場合、アップグレードがスケジュールされた後にカタログに追加されたマシンは、既存のスケジュールされたアップグレードの一部として含まれません。

主な違い

機能	カタログごとのアップグレード	マシンごとのアップグレード	マシンのグループ
アップグレードの範囲	カタログ全体	個々のマシン	マシンカタログからのマシンのグループ
スケジュール制御	単一のスケジュールがマシンカタログ内のすべてのVDAに適用され、大規模なアップグレード操作に最適です	VDAは個別にスケジュールされ、主にテストや1回限りのアップグレードに使用されます	VDAはグループでスケジュールされ、異なるVDAグループを異なる時間にアップグレードする柔軟性を提供します
管理	Web Studioのマシンカタログノードまたは `New-VusCatalogSchedule` コマンドレットを介して管理されます	Web Studioの検索ノードまたは `New-VusMachineUpgrade` コマンドレットを介して管理されます	Web Studioの検索ノードを介して、またはマシンのリストを `New-VusMachineUpgrade` コマンドレットに渡すことによって管理されます
ユースケース	マシンカタログ全体のバルクアップグレード	ターゲットアップグレードおよびテストシナリオのためのきめ細かな制御	VDAのサブセットのターゲット制御。カタログ内のアップグレードを段階的に実行するために使用できます
利用可能なVDAバージョン	CRおよび現在サポートされているすべてのLTSR VDAバージョンでは、最新バージョンと2つ前のバージョン (N-2) にアップグレードできます。詳細については、「利用可能なVDAバージョン」を参照してください。	CRおよび現在サポートされているすべてのLTSR VDAバージョンでは、最新バージョンと2つ前のバージョン (N-2) にアップグレードできます。詳細については、「利用可能なVDAバージョン」を参照してください。	最新のLTSRまたはCR VDAバージョンのみアップグレード可能です。

機能	カタログごとのアップグレード	マシンごとのアップグレード	マシンのグループ
追加コンポーネント	各VDAにVDAコンポーネントをインストールまたはアップグレードします。コンポーネントのチェックを外しても機能はアンインストールされませんが、そのコンポーネントはアップグレードされません。	VDAにVDAコンポーネントをインストールまたはアップグレードします。コンポーネントのチェックを外しても機能はアンインストールされませんが、そのコンポーネントはアップグレードされません。	マシンのグループをアップグレードする場合、追加コンポーネントはVDAアップグレードサービスで管理できません。注：「復元クリーンアップを有効にする」などの追加機能は、マシンのグループのアップグレードで利用できます。
追加機能	追加機能を有効またはアップグレードできます。	追加機能を有効またはアップグレードできます。	追加機能を有効またはアップグレードできます。
同時実行	アップグレードのスケジュール設定時に設定として制御されます。詳細については、「同時実行」を参照してください。	単一のVDAがアップグレードされます。	アップグレードスケジュールの一部として選択されたVDAの数に基づいて、自動的に負荷分散されます
失敗しきい値	指定された数のVDAのアップグレードが失敗した場合に、それ以降のアップグレードを防止するために、失敗しきい値を設定できます。詳細については、失敗しきい値を参照してください。	失敗しきい値は、マシンごとのアップグレードには適用されません。	失敗しきい値は、マシンのグループのアップグレードには利用できません。アップグレードするマシンのグループのサイズを、許容できる失敗数となるVDAの最大数に設定することを検討してください。

スケジュールされたアップグレードの仕組み

VDA上のVDAアップグレードエージェントは、VDAをアップグレードする必要があるかどうかを判断するために、定期的にDelivery Controllerと通信します。 VDAは、すぐにアップグレードするように、または最大7日前にアップグレードするようにスケジュールできます。事前にアップグレードをスケジュールする場合、アップグレードが開始される日付と時刻（UTC）を設定できます。

アップグレード期間は、スケジュールされたアップグレード開始時刻からアップグレードが実行されるまでの時間を設定します。デフォルトでは、マシンカタログおよびマシンのグループのアップグレードの場合、Citrixはパフォーマンスを向上させ、ボトルネックを回避するために、アップグレード期間全体にわたってVDAアップグレードの負荷分散を行います。

アップグレードが開始されると、VDAはアップグレードが完了するまでメンテナンスモードになります。VDAでセッションが実行されている場合、セッションがなくなるまでVDAはアップグレードされません。メンテナンスモードの間は、新しいセッションをVDAに仲介することはできません。アップグレード期間中にユーザーがセッションから切断した場合、アップグレードが完了するまで再接続できません。

VDAは、スケジュールされたアップグレード期間が完了するまでアップグレードを試行し続けます。アップグレード期間全体にわたってセッションが存在する場合、アップグレードはキャンセルされ、VDAのメンテナンスモードはオフになります。VDAアップグレードの成功率を向上させるために、より長いアップグレード期間を検討してください。

> **注:**
>
> スケジュールされたアップグレードの前に手動でメンテナンスモードに設定されたVDAは、アップグレードに失敗します。

利用可能なVDAバージョン

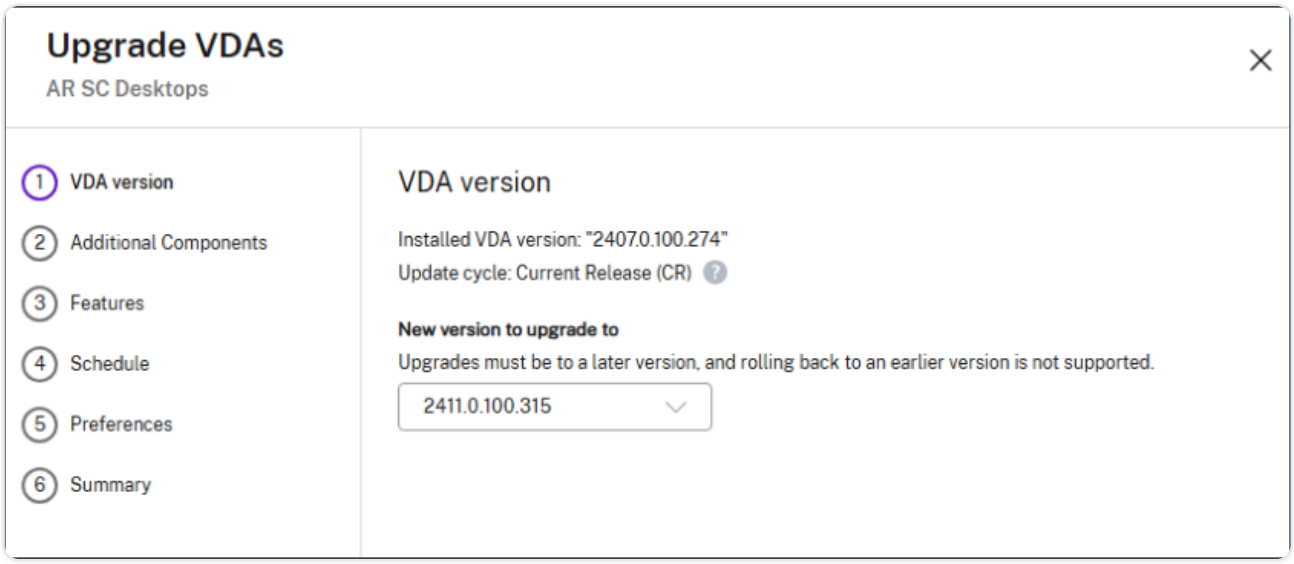
VDAアップグレードサービスは、CRバージョンについてはVDAのN-2バージョンを、現在サポートされているすべてのLTSRバージョンについてはN-2 CUバージョンを維持します。

新しいCVADバージョンがリリースされると、サイト全体を更新することなく、VUSを更新してより新しいVDAバージョンを含めることができます。VUSは、利用可能なVDAバージョンを読み込むために**vda_releases.xml**ファイルを使用します。**vda_releases.xmld**ファイルは、CVADメタインストーラーの次の場所にあります。

<CVAD-ISO\>\Support\VdaUpdateServiceMetadata\vda_releases.xml

新しいvda_releases.xmlファイルをVUSにインポートするには、次のコマンドレットを実行します。 `Import-VusVdaReleasesMetadata -Path '[Path to vda_releases.xml]'`

Web Studioで、カタログまたは個々のマシンをアップグレードする際に、UIはVDAをアップグレードするバージョンを尋ねます。



PowerShell を使用して利用可能なVDAバージョンを特定するには、`Get-VusAvailableVdaVersion` コマンドレットを使用します。

コマンドレットにマシンまたはカタログを渡さない場合、コマンドレットはすべてのアップグレードトラックで利用可能な最新バージョンを返します。

リソースで利用可能な特定のバージョンを取得するには、VDA（-MachineName、-MachineUid、または-MachineUuid）またはカタログ（-CatalogName、-CatalogUid、または-CatalogUuid）を `Get-VusAvailableVdaVersion` コマンドレットに渡します。

例: `Get-VusAvailableVdaVersion -CatalogName '[Name of your Machine Catalog]'`

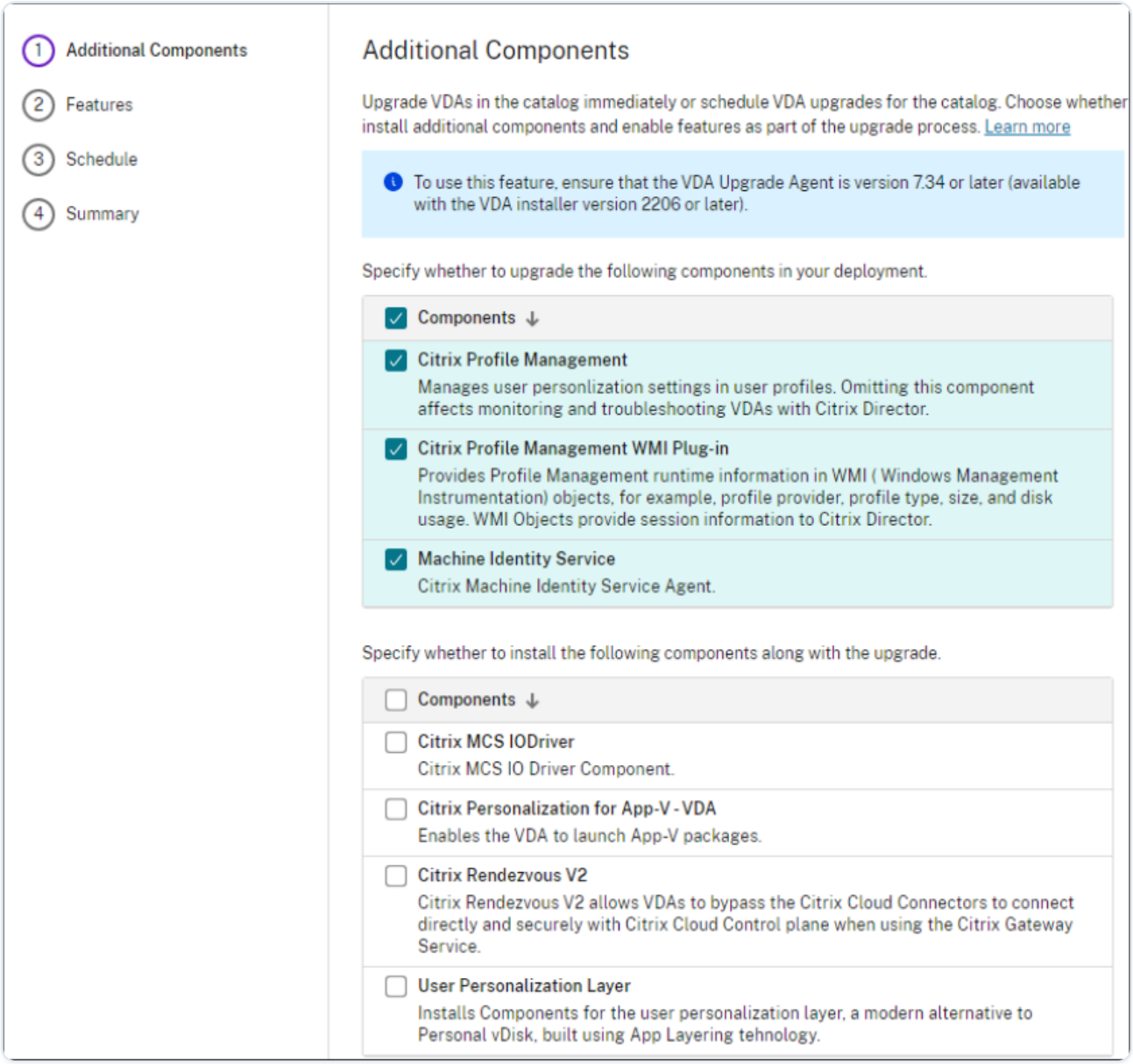
```
PS V:\> Get-VusAvailableVdaVersion -CatalogName 'CR-2303'

UpgradeType Version
----------- -------
         CR 2411.0.100.315
         CR 2407.0.100.274
         CR 2402.0.100.629
```

追加コンポーネント

マシンカタログまたは個々のマシンでVDAをアップグレードする際に、追加コンポーネントをインストールまたはアップグレードできます。コンポーネントをチェックしない場合、そのコン

ポーネントはアンインストールされませんが、VDA全体のアップグレードの一部としてアップグレードされることもありません。

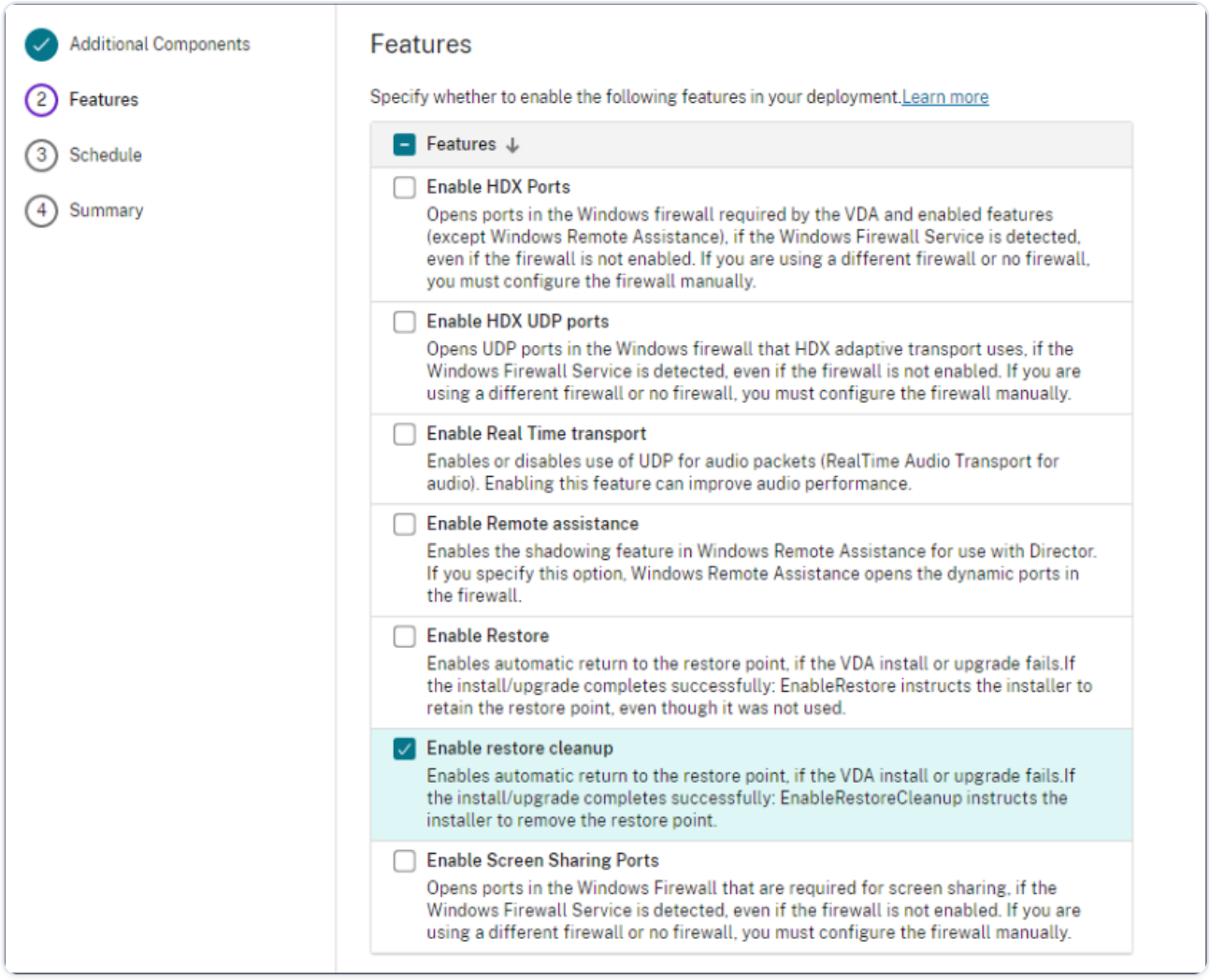


機能

VDAアップグレードサービスを通じて、VDA上で機能を有効化またはアップグレードできます。機能をチェックしない場合、その機能は無効化されませんが、VDA全体のアップグレードの一部としてアップグレードされることもありません。

デフォルトでは、**復元クリーンアップを有効にする**チェックボックスが選択されています。Citrixは、管理を容易にし、失敗したアップグレードからの回復を改善するために、復元クリーンアップ機能を有効にすることを推奨します。この機能が有効になっている場合、アップグレードが開始される前にシステム復元ポイントが作成されます。アップグレードが失敗した場合、VDAはシステム復元ポイントに復元されます。VDAのインストールが成功した後、復元ポイントは削除さ

れます。詳細については、「インストールまたはアップグレードの失敗時の復元」を参照してください。



注記:

Windows システムの復元は、シングルセッションオペレーティングシステム（例: Windows 10 および 11）でのみサポートされています。「復元のクリーンアップを有効にする」機能が動作するためには、VDA で Windows システムの復元機能を有効にする必要があります。「復元を有効にする」または「復元のクリーンアップを有効にする」が選択されていても、VDA で Windows システムの復元が構成されていない場合、アップグレードが失敗する可能性があります。

同時実行性

マシンカタログをアップグレードする際、VUS を使用すると、同時にアップグレードする VDA の最大数を定義できます。これにより、インターネット接続やファイルサーバーへの負荷を軽減で

き、障害しきい値と組み合わせて使用すると、多数の VDA のアップグレードが失敗した場合にアップグレードを停止できます。

スケジュールされたアップグレードが開始されるとすぐに、カタログ内のすべての VDA はメンテナンスモードになります。定義された最大同時実行設定に一致する数の VDA でアップグレードが開始されます。VDA のアップグレードが完了するとすぐに、同時にアップグレードする VDA の同時実行数を維持するために、別の VDA がアップグレードを開始します。

マシンカタログのスケジュールされたアップグレードで同時実行が指定されていない場合、Citrix は、カタログ内の VDA の総数とアップグレード期間に基づいて、デフォルトの同時実行値を使用します。

アップグレードの完了には平均約30分かかりますが、これは環境条件によって大きく異なる場合があります。提供されたアップグレード期間内にすべての VDA がアップグレードできるような同時実行数を設定することを検討してください。たとえば、4時間でアップグレードするように設定された20台の VDA がある場合、1時間あたり5台の VDA をアップグレードする必要があります。平均アップグレード期間が30分の場合、同時実行値を3に設定すると、1時間あたり5台の VDA アップグレード要件を満たすことができます（30分あたり3回のアップグレードで、1時間あたり6回の更新になります）。

失敗しきい値

マシンカタログをアップグレードする際、特定の数の VDA が失敗した場合に、それ以上の VDA がアップグレードされないように、障害しきい値を使用します。障害しきい値は、アップグレードの失敗を引き起こす問題の影響範囲を縮小し、管理者のトラブルシューティング作業を軽減できます。

障害しきい値は、将来の VDA がアップグレードを開始するのを防ぎますが、すでにアップグレードを開始している VDA を停止することはありません。たとえば、マシンカタログに100台の VDA があり、同時実行が10台の VDA に設定され、障害しきい値が3に設定されている場合、すべての VDA アップグレードが失敗した場合、少なくとも13台の VDA がアップグレードを試行し、残りの87台は開始されず、アップグレードはキャンセルされます。

スケジュールされたアップグレードの開始時に10台の同時実行 VDA がアップグレードを開始します。最初のアップグレードが失敗した場合、10台の同時実行アップグレードを維持するために別の VDA がアップグレードを開始します。2番目のアップグレードが失敗した場合、別の VDA がアップグレードを開始します。3番目のアップグレードが失敗した場合、現在アップグレードプロセス中のすべての VDA は続行され、アップグレードスケジュール内の残りの VDA のアップグレードはキャンセルされます。

VDA インストーラーの場所

VDA インストーラーは、環境内のローカルファイル共有でホストする必要があります。ファイル共有と VDA インストーラーの要件を以下に示します。

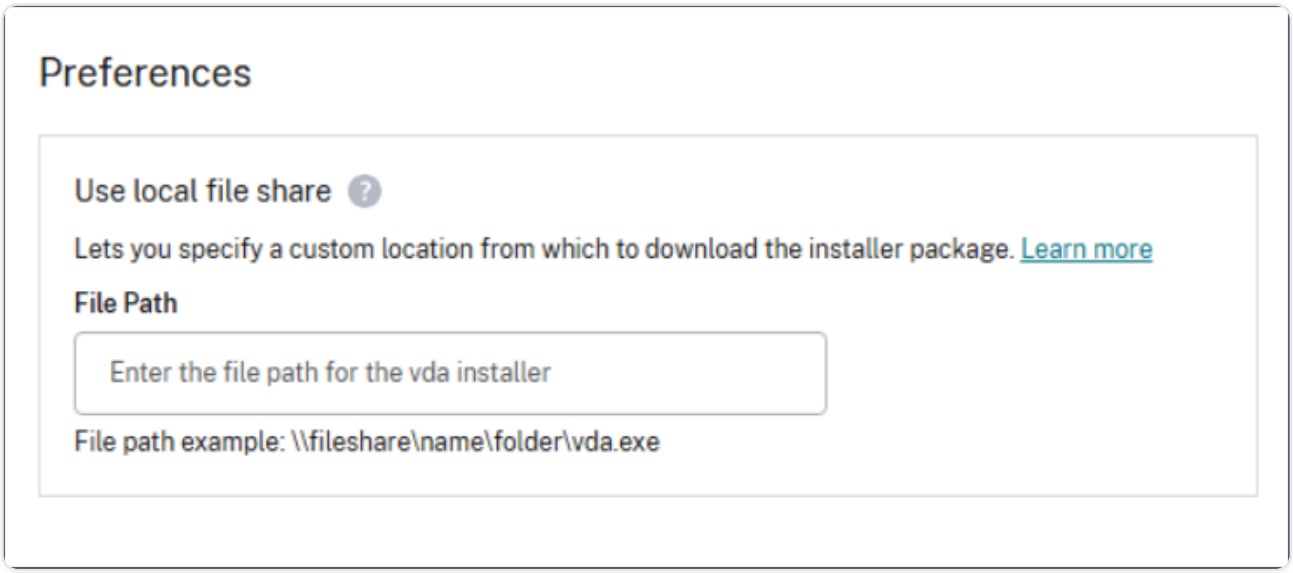
ファイル共有には、次の前提条件が必要です。

- ファイル共有のアクセス許可
  - VDAインストーラーパッケージを含むネットワーク共有には、ローカルシステム（NT AUTHORITY\SYSTEMプリンシパル）として実行されるVDAアップグレードエージェントサービスに対する読み取りアクセス権が必要です。
  - ドメイン参加済みVDA:
    - ローカルシステムアカウント（VUAはローカルシステムとして実行）は、ネットワーク共有にアクセスするときにコンピューターの資格情報を使用します。
    - ファイル共有には、ドメインコンピューターへの読み取りアクセス権を付与する必要があります。
    - 共有の詳細設定で、**ファイルとプリンターの共有**を有効にする必要があります。
  - ドメインに参加していないVDA:
    - ローカルシステムアカウント（VUAはローカルシステムとして実行）は、ネットワーク共有にアクセスするときに**ANONYMOUS LOGON**を使用します。
    - 「**ネットワークと共有センター、パスワード保護共有**」は無効にする必要があります。
    - フォルダーのアクセス許可の**セキュリティ**タブで、**ANONYMOUS LOGON**に読み取りアクセス許可を付与する必要があります。
    - 詳細共有設定で、**ファイルとプリンターの共有**を有効にする必要があります。
    - 共有フォルダー名は、**ネットワークアクセスセキュリティポリシー**に追加する必要があります。
- VDAインストーラー
  - VDAインストーラーは、Citrix Downloads Webサイトからダウンロードし、ファイル共有に配置する必要があります。
  - マシンカタログに関連するVDAインストーラーをダウンロードする必要があります。
    - カタログの種類がマルチセッションの場合は、**マルチセッションOS VDAインストーラー**を使用します。

    - カタログの種類がシングルセッションの場合は、**シングルセッションOS VDAインストーラー**を使用します。

  - 特定のアップグレードの場合、ファイル共有上のインストーラーのバージョンは、VUSによって公開されたバージョンと完全に一致している必要があります。利用可能なバージョンを確認するには、`Get-VusAvailableVersion` PowerShellコマンドレットを使用します。

インストーラーへのパスは、実行可能ファイルを含むファイルパスである必要があります。例: `\\hostname\VDA-Packages\VDAWorkstationSetup_2308.exe`。



PowerShellを介してVUSを使用する場合、アップグレードをスケジュールする際に、`-VdaWorkstationPackageUri` (シングルセッションOS) または `-VdaServerPackageUri` (マルチセッションOS) パラメーターを使用します。

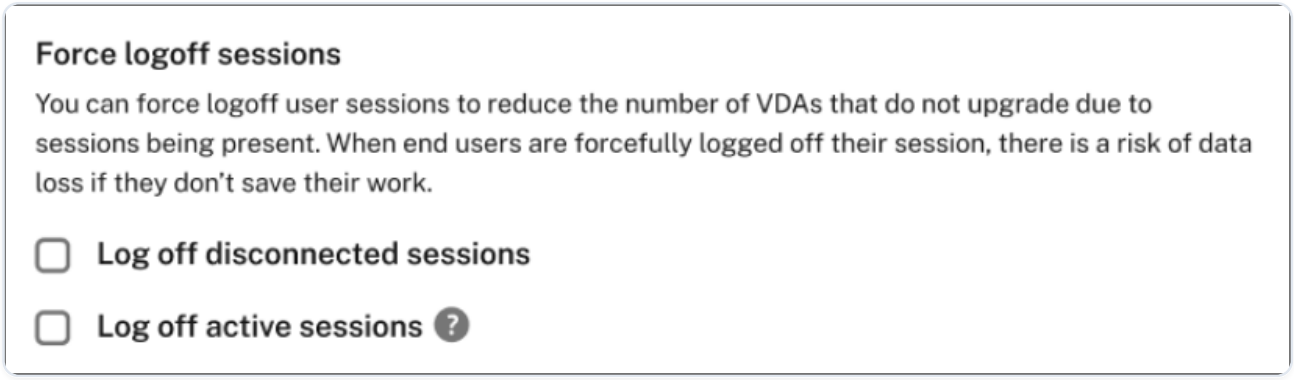
セッションの強制ログオフ

スケジュールされたアップグレード中にアップグレード可能なVDAの数を増やすには、アップグレード中にユーザーセッションを強制的にログオフすることを検討してください。強制ログオフは、全体のスケジュールされたアップグレード期間の開始時ではなく、個々のVDAのアップグレードが開始されるときに発生します。

スケジュールされた期間内で異なるVDAが異なる時間にアップグレードを開始するため、ユーザーは自身の特定のVDAがアップグレードを開始したときにのみログオフされます。

Web Studioを使用してスケジュールされたアップグレード中に切断されたセッションを強制的にログオフするには、**切断されたセッションをログオフ**オプションを選択します。

Web Studioを使用してスケジュールされたアップグレード中にアクティブなセッションを強制的にログオフするには、**アクティブなセッションをログオフ**オプションを選択します。アクティブなセッションをログオフする場合、ユーザーはアップグレード開始の10分前にセッション内で通知を受け取り、自動的にログオフされる前に作業を保存するよう促されます。



PowerShellを使用してスケジュールされたアップグレード中に切断されたセッションを強制的にログオフするには、アップグレードをスケジュールする際に`-LogoffOption`パラメーターを使用します。`-LogoffOption`で利用可能なオプションは以下のとおりです。

- **ActiveSessionsOnly:** スケジュールされたアップグレード期間中にVDAでアクティブなセッションがある場合、ユーザーはログオフされます。ユーザーがログオフされる10分前に警告としてバナーが表示されます。切断されたセッションを持つVDAは、アップグレード期間中にログオフされません。切断されたセッションがアップグレード期間中ずっと残っている場合、そのVDAのアップグレードはキャンセルされます。
- **DisconnectedSessionsOnly:** スケジュールされたアップグレード期間中にVDAで切断されたセッションがある場合、ユーザーはログオフされます。ユーザーは、切断されたセッションがログオフされることを通知されません。アクティブなセッションを持つVDAは、アップグレード期間中にログオフされません。アクティブなセッションがアップグレード期間中ずっと残っている場合、そのVDAのアップグレードはキャンセルされます。
- **ActiveAndDisconnectedSessions:** スケジュールされたアップグレード期間中にVDAで切断されたセッションまたはアクティブなセッションがある場合、ユーザーはログオフされます。アクティブなセッションの場合、ユーザーがログオフされる10分前に警告を示すバナーが表示されます。
- **DoNotLogoff:** アクティブなセッションと切断されたセッションはログオフされません。アップグレードスケジュールの期間中ずっとVDAにセッションが存在する場合、アップグレードはスケジュールされたアップグレード期間の終了時にキャンセルされます。

可能な場合、Citrixは、アップグレードが正常に完了するVDAの数を増やすために、セッションを強制的にログオフすることをお勧めします。

> **重要：**
>
> セッションを強制的にログオフすると、ユーザーはセッションから保存されていない作業を失う可能性があります。

VDAワークフローの編集またはキャンセル

カタログのアップグレードをスケジュールした後、アップグレードの開始時刻と期間を編集したり、アップグレード全体をキャンセルしたりできます。

マシンカタログレベルでUIを使用してアップグレードを編集またはキャンセルするには、既存のスケジュールされたアップグレードがあるマシンカタログを右クリックし、「**スケジュールされたVDAアップグレードの編集**」をクリックします。PowerShellを使用して既存のマシンカタログレベルのアップグレードを編集するには、`Set-VusCatalogUpgrade`および`Remove-VusCatalogUpgrade`コマンドレットを使用します。

マシンレベルでアップグレードを編集またはキャンセルするには、検索ノードで、既存のスケジュールされたアップグレードがあるマシンを右クリックし、「**スケジュールされたVDAアップグレードの編集**」をクリックします。複数のマシンに対して同時にスケジュールされたVDAアップグレードを編集することはできません。PowerShellを使用して既存のマシンレベルのアップグレードを編集するには、`Set-VusMachineUpgrade`および`Remove-VusMachineUpgrade`コマンドレットを使用します。

VUSの監視とトラブルシューティング

スケジュールされたVDAアップグレードの監視

VDAとマシンカタログには、VDAアップグレードの準備状況と現在のステータスを監視するのに役立つ2つの属性があります。これらは、StudioまたはVDAやカタログの詳細ペインでフィルタリングに使用できる列として表示されます。

- VDAアップグレード
- VDAアップグレードの状態

VDAアップグレード

VDAアップグレードは、VDAまたはマシンカタログにVDAアップグレードエージェントが構成されているかどうか、およびVDAが最新であるか、またはアップグレードが利用可能であるかに関する情報を提供します。利用可能なステータスは次のとおりです。

VDAアップグレード (STUDIO)	VDAアップグレード (POWERSHELL)	説明
カタログレベル		
未構成	MissingUpgradeType	マシンカタログに対して、アップグレードトラック (CR、LTSR、CR EAR、またはLTSR EAR) が選択されていません。
スケジュール済み	UpgradeScheduled	マシンカタログのアップグレードがスケジュールされています。
利用可能	UpgradeAvailable	カタログ内のVDAは、アップグレードトラックの最新バージョンではありません。アップグレードが推奨されます。
最新	UpToDate	カタログ内のVDAはアップグレードトラックの最新バージョンです。アクションは不要です。
不明	不明	最新のVDAアップグレード状態を取得しています。
マシンレベル		
未構成	MissingUpgradeType	VDAのマシンカタログに対して、アップグレードトラック（CR、LTSR、CR EAR、またはLTSR EAR）が選択されていません。
スケジュール済み	UpgradeScheduled	VDAのアップグレードがスケジュールされています。
利用可能	UpgradeAvailable	VDAはアップグレードトラックの最新バージョンではありません。アップグレードが推奨されます。

VDAアップグレード (STUDIO)	VDAアップグレード (POWERSHELL)	説明
最新	UpToDate	VDAはアップグレードトラックの最新バージョンです。アクションは不要です。
状態を確認中	不明	最新のVDAアップグレード状態を取得しています。

注:

LTSRトラックを使用しているVDAの場合、カタログは、VDAが最新の長期サービス (LTSR) バージョンの最新の累積更新プログラム (CU) にある場合にのみ「最新」と表示されます。VDAが以前のLTSRバージョンの最新CUにある場合でも、VDAアップグレードは**利用可能**と表示されます。

VDAアップグレードの状態

VDAアップグレードの状態は、スケジュールされたアップグレードのステータスに関する情報を提供します。VDAアップグレードの状態のステータスは次のとおりです。

VDAアップグレードの状態 (STUDIO)	VDAアップグレードの状態 (POWERSHELL)	説明
カタログレベル		
スケジュールされていません	NotScheduled	カタログに対してアップグレードはスケジュールされていません。
スケジュール済み	UpgradeScheduled	カタログに対してアップグレードがスケジュールされています。
進行中	UpgradeInProgress	カタログに対してアップグレードが進行中です。
キャンセル済み	アップグレードキャンセル済み	カタログのアップグレードがキャンセルされました。これは、手動によるキャンセル、

VDAアップグレードの状態 (STUDIO)	VDAアップグレードの状態 (POWERSHELL)	説明
		または失敗のしきい値に達したことが原因である可能性があります。
失敗	アップグレード失敗	カタログのスケジュールされたアップグレードが失敗しました。
成功	アップグレード成功	カタログのスケジュールされたアップグレードが正常に完了しました。注: アップグレードが成功したからといって、カタログ内のすべてのVDAが正常にアップグレードされたわけではありません。
-	空	カタログのアップグレードはスケジュールされていません。
マシンレベル		
スケジュール済み	アップグレードスケジュール済み	VDAのアップグレードがスケジュールされています。
アップグレード待機中	UpgradeInUpgradeWindow	スケジュールされたアップグレードはアクティブですが、VDAはまだアップグレードを開始していません。VDAアップグレードがどのように負荷分散されるかについては、「同時実行」を参照してください。
進行中	UpgradeInProgress	VDAは現在アップグレード中です。
キャンセル済み	UpgradeCancelled	アップグレードが開始される前に、VDAのスケジュールさ

VDAアップグレードの状態 (STUDIO)	VDAアップグレードの状態 (POWERSHELL)	説明
		れたアップグレードがキャンセルされました。
アップグレード失敗	UpgradeFailed	VDAはアップグレードを開始しましたが、アップグレードは正常に完了しませんでした。「トラブルシューティング」を参照して、詳細を確認してください。
成功	UpgradeSuccess	VDAは正常にアップグレードされました。
検証に失敗しました	UpgradeValidationFailed	VDAインストーラーのメタデータをダウンロード中に証明書の検証に失敗しました。
-	空	VDAのアップグレードはスケジュールされていません。

スケジュールされたVDAアップグレードのトラブルシューティング

アップグレードの失敗が発生した場合、以下のログは問題の特定とトラブルシューティングに役立ちます。これらのログをCitrixテクニカルサポートと共有することで、サポートプロセスを迅速化することもできます。

VDAインストールログ

アップグレードの失敗をトラブルシューティングする際は、VDAの初回インストールと失敗したアップグレードの両方のログを収集して確認してください。インストールおよびアップグレードのログは、以下の場所にあります。

- VDAインストールのインストールログは以下にあります。
  - %temp%/Citrix/XenDesktop インストーラー
- VDAインストールのアップグレードログは以下のいずれかの場所にあります。
  - C:\Windows\Temp\Citrix\XenDesktop Installer **または**
  - C:\Windows\SystemTemp\Citrix\XenDesktop インストーラー

VDA アップグレードエージェントのバージョン

VUSを介したアップグレードの失敗をトラブルシューティングするためにデータを収集する際、VDA上のアップグレードエージェントのバージョンを知ることが重要です。VDAアップグレードエージェントのバージョンを確認するには、次のコマンドレットを使用します: `Get-VusComponentVersion -ComponentType VUS`。これにより、すべてのVDAとそのVDAアップグレードエージェントのバージョンが一覧表示されます。

カタログレベルで VDA アップグレードエージェントのバージョンを確認するには、次のスクリプトを使用できます。

> **注:**

> このスクリプトは例として提供されており、特定の環境に合わせて調整する必要がある場合があります。本番環境で使用する前に、スクリプトを十分にテストすることをお勧めします。

```
Param( [Parameter (Mandatory=$true)] [string] $CatalogName ) try { $Uuids = Get-BrokerMachine -CatalogName $CatalogName | Select-Object -Property UUID
```

```
if($Uuids -eq $null) { throw "Cannot find CatalogName " +$CatalogName } Write-Output("Catalog Name passed is "+$CatalogName)
```

```
foreach($Uuid in $Uuids) { $compVersion = Get-VusComponentVersion -MachineId $machine.UUID -ComponentType VUS $Machine = Get-BrokerMachine -UUID $compVersion.MachineId Write-Output(“MachineName: “+ $Machine.MachineName+”, Machine UUID:”+$machine.MachineId+”, VUA Version:”+ $compVersion.Version) } } catch { Write-Output(“Exception Occured”) Write-Host $_ }
```

VDA アップグレードエージェントに関連するログ

VDAアップグレードエージェント (VUA) のログは、アップグレードの失敗やVUAとVDAアップグレードサービス間の通信に関する問題のトラブルシューティングに不可欠な情報を提供できます。収集できるログには次のものがあります。

- Citrix Diagnostic Facility (CDF) トレース。CDFモジュール名は`VdaUpgradeAgent`です。
- Windowsイベントログ。ログは**イベントビューアー > Windowsログ > アプリケーション > Citrix VDA Upgrade Agent Service**で表示します。

管理者がトラブルシューティングに不可欠な情報をキャプチャしつつ、ログファイルが肥大化するのを防ぐローテーションログファイルを有効にできるレジストリ設定があります。ログファイルの合計サイズは20 MBに制限されています。ファイルへのログ記録を有効にするには、次のレジストリキーを作成します。

- **キー：** `HKLM:\SOFTWARE\Citrix\UpdateServices\UpdateAgent`
- **値の名前：** `LogToFile`
- **値の型:** `REG_DWORD`
- **値のデータ:**
  - `0` - ファイルトレース無効
  - `1` - ファイルトレース有効

PowerShell を使用して VDA 上に LogToFile レジストリキーを作成するには、次のコマンドレットを使用します:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\UpdateServices\UpdateAgent -Name LogToFile -Value 1 -PropertyType DWord -Force
```

大規模なマシン群で LogToFile を有効にするには、グループポリシー設定を使用してすべての VDA 組織単位 (OU) に LogToFile レジストリを作成することを検討してください。

> **注:**
>
> - `LogToFile=1` が設定されている場合、ログはファイルにのみ書き込まれます。CDF トレースには表示されません。
> - レジストリの変更を有効にするには、VDA Upgrade Agent サービスの再起動が必要です。
> - ログファイルは C:\ProgramData\Citrix\Update Services\Logs フォルダーに作成されます。

VDAアップグレードのダウンロード失敗のトラブルシューティング

VDA アップグレード機能に関連するダウンロード失敗のトラブルシューティングと解決には、以下の手順に従ってください。

1. URLフィルタリングが有効な場合は、関連するURLが許可リストに追加されていることを確認してください。接続性を参照してください。
2. 必要なURLを許可リストに追加した後、VDAアップグレードの再スケジュールを試してください。

詳細なログを分析用に取得するには、CDFトレースを有効にするか、`LogToFile` を `1` に設定します。ダウンロードの失敗が続く場合は、エラーを確認してください。「Download Failed: This access control list is not in canonical form and therefore cannot be modified」というエラーメッセージが表示される場合、それはフォルダー `C:\ProgramData\Citrix\UpgradeServices\Downloads\VDA` の権限が正しくないことを示しています。

この問題に対処するには、次のいずれかを実行します。

- **オプション1：** 次のコマンドを使用して、フォルダーのアクセス制御リスト（ACL）をリセットします。（このコマンドは、一致するすべてのファイルに対して、デフォルトで継承されたACLでACLをリセットします。）
    - icacls.exe "C:\ProgramData\Citrix\UpgradeServices\Downloads\VDA" /reset /T /C /L /Q
- **オプション2：** Downloadsの下にあるVDAフォルダーを削除し、VDAアップグレードをスケジュールします。

VDA アップグレード検証の失敗のトラブルシューティング

VDA アップグレード機能に関連するダウンロードの失敗をトラブルシューティングして解決するには、以下の手順に従ってください。

1. URLフィルタリングが有効になっている場合は、関連するURL、特に失効チェックに必要な証明書失効リスト (CRL) またはオンライン証明書ステータスプロトコル (OCSP) のURLが許可リストに追加されていることを確認してください。VDAアップグレード要件を参照してください。
2. 必要な URL を許可リストに追加した後、VDA アップグレードの再スケジュールを試行してください。

詳細なログを分析用に取得するには、CDFトレースを有効にするか、`LogToFile` を `1` に設定することをお勧めします。ログには次のエラーが含まれる場合があります。

- RevocationStatusUnknown
- 失効機能は、証明書の失効ステータスを確認できませんでした。
- 失効サーバーがオフラインであったため、失効機能は失効を確認できませんでした。

VDAアップグレードエージェントは、証明書の検証と失効チェックの実行にWindowsシステムコールに依存しています。上記のエラーは、エージェントがCRLまたはOCSPのURLへの接続を確立できないことを示しています。

Windows CryptoAPIは現在、プロキシ設定をサポートしていません。アウトバウンドCRL呼び出しを容易にするためにVDAプロキシを構成する方法については、プロキシ構成を持つVDAセクションを確認してください。

Citrix Always on Tracing

コアコンセプト

アーキテクチャ図(/en-us/citrix-virtual-apps-desktops/2511/media/architecture-overview.png)

Always on Tracing (AOT) アーキテクチャは、Citrix Virtual Apps and Desktops (CVAD) および DaaS 環境全体で継続的なリアルタイムログ収集を提供するように設計されています。これにより、IT管理者とCitrixサポートは、手動でのログ開始や問題の再現を必要とせずに、ユーザーおよびインフラストラクチャの問題をトラブルシューティングできます。

AOTシステムは、複数のCitrixインフラストラクチャ層からログをキャプチャ、転送、保存するために連携して動作する、いくつかの統合されたコンポーネントで構築されています。

主要コンポーネントとワークフロー

1. **AOT ログジェネレーター (Citrix コアコンポーネント)**: Virtual Delivery Agent (VDA)、Delivery Controller (DDC)、StoreFront などの Citrix コンポーネントは、ログジェネレーターとして機能します。これらのコンポーネントには、テレメトリーサービスまたは同様のサービスが搭載されており、AOT API を使用してトレースデータをキャプチャし、事前定義されたステップトレースを記録し、ユーザーセッションとトランザクションに関連するエラーイベントをログに記録します。
2. **ログ収集の有効化**: 管理者がログ収集のリクエストを開始すると (通常、Web Studioの設定を通じて行われ、指示はサイトデータベースに保存され、ブローカーに送信されます。ブローカーは、ブローカー、StoreFront、VDAなどの関連コンポーネント全体でログ収集プロセスを調整します)。管理者は、Session Recording、PVS、FASなどの他のコンポーネントからPowerShellコマンドを通じて個別にログ収集のリクエストを開始します。
3. **テレメトリーサービス**: Citrix Web Studioでログサーバーアドレスを設定し、設定が伝播されると、各コンポーネントのテレメトリーサービスは、事前定義されたイベント、障害、またはトリガーポイントに基づいてログを収集する新しいリアルタイムAOTリスナーをアクティブ化します。
4. **集中ログサーバーへのログ転送**: ログが収集されると、テレメトリーサービスまたは独立したサービスが、それらを直接、集中ログサーバーに安全に転送します。エンドポイントがCitrix Gatewayを介して外部ネットワークから接続されている環境では、転送は通常、SOCKSトンネルを介して行われ、安全でシームレスな転送を保証します。

5. **ログの保存と整理**: 集中ログサーバーは、AOTログを、インデックス付きデータベースバックエンド (デフォルトではOpenSearch) を使用して、構造化された検索可能な形式で受信、解析、保存します。ログはセッション、コンポーネント、およびタイムスタンプでタグ付けされ、容易なアクセスと効率的なトラブルシューティングを可能にします。

Citrix AOTシステム内のログは、構造化された検索可能な形式で保存され、容易なアクセスと効率的なトラブルシューティングを可能にするために、さまざまなフィールドでタグ付けされています。これらのタグには以下が含まれます。

- **MachineName**: ログが生成されたマシンの名前。
- **MachineIP**: マシンのIPアドレス。
- **Role**: Citrixコンポーネントの役割 (例: VDA、DDC、StoreFront)。
- **TimeStamp**: ログイベントが発生したUTCタイムスタンプ。
- **メッセージ**: 実際のログメッセージの内容です。単語で検索したり、フィルタリングしたりできます。
- **Level**: ログの重大度レベル（例：情報、警告、エラー）。
- **Module**: ログを生成した特定のソフトウェアモジュール。
- **ProcessName**: ログを生成したプロセスの名前。
- **ProcessId**: プロセスのID。
- **Thread**: プロセス内のスレッドID。
- **Cpu**: ログ記録時のCPU IDに関連する情報。
- **SessionId**: ログに関連付けられたユーザーセッションのID。
- **Class**: モジュール内のクラスまたはコンポーネント。

これらの詳細なタグにより、管理者は特定の基準に基づいてログを迅速にフィルタリング、検索、分析でき、問題の特定と解決が容易になります。

要約すると、AOTワークフローはCitrixコンポーネントがログを生成することから始まります。これらのログを収集するための一元的なリクエストが開始され、テレメトリサービスが関連コンポーネントからログを収集します。収集されたログは、インデックス作成、保存、およびその後の分析のために、一元化されたログサーバーに安全に転送されます。

AOTの仕組み

Citrix Always on Tracing (AOT) は、環境内の主要コンポーネントからログデータを継続的にキャプチャします。トリガーされると、ログは自動的に収集され、一元化されたログサーバーに安全

に転送され、分析のために保持されます。これにより、手動でのトレースが不要になり、トラブルシューティングが簡素化されます。

トレースのトリガーとログ収集: VDA、DDC、StoreFrontなどのCitrixコンポーネントは、重要な手順やエラーを追跡するためのAOT APIを備えています。これらのコンポーネントはAOTログジェネレーターとして機能します。管理者がDelivery Controllerからログ収集リクエストを開始すると、次のようになります。

- DDCは関連するCitrixコンポーネントに指示を送信します。各コンポーネントは、そのリクエストをローカルのテレメトリサービスに転送します。
- テレメトリーサービスは、AOTログを収集するためにリアルタイムAOTリスニングプログラムを開始し、ログを一元ログサーバーに転送します。

ログの保存と保持: AOTログを受信すると、一元ログサーバーはそれらをフォーマットし、構造化された検索可能なデータベースにインデックス化します。ログは、ストレージ使用量を最適化するために、定義された保持ポリシーに基づいて保持されます。デフォルトでは、AOTログは7日間保持され、その後、スペースを節約するために自動的にパージされます。

AOTと従来のログ記録の比較

側面	AOT	従来のCDFトレース
アクティベーション	自動、継続的	手動、問題の再現が必要
複雑さ	ユーザーフレンドリーで読みやすいログ	エンジニアリングレベルの解析
診断速度	即座にログが利用可能	再現作業により遅延
リソース使用量	最適化されたバッファによる低オーバーヘッド	誤って使用すると中程度から高程度

従来のトレースツールは手作業が必要で、問題が発生している最中に捕捉した場合にのみ機能します。AOT を使用すると、ログはバックグラウンドで継続的に実行されるため、監視していなくても問題が発生したときに捕捉されます。これにより、時間が節約され、トラブルシューティングがはるかに簡単になります。

AOTのハイライト

- **常時オン**: トレースは常に実行され、手動でオンにする必要はありません。
- **自動キャプチャ**: 問題が発生すると常にログが収集されます。

- **中央ログサーバー**: すべてのログは一元的に保存され、簡単にアクセスできます。
- **トラブルシューティングの簡素化**: 一般的な障害を迅速に特定するのに役立ちます。
- **再現不要**: 問題を再現する必要はありません。すでに捕捉されています。

集中型AOTログサーバー

AOTログサーバーは、さまざまなCitrixコンポーネントからAlways on Tracing (AOT) ログを収集および保存するための一元化された保存先として機能します。Dockerテクノロジーを使用してコンテナ化されており、Linuxへの展開が推奨されますが、Docker Desktopを介したWindows環境やCitrix Connectorアプライアンス上でもサポートされています。

AOTログサーバーの主な機能

- **集中型ログストレージ**: 複数のCitrixコンポーネントからのログを集約し、統合された検索可能な場所に保存します。
- **保持ポリシー**: ストレージの使用量とパフォーマンスを最適化するため、ログは構成可能なポリシー (デフォルト: 7日間) に基づいて保持されます。
- **展開**: ログサーバーは、パッケージ化されたインストーラースクリプトとDockerコンテナを使用して展開されます。セットアップには、互換性のあるハードウェアとDockerランタイム環境、またはCloud Connectorアプライアンス (選択した場合) が必要です。
- **安全なログアクセス**: ログは、ログサーバーに含まれるCLIツールを使用して取得できます。すべてのアクセスには、セキュリティとコンプライアンスを確保するために適切な認証が必要です。
- **Citrixコアコンポーネントとの統合**: AOTテレメトリーサービスは、Citrixコアコンポーネントに組み込まれており、これにより、それらがログジェネレーターとして機能できるようになります。テレメトリーサービスは、これらのコンポーネント全体でシームレスかつ自動化されたログキャプチャを保証し、Citrixインフラストラクチャ全体で一貫したログの可視性を可能にします。

AOTログサーバーの展開と構成

AOTの前提条件

AOTログサーバーは、機能するためにDockerコンテナテクノロジーに依存しています。Linuxが推奨されるホストオペレーティングシステムですが、Docker Desktopを使用すればWindowsへのインストールも可能です。あるいは、Citrix Connector Applianceを使用すると、ホストとDockerインフラストラクチャを管理する必要がなくなるパッケージソリューションが提供されます。

1つのログサーバーは、常に**最大128,000のアクティブなコンポーネント接続**をサポートでき、**1秒あたり最大10,000のログイベント**を処理できます。サイジングまたは展開の推奨事項は、これら2つの要素に基づいている必要があります。

- **接続容量**は、同時に接続できるコンポーネントの数を決定します。
- **ログスループット**は、パフォーマンスに影響を与えることなくシステムが取り込み、インデックス化できるログの数を決定します。

環境がこれらの制限内に収まっている限り、1つのログサーバーで十分です。

Citrix Connector アプライアンス

- Citrix Connector Appliance の最新バージョンを実行していることを確認してください。
- お持ちでない場合は、Citrix Cloud から最新バージョンをダウンロードしてインストールしてください。

Linux

- **サポートされているOS**: Ubuntu 24.04 および RHEL 8.10, 9.4
- **ハードウェア要件**: 4 コアの CPU、16 GB の RAM、および 500 GB の空きディスク容量。
- **ソフトウェア要件**: Linux 用 Docker Engine または Linux 用 Docker Desktop をインストールします。
- **ユーザー権限**: ユーザーが root 権限を必要とせずに Docker を起動できることを確認してください。

Windows

- **サポートされているOS**: Windows 11、Windows 10、Windows Server 2022、および Windows Server 2025。Azure VM については、こちらの推奨事項を参照してください。
- **ハードウェア要件**: 8 コアの CPU、24 GB の RAM、および 500 GB の空きディスク容量。
- **ソフトウェア要件**: Windows 用 Docker Desktop をインストールします（サブスクリプションが必要な場合があります）。
    - **WSL バージョン 2.1.5** 以降が必要です。
    - **Hyper-V** と **Containers** の Windows 機能を有効にします。
    - Docker Desktopの設定でメモリ制限を12 GB以上に設定します。

ログサーバーの推奨事項

1日のログ量 (ストレージ)

項目	マシンの数	1日あたりのセッション数/マシン	セッションあたりの平均ログサイズ	1日あたりの合計ログ数
永続VDA	1000	2	2 MB	4,000 MB (約4 GB)
プールされたVDA	1000	50	2 MB	100,000 MB (約100 GB)
CWA エンドポイント	8000	4	1〜1.5 MB	48,000 MB (約48 GB)
デリバリーコントローラー	4	—	DDC あたり300 MB	1,200 MB (約1.2 GB)
StoreFront サーバー	4	—	サーバーあたり300 MB	1,200 MB (約1.2 GB)
NetScaler Gateway /PVS/ Session Recording/ FSA およびその他のサーバー	4	—	サーバーあたり300 MB	1,200 MB (約1.2 GB)
1日の合計ログサイズ（圧縮後）	—	—	—	**圧縮前は約156 GB/日**
				圧縮後は80 GB〜125 GB/日

サイジングの前提条件

- この例は、約10,000の管理対象エンドポイントとインフラストラクチャコンポーネントのリファレンス展開を表しています。

- サイジングの目的では、Delivery Controllers、StoreFrontサーバー、Gateway、PVS、FAS、Session Recording、およびその他のインフラストラクチャコンポーネントは、サーバーあたり1日300 MBと見積もられています。
- サーバーあたり300 MBという値は、ストレージ計画と容量計算に使用される控えめな見積もりです。

注:

1. これらの値は概算であり、展開によって大きく異なる場合があります。ログの量は、サイトの規模、ユーザーアクティビティ、コンポーネントの組み合わせ、および保持要件によって異なります。これらの数値は計画を開始するためのベースラインとしてのみ使用し、環境の実際の使用状況、成長傾向、およびパフォーマンス テストに基づいてストレージ割り当てを調整してください。
2. ログサーバーはデフォルトでLZ4圧縮アルゴリズムを使用します。圧縮率は20%から50%の間になる可能性があります。これは、最大圧縮時にはLogServerがディスクスペースの半分を占め、最小圧縮時には80%を占めることを意味します。
3. 単一のAOTログサーバーは、最大**128,000のアクティブなコンポーネント接続**をサポートし、**毎秒最大10,000のログイベント**を処理できます。ログサーバーは、環境がこれらの接続およびスループットのしきい値内にある限り、AOTログを24時間体制で継続的に収集および保存するように設計されています。
4. これらの推奨事項は、仮想マシンのサイズではなく、受信AOTログを取り込み、処理し、保存する基盤となる**検索およびインデックス作成エンジン**の容量によって決定されます。この検索レイヤーは、インデックス作成、クエリ、および保持操作を処理するため、最終的に最大スケールを決定します。環境が成長するにつれて、このレイヤーはパフォーマンスを維持するために水平方向にスケールする必要があります。
5. 現在、ログサーバーは、ログサーバーサービスと検索/インデックスエンジンを両方含む単一の結合ノードとして提供されています。これにより展開は簡素化されますが、検索層を独立してスケーリングする能力が制限されます。
6. 今後のリリースでは、Citrixは**分離されたアーキテクチャ**に移行し、取り込みとストレージ/インデックス作成が独立したノードで実行されるようになります。これにより、お客様は環境の成長に合わせて検索層をスケーリングし、大規模またはマルチサイト展開全体でパフォーマンスを向上させ、現在のシングルノード設計によって課せられているスケーラビリティの天井を取り除くことができます。

7. AOTログサーバーはSSDベースのストレージに展開してください。特に大量の環境では、信頼性の高いログ取り込み、高速な検索パフォーマンス、効率的な相関関係を確保するために、SSDを強くお勧めします。

AOTログサーバーのストレージサイジング

AOTログサーバーを計画する上で、ストレージを正しくサイジングすることは最も重要な手順の1つです。必要な総ストレージ容量は、AOTログを送信するマシンの数、1日あたりに生成されるデータ量、およびログを保持する必要がある期間によって異なります。

各Citrix環境の動作は異なるため、お客様はまず、VDA、Citrix Workspace Appエンドポイント、Delivery Controller、およびStoreFrontサーバーのログ生成パターンを使用して、1日のログ量を推定する必要があります。1日のログ量がわかったら、以下の式を使用して総ストレージ容量を計算できます。

ストレージ計算式 総ストレージ (GB) = 1日のログ量 (GB) × 保持日数

AOTログサーバーのストレージサイジングガイダンス

展開規模に基づいた1日のログ量とストレージ要件の推定には、以下の表を参照してください。これらの推定値は容量計画を目的としており、ユーザーアクティビティ、セッション密度、有効なコンポーネント、および展開アーキテクチャによって異なる場合があります。

1日のログ量推定

展開規模	圧縮前の1日のログ量	圧縮後の1日のログ量 (LZ4)	推奨カテゴリ
5,000台のマシン	約78 GB/日	約40〜63 GB/日	小規模
10,000台のマシン	~156 GB/日	~80〜125 GB/日	中
50,000台のマシン	~780 GB/日	~400〜625 GB/日	大規模
100,000台のマシン	~1.56 TB/日	~800 GB〜1.25 TB/日	エンタープライズ

保持期間に基づくストレージの見積もり

展開サイズ	7日間の保持	10日間の保持
5,000台のマシン	~300〜450 GB	約400〜630 GB
10,000台のマシン	約600 GB〜1 TB	約800 GB〜1.25 TB
50,000台のマシン	約3〜5 TB	約4〜6.3 TB
100,000台のマシン	約6〜10 TB	約8〜12.5 TB

注:

- これらの値は、容量計画を目的としたおおよその見積もりです。実際のストレージ要件は、展開アーキテクチャ、ユーザーアクティビティ、有効なコンポーネント、保持期間、および圧縮効率によって異なります。
- 見積もりは、10,000台のマシンリファレンス展開モデルに基づいており、線形にスケーリングされています。

Always on Tracing (AOT) の最小サポートバージョン

この表は、Always On Tracing (AOT) のログ収集を有効にするために必要なCitrixコンポーネントの最小サポートバージョンを示しています。バージョン要件は、ユーザーがリソースにアクセスする方法によって異なる場合があります。アクセス方法は、**直接アクセス** (例: StoreFrontへの直接アクセス) または **Gatewayベースのアクセス** (Citrix GatewayまたはCloud Gateway Services) のいずれかです。

コンポーネント / プラットフォーム	種類	最小バージョン (直接アクセス)	最小バージョン (GATEWAY経由のアクセス)
Citrix Workspace アプリ ウィンドウズ	クライアント	2511.10 および 2507 CU1 以降	2603 および 2507 CU2 以降
Citrix Workspace アプリ マック	クライアント	2603 以降	2603 以降

コンポーネント / プラットフォーム	種類	最小バージョン (直接アクセス)	最小バージョン (GATEWAY経由のアクセス)
シトリックス ワークスペース アプリ Linux	クライアント	近日公開	近日公開
Citrix Workspaceアプリ HTML5	クライアント	2511以降	2603以降
Citrix Workspaceアプリ ChromeOS	クライアント	2511以降	2603以降
Citrix Workspace アプリ アンドロイド	クライアント	2603以降	2603以降
Citrix Workspace アプリ iOS	クライアント	2603以降	2603以降
シトリックス バーチャル アプリケーションズ アンド デスクトップ (Windows VDA、DDC、PVS、FAS、セッション レコーディング、STF、Linux VDA、Mac VDA、WEM、UPM)	プラットフォーム	2402 CU4、2507 CU1、2511以降	2402 CU4、2507 CU1、2511以降
シトリックス DaaS *	サービス	2026年2月以降	2026年2月以降
シトリックス NetScaler	インフラストラクチャ	14.1.60.57	14.1.60.57
Citrixライセンスサーバー		540000 以降	54000 以降

*Citrix DaaS展開の場合、AOTログ収集は同じプロセスに従います。ログをAOTログサーバーに転送するようにDaaS設定を構成する必要があります。リソースの場所に展開されたすべてのコンポーネントは、構成されるとログをログサーバーに転送できます。Citrix DaaSコントロールプレーンコンポーネントは、顧客管理のログサーバーにログを送信せず、代わりにCitrix管理のクラ

ウドテレメトリ（Splunk）にログを転送し続けます。この動作は、これらのクラウドコントロールプレーンコンポーネントが、該当する場合にWorkspace Platformの代わりにStoreFrontを使用したり、Cloud Gateway Servicesの代わりにCitrix Gatewayを使用したりするなど、顧客管理のCVADコンポーネントに置き換えられたり補完されたりしない限り適用されます。異なる展開モデルでのログの可用性の詳細については、「AOT Logs Availability Across Deployment Scenarios」セクションを参照してください。

注：

ダイレクトアクセスとは、ゲートウェイが関与しないシナリオ（例：StoreFrontへの直接アクセス）を指します。

Gateway経由のアクセスには、Citrix GatewayおよびCloud Gateway Services (CGS) が含まれます。

「近日公開」は、今後のリリースで予定されているサポートを示します。

ログサーバーのインストールと構成

ログサーバーは、個別のLinuxまたはWindowsサーバーにセットアップすることも、Citrix Connector Applianceでホストして常時更新を利用することもできます。各オプションのインストールおよび構成手順については、関連セクションを参照してください。

インストールに関する注意

- セキュリティ強化のため、展開ではHTTPSの使用を推奨します。
- 選択したポートが既に使用されていないことを確認してください。
- 管理者またはシステムレベルの権限が必要となるため、特権ポート（0〜1023）の使用は避けてください。
- ファイアウォールルールが選択したポートでのトラフィックを許可していることを確認してください。
- 有効な範囲（0〜65535）内のポート番号を使用しますが、競合を避けるため、システムサービスで一般的に使用されるポートは避けてください。

- Citrix Connector Applianceを使用してログサーバーを展開する場合は、ポート443のみが構成されていることを確認してください。
- 例で使用されているポート番号（HTTPの場合は8080、HTTPSの場合は8443）は参照用です。これらのポートを厳密に使用する必要はありません。環境に基づいて適切なポート番号を選択し、AOTログサーバーを構成する際には、上記のインストールガイドラインに従ってください。

Citrix Connector Applianceを介したログサーバーのインストール

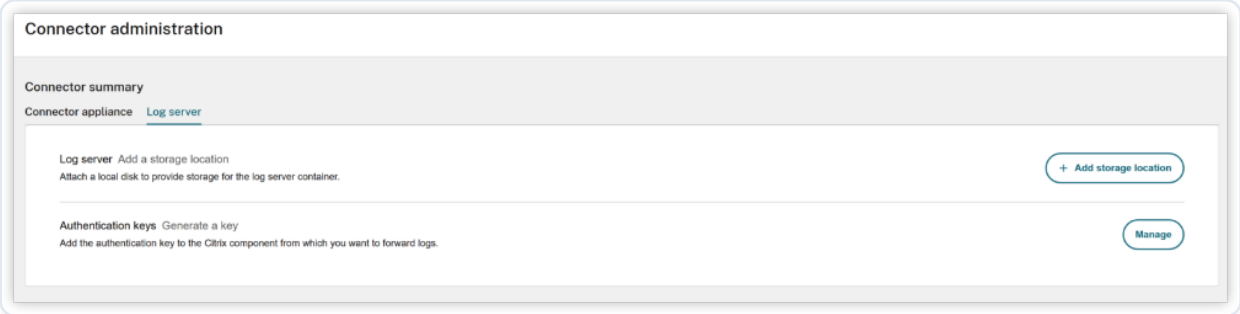
ログサーバーはCitrix Connector Appliance内に展開できます。このアプローチにより、ホストVMの展開と管理、イメージの手動ダウンロード、またはコンテナコマンドの実行が不要になります。ログサーバーはConnector Applianceのアップグレード中に自動的にオンボーディングされ、継続的なコネクタアップデートを通じて最新の状態に保たれるため、常に最新バージョンを使用できます。詳細については、「Connector appliance updates」を参照してください。

Citrix Connector Applianceを介してログサーバーを展開する手順

1. 環境にConnector Applianceがまだない場合は、ハイパーバイザーまたはパブリッククラウドマーケットプレイスからアプライアンスを展開してください。Citrix Connector Applianceの最小要件は11.4.1.444です。インポート後、アプライアンスをCitrix Cloudに登録します。詳細については、「Obtain the connector appliance」を参照してください。
2. デフォルトでは、Connector Applianceは2 vCPUと4GBのメモリを備えています。ログサーバーの要求を処理するには、リソースを少なくとも4 vCPUと16GBのメモリに増やしてください。
3. サポートされているコンポーネントがログサーバーのホスト名を解決できるように、Connector Appliance FQDNのDNS「A」レコードを作成します。Connector ApplianceをActive Directoryドメインに参加させることはオプションです。
4. Cloud Monitorは、リソースの場所にある**サポートされているWindows Cloud Connectorで実行されているMonitor Connectorサービス**を介してAOTログを取得します。ログサーバーがCitrix Connector Applianceに展開されている場合、サポートされているWindows Cloud Connectorも同じリソースの場所に存在する必要があります。Cloud MonitorがAOTトレースを取得するには、Connector Applianceだけでは不十分です。Cloud Connectorはバージョン**6.141.0.13739**（または**4.420.0.13739**）以降を実行している必要があります。以前のバージョンでは、`GetAotTraces` API呼び出しが失敗し、MonitorでHTTP 500エラーが発生します。
5. Connector Applianceは、Connector Appliance管理ページに接続するブラウザに提供される自己署名証明書を提供します。HTTPs経由でログサーバーに接続できるようにするには、この自

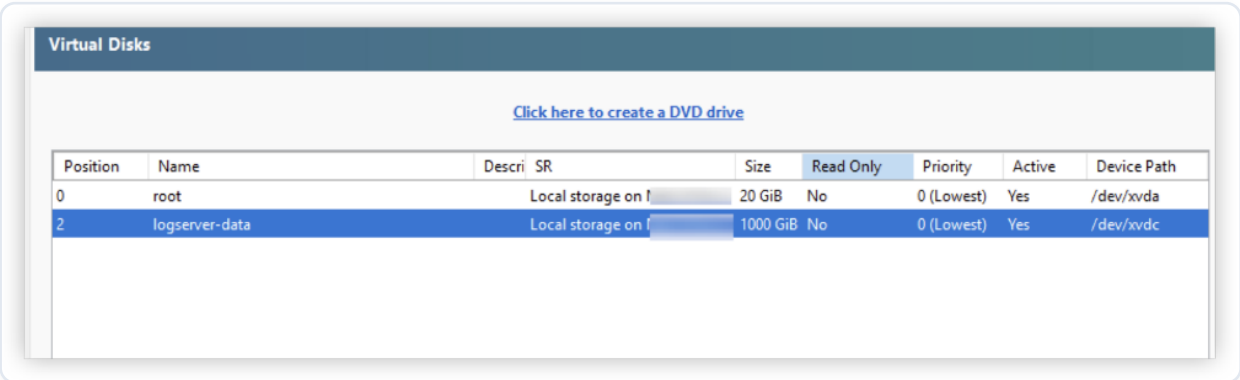
己署名証明書を、組織によって署名された、または組織の信頼チェーンを使用して生成された独自の証明書に置き換える必要があります。詳細については、証明書の管理またはサーバー証明書の置換を参照してください。

6. アップグレードが完了したら、`https://<connector-appliance-FQDN>/?enable=logserver` のConnector Appliance UIにログインし、「?enable=logserver」があることを確認して、ログサーバーUIを表示できるようにします。新しいLog Serverタブには、ストレージと認証キー管理オプションが表示されます。



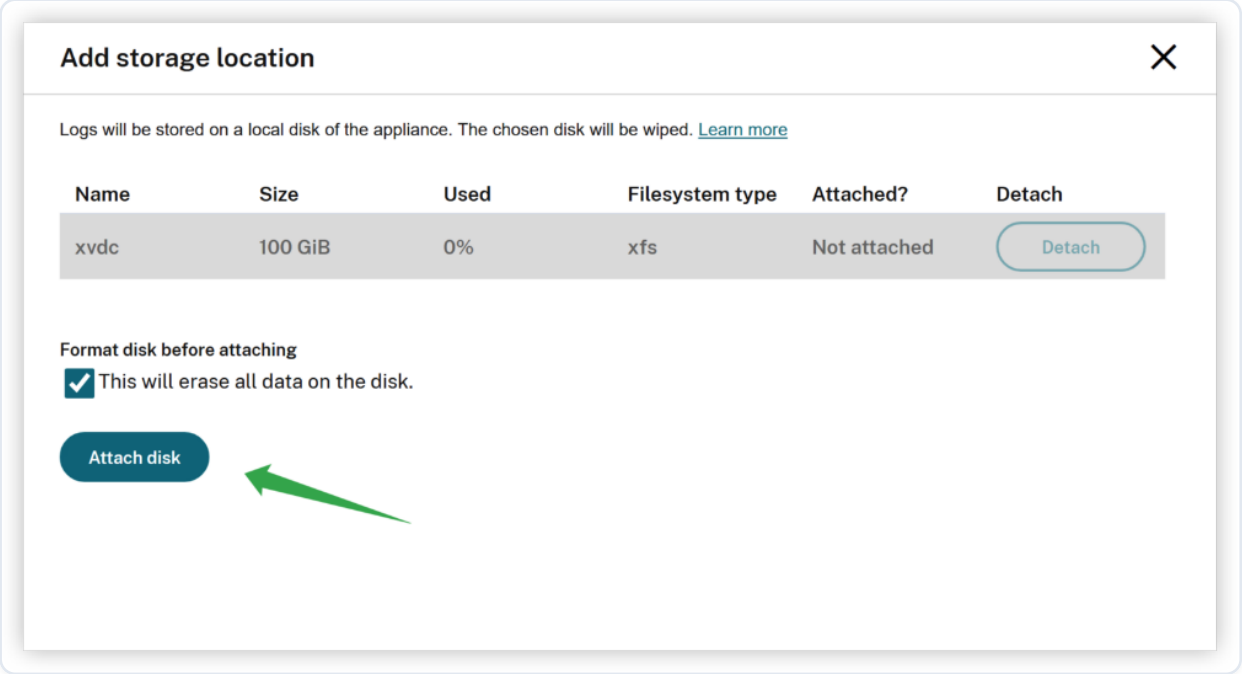
7. コネクタアプライアンスのブートディスクの容量は20GBです。ログサーバーで効率的なログストレージをサポートするには、ハイパーバイザーまたはクラウド管理プラットフォームを使用して、コネクタアプライアンスに別の仮想ディスクを追加する必要があります。この追加ディスクには、ログストレージのニーズを満たすのに十分なスペースが必要です（前のセクションで説明したとおり）。

   下のXenServerのスクリーンショットは、追加ディスクが構成されたコネクタアプライアンスの例を示しています。

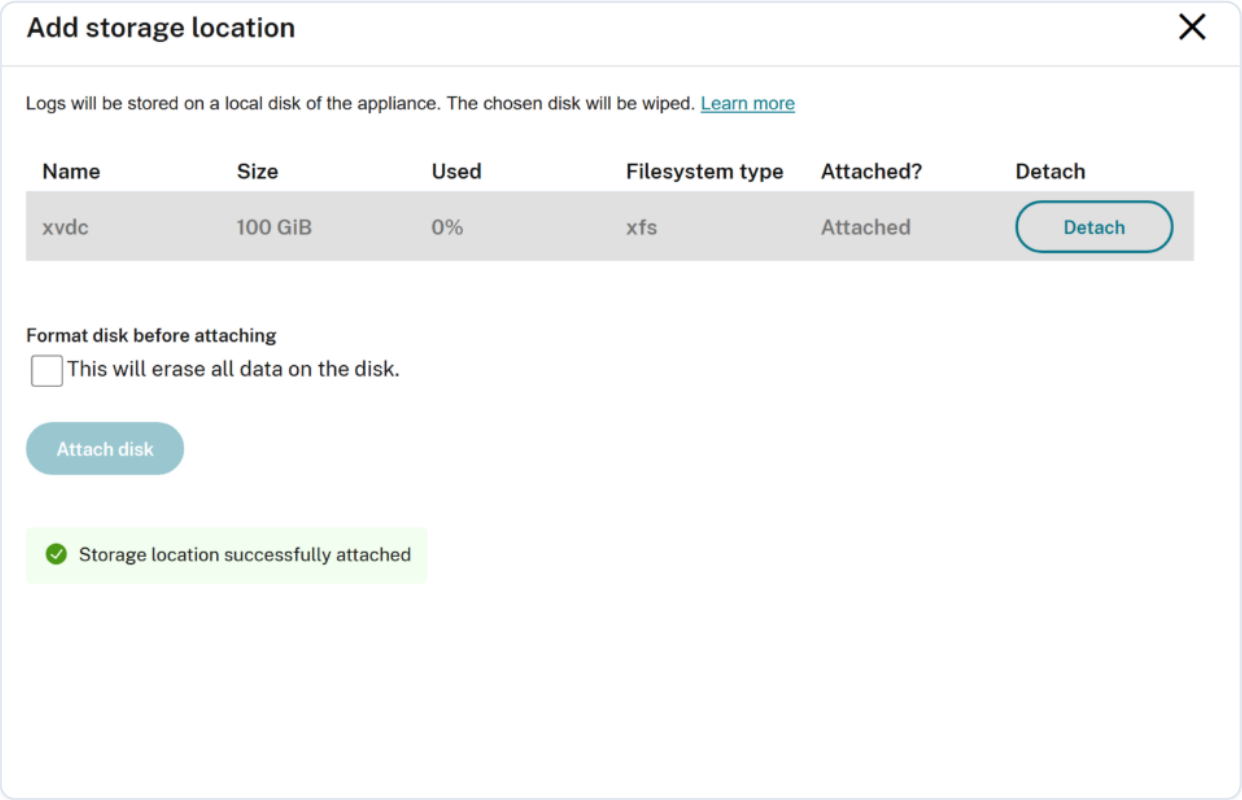


> **注:**
>
> **VMware ESXi の既知の要件:** ユーザーは、追加のデータディスクをルートディスクが使用する SCSI コントローラーとは異なる SCSI コントローラーに接続する必要があります。

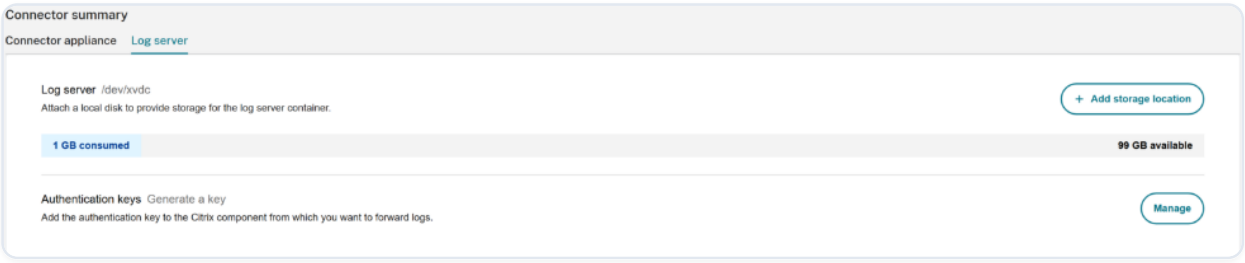
8. キーディスクを追加すると、ログサーバーUIが自動的にそれを検出し、Connector Appliance上のログサーバーコンテナにフォーマットしてマウントできるようになります。



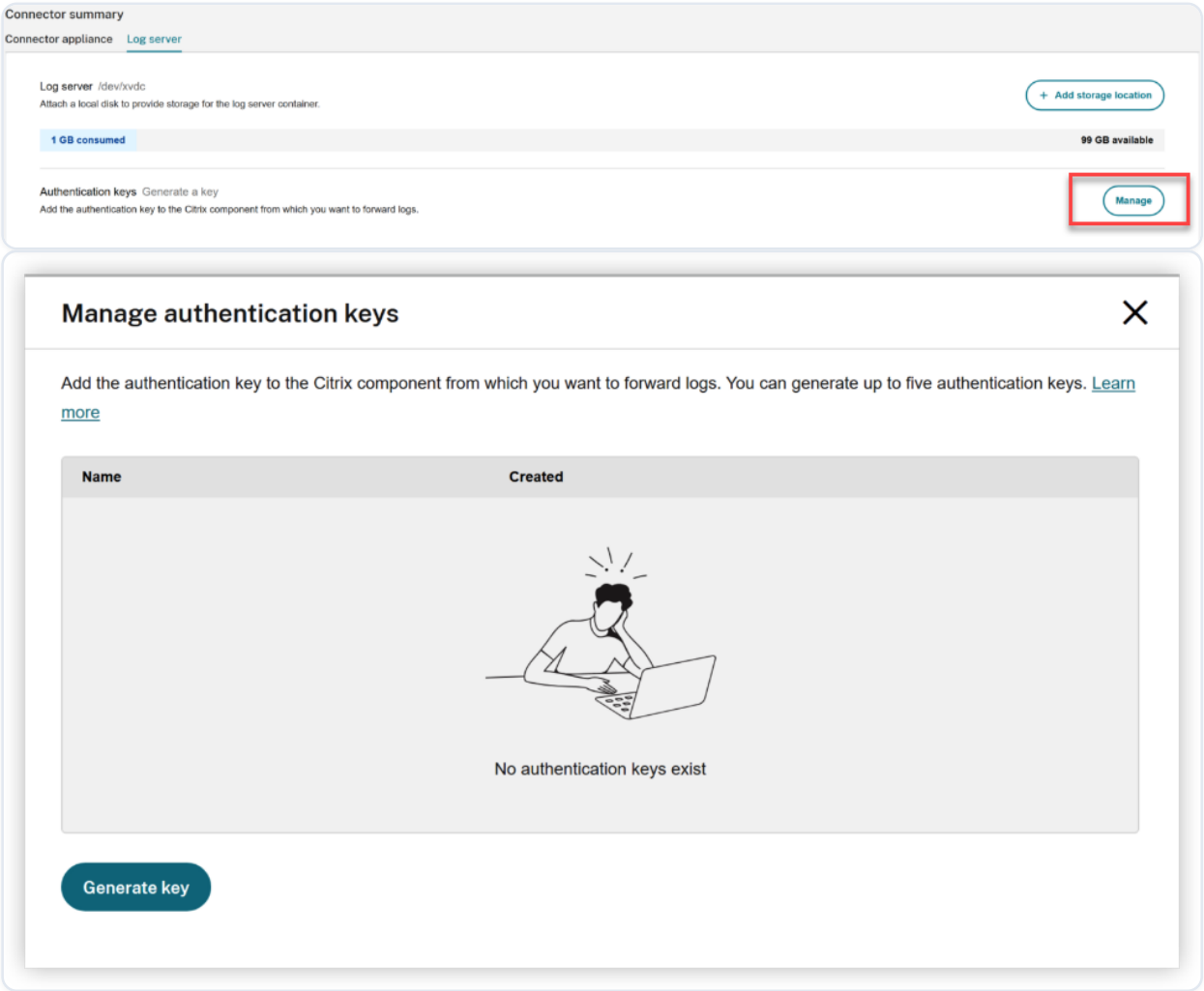
9. 「ディスクの接続」ボタンをクリックすると、ディスクはログサーバーコンテナにマウントされます。

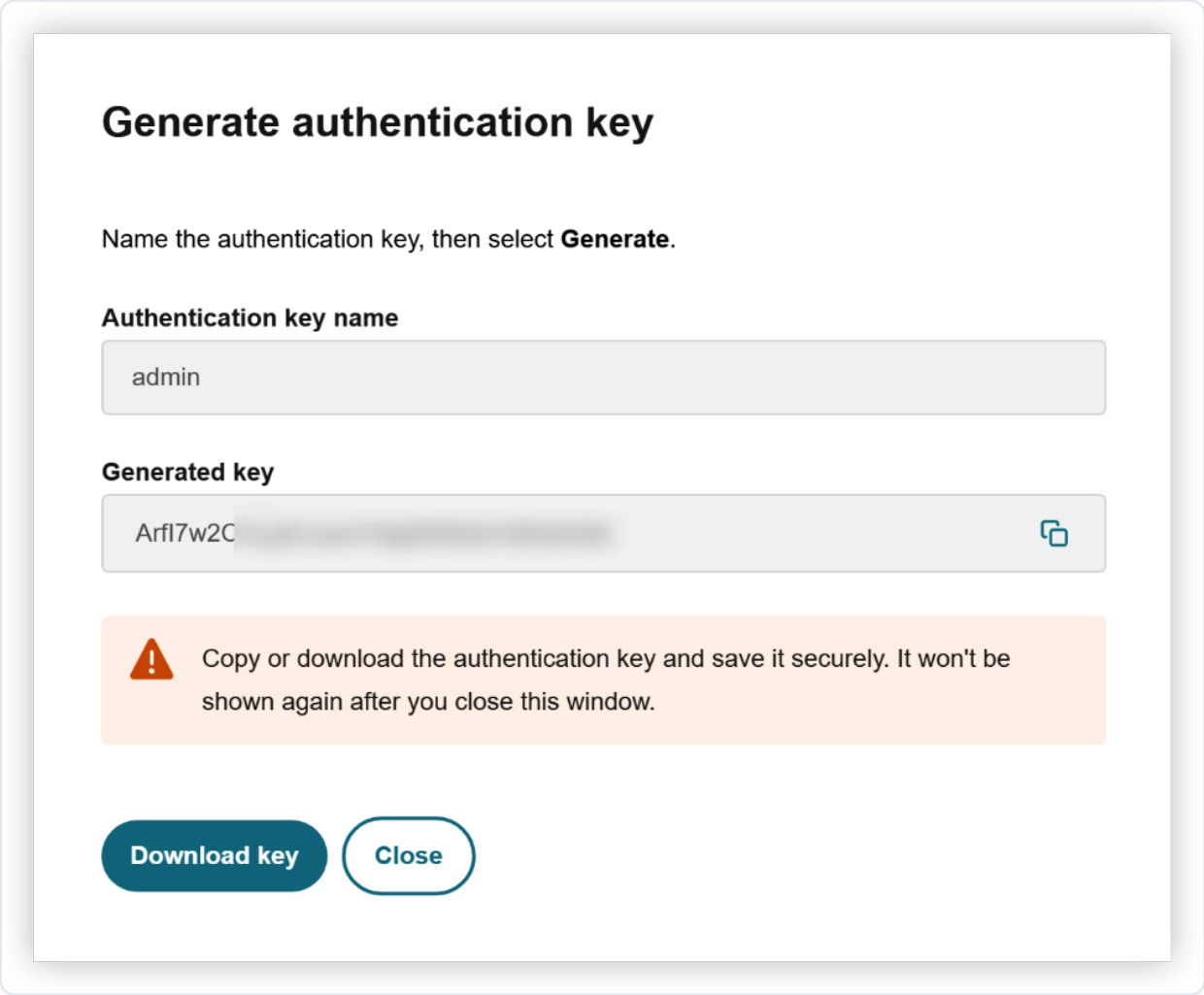


10. メインページには、ディスクサイズと、使用済みスペースおよび残りのスペースに関する情報が表示されます。



11. ディスクがアタッチされた後、pingエンドポイントを呼び出してログサーバーが実行されていることを確認します: `https://<connector-appliance-FQDN>/ctxlogserver/Ping`。pong応答は、ログサーバーが正常に起動したことを確認します。
12. 「管理」ボタンをクリックし、「キーを生成」をクリックします。次に、ロール名を入力し、認証キーをコピーまたはダウンロードします。ウィンドウを閉じると、キーは再度表示されません。





Linuxへのインストール

1. ログサーバーのDockerコンテナイメージをCitrixダウンロードからダウンロードします。
2. ダウンロードしたファイルを同じディレクトリに配置します。
3. ターミナル (Linux) またはコマンドプロンプト (Windows) を使用してディレクトリ内でインストーラーを実行し、指示に従います:

```
chmod +x ./InstallLogServer



#Install with https mode with port 8443 with default path

./InstallLogServer --https --cert </path/your_private_cert_key.pfx> --port
8443
```

```
#Install with http mode, with port 8080 with default path

./InstallLogServer --port 8080



#Command to change the config path and data path of your choice with https
mode

./InstallLogServer --https --cert </path/your_private_cert_key.pfx> --port
8443 --config /Path/LogServer/Config --database /Path/LogServer/Data



#Command to change the config path and data path of your choice with http
mode

./InstallLogServer --port 8080 --config /Path/LogServer/Config --
database /Path/LogServer/Data



#To support CWA client uploading AOT logs, some additional parameters need
to be added after the install log server command.

--sta-server http://STA_SERVER_FQDN:port --log-server LOG_SERVER_FQDN:PORT
```

ここで、,

- STA_SERVER_FQDNは、STAサーバーのホスト名またはIPアドレスです (オンプレミスインストールでは、STAサーバーは通常DDCとともにインストールされます)。
- LOG_SERVER_FQDNとPORTは、ログサーバー自体のホスト名、および指定されたポート (8080、8443、またはインストールパラメーターの –port 値) です。
- ログサーバー証明書 your_private_cert_key.pfx は、AOTクライアントがTLS接続を使用してログをアップロードする他のCitrixコンポーネントによって信頼されている必要があります。

STA_SERVERアドレスにより、StoreFrontが再接続STAチケットを提供できない場合 (セッションタイムアウト後など) でも、ログサーバーはCitrix Workspaceアプリ (CWA) クライアントに再接続STAチケットを発行できます。これにより、接続が切断された場合でも、CWAクライアントはログサーバーと直接接続を再確立できます。

「**LOG_SERVER**」アドレスは、ログサーバーが構成済みのSTAサーバーからSTAチケットを要求する際に使用されます。STAサーバーは、ログサーバーエンドポイントへの接続を特別に承認するチケットを返します。

CWAクライアントが再接続STAチケットを必要としない場合、またはゲートウェイなしでLogServerに直接接続する場合は、これらのパラメーターはオプションです。

Linuxでのインストール後

インストール後、いくつかの便利なスクリプトファイルが生成されます。

```
# In Linux, sh scripts will be generated

DownloadLogsByTime.sh

DownloadLogsByWords.sh

GetAuthKey.sh

ListMachines.sh

StartLogServer.sh
```

LogServerが正常に起動したことを確認するには、`./StartLogServer.sh to start the server. Check your configpath/weblogs.txt`を使用します。

LogServerが正常に起動すると、weblogsファイルに以下のメッセージが表示されます。ポート5000は、選択されたhttpまたはhttpsプロトコルで、LogServerによってDockerコンテナ内で内部的に使用されます。

```
Now listening on https://[::]:5000
```

ログサーバーがHTTPモードでインストールされた場合、正常なログには以下が表示されます。

```
Now listening on http://[::]:5000
```

LogServerがHTTPSを使用する場合、AOTログをアップロードするすべてのマシンでその証明書が信頼されていることを確認してください。

> **注:**

- インストール手順で構成されたポート（8080または8443、あるいは指定された任意のポート）は、DDC、Storefront、VDAなどでLogServerのURLを構成する際に使用する必要があります。
- 通常、Linuxでの起動には30秒から60秒かかります。

Windowsへのインストール

1. ログサーバーのDockerコンテナイメージをCitrix downloadsからダウンロードします。
2. ダウンロードしたファイルを同じディレクトリに配置します。
3. ターミナル（Linux）またはコマンドプロンプト（Windows）を使用して、そのディレクトリでインストーラーを実行し、指示に従います。

ステップ1

ログサーバーVMにWindows用Docker Desktop（サブスクリプションが必要な場合があります）をインストールします。WSL 2に依存するWindowsシステムにDocker Desktopが正しくインストールされ、起動することを確認するには、以下の手順に従ってください。

1. docker desktop settingsでメモリ制限を12 GB以上に設定します
2. Docker Desktop には以下の Windows 機能が必要です。これらの機能が有効になっていることを確認してください。
   - ハイパーV
   - 仮想マシン プラットフォーム
   - Linux 用 Windows サブシステム (WSL)
3. 不足している機能がある場合は、それらをインストールし、VMを再起動して適用します。
4. システムの再起動後、**PowerShell** を管理者として実行し、コマンド `wsl --update` を実行して WSL を更新します。
5. Docker DesktopにはWSL 2が必要です。コマンド `wsl --set-default-version 2` を実行して、WSL 2をデフォルトとして構成します。
6. WSL が更新され、必要な Windows 機能が有効になると、Docker Desktop Engine は正常に起動するはずです。

ステップ 2

インストールを続行するには、以下のコマンドを実行します。

注：

Config および Database (Data) フォルダーのデフォルトの場所は、C:\Users\<username>\LogServer の下に作成されます。これらは以下のコマンドで変更できます。

```
#Install with https mode with port 8443 with default path

InstallLogServer.exe --https --cert <c:\path\cert.pfx> --port 8443



#Install with http mode, with port 8080 with default path

InstallLogServer.exe --port 8080



#Command to change the config path and data path of your choice with https mode

InstallLogServer.exe --https --cert <c:\path\cert.pfx> --port 8443 --config C:\LogServer\Config --database C:\LogServer\Datacmd



#Install with specific config path and data path

InstallLogServer.exe --port 8080 --config C:\LogServer\Config --database C:\LogServer\Datacmd



#To support CWA client uploading AOT logs, some additional parameters need to be added after the install log server command.

--sta-server http://STA_SERVER_FQDN:port --log-server LOG_SERVER_FQDN:PORT
```

ここで、,

- STA_SERVER_FQDN は STA サーバーのホスト名または IP アドレスです（オンプレミス環境では、STA サーバーは通常 DDC と一緒にインストールされます）。
- LOG_SERVER_FQDN と PORT は、ログサーバー自体のホスト名と、指定されたポート（8080、8443、またはインストールパラメーターの –port 値）です。
- ログサーバー証明書 your_private_cert_key.pfx は、他の Citrix コンポーネントによって信頼されている必要があります。AOT クライアントは TLS 接続を使用してログをアップロードします。

STA_SERVER アドレスにより、セッションタイムアウトのために StoreFront が再接続 STA チケットを提供できない場合でも、LogServer が CWA クライアントに再接続 STA チケットを供給できるようになります。その結果、CWA クライアントは接続障害が発生した場合に LogServer から直接再接続チケットを取得できます。

LOG_SERVER アドレスは、ログサーバーが STA_SERVER から STA チケットを要求するときに利用されます。STA_SERVER は、LOG_SERVER アドレスへの接続のみを承認する STA チケットを発行します。

これらのパラメーターは、CWA クライアントが再接続 STA チケットを必要としない場合、またはゲートウェイなしで LogServer に直接接続する場合はオプションです。

Windows でのインストール後

インストール後、インストーラーファイルを保存したのと同じディレクトリに、いくつかの便利なスクリプトファイルが生成されます。

> **注：**
>
> これらのファイルは別の場所に移動できます。ただし、ログサーバーを構成する際に再度必要になるため、新しい場所を覚えておいてください。

```
#In Windows, bat scripts will be generated in the same directory where you saved the installer files.

DownloadLogsByTime.bat

DownloadLogsByWords.bat

GetAuthKey.bat
```

> ListMachines.bat
>
> StartLogServer.bat

ログサーバーを起動するには `StartLogServer.bat` を使用します。

LogServer が正常に起動したことを確認するには、`configpath\weblogs.txt` を確認してください。

ログに以下が表示された場合、ログサーバーが正常に起動したことを意味します。LogServer が正常に起動すると、weblogs ファイルに以下のメッセージが表示されます。ポート 5000 は、LogServer が選択された http または https プロトコルで Docker コンテナ内で内部的に使用します。

```
Now listening on: https://[::]:5000
```

ログサーバーが HTTP モードでインストールされた場合、成功したログには以下が表示されるはずです。

```
Now listening on: http://[::]:5000
```

LogServerがHTTPSを使用する場合、AOTログをアップロードするすべてのマシンでその証明書が信頼されていることを確認してください。

> **注:**
>
> - インストール手順で構成されたポート（8080、8443、または指定された任意のポート）は、DDC、Storefront、VDAなどでログサーバーURLを構成する際に使用する必要があります。
> - 通常、Windowsではハードウェアによって1〜10分かかります。

相互TLS認証（オプション）

相互TLS (mTLS) は、ログサーバーとクライアント (VDA、DDC、StoreFront、CWA) の間にセキュリティの追加レイヤーを提供します。mTLSが有効な場合、クライアントとサーバーは両方とも、エンタープライズPKIによって発行された証明書を使用して相互に認証します。

mTLSは、次のような環境で役立ちます。

- ネットワークセグメントが信頼されていない、または共有されている
- ログサーバーだけでなく、各AOTログクライアントも認証する必要がある
- 顧客が不正なシステムによるログデータの送信を防止したい
- 規制またはコンプライアンスポリシーにより、証明書ベースの認証が必要である。

mTLSはオプションですが、信頼されたCitrixコンポーネントのみがログサーバーと通信できるようにし、ログサーバーがテレメトリデータを受け入れる前にすべての着信接続を検証できるようにすることで、セキュリティを強化します。

証明書の要件

mTLSを構成するには、次の証明書を生成する必要があります。

- **aotclient.pfx** – AOTログクライアント (VDA、DDC、StoreFront、CWA) で使用される証明書
- **logserver.pfx** – Log Serverが使用する証明書
- **enterprise-ca.cer** – 両方の.pfxファイルに署名するために使用されるルート証明書または中間証明書

> **注**
>
> - Citrix Connector Applianceを使用している場合、相互TLSはサポートされていないため、この相互TLSセクションはスキップしてください。
> - enterprise-ca.cerファイルは、ログサーバーとテレメトリクライアントの両方の信頼されたルート証明機関ストアにインポートする必要があります。
> - aotclient.pfxおよびlogserver.pfx証明書はパスワードで保護しないでください。
> - aotclient.pfxのサブジェクトはCitrixAOTClientである必要があります。これにより、テレメトリクライアントは実行時に証明書を自動的に見つけることができます。

mTLSを有効にするには、ログサーバーのインストールコマンドに--caパラメーターを含めます。 このパラメーターは、enterprise-ca.cer証明書へのパスを指定します。

```
# with default path

./InstallLogServer --https --cert logserver.pfx --ca enterprise-ca.cer --
```

```
port 8443



# with customized path

./InstallLogServer --config /YourPath/LogServer/Config --database /
YourPath/LogServer/Data --cert /YourPath/logserver.pfx --ca /YourPath/
enterprise-ca.cer --port 8443



# delete temp certificate logserver.pfx in current install directory

sudo rm -rf /YourPath/logserver.pfx



# keep logserver.pfx accessed only by the container process user 'ubuntu'.

sudo chmod 400 LogServer/Config/logserver.pfx

sudo chown ubuntu:ubuntu LogServer/Config/logserver.pfx
```

相互TLS認証が必要な場合は、DDC、Storefront、VDA、およびその他のCVADコンポーネントで管理者権限を使用して、次のPowerShellコマンドを実行します。

```
# import client cert at the machine aot client

Import-PfxCertificate -CertStoreLocation Cert:\LocalMachine\My\ -FilePath
c:\aotclient.pfx



# Verify successful import

Get-ChildItem Cert:\LocalMachine\My | Where-Object { $_.Subject -like
"*AOTclient*" }



# delete temp certificate aotclient.pfx
```

```
Remove-Item -Path "C:\aotclient.pfx" -Force

# Ensure LogServer’s certificate is trusted on all machines uploading AOT
logs.
```

注:

テレメトリサービスは「ネットワークサービス」アカウントで実行されているため、certlm.mscグラフィカルインターフェイスを使用して、CitrixAOTClient証明書の秘密キーに対するNETWORK SERVICEのフルコントロールを手動で付与する必要があります。

1. Win + Rを押し、certlm.mscと入力してEnterキーを押し、証明書（ローカルコンピューター）コンソールを開きます。
2. 証明書（ローカルコンピューター） > 個人 > 証明書を展開します。
3. 右側のペインで、CitrixAOTClientに発行された証明書を見つけます。
4. 「秘密キーの管理」を開きます
5. 証明書を右クリックし、「すべてのタスク」>「秘密キーの管理」を選択します。
6. アクセス許可ダイアログで、 を選択し、「NETWORK SERVICE」と入力して、 をクリックします（NT AUTHORITY\NETWORK SERVICEに解決されるはずです）。
7. をクリックしてアクセス許可を適用します。

お客様が自己署名証明書を提供する場合、次のようにします。

- ログサーバー側では、logserver.pfx と aotclient.cer は前述のとおりインストールされます。aotclient.cer は enterprise-ca.cer の役割を果たします。
- クライアント側では、aotclient.pfx と logserver.cer は前述のとおりインポートされます。logserver.cer は enterprise-ca.cer の役割を果たします。
- 詳細については、「新しい証明書の作成」(/ja-jp/citrix-virtual-apps-desktops/2511/secure/certificates.html#create-a-new-certificate) を参照してください。

ログサーバーの確認

Log Server、VDA、またはDDCでブラウザを開き、`<http://YourLogServerFQDN:8080/Ping>` にアクセスします

ブラウザに「Pong UTC:08/19/2025 01:03:29 Version: 2511.1.6」という応答文字列が表示されます。UTC時刻はLogServerのUTC時刻である必要があります。バージョン文字列には、リリース名とビルダー番号が含まれます。

> **注:**

> デフォルトポートを使用していない場合は、ポート8080を構成済みのポートに変更し、HTTPSモードでインストールされている場合はhttpをhttpsに変更します。

> ログサーバーの検証に失敗した場合は、以下のログを確認してください。

- docker logs logserver を実行してDockerログを確認します。
- Linuxの場合 - `$HOME/LogServer/Config/weblogs.txt` (デフォルトを使用していない場合は、$HOME/LogServer を実際のインストールパスに変更してください)
- Windowsの場合 - `C:\Users\YourUserName\LogServer\Config\weblogs.txt` (YourUserNameを実際のユーザー名に変更します。C:\Users\YourUserName\LogServerを、デフォルトを使用しない場合は実際のインストールパスに変更します)

ログサーバーの詳細設定

Linux または Windows の場合

`docker stop logserver` を実行してログサーバーを停止します

デフォルトでは、ログサーバーは以下の値で構成されています。変更を行うには、Windowsにインストールされている場合は`StartLogServer.sh`または`StartLogServer.bat`を編集します。

```
-e MAX_RESERVE_DAYS=7

-e MAX_DISK_USAGE_PERCENTAGE=85

-e LOCAL_DOWN_ONLY=true

-e OPENSEARCH_JAVA_OPTS="-Xms2G -Xmx2G"
```

LOGSERVER構成オプション	デフォルト値	値の範囲	説明
LOG_LEVEL	2	0-4	0=トレース, 1=デバッグ, 2=情報, 3=警告, 4=エラー
CORS_ORIGINS		"Url" または "url1;url2;url3"	CWA H5/Chromeクライアントが AOTログをアップロードできるように、この値を変更します。複数のURLを「;」で区切って指定できます。
MAX_RESERVE_DAYS	7	1~30	ログサーバーは、タイムスタンプフィールドに基づいてログエントリを最大日数保存します。7日前に挿入されたログは削除されます。10分ごとに確認します。
MAX_DISK_USAGE_PERCENTAGE	85	10~90	ログサーバーはデータストレージの使用率を監視します。使用率が90%を超えた場合、ログサーバーは使用率が90%未満になるまで古いログを毎日削除します。10分ごとに確認します。
LOCAL_DOWN_ONLY	有効	true/false	trueの場合、ログサーバーがインストールされているマシンのみが/Download/*APIにアクセスできます。falseの場合、

LOGSERVER構成オプション	デフォルト値	値の範囲	説明
			AuthKeyを持つ他のマシンが/Download/*APIにアクセスできます。
OPENSEARCH_JAVA_OPTS	"-Xms2G -Xmx2G"	2G 〜 MaxMem/2	Opensearch のメモリ構成。ログをログサーバーに送信するマシンが多い場合は、より多くのメモリを割り当ててください。例: 0〜999台のマシン: 2GB、1000〜1999台のマシン: 4GB、2000〜9999台のマシン: 6GB

Linux で `./StartLogServer.sh` を実行して、変更が更新されたことを確認します。

Windows で `StartLogServer.bat` を実行して、変更が更新されたことを確認します。

Citrix コネクタ アプライアンスで

以下は、Citrix Connector Appliance でローカルAPIを介してログサーバーの詳細設定を構成する手順です。

これはPostman、Curl、またはPowerShellのいずれかで実行できます。以下はPostmanで実行された指示の例です。

1. **認証: JWTの生成**

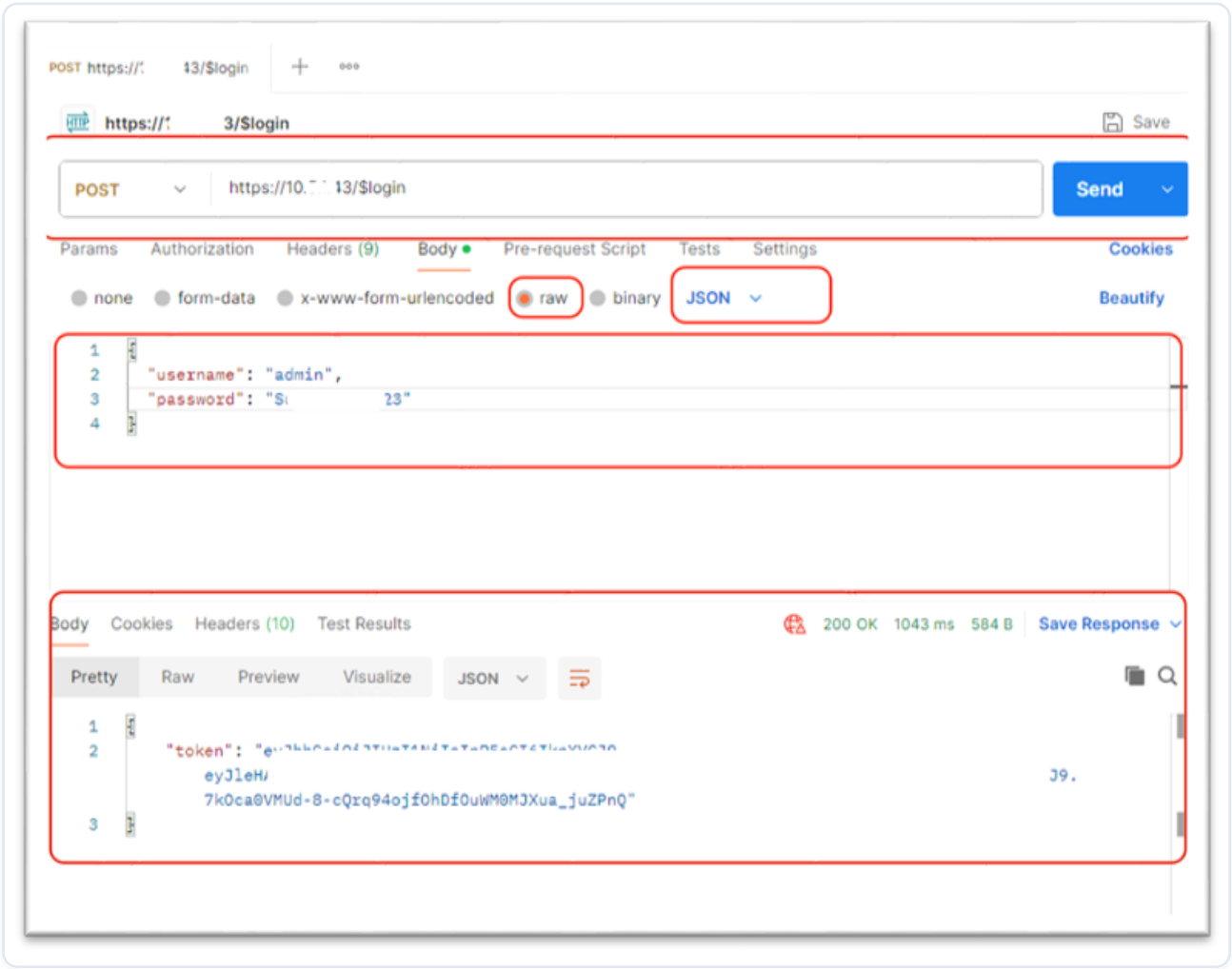
すべてのAPI呼び出しは、JSON Web Token (JWT) を使用して認証する必要があります。まずトークンを生成し、そのトークンを後続のリクエストのヘッダーに含める必要があります。

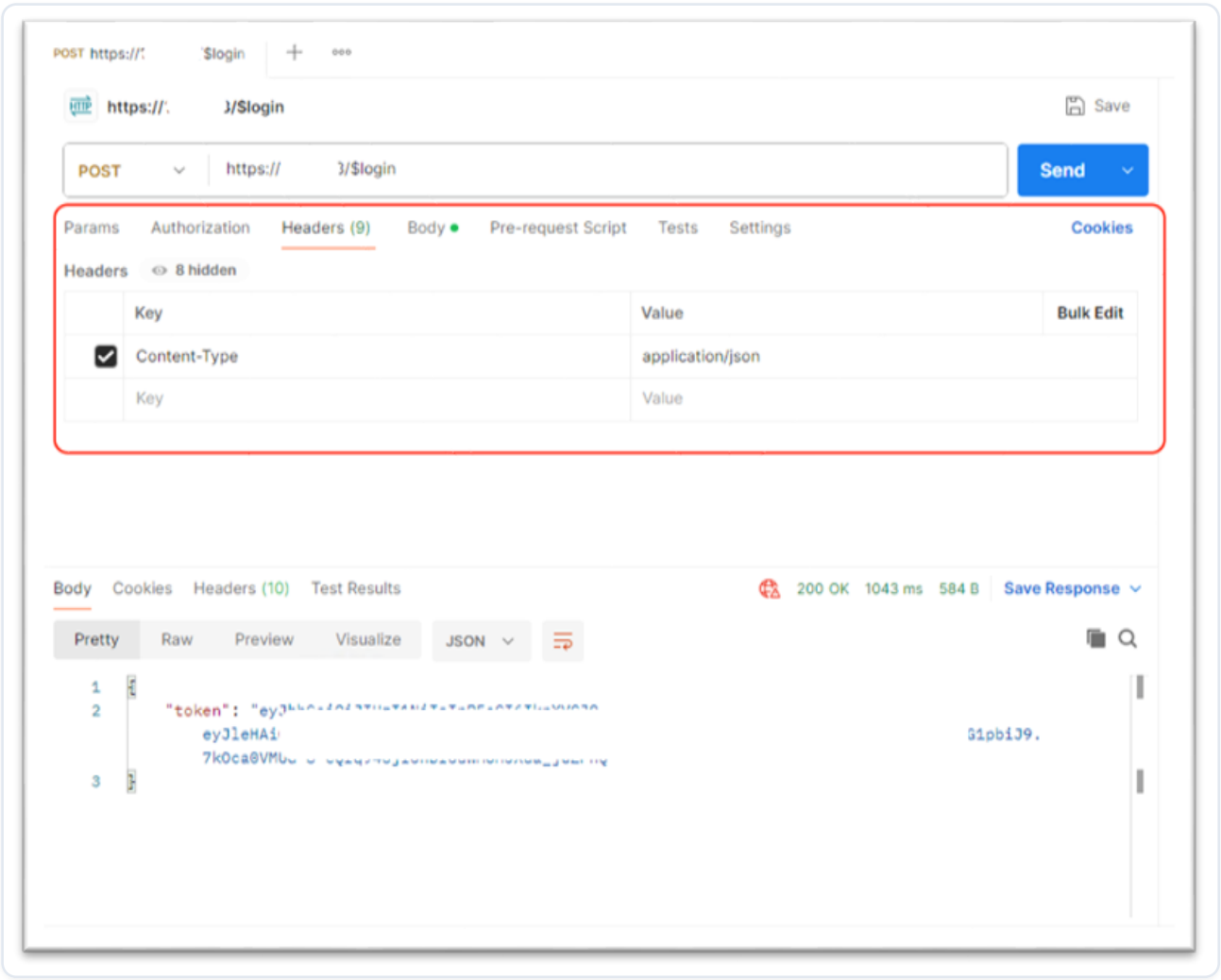
ステップ 1.1: トークンの生成

トークンを生成するには、$login エンドポイントにPOSTリクエストを実行します。

- エンドポイント: POST https:///$login

- 本文: 認証に必要なJSONペイロード (例: ユーザー名とパスワード) を含める必要があります。資格情報が正しい場合、APIはトークンを返します。



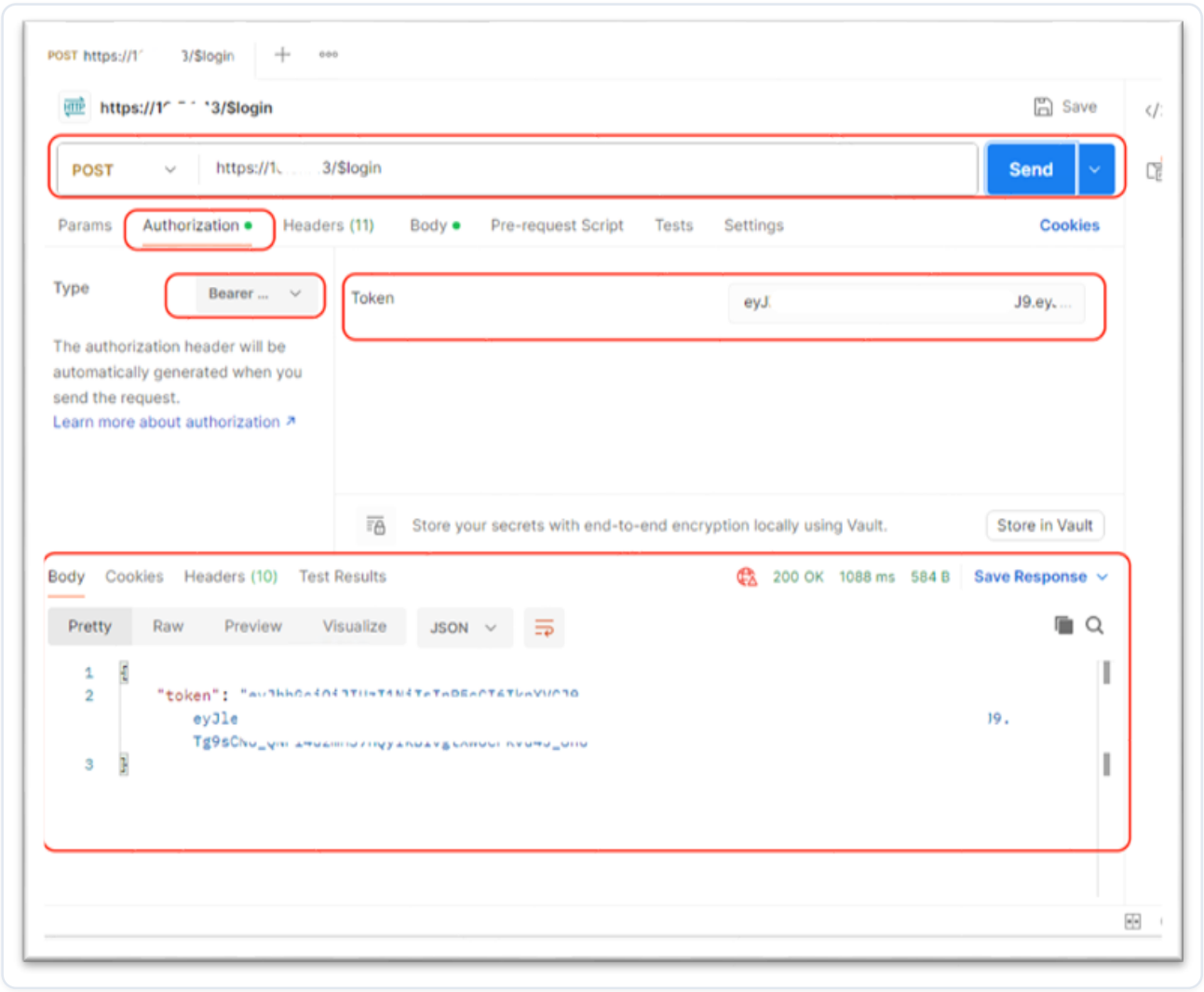


このトークン値をコピーして、次の手順で使用します。

ステップ1.2: API呼び出しを認証する

生成されたトークンを、以降のすべてのAPI呼び出しのAuthorizationヘッダーに含めます。トークンにはBearerをプレフィックスとして付ける必要があります。

認可: **Bearer abCD.efGH.ijKL**



有効なトークンはAPI呼び出しの続行を許可します。無効なトークンまたは期限切れのトークンは、エラーメッセージとともに拒否されます。

1. **詳細設定の追加**

認証後、ログサーバーのようなターゲットコンテナの設定を構成できます。
MAX_RESERVE_DAYSを構成する

このアクションは、ログサーバーのMAX_RESERVE_DAYSを構成します。

- エンドポイント: https:///providers/logserver-provider/environment
- メソッド: PATCH

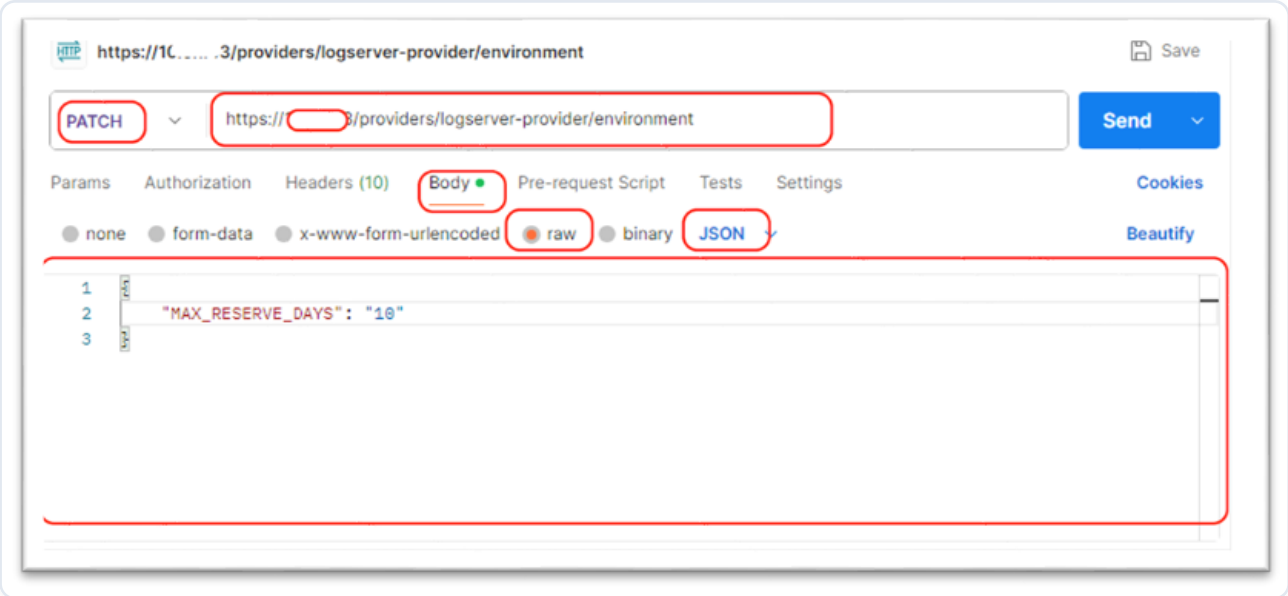
リクエストボディ

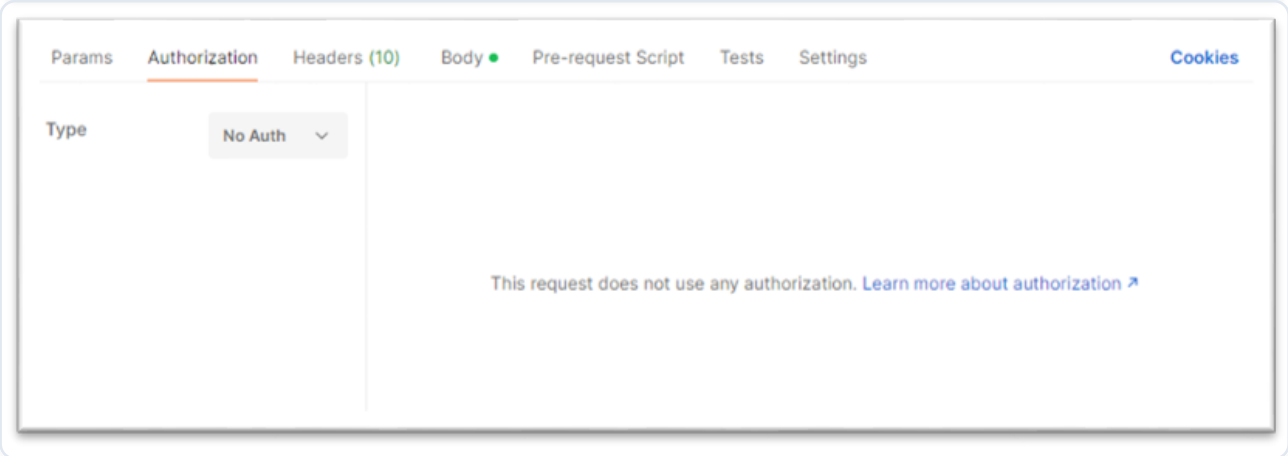
{ "MAX_RESERVE_DAYS": "7" }

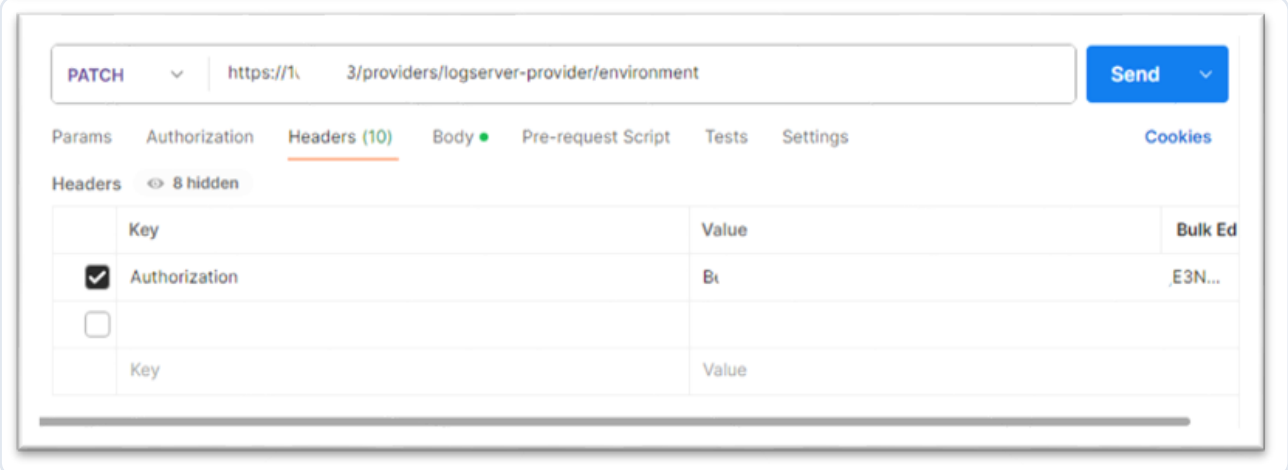
フィールド

- MAX_RESERVE_DAYS (string, 必須): デフォルト値は7日です。ログサーバーは、TimeStamp フィールドに基づいてログエントリを最大日数保存します。7日前に挿入されたログは削除されます。10分ごとにチェックします。

この例では、10日に変更しています。

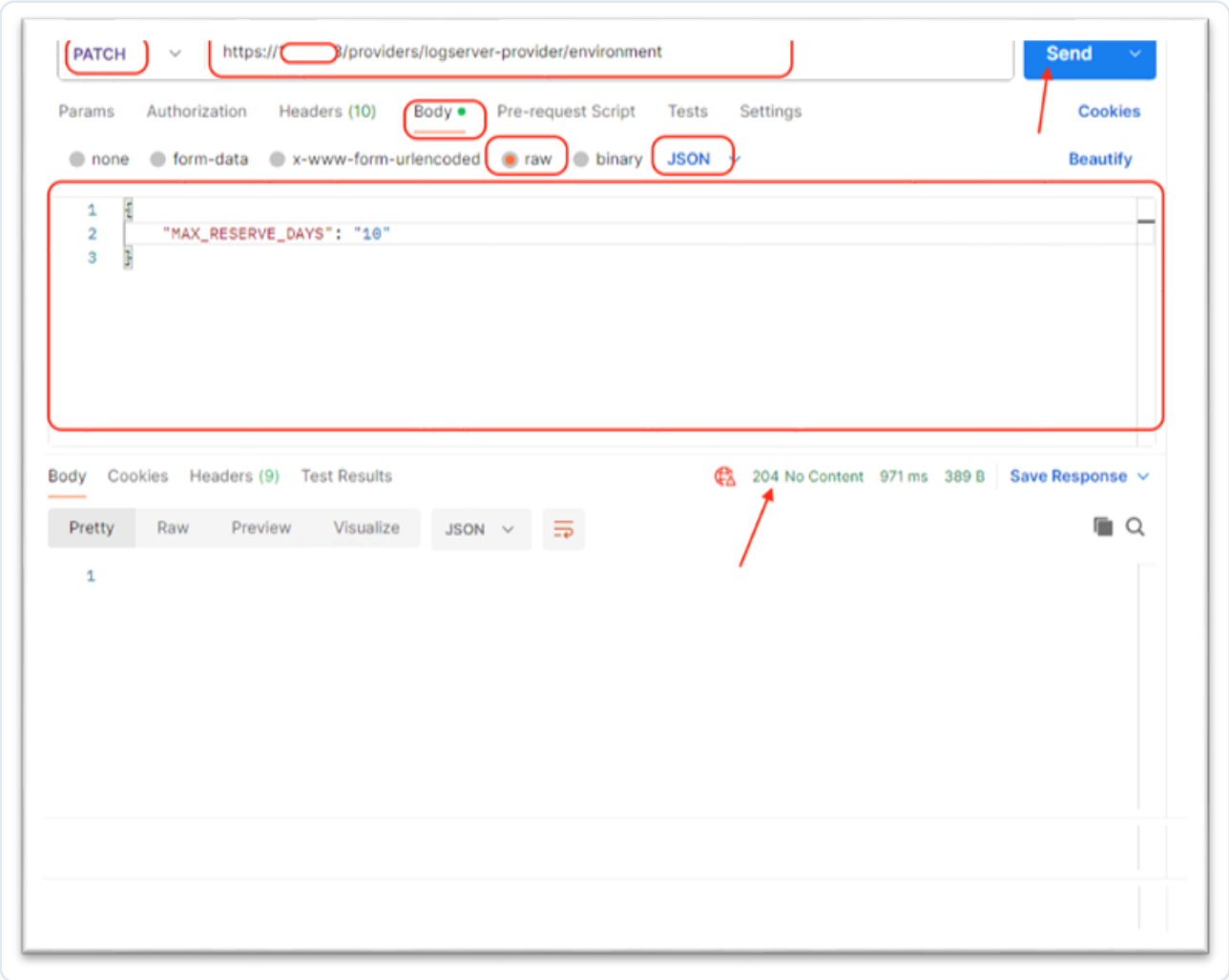




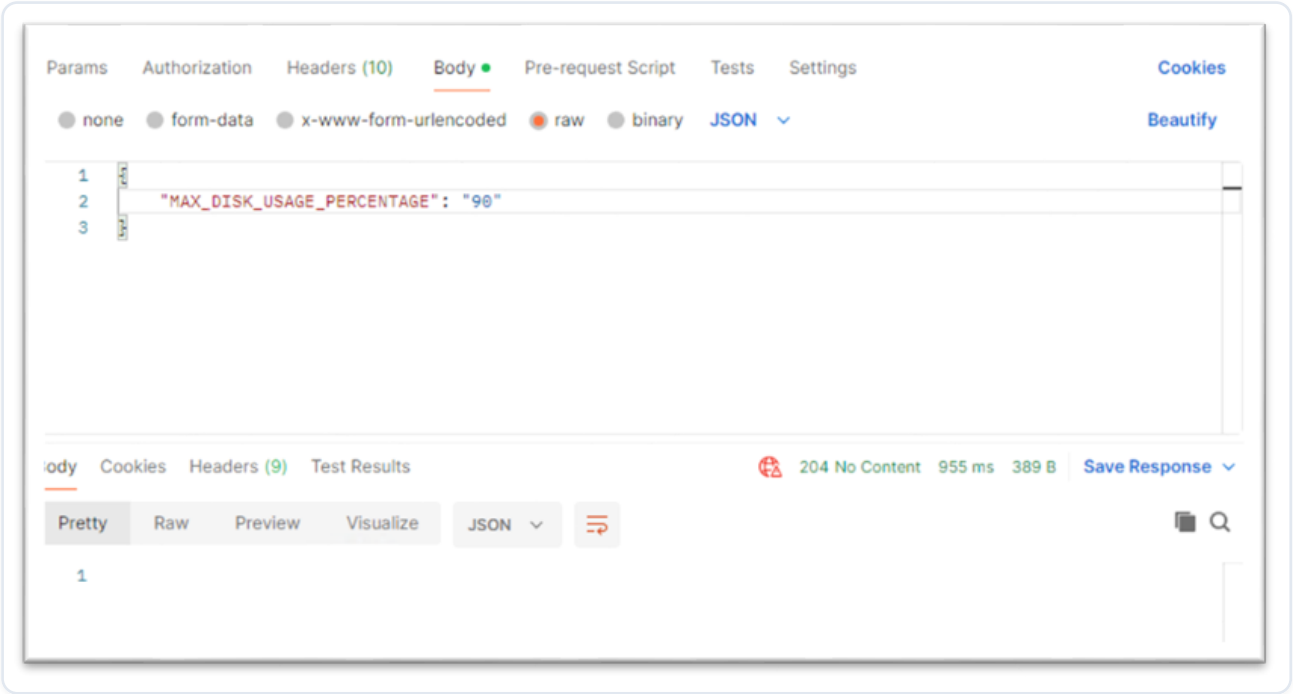


応答

✓ 成功 (204 OK) 設定が正しく構成されていることを示します



同様に、最大ディスク使用率もデフォルトの85から調整できます。ここでは90に変更します。ディスク使用率が90%に達すると、新しいログのためのスペースを確保するために古いログが削除されます。



応答

✓ 成功 (204 OK) 設定が正しく構成されていることを示します

ログサーバーのアンインストール

1. Linux でログサーバーをアンインストールする

ターミナルで以下のコマンドを実行します。

```
docker rm -f logserver

docker rmi logserver



# List containers and images to make sure



docker ps -a

docker images



# Delete Log Server config and data files if not needed any more, change
```

```
$HOME/LogServer to real installed path if not installed with the default
one



rm -r $HOME/LogServer
```

2. Windows でログサーバーをアンインストールする

PowerShell で以下のコマンドを実行します。

```
docker rm -f logserver

docker rmi logserver



# List containers and images to make sure



docker ps -a

docker images



# Delete Log Server config and data files if not needed any more, change
~/LogServer to real installed path if not installed with the default one



Remove-Item -Recurse -Force ~/LogServer
```

CVADコアコンポーネントからのAOTログのアップロード

CVAD 2507 CU1およびCVAD 2511以降、AOTログはすべての該当するコンポーネントから収集されます。サポートされているコンポーネントには、DDC、StoreFront、Citrix Director、Windows VDA、Linux VDA、Mac VDA、License Server、FAS、Cloud Connector、PVS、WEM、Session Recording、Citrix Workspace UI、およびCitrix Gatewayが含まれます。

CVADオンプレミス向けCitrix Web Studioを介した集中型ログ転送構成

Citrix Web Studioは、サイト全体でAlways-on Tracing (AOT) ログ転送を構成するための集中管理された場所を提供します。この設定は、AOTログの送信先を定義し、環境内の関連コンポーネントに構成を自動的に伝播します。

Web Studio でログサーバーを構成すると、次のようになります。

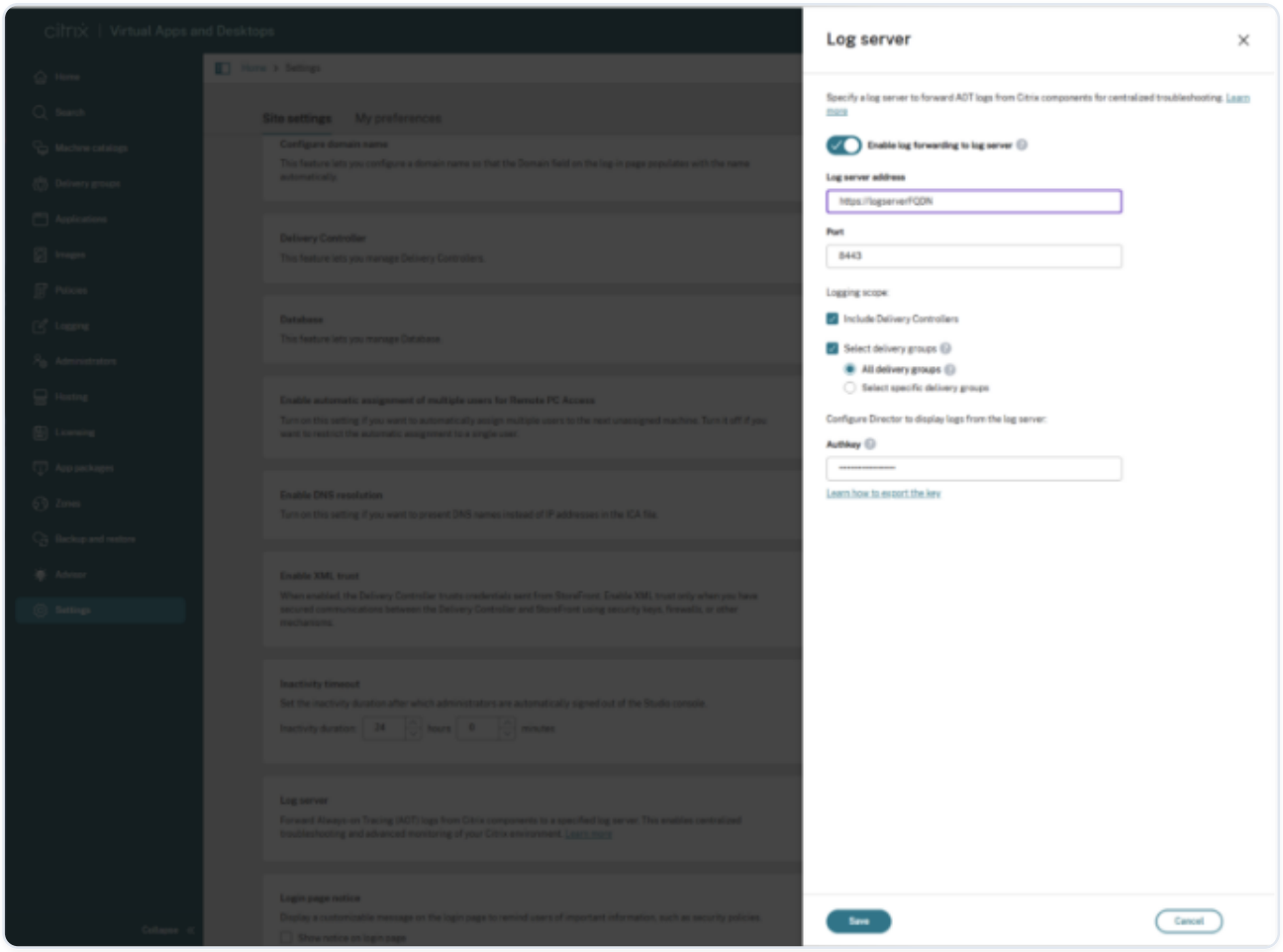
- 構成は**サイトデータベース**に書き込まれます。
- **Delivery Controller**は更新された設定を取得し、選択されたデリバリーグループ内のVDAに配布します。
- **VDA**は受信した構成を使用して、AOTログを指定されたログサーバーに転送します。
- AOTログ記録に参加する**StoreFront**は、同じ集中管理メカニズムを通じて必要な詳細情報を受け取ります。
- **Director**は、提供されたAuthKeyとログサーバーの詳細を使用して、監視およびトラブルシューティングのためにAOTログをクエリして表示します。

この集中管理アプローチにより、各コンポーネントを個別に構成する必要がなくなります。Web Studioでログサーバーの詳細を一度設定するだけで、Citrixがサイト全体に構成を自動的に伝播します。

Web Studio で設定されると、ログサーバーの詳細が取得されるコンポーネントのリストは次のとおりです。

- シトリックス ディレクター/モニター
- シトリックス デリバリーコントローラー
- ウィンドウズ VDA
- リナックス VDA
- Mac VDA
- StoreFront
- セッションレコーディングエージェント
- CWA

オンプレミス環境のログサーバー設定を構成するには



1. **Web Studio** にサインインし、左ペインで を選択します。
2. タイルで、ログサーバーが構成されていない場合は を選択します。
3. ページで、 をオンにします。
4. と を入力します。VDA と Delivery Controller はこの情報を使用して AOT ログを転送します。

> **注:**
>
> a. Citrix Connector Appliance を使用してログサーバーを展開する場合は、ポート 443 のみが構成されていることを確認してください。
>
> b. Citrix Studio でログサーバーのアドレスとポートを更新すると、最初は機能しますが、設定を再確認し、認証キーを再入力せずにログサーバーの詳細を変更すると、操作が成功したように見えても、保存後に認証キーのプレースホルダーが空になります。これにより、Director および Monitor で構成が欠落したり無効になったりします。この問題が解決されるまで、回避策として、ログサーバー設定を変更する際は常に認証キーを再入力して検証してください。

5. ログを転送するコンポーネントを選択します。

    a. **Delivery Controllerを含める**: すべてのDelivery ControllerからAOTログを送信します。

    b. **デリバリーグループを選択**: 選択したデリバリーグループ内のVDAからログを送信します。

    - **すべてのデリバリーグループ**: すべてのVDAからログを送信します。
    - **特定のデリバリーグループを選択**: 含める個々のデリバリーグループを選択します。

6. ログサーバーで生成されたAuthKeyを入力します。dDirectorはこのキーを使用してログを認証および取得します。
7. 構成を適用するには、 を選択します。

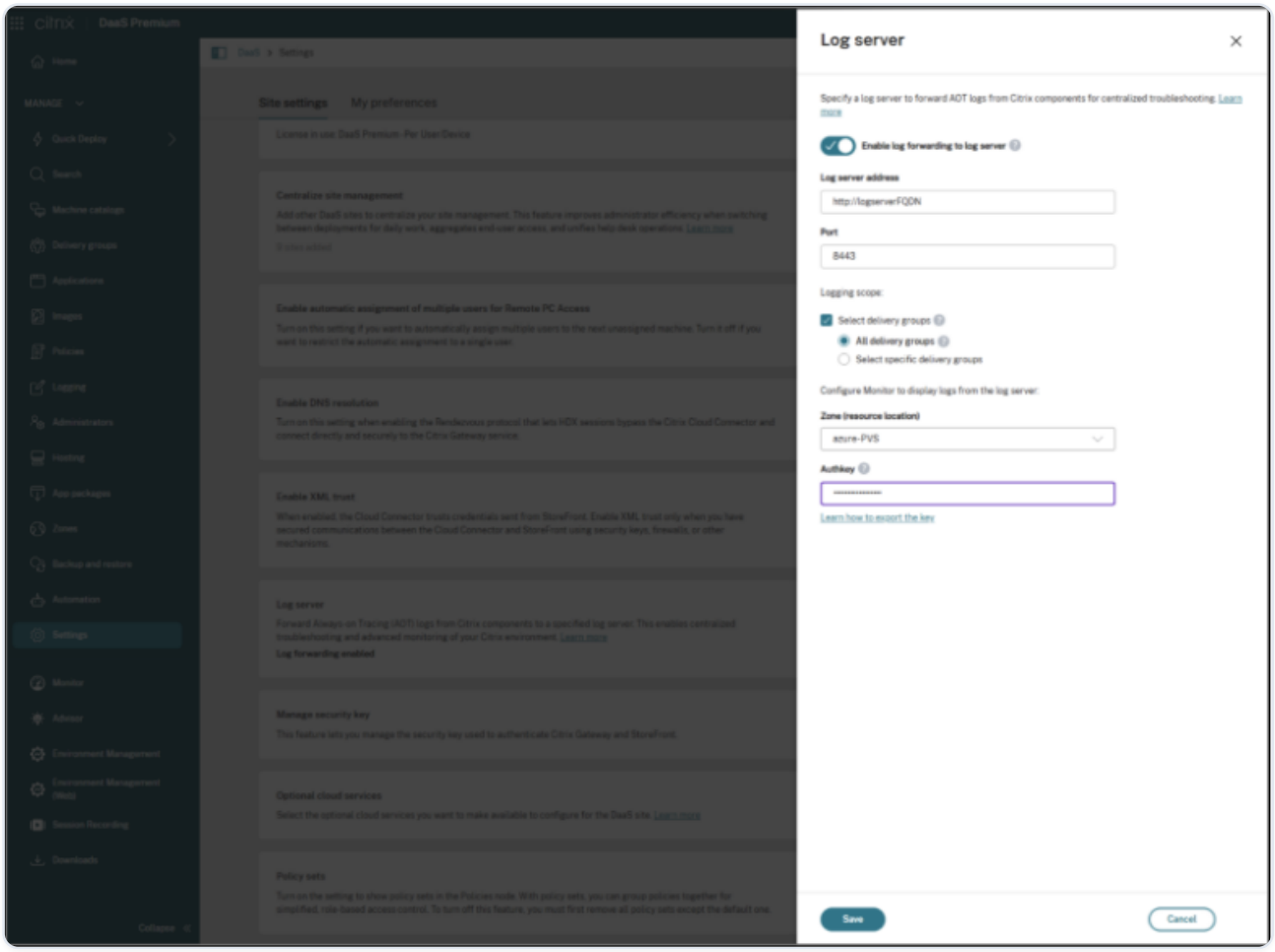
既存の構成を編集するには

ログサーバーを更新するか、ロギングスコープを変更するには、 > に移動し、 を選択します。

DaaS設定を介してCitrix DaaS/Cloud環境のログサーバー設定を構成する

Always On Tracing (AOT) は、オンプレミス (CVAD) とCitrix DaaS (クラウド) の両方の展開でサポートされています。ただし、コンポーネントがホストされている場所によってログ収集の動作が異なります。

AOTログサーバー (Linux、Windows、またはコネクタアプライアンス上) をインストールして構成した後、クラウド展開用のCitrix DaaS設定でログサーバーへのログ転送を有効にするには、以下を完了してください。



DaaS用Citrix Web Studio (DaaS設定) は、クラウド管理サイトのAlways-on Tracing (AOT) ログ転送を構成するための一元的な場所を提供します。この構成は、AOTログがどこに送信されるかを決定し、どのVDAがログ転送に参加するかを制御します。Monitorはこれらの設定を使用して、トラブルシューティングのためにログを取得および表示します。

1. DaaS用**Web Studio** (DaaS設定) にサインインし、左ペインで**** を選択します。
2. タイルで、現在ログサーバーが構成されていない場合は**** を選択します。
3. 「**ログサーバー**」ページで、「**ログサーバーアドレス**」と「**ポート**」を入力します。VDAは、この情報を使用してAOTログをサーバーに転送します。
4. どのVDAがログを転送するかを定義します。

    a. 範囲を制御するには、「**デリバリーグループの選択**」を選択します。

    b. 「**すべてのデリバリーグループ**」（既定）は、サイト内のすべてのVDAからログを転送します。

    c. 特定のVDAを対象とするには、「**特定のデリバリーグループを選択**」を選択し、含めるデリバリーグループを選択します。

> **注:**

> Citrix Connector Applianceを使用してログサーバーを展開する場合は、ポート443のみが構成されていることを確認してください。

5. ログサーバーが展開されているゾーン（リソースの場所）を選択します。
6. ログサーバーによって生成された認証キーを入力します。Monitorは、このキーを使用して認証し、表示用のログを取得します。
7. 構成を適用するには、「保存」を選択します。

その他のコンポーネントのログ転送構成

Citrix Cloud展開におけるStoreFrontのAOTログアップロードの構成

Citrix Cloud（ハイブリッド）展開の場合、Cloud DDCでオンプレミスのStoreFront（Citrix Workspaceの代わりに）を使用すると、StoreFrontはCloud ConnectorからAOTログサーバー構成を自動的に受信しません。StoreFrontサーバーで次のPowerShellコマンドを実行して、AOTログサーバーエンドポイントを手動で構成します。

```
# Enable - Run the following command in StoreFront PowerShell



Enable-CitrixAOTUpload -AoTDataStoreEndpoint https://
<FQDNofLogServer>:<server_port> -Role StoreFront



# Disable - Run the following command in StoreFront PowerShell

Disable-CitrixAOTUpload
```

注:

> このコマンドは、Cloud DDCを使用するCitrix Cloud（ハイブリッド）展開の場合にのみ実行してください。StoreFrontがオンプレミスのDelivery Controllerとペアになっているオンプレミスの CVAD展開では、ログサーバー構成は自動的に同期されるため、手動での構成は不要です。このコマンドを実行しないでください。

セッションレコーディングサーバーのAOTログアップロードの構成

Session Recording Server マシンで次の PowerShell コマンドを実行すると、Session Recording Server が AOT ログを中央ログサーバーにアップロードするように構成できます。

```
#Enable - run following command in Session Recording Server PowerShell

Enable-CitrixAOTUpload -AotDataStoreEndpoint <https://
FQDNofServer>:<server port> -Role SessionRecording



#Disable - run following command in Session Recording Server PowerShell

Disable-CitrixAOTUpload
```

FASのAOTログアップロードの構成

FAS サーバーで次の PowerShell コマンドを実行すると、FAS が AOT ログを中央ログサーバーにアップロードするように構成できます。

```
#Enable - run following command in FAS PowerShell

Enable-CitrixAOTUpload -AotDataStoreEndpoint <https://
FQDNofServer>:<server port> -Role FAS



#Disable - run following command in FAS PowerShell

Disable-CitrixAOTUpload
```

注:

FAS インストーラーの MSI ファイル (FederatedAuthenticationService_x64.msi) を使用してインストールまたはアップグレードした場合、常時オンのトレースは利用できません。

FASは常にCVAD MetaInstallerまたはXenDesktopFasSetup.exeまたはFasSetup_xxxx.exeからインストールしてください。

PVSのAOTログアップロードの構成

PVS サーバーで次の PowerShell コマンドを実行すると、PVS が AOT ログを中央ログサーバーにアップロードするように構成できます。

```
#Enable - run following command in PVS PowerShell

Enable-CitrixAOTUpload -AotDataStoreEndpoint <https://
FQDNofServer>:<server port> -Role PVS



#Disable - run following command in PVS PowerShell

Disable-CitrixAOTUpload
```

注:

複数のPVSサーバーがある場合は、それぞれのサーバーでAOTログのアップロードを有効または無効にするコマンドを実行してください。

License Server の AOT ログのアップロード

- Logserver URL は、SLS 設定ファイル内で更新する必要があります。このファイルは「C:\Program Files (x86)\Citrix\Licensing\WebServicesForLicensing\SimpleLicenseServiceConfig.xml」にあり、XML タグ「AotServerURL」で指定されます。

例：

```
<AotServerURL>https://<FQDNofLogServer:443>//ctxlogserver/
UploadCitrixLogStream</AotServerURL>
```

注:

License Server でログはいつ生成されますか？

> ライセンスサーバーのAOTログは、ライセンスサーバーのインストールまたはアップグレード、WSL (Citrix Web Services for Licensing) サービスの再起動、ライセンスアクティベーションの失敗、ダークサイトアクティベーションの失敗、クロック関連のライセンス問題など、特定のイベント中にのみ生成されます。

> これらのイベントのいずれも最近発生していない場合、ログがないことは必ずしも問題を示しているわけではありません。

クイックチェック

1. 最近、対象となるイベント（再起動、アップグレード、アクティベーションの問題など）が発生したかどうかを確認します。
2. Citrix Web Services for Licensing サービスを再起動し、アップロード処理に最大1時間かかります。
3. AOT Log Server URL が正しく構成されていることを確認します。
4. Citrix Web Services for Licensing サービスが実行中であることを確認します。
5. 確認: `C:\Program Files (x86)\Citrix\Licensing\LS\resource\aot` ファイルにデータが含まれている場合、ログはアップロードを待機している可能性があります。

> **注:**
>
> ライセンスサーバーのAOTログはイベント駆動型であり、継続的ではありません。適格なイベントが発生していない場合にログが表示されないのは正常です。

- License Server は、定期的にログを AOT サーバーに自動的にアップロードします。

Citrix Connector の AOT ログアップロードを構成する

AOT Log Server で Cloud Connector ログを収集するには、次の要件が適用されます。

- Cloud Connector は **バージョン 6.169.0.22492 以降**である必要があります。
- **Cloud DDC 展開**では、ログサーバーの構成詳細は**5月リリース**でレジストリに自動的に同期され、手動での構成は不要です。
- **ハイブリッド展開（オンプレミスDDC）**では、ログ収集を有効にするために手動でのレジストリ構成が必要です。Cloud Connectorマシンで以下のレジストリエントリを作成します。

パス: `HKLM\Software\Citrix\ConfigSyncService`

エントリ:

- `LogServerEnabled (REG_DWORD) = 1`
- `LogServerEndpoint (REG_SZ) =` https://<logserver-fqdn `:<port>>`

Citrix Workspace アプリの AOT ログアップロードを構成する

Citrixは、Citrix Workspaceアプリクライアントが診断ログを一元化されたログサーバーに自動的にアップロードする機能を提供します。この機能により、管理者は手動でのログ収集を必要とせずにクライアント側の診断情報に即座にアクセスできるようになり、トラブルシューティングの効率が向上します。クライアント側のAOTは自動的にアップロードされ、CVAD環境全体でAOT機能が有効になっている場合、およびユーザーがリソースを起動した場合にトリガーされます。

システム要件

- Citrix Virtual Apps and Desktops 2511 または CVAD 2507 CU1 以降のバージョン
- Citrix Workspace アプリ 2511 または CWA 2507.1 CU1 以降のバージョン
- 選択した Citrix Workspace アプリ (CWA) の必要なバージョンがインストールされていることを確認してください。詳細については、サポートされているバージョンを参照してください。

前提条件

CITRIX WORKSPACE アプリの WEB 起動

Citrix WorkspaceアプリのWeb起動（WebHelper、直接ICAファイルダウンロード、Webブラウザ拡張機能起動方法を含む）の場合、StoreFrontは最新のユーザーインターフェイス（UIエクスペリエンス）を使用するように構成する必要があります。 最新のUIエクスペリエンスを有効にする手順については、StoreFrontのドキュメントを参照してください。

> **注:**
>
> この前提条件は Web ベースの起動にのみ適用され、ネイティブの Citrix Workspace アプリの起動には必要ありません。

NetScaler の AOT ログアップロードを構成する

- NetScaler CLIにSSHで接続し、「shell」コマンドを実行してNetScalerシェルに入ります。
- /var/analytics_confディレクトリに移動します

```
cd /var/analytics_conf
```

- 対話型Pythonスクリプト「python {auditlog_schema_generator_for_hec_export.py}」を実行してスキーマファイルを生成します。スキーマファイルは、HTTPヘッダー（Auth-token、User-Agentなど）とペイロード属性（Role、Machine IPなど）を定義します。

このスクリプトによって生成された出力のスニペット

```
root@Raju-adc2# python auditlog_schema_generator_for_hec_export.py

Schema Builder: Follow the prompts to define your schema.

Include 'Auth-Token'? (Y/n):

Enter the display name (alias) for 'Auth-Token' (press Enter to keep as
is): Authkey

'Auth-Token' can only go in 'header'. Automatically selected.

Include 'HostName'? (Y/n): n

Include 'Content-type'? (Y/n): y

Enter the display name (alias) for 'Content-type' (press Enter to keep as
is):

'Content-type' can only go in 'header'. Automatically selected.

Default value for 'Content-type' is 'application/json'.

Do you want to change it? (y/N):

Include 'User-agent'? (Y/n):

Enter the display name (alias) for 'User-agent' (press Enter to keep as
is):

'User-agent' can only go in 'header'. Automatically selected.

Default value for 'User-agent' is 'AUDITLOGS/1.0'.

Do you want to change it? (y/N):

Include 'Role'? (Y/n): y
```

```
Enter the display name (alias) for 'Role' (press Enter to keep as is):

Where should 'Role' be included? (HEADER/payload): HEADER

Default value for 'Role' is 'GW'.

Do you want to change it? (y/N): y

Enter new default value for 'Role': Gateway
```

生成されたサンプルスキーマファイル

```
{

     "Header": {

         "Auth-Token": {

             "name": "AuthKey"

         },

         "Content-type": {

             "name": "Content-type",

             "value": "application/json"

         },

         "User-agent": {

             "name": "User-agent",

             "value": "AUDITLOGS/1.0"

         },

         "Role": {

             "name": "Role",
```

```
            "value": "Gateway"
        },
        "MachineIP": {
            "name": "MachineIP"
        },
        "MachineName": {
            "name": "MachineName"
        }
    },
    "Payload": {
        "LogLevel": "Level",
        "MessageContent": "Message",
        "ModuleName": "Module",
        "Time": "TimeStamp"
    },
    "Format": {
        "delimiter": ""
    }
}
```

- シェルを終了し、NetScaler CLIに戻ります
- Syslogサーバー、ポート、および（前のステップで作成した）スキーマファイルなどを定義するsyslogアクションを作成します。

```
add audit syslogAction {Action Name} {AOT Server IP/FQDN} -serverPort
{Destination Port} -logLevel {Log Level} -transport HTTP -httpAuthToken
{Authentication Token generated on the AOT sever} -httpEndpointUrl {AOT
Server URL where logs will be sent} -httpSchemaFile {Schema File created
in Previous Step}
```

例:

```
add audit syslogAction act1 10.102.154.196 -serverPort 8088 -logLevel ALL
-transport HTTP -httpAuthToken
fbb94d5b234d86a6cb155e3f808dd33c9698a0d1a866e814573b1909e4c9e56896f433da10
71e3276bd133269fd69203d8f29166816f4d427e709773ceb9d41d531043331f7f76
-httpEndpointUrl "/services/collector/event" -httpSchemaFile sample.json
```

- syslogActionを監査Syslogポリシーにバインドします

```
add audit syslogPolicy {PolicyName} True {Name of the Syslog Action}
```

例:

```
add audit syslogPolicy pol1 true act1
```

AOTログの表示と使用

Director UI経由でのログへのアクセス

ステップ1

`StartLogServer.bat`ファイルを編集する

`StartLogServer.bat`ファイルには、AOTログサーバーコンテナの起動に使用されるすべての構成パラメータが含まれており、ログアクセスと動作を制御するいくつかの環境変数も含まれています。主要な設定の1つは**LOCAL_DOWN_ONLY**です。

- **LOCAL_DOWN_ONLY=false**の場合、ログサーバーはリモートログ表示要求を受け入れます。これにより、**Citrix Director/Monitor**がログサーバーに接続し、Monitor UIにAOTログを直接表示できるようになります。

- **LOCAL_DOWN_ONLY=true**の場合、ログサーバーはログアクセスをローカル接続のみに制限します。このモードでは、ログを表示するにはログサーバーマシンに直接接続する必要があり、**Citrix Director Monitorはログを取得または表示できません。**



ステップ 2

Web Studioには、**Citrix Director**がAOTログサーバーに接続し、Monitorコンソールにログを表示できるようにする専用の設定が用意されています。Web Studioの設定が保存されると、デリバリーコントローラーはサイト構成を更新し、Directorはログサーバーのアドレス、ポート、認証キーを含むログサーバーの詳細を受け取ります。Directorはこれらの設定を使用して、ログサーバーへの安全な接続を確立します。

ステップ3

構成後：

1. **Citrix Director**を開きます。
2. 左側のナビゲーションパネルに新しい**ログ**オプションが表示されます。
3. **ログ**を選択すると、「はじめに」ページが表示されます。これらの設定はすでに完了しているため、**閉じる**をクリックしてスキップしてください。
4. これで、Director がログサーバーから直接 AOT ログを取得して表示するようになります。



Directorの**ログ**ページでは、Delivery Controller、VDA、StoreFrontサーバー、およびその他のCitrixコンポーネントからのAOTイベントを統合的に表示できます。ログをリアルタイムで検索、フィルター処理、検査して、問題を迅速にトラブルシューティングできます。

フリーテキスト検索: ログページの上部には、フリーテキスト検索バーがあります。キーワードを入力して結果を絞り込むことができます。フィルターを適用すると、検索結果は即座に更新されます。例を次に示します。

- ユーザー名
- マシン名
- イベントキーワード（例：登録、認証、STA）
- トランザクションID
- エラーメッセージまたは部分文字列

時間フィルター: 時間セレクター（例：過去5分、過去1時間、過去24時間）を使用して、特定の期間内に生成されたログを表示します。これにより、問題が発生した正確な時刻周辺のイベントを迅速に特定できます。

カテゴリフィルター: フィールドを使用すると、イベントまたはサブシステムの種類に基づいてログをフィルター処理できます。これにより、アプリケーション起動、登録、VDA 構成、グラフィック、HDX Direct、ICA 接続などに関連するログに焦点を当てることができます。

ログクラスフィルター: ログクラスフィルターは、ログを重大度またはイベントタイプでグループ化します。これにより、トラブルシューティング時にエラーや重要なイベントのみに焦点を当てることができます。一般的なクラスには次のものがあります。

- 情報
- 警告
- エラー
- 失敗

ホスト名フィルター: ホスト名フィルターを使用すると、VDA、デリバリーコントローラー、CWA、StoreFrontサーバーなどの特定のコンピューターを選択できます。これは、展開全体を検索するのではなく、単一のエンドポイントまたはVMのログを詳しく調べたい場合に役立ちます。

この一元化されたアクセスにより、単一のコンソールからログを迅速に取得および分析できるため、トラブルシューティングが効率化されます。前提条件と開始方法の詳細については、Director - ログを参照してください。

ログサーバーを介したログへのアクセス

以下の内容でAuthKeyを生成します。ログへのアクセスを有効にするには、ユーザーは以下を行う必要があります。

1. `StartLogServer.bat`スクリプトの「**LOCAL_DOWN_ONLY=false**」を修正します。
2. AuthKeyを生成する

ログを安全に保つため、ダウンロードする前に**AuthKey**が必要です。手順は次のとおりです。

1. **AuthKeyを取得する** – 自身のロール名/名前を使用して生成します。
2. **ローカルで実行する** – スクリプトは、Dockerコンテナがインストールされているマシンでのみ実行できます。
3. **Windowsユーザー** – シェルスクリプトの代わりに`GetAuthKey.bat`スクリプトを使用してください。

4. **ログをダウンロードする** – 認証が完了すると、安全にログを取得できます。

AOTログサーバーの認証キーの生成と管理

提供されている.sh (Linux) または .bat (Windows) スクリプトを使用すると、特定のロールまたはユーザーの新しい認証キーを迅速に生成できます。これらのスクリプトは、生成されたキーと関連するロールを返すことでプロセスを簡素化します。

Linuxの場合

```
./GetAuthKey.sh role-name
```

Windows向け

```
GetAuthKey.bat role-name
```

AOTログサーバーは、さまざまなロールまたはユーザーに関連付けられた認証キーを管理するためのコマンドを提供します。これらのコマンドにより、管理者はコンテナから直接認証キーを**追加、一覧表示、検証**し、**削除**できます。利用可能なdocker execコマンドをログサーバーコンテナで直接使用してください。

- **新しい認証キーを追加する**: 指定されたロールまたはユーザーの新しい認証キーを作成します。

```
docker exec logserver /app/authkey add <RoleName>
```

- **すべての認証キーを一覧表示**: 認証キーが作成されている既存のすべてのロール/ユーザーを表示します。

```
docker exec logserver /app/authkey list
```

- **認証キーを検証**: 指定された認証キーが有効であるかどうかを確認し、関連付けられているロールを識別します。

```
docker exec logserver /app/authkey validate <key>
```

- **認証キーを削除**: 特定のロールに関連付けられている認証キーを削除します。

```
docker exec logserver /app/authkey del <RoleName>
```

- **コマンドの使用法を表示**: 認証キー管理で利用可能なオプションを表示します。

```
docker exec logserver /app/authkey ??
```
?

以下の例は、認証キーの管理方法を示しています。



AOTログをログサーバーにすでに送信したマシン名を一覧表示

このパラメーターは、GetAuthKey.sh から取得したキーです。

Linuxの場合

```
./ListMachines.sh ebac9b7726cb4be597c92c6769134d25

{"machines":["MachineName"]}
```

空のマシンは、ログがないことを意味します。

Windowsの場合

```
ListMachines.bat ebac9b7726cb4be597c92c6769134d25

{"machines":["MachineName"]}
```

LogServerが「-e LOCAL_DOWN_ONLY=false」で起動する場合のWindows PowerShell:

```
Invoke-WebRequest -Uri "https://logserver_fqdn:8443/ctxlogserver/Download/
ListMachine" -Headers @{ AuthKey = "ebac9b7726cb4be597c92c6769134d25" }
```

logserver_fqdn をログサーバーの実際のFQDNに、8443 をログサーバーの実際のポートに置き換えます。HTTPモードでインストールされている場合は、https を http に置き換えます。

空のマシンは、ログがないことを意味します。

マシン名と時間範囲でログをダウンロードします。

時刻はUTC形式です: YYYY-mm-ddTHH:MM:SSZ。

```
#Usage: ./DownloadLogsByTime.sh [AuthKey] [MachineName] [StartTime|YYYY-
mm-ddTHH:MM:SSZ] [EndTime|YYYY-mm-ddTHH:MM:SSZ] [OutputFile]

#Example:
```

Linuxの場合

```
./DownloadLogsByTime.sh ebac9b7726cb4be597c92c6769134d25 MachineName
2025-01-01T00:00:00Z 2025-01-02T00:00:00Z logs.csv
```

Windowsの場合

```
DownloadLogsByTime.bat ebac9b7726cb4be597c92c6769134d25 MachineName
2025-01-01T00:00:00Z 2025-01-02T00:00:00Z logs.csv
```

LogServerが「-e LOCAL_DOWN_ONLY=false」で起動する場合のWindows PowerShell:

```
Invoke-WebRequest -Uri "https://logserver_fqdn:8443/ctxlogserver/Download/
TimeRange?start=2025-01-01T00:00:00Z&end=2025-01-02T00:00:00Z" -Headers
@{ AuthKey = "ebac9b7726cb4be597c92c6769134d25" } -OutFile logs.csv
```

キーワード/フィルターでログをダウンロードします。時刻はUTC形式です

注:

- キーワードは単一の単語でも、複数の単語の組み合わせでも構いません。
- キーワードはログメッセージ内のどこにでも一致させることができます。
- **トランザクションID**もキーワードとして使用できます。

```
#Usage: ./DownloadLogsByWords.sh [AuthKey] [StartTime|YYYY-mm-
ddTHH:MM:SSZ] [EndTime|YYYY-mm-ddTHH:MM:SSZ] [SearchWords] [OutputFile]

#Example:
```

Linuxの場合

```
./DownloadLogsByWords.sh authkey 2025-01-01T00:00:00.000Z
2025-12-31T23:59:59.999Z "session launch" logs.csv
```

Windowsの場合

```
DownloadLogsByWords.bat authkey 2025-01-01T00:00:00.000Z
2025-12-31T23:59:59.999Z "failed vda" logs.csv
```

LogServerが「-e LOCAL_DOWN_ONLY=false」で起動する場合のWindows PowerShell:

```
Invoke-WebRequest -Uri "https://logserver_fqdn:8443/ctxlogserver/Download/
SearchLog?start=2025-01-01T00:00:00Z&end=2025-01-02T00:00:00Z&words=failed
vda" -Headers @{ AuthKey = "ebac9b7726cb4be597c92c6769134d25" } -OutFile
logs.csv
```

単語はスペースで区切られます

Always On Tracing の一般的な問題のトラブルシューティング

対象: Citrix Virtual Apps and Desktops 2402 CU4、2507 CU1、2511、2603 以降、DaaS

必須: AOT Log Server が展開されていること。AuthKey が Director または Monitor の設定で構成されていること。

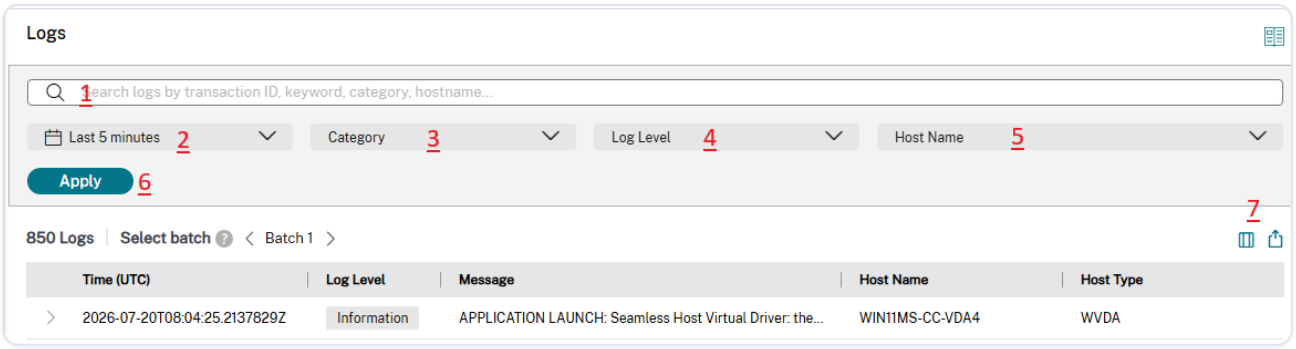
Always On Tracing (AOT) は、すべての Citrix コンポーネント（VDA、Delivery Controller、StoreFront、License Server、Citrix Workspace App）でログを継続的にキャプチャします。問題が報告されたときには、すでにデータが存在しています。この記事では、Citrix Director または Monitor の **ログ** ノードを使用して問題の原因を特定する方法と、Citrix テクニカルサポートに提出するために Director または Monitor からログをエクスポートする方法について説明します。

開始する前に — すべてのシナリオでこれを収集してください

- **影響を受けるユーザーまたはマシン** — 特定のユーザー名、VDA ホスト名、またはデリバリーグループ名
- **障害発生時刻** — おおよその時間帯でも、デフォルトの時間フィルターを絞り込むのに役立ちます。報告された障害発生前の期間をカバーするように時間範囲を調整してください。
- **スコープ** — 1人のユーザー、1台のマシン、それとも環境全体か？ログを開く前に、スコープだけで正しい障害パターンがわかることがよくあります。
- **最近の変更** — 関連する期間における CVAD の更新、グループポリシーの変更、電源管理の変更、またはネットワークの変更

Director および Monitor のログノード

ログノードは、**Citrix Director** (オンプレミス CVAD) と **Citrix Monitor** (DaaS) の両方で利用できます。アクセスするには、左側のナビゲーションパネルから **ログ** を選択します。インターフェイスはどちらの環境でも同じです。



1. **検索バー** — キーワード、トランザクション ID、カテゴリ、またはホスト名
2. **時間フィルター** — 障害をカバーする時間帯を選択します
3. **カテゴリフィルター** — イベントタイプでフィルターします
4. **ログレベルフィルター** — 重大度でフィルター
5. **ホスト名フィルター** — 1台以上のマシンを選択
6. **適用ボタン** — すべてのアクティブなフィルター選択を適用します
7. **エクスポートアイコン** — ログをダウンロードしてCitrixテクニカルサポートに提出します

フィルターバー

フィルターバーには4つのフィルターと、独立した**適用**ボタンがあります。まずフィルターを設定し、**適用**をクリックしてログビューを更新します。現在のログ数はフィルターバーの下に表示されます（例: *バッチ1に850個のログ*）。バッチナビゲーション矢印を使用して、大規模な結果セットをページ移動します。

フィルター	機能	オプション
時間	ログ取得の時間枠を設定します。報告された障害の前に開始する時間枠に設定して、その障害につながったイベントをキャプチャします。	過去5分 · 過去1時間 · 過去24時間 · 過去48時間 · 過去7日間 · カスタム (UTC) *(CVAD 2603以降のクラウドリリースのみ)*
カテゴリ	イベントタイプでフィルターします。各カテゴリは、Citrixコンポーネントのライフサイクルの特定の側面に対応して	アプリケーション起動 · クリップボード · CWA-PostLaunch · CWA-

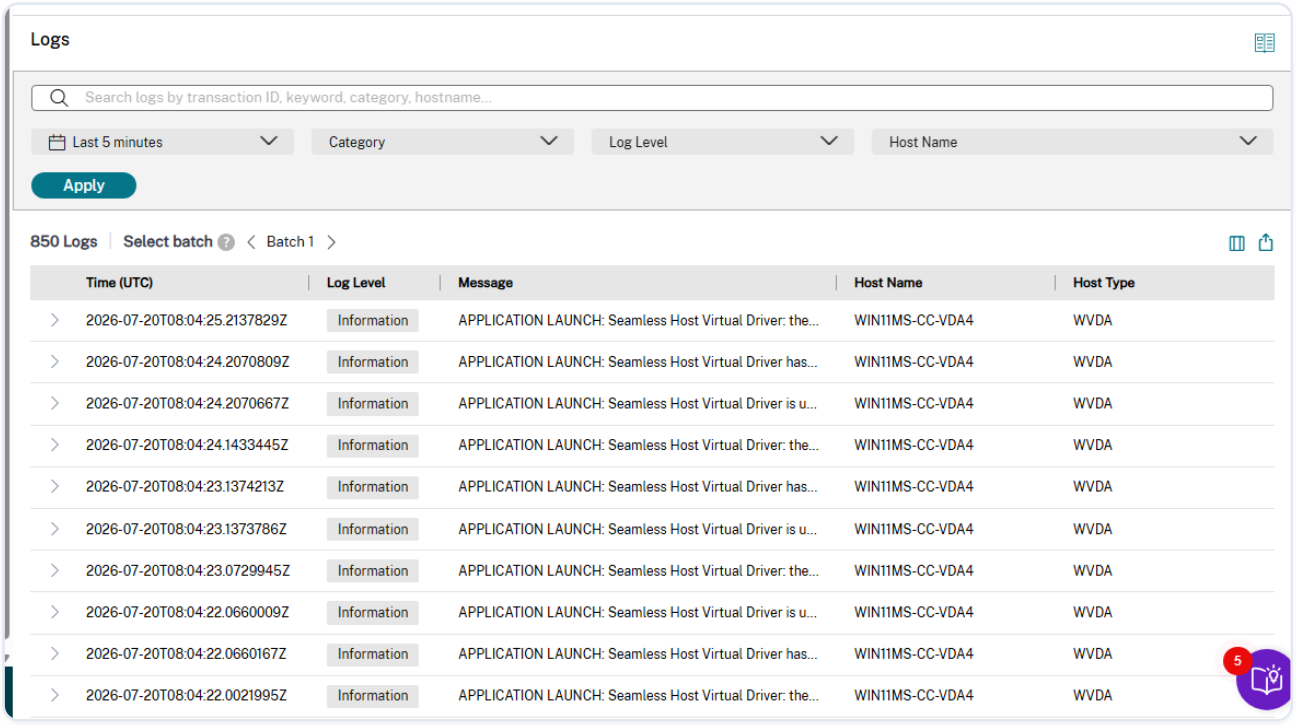
フィルター	機能	オプション
	います。カテゴリ名をすばやく見つけるための検索カテゴリフィールドが含まれています。	PreLaunch · データベース · デバイス · など
ログレベル	重大度でフィルタリングします。1つ以上選択します。選択がアクティブな場合、ボタンのラベルには選択された数（例：*1 Log Level Selected*）が表示されます。	情報 · 警告 · エラー · 重大
ホスト名	1つ以上の特定のコンピューターにフィルタリングします。ホスト検索フィールドと、現在ログをログサーバーに送信しているすべてのコンピューターのチェックボックスリストが含まれます。アクティブな場合、*N Hostname Selected*と表示されます。	ログサーバーに登録されているすべてのコンピューター

ログレベル	使用するタイミング
情報	標準コンポーネントイベント — セッション開始、VDA登録、ライセンスチェックアウト。完全なライフサイクルシーケンスを確認するために使用します。
警告	問題を示す可能性のある重要ではない問題 — セッション切断、アイドルタイムアウト、ハートビート警告。**切断シナリオの場合はここから開始します。**
エラー	調査が必要な障害 — 起動エラー、登録失敗、ライセンス枯渇。**ほとんどのシナリオの場合はここから開始します。**

ログレベル	使用するタイミング
重大	サービスに影響を与える重大な障害 — 通常、コンポーネントのクラッシュまたは回復不能な状態

ログテーブル — 列

ログテーブルには、各エントリに対してデフォルトで5つの列が表示されます。「列」ボタンをクリックすると、新しい列を追加できます。任意の行の > 展開矢印をクリックすると、完全なログメッセージと追加フィールドが表示されます。



アプリケーション起動カテゴリがアクティブなログテーブル。ログ数とバッチナビゲーションはテーブルの上に表示されます。> 矢印で任意の行を展開して、完全なメッセージを読みます。

列	表示される内容
時刻 (UTC)	イベントのUTCタイムスタンプ。ミリ秒単位の精度。発生順にイベントのシーケンスを読み取るには、昇順でソートします。
ログレベル	重大度バッジ: 情報、警告、エラー、または致命的
メッセージ	コンポーネントからのログメッセージ。テーブルでは切り詰められています。行の > 展開矢印をクリックして、完全なメッセージを読み取

列	表示される内容
	ります。完全なメッセージは主要な診断テキストです。
ホスト名	ログエントリを生成したマシン
ホストタイプ	コンポーネントタイプ: DDC、StoreFront、WVDA (Windows VDA)、CWAWindows、その他Log Serverに登録されているものによって異なります

Citrixテクニカルサポート向けログのエクスポート

エクスポートアイコン (上記の注釈付きスクリーンショットの**7**) は、ログセクションの右上隅に表示されます。これを使用して、現在フィルターされているログビューをファイルとしてダウンロードします。エクスポートする前に:

> **バージョン提供状況:**

> エクスポートアイコンは、Cloud 129 (2026年4月〜5月) リリース以降のDaaSで利用でき、CVAD 2603以降のCitrix Virtual Apps and Desktopsでも利用できます。それ以前のバージョンではこのオプションは利用できません。

> **AuthKeyが必要です:**

> 「ログ」ノードは、AuthKeyがDirectorまたはMonitorの設定で構成されている場合にのみデータを表示します。AuthKeyはログサーバーのセットアップ中に生成されます。AuthKeyがない場合、「ログ」ノードにはエントリが表示されません。

シナリオ1: セッション起動の失敗

ユーザーが公開されたデスクトップまたはアプリケーションをクリックすると、起動エラーが発生します。セッションは開かれません。エラーはCitrix Workspace Appの画面に表示されるか、プログレスバーが停止してタイムアウトし、セッションが接続されない場合があります。

ログノードで、**カテゴリ**を**Application Launch**に、**ログレベル**を**Error**に設定し、**時間**を障害発生期間をカバーするように調整します。**適用**をクリックします。**時間 (UTC)** で昇順にソートし、

メッセージと**ホストタイプ**の列を合わせて読みます。これらは、起動パスのどのコンポーネントが失敗し、何を報告したかを示します。

> **参照のみ：**

> 以下のログメッセージは例示です。実際の環境でのメッセージは同じ形式と列構造に従いますが、正確な文言は異なる場合があります。

例: デリバリーグループで利用可能なVDAがありません

DDCは起動要求を受け取りましたが、デスクトップを割り当てることができませんでした。デリバリーグループ内のすべてのVDAが未登録であるか、セッション容量に達していました。

時刻 (UTC)	ログレベル	メッセージ	ホスト名	ホストの種類
2026-07-20T09:14:22.1034Z	情報	APPLICATION LAUNCH: ユーザー DOMAIN\jsmith がデリバリーグループ 'Windows 11 VDAs' からデスクトップを要求しました	DDC-01	DDC
2026-07-20T09:14:22.3841Z	エラー	APPLICATION LAUNCH: 適切なデスクトップが見つかりませんでした — デリバリーグループ 'Windows 11 VDAs' 内のすべての VDA が未登録であるか、セッション容量に達しています	DDC-01	DDC
2026-07-20T09:14:22.4102Z	エラー	APPLICATION LAUNCH: ユー	STF-01	StoreFront

時刻 (UTC)	ログレベル	メッセージ	ホスト名	ホストの種類
		ザー DOMAIN\jsmith の起動に失敗しました — 利用可能なリソースがありません		

DDCからのエラーは、ブローカーが利用可能なVDAを見つけられなかったことを示しています。Web Studio → マシンの検索 でVDA登録を確認してください。VDA登録のトラブルシューティングについては、シナリオ2：VDA登録の失敗を参照してください。

例：VDAは割り当てられたが、セッションの初期化に失敗した

DDCはVDAを割り当てましたが、VDAはセッションを開始できませんでした。一般的な原因は次のとおりです。FSLogixまたはローミングプロファイルコンテナの障害、グループポリシー処理エラー、またはVDAリソースの枯渇です。

時刻 (UTC)	ログレベル	メッセージ	ホスト名	ホストの種類
2026-07-20T09:22:11.0234Z	情報	アプリケーション起動: ユーザー DOMAIN\jsmith の VDA WIN11MS-CC-VDA4 が選択されました	DDC-01	DDC
2026-07-20T09:22:11.8820Z	エラー	アプリケーション起動: ユーザー DOMAIN\jsmith のセッション初期化に失敗しました — FSLogix プロファイルコンテナを \fileserver\profiles\jsmith.vhdx	WIN11MS-CC-VDA4	WVDA

時刻 (UTC)	ログレベル	メッセージ	ホスト名	ホストの種類
		にマウントできませんでした		
2026-07-20T09:22:12.0011Z	エラー	アプリケーション起動: 起動要求に失敗しました — VDA WIN11MS-CC-VDA4 はユーザー DOMAIN\jsmith のセッション準備エラーを報告しました	DDC-01	DDC

ホストタイプ WVDA からのエラーは、VDA が障害点であることを示しており、メッセージには正確な原因が表示されています。その行の **>** 展開矢印をクリックして、完全なプロファイルコンテナパスとエラーコードを含む完全なメッセージを読み取ってください。

例: CWA起動中の仮想チャネルエラー

セッションはVDA側で作成されましたが、CWAクライアントはICA®仮想チャネル接続を確立できませんでした。クライアント側のエラーを確認するには、**ホスト名**をCWAマシンにフィルターしてください。

時刻 (UTC)	ログレベル	メッセージ	ホスト名	ホストの種類
2026-07-20T09:31:04.5521Z	情報	アプリケーション起動: シームレスホスト仮想ドライバーが正常に初期化されました	WIN11MS-CC-VDA4	WVDA
2026-07-20T09:31:05.1204Z	エラー	CWA-POSTLAUNCH::VIRTUAL CHANNEL: 仮想ドライバーのロードに失敗しました — チャ	ウィン22-CC-01	CWA (ウィンドウズ版)

時刻 (UTC)	ログレベル	メッセージ	ホスト名	ホストの種類
		ネルネゴシエーションがタイムアウトしました。ポート 1494および 2598のファイアウォールルールを確認してください。		

ホストタイプ CWAWindows で CWA-POSTLAUNCH エラーが発生した場合、VDA は準備ができていたものの、クライアントと VDA 間の ICA データパスがブロックされたことを意味します。クライアントマシンから VDA へのポート 1494 および 2598 が開いていることを確認してください。

シナリオ 2: VDA 登録の失敗

Director または Web Studio → で VDA が **未登録** と表示されます。ユーザーには「現在、利用可能なデスクトップはありません。」と表示されます。公開されたデスクトップは StoreFront™ または Citrix Workspace™ でグレー表示されます。

ノードで、**カテゴリ** を **VDA 登録** に、**ログレベル** を **エラー** に設定し、**ホスト名** を影響を受ける VDA と DDC の両方に設定します。**適用** をクリックします。登録ハンドシェイクの両側（同じタイムスタンプの VDA 行と DDC 行）を合わせて読むことで、障害がどこで発生したかを正確に示します。

> **参照のみ:**
>
> 以下のログメッセージは例示です。実際の環境でのメッセージは、同じ形式と列構造に従いますが、正確な表現は異なる場合があります。

例: VDA が Delivery Controller に到達できない

VDA は登録を試行していますが、DDC は要求を受信しません。VDA 側のエラーのみが表示され、同じタイムスタンプの DDC 行は表示されません。

時刻 (UTC)	ログレベル	メッセージ	ホスト名	ホストの種類
2026-07-20T08:30:11.2341Z	エラー	登録: ポート443でDelivery Controller DDC-01.domain.comに接続できませんでした — 接続がタイムアウトしました	WIN11MS-CC-VDA4	WVDA
2026-07-20T08:30:41.2341Z	エラー	登録: ポート443でDelivery Controller DDC-01.domain.comに接続できませんでした — 接続がタイムアウトしました	WIN11MS-CC-VDA4	WVDA
2026-07-20T08:31:11.2341Z	エラー	登録: ポート443でDelivery Controller DDC-01.domain.comに接続できませんでした — 接続がタイムアウトしました	WIN11MS-CC-VDA4	WVDA

同じエラーが一定の間隔で繰り返されるのは、再試行ループです。VDAは稼働していますが、ブロックされています。VDAからDDCへのポート80および443が開いていることを確認し、VDA上の`ListOfDDCs`レジストリキーで古いまたは誤ったDDCアドレスがないか確認してください。

例: DDCが登録要求を拒否する

VDAはDDCに到達しましたが、DDCは登録を拒否しました。VDAとDDCの両方の行が表示されます。拒否理由についてはDDCメッセージを読んでください。

時刻 (UTC)	ログレベル	メッセージ	ホスト名	ホストの種類
2026-07-20T08:30:11.2341Z	情報	REGISTRATION: VDA WIN11MS-CC-VDA4 が DDC-01.domain.com への登録を試行しています	WIN11MS-CC-VDA4	WVDA
2026-07-20T08:30:11.8820Z	エラー	REGISTRATION: 登録が拒否されました — マシンアカウント WIN11MS-CC-VDA4$ が無効になっているか、Active Directory に見つかりません	DDC-01	DDC

「エラー」行はホストタイプDDCから来ています。DDCが障害点であり、VDAではありません。DDC行の**>**展開矢印をクリックして、拒否理由の全文を読んでください。一般的な理由としては、Active Directoryでのマシンアカウントの無効化、VDA/DDCのバージョン不一致、またはライセンスプールの枯渇などがあります。

例：VDAが登録された後、すぐに登録解除される

登録は成功しますが、DDCが数秒以内に登録解除を開始します。これがループで繰り返されます。電源管理ドレインポリシーにより、VDAがセッションを受け入れる前にシャットダウンされています。

時間 (UTC)	ログレベル	メッセージ	ホスト名	ホストタイプ
2026-07-20T09:01:33.1240Z	情報	登録: VDA WIN11MS-CC-VDA4 は DDC-01.domain.com に正常に登録されました	WIN11MS-CC-VDA4	WVDA

時間 (UTC)	ログレベル	メッセージ	ホスト名	ホストタイプ
2026-07-20T09:01:47.4421Z	エラー	POWER MANAGEMENT: PowerManagementDrain が開始されました — デリバリーグループの電源ポリシーにより、マシンのシャットダウンがスケジュールされました	WIN11MS-CC-VDA4	WVDA
2026-07-20T09:01:47.6830Z	エラー	REGISTRATION: VDA WIN11MS-CC-VDA4 の登録が解除されました — 理由: 電源管理ドレイン	DDC-01	DDC

登録と登録解除の間の14秒のギャップが原因を示しています。Web Studio → デリバリーグループ → 電源管理で、営業時間中に適用されているドレインまたはシャットダウンのスケジュールを確認してください。

> **注:**
>
> この記事のシナリオは、Citrix DirectorまたはMonitorでログを検索および調査する方法の例です。同じ方法論は、セッション障害、認証エラー、接続の問題、VDAの不安定性、その他のコンポーネントレベルの問題など、遭遇するCitrix関連のあらゆる問題に適用されます。適切な**カテゴリ**、**ログレベル**、**ホスト名**フィルターを設定し、**時間 (UTC)** 順にログシーケンスを読み、個々の行を展開して完全な**メッセージ**を読みます。最初にエラーをログに記録したコンポーネントとメッセージの内容が、シナリオに関係なく根本原因を示します。

> **ヒント — Citrix Aidrienアクセス権を持つDaaSのお客様:** AOTログからエラーメッセージをコピーし、Citrix Aidrienに直接貼り付けます。Aidrienがエラーを説明し、推奨されるトラブルシューティング手順を提供します。これによりすべての問題が解決するわけではありませんが、根本原因を絞り込み、多くの場合、Citrixテクニカルサポートに連絡する前に解決策に導いてくれます。

Citrixテクニカルサポートへのエスカレーション

セルフサービスによる調査で問題が解決しない場合は、サポートチケットを開く際に以下を含めてください。

- **障害発生期間をカバーするエクスポートされたログファイル** — 上記オプション7で説明されているエクスポートアイコンを使用します。お持ちの状況に応じて、2つの方法でエクスポートできます。
  - **ターゲットを絞ったエクスポート** — 時間、カテゴリ、ホスト名フィルターを適用してからエクスポートします。これにより、サポートは障害に限定された集中的なログセットを得ることができます。
  - **広範囲なエクスポート** — 時間フィルターのみを適用し、他のフィルターなしでエクスポートします。これにより、サポートは障害発生期間の完全なログ情報を得ることができ、範囲が不明確な場合に役立ちます。

  ファイルがダウンロードされると、ファイル名には**AOT**というプレフィックスが付きます。このプレフィックスを削除したり、名前を変更したりしないでください。ファイル名の後続部分は編集できますが、常に先頭に**AOT**を保持してください。
- 上記のセクションで特定された障害パターン
- CVADバージョン、コンポーネントバージョン（VDA、DDC、StoreFront）、およびログサーバーバージョン
- 失敗したイベントのトランザクションIDまたはセッションID — プレースホルダー「*"Search logs by transaction ID, keyword, category, hostname"*」を使用してログノードの検索バーで検索可能

AOTはログを継続的にキャプチャし、すべてのエントリにホスト名、ホストタイプ、タイムスタンプが含まれているため、Citrixテクニカルサポートは、問題の再現や新しいトレースの収集を依頼することなく、すぐに分析を開始できます。

よくある質問

1. **MAX_RESERVE_DAYS のような、実行中のログサーバー構成を確認するにはどうすればよいですか？**

   以下のいずれかのコマンドを使用して、コンテナ環境の値を確認できます。

   `docker inspect logserver |findstr MAX_RESERVE_DAYS` または、コンテナ環境を確認する： `docker exec -it logserver env |grep MAX_RESERVE_DAYS`

   何も返されない場合、ログサーバーはデフォルト値を使用しています。
   MAX_RESERVE_DAYS=7

2. **Windows にログサーバーコンテナイメージをインストールする場合、Docker Desktop ライセンスを購入する必要がありますか？**

   はい。有効な Docker Desktop ライセンスが必要です。

3. **ログサーバーのインストールには新しいサーバーを使用すべきですか？**

   はい。パフォーマンスと分離を確保するため、ログサーバーのインストールには専用サーバーを使用することをお勧めします。

4. **単一の AOT ログサーバーの持続的な取り込み容量はどれくらいですか？最大および安全な 1 秒あたりのイベント数 (EPS) の制限は何ですか？**

   単一の AOT ログサーバーは、**1 秒あたり 10,000 イベント (EPS)** の持続的な取り込み容量をサポートします。この値は、継続的な取り込みにおける**最大値**と**安全な運用しきい値**の両方を表します。

5. **単一の AOT Log Server はいくつのコンポーネントを処理できますか？最大制限はありますか？**

   単一の Log Server は最大 128,000 のコンポーネントに接続できますが、1 秒あたり約 10,000 のログしか処理できません。そのため、マシンの数が問題になることはほとんどなく、実際のサイジング要因は、ピークアクティビティ中にユーザーが生成するログの数です。

6. **AOT ログサーバーのバースト耐性はどれくらいですか？損失やバックログの超過なしに、どれくらいの突然のログスパイクを処理できますか？**

   AOT Log Server は、ログを失うことなく、**通常のイベントレートの 2 倍**までの短期的なバーストを処理できます。ログの量がこれを超えて急増した場合（例えば 5 倍）、システムはイベントを確実に永続化できなくなり、**OpenSearch はログのインデックス作成が間に合わないため、ログを破棄し始めます。**

7. **AOTログサーバーはログを圧縮できますか？どのくらいの圧縮率を期待できますか？**

はい。AOTログサーバーは、OpenSearchにログを保存するためにデフォルトの**LZ4圧縮アルゴリズム**を使用します。一般的な圧縮率は約**2:1**で、ログデータは元のサイズの半分以下に削減され、高速な読み書きパフォーマンスを維持します。

8. **各インフラストラクチャタイプ（シングルサイトオンプレミス、マルチサイトオンプレミス、シングルリージョンクラウド、マルチリージョンクラウド、ハイブリッド、MSP/テナント）において、AOTログサーバーはどこにデプロイすべきですか？また、その理由は何ですか？**

   AOTログサーバーは、常に**VDAと同じ視線上に**デプロイする必要があります。これにより、安定した接続が確保され、ログを生成するコンポーネントとそれを取り込むログサーバー間の低遅延が維持されます。すべてのコンポーネント（VDA、DDC、StoreFront、Gatewayなど）がログサーバーに確実に到達できる限り、環境は正常に機能します。

9. **リージョンごとに1つのログサーバーが必要ですか、それともすべてを集中化できますか？遅延とエグレスについてはどうですか？**

   ログサーバーを集中化することは可能ですが、お客様は自身の環境における**遅延**と**エグレスコスト**の影響を評価する必要があります。**リージョン間の遅延はログの取り込みに影響を与える可能性があり**、特にトラフィック量の多い期間には顕著です。往復遅延が大きい場合、ログの急増やバーストにより、ピーク負荷時に遅延、バックログの蓄積、または潜在的な損失が発生する可能性があります。ログがリージョンまたはクラウドの境界を越える場合、エグレス料金が発生する場合があります。

10. **AOTは大量のネットワーク帯域幅やシステムリソースを消費しますか？**

    いいえ。AOTは、エンドポイント、VDA、その他のコンポーネント、およびネットワークパフォーマンスへの影響を最小限に抑えるように設計されています。

    AOTはログを継続的に収集し、HTTPS経由でほぼリアルタイムにAOTログサーバーにアップロードします。個々のログレコードは通常非常に小さく（多くの場合わずか数キロバイト）、これにより通常の運用中のネットワークオーバーヘッドを最小限に抑えることができます。

    消費される全体的な帯域幅は、アクティブなセッション数、有効なコンポーネント、および環境のアクティビティによって異なります。ほとんどの展開において、AOTログトラフィックはネットワーク全体の利用率のごく一部を占めるにすぎません。

    AOTは、ストレージ要件を削減し、ログサーバーへのデータ転送を最適化するために圧縮も使用します。

11. **AOTログサーバーで1,000台のマシンをサポートするための最小ハードウェア仕様は何ですか？**

1,000台までのマシンがある環境では、次のものが必要です。**1ノード**（ログサーバーとOpenSearchの組み合わせ）、**4 vCPU、8 GB RAM、2,000 IOPS**以上（SSDまたはNVMeを推奨）、**1 Gbps NIC**。このセットアップは、ログ量が中程度の小規模またはシングルサイト展開に適しています。

12. **ログサーバーに問題がある場合、どのようにトラブルシューティングできますか？**

    LogServerはDockerコンテナとして実行されているため、すべてのDockerコマンドを使用して問題を見つけることができます。

    ```
    docker logs logserver

    docker inspect logserver
    ```

    また、ユーザーは実行中のコンテナにアタッチして、ログサーバー自体のログを表示することもできます。

    ```
    docker exec –it logserver bash
    ```

    logserver docker コンテナのbashシェルで、ユーザーはlogserverとopensearchの健全性を確認できます。

    ```
    curl http://localhost:5000/Ping

    curl http://localhost:9200/_cluster/health?pretty
    ```

    そして、コンテナ内のログを確認します。

    ```
    tail Config/applogs.txt

    tail Config/weblogs.txt
    ```

    さらにログが必要な場合は、ユーザーはStartLogServer.sh/StartLogServer.batでLOG_LEVEL=0を変更し、これらのスクリプトファイルでlogserverを再起動できます。そうすると、詳細なログにはTRACE、DEBUG、INFO、WARN、ERRORのすべてのレベルが含まれるようになります。

13. **不適切にデタッチされたログサーバーのストレージディスクからの回復**

Citrix Connector Applianceの管理UIから最初にデタッチせずに、ログサーバーのストレージディスクを**ハイパーバイザー**または**クラウドプロバイダー**から直接削除またはデタッチした場合、Connector Applianceはストレージ構成を保持し、ディスクがまだアタッチされていると見なします。その結果、以前にアタッチされたディスクはConnector Applianceに構成されたままであり、新しいディスクのアタッチは失敗し、「**ローカルディスクはすでにプロバイダーにマウントされています**」のようなエラーが表示されることがあります。

オプション1（推奨）： 元のディスクがまだ利用可能な場合：

a. ハイパーバイザーまたはクラウドプロバイダーから、元のディスクをConnector Appliance VMに再接続します。
b. Connector Applianceを再起動します。
c. アプライアンスが正常に起動した後、Connector Applianceの管理UIを使用してディスクをデタッチします。
d. 必要に応じて、新しいディスクを接続できるようになります。

オプション2： 元のディスクが利用できなくなった場合は、以下のAPIリクエストを実行して、古いストレージ構成を手動で削除します。認証トークンを取得し、適切なコマンドを実行します。

リナックス:

```
curl -X POST "https://<connector-fqdn>/storage/$detach" \

-H "Content-Type: application/json" \

-H "Authorization: Bearer <token>" \

-d '{"targetProvider":"logserver-provider","storageType":"local"}'
```

ウィンドウズ:

```
curl -X POST "https://<connector-fqdn>/storage/$detach" ^

-H "Content-Type: application/json" ^

-H "Authorization: Bearer <token>" ^
```

```
-d "{\"targetProvider\":\"logserver-provider\",\"storageType\":
\"local\"}"
```

注:

古いストレージ構成が正常に削除された場合でも、APIがエラーを返すことがあります。ディスクのアタッチを再試行する前に、ストレージ構成を確認してください。

ベストプラクティスとして、ハイパーバイザーまたはクラウドプロバイダーからディスクを削除またはデタッチする前に、必ずLog Serverストレージディスクを Connector Appliance管理UIからデタッチしてください。これにより、Connector Applianceはストレージ構成をクリーンアップし、古いストレージ参照を防ぎます。

既知の問題と制限事項

- **環境ごとにサポートされるログサーバーは1つのみ**

  現在のアーキテクチャでは、環境ごとに単一のAOTログサーバーのみがサポートされており、Web StudioとDirector/Monitorの両方が単一のログサーバー構成でのみ動作するように設計されています。すべてのコンポーネントは同じログサーバーを指す必要があります。複数のログサーバーにわたるワークロードの構成や分散は、現在サポートされていません。この単一のログサーバーは、最大128,000のアクティブなコンポーネント接続を処理し、毎秒最大10,000のログイベントを処理できます。これはほとんどの展開で十分です。これらの制限は、コンポーネントの数ではなく、接続容量とログスループットに基づいているため、非常に大規模な環境でも、スループットのしきい値内に収まっている限り、1つのログサーバーで運用できます。

  ただし、ピーク時のログ量が非常に多いお客様は、水平スケーリングがないため、取り込みまたはインデックス作成の制限に達する可能性があります。複数のログサーバーのサポートとより広範なスケーリングオプションは、進化するアーキテクチャの一部として将来のリリースで導入される予定です。

- **XenServerでホストされているWindows VM**でAOTログサーバーを実行することは**サポートされていません**。 XenServerはネストされた仮想化をサポートしていないため、ゲストVM内でDockerを実行できません。その結果、この構成ではログサーバーコンテナを展開できません。
- **Windows上のDocker Desktopは、AOTログサーバーのためにアクティブなユーザーセッションを必要とします**

Docker Desktopを使用してWindows VMにAOTログサーバーを展開すると、コンテナはDocker Desktopを起動したユーザーセッションのコンテキスト内で実行されます。Docker Desktopはユーザーセッションベースのアプリケーションとして設計されており、Windows上でシステムレベルのサービスとして実行されません。その結果、ユーザーがログアウトするとDocker Desktopが停止し、AOTログサーバーコンテナも停止します。この動作のため、展開が特定のユーザーセッションに依存しているため、ユーザーがログアウトするとAOTログサーバーが停止します。他の管理者は実行中のコンテナにアクセスしたり管理したりできません。

回避策: Docker DesktopとAOTログサーバーコンテナが継続して実行されるように、ユーザーセッションをアクティブな状態または切断された状態に保ちます（ログアウトしないでください）。

推奨事項: 本番環境での展開には、次のいずれかを使用してください。

- Docker Engineを使用してLinux VMにAOTログサーバーをデプロイする
- サポートされている場合は、Citrix Connector Appliance (CCA) ベースの展開を使用する

これらのオプションにより、ログサーバーはユーザーセッションから独立して実行され、より信頼性の高い常時稼働の展開モデルが提供されます。

> **注:**
>
> このアプローチは、セッションタイムアウトや厳格なセキュリティポリシーがある環境では信頼できない場合があります。
>
> この動作は、Windows上のDocker Desktopの既知の制限であり、AOTログサーバーに固有のものではありません。

- **ライセンスサーバーログがDirector/Monitorで不正なホストタイプで表示される**

  Directorでライセンスサーバーから AOTログを表示すると、ホスト名は正しいにもかかわらず、**ホストタイプ**列に値が**DDC**ではなく**License Server**と誤って表示される場合があります。

  この問題は、Directorでのホストタイプの表示方法に限定されており、ログの収集や機能には影響しません。この問題は、最新のライセンスサーバーリリースで解決されており、**License Server version: 55000 or later**以降で修正されています。

- **MonitorでAOTログを表示するにはCitrix Cloud Connectorが必要です**

AOTログを表示するために**Citrix Monitor**を使用するお客様は、環境に少なくとも1つの**Citrix Cloud Connector**を展開している必要があります。この要件は、AOTログサーバーがホストされている場所（Linux VM、Windows VM、Citrix Connector Applianceなど）に関係なく適用されます。

Citrix Monitorは、構成されたログサーバーからログを取得し、UIに表示するために、**Cloud Connectorで実行されているMonitorサービス**に依存しています。

Windows Cloud Connectorがない場合、AOTログはMonitorで取得または表示できません。

- **Citrix DirectorでADC Gatewayログが正しく表示されない**

  症状: Citrix DirectorでCitrix ADC GatewayのAlways On Tracing (AOT) ログを表示すると、次の現象が見られる場合があります。

  - ログレベルが**Debug**または**Info**ではなく**Error**と表示される。
  - **メッセージ**列に生のログエントリ全体が表示される。
  - 表示されるタイムスタンプが元のイベントタイムスタンプと異なる。
  - 不正な形式のJSONログレコードのみが影響を受けます。有効なログレコードは正しく表示されます。

  影響を受けるバージョン: 14.1-73.xより前のCitrix ADCおよび**15.1-8.x**より前のCitrix ADC。

  原因: Citrix ADC Gatewayが、AOTログサーバーで解析できない不正な形式のJSONログレコードをアップロードします。その結果、ログサーバーは生のログエントリを保存し、エラーとして分類します。

  解決策: Citrix ADCを次のいずれかのバージョン以降にアップグレードしてください。

  - 14.1-73.x
  - 15.1-8.x

  修正済み: Citrix ADC **14.1-73.x** および Citrix ADC **15.1-8.x**。

  - AOTログサーバーは現在、**FIPS準拠の展開**をサポートしていません。FIPS要件が義務付けられているお客様は、FIPSサポートが利用可能になるまで本番環境への展開を延期する必要があります。

    FIPS準拠を必要としないお客様は、サポートされている環境でAOTログサーバーの展開と評価を継続できます。

第三者通知

このCitrix Virtual Apps and Desktops™のリリースには、以下のドキュメントに定義されている条件に基づいてライセンス供与されたサードパーティ製ソフトウェアが含まれる場合があります。

- Citrix Virtual Apps and Desktops 第三者通知 (PDFダウンロード)
- Citrix Assistant App 第三者通知 - プレビュー (PDFダウンロード)
- FlexNet Publisher 2017 (11.15.0.0) の非商用ソフトウェア開示(/ja-jp/citrix-virtual-apps-desktops/2511/downloads/fnp-licensing-11-15-0-ncsd-summary.pdf) (PDFダウンロード)
- FlexNet Publisher 11.15.0 で使用されている FlexNet Publisher ドキュメント補足 第三者およびオープンソースソフトウェア (PDFダウンロード)

SDKおよびAPI

このリリースでは、いくつかのSDKとAPIが利用可能です。SDKとAPIにアクセスするには、Build anything with Citrixにアクセスしてください。そこから、**Citrix Workspace**を選択して、Citrix Virtual Apps and Desktopsおよび関連コンポーネントのプログラミング情報にアクセスします。

> **注:**
>
> Citrix Virtual Apps and Desktops™ SDKとCitrix Group Policy SDKは、モジュールまたはスナップインとしてインストールできます。いくつかのコンポーネントSDK（Citrix Licensing、Citrix Provisioning、StoreFrontなど）は、スナップインのみを使用してインストールされます。

> この製品は、PowerShellバージョン3から5をサポートしています。

Citrix Virtual Apps™およびデスクトップのエスディーケー

このSDKは、Delivery Controller™またはStudioをインストールすると、PowerShellモジュールとして自動的にインストールされます。これにより、スナップインを追加することなく、このSDKのコマンドレットを使用できます。（このSDKをスナップインとしてインストールすることを選択した場合、手順は以下に記載されています。）

権限

Citrix管理権限を持つIDを使用して、シェルまたはスクリプトを実行する必要があります。Controller上のローカル管理者グループのメンバーは、Citrix Virtual AppsまたはCitrix Virtual Desktops™をインストールするための完全な管理権限を自動的に持ちますが、Citrixは、通常の運用では、ローカル管理者アカウントを使用するのではなく、適切な権限を持つCitrix管理者を作成することを推奨します。

コマンドレットにアクセスして実行する

1. PowerShellでシェルを起動します。Studioを開き、**PowerShell**タブを選択し、**Launch PowerShell**をクリックします。

2. スクリプト内でSDKコマンドレットを使用するには、PowerShellで実行ポリシーを設定します。PowerShellの実行ポリシーの詳細については、Microsoftのドキュメントを参照してください。
3. モジュールではなくスナップインを使用したい場合は、`Add-PSSnapin`（または`asnp`）コマンドレットを使用してスナップインを追加します。

   V1とV2はスナップインのバージョンを示します。XenDesktop 5のスナップインはバージョン1です。Citrix Virtual Apps and Desktops、およびそれ以前のXenDesktop 7バージョンのスナップインはバージョン2です。たとえば、Citrix Virtual Apps and Desktopsスナップインをインストールするには、`Add-PSSnapin Citrix.ADIdentity.Admin.V2`と入力します。すべてのコマンドレットをインポートするには、次のように入力します: `Add-PSSnapin Citrix.*.Admin.V*`

これで、コマンドレットとヘルプファイルを使用できます。

- このSDKのヘルプファイルにアクセスするには、Categoriesリストで製品またはコンポーネントを選択し、次に**Citrix Virtual Apps and Desktops SDK**を選択します。
- PowerShellのガイダンスについては、Windows PowerShell Integrated Scripting Environment (ISE)を参照してください。

グループポリシーSDK

Citrix Group Policy SDKを使用すると、グループポリシーの設定とフィルターを表示および構成できます。このSDKは、PowerShellプロバイダーを使用して、マシンおよびユーザーの設定とフィルターに対応する仮想ドライブを作成します。このプロバイダーは、`New-PSDrive`の拡張機能として表示されます。

Group Policy SDKを使用するには、StudioまたはCitrix Virtual Apps and Desktops SDKのいずれかがインストールされている必要があります。

Citrix Group Policy PowerShellプロバイダーは、モジュールまたはスナップインとして利用できます。

- モジュールを使用する場合、追加の作業は不要です。
- スナップインを追加するには、`Add-PSSnapin citrix.common.grouppolicy`と入力します。

ヘルプにアクセスするには、`help New-PSDrive -path localgpo:/`と入力します。

仮想ドライブを作成し、設定をロードするには、`New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>`と入力します。ここで、Controller文字列は、接続して設定をロードするサイト内のControllerの完全修飾ドメイン名です。

シトリックス バーチャル アプリケーションズ アンド デスクトップ REST API

Citrix Virtual Apps and Desktops REST APIを使用すると、Citrix Virtual Apps and Desktops展開内のリソースの管理を自動化できます。

Citrix Virtual Apps and Desktops REST APIは`<https://developer.cloud.com/citrixworkspace/citrix-daas-rest-apis/docs/citrix-virtual-apps-and-desktops-apis>`で利用できます。Citrix Virtual Apps and Desktopsに適用されないAPIは、そのようにマークされています。そこにあるガイダンスに従って、APIサービスへのアクセスを構成し、APIを使用してリソースを管理および最適化してください。

モニターサービスOData

Monitor APIは、OData APIのバージョン3または4を使用してMonitor Serviceデータへのアクセスを許可します。Monitor Serviceデータからクエリされたデータに基づいて、カスタマイズされた監視およびレポートダッシュボードを作成できます。OData V.4はASP.NET Web APIに基づいており、集計クエリをサポートしています。

詳細については、Monitor Service OData APIを参照してください。

__index__

Citrix Always On トレース

Always On Tracing (AOT) は、Citrix Virtual Apps and Desktops (CVAD) 環境全体で関連するログデータを継続的にキャプチャするように設計された、Citrixが提供する最新の診断フレームワークです。AOTは、Citrix Diagnostic Facility (CDF) トレースのサブセットであり、他のコンポーネントからの追加ログも含まれており、一般的な障害（VDA登録やアプリケーション/デスクトップの起動など）のトラブルシューティングに役立ちます。

手動での介入が必要な従来のツールとは異なり、AOT はデフォルトでバックグラウンドで実行され、問題が再現できない場合でも、問題発生時に重要な情報が利用可能であることを保証します。

AOTは、IT管理者とCitrixサポートチームのトラブルシューティングを簡素化し、平均解決時間（MTTR）を改善するために、以下のことを行います。

- ユーザーセッションとシステムイベントのログデータを自動的にキャプチャする。
- 問題の再現の必要性を排除する。
- エンジニアリングレベルの専門知識なしに、ログを簡単にアクセス可能で読みやすくする。
- Citrixサポートへの依存を減らすために、セルフサービスログデータを有効にする。

主な利点

- MTTR（平均解決時間）の高速化
- 常時稼働、手動でのトレース開始は不要
- 一般的な問題の自己診断
- 完全なコンテキスト付きでCitrixサポートへのエスカレーションを合理化
- 機密データの編集機能を備えた、安全で準拠したログ処理

サイト全体の履歴トレンドを監視する

トレンドビューでは、各サイトの履歴トレンド情報に次のパラメーターでアクセスできます。

- セッション

- 接続障害
- マシンの障害
- ログオンパフォーマンス
- 負荷評価
- キャパシティ管理
- マシン使用状況
- リソース使用率
- 各サイトのネットワーク分析。

この情報を見つけるには、**トレンド**メニューをクリックします。

ズームインしてドリルダウンする機能を使用すると、期間を拡大（グラフのデータポイントをクリック）し、トレンドに関連付けられた詳細を表示するためにドリルダウンすることで、トレンドグラフをナビゲートできます。この機能により、誰が、または何が影響を受けているかの詳細をよりよく理解できます。

各グラフのデフォルトのスコープを変更するには、データに別のフィルターを適用します。

履歴トレンド情報が必要な期間を選択します。期間の可用性は、Directorの展開によって次のように異なります。

- Premiumライセンスサイトでは、最大「昨年」（365日間）までのトレンドレポートが利用できます。
- Advancedライセンスサイトでは、最大「先月」（31日間）までのトレンドレポートが利用できます。
- PremiumおよびAdvanced以外のライセンスサイトでは、最大「過去7日間」までのトレンドレポートが利用できます。

> **注:**
>
> - すべてのDirector展開において、期間が「先月」（**現在まで**）またはそれより短い期間に設定されている場合、セッション、障害、ログオンパフォーマンスのトレンド情報はグラフおよびテーブルとして利用できます。カスタム終了日を指定した「先月」または「昨年」として選択された期間の場合、トレンド情報はグラフとしてのみ利用でき、テーブルとしては利用できません。

- Monitor Serviceのグルーミング保持値によって、トレンドデータの可用性が制御されます。デフォルト値については、データ粒度と保持を参照してください。Premiumライセンスサイトのお客様は、グルーミング保持を希望する保持日数に変更できます。
- IISマネージャーの以下のパラメーターは、選択可能なカスタム終了日の範囲を制御します。ただし、選択された日付のデータ可用性は、測定対象の特定のメトリックに対するグルーミング保持設定によって異なります。

パラメーター	デフォルト値
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

利用可能なトレンド

セッションのトレンドを表示: セッションタブから、デリバリーグループと期間を選択して、同時セッション数に関する詳細情報を表示します。

セッションの自動再接続列には、セッション内の自動再接続の数が表示されます。自動再接続は、セッションの信頼性ポリシーまたはクライアントの自動再接続ポリシーが有効な場合に有効になります。エンドポイントでネットワークが中断されると、次のポリシーが有効になります。

- セッションの信頼性が有効になり（デフォルトで3分間）、Citrix Receiver™またはCitrix Workspace™アプリがVDAへの接続を試行します。
- クライアントの自動再接続が3分から5分の間に有効になり、クライアントがVDAへの接続を試行します。

両方の再接続がキャプチャされ、ユーザーに表示されます。この情報は、再接続が発生してからDirector UIに表示されるまでに最大5分かかる場合があります。

自動再接続情報は、中断のあるネットワーク接続の表示とトラブルシューティングに役立ちます。また、シームレスなエクスペリエンスを持つネットワークも分析します。フィルターで選択した特定のデリバリーグループまたは期間の再接続数を表示できます。ドリルダウンでは、セッ

ションの信頼性やクライアントの自動再接続、タイムスタンプ、エンドポイントIP、Workspaceアプリがインストールされているマシンのエンドポイント名などの追加情報が提供されます。

デフォルトでは、ログはイベントのタイムスタンプの降順でソートされます。この機能は、Windows用Citrix Workspaceアプリ、Mac用Citrix Workspaceアプリ、Windows用Citrix Receiver、およびMac用Citrix Receiverで利用できます。この機能には、Delivery Controller™バージョン7 1906以降、およびVDA 1906以降が必要です。

セッションの再接続の詳細については、「セッション」を参照してください。

ポリシーの詳細については、クライアントの自動再接続ポリシー設定およびセッションの信頼性ポリシー設定を参照してください。

自動再接続データがDirectorに表示されない場合があります。その理由は次のとおりです。

- Workspaceアプリが自動再接続データをVDAに送信していません。
- VDAがモニターサービスにデータを送信していません。
- デリバリーコントローラーは、対応するセッションがない可能性があるため、VDAペイロードを破棄します。

> **注:**
>
> 場合によっては、特定のCitrix Gatewayポリシーが設定されていると、クライアントIPアドレスが正しく取得されないことがあります。

> **接続障害の傾向を表示:** タブから、接続、マシンタイプ、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のユーザー接続障害に関する詳細情報を含むグラフを表示します。

マシン障害の傾向を表示: シングルセッションOSマシン障害タブまたはマルチセッションOSマシンタブから、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のマシン障害に関する詳細情報を含むグラフを表示します。

ログオンと再接続のパフォーマンスの傾向を表示: タブから、デリバリーグループと期間を選択して、サイト全体のユーザーログオンおよび再接続の期間に関する詳細情報を含むグラフを表示します。このビューは、ログオンまたは再接続の数と全体的なパフォーマンスを把握するのに役立ちます。

グラフには以下が含まれます。

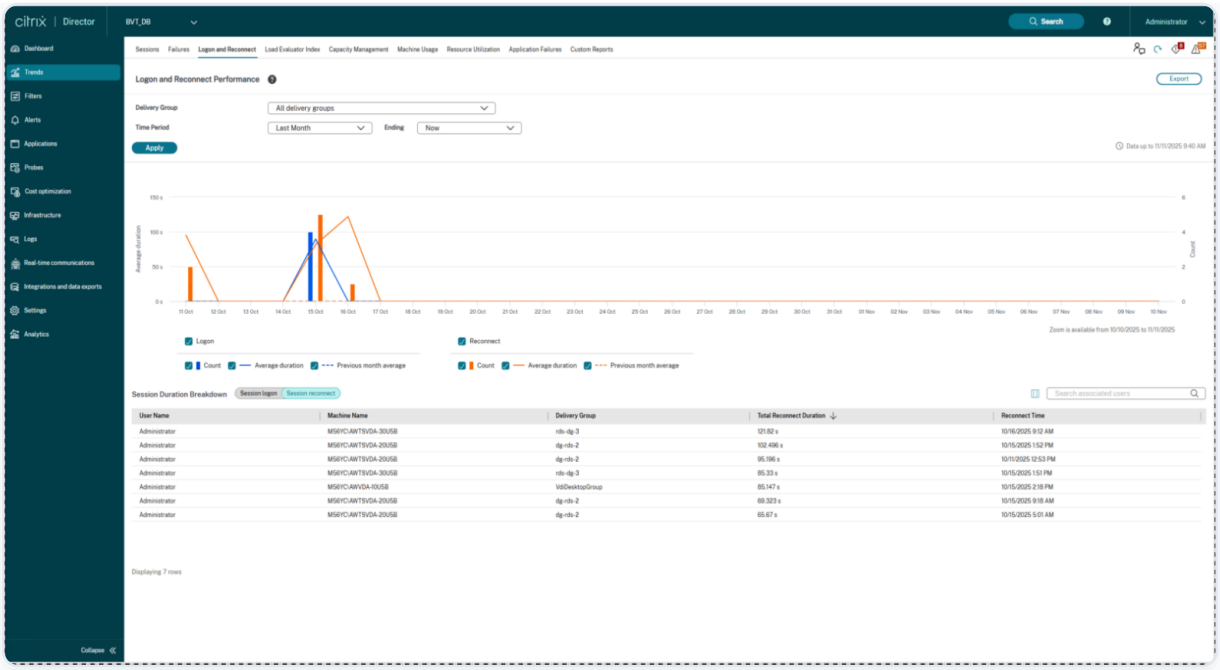
- **ログオンイベント、ログオン期間、およびフェーズ**(ブローカリング、対話型セッションなど)は、新しいセッションを起動する際のユーザーエクスペリエンスに関する洞察を提供します。
- **再接続イベントと再接続期間**。切断されたセッションから再接続する際のユーザーエクスペリエンスに関する洞察を提供します。

凡例を使用して、分析されている傾向に基づいて必要なメトリックを選択します。

- カウント
- 平均期間
- 以前の（期間）平均

グラフの下のテーブルには、ユーザーセッションまたは接続ごとの**セッションログオン**と**セッション再接続**の詳細が表示されます。テーブルの上の選択肢を使用してメトリックを切り替えたり、表示する列を選択したり、任意の列で並べ替えたり、レポートをPDF、Excel、またはCSV形式でエクスポートしたりできます。

> **注:**
>
> セッション再接続時間は、**DirectorおよびVDAバージョン2511 CR以降**でサポートされています。



負荷評価の傾向を表示: 負荷評価インデックスタブから、マルチセッションOSマシン間に分散されている負荷に関する詳細情報を含むグラフを表示します。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のマルチセッションOSマシン、マルチ

セッションOSマシン（デリバリーグループ内のマルチセッションOSマシンが選択されている場合にのみ利用可能）、および範囲が含まれます。

ホストされているアプリケーションの使用状況を表示: この機能の利用可否は、組織のライセンスによって異なります。 **キャパシティ管理**タブから、**ホストされているアプリケーションの使用状況**タブを選択します。デリバリーグループと期間を選択して、ピーク時の同時使用状況を示すグラフと、アプリケーションベースの使用状況を示すテーブルを表示します。アプリケーションベースの使用状況テーブルから、特定のアプリケーションを選択して詳細を表示したり、そのアプリケーションを使用している、または使用したユーザーのリストを表示したりできます。

Single-sessionおよびMulti-session OSの使用状況を表示: トレンドビューには、サイト別およびデリバリーグループ別のSingle-session OSの使用状況が表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、ユーザーごとの使用状況が表示されます。 トレンドビューには、サイト別、デリバリーグループ別、およびマシン別のMulti-session OSの使用状況も表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、マシンごとおよびユーザーごとの使用状況が表示されます。マシンが選択されている場合は、ユーザーごとの使用状況が表示されます。

仮想マシンの使用状況を表示: マシン使用状況タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択すると、VM使用状況のリアルタイムビューが表示され、サイトのキャパシティニーズを迅速に評価できます。 シングルセッションOSの可用性 - サイト全体または特定のデリバリーグループの可用性別に、シングルセッションOSマシン（VDI）の現在の状態を表示します。 マルチセッションOSの可用性 - サイト全体または特定のデリバリーグループの可用性別に、マルチセッションOSマシンの現在の状態を表示します。

表示されるバナーの以下のリンクをクリックすると、**コスト最適化**によるマシン使用状況の可視性を高めることができます。

- 推定節約額 - このリンクをクリックすると、**コスト最適化**ページの**推定節約額**セクションに移動し、すべてのデリバリーグループの詳細が表示されます。
- 節約レポート - このリンクをクリックすると、**コスト最適化**ページの**節約レポート**セクションに移動し、すべてのデリバリーグループの詳細が表示されます。

> **注:**
>
> 利用可能カウンターに表示されるマシンの数には、メンテナンスモードのマシンが含まれます。

リソース使用率を表示: リソース使用率タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択すると、各VDIマシンのCPUおよびメモリ使用量、IOPS、ディスク遅延に関する履歴傾向データが把握でき、より適切なキャパシティプランニングが可能になります。 この機能には、Delivery ControllerおよびVDAの**バージョン7.11**以降が必要です。 グラフには、平均CPU、平均メモリ、平均IOPS、ディスク遅延、およびピーク時の同時セッションのデータが表示されます。マシンにドリルダウンして、CPUを消費している上位10個のプロセスのデータとグラフを表示できます。

デリバリーグループと期間でフィルターします。CPU、メモリ使用量、およびピーク時の同時セッションのグラフは、過去2時間、24時間、7日間、1か月、1年間で利用できます。平均IOPSとディスク遅延のグラフは、過去24時間、1か月、1年間で利用できます。バナーの**チェックアウト**リンクをクリックすると、コスト最適化によるマシン使用状況の可視性を高めることができます。このリンクをクリックすると、**コスト最適化**ページの**ワークロードの適正化**タブに移動し、**リソース使用率**タブから選択されたデリバリーグループの詳細が表示されます。

注:

- 履歴マシン使用率ページの「上位10プロセス」テーブルでデータを収集して表示するには、監視ポリシー設定の**プロセス監視を有効にする**を**許可**に設定する必要があります。このポリシーは、デフォルトで**禁止**に設定されています。すべてのリソース使用率データはデフォルトで収集されます。これは、**リソース監視を有効にする**ポリシー設定を使用して無効にできます。グラフの下のテーブルには、マシンごとのリソース使用率データが表示されます。詳細については、「監視ポリシー設定」を参照してください。
- 平均IOPSは日次平均を表示します。ピークIOPSは、選択した時間範囲におけるIOPS平均の最高値として計算されます。(IOPS平均とは、VDAで1時間内に収集されたIOPSの時間平均です)。
- マシンのドリルダウンは、平均CPU使用率または平均メモリ使用率が1%を超えるプロセスを一覧表示します。これは、場合によっては10未満のプロセスしか表示されない可能性があることを意味します。

ネットワーク分析データの表示: この機能の可用性は、組織のライセンスと管理者権限によって異なります。この機能には、Delivery Controllerの**バージョン7.11**以降が必要です。

ネットワークタブから、ネットワーク分析を監視します。これにより、ネットワークのユーザー、アプリケーション、デスクトップのコンテキストビューが提供されます。この機能により、

DirectorはCitrix ADMからのHDX Insightレポートを通じて、展開におけるICAトラフィックの高度な分析を提供します。詳細については、「ネットワーク分析の構成」を参照してください。

アプリケーション障害の表示: アプリケーション障害タブは、VDA上の公開アプリケーションに関連する障害を表示します。

この機能には、Delivery ControllerおよびVDA **バージョン7.15**以降が必要です。Windows Vista以降を実行するシングルセッションOS VDA、およびWindows Server 2008以降を実行するマルチセッションOS VDAがサポートされています。 詳しくは、「履歴アプリケーション障害監視」を参照してください。

デフォルトでは、マルチセッションOS VDAからのアプリケーション障害のみが表示されます。監視ポリシーを使用して、アプリケーション障害の監視を設定できます。詳細については、「監視ポリシー設定」を参照してください。

プローブ結果の表示: プローブ結果タブは、構成ページでプローブ用に構成されたアプリケーションおよびデスクトップのプローブ結果を表示します。ここには、障害が発生した起動の段階が記録されます。

詳しくは、「アプリケーションおよびデスクトップのプローブ」を参照してください。

カスタマイズされたレポートの作成: カスタムレポートタブは、監視データベースからのリアルタイムデータと履歴データを含むカスタムレポートを表形式で生成するためのユーザーインターフェイスを提供します。

この機能には、Delivery Controllers **バージョン7.12**以降が必要です。

以前に保存したカスタムレポートクエリのリストから、**実行してダウンロード**をクリックしてレポートをCSV形式でエクスポートしたり、**ODataをコピー**をクリックして対応するODataクエリをコピーして共有したり、**編集**をクリックしてクエリを編集したりできます。 マシン、接続、セッション、またはアプリケーションインスタンスに基づいてカスタムレポートクエリを作成できます。マシン、デリバリーグループ、期間などのフィールドに基づいてフィルター条件を指定します。カスタムレポートに必要な追加の列を指定します。プレビューには、レポートデータのサンプルが表示されます。カスタムレポートクエリを保存すると、保存されたクエリのリストに追加されます。

コピーしたODataクエリに基づいてカスタムレポートクエリを作成できます。これを行うには、ODataクエリオプションを選択し、コピーしたODataクエリを貼り付けます。結果のクエリは後で実行するために保存できます。

> **注:**

ODataクエリを使用して生成されたプレビューおよびエクスポートレポートの列名はローカライズされておらず、英語で表示されます。

グラフ上のフラグアイコンは、特定の期間における重要なイベントまたはアクションを示します。フラグにマウスを合わせ、クリックしてイベントまたはアクションを一覧表示します。

注:

- HDX™接続ログオンデータは、7より前のVDAでは収集されません。それより前のVDAの場合、グラフデータは0と表示されます。
- Citrix Studioで削除されたデリバリーグループは、関連データが整理されるまで、Director Trendsフィルターで選択可能です。削除されたデリバリーグループを選択すると、保持期間までの利用可能なデータのグラフが表示されます。ただし、テーブルにはデータは表示されません。
- アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、新しいデリバリーグループの**リソース使用率と負荷評価インデックス**テーブルに、古いデリバリーグループと新しいデリバリーグループから統合されたメトリックが表示されます。

Citrix Infrastructure Monitor の自動接続

新しい自動接続機能は、以下の手順を自動的に実行することで、オンボーディングプロセスを簡素化します。

- Citrix Infrastructure Monitor のダウンロードとインストール
- 接続の検証

自動接続では、コンポーネントの詳細を手動で追加するだけで済みます。手動接続プロセスは変更されておらず、ユーザーはエージェントをダウンロードし、ターゲットマシンにインストールし、必要な詳細情報を提供する必要があります。

この変更に対応するため、UI には以下の2つのタブが追加されました。

- 自動接続

- 手動接続

自動接続プロセスには、資格情報を入力する前にすべての前提条件が満たされていることを確認するためのチェックボックスが含まれています。

自動接続の目的は、ユーザーにとってオンボーディングプロセスを可能な限りシームレスにすることです。

前提条件

Director UI からマシンに Citrix Infrastructure Monitor サービスをリモートでインストールできます。Director UI からのリモートインストールには、Provisioning Service および StoreFront™ マシンに対して以下が必要です。

- Citrix Infrastructure Monitor がインストールされるターゲットマシンで、ローカル管理者権限が必要です。
- ターゲットマシンで WMI が利用可能である必要があります。ファイアウォールで WMI が許可されていることを確認してください。詳細については、「リモート WMI 接続のセットアップ」を参照してください。
- ターゲットマシンで RPC が利用可能である必要があります。管理共有 (Admin$ および C$) は Delivery Controller™ マシンからアクセス可能である必要があります。
- ターゲットマシンは解決可能なDNSホスト名を持っている必要があります。

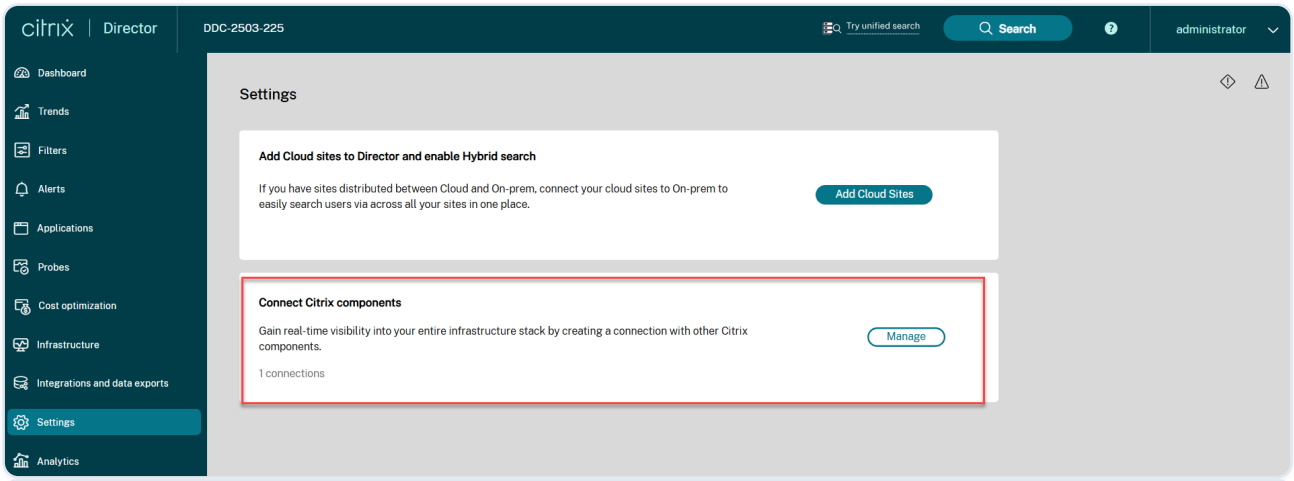
これらの要件が環境で満たせない場合は、「Citrix Infrastructure Monitorの手動オンボーディング」を参照してください。

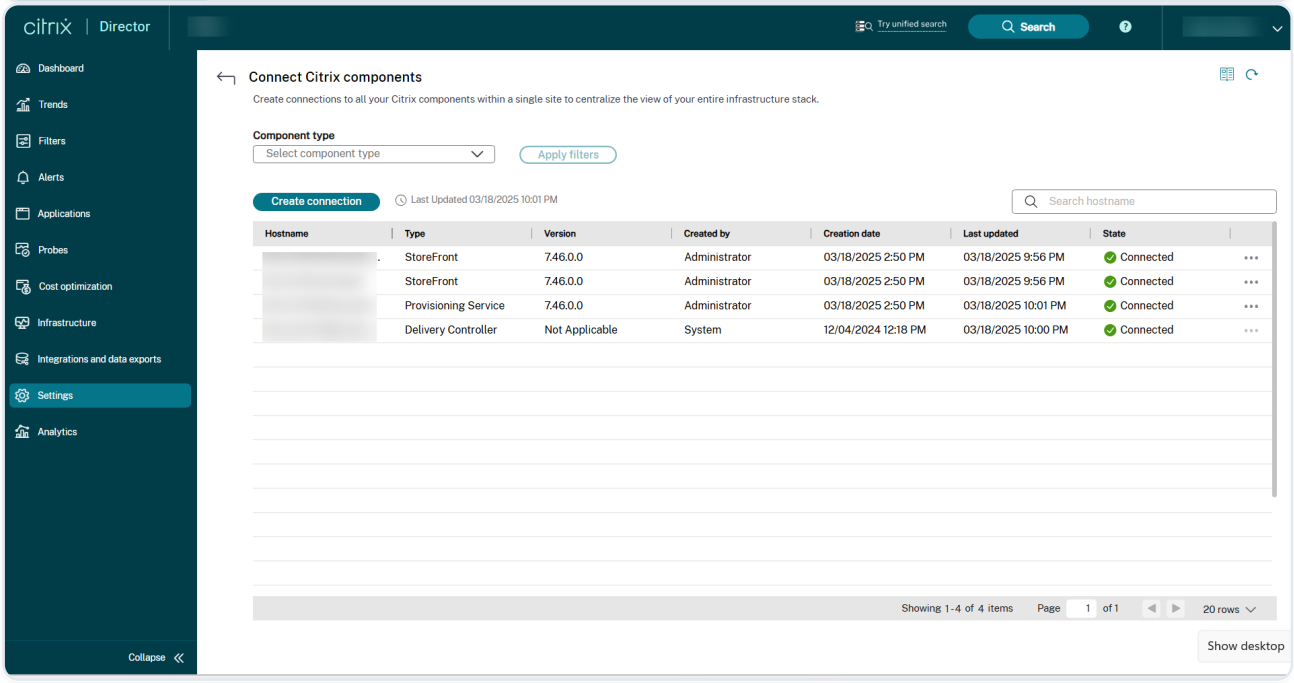
Citrix Infrastructure Monitor を自動的に登録する

Director UIを使用してCitrix Infrastructure Monitorを登録できます。以下の手順でDirector UIでの登録を完了してください。

ステップ1: Citrixコンポーネントの接続ページに移動する

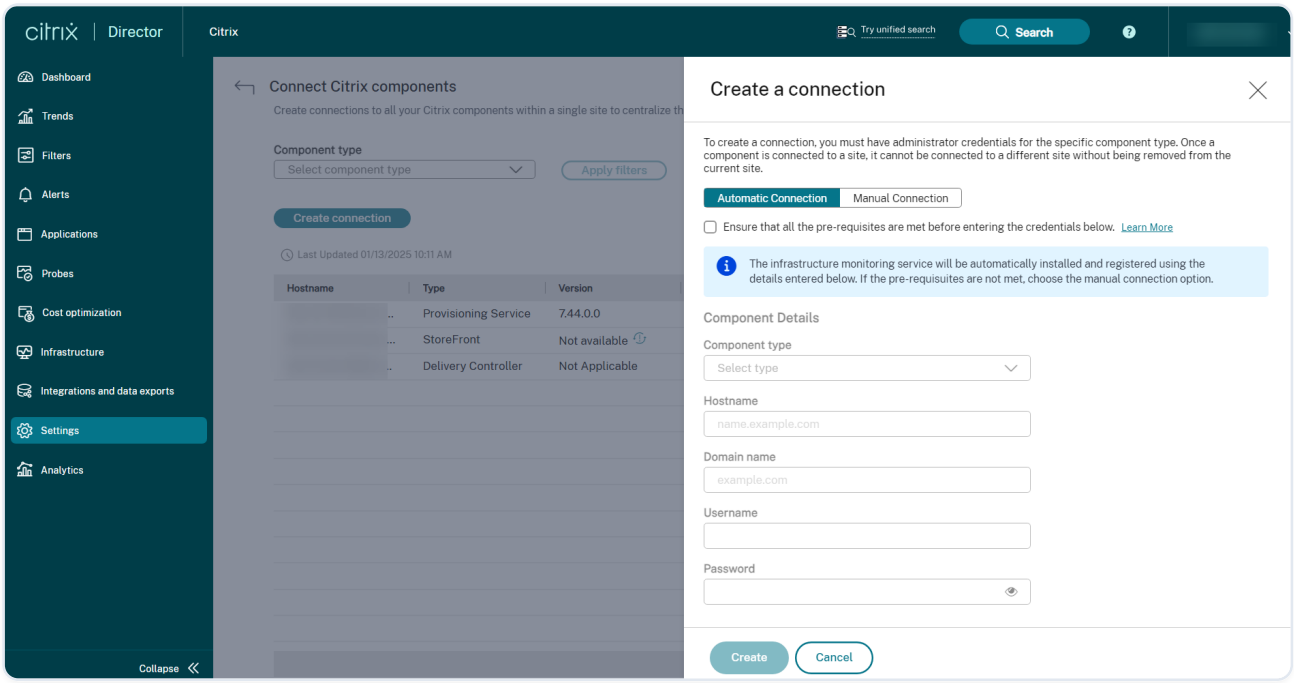
［設定］ > ［Citrix コンポーネントの接続］ > ［管理］ の順にクリックします。





ステップ2: コンポーネントの詳細を入力する

Citrixコンポーネントの接続画面で、**接続の作成** をクリックします。**接続の作成** ウィンドウが表示されます。**自動接続** タブがデフォルトで強調表示されています。



安全な接続を確立するために必要なコンポーネントの詳細を入力します。

- ドロップダウンリストからコンポーネントの種類を選択します。コンポーネントはProvisioning ServiceまたはStoreFrontのいずれかです。
- ホスト名を入力します。
- ドメイン名を入力します。
- Provisioning ServiceまたはStoreFrontマシンのユーザー名を入力します。
- Provisioning ServiceまたはStoreFrontマシンのパスワードを入力します。

インフラストラクチャ監視サービスは、上記詳細を使用して自動的にインストールおよび登録されます。

ステップ3：接続を作成する

詳細が入力されたら、**作成**をクリックします。リクエストが承認される前に、特定の事前チェックが実行されます。これらのチェックは、続行する前に前提条件が満たされていることを検証します。前提条件が満たされると、自動接続プロセスは、コピー、インストール、登録の各ステップを示す進行状況バーを表示します。いずれかのステップが失敗した場合、ユーザーには再試行オプションが表示されます。

自動接続プロセスの詳細を表示するには、**詳細の表示**をクリックします。

接続の進行状況(/en-us/citrix-virtual-apps-desktops/2511/media/connection-in-progress.png)

MSIファイルがダウンロードされ、インストール場所にコピーされ、そこでインストールおよび登録されます。完了すると、作成された接続は、「Citrixコンポーネントの接続」ページの接続リストで利用可能になります。

接続が失敗した場合は、接続を再試行できます。再試行するには、管理者資格情報を提供する必要があります。

自動オンボーディング(/en-us/citrix-virtual-apps-desktops/2511/media/auto-onboarding-connect.png)

エラー処理

システムは前提条件の事前チェックを実行し、いずれかのチェックが失敗した場合はエラーメッセージを表示します。

> **注：**
>
> 事前チェックは特定の順序で実行されます。たとえば、WMIエラーをチェックするには、資格情報が正しい必要があります。

次の表に、エラーメッセージと対応する解決策を示します。

エラーシナリオ	説明
無効な FQDN 形式	FQDN形式が無効です。この問題を解決するには、FQDN形式を修正してください。
到達不能なFQDN	FQDNマシンに到達できません。
無効な資格情報	ユーザー名またはパスワードが無効です。
リモートマシンでHTTPSが設定されていません。	Monitor構成でHTTPSが有効になっているにもかかわらず、リモートマシンでHTTPSを有効にするための環境変数が設定されていません。この問題を解決するには、**System Properties** > **Advanced** > **Environment Variables** > **Edit system variable**で値を設定してください。

エラーシナリオ	説明
リモートマシンでHTTPSが誤って設定されています	Monitor構成でHTTPSが無効になっているにもかかわらず、リモートマシンでHTTPSを有効にするための環境変数が設定されています。この問題を解決するには、**System Properties** > **Advanced** > **Environment Variables** > **Edit system variable**で値を削除してください。
リモートマシンでWindows Management Instrumentation (WMI)がブロックされています。	WindowsファイアウォールディフェンダーのWMIの**Allowed apps and features**セクションのチェックボックスが選択されていません。この問題を解決するには、WMIがファイアウォールを介してアクセスできることを確認してください。
リモートマシンでSMBポートがブロックされています。	ポート445は、Delivery Controllerからのインバウンド TCP接続に対して有効にする必要があります。
リモートマシンで管理者共有が無効になっています	自動接続の前提条件が満たされていません。

アップグレードプロセス

Citrix Infrastructure Monitorの以前のバージョンを使用している場合、アップグレードするオプションがあります。これはProvisioning ServiceとStoreFrontにのみ適用されます。自動アップグレードでは進行状況バーが表示され、管理者資格情報が必要です。

アップグレードプロセス(/en-us/citrix-virtual-apps-desktops/2511/media/upgrade-auto.png)

自動または手動でアップグレードを選択できます。

アップグレードプロンプトは、新しいバージョンが利用可能な場合にのみ表示されます。アップグレードに登録は不要です。アップグレード後、最新バージョンが反映されるまでに約5分かかります。

Citrix Infrastructure MonitorのHTTPSを構成する手順

> **注:**

> Citrix Infrastructure MonitorサービスはHTTPモードでも動作するため、この場合、以下の設定は不要です。ただし、HTTPSモードでの使用を推奨します。Citrix Infrastructure MonitorでHTTPSを設定する必要がある場合にのみ、以下の手順を実行してください。

ステップ1：証明書をマシンにアップロードする

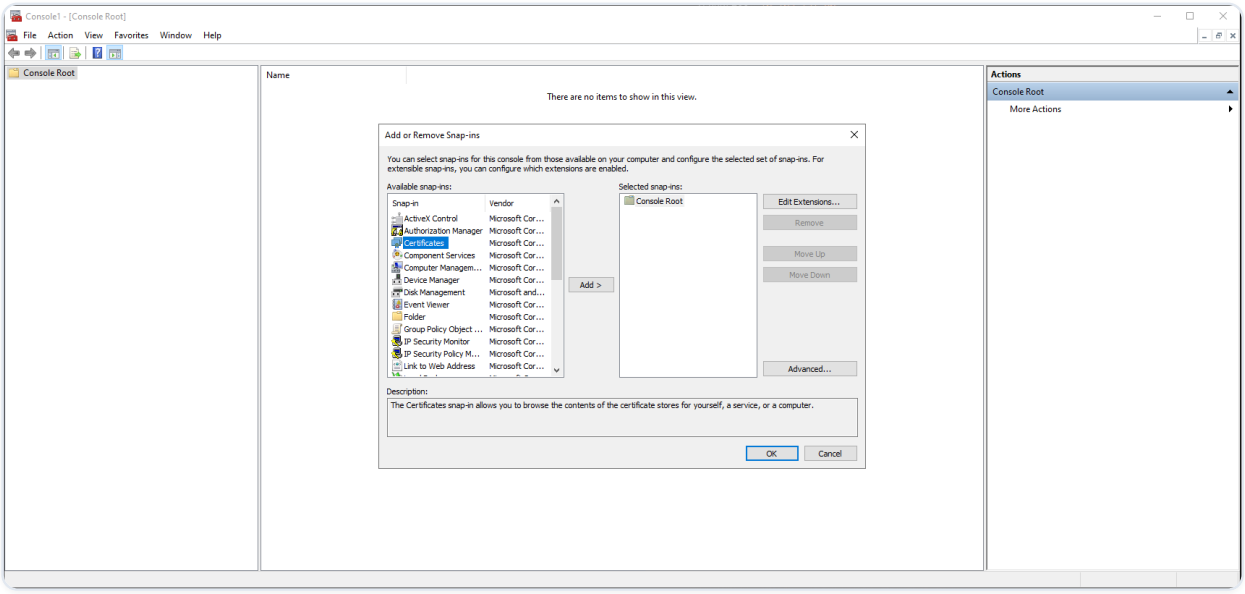
1. Citrix Infrastructure Monitor がインストールされているマシン用の `PFX` 証明書を取得します。PFX ファイルの生成の詳細については、「PFX ファイルを作成する方法」を参照してください。

   > **注:**
   >
   > パスワードで保護されたPFXファイルも使用できます。

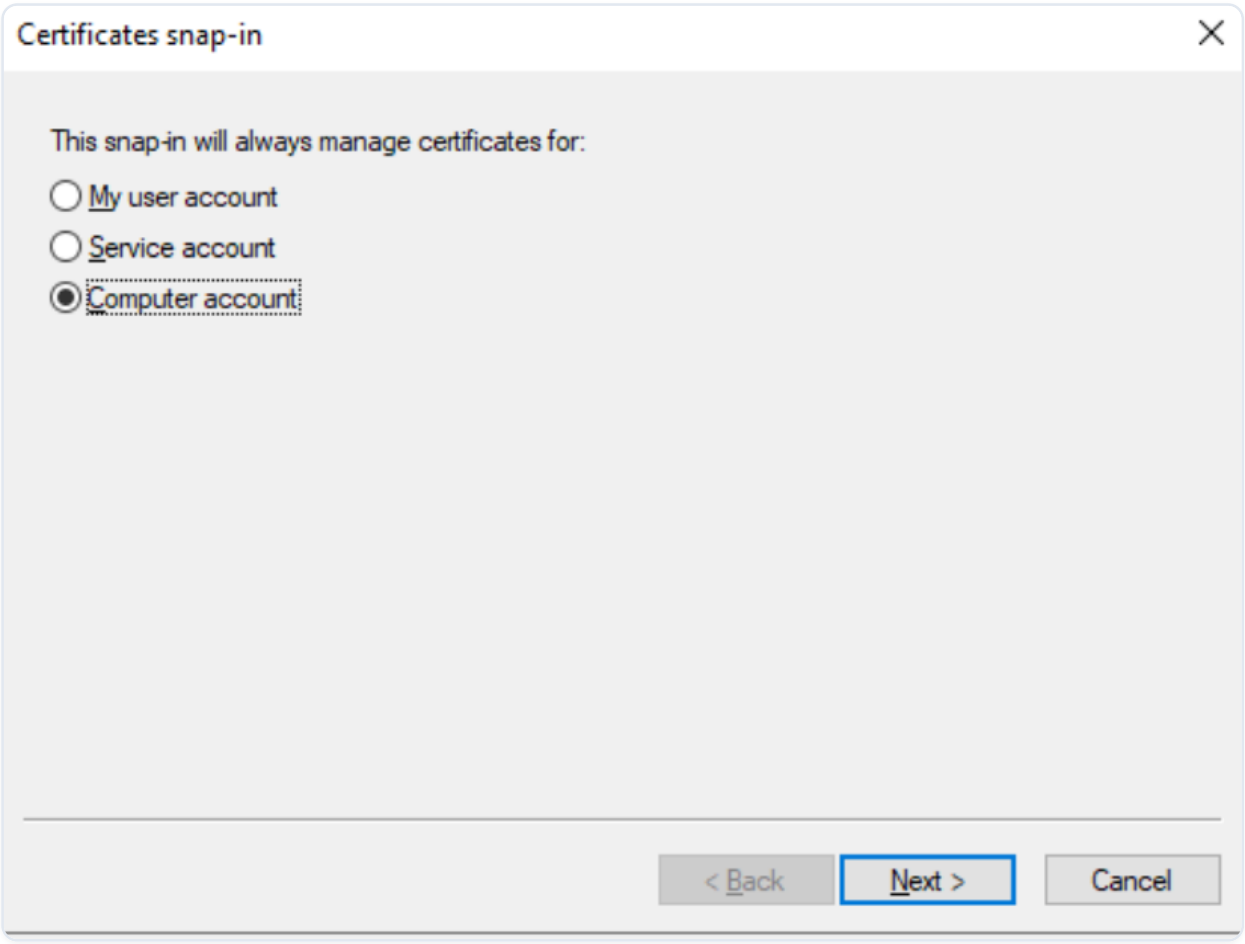
2. 証明書をマシンの任意の場所にアップロードします。

ステップ2：証明書をコンピューター証明書にインポートする

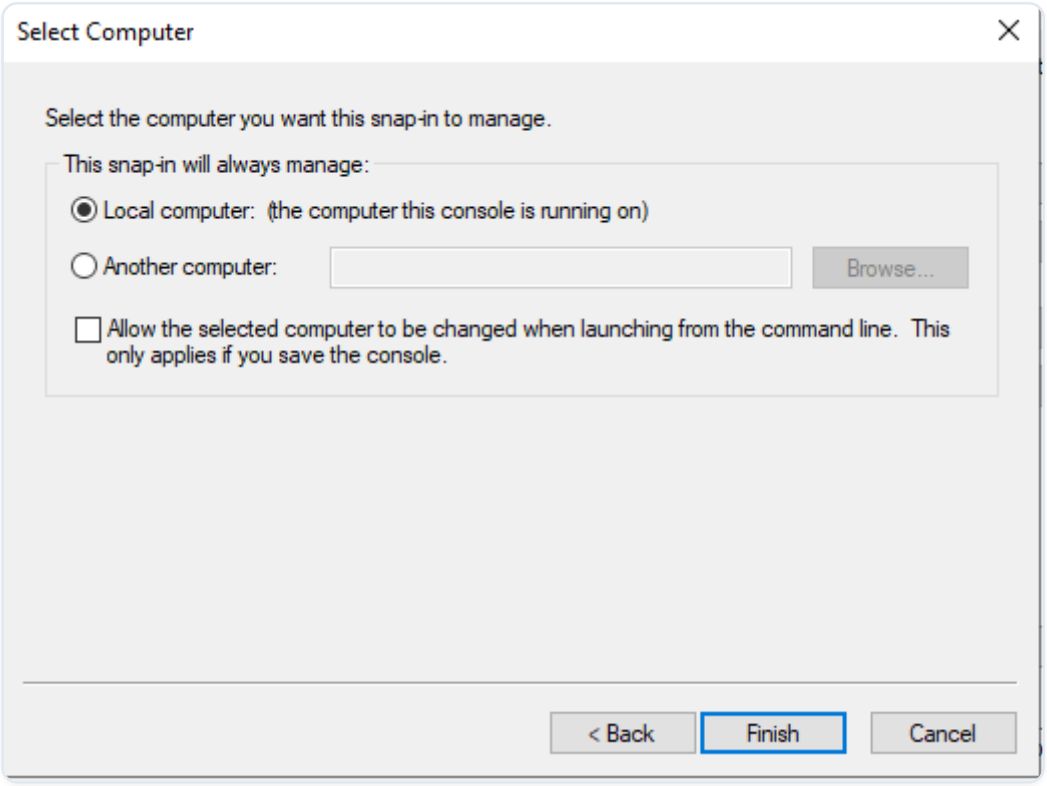
1. > をクリックし、`mmc` と入力して をクリックします。**[コンソール 1 -]** ウィンドウが表示されます。
2. メニューで をクリックします。 ウィンドウが表示されます。



3. 「**スナップイン**」の下で、「**証明書**」をダブルクリックします。「**証明書スナップイン**」ウィンドウが表示されます。

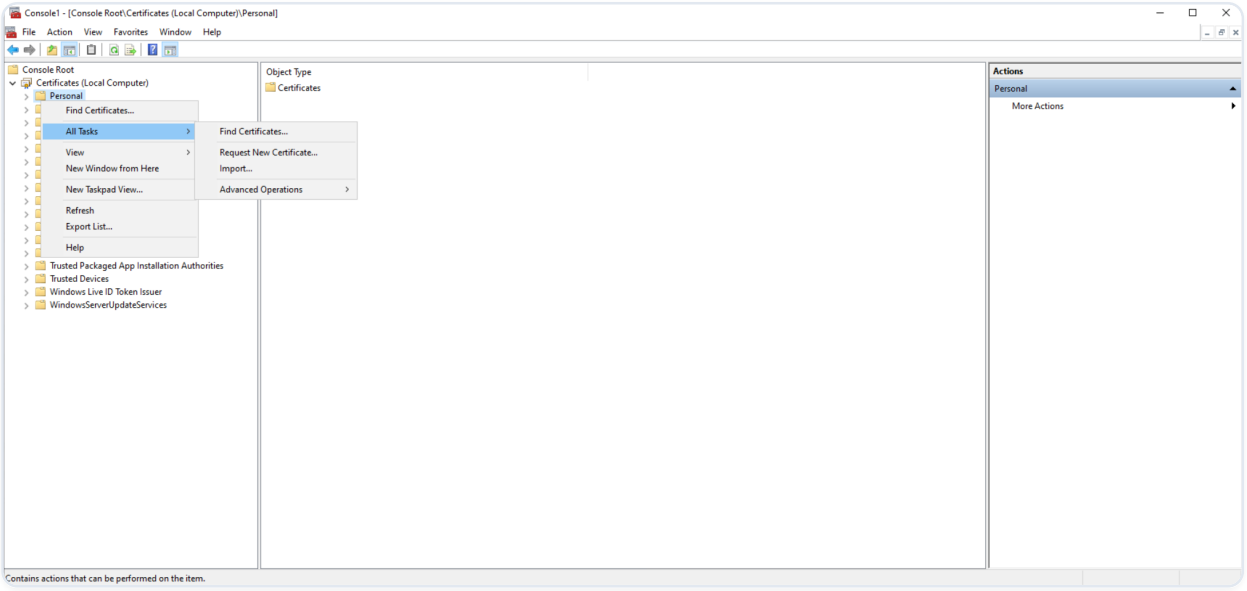


4. 「**コンピューターアカウント**」を選択し、「**次へ**」をクリックします。「**コンピューターの選択**」ウィンドウが表示されます。

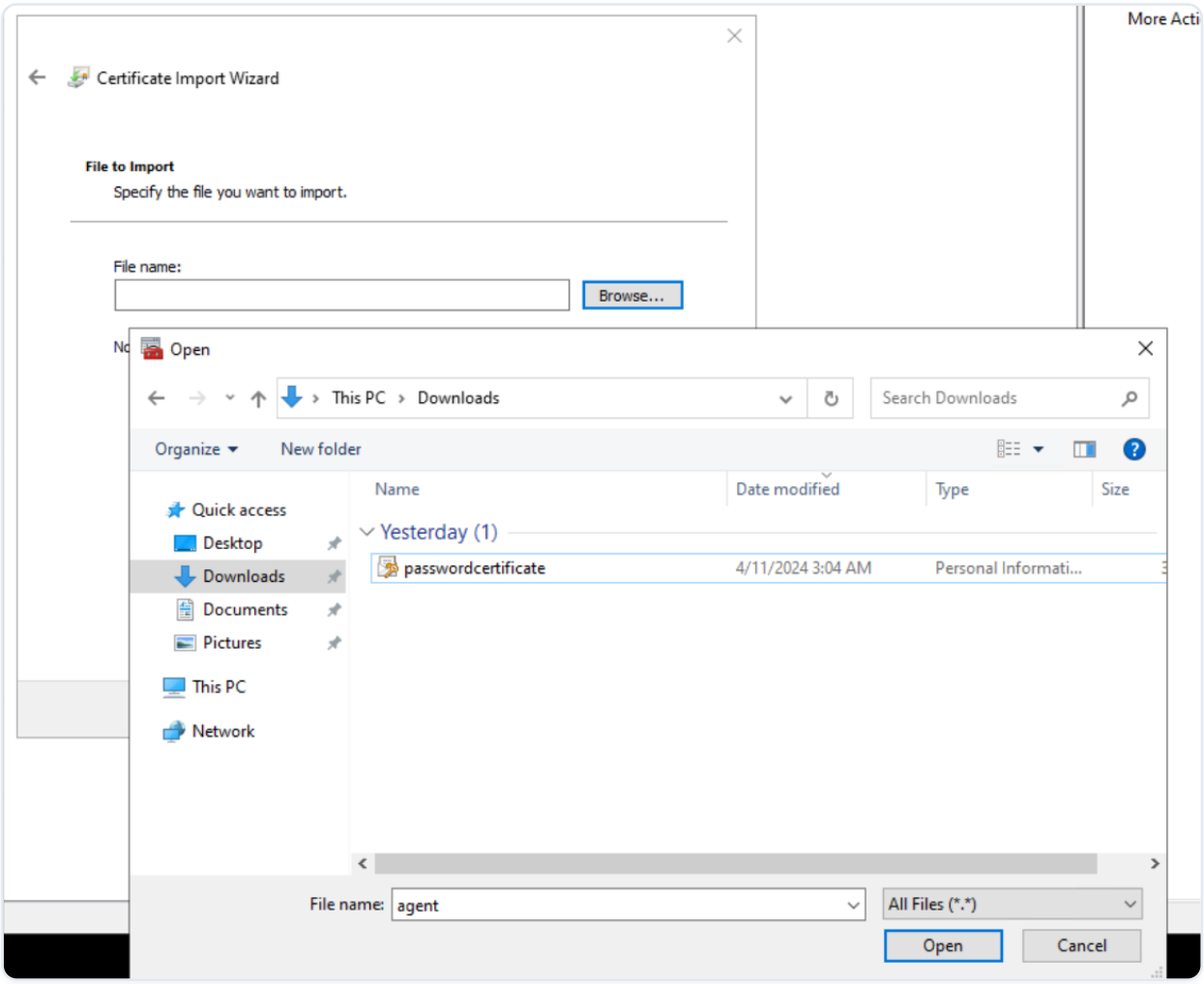


5. **ローカルコンピューター**を選択します。

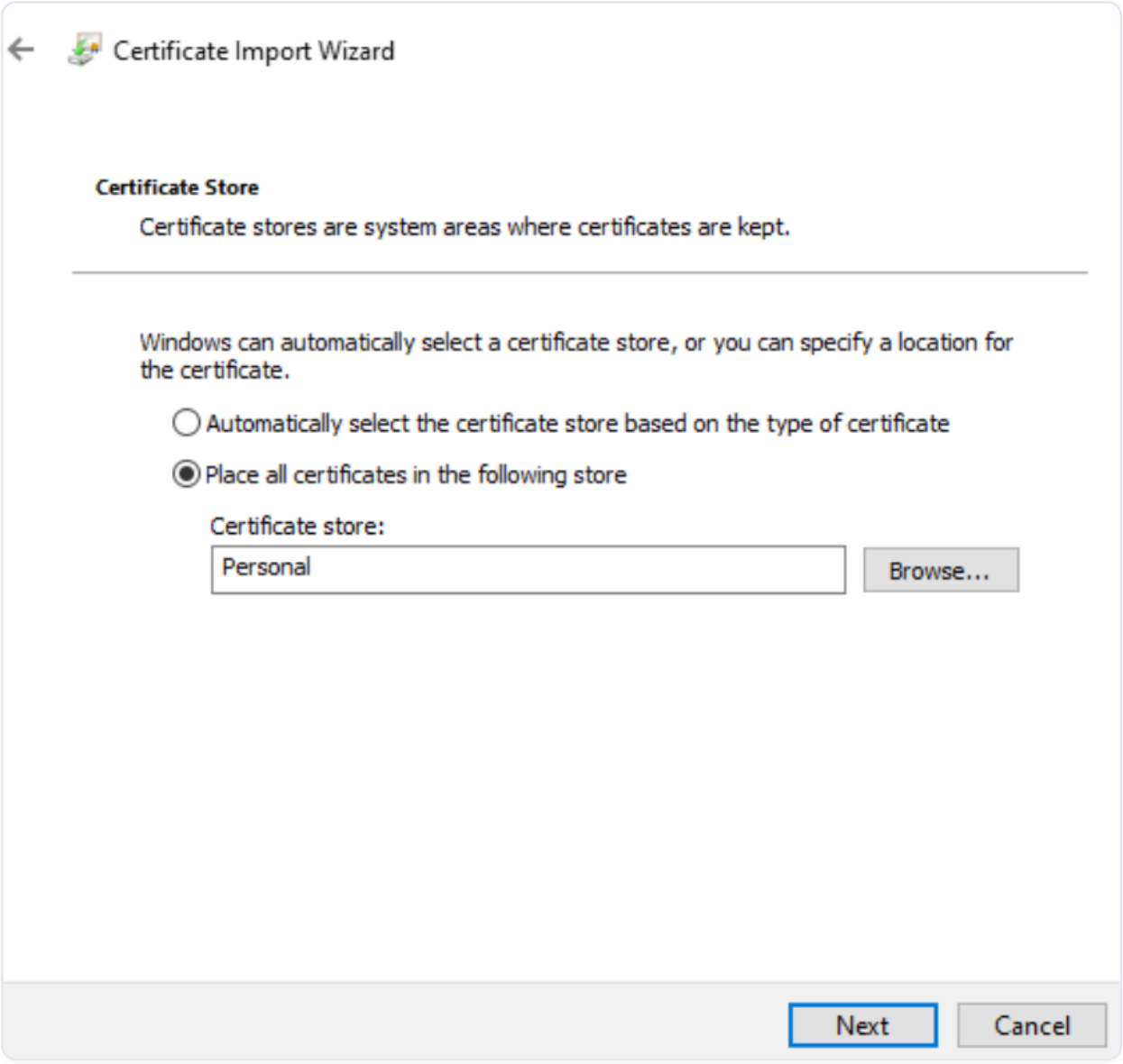
6. **完了**をクリックします。新しいコンソールの選択されたスナップインのリストに、**証明書(ローカルコンピューター)**セクションが表示されます。
7. **OK**をクリックします。
8. **証明書**を展開し、**個人**を右クリックして、**すべてのタスク** > **インポート**を選択します。**証明書のインポートウィザードへようこそ**が表示されます。



9. **次へ** > **ファイルの参照**を選択します。PFXファイルをアップロードした場所に移動し、ファイルの種類を**すべてのファイル**に変更してから、該当するPFX証明書を選択します。



10. PFXパスワードを入力します。パスワードがない場合は空白のままにできます。
11. **次へ**をクリックします。
12. 証明書ストアについては、**証明書をすべて次のストアに配置する**オプションが選択され、**証明書ストア**が**個人**として選択されていることを確認します。



13. **Next**をクリックします。
14. 詳細を確認し、**完了**をクリックします。
15. 確認を待ちます。*インポートは正常に完了しました*というメッセージが表示されます。
16. 「**証明書**」>「**個人**」に移動し、証明書が存在することを確認します。
17. マシンからPFX証明書ファイルを削除します。

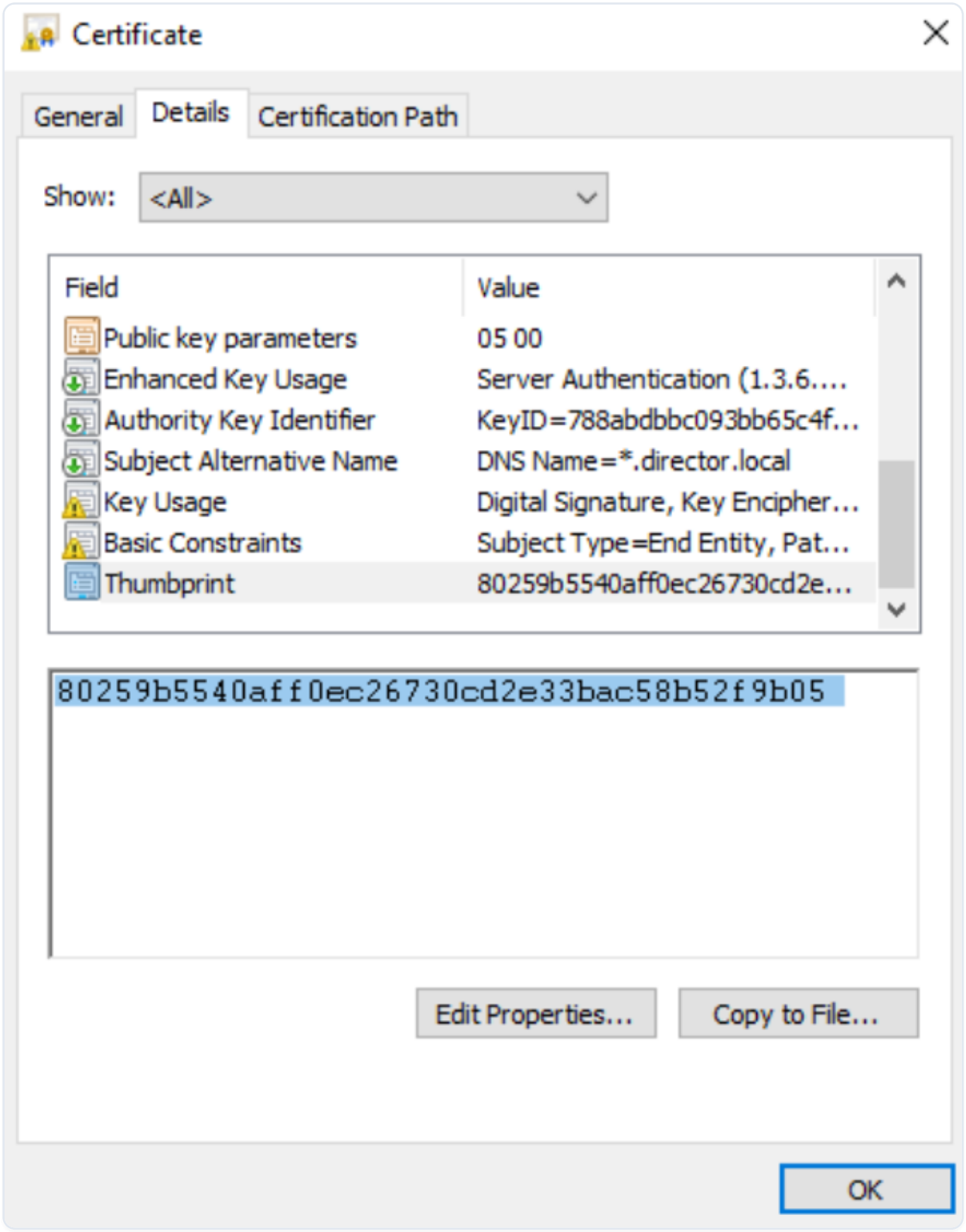
ステップ3：証明書への読み取りアクセスを許可する

1. インポートした証明書を右クリックし、**すべてのタスク** > **秘密キーの管理**を選択します。
2. 開いたダイアログで、**追加**を選択し、**Network Service**を検索します。 **OK**をクリックします。
3. **グループ**または**ユーザー名**の下にある**NETWORK SERVICE**を選択します。
4. **NETWORK SERVICEのアクセス許可**の下で*読み取り*アクセスを許可します。

5. **OK**をクリックします。

ステップ4：サムプリントを取得する

1. インポートした証明書をダブルクリックします。
2. 開いたダイアログで、**詳細**タブに移動し、一番下までスクロールします。
3. **Thumbprint**をクリックします。

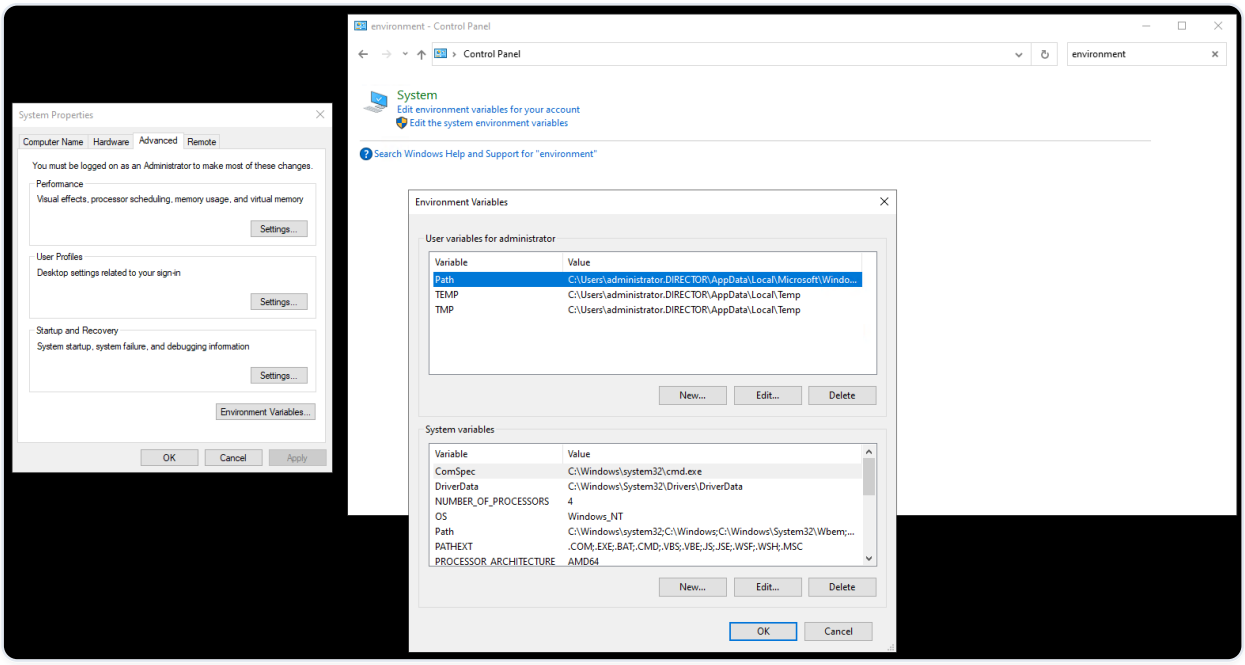


4. 値をコピーし、次のステップのために準備しておきます。

ステップ5：環境変数の設定

1. コントロールパネルを開きます。
2. 「環境」を検索し、**システム環境変数の編集**を選択します。

3. **システム環境変数 (すべてのユーザー)** の下で、**新規**をクリックします。



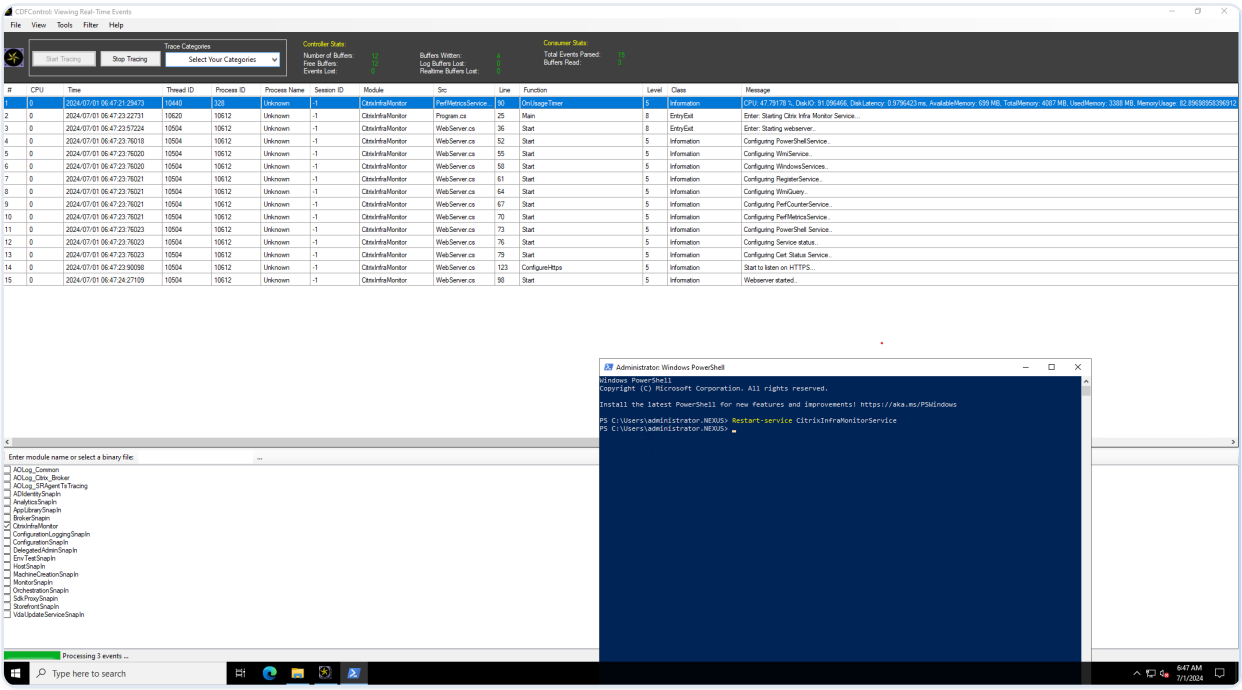
4. **変数**名として *DIRECTOR_AGENT_HTTPS_CERTIFICATE_THUMBPRINT* を指定します。
5. **変数値**の下に、前の手順で取得したサムプリントを指定します。
6. **OK**をクリックします。

手順 6: CitrixInfraMonitorService を再起動する

1. PowerShellを開き、次のコマンドを実行します。

```
Restart-Service CitrixInfraMonitorService
```

2. **CitrixInfraMonitorService** モジュールをキャプチャし、ログ行 **Start to listen on HTTPS...** を探して、HTTPS が有効になっていることを確認します。



手順 7: モニター構成で HTTPS を有効にする

Delivery Controller™マシンで次のコマンドを実行します。

```
Set-MonitorConfiguration -DirectorAgentEnableHttps $true
```

Citrix Infrastructure Monitor の手動接続

注:

以下の2つの手順は、Provisioning ServiceおよびStoreFront™コンポーネントの監視にのみ有効です。

ステップ 1: Citrix Infrastructure Monitor のインストール

安全なデータ収集のための接続を確立するため、ターゲットコンポーネントへのインストールを完了するには、以下の手順を実行します。

注:

Citrix Infrastructure Monitor をインストールするマシンには、Provisioning Service または StoreFront のいずれかがすでにインストールされている必要があります。

ステップ 1.1: ターゲットコンポーネントの特定

監視が必要なProvisioning ServiceやStoreFrontサーバーなどのターゲットコンポーネントを特定します。

ステップ 1.2 Citrix Infrastructure Monitor のダウンロード

ステップ 1.1 で特定されたターゲットサーバーの Citrix downloads ページから `CitrixInfraMonitor.msi` をダウンロードできます。

ステップ 1.3: Citrix Infrastructure Monitor の実行

インストールウィザードの指示に従って、ターゲットコンポーネントで `CitrixInfraMonitor.msi` インストーラーを実行します。

> **注:**
>
> 管理者権限を持つユーザーは、ターゲットコンポーネントに Citrix Infrastructure Monitor をインストールして構成できます。

> シトリックス インフラストラクチャ モニター(/en-us/citrix-virtual-apps-desktops/2511/media/citrixinframonitoring-resize.gif)

インストールが正常に完了すると、「**サービス**」セクションでCitrix Infrastructure Monitorサービスを表示できます。

シトリックス インフラストラクチャ モニター(/en-us/citrix-virtual-apps-desktops/2511/media/infra-services.png)

ステップ1.4: 登録トークンを取得する

Citrix Infrastructure Monitorがインストールされているシステムで、`C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt` にある `RegistrationToken.txt` ファイルで提供されているトークンを取得し、ステップ2: Citrix Infrastructure Monitorを登録するで使用できるように準備しておきます。

ポート要件

`CitrixInfraMonitor.msi` を正常にインストールすると、インストーラーはポート9595の例外を作成します。サードパーティのファイアウォールを使用している場合は、Citrix Infrastructure

Monitoringサービスを使用するために、このポートのTCP通信を手動で許可する必要がある場合があります。

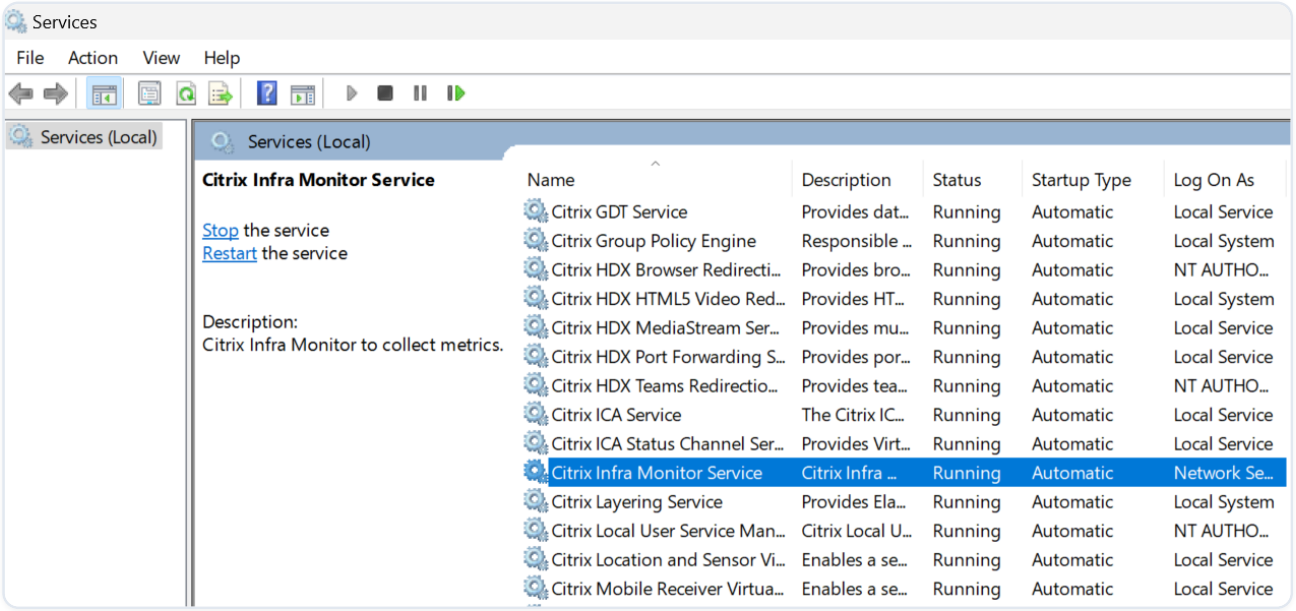
次の表に、Provisioning ServiceおよびStoreFrontマシンに対する受信ポート要件の詳細を示します。

ソース	ターゲット	タイプ	ポート	プロトコル	目的
DDC	Provisioning Service または StoreFront マシン	TCP	9595	HTTP または HTTPS	Provisioning Service または StoreFront マシンからメトリックを収集するための呼び出し。

> **注:**
>
> Provisioning Service および StoreFront マシンは、インフラストラクチャ監視サービスに対してアウトバウンド呼び出しを行いません。

ステップ 2: Citrix Infrastructure Monitor を登録する

Citrix Infrastructure Monitor は、次の方法で登録できます。



ステップ 1.4: 登録トークンを取得する

シトリックス インフラストラクチャ モニターがインストールされているシステムで、`C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt`にある`RegistrationToken.txt`ファイルに記載されているトークンを取得し、ステップ 2: シトリックス インフラストラクチャ モニターを登録するで使用できるように準備してください。

ポート要件

`CitrixInfraMonitor.msi`を正常にインストールすると、インストーラーは9595ポートの例外を作成します。サードパーティのファイアウォールを使用している場合は、Citrix Infrastructure Monitoringサービスを使用するために、このポートのTCP通信を手動で許可する必要がある場合があります。

次の表は、Provisioning ServiceおよびStoreFrontマシンに対するインバウンドポート要件の詳細を示しています。

送信元	ターゲット	タイプ	ポート	プロトコル	目的
DDC	Provisioning ServiceまたはStoreFrontマシン	TCP	9595	HTTPまたはHTTPS	Provisioning ServiceまたはStoreFrontマシンからメトリックを収集するための呼び出し。

> **注:**

> Provisioning ServiceおよびStoreFrontマシンは、Infrastructure Monitoringサービスに対してアウトバウンド呼び出しを行いません。

ステップ2：Citrix Infrastructure Monitorを登録する

Citrix Infrastructure Monitorは、以下の方法で登録できます。

- ディレクターユーザーインターフェース
- PowerShell SDK

Director UI から

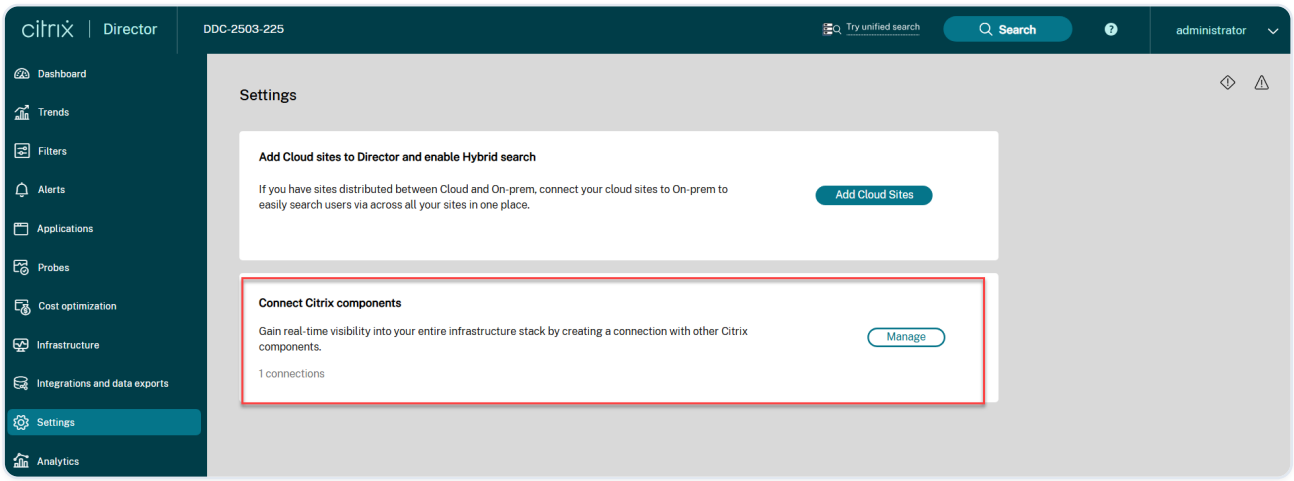
次の手順で Director UI で登録を完了します。

ステップ 2.1: Citrix コンポーネントの接続ページに移動する

設定 > **Citrix コンポーネントの接続** > **管理** をクリックします。

または、,

インフラストラクチャ > **管理**をクリックします。



](/en-us/citrix-virtual-apps-desktops/2511/media/connect-citrix-components.png)

ステップ2.2：コンポーネントの詳細を入力する

［**Citrix コンポーネントの接続**］ 画面で、［**接続の作成**］ をクリックします。［**接続の作成**］ ウィンドウが表示されます。

](/en-us/citrix-virtual-apps-desktops/2511/media/create-a-connectiOn.png)

ターゲットに`CitrixInfraMonitor.msi`がダウンロードされ、インストールされていることを確認してください。詳細については、このドキュメントの手順1を参照してください。画面の指示に従い、セキュアな接続を確立するために必要なコンポーネントの詳細を入力します。

- ドロップダウンリストからコンポーネントの種類を選択します。コンポーネントは Provisioning Service または StoreFront のいずれかです。
- ホスト名を入力します。
- ドメイン名を入力します。
- Provisioning Service または StoreFront マシンのユーザー名を入力します。
- Provisioning Service または StoreFront マシンのパスワードを入力します。

ステップ2.3：接続を承認する

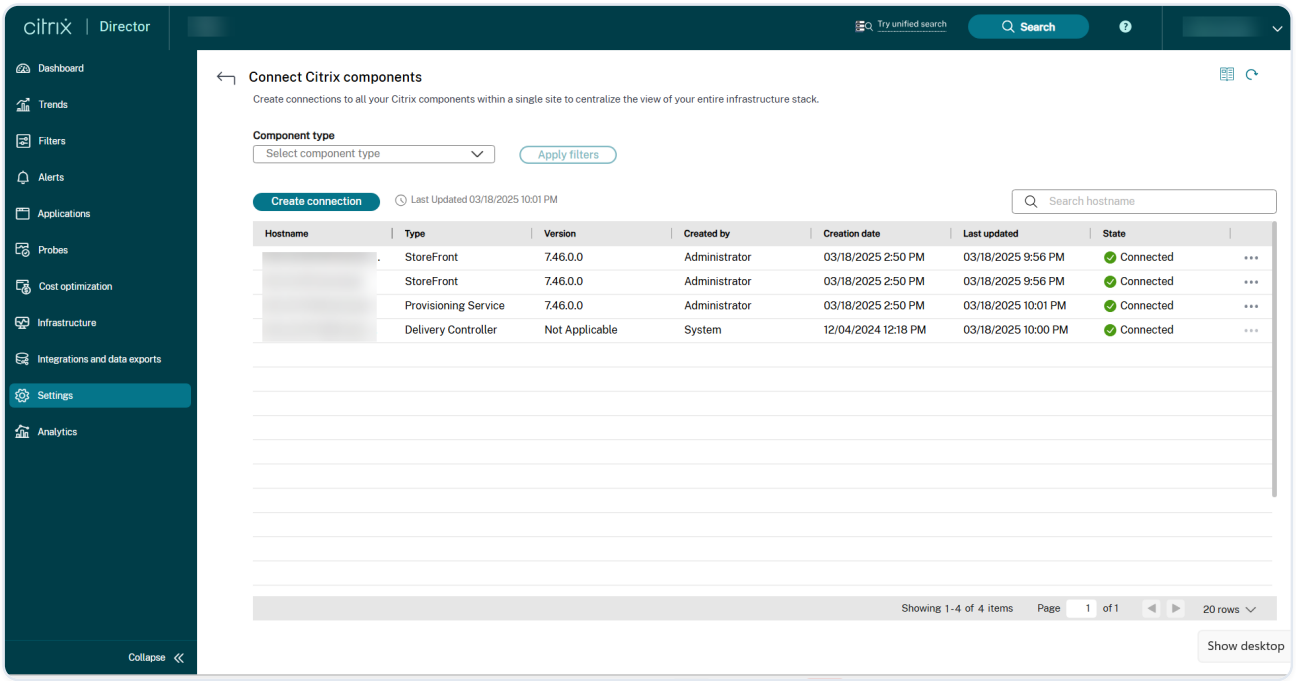
Citrix Infrastructure Monitorがインストールされているシステムで、`C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt`にある`RegistrationToken.txt`ファイルからCitrix Infrastructure Monitorトークンを取得します。

Director UIで取得したトークンの詳細を入力します。このトークンは、サイトとコンポーネント間の接続を認証します。

Citrix Infrastructure Monitorサービスを再起動すると、`RegistrationToken.txt`ファイルに存在するトークンテキストが再生成されます。登録が成功すると、トークンファイルはマシンから削除されます。何らかの理由で新しいトークンファイルを再作成する必要がある場合は、Citrix Infrastructure Monitorサービスを再起動してください。セキュリティ上の理由から、無効なトークンによる登録試行が3回失敗すると、トークンファイルは削除されます。

ステップ 2.4: 接続を作成する

詳細が入力されたら、**作成**をクリックします。作成された接続は、**Citrixコンポーネントの接続**ページにある接続リストの下に表示されます。



リモート PowerShell SDK の使用

前提条件：

- Citrix Infrastructure Monitor が StoreFront または PVS マシンにインストールされていることを確認します。

PVS または StoreFront マシンと通信するために、Citrix Infrastructure Monitor を DDC に登録します。この登録は、PVS または StoreFront マシンで収集されたインフラストラクチャの正常性メトリックを DDC に送信するためのものです。

Citrix Infrastructure Monitor に登録するには、Delivery Controller™ で次の PowerShell コマンドを実行します。

```
Add-MonitorDirectorAgent -Fqdn <FQDN of component> -Component <component>
-Domain <domain> -Username <username> -Password <password> -Token <token>
```

注:

ユーザー名とパスワードはオプションのパラメーターです。ただし、これらのパラメーターを指定しない場合、一部のメトリックは利用できません。

前述のコマンドのパラメーターは次のとおりです。

パラメーター	説明
`Fqdn`	PVSまたはStoreFrontサーバーのFQDN。
`Component`	オンボーディングするコンポーネント。例: PVSまたはSF。PVSはCitrix Provisioning™、SFはStoreFrontを表します。
`Domain`	すべてのコンポーネントが属するドメイン。
`Username`	管理者ユーザーのユーザー名。
`Password`	管理者ユーザーのパスワード。
`Token`	Citrix Infrastructure Monitorがインストールされているシステムで、`C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt`にある`RegistrationToken.txt`ファイルからCitrix Infrastructure Monitorトークンを取得します。

注:

- `RegistrationToken.txt`ファイルに存在するトークンテキストは、Citrix Infrastructure Monitorサービスを再起動すると再生成されます。登録が成功すると、トークンファイルはマシンから削除されます。再登録する必要がある場合は、Citrix Infrastructure Monitorサービスを再起動してください。
- セキュリティ上の理由から、無効なトークンによる登録試行が3回失敗すると、トークンファイルは削除されます。

PVS または StoreFront マシンの登録が正常に完了すると、マシン名の詳細が **Director** > **インフラストラクチャ**タブに表示されます。

Citrix Infrastructure Monitorに登録するためのコマンド例は次のとおりです。

インフラモニターを再起動(/en-us/citrix-virtual-apps-desktops/2511/media/sm-sample-comand-im-register-on-prem.png)

統合とデータのエクスポート

Citrix Directorは、統合とデータのエクスポートのための新しいUIを提供するようになりました。この機能は、Citrix Directorで利用可能なさまざまなインターフェイスとサードパーティ統合の認識を高めるのに役立ちます。新しく導入された**統合とデータのエクスポート**ページには、次のものが一覧表示されます。

- 利用可能な統合
- サポートされている開発者ツール

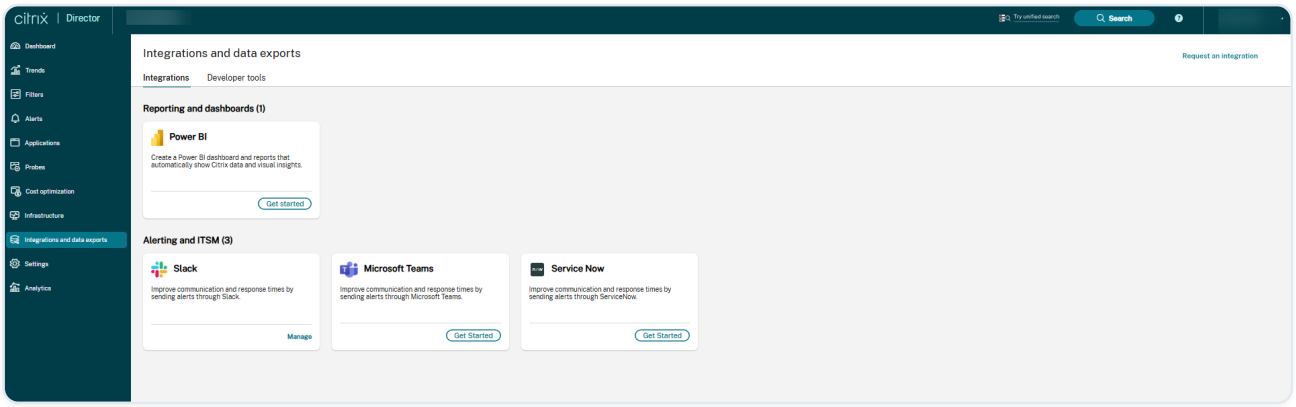
このページでは、データエクスポート用のREST APIの設定についても説明しています。また、統合と開発者ツールの使用を開始するためのガイドとドキュメントへの参照リンクも提供しています。

Citrix監視メトリックを収集するために、次の統合オプションが提供されています。

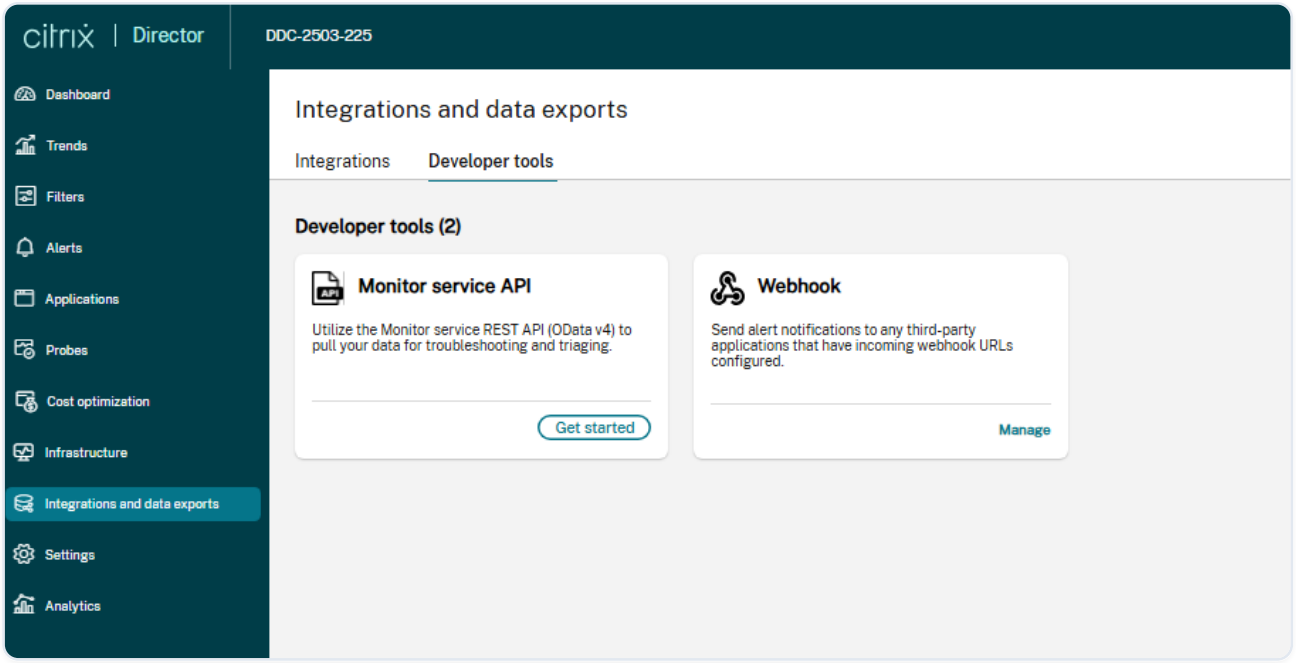
- Citrix MonitorサービスAPI - Citrix MonitorサービスAPIを使用して、Citrix Monitorからパフォーマンスデータとイベントを収集し、Power BIにエクスポートできます。
- アラートとITSM - 受信Webhook URLが構成されている次のサードパーティアプリケーションにアラート通知を送信できます。

- スラック
- マイクロソフト Teams
- ServiceNow

左側のナビゲーションメニューから**統合とデータのエクスポート**をクリックします。**統合とデータのエクスポート**ページが表示されます。



開発者ツール:



利用可能な統合を表示

統合タブには、Citrix Director で利用可能な統合が表示されます。利用可能な統合は、以下のように分類されます。

- レポートとダッシュボード
- アラートとITSM

レポートとダッシュボード

Power BIは、Citrix Director APIを通じて収集されたメトリックを視覚化するために使用できます。**開始**をクリックします。**REST API**開発者ツール詳細ページが表示されます。

Monitor サービス API をクリックすると、PowerBI との統合に関するリソースやブログへの参照リンクが表示されます。

このページには、リソースやブログへの参照リンクが記載されています。

アラートおよびITSMツールとの統合

アラートおよびITSMツールには、以下が含まれます。

- スラック
- マイクロソフト チームズ
- ServiceNow

アラートおよびITSMツールをWebhookと統合するには、ツールの横にある**開始する**リンクをクリックします。このリンクをクリックすると、特定の警告およびITSMツールの統合ページが開き、前提条件とアラートを送信するための具体的な手順の詳細が表示されます。ツールとWebhook URLを設定できます。たとえば、Slackを統合するには、Slackのドキュメントに従ってチャネルとWebhook URLを作成する必要があります。

それが完了したら、次のステップとしてWebhookプロファイルを作成します。

参照リソースも確認できます。たとえば、Slack と統合するための前提条件と手順は次のとおりです。

Slack統合(/en-us/citrix-virtual-apps-desktops/2511/media/slack-integration.png)

Webhookとの統合

1. **Integrations**タブ > **Alerting and ITSM**セクション > 選択したツールの横にある**Get started**をクリックします。そのツールの**Integration**ページが開きます。
2. リソースやブログへの参照リンクにアクセスできます。
3. ステップ1に従います。
4. ステップ2の一部として**Create webhook**プロファイルをクリックします。`<name of the tool>` **Create Webhook profile**ページが表示されます。
5. Webhookプロファイルの**Name**を入力します。
6. Webhookプロファイルの**Description**を入力します。

7. **Webhook configuration**セクションで、希望する**Method**を選択します。
8. 前のステップで選択したメソッドに従って、**API/Webhook** URLを入力します。
9. **Message**形式を表示します。
10. **Headers**セクションにキーと値を追加します。
11. 作成したWebhookを検証するには、**Test**をクリックします。
12. Webhookが正常に検証されたら、**Create Webhook**をクリックします。Webhookが作成されます。
13. 作成したWebhookプロファイルは、**Developer tools** > **Webhook** > **Manage**で表示できます。**Webhook profiles developer tool details**ページが開きます。

Webhookプロファイルは、**開発者ツール** > **Webhook** > **Webhookプロファイルの作成**でも作成できます。

WebhookプロファイルをCitrix Alertsと統合する

作成したWebhookプロファイルは、**Alerts** > **Advanced Alert Policies** > **Create Policy**セクションで表示し、Citrix Alertsの一部として使用できます。

Webhookプロファイルを新しいCitrixアラートポリシーと統合するには、次の手順を実行します。

1. **アラート** > **高度なアラートポリシー** > **ポリシーの作成**をクリックします。**高度なアラートポリシーの作成**ページが表示されます。
2. **通知チャネル** > **Webhookの使用**セクションに移動します。
3. Webhookプロファイルを選択します。
4. アラートポリシーを保存します。

Webhookプロファイルを既存のアラートポリシーと統合するには、次の手順を実行します。

1. **アラート** > **高度なアラートポリシー** > **ポリシーの編集**をクリックします。**高度なアラートポリシーの編集**ページが表示されます。
2. **通知チャネル** > **Webhookの使用**セクションに移動します。
3. Webhookプロファイルを選択または変更します。
4. アラートポリシーを更新して保存します。

サポートされている開発者ツールを表示する

利用可能な開発者ツールを表示するには、**Developer tools**タブをクリックします。

利用可能な開発者ツールは、Monitor service APIとWebhookです。

開発者ツール）](/en-us/citrix-daas/media/integrations-developer-tools.png)

モニターサービスAPI

「**開始する**」をクリックします。「**Monitor Service API**」開発者ツール詳細ページが開きます。リソースやブログへの参照リンクにアクセスできます。

ウェブフック

Webhook プロファイルは、**開発者ツール** > **Webhook** > **Webhook プロファイルの作成**で表示および作成できます。

Ansible を使用して VDA をインストールする

概要

この記事では、Ansible を使用して VDA を展開する方法について説明します。詳細については、Ansible ドキュメントを参照してください。

> **注:**
>
> この記事では、Citrix® が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、お客様のニーズに合わせてカスタマイズできます。Citrix は、お客様のニーズに合わせて必要な更新や調整について責任を負いません。

Ansible を使用して VDA を展開するための主要な手順

1. 仮想マシン環境を構成する。
2. Ansible をインストールする
3. Kerberos の構成
    a. Kerberos をインストールする
    b. Kerberos を構成する
4. Ansible を構成する

ステップ 1: 仮想マシン環境を構成する

Windows サーバーで次のコマンドを実行します。

1. PS RemoteSigned を設定します。 `Set-ExecutionPolicy RemoteSigned`
2. WinRM を暗号化なしで使用するように設定します。 `winrm set winrm/config/service '@{AllowUnencrypted="true"}'`

   > **注:**
   >
   > このステップでエラーが発生した場合は、次のコマンドを使用します: `Enable-PSRemoting -Force`

3. ファイアウォールポート5985を開きます。 `New-NetFirewallRule -DisplayName "Allow WinRm port 5985" -Direction Inbound -Profile Any -Action Allow -LocalPort 5985 -Protocol tcp`

ステップ2: Ansibleをインストールする

Ubuntu 20.4以降でAnsibleをインストールするには、次のコマンドを実行します。

- `sudo apt update`
- `sudo apt install software-properties-common`
- `sudo add-apt-repository --yes --update ppa:ansible/ansible`
- `sudo apt install ansible`
- `sudo apt install python3-pip`

ステップ2i: Kerberosをインストールする

Kerberosをインストールするには、次のコマンドを実行します。

`sudo apt install python3-dev libkrb5-dev krb5-user`

ステップ2ii: Kerberosを構成する

Kerberosを構成するには、次のコマンドを実行します。

`Edit /etc/krb5.conf`

```
[libdefaults]
        default_realm = [redacted]

# The following krb5.conf variables are only for MIT Kerberos.
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true

# The following encryption type specification will be used by MIT Kerberos
# if uncommented.  In general, the defaults in the MIT Kerberos code are
# correct and overriding these specifications only serves to disable new
# encryption types as they are added, creating interoperability problems.
#
# The only time when you might need to uncomment these lines and change
# the enctypes is if you have local software that will break on ticket
# caches containing ticket encryption types it doesn't know about (such as
# old versions of Sun Java).

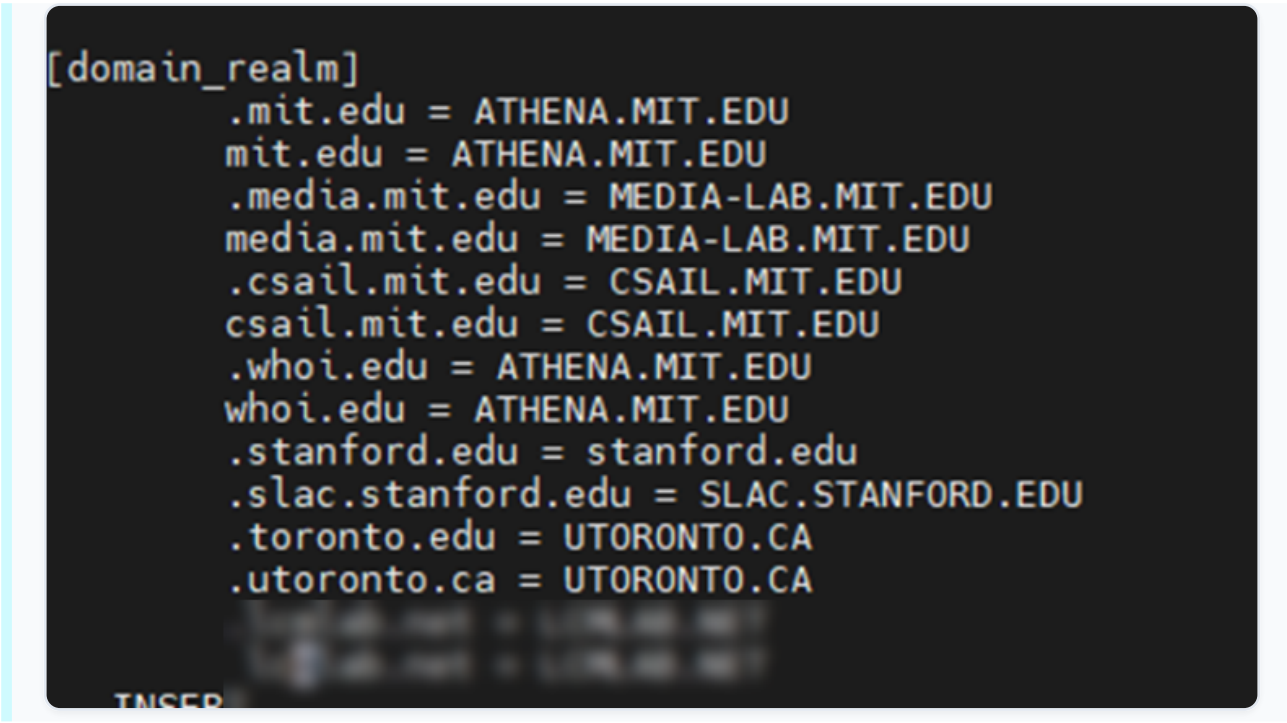
#       default_tgs_enctypes = des3-hmac-sha1
#       default_tkt_enctypes = des3-hmac-sha1
#       permitted_enctypes = des3-hmac-sha1

# The following libdefaults parameters are only for Heimdal Kerberos.
        fcc-mit-ticketflags = true

[realms]
        LTSRLAB.NET = {
                kdc = [redacted]
                admin_server = [redacted]
        }
        ATHENA.MIT.EDU = {
                kdc = [redacted]
```

注:

Kerberosレルム名には大文字を使用します。



ステップ3：Ansibleの構成

Ansibleホストを構成するには、次の手順を実行します。

1. 次のコマンドを実行します。

   ```
   Edit /etc/ansible/hosts
   ```

2. Delivery Controller `Install.yaml` ファイルを構成します

   ```
   /QUIET /NOREBOOT /NORESUME /OPTIMIZE /VERBOSELOG /COMPONENTS VDA /CONTROLLERS 'MyDDC.xd.local' /ENABLE_HDX_PORTS /ENABLE_REAL_TIME_TRANSPORT
   ```

   「デリバリーコントローラー」(/en-us/citrix-virtual-apps-desktops/2511/media/delivery-controller-yaml-1.png)

   「デリバリーコントローラー」(/en-us/citrix-virtual-apps-desktops/2511/media/delivery-controller-yaml-2.png)

   「デリバリーコントローラー」(/en-us/citrix-virtual-apps-desktops/2511/media/delivery-controller-yaml-3.png)

```
- name: Resume VDA install
  win_package:
    path: C:\Temp\X64\Xendesktop Setup\XendesktopVdaSetup.exe
    expected_return_code: [0,3,3010]
  when: install_vda.changed
  register: vda_resume

- name: debug 2
  debug:
    msg: "{{vda_resume}}"

- name: Restart server after VDA install
  win_reboot:
  when: vda_resume.changed

- name: find files
  win_find:
    paths: C:\ProgramData\Citrix\XendesktopSetup\XendesktopVdaSetup.exe
  register: vda_install_find

- name: Restart server after VDA install
  win_reboot:
  when: vda_install_find.matched == 0

- name: remove temp folder
  win_file:
    path: C:\Temp\
    state: absent
```

3. 次のコマンドでyamlファイルを実行します。 `sudo ansible-playbook install.yml -vvv` (詳細モード)
4. 設定ファイルで、他の追加設定とともに複数のホストを構成できます。

`Edit /etc/ansible/hosts`

```
[WSVDA]
[redacted]

[TSVDA]
[redacted]

[WSVDA:vars]
ansible_port=[redacted]
ansible_user = [redacted]
ansible_password = [redacted]
ansible_connection = winrm
ansible_winrm_transport = kerberos
ansible_winrm_server_cert_validation = ignore

[TSVDA:vars]
ansible_port=[redacted]
ansible_user = [redacted]
ansible_password = [redacted]
ansible_connection = winrm
ansible_winrm_transport = kerberos
ansible_winrm_server_cert_validation = ignore
```

Call Home の主要データポイント

Call Home は以下の主要データポイントを収集します。

(M) = 手動収集時のみ取得 (PowerShell コマンドレット `Start-CitrixCallHomeUpload`)

ファイル名	カテゴリ	データグループ

		マシン
		XDサイト
		サイト情報
		Broker DB 情報 (M)
		インストールされている DB バージョン (M)
		Broker サービスステータス (M)
		登録済みサービスインスタンス (M)
		ブローカーライセンステスト (M)
		アクティブなHDX™セッション (M)
		ブローカー管理者
		ブローカー管理者権限
		RDS構成 (LicensingSettings、SessionSettings、SpecifiedLicenseServers、RegisteredLicenseServersを含む)
		監視サービス (M) (MonitorConfiguration、MonitorDataStore、MonitorDBConnection、MonitorDBSchemaVersion、MonitorService、MonitorServiceAddedCapability、MonitorServiceInstance、MonitorServiceStatus、

		MonitorInstalledDBVersionを含む)
		構成ログ
		接続ログ
		ハイパーバイザー接続 (M)
		ブローカーハイパーバイザー接続
		ハイパーバイザーアラート
		カタログ
		マルチセッションOSエージェント (M)
		シングルセッションOSエージェント (M)
		公開アプリケーション
		デリバリー グループ
		構成済みデリバリーエージェント

		Citrixインストール済みコンポーネント
		シトリックス ブローカーサービス情報
		Broker Service構成ファイル
		Machine Creation Services™ 構成ファイル
		ホストサービス構成ファイル

		AD Identity Service構成ファイル
		構成サービス構成ファイル
		構成ログサービス構成ファイル
		委任管理サービス構成ファイル
		環境テストサービス構成ファイル
		監視サービス構成ファイル
		Storefront™ サービス構成ファイル
		ワークステーションエージェント構成ファイル
		Citrix VDA情報
		Citrix XD ホットフィックス
		Citrix_VirtualChannel_Graphics_Enum
		Citrix_VirtualChannel_Flash_Enum
		Citrix_VirtualChannel_Printer_Enum

		コンピューター
		BIOS
		メモリ情報
		プロセッサ

		PNP デバイス
		デバイス
		ディスクドライブ
		論理ドライブ
		ページファイル使用状況
		ネットワークアダプター
		ネットワークアダプター構成
		ipConfig
		ビデオコントローラー
		IDE コントローラー
		SCSI コントローラー

		HKLM:\Software\Wow6432Node\Citrix
		HKLM:\System\CurrentControlSet\Control\Citrix
		HKLM:\SOFTWARE\Policies\Citrix
		HKLM:\Software\Microsoft\Cryptography
		HKLM:\Software\Wow6432Node\Microsoft\Cryptography

		HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Windows
		HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
		HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
		HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer
		HKLM:\SYSTEM\CurrentControlSet\Control\Print\Environments
		HKLM:\System\CurrentControlSet\Control\Session Manager
		HKLM:\System\CurrentControlSet\Control\Terminal Server
		HKCU:\Control Panel\Desktop
		HKLM:\SOFTWARE\Classes\ShockwaveFlash.ShockwaveFlash\CurVer
		HKLM:\SYSTEM\CurrentControlSet\Control\SystemInformation

		HKLM: \SYSTEM\CurrentControlSet\ Control\FileSystem
		HKLM: \SYSTEM\CurrentControlSet\ Control\Windows
		HKLM: \SYSTEM\CurrentControlSet\ Control\TimeZoneInformation

		ドライバー
		EnvVariables
		OS
		プロセス
		サービス
		サービスパック
		ジーピーリザルト
		Microsoft ホットフィックス
		ネットスタット
		PNP ドライバー

		システムイベントログ
		AOT (常時オンのトレース)
		クラッシュダンプ

		アップタイム
		メモリ

		コンピューターシステム
		プロセッサ
		ビデオコントローラー
		ディスクドライブ
		ブラウザ情報
		再起動回数
		メモリ使用量
		ディスク使用量
		ICAセッション解像度
		ICAカラー深度
		メタインストーラーCEIPマシンID

		ストア数
		サーバーグループ内のサーバー数
		ストアあたりのDelivery Controller™数
		HTTPS有効
		Citrix Receiver™向けクラシックエクスペリエンス有効
		シトリックス レシーバー 向け HTML5 レシーバー 設定
		Citrix Receiver向けワークスペースコントロール有効

		ストア向けリモートアクセス有効
		ゲートウェイ数
		統合NetScaler®認証用明示的JSONサービス

プロファイルコンテナのポリシー設定

プロファイルコンテナ

ユーザープロファイルに関連付けられた大きなフォルダーは、ログオンの遅延を引き起こします。Citrix Profile Managementは、プロファイルディスク（VHDXファイル）に含めるフォルダーを指定できるVHDXベースのプロファイルソリューションを提供します。このソリューションは、指定されたフォルダーをネットワークに保存されているプロファイルディスクにマッピングすることで、ログオン時間を短縮します。プロファイルコンテナは、ログオン中にこれらのフォルダーを含むプロファイルディスクをアタッチするため、フォルダーのコピーをローカルプロファイルに保存する必要がなくなります。これにより、ログオン時間が短縮されます。

プロファイルコンテナのローカルキャッシュを有効にする

このポリシーは、Citrix Profile Managementプロファイルコンテナのローカルキャッシュサポートを有効にします。ポリシーが**有効**に設定されている場合、各ローカルプロファイルは、そのCitrix Profile Managementプロファイルコンテナのローカルキャッシュとして機能します。プロファイルストリーミングが使用されている場合、ローカルにキャッシュされたファイルはオンデマンドで作成されます。それ以外の場合は、ユーザーログオン時に作成されます。ローカルキャッシュ機能を使用するには、ユーザープロファイル全体をCitrix Profile Managementプロファイルコンテナに配置します。

プロファイルコンテナから除外するフォルダー

Citrix Profile Managementプロファイルコンテナから除外するフォルダーのリスト。

プロファイルコンテナに含めるフォルダー

親フォルダーが除外されている場合に、Citrix Profile Managementプロファイルコンテナに保持するフォルダーのリスト。

このリストのフォルダーは、除外されたフォルダーのサブフォルダーである必要があります。そうでない場合、この設定は機能しません。

プロファイルコンテナに含めるファイル

Citrix Profile Managementプロファイルコンテナに含めるファイルのリスト。

このリストのファイルは、除外されたフォルダー内にある必要があります。そうでない場合、この設定は機能しません。

プロファイルコンテナから除外するファイル

Citrix Profile Managementプロファイルコンテナから除外するファイルのリスト。

VHDディスクの圧縮を有効にする

Profile ManagementのVHDディスク圧縮を有効にできます。有効にすると、特定の条件が満たされたときに、ユーザーのログオフ時にVHDディスクが自動的に圧縮されます。このポリシーにより、プロファイルコンテナ、OneDriveコンテナ、およびミラーフォルダコンテナによって消費されるストレージスペースを節約できます。

必要性と利用可能なリソースに応じて、詳細設定にある「**VHDディスク圧縮をトリガーする空き領域の比率**」、「**VHDディスク圧縮をトリガーするログオフ回数**」、「**VHDディスク圧縮のデフラグを無効にする**」の各ポリシーを使用して、デフォルトのVHD圧縮設定と動作を調整できます。

プロファイルコンテナのVHD自動拡張を有効にする

プロファイルコンテナのVHD自動拡張を有効にするかどうかを指定できます。有効にすると、すべてのVHD自動拡張設定がプロファイルコンテナに適用されます。

構成の優先順位:

- このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここでも.iniファイルでも構成されていない場合、無効になります。

VHDコンテナへの排他的アクセスを有効にする

デフォルトでは、VHDコンテナは同時アクセスを許可します。この設定を有効にすると、一度に1つのアクセスのみを許可します。この機能は、プロファイルコンテナとOneDriveコンテナに適用されます。

> **注:**

> コンテナベースのプロファイルソリューションでプロファイルコンテナに対してこの設定を有効にすると、「*プロファイルコンテナのマルチセッションライトバックを有効にする*」設定が自動的に無効になります。

> 構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、設定は無効になります。

ログオン時にプロファイルコンテナが利用できない場合にユーザーをログオフする

ユーザーログオン時にプロファイルコンテナが利用できない場合に、ユーザーを強制的にログオフさせ、(オプションで)ユーザーに表示されるエラーメッセージをカスタマイズできます。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
2. ここでも.iniファイルでもこのポリシーが構成されていない場合、この設定は無効になります。

プロファイルコンテナにアクセスするユーザーとグループ

プロファイルコンテナに対して`Read & Execute`権限を持つADドメインユーザーとグループを指定できます。デフォルトでは、プロファイルコンテナはその所有者のみがアクセスできます。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.iniファイルの設定が使用されます。
2. ここでも.iniファイルでもこのポリシーが構成されていない場合、プロファイルコンテナはその所有者のみがアクセスできます。