シトリックス バーチャル アプリケーションズ アンド デスクトップ™ 7 2411

ファイルベースのライセンスシステム EOL通知

従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきたファイルベースのライセンスシステムは、April 15, 2026 にサポート終了 (EOL) となります。License Activation Service (LAS) は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。April 15, 2026 以降、Citrixオンプレミスコンポーネントをアクティベートおよびライセンス供与する唯一の方法はLASになります。サポートを継続するには、Citrix Virtual Apps and Desktopsの展開がLAS互換バージョンである必要があります。LAS互換の最小要件となるCVADバージョンは次のとおりです。

- CVAD 2203 LTSR CU7
- CVAD 2402 LTSR CU3
- CVAD 2507 LTSR
- CVAD 2411

ご質問やご不明な点がある場合は、カスタマーケアにお問い合わせください。Citrixは、これらの要件を遵守しない場合、Citrixが法律または衡平法上持つ可能性のあるその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止する場合があります。これらの要件は、法律または規制によって禁止されている場合は適用されません。

リリースについて

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

- **サイトのインストールまたはアップグレード**: このリリースのISOを使用して、コアコンポーネントとVDAをインストールまたはアップグレードします。最新バージョンにインストールまたはアップグレードすると、最新の機能を使用できます。

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

  VDAをこのバージョン (バージョン7.9以降) にアップグレードした後、マシンカタログの機能レベルを更新する必要はありません。**7.9 (またはそれ以降)** の値はデフォルトの機能レベルのままであり、このリリースで有効です。詳しくは、「VDAバージョンと機能レベル」を参照してください。

インストールとアップグレードの手順：

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

シトリックス バーチャルアプリおよびデスクトップ 7 2411

ライセンスアクティベーションサービス

ライセンスアクティベーションサービス (LAS) は、従来のCitrixレガシーライセンスに代わる新しいクラウドベースのライセンスソリューションです。ライセンスサーバーをアップグレードし、Citrix Cloudに登録するだけで済みます。互換性のある製品がライセンスサーバーを指すように設定されると、自動的にアクティベートされます。詳細については、ライセンスアクティベーションサービスを参照してください。

ローカルホストキャッシュにおける1回限りの使用プールデスクトップ

ローカルホストキャッシュ (LHC) の停止モード中に、プールされたデスクトップの1回限りの使用を設定できるようになりました。これは、VDAバージョン2407以降にのみ配布される衛生ブロブを活用します。対応するマシンは、単一の停止セッション後に自動的に再起動がスケジュールされ、クリーンな状態が保証されます。この機能により、停止時の可用性がよりシームレスになり、顧客満足度が向上します。詳細については、ローカルホストキャッシュにおける1回限りの使用プールデスクトップを参照してください。

HDX 接続

HDX Direct - 内部

内部ユーザー向けのHDX Directが一般提供されるようになりました。これにより、直接通信が可能な場合、内部クライアントデバイスはセッションホストと安全な直接接続を確立できます。詳細については、HDX Directを参照してください。

グラフィック

インタラクティブ性の最適化

特定のユースケースにおいて、帯域幅よりもインタラクティブ性を優先するデフォルトの最適化を追加します。これにより、リアルタイムシナリオでの応答性が向上し、よりスムーズなユーザーエクスペリエンスが提供されます。デフォルトで有効になっているため、設定は不要です。

最大ビデオバッファサイズ設定

VDAバージョン2311以降では、最大ビデオバッファサイズ設定でキロバイト単位の任意の値をサポートするようになりました。設定されていない場合、または0に設定されている場合、デフォルトでは最大値はありません。VDA 2308以前では、範囲は128～4,194,303 KBで、デフォルトは65,536 KBのままです。Citrixは、HDXがセッションのニーズに基づいて必要なメモリを動的に割り当て、高解像度と複数のモニターをサポートするため、VDA 2311以降ではデフォルトのままにすることをお勧めします。詳細については、表示メモリ制限を参照してください。

Teamsおよびその他のプラットフォーム向けに最適化されたコンテンツ共有

この設定により、Citrix VCSDKを使用して、Microsoft Teams、Zoom、Webex、およびその他のビデオ会議プラットフォーム向けに最適化されたアプリケーションとデスクトップの共有を構成できます。Windows、Mac、Linux、およびVDA環境でのアプリとデスクトップの共有をサポートします。デフォルトでは、両方の共有オプションが有効になっており、カスタマイズできます。この設定はUCアプリケーションに固有のものであり、構成されている場合、VDA UseWsProviderレジストリキーを上書きします。詳細については、「Teamsおよびその他のプラットフォーム向けに最適化されたコンテンツ共有」を参照してください。

シームレスセッション向けに強化された起動アプリケーションのサポート

Citrix Virtual Apps and Desktops 2212以降では、シームレスアプリケーションがデスクトップセッションと同様にWindowsの起動アプリケーションを処理するようになりました。シェルラン

チャー (ShellAppRuntime.exe) は、OneDriveやMicrosoft Teamsなどのユーザーのプログラムをシームレスアプリと並行して起動し、セッション管理と起動の一貫性を向上させます。詳細については、「シームレスアプリケーションと起動アプリケーション」を参照してください。

マルチメディア

UI の視認性向上のため、HDX 最適化ウェブカメラの表示名を更新

HDX 最適化ウェブカメラの表示名が、「Citrix HDX Webcam - 」から「HDX - 」へと短いプレフィックスに変更され、UI ドロップダウンでの名前の切り捨てを防ぎます。USB リダイレクトされたウェブカメラは、現在の命名規則、つまり表示名にプレフィックスを含まず、単に「」を維持します。この更新は、ウェブカメラの名前を標準化し、VDA プラットフォーム全体での切り捨てを減らすことを目的としています。

仮想チャネルプラグインマネージャー

仮想チャネルプラグインマネージャーは、VDA 上のエンドユーザーがサードパーティアプリケーション（例：新しい Microsoft Teams）を起動したときにそれを検出し、そのVDIプラグインがエンドポイントにすでにインストールされているかどうかを確認し、インストールされていない場合はユーザーにプラグインのインストールを促すことができます。このプロンプトにより、エンドユーザーの許可を得てプラグインがダウンロードされ、自動的にインストールされます。

サポートされるアプリケーション: 新しい Microsoft Teams

詳細については、「仮想チャネルプラグインマネージャー」を参照してください。

デバイス

非Windowsクライアントプラットフォームでのスキャン – SANEリダイレクト

ChromeOSエンドポイント上のTWAINアプリケーションからドキュメントをスキャンできるようになりました。スキャン要求はローカルスキャナーにリダイレクトされ、スキャンが完了するとファイルはVDAに転送され、ChromeOSユーザーにシームレスな統合を提供します。詳細については、「非Windowsクライアントプラットフォームでのスキャン - SANEリダイレクト」を参照してください。

ウェブスタジオ

依存ポリシーの明確化

一部の設定は他の設定に依存しています。たとえば、子設定が構成されていても、その親設定が有効になっていない場合、構成された子設定は有効になりません。以前は、依存関係が明確ではありませんでした。このリリースから、子ポリシーを構成する前に最初に構成する必要がある親ポリシーが明確になりました。詳細については、「ポリシー設定」を参照してください。

複数選択ポリシー

複数のポリシーを選択できるようになり、以下の機能強化を確認できます。

- **ポリシー行をクリックする**: ポリシー行をクリックすると、上部のアクションバーに単一ポリシーのアクションが表示されます。下部の詳細ペインには、そのポリシーに関する情報が表示されます。
- **複数のポリシーのチェックボックスを選択する**: ステータスが有効または無効の複数のポリシーのチェックボックスを選択すると、上部のアクションバーに複数のポリシーのアクションが表示されます。下部の詳細ペインには、選択されたポリシーの数が表示されます。

> **注:**
>
> 複数のポリシーを選択した後、別の単一ポリシーの行をクリックすることで、その詳細を表示できます。この操作によって、以前に選択したポリシーがクリアされることはありません。ただし、右クリックアクションでは、そのポリシー行のアクションは表示されません。

Web Studioを使用したバックアップと復元

Web Studio で利用可能な**バックアップと復元**ノードを使用できるようになりました。この機能により、オンデマンドおよびスケジュールされたバックアップを作成し、削除されたアプリケーション、ポリシーなどを復元できます。詳細については、「Web Studio を使用したバックアップと復元」を参照してください。

Azure SQLのサポート

Citrix Virtual Apps and Desktops データベースを**Azure SQL Managed Instance**でホストできるようになりました。この機能をサポートするために、以下の UI を更新しました。

- **Citrix Site Manager**ウィザード: Azure SQL Managed Instance にデータベースを作成できます。

- **Settings**ページ (Web Studio): Azure SQL でホストされているデータベースの場所を変更できます。 詳細については、「データベースのセットアップ」および「データベースの場所の変更」を参照してください。

Studio ログインページのデフォルトドメイン名を設定する

Studio ログインページのドメインフィールドに自動入力されるドメイン名を構成できる機能が導入されました。この機能強化により、ログインプロセスが効率化され、入力エラーが減少します。詳細については、「デフォルトドメイン名の設定」を参照してください。

イメージ管理が一般提供開始になりました

イメージ管理機能が、AzureおよびVMware仮想化環境で一般提供されるようになりました。また、**Images**ノードを使用すると、AzureおよびVMware仮想化環境の同じホスティング接続内のホスティングユニット間でイメージバージョンを共有できるようになりました。この実装により、異なるホストユニット間でのイメージの一貫性と均一性が確保され、展開の柔軟性と運用効率が向上します。この目的を達成するために、PowerShellコマンドを使用することもできます。詳しくは、「イメージ管理」を参照してください。

Web Studioでのドメイン非参加VDAのプロビジョニングのサポート

この機能により、MCSは、お客様が管理するCitrix Virtual Apps and Desktops展開で、ドメイン非参加VMのプロビジョニングをサポートします。詳しくは、「ドメイン非参加マシンIDのIDプール」を参照してください。

Google Cloud PlatformのMachine Creation Services™ (MCS) カタログ作成後にライトバックキャッシュ設定を更新するオプション

Google Cloud PlatformのMCSカタログの場合、カタログ作成後に、Machine Creation Services (MCS) Storage Optimization (MCSIO) が有効になっているときに、ライトバックキャッシュのメモリとディスクキャッシュサイズを更新するオプションが利用できるようになりました。詳しくは、「Web Studioを使用してマシンカタログを作成する」を参照してください。

ハイブリッドAAD参加タイプのマシンをMicrosoft Intuneに登録して共同管理する

マシンカタログ作成時に、**ハイブリッドAAD参加**タイプのマシンをMicrosoft Intune (Configuration Managerを使用) に登録して共同管理できるようになりました。この機能は、シングルセッションおよびマルチセッション、永続的および非永続的VM、およびすべてのハイパーバイザーとクラウドサービスに適用され、インフラストラクチャ全体で統一されたデバイス管理を保証します。この機能は、VDAバージョン2407以降にのみ適用されます。詳しくは、「Microsoft Intuneに登録され

たハイブリッドAzure AD参加カタログ」および「Microsoft Intuneに登録されたハイブリッドAzure AD参加カタログを作成する」を参照してください。

Azure VMの複数NICサポート

Web Studioを使用すると、複数のNICを持つAzure VMを作成できるようになりました。VMの最大NIC数はマシンサイズ設定によって決定され、実際に許可されるNIC数はマシンプロファイル設定によって定義されます。詳しくは、「マシンカタログを作成する」を参照してください。

マスターイメージからDES設定を継承するAzureカタログのサポート

以前は、Web Studioはマシンプロファイルに基づいてのみAzureカタログのデフォルトのDES設定を行っていました。この機能強化により、マシンプロファイルが選択されていない場合、またはプロファイルがプラットフォーム管理キー (PMK) を指定している場合、Web Studioはマスターイメージに基づいてAzureカタログのデフォルトのDES設定を直接行います。詳しくは、「Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する」を参照してください。

FlexApp形式のパッケージアプリケーション配信のサポート

Web Studioを使用すると、FlexAppパッケージアプリケーションを展開にアップロードし、ユーザーに配信できるようになりました。詳しくは、「アプリパッケージ」を参照してください。

ファイルタイプ関連付けによるアプリケーション公開の強化

Web Studioでアプリケーションを公開するためのオプション「**ファイルタイプ関連付け**」を追加しました。この機能により、アプリケーションを公開する際に、そのファイル拡張子を指定および管理できます。

- ローカルアプリアクセスアプリケーションを追加すると、このオプションが左ペインに表示されます。
- デリバリーまたはアプリケーショングループにアプリケーションを追加すると、このオプションは、アプリケーションの**プロパティ**メニューからアクセスできます。

リモートPCアクセス カタログの電源管理接続を選択するサポート

以前は、Studioを使用して、リソースの場所にWake on LANホスト接続を作成できました（接続タイプとして**Remote PC Wake on LAN**を選択）。しかし、その接続をリモートPCアクセス カタログに関連付けるには、PowerShellが唯一の選択肢でした。現在では、Studioを使用してそれを実現できます。詳細については、「Studioを使用してWake on LANを構成する」を参照してください。

プロビジョニングプロセスのステータス表示のサポート

Web Studioでマシンカタログを作成する際、カタログのプロビジョニングプロセスのステータスを表示できるようになりました。プロビジョニングプロセスが現在どのステップにあるか、および完了までに残りのステップ数を確認できます。

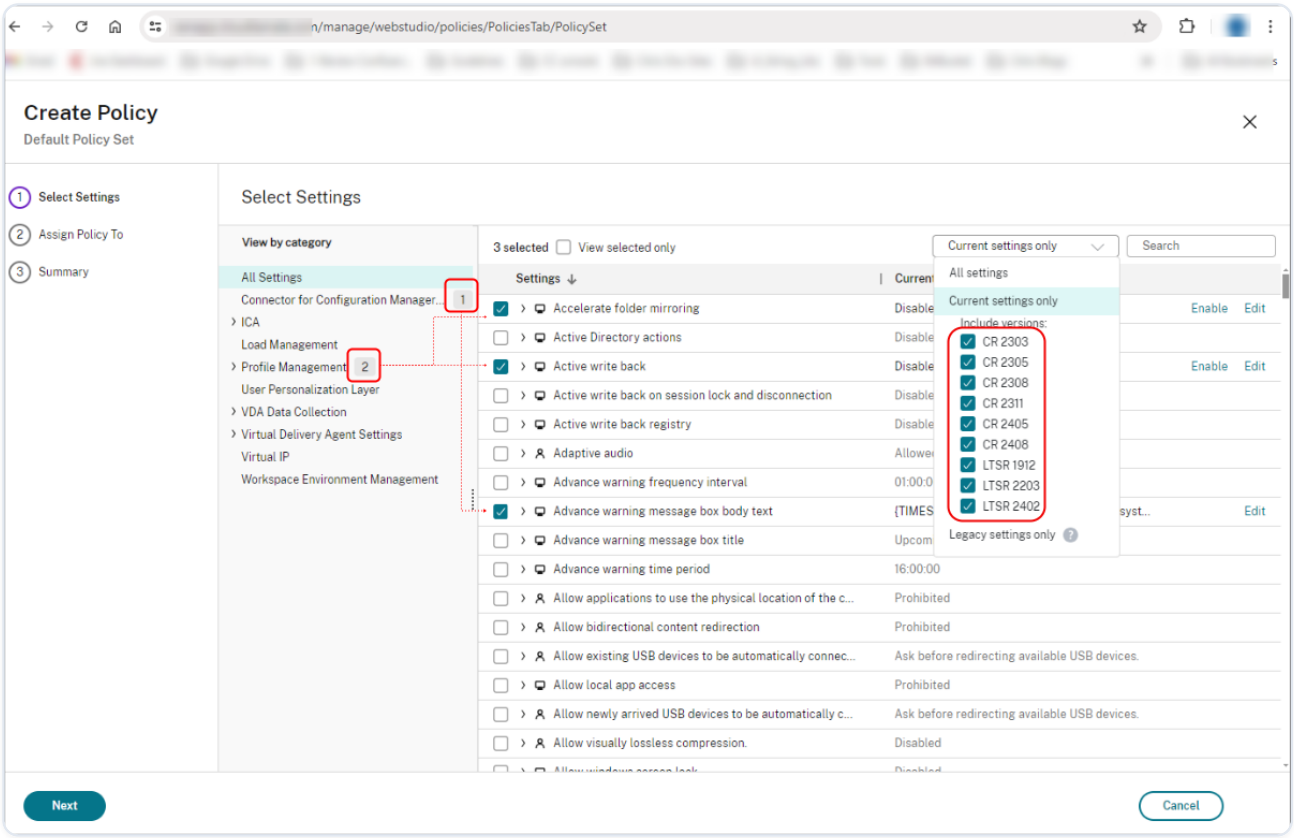
ポリシー情報で強化されたデリバリーグループの詳細ビュー

選択したグループに割り当てられたポリシーを表示する専用タブを追加することで、デリバリーグループの**詳細**ビューを強化しました。この改善により、関連するポリシー情報にすばやくアクセスできるようになり、デリバリーグループのポリシー管理、構成、トラブルシューティングが簡素化されます。

ユーザーエクスペリエンス向上のためのポリシー UI の改善

ポリシーノードのUIデザインを強化し、その全体的な使いやすさと機能を向上させました。詳細な改善点は次のとおりです。

- **作成および編集 UI の全画面表示。 ポリシー** ノードでの作成および編集エクスペリエンスを向上させ、より効率的にするために、全画面モードが使用されるようになりました。
- **設定フィルタリングの簡素化。 現在の設定のみ**フィルターの下に、サポートされているVDAバージョンのドロップダウンリストが利用可能になり、VDAバージョンに基づいて設定をフィルタリングできるようになりました。
- **設定の分類の強化。** 複数の設定を選択すると、選択された設定の数が左ペインの関連するカテゴリとサブカテゴリの横に表示されるようになりました。この改善により、選択された各設定がどのカテゴリとサブカテゴリに属するかをすばやく特定できるようになり、ポリシー管理が効率化されます。



プリンター構成エクスペリエンスの簡素化

Studioを強化し、プリンター構成をより簡単にしました。プリンターのUNCパスを入力するだけでなく、ネットワーク全体または指定されたプリンターサーバーでプリンターを検索できるようになりました。この機能強化により、プリンターを構成するためのより直感的で信頼性の高い方法が提供されます。さらに、プリンターサーバーでプリンターを検索する際に、ユーザー名とパスワード以外の資格情報を使用できる新しいオプションが追加されました。詳細については、デフォルトプリンター、プリンターの割り当て、およびセッションプリンターを参照してください。

エクスポート機能がすべての管理ノードに拡張されました

Web Studioの任意の管理ノードのメインビューからレコードをCSVファイルにエクスポートできるようになりました。次の点に注意してください。

- データ読み込み中は、**検索**ノードと**アプリケーション**ノードを除き、**エクスポート**アイコンは無効になります。
- **表示する列**機能を持つノードの場合、エクスポートされたデータには選択された列のみが含まれます。

マシンカタログ、デリバリーグループ、およびアプリケーションのデフォルト表示設定の強化

マシンカタログ、デリバリーグループ、およびアプリケーションに新しいデフォルト表示オプションを導入し、より高い柔軟性とカスタマイズ性を提供します。

- **デフォルトビューの選択。** 以前は、これらのノードはフォルダービューがデフォルトでしたが、これはフォルダーベースの管理構造を使用する組織に適していました。アクションバーに**フォルダー**アイコンが導入されたことで、フォルダービューとリストビューを切り替えて、好みのデフォルトビューとして設定できるようになりました。
- **改善されたフォルダービュー。** **すべて表示**トグルは、再サインイン時に前回の選択を保持するようになりました。以前にオフにされていた場合、ルートフォルダーが選択され、第1レベルのサブフォルダーが展開された状態でオフのままになります。

Web Studioノードの詳細タブのデータキャッシュ

Web Studioのすべての管理ノードの**詳細**タブにデータキャッシュを導入しました。この機能強化により、**詳細**タブのデータ読み込み時間が大幅に短縮され、全体的なユーザーエクスペリエンスが向上します。

メンテナンスモードのメモ追加のサポート

マシン、デリバリーグループ、または接続をメンテナンスモードにする際にメモを追加できるようになりました。これらのメモは、詳細ペインの**メンテナンス理由フィールド**に表示され、管理者や他のユーザーがメンテナンスの理由を理解するのに役立ちます。

シトリックス スタジオ

MMCベースのStudioの非推奨化

2411以降、MMCベースのStudioは非推奨となり、今後のリリースで削除されます。これは、新しい機能が追加されず、今後のアップデートは安定性とセキュリティにのみ焦点を当てることを意味します。MMCベースのStudioと同じ機能に加え、最新のインターフェイスと強化された機能を提供するWeb Studioへの移行をお勧めします。

Citrix Director (シトリックス ディレクター)

使用頻度の低い公開アプリと未使用の公開アプリのレポート

アプリケーションページでは、Citrix Workspace™アプリを介してアクセスされる公開済みアプリの詳細な使用状況情報が提供され、管理者はアプリの管理とリソースの割り当てを最適化できます。

この機能は、組織内のアプリケーション使用パターンを理解するのに役立ち、顧客がデータに基づいた意思決定を行い、Citrix展開をより効率的にするのに役立ちます。

> **注:**
>
> この機能は、プラチナライセンスサイトでのみ利用できます。

> 強化された「**アプリケーション**」ページには、以下の使用状況セクションが含まれています。

- **公開済みアプリの合計数：** 公開済みアプリの総数を識別します。
- **使用頻度の低いアプリ：** あまり使用されないアプリの保持または削除、リソース割り当ての最適化、およびライセンス管理について、情報に基づいた意思決定を行うのに役立ちます。このセクションには以下がリストされます。
  - **過去30日間のユニークユーザー数**
  - **合計起動回数**
  - **ピーク時の同時インスタンス数**
  - **トレンドチャート：** 時間経過に伴うユニークユーザー数を示すグラフを表示します。
- **未使用のアプリ:** 未使用のアプリを特定し、メモリ、構成リソースを解放し、ライセンス費用を節約するのに役立ちます。このセクションには、アプリの名前、対応するデリバリーグループ、およびアプリの状態が一覧表示されます。

エクスポートオプションを使用して、**最も使用頻度の低い**および**未使用の**セクションのデータをエクスポートすることもできます。

> **注:**

> 現在、公開されているアプリ（Citrix Workspaceアプリのデスクトップアプリ）のみがこの機能強化に含まれています。

> 強化されたアプリケーションページ(/en-us/citrix-virtual-apps-desktops/2411/media/application-monitoring.png)

詳細については、最も使用頻度の低いアプリと未使用の公開アプリのレポートのドキュメントを参照してください。

LTSR展開用Directorの独立リリース

LTSR展開向けのDirectorの独立したリリースにより、Citrix環境でのトラブルシューティングと監視を強化するための最新のDirector機能に、互換性のあるLTSR環境でアクセスするオプションが提供されるようになりました。この機能により、お客様は2402 LTSR展開で最新のDirectorバージョンを使用できます。また、LTSR発表後にリリースされた機能に、アプリケーション配信インフラストラクチャに影響を与えることなくアクセスできます。

スタンドアロンインストーラーには、Monitor サービス、Director サービス、および Monitor スナップインの最新の .msi が含まれています。これらの新しい .msi ファイルを使用すると、2402 LTSR CU1 を現在のリリース機能でアップグレードできます。

2402 LTSRリリース以降の現在のリリースに含まれるDirector機能については、以下を参照してください。

- シトリックス バーチャルアプリおよびデスクトップ 2407 リリース
- シトリックス バーチャルアプリおよびデスクトップ 2411 リリース

最小VDAバージョンのDirectorの特定の機能の詳細については、Directorバージョンマトリックスを参照してください。

主な考慮事項

- **ターゲットアップグレード:** Directorコンポーネントのみをアップグレードすることで、LTSR展開で最新機能にアクセスできます。
- **LTSRサポート:** 新しくアップグレードされたDirectorおよび監視サービスコンポーネントはLTSRサポートの対象外ですが、残りのLTSRインフラストラクチャは既存のサポートを維持します。
- **ロールバックオプション:** 必要に応じて、以前のDirectorバージョンにロールバックする柔軟性があります。

詳細については、「LTSR展開向けDirectorの独立リリース」を参照してください。

高度なアラートポリシーの機能強化

以前はインフラストラクチャポリシーとして知られていたインフラストラクチャ監視に関連するアラートは、高度なアラートポリシーの一部になりました。

選択したデータソースに基づいて、依存サービスを選択できます。Cloud Connector のアラートも作成できます。

> **注:**
>
> Provisioning Service および StoreFront™ 用に作成された既存のインフラストラクチャポリシーは、**高度なアラートポリシー**セクションに移行されます。

> 詳細については、「高度なアラートポリシー」を参照してください。

アラートの一括解除

この機能は、より高い柔軟性を提供し、アラート疲労を軽減することで、管理者向けのアラート管理プロセスを最適化することを目的としています。これにより、管理者は時間、種類、またはカテゴリ別にアラートを一括解除でき、特にメンテナンスモード中やハイパーバイザーおよびその他の環境からのアラートを処理する際に、アラートの管理が容易になります。

アラートの一括解除を許可することで、管理者はワークロードをより効率的に管理し、大量のアラートに圧倒されることを避けることができます。

詳細については、「アラートの一括解除」を参照してください。

PowerShell SDKを使用したWebhook構成

PowerShell SDKを使用したWebhook構成機能により、管理者はWebhookプロファイルの作成、変更、削除、および一覧表示を行うことができます。この機能は、ヘッダー、認証タイプ、コンテンツタイプ、ペイロード、およびWebhook URLの指定を可能にすることで、Webhook構成の柔軟性を提供します。

> **注:**

サポートされているペイロード形式はテキストであり、エンドユーザーはWebhookでテキストを有効にする必要があります。

詳細については、「PowerShell SDKを使用したWebhook構成」を参照してください。

ワークロードの適正化の改善

ワークロードの適正化（旧称：**インフラストラクチャの適正化**）タブに、パワーユーザーを識別するオプションが追加されました。この機能を使用すると、パワーユーザーの詳細をエクスポートできます。

注:

この機能は、シングルセッションOSデリバリーグループでのみ利用可能です。

データのエクスポートには、**ユーザー名**、**合計セッション数**、**平均セッション期間 (分)**、**CPU使用率のピーク (%)**、**メモリ使用率のピーク (%)** が含まれます。

この機能強化により、リソース使用率に関する貴重な洞察が得られ、ユーザーの行動に基づいた効率的なリソース割り当てを確保することで、インフラストラクチャコストの最適化に役立ちます。

詳細については、「ワークロードの適正化」ページを参照してください。

マシンの正味アクティブ使用量

ワークロードの適正化ページには、マシンの純アクティブ使用状況に関する詳細なインサイトが含まれるようになり、以下の詳細が提供されます。

- 正味アクティブ使用量の割合
- 平均マシン稼働時間
- セッションなしの時間
- アイドル時間
- 切断時間

この機能により、詳細なマシン使用状況情報を確認でき、それに応じてコストを最適化できます。

詳細については、「ワークロードの適正化」を参照してください。

ストレージ使用量を最適化することによるコスト削減

コスト削減ページで、マシンの電源がオフになったときにストレージの最適化によって達成された削減額が確認できるようになりました。以前は、コンピューティング関連のコスト削減のみが表示されていました。この機能強化には、次の2種類のストレージ削減が含まれます。

- ライトバックディスク：非永続マシンがシャットダウンされたときにライトバックディスクを削除することによる節約。
- OSディスク：いずれかのマシンがシャットダウンされたときに、OSディスクをPremiumからStandard HDDにダウングレードすることによる節約。

前提条件：

- コンピューティングコストを最適化するには、Autoscaleを有効にする必要があります。詳細については、「Autoscaleの概要」を参照してください。
- ストレージコストを最適化するには、VMがシャットダウンされたときにストレージタイプを下位層に変更します。詳細については、「VMがシャットダウンされたときにストレージタイプを下位層に変更する」ドキュメントを参照してください。
- この機能はAzureマシンにのみ適用されます。

この機能強化には、次のものが含まれます。

- マシンの電源オフ（Autoscale™またはユーザーによる開始）によるストレージ削減の詳細レポートが、**推定インフラストラクチャ削減**セクションで利用できるようになりました。
- 合計削減額の計算には、コンピューティングとストレージの両方の削減額が、ソース（Autoscaleまたはユーザーアクション）別に内訳されて含まれるようになりました。履歴トレンドグラフでは、コンピューティングとストレージの削減額が視覚的に区別され、ツールチップにホバーすると詳細が表示されます。
- 「**カタログの詳細**」セクションに「**1時間あたりのコンピューティングコスト**」と「**1時間あたりのストレージコスト**」が追加されました。

詳細については、コスト削減 [プレビュー]を参照してください。

コスト概要

コスト概要ページでは、Citrix環境の実行に関連する費用の包括的な概要が提供されます。この機能強化により、次の情報が可視化されます。

- ユーザーあたりの総コスト

- 選択されたワークロードプロバイダー、デスクトップの種類、およびVMシリーズセットによる仮想化提供のコスト

このページでは、以下を提供します。

- ユーザーに仮想化されたアプリまたはデスクトップを提供するコストに関するインサイト 節約された金額
- コストと節約に関する情報（以下で分類）
  - プラットフォームプロバイダー
  - OSの種類
  - デスクトップの種類
  - VMシリーズ

> **注：**
>
> **コスト概要**ページは、サイトが1か月に少なくとも15日間稼働している場合にのみ利用できます。

> 詳細については、コスト概要ページを参照してください。

コスト最適化ページからデータをエクスポートする

コスト最適化ページ上のデータは、データ統合およびODATAクエリを使用してエクスポートできます。データをエクスポートするには、以下のいずれかのオプションを使用できます。

- データ統合のセットアップ - コスト最適化データをMonitor Service APIと統合することで、問題のトラブルシューティングやトリアージのためにデータを収集できます。詳細については、統合とデータエクスポートページを参照してください。
- コスト最適化のためのODATAクエリ - **コスト最適化**ページで利用可能なサンプルODATAクエリを使用してデータをエクスポートできます。

詳細については、データのエクスポートを参照してください。

デリバリーコントローラー™ の監視

Delivery Controllerコンポーネントがインフラストラクチャ監視ダッシュボードに追加され、オンプレミス展開のためにCitrix Virtual Apps and Desktopsサイトに接続されると、デリバリーコントローラーは自動的にオンボーディングされます。

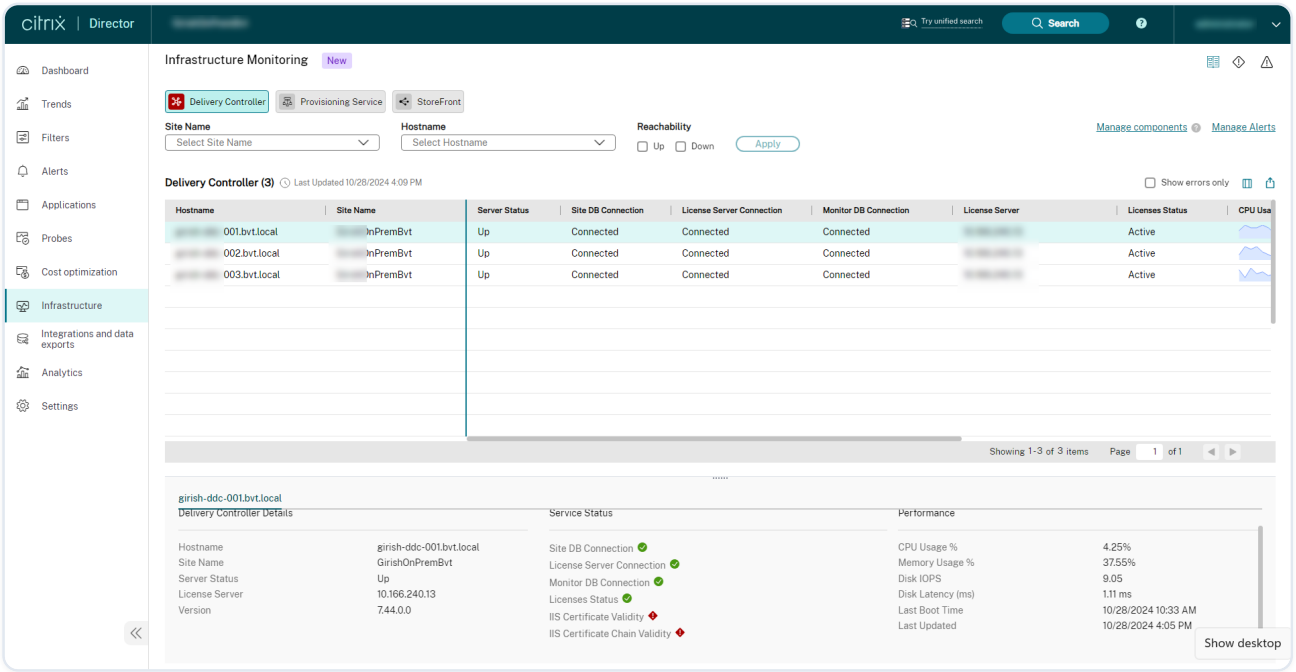
この機能により、管理者は単一のダッシュボードビューを使用してDelivery Controllerの健全性を監視し、プロアクティブにアラートを設定できます。

> **注：**
>
> Delivery Controllerを監視するために`CitrixInfraMonitor.msi`をインストールする必要はありません。

> **利点：**

- 包括的な監視: ライセンスサーバーや証明書の有効性など、Delivery Controllerの重要な健全性指標を可視化します。
- 設定可能なアラート: 関心のある健全性メトリックについてアラートを設定し、重要度を定義し、アラート設定に従って管理者が詳細なアラートを受信するためのスコープを定義できます。

Delivery Controller を監視するには、Director の タブをクリックします。 ページが開きます。



詳細については、デリバリーコントローラーの健全性メトリックを参照してください。

UI から Citrix コンポーネントを接続する

管理者は、Monitor UIを使用して、インフラストラクチャ監視のためにCitrixコンポーネントを登録できます。`Citrixinframonitor.msi`をインストールした後、UIベースのワークフローを使用し

て、PowerShellコマンドを使用せずに登録プロセスを完了できます。この機能強化により、Citrixコンポーネントの登録、登録解除、および更新のプロセスが簡素化されます。

新しい ページでは、Citrix コンポーネントと Citrix DaaS™ サイト間の接続を管理できます。このページでは、Provisioning Service、StoreFront、および Cloud Connector から利用可能な接続を表示することもできます。

> **注:**
>
> Delivery Controller は監視のために自動的にオンボーディングされます。

> これらの更新により、Citrix コンポーネントの管理と統合が合理化され、インフラストラクチャの保守とアップグレードが容易になります。

詳細については、接続の管理を参照してください。

ページの機能強化

トレンドページに、**コスト最適化**ページへの2つの新しいバナーが追加され、コスト削減情報とレポートへのアクセスが迅速になりました。**マシンの使用状況**タブには**推定節約額**と**節約レポート**へのリンクが含まれ、**リソース使用率**タブには**ワークロードの適正化**へのリンクが提供されています。これらの機能強化により、ナビゲーションが合理化され、可視性が向上し、ユーザーはコスト最適化のためのデータに基づいた意思決定を行うことができます。

詳細については、利用可能なトレンドページを参照してください。

パフォーマンスメトリックパネルの改善

パフォーマンスメトリックパネルでは、履歴データメトリックの視覚化が強化されました。**セッションパフォーマンス**タブをクリックすると、過去15分間のデータに加えて、ICARTTおよびICA®レイテンシーの過去48時間分のデータを表示できます。この機能強化により、セッションが過去48時間以内に終了した場合でも、管理者が問題をトリアージできるようになり、解決までの平均時間が短縮されます。 詳細については、パフォーマンスメトリックセクションを参照してください。

タブの更新

セッションパフォーマンスタブの**セッショントポロジ**セクションが拡張され、以下が含まれるようになりました。

- プロトコル - EDTプロトコルのMTU値を表示します。例: シングルストリーム: EDT (MTU = 1500) マルチストリーム: EDT (MTUストリームID 0=1500, 1=1500)
- Microsoft Teams - HDX最適化されているか、HDX最適化されていないかを表示します
- HDX接続タイプ - HDX接続タイプを表示します。例: HDX、HDX Direct、Rendezvous
- **1秒あたりのフレーム数**は、以下に関する情報を提供します。
  - 入力1秒あたりのフレーム数
  - 出力1秒あたりのフレーム数
- Windows版Citrix Workspaceアプリに存在するエンドポイントメトリック：
  - パブリックIPアドレス
  - インターネットサービスプロバイダー
  - 国や都市などの場所
  - Citrix Workspaceアプリセッションがネイティブアプリで開かれているか、ブラウザ (HTML5) で開かれているか
  - WorkspaceまたはStoreFrontを使用してアクセス
  - CPU %、メモリ %、GPU (全体 %) などのリソース使用率
  - ネットワーク遅延

この機能強化により、セッションの問題を迅速にトラブルシューティングできます。

詳細については、「セッションパフォーマンスメトリック」を参照してください。

フィルタータブの機能強化

このリリースでは、**セッション**タブに以下の追加フィルターが追加されました。

- **すべて** - すべてのセッションを表示します
- **アクティブ、接続済み、および切断済み** - アクティブ、接続済み、および切断済みのセッションのみを表示します。
- **終了済み** - 過去48時間以内に終了したセッションのみを表示します。 デフォルトのフィルターは**アクティブ、接続済み、および切断済み**です。

アラートと使いやすさに関するユーザーエクスペリエンスの改善

お客様からの機能強化リクエストに応え、最大負荷状態のマシンをエラーとして表示しないようにすることで、ユーザーエクスペリエンスが改善されました。この変更は、最大負荷が予想されるVertical Load Balancingを使用しているお客様にとって有益です。

この改善により、ダッシュボード、フィルター、トレンドページから最大負荷データが削除されます。最大負荷に達したマシンを表示するには、Monitor OData APIを使用してすべてのマシンのステータスを取得できます。Director UIを使用して、最大負荷状態のマシンを表示することもできます。

Director UIから最大負荷状態のマシンを表示するには：

1. **フィルター**タブに移動します。
2. デフォルトのフィルター - **すべてのマシン**を選択します。
3. 他のフィルターが適用されていないことを確認します。
4. **障害タイプ** で並べ替えます。

マシンをフィルターする(/en-us/citrix-virtual-apps-desktops/2411/media/filter-machines.png)

この機能により、最大負荷状態のマシンがエラーとして警告されることなく表示できるようになります。

終了したセッションの機能強化

終了したセッション（以前の履歴セッション）では、**セッションパフォーマンス**タブに過去48時間のデータが表示されます。また、終了したセッションの**セッションログオン**タブを表示できます。

詳細については、「終了したユーザーセッションの診断 [プレビュー]」を参照してください。

Secure Private Accessアプリのセッショントポロジビューに関する追加の詳細（プレビュー）

Secure Private Accessアプリの**セッショントポロジ**ビューで、以下の追加の詳細を表示できるようになりました。この変更は、WebアプリとSaaSアプリの両方、およびTCP/UDPアプリに適用されます。

エンドポイント:

- **エンドポイントの種類:** Secure Access AgentまたはCitrix Workspaceアプリのいずれかです。

- **アクセスの詳細:** エンドポイントがStoreFrontまたはCitrix Workspaceアプリのどちらを介してアクセスされるかを表示します。
- **エンドポイントOS:** 例: Windows。
- **場所のタイプ:** 場所が内部か外部かを示します。

リソースの場所:

> **注:**
>
> リソースの場所は、WebアプリとSaaSアプリにのみ適用されます。

- **列挙されたアプリケーションの数:** 列挙されたアプリケーションの数とストアのURLを表示します。
- **アクセス方法:** エンドポイントがStoreFrontまたはCitrix Workspaceアプリを介してアクセスされるかどうかを示します。

セキュアプライベートアクセス:

- **構成されたポリシー:** 構成されたポリシーの数を表示します。
- **FQDNプラグイン:** リクエストを処理したエージェントのFQDNを表示します。

WebおよびSaaSアプリ / クライアントサーバーアプリ (TCP/UDP):

- **アプリ名:** アプリの名前です。
- **トップレベルURL:** WebアプリまたはSaaSアプリの場合、公開されたアプリのURLが表示されます。TCP/UDPアプリの場合、アプリのプロトコルIPアドレスが表示されます。
- **アプリの種類:** アプリがWebアプリかSaaSアプリか、またはTCP/UDPアプリかを示します。
- **アプリの公開タイプ:** アプリが外部公開されているか内部公開されているかを示します。

詳細については、「Secure Private Accessアプリのセッショントポロジビュー」セクションを参照してください。

TCPまたはUDPアプリ向けに強化されたアクティビティマネージャー (プレビュー)

アクティビティマネージャーの**利用可能なアプリ**で、TCPまたはUDPアプリの列挙されたアプリケーションの詳細を表示できるようになりました。また、リソースURLとアクセスされたリソース

の種類 (TCPまたはUDP) も表示できます。この機能強化は、Secure Private Accessの問題のトラブルシューティングに役立ちます。

詳細については、「Secure Private Accessアプリのセッショントポロジビュー」セクションを参照してください。

スカウト

Scout は TraceLogging プロバイダーをサポートします

以前は、Scout は Windows パフォーマンスプロバイダーのみをサポートしており、これには追加のデコードファイルが必要で、同じプロバイダーの単一セッションからのセッションとイベントのみをトレースしていました。

このリリースでは、ScoutがTraceLoggingプロバイダーをサポートするようになりました。このプロバイダーは、追加のデコードファイルを必要とせず、同じプロバイダーに対して最大8つのトレースセッションからイベントを有効にして受信できます。この機能はデフォルトで有効になっています。

Scout 機能のコマンドラインインターフェイス

Scout の機能にコマンドラインインターフェイスを使用できるようになり、Scout UI を開かずに必要なログとデータを収集できます。この機能は、高度なユーザーがターゲットマシンまたはサイトのログまたはトレースプロセスをローカルまたはリモートで自動化するのに便利です。この機能はデフォルトで有効になっています。

次の機能にコマンドが追加されました。

- ヘルプ
- 診断情報の収集
- トレースの開始と停止
- セッションのリスト
- CDC の開始と停止

> **注:**
>
> リモートトレースセッションを実行する場合、新しいテレメトリバージョンが VDA と DDC の両方にインストールされている必要があります。Scout コマンドラインは Citrix Virtual

> Apps and Desktops バージョン 2411 からサポートされており、`TelemetryService` の以前のバージョンはこの機能をサポートしていないため、このインストールが必要です。

> 詳細については、「Scout 機能のコマンドラインインターフェイス」を参照してください。

マシン作成サービス (MCS)

Azure での事前フォーマット済み WBC ディスクカタログ作成のサポート

この機能により、Azure 仮想化環境で、新しく作成されたカタログに事前フォーマット済みの WBC ディスクを利用できます。この操作により、MCS または MCS プロビジョニングされた Citrix Provisioning™ マシンカタログの各 VM を起動するのに必要な時間が大幅に短縮されます。この機能を実装するには、WBC を有効にした Azure カタログを作成し、追加のカスタムプロパティ `PreformatWriteBackCache` を `True` として含めます。

既存のカタログは、`Set-ProvScheme` コマンドを使用して WBC ディスクサイズを更新できます。

この機能は、MCS がマスタリングフェーズをプロビジョニングワークフロー全体から分離するイメージ管理ワークフローと互換性があります。詳細については、「事前フォーマット済み WBC ディスクカタログの作成」を参照してください。

MCS プロビジョニングされた Citrix Provisioning カタログのシャットダウン時に WBC ディスクを削除する

この機能により、Azure の MCS プロビジョニングされた Citrix Provisioning カタログで、シャットダウン時にライトバックキャッシュ (WBC) ディスクを削除するオプションが提供されます。この実装は、永続的な WBC ディスクが不要な場合にコストを節約するのに役立ちます。この機能は既存のカタログにも適用できます。詳細については、「MCS プロビジョニングされた Citrix Provisioning カタログのシャットダウン時に WBC ディスクを削除する」を参照してください。

GCP でのディスクのマルチリージョン スナップショットまたはディスクのイメージをマスターイメージとして使用するサポート

GCP のディスクのスナップショットまたはイメージは、リージョンまたはマルチリージョンにすることができます。リージョンスナップショットとディスクイメージは特定のリージョン (例: `us-central1`) に関連付けられますが、マルチリージョンスナップショットとディスクイメージは地理的な場所 (例: `US`) に関連付けられます。この機能により、GCP で MCS マシンカタログを

作成する際に、OS ディスクのマルチリージョンスナップショットまたはディスクのイメージをマスターイメージ入力として使用できます。ホスティングユニットのインベントリパスの下にある `snapshots.folder` の場所で、すべてのスナップショット (リージョンとマルチリージョンの両方) のリストを、`images.folder` の下でディスクイメージ (リージョンとマルチリージョンの両方) のリストを確認できます。

MCS で作成された AWS VM インスタンスに対する NitroTPM および UEFI セキュアブート機能のサポート

この機能により、AWS 環境でカタログを作成する際に、NitroTPM および/または UEFI セキュアブートが有効なマスターイメージ (AMI) を選択できるようになりました。これにより、カタログ内のプロビジョニングされた VM も NitroTPM および/または UEFI セキュアブートが有効になります。この実装により、VM のセキュリティと信頼性が確保されます。NitroTPM および UEFI セキュアブートの詳細については、AWS ドキュメント を参照してください。NitroTPM および UEFI セキュアブートが有効なカタログの作成については、「VM インスタンスの NitroTPM および UEFI セキュアブートを有効にする」を参照してください。

ネットワークセキュリティグループの作成のサポート

この機能により、Citrix にネットワークセキュリティグループの自動作成と変更を要求する代わりに、イメージ準備用の **Deny-All** ネットワークセキュリティグループを自分で作成できるようになりました。PowerShell コマンド Set-Item を使用してホスティングユニットのカスタムプロパティを編集し、`NsgForPreparation` パラメーターを含めて Deny-All ネットワークセキュリティグループを指定します。PowerShell コマンドの使用方法の詳細については、「事前作成されたネットワークセキュリティグループを使用する」を参照してください。

既存の MCS マシンカタログで Azure 一時ディスクを WBC ディスクとして使用するサポート

この機能により、既存の MCS マシンカタログおよび既存の VM で、Azure 一時ディスクをライトバックキャッシュ (WBC) ディスクとして使用できるようになりました。既存のカタログを更新するには、`Set-ProvSchem` PowerShell コマンドを使用します。Azure 一時ディスクは無料であるため、この実装によりストレージコストが節約されます。手順については、「既存のカタログと VM の WBC ディスクとして一時ディスクを使用する」を参照してください。

空のリソースグループをフィルタリングする

この機能を使用すると、マシンカタログ作成時にマスターイメージ、マシンプロファイル、または準備済みイメージを選択する際に、空のリソースグループを除外できます。これはPowerShellコ

マンド `Get-HypInventoryItem` を使用して実行できます。詳細については、空のリソースグループをフィルタリングする を参照してください。

XenServer®における永続VMおよび非永続VMの移行

この機能により、XenServer環境で、`Move-ProvVMDisk` PowerShellコマンドを使用して、以下のVMディスクをあるストレージから別のストレージに移行できます。

- 永続的なフルクローンVMの場合: OSディスク、IDディスク、および非MCSプロビジョニングディスク。
- 非永続VMの場合: OSディスク、IDディスク、およびライトバックキャッシュ (WBC) ディスク。

詳細については、永続VMおよび非永続VMのストレージ移行 を参照してください。

AWS環境でMCSマシンカタログを作成する前に構成を検証する

この機能を使用すると、`New-ProvScheme` コマンドの `-validate` パラメータを使用して、MCSマシンカタログを作成する前に構成設定を検証できるようになりました。このPowerShellコマンドをパラメータ付きで実行すると、誤ったパラメータが使用された場合や、あるパラメータが別のパラメータと競合する場合に、適切なエラーメッセージが表示されます。その後、エラーメッセージを使用して問題を解決し、PowerShellを使用してMCSマシンカタログを正常に作成できます。

現在、この機能はAWS、Azure、GCP、およびVMwareの仮想化環境に適用できます。詳細については、MCSマシンカタログを作成する前に構成を検証する を参照してください。

SCVMMにおけるアクティブなコンピューターアカウントのID情報を修復する

SCVMM環境では、ID関連の問題があるアクティブなコンピューターアカウントのID情報をリセットできるようになりました。マシンパスワードと信頼キーのみをリセットするか、IDディスクのすべての構成をリセットするかを選択できます。この実装は、永続および非永続MCSマシンカタログの両方に適用できます。現在、この機能はAWS、Azure、SCVMM、およびVMwareの仮想化環境でのみサポートされています。詳細については、アクティブなコンピューターアカウントのID情報を修復する を参照してください。

Azureにおけるオンデマンド容量予約のサポート

この機能を使用すると、マシンプロファイル（VMまたはテンプレート仕様）を使用して、オンデマンド容量予約付きのAzure VMのMCSマシンカタログを作成できます。この機能は、永続および

非永続マシンカタログに適用できます。既存のマシンカタログと既存のVMを更新して、オンデマンド容量予約を設定または削除できます。

Azureのオンデマンド容量予約の詳細については、Microsoftのドキュメントオンデマンド容量予約を参照してください。オンデマンド容量予約付きのMCSマシンカタログの作成と更新については、オンデマンド容量予約VMのカタログを作成する を参照してください。

WBCディスクをOSディスクと同じストレージ場所に配置するサポート

XenServer、VMware、およびSCVMM仮想化環境では、ホスト接続の作成時に利用可能なOSストレージリストを利用可能な一時ストレージリストと同じように構成すると、MCSはライトバックキャッシュ（WBC）ディスクをOSディスクと同じストレージ場所に配置するようになりました。

この実装により、OSディスクとWBCディスクの管理の複雑さを軽減できます。

ホスト接続の作成については、「接続とリソースの作成」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/connections)を参照してください。

Azure上のVMごとの複数NICのサポート

以前は、Azure環境では、MCSはVMごとに1つのネットワークインターフェースカード（NIC）のみをサポートしていました。この機能により、MCSはVMごとに複数のNICをサポートするようになりました。VM上の複数のNICを複数のサブネットに関連付けることができますが、それらのサブネットは同じ仮想ネットワーク（vNet）内にある必要があります。詳細については、「VMごとに複数のNICを持つカタログを作成または更新する」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure#create-or-update-a-catalog-with-multiple-nics-per-vm)を参照してください。

Azure Sovereign Airgapクラウド環境に接続する

この機能により、ホスト接続の作成時にカスタムプロパティ`DisableInstanceDiscovery`を使用してAzure Sovereign Airgapクラウド環境に接続できます。Azure Sovereign Airgapクラウド環境は、分離されたネットワークドメイン上にある必要がある極秘のワークロードに適しています。この環境へのホスト接続の作成の詳細については、「Azure Sovereign Airgapクラウド環境への接続」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/connections/connection-azure-resource-manager#connect-to-azure-sovereign-airgap-cloud-environment)を参照してください。

休止状態のVMの再起動スケジュール

この機能により、デリバリーグループで休止状態が有効になっている場合、休止状態のVMの再起動スケジュールを構成できます。再起動サイクルでは、VMは再開され、その後シャットダウンされます。再起動スケジュールは、毎週、毎日、毎月、および1回に設定できます。複数のスケ

ジュールを構成できます。休止状態から再開するVMには数分かかる場合があることに注意してください。

プロファイル管理

新機能については、別のドキュメントの「新機能」を参照してください。

シトリックス プロビジョニング

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

macOS 用 Citrix バーチャル デリバリー エージェント

新機能については、別のドキュメントの 新機能 の記事を参照してください。

リナックス ブイディーエー

新機能については、独自のドキュメントにある新機能の記事を参照してください。

セッションレコーディング

新機能については、独自のドキュメントにある新機能の記事を参照してください。

ワークスペース環境管理™

新機能については、独自のドキュメントにある新機能の記事を参照してください。

フェデレーション認証サービス

新機能については、独自のドキュメントにある新機能の記事を参照してください。

修正された問題

Citrix Virtual Apps and Desktops™ 7 2411 には、以下の修正された問題が含まれています。

全般

- Day 0 統合を実行し、データベースを構成しようとすると、手動モードから自動モードに切り替えた後、警告ポップアップ内のテキストが表示されません。警告アイコンにカーソルを合わせるとメッセージが表示されます。
- VDAWorkstationSetup_2402、VDAServerSetup_2402、または VDAWorkstationCoreSetup_2402パッケージを使用してCitrix Rendezvous V2をインストールすると、これらのパッケージにCitrix.Diagnostics.Tracing.dllファイルがないため、インストールが失敗する可能性があります。
- シングルサインオンに拡張ドメインパススルーを使用する場合、クライアントデバイスまたはセッションホストがWindows 11を実行していると、セッションへのSSOが失敗する可能性があります。
- 無効なポリシー設定でサイトがアップグレードされると、ポリシーデータが失われる可能性があります。この問題が発生した場合は、Citrixサポートポータルを使用してテクニカルサポートケースをオープンしてください。
- Citrixは、Citrixが生成したバイナリとサードパーティのバイナリの両方に署名します。これは、バイナリがCitrixによって認証されることを意味します。サードパーティのバイナリのバージョンは、サードパーティから調達されたものと同じままです。バイナリがすでにインストールされている場合、バージョンが一致するため、VDAアップグレードではバイナリはインストールされません。
- クライアントからICA®セッションへの100MBを超えるデータのクリップボードコピー＆ペーストが失敗する場合があります。大容量バッファのコピーはサポートされていません。
- 特定のシナリオで、クライアントIPポリシーフィルターを使用すると、ポリシーの評価に使用されるIPアドレスが正しくありません。

グラフィック

- Theora圧縮を使用して64ビットのウェブカメラアプリでビデオプレビューを開始すると、セッションがクラッシュする可能性があります。

印刷

- 仮想デスクトップで選択されたUniversal Print Serverプリンターは、コントロールパネルの**デバイスとプリンター**ウィンドウに表示されません。ただし、ユーザーがアプリケーションで作業している場合、それらのプリンターを使用できます。この問題はWindows 10でのみ発生します。詳細については、CTX213540を参照してください。
- 印刷ダイアログウィンドウでデフォルトプリンターが正しくマークされない場合があります。この問題は、デフォルトプリンターに送信される印刷ジョブには影響しません。

- Universal Print Servers への SSL 接続が有効になっている場合、ロードバランスされたネットワークプリンターからの印刷ジョブの一部が失敗する場合があります。これは、印刷ジョブが次々と高速に実行されたときに発生します。
- セッションホストに FSLogix 2201 HF1 がインストールされている場合、セッションの起動時に黒い画面が表示されることがあります。この問題に対処するには、FSLogix を新しいバージョンにアップグレードする必要があります。

スタジオ

- ディスクに CMEK を使用して Google Cloud 用の Web Studio でカタログを編集する際、ウィザードのステップをスキップすると、将来的にマシンを追加する際に失敗する可能性があります。この問題を回避するには、ウィザードのすべてのステップをスキップせずに完了するか、PowerShell SDK を使用して操作を実行してください。

既知の問題

Citrix Virtual Apps and Desktops™ 7 2411 には、以下の既知の問題が含まれています。

注

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

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

全般

- Citrix Virtual Apps and Desktops バージョン 2411 では、Azure Arc Onboarding はサポートされていません。
- 以前の Citrix Virtual Apps and Desktops バージョンからバージョン 2411 にアップグレードする場合、またはバージョン 2411 に新しいサイトを展開する場合、SQL Server 2016 データベースを使用するとサイト作成が失敗します。この問題により、インストールとセットアップ

が正常に完了せず、Citrix Virtual Apps and Desktops の最新バージョンへの移行または展開が妨げられます。

- Windows Server 2025 を実行しているマシンに Citrix Virtual Apps and Desktops コンポーネントをインストールするためにメタインストーラーを使用すると、`MsiInstall` イベントがイベントログに書き込まれません。
- アプリバーを起動してから、Windows 向け Citrix Workspace™ アプリで接続センターメニューを開くと、アプリバーがホストサーバーの下に表示されません。
- Windows 向け Citrix Workspace アプリを使用し、アプリバーを垂直位置で起動すると、バーがスタートメニューまたはシステムクロックトレイを覆います。
- ユーザーがホスト上で既にフォーカスされているコンボボックスを選択すると、コンボボックスが正しく表示されない場合があります。回避策として、別の UI 要素を選択してからコンボボックスを選択してください。
- Windows 10 から Windows 11 へのインプレース OS アップグレードを実行した後、Citrix Desktop Service が起動しない場合があります。この問題を解決するには、マシンを再起動してください。
- Windows Server 2022、Windows 10 Enterprise multi-session、および Windows 11 Enterprise multi-session を実行しているセッションホストでは、マルチセッション VDA の **セッション制限** 設定が拒否されます。 回避策として、GPO を介して **RDS セッション時間制限** を構成できます。
- Microsoft は、Modern Print Dialog を使用している場合に印刷ジョブ間で印刷設定が保持されない問題があることを確認しており、現在その問題に対処しています。現在の予測では、2025 年上半期に解決される予定です。Modern Print Dialog は、Windows 11 や Windows Server 2025 などの新しい OS バージョンでデフォルトで有効になっています。以下の手順を実行することで、OS をレガシー印刷ダイアログを使用するように構成できます。

1. レジストリエディターを開きます
2. HKEY_CURRENT_USER\Software\Microsoft\Print\UnifiedPrintDialog に移動します
3. 右クリックして、新規 > DWORD (32 ビット) 値 を選択します
4. 値を PreferLegacyPrintDialog に名前変更します
5. PreferLegacyPrintDialog を右クリックして、修正 を選択します
6. 値のデータを 1 に設定し、OK をクリックします

- 管理者権限でアプリケーションを実行している場合、FIDO2 に関連付けられた Windows セキュリティダイアログボックスは ICA® セッションウィンドウの前面に表示されません。これは、昇格されたプロセスとして実行されている場合、Windows セキュリティダイアログボッ

クスが ICA セッションウィンドウの背後に隠れるというオペレーティングシステムの設計によるものです。

- Windows 10 または Windows 11 Multi-session OS は Windows システムの復元をサポートしていません。そのため、UI で復元ポイントを作成するオプションは利用できません。コマンドラインオプション `/EnableRestore` または `/EnableRestoreCleanup` は無視され、「Windows 10/11 Multi Session OS では **システムの復元を無効にする** は現在サポートされていません」というメッセージがログに記録されます。
- CVAD 2411 では、Desktop Viewer ツールバーの **接続強度インジケーター** (CSI) が正しいプロトコル情報を表示しません。代わりに、CSI の詳細ではプロトコルが **N/A** と表示されます。
- 任意のポリシー設定の更新とサイトサービスでの BLOB の生成との間に 5 分の遅延があります。その結果、ポリシーがセッションに反映されるまでに時間がかかる場合があります。
- RemotePC ユーザーは、HDX セッション内で Zoom や Microsoft Teams などのビデオ会議アプリケーションを起動する際にクラッシュを経験する可能性があります。

オーディオ

シングルセッション VDA で実行されている一部のサードパーティアプリケーション (例: Zoom アプリまたは Teams アプリ) では、ICA セッションの切断、再接続、またはハードリセット後に、オーディオデバイス名がサードパーティアプリケーションで適切に更新されません。

回避策として、サードパーティ製アプリケーションを再起動すると、オーディオデバイス名が期待どおりに更新されます。

ウェブスタジオ

- 現在、サイトデータベースをローカルのSQL ServerからAzure SQLに移行することはサポートされていません。推奨されるアプローチは、Azure Databaseで新しいサイトを作成し、サイト移行にはCitrix Automated Configuration Toolなどのツールを使用することです。

ウェブスタジオによるセキュアプライベートアクセス

- ユーザーが「概要」タブ > 「ライセンスサーバーURLの追加」リンクから「設定」 > 「統合」ページにリダイレクトされると、ナビゲーションバーが部分的に表示されます。ページを更新すると、ナビゲーションバーが表示されます。
- 不正確なゲートウェイURLが入力されると、空白の警告ポップアップが表示されます。警告アイコンにカーソルを合わせると、警告メッセージが表示されます。
- コンソールのすべてのタブで垂直スクロールバーが部分的に表示されます。この問題に対する回避策は不要であり、機能やユーザーエクスペリエンスに影響はありません。

- **設定 > 統合**タブで、ブラウザウィンドウが小さい場合、ページ下部に水平スクロールバーが表示されません。ブラウザウィンドウが最大化されている場合、水平スクロールバーは不要です。
- **トラブルシューティング**ログで、ログ詳細ダイアログボックスが開いているときに、ページ下部に垂直スクロールバーが表示されません。この問題に対する回避策は不要であり、機能やユーザーエクスペリエンスに影響はありません。
- Secure Private Accessコンソールにログインするとき、またはWSに戻ってSecure Private Accessコンソールに戻るときに、**概要**タブが強調表示されません。この問題に対する回避策は不要であり、機能やユーザーエクスペリエンスに影響はありません。
- **設定 > 統合**タブで、エラーメッセージがダイアログボックスの手前ではなく、その背後に表示されます。この問題に対する回避策は不要であり、機能やユーザーエクスペリエンスに影響はありません。

注:

上記のすべての問題は、Web StudioからSecure Private Accessにアクセスした場合にのみ発生します。スタンドアロンのSecure Private Accessにアクセスした場合は適用されません。

グラフィック

- Skype for desktopアプリで、リモートデスクトップに接続されている余分なWebカメラに気づくかもしれません。これらの余分なWebカメラのプレビューはブロックされ、セキュリティ上の理由から黒い画面が表示される場合があります。余分なWebカメラは無視し、エンドポイント用のWebカメラを引き続き使用できます。

ディレクター

- Director OData API を介して `MonthlyCostSummaries` の OData V4 または V3 リクエストを開始すると、500 内部エラーが発生する場合があります。回避策として、Director UI の **Trends** > **Custom Reports** > **OData query** セクションから OData クエリを使用してください。

マシン作成サービス™

- AWS でホストされている VMware 環境では、マスターイメージで vTPM が有効になっている場合、MCS マシンカタログの作成が失敗します。この問題は、すべての Citrix Virtual Apps and Desktops バージョンに影響し、VMware 環境の問題が原因です。サポートについては、VMware support にお問い合わせください。

サードパーティの問題

- Chromeは、ウェブページ周辺のツールバー、タブ、メニュー、ボタンに対してのみUIオートメーションをサポートします。このChromeの問題により、タッチデバイス上のChromeブラウザでは、自動キーボード表示機能が動作しない場合があります。回避策として、`chrome --force-renderer-accessibility`を実行するか、新しいブラウザタブを開いて`chrome://accessibility`と入力し、特定のページまたはすべてのページで**Native accessibility API**のサポートを有効にすることができます。さらに、シームレスアプリを公開する際、`--force-renderer-accessibility`スイッチを使用してChromeを公開できます。

プロファイル管理

- Profile Management 2411 documentation には、このリリースでの更新に関する具体的な情報が記載されています。

リナックス VDA

- Linux VDA 2411 documentation には、このリリースでの更新に関する具体的な情報が記載されています。

セッション録画

- Session Recording 2411 documentation には、このリリースでの更新に関する具体的な情報が記載されています。

ワークスペース環境管理™

- Workspace Environment Management 2411 documentation には、このリリースでの更新に関する具体的な情報が記載されています。

シトリックス プロビジョニング™

- Citrix Provisioning 2411 documentation は、このリリースの更新に関する特定の情報を提供します。

フェデレーション認証サービス

- Federated Authentication Service 2411 documentation は、このリリースの更新に関する特定の情報を提供します。

廃止予定

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

非推奨および削除

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

非推奨

非推奨とは、将来のリリースからその機能または機能を削除する予定であることを意味します。その機能または機能は、正式に削除されるまで引き続き動作し、完全にサポートされます。この非推奨通知は、数か月から数年にわたる場合があります。削除後、その機能または機能は動作しなくなります。この通知は、機能または機能が削除される前に、お客様が計画を立ててコードを更新するのに十分な時間を与えるためのものです。非推奨の項目については、可能な限り代替案が提案されます。

項目	非推奨が発表されたバージョン	代替
ファイルベースのライセンス	2507	ライセンスアクティベーションサービス (LAS) は、Citrix製品スイート全体で製品アクティベーションを行う次世代テクノロジーです。ファイルベースのライセンスを使用しているお客様は、互換性のあるリリースにアップグレードし、このテクノロジー移行を April 15, 2026 までに

項目	非推奨が発表されたバージョン	代替
		実行する必要があります。LASは、April 15, 2026 以降、Citrixオンプレミスコンポーネントをアクティベートおよびライセンス供与する唯一の方法となります。
3D HDXグラフィックポリシーの最適化	2411	圧縮にビデオコーデックを使用する設定を「画面全体」に設定します。`<https://docs.citrix.com/ja-jp/citrix-virtual-apps-desktops/2411/policies/reference/ica-policy-settings/graphics-policy-settings.html#use-video-codec-for-compression>`を参照してください。
NVIDIA GPU ハードウェアエンコーディング (NVENC) (vGPU 15以前、およびドライバーバージョン529.19以前を使用).	2411	現在サポートされているNVIDIAドライバーを使用してください: vGPU 16以降、およびドライバーバージョン536.22以降。詳細については、NVIDIAがサポートするvGPUおよびドライバーバージョンに関する`<https://`

項目	非推奨が発表されたバージョン	代替
		`docs.nvidia.com/vgpu/index.html#driver-versions>`を参照してください。
以下の`-AcctADAccount` PowerShellコマンドのサポート • New-AcctADAccount • Add-AcctADAccount • Update-AcctADAccount • Remove-AcctADAccount コマンドレット • Unlock-AcctADAccount コマンドレット • Get-AcctADAccount	2411	-AcctIdentity PowerShellコマンドを使用します • New-AcctIdentity • Add-AcctIdentity • Update-AcctIdentity • Remove-AcctIdentity コマンドレット • Unlock-AcctIdentity コマンドレット • Get-AcctIdentity
`-ResetIdentityInfo` PowerShellコマンドのサポート	2411	`-Recreate`を使用してIDディスクを再作成します。詳細については、「アクティブなコンピューターアカウントのID情報を修復する」を参照してください。

項目	非推奨が発表されたバージョン	代替
MMCベースのStudio	2411	Web Studioを使用してください。
複数モニターフック	2407	-
ドメインパススルー認証	2407	シングルサインオンには、(/ja-jp/citrix-workspace-app-for-windows/domain-passthrough-for-single-sign-on)を使用してください。
ランデブー V1	2402	Rendezvous V2を使用してください。
セキュア ICA®	2402	-
Windows Server 2016でのVDAサポート	2402	最新のWindows Serverバージョンにアップグレードしてください。
Windows Server 2016でのDelivery Controller™、Web Studio、Citrix Director、Citrix License Server、Citrix StoreFront、シングルセッションOS用サーバーVDI、マルチセッションOS用VDA、Active Directoryフォレストおよびドメイン、Universal Print Serverのサポート	2402	最新バージョンのWindows Serverにアップグレードしてください。

項目	非推奨が発表されたバージョン	代替
サイト構成、構成ログ、および監視データベース用のMicrosoft SQL Serverバージョン2016および2017のサポート	2402	最新バージョンのMicrosoft SQL Serverにアップグレードしてください。
オンデマンドプロビジョニング機能より前に作成されたAzureカタログ（「レガシー」カタログ）のサポート	2402	AzureレガシーカタログVMを再作成します。カタログはオンデマンドとしてプロビジョニングされ、ストレージコストを節約できます。
ターゲット最小フレームレートポリシー	2311	**グラフィックステータスインジケーター**を使用して、ターゲット最小フレームレートを変更します。
システムセンターコンフィギュレーションマネージャー用Citrixコネクタ3.1のサポート	2311	イメージまたはアプリケーションの更新を手動で行います。
カタログが作成されたリージョンとは異なるリージョンでマスターイメージを使用するためのサポート	2311	Azure Compute Gallery を使用して、マスターイメージを目的のリージョンにレプリケートします。
HDX Graphics ディスプレイメモリ制限設定	2311	クライアントのディスプレイレイアウトが完全に収容されるように、必要な最小

項目	非推奨が発表されたバージョン	代替
		限のメモリが割り当てられます。
HDX Graphics におけるプログレッシブモードのサポート	2311	Thinwire を使用します。「プログレッシブモード」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2411/policies/reference/hdx-registry-settings#progressive-mode).
Internet Explorer 11 におけるブラウザコンテンツリダイレクトのサポート	2311	Google Chrome ベースのブラウザコンテンツリダイレクトを使用します。
AWS ボリュームワーカーのサポートを削除しました	2311	ダイレクトディスクのアップロードとダウンロードを使用します。「ダイレクトディスクのアップロードとダウンロード」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/connections/connection-aws#direct-disk-upload-and-download).
BrokerでのSQL Server 2016のサポート	2308	最新バージョンを使用してください。詳細については、「シ

項目	非推奨が発表されたバージョン	代替
		ステム要件」を参照してください。
DirectorでのXenApp 5.xのサポート	2308	---
DirectorでのXenApp 6.xのサポート	2308	---
Directorでのアラート用SCOMパック	2308	---
Directorでのプラグインのサポート	2308	---
WebRTC SDP形式 (Plan B) のサポート	2308	Citrix Workspace™ Appをサポートされているバージョンにアップグレードしてください。
Microsoft Teams最適化におけるシングルウィンドウモードのサポート	2308	Citrix Workspace Appをマルチウィンドウモードをサポートするバージョンにアップグレードしてください。詳細については、機能マトリックスとバージョンサポートを参照してください。
AWS環境で使用される `AwsCaptureInstanceProperties` のサポート	2308	マシンプロファイルを使用してください。マシンプロファイルを使用したカタログの作成を参照してください。

項目	非推奨が発表されたバージョン	代替
`Schedule-ProvVMUpdate` PowerShellコマンド	2305	`Set-ProvVMUpdateTimeWindow` を使用してください。
`Request-ProvVMUpdate` PowerShellコマンド	2305	`Set-ProvVMUpdateTimeWindow` を `-StartsNow` および `-DurationInMinutes -1` パラメーターとともに使用してください。
`Cancel-ProvVMUpdate` PowerShell コマンド	2305	`Clear-ProvVMUpdateTimeWindow` を使用してください。
`New-ProvScheme` コマンドで使用される `DedicatedTenancy` パラメーター	2303	`TenancyType` パラメーターを使用してください。
ライセンスサーバー VPX	2206	---
Azure 環境で VM をプロビジョニングするためのアンマネージドディスク。	2206	マネージドディスクを使用。
ホストからクライアントへの (URL) リダイレクト	2203	双方向コンテンツリダイレクト。
Cloud およびオンプレミス環境で使用さ	2203	---

項目	非推奨が発表されたバージョン	代替
れる、AWS 固有の4つのコマンドのサポート: `Revoke-HypSecurityGroupIngress`, `Revoke-HypSecurityGroupEgress`, `Grant-HypSecuritygroupegress`, および `Grant-HypSecurityGroupIngress`。		
VDAメタインストーラーからのCitrix Files for WindowsおよびCitrix Files for Outlook。	2203	スタンドアロンインストーラーを使用してください。
VDAメタインストーラーからのWEM Agentコンポーネント。	2203	---
Remote PC Access用のSCCM統合Wake on LANオプション。	2012	スタンドアロンのWake on LAN機能を使用してください。
XenAppおよびXenDesktop、Provisioning Services、StoreFront 用のCitrix SCOM Management Pack。監視可能な製品バージョンについては、Citrix SCOM Management Packs documentationを参照してください。	1912	展開の監視と管理にはDirectorを使用してください。SCOMのEOLと代替に関する詳細については、https://support.citrix.com/article/CTX266943を参照してください。

項目	非推奨が発表されたバージョン	代替
モビリティSDK / モバイルSDK (旧Citrix Labs製)	7.16	モバイルエクスペリエンスポリシー設定、およびホスト型デスクトップ/アプリのネイティブエクスペリエンスに置き換えられました。

削除された機能

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

項目	廃止が発表されたバージョン	削除されたバージョン	代替
SQL Server 2016および2017のサポート	2402および2308	2411	SQL Server 2019および2022を使用する
MCS I/Oライトバックキャッシュを、ディスクキャッシュのみを含みメモリキャッシュを含まないように構成するサポート	2402	2411	ライトバックキャッシュを有効にしてマシンを作成する場合、**メモリキャッシュサイズ (MB)** オプションを選択し、ゼロ以外のサイズを指定します。
Citrix StudioでのPVSインポートウィザードのサポート	1912 LTSR	2311	以下のいずれかの方法でCitrix Provisioning™ マシンをプロ

項目	廃止が発表されたバージョン	削除されたバージョン	代替
			ビジョニングする • Citrix Provisioning Consoleを使用してマシンをプロビジョニングし、Citrix Provisioning Devices Export Wizardを使用してCitrix Virtual Apps and Desktopsにエクスポートします。詳細については、Export Devices Wizardを参照してください。 • Web Studioを使用してCitrix Provisioningカタログを作成しま

項目	廃止が発表されたバージョン	削除されたバージョン	代替
			す。詳細については、Create Citrix Provisioning catalogs in Citrix Studioを参照してください。
Windows向けCitrix Workspaceアプリ1912	---	2402	最新バージョンを使用してください。
HDX Graphics FullScreen + テキスト最適化	2311	2311	
HDX 3D ProでのNVIDIA Frame Buffer Capture (NVFBC) のサポート	2308	2311	Desktop Duplication API (DDAPI) を使用してください。
ポリシー設定「インボックスプリンタードライバーの自動インストール」に対するVDAのサポート.	7.16	2311	なし。このポリシー設定は、以前のOS (Windows 7、Windows Server 2012 R2以前) のVDAでのみサポートされます。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
NVIDIA GPU ハードウェアエンコード (NVENC) (vGPU 11以前、およびドライバーバージョン466.77以前).	2305	2305	現在サポートされている NVIDIAドライバーを使用してください: vGPU 13以降、バージョン 471.41以降。
VDAメタインストーラーからの Citrix Supportability Tools (SupportabilityTool_x64 .msi)。	---	2212	---
Citrix License Administration Console (Windows License Server 11.16.3 build 30000に最後に含まれ、Windows License Server v11.16.6 build 31000で削除されました)。	2003	2006	Citrix Licensing Managerを使用してください。
Windows 10 バージョン 1709以前での Citrix Indirect Display Driver (IDD) グラフィックアダプターのサポート。	2003	2003	Citrix Virtual Apps and Desktops 7 1912 LTSR VDAを使用してください。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
GRID 9 以前のディスプレイドライバーを使用したNVIDIA GPU (NVENC) によるハードウェアエンコーディング。	2003	2003	Citrix Virtual Apps and Desktops 7 2003 以降のVDAでGRID 10 ディスプレイドライバーを使用するか、Citrix Virtual Apps and Desktops 7 1912 LTSR VDAを使用します。
セルフサービスパスワードリセット (SSPR) 機能。	2003	2006	---
VDAおよびコアサーバーコンポーネント向けの Microsoft .NET Framework バージョン4.8 より前のバージョンに対するサポート。Delivery Controller、Studio、Directorが含まれます。	1912	2003	.NET Framework バージョン4.8 にアップグレードします。
Windows Server 2012 R2 上の仮想デスクトップエージェント。	1912	2003	サポートされているオペレーティングシステムにVDAをイン

項目	廃止が発表されたバージョン	削除されたバージョン	代替
			ストールします。
Citrix Virtual Apps and Desktops Premiumエディションの AppDNA®アプリケーション移行コンポーネント。	1909	2003	---
32ビット（x86）マシンへのStudioのインストール。	1909	2003	サポートされているx64オペレーティングシステムにインストールします。
シームレスアプリケーションでのExcelフックのサポート。これは、Microsoft Excel 2010の各ワークブックに個別のタスクバーアイコンを作成するために使用されていました。	1909	1909	---
Windows Server 2012 R2（サービスパックを含む）上のコアサーバーコンポーネント。含まれるもの：Delivery Controller、	1906	2003	より新しいサポート対象のオペレーティングシステムにインストールしてください。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
Studio、Director。			
Microsoft SQL Server バージョン 2008 R2、2012、2014 (すべてのサービスパックとエディションを含む) 上でのサイト構成、構成ログ、および監視データベースのサポート。	1906	2003	サポートされているMicrosoft SQL Server バージョンにデータベースをインストールしてください。
x86プラットフォーム上のWindows 10でのVDAのサポート。	1906	1909*	サポートされているx64オペレーティングシステムにVDAをインストールしてください。*この機能は、Citrix Virtual Apps and Desktops 7 1912 LTSRでは引き続きサポートされています。
Citrix Virtual Apps and Desktopsインストールメディアからの Citrix Smart Tools Agentの削除。	1903	1906	---

項目	廃止が発表されたバージョン	削除されたバージョン	代替
Red Hat Enterprise Linux/CentOS 7.5でのLinux VDAのサポート。	1903	1903	Red Hat Enterprise Linuxのそれ以降のバージョンにLinux VDAをインストールします。
Citrix Virtual Apps and Desktops（旧XenApp and XenDesktop）とCitrix Receiver、およびWorkspace Hub間のTLS 1.0およびTLS 1.1プロトコルに対するStoreFrontのサポート。	7.17	2203	Citrix ReceiverをTLS 1.2プロトコルをサポートするCitrix Workspaceアプリにアップグレードします。Citrix Workspaceアプリの詳細については、https://docs.citrix.com/ja-jp/citrix-workspace-app を参照してください。
ポリシー設定「インボックスプリンタードライバーの自動インストール」に対するVDAのサポート。	7.16	2311	なし。このポリシー設定は、以前のOS（Windows 7、Windows Server 2012 R2以前）上のVDAでのみサポートされます。
Framehawkディスプレイリモートテクノロジーのサポート	1811	1903	Thinwireをadaptive transportを有効にして使用します。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
すべての Citrix Virtual Apps and Desktops (および XenApp and XenDesktop) バージョンにおける Citrix Smart Scale のサポート。この機能は 31 May 2019 にサポート終了となります。	1808	1906	強化された電源管理機能のために、Citrix Cloud の Virtual Apps and Desktops Service の使用を検討してください。
Citrix StoreFront、Citrix VDA、Citrix Studio、Citrix Director、および Citrix Delivery Controller による Microsoft .NET Framework バージョン 4.5.1、4.5.2、4.6、4.6.1、4.6.2、および 4.7 のサポート。	7.18	1808	.NET Framework バージョン 4.7.1 以降にアップグレードしてください。(インストーラーは、まだインストールされていない場合、.NET Framework 4.7.1 を自動的にインストールします。)
Red Hat Enterprise Linux 7.3 における Linux VDA のサポート。	7.18	1808	Red Hat Enterprise Linux のそれ以降のバージョンに Linux VDA

項目	廃止が発表されたバージョン	削除されたバージョン	代替
			をインストールしてください。
SUSE Linux Enterprise Server 11 Service Pack 4 における Linux VDA のサポート。	7.16	7.16	サポートされているSUSEバージョンにLinux VDAをインストールします。
VDAでのCitrix WDDMドライバーのサポート	7.16	7.16	Citrix WDDMドライバーは、VDAとともにインストールされなくなりました。
Windows 10 バージョン1511 (Threshold 2) およびそれ以前のWindowsシングルセッションOSリリース (Windows 8.xおよびWindows 7を含む) 上のVDA (<https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/>を参照)。	7.15 LTSR (および 7.12)	7.16	Windows 10の最小バージョン1607 (Redstone 1) またはそれ以降の半期チャネルにシングルセッションOS VDAをインストールします。1607 LTSBを使用している場合は、7.15 VDAを推奨します。CTX224843を参照してください。
Windows Server 2008 R2 およびWindows	7.15 LTSR (および 7.12)	7.16	サポートされているオペレーティングシステ

項目	廃止が発表されたバージョン	削除されたバージョン	代替
Server 2012 (サービスパックを含む) 上のVDA			ムにVDAをインストールします。
デスクトップコンポジションリダイレクト (以前はDirectXコマンドリモート処理として知られていた) (DCR)	7.15 LTSR	7.16	Thinwireを使用します。
Windows Server 2012およびWindows Server 2008 R2上のコアコンポーネント（サービスパックを含む）。以下が含まれます: Delivery Controller、Studio、Director、StoreFront、License Server、およびUniversal Print Server。	7.15 LTSR	7.18	サポートされているオペレーティングシステムにコンポーネントをインストールします。
Windows Server 2012およびWindows Server 2008 R2上のセルフサービスパスワードリセット	7.15 LTSR	7.18	より新しいサポートされているオペレーティングシステムにインストールします。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
(SSPR) 機能（サービスパックを含む）			
Windows 7、Windows 8、およびWindows 8.1上のStudio（サービスパックを含む）	7.15 LTSR	7.18	サポートされているオペレーティングシステムにStudioをインストールします。
Flashリダイレクト	7.15 LTSR	1912	ビデオコンテンツをHTML5ビデオとして作成します。管理対象コンテンツにはHTML5ビデオリダイレクトを、公開Webサイトにはブラウザコンテンツリダイレクトを使用します。詳細については、Flash Redirection End of Lifeの注記を参照してください。
StoreFrontとのCitrix Online統合 (Goto製品)	7.14 (およびStoreFront 3.11)	StoreFront 3.12	---
VDAインストール中に作成され、VDAマシンのローカル管理者グループに追加されていたユーザーアカウ	7.14	7.14	Windowsサービス CtxAppVServiceは同じ機能を実行します。これは自動的にインストールおよ

項目	廃止が発表されたバージョン	削除されたバージョン	代替
ント CtxAppVCOMAdminは、作成されなくなりました。基盤となる「COM」メカニズムも削除されました。			び構成され、ユーザーによる操作は不要です。
Windows Server 2008 32 ビット版での Universal Print Server UpsServerコンポーネントのサポート	7.14	7.14	より新しいサポート対象のオペレーティングシステムにインストールしてください。
Internet Explorer 8 上のストアフロントおよびウェブ用レシーバー	7.13	7.13	---
Citrix App-V コンポーネントのインストールを防ぐための VDA コマンドラインインストールオプション /no_appv	7.13	7.13	コマンドラインインストールオプション /exclude "Citrix Personalization for App-V – VDA" を使用します。
フル製品インストーラーは、新規インストール時に Citrix.Common.Commands スナップインをインストールしな	7.13	7.13	Citrix.Common.Commands スナップインによって提供されていた一部の PowerShell コマンドは、XenApp 6.5

項目	廃止が発表されたバージョン	削除されたバージョン	代替
くなり、既存のインストールをアップグレードする際に自動的に削除します。			SDK で引き続き利用できます。
*-CtxIcon コマンドレットによって提供されていたアイコンデータを操作する部分的な機能。	7.13	7.13	現在、Broker Service の *-BrokerIcon コマンドレットによって提供されています。
レガシー Thinwireモード	7.12	7.16	Thinwireを使用してください。Windows Server 2008 R2でレガシー Thinwireモードを使用している場合は、Windows Server 2012 R2またはWindows Server 2016に移行し、Thinwireを使用してください。
StoreFront 2.0、2.1、2.5、および2.5.2からのインプレースアップグレード	7.13	7.16	これらのバージョンのいずれかから、サポートされている新しいバージョンにアップグレードし、その後XenAppおよびXenDesktop 7.16にアップグ

項目	廃止が発表されたバージョン	削除されたバージョン	代替
			レードしてください。
XenDesktop 5.6または5.6 FP1からのインプレースアップグレード	7.12	7.16	XenDesktop 5.6または5.6 FP1の展開を現在のXenDesktopバージョンに移行してください。これを行うには、まずXenDesktop 7.6 LTSR（最新のCUを含む）にアップグレードし、その後、最新のCitrix Virtual Desktops（旧XenDesktop）リリースまたはLTSRバージョンにアップグレードしてください。
32ビット（x86）マシンへのDelivery Controller、Director、StoreFront、またはLicense Serverのインストール。	7.12	7.16	サポートされているx64オペレーティングシステムにインストールします。
接続リース	7.12	7.16	ローカルホストキャッシュを使用します。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
Windows XPで使用されるXenDesktop 5.6。Windows XPへのVDAインストールはサポートされていません。	7.12	7.16	サポートされているオペレーティングシステムにVDAをインストールします。
CloudPlatform接続のサポート	7.12	2003	別のサポートされているハイパーバイザーまたはクラウドサービスを使用します。
Azure Classic（Azure Service Managementとも呼ばれる）接続のサポート	7.12	2003	Citrix Cloud上のVirtual Apps and Desktops Serviceの使用を検討してください。
AppDisks機能（およびそれをサポートするStudioへのAppDNA統合）	7.13	2003	Citrix App Layeringを使用してください。
パーソナル ブイディスク機能	7.15	2006†	(https://docs.citrix.com/ja-jp/citrix-app-layering/4/layer/enable-user-layers.html)または(https://docs.citrix.com/ja-jp/citrix-virtual-apps-desktops/2411/-

			ltsr/1912/install-configure/user-personalization-layer.html)テクノロジーを使用してください。

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

システム要件

はじめに

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

インストールを開始する前に、インストールの準備を確認してください。

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

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

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

ハードウェア要件

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

次の表に、コアコンポーネントの最小要件を示します。

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

デスクトップとアプリケーションを提供する VM のサイジング

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

詳細については、以下を参照してください。

- Citrix Tech Zone には、サイジングに関するガイダンスが含まれています。
- 「Citrix Virtual Apps and Desktops Single Server Scalability」(/ja-jp/tech-zone/design/design-decisions/single-server-scalability.html)では、単一の物理ホストでサポートできるユーザー数またはVM数について説明しています。

マイクロソフト ビジュアル C++

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

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

デリバリーコントローラー

サポートされているオペレーティングシステム:

- ウィンドウズ サーバー 2025
- ウィンドウズ サーバー コア 2022
- ウィンドウズ サーバー 2022
- Windows Server 2019、StandardおよびDatacenterエディション、およびServer Coreオプション

要件:

- Microsoft .NET Framework 4.8（またはそれ以降のバージョン）がまだインストールされていない場合、自動的にインストールされます。
- Windows PowerShell 3.0、4.0、または5.0。
- Microsoft Visual C++ 2015–2022 再頒布可能パッケージ。
- Citrix Virtual Apps and Desktopsバージョン2407から2411以降にアップグレードする場合、またはバージョン2411以降を新規インストールする場合は、まずLicense Serverを最新バージョン（バージョン11.2.17ビルド51000以降）に更新してください。その後、Delivery Controllerをアップグレードします。これを怠ると、UIに警告メッセージが表示され、コマンドラインインストールが失敗します。

データベース

> **注:**

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

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

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

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

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

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

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

- Controllerをインストールすると、Local Host Cache機能で使用するために、累積更新プログラム14が適用されたMicrosoft SQL Server Express LocalDB 2022がインストールされます。（このインストールは、サイトデータベース用のデフォルトのSQL Server Expressインストールとは別です。）
- Controllerをアップグレードする際、既存のMicrosoft SQL Server Express LocalDBバージョンは自動的にアップグレードされません。交換要件と手順については、SQL Server Express LocalDBの交換を参照してください。

その他のデータベース情報:

- データベース
- CTX114501には、現在サポートされている最新のデータベースがリストされています。
- データベースのサイジングに関するガイダンス

- ローカルホストキャッシュ

ウェブ スタジオ

> **注:**
>
> - Citrix Virtual Apps and Desktops™の展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。
> - Web Studioは、オンプレミスのCitrix Virtual Apps and Desktops展開を構成および管理できるWebベースの管理コンソールです。これは、ユーザーエクスペリエンスの向上を目的として設計されており、Windowsベースの管理コンソールであるCitrix Studioよりも一般的に応答が高速です。「Web Studioのインストール」を参照してください。

サポートされているオペレーティングシステム:

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

シトリックス ディレクター

サポートされているオペレーティングシステム:

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

要件:

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

シトリックス プロファイル管理:

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

System Center Operations Manager (SCOM) との統合に関する要件:

- システムセンター 2012 R2 オペレーションズマネージャー

Directorの表示でサポートされているブラウザー:

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

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

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

サポートされているオペレーティングシステム:

- ウィンドウズ 11
- Windows 10 (x64のみ)、現在メインストリームサポート中のすべてのバージョン。
    - エディションのサポートについては、Knowledge Centerの記事 CTX224843 を参照してください。

要件:

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

リモートPCアクセスは、物理オフィスPCにインストールするこのVDAを使用します。このVDAは、Windows 11およびWindows 10上のCitrix Virtual Desktops™リモートPCアクセスでセキュアブートをサポートします。

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

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

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

Windows 7マシンへのVDAのインストールについては、以前のオペレーティングシステムを参照してください。

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

サポートされているオペレーティングシステム:

- ウィンドウズ サーバー 2025
- Windows 11 (Citrix DaaS™でのみサポート)
- Windows 10 (x64のみ、Citrix DaaSでのみサポート)、現在メインストリームサポート中のすべてのバージョン。
- ウィンドウズ サーバー 2022
- Windows Server 2019、Standard および Datacenter エディション

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

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

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

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

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

- Windows Media リダイレクト
- HTML5 ビデオ リダイレクト
- HDX™ RealTime Webcam リダイレクト

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

Windows Server 2008 R2 マシンへの VDA のインストールに関する情報については、以前のオペレーティングシステム を参照してください。

ホスト / 仮想化リソース

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

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

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

サポートされているハイパーバイザー:

- **XenServer（以前の名称はCitrix Hypervisor™）**

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

  詳細については、XenServer 仮想化環境 を参照してください。
- **マイクロソフト システム センター バーチャル マシン マネージャー**

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

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

  詳細については、Microsoft System Center Virtual Machine Manager virtualization environmentsを参照してください。
- **Nutanix アクロポリス**

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

  詳細については、Nutanix virtualization environmentsを参照してください。
- **ヴイエムウェア vSphere (vCenter + ESXi)**

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

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

  詳細については、VMware virtualization environmentsを参照してください。

サポートされているパブリッククラウドホスト:

- **アマゾン ウェブ サービス (AWS)**

  AWSを使用して仮想マシンをプロビジョニングする方法については、Amazon Web Services virtualization environmentsを参照してください。
- **Google Cloud Platform** 詳細については、Google Cloud Platform virtualization environments およびGetting Started with Citrix DaaS on Google Cloudを参照してください。
- **マイクロソフト アジュール リソース マネージャー**

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

- **Nutanix クラウドおよびパートナーソリューション**

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

- **VMware クラウドおよびパートナーソリューション**

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

パブリッククラウドホスト接続をデプロイに加える際は、以下を考慮してください。

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

Active Directoryの機能レベル

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

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

> **注:**

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

HDX

オーディオ

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

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

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

HDX ウィンドウズ メディア配信

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

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

HDX 3D プロ

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

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

- GPUパススルーは以下で利用可能です。
  - XenServer®
  - ニュータニックス AHV

    - VMware vSphereおよびVMware ESX（仮想ダイレクトグラフィックスアクセラレーション (vDGA) と呼ばれます）

- vGPU は以下で利用可能です:

    - XenServer
    - ニュータニックス AHV
    - ヴイエムウェア vSphere

`<https://docs.citrix.com/ja-jp/citrix-virtual-apps-desktops/2411/graphics/hdx-3d-pro>`を参照してください。

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

グラフィックス処理ユニット (GPU):

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

ユーザーデバイス:

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

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

ユニバーサル プリント サーバー

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

UpsServerコンポーネントは、以下でサポートされています。

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

要件：

- Microsoft Visual C++ 2015–2022 再頒布可能パッケージ
- マイクロソフト .NET Framework 4.8 以降

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

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

詳しくは、「プリンターのプロビジョニング」を参照してください。

その他

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

バージョン互換性の詳細については、製品マトリックスを参照してください。

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

Citrixポリシー情報をサイト構成データベースではなくActive Directoryに保存する場合は、Microsoft Group Policy Management Console（GPMC）が必要です。`CitrixGroupPolicyManagement_x64.msi`を個別にインストールする場合（たとえば、Citrix

Virtual Apps and Desktopsのコアコンポーネントがインストールされていないマシンにインストールする場合）、そのマシンにはVisual Studio 2015ランタイムがインストールされている必要があります。詳しくは、Microsoftのドキュメントを参照してください。

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

複数のNICがサポートされています。

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

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

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

この製品はPowerShellバージョン3～5をサポートしています。

技術概要

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

Citrix Virtual Apps and Desktops は、次のことを可能にします。

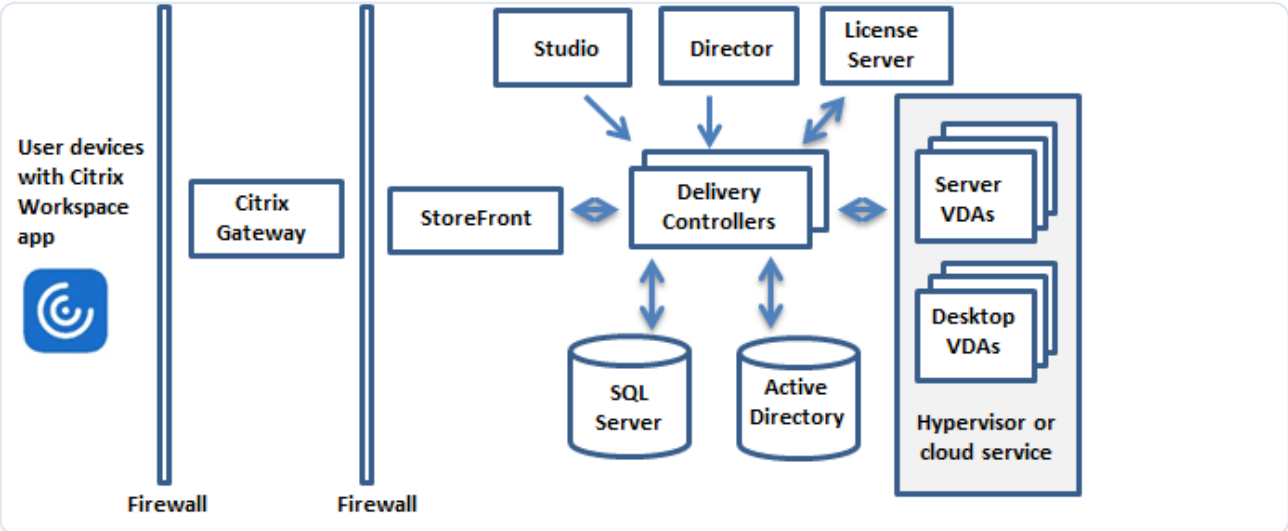
- エンドユーザーがデバイスのオペレーティングシステムやインターフェイスに依存せずにアプリケーションやデスクトップを実行すること。
- 管理者がネットワークを管理し、選択したデバイスまたはすべてのデバイスからのアクセスを制御すること。
- 管理者が単一のデータセンターからネットワーク全体を管理すること。

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

主要コンポーネント

Citrix Virtual Apps and Desktops を初めて使用する場合、この記事は特に役立ちます。

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



デリバリーコントローラー™

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

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

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

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

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

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

データベース

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

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

仮想配信エージェント (VDA)

VDAは、ユーザーに提供するサイト内の各物理または仮想マシンにインストールされます。これらのマシンはアプリケーションまたはデスクトップを提供します。VDAはマシンがControllerに登

録できるようにし、それにより、マシンとそれがホストするリソースがユーザーに利用可能になります。VDAはマシンとユーザーデバイス間の接続を確立および管理します。VDAは、ユーザーまたはセッションにCitrix®ライセンスが利用可能であることを確認し、セッション用に構成されたポリシーを適用します。

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

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

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

シトリックス ストアフロント™

StoreFrontは、ユーザーを認証し、ユーザーがアクセスするデスクトップとアプリケーションのストアを管理します。エンタープライズアプリケーションストアをホストでき、ユーザーは利用可能なデスクトップとアプリケーションにセルフサービスでアクセスできます。また、ユーザーのアプリケーションサブスクリプション、ショートカット名、その他のデータを追跡します。これにより、ユーザーは複数のデバイス間で一貫したエクスペリエンスを得ることができます。

Citrix Workspace™アプリ

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

スタジオ

Citrix Virtual Apps and Desktopsの展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この製品ドキュメントでは、Web

Studioのみを扱います。Citrix Studioの詳細については、Citrix Virtual Apps and Desktops 7 2212以前を参照してください。

ウェブスタジオ

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

シトリックス スタジオ

Citrix Studioは、Citrix Virtual Apps and Desktopsの展開を構成および管理する管理コンソールです。Citrix Studioは、アプリケーションとデスクトップの配信を管理するための個別の管理コンソールの必要性を排除します。Citrix Studioは、環境設定、アプリケーションとデスクトップをホストするワークロードの作成、およびユーザーへのアプリケーションとデスクトップの割り当てをガイドするウィザードを提供します。Studioを使用して、サイトのCitrixライセンスを割り当てて追跡することもできます。

Citrix Studioは、コントローラー内のBroker Serviceから表示する情報を取得し、TCPポート80を介して通信します。

セキュア プライベート アクセス

Citrix Secure Private Accessオンプレミスソリューションは、StoreFrontをWebおよびSaaSアプリへの統合アクセス ポータルとして使用し、仮想アプリおよびデスクトップとCitrix Workspaceの統合された一部として、ブラウザベースのアプリ（内部WebアプリおよびSaaSアプリ）へのゼロトラストネットワークアクセスを簡単に提供する機能により、組織全体のセキュリティとコンプライアンス体制を強化します。このソリューションは、NetScalerおよびStoreFrontの既存のリリースと互換性があり、バージョンに変更を加える必要はありません。詳細については、オンプレミス向けSecure Private Accessを参照してください。

シトリックス ディレクター

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

Directorは以下を表示します。

- コントローラー内のブローカーサービスからのリアルタイムセッションデータ。これには、ブローカーサービスがVDA内のブローカーエージェントから取得するデータが含まれます。
- コントローラー内のモニターサービスからの履歴サイトデータ。

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

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

シトリックス ライセンスサーバー

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

ハイパーバイザーまたはその他のサービス

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

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

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

追加コンポーネント

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

シトリックス プロビジョニング™

Citrix Provisioning (旧 Provisioning Services) は、一部のエディションで利用可能なオプションコンポーネントです。仮想マシンをプロビジョニングするための MCS の代替手段を提供します。

MCS がマスターイメージのコピーを作成するのに対し、PVS はマスターイメージをユーザーデバイスにストリーミングします。PVS はこれを行うためにハイパーバイザーを必要としないため、物理マシンをホストするために使用できます。PVS は Controller と通信してユーザーにリソースを提供します。

シトリックス ゲートウェイ

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

シトリックス SD-WAN™

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

一般的な展開の仕組み

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

展開におけるコンポーネント間の通信(/en-us/citrix-virtual-apps-desktops/2411/media/deployment-overview.png)

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

Controller は、リソース、アプリケーション、デスクトップを管理し、ユーザー接続を最適化およびバランス調整する独立した Windows サービスで構成されています。各サイトには 1 つ以上の

Controller があります。セッションは遅延、帯域幅、ネットワークの信頼性の影響を受けるため、可能であればすべての Controller を同じ LAN 上に配置してください。

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

ユーザー接続の処理方法

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

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

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

ユーザー接続フロー(/en-us/citrix-virtual-apps-desktops/2411/media/user-connections.png)

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

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

Controller はユーザーの資格情報を含むメッセージを VDA に送信し、その後、ユーザーと接続に関するすべてのデータを VDA に送信します。VDA は接続を受け入れ、同じ経路を通じて Citrix Workspace アプリに情報を送り返します。StoreFront で必要なパラメーターのセットが収集されます。これらのパラメーターは、Citrix-Workspace-app-StoreFront プロトコル会話の一部として Citrix Workspace アプリに送信されるか、または Independent Computing Architecture (ICA) ファイルに変換されてダウンロードされます。サイトが適切に設定されている限り、資格情報はプロセス全体で暗号化されたままになります。

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

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

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

データアクセスが機能する仕組み

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

展開におけるデータアクセス(/en-us/citrix-virtual-apps-desktops/2411/media/data-access.png)

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

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

Director は Citrix Gateway にアクセスして、HDX データに関する情報を取得することもできます。

デスクトップとアプリケーションの配信

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

マシンカタログ

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

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

有効なマシンタイプは次のとおりです。

- **マルチセッションOS:** マルチセッションオペレーティングシステムを搭載した仮想マシンまたは物理マシン。Citrix Virtual Apps公開アプリケーション（サーバーベースのホスト型アプリケーションとも呼ばれる）およびCitrix Virtual Apps公開デスクトップ（サーバーホスト型デスクトップとも呼ばれる）の配信に使用されます。これらのマシンには、複数のユーザーが同時に接続できます。
- **シングルセッションOS:** シングルセッションオペレーティングシステムを搭載した仮想マシンまたは物理マシン。VDIデスクトップ（オプションでパーソナライズできるシングルセッションOSを実行するデスクトップ）、VMホスト型アプリケーション（シングルセッションOSからのアプリケーション）、およびホスト型物理デスクトップの配信に使用されます。これらのデスクトップには、一度に1人のユーザーのみが接続できます。
- **Remote PC Access:** リモートユーザーがCitrix Workspaceアプリを実行している任意のデバイスから物理オフィスPCにアクセスできるようにします。オフィスPCはCitrix Virtual Desktops展開を通じて管理され、ユーザーデバイスは許可リストに指定されている必要があります。

詳細については、Citrix Virtual Apps and Desktopsのイメージ管理およびマシンカタログの作成を参照してください。

デリバリーグループ

デリバリーグループは、どのユーザーがどのマシンでどのアプリケーション、デスクトップ、またはその両方にアクセスできるかを指定します。デリバリーグループには、マシンカタログのマシンと、サイトにアクセスできるActive Directoryユーザーが含まれます。Active Directoryグループとデ

リバリーグループは、同様の要件を持つユーザーをグループ化する方法であるため、Active Directoryグループによってユーザーをデリバリーグループに割り当てることができます。

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

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

詳細については、デリバリーグループの作成を参照してください。

アプリケーショングループ

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

詳細については、アプリケーショングループの作成を参照してください。

詳細情報

- シトリックス 仮想アプリおよびデスクトップの図
- ネットワークポート
- データベース
- サポートされるハイパーバイザーおよびその他のサービス

データベース

> **注:**

> Citrix Virtual Apps and Desktops™の展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

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

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

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

Citrixは、データベースに関して以下を推奨します。

- **定期的にバックアップします。**データベースサーバーが故障した場合にバックアップから復元できるように、データベースを定期的にバックアップしてください。各データベースのバックアップ戦略は異なる場合があります。詳細については、CTX135207を参照してください。ただし、これはCitrixXenDesktopDBを参照していますが、これは現在サポートされておらず、お客様は利用できません。
- **サイト、監視、ログのSQL Serverデータベースを定期的にバックアップおよび復元します。**SQL Serverデータベースに関する具体的な情報については、「SQL Serverデータベースの完全バックアップと差分バックアップの作成」を参照してください。

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

高可用性

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

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

ローカルホストキャッシュ機能は、SQL Serverの高可用性ベストプラクティスを補完します。ローカルホストキャッシュにより、サイトデータベースが利用できない場合でも、ユーザーはアプリケーションやデスクトップに接続および再接続できます。詳しくは、「ローカルホストキャッシュ」を参照してください。

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

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

データベースソフトウェアのインストール

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

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

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

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

ほとんどの運用環境の展開、およびMicrosoftの高可用性機能を使用するすべての展開では、サポートされているSQL ServerのExpress Edition以外のエディションのみを使用することをお勧めします。最初のControllerがインストールされているサーバー以外のマシンにSQL Serverをインストールします。システム要件には、サポートされているSQL Serverのバージョンが記載されています。データベースは1台以上のマシンに配置できます。

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

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

サイト作成ウィザードからデータベースをセットアップする

サイト作成ウィザードの**データベース**ページで、データベース名とアドレス（場所）を指定します。（(#database-address-formats)を参照）。DirectorがMonitor Serviceを照会する際に発生する可能性のあるエラーを回避するため、監視データベースの名前に空白を使用しないでください。

データベースページでは、データベースをセットアップするための2つのオプション（自動とスクリプトの使用）が提供されます。一般に、必要なデータベース権限がある場合（Web Studioユーザーおよびシトリックス管理者）、自動オプションを使用できます。（(#permissions-required-to-set-up-databases)を参照）。

構成ログおよび監視データベースの場所は、サイト作成後に変更できます。(#change-database-locations)を参照してください。

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

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

サイト作成後にミラーリングを確認するには、PowerShellコマンドレット`get-configdbconnection`を実行して、接続文字列のFailover Partnerがミラーに設定されていることを確認します。

ミラーデータベース環境で後からDelivery Controllerを追加、移動、または削除する場合は、(/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/delivery-controllers.html)を参照してください。

自動セットアップ

必要なデータベース権限がある場合は、サイト作成ウィザードの**データベース**ページで、**Studioからデータベースを作成してセットアップする**を選択します。次に、プライマリデータベースの名前とアドレスを指定します。

指定したアドレスにデータベースが存在する場合、それは空である必要があります。指定したアドレスにデータベースが存在しない場合、データベースが見つからないことが通知され、データベースを作成するかどうかを尋ねられます。その操作を確定すると、Web Studioは自動的にデー

タベースを作成し、プライマリデータベースとレプリカデータベースの初期化スクリプトを適用します。

スクリプトによるセットアップ

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

1. サイト作成ウィザードの**データベース**ページで、**手動でセットアップするスクリプトを生成**を選択します。この操作により、以下のプライマリデータベースとレプリカデータベース（サイト、監視、ログデータベース）ごとに、次の3種類のスクリプトが生成されます。

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

   スクリプトの保存場所を指定できます。

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

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

データベース管理者がデータベースを作成します。各データベースは、次の特性を持つ必要があります。

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

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

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

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

すべてのスクリプトが正常に完了したら、データベース管理者は Citrix 管理者に 3 つのプリンシパルデータベースアドレスを渡します。

Web Studioはサイト作成を続行するように促します。**データベース**ページに戻ります。アドレスを入力します。データベースをホストしているサーバーのいずれかに接続できない場合、エラーメッセージが表示されます。

データベースのセットアップに必要な権限

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

操作	目的	サーバーロール	データベースロール
データベースの作成	適切な空のデータベースを作成する	`dbcreator`	

操作	目的	サーバーロール	データベースロール
スキーマの作成	すべてのサービス固有のスキーマを作成し、最初のControllerをサイトに追加します	`securityadmin` *	`db_owner`
Controllerを追加する	(最初のController以外の) Controllerをサイトに追加する	`securityadmin` *	`db_owner`
Controller (ミラーサーバー) を追加する	ミラーデータベースのミラーロールにある現在のデータベースサーバーにControllerログインを追加する	`securityadmin` *	
Controllerを削除する	サイトからControllerを削除する	**	`db_owner`
スキーマを更新する	スキーマの更新またはホットフィックスを適用する		`db_owner`

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

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

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

優先データベース権限スクリプト

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

PowerShell を使用して、推奨されるデータベース権限を指定できます。デフォルト以外の値を指定すると、個別のスクリプトが作成されます。1つのスクリプトには `securityadmin` ロールを必要とするタスクが含まれます。もう1つのスクリプトは `db_owner` 権限のみを必要とし、データベース管理者に連絡することなく、Citrix 管理者が実行できます。

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

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

詳細については、コマンドレットのヘルプを参照してください。

データベースアドレスの形式

データベースアドレスは、次のいずれかの形式で指定できます。

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

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

データベースの場所を変更する

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

- 以前のデータベースのデータは、新しいデータベースにはインポートされません。

- ログを取得する際に、両方のデータベースからログを集約することはできません。
- 新しいデータベースの最初のログエントリには、データベースの変更が発生したことが示されますが、以前のデータベースは特定されません。
- 強制ログが有効になっている場合、構成ログデータベースの場所を変更することはできません。
- SQL ServerとAzure SQL間でのデータベースの場所の変更はサポートされていません。

データベースの場所を変更するには：

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

詳細情報

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

配信方法

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

はじめに

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

- **インストール済みアプリ:** アプリケーションはベースデスクトップイメージの一部です。インストールプロセスには、レジストリの変更に加えて、イメージドライブにコピーされるdll、exe、その他のファイルが含まれます。詳細については、「マシンカタログの作成」を参照してください。
- **ストリーミングアプリ (Microsoft App-V):** アプリケーションはプロファイルされ、ネットワーク経由でオンデマンドでデスクトップに配信されます。アプリケーションファイルとレジストリ設定は、仮想デスクトップ上のコンテナに配置され、ベースオペレーティングシステムおよび相互から分離されます。この分離により、互換性の問題に対処できます。詳細については、「App-Vアプリケーションの展開と配信」を参照してください。
- **レイヤー化されたアプリ (Citrix App Layering):** 各レイヤーには、単一のアプリケーション、エージェント、またはオペレーティングシステムが含まれています。1つのOSレイヤー、1つのプラットフォームレイヤー (VDA、Citrix Provisioningエージェント)、および多数のアプリケーションレイヤーを統合することで、管理者は新しい展開可能なイメージを簡単に作成できます。OS、エージェント、およびアプリケーションが単一のレイヤーに存在するため、レイヤー化により継続的なメンテナンスが簡素化されます。レイヤーを更新すると、そのレイヤーを含むすべての展開済みイメージが更新されます。詳細については、「Citrix App Layering」を参照してください。
- **ホスト型Windowsアプリ:** マルチユーザーのCitrix Virtual Appsホストにインストールされ、デスクトップではなくアプリケーションとして展開されるアプリケーション。ユーザーは、VDIデスクトップまたはエンドポイントデバイスからホスト型Windowsアプリにシームレスにアクセスでき、アプリがリモートで実行されているという事実を隠します。詳細については、「デリバリーグループの作成」を参照してください。
- **ローカルアプリ:** エンドポイントデバイスに展開されたアプリケーション。アプリケーションインターフェイスは、エンドポイントで実行されているにもかかわらず、ユーザーのホスト型VDIセッション内に表示されます。詳細については、「ローカルアプリアクセスとURLリダイレクト」を参照してください。

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

Citrix Virtual Apps™ 公開アプリケーションおよびデスクトップ

マルチセッションOSマシンを使用して、Citrix Virtual Apps and Desktopsの公開アプリケーションおよび公開デスクトップを配信します。

ユースケース:

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

利点と考慮事項:

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

ユーザーエクスペリエンス:

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

アプリケーションの処理、ホスト、および配信:

- アプリケーションの処理は、ユーザーデバイスではなく、ホスティングマシンで行われます。ホスティングマシンは、物理マシンまたは仮想マシンです。
- アプリケーションとデスクトップは、マルチセッションOSマシン上に存在します。
- マシンはマシンカタログを通じて利用可能になります。

- マシンカタログからのマシンは、同じアプリケーションセットをユーザーグループに配信するデリバリーグループに編成されます。
- マルチセッションOSマシンは、デスクトップまたはアプリケーション、あるいはその両方をホストするデリバリーグループをサポートします。

セッション管理と割り当て:

- マルチセッションOSマシンは、単一のマシンから複数のセッションを実行し、複数のアプリケーションとデスクトップを複数の同時接続ユーザーに提供します。各ユーザーは、ホストされているすべてのアプリケーションを実行できる単一のセッションを必要とします。

  たとえば、ユーザーがログオンしてアプリケーションを要求すると、そのマシン上の1つのセッションは他のユーザーが利用できなくなります。2人目のユーザーがログオンし、そのマシンがホストするアプリケーションを要求すると、同じマシン上の2つ目のセッションが利用できなくなります。両方のユーザーがさらにアプリケーションを要求した場合、ユーザーは同じセッションを使用して複数のアプリケーションを実行できるため、追加のセッションは必要ありません。さらに2人のユーザーがログオンしてデスクトップを要求し、同じマシンで2つのセッションが利用可能な場合、その単一のマシンは4つのセッションを使用して4人の異なるユーザーをホストしていることになります。
- ユーザーが割り当てられているデリバリーグループ内で、最も負荷の低いサーバー上のマシンが選択されます。セッションが利用可能なマシンは、ユーザーがログオンしたときに、そのユーザーにアプリケーションを配信するためにランダムに割り当てられます。

VMホスト型アプリ

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

ユースケース:

- セキュアで一元管理を提供し、ホストサーバーあたり多数のユーザーをサポートするクライアントベースのアプリケーション配信ソリューションを求めているとします。これらのユーザーに、高解像度でシームレスに表示されるアプリケーションを提供したいと考えています。
- ユーザーは、社内ユーザー、外部請負業者、サードパーティの共同作業者、およびその他の暫定的なチームメンバーです。ユーザーは、ホストされているアプリケーションへのオフラインアクセスを必要としません。
- アプリケーションの種類: 他のアプリケーションとうまく連携しない可能性のあるアプリケーションや、Microsoft .NET Frameworkのようにオペレーティングシステムと相互作用する可能性のあるアプリケーション。これらの種類のアプリケーションは、仮想マシンでのホスティングに最適です。

利点と考慮事項:

- マスターイメージ上のアプリケーションとデスクトップは、データセンター内のマシンで安全に管理、ホスト、実行され、より費用対効果の高いアプリケーション配信ソリューションを提供します。
- ログオン時に、ユーザーは同じアプリケーションをホストするように構成されたデリバリーグループ内のマシンにランダムに割り当てることができます。また、ユーザーがログオンするたびに、単一のマシンを単一のユーザーにアプリケーションを配信するように静的に割り当てることもできます。静的に割り当てられたマシンでは、ユーザーは仮想マシンに独自のアプリケーションをインストールおよび管理できます。
- シングルセッションOSマシンでは、複数のセッションの実行はサポートされていません。そのため、ユーザーがログオンすると、各ユーザーはデリバリーグループ内の単一のマシンを消費し、ユーザーはアプリケーションにアクセスするためにオンラインである必要があります。
- この方法により、アプリケーション処理用のサーバーリソースの量が増加し、ユーザーデータ用のストレージの量が増加する可能性があります。

ユーザーエクスペリエンス：

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

アプリケーションの処理、ホスト、および配信：

- マルチセッションOSマシンと同じですが、仮想シングルセッションOSマシンである点が異なります。

セッション管理と割り当て：

- シングルセッションOSマシンは、1台のマシンから単一のデスクトップセッションを実行します。アプリケーションのみにアクセスする場合、オペレーティングシステムは各アプリケーションを新しいセッションと見なすため、1人のユーザーが複数のアプリケーションを使用できます（単一のアプリケーションに限定されません）。
- デリバリーグループ内で、ユーザーがログオンすると、静的に割り当てられたマシン（ユーザーがログオンするたびに同じマシン）、またはセッションの可用性に基づいて選択されるランダムに割り当てられたマシンにアクセスできます。

VDIデスクトップ

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

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

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

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

- **ランダム非永続デスクトップ（プール型VDIデスクトップとも呼ばれる）：** ユーザーがこれらのデスクトップのいずれかにログオンするたびに、そのユーザーはデスクトップのプールから選択されたデスクトップに接続します。このプールは単一のマスターイメージに基づいています。デスクトップへのすべての変更は、マシンが再起動すると失われます。
- **静的非永続デスクトップ：** 最初のログオン時に、ユーザーはデスクトップのプールからデスクトップを割り当てられます。（プール内の各マシンは単一のマスターイメージに基づいています。）最初の使用後、ユーザーがデスクトップを使用するためにログオンするたびに、そのユーザーは最初の使用時に割り当てられたのと同じデスクトップに接続します。デスクトップへのすべての変更は、マシンが再起動すると失われます。
- **静的永続デスクトップ:** 他の種類のVDIデスクトップとは異なり、ユーザーはこれらのデスクトップを完全にパーソナライズできます。最初のログオン時に、ユーザーはデスクトッププールからデスクトップを割り当てられます。その後のログオンでは、そのユーザーは初回使用時に割り当てられた同じデスクトップに接続します。マシンの再起動後もデスクトップへの変更は保持されます。

リモートPCアクセス

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

Remote PC Accessは、仮想デスクトップとアプリケーションを提供するCitrix Virtual Apps and Desktopsのコンポーネントと同じものを使用します。その結果、Remote PC Accessの展開と構成

の要件およびプロセスは、仮想リソースの配信のためにCitrix Virtual Apps and Desktopsを展開する際に必要なものと同じです。この一貫性により、一貫性のある統合された管理エクスペリエンスが提供されます。ユーザーは、Citrix HDX™を使用してオフィスPCセッションを配信することで、最高のエクスペリエンスを得ることができます。

詳細については、Remote PC Accessを参照してください。

ネットワークポート

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

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

ポート情報が必要になる場合があります。

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

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

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

HDX™

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

> Citrix HDXは、あらゆるデバイスとネットワーク上で、一元化されたアプリケーションとデスクトップのユーザーに高精細なエクスペリエンスを提供する幅広いテクノロジーセットを表します。

仮想チャネル(/en-us/citrix-virtual-apps-desktops/2411/media/hdx-vir-channels.png)

HDXは、次の3つの技術原則に基づいて設計されています。

- インテリジェントリダイレクト
- 適応型圧縮
- データ重複排除

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

- **インテリジェントなリダイレクト** - インテリジェントなリダイレクトは、画面アクティビティ、アプリケーションコマンド、エンドポイントデバイス、ネットワークおよびサーバーの機能を分析し、アプリケーションまたはデスクトップのアクティビティをどこでどのようにレンダリングするかを即座に決定します。レンダリングは、エンドポイントデバイスまたはホスティングサーバーのいずれかで実行できます。
- **適応型圧縮** - 適応型圧縮により、貧弱なネットワーク接続でもリッチなマルチメディア表示を配信できます。HDXはまず、入力、デバイス、表示の種類（テキスト、ビデオ、音声、マルチメディア）など、いくつかの変数を評価します。最適な圧縮コーデックと、CPUおよびGPU使用率の最適な比率を選択します。その後、各固有のユーザーと状況に基づいてインテリジェントに適応します。このインテリジェントな適応は、ユーザーごと、あるいはセッションごとに行われます。

  適応型圧縮(/en-us/citrix-virtual-apps-desktops/2411/media/hdx-adaptive-compression.png)
- **データ重複排除** - ネットワークトラフィックの重複排除により、クライアントとサーバー間で送信される集約データが削減されます。これは、ビットマップグラフィック、ドキュメント、

印刷ジョブ、ストリーミングメディアなど、一般的にアクセスされるデータ内の繰り返しパターンを利用することで実現されます。これらのパターンをキャッシュすることで、変更のみがネットワーク経由で送信され、重複するトラフィックが排除されます。HDXはまた、マルチメディアストリームのマルチキャストもサポートしており、ソースからの単一の送信が、各ユーザーへの1対1の接続ではなく、1つの場所で複数のサブスクライバーによって視聴されます。

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

デバイス上での動作

HDXは、ユーザーデバイスのコンピューティング能力を利用して、ユーザーエクスペリエンスを向上および最適化します。HDXテクノロジーにより、ユーザーは仮想デスクトップまたはアプリケーションでマルチメディアコンテンツをスムーズかつシームレスに利用できます。ワークスペースコントロールを使用すると、ユーザーは仮想デスクトップとアプリケーションを一時停止し、中断した時点から別のデバイスで作業を再開できます。

ネットワーク上

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

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

データセンター内

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

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

HDX インサイト

HDX Insightは、NetScaler® Network InspectorとPerformance ManagerをDirectorと統合したものです。ICAトラフィックに関するデータを取得し、リアルタイムおよび履歴の詳細をダッシュボードビューで提供します。このデータには、クライアント側およびサーバー側のICAセッション遅

延、ICAチャネルの帯域幅使用量、および各セッションのICAラウンドトリップタイム値が含まれます。

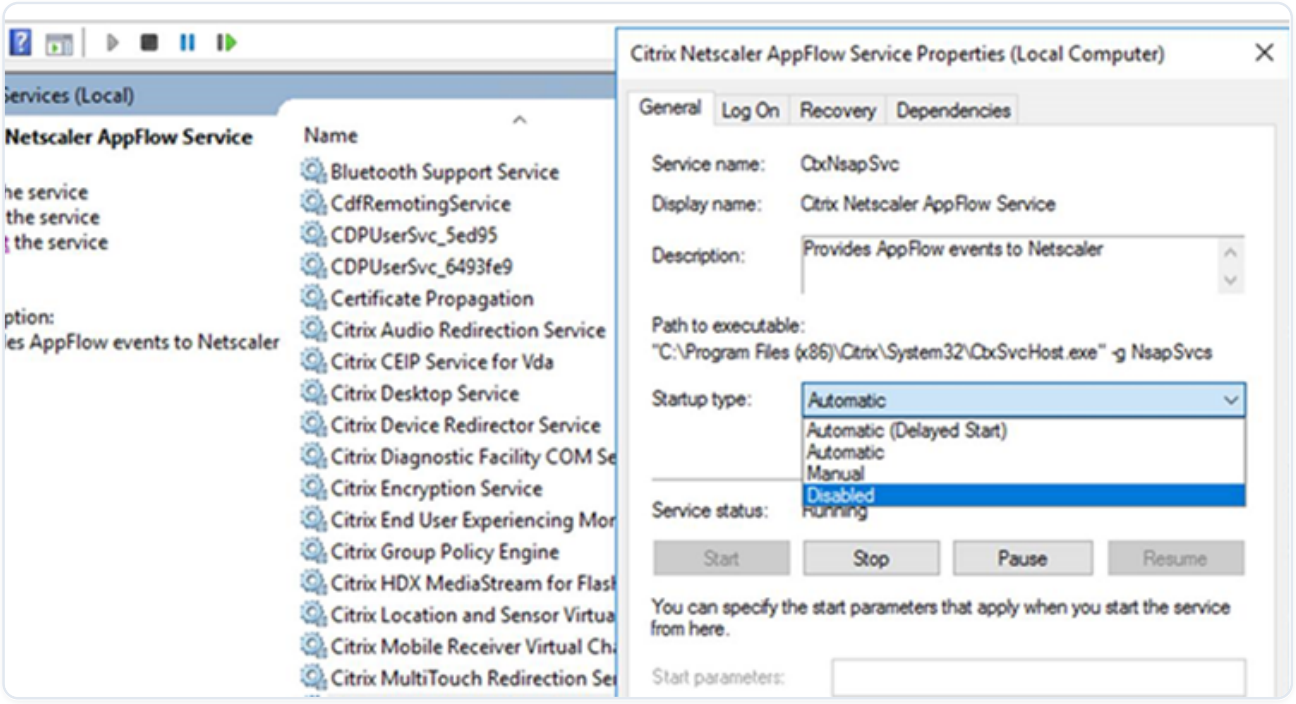
NetScalerでHDX Insight仮想チャネルを使用して、必要なすべてのデータポイントを非圧縮形式で移動させることができます。この機能を無効にすると、NetScalerデバイスは、さまざまな仮想チャネルに分散されたICA®トラフィックを復号化および解凍します。単一の仮想チャネルを使用することで、複雑さが軽減され、スケーラビリティが向上し、費用対効果が高まります。

最小要件:

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

HDX Insight仮想チャネルの有効化または無効化

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



仮想デスクトップからHDX機能を体験する

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

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

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

- HDXが高品位オーディオをどのように配信するかを確認するには：

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

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

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

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

知っておくと良いこと:

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

自動クライアント再接続とセッションの信頼性

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

自動クライアント再接続:

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

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

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

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

自動クライアント再接続のデフォルト設定:

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

詳細については、(/ja-jp/citrix-virtual-apps-desktops/2411/policies/reference/ica-policy-settings/auto-client-reconnect-policy-settings.html)のを参照してください。

セッションの信頼性:

セッションの信頼性により、ネットワークの中断を越えてICAセッションがシームレスに再接続されます。セッションの信頼性は、設定で指定された時間の後にユーザーセッションを閉じ（または切断し）ます。セッションの信頼性タイムアウト後、自動クライアント再接続設定が有効になり、切断されたセッションにユーザーを再接続しようとします。セッションの信頼性が進行中の場合、アプリケーションおよびデスクトップのネットワーク中断通知は次のようにユーザーに送信されます。

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

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

再接続時、クライアントとサーバーはプロトコル交換の同じポイントで再開します。セッションウィンドウは半透明性を失い、アプリケーションには適切な通知領域ポップアップが表示されます。

デフォルトのセッションの信頼性設定

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

詳細については、「セッション信頼性ポリシー設定」を参照してください。

NetScalerと自動クライアント再接続およびセッションの信頼性:

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

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

HDX アダプティブスループット

HDXアダプティブスループットは、出力バッファを調整することで、ICAセッションのピークスループットをインテリジェントに微調整します。出力バッファの数は、最初は高い値に設定されます。この高い値により、特に高遅延ネットワークにおいて、データがより迅速かつ効率的にクライアントに送信されることが可能になります。より優れた対話性、高速なファイル転送、スムーズなビデオ再生、高いフレームレート、および解像度を提供することで、ユーザーエクスペリエンスが向上します。

セッションの対話性は、ICAセッション内のデータストリームが対話性に悪影響を与えているかどうかを判断するために常に測定されます。そのような場合、大量のデータストリームがセッションに与える影響を軽減し、対話性が回復するようにスループットは低下します。

> **重要:**
>
> HDXアダプティブスループットは、出力バッファの設定方法を、このメカニズムをクライアントからVDAに移動することで変更し、手動での設定は不要です。

> この機能には、以下の要件があります。

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

ユーザーデバイスに送信される画質の向上

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

- 視覚品質。ユーザーデバイスに表示される画像の視覚品質を制御します: 中、高、常にロスレス、ロスレスに構築（デフォルト = 中）。デフォルト設定の「中」を使用した場合の実際のビデオ品質は、利用可能な帯域幅によって異なります。
- ターゲットフレームレート。仮想デスクトップからユーザーデバイスに送信される1秒あたりの最大フレーム数を指定します（デフォルト = 30）。CPUが遅いデバイスの場合、低い値を指定するとユーザーエクスペリエンスが向上する可能性があります。サポートされる1秒あたりの最大フレームレートは60です。
- 表示メモリ制限。セッションの最大ビデオバッファサイズをキロバイト単位で指定します（デフォルト = 65536 KB）。より多くの色深度と高解像度を必要とする接続の場合、制限を増やします。必要な最大メモリを計算できます。

> **注:**
>
> 「**表示メモリ制限**」設定は非推奨になりました。この変更により、Citrixは表示メモリを制限しなくなりました。代わりに、クライアントの表示レイアウトが完全に収容されるように、必要な最小限のメモリが割り当てられます。

ビデオ会議のパフォーマンスを向上させる

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

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

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

- クライアントオーディオリダイレクト

- クライアントマイクのリダイレクト
- マルチメディア会議

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

ネットワークトラフィックの優先順位

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

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

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

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

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

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

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

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

  追加のTCPトラフィックを許可するように、VDA上のファイアウォールを明示的に構成します。
- Multi-Stream computer setting - この設定はデフォルトで無効になっています。環境でMulti-StreamをサポートするCitrix NetScaler SD-WANを使用している場合、この設定を構成する必要はありません。目的のQuality of Serviceを実現するために、サードパーティ製ルーターまたはレガシーNetScaler SD-WANを使用する場合は、このポリシー設定を構成してください。
- マルチストリームユーザー設定 - この設定はデフォルトで無効になっています。

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

リモート言語バーの表示/非表示

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

VDAから言語バー機能のクライアント制御を無効にするには：

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

Unicodeキーボードマッピング

非 Windows 版 Citrix Receiver は、ローカルキーボードレイアウト（Unicode）を使用します。ユーザーがローカルキーボードレイアウトとサーバーキーボードレイアウト（スキャンコード）を変更した場合、それらが同期せず、出力が正しくない可能性があります。たとえば、User1 がローカルキーボードレイアウトを英語からドイツ語に変更します。その後、User1 はサーバー側のキーボードをドイツ語に変更します。両方のキーボードレイアウトがドイツ語であっても、同期しない可能性があり、文字出力が正しくない原因となります。

Unicode キーボードレイアウトマッピングを有効または無効にする

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

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名前: EnableKlMap

種類: DWORD

値: 1

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

Unicode キーボードレイアウトマッピング互換モードを有効にする

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

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名前: DisableWindowHook

種類: DWORD

値: 1

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

Citrix ICA® 仮想チャネル

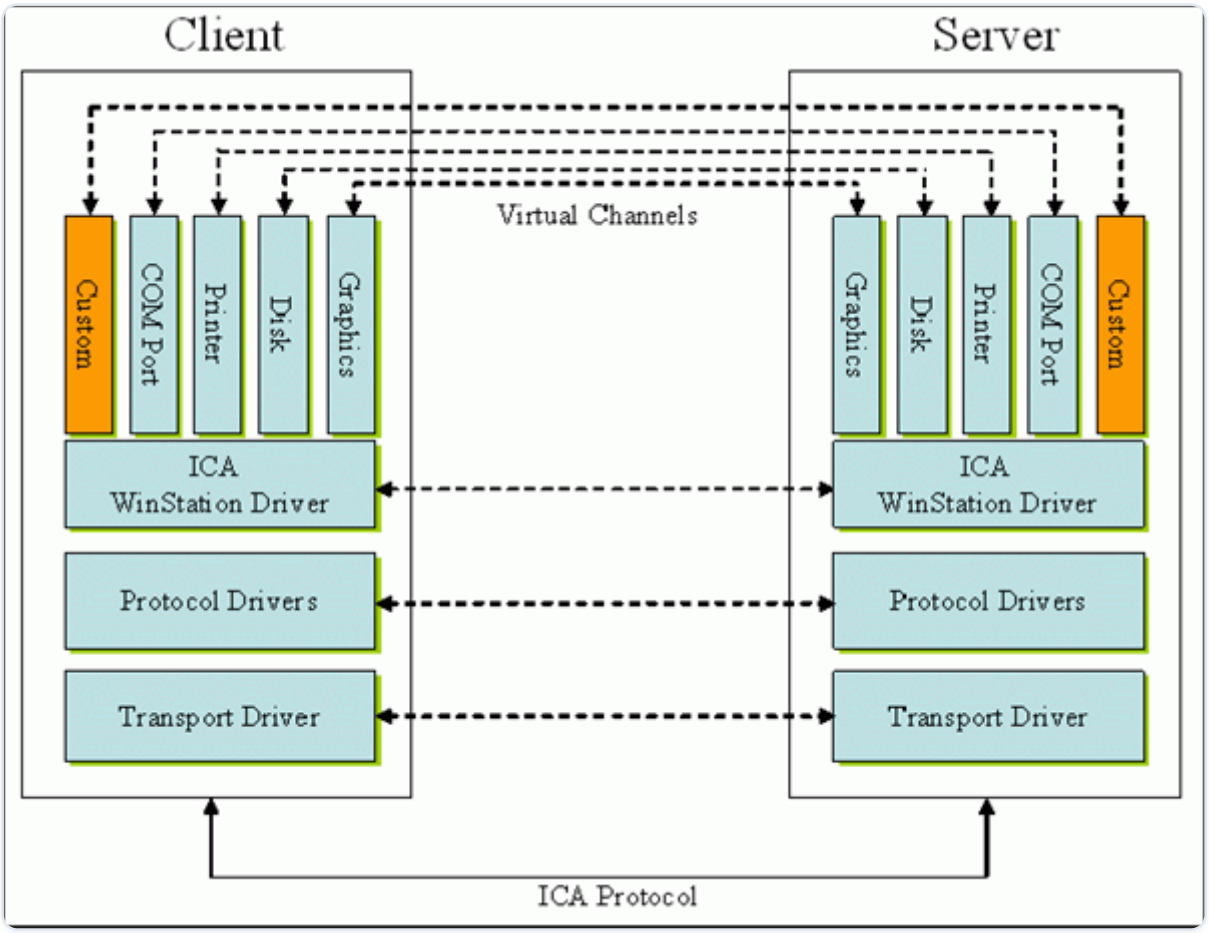
> **警告:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じた問題が解決できることを保証できません。レジストリエディターは、お客様ご自身の責任において使用してください。編集する前に、必ずレジストリをバックアップしてください。

ICA仮想チャネルとは?

Citrix Workspace™アプリとCitrix Virtual Apps and Desktops™サーバー間の機能と通信の大部分は、仮想チャネルを介して行われます。仮想チャネルは、Citrix Virtual Apps and Desktopsサーバーでのリモートコンピューティングエクスペリエンスに不可欠な部分です。仮想チャネルは次の目的で使用されます。

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

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



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

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

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

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

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

または

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

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

> **注記:**

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

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

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

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

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

64ビット互換性

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

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

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

汎用USB仮想チャネル

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

- ctxusbm.sys
- ctxusbr.sys

ICA仮想チャネルの仕組み

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

シェルによってロードされる仮想チャネルモジュール（例：）：

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

一部はカーネルモードとしてロードされます。例：

- CtxDvcs.sys – ダイナミック仮想チャネル
- Icausbb.sys – 汎用USBリダイレクト
- Picadm.sys – クライアントドライブマッピング

- Picaser.sys – COMポートリダイレクト
- Picapar.sys – LPTポートリダイレクト

サーバー側のグラフィック仮想チャネル

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

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

Windowsサービスでの特殊チャネルのホスティング

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

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

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

サーバー側では、すべてのクライアント仮想チャネルは、WinStationドライバー (Wdica.sys) を介してルーティングされます。クライアント側では、wfica32.exe に組み込まれている対応するWinStationドライバーがクライアント仮想チャネルをポーリングします。この図は、仮想チャネルのクライアント-サーバー接続を示しています。

仮想チャネル接続(/en-us/citrix-virtual-apps-desktops/2411/media/virtual-channel-connection.png)

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

1. クライアントは Citrix Virtual Apps and Desktops サーバーに接続します。クライアントは、サポートする仮想チャネルに関する情報をサーバーに渡します。
2. サーバー側アプリケーションが起動し、仮想チャネルへのハンドルを取得し、必要に応じてチャネルに関する追加情報を問い合わせます。
3. クライアント仮想ドライバーとサーバー側アプリケーションは、次の2つの方法を使用してデータを渡します。
    - サーバーアプリケーションがクライアントに送信するデータを持っている場合、データはすぐにクライアントに送信されます。クライアントがデータを受信すると、WinStationドライバーは仮想チャネルデータをICAストリームから逆多重化し、すぐにクライアント仮想ドライバーに渡します。
    - If the client virtual driver has data to send to the server, the data is sent the next time the WinStation driver polls it. When the server receives the data, it is queued until the virtual channel application reads it. There is no way to alert the server virtual channel application that data was received.
4. サーバー仮想チャネルアプリケーションが完了すると、仮想チャネルを閉じ、割り当てられたリソースを解放します。

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

> **注:**

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

> Virtual Channel SDK を使用して仮想チャネルを作成するには、中程度のプログラミング知識が必要です。この方法を使用して、クライアントとサーバー間の主要な通信パスを提供します。たとえば、セッション内のプロセスで使用するために、クライアント側でスキャナーなどのデバイスの使用を実装する場合などです。

> **注:**

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

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

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

重要:

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

仮想チャネルのパススルー機能

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

次の機能は、シングルホップまたはマルチホップで同じように動作します。

- クライアント COM ポートマッピング
- クライアントドライブマッピング
- クライアントプリンターマッピング
- クライアント UPD
- エンドユーザーエクスペリエンス監視
- 汎用 USB
- ケルベロス
- マルチメディアサポート
- スマートカードサポート

- 透明なキーパススルー
- トウェイン

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

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

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

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

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

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

以下の従来の仮想チャネルとその機能がサポートされています。

- クライアント
- クライアントCOMポートマッピング
- クライアントドライブマッピング
- クライアントプリンターマッピング
- 汎用USB (パフォーマンス上の理由により制限あり)

- マルチメディアサポート
- スマートカードサポート
- SSON
- 透過的なキーパススルー

セキュリティとICA仮想チャネル

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

ベストプラクティス

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

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

仮想チャネルの命名:

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

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

仮想チャネルは、7文字（またはそれ以下）のASCII名で参照されます。ICAプロトコルの以前のバージョンでは、仮想チャネルは番号付けされていました。現在、番号はASCII名に基づいて動的に割り当てられるため、実装が容易になります。内部使用のみを目的として仮想チャネルコードを開発しているユーザーは、既存の仮想チャネルと競合しない任意の7文字の名前を使用できます。数字と大文字小文字のASCIIのみを使用してください。独自の仮想チャネルを追加する際は、既存の命名規則に従ってください。いくつかの事前定義されたチャネルがあります。事前定義されたチャネルはOEM識別子CTXで始まり、Citrixのみが使用できます。

ダブルホップサポート:

仮想チャネル	ダブルホップはサポートされていますか？
オーディオ	いいえ

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

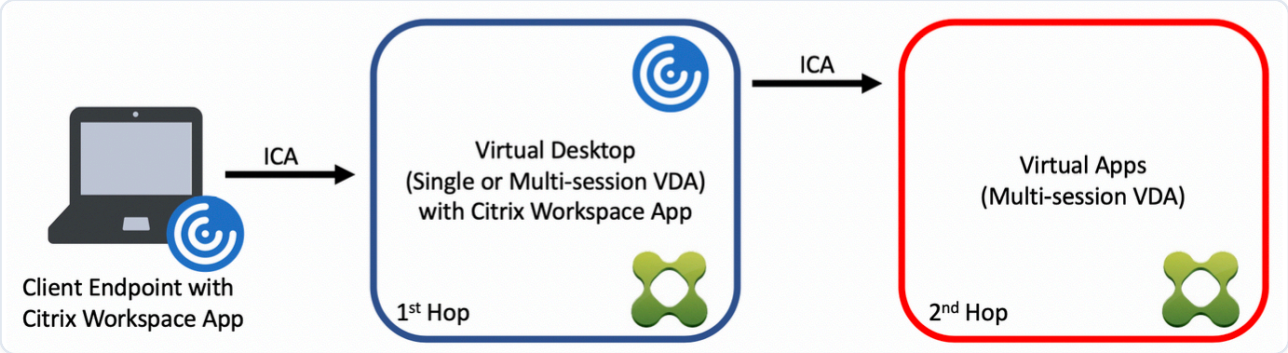
参照

- ICA仮想チャネルSDK
- Citrix Developer Networkは、Citrix SDKの使用に関するすべての技術リソースと議論の場です。このネットワークでは、SDK、サンプルコードとスクリプト、拡張機能とプラグイン、お

よびSDKドキュメントにアクセスできます。また、各Citrix SDKに関する技術的な議論が行われるCitrix Developer Networkフォーラムも含まれています。

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

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



ダブルホップシナリオでは、ユーザーがシングルセッションOS VDA（VDIとして知られる）またはマルチセッションOS VDA（公開デスクトップとして知られる）で実行されているCitrix Virtual Desktopsに接続する場合、それがファーストホップと見なされます。ユーザーが仮想デスクトップに接続した後、Citrix Virtual Apps™セッションを起動できます。それがセカンドホップと見なされます。

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

システム要件

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

ファーストホップでは、シングルセッションまたはマルチセッションOS VDAとCitrix Workspaceアプリのサポートされているバージョンを使用する必要があります。セカンドホップでは、マルチセッションOS VDAのサポートされているバージョンを使用する必要があります。サポートされているバージョンについては、製品マトリックスページを参照してください。

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

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

ダブルホップにおけるHDX™の展開に関する考慮事項

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

グラフィック

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

遅延

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

マルチメディア

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

USBデバイスリダイレクト

HDXには、幅広いUSBデバイスタイプをサポートするための汎用および最適化されたリダイレクトモードが含まれています。各ホップで使用されているモードに特に注意し、最良の結果を得る

ための参照として以下の表を使用してください。汎用および最適化されたリダイレクトモードの詳細については、「汎用USBデバイス」を参照してください。

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

注:

USBプロトコルの本質的なチャッティネスにより、ホップ間でパフォーマンスが低下する可能性があります。機能と結果は、特定のデバイスとアプリケーションの要件によって異なります。デバイスリダイレクトのすべての場合において、特にダブルホップシナリオでは、検証テストを強くお勧めします。

サポートの例外

ダブルホップセッションは、ほとんどのHDX機能と機能をサポートしますが、次のものは除きます。

- ブラウザコンテンツリダイレクト
- ローカルアプリアクセス
- Skype for Business向けリアルタイム最適化パック(/ja-jp/hdx-optimization/current-release.html)
- Microsoft Teams向け最適化

インストールと構成

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

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

準備

インストール準備 を確認し、必要なタスクをすべて完了してください。

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

コアコンポーネントのインストール

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

サイトの作成

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

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

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

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

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

オプションコンポーネントのインストール

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

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

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

オプションで、Citrix Virtual Apps and Desktops展開にさらにCitrixコンポーネントを統合します。

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

マシンカタログを作成する

Studioでサイトを作成すると、マシンカタログの作成が案内されます。

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

デリバリーグループを作成する

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

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

アプリケーショングループの作成（オプション）

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

既知の制限事項

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

マシンID

各マシンには、コンピューターアカウントとも呼ばれる固有のマシンIDが必要です。マシンIDは、マシンローカルまたはディレクトリで作成および管理できます。Citrix®は、Active Directoryに参加済み、ハイブリッドAzure Active Directoryに参加済み、またはドメインに参加していないマシンでの仮想アプリケーションおよびデスクトップのホスティングをサポートしています。

マシンIDの種類

以下のマシンIDの種類がサポートされています。

マシンIDの種類	説明
AD参加済み	IDはオンプレミスのActive Directoryで作成および管理されます。プロビジョニングされたマシンは、割り当てられたマシンIDを使用してオンプレミスのActive Directoryに参加します。
ハイブリッドAzure AD参加済み	IDはオンプレミスのActive Directoryで作成され、Azure AD Connectを介してAzure ADと同期されます。プロビジョニングされたマシンはオンプレミスのActive Directoryに参加します。その後、マシンはハイブリッドAzure ADに参

マシンIDの種類	説明
	加します。ハイブリッドAzure AD参加済みVMをインポートする場合、そのVMはCitrix Virtual Apps and DesktopsによってActive Directory参加済みVMとして扱われます。
ドメイン非参加	IDはマシンローカルで作成および管理されます。Citrix Virtual Apps and DesktopsへのVMのインポートはサポートされていません。

サポートされる構成

各シナリオでサポートされる構成の詳細は次のとおりです。

サポートされるインフラストラクチャ

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

サポートされているワークスペース認証IDプロバイダー

マシンID	アジュールACTIVE DIRECTORY	アクティブディレクトリ	ACTIVE DIRECTORYとトークン	オクタ	SAML	シトリックス ゲートウェイ	アダプティブ認証
AD参加済み	はい	はい	はい	はい	はい	はい	はい
ハイブリッドAzure AD参加済み	はい	はい	はい	はい	はい	はい	はい
ドメイン非参加	はい	はい	はい	はい	はい	はい	はい

Active Directory参加済み

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

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

この製品は以下をサポートします。

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

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

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

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

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

複数のActive Directoryフォレスト環境での展開

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

フォレスト間に適切なDNSフォワーダーが配置されている場合、DNSインフラストラクチャに逆引きDNSゾーンは必要ありません。

VDAとControllerが別々のフォレストにある場合、Active Directory名とNetBIOS名が異なるかどうかにかかわらず、`SupportMultipleForest`キーが必要です。VDAとDelivery Controllerにレジストリキーを追加するには、以下の情報を使用してください。

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

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

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

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

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

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

VDAでのNTLM認証の不要な有効化（Kerberosよりも安全性が低い）を回避するために、レジストリエントリが追加されました。このエントリは、下位互換性のために引き続き使用できる`SupportMultipleForest`エントリの代わりに使用できます。

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

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

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

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

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

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

外部信頼が設定されている場合、VDAで以下の変更を行います。

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

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

次の表に、サポートされている信頼の種類を示します。

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

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

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

次のステップ

オンプレミスのActive Directory (AD) に参加しているマシンIDのIDプールを作成する方法については、「オンプレミスのActive Directoryに参加しているマシンIDのIDプール」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/identity-pools-different-machine-identity-join-types/identity-pool-on-premises-active-directory-joined.html)を参照してください。

ハイブリッド Azure Active Directory 参加済み

> **注記：**
>
> 2023年7月以降、Microsoft は Azure Active Directory (Azure AD) を Microsoft Entra ID に名称変更しました。このドキュメントでは、Azure Active Directory、Azure AD、または AAD へのすべての参照は、Microsoft Entra ID を指します。

この記事では、システム要件セクションで概説されている要件に加えて、Hybrid Azure Active Directory (HAAD) 参加済みカタログおよび Microsoft Intune に登録されている Hybrid Azure AD 参加済みカタログのIDプールを作成するための要件について説明します。

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

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

Hybrid Azure Active Directory 参加済みの要件

- VDAの種類：シングルセッション（デスクトップのみ）またはマルチセッション（アプリとデスクトップ）
- VDAバージョン：2212以降
- プロビジョニングの種類：Machine Creation Services™ (MCS)、永続的および非永続的
- 割り当ての種類：専用およびプール
- ホスティングプラットフォーム：任意のハイパーバイザーまたはクラウドサービス

Hybrid Azure Active Directory 参加済みの制限事項

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

ハイブリッド Azure Active Directory 参加済みの考慮事項

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

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

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

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

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

$MaxCount = 60



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

{

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

  {

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

    if ($provider -eq 'Citrix')

    {

        break;

    }



    if ($provider -eq 1)

    {

        Set-ItemProperty -Path $VirtualDesktopKeyPath -Name "Provider"
```

```
-Value "Citrix" -Force

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

        Start-Sleep 5

        dsregcmd /join

        break

    }

  }



  Start-Sleep 1

}
```

- デフォルトでは、Azure AD Connectは30分ごとに同期します。プロビジョニングされたマシンが最初の起動時にハイブリッド Azure ADに参加するまでには、最大30分かかる場合があります。

Microsoft Intuneに登録されたハイブリッド Azure AD参加済みカタログ

Microsoft Intuneに登録されたハイブリッド Azure AD参加済みカタログ、永続的なシングルセッションおよびマルチセッションVMは、共同管理機能を持つデバイス資格情報を使用します。

共同管理により、Configuration ManagerとMicrosoft Intuneの両方を使用して、Windows 10以降のデバイスを同時に管理できます。詳細については、共同管理を参照してください。

Microsoft Intuneに登録されているHybrid Azure AD参加済みカタログの前提条件

この機能を有効にする前に、以下を確認してください。

- お使いのAzure環境がMicrosoft Intuneを使用するためのライセンス要件を満たしていること。詳細については、Microsoftドキュメントを参照してください。
- 共同管理が有効な有効なConfiguration Manager展開があること。詳細については、Microsoftドキュメントを参照してください。

Microsoft Intuneに登録されたハイブリッドAzure AD参加済みカタログの要件

- VDAの種類: シングルセッションまたはマルチセッション
- VDAバージョン: 2407以降
- プロビジョニングの種類: Machine Creation Service (MCS)、Persistent。非永続的なシングルおよびマルチセッションVM向けのMicrosoft Intuneに登録されたハイブリッドAzure AD参加済みカタログは、現在Preview段階です。Microsoft IntuneへのハイブリッドEntra ID参加済み非永続VMの登録を参照してください。
- 割り当ての種類: 専用およびプール
- ホスティングプラットフォーム: 任意のハイパーバイザーまたはクラウドサービス

Microsoft Intuneに登録されたハイブリッドAzure AD参加済みカタログの制限事項

- マシンカタログの作成または更新時にイメージの準備をスキップしないでください。
- Configuration Manager のインターネットベースのクライアント管理 (IBCM) はサポートされていません。

Microsoft Intuneに登録されたハイブリッドAzure AD参加済みカタログに関する考慮事項

- カタログ内の多数のマシンが同時に電源オンになると、Intune への登録が遅れる可能性があります。

  Microsoft は、特定の期間内に登録できるデバイスの数を制限するテナントごとの Intune 登録制限を課しています。許可されるデバイスの数は、テナントに関連付けられている Microsoft Intune ライセンスの数によって異なります。テナントの許可される制限については、Microsoft アカウントチームにお問い合わせください。このアプローチにより、大規模な環境での Microsoft Intune 登録のスケーリングが向上します。

  永続マシンでは、すべてのデバイスが Intune 登録を完了するまでに初期の待機時間が必要になる場合があります。

  非永続マシンについては、Autoscale™ または手動電源操作のいずれかで同時電源操作を制限することを検討してください。

- Configuration Manager の Cloud Attach を構成します。詳細については、Microsoft ドキュメントを参照してください。
- マスターVMにConfiguration Managerクライアントを手動でインストールし、`.\CCMSetup.exe /mp:SCCMServer /logon FSP=SCCMServer`でサイトコードを割り当てないでください。SCCMServer は、お使いの環境の SCCM サーバー名です。詳細については、Microsoft ドキュメントを参照してください。

- MCSで作成されたマシンは、Active Directory Domain Servicesに公開されているサイト境界グループを見つけるために、自動サイト割り当てメカニズムを使用します。お使いの環境で **Configuration Manager** の 境界と境界グループが構成されていることを確認してください。自動サイト割り当てが利用できない場合は、以下のレジストリ設定を通じて、マスターVMに静的なConfiguration Managerサイトコードを構成できます。

  キー:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MachineIdentityServiceAgent\DeviceMa
  nagement
  ```

  値の名前: `MdmSccmSiteCode`

  値の型: **String**

  値のデータ: `the site code to be assigned`

次のステップ

Hybrid Azure Active Directory 参加済みカタログのIDプール作成の詳細については、Hybrid Azure Active Directory 参加済みマシンIDのIDプールを参照してください。

ドメインに参加していない

この記事では、システム要件セクションで概説されている要件に加えて、Citrix Virtual Apps and Desktops を使用してドメインに参加していないカタログを作成するための要件について説明します。

要件

- コントロールプレーン: サポートされる構成を参照
- VDAタイプ: シングルセッション (デスクトップのみ) またはマルチセッション (アプリとデスクトップ)
- VDAバージョン: 2311以降
- プロビジョニングの種類: Machine Creation Services™ (MCS)、永続的および非永続的
- 割り当ての種類: 専用およびプール
- ホスティングプラットフォーム: MCSでサポートされているすべてのプラットフォーム
- Rendezvous V2を有効にする必要があります

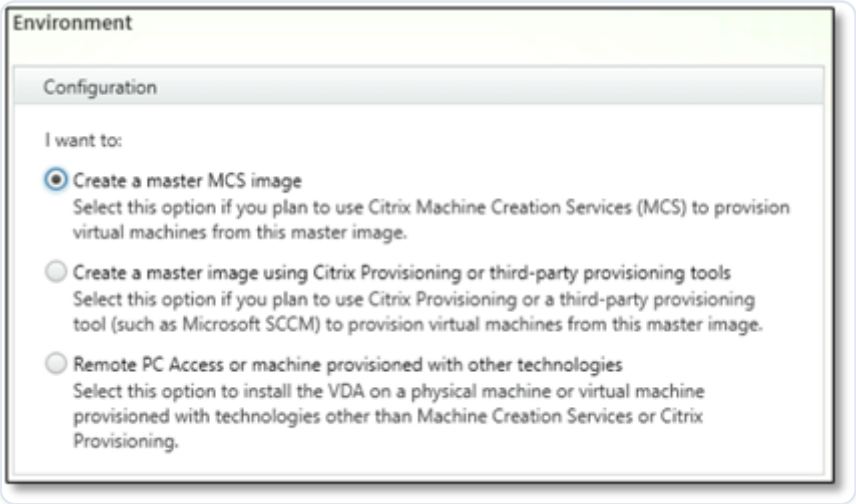
制限事項

- サービス継続性はサポートされていません。
- マルチセッションのドメインに参加していないVDAを使用する場合、ローカルユーザーのプロファイルデータは保持されず、ログオフ時に削除されます。

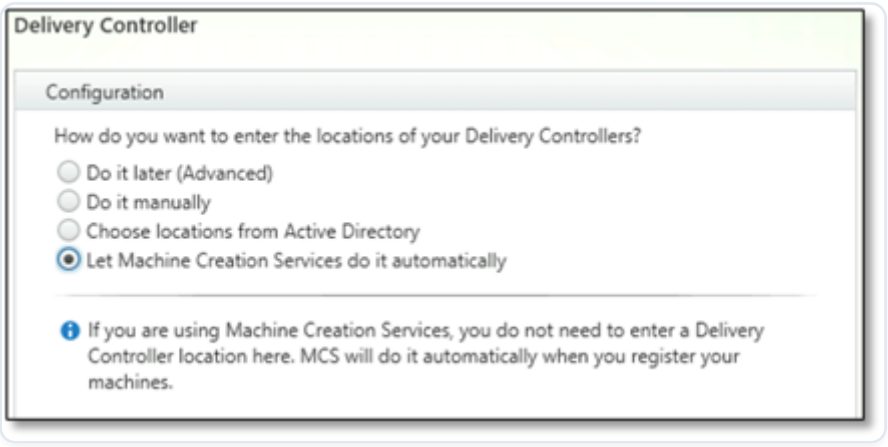
VDAのインストールと構成

VDAをインストールする手順に従います。

1. インストールウィザードで次のオプションを選択してください。
    - 「環境」ページで、**「マスターMCSイメージを作成」**を選択します。



    - 「Delivery Controller™」ページで、**「Machine Creation Servicesに自動的に実行させる」**を選択します。



次のステップ

リソースの場所とホスティング接続が利用可能になったら、IDプールを作成します。ドメインに参加していないマシンIDのIDプールの作成に関する詳細については、ドメインに参加していないマシンIDのIDプールを参照してください。

インストール準備

Citrix Virtual Apps and Desktops™ の展開は、以下のコンポーネントのインストールから始まります。このプロセスにより、ファイアウォール内のユーザーにアプリケーションとデスクトップを配信する準備が整います。

- 1つ以上のDelivery Controller
- Citrix Director (シトリックス ディレクター)
- Citrix StoreFront™ (シトリックス ストアフロント™)
- Citrixライセンスサーバー
- 1つ以上のCitrix Virtual Delivery Agent (VDA) (シトリックス バーチャル デリバリー エージェント)
- Universal Print Server、Federated Authentication Service、Self-Service Password Resetなどのオプションコンポーネントおよびテクノロジー

ファイアウォールの外部のユーザー向けには、Citrix Gatewayなどの追加コンポーネントをインストールして構成します。概要については、「Citrix Virtual Apps and DesktopsとCitrix Gatewayの統合」を参照してください。

注:

サーバーOSおよびワークステーションOSで、以下のMicrosoftの前提条件が満たされていることを確認してください。

- Microsoft **Volume Shadow Copy** および **Microsoft Software Shadow Copy Provider** サービスが実行されていること。詳細については、「ボリュームシャドウコピーサービス」を参照してください。
- **MS-Defender** のバージョンは4.18.2105.5より高い必要があります。詳細については、「Microsoft Defender Antivirusのセキュリティインテリジェンスと製品の更新」を参照してください。

展開にWindows Serverワークロードが含まれている場合は、「Microsoft RDSライセンスサーバーを構成する」を参照してください。

製品ISOに含まれるフル製品インストーラーを使用して、多くのコンポーネントとテクノロジーを展開できます。VDAのインストールには、スタンドアロンVDAインストーラーを使用できます。スタンドアロンVDAインストーラーは、Citrixダウンロードサイトで入手できます。すべてのインストーラーには、グラフィカルインターフェイスとコマンドラインインターフェイスが用意されています。「インストーラー」を参照してください。

製品ISOには、Active Directory内のマシンにVDAをインストール、アップグレード、または削除するサンプルスクリプトが含まれています。これらのスクリプトを使用して、Machine Creation Services (MCS) およびCitrix Provisioning (旧Provisioning Services) で使用されるイメージを管理することもできます。詳細については、「スクリプトを使用したVDAのインストール」を参照してください。

インストール前に確認する情報

- 技術概要: 製品とそのコンポーネントに慣れるため。
- セキュリティ: 展開環境を計画する際。
- 既知の問題: このバージョンで発生する可能性のある問題。
- データベース: システムデータベースとその構成方法について学習します。Controllerのインストール中に、サイトデータベースとして使用するためにSQL Server Expressをインストールできます。ほとんどのデータベース情報は、コアコンポーネントのインストール後にサイトを作成するときに構成します。
- Remote PC Access: ユーザーがオフィスにある物理マシンにリモートでアクセスできるようにする環境を展開する場合。
- 接続とリソース: アプリケーションとデスクトップ用のVMをホストまたはプロビジョニングするためにハイパーバイザーまたはその他のサービスを使用している場合。最初の接続は、サイトを作成するとき（コアコンポーネントのインストール後）に構成できます。それまでに仮想化環境をセットアップしてください。
- Microsoft System Center Configuration Manager: ConfigMgrを使用してアプリケーションとデスクトップへのアクセスを管理している場合、またはRemote PC AccessでWake on LAN機能を使用している場合。
- **パブリッククラウドホスト接続:** Hybrid Rights Licenseをお持ちの場合、パブリッククラウドへのホスト接続を作成できます。Hybrid Rights Licenseに関する情報については、「Hybrid Rights Renewals」を参照してください。パブリッククラウドのエンタイトルメントとこの変更の理由に関する情報については、「CTX270373」を参照してください。

コンポーネントのインストール場所

サポートされているプラットフォーム、オペレーティングシステム、およびバージョンについては、「システム要件」を確認してください。コンポーネントの前提条件は、特に記載がない限り自動的にインストールされます。Citrix StoreFrontおよびCitrix License Serverのサポートされているプラットフォームと前提条件については、それぞれのドキュメントを参照してください。

コアコンポーネントは、同じサーバーまたは異なるサーバーにインストールできます。

- すべてのコアコンポーネントを1台のサーバーにインストールする方法は、評価、テスト、または小規模な実稼働環境の展開に有効です。
- 将来の拡張に対応するため、コンポーネントを異なるサーバーにインストールすることを検討してください。たとえば、StudioをControllerをインストールしたサーバーとは別のマシンにインストールすると、サイトをリモートで管理できます。
- ほとんどの本番環境の展開では、コアコンポーネントを別々のサーバーにインストールすることをお勧めします。

  他のサーバーに他のコンポーネントをインストールする前に、Citrix License Serverとライセンスをインストールしてください。
- Server CoreOS (Delivery Controllerなど) にサポートされているコンポーネントをインストールするには、コマンドラインを使用する必要があります。このOSタイプにはグラフィカルインターフェイスがないため、Studioやその他のツールは別の場所にインストールし、それらをControllerサーバーにポイントしてください。

同じサーバーにDelivery Controller™とマルチセッションOS用VDAの両方をインストールできます。インストーラーを起動し、Delivery Controller (およびそのマシンにインストールしたい他のコアコンポーネント) を選択します。その後、インストーラーを再度起動し、マルチセッションOS用の**Virtual Delivery Agent**を選択します。

各オペレーティングシステムに最新のアップデートが適用されていることを確認してください。

すべてのマシンのシステムクロックが同期されていることを確認してください。マシン間の通信を保護するKerberosインフラストラクチャには同期が必要です。

XenServerを使用している場合、仮想マシンの電源状態が登録済みであっても不明と表示されることがあります。この問題を解決するには、ホストとの時刻同期を無効にするために、レジストリキー`HostTime`の値を編集します。

```
HKEY_LOCAL_MACHINE\Software\Citrix\XenTools\HostTime="Local"
```

```
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\XenTools\HostTime="Local"
```

ヒント:

デフォルト値は`HostTime="UTC"`です。この値をUTC以外のもの、たとえば`Local`に変更してください。この変更により、ホストとの時刻同期が効果的に無効になります。

Windows 10シングルセッションマシン向けの最適化ガイダンスは、CTX216252で入手できます。

コンポーネントをインストールしない場所:

- Active Directoryドメインコントローラーには、いかなるコンポーネントもインストールしないでください。
- SQL Serverクラスタリングインストール、SQL Serverミラーリングインストール、またはHyper-Vを実行しているサーバーのノードにControllerをインストールすることはサポートされていません。

この製品バージョンがサポートしていないWindows OSにVDAをインストールまたはアップグレードしようとすると、オプションを説明する記事へのメッセージが表示されます。

権限とActive Directoryの要件

コンポーネントをインストールするマシンでは、ドメインユーザーであり、ローカル管理者である必要があります。

スタンドアロンVDAインストーラーを使用するには、管理者特権があるか、**管理者として実行**を使用する必要があります。

インストールを開始する前に、Active Directory ドメインを構成してください。

- システム要件には、サポートされているActive Directoryの機能レベルが記載されています。Active Directoryへの参加には、詳細情報が含まれています。
- Active Directoryドメインサービスを実行しているドメインコントローラーが少なくとも1つ必要です。
- ドメインコントローラーには、Citrix Virtual Apps and Desktopsのコンポーネントをインストールしないでください。
- Studioで組織単位名を指定する際に、スラッシュ (/) を使用しないでください。

Citrix License Serverのインストールに使用されるWindowsユーザーアカウントは、委任管理のフル管理者として自動的に構成されます。

詳細については、以下を参照してください。

- セキュリティのベストプラクティス
- 委任管理
- Active Directory構成に関するMicrosoftドキュメント

インストールのガイダンス、考慮事項、およびベストプラクティス

任意のコンポーネントのインストール中

- フルプロダクトメディアからDelivery Controller、Studio、License Server、またはDirectorをインストールまたはアップグレードする際に、Citrixインストーラーが、以前のWindowsインストールによる再起動がマシンで保留中であることを検出すると、インストーラーは終了コード9で停止します。マシンの再起動を求められます。

  これは Citrix による強制的な再起動ではありません。マシンに以前インストールされた他のコンポーネントが原因です。この状況が発生した場合は、マシンを再起動してから、Citrix インストーラーを再度起動してください。

  コマンドラインインターフェイスを使用する場合、コマンドに `/no_pending_reboot_check` オプションを含めることで、保留中の再起動のチェックを回避できます。
- 通常、コンポーネントに前提条件がある場合、インストーラーはそれらが存在しない場合に展開します。一部の前提条件では、マシンの再起動が必要になる場合があります。
- インストール前、インストール中、インストール後にオブジェクトを作成するときは、各オブジェクトに一意の名前を指定してください。たとえば、ネットワーク、グループ、カタログ、リソースには一意の名前を付けてください。
- コンポーネントが正常にインストールされない場合、インストールはエラーメッセージとともに停止します。正常にインストールされたコンポーネントは保持されます。それらを再インストールする必要はありません。
- コンポーネントをインストール（またはアップグレード）すると、Citrix Analyticsが自動的に収集されます。デフォルトでは、インストールが完了するとそのデータは自動的にCitrixにアップロードされます。また、コンポーネントをインストールすると、匿名データをアップロードするCitrix Customer Experience Improvement Program (CEIP) に自動的に登録されます。

  インストール中に、メンテナンスとトラブルシューティングのために診断情報を収集する他のCitrixテクノロジーに参加することも選択できます。これらのプログラムの詳細については、「Citrix Insight Services」を参照してください。

- Studioをインストール（またはアップグレード）すると、Google Analyticsが自動的に収集され（後でアップロードされ）ます。Studioのインストール後、レジストリキー `HKLM\Software\Citrix\DesktopStudio\GAEnabled` を使用してこの設定を変更できます。値が**1**の場合は収集とアップロードが有効になり、**0**の場合は収集とアップロードが無効になります。
- VDAのインストールが失敗した場合、MSIアナライザーは失敗したMSIログを解析し、正確なエラーコードを表示します。既知の問題である場合、アナライザーはCTX記事を提案します。アナライザーは、失敗エラーコードに関する匿名化されたデータも収集します。このデータは、CEIPによって収集された他のデータに含まれます。CEIPへの登録を終了すると、収集されたMSIアナライザーデータはCitrixに送信されなくなります。

VDAのインストール中

- Citrix Workspace™ app for Windowsは利用可能ですが、VDAをインストールする際にはデフォルトではインストールされません。ユーザーはCitrix WebサイトからCitrix Workspace app for Windowsおよびその他のCitrix Workspaceアプリをダウンロード、インストール（およびアップグレード）できます。または、StoreFrontサーバーからこれらのCitrix Workspaceアプリを利用可能にすることもできます。StoreFrontのドキュメントを参照してください。
- Microsoft Print Spoolerサービスは有効にする必要があります。このサービスが無効になっている場合、VDAを正常にインストールすることはできません。
- ほとんどのサポートされているWindowsエディションには、Microsoft Media Foundationがすでにインストールされています。マシンにMedia Foundationがない場合（Nエディションなど）、いくつかのマルチメディア機能はインストールされず、動作しません。
  - Windows Media リダイレクト
  - HTML5 ビデオ リダイレクト
  - HDX™ RealTime Webカメラ リダイレクト

  制限を認識するか、VDA のインストールを終了し、Media Foundation のインストール後に再開できます。グラフィカルインターフェイスでは、この選択肢はメッセージで表示されます。コマンドラインでは、`/no_mediafoundation_ack` オプションを使用して制限を認識できます。
- VDA をインストールすると、**Direct Access Users** という新しいローカルユーザーグループが自動的に作成されます。シングルセッションOS 用の VDA では、このグループは RDP 接続にのみ適用されます。マルチセッションOS 用の VDA では、このグループは ICA® および RDP 接続に適用されます。

- VDA は、通信するための有効なコントローラーアドレスを持っている必要があります。そうでない場合、セッションを確立できません。コントローラーアドレスは、VDA のインストール時または後で指定できます。これを行う必要があることを忘れないでください。詳細については、「VDA 登録」を参照してください。

VDA インストール後およびインストール中の再起動

VDA インストールの終了時に再起動が必要です。その再起動はデフォルトで自動的に行われます。

VDA をバージョン 7.17 (またはそれ以降のサポートされているバージョン) にアップグレードする場合、アップグレード中に再起動が発生します。これは回避できません。

VDA インストール中に必要な再起動の回数を最小限に抑えるには：

- VDA のインストールを開始する前に、サポートされている .NET Framework バージョンがインストールされていることを確認してください。
- Windows マルチセッションOS マシンでは、VDA をインストールする前に RDS ロールサービスをインストールして有効にしてください。

VDA をインストールする前にこれらの前提条件をインストールしない場合：

- グラフィカルインターフェイスまたは `/noreboot` オプションなしでコマンドラインインターフェイスを使用している場合、前提条件のインストール後にマシンは自動的に再起動します。
- `/noreboot` オプションを使用してコマンドラインインターフェイスを使用している場合、再起動を開始する必要があります。

VDAバージョンをアップグレードする際、アップグレード中に再起動が発生します。これは回避できません。

インストールまたはアップグレードの失敗時の復元

> **注:**
>
> この機能は、シングルセッションおよびマルチセッションVDAで利用できます。

> シングルセッションVDAのインストールまたはアップグレードが失敗し、「障害時の復元」機能が有効になっている場合、マシンはインストールまたはアップグレードが開始される前に設定された復元ポイントに戻されます。

マルチセッションVDAのインストールまたはアップグレードが失敗し、「障害発生時の復元」機能が有効になっている場合、マシンはインストールまたはアップグレードが開始される前に実行されたバックアップの状態に戻されます。

この機能が有効な状態でシングルセッションVDAのインストールまたはアップグレードが開始されると、インストーラーは実際のインストールまたはアップグレードを開始する前にシステム復元ポイントを作成します。VDAのインストールまたはアップグレードが失敗した場合、マシンは復元ポイントの状態に戻されます。`%temp%/Citrix`フォルダーには、展開ログと復元に関するその他の情報が含まれています。

この機能が有効な状態でマルチセッションVDAのインストールまたはアップグレードが開始されると、インストーラーは実際のインストールまたはアップグレードを開始する前にサーバーバックアップを作成します。VDAのインストールまたはアップグレードが失敗した場合、マシンはバックアップの状態に戻されます。`%temp%/Citrix`フォルダーには、展開ログと復元に関するその他の情報が含まれています。サーバーバックアップの作成にかかる時間は、必要なバックアップのサイズとサーバーで利用可能なリソースの量に基づきます。バックアップは *C:\WindowsImageBackup\servername* に保存されます。

デフォルトでは、この機能は無効になっています。

この機能を有効にする予定がある場合は、GPO設定 (`Computer Configuration > Administrative Templates > System > System Restore`) によってシステム復元が無効になっていないことを確認してください。

> **注:**
>
> このGPO設定は、マルチセッションVDAの復元には適用されません。

> シングルセッションまたはマルチセッションVDAのインストールまたはアップグレード時にこの機能を有効にするには：

- VDAインストーラーのグラフィカルインターフェイスを使用する場合（**Autostart** または復元オプションやサイレントオプションなしの `XenDesktopVDASetup.exe` コマンドを使用する場合など）は、**Summary** ページで **Enable automatic restore if update fails** チェックボックスをオンにします。

  インストール/アップグレードが正常に完了した場合、復元ポイント/バックアップは使用されませんが、保持されます。

- コマンドラインを使用して、`/enablerestore` または `/enablerestorecleanup` オプションのいずれかでVDAインストーラーを実行します。
  - `/enablerestorecleanup` オプションを使用し、インストール/アップグレードが正常に完了した場合、復元ポイント/サーバーバックアップは自動的に削除されます。
  - `/enablerestore` オプションを使用し、インストール/アップグレードが正常に完了した場合、復元ポイントは使用されませんが、保持されます。

インストーラー

フルプロダクトインストーラー

ISOで提供されているフルプロダクトインストーラーを使用して、次のことができます。

- コアコンポーネント（Delivery Controller、Studio、Director、License Server）をインストール、アップグレード、または削除します。
- StoreFrontをインストールまたはアップグレードします。
- シングルセッションまたはマルチセッションオペレーティングシステム用のWindows VDAをインストールまたはアップグレードします。
- 印刷サーバーにUniversal Print Server `UpsServer` コンポーネントをインストールします。
- フェデレーション認証サービス をインストールします。
- Session Recording をインストールします。
- Workspace Environment Management をインストールします。

> **注:**
>
> Workspace Environment Management™ Agentインストーラーはローカライズされていません。英語でのみ利用可能です。

マルチセッションOSから1人のユーザー（Web開発など）にデスクトップを配信するには、製品版インストーラーのコマンドラインインターフェイスを使用します。詳細については、「サーバーVDI」を参照してください。

スタンドアロン VDA インストーラー

スタンドアロンVDAインストーラーは、Citrixダウンロードページから入手できます。（製品のインストールメディアからは入手できません。）スタンドアロンVDAインストーラーは、製品版ISOよりもはるかに小さくなっています。これらは、次のような展開に容易に対応できます。

- ステージングまたはローカルにコピーされた電子ソフトウェア配信（ESD）パッケージを使用する
- 物理マシンを使用する
- リモートオフィスを持つ

デフォルトでは、自己解凍型スタンドアロンVDAのファイルは**Temp**フォルダーに抽出されます。**Temp**フォルダーに抽出する場合、製品版インストーラーを使用する場合よりも多くのディスク容量がマシンに必要です。ただし、**Temp**フォルダーに抽出されたファイルは、インストール完了後に自動的に削除されます。または、絶対パスを指定して`/extract`コマンドを使用することもできます。

3つのスタンドアロンVDAインストーラーをダウンロードできます。

VDAServerSetup.exe:

マルチセッションOS用VDAをインストールします。製品版インストーラーで利用可能なマルチセッションOS用VDAのすべてのオプションをサポートします。

VDAWorkstationSetup.exe:

シングルセッションOS用VDAをインストールします。製品版インストーラーで利用可能なシングルセッションOS用VDAのすべてのオプションをサポートします。

VDAWorkstationCoreSetup.exe:

Remote PC Access展開またはコアVDIインストール用に最適化されたシングルセッションOS用VDAをインストールします。Remote PC Accessは物理マシンを使用します。コアVDIインストールは、イメージとして使用されていないVMです。このような展開のVDA接続に必要なコアサービスのみをインストールします。そのため、製品版または`VDAWorkstationSetup.exe`インストーラーで有効なオプションのサブセットのみをサポートします。

このインストーラーは、次の用途に使用されるコンポーネントをインストールまたは含みません。

- アップブイ。

- プロファイル管理。Citrixプロファイル管理をインストールから除外すると、Citrix Directorの表示に影響します。詳細については、「VDAのインストール」を参照してください。
- マシン アイデンティティ サービス。
- シトリックス サポービリティ ツール。
- シトリックス ファイルズ フォー ウィンドウズ。
- シトリックス ファイルズ フォー アウトルック。

`VDAWorkstationCoreSetup.exe`インストーラーは、Windows向けCitrix Workspaceアプリをインストールしたり、含んだりしません。

`VDAWorkstationCoreSetup.exe`を使用することは、フルプロダクトまたは`VDAWorkstationSetup`インストーラーを使用してシングルセッションOS VDAをインストールすることと等価であり、以下のいずれかに該当します。

- グラフィックインターフェイスの場合：**環境**ページでRemote PC Accessオプションを選択する。
- コマンドラインインターフェイスの場合：`/remotepc`オプションを指定する。
- コマンドラインインターフェイスの場合：`/components vda`と、有効な追加コンポーネント名をすべてリストする`/exclude`オプションを指定する。

省略されたコンポーネント/機能は、後でフルプロダクトインストーラーを実行してインストールできます。この操作により、不足しているすべてのコンポーネントをインストールできます。

`VDAWorkstationCoreSetup.exe` インストーラーは、Browser Content Redirection MSI を自動的にインストールします。この自動インストールは、VDA リリース 2003 以降のサポート対象リリースに適用されます。

Citrix インストールリターンコード

インストールログには、コンポーネントインストールの結果がMicrosoftの値ではなく、Citrixのリターンコードとして含まれています。

- 0 = 成功
- 1 = 失敗
- 2 = 部分的な成功
- 3 = 部分的な成功と再起動が必要
- 4 = 失敗と再起動が必要
- 5 = ユーザーがキャンセル

- 6 = 不正なコマンドライン引数
- 7 = 新しいバージョンが見つかりました
- 8 = 成功したが再起動が必要
- 9 = ファイルロックによる再起動
- 10 = 中止
- 11 = メディアの失敗
- 12 = ライセンスの失敗
- 13 = 事前チェックの失敗
- 14 = 再起動保留チェックにより中止

たとえば、Microsoft System Center Configuration Manager などのツールを使用する場合、インストールログにリターンコード3が含まれていると、スクリプトによるVDAインストールが失敗したように見えることがあります。これは、VDAインストーラーが、ユーザーが開始する必要がある再起動（たとえば、サーバーでのRDSロールの前提条件のインストール後など）を待機している場合に発生する可能性があります。VDAのインストールは、すべての前提条件と選択されたコンポーネントがインストールされ、インストール後にマシンが再起動された場合にのみ成功と見なされます。

または、インストールをCMDスクリプト（Microsoftの終了コードを返します）でラップするか、Configuration Managerパッケージの成功コードを変更することもできます。

Windows Serverワークロード向けにMicrosoft RDSライセンスサーバーを構成する

この製品は、Windows 2016などのWindows Serverワークロードを提供するときに、Windows Serverのリモートセッション機能にアクセスします。これには通常、Remote Desktop Servicesクライアントアクセスライセンス（RDS CAL）が必要です。VDAは、RDS CALを要求するためにRDSライセンスサーバーに接続できる必要があります。ライセンスサーバーをインストールしてアクティブ化します。詳しくは、Microsoftドキュメント「Remote Desktop Servicesライセンスサーバーをアクティブ化する」を参照してください。概念実証環境では、Microsoftが提供する猶予期間を使用できます。

この方法では、このサービスにライセンスサーバー設定を適用させることができます。イメージ上のRDSコンソールで、ライセンスサーバーとユーザーごとのモードを構成できます。Microsoftグループポリシー設定を使用してライセンスサーバーを構成することもできます。詳しくは、Microsoftドキュメント「クライアントアクセスライセンス（CAL）を使用してRDS展開をライセンスする」を参照してください。

グループポリシー設定を使用してRDSライセンスサーバーを構成するには:

1. 利用可能なマシンにRemote Desktop Servicesライセンスサーバーをインストールします。マシンは常に利用可能である必要があります。Citrix製品のワークロードは、このライセンスサーバーに到達できる必要があります。
2. Microsoftグループポリシーを使用して、ライセンスサーバーのアドレスとユーザーごとのライセンスモードを指定します。詳しくは、Microsoftドキュメント「RDセッションホストサーバーのリモートデスクトップライセンスモードを指定する」を参照してください。

Windows 10ワークロードには、適切なWindows 10ライセンスのアクティブ化が必要です。Windows 10ワークロードをアクティブ化するには、Microsoftのドキュメントに従うことをお勧めします。

詳細情報

特定のホストタイプの場所リソースを設定するには：

- AWSクラウド環境
- XenServer仮想化環境
- Google Cloud環境
- Microsoft Azure Resource Managerクラウド環境
- マイクロソフト システム センター コンフィギュレーション マネージャー 環境
- マイクロソフト System Center Virtual Machine Manager 仮想化環境
- Nutanix仮想化環境
- Nutanixクラウドおよびパートナーソリューション
- VMware 仮想化環境
- VMware クラウドおよびパートナーソリューション

AWSクラウド環境

この記事では、Citrix Virtual Apps and Desktops で使用できるリソースロケーションとして AWS アカウントを設定する手順を説明します。このリソースロケーションには、概念実証や、複数のアベイラビリティゾーンにリソースを分散させる必要のないその他の展開に最適な基本的なコンポーネントセットが含まれています。これらのタスクを完了すると、VDAs のインストール、マシンのプロビジョニング、マシンカタログの作成、およびデリバリーグループの作成が可能になります。

この記事のタスクを完了すると、リソースロケーションには次のコンポーネントが含まれます。

- 単一のアベイラビリティゾーン内にパブリックサブネットとプライベートサブネットを持つ仮想プライベートクラウド (VPC)。
- VPC のプライベートサブネットに配置され、Active Directory Domain Controller と DNS サーバーの両方として実行されるインスタンス。
- VPC のパブリックサブネットで踏み台ホストとして機能するインスタンス。このインスタンスは、管理目的でプライベートサブネット内のインスタンスへの RDP 接続を開始するために使用されます。リソースロケーションの設定が完了したら、このインスタンスをシャットダウンして、簡単にアクセスできないようにすることができます。プライベートサブネット内の他のインスタンス（VDA インスタンスなど）を管理する必要がある場合は、踏み台ホストインスタンスを再起動できます。

タスクの概要

パブリックサブネットとプライベートサブネットを持つ仮想プライベートクラウド (VPC) をセットアップします。 このタスクを完了すると、AWS はパブリックサブネットに Elastic IP address を持つ NAT gateway を展開します。これにより、プライベートサブネット内のインスタンスがインターネットにアクセスできるようになります。パブリックサブネット内のインスタンスはインバウンドのパブリックトラフィックにアクセスできますが、プライベートサブネット内のインスタンスはアクセスできません。

セキュリティグループを構成します。 セキュリティグループは、VPC 内のインスタンスのトラフィックを制御する仮想ファイアウォールとして機能します。パブリックサブネット内のインスタンスがプライベートサブネット内のインスタンスと通信できるようにするルールをセキュリティグループに追加します。また、これらのセキュリティグループを VPC 内の各インスタンスに関連付けます。

DHCP オプションセットを作成します。 Amazon VPC では、DHCP および DNS サービスがデフォルトで提供されており、これは Active Directory Domain Controller での DNS の構成方法に影響します。Amazon の DHCP は無効にできず、Amazon の DNS はパブリック DNS 解決にのみ使用でき、Active Directory 名解決には使用できません。DHCP を介してインスタンスに渡されるドメインとネームサーバーを指定するには、DHCP オプションセットを作成します。このセットは、Active Directory ドメインサフィックスを割り当て、VPC 内のすべてのインスタンスの DNS サーバーを指定します。インスタンスがドメインに参加したときに Host (A) and Reverse Lookup (PTR) records が自動的に登録されるようにするには、プライベートサブネットに追加する各インスタンスのネットワークアダプタープロパティを構成します。

踏み台ホストと Domain Controller を VPC に追加します。 踏み台ホストを介して、プライベートサブネット内のインスタンスにログオンし、ドメインを設定してインスタンスをドメインに参加させることができます。

タスク1: VPC をセットアップする

1. AWS 管理コンソールから、**VPC**を選択します。
2. VPC ダッシュボードから、**VPCを作成**を選択します。
3. **VPCなど**を選択します。
4. 「NATゲートウェイ ($)」の下で、「**In 1 AZ**」または「**1 per AZ**」を選択します。
5. 「DNSオプション」の下で、「**Enable DNS hostnames**」が選択されたままにします。
6. 「**Create VPC**」を選択します。AWSは、パブリックサブネットとプライベートサブネット、インターネットゲートウェイ、ルートテーブル、およびデフォルトのセキュリティグループを作成します。

タスク2：セキュリティグループの構成

このタスクでは、VPC用に以下のセキュリティグループを作成および構成します。

- パブリックサブネット内のインスタンスに関連付けるパブリックセキュリティグループ。
- プライベートサブネット内のインスタンスに関連付けるプライベートセキュリティグループ。

セキュリティグループを作成するには：

1. VPCダッシュボードで、「**Security Groups**」を選択します。
2. パブリックセキュリティグループ用のセキュリティグループを作成します。「**Create Security Group**」を選択し、グループの名前タグと説明を入力します。VPCで、以前に作成したVPCを選択します。「**Yes, Create**」を選択します。

パブリックセキュリティグループを構成する

1. セキュリティグループのリストから、パブリックセキュリティグループを選択します。
2. 「**Inbound Rules**」タブを選択し、「**Edit**」を選択して、以下のルールを作成します。

タイプ	送信元
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	パブリックセキュリティグループを選択します。
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0

タイプ	送信元
80 (HTTP)	0.0.0.0/0
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (セッションの信頼性)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. 完了したら、**保存**を選択します。
4. **アウトバウンドルール**タブを選択し、**編集**を選択して次のルールを作成します。

タイプ	送信先
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	0.0.0.0/0
ICMP	0.0.0.0/0

5. 完了したら、**保存**を選択します。

プライベートセキュリティグループを構成する

1. セキュリティグループリストから、プライベートセキュリティグループを選択します。
2. パブリックセキュリティグループからのトラフィックを設定していない場合は、TCPポートを設定する必要があります。「**インバウンドルール**」タブを選択し、「**編集**」を選択して、次のルールを作成します。

タイプ	送信元
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	パブリックセキュリティグループを選択します。

タイプ	送信元
ICMP	パブリックセキュリティグループを選択します。
TCP 53 (DNS)	パブリックセキュリティグループを選択します。
UDP 53 (DNS)	パブリックセキュリティグループを選択します。
80 (HTTP)	パブリックセキュリティグループを選択します。
TCP 135	パブリックセキュリティグループを選択します。
TCP 389	パブリックセキュリティグループを選択します。
UDP 389	パブリックセキュリティグループを選択します。
443 (HTTPS)	パブリックセキュリティグループを選択します。
TCP 1494 (ICA/HDX)	パブリックセキュリティグループを選択します。
TCP 2598 (セッションの信頼性)	パブリックセキュリティグループを選択します。
3389 (RDP)	パブリックセキュリティグループを選択します。
TCP 49152–65535	「パブリックセキュリティグループ」を選択します。

3. 完了したら、「**保存**」を選択します。
4. 「**アウトバウンドルール**」タブを選択し、「**編集**」を選択して、次のルールを作成します。

タイプ	宛先
すべてのトラフィック	「プライベートセキュリティグループ」を選択します。
すべてのトラフィック	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

5. 完了したら、「**保存**」を選択します。

タスク 3: インスタンスの起動

2つのEC2インスタンスを作成し、Amazonが生成するデフォルトの管理者パスワードを復号化するには、次の手順を実行します。

1. AWS管理コンソールから、**EC2**を選択します。
2. EC2ダッシュボードから、**インスタンスの起動**を選択します。
3. Windows Serverマシンイメージとインスタンスタイプを選択します。
4. **インスタンスの詳細の設定**ページで、インスタンスの名前を入力し、以前に設定したVPCを選択します。
5. **サブネット**で、各インスタンスについて次の選択を行います。
   - Bastionホスト：パブリックサブネットを選択します
   - ドメインコントローラー：プライベートサブネットを選択します
6. **パブリックIPの自動割り当て**で、各インスタンスについて次の選択を行います。
   - 踏み台ホスト: **有効**を選択します。
   - ドメインコントローラー: **デフォルト設定を使用**または**無効**を選択します。
7. **ネットワークインターフェイス**で、ドメインコントローラーのプライベートサブネットのIP範囲内でプライマリIPアドレスを入力します。
8. 必要に応じて、**ストレージの追加**ページでディスクサイズを変更します。
9. **インスタンスのタグ付け**ページで、各インスタンスにわかりやすい名前を入力します。
10. 「**セキュリティグループの設定**」ページで、「**既存のセキュリティグループを選択**」を選択し、各インスタンスについて次の選択を行います。

- バスティオンホスト: パブリックセキュリティグループを選択します。
- ドメインコントローラー: プライベートセキュリティグループを選択します。

11. 選択内容を確認し、「**起動**」を選択します。
12. 新しいキーペアを作成するか、既存のキーペアを選択します。新しいキーペアを作成する場合は、秘密鍵 (.pem) ファイルをダウンロードして安全な場所に保管してください。インスタンスのデフォルトの管理者パスワードを取得する際には、秘密鍵を提供する必要があります。
13. 「**インスタンスの起動**」を選択します。「**インスタンスの表示**」を選択して、インスタンスのリストを表示します。新しく起動したインスタンスがすべてのステータスチェックに合格するまで待ってからアクセスしてください。
14. 各インスタンスのデフォルトの管理者パスワードを取得します。
    a. インスタンスリストからインスタンスを選択し、「**接続**」を選択します。
    b. 「**RDPクライアント**」タブに移動し、「**パスワードの取得**」を選択し、プロンプトが表示されたら秘密鍵 (`.pem`) ファイルをアップロードします。
    c. 「**パスワードの復号**」を選択して、人間が読めるパスワードを取得します。AWSがデフォルトのパスワードを表示します。
15. ステップ2から繰り返して、2つのインスタンスを作成します。
    - パブリックサブネット内のBastionホストインスタンス1つ
    - プライベートサブネット内の、ドメインコントローラーとして使用するインスタンス1つ。

タスク4：DHCPオプションセットを作成する

1. VPCダッシュボードから、「**DHCPオプションセット**」を選択します。
2. 次の情報を入力します。
    - 名前タグ: セットのわかりやすい名前を入力します。
    - ドメイン名: ドメインコントローラーインスタンスを構成するときに使用する完全修飾ドメイン名を入力します。
    - ドメインネームサーバー: ドメインコントローラーインスタンスに割り当てたプライベートIPアドレスと、コンマで区切られた文字列 **AmazonProvidedDNS** を入力します。
    - NTPサーバー: このフィールドは空白のままにします。
    - NetBIOSネームサーバー: ドメインコントローラーインスタンスのプライベートIPアドレスを入力します。
    - NetBIOSノードタイプ: **2** と入力します。

3. **はい、作成**を選択します。
4. 新しいセットをVPCに関連付けます。
    a. VPCダッシュボードから、**Your VPCs**を選択し、以前に設定したVPCを選択します。
    b. **アクション > DHCPオプションセットの編集**を選択します。
    c. プロンプトが表示されたら、作成した新しいセットを選択し、「**保存**」を選択します。

タスク5: インスタンスを構成する

1. RDPクライアントを使用して、踏み台ホストインスタンスのパブリックIPアドレスに接続します。プロンプトが表示されたら、管理者アカウントの資格情報を入力します。
2. 踏み台ホストインスタンスからリモートデスクトップ接続を起動し、構成するインスタンスのプライベートIPアドレスに接続します。プロンプトが表示されたら、インスタンスの管理者資格情報を入力します。
3. プライベートサブネット内のすべてのインスタンスについて、DNS設定を構成します。
    a. **スタート > コントロールパネル > ネットワークとインターネット > ネットワークと共有センター > アダプターの設定の変更**を選択します。表示されているネットワーク接続をダブルクリックします。
    b. **プロパティ > インターネットプロトコルバージョン4 (TCP/IPv4) > プロパティ**を選択します。
    c. 「**詳細設定 > DNS**」を選択します。次の設定が有効になっていることを確認し、「**OK**」を選択します。
        - この接続のアドレスをDNSに登録する
        - この接続のDNSサフィックスをDNS登録で使用する
4. ドメインコントローラーを構成するには:
    a. Server Manager を使用して、Active Directory ドメインサービス の役割をすべてのデフォルト機能とともに追加します。
    b. インスタンスをドメインコントローラーに昇格させます。昇格中にDNSを有効にし、DHCPオプションセットを作成したときに指定したドメイン名を使用します。プロンプトが表示されたらインスタンスを再起動します。

次のステップ

- コアコンポーネントをインストールする
- VDAのインストール

- サイトを作成する
- AWS での接続の作成と管理については、AWS への接続を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

XenServer® 仮想化環境

XenServer は運用管理を簡素化し、負荷の高いワークロードでも高精細なユーザーエクスペリエンスを保証します。

XenServer をセットアップするには、「インストール準備」を参照してください。

次に行うこと

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- XenServer で接続を作成および管理する方法については、「XenServer への接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Google Cloud環境

Citrix Virtual Apps and Desktops™ を使用すると、Google Cloud 上でマシンをプロビジョニングおよび管理できます。

要件

- Citrix Cloud™ アカウント。この記事で説明されている機能は、Citrix Cloud でのみ利用できます。
- Google Cloud プロジェクト。このプロジェクトには、マシンカタログに関連付けられているすべてのコンピューティングリソースが保存されます。既存のプロジェクトでも新規のプロジェクトでもかまいません。

- Google Cloud プロジェクトで4つのAPIを有効にします。詳細については、「Google Cloud APIを有効にする」を参照してください。
- Google Cloud サービスアカウント。サービスアカウントはGoogle Cloudに対して認証を行い、プロジェクトへのアクセスを有効にします。詳細については、「サービスアカウントの構成と更新」を参照してください。
- Googleプライベートアクセスを有効にします。詳細については、「Googleプライベートアクセスを有効にする」を参照してください。

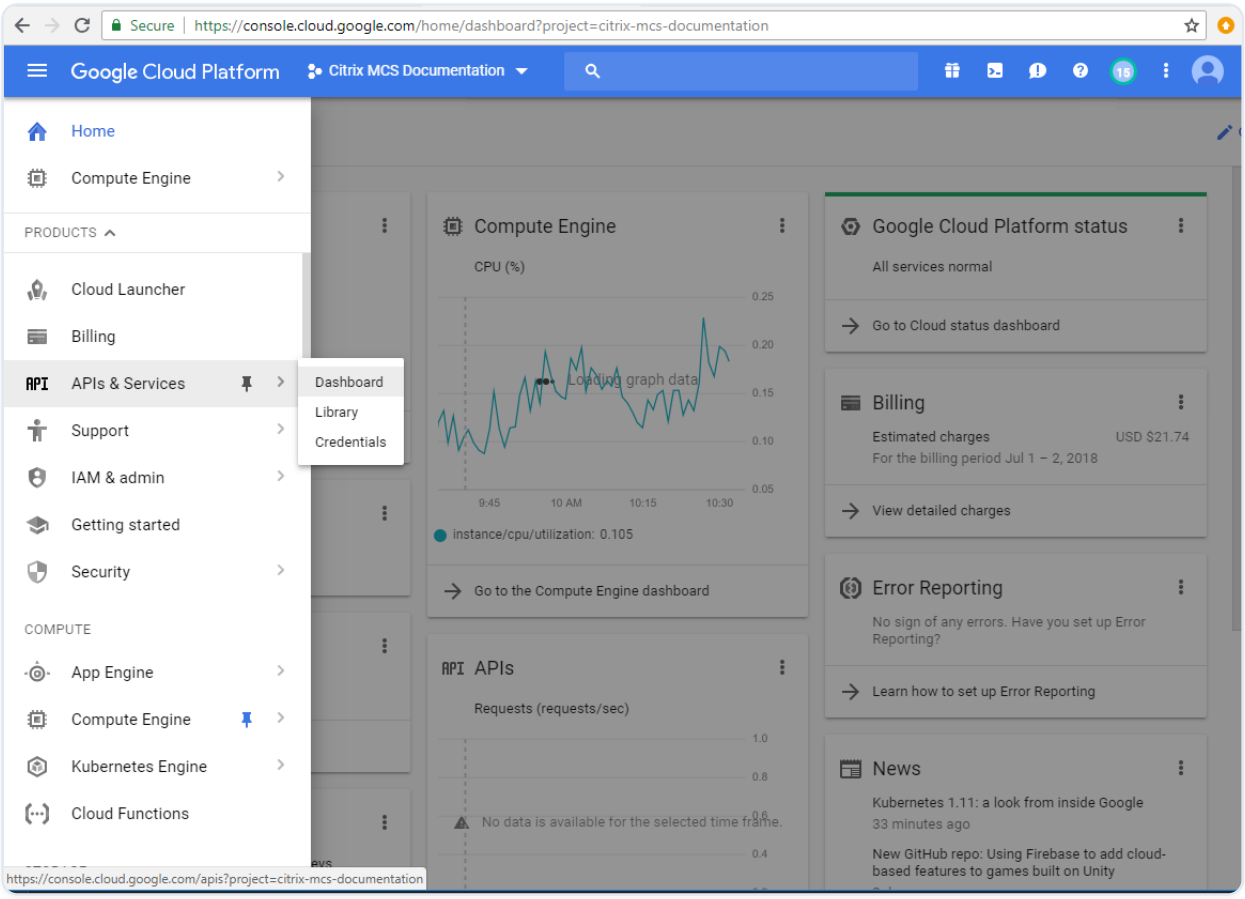
Google Cloud APIを有効にする

Web Studioを介してGoogle Cloud機能を使用するには、Google Cloudプロジェクトで次のAPIを有効にします。

- コンピュートエンジン API
- クラウド リソース マネージャー API
- ID およびアクセス管理 (IAM) API
- クラウド ビルド API
- クラウド キー管理サービス (KMS)

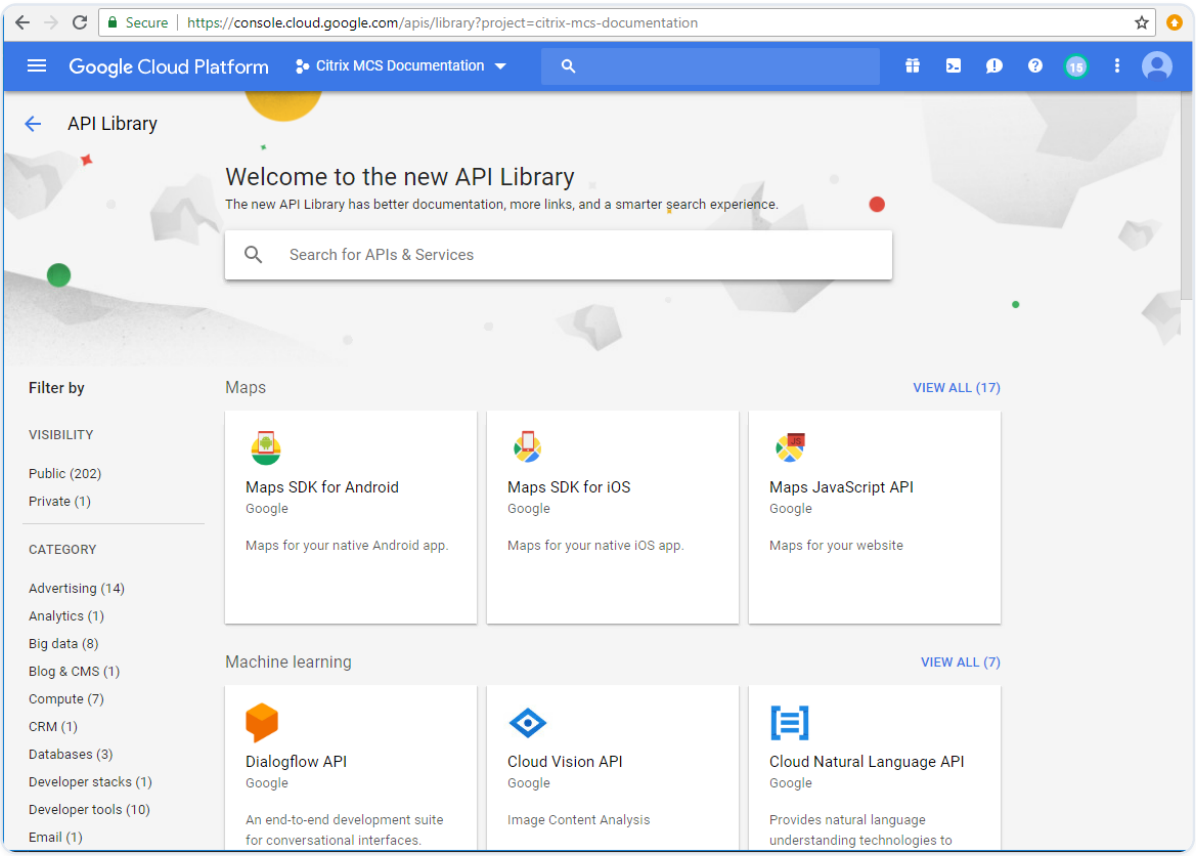
Google Cloudコンソールから、次の手順を実行します。

1. 左上のメニューで、**「APIとサービス」>「ダッシュボード」**を選択します。



2. 「**ダッシュボード**」画面で、Compute Engine API が有効になっていることを確認します。有効になっていない 場合は、次の手順に従います。

   a. 「**APIとサービス > ライブラリ**」に移動します。



b. 検索ボックスに「*Compute Engine*」と入力します。

c. 検索結果から「**Compute Engine API**」を選択します。

d. 「**Compute Engine API**」ページで、「**有効にする**」を選択します。

3. Cloud Resource Manager APIを有効にします。

a. 「**APIとサービス > ライブラリ**」に移動します。

b. 検索ボックスに「*Cloud Resource Manager*」と入力します。

c. 検索結果から「**Cloud Resource Manager API**」を選択します。

d. 「**Cloud Resource Manager API**」ページで、「**有効にする**」を選択します。APIのステータスが表示されます。

4. 同様に、**Identity and Access Management (IAM) API**と**Cloud Build API**を有効にします。

Google Cloud Shell を使用して API を有効にすることもできます。これを行うには、次の手順を実行します。

1. Googleコンソールを開き、Cloud Shellをロードします。
2. Cloud Shellで次の4つのコマンドを実行します。

- gcloud services enable compute.googleapis.com を実行します。

- gcloud services enable cloudresourcemanager.googleapis.com を実行します。
- gcloud services enable iam.googleapis.com を実行します。
- gcloud services enable cloudbuild.googleapis.com を実行します。

3. Cloud Shellがプロンプトを表示した場合、「**承認**」をクリックします。

サービスアカウントの構成と更新

> **注:**
>
> GCP は、Cloud Build Service のデフォルトの動作とサービスアカウントの使用に関して、April 29, 2024 以降に変更を導入します。詳細については、「Cloud Build Service Account Change」を参照してください。April 29, 2024 より前に Cloud Build API が有効になっている既存の Google プロジェクトは、この変更の影響を受けません。ただし、April 29 以降も既存の Cloud Build Service の動作を維持したい場合は、Cloud Build API を有効にする前に、組織ポリシーを作成または適用して制約の適用を無効にすることができます。その結果、以下のコンテンツは「Before April 29, 2024」と「After April 29, 2024」の2つに分かれています。新しい組織ポリシーを設定した場合は、「Before April 29, 2024」のセクションに従ってください。

April 29, 2024 以前

Citrix Cloudは、Google Cloudプロジェクト内で3つの個別のサービスアカウントを使用します。

- *Citrix Cloudサービスアカウント*: このサービスアカウントにより、Citrix CloudはGoogleプロジェクトにアクセスし、マシンをプロビジョニングおよび管理できます。このサービスアカウントは、Google Cloudによって生成されたキーを使用してGoogle Cloudに認証します。

  ここに概説されているように、このサービスアカウントを手動で作成する必要があります。詳細については、Citrix Cloudサービスアカウントの作成を参照してください。

  このサービスアカウントは、メールアドレスで識別できます。例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`。
- *Cloud Build サービスアカウント*: このサービスアカウントは、Google Cloud API を有効にするで言及されているすべての API を有効にすると、自動的にプロビジョニングされます。自動的に作成されたすべてのサービスアカウントを表示するには、**Google Cloud** コンソールで **IAM と管理 > IAM** に移動し、**Google 提供のロール付与を含める**チェックボックスを選択します。

このサービスアカウントは、**プロジェクト ID** と **cloudbuild** という単語で始まるメールアドレスで識別できます。例: `<project-id>@cloudbuild.gserviceaccount.com`

サービスアカウントに次のロールが付与されていることを確認します。ロールを追加する必要がある場合は、Cloud Build サービスアカウントにロールを追加する に記載されている手順に従ってください。

- Cloud Build サービスアカウント
- Compute インスタンス管理者
- サービスアカウントユーザー

- *Cloud Compute サービスアカウント*: このサービスアカウントは、Compute API がアクティブ化されると、Google Cloud によって Google Cloud で作成されたインスタンスに追加されます。このアカウントには、操作を実行するための IAM 基本編集者ロールがあります。ただし、よりきめ細かな制御を行うためにデフォルトの権限を削除した場合、次の権限を必要とする **ストレージ管理者** ロールを追加する必要があります。
  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

このサービスアカウントは、**プロジェクト ID** と **compute** という単語で始まるメールアドレスで識別できます。例: `<project-id>-compute@developer.gserviceaccount.com`。

CITRIX CLOUD サービスアカウントを作成する

Citrix Cloud サービスアカウントを作成するには、次の手順に従います。

1. Google Cloud コンソールで、**IAM と管理 > サービスアカウント**に移動します。
2. **サービスアカウント**ページで、**サービスアカウントを作成**を選択します。
3. **サービスアカウントの作成**ページで、必要な情報を入力し、**作成して続行**を選択します。
4. **このサービスアカウントにプロジェクトへのアクセスを許可**ページで、**ロールを選択**ドロップダウンメニューをクリックし、必要なロールを選択します。さらにロールを追加する場合は、**+別のロールを追加**をクリックします。

   各アカウント（個人またはサービス）には、プロジェクトの管理を定義するさまざまなロールがあります。このサービスアカウントには、以下のロールを付与してください。

   - Compute 管理者

- Storage管理者
- Cloud Build編集者
- サービスアカウントユーザー
- クラウド データストア ユーザー
- Cloud KMS 暗号化オペレーター

Cloud KMS 暗号オペレーターには、以下の権限が必要です。

- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.get
- cloudkms.keyRings.list
- cloudkms.cryptoKeyVersions.useToDecrypt
- cloudkms.cryptoKeyVersions.useToEncrypt

> **注:**
>
> 新しいサービスアカウントを作成する際に利用可能なロールの完全なリストを取得するには、すべてのAPIを有効にしてください。

5. **CONTINUE**をクリックします
6. **Grant users access to this service account**ページで、ユーザーまたはグループを追加して、このサービスアカウントでアクションを実行するアクセス権を付与します。
7. **DONE**をクリックします。
8. IAMメインコンソールに移動します。
9. 作成されたサービスアカウントを特定します。
10. ロールが正常に割り当てられていることを検証します。

考慮事項:

サービスアカウントを作成する際は、以下を考慮してください。

- **Grant this service account access to project**および**Grant users access to this service account**の手順はオプションです。これらのオプションの構成手順をスキップすることを選択

した場合、新しく作成されたサービスアカウントは**IAM & Admin > IAM**ページに表示されません。

- サービスアカウントに関連付けられたロールを表示するには、オプションの手順をスキップせずにロールを追加します。このプロセスにより、構成されたサービスアカウントにロールが表示されるようになります。

CITRIX CLOUDサービスアカウントキー

Citrix DaaSで接続を作成するには、Citrix Cloudサービスアカウントキーが必要です。キーは資格情報ファイル（.json）に含まれています。キーを作成すると、ファイルは自動的にダウンロードされ、**ダウンロード**フォルダーに保存されます。キーを作成する際は、キータイプをJSONに設定してください。そうしないと、Web Studioがそれを解析できません。

サービスアカウントキーを作成するには、**IAMと管理 > サービスアカウント**に移動し、Citrix Cloudサービスアカウントのメールアドレスをクリックします。**キー**タブに切り替え、**キーを追加 > 新しいキーを作成**を選択します。キータイプとして**JSON**を選択していることを確認してください。

> **ヒント:**
>
> Google Cloud コンソールで、**サービスアカウント**ページを使用してキーを作成します。セキュリティ上の理由から、キーを定期的に変更することをお勧めします。既存の Google Cloud 接続を編集することで、Citrix Virtual Apps and Desktops アプリケーションに新しいキーを提供できます。

CITRIX CLOUD サービスアカウントにロールを追加する

Citrix Cloud サービスアカウントにロールを追加するには、次の手順を実行します。

1. Google Cloud コンソールで、**IAM と管理 > IAM** に移動します。
2. **IAM > 権限**ページで、作成したサービスアカウントを電子メールアドレスで特定し、見つけます。

   例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. 鉛筆アイコンを選択して、サービスアカウントのプリンシパルへのアクセスを編集します。
4. 選択したプリンシパルオプションの**「project-id」へのアクセスを編集**ページで、**別の役割を追加**を選択して必要な役割をサービスアカウントに1つずつ追加し、**保存**を選択します。

CLOUD BUILD サービスアカウントにロールを追加する

Cloud Build サービスアカウントにロールを追加するには、次の手順を実行します。

1. Google Cloudコンソールで、**IAMと管理 > IAM**に移動します。
2. 「**IAM**」ページで、**プロジェクトID**と「**cloudbuild**」という単語で始まるメールアドレスで識別できるCloud Buildサービスアカウントを見つけます。

   例: `<project-id>@cloudbuild.gserviceaccount.com`
3. 鉛筆アイコンを選択して、Cloud Build アカウントのロールを編集します。
4. 選択したプリンシパルオプションの**「"project-id"へのアクセスを編集」ページで、「別のロールを追加」を選択して、必要なロールをCloud Buildサービスアカウントに1つずつ追加し、「保存」**を選択します。

   > **注:**
   >
   > すべてのAPIを有効にして、ロールの完全なリストを取得します。

April 29, 2024 以降

Citrix Cloudは、Google Cloudプロジェクト内で2つの異なるサービスアカウントを使用します。

- *Citrix Cloudサービスアカウント*: このサービスアカウントにより、Citrix CloudはGoogleプロジェクトにアクセスし、マシンをプロビジョニングおよび管理できます。このサービスアカウントは、Google Cloudによって生成されたキーを使用してGoogle Cloudに認証されます。

  このサービスアカウントは手動で作成する必要があります。

  このサービスアカウントは、メールアドレスで識別できます。例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`。
- *Cloud Computeサービスアカウント*: このサービスアカウントは、Google Cloud APIを有効にするで言及されているすべてのAPIを有効にすると自動的にプロビジョニングされます。自動的に作成されたすべてのサービスアカウントを表示するには、**Google Cloud**コンソールで「**IAMと管理 > IAM**」に移動し、「**Google提供の役割付与を含める**」チェックボックスを選択します。このアカウントには、操作を実行するためのIAM基本編集者ロールがあります。ただし、より詳細な制御のためにデフォルトの権限を削除した場合、次の権限を必要とする**Storage Admin**ロールを追加する必要があります。
  - resourcemanager.projects.get

- storage.objects.create
- storage.objects.get
- storage.objects.list

このサービスアカウントは、**プロジェクトID**と**compute**という単語で始まるメールアドレスで識別できます。例：`<project-id>-compute@developer.gserviceaccount.com.`.

サービスアカウントに次のロールが付与されていることを確認します。

- Cloud Build サービスアカウント
- Compute Instance 管理者
- サービスアカウントユーザー

CITRIX CLOUD サービスアカウントを作成する

Citrix Cloud サービスアカウントを作成するには、次の手順に従います。

1. Google Cloud コンソールで、 **>** に移動します。
2. ページで、 を選択します。
3. ページで、必要な情報を入力し、 を選択します。
4. ページで、 ドロップダウンメニューをクリックし、必要なロールを選択します。さらにロールを追加する場合は、 をクリックします。

   各アカウント（個人またはサービス）には、プロジェクトの管理を定義するさまざまなロールがあります。このサービスアカウントに以下のロールを付与します。

   - Compute 管理者
   - Storage 管理者
   - Cloud Build 編集者
   - サービスアカウントユーザー
   - クラウド データストア ユーザー
   - Cloud KMS 暗号オペレーター

   Cloud KMS 暗号オペレーターには、次の権限が必要です。

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get

- cloudkms.keyRings.list

> **注:**
>
> 新しいサービスアカウントを作成する際に利用可能なロールの完全なリストを取得するには、すべてのAPIを有効にします。

5. **続行**をクリックします
6. **このサービスアカウントへのユーザーアクセスを許可**ページで、ユーザーまたはグループを追加して、このサービスアカウントでアクションを実行するアクセス権を付与します。
7. **完了**をクリックします。
8. IAMメインコンソールに移動します。
9. 作成されたサービスアカウントを特定します。
10. ロールが正常に割り当てられていることを検証します。

考慮事項:

サービスアカウントを作成する際は、以下を考慮してください。

- 手順**このサービスアカウントにプロジェクトへのアクセスを許可する**および**このサービスアカウントにユーザーアクセスを許可する**はオプションです。これらのオプションの構成手順をスキップすることを選択した場合、新しく作成されたサービスアカウントは**IAMと管理 > IAM**ページに表示されません。
- サービスアカウントに関連付けられたロールを表示するには、オプションの手順をスキップせずにロールを追加します。このプロセスにより、構成されたサービスアカウントにロールが表示されるようになります。

CITRIX CLOUDサービスアカウントキー

Citrix Cloudサービスアカウントキーは、Citrix DaaSで接続を作成するために必要です。キーは資格情報ファイル（.json）に含まれています。キーを作成すると、ファイルは自動的にダウンロードされ、**ダウンロード**フォルダーに保存されます。キーを作成する際は、キータイプをJSONに設定してください。そうしないと、Web Studioはそれを解析できません。

サービスアカウントキーを作成するには、**IAMと管理 > サービスアカウント**に移動し、Citrix Cloudサービスアカウントのメールアドレスをクリックします。**キー**タブに切り替え、**キーを追加 > 新しいキーを作成**を選択します。キータイプとして**JSON**が選択されていることを確認してください。

ヒント:

Google Cloudコンソールの**サービスアカウント**ページを使用してキーを作成します。セキュリティ上の理由から、キーを定期的に変更することをお勧めします。既存のGoogle Cloud接続を編集することで、新しいキーをCitrix Virtual Apps and Desktopsアプリケーションに提供できます。

CITRIX CLOUD サービスアカウントにロールを追加する

Citrix Cloud サービスアカウントにロールを追加するには、次の手順を実行します。

1. Google Cloud コンソールで、**IAM と管理 > IAM** に移動します。
2. **IAM > 権限**ページで、作成したサービスアカウントを電子メールアドレスで特定し、見つけます。

   例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. 鉛筆アイコンを選択して、サービスアカウントのプリンシパルへのアクセスを編集します。
4. 選択したプリンシパルオプションの「**"project-id"へのアクセスを編集**」ページで、「**別のロールを追加**」を選択して、必要なロールをサービスアカウントに1つずつ追加し、次に「**保存**」を選択します。

CLOUD COMPUTE SERVICE ACCOUNT にロールを追加する

Cloud Compute Service Account にロールを追加するには、次の手順を実行します。

1. Google Cloudコンソールで、「**IAMと管理 > IAM**」に移動します。
2. 「**IAM**」ページで、Cloud Computeサービスアカウントを見つけます。これは、**プロジェクトID**と「**compute**」という単語で始まるメールアドレスで識別できます。

   例えば、`<project-id>-compute@developer.gserviceaccount.com`
3. 鉛筆アイコンを選択して、Cloud Buildアカウントのロールを編集します。
4. 選択したプリンシパルオプションの「**"project-id"へのアクセスを編集**」ページで、「**別のロールを追加**」を選択して、必要なロールをCloud Buildサービスアカウントに1つずつ追加し、次に「**保存**」を選択します。

注:

すべてのAPIを有効にして、ロールの完全なリストを取得します。

ストレージの権限とバケット管理

Citrix Virtual Apps and Desktopsは、Google Cloudサービスのクラウドビルド失敗のレポートプロセスを改善します。このサービスはGoogle Cloudでビルドを実行します。Citrix Virtual Apps and Desktopsは、Google Cloudサービスがビルドログ情報をキャプチャする`citrix-mcs-cloud-build-logs-{region}-{5 random characters}`という名前のストレージバケットを作成します。このバケットには、30日後にコンテンツを削除するオプションが設定されています。このプロセスでは、接続に使用されるサービスアカウントに`storage.buckets.update`に設定されたGoogle Cloud権限が必要です。サービスアカウントにこの権限がない場合、Citrix Virtual Apps and Desktopsはエラーを無視し、カタログ作成プロセスを続行します。この権限がないと、ビルドログのサイズが増加し、手動でのクリーンアップが必要になります。

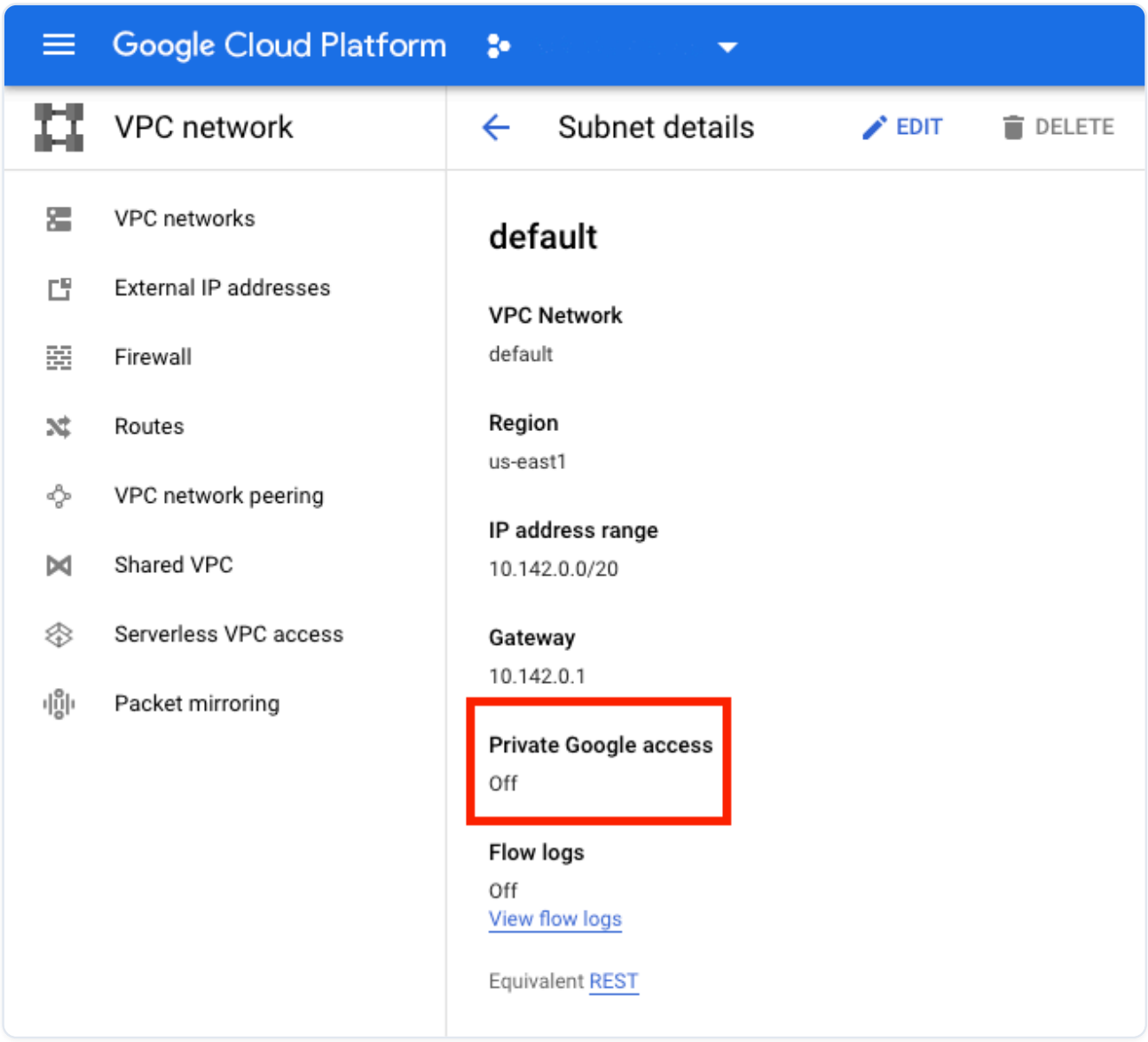
プライベート Google アクセスを有効にする

VM のネットワークインターフェイスに外部 IP アドレスが割り当てられていない場合、パケットは他の内部 IP アドレスの宛先にのみ送信されます。プライベートアクセスを有効にすると、VM は Google API および関連サービスで使用される外部 IP アドレスのセットに接続します。

> **注:**
>
> プライベート Google アクセスが有効になっているかどうかにかかわらず、パブリック IP アドレスを持つ VM と持たない VM の両方が、特にサードパーティのネットワークアプライアンスが環境にインストールされている場合、Google Public API にアクセスできる必要があります。

MCSプロビジョニングのために、サブネット内のVMがパブリックIPアドレスなしでGoogle APIにアクセスできるようにするには、次の手順を実行します。

1. Google Cloudで、**VPC network configuration**にアクセスします。
2. サブネットの詳細画面で、「**Private Googleアクセス**」をオンにします。



詳細については、「Configuring Private Google Access」を参照してください。

> **重要:**
>
> ネットワークがVMのインターネットアクセスを防止するように構成されている場合、VMが接続されているサブネットに対してPrivate Googleアクセスを有効にすることに関連するリスクを組織が負うことを確認してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成

- Google Cloud 環境での接続の作成と管理については、「Google Cloud 環境への接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

HPE Moonshot 仮想化環境

Citrix Virtual Apps and Desktops™ は、Citrix 管理の HPE Moonshot プラグインを介して HPE Moonshot ワークロードを管理します。このプラグインを使用すると、HPE Moonshot シャーシへの接続の作成、カタログの作成、およびカタログ内のマシンの電源管理を行うことができます。

要件

Citrix 管理の HPE Moonshot プラグインを Delivery Controller にインストールします。

> **注：**
>
> - Citrix 管理と HPE 管理の両方の HPE Moonshot プラグインがインストールされている場合、Delivery Controller は Citrix 管理の HPE Moonshot プラグインを使用します。
> - Citrix 管理と HPE 管理の両方の HPE Moonshot プラグインがインストールされており、HPE 管理の Moonshot プラグインを使用したい場合は、Citrix 管理の HPE Moonshot プラグインをアンインストールし、`RegisterPlugin` キャッシュを更新してください。

Citrix 管理の HPE Moonshot プラグインをインストールする

Citrix 管理の HPE Moonshot プラグインをインストールするには、次の手順を実行します。

1. `E:\x64\Citrix Desktop Delivery Controller\MoonshotPlugin`.msi をインストールします。`E:\` は ISO です。
2. PowerShell を管理者として開き、次のコマンドを実行します。

   ```
   C:\Program Files\Common Files\Citrix\HCLPlugins> .\RegisterPlugins.exe
   -pluginsroot .\CitrixMachineCreation\v1.0.0.0\
   ```

3. プラグインの登録が成功したら、**タスクマネージャー**から次のサービスを再起動します。

a. CitrixBrokerService
b. CitrixHostService
c. CitrixMachineCreationService

4. デリバリーコントローラーにプラグインがインストールされているかを確認するには、`Get-HypHypervisorPlugins`を実行します。出力の**DisplayName**フィールドには、**HPE Moonshot**と表示される必要があります。

Citrix 管理の HPE Moonshot プラグインをアンインストールし、RegisterPlugin キャッシュを更新する

Citrix管理とHPE管理の両方のHPE Moonshotプラグインがインストールされており、HPE管理のMoonshotプラグインを使用したい場合は、Citrix管理のHPE Moonshotプラグインをアンインストールし、`RegisterPlugin`キャッシュを更新する必要があります。そのためには：

1. Citrix管理のHPE Moonshotプラグインをアンインストールします。
2. 管理者としてPowerShellを開き、次のコマンドを実行します。

```
cd `C:\Program Files\Common Files\Citrix\HCLPlugins\`

C:\Program Files\Common Files\Citrix\HCLPlugins> .\RegisterPlugins.exe
-PluginsRoot ` C:\Program Files\Common
Files\Citrix\HCLPlugins\ManagedMachine\v2.5.0.0\`
```

3. プラグインの登録が成功したら、**タスクマネージャー**から次のサービスを再起動します。

a. CitrixBrokerService
b. CitrixHostService
c. CitrixMachineCreationService

4. デリバリーコントローラーにプラグインがインストールされているかを確認するには、`Get-HypHypervisorPlugins`を実行します。出力の**DisplayName**フィールドには、**HPE Moonshot Machine Manager**と表示される必要があります。

主な手順

1. HPE環境を設定します。
2. HPE Moonshotシャーシへの接続を作成します。
3. マシンカタログを作成します。

> **注:**
>
> カタログを作成する前に、1 つ以上の HPE Moonshot カートリッジノードがあることを確認し、それらのノードに VDA をインストールしてください。HPE Moonshot シャーシをハイパーバイザー、カートリッジノードを VM と考えることができます。

4. デリバリーグループを作成します。
5. 管理されていない残りの HPE Moonshot ノードを、管理対象のカタログまたはデリバリーグループに移行します。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- HPE Moonshotで接続を作成および管理する方法については、「HPE Moonshotへの接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Microsoft Azure Resource Manager クラウド環境

Citrix Virtual Apps and Desktops™ 展開環境で Microsoft Azure Resource Manager を使用して仮想マシンをプロビジョニングする場合は、以下の点について理解を深めてください。

- アジュール アクティブ ディレクトリ：`<https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-whatis/>`
- 同意フレームワーク: `<https://docs.microsoft.com/ja-jp/azure/active-directory/manage-apps/plan-an-application-integration>`
- サービスプリンシパル: `<https://docs.microsoft.com/ja-jp/azure/active-directory/develop/app-objects-and-service-principals/>`

Microsoft Azure Resource Manager をセットアップするには、インストール準備 を参照してください。

次のステップ

- コアコンポーネントのインストール
- VDA のインストール
- サイトの作成
- Azure 環境で接続を作成および管理するには、Microsoft Azure への接続 を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成
- CTX219211: Microsoft Azure Active Directory アカウントをセットアップする
- CTX219243: XenApp および XenDesktop に Azure サブスクリプションへのアクセスを許可する
- CTX219271: サイト間 VPN を使用してハイブリッドクラウドを展開する

マイクロソフト システムセンター コンフィギュレーションマネージャー 環境

アプリケーションとデスクトップへのアクセスを管理するためにMicrosoft System Center Configuration Manager (Configuration Manager)を使用しているサイトは、次のオプションを使用してその使用をCitrix Virtual Apps and Desktops™に拡張できます。

- SCCM を使用した VDA のインストール。
- **Configuration Manager Wake Proxy 機能：** Remote PC Access の Wake on LAN 機能は Configuration Manager でサポートされています。詳細については、「Wake on LAN - SCCM 統合」を参照してください。
- **Citrix Virtual Apps and Desktops のプロパティ：** プロパティを使用すると、Configuration Manager を介して管理する Citrix Virtual Desktops™ を識別できます。（一部のバージョンでは、Configuration Manager は Citrix Virtual Apps and Desktops の旧称である XenApp and XenDesktop を使用します。）

プロパティ

仮想デスクトップを管理するためのプロパティは、Microsoft System Center Configuration Manager で利用できます。

Configuration Manager に表示されるブール型プロパティは、true または false ではなく、`1` または `0` として表示されます。

プロパティは、`Root\Citrix\DesktopInformation` 名前空間の `Citrix_virtualDesktopInfo` クラスで利用できます。プロパティ名は、Windows Management Instrumentation (WMI) プロバイダーから取得されます。

プロパティ	説明
`AssignmentType`	IsAssigned の値を設定します。有効な値は、`ClientIP`、`ClientName`、`None`、および `User` です（`IsAssigned` を `True` に設定します）。
`BrokerSiteName`	`HostIdentifier` と同じ値を返します。
`DesktopCatalogName`	デスクトップに関連付けられているマシンカタログ。
`DesktopGroupName`	デスクトップに関連付けられているデリバリーグループ。
`HostIdentifier`	`BrokerSiteName`と同じ値を返します。
`IsAssigned`	デスクトップをユーザーに割り当てる場合は `True`、ランダムなデスクトップの場合は `False`に設定します。
`IsMasterImage`	環境に関する決定を可能にします。たとえば、プロビジョニングされたマシンではなく、イメージにアプリケーションをインストールします。有効な値は次のとおりです。イメージとして使用されるVM上の`True`。この値は、選択に基づいてインストール中に設定されるか、そのイメージからプロビジョニングされたVM上でクリアされます。
`IsVirtualMachine`	仮想マシンの場合は`True`、物理マシンの場合は`false`。
`OSChangesPersist`	デスクトップオペレーティングシステムイメージが再起動のたびにクリーンな状態にリ

プロパティ	説明
	セットされる場合は`False`。それ以外の場合は`true`。
`PersistentDataLocation`	Configuration Managerが永続データを保存する場所。これはユーザーにはアクセスできません。
`BrokerSiteName`, `DesktopCatalogName`, `DesktopGroupName`, `HostIdentifier`	デスクトップがControllerに登録されたときに決定されます。完全に登録されていないデスクトップの場合、これらはnullです。

プロパティを収集するには、Configuration Managerでハードウェアインベントリを実行します。プロパティを表示するには、Configuration Manager Resource Explorerを使用します。これらの場合、名前にはスペースが含まれるか、プロパティ名とわずかに異なります。たとえば、`BrokerSiteName` は `Broker Site Name` として表示されます。

- Citrix VDA から Citrix WMI プロパティを収集するように Configuration Manager を構成する
- Citrix WMI プロパティを使用してクエリベースのデバイスコレクションを作成する
- Citrix WMI プロパティに基づいてグローバル条件を作成する
- グローバル条件を使用してアプリケーション展開タイプの要件を定義する

また、`Root\ccm_vdi` 名前空間の Microsoft クラス `CCM_DesktopMachine` にある Microsoft プロパティを使用することもできます。詳細については、Microsoft のドキュメントを参照してください。

Microsoft System Center 仮想マシンマネージャー仮想化環境

仮想マシンを提供する目的で、Hyper-V と Microsoft System Center Virtual Machine Manager (VMM) を使用する場合は、このガイダンスに従ってください。

このリリースでは、システム要件に記載されているVMMバージョンがサポートされています。

> **注:**
>
> 混在Hyper-Vクラスター（異なるHyper-Vバージョンを実行しているサーバーを含む）はサポートされていません。

Citrix Provisioning (旧Provisioning Services) および Machine Creation Services™ を使用して、以下をプロビジョニングできます。

- 第1世代でサポートされているデスクトップまたはサーバーOSのVM。
- セキュアブートのサポートを含む、第2世代でサポートされているデスクトップまたはサーバーOSのVM。

ハイパーバイザーのインストールと構成

重要:

すべてのDelivery Controllerは、VMMサーバーと同じフォレスト内にある必要があります。

1. Microsoft Hyper-VサーバーとVMMをサーバーにインストールします。
2. すべてのControllerにSystem Center Virtual Machine Managerコンソールをインストールします。コンソールのバージョンは、管理サーバーのバージョンと一致している必要があります。以前のバージョンのコンソールでも管理サーバーに接続できますが、バージョンが異なる場合、VDAのプロビジョニングは失敗します。
3. 次のアカウント情報を確認します。

   Studioでホストを指定するために使用するアカウントは、関連するHyper-Vマシンに対するVMM管理者またはVMM委任管理者である必要があります。このアカウントがVMMで委任管理者ロールのみを持っている場合、ホスト作成プロセス中にStudioにストレージデータは表示されません。

   Studio統合に使用されるユーザーアカウントは、各Hyper-Vサーバー上の管理者ローカルセキュリティグループのメンバーである必要もあります。この構成は、VMの作成、更新、削除などのVMライフサイクル管理をサポートします。

   Hyper-Vを実行しているサーバーにControllerをインストールすることはサポートされていません。

単一のSCVMMが異なるデータセンター内の複数のクラスターを管理する大規模な展開では、委任された管理者のホストグループのスコープを制限できます。

ホストグループのスコープを制限するには、Microsoft System Center Virtual Machine Manager (VMM) コンソールで委任管理者ロールを使用します。

1. 「**ユーザーロールの作成ウィザード**」で、ユーザーロールとして「ファブリック管理者 (委任管理者)」を選択します。
2. 「**メンバー**」で、委任管理者として使用したいActive Directoryのユーザーアカウントを追加します。
3. 「**スコープ**」で、委任管理者にアクセスさせたいホストグループを選択します。
4. 委任管理者ユーザーの資格情報を使用して、新しい「**実行アカウント**」を作成します。これらの資格情報を使用して、後でハイパーバイザー接続を作成します。メインの管理者ロールアカウントは使用しないでください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- SCVMMでの接続の作成と管理については、「Microsoft System Center Virtual Machine Managerへの接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Nutanix仮想化環境

Citrix Virtual Apps and Desktops™ 展開環境で Nutanix Acropolis を使用して仮想マシンを提供する場合は、このガイダンスに従ってください。セットアッププロセスには、次のタスクが含まれます。

- Citrix Virtual Apps and Desktops 環境に Nutanix プラグインをインストールして登録します。
- Nutanix Acropolis ハイパーバイザーへの接続を作成します。
- Nutanix ハイパーバイザーで作成したマスターイメージのスナップショットを使用するマシンカタログを作成します。

詳細については、Nutanix Support Portal で入手できる Nutanix Acropolis MCS プラグインインストールガイドを参照してください。

Nutanixプラグインのインストールと登録

すべての Delivery Controller に Nutanix プラグインをインストールして登録するには、次の手順を完了します。Citrix Studio を使用して Nutanix への接続を作成します。その後、Nutanix 環境で作成したマスターイメージのスナップショットを使用するマシンカタログを作成します。

> **ヒント:**
>
> Nutanix プラグインをインストールまたは更新する際は、Citrix Host Service、Citrix Broker Service、および Machine Creation Services™ を停止してから再起動することをお勧めします。
>
> Nutanix プラグインのインストールについては、Nutanix Documentation site を参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- Nutanix環境で接続を作成および管理する方法については、Connection to Nutanixを参照してください。

詳細情報

- 接続とリソースの作成と管理
- マシンカタログの作成

Nutanix クラウドおよびパートナーソリューション

Citrix Virtual Apps and Desktops™ は、以下の Nutanix クラウドおよびパートナーソリューションをサポートしています。

- AWS 上の ニュータニックス クラウド クラスター

AWS 上の ニュータニックス クラウド クラスター

Citrix Virtual Apps and Desktops は、Nutanix Cloud Clusters on AWS をサポートしています。Nutanix クラスターは、プライベートクラウドまたは複数のパブリッククラウドでアプリケーショ

ンを実行する方法を簡素化します。Nutanix Cloud Clusters on AWS の詳細については、「Nutanix Cloud Clusters on AWS Deployment and User Guide」を参照してください。

> **ヒント:**
>
> このサポートは、Nutanix オンプレミス クラスターと同じ機能を提供します。サポートされるクラスターは、*Prism Element* の 1 つのみです。詳細については、こちら を参照してください。

要件

Nutanix Clusters on AWS を使用するには、以下が必要です。

- Nutanix アカウント。
- 以下の権限を持つ AWS アカウント。
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

Nutanix クラスターの作成

Nutanix Clusterを作成するには：

1. Nutanixアカウントにログインします。
2. 「**Nutanix cluster**」オプションを見つけて、「**Launch**」をクリックします。「**Nutanix Console**」が開きます。詳細については、「Get Started with Nutanix Cluster on AWS」を参照してください。
3. **新しいVPC**を作成することを選択します。

クラスター作成プロセスは、以下のエラーで失敗する可能性があります:

- クラスターが指定された時間内に作成できませんでした。クラスターを削除しています。
- ホスト Nutanix クラスター - ノード `XXXXXXXXXX: Instance i-xxxxxxxxxxxxx: disable network interface source/dest check error.`.
- ホスト Nutanix クラスター - ノード `XXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxx network interface info.`.

クラスターの作成に失敗した場合：

- 別のリージョンで再作成してみてください。
- 再試行する前に、Nutanix CloudFormation Stack (CFS) を削除してください。

他のリソースに加えて、Nutanix CFSは以下を作成します。

- *Nutanix Cluster xxxxxxxxxxxx* 10.0.0.0/16 という名前のVPCを1つ
- 10.0.128.0/24 と 10.0.129.0/24 の2つのサブネット
- 1つのインターネットゲートウェイ
- 1 NAT ゲートウェイ

クラスターが作成されたら、**Nutanix Prism** のアドレスを取得します。

1. **Nutanix Console** に移動します。
2. コンソールの右上隅で、**Launch Prism Element** リンクにマウスカーソルを合わせ、URL をコピーします。

次のステップ

- コアコンポーネントのインストール
- VDA のインストール
- サイトの作成
- Nutanix クラウドおよびパートナーソリューションの接続の作成と管理については、Nutanix クラウドおよびパートナーソリューションへの接続 を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

VMware 仮想化環境

仮想マシンを提供するのにVMwareを使用する場合は、このガイダンスに従ってください。

vCenter Serverと適切な管理ツールをインストールします。(vSphere vCenter Linked Mode操作はサポートされていません。)

MCSを使用する予定がある場合は、vCenter ServerのDatastore Browser機能（`<https://kb.vmware.com/s/article/2101567>`に記載）を無効にしないでください。この機能を無効にすると、MCSが正しく動作しません。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- VMware環境での接続の作成と管理については、「Connection to VMware」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

VMware クラウドおよびパートナーソリューション

Citrix Virtual Apps and Desktops™ は、以下の VMware クラウドおよびパートナーソリューションをサポートしています。

- Azure VMware ソリューション (AVS)
- Google Cloud VMware エンジン
- Amazon Web Services (AWS) 上で稼働する VMware クラウド

Azure VMware Solution (AVS) との統合について

Citrix Virtual Apps and Desktopサービスは、AVSをサポートしています。AVSは、Azureインフラストラクチャによって作成されたvSphereクラスターを含むクラウドインフラストラクチャを提供します。Citrix Virtual Apps and Desktopサービスを活用して、オンプレミス環境でvSphereを使用するのと同じ方法で、AVSを使用してVDAワークロードをプロビジョニングします。

AVS クラスターのセットアップ

Citrix Virtual Apps™ and Desktop サービスで AVS を使用できるようにするには、Azure で次の手順を実行します。

- ホストクォータを要求する
- Microsoft.AVS リソース プロバイダーを登録する
- ネットワークチェックリスト
- Azure VMware Solution プライベートクラウドを作成する
- Azure VMware Solution プライベートクラウドにアクセスする
- AzureでVMwareプライベートクラウドのネットワークを構成する

- Azure VMware Solution の DHCP を構成する
- Azure VMware Solution にネットワークセグメントを追加する
- Azure VMware Solution 環境を確認する

AZURE ENTERPRISE AGREEMENT のお客様向けのホストクォータを要求する

Azure ポータルの ページで、 を選択し、次の情報を含めます。

- 問題の種類: 技術
- サブスクリプション: サブスクリプションを選択してください
- サービス: すべてのサービス > Azure VMware Solution
- リソース: 一般的な質問
- 概要: 容量が必要
- 問題の種類: 容量管理の問題
- 問題のサブタイプ: 追加のホストクォータ/容量に関する顧客からの要求

サポートチケットの で、 タブに次の情報を含めます。

- POC または本番環境
- リージョン名
- ホスト数
- その他の詳細

> **注:**
>
> AVS には最低 3 台のホストが必要であり、N+1 ホストの冗長性を使用することをお勧めします。

> サポートチケットの詳細を指定したら、**Review + Create** を選択して Azure にリクエストを送信します。

MICROSOFT.AVS リソース プロバイダーを登録する

ホスト クォータを要求した後、リソース プロバイダーを登録します。

1. Azure ポータルにサインインします。
2. Azure ポータルメニューで、**All services** を選択します。
3. **All services** メニューで、サブスクリプションを入力し、**Subscriptions** を選択します。

4. サブスクリプションリストからサブスクリプションを選択します。
5. **Resource providers** を選択し、検索バーに **Microsoft.AVS** と入力します。
6. リソースプロバイダーが登録されていない場合は、**Register** を選択します。

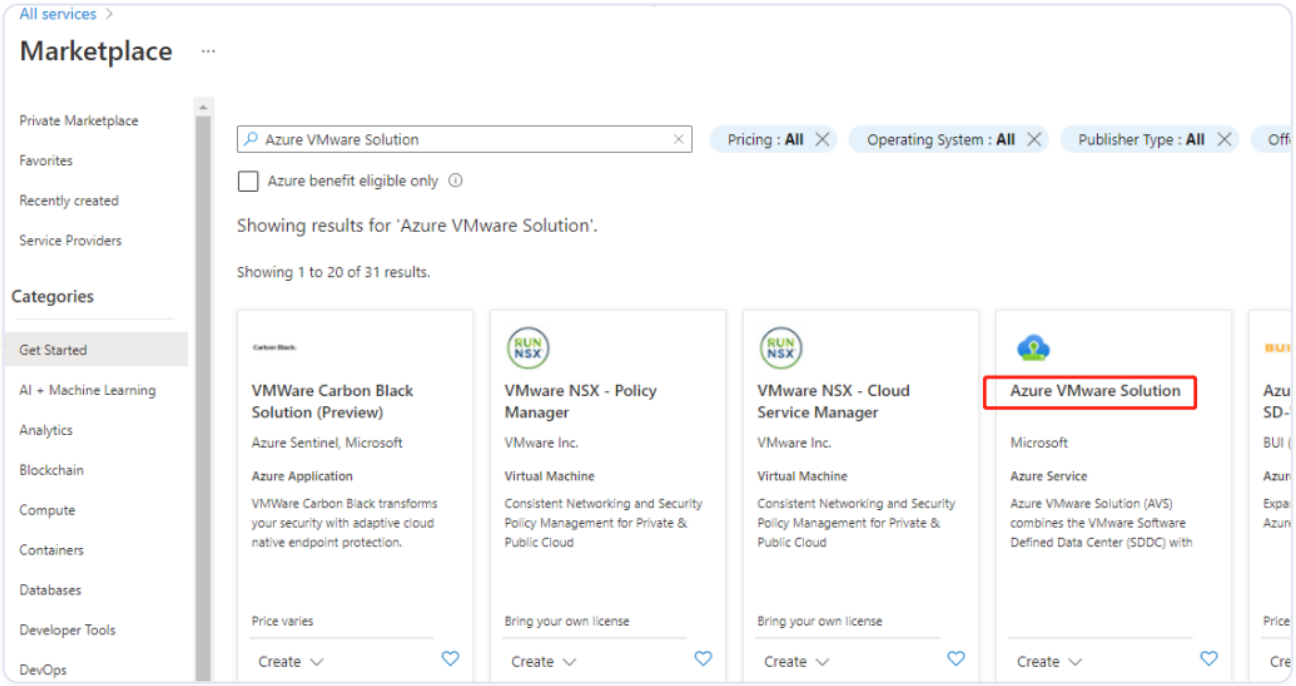
ネットワークに関する考慮事項

AVS は、特定のネットワークアドレス範囲とファイアウォールポートを必要とするネットワークサービスを提供します。詳細については、Azure VMware Solution のネットワーク計画チェックリスト を参照してください。

AZURE VMWARE SOLUTION プライベートクラウドを作成する

環境のネットワーク要件を考慮した後、AVS プライベートクラウドを作成します。

1. Azureポータルにサインインします。
2. **新しいリソースの作成**を選択します。
3. **Marketplace の検索**テキストボックスに、*Azure VMware Solution*と入力し、リストから**Azure VMware Solution**を選択します。



画像

Azure VMware Solutionウィンドウで、:

1. **作成**を選択します。
2. **基本**タブをクリックします。
3. 以下の表の情報を使用して、フィールドに値を入力します。

フィールド	値
サブスクリプション	デプロイに使用するサブスクリプションを選択します。Azure サブスクリプション内のすべてのリソースはまとめて課金されます。
リソースグループ	プライベートクラウドのリソースグループを選択します。Azure リソースグループは、Azure リソースがデプロイおよび管理される論理コンテナです。または、プライベートクラウド用に新しいリソースグループを作成することもできます。
場所	east us などの場所を選択します。これは、計画フェーズで定義したリージョンです。
リソース名	Azure VMware Solution プライベートクラウドの名前を指定します。
SKU	AV36 を選択します。
ホスト	プライベートクラウドクラスターに割り当てられたホストの数を表示します。デフォルト値は 3 で、デプロイ後に増減できます。
アドレスブロック	プライベートクラウドの IP アドレスブロックを指定します。CIDR はプライベートクラウド管理ネットワークを表し、vCenter Server や NSX-T Manager などのクラスター管理サービスに使用されます。たとえば、10.175.0.0/22 のように /22 アドレス空間を使用します。アドレスは一意であり、他の Azure 仮想ネットワークやオンプレミスネットワークと重複しないようにする必要があります。
仮想ネットワーク	Azure VMware Solution ExpressRoute 回線はデプロイ後の手順として確立されるため、ここは空白のままにします。

プライベートクラウドの作成画面で：

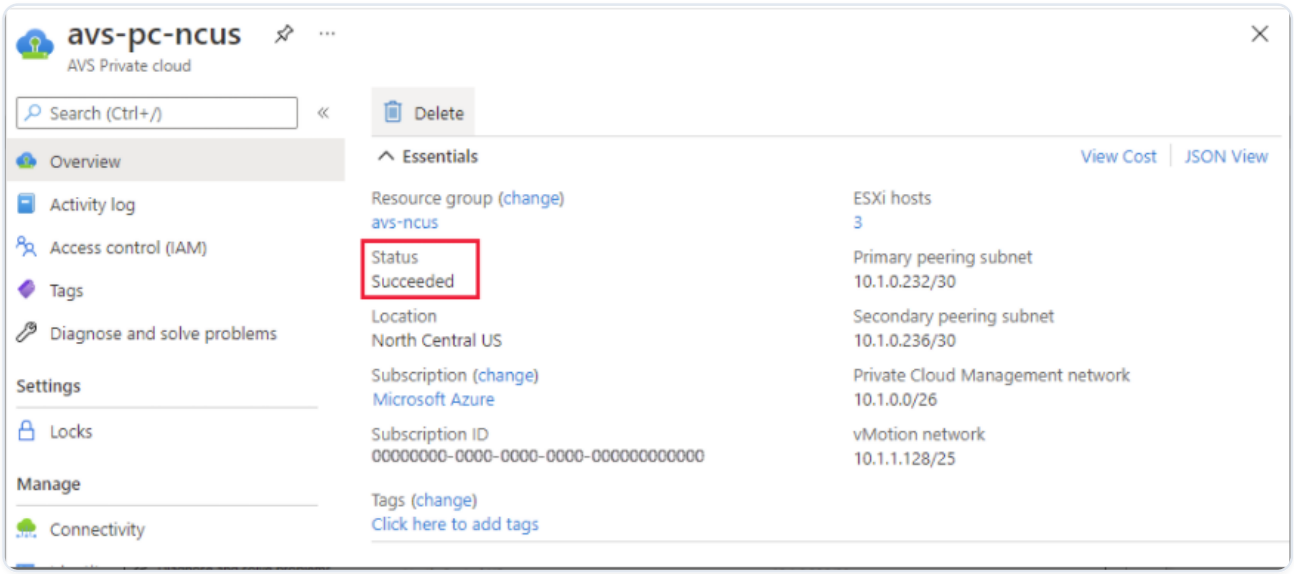
1. フィールドで、AVS が存在するリージョンを選択します。リソースグループのリージョンは AVS リージョンと同じです。

2. フィールドで、 を選択します。
3. 「**アドレスブロック**」フィールドにIPアドレスを指定します。例: 10.15.0.0/22。
4. 「**確認 + 作成**」を選択します。
5. 情報を確認したら、「**作成**」をクリックします。

Azure ASV プライベートクラウドの作成(/en-us/citrix-virtual-apps-desktops/2411/media/azure-avs-create-private-cloud.png)

> **ヒント:**
>
> プライベートクラウドの作成には3〜4時間かかる場合があります。クラスターに単一のホストを追加するには30〜45分かかる場合があります。

> 展開が成功したことを確認します。作成したリソースグループに移動し、プライベートクラウドを選択します。**ステータス**が**成功**になったら、展開は完了です。



AZURE VMWARE SOLUTION プライベートクラウドへのアクセス

プライベートクラウドを作成したら、Windows VMを作成し、プライベートクラウドのローカルvCenterに接続します。
新しいWindows仮想マシンの作成

1. リソースグループで、「**+ Add**」を選択し、「**Microsoft Windows 10/2016/2019**」を検索して選択します。
2. 「**Create**」をクリックします。
3. 必要な情報を入力し、「**Review + Create**」を選択します。

4. 検証が完了したら、**作成**を選択して仮想マシンの作成プロセスを開始します。

プライベートクラウドのローカルvCenterに接続する

1. クラウド管理者として**VMware vCenter SSO を使用した vSphere Client**にサインインします。

   Azure ASV vSphere ログイン(/en-us/citrix-virtual-apps-desktops/2411/media/azure-avs-vsphere-login.png)

2. Azureポータルで、プライベートクラウドを選択し、次に**管理 > ID**を選択します。

プライベートクラウドのvCenterとNSX-T ManagerのURLとユーザー資格情報が表示されます。

Azure ASV セットアップ vCenter(/en-us/citrix-virtual-apps-desktops/2411/media/azure-avs-setup-vcenter.png)

URLとユーザー資格情報を確認後:

1. 前の手順で作成したVMに移動し、仮想マシンに接続します。
2. Windows VMでブラウザを開き、2つのブラウザタブでvCenterとNSX-T ManagerのURLに移動します。vCenterタブで、前のステップで取得した*cloudadmin@vmcp.local*のユーザー資格情報を入力します。

AZUREでVMWAREプライベートクラウドのネットワークを構成する

ASVプライベートクラウドにアクセスした後、仮想ネットワークとゲートウェイを作成してネットワークを構成します。
仮想ネットワークを作成する

1. Azure portal にサインインします。
2. 以前に作成したリソースグループに移動します。
3. 「**+ 追加**」を選択して、新しいリソースを定義します。
4. テキストボックスに「*仮想ネットワーク*」と入力します。仮想ネットワークリソースを見つけて選択します。
5. ページで、 を選択してプライベートクラウドの仮想ネットワークを設定します。
6. ページで、仮想ネットワークの詳細を入力します。
7. タブで、仮想ネットワークの名前を入力し、適切なリージョンを選択して、 をクリックします。
8. タブの IPv4 アドレス空間で、以前に作成したアドレスを入力します。

> **重要:**

> プライベートクラウドを作成したときに使用したアドレス空間と重複しないアドレスを使用してください。

> アドレス空間を入力した後:

1. を選択します。
2. ページで、サブネットに名前と適切なアドレス範囲を割り当てます。
3. をクリックします。
4. を選択します。
5. 情報を確認し、 をクリックします。デプロイが完了すると、仮想ネットワークがリソースグループに表示されます。

仮想ネットワークゲートウェイを作成する
仮想ネットワークを作成した後、仮想ネットワークゲートウェイを作成します。

1. リソースグループで、「**+ 追加**」を選択して新しいリソースを追加します。
2. 「**Search the Marketplace**」テキストボックスに「*virtual network gateway*」と入力します。仮想ネットワークリソースを見つけて選択します。
3. 「**Virtual Network gateway**」ページで、「**Create**」をクリックします。
4. 「**Create virtual network gateway**」ページの「**Basics**」タブで、フィールドに値を入力します。
5. 「**Review + create**」をクリックします。

Azure ASV セットアップ vCenter(/en-us/citrix-virtual-apps-desktops/2411/media/azure-avs-create-virtual-gateway.png)

仮想ネットワークゲートウェイの構成を確認したら、**作成**をクリックして仮想ネットワークゲートウェイを展開します。 展開が完了したら、**ExpressRoute**接続をAzure AVSプライベートクラウドを含む仮想ネットワークゲートウェイに接続します。

EXPRESSROUTEを仮想ネットワークゲートウェイに接続する

仮想ネットワークゲートウェイを展開した後、それとAzure AVSプライベートクラウドの間に接続を追加します。

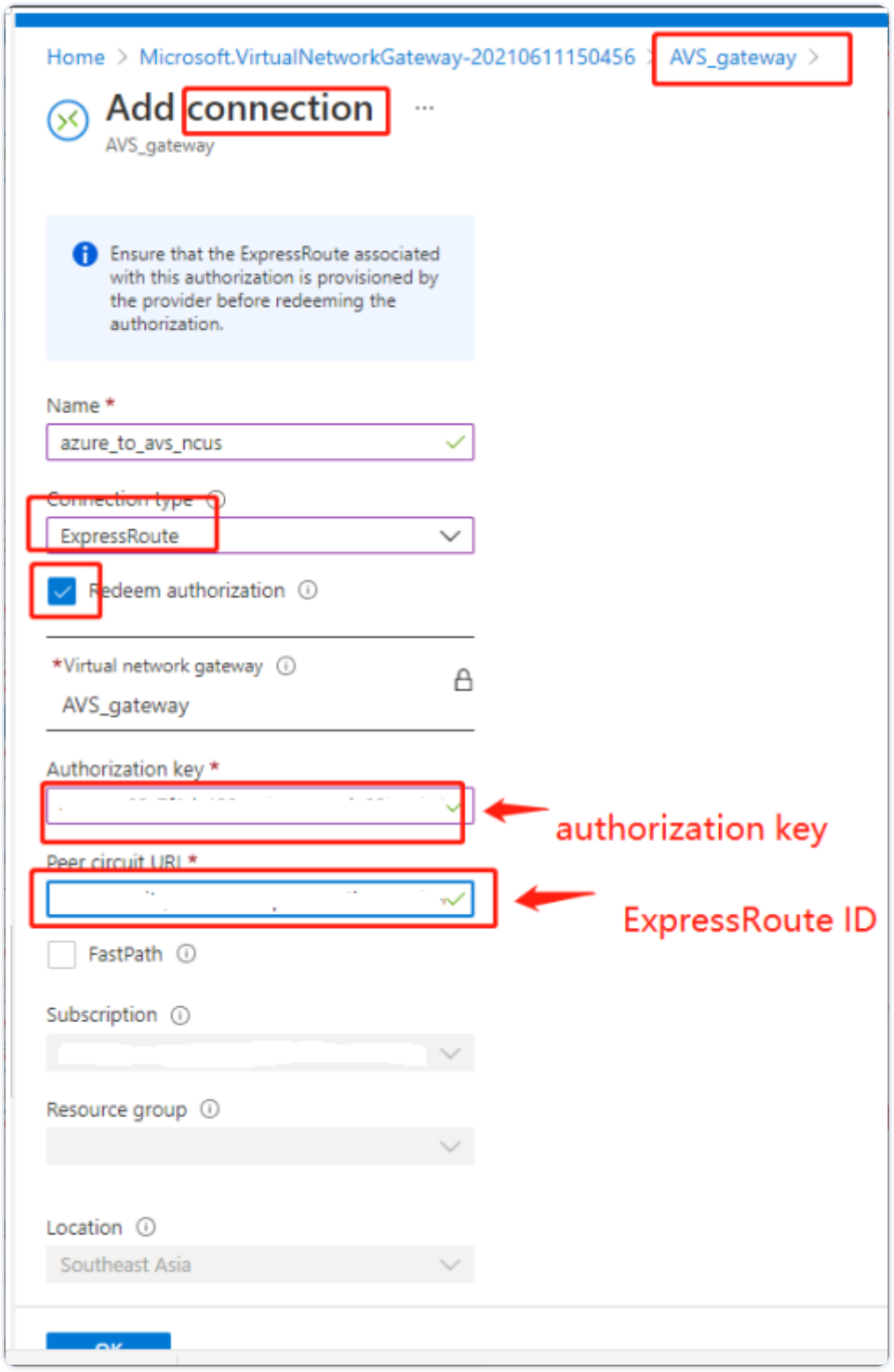
1. ExpressRoute承認キーを要求します。

2. Azureポータルで、**Azure VMware Solution private cloud**に移動します。「**Manage> Connectivity > ExpressRoute**」を選択し、次に「**+ Request an authorization key**」を選択します。

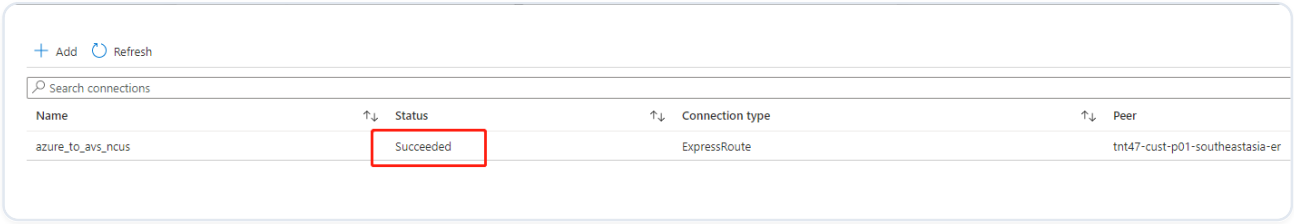
Azure ASV 承認キーの要求(/en-us/citrix-virtual-apps-desktops/2411/media/azure-avs-expressroute.png)

承認キーを要求した後：

1. キーの名前を入力し、**作成**をクリックします。キーの作成には約30秒かかる場合があります。作成されると、新しいキーはプライベートクラウドの承認キーのリストに表示されます。
2. 「**承認キー**」と「**ExpressRoute ID**」をコピーします。これらはピアリングプロセスを完了するために必要です。承認キーはしばらくすると消えるため、表示されたらすぐにコピーしてください。
3. 使用する予定の「**仮想ネットワークゲートウェイ**」に移動し、「**Connections > + Add**」を選択します。
4. 「**接続の追加**」ページで、フィールドに値を入力し、「**OK**」を選択します。



ExpressRoute回線と仮想ネットワーク間の接続が確立されます。



AZURE VMWARE SOLUTION の DHCP を構成する

ExpressRouteを仮想ゲートウェイに接続した後、DHCPを構成します。
NSX-T を使用して DHCP サーバーをホストする
NSX-T Manager で、次の手順を実行します。

1. 「**Networking > DHCP**」を選択し、次に「**サーバーの追加**」を選択します。
2. 「**サーバータイプ**」に「**DHCP**」を選択し、サーバー名と IP アドレスを入力します。
3. 「**保存**」をクリックします。
4. 「**Tier 1 ゲートウェイ**」を選択し、Tier-1 ゲートウェイの縦の省略記号を選択し、次に「**編集**」を選択します。
5. サブネットを追加するには、「**IP割り当てなし**」を選択します。
6. 「**タイプ**」に「**DHCP ローカルサーバー**」を選択します。
7. 「**DHCP サーバー**」には「**デフォルト DHCP**」を選択し、「**保存**」をクリックします。
8. もう一度「**保存**」をクリックし、「**編集を閉じる**」を選択します。

Azure ASV NSX-Tサーバーの追加(/en-us/citrix-virtual-apps-desktops/2411/media/azure-avs-nsx-t-add-server.png)

AZURE VMWARE SOLUTIONでネットワークセグメントを追加する

DHCPを設定した後、ネットワークセグメントを追加します。

ネットワークセグメントを追加するには、NSX-T Managerで**Networking> Segments**を選択し、**Add Segment**をクリックします。

Azure ASV NSX-Tセグメントの追加(/en-us/citrix-virtual-apps-desktops/2411/media/azure-avs-nsx-t-add-segment.png)

「**セグメントプロファイル**」画面で:

1. セグメントの「**名前**」を入力します。
2. 「**接続済みゲートウェイ**」として「**Tier-1 Gateway (TNTxx-T1)**」を選択し、「**タイプ**」は「**フレキシブル**」のままにします。
3. 事前設定されたオーバーレイ「**トランスポートゾーン (TNTxx-OVERLAY-TZ)**」を選択します。
4. 「**サブネットの設定**」をクリックします。

Azure ASV NSX-Tセグメントプロファイルの追加(/en-us/citrix-virtual-apps-desktops/2411/media/azure-avs-nsx-t-segment-profiles.png)

「**サブネット**」セクションで:

1. ゲートウェイIPアドレスを入力します。
2. **Add**を選択します。

> **重要:**

> このセグメントのIPアドレスは、Azureゲートウェイの IPアドレス (10.15.0.0/22) に属している必要があります。

> DHCP範囲はセグメントIPアドレスに属している必要があります。

Azure ASVでNSX-Tセグメントの DHCP範囲を追加(/en-us/citrix-virtual-apps-desktops/2411/media/azure-avs-nsx-t-dhcp-range.png)

セグメントの構成を続行するオプションを拒否するには、 を選択します:

Azure ASVでNSX-Tのセットアップを完了(/en-us/citrix-virtual-apps-desktops/2411/media/azure-avs-nsx-t-finish-setup.png)

vCenterで、 **>** を選択します:

Azure ASVでNSX-T vCenterを追加(/en-us/citrix-virtual-apps-desktops/2411/media/azure-avs-nsx-t-vcenter.png)

AZURE AVS環境を確認する

Azureリソースグループで直接接続とコネクタを設定します。

Azure ASVでASV接続を確認(/en-us/citrix-virtual-apps-desktops/2411/media/azure-avs-verify-connection-create-dc-v2.png)

vCenterの資格情報で接続を確認します。

Azure ASVでNSX-T vCenterを追加(/en-us/citrix-virtual-apps-desktops/2411/media/azure-avs-final-setup.png)

グーグル クラウド ヴイエムウェア エンジン

Citrix Virtual Apps and Desktopsを使用すると、VMwareベースのオンプレミスCitrixワークロードをGoogle Cloud VMware Engineに移行できます。

Google Cloud VMware Engineを構成する

次の手順では、Google Cloud VMware Engineでクラスターを取得してセットアップする方法について説明します。

VMWARE ENGINEポータルにアクセスする

1. **Google Cloud Console**で、ナビゲーションメニューをクリックします。
2. **Compute**セクションで、**VMware Engine**をクリックして、新しいブラウザータブでVMware Engineを開きます。

最初のプライベートクラウドを作成するための要件

Google Cloud VMware Engineへのアクセス権、利用可能なVMware Engineノードクォータ、および適切なIAMロールが必要です。プライベートクラウドの作成を続行する前に、次の要件を準備してください。

1. APIアクセスとノードクォータをリクエストします。詳細については、「APIアクセスとクォータのリクエスト」を参照してください。
2. VMware管理アプライアンスおよびHCX展開ネットワークに使用するアドレス範囲をメモします。詳細については、「ネットワーク要件」を参照してください。
3. VMware Engine Service Admin IAMロールを取得します。

最初のプライベートクラウドを作成する

1. VMware Engineポータルにアクセスします。
2. VMware Engineのホーム画面で、 をクリックします。ホスティング場所とハードウェアノードの種類が一覧表示されます。
3. プライベートクラウドのノード数を選択します。少なくとも3つのノードが必要です。
4. VMware管理ネットワークのクラスレス・インタードメイン・ルーティング（CIDR）範囲を入力します。
5. HCXデプロイメントネットワークのCIDR範囲を入力します。

> **重要:**
>
> CIDR範囲は、オンプレミスまたはクラウドのサブネットと重複してはなりません。
> CIDR範囲は/27以上である必要があります。

6. **確認して作成**を選択します。
7. 設定を確認します。設定を変更するには、**戻る**をクリックします。

8. プライベートクラウドの作成を開始するには、**作成**をクリックします。

VMware Engineが新しいプライベートクラウドを作成すると、いくつかのVMwareコンポーネントがデプロイされ、プライベートクラウド内のクラスターの初期Autoscale™ポリシーが設定されます。プライベートクラウドの作成には30分から2時間かかる場合があります。プロビジョニングが完了すると、メールが届きます。

GOOGLE CLOUD VMWARE ENGINE VPNゲートウェイをセットアップする

Google Cloud VMware Engineへの初期接続を確立するには、VPNゲートウェイを使用できます。これはOpenVPNベースのクライアントVPNであり、これを使用してVMware Software Defined Data Center (SDDC) vCenterに接続し、必要な初期構成を行うことができます。

VPNゲートウェイをデプロイする前に、SDDCがデプロイされているリージョンの**Edge Services**範囲を構成します。これを行うには：

1. **Google Cloud VMware Engine**ポータルにログオンし、**Network > Regional Settings**に移動します。**Add Region**をクリックします。
2. SDDCがデプロイされているリージョンを選択し、**Internet Access**と**Public IP Service**を有効にします。
3. 計画時にメモしたEdge Services範囲を入力し、**Submit**をクリックします。これらのサービスを有効にするには10〜15分かかります。

   完了すると、エッジサービスは地域設定ページで**有効**と表示されます。これらの設定を有効にすると、パブリックIPがSDDCに割り当てられるようになり、これはVPNゲートウェイを展開するための要件です。

VPNゲートウェイを展開するには：

1. **Google Cloud VMware Engine**ポータルで、**ネットワーク > VPNゲートウェイ**に移動します。**新しいVPNゲートウェイの作成**をクリックします。
2. VPNゲートウェイの名前と、計画中に予約したクライアントサブネットを入力します。**次へ**をクリックします。
3. VPNアクセスを許可するユーザーを選択します。**次へ**をクリックします。
4. VPN経由でアクセス可能にする必要があるネットワークを指定します。**次へ**をクリックします。
5. 概要画面が表示されます。選択内容を確認し、**送信**をクリックしてVPNゲートウェイを作成します。VPNゲートウェイページには、新しいVPNゲートウェイのステータスが**作成中**として表示されます。
6. ステータスが**稼働中**に変わったら、新しいVPNゲートウェイをクリックします。

7. **VPN構成をダウンロード**をクリックして、VPNゲートウェイ用に事前設定されたOpenVPNプロファイルを含むZIPファイルをダウンロードします。UDP/1194およびTCP/443経由で接続するためのプロファイルが利用可能です。好みのものを選択してOpen VPNにインポートし、接続します。
8. **リソース**に移動し、SDDCを選択します。

VPNを接続する

1. VPNゲートウェイの設定を通じて、オンプレミスネットワークとプライベートクラウド間のポイントツーサイト接続を確立します。Google Cloud VMware Engine VPNゲートウェイを設定するを参照してください。
2. Google Cloud VMware Engine VPNゲートウェイを設定するでダウンロードしたVPN構成をアップロードします。
3. VPNクライアント（例: OpenVPN Connect）にインポートします。

詳細については、VPNを使用した接続を参照してください。

最初のサブネットを作成する

VMware EngineポータルからNSX-T Managerにアクセスする
サブネットの作成プロセスはNSX-Tで行われ、NSX-TにはVMware Engineを介してアクセスします。NSX-T Managerにアクセスするには、次の手順を実行します。

1. **Google Cloud VMware Engine**ポータルにログオンします。
2. メインナビゲーションから、**リソース**に移動します。
3. サブネットを作成するプライベートクラウドに対応する**プライベートクラウド名**をクリックします。
4. プライベートクラウドの詳細ページで、**vSphere Management Network**タブをクリックします。
5. NSX-T Managerに対応する**FQDN**をクリックします。
6. プロンプトが表示されたら、サインイン資格情報を入力します。vIDMを設定し、Active DirectoryなどのIDソースに接続している場合は、代わりにIDソースの資格情報を使用します。

> **注意:**
>
> 生成された資格情報は、プライベートクラウドの詳細ページから取得できます。

サブネットのDHCPサービスを設定する

サブネットを作成する前に、DHCPサービスを設定します。

NSX-T マネージャーで：

1. **ネットワーク > DHCP**に移動します。ネットワークダッシュボードには、DHCPサービスが1つのTier-0ゲートウェイと1つのTier-1ゲートウェイを作成することが示されます。
2. DHCPサーバーのプロビジョニングを開始するには、**Add Server** をクリックします。
3. **Server Type** に **DHCP** を選択し、サーバー名とIPアドレスを入力します。
4. DHCPサービスを作成するには、**Save** をクリックします。

このDHCPサービスを関連するTier-1ゲートウェイにアタッチするには、次の手順を実行します。デフォルトのTier-1ゲートウェイは、DHCPサービスによってすでにプロビジョニングされています。

1. 「**Tier 1 Gateways**」を選択し、Tier-1 ゲートウェイの縦の省略記号を選択し、「**Edit**」を選択します。
2. 「**IP Address Management**」フィールドで、「**No IP Allocation Set**」を選択します。
3. 「**Type**」に「**DHCP Local Server**」を選択します。
4. 「**DHCP Server**」には、作成した DHCP サーバーを選択します。
5. 「**保存**」をクリックします。
6. 「**Close Editing**」をクリックします。

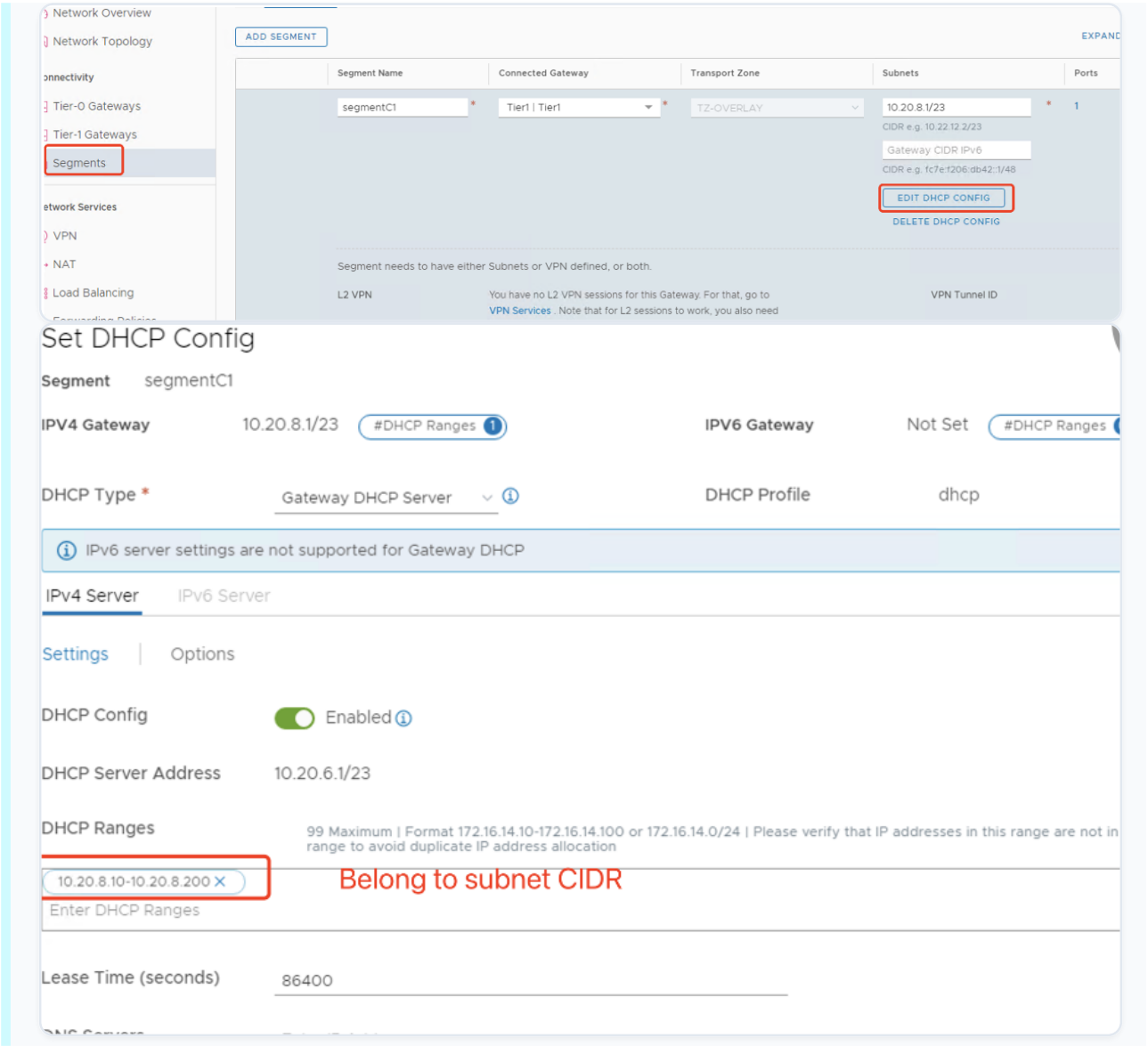
これで、NSX-Tでネットワークセグメントを作成できます。NSX-TでのDHCPの詳細については、VMware documentation for DHCPを参照してください。
NSX-T でネットワークセグメントを作成する
ワークロード VM の場合、プライベートクラウドの NSX-T ネットワークセグメントとしてサブネットを作成します。

1. NSX-T Manager で、「**Networking > Segments**」に移動します。
2. 「**Add Segment**」をクリックします。
3. セグメントの名前を入力します。
4. **Tier-1** を **Connected Gateway** として選択し、タイプは **Flexible** のままにします。
5. **Set Subnets** をクリックします。
6. **Add Subnets** をクリックします。
7. **Gateway IP/Prefix Length** にサブネット範囲を入力します。最後のオクテットを **.1** としてサブネット範囲を指定します。例: **10.12.2.1/24**。

8. DHCP 範囲を指定し、**ADD** をクリックします。
9. **Transport Zone** で、ドロップダウンリストから **TZ-OVERLAY** を選択します。
10. **Save** をクリックします。これで、VM の作成時に vCenter でこのネットワークセグメントを選択できるようになります。

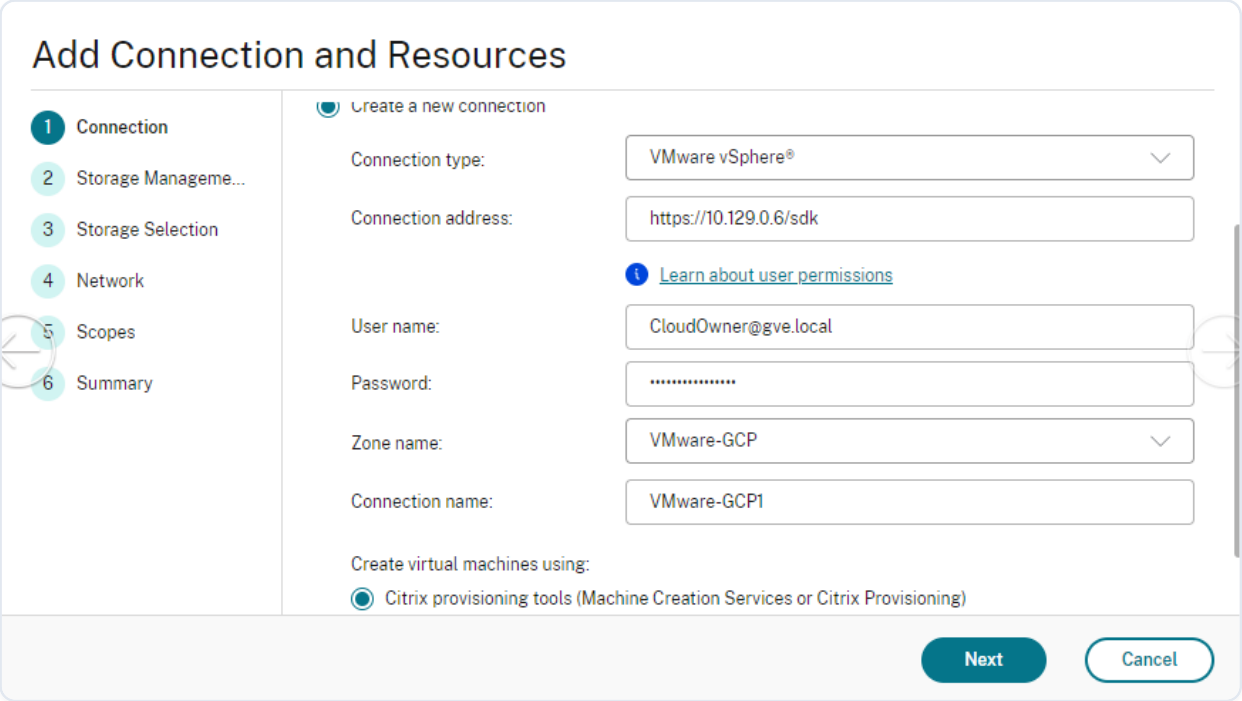
特定のリージョンでは、プライベートサービスアクセスを使用して、VMware Engine から VPC ネットワークへの一意のルートを最大 100 個設定できます。これには、たとえば、プライベートクラウド管理 IP アドレス範囲、NSX-T ワークロードネットワークセグメント、HCX ネットワーク IP アドレス範囲が含まれます。この制限には、リージョン内のすべてのプライベートクラウドが含まれます。

> **注：**
>
> Google Cloud の構成の問題により、DHCP 範囲設定を複数回構成する必要があります。したがって、Google Cloud の構成後に DHCP 範囲設定を構成するようにしてください。DHCP 範囲を構成するには、**EDIT DHCP CONFIG** をクリックします。



CITRIX STUDIO で GOOGLE CLOUD VMWARE 接続を作成する

1. vCenter でマシンを作成します。
2. Citrix Studio を起動します。
3. ホスティングノードを選択し、**接続とリソースの追加**をクリックします。
4. **接続**画面で、**新しい接続を作成**を選択し、次の詳細を入力します。



a. **接続の種類**として**VMware vSphere**を選択します。

b. **接続アドレス**に、vCenterのプライベートIPアドレスを入力します。

c. vCenterの資格情報を入力します。

d. 接続名を入力します。

e. 仮想マシンを作成するツールを選択します。

5. **ネットワーク**画面で、NSX-Tサーバーで作成されたサブネットを選択します。

6. ウィザードを完了します。

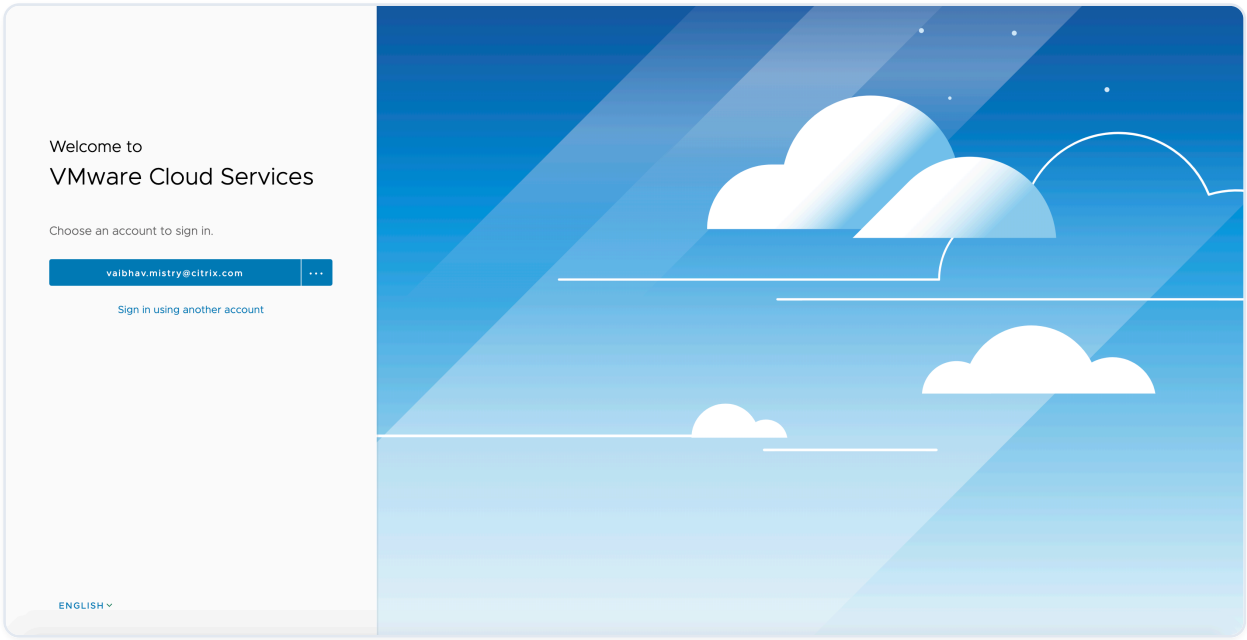
Amazon Web Services (AWS) 上のVMware クラウド

Amazon Web Services (AWS) 上のVMware Cloudを使用すると、VMwareベースのオンプレミスCitrixワークロードをAWS Cloudに移行できます。

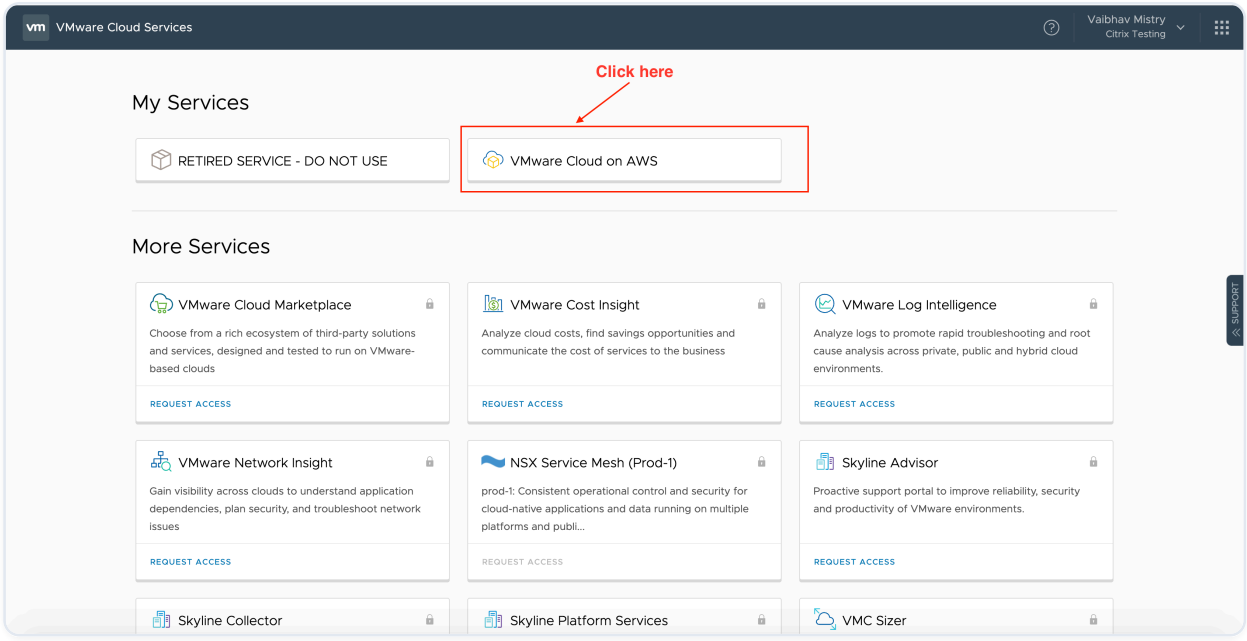
この記事では、AWS上にVMware Cloudをセットアップする手順について説明します。

VMware Cloud環境にアクセスする

1. URL `<https://console.cloud.vmware.com/>` を使用してVMware Cloudサービスにログインします。



2. **VMware Cloud on AWS** をクリックします。Software-Defined Data Centers (SDDC) ページが表示されます。



3. **OPEN VCENTER** をクリックし、次に **SHOW CREDENTIALS** をクリックします。後で使用するために資格情報を控えておきます。

   vCenter を開く(/en-us/citrix-virtual-apps-desktops/2411/media/vmc-sddc.png)

   「資格情報を表示」(/en-us/citrix-virtual-apps-desktops/2411/media/show-credentials-vmc.png)

4. Web ブラウザを開き、vSphere Web Client の URL を入力します。
5. 控えておいた資格情報を入力し、**Login** をクリックします。vSphere クライアントの Web ページは、オンプレミス環境と似ています。

vSphere クライアントの Web ページ(/en-us/citrix-virtual-apps-desktops/2411/media/vcenter-page.png)

VMwareクラウド環境について

vSphere クライアントの Web ページには 4 つのビューがあります。

- ホストおよびクラスタービュー: 新しいクラスターを作成することはできませんが、クラウド管理者は複数のリソースプールを作成できます。

  「ホストおよびクラスタービュー」(/en-us/citrix-virtual-apps-desktops/2411/media/host-cluster-view.png)
- VM およびテンプレートビュー: クラウド管理者は多くのフォルダを作成できます。

  VM およびテンプレートビュー(/en-us/citrix-virtual-apps-desktops/2411/media/vm-template-view.png)
- ストレージビュー: Citrix Studioでホスティングユニットを追加する際は、**WorkloadDatastore** ストレージを選択してください。Workload Datastoreにのみアクセスできるためです。

  「ストレージビュー」(/en-us/citrix-virtual-apps-desktops/2411/media/storage-view.png)
- ネットワークビュー: VMwareクラウドネットワークと不透明なネットワークでは、アイコンが異なります。

  「ネットワークビュー」(/en-us/citrix-virtual-apps-desktops/2411/media/network-view.png)

クラスターのセットアップ後、接続とリソースの追加については、VMware仮想化環境を参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- 接続の作成と管理については、「VMware CloudおよびパートナーソリューションへのConnecting」を参照してください。

詳細情報

- 接続とリソースを作成および管理する
- マシンカタログを作成する

コアコンポーネントをインストールする

重要:

Citrix は、ライセンスコンプライアンスを含む正当な利益のために、必要に応じて基本的なライセンスデータを収集します。詳細については、「Citrix ライセンスデータ」を参照してください。

コアコンポーネントは、Citrix Delivery Controller™、Citrix Studio、Web Studio、Citrix Director、および Citrix License Server です。

注:

Citrix Studio は、オンプレミスの Citrix Virtual Apps and Desktops 展開を構成および管理できる Windows ベースの管理コンソールです。Web Studio は Citrix Studio の次世代版であり、Citrix Studio と完全に同等の機能を備えた Web ベースの管理コンソールです。Web Studio の詳細については、「Web Studio のインストール」を参照してください。

(2003 より前のバージョンでは、コアコンポーネントに Citrix StoreFront が含まれていました。**Citrix StoreFront** タイルをクリックするか、インストールメディアで利用可能なコマンドを実行することで、StoreFront をインストールできます。)

インストールを開始する前に、この記事と「インストールの準備」を確認してください。

この記事では、コアコンポーネントをインストールする際のインストールウィザードのシーケンスについて説明します。コマンドラインの同等機能も提供されています。詳細については、「コマンドラインを使用したインストール」を参照してください。

ステップ 1. 製品ソフトウェアをダウンロードしてウィザードを起動する

Citrix アカウントの資格情報を使用して、Citrix Virtual Apps and Desktops™ のダウンロードページにアクセスします。製品の ISO ファイルをダウンロードします。

ファイルを解凍します。必要に応じて、ISO ファイルを DVD に書き込みます。

コアコンポーネントをインストールするマシンに、ローカル管理者アカウントを使用してログオンします。

DVD をドライブに挿入するか、ISO ファイルをマウントします。インストーラーが自動的に起動しない場合は、**AutoSelect** アプリケーションまたはマウントされたドライブをダブルクリックします。

ステップ 2. インストールする製品を選択する

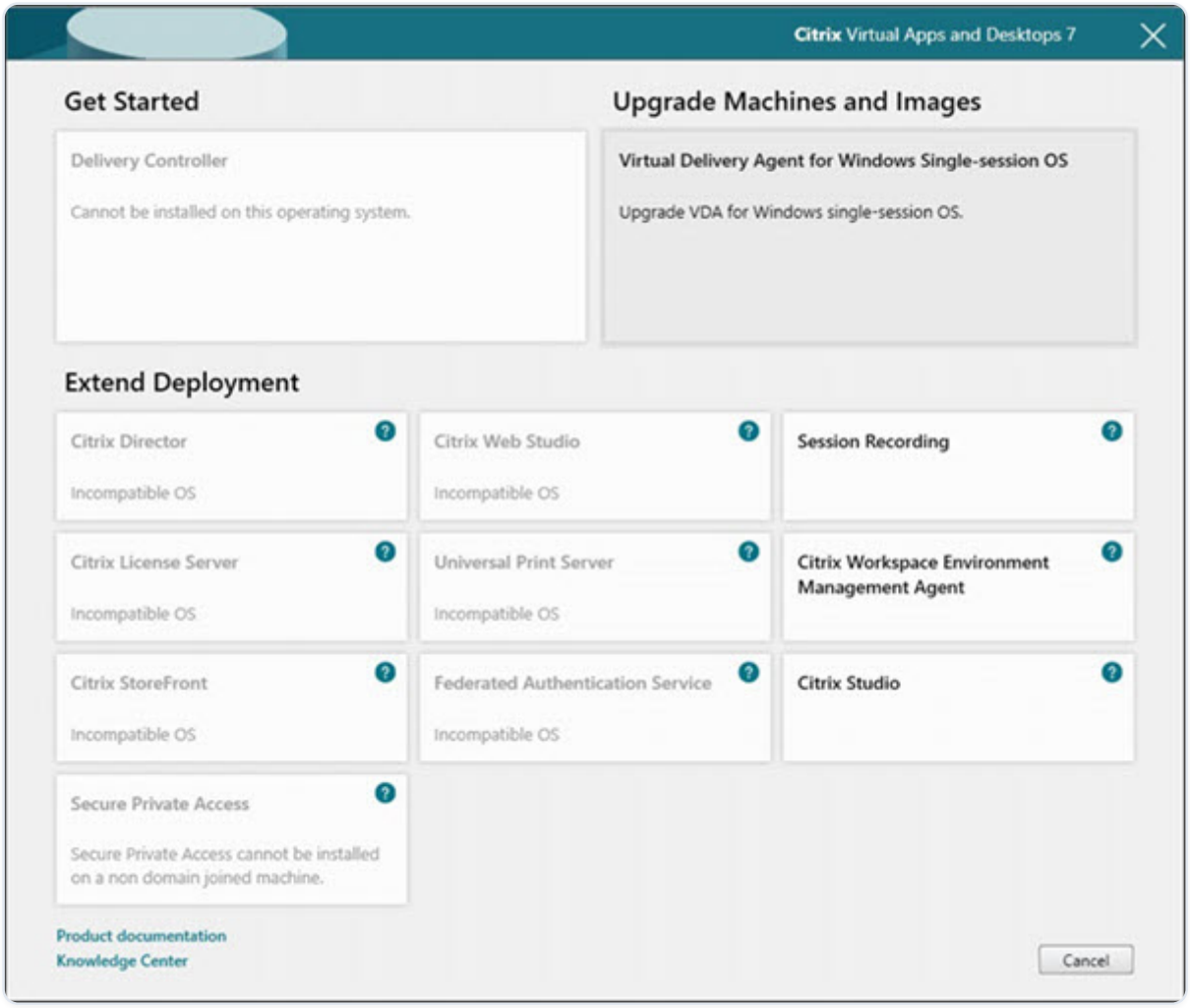


インストールする製品（Virtual Apps または Virtual Apps and Desktops）の横にある をクリックします。

（マシンにCitrix Virtual Apps and Desktopsコンポーネントがすでにインストールされている場合、このページは表示されません。）

コマンドラインオプション: Citrix Virtual Appsをインストールするには `/xenapp`。オプションを省略すると、Citrix Virtual Apps and Desktopsがインストールされます。

ステップ 3. インストールするものを選択する

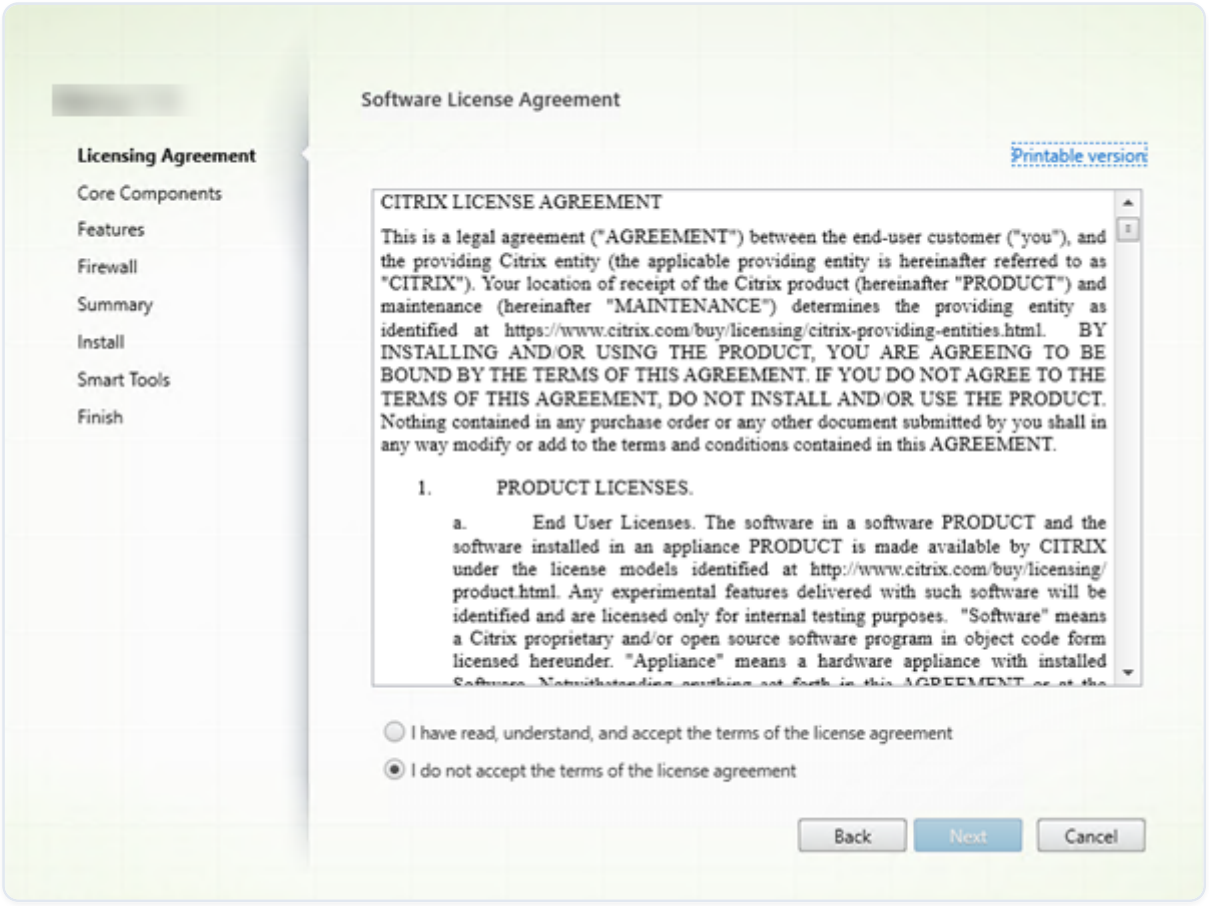


初めて使用する場合は、 を選択します。（後のページで、このマシンにインストールする特定のコンポーネントを選択します。）

（このマシンまたは別のマシンに）すでにControllerをインストールしていて、別のコンポーネントをインストールしたい場合は、 セクションからコンポーネントを選択します。

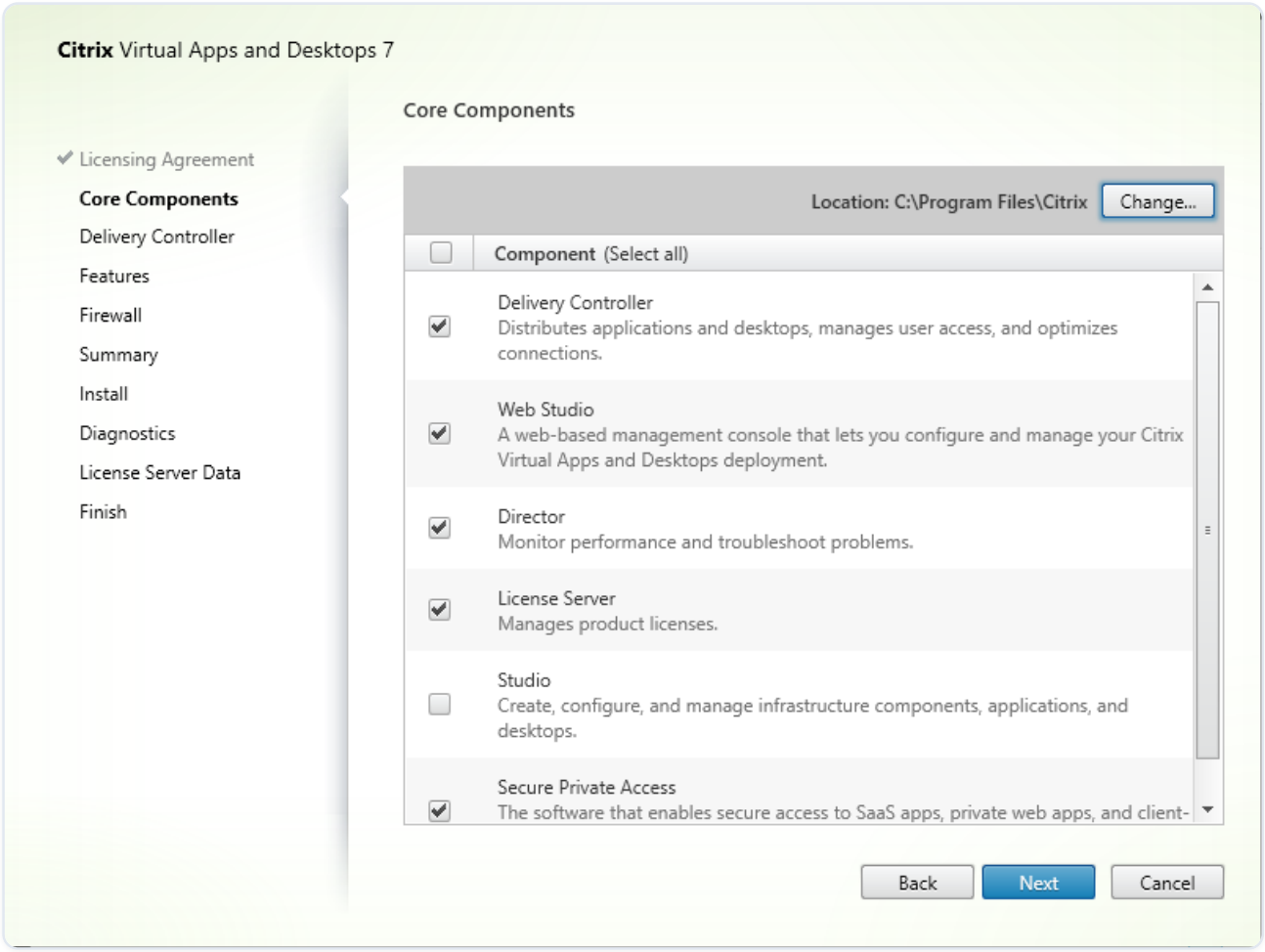
コマンドラインオプション: `/components`

ステップ 4. ライセンス契約を読んで同意する



ページで、ライセンス契約を読んだ後、それを読んで同意したことを示します。次に をクリックします。

ステップ 5. インストールするコンポーネントとインストール場所を選択する



ページで:

- **場所:** デフォルトでは、コンポーネントは`C:\Program Files\Citrix`にインストールされます。ほとんどの展開では、デフォルトで問題ありません。別の場所を指定する場合、その場所にはネットワークサービスに対する実行権限が必要です。
- **コンポーネント:** デフォルトでは、すべてのコアコンポーネントのチェックボックスが選択されています。すべてのコアコンポーネントを1台のサーバーにインストールすることは、概念実証、テスト、または小規模な本番展開には問題ありません。大規模な本番環境では、CitrixはDirector、StoreFront、Secure Private Access、およびLicense Serverを別々のサーバーにインストールすることを推奨します。

> **注:**
>
> 複数のサーバーにコンポーネントをインストールする場合は、他のサーバーに他のコンポーネントをインストールする前に、まずCitrix License Serverとライセンスをインス

> トールしてください。ガイダンスについては、Licensing Guide for Citrix Virtual Apps and Desktopsの「自動インストール」セクションを参照してください。

> このマシンに必須のコアコンポーネントをインストールしないことを選択した場合、アイコンで警告が表示されます。この警告は、そのコンポーネントをインストールする必要があることを通知しますが、必ずしもこのマシンにインストールする必要はありません。

Nextをクリックします。

コマンドラインオプション: `/installdir`, `/components`, `/exclude`

ハードウェアチェック

Delivery Controller をインストールまたはアップグレードすると、ハードウェアがチェックされます。マシンに推奨される RAM 容量 (5 GB) より少ない場合、インストーラーは警告を表示します。これはサイトの安定性に影響を与える可能性があります。詳細については、「ハードウェア要件」を参照してください。

グラフィカルインターフェイス: ダイアログボックスが表示されます。

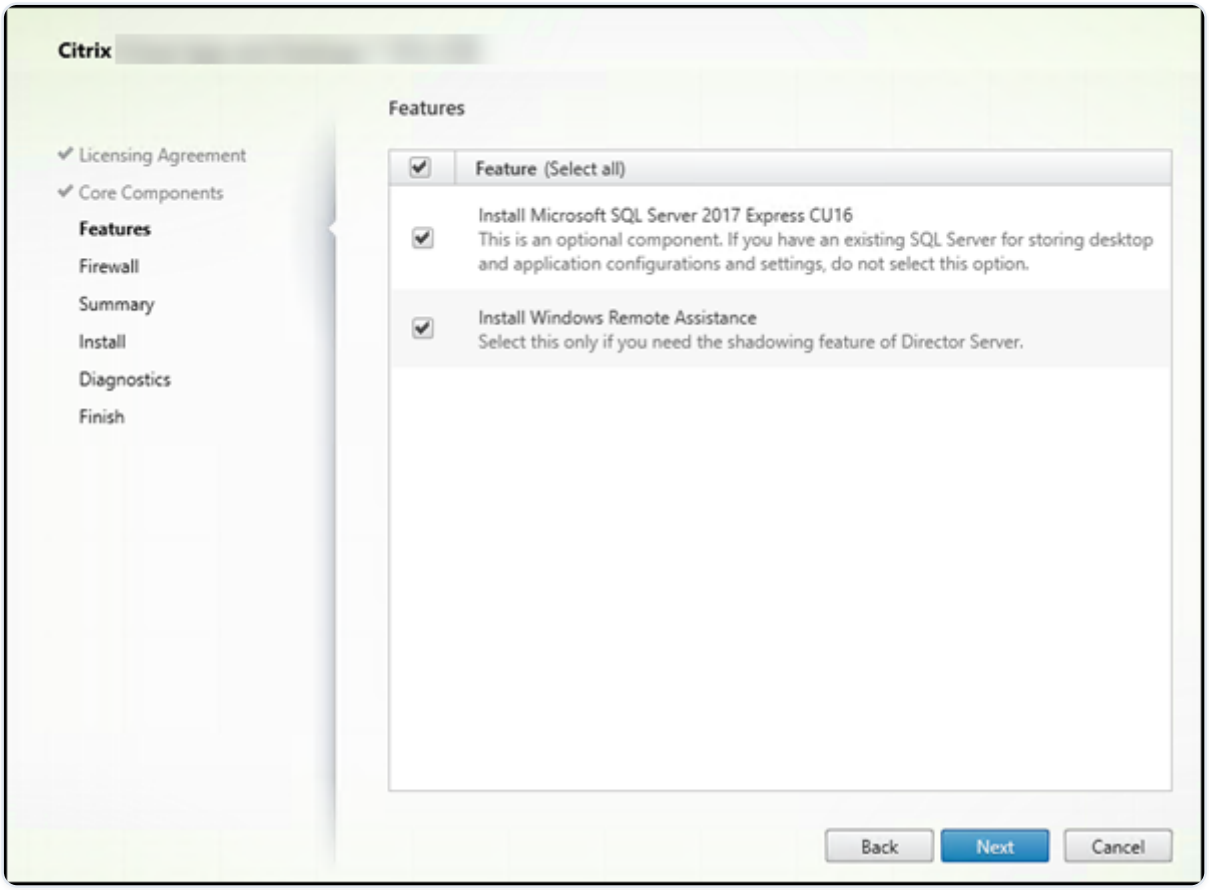
- 推奨: インストールを停止するには、**キャンセル**をクリックします。マシンにRAMを追加してから、再度インストールを開始してください。
- または、**次へ**をクリックしてインストールを続行します。サイトの安定性に問題が発生する可能性があります。

コマンドラインインターフェイス: インストール/アップグレードは終了します。インストールログには、検出された内容と利用可能なオプションを説明するメッセージが含まれています。

- 推奨: マシンにRAMを追加してから、再度コマンドを実行してください。
- または、警告を上書きするために、`/ignore_hw_check_failure`オプションを指定して再度コマンドを実行してください。サイトの安定性に問題が発生する可能性があります。

アップグレード時に、OSまたはSQL Serverのバージョンがサポートされなくなった場合も通知されます。展開のアップグレードを参照してください。

手順 6. 機能の有効化または無効化



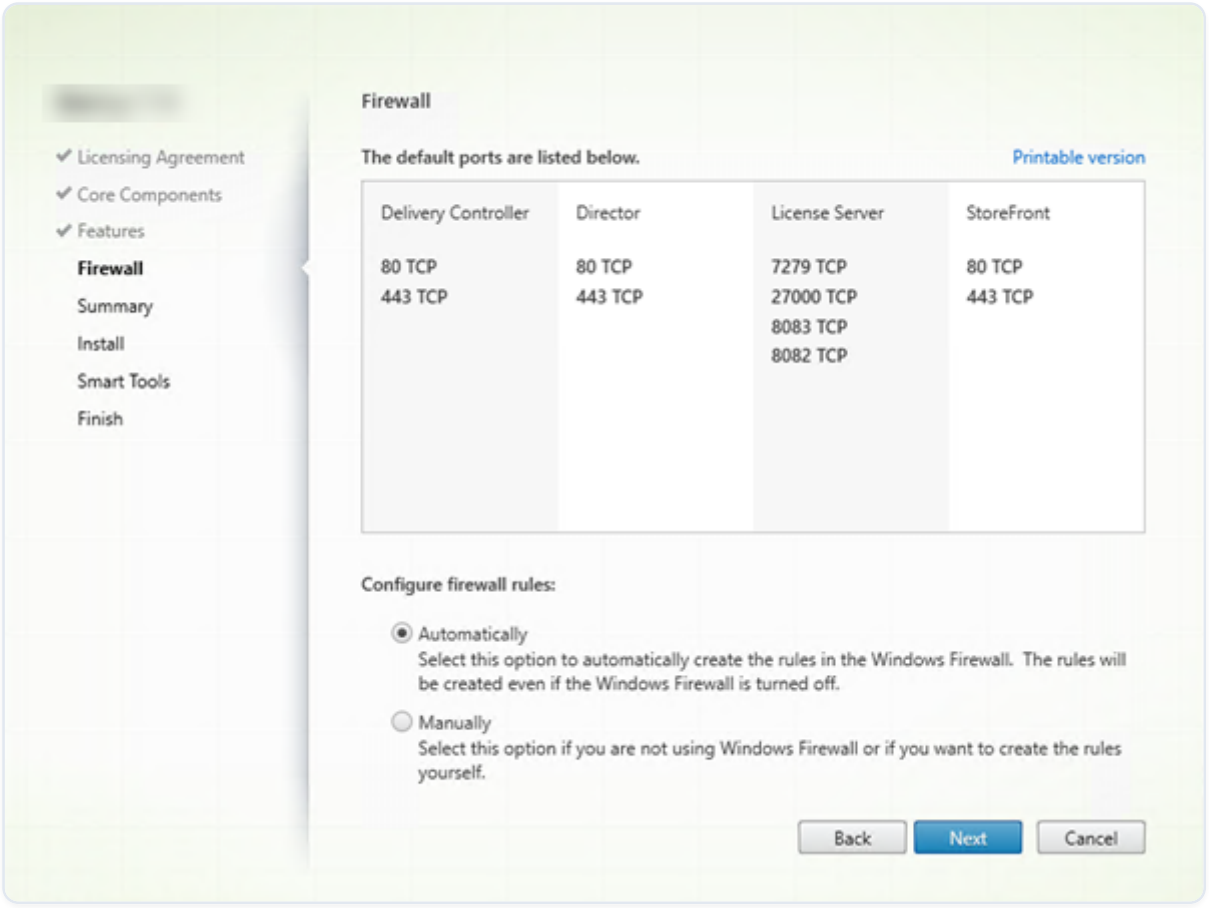
「**機能**」ページで：

- サイトデータベースとして使用するためにMicrosoft SQL Server Expressをインストールするかどうかを選択します。デフォルトでは、この選択は有効になっています。Citrix Virtual Apps and Desktopsデータベースに慣れていない場合は、データベースを確認してください。
- Directorをインストールすると、Windowsリモートアシスタンスが自動的にインストールされます。Directorのユーザーシャドウイングで使用するために、Windowsリモートアシスタンスでシャドウイングを有効にするかどうかを選択します。シャドウイングを有効にすると、TCPポート3389が開きます。デフォルトでは、この機能は有効になっています。ほとんどの展開では、デフォルト設定で問題ありません。この機能は、Directorをインストールしている場合にのみ表示されます。

Nextをクリックします。

コマンドラインオプション：`/nosql`（インストールを防止するため）、`/no_remote_assistance`（有効化を防止するため）

手順7. Windowsファイアウォールポートを開く



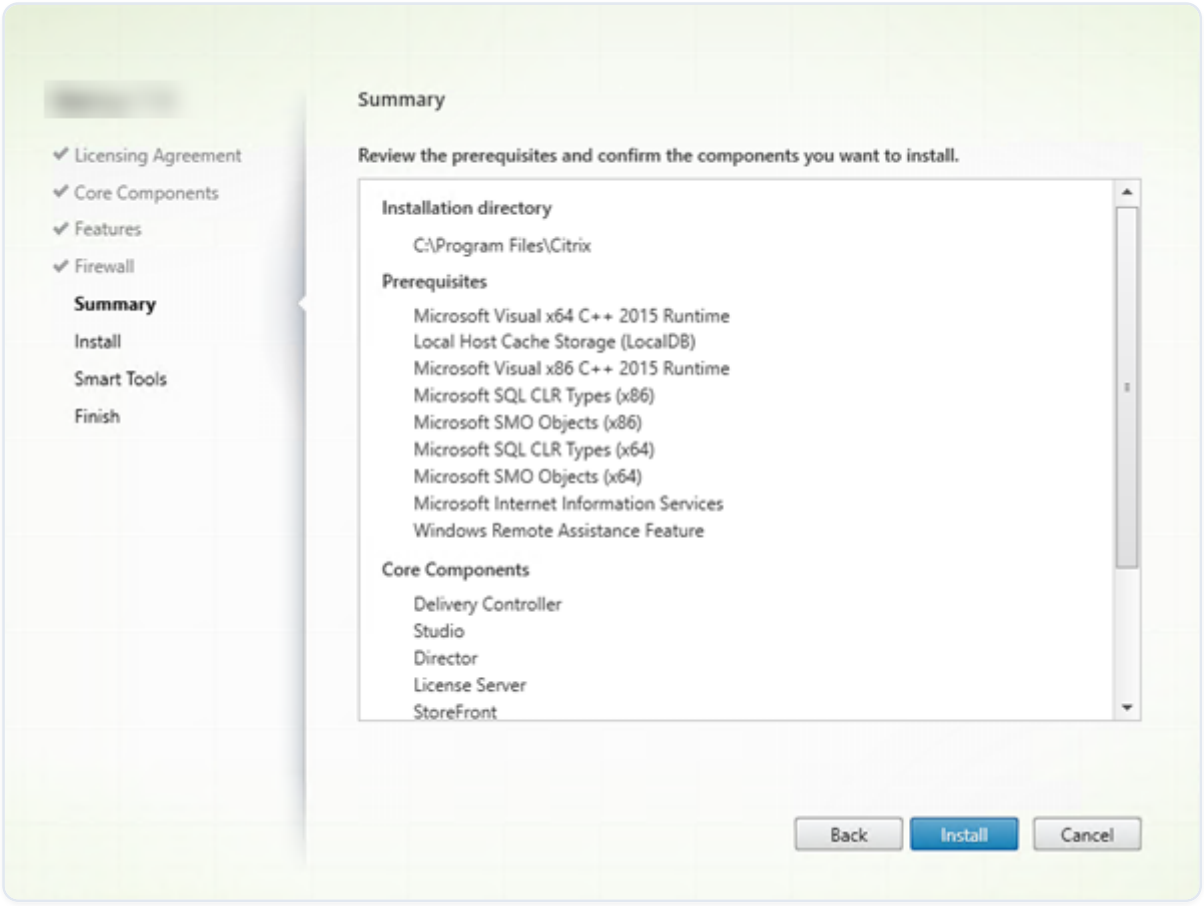
デフォルトでは、Windowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても、**ファイアウォール**ページのポートは自動的に開かれます。ほとんどの展開では、デフォルト設定で問題ありません。ポート情報については、ネットワークポートを参照してください。

Nextをクリックします。

（このグラフィックは、このマシンにすべてのコアコンポーネントをインストールしたときのポートリストを示しています。この種のインストールは通常、テスト展開のみを対象としています。）

コマンドラインオプション：`/configure_firewall`

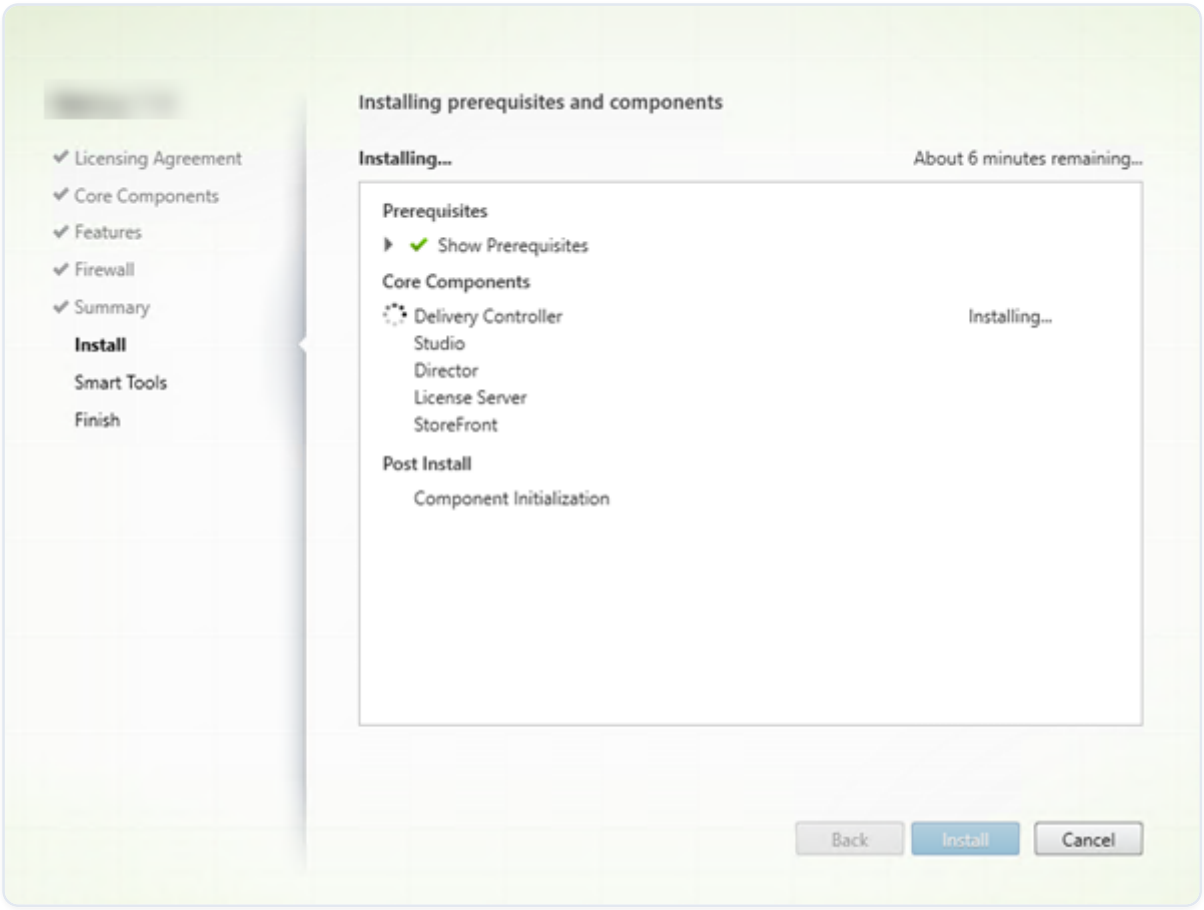
手順8. 前提条件を確認し、インストールを確定する



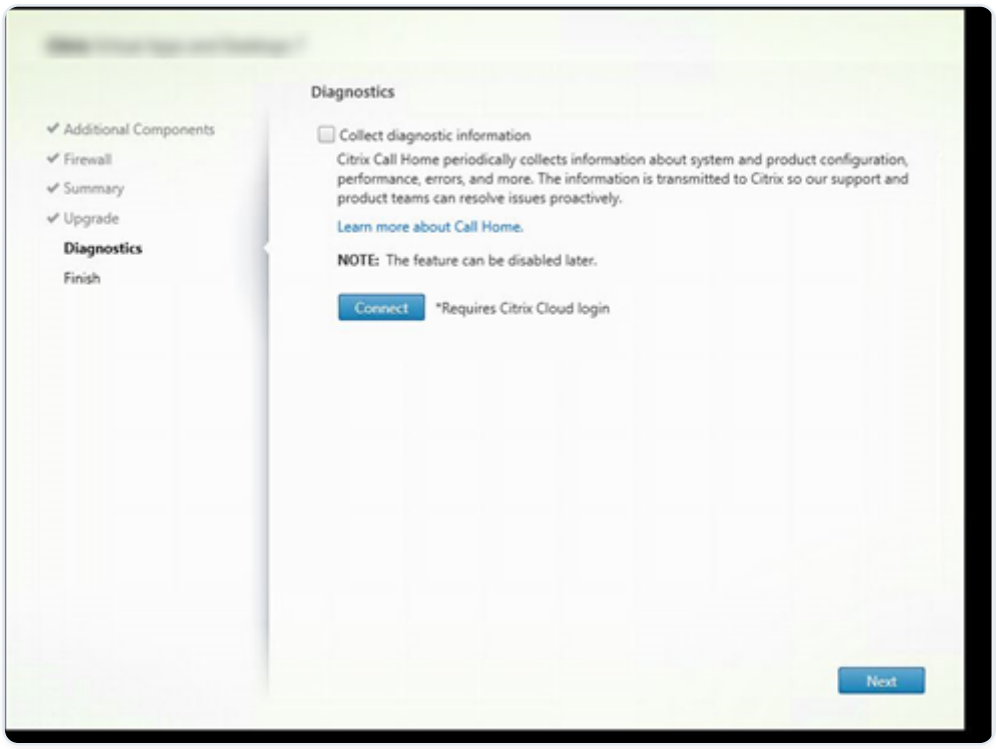
概要ページには、インストールされるものが一覧表示されます。必要に応じて、**戻る**ボタンを使用して以前のウィザードページに戻り、選択を変更します。

準備ができたら、**インストール**をクリックします。

ディスプレイにはインストールの進行状況が表示されます。



ステップ9. Cloud Software Groupとの診断情報の共有



診断ページで、Citrix Call Homeに参加するかどうかを選択します。

このページは、グラフィカルインターフェイスを使用してDelivery Controllerをインストールするときに表示されます。StoreFrontをインストールする場合（ただしControllerではない場合）、ウィザードはこのページを表示します。他のコアコンポーネントをインストールする場合（ただしControllerまたはStoreFrontではない場合）、ウィザードはこのページを表示しません。

アップグレード中に、Call Homeがすでに有効になっている場合、またはインストーラーがCitrix Telemetry Serviceに関連するエラーを検出した場合、このページは表示されません。

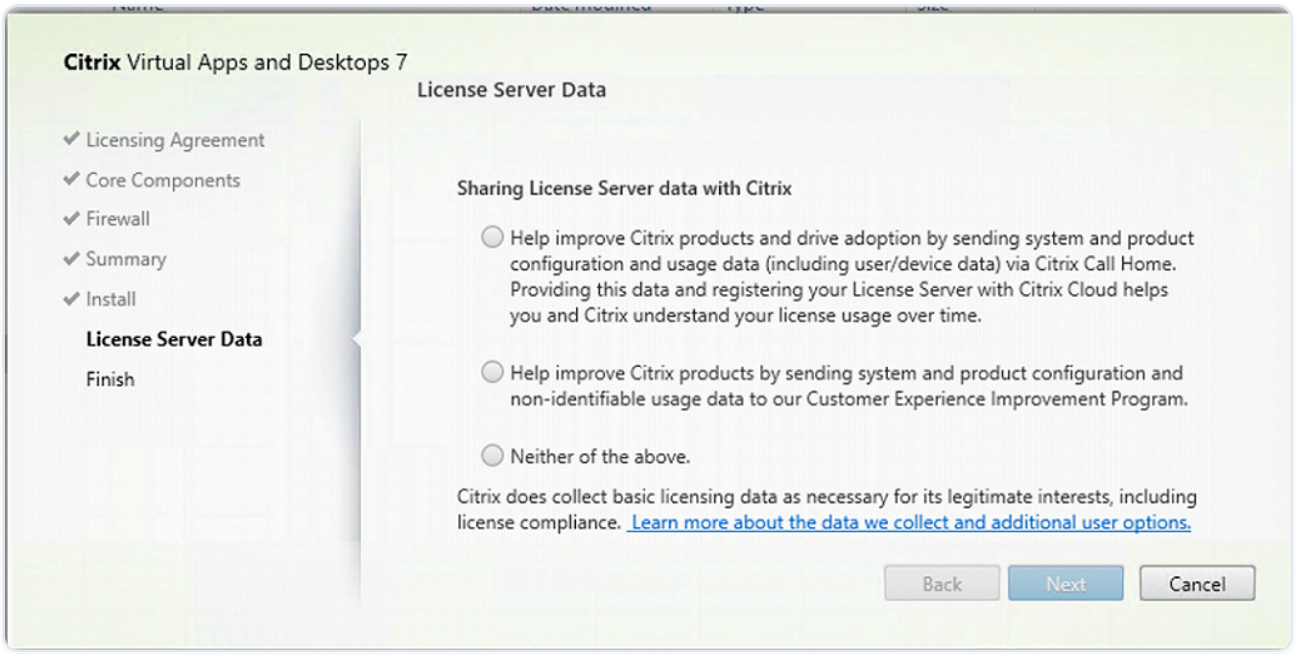
参加することを選択した場合（デフォルト）、**接続**をクリックします。プロンプトが表示されたら、Citrixアカウントの資格情報を入力します。登録の選択は、インストール後に変更できます。

資格情報が検証された後（または参加しないことを選択した場合）、**次へ**をクリックします。

診断ページで、最初に**診断情報の収集**を選択せずに**接続**をクリックすると、**Citrix Insight Servicesに接続**ダイアログを閉じた後、**次へ**ボタンが無効になります。次のページに進むことはできません。**次へ**ボタンを再度有効にするには、**診断情報の収集**を選択し、すぐに選択を解除します。

詳細については、Call Homeを参照してください。

ステップ10. Cloud Software Groupとのライセンスサーバーデータの共有



ライセンスサーバーデータページでは、お客様を支援するために、Call Homeデータまたはカスタマーエクスペリエンス向上プログラム（CEIP）データのいずれかを共有していただくようお願いしています。さらに、Cloud Software Groupは、正当な利益のために必要に応じて、ライセンスコンプライアンスを含む基本的なライセンスデータの収集も要求します。

ライセンスサーバーデータページは、ライセンスサーバーをインストールしたときに表示されます。

- スタンドアロンとして。
- Delivery Controllerのインストール中に、コアコンポーネントとして。

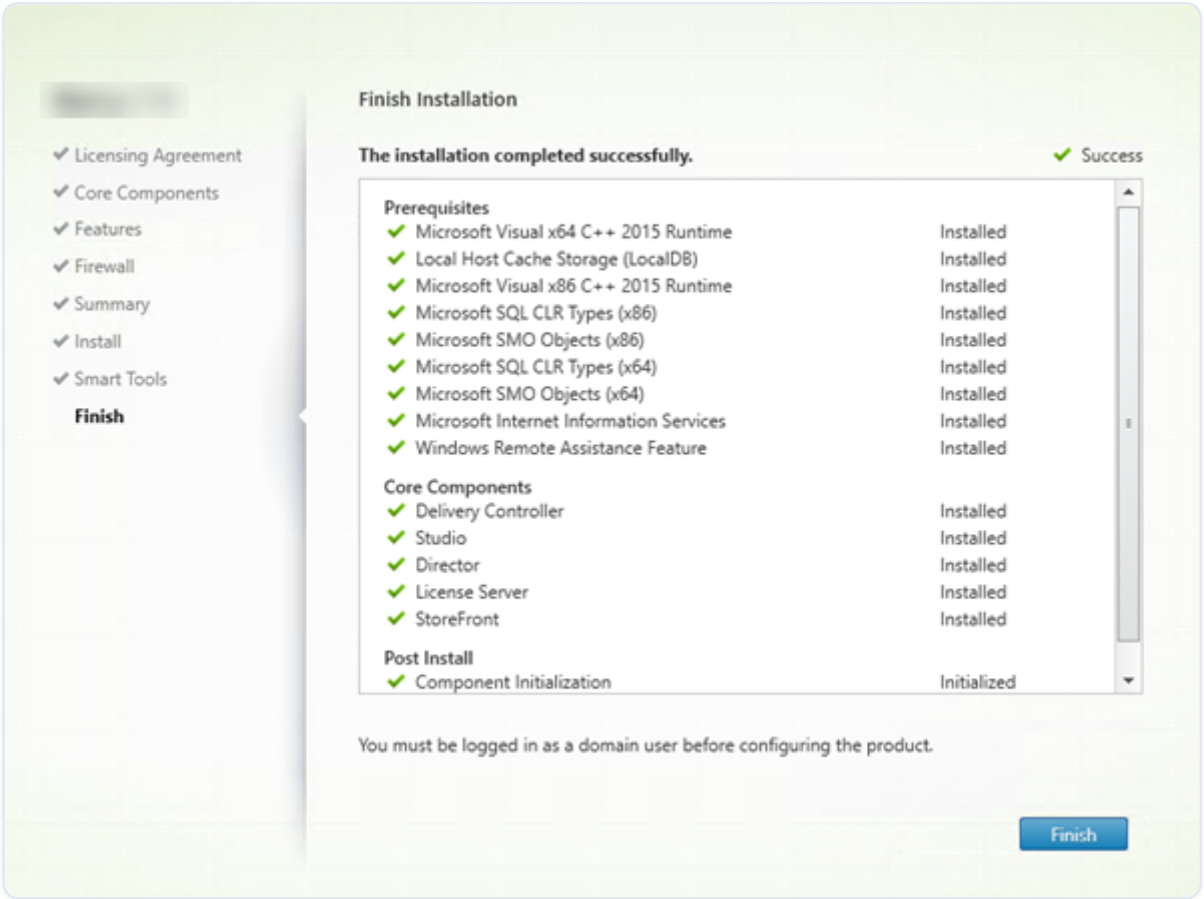
アップグレード中に、`/CITRIX.opt:` ファイルで構成がすでに設定されている場合、このページは表示されません。

ライセンスサーバーは、ライセンスデータ、Call Homeデータ、CEIPデータなど、いくつかの種類のユーザーデータを監視します。Call HomeデータとCEIPデータの収集を有効にするには、参加（オプトイン）を選択する必要があります。

コマンドラインを使用してインストールする際にCall HomeおよびCEIPデータの収集を有効にする方法の詳細については、「コアコンポーネントをインストールするためのコマンドラインオプション」を参照してください。

Cloud Software Groupのライセンスデータ収集の詳細については、「Citrixライセンスデータ収集プログラム」を参照してください。

ステップ11. このインストールを完了する



完了ページには、正常にインストールおよび初期化されたすべての前提条件とコンポーネントに緑色のチェックマークが表示されます。

完了をクリックします。

ステップ12. 残りのコアコンポーネントを他のマシンにインストールする

すべてのコアコンポーネントを1台のマシンにインストールした場合は、「次のステップ」に進みます。そうでない場合は、他のマシンでインストーラーを実行して他のコンポーネントをインストールします。他のサーバーにControllerを追加でインストールすることもできます。

次のステップ

必要なすべてのコンポーネントをインストールしたら、Studioを使用してサイトを作成します。

サイトを作成したら、(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/install-vdas.html)VDAをインストールします。

いつでも、フルプロダクトインストーラーを使用して、以下のコンポーネントで展開を拡張できます。

- **Universal Print Serverサーバーコンポーネント:** ご使用のプリントサーバーでインストーラーを起動します。

  a. **展開の拡張**セクションで**Universal Print Server**を選択します。

  b. ライセンス契約に同意します。

  c. **ファイアウォール**ページでは、Windowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていない場合でも、デフォルトでTCPポート7229および8080がファイアウォールで開かれます。ポートを手動で開きたい場合は、このデフォルトのアクションを無効にできます。

  このコンポーネントをコマンドラインからインストールするには、(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/install-command.html#command-line-options-for-installing-a-universal-print-server)Universal Print Serverをインストールするためのコマンドラインオプションを参照してください。
- (/ja-jp/federated-authentication-service.html)フェデレーション認証サービス。
- (/ja-jp/session-recording.html)セッションレコーディング。
- ワークスペース エンバイロメント マネジメント。

コマンドラインを使用してインストールする

重要:

- アップグレードする場合で、現在のバージョンがPersonal vDiskまたはAppDisksソフトウェアを使用しているか、インストールされている場合は、「PvD、AppDisks、およびサポートされていないホストの削除」を参照してください。
- Citrixは、ライセンスコンプライアンスを含む正当な利益のために、必要に応じて基本的なライセンスデータを収集します。詳細については、「Citrixライセンスデータ」を参照してください。

はじめに

この記事は、Windowsオペレーティングシステムを搭載したマシンへのコンポーネントのインストールに適用されます。Linuxオペレーティングシステム用VDAについては、「Linux Virtual Delivery Agents」を参照してください。

この記事では、製品インストールコマンドの発行方法について説明します。インストールを開始する前に、「インストールの準備」を確認してください。この記事には、利用可能なインストーラーの説明が含まれています。

コマンドの実行の進行状況と戻り値を確認するには、元の管理者であるか、「**管理者として実行**」を使用する必要があります。詳しくは、Microsoftのコマンドに関するドキュメントを参照してください。

インストールコマンドを直接使用することに加えて、Active Directory内のマシンにVDAをインストール、アップグレード、または削除するサンプルスクリプトが製品ISOに用意されています。詳細については、「スクリプトを使用したVDAのインストール」を参照してください。

このCitrix Virtual Apps and Desktopsバージョンでサポートされていないバージョンにインストールまたはアップグレードしようとすると、オプションに関する情報を示すメッセージが表示されます。「以前のオペレーティングシステム」を参照してください。

Citrixがコンポーネントインストールの結果を報告する方法については、「Citrixインストールの戻りコード」を参照してください。

フル製品インストーラーを使用する

フル製品インストーラーのコマンドラインインターフェイスにアクセスするには：

1. Citrixから製品パッケージをダウンロードします。ダウンロードサイトにアクセスするには、Citrixアカウントの資格情報が必要です。
2. ファイルを解凍します。必要に応じて、ISOファイルをDVDに書き込みます。
3. コンポーネントをインストールするサーバーに、ローカル管理者アカウントを使用してログオンします。
4. DVDをドライブに挿入するか、ISOファイルをマウントします。
5. メディアの `\x64\XenDesktop Setup` ディレクトリから、適切なコマンドを実行します。

   コアコンポーネントをインストールするには： コアコンポーネントのインストール用コマンドラインオプションに記載されているオプションを指定して、`XenDesktopServerSetup.exe` を実行します。

   VDAをインストールするには： VDAのインストール用コマンドラインオプションに記載されているオプションを指定して、`XenDesktopVDASetup.exe` を実行します。

   StoreFrontをインストールするには： インストールメディアの `x64 > StoreFront` フォルダーで `CitrixStoreFront-x64.exe` を実行します。

   Universal Print Serverをインストールするには： Universal Print Serverのインストール用コマンドラインオプションのガイダンスに従ってください。

   Federated Authentication Serviceをインストールするには： Citrixでは、グラフィックインターフェイスの使用を推奨しています。

   Session Recordingをインストールするには: Session Recording のガイダンスに従ってください。

   Workspace Environment Managementをインストールするには： Workspace Environment Managementのガイダンスに従ってください。

   Secure Private Accessをインストールするには： インストールメディアの `x64 > XenDesktop` Setupフォルダーで `XenDesktopSPASetup.exe` を実行します。Secure Private Accessのインストール用コマンドラインオプションのガイダンスに従ってください。

コアコンポーネントのインストール用コマンドラインオプション

`XenDesktopServerSetup.exe` コマンドを使用してコアコンポーネントをインストールする場合、次のパラメーターオプションが有効です。オプションの詳細については、コアコンポーネントのインストールを参照してください。

注:

- コアコンポーネントのインストール用コマンドラインオプションを使用している間は、`/exclude` を使用しないでください。
- `/components` を使用して1つのコンポーネントをアップグレードすると、他のコンポーネントもアップグレードされる場合があります。これは、異なるコンポーネント間の潜在的な互換性の問題を回避するためです。
- 1つのコンポーネントのみをアップグレードする場合は、そのコンポーネントの個別のインストーラーを使用してください。展開のアップグレード を参照してください。

- **/ceipoptin** *ceipoptin* など.

  Call Homeデータおよびカスタマーエクスペリエンス向上プログラム（CEIP）データの収集を有効にします。有効な値は次のとおりです。

  - `DIAGNOSTIC`: Citrix LicensingがCall Homeデータを収集できるようにするには、この値を選択します。
  - `ANONYMOUS`: Citrix Licensingが未識別CEIPデータ（ユーザーを特定しないデータ）を収集できるようにするには、この値を選択します。
  - `NONE`: Citrix LicensingによるCEIPデータの収集を無効にするには、この値を選択します。

  Call Homeデータ収集の詳細については、Citrix Licensing Call Home を参照してください。

  CEIPデータ収集の詳細については、Citrix Licensing Customer Experience Improvement Program を参照してください。

  CEIPデータの詳細については、Citrix Licensing CEIP data elements を参照してください。

  License Serverのライセンスデータの詳細については、Citrix Licensing Data を参照してください。

- **/components** *コンポーネント ...*

  インストールまたは削除するコンポーネントのコンマ区切りリスト。有効な値は次のとおりです。

  - `CONTROLLER`: コントローラー
  - `DESKTOPSTUDIO`: スタジオ

- `WEBSTUDIO`: ウェブスタジオ
- `DESKTOPDIRECTOR`: ディレクター
- `LICENSESERVER`: Citrix ライセンスサーバー
- `SECUREPRIVATEACCESS`: セキュアプライベートアクセス

このオプションを省略すると、すべてのコンポーネントがインストールされます（`/remove` オプションも指定されている場合は削除されます）。

(2003年より前のリリースでは、有効な値に`STOREFRONT`が含まれていました。バージョン2003以降では、Use the full-product installerに記載されている専用のStoreFrontインストールコマンドを使用してください)。

- **/onlyprereqs** オプション

  選択したコンポーネントの前提条件のみがインストールされます。Citrix製品コンポーネントはインストールされません。

- **/configure_firewall**

  インストールされているコンポーネントが使用するWindowsファイアウォールのすべてのポートを開きます。Windowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても開きます。サードパーティ製ファイアウォールまたはファイアウォールを使用していない場合は、手動でポートを開く必要があります。

- **/disableexperiencemetrics** オプション

  インストール、アップグレード、または削除中に収集された分析データがCitrixに自動的にアップロードされるのを防ぎます。

- **/help** または **/h**

  コマンドヘルプを表示します。

- **/ignore_hw_check_failure**

  ハードウェアチェックが失敗した場合（例えば、RAM不足のためなど）でも、Delivery Controllerのインストールまたはアップグレードを続行できます。詳細については、「ハードウェアチェック」を参照してください。

- **/ignore_site_test_failure**

  Controllerのアップグレード中にのみ有効です。通常、サイトテストの失敗は無視され、アップグレードは続行されます。省略された場合（またはfalseに設定された場合）、サイトテスト

の失敗があると、アップグレードを実行せずにインストーラーが失敗します。デフォルト = false

アップグレード中に、サポートされていないSQL Serverバージョンが検出された場合、このオプションは無視されます。詳細については、「SQL Serverバージョンチェック」を参照してください。

- **/installdir** *ディレクトリ*

  コンポーネントがインストールされる既存の空のディレクトリ。デフォルト = `c:\Program Files\Citrix`。

- **/logpath** *パス*

  ログファイルの場所。指定されたフォルダーは存在している必要があります。インストーラーは作成しません。デフォルト = `TEMP%\Citrix\XenDesktop Installer`

- **/no_remote_assistance**

  Directorのインストール時にのみ有効です。Windowsリモートアシスタンスを使用するユーザーシャドウイング機能を無効にします。

- **再起動なし**

  インストール後の再起動を防止します。（ほとんどのコアコンポーネントでは、再起動はデフォルトで有効になっていません。）

- **再開しない**

  デフォルトでは、インストール中にマシンの再起動が必要な場合、再起動が完了するとインストーラーは自動的に再開します。このデフォルトを上書きするには、`/noresume` を指定します。これは、メディアを再マウントする必要がある場合や、自動インストール中に情報を取得したい場合に役立ちます。

- **ノースキューエル**

  コントローラーをインストールするサーバーへのMicrosoft SQL Server Expressのインストールを防止します。このオプションを省略すると、SQL Server Expressがサイトデータベースとして使用するためにインストールされます。

  このオプションは、ローカルホストキャッシュに使用されるSQL Server Express LocalDBのインストールには影響しません。

- **サイレント** または **パッシブ**

インストール中にユーザーインターフェイスは表示されません。インストールプロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **/削除**

  `/components`オプションで指定されたコアコンポーネントを削除します。

- **/すべて削除**

  インストールされているすべてのコアコンポーネントを削除します。

- **/SKIPHDXDRIVERCHECK**

  VDAメタインストーラーへのHDX™ドライバーのチェックをスキップします。

- **/エクスペリエンスメトリックを送信**

  インストール、アップグレード、または削除中に収集された分析データをCitrixに自動的に送信します。このオプションを省略した場合（または`/disableexperiencemetrics`が指定された場合）、分析データはローカルで収集されますが、自動的には送信されません。

- **/一時ディレクトリ** *ディレクトリ*

  インストール中に一時ファイルを保持するディレクトリ。デフォルト = `c:\Windows\Temp`。

- **/XenApp**

  Citrix Virtual Apps をインストールします。このオプションを省略すると、Citrix Virtual Apps and Desktops™ がインストールされます。

コアコンポーネントのインストール例

次のコマンドは、サーバーにDelivery Controller™、Studio、Citrix Licensing、およびSQL Server Expressをインストールします。コンポーネント通信に必要なファイアウォールポートは自動的に開かれます。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver /configure_firewall
```

次のコマンドは、サーバーにCitrix Virtual Apps™ Controller、Studio、およびSQL Server Expressをインストールします。コンポーネント通信に必要なファイアウォールポートは自動的に開かれます。

```
\x64\XenDesktop Setup\\XenDesktopServerSetup.exe /xenapp /components controller,desktopstudio /configure_firewall
```

次のコマンドは、サーバーにDelivery Controller、Secure Private Access、およびSQL Server Expressをインストールします。コンポーネント通信に必要なファイアウォールポートは自動的に開かれます。

`\x64\XenDesktop Setup XenDesktopServerSetup.exe /xenapp /components controller,secureprivateaccess /configure_firewall`

Citrix Virtual Apps and Desktops バージョン 2407 から 2411 以降にアップグレードする場合、またはバージョン 2411 以降を新規インストールする場合は、最初のステップとして License Server を最新バージョン（バージョン 11.2.17 ビルド 51000）に更新してください。その後、Delivery Controller をアップグレードします。これを怠ると、コマンドラインでのインストールとアップグレードが失敗します。License Server および Delivery Controller、Web Studio、Citrix Director などのコンポーネントをアップグレードするには、次のコマンドを実行します（マウントされた ISO の \x64 フォルダー内にいることを前提とします）。

1. 次を実行します。

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet
   ```

   ライセンスバイナリをローカルドライブのいずれかにコピーしている場合は、次のコマンドを実行します。

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet /l install.log
   ```

2. 次を実行します。

   ```
   \x64\XenDesktop Setup\XenDesktopServerSetup.exe  /components
   "CONTROLLER,DESKTOPSTUDIO,DESKTOPDIRECTOR" /CONFIGURE_FIREWALL
   ```

スタンドアロンVDAインストーラーを使用する

ダウンロードサイトにアクセスするには、Citrixアカウントの資格情報が必要です。インストールを開始する前に管理者権限を昇格させるか、**管理者として実行**を使用する必要があります。

1. Citrixから適切なパッケージをダウンロードします。

   - マルチセッションOS仮想デリバリーエージェント: `VDAServerSetup_xxxx.exe`
   - シングルセッションOS仮想デリバリーエージェント: `VDAWorkstationSetup_xxxx.exe`

- シングルセッションOSコアサービス仮想デリバリーエージェント: `VDAWorkstationCoreSetup_xxxx.exe`

2. まず、パッケージから既存のディレクトリにファイルを抽出し、その後インストールコマンドを実行するか、または単にパッケージを実行します。

   ファイルをインストールする前に抽出するには、絶対パスを指定して`/extract`を使用します（例: `C:\YourExtractFolder\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`）。ディレクトリは存在している必要があります。そうでない場合、抽出は失敗します。その後、別のコマンドで、この記事に記載されている有効なオプションを使用して、適切なコマンドを実行します。

   - `VDAServerSetup_XXXX.exe`の場合、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`を実行します
   - `VDAWorkstationCoreSetup_XXXX.exe`の場合、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe`を実行します
   - `VDAWorkstationSetup_XXXX.exe`の場合、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`を実行します

   ダウンロードしたパッケージを実行するには、その名前（`VDAServerSetup.exe`、`VDAWorkstationSetup.exe`、または`VDAWorkstationCoreSetup.exe`）を実行します。この記事に記載されている有効なオプションを使用してください。

フル製品インストーラーに慣れている場合：

- スタンドアロンの`VDAServerSetup.exe`または`VDAWorkstationSetup.exe`インストーラーを、名前以外はすべて`XenDesktopVdaSetup.exe`コマンドであるかのように実行します。
- `VDAWorkstationCoreSetup.exe`インストーラーは異なります。これは、他のインストーラーで利用可能なオプションのサブセットをサポートしているためです。

VDA をインストールするためのコマンドラインオプション

次のオプションは、以下の1つ以上のコマンド（インストーラー）で有効です。`VDAServerSetup_xxxx.exe`、`VDAWorkstationSetup_xxxx.exe`、および`VDAWorkstationCoreSetup_xxxx.exe`。

オプションの詳細については、VDAのインストールを参照してください。

- **/コンポーネント** *コンポーネント*\[,*コンポーネント*\]

インストールまたは削除するコンポーネントのコンマ区切りリスト。有効な値は次のとおりです。

- `VDA`: バーチャル デリバリー エージェント
- `PLUGINS`: シトリックス ワークスペース™ アプリ for Windows

VDA と Windows 用 Citrix Workspace アプリをインストールするには、`/components vda,plugins` を指定するか、コンポーネントをまったく指定しないでください。コンポーネントが指定されていない場合、デフォルトでは VDA のみがインストールされます。

VDA のみをインストールし、Citrix Workspace アプリのインストールを除外するには、`/components vda` を指定します。

このオプションは、`VDAWorkstationCoreSetup_xxxx.exe`インストーラーを使用している場合は無効です。そのインストーラーはCitrix Workspaceアプリをインストールできません。

- **前提条件のみ**

  選択したコンポーネントの前提条件のみがインストールされます。Citrix 製品コンポーネントはインストールされません。

- **/controllers** "*コントローラー*\[*コントローラー*\]"

  VDAが通信できるコントローラーのスペース区切りのFQDNを、二重引用符で囲んで指定します。`/site_guid`オプションと`/controllers`オプションの両方を指定しないでください。

- **disableexperiencemetrics** オプション

  インストール、アップグレード、または削除中に収集された分析データがCitrixに自動的にアップロードされるのを防ぎます。

- **/enable_hdx_ports**

  Windowsファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、VDAおよび有効な機能（Windowsリモートアシスタンスを除く）に必要なWindowsファイアウォールのポートを開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、ネットワークポートを参照してください。

  HDX アダプティブトランスポートが使用する UDP ポートを開くには、この `/enable_hdx_ports` オプションに加えて、`/enable_hdx_udp_ports` オプションを指定します。

- **/enable_hdx_udp_ports**

Windows Firewall Serviceが検出された場合、ファイアウォールが有効になっていなくても、HDXアダプティブトランスポートが使用するUDPポートをWindowsファイアウォールで開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、手動でファイアウォールを構成する必要があります。ポート情報については、「ネットワークポート」を参照してください。

VDAが使用する追加ポートを開くには、この`/enable_hdx_udp_ports`オプションに加えて、`/enable_hdx_ports`オプションを指定します。

- **/enable_hdx_tls_dtls**

  HDX Direct V1用にTCPおよびUDPポート443を開きます。

- **/enable_real_time_transport**

  オーディオパケットにUDPを使用するかどうかを有効または無効にします（オーディオ用のRealTime Audio Transport）。この機能を有効にすると、オーディオパフォーマンスが向上する可能性があります。Windows Firewall Serviceが検出されたときにUDPポートを自動的に開く場合は、`/enable_hdx_ports`オプションを含めます。

- **/enable_remote_assistance**

  Directorで使用するために、Windowsリモートアシスタンスのシャドウイング機能を有効にします。このオプションを指定すると、Windowsリモートアシスタンスはファイアウォールで動的ポートを開きます。

- **/enablerestore** または **/enablerestorecleanup**

  （シングルセッションVDAのみ有効）VDAのインストールまたはアップグレードが失敗した場合に、復元ポイントへの自動復帰を有効にします。

  インストール/アップグレードが正常に完了した場合：

  - `/enablerestorecleanup`は、インストーラーに復元ポイントを削除するよう指示します。
  - `/enablerestore`は、使用されなかった場合でも、インストーラーに復元ポイントを保持するように指示します。

  詳細については、インストールまたはアップグレードの失敗時の復元を参照してください。

- **/ENABLE_SECURE_DEFAULTS**

  より安全な初期設定のために、さまざまな機能のデフォルト設定を有効から無効に変更します。関連する機能は次のとおりです: クライアントドライブリダイレクト、特殊フォルダーリダイレクト、ドラッグアンドドロップ、クライアントTWAINデバイスリダイレクト、クライア

ントUSBプラグアンドプレイデバイスリダイレクト、クライアントプリンターリダイレクト、クライアントクリップボードリダイレクト、およびクライアントマイクデバイスリダイレクト。

- **/enable_ss_ports**

  Windowsファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、画面共有に必要なWindowsファイアウォールのポートを開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。

- **/exclude** "*コンポーネント*"\[,"*コンポーネント*"\]

  1つまたは複数のコンマ区切りのオプションコンポーネントのインストールを防止します。各コンポーネントは二重引用符で囲まれています。たとえば、MCSによって管理されていないイメージにVDAをインストールまたはアップグレードする場合、Machine Identity Serviceコンポーネントは必要ありません。有効な値は次のとおりです。

マルチセッションOS	シングルセッションOS	シングルセッションOSコアサービス
`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`
`Citrix Backup and Restore`	`Citrix Backup and Restore`	`Citrix Browser Content Redirection`
`Citrix Browser Content Redirection`	`Citrix Browser Content Redirection`	`Citrix Personalization for App-V - VDA`
`Citrix MCS IODriver`	`Citrix MCS IODriver`	`Citrix Telemetry Service`
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`	`Citrix Universal Print Client`
`Citrix Profile Management`	`Citrix Profile Management`	`Citrix Vda Log Capture Service`
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`	`CSE Component`

マルチセッションOS	シングルセッションOS	シングルセッションOSコアサービス
Citrix Rendezvous V2	Citrix Rendezvous V2	Director VDA Plug-in
Citrix Telemetry Service	Citrix Telemetry Service	Machine Management Provider
Citrix Universal Print Client	Citrix Universal Print Client	VDA Monitor Plug-in
Citrix Vda Log Capture Service	Citrix Vda Log Capture Service	VDA WMI Proxy Plug-in
Citrix VDA Upgrade Agent	Citrix VDA Upgrade Agent	
CSE Component	CSE Component	
Director VDA Plug-in	Director VDA Plug-in	
Machine Identity Service	Machine Identity Service	
Machine Management Provider	Machine Management Provider	
VDA Monitor Plug-in	User Personalization Layer	
VDA WMI Proxy Plug-in	VDA Monitor Plug-in	
	VDA WMI Proxy Plug-in	
Citrix App Protection Component	Citrix App Protection Component	Citrix App Protection Component
Citrix HyperV Filter Driver	Citrix HyperV Filter Driver	
Citrix Personalization for App-V - VDA	Citrix Personalization for App-V - VDA	Citrix Personalization for App-V - VDA

Citrix Profile Management をインストールから除外すると (`/exclude "Citrix Profile Management"`)、Citrix Director を使用した VDA の監視とトラブルシューティングに影響します。**ユーザーの詳細**ページと**エンドポイント**ページでは、パーソナライゼーションパネルとログオン期間パネルが機能しません。**ダッシュボード**ページと**トレンド**ページでは、平均ログオン期間パネルは、Profile Management がインストールされているマシンのみのデータを表示します。

サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrix Profile Management Service をインストールして実行することをお勧めします。Citrix Profile Management Service を有効にする必要はありません。

同じコンポーネント名で `/exclude` と `/includeadditional` の両方を指定した場合、そのコンポーネントはインストールされません。

このオプションは、`VDAWorkstationCoreSetup.exe` インストーラーを使用する場合は無効です。そのインストーラーは、これらの項目の多くを自動的に除外します。

- **/h** または **/help**

  コマンドのヘルプを表示します。

- **/includeadditional** "*コンポーネント*"\[,"*コンポーネント*"\]

  1つまたは複数のコンマ区切りのオプションコンポーネント（それぞれを引用符で囲む）のインストールを含めます。このオプションは、Remote PC Access 展開を作成していて、デフォルトでは含まれていない他のコンポーネントをインストールしたい場合に役立ちます。有効な値は次のとおりです。

マルチセッションOS	シングルセッションOS
`Citrix Backup and Restore`	`Citrix Backup and Restore`
`Citrix MCS IODriver`	`Citrix MCS IODriver`
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`
`Citrix Profile Management`	`Citrix Profile Management`
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`
`Citrix Rendezvous V2`	`Citrix Rendezvous V2`

マルチセッションOS	シングルセッションOS
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`
`Citrix Web Socket Vda Registration Tool`	`Citrix Web Socket Vda Registration Tool`
`Machine Identity Service`	`Machine Identity Service`
	`User Personalization Layer`

同じコンポーネント名で`/exclude`と`/includeadditional`の両方を指定した場合、そのコンポーネントはインストールされません。

- **/installdir** *ディレクトリ*

  コンポーネントがインストールされる既存の空のディレクトリ。デフォルト = `c:\Program Files\Citrix`。

- **/install_mcsio_driver**

  使用しないでください。代わりに`/includeadditional "Citrix MCS IODriver"`または`/exclude "Citrix MCS IODriver"`を使用してください。

- **/logpath** *パス*

  ログファイルの場所。指定されたフォルダーは存在している必要があります。インストーラーは作成しません。デフォルト = 「`%TEMP%\Citrix\XenDesktop Installer`」

  このオプションはグラフィカルインターフェイスでは使用できません。

- **マスターイメージ**

  VMにVDAをインストールする場合にのみ有効です。VDAを他のマシンを作成するために使用するイメージとして設定します。このオプションは`/mastermcsimage`と同等です。

  このオプションは、`VDAWorkstationCoreSetup_xxxx.exe`インストーラーを使用している場合は無効です。

- **/マスターMCSイメージ**

  このマシンがMachine Creation Servicesでイメージとして使用されることを指定します。このオプションは`/masterimage`と同等です。

- **/マスターPVSイメージ**

このマシンが、Citrix Provisioning™ またはサードパーティのプロビジョニングツール (Microsoft System Center Configuration Manager など) を使用して、VM をプロビジョニングするためのイメージとして使用されることを指定します。

- **/ウェブソケットトークン** *WebSocketToken*

  Web Socket VDAを作成します。WebSocketTokenは、必要なトークン用です。

- **/ウェブソケットトークンファイル** *FileContainingWebSockToken*

  Web Socket VDAを作成します。*FileContainingWebSockToken* は、必要なトークンを含むファイル用です。

- **/ウェブソケットトークンstdin** *<WebSocketToken*

  Web Socket VDAを作成します。*<WebSocketToken* は、STDINによって渡される必要なトークン用です。

- **/no_mediafoundation_ack**

  Microsoft Media Foundationがインストールされていないことを確認し、いくつかのHDXマルチメディア機能がインストールされず、動作しないことを承認します。このオプションが省略され、Media Foundationがインストールされていない場合、前提条件が満たされていないため、VDAのインストールは終了します。ほとんどのサポートされているWindowsエディションには、Nエディションを除き、Media Foundationがすでにインストールされています。Windowsの機能 > メディア機能 を *手動* で 有効にした場合、Citrix Meta Installerが探すレジストリキーに値が設定されていない可能性があります。インストールプロセスを開始する前に、`SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\Windows-Features\WindowsMediaVersion` レジストリキーをチェックして、値が存在し、空でないことを確認してください。

- **/ノードキュメントエクスペリエンス**

  拡張デスクトップエクスペリエンス機能は利用できなくなりました。このオプション（およびポリシー設定）は、指定されても無視されます。

  マルチセッションOS用VDAのインストール時にのみ有効です。拡張デスクトップエクスペリエンス機能の有効化を防止します。この機能は、拡張デスクトップエクスペリエンスCitrixポリシー設定でも制御されます。

- **/noreboot** 再起動しない

  インストール後の再起動を防止します。VDAは再起動後まで使用できません。

- **/noresume** 再開しない

デフォルトでは、インストール中にマシンの再起動が必要な場合、再起動が完了するとインストーラーは自動的に再開します。デフォルトを上書きするには、`/noresume` を指定します。これは、メディアを再マウントする必要がある場合や、自動インストール中に情報を取得したい場合に役立ちます。

- **/physicalmachine** 物理マシン

  RemotePCインストールでは、この引数を `/remotepc` とともに使用します。そうしないと、特定のユーザーシナリオでVDAが予期したとおりに動作しない可能性があります。

- **/portnumber** *port* ポート番号

  `/reconfig` オプションが指定されている場合にのみ有効です。VDAとController間の通信を有効にするポート番号。以前に構成されたポートは、ポート80でない限り無効になります。

- **/proxyconfig** “*address or PAC file path*” プロキシ構成

  環境でGateway Serviceなどのサービスと Rendezvous V2プロトコルを使用する予定があり、ネットワークにアウトバウンド接続用の非透過型プロキシがある場合は、ここでプロキシを指定します。HTTPプロキシのみがサポートされています。Rendezvousプロトコルで使用するプロキシのアドレスまたはPACファイルのパス。このコマンドラインは、/includeadditional "Citrix Rendezvous V2" が使用されたかのように、Citrix Rendezvous V2を自動的にインストールします。機能の詳細については、Rendezvous protocol を参照してください。

  - プロキシアドレスの形式: `http://<url-or-ip>:<port>`
  - PACファイルの形式: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **/quiet** または **/passive**

  インストール中にユーザーインターフェイスは表示されません。インストールおよび構成プロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **/再構成**

  `/portnumber`、`/controllers`、または `/enable_hdx_ports` オプションと組み合わせて使用すると、以前に構成されたVDA設定をカスタマイズします。このオプションを `/quiet` オプションも指定せずに指定すると、VDAをカスタマイズするためのグラフィカルインターフェイスが起動します。

- **/リモートPC**

リモートPCアクセス展開（シングルセッションOS）またはブローカー接続（マルチセッションOS）の場合にのみ有効です。追加コンポーネントのインストールを除外します（`/exclude` および `/includeadditional` オプションのコンポーネントリストを参照）。

このオプションは、`VDAWorkstationCoreSetup.exe` インストーラーを使用する場合は無効です。そのインストーラーは、これらのコンポーネントのインストールを自動的に除外します。

`/remotepc` は `/servervdi` オプションと互換性がありません。

- **/削除**

  `/components` オプションで指定されたコンポーネントを削除します。

- **/remove_appdisk_ack**

  インストールされている場合、AppDisks™ VDAプラグインをアンインストールすることをVDAインストーラーに許可します。

- **/remove_pvd_ack**

  インストールされている場合、Personal vDiskをアンインストールすることをVDAインストーラーに許可します。

- **/すべて削除**

  VDAを削除します。Citrix Workspaceアプリ（インストールされている場合）は削除しません。

- **/REMOVEALLWITHCWA**

  VDA とともに CWA を削除します。

- **/エクスペリエンスメトリック送信**

  インストール、アップグレード、または削除中に収集された分析データをCitrixに自動的に送信します。このオプションを省略した場合（または `/disableexperiencemetrics` オプションが指定された場合）、分析データはローカルで収集されますが、自動的には送信されません。

- **/サーバーVDI**

  サポートされているWindowsマルチセッションマシンにシングルセッションOS用VDAをインストールします。Windowsマルチセッションマシンにマルチセッション OS用VDAをインストールする場合は、このオプションを省略してください。

  このオプションを使用する前に、サーバーVDI を参照してください。

このオプションは、フルプロダクトVDAインストーラーでのみ使用してください。

- **/サイトGUID** *GUID*

  サイトのActive Directory組織単位（OU）のグローバル一意識別子。これは、検出にActive Directoryを使用している場合に、仮想デスクトップをサイトに関連付けます（自動更新が推奨されるデフォルトの検出方法です）。サイトGUIDは、Studioに表示されるサイトプロパティです。`/site_guid`と`/controllers`の両方のオプションを指定しないでください。

- **/一時ディレクトリ** *ディレクトリ*

  インストール中に一時ファイルを保持するディレクトリ。デフォルト = `c:\Windows\Temp`。

  このオプションはグラフィカルインターフェイスでは利用できません。

- **/仮想マシン**

  VMにVDAをインストールする場合にのみ有効です。BIOS情報がVMに渡されることで物理マシンとして認識される、物理マシンのインストーラーによる検出を上書きします。

  このオプションはグラフィカルインターフェイスでは利用できません。

- **/ゼンデスクトップクラウド**

  VDAがCitrix DaaS (Citrix Cloud™) 展開環境にインストールされていることを示します。

VDAのインストール例

フルプロダクトインストーラーを使用してVDAをインストールする:

次のコマンドは、シングルセッションOSおよびCitrix Workspaceアプリ用のVDAを、VM上のデフォルトの場所にインストールします。このVDAはイメージとして使用され、MCSを使用してVMをプロビジョニングします。VDAは、`mydomain`ドメイン内の`Contr-Main`という名前のサーバー上のControllerに最初に登録されます。VDAはユーザーパーソナライゼーションレイヤーとWindowsリモートアシスタンスを使用します。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins /controllers "Contr-Main.mydomain.local" /enable_hdx_ports /includeadditional "user personalization layer" /mastermcsimage /enable_remote_assistance
```

VDAWorkstationCoreSetupスタンドアロンインストーラーを使用してシングルセッションOS VDAをインストールする:

次のコマンドは、リモートPCアクセスまたはVDI展開環境で使用するために、シングルセッションOSにコアサービスVDAをインストールします。Citrix Workspaceアプリおよびその他の非コア

サービスはインストールされません。Controllerのアドレスが指定され、Windowsファイアウォールサービスのポートは自動的に開かれます。管理者が再起動を処理します。

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.com" /enable_hdx_ports /noreboot
```

VDAをカスタマイズする

VDAをインストールした後、いくつかの設定をカスタマイズできます。製品メディアの`\x64\XenDesktop Setup`ディレクトリから、VDAのインストール用コマンドラインオプションで説明されている以下のオプションを1つ以上使用して、`XenDesktopVdaSetup.exe`を実行します。

- `/reconfigure`（VDAをカスタマイズする際に必須）
- `/h` または `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

VDAのトラブルシューティング

- デリバリーグループのStudio表示では、**詳細**ペインの**インストール済みVDAバージョン**エントリが、マシンにインストールされているバージョンではない場合があります。マシンのWindowsのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされた後、Delivery Controllerに登録されるまで、ユーザーにアプリやデスクトップを配信することはできません。

  VDA登録方法と登録の問題のトラブルシューティング方法については、「VDA登録」(/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/vda-registration.html)を参照してください。

Universal Print Serverをインストールするためのコマンドラインオプション

次のオプションは、`XenDesktopPrintServerSetup.exe`コマンドで有効です。

- **/enable_upsserver_port**

このオプションが指定されていない場合、インストーラーはグラフィカルインターフェイスから**ファイアウォール**ページを表示します。インストーラーにWindowsファイアウォールルールを自動的に追加させるには**自動**を選択し、管理者が手動でファイアウォールを構成できるようにするには**手動**を選択します。

印刷サーバーにソフトウェアをインストールした後、(/ja-jp/citrix-virtual-apps-desktops/2411/printing/printing-provision-printers.html)のガイダンスを使用してUniversal Print Serverを構成します。

Secure Private Accessをインストールするためのコマンドラインオプション

以下のオプションは、両方で有効です。

1. CVADインストーラー: `XenDesktopSPASetup.exe`
2. SPAオンプレミスインストーラー: `SecurePrivateAccessSetup_XXXX.exe`

- **/enable_spa_ports**

  Windows Firewallサービスが検出された場合、ファイアウォールが有効になっていなくても、Secure Private Accessに必要なポートをWindowsファイアウォールで開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、手動でファイアウォールを構成する必要があります。ポート情報については、「ネットワークポート」を参照してください。

- **ノーエスキューエル**

  Secure Private Accessをインストールするサーバーへの Microsoft SQL Server Expressのインストールを防止します。このオプションを省略すると、サイトデータベースとしてSQL Server Expressがインストールされます。

- **/help または /h または /?**

  コマンドのヘルプを表示します

- **/noreboot** オプション

  インストール後の再起動を防止します。再起動するまでSecure Private Accessは使用できません。

- **/quiet または /passive**

  インストール中にユーザーインターフェイスは表示されません。インストールと構成プロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- /削除

  Secure Private Accessを削除します。

オプションの詳細については、「Secure Private Accessインストーラー」を参照してください。

詳細情報

Citrixがコンポーネントインストールの結果を報告する方法については、「Citrixインストールのリターンコード」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/install-prepare.html#citrix-installation-return-codes)を参照してください。

Web Studio のインストール

はじめに

Citrix Studio は、Citrix Virtual Apps and Desktops 展開を構成および管理できる Windows ベースの管理コンソールです。Web Studio は、Citrix Studio の次世代版であり、Citrix Studio と完全に同等の機能を備えた Web ベースの管理コンソールです。(/ja-jp/citrix-daas/overview#studio) と同じルックアンドフィールで、Web Studio はネイティブの Web エクスペリエンスを提供することで、管理エクスペリエンスを最新化します。

Web Studio は、Internet Information Service (IIS) がインストールされている任意の Windows サーバーに展開できます。展開オプションは次の2つです。

- 専用サーバーにインストールする:

  パフォーマンスとスケーラビリティが重要となる大規模な環境では、Web Studio を専用サーバーにインストールすることをお勧めします。このサーバーは、オプションで Director もホストできます。

- Delivery Controller™ と統合する:

  迅速な展開やシンプルな環境では、Web Studio を Delivery Controller に直接インストールします。このアプローチは、管理オーバーヘッドの最小化が優先される小規模な展開に最適です。

次の図は、Web Studio のアーキテクチャを示しています。

Web Studio のアーキテクチャ(/en-us/citrix-virtual-apps-desktops/2411/media/web-studio-architecture.png)

Web Studio を稼働させるための一般的なワークフローは次のとおりです。

1. Web Studio をインストールする。

2. TLS 用の証明書を構成する。
3. サイトをセットアップする。
4. 管理のために Delivery Controller を Web Studio に追加する。
5. (オプション) Delivery Controller のプロキシとして Web Studio を構成する
6. (オプション) Pendo を無効にする。
7. Web Studio にサインインする。

負荷分散された Web Studio 展開をセットアップするには、こちらの記事を参照してください。

Web Studio で利用可能な新機能

新機能の記事を参照してください。

システム要件

サポートされているオペレーティングシステム:

- Windows Server 2025、Standard および Datacenter Edition、および Server Core オプション
- Windows Server 2022、Standard および Datacenter Edition、および Server Core オプション
- Windows Server 2019、Standard および Datacenter Edition、および Server Core オプション
- Windows Server 2016、Standard および Datacenter Edition、および Server Core オプション

サポートされているブラウザー:

- マイクロソフト エッジ 92
- ファイアフォックス ESR (延長サポート版) 90
- グーグル クローム 92
- サファリ 14

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

前提条件

Web Studioのこのリリースは、Citrix Virtual Apps and Desktops™ 2212展開以降と互換性があります。

2212より前の展開の場合、まず2212にアップグレードしてからWeb Studioをインストールします。

既知の制限事項

Web StudioとCitrix Studioを相互に利用する場合、以下の制限事項を考慮してください。Web Studioで作成されたテンプレートはCitrix Studioに表示されず、その逆も同様です。これは、Web Studioがテンプレートを保存するためにCitrix Studioとは異なるデータベースを使用しているためです。回避策として、Web Studioでテンプレートからポリシーを作成し、その後Citrix Studioでこのポリシーからテンプレートを作成し、その逆も同様に行ってください。

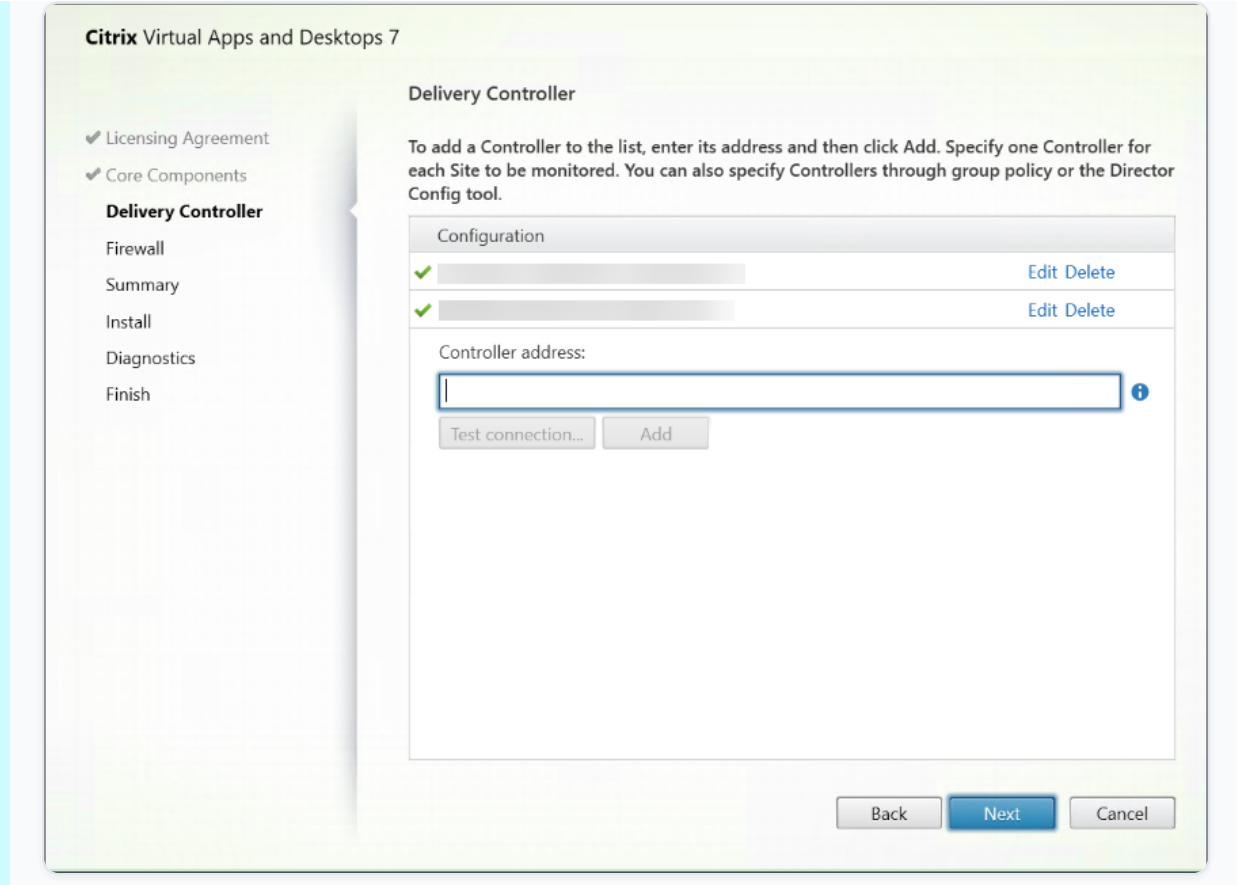
- Web Studioのインストールを成功させるには、Internet Information Services (IIS) マネージャーでデフォルトのサイト名 (**Default Web Site**) を変更しないでください。デフォルトのサイト名を変更すると、インストールが失敗します。

Web Studioのインストール

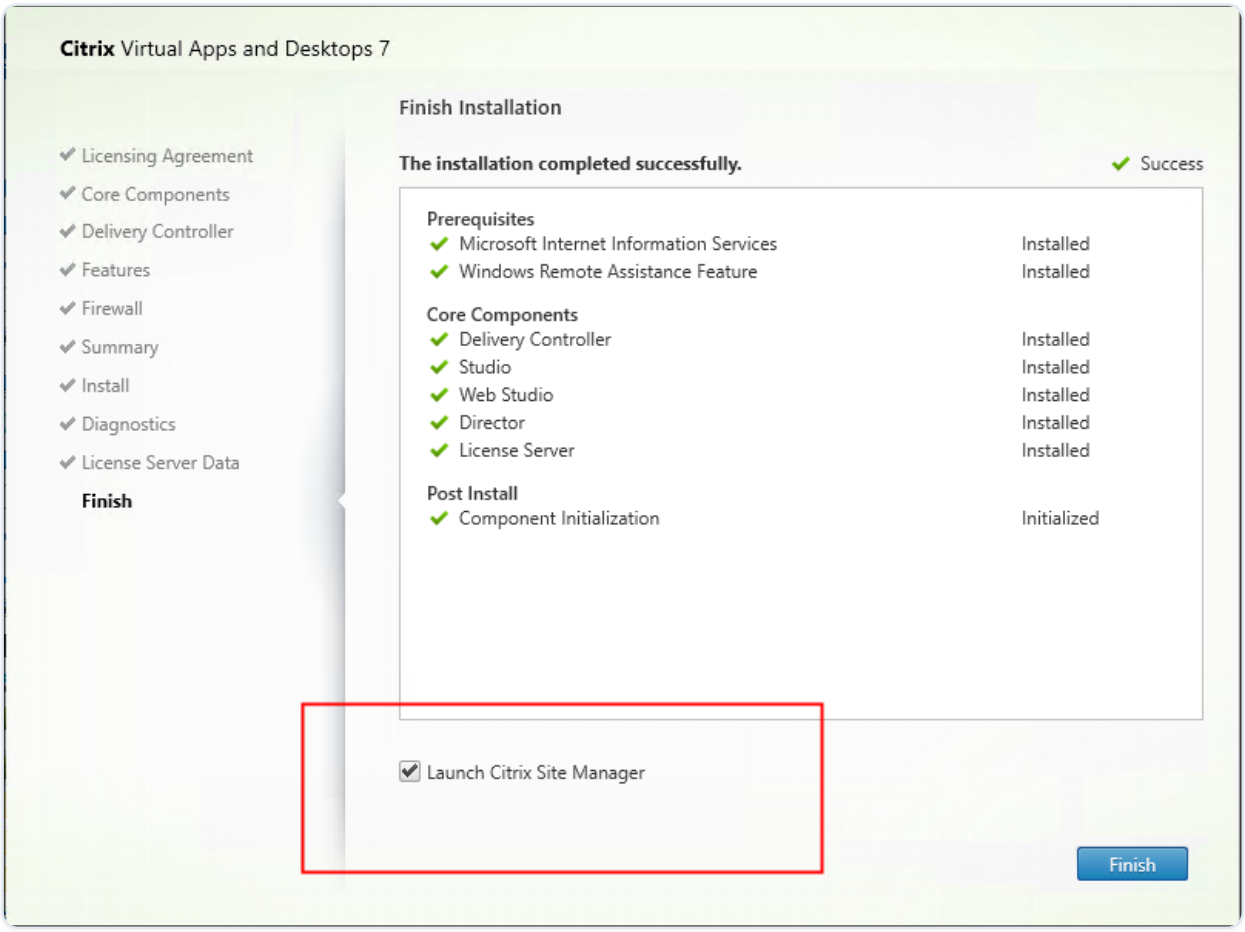
以下の情報は、コアコンポーネントのインストールのガイダンスを補足するものです。Web Studioをインストールするには：

- Citrix Virtual Apps and Desktopsのフル製品ISOインストーラーを使用してWeb Studioをインストールします。ISOインストーラーは前提条件を確認し、不足しているコンポーネントをインストールし、Web Studio Webサイトをセットアップし（Delivery Controllerのインストールに含まれている場合はDelivery Controller上に）、基本的な構成を実行します。
- インストール時にWeb Studioが含まれていなかった場合は、インストーラーを使用してWeb Studioを追加します。
- Web Studioのインストール時に、Delivery ControllerのFQDNを入力するよう求められます。

> **注：**
>
> - 複数のDelivery Controllerを追加できます。Web Studioは、ランダムな順序でそれらに接続を試みます。Web Studioが接続しようとしているDelivery Controllerに到達できない場合、Web Studioは自動的に他のDelivery Controllerにフォールバックします。
> - Directorが**コアコンポーネント**で選択されインストールされている場合、ここに追加するDelivery ControllerはWeb StudioとDirectorの両方で使用されます。
> - デリバリーコントローラーがTLS用に構成されている（推奨）場合、入力されたFQDNは、デリバリーコントローラーにインストールされている証明書の共通名またはサブジェクトの別名と一致する必要があります。



- **完了**ページで、**サイトマネージャーを起動**チェックボックスがデフォルトで選択されているため、Citrix Site Managerが自動的に開きます。後で起動するには、デスクトップのスタートメニューを開き、**Citrix > Citrix Site Manager**を選択します。Web Studioを起動する前に、Citrix Site Managerを使用してサイトを作成するか、既存のサイトに参加する必要があります。詳しくは、サイトのセットアップを参照してください。



注:

コマンドラインを使用してWeb Studioをインストールすることもできます。例：`.\XenDesktopServerSetup.exe /components webstudio /controllers "ddc1.studio.local" /configure_firewall /quiet`。詳しくは、コマンドラインを使用したインストールを参照してください。

TLS 用の証明書を構成する

デフォルトでは、IISがHTTPS用にまだ構成されていない場合、インストーラーはサーバーのFQDNを証明書の共通名として使用して自己署名証明書を作成し、それをポート443にバインドします。この動作により、ユーザーはローカルマシンからWeb Studioにアクセスできますが、証明書が信頼されていないため、他のマシンから接続するユーザーにはセキュリティ警告が表示されます。この証明書を、エンタープライズまたはパブリック認証局（CA）によって署名された証明書に置き換えることをお勧めします。詳しくは、Web StudioおよびDirectorでTLSを有効にするを参照してください。TLS証明書がIISにすでに構成されている場合、インストーラーは変更を行いません。

サイトをセットアップする

Citrix Virtual Apps and Desktops展開（サイトとも呼ばれます）をセットアップするには、Citrix Site Managerツールを使用します。このツールは、Delivery Controllerとともに自動的にインストールされます。

サイトをセットアップするには、次の手順に従います。

1. Delivery Controller で、デスクトップのスタートメニューを開き、**Citrix > Citrix Site Manager** を選択します。
2. Citrix Site Manager で、**Create a site** を選択します。サイトセットアップウィザードが表示されます。
3. サイトを作成し、その設定を次のように構成します。

   - **Introduction** ページで、サイトの名前を入力します。
   - **Databases** ページには、サイト、監視、および構成ログのデータベースを設定するための選択肢が含まれています。詳細については、「手順 3. データベース」を参照してください。
   - **Licensing** ページで、ライセンスサーバーのアドレスを指定し、使用する（インストールする）ライセンスを示します。詳細については、「手順 4. ライセンス」を参照してください。

4. **Summary** ページで、すべての設定を確認し、**Submit** をクリックします。

   このControllerのIPアドレスは、サイトに自動的に追加されます。

> **注:**
>
> サイトを作成したユーザーは、そのサイトのフル管理者になります。詳細については、「委任管理」を参照してください。

サイトの作成後に新しいControllerをインストールする場合は、そのControllerをサイトに追加する必要があります。詳細な手順は次のとおりです。

1. この新しいControllerでCitrix Site Managerを実行します。
2. **Join an existing site** を選択します。
3. サイトに既に追加されているControllerのアドレスを入力します。
4. **Submit** をクリックします。

管理のためにDelivery ControllerをWeb Studioに追加する

Studio構成ツールを使用して、管理のためにDelivery ControllerをWeb Studioに追加します。このツールはWeb Studioのインストールフォルダーにあります。

既定では、ツールは次の既定のフォルダーにインストールされます。

- `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`

Web Studio で管理するサイト用に、次の 2 つの Delivery Controller (`ddc1.studio.local` と `ddc2.studio.local`) を構成するとします。次の PowerShell コマンドを実行します。

- `.\StudioConfig.exe --server "ddc1.studio.local,ddc2.studio.local"`

> **注：**
>
> - このツールには、コンピューターの管理者権限が必要です。
> - IIS サーバーのキャッシュ設定により、Delivery Controller の構成変更がすぐに有効にならない場合があります。すぐに有効にするには、Web Studio サーバーに移動し、インターネットインフォメーションサービス（IIS）マネージャーを開き、*Server_name* **> サイト > Default Web Site** に移動して、 ペインで を選択します。
> - 新しい FQDN で Delivery Controller を再展開する場合は、`StudioConfig.exe` を使用して Web Studio で、および `C:\Program Files\Citrix\Web Studio\Site\assets\json\manifest.json` ファイルで FQDN を更新します。`manifest.json` ファイルを更新しないと、古い FQDN が Web Studio のサインインウィンドウに表示されたままになります。その結果、サインイン時に新しい FQDN を代替として入力する必要があります。
> - サポートされているすべてのパラメーターを表示するには、`StudioConfig.exe --help` を実行します。

(オプション) Web Studio を Delivery Controller のプロキシとして構成する

既定では、Web Studio コンソールを使用して展開を管理する場合、Web ブラウザーを介して Web Studio サーバーと Delivery Controller の両方に接続します。Web Studio サーバーを Delivery Controller のプロキシとして構成するオプションが用意されています。その結果、展開を管理するときは Web Studio サーバーにのみ接続します。

このセクションでは、Web Studio サーバーを Delivery Controller のプロキシとして構成する方法について説明します。Web Studio と Delivery Controller が異なるサーバーにインストールされていることを前提としています。

開始する前に、展開に必要なすべてのコアコンポーネントがインストールされていることを確認してください。詳しくは、「コアコンポーネントのインストール」を参照してください。

Web Studio のプロキシモードを有効にするには、次の手順に従います。

1. Web Studio サーバーで、Windows PowerShell を管理者として実行します。
2. 次のコマンドを実行し、`fqdn_of_webstudio_machine` を Web Studio サーバーの FQDN に置き換えます。

   `& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --enableproxy --proxyserver "fqdn_of_webstudio_machine"`

   > **注:**
   >
   > 負荷分散された Web Studio 展開がある場合は、`fqdn_of_webstudio_machine` をロードバランサーサーバー (仮想サーバーとも呼ばれます) の FQDN に置き換えます。詳細については、「負荷分散された Web Studio 展開のセットアップ」を参照してください。

Web Studio のプロキシモードを無効にするには、この PowerShell コマンドを実行します。

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --disableproxy
```

(オプション) Pendo を有効または無効にする

バージョン 2411 以降、Web Studio は Pendo を統合しており、これはデフォルトで有効になっています。Pendo は、Citrix プライバシーポリシー に従って使用状況データを収集します。また、Web Studio の右下隅にアイコンを追加し、コンテキストに応じた機能情報とフィードバックオプションを提供します。使用状況データを共有したくない場合は、Studio 構成ツールを使用して Pendo を無効にできます。

このツールは Web Studio のインストールフォルダーにあります。デフォルトでは、ツールは次のフォルダーにインストールされます: `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`。

Pendo を無効にするには、次の手順に従います。

1. Web Studio にサインインします。右下隅にアイコンが表示されている場合、Pendo は有効になっています。
2. Web Studio サーバーで、Windows PowerShell を管理者として実行します。 この PowerShell コマンドを実行します。

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --disablependo
```

Pendo を有効にするには、このコマンドを実行します。

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --enablependo
```

Web Studio にサインインする

1. デフォルトのポート番号 443 が使用されている場合は、`https://<address of the server hosting Web Studio>/Citrix/Studio` で Web Studio にアクセスします。別のポートが構成されている 場合は、`https://<address of the server hosting Web Studio>:<port number>/Citrix/Studio` を使用します。

   Delivery Controller を Web Studio に追加 しており、それらに到達可能な場合、サインインページが表示されます。

   > **注:**
   >
   > 以下の場合は、**サインインできません**ページが表示されます。
   >
   > - サイトにDelivery Controllerが指定されていません。接続するためにDelivery Controllerを追加するよう求められます。
   > - 指定されたDelivery Controllerに到達できません。接続を確認するには、**テスト**をクリックします。または、代替のDelivery Controllerを入力して**接続**をクリックします。

2. **ユーザー名**、**パスワード**、**ドメイン**を入力します。
3. **サインイン**をクリックします。

次のステップ

1. VDAのインストール
2. Web Studioを使用して、次の方法で仮想アプリとデスクトップをユーザーに配信します。
    a. マシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create.html)
    b. デリバリーグループを作成する(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/delivery-groups-create.html)
    c. アプリケーショングループを作成する（オプション）(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/application-groups-create.html)

VDAのインストール

> **重要:**
>
> - アップグレード中で、現在のバージョンにPersonal vDiskまたはAppDisksソフトウェアがインストールされている場合は、「PvD、AppDisks、およびサポートされていないホストの削除」(/ja-jp/citrix-virtual-apps-desktops/2411/upgrade-migrate/upgrade.html#remove-pvd-appdisks-and-unsupported-hosts)を参照してください。
> - Citrix®によって配布されるバイナリは署名されています。署名されたバイナリは、Citrixが生成した証明書または信頼できるサードパーティの証明書のいずれかによって検証されていることを示します。

> Windowsマシン用のVDAには、マルチセッションOS用VDAとシングルセッションOS用VDAの2種類があります。（Linuxマシン用VDAについては、「Linux Virtual Delivery Agent」(/ja-jp/linux-virtual-delivery-agent.html)のドキュメントを参照してください。）

インストールを開始する前に、「インストールの準備」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/install-prepare.html)を確認し、すべての準備タスクを完了してください。

VDAをインストールする前に、コアコンポーネントをインストールしてください。VDAをインストールする前にサイトを作成することもできます。

この記事では、VDAをインストールする際のインストールウィザードの順序について説明します。コマンドラインの同等機能が提供されています。詳細については、「コマンドラインを使用し

たインストール」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/install-core/install-command)を参照してください。

ステップ1. 製品ソフトウェアをダウンロードしてウィザードを起動する

フルプロダクトインストーラーを使用している場合:

1. 製品ISOをまだダウンロードしていない場合:
   - Citrixアカウントの資格情報を使用して、Citrix Virtual Apps and Desktops™のダウンロードページにアクセスします。製品ISOファイルをダウンロードします。
   - ファイルを解凍します。必要に応じて、ISOファイルをDVDに書き込みます。
2. VDAをインストールするイメージまたはマシンで、ローカル管理者アカウントを使用します。DVDをドライブに挿入するか、ISOファイルをマウントします。インストーラーが自動的に起動しない場合は、マウントされたドライブ上の**AutoSelect**アプリケーションをダブルクリックします。

   インストールウィザードが起動します。

スタンドアロンパッケージを使用している場合:

1. Citrixアカウントの資格情報を使用して、Citrix Virtual Apps and Desktopsダウンロードページにアクセスします。適切なパッケージをダウンロードします:
   - `VDAServerSetup_2308.exe`: マルチセッションOS VDA *バージョン*
   - `VDAWorkstationSetup_2308.exe`: シングルセッションOS VDA *バージョン*
   - `VDAWorkstationCoreSetup_2308.exe`: シングルセッションOSコアサービスVDA *バージョン*
2. パッケージを右クリックし、**管理者として実行**を選択します。

   インストールウィザードが起動します。

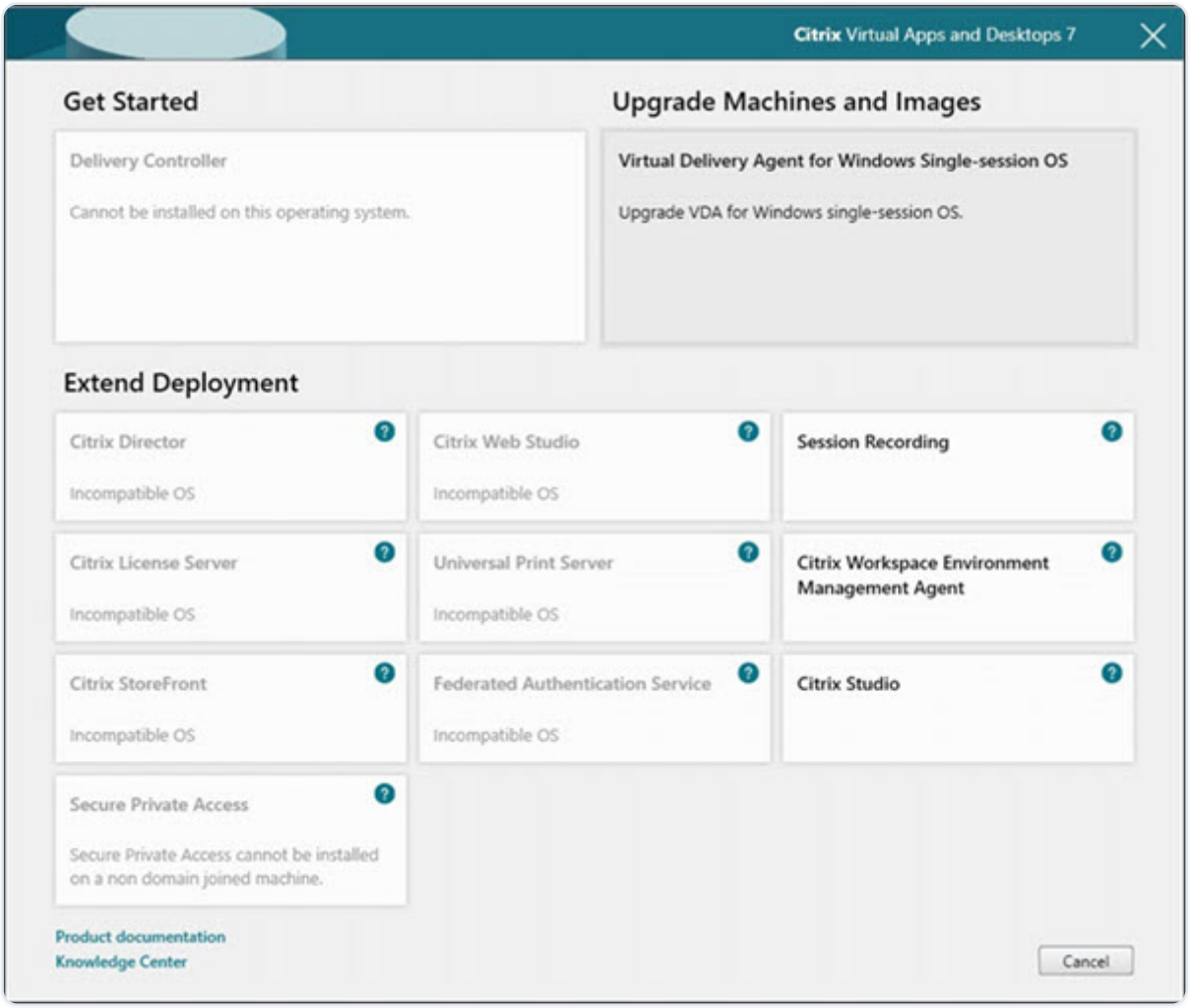
ステップ2. インストールする製品を選択する



インストールする製品（Citrix Virtual AppsまたはCitrix Virtual Desktops）の横にある**開始**をクリックします。(マシンにCitrix Virtual AppsまたはCitrix Virtual Desktopsコンポーネントがすでにインストールされている場合、このページは表示されません。)

コマンドラインオプション: Citrix Virtual Appsをインストールするための`/xenapp`。このオプションが省略された場合、Citrix Virtual Desktopsがインストールされます。

ステップ3. VDAを選択する

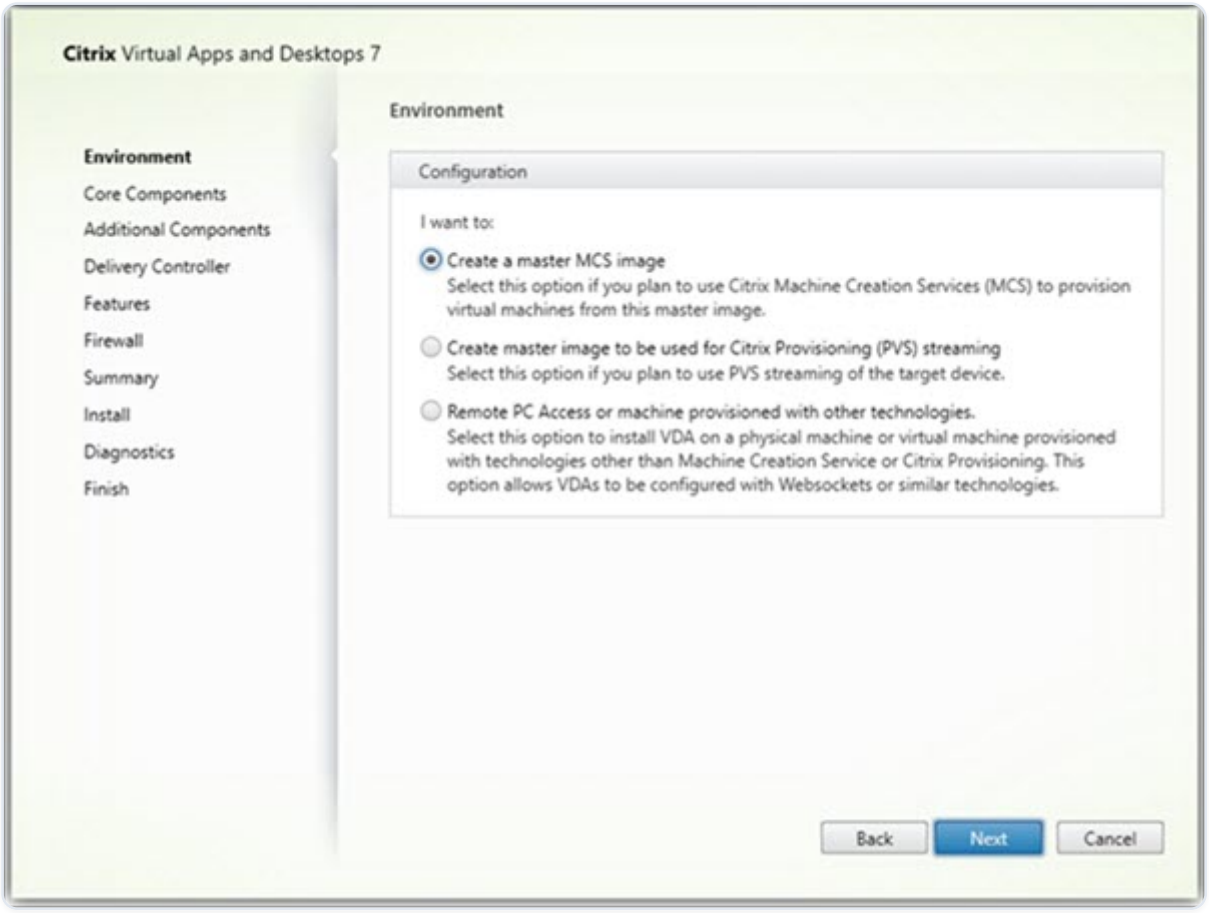


Virtual Delivery Agentエントリを選択します。インストーラーは、シングルセッションOSまたはマルチセッションOSのどちらで実行されているかを認識しているため、適切なVDAタイプのみを提供します。

例えば、Windows Server 2019マシンでインストーラーを実行すると、マルチセッションOS用VDAオプションが利用可能です。シングルセッションOS用VDAオプションは提供されません。

このCitrix Virtual Apps and Desktopsバージョンでサポートされていないオスにwindows VDAをインストール（またはアップグレード）しようとすると、オプションに関する情報を示すメッセージが表示されます。

ステップ4. VDAの使用方法を指定する



環境ページで、VDAの使用方法を指定します。このマシンをイメージとして使用して、さらに多くのマシンをプロビジョニングするかどうかを示します。

選択したオプションは、Citrix Provisioning™ツールが自動的にインストールされるかどうか（もしあれば）、およびVDAインストーラーの追加コンポーネントページのデフォルト値に影響します。

VDAをインストールすると、いくつかのMSI（プロビジョニング用およびその他）が自動的にインストールされます。これらのインストールを防ぐ唯一の方法は、コマンドラインインストールで`/exclude`オプションを使用することです。

次のいずれかを選択します。

- **マスターMCSイメージを作成する:** Machine Creation Services™を使用してVMをプロビジョニングする予定がある場合は、このオプションを選択してVDAをVMイメージにインストールします。このオプションは、Machine Identity Serviceをインストールします。これがデフォルトのオプションです。

  コマンドラインオプション：`/mastermcsimage`または`/masterimage`

> **重要:**
>
> インストールメディアまたはISOイメージはローカルにマウントする必要があります。ソフトウェアのインストールを目的として、ネットワークドライブからISOイメージをマウントすることはサポートされていません。

- **Citrix Provisioningまたはサードパーティのプロビジョニングツールを使用してマスターイメージを作成する:** Citrix Provisioningまたはサードパーティのプロビジョニングツール（Microsoft System Center Configuration Managerなど）を使用してVMをプロビジョニングする予定がある場合は、このオプションを選択してVDAをVMイメージにインストールします。

  コマンドラインオプション：`/masterpvsimage`
- （マルチセッションOSマシンでのみ表示）**サーバーへの仲介接続を有効にする：** 他のマシンをプロビジョニングするためのイメージとして使用されない物理マシンまたは仮想マシンにVDAをインストールするには、このオプションを選択します。

  コマンドラインオプション：`/remotepc`
- (シングルセッションOSマシンにのみ表示) **Remote PC Access を有効にする:** このオプションを選択すると、Remote PC Access で使用する VDA を物理マシンにインストールできます。

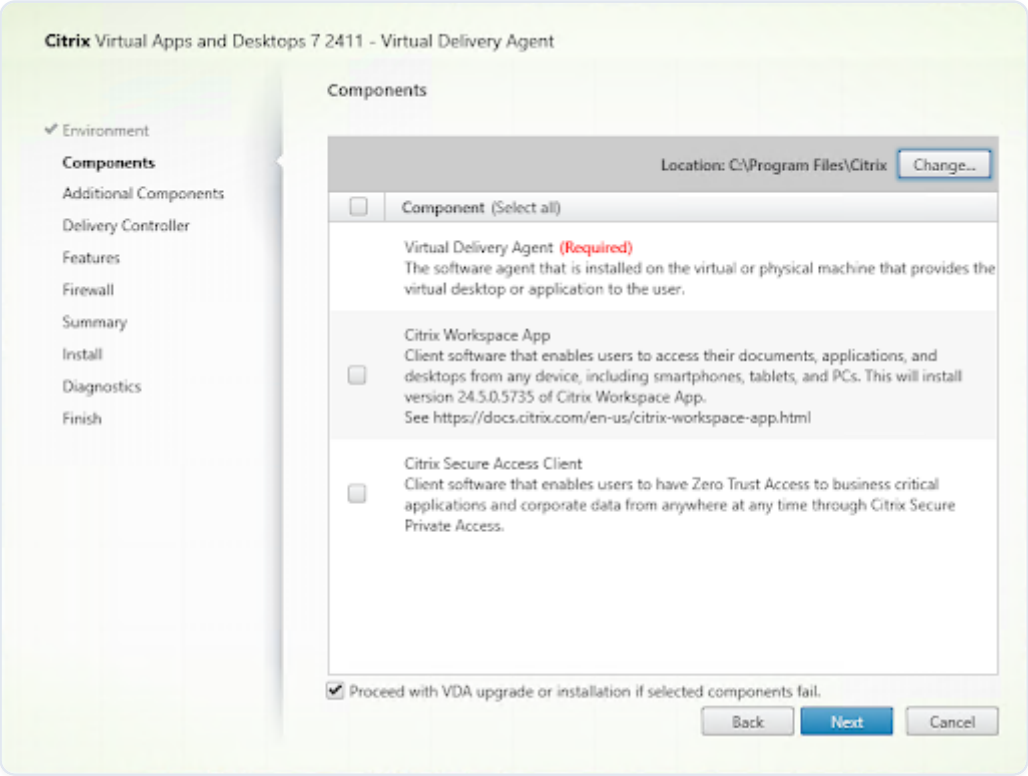
  コマンドラインオプション: `/remotepc`

Nextをクリックします。

このページは表示されません。

- VDA をアップグレードする場合
- `VDAWorkstationCoreSetup_2308.exe`、`VDAServerSetup_2308.exe`、または `VDAWorkstationSetup_2308.exe` インストーラーを使用している場合

手順 5. インストールするコンポーネントとインストール場所を選択する



コンポーネントページで、次の操作を行います。

- **場所:** デフォルトでは、コンポーネントは `C:\Program Files\Citrix` にインストールされます。ほとんどの展開では、このデフォルトで問題ありません。別の場所を指定する場合、その場所にはネットワークサービスに対する `execute` 権限が必要です。
- **コンポーネント:** デフォルトでは、Citrix Workspace App for Windows は VDA と一緒にインストールされません。`VDAWorkstationCoreSetup.exe` インストーラーを使用している場合、Citrix Workspace App for Windows はインストールされないため、このチェックボックスは表示されません。

Nextをクリックします。

コマンドラインオプション: `/installdir`、`/components vda,plugin` (VDA と Citrix Workspace App for Windows をインストールする場合)

> **注：**
>
> 以下のシナリオでは、VDA のインストール、アップグレード、またはアンインストール中に、Citrix Workspace™ app および Citrix Secure Access™ Client をインストール、アップグレード、またはアンインストールすることを選択できます。

- VDAインストール中に、Citrix Workspace AppとCitrix Secure Access Clientをインストールすることを選択できます。デフォルトでは、VDAインストール中にCitrix Workspace appとCitrix Secure Access Clientはインストールされません。
- VDAのアップグレード中に、Citrix Workspace appとCitrix Secure Access ClientがVDAにまだインストールされていない場合、それらをインストールすることを選択できます。
- VDAのアップグレード中に、Citrix Workspace appとCitrix Secure Access Clientのバージョンをアップグレードできる場合、それらをアップグレードするオプションが表示されます。
- VDAのアンインストール中に、Citrix Workspace appをアンインストールしないことを選択できます。デフォルトでは、VDAのアンインストール中にCitrix Workspace appとCitrix Secure Access Clientはアンインストールされます。

ステップ6. 追加コンポーネントをインストールします

VDAインストーラーの追加コンポーネントページ(/en-us/citrix-virtual-apps-desktops/2411/media/vda-ss-addtnl-components.png)

「**追加コンポーネント**」ページには、VDAとともに他の機能やテクノロジーのインストールを有効または無効にするためのチェックボックスが含まれています。コマンドラインインストールでは、`/exclude`または`/includeadditional`オプションを使用して、利用可能なコンポーネントを明示的に除外または含めることができます。

- **/includeadditional** "*コンポーネント*"\[,"*コンポーネント*"\] ...
- **/除外** "*コンポーネント*"\[,"*コンポーネント*"\] ...

次の表は、このページの項目のデフォルト設定を示しています。デフォルト設定は、「**環境**」ページで選択したオプションによって異なります。

追加コンポーネントページ	環境ページ：「MCSを使用したマスターイメージ」または「CITRIX PROVISIONINGを使用したマスターイメージ」が選択されている場合	環境ページ：「サーバーへの仲介接続を有効にする」（マルチセッションOSの場合）または「リモートPCアクセス」（シングルセッションOSの場合）が選択されている場合
Citrix App-V向けパーソナライゼーション - VDA	選択されていません	選択されていません

追加コンポーネントページ	環境ページ：「MCSを使用したマスターイメージ」または「CITRIX PROVISIONINGを使用したマスターイメージ」が選択されている場合	環境ページ：「サーバーへの仲介接続を有効にする」（マルチセッションOSの場合）または「リモートPCアクセス」（シングルセッションOSの場合）が選択されている場合
ユーザーパーソナライゼーションレイヤー	選択されていません	このユースケースでは無効なため表示されません。
Citrix プロファイル管理	選択済み	選択されていません
Citrix Profile Management WMI プラグイン	選択済み	選択されていません
Citrix VDA アップグレードエージェント	選択されていません	選択されていません
Citrix バックアップと復元	選択されていません	未選択
Citrix MCS IOドライバー	未選択	未選択
Citrix ランデブー V2	未選択	未選択

このページは、次の場合には表示されません。

- `VDAWorkstationCoreSetup.exe` インストーラーを使用している場合。また、追加コンポーネントのコマンドラインオプションは、そのインストーラーでは無効です。
- VDAをアップグレードしており、すべての追加コンポーネントがすでにインストールされている場合。一部の追加コンポーネントがすでにインストールされている場合は、インストールされていないコンポーネントのみがページに表示されます。

次のチェックボックスをオンまたはオフにします。(コンポーネントはインストーラーで異なる順序で表示される場合があります。)

- **Citrix Personalization for App-V:** Microsoft App-V パッケージのアプリケーションを使用する場合は、このコンポーネントをインストールします。詳細については、「App-V アプリケーションの展開と配信」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Personalization for App-V – VDA"`、コンポーネントのインストールを防止するには `/exclude "Citrix Personalization for App-V – VDA"`。

- **Citrix User Personalization Layer:** ユーザーパーソナライゼーションレイヤー用のMSIをインストールします。詳細については、「ユーザーパーソナライゼーションレイヤー」を参照してください。

  このコンポーネントは、シングルセッションのWindows 10マシンにVDAをインストールする場合にのみ表示されます。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "User Personalization Layer"`、コンポーネントのインストールを防止するには `/exclude "User Personalization Layer"`。

- **Citrix Profile Management:** このコンポーネントは、ユーザープロファイル内のユーザーパーソナライゼーション設定を管理します。詳細については、「Profile Management」を参照してください。

  Citrix Profile Managementをインストールから除外すると、Citrix DirectorでのVDAの監視とトラブルシューティングに影響します。**ユーザーの詳細**ページと**エンドポイント**ページでは、**パーソナライズ**パネルと**ログオン期間**パネルが機能しません。**ダッシュボード**ページと**傾向**ページでは、**平均ログオン期間**パネルはProfile Managementがインストールされているマシンのみのデータを表示します。

  サードパーティ製のユーザープロファイル管理ソリューションを使用している場合でも、Citrix Profile Management Serviceをインストールして実行することをお勧めします。Citrix Profile Management Serviceを有効にする必要はありません。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Profile Management"`、コンポーネントのインストールを防止するには `/exclude "Citrix Profile Management"`。

- **Citrix Profile Management WMIプラグイン:** このプラグインは、WMI（Windows Management Instrumentation）オブジェクト（プロファイルプロバイダー、プロファイルタイプ、サイズ、ディスク使用量など）でProfile Managementのランタイム情報を提供します。WMIオブジェクトは、Directorにセッション情報を提供します。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Profile Management WMI Plug-in"`、コンポーネントのインストールを防止するには `/exclude "Citrix Profile Management WMI Plug-in"`。

- **VDAアップグレードエージェント:** Citrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）の展開にのみ適用されます。VDAがVDAアップグレード機能に参加できるようにします。この機能を使用して、管理コンソールからカタログのVDAを即座に、またはスケジュールされた時

間にアップグレードできます。このエージェントがインストールされていない場合、マシン上でVDAインストーラーを実行することでVDAをアップグレードできます。

コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix VDA Upgrade Agent"`、コンポーネントのインストールを防止するには `/exclude "Citrix VDA Upgrade Agent"`。

- **ストレージ最適化のためのMCSIOライトキャッシュ:** Citrix MCS I/Oドライバーをインストールします。詳細については、「ハイパーバイザーによって共有されるストレージ」および「一時データ用のキャッシュの構成」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix MCS IODriver"`、コンポーネントのインストールを防止するには `/exclude "Citrix MCS IODriver"`。

- **プロキシ構成:** 環境でRendezvousプロトコルをGateway Service、VDA Upgrade Serviceなどで使用する予定があり、ネットワークにアウトバウンド接続用の非透過型プロキシがある場合は、ここでプロキシを指定します。HTTPプロキシのみがサポートされます。

  このコンポーネントをインストールする場合は、**Rendezvousプロキシ構成**ページでプロキシのアドレスまたはPACファイルのパスを指定します。機能の詳細については、「Rendezvousプロトコル」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Rendezvous V2"`、コンポーネントのインストールを防止するには `/exclude "Citrix Rendezvous V2"`。

- **Citrix Backup and Restore:** VDAのインストールまたはアップグレードが失敗した場合、このコンポーネントは、インストールまたはアップグレード前に実行されたバックアップにマシンを戻すことができます。

  「インストール準備」に記載されているように、Microsoft の前提条件が満たされていることを確認してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Backup and Restore"`、コンポーネントのインストールを防止するには `/exclude "Citrix Backup and Restore"`。

> **注:**

> MCS ストレージ最適化が有効になっている場合、Windows サーバーまたはデスクトップオペレーティングシステムのバックアップまたは復元が失敗する可能性があります。これを解決するには、メタインストーラーで MCS ストレージ最適化オプションを無効にしてください。

ステップ 7. Delivery Controller™ のアドレス

VDA インストーラーの Delivery Controller ページ (/en-us/citrix-virtual-apps-desktops/2411/media/vda-ss-delivery-controller.png)

Delivery Controller ページで、インストールされている Controller のアドレスを入力する方法を選択します。Citrix では、VDA のインストール中にアドレスを指定することをお勧めします (**手動で実行**)。VDA はこの情報がないと Controller に登録できません。VDA が登録できない場合、ユーザーはその VDA 上のアプリケーションやデスクトップにアクセスできません。

- **手動で実行:** (デフォルト) インストールされている Controller の FQDN を入力し、**追加** をクリックします。複数の Controller をインストールしている場合は、それらのアドレスを追加します。
- **後で実行 (詳細設定):** このオプションを選択すると、ウィザードは続行する前にその操作を実行するかどうかを確認します。アドレスを後で指定するには、インストーラーを再実行するか、Citrix グループポリシーを使用します。ウィザードは **概要** ページでも通知します。
- **Active Directory から場所を選択:** マシンがドメインに参加しており、ユーザーがドメインユーザーである場合にのみ有効です。
- **WebSocket トークンを使用 (テクニカルプレビュー):** WebSocket VDA を作成します。WebSocketToken は、必要なトークン用です。
- **Machine Creation Services に自動的に実行させる:** MCS を使用してマシンをプロビジョニングする場合にのみ有効です。

次へ をクリックします。**後で実行 (詳細設定)** を選択した場合、Controller アドレスを後で指定することを確認するよう求められます。

その他の考慮事項:

- アドレスには英数字以外の文字を含めることはできません。
- VDAインストール時とグループポリシーでアドレスを指定した場合、ポリシー設定がインストール時に指定された設定を上書きします。

- VDAの登録を成功させるには、Controllerとの通信に使用されるファイアウォールポートが開いている必要があります。このアクションは、ウィザードの**ファイアウォール**ページでデフォルトで有効になっています。
- Controllerの場所を指定した後（VDAインストール中またはインストール後）、Controllerが追加または削除されたときにVDAを更新するために自動更新機能を使用できます。VDAがControllerを検出して登録する方法の詳細については、VDA登録を参照してください。

コマンドラインオプション: `/controllers`

ステップ8. プロキシ構成

VDAインストーラーのランデブープロキシ構成ページ(/en-us/citrix-virtual-apps-desktops/2411/media/vda-rendezvous-proxy-config.png)

プロキシ構成ページは、**追加コンポーネント**ページで**プロキシ構成**チェックボックスを有効にした場合にのみ表示されます。

1. プロキシソースをプロキシアドレスで指定するか、PACファイルパスで指定するかを選択します。
2. プロキシアドレスまたはPACファイルパスを指定します。
   - プロキシアドレスの形式: `http://<url-or-ip>:<port>`
   - PACファイルの形式: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

接続テストを成功させるには、プロキシポートのファイアウォールが開いている必要があります。プロキシへの接続ができない場合でも、VDAのインストールを続行するかどうかを選択できます。

コマンドラインオプション: `/proxyconfig`

ステップ9. 機能の有効化または無効化

VDAインストーラーの機能ページ(/en-us/citrix-virtual-apps-desktops/2411/media/vda-ss-features.png)

「**機能**」ページで、使用する機能を有効または無効にするには、チェックボックスを使用します。

- **Windows リモートアシスタンスを使用する:** この機能を有効にすると、Director のユーザーシャドウ機能で Windows リモートアシスタンスが使用されます。Windows リモートアシスタンスは、ファイアウォールで動的ポートを開きます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_remote_assistance`

- **オーディオにリアルタイムオーディオトランスポートを使用する:** ネットワークで VoIP (Voice-over-IP) が広く使用されている場合は、この機能を有効にします。この機能により、遅延が減少し、損失の多いネットワークでのオーディオの回復性が向上します。これにより、RTP over UDP トランスポートを使用してオーディオデータを送信できます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_real_time_transport`

- **画面共有を使用する:** 有効にすると、画面共有で使用されるポートが Windows ファイアウォールで開かれます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_ss_ports`

- **この VDA はクラウド内の VM にインストールされていますか:** この設定は、Citrix がテレメトリ目的でオンプレミスおよびサービス (Citrix Cloud™) VDA 展開のリソースの場所を正しく識別するのに役立ちます。この機能は、顧客側の利用には影響しません。展開で Citrix DaaS を使用する場合は、この設定を有効にします。(デフォルト = 無効).

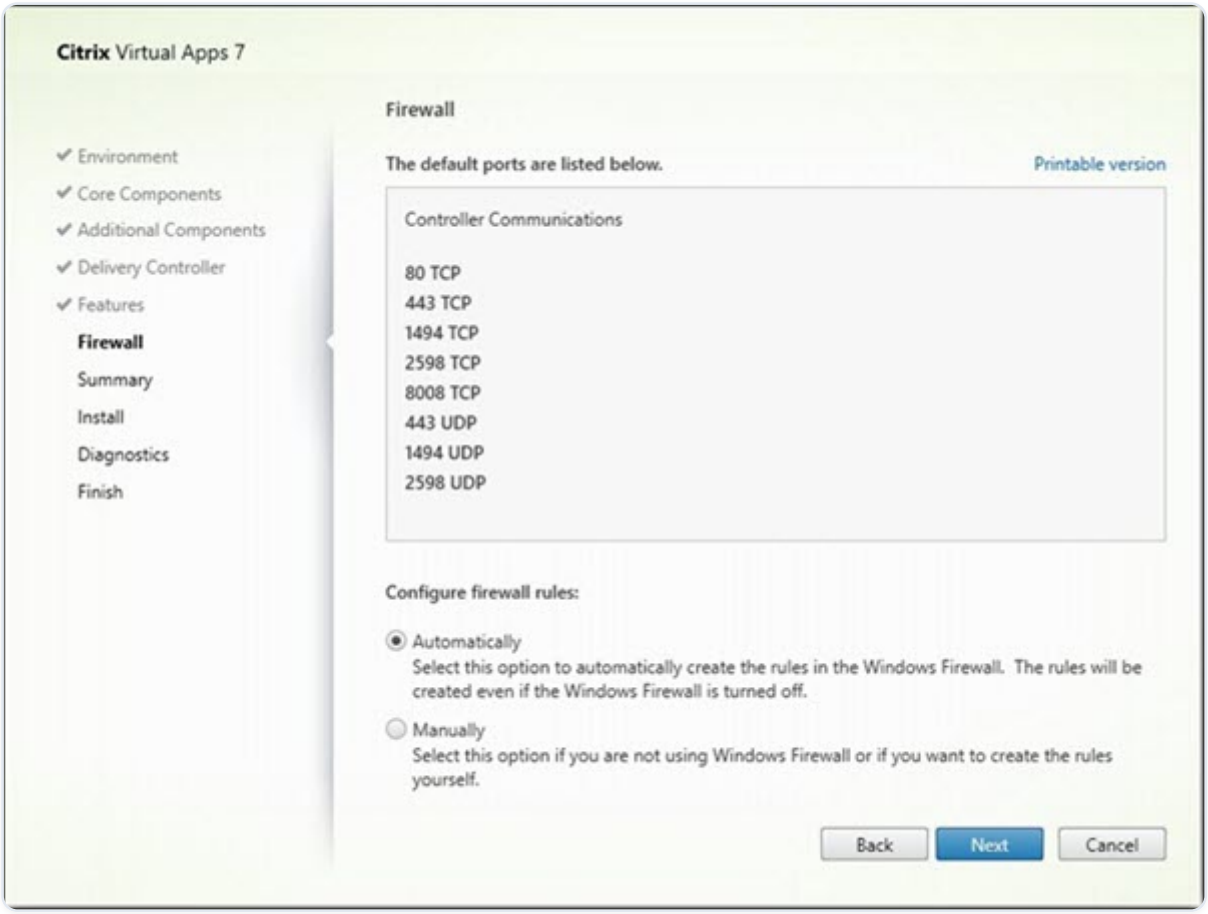
  コマンドラインオプション: `/xendesktopcloud`

- **セキュアなデフォルト設定:** このオプションは、よりセキュアな初期設定のために、さまざまな機能のデフォルト設定を有効から無効に変更します。関連する機能は次のとおりです: クライアントドライブリダイレクト、特殊フォルダーリダイレクト、ドラッグアンドドロップ、クライアント TWAIN デバイスリダイレクト、クライアント USB プラグアンドプレイデバイスリダイレクト、クライアントプリンターリダイレクト、クライアントクリップボードリダイレクト、およびクライアントマイクのリダイレクト。

コマンドラインオプション: `/ENABLE_SECURE_DEFAULTS`

次へをクリックします。

ステップ 10. ファイアウォールポート



「**ファイアウォール**」ページでは、Windows ファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても、ポートはデフォルトで自動的に開かれます。このデフォルト設定は、ほとんどの展開で問題ありません。ポート情報については、「ネットワークポート」を参照してください。

Nextをクリックします。

コマンドラインオプション: `/enable_hdx_ports`

手順 11. 前提条件を確認し、インストールを確定する

VDAインストーラーの概要ページ(/en-us/citrix-virtual-apps-desktops/2411/media/vda-ss-summary.png)

「**概要**」ページには、インストールされるものが表示されます。「**戻る**」ボタンを使用して、以前のウィザードページに戻り、選択を変更できます。

準備ができたら、「**インストール**」をクリックします。

前提条件がまだインストールまたは有効になっていない場合、マシンは1回以上再起動する可能性があります。「インストールの準備」を参照してください。

ステップ12. 診断

VDAインストーラーの診断ページ(/en-us/citrix-virtual-apps-desktops/2411/media/vda-ss-diagnostics.png)

「**診断**」ページで、Citrix Call Homeに参加するかどうかを選択します。参加することを選択した場合（デフォルト）、「**接続**」をクリックします。プロンプトが表示されたら、Citrixアカウントの資格情報を入力します。

資格情報が検証された後（または参加しないことを選択した場合）、「**次へ**」をクリックします。

フル製品インストーラーを使用している場合、「**診断**」ページで最初に「**診断情報の収集**」を選択せずに「**接続**」をクリックすると、「**Citrix Insight Servicesへの接続**」ダイアログを閉じた後、「**次へ**」ボタンが無効になります。次のページに進むことはできません。「**次へ**」ボタンを再度有効にするには、「**診断情報の収集**」を選択し、すぐに選択を解除します。

詳細については、「Call Home」を参照してください。

ステップ13. このインストールを完了する

VDAインストーラーのインストール完了ページ(/en-us/citrix-virtual-apps-desktops/2411/media/vda-ss-finish.png)

完了ページには、正常にインストールおよび初期化されたすべての前提条件とコンポーネントの緑色のチェックマークが表示されます。

「**完了**」をクリックします。デフォルトでは、マシンは自動的に再起動します。この自動再起動を無効にすることはできますが、マシンが再起動するまでVDAは使用できません。

次のステップ

必要に応じて、上記のプロシージャを繰り返して、他のマシンまたはイメージにVDAをインストールします。

すべてのVDAをインストールしたら、Studioを起動します。まだサイトを作成していない場合は、Studioが自動的にそのタスクに誘導します。それが完了すると、Studioはマシンカタログを作成し、次にデリバリーグループを作成するように誘導します。参照：

- サイトの作成
- マシンカタログの作成
- デリバリーグループの作成

シトリックス オプティマイザー

Citrix Optimizerは、Citrix管理者がさまざまなコンポーネントを削除および最適化することでVDAを最適化するのに役立つWindows OS用のツールです。

VDAをインストールし、最終的な再起動が完了したら、Citrix Optimizerをダウンロードしてインストールします。CTX224676を参照してください。CTX記事には、ダウンロードパッケージと、Citrix Optimizerのインストールおよび使用方法に関する手順が含まれています。

VDAのカスタマイズ

インストール済みのVDAをカスタマイズするには：

1. プログラムの削除または変更のためのWindows機能から、「**Citrix Virtual Delivery Agent**」または「**Citrix Remote PC Access/VDI Core Services VDA**」を選択します。次に右クリックして「**変更**」を選択します。
2. 「**Virtual Delivery Agent設定のカスタマイズ**」を選択します。インストーラーが起動したら、以下を変更できます。

    - コントローラーアドレス
    - コントローラーに登録するためのTCP/IPポート (デフォルト = 80)
    - Windowsファイアウォールポートを自動的に開くかどうか

トラブルシューティング

- コンポーネントインストールの結果をCitrixが報告する方法については、「Citrixインストールリターンコード」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/install-prepare.html#citrix-installation-return-codes)を参照してください。
- デリバリーグループのStudio表示で、**詳細**ペインの**インストール済みVDAバージョン**エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンのWindowsのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされても、Delivery Controllerに登録されるまでは、ユーザーにアプリやデスクトップを配信できません。

    VDA登録方法と登録問題のトラブルシューティング方法については、「VDA登録」(/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/vda-registration.html)を参照してください。

既知の制限事項

Citrix Workspace app for Windowsバージョン1912以前を使用している場合、しばらくするとセッションが切断されます。この問題は、Citrix Workspace appの新しいLTSRおよびCRバージョンで

修正されています。 サポートされているリリースバージョンの詳細については、「Citrix Workspace app for Windows / Citrix Receiver for Windows Long Term Service Releases」を参照してください。

VDAインストールに関連するWindows Defenderアクセス制御の構成

お客様は、署名されていないバイナリの読み込みを禁止するために、Windows Defenderアクセス制御 (WDAC) 設定を構成します。VDAインストーラーを通じて配布される署名されていないバイナリは、VDAのインストールを制限するため、禁止されます。

Citrix® は現在、すべてのCitrix生成バイナリをCitrixコード署名証明書で署名しています。さらに、Citrixは、製品とともに配布されるサードパーティ製バイナリも、それらのサードパーティ製バイナリを信頼できるバイナリとして認証する証明書で署名しています。

重要:

署名されていないサードパーティ製バイナリを含む古いVDAから、署名されたバイナリを含む新しいVDAバージョンにアップグレードしても、アップグレードされたマシンに常に署名されたバイナリが配置されるとは限りません。 これは、OS内のメカニズムにより、システムのアップグレードで同じバージョンのバイナリが置き換えられないためです。 サードパーティ製バイナリは署名されていますが、サードパーティによって制御されるそのバージョンはCitrixによって更新できないため、これらのバイナリは更新されません。この制限を回避するには：

1. バイナリを許可リストに含めます。これにより、バイナリに署名する必要がなくなります。
2. 古いVDAをアンインストールし、新しいVDAをインストールします。これはVDAの新規インストールに似ており、署名されたバージョンがインストールされます。

ウィザードを使用して新しいベースポリシーを作成する

WDACを使用すると、信頼できるバイナリをシステムで実行できるように追加できます。WDACのインストール後、**Windows Defender Application Control Policy Wizard** が自動的に開きます。

バイナリを追加するには、新しいベースWDACポリシーを作成する必要があります。ベースポリシーを作成するためのCitrix推奨ガイドラインをこのセクションで説明します。

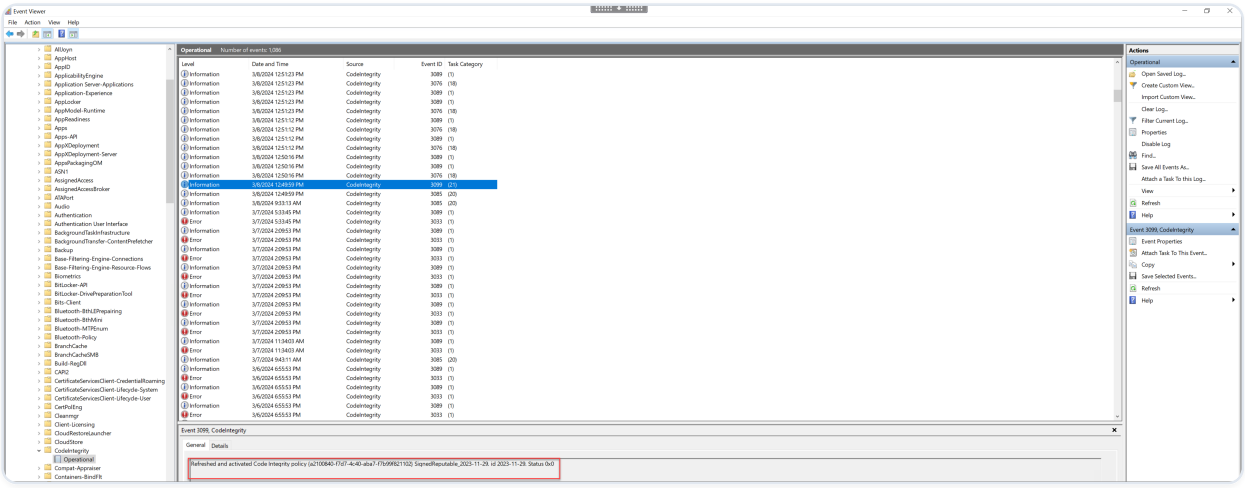
- Windowsオペレーティングコンポーネント、Microsoft Storeからインストールされたアプリ、すべてのMicrosoft署名済みソフトウェア、およびサードパーティのWindowsハードウェア互換ドライバーを承認するため、ベーステンプレートとして**署名済みおよび評判の良いモード**を選択します。
- 新しいWindows Defender Application Controlポリシーを適用する前にテストできるため、**監査モードを有効にする**を選択します。
- アプリケーションが識別され信頼されるレベルを指定し、参照ファイルを提供するために、**ファイルルール**に**カスタムルール**を追加します。ルールタイプとして「発行元」を選択すると、Citrix証明書のいずれかで署名された参照ファイルを選択できます。
- ルールを追加したら、`.XML` および `.CIP` ファイルが保存されているフォルダーに移動します。`.XML` ファイルには、ポリシーで定義されているすべてのルールが含まれています。任意のルールを変更、追加、または削除するように構成できます。
- WDACポリシーを展開する前に、`.XML` ファイルをバイナリ形式に変換する必要があります。WDACファイルは、`.XML` ファイルを `.CIP` ファイルに変換します。
- `.CIP`ファイルをC:\WINDOWS\System32\CodeIntegrity\CiPolicies\Activeにコピーして貼り付け、マシンを再起動します。生成されたポリシーは監査モードで適用されます。
- ベースポリシーを作成するステップバイステップのプロセスについては、ウィザードを使用して新しいベースポリシーを作成するを参照してください。

このポリシーが適用されると、WDACは、指定された発行元/CA機関によって署名されたCitrixファイルについて警告を発しません。

同様に、サードパーティによって署名されたファイルに対して、発行元レベルのルールを作成できます。

適用されたポリシーを確認する

1. マシンが再起動された後、**イベントビューアー**を開き、**アプリケーションとサービスログ > Microsoft > Windows > CodeIntegrity > Operational**に移動します。
2. 適用されたポリシーがアクティブになっていることを確認します。



3. ポリシーに違反したログを探し、そのファイルのプロパティを確認します。まず、署名されていることを確認します。署名されていない場合で、このマシンがVDAアップグレードを経ている場合は、上記の制限事項で説明されているケースである可能性が高いです。署名されている場合は、このファイルは前述のとおり、代替証明書で署名されている可能性があります。

Citrix証明書で署名されたCitrix生成ファイルの例は`C:\Windows\System32\drivers\picadm.sys`です。 Citrixサードパーティ証明書で署名されたサードパーティバイナリの例は`C:\Program Files\Citrix\IcaConfigTool\Microsoft.Practices.Unity.dll`です。

スクリプトを使用してVDAをインストールする

> **注:**
>
> Citrixは、お客様の運用環境に合わせて調整されたスクリプトによって引き起こされる問題について責任を負いません。インストール関連のCitrixの問題については、Citrixサポートポータルを使用して、関連するインストールログとともにテクニカルサポートケースをオープンしてください。

> この記事は、Windowsオペレーティングシステムを搭載したマシンへのVDAのインストールに適用されます。Linuxオペレーティングシステム用VDAの詳細については、Linux Virtual Delivery Agentのドキュメントを参照してください。

インストールメディアには、Active Directory内のマシンにVirtual Delivery Agent (VDA) をインストール、アップグレード、または削除するサンプルスクリプトが含まれています。これらのスクリプトは、Machine Creation Services™およびCitrix Provisioning (旧Provisioning Services) で使用されるマスターイメージの保守にも使用できます。

必要なアクセス権:

- スクリプトは、VDAインストールコマンドが配置されているネットワーク共有への「Everyone読み取り」アクセス権を必要とします。インストールコマンドは、完全な製品ISOでは`XenDesktopVdaSetup.exe`、スタンドアロンインストーラーでは`VDAWorkstationSetup.exe`または`VDAServerSetup.exe`です。
- ログの詳細は各ローカルマシンに保存されます。レビューと分析のために結果を一元的にログに記録するには、スクリプトは適切なネットワーク共有への「Everyone読み取りおよび書き込み」アクセス権を必要とします。

スクリプトの実行結果を確認するには、中央ログ共有を調べます。キャプチャされたログには、スクリプトログ、インストーラーログ、MSIインストールログが含まれます。各インストールまたは削除の試行は、タイムスタンプ付きのフォルダーに記録されます。フォルダーのタイトルは、PASSまたはFAILのプレフィックスで操作結果を示します。標準のディレクトリ検索ツールを使用して、中央ログ共有で失敗したインストールまたは削除を見つけることができます。これらのツールは、ターゲットマシンでローカルに検索する代替手段を提供します。

インストールを開始する前に、インストールの準備のタスクを読み、完了してください。

スクリプトを使用してVDAをインストールまたはアップグレードする

1. インストールメディアの\\Support\\AdDeploy\\からサンプルスクリプト**InstallVDA.bat**を入手します。Citrixは、スクリプトをカスタマイズする前に元のスクリプトのバックアップを作成することをお勧めします。
2. スクリプトを編集します。
    - インストールするVDAのバージョンを指定します: `SET DESIREDVERSION`。完全な値は、インストールメディアのProductVersion.txtファイルに記載されています。ただし、完全な一致は必須ではありません。
    - インストーラーが呼び出されるネットワーク共有を指定します。レイアウトのルート（ツリーの最上位）を指します。スクリプトの実行時に、インストーラーの適切なバージョン（32ビットまたは64ビット）が自動的に呼び出されます。例: `SET DEPLOYSHARE=\\fileserver1\share1`。
    - 集中ログを保存するためのネットワーク共有場所をオプションで指定します。例: `SET LOGSHARE=\\fileserver1\log1)`。
    - コマンドラインを使用したインストールで説明されているVDA構成オプションを指定します。`/quiet`と`/noreboot`オプションは、スクリプトにデフォルトで含まれており、必須です: `SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT /NORESUME`。

3. グループポリシー起動スクリプトを使用して、スクリプトをマシンを含むOUに割り当てます。このOUには、VDAをインストールするマシンのみを含める必要があります。そのOU内のマシンが再起動されると、スクリプトはすべてのマシンで実行されます。サポートされているオペレーティングシステムを持つ各マシンにVDAがインストールされます。

スクリプトを使用してVDAを削除する

1. インストールメディアの\\Support\\AdDeploy\\からサンプルスクリプトUninstallVDA.batを入手します。Citrixは、元のスクリプトをカスタマイズする前にバックアップを作成することを推奨します。
2. スクリプトを編集します。
   - 削除するVDAのバージョンを指定します: `SET CHECK\_VDA\_VERSION`。完全な値は、インストールメディアのProductVersion.txtファイル（例: 7.0.0.3018）にあります。ただし、完全な一致は必要ありません。
   - 集中ログを保存するためのネットワーク共有場所をオプションで指定します。
3. グループポリシー起動スクリプトを使用して、スクリプトをマシンを含むOUに割り当てます。このOUには、VDAを削除するマシンのみを含める必要があります。OU内のマシンが再起動されると、スクリプトはすべてのマシンで実行されます。各マシンからVDAが削除されます。

トラブルシューティング

- スクリプトは、スクリプトの実行の進行状況を記述する内部ログファイルを生成します。スクリプトは、展開の開始から数秒以内に`Kickoff_VDA_Startup_Script`ログを中央ログ共有にコピーします。全体的なプロセスが機能していることを確認できます。このログが期待どおりに中央ログ共有にコピーされない場合は、ローカルマシンを検査してさらにトラブルシューティングを行ってください。スクリプトは、各マシンの`%temp%`フォルダーに2つのデバッグログファイルを配置します。
  - `Kickoff_VDA_Startup_Script_<DateTimeStamp>.log`
  - `VDA_Install_ProcessLog_<DateTimeStamp>.log`

  スクリプトが次の状態であることを確認するために、これらのログを確認します。
  - 期待どおりに実行されている。
  - ターゲットオペレーティングシステムを適切に検出している。
  - `DEPLOYSHARE`共有の`ROOT`を指すように正しく構成されている（`AutoSelect.exe`という名前のファイルが含まれている）。

  - `DEPLOYSHARE`と`LOG`の両方の共有に対して認証できる。

- Citrixがコンポーネントインストールの結果を報告する方法については、Citrixインストールリターンコードを参照してください。
- デリバリーグループのStudio表示では、**詳細**ペインの**インストール済みVDAバージョン**エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされた後、Delivery Controllerに登録されるまで、ユーザーにアプリやデスクトップを配信できません。

  VDA登録方法と登録の問題のトラブルシューティング方法については、「VDA登録」を参照してください。

サードパーティ製VDA展開方法

SCCM を使用して VDA をインストールする

概要

Microsoft Endpoint Configuration Manager (旧称 System Center Configuration Manager (SCCM)) は、企業全体のデバイスとアプリケーションの管理、展開、セキュリティを可能にする Windows 製品です。

> **注:**
>
> 以下の記事では、Citrix® が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、必要に応じてカスタマイズできます。Citrix は、顧客のニーズに合わせてこれに必要な更新や調整について責任を負いません。

推奨事項

- SCCM または同様のソフトウェア配布ツールを使用して Virtual Delivery Agent (VDA) を正常に展開するには、Citrix はVDA インストーラーを段階的に使用することを推奨します。
- Citrix は、VDA のインストールまたはアップグレードの一部として VDA Cleanup Utility を使用することを推奨しません。VDA Cleanup Utility は、VDA インストーラーが以前に失敗した場合という限られたケースでのみ使用してください。

開始する前に

VDA のインストール中に必要な再起動の回数は、環境によって異なります。例：

- 以前のソフトウェアインストールからの保留中の更新または再起動のために、再起動が必要になる場合があります。
- 他のプロセスによって以前にロックされたファイルは更新が必要になる場合があり、追加の再起動が強制されます。
- VDA インストーラー内の一部のオプションコンポーネント (Citrix Profile Management や Citrix Files など) は、再起動が必要になる場合があります。
- VDA をアップグレードする場合、それがインストールされているマシンは、セッションがない状態でメンテナンスモードである必要があります。
- マシンで VDA インストールが初めて実行されると、使用されている VDA インストーラーはそのマシンにコピーされます。 VDA のインストールに関する詳細については、インストーラーを参照してください。

SCCM タスクシーケンサーは、必要なすべての再起動を管理します。

SCCM を使用して VDA を展開するための主要な手順

以下の手順では、仮想マシン上で SCCM を使用して VDA を展開する方法について説明します。

1. VDA をインストールする。
2. 組織単位 (OU) を作成する。
3. マシンを検証する。
4. VDA を使用してコンテンツを配布する。

ステップ 1: VDA をインストールする

すべての前提条件を特定した後、「**SCCM タスクシーケンサー**」を使用して以下のタスクを完了します。

1. インストールメディアのアクセス可能なコピーから、またはVDAスタンドアロンインストーラーのいずれかからVDAをインストールします。

   - `VDAWorkstationSetup_XXXX.exe`
   - `VDAServerSetup_XXXX.exe`
   - `VDAWorkstationCoreSetup_XXXX.exe`

   VDA インストーラーの詳細については、インストーラーを参照してください。

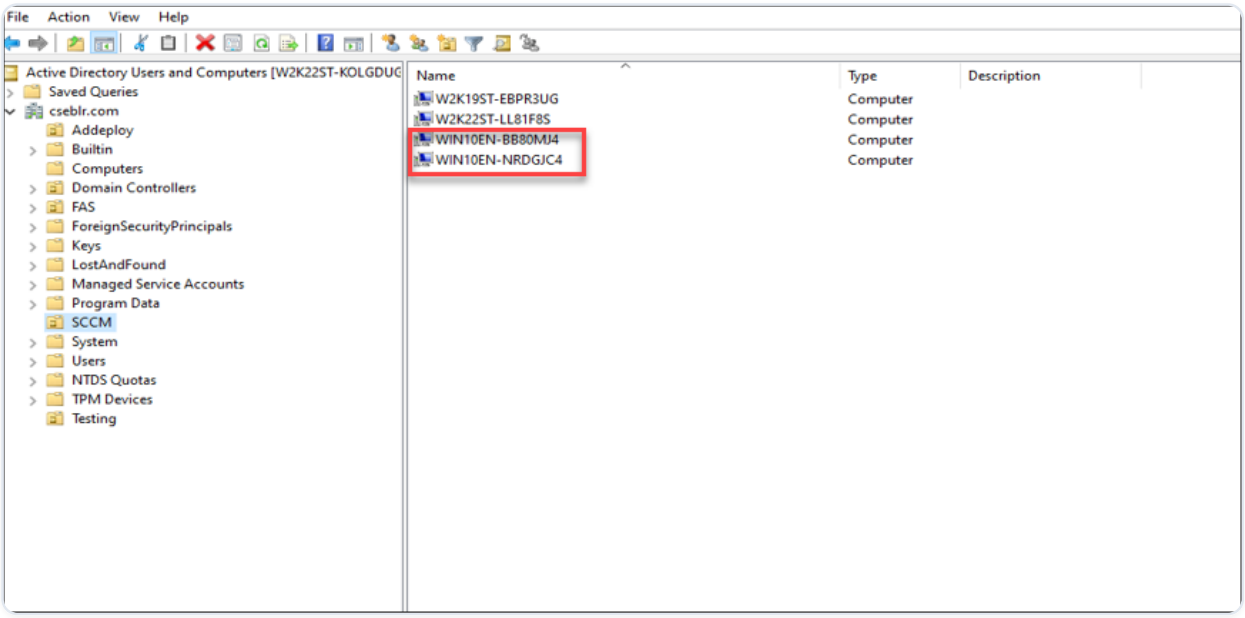
   > **注:**

> VDAをアップグレードする場合、VDAがインストールされているマシンは、セッションがないメンテナンスモードである必要があります。

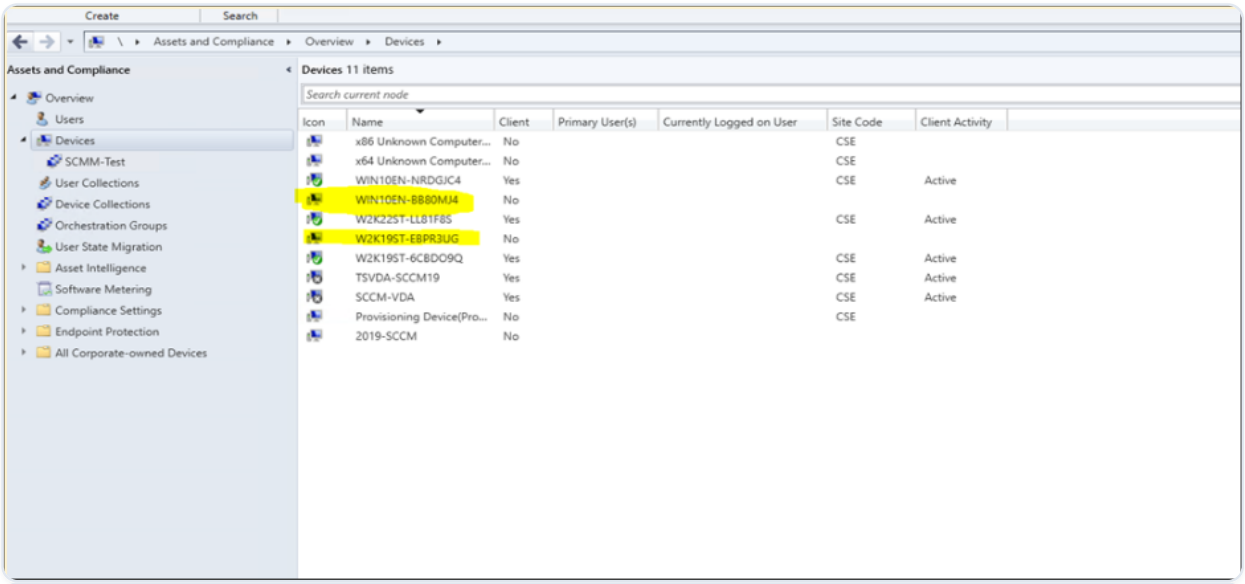
2. マシンでVDAのインストールが初めて実行されると、使用されているVDAインストーラーがそのマシンにコピーされます。
   - `VDAWorkstationCoreSetup_XXXX.exe` 以外のVDAインストーラーを使用すると、VDAインストーラーは `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe` にコピーされます。
   - `VDAWorkstationCoreSetup_XXXX.exe` を使用すると、VDAインストーラーは `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe.` にコピーされます。
3. VDAインストーラーのディレクトリの場所は、レジストリ `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall” “MetaInstallerInstallLocation”` にも保存されます。
4. コマンドラインオプションに `/NOREBOOT`、`/NORESUME`、および `/QUIET` を追加します。
   - `/QUIET`: インストール中にユーザーインターフェイスを表示しないようにします。これにより、SCCMがインストールプロセスを制御できます。
   - `/NOREBOOT`: VDAインストーラーが自動的に再起動するのを抑制します。SCCMは必要に応じて再起動をトリガーします。
   - `/NORESUME`: 通常、インストール中に再起動が必要な場合、VDAインストーラーはrunonceレジストリキー（`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`）を設定します。Windowsは、マシンが再起動したときにこのキーを使用してVDAインストーラーを開きます。SCCMはインストールを監視して終了コードをキャプチャできないため、これはSCCMにとって問題となります。

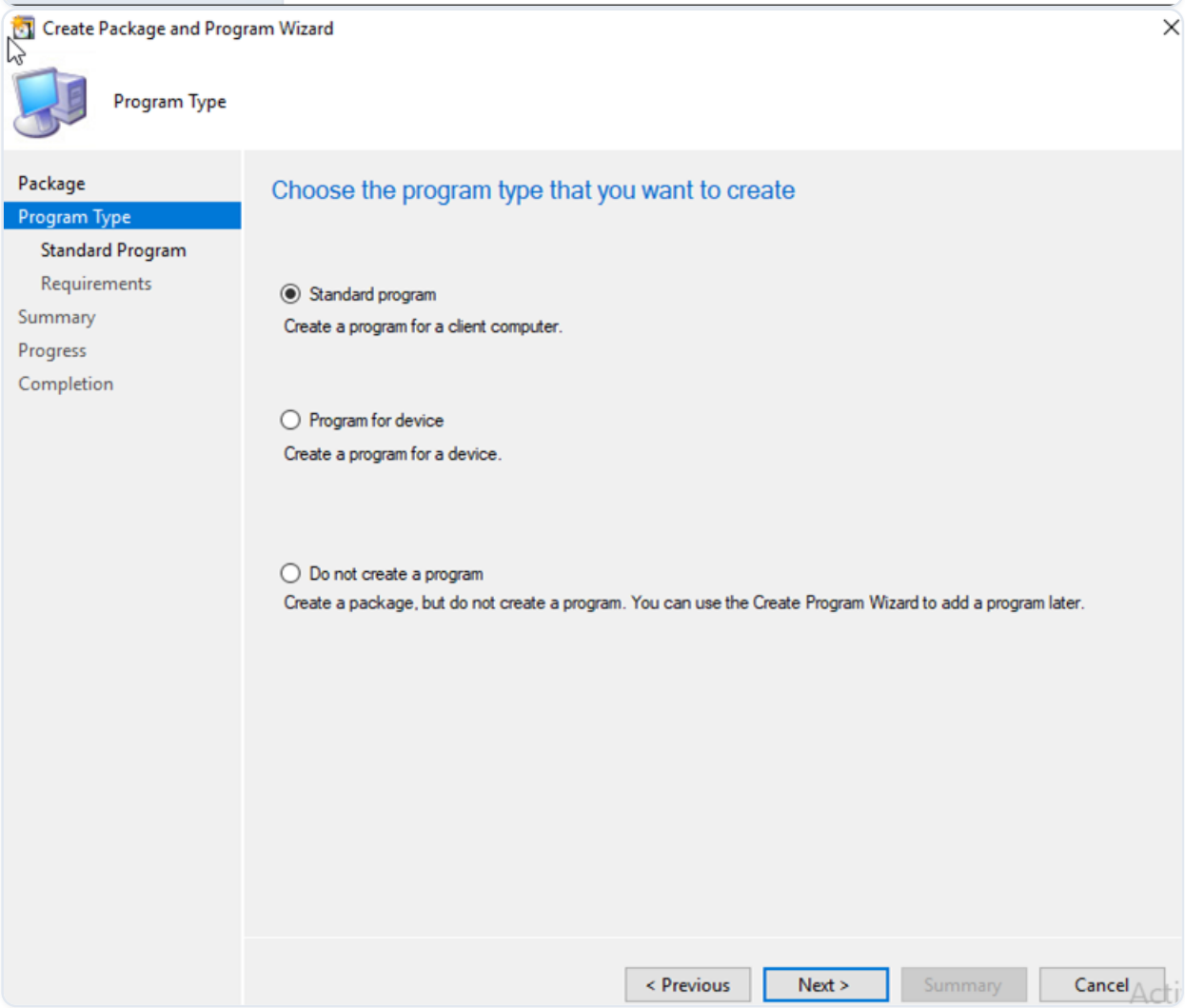
ステップ2: 組織単位 (OU) を作成する

1. OU に追加するドメイン参加済み仮想マシンを 2 台作成します。仮想マシンが最初に作成されると、**Computers** フォルダーにあります。仮想マシンを **SCCM** フォルダーに移動します。
   例: WIN10EN-BB80MJ4.cseblr.com W2K19ST-EBPR3UG.cseblr.com

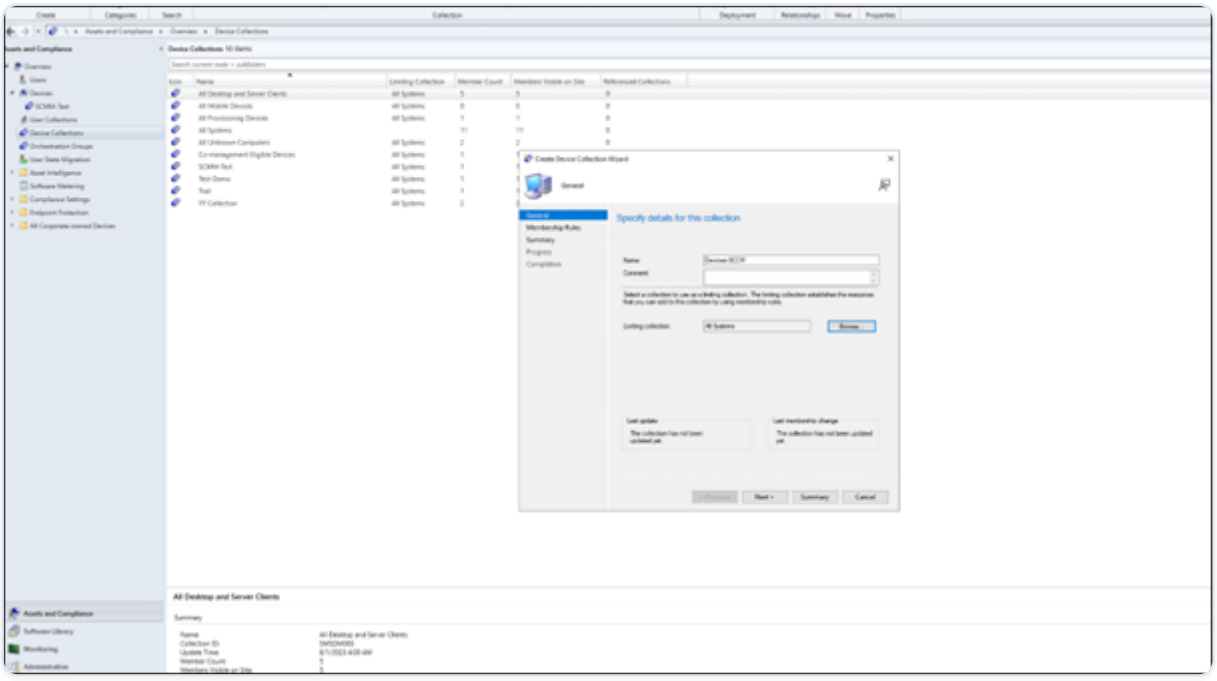


2. Microsoft Configuration Manager で、`\Administration\Overview\Hierarchy Configuration\Discovery Methods\` に移動します。
3. **Active Directory System Discovery**をクリックし、**Enable Active Directory System Discovery**チェックボックスをオンにして、新しく作成された仮想マシンの自動検出を有効にします。
4.  アイコンをクリックして、新しいコンテナーを選択します。
5. 「**場所**」セクションで、SCCM仮想マシンが配置されている**パス**を追加します。
6. `\Administration\Overview\Site Configuration\Sites` に移動し、SCCM VDA を右クリックします。
7. **クライアントインストール設定 > クライアントプッシュインストール**を選択します。「**クライアントプッシュインストールのプロパティ**」ウィンドウが開きます。
8. VM が `Enabled` に設定されると、次の図に示すように VM のリストが表示されます。





9. OU を作成するために**デバイスコレクション**を作成します。コレクション名の**名前**を入力します。



10. ウィザードの指示に従います。

    メンバーシップルール(/en-us/citrix-virtual-apps-desktops/2411/media/sccm-membership-rules.png)

    OU が作成されました。

    OUの作成(/en-us/citrix-virtual-apps-desktops/2411/media/sccm-create-device-collection-wizard.png)

11. 作成した VM を新しく作成したデバイスコレクションに追加します。

    a. VM を右クリックします。**選択したアイテムの追加 > 選択したアイテムを既存のデバイスコレクションに追加**を選択します。

       項目の追加(/en-us/citrix-virtual-apps-desktops/2411/media/sccm-add-item-to-device-collection.png)

    b. 「**コレクションの選択**」ウィンドウで、必要なデバイス名を選択します。この例では、`Devices-SCCM`です。

       デバイスリスト(/en-us/citrix-virtual-apps-desktops/2411/media/sccm-list.png)

    `Devices-SCCM`は、「**資産とコンプライアンス > 概要 > デバイスコレクション**」に表示されます。

    デバイスがリストされました(/en-us/citrix-virtual-apps-desktops/2411/media/devices-sccm.png)

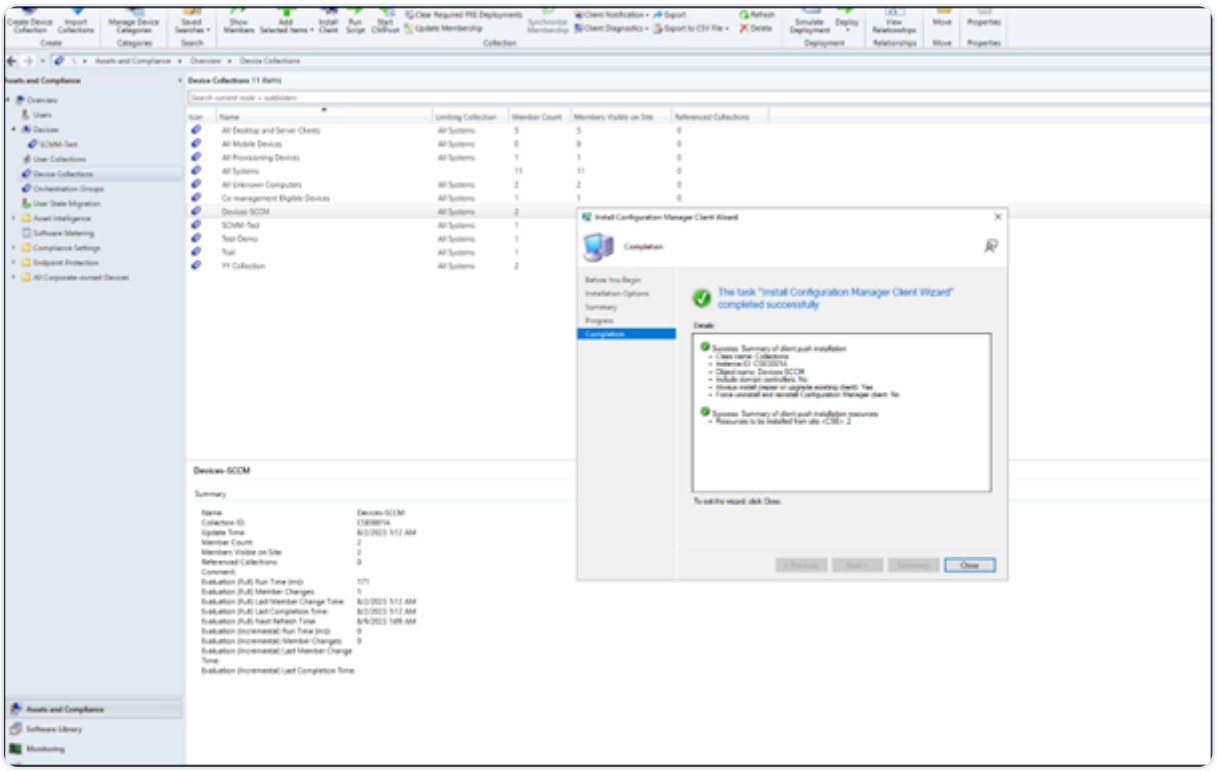
12. デバイスコレクターで「**クライアントのインストール**」を選択します。

クライアントのインストール(/en-us/citrix-virtual-apps-desktops/2411/media/sccm-install-client.png)

13. 必要なインストール「**サイト**」を選択します。

    サイトのインストール(/en-us/citrix-virtual-apps-desktops/2411/media/sccm-install-client-1.png)

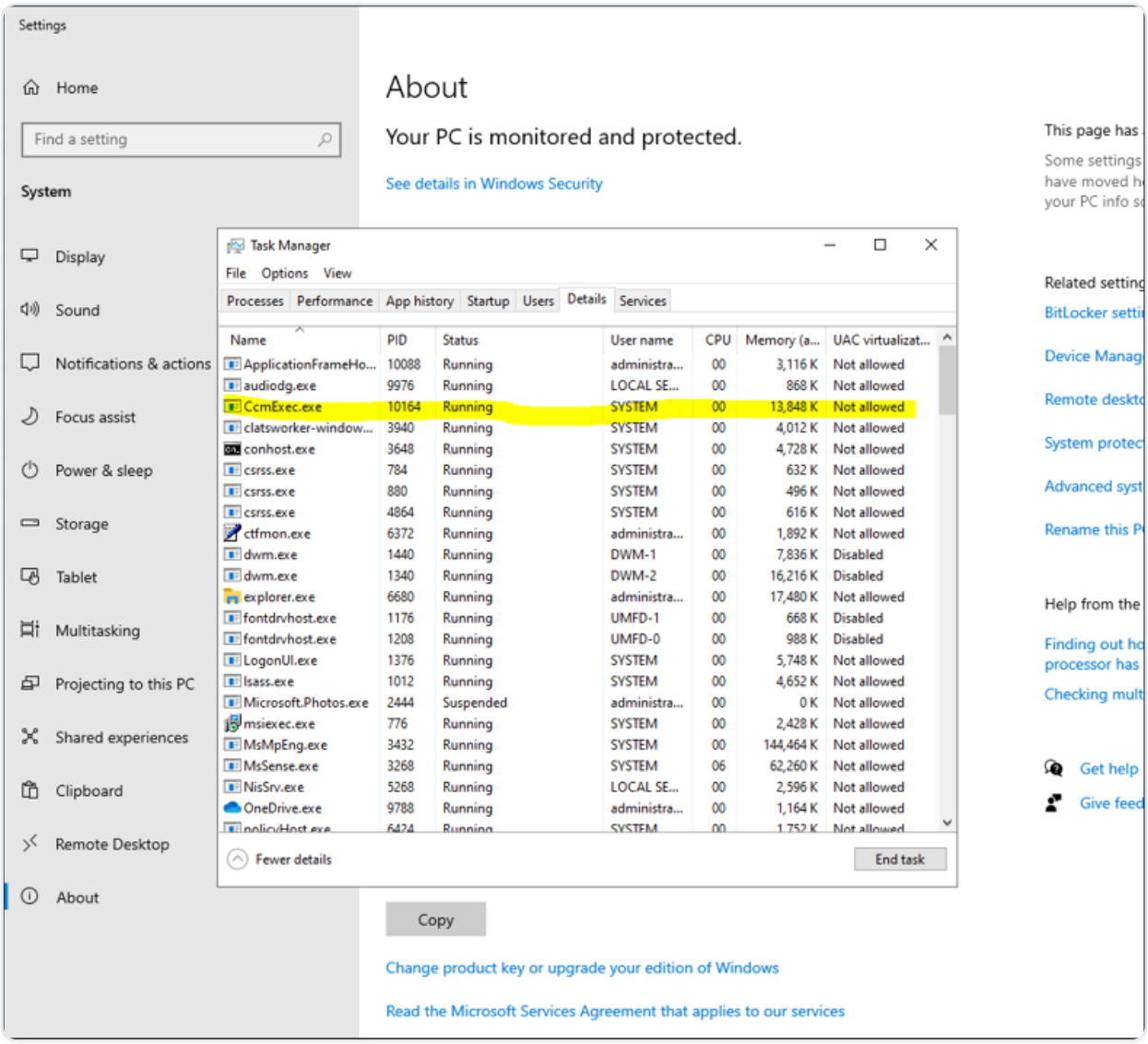
14. ウィザードの指示に従います。**Install Configuration Manager Client Wizard** が正常に完了しました。



詳細については、Microsoft ドキュメントの コレクションの管理 を参照してください。

ステップ 3: マシンの検証

1. クライアントマシンで、`CCMExec` プロセスが実行されていることを確認して、クライアントがインストールされていることを検証します。



2. SCCM 上の VM でクライアントが実行されていることを確認します。

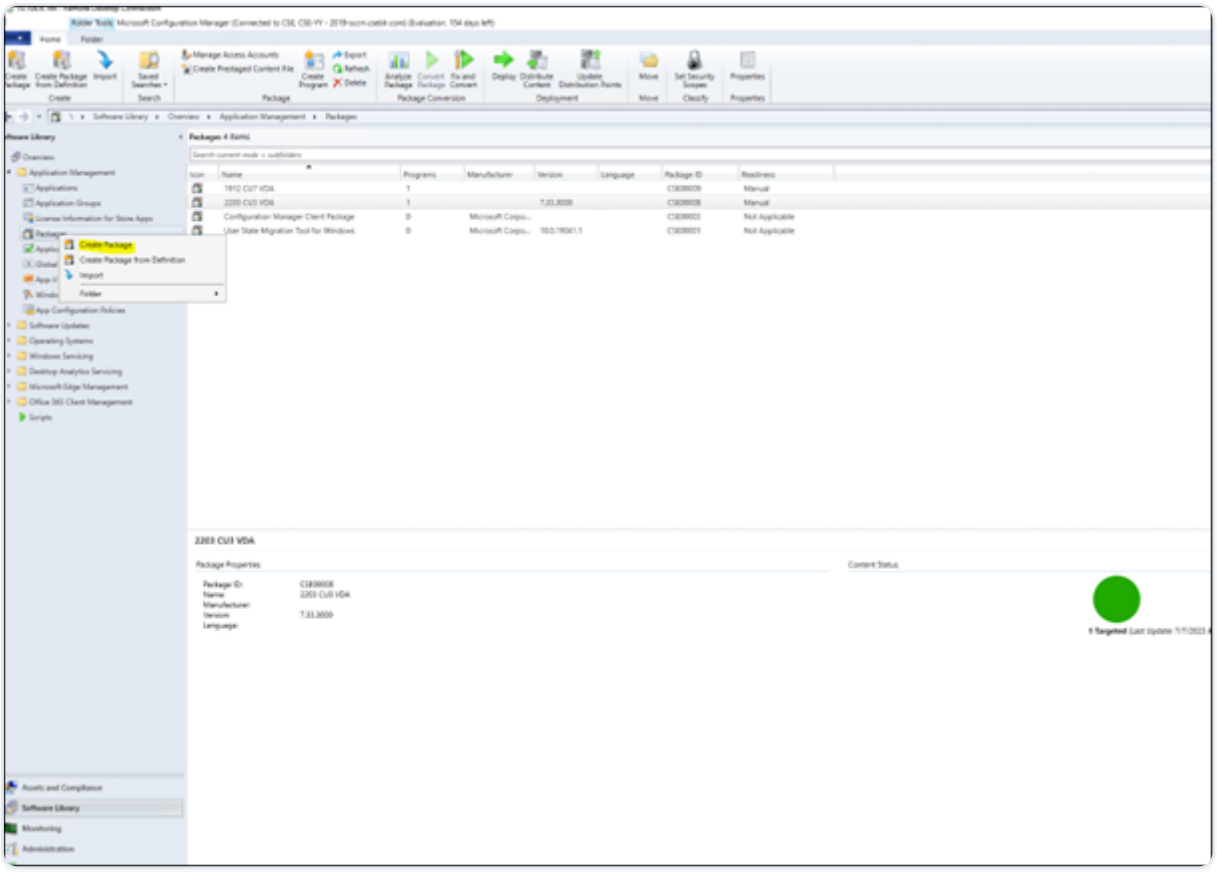
ステップ 4: VDA を使用してコンテンツを配布する

以下の手順では、展開されたVDAを使用して、関連する仮想マシンにコンテンツを配布する方法について説明します。

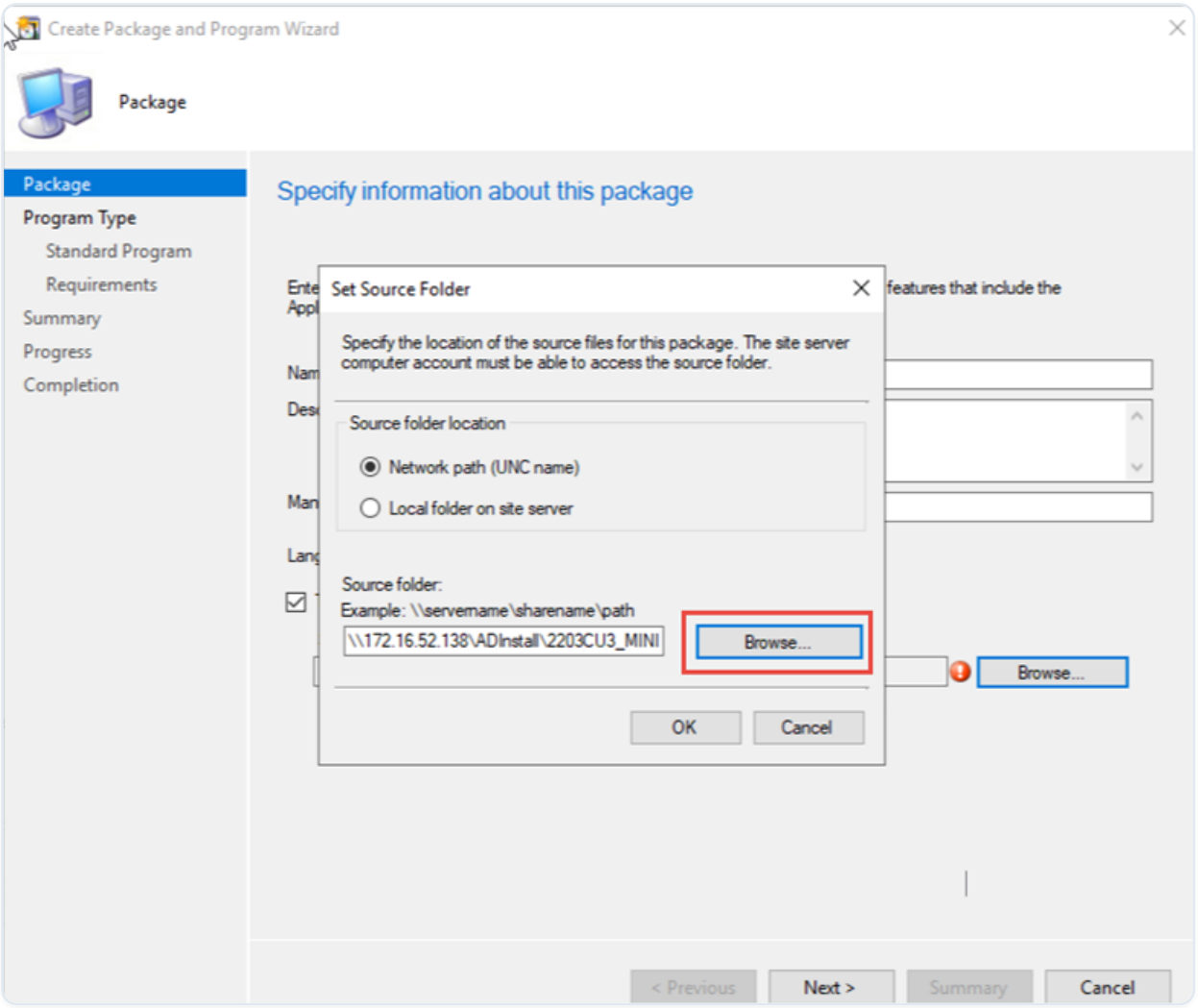
1. パッケージの作成
2. コンテンツの配布

パッケージの作成

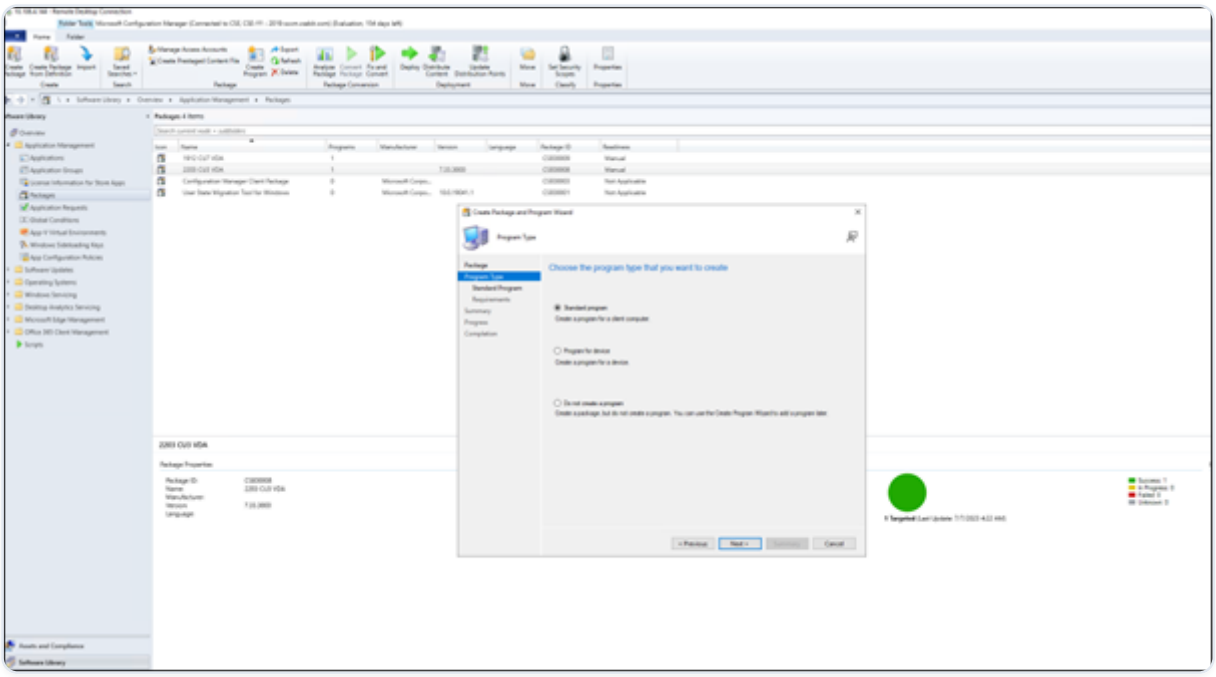
1. パッケージを作成するには、目的の VDA を右クリックし、 をクリックします。



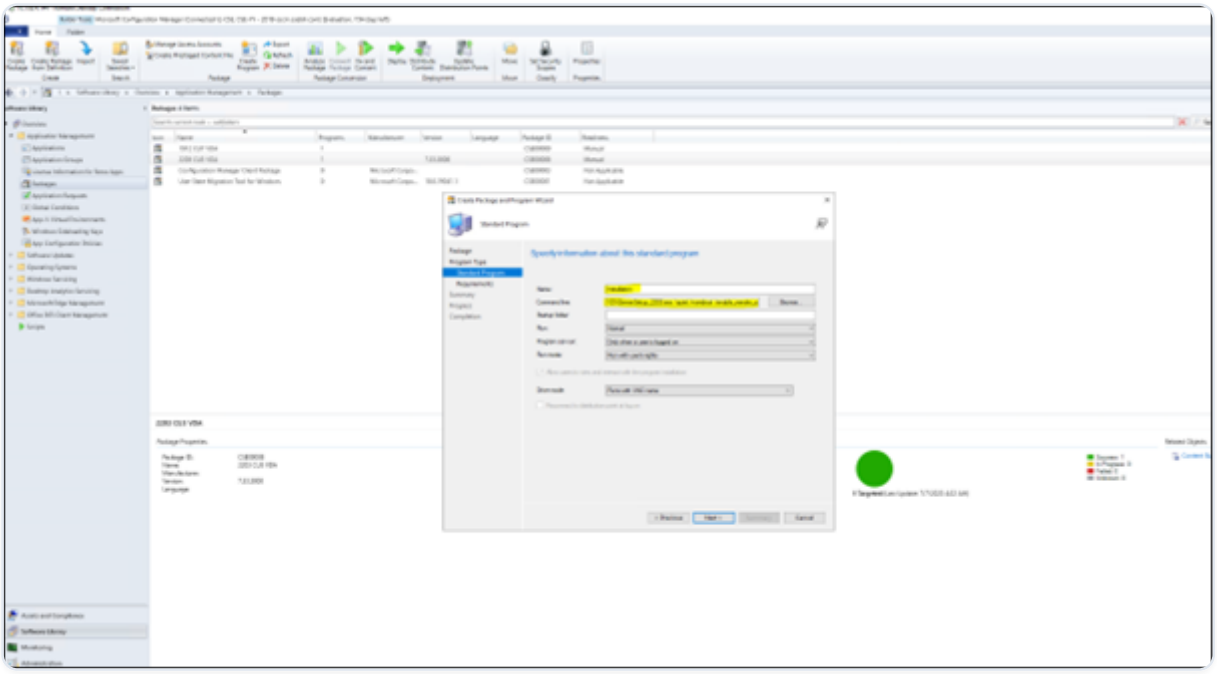
2. をクリックして、このパッケージのソースファイルの場所を指定します。



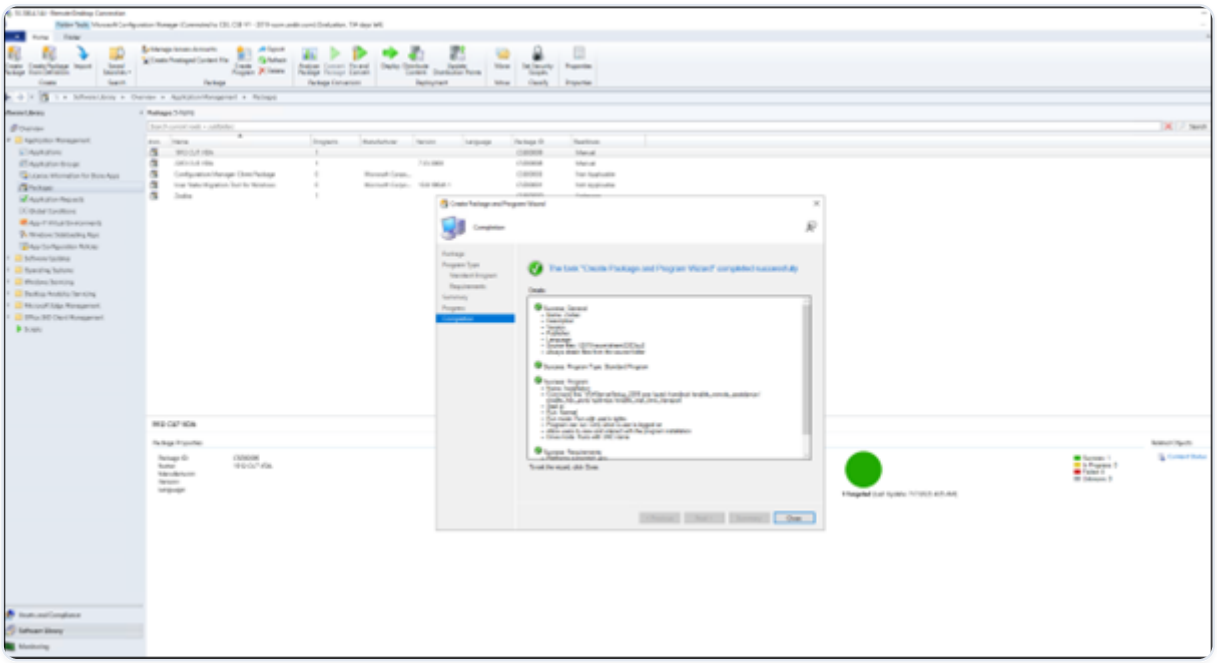
3. 必要なパッケージの種類を選択します。



4. パッケージの**名前**と**コマンドライン**を入力します。



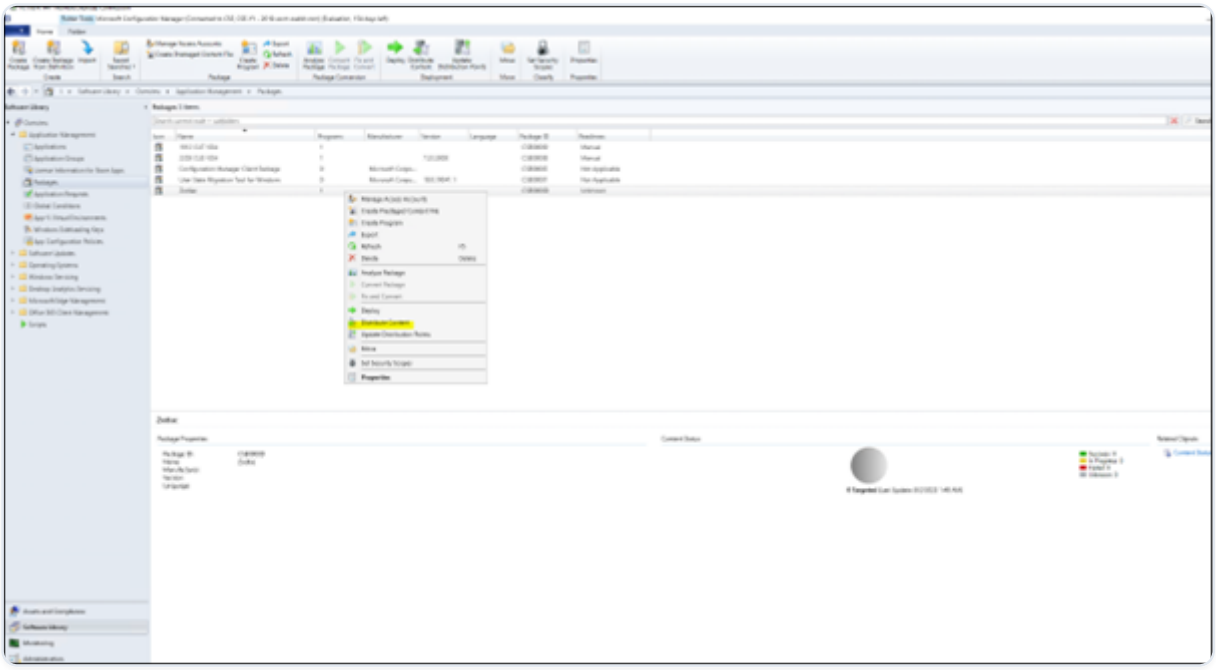
5. **Next**をクリックします。



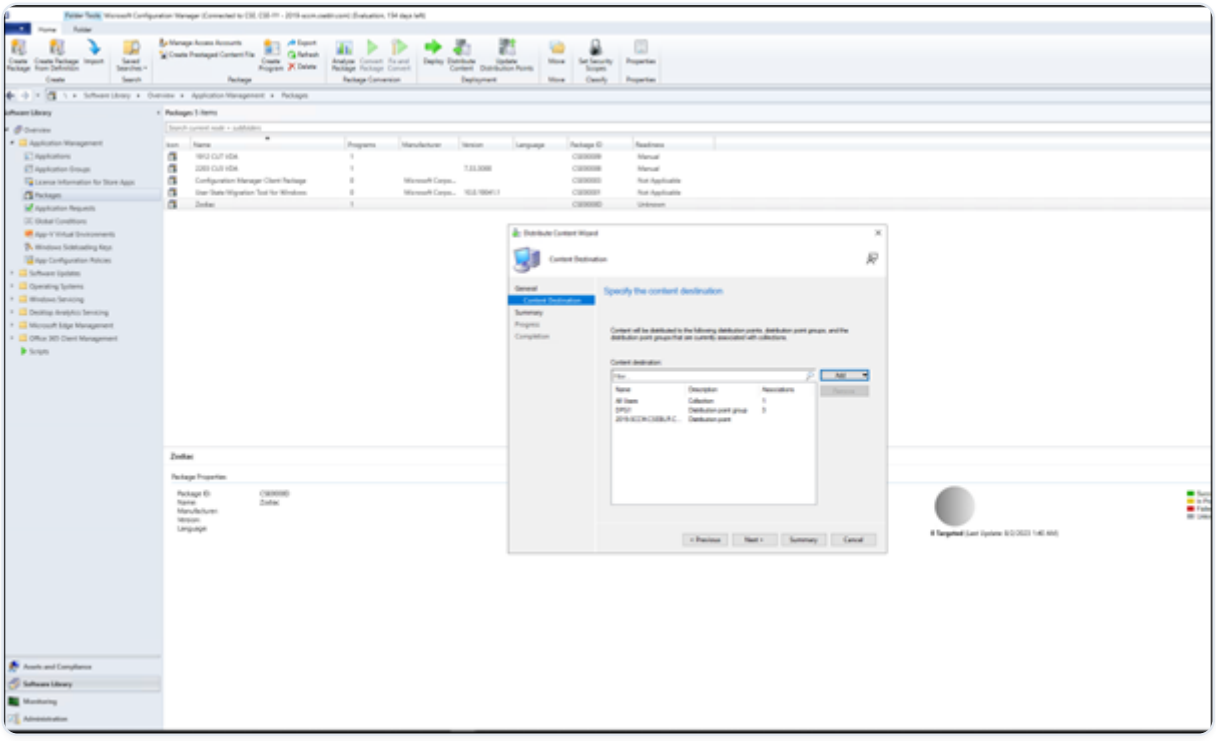
詳細については、Microsoft ドキュメントの「Configuration Manager のパッケージとプログラム」を参照してください。

コンテンツの配布

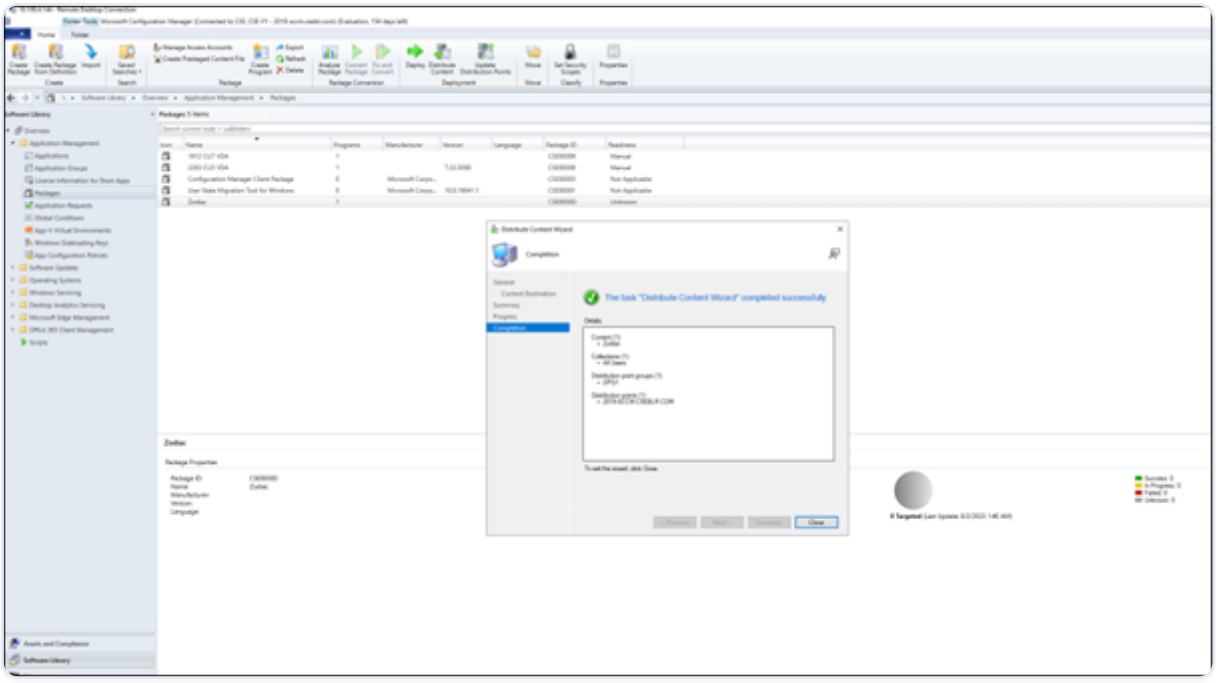
1. 作成したパッケージ名を右クリックします。
2. を選択します。



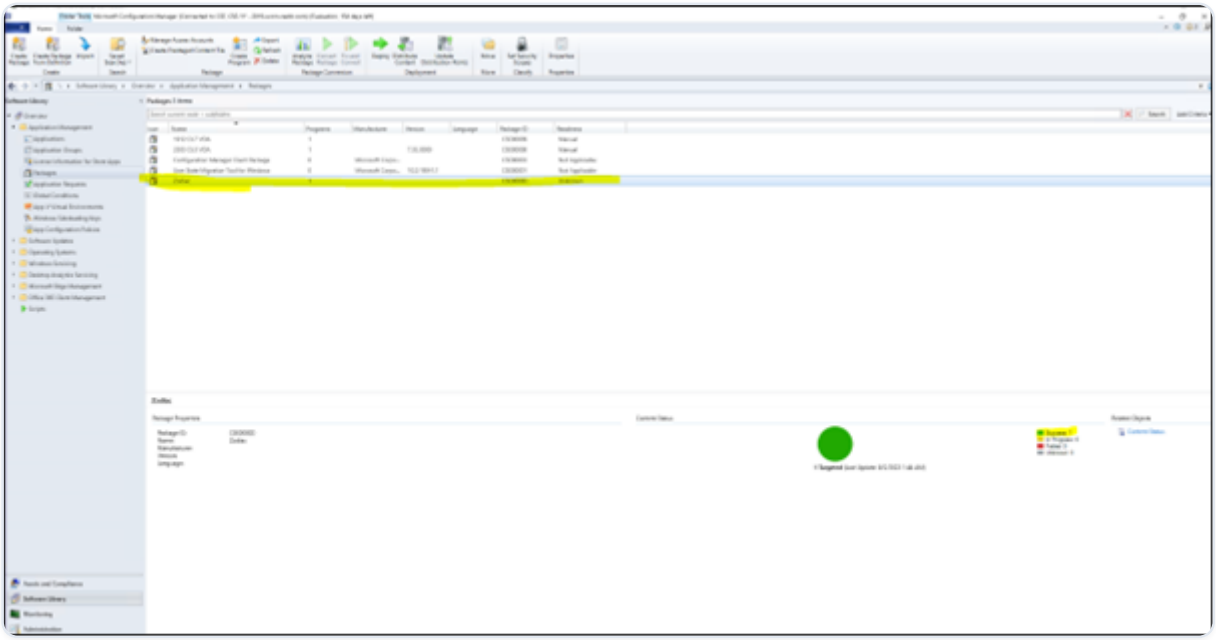
3. ウィンドウで、作成したパッケージのソースファイルの場所を選択します。この例では、`2019-SCCM` です。 をクリックします。



4. パッケージ (この例では `Zodiac`) が展開可能であることを確認します。



以下の画像は、パッケージが展開可能であることを示しています。



詳細については、Microsoft ドキュメントの「Configuration Manager のコンテンツの展開と管理」を参照してください。

SCCM を使用したインストールシーケンスの例

次の例は、インストールシーケンスを示しています。

1. **コンピューターの再起動:** マシンを再起動して準備します。

   「コンピューターの再起動」(/en-us/citrix-virtual-apps-desktops/2411/media/restart-computer.png)

2. **VDAのインストール（初回）:** VDAのインストールを開始します。

a. コマンドラインオプションに`/quiet`、`/noreboot`、および`/noresume`オプションを追加します。
b. 選択した VDA インストーラー (ローカルイメージまたは最小インストーラーのいずれか) を実行します。

「VDAのインストール（初回）」(/en-us/citrix-virtual-apps-desktops/2411/media/install-vda-first-attempt.png)

c. SCCM はリターンコードをキャプチャする必要があります。

- リターンコードが 0 または 8 の場合、インストールは完了しており、再起動が必要です。

「SCCMがリターンコードをキャプチャ」(/en-us/citrix-virtual-apps-desktops/2411/media/sccm-return-code.png)

- リターンコードが3の場合、マシンを再起動し、**VDAのインストール（2回目）**に制御を渡します。

「マシンの再起動」(/en-us/citrix-virtual-apps-desktops/2411/media/restart-machine.png)

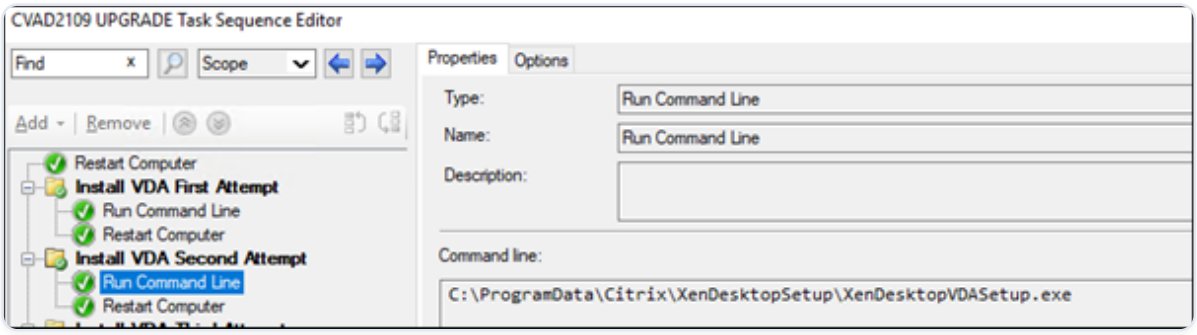
3. **VDAのインストール（2回目）：**VDAのインストールを続行します。

a. **VDAのインストール（初回）**の後、ファイル`%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml`が存在する場合、インストールは完了しておらず、再起動が完了した後に続行する必要があります。

「VDAのインストール（2回目）」(/en-us/citrix-virtual-apps-desktops/2411/media/install-vda-second-attempt.png)

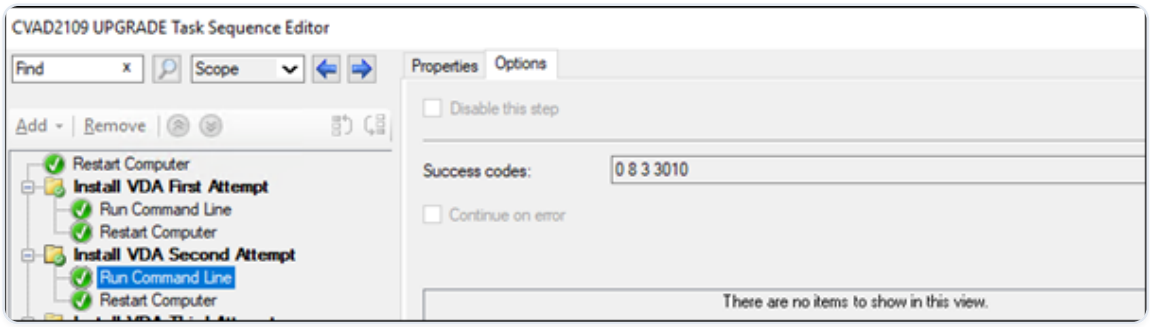
b. **VDAのインストール（2回目）**は、ファイル`%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml`が存在しなくなるか、0または8以外のリターンコードが返されるまで繰り返されます。その他のリターンコードはエラーとして扱い、INSTALL VDA SECOND ATTEMPTはエラーを報告して停止する必要があります。
c. コマンドラインパラメーターなしで、ファイル`%programdata%\Citrix\XenDesktopSetup\`ディレクトリから適切なVDAインストーラー（ほとんどの場合`XenDesktopVdaSetup.exe`、`VDAWorkstationCoreSetup_XXXX.exe`が使用された場合は`XenDesktopRemotePCSetup.exe`）を実行して、VDAのインストールを再開します。

（VDAインストーラーは、インストーラーの初回実行時に保存したパラメーターを使用します。）



d. VDAインストーラーからのリターンコードを確認してください。

- 0または8：成功、インストール完了、再起動が必要です。



- 3: インストールは完了していません。マシンを再起動し、ファイル `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` が存在しなくなるか、0 または 8 が返されるまで INSTALL VDA SECOND ATTEMPT を繰り返します。その他のリターンコードはエラーとして扱い、INSTALL VDA SECOND ATTEMPT はエラーを報告して終了する必要があります。

リターンコードの詳細については、Citrix インストールリターンコード を参照してください。

VDAインストールコマンドの例

利用可能なインストールオプションは、使用するインストーラーによって異なります。コマンドラインオプションの詳細については、以下の記事を参照してください。

- VDA のインストール
- コマンドラインを使用したインストール

REMOTE PC ACCESS のインストールコマンド

- 次のコマンドは、シングルセッションコア VDA インストーラー（`VDAWorkstationCoreSetup.exe`）を使用します。

```
VDAWorkstationCoreSetup.exe /quiet /controllers “control.domain.com” /
enable_hdx_ports /noresume /noreboot
```

- 次のコマンドは、シングルセッションフル VDA インストーラー（`VDAWorkstationSetup.exe`）を使用します。

```
VDAWorkstationSetup.exe /quiet /remotepc /physicalmachine /controllers
“control.domain.com” /enable_hdx_ports /noresume /noreboot
```

専用 VDI のインストールコマンド

- 次のコマンドは、シングルセッションフル VDA インストーラー（`VDAWorkstationSetup.exe`）を使用します。

```
VDAWorkstationSetup.exe /quiet /components vda /controllers
“control.domain.com” /enable_hdx_ports /enable_remote_assistance /noresume /
noreboot
```

Microsoft Intune を使用した VDA のインストール

概要

この記事では、Microsoft Intune を使用して VDA を展開する方法について説明します。詳細については、Microsoft のドキュメントを参照してください。

> **注：**
>
> 以下の記事は、Citrix® が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、お客様のニーズに合わせてカスタマイズできます。Citrix は、お客様のニーズに合わせてこれに必要な更新や調整について責任を負いません。

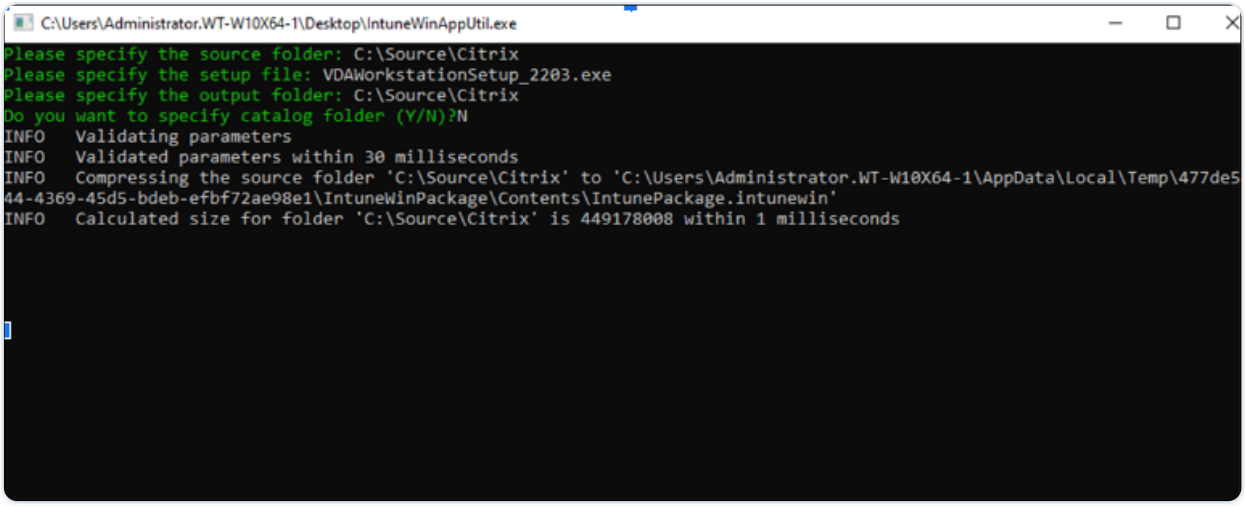
Microsoft Intune を使用して VDA を展開するための主要な手順

1. Citrix VDA のインストールを準備する。
2. Microsoft 365 開発者プログラムサブスクライバーを設定する。
3. アプリを追加して割り当てる。
4. 登録済みデバイスにアプリをインストールする。

ステップ 1: CITRIX VDA のインストールを準備する

1. 更新された IntuneWinAppUtil.exe を GitHub からダウンロードします。

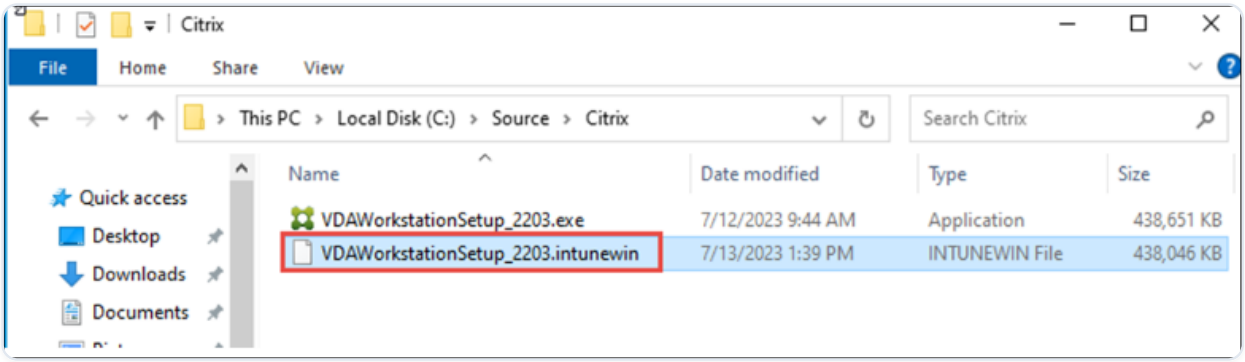
2. **管理者として実行**を使用して `IntuneWinAppUtil.exe` ファイルを実行します。
3. 次のデータを入力します。



   a. **ソースフォルダーを指定してください**: アプリケーションのセットアップファイルが含まれるフォルダーを入力します。例: C:\source\Citrix。
   b. **セットアップファイルを指定してください**: セットアップファイル名（setup.exeやsetup.msiなど）を入力します。例: VDAWorkstationSetup_2203.exe。
   c. **出力フォルダーを指定してください**: .intunewinファイルを生成するための出力フォルダーのパスを入力します。例: C:\source\Citrix。
   d. **カタログフォルダーを指定しますか (Y/N)**: Nと入力します。

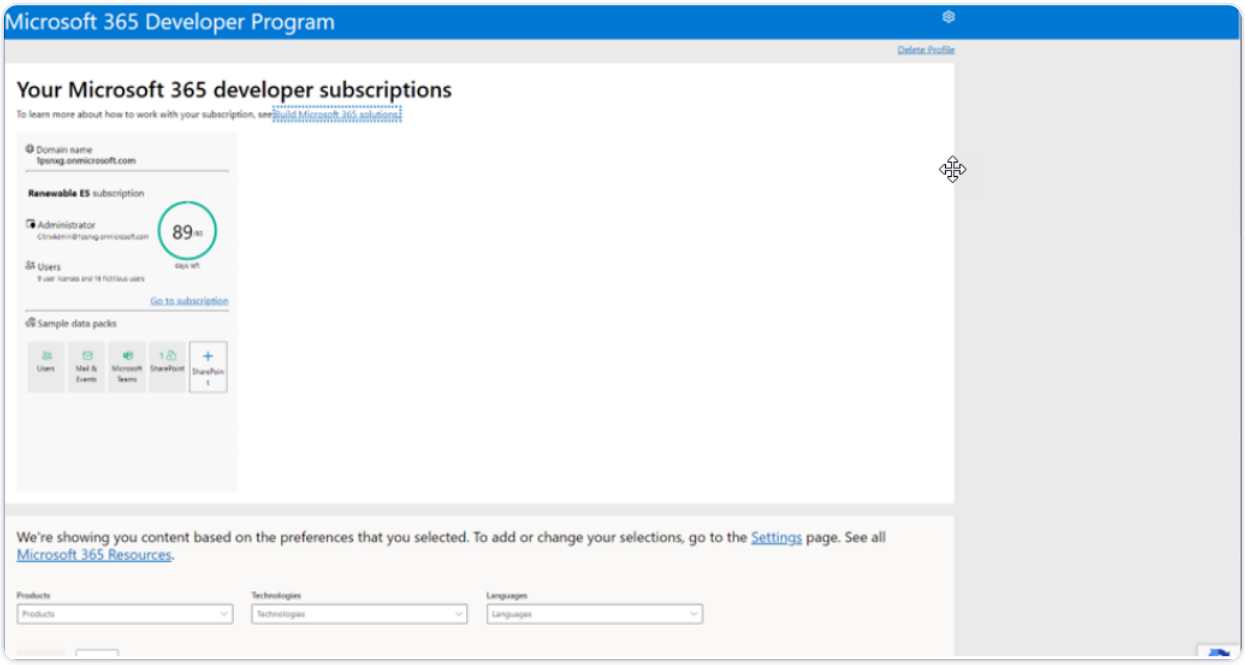
> **注:**
>
> **Win32 Content Prep Tool** の実行中は数分間お待ちください。`.intunewin` ファイルが生成されると、コマンドプロンプトの下部にステータスが 100% と表示されます。

4. プロセスが完了したら、出力フォルダー（この例では `C:\source\Citrix`）に移動して、Microsoft Intune展開ファイルを取得します。
5. Microsoft Intuneの無料試用版にサインアップします。

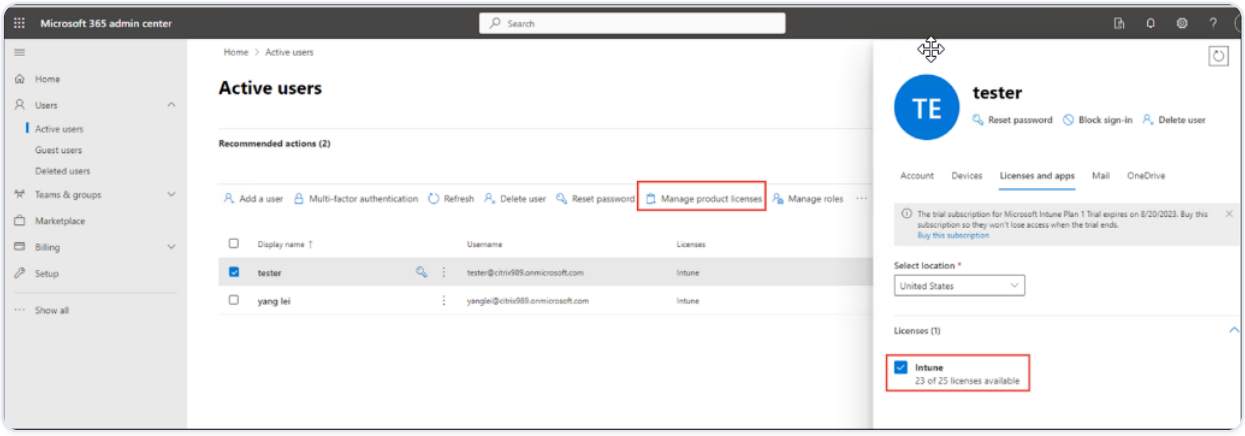


ステップ2: MICROSOFT 365開発者プログラムサブスクライバーを設定する

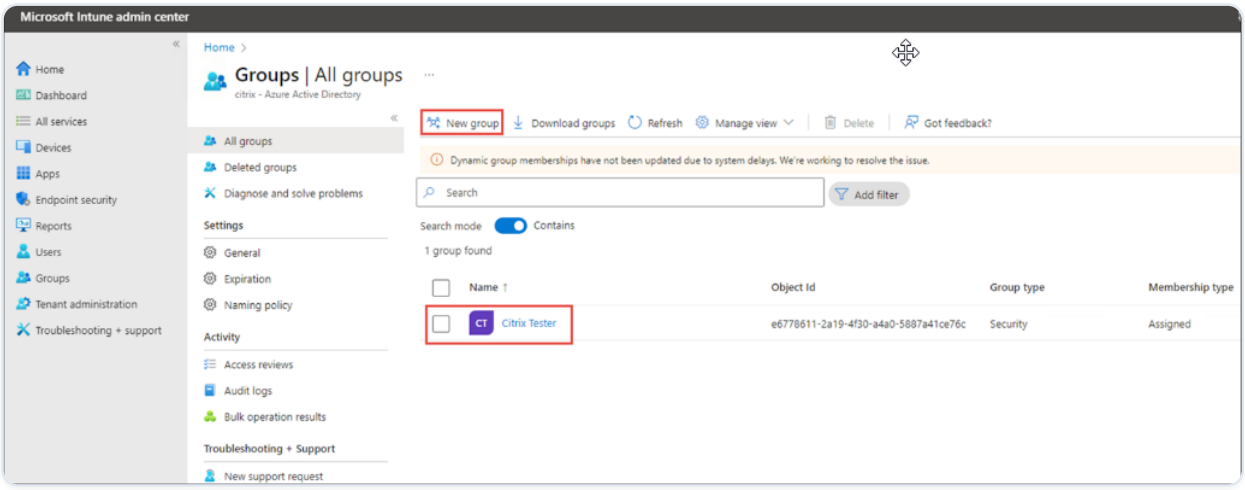
1. インスタントサンドボックスを作成してサブスクリプションをアクティブ化します。 開発者サンドボックスを取得するには、Microsoft 365開発者プログラムダッシュボード にアクセスし、**新しいサブスクリプションの追加**を選択します。



2. Microsoft 365管理センターでユーザーを作成し、そのユーザーにライセンスを割り当てます。



3. グループを作成します。



4. グループが作成されたら、そのグループにMDM機関を提供する必要があります。自動登録を設定します。アクティブ化には1分ほどかかる場合があります。 または、以下の手順を完了して、MDM機関をグループに手動で追加することもできます。

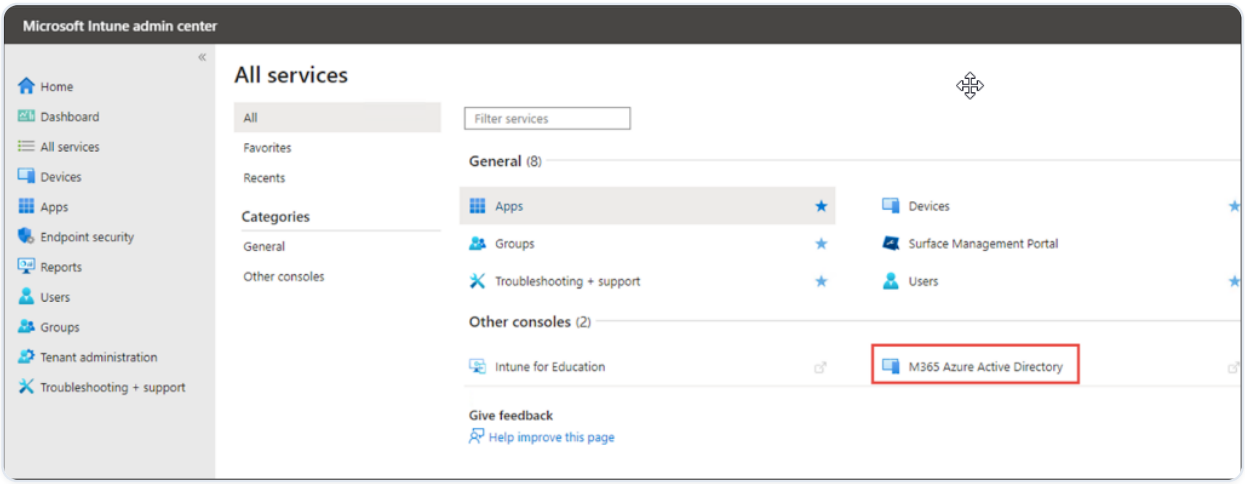
   a. **すべてのサービス > Microsoft Entra** に移動します。

   b. 「**設定 > モビリティ**」に移動し、「**Microsoft Intune**」を選択します。

   c. 作成したばかりのグループを選択します。これにより、MDMユーザー範囲のページが開きます。

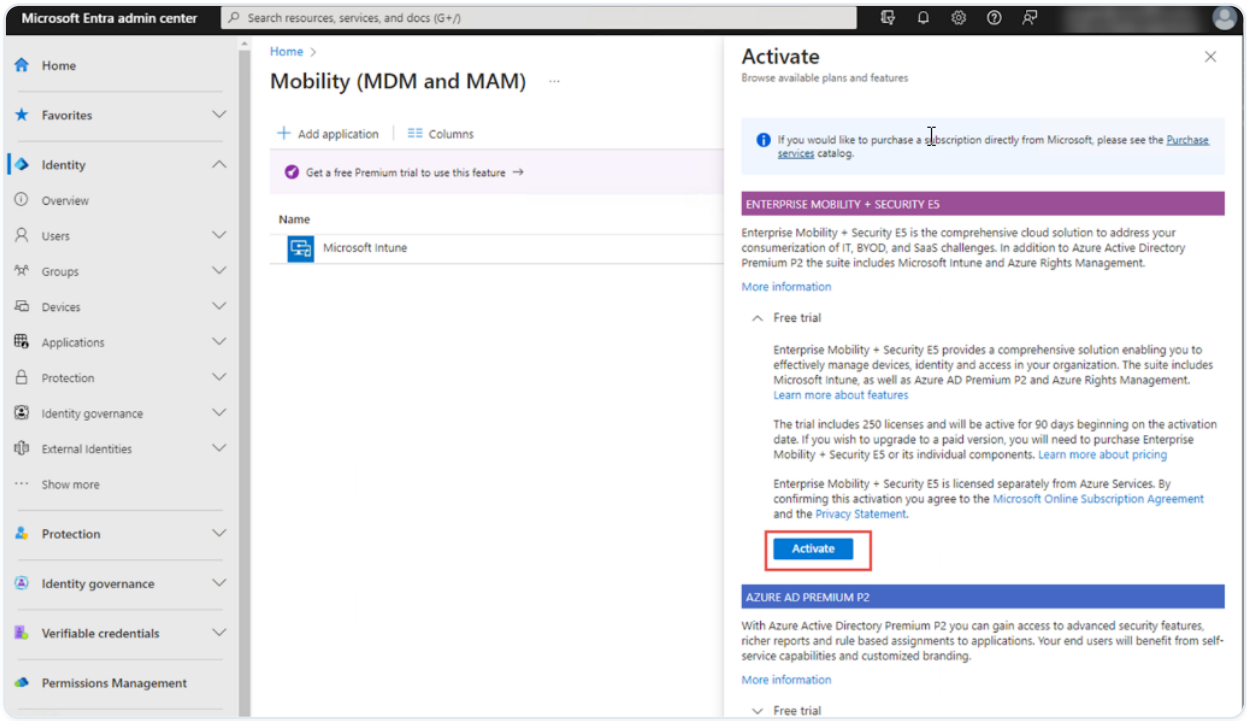
   d. 「**保存**」をクリックします。

5. 「**すべてのサービス**」タブで、「**M365 Azure Active Directory**」をクリックします。

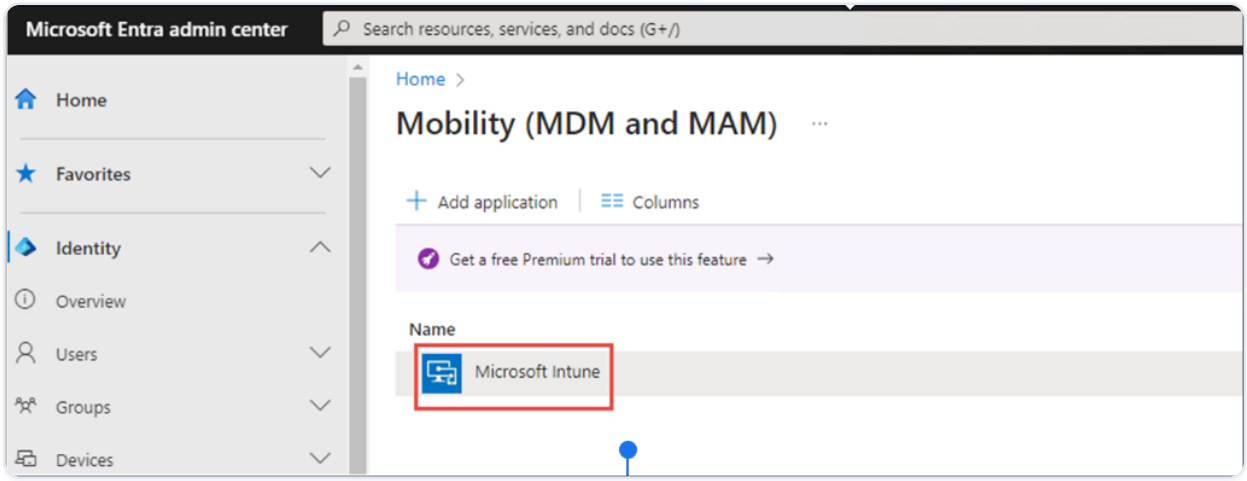


6. **この機能を使用するために無料のPremium試用版を入手する** をクリックします。 「Intune MDM」(/en-us/citrix-virtual-apps-desktops/2411/media/intune-mdm.png)

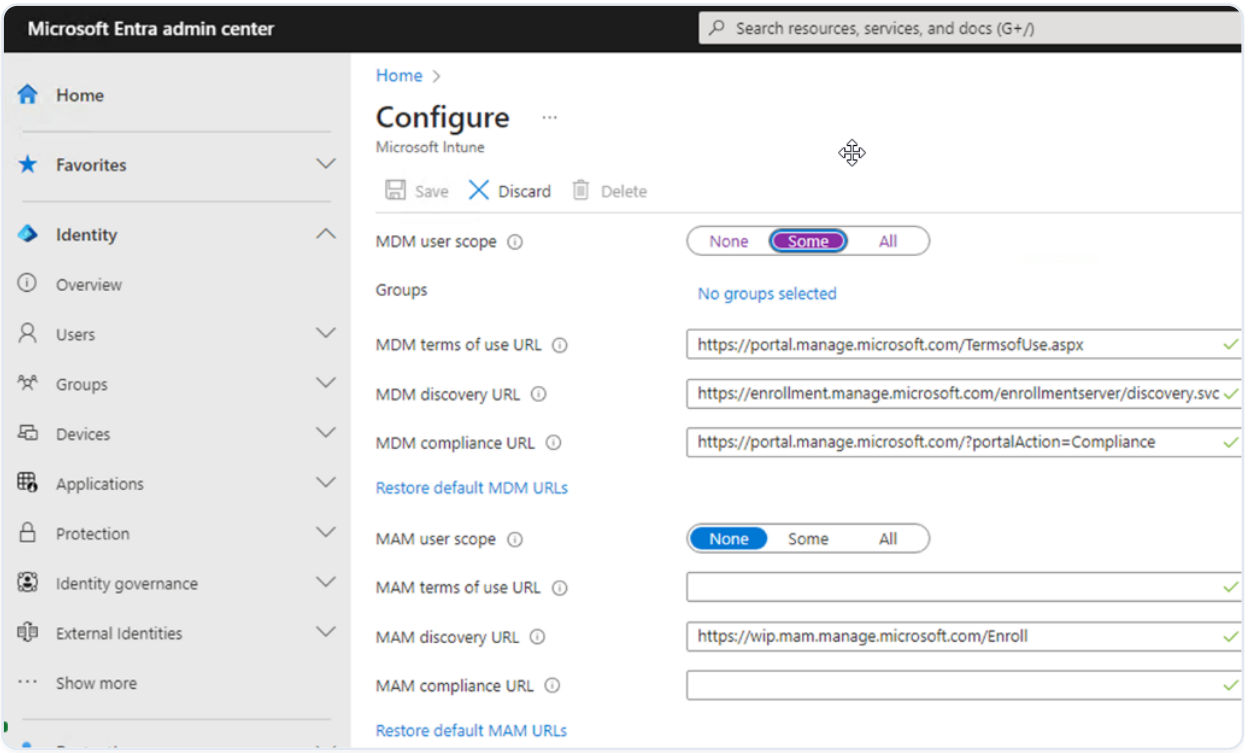
7. 「**アクティブ化**」をクリックします。



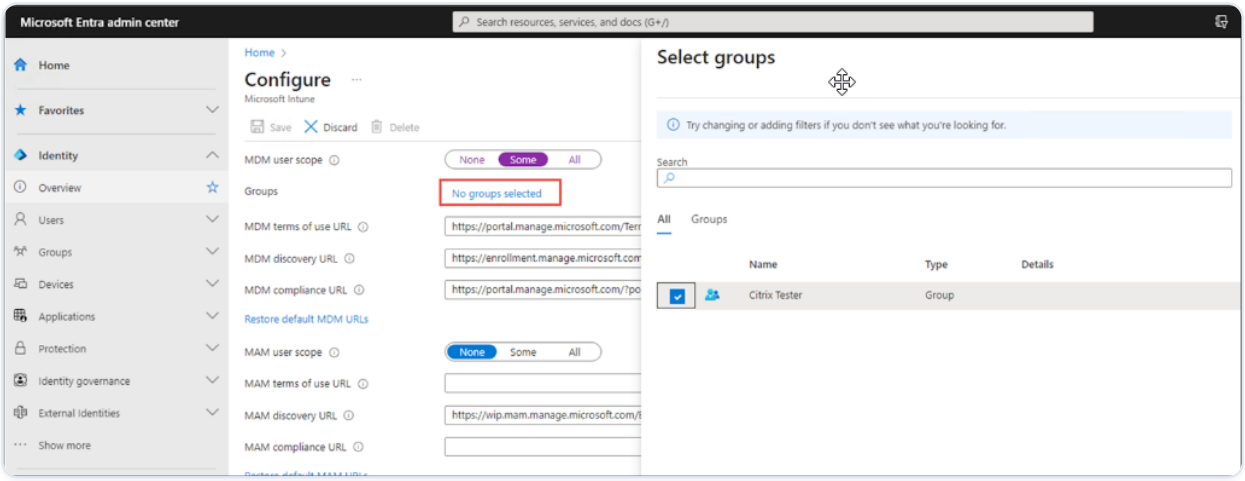
8. 次に、「**Microsoft Intune**」をクリックします。



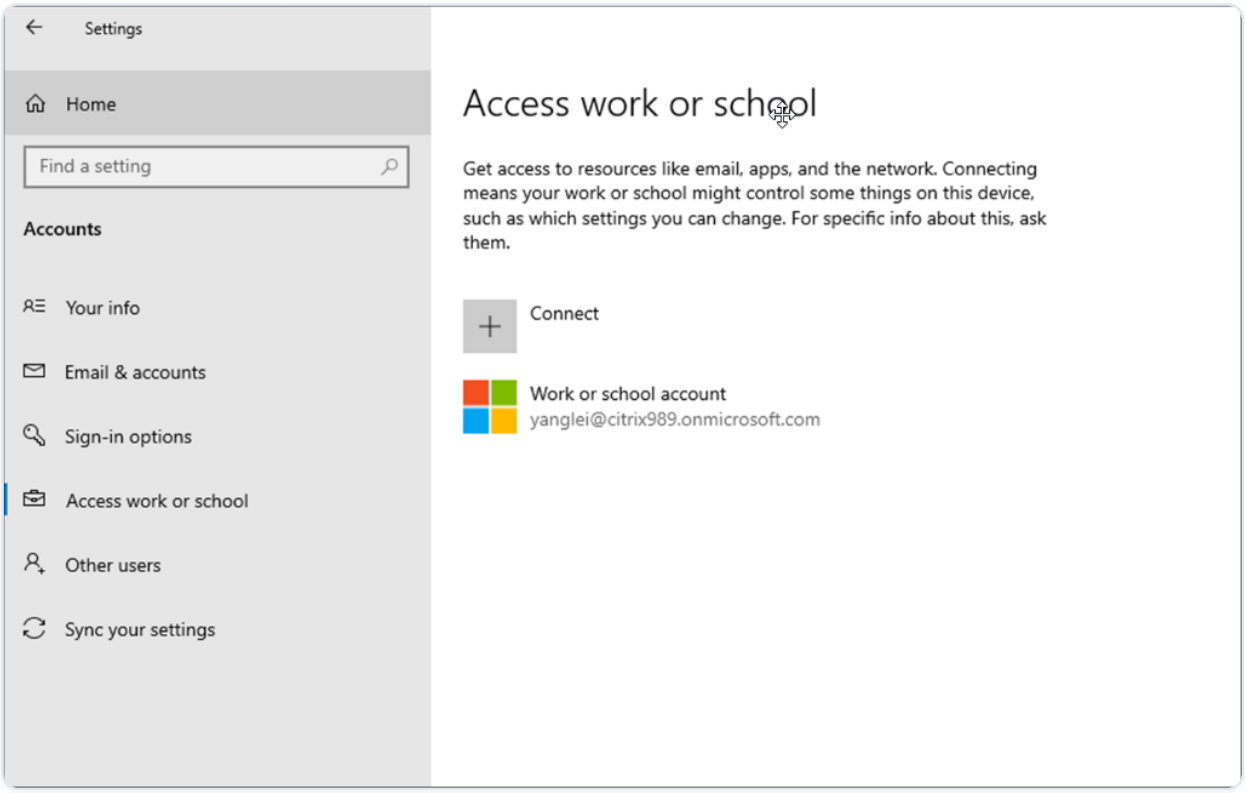
9. 「**構成**」タブで、必要な構成を入力します。



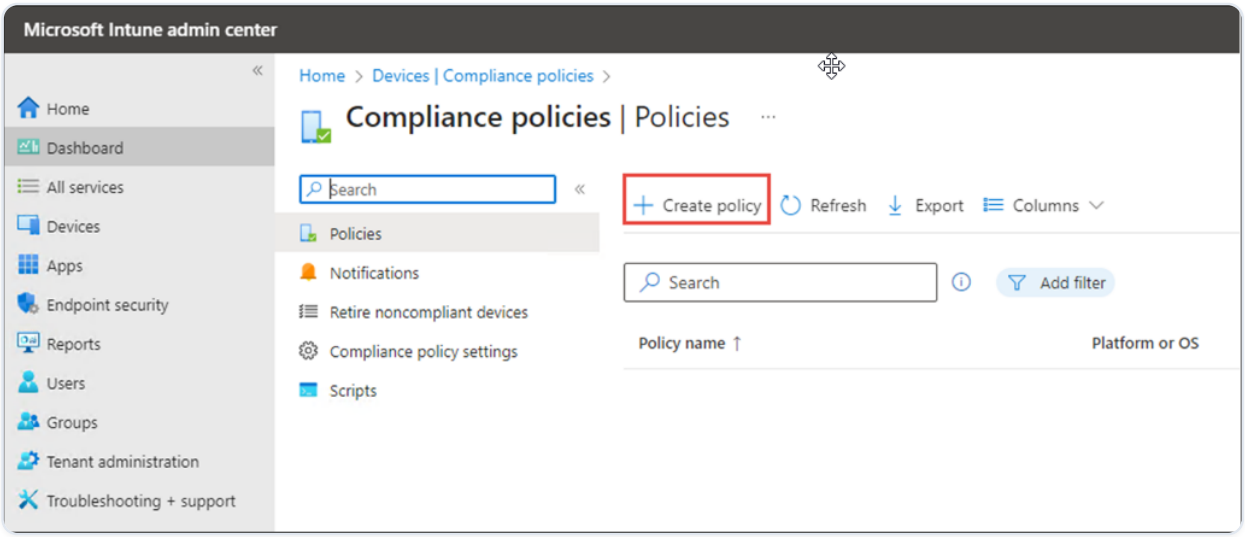
10. グループを追加するには、**グループが選択されていません**をクリックします。



11. デバイスを登録します。



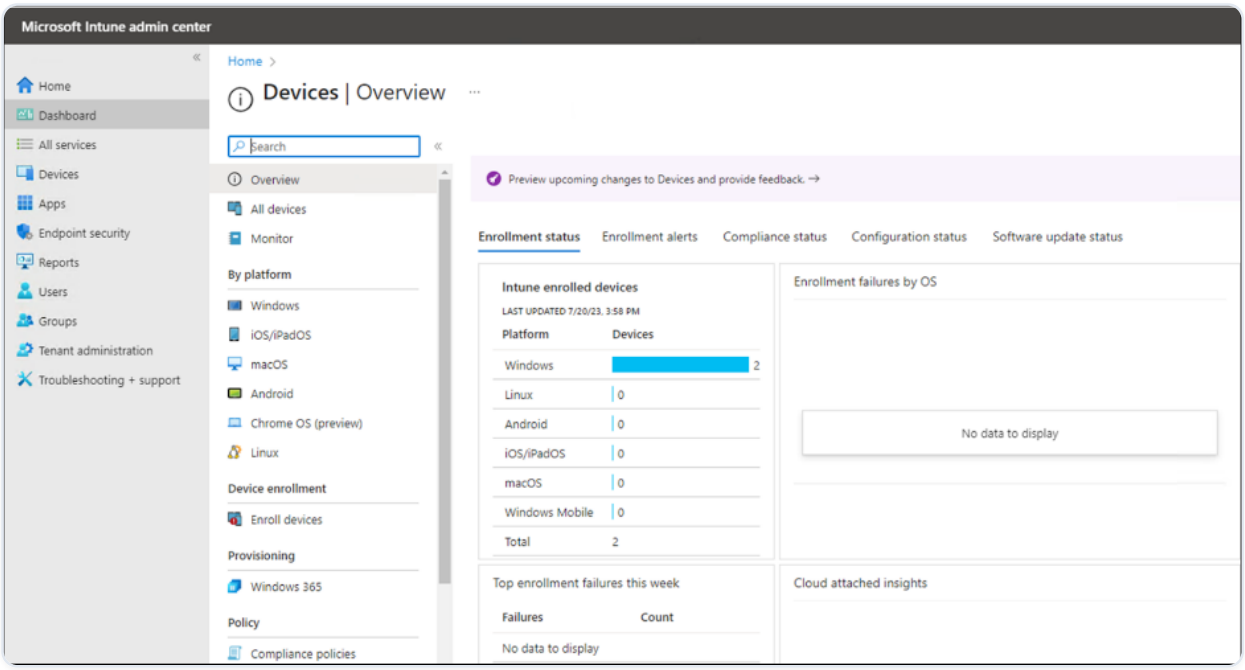
12. 新しく作成したデバイスのコンプライアンスを`Compliant`に変更するためのデバイスコンプライアンスポリシーを作成します。



13. **割り当て**タブに移動して、新しく作成したグループを追加します。

    完全に管理(/en-us/citrix-virtual-apps-desktops/2411/media/intune-fully-managed-and-dedicated.png)

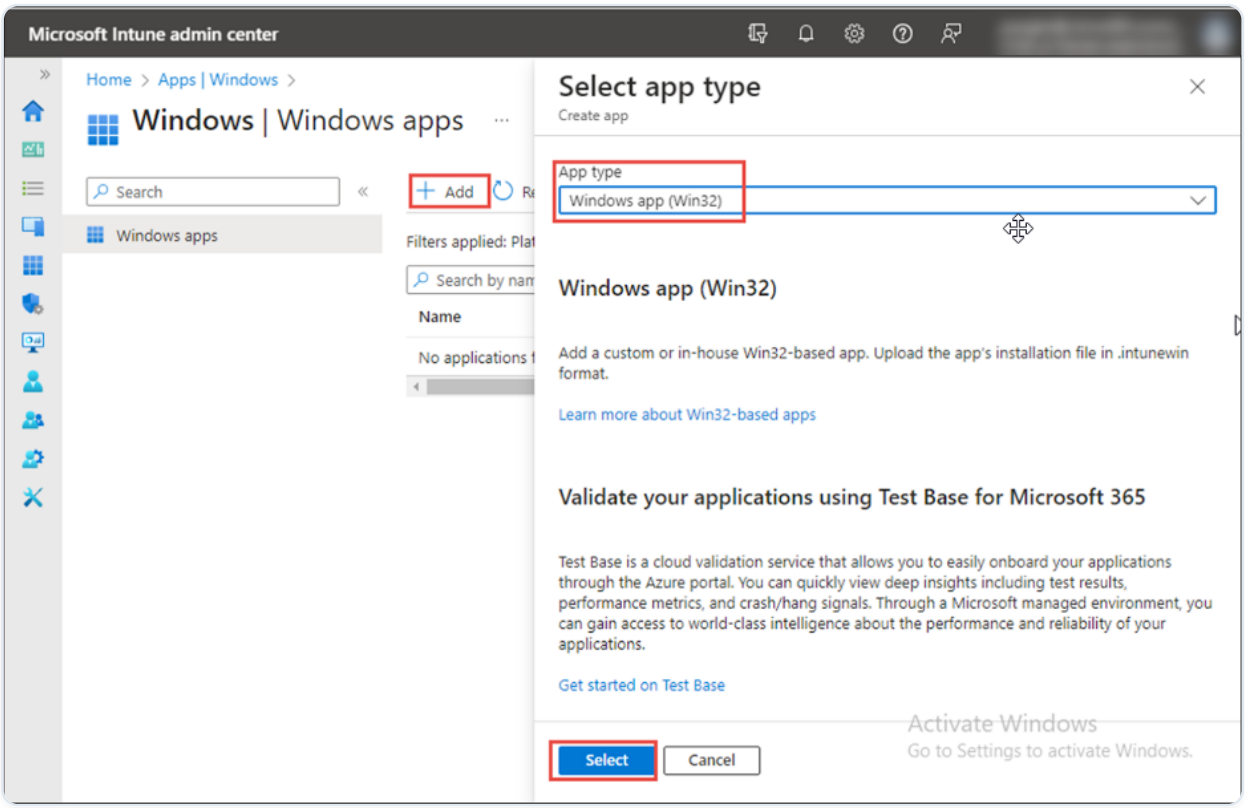
14. デバイスの登録を確認します。



詳細については、Microsoft 365 開発者プログラムを参照してください。

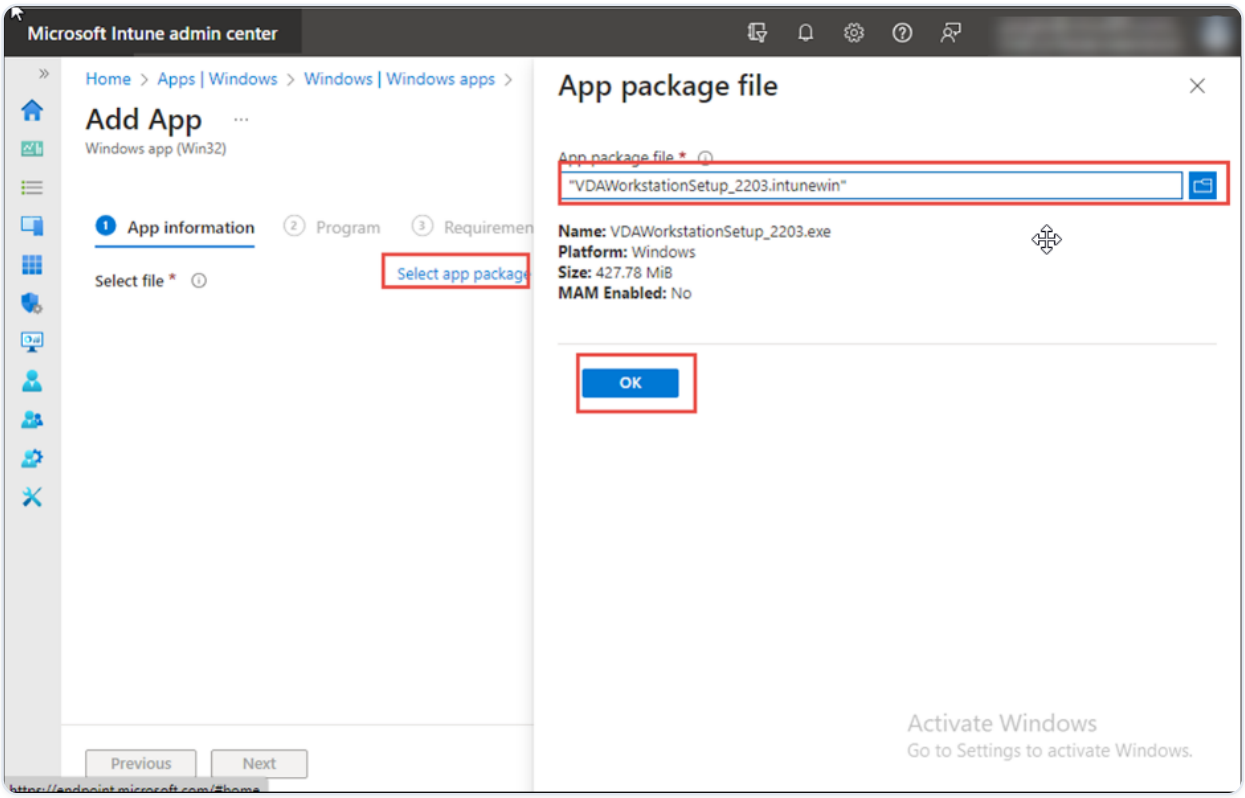
ステップ3：アプリの追加と割り当て

1. Microsoft Intune 管理センターにサインインします。
2. **アプリ > すべてのアプリ > 追加**を選択するか、**アプリ > Windows > Windows アプリ**に移動します。



3. ペインで、 > を選択し、 をクリックします。

4. ペインで、 をクリックします。 をクリックします。
5. 拡張子 `.intunewin` の準備済みファイルを選択します。この準備済みファイルは、Citrix VDA のインストールの準備 の手順で作成されます。アプリに関する詳細情報を含むページが表示されます。

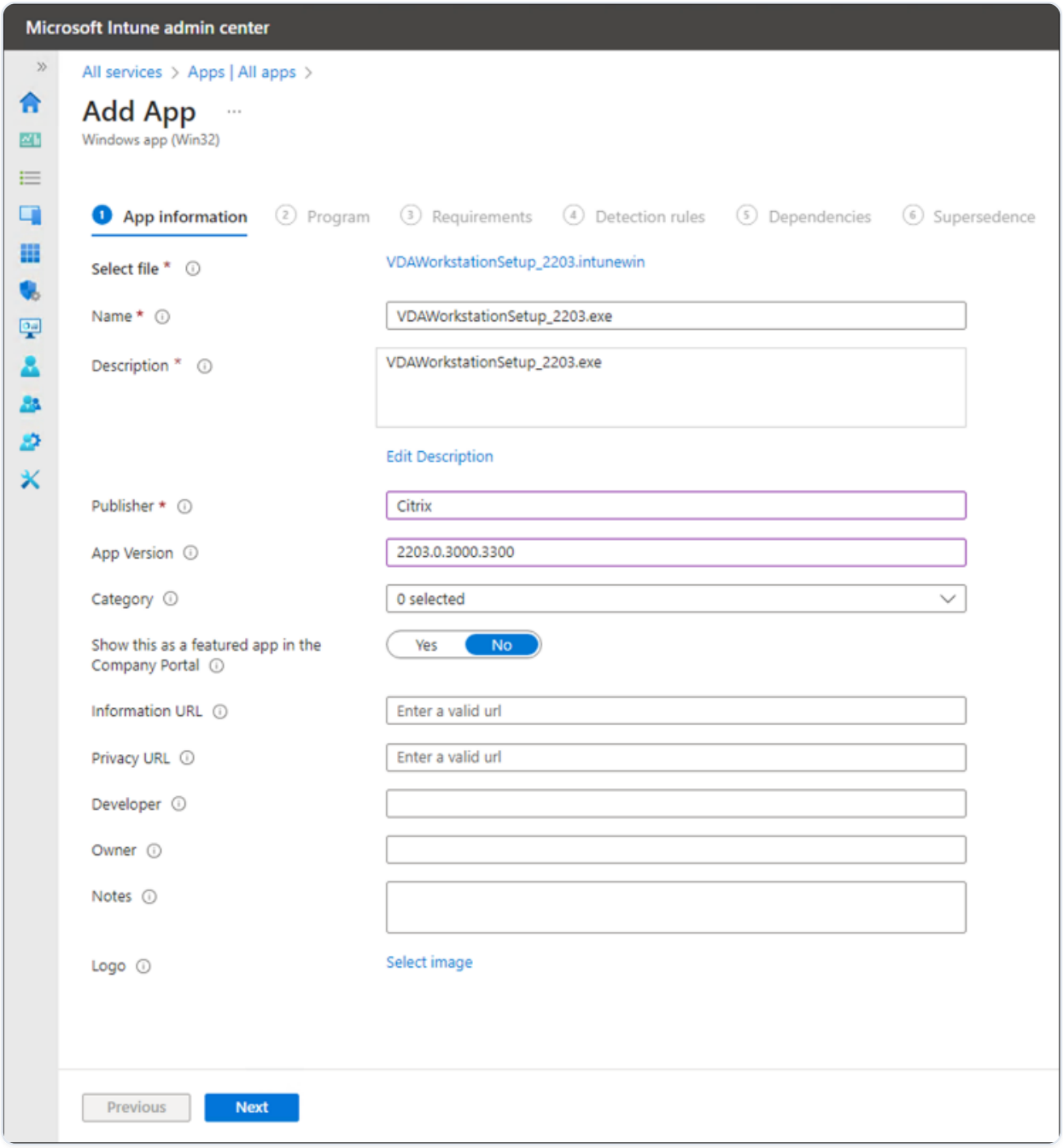


注：

- サーバーコアマシンを使用している場合は、VDAワークステーションコアを使用する必要があります。
- Windows 10デスクトップOSを使用している場合は、VDAワークステーションを使用する必要があります。
- サーバーOS（例：Windows 2022）を使用している場合は、VDAサーバーセットアップを使用する必要があります。
- この例ではバージョン2203を使用していますが、これはすべてのバージョンに適用されます。

6. **App package file**ペインで**OK**をクリックします。

7. 次の画面で、「**アプリ情報**」タブの下にあるアプリの「**名前**」とWindowsアプリの「**説明**」を入力します。「**発行元**」の名前を `Citrix` として入力し、ここで追加のアプリ情報を指定できます。「**次へ**」をクリックします。



8. 次の画面で、以下の値を入力します。

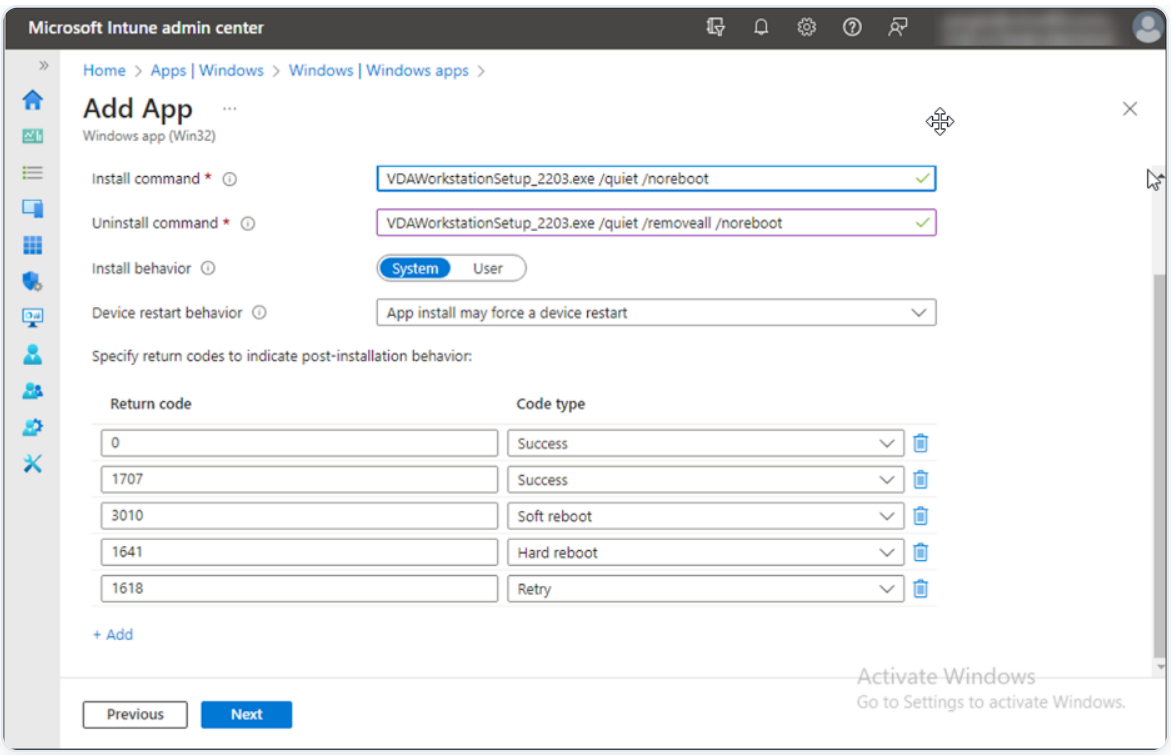
   - **インストールコマンド**: `VDAWorkstationSetup_2203.exe /quiet /noreboot`
   - **アンインストールコマンド**: `VDAWorkstationSetup_2203.exe /quiet /removeall /noreboot`
   - **インストール動作**:

- **システム**：グループ内のすべてのデバイスにアプリをインストールするには、このオプションを選択します。
- **ユーザー**：グループ内の特定のユーザーデバイスにのみアプリをインストールするには、このオプションを選択します。

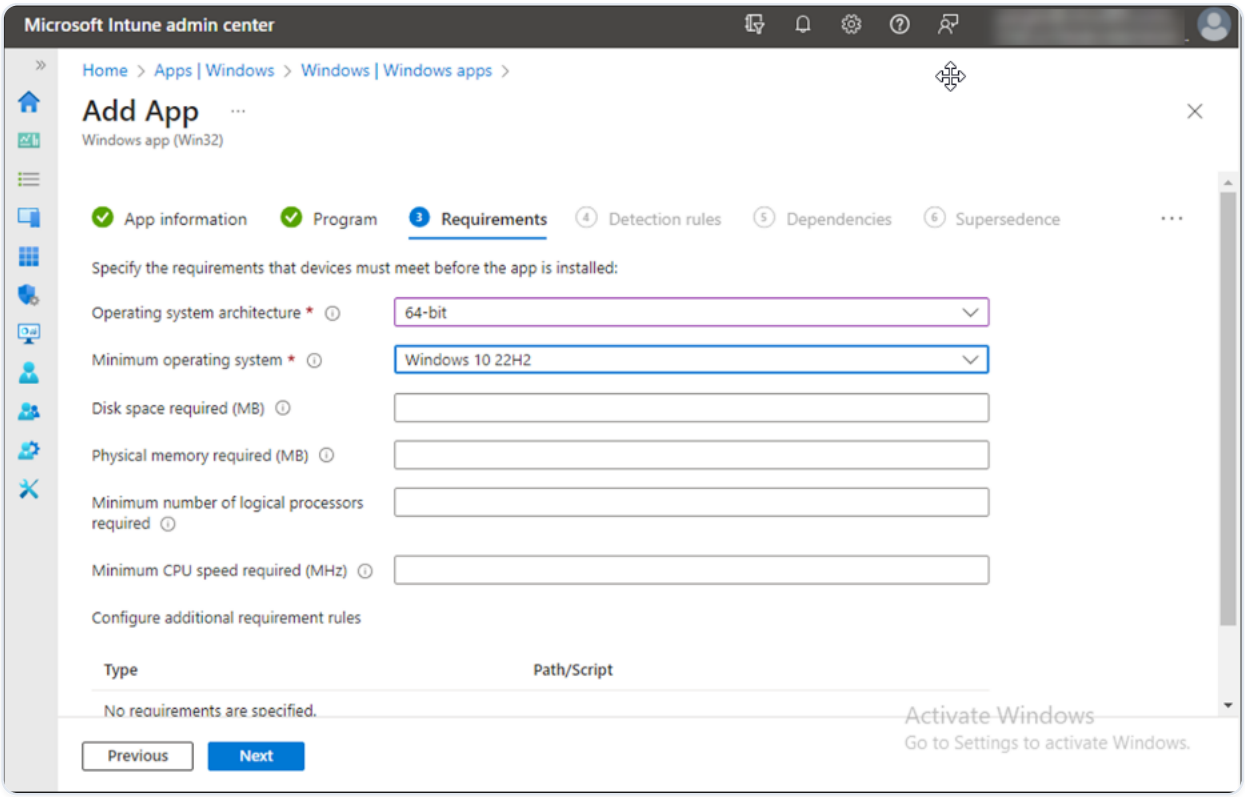
9. **次へ**」をクリックします。

注:

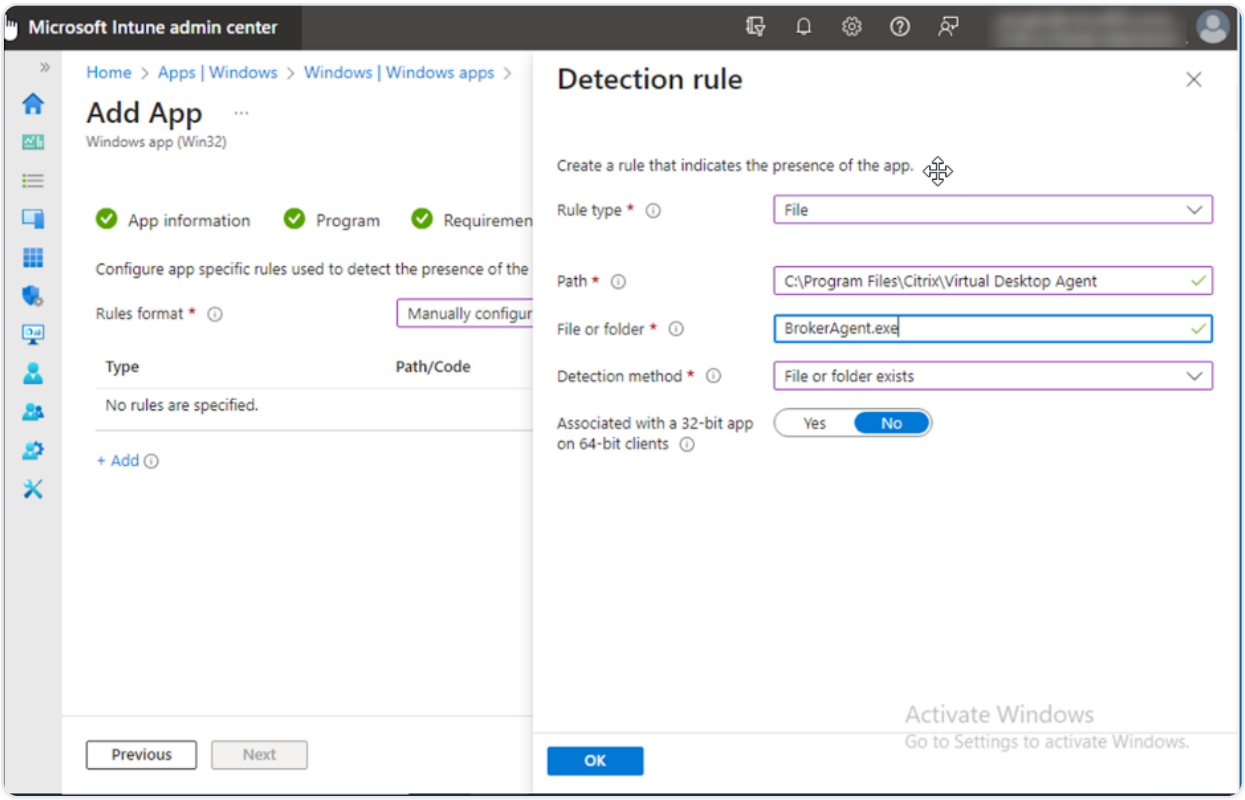
- この例ではバージョン2203を使用していますが、どのバージョンでも使用できます。
- コマンドに`/noreboot`を追加しても、インストールまたは展開中に再起動がないという意味ではなく、強制的な再起動を適用するだけです。 スクリプトの詳細については、「VDAをインストールするためのコマンドラインオプション」を参照してください。
- **デバイスの再起動動作**」で、「**Intuneは強制的にデバイスを再起動します**」を選択します。
- **リターンコード**」テキストボックスに、インストール後の成功のために`0`、`3`、および`8`を入力します。 その他のリターンコードについては、「Citrixインストールのリターンコード」を参照してください。



10. 次の画面で、「**要件**」タブの下に、必要な値を入力します。「**次へ**」をクリックします。

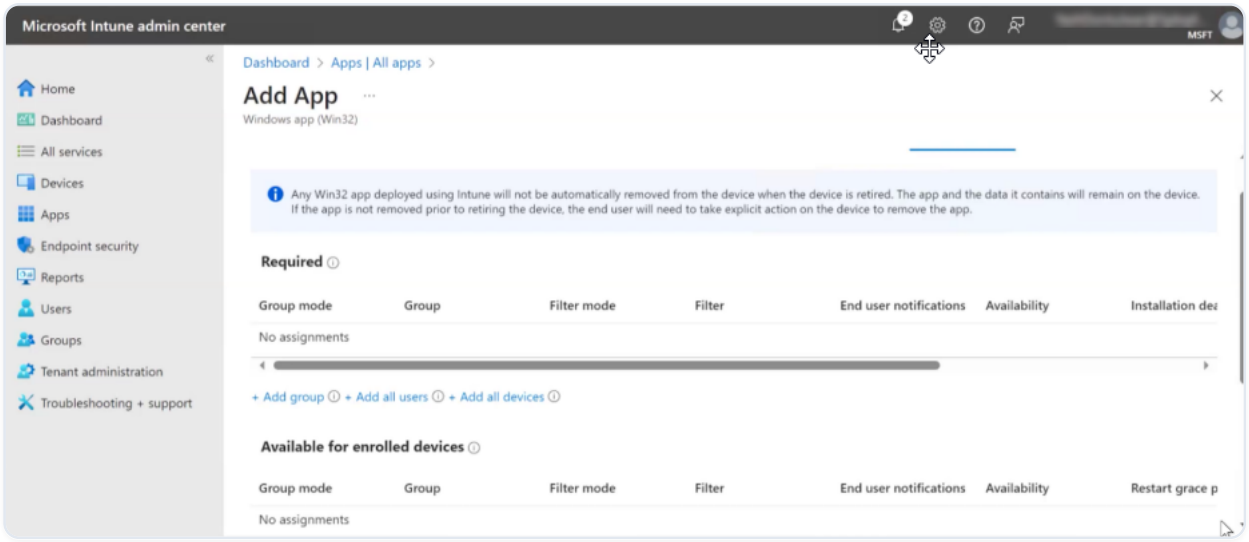


11. 次の画面で、「**検出ルール**」タブの下に、Brokerエージェントを追加するための「**検出ルール**」を追加します。「**OK**」をクリックします。

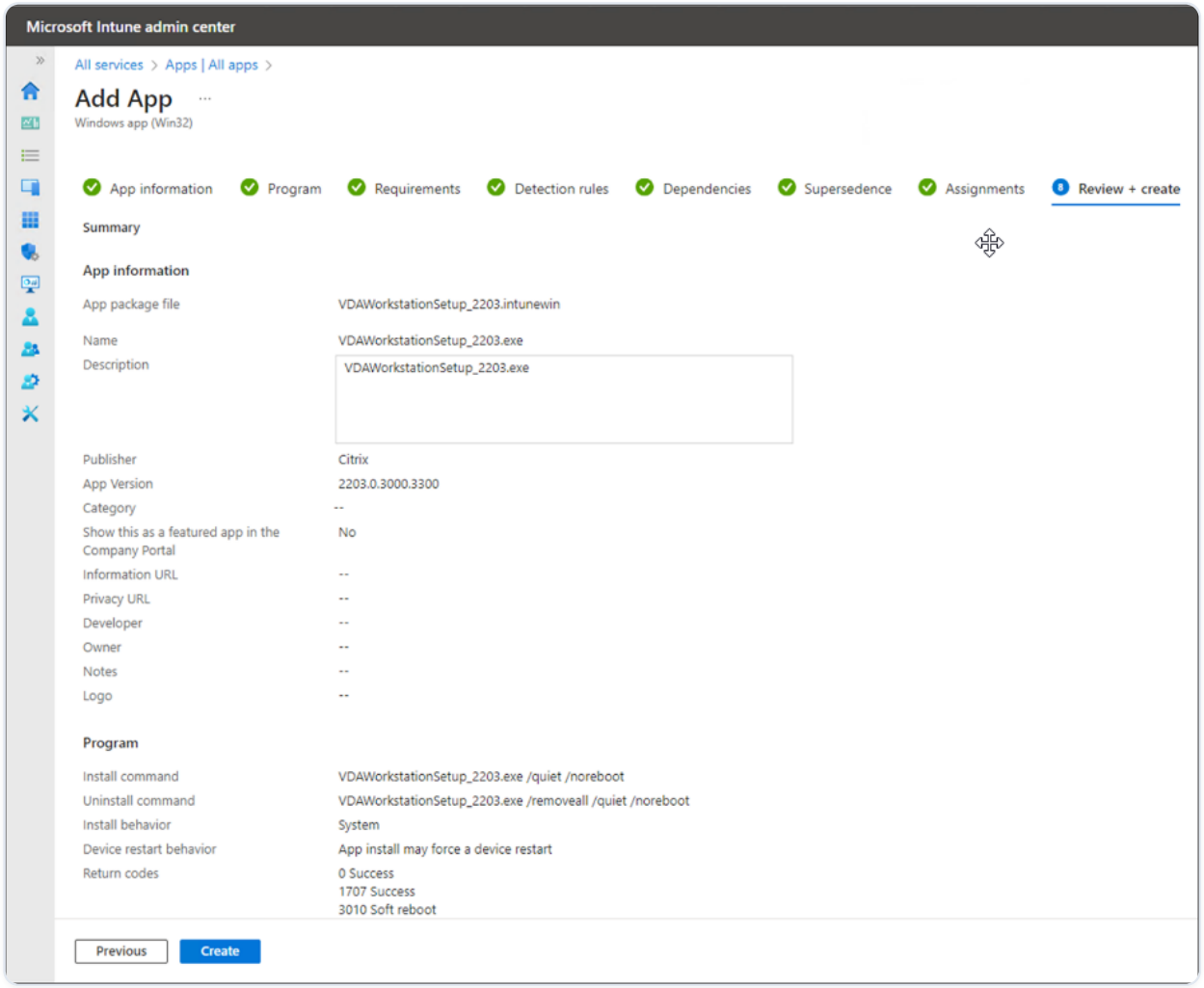


12. **割り当て**」タブで、次のデバイスを追加できます。

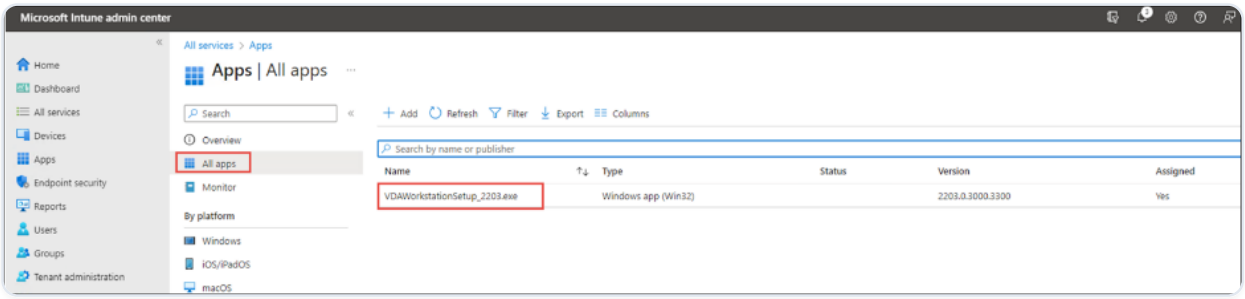
- **必須**: 更新が自動的に行われるデバイス。
- **登録済みデバイスで利用可能**: 更新が手動で行われるデバイス。



13. 詳細を確認し、「**作成**」をクリックします。



アプリが正常に割り当てられました。



詳細については、「アプリの追加と割り当て」を参照してください。

ステップ4：登録済みデバイスにアプリをインストールする

1. 登録済みのWindows 10デスクトップデバイスにサインインします。 デバイスはMicrosoft Intuneに登録されている必要があります。また、アプリに割り当てたグループに含まれるアカウントを使用してデバイスにサインインする必要があります。詳細については、Microsoftのドキュメントを参照してください。
2. **スタート**メニューから**Microsoft Store**を開きます。
3. **Company Portal**アプリを検索してインストールします。

   
4. 「**Company Portal**」アプリを実行します。
5. Microsoft Intuneを使用して追加したアプリをクリックします。 Intuneユーザーにアプリが正常に割り当てられていない場合、次のメッセージが表示されます。 `Your IT administrator did not make any apps available to you.`
6. **インストール** をクリックします。

サイトを作成する

> **注：**
>
> - サイト作成中に、ハイブリッド権限ライセンスを有効にするライセンスを追加した後、サイト作成が完了するまで、パブリッククラウドホスト（Microsoft Azure、Google Cloud Platform、Amazon Web Servicesなど）は接続タイプリストに表示されません。
> - ライセンスアクティベーションサービスを有効にしている間、または有効にした後に、製品エディションやライセンスモデルを手動で変更しないでください。

> サイトとは、Citrix Virtual Apps and Desktops™展開に付ける名前です。これには、Delivery Controllerおよびその他のコアコンポーネント、Virtual Delivery Agent (VDA)、ホストへの接続、マシンカタログ、およびデリバリーグループが含まれます。サイトは、コアコンポーネントをインストールした後、最初のマシンカタログとデリバリーグループを作成する前に作成します。

ControllerがServer Coreにインストールされている場合は、サイトを作成するためにCitrix Virtual Apps and Desktops SDKのPowerShellコマンドレットを使用します。

サイトを作成すると、Citrixカスタマーエクスペリエンス向上プログラム（CEIP）に自動的に登録されます。CEIPは匿名の統計情報と使用状況情報を収集し、Citrixに送信します。最初のデータパッケージは、サイト作成後約7日後にCitrixに送信されます。サイト作成後いつでも登録を変更できます。Web Studioの左ペインで**設定**を選択し、**Citrixカスタマーエクスペリエンス向上プログラム**の設定を見つけます。詳細については、`<http://more.citrix.com/XD-CEIP>`を参照してください。

サイトを作成したユーザーは、フル管理者になります。詳細については、委任管理を参照してください。

サイトを作成する前にこの記事を確認して、何が期待できるかを知っておいてください。

ステップ1. サイト作成ウィザードを開く - Citrix Site Manager

Citrix Virtual Apps and Desktops展開（サイトとも呼ばれます）を設定するには、Citrix Site Managerツールを使用します。このツールは、Delivery Controllerをインストールすると自動的にインストールされます。

このツールを実行するには、Delivery Controllerでデスクトップのスタートメニューを開き、**Citrix > Citrix Site Manager**を選択します。Web Studioのインストールを参照してください。

ステップ2. サイト名

はじめにページで、サイトの名前を入力します。

ステップ3. データベース

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

データベースページには、サイト、監視、および構成ログのデータベースを設定するための選択肢が含まれています。データベースのセットアップの選択肢と要件の詳細については、データベースを参照してください。

注：

SQL Server Always Onリスナーが TLS暗号化用に構成されている場合、データベース作成権限を持つ資格情報の入力を求められることがあります。有効な管理者資格情報を入力しても、データベースの作成は引き続き失敗します。SQL Server証明書に、サブジェクト代替名（SAN）にリスナーのDNS名が含まれていることを確認してください。詳細については、`<https://docs.microsoft.com/ja-jp/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover#SSLcertificates>` を参照してください。

サイトデータベースとしてSQL Server Expressをインストールすることを選択した場合（デフォルト）、そのソフトウェアのインストール後に再起動が発生します。サイトデータベースとしてSQL Server Expressソフトウェアをインストールしないことを選択した場合は、その再起動は発生しません。

デフォルトのSQL Server Expressを使用しない場合は、サイトを作成する前にSQL Serverソフトウェアがマシンにインストールされていることを確認してください。システム要件にサポートされているバージョンが記載されています。

サイトにDelivery Controllerを追加したい場合で、すでに他のサーバーにControllerソフトウェアをインストールしている場合は、このページからそれらのControllerを追加できます。データベースを設定するスクリプトを生成する予定がある場合は、スクリプトを生成する前にControllerを追加してください。

ステップ4. ライセンス

ライセンスページで、ライセンスサーバーのアドレスを指定し、使用する（インストールする）ライセンスを示します。

注：

- License Activation Service (LAS) は、従来のCitrixレガシーライセンスに代わる新しいクラウドベースのライセンスソリューションです。詳細については、以下を参照してください。
  - Citrix Virtual Apps and Desktops ドキュメント: ライセンスアクティベーションサービス
  - ライセンスドキュメント: License Activation Service
- License Activation Serviceを有効にしている間または有効にした後に、製品エディションやライセンスモデルを手動で変更しないでください。

- `name:[port]`の形式でライセンスサーバーのアドレスを指定します。*名前*はFQDN、NetBIOS、またはIPアドレスである必要があります。FQDNを推奨します。ポート番号を省略した場合、デフォルトは27000です。**接続**をクリックします。ライセンスサーバーへの接続が成功するまで、次のページに進むことはできません。
- 接続が確立されると、デフォルトで**既存のライセンスを使用**が選択されます。表示には、現在インストールされているライセンスに基づいて、この製品として構成できる互換性のある製品がリストされます。
  - ライセンスサーバーがLicense Activation Service (LAS)を使用するように構成されている場合、メタインストーラーはエンタイトルメントを表示します。エンタイトルメントは、対応するライセンス有効期限とともに提供されます。これらのライセンスのいずれかを使用して、この製品をリストされている製品の1つとして構成したい場合は、そのエントリを選択します。
  - この製品で使用するためにライセンスを割り当ててダウンロード済み（Citrix Manage Licenses Toolを使用）だが、まだライセンスをインストールしていない場合：
    - **ライセンスファイルを参照**をクリックします。
    - ファイルエクスプローラーで、ダウンロードしたライセンスを見つけて選択します。関連する製品がサイト作成ウィザードの**ライセンス**ページに表示されます。使用したいエントリを選択します。
  - 目的の製品が表示されない場合、または割り当て済みでダウンロード済みのライセンスがない場合は、ライセンスを割り当て、ダウンロードしてインストールできます。これを行うには、ライセンスサーバーがインターネットにアクセスできる必要があります。目的の製品のライセンスアクセスコードが必要です。Citrixからそのコードがメールで送信されます。

- **割り当ててダウンロード**をクリックします。
- **ライセンスの割り当て**ダイアログで、Citrixから送信されたライセンスアクセスコードを入力します。**ライセンスを割り当てる**をクリックします。
- 新しいライセンスに関連付けられている製品が、サイト作成ウィザードの**ライセンス**ページに表示されます。使用するエントリを選択します。

- または、**30日間の無料試用版を使用**を選択し、後でライセンスをインストールします。詳細については、ライセンスドキュメントを参照してください。

手順5. 概要

概要ページには、指定した情報が一覧表示されます。何か変更したい場合は、**戻る**ボタンを使用します。完了したら、**完了**をクリックします。

詳細情報

ホスト接続、ネットワーク、およびストレージ

ハイパーバイザーまたはその他のサービス上のVMを使用してアプリケーションとデスクトップを配信する場合、オプションでそのホストへの最初の接続を作成できます。その接続のストレージおよびネットワークリソースも指定できます。サイト作成後、この接続とリソースを変更したり、さらに接続を作成したりできます。詳細については、「接続とリソース」を参照してください。

- **接続**ページで指定される情報については、「接続とリソース」を参照してください。
  - ハイパーバイザーまたはその他のサービス上のVMを使用しない場合（またはWeb Studioを使用して専用ブレードPC上のデスクトップを管理する場合）は、接続の種類として**なし**を選択します。
  - Remote PC Accessサイトを構成していて、Wake on LAN機能を使用する予定がある場合は、**Microsoft System Center Virtual Machine Manager**または**Remote PC Wake on LAN**の種類を選択します。詳細については、「Wake on LAN」を参照してください。

  接続の種類に加えて、Citrixツール（Machine Creation Services™など）またはその他のツールを使用してVMを作成するかどうかを指定します。
- **ストレージ**および**ネットワーク**ページで指定される情報については、「ホストストレージ」、「ストレージ管理」、および「ストレージの選択」を参照してください。
- ハイブリッド権限ライセンスをお持ちで、パブリッククラウドホスト接続（AWSなど）を追加している場合、それらの接続がここに一覧表示されます。これらのパブリッククラウドホスト接続を表示するには、追加後数分経ってからWeb Studioを更新してください。

リモートPCアクセス

Remote PC Accessの展開については、「Remote PC Access」を参照してください。

Wake on LAN機能を使用する場合は、サイトを作成する前にMicrosoft System Center Configuration Managerで構成手順を完了してください。詳細については、「Configuration ManagerとRemote PC Access Wake on LAN」を参照してください。

接続とリソースの作成および管理

重要：

Citrix Virtual Apps and Desktops™ 7 2006以降、現在の展開で以下のいずれかのテクノロジーを使用している場合、それらのテクノロジーを使用するサポート終了（EOL）項目を削除した後にのみ、現在のリリースに展開をアップグレードできます。

- パーソナル vDisk (PvD)
- AppDisks™
- パブリッククラウドホストの種類：Citrix CloudPlatform、Microsoft Azure Classic

詳細については、「PVD、AppDisks、およびサポートされていないホストの削除」を参照してください。

注：

Citrix Virtual Apps and Desktopsの展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

展開にパブリッククラウドホスト接続を使用する場合は、新規インストールまたは現在のリリースへのアップグレードを完了するためにHybrid Rights Licenseが必要です。

インストーラーがサポートされていないテクノロジーまたはHybrid Rights Licenseのないホスト接続を1つ以上検出すると、アップグレードが一時停止または停止し、説明メッセージが表示されま

す。インストーラーログには詳細が含まれています。詳しくは、「展開のアップグレード」を参照してください。

Hybrid Rights Licenseがホスト接続に与える影響

Hybrid Rights Licenseの資格に基づいて、パブリッククラウドホストへのホスト接続が影響を受けるシナリオは3つあります。

- パブリッククラウドホストへの新しいホスト接続を作成するには、Hybrid Rights Licenseが必要です。
- Hybrid Rights Licenseを所有しているがライセンスの有効期限が切れている場合、パブリッククラウドホストへの既存の接続は資格なしとマークされ、メンテナンスモードに入ります。既存のホスト接続がメンテナンスモードの場合、次の操作はできません。
  - ホスト接続の追加または変更
  - カタログの作成とイメージの更新
  - 電源操作を実行する
- 資格のないホスト接続が資格のあるものに変更されると、既存のホスティング接続が再度有効になります。

はじめに

サイトを作成するときに、ホスティングリソースへの最初の接続をオプションで作成できます。後で、その接続を変更したり、他の接続を作成したりできます。接続の構成には、サポートされているハイパーバイザーの中から接続タイプを選択すること、およびその接続のリソースから選択するストレージとネットワークが含まれます。

読み取り専用管理者は、接続とリソースの詳細を表示できます。接続とリソースの管理タスクを実行するには、フル管理者である必要があります。詳細については、「委任管理」を参照してください。

接続タイプに関する情報の入手先

サポートされている仮想化プラットフォームを使用して、Citrix Virtual AppsまたはCitrix Virtual Desktops環境でマシンをホストおよび管理できます。「システム要件」の記事にサポートされているタイプが記載されています。

詳細については、以下の情報源を参照してください。

- **XenServer (旧称は Citrix Hypervisor™):**

  - XenServer仮想化環境。
  - XenServer®ドキュメント。

- **ニュータニックス アクロポリス:**
  - Nutanix仮想化環境。
  - Nutanixドキュメント。

- **VMware (ヴイエムウェア):**
  - VMware仮想化環境。
  - VMware製品ドキュメント。

- **Microsoft ハイパーV:**
  - Microsoft System Center Virtual Machine Manager 仮想化環境の記事。
  - Microsoft ドキュメント。

- **パブリッククラウドホスト接続（AWS、Google Cloud、Microsoft Azure、Nutanix Cloudおよびパートナーソリューション、VMware Cloudおよびパートナーソリューション）：** パブリッククラウドホストに関する情報については、「リソースタイプのセットアップ」を参照してください。

> **注:**
>
> 情報源はCitrix DaaS™ドキュメントを参照するよう指示しています。Citrix DaaS製品のパブリッククラウドホストに精通している場合でも、オンプレミスバージョンにはいくつかの違いがあります。オンプレミスのVirtual Apps and Desktopsでは、管理インターフェイスはWeb Studioとして知られています。サービスへの更新は、約4週間ごとに展開されます。そのため、サービスで利用可能な特定の機能がオンプレミスバージョンでは利用できない場合があります。

ホストストレージ

サポートされているハイパーバイザーによって管理されている場合、ストレージ製品はサポートされます。Citrixサポートは、これらのストレージ製品ベンダーが問題のトラブルシューティングと解決を支援し、必要に応じてナレッジセンターにそれらの問題を文書化します。

マシンをプロビジョニングする際、データはタイプ別に分類されます。

- マスターイメージを含むオペレーティングシステム（OS）データ。
- 一時データ。このデータには、MCSプロビジョニングマシンに書き込まれるすべての非永続データ、Windowsページファイル、ユーザープロファイルデータ、およびShareFileと同期されるすべてのデータが含まれます。このデータは、マシンが再起動するたびに破棄されます。

各データタイプに個別のストレージを提供することで、各ストレージデバイスの負荷を軽減し、パフォーマンスを向上させ、ホストの利用可能なリソースを最大限に活用できます。また、異なるデータタイプに適切なストレージを使用できるようになります。一部のデータでは、永続性と回復性が他のデータよりも重要です。

ストレージは共有（中央に配置され、どのホストからも独立しており、すべてのホストで使用される）することも、ハイパーバイザーにローカルに配置することもできます。たとえば、中央共有ストレージは、1つ以上のWindows Server 2012クラスター化ストレージボリューム（接続ストレージの有無にかかわらず）、またはストレージベンダーのアプライアンスである場合があります。中央ストレージは、ハイパーバイザーストレージ制御パスやパートナープラグインを介した直接アクセスなど、独自の最適化を提供する可能性もあります。

一時データをローカルに保存することで、共有ストレージにアクセスするためにネットワークを介する必要がなくなります。また、共有ストレージデバイスの負荷も軽減されます。共有ストレージはより高価になる可能性があるため、データをローカルに保存することで費用を削減できます。これらの利点は、ハイパーバイザーサーバー上の十分なストレージの可用性と比較検討する必要があります。

接続を作成する際、ハイパーバイザー間で共有されるストレージ、またはハイパーバイザーにローカルなストレージの2つのストレージ管理方法のいずれかを選択します。

1つ以上のXenServerホストで一時データストレージにローカルストレージを使用する場合、プール内の各ストレージの場所に一意の名前があることを確認してください。（XenCenter®で名前を変更するには、ストレージを右クリックして名前プロパティを編集します。）

ハイパーバイザーで共有されるストレージ

ハイパーバイザーによって共有されるストレージ方式は、長期的な永続性が必要なデータを中央に保存し、一元化されたバックアップと管理を提供します。そのストレージにはOSディスクが格納されます。

この方法を選択すると、一時的なマシンデータにローカルストレージ（同じハイパーバイザープール内のサーバー上）を使用するかどうかを選択できます。この方法は、共有ストレージ内のデータほど永続性や回復性を必要としません。これは*一時データキャッシュ*と呼ばれます。ローカルディスクは、メインOSストレージへのトラフィックを削減するのに役立ちます。このディスクは、マシンが再起動するたびにクリアされます。ディスクはライトスルーメモリキャッシュを介し

てアクセスされます。一時データにローカルストレージを使用する場合、プロビジョニングされたVDAは特定のハイパーバイザーホストに紐付けられます。そのホストが故障すると、VMは起動できません。

例外: Microsoft System Center Virtual Machine Managerでは、クラスター共有ボリューム（CSV）を使用している場合、ローカルストレージ上の一時データキャッシュディスクは許可されません。

一時データをローカルに保存するための接続を作成し、各VMのキャッシュディスクサイズとメモリサイズの非デフォルト値を有効にして構成します。デフォルト値は接続タイプに合わせて調整されており、ほとんどのケースで十分です。詳細については、「マシンカタログの作成」を参照してください。

ハイパーバイザーは、ディスクイメージのローカルでの読み取りキャッシュを介して最適化テクノロジーを提供することもできます。たとえば、XenServerはIntelliCache™を提供しており、これにより中央ストレージへのネットワークトラフィックが削減されます。

ハイパーバイザーのローカルストレージ

ハイパーバイザーにローカルなストレージ方式では、データをハイパーバイザーにローカルに保存します。この方式では、マスターイメージやその他のOSデータがサイト内のハイパーバイザーに転送されます。このプロセスは、最初のマシン作成時と将来のイメージ更新時に発生します。このプロセスにより、管理ネットワークでかなりのトラフィックが発生します。イメージ転送には時間がかかり、イメージは各ホストで異なるタイミングで利用可能になります。

接続とリソースを作成する

サイトを作成する際に、最初の接続をオプションで作成できます。サイト作成ウィザードには、以下のセクションで説明されている接続関連のページが含まれています。

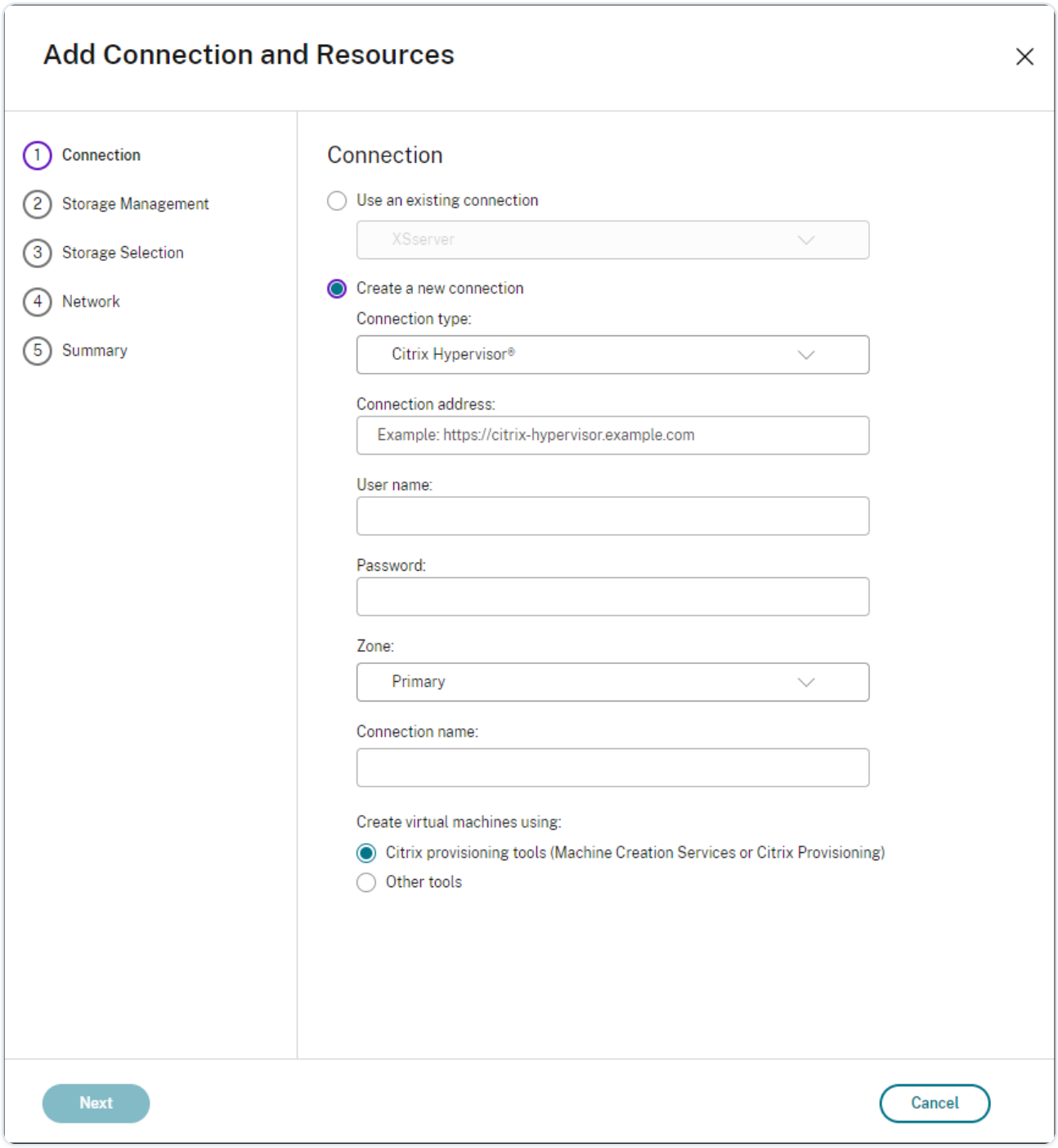
サイトの作成後に接続を作成する場合は、手順1から開始します。

> **重要:**
>
> 接続を作成する前に、ホストリソース（ストレージとネットワーク）が利用可能である必要があります。

1. Web Studioにサインインします。
2. 左側のペインで**ホスティング**を選択します。

3. アクションバーで**接続とリソースの追加**を選択します。
4. ウィザードは以下のページを案内します（特定のページコンテンツは選択した接続タイプによって異なります）。各ページを完了したら、**概要**ページに到達するまで**次へ**をクリックします。

接続

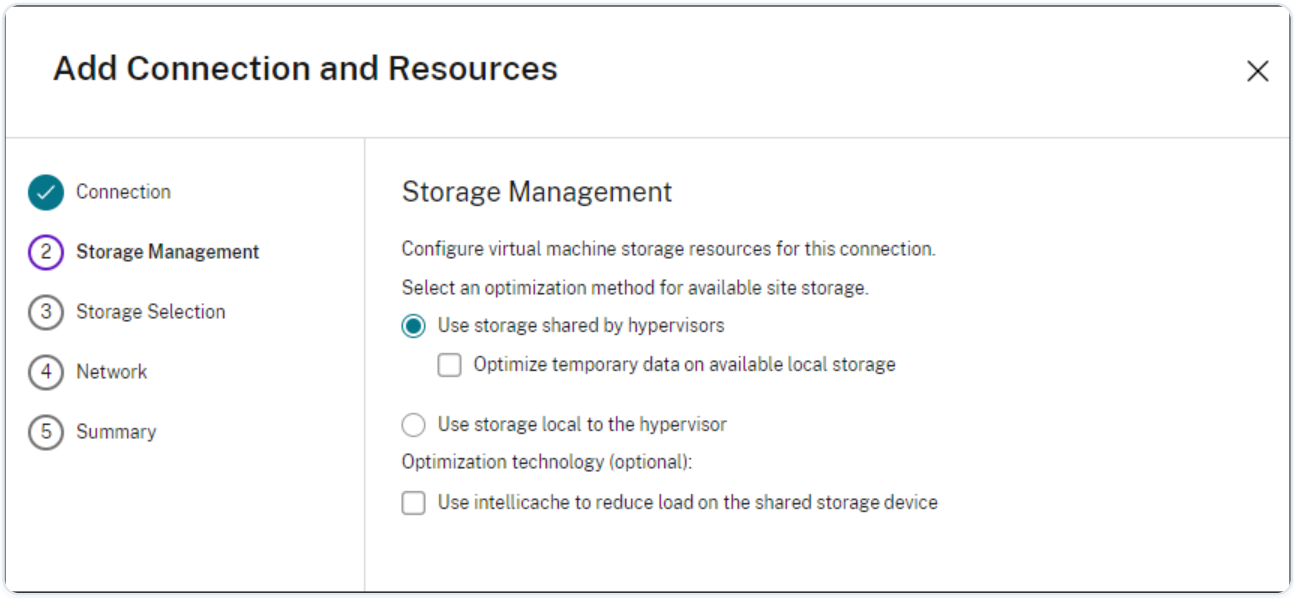


「**接続**」ページで：

- 接続を作成するには、**新しい接続の作成**を選択します。既存の接続と同じホスト構成に基づいて接続を作成するには、**既存の接続を使用**を選択し、関連する接続を選択します。

- **接続の種類**フィールドで、使用しているハイパーバイザーを選択します。パブリッククラウドホスト接続は、ハイブリッド権限ライセンスを使用している場合にのみドロップダウンリストに表示されます。または、PowerShellコマンド`Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false/trueを使用して、以下を取得できます。
  - サードパーティ製プラグインを含む、Citrixがサポートするすべてのハイパーバイザープラグインのリスト。
  - ハイパーバイザープラグインの可用性。可用性ステータスが**false**の場合、ハイパーバイザープラグインが正しくインストールされていないか、ハイブリッド権限ライセンスが付与されていない可能性があります。
- 接続アドレスと資格情報フィールドは、選択した接続タイプによって異なります。要求された情報を入力してください。
- 接続名を入力します。この名前はWeb Studioに表示されます。
- 仮想マシンの作成に使用するツールを選択します: Web Studioツール (Machine Creation Services™やCitrix Provisioningなど) またはその他のツール。

ストレージ管理



ストレージ管理の種類と方法については、「ホストストレージ」を参照してください。

Hyper-V または VMware ホストへの接続を構成している場合は、クラスター名を参照して選択します。その他の接続タイプでは、クラスター名は要求されません。

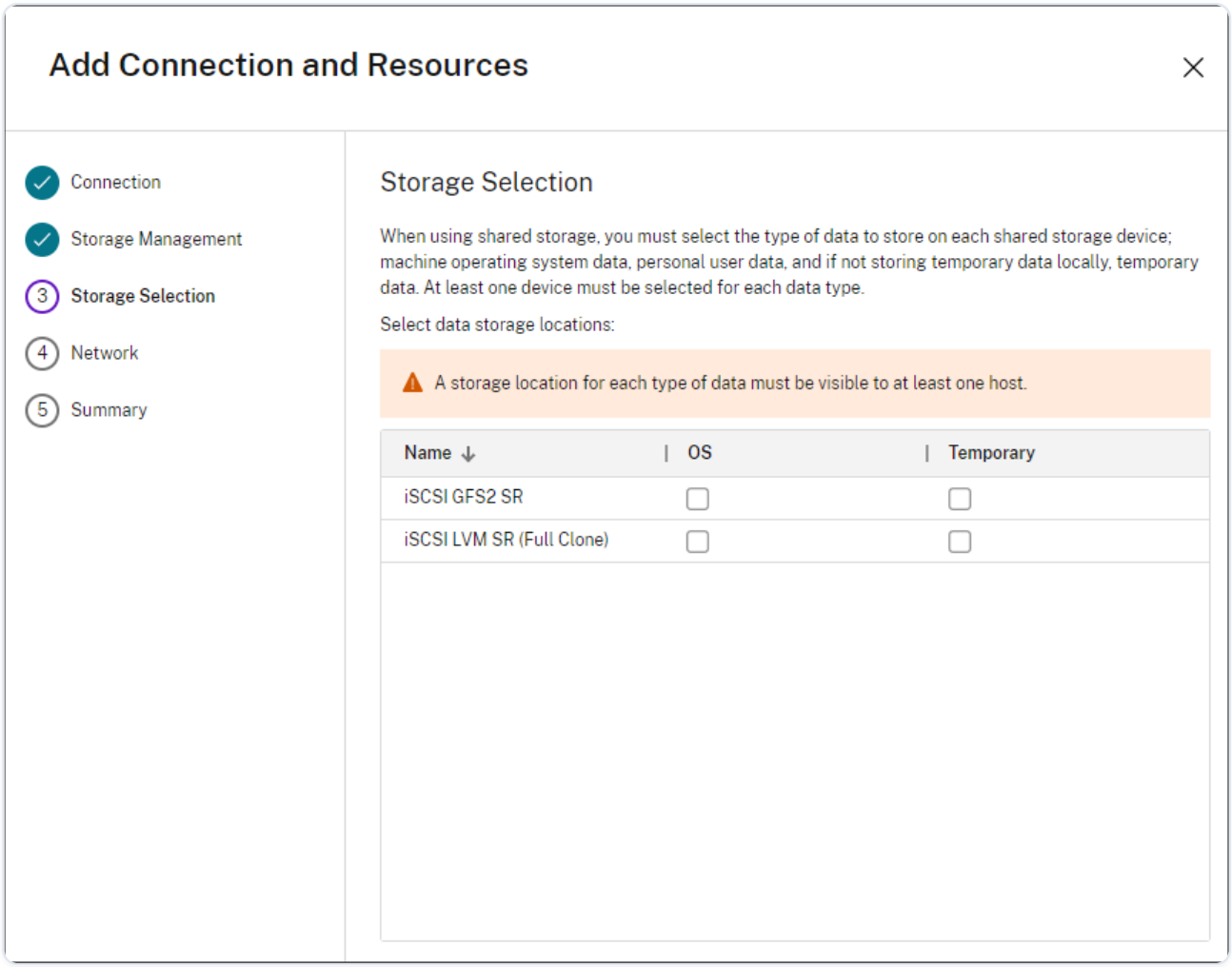
ストレージ管理方法を選択します: ハイパーバイザー間で共有されるストレージ、またはハイパーバイザーにローカルなストレージ。

- ハイパーバイザー間で共有されるストレージを選択した場合、利用可能なローカルストレージに一時データを保持するかどうかを指定します。(この接続を使用するマシンカタログで、デフォルト以外のテンポラリストレージサイズを指定できます。) **例外:** クラスター共有ボリューム (CSV) を使用する場合、Microsoft System Center Virtual Machine Managerはローカルストレージ上の一時データキャッシュディスクを許可しません。Web Studioでそのストレージ管理設定を構成すると失敗します。

XenServerプールで共有ストレージを使用する場合、共有ストレージデバイスの負荷を軽減するためにIntelliCacheを使用するかどうかを指定します。「XenServer接続にIntelliCacheを使用する」を参照してください。

> **注:**
>
> XenServer、VMware、およびSCVMM仮想化環境では、OSディスクと同じストレージ場所にライトバックキャッシュ (WBC) ディスクを配置できます。この場合、**利用可能なローカルストレージ上の一時データを最適化する**は選択しないでください。

ストレージの選択



ストレージの選択の詳細については、「ホストストレージ」を参照してください。

利用可能な各データタイプに対して、少なくとも1つのホストストレージデバイスを選択します。前のページで選択したストレージ管理方法によって、このページで選択できるデータタイプが決まります。ウィザードの次のページに進む前に、サポートされている各データタイプに対して少なくとも1つのストレージデバイスを選択してください。

> **注:**
>
> XenServer、VMware、SCVMM仮想化環境では、利用可能なOSストレージリストと利用可能な一時ストレージリストを同じに構成した場合、MCSはライトバックキャッシュ (WBC) ディスクをOSディスクと同じストレージの場所に配置します。

> **ストレージの選択**ページの最下部には、前のページでハイパーバイザーによって共有されるストレージを選択し、**利用可能なローカルストレージで一時データを最適化**を有効にした場

> 合、追加の構成オプションが含まれています。一時データに使用するローカルストレージデバイスを選択できます。

現在選択されているストレージデバイスの数が表示されます (前の図では、「1つのストレージデバイスが選択されています」)。そのエントリにマウスカーソルを合わせると、選択されたデバイス名が表示されます。

1. **選択**をクリックして、使用するストレージデバイスを変更します。
2. **ストレージの選択**ダイアログボックスで、ストレージデバイスのチェックボックスをオンまたはオフにして、**OK**をクリックします。

ネットワーク

ネットワークページで、リソースの名前を入力します。この名前は、Web Studioに表示され、接続に関連付けられたストレージとネットワークの組み合わせを識別します。

VMが使用するネットワークを1つ以上選択します。

概要

概要ページで、選択内容を確認します。完了したら、**完了**をクリックします。

注意: 一時データをローカルに保存すると、この接続を使用するマシンを含むマシンカタログを作成するときに、一時データストレージの非デフォルト値を構成できます。マシンカタログの作成を参照してください。

接続設定の編集

接続の名前変更や接続の作成には、この手順を使用しないでください。これらの接続は異なる操作です。アドレスは、現在のホストマシンに新しいアドレスがある場合にのみ変更してください。別のアドレスを別のマシンに入力すると、接続のマシンカタログが破損します。

このリソースにアクセスするマシンカタログは、適切なGPU固有のマスターイメージを使用する必要があるため、接続の**GPU**設定は変更できません。接続を作成してください。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**接続の編集**を選択します。
4. 接続を編集する際に利用できる設定のガイダンスに従ってください。
5. 完了したら、**適用**をクリックして変更を適用しウィンドウを開いたままにするか、**保存**をクリックして変更を適用しウィンドウを閉じます。

接続プロパティページ:

- 接続アドレスと資格情報を変更するには、**設定の編集...**を選択し、新しい情報を入力します。
- XenServer接続の高可用性サーバーを指定するには、**サーバーの編集...**を選択し、サーバーを選択します。Citrixでは、プールマスターが失敗した場合にXenServerとの通信を可能にするため、プール内のすべてのサーバーを選択することをお勧めします。

> **注:**
>
> HTTPSを使用しており、高可用性サーバーを構成したい場合は、プール内のすべてのサーバーにワイルドカード証明書をインストールしないでください。各サーバーに個別の証明書が必要です。

詳細ページ:

- Remote PC Accessで使用されるMicrosoft System Center Configuration Manager (ConfMgr) Wake on LAN接続タイプの場合、**ConfMgr Wake Proxy**、マジックパケット、およびパケット送信情報を入力します。
- スロットリングしきい値設定を使用すると、接続で許可される電源アクションの最大数を指定できます。これらの設定は、電源管理設定によって同時に起動できるマシンの数が多すぎたり少なすぎたりする場合に役立ちます。各接続タイプには、ほとんどのケースに適した特定のデフォルト値があり、変更してはなりません。
- **同時アクション (すべてのタイプ)** 設定では、この接続で同時に発生できる最大絶対数と、この接続を使用するすべてのマシンの最大パーセンテージの2つの値を指定します。絶対値とパーセンテージ値の両方を指定する必要があります。実際に適用される制限は、これらの値の小さい方です。

  たとえば、34台のマシンがある展開で、**同時アクション (すべてのタイプ)** が絶対値10、パーセンテージ値10に設定されている場合、実際に適用される制限は3です（つまり、34の10パーセントを最も近い整数に丸めたもので、絶対値10台のマシンよりも小さい値です）。
- 「**1分あたりの最大新規アクション数**」は絶対数です。パーセンテージ値はありません。
- 「**接続オプション**」フィールドには、Citrixサポート担当者の指示または明示的なドキュメントの指示がある場合にのみ情報を入力してください。

共有テナントページ:

この接続のサブスクリプションとAzure Compute Galleryを共有するテナントとサブスクリプションを追加します。これにより、カタログの作成または更新時に、それらのテナントとサブスクリプションから共有イメージを選択できます。

- この接続に関連付けられているアプリケーションの**アプリケーションID**と**アプリケーションシークレット**を入力します。この情報を使用して、Azureに認証できます。セキュリティを確保するために、定期的にキーを変更することをお勧めします。
- 共有テナントとサブスクリプションを指定します。最大8つの共有テナントを追加できます。各テナントにつき、最大8つのサブスクリプションを追加できます。
- 完了したら、**保存**と**適用**をクリックします。

「**接続オプション**」フィールドには、Citrixサポート担当者の指示がある場合にのみ情報を入力してください。

ネットワークの編集

接続のネットワークを変更できます。次の手順を実行します。

1. **ホスティング**に移動します。
2. 接続下のターゲットリソースを選択し、アクションバーで**ネットワークの編集**を選択します。
3. 仮想マシンが使用するネットワークを1つ以上選択します。
4. **保存**をクリックして変更を保存し、終了します。

接続のメンテナンスモードをオンまたはオフにする

接続のメンテナンスモードをオンにすると、その接続に格納されているマシンに新しい電源操作が影響を与えるのを防ぎます。ユーザーは、メンテナンスモードのマシンに接続できません。ユーザーがすでに接続している場合、メンテナンスモードはログオフ時に有効になります。

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. 接続を選択します。メンテナンスモードをオンにするには、アクションバーで を選択します。メンテナンスモードをオフにするには、 を選択します。

個々のマシンに対してメンテナンスモードをオンまたはオフにすることもできます。また、マシンカタログまたはデリバリーグループ内のマシンに対してメンテナンスモードをオンまたはオフにすることもできます。

接続を削除する

接続を削除すると、多数のマシンが削除され、データが失われる可能性があります。影響を受けるマシン上のユーザーデータがバックアップされているか、不要であることを確認してください。

接続を削除する前に、以下を確認してください。

- 接続に格納されているマシンからすべてのユーザーがログオフしていること。
- 切断されたユーザーセッションが実行されていないこと。
- プールされたマシンと専用マシンのメンテナンスモードがオンになっていること。
- 接続で使用されているマシンカタログ内のすべてのマシンは電源がオフになります。

カタログによって参照されている接続を削除すると、そのマシンカタログは使用できなくなります。この接続がカタログによって参照されている場合、カタログを削除するオプションがあります。カタログを削除する前に、他の接続で使用されていないことを確認してください。

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. 接続を選択し、アクションバーで**接続の削除**を選択します。
4. この接続にマシンが格納されている場合、マシンを削除するかどうかを確認するメッセージが表示されます。削除する場合は、関連付けられているActive Directoryコンピューターアカウントをどうするかを指定します。

接続の名前変更またはテスト

1. Web Studioにサインインします。
2. 左側のペインで**ホスト**を選択します。
3. 接続を選択し、アクションバーで**接続の名前変更**または**接続のテスト**を選択します。

接続上のマシンの詳細を表示

1. Web Studioにサインインします。
2. 左側のペインで**ホスト**を選択します。
3. 接続を選択し、アクションバーで**マシンの表示**を選択します。

上部のペインには、接続を介してアクセスされるマシンが一覧表示されます。マシンを選択すると、下部のペインにその詳細が表示されます。開いているセッションのセッション詳細も表示されます。

検索機能を使用して、マシンをすばやく見つけます。ウィンドウ上部のリストから保存された検索を選択するか、検索を作成します。マシン名の全部または一部を入力して検索するか、高度な検索に使用する式を作成できます。式を作成するには、**展開**をクリックし、プロパティと演算子のリストから選択します。

接続上のマシンを管理する

1. Web Studioにサインインします。
2. 左側のペインで**ホスト**を選択します。
3. 接続を選択し、**アクション**ペインで**マシンを表示**を選択します。
4. アクションバーで次のいずれかを選択します。マシンの状態と接続ホストの種類によっては、一部のアクションが利用できない場合があります。

アクション	説明
起動	電源がオフまたは一時停止されている場合にマシンを起動します。
一時停止	マシンをシャットダウンせずに一時停止し、マシンの一覧を更新します。
シャットダウン	オペレーティングシステムにシャットダウンを要求します。
強制シャットダウン	マシンを強制的に電源オフにし、マシンリストを更新します。
再起動	オペレーティングシステムにシャットダウンを要求し、その後マシンを再起動します。オペレーティングシステムがこれに応じられない場合、デスクトップは現在の状態のままになります。
メンテナンスモードを有効にする	マシンへの接続を一時的に停止します。この状態のマシンにはユーザーは接続できません。ユーザーが接続している場合、メンテナンスモードはログオフ時に有効になります。（上記のとおり、接続を介してアクセスされるすべてのマシンに対してメンテナンスモードをオン/オフにすることもできます。）

アクション	説明
デリバリーグループから削除	マシンをデリバリーグループから削除しても、そのデリバリーグループが使用するマシンカタログからは削除されません。マシンは、ユーザーが接続していない場合にのみ削除できます。マシンを削除している間、ユーザーが一時的に接続できないようにするには、メンテナンスモードをオンにします。
削除	マシンを削除すると、ユーザーはそのマシンにアクセスできなくなり、マシンはマシンカタログから削除されます。マシンを削除する前に、すべてのユーザーデータがバックアップされているか、不要であることを確認してください。マシンは、ユーザーが接続していない場合にのみ削除できます。マシンを削除している間、ユーザーが一時的に接続できないようにするには、メンテナンスモードをオンにします。

マシンのシャットダウンを伴う操作の場合、マシンが10分以内にシャットダウンしないと、電源がオフになります。シャットダウン中にWindowsが更新プログラムのインストールを試みると、更新が完了する前にマシンの電源がオフになるリスクがあります。

ストレージの編集

接続を使用するVMのオペレーティングシステムデータと一時データを保存するために使用されるサーバーのステータスを表示できます。また、各データタイプのストレージに使用するサーバーを指定することもできます。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**ストレージの編集**を選択します。
4. 左側のペインで、データタイプ（オペレーティングシステムまたは一時）を選択します。
5. 選択したデータタイプについて、1つ以上のストレージデバイスのチェックボックスをオンまたはオフにします。
6. **OK**をクリックします。

リスト内の各ストレージデバイスには、その名前とストレージステータスが含まれています。有効なストレージステータス値は次のとおりです。

- **使用中:** ストレージはマシンの作成に使用されています。
- **廃止済み:** ストレージは既存のマシンにのみ使用されています。このストレージには新しいマシンは追加されません。
- **未使用:** ストレージはマシンの作成に使用されていません。

現在**使用中**のデバイスのチェックボックスをオフにすると、そのステータスは**廃止済み**に変わります。既存のマシンはそのストレージデバイスを引き続き使用し（データを書き込むこともできます）、そのため、マシンの作成に使用されなくなった後でも、その場所がいっぱいになる可能性があります。

リソースの削除、名前の変更、またはテスト

1. Web Studioにサインインします。
2. 左側のペインで**ホスティング**を選択します。
3. リソースを選択し、アクションバーで適切なエントリを選択します: **リソースの削除**、**リソースの名前変更**、または**リソースのテスト**。

孤立したAzureリソースの検出

孤立したリソースは、システム内に存在する使用されていないリソースであり、不要な費用につながる可能性があります。

この機能を使用すると、Citrix Virtual Apps and Desktopsサイトのホストにある孤立したAzureリソースを検出できます。

Web Studioで次の手順を実行します。

1. **管理**から、左側のペインで**ホスティング**を選択します。
2. 接続を選択し、アクションバーで**孤立したリソースの検出**を選択します。**孤立したリソースの検出**ダイアログボックスに、孤立したリソースのレポートが表示されます。
3. 孤立したリソースのレポートを表示するには、**レポートの表示**を選択します。

PowerShell を使用して、孤立した Azure リソースを検出することもできます。詳細については、「孤立したリソースのリストを取得する」を参照してください。

孤立したリソースの原因を理解し、その後の対処方法については、「Citrix を使用して孤立した Azure リソースを効率的に管理する」を参照してください。

接続タイマー

ポリシー設定を使用して、3つの接続タイマーを構成できます。

- **最大接続タイマー:** ユーザーデバイスと仮想デスクトップ間の途切れない接続の最大継続時間を決定します。**セッション接続タイマー**および**セッション接続タイマー間隔**ポリシー設定を使用します。
- **接続アイドルタイマー:** ユーザーからの入力がない場合に、仮想デスクトップへの途切れないユーザーデバイス接続が維持される期間を決定します。**セッションアイドルタイマー**および**セッションアイドルタイマー間隔**ポリシー設定を使用します。
- **切断タイマー:** 切断されロックされた仮想デスクトップが、セッションがログオフされるまでロックされたままになる期間を決定します。**切断セッションタイマー**および**切断セッションタイマー間隔**ポリシー設定を使用します。

これらの設定のいずれかを更新する場合は、展開全体で一貫性があることを確認してください。

詳細については、ポリシー設定のドキュメントを参照してください。

孤立したリソースのリストを取得する

MCS によって作成されたが、MCS によって追跡されなくなった孤立したリソースのリストを取得できます。これは現在、Azure 環境に適用されます。リストを取得するには、PowerShell コマンドを使用できます。接続を使用してフィルター処理できます。

> **注：**
>
> - プロビジョニングまたはイメージの更新が進行中の場合、PowerShell コマンドは拒否されます。
> - すべての Citrix タグがタグ付けされた顧客管理リソースは、孤立したリソースとして検出されます。ただし、そのリソースに値が true の別のタグ CitrixDetectIgnore を追加すると、孤立したリソースの検出中にそのリソースは無視されます。

制限事項

- 組み込みのフル管理者またはクラウド管理者ロールの管理者ユーザーのみが、PowerShellコマンドを実行して孤立したリソースのリストを取得できます。
- 孤立したリソースの誤認識を避けるため、孤立したリソースをフィルタリングしている間はVMの電源をオンにしないでください。

- 負荷が高い可能性がある場合、約2,000件のレコードが孤立していると表示されます。

孤立リソースのリストを表示するには：

1. **PowerShell**ウィンドウを開きます。
2. 次のコマンドを実行します。
   a. 接続UIDを取得します。接続UIDは、HypervisorConnectionUid属性の値です。

```
Get-ChildItem xdhyp:\connections | where { $_.PluginId -like
'Azure*' }"
```

   b. 孤立したリソースのリストを取得します。

```
get-provorphanedresource -HypervisorConnectionUid <connection uid>
```

サブスクリプションIDから孤立リソースのリストを表示するには：

1. **PowerShell**ウィンドウを開きます。
2. 次のコマンドを実行します。
   a. サブスクリプションIDを使用して接続UIDを見つけます。接続UIDは、HypervisorConnectionUid属性の値です。

```
Get-ChildItem xdhyp:\connections | where { $_.CustomProperties
-match '<subscriptionId>' }
```

   b. 孤立リソースのリストを取得します。

```
get-provorphanedresource -HypervisorConnectionUid <connection uid>
```

注:

削除する前にリソースを慎重に確認してください。

次のステップ

特定のホストタイプへの接続については、以下を参照してください。

- AWSへの接続
- XenServerへの接続
- Google Cloud環境への接続
- Microsoft Azureへの接続
- マイクロソフト システム センター バーチャル マシン マネージャー への接続
- Nutanixへの接続
- Nutanixクラウドおよびパートナーソリューションへの接続
- VMwareへの接続
- VMwareクラウドおよびパートナーソリューションへの接続

初期展開プロセス中の場合は、マシンカタログを作成します。

AWSへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明します。以下の情報は、AWSクラウド環境に固有の詳細を扱っています。

> **注:**
>
> AWSへの接続を作成する前に、まずAWSアカウントをリソースの場所として設定する必要があります。AWSクラウド環境を参照してください。

接続を作成する

Web Studioから接続を作成する場合：

- APIキーとシークレットキーの値を指定する必要があります。これらの値を含むキーファイルをAWSからエクスポートしてインポートできます。また、リージョン、アベイラビリティゾーン、VPC名、サブネットアドレス、ドメイン名、セキュリティグループ名、および資格情報も指定する必要があります。
- ルートAWSアカウントの資格情報ファイル（AWSコンソールから取得）は、標準のAWSユーザー向けにダウンロードされた資格情報ファイルと同じ形式ではありません。そのため、Citrix Virtual Apps and Desktops™管理では、このファイルを使用してAPIキーとシークレットキーのフィールドに入力することはできません。AWS Identity Access Management (IAM) 資格情報ファイルを使用していることを確認してください。

> **注:**
>
> 接続を作成した後、APIキーとシークレットキーの更新が失敗する場合があります。この問題を解決するには、プロキシサーバーまたはファイアウォールの制限を確認し、次のアドレスにアクセスできることを確認してください: `https://*.amazonaws.com`。

ホスト接続のデフォルト値

AWSクラウド環境でホスト接続を作成すると、次のデフォルト値が表示されます。

オプション	絶対	パーセンテージ
同時実行アクション（すべての種類）	125	100
1分あたりの新規アクションの最大数	125	

MCS は、デフォルトで最大 100 の同時プロビジョニング操作をサポートしています。

サービスエンドポイントURL

標準ゾーンサービスエンドポイントURL

MCS を使用すると、API キーと API シークレットを持つ新しい AWS 接続が追加されます。この情報と認証済みアカウントを使用して、MCS は AWS DescribeRegions EC2 API 呼び出しを使用して、サポートされているゾーンについて AWS にクエリを実行します。クエリは、汎用 EC2 サービスエンドポイント URL `https://ec2.amazonaws.com/` を使用して行われます。MCS を使用して、サポートされているゾーンのリストから接続するゾーンを選択します。優先される AWS サービスエンドポイント URL は、そのゾーンに対して自動的に選択されます。ただし、サービスエンドポイント URL を作成した後は、その URL を設定または変更することはできません。

IAM権限を定義する

このセクションの情報を使用して、AWS 上の Citrix Virtual Apps and Desktops の IAM 権限を定義します。Amazon の IAM サービスは、複数のユーザーを持つアカウントを許可しており、それらのユーザーはさらにグループに編成できます。これらのユーザーは、アカウントに関連する操作を実行する能力を制御するために、異なる権限を持つことができます。IAM 権限の詳細については、IAM JSON ポリシーリファレンス を参照してください。

新しいユーザーグループにIAM権限ポリシーを適用するには：

1. AWSマネジメントコンソールにログインし、ドロップダウンリストから**IAMサービス**を選択します。
2. **新しいユーザーグループの作成**を選択します。
3. 新しいユーザーグループの名前を入力し、**続行**を選択します。
4. 「**Permissions**」ページで、「**Custom Policy**」を選択します。「**Select**」を選択します。
5. 「**Permissions policy**」の名前を入力します。
6. 「**Policy Document**」セクションで、関連する権限を入力します。

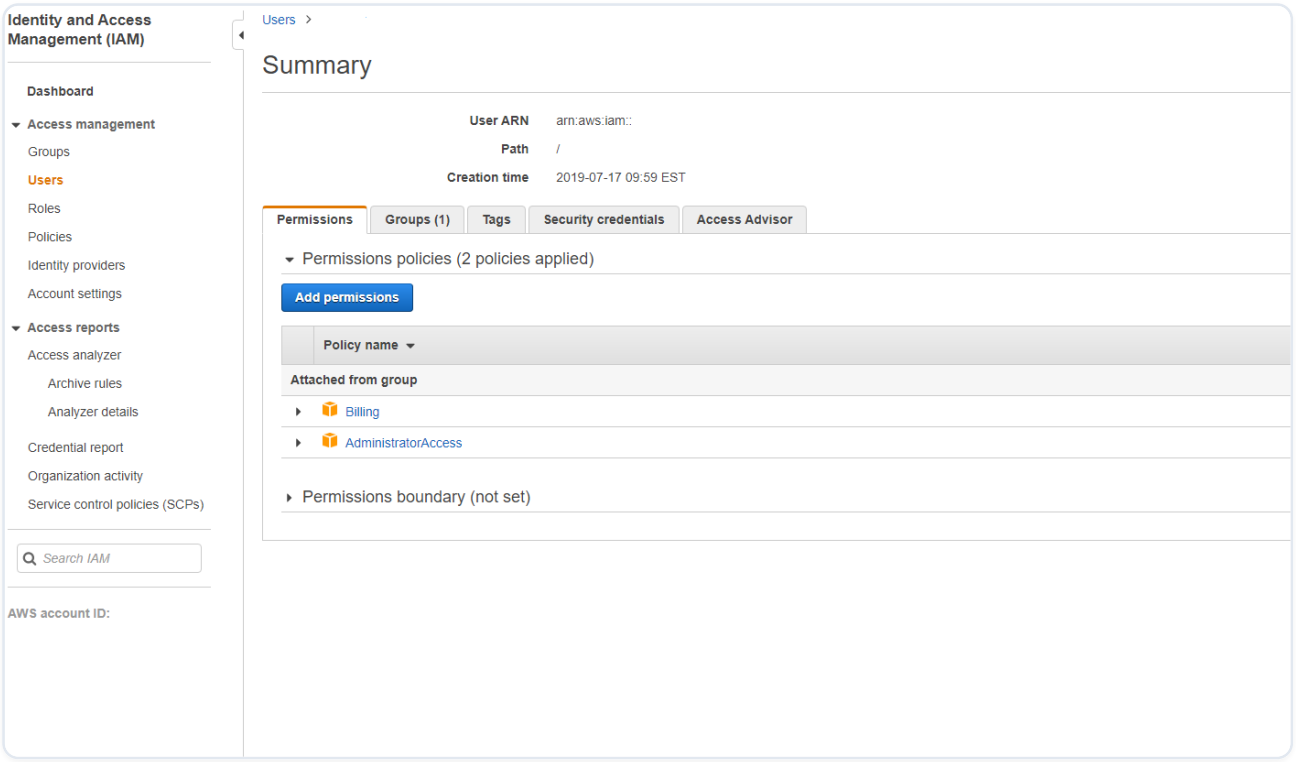
ポリシー情報を入力したら、**Continue** を選択してユーザーグループを完了します。グループ内のユーザーには、Citrix Virtual Apps and Desktops に必要なアクションのみを実行する権限が付与されます。

> **重要:**
>
> 前述の例で提供されているポリシーテキストを使用して、Citrix Virtual Apps and Desktops が AWS アカウント内でアクションを実行するために使用するアクションを、特定のリソースに制限することなくリストします。Citrix は、テスト目的でこの例を使用することをお勧めします。本番環境では、リソースにさらなる制限を追加することを選択できます。

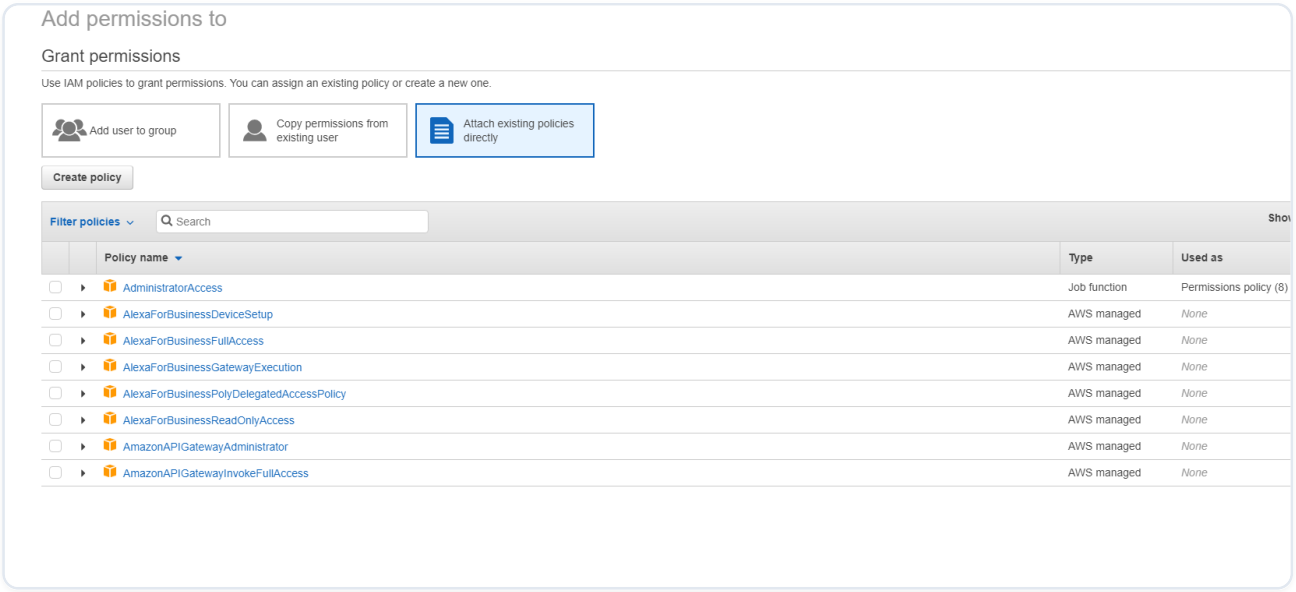
IAM権限を設定する

AWS Management Console の「**IAM**」セクションで権限を設定します。

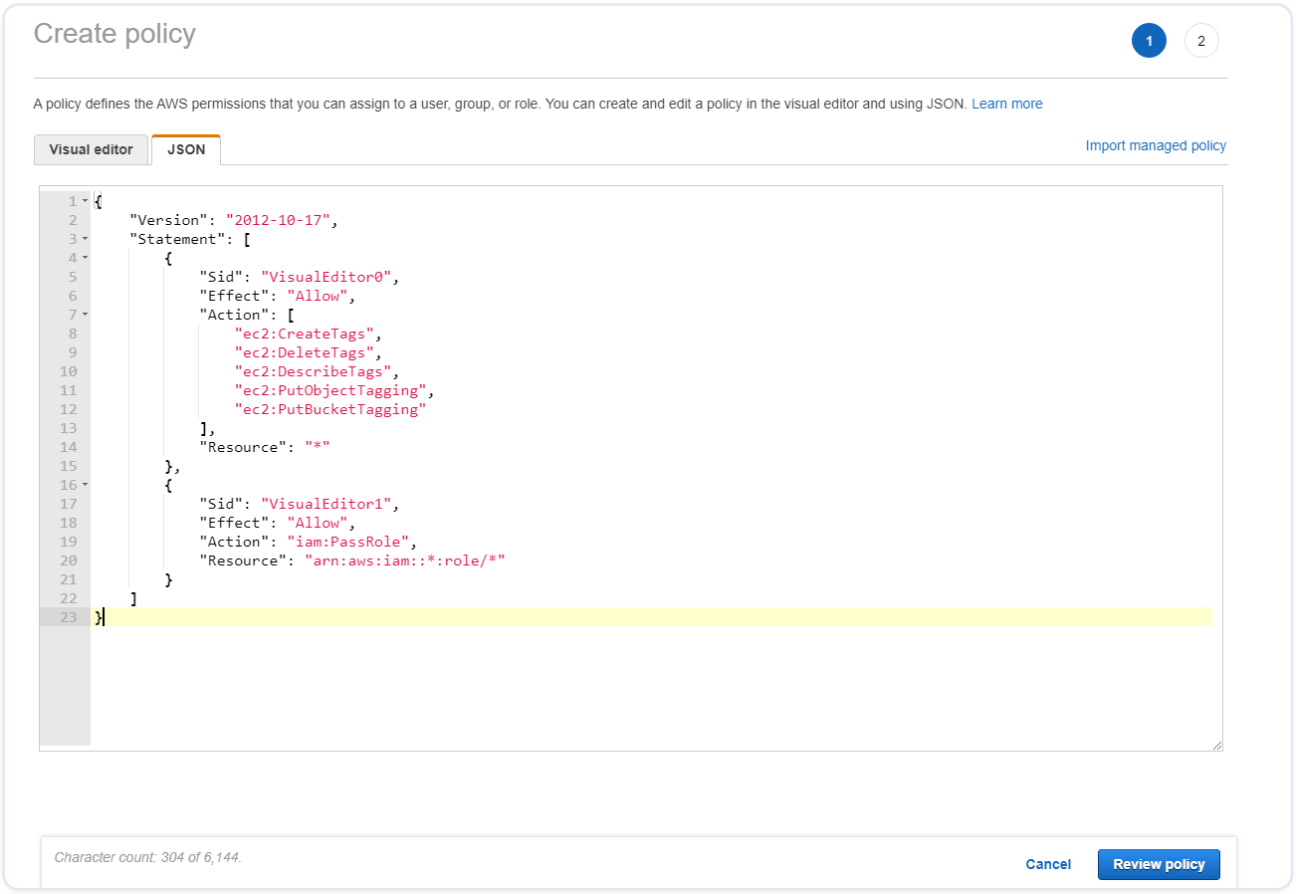
1. 「**Summary**」パネルで、「**Permissions**」タブを選択します。
2. 「**Add permissions**」を選択します。



「**Add Permissions to**」画面で、権限を付与します。



「**JSON**」タブで、以下を例として使用します。



ヒント:

記載されているJSONの例には、お使いの環境に必要なすべての権限が含まれていない場合があります。詳細については、How to Define Identity Access Management Permissions Running Citrix Virtual Apps and Desktops on AWSを参照してください。

必要なAWS権限

このセクションには、AWS権限の完全なリストが含まれています。

注:

iam:PassRole 権限は、**role_based_auth** の場合にのみ必要です。

ホスト接続の作成

AWSからの情報を使用して、新しいホスト接続が追加されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",,
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs"
                "ec2:DescribeRegions",
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

VM の電源管理

VMの電源がオンまたはオフになります。

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

```
                "ec2:DescribeInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:RebootInstances",
                "ec2:DescribeInstanceStatus"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

仮想マシンの作成、更新、または削除

AWSインスタンスとしてプロビジョニングされたVMを使用して、マシンカタログが作成、更新、または削除されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
```

```
                "ec2:AuthorizeSecurityGroupIngress",

                "ec2:CreateImage",

                "ec2:CreateLaunchTemplate",

                "ec2:CreateSecurityGroup",

                "ec2:CreateTags",

                "ec2:CreateVolume",

                "ec2:DeleteVolume",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",
```

```
                "ec2:DescribeSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",
                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
            ],
            "Effect": "Allow",
```

```
            "Resource": "*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

注:

セキュリティグループに関連するEC2セクションは、カタログ作成中に準備VM用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが完了すると、これらの権限は不要になります。

ディスクの直接アップロードとダウンロード

直接ディスクアップロードは、マシンカタログプロビジョニングにおけるボリュームワーカーの要件を排除し、代わりにAWSが提供するパブリックAPIを使用します。この機能により、追加のストレージアカウントに関連するコストと、ボリュームワーカー操作の維持に関する複雑さが軽減されます。

> **注:**
>
> ボリュームワーカーのサポートは非推奨になりました。
>
> 以下の権限をポリシーに追加する必要があります。

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

> **重要:**
>
> - ボリュームワーカーAMIやボリュームワーカーVMなどのボリュームワーカー操作なしで、既存のマシンカタログにVMを追加できます。
> - 以前にボリュームワーカーを使用していた既存のカタログを削除すると、ボリュームワーカー関連を含むすべてのアーティファクトが削除されます。

作成されたボリュームのEBS暗号化

AMIが暗号化されている場合、またはEBSがすべての新しいボリュームを暗号化するように構成されている場合、EBSは新しく作成されたボリュームを自動的に暗号化できます。ただし、この機能を実装するには、IAMポリシーに次の権限を含める必要があります。

```
{
     "Version": "2012-10-17",
     "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        }
    ]
}
```

注:

権限は、ユーザーの裁量でリソースと条件ブロックを含めることにより、特定のキーに制限できます。例：**条件付きKMS権限**：

```
{
     "Version": "2012-10-17",
     "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-
a123-456d-a12b-a123b4cd56ef"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
```

```
        }

    ]

}
```

次のキーポリシーステートメントは、アカウントがIAMポリシーを使用してKMSキーに対するすべてのアクション（kms:*）の権限を委任できるようにするために必要な、KMSキーのデフォルトのキーポリシー全体です。

```
{

"Sid": "Enable IAM policies",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::111122223333:root"

},

"Action": "kms:",

"Resource": ""

}
```

詳細については、「AWS Key Management Service 公式ドキュメント」を参照してください。

IAMロールベース認証

ロールベース認証をサポートするために、次の権限が追加されます。

```
{

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

     "Statement": [

        {
```

```
            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]

}
```

最小限のIAM権限ポリシー

次のJSONは、現在サポートされているすべての機能に使用できます。このポリシーを使用して、ホスト接続の作成、VMの作成、更新、削除、および電源管理を行うことができます。 このポリシーは、IAM権限の定義セクションで説明されているようにユーザーに適用することも、**role_based_auth**セキュリティキーとシークレットキーを使用してロールベース認証を使用することもできます。

重要:

role_based_authを使用するには、まずサイト内のすべてのDelivery Controllerで目的のIAMロールを構成します。Web Studioを使用して、ホスティング接続を追加し、認証キーとシークレットにrole_based_authを指定します。これらの設定を持つホスティング接続は、ロールベース認証を使用します。

```
{

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

    "Statement": [

        {

            "Action": [

                "ec2:AttachVolume",
```

```
                "ec2:AssociateIamInstanceProfile",

                "ec2:AuthorizeSecurityGroupEgress",

                "ec2:AuthorizeSecurityGroupIngress",

                "ec2:CreateImage",

                "ec2:CreateLaunchTemplate",

                "ec2:CreateNetworkInterface",

                "ec2:CreateTags",

                "ec2:CreateVolume",

                "ec2:DeleteLaunchTemplate",

                "ec2:DeleteNetworkInterface",

                "ec2:DeleteSecurityGroup",

                "ec2:DeleteSnapshot",

                "ec2:DeleteTags",

                "ec2:DeleteVolume",

                "ec2:DeregisterImage",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeInstanceStatus",
```

```
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",
                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
```

```
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:GenerateDataKey",
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
        }
    ]
```

```
}
```

注:

- SecurityGroupsに関連するEC2セクションは、カタログ作成時に準備VM用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが完了すると、これらの権限は不要になります。
- KMSセクションは、EBSボリューム暗号化を使用する場合にのみ必要です。
- iam:PassRole 権限セクションは、**role_based_auth** の場合にのみ必要です。
- 要件と環境に基づいて、フルアクセスではなく特定のリソースレベルの権限を追加できます。詳細については、AWSドキュメントのDemystifying EC2 Resource-Level Permissions および Access management for AWS resources を参照してください。

ホスト接続の権限を検証する

ホスト接続で権限を検証して、MCSマシンカタログの作成と管理に関連するタスクを実行できます。この実装は、VMの作成、削除、更新、VMの電源管理、EBS暗号化など、さまざまなシナリオで必要な不足している権限を事前に特定するのに役立ち、重要な時期にブロックされるのを回避できます。

PowerShellコマンド `Test-HypHypervisorConnection` を使用して、ホスト接続の権限を検証できます。コマンドの結果はリストとしてキャプチャされ、リスト内の各項目は3つのセクションに分かれています。

- カテゴリ: ユーザーがMCSマシンカタログを作成および管理するために実行できるアクションまたはタスク。
- 修正措置: 管理者がユーザーの不足している権限の不一致を解決するために実行する必要がある手順。
- 不足している権限: カテゴリの不足している権限のリスト。

権限を検証するには、次の手順を実行します。

1. AWSへのホスト接続を作成します。
2. Delivery Controller™ホストからPowerShellウィンドウを開きます。
3. Citrix固有のPowerShellモジュールをロードするために `asnp citrix*` を実行します。

4. 権限を検索するために必要な権限があるかどうかを確認するには、次のコマンドを実行します。

```
Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\AWSCon"
```

5. 権限を検索するために必要な不足している権限を追加した後、次のカテゴリの権限があるかどうかを確認するために、次のコマンドを実行します。

   - 作成、更新、削除
   - 電源管理
   - EBS暗号化

```
Test-HypHypervisorConnection -LiteralPath "XDHyp:
\Connections\AWSCon" [-SecurePassword -Password] "password" -UserName
"" -CustomProperties ""
```

権限の追加について詳しくは、「IAM 権限の設定」を参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- AWS 固有の情報については、「AWS カタログの作成」を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

XenServer® への接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明します。以下の情報は、XenServer仮想化環境に固有の詳細を扱っています。

> **注:**
>
> XenServerへの接続を作成する前に、まずXenServerアカウントをリソースの場所として設定を完了する必要があります。「XenServer仮想化環境」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/install-prepare/xenserver.html)を参照してください。

XenServerへの接続を作成する

XenServer（旧Citrix Hypervisor™）への接続を作成する際は、VM Power Admin以上のユーザーの資格情報を指定する必要があります。

Citrixでは、XenServerとの通信を保護するためにHTTPSを使用することを推奨しています。HTTPSを使用するには、XenServerにインストールされているデフォルトの SSL証明書を置き換える必要があります。

XenServerサーバーで高可用性が有効になっている場合、高可用性を構成できます。Citrix Virtual Apps and Desktopsのバージョン2507 LTSRより前のバージョンでは、プール内のすべてのサーバーにワイルドカード証明書をインストールすることはできません。各サーバーに個別の証明書が必要です。

XenServerがvGPUをサポートしている場合、GPUの種類とグループを選択するか、パススルーすることができます。表示は、選択に専用のGPUリソースがあるかどうかを示します。

一時的なデータストレージとして1つ以上のXenServerホストでローカルストレージを使用する場合、プール内の各ストレージの場所に一意の名前があることを確認してください。（XenCenter®で名前を変更するには、ストレージを右クリックして名前プロパティを編集します。）

Citrix Provisioning（旧Provisioning Services）およびMachine Creation Services™（MCS）を使用して、以下をプロビジョニングできます。

- サポートされているデスクトップまたはサーバーOS VM用のレガシーBIOS。
- セキュアブートを含む、サポートされているデスクトップまたはサーバーOS VM用のUEFI。

> **注:**
>
> MCSを構成する際には、プールオペレーター以上の権限が必要です。

XenServer接続にIntelliCache™を使用する

IntelliCacheを使用すると、共有ストレージとローカルストレージの組み合わせを使用できるため、ホスト型VDI展開の費用対効果が高まります。これにより、パフォーマンスが向上し、ネットワークトラフィックが削減されます。ローカルストレージは共有ストレージからマスターイメージをキャッシュするため、共有ストレージへの読み取り回数が減少します。共有デスクトップの場合、差分ディスクへの書き込みは、共有ストレージではなくホスト上のローカルストレージに書き込まれます。

- IntelliCacheを使用する場合、共有ストレージはNFSである必要があります。

- Citrixでは、可能な限り最速のデータ転送を確保するために、高性能なローカルストレージデバイスを使用することをお勧めします。

IntelliCacheを使用するには、この製品とXenServerの両方で有効にする必要があります。

- XenServerのインストール時に、**Enable thin provisioning (Optimized storage for Virtual Desktops)** を選択します。Citrixは、IntelliCacheが有効なサーバーと無効なサーバーが混在するプールをサポートしていません。詳しくは、XenServerのドキュメントを参照してください。
- Citrix Virtual Apps and Desktops™では、IntelliCacheはデフォルトで無効になっています。この設定はXenServer接続の作成時にのみ変更でき、後でIntelliCacheを無効にすることはできません。XenServer接続を追加するときは、次の手順を実行します。
  - ストレージの種類として **Shared** を選択します。
  - **Use IntelliCache** チェックボックスをオンにします。

必要なXenServer権限

XenServerの権限はロールベース（RBAC）です。XenServerのロールベースアクセス制御（RBAC）機能を使用すると、ユーザー、ロール、および権限を割り当てて、XenServerへのアクセス権を持つユーザーと実行できるアクションを制御できます。XenServer RBACシステムは、ユーザー（またはユーザーグループ）を定義されたロール（名前付きの権限セット）にマッピングします。ロールには、特定の操作を実行するための関連するXenServer権限があります。

詳しくは、「ロールベースのアクセス制御」を参照してください。

権限が増加する順のロール階層は、次のとおりです：Read-Only → VM Operator → VM Admin → VM Power Admin → Pool Operator → Pool Admin。

次のセクションでは、各プロビジョニングタスクに必要な最小限のロールをまとめます。

ホスト接続の作成

タスク	必要な最小ロール
XenServer から取得した情報を使用してホスト接続を追加する	読み取り専用
ユーザーとその割り当てられた役割を表示する	読み取り専用

VM の電源管理

タスク	必要な最小限の役割
VM の電源をオンまたはオフにする	VM オペレーター

VM の作成、更新、または削除

タスク	必要な最小限の役割
既存のスナップショットスケジュールに VM を追加または削除する	VM 電源管理者
スナップショットスケジュールの追加、変更、削除	プールオペレーター
マスターイメージの公開	プールオペレーター（スイッチポートロックが必要）
マシンカタログの作成	プールオペレーター: スイッチポートロックが必要
VM の追加または削除 (GPU が有効になっていない VM)	VM 管理者
VM の追加または削除 (GPU が有効になっている VM)	プールオペレーター
仮想ディスクまたはCDデバイスの追加、削除、または構成	VM 管理者
タグの管理	VM オペレーター

RBACの役割と権限の詳細については、「RBACの役割と権限」を参照してください。

スイッチポートロックの詳細については、「スイッチポートロックの使用」を参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create.html)を参照してください。

- XenServer固有の情報については、「XenServerカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create/create-machine-catalog-citrix-hypervisor.html)を参照してください。

詳細情報

- 「接続とリソース」(/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/connections.html)
- 「マシンカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create.html)

Google Cloud環境への接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報は、Google Cloud環境に固有の詳細を扱っています。

> **注：**
>
> Google Cloud環境への接続を作成する前に、まずGoogle Cloudアカウントをリソースの場所として設定を完了する必要があります。「Google Cloud環境」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/install-prepare/gcp.html)を参照してください。

接続の追加

「接続とリソースの作成」(/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/connections.html)のガイダンスに従ってください。以下の説明は、ホスティング接続の設定について案内します。

1. **管理 > 構成**から、左側のペインで**ホスティング**を選択します。
2. アクションバーで**「接続とリソースの追加」**を選択します。
3. **「接続」ページで、「新しい接続の作成」と「Citrix provisioning™ tools」を選択し、「次へ」**を選択します。
   - **接続の種類**。メニューから**Google Cloud**を選択します。
   - **接続名**。接続の名前を入力します。
4. **リージョン**ページで、メニューからプロジェクト名を選択し、使用するリソースを含むリージョンを選択してから、**次へ**を選択します。

5. **ネットワーク**ページで、リソースの名前を入力し、メニューから仮想ネットワークを選択し、サブセットを選択してから、**次へ**を選択します。リソース名は、リージョンとネットワークの組み合わせを識別するのに役立ちます。名前に「*(Shared)*」というサフィックスが付いている仮想ネットワークは、共有VPCを表します。共有VPCのサブネットレベルのIAMロールを構成した場合、共有VPCの特定のサブネットのみがサブネットリストに表示されます。

   > **注：**
   >
   > - リソース名は1～64文字で、空白のみ、または文字`\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' )`を含めることはできません。

6. 「**概要**」ページで情報を確認し、「**完了**」を選択して「**接続とリソースの追加**」ウィンドウを終了します。

接続とリソースを作成すると、作成した接続とリソースが一覧表示されます。接続を構成するには、接続を選択し、アクションバーで該当するオプションを選択します。

同様に、接続の下に作成されたリソースを削除、名前変更、またはテストできます。これを行うには、接続の下のリソースを選択し、アクションバーで該当するオプションを選択します。

サービスエンドポイントURL

次のURLにアクセスできる必要があります。

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`
- `https://compute.googleapis.com`
- `https://storage.googleapis.com`
- `https://cloudbuild.googleapis.com`

Google Cloudプロジェクト

Google Cloudプロジェクトには基本的に2つのタイプがあります。

- プロビジョニングプロジェクト：この場合、現在の管理者アカウントがプロジェクト内のプロビジョニングされたマシンを所有します。このプロジェクトはローカルプロジェクトとも呼ばれます。

- 共有VPCプロジェクト: プロビジョニングプロジェクトで作成されたマシンが、共有VPCプロジェクトのVPCを使用するプロジェクト。プロビジョニングプロジェクトに使用される管理者アカウントは、このプロジェクトで限られた権限、具体的にはVPCを使用する権限のみを持ちます。

GCP管理トラフィックのセキュアな環境を作成する

Google Cloudプロジェクトへのプライベートアクセスを許可できます。この実装により、機密データを処理するためのセキュリティが強化されます。これを実現するには、次のいずれかを実行できます。

- Cloud BuildサービスアカウントのVPCサービスコントロールの以下のイングレスルールを含めます。この手順を実行する場合は、GCP管理トラフィックのセキュアな環境を作成するための以下の手順に従わないでください。

```
Ingress Rule 1

From:

Identities:

<ProjectID>@cloudbuild.gserviceaccount.com

Source > All sources allowed

To:

Projects =

All projects

Services =

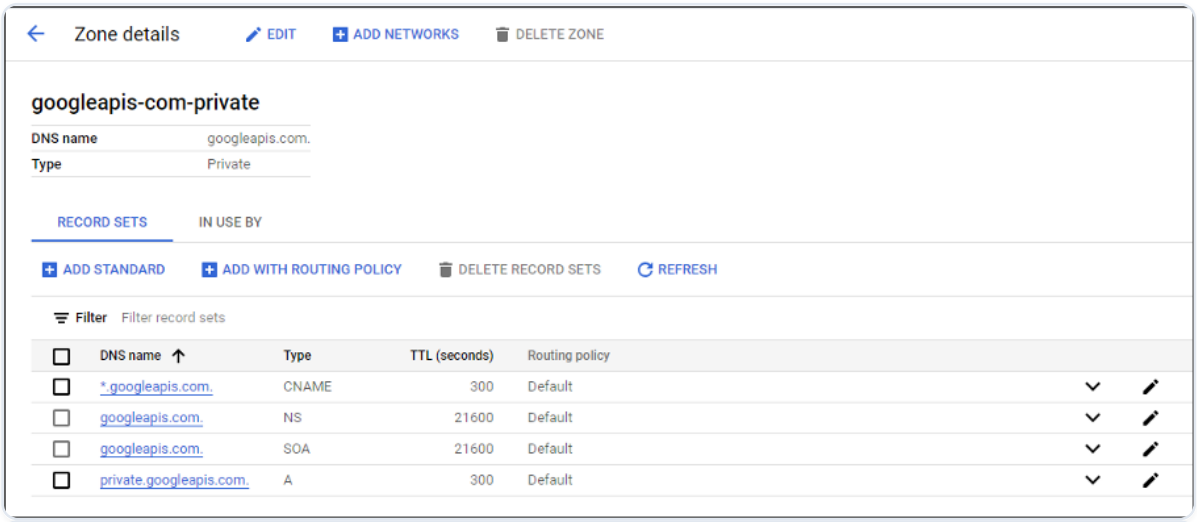
Service name: All services
```

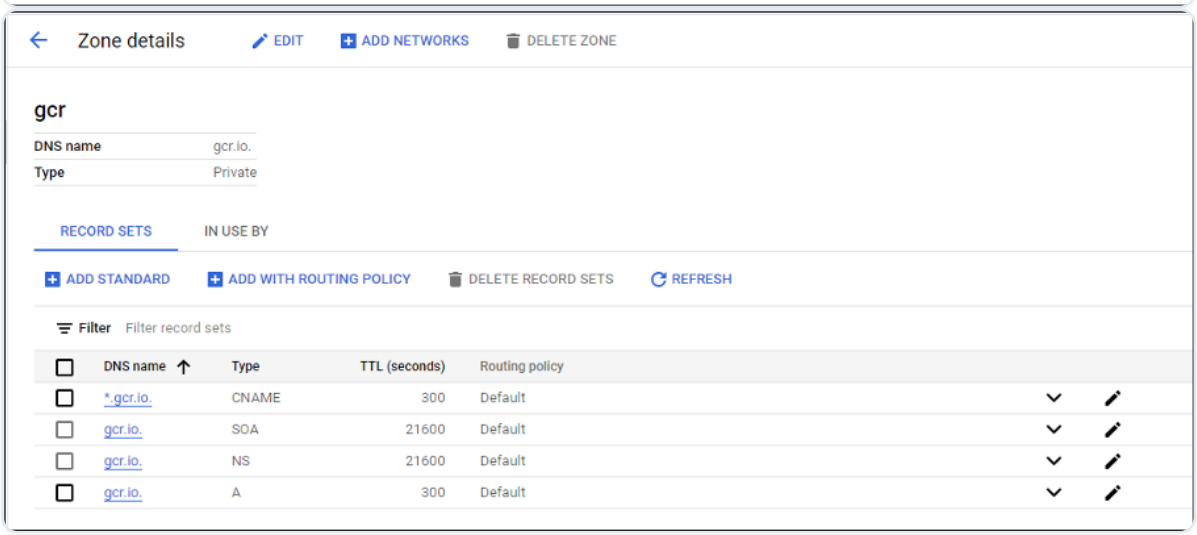
- プライベートワーカープールを使用している場合は、`CustomProperties`に`UsePrivateWorkerPool`を追加します。プライベートワーカープールの詳細については、プライベートプール概要を参照してください。

GCP管理トラフィックのセキュアな環境を作成するための要件

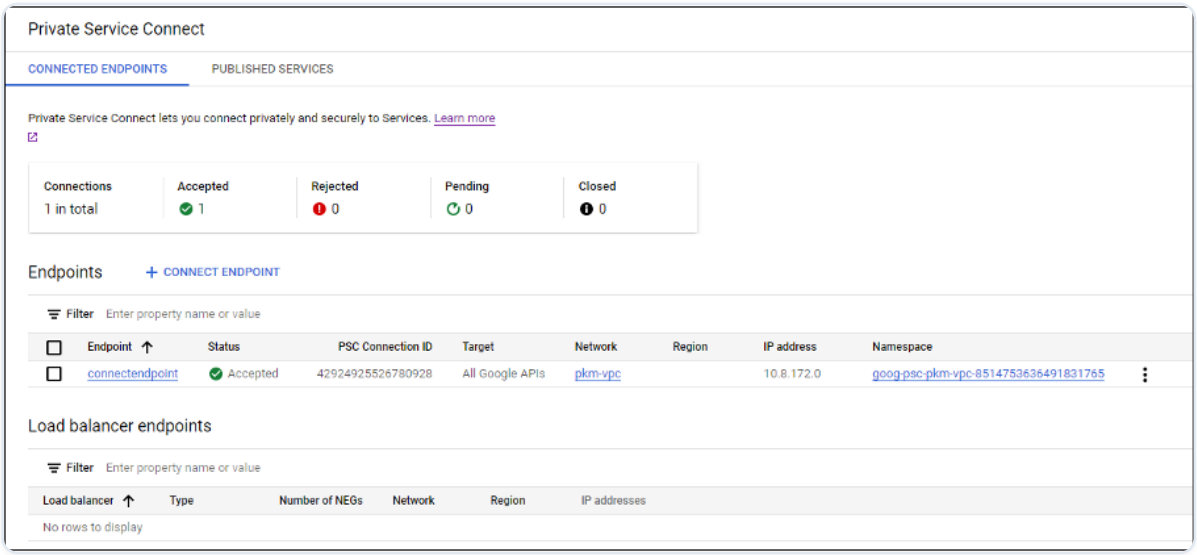
GCP管理トラフィックのセキュアな環境を作成するための要件は次のとおりです。

- カスタムプロパティを更新する際は、ホスティング接続がメンテナンスモードであることを確認してください。
- プライベートワーカープールを使用するには、次の変更が必要です。
  - Citrix Cloud™サービスアカウントには、以下のIAMロールを追加します。
    - Cloud Build サービスアカウント
    - Compute Instance 管理者
    - サービスアカウントユーザー
    - サービスアカウントトークン作成者
    - Cloud Build WorkerPool オーナー
  - ホスティング接続の作成に使用するのと同じプロジェクトにCitrix Cloudサービスアカウントを作成します。
  - DNS構成で説明されているように、`private.googleapis.com`および`gcr.io`のDNSゾーンを設定します。

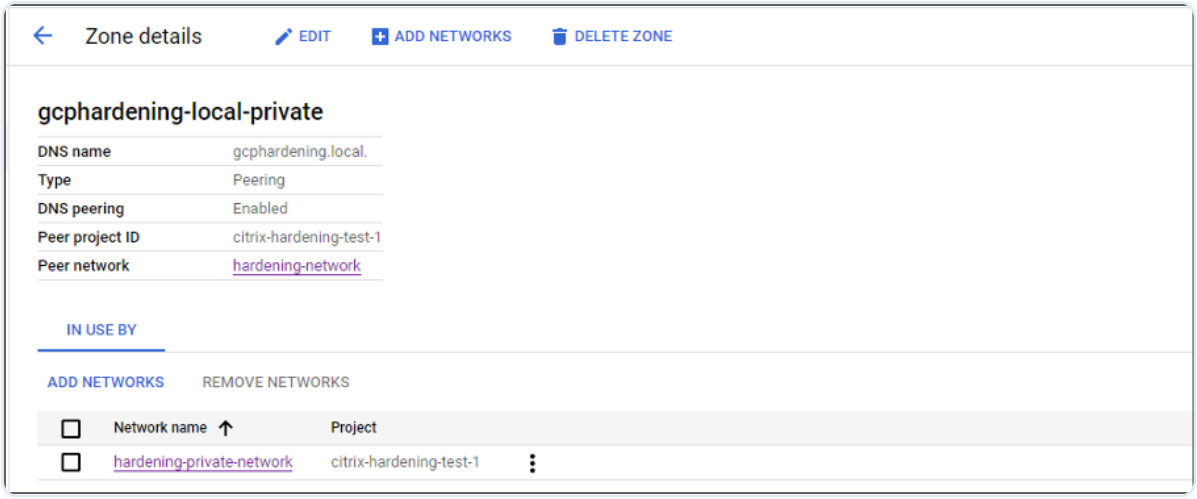




- プライベートネットワークアドレス変換 (NAT) を設定するか、プライベートサービス接続を使用します。詳細については、「エンドポイントを介したGoogle APIへのアクセス」を参照してください。



- ピアリングされたVPCを使用している場合は、ピアリングされたVPCへのCloud DNSゾーンピアリングを作成します。詳細については、「ピアリングゾーンの作成」を参照してください。



- VPC サービスコントロールで、API と VM がインターネットと通信できるようにエグレスルールを設定します。イングレスルールはオプションです。例：

```
Egress Rule 1

From:

Identities:ANY_IDENTITY

To:
```

```
Projects =

All projects

Service =

Service name: All services
```

プライベートワーカープールを有効にする

プライベートワーカープールを有効にするには、ホスト接続でカスタムプロパティを次のように設定します。

1. Delivery ControllerホストからPowerShellウィンドウを開くか、Remote PowerShell SDKを使用します。Remote PowerShell SDKの詳細については、「SDKとAPI」を参照してください。
2. 次のコマンドを実行します。
   a. `Add-PSSnapin citrix*`
   b. `cd XDHyp:\Connections\`
   c. `dir`
3. 接続から`CustomProperties`をメモ帳にコピーします。
4. プロパティ設定`<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool" Value="True"/>`を追加します。例：

```
```

<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.citrix.com/2014/xd/machinecreation">

<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool"
Value="True"/>

</CustomProperties>

```
```

5. PowerShellウィンドウで、変更されたカスタムプロパティに変数を割り当てます。例：`$customProperty = '<CustomProperties…</CustomProperties>'`。

6. `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"` を実行します。
7. `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"` を実行します。
8. `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force` を実行します。
9. 既存のホスト接続を更新するには、以下を実行します。

```
Set-Item -PassThru -Path @('XDHyp:\\Connections\\<ENTER YOUR CONNECTION NAME HERE>') -SecurePassword $securePassword -UserName $gcpServiceAccount -CustomProperties $customProperty
```

CMEK のグローバルキーとリージョンキーを指定する

> **注:**
>
> GCP での CMEK のサポートは現在プレビュー中です。

> GCPには、顧客管理の暗号化キー (CMEK) には2種類あります。

- リージョン：同じリージョン内のリソースのみが使用できる暗号化キー。
- グローバル：複数のリージョンのリソースが使用できる暗号化キー。

サービスアカウントがアクセスできるすべてのプロジェクトから、グローバルまたはリージョンの顧客管理の暗号化キー (CMEK) を参照して使用できます。その後、そのキーを使用してCMEK対応のMCSマシンカタログを作成し、`Set-ProvScheme` コマンドを使用して既存のCMEK対応のMCSマシンカタログを更新できます。PowerShellを使用してCMEK対応カタログを作成する方法については、「カスタムプロパティを使用してCMEKでカタログを作成する」を参照してください。

この機能には、次の2つのサービスアカウントに追加の権限が必要です。

- ホスティング接続が作成される現在のプロジェクトのサービスアカウント。
- 現在のプロジェクトのCompute Engineサービスエージェント (メールアドレス: `service-PROJECT_NUMBER@compute-system.iam.gserviceaccount.com` を持つ)。詳細については、Compute Engine Service Agent を参照してください。

サービスアカウントで、使用する暗号キーを持つプロジェクト (例: 共有プロジェクト) に次の役割を割り当てる必要があります。

- Cloud KMS ビューアー
- クラウド KMS クリプトキー エンクリプター/ディクリプター

役割を割り当てない場合は、次の権限があることを確認してください:

- resourcemanager.projects.get
- cloudkms.keyRings.list
- cloudkms.keyRings.get
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.cryptoKeyVersions.useToDecrypt
- cloudkms.cryptoKeyVersions.useToEncrypt

暗号化キーを一覧表示する

PowerShellコマンドを使用して、同じプロジェクト内およびアクセス可能な他のすべてのプロジェクト内で、グローバルおよびリージョンの暗号化キーを一覧表示できます。これを行うには:

1. Delivery Controller™ ホストまたはリモートPowerShellからPowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、コマンド `asnp citrix*` を実行します。
3. 暗号化キーを一覧表示するには、次のコマンドを実行します。例：
   - `encryptionKeys` フォルダーの内容を一覧表示するには：

     ```
     Get-ChildItem XDHyp:\HostingUnits\my-
     hostingunit\encryptionKeys.folder
     ```

   - 同じプロジェクト内のグローバル暗号化キーを取得するには：

     ```
     Get-Item XDHyp:\HostingUnits\my-
     hostingunit\encryptionKeys.folder\myglobalkeyring.globalkeyring\mygl
     obalkey.cryptokey
     ```

   - 同じプロジェクト内のリージョン暗号化キーを取得するには：

```
Get-Item XDHyp:\HostingUnits\my-
hostingunit\encryptionKeys.folder\regional-ring.keyring\shared-
key.cryptokey
```

- アクセス可能な別のプロジェクト（例：myanotherproject）からグローバル暗号化キーを取得するには：

```
Get-Item XDHyp:\HostingUnits\my-
hostingunit\encryptionKeys.folder\myanotherproject.project\shared-
global-ring.globalkeyring\shared-key.cryptokey
```

- アクセス可能な別のプロジェクト（例：myanotherproject）からリージョン暗号化キーを取得するには：

```
Get-Item XDHyp:\HostingUnits\my-
hostingunit\encryptionKeys.folder\myanotherproject .project.project\
shared-uscentral.keyring\shared-uscentral-key.cryptokey
```

注：

- グローバルキーリングのキーリングインベントリアイテムの拡張子は `.globalkeyring` です。
- グローバルキーリングのIDには、`global` という単語が含まれています。

必要なGCP権限

このセクションには、GCP権限の完全なリストが含まれています。機能が正しく動作するように、このセクションに記載されている権限の完全なセットを使用してください。

注：

GCP は、April 29, 2024 以降、Cloud Build Services のデフォルトの動作とサービスアカウントの使用に変更を導入しています。詳細については、Cloud Build Service Account Change を参照してください。April 29, 2024 より前に Cloud Build API が有効になっている既存の Google プロジェクトは、この変更の影響を受けません。ただし、April 29 以降も既存の

> Cloud Build Service の動作を維持したい場合は、API を有効にする前に、制約の適用を無効にする組織ポリシーを作成または適用できます。新しい組織ポリシーを設定した場合でも、このセクションの既存の権限と、**Before Cloud Build Service Account Change** とマークされている項目に従うことができます。そうでない場合は、既存の権限と、**After Cloud Build Service Account Change** とマークされている項目に従ってください。

ホスト接続の作成

- プロビジョニングプロジェクトのCitrix Cloudサービスアカウントに必要な最小限の権限：

  ```
  compute.instanceTemplates.list

  compute.instances.list

  compute.networks.list

  compute.projects.get

  compute.regions.list

  compute.subnetworks.list

  compute.zones.list

  resourcemanager.projects.get
  ```

  次の Google 定義ロールには、上記にリストされている権限があります:

  - Compute 管理者
  - クラウド データストア ユーザー

- Shared VPCプロジェクトにおけるCitrix Cloudサービスアカウントの Shared VPCに必要な追加の権限:

  ```
  compute.networks.list

  compute.subnetworks.list

  resourcemanager.projects.get
  ```

  次の Google 定義ロールには、上記にリストされている権限があります:

    - コンピュート ネットワーク ユーザー

- サービスアカウントでは、使用する暗号鍵があるプロジェクト（共有プロジェクトなど）に以下のロールを割り当てる必要があります:

    - Cloud KMS 閲覧者
    - クラウド KMS クリプトキー 暗号化/復号化

    これらのロールを割り当てない場合は、以下の権限があることを確認してください:

    - resourcemanager.projects.get
    - cloudkms.keyRings.list
    - cloudkms.keyRings.get
    - cloudkms.cryptoKeys.get
    - cloudkms.cryptoKeys.list
    - cloudkms.cryptoKeyVersions.useToDecrypt
    - cloudkms.cryptoKeyVersions.useToEncrypt

VMの電源管理

電源管理のみのカタログの場合、プロビジョニングプロジェクト内のCitrix Cloudサービスアカウントに必要な最小限の権限:

```
compute.instanceTemplates.list

compute.instances.list

compute.instances.get

compute.instances.reset

compute.instances.resume

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.networks.list
```

```
compute.projects.get

compute.regions.list

compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get

compute.zoneOperations.get
```

次のGoogle定義のロールには、上記にリストされている権限があります:

- Compute管理者
- クラウド データストア ユーザー

VMの作成、更新、または削除

- プロビジョニングプロジェクト内のCitrix Cloudサービスアカウントに必要な最小限の権限:

```
cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.list
```

```
compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk
```

```
compute.instances.get

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete
```

```
compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list

iam.serviceAccounts.actAs

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list
```

```
compute.networks.get

compute.resourcePolicies.use
```

次のGoogle定義のロールには、上記にリストされている権限があります:

- Compute 管理者
- Storage 管理者
- Cloud Build 編集者
- サービスアカウントユーザー
- クラウド データストア ユーザー

- Shared VPCプロジェクトでVPCとサブネットワークを使用してホスティングユニットを作成するために、Shared VPCプロジェクト内のCitrix Cloudサービスアカウントに Shared VPCで追加で必要な権限:

```
compute.firewalls.list

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zones.list

resourcemanager.projects.get
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- コンピュート ネットワーク ユーザー
- クラウド データストア ユーザー

準備指示ディスクをMCSにダウンロードする際に必要な最小限の権限:

- (Cloud Buildサービスアカウントの変更前): これらの権限をプロビジョニングプロジェクトのCloud Buildサービスアカウントに割り当てます。
- (Cloud Buildサービスアカウントの変更後): これらの権限をプロビジョニングプロジェクトのCloud Computeサービスアカウントに割り当てます。

```
compute.disks.create

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.images.get

compute.images.list

compute.images.useReadOnly

compute.instances.create

compute.instances.delete

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount
```

```
compute.machineTypes.list

compute.networks.get

compute.networks.list

compute.projects.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zones.list

iam.serviceAccounts.actAs

logging.logEntries.create

pubsub.topics.publish

resourcemanager.projects.get

source.repos.get

source.repos.list

storage.buckets.create

storage.buckets.get

storage.buckets.list

storage.objects.create

storage.objects.delete

storage.objects.get
```

```
storage.objects.list
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- Cloud Buildサービスアカウント (Cloud Buildサービスアカウントの変更後はCloud Computeサービスアカウント)
- Compute Instance 管理者
- サービスアカウントユーザー

- 準備指示ディスクをMCSにダウンロードする際にGoogle Cloud Buildサービスによって必要とされる、プロビジョニングプロジェクトのCloud Computeサービスアカウントに必要な最小限の権限:

```
resourcemanager.projects.get

storage.objects.create

storage.objects.get

storage.objects.list
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- コンピュート ネットワーク ユーザー
- ストレージアカウントユーザー
- クラウド データストア ユーザー

MCS に準備指示ディスクをダウンロードする際の共有 VPC に必要な追加の権限:

- (Cloud Build サービスアカウントの変更前): これらの権限をプロビジョニングプロジェクトの Cloud Build サービスアカウントに割り当てます。
- (Cloud Build サービスアカウントの変更後): これらの権限をプロビジョニングプロジェクトの Cloud Compute サービスアカウントに割り当てます。

```
compute.firewalls.list

compute.networks.list

compute.subnetworks.list
```

```
compute.subnetworks.use

resourcemanager.projects.get
```

次の Google 定義ロールには、上記にリストされている権限があります:

- コンピュート ネットワーク ユーザー
- ストレージアカウントユーザー
- クラウド データストア ユーザー

- プロビジョニングプロジェクトの Citrix Cloud サービスアカウントの Cloud Key Management Service (KMS) に必要な追加の権限:

```
cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list
```

次の Google 定義ロールには、上記にリストされている権限があります:

- Compute KMS 閲覧者

一般的な権限

以下は、MCS でサポートされているすべての機能について、プロビジョニングプロジェクトの Citrix Cloud サービスアカウントの権限です。これらの権限は、今後の最適な互換性を提供します:

```
resourcemanager.projects.get

cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get
```

```
compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list
```

```
compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.instances.update

compute.instances.updateAccessConfig

compute.instances.updateDisplayDevice

compute.instances.updateSecurity

compute.instances.updateShieldedInstanceConfig

compute.instances.updateShieldedVmConfig
```

```
compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list
```

```
resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list

compute.disks.list

compute.instances.setServiceAccount

compute.networks.get

compute.networks.use

compute.networks.useExternalIp

iam.serviceAccounts.actAs

compute.resourcePolicies.use

cloudkms.cryptoKeyVersions.useToDecrypt
```

```
cloudkms.cryptoKeyVersions.useToEncrypt
```

次のステップ

- 初期展開プロセス中の場合は、マシンカタログの作成を参照してください。
- Google Cloud Platform (GCP)固有の情報については、Google Cloud Platformカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

HPE Moonshotへの接続

「接続とリソースの作成および管理」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/connections.html)は、接続を作成するウィザードについて説明しています。以下の情報は、HPE Moonshotに固有の詳細を説明しています。

注:

HPE Moonshotへの接続を作成する前に、まずHPEアカウントの設定を完了する必要があります。「HPE Moonshot仮想化環境」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/install-prepare/hpe-moonshot.html)を参照してください。

接続を作成する

HPE Moonshotへの接続は、以下を使用して作成できます。

- ウェブスタジオ
- PowerShellコマンド

Web Studioを使用して接続を作成する

1. **接続とリソースの追加**ページで、接続の種類として**HPE Moonshot**を選択します。
2. Moonshot iLO Chassis Managerの接続アドレスを入力します。アドレスには、IPアドレス、ホスト名、またはFQDNを使用できます。
3. シャーシの管理者資格情報とわかりやすい接続名を入力します。

以下のいずれかの状況が発生すると、接続設定は停止します。

- Citrix Virtual Apps and Desktops™がエラーのある公開CA署名証明書を受信した場合：エラーメッセージが表示されます。画面の指示に従って問題を修正してください。そうしないと、接続の作成に進むことはできません。
- Citrix Virtual Apps and DesktopsがプライベートCA署名証明書を受信した場合。警告ページが表示されます。受信したサムプリントをサーバーのものと比較して、証明書の有効性を確認します。有効な場合は、**証明書を信頼する**を選択し、**OK**をクリックして接続の作成に進みます。その後、Citrix Virtual Apps and Desktopsは証明書を信頼し、将来の検証のためにサムプリントを保存します。

PowerShellコマンドを使用して接続を作成する

PowerShellコマンドを使用して接続を作成する場合、次の情報を提供します。

- IP: HPEサーバーのIPアドレス
- ユーザー名: HPEユーザー名
- パスワード: HPEパスワード

例:

```
New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata
@{"Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false"} -Path
@("XDHyp:\Connections\$connectionName") -Persist -PluginId
"HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
$UserName -sslthumbprint $SslThumbprint New-BrokerHypervisorConnection
-HypHypervisorConnectionUid $HypervisorConnectionID
```

> **注:**
>
> `sslthumbprint`パラメーターは、プライベートCA署名付き証明書の場合にのみ必要です。

証明書とサムプリントの検証

HPE Moonshotへの接続を正常に作成するには、証明書にエラーがなく、サムプリントが正しい値である必要があります。証明書とサムプリントの検証に関連するユースケースは次のとおりです。

- パブリックCA署名付き証明書にエラーがあります。接続は正常に作成されません。エラーの詳細を確認し、問題を解決してください。
- エラーのないパブリックCA署名付き証明書。接続は正常に作成され、`SslThumbprints` の値は**Null**です。
- エラーがなく、`sslthumbprint` の値を持つプライベートCA署名付き証明書。接続は正しい `SslThumbprints` の値で正常に作成されます。
- 不正なサムプリント値を持つプライベートCA署名付き証明書。接続は正常に作成されません。
- エラーのないプライベートCA署名付き証明書。接続は正常に作成されます。接続作成時に `SSlThumbprints` は**Null**です。`SSlThumbprints` の値は、サイトサービスによって値に更新されます。

接続の管理

このセクションでは、接続を管理する方法について詳しく説明します。

- Web Studioを使用して証明書の問題を修正する
- PowerShellコマンドを使用してサムプリント値を更新する

証明書の問題を修正する

Citrix Virtual Apps and Desktops は、証明書の問題が発生した場合に HPE Moonshot 接続をブロックし、関連する HPE Moonshot ノードでのワークロードの配信と管理を妨げます。**ホスト接続**リストの接続の横にエラーアイコンが表示されます。特定の問題と解決策については、次の表を参照してください。

問題	解決策
公開 CA 署名証明書で証明書エラーが発生する	接続をクリックし、**トラブルシューティング**タブを選択します。エラーの詳細を表示し、問題を解決します。
受信した証明書がプライベート CA 署名であるか、期限切れです。	ホスト接続を編集して、証明書のサムプリントを更新します。詳細な手順：
	1. 接続を選択し、**接続の編集**をクリックします。

問題	解決策
	1. **Connection Properties** ページで、**Edit settings** をクリックします。
	1. HPE Moonshot シャーシに接続するためのパスワードを入力し、**Save** をクリックします。
	1. 表示される **Warning** ページで、受信したサムプリントをサーバーのものと比較して、証明書の有効性を確認します。
	1. 同じ場合は、**Trust certificate** を選択し、**OK** をクリックします。

サムプリント値の更新

接続を作成した後、`Set-Item` PowerShellコマンドを使用して接続のサムプリント値を更新できます。たとえば、次のコマンドを実行します。

1. 接続の接続詳細を取得します。例：

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

2. サムプリント値を更新します。例:

```
Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
Administrator -SslThumbprint xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
```

3. 更新されたサムプリント値を確認します。例:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

注:

`Set-Item` コマンドで誤ったサムプリント値を指定すると、更新は失敗します。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- AWS固有の情報については、「HPE Moonshotマシンカタログの作成」を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

Microsoft Azure への接続

注:

2023 年 7 月以降、Microsoft は Azure Active Directory (Azure AD) を Microsoft Entra ID に名称変更しました。このドキュメントでは、Azure Active Directory、Azure AD、または AAD へのすべての参照は、Microsoft Entra ID を指します。

接続とリソースの作成および管理 では、接続を作成するウィザードについて説明します。以下の情報では、Azure Resource Manager クラウド環境に固有の詳細について説明します。

注:

Microsoft Azure への接続を作成する前に、Azure アカウントをリソースの場所として設定を完了する必要があります。Microsoft Azure Resource Manager クラウド環境 を参照してください。

サービスプリンシパルと接続を作成する

接続を作成する前に、接続が Azure リソースにアクセスするために使用するサービスプリンシパルを設定する必要があります。接続は次の 2 つの方法で作成できます。

- Web Studio を使用してサービスプリンシパルと接続を同時に作成する

- 以前に作成したサービスプリンシパルを使用して接続を作成する

このセクションでは、次のタスクを完了する方法について説明します。

- Web Studio を使用してサービスプリンシパルと接続を作成する
- PowerShell を使用してサービスプリンシパルを作成する
- Azure でアプリケーションシークレットを取得する
- 既存のサービスプリンシパルを使用して接続を作成する

考慮事項

- Citrix® は、共同作成者ロールを持つサービスプリンシパルの使用を推奨しています。ただし、最小限の権限のリストについては、最小限の権限セクションを参照してください。
- 最初の接続を作成する際、Azure は必要な権限を付与するよう求めます。今後の接続では引き続き認証が必要ですが、Azure は以前の同意を記憶しているため、プロンプトは再度表示されません。
- 認証に使用されるアカウントは、Azure RBAC を使用してサブスクリプション内でロールを割り当てる権限を持っている必要があります。例として、サブスクリプションの所有者、ロールベースのアクセス制御管理者、またはユーザーアクセス管理者などです。
- 認証に使用されるアカウントは、サブスクリプションのディレクトリのメンバーである必要があります。注意すべきアカウントの種類は、「職場または学校」と「個人用 Microsoft アカウント」の2種類です。詳細については、CTX219211を参照してください。
- 既存の Microsoft アカウントをサブスクリプションのディレクトリのメンバーとして追加して使用することはできますが、ユーザーが以前にディレクトリのリソースのいずれかへのゲストアクセスを許可されていた場合、問題が発生する可能性があります。この場合、ディレクトリ内に必要な権限を付与しないプレースホルダーエントリが存在し、エラーが返されることがあります。

  これを修正するには、ディレクトリからリソースを削除し、明示的に再度追加します。ただし、このオプションは、アカウントがアクセスできる他のリソースに意図しない影響を与える可能性があるため、慎重に実行してください。
- 特定のアカウントが実際にはメンバーであるにもかかわらず、ディレクトリゲストとして検出される既知の問題があります。このような構成は、通常、古くから確立されたディレクトリアカウントで発生します。回避策：ディレクトリにアカウントを追加すると、適切なメンバーシップ値が取得されます。

- リソースグループは単にリソースのコンテナであり、自身のリージョン以外のリージョンからのリソースを含むことができます。リソースグループのリージョンに表示されるリソースが利用可能であると期待している場合、これは混乱を招く可能性があります。
- 必要な数のマシンをホストするのに十分な大きさのネットワークとサブネットがあることを確認してください。これにはある程度の先見性が必要ですが、Microsoft はアドレス空間の容量に関するガイダンスを提供し、適切な値を指定するのに役立ちます。

Web Studio を使用してサービスプリンシパルと接続を作成する

> **重要:**
>
> この機能は、Azure China サブスクリプションではまだ利用できません。

> Web Studio を使用すると、単一のワークフローでサービスプリンシパルと接続の両方を作成できます。サービスプリンシパルは、接続に Azure リソースへのアクセスを許可します。サービスプリンシパルを作成するために Azure に認証すると、アプリケーションが Azure に登録されます。登録されたアプリケーションには、秘密鍵 (クライアントシークレットまたはアプリケーションシークレットと呼ばれます) が作成されます。登録されたアプリケーション (この場合は接続) は、クライアントシークレットを使用して Azure AD に認証します。

開始する前に、以下の前提条件を満たしていることを確認してください。

- サブスクリプションのAzure Active Directoryテナントにユーザーアカウントがあること。
- 認証に使用するアカウントには、Azure RBACを使用してサブスクリプションでロールを割り当てる権限が必要です。例として、サブスクリプションの所有者、ロールベースのアクセス制御管理者、またはユーザーアクセス管理者などです。
- 認証には、グローバル管理者、アプリケーション管理者、またはアプリケーション開発者のアクセス許可が必要です。これらのアクセス許可は、ホスト接続の作成後に取り消すことができます。ロールの詳細については、Azure AD の組み込みロールを参照してください。

接続とリソースの追加ウィザードを使用して、サービスプリンシパルと接続を一緒に作成します。

1. **接続**ページで、**新しい接続の作成**、**Microsoft Azure**接続タイプ、およびAzure環境を選択します。
2. 仮想マシンを作成するために使用するツールを選択し、**次へ**を選択します。

3. ページで、Azure サブスクリプション ID と接続の名前を入力します。サブスクリプション ID を入力すると、 ボタンが有効になります。

   > **注:**
   >
   > 接続名には 1〜64 文字を含めることができ、空白のみ、または文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。

4. を選択し、Azure Active Directory アカウントのユーザー名とパスワードを入力します。
5. **サインイン**を選択します。
6. 「**Accept**」を選択して、Citrix Virtual Apps and Desktops™ に一覧表示された権限を付与します。Citrix Virtual Apps and Desktops は、指定されたユーザーに代わって Azure リソースを管理できるようにするサービスプリンシパルを作成します。
7. 「**Accept**」を選択すると、ウィザードの「**Connection**」ページに戻ります。

   > **注:**
   >
   > Azure への認証が正常に完了すると、「**Create new**」ボタンと「**Use existing**」ボタンが消えます。「**Connection successful**」というテキストが緑色のチェックマークとともに表示され、Azure サブスクリプションへの接続が成功したことを示します。

8. 「**Connection Details**」ページで、「**Next**」を選択します。

   > **注:**
   >
   > Azure への認証が正常に完了し、必要な権限の付与に同意するまで、次のページに進むことはできません。

9. 接続のリソースを構成します。リソースには、リージョンとネットワークが含まれます。
   - 「**地域**」ページで、地域を選択します。
   - 「**ネットワーク**」ページで、次の操作を行います。

- リージョンとネットワークの組み合わせを識別するために、1〜64文字のリソース名を入力します。リソース名には、空白のみを含めることや、文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。
- 仮想ネットワーク/リソースグループのペアを選択します。（同じ名前の仮想ネットワークが複数ある場合、ネットワーク名をリソースグループとペアにすることで、一意の組み合わせが提供されます。）前のページで選択したリージョンに仮想ネットワークがない場合は、そのページに戻り、仮想ネットワークがあるリージョンを選択してください。

10. 「**概要**」ページで、設定の概要を確認し、「**完了**」を選択してセットアップを完了します。

アプリケーションIDを表示する

接続を作成した後、その接続がAzureリソースへのアクセスに使用するアプリケーションIDを表示できます。

「**接続とリソースの追加**」リストで、詳細を表示する接続を選択します。「**詳細**」タブにアプリケーションIDが表示されます。

PowerShellを使用してサービスプリンシパルを作成する

PowerShellを使用してサービスプリンシパルを作成するには、Azure Resource Managerサブスクリプションに接続し、以下のセクションで提供されているPowerShellコマンドレットを使用します。

次の項目を準備してください。

- **SubscriptionId:** VDAsをプロビジョニングするサブスクリプションのAzure Resource Manager `SubscriptionID`。
- **ActiveDirectoryID**: Azure ADに登録したアプリケーションのTenant ID。
- **ApplicationName:** Azure ADで作成するアプリケーションの名前。

詳細な手順は次のとおりです。

Azure Resource Manager サブスクリプションに接続します。

```
`Connect-AzAccount`
```

1. サービスプリンシパルを作成する Azure Resource Manager サブスクリプションを選択します。

```
Get-AzSubscription -SubscriptionId $subscriptionId | Select-AzSubscription
```

2. AD テナントにアプリケーションを作成します。

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

3. サービスプリンシパルを作成します。

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

4. サービスプリンシパルにロールを割り当てます。

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

5. PowerShell コンソールの出力ウィンドウから ApplicationId をメモします。ホスト接続を作成する際に、その ID を指定します。

Azure でアプリケーションシークレットを取得する

既存のサービスプリンシパルを使用して接続を作成するには、まず Azure portal でサービスプリンシパルのアプリケーションIDとシークレットを取得する必要があります。

詳細な手順は次のとおりです。

1. Web Studio から、または PowerShell を使用して「**Application ID**」を取得します。
2. Azureポータルにサインインします。
3. Azure で、「**Azure Active Directory**」を選択します。
4. Azure AD の「**App registrations**」から、アプリケーションを選択します。
5. **証明書とシークレット**に移動します。
6. **クライアントシークレット**をクリックします。

既存のサービスプリンシパルを使用して接続を作成する

サービスプリンシパルが既にある場合は、それを使用して Web Studio で接続を作成できます。

次の項目を準備してください。

- SubscriptionId
- ActiveDirectoryID (テナントID)
- アプリケーションID
- アプリケーションシークレット

  詳細については、「アプリケーションシークレットの取得」(#get-the-application-secret-in-azure)を参照してください。

- シークレットの有効期限

詳細な手順は次のとおりです。

接続とリソースの追加ウィザードで、:

1. **接続**ページで、**新しい接続の作成**、**Microsoft Azure**接続タイプ、およびAzure環境を選択します。
2. 仮想マシンの作成に使用するツールを選択し、**次へ**を選択します。
3. 「**接続の詳細**」ページで、Azure サブスクリプション ID と接続の名前を入力します。

   > **注：**
   >
   > 接続名には 1～64 文字を含めることができ、空白のみ、または文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。

4. **既存を使用**を選択します。**既存のサービスプリンシパルの詳細**ウィンドウで、既存のサービスプリンシパルに対して次の設定を入力します。詳細を入力すると、**保存**ボタンが有効になります。**保存**を選択します。有効な詳細情報を提供するまで、このページから先に進むことはできません。

   - **サブスクリプションID**。AzureサブスクリプションIDを入力します。サブスクリプションIDを取得するには、Azureポータルにサインインし、**サブスクリプション > 概要**に移動します。
   - **Active Directory ID**（テナントID）。Azure ADに登録したアプリケーションのディレクトリ（テナント）IDを入力します。
   - **アプリケーションID**。Azure ADに登録したアプリケーションのアプリケーション（クライアント）IDを入力します。
   - **アプリケーションシークレット**。シークレットキー（クライアントシークレット）を作成します。登録されたアプリケーションは、このキーを使用してAzure ADに認証します。セキュリティ上の理由から、定期的にキーを変更することをお勧めします。後でキーを取得できないため、必ずキーを保存してください。
   - **シークレットの有効期限**。アプリケーションシークレットの有効期限が切れる日付を入力します。シークレットキーの有効期限が切れる14日前から、**ホスティング**ノードの特定のホスト接続に警告アイコンが表示されます。ただし、シークレットキーの有効期限が切れると、エラーが発生します。

> **注:**
>
> セキュリティ上の理由から、有効期限は現在から2年を超えることはできません。

- **認証 URL**。このフィールドは自動的に入力され、編集できません。
- **管理 URL**。このフィールドは自動的に入力され、編集できません。
- **ストレージサフィックス**。このフィールドは自動的に入力され、編集できません。
- **ディスクまたはスナップショットをアップロードまたはダウンロードするためのAzure BLOBストレージエンドポイント**。このフィールドは自動的に入力され、編集できません。
- **Key Vaultサービス**。このフィールドは自動的に入力され、編集できません。
- **サービスバスサフィックス**。このフィールドは自動的に入力され、編集できません。

  AzureでMCSカタログを作成するには、以下のエンドポイントへのアクセスが必要です。これらのエンドポイントへのアクセスにより、ネットワークとAzureポータルおよびそのサービス間の接続が最適化されます。

  - 認証URL: `https://login.microsoftonline.com`
  - 管理URL: `https://management.azure.com`。これはAzure Resource Managerプロバイダー APIのリクエストURLです。管理用のエンドポイントは環境によって異なります。たとえば、Azure Globalの場合は `https://management.azure.com`、Azure US Governmentの場合は `https://management.usgovcloudapi.net` です。
  - ストレージサフィックス: `https://*.core.windows.net`。これはストレージサフィックスのワイルドカード文字です (*)。たとえば、`https://demo.table.core.windows.net`。
  - ディスクまたはスナップショットをアップロードまたはダウンロードするためのAzure BLOBストレージエンドポイント: `https://*.storage.azure.net`。これはBLOBストレージのインポートおよびエクスポート操作のワイルドカード文字です (*)。たとえば、`https://md-impexp-xxxxx.z[00-50].blob.storage.azure.net`。
  - Key Vaultサービス: `https://*.vault.azure.net`。これはキーコンテナー名のワイルドカード文字です (*)。たとえば、`https://<your-key-vault-name>.vault.azure.net`。
  - サービスバスサフィックス: `https://*.servicebus.windows.net`。これはグローバルAzureクラウドで作成された名前空間のワイルドカード文字です (*)。たとえば、`https://{serviceNamespace}.servicebus.windows.net/{path}`。

5. **保存**を選択すると、「**接続の詳細**」ページに戻ります。「**次へ**」を選択して次のページに進みます。
6. 接続のリソースを構成します。リソースは、リージョンとネットワークで構成されます。
   - 「**地域**」ページで、地域を選択します。
   - 「**ネットワーク**」ページで、次の操作を行います。
     - リージョンとネットワークの組み合わせを識別しやすくするために、1〜64 文字のリソース名を入力します。リソース名には空白のみ、または文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。
     - 仮想ネットワーク/リソースグループのペアを選択します。（同じ名前の仮想ネットワークが複数ある場合、ネットワーク名とリソースグループをペアにすることで、一意の組み合わせが提供されます。）前のページで選択した地域に仮想ネットワークがない場合は、そのページに戻り、仮想ネットワークがある地域を選択してください。
7. 「**概要**」ページで、設定の概要を確認し、「**完了**」を選択してセットアップを完了します。

サービスプリンシパルと接続を管理する

このセクションでは、サービスプリンシパルと接続を管理する方法について詳しく説明します。

- Azureスロットル設定を構成する
- Azureでイメージ共有を有効にする
- Web Studioを使用して共有テナントを接続に追加する
- PowerShellを使用してイメージ共有を実装する
- アプリケーションシークレットとシークレットの有効期限を管理する

Azure スロットリング設定の構成

Azure Resource Manager は、サブスクリプションとテナントの要求をスロットルし、プロバイダーの特定のニーズに合わせて調整された定義済みの制限に基づいてトラフィックをルーティングします。詳細については、Microsoft サイトの「Resource Manager の要求のスロットリング」を参照してください。サブスクリプションとテナントには制限があり、多数のマシンを管理すると問題が発生する可能性があります。たとえば、多数のマシンを含むサブスクリプションでは、電源操作に関連するパフォーマンスの問題が発生する可能性があります。

> **ヒント:**

> 詳細については、「Machine Creation Services を使用した Azure パフォーマンスの向上」を参照してください。

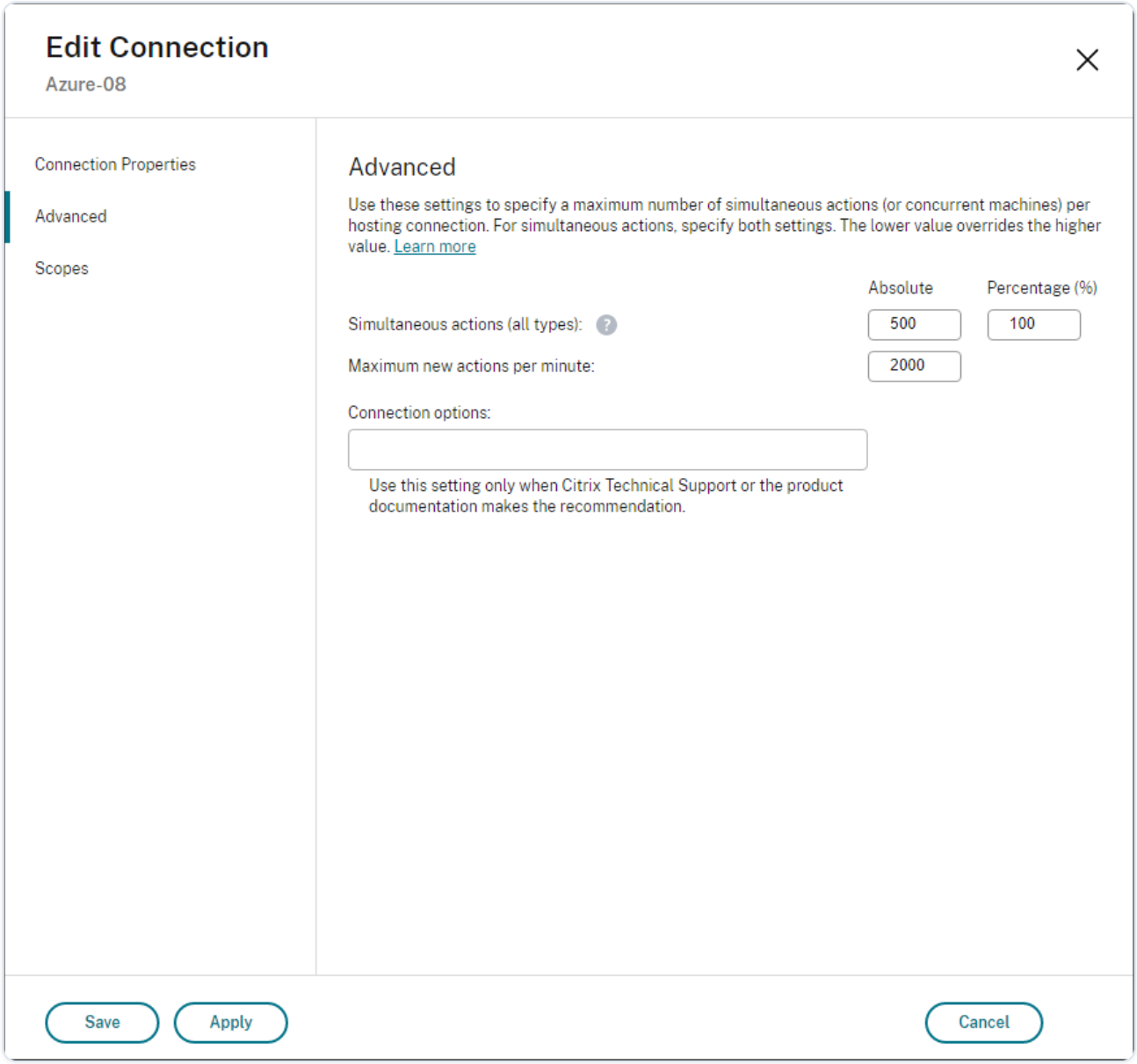
> これらの問題を軽減するために、MCS の内部スロットリングを削除して、Azure から利用可能な要求クォータをより多く使用できます。

大規模なサブスクリプション (たとえば、1,000 台の VM を含むサブスクリプション) で VM の電源をオンまたはオフにする場合、次の最適な設定をお勧めします。

- 絶対同時操作数: 500
- 1 分あたりの最大新規操作数: 2000
- 最大同時操作数: 500

Web Studio を使用して、特定の Azure 接続の Azure 操作を構成します。

1. Web Studio で、左側のペインで を選択します。
2. 接続を選択します。
3. ウィザードで、 を選択します。
4. ページで、構成オプションを使用して、同時アクションの数、1 分あたりの最大新規アクション数、および追加の接続オプションを指定します。



MCS は、デフォルトで最大 500 の同時操作をサポートします。または、Remote PowerShell SDK を使用して、最大同時操作数を設定することもできます。

PowerShell プロパティ `MaximumConcurrentProvisioningOperations` を使用して、Azure プロビジョニング操作の同時実行最大数を指定します。このプロパティを使用する際は、以下を考慮してください。

- `MaximumConcurrentProvisioningOperations` のデフォルト値は 500 です。
- PowerShell コマンド `Set-item` を使用して、`MaximumConcurrentProvisioningOperations` パラメーターを構成します。

Azure でのイメージ共有を有効にする

マシンカタログを作成または更新する際、異なる Azure テナントおよびサブスクリプションからの共有イメージ（Azure Compute Gallery を介して共有）を選択できます。テナント内またはテナント間でイメージ共有を有効にするには、Azure で必要な設定を行う必要があります。

- テナント内でのイメージ共有（サブスクリプション間）
- テナント間でのイメージ共有

テナント内でのイメージ共有（サブスクリプション間）

異なるサブスクリプションに属する Azure Compute Gallery のイメージを選択するには、そのサブスクリプションのサービスプリンシパル (SPN) とイメージを共有する必要があります。

たとえば、Studio で次のように構成されているサービスプリンシパル (SPN 1) がある場合：

サービスプリンシパル: SPN 1

サブスクリプション: subscription 1

テナント: tenant 1

イメージは別のサブスクリプションにあり、Studio では次のように構成されています。

サブスクリプション: subscription 2

テナント: tenant 1

サブスクリプション 2 のイメージをサブスクリプション 1 (SPN 1) と共有したい場合は、サブスクリプション 2 に移動し、リソースグループを SPN1 と共有します。

イメージは、Azure ロールベースのアクセス制御 (RBAC) を使用して別の SPN と共有する必要があります。Azure RBAC は、Azure リソースへのアクセスを管理するために使用される承認システムです。Azure RBAC の詳細については、Microsoft ドキュメント「Azure ロールベースのアクセス制御 (Azure RBAC) とは」を参照してください。アクセスを許可するには、共同作成者ロールを持つリソースグループスコープでサービスプリンシパルにロールを割り当てます。Azure ロールを割り当てるには、ユーザーアクセス管理者や所有者などの `Microsoft.Authorization/roleAssignments/write` 権限が必要です。別の SPN とイメージを共有する方法の詳細については、Microsoft ドキュメント「Azure portal を使用して Azure ロールを割り当てる」を参照してください。

PowerShell コマンドを使用して別のサブスクリプションからイメージを選択する方法については、「」(#select-an-image-from-a-different-subscription) を参照してください。

テナント間でイメージを共有する

Azure Compute Gallery を使用してテナント間でイメージを共有するには、アプリケーション登録を作成します。

たとえば、2つのテナント (テナント1とテナント2) があり、テナント1とイメージギャラリーを共有したい場合は、次の手順を実行します。

1. テナント1のアプリケーション登録を作成します。詳細については、「アプリ登録の作成」を参照してください。
2. ブラウザを使用してサインインを要求することで、テナント2にアプリケーションへのアクセスを許可します。`Tenant2 ID` をテナント1のテナントIDに置き換えます。`Application (client) ID` を作成したアプリケーション登録のアプリケーションIDに置き換えます。置換が完了したら、URLをブラウザに貼り付け、サインインプロンプトに従ってテナント2にサインインします。例:

   ```
   https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
   client_id=<Application (client)
   ID>&response_type=code&redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
   ```

   詳細については、「テナント 2 にアクセスを許可する」を参照してください。
3. アプリケーションにテナント 2 のリソースグループへのアクセスを許可します。テナント 2 としてサインインし、ギャラリーイメージがあるリソースグループにアプリケーション登録のアクセスを許可します。詳細については、「テナント間で要求を認証する」を参照してください。

PowerShell コマンドを使用して別のテナントのイメージからカタログを作成するには:

1. 「」(#update-hosting-connection-custom-properties-with-shared-tenant-ids)。
2. 「」(#select-an-image-from-a-different-tenant)。

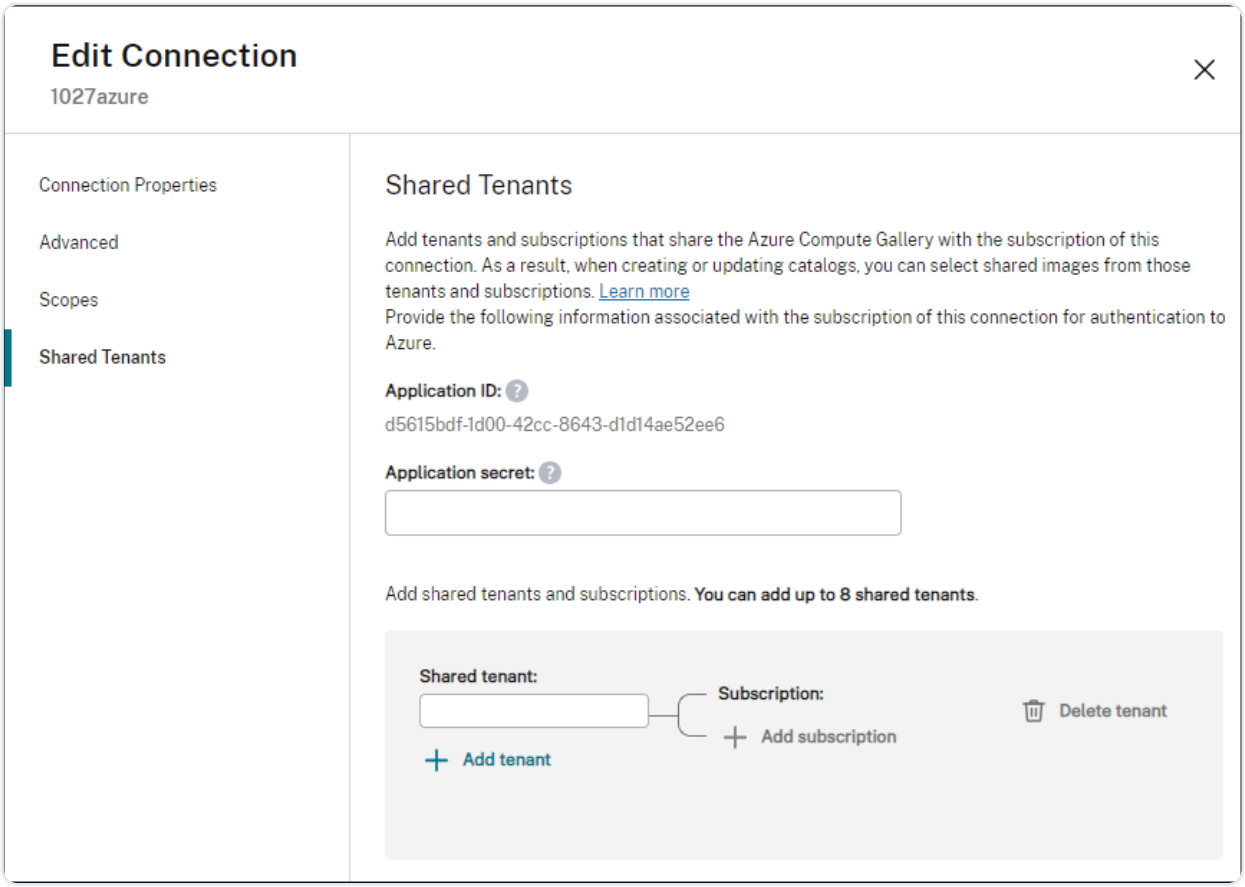
Web Studio を使用して共有テナントを接続に追加する

Web Studioでマシンカタログを作成または更新する際に、異なるAzureテナントおよびサブスクリプション（Azure Compute Galleryを介して共有）から共有イメージを選択できます。この機能を使用するには、関連するホスト接続の共有テナントおよびサブスクリプション情報を提供する必要があります。

> **注:**
>
> テナント間でイメージ共有を有効にするために、Azureで必要な設定が構成されていることを確認してください。詳細については、「テナント間でイメージを共有する」を参照してください。

接続に対して次の手順を完了します。

1. Web Studioで、左ペインの**「ホスティング」**を選択します。
2. 接続を選択し、アクションバーで**「接続の編集」**を選択します。



3. **「共有テナント」**で、次の操作を行います。

   - 接続のサブスクリプションに関連付けられているアプリケーションIDとアプリケーションシークレットを指定します。Citrix Virtual Apps and Desktopsは、この情報を使用してAzure ADに認証します。
   - 接続のサブスクリプションとAzure Compute Galleryを共有するテナントとサブスクリプションを追加します。各テナントにつき、最大8つの共有テナントと8つのサブスクリプションを追加できます。

4. 完了したら、**「適用」を選択して変更を適用し、ウィンドウを開いたままにするか、「OK」**を選択して変更を適用し、ウィンドウを閉じます。

PowerShellを使用したイメージ共有の実装

このセクションでは、PowerShellを使用してイメージを共有するプロセスについて説明します。

- 別のサブスクリプションからイメージを選択する
- ホスティング接続のカスタムプロパティを共有テナントIDで更新する
- 別のテナントからイメージを選択する(#select-an-image-from-a-different-tenant)

別のサブスクリプションからイメージを選択する

同じAzureテナント内の別の共有サブスクリプションに属するAzure Compute Galleryのイメージを選択して、PowerShellコマンドを使用してMCSカタログを作成および更新できます。

1. ホスティングユニットのルートフォルダーに、Citrixは`sharedsubscription`という新しい共有サブスクリプションフォルダーを作成します。
2. テナント内のすべての共有サブスクリプションを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\sharedsubscription.folder"
```

3. 1つの共有サブスクリプションを選択し、その共有サブスクリプションのすべての共有リソースグループを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription"
```

4. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\
xyz.resourcegroup"
```

5. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\testgallery.gallery"
```

6. 1つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\sigtestdef.imagedefinition"
```

7. 次の要素を使用してMCSカタログを作成および更新します。

   - リソースグループ

- ギャラリー
- ギャラリーイメージ定義
- ギャラリーイメージバージョン

Remote PowerShell SDK を使用したカタログの作成方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>` を参照してください。

共有テナントIDでホスティング接続のカスタムプロパティを更新する

`Set-Item` を使用して、共有テナントIDとサブスクリプションIDでホスティング接続のカスタムプロパティを更新します。`CustomProperties` にプロパティ `SharedTenants` を追加します。`Shared Tenants` の形式は次のとおりです。

```
[{"Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":
["7bb42f40-8d7f-4230-a920-be2781f6d5d9"]},{"Tenant":"50e83564-c4e5-4209-
b43d-815c45659564","Subscriptions":["06ab8944-6a88-47ee-
a975-43dd491a37d0"]}]
```

例:

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
Value=`"123`" />

<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
Value=`"https://management.azure.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
Value=`"https://login.microsoftonline.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`"
Value=`"core.windows.net`" />

<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`" /
>

<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`"
Value=`"`[ { 'Tenant':'123abc', 'Subscriptions':['345', '567'] } ]`"` />
```

```
</CustomProperties>"

-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "advc345"
-SecurePassword

$psd
```

注:

複数のテナントを追加できます。各テナントは複数のサブスクリプションを持つことができます。

別のテナントからイメージを選択する

PowerShellコマンドを使用してMCSカタログを作成および更新するために、別のAzureテナントに属するAzure Compute Gallery内のイメージを選択できます。

1. ホスティングユニットのルートフォルダーに、Citrixは `sharedsubscription` という新しい共有サブスクリプションフォルダーを作成します。
2. すべての共有サブスクリプションを一覧表示します。

   ```
   Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
   ```

3. 1つの共有サブスクリプションを選択し、その共有サブスクリプションのすべての共有リソースグループを一覧表示します。

   ```
   Get-ChildItem XDHyp:
   \HostingUnits\azres\image.folder\abc123.sharedsubscription
   ```

4. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

   ```
   Get-ChildItem XDHyp:
   \HostingUnits\azres\image.folder\abc123.sharedsubscription\
   xyz.resourcegroup
   ```

5. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery
```

6. 1つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery\hij.imagedefinition
```

7. 次の要素を使用してMCSカタログを作成および更新します。

   - リソースグループ
   - ギャラリー
   - ギャラリーイメージ定義
   - ギャラリーイメージバージョン

   Remote PowerShell SDK を使用したカタログの作成方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>` を参照してください。

アプリケーションシークレットとシークレットの有効期限を管理する

シークレットの有効期限が切れる前に、接続のアプリケーションシークレットを必ず変更してください。シークレットキーの有効期限が切れる14日前から、**ホスティング**ノードの特定のホスト接続に警告アイコンが表示されます。ただし、シークレットキーの有効期限が切れると、エラーが発生します。

AZURE でアプリケーションシークレットを作成する

Azure portal を使用して、接続のアプリケーションシークレットを作成できます。

1. **Azure Active Directory** を選択します。
2. Azure AD の **アプリの登録** から、アプリケーションを選択します。
3. **証明書とシークレット** に移動します。
4. **クライアントシークレット > 新しいクライアントシークレット** をクリックします。
5. シークレットの説明を入力し、期間を指定します。完了したら、**追加** を選択します。

> **注：**
>
> クライアントシークレットは後で取得できないため、必ず保存してください。

6. クライアントシークレットの値と有効期限をコピーします。
7. Web Studio で、対応する接続を編集し、**Application secret** および **Secret expiration date** フィールドの内容をコピーした値に置き換えます。

シークレットの有効期限を変更する

Web Studio を使用して、使用中のアプリケーションシークレットの有効期限を追加または変更できます。

> **注:**
>
> シークレットキーの有効期限が切れる14日前から、ホスティングノードの特定のホスト接続に警告アイコンが表示されます。

1. **接続とリソースの追加**ウィザードで、接続を右クリックし、**接続の編集**をクリックします。
2. **接続プロパティ**ページで、**シークレットの有効期限**をクリックして、使用中のアプリケーションシークレットの有効期限を追加または変更します。

事前作成されたネットワークセキュリティグループを使用する

CitrixにNSGの作成と変更を要求する代わりに、イメージ準備用のDeny-Allネットワークセキュリティグループを作成します。PowerShellコマンド `Set-Item` を使用してホスティングユニットのカスタムプロパティを編集し、Deny-Allネットワークセキュリティグループを提供するためのパラメーター `NsgForPreparation` を含めます。

前提条件

サービスプリンシパルに必要な以下の権限を構成します。

- `Microsoft.Network/networkSecurityGroups/join/action`: ネットワークセキュリティグループをサブネットまたはネットワークインターフェイスに関連付ける
- `Microsoft.Network/networkSecurityGroups/read`: ネットワークセキュリティグループを取得する
- `Microsoft.Network/networkSecurityGroups/securityRules/read`: ルールを取得する

事前作成されたDeny-Allネットワークセキュリティグループを追加する

事前作成されたDeny-Allネットワークセキュリティグループを追加するには、ホスティングユニットでカスタムプロパティを次のように設定します。

1. Remote PowerShell SDKを使用してPowerShellウィンドウを開きます。
2. 次のコマンドを実行します。

```
Add-PSSnapin citrix*.

cd XDHyp:\HostingUnits\

Dir
```

3. 詳細を取得するホスティングユニットを選択します。

```
Get-Item "XDHyp:\HostingUnits\<hostingunitname>"
```

4. CustomPropertiesをメモ帳にコピーし、プロパティ設定`<Property xsi:type="StringProperty`" Name=`"NsgForPreparation`" Value=`"{ResourceGroupName}/{NetworkSecurityGroupName}"/>`を追加します。例：

```
<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"NsgForPreparation`" Value=`{ResourceGroupName}/
{NetworkSecurityGroupName}`"/></CustomProperties>
```

5. PowerShell ウィンドウで、変更されたカスタムプロパティに変数を割り当てます。例:

```
$customProperty = "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"NsgForPreparation`" Value=`"{ResourceGroupName}/
{NetworkSecurityGroupName}`"/></CustomProperties>"
```

6. `$cred = Get-Credential`を実行します。プロンプトが表示されたら、接続資格情報を入力します。資格情報は Azure アプリケーション ID とシークレットです。
7. 次のコマンドを実行します。

```
Set-Item -PSPath XDHyp:\HostingUnits\<hostingunitname>
-CustomProperties $customProperty -username $cred.username
-Securepassword $cred.password
```

重要:

SubscriptionIdが不足しているというメッセージが表示された場合は、カスタムプロパティ内のすべての二重引用符（“）をバックティックと二重引用符（`”）に置き換えます。

8. 更新された `CustomProperties` 設定を確認するには、`dir` を実行します。

注:

更新が反映されるまでに1分以上かかります。

ネットワークセキュリティグループの詳細を取得する

ネットワークセキュリティグループの詳細を取得するには、まずネットワークセキュリティグループを含むリソースグループを取得し、次にリソースグループ名に基づいてネットワークセキュリティグループを取得します。

1. ネットワークセキュリティグループを含むリソースグループを取得します。例：

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes":
["networksecuritygroup"]}'
```

2. リソースグループ名に基づいてネットワークセキュリティグループを取得します。例：

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType securitygroup -MaxRecords
5 -AdditionalDataFilter '{"location": ["eastus", "westus"],
"resourcegroup":["resourcegroupname"]}'
```

空のリソースグループをフィルターする

マシンカタログ作成時にマスターイメージ、マシンプロファイル、または準備済みイメージを選択する際に、PowerShellコマンド`Get-HypInventoryItem`を使用して空のリソースグループをフィルターします。

例:

- ページ内の最大レコード数を取得する:

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5
```

- 1ページあたりの最大レコード数を取得し、特定のリソースを持つリソースコンテナを見つけるためにフィルターします。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
```

- スキップを使用してページを直接指定して取得し、特定のリソースを持つリソースコンテナを見つけるためにフィルターします。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -skip 20 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
```

- トークンを使用して次のページを取得し、特定のリソースを持つリソースコンテナを見つけるためにフィルターします。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
-ContinuationToken
'ew0KICAiJGlkIjogIjEiLA0KICAiTWF4Um93cyI6IDUsDQogICJSb3dzVG9Ta2lwIjogMj
```

```
UsDQogICJLdXN0b0NsdXN0ZXJVcmwiOiAiaHR0cHM6Ly9hcmctbmV1LTEzLXNmLmFyZy5jb
3JlLndpbmRvd3MubmV0Ig0KfQ=='
```

- タグ「Citrix internal tag」を持つすべてのリソースグループを取得し、`MaxRecords`で最大レコード数を制限する。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5
```

- タグ「Citrix internal tag」を持つマシンプロファイル（マスターイメージ）をフィルタリングし、`MaxRecords`で最大レコード数を制限する。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"templatespecversion"]}'
```

- タグ「Citrix internal tag」を持つ準備済みイメージをフィルタリングし、`MaxRecords`で最大レコード数を制限する。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion"]}'
```

- タグ「Citrix internal tag」を持つマシンプロファイル（準備済みイメージ）をフィルタリングし、`MaxRecords`で最大レコード数を制限する。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"templatespecversion"]}'
```

- タグ「Citrix internal tag」を持つイメージをフィルタリングし、`MaxRecords`と場所で最大レコード数を制限する。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion", "storageaccount"], "location": ["eastus",
"westus"]}'
```

- タグを考慮せずにすべてのリソースグループを取得する `CitrixResource`。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
50 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion", "storageaccount"]}' -Force $true
```

Azure Sovereign Airgap クラウド環境に接続する

Azure Sovereign Airgap クラウド環境は、分離されたネットワークドメイン上にある必要がある極秘のワークロードに適しています。ホスト接続を作成する際に、カスタムプロパティ `DisableInstanceDiscovery` を使用して Azure Sovereign Airgap クラウド環境に接続できます。

```
<Property xsi:type="StringProperty" Name="DisableInstanceDiscovery"
Value="true" />
```

Azure ホスト接続の作成に関する詳細については、Create-HostingConnection.ps1 を参照してください。

必要なAzure権限

このセクションには、Azure に必要な最小限の一般的な権限が含まれています。

最小限の権限

最小限の権限は、より優れたセキュリティ制御を提供します。ただし、追加の権限を必要とする新機能は、最小限の権限のみを使用しているため失敗します。

ホスト接続の作成

Azure から取得した情報を使用して、新しいホスト接続を追加します。

```
"Microsoft.Network/virtualNetworks/read",

"Microsoft.Compute/virtualMachines/read",
```

```
"Microsoft.Compute/disks/read",

"Microsoft.Resources/providers/read",

"Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/tenants/read",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/securityRules/read"
```

VM の電源管理

マシンインスタンスの電源をオンまたはオフにします。

```
"Microsoft.Compute/virtualMachines/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Insights/diagnosticsettings/delete",

"Microsoft.Insights/diagnosticsettings/read",

"Microsoft.Insights/diagnosticsettings/write",
```

仮想マシンの作成、更新、または削除

マシンカタログを作成し、マシンを追加、削除、更新し、マシンカタログを削除します。

以下は、マスターイメージがマネージドディスクである場合、またはスナップショットがホスティング接続と同じリージョンにある場合に必要となる最小限の権限のリストです。

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
read",

"Microsoft.Compute/skus/read",

"Microsoft.Compute/virtualMachines/extensions/read",
```

```
"Microsoft.Compute/virtualMachines/extensions/write",

"Microsoft.Features/providers/features/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/locations/usages/read",

"Microsoft.Compute/capacityReservationGroups/capacityReservations/read"
```

以下の機能の最小限の権限に基づいて、以下の追加の権限が必要です。

- マスターイメージが、ホスティング接続と同じリージョンにあるストレージアカウント内のVHDである場合:

  ```
  "Microsoft.Storage/storageAccounts/read",

  "Microsoft.Storage/storageAccounts/listKeys/action",
  ```

- マスターイメージがShared Image GalleryのImageVersionである場合:

```
"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/read",
```

- マスターイメージがマネージドディスクであり、スナップショットまたはVHDがホスティング接続のリージョンとは異なるリージョンにある場合:

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",
```

- Citrix管理のリソースグループを使用する場合:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
```

- マスターイメージを共有テナントまたはサブスクリプションのAzure Compute Gallery (旧 Shared Image Gallery) に配置する場合:

```
"Microsoft.Compute/galleries/write",

"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/images/versions/write",

"Microsoft.Compute/galleries/read",
```

```
"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/versions/delete",

"Microsoft.Resources/subscriptions/read",
```

- Azure専用ホストサポートを使用する場合:

```
"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",

"Microsoft.Compute/hostGroups/hosts/read",
```

- 顧客管理キー (CMK) を使用したサーバー側暗号化 (SSE) を使用する場合:

```
"Microsoft.Compute/diskEncryptionSets/read",
```

- ARMテンプレート (マシンプロファイル) を使用してVMを展開する場合:

```
"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/delete",

"Microsoft.Insights/DataCollectionRuleAssociations/Read",

"Microsoft.Insights/dataCollectionRules/read",
```

- Azureテンプレート仕様をマシンプロファイルとして使用する場合:

```
"Microsoft.Resources/templateSpecs/read",

"Microsoft.Resources/templateSpecs/versions/read",
```

アンマネージドディスクを持つマシンの作成、更新、および削除

マスターイメージがVHDであり、管理者が提供するリソースグループを使用する場合に必要な最小限の権限のリストは次のとおりです:

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",
```

```
"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/locations/usages/read",
```

一般権限

共同作成者ロールは、すべてのリソースを管理するためのフルアクセス権を持っています。この権限セットは、新機能の取得を妨げるものではありません。

以下の権限セットは、現在の機能セットで必要とされる以上の権限を含んでいますが、今後最高の互換性を提供します:

```
"Microsoft.Compute/diskEncryptionSets/read",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/galleries/delete",
```

```
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/hostGroups/hosts/read",
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/write",
```

```
"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
read",

"Microsoft.Compute/skus/read",

"Microsoft.Compute/virtualMachines/extensions/read",

"Microsoft.Compute/virtualMachines/extensions/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/locations/usages/read",

"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/delete",
```

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Resources/providers/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Resources/subscriptions/read",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Resources/tenants/read",
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
"Microsoft.Features/providers/features/read",
"Microsoft.Insights/DataCollectionRuleAssociations/Read",
"Microsoft.Insights/dataCollectionRules/read",
"Microsoft.Insights/diagnosticsettings/delete",
```

```
"Microsoft.Insights/diagnosticsettings/read",

"Microsoft.Insights/diagnosticsettings/write",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/securityRules/read",

"Microsoft.Compute/capacityReservationGroups/capacityReservations/read"
```

ホスト接続の権限を検証する

ホスト接続のアクセス許可を検証して、MCSマシンカタログの作成と管理に関連するタスクを実行できます。この実装により、VMの作成、削除、更新、VMの電源管理など、さまざまなシナリオに必要な不足しているアクセス許可を事前に特定できるため、重要なときにブロックされるのを回避できます。

PowerShellコマンド `Test-HypHypervisorConnection` を使用して、ホスト接続の権限を検証できます。コマンドの結果はリストとしてキャプチャされ、リスト内の各項目は3つのセクションに分かれています。

- カテゴリ: ユーザーがMCSマシンカタログを作成および管理するために実行できるアクションまたはタスク。
- 是正措置: 管理者がユーザーの不足しているアクセス許可の不一致を解決するために実行する必要がある手順。
- 不足しているアクセス許可: カテゴリに不足しているアクセス許可のリスト。

権限を検証するには、次の手順を実行します。

1. Azureへのホスト接続を作成します。
2. Delivery Controller™ホストからPowerShellウィンドウを開きます。
3. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*` を実行します。
4. 接続をテストするために必要なアクセス許可があるかどうかを確認するには、次のコマンドを実行します。

   ```
   Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\AzureCon"
   ```

SPNに必要なロールレベルの権限:

- Microsoft.Authorization/roleDefinitions/read (サブスクリプションレベル、またはリソースグループが指定されている場合はリソースグループレベル)
- Microsoft.Authorization/roleAssignments/read (サブスクリプションレベル、またはリソースグループが指定されている場合はリソースグループレベル)

SPN に必要な API レベルの権限:

Microsoft.Graph:

- Application.Read.All
- Directory.Read.All
- ServicePrincipalEndpoint.Read.All

5. 権限を検索するために必要な不足している権限を追加した後、次のコマンドを実行して、さまざまなカテゴリで権限があるかどうかを確認します。

   例:

   より高いレベルの承認が必要なサブスクリプションレベルで接続をテストするには:

   ```
   Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\ AzureCon
   -SecurePassword $password -UserName 922e65d5-38ae-4cf5-xxxx-xxxxxxxxx
   ```

   例:

   高レベルの承認なしでリソースグループレベルで接続をテストするには:

   ```
   Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\testles
   -CustomProperties $customProperties | Format-List
   ```

   注:

   CustomPropertiesパラメーターは、リソースグループが接続固有の情報であるため、リソースグループレベルを提供するために使用されます。

   例:

リソースグループレベルでより高いレベルの承認を使用して接続をテストするには:

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\testles
-SecurePassword $password -UserName
922e65d5-38ae-4cf5-832b-54122196b7dd -CustomProperties
$customProperties
```

権限の詳細については、必要なAzure権限を参照してください。

次のステップ

- 初期展開プロセス中の場合は、(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create.html)を参照してください。
- Azure固有の情報については、(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html)を参照してください。

詳細情報

- 接続とリソース(/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/connections.html)
- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create.html)

マイクロソフト システムセンター バーチャル マシン マネージャーへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報は、Microsoft System Center Virtual Machine Manager (VMM) に固有の詳細を扱っています。

注:

VMM への接続を作成する前に、まず VMM アカウントをリソースの場所として設定する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/install-prepare/msscvmm.html)を参照してください。

接続を作成する

MCSを使用してVMをプロビジョニングした場合は、接続作成ウィザードで次の操作を行います。

- ホストサーバーの完全修飾ドメイン名としてアドレスを入力します。

- 以前に設定した管理者アカウントの資格情報を入力します。このアカウントには、新しいVMを作成する権限が必要です。
- 「ホストの詳細」ダイアログボックスで、VMの作成時に使用するクラスターまたはスタンドアロンホストを選択します。

> **重要**
>
> 単一のHyper-Vホスト展開を使用している場合でも、クラスターまたはスタンドアロンホストを参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- SMB 3 ファイル共有でMCSを使用してマシンカタログを作成する方法については、(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create/create-machine-catalog-mscvmm.html)を参照してください。

詳細情報

- 接続とリソース(/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/connections.html)
- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create.html)

Nutanixへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報はNutanixに固有の詳細を扱っています。

> **注:**
>
> Nutanixへの接続を作成する前に、まず、リソースの場所としてNutanixアカウントの設定を完了する必要があります。Nutanix仮想化環境を参照してください。

Nutanixへの接続を作成する

以下の情報は、「接続とリソース」(/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/connections.html)のガイダンスを補足するものです。Nutanix接続を作成するには、その記事の一般的なガイダンスに従い、Nutanixに固有の詳細に注意してください。

接続とリソースの追加ウィザードで、**接続**ページでNutanix接続の種類を選択し、アドレスと資格情報、および接続の名前を指定します。**ネットワーク**ページで、ホスティングユニットのネットワークを選択します。

選択できる接続の種類は、**Nutanix AHV**、**Nutanix AHV DRaaS**、**Nutanix AHV PC**です。

- **Nutanix AHV**の場合、Prism Element（PE）クラスターのアドレスと資格情報を指定します。
- **Nutanix AHV PC**の場合、Prism Central（PC）のアドレスと資格情報を指定します。

> **注:**
>
> 現在、接続タイプNutanix AHV PCは、Azure上のNutanix Cloud Cluster（NC2）への接続を作成する場合にのみ使用されます。また、マシンカタログは、Azure接続上のNC2内の単一クラスターでのみホストできます。

- **Nutanix AHV DRaaS**の場合、DRaaSテナントのアドレスとユーザー名を指定します。プライベートおよびパブリックのNutanix DRaaS資格情報ファイル（`.pem`）をインポートします。

> **ヒント:**
>
> Nutanix AHV (Prism Element) をリソースとして使用してマシンを展開する場合、VMのディスクが存在するコンテナを選択します。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create.html)を参照してください。
- Nutanix固有の情報については、「Nutanixカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create/create-machine-catalog-nutanix.html)を参照してください。

詳細情報

- 「接続とリソース」(/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/connections.html)
- 「マシンカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create.html)

Nutanix クラウドおよびパートナーソリューションへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明します。以下の情報は、Nutanix クラウドおよびパートナーソリューションに固有の詳細を扱います。

Citrix Virtual Apps and Desktops™ は、以下の Nutanix クラウドおよびパートナーソリューションをサポートしています。

- AWS 上の ニュータニックス クラウド クラスターズ

> **注:**
>
> Nutanix クラウドおよびパートナーソリューションへの接続を作成する前に、まずそれぞれのCitrixアカウントをリソースの場所として設定を完了する必要があります。Nutanix クラウドおよびパートナーソリューションを参照してください。

Nutanix Prismへの接続

Nutanix クラスターを作成したら、Nutanix Prism に接続します。

Nutanix Prism に接続するには:

1. 10.0.129.0/24サブネットに踏み台VMを作成します。
2. 踏み台VMにRDP接続し、前のセクションでコピーした**Prism Element**のURLにアクセスします。
3. デフォルトの資格情報 `admin:nutanix/4u` を使用してログインします。パスワードを変更することを忘れないでください。

Nutanixクラスター上にVMを作成する

Nutanix Prism に接続した後、Nutanix クラスター上に VM を作成します。

VMにインターネットアクセスが必要な場合

1. AWSコンソールに移動します。
2. Nutanix CFS によって作成された VPC と同じ VPC 内に、新しいサブネット 10.0.130.0/24 を作成します。
3. このサブネットのルートテーブルに、すべての非ローカルトラフィックを上記のNATゲートウェイにルーティングするルートを追加します。

4. Bastion VMにRDP接続し、前のセクションでコピーした**Prism Element**のURLにアクセスしてログインします。
5. 新しいネットワークを追加します。**Settings>Network Configuration>Create Subnet**に移動します。AWSで使用したのと同じサブネット10.0.130.0/24を使用します。
6. その新しいサブネット内に、すべてのVM (AD、CC、VDAなど) を作成します。

VM がインターネットアクセスを必要としない場合

1. 踏み台VMにRDP接続し、前のセクションでコピーした**Prism Element**のURLにアクセスしてログインします。
2. 新しいネットワークを追加します。**Settings>Network Configuration>Create Subnet** に移動します。サブネット 10.0.129.0/24 を使用します。
3. そのサブネットにすべての VM (AD、CC、VDA など) を作成します。

> **ヒント:**
>
> VM の時刻とタイムゾーン情報が正しく設定されていることを確認してください。これは特に AD に当てはまります。

ホスト接続を作成する

1. Web Studio を起動します。
2. ホスティングノードを選択し、 をクリックします。
3. **Connection** 画面で、**Create a new Connection** を選択し、**Connection address** に `https://xxx.xxx.xxx.xxx:9440` を入力します。
4. UI に従ってウィザードを完了します。

> **注:**
>
> Web StudioでNutanixのオプションを表示するには、すべてのコネクタVMにNutanixプラグインがインストールされている必要があります。Nutanixゾーンで使用されていない場合でも同様です。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。

- Nutanix 固有の情報については、「Nutanix カタログの作成」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create/create-machine-catalog-nutanix.html)

詳細情報

- 接続とリソース
- マシンカタログの作成

VMwareへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報は、VMware仮想化環境に固有の詳細を扱っています。

> **注：**
>
> VMwareへの接続を作成する前に、まずVMwareアカウントをリソースの場所として設定を完了する必要があります。VMware仮想化環境を参照してください。

接続を作成する

接続作成ウィザードで：

1. VMware接続タイプを選択します。
2. vCenter SDKのアクセスポイントのアドレスを指定します。
3. 以前に設定した、VMを作成する権限を持つVMwareユーザーアカウントの資格情報を指定します。ユーザー名はdomain/usernameの形式で指定します。

VMware SSLサムプリント

VMware SSLサムプリント機能により、VMware vSphereハイパーバイザーへのホスト接続を手動で作成する必要がなくなります。接続を作成する前に、サイト内のDelivery Controllerとハイパーバイザーの証明書との間に信頼関係を手動で作成する必要はなくなりました。

VMware SSLサムプリント機能は、信頼されていない証明書のサムプリントをサイトデータベースに保存します。この構成により、ハイパーバイザーは、Controllerによって信頼されていなくても、Citrix Virtual Apps and Desktops™によって継続的に信頼されていると識別されるようになります。

StudioでvSphereホスト接続を作成する際、接続先のマシンの証明書を表示できるダイアログボックスが表示されます。その後、それを信頼するかどうかを選択できます。

必要な権限

この記事に記載されている権限のセットまたはすべての権限を持つVMwareユーザーアカウントと1つ以上のVMwareロールを作成します。ロールの作成は、ユーザーがいつでもさまざまなCitrix DaaS™操作を要求するために必要な権限の特定の粒度レベルに基づいて行います。ユーザー固有の権限をいつでも付与するには、**子に伝播**オプションを選択した状態で、データセンターレベルで、それぞれのロールに関連付けます。ただし、`StorageProfile`権限と特定の`Tags`権限については、**子に伝播**なしで、ルートvCenter Serverレベルで権限を適用します。各テーブルの注記を参照してください。

以下の表は、Citrix Virtual Apps and Desktops の操作と、必要となる最小限の VMware 権限とのマッピングを示しています。

> **注:**
>
> 権限リストの表示名、特に *ユーザーインターフェイス* は、vSphere のバージョンによって異なります。たとえば、vSphere 6.7 では、*ユーザーインターフェイス* 権限は、このページに記載されている必要な権限で説明されている **設定** と **メモリ** ではなく、**メモリの変更** と **設定の変更** です。

接続とリソースを追加する

SDK	ユーザーインターフェイス
System. アノニマス, System. リード, および System. ビュー	自動的に追加されます。組み込みの読み取り専用ロールを使用できます。

電源管理

SDK	ユーザーインターフェイス
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > 操作 > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > 操作 > リセット

SDK	ユーザーインターフェイス
VirtualMachine.Interact.Suspend	仮想マシン > 操作 > サスペンド
Datastore.Browse	データストア > データストアの参照

マシンのプロビジョニング (Machine Creation Services™)

MCS を使用してマシンをプロビジョニングするには、次の権限が必要です。

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	Datastore > スペースの割り当て
Datastore.Browse	Datastore > データストアの参照
Datastore.FileManagement	Datastore > 低レベルファイル操作
Network.Assign	Network > ネットワークの割り当て
Resource.AssignVMToPool	リソース > 仮想マシンをリソースプールに割り当てる
VirtualMachine.Config.AddExistingDisk	仮想マシン > 構成 > 既存のディスクを追加
VirtualMachine.Config.AddNewDisk	仮想マシン > 構成 > 新しいディスクを追加
仮想マシン.Config.デバイスの追加または削除	仮想マシン > 構成 > デバイスの追加または削除
VirtualMachine.Config.AdvancedConfig	仮想マシン > 構成 > 詳細設定
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Config.CPUCount	仮想マシン > 構成 > CPU数の変更
VirtualMachine.Config.Memory	仮想マシン > 構成 > メモリの変更
VirtualMachine.Config.Settings	仮想マシン > 構成 > 設定の変更
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > 操作 > 電源オン

SDK	ユーザーインターフェイス
VirtualMachine.Interact.Reset	仮想マシン > 操作 > リセット
VirtualMachine.Interact.Suspend	仮想マシン > 操作 > サスペンド
VirtualMachine.Inventory.CreateFromExisting	仮想マシン > インベントリ > 既存から作成
VirtualMachine.Inventory.Create	仮想マシン > インベントリ > 新規作成
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除
VirtualMachine.Provisioning.Clone	仮想マシン > プロビジョニング > 仮想マシンのクローン作成
VirtualMachine.State.CreateSnapshot	vSphere 5.0 Update 2、vSphere 5.1 Update 1、および vSphere 6.x Update 1: 仮想マシン > 状態 > スナップショットの作成。vSphere 5.5: 仮想マシン > スナップショット管理 > スナップショットの作成

イメージの更新とロールバック

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	データストア > スペースの割り当て
Datastore.Browse	データストア > データストアの参照
Datastore.FileManagement	データストア > 低レベルファイル操作
Network.Assign	ネットワーク > ネットワークの割り当て
Resource.AssignVMToPool	リソース > 仮想マシンをリソースプールに割り当てる
VirtualMachine.Config.AddExistingDisk	仮想マシン > 構成 > 既存のディスクを追加
VirtualMachine.Config.AddNewDisk	仮想マシン > 構成 > 新しいディスクを追加
VirtualMachine.Config.AdvancedConfig	仮想マシン > 構成 > 詳細設定
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除

SDK	ユーザーインターフェイス
VirtualMachine.Interact.PowerOff	仮想マシン > 相互作用 > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > 相互作用 > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > 相互作用 > リセット
VirtualMachine.Inventory.CreateFromExisting	仮想マシン > インベントリ > 既存から作成
VirtualMachine.Inventory.Create	仮想マシン > インベントリ > 新規作成
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除
VirtualMachine.Provisioning.Clone	仮想マシン > プロビジョニング > 仮想マシンのクローン作成

プロビジョニングされたマシンの削除

SDK	ユーザーインターフェイス
Datastore.Browse	データストア > データストアの参照
Datastore.FileManagement	Datastore > 低レベルファイル操作
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除

ストレージプロファイル (vSAN)

vSANデータストアでのカタログ作成中にストレージポリシーを表示、作成、または削除するには、次の権限が必要です。

SDK	ユーザーインターフェイス
StorageProfile.Update	プロファイル駆動型ストレージ > プロファイル駆動型ストレージの更新。vSphere 8 の場合: VM ストレージポリシー > VM ストレージポリシーの更新

SDK	ユーザーインターフェイス
StorageProfile.View	プロファイル駆動型ストレージ > プロファイル駆動型ストレージの表示。vSphere 8 の場合: VM ストレージポリシー > VM ストレージポリシーの表示

注:

ストレージプロファイルの権限は、**子への伝播**なしで、ルート vCenter Server レベルで適用します。

タグとカスタム属性

タグとカスタム属性を使用すると、vSphere インベントリで作成された VM にメタデータを添付し、これらのオブジェクトの検索とフィルタリングを容易にすることができます。タグまたはカテゴリを作成、編集、割り当て、削除するには、次の権限が必須です。

SDK	ユーザーインターフェイス
InventoryService.Tagging.CreateTag	vSphere タグ付け > vSphere タグの作成
InventoryService.Tagging.CreateCategory	vSphere タグ付け > vSphere タグカテゴリの作成
InventoryService.Tagging.EditTag	vSphere タグ付け > vSphere タグの編集
InventoryService.Tagging.EditCategory	vSphere タグ付け > vSphere タグカテゴリの編集
InventoryService.Tagging.DeleteTag	vSphere タグ付け > vSphere タグの削除
InventoryService.Tagging.DeleteCategory	vSphere タグ付け > vSphere タグカテゴリの削除
InventoryService.Tagging.AttachTag	vSphere タグ付け > vSphere タグの割り当てまたは割り当て解除
InventoryService.Tagging.ObjectAttachable	vSphere タグ付け > オブジェクトへのvSphere タグの割り当てまたは割り当て解除

SDK	ユーザーインターフェイス
Global.ManageCustomFields	グローバル > カスタム属性の管理
Global.SetCustomField	グローバル > カスタム属性の設定

注:

- MCSがマシンカタログを作成すると、ターゲットVMに特別な名前タグが付けられます。これらのタグは、マスターイメージをMCSによって作成されたVMと区別し、MCSによって作成されたVMをイメージ準備に使用することを防ぎます。vCenterの `XdProvisioned` 属性の値によって違いを識別できます。MCSがVMを作成する場合、この属性は**True**に設定されます。
- **子への伝播**なしで、ルートvCenter Serverレベルで `InventoryService.Tagging.AttachTag` 権限を適用します。

暗号化操作

暗号化操作の特権は、誰がどの種類のオブジェクトに対してどの種類の暗号化操作を実行できるかを制御します。vSphere Native Key Provider は `Cryptographer.*` 特権を使用します。暗号化操作には、以下の最小限の権限が必要です。

注:

これらの権限は、vTPMを搭載したVMでMCSマシンカタログを作成するために必要です。

SDK	ユーザーインターフェイス
Cryptographer.Access	特権 > すべての特権 > 暗号化操作 > 直接アクセス
Cryptographer.AddDisk	特権 > すべての特権 > 暗号化操作 > ディスクの追加

SDK	ユーザーインターフェイス
Cryptographer.Clone	特権 > すべての特権 > 暗号化操作 > クローン
Cryptographer.Encrypt	特権 > すべての特権 > 暗号化操作 > 暗号化
Cryptographer.EncryptNew	特権 > すべての特権 > 暗号化操作 > 新規暗号化
Cryptographer.Decrypt	特権 > すべての特権 > 暗号化操作 > 復号化
Cryptographer.Migrate	特権 > すべての特権 > 暗号化操作 > 移行
Cryptographer.ReadKeyServersInfo	特権 > すべての特権 > 暗号化操作 > KMS情報の読み取り

マシンのプロビジョニング (Citrix Provisioning™)

テンプレートをクローンして展開するためのこれらの権限は、Citrix Provisioningコンソールを介してCitrix Virtual Apps and Desktopsセットアップウィザードおよびデバイスエクスポートウィザードを使用してVMをプロビジョニングするために必要です。ホスティング接続の作成時に権限を設定します。マシンのプロビジョニング (Machine Creation Services) からのすべての権限と、以下の権限が必要です。

SDK	ユーザーインターフェイス
VirtualMachine.Config.AddRemoveDevice	仮想マシン > 構成 > デバイスの追加または削除
VirtualMachine.Config.CPUCount	仮想マシン > 構成 > CPU数の変更
VirtualMachine.Config.Memory	仮想マシン > 構成 > メモリ
VirtualMachine.Config.Settings	仮想マシン > 構成 > 設定
VirtualMachine.Provisioning.CloneTemplate	仮想マシン > プロビジョニング > テンプレートのクローン作成
VirtualMachine.Provisioning.DeployTemplate	仮想マシン > プロビジョニング > テンプレートの展開

SDK	ユーザーインターフェイス
VApp.Export	vApp > エクスポート

> **注:**
>
> マシンプロファイルを使用してMCSマシンカタログを作成するには、`VApp.Export`が必要です。

証明書を取得してインポートする

vSphere 通信を保護するため、Citrix® は HTTP ではなく HTTPS を使用することを推奨しています。

HTTPSにはデジタル証明書が必要です。組織のセキュリティポリシーに準拠した認証局から発行されたデジタル証明書を使用してください。

認証局から発行されたデジタル証明書を使用できない場合は、VMwareがインストールした自己署名証明書を使用できます。この方法は、組織のセキュリティポリシーで許可されている場合にのみ使用してください。VMware vCenter証明書を各Delivery Controllerに追加します。

1. vCenter Serverを実行しているコンピューターの完全修飾ドメイン名（FQDN）を、そのサーバーのhostsファイル（`%SystemRoot%/WINDOWS/system32/Drivers/etc/`）に追加します。この手順は、vCenter Serverを実行しているコンピューターのFQDNがドメインネームシステムにまだ存在しない場合にのみ必要です。
2. 以下の3つの方法のいずれかを使用して vCenter 証明書を取得します。

   vCenterサーバーから。

   a. vCenter サーバーからファイル rui.crt を、Delivery Controller からアクセス可能な場所にコピーします。

   b. Controller で、エクスポートされた証明書の場所に移動し、rui.crt ファイルを開きます。

   Web ブラウザーを使用して証明書をダウンロードします。 Internet Explorer を使用している場合は、Internet Explorer を右クリックし、**管理者として実行**を選択して証明書をダウンロードまたはインストールします。

   a. Web ブラウザーを開き、vCenter サーバーへの安全な Web 接続を行います (例: `<https://server1.domain1.com)>`)。

b. セキュリティ警告を受け入れます。

c. 証明書エラーが表示されているアドレスバーをクリックします。

d. 証明書を表示し、 タブをクリックします。

e. 「**ファイルにコピーして.CER形式でエクスポート**」を選択し、プロンプトが表示されたら名前を指定します。

f. エクスポートした証明書を保存します。

g. エクスポートした証明書の場所に移動し、.CERファイルを開きます。

管理者として実行している Internet Explorer から直接インポートします。

- Web ブラウザーを開き、vCenter サーバーへの安全な Web 接続を行います (例: `<https://server1.domain1.com)>`)。
- セキュリティ警告を受け入れます。
- 証明書エラーが表示されているアドレスバーをクリックします。
- 証明書を表示します。

3. 各Controllerの証明書ストアに証明書をインポートします。

a. **証明書のインストール**オプションをクリックし、**ローカルコンピューター**を選択して、**次へ**をクリックします。

b. **証明書をすべて次のストアに配置する**を選択し、**参照**をクリックします。**信頼されたユーザー**を選択し、**OK**をクリックします。**次へ**をクリックし、**完了**をクリックします。

インストール後にvSphereサーバーの名前を変更した場合は、新しい証明書をインポートする前に、そのサーバーで新しい自己署名証明書を生成する必要があります。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- VMware固有の情報については、「VMwareカタログの作成」を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

VMware クラウドおよびパートナーソリューションへの接続

Azure VMware Solution (AVS) クラスター、Google Cloud VMware Engine、およびVMware cloud on AWS を設定した後、接続を作成します。接続の作成については、VMwareへの接続 を参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- VMware固有の情報については、VMwareカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

イメージ管理

はじめに

MCSカタログの作成または更新プロセスには、次の2つのフェーズがあります。

- マスタリング: ソースイメージが公開イメージに変換されます
- クローニング: 公開イメージから新しいVMが作成されます

イメージ管理機能を使用すると、MCSはマスタリングフェーズをプロビジョニングワークフロー全体から分離します。

単一のソースイメージからさまざまなMCSイメージバージョン（準備済みイメージ）を準備し、複数の異なるMCSマシンカタログでそれを使用できます。また、同じホスト接続内のホスティングユニット間で準備済みイメージバージョンを共有することもできます。この実装により、ストレージと時間のコストが大幅に削減され、VMの展開とイメージの更新プロセスが簡素化されます。

このイメージ管理機能を使用する利点は次のとおりです。

- カタログを作成せずに、準備済みイメージを事前に生成します。
- カタログの作成や更新など、複数のシナリオで準備済みイメージを再利用します。
- カタログの作成または更新時間を大幅に短縮します。
- 同じホスト接続内のホスティングユニット間で準備済みイメージバージョンを共有します。

注:

- この機能は現在、AzureおよびVMware仮想化環境に適用されます。
- 準備済みイメージを使用せずにMCSマシンカタログを作成できます。その場合、この機能の利点を得ることはできません。

ユースケース

イメージ管理機能のユースケースの一部を次に示します。

- *バージョン管理*: イメージバージョンを使用すると、次のことが可能になります。
  - 特定のイメージに対するさまざまなイテレーションや更新を管理する。
  - さまざまな目的のために、イメージの複数のバージョンを維持する。
- *論理的なグループ化*: 複数のイメージ定義を作成して、次のことが可能になります。
  - プロジェクト、部門、アプリケーション、デスクトップの種類など、さまざまな基準に基づいてイメージのバージョンを論理的にグループ化する。
  - 組織内でイメージをより効率的に管理する。
- *イメージ共有*: 同じホスト接続内のホスティングユニット間で準備済みイメージバージョンを共有して、次のことが可能になります。
  - 異なるホスティングユニット間でイメージの一貫性と均一性を確保する。

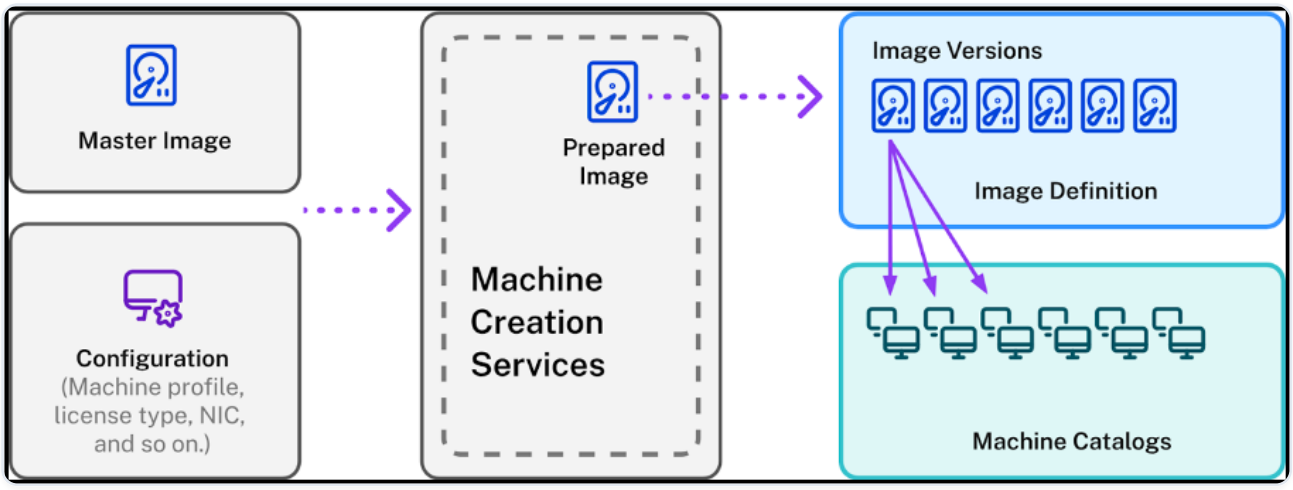
準備されたイメージとは何ですか?

イメージ管理機能により、MCSはマスタリングフェーズをカタログ作成または更新ワークフロー全体から切り離し、プロセスを2つの段階に分割します。

1. 単一のソースイメージから準備されたイメージを作成する。
2. 準備されたイメージを使用して、MCSマシンカタログを作成または更新する。

準備されたイメージは事前に作成できます。単一の準備されたイメージを使用して、複数のMCSプロビジョニング済みマシンカタログを作成または更新できます。

イメージからWeb Studioを使用する場合に、準備されたイメージが複数のMCSマシンカタログでどのように使用されるかを理解してください。



イメージ定義: イメージ定義は、イメージのバージョンの論理的なグループ化です。イメージ定義には、次の情報が含まれます。

- イメージが作成された理由
- どのOS用であるか
- イメージの使用に関するその他の情報。

カタログはイメージ定義から作成されるのではなく、イメージ定義に基づいて作成されたイメージバージョンから作成されます。

イメージバージョン: イメージバージョンは、イメージ定義のバージョン管理を行います。1つのイメージ定義には複数のイメージバージョンを含めることができます。イメージバージョンを準備されたイメージとして使用して、カタログを作成または更新します。AzureおよびVMware仮想化環境では、同じホスト接続内のホスティングユニット間でイメージバージョンを共有できます。

あるいは、PowerShellコマンドを使用してプロビジョニングスキームを作成し、カタログを作成または更新する場合は、環境に応じて、マスターイメージバージョン仕様に基づいて準備されたイメージバージョン仕様を作成する必要があります。準備されたイメージバージョン仕様を、同じホスティング接続内の別のホスティングユニットと共有することもできます。

要件

- Windowsマスターイメージの場合、VDAイメージバージョン2311以降のみがサポートされます。MCS/IOコンポーネントは明示的に選択してインストールする必要があります。MCS I/O構成の有効化または無効化は、デフォルトでは有効になっていないため、マシンカタログの作成または更新時に決定する必要があります。

制限事項

現在、この機能は以下をサポートしていません。

- Azureでの複数のNIC
- 永続データディスク機能
- マルチセッションの休止状態
- イメージタイプの変更
- Azure のホスティングユニット間で準備済みイメージバージョンを共有する場合、以下の共有方法は許可されていません。
  - 直接共有
  - パブリックコミュニティギャラリーに共有
- 現在、Azure 機密 VM はイメージ管理でサポートされていません。

Web Studio を使用したイメージライフサイクル管理

Web Studio を使用する場合のイメージのライフサイクルは次のとおりです。

1. 準備済みイメージの作成: イメージ定義とその初期イメージバージョンを作成します。
2. 初期イメージバージョンからイメージバージョンを作成します。
3. 他のホスティングユニットでイメージバージョンを使用したい場合は、同じホスティング接続内の別のホスティングユニットとイメージバージョンを共有します。
4. イメージバージョンを準備済みイメージとして使用して、カタログを作成します。
5. 別の準備済みイメージでマシンカタログを更新します。
6. イメージ定義とバージョンを管理する: イメージバージョンの名前と説明、およびイメージ定義の説明を編集します。
7. イメージバージョンを削除します。
8. イメージ定義を削除する。

あるいは、PowerShell を使用してイメージを管理することもできます。(#image-lifecycle-management-using-powershell)を参照してください。

PowerShell を使用したイメージのライフサイクル管理

PowerShell コマンドを使用してプロビジョニングスキームを作成する場合は、環境の必要に応じて、マスターイメージバージョン仕様に基づいて準備済みイメージバージョン仕様を作成する必要があります。

マスターイメージバージョン仕様: マスターイメージバージョン仕様は、イメージバージョンに追加または作成された特定のイメージです。ハイパーバイザー内の既存のイメージをマスターイメージバージョン仕様として追加するか、環境の必要に応じてマスターイメージバージョン仕様に基づいて準備済みイメージバージョン仕様を作成できます。準備済みイメージバージョン仕様は、複数のプロビジョニングスキームに使用できます。

AzureおよびVMware環境では、同じホスティング接続内のホスティングユニット間で準備済みイメージバージョンスペックを共有することもできます。Azureでは、Azure Compute Gallery (ACG) のディスク共有機能を使用して共有が実現されます。

PowerShellコマンドを使用する場合のイメージのライフサイクルは次のとおりです。

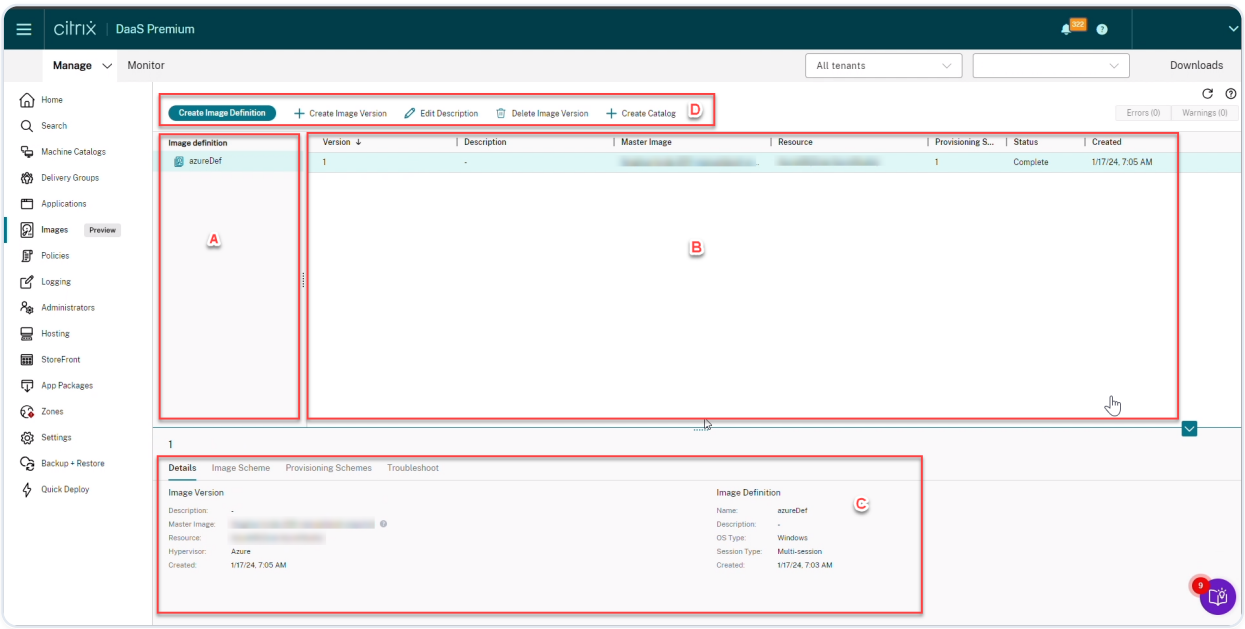
1. イメージを作成する:
    a. イメージ定義を作成する。
    b. 指定されたホスティング接続にイメージ定義の新しい構成を追加する。
    c. イメージバージョンを作成する。
    d. マスターイメージバージョン仕様を追加する。
    e. 準備済みイメージバージョン仕様を作成する。
2. 他のホスティングユニットでイメージバージョンを使用する場合は、同じホスティング接続内の別のホスティングユニットと準備済みイメージバージョン仕様を共有する。
3. 準備済みイメージバージョン仕様を使用して MCS マシンカタログを作成する:
    a. ブローカーカタログを作成します。
    b. IDプールを作成します。
    c. `New-ProvScheme`コマンドを使用して、準備済みイメージバージョン仕様のUidパラメーターを持つプロビジョニングスキームを作成します。
    d. ブローカーカタログをプロビジョニングスキームにリンクします。
4. MCSマシンカタログにVMを作成します。
5. `Set-ProvScheme` コマンドを使用して、プロビジョニングスキームの準備済みイメージバージョンスペックを変更します。
6. イメージ定義とバージョンを管理する: イメージバージョンとイメージ定義を編集します。
7. MCSマシンカタログを削除する: 削除順序は、マシンカタログ > 共有準備済みイメージバージョン仕様 (イメージ共有の場合) > 準備済みイメージバージョン仕様 > マスターイメージバージョン仕様 > イメージバージョン > 指定されたホスティング接続内のイメージ定義の構成 >

イメージ定義です。イメージバージョン仕様を削除する前に、準備済みイメージバージョン仕様がどのMCSマシンカタログとも関連付けられていないことを確認してください。

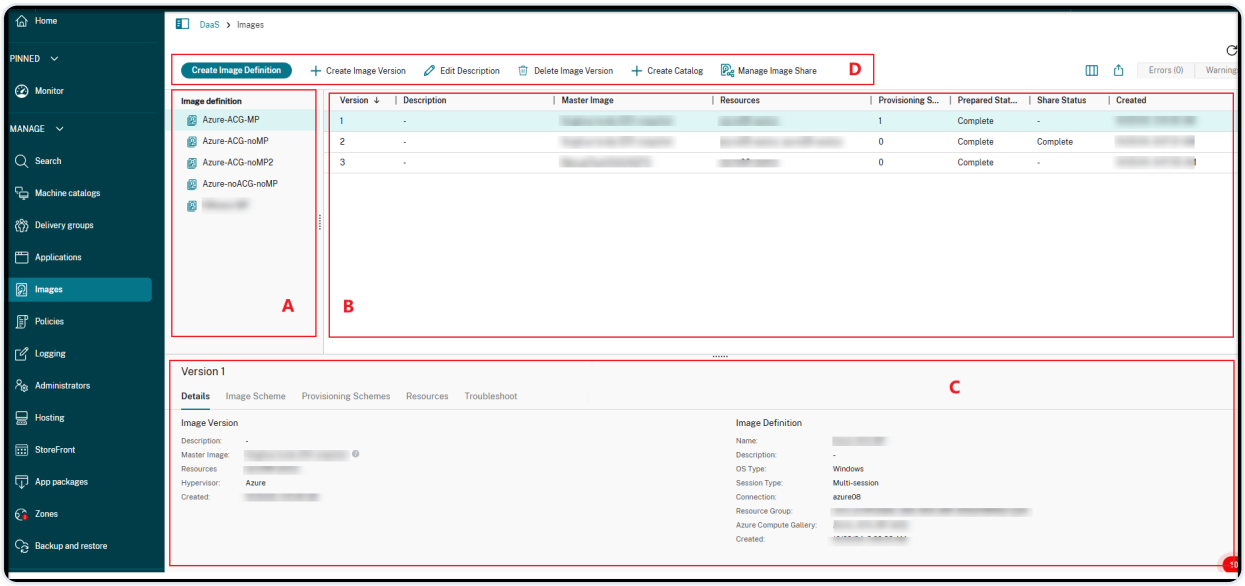
イメージノードについて理解する

イメージノードを使用して、MCSで準備されたイメージを作成および管理します。そのメインビューは4つの部分に分かれています:

- ホストユニット間で準備済みイメージが共有されていない場合



- ホストユニット間で準備済みイメージが共有されている場合:



ラベル	部分	説明
A	イメージ定義	以前に作成されたイメージ定義を一覧表示します。
B	イメージバージョン	選択したイメージ定義のイメージバージョンを表示します。
C	詳細	• **詳細**タブには、選択したイメージ定義またはバージョンに関する詳細情報（マスターイメージ、リソース、ハイパーバイザー、イメージ定義の名前、OSタイプ、セッションタイプなど）が表示されます。 • **イメージスキーム**タブには、ハードディスク、マシンサイズ、ライセンスタイプ、ディスク暗号化セット、マシンプロファイルなど、イメージの準備に使用されるテンプレートに関

ラベル	部分	説明	
		する情報が表示されます。 • 「**プロビジョニングスキーム**」タブには、カタログの作成に使用されたプロビジョニングスキーム名が表示されます。 • 「**トラブルシューティング**」タブには、選択したイメージバージョンのエラー状態が表示されます。 • イメージ共有の場合：「**リソース**」タブには、イメージバージョンの共有の状態が表示されます。	
D	アクションバー	イメージ定義とバージョンに対して実行できるアクション（**イメージバージョンの作成**、**説明の編集**、**イメージ共有の管理**（準備済みイメージ共有の場合）、**イメージバージョンの削除**、**カタログの作**	

ラベル	部分	説明
		成など）を一覧表示します。

次のステップ

準備済みイメージマシンカタログを作成する

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

準備済みイメージのマシンカタログを作成する

準備済みイメージを作成し、その準備済みイメージを使用して、次の方法でMCSマシンカタログを作成します。

- ウェブスタジオ
- PowerShellコマンド

現在、AzureおよびVMware仮想化環境で、準備済みイメージマシンカタログを作成できます。

詳細情報

- イメージ管理

次のステップ

- Azureで準備済みイメージのマシンカタログを作成する
- VMwareで準備済みイメージのマシンカタログを作成する
- 準備済みイメージマシンカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/manage-prepared-image-machine-catalogs.html)

Azure で準備済みイメージのマシンカタログを作成する

準備済みイメージを作成し、その準備済みイメージを使用して、次の方法で MCS マシンカタログを作成します。

- ウェブスタジオ
- PowerShell コマンド

準備済みイメージを使用して MCS マシンカタログを作成する主な手順は次のとおりです。

1. イメージ定義と初期イメージバージョンを作成します。
2. イメージバージョンを準備済みイメージとして使用してカタログを作成します。

Web Studio を使用する

イメージ定義と初期イメージバージョンを作成する

イメージ定義と初期イメージバージョンを作成するには、次の手順を実行します。

1. Web Studio で、 ノードに移動し、 をクリックします。 ページで をクリックします。
2. ページで、イメージ定義の と を指定します。
3. 既存のリソースグループを選択するか、イメージリソースを保持するための新しいリソースグループを作成します。イメージ共有を有効にするには、Azure Compute Gallery で を選択し、新しいギャラリーを作成するか、既存のギャラリーを使用してイメージバージョンを保持するかを選択します。
4. ページで、 (設定された接続に適用可能なリソースのみが一覧表示されます) と、イメージバージョンを作成するためのテンプレートとして使用するマスターイメージを選択します。 チェックボックスをオンにして、マシンプロファイルを選択できます。

   > **注:**
   >
   > イメージを選択する前に、マスターイメージにVDA 2311以降がインストールされており、MCSIOドライバーがVDAにインストールされていることを確認してください。

5. **ストレージとライセンスの種類**ページで、イメージ準備プロセスの一部として使用するストレージとライセンスの種類を選択します。

   > **注:**
   >
   > **イメージ**ページでマシンプロファイルを選択すると、プロファイル設定に基づいてマシンプロファイルのライセンスタイプが事前に選択されます。

6. **マシン仕様**ページで、マシンサイズを選択します。**イメージ**ページでマシンプロファイルを選択すると、マシンプロファイルのマシンサイズがデフォルトで選択されます。
7. **NIC**ページで、準備イメージのNICを選択または追加します。各NICについて、関連する仮想ネットワークを選択します。

8. **ディスク設定**ページで、顧客管理の暗号化キー（CMEK）を選択します。マシンプロファイルにCMEKがないが、マスターイメージにある場合は、マスターイメージからCMEKが事前に選択されます。
9. 「**Version Description**」ページで、作成された初期イメージバージョンの説明を入力します。
10. 「**概要**」ページで、イメージ定義と作成された初期イメージバージョンの詳細を確認します。イメージ定義の名前と説明を入力します。「**完了**」をクリックします。

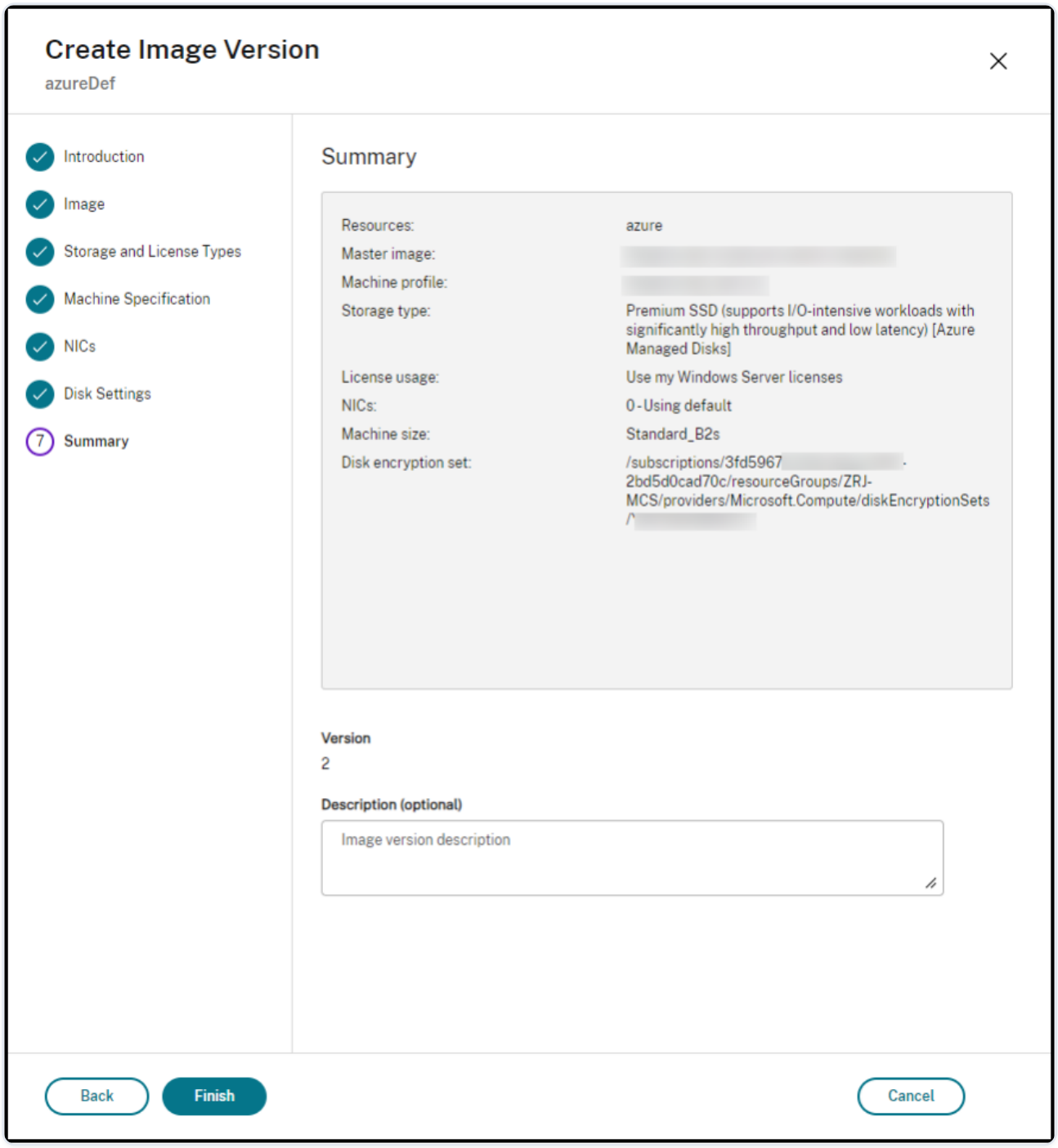
イメージバージョンを作成する

イメージバージョンを使用すると、特定のイメージに対するさまざまなイテレーションや更新を管理できます。この機能により、さまざまな目的のためにイメージの複数のバージョンを維持できます。

初期イメージバージョンからイメージバージョンを作成するには、次の手順を実行します。

> **注:**
>
> すべてのイメージバージョンのホスティングユニットは同じである必要があります。

1. ノードに移動し、イメージバージョンまたはイメージ定義を選択して、 をクリックします。
2. 「イメージ定義」ページで、ホスティングユニットを変更し、そのイメージバージョン用のマスターイメージとマシンプロファイルを再選択できます。
3. イメージバージョンの構成を、最初に構成されたイメージバージョンと異なるものにしたい場合は、「**イメージバージョンの作成**」ダイアログの「**ストレージとライセンスの種類**」、「**マシン仕様**」、「**NIC**」、「**ディスク設定**」ページで設定を構成します。
4. イメージバージョンの説明を追加します。「**完了**」をクリックします。



注：

何らかの理由でイメージバージョンの作成に失敗した場合、下部にある「**トラブルシューティング**」タブに「**再試行**」オプションが表示されます。

共有準備済みイメージ

Azure の異なるホストユニット間で準備済みイメージを共有するには、次の手順に従います。

1. イメージバージョンを右クリックし、「**イメージ共有の管理**」を選択します。選択した接続下のすべてのホストユニットが一覧表示されます。イメージバージョンが作成されたリソースは、すべてのアクションに対して無効になっています。
2. イメージを共有するホストユニットを選択し、「**保存**」をクリックします。「**共有ステータス**」列に「進行中」と表示されます。
3. 共有ステータスの詳細については、「**リソース**」タブをクリックします。

> **注：**
>
> イメージバージョンの共有のステータスが進行中の場合、**イメージバージョンの削除**または**イメージ共有の管理**のオプションは無効になります。

イメージノードからマシンカタログを作成する

「**イメージ**」ノードの「**カタログの作成**」オプションを使用して、イメージバージョンでカタログを作成します。

または、**マシンカタログ**ノードでカタログを作成する際にバージョンを選択し、カタログ作成ワークフローの準備済みイメージオプションにリンクすることもできます。詳細については、マシンカタログノードからマシンカタログを作成するを参照してください。

「**イメージ**」ノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. イメージバージョンを選択し、「**カタログの作成**」をクリックします。「**はじめに**」ページで「**次へ**」をクリックします。
2. **デスクトップエクスペリエンス**ページで、必要なデスクトップエクスペリエンスを選択します。
3. **イメージ**ページから**ディスク設定**ページまで、設定は選択したイメージバージョンに基づいて事前に選択されています。
4. **リソースグループ**ページで、新しいリソースグループを作成するか、既存のリソースグループを使用してこのカタログのリソースを配置するかを選択できます。
5. 次のページで設定を完了します。
6. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。
7. 作成されたマシンカタログを表示するには、**マシンカタログ**ノードに移動します。

「マシンカタログ」ノードからマシンカタログを作成する

マシンカタログノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. 左側のナビゲーションペインで**マシンカタログ**をクリックします。
2. **マシンカタログの作成**をクリックします。**マシンカタログのセットアップ**ページが表示されます。**はじめに**、**マシンタイプ**、および**マシン管理**の各ページで**次へ**をクリックします。
3. **イメージ**ページで:
    a. **準備済みイメージ**を選択します。
    b. 「**準備済みイメージ**」の下で、イメージ定義のイメージバージョンを選択します。
    c. イメージバージョン名をクリックします。選択したイメージバージョンの詳細を表示するには、下線が引かれているバージョン番号をクリックします。
    d. 選択したイメージバージョンがマシンプロファイルで構成されている場合は、マシンプロファイルを選択します。選択したイメージバージョンがマシンプロファイルで構成されていない場合、マシンプロファイルを使用することはできません。
4. 次のページで設定を構成します。
5. 「**ディスク設定**」ページで、選択した準備済みイメージがディスク暗号化セットを使用している場合、暗号化セットを削除することはできませんが、キーを別の暗号化キーに変更することはできます。
6. 「**リソースグループ**」ページで、新しいリソースグループを作成するか、既存のリソースグループを使用してこのカタログのリソースを配置するかを選択できます。
7. 次のページで設定を完了します。
8. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。

PowerShell を使用する

準備済みイメージを作成する

準備済みイメージバージョン仕様を作成するための詳細な PowerShell コマンドは次のとおりです。

1. `Test-ProvImageDefinitionNameAvailable command`を使用して、利用可能なイメージ定義名を確認します。例:

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
```

2. `New-ProvImageDefinition`コマンドを使用してイメージ定義を作成します。例:

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession
```

3. `Add-ProvImageDefinitionConnection` コマンドを使用して、指定されたホスティング接続でイメージ定義の新しい構成を作成します。

   `Add-ProvImageDefinitionConnection`の`CustomProperties`には、次のものが含まれます。パラメーターを使用しない場合、デフォルト値が使用されます。

   - `ResourceGroups`: ベースディスクがあるリソースグループ。
   - `UseSharedImageGallery`: ベースディスクの種類のインジケーター。ACG (イメージ共有) には `true` を、スナップショットには `false` を使用します。
   - `ImageGallery`: ベースディスクがACGイメージバージョンである場合のギャラリー名。

   例:

   - スナップショットと顧客が提供するリソースグループの場合:

```
$CustomerOwnRsourceGroupProperties = @"

<CustomProperties xmlns="http:// schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="yangj_image" />

</CustomProperties>

"@
```

   - ACGと顧客が提供するリソースグループおよびイメージギャラリーの場合:

```
$CustomerOwnAllProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
```

```
<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="rg" />

<Property xsi:type="StringProperty" Name="ImageGallery"
Value="gallery" />

</CustomProperties>

"@
```

- ACGと顧客が提供するリソースグループのみの場合:

```
$CustomerOwnResourceGroupProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="rg" />

</CustomProperties>

"@
```

- ACGとCitrix®が管理するリソースグループおよびイメージギャラリーの場合:

```
$CustomerOwnResourceGroupNothingProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />
```

```
</CustomProperties>

"@
```

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName Azure28 [-CustomProperties $CustomProperties]
```

4. `New-ProvImageVersion` コマンドを使用してイメージバージョンを作成します。例:

```
New-ProvImageVersion -ImageDefinitionName image1 -Description "version
1"
```

5. `Add-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様をイメージバージョンに追加します。例:

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
ImageVersionNumber  1 -HostingUnitName azure -MasterImagePath "XDHyp:
\HostingUnits\azure\image.folder\azureresourcegroup.resourcegroup\win20
22-snapshot.snapshot"
```

注:

ホスティングユニットの1つのイメージバージョンには、1つのマスターイメージバージョン仕様のみを追加できます。

6. `New-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様から準備済みイメージバージョン仕様を作成します。例:

```
New-ProvImageVersionSpec

-SourceImageVersionSpecUid  c6e7384c-b2f8-46d6-9519-29a2c57ed3cb

-NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resou
rcegroup\azure-vnet-eastus.virtualprivatecloud\dev.network"}

-ServiceOffering"XDHyp:
```

```
\HostingUnits\azure\serviceoffering.folder\Standard_B2ms.serviceofferin
g" -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"></CustomProperties>"
-RunAsynchronously
```

7. `Add-ProvImageVersionSpecHostingUnit` コマンドを使用して、同じホスティング接続内の別のホスティングユニットと準備済みイメージバージョン仕様を共有することもできます。例:

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName AzureWest
```

注:

1つのホスティングユニットと準備タイプには、準備済みインスタンスを1つのみ持つことができます。

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を作成するための PowerShell コマンドの完全なセットの例:

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession



$CustomProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

    <Property xsi:type="StringProperty" Name="ResourceGroups" Value="rg" /
>

    <Property xsi:type="StringProperty" Name="ImageGallery"
Value="gallery" />
```

```
</CustomProperties>

"@



Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName Azure28 -CustomProperties $CustomProperties



$imageVersion = New-ProvImageVersion -ImageDefinitionName image1
-Description "version 1"



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -MasterImagePath "XDHyp:
\HostingUnits\azure28\image.folder\abc.resourcegroup\def-
snapshot.snapshot"



New-ProvImageVersionSpec -NetworkMapping @{"0" = "XDHyp:
\HostingUnits\azure28\virtualprivatecloud.folder\East
US.region\virtualprivatecloud.folder\studio-mcs-
infrastructure.resourcegroup\studio-mcs-vnet-
eastus.virtualprivatecloud\mcs-dev.network" } -CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Server`" /></CustomProperties>" -ServiceOffering "XDHyp:
\HostingUnits\azure28\serviceoffering.folder\Standard_B2s.serviceoffering"
-SourceImageVersionSpecUid $SourceImageVersionSpec.ImageVersionSpecUid

Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName AzureWest

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
```

```
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

注:

- イメージ定義内のすべてのイメージバージョン仕様は、同じホスティングユニットに属している必要があります。
- イメージバージョンには、マスターイメージバージョン仕様を1つと、準備済みイメージバージョン仕様を1つのみ含めることができます。
- すべてのイメージバージョン仕様はマシンプロファイルを持つか、またはどのイメージバージョン仕様もマシンプロファイルを持たないかのいずれかである必要があります。

準備済みイメージバージョン仕様を使用してカタログを作成する

`New-ProvScheme` コマンドを使用して、準備済みイメージバージョン仕様から MCS マシンカタログを作成します。例:

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

または、,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
```

```
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

ACGイメージバージョン仕様を使用する場合は、`UseSharedImageGallery` を `true` に設定します。例：

```
$provSchemeCustomProperties= @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

    <Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" />

</CustomProperties>

"@

New-ProvScheme -ProvisioningSchemeName assignimage -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -IdentityPoolUid $IdentityPool.IdentityPoolUid `

    -CleanOnBoot -Scope @() -SecurityGroup @() `

    -ServiceOffering "XDHyp:
\HostingUnits\azure28\serviceoffering.folder\Standard_B2s.serviceoffering"
`

    -NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure28\virtualprivatecloud.folder\East
US.region\virtualprivatecloud.folder\studio-mcs-
infrastructure.resourcegroup\studio-mcs-vnet-
eastus.virtualprivatecloud\mcs-dev.network"} `

    -CustomProperties $provSchemeCustomProperties
```

カタログを作成するためのPowershellコマンドの完全なセットの例：

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "azurecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"



$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "azure.local"
-IdentityPoolName "azurecatalog" -IdentityType "ActiveDirectory"  -
NamingScheme "azure##" -NamingSchemeType "Numeric" -Scope @()



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



$Task = New-ProvScheme -ProvisioningSchemeName azurecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName azure -IdentityPoolName azurecatalog -CleanOnBoot -Scope
@() -SecurityGroup @() -ServiceOffering "XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2s.serviceoffering"
-NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resource
group\azure-vnet-eastus.virtualprivatecloud\dev.network"}
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">    <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="true" /><Property
xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"StandardSSD_LRS`" /></CustomProperties>" -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName azurecatalog
```

```
Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

詳細情報

- イメージ管理

次のステップ

- 準備済みイメージマシンカタログの管理

VMware で準備済みイメージのマシンカタログを作成する

準備済みイメージを作成し、その準備済みイメージを使用して、次の方法でMCSマシンカタログを作成します。

- ウェブスタジオ
- PowerShell コマンド

準備済みイメージを使用して MCS マシンカタログを作成する主な手順は次のとおりです。

1. イメージ定義と初期イメージバージョンを作成します。
2. イメージバージョンを準備済みイメージとして使用してカタログを作成します。

Web Studio を使用する

イメージ定義と初期イメージバージョンを作成する

イメージ定義と初期イメージバージョンを作成するには、次の手順を実行します。

1. Studio から、**イメージ**ノードに移動し、**イメージ定義の作成**をクリックします。**はじめに**ページで**次へ**をクリックします。
2. **イメージ定義**ページで、イメージ定義の**OS タイプ**と**セッションタイプ**を指定します。
3. **イメージ**ページで、**リソース**（設定された接続に適用可能なリソースのみが一覧表示されます）と、イメージバージョンを作成するためのテンプレートとして使用するマスターイメージを選択します。**マシンプロファイルを使用**チェックボックスを選択し、マシンプロファイルを選択できます。

> **注:**

> イメージを選択する前に、マスターイメージにVDA 2311以降がインストールされており、MCSIOドライバーがVDAにインストールされていることを確認してください。

4. 「**マシン仕様**」ページで、マシンサイズを選択します。マシンプロファイルを選択した場合、マシンプロファイルから派生した仮想CPU数が表示され、変更できません。マシンプロファイルを選択しない場合、マスターイメージから派生したメモリサイズのみが表示されます。
5. 「**NIC**」ページで、準備イメージのNICを選択または追加します。各NICについて、関連付けられた仮想ネットワークを選択します。マシンプロファイルを選択しない場合、マスターイメージに関連付けられたNICがデフォルトで選択されます。マシンプロファイルを選択した場合、NICはマシンプロファイルから派生し、その数は変更できません。
6. 「**バージョン説明**」ページで、作成された初期イメージバージョンの説明を入力します。
7. 「**概要**」ページで、イメージ定義と作成された初期イメージバージョンの詳細を確認します。イメージ定義の名前と説明を入力します。「**完了**」をクリックします。

イメージバージョンを作成する

イメージバージョンを使用すると、特定のイメージに対するさまざまなイテレーションや更新を管理できます。この機能により、さまざまな目的のためにイメージの複数のバージョンを維持できます。

初期イメージバージョンからイメージバージョンを作成するには、次の手順を実行します。

1. 「**イメージ**」ノードに移動し、イメージバージョンまたはイメージ定義を選択して、「**イメージバージョンを作成**」をクリックします。
2. 「**イメージ**」ページでは、同じホスティング接続内でホスティングユニットを変更したり、そのイメージバージョンのマスターイメージとマシンプロファイルを再選択したりできます。
3. イメージバージョンの構成を最初に構成されたイメージバージョンと異なるようにしたい場合は、「**イメージバージョンを作成**」ダイアログの「**マシン仕様**」ページと「**NIC**」ページで設定を構成します。
4. イメージバージョンの説明を追加します。「**完了**」をクリックします。

> **注:**
>
> 何らかの理由でイメージバージョンの作成が失敗した場合、下部の「**トラブルシューティング**」タブに「**再試行**」オプションが表示されます。

準備済みイメージを共有する

前提条件

準備済みイメージの共有は、コールドマイグレーションを使用して vCenter Server インスタンス間でイメージを複製します。異なるホスティング接続に属するホスティングユニットには、次の前提条件が適用されます。

- vCenter Server 間でのコールドマイグレーション: コールドマイグレーションには、両方の環境でクロス vCenter マイグレーションのサポートが必要です。
  - 両方のvCenter ServerでvSphere 7.0以降が実行されている必要があります (vSphere 8.0以降を推奨)。
  - 拡張リンクモードは不要です。

  ポート要件: マイグレーションのために次のポートが開いていることを確認してください。

送信元	宛先	ポート	プロトコル	目的
送信元vCenter Server	ターゲットvCenter Server	443	TCP	vCenter間のAPI通信
ソースESXiホスト	ターゲットESXiホスト	902	TCP	NFC (ネットワークファイルコピー) データ転送
ソースESXiホスト	ターゲットESXiホスト	8000	TCP	vMotionトラフィック

> **注:**
>
> ポートは双方向に開いている必要があります。移行では主にデータにNFC (ポート902) を使用し、管理にポート443を使用します。パスによってはポート8000が使用される場合があります。クローン操作中に、ソースvCenterはターゲットのSSL証明書サムプリントを検証する必要があります。

> VMkernelアダプターの構成:

ESXIホスト	必要なサービス
ソースESXiホスト	プロビジョニングまたは管理
ターゲットESXiホスト	ソースと同じサービス (プロビジョニングまたは管理)

両側でVMkernelアダプターに同じトラフィックサービス（プロビジョニングまたは管理）を有効にする必要があります。不一致は移行の失敗を引き起こします。

vSphere Clientで、**ホスト > 構成 > ネットワーク > VMkernelアダプター** の下を確認してください。

既知の制限事項：カスタムストレージポリシーは、vCenter間レプリケーション中に保持されません。ターゲットデータストアのデフォルトストレージポリシーが適用されます。

- vTPM対応マシンプロファイル：キープロバイダーの互換性。vTPMを持つプロファイルの場合、両方のvCenter Serverが互換性のあるキープロバイダーにアクセスできる必要があります。

要件	詳細
同じキープロバイダーへのアクセス	宛先vCenterは、ソースと同じキープロバイダーにアクセスできるか、ネイティブキープロバイダーをブリッジとして使用できる必要があります
キーマテリアル	外部KMSの場合: 両方のvCenterは同じKMSクラスター (またはキーマテリアルを共有するKMSクラスター) に登録されている必要があります。
ネイティブキープロバイダー	両方のvCenter ServerでNative Key Providerを構成します。各vCenterのNative Key Providerは独立していますが、vSphereはこの組み合わせをvCenter間操作で受け入れます。Native Key Providerは、ソースと宛先が外部KMSを共有していない場合、ブリッジとしても機能します。Native Key Providerは、使用する前に両方のvCenterでバックアップする必要があります。

注:

Native Key Providerは最も簡単なオプションです。両方のサーバーで構成し、バックアップしてください。外部KMSを使用する場合は、両方のvCenterが同じクラスターまたはキーマテリアルを共有していることを確認してください。vTPM対応カタログのイメージ共有を有効にする前に、**vSphere ClientのvCenter > Configure > Security > Key Providers**でKey Providerの構成を確認してください。

異なるホストユニット間で準備済みイメージを共有する

異なるホストユニット間で準備済みイメージを共有するには、次の手順に従ってください。

1. イメージバージョンを右クリックし、**Manage Image Share**を選択します。選択した接続下のすべてのホストユニットが一覧表示されます。イメージバージョンが作成されたリソースは、いかなる操作も無効になっています。
2. イメージを共有したいホストユニットを選択し、**Save**をクリックします。 **Share Status**列に**In progress**と表示されます。
3. 共有ステータスの詳細については、下部にある**Resources**タブをクリックします。

注:

イメージバージョンの共有ステータスが進行中の場合、**Delete Image Version**または**Manage Image Share**のオプションは無効になります。

Imagesノードからマシンカタログを作成する

Imagesノードの**Create catalog**オプションを使用して、イメージバージョンでカタログを作成します。

または、**Machine Catalogs**ノードでカタログを作成する際にバージョンを選択し、カタログ作成ワークフローの準備済みイメージオプションにリンクすることもできます。「Machine Catalogsノードからマシンカタログを作成する」を参照してください。

ImagesノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. イメージバージョンを選択し、**Create catalog**をクリックします。**Introduction**ページで**Next**をクリックします。
2. 「**デスクトップエクスペリエンス**」ページで、必要なデスクトップエクスペリエンスを選択します。

3. 「**イメージ**」ページから「**仮想マシン**」ページまで、設定は選択したイメージバージョンに基づいて事前に選択されています。
4. 次のページで設定を完了します。
5. 「**概要**」ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。「**完了**」をクリックします。
6. 作成したマシンカタログを表示するには、「**マシンカタログ**」ノードに移動します。

「マシンカタログ」ノードからマシンカタログを作成する

マシンカタログノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. 左側のナビゲーションペインで**マシンカタログ**をクリックします。
2. **マシンカタログの作成**をクリックします。**マシンカタログのセットアップ**ページが表示されます。**はじめに**、**マシンタイプ**、**マシン管理**の各ページで**次へ**をクリックします。
3. **イメージ**ページで：
    a. **準備済みイメージ**を選択します。
    b. 「**準備済みイメージ**」の下で、イメージ定義のイメージバージョンを選択します。
    c. イメージバージョン名をクリックします。選択したイメージバージョンの詳細を表示するには、下線が引かれているバージョン番号をクリックします。
    d. 選択したイメージバージョンがマシンプロファイルで構成されている場合は、マシンプロファイルを選択します。選択したイメージバージョンがマシンプロファイルで構成されていない場合、マシンプロファイルを使用することを選択できません。
4. 次のページで設定を構成します。
5. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。

PowerShell の使用

準備済みイメージの作成

準備済みイメージバージョン仕様を作成するための詳細な PowerShell コマンドは次のとおりです。

1. `Test-ProvImageDefinitionNameAvailable command` を使用して、利用可能なイメージ定義名を確認します。例:

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
```

2. `New-ProvImageDefinition` コマンドを使用してイメージ定義を作成します。例:

```
New-ProvImageDefinition -ImageDefinitionName image2 -OsType Windows
-VdaSessionSupport SingleSession
```

3. `Add-ProvImageDefinitionConnection` コマンドを使用して、指定されたホスティング接続でイメージ定義の新しい構成を作成します。例:

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image2
-HypervisorConnectionName VMware
```

4. `New-ProvImageVersion` コマンドを使用してイメージバージョンを作成します。例:

```
New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"
```

5. `Add-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様をイメージバージョンに追加します。例:

```
$MasterImagePath = "XDHyp:\HostingUnits\vmware\win10-master.vm\win10-
master-snap.snapshot"

$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageVersion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName vmware
-MasterImagePath $MasterImagePath
```

> **注:**
>
> ホスティングユニットの1つのイメージバージョンには、マスターイメージバージョン仕様を1つだけ追加できます。

6. `New-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様から準備済みイメージバージョン仕様を作成します。例:

```
New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping
@{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-VM Network.network"}
-VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
```

7. `Add-ProvImageVersionSpecHostingUnit` コマンドを使用して、同じホスティング接続内の別のホスティングユニットと準備済みイメージバージョン仕様を共有することもできます。例:

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName VMwareabc
```

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を作成するための PowerShell コマンドの完全なセットの例:

```
New-ProvImageDefinition -ImageDefinitionName image2 -OsType Windows
-VdaSessionSupport Single



Add-ProvImageDefinitionConnection -ImageDefinitionName image2
-HypervisorConnectionName VMware



$imageVersion = New-ProvImageVersion -ImageDefinitionName image2



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -MasterImagePath "XDHyp:\HostingUnits\vmware\shuaiz-win10-
master.vm\shuaiz-win10-master-snap.snapshot"



New-ProvImageVersionSpec -SourceImageVersionSpecUid
$SourceImageVersionSpec.ImageVersionSpecUid `
```

```
    -NetworkMapping @{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-
VMNetwork.network"} `

    -VMCpuCount 2 -VMMemoryMB 4096




Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName VMwareabc

 $PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

注:

- イメージ定義内のすべてのイメージバージョン仕様は、同じホスティングユニットに属している必要があります。
- イメージバージョンには、マスターイメージバージョン仕様を1つ、準備済みイメージバージョン仕様を1つだけ含めることができます。
- すべてのイメージバージョン仕様はマシンプロファイルを持つか、またはどのイメージバージョン仕様もマシンプロファイルを持たないかのいずれかである必要があります。

準備済みイメージバージョン仕様を使用してカタログを作成する

`New-ProvScheme` コマンドを使用して、準備済みイメージバージョン仕様から MCS マシンカタログを作成します。例:

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
```

```
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

または、,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

VMwareで準備されたイメージバージョンの仕様を使用してカタログを作成する例:

```
New-ProvScheme -ProvisioningSchemeName assignimage -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid `

    -HostingUnitName $hostingunit.c-IdentityPoolName
$IdentityPool.IdentityPoolName `

    -CleanOnBoot -Scope @() -SecurityGroup @() -VMCpuCount 2 -VMMemoryMB
8192 `

    -NetworkMapping @{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-VM
Network.network"}
```

カタログを作成するためのPowershellコマンドの完全なセットの例：

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "vmwarecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"

$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain
"vmware.local" -IdentityPoolName "vmwarecatalog" -IdentityType
"ActiveDirectory"  -NamingScheme "vmware##" -NamingSchemeType "Numeric"
-Scope @()
```

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image2 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"

$Task = New-ProvScheme -ProvisioningSchemeName vmwarecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName vmware -IdentityPoolName vmwarecatalog -CleanOnBoot
-Scope @() -SecurityGroup @() -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vmware\\DSwitch-VM Network.network"} -VMCpuCount 2
-VMMemoryMB 4096 -RunAsynchronously

Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName vmwarecatalog

Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

詳細情報

- イメージ管理

次のステップ

- 準備済みイメージマシンカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/manage-prepared-image-machine-catalogs.html)

準備済みイメージのマシンカタログを管理する

既存のMCSマシンカタログを別の準備済みイメージで更新し、イメージの定義とバージョンを管理するには、次の方法を使用します。

- ウェブスタジオ
- PowerShell

Web Studioを使用する

マシンカタログを別の準備済みイメージで更新する

既存のMCSマシンカタログを別の準備済みイメージで更新するには、次の手順を実行します。

1. 左側のナビゲーションペインで をクリックし、更新するマシンカタログを選択します。右クリックして を選択します。

2. **イメージ**ページで、準備済みイメージを選択します。

> **注:**
>
> Azureに適用可能：ACGが有効になっていないイメージを選択し、後で チェックボックスをオンにして、イメージをギャラリーに配置することもできます。

3. **ロールアウト戦略**ページで、選択した準備済みイメージでこのカタログを更新するタイミングを選択します。
4. ページで詳細を確認します。 をクリックします。

カタログに対して行われたイメージ変更の履歴を確認できます。履歴を確認するには、次の手順を実行します。

1. マシンカタログを選択します。
2. タブの フィールドで、 をクリックします。

イメージ定義とバージョンを管理する

イメージ定義とバージョンを編集および削除して、作成されたさまざまなイメージバージョンと定義の使用を管理できます。

イメージ定義を編集する

イメージ定義の名前と説明を編集できます。

イメージ定義を編集するには、次の手順を実行します。

1. **イメージ**ノードに移動し、イメージ定義を選択して、**イメージ定義の編集**を選択します。

イメージバージョンを編集する

イメージバージョンの説明を編集して、そのイメージバージョンの目的を指定できます。

イメージバージョンを編集するには、次の手順を実行します。

1. **イメージ**ノードに移動し、イメージバージョンを選択して、**説明の編集**を選択します。

イメージバージョンを削除する

イメージバージョンを削除するには、次の手順を実行します。

1. **イメージ**ノードに移動し、イメージバージョンを選択して、**イメージバージョンの削除**を選択します。

> **注:**
>
> マシンカタログで使用されているイメージバージョンは削除できません。

イメージ定義を削除する

イメージ定義を削除するには、次の手順を実行します。

1. **イメージ**ノードに移動し、イメージ定義を選択して、**イメージ定義の削除**を選択します。

> **注:**
>
> イメージバージョンが含まれているイメージ定義は削除できません。

PowerShell を使用する

準備済みイメージバージョン仕様を使用してカタログを更新する

`Set-ProvSchemeImage` コマンドを使用してカタログを更新できます。例:

```
Set-ProvSchemeImage -ProvisioningSchemeUid <Guid> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess]
```

または、,

```
Set-ProvSchemeImage -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess]
```

カタログを更新するための PowerShell コマンドの完全なセットの例:

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 2 -Filter "PreparationType -eq 'Mcs'"



Set-ProvSchemeImage -ProvisioningSchemeName azurecatalog
```

```
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-RunAsynchronously
```

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を削除する

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を削除する前に、以下を考慮してください。

- イメージバージョンが含まれているイメージ定義は削除できません。
- イメージバージョン仕様が含まれているイメージバージョンは削除できません。
- マスターイメージバージョン仕様が他の準備済みイメージバージョン仕様で使用されている場合、削除できません。
- 準備済みイメージバージョン仕様がMCSマシンカタログで使用されている場合、削除できません。
- ホスティングユニットが他の準備済みイメージバージョン仕様で使用されている場合、削除できません。

詳細な手順は次のとおりです。

1. マシンカタログを削除します。例:

```
Remove-ProvScheme -ProvisioningScheneName decouplingCatalog
```

2. 共有準備済みイメージバージョン仕様を削除します。例:

```
Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid <uid>
-HostingUnitName AzureWest
```

3. 準備済みイメージバージョン仕様を削除します。例:

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec
-ImageDefinitionName image1 -ImageVersionNumber 1 -Filter
"PreparationType -eq 'Mcs'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
```

4. マスターイメージバージョン仕様を削除します。例:

```
$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronousl
```

> **注:**
>
> マスターイメージバージョン仕様は、関連付けられた準備済みイメージバージョン仕様がない場合にのみ削除できます。

5. イメージバージョンを削除します。例:

```
Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber
1
```

6. 指定されたホスティング接続でイメージ定義の構成を削除します。例:

```
Remove-ProvImageDefinitionConnection -ImageDefinitionName xx
-HypervisorConnectionName xxx
```

7. イメージ定義を削除します。例:

```
Remove-ProvImageDefinition -ImageDefinitionName image1
```

準備済みイメージがホストユニット間で共有されていない場合のPowerShellコマンドの完全なセットの例:

```
Remove-ProvScheme -ProvisioningSchemeName decouplingCatalog



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"
```

```
Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously


$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"


Remove-ProvImageVersionSpec -ImageVersionSpecUid
$MasterImageVersionSpec.ImageVersionSpecUid -RunAsynchronously


Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber 1


Remove-ProvImageDefinition -ImageDefinitionName image1
```

準備済みイメージがホストユニット間で共有されている場合のPowerShellコマンドの完全なセットの例:

```
Remove-ProvScheme -ProvisioningSchemeName decouplingCatalog


Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid <uid>

-HostingUnitName AzureWest


$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"


Remove-ProvImageVersionSpec -ImageVersionSpecUid
```

```
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously



$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$MasterImageVersionSpec.ImageVersionSpecUid -RunAsynchronously



Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber 1



Remove-ProvImageDefinitionConnection -ImageDefinitionName xx
-HypervisorConnectionName xxx



Remove-ProvImageDefinition -ImageDefinitionName image1
```

イメージ定義とイメージバージョンの管理

イメージ定義の名前を変更および編集したり、イメージバージョンを編集したりできます。

- `Rename-ProvImageDefinition` コマンドを使用してイメージ定義の名前を変更します。例:

  ```
  Rename-ProvImageDefinition -ImageDefinitionUid <Guid>
  -NewImageDefinitionName <string>
  ```

  または、,

  ```
  Rename-ProvImageDefinition -ImageDefinitionName <string>
  -NewImageDefinitionName <string>
  ```

- `Set-ProvImageDefinition` コマンドを使用してイメージ定義を編集します。例:

```
Set-ProvImageDefinition -ImageDefinitionUid <Guid> [-Description
<string>]
```

または、,

```
Set-ProvImageDefinition -ImageDefinitionName <string> [-Description
<string>]
```

- `Set-ProvImageVersion` コマンドを使用してイメージバージョンを編集します。例:

```
Set-ProvImageVersion -ImageVersionUid <Guid> [-Description <string>]
```

または、,

```
Set-ProvImageVersion -ImageDefinitionName <string> -ImageVersionNumber
<int> [-Description <string>]
```

イメージ定義、イメージバージョン、準備されたイメージバージョンの仕様、およびプロビジョニングスキームの詳細を取得する

- `Get-ProvImageDefinition` コマンドを使用してイメージ定義の詳細を取得します。例:

```
Get-ProvImageDefinition [-ImageDefinitionName <string>] [-
ImageDefinitionUid <Guid>] [-ReturnTotalRecordCount] [-MaxRecordCount
<int>] [-Skip <int>] [-SortBy <string>] [-Filter <string>]
```

- `Get-ProvImageVersion` コマンドを使用してイメージバージョンの詳細を取得します。例:
  - イメージ定義内のイメージバージョンを一覧表示するには、,

    ```
    Get-ProvImageVersion -ImageDefinitionUid <Guid>
    ```

    または、,

    ```
    Get-ProvImageVersion -ImageDefinitionName <string>
    ```

  - イメージバージョンの詳細を取得するには、,

```
Get-ProvImageVersion -ImageVersionUid <Guid>
```

または、,

```
Get-ProvImageVersion -ImageDefinitionName <string>
-ImageVersionNumber <int>
```

- `Get-ProvImageVersionSpec` コマンドを使用して、準備済みイメージバージョン仕様を取得します。例:
  - イメージバージョン内のすべての準備済みイメージバージョン仕様を一覧表示するには、,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid>
```

  - 準備済みイメージバージョン仕様内のマスターイメージバージョン仕様を一覧表示するには、,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "None"'
```

  - マスターイメージに関連付けられているイメージバージョン内の準備済みイメージバージョン仕様を一覧表示するには、,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"'
```

  - イメージバージョン内の成功した準備済みイメージバージョン仕様を取得するには、,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" -and ImageVersionSpecStatus
-eq "Complete"'
```

  - 準備済みイメージバージョン仕様の詳細を取得するには、,

```
Get-ProvImageVersionSpec -ImageVersionSpecUid <Guid>
```

- `Get-ProvScheme` コマンドを使用して、プロビジョニングスキームの詳細を取得します。例:

```
Get-ProvScheme [[-ProvisioningSchemeName] <String>] [-
ProvisioningSchemeUid <Guid>] [-ScopeId <Guid>] [-ScopeName <String>]
[-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-
SortBy <String>] [-Filter <String>] [-FilterScope <Guid>]
```

- `Get-ProvSchemeImageVersionSpecHistory` コマンドを使用して、プロビジョニングスキームの準備済みイメージバージョン仕様の履歴を取得します。例:

```
Get-ProvSchemeImageVersionSpecHistory [-ProvisioningSchemeName
<String>] [-ProvisioningSchemeUid <Guid>] [-ImageVersionSpecUid <Guid>]
[-ImageVersionSpecHistoryUid <Guid>] [-ReturnTotalRecordCount] [-
MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter
<String>] [-FilterScope <Guid>]
```

詳細情報

- イメージ管理

マシンカタログを作成する

重要:

Citrix Virtual Apps and Desktops™ 7 2006以降、現在の展開で以下のいずれかのテクノロジーを使用している場合、それらのテクノロジーを使用するサポート終了（EOL）アイテムを削除した後にのみ、現在のリリースに展開をアップグレードできます。

- パーソナルvDisk (PvDs)
- AppDisks™
- パブリッククラウドホストの種類：Citrix CloudPlatform、Microsoft Azure Classic

詳細については、「PvD、AppDisks、およびサポートされていないホストの削除」を参照してください。

> **注:**
>
> Citrix Virtual Apps and Desktopsの展開は、Web Studio (Webベース) とCitrix Studio (Windowsベース) の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> 展開にパブリッククラウドホスト接続を使用する場合は、新規インストールまたは現在のリリースへのアップグレードを完了するためにHybrid Rights Licenseが必要です。

インストーラーがサポートされていないテクノロジーの1つ以上、またはHybrid Rights Licenseなしのホスト接続を検出すると、アップグレードは一時停止または停止します。説明メッセージが表示されます。インストーラーログには詳細が含まれています。詳細については、「展開のアップグレード」を参照してください。

はじめに

物理マシンまたは仮想マシンのコレクションは、マシンカタログと呼ばれる単一のエンティティとして管理されます。カタログ内のすべてのマシンは、マルチセッションOSまたはシングルセッションOS、およびWindowsまたはLinuxマシンといった、同じ種類のオペレーティングシステムを持っています。

Web Studioは、サイトを作成した後に最初のマシンカタログを作成するようガイドします。最初のカタログを作成した後、Web Studioは最初のデリバリーグループを作成するようガイドします。後で、作成したカタログを変更したり、さらにカタログを作成したりできます。

> **ヒント:**
>
> 既存の展開をアップグレードすると、Machine Creation Services (MCS) ストレージ最適化 (MCS I/O) 機能が有効になり、追加の構成は不要です。Virtual Delivery Agent (VDA) と Delivery Controller のアップグレードが MCS I/O のアップグレードを処理します。

概要

VM のカタログを作成するときは、それらの VM をプロビジョニングする方法を指定します。Machine Creation Services™ (MCS) を使用することも、独自のツールを使用してマシンを提供することもできます。

考慮事項:

- MCS は、仮想マシンイメージからの単一のシステムディスクをサポートします。そのイメージに接続されている残りのデータディスクは無視されます。
- MCS を使用して VM をプロビジョニングする場合、カタログに同一の VM を作成するためにマスターイメージ（またはイメージのスナップショット）を提供します。カタログを作成する前に、まずツールを使用してマスターイメージを作成および構成します。このプロセスには、イメージへの Virtual Delivery Agent (VDA) のインストールが含まれます。次に、Web Studio でマシンカタログを作成します。そのイメージ（またはスナップショット）を選択し、カタログに作成する VM の数を指定し、追加情報を構成します。
- マシンがすでに利用可能な場合でも、それらのマシン用に1つ以上のマシンカタログを作成する必要があります。
- PowerShell SDK を直接使用してカタログを作成する場合、イメージまたはスナップショットではなく、ハイパーバイザーテンプレート（**VMTemplates**）を指定できます。
- テンプレートを使用してカタログをプロビジョニングすることは、実験的な機能と見なされます。この方法を使用すると、仮想マシンの準備が失敗する可能性があります。その結果、テンプレートを使用してカタログを公開できません。

MCS または Citrix Provisioning™ を使用して最初のカタログを作成する場合、サイトを作成したときに構成したホスト接続を使用します。後で（最初のカタログとデリバリーグループを作成した後）、その接続に関する情報を変更したり、さらに接続を作成したりできます。

カタログ作成ウィザードを完了すると、正しく構成されていることを確認するためのテストが自動的に実行されます。テストが完了すると、テストレポートを表示できます。Web Studio からいつでもテストを実行できます。

> **注：**
>
> MCS は Windows 10 IoT Core および Windows 10 IoT Enterprise をサポートしていません。詳細については、Microsoft のサイト を参照してください。

> Citrix Provisioning ツールに関する技術的な詳細については、「Citrix Virtual Apps and Desktops Image Management」を参照してください。

RDS ライセンスチェック

Web Studioは現在、WindowsマルチセッションOSマシンを含むマシンカタログの作成中に、有効なMicrosoft RDSライセンスのチェックを実行しません。Windowsの**マルチセッションOSマシン**

のMicrosoft RDSライセンスのステータスを表示するには、Citrix Directorに移動します。**マシン詳細**パネルでMicrosoft RDSライセンスのステータスを表示します。このパネルは、**マシン詳細とユーザー詳細**ページにあります。詳細については、「Microsoft RDSライセンスの健全性」(/ja-jp/citrix-virtual-apps-desktops/2411/director/troubleshoot-deployments/machines.html#microsoft-rds-license-health)を参照してください。

VDA登録

ブローカーセッションを起動するときは、VDAをDelivery Controller™に登録する必要があります。未登録のVDAは、利用可能なリソースの利用率低下につながる可能性があります。VDAが登録されない理由はさまざまであり、その多くは管理者がトラブルシューティングできます。Web Studioは、カタログ作成ウィザードで、またカタログからデリバリーグループにマシンを追加した後に、トラブルシューティング情報を提供します。

ウィザードを使用して既存のマシンを追加すると、コンピューターアカウント名の一覧に、各マシンがカタログに追加するのに適しているかどうかが示されます。各マシンの横にあるアイコンにマウスカーソルを合わせると、そのマシンに関する情報メッセージが表示されます。

メッセージで問題のあるマシンが特定された場合は、そのマシンを削除するか、マシンを追加します。たとえば、マシンに関する情報が取得できない可能性があることを示すメッセージが表示された場合でも、マシンを追加します。

詳細については、以下を参照してください。

- VDA登録のトラブルシューティングガイダンスについては、CTX136668を参照してください。
- VDAのバージョンと機能レベル
- VDA登録方法

MCSカタログ作成の概要

カタログ作成ウィザードで情報を提供した後の、デフォルトのMCSアクションの概要を以下に示します。

- マスターイメージ（スナップショットではない）を選択した場合、MCSはスナップショットを作成します。
- MCSはスナップショットの完全なコピーを作成し、ホスト接続で定義されている各ストレージの場所にそのコピーを配置します。
- MCSはマシンをActive Directoryに追加し、一意のIDを作成します。

- MCSは、ウィザードで指定された数のVMを作成し、各VMに2つのディスクを定義します。各VMの2つのディスクに加えて、マスターも同じストレージの場所に保存されます。複数のストレージの場所が定義されている場合、それぞれに次のディスクタイプが割り当てられます。
  - 新しく作成されたVM間で共有される、読み取り専用のスナップショットの完全なコピー。
  - 各VMに一意のIDを付与する、一意の16 MBのIDディスク。各VMはIDディスクを取得します。
  - VMへの書き込みを保存するための一意の差分ディスク。このディスクはシンプロビジョニングされており（ホストストレージでサポートされている場合）、必要に応じてマスターイメージの最大サイズまで増加します。各VMは差分ディスクを取得します。差分ディスクにはセッション中に行われた変更が保持されます。専用デスクトップの場合は永続的です。プールされたデスクトップの場合、デリバリーコントローラーを介した再起動ごとに削除され、新しいものが作成されます。

あるいは、静的デスクトップを提供するためにVMを作成する場合、カタログ作成ウィザードの**マシン**ページで、シック（完全コピー）VMクローンを指定できます。完全クローンは、すべてのデータストアにマスターイメージを保持する必要はありません。各VMは独自のファイルを持っています。

MCSストレージに関する考慮事項

MCSのストレージソリューション、構成、容量を決定する際には、多くの要因があります。以下の情報は、ストレージ容量に関する適切な考慮事項を提供します。

容量に関する考慮事項:

- ディスク

  デルタディスクまたは差分ディスク（Diffディスク）は、ほとんどのMCS展開において、各VMで最大のスペースを消費します。MCSによって作成される各VMには、作成時に最低2つのディスクが割り当てられます。

  - Disk0 = 差分ディスク：マスターベースイメージからコピーされたOSが含まれます。
  - Disk1 = IDディスク: 16 MB - 各VMのActive Directoryデータを格納します。

  製品の進化に伴い、特定のユースケースや機能の消費を満たすために、さらにディスクを追加する必要がある場合があります。例:

  - MCS Storage Optimizationは、各VMにライトキャッシュスタイルのディスクを作成します。XenServer、VMware、およびSCVMM仮想化環境では、ホスト接続の作成時に利用可能なOSストレージリストと利用可能な一時ストレージリストを同じに構成した場合、

MCSはライトバックキャッシュ（WBC）ディスクをOSディスクと同じストレージ場所に配置します。

- MCSは、前のセクションで説明したデルタディスクのシナリオとは対照的に、フルクローンを使用する機能を追加しました。

ハイパーバイザーの機能も考慮に入れる必要があるかもしれません。例:

- XenServer IntelliCacheは、各XenServerのローカルストレージに読み取りディスクを作成します。このオプションにより、共有ストレージの場所に保持されている可能性のあるマスターイメージに対するIOPSを節約できます。

- ハイパーバイザーのオーバーヘッド

  異なるハイパーバイザーは、VM のオーバーヘッドを発生させる特定のファイルを使用します。ハイパーバイザーは、管理および一般的なログ記録操作にもストレージを使用します。オーバーヘッドを含めるスペースを計算します。

  - ログファイル
  - ハイパーバイザー固有のファイル。例:
    - VMware は、**VM storage** フォルダーにさらにファイルを追加します。VMware Best Practices を参照してください。
    - 仮想マシンの合計サイズ要件を計算します。仮想ディスクに 20 GB、スワップファイルに 16 GB、ログファイルに 100 MB を含む仮想マシンを考慮すると、合計で 36.1 GB を消費します。
  - XenServer のスナップショット; VMware のスナップショット。

- プロセスオーバーヘッド

  カタログの作成、マシンの追加、およびカタログの更新には、それぞれ固有のストレージへの影響があります。例:

  - 初期カタログ作成 では、ベースディスクのコピーを各ストレージの場所にコピーする必要があります。
    - また、一時的に 準備用 VM を作成する必要があります。
  - カタログに マシンを追加 する場合、ベースディスクを各ストレージの場所にコピーする必要はありません。カタログの作成は、選択された機能によって異なります。

- カタログを更新 すると、各ストレージの場所に余分なベースディスクが作成されます。カタログの更新では、カタログ内の各 VM が一定期間 2 つの差分ディスクを持つため、一時的なストレージのピークも発生します。

その他の考慮事項：

- **RAMサイジング:** I/O最適化ディスク、ライトキャッシュ、スナップショットファイルなど、特定のハイパーバイザーファイルとディスクのサイズに影響します。
- **シンIシックプロビジョニング:** シンプロビジョニング機能があるため、NFSストレージが推奨されます。

Machine Creation Services (MCS) ストレージ最適化

MCS I/O と呼ばれる Machine Creation Services (MCS) ストレージ最適化機能では、次のようになります。

- ライトキャッシュコンテナは*ファイルベース*であり、Citrix Provisioning と同じ機能です。たとえば、Citrix Provisioning のライトキャッシュファイル名は `D:\vdiskdif.vhdx` で、MCS I/O のライトキャッシュファイル名は `D:\mcsdif.vhdx` です。
- ライトキャッシュディスクに書き込まれるWindowsクラッシュダンプファイルのサポートを含めることで、診断の改善を実現します。
- MCS I/O は、最適なマルチティアライトキャッシュソリューションを提供するために、*RAM内キャッシュとハードディスクへのオーバーフロー*というテクノロジーを保持しています。この機能により、管理者は各層（RAM とディスク）のコストとパフォーマンスのバランスを取り、目的のワークロードの期待に応えることができます。

書き込みキャッシュ方式を*ディスクベース*から*ファイルベース*に更新するには、次の変更が必要です。

1. MCS I/O は RAM のみのキャッシュをサポートしなくなりました。マシンカタログ作成時に Web Studio でディスクサイズを指定してください。
2. VM のライトキャッシュディスクは、VM の初回起動時に自動的に作成およびフォーマットされます。VM が起動すると、ライトキャッシュファイル `mcsdif.vhdx` はフォーマットされたボリューム `MCSWCDisk` に書き込まれます。
3. ページファイルはこのフォーマットされたボリューム `MCSWCDisk` にリダイレクトされます。その結果、このディスクサイズはディスク領域の合計量を考慮します。これには、ディスクサイズと生成されたワークロードの差分に加えて、ページファイルサイズが含まれます。これは通常、VM の RAM サイズに関連付けられます。

MCS ストレージ最適化の更新の有効化

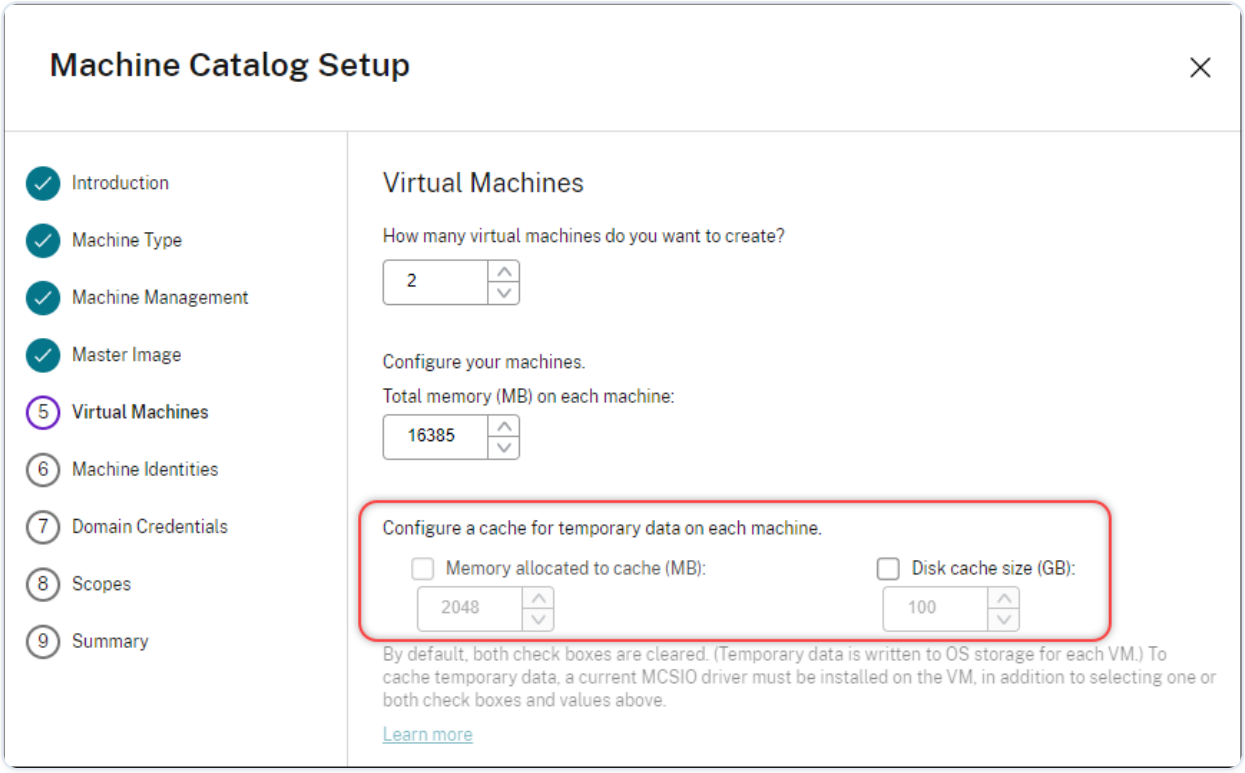
MCS I/O ストレージ最適化機能を有効にするには、Delivery Controller と VDA を Citrix Virtual Apps and Desktops の最新バージョンにアップグレードしてください。

注:

MCS I/O が有効になっている既存の展開をアップグレードする場合、追加の構成は必要ありません。VDA と Delivery Controller のアップグレードによって MCS I/O のアップグレードが処理されます。

MCS ストレージ最適化の更新を有効にする際は、次の点を考慮してください。

- マシンカタログを作成する際、管理者は RAM とディスクサイズを構成できます。



- バージョン 1903 用に構成された VDA を含む新しい VM スナップショットに既存のマシンカタログを更新すると、次の動作になります。新しいスナップショットは、既存のカタログの RAM およびディスクサイズに対する MCS I/O 設定を引き続き使用します。既存の生ディスクはフォーマットされます。

重要:

> Citrix Virtual Apps and Desktops バージョン 1903 で MCS ストレージ最適化が変更されました。このリリースでは、ファイルベースのライトキャッシュテクノロジがサポートされ、パフォーマンスと安定性が向上しています。MCS I/O によって提供される新しい機能では、以前の Citrix Virtual Apps and Desktops リリースと比較して、より高いライトキャッシュストレージ要件が必要になる場合があります。Citrix は、割り当てられたワークフローと追加のページファイルサイズに対して十分なディスク容量があることを確認するために、ディスクサイズを再評価することをお勧めします。ページファイルサイズは通常、システム RAM の量に関連しています。既存のカタログディスクサイズが不十分な場合は、マシンカタログを作成し、より大きなライトキャッシュディスクを割り当ててください。

MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てる

MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てることができます。この実装により、使用するアプリケーションのドライブ文字とMCS I/Oライトバックキャッシュディスクのドライブ文字との間の競合を回避できます。MCS I/Oライトバックキャッシュディスクにドライブ文字を割り当てるには、PowerShellコマンドを使用できます。サポートされているハイパーバイザーは、Azure、GCP、VMware、SCVMM、およびXenServerです。

> **注:**
>
> この機能には、VDAバージョン2305以降が必要です。

制限事項

- Windowsオペレーティングシステムのみに適用
- ライトバックキャッシュディスクに適用可能なドライブ文字：`E`から`Z`
- Azure一時ディスクがライトバックキャッシュディスクとして使用されている場合は適用されません
- 新しいマシンカタログを作成する場合にのみ適用されます

ライトバックキャッシュディスクにドライブ文字を割り当てる

ライトバックキャッシュディスクにドライブ文字を割り当てるには、次の手順を実行します。

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*`を実行します。

3. まだ作成されていない場合は、IDプールを作成します。
4. プロパティ `WriteBackCacheDriveLetter` を指定して、 `New-ProvScheme` コマンドを使用してプロビジョニングスキームを作成します。例：

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "<name>" `

-IdentityPoolName $schemeName `

-ProvisioningSchemeName $schemeName `

-InitialBatchSizeHint 1 `

-UseWriteBackCache -WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `

-MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
resources.resourcegroup\MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxxx2130aa
145ec77.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\name\
\virtualprivatecloud.folder\\East US.region\
\virtualprivatecloud.folder\\abcd-resources.resourcegroup\\abcd-
resources-vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.folder\
\Standard_D2s_v5.serviceoffering" `

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS"/>

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />
```

```
<Property xsi:type="StringProperty" Name="PersistOsDisk"
Value="false" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
Value="false" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-
group1" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

5. カタログの作成を完了します。詳細については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

マスターイメージを準備する

接続ホストの作成については、「接続とリソース」を参照してください。

マスターイメージには、オペレーティングシステム、仮想化されていないアプリケーション、VDA、およびその他のソフトウェアが含まれています。

知っておくと良いこと:

- マスターイメージは、クローンイメージ、ゴールデンイメージ、ベースVM、またはベースイメージとも呼ばれることがあります。ホストベンダーは異なる用語を使用します。
- ホストが、作成されるマシンの数に対応できる十分なプロセッサ、メモリ、ストレージを備えていることを確認してください。
- デスクトップおよびアプリケーションに必要なハードディスク容量を正しく構成してください。この値は、後で変更したり、マシンカタログで変更したりすることはできません。

- Remote PC Accessマシンカタログは、マスターイメージを使用しません。

マスターイメージに以下のソフトウェアをインストールして構成します:

- ハイパーバイザー用の統合ツール（Citrix VM Tools、Hyper-V Integration Services、VMware toolsなど）。この手順を省略すると、アプリケーションやデスクトップが正しく機能しない可能性があります。
- VDA。Citrixは、最新機能にアクセスできるように最新バージョンのインストールを推奨しています。マスターイメージにVDAをインストールしないと、カタログ作成が失敗します。
- 必要に応じて、アンチウイルスソフトウェアや電子ソフトウェア配布エージェントなどのサードパーティツール。ユーザーとマシンタイプに適した設定（更新機能など）でサービスを構成します。
- 仮想化しないサードパーティアプリケーション。Citrixはアプリケーションの仮想化を推奨しています。仮想化により、アプリケーションの追加または再構成後にマスターイメージを更新する必要がなくなるため、コストが削減されます。また、インストールされるアプリケーションが少ないほど、マスターイメージのハードディスクサイズが小さくなり、ストレージコストを節約できます。
- App-Vアプリケーションを公開する予定がある場合は、推奨設定のApp-Vクライアント。App-VクライアントはMicrosoftから入手できます。
- MCSを使用する場合、Microsoft Windowsをローカライズする際は、ロケールと言語パックをインストールしてください。プロビジョニング中にスナップショットが作成されると、プロビジョニングされたVMはインストールされているロケールと言語パックを使用します。

重要:

MCSを使用している場合は、マスターイメージでSysprepを実行しないでください。

マスターイメージを準備するには：

1. ハイパーバイザーの管理ツールを使用してマスターイメージを作成し、オペレーティングシステム、すべてのサービスパック、および更新プログラムをインストールします。vCPUの数を指定します。PowerShellを使用してマシンカタログを作成する場合も、vCPUの値を指定できます。Web Studioを使用してカタログを作成する場合、vCPUの数を指定することはできません。デスクトップとアプリケーションに必要なハードディスク容量を構成します。この値は後で変更したり、カタログ内で変更したりすることはできません。

2. ハードディスクがデバイスロケーション0に接続されていることを確認します。ほとんどの標準マスターイメージテンプレートでは、このロケーションがデフォルトで構成されていますが、一部のカスタムテンプレートではそうでない場合があります。
3. 上記のソフトウェアをマスターイメージにインストールして構成します。
4. MCSを使用していない場合は、マスターイメージをアプリケーションとデスクトップが属するドメインに参加させます。マスターイメージがマシンが作成されるホストで利用可能であることを確認します。MCSを使用している場合、マスターイメージをドメインに参加させる必要はありません。プロビジョニングされたマシンは、カタログ作成ウィザードで指定されたドメインに参加します。
5. Citrixは、マスターイメージのスナップショットを作成して名前を付けることを推奨しています。カタログ作成時にスナップショットではなくマスターイメージを指定した場合、Web Studioはスナップショットを作成しますが、名前を付けることはできません。

ボリュームライセンス認証

MCSは、WindowsオペレーティングシステムとMicrosoft Officeのアクティベーションを自動化および管理するためのボリュームライセンス認証をサポートしています。MCSがサポートするボリュームライセンス認証の3つのモデルは次のとおりです。

- キー管理サービス (KMS)
- Active Directoryベースの認証 (ADBA)
- マルチプルアクティベーションキー (MAK)

マシンカタログの作成後に、アクティベーション設定を変更できます。

キー管理サービス (KMS)

KMSは、専用のシステムを必要とせず、他のサービスを提供するシステム上で簡単に共存できる軽量なサービスです。この機能は、Citrixがサポートするすべてのバージョンでサポートされています。イメージ準備中に、MCSはMicrosoft WindowsおよびMicrosoft OfficeのKMSリアームを実行します。`Set-Provserviceconfigurationdata`コマンドを実行することで、リアームをスキップできます。イメージ準備中のMicrosoft Windows KMSリアームおよびMicrosoft Office KMSリアームの詳細については、「Machine Creation Services: Image Preparation Overview and Fault-Finding」を参照してください。KMSアクティベーションの詳細については、「Activate using Key Management Service」を参照してください。

> **注:**

`Set-Provserviceconfigurationdata`コマンドの実行後に作成されたすべてのマシンカタログは、コマンドで指定されたものと同じ設定になります。

Active Directoryベースのアクティベーション (ADBA)

ADBAを使用すると、ドメイン接続を介してマシンをアクティベートできます。マシンはドメインに参加するとすぐにアクティベートされます。これらのマシンは、ドメインに参加し、ドメインと通信している限りアクティベートされたままになります。この機能は、Citrixがサポートするすべてのバージョンでサポートされています。Active Directoryベースの認証の詳細については、「Active Directory-based activation」を使用してアクティベートするを参照してください。

マルチプルアクティベーションキー (MAK)

MAKは、Microsoftサーバーの助けを借りて、ボリュームをアクティベートし、Windowsシステムを認証する方法です。MicrosoftからMAKキーを購入する必要があります。このキーには、固定されたアクティベーション数が割り当てられています。Windowsシステムがアクティベートされるたびに、アクティベーション数が減少します。システムをアクティベートする方法は2つあります。

- オンラインアクティベーション：アクティベートしたいWindowsシステムがインターネットにアクセスできる場合、プロダクトキーをインストールするとシステムは自動的にWindowsをアクティベートします。このプロセスにより、対応するMAKのアクティベーション数が1減少します。
- オフラインアクティベーション: Windowsシステムがインターネットに接続してオンラインアクティベーションを実行できない場合、MCSはMicrosoftサーバーから確認IDとインストールIDを取得してWindowsシステムをアクティベートします。このアクティベーション方法は、非永続的なマシンカタログに役立ちます。

注：

- MCSは、MAKを使用したMicrosoft Officeのアクティベーションをサポートしていません。
- 必要なVDAの最小バージョンは2303です。

主な要件

- Delivery Controllerはインターネットにアクセスできる必要があります。
- 更新する新しいイメージが元のイメージと異なるMAKキーを持っている場合は、新しいカタログを作成します。

- マスターイメージにMAKキーをインストールします。WindowsシステムにMAKキーをインストールする手順については、「MAKアクティベーションの展開」を参照してください。
- イメージ準備を使用しない場合：

  a. レジストリDWORD値 `Manual` を `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation` の下に追加します。

  b. 値を `1` に設定します。

アクティベーション数

MAKキーの残りのアクティベーション数を確認したり、VMが2つ以上のアクティベーションを消費しているかどうかを確認したりするには、ボリュームライセンス認証管理ツール（VAMT）を使用します。「VAMTのインストール」を参照してください。

MAKを使用してWindowsシステムをアクティベートする

MAKを使用してWindowsシステムをアクティベートするには：

1. マスターイメージにプロダクトキーをインストールします。この手順で1つのアクティベーションカウントが消費されます。
2. MCSマシンカタログを作成します。
3. イメージ準備を使用しない場合：

   a. `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`の下にレジストリDWORD値`Manual`を追加します。

   b. 値を`1`に設定します。

   この方法では、オンラインアクティベーションのオプションが無効になります。
4. マシンカタログにVMを追加します。
5. VMの電源をオンにします。
6. オンラインアクティベーションかオフラインアクティベーションかに応じて、Windowsシステムがアクティベートされます。

   - アクティベーションがオンラインの場合、プロダクトキーがインストールされた後にWindowsシステムがアクティベートされます。
   - アクティベーションがオフラインの場合、MCSはプロビジョニングされたVMと通信してWindowsシステムのアクティベーションステータスを取得します。その後、MCSは

Microsoftサーバーから確認IDとインストール済みIDを取得します。これらのIDはWindowsシステムのアクティベーションに使用されます。

トラブルシューティング

プロビジョニングされた VM がインストール済みの MAK キーでアクティベートされない場合は、PowerShell ウィンドウで `Get-ProvVM` または `Get-ProvScheme` コマンドを実行します。

- `Get-ProvScheme` コマンド: 最新のマスターイメージから MCS マシンカタログに関連付けられているパラメーター `WindowsActivationType` を参照してください。
- `Get-ProvVM` コマンド。パラメーター `WindowsActivationType`、`WindowsActivationStatus`、`WindowsActivationStatusErrorCode`、および `WindowsActivationStatusError` を参照してください。

エラーを確認し、問題を解決するための手順を検証できます。

Web Studio を使用してマシンカタログを作成する

カタログを作成する前に:

- このセクションを確認して、選択する項目と提供する情報について学習してください。
- マシンをホストするハイパーバイザー、クラウドサービス、およびその他のリソースへの接続が作成されていることを確認してください。
- マシンをプロビジョニングするためのマスターイメージを作成した場合は、そのイメージに VDA がインストールされていることを確認してください。

カタログ作成ウィザードを開始するには：

1. これが最初に作成するカタログである場合、適切な選択肢（「マシンをセットアップし、アプリとデスクトップを実行するためのマシンカタログを作成する」など）に誘導されます。カタログ作成ウィザードが開きます。
2. 既にカタログを作成済みで、別のカタログを作成したい場合は、次の手順に従ってください:

    a. Web Studio にサインインし、左側のペインで **Machine Catalogs** を選択し、アクションバーで **Create Machine Catalog** を選択します。

    b. フォルダーを使用してカタログを整理するには、デフォルトの**Machine Catalogs**フォルダーの下にフォルダーを作成します。詳細については、(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-manage.html#create-a-catalog-folder)を参照してください。

c. カタログを作成したいフォルダーを選択し、**Create Machine Catalog**をクリックします。カタログ作成ウィザードが開きます。

ウィザードは次の項目について説明します。表示されるウィザードページは、選択内容によって異なります。

オペレーティングシステム

各カタログには、1種類のマシンのみが含まれます。1つ選択してください。

- **マルチセッションOS:** マルチセッションOSカタログは、ホストされた共有デスクトップを提供します。マシンはサポートされているバージョンのWindowsまたはLinuxオペレーティングシステムを実行できますが、カタログに両方を含めることはできません。（そのOSの詳細については、Linux VDAのドキュメントを参照してください。）
- **シングルセッションOS:** シングルセッションOSカタログは、さまざまなユーザーに割り当てることができるVDIデスクトップを提供します。
- **リモートPCアクセス:** リモートPCアクセス カタログは、ユーザーに物理的なオフィスデスクトップマシンへのリモートアクセスを提供します。リモートPCアクセスは、セキュリティを提供するためにVPNを必要としません。

マシン管理

リモートPCアクセス カタログを作成している場合、このページは表示されません。

マシン管理ページには、マシンの管理方法と、マシンの展開に使用するツールが示されます。

カタログ内のマシンをWeb Studio経由で電源管理するかどうかを選択します。

- マシンはWeb Studioを介して電源管理されます。たとえば、VMやブレードPCなどです。このオプションは、ホストへの接続をすでに構成している場合にのみ利用可能です。
- マシンはWeb Studioを介して電源管理されません。たとえば、物理マシンなどです。

マシンがWeb Studioを介して電源管理されることを指定した場合は、VMの作成に使用するツールを選択します。

- Citrix Provisioningテクノロジー
    - **Citrix Machine Creation Services (MCS)** MCSを使用してプロビジョニングおよびイメージ化されたVMのカタログを作成します。MCSは、マスターイメージからクローンされたイメージをこれらのVMにコピーします。

- **Citrix Provisioning Services (PVS)** MCSを使用してプロビジョニングされ、PVSを使用してイメージ化されたVMのカタログを作成します。これらのVMはPVSターゲットデバイスとして機能し、PVSサーバーは単一の共有ディスクイメージをそれらにストリーミングできます。

  > **注:**
  >
  > - このオプションは、Citrix Cloud™に登録されているPVSサイトでのみ利用可能であり、現在はAzureリソースに限定されています。
  > - Citrix Provisioningカタログを作成する際に、「**ターゲットデバイス**」ページで、プロビジョニングするマシンのファームとサイトを選択するドロップダウンメニューに、すでに存在しないファームとサイトがリストされている場合があります。回避策として、PowerShellコマンド `Unregister-HypPvsSite` を実行して、データベースからファームとサイトを削除できます。PowerShellコマンドの詳細については、「Unregister-HypPvsSite」を参照してください。

- **その他のサービスまたはテクノロジー** データセンターに既に存在するマシンを管理するツールです。Citrixでは、カタログ内のマシンの一貫性を確保するために、Microsoft System Center Configuration Managerまたはその他のサードパーティ製アプリケーションを使用することをお勧めします。

デスクトップの種類（デスクトップエクスペリエンス）

> 「**注：**」:
>
> 「**デスクトップエクスペリエンス**」ページに表示されるオプションは、「**マシンタイプ**」ページで選択したマシンタイプによって異なります。

- 「**マルチセッションOS**」マシンでは、ユーザーはログオンするたびにランダムなデスクトップを割り当てられます。次のいずれかのオプションを選択します。
  - 「**はい、仮想デスクトップをホストするマシンのローカルディスクに変更を保存します。**」（永続的）
  - 「**いいえ、すべての変更を破棄し、ユーザーがログオフしたときに仮想デスクトップをクリアします。**」（非永続的）

> 「**注：**」：
>
> 永続的なマルチセッションマシンでは、ユーザーがデスクトップに行った変更は保存され、すべての承認済みユーザーがアクセスできます。

- 「**シングルセッションOS**」マシンでは、「**デスクトップエクスペリエンス**」ページで次のオプションが表示されます。
  - 「**ユーザーがログオンするたびに新しい（ランダムな）デスクトップに接続するようにします。**」.
  - 「**ユーザーがログオンするたびに同じ（静的な）デスクトップに接続するようにします。**」.

    静的デスクトップの場合、ユーザーが行った変更をログオフ後に保存するか破棄するかをさらに決定できます。

イメージとマシンプロファイル

このページは、MCSを使用してVMを作成している場合にのみ表示されます。

1. マシンカタログのイメージタイプを選択し、イメージを選択します。利用可能なイメージタイプは2つあります。
   - **マスターイメージ。** イメージ準備プロセスをまだ経ていないイメージです。イメージ準備プロセスは、カタログ作成が開始されると自動的に開始されます。

     > **注:**
     >
     > - MCSを使用している場合、マスターイメージでSysprepを実行しないでください。
     > - スナップショットではなくマスターイメージを指定した場合、Web Studioはスナップショットを作成しますが、名前を付けることはできません。

   - **準備済みイメージ。** イメージ準備プロセスを完了し、VM 作成に直接使用できるイメージ。カタログ作成時にマスターイメージではなく準備済みイメージを選択すると、より高

速で信頼性の高いマシンカタログ作成が保証され、イメージライフサイクル管理が合理化されます。

> **注:**
>
> - 準備済みイメージを使用して作成された VM は、休止状態をサポートしません。
> - 現在、準備済みイメージを使用したカタログ作成は、Azure および VMware 環境でのみ利用可能です。

準備されたイメージの作成方法の詳細については、Image management (preview)を参照してください。

イメージを選択する際、必要に応じて、選択したイメージにメモを追加できます。

最新の製品機能を使用できるようにするには、マスターイメージに最新の VDA バージョンがインストールされていることを確認してください。デフォルトの最小 VDA 選択を変更しないでください。ただし、以前の VDA バージョンを使用する必要がある場合は、「VDA バージョンと機能レベル」を参照してください。

ウィザードで以前に選択したマシン管理テクノロジーと互換性のないスナップショットまたはVMを選択すると、エラーメッセージが表示されます。

2. 既存のVMをマシンプロファイルとして使用するには、**Use a machine profile**を選択し、その後、VMを選択します。

> **注記：**
>
> 現在、マシンプロファイルの使用は、Azure、AWS、GCP、およびVMware VMに限定されています。

> VMware展開の場合、マシンプロファイルを使用してマシンカタログを作成する際、仮想マシンを保持するフォルダーを指定する必要があります。

仮想マシンフォルダーの場所を指定するには、カタログ作成ウィザードで**仮想マシン**ページに移動し、**マシンを配置するフォルダーを選択**セクションに移動して仮想マシンフォルダーの場所を選択します。指定されていない場合、システムは、選択されたマシンプロファイルのフォルダーをデフォルトの場所と見なします。

3. カタログの最小機能レベルを選択します。最新の製品機能を使用できるようにするには、マスターイメージに最新のVDAバージョンがインストールされていることを確認してください。

マシン

リモートPCアクセスカタログを作成している場合、このページは表示されません。

このページのタイトルは、**マシン管理**ページで選択した内容によって異なります。**マシン**、**仮想マシン**、または**VMとユーザー**です。

MCSを使用する場合：

- 作成する仮想マシンの数を指定します。作成しない場合は**0**（ゼロ）を入力します。後で、**マシンの追加**を実行して、空のカタログにVMを作成できます。
- 各VMが持つメモリ量（MB単位）を選択します。
- 作成された各VMにはハードディスクがあります。そのサイズはマスターイメージで設定されます。カタログでハードディスクのサイズを変更することはできません。
- 展開に複数のゾーンが含まれている場合、カタログのゾーンを選択できます。
- 静的デスクトップVMを作成している場合、仮想マシンコピーモードを選択します。「仮想マシンコピーモード」を参照してください。
- vDiskを使用しないランダムデスクトップVMを作成している場合、各マシンの一時データに使用するキャッシュを構成できます。「一時データ用のキャッシュを構成する」を参照してください。

その他のツールを使用する場合：

Active Directoryマシンアカウント名を追加（またはリストをインポート）します。VMを追加/インポートした後、そのVMのActive Directoryアカウント名を変更できます。**Desktop Experience**ページで静的マシンを指定した場合、追加する各VMのActive Directoryユーザー名をオプションで指定できます。

名前を追加またはインポートした後、このページにいる間に、**削除**ボタンを使用してリストから名前を削除できます。

他のツールを使用する場合（ただしMCSではない場合）：

追加（またはインポート）された各マシンには、カタログに追加できない可能性のあるマシン、またはDelivery Controllerに登録できない可能性のあるマシンを識別するのに役立つアイコンとツールヒントが表示されます。詳細については、「VDAバージョンと機能レベル」を参照してください。

仮想マシン作成時にSIDを追加する

新しい仮想マシンを作成する際に、マシンを一意に識別するためにパラメーター`ADAccountSid`を追加できるようになりました。

これを行うには：

1. サポートされているIDタイプでカタログを作成します。
2. `NewProvVM`を使用してカタログにマシンを追加します。例：

```
New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID ")  -
RunAsynchronously
```

ただし、次のマシンをプロビジョニングすることはできません。

- カタログIDプールにないADアカウント
- 利用可能な状態ではないADアカウント

仮想マシンのコピーモード

マシンページで指定するコピーモードによって、MCSがマスターイメージからシン（高速コピー）クローンを作成するか、シック（完全コピー）クローンを作成するかが決まります。（デフォルト = シンクローン）

- ストレージをより効率的に使用し、マシンの作成を高速化するには、高速コピーのクローンを使用します。
- マシン作成後のIOPSを削減できる可能性があり、より優れたデータ回復と移行サポートのために、完全コピーのクローンを使用します。

VDAのバージョンと機能レベル

カタログの機能レベルは、カタログ内のマシンで利用できる製品機能を制御します。新しい製品バージョンで導入された機能を使用するには、新しいVDAが必要です。ただし、以前のVDAバージョンを使用しているカタログ内のマシンは登録できません。

マシン (または **デバイス**) ページの下部にあるメニューで、最小VDAレベルを選択できます。これにより、カタログの最小機能レベルが設定されます。デフォルトでは、オンプレミス展開の場合、最新の機能レベルが選択されます。Citrixの推奨に従って、VDAとコアコンポーネントを常に最新バージョンにインストールおよびアップグレードする場合は、この選択を変更する必要はありません。ただし、古いVDAバージョンを使い続ける必要がある場合は、正しい値を選択してください。

Citrix Virtual Apps and Desktopsのリリースには、新しいVDAバージョンが含まれていない場合や、新しいVDAが機能レベルに影響を与えない場合があります。そのような場合、機能レベルは、インストールまたはアップグレードされたコンポーネントよりも古いVDAバージョンを示すことがあります。各リリースの新機能の記事には、デフォルトの機能レベルの変更が示されています。

選択された機能レベルは、その上にあるマシンのリストに影響します。リストでは、各エントリの横にあるツールヒントが、その機能レベルでマシンのVDAがカタログと互換性があるかどうかを示します。

各マシンのVDAが選択された最小機能レベルを満たしていないか、それを超えていない場合、ページにメッセージが表示されます。ウィザードを続行できます。それらのマシンは、後でControllerに登録できない可能性があります。または、次のことができます。

- 古いVDAを含むマシンをリストから削除し、VDAをアップグレードしてから、カタログに再度追加します。
- 最新の製品機能へのアクセスを妨げる、より低い機能レベルを選択します。

マシンが間違ったマシンタイプであるためにカタログに追加されなかった場合も、メッセージが表示されます。例としては、サーバーをシングルセッションOSカタログに追加しようとする場合や、ランダム割り当て用に作成されたシングルセッションOSマシンを静的マシンのカタログに追加する場合などがあります。

重要:

リリース1811で、追加の機能レベル **1811 (またはそれ以降)** が追加されました。このレベルは、将来のCitrix Virtual Apps and Desktops機能で使用することを目的としています。**7.9 (またはそれ以降)** の選択はデフォルトのままです。このデフォルトは、現在すべての展開で有効です。

1811 (またはそれ以降) を選択した場合、そのカタログ内の以前のVDAバージョンはControllerに登録できません。ただし、カタログにバージョン1811以降のサポートされているVDAのみが含まれている場合、それらはすべて登録の対象となります。これには、バージョン1903や現在のリリース以前の他の19XXリリースを含む、後のCitrix Virtual Apps and Desktopsリリース用に構成されたVDAを含むカタログも含まれます。

一時データのキャッシュを構成する

MCSを使用してカタログ内のランダムな非永続マシンを管理する場合、I/Oパフォーマンスを向上させるために、マシンに対してライトバックキャッシュを有効にできます。

ライトバックキャッシュはMCSIOと呼ばれます。詳細については、こちらのブログ記事を参照してください。

前提条件

ライトバックキャッシュを有効にするには、カタログが以下の要件を満たしている必要があります。

- 一時データ用のストレージを指定する接続を使用していること。詳細については、接続とリソースを参照してください。
- VDAはバージョン7.9以降であり、最新のMCSIOドライバーがインストールされていること。

> **注:**
>
> このドライバーのインストールは、VDAをインストールまたはアップグレードする際のオプションです。デフォルトでは、このドライバーはインストールされません。

- ディスクキャッシュのドライブ文字割り当てを有効にするには、VMは以下の追加要件を満たす必要があります。
  - オペレーティングシステム：Windows
  - VDAバージョン：2305以降

考慮事項

- ライトバックキャッシュには、*メモリ*キャッシュと*ディスク*キャッシュがあります。デフォルトでは、接続タイプによってその既定値が異なります。通常、既定値はほとんどのケースで十分ですが、以下のために必要な領域を考慮してください。
  - Windows自体によって作成される一時データファイル（Windowsページファイルを含む）。
  - ユーザープロファイルデータ。
  - ユーザーのセッションに同期されるShareFileデータ。

  - セッションユーザーによって作成またはコピーされる可能性のあるデータ、またはユーザーがセッション内にインストールする可能性のあるアプリケーションによって作成またはコピーされる可能性のあるデータ。

ストレージイメージ(/en-us/citrix-virtual-apps-desktops/2411/media/storage-temp2.png)

- ディスクキャッシュとメモリキャッシュなしでライトバックキャッシュを構成する機能は削除されました。一時データのキャッシュを有効にするには、**ディスクキャッシュサイズ (GB)** と **キャッシュに割り当てられるメモリ (MB)** を選択し、メモリキャッシュに0より大きいサイズを指定することをお勧めします。一時データは最初にメモリキャッシュに書き込まれます。メモリキャッシュが構成された制限に達すると、最も古いデータは一時データキャッシュディスクに移動されます。
- メモリキャッシュは、各マシン上の総メモリ量の一部です。したがって、**メモリキャッシュサイズ (MB) (推奨)** チェックボックスを有効にする場合は、各マシン上の総メモリ量を増やすことを検討してください。
- **メモリキャッシュサイズ (MB) (推奨)** チェックボックスをオフのままにすると、一時データは、最小限のメモリを使用してディスクキャッシュに直接書き込まれます。
- **ディスクキャッシュサイズ (GB)** をデフォルト値から変更すると、パフォーマンスに影響を与える可能性があります。サイズは、ユーザー要件とマシンにかかる負荷に合わせる必要があります。

> **重要:**
>
> ディスクキャッシュの容量が不足すると、ユーザーのセッションは使用できなくなります。

- **ディスクキャッシュサイズ**チェックボックスをオフにすると、キャッシュディスクは作成されません。この場合、すべての一時データを保持するのに十分な大きさの**キャッシュに割り当てられたメモリ**の値を指定します。これは、各VMに割り当てるための大量のRAMが利用可能な場合にのみ可能です。
- 両方のチェックボックスをオフにすると、一時データはキャッシュされません。各VMの差分ディスク（OSストレージにあります）に書き込まれます。（これは、7.9より前のリリースでのプロビジョニングアクションです。）
- このカタログを使用してAppDiskを作成する予定がある場合は、キャッシュを有効にしないでください。
- マシンカタログの作成後、キャッシュ値を変更することはできません。

NIC (NIC)

リモートPCアクセス カタログを作成している場合、このページは表示されません。

複数のNICを使用する予定がある場合、各カードに仮想ネットワークを関連付けます。例えば、一方のカードを特定のセキュアなネットワークへのアクセスに割り当て、もう一方のカードをより一般的に使用されるネットワークへのアクセスに割り当てることができます。このページからNICを追加または削除することもできます。

マシンアカウント

このページは、リモートPCアクセス カタログを作成する場合にのみ表示されます。

マシンアカウントページで、ユーザーまたはユーザーグループに対応するActive Directoryマシンアカウントまたは組織単位（OU）を追加するように指定します。OU名にスラッシュ（/）を使用しないでください。

OUを追加する際、ドメインがリストに表示されない場合は、次の操作を実行できます。

- 完全一致で検索します。
- すべてのドメインを参照して見つけます。

以前に構成した電源管理接続を選択するか、電源管理を使用しないことを選択できます。電源管理を使用したいが、適切な接続がまだ構成されていない場合は、後でその接続を作成し、マシンカタログを編集して電源管理設定を更新できます。

マシンID

このページは、MCSを使用してVMを作成する場合にのみ表示されます。

カタログ内の各マシンには一意のIDが必要です。このページでは、カタログ内のマシンのIDを構成できます。マシンはプロビジョニング後にIDに結合されます。カタログ作成後にIDの種類を変更することはできません。

このページで設定を構成するための一般的なワークフローは次のとおりです。

1. リストからIDを選択します。
2. アカウントを作成するか既存のアカウントを使用するか、およびそれらのアカウントの場所（ドメイン）を指定します。

次のいずれかのオプションを選択できます。

- **オンプレミスActive Directory**。組織が所有し、その組織に属するActive Directoryアカウントでサインインするマシン。それらはオンプレミスに存在します。
- **ハイブリッドAzure Active Directory参加済み**。組織が所有し、その組織に属するActive Directory Domain Servicesアカウントでサインインするマシン。それらはクラウドとオンプレミスに存在します。要件、制限、考慮事項については、「ハイブリッドAzure Active Directory参加済み」を参照してください。

  注:

  - ハイブリッドAzure Active Directory参加を使用する前に、Azure環境が前提条件を満たしていることを確認してください。「Microsoft Entra ハイブリッド参加の構成」を参照してください。
  - このオプションでは、マスターイメージがオペレーティングシステムの前提条件を満たしている必要があります。詳細については、「Microsoft Entra ハイブリッド参加済みデバイス」を参照してください。

- **ドメイン非参加**。どのドメインにも参加していないマシン。要件と制限については、「ドメイン非参加」を参照してください。

重要:

- IDタイプとして**オンプレミスActive Directory**または**ハイブリッドAzure Active Directory参加済み**を選択した場合、カタログ内の各マシンには、対応するActive Directoryコンピューターアカウントが必要です。
- **ドメイン非参加**IDタイプでは、カタログの最小機能レベルとしてVDAバージョン2311以降が必要です。これを使用可能にするには、最小機能レベルを更新してください。

アカウントを作成する場合、マシンが存在するOUでコンピューターアカウントを作成する権限が必要です。カタログ内の各マシンには一意の名前が必要です。作成するマシンのアカウント命名スキームを指定します。詳細については、「マシンアカウント命名スキーム」を参照してください。

注:

> OU名にスラッシュ (`/`) を使用しないようにしてください。

> 既存のアカウントを使用する場合は、アカウントを参照するか、**インポート**をクリックしてアカウント名を含む.csvファイルを指定します。インポートされたファイルの内容は、次の形式を使用する必要があります。

- ADcomputeraccountname.domain

追加するすべてのマシンに対して十分なアカウントがあることを確認してください。Web Studioインターフェイスがそれらのアカウントを管理します。したがって、そのインターフェイスですべてのアカウントのパスワードをリセットできるようにするか、すべてのアカウントで同じパスワードを指定してください。

物理マシンまたは既存のマシンを含むカタログの場合、既存のアカウントを選択またはインポートし、各マシンをActive Directoryコンピューターアカウントとユーザーアカウントの両方に割り当てます。

マシンアカウントの命名規則

カタログ内の各マシンには、一意の名前が必要です。カタログを作成する際には、マシンアカウントの命名規則を指定する必要があります。名前に表示される連番または文字のプレースホルダーとして、ワイルドカード（ハッシュマーク）を使用します。

命名規則を指定する際は、以下のルールに注意してください。

- 命名スキームには少なくとも1つのワイルドカードを含める必要があります。すべてのワイルドカードはまとめて配置する必要があります。
- ワイルドカードを含む名前全体は、2文字以上15文字以下である必要があります。少なくとも1つの非数字文字と1つの#（ワイルドカード）文字を含める必要があります。
- 名前にスペースや以下の文字を含めることはできません: `,~!@'$%\^&.()}{\/*?"<>|=+[];:_".`。
- 名前をハイフン（-）で終わらせることはできません。

また、命名規則を指定する際は、将来の拡張に十分な余地を残してください。この例を考えてみましょう。「veryverylong#」というスキームで1,000個のマシンアカウントを作成した場合、最後に作成されるアカウント名（veryverylong1000）は16文字になります。したがって、この命名規則では、最大15文字を超えるマシン名が1つ以上生成されることになります。

シーケンシャル値が数字（0-9）か文字（A-Z）かを示すことができます。

- **0-9**。選択した場合、指定されたワイルドカードは連番に解決されます。

> **注:**
>
> ワイルドカードが1つの場合、アカウント名は1から始まります。2つの場合、アカウント名は01から始まります。3つの場合、アカウント名は001から始まります。以降も同様です。

- **A-Z**。選択した場合、指定されたワイルドカードは連続する文字に解決されます。

例えば、PC-Sales-## (**0-9** が選択されている場合) という命名スキームでは、PC-Sales-01、PC-Sales-02、PC-Sales-03 などのアカウントが作成されます。

オプションで、アカウント名の開始文字を指定できます。

- **0-9** を選択すると、アカウントは指定された数字から順に命名されます。前のフィールドで使用するワイルドカードの数に応じて、1桁以上の数字を入力します。たとえば、2つのワイルドカードを使用する場合は、2桁以上の数字を入力します。
- **A-Z** を選択すると、アカウントは指定された文字から順に命名されます。前のフィールドで使用するワイルドカードの数に応じて、1文字以上の文字を入力します。たとえば、2つのワイルドカードを使用する場合は、2文字以上の文字を入力します。

ドメイン資格情報

資格情報の入力を選択し、ターゲットのActive Directoryドメインでアカウント操作を実行する権限を持つ管理者の資格情報を入力します。

名前の確認オプションを使用して、ユーザー名が有効か一意であるかを確認します。このオプションは、たとえば次のような場合に役立ちます。

- 同じユーザー名が複数のドメインに存在する場合。目的のユーザーを選択するよう求められます。
- ドメイン名を覚えていない場合。ドメイン名を指定せずにユーザー名を入力できます。確認が成功すると、ドメイン名が自動的に入力されます。

> **注:**

> **マシンID**で選択したIDの種類が**ハイブリッドAzure Active Directory参加済み**の場合、入力する資格情報には `Write userCertificate` 権限が付与されている必要があります。

概要、名前、および説明

「**概要**」ページで、指定した設定を確認します。カタログの名前と説明を入力します。この情報はWeb Studioに表示されます。

完了したら、**「完了」をクリックしてカタログの作成を開始します。 完了したら、**「完了」**を選択してカタログの作成を開始します。

マシンカタログに、新しいカタログがインラインの進行状況バーとともに表示されます。

作成の進行状況の詳細を表示するには：

1. マシンカタログにマウスを重ねます。
2. 表示されるツールヒントで、 をクリックします。

   段階的な進行状況グラフが表示され、次の項目を確認できます。

   - 手順の履歴
   - 現在のステップの進行状況と実行時間
   - 残りのステップ

MCS時刻同期

時刻同期は、マスターイメージと、マシンIDが結合されたカタログの種類によって決定されます。マスターイメージとカタログに応じて、次の時刻同期方法が適用されます。

マスターイメージ	カタログ	結果の時刻同期方法
NDJ	ADまたはハイブリッドAzure AD	デフォルトでは、NT5DS。マスターイメージのレジストリ設定を使用して、MCSが時刻同期設定を変更するのを無効にできます。
NDJ	NDJ または Azure AD	元の時刻同期設定と同じ
AD または Hybrid Azure AD	AD または Hybrid Azure AD	元の時刻同期設定と同じ
アジュール AD	アジュール AD	元の時刻同期設定と同じ

注:

元の時刻同期は、次のレジストリ設定によって制御され、変更できません。

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config

値: MaxAllowedPhaseOffset、MaxNegPhaseCorrection、およびMaxPosPhaseCorrection

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

値: Type

MCSが時刻同期設定を変更するのを無効にするには、マスターイメージで次のレジストリ設定の値を設定します。

- `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix`
- 名前: TimeSyncMethodKeep
- 種類: DWORD
- 0 (または、値 TimeSyncMethodKeep が構成されていない場合): 元の時刻同期設定を保持しません。
- 1: 元の時刻同期設定とデフォルトのパラメーター値を保持します。

カスタムプロパティの設定に関する重要な考慮事項

GCPおよびAzure環境では、`New-ProvScheme` および `Set-ProvScheme` でカスタムプロパティを正しく設定する必要があります。存在しないカスタムプロパティを指定すると、以下のエラーメッセージが表示され、コマンドの実行に失敗します。

- Azureの場合: `Invalid property found: <invalid property>. Ensure that the CustomProperties parameter supports the property.`.
- GCPの場合: `Invalid property found: <invalid property>. Ensure that the value supplied for the property is supported in the Hypervisor.`.

トラブルシューティング

重要:

Web Studioを使用してマシンカタログを作成した後、マシンカタログ作成に関連するタスクを取得するために `Get-ProvTask` PowerShellコマンドを使用することはできません。この制限は、カタログが正常に作成されたかどうかにかかわらず、Web Studioがマシンカタログ作成後にそれらのタスクを削除するためです。

Citrixは、サポートチームが解決策を提供できるよう、ログを収集することをお勧めします。Citrix Provisioningを使用している場合は、ログファイルを生成するために次の手順を使用します。

1. マスターイメージで、値1 (DWORD (32ビット) 値として) を持つ次のレジストリキーを作成します: `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`。
2. マスターイメージをシャットダウンし、スナップショットを作成します。
3. Delivery Controllerで、次のPowerShellコマンドを実行します: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`。
4. そのスナップショットに基づいてカタログを作成します。
5. 準備用VMがハイパーバイザー上に作成されたら、ログインしてC:\\のルートから次のファイル（Image-prep.logおよびPvsVmAgentLog.txt）を抽出します。
6. マシンをシャットダウンすると、その時点で障害が報告されます。
7. イメージ準備マシンの自動シャットダウンを再度有効にするには、次の PowerShell コマンドを実行します: `Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown`。

MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てる

MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てることができます。この実装により、使用するアプリケーションのドライブ文字とMCS I/Oライトバックキャッシュディスクのドライブ文字との競合を回避できます。これを行うには、PowerShellコマンドを使用します。サポートされているハイパーバイザーは、Azure、GCP、VMware、SCVMM、XenServerです。

> **注:**
>
> この機能にはVDAバージョン2305以降が必要です。

制限事項

- Windowsオペレーティングシステムのみに適用
- ライトバックキャッシュディスクに適用可能なドライブ文字: `E`から`Z`
- Azure一時ディスクがライトバックキャッシュディスクとして使用されている場合は適用されません
- 新しいマシンカタログを作成する場合にのみ適用

ライトバックキャッシュディスクにドライブ文字を割り当てる

ライトバックキャッシュディスクにドライブ文字を割り当てるには:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*` を実行します。
3. まだ作成されていない場合は、IDプールを作成します。詳しくは、カタログの作成 を参照してください。
4. `New-ProvScheme` コマンドとプロパティ `WriteBackCacheDriveLetter` を使用してプロビジョニングスキームを作成します。例:

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "<name>" `

-IdentityPoolName $schemeName `

-ProvisioningSchemeName $schemeName `

-InitialBatchSizeHint 1 `

-UseWriteBackCache -WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `

-MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
resources.resourcegroup\MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxx2130aa
145ec77.manageddisk" `
```

```
-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\name\
\virtualprivatecloud.folder\\East US.region\
\virtualprivatecloud.folder\\abcd-resources.resourcegroup\\abcd-
resources-vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.folder\
\Standard_D2s_v5.serviceoffering" `

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS"/>

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk"
Value="false" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
Value="false" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-
group1" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
```

```
</CustomProperties>'
```

5. カタログの作成を完了します。

MCSマシンカタログを作成する前に構成を検証する

`New-ProvScheme` コマンドでパラメーター `-validate` を使用して、MCS マシンカタログを作成する前に構成設定を検証できます。この PowerShell コマンドをパラメーターと共に実行すると、誤ったパラメーターが使用されている場合や、パラメーターが別のパラメーターと競合している場合に、適切なエラーメッセージが表示されます。その後、エラーメッセージを使用して問題を解決し、PowerShell を使用して MCS マシンカタログを正常に作成できます。現在、この機能は AWS、Azure、GCP、および VMware 仮想化環境に適用されます。

注:

検証中は、実際の MCS マシンカタログを作成してはなりません。コマンドの結果を使用してエラーを修正し、正常なカタログを作成する必要があります。したがって、`New-ProvScheme` コマンドを実行するときは、偽の ID プール名を使用してください。

構成を検証するには、次の手順を実行します。

1. Delivery ControllerホストからPowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*` を実行します。
3. `New-ProvScheme` コマンドを実行し、パラメーター `-validate` を使用します。コマンドが機能するように、架空のIDプール名を提供します。例：

```
$result =New-ProvScheme  -CleanOnBoot -HostingUnitName "vSanRg"
-IdentityPoolName "mptmpcatalogdemo" -InitialBatchSizeHint 1  -
MasterImageVM "XDHyp:
\HostingUnits\vSanRg\Windows19MasterImage.vm\Citrix_XD_NonMachineProfil
eWin19Machines.snapshot" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vSanRg\\VM Network.network"} -ProvisioningSchemeName
"MachineProfileW10Machines"  -Scope @()

-VMCpuCount 2  -VM

MemoryMB 6143 -MachineProfile "XDHyp:\HostingUnits\vSanRg\TRW-Win11-
tpm-BL-TEMPLATE.template" -TenancyType Shared  -FunctionalLevel "L7_20"
```

```
-Validate

$result.TerminatingError | Format-List -Property *
```

エラーメッセージ：

```
ErrorData    : {[[ValidationFailureCount, xxx], [InvalidMemoryValue,
The memory size provided 6143 must be a multiple of 4 MB and must be
greater than or equal to 4 MB.], [InconsistentGuestOsSetting, The
GuestOs setting - windows9_64Guest of the selected machine profile does
not match with the setting - windows2019srv_64Guest of master image.
Please select a machine profile that matches the GuestOs setting of the
master image.], [InconsistentVtpmSetting, The vTPM setting of the
selected machine profile does not match with the selected master image.
Please select a machine profile that matches the vTPM setting of the
master image.], [InconsistentFirmwareSetting, The firmware setting -
efi of the selected machine profile does not match with the setting -
bios of master image. Please select a machine profile that matches the
firmware setting of the master image ErrorId      : ValidationFailure

ErrorMessage : ValidationFailure

Operation    : ValidatingInputs
```

4. 構成設定を検証した後、実際のIDプール名と正しいパラメーターを使用してMCSマシンカタログを作成できます。

次のステップ

特定のクラウドサービスカタログの作成については、以下を参照してください。

- AWS カタログを作成する
- XenServerカタログを作成する
- Google Cloud Platform カタログを作成する
- Microsoft Azure カタログを作成する
- Microsoft System Center Virtual Machine Manager カタログを作成する
- Nutanix カタログを作成する
- VMwareカタログを作成する

これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。

設定プロセス全体を確認するには、インストールと構成を参照してください。

Web StudioとPowerShellを使用してCitrix Provisioningカタログを作成できます。 この実装には、次の利点があります。

- MCSとCitrix Provisioningカタログの両方を管理するための単一の統合コンソール。
- ID管理ソリューション、オンデマンドプロビジョニングなどのCitrix Provisioningカタログの新機能があります。

現在、この機能はAzureおよびVMwareワークロードでのみ利用可能です。ただし、VMware環境では、現在PowerShellコマンドのみを使用してカタログを作成できます。詳細については、Citrix StudioでCitrix Provisioningカタログを作成するを参照してください。

詳細情報

- 接続とリソースの作成および管理(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/connections.html)
- 異なる結合タイプのカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/create-machine-identities-joined-catalogs.html)
- マシンカタログの管理(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-manage.html)

AWSカタログを作成する

マシンカタログの作成では、マシンカタログを作成するウィザードについて説明しています。以下の情報は、AWS仮想化環境に固有の詳細を扱っています。

> **注:**
>
> AWSカタログを作成する前に、AWSへの接続の作成を完了する必要があります。AWSへの接続を参照してください。

制限事項

Citrix Virtual Apps and Desktops™ 2203 LTSR以降では、MCS AWSプラグインが `DescribeInstanceTypes` AWS API呼び出しを行い、それが成功すると、MCSはAPI応答から作成されたインベントリ名を使用します。

したがって、CVAD 1912から2203以降にアップグレードする場合は、AWSの `DefineInstanceType` 権限を無効にし、`Set-ProvScheme` コマンドを使用して既存のカタログを更新してAWSの命名スキームに合わせます。その後、カタログの更新が完了し、サービス提供がAWSの命名スキームに一致したら、`DescribeInstanceType` 権限を再度追加します。

イメージ準備中のネットワーク設定

イメージ準備中に、元のVMに基づいて準備用仮想マシン（VM）が作成されます。この準備用VMはネットワークから切断されます。準備用VMからネットワークを切断するために、すべてのインバウンドおよびアウトバウンドトラフィックを拒否するネットワークセキュリティグループが作成されます。このネットワークセキュリティグループは永続化され、再利用されます。ネットワークセキュリティグループの名前は `Citrix.XenDesktop.IsolationGroup-GUID` で、GUIDはランダムに生成されます。

AWSテナンシーを構成する

AWSは以下のテナンシーオプションを提供します。

- 共有テナンシー（デフォルトタイプ）：異なる顧客の複数のAmazon EC2インスタンスが同じ物理ハードウェア上に存在する場合があります。
- 専用テナンシー：EC2インスタンスは、デプロイした他のインスタンスと同じハードウェア上でのみ実行されます。他の顧客は同じハードウェアを使用しません。

PowerShellを使用して、MCSでAWS専用ホストをプロビジョニングできます。

PowerShellを使用したAWS専用ホストテナンシーの構成

PowerShellを通じてホストテナンシーが定義されたマシンカタログを作成できます。

Amazon 専用ホストは、インスタンス容量を持つ物理サーバーであり、完全に専用であるため、既存のソケットごとまたはVMごとのソフトウェアライセンスを使用できます。

専用ホストには、インスタンスタイプに基づいて事前設定された利用率があります。たとえば、C4 Large インスタンスタイプの単一の割り当てられた専用ホストは、16 インスタンスの実行に制限されます。詳細については、AWS サイト を参照してください。

AWSホストへのプロビジョニングの要件は次のとおりです。

- インポートされたBYOL（bring your own license）イメージ（AMI）。専用ホストでは、既存のライセンスを使用および管理します。
- プロビジョニング要求を満たすのに十分な利用率を持つ専用ホストの割り当て。
- **自動配置**を有効にします。

PowerShell を使用して AWS の専用ホストにプロビジョニングするには、**New-ProvScheme** コマンドレットを、パラメーター `TenancyType` を *Host* に設定して使用します。

詳細については、Citrix Developer Documentation を参照してください。

AMI からマシンプロパティをキャプチャする

AWS で Machine Creation Services (MCS) を使用してマシンをプロビジョニングするためのカタログを作成するときは、そのカタログのマスター/ゴールデンイメージを表す AMI を選択します。その AMI から、MCS はディスクのスナップショットを使用します。以前のリリースでは、マシンにロールやタグを設定したい場合、AWS コンソールを使用して個別に設定していました。この機能はデフォルトで有効になっています。

> **ヒント:**
>
> AWS インスタンスプロパティキャプチャを使用するには、AMI に関連付けられた VM が必要です。

> このプロセスを改善するために、**MCS は** AMI が取得されたインスタンスからプロパティを読み取り、そのマシンの Identity Access Management (IAM) ロールとタグを、特定のカタログ用にプロビジョニングされたマシンに適用します。このオプション機能を使用する場合、カタログ作成プロセスは、選択された AMI ソースインスタンスを見つけ、限られたプロパティセットを読み取ります。これらのプロパティは AWS Launch Template に保存され、そのカタログのマシンをプロビジョニングするために使用されます。カタログ内のすべてのマシンは、キャプチャされたインスタンスプロパティを継承します。

キャプチャされるプロパティには以下が含まれます。

- IAMロール – プロビジョニングされたインスタンスに適用されます。
- タグ – プロビジョニングされたインスタンス、そのディスク、およびNICに適用されます。これらのタグは、S3バケットとオブジェクト、AMI、スナップショット、起動テンプレートを含む、一時的なCitrix®リソースに適用されます。

> **ヒント:**
>
> 一時的なCitrixリソースのタグ付けはオプションであり、カスタムプロパティ `AwsOperationalResourcesTagging` を使用して構成できます。

AWS インスタンスプロパティをキャプチャする

AWSホスティング接続のプロビジョニングスキームを作成する際に、カスタムプロパティ `AwsCaptureInstanceProperties` を指定することで、この機能を使用できます。

`New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true" …<standard provscheme parameters`

詳細については、Citrix Developer Documentation を参照してください。

> **注:**
>
> `AwsCaptureInstanceProperties` は非推奨です。代わりに、VMのプロパティを指定するにはマシンプロファイルを使用することをお勧めします。

マシンプロファイルからマシンプロパティをキャプチャする

MCSを使用してAWSマシンをプロビジョニングするためのカタログを作成する際、マシンプロファイルを使用して特定のマシンプロパティ設定をプリセットできます。

これを行うには、次の手順に従います。

1. このカタログを作成するリソースと同じアベイラビリティゾーンにマシンプロファイルを保存します。
2. カタログ作成ウィザードの ページで、 を選択します。選択したリソースと同じアベイラビリティゾーンにあるマシンプロファイルが表示されます。
3. 必要に応じてマシンプロファイルを選択します。

> **注：**
>
> マシンプロファイルまたはAMIのいずれかを使用して、マシンのプロパティをキャプチャできます。Web Studioで、**マシンプロファイルを使用**を選択すると、**仮想マシンにマシンテンプレートプロパティを適用**オプションは自動的に非表示になります。

AWS運用リソースのタグ付け

MCSを使用してAWSでマシンをプロビジョニングするためのカタログを作成する際、IAMロールとタグプロパティをそれらのマシンに適用するかどうかを制御できます。また、マシンタグを運用リソースに適用するかどうかも制御できます。

Amazon Machine Image (AMI) は、Amazon Cloud環境内で仮想マシンを作成するために使用される仮想アプライアンスの一種であり、一般にEC2と呼ばれます。AMIを使用して、EC2環境を使用するサービスを展開します。MCS for AWSを使用してマシンをプロビジョニングするためのカタログを作成する際、そのカタログのゴールデンイメージとして機能する**AMI**を選択します。

> **重要：**

> インスタンスプロパティと起動テンプレートをキャプチャしてカタログを作成することは、運用リソースのタグ付けを使用するために必要です。

> AWSカタログを作成するには、まずゴールデンイメージとするインスタンスのAMIを作成する必要があります。MCSはそのインスタンスからタグを読み取り、起動テンプレートに組み込みます。その後、起動テンプレートのタグは、AWS環境で作成されたすべてのCitrixリソースに適用されます。これには以下が含まれます。

- 仮想マシン
- VMディスク
- VMネットワークインターフェイス
- S3バケット
- S3オブジェクト
- 起動テンプレート
- エーエムアイ

運用リソースにタグ付けする

PowerShell を使用してリソースにタグを付けるには:

1. DDC ホストから PowerShell ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、コマンド `asnp citrix` を実行します。

プロビジョニングされた VM のリソースにタグを付けるには、新しいカスタムプロパティ `AwsOperationalResourcesTagging` を使用します。このプロパティの構文は次のとおりです。

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true;AwsOperationalResourcesTagging,true" …<standard provscheme parameters>
```

VM のタグをコピー

NIC、およびマシンプロファイルで指定されたディスク（ID ディスク、ライトバックキャッシュディスク、OS ディスク）上のタグを、MCS マシンカタログで新しく作成された VM にコピーできます。これらのタグは、マシンプロファイルソース（AWS VM インスタンスまたは AWS 起動テンプレートバージョン）のいずれかで指定できます。この機能は、永続および非永続マシンカタログと VM に適用されます。

注:

- AWS EC2 コンソールでは、**起動テンプレートバージョンリソースタグ**の下に**ネットワークインターフェイスのタグ付け**の値は表示されません。ただし、PowerShell コマンド `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` を実行してタグの仕様を確認できます。
- マシンプロファイルソース（VM または起動テンプレートバージョン）に 2 つのネットワークインターフェイス（eni-1 と eni-2）があり、eni-1 にタグ t1、eni-2 にタグ t2 がある場合、VM は両方のネットワークインターフェイスのタグを取得します。

マシンプロファイルを使用してカタログを作成する

マシンプロファイルを使用して、EC2インスタンス (VM) または起動テンプレートバージョンからハードウェアプロパティを取得し、プロビジョニングされたマシンに適用できます。取得されるプロパティには、例えば、EBSボリュームプロパティ、インスタンスタイプ、EBS最適化、CPUオプション、テナンシータイプ、ハイバネーション機能、その他のサポートされているAWS構成が含まれます。

マシンプロファイルの入力として、AWS EC2インスタンス (VM) またはAWS起動テンプレートバージョンを使用できます。

注：

- EBSボリュームのプロパティは、マシンプロファイルからのみ派生します。
- MCSは、GP3ボリュームタイプのIDディスクを持つVMをプロビジョニングします。GP3ボリュームタイプはAWSが提供する最も安価なオプションであるため、この機能はコストを最小限に抑えます。この実装は、新しいカタログに追加されたVMと、既存のカタログに追加された新しいVMにのみ適用されます。この機能が導入される前に作成された既

> 存のVMは、IDディスクがリセットされない限り、GP2ボリュームタイプのIDディスクを引き続き使用します。

重要な考慮事項

MCSマシンカタログを作成する際の重要な考慮事項：

- `New-ProvScheme`および`Set-ProvScheme`コマンドでマシンハードウェアプロパティパラメータを追加すると、パラメータで指定された値がマシンプロファイルの値よりも優先されます。
- `AwsCaptureInstanceProperties`を`true`として設定し、`MachineProfile`プロパティを設定しない場合、IAMロールとタグのみがキャプチャされます。
- `AwsCaptureInstanceProperties`と`MachineProfile`を同時に設定することはできません。

  > **注：
  >
  > `AwsCaptureInstanceProperties` は非推奨です。

- マシンプロファイルが提供されていない場合は、以下のプロパティの値を明示的に指定する必要があります。
  - セキュリティグループ
  - ENI または仮想ネットワーク
- `AwsOperationalResourcesTagging` は、`AwsCaptureInstanceProperties` を有効にするか、マシンプロファイルを指定した場合にのみ有効にできます。

MCSマシンカタログ作成後の重要な考慮事項：

- マシンプロファイルベースのカタログから非マシンプロファイルベースのカタログにカタログを変更することはできません。

マシンプロファイルを使用してマシンカタログを作成する

マシンプロファイルを使用してマシンカタログを作成するには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。

3. まだ作成されていない場合は、IDプールを作成します。例：

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain abcdf -NamingSchemeType Numeric
```

4. New-ProvSchemeコマンドを実行します。例：

```
New-ProvScheme -ProvisioningSchemeName demet-test-1

-HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1

-IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4

-CleanOnBoot

-MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-demet-
ami.0 (ami-0ca813xxxxxx061ef).template'

-MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-
east-1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).vm'
```

5. カタログの作成を完了します。詳しくは、「Citrix PowerShell SDK」を参照してください。

マシンプロファイルを更新する

マシンプロファイルで最初にプロビジョニングされたカタログのマシンプロファイルを更新するには、次の手順を実行します。MCSマシンカタログを編集する際に、マシンプロファイルソースのテナンシータイプとハイバネーション機能を変更することもできます。

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme `

-ProvisioningSchemeUid "<ID" `

-MachineProfile "XDHyp:\HostingUnits\abc\us-
east-1a.availabilityzone\citrix-cvad-machineprofile-instance
(i-0xxxxxxxx).vm"
```

起動テンプレートバージョンでカタログを作成する

起動テンプレートバージョンをマシンプロファイル入力として使用して、MCSマシンカタログを作成できます。また、マシンプロファイルカタログの入力をVMから起動テンプレートバージョンへ、または起動テンプレートバージョンからVMへ更新することもできます。

AWS EC2コンソールで、起動テンプレートのインスタンス構成情報をバージョン番号とともに提供できます。マシンカタログの作成または更新時に、起動テンプレートバージョンをマシンプロファイル入力として指定すると、その起動テンプレートバージョンのプロパティがプロビジョニングされたVDA VMにコピーされます。

以下のプロパティは、マシンプロファイル入力を使用するか、`New-ProvScheme`または`Set-ProvScheme`コマンドで明示的にパラメーターとして指定できます。`New-ProvScheme`または`Set-ProvScheme`コマンドで指定された場合、これらのプロパティのマシンプロファイル値よりも優先されます。

- サービスオファリング
- ネットワーク
- セキュリティグループ
- テナンシータイプ

> **注:**
>
> マシンプロファイルの起動テンプレートでサービス提供が指定されていない場合、または`New-ProvScheme`コマンドのパラメーターとして指定されていない場合、適切なエラーが発生します。

> マシンプロファイルの入力として起動テンプレートバージョンを使用してカタログを作成するには:

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. 起動テンプレートの起動テンプレートバージョンの一覧を取得します。例:

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate> ls |
Select FullPath
```

4. 作成されていない場合は、IDプールを作成します。例:

```
New-AcctIdentityPool `

-IdentityPoolName "abc11" `

-NamingScheme "abc1-##" `

-NamingSchemeType Numeric `

-Domain "citrix-xxxxxx.local" `

-ZoneUid "xxxxxxxx" `
```

5. マシンプロファイルの入力として起動テンプレートバージョンを使用してプロビジョニングスキームを作成します。例:

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-persistent-
vda-win2022 (ami-0axxxxxxxxxxx).template" `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

6. プロビジョニングスキームをブローカーカタログとして登録します。例：

```
New-BrokerCatalog -Name "MPLT1" `

-AllocationType Random `

-Description "Machine profile catalog" `
```

```
-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `

-ProvisioningType Mcs `

-SessionSupport MultiSession `

-PersistUserChanges Discard
```

7. カタログの作成を完了します。詳細については、「Citrix PowerShell SDK」を参照してください。

マシンプロファイルカタログの入力を、VMから起動テンプレートバージョンへ、または起動テンプレートバージョンからVMへ更新することもできます。例:

- VMから起動テンプレートバージョンへ、マシンプロファイルカタログの入力を更新するには：

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-0bxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxx
(1).launchtemplateversion"
```

- 起動テンプレートバージョンからVMへ、マシンプロファイルカタログの入力を更新するには：

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-
east-1a.availabilityzone\apollo-non-persistent-vda-win2022-2
(i-08xxxxxxxx).vm"
```

OSディスクとIDディスクの暗号化

AWS KMSキー（カスタマーマネージドキーおよびAWSマネージドキー）を使用して、OSディスクとIDディスクの暗号化に使用できる永続的および非永続的なVMカタログを作成できます。

- AWSマネージドキーは毎年自動的にローテーションされます。
- カスタマーマネージドキーは自動ローテーションがオプションであり、手動で管理できます。

KMSキーの詳細については、以下のAWSドキュメントを参照してください。

- AWS KMSの概念
- 自動キーローテーションの仕組み。

OSディスクとIDディスクの暗号化には、次のいずれかを構成します。

- 暗号化されたマスターイメージを使用する（例：KMSキーで暗号化されたEBSルートボリュームを含むインスタンスまたはスナップショットから作成されたAMI）
- 暗号化されたEBSルートボリュームを含むマシンプロファイルソース（VMまたは起動テンプレート）を使用する。

制限事項

以下の制限事項を考慮してください。

- MCS は現在、マスターイメージ AMI 上のディスクを 1 つのみサポートしています。
- 既存の暗号化されていない EBS ボリュームまたはスナップショットを直接暗号化したり、既存の暗号化されたボリュームの KMS キーを変更したりすることはできません。これを行うには、次の手順を実行する必要があります。

  a. そのボリュームの新しいスナップショットを作成します。

  b. そのスナップショットから新しいボリュームを作成します。

  c. 新しいボリュームを暗号化します。

以下の AWS ドキュメントを参照してください。

- 暗号化されていないリソースを暗号化する
- EBSボリュームの自動またはデフォルトの暗号化の制限: 既存および新規のAmazon EBSボリュームを自動的に暗号化する。

ディスク暗号化を使用してカタログを作成する

ディスク暗号化を使用してMCSマシンカタログを作成するには、次の方法があります。

- マスターイメージ
- マシンプロファイル

ディスク暗号化にマシンプロファイル入力を使用する際の考慮事項:

- マシンプロファイル入力のKMSキーは、マスターイメージのKMSキーよりも優先されます。

- マシンプロファイル入力が提供されない場合、マスターイメージAMIのKMSキーがカタログVMのディスクを暗号化するために使用されます。
- マシンプロファイルにブロックデバイスマッピングが存在する場合、マスターイメージテンプレート（AMI）とマシンプロファイルに存在するブロックデバイスは一致している必要があります。たとえば、AMIに`/dev/sda1`で定義されたデバイスがある場合、マシンプロファイルにも`/dev/sda1`で定義されたデバイスが必要です。
- マシンプロファイルソースにキーがなく、マスターイメージが暗号化されていない場合、カタログVMのディスクは暗号化されません。
- マスターイメージが暗号化されている場合、マシンプロファイルソースVMまたは起動テンプレートには、有効な入力と見なされるために暗号化されたルートボリュームが必要です。

既存のカタログを変更する

`Set-ProvScheme`を使用して既存のカタログを変更し、以下を持たせることができます。

- 新しいKMSキーを含むボリュームを持つマシンプロファイル入力。
- 新しいKMSキーで暗号化されたマスターイメージテンプレートAMI。

重要な考慮事項

- カタログに追加された新しいVMのボリュームは、新しいKMSキーで暗号化されます。
- 既存のマシンプロファイルがある場合に暗号化設定を更新するには、新しいマシンプロファイルで`Set-ProvScheme`を実行します。
- 既存のカタログを、暗号化されたボリュームから暗号化されていないボリュームに変更することはできません。 暗号化されたマスターAMIから暗号化されていないマスターAMIへのイメージ更新はできません。

VMインスタンスでNitroTPMとUEFIセキュアブートを有効にする

カタログを作成する際、NitroTPMおよび/またはUEFIセキュアブートが有効なマスターイメージ（AMI）を選択できるようになりました。これにより、カタログ内のプロビジョニングされたVMもNitroTPMおよび/またはUEFIセキュアブートが有効になります。この実装により、VMのセキュリティと信頼性が確保されます。NitroTPMとUEFIセキュアブートの詳細については、Amazonドキュメントを参照してください。

制限事項

- 現在、中国を除くすべてのAWSリージョン（AWS GovCloud (US) リージョンを含む）で、NitroTPMとセキュアブートの両方を使用できます。

- 既存のカタログでNitroTPMとUEFIセキュアブートを有効にすることはできません。NitroTPMとUEFIセキュアブートが有効なカタログが必要な場合は、新しいカタログを作成してください。

主な手順

1. AWS環境をセットアップします。
2. AWSへの接続を作成します。
3. NitroTPMおよび/またはUEFIセキュアブートが有効なマスターイメージ (AMI) を作成する (#create-an-ami-that-supports-nitrotpm-and-uefi-secure-boot)。
4. Web StudioのカタログでNitroTPMおよびUEFIセキュアブートが有効なマスターイメージを選択するか、PowerShellコマンドを使用してプロビジョニングスキームを作成することで、マシンカタログを作成します。

作成されたカタログに追加されたVMには、NitroTPMとUEFIセキュアブートが有効になっています。

NitroTPMとUEFIセキュアブートをサポートするAMIを作成する

1. NitroTPMおよび/またはUEFIセキュアブートが有効なVMからAMIを作成できます。
   a. AWS Marketplaceイメージを使用してインスタンスを作成します。例: `TPM-Windows_Server-2022-English-Full-Base on the aws-marketplace`を検索します。
   b. シングルセッションまたはマルチセッションVDAをダウンロードします。
   c. そのVMからAMIを作成します。
2. register-imageコマンドを使用します。

   ```
   --boot-mode (string)

   --tpm-support (string)
   ```

   詳しくは、register-imageを参照してください。

以下のAWSドキュメントを参照してください。

- EC2インスタンスタイプのサポートされているブートモードを決定する
- Amazon EC2 インスタンスで NitroTPM を使用するための要件/.

Delivery Controller™ ホストから PowerShell ウィンドウを開き、特定の項目を確認できます。

- サービス提供が NitroTPM または UEFI セキュアブートをサポートしているか

```
(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.BootMode

(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.NitroTpmSupportVersions
```

- テンプレートが NitroTPM または UEFI セキュアブートをサポートしているか

```
(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.BootMode



(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.TpmSupport
```

既存のカタログのサービスオファリングを更新する

`Set-ProvScheme` を使用して、既存のカタログのサービス提供を変更できます。この変更は、新しく追加された VM に適用されます。ただし、次のシナリオではエラーが発生します。

AMI のブートモード	AMI は NITRO TPM をサポートしていますか？	サービス提供は NITROTPM と UEFI セキュアブートをサポートしていますか？
UEFI	いいえ	いいえ
レガシー BIOS	はい	いいえ
UEFI	はい	いいえ
UEFI優先	はい	いいえ

VMインスタンスのフィルタリング

マシンプロファイルVMとして使用するAWS EC2インスタンスは、マシンカタログが正しく作成され、機能するために互換性がある必要があります。マシンプロファイルの入力VMとして使用できるAWS EC2インスタンスを一覧表示するには、`Get-HypInventoryItem` コマンドを使用でき

ます。このコマンドは、ホスティングユニットで利用可能なVMのインベントリをページングおよびフィルタリングできます。

ページネーション:

Get-HypInventoryItem は、2つのページネーションモードをサポートしています。

- ページングモードは、`-MaxRecords`および`-Skip`パラメーターを使用してアイテムのセットを返します。
  - `-MaxRecords`: デフォルトは**1**です。これは、返されるアイテムの数を制御します。
  - `-Skip`: デフォルトは**0**です。これは、ハイパーバイザー内のリストの絶対的な先頭（または絶対的な末尾）からスキップするアイテムの数を制御します。
- スクロールモードは、`-MaxRecords`、`-ForwardDirection`、および`-ContinuationToken`パラメーターを使用してレコードのスクロールを可能にします。
  - `-ForwardDirection`: デフォルトは**True**です。これは`-MaxRecords`と組み合わせて使用され、一致するレコードの次のセットまたは前のセットのいずれかを返します。
  - `-ContinuationToken`: `ContinuationToken` で指定された項目を含まず、その直後にある項目 (または、`ForwardDirection` が **false** の場合はその前にある項目) を返します。

ページネーションの例:

- 最も名前が小さいマシンテンプレートの単一のレコードを返すには。`AdditionalData`フィールドには`TotalItemsCount`と`TotalFilteredItemsCount`があります:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template
```

- 最も名前が小さいマシンテンプレートのレコードを10個返すには:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 10 | select Name
```

- 最も名前の大きいレコードで終わるレコードの配列を返します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ForwardDirection $False -MaxRecords 10 | select
Name
```

- 指定された `ContinuationToken` に関連付けられたマシンテンプレートから始まるレコードの配列を返します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ContinuationToken "ami-07xxxxxxxxx"
-MaxRecords 10
```

フィルタリング:

フィルタリングでは、以下の追加のオプションパラメーターがサポートされています。これらのパラメーターは、ページネーションオプションと組み合わせることができます。

- `-ContainsName "my_name"`: 指定された文字列がAMI名の一部と一致する場合、そのAMIは `Get` 結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -ContainName ‘apollo’ | select
Name
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: AMIにこれらのタグの少なくとも1つがある場合、それは `Get` 結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -Tags '{"opex owner": "Not
tagged"}' | select Name
```

> **注:**
>
> 2つのタグ値がサポートされています。**タグなし** のタグ値は、タグのリストに指定されたタグがない項目と一致します。**すべての値** のタグ値は、タグの値に関係なくタグを持つ項目と一致します。それ以外の場合、一致は、項目にタグがあり、その値がフィルターで指定されたものと等しい場合にのみ発生します。

- `-Id "ami-0a2d913927e0352f3"`: AMIが指定されたIDと一致する場合、それは `Get` 結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -Id ami-xxxxxxxxxxxx
```

AdditionalDataパラメーターでのフィルタリング:

`AdditionalData`フィルターパラメータは、テンプレートまたはVMを、その機能、サービス提供、またはAdditionalDataにある任意のプロパティに基づいてリストします。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200).AdditionalData
```

互換性のないVMを示すために、`-Warn` パラメーターを追加することもできます。VMには、**Warning** という名前の `AdditionalData` フィールドが含まれます。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-015xxxxxxxxx"
-Warn $true).AdditionalData
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、「」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure.html)を参照してください。
- カタログを管理するには、「マシンカタログの管理」および「AWSカタログの管理」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- AWSへの接続
- マシンカタログの作成

XenServer®カタログを作成する

マシンカタログの作成は、マシンカタログを作成するウィザードについて説明しています。以下の情報は、XenServer仮想化環境に固有の詳細を扱っています。

> **注：**
>
> XenServerカタログを作成する前に、XenServerへの接続の作成を完了する必要があります。XenServerへの接続を参照してください。

XenServer接続を使用してマシンカタログを作成する

GPU対応マシンには専用のマスターイメージが必要です。これらのVMには、GPUをサポートするビデオカードドライバーが必要です。GPU対応マシンを構成して、VMがGPUを操作に使用するソフトウェアで動作できるようにします。

1. XenCenter®で、標準VGA、ネットワーク、およびvCPUを備えたVMを作成します。
2. VM構成を更新して、GPUの使用（パススルーまたはvGPUのいずれか）を有効にします。
3. サポートされているオペレーティングシステムをインストールし、RDPを有効にします。
4. Citrix VM ToolsおよびNVIDIAドライバーをインストールします。
5. Virtual Network Computing (VNC) 管理コンソールをクリアしてパフォーマンスを最適化し、VMを再起動します。
6. RDPを使用するように求められます。RDPを使用してVDAをインストールし、VMを再起動します。
7. 必要に応じて、VMのスナップショットを他のGPUマスターイメージのベースラインテンプレートとして作成します。
8. RDPを使用して、XenCenterで構成されGPU機能を使用する顧客固有のアプリケーションをインストールします。

制限事項

- Citrix Hypervisor 8.2 Cumulative Update 1でホストされているVMを使用するCitrix Virtual Apps and Desktops展開で、単一のMCSカタログで複数のGFS2 SRを使用している場合、展開中にカタログ内のVMがVDIにアクセスできません。「VDI is currently in use」というエラーが報告されます。
- Citrix Hypervisor 8.2 Cumulative Update 1は、GFS2 SRを使用するMCSフルクローンVMをサポートしていません。

詳細については、制約を参照してください。

これらの制約は、XenServer 8 以降には適用されません。

マシンプロファイルを使用してマシンカタログを作成する

MCSを使用してマシンをプロビジョニングするカタログを作成するとき、マシンプロファイルを使用して、仮想マシンからハードウェアプロパティをキャプチャし、カタログ内の新しくプロビジョニングされたVMに適用できます。`MachineProfile`パラメーターが使用されていない場合、ハードウェアプロパティはマスターイメージVMまたはスナップショットからキャプチャされます。

> **注:**
>
> 現在、マシンプロファイルの入力としてVMのみを使用できます。

> 次のパラメータを明示的に構成することで、マシンプロファイルの入力にあるパラメータの値を上書きできます。

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

マシンプロファイルを使用してカタログを作成するには：

1. PowerShellウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. IDプールを作成します。IDプールは、作成されるVMのActive Directory (AD) アカウントのコンテナです。例:

   ```
   New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -IdentityPoolName
   "ExampleIdentityPool" -NamingScheme "abc1-##" -NamingSchemeType
   "Numeric" -Scope @() -ZoneUid "xxxxxxxx"
   ```

4. Active Directoryで必要なADコンピューターアカウントを作成します。

   ```
   $password = "password123" | ConvertTo-SecureString -AsPlainText -Force

   New-AcctIdentity -IdentityPoolName "ExampleIdentityPool" -Count 10
   -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
   ```

```
Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
```

5. `New-ProvScheme`コマンドを実行してカタログを作成します。例:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
-IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

</CustomProperties>'

-MasterImageVM "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleVDA.vm\ExampleVDA.snapshot"
-ProvisioningSchemeName "ExampleCatalog" -Scope @() -SecurityGroup @()

-MachineProfile "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfile.vm"
```

6. プロビジョニングスキームをブローカーカタログとして登録します。例:

```
$ConfigZone = Get-ConfigZone | Where-Object { $_.Name -eq "xxxxxx" }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -Description
"Machine profile catalog" -ProvisioningSchemeId fe7df345-244e-4xxxx-
xxxxxxxxx -ProvisioningType Mcs -SessionSupport MultiSession
-PersistUserChanges Discard -ZoneUid ($ConfigZone.Uid)
```

7. カタログにVMを追加します。

新しいマシンプロファイルでカタログを更新するには:

1. `Set-ProvScheme`コマンドを実行します。例:

```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -MachineProfile
"XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfileVm.vm\ExampleMach
ineProfileSnapshot.snapshot"
```

Set-ProvSchemeコマンドの詳細については、Set-ProvSchemeを参照してください。

注:

- この場合、`Set-ProvScheme`コマンドはカタログ内の既存のVMのマシンプロファイルを変更しません。カタログに追加された新しく作成されたVMのみが新しいマシンプロファイルを持ちます。
- マシンプロファイルベースのマシンカタログを、非マシンプロファイルベースのマシンカタログに変換することはできません。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループを作成するように案内します
- 構成プロセス全体を確認するには、インストールと構成を参照してください
- カタログを管理するには、マシンカタログの管理およびXenServerカタログの管理を参照してください

詳細情報

- 接続とリソースの作成および管理
- XenServerへの接続
- マシンカタログの作成

Google Cloud Platformカタログを作成する

(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create.html)は、マシンカタログを作成するウィザードについて説明しています。以下の情報は、Googleクラウド環境に固有の詳細を扱っています。

注:

> Google Cloud Platform (GCP) カタログを作成する前に、GCPへの接続の作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/connections/connection-gcp.html)を参照してください。

マスターVMインスタンスと永続ディスクを準備する

> **ヒント:**
>
> 永続ディスクは、仮想ディスクを指すGoogle Cloudの用語です。

> マスターVMインスタンスを準備するには、計画しているマシンカタログ内のクローンVDAインスタンスに求める構成と一致するプロパティを持つVMインスタンスを作成および構成します。この構成は、インスタンスのサイズとタイプにのみ適用されるわけではありません。メタデータ、タグ、GPU割り当て、ネットワークタグ、サービスアカウントのプロパティなどのインスタンス属性も含まれます。

マスタリングプロセスの一環として、MCSはマスターVMインスタンスを使用してGoogle Cloudの*インスタンステンプレート*を作成します。このインスタンステンプレートは、マシンカタログを構成するクローンVDAインスタンスの作成に使用されます。クローンインスタンスは、インスタンステンプレートが作成されたマスターVMインスタンスのプロパティ（VPC、サブネット、永続ディスクのプロパティを除く）を継承します。

マスターVMインスタンスのプロパティを要件に合わせて構成したら、インスタンスを起動し、そのインスタンスの永続ディスクを準備します。

ディスクのスナップショットまたはディスクのイメージを手動で作成することをお勧めします。これにより、意味のある命名規則を使用してバージョンを追跡し、マスターイメージの以前のバージョンを管理するためのより多くのオプションが得られ、マシンカタログ作成の時間を節約できます。独自のスナップショットを作成しない場合、MCSは一時的なスナップショットを作成します（これはプロビジョニングプロセスの終了時に削除されます）。OSディスクまたはイメージのマルチリージョンスナップショットを手動で作成すると、異なるGCPリージョンのマシンカタログに同じマスターイメージを使用することもできます。

マシンカタログを作成する

マシンカタログは、次の2つの方法で作成できます。

- (/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create/create-machine-catalog-gcp.html#create-a-machine-catalog-using-web-studio)
- (/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create/create-machine-catalog-gcp.html#create-a-machine-catalog-using-powershell)

Web Studio を使用してマシンカタログを作成する

> **注:**
>
> マシンカタログを作成する前に、リソースを作成してください。マシンカタログを構成する際は、Google Cloud で確立されている命名規則を使用してください。詳細については、「バケットとオブジェクトの命名ガイドライン」を参照してください。

(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create.html)のガイダンスに従ってください。以下の説明は、Google Cloud カタログに固有のものです。

1. Web Studio にサインインし、左側のペインで を選択します。
2. アクションバーで を選択します。
3. ページで、 を選択し、 を選択します。
   - Citrix Virtual Apps and Desktops™ は、シングルセッションOSもサポートしています。
4. ページで、 と オプションを選択し、 を選択します。複数のリソースがある場合は、メニューから1つ選択します。
5. ページで、必要に応じてこれらの手順を完了し、 をクリックします。
   a. マスターイメージとしてスナップショットまたはVMを選択します。単一テナンシー機能を使用する場合は、ノードグループプロパティが正しく構成されているイメージを選択してください。「ゾーン選択の有効化」を参照してください。
   b. 既存のVMをマシンプロファイルとして使用するには、「マシンプロファイルを使用」を選択し、その後、VMを選択します。

      > **注:**
      >
      > 現在、このカタログ内のVMは、ディスク暗号化セットID、マシンサイズ、ストレージタイプ、およびゾーン設定をマシンプロファイルから継承します。

c. カタログの最小機能レベルを選択します。単一テナンシー機能を使用する場合は、ノードグループプロパティが正しく構成されているイメージを選択してください。

6. 「**ストレージの種類**」ページで、このマシンカタログのオペレーティングシステムを格納するために使用するストレージの種類を選択します。以下の各ストレージオプションには、それぞれ独自の価格とパフォーマンス特性があります。（IDディスクは常にゾーン標準永続ディスクを使用して作成されます。）

   - 標準永続ディスク
   - バランス永続ディスク
   - SSD永続ディスク

   Google Cloud のストレージオプションの詳細については、`<https://cloud.google.com/compute/docs/disks/>`を参照してください。

7. 「**仮想マシン**」ページで、作成するVMの数を指定し、VMの詳細な仕様を確認してから、「**次へ**」を選択します。マシンカタログに単一テナントノードグループを使用する場合は、予約済みの単一テナントノードが利用可能なゾーンを**のみ**選択するようにしてください。ゾーン選択を有効にするを参照してください。

8. **ディスク設定**ページで、次の設定を構成できます。

   - ライトバックキャッシュを有効にするかどうかを選択します。ライトバックキャッシュを有効にすると、次のことができます。

     - 一時データのキャッシュに使用するディスクとRAMのサイズを構成します。詳細については、一時データのキャッシュを構成するを参照してください。
     - ライトバックキャッシュディスクのストレージタイプを選択します。ライトバックキャッシュディスクには、次のストレージオプションを使用できます。

       - 標準永続ディスク
       - バランス永続ディスク
       - SSD永続ディスク

       Google Cloudのストレージオプションの詳細については、「ストレージオプション」を参照してください。

     - ライトバックキャッシュディスクの種類を選択します。

       - **非永続ライトバックキャッシュディスクを使用する**。選択した場合、ライトバックキャッシュディスクはプロビジョニングされたVMに永続しません。ディスクは電

源サイクル中に削除され、ディスクにリダイレクトされたデータはすべて失われます。

- **永続ライトバックキャッシュディスクを使用する**。選択した場合、ライトバックキャッシュディスクはプロビジョニングされたVMに永続します。このオプションを有効にすると、ストレージコストが増加します。

- MCSストレージ最適化（MCS I/O）が有効になっている場合、次のいずれかを実行できます。
  - 電源サイクル中にVDAのシステムディスクを保持するかどうかを選択します。詳しくは、「MCSストレージ最適化の更新を有効にする」を参照してください。
  - メモリとディスクキャッシュのサイズを更新します。
- ディスクコンテンツを保護するために独自のキーを使用するかどうかを選択します。この機能を使用するには、まず独自の顧客管理暗号化キー（CMEK）を作成する必要があります。詳しくは、「顧客管理暗号化キー（CMEK）を使用する」を参照してください。

> **注:**
>
> Studioインターフェイスでのみ利用可能です。
>
> キーを作成した後、リストからいずれかのキーを選択できます。カタログを作成した後は、キーを変更できません。Google Cloudは、既存の永続ディスクまたはイメージでのキーのローテーションをサポートしていません。したがって、カタログをプロビジョニングした後、カタログは特定のバージョンのキーに紐付けられます。そのキーが無効化または破棄された場合、キーが再度有効化または復元されるまで、そのキーで暗号化されたインスタンスとディスクは使用できなくなります。

9. ページで、Active Directory アカウントを選択し、 を選択します。
   - **新しいActive Directoryアカウントを作成する**を選択した場合は、ドメインを選択し、Active Directoryで作成されるプロビジョニングされたVMコンピューターアカウントの命名スキームを表す文字のシーケンスを入力します。アカウント命名スキームは1〜64文字で構成でき、空白、非ASCII文字、特殊文字を含めることはできません。
   - **既存のActive Directoryアカウントを使用する**を選択した場合は、**参照**を選択して、選択したマシン用の既存のActive Directoryコンピューターアカウントに移動します。

10. **ドメイン資格情報**ページで、**資格情報を入力**を選択し、ユーザー名とパスワードを入力して、**保存**を選択し、**次へ**を選択します。

    - 入力する資格情報には、Active Directoryアカウント操作を実行する権限が必要です。

11. **概要**ページで、情報を確認し、カタログの名前を指定して、**完了**を選択します。

> **注:**
>
> バージョン2402以降、GCPカタログ名は、以下の規則に準拠する必要があります。
>
> - 小文字で始まること。
> - 小文字 (a-z)、数字、ハイフンのみを含めること。
> - 小文字または数字で終わること。 これらの規則に準拠していない既存のGCPカタログの名前を変更しようとすると、エラーメッセージが表示され、更新された規則に従って名前を変更するように案内されます。

マシンカタログの作成には時間がかかる場合があります。マシンがターゲットノードグループに作成されていることを確認するには、Google Cloudコンソールに移動します。

手動で作成されたGoogle Cloudマシンをインポートする

*Google Cloudへの接続を作成*し、次に*Google Cloudマシンを含むカタログを作成*できます。その後、Citrix Virtual Apps and Desktopsを介してGoogle Cloudマシンを手動で電源サイクルできます。この機能を使用すると、次のことができます。

- 手動で作成されたGoogle CloudマルチセッションOSマシンをCitrix Virtual Apps and Desktopsマシンカタログにインポートする。
- 手動で作成されたGoogle CloudマルチセッションOSマシンをCitrix Virtual Apps and Desktopsカタログから削除する。
- 既存のCitrix Virtual Apps and Desktopsの電源管理機能を使用して、Google Cloud WindowsマルチセッションOSマシンの電源を管理する。たとえば、それらのマシンの再起動スケジュールを設定します。

この機能は、既存のCitrix Virtual Apps and Desktopsプロビジョニングワークフローの変更や、既存の機能の削除を必要としません。手動で作成されたGoogle Cloudマシンをインポートする代わりに、Web StudioでMCSを使用してマシンをプロビジョニングすることをお勧めします。

共有仮想プライベートクラウド

共有仮想プライベートクラウド (VPC) は、ホストプロジェクトで構成されます。そこから共有サブネットが利用可能になり、リソースを使用する1つ以上のサービスプロジェクトが含まれます。共有VPCは、共有の企業Googleクラウド リソースの一元的な制御、使用、および管理を提供するため、大規模なインストールに適したオプションです。詳細については、Googleドキュメントサイトを参照してください。

この機能により、Machine Creation Services (MCS) は、共有VPCに展開されたマシンカタログのプロビジョニングと管理をサポートします。このサポートは、現在ローカルVPCで提供されているサポートと機能的に同等ですが、次の2つの点で異なります。

1. ホスト接続の作成に使用されるサービスアカウントに追加の権限を付与する必要があります。このプロセスにより、MCSは共有VPCリソースにアクセスして使用できるようになります。
2. イングレス用とエグレス用にそれぞれ1つずつ、2つのファイアウォールルールを作成する必要があります。これらのファイアウォールルールは、イメージマスタリングプロセス中に使用されます。

必要な新しい権限

ホスト接続を作成する際には、特定の権限を持つGoogle Cloudサービスアカウントが必要です。これらの追加権限は、共有VPCベースのホスト接続の作成に使用されるすべてのサービスアカウントに付与する必要があります。

> **ヒント:**
>
> これらの追加権限は、Citrix Virtual Apps and Desktopsにとって新しいものではありません。これらはローカルVPCの実装を容易にするために使用されます。共有VPCでは、これらの追加権限により、他の共有VPCリソースへのアクセスが可能になります。

> 共有VPCをサポートするために、ホスト接続に関連付けられたサービスアカウントに最大4つの追加権限を付与する必要があります。

1. **compute.firewalls.list** - この権限は必須です。これにより、MCSは共有VPCに存在するファイアウォールルールの一覧を取得できます。
2. **compute.networks.list** - この権限は必須です。これにより、MCSはサービスアカウントが利用できる共有VPCネットワークを識別できます。

3. **compute.subnetworks.list** – この権限は、VPCの使用方法によってオプションです。これにより、MCSは可視の共有VPC内のサブネットを識別できます。この権限はローカルVPCを使用する場合にすでに必要ですが、共有VPCホストプロジェクトでも割り当てる必要があります。
4. **compute.subnetworks.use** - この権限は、VPCの使用方法によってオプションです。プロビジョニングされたマシンカタログでサブネットリソースを使用するために必要です。この権限はローカルVPCを使用する場合にすでに必要ですが、共有VPCホストプロジェクトでも割り当てる必要があります。

これらの権限を使用する際には、マシンカタログの作成に使用される権限の種類に基づいて異なるアプローチがあることを考慮してください。

- プロジェクトレベルの権限:
  - ホストプロジェクト内のすべての共有VPCへのアクセスを許可します。
  - サービスアカウントに権限 #3 と #4 を割り当てる必要があります。
- サブネットレベルの権限:
  - 共有 VPC 内の特定のサブネットへのアクセスを許可します。
  - 権限 #3 と #4 はサブネットレベルの割り当てに固有のものであるため、サービスアカウントに直接割り当てる必要はありません。

組織のニーズとセキュリティ基準に合ったアプローチを選択してください。

> **ヒント:**
>
> プロジェクトレベルとサブネットレベルの権限の違いの詳細については、Google Cloud ドキュメントを参照してください。

ファイアウォールルール

マシンカタログの準備中に、カタログのマスターイメージシステムディスクとして機能するマシンイメージが準備されます。このプロセスが発生すると、ディスクは一時的に仮想マシンに接続されます。このVMは、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを防止する隔離された環境で実行する必要があります。これは、イングレス用とエグレス用の2つのすべて拒否ファイアウォールルールによって実現されます。Google Cloud のローカル VCP を使用する場合、MCS はこのファイアウォールをローカルネットワークに作成し、マスタリング用のマシンに適用します。マスタリングが完了すると、ファイアウォールルールはイメージから削除されます。

共有 VPC を使用するために必要な新しい権限の数を最小限に抑えることをお勧めします。共有 VPC はより上位の企業リソースであり、通常、より厳格なセキュリティプロトコルが導入されています。このため、ホストプロジェクトの共有 VPC リソースに、イングレス用とエグレス用のファイアウォールルールをペアで作成します。それらに最高の優先順位を割り当てます。次の値を使用して、これらの各ルールに新しいターゲットタグを適用します。

`citrix-provisioning-quarantine-firewall`

MCS がマシンカタログを作成または更新するとき、このターゲットタグを含むファイアウォールルールを検索します。次に、ルールの正確性を確認し、カタログのマスターイメージを準備するために使用されるマシンに適用します。ファイアウォールルールが見つからない場合、またはルールが見つかってもルールやその優先順位が正しくない場合、次のようなメッセージが表示されます。

`"Unable to find valid INGRESS and EGRESS quarantine firewall rules for VPC <name> in project <project>. " Please ensure you have created 'deny all' firewall rules with the network tag 'citrix-provisioning-quarantine-firewall' and proper priority." "Refer to Citrix Documentation for details."`

共有 VPC の構成

Web Studio で共有 VPC をホスト接続として追加する前に、プロビジョニングする予定のプロジェクトからサービスアカウントを追加するために、次の手順を完了してください。

1. IAMロールを作成します。
2. CVADホスト接続の作成に使用されるサービスアカウントを、共有VPCホストプロジェクトのIAMロールに追加します。
3. プロビジョニングする予定のプロジェクトのCloud Buildサービスアカウントを、共有VPCホストプロジェクトのIAMロールに追加します。
4. ファイアウォールルールを作成します。

IAMロールを作成する

ロールのアクセスレベルを決定します — *プロジェクトレベルのアクセス*、または*サブネットレベルのアクセス*を使用するより制限されたモデル。

IAMロールのプロジェクトレベルのアクセス。プロジェクトレベルのIAMロールには、次の権限を含めます。

- compute.firewalls.list
- compute.networks.list

- compute.subnetworks.list
- compute.subnetworks.use

プロジェクトレベルのIAMロールを作成するには：

1. Google Cloudコンソールで、**IAMと管理 > ロール**に移動します。
2. **ロール**ページで、**ロールを作成**を選択します。
3. **ロールの作成**ページで、ロール名を指定します。**権限を追加**を選択します。
    a. 「**権限を追加**」ページで、ロールに個別に権限を追加します。権限を追加するには、「**テーブルをフィルタリング**」フィールドに権限の名前を入力します。権限を選択し、「**追加**」を選択します。
    b. 「**作成**」を選択します。

サブネットレベルのIAMロール。このロールは、「**ロールを作成**」を選択した後に、権限`compute.subnetworks.list`と`compute.subnetworks.use`の追加を省略します。このIAMアクセスレベルの場合、権限`compute.firewalls.list`と`compute.networks.list`を新しいロールに適用する必要があります。

サブネットレベルのIAMロールを作成するには：

1. Google Cloudコンソールで、「**VPCネットワーク**」>「**共有VPC**」に移動します。「**共有VPC**」ページが表示され、ホストプロジェクトに含まれる共有VPCネットワークのサブネットが表示されます。
2. 「**共有VPC**」ページで、アクセスするサブネットを選択します。
3. 右上隅で、「**メンバーを追加**」を選択してサービスアカウントを追加します。
4. 「**メンバーを追加**」ページで、次の手順を完了します。
    a. 「**新しいメンバー**」フィールドにサービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。
    b. 「**ロールを選択**」フィールドを選択し、「**Compute Network User**」を選択します。
    c. 「**保存**」を選択します。
5. Google Cloudコンソールで、「**IAMと管理**」>「**ロール**」に移動します。
6. 「**ロール**」ページで、「**ロールを作成**」を選択します。
7. 「**ロールを作成**」ページで、ロール名を指定します。「**権限を追加**」を選択します。

a. 「**権限を追加**」ページで、ロールに個別に権限を追加します。権限を追加するには、「**テーブルをフィルタリング**」フィールドに権限の名前を入力します。権限を選択し、「**追加**」を選択します。

b. 「**作成**」を選択します。

ホストプロジェクトのIAMロールにサービスアカウントを追加する

IAMロールを作成したら、ホストプロジェクトにサービスアカウントを追加するために、以下の手順を実行します。

1. Google Cloudコンソールで、ホストプロジェクトに移動し、「**IAMと管理 > IAM**」に移動します。
2. 「**IAM**」ページで、「**追加**」を選択してサービスアカウントを追加します。
3. 「**メンバーを追加**」ページで：

   a. 「**新しいメンバー**」フィールドにサービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。

   b. ロールフィールドを選択し、作成したIAMロールを入力し、メニューからそのロールを選択します。

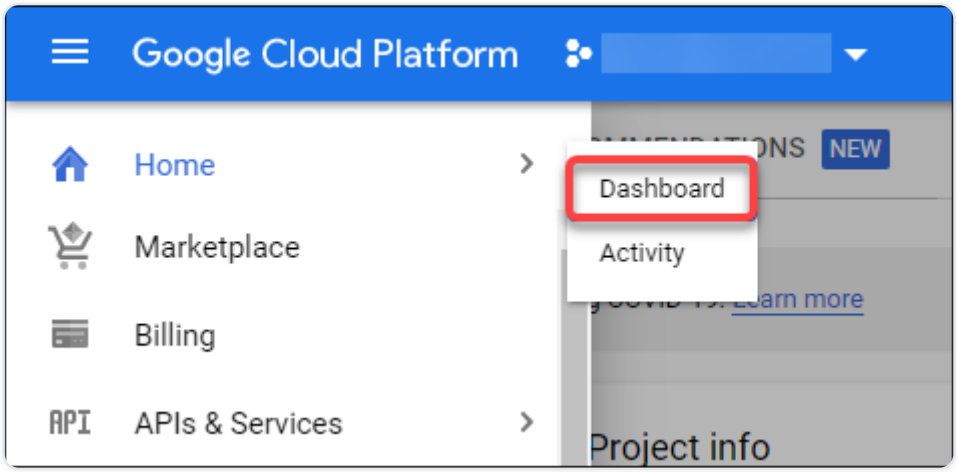
   c. 「**保存**」を選択します。

サービスアカウントがホストプロジェクト用に構成されました。

クラウドビルドサービスアカウントを共有VPCに追加する

すべてのGoogle Cloudサブスクリプションには、プロジェクトID番号の後に `cloudbuild.gserviceaccount` が続く名前のサービスアカウントがあります。例：`705794712345@cloudbuild.gserviceaccount`。

Google Cloud コンソールで **Home** と **Dashboard** を選択すると、プロジェクトのプロジェクト ID 番号を確認できます。



画面の **Project Info** エリアの下にある **Project Number** を見つけます。

共有 VPC に Cloud Build サービスアカウントを追加するには、次の手順を実行します。

1. Google Cloud コンソールで、ホストプロジェクトに移動し、**IAM と管理** > **IAM** に移動します。
2. **権限**ページで、アカウントを追加するために**追加**を選択します。
3. **メンバーの追加**ページで、次の手順を完了します。
    a. **新しいメンバー**フィールドに Cloud Build サービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。
    b. **ロールの選択**フィールドを選択し、`Computer Network User` と入力して、メニューからロールを選択します。
    c. **保存**を選択します。

ファイアウォールルールを作成する

マスタリングプロセスの一環として、MCS は選択したマシンイメージをコピーし、それを使用してカタログ用のマスターイメージシステムディスクを準備します。マスタリング中に、MCS はディスクを一時的な仮想マシンに接続し、その仮想マシンが準備スクリプトを実行します。この VM は、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを禁止する分離された環境で実行する必要があります。分離された環境を作成するために、MCS は2つの *すべて拒否* ファイアウォールルール（イングレスルールとエグレスルール）を必要とします。したがって、*ホストプロジェクト* に次の2つのファイアウォールルールを作成します。

1. Google Cloud コンソールで、ホストプロジェクトに移動し、**VPC ネットワーク > ファイアウォール**に移動します。
2. **ファイアウォール**ページで、**ファイアウォールルールを作成**を選択します。
3. **ファイアウォールルールの作成**ページで、以下を完了します。
    - **名前**。ルールの名前を入力します。
    - **ネットワーク**。イングレスファイアウォールルールが適用される共有 VPC ネットワークを選択します。
    - **優先度**。値が小さいほど、ルールの優先度が高くなります。小さい値（例: 10）をお勧めします。
    - **トラフィックの方向**。**イングレス** を選択します。
    - **一致時のアクション**。**拒否** を選択します。
    - **ターゲット**。デフォルトの **指定されたターゲットタグ** を使用します。

- **ターゲットタグ**。`citrix-provisioning-quarantine-firewall` と入力します。
- **ソースフィルター**。デフォルトの **IP 範囲** を使用します。
- **ソース IP 範囲**。すべてのトラフィックに一致する範囲を入力します。`0.0.0.0/0` と入力します。
- **プロトコルとポート**。「**すべて拒否**」を選択します。

4. 「**作成**」を選択してルールを作成します。
5. 手順1～4を繰り返して別のルールを作成します。**トラフィックの方向**には「**エグレス**」を選択します。

接続の追加

Google Cloud環境への接続を追加します。「接続を追加する」を参照してください。

ゾーン選択を有効にする

Citrix Virtual Apps and Desktops はゾーン選択をサポートしています。ゾーン選択を使用すると、VM を作成するゾーンを指定できます。ゾーン選択を使用すると、管理者は選択したゾーンに単一テナントノードを配置できます。単一テナンシーを構成するには、Google Cloud で以下を完了する必要があります。

- Google Cloud の単一テナントノードを予約する
- VDA マスターイメージを作成する

Google Cloud の単一テナントノードの予約

単一テナントノードを予約するには、Google Cloud のドキュメントを参照してください。

> **重要:**
>
> ノードテンプレートは、ノードグループに予約されているシステムのパフォーマンス特性を示すために使用されます。これらの特性には、vGPU の数、ノードに割り当てられるメモリ量、およびノード上に作成されるマシンに使用されるマシンタイプが含まれます。詳細については、Google Cloud のドキュメントを参照してください。

VDA マスターイメージの作成

単一テナントノードにマシンを正常に展開するには、マスター VM イメージを作成する際に追加の手順を実行する必要があります。Google Cloud のマシンインスタンスには、*ノードアフィニティラベル*と呼ばれるプロパティがあります。単一テナントノードに展開されるカタログのマス

ターイメージとして使用されるインスタンスには、**ターゲットノードグループ**の名前と一致する*ノードアフィニティラベル*が必要です。これを実現するには、次の点に留意してください。

- 新しいインスタンスの場合は、インスタンスの作成時に Google Cloud コンソールでラベルを設定します。詳細については、「インスタンスの作成時にノードアフィニティラベルを設定する」を参照してください。
- 既存のインスタンスの場合は、**gcloud** コマンドラインを使用してラベルを設定します。詳細については、「既存のインスタンスにノードアフィニティラベルを設定する」を参照してください。

> **注:**
>
> 共有 VPC で単一テナンシーを使用する場合は、「共有仮想プライベートクラウド」を参照してください。

インスタンスの作成時にノードアフィニティラベルを設定する

ノードアフィニティラベルを設定するには：

1. Google Cloud コンソールで、**Compute Engine > VM インスタンス**に移動します。
2. **VM インスタンス**ページで、**インスタンスを作成**を選択します。
3. **インスタンスの作成**ページで、必要な情報を入力または構成し、**管理、セキュリティ、ディスク、ネットワーク、単一テナンシー**を選択して設定パネルを開きます。
4. **Sole tenancy**タブで、**参照**を選択して現在のプロジェクトで利用可能なノードグループを表示します。**Sole-tenant node**ページが表示され、利用可能なノードグループのリストが表示されます。
5. **Sole-tenant node**ページで、リストから該当するノードグループを選択し、**選択**を選択して**Sole tenancy**タブに戻ります。ノードアフィニティラベルフィールドに、選択した情報が入力されます。この設定により、インスタンスから作成されたマシンカタログが、選択したノードグループに展開されることが保証されます。
6. インスタンスを作成するには、**作成**を選択します。

既存のインスタンスにノードアフィニティラベルを設定する

ノードアフィニティラベルを設定するには：

1. Google Cloud Shellターミナルウィンドウで、*gcloud compute instances*コマンドを使用してノードアフィニティラベルを設定します。**gcloud**コマンドに以下の情報を含めます。

- **VMの名前**。たとえば、`s*2019-vda-base`.*という既存のVMを使用します。
- **ノードグループの名前**。以前に作成したノードグループ名を使用します。たとえば、`mh-sole-tenant-node-group-1`。
- **インスタンスが存在するゾーン**。たとえば、VMは`*us-east-1b* zone`にあります。

たとえば、ターミナルウィンドウで次のコマンドを入力します:

- `gcloud compute instances set-scheduling "s2019-vda-base" --node-group="mh-sole-tenant-node-group-1" --zone="us-east1-b"`

*gcloud compute instances*コマンドの詳細については、`<https://cloud.google.com/sdk/gcloud/reference/beta/compute/instances/set-scheduling>`にあるGoogle Developer Toolsのドキュメントを参照してください。

2. インスタンスの**VMインスタンスの詳細**ページに移動し、**ノードアフィニティ**フィールドにラベルが入力されていることを確認します。

マシンカタログを作成する

ノードアフィニティラベルを設定したら、マシンカタログを構成します。

顧客管理の暗号化キー (CMEK)

MCSカタログには、顧客管理の暗号化キー (CMEK) を使用できます。この機能を使用する場合、Google Cloud Key Management Service `CryptoKey Encrypter/Decrypter` ロールをCompute Engineサービスエージェントに割り当てます。Citrix Virtual Apps and Desktopsアカウントは、キーが保存されているプロジェクトで適切な権限を持っている必要があります。詳細については、「Cloud KMSキーを使用してリソースを保護する」を参照してください。

Compute Engineサービスエージェントは、`service-<Project _Number>@compute-system.iam.gserviceaccount.com` の形式です。この形式は、デフォルトのCompute Engineサービスアカウントとは異なります。

> **注:**
>
> このCompute Engineサービスアカウントは、Google Consoleの **IAM Permissions** 表示に表示されない場合があります。そのような場合は、「Cloud KMSキーを使用してリソースを保護する」で説明されているように、`gcloud` コマンドを使用してください。

Citrix Virtual Apps and Desktops アカウントに権限を割り当てる

Google Cloud KMSの権限は、さまざまな方法で構成できます。*プロジェクトレベル*のKMS権限、または*リソースレベル*のKMS権限のいずれかを付与できます。詳細については、「権限とロール」を参照してください。

プロジェクトレベルの権限

1つのオプションは、Citrix Virtual Apps and Desktopsアカウントに、Cloud KMSリソースを参照するためのプロジェクトレベルの権限を付与することです。これを行うには、カスタムロールを作成し、次の権限を追加します。

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

このカスタムロールを Citrix Virtual Apps and Desktops に割り当てます。これにより、インベントリ内の関連プロジェクトでリージョンキーを参照できます。

リソースレベルの権限

もう1つのオプションであるリソースレベルの権限の場合、Google Cloud コンソールで、MCS プロビジョニングに使用する `cryptoKey` を参照します。Citrix Virtual Apps and Desktops アカウントを、カタログプロビジョニングに使用するキーリングまたはキーに追加します。

> **ヒント:**
>
> このオプションでは、Citrix Virtual Apps and DesktopsアカウントにCloud KMSリソースに対するプロジェクトレベルのリスト権限がないため、インベントリでプロジェクトのリージョンキーを参照することはできません。ただし、以下に説明するように、`ProvScheme`カスタムプロパティで正しい`cryptoKeyId`を指定することで、CMEKを使用してカタログをプロビジョニングすることは可能です。

カスタムプロパティを使用したCMEKによるプロビジョニング

PowerShellでプロビジョニングスキームを作成する際に、`ProvScheme CustomProperties`で`CryptoKeyId`プロパティを指定します。例：

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId"
Value="<yourCryptoKeyId>" />

</CustomProperties>'
```

`cryptoKeyId`は次の形式で指定する必要があります。

`projectId:location:keyRingName:cryptoKeyName`

たとえば、リージョン`us-east1`のキーリング`my-example-key-ring`にあるキー`my-example-key`と、IDが`my-example-project-1`のプロジェクトを使用したい場合、`ProvScheme`カスタム設定は次のようになります。

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
example-project-1:us-east1:my-example-key-ring:my-example-key" />

</CustomProperties>'
```

このプロビジョニングスキームに関連するすべてのMCSプロビジョニング済みディスクとイメージは、この顧客管理暗号化キーを使用します。

ヒント:

グローバルキーを使用する場合、顧客プロパティの場所は、上記の例の**us-east1**のような**リージョン**名ではなく、`global`と記述する必要があります。例：`<Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-example-project-1:global:my-example-key-ring:my-example-key" />`。

顧客管理キーのローテーション

Google Cloudは、既存の永続ディスクまたはイメージでのキーのローテーションをサポートしていません。マシンがプロビジョニングされると、作成時に使用されていたキーバージョンに紐付けられます。ただし、新しいバージョンのキーを作成することができ、その新しいキーは、新しく

プロビジョニングされたマシンや、新しいマスターイメージでカタログが更新されたときに作成されるリソースに使用されます。

キーリングに関する重要な考慮事項

キーリングの名前変更や削除はできません。また、キーリングを構成する際に予期せぬ料金が発生する可能性があります。キーリングを削除または削除すると、Google Cloudはエラーメッセージを表示します。

```
Sorry, you can't delete or rename keys or key rings. We were concerned
about the security implications of allowing multiple keys or key versions
over time to have the same resource name, so we decided to make names
immutable. (And you can't delete them, because we wouldn't be able to do a
true deletion--there would still have to be a tombstone tracking that this
name had been used and couldn't be reused).

We're aware that this can make things untidy, but we have no immediate
plans to change this.

If you want to avoid getting billed for a key or otherwise make it
unavailable, you can do so by deleting all the key versions; neither keys
nor key rings are billed for, just the active key versions within the
keys.
```

ヒント:

詳細については、「コンソールからキーリングを編集または削除する」を参照してください。

均一なバケットレベルのアクセスの互換性

Citrix Virtual Apps and Desktopsは、Google Cloudの均一なバケットレベルのアクセス制御ポリシーと互換性があります。この機能は、サービスアカウントに権限を付与してストレージバケットを含むリソースの操作を可能にするIAMポリシーの使用を強化します。均一なバケットレベルのアクセス制御により、Citrix Virtual Apps and Desktopsでは、アクセス制御リスト（ACL）を使用して、ストレージバケットまたはそこに保存されているオブジェクトへのアクセスを制御できます。Google Cloudの均一なバケットレベルのアクセスの概要については、均一なバケットレベルのアクセスを参照してください。構成情報については、均一なバケットレベルのアクセスを要求するを参照してください。

PowerShellを使用してマシンカタログを作成する

このセクションでは、PowerShellを使用してカタログを作成する方法について詳しく説明します。

- 永続的なライトバックキャッシュディスクを持つカタログを作成する
- MCSIOで起動パフォーマンスを向上させる
- マシンプロファイルを使用してマシンカタログを作成する
- インスタンステンプレートとしてマシンプロファイルを持つマシンカタログを作成する
- PowerShellを使用してシールドされたVMを持つカタログを作成する
- 単一テナントノードにWindows 11 VMを作成する

永続的なライトバックキャッシュディスクを持つカタログを作成する

永続的なライトバックキャッシュディスクを持つカタログを構成するには、PowerShellパラメーター`New-ProvScheme``CustomProperties`を使用します。

> **ヒント:**
>
> ここで PowerShell パラメーターを使用するのは、クラウドベースのホスティング接続の場合のみです。オンプレミスソリューション（XenServer® など）で永続的なライトバックキャッシュディスクを使用してマシンをプロビジョニングする場合、ディスクは自動的に永続化されるため、PowerShell は必要ありません。

> このパラメーターは、MCSプロビジョニングされたマシンに対してライトバックキャッシュディスクがどのように永続化されるかを決定するために使用される追加のプロパティ`PersistWBC`をサポートします。`PersistWBC`プロパティは、`UseWriteBackCache`パラメーターが指定され、かつ`WriteBackCacheDiskSize`パラメーターがディスクが作成されることを示すように設定されている場合にのみ使用されます。

> **注:**
>
> この動作は、AzureとGCPの両方に適用され、電源サイクル時にデフォルトのMCSIOライトバックキャッシュディスクが削除され、再作成されます。ディスクの削除と再作成を避けるために、ディスクを永続化することを選択できます。

`PersistWBC` プロパティを `true` に設定すると、Citrix Virtual Apps and Desktops 管理者が管理インターフェイスからマシンをシャットダウンしても、ライトバックキャッシュディスクは削除されません。

`PersistWBC` プロパティを `false` に設定すると、Citrix Virtual Apps and Desktops 管理者が管理インターフェイスからマシンをシャットダウンしたときに、ライトバックキャッシュディスクが削除されます。

注:

`PersistWBC` プロパティが省略された場合、プロパティはデフォルトで `false` になり、管理インターフェイスからマシンがシャットダウンされるとライトバックキャッシュは削除されます。

例として、CustomPropertiesパラメーターを使用して `PersistWBC` を `true` に設定する場合：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

注:

`PersistWBC` プロパティは、`New-ProvScheme` PowerShellコマンドレットを使用してのみ設定できます。作成後にプロビジョニングスキームの `CustomProperties` を変更しようと

しても、マシンカタログや、マシンがシャットダウンされたときのライトバックキャッシュディスクの永続性には影響しません。

たとえば、`New-ProvScheme` を設定してライトバックキャッシュを使用し、同時に `PersistWBC` プロパティを `true` に設定します。

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127
```

```
-WriteBackCacheMemorySize 256
```

MCSIOで起動パフォーマンスを向上させる

MCSIOが有効な場合、AzureおよびGCPマネージドディスクの起動パフォーマンスを向上させることができます。この機能を構成するには、`New-ProvScheme`コマンドでPowerShell `PersistOSDisk`カスタムプロパティを使用します。`New-ProvScheme`に関連するオプションは次のとおりです。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->

````````Groups" Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```

この機能を有効にするには、`PersistOSDisk`カスタムプロパティを`true`に設定します。例：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"
```
```

```
-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

マシンプロファイルを使用してマシンカタログを作成する

Machine Creation Services (MCS) を使用してマシンをプロビジョニングするためのカタログを作成する場合、仮想マシンからハードウェアプロパティをキャプチャし、カタログ内の新しくプロビジョニングされたVMに適用するために、マシンプロファイルを使用できます。`MachineProfile`パラメーターが使用されていない場合、ハードウェアプロパティはマスターイメージVMまたはスナップショットからキャプチャされます。 明示的に定義する一部のプロパティ（例: `StorageType`、`CatalogZones`、`CryptoKeyIs`）は、マシンプロファイルから無視されます。

- マシンプロファイルを使用してカタログを作成するには、`New-ProvScheme`コマンドを使用します。例: `New-ProvScheme –MachineProfile "path to VM"`。`MachineProfile`パラメーターを指定しない場合、ハードウェアプロパティはマスターイメージVMからキャプチャされます。
- 新しいマシンプロファイルでカタログを更新するには、`Set-ProvScheme`コマンドを使用します。例: `Set-ProvScheme –MachineProfile "path to new VM"`。このコマンドは、カタログ内の既存のVMのマシンプロファイルを変更しません。カタログに追加された新しく作成されたVMのみが新しいマシンプロファイルを持ちます。

- マスターイメージを更新することもできますが、マスターイメージを更新してもハードウェアプロパティは更新されません。ハードウェアプロパティを更新する場合は、`Set-ProvScheme` コマンドを使用してマシンプロファイルを更新する必要があります。これらの変更は、カタログ内の新しいマシンにのみ適用されます。既存のマシンのハードウェアプロパティを更新するには、`Set-ProvVMUpdateTimeWindow` コマンドを `-StartsNow` および `-DurationInMinutes -1` パラメーターとともに使用できます。

  > **注:**
  >
  > - `StartsNow` は、スケジュールされた開始時刻が現在の時刻であることを示します。
  > - 負の数（例: –1）を指定した `DurationInMinutes` は、スケジュールの時間枠に上限がないことを示します。

マシンプロファイルをインスタンステンプレートとして使用してマシンカタログを作成する

マシンプロファイルの入力としてGCPインスタンステンプレートを選択できます。インスタンステンプレートはGCPの軽量リソースであるため、非常に費用対効果が高いです。

マシンプロファイルをインスタンステンプレートとして使用して新しいマシンカタログを作成する

1. PowerShellウィンドウを開きます。
2. `asnp citrix*` を実行して、Citrix固有のPowerShellモジュールをロードします。
3. 次のコマンドを使用して、GCPプロジェクトでインスタンステンプレートを見つけます。

```
cd XDHyp:\HostingUnits\<HostingUnitName>\instanceTemplates.folder
```

4. NewProvSchemeコマンドを使用して、マシンプロファイルをインスタンステンプレートとして新しいマシンカタログを作成します。

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -HostingUnitName
<HostingUnitName> -IdentityPoolName <identity pool name> -MasterImageVM

XDHyp:\HostingUnits\<HostingUnitName> \Base.vm\Base.snapshot
-MachineProfile XDHyp:
```

```
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\mytemplate.tem
plate
```

New-ProvSchemeコマンドの詳細については、https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/を参照してください。

5. PowerShell コマンドを使用してマシンカタログの作成を完了します。Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/ を参照してください。

既存のマシンカタログのマシンプロファイルをインスタンステンプレートに変更する

既存のマシンカタログのマシンプロファイルをインスタンステンプレートに変更する詳細な手順は次のとおりです。

1. PowerShell ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. 次のコマンドを実行します。

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -MachineProfile
XDHyp:
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\<TemplateName>
.template
```

Set-ProvSchemeコマンドの詳細については、https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/を参照してください。

PowerShell を使用して、シールドされたVMでカタログを作成する

シールドされたVMプロパティを持つMCSマシンカタログを作成できます。シールドされた仮想マシンは、セキュアブート、仮想トラステッドプラットフォームモジュール、UEFIファームウェア、整合性監視などの高度なプラットフォームセキュリティ機能を使用して、Compute Engineインスタンスの検証可能な整合性を提供する一連のセキュリティ制御によって強化されています。

MCSは、マシンプロファイルワークフローを使用してカタログを作成することをサポートしています。マシンプロファイルワークフローを使用する場合、VMインスタンスのシールドされたVMプロパティを有効にする必要があります。その後、このVMインスタンスをマシンプロファイルの入力として使用できます。

マシンプロファイルワークフローを使用して、シールドされたVMでMCSマシンカタログを作成するには。

1. Google Cloud コンソールでVMインスタンスのシールドされたVMオプションを有効にします。クイックスタート: シールドされたVMオプションを有効にするを参照してください。
2. VMインスタンスを使用して、マシンプロファイルワークフローでMCSマシンカタログを作成します。

   a. PowerShell ウィンドウを開きます。

   b. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。

   c. まだ作成されていない場合は、IDプールを作成します。

   d. `New-ProvScheme`コマンドを実行します。例：

   ```
   New-ProvScheme -ProvisioningSchemeName <catalog-name>

   -HostingUnitName gcp-hostint-unit

   -MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-vda.vm

   -MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
   machine.vm
   ```

3. マシンカタログの作成を完了します。

新しいマシンプロファイルでマシンカタログを更新するには:

1. `Set-ProvScheme`コマンドを実行します。例：

   ```
   Set-ProvScheme -ProvisioningSchemeName <catalog-name>

   -MasterImageVM XDHyp:\HostingUnits\<hostin-unit>\catalog-vda.vm

   -MachineProfile "DHyp:\HostingUnits\<hostin-unit>\catalog-machine.vm
   ```

`Set-ProvScheme` で行った変更を既存のVMに適用するには、`Set-ProvVMUpdateTimeWindow` コマンドを実行します。

1. `Set-ProvVMUpdateTimeWindow` コマンドを実行します。例:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
   <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
   ```

2. VMを再起動します。

シングルテナントノード上にWindows 11 VMを作成する

GCPでWindows 11 VMを作成できます。ただし、マスターイメージにWindows 11をインストールする場合は、マスターイメージ作成プロセス中にvTPMを有効にする必要があります。また、マシンプロファイルソース（VMまたはインスタンステンプレート）でvTPMを有効にする必要があります。

シングルテナントノード上にWindows 11 VMを作成するための主要な手順は次のとおりです。

1. Google Cloud仮想化環境をセットアップします。詳細については、Google Cloud environmentsを参照してください。
2. VDAをインストールします。Install VDAsを参照してください。
3. Google Cloud環境への接続を作成します。詳細については、Connection to Google cloud environmentsを参照してください。
4. Windows 11 Bring Your Own License (BYOL) マスターイメージを作成し、そのイメージをGoogle Cloudにインポートします。詳細については、Windows 11 BYOL マスターイメージの作成を参照してください。
5. マシンプロファイルソースを作成します。単一テナントノードにVMをプロビジョニングし、ソースマシンプロファイルのvTPMを有効にします。詳細については、単一テナントノードでのVMのプロビジョニングを参照してください。
6. vTPMが有効なWindows 11マシンプロファイルソースを使用してMCSマシンカタログを作成します。マシンプロファイルソースは、単一テナントノードで説明されているインスタンスタイプと同じである必要があります。詳細については、Windows 11マシンプロファイルソースを使用したMCSマシンカタログの作成を参照してください。

Windows 11 BYOLマスターイメージを作成する

Windows 11 BYOLマスターイメージを作成し、そのマスターイメージをGoogle Cloudにインポートするには、次の2つのオプションがあります。

- Google Cloud Cloud Build Tools を使用する
- 他のハイパーバイザーでマスターイメージを作成する

GOOGLE CLOUD CLOUD BUILD TOOLS を使用する

1. Windows 11 ISO、GCP SDK、.NET Framework、およびPowerShellインストーラーファイルをGCPストレージバケットにアップロードします。
2. クラウドビルド`.yaml`ファイルで、ファイルの場所をパラメーターとして指定します。

3. コマンドラインから次のCloud Buildを実行して、最終的なWindows 11イメージをビルドします。GCPは、GCPのDaisyワークフローを使用して、選択したプロジェクトでマスターイメージをブートストラップして作成し、そのマスターイメージはGCPにインポートされます。

```
gcloud compute instances import INSTANCE-NAME--source-uri=gs://BUCKET/
IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
machine-type=MACHINE-TYPE --zone=ZONE
```

> **注:**
>
> すべての大文字のテキストを実際の詳細リソースに置き換えます。

詳細については、カスタムWindows BYOLイメージの作成を参照してください。

他のハイパーバイザーでマスターイメージを作成する

1. 他のハイパーバイザーを使用して Windows 11 マスターイメージを作成します。
2. マスターイメージを OVF 形式でローカルマシンにエクスポートします。
3. ローカルの gcloud CLI を使用して、OVF ファイルを GCP ストレージバケットにアップロードします。

```
gsutil cp LOCAL_IMAGE_PATH_OVF_FILES gs://BUCKET_NAME/
```

4. コマンドラインから以下のCloud Buildを実行して、最終的なWindows 11イメージをビルドします。GCPは、GCPのDaisyワークフローを使用して、選択したプロジェクトでマスターイメージをブートストラップして作成し、マスターイメージはGCPにインポートされます。

```
gcloud compute instances import INSTANCE-NAME --source-uri=gs://BUCKET/
IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
machine-type=MACHINE-TYPE --zone=ZONE
```

> **注:**
>
> すべての大文字のテキストを実際のリソースの詳細に置き換えてください。

シングルテナントノードでのVMのプロビジョニング

シングルテナントノードを使用すると、VMを他のプロジェクトのVMから物理的に分離したり、同じホストハードウェア上にVMをグループ化したりできます。シングルテナントノードの詳細については、GCPドキュメント「シングルテナンシーの概要」を参照してください。

シングルテナントノードでのVM（マシンプロファイルソース）のプロビジョニングについては、GCPドキュメント「シングルテナントノードでのVMのプロビジョニング」を参照してください。

注:

- ノードグループと同じインスタンスタイプとリージョンを選択します。
- シールドされたVMセクションでvTPMを有効にします。詳細については、「クイックスタート：シールドされたVMオプションを有効にする」を参照してください。
- ソースVMでBitlockerを無効にします。

Windows 11のマシンプロファイルソースを使用してMCSマシンカタログを作成する

Web StudioまたはPowerShellコマンドを使用して、Windows 11 VMを作成するためのMCSマシンカタログを作成できます。

注:

- マスターイメージには、Windows 11のスナップショットまたはVMを選択します。
- マシンプロファイルソースには、Windows 11 VMをマシンプロファイルとして選択します。マシンプロファイルソースは、単一テナントノードで説明されているものと同じインスタンスタイプである必要があります。

Web Studioの使用方法については、Web Studioを使用してマシンカタログを作成するを参照してください。

PowerShellコマンドの詳細については、マシンプロファイルを使用してマシンカタログを作成するを参照してください。

カタログを作成してVMの電源をオンにすると、Google Cloudコンソールで、単一テナントノードで実行されているWindows 11 VMを確認できます。

継承されたラベルを持つ VM とディスク

MCSマシンカタログのVMとディスク（IDディスク、ライトキャッシュバックディスク、OSディスク）は、マシンプロファイルソース（GCP VMインスタンスまたはインスタンステンプレート）のラベルを継承できます。ラベルを使用して、異なるチームが所有するインスタンス（例：team:research、team:analytics）を区別し、さらにコスト計算や予算編成に利用できます。ラベルの詳細については、GCPドキュメントラベルを使用してリソースを整理するを参照してください。

マシンプロファイルソースを使用して、新しいカタログを作成したり、既存のカタログを更新したり、既存のVMを更新してラベルを継承させたりできます。

この機能は、永続的および非永続的なMCSマシンカタログに適用されます。

次のことができます。

- 継承されたラベルを持つカタログを作成する
- 継承されたラベルを持つ既存のカタログを更新する
- 継承されたラベルを持つ既存のVMを更新する
- VMおよびブートディスクのラベル情報を取得する
- VMを削除する(#remove-a-vm)

継承されたラベルを持つカタログを作成する

VMとディスクがマシンプロファイルソースからラベルを継承するMCSマシンカタログを作成するには、次の手順を実行します。

1. ラベル付きのマシンプロファイルソース（VMインスタンスまたはインスタンステンプレート）を作成します。ラベル付きVMの作成については、GCPドキュメント「ラベル付きリソースの作成」を参照してください。インスタンステンプレートはVMから作成され、VMで定義されたラベルを引き継ぎます。
2. Web StudioまたはPowerShellコマンドを使用してMCSカタログを作成します。
3. Web Studioを使用する場合は、**Image**ページで**Use a machine profile**を選択し、VMまたはテンプレートを選択します。
4. PowerShellコマンドを使用する場合は、次の手順を実行します。
    a. PowerShellウィンドウを開きます。
    b. asnp citrix*を実行します。
    c. IDプールを作成します。IDプールは、作成されるVMのActive Directory（AD）アカウントのコンテナです。

d. Active Directoryで必要なADコンピューターアカウントを作成します。

e. カタログを作成するには、`New-ProvScheme`コマンドを実行します。例：

New-ProvScheme（マシンプロファイル入力としてのテンプレート）（永続カタログ）：

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `
```

New-ProvScheme（マシンプロファイル入力としてのインスタンステンプレート）（非永続カタログ）：

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `

-CleanOnBoot
```

New-ProvScheme（マシンプロファイル入力としてのVMインスタンス）（永続カタログ）：

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

マシンプロファイル入力としてVMインスタンスを使用するNew-ProvScheme (非永続カタログ):

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-CleanOnBoot
```

f. プロビジョニングスキームをブローカーカタログとして登録します。

g. カタログにVMを追加します。

継承されたラベルで既存のカタログを更新する

既存のカタログを新しいマシンプロファイルを持つように更新するには、Set-ProvSchemeコマンドを実行します。このコマンドを実行すると、カタログに追加されたすべての新しいVMは、新しいマシンプロファイルソースのラベルを持つようになります。非永続カタログは次回の電源投入時に更新されます。

例:

インスタンステンプレートをマシンプロファイル入力として使用するSet-ProvScheme:

```
Set-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `
```

VMインスタンスをマシンプロファイル入力として使用するSet-ProvScheme:

```
Set-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

継承されたラベルで既存のVMを更新する

更新されたマシンプロファイルソースで既存のVMを更新するには、次のコマンドを実行します。

1. `Set-ProvScheme`
2. `Set-ProvVMUpdateTimeWindow`。例：

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
   <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
   ```

3. VMを再起動します。

VMおよびブートディスクラベルの情報を取得する

VMを作成した後、`AdditionalData`パラメーターを指定した`Get-Item`コマンドを使用して、VMおよびブートディスクのラベルの情報を取得できます。

VMラベルの情報を取得するには、次のコマンドを実行します。

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-
name\vm_name.vm).AdditionalData.Tags
```

ブートディスクラベルの情報を取得するには、次のコマンドを実行します。

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-name\vm_name.vm\bootdisk-
name.attacheddisk).AdditionalData.Tags
```

注:

さまざまなハイパーバイザー間で一貫性を保つため、GCPラベルを表示するために「タグ」という用語を使用しています。

VMを削除する

カタログからVMを削除することはできますが、GCPからVMを削除しないように選択できます。この場合、Citrixラベルのみがから削除されます。その他の追加されたラベルはVMから削除されません。Web Studioを使用するか、PowerShellコマンドを使用してVMを削除できます。

WEB STUDIOの使用

1. VMを選択して右クリックします。
2. **削除**をクリックします。
3. **カタログから仮想マシンを削除しますが、仮想マシンは削除しません**を選択します。

POWERSHELLコマンドの使用

`ForgetVM`パラメーターを指定して`Remove-ProvVM`を実行します。詳細については、SDKドキュメントのRemove-ProvVMを参照してください。

Google Cloud マーケットプレイス

Google Cloud MarketplaceでCitrixが提供するイメージを参照して選択し、マシンカタログを作成できます。現在、MCSはこの機能に対してマシンプロファイルワークフローのみをサポートしています。

Google Cloud MarketplaceでCitrix VDA VM製品を検索するには、https://console.cloud.google.com/marketplaceにアクセスしてください。

カスタムイメージまたは**Google Cloud Marketplace**のCitrix ready®イメージを使用して、マシンカタログのイメージを更新できます。

注：

> マシンプロファイルにストレージタイプの情報が含まれていない場合、その値はカスタムプロパティから派生します。

> サポートされているGoogle Cloud Marketplaceイメージは次のとおりです。

- Windows 2019シングルセッション
- Windows 2019マルチセッション
- ウブントゥ

Citrix readyイメージをマシンカタログ作成のソースとして使用する例：

```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \

-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \

-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
win2019-single-vda-v20220819.publicimage \

-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
```

次のステップ

- これが最初に作成するカタログである場合、Web Studioはデリバリーグループの作成に誘導します。
- 構成プロセス全体を確認するには、「インストールと構成」を参照してください。
- カタログを管理するには、「マシンカタログの管理」および「Google Cloud Platformカタログの管理」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- Google Cloud環境への接続
- マシンカタログを作成](/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create.html)

HPE Moonshot マシンカタログを作成する

「マシンカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create.html)では、マシンカタログを作成するウィザードについて説明します。以下の情報は、HPE Moonshot環境に固有の詳細を扱っています。

注：

- HPE Moonshotへの接続を作成する
- 1つ以上のHPE Moonshotノードが利用可能であることを確認し、それらのノードにVDAをインストールしてください。
- 最初のHPE Moonshotカートリッジイメージの作成については、OS Deployment on Moonshot ユーザーガイドを参照してください。

HPE Moonshotマシンカタログは、以下を使用して作成できます。

- ウェブ スタジオ
- PowerShellコマンド

Web Studioを使用してマシンカタログを作成する

マシンカタログセットアップウィザードで：

1. **オペレーティングシステム**ページで、**マルチセッションOS**または**シングルセッションOS**を選択します。
2. **マシン管理**ページで、**電源管理されているマシン**と**別のサービスまたはテクノロジー**を選択します。
3. **仮想マシン**ページで、マシンとそのActive Directoryマシンアカウントを追加します。次のいずれかを実行できます。
   - **マシンの追加**をクリックして、マシンを手動で追加します。**VMの選択**ウィンドウが表示されます。以前に作成したHPE Moonshotシャーシ接続を展開し、追加するノード（VM）を選択します。次に、関連するマシンアカウント名を追加します。
   - マシンを一括追加するには、「**CSVファイルの追加**」をクリックします。CSVファイルを使用してマシンを追加する方法については、「CSVファイルを使用してマシンをカタログに一括追加する」を参照してください。

スコープページと**概要**ページには、HPE Moonshot固有の情報は含まれていません。

PowerShellコマンドを使用してマシンカタログを作成する

`New-BrokerCatalog`および`New-BrokerMachine` PowerShellコマンドを実行して、ブローカーカタログを作成し、マシンをブローカーカタログにインポートします。

例:

```
New-BrokerCatalog  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -AllocationType "Random" -IsRemotePC $False
-MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "BurMC"
-PersistUserChanges "OnLocal" -ProvisioningType "Manual" -Scope @()
-SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc-4578-bc07-
bcf2a82d1463"

New-BrokerMachine  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -CatalogUid 3 -HostedMachineId "c10n1"
-HypervisorConnectionUid 4 -IsReserved $False -MachineName
"S-1-5-21-2589939477-3963209805-1860259709-1121"
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します
- 構成プロセス全体を確認するには、「インストールと構成」を参照してください
- カタログを管理するには、「マシンカタログの管理」および「HPE Moonshotカタログの管理」を参照してください

詳細情報

- 接続とリソースの作成および管理
- HPE Moonshotへの接続
- マシンカタログの作成

Microsoft Azure カタログを作成する

> **注:**

2023年7月以降、MicrosoftはAzure Active Directory (Azure AD) をMicrosoft Entra IDに名称変更しました。このドキュメントでは、Azure Active Directory、Azure AD、またはAADへの言及はすべてMicrosoft Entra IDを指します。

(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create.html)は、マシンカタログを作成するウィザードについて説明しています。以下の情報は、Microsoft Azure Resource Managerクラウド環境に固有の詳細を扱います。

注:

Microsoft Azureカタログを作成する前に、Microsoft Azureへの接続の作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/connections/connection-azure-resource-manager.html)を参照してください。

マシンカタログの作成

マシンカタログは、次の2つの方法で作成できます。

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

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

イメージは、ディスク、スナップショット、またはAzure Compute Gallery内のイメージ定義のイメージバージョンであり、マシンカタログ内のVMを作成するために使用されます。マシンカタログを作成する前に、Azure Resource Managerでイメージを作成します。イメージに関する一般的な情報については、「マシンカタログの作成」を参照してください。

注:

ホスト接続で構成されているリージョンとは異なるリージョンからマスターイメージを使用するサポートは非推奨です。Azure Compute Galleryを使用して、マスターイメージを目的のリージョンにレプリケートしてください。

MCSマシンカタログを作成する際、DHCPの有効化やライセンスのリアームなどの準備タスクを実行するために、元のVMに基づいて一時的なVMが作成されます。この一時的なVMは準備VMと呼ばれます。この準備VMの名前は**Preparati-84x9n**という形式に従い、最後の5文

> 字は重複を避けるためにランダムに生成されます。この準備VMの命名規則は固定されており、カスタマイズできません。準備タスクが完了すると、準備VMは破棄されます。

準備VMからネットワークを切断するために、すべてのインバウンドおよびアウトバウンドトラフィックを拒否するネットワークセキュリティグループが作成されます。ネットワークセキュリティグループは、カタログごとに1回自動的に作成されます。ネットワークセキュリティグループの名前は`Citrix-Deny-All-a3pgu-GUID`で、GUIDはランダムに生成されます。例: `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`。

マシンカタログ作成ウィザードで:

- 「**マシンタイプ**」および「**マシン管理**」ページには、Azure固有の情報は含まれていません。マシンカタログの作成の記事のガイダンスに従ってください。
- 「**イメージ**」ページで、このカタログでマシンを作成するためのテンプレートとして使用するイメージを選択します。

  使用するイメージタイプとして**マスターイメージ**を選択する場合は、**イメージの選択**をクリックし、必要に応じてマスターイメージを選択するために次の手順に従います:

  a. （テナント内またはテナント間で共有イメージが構成されている接続にのみ適用）イメージが存在するサブスクリプションを選択します。
  b. リソースグループを選択します。
  c. Azure VHD、Azure Compute Gallery、またはAzureイメージバージョンに移動します。必要に応じて、選択したイメージにメモを追加します。

  イメージを選択する際は、以下を考慮してください:

  - Citrix VDAがイメージにインストールされていることを確認します。
  - VMに接続されているVHDを選択する場合は、次の手順に進む前にVMをシャットダウンする必要があります。

> **注:**
>
> - カタログ内のマシンを作成した接続（ホスト）に対応するサブスクリプションは、緑色の点で示されます。その他のサブスクリプションは、Azure Compute Galleryがそのサブスクリプションと共有されているものです。これらのサブスクリプションでは、共有ギャラリーのみが表示されます。共有サブスクリプションの構成方法につい

ては、テナント内でイメージを共有する（サブスクリプション間）およびテナント間でイメージを共有するを参照してください。

- 信頼できる起動が有効になっているイメージまたはスナップショットを選択する場合、**セキュリティの種類**として信頼できる起動を持つマシンプロファイルを使用することが必須です。その後、マシンプロファイルでSecureBootとvTPMの値を指定することで、それらを有効または無効にできます。信頼できる起動はShared Image Galleryではサポートされていません。Azureの信頼できる起動の詳細については、`<https://docs.microsoft.com/ja-jp/azure/virtual-machines/trusted-launch>`を参照してください。
- 信頼できる起動を備えたWindowsでエフェメラルOSディスクを使用してプロビジョニングスキームを作成できます。信頼できる起動を備えたイメージを選択する場合、vTPMが有効になっている信頼できる起動を備えたマシンプロファイルを選択する必要があります。エフェメラルOSディスクを使用してマシンカタログを作成する方法については、エフェメラルOSディスクを使用してマシンを作成する方法を参照してください。
- イメージのレプリケーションが進行中の場合でも、続行してそのイメージをマスターイメージとして選択し、セットアップを完了できます。ただし、イメージのレプリケーション中にカタログの作成が完了するまでに時間がかかる場合があります。MCSでは、カタログ作成から1時間以内にレプリケーションが完了する必要があります。レプリケーションがタイムアウトすると、カタログの作成は失敗します。Azureでレプリケーションステータスを確認できます。レプリケーションがまだ保留中の場合、またはレプリケーションが完了した後に、もう一度試してください。
- Azureでマシンカタログのマスターイメージを選択すると、MCSは選択したマスターイメージとマシンプロファイルに基づいてOSの種類を識別します。MCSが識別できない場合は、マスターイメージと一致するOSの種類を選択してください。
- Gen2イメージを使用してGen2 VMカタログをプロビジョニングすると、起動時間のパフォーマンスを向上させることができます。ただし、Gen1イメージを使用してGen2マシンカタログを作成することはサポートされていません。同様に、Gen2イメージを使用してGen1マシンカタログを作成することもサポートされていません。また、世代情報を持たない古いイメージはすべてGen1イメージです。

使用するイメージの種類として**準備済みイメージ**を選択する場合は、**イメージの選択**をクリックし、必要に応じて準備済みイメージを選択します。

VMの作成を成功させるには、イメージにCitrix VDA 2311以降がインストールされており、VDAにMCSIOが存在することを確認してください。

イメージを選択すると、**マシンプロファイルを使用する（Azure Active Directoryに必須）**チェックボックスが自動的に選択されます。**マシンプロファイルの選択**をクリックして、リソースグループのリストからVMまたはARMテンプレート仕様を参照します。カタログ内のVMは、選択したマシンプロファイルから構成を継承できます。

ARMテンプレート仕様がマシンカタログを作成するためのマシンプロファイルとして使用できることを確認するために検証します。ARMテンプレート仕様を検証する方法は2つあります。

- リソースグループリストからARMテンプレート仕様を選択した後、**次へ**をクリックします。ARMテンプレート仕様にエラーがある場合、エラーメッセージが表示されます。
- 次のPowerShellコマンドのいずれかを実行します。
  - `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  - `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

VMがマシンプロファイルから継承できる構成の例は次のとおりです。

- アクセラレーテッドネットワーク
- ブート診断
- ホストディスクキャッシュ (OSおよびMCSIOディスクに関連)
- マシンサイズ (別途指定がない限り)
- VMに配置されたタグ

カタログを作成した後、イメージがマシンプロファイルから継承する構成を表示できます。**マシンカタログ**ノードでカタログを選択し、下部のペインでその詳細を表示します。次に、**テンプレートプロパティ**タブをクリックして、マシンプロファイルのプロパティを表示します。**タグ**セクションには、最大3つのタグが表示されます。VMに配置されたすべてのタグを表示するには、**すべて表示**をクリックします。

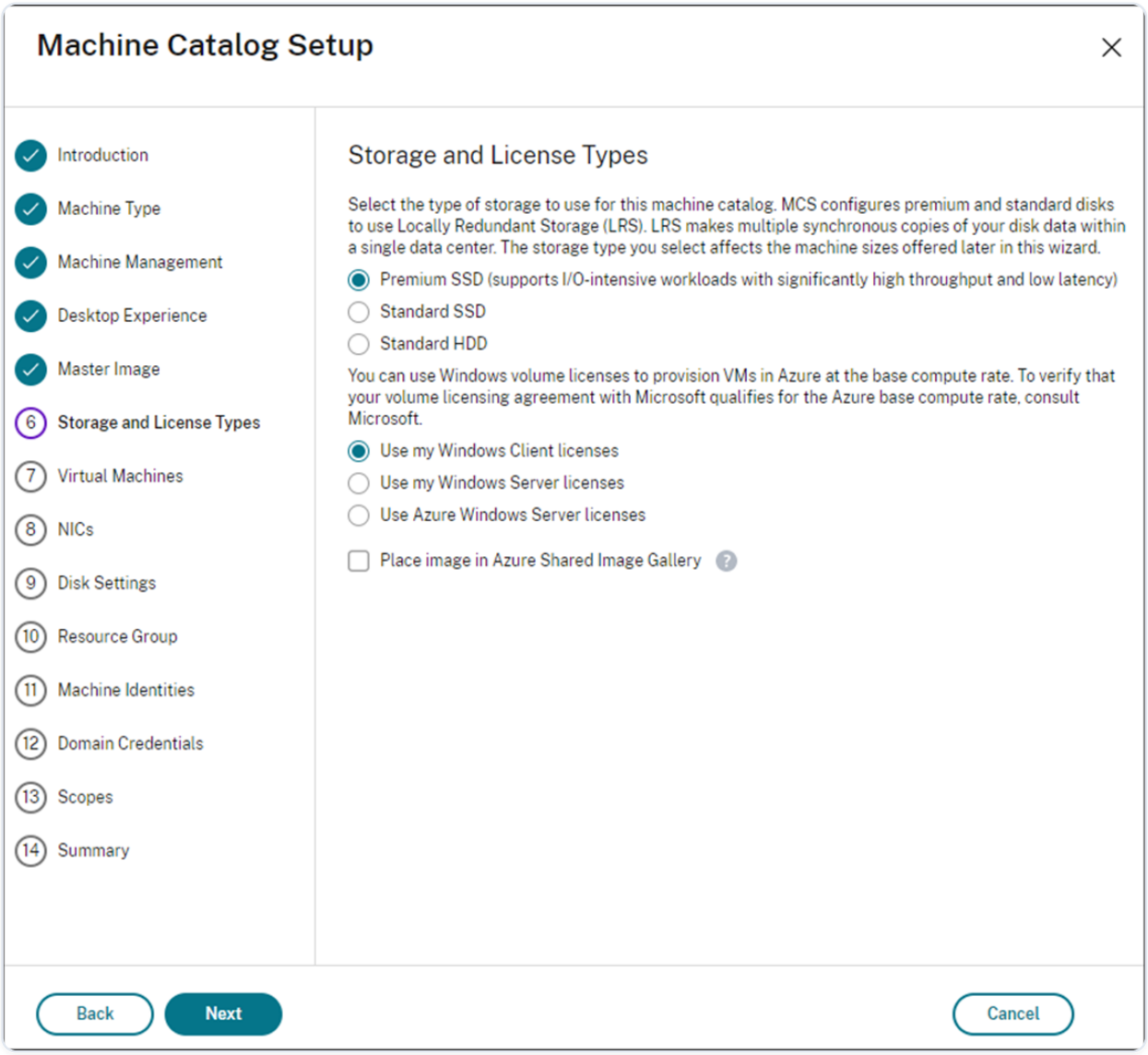
MCSでAzure専用ホストにVMをプロビジョニングする場合は、**専用ホストグループを使用する**チェックボックスを有効にしてから、リストからホストグループを選択します。ホストグループは、専用ホストのコレクションを表すリソースです。専用ホストは、1つ以上のVMをホストする物理サーバーを提供するサービスです。お客様のサーバーはAzureサブスクリプション専用であり、他のサブスクライバーと共有されることはありません。専用ホストを使用すると、Azureは、お客様のVMがそのホストで実行されている唯一のマシンであることを保証しま

す。この機能は、規制要件または内部セキュリティ要件を満たす必要があるシナリオに適しています。ホストグループとそれらを使用する際の考慮事項の詳細については、「Azure 専用ホスト」を参照してください。

重要:

- Azure自動配置が有効になっているホストグループのみが表示されます。
- ホストグループを使用すると、ウィザードの後半で提供される**仮想マシン**ページが変更されます。選択したホストグループに含まれるマシンサイズのみがそのページに表示されます。また、可用性ゾーンは自動的に選択され、選択できません。

- Azure Resource Managerイメージを使用する場合にのみ、**ストレージとライセンスの種類**ページが表示されます。



マシンカタログで使用できるストレージの種類は次のとおりです。

- **プレミアムSSD**。I/O集中型ワークロードを持つVMに適した、高性能で低遅延のディスクストレージオプションを提供します。
- **Standard SSD**。低いIOPSレベルで一貫したパフォーマンスを必要とするワークロードに適した、費用対効果の高いストレージオプションを提供します。
- **Standard HDD**。待機時間に影響を受けにくいワークロードを実行するVMに適した、信頼性の高い低コストのディスクストレージオプションを提供します。
- **Azureエフェメラルosディスク**。VMのローカルディスクを再利用してオペレーティングシステムディスクをホストする、費用対効果の高いストレージオプションを提供します。または、PowerShellを使用してエフェメラルOSディスクを使用するマシンを作成することもできます。詳細については、「Azure エフェメラルディスク」を参照してください。エフェメラルOSディスクを使用する際の以下の考慮事項に注意してください。
  - AzureエフェメラルOSディスクとMCS I/Oは同時に有効にできません。
  - エフェメラルOSディスクを使用するマシンを更新するには、VMのキャッシュディスクまたは一時ディスクのサイズを超えないイメージを選択する必要があります。
  - ウィザードの後半で提示される**電源サイクル中にVMとシステムディスクを保持する**オプションは使用できません。

> **注:**
>
> IDディスクは、選択したストレージタイプに関係なく、常にStandard SSDを使用して作成されます。

> ストレージタイプによって、ウィザードの**仮想マシン**ページで提供されるマシンサイズが決まります。MCSは、プレミアムディスクと標準ディスクをローカル冗長ストレージ（LRS）を使用するように構成します。LRSは、単一のデータセンター内でディスクデータの複数の同期コピーを作成します。AzureエフェメラルOSディスクは、VMのローカルディスクを使用してオペレーティングシステムを保存します。Azureストレージタイプとストレージレプリケーションの詳細については、以下を参照してください。

- `<https://docs.microsoft.com/ja-jp/azure/storage/common/storage-introduction/>`
- `<https://docs.microsoft.com/ja-jp/azure/virtual-machines/premium-storage-performance/>`

- `<https://docs.microsoft.com/ja-jp/azure/storage/common/storage-redundancy/>`

既存のWindowsライセンスまたはLinuxライセンスを使用するかどうかを選択します。

- Windowsライセンス：Windowsイメージ（Azureプラットフォームサポートイメージまたはカスタムイメージ）とともにWindowsライセンスを使用すると、AzureでWindows VMを低コストで実行できます。ライセンスには次の2種類があります。
  - **Windows Serverライセンス**。Windows ServerまたはAzure Windows Serverライセンスを使用でき、Azureハイブリッド特典を利用できます。詳細については、`<https://azure.microsoft.com/ja-jp/pricing/hybrid-benefit/>`を参照してください。Azureハイブリッド特典は、AzureでVMを実行するコストを基本コンピューティング料金に削減し、Azureギャラリーからの追加のWindows Serverライセンスのコストを免除します。
  - **Windowsクライアントライセンス**。Windows 10およびWindows 11ライセンスをAzureに持ち込み、追加のライセンスなしでAzureでWindows 10およびWindows 11 VMを実行できます。詳細については、クライアントアクセスライセンスと管理ライセンスを参照してください。

プロビジョニングされたVMがライセンス特典を使用していることを確認するには、次のPowerShellコマンドを実行します: `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`。

- Windows Serverライセンスタイプの場合、ライセンスタイプが **Windows_Server** であることを確認します。詳細な手順は `<https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/hybrid-use-benefit-licensing/>` で入手できます。
- Windowsクライアントライセンスタイプの場合、ライセンスタイプが**Windows_Client**であることを確認します。詳細な手順は`<https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/>`で入手できます。

または、`Get-Provscheme` PowerShell SDKを使用して検証を行うこともできます。例: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`。このコマンドレットの詳細については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/>`を参照してください。

- Linuxライセンス: BYOS (bring-your-own-subscription) Linuxライセンスを使用すると、ソフトウェアの料金を支払う必要はありません。BYOS料金には、コンピューティングハードウェア料金のみが含まれます。ライセンスには2種類あります。
  - **RHEL_BYOS**: RHEL_BYOSタイプを正常に使用するには、AzureサブスクリプションでRed Hat Cloud Accessを有効にしてください。
  - **SLES_BYOS**: SLESのBYOSバージョンには、SUSEからのサポートが含まれています。

`New-ProvScheme`および`Set-ProvScheme`でLicenseTypeの値をLinuxオプションに設定できます。

`New-ProvScheme`でLicenseTypeをRHEL_BYOSに設定する例:

```
New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "azureCatalog"
-RunAsynchronously -Scope @() -SecurityGroup @() -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" /><Property xsi:type="StringProperty"
Name="StorageAccountType" Value="StandardSSD_LRS" /><Property
xsi:type="StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /
><Property xsi:type="StringProperty" Name="OsType" Value="Linux" /
><Property xsi:type="StringProperty" Name="LicenseType"
Value="RHEL_BYOS" /></CustomProperties>'
```

`Set-ProvScheme`でLicenseTypeをSLES_BYOSに設定する例:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog"
-CustomProperties '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"><Property
xsi:type="StringProperty" Name="UseManagedDisks" Value="true" /
><Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" /><Property xsi:type="StringProperty"
Name="ResourceGroups" Value="hu-dev-mcs" /><Property
xsi:type="StringProperty" Name="OsType" Value="Linux" /><Property
xsi:type="StringProperty" Name="LicenseType" Value="SLES_BYOS" /></
CustomProperties>'
```

> **注:**
>
> `LicenseType`の値が空の場合、デフォルト値はOsTypeの値に応じて、Azure Windows Server LicenseまたはAzure Linux Licenseになります。

LicenseTypeを空に設定する例:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog"
-CustomProperties '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"><Property
xsi:type="StringProperty" Name="UseManagedDisks" Value="true" /
><Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" /><Property xsi:type="StringProperty"
Name="ResourceGroups" Value="hu-dev-mcs" /><Property
xsi:type="StringProperty" Name="OsType" Value="Linux" /></
CustomProperties>'
```

ライセンスの種類とその利点については、以下のドキュメントを参照してください。

- `<https://docs.microsoft.com/ja-jp/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet>`
- `<https://docs.microsoft.com/ja-jp/azure/virtual-machines/linux/azure-hybrid-benefit-linux>`

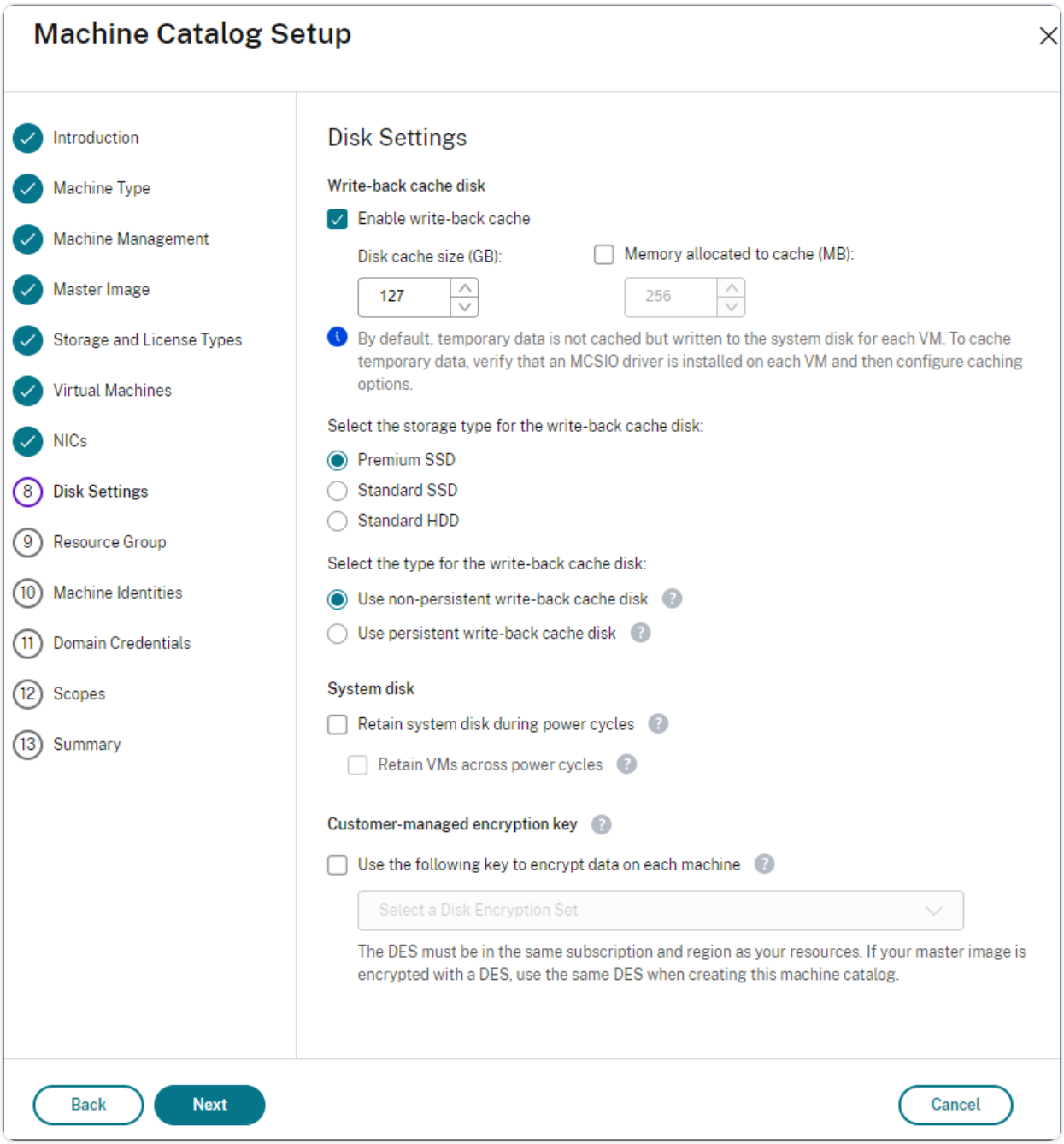
Azure Compute Gallery（旧称Azure Shared Image Gallery）は、イメージを管理および共有するためのリポジトリです。これにより、組織全体でイメージを利用できるようになります。大規模な非永続マシンカタログを作成する際には、SIGにイメージを保存することをお勧めします。そうすることで、VDA OSディスクのリセットが高速化されるためです。**Azure Compute Galleryに準備済みイメージを配置**を選択すると、**Azure Compute Gallery設定**セクションが表示され、追加のAzure Compute Gallery設定を指定できます。

- **仮想マシンとイメージレプリカの比率**。Azureに保持させたい仮想マシンとイメージレプリカの比率を指定できます。デフォルトでは、Azureは非永続マシン40台ごとに1つのイメージレプリカを保持します。永続マシンの場合、この数値はデフォルトで1,000になります。

- **最大レプリカ数**。Azure に保持させるイメージレプリカの最大数を指定できます。デフォルトは 100 です。

> **注:**
>
> イメージを保存するために、ACG にギャラリーが作成されます。このギャラリーは、VM 作成のために MCS からのみアクセス可能であり、**イメージの選択**ページには表示されません。

- **仮想マシン**ページで、作成するVMの数を指定します。少なくとも1つを指定し、マシンサイズを選択する必要があります。カタログ作成後、カタログを編集してマシンサイズを変更できます。
- **NICs**ページにはAzure固有の情報は含まれていません。マシンカタログの作成の記事のガイダンスに従ってください。
- **ディスク設定**ページで、ライトバックキャッシュを有効にするかどうかを選択します。MCS ストレージ最適化機能が有効になっている場合、カタログ作成時に以下の設定を構成できます。これらの設定は、Azure と GCP の両方の環境に適用されます。



ライトバックキャッシュを有効にした後、以下を実行できます。

- 一時データのキャッシュに使用されるディスクとRAMのサイズを構成します。詳細については、一時データのキャッシュを構成するを参照してください。
- ライトバックキャッシュディスクのストレージタイプを選択します。ライトバックキャッシュディスクに使用できるストレージオプションは次のとおりです。
  - プレミアム SSD
  - スタンダード SSD
  - スタンダード HDD

- プロビジョニングされたVMに対してライトバックキャッシュディスクを永続化するかどうかを選択します。オプションを有効にするには、**ライトバックキャッシュを有効にする**を選択します。デフォルトでは、**非永続ライトバックキャッシュディスクを使用する**が選択されています。
- ライトバックキャッシュディスクの種類を選択します。
  - **非永続ライトバックキャッシュディスクを使用**。選択した場合、ライトバックキャッシュディスクは電源サイクル中に削除されます。そこにリダイレクトされたデータはすべて失われます。VMの一時ディスクに十分な空き容量がある場合、コストを削減するために、その一時ディスクがライトバックキャッシュディスクのホストとして使用されます。カタログ作成後、プロビジョニングされたマシンが一時ディスクを使用しているかどうかを確認できます。これを行うには、カタログをクリックし、「**テンプレートプロパティ**」タブの情報を確認します。一時ディスクが使用されている場合、「**非永続ライトバックキャッシュディスク**」とその値が「**はい（VMの一時ディスクを使用）**」と表示されます。そうでない場合、「**非永続ライトバックキャッシュディスク**」とその値が「**いいえ（VMの一時ディスクを使用しない）**」と表示されます。
  - **永続ライトバックキャッシュディスクを使用**。選択した場合、ライトバックキャッシュディスクはプロビジョニングされたVMに対して永続化されます。このオプションを有効にすると、ストレージコストが増加します。
- 電源サイクル中にVDAのVMとシステムディスクを保持するかどうかを選択します。

  電源サイクル中にVMとシステムディスクを保持。これは「**ライトバックキャッシュを有効にする**」を選択した場合に利用可能です。デフォルトでは、VMとシステムディスクはシャットダウン時に削除され、起動時に再作成されます。VMの再起動時間を短縮したい場合は、このオプションを選択します。このオプションを有効にすると、ストレージコストも増加することに注意してください。
- 「**ストレージコストの節約**」を有効にするかどうかを選択します。有効にすると、VMがシャットダウンしたときにストレージディスクをStandard HDDにダウングレードすることで、ストレージコストを節約できます。VMは再起動時に元の設定に戻ります。このオプションは、ストレージディスクとライトバックキャッシュディスクの両方に適用されます。または、PowerShellを使用することもできます。「VMシャットダウン時にストレージタイプを下位層に変更する」を参照してください。

> **注:**

> Microsoftは、VMシャットダウン中のストレージタイプの変更に制限を課しています。また、Microsoftが将来的にストレージタイプの変更をブロックする可能性もあります。詳細については、このMicrosoftの記事を参照してください。

- このカタログ内のマシンのデータを暗号化するかどうか、および使用する暗号化キーを選択します。顧客管理キー（CMK）によるサーバー側暗号化を使用すると、マネージドディスクレベルで暗号化を管理し、カタログ内のマシンのデータを保護できます。デフォルト設定は、マシンプロファイルまたはマスターイメージのいずれかから継承され、プロファイルが優先されます。
  - *CMK*を使用する*マシンプロファイル*を使用している場合、「**各マシン上のデータを暗号化するために次のキーを使用する**」オプションが自動的に選択され、*マシンプロファイル*からのキーがデフォルトになります。
  - Platform Managed Key (PMK)を使用する*マシンプロファイル*を使用しており、*マスターイメージ*が*CMK*で暗号化されている場合、「**各マシン上のデータを暗号化するために次のキーを使用する**」オプションが自動的に選択され、マスターイメージからのキーがデフォルトになります。
  - *マシンプロファイルを使用しておらず、マスターイメージ*が*CMK*で暗号化されている場合、「**各マシン上のデータを暗号化するために次のキーを使用する**」オプションが自動的に選択され、*マスターイメージ*からのキーがデフォルトになります。

  詳細については、「Azureサーバー側暗号化」を参照してください。

- 「**リソースグループ**」ページで、リソースグループを作成するか、既存のグループを使用するかを選択します。
  - リソースグループを作成することを選択した場合は、「**次へ**」を選択します。
  - 既存のリソースグループを使用することを選択した場合は、「**利用可能なプロビジョニングリソースグループ**」リストからグループを選択します。**注意**: カタログで作成するマシンを収容するのに十分なグループを選択してください。選択したグループが少なすぎる場合はメッセージが表示されます。後でカタログにVMを追加する予定がある場合は、必要最小限よりも多く選択することをお勧めします。カタログ作成後に、カタログにリソースグループを追加することはできません。

  詳細については、「Azure リソース グループ」を参照してください。

- **マシン ID** ページで、ID タイプを選択し、このカタログ内のマシンの ID を構成します。VM を **Azure Active Directory に参加済み**として選択した場合、それらを Azure AD セキュリティ グループに追加できます。詳細な手順は次のとおりです。

a. **ID タイプ**フィールドから、**Azure Active Directory に参加済み**を選択します。**Azure AD セキュリティ グループ (オプション)**オプションが表示されます。

b. **Azure AD セキュリティ グループ: 新規作成**をクリックします。

c. グループ名を入力し、**作成**をクリックします。

d. 画面の指示に従って Azure にサインインします。 グループ名が Azure に存在しない場合、緑色のアイコンが表示されます。それ以外の場合は、新しい名前を入力するよう求めるエラーメッセージが表示されます。

e. VM のマシンアカウントの命名スキームを入力します。

カタログ作成後、Citrix Virtual Apps and Desktops™ はユーザーに代わって Azure にアクセスし、セキュリティグループと、そのグループの動的メンバーシップルールを作成します。このルールに基づき、このカタログで指定された命名スキームを持つ VM は自動的にセキュリティグループに追加されます。

このカタログに異なる命名スキームを持つ VM を追加するには、Azure にサインインする必要があります。その後、Citrix Virtual Apps and Desktops は Azure にアクセスし、新しい命名スキームに基づいて動的メンバーシップルールを作成できます。

このカタログを削除する際、Azure からセキュリティグループを削除するには、Azure へのサインインも必要です。

- **ドメイン資格情報**および**概要**ページには、Azure 固有の情報は含まれていません。マシンカタログの作成の記事のガイダンスに従ってください。

ウィザードを完了します。

Azure一時ディスクがライトバックキャッシュディスクとして適格であるための条件

Azure一時ディスクをライトバックキャッシュディスクとして使用できるのは、以下のすべての条件が満たされている場合のみです。

- Azure 一時ディスクは永続データに適していないため、ライトバックキャッシュディスクは非永続的である必要があります。
- 選択したAzure VMサイズには一時ディスクが含まれている必要があります。
- エフェメラルOSディスクを有効にする必要はありません。
- ライトバックキャッシュファイルをAzure一時ディスクに配置することを受け入れます。
- Azure一時ディスクのサイズは、（ライトバックキャッシュディスクサイズ + ページングファイル用の予約スペース + 1 GBのバッファースペース）の合計サイズよりも大きい必要があります。

非永続的なライトバックキャッシュディスクのシナリオ

次の表は、マシンカタログの作成時に一時ディスクをライトバックキャッシュに使用する場合の3つの異なるシナリオについて説明しています。

シナリオ	結果
ライトバックキャッシュに一時ディスクを使用するためのすべての条件が満たされています。	WBCファイル `mcsdif.vhdx` は一時ディスクに配置されます。
一時ディスクには、ライトバックキャッシュの使用に十分なスペースがありません。	VHDディスク `MCSWCDisk` が作成され、WBCファイル `mcsdif.vhdx` がこのディスクに配置されます。
一時ディスクにはライトバックキャッシュの使用に十分なスペースがありますが、`UseTempDiskForWBC` が **false** に設定されています。	VHDディスク `MCSWCDisk` が作成され、WBCファイル `mcsdif.vhdx` がこのディスクに配置されます。

Azure テンプレート仕様を作成する

Azure ポータルで Azure テンプレート仕様を作成し、Web Studio および PowerShell コマンドで使用して、MCS マシンカタログを作成または更新できます。

既存のVMのAzureテンプレートスペックを作成するには：

1. Azure portalに移動します。リソースグループを選択し、VMとネットワークインターフェイスを選択します。上部にある**...**メニューから、**テンプレートのエクスポート**をクリックします。
2. カタログプロビジョニング用のテンプレートスペックを作成する場合は、**パラメーターを含める**チェックボックスをオフにします。JSONファイルで `parameters` および `variables` セクションが次のようになっていることを確認します。

   ```
   "parameters": {},

   "variables": {}
   ```

3. **ダウンロード**をクリックして、テンプレートをJSONファイルとして保存します。
4. Azureポータルで、**テンプレートスペック**を選択し、**テンプレートのインポート**をクリックします。

5. コンピューターに保存されているマシンプロファイル（JSON形式）を参照してインポートします。
6. **名前**、**サブスクリプション**、**リソースグループ**、**場所**、および**バージョン**を指定します。**次へ: テンプレートの編集**をクリックします。
7. **確認と作成**を実行し、テンプレートスペックを作成します。
8. **テンプレートスペック**ページで、作成したテンプレートスペックを確認します。テンプレートスペックをクリックします。左側のパネルで、**バージョン**をクリックします。
9. **新しいバージョンの作成**をクリックして、新しいバージョンを作成できます。新しいバージョン番号を指定し、現在のテンプレートスペックに変更を加え、**確認と作成**をクリックして、テンプレートスペックの新しいバージョンを作成します。

以下のPowerShellコマンドを使用して、テンプレートスペックとテンプレートバージョンの情報を取得できます。

- テンプレートスペックの情報を取得するには、以下を実行します。

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec
```

- テンプレートスペックバージョンの情報を取得するには、以下を実行します。

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec\bgg1.0.templatespecversion
```

カタログの作成または更新でテンプレート仕様を使用する

MCSマシンカタログは、マシンプロファイル入力としてテンプレート仕様を使用して作成または更新できます。これを行うには、Web StudioまたはPowerShellコマンドを使用できます。

- Web Studioについては、「Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する」(#create-a-machine-catalog-using-an-azure-resource-manager-image-in-web-studio)を参照してください。
- PowerShellについては、「PowerShellを使用してカタログを作成または更新する際にテンプレート仕様を使用する」(#use-template-spec-in-creating-or-updating-a-catalog-using-powershell)を参照してください。

Azureサーバー側暗号化

Citrix Virtual Apps and Desktopsは、Azure Key Vaultを介したAzureマネージドディスクの顧客管理暗号化キーをサポートしています。このサポートにより、独自の暗号化キーを使用してマシンカタログのマネージドディスクを暗号化することで、組織およびコンプライアンス要件を管理できます。詳細については、「Azure Disk Storageのサーバー側暗号化」を参照してください。

マネージドディスクでこの機能を使用する場合：

- ディスクの暗号化に使用されるキーを変更するには、`DiskEncryptionSet`で現在のキーを変更します。その`DiskEncryptionSet`に関連付けられているすべてのリソースは、新しいキーで暗号化されるように変更されます。
- キーを無効にするか削除すると、そのキーを使用しているディスクを持つVMは自動的にシャットダウンします。シャットダウン後、キーが再度有効になるか、新しいキーを割り当てない限り、VMは使用できません。そのキーを使用しているカタログは電源をオンにできず、VMを追加することもできません。

顧客管理暗号化キーを使用する際の重要な考慮事項

この機能を使用する際は、以下を考慮してください。

- 顧客管理キーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンに存在する必要があります。
- 顧客管理キーで暗号化されたディスク、スナップショット、およびイメージは、別のリソースグループやサブスクリプションに移動できません。
- リージョンごとのディスク暗号化セットの制限については、Microsoft サイトを参照してください。

> **注:**
>
> Azure サーバー側暗号化の構成については、クイックスタート: Azure portal を使用して Key Vault を作成する を参照してください。

Azureカスタマーマネージド暗号化キー

マシンカタログを作成する際、カタログにプロビジョニングされたマシン上のデータを暗号化するかどうかを選択できます。カスタマーマネージド暗号化キーによるサーバー側暗号化を使用すると、マネージドディスクレベルで暗号化を管理し、カタログ内のマシン上のデータを保護でき

ます。ディスク暗号化セット (DES) は、カスタマーマネージドキーを表します。この機能を使用するには、まずAzureでDESを作成する必要があります。DESは次の形式です。

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryptionSet`

リストからDESを選択します。選択するDESは、リソースと同じサブスクリプションおよびリージョンにある必要があります。

を参照してください。(#create-a-machine-catalog-with-customer-managed-encryption-key).

ホストでのAzureディスク暗号化

ホストでの暗号化機能を備えたMCSマシンカタログを作成できます。現在、MCSはこの機能に対してマシンプロファイルワークフローのみをサポートしています。マシンプロファイルの入力として、VMまたはテンプレート仕様を使用できます。

この暗号化方法は、Azureストレージを介してデータを暗号化しません。VMをホストするサーバーがデータを暗号化し、その後、暗号化されたデータがAzureストレージサーバーを介して流れます。したがって、この暗号化方法はデータをエンドツーエンドで暗号化します。

制限事項：

ホストでのAzureディスク暗号化は次のとおりです。

- すべてのAzureマシンサイズでサポートされているわけではありません
- Azure ディスク暗号化と互換性がありません

ホストでの暗号化機能を備えたマシンカタログを作成するには：

1. サブスクリプションでホストでの暗号化機能が有効になっているかどうかを確認します。これを行うには、`<https://learn.microsoft.com/ja-jp/rest/api/resources/features/get?tabs=HTTP/>`を参照してください。有効になっていない場合は、サブスクリプションでこの機能を有効にする必要があります。サブスクリプションで機能を有効にする方法については、`<https://learn.microsoft.com/ja-jp/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/>`を参照してください。
2. 特定のAzure VMサイズがホストでの暗号化をサポートしているかどうかを確認します。これを行うには、PowerShellウィンドウで次のいずれかを実行します。

```
PS XDHyp:\Connections\<your connection>\east
us.region\serviceoffering.folder>
```

```
PS XDHyp:\HostingUnits\<your hosting unit>\serviceoffering.folder>
```

3. Azure portalで、ホストでの暗号化を有効にして、マシンプロファイルの入力としてVMまたはテンプレート仕様を作成します。
   - VMを作成する場合は、ホストでの暗号化をサポートするVMサイズを選択します。VMを作成すると、VMプロパティの**ホストでの暗号化**が有効になります。
   - テンプレート仕様を使用する場合は、`securityProfile`内でパラメータ`Encryption at Host`を**true**として割り当てます。
4. VMまたはテンプレート仕様のいずれかを選択して、マシンプロファイルワークフローでMCSマシンカタログを作成します。
   - OSディスク/データディスク: 顧客管理キーとプラットフォーム管理キーによって暗号化されます。
   - エフェメラルOSディスク: プラットフォーム管理キーによってのみ暗号化されます。
   - キャッシュディスク: 顧客管理キーとプラットフォーム管理キーによって暗号化されます。

   Web StudioまたはPowerShellコマンドを実行して、マシンカタログを作成できます。

マシンプロファイルからホストでの暗号化情報を取得する

`AdditionalData`パラメータを指定してPowerShellコマンドを実行すると、マシンプロファイルからホストでの暗号化情報を取得できます。`EncryptionAtHost`パラメータが**True**の場合、マシンプロファイルでホストでの暗号化が有効になっていることを示します。

例: マシンプロファイルの入力がVMの場合、次のコマンドを実行します。

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def.v
m).AdditionalData
```

例: マシンプロファイルの入力がテンプレート仕様の場合、次のコマンドを実行します。

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def_t
emplatespec.templatespec\EncryptionAtHost.templatespecversion).AdditionalD
ata
```

マネージドディスクの二重暗号化

二重暗号化を使用してマシンカタログを作成できます。この機能で作成されたすべてのカタログは、プラットフォーム管理キーと顧客管理キーの両方でサーバー側で暗号化されたすべてのディスクを持ちます。Azure Key Vault、暗号化キー、およびディスク暗号化セット（DES）は、お客様が所有および管理します。

二重暗号化は、プラットフォーム側暗号化（デフォルト）と顧客管理暗号化（CMEK）です。したがって、暗号化アルゴリズム、実装、または侵害されたキーに関連するリスクを懸念するセキュリティ意識の高いお客様は、この二重暗号化を選択できます。永続的なOSディスクとデータディスク、スナップショット、およびイメージはすべて、二重暗号化によって保存時に暗号化されます。

注記:

- Web StudioとPowerShellコマンドを使用して、二重暗号化されたマシンカタログを作成および更新できます。PowerShellコマンドについては、「二重暗号化されたマシンカタログの作成」を参照してください。
- 二重暗号化されたマシンカタログを作成または更新するには、マシンプロファイルに基づかないワークフロー、またはマシンプロファイルに基づくワークフローを使用できます。
- マシンプロファイルに基づかないワークフローを使用してマシンカタログを作成する場合、保存されている`DiskEncryptionSetId`を再利用できます。
- マシンプロファイルを使用する場合、VMまたはテンプレート仕様をマシンプロファイルの入力として使用できます。

制限事項:

- 二重暗号化は、Ultra DisksまたはPremium SSD v2ディスクではサポートされていません。
- 二重暗号化は、アンマネージドディスクではサポートされていません。

- カタログに関連付けられているDiskEncryptionSetキーを無効にすると、そのカタログのVMは無効になります。
- お客様が管理するキーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンに存在する必要があります。
- サブスクリプションごとに、リージョンあたり最大50個のディスク暗号化セットしか作成できません。

Azureリソースグループ

Azureプロビジョニングリソースグループは、ユーザーにアプリケーションとデスクトップを提供するVMをプロビジョニングする方法を提供します。MCSマシンカタログでVMをプロビジョニングするために、リソースグループを作成するか、既存のリソースグループを使用できます。複数のマシンカタログで同じリソースグループを使用できます。Azureリソースグループの詳細については、Microsoftドキュメントを参照してください。

Azureリソースグループの使用状況

Azureリソースグループあたりの仮想マシン、マネージドディスク、スナップショット、イメージの数に制限はありません。（Azureリソースグループあたり240個のVM、800個のマネージドディスクという制限は削除されました。）

- マシンカタログを作成するためにフルスコープのサービスプリンシパルを使用する場合、MCS は 1 つの Azure リソースグループのみを作成し、そのグループをカタログに使用します。
- マシンカタログを作成するためにナロースコープのサービスプリンシパルを使用する場合、カタログ用に空の、事前に作成された Azure リソースグループを提供する必要があります。

Azure エフェメラルディスク

Azure エフェメラルディスク を使用すると、キャッシュディスクまたは一時ディスクを再利用して、Azure 対応仮想マシンの OS ディスクを保存できます。この機能は、標準の HDD ディスクよりも高性能な SSD ディスクを必要とする Azure 環境で役立ちます。Azure エフェメラルディスクを使用してカタログを作成する方法については、「Azure エフェメラルディスクを使用してカタログを作成する」を参照してください。

> **注:**
>
> 永続カタログはエフェメラル OS ディスクをサポートしていません。

> エフェメラル OS ディスクでは、プロビジョニングスキームでマネージドディスクと共有イメージギャラリーを使用する必要があります。

エフェメラル OS 一時ディスクの保存

エフェメラル OS ディスクを VM の一時ディスクまたはリソースディスクに保存するオプションがあります。この機能により、キャッシュがない、またはキャッシュが不足している VM でエフェメラル OS ディスクを使用できます。このような VM には、`Ddv4` のように、エフェメラル OS ディスクを保存するための一時ディスクまたはリソースディスクがあります。

次の点を考慮してください。

- エフェメラルディスクは、VM キャッシュディスクまたは VM の一時（リソース）ディスクのいずれかに保存されます。キャッシュディスクが OS ディスクのコンテンツを保持するのに十分な大きさでない限り、一時ディスクよりもキャッシュディスクが優先されます。
- 更新の場合、キャッシュディスクより大きく、一時ディスクより小さい新しいイメージは、エフェメラル OS ディスクを VM の一時ディスクに置き換えることになります。

Azure エフェメラルディスクと Machine Creation Services (MCS) ストレージ最適化 (MCS I/O)

Azure エフェメラル OS ディスクと MCS I/O は同時に有効にできません。

重要な考慮事項は次のとおりです。

- エフェメラルOSディスクとMCS I/Oの両方を同時に有効にしたマシンカタログを作成することはできません。
- `New-ProvScheme` または `Set-ProvScheme` でPowerShellパラメーター（`UseWriteBackCache` および `UseEphemeralOsDisk`）を**true**に設定すると、適切なエラーメッセージが表示されて失敗します。
- 両方の機能が有効になっている既存のマシンカタログについては、引き続き次の操作を実行できます。
    - マシンカタログを更新する。
    - VMを追加または削除する。
    - マシンカタログを削除する。

アジュール コンピュート ギャラリー

AzureでMCSによってプロビジョニングされたマシン用の公開イメージリポジトリとして、Azure Compute Gallery（旧称：Azure Shared Image Gallery）を使用します。公開イメージをギャラリーに保存することで、OSディスクの作成とハイドレーションを高速化し、非永続VMの起動時間

とアプリケーション起動時間を改善できます。共有イメージギャラリーには、次の3つの要素が含まれています。

- *ギャラリー*: イメージはここに保存されます。MCSは、マシンカタログごとに1つのギャラリーを作成します。
- *ギャラリーイメージ定義*: この定義には、公開イメージに関する情報（オペレーティングシステムの種類と状態、Azureリージョン）が含まれています。MCSは、カタログ用に作成されたイメージごとに1つのイメージ定義を作成します。
- *ギャラリーイメージバージョン*: Shared Image Gallery内の各イメージは複数のバージョンを持つことができ、各バージョンは異なるリージョンに複数のレプリカを持つことができます。各レプリカは、公開イメージの完全なコピーです。

> **注:**
>
> Shared Image Gallery機能は、マネージドディスクとのみ互換性があります。レガシーマシンカタログでは使用できません。

> 詳細については、「Azure Compute Gallery の概要」を参照してください。

PowerShellを使用してAzure Compute Galleryイメージでマシンカタログを作成または更新する方法については、「Azure Compute Galleryイメージを使用してマシンカタログを作成または更新する」を参照してください。

Azure 機密 VM

Azure 機密コンピューティング VM は、仮想デスクトップがメモリ内で暗号化され、使用中に保護されることを保証します。

MCSを使用してAzure機密VMを含むカタログを作成できます。このようなカタログを作成するには、マシンプロファイルワークフローを使用する必要があります。VMとARMテンプレート仕様の両方をマシンプロファイル入力として使用できます。

機密VMに関する重要な考慮事項

サポートされているVMサイズと、機密VMを使用したマシンカタログの作成に関する重要な考慮事項は次のとおりです。

- サポートされているVMサイズ: 機密VMは、次のVMサイズをサポートしています:
    - DCasv5 シリーズ

  - DCadsv5 シリーズ
  - ECasv5 シリーズ
  - ECadsv5 シリーズ

- 機密VMを使用してマシンカタログを作成します。
  - Web StudioおよびPowerShellコマンドを使用して、Azure 機密VMを含むマシンカタログを作成できます。
  - Azure 機密VMを含むマシンカタログを作成するには、マシンプロファイルベースのワークフローを使用する必要があります。マシンプロファイルの入力として、VMまたはテンプレート仕様を使用できます。
  - マスターイメージとマシンプロファイルの入力は、同じ機密セキュリティタイプで有効にする必要があります。セキュリティタイプは次のとおりです。
    - **VMGuestStateOnly**: VMゲストの状態のみが暗号化された機密VM
    - **DiskWithVMGuestState**: OSディスクとVMゲスト状態の両方がプラットフォーム管理キーまたは顧客管理キーで暗号化された機密VM。通常のOSディスクとエフェメラルOSディスクの両方を暗号化できます。
  - マネージドディスク、スナップショット、Azure Compute Galleryイメージ、VM、ARMテンプレート仕様など、さまざまなリソースタイプの機密VM情報をAdditionalDataパラメーターを使用して取得できます。例:

    ```
    PS C:\Users\username> (get-item XDHyp:
    \HostingUnits\mynetwork\image.folder\username-dev-testing-
    rg.resourcegroup\username-dev-tsvda.vm).AdditionalData
    ```

    追加データフィールドは次のとおりです。
    - DiskSecurityType
    - ConfidentialVMDiskEncryptionSetId
    - DiskSecurityProfiles

    マシンサイズの機密コンピューティングプロパティを取得するには、次のコマンドを実行します: `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

    追加データフィールドは`ConfidentialComputingType`です。

- マスターイメージまたはマシンプロファイルを、機密から非機密セキュリティタイプへ、あるいは非機密から機密セキュリティタイプへ変更することはできません。
- 不適切な構成に対しては、適切なエラーメッセージが表示されます。

マスターイメージとマシンプロファイルの準備

機密VMのセットを作成する前に、次の手順に従ってマスターイメージとマシンプロファイルを準備します。

1. Azureポータルで、次のような特定の設定で機密VMを作成します。
   - **セキュリティの種類**: 機密仮想マシン
   - **機密OSディスク暗号化**: 有効。
   - **キー管理**：プラットフォーム管理キーによる機密ディスク暗号化 機密VMの作成に関する詳細については、こちらのMicrosoft記事を参照してください。
2. 作成したVMでマスターイメージを準備します。作成したVMに必要なアプリケーションとVDAをインストールします。

   > **注:**
   >
   > VHDを使用した機密VMの作成はサポートされていません。代わりに、Azure Compute Gallery、マネージドディスク、またはスナップショットを使用してください。

3. 次のいずれかの方法でマシンプロファイルを作成します。
   - ステップ1で作成した既存のVMが必要なマシンプロパティを持っている場合は、それを使用します。
   - マシンプロファイルとしてARMテンプレート仕様を選択する場合は、必要に応じてテンプレート仕様を作成します。具体的には、*SecurityEncryptionType*や*diskEncryptionSet*（顧客管理キーの場合）など、機密VMの要件を満たすパラメーターを構成します。詳細については、Azureテンプレート仕様の作成を参照してください。

     > **注:**
     >
     > - マスターイメージとマシンプロファイルが同じセキュリティキータイプであることを確認してください。

- 顧客管理キーによる機密OSディスク暗号化を必要とする機密VMを作成するには、マスターイメージとマシンプロファイルの両方でディスク暗号化セットIDが同じであることを確認してください。

Web Studio または PowerShell コマンドを使用して機密VMを作成する

機密VMのセットを作成するには、マスターイメージと、目的の機密VMから派生したマシンプロファイルを使用してマシンカタログを作成します。

Web Studioを使用してカタログを作成するには、マシンカタログの作成に記載されている手順に従います。以下の考慮事項に留意してください。

- **イメージ**ページで、機密VM作成のために準備したマスターイメージとマシンプロファイルを選択します。マシンプロファイルの選択は必須であり、選択したマスターイメージと同じセキュリティ暗号化タイプに一致するプロファイルのみが選択可能です。
- **仮想マシン**ページでは、機密VMをサポートするマシンサイズのみが選択肢として表示されます。
- 「**ディスク設定**」ページでは、選択したマシンプロファイルから継承されるため、ディスク暗号化セットを指定できません。

Azure Marketplace (アジュール マーケットプレイス)

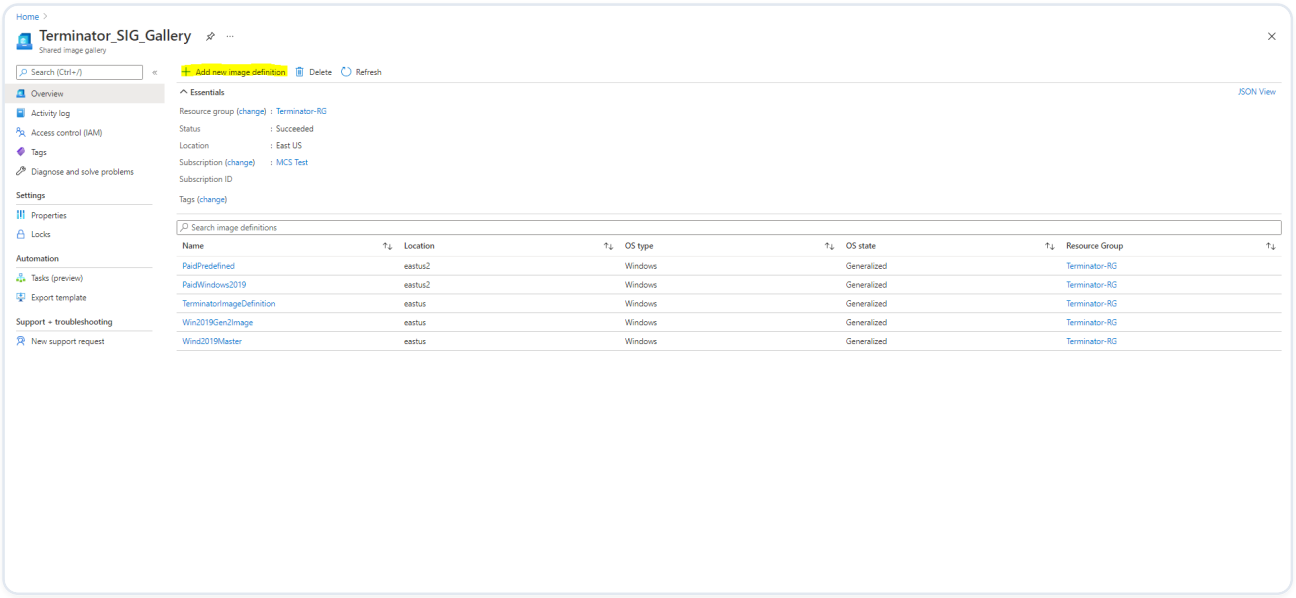
Citrix Virtual Apps and Desktopsは、プラン情報を含むAzure上のマスターイメージを使用してマシンカタログを作成することをサポートしています。詳細については、「Microsoft Azure Marketplace」を参照してください。

ヒント:

標準のWindows Serverイメージなど、Azure Marketplaceで見つかる一部のイメージには、プラン情報が追加されていません。Citrix Virtual Apps and Desktopsの機能は、有料イメージ向けです。

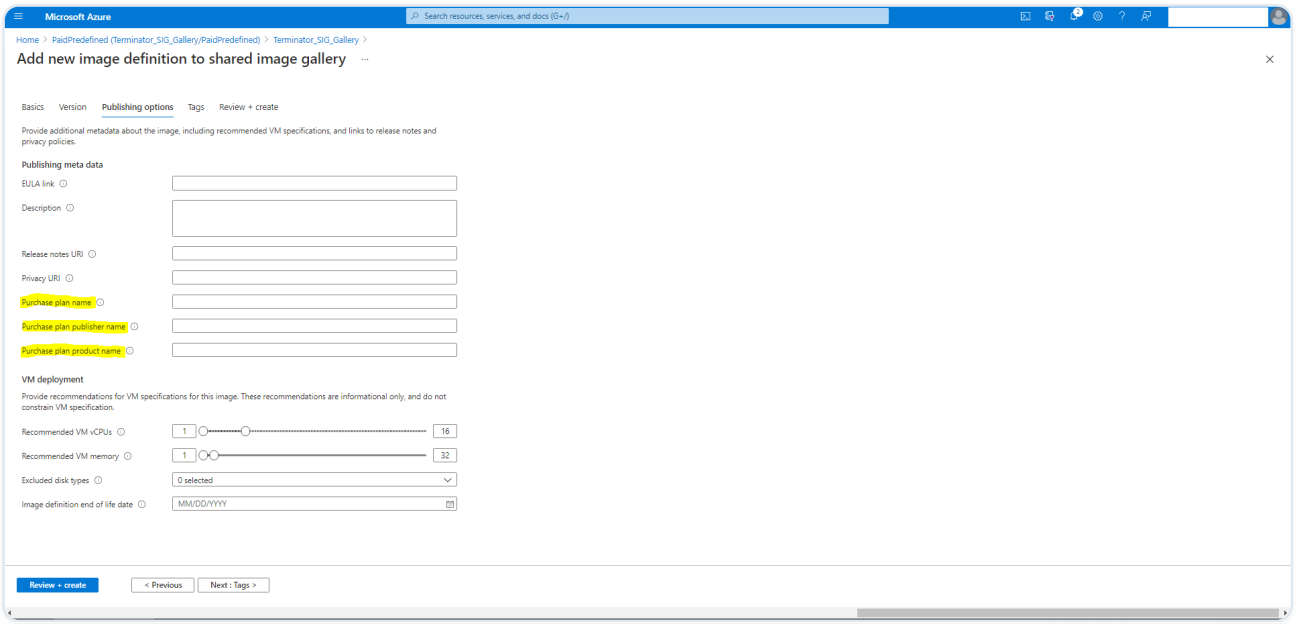
Shared Image Galleryで作成されたイメージにAzureプラン情報が含まれていることを確認する

このセクションの手順を使用して、Web StudioでShared Image Galleryのイメージを表示します。これらのイメージは、オプションでマスターイメージとして使用できます。イメージをShared Image Galleryに配置するには、ギャラリーでイメージ定義を作成します。

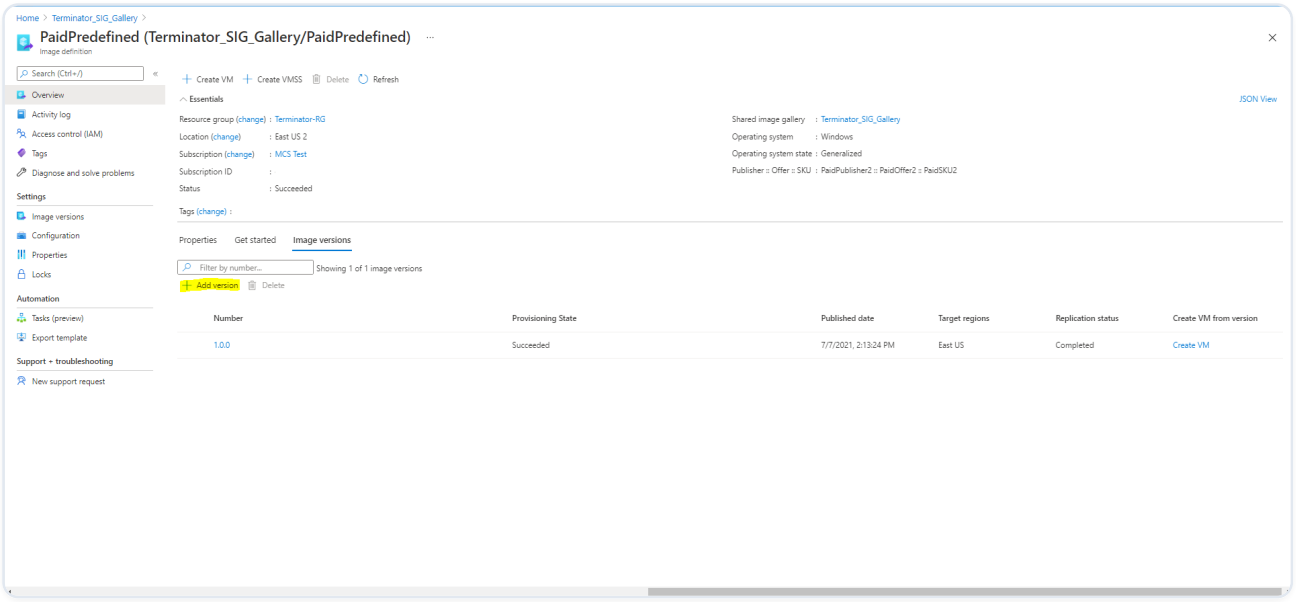


公開オプションページで、購入プラン情報を確認します。

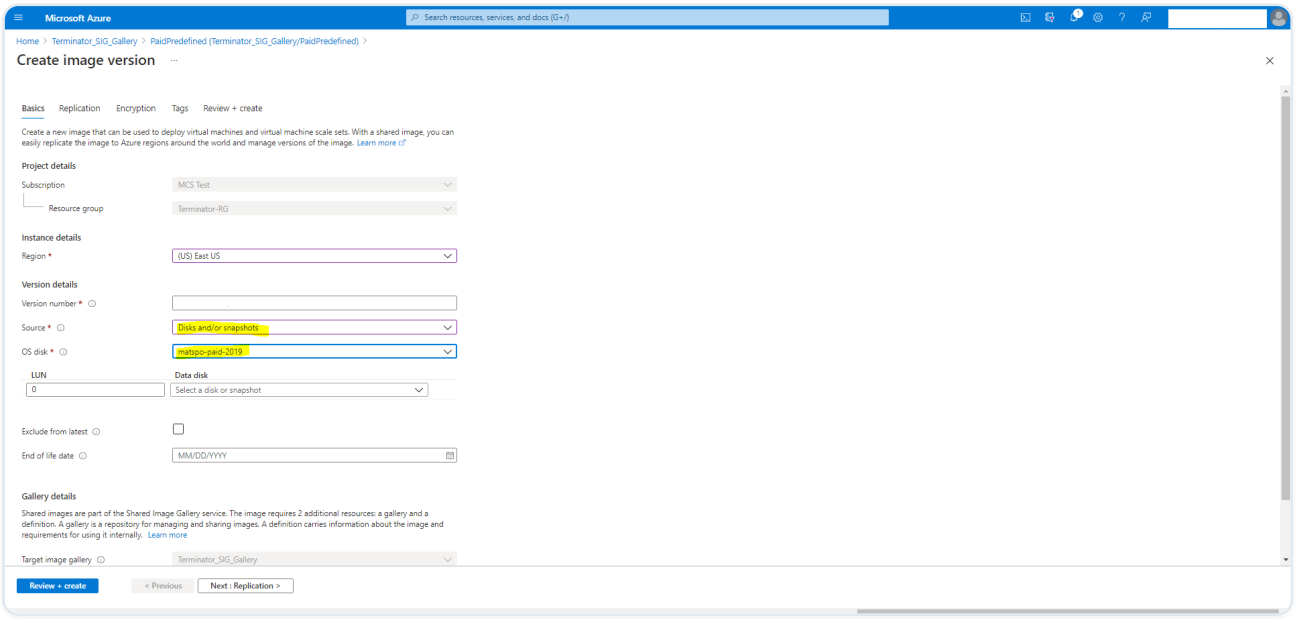
購入プラン情報フィールドは最初は空です。これらのフィールドに、イメージに使用する購入プラン情報を入力します。購入プラン情報を入力しないと、マシンカタログのプロセスが失敗する可能性があります。



購入プラン情報を確認した後、定義内にイメージバージョンを作成します。これはマスターイメージとして使用されます。**バージョンの追加**をクリックします。



バージョン詳細セクションで、イメージスナップショットまたはマネージドディスクをソースとして選択します。



オンデマンド容量予約VMのカタログを作成する

オンデマンド容量予約を使用すると、Azureリージョンまたは可用性ゾーンで任意の期間、コンピューティング容量を予約できます。Azureオンデマンド容量予約の詳細については、Microsoftドキュメント「オンデマンド容量予約」を参照してください。

マシンプロファイル（VMまたはテンプレート仕様）を使用して、オンデマンド容量予約付きのAzure VMのMCSマシンカタログを作成できます。また、既存のマシンカタログと既存のVMを更新して、オンデマンド容量予約を追加または削除することもできます。

この機能は、永続的および非永続的なマシンカタログに適用されます。

制限事項

この機能は以下には適用されません。

- スポットVM
- ホストグループ
- 休止状態が有効なVM

制限の詳細については、Microsoft ドキュメントの「制限事項」を参照してください。

オンデマンド容量予約VMのカタログを作成する手順

1. マシンプロファイルソース（VMまたはARMテンプレート仕様）を作成します。VMまたはARMテンプレート仕様の作成については、VMを容量予約グループに関連付けるを参照してください。
2. マシンプロファイルでオンデマンド容量予約が有効になっているかどうかを確認するには、次のPowerShellコマンドを実行します。マシンプロファイルでオンデマンド容量予約が有効になっている場合、`capacityReservationGroup id`を取得します。

   例：

   マシンプロファイルソースがVMの場合、次のコマンドを実行します。

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-
   conn2\machineprofile.folder\fifthcolumn.resourcegroup\demand-
   capacity.vm").AdditionalData
   ```

   マシンプロファイルソースがテンプレート仕様の場合、次のコマンドを実行します。

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-
   conn2\machineprofile.folder\fifthcolumn.resourcegroup\fc-aeh-
   templatespec.templatespec\14.0.0-capacity-
   reservation.templatespecversion").AdditionalData
   ```

3. Web StudioまたはPowerShellコマンドを使用して、マシンプロファイルを使用してマシンカタログを作成します。

`Set-ProvScheme`コマンドを使用してカタログを更新できます。PowerShellコマンド`Set-ProvVmUpdateTimeWindow`を使用して既存のVMを更新することもできます。マシンプロファイルは次回の電源投入時に更新されます。

ネストされた仮想化

ネストされた仮想化が有効になっているマスターVMを構成すると、そのマスターVMを使用して作成されたMCSマシンカタログ内のすべてのVMでネストされた仮想化が有効になります。この機能は、永続VMと非永続VMの両方に適用されます。既存のMCSマシンカタログと既存のVMをイメージ更新によってネストされた仮想化を持つように更新できます。

現在、Dv3およびEv3 VMサイズのみがネストされた仮想化をサポートしています。

ネストされた仮想化の詳細については、Microsoft のブログ Nested Virtualization in Azure を参照してください。

PowerShell を使用してマシンカタログを作成する

このセクションでは、PowerShell を使用してカタログを作成する方法について詳しく説明します。

- 非永続ライトバックキャッシュディスクを使用したカタログの作成
- 永続ライトバックキャッシュディスクを使用したカタログの作成
- MCSIOによる起動パフォーマンスの向上
- PowerShellを使用したカタログの作成または更新におけるテンプレート仕様の使用
- 信頼できる起動を備えたマシンカタログ
- マシンプロパティ値の使用
- 顧客管理の暗号化キーを使用してマシンカタログを作成する(#create-a-machine-catalog-with-customer-managed-encryption-key)
- 二重暗号化でマシンカタログを作成する
- Azure エフェメラルディスクを持つカタログを作成する
- Azure 専用ホスト
- Azure Compute Gallery イメージを使用してマシンカタログを作成または更新する
- Shared Image Gallery を構成する
- 指定された可用性ゾーンにマシンをプロビジョニングする
- ストレージの種類
- ページファイル設定の更新(#update-page-file-setting)
- Azure Spot VMを使用してカタログを作成する(#create-a-catalog-using-azure-spot-vms)
- バックアップVMサイズを構成する
- すべてのリソースのタグをコピーする

- Azure Monitor Agentがインストールされたカタログ VMのプロビジョニング(#provision-catalog-vms-with-azure-monitor-agent-installed)

非永続的なライトバックキャッシュディスクを持つカタログの作成

非永続的なライトバックキャッシュディスクを使用してカタログを構成するには、PowerShellパラメーター`New-ProvScheme CustomProperties`を使用します。カスタムプロパティ`UseTempDiskForWBC`は、ライトバックキャッシュファイルを保存するためにAzure一時ストレージを使用することを受け入れるかどうかを示します。一時ディスクをライトバックキャッシュディスクとして使用する場合は、`New-ProvScheme`の実行時にこれをtrueに構成する必要があります。このプロパティが指定されていない場合、パラメーターはデフォルトで**False**に設定されます。

例えば、`CustomProperties` パラメーターを使用して、`UseTempDiskForWBC` を **true** に設定する場合:

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="true"/
> `

</CustomProperties>'
```

> **注：**

> マシンカタログをコミットして、書き戻しキャッシュファイルにAzureローカル一時ストレージを使用するように設定した後で、VHDを使用するように変更することはできません。

永続的なライトバックキャッシュディスクを持つカタログを作成する

永続的な書き戻しキャッシュディスクを持つカタログを構成するには、PowerShellパラメーター `New-ProvScheme CustomProperties` を使用します。このパラメーターは、MCSプロビジョニングされたマシンに対して書き戻しキャッシュディスクがどのように永続化するかを決定するために使用される追加のプロパティ `PersistWBC` をサポートします。`PersistWBC` プロパティは、`UseWriteBackCache` パラメーターが指定され、`WriteBackCacheDiskSize` パラメーターがディスクが作成されることを示すように設定されている場合にのみ使用されます。

`PersistWBC` をサポートする前の `CustomProperties` パラメーターに見られるプロパティの例を次に示します。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

</CustomProperties>
```

これらのプロパティを使用する場合、`CustomProperties` パラメーターからプロパティが省略されていると、それらはデフォルト値を含むことに注意してください。`PersistWBC` プロパティには、**true**または**false**の2つの可能な値があります。

`PersistWBC` プロパティを**true**に設定すると、Citrix Virtual Apps and Desktops管理者がWeb Studioを使用してマシンをシャットダウンしても、ライトバックキャッシュディスクは削除されません。

`PersistWBC` プロパティを**false**に設定すると、Citrix Virtual Apps and Desktops管理者がWeb Studioを使用してマシンをシャットダウンしたときに、ライトバックキャッシュディスクが削除されます。

注：

`PersistWBC` プロパティが省略されている場合、プロパティはデフォルトで **false** になり、Web Studioを使用してマシンがシャットダウンされると、書き戻しキャッシュは削除されます。

例えば、`CustomProperties` パラメーターを使用して、`PersistWBC` を true に設定する場合:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

重要：

`PersistWBC`プロパティは、`New-ProvScheme` PowerShellコマンドレットを使用してのみ設定できます。作成後にプロビジョニングスキームの`CustomProperties`を変更しようとしても、マシンカタログや、マシンがシャットダウンされたときのライトバックキャッシュディスクの永続性には影響しません。

例えば、`New-ProvScheme`をライトバックキャッシュを使用するように設定し、同時に`PersistWBC`プロパティをtrueに設定する場合：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

MCSIO を使用して起動パフォーマンスを向上させる

MCSIO が有効になっている場合、Azure および GCP のマネージドディスクの起動パフォーマンスを向上させることができます。この機能を構成するには、`New-ProvScheme` コマンドで

PowerShell の `PersistOSDisk` カスタムプロパティを使用します。`New-ProvScheme` に関連するオプションは次のとおりです。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->

````````Groups" Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```

この機能を有効にするには、`PersistOSDisk` カスタムプロパティを `true` に設定します。例:

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
```
```

```
-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

PowerShell を使用してカタログを作成または更新する際にテンプレート仕様を使用する

マシンプロファイルの入力としてテンプレート仕様を使用して、MCS マシンカタログを作成または更新できます。これを行うには、Web Studio または PowerShell コマンドを使用します。

Web Studio については、「Web Studio で Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

PowerShell コマンドを使用する:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*` を実行します。
3. カタログを作成または更新します。
    - カタログを作成するには:
        a. マシンプロファイルの入力としてテンプレート仕様を指定して `New-ProvScheme` コマンドを使用します。例:

```
New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
image.folder/fgthj.resourcegroup/nab-ws-
vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/test.templatespec/V1.templatespecversion"
```

```
-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>

[-LoggingId <Guid>]

[-BearerToken <String>][-AdminAddress <String>]

[<CommonParameters>]
```

b. カタログの作成を完了します。

- カタログを更新するには、マシンプロファイルの入力としてテンプレート仕様を指定して `Set-ProvScheme` コマンドを使用します。例:

```
Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
Us.region/vm.folder/MasterDisk.vm'

MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/testing.templatespec/V1.templatespecversion'

[-ProvisioningSchemeName] <String>

[-CustomProperties <String>][-ServiceOffering <String>] [-PassThru]

[-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <String>]
[<CommonParameters>]
```

信頼された起動を使用するマシンカタログ

信頼できる起動でマシンカタログを正常に作成するには、以下を使用します。

- 信頼できる起動を備えたマシンプロファイル
- 信頼できる起動をサポートするVMサイズ
- 信頼できる起動をサポートするWindows VMバージョン。現在、Windows 10、Windows 11、Windows Server 2016、2019、および2022が信頼できる起動をサポートしています。

重要:

MCSは、信頼できる起動が有効なVMを使用して新しいカタログを作成することをサポートしています。ただし、既存の永続カタログと既存のVMを更新するには、Azureポータルを使用する必要があります。非永続カタログの信頼できる起動を更新することはできません。詳細については、Microsoftドキュメント「既存のAzure VMで信頼できる起動を有効にする」を参照してください。

Citrix Virtual Apps and Desktopsの提供インベントリアイテムを表示し、VMサイズが信頼できる起動をサポートしているかどうかを判断するには、次のコマンドを実行します。

1. PowerShell ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、**asnp citrix***を実行します。
3. 次のコマンドを実行します。

```
$s = (ls XDHyp:\HostingUnits\<name of hosting
unit>\serviceoffering.folder\"<VM size>.serviceoffering)
```

4. `$s | select -ExpandProperty Additionaldata` を実行します。
5. `SupportsTrustedLaunch` 属性の値を確認します。
   - `SupportsTrustedLaunch` が**True**の場合、VMサイズは信頼できる起動をサポートしています。
   - `SupportsTrustedLaunch` が**False**の場合、VMサイズは信頼できる起動をサポートしていません。

AzureのPowerShellに従って、信頼できる起動をサポートするVMサイズを特定するには、次のコマンドを使用できます。

```
(Get-AzComputeResourceSku | where {$_.Locations.Contains($region) -and
($_.Name -eq "<VM size>") })[0].Capabilities
```

Azure PowerShellコマンドを実行した後、VMサイズが信頼できる起動をサポートするかどうかを説明する例を以下に示します。

- *例1*: Azure VMがGeneration 1のみをサポートしている場合、そのVMは信頼できる起動をサポートしません。したがって、Azure PowerShellコマンドを実行しても `TrustedLaunchDisabled` 機能は表示されません。
- *例2*: Azure VMがGeneration 2のみをサポートし、`TrustedLaunchDisabled` 機能が**True**の場合、Generation 2のVMサイズは信頼できる起動ではサポートされません。
- *例3*: Azure VMがGeneration 2のみをサポートし、PowerShellコマンドを実行しても `TrustedLaunchDisabled` 機能が表示されない場合、Generation 2のVMサイズは信頼できる起動でサポートされます。

Azure仮想マシンのトラステッド起動の詳細については、Microsoftドキュメント「Azure仮想マシンのトラステッド起動」を参照してください。

トラステッド起動でマシンカタログを作成する

1. 信頼できる起動が有効なマスターイメージを作成します。Microsoftドキュメント「Trusted launch VM Images」を参照してください。
2. セキュリティの種類を**信頼できる起動仮想マシン**としてVMまたはテンプレート仕様を作成します。VMまたはテンプレート仕様の作成の詳細については、Microsoftドキュメント「Deploy a trusted launch VM」を参照してください。
3. Web StudioまたはPowerShellコマンドを使用してマシンカタログを作成します。

   - Web Studioを使用する場合は、「Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する」を参照してください。
   - PowerShellコマンドを使用する場合は、VMまたはテンプレート仕様をマシンプロファイルの入力として `New-ProvScheme` コマンドを使用します。カタログを作成するためのコマンドの完全なリストについては、「カタログの作成」を参照してください。

     VMをマシンプロファイルの入力とする `New-ProvScheme` の例:

     ```
     New-ProvScheme -CleanOnBoot -HostingUnitName "name"
     -IdentityPoolName "name" -InitialBatchSizeHint 1

     -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
     fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

     -MachineProfile "XDHyp:
     \HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<mac
     hine profile vm.vm>"

     -ProvisioningSchemeName <String>
     ```

```
-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>]

[<CommonParameters>]
```

テンプレート仕様をマシンプロファイルの入力とする`New-ProvScheme`の例:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name"
-IdentityPoolName "name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>]

[<CommonParameters>]
```

信頼された起動でマシンカタログを作成する際のエラー

信頼された起動でマシンカタログを作成する際に、以下のシナリオで適切なエラーが発生します。

シナリオ	エラー
アンマネージドカタログの作成中にマシンプロファイルを選択した場合	`MachineProfileNotSupportedForUnmanagedCatalog`
マスターイメージとしてアンマネージドディスクを使用するカタログを作成する際に、信頼	`SecurityTypeNotSupportedForUnmanagedDisk`

シナリオ	エラー
された起動をサポートするマシンプロファイルを選択した場合	
セキュリティの種類として信頼された起動を持つマスターイメージソースを使用してマネージドカタログを作成する際に、マシンプロファイルを選択しない場合	`MachineProfileNotFoundForTrustedLaunchMasterImage`
マスターイメージのセキュリティの種類とは異なるセキュリティの種類を持つマシンプロファイルを選択した場合	`SecurityTypeConflictBetweenMasterImageAndMachineProfile`
カタログ作成時に、信頼された起動をサポートしないVMサイズを選択したが、信頼された起動をサポートするマスターイメージを使用した場合	`MachineSizeNotSupportTrustedLaunch`

マシンプロファイルプロパティ値の使用

マシンカタログは、カスタムプロパティで定義されている次のプロパティを使用します。

- アベイラビリティゾーン
- 専用ホストグループID
- ディスク暗号化セットID
- OSの種類
- ライセンスの種類
- ストレージの種類

これらのカスタムプロパティが明示的に定義されていない場合、プロパティ値は、マシンプロファイルとして使用されるARMテンプレート仕様またはVMから設定されます。さらに、`ServiceOffering`が指定されていない場合、マシンプロファイルから設定されます。

> **注:**
>
> マシンプロファイルに一部のプロパティが欠落しており、カスタムプロパティで定義されていない場合、該当する場合、プロパティのデフォルト値が適用されます。

以下のセクションでは、`New-ProvScheme`と`Set-ProvScheme`におけるいくつかのシナリオについて説明します。このシナリオでは、`CustomProperties`がすべてのプロパティを定義しているか、値がMachineProfileから派生しています。

- New-ProvSchemeのシナリオ
  - MachineProfileにすべてのプロパティがあり、CustomPropertiesが定義されていない場合。
    例:

    `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

    カタログのカスタムプロパティとして、次の値が設定されます:

    ```
    Get-ProvScheme | select CustomProperties

    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">

    <Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<mpA-value>"/>

    <Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
    value>"/>

    <Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
    value>"/>

    <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="<mpA-value>"/>

    <Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
    Value="<mpA-value>"/>

    <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
    value>"/>

    </CustomProperties>
    ```

  - MachineProfileに一部のプロパティがあり、CustomPropertiesが定義されていない場合。
    例: MachineProfileにはLicenseTypeとOsTypeのみがあります。

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
value>"/>

</CustomProperties>
```

- MachineProfileとCustomPropertiesの両方がすべてのプロパティを定義している場合。例:

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

カスタムプロパティが優先されます。カタログのカスタムプロパティとして、次の値が設定されます。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>
```

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones"
Value="<CustomPropertiesA-value>"/>

</CustomProperties>
```

- MachineProfileで一部のプロパティが定義され、CustomPropertiesで一部のプロパティが定義されている場合。例:
  - CustomProperties は LicenseType と StorageAccountType を定義します
  - MachineProfile は LicenseType、OsType、および Zones を定義します

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
value>"/>
```

```
</CustomProperties>
```

- 一部のプロパティは MachineProfile で定義され、一部のプロパティは CustomProperties で定義されています。さらに、ServiceOffering は定義されていません。例:
  - CustomProperties は StorageType を定義します
  - MachineProfile は LicenseType を定義します

```
New-ProvScheme -MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mp
.vm"

-ServiceOffering "XDHyp:
\HostingUnits\azureunit\serviceoffering.folder\<explicit-machine-
size>.serviceoffering"
```

カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<explicit-machine-size>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="explicit-storage-type"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="value-
from-machineprofile"/>

</CustomProperties>
```

- OsTypeがCustomPropertiesにもMachineProfileにもない場合、次のようになります:

    - 値はマスターイメージから読み取られます。
    - マスターイメージがアンマネージドディスクの場合、OsType は Windows に設定されます。例:

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -MasterImageVM "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-image.manageddisk"`

マスターイメージからの値は、この場合 Linux のカスタムプロパティに書き込まれます。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="OSType" Value="Linux"/>

</CustomProperties>
```

- Set-ProvSchemeのシナリオ
    - 既存のカタログで、以下を含むもの:
        - `StorageAccountType`とOsTypeのカスタムプロパティ
        - ゾーンを定義するMachineProfile `mpA.vm`
    - 更新:
        - StorageAccountType を定義する MachineProfile mpB.vm
        - LicenseTypeとOsTypeを定義する新しいカスタムプロパティセット $CustomPropertiesB

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm" -CustomProperties $CustomPropertiesB`

以下の値がカタログのカスタムプロパティとして設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesB-value>"/>

    </CustomProperties>
```

- 既存のカタログで、以下を含むもの:
  - S`torageAccountType`とOsTypeのカスタムプロパティ
  - StorageAccountType と LicenseType を定義する MachineProfile `mpA.vm`
- 更新:
  - StorageAccountTypeとOsTypeを定義する新しいカスタムプロパティセット $CustomPropertiesB。

`Set-ProvScheme -CustomProperties $CustomPropertiesB`

カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>
```

```
<Property xsi:type="StringProperty" Name="LicenseType" Value="<mp-A-value>"/>

</CustomProperties>
```

- 既存のカタログで:
  - `StorageAccountType` と OsType の CustomProperties
  - Zonesを定義するMachineProfile `mpA.vm`
- 更新:
  - StorageAccountType と LicenseType を定義する MachineProfile mpB.vm
  - `ServiceOffering`は指定されていません

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm"`

カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<value-from-machineprofile>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="StorageAccountType" Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<prior-CustomProperties-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpB-value>"/>
```

```
</CustomProperties>
```

VMごとに複数のNICを持つカタログを作成または更新する

MCSはVMごとに複数のNICをサポートしています。VM上の複数のNICを複数のサブネットに関連付けることができますが、それらのサブネットは同じ仮想ネットワーク (VNet) 内にある必要があります。PowerShellコマンドを使用して、次のことができます。

- VM上に複数のNICを持つカタログを作成する
- 既存のカタログ構成を更新して、VMに複数のNICを持たせ、新しく作成されたVMが複数のNICを持つようにする(#update-a-catalog-to-have-multiple-nics-on-a-vm)
- 既存のVMを更新して、複数のNICを持つようにする(#update-an-existing-vm-to-have-multiple-nics-on-a-vm)

マシンプロファイルに基づかないマシンカタログと、マシンプロファイルに基づくマシンカタログを作成または更新して、VMに複数のNICを持たせることができます。現在、マシンプロファイルに基づくマシンカタログの場合、マシンプロファイルのソースで指定されたのと同じ数のNICしか持てません。

アクセラレーテッドネットワーキングなどのプロパティは、マシンプロファイルソースから派生します。

注：

VMサイズは、同じ数のNICと対応するアクセラレーテッドネットワーキングをサポートしている必要があります。そうでない場合、エラーが発生します。

選択したVMサイズに関連付けられているNICの最大数を取得できます。`AdditionalData`パラメーターを指定してPowerShell `get-item`コマンドを実行すると、`MaxNetworkInterfaces`というPowerShellプロパティにNICの最大数が表示されます。

NICの最大数を取得する

NICの最大数を取得するには：

1. Delivery Controller™ホストから**PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために、`asnp citrix*`を実行します。

3. 利用可能なすべてのVMサイズを一覧表示するために、`Get-ChildItem -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder"`を実行します。
4. `get-item -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder\Standard_M416ms_v2.serviceoffering").AdditionalData`を実行します
5. NICの最大数を知るために、`MaxNetworkInterfaces`を確認します。

VMに複数のNICを持つカタログを作成する

VM上に複数のNICを持つカタログを作成するには、次の手順を実行します。

1. Delivery ControllerホストからPowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. まだ作成されていない場合は、IDプールを作成します。
4. プロビジョニングスキームを作成します。

   - マシンプロファイルに基づかないマシンカタログを作成する場合は、`NetworkMappings`パラメーターを指定して`New-ProvScheme`コマンドを実行します。パラメーター`NetworkMappings`に複数のサブネットを追加できます。例：

     ```
     New-Provscheme -NetworkMappings
     @{"0"="subnetpath1";"1"="subnetpath1"}
     ```

   - マシンプロファイルに基づいたマシンカタログを作成する場合：

     a. 複数のNICを持つVMをAzureに作成します。詳細については、「複数のNICを持つWindows仮想マシンの作成と管理」を参照してください。新しいVMを作成し、Azureポータルの「ネットワーク」ページでネットワークインターフェイスをアタッチすることもできます。

     b. VMをマシンプロファイルの入力として、`New-ProvScheme`コマンドを実行します。

     > **注:**
     >
     > マシンプロファイルに基づいたマシンカタログを作成する場合、`NetworkMappings`の数はマシンプロファイルの`NetworkInterfaceCount`と同じである必要がありま

> す。`NetworkInterfaceCount`は`Get-item -Path "machine profile path"`の`AdditionalData`から取得できます。

5. カタログの作成を完了します。

VM上に複数のNICを持つようにカタログを更新する

VM上に複数のNICを持つようにカタログを更新するには、次の手順を実行します。

1. Delivery Controllerホストから**PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. プロビジョニングスキームを更新します。

   - マシンプロファイルに基づかないマシンカタログを作成する場合は、`NetworkMappings`パラメーターを指定して`Set-ProvScheme`コマンドを実行します。パラメーター`NetworkMappings`に複数のサブネットを追加できます。例：

     ```
     Set-Provscheme -NetworkMappings
     @{"0"="subnetpath1";"1"="subnetpath1"}
     ```

   - マシンプロファイルに基づいてマシンカタログを作成する場合：

     a. 複数のNICを持つVMをAzureに作成します。詳しくは、「複数のNICを持つWindows仮想マシンの作成と管理」を参照してください。

     b. VMをマシンプロファイルの入力として使用して、`Set-ProvScheme`コマンドを実行します。

既存のVMを更新して、VMに複数のNICを持たせる

既存のVMを`Set-ProvVMUpdateTimeWindow`を使用して更新し、更新時間枠中に既存のVMの電源を再投入することもできます。

Azure Monitor Agentがインストールされたカタログ VMをプロビジョニングする

Azure監視は、Azureおよびオンプレミス環境からのテレメトリデータを収集、分析し、それに基づいて行動するために使用できるサービスです。

Azure Monitor Agent（AMA）は、仮想マシンなどのコンピューティングリソースから監視データを収集し、そのデータをAzure Monitorに配信します。現在、イベントログ、Syslog、パフォーマンスメトリックの収集をサポートし、Azure Monitor MetricsおよびAzure Monitor Logsデータソースに送信します。

監視データ内のVMを一意に識別して監視を有効にするには、AMAが拡張機能としてインストールされたMCSマシンカタログのVMをプロビジョニングできます。

要件

- 権限：必要なAzure権限で指定されている最小限のAzure権限と、Azure Monitorを使用するための以下の権限があることを確認してください。
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- データ収集ルール: Azure portal でデータ収集ルールを設定します。DCR の設定については、「データ収集ルールを作成する」を参照してください。DCR はプラットフォーム固有です (Windows または Linux)。必要なプラットフォームに応じて DCR を作成してください。 AMA は、データ収集ルール (DCR) を使用して、VM などのリソースと、Azure Monitor メトリックや Azure Monitor ログなどのデータソース間のマッピングを管理します。
- デフォルトワークスペース: Azure portal でワークスペースを作成します。ワークスペースの作成については、「Log Analytics ワークスペースを作成する」を参照してください。ログとデータを収集すると、その情報はワークスペースに保存されます。ワークスペースには、一意のワークスペース ID とリソース ID があります。ワークスペース名は、指定されたリソースグループ内で一意である必要があります。ワークスペースを作成したら、データソースとソリューションを設定して、データをワークスペースに保存します。
- モニター拡張機能をホワイトリストに登録しました: 拡張機能 `AzureMonitorWindowsAgent` および `AzureMonitorLinuxAgent` は、Citrix が定義したホワイトリスト登録済み拡張機能です。ホワイトリスト登録済み拡張機能のリストを表示するには、PoSH コマンド `Get-ProvMetadataConfiguration` を使用します。
- マスターイメージ: Microsoft は、既存のマシンから新しいマシンを作成する前に、既存のマシンから拡張機能を削除することを推奨しています。拡張機能が削除されない場合、残存ファイルや予期しない動作につながる可能性があります。詳細については、「既存の VM から VM を再作成する場合」を参照してください。

AMA を有効にしてカタログ VM をプロビジョニングするには:

1. マシンプロファイルテンプレートを設定します。
   - VMをマシンプロファイルテンプレートとして使用する場合：

a. Azure portal で VM を作成します。

b. VMの電源を入れます。

c. **リソース**の下のデータ収集ルールにVMを追加します。これにより、テンプレートVMにエージェントのインストールが呼び出されます。

> **注:**
>
> Linuxカタログを作成する必要がある場合は、Linuxマシンを設定します。

- テンプレート仕様をマシンプロファイルテンプレートとして使用する場合：

a. テンプレート仕様を設定します。

b. 生成されたテンプレート仕様に、次の拡張機能とデータ収集ルール関連付けを追加します。

```
{

"type": "Microsoft.Compute/virtualMachines/extensions",

"apiVersion": "2022-03-01",

"name": "<vm-name>/AzureMonitorWindowsAgent",

"dependsOn": [

    "Microsoft.Compute/virtualMachines/<vm-name>"

],

"location": "<azure-region>",

"properties": {

    "publisher": "Microsoft.Azure.Monitor",

    "type": "AzureMonitorWindowsAgent",

    "typeHandlerVersion": "1.0",

    "autoUpgradeMinorVersion": true,
```

```
    "enableAutomaticUpgrade": true

}

},

 {

    "type": "Microsoft.Insights/dataCollectionRuleAssociations",

    "apiVersion": "2021-11-01",

    "name": "<associatio-name>",

    "scope": "Microsoft.Compute/virtualMachines/<vm-name>",

    "dependsOn": [

     "Microsoft.Compute/virtualMachines/<vm-name>",

    "Microsoft.Compute/virtualMachines/<vm-name>/extensions/
AzureMonitorWindowsAgent"

    ],

    "properties": {

       "description": "Association of data collection rule.
Deleting this association will break the data collection for this
Arc server.",

     "dataCollectionRuleId": "/subscriptions/<azure-
subscription>/resourcegroups/<azure-resource-group>/providers/
microsoft.insights/datacollectionrules/<azure-data-collection-
rule>"

     }

    }
```

2. 既存のMCSマシンカタログを作成または更新します。

- 新しいMCSカタログを作成するには:
  a. Web Studio で、その VM またはテンプレート仕様をマシンプロファイルとして選択します。
  b. カタログを作成するための次の手順に進みます。
- 既存の MCS カタログを更新するには、次の PoSH コマンドを使用します。
  - 新しい VM に更新されたマシンプロファイルテンプレートを取得させるには、次のコマンドを実行します。

```
Set-ProvScheme -ProvisioningSchemeName "name"

-MachineProfile "XDHyp:
\HostingUnits\Unit1\machineprofile.folder\abc.resourcegroup\ab-
machine-profile.vm"
```

  - 既存の VM を更新されたマシンプロファイルテンプレートで更新するには：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

3. カタログVMの電源をオンにします。
4. Azureポータルに移動し、モニター拡張機能がVMにインストールされていること、およびVMがDCRのリソースの下に表示されていることを確認します。数分後、監視データがAzure Monitorに表示されます。

トラブルシューティング

Azure Monitor Agentのトラブルシューティングガイダンスについては、以下を参照してください。

- https://learn.microsoft.com/ja-jp/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/ja-jp/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

顧客管理の暗号化キーでマシンカタログを作成する

顧客管理の暗号化キーを使用してマシンカタログを作成する詳細な手順は次のとおりです。

1. PowerShellウィンドウを開きます。

2. Citrix固有のPowerShellモジュールをロードするために `asnp citrix*` を実行します。
3. `cd xdhyp:/` を入力します。
4. `cd .\HostingUnits\(your hosting unit)` を入力します。
5. `cd diskencryptionset.folder` を入力します。
6. ディスク暗号化セットのリストを取得するには、`dir` を入力します。
7. ディスク暗号化セットのIDをコピーします。
8. ディスク暗号化セットのIDを含めるカスタムプロパティ文字列を作成します。例：

```
$customProperties = "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"Standard_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"persistWBC`"
Value=`"False`" />

<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"false`" />

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/resourceGroups/
abc/providers/Microsoft.Compute/diskEncryptionSets/abc-des`"/>

</CustomProperties>
```

9. まだ作成されていない場合は、IDプールを作成します。例：

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain def.local -NamingSchemeType Numeric
```

10. New-ProvSchemeコマンドを実行します。例：

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\azure-
res2\image.folder\def.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-res2\
\virtualprivatecloud.folder\def.resourcegroup\def-
vnet.virtualprivatecloud\subnet1.network"}

-ProvisioningSchemeName "name"

-ServiceOffering "XDHyp:\HostingUnits\azure-
res2\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-MachineProfile "XDHyp:
\HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<machin
e profile vm.vm>"

-CustomProperties $customProperties
```

11. マシンカタログの作成を完了します。

二重暗号化されたマシンカタログを作成する

Web Studio および PowerShell コマンドを使用して、二重暗号化されたマシンカタログを作成および更新できます。

二重暗号化でマシンカタログを作成する詳細な手順は次のとおりです。

1. プラットフォーム管理キーと顧客管理キーを使用して Azure Key Vault と DES を作成します。Azure Key Vault と DES の作成方法については、「マネージドディスクの保存時の二重暗号化を有効にするために Azure ポータルを使用する」を参照してください。
2. ホスティング接続で利用可能な DiskEncryptionSets を参照するには：
   a. **PowerShell** ウィンドウを開きます。
   b. 次の PowerShell コマンドを実行します。
      i. `asnp citrix*`
      ii. `cd xdhyp:`:
      iii. `cd HostingUnits`

iv. `cd YourHostingUnitName` (例えば azure-east)

v. `cd diskencryptionset.folder`

vi. `dir`

`DiskEncryptionSet` の ID を使用して、カスタムプロパティでカタログを作成または更新できます。

3. マシンプロファイルワークフローを使用する場合は、VM またはテンプレート仕様をマシンプロファイル入力として作成します。

   - VMをマシンプロファイルの入力として使用する場合：

     a. Azure PortalでVMを作成します。

     b. **ディスク>キー管理**に移動し、`DiskEncryptionSetID`を使用してVMを直接暗号化します。

   - テンプレート仕様をマシンプロファイルの入力として使用する場合：

     a. テンプレートの`properties>storageProfile>osDisk>managedDisk`の下に、`diskEncryptionSet`パラメーターを追加し、二重暗号化DESのIDを追加します。

4. マシンカタログを作成します。

   - Web Studio を使用している場合は、マシンカタログの作成 の手順に加えて、次のいずれかを実行します。

     ◦ マシンプロファイルベースのワークフローを使用しない場合は、 ページで、 を選択します。次に、ドロップダウンメニューから二重暗号化DESを選択します。カタログの作成を続行します。

     ◦ マシンプロファイルワークフローを使用している場合は、 ページでマスターイメージとマシンプロファイルを選択します。マシンプロファイルのプロパティにディスク暗号化セット ID があることを確認します。

     カタログで作成されたすべてのマシンは、選択した DES に関連付けられたキーによって二重に暗号化されます。

   - PowerShellコマンドを使用する場合は、次のいずれかを実行します。

     ◦ マシンプロファイルベースのワークフローを使用しない場合は、`New-ProvScheme`コマンドにカスタムプロパティ`DiskEncryptionSetId`を追加します。例:

```
New-ProvScheme -CleanOnBoot -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />

</CustomProperties>'

-HostingUnitName "Redacted"

-IdentityPoolName "Redacted"

-InitialBatchSizeHint 1

-MasterImageVM "Redacted"

-NetworkMapping @{"0"="Redacted"}

-ProvisioningSchemeName "Redacted"

-ServiceOffering "Redacted"
```

- マシンプロファイルベースのワークフローを使用する場合は、`New-ProvScheme`コマンドでマシンプロファイル入力を指定します。例：

```
New-ProvScheme -CleanOnBoot

-HostingUnitName azure-east

-IdentityPoolName aio-ip

-InitialBatchSizeHint 1
```

```
-MasterImageVM XDHyp:\HostingUnits\azure-
east\image.folder\abc.resourcegroup\fgb-vda-snapshot.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-
east\virtualprivatecloud.folder\apa-
resourceGroup.resourcegroup\apa-resourceGroup-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName aio-test

-MachineProfile XDHyp:\HostingUnits\azure-
east\machineprofile.folder\abc.resourcegroup\abx-
mp.templatespec\1.0.0.templatespecversion
```

5. リモートPowerShell SDKを使用してカタログの作成を完了します。リモートPowerShell SDKを使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。カタログで作成されたすべてのマシンは、選択したDESに関連付けられたキーによって二重に暗号化されます。

暗号化されていないカタログを二重暗号化を使用するように変換する

マシンカタログの暗号化タイプ（カスタムプロパティまたはマシンプロファイルを使用）を更新できます。

- マシンプロファイルベースのワークフローを使用しない場合は、`Set-ProvScheme`コマンドでカスタムプロパティ DiskEncryptionSetId を追加します。例:

```
Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/12345678-xxxx-1234-1234-123456789012/resourceGroups/
Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/
SampleEncryptionSet" />

</CustomProperties>'
```

- マシンプロファイルベースのワークフローを使用する場合は、`Set-ProvScheme`コマンドでマシンプロファイル入力を利用します。例:

```
Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
XDHyp:\HostingUnits\azure-
east\machineprofile.folder\aelx.resourcegroup\elx-
mp.templatespec\1.0.0.templatespecversion
```

成功すると、カタログに追加するすべての新しいVMは、選択したDESに関連付けられたキーによって二重暗号化されます。

カタログが二重暗号化されていることを確認する

- ウェブスタジオで：

  a. **マシンカタログ**に移動します。

  b. 確認するカタログを選択します。画面下部にある**テンプレートプロパティ**タブをクリックします。

  c. **Azureの詳細**の下で、**ディスク暗号化セット**のディスク暗号化セットIDを確認します。カタログのDES IDが空白の場合、カタログは暗号化されていません。

  d. Azure Portal で、DES ID に関連付けられている DES の暗号化の種類がプラットフォーム管理キーと顧客管理キーであることを確認します。

- PowerShellコマンドを使用する:

  a. **PowerShell** ウィンドウを開きます。

  b. `asnp citrix*` を実行して、Citrix 固有の PowerShell モジュールをロードします。

  c. `Get-ProvScheme` を使用して、マシンカタログの情報を取得します。例:

```
Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
```

  d. マシンカタログの DES ID カスタムプロパティを取得します。例:

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-1234-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />
```

e. Azure Portal で、DES ID に関連付けられている DES の暗号化の種類がプラットフォーム管理キーと顧客管理キーであることを確認します。

Azure エフェメラルディスクを使用してカタログを作成する

エフェメラルディスクを使用するには、`New-ProvScheme` の実行時にカスタムプロパティ `UseEphemeralOsDisk` を **true** に設定する必要があります。

> **注:**
>
> カスタムプロパティ `UseEphemeralOsDisk` が **false** に設定されているか、値が指定されていない場合、プロビジョニングされたすべての VDA はプロビジョニングされた OS ディスクを引き続き使用します。

プロビジョニングスキームで使用するカスタムプロパティの例を次に示します。

```
"CustomProperties": [

            {

                "Name": "UseManagedDisks",

                "Value": "true"

            },

            {

                "Name": "StorageType",

                "Value": "Standard_LRS"

            },

            {

                "Name": "UseSharedImageGallery",

                "Value": "true"

            },
```

```
            {
                "Name": "SharedImageGalleryReplicaRatio",
                "Value": "40"
            },
            {
                "Name": "SharedImageGalleryReplicaMaximum",
                "Value": "10"
            },
            {
                "Name": "LicenseType",
                "Value": "Windows_Server"
            },
            {
                "Name": "UseEphemeralOsDisk",
                "Value": "true"
            }
        ],
```

カタログのエフェメラルディスクを構成する

カタログの Azure エフェメラル OS ディスクを構成するには、`Set-ProvScheme` で `UseEphemeralOsDisk` パラメーターを使用します。`UseEphemeralOsDisk` パラメーターの値を **true** に設定します。

> **注:**

この機能を使用するには、`UseManagedDisks` および `UseSharedImageGallery` パラメーターも有効にする必要があります。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk"
Value="true" />

</CustomProperties>'
```

エフェメラルディスクに関する重要な考慮事項

`New-ProvScheme` を使用してエフェメラル OS ディスクをプロビジョニングするには、次の制約を考慮してください。

- カタログに使用される VM サイズは、エフェメラル OS ディスクをサポートしている必要があります。
- VM サイズに関連付けられているキャッシュまたは一時ディスクのサイズは、OS ディスクのサイズ以上である必要があります。
- 一時ディスクのサイズは、キャッシュディスクのサイズよりも大きくする必要があります。

以下の際にもこれらの問題を考慮してください:

- プロビジョニングスキームを作成する際。
- プロビジョニングスキームを変更する際。
- イメージを更新する際。

Azure専用ホスト

MCSを使用して、Azure専用ホストにVMをプロビジョニングできます。Azure専用ホストにVMをプロビジョニングする前に:

- ホストグループを作成します。
- そのホストグループにホストを作成します。
- カタログと仮想マシンを作成するために、十分なホスト容量が予約されていることを確認してください。

次のPowerShellスクリプトを使用して、ホストテナンシーが定義されたマシンのカタログを作成できます。

```
New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <Property xsi:type="StringProperty" Name="HostGroupId"
Value="myResourceGroup/myHostGroup" />

 ...other Custom Properties...

 </CustomProperties>
```

MCSを使用してAzure専用ホストに仮想マシンをプロビジョニングする場合、以下を考慮してください。

- *専用ホスト*はカタログのプロパティであり、カタログが作成されると変更できません。専用テナンシーは現在 Azure ではサポートされていません。
- `HostGroupId` パラメータを使用する場合、ホスティングユニットのリージョンに、事前に構成された Azure ホストグループが必要です。
- Azure の自動配置が必要です。この機能は、ホストグループに関連付けられたサブスクリプションをオンボードする要求を行います。詳細については、VM Scale Set on Azure Dedicated Hosts - Public Preview を参照してください。自動配置が有効になっていない場合、MCS はカタログ作成中にエラーをスローします。

Azure Compute Galleryイメージを使用してマシンカタログを作成または更新する

マシンカタログの作成に使用するイメージを選択する際、Azure Compute Gallery で作成したイメージを選択できます。

これらのイメージを表示するには、以下を行う必要があります。

1. Citrix Virtual Apps and Desktops サイトを構成する。
2. Azure Resource Manager に接続する。

3. Azure portal で、リソースグループを作成します。詳細については、「ポータルを使用して Azure Compute Gallery を作成する」を参照してください。
4. リソースグループ内で、Azure Compute Gallery を作成します。
5. Azure Compute Gallery 内で、イメージ定義を作成します。
6. イメージ定義内で、イメージバージョンを作成します。

Azure Compute Gallery のイメージを使用してマシンカタログを作成または更新するには、次の PowerShell コマンドを使用します。

1. PowerShell ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group")
```

4. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group\sharedImageGallery.sharedimagegallery")
```

5. 1つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group\sharedImageGallery.sharedimagegallery\sigtestimage.imagedefinitio
n")
```

6. 次の要素を使用してMCSカタログを作成および更新します。
   - リソースグループ
   - ギャラリー
   - ギャラリーイメージ定義
   - ギャラリーイメージバージョン

Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/ を参照してください。

共有イメージギャラリーの構成

`New-ProvScheme` コマンドを使用して、共有イメージギャラリーをサポートするプロビジョニングスキームを作成します。`Set-ProvScheme` コマンドを使用して、プロビジョニングスキームのこの機能を有効または無効にし、レプリカ比率とレプリカの最大値を変更します。

Shared Image Gallery 機能をサポートするために、プロビジョニングスキームに3つのカスタムプロパティが追加されました。

`UseSharedImageGallery`

- 公開されたイメージを保存するために共有イメージギャラリーを使用するかどうかを定義します。**True** に設定されている場合、イメージは共有イメージギャラリーイメージとして保存され、それ以外の場合はスナップショットとして保存されます。
- 有効な値は **True** と **False** です。
- プロパティが定義されていない場合、デフォルト値は **False** です。

`SharedImageGalleryReplicaRatio`

- マシンとギャラリーイメージバージョンレプリカの比率を定義します。
- 有効な値は0より大きい整数です。
- プロパティが定義されていない場合、デフォルト値が使用されます。永続OSディスクのデフォルト値は1000、非永続OSディスクのデフォルト値は40です。

`SharedImageGalleryReplicaMaximum`

- 各ギャラリーイメージバージョンに対するレプリカの最大数を定義します。
- プロパティが定義されていない場合、デフォルト値は100です。
- プロパティが定義されていない場合、デフォルト値は100です。

> **ヒント:**

> Shared Image Galleryを使用してMCSプロビジョニング済みカタログの公開イメージを保存する場合、MCSはカタログ内のマシンの数、レプリカ比率、およびレプリカの最大値に基づいてギャラリーイメージバージョンのレプリカ数を設定します。レプリカ数は、カタログ内

> のマシンの数をレプリカ比率で割って（最も近い整数に切り上げて）、その値を最大レプリカ数で制限することによって計算されます。たとえば、レプリカ比率が20、最大値が5の場合、0〜20台のマシンには1つのレプリカが作成され、21〜40台には2つのレプリカ、41〜60台には3つのレプリカ、61〜80台には4つのレプリカ、81台以上には5つのレプリカが作成されます。

ユースケース：Shared Image Galleryのレプリカ比率とレプリカ最大値の更新

既存のマシンカタログはShared Image Galleryを使用しています。`Set-ProvScheme`コマンドを使用して、カタログ内のすべての既存マシンおよび将来のマシンのカスタムプロパティを更新します。

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

ユースケース：スナップショットカタログをShared Image Galleryカタログに変換する

このユースケースの場合：

1. `UseSharedImageGallery`フラグを**True**に設定して`Set-ProvScheme`を実行します。オプションで`SharedImageGalleryReplicaRatio`および`SharedImageGalleryReplicaMaximum`プロパティを含めます。
2. カタログを更新します。
3. マシンをパワーサイクルして、強制的に更新します。

例：

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
```

```
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

ヒント：

パラメーター `SharedImageGalleryReplicaRatio` と `SharedImageGalleryReplicaMaximum` は必須ではありません。`Set-ProvScheme` コマンドが完了しても、共有イメージギャラリーのイメージはまだ作成されていません。カタログがギャラリーを使用するように構成されると、次回のカタログ更新操作で公開されたイメージがギャラリーに保存されます。カタログ更新コマンドは、ギャラリー、ギャラリーイメージ、およびイメージバージョンを作成します。マシンを再起動すると更新され、必要に応じてレプリカ数が更新されます。その時点から、既存のすべての非永続マシンは共有イメージギャラリーのイメージを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはそのイメージを使用して作成されます。古いスナップショットは数時間以内に自動的にクリーンアップされます。

ユースケース：共有イメージギャラリーカタログをスナップショットカタログに変換する

このユースケースの場合：

1. `UseSharedImageGallery` フラグを **False** に設定するか、未定義のままにして `Set-ProvScheme` を実行します。
2. カタログを更新します。
3. マシンを再起動して更新を強制します。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
```

```
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

ヒント:

パラメーター `SharedImageGalleryReplicaRatio` と `SharedImageGalleryReplicaMaximum` は必須ではありません。`Set-ProvScheme` コマンドが完了しても、共有イメージギャラリーのイメージはまだ作成されていません。カタログがギャラリーを使用するように構成されると、次回のカタログ更新操作で公開されたイメージがギャラリーに保存されます。カタログ更新コマンドは、ギャラリー、ギャラリーイメージ、およびイメージバージョンを作成します。マシンを再起動すると更新され、必要に応じてレプリカ数が更新されます。その時点から、既存のすべての非永続マシンは共有イメージギャラリーのイメージを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはそのイメージを使用して作成されます。古いスナップショットは数時間以内に自動的にクリーンアップされます。

ユースケース: 共有イメージギャラリーカタログをスナップショットカタログに変換する

このユースケースの場合：

1. `UseSharedImageGallery` フラグを **False** に設定するか、未定義のままにして `Set-ProvScheme` を実行します。
2. カタログを更新します。
3. マシンをパワーサイクルして、強制的に更新します。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
```

ヒント:

スナップショットから共有イメージギャラリーカタログへの更新とは異なり、各マシンのカスタムデータは新しいカスタムプロパティを反映するようにまだ更新されていません。元の共有イメージギャラリーのカスタムプロパティを表示するには、次のコマンドを実行します: `Get-ProvVm -ProvisioningSchemeName catalog-name`。`Set-ProvScheme` コマンドが完了しても、イメージスナップショットはまだ作成されていません。カタログがギャラリーを使用しないように構成されると、次回のカタログ更新操作で公開されたイメージがスナップショットとして保存されます。その時点から、既存のすべての非永続マシンはスナップショットを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはスナップショットから作成されます。マシンを再起動すると更新され、その時点でカスタムマシンデータが更新され、`UseSharedImageGallery` が **False** に設定されていることが反映されます。古い共有イメージギャラリーのアセット（ギャラリー、イメージ、バージョン）は数時間以内に自動的にクリーンアップされます。

指定された可用性ゾーンにマシンをプロビジョニングする

Azure環境では、特定の可用性ゾーンにマシンをプロビジョニングできます。これはPowerShellを使用して実現できます。

注:

ゾーンが指定されていない場合、MCSはAzureにリージョン内にマシンを配置させます。複数のゾーンが指定されている場合、MCSはそれらのゾーンにマシンをランダムに分散します。

PowerShellによる可用性ゾーンの構成

PowerShell を使用して、`Get-Item` を使用して提供インベントリ項目を表示できます。たとえば、*米国東部リージョン* `Standard_B1ls` サービス提供を表示するには、次のようにします。

```
$serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-
name\East US.region\serviceoffering.folder\Standard_B1ls.serviceoffering"
```

ゾーンを表示するには、項目に `AdditionalData` パラメーターを使用します。

`$serviceOffering.AdditionalData`

可用性ゾーンが指定されていない場合、マシンのプロビジョニング方法に変更はありません。

PowerShell を使用してアベイラビリティゾーンを構成するには、`New-ProvScheme` 操作で利用できる **Zones** カスタムプロパティを使用します。**Zones** プロパティは、マシンをプロビジョニングするアベイラビリティゾーンのリストを定義します。これらのゾーンには、1つ以上のアベイラビリティゾーンを含めることができます。たとえば、ゾーン 1 および 3 の場合は `<Property xsi:type="StringProperty" Name="Zones" Value="1, 3"/>` です。

プロビジョニングスキームのゾーンを更新するには、`Set-ProvScheme`コマンドを使用します。

無効なゾーンが指定された場合、プロビジョニングスキームは更新されず、無効なコマンドを修正する方法を示すエラーメッセージが表示されます。

> **ヒント:**
>
> 無効なカスタムプロパティを指定すると、プロビジョニングスキームは更新されず、関連するエラーメッセージが表示されます。

ストレージの種類

MCS を使用する Azure 環境の仮想マシンには、異なるストレージの種類を選択します。ターゲット VM の場合、MCS は以下をサポートします。

- OSディスク: プレミアムSSD、SSD、またはHDD
- ライトバックキャッシュディスク: プレミアムSSD、SSD、またはHDD

これらのストレージの種類を使用する場合は、次の点を考慮してください。

- 選択したストレージの種類をVMがサポートしていることを確認してください。
- 構成でAzureエフェメラルディスクを使用している場合、ライトバックキャッシュディスク設定のオプションは表示されません。

> **ヒント:**
>
> `StorageType` はOSタイプとストレージアカウント用に構成されます。`WBCDiskStorageType` はライトバックキャッシュストレージタイプ用に構成されます。通常のカタログには `StorageType` が必要です。`WBCDiskStorageType` が構成されていない場合、`StorageType` が `WBCDiskStorageType` のデフォルトとして使用されます。

> WBCDiskStorageType が構成されていない場合、StorageType が WBCDiskStorageType のデフォルトとして使用されます。

ストレージの種類を構成する

VMのストレージタイプを構成するには、`New-ProvScheme` の `StorageType` パラメーターを使用します。`StorageType` パラメーターの値をサポートされているストレージタイプのいずれかに設定します。

以下は、プロビジョニングスキームにおける `CustomProperties` パラメーターの設定例です。

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>'
```

ゾーン冗長ストレージを有効にする

カタログ作成時にゾーン冗長ストレージを選択できます。これにより、Azureマネージドディスクが複数の可用性ゾーン間で同期的にレプリケートされ、あるゾーンでの障害発生時に他のゾーンの冗長性を利用して回復できるようになります。

ストレージタイプのカスタムプロパティで **Premium_ZRS** および **StandardSSD_ZRS** を指定できます。ZRSストレージは、既存のカスタムプロパティを使用するか、**MachineProfile** テンプレートを介して設定できます。ZRSストレージは、`-StartsNow` および `-DurationInMinutes -1` パラメーターを持つ `Set-ProvVMUpdateTimeWindow` コマンドでもサポートされており、既存のマシンをLRSからZRSストレージに変更できます。

制限事項:

- マネージドディスクのみをサポート
- プレミアムおよび標準ソリッドステートドライブ（SSD）のみをサポート
- `StorageTypeAtShutdown` ではサポートされていません

- 特定のリージョンでのみ利用可能です。
- 大規模にZRSディスクを作成すると、Azureのパフォーマンスが低下します。そのため、最初の電源投入時には、マシンを小規模なバッチ（一度に300台未満）で起動してください。

ゾーン冗長ストレージをディスクストレージタイプとして設定する

ゾーン冗長ストレージは、最初のカタログ作成時に選択することも、既存のカタログでストレージタイプを更新することもできます。

POWERSHELLコマンドを使用してゾーン冗長ストレージを選択する

`New-ProvScheme` PowerShellコマンドを使用してAzureで新しいカタログを作成する場合、`StorageAccountType` の値として `Standard_ZRS` を使用します。 例:

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_ZRS" />
```

この値を設定すると、それが適切に使用できるかどうかを判断する動的APIによって検証されます。ZRSの使用がカタログに対して有効でない場合、以下の例外が発生する可能性があります。

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: StorageTypeAtShutdownカスタムプロパティはZRSストレージでは使用できません。
- **StorageAccountTypeNotSupportedInRegion**: この例外は、ZRSをサポートしていないAzureリージョンでZRSストレージを使用しようとすると発生します。
- **ZrsRequiresManagedDisks**: ゾーン冗長ストレージはマネージドディスクでのみ使用できます。

以下のカスタムプロパティを使用して、ディスクストレージタイプを設定できます。

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

注:

カタログ作成時、カスタムプロパティが設定されていない場合は、マシンプロファイルのOSディスク `StorageType` が使用されます。

マシンプロファイルからVMとNICの診断設定をキャプチャする

マシンカタログの作成時、既存のマシンカタログの更新時、および既存のVMの更新時に、マシンプロファイルからVMとNICの診断設定をキャプチャできます。

VMまたはテンプレート仕様をマシンプロファイルのソースとして作成できます。

主な手順

1. Azureで必要なIDを設定します。これらのIDはテンプレート仕様で指定する必要があります。
    - ストレージアカウント
    - Log Analyticsワークスペース
    - 標準ティアの価格設定のEvent Hub名前空間
2. マシンプロファイルソースを作成します。
3. 新しいマシンカタログを作成するか、既存のカタログを更新するか、既存のVMを更新します。

Azureで必要なIDを設定する

Azureで次のいずれかを設定します。

- ストレージアカウント
- ログ分析ワークスペース
- Standardティアの価格設定を持つイベントハブ名前空間

ストレージアカウントを設定する

Azureで標準ストレージアカウントを作成します。テンプレート仕様では、ストレージアカウントの完全なresourceIdを`storageAccountId`として指定します。

VM がストレージアカウントにデータをログするように設定されると、データは`insights-metrics-pt1m`コンテナの下にあります。

ログ分析ワークスペースを設定する

ログ分析ワークスペースを作成します。テンプレート仕様では、ログ分析ワークスペースの完全なresourceIdをworkspaceIdとして指定します。

VM がワークスペースにデータをログするように設定されると、Azure の でデータをクエリできます。Azure の で次のコマンドを実行すると、リソースによってログに記録されたすべてのメトリックの数を表示できます。

```
AzureMetrics | summarize Count=count() by ResourceId
```

イベントハブを設定する

Azureポータルでイベントハブを設定するには、次の手順を実行します。

1. 標準ティアの価格設定でイベントハブ名前空間を作成します。
2. 名前空間の下にイベントハブを作成します。
3. イベントハブの下にある に移動します。Avro 出力タイプでキャプチャするには、トグルをオンにします。
4. ログをキャプチャするために、既存のストレージアカウントに新しいコンテナを作成します。
5. テンプレートスペックで、次の形式で`eventHubAuthorizationRuleId`を指定します: `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. イベントハブの名前を指定します。

VMがイベントハブにデータをログするように設定されると、データは構成されたストレージコンテナにキャプチャされます。

マシンプロファイルソースを作成する

VMまたはテンプレート仕様をマシンプロファイルソースとして作成できます。

診断設定を含むVMベースのマシンプロファイルを作成する

VMをマシンプロファイルとして作成する場合は、まずテンプレートVM自体に診断設定をセットアップします。詳細な手順については、MicrosoftドキュメントのAzure Monitorの診断設定を参照してください。

次のコマンドを実行して、VMまたはNICに関連付けられた診断設定があることを確認できます。

```
az monitor diagnostic-settings list --resource-group matspo --resource
matspo-tog-cc2659 --resource-type microsoft.network/networkInterfaces
```

```
az monitor diagnostic-settings list --resource-group matspo --resource
matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
```

診断設定を含むテンプレートスペックベースのマシンプロファイルを作成する

診断設定が有効になっているVMを使用し、それをARMテンプレート仕様にエクスポートする場合、これらの設定はテンプレートに自動的に含まれません。ARMテンプレート内で診断設定を手動で追加または変更する必要があります。

ただし、VMをマシンプロファイルとして使用する場合、MCSは、重要な診断設定が正確にキャプチャされ、MCSカタログ内のリソースに適用されることを保証します。

1. VMとNICを定義する標準テンプレート仕様を作成します。
2. 仕様に従って診断設定を展開するための追加リソースを追加します: Microsoft.Insights diagnosticSettings。スコープについては、テンプレート内のVMまたはNICを部分IDを持つ名前で参照します。たとえば、テンプレート仕様でtest-VMという名前のVMにアタッチされた診断設定を作成する場合、スコープは次のように指定します。

   ```
   "scope": "microsoft.compute/virtualMachines/test-VM",
   ```

3. テンプレート仕様をマシンプロファイルソースとして使用します。

診断設定を含むカタログを作成または更新する

マシンプロファイルソースを作成した後、`New-ProvScheme`コマンドを使用してマシンカタログを作成したり、`Set-ProvScheme`コマンドを使用して既存のマシンカタログを更新したり、`Request-ProvVMUpdate`コマンドを使用して既存のVMを更新したりできます。

ページファイルの場所の決定

ページファイルの場所は、次のシナリオに従って決定されます。

注:

デフォルトのページファイルの場所は OS ディスクです。

シナリオ	場所
ページファイルの設定がカスタムプロパティで指定されている	カスタムプロパティで指定されているとおり
エフェメラルOSディスクまたはハイバネーションが有効になっている	OSディスク
VMに一時ディスクがある	一時ディスク
MCS I/O が有効になっています	WBCディスク

ページファイル設定のシナリオ

以下の表は、イメージ準備中およびプロビジョニングスキーム更新中に発生しうるページファイル設定のシナリオの一部を示しています。

期間	シナリオ	結果
イメージ準備	プロビジョニングスキームで指定したVMサイズには一時ディスクがないにもかかわらず、ソースイメージのページファイルを一時ディスクに設定しました	ページファイルはOSに配置されます
イメージ準備	プロビジョニングスキームで指定したVMサイズには一時ディスクがあるにもかかわらず、ソースイメージのページファイルをOSディスクに設定しました	ページファイルは一時ディスクに配置されます
イメージ準備	ソースイメージのページファイルを一時ディスクに設定し、プロビジョニングスキームでエフェメラルOSディスクを有効にします	ページファイルはOSディスクに配置されます
プロビジョニングスキームの更新	VDAバージョンが2311より古い場合に、プロビジョニングスキームを更新しようとします	警告付きでページファイル設定を変更します
プロビジョニングスキームの更新	VDAバージョンが2311以降の場合にプロビジョニングスキームの更新を試行します	(#page-file-location-determination) に従ってページファイルの場所を決定します

ページファイル設定の指定

PowerShellコマンドを使用して、場所やサイズを含むページファイル設定を指定できます。これにより、ページファイルの場所の決定に従ってMCSによって決定されたページファイル設定が上書きされます。これは、マシンカタログ作成中に次の`New-ProvScheme`コマンドを実行することで行えます。

重要な考慮事項

カタログ作成を進める前に、以下を考慮してください。

- すべてのカスタムプロパティ（'PageFileDiskDriveLetterOverride'、'InitialPageFileSizeInMB'、'MaxPageFileSizeInMB'）を `New-ProvScheme` コマンドで指定するか、または何も指定しないでください。
- この機能はCitrix Studioではサポートされていません。
- 初期ページファイルサイズは16 MBから16777216 MBの間である必要があります。
- 最大ページファイルサイズは、初期ページファイルサイズ以上で、かつ16777216 MB未満である必要があります。
- 初期ページファイルサイズと最大ページファイルサイズの両方を同時にゼロに設定できます。

> **注:**
>
> マスターイメージを更新することなく、既存のカタログに新しく追加されたVMのページファイル設定を変更できます。ページファイル設定を変更するには、VDAバージョン2311以降が必要です。PowerShellコマンドを使用してページファイル設定を変更できます。詳細については、(#modify-page-file-settings) を参照してください。

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "zijinnet" `

-IdentityPoolName "PageFileSettingExample" `

-ProvisioningSchemeName "PageFileSettingExample" `

-InitialBatchSizeHint 1 `

-MasterImageVM "XDHyp:\HostingUnits\zijinnet\image.folder\neal-zijincloud-
resources.resourcegroup\CustomWin10VDA_OsDisk_1_9473d7c8a6174b2c8284c7d3ef
eea88f.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\zijinnet\
\virtualprivatecloud.folder\\East US.region\\virtualprivatecloud.folder\
\neal-zijincloud-resources.resourcegroup\\neal-zijincloud-resources-
vnet.virtualprivatecloud\\default.network"} `
```

```
-ServiceOffering "XDHyp:\\HostingUnits\\zijinnet\\serviceoffering.folder\
\Standard_B2ms.serviceoffering" `

-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride"
Value="d"/> `

<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
Value="2048"/> `

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB"
Value="8196"/> `

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `

</CustomProperties>'
```

ページファイル設定の変更

マスターイメージを更新することなく、既存のカタログに新しく追加されたVMのページファイル設定を変更できます。現在、この機能はAzure環境のみに適用されます。

ページファイル設定を変更するには、VDAバージョン2311以降が必要です。PowerShellコマンドを使用してページファイル設定を変更できます。

Azure環境で変更できるページファイル設定は次のとおりです。

- `PageFileDiskDriveLetterOverride`
- `InitialPageFileSizeInMB`
- `MaxPageFileSizeInMB`

既存のカタログのページファイル設定を変更する

既存のマシンカタログのページファイル設定を変更するには、`Set-ProvScheme`コマンドを実行します。この場合、更新はカタログに追加された新しいVMにのみ適用されます。例:

```
Set-ProvScheme -ProvisioningSchemeName $schemeName -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="StandardSSD_LRS" />

<Property xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride"
Value="D" />

<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
Value="2048" />

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB"
Value="8196" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property  xsi:type="StringProperty" Name="Zones" Value="1" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="neal-
test-group1" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

注:

ライトバックキャッシュを有効にして、PowerShell コマンドを使用して`PageFileDiskDriveLetterOverride`を`C:`に設定しようとすると、MCS IO ドライバー

> はページファイルを自動的に正しいディスクドライブにリダイレクトし、`C:` にはリダイレクトしません。

Azure Spot VMを使用してカタログを作成する

Azure Spot VMを使用すると、Azureの未使用のコンピューティング能力を大幅なコスト削減で活用できます。ただし、Azure Spot VMを割り当てる能力は、現在の容量と価格設定に依存します。そのため、Azureは退去ポリシーに従って、実行中のVMを退去させたり、VMの作成に失敗したり、VMの電源投入に失敗したりする可能性があります。したがって、Azure Spot VMは一部の重要でないアプリケーションやデスクトップに適しています。詳細については、Azure Spot Virtual Machinesの使用を参照してください。

制限事項

- すべてのVMサイズがAzure Spot VMでサポートされているわけではありません。詳細については、制限事項を参照してください。

  PowerShellコマンドを実行して、VMサイズがSpot VMをサポートしているかどうかを確認できます。VMサイズがSpot VMをサポートしている場合、`SupportsSpotVM` は**True**です。

  ```
  (Get-Item "XDHyp:\HostingUnits\azure-res-
  conn2\serviceoffering.folder\Standard_D2ds_v4.serviceoffering").
  AdditionalData
  ```

- 現在、Azure Spot VMは休止状態をサポートしていません。

要件

Azure Spot VMカタログのマシンプロファイルソース（VMまたはテンプレート仕様）を作成する際、(VMを使用している場合は) Azure Spot Instanceを選択するか、(テンプレート仕様を使用している場合は) `priority` を `Spot` として設定する必要があります。

Azure Spot VMを使用してカタログを作成する手順

1. マシンプロファイルソース（VMまたは起動テンプレート）を作成します。

   - Azureポータルを使用してVMを作成するには、Azureポータルを使用してAzure Spot Virtual Machinesを展開するを参照してください。
   - テンプレート仕様を作成するには、テンプレート仕様の**resources > type: Microsoft.Compute/virtualMachines > properties**の下に次のプロパティを追加します。例：

```
"priority": "Spot",

"evictionPolicy": "Deallocate",

"billingProfile": {

"maxPrice": 0.01

}
```

注:

- 削除ポリシーは**Deallocate**または**Delete**にすることができます。
  - 非永続VMの場合、MCSは常に削除ポリシーを**Delete**に設定します。VMが削除された場合、非永続ディスク（例：OSディスク）とともに削除されます。永続ディスク（例：IDディスク）は削除されません。ただし、カタログタイプが永続であるか、`PersistOsDisk`カスタムプロパティがTrueに設定されている場合、OSディスクは永続です。同様に、`PersistWbc`カスタムプロパティが**True**に設定されている場合、WBCディスクは永続です。
  - 永続VMの場合、MCSは常に削除ポリシーをDeallocateに設定します。VMが削除された場合、割り当て解除されます。ディスクに変更は加えられません。
- 最大価格は、1時間あたりに支払ってもよい価格です。**容量のみ**を使用している場合、これは**-1**です。最大価格は、null、-1、またはゼロより大きい小数のみです。詳細については、価格を参照してください。

2. マシンプロファイルがAzure Spot VM対応であるかどうかを確認するには、次のPowerShellコマンドを実行します。`SpotEnabled`パラメーターが**True**で、`SpotEvictionPolicy`が**Deallocate**または**Delete**に設定されている場合、マシンプロファイルはAzure Spot VM対応です。例：

   - マシンプロファイルのソースがVMの場合、次のコマンドを実行します。

```
(Get-Item "XDHyp:\HostingUnits\azure-res-
conn2\machineprofile.folder\fifthcolumn.resourcegroup\kb-spot-
delete.vm"). AdditionalData
```

- マシンプロファイルのソースがテンプレート仕様の場合、次のコマンドを実行します。

```
(Get-Item "XDHyp:\HostingUnits\azure-res-
conn2\machineprofile.folder\fifthcolumn.resourcegroup\fc-aeh-
templatespec.templatespec\14.0.0-spot-
delete.templatespecversion").AdditionalData
```

3. `New-ProvScheme` PowerShellコマンドを使用して、マシンプロファイルでマシンカタログを作成します。

`Set-ProvScheme`コマンドを使用してカタログを更新できます。既存のVMをPowerShellコマンド`Set-ProvVmUpdateTimeWindow`を使用して更新することもできます。マシンプロファイルは次回の電源投入時に更新されます。

実行中のAzure Spot VMでの強制排除

コンピューティング容量が利用できない場合、または時間あたりの価格が設定された最大価格よりも高い場合、Azureは実行中のSpot VMを強制排除します。デフォルトでは、強制排除の通知はされません。VMは単にフリーズし、強制排除されます。Microsoftは、強制排除を監視するためにScheduled Eventsを使用することを推奨しています。強制排除を継続的に監視するを参照してください。また、VM内からスクリプトを実行して、強制排除前に通知を受け取ることもできます。例えば、MicrosoftはPythonでポーリングスクリプトScheduledEvents.csを提供しています。

トラブルシューティング

- プロビジョニングされたVMのcustomMachineDataで、`Get-ProvVM`コマンドを使用してSpot VMのプロパティを確認できます。優先度フィールドが**Spot**に設定されている場合、Spotが使用されています。
- Azure PortalでVMがSpotを使用しているかどうかを確認できます。

  a. Azure PortalでVMを見つけます。

  b. **概要**ページに移動します。

  c. 下にスクロールして、**Azure Spot**セクションを見つけます。

    - Spotが使用されていない場合、このフィールドは空です。
    - Spotが使用されている場合、**Azure Spot**および**Azure Spot eviction policy**フィールドが設定されます。

1. 構成ページで、VMの課金プロファイルまたは1時間あたりの最大価格を確認できます。

バックアップVMサイズの構成

パブリッククラウドでは、特定のVMサイズで容量が不足することがあります。また、Azure Spot VMを使用している場合、Azureの容量ニーズに基づいてVMはいつでも強制排除されます。Azureの容量不足やSpot VMの電源投入失敗といった場合、MCSはバックアップVMサイズにフォールバックします。MCSマシンカタログの作成または更新時に、カスタムプロパティ `BackupVmConfiguration` を使用してバックアップVMサイズのリストを提供できます。MCSは、リストで指定された順序でバックアップVMサイズにフォールバックしようとします。

MCSがVMに特定のバックアップ構成を使用する場合、次回のシャットダウンまでその構成を使い続けます。次回の電源投入時には、MCSはプライマリVM構成を起動しようとします。失敗した場合、MCSはリストに従ってバックアップVMサイズ構成を再度起動しようとします。

この機能は以下をサポートします。

- マシンプロファイルを使用するカタログ
- 永続的および非永続的なMCSマシンカタログ
- 現在のAzure環境

重要な考慮事項

- リストには複数のバックアップVMサイズを指定できます。
- リストは一意である必要があります。
- リスト内の各VMにインスタンスタイププロパティを追加できます。タイプは**Spot**または**Regular**のいずれかです。タイプが指定されていない場合、MCSはVMを**Regular**と見なします。
- 既存のカタログのバックアップVMサイズリストは、`Set-ProvScheme` PowerShellコマンドを使用して変更できます。
- カタログに関連付けられたプロビジョニングスキームから作成された既存のVMは、`Set-ProvVMUpdateTimeWindow` コマンドを使用して更新できます。
- 選択した数の既存のMCS VMに対して、`Set-ProvVM` コマンドを使用してバックアップVMサイズリストを構成できます。ただし、更新を適用するには、`Set-ProvVMUpdateTimeWindow` を使用してVMの更新時間枠を設定し、その時間枠内でVMを起動します。VMで `Set-ProvVm` コマンドが使用された場合、プロビジョニングスキームのリストが後で更新されても、VMはその特定のVMに設定されたバックアップVMサイズリストを引き続き使用します。VMにプロビジョニングスキームのバックアップリストを使用させるには、`Set-ProvVM` を `-RevertToProvSchemeConfiguration` とともに使用できます。

バックアップVMサイズでカタログを作成する

> **注:**
>
> Studio UIがフリーズする問題に対処するには、PowerShellコマンドの実行中にすべてのシングルクォートを`"`に置き換えてください。

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために、`asnp citrix*`を実行します。
3. ブローカーカタログを作成します。このカタログには、これから作成されるマシンが投入されます。
4. IDプールを作成します。これは、作成されるマシン用に作成されたADアカウントのコンテナとなります。
5. マシンプロファイルを使用してプロビジョニングスキームを作成します。バックアップ構成の構成方法を参照してください。
6. プロビジョニングスキームの一意のIDでBrokerCatalogを更新します。
7. VMを作成し、カタログに追加します。

既存のカタログを更新する

`Set-ProvScheme`コマンドを使用してプロビジョニングスキームを更新できます。「バックアップ構成を構成する方法」を参照してください。

既存のVMを更新する

`Set-ProvVMUpdateTimeWindow` PowerShellコマンドを使用して、カタログ内の既存のVMを更新できます。このコマンドは、指定された時間枠内で次回の電源投入時に、カタログに関連付けられたプロビジョニングスキームから作成されたVMを更新します。例：

- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartTimeInUTC "3/12/2022 3am" -DurationInMinutes 60`
- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartsNow -DurationInMinutes 60`

> **注:**

`StartsNow` はスケジュールされた開始時間を示します。`DurationInMinutes` はスケジュールの時間枠です。

選択した数の既存のMCS VMのバックアップVMサイズリストは、`Set-ProvVM`コマンドを使用して構成できます。ただし、更新を適用するには、`Set-ProvVMUpdateTimeWindow`を使用してVMの更新時間枠を設定し、その時間枠内でVMを起動します。例：

1. 選択した既存のMCS VMのバックアップVMサイズリストを構成するには、`Set-ProvVM`コマンドを実行します。例：

```
Set-ProvVM -ProvisioningSchemeName "name" -VMName "Vm-001"

-CustomProperties

"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Server`"/>

<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
Value=`"true`"/>

<Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration`"
Value=`"[{&amp;quot;ServiceOffering&amp;quot;: &amp;quot;Standard_D2as_v4&amp;quot;,
&amp;quot;Type&amp;quot;: &amp;quot;Spot&amp;quot;}, {&amp;quot;ServiceOffering&amp;quot;:
&amp;quot;Standard_D2s_v3&amp;quot;, &amp;quot;Type&amp;quot;: &amp;quot;Regular&amp;quot;},
{&amp;quot;ServiceOffering&amp;quot;: &amp;quot;Standard_D2s_v3&amp;quot;,
&amp;quot;Type&amp;quot;: &amp;quot;Spot&amp;quot;}]`"/>

</CustomProperties>"
```

2. 更新を適用するには、`Set-ProvVMUpdateTimeWindow`コマンドを実行します。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartsNow -DurationInMinutes 60
```

すべてのリソースにタグをコピーする

マシンプロファイルで指定されたタグを、新しいVMまたはマシンカタログ内の既存のVMの複数のNICやディスク（OSディスク、IDディスク、ライトバックキャッシュディスク）などのすべてのリソースにコピーできます。マシンプロファイルのソースは、VMまたはARMテンプレート仕様にすることができます。

注:

リソースにタグを保持するには、タグに関するポリシーを追加するか（タグコンプライアンスのポリシー定義を割り当てる を参照）、マシンプロファイルソースにタグを追加する必要があります。

前提条件

そのVMのVM、ディスク、NICにタグを付けるには、マシンプロファイルソース（VMまたはARMテンプレート仕様）を作成します。

- VMをマシンプロファイルの入力として使用したい場合は、AzureポータルでVMとすべてのリソースにタグを適用します。Azureポータルでタグを適用する を参照してください。
- ARMテンプレート仕様をマシンプロファイルの入力として使用したい場合は、各リソースの下に次のタグブロックを追加します。

```
 "tags": {

"TagC": "Value3"

},
```

注:

テンプレート仕様には、最大1つのディスクと少なくとも1つのNICを含めることができます。

新しいマシンカタログ内のVMのリソースにタグをコピーする

1. VMまたはARMテンプレート仕様をマシンプロファイルの入力として使用して、非永続または永続カタログを作成します。
2. カタログにVMを追加して電源を入れます。マシンプロファイルで指定されたタグが、そのVMの対応するリソースにコピーされていることを確認する必要があります。

> **注:**
>
> マシンプロファイルで提供されるNICの数と、VMで使用するNICの数に不一致がある場合、エラーが発生します。

既存のVMのリソース上のタグを変更する

1. すべてのリソースにタグを付けたマシンプロファイルを作成します。
2. 既存のマシンカタログを、更新されたマシンプロファイルで更新します。例：

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName>
-MachineProfile <PathToYourMachineProfile>
```

3. 更新を適用したいVMの電源をオフにします。
4. VMのスケジュールされたアップデートを要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <YourCatalogName>  -
VMName machine1 -StartsNow -DurationInMinutes -1
```

5. VMの電源をオンにします。
6. マシンプロファイルで指定されたタグが、対応するリソースにコピーされていることを確認する必要があります。

> **注:**
>
> マシンプロファイルで提供されるNICの数と、`Set-ProvScheme`で提供されるNICの数に不一致がある場合、エラーが発生します。

事前フォーマットされたWBCディスクカタログを作成する

プロビジョニングされたマシンの起動パフォーマンスを向上させるために、事前フォーマットされたWBCディスクカタログを作成できます。この機能を実装するには、WBCが有効なAzureカタログを作成し、追加のカスタムプロパティ`PreformatWriteBackCache`を`True`として含めます。

既存のカタログは、`Set-ProvScheme`コマンドを使用してWBCディスクサイズを更新できます。

この機能は、MCSがマスタリングフェーズをプロビジョニングワークフロー全体から分離するイメージ管理ワークフローと互換性があります。イメージ管理の詳細については、イメージ管理を参照してください。

WBCを有効にし、`PreformatWriteBackCache`を`True`としてAzureカタログを作成する例:

```
$customProperties = @'

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="PreformatWriteBackCache"
Value="true" />

</CustomProperties>

'@



New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName "provisioningschemename" `

-HostingUnitName "hostingunitname" `

-IdentityPoolName "identitypoolnamename" `

-MasterImageVM "XDHyp:
\HostingUnits\AzureHostingUnit\image.folder\rg.resourcegroup\masterImage.m
anageddisk" `

-CustomProperties $customProperties `
```

```
-NetworkMapping $networkMapping `

-UseWriteBackCache `

-WriteBackCacheDiskSize 30
```

既存のカタログのWBCディスクキャッシュサイズを更新する例:

```
Set-ProvScheme -ProvisioningSchemeName provisioningschemename
-WriteBackCacheDiskSize 127
```

MCSプロビジョニングされたCitrix Provisioning™カタログのシャットダウン時にWBCディスクを削除する

AzureでMCSプロビジョニングされたCitrix Provisioningカタログを作成する際、WBCディスクを非永続的（`PersistWBC` を False に設定）にプロビジョニングできます。この構成により、AzureでMCSプロビジョニングされたCitrix ProvisioningカタログのVMをシャットダウンした後、ライトバックキャッシュ（WBC）ディスクを削除するのに役立ちます。

条件:

この機能が動作するためには、カスタムプロパティ`PreformatWriteBackCache`を`True`として設定する必要があります。

`PersistWBC`を`False`として、`PreformatWriteBackCache`を`True`としてAzureカタログを作成する例:

```
$customProperties = @'

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PreformatWriteBackCache"
Value="true" />

</CustomProperties>

'@
```

```
New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName "provisioningschemename" `

-HostingUnitName "hostingunitname" `

-IdentityPoolName "identitypoolnamename" `

-MasterImageVM "XDHyp:
\HostingUnits\AzureHostingUnit\image.folder\rg.resourcegroup\masterImage.m
anageddisk" `

-CustomProperties $customProperties `

-NetworkMapping $networkMapping `

-UseWriteBackCache `

-WriteBackCacheDiskSize 30
```

既存のカタログを`Set-ProvScheme`コマンドを使用して更新し、`PersistWBC`カスタムプロパティを更新することもできます。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成に誘導します。
- 構成プロセス全体を確認するには、「インストールと構成」を参照してください。
- カタログを管理するには、「マシンカタログの管理」および「Microsoft Azureカタログの管理」を参照してください。

詳細情報

- 接続とリソースの作成および管理(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/connections.html)
- マイクロソフト アジュール リソースマネージャー への接続
- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create.html)

Microsoft System Center Virtual Machine Managerカタログを作成する

「マシンカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create.html)では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Microsoft System Center Virtual Machine Manager (VMM) 仮想化環境に固有の詳細を扱っています。

> **注:**
>
> VMMカタログを作成する前に、VMMへの接続の作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/connections/connection-mscvmm.html)を参照してください。

マスターVMを作成する

1. マスターVMにVDAをインストールし、パフォーマンスを向上させるためにデスクトップを最適化するオプションを選択します。
2. マスターVMのスナップショットを作成し、バックアップとして使用します。
3. 仮想デスクトップを作成します。

SMB 3ファイル共有上のMCS

VMストレージ用のSMB 3ファイル共有でMCSを使用して作成されたマシンカタログの場合、資格情報が次の要件を満たしていることを確認してください。これらの要件により、ControllerのHypervisor Communications Library（HCL）からの呼び出しがSMBストレージに正常に接続されます。

- VMMユーザーの資格情報には、SMBストレージへの完全な読み取り/書き込みアクセス権を含める必要があります。
- VMライフサイクルイベント中のストレージ仮想ディスク操作は、VMMユーザーの資格情報を使用してHyper-Vサーバー経由で実行されます。

SMBストレージを使用する場合は、Controllerから個々のHyper-Vマシンへの認証資格情報セキュリティサポートプロバイダー（CredSSP）を有効にします。このプロセスは、Windows Server 2012上のHyper-VとVMM 2012 SP1で使用します。詳細については、CTX137465を参照してください。

HCLは`CredSSP`を使用してHyper-Vマシンへの接続を開きます。この機能は、Kerberosで暗号化されたユーザー資格情報をHyper-Vマシンに渡します。リモートHyper-Vマシン上のセッションで

実行される**PowerShell**コマンドは、提供された資格情報で実行されます。この場合、VMMユーザーの資格情報が使用されるため、ストレージへの通信コマンドが正しく機能します。

次のタスクでは、HCLで生成され、SMB 3.0ストレージに対して動作するためにHyper-Vマシンに送信されるPowerShellスクリプトを使用します。

- **マスターイメージの統合**: マスターイメージはMCSプロビジョニングスキーム（マシンカタログ）を作成します。新しく作成されたディスクからVMを作成できるようにマスターVMをクローンしてフラット化します（そして元のマスターVMへの依存関係を削除します）。

  root\\virtualization\\v2 名前空間での ConvertVirtualHardDisk

  例:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)

$result
```

- **差分ディスクの作成**: マスターイメージを統合して生成されたマスターイメージから差分ディスクを作成します。その後、差分ディスクは新しいVMに接続されます。

  root\\virtualization\\v2 名前空間での CreateVirtualHardDisk

  例:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.CreateVirtualHardDisk($vhdastext);

$result
```

- **IDディスクのアップロード**: HCLはIDディスクをSMBストレージに直接アップロードできません。そのため、Hyper-VマシンがIDディスクをストレージにアップロードしてコピーする必要があります。Hyper-Vマシンはコントローラーからディスクを読み取ることができないため、HCLはまずHyper-Vマシンを介してIDディスクを次のようにコピーする必要があります。

  a. HCLは管理者共有を介してIDをHyper-Vマシンにアップロードします。

  b. Hyper-Vマシンは、PowerShellリモートセッションで実行されているPowerShellスクリプトを介して、ディスクをSMBストレージにコピーします。Hyper-Vマシン上にフォルダー

が作成され、そのフォルダーのアクセス許可はVMMユーザーのみにロックされます（リモートPowerShell接続を介して）。

c. HCLは管理者共有からファイルを削除します。

d. HCLがIDディスクのHyper-Vマシンへのアップロードを完了すると、リモートPowerShellセッションはIDディスクをSMBストレージにコピーします。その後、Hyper-Vマシンから削除します。

IDディスクフォルダーは、削除された場合でも再利用できるように再作成されます。

- **IDディスクのダウンロード**: アップロードと同様に、IDディスクはHyper-Vマシンを介してHCLに渡されます。以下のプロセスでは、Hyper-Vサーバー上にVMMユーザー権限のみを持つフォルダーが存在しない場合に作成します。

  a. Hyper-Vマシンは、PowerShellスクリプトを介してSMBストレージからローカルのHyper-Vストレージにディスクをコピーします。このスクリプトは、PowerShell V3リモートセッションで実行されます。

  b. HCL は、Hyper-V マシンの管理者共有からディスクをメモリに読み込みます。

  c. HCL は、管理者共有からファイルを削除します。

マシンプロファイルを使用してカタログを作成する

System Center Virtual Machine Manager (SCVMM) 環境では、マシンプロファイルを使用して MCS マシンカタログを作成および更新できます。vTPM を有効にできます。また、マシンプロファイル VM のカスタムタグをプロビジョニングされた VM に追加することもできます。

重要な考慮事項

- マスターイメージはスナップショットのみで、VM にはできません。
- マシンプロファイルのソースとして使用できるのは VM のみです。
- VTPM は Hyper-V コンソールから構成でき、SCVMM コンソールからは構成できません。
- マスターイメージで vTPM が有効になっている場合、マシンプロファイルソースで vTPM を有効にする必要があります。
- vTPM は第 2 世代のマシンでのみサポートされています。
- 個別に指定した場合、以下のパラメーターはマシンプロファイルでキャプチャされた値を上書きします。
  - VMCpuCount
  - VMMemoryMB
  - ディスクストレージ

- カスタムタグはマシンプロファイルからのみ継承され、マスターイメージからは継承されません。`CitrixProvisioningSchemeId` タグはデフォルトで VM に追加されます。`CitrixProvisioningSchemeId` タグを含めたくない場合は、ホスティングユニットの作成時に `-NoVmTagging` パラメーターを追加します。例:

```
New-Item -HypervisorConnectionName  $ConnectionName `

    -NetworkPath @($NetworkPath) `

    -Path @($HostingUnitPath) `

    -PersonalvDiskStoragePath @() `

    -RootPath $RootPath `

    -StoragePath @($StoragePath) `

    -NoVmTagging

    ```
```

- 既存のカタログは、`Set-ProvScheme`コマンドを使用して更新できます。

マシンプロファイルを使用してマシンカタログを作成する

1. マシンプロファイルのソースとなるVMを作成します。詳しくは、「VMMファブリックで仮想マシンをプロビジョニングする」を参照してください。**世代**は一度選択すると変更できません。SCVMMでは、次のことができます。
    - vTPMを有効にするには：
        a. VMを作成したら、Hyper-Vホストにログインし、**Hyper-Vマネージャー**でVMを見つけます。
        b. VMを右クリックし、**設定**に移動します。
        c. **セキュリティ**で、**トラステッドプラットフォームモジュールを有効にする**チェックボックスをオンにします。
2. **PowerShell**ウィンドウを開きます。
3. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
4. Brokerカタログを作成します。このカタログには、作成される予定のマシンが格納されます。
```

5. IDプールを作成します。これは、作成されるマシン用に作成されたADアカウントのコンテナになります。
6. マシンプロファイルを使用してプロビジョニングスキームを作成します。例：

```
New-ProvScheme -HostingUnitName "<hostingunit name>"

-IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1\<path
to the checkpoint/snapshot>"

-ProvisioningSchemeName "<catalogname>"  -MachineProfile "XDHyp:\<path
to the machine profile VM>"
```

7. プロビジョニングスキームの一意のIDでBrokerカタログを更新します。
8. カタログにVMを作成して追加します。

既存のカタログを更新する

Set-ProvSchemeコマンドを使用して、既存のカタログを更新できます。例：

```
Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile
"XDHyp:\<path to the machine profile VM>"
```

VMを削除する

カタログから VM を削除することを選択できますが、SCVMM から VM を削除することはできません。この場合、`CitrixProvisioningSchemeId` タグは VM からのみ削除されます。カスタムタグは VM から削除されません。Web Studio または PowerShell コマンドを使用して VM を削除できます。

WEB STUDIO を使用して VM を削除する

1. VMを選択して右クリックします。
2. **削除**」をクリックします。
3. **仮想マシンをカタログから削除しますが、仮想マシンは削除しません**を選択します。

POWERSHELLコマンドの使用

`ForgetVM` パラメーターを指定した `Remove-ProvVM`。詳細については、以下を参照してください。

- タグを削除する
- ハイパーバイザーアクセスなしでマシンを削除する

次のステップ

- これが最初に作成されたカタログである場合、Web Studio は デリバリーグループの作成 に誘導します
- 構成プロセス全体を確認するには、インストールと構成 を参照してください
- カタログを管理するには、マシンカタログの管理 および Microsoft System Center Virtual Machine Manager カタログの管理 を参照してください

詳細情報

- 接続とリソースを作成および管理する(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/connections.html)
- マイクロソフト システム センター バーチャル マシン マネージャーへの接続
- マシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create.html)

Nutanixカタログを作成する

「(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create.html)」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Nutanix仮想化環境に固有の詳細を扱っています。

> **注:**
>
> Nutanixカタログを作成する前に、Nutanixへの接続の作成を完了する必要があります。「(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/connections/connection-nutanix.html)」を参照してください。

Nutanixスナップショットを使用してマシンカタログを作成する

選択したスナップショットは、カタログ内のVMを作成するために使用されるテンプレートです。カタログを作成する前に、Nutanixでイメージとスナップショットを作成してください。詳細については、Nutanixのドキュメントを参照してください。

カタログ作成ウィザードで：

- **オペレーティングシステム**ページと**マシン管理**ページには、Nutanix固有の情報は含まれていません。
- **コンテナ**または**クラスターとコンテナ**ページはNutanix固有です。

Nutanix AHV XI をリソースとして使用してマシンを展開する場合、**Container** ページが表示されます。VMのIDディスクが配置されるコンテナを選択します。

Nutanix AHV Prism Central (PC) をリソースとして使用してマシンを展開する場合、**Cluster and Container** ページが表示されます。VMの展開に使用するクラスターを選択し、次にコンテナを選択します。

- **イメージ**ページで、イメージスナップショットを選択します。Citrix Virtual Apps and Desktopsで使用するには、Acropolisスナップショット名に「XD_」をプレフィックスとして付ける必要があります。必要に応じて、Acropolisコンソールを使用してスナップショットの名前を変更してください。スナップショットの名前を変更した場合は、カタログ作成ウィザードを再起動して、更新されたリストを表示してください。
- **Virtual Machines**ページで、仮想CPUの数とvCPUあたりのコア数を指定します。
- **ネットワークカード**ページで、関連するネットワークをフィルター処理するためのNICタイプを選択します。NICタイプは**VLAN**と**OVERLAY**の2種類があります。マスターイメージに含まれるNICを1つ以上選択し、各NICに関連付けられた仮想ネットワークを選択します。
- **Machine Identities**、**Domain Credentials**、**Scopes**、および**Summary**ページには、Nutanix固有の情報は含まれていません。

制限事項

Nutanixホスト接続（特にNutanix AHVプラグイン2.7.1）を使用してMCSカタログを作成する場合、プロビジョニングされたVMのハードディスクサイズがWeb Studioで誤って表示されます。表示されるサイズは、実際のストレージサイズ（50 GB）よりもはるかに小さい（1 GB）です。ハードディスクサイズはNutanixコンソールで正しく表示されます。

次のステップ

- これが最初に作成するカタログである場合、Web Studioは、デリバリーグループの作成に誘導します。
- 構成プロセス全体を確認するには、インストールと構成を参照してください。
- カタログを管理するには、マシンカタログの管理を参照してください。

詳細情報

- 接続とリソースの作成および管理
- Nutanixへの接続
- Nutanixクラウドおよびパートナーソリューションへの接続
- マシンカタログの作成

VMwareカタログを作成する

マシンカタログの作成は、マシンカタログを作成するウィザードについて説明しています。以下の情報は、VMware仮想化環境に固有の詳細を扱っています。

> **注:**
>
> VMwareカタログを作成する前に、VMwareへの接続の作成を完了する必要があります。VMwareへの接続を参照してください。

マスターVMを作成する

マシンカタログでユーザーデスクトップとアプリケーションを提供するには、マスターVMを使用します。ハイパーバイザーで、次の操作を行います。

1. マスターVMにVDAをインストールし、デスクトップを最適化するオプションを選択します。これにより、パフォーマンスが向上します。
2. マスターVMのスナップショットを作成し、バックアップとして使用します。

> **注:**
>
> MCSを使用してvSAN 8.0環境でVMをプロビジョニングできます。

マシンプロファイルを使用してマシンカタログを作成する

マシンプロファイルを使用してMCSマシンカタログを作成できます。マシンプロファイルの入力元はVMwareテンプレートです。マシンプロファイルは、VMwareテンプレートからハードウェアプロパティを取得し、カタログ内の新しくプロビジョニングされたVMに適用します。

> **注:**
>
> - マスターイメージ入力（スナップショット）とマシンプロファイル入力（VMwareテンプレート）は、両方ともvTPMが有効であるか、両方ともvTPMが無効である必要があります。このルールは、`New-ProvScheme`と`Set-ProvScheme`の両方に適用されます。
> - マスターイメージでvTPMが有効になっている場合、VMwareテンプレートはマスターイメージと同じVMソースからのみ取得できます。

- 暗号化ストレージポリシーはフルクローンのみをサポートします。
- マシンプロファイルベースのカタログは、提供されたVMwareテンプレートを利用してストレージコントローラー情報を収集し、接続された仮想ディスクに依存します。テンプレートには、仮想マシンの仮想ディスクを構成するために使用されるストレージコントローラー情報を取得するために必要な仮想ディスクが含まれている必要があります。

カタログへのVMのプロビジョニングを許可するには、マシンプロファイル内のVMwareテンプレートがカタログのライフサイクル中に存在する必要があります。VMwareテンプレートがない場合、新しいVMをプロビジョニングすることはできません。VMwareテンプレートが削除された場合は、`Set-ProvScheme`コマンドを使用して新しいテンプレートを提供する必要があります。

- MCSはVMwareテンプレートのプロパティをキャプチャします。Get-Provschemeコマンドを使用して、VMwareテンプレートの保存されたプロパティを参照する新しいVMwareテンプレートを作成できます。
- あるいは、マシンカタログとプロビジョニングされたVMが存在する場合、MCSでプロビジョニングされたマシンを使用して新しいVMwareテンプレートを作成することもできます。

異なるOSに基づいて、異なる構成でマシンカタログを作成できます。

- マスターイメージにWindows 11がインストールされている場合、マスターイメージに対してvTPMを有効にすることが要件となります。したがって、マシンプロファイルのソースであるVMwareテンプレートにはvTPMがアタッチされている必要があります。
- vTPMがアタッチされていないマスターイメージにWindows 10がインストールされている場合、マシンプロファイルのソースとして非vTPM VMwareテンプレートを使用してマシンカタログを作成できます。

暗号化されたストレージポリシーが適用されたマシンプロファイルテンプレートを使用して、フルコピーディスクモードでマシンカタログを作成できる別の構成があります。

マシンプロファイルをインプットとしてPowerShellコマンドを使用してマシンカタログを作成するには：

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. 次のコマンドを実行します。

- マシンプロファイル入力のソースとしてvTPMがアタッチされたVMwareテンプレートとWindows 11がインストールされたマスターイメージを使用してマシンカタログを作成するには：

```
$identityPool = New-AcctIdentityPool  -IdentityPoolName "<string>"

-NamingScheme "<string>-###"

-NamingSchemeType Numeric

-Domain "<domain name"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme  -CleanOnBoot

-HostingUnitName "vSanRg"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<network name>.network"}

-ProvisioningSchemeName "<string>"

-Scope @() -VMCpuCount 4

-VMMemoryMB 6144

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template" -TenancyType Shared

-FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False

-MinimumFunctionalLevel 'L7_9'

-Name "<catalog name>"

-ProvisioningType 'MCS'

-Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- マシンプロファイルのソースとして非vTPM VMwareテンプレートとWindows 10がインストールされたマスターイメージを使用してマシンカタログを作成するには：

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###" -NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-CleanOnBoot -HostingUnitName "<string>"
```

```
-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4  -
VMMemoryMB 8192

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template"

-TenancyType Shared  -FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False

-MinimumFunctionalLevel 'L7_9' -Name "<string>" -ProvisioningType
'MCS' -Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- 暗号化されたストレージポリシーが適用されたマシンプロファイルテンプレートを使用して、フルコピーディスクモードでマシンカタログを作成するには：

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###"

-NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-HostingUnitName "<string>"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"

-Scope @() -VMCpuCount 4  -VMMemoryMB 8192 -MachineProfile "XDHyp:
\HostingUnits\<hosting unit name>\<template name>.template"

-TenancyType Shared

-FunctionalLevel "L7_20" -UseFullDiskCloneProvisioning
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"
```

```
-Description "<string>"  -IsRemotePC $False

-MinimumFunctionalLevel 'L7_9'

-Name "<string>" -ProvisioningType 'MCS' -Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

マシンプロファイルを更新するには、Set-ProvSchemeコマンドを使用します。例：

```
Set-ProvScheme -ProvisioningSchemeName 'name' -IdentityPoolName 'name'
-MachineProfile 'XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template'
```

複数のNICの確認

マシンプロファイルと、`New-ProvScheme` および `Set-ProvScheme` コマンドの `NetworkMapping` パラメーターを使用している場合、複数のNICの事前チェック中にさまざまなエラーメッセージが表示されます。

複数のNICの事前チェックリストは次のとおりです。

- マシンプロファイルテンプレートからのNIC数のみが使用され、検証されます。これらのNICが指すネットワークは、ホスティングユニットネットワークに対して使用または検証されません。
- マシンプロファイルテンプレートのNIC数がホスティングユニットのネットワーク数よりも多い場合、エラーメッセージが表示されます。
- マシンプロファイルテンプレートのNIC数がゼロの場合、エラーメッセージが表示されます。マシンプロファイルテンプレートのNIC数が1の場合：
    - `New-ProvScheme` または `Set-ProvScheme` コマンドでネットワークマッピングが指定されておらず、ホスティングユニットネットワークが1つの場合、ホスティングユニットネットワークが使用されます。

  - ネットワークマッピングが指定されている場合、指定されたネットワークマッピングが有効であれば使用されます。

- マシンプロファイルテンプレートのNIC数が1より大きい場合、またはホスティングユニットネットワーク数が1より大きい場合：

  - コマンドには有効なネットワークマッピングが必要であり、各NICのマッピングを提供する必要があります（つまり、NetworkMappingの数はマシンプロファイルのNIC数と同じである必要があります）。
  - 複数のNICをホスティングユニット内の同じネットワークにマッピングすることはできません。
  - `NetworkMapping` の数とマシンプロファイルのNIC数は、ホスティングユニットのネットワーク数以下である必要があります。
  - `NetworkMapping` は、0からn-1までの各IDに対して提供される必要があります。ここで、nはマシンプロファイルテンプレート内のネットワークアダプターの数です。

トラブルシューティング

カタログの作成に失敗した場合は、CTX294978を参照してください。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、「」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure.html)を参照してください。
- カタログを管理するには、マシンカタログの管理およびVMwareカタログの管理を参照してください。

詳細情報

- 接続とリソースの作成および管理
- VMwareへの接続
- マシンカタログの作成

異なるマシンID結合タイプのIDプール

MCS を使用すると、オンプレミス AD 参加、ハイブリッド Azure AD 参加、またはドメイン非参加としてマシンをプロビジョニングできます。

Web Studioでマシンを構成する方法については、マシンカタログの作成を参照してください。

異なるマシンID参加タイプのIDプールを作成する方法の詳細については、以下を参照してください。

- オンプレミスActive Directory参加済みマシンIDのIDプール
- ハイブリッド Azure Active Directory 参加済みマシンIDのIDプール
- ドメインに参加していないマシンIDのIDプール

オンプレミスActive Directory参加済みマシンIDのIDプール

この記事では、オンプレミスActive Directory参加済みマシンIDのIDプールを作成する方法について説明します。

Web Studioを使用する

以下の情報は、マシンカタログの作成のガイダンスを補足するものです。

カタログ作成ウィザードで、次のようにします。

1. **マシンID**ページで、次のようにします。
    a. IDの種類として**オンプレミスActive Directory**を選択します。
    b. Active Directoryアカウントオプションを選択します。
        - **新しいActive Directoryアカウントを作成する**:
            - **新しいActive Directoryアカウントを作成する**を選択し、既存のIDプールを使用して新しいアカウントを作成する場合は、それらのアカウントのドメインを選択し、アカウント命名スキームを指定します。
            - **新しいActive Directoryアカウントを作成する**を選択し、既存のIDプールを使用して新しいアカウントを作成する場合は、リストからIDプールを選択します。
        - **既存のActive Directoryアカウントを使用する**: CSVファイルから参照またはインポートし、パスワードをリセットするか、すべてのアカウントに同じパスワードを指定できます。
    c. **次へ**をクリックします。
2. 「**ドメイン資格情報**」ページで、資格情報を手動で入力します。

PowerShell を使用する

IDプールを作成するか、既存のIDプールを更新できます。

例: 新しいIDプールを作成するには、以下を実行します。

```
New-AcctIdentityPool -IdentityType ActiveDirectory -IdentityPoolName
MyPool -NamingScheme Acc#### -Domain MyDomain.com -NamingSchemeType
Numeric -OU "CN=MyOU,DC=MyDomain,DC=com"
```

例: 既存のIDプールを更新するには、以下を実行します。

```
$identityPoolUid = (Get-ProvScheme -ProvisioningSchemeName
"MyProvScheme").IdentityPoolUid

Set-AcctIdentityPool -IdentityPoolUid $identityPoolUid
```

Hybrid Azure Active Directory参加済みマシンIDのIDプール

注:

2023 年 7 月以降、Microsoft は Azure Active Directory (Azure AD) を Microsoft Entra ID に名称変更しました。このドキュメントでは、Azure Active Directory、Azure AD、または AAD へのすべての参照は、Microsoft Entra ID を指します。

この記事では、以下のIDプールを作成する方法について説明します。

- Hybrid Azure Active Directory (AD) 参加済みカタログ
- Microsoft Intuneに登録されているHybrid Azure AD参加済みカタログ

要件、制限、および考慮事項については、Hybrid Azure Active Directory 参加済み を参照してください。

Hybrid Azure Active Directory (AD) 参加済みカタログの作成

Web Studioを使用する

以下の情報は、マシンカタログの作成 のガイダンスを補足するものです。

カタログ作成ウィザードの ページで、次のようにします。

- **Hybrid Azure Active Directory参加済み**を選択します。作成されたマシンは組織によって所有され、その組織に属するActive Directoryアカウントでサインインされます。
- デバイス管理のために作成されたマシンを Microsoft Intune (Configuration Manager を含む) に登録するには、 を選択します。カタログ作成中のエラーを回避するには、マスターイメージが次の要件を満たしていることを確認してください。
  - VDA バージョン 2405 以降がインストールされていること。
  - サイトコードが割り当てられていない **Configuration Manager クライアント**がインストールされていること。詳細については、この Microsoft の記事を参照してください。

> **注:**
>
> IDタイプとして**ハイブリッド Azure Active Directory 参加済み**を選択した場合、カタログ内の各マシンには対応するADコンピューターアカウントが必要です。

PowerShell を使用する

以下は、Web Studio での操作に相当する PowerShell の手順です。Remote PowerShell SDK を使用してカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>` を参照してください。

オンプレミスAD参加済みカタログとHybrid Azure AD参加済みカタログの違いは、IDプールとマシンアカウントの作成にあります。

Hybrid Azure AD参加済みカタログのアカウントとともにIDプールを作成するには、次の手順を実行します。

```
New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -Domain
"corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -NamingScheme
"HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU
"CN=AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"

New-AcctIdentity -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
-ADUserName "corp\admin1" -ADPassword $password
```

```
Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -All
-ADUserName "corp\admin1" -ADPassword $password
```

注:

`$password` は、書き込み権限を持つADユーザーアカウントの一致するパスワードです。

ハイブリッドAzure AD参加済みカタログを作成するために使用される他のすべてのコマンドは、従来のオンプレミスAD参加済みカタログと同じです。

Hybrid Azure AD参加プロセスのステータスの表示

Web Studioでは、デリバリーグループ内のハイブリッドAzure AD参加済みマシンが電源オンの状態にある場合、ハイブリッドAzure AD参加プロセスのステータスが表示されます。ステータスを表示するには、検索を使用してそれらのマシンを特定し、各マシンの下部ペインにある**詳細**タブで**マシンID**を確認します。**マシンID**には次の情報が表示されます。

- ハイブリッドAzure AD参加済み
- Azure ADにまだ参加していません

注:

- マシンが最初に電源オンになったときに、ハイブリッドAzure AD参加の遅延が発生する場合があります。これは、デフォルトのマシンID同期間隔（Azure AD Connectの30分）が原因です。マシンは、マシンIDがAzure AD Connectを介してAzure ADに同期された後にのみ、ハイブリッドAzure AD参加済み状態になります。
- マシンがハイブリッド Azure AD 参加状態にならなかった場合、Delivery Controller に登録されません。登録ステータスは **Initialization** と表示されます。

また、Web Studio を使用して、マシンが利用できない理由を確認できます。そのためには、**検索**ノードでマシンをクリックし、下部ペインの**詳細**タブで**登録**を確認し、ツールチップを読んで追加情報を確認します。

トラブルシューティング

マシンがハイブリッド Azure AD 参加に失敗した場合は、次の操作を行います。

- マシンアカウントが Microsoft Azure AD ポータルを通じて Azure AD に同期されているか確認します。同期されている場合、**Not yet joined to Azure AD** と表示され、登録が保留中であることを示します。

  マシンアカウントを Azure AD に同期するには、以下を確認してください。

  - マシンアカウントが Azure AD と同期するように構成されている OU にあること。**userCertificate** 属性を持たないマシンアカウントは、同期するように構成されている OU にあっても Azure AD に同期されません。
  - マシンアカウントに属性 **userCertificate** が設定されていること。属性を表示するには、Active Directory Explorer を使用します。
  - マシンアカウントが作成された後、Azure AD Connect が少なくとも一度は同期されている必要があります。同期されていない場合は、Azure AD Connect マシンの PowerShell コンソールで `Start-ADSyncSyncCycle -PolicyType Delta` コマンドを手動で実行して、即時同期をトリガーします。

- ハイブリッド Azure AD 参加用の Citrix 管理デバイスキーペアがマシンに正しくプッシュされているか、**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix** の下の **DeviceKeyPairRestored** の値をクエリして確認します。

  値が 1 であることを確認します。そうでない場合、考えられる理由は次のとおりです。

  - プロビジョニングスキームに関連付けられている ID プールの `IdentityType` が `HybridAzureAD` に設定されていません。これは `Get-AcctIdentityPool` を実行して確認できます。
  - マシンが、マシンカタログと同じプロビジョニングスキームを使用してプロビジョニングされていない。
  - マシンがローカルドメインに参加していない。ローカルドメインへの参加は、ハイブリッド Azure AD 参加の前提条件です。

- MCS でプロビジョニングされたマシンで `dsregcmd /status /debug` コマンドを実行して、診断メッセージを確認します。

  - ハイブリッドAzure AD参加が成功した場合、コマンドラインの出力で**AzureAdJoined**と**DomainJoined**が**YES**になります。
  - そうでない場合、問題をトラブルシューティングするにはMicrosoftのドキュメントを参照してください: `<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current>`。

- エラーメッセージ **Server Message: The user certificate is not found on the device with id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx** が表示された場合は、次の PowerShell コマンドを実行してユーザー証明書を修復してください:

  ```
  Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
  UserCertificate
  ```

  ユーザー証明書の問題の詳細については、CTX566696を参照してください。

Microsoft Intuneに登録されたハイブリッドAzure AD参加カタログの作成

Microsoft Intuneに登録されたハイブリッドAzure AD参加カタログ向けに、永続的なシングルセッションおよびマルチセッションVM用の共同管理対応カタログを作成できます。共同管理対応カタログは、StudioとPowerShellの両方を使用して作成できます。

Web Studioを使用する

以下の情報は、マシンカタログの作成のガイダンスを補足するものです。

マシンカタログのセットアップウィザードで、:

- **マシンID**ページで、**ハイブリッドAzure Active Directory参加済み**を選択し、次に**Configuration Managerを使用してMicrosoft Intuneにマシンを登録**を選択します。このアクションを使用すると、Configuration ManagerとMicrosoft Intune（つまり、共同管理）がVMを管理します。

PowerShell を使用する

以下は、Studio の手順に相当する PowerShell の手順です。

Remote PowerShell SDK を使用して Configuration Manager でマシンを Microsoft Intune に登録するには、`New-AcctIdentityPool` の `DeviceManagementType` パラメーターを使用します。この機能には、カタログがハイブリッド Azure AD 参加済みであり、Azure AD が適切な Microsoft Intune ライセンスを所有している必要があります。

ハイブリッドAzure AD参加カタログと共同管理対応カタログの違いは、IDプールの作成方法にあります。例：

```
New-AcctIdentityPool -AllowUnicode -DeviceManagementType "IntuneWithSCCM"
IdentityType="HybridAzureAD" -IdentityPoolName "CoManagedCatalog"
-NamingScheme "CoManaged-VM-##" -NamingSchemeType "Numeric" -Scope @()
-ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
```

トラブルシューティング

マシンがMicrosoft Intuneへの登録に失敗したり、共同管理状態に到達できなかったりした場合は、次の操作を行います。

- Intuneライセンスを確認する

  Azure ADテナントに適切なIntuneライセンスが割り当てられているか確認します。Microsoft Intuneのライセンス要件については、Microsoft Intune licensingを参照してください。

- Hybrid Azure AD参加の状態を確認する

  MCSでプロビジョニングされたマシンがHybrid Azure ADに参加しているか確認します。Hybrid Azure ADに参加していない場合、マシンは共同管理の対象になりません。Hybrid Azure AD参加の問題のトラブルシューティングについては、Troubleshootを参照してください。

- 共同管理の適格性を確認する

  - MCSでプロビジョニングされたマシンに、予期されるConfiguration Managerサイトが正しく割り当てられているか確認します。割り当てられたサイトを取得するには、影響を受けるマシンで次のPowerShellコマンドを実行します。

    ```
    (New-Object -ComObject "Microsoft.SMS.Client").GetAssignedSite()
    ```

  - VMにサイトが割り当てられていない場合は、次のコマンドを使用して、Configuration Managerサイトが自動的に検出できるか確認します。

    ```
    (New-Object -ComObject "Microsoft.SMS.Client").AutoDiscoverSite()
    ```

  - サイトコードが検出できない場合は、Configuration Manager 環境で境界と境界グループが適切に構成されていることを確認してください。詳細については、Considerations を参照してください。

  - Configuration Manager クライアントのサイト割り当てに関する問題がないか、`C:\Windows\CCM\Logs\ClientLocation.log` を確認してください。

  - マシンの共同管理状態を確認します。影響を受けるマシンで**Configuration Managerコントロールパネル**を開き、**全般**タブに移動します。共同管理プロパティの値は**Enabled**である必要があります。そうでない場合は、`C:\Windows\CCM\Logs\CoManagementHandler.log`の下のログを確認してください。

- Intune 登録を確認する

すべての前提条件が満たされていても、マシンが Microsoft Intune への登録に失敗する場合があります。Intune 登録の問題については、**Application and Services Logs > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider** の下の Windows イベントログを確認してください。

非ドメイン参加型マシンIDのIDプール

この記事では、Citrix Virtual Apps and Desktopsを使用して、ドメインに参加していないカタログのIDプールを作成する方法について説明します。

要件、制限、考慮事項については、ドメインに参加していないを参照してください。

マシンカタログを作成する前に、以下が必要です。

1. 新しいリソースの場所
    - Citrix Cloud™管理UI > 左上のハンバーガーメニュー > **リソースの場所**に移動します。
    - **+ リソースの場所**をクリックします。
    - 新しいリソースの場所に名前を入力し、**保存**をクリックします。
2. ホスティング接続を作成します。詳細については、接続の作成と管理セクションを参照してください。

Citrix Virtual Apps and Desktopsを使用すると、ワークグループまたはドメインに参加していないマシンに基づいてカタログを作成できます。ドメインに参加していないマシンの作成は、アカウントIDプールがどのように作成されるかによって異なります。アカウントIDプールは、カタログプロビジョニング中にMCSがマシン名を作成および追跡するために使用するメカニズムです。

Web Studioの使用

以下の情報は、マシンカタログの作成のガイダンスを補足するものです。

カタログ作成ウィザードで：

- **マシンID**ページで、**ドメインに参加していない**を選択します。作成されたマシンはどのドメインにも参加しません。

> **注:**
>
> **非ドメイン参加**のIDタイプでは、カタログの最小機能レベルとしてVDAバージョン2311以降が必要です。利用可能にするには、必要に応じて最小機能レベルを更新してください。

PowerShell を使用する

Remote PowerShell SDKを使用して、非ドメイン参加カタログのIDプールを作成できます。

PowerShellパラメーターの**WorkgroupMachine**と**IdentityType**を使用して、非ドメイン参加カタログのIDプールを作成します。これらのパラメーターにより、ドメイン管理者資格情報を含むすべてのAD固有のパラメーターを指定する必要がなくなります。

```
New-AcctIdentityPool -AllowUnicode -IdentityType "Workgroup"
-WorkgroupMachine -IdentityPoolName "NonDomainJoinedCatalog" -NamingScheme
"NDJ-VM-##" -NamingSchemeType "Numeric" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"
```

非ドメイン参加カタログの作成に使用されるその他のすべてのコマンドは、従来のオンプレミスActive Directory参加カタログの場合と同じです。

マシンカタログを管理する

注:

Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioの詳細については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

マシンカタログへのマシンの追加または削除、名前の変更、説明の変更、またはカタログのActive Directoryコンピューターアカウントの管理を行うことができます。

カタログの保守には、各マシンが最新のOSアップデートを適用していることを確認することも含まれます。これには、ウイルス対策の更新、オペレーティングシステムのアップグレード、または構成の変更が含まれます。

- Machine Creation Services™ (MCS) を使用して作成されたプールされたランダムマシンを含むカタログは、カタログで使用されるマスターイメージを更新し、その後マシンを更新することでマシンを保守します。この方法により、多数のユーザーマシンを効率的に更新できます。

- 静的で永続的に割り当てられたマシンを含むカタログ、およびリモートPCアクセス マシンカタログの場合、ユーザーマシンの更新はWeb Studioの外部で管理します。このタスクは、個別に、またはサードパーティのソフトウェア配布ツールを使用して一括で実行します。

ホストハイパーバイザーへの接続の作成と管理については、「接続とリソース」を参照してください。

> **注:**
>
> MCSはWindows 10 IoT CoreおよびWindows 10 IoT Enterpriseをサポートしていません。詳細については、Microsoftサイトを参照してください。

永続インスタンスについて

永続的または専用インスタンスを使用して作成されたMCSカタログを更新する場合、カタログ用に作成された新しいマシンはすべて更新されたイメージを使用します。既存のインスタンスは引き続き元のインスタンスを使用します。イメージの更新プロセスは、他の種類のカタログと同じ方法で行われます。以下を考慮してください。

- 永続ディスクカタログの場合、既存のマシンは新しいイメージに更新されませんが、カタログに追加される新しいマシンは新しいイメージを使用します。
- 非永続ディスクカタログの場合、マシンイメージはマシンがリセットされるたびに更新されます。
- 永続マシンカタログでは、イメージを更新すると、それを使用するカタログインスタンスも更新されます。
- 永続的ではないカタログの場合、異なるマシンに異なるイメージを使用したい場合は、イメージは個別のカタログに存在する必要があります。

マシンカタログを管理する

マシンカタログは次の2つの方法で管理できます。

- Web Studioの使用
- PowerShellを使用する

Web Studioを使用する

このセクションでは、Web Studioを使用してカタログを管理する方法について詳しく説明します。

- マシンカタログの管理
  - はじめに
  - 永続インスタンスについて
- マシンカタログの管理
- Web Studioの使用
- カタログの詳細の表示
  - カタログへのマシンの追加
  - カタログからマシンを削除する
- カタログを編集する
- カタログの名前を変更する
- カタログを別のゾーンに移動する
- カタログを削除する
- カタログ内のActive Directoryコンピューターアカウントを管理する
- カタログを更新する
  - マスターイメージを更新または作成する
  - マスターイメージを変更する
  - マスターイメージをロールバックする
- 機能レベルを変更または変更を元に戻す
- カタログをクローンする
- フォルダーを使用してカタログを整理する
  - カタログフォルダーを作成する
  - カタログを移動する
  - カタログフォルダーの管理(#manage-catalog-folders)
- カタログ作成の再試行(#retry-catalog-creation)
- トークンを使用してMCS以外でプロビジョニングされたVDAを登録する（プレビュー）(#enroll-non-mcs-provisioned-vdas-using-tokens-preview)
- PowerShellの使用(#use-powershell)

- カタログに関連付けられた警告とエラーの取得(#retrieve-warnings-and-errors-associated-with-a-catalog)
- イメージへの説明の追加(#add-descriptions-to-an-image)
- OSディスクのリセット(#reset-os-disk)
- 既存のプロビジョニングスキームのネットワーク設定の変更(#change-the-network-setting-for-an-existing-provisioning-scheme)
- マシンカタログのバージョンの管理(#manage-versions-of-a-machine-catalog)
- マシンプロファイルに基づかないマシンカタログをマシンプロファイルに基づくマシンカタログに変換する(#convert-a-non-machine-profile-based-machine-catalog-to-machine-profile-based-machine-catalog)
- アクティブなコンピューターアカウントのID情報の修復(#repair-the-identity-information-of-active-computer-accounts)
  - 条件(#conditions)
  - IDディスクをリセットする(#reset-identity-disk)
- 既存のマシンカタログのキャッシュ構成を変更する(#change-cache-configuration-on-an-existing-machine-catalog)
  - 要件
  - キャッシュ構成を変更する
- ローカルファイル共有アクセスによるVDA更新のサポート
  - PowerShell コマンドレット
  - 前提条件
  - ファイル共有のアクセス許可を設定する方法
  - ローカルファイル共有からのVDA更新
- トラブルシューティング
- 次のステップ

カタログの詳細を表示

1. 検索機能を使用して特定のマシンカタログを見つけます。手順については、インスタンスの検索を参照してください。
2. 検索結果から、必要に応じてカタログを選択します。

3. カタログ列の説明については、次の表を参照してください。
4. このカタログの詳細については、下部の詳細ペインのタブをクリックしてください。

列	説明	
マシンカタログ	カタログの名前と割り当てタイプ。割り当てタイプには以下が含まれます。 • ランダム: カタログ内のマシンはユーザーにランダムに割り当てられます。 • 永続: カタログ内のマシンはユーザーに永続的に割り当てられます。	
マシンタイプ	カタログ内のマシンでサポートされているセッションタイプ。可能な値は次のとおりです。 • OSタイプ: マルチセッションOS (仮想); ユーザーデータ: 破棄。 • OSタイプ: マルチセッションOS (仮想); ユーザーデータ: ローカルディスク上 • OSタイプ: シングルセッションOS (リモートPCアクセス) • OSタイプ: シングルセッションOS (仮想); ユーザーデータ: 破棄	

列	説明
	• OSタイプ: シングルセッションOS (仮想); ユーザーデータ: ローカルディスク上
マシン数	カタログ内のマシン数とプロビジョニング方法。可能なプロビジョニング方法には、マシン作成サービス (MCSマシン)、手動、Citrix Provisioning™サービスがあります。
割り当て済み数	デリバリーグループに割り当てられているカタログ内のマシン数。
フォルダー	**マシンカタログ**ツリー内でのカタログの場所。カタログが存在するフォルダーの名前 (末尾のバックスラッシュを含む) を表示します。または、カタログがルートレベルにある場合は `-` を表示します。
VDAアップグレード	VDAアップグレードの状態。可能な値は、未構成、スケジュール済み、利用可能、および最新です。
イメージステータス	カタログのイメージ更新ステータス。非永続マシンカタログにのみ適用されます。指定できる値は、完全に更新済み、部分的に更新済み、更新保留中、準備中です。

マシンをカタログに追加する

開始する前に:

- 仮想化ホストに、追加のマシンを収容するのに十分なプロセッサ、メモリ、ストレージがあることを確認します。
- 未使用のActive Directoryコンピューターアカウントが十分にあることを確認します。既存のアカウントを使用している場合、追加できるマシンの数は、利用可能なアカウントの数によって制限されます。
- Web Studioを使用して追加のマシン用のActive Directoryコンピューターアカウントを作成する場合、適切なドメイン管理者権限が必要です。

カタログにマシンを追加するには:

1. Web Studioにサインインします。
2. 左側のペインで**マシンカタログ**を選択します。
3. マシンカタログを選択し、アクションバーで**マシンの追加**を選択します。
4. 追加する仮想マシンの数を選択します。
5. 追加するVMの数に対して既存のActive Directoryアカウントが不足している場合は、アカウントが作成されるドメインと場所を選択します。アカウントの命名スキームを指定します。連続する数字または文字が表示される場所を示すには、ハッシュマークを使用します。OU名にスラッシュ（/）を使用しないでください。名前は数字で始めることはできません。たとえば、PC-Sales-##（0〜9を選択）という命名スキームでは、PC-Sales-01、PC-Sales-02、PC-Sales-03などのコンピューターアカウントが作成されます。
6. 既存のActive Directoryアカウントを使用する場合は、アカウントを参照するか、**インポート**をクリックしてアカウント名を含む.csvファイルを指定します。追加するすべてのマシンに対して十分なアカウントがあることを確認してください。Web Studioはこれらのアカウントを管理します。Web Studioにすべてのアカウントのパスワードをリセットさせるか、すべてのアカウントで同じである必要があるアカウントパスワードを指定します。

マシンはバックグラウンドプロセスとして作成され、多数のマシンを作成する場合は時間がかかることがあります。Web Studioを閉じても、マシンの作成は続行されます。

カタログからマシンを削除する

マシンカタログからマシンを削除すると、ユーザーはそのマシンにアクセスできなくなります。そのため、マシンを削除する前に、以下を確認してください。

- ユーザーデータがバックアップされているか、不要になっている。

- すべてのユーザーがログオフしている。メンテナンスモードをオンにすると、マシンへの新しい接続が停止します。
- マシンは電源オフになっています。

カタログからマシンを削除するには：

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**マシンを表示**を選択します。
4. 1つ以上のマシンを選択し、アクションバーで**削除**を選択します。

削除するマシンを削除するかどうかを選択します。マシンを削除することを選択した場合、それらのマシンのActive Directoryアカウントを保持するか、無効にするか、削除するかを指定します。

カタログを編集する

1. **説明**ページで、カタログの説明を変更します。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**マシンカタログの編集**を選択します。
4. **スコープ**ページで、スコープを変更します。
5. **NIC**ページで、次のアクションを実行します。

    - NICのサブネットマッピングを変更するには、**関連ネットワーク**フィールドからネットワークを選択します。
    - サブネットマッピングを追加するには、**NICの追加**を選択し、**関連ネットワーク**フィールドからネットワークを選択して、**保存**をクリックします。

    カタログに関連付けられたホストに存在するサブネットのみが、「**関連ネットワーク**」フィールドに表示されます。

    マシンプロファイルのないAzureマシンカタログにのみNICを追加できます。

> 「**注：**」：
>
> - AWSマシンカタログの場合、同じサブネットを複数のNICにマッピングすることはできません。

- マシンプロファイルを持つマシンカタログの場合、カタログ上のNICの数は、マシンプロファイル上のNICの数と等しくなければなりません。
- この機能は、IBM Cloudハイパーバイザーではサポートされていません。
- この機能は、Nutanixハイパーバイザーの場合、Nutanix Prism Elementでのみサポートされています。

6. カタログの種類によっては、他のページが表示される場合があります。

   Azure Resource Managerイメージを使用して作成されたカタログの場合、次のページが表示されます。加えた変更は、後でカタログに追加するマシンにのみ適用されることに注意してください。既存のマシンは変更されません。

   - 「**仮想マシン**」ページで、マシンを作成するマシンサイズとアベイラビリティゾーンを変更します。

     「**注：**」：

     - カタログがサポートするマシンサイズのみが表示されます。
     - 必要に応じて、「**他のマシンカタログで使用されているマシンサイズのみを表示**」を選択して、マシンサイズリストをフィルターします。

   - 「**マシンプロファイル**」ページで、マシンプロファイルを使用するか変更するかを選択します。
   - （カタログが専用グループホストで構成されている場合にのみ表示）「**専用ホストグループ**」ページで、ホストグループを変更するかどうかを選択します。
   - **ストレージとライセンスの種類**ページで、ストレージの種類、ライセンスの種類、およびAzure Computer Galleryの設定を変更するかどうかを選択します（**準備されたイメージをAzure Galleryに配置**が使用されている場合にのみ利用可能）。

   注:

   新しく選択した設定が現在のマシンサイズをサポートしていない場合、設定を変更するとマシンサイズの設定がリセットされることを通知する警告ダイアログボックスが表示

> されます。続行を選択すると、「**仮想マシン**」メニューの横に赤い点が表示され、新しいマシンサイズを選択するように促されます。

- **ライセンスの種類**ページで、WindowsライセンスまたはLinuxライセンスの設定を変更するかどうかを選択します。

リモートPCアクセス カタログの場合、次のページが表示されます。

- **電源管理**ページで、電源管理設定を変更し、電源管理接続を選択します。
- **組織単位**ページで、Active Directory OUを追加または削除します。

7. 加えた変更を適用するには「**適用**」をクリックし、終了するには「**保存**」をクリックします。

カタログの名前を変更する

1. Web Studioにサインインします。
2. 左ペインで「**マシンカタログ**」を選択します。
3. カタログを選択し、アクションバーで「**マシンカタログの名前を変更**」を選択します。
4. 新しい名前を入力します。

カタログを別のゾーンに移動する

展開に複数のゾーンがある場合、カタログをあるゾーンから別のゾーンに移動できます。

カタログ内のVMを含むハイパーバイザーとは異なるゾーンにカタログを移動すると、パフォーマンスに影響します。

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. カタログを選択し、アクションバーで を選択します。
4. カタログを移動するゾーンを選択します。

カタログを削除する

カタログを削除する前に、以下を確認してください。

- すべてのユーザーがログオフしており、切断されたセッションが実行されていないこと。
- 新しい接続ができないように、カタログ内のすべてのマシンでメンテナンスモードがオンになっていること。
- カタログ内のすべてのマシンが電源オフになっていること。

- カタログがデリバリーグループに関連付けられていないこと。つまり、デリバリーグループにそのカタログのマシンが含まれていないこと。

カタログを削除するには：

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. カタログを選択し、アクションバーで を選択します。
4. カタログ内のマシンが削除されるかどうかを示します。マシンを削除することを選択した場合、それらのマシンのActive Directoryコンピューターアカウントを保持、無効化、または削除するかどうかを示します。

カタログ内のActive Directoryコンピューターアカウントを管理する

マシンカタログ内のActive Directoryアカウントを管理するには、次の操作を実行できます。

- シングルセッションOSおよびマルチセッションOSカタログからActive Directoryコンピューターアカウントを削除して、未使用のマシンアカウントを解放します。これらのアカウントは、他のマシンで使用できます。
- アカウントを追加して、カタログにマシンが追加されたときにコンピューターアカウントがすでに存在するようにします。OU名にスラッシュ (/) を使用しないでください。

Active Directoryアカウントを管理するには：

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. カタログを選択し、アクションバーで を選択します。
4. コンピューターアカウントを追加するか削除するかを選択します。アカウントを追加する場合は、アカウントのパスワードをどうするかを指定します。すべてリセットするか、すべてのアカウントに適用されるパスワードを入力します。

   現在のアカウントパスワードがわからない場合は、パスワードをリセットできます。パスワードのリセットを実行する権限が必要です。パスワードを入力すると、アカウントがインポートされるときにパスワードが変更されます。アカウントを削除するときは、Active Directoryのアカウントを保持、無効化、または削除するかを選択します。

カタログからマシンを削除したり、カタログを削除したりするときに、Active Directoryアカウントを保持、無効化、または削除するかどうかを示します。

カタログを更新する

カタログ内のマシンを更新する前に、マスターイメージのコピーまたはスナップショットを保存することをお勧めします。データベースには、各マシンカタログで使用されたマスターイメージの履歴レコードが保持されます。カタログ内のマシンをロールバックまたは元に戻して、マスターイメージの以前のバージョンを使用します。ユーザーがデスクトップに展開した更新プログラムで問題が発生した場合に、このタスクを実行します。これにより、ユーザーのダウンタイムが最小限に抑えられます。マスターイメージを削除、移動、または名前変更しないでください。それらを使用してカタログを元に戻すことはできません。

マシンが更新されると、自動的に再起動します。

マスターイメージを更新または作成する

マシンカタログを更新する前に、既存のマスターイメージを更新するか、ホストハイパーバイザー上に新しいマスターイメージを作成します。

1. ハイパーバイザーで、現在のVMのスナップショットを作成し、意味のある名前を付けます。このスナップショットは、必要に応じてカタログ内のマシンを元に戻す（ロールバックする）ために使用できます。
2. 必要に応じて、マスターイメージの電源をオンにし、ログオンします。
3. 更新プログラムをインストールするか、マスターイメージに必要な変更を加えます。
4. VMの電源をオフにします。
5. VMのスナップショットを作成します。Web Studioでカタログが更新されたときに認識される、意味のある名前を付けます。Web Studioでスナップショットを作成することもできますが、Citrixではハイパーバイザー管理コンソールを使用して作成することをお勧めします。その後、Web Studioでそのスナップショットを選択します。このプロセスにより、自動生成された名前ではなく、意味のある名前と説明を提供できます。GPUマスターイメージの場合、マスターイメージの変更はXenServer®コンソールからのみ可能です。

マスターイメージを変更する

カタログ内のすべてのマシンに更新プログラムを準備して展開するには：

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで **［マスターイメージの変更］** を選択します。
4. **［イメージ］** ページで、展開するホストとイメージを選択します。

> **ヒント:**
>
> MCSで作成されたカタログの場合、イメージにメモを追加して注釈を付けることができます。メモは最大500文字まで含めることができます。マスターイメージを変更するたびに、メモを追加したかどうかにかかわらず、メモ関連のエントリが作成されます。メモを追加せずにカタログを更新した場合、エントリはnull (-) と表示されます。イメージのメモ履歴を表示するには、カタログを選択し、下部のペインで をクリックしてから、 をクリックします。

5. 「**ロールアウト戦略**」ページで、マシンカタログ内のマシンを新しいマスターイメージで更新するタイミング（次回のシャットダウン時または即時）を選択します。

> 「**注：**」:
>
> 「**ロールアウト戦略**」ページは、ロールアウトが非永続VMにのみ適用されるため、永続VMでは利用できません。

6. 「**概要**」ページで情報を確認し、「**完了**」をクリックします。各マシンは更新後に自動的に再起動します。

更新の進行状況を追跡するには、「**マシンカタログ**」でカタログを見つけ、インラインの進行状況バーと段階的な進行状況グラフを表示します。

Web StudioではなくPowerShell SDKを直接使用してカタログを更新する場合は、ハイパーバイザーテンプレート（**VMTemplates**）を指定します。これは、イメージまたはイメージのスナップショットの代替として使用します。

「**ロールアウト戦略：**」:

次回のシャットダウン時にイメージを更新すると、現在使用されていないマシン、つまりアクティブなユーザーセッションがないマシンにすぐに影響します。使用中のシステムは、現在のアクティブセッションが終了したときに更新を受け取ります。以下を考慮してください。

- 該当するマシンでの更新が完了するまで、新しいセッションは起動できません。
- シングルセッションOSマシンでは、マシンが使用されていないとき、またはユーザーがログインしていないときに、マシンはすぐに更新されます。

- 子マシンを持つマルチセッションOSの場合、再起動は自動的に行われません。更新されたマスターイメージを適用するには、Studio、PowerShell、またはWorkspaceを使用してマシンを再起動します。マシンまたはハイパーバイザーからの再起動では、更新は適用されません。

> 「ヒント：」:

> ホスト接続の詳細設定を使用して、再起動されるマシンの数を制限します。これらの設定を使用して、特定のカタログに対して実行されるアクションを変更します。詳細設定はハイパーバイザーによって異なります。

マスターイメージをロールバックする

更新された、または新しいマスターイメージを展開した後、それをロールバックできます。このプロセスは、新しく更新されたマシンで問題が発生した場合に必要になることがあります。ロールバックすると、カタログ内のマシンは最後に正常に動作していたイメージにロールバックされます。新しいイメージを必要とする新機能は利用できなくなります。展開と同様に、マシンのロールバックには再起動が含まれます。

1. Web Studio にサインインします。
2. 左側のペインで を選択します。
3. カタログを選択し、アクションバーで を選択します。
4. ロールアウト操作の前のセクションで説明されているように、以前のマスターイメージをマシンに適用するタイミングを指定します。

ロールバックは、元に戻す必要があるマシンにのみ適用されます。新しいまたは更新されたマスターイメージで更新されていないマシンは、通知メッセージを受信せず、強制的にログオフされることもありません。

ロールバックの進行状況を追跡するには、 でカタログを見つけ、インラインの進行状況バーと段階的な進行状況グラフを表示します。

機能レベルを変更する、または変更を元に戻す

マシンの VDA を新しいバージョンにアップグレードした後、マシンカタログの機能レベルを変更します。Citrix は、すべての最新機能にアクセスできるように、すべての VDA を最新バージョンにアップグレードすることをお勧めします。

マシンカタログの機能レベルを変更する前に、次の点に注意してください。

- アップグレードされたマシンを起動して、Controller に登録します。このプロセスにより、Web Studio はカタログ内のマシンがアップグレードを必要としていることを判断できます。

カタログの機能レベルを変更するには：

1. Web Studio にサインインします。
2. 左側のペインで を選択します。
3. カタログを選択します。下部のペインの タブにバージョン情報が表示されます。
4. を選択します。Web Studio がカタログのアップグレードが必要であると検出した場合、メッセージが表示されます。プロンプトに従います。1 台以上のマシンをアップグレードできない場合、その理由を説明するメッセージが表示されます。すべてのマシンが正常に機能するように、Citrix は をクリックして続行する前に、マシンの問題を解決することをお勧めします。

カタログの変更が完了したら、カタログを選択し、アクションバーで**機能レベルの変更を元に戻す**を選択することで、マシンを以前のVDAバージョンに戻すことができます。

カタログをクローンする

カタログをクローンする前に、以下の考慮事項に注意してください。

- オペレーティングシステムおよびマシン管理に関連する設定は変更できません。クローンされたカタログは、元のカタログからこれらの設定を継承します。
- カタログのクローン作成には時間がかかる場合があります。必要に応じて、**進行状況を非表示**を選択して、バックグラウンドでクローン作成を実行します。
- クローンされたカタログは元のカタログの名前を継承し、サフィックス`Copy`が付きます。名前は変更できます。カタログの名前を変更するを参照してください。
- クローン作成が完了したら、クローンされたカタログをデリバリーグループに割り当ててください。

1. Web Studioにサインインし、左ペインで**マシンカタログ**を選択します。
2. カタログを選択し、アクションバーで**クローン**を選択します。
3. **選択したマシンカタログのクローン**ウィンドウで、クローンされたカタログの設定を表示し、必要に応じて設定を構成します。**次へ**を選択して次のページに進みます。
4. **概要**ページで、設定の概要を確認し、**完了**を選択してクローン作成を開始します。
5. 必要に応じて、**進行状況を非表示**を選択して、バックグラウンドでクローン作成を実行します。

フォルダーを使用してカタログを整理する

フォルダーを作成してカタログを整理し、簡単にアクセスできるようにすることができます。たとえば、イメージタイプ別や組織構造別にカタログを整理できます。

> **ヒント:**
>
> アクションバーの右上にある**フォルダー**アイコンをクリックすると、マシンカタログノードの優先デフォルトビュー（フォルダービューまたはリストビュー）を設定できます。

カタログフォルダーを作成する

開始する前に、まずカタログの整理方法を計画してください。次の点を考慮してください。

- フォルダーは最大5レベルまでネストできます（デフォルトのルートフォルダーを除く）。
- カタログフォルダーには、カタログとサブフォルダーを含めることができます。
- Web Studioのすべてのノード（**マシンカタログ**、**デリバリーグループ**、**アプリケーション**、**アプリケーショングループ**など）は、バックエンドで同じフォルダーツリーを共有します。フォルダーの名前変更や移動の際に名前の競合を避けるため、異なるノード間で最上位フォルダーには一意の名前を使用してください。

  `New-BrokerAdminFolder` SDKコマンドレットを使用してフォルダーを作成し、それを**マシンカタログ**ノードの下に表示させたい場合は、`Set-BrokerAdminFolderMetadata`コマンドレットを使用して`ContainsMachineCatalogs`メタデータを追加する必要があります。

  例:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsMachineCatalogs -Value true
  ```

カタログフォルダーを作成するには、次の手順に従います。

1. 左側のペインで**Machine Catalogs**を選択します。
2. フォルダー階層でフォルダーを選択し、**アクション**バーで**フォルダーの作成**を選択します。
3. 新しいフォルダーの名前を入力し、**完了**をクリックします。

> **ヒント:**

> 意図しない場所にフォルダーを作成した場合でも、正しい場所にドラッグして移動できます。

カタログを移動する

カタログはフォルダー間で移動できます。詳細な手順は次のとおりです。

1. 左ペインで**マシンカタログ**を選択します。
2. フォルダーごとにカタログを表示します。フォルダー階層の上にある**すべて表示**をオンにして、すべてのカタログを一度に表示することもできます。
3. カタログを右クリックし、**マシンカタログの移動**を選択します。
4. カタログの移動先のフォルダーを選択し、**完了**をクリックします。

> **ヒント:**

> カタログをフォルダーにドラッグできます。

カタログフォルダーの管理

カタログフォルダーの削除、名前の変更、移動ができます。

フォルダーとそのサブフォルダーにカタログが含まれていない場合にのみ、フォルダーを削除できます。

フォルダーを管理するには、以下の手順に従います。

1. 左側のペインで**Machine Catalogs**を選択します。
2. フォルダー階層でフォルダーを選択し、必要に応じて**アクション**バーでアクションを選択します。
    - フォルダーの名前を変更するには、**フォルダー名の変更**を選択します。
    - フォルダーを削除するには、**フォルダーの削除**を選択します。
    - フォルダーを移動するには、**フォルダーの移動**を選択します。
3. 画面の指示に従って、残りの手順を完了します。

カタログ作成を再試行する

> **注:**
>
> この機能はMCSカタログにのみ適用されます。

> 失敗したカタログにはエラーアイコンが表示されます。詳細を確認するには、各カタログの**トラブルシューティング**タブに移動します。カタログの作成を再試行する前に、以下の考慮事項に注意してください。

- まずトラブルシューティング情報を確認し、問題を解決してください。この情報には、見つかった問題が記述されており、それらを解決するための推奨事項が提供されています。
- オペレーティングシステムおよびマシン管理に関連する設定は変更できません。カタログは、元の設定を継承します。
- 作成には時間がかかる場合があります。必要に応じて、**進行状況を非表示**を選択して、バックグラウンドで作成を実行します。

カタログの作成を再試行するには、次の手順を実行します。

1. Web Studioから、左側のペインで**マシンカタログ**を選択します。
2. カタログを選択し、その**トラブルシューティング**タブに移動します。
3. 再試行ハイパーリンクをクリックして、カタログの作成を再試行します。
4. 表示されるウィザードで、必要に応じて設定を変更します。変更する必要がない場合は、直接**概要**ページに移動できます。
5. 完了したら、**完了**を選択して作成を開始します。

トークンを使用して非MCSプロビジョニングVDAを登録する（プレビュー）

MCSでプロビジョニングされていないVDAの登録トークンを生成および管理できるようになりました。この実装により、MCSでVDAをプロビジョニングすることなく、WebSocket経由でVDAを登録できます。この機能は、Linux Virtual Delivery Agent、macOS用Citrix Virtual Delivery Agent、およびCitrix Virtual Apps and Desktopsを使用するドメインに参加していないVDAもサポートします。

始める前に

1. サイトを構成します。詳細については、「サイトの作成」を参照してください。
2. Delivery ControllerにTLS証明書をインストールします。詳細については、「ControllerにTLSサーバー証明書をインストールする」を参照してください。

3. Delivery Controllerを信頼するために、VDAにルートCAと中間CAをインストールします。
4. Delivery ControllerでWebSocket接続を有効にします。サイトにある各Delivery Controllerで次のコマンドを実行します。

```
New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy"
-Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -Force
```

> **注:**
>
> WebSocketを有効にした後、Delivery Controllerを再起動してください。

登録トークンの生成

Citrix以外でプロビジョニングされたマシン向けにトークンベースの登録を有効にすることを決定したら、まずマシンカタログごとにトークンを生成し、その後、VDAインストール管理者と共有する必要があります。

登録トークンの特徴：

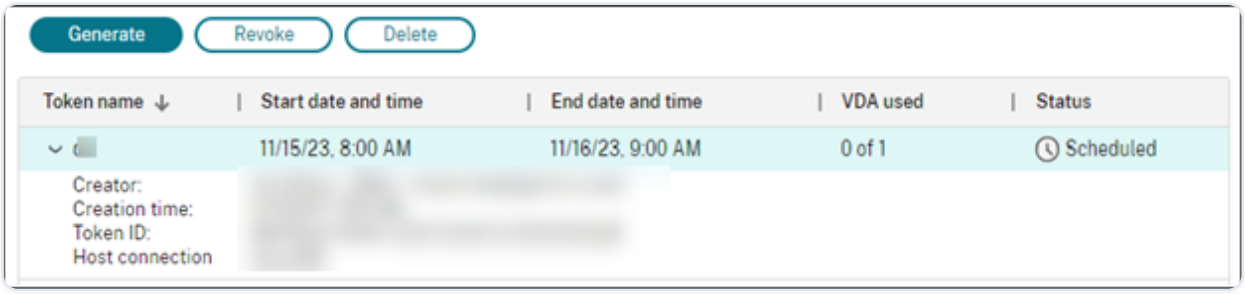
- 登録範囲: 1〜100台のVDAマシン
- 有効期間：最大14日間

Web Studioを使用してカタログのトークンを生成するには、次の手順に従います。

1. 「**Web Studio > Machine Catalogs**」で、非MCSプロビジョニングカタログを見つけます。このカタログには、「**Machine Count**」列に「**Provisioning method: Manual**」と表示されています。
2. カタログを右クリックし、「**Manage Enrollment Tokens**」を選択します。
3. 表示される「**Generate enrollment token**」ページで、以下のトークン情報を提供します。
   - トークンの名前を入力します。
   - 有効期間を入力します。期間は14日以内である必要があります。トークンは指定された期間のみ有効です。
   - (オプション) トークンで登録されたVDAの電源管理のためにホスト接続を選択します。オプションには、このカタログのゾーン下のすべてのホスト接続が含まれます。
   - トークンの使用制限を入力します (1〜100)。
4. 「**Generate**」をクリックします。

5. 表示される「**Token successfully generated**」ウィンドウで、トークンをコピーして安全な場所に保存するか、「**Download**」をクリックして「**Downloads**」フォルダーにダウンロードします。

   トークンリストにトークンレコードが表示されます。



6. トークンをVDAインストール管理者と共有します。

   マシンにVDAとトークンをインストールする方法の詳細については、「Install VDAs」を参照してください。

トークンの管理

トークンを取り消し、VDA登録に使用できないようにするには、2つのオプションがあります。

- 取り消し: トークンを取り消しますが、ログ記録のためにリストに残します。
- 削除: トークンを取り消し、リストから削除します。

> **注記:**
>
> 期限切れのトークンは14日後に自動的に削除されます。

WebSocket VDA登録ツールを使用してマシンをカタログに登録する

WebSocket VDA登録ツールは、VDAマシンのトークンベースの登録を容易にします。このツールは、登録トークンを使用してVDAをマシンカタログに追加することで、接続をWebSocket接続に変換するのに役立ちます。

> **注記:**
>
> このツールは、どのマシンカタログにも登録されていないVDAマシンを登録するように設計されています。

> 登録ツールを実行するには、以下の手順に従ってください。

1. VDAにログオンします。
2. `C:\Program Files\Citrix\Virtual Desktop Agent\Web Socket Vda Enrollment Tool` にあるツール `EnrollMachine.exe` を見つけます。
3. 適切な入力パラメーターを指定してツールを実行します。例: `EnrollMachine.exe -websocket_token_string:xxxxxxxxx`

次の表は、登録ツールの入力パラメータについて説明しています。

パラメータ名	必須	説明	例
`-websocket_token_stdin`	はい	登録トークンを読み取ります。	`.\EnrollMachine.exe -websocket_token_stdin`
`-websocket_token_string`		コマンドラインパラメータから登録トークンを直接読み取ります。	`.\EnrollMachine.exe -websocket_token_string:<token>`
`-websocket_token_file:[token-file-path]`		指定されたパスから登録トークンを読み取ります。	`.\EnrollMachine.exe -websocket_token_file:C:\token\test2.txt`
`log:[log-file-path]`	いいえ	登録ツールのログを表示します。	`.\EnrollMachine.exe log:[C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt]`

パラメータ名	必須	説明	例
`-help`	いいえ	短いヘルプテキストを表示します。	`.\EnrollMachine.exe -help`

登録が成功すると、ツールとログに成功メッセージが表示されます。Web Studioにサインインして、VDAマシンがカタログに追加され、マシンのステータスが登録済みであることを確認してください。

トラブルシューティング

デフォルトでは、登録ツールのログは次の場所にあります。

`C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt`

ログに別のパスを指定した場合は、`log:[log-file-path]` を使用してログを取得できます。

次の表に、登録ツールによって返されるコードを示します。

コード	文字列	説明
0	成功	VDAがマシンカタログに正常に追加されました。
-1	無効な引数	登録トークン内の入力パラメーターが無効です。
-2	ブローカーエージェントが見つかりません	ブローカーエージェントサービスが見つかりません。
-3	トークンが無効です	入力されたトークンが無効です。
-4	トークンに必須のクレームがありません	トークンに必要なクレーム（例: CustomerId、Enrollment URIs）がありません。
-5	InternalError	一般的なエラーが発生しました。

コード	文字列	説明
-6	TimedOut	タスクがタイムアウトしました。
-7	FailedToDetermineMachineADJoinedStatus	マシンのAD参加ステータスを返すサービスが失敗しました。
-8	ADMachineFailedToFindSid	ADマシンのSidを返すサービスが失敗しました。
-9	EnrollRequestFailed	HTTPエラーによりリクエストが失敗しました。
-10	EnrollResponseMissingRequiredFields	登録ツールの応答にパラメーター `VirtualSiteId` がありません。
-11	InsufficientPermission	タスクを実行するために必要な権限がありません。
-12	FailedToDetermineMachineAadJoinedStatus	マシンのAD参加ステータスを確認するサービスがエラーをスローしました。
-13	AadMachineFailedToFindDeviceId	システムによって追加された追加パラメーター `AAD device id` が空です。
-14	AadDeviceIdNotValid	システムによって追加された追加パラメーター `AAD device id` は有効な GUID ではありません。
-15	NoValidMacAddress	無効な MAC アドレスです。
-16	FailedToGetComputerHostNameForVdaInstanceName	追加パラメーター `VdaInstanceName` を設定するためのコンピューターホスト名の取得に失敗しました。

コード	文字列	説明
-17	VirtualDesktopAgentRegistryKeyFailedToOpen	デリバリーコントローラーのリストを書き込むためのVDA レジストリキーを開けませんでした。
-18	失敗したトークンが最大数に達しました	失敗したトークンが最大数に達しました。

PowerShell を使用する

このセクションでは、PowerShellを使用してカタログを管理する方法について詳しく説明します。

- カタログに関連付けられている警告とエラーを取得する(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-manage.html#retrieve-warnings-and-errors-associated-with-a-catalog)
- イメージに説明を追加する
- OSディスクをリセットする
- 既存のプロビジョニングスキームのネットワーク設定を変更する
- マシンカタログのバージョンを管理する(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-manage.html#manage-versions-of-a-machine-catalog)
- マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換する(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-manage.html#convert-a-non-machine-profile-based-machine-catalog-to-machine-profile-based-machine-catalog)
- アクティブなコンピューターアカウントのID情報を修復する(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-manage.html#repair-the-identity-information-of-active-computer-accounts)
- 既存のマシンカタログのキャッシュ構成を変更する(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-manage.html#change-cache-configuration-on-an-existing-machine-catalog)
- ローカルファイル共有アクセスによるVDA更新のサポート(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-manage.html#vda-update-support-via-local-file-share-access)

カタログに関連付けられた警告とエラーを取得する

履歴エラーと警告を取得して、MCSマシンカタログの問題を把握し、それらの問題を修正できます。

PowerShellコマンドを使用して、次のことができます。

- エラーまたは警告のリストを取得する
- 警告の状態を**新規**から**確認済み**に変更する
- エラーまたは警告を削除する

PowerShellコマンドを実行するには:

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。

エラーと警告のリストを取得するには：

`Get-ProvOperationEvent` コマンドを実行します。

- パラメーターなしの場合：すべてのエラーと警告を取得します
- `LinkedObjectType` および `LinkedObjectUid` パラメーターを使用する場合：特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告を取得します
- `EventId` パラメーターを使用する場合：このイベント ID に一致する特定のエラーまたは警告を取得します
- `Filter`パラメーターを使用: カスタマイズされたフィルターでエラーまたは警告を取得します

エラーまたは警告の状態を **New** から **Acknowledged** に変更するには：

`Confirm-ProvOperationEvent` コマンドを実行します。

- `EventId`パラメーターを使用：このイベントIDに一致する特定のエラーまたは警告の状態を設定します。特定のイベントまたは警告の`EventId`は、`Get-ProvOperationEvent`コマンドの出力として取得できます。
- `LinkedObjectType`および`LinkedObjectUid`パラメーターを使用：特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告の状態を設定します
- `All`パラメーターを使用：すべてのエラーと警告の状態を**確認済み**に設定します

エラーまたは警告を削除するには：

`Remove-ProvOperationEvent` コマンドを実行します。

- `EventId` パラメーターを使用: このイベント ID に一致する特定のエラーまたは警告を削除します。特定のイベントのエラーまたは警告の `EventId` は、`Get-ProvOperationEvent` コマンドの出力として取得できます。
- `LinkedObjectType` と `LinkedObjectUid` パラメーターを使用: 特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告を削除します。
- `All` パラメーターを使用: すべてのエラーと警告を削除します。

詳細については、Citrix PowerShell SDK を参照してください。

ハイパーバイザーアクセスなしでマシンを削除する

VM またはプロビジョニングスキームを削除する場合、MCS は VM から、場合によってはベースディスクからもタグを削除する必要があります。これにより、削除オプションに含まれるリソースが MCS によって追跡または識別されなくなります。ただし、これらのリソースの一部はハイパーバイザーを介してのみアクセス可能です。ハイパーバイザーアクセスがない場合でも、データベースから VM、ベースディスク、ACG 内のイメージなどの VM リソースオブジェクトを削除するには、`Remove-ProvVM` PowerShell の `PurgeDBOnly` オプションを使用します。

このオプションは以下で有効になります。

- サポートされているすべてのハイパーバイザー
- 永続VMと非永続VM

制限事項

-PurgeDBOnly コマンドと -ForgetVM コマンドを同時に使用することはできません。

PurgeDBOnly コマンドを使用する

PowerShell コマンド `Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -ForgetVM` を実行すると、次のようなシナリオで削除操作が失敗する可能性があります。

- ホスト接続がメンテナンスモードになっている
- 無効な資格情報
- 認証失敗
- 許可されていない操作
- ハイパーバイザーに到達できません

> **注:**
>
> Remove-provVM -ForgetVM は永続VMのみを対象とします。リスト内のVMのいずれかが非永続である場合、操作は失敗します。
>
> ハイパーバイザーに到達できないために操作が失敗した場合、次のプロンプトが表示されます。

`Try to use -PurgeDBOnly option to clean DDC database.`.

MCSデータベースからVMの参照を削除するには、`Remove-ProvVM` PowerShellコマンドで`-PurgeDBOnly`オプションを使用します。例：

```
Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -PurgeDBOnly
```

イメージに説明を追加する

マシンカタログのイメージ更新に関連する変更について、情報提供の記述を追加できます。この機能を使用して、カタログの作成時、またはカタログの既存のマスターイメージを更新する際に説明を追加します。カタログ内の各マスターイメージの情報を表示することもできます。イメージの説明を追加または表示するには、次のコマンドを使用します。

- マスターイメージを使用してマシンカタログを作成する際にメモを追加するには、`NewProvScheme`コマンドでパラメーター`MasterImageNote`を使用します。例：

  ```
  C:\PS>New-ProvScheme -ProvisioningSchemeName <name> -HostingUnitName
  <name> -IdentityPoolName <name> -MasterImageVM

  XDHyp:\HostingUnits\<hosting unit name>\<vm name>.vm\Base.snapshot
  -MasterImageNote "Note"
  ```

- マシンカタログに関連付けられているマスターイメージを更新するには、`Publish-ProvMasterVMImage`コマンドでパラメーター`MasterImageNote`を使用します。例：

  ```
  C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName <name>
  -MasterImageVM XDHyp:\HostingUnits\<hosting unit name>\<vm
  name>.vm\base.snapshot -MasterImageNote "Note"
  ```

- 各イメージの情報を表示するには、Get-ProvSchemeMasterVMImageHistoryコマンドを使用します。例：

```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
MyScheme -Showall
```

ロールバックの進行状況を追跡するには、**マシンカタログ**でカタログを見つけて、インラインの進行状況バーと段階的な進行状況グラフを表示します。

次のシナリオを含む特定の状況では、ロールバックできません。（**マスターイメージのロールバック**オプションは表示されません）。

- ロールバックする権限がありません。
- カタログがMCSを使用して作成されていません。
- カタログがOSディスクのイメージを使用して作成されました。
- カタログの作成に使用されたスナップショットが破損しています。
- カタログ内のマシンに対するユーザーの変更が保持されません。
- カタログ内のマシンが実行中です。

OSディスクをリセットする

MCSで作成されたマシンカタログ内の永続VMのOSディスクをリセットするには、PowerShellコマンド`Reset-ProvVMDisk`を使用します。現在、この機能はAWS、Azure、XenServer、Google Cloud、SCVMM、VMwareの仮想化環境に適用できます。

PowerShellコマンドを正常に実行するには、以下を確認してください。

- ターゲットVMが永続的なMCSカタログにあります。
- MCSマシンカタログが正常に機能しています。
- これは、プロビジョニングスキームとホストが存在し、プロビジョニングスキームに正しいエントリがあることを意味します。
- ハイパーバイザーがメンテナンスモードではありません。
- ターゲットVMは電源オフされ、メンテナンスモードになっています。

OSディスクをリセットするには、次の手順を実行します。

1. PowerShell ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、**asnp citrix***を実行します。

3. 次のいずれかの方法でPowerShellコマンド`Reset-ProvVMDisk`を実行します。

   - VMのリストをコンマ区切りリストとして指定し、各VMでリセットを実行します。

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc","def")
     -OS
     ```

   - `Get-ProvVM`コマンドからの出力としてVMのリストを指定し、各VMでリセットを実行します。

     ```
     (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk "abc"
     -OS
     ```

   - 名前で単一のVMを指定します。

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
     ```

   - `Get-ProvVM`コマンドによって返される各VMに対して個別のリセットタスクを作成します。各タスクがハイパーバイザー機能チェック、各VMの接続チェックなど、同じ冗長なチェックを実行するため、これは効率的ではありません。

     ```
     Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk
     -ProvisioningSchemeName "xxx" -OS
     ```

4. リセットされるVMのリストと、回復不能な操作であるという警告メッセージが表示される確認プロンプトが表示されます。回答を入力せずに**Enter**キーを押すと、それ以上の操作は行われません。

   注:

   リセットプロセスが完了するまで、VMをメンテナンスモードから解除したり、電源をオンにしたりしないでください。

   PowerShellコマンド`-WhatIf`を実行して、実行されるアクションを表示し、アクションを実行せずに終了することができます。

   次のいずれかの方法を使用して、確認プロンプトをバイパスすることもできます。

- `-Force` パラメーターを指定します。

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
-Force
```

- `-Confirm:$false` パラメーターを指定します。

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
-Confirm:$false
```

- `Reset-ProvVMDisk` を実行する前に、`$ConfirmPreference` を**None**に変更します。

```
PS C:\Windows\system32> $ConfirmPreference='None'

PS C:\Windows\system32> $ConfirmPreference

None

PS C:\Windows\system32> Reset-ProvVMDisk -ProvisioningSchemeName
"xxx" -VMName "abc" -OS
```

5. `Reset-ProvVMDisk` コマンドによって返されるタスクのステータスを取得するには、`Get-ProvTask` を実行します。

既存のプロビジョニングスキームのネットワーク設定を変更する

既存のプロビジョニングスキームのネットワーク設定を変更して、新しいVMが新しいサブネットワーク上に作成されるようにすることができます。ネットワーク設定を変更するには、`Set-ProvScheme` コマンドで `-NetworkMapping` パラメーターを使用します。

注:

この機能は、Citrix Virtual Apps and Desktops 2203 LTSR CU3以降のバージョンでサポートされています。

既存のプロビジョニングスキームのネットワーク設定を変更するには、次の手順を実行します。

1. PowerShellウィンドウで、`asnp citrix*`コマンドを実行してPowerShellモジュールをロードします。
2. 変更するネットワークパスを取得するには、`(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps`を実行します。
3. 新しいネットワーク設定に変数を割り当てます。例：

```
$NewNetworkMap = @{"0"= "XDHYP:\HostingUnits\MyNetworks\Network
0.network"}
```

4. `Set-ProvScheme -ProvisioningSchemeName "name" -NetworkMapping $NewNetworkMap`を実行します。
5. 既存のプロビジョニングスキームの新しいネットワーク設定を確認するには、`(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps`を実行します。

マシンカタログのバージョンを管理する

`Set-ProvScheme`コマンドでMCSマシンカタログが更新されると、現在の構成がバージョンとして保存されます。その後、PowerShellコマンドを使用してマシンカタログのさまざまなバージョンを管理できます。次のことができます。

- マシンカタログのバージョンの一覧を表示する
- 以前のバージョンを使用してマシンカタログを更新する
- そのマシンカタログのVMで使用されていないバージョンは手動で削除する
- マシンカタログが保持するバージョンの最大数を変更する（デフォルトは99）

バージョンには、マシンカタログの次の情報が含まれます。

- VMCpuCount
- VMMemoryMB
- CustomProperties
- ServiceOffering
- MachineProfile
- NetworkMapping
- SecurityGroup

マシンカタログのさまざまなバージョンを管理するには、次のコマンド（例として提供）を実行します。

- マシンカタログのさまざまなバージョンの構成の詳細を表示するには：

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
```

- マシンカタログの特定のバージョンの構成の詳細を表示するには：

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version 2
```

- マシンカタログに関連付けられているバージョンの総数を確認するには：

```
(Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count
```

- 以前のバージョンを使用してマシンカタログを更新するには：

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
```

- そのマシンカタログのVMによって使用されていないバージョンを手動で削除するには：

```
Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version
3
```

- マシンカタログが保持する最大バージョン数を設定するには（デフォルトは99）。この設定はすべてのカタログに適用されます。たとえば、この場合、すべてのMCSプロビジョニング済みカタログに対して最大15バージョンが保持されます。

```
Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -Value
15
```

バージョン数が最大バージョン数に達した場合、マシンカタログ内のいずれかのVMで古いバージョンが使用されていると、新しいバージョンを作成できません。その場合は、次のいずれかを実行してください。

- マシンカタログによって保持される最大バージョン数の制限を増やします。
- 古いバージョンを使用している一部のVMを更新して、それらの古いバージョンがどのVMからも参照されなくなり、削除できるようにします。

マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換する

VM、テンプレート仕様（Azureの場合）、または起動テンプレート（AWSの場合）をマシンプロファイルの入力として使用して、マシンプロファイルに基づかないマシンカタログをマシンプロファイルに基づくマシンカタログに変換できます。カタログに追加された新しいVMは、明示的なカスタムプロパティによって上書きされない限り、マシンプロファイルからプロパティ値を取得します。

> **注:**
>
> 既存のマシンプロファイルベースのマシンカタログを、マシンプロファイルベースではないマシンカタログに変更することはできません。

これを行うには：

1. VMを含む、マシンプロファイルなしの永続的または非永続的なマシンカタログを作成します。
2. **PowerShell**ウィンドウを開きます。
3. `Set-ProvScheme`コマンドを実行して、マシンプロファイルからのプロパティ値を、マシンカタログに追加された新しいVMに適用します。例:

   - Azureの場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile XDHyp:
     \HostingUnits\<HostingUnitName>\machineprofile.folder\<ResourceGroup
     Name>\<TemplateSpecName>\<VersionName>
     ```

   - AWSの場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile "XDHyp:
     \HostingUnits\<hosting-unit>\<launch-
     template>.launchtemplate\<launch-template-
     version>.launchtemplateversion"
     ```

アクティブなコンピューターアカウントのID情報を修復する

ID関連の問題があるアクティブなコンピューターアカウントのID情報をリセットできます。マシンパスワードと信頼キーのみをリセットするか、IDディスクのすべての構成をリセットするかを選択できます。この実装は、永続的および非永続的な両方のMCSマシンカタログに適用できます。

> **注:**
>
> 現在、この機能はAWS、GCP、Azure、SCVMM、XenServer、およびVMwareの仮想化環境でサポートされています。

条件

IDディスクを正常にリセットするには、以下を確認してください。

- VMをシャットダウンし、メンテナンスモードに設定します
- PowerShellコマンドにパラメーター-OSを含めないでください

IDディスクのリセット

IDディスクをリセットするには：

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*` を実行して、Citrix固有のPowerShellモジュールをロードします。
3. ID情報をリセットします。
   - マシンのパスワードと信頼キーのみをリセットするには、次のコマンドを実行します。

     ```
     Repair-AcctIdentity -IdentityAccountName TEST\VM1
     -PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
     -Target IdentityInfo
     ```

     コマンドで使用されるパラメーターの説明は次のとおりです。

     - IdentityAccountName: 修復する必要があるIDアカウントの名前。
     - PrivilegedUserName: IDプロバイダー (ADまたはAzureAD) に対する書き込み権限を持つユーザーアカウント。
     - PrivilegedUserPassword: PrivilegedUserNameのパスワード。

    - Target: 修復アクションのターゲット。アカウントのパスワード/信頼キーを修復するためのIdentityInfo、およびHybrid AzureADに参加しているマシンIDのユーザー証明書属性を修復するためのUserCertificateを指定できます。

- IDディスクのすべての構成をリセットするには、次のコマンドを次の順序で実行します。

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1
-PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
-Target IdentityInfo
```

```
Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>  -
Identity
```

- IDディスクを完全に再作成するには:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name>
-Identity -Recreate
```

4. アクションを確定するには「**y**」と入力します。`-Force`パラメーターを使用して確認プロンプトをスキップすることもできます。例：

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name>
-Identity -Force
```

5. 更新されたIDディスク設定を確認するには、`Get-ProvVM -ProvisioningSchemeName <name -VMName <name>`を実行します。IDディスクの属性（例: `IdentityDiskId`）は更新されている必要があります。`StorageId`と`IdentityDiskIndex`は変更されていてはなりません。

既存のマシンカタログのキャッシュ構成を変更する

MCSIOを有効にして非永続カタログを作成した後、Set-ProvSchemeコマンドを使用して以下のパラメータを変更できます。

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

この機能は現在、以下に適用されます。

- GCPおよびMicrosoft Azure環境、および

- MCSIOが有効な非永続カタログ

要件

キャッシュ構成を変更するための要件は次のとおりです。

- VDA を最新バージョン (2308 以降) に更新します。
- 既存のマシンカタログでパラメーター `UseWriteBackCache` を有効にします。`UseWriteBackCache` が有効なマシンカタログを作成するには、`New-ProvScheme` を使用します。例:

```
New-ProvScheme -ProvisioningSchemeName $CatalogName -HostingUnitUid
$HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

-MasterImageVM $MasterImage `

-ServiceOffering $ServiceOffering `

-NetworkMap $NetworkMap `

-SecurityGroup $SecurityGroup `

-UseWriteBackCache -WriteBackCacheDiskSize 8
```

キャッシュ構成を変更する

Set-ProvSchemeコマンドを実行します。例:

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.ProvisioningSchemeName
-WriteBackCacheDisk32 -WriteBackCacheMemorySize 128
```

注:

- `WriteBackCacheDiskSize` の値は、少なくとも 1 GB のキャッシュディスクストレージが必要なため、ゼロより大きい値である必要があります。

- `WriteBackCacheMemorySize` の値は、マシンカタログのメモリサイズよりも小さい値である必要があります。
- これらの変更は、変更後にカタログに追加された新しい VM にのみ影響します。既存の VM はこれらの変更の影響を受けません。

ローカルファイル共有アクセスによるVDAアップデートのサポート

PowerShellコマンドレットを介してVDAインストーラーの場所を指定することで、各VDAがCitrix Managed Azure CDNから新しいVDAインストーラーを取得できるようにするためのネットワークルールを提供する手間を省くことができます。

PowerShellコマンドレット

ローカルファイル共有からインストーラーを使用できるようにする、**New-VusCatalogSchedule**および**New-VusMachineUpgrade**コマンドレットに追加された2つの新しいオプションパラメーター

- **VdaWorkstationPackageUri** - ワークステーションOS VDAインストーラーへのUNCパスを指定します。
- **VdaServerPackageUri** - サーバーOS VDAインストーラーへのUNCパスを指定します。

前提条件

- VDA 2311に付属するVUSエージェントインストーラー
- VDAアップグレードエージェントをバージョン7.40.0.35以降にアップグレードする（VDAインストーラーバージョン2311以降を使用）
- Virtual Apps and Desktops Remote PowerShell SDK バージョン 7.40 以降 (Jan 10, 2024 以降にリリース)

ファイル共有のアクセス許可を設定する方法

VDAインストーラーパッケージを含むネットワーク共有には、ローカルシステム（NT AUTHORITY\SYSTEMプリンシパル）として実行されるVDAアップグレードエージェントサービスに対する読み取りアクセス権が必要です。

- **ドメイン参加済みファイル共有権限**

  VDAマシンがドメインに参加している場合、**ローカルシステム**アカウント（VUAはローカルシステムとして実行されます）は、ネットワーク共有にアクセスする際にコンピューターの資格情報を使用します。

最小特権のアクセス許可は、Domain Computers に **読み取り** アクセスを付与することで設定できます。

a. ファイルを共有するネットワーク上のユーザーを選択します。

b. **詳細な共有設定** をクリックし、**ファイルとプリンターの共有** をオンにします。

- **ドメイン非参加ファイル共有権限**

VDA マシンがドメインに参加していない場合、**ローカルシステム** アカウント (VUA はローカルシステムとして実行されます) は、ネットワーク共有にアクセスするときに **ANONYMOUS LOGON** を使用します。

a. 共有フォルダーを選択します。

b. パスワード保護を無効にします。

   a. フォルダーの**プロパティ**に移動します。

   b. **ネットワークと共有センター**を選択します。

   c. **パスワード保護共有**をオフにします。

c. 共有アクセス許可を付与するには、**詳細な共有**をクリックします。

   a. **アクセス許可**を選択します。

   b. **匿名ログオン**に**読み取り**共有アクセス許可を付与します。

d. フォルダーのアクセス許可を付与するには、**セキュリティ**タブを選択します。

   a. 共有フォルダーにアクセス許可を追加するには、**編集**をクリックします。

   b. **匿名ログオン**にフォルダーのアクセス許可を付与するには、共有フォルダーを選択します。

e. **ファイルとプリンターの共有**をオンにするには、**詳細設定**をクリックします。

f. 共有フォルダー名を**ネットワークアクセスセキュリティポリシー**に追加します。

> **注：**
>
> 変更をすぐに有効にするには、マシンを再起動します。

ローカルファイル共有からのVDAアップデート

1. VDAインストーラーをダウンロードし、共有ファイルに配置します。

> **注:**
>
> Virtual Upgrade Serviceを使用すると、Current ReleaseトラックまたはLTSRトラックのいずれかを選択できます。
>
> **例:** マシンカタログがCurrent Release（2311）に設定されており、VDAバージョンが2305の場合、VDAをバージョン2311にアップグレードする必要があります。

a. 弊社のWebサイトの**ダウンロード**ページに移動します。
b. 製品として**Citrix Virtual Apps and Desktops**を選択します。
c. **シトリックス バーチャル アプリケーションズ アンド デスクトップス 7 2311, All Editions**を選択します。
d. 展開可能な**製品ISOに含まれるが個別にパッケージ化されているコンポーネント**からVDAインストーラーを選択します。

2. カタログの種類に基づいて、関連するVDAインストーラーを選択します。

- カタログの種類が**マルチセッション**の場合は、**Multi-session OS VDAインストーラー**をダウンロードします。
- カタログの種類が**シングルセッション**の場合は、**Single-session OS VDAインストーラー**をダウンロードします。
- カタログの種類が**Remote PC Access**の場合は、**Single-session OS Core Services VDAインストーラー**をダウンロードします。

> **注:**
>
> ファイル共有インストーラーのバージョンは、VUSがクラウドに公開した最新のインストーラーバージョンのバージョンと**完全に**一致している必要があります。

トラブルシューティング

- 「Power State Unknown」ステータスのマシンについては、ガイダンスとしてCTX131267を参照してください。
- 不明な電源状態を継続的に表示するVMを修正するには、How to fix VMs that continuously show an unknown power stateを参照してください。

次のステップ

特定のクラウドサービスカタログの管理については、以下を参照してください。

- AWSカタログの管理
- XenServerカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-manage/manage-machine-catalog-citrix-hypervisor.html)
- Google Cloud Platformカタログの管理
- Microsoft Azureカタログの管理
- マイクロソフト システムセンター バーチャルマシンマネージャー カタログの管理
- VMwareカタログの管理

AWSカタログを管理する

(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-manage.html)は、マシンカタログを管理するウィザードについて説明しています。以下の情報は、AWSクラウド環境に固有の詳細をカバーしています。

> **注:**
>
> AWSカタログを管理する前に、AWSカタログの作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create/create-machine-catalog-aws.html)を参照してください。

タグを削除する

カタログまたはVMを作成すると、MCSによって作成されたタグが以下のリソースに作成されます。

- 仮想マシン
- ルートディスクボリューム
- 識別ディスクボリューム
- NIC
- ルートディスクイメージ（AMI）
- 起動テンプレート
- AMIまたはルートディスクのスナップショット

Citrix®データベースからVMとマシンカタログを削除し、MCSによって作成されたタグを削除できます。以下を使用できます。

- マシンカタログから単一のVMまたはVMのリストからVMとMCSによって作成されたタグを削除するには、`ForgetVM`パラメーターを指定した`Remove-ProvVM`を使用します。
- `ForgetVM` パラメーターを指定して `Remove-ProvScheme` を実行し、Citrixデータベースからマシンカタログを、マシンカタログからリソースを削除します。

この機能は、永続VMにのみ適用されます。

これを行うには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*` を実行します。
3. VMを削除する前に、VMのロックを解除します。例：

```
Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
```

4. リソースからVM、マシンカタログ、およびMCSで作成されたタグを削除するには、次のいずれかのコマンドを実行します。
   - Citrixデータベースから VMを、VMからタグを削除するには、`ForgetVM` を指定して `Remove-ProvVM` を実行します。例：

```
Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"
-ForgetVM
```

   - Citrixデータベースからマシンカタログを、マシンカタログからリソースを削除するには、`Remove-ProvScheme` を実行します。例：

```
Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -ForgetVM
```

5. VMがDelivery Controller™から削除されていることを確認しますが、ハイパーバイザーからは削除されていません。
   a. `Get-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"` を実行します。これは何も返さないはずです。
   b. AWS EC2コンソールに移動します。VMは表示されますが、タグは削除されています。次のリソースからタグが削除されます。

- 仮想マシン
- ルートディスクボリューム
- 識別ディスクボリューム
- NIC

6. マシンカタログを削除した場合は、そのカタログがDelivery Controllerから削除されていることを確認してください。

   a. `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`を実行します。これはエラーを返すはずです。

   b. AWS EC2コンソールで、以下のリソースが削除されていることを確認します。

      - ルートディスクイメージ (AMI)
      - 起動テンプレート
      - AMIまたはルートディスクのスナップショット

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
IDディスク	"名前": "VMName_IdentityDisk"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
イメージ	"Xd設定": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
NIC	"説明": "XD NIC"
	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

リソース名	タグ
OSディスク	"名前": "VMName_rootDisk"
	"XdConfig": "XdProvisioned=True"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "Citrix リソース": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
PrepVM	"Name": "準備 - カタログ名 - xxxxxxxxxx"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "Citrix リソース": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
公開されたスナップショット	"XdConfig": "XdProvisioned=true"
	ボリュームワーカーAMIのスナップショットでない場合、"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
テンプレート	[when AwsCaptureInstanceProperties = true] タグ: "XdConfig": "XdProvisioned=true"
	[when AwsCaptureInstanceProperties = true] "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

リソース名	タグ
	[when AwsCaptureInstanceProperties = true] "CitrixResource": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
カタログ内のVM	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "CitrixResource": ""
	[when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:id":"lt-xxxx"
	[when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:version": "n"
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
ボリュームワーカーAMI	"XdConfig": "XdProvisioned=true"
ボリュームワーカーブートストラッパー	"Name": "XenDesktop® 一時"
	"XdConfig": "XdProvisioned=true"
	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixVolumeWorkerBootstrapper": ""
ボリュームワーカーインスタンス	"名前": "Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx"

リソース名	タグ
	"Xdコンフィグ": "Xdプロビジョニング済み=true"

詳細情報

- 接続とリソースの作成および管理
- AWSへの接続
- マシンカタログの作成
- AWS カタログを作成する
- マシンカタログの管理

XenServer®カタログを管理する

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、XenServer仮想化環境に固有の詳細を扱います。

> **注：**
>
> XenServerカタログを管理する前に、XenServerカタログの作成を完了する必要があります。「XenServerカタログの作成」を参照してください。

永続VMと非永続VMのストレージ移行

`Move-ProvVMDisk` PowerShellコマンドを使用して、以下のVMディスクをあるストレージから別のストレージに移行できます。

- 永続的なフルクローンVMの場合：OSディスク、IDディスク、およびMCS以外でプロビジョニングされたディスク。
- 非永続VMの場合：OSディスク、IDディスク、およびライトバックキャッシュ（WBC）ディスク。

前提条件

新しいストレージは、以下の条件を満たす必要があります。

- VMが実行されているホストは、古いデータストアと新しいデータストアの両方にアクセスできる必要があります。

制限事項

永続VMと非永続VMを移行する際には、以下の制限事項を考慮してください。

- 永続的なフルクローンVMの場合：移動するVMにスナップショットがある場合、移行後に、追加の統合ディスクがより多くのディスク領域を消費する可能性があります。たとえば、移行前（snapshot1 100G + snapshot2 20G + 10G OSファイル）。移行後（統合ディスク 130G + snapshot1 100G + snapshot2 20G）。
- 非永続VMの場合：スナップショットの移行はサポートされていません。

ディスクストレージの移行

ディスクストレージを移行するには：

1. 既存のホスティングユニットに宛先ストレージを追加します。宛先ストレージを追加するには、PowerShellコマンド `Add-Hyphostingunitstorage` を実行します。

   古いストレージに新しいVMを追加したくない場合は、古いストレージを「置き換え済み」に変更します。これはStudioまたはPowerShellコマンドを使用して実行できます。ストレージの編集 を参照してください。また、古いストレージでの新しいVM作成を無効にするには、`tru` として `Set-Hyphostingunitstorage` と `Superseded` を実行することもできます。

   > **注:**
   >
   > 非永続VMの場合：
   >
   > - WBCを使用する場合は、ホスティングユニットでWBC宛先ストレージを構成します。
   > - OS宛先ストレージが構成されている場合、WBC（使用されている場合）はOS宛先ストレージと互換性がある必要があります。
   > - OS宛先ストレージが構成されていない場合、WBC（使用されている場合）は現在のOSストレージと互換性がある必要があります。

2. VMをシャットダウンし、メンテナンスモードをオンにします。
3. プロビジョニングスキーム、ホスティングユニット、OSディスクストレージ、およびWBCディスクストレージに関する情報を取得します。OSストレージ情報については、`ProvResourceInStorage`を参照してください。例：

```
$result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName xxxxx

$result

$result.ProvResourceInStorage | Format-List -Property *
```

WBCストレージ情報については、`TemporaryStorageInfo`を参照してください。例：

```
$result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName xxxxx

$result

$result.TemporaryStorageInfo | Format-List -Property *
```

4. OSディスク、IDディスク、およびWBCディスク（非永続VMに適用）を`Move-ProvVMDisk PowerShell`コマンドを使用して宛先ストレージに移行します。

> **注:**
>
> - `DiskType`および`DestinationStorageId`パラメーターには、常にOSディスクとIDディスクを指定してください。
> - OSディスクとIDディスクの`DestinationStorageId`は同じである必要があります。

例:

永続VM：

```
(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk
-ProvisioningSchemeName "myFullCloneProvScheme" -VMName "machine01"
-DiskType OS,Identity -DestinationStorageId datastore1,datastore1
```

> **重要:**
>
> 永続VMの場合、すべてのディスクが移動されます。どのディスクを移動するかを選択することはできません。

非永続VM：

```
(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk
-ProvisioningSchemeName "myCleanOnBootProvScheme" -VMName "machine01"
-DiskType OS,Identity,WBC -DestinationStorageId None,None,datastore1
```

重要:

- 特定のディスクを移行したくない場合は、`DestinationStorageId`パラメーターの値を「なし」に設定します。
- VMにWBCディスクがある場合は、`DiskType`パラメーターにWBCディスクを追加し、`DestinationStorageId`パラメーターに必要な情報を追加します。

トラブルシューティング

いずれかのディスクの移行に失敗した場合、どのディスクも宛先ストレージに移行されません。以下のコマンドを使用して失敗レポートを取得できます。

```
(Get-ProvTask -TaskID xxxxxxxxx).DiskMoveFailedVirtualMachines
```

MCSによって作成されたリソースの識別

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
公開されたベースディスクと、各ネットワークまたはローカルストレージ上のそのコピー	「CitrixProvisioningSchemeId」：「xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx」
IDディスク	「CitrixProvisioningSchemeId」：「xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx」
OSディスク	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
準備用VM	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

リソース名	タグ
カタログ内のVM	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
WBCディスク	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

詳細情報

- 接続とリソースの作成および管理
- XenServerへの接続
- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create.html)
- XenServerカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create/create-machine-catalog-citrix-hypervisor.html)
- マシンカタログの管理(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-manage.html)

Google Cloud Platformカタログを管理する

マシンカタログを管理するウィザードについては、マシンカタログの管理で説明しています。以下の情報は、Google Cloud環境に固有の詳細を扱っています。

> **注:**
>
> Google Cloud Platformカタログを管理する前に、Google Cloud Platformカタログの作成を完了する必要があります。Google Cloud Platformカタログの作成を参照してください。

マシンカタログの管理

カタログへのマシンの追加、マシンの更新、および更新のロールバックについては、マシンカタログの管理を参照してください。

電源管理

Citrix DaaS™を使用すると、Google Cloudマシンの電源管理を行うことができます。電源管理を行うマシンを見つけるには、左ペインの**検索**ノードを使用します。次の電源操作が利用可能です。

- 削除
- 起動
- 再起動
- 強制再起動
- シャットダウン
- 強制シャットダウン
- デリバリーグループに追加
- タグの管理
- メンテナンスモードをオンにする

Autoscale を使用して Google Cloud マシンを電源管理することもできます。そのためには、Google Cloud マシンをデリバリーグループに追加し、そのデリバリーグループで Autoscale を有効にします。Autoscale の詳細については、Autoscale を参照してください。

PowerShell を使用してプロビジョニング済みマシンを更新する

`Set-ProvScheme` コマンドはプロビジョニングスキームを変更します。ただし、既存のマシンには影響しません。PowerShell コマンド `Set-ProvVMUpdateTimeWindow` を使用すると、現在のプロビジョニングスキームを既存の永続マシンまたは非永続マシン、あるいはマシンセットに適用できるようになりました。現在、GCP では、この機能でサポートされているプロパティの更新はマシンプロファイルです。

更新できるもの:

- 単一の VM
- 特定の VM のリスト、またはプロビジョニングスキーム ID に関連付けられているすべての既存の VM
- 特定の VM のリスト、またはプロビジョニングスキーム名に関連付けられているすべての既存の VM

既存の VM を更新するには：

1. 既存のマシンの構成を確認します。例えば、,

```
Get-ProvScheme | select ProvisioningSchemeName,
ProvisioningSchemeVersion
```

2. プロビジョニングスキームを更新します。例えば、,

```
`Set-ProvScheme –ProvisioningSchemeName "my-catalog" –MachineProfile
"XDHyp:\HostingUnits\<hosting-unit>\machineprofileinstance.vm"
```

3. VM の現在のプロパティが現在のプロビジョニングスキームと一致するか、および VM に保留中の更新アクションがあるかを確認します。例：

   ```
   Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
   ```

   特定のバージョンのマシンを見つけることもできます。例えば、,

   ```
   Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
   ProvisioningSchemeVersion
   ```

4. 既存のマシンを更新します。

   - すべての既存のマシンを更新するには:

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -StartsNow -DurationInMinutes -1
     ```

   - 特定のリストのマシンを更新するには:

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
     ```

   - `Get-ProvVM`の出力に基づいてマシンを更新するには：

     ```
     Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
     ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
     -DurationInMinutes -1
     ```

5. 更新がスケジュールされているマシンを見つけます。例えば、,

   ```
   Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
   ProvisioningSchemeUpdateAfter
   ```

6. マシンを再起動します。次回の電源投入時に、プロパティの変更が既存のマシンに適用されます。更新されたステータスは、次のコマンドを使用して確認できます:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

既存のカタログのディスク関連のカスタムプロパティを変更する

既存のカタログおよびカタログの既存のVMの、以下のディスク関連のカスタムプロパティを変更できます:

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

注:

- `StorageType` プロパティは OS ディスク用です
- `PersistOsDisk` プロパティは、ライトバックキャッシュが有効な非永続カタログに対してのみ設定できます

この実装により、カタログ作成後でもディスクごとに異なるストレージタイプを選択できるようになり、異なるストレージタイプに関連する価格設定のバランスを取ることができます。

これを行うには、PowerShellコマンド `Set-ProvScheme` と `Set-ProvVMUpdateTimeWindow` を使用します。

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*` を実行します。
3. カスタムプロパティを取得するには、`Get-ProvVM -VMName <VM name>` を実行します。
4. カスタムプロパティ文字列を変更します。
   a. カスタムプロパティをメモ帳にコピーし、カスタムプロパティを変更します。

b. **PowerShell** ウィンドウで、メモ帳から変更したカスタムプロパティを貼り付け、変更したカスタムプロパティに変数を割り当てます。例:

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com/2014/xd/
machinecreation xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="CatalogZones" Value="" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" /
>

<Property xsi:type="StringProperty" Name="PersistOSDisk"
Value="true" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="pd-standard" />

<Property xsi:type="StringProperty" Name="StorageType" Value="pd-
standard" />

</CustomProperties>'
```

5. 既存のカタログを更新します。例:

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName>
-CustomProperties $cp
```

6. 既存の VM を更新します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

7. VMを再起動します。次回の起動時に、カスタムプロパティの変更が既存のVMに適用されます。

偶発的なマシン削除からの保護

Citrix DaaS を使用すると、Google Cloud 上の MCS リソースを保護して、偶発的な削除を防ぐことができます。プロビジョニングされた VM を構成するには、`deletionProtection` フラグを TRUE に設定します。

デフォルトでは、MCSまたはGoogle Cloudプラグインを介してプロビジョニングされたVMは、InstanceProtectionが有効な状態で作成されます。この実装は、永続カタログと非永続カタログの両方に適用されます。非永続カタログは、インスタンスがテンプレートから再作成されるときに更新されます。既存の永続マシンについては、Google Cloudコンソールでフラグを設定できます。フラグの設定の詳細については、「Googleドキュメントサイト」を参照してください。永続カタログに追加される新しいマシンは、`deletionProtection`が有効な状態で作成されます。

`deletionProtection`フラグを設定したVMインスタンスを削除しようとすると、リクエストは失敗します。ただし、`compute.instances.setDeletionProtection`権限が付与されているか、IAMの**Compute Admin**ロールが割り当てられている場合は、フラグをリセットしてリソースを削除できるようにすることができます。

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
IDディスク	"CitrixResource": "内部"
	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
イメージ	"CitrixResource": "内部"
	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OSディスク	"CitrixResource": "内部"
	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
PrepVM	"CitrixResource": "内部"
	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
公開済みスナップショット	"CitrixResource": "内部"
ストレージバケット	"Citrixリソース": "内部"
テンプレート	"CitrixResource": "内部"

リソース名	タグ
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
カタログ内のVM	"CitrixResource": "内部"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"。プラグインは、MCSでプロビジョニングされたVMにもこのラベルを追加します: "citrix-provisioning-scheme-id": "provSchemeId"。このラベルを使用して、GCPコンソールでカタログによるフィルタリングが可能です。
WBCディスク	"CitrixResource": "内部"
	CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

注:

MCSによって作成されたリソースとして識別するために**CitrixResource**タグが追加されている場合、VMはCitrixインベントリに表示されません。VMを表示させるには、タグを削除または名前変更できます。

詳細情報

- 接続とリソースの作成および管理
- Google Cloud環境への接続
- マシンカタログの作成
- Google Cloud Platform カタログを作成する
- マシンカタログの管理

HPE Moonshot カタログの管理

「マシンカタログの管理」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-manage.html)では、マシンカタログを管理するウィザードについて説明します。以下の情報は、HPE Moonshotカタログに固有の詳細を扱います。

注:

HPE Moonshotカタログを管理する前に、HPE Moonshotカタログの作成を完了する必要があります。

電源管理

Citrix Virtual Apps and Desktops™では、HPE Moonshotマシンの電源管理を行うことができます。ナビゲーションペインの**検索**ノードを使用して、電源管理したいマシンを見つけます。以下の電源操作が利用可能です。

- 起動
- シャットダウン
- 強制シャットダウン
- 再起動
- リセット

注:

一時停止および**再開**の電源操作はサポートされていません。

詳細情報

- 接続とリソースの作成および管理(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/connections.html)
- HPE Moonshotへの接続(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/connections/connection-hpe-moonshot.html)
- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create.html)
- HPE Moonshotマシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create/create-machine-catalog-hpe-moonshot.html)
- マシンカタログの管理(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-manage.html)

Microsoft Azureカタログを管理する

注:

2023 年 7 月以降、Microsoft は Azure Active Directory (Azure AD) を Microsoft Entra ID に名称変更しました。このドキュメントでは、Azure Active Directory、Azure AD、または AAD へのすべての参照は、Microsoft Entra ID を指します。

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明しています。以下の情報は、Microsoft Azure Resource Managerクラウド環境に固有の詳細を扱っています。

注:

Microsoft Azureカタログを管理する前に、Microsoft Azureカタログの作成を完了する必要があります。Microsoft Azureカタログの作成を参照してください。

VMのシャットダウン時にストレージタイプを下位層に変更する

VMをシャットダウンするときに、管理ディスクのストレージタイプを下位層に切り替えることで、ストレージコストを節約できます。これを行うには、`StorageTypeAtShutdown`カスタムプロパティを使用します。

VMをシャットダウンすると、ディスクのストレージタイプは下位層（`StorageTypeAtShutdown`カスタムプロパティで指定）に変更されます。VMの電源をオンにすると、ストレージタイプは元の状態（`StorageType`カスタムプロパティまたは`WBCDiskStorageType`カスタムプロパティで指定）に戻ります。

重要:

ディスクは、VMが少なくとも一度電源オンになるまで存在しません。したがって、VMを最初に電源オンにしたときにストレージタイプを変更することはできません。

要件

- 管理ディスクに適用されます。これは、カスタムプロパティ`UseManagedDisks`をtrueに設定することを意味します。
- 永続OSディスクを持つ永続および非永続カタログに適用されます。これは、カスタムプロパティ`persistOsDisk`をtrueに設定することを意味します。
- 永続WBCディスクを持つ非永続カタログに適用されます。これは、カスタムプロパティ`persistWBC`をtrueに設定することを意味します。

制限

- Microsoftによると、ディスクの種類は1日2回しか変更できません。Microsoftドキュメントを参照してください。Citrixによると、VMの開始または割り当て解除アクションがあるたびに`StorageType`の更新が行われます。したがって、VMあたりの電源アクションの数を1日2回に制限してください。たとえば、午前中にVMを開始するための電源アクションを1回、夕方にVMを割り当て解除するための電源アクションを1回実行します。

ストレージの種類を下位層に変更する

手順を進める前に、要件と制限を参照してください。

1. カスタムプロパティ`StorageTypeAtShutdown`を追加し、値をStandard_LRS (HDD)に設定して、`New-ProvScheme`を使用してカタログを作成します。PowerShellを使用してカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

   > **注:**
   >
   > `StorageTypeAtShutdown`が空またはStandard_LRS (HDD)以外の値を持つ場合、操作は失敗します。

   永続カタログの作成中にカスタムプロパティを設定する例：

   ```
   $customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
   2014/xd/machinecreation"

   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

   <Property xsi:type="StringProperty" Name="UseManagedDisks"
   Value="true" />
   ```

```
<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

非永続カタログの作成中にカスタムプロパティを設定する例：

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
```

```
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

注:

マシンプロファイルを使用する場合、カスタムプロパティは`MachineProfile`で定義されたプロパティよりも優先されます。

2. VMをシャットダウンし、AzureポータルでVMのストレージタイプを確認します。ディスクのストレージタイプは、`StorageTypeAtShutdown`カスタムプロパティで指定されたとおり、下位層に変更されます。
3. VMをオンにします。ディスクのストレージタイプは、以下に記載されているストレージタイプに戻ります。
   - OSディスクの`StorageType`カスタムプロパティ
   - `CustomProperties`で指定した場合にのみ、WBCディスクの`WBCDiskStorageType`カスタムプロパティ。それ以外の場合は、`StorageType`に記載されているストレージタイプに戻ります。

既存のカタログに`StorageTypeAtShutdown`を適用する

手順に進む前に、要件と制限を参照してください。

既存のカタログにVMを追加するには、`Set-ProvScheme`を使用します。この機能は、`Set-ProvScheme`の実行後に追加された新しいVMに適用されます。既存のマシンには影響しません。

既存のカタログにVMを追加する際にカスタムプロパティを設定する例:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'



$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName



Set-ProvScheme -ProvisioningSchemeName $ProvScheme.ProvisioningSchemeName
-CustomProperties $customProperties
```

既存のVMのストレージタイプをシャットダウン時に下位層に変更する

手順に進む前に、要件と制限を参照してください。

VMがシャットダウンされているときに、既存のVMのストレージタイプを下位の層に変更することで、ストレージコストを節約できます。これを行うには、`StorageTypeAtShutdown`カスタムプロパティを使用します。

VMがシャットダウンされたときに、カタログ内の既存のマシンのストレージタイプを下位層に変更するには:

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. `Get-Provscheme -ProvisioningSchemeName $CatalogName`を実行します。
4. カスタムプロパティ文字列を変更します。

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

5. 既存のカタログのプロビジョニングスキームを更新します。この更新は、`Set-ProvScheme`の実行後に追加された新しいVMに適用されます。

```
Set-ProvScheme -ProvisioningSchemeName $CatalogName -CustomProperties
$customProperties
```

6. 既存のVMを更新して`StorageTypeAtShutdown`を有効にします。

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName $CatalogName
-StartsNow -DurationInMinutes -1
```

7. 次回マシンを起動すると、マシンの`StorageTypeAtShutdown`プロパティが更新されます。ストレージタイプは次回のシャットダウン時に変更されます。
8. カタログ内の各VMの`StorageTypeAtShutdown`値を表示するには、次のコマンドを実行します。

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach { $vmName =
$_.VMName; $storageTypeAtShutdown = ($_.CustomVmData | ConvertFrom-
Json).StorageTypeAtShutdown.DiskStorageAccountType; return New-Object
```

```
psobject -Property @{ "VMName" = $vmName; "StorageTypeAtShutdown" =
$storageTypeAtShutdown } }
```

プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する

`Set-ProvScheme` コマンドはプロビジョニングスキームを変更します。ただし、既存のマシンには影響しません。PowerShellコマンド `Set-ProvVMUpdateTimeWindow` を使用して、現在のプロビジョニングスキームを既存の永続的または非永続的なマシン、またはマシンセットに適用できます。既存のMCSプロビジョニング済みマシンの構成更新のために時間枠をスケジュールすることもできます。スケジュールされた時間枠内での電源オンまたは再起動により、スケジュールされたプロビジョニングスキームの更新がマシンに適用されます。現在、Azureでは、`ServiceOffering`、`MachineProfile`、および次のカスタムプロパティを更新できます。

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

注:

- Azure環境でマネージドディスクを使用するカタログの場合、`StorageType`、`WBCDiskStorageType`、および `IdentityDiskStorageType` のカスタムプロパティのみを更新できます。
- `Set-ProvVMUpdateTimeWindow` を2回実行した場合、最新のコマンドが有効になります。

更新できるもの:

- 単一のVM
- プロビジョニングスキームIDに関連付けられた特定のVMのリスト、または既存のすべてのVM

- プロビジョニングスキーム名（マシンカタログ名）に関連付けられた特定のVMのリスト、または既存のすべてのVM

プロビジョニングスキームに以下の変更を加えると、Azureの永続カタログのVMインスタンスが再作成されます。

- `MachineProfile`を変更する
- 削除 `LicenseType`
- 削除 `DedicatedHostGroupId`

> **注:**
>
> 既存のマシンのOSディスクとそのすべてのデータはそのまま残り、新しいVMがそのディスクに接続されます。

既存のVMを更新する前に:

1. 既存のマシンの構成を確認します。たとえば、,

```
Get-ProvScheme | select ProvisioningSchemeName,
ProvisioningSchemeVersion
```

2. プロビジョニングスキームを更新します。たとえば、,

   - マシンプロファイルの入力としてVMを使用する場合：

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -MachineProfile
"XDHyp:\HostingUnits\<hosting-unit>\machineprofile.folder\<resource-
group>.resourcegroup\<virtual-machine>.vm"
```

   - マシンプロファイルの入力としてテンプレート仕様を使用する場合：

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog"

-MachineProfile "XDHyp:\HostingUnits\<hosting-
unit>\machineprofile.folder\<resource-
group>.resourcegroup\<template-spec>.templatespec\<template-spec-
version>.templatespecversion"
```

```
-ServiceOffering "XDHyp:\HostingUnits\<hosting-
unit>\serviceoffering.folder\<service-offering>.serviceoffering"
```

- サービス提供のみの場合：

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -ServiceOffering
"XDHyp:\HostingUnits\<hosting-unit>\serviceoffering.folder\<service-
offering>.serviceoffering"
```

3. VM の現在のプロパティが現在のプロビジョニングスキームと一致するかどうか、および VM に保留中の更新アクションがあるかどうかを確認します。例:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

特定のバージョンのマシンを見つけることもできます。例えば、,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
ProvisioningSchemeVersion
```

既存のマシンに次回の再起動時に適用される更新を要求するには:

1. 既存のマシンを更新し、次回の再起動時に更新が適用されるようにするには、次のコマンドを実行します。

   - すべての既存のマシンを更新するには。例えば、,

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
   -StartsNow -DurationInMinutes -1
   ```

   - 特定の仮想マシンのリストを更新する場合。例：

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
   -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
   ```

   - Get-ProvVM の出力に基づいてマシンを更新する場合。例：

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
-DurationInMinutes -1
```

注:

- `StartsNow` は、スケジュールされた開始時刻が現在の時刻であることを示します。
- 負の数（例：–1）の `DurationInMinutes` は、スケジュールの時間枠に上限がないことを示します。

2. 更新がスケジュールされているマシンを見つける。例：

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

3. マシンを再起動します。次回の電源投入時に、プロパティの変更が既存のマシンに適用されます。以下のコマンドを使用して、更新されたステータスを確認できます。例：

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

スケジュールされた時間枠内で次回起動時に最新のプロビジョニング設定に更新するようにVMをスケジュールするには：

1. 次のコマンドを実行します。

- 開始時刻を現在時刻として更新をスケジュールするには

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName vm1 -StartsNow -DurationInMinutes 120
```

- 週末に更新をスケジュールするには

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
-VMName “vm1” -StartTimeInUTC “10/15/2022 9:00am” -DurationInMinutes
(New –TimeSpan –Days 2).TotalMinutes
```

> **注：**
>
> - `VMName` はオプションです。指定しない場合、更新はカタログ全体に対してスケジュールされます。
> - `StartTimeInUTC` の代わりに `StartsNow` を使用して、スケジュール開始時刻が現在時刻であることを示します。
> - `DurationInMinutes` はオプションです。デフォルトは120分です。負の数（例：-1）は、スケジュールの時間枠に上限がないことを示します。

2. 更新ステータスを確認します。

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
```

3. VM の電源を入れます。スケジュールされた時間枠の後にマシンの電源を入れた場合、構成の更新は適用されません。スケジュールされた時間枠内にマシンの電源を入れた場合、,
   - マシンの電源がオフで、
     - マシンの電源を入れない場合、構成の更新は適用されません
     - マシンの電源を入れた場合、構成の更新が適用されます
   - マシンの電源がオンで、
     - マシンを再起動しない場合、構成の更新は適用されません
     - マシンを再起動した場合、構成の更新が適用されます

構成の更新をキャンセルするには：

単一のVM、複数のVM、またはカタログ全体の構成更新をキャンセルすることもできます。構成更新をキャンセルするには：

1. `Clear-ProvVMUpdateTimeWindow`を実行します。例:
   - 単一のVMにスケジュールされた構成の更新をキャンセルするには:

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
-VMName “vm1”
```

- 複数のVMにスケジュールされた構成の更新をキャンセルするには:

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog"
-VMName "vm1","vm2"
```

> **注:**
>
> VM は同じカタログのものである必要があります。

個々のVMのプロパティを更新する

永続的なMCSマシンカタログ内の個々のVMのプロパティを、PowerShellコマンド`Set-ProvVM`を使用して更新できます。ただし、更新はすぐに適用されません。更新を適用するには、PowerShellコマンド`Set-ProvVMUpdateTimeWindow`を使用して時間枠を設定する必要があります。

この実装により、マシンカタログ全体を更新することなく、個々のVMを効率的に管理できます。現在、この機能はAzure環境にのみ適用可能です。

現在、更新できるプロパティは次のとおりです。

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

この機能を使用すると、次のことができます。

- VMのプロパティを更新する
- マシンカタログが更新された後も、VMで更新されたプロパティを保持する
- VMに適用された構成の更新を元に戻す(#revert-the-configuration-updates-applied-to-a-vm)

VMのプロパティを更新する前に：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. 既存のマシンカタログの構成を確認します。例：

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

4. 更新を適用するVMの構成を確認します。例：

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

VMのプロパティを更新する

VMのプロパティを更新するには、次の手順を実行します:

1. 更新を適用するVMをシャットダウンします。
2. VMのプロパティを更新します。たとえば、VMのストレージタイプ (`StorageType`) カスタムプロパティを更新する場合は、次を実行します:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

マシンカタログ内の2つのVMのプロパティを同時に更新できます。例:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2
-CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

> **注:**
>
> 更新はすぐに適用されません。

3. 更新が指定されているプロパティのリストと構成バージョンを取得します。例:

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -VMName
machine1
```

`Version`のプロパティ値と、更新されるプロパティ (この場合は`StorageType`) を確認します。

4. 構成バージョンを確認します。例：

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion` のプロパティ値を確認します。更新はまだ適用されていません。VMはまだ古い構成のままです。

5. スケジュールされた更新を要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog
-StartsNow -DurationInMinutes -1
```

スケジュールされた更新の詳細については、プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する を参照してください。

> **注:**
>
> 保留中のプロビジョニングスキームの更新も適用されます。

6. VMを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

7. 構成バージョンを確認します。例：

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion` のプロパティ値を確認します。更新が適用されました。VMは新しい構成になりました。

8. VM にさらに構成更新を適用するには、VM をシャットダウンし、手順を繰り返します。

マシンカタログの更新後にVMで更新されたプロパティを保持する

VMで更新されたプロパティを保持するには、以下を実行します。

1. 更新を適用したいVMをシャットダウンします。

2. マシンカタログを更新します。たとえば、VM サイズ (`ServiceOffering`) とストレージタイプ (`StorageType`) を変更したい場合は、次を実行します。

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -ServiceOffering
Standard_E4_v3 -CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

3. マシンカタログの構成詳細を取得します。例:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

`ProvisioningSchemeVersion` は1つ増分されます。VM サイズとストレージの種類も更新されます。

4. VM のプロパティを更新します。たとえば、VM にマシンプロファイルを提供します。

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-MachineProfile "XDHyp:\HostingUnits\<hosting-
unit>\machineprofile.folder\<resource-group>.resourcegroup\<template-
spec>.templatespec\<template-spec-version>.templatespecversion"
```

> **注:**
>
> マシンプロファイルの入力には、タグと異なる VM サイズ (`ServiceOffering`) が指定されています。

5. VM の構成更新とマシンカタログの更新をマージした後に VM が持つプロパティのリストを取得します。例:

```
Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName
AzureCatalog -VMName machine1
```

> **注:**
>
> VM に対する更新は、マシンカタログに対して行われた更新を上書きします。

6. VM のスケジュールされた更新を要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -VMName
machine1 -StartsNow -DurationInMinutes -1
```

7. VM を再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

   VM は、マシンプロファイルから派生した更新された VM サイズを保持します。マシンプロファイルで指定されたタグ値も VM に適用されます。ただし、ストレージの種類は最新のプロビジョニングスキームから派生します。

8. VM の構成バージョンを取得します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

   `ProvisioningSchemeVersion` と `ProvVMConfigurationVersion` に最新バージョンが表示されます。

VM に適用された構成更新を元に戻す

1. VM に更新を適用した後、VM の電源を切ります。
2. VM に適用されている更新を削除するには、次のコマンドを実行します。例:

```
Set-ProvVM -RevertToProvSchemeConfiguration -ProvisioningSchemeName
AzureCatalog -VMName machine1
```

3. VMのスケジュールされたアップデートを要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -VMName
machine1 -StartsNow -DurationInMinutes -1
```

4. VMを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

5. VMの構成バージョンを確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion` の値が、マシンカタログの構成バージョンになります。

ディスク暗号化の変更

Azure仮想化環境でディスク暗号化を変更し、次の操作を実行できます。

- `New-ProvScheme` コマンドを使用して、マスターイメージのDESとは異なるディスク暗号化セット（DES）を持つMCSマシンカタログを作成します。例：

```
$customProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="DiskEncryptionSetId" Name="Zones" Value="/
subscriptions/XXXXXXXXXXXXXXXXXXXXXXXXXXXX/resourceGroups/testrsg/
providers/Microsoft.Compute/diskEncryptionSets/test-diskEncryptionSet"/
>

</CustomProperties>

"@

New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName $provisioningSchemeName `

-HostingUnitName $hostingUnitName `

-IdentityPoolName $identityPoolName `

-InitialBatchSizeHint $numberOfVms `

-masterImagePath $masterImagePath `

-NetworkMapping $networkMapping `

-CustomProperties $customProperties
```

- 既存のMCSマシンカタログおよび既存のVMのディスク暗号化タイプを、あるDESキーから別のDESキーに変更するには、`Set-ProvScheme`および`Set-ProvVMUpdateTimeWindow`コマンドを使用します。VMを再起動すると、更新されたDESキーが表示されます。例：

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties

Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- 以前CMEKが有効になっていなかったMCSマシンカタログとVMを、`Set-ProvScheme`および`Set-ProvVMUpdateTimeWindow`コマンドを使用して、顧客管理の暗号化キー（CMEK）暗号化（DES）、ホストでのディスク暗号化、または二重暗号化を持つように更新します。異なる暗号化タイプについては、Azure サーバー側暗号化、ホストでのAzureディスク暗号化、およびマネージドディスクの二重暗号化を参照してください。
- 以前暗号化されていた既存のMCSマシンカタログとVMを非暗号化にするには、`Set-ProvScheme`および`Set-ProvVMUpdateTimeWindow`コマンドを使用します。例：

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- プライベートエンドポイントを使用したディスク暗号化を有効にします（`ProxyHypervisorTrafficThroughConnector` で有効化されたホスト接続を使用したMCSマシンカタログ）。プライベートエンドポイントを使用したディスク暗号化を有効にする方法については、プライベートエンドポイントを使用したディスク暗号化を有効にするを参照してください。

プライベートエンドポイントでディスク暗号化を有効にする

Azureの制限により、現在、プライベートエンドポイントに対して顧客管理キーによるサーバー側暗号化を使用することはできません。ただし、既存のMCSマシンカタログとプライベートエンドポイントを持つVMをDESキーで暗号化するように更新することは可能です。

プライベートエンドポイントを持つ既存のマシンカタログを更新する

プライベートエンドポイントを持つ既存のマシンカタログを更新する詳細な手順は次のとおりです。

1. ディスク暗号化なしでカタログを`ProxyHypervisorTrafficThroughConnector`経由で作成します。
2. `Set-ProvScheme`を実行して、`DiskEncryptionSetId`でカタログを更新します。

> **注:**
>
> `DiskEcryptionSetId`は、`CustomProperties`または`MachineProfile`を介して構成できます。`CustomProperties`と`MachineProfile`の両方で定義されている場合、`CustomProperties`で定義されているプロパティが適用されます。

`CustomProperties` を使用する場合の例:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1"/>
```

```
</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

MachineProfileを使用する場合の例：ディスク暗号化が有効なVM、またはディスク暗号化設定を持つテンプレート仕様を使用します。

```
Set-ProvScheme -ProvisioningSchemeName azure-catalog -MachineProfile
"XDHyp:
\HostingUnits\azureunit\machineprofile.folder\testrg.resourcegroup\new-
template.vm"
```

または、Web Studioを使用してマシンプロファイルを更新することもできます。

3. 既存のカタログ VM を更新するには、`Set-ProvVMUpdateTimeWindow` を実行します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

4. VMを再起動すると、AzureポータルのVMディスクで更新されたディスク暗号化を確認できます。
5. 新しいカタログVMを追加する前に、ディスク暗号化を解除するには`Set-ProvScheme`を実行します。

注:

プライベートエンドポイントカタログを更新しているため、この手順は必須です。この手順を実行しないと、新しいVMをカタログに追加しようとしたときにエラーが発生します。

例:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
```

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

6. 新しいVMをカタログに追加します。

個々のカタログ VM を更新する

個々のカタログ VM を更新する詳細な手順は次のとおりです。

1. `ProxyHypervisorTrafficThroughConnector` を介してディスク暗号化なしでカタログを作成します。
2. `DiskEncryptionSetId` を使用してカタログVMを更新するには、`Set-ProvVM` を実行します。

> **注:**
>
> The `DiskEcryptionSetId` は、`CustomProperties` または `MachineProfile` のいずれかを使用して構成できます。
>
> `CustomProperties` を使用する場合の例:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />

</CustomProperties>'

Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01
-CustomProperties $customProperties
```

MachineProfile を使用する場合の例:

```
Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01
-MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\testrg.resourcegroup\new-
template.vm"
```

3. 既存のカタログVMを更新するには、`Set-ProvVMUpdateTimeWindow` を実行します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01 -StartsNow -DurationInMinutes -1
```

4. VMを再起動すると、AzureポータルでVMディスクの更新されたディスク暗号化を確認できます。
5. カタログに新しいVMを追加します。

既存のカタログのWBCディスクとして一時ディスクを使用する

既存のMCSマシンカタログのライトバックキャッシュディスク（WBC）ディスクとしてAzure一時ディスクを使用できます。既存のカタログとVMを更新するには、`Set-ProvScheme` PowerShellコマンドを使用します。

前提条件

既存のカタログは、次の条件を満たしている必要があります。

> **注:**
>
> 既存のカタログが次の要件を満たしていない場合、WBCディスクは一時ディスク内に配置されません。

- MCSIOが有効になっている：カスタムプロパティ`WriteBackCacheMemorySize`、`WriteBackCacheDiskSize`、および`UseWriteBackCache`が有効になっています。
- エフェメラルOSディスクが有効になっていない。
- WBCが非永続的である：`PersistWBC`が`false`である。
- `UseTempDiskForWBC`がnullまたはfalseである。

- 一時ディスクのサイズは、（ライトバックキャッシュディスクサイズ + ページングファイル用の予約スペース + 1 GBのバッファースペース）の合計サイズよりも大きくする必要があります。

> **重要：**
>
> 一時ディスクを持つサービスオファリングから持たないサービスオファリングへの変更、またはその逆は許可されていません。

既存のカタログを更新する

既存のカタログを更新するには、次のコマンドを実行します。

1. 既存のカタログで`Set-ProvScheme`を実行して、`UseTempDiskForWBC`を`true`に更新します。例：

```
Set-ProvScheme -ProvisioningSchemeName name -CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Standard_LRS`"/><Property
xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"True`"/
><Property xsi:type=`"StringProperty`" Name=`"ManagedDisksPreview`"
Value=`"False`"/><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"False`"/><Property
xsi:type=`"StringProperty`" Name=`"UseTempDiskForWBC`" Value=`"True`"/
><Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
Value=`"False`"/></CustomProperties>"
```

2. カタログに新しいマシンを追加して電源を入れます。新しい VM には、一時ディスク内に WBC ディスクがあります。

Azure VM、スナップショット、OS ディスク、およびギャラリーイメージ定義の情報を取得する

Azure VMのOSディスクと種類、スナップショット、ギャラリーイメージ定義を含む情報を表示できます。この情報は、マシンカタログが割り当てられたときにマスターイメージ上のリソースに対して表示されます。この機能を使用して、LinuxまたはWindowsイメージを表示および選択します。PowerShellプロパティ`TemplateIsWindowsTemplate`が`AdditionDatafield`パラメーターに追加されました。このフィールドには、VMの種類、OSディスク、ギャラリーイメージ情報、

OSの種類情報など、Azure固有の情報が含まれています。`TemplateIsWindowsTemplate`を**True**に設定するとOSの種類がWindowsであることを示し、`TemplateIsWindowsTemplate`を**False**に設定するとOSの種類がLinuxであることを示します。

ヒント：

`TemplateIsWindowsTemplate` PowerShellプロパティによって表示される情報は、Azure APIから取得されます。このフィールドは空の場合があります。たとえば、データディスクからのスナップショットには`TemplateIsWindowsTemplate`フィールドが含まれていません。これは、OSタイプをスナップショットから取得できないためです。

たとえば、PowerShellを使用して、Windows OSタイプの場合にAzure VMの`AdditionData`パラメーターを**True**に設定します。

```
PS C:\Users\username> (get-item XDHyp:
\HostingUnits\mynetwork\image.folder\username-dev-testing-
rg.resourcegroup\username-dev-tsvda.vm).AdditionalData

Key Value

ServiceOfferingDescription Standard_B2ms

HardDiskSizeGB 127

ResourceGroupName FENGHUAJ-DEV-TESTING-RG

ServiceOfferingMemory 8192

ServiceOfferingCores 2

TemplateIsWindowsTemplate True

ServiceOfferingWithTemporaryDiskSizeInMb 16384

SupportedMachineGenerations Gen1,Gen2
```

MCSによって作成されたリソースを識別する

以下は、MCSがリソースに追加するタグです。表内のタグは「"key":"value"」として表されます。

リソース名	タグ
ID ディスク	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
イメージ	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
NIC	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
OSディスク	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
PrepVM	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
公開スナップショット	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
リソースグループ	"CitrixResource" : "内部"
	CitrixSchemaVersion: 2.0
	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
ストレージアカウント	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"

リソース名	タグ
カタログ内のVM	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
WBCディスク	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"

注:

MCSによって作成されたリソースとして識別するために**CitrixResource**タグが追加されている場合、VMはCitrixインベントリに表示されません。表示させるには、タグを削除または名前変更できます。

タグの削除

カタログまたはVMを作成すると、以下のリソースにタグが作成されます。

- リソースグループ
- 仮想マシン
- OSディスク
- 識別ディスク
- ネットワークインターフェイス
- ストレージアカウント

CitrixデータベースからVMとマシンカタログを削除し、タグを削除できます。以下を使用できます。

- マシンカタログから単一のVMまたはVMのリストからVMとタグを削除するには、`ForgetVM` パラメーターを指定した`Remove-ProvVM`を使用します。
- Citrixデータベースからマシンカタログを削除し、マシンカタログ全体からタグを削除するには、`ForgetVM` パラメーターを指定した`Remove-ProvScheme`を使用します。

この機能は、永続VMにのみ適用されます。

これを行うには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、**asnp citrix***を実行します。
3. CitrixデータベースからVMを削除し、VMからタグを削除するには、`Remove-ProvVM`を実行します。 例：

```
Remove-ProvVM -ProvisioningSchemeName “ProvisioningSchemeName” -VMName “vmname” -ForgetVM
```

4. Citrixデータベースからマシンカタログを削除し、マシンカタログからタグを削除するには、`Remove-ProvScheme`を実行します。例：

```
Remove-ProvScheme -ProvisioningSchemeName “ProvisioningSchemeName” -ForgetVM
```

> **注:**
>
> `Remove-ProvScheme`で`ForgetVM`パラメーターを使用すると、プロビジョニングスキームがBYORG（Bring Your Own Resource Group）またはCitrix管理リソースグループのいずれかに存在する場合、MCSはベースディスクスナップショットを含むすべてのスナップショットを削除します。

詳細情報

- 接続とリソースの作成および管理
- Microsoft Azureへの接続
- マシンカタログの作成
- Microsoft Azureカタログの作成
- マシンカタログの管理

Microsoft System Center Virtual Machine Manager カタログを管理する

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Microsoft System Center Virtual Machine Manager (VMM) 仮想化環境に固有の詳細を扱っています。

注:

VMMカタログを管理する前に、VMMカタログの作成を完了する必要があります。詳細については、(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create/create-machine-catalog-mscvmm.html)を参照してください。

MCSによって作成されたリソースを識別する

以下は、MCSがリソースに追加するタグです。表のタグは「key":"value」として表されます。

リソース名	タグ
準備VM	タグとして使用される文字列: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	カスタムプロパティエントリ: "XdConfig:"XdProvisioned=True"
カタログ内のVM	タグとして使用される文字列: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	カスタムプロパティエントリ: "XdConfig:"XdProvisioned=True"

詳細情報

- 接続とリソースの作成および管理(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/connections.html)
- マイクロソフト システム センター バーチャル マシン マネージャーへの接続
- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create.html)
- マイクロソフト システム センター バーチャル マシン マネージャーカタログの作成
- マシンカタログの管理(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-manage.html)

VMwareカタログの管理

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、VMware仮想化環境に固有の詳細を扱います。

> **注:**
>
> VMwareカタログを管理する前に、VMwareカタログの作成を完了する必要があります。VMwareカタログの作成を参照してください。

マシンカタログのフォルダーIDを更新する

MCSマシンカタログのフォルダーIDは、`Set-ProvScheme`コマンドのカスタムプロパティで`FolderId`を指定することで更新できます。フォルダーIDの更新後に作成されたVMは、この新しいフォルダーIDの下に作成されます。このプロパティが`CustomProperties`で指定されていない場合、VMはマスターイメージが配置されているフォルダーの下に作成されます。

マシンカタログのフォルダーIDを更新するには、次の手順を実行します。

1. Webブラウザーを開き、**vSphere Web Client**のURLを入力します。
2. 資格情報を入力し、**ログイン**をクリックします。
3. **vSphere Web Client**でVM配置フォルダーを作成します。
4. PowerShellウィンドウを開きます。
5. **asnp citrix®***を実行して、Citrix固有のPowerShellモジュールをロードします。
6. `Set-ProvScheme`の`CustomProperties`で`FolderID`を指定します。この例では、フォルダーIDの値は`group-v2406`です。

   ```
   Set-ProvScheme -ProvisioningSchemeUid
   "50bb319c-2e83-4a37-9ea1-94f630687372" -CustomProperties
   "<CustomProperties xmlns=""http://schemas.citrix.com/2014/xd/
   machinecreation"" xmlns:xsi=""http://www.w3.org/2001/XMLSchema-
   instance""><Property xsi:type=""StringProperty"" Name=""FolderId""
   Value=""group-v2406"" /></CustomProperties>"
   ```

7. Studioを使用してマシンカタログにVMを追加します。
8. vSphere Web Clientで新しいVMを確認します。新しいVMは新しいフォルダーの下に作成されます。

vSphere でフォルダー ID を見つける

任意の ESXi または vCenter サーバーシステムで Managed Object Browser (MOB) にアクセスし、VM のフォルダー ID を見つけます。

MOB は、すべての ESX/ESXi および vCenter サーバーシステムに組み込まれている Web ベースのサーバーアプリケーションです。この vSphere ユーティリティを使用すると、VM、データストア、リソースプールなどのオブジェクトに関する詳細情報を表示できます。

1. Web ブラウザーを開き、`http://x.x.x.x/mob` を入力します。ここで、x.x.x.x は vCenter Server または ESX/ESXi ホストの IP アドレスです。例: `<https://10.60.4.70/mob>`。
2. MOB の **Home** ページで、プロパティ **content** の値をクリックします。
3. **rootFolder** の値をクリックします。
4. **childEntity** の値をクリックします。
5. **vmFolder** の値をクリックします。
6. フォルダー ID は **childEntity** の値で見つけることができます。

VM のストレージ移行

既存の VM のディスクストレージを古いストレージから新しいストレージに移動できます。移行中、MCS は電源管理、OS ディスクのリセットなどの VM 機能は保持します。新しいディスクストレージを使用して、新しい VM をマシンカタログに追加することもできます。これを行うには、PowerShell コマンド `Move-ProvVMDisk` を使用します。

現在、フルクローン永続 VM のみ移行できます。

新しいストレージは、次の条件を満たす必要があります。

- 古いストレージと同じクラスター内にある必要があります。
- VM が実行されているホストは、古いデータストアと新しいデータストアの両方にアクセスできる必要があります。

以下のタスクを実行できます。

- ディスクストレージの移行
- 古いストレージを非推奨にする

ディスクストレージの移行

ディスクストレージを移行するには：

1. 既存のホスティングユニットに新しいストレージを追加します。古いストレージを**Superseded**に変更します。これはWeb StudioまたはPowerShellコマンドを使用して実行できます。

   - Web Studioを使用する場合は、「ストレージの編集」を参照してください。
   - PowerShellコマンドを使用する場合：

     - `Add-Hyphostingunitstorage`を実行して、既存のホスティングユニットに新しいストレージを追加します。
     - 古いストレージでの新しいVM作成を無効にするには、**Superseded**をtrueに設定して`Set-Hyphostingunitstorage`を実行します。

2. VMをシャットダウンし、**メンテナンスモード**をオンにします。
3. VMのディスクストレージを新しいストレージに移動し、ストレージ情報を更新します。例:

```
Move-ProvVMDisk -ProvisioningSchemeName "myFullCloneProvScheme" -VMName
("VMware-TestVM01", "VMware-TestVM02") -DiskType OS,Identity
-DestinationStorageId datastore1,datastore1
```

4. 移行のタスクIDを取得します。例:

```
,(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk
-ProvisioningSchemeName xxxxx -DiskType OS,Identity
-DestinationStorageId datastore1,datastore1
```

5. 移行のステータスを確認します。

   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMovedVirtualMachines`: ディスク移行が成功したVMのリストを提供します。これには、すでに新しいストレージに移行されたVMも含まれます。
   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMoveFailedVirtualMachines`: 移行に失敗したVMのリストを提供します。
   - `(Get-ProvTask -TaskID xxxxxxxxx).NotStartedVirtualMachines`: 移行がまだ開始されていないVMのリストを提供します。
   - `Get-ProvVM -ProvisioningSchemeName xxxxx -VMName "VMware-TestVM01`: 移行後の更新されたVMプロパティを提供します。`StorageId`、`AssignedImage`、`BootedImage`、`IdentityDiskId`、`IdentityDiskStorage`、`LastBootTime`などのプロパティを確認してください。

スナップショット付きのMCSで作成されたVMのディスクを移行した後、**Consolidation is required in the VSphere Client** という警告が表示されることがあります。統合してデータ損失を回避するには:

1. VMware VMのバックアップを取ります。たとえば、すべてのVMファイルをデータストア上の別のフォルダーに転送します。
2. 警告が表示されたら、**統合**をクリックし、次に**OK**をクリックして統合を確認します。

古いストレージの廃止

VMディスク移行後に古いストレージを非推奨にするには：

1. ホスティングユニットの各ディスクストレージにおけるベースディスクとマシン数に関する情報を取得します。例：

   ```
   $result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName xxxxx

   $result

   $result.ProvResourceInStorage | Format-List -Property *
   ```

   移行が成功すると、MCSは古いベースディスクを自動的に削除し、古いストレージにはマシンがなくなります。したがって、コマンドを実行した後、古いストレージにマシンとベースディスクがないことを確認してください。
2. ホスティングユニットから古いストレージを完全に削除するには、`Remove-Hyphostingunitstorage` を実行します。Web Studio を使用して古いストレージを削除することもできます。

MCSによって作成されたリソースを識別する

以下は、MCSがリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
準備用 VM	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"XdConfig:"XdProvisioned=真"
カタログ内のVM	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

リソース名	タグ
	"XdConfig:"XdProvisioned=真"

詳細情報

- 接続とリソースの作成および管理
- VMwareへの接続
- マシンカタログの作成
- VMwareカタログを作成する
- マシンカタログの管理

電源管理

Citrix Virtual Apps and Desktops™ を使用すると、さまざまなサポート対象のハイパーバイザーとクラウドサービスで、MCSプロビジョニングされたVMの電源管理を行うことができます。電源管理操作により、以下が提供されます。

- 最適なユーザーエクスペリエンス
- コスト管理と電力節約

利用可能な電源操作は次のとおりです。

- 起動
- シャットダウン
- 再起動
- 一時停止
- 再開
- 強制再起動
- 強制シャットダウン

> **注:**
>
> - 非永続VMの場合、電源サイクル（シャットダウン/起動および再起動）によりOSディスクがリセットされます。

- 電源操作の機能と動作は、ハイパーバイザーまたはクラウドサービスによって異なります。

この記事では、特定のサポート対象ハイパーバイザーに関連する主要な電源管理機能について説明します。

- AWS VMの電源管理
- Azure VMの電源管理

AWS VM の電源管理

必要な権限については、「必要な AWS 権限」を参照してください。

インスタンスの休止

休止プロセスは、インスタンスのメモリ内状態と、そのプライベート IP アドレスおよびエラスティック IP アドレスを保存し、中断したところから正確に再開できるようにします。

インスタンスに休止が指示されると、メモリ内状態をルート EBS ボリュームのファイルに書き込み、その後シャットダウンします。Amazon EBS ボリュームは、インスタンスにアタッチできる耐久性のあるブロックレベルのストレージデバイスです。ボリュームをインスタンスにアタッチすると、物理ハードドライブと同じように使用できます。インスタンスのルート EBS ボリュームを暗号化します。暗号化により、機密データがメモリから EBS ボリュームにコピーされる際に適切に保護されます。EBS 暗号化の詳細については、「Amazon EBS 暗号化」を参照してください。

サポートされているインスタンス休止の制限事項は次のとおりです。

- インスタンスメモリ (RAM) は最大 150 GB のみがサポートされています
- UEFI ブートモードはサポートされていません
- EBS ボリュームタイプとしてサポートされているのは、汎用 SSD とプロビジョンド IOPS SSD のみです。

休止対応 VM の作成

休止対応 VM を作成するには：

1. ホスト接続を作成します。「AWS への接続」を参照してください。
2. EBS ルートが暗号化され、**Stop-Hibernate** プロパティが有効になっているインスタンスを起動します。インスタンスの起動方法、ルート EBS ボリュームの暗号化、および休止の有効化の詳細については、`<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/`

`launching-instance.html/>` を参照してください。このインスタンスをマスターイメージとして使用して AMI を作成します。

3. マスターイメージを準備します。

   a. マスターイメージに VDA をインストールします。Citrix は、最新機能にアクセスできるように、最新バージョンのインストールを推奨しています。マスターイメージに VDA をインストールしないと、カタログの作成が失敗します。VDA のインストール方法の詳細については、「VDA のインストール」を参照してください。

   b. マスターイメージを、アプリケーションとデスクトップが属するドメインに参加させます。マスターイメージが、マシンが作成されるホストで利用可能であることを確認してください。

4. そのインスタンスからAMIを作成します。インスタンスからAMIを作成する方法については、「Amazon EC2インスタンスからAMIを作成する」を参照してください。

5. `New-ProvScheme`コマンドを使用してマシンカタログを作成します。`AwsCaptureInstanceProperties`カスタムプロパティを**True**に設定します。Web StudioでAWSインスタンスプロパティを有効にする方法については、「**Web StudioでのAWSインスタンスプロパティの適用と運用リソースのタグ付け**」を参照してください。

   ```
   New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot

   -CustomProperties "AwsCaptureInstanceProperties,true;"

   -HostingUnitName "xxx" -IdentityPoolName $catalog_name
   -InitialBatchSizeHint 1

   -MasterImageVM "xyz.template" -NetworkMapping @{"0"="XDHyp:
   \HostingUnits\MyConn\\us-east-2a.availabilityzone\10.0.0.0``/24
   (vpc-0f1771e45671aedcd).network"}

   -ProvisioningSchemeName $catalog_name

   -RunAsynchronously -Scope @() -SecurityGroup @("xxx") -ServiceOffering
   "xxx"
   ```

   PowerShell コマンドを使用してマシンカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/>` を参照してください。

ハイバネート可能な VM は、次の場合に作成されます。

- **Stop-Hibernate** プロパティが有効になっているマスターイメージから作成された AMI を選択した場合。
- マスター VM がドメインに参加しており、VDA がインストールされている場合。
- 休止状態を処理できる正しいVMサイズ（サービス提供）を選択します。

New-ProvSchemeコマンドは、次の場合に適切なエラーメッセージで失敗します。

- マスターVMは休止状態が有効になっているが、サービス提供が休止状態を処理できない場合。
- マスターVMがドメインに参加しておらず、VDAがインストールされていない場合。

サービス提供とAMIの休止状態

サービス提供とAMI（テンプレート）の休止状態を取得するには、次のコマンドを実行します。

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b (ami-0e6c5b33a52d2a6b6).template'`
- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

既存のハイバネーション対応プロビジョニングスキームのサービスオファリングを更新

1. `Set-ProvScheme`コマンドを実行します。例:

```
Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering
<String>
```

サービスオファリングに互換性がない場合、システムは例外メッセージを表示します。

ハイバネーションサポート付きのマシンカタログを作成する

マシンカタログを作成する際、ハイバネーションをサポートするマシンプロファイルを使用できます。

1. カタログ作成ウィザードで、マシンプロファイルの選択まで指示に従って進みます。
2. **マシンテンプレート**ページで、**マシンプロファイルの選択**をクリックし、マシンプロファイルを選択します。
3. **仮想マシン**ページで、**編集**アイコンをクリックし、VMを選択します。

> **注:**

> マシンプロファイルがハイバネーション対応の場合、システムはハイバネート可能なVMのみを表示します。

4. 画面の指示に従ってすべての設定を完了します。**概要**ページには、カタログのハイバネーションステータスが表示されます。

> **注:**
>
> マシンカタログの編集で、マシンプロファイルをハイバネーション対応のものに変更すると、それに応じてVMを再構成するよう求められます。

ハイバネーションをサポートするマシンカタログを更新する

既存のマシンカタログをハイバネーションをサポートしないマシンカタログで更新しようとすると、適切なエラーメッセージとともに更新は失敗します。

休止状態のVMの電源管理

休止状態のVMに対して、以下の電源管理操作を実行できます。

1. 実行中の状態からVMを一時停止する。
2. 一時停止状態からVMを再開する。
3. 一時停止状態からVMを再起動する。

Azure VM の電源管理

必要な権限については、「必要なAzure権限」を参照してください。

Azure オンデマンドプロビジョニング

Azureオンデマンドプロビジョニングでは、プロビジョニングが完了した後、Citrix Virtual Apps and Desktops™が電源オンアクションを開始した場合にのみVMが作成されます。

MCSを使用してAzure Resource Managerでマシンカタログを作成する場合、Azureオンデマンドプロビジョニング機能は次のとおりです。

- ストレージコストを削減します
- カタログ作成を高速化します

MCSカタログを作成すると、Azureポータルにリソースグループ内のネットワークセキュリティグループ、ネットワークインターフェイス、ベースイメージ、およびIDディスクが表示されます。

Citrix Virtual Apps and DesktopsがVMの電源オンアクションを開始するまで、AzureポータルにはVMが表示されません。次の違いを持つ2種類のマシンがあります。

- プールされたマシンでは、オペレーティングシステムディスクとライトバックキャッシュはVMが存在する場合にのみ存在します。コンソールでプールされたマシンをシャットダウンすると、AzureポータルにはVMが表示されません。マシンを定期的にシャットダウンする場合（たとえば、営業時間外）、ストレージコストを大幅に節約できます。
- 専用マシンでは、VMが最初に電源オンされたときにオペレーティングシステムディスクが作成されます。AzureポータルのVMは、マシンIDが削除されるまでストレージに残ります。コンソールで専用マシンをシャットダウンしても、AzureポータルにはVMが表示されたままになります。

注：

オンデマンドプロビジョニング機能より前に作成されたAzureカタログ（「レガシー」カタログ）のサポートは非推奨です。したがって、Azureレガシーカタログ VMを再作成してください。カタログはオンデマンドとしてプロビジョニングされ、ストレージコストを節約できます。

電源サイクル時にプロビジョニングされた仮想マシンを保持する

電源サイクル時にプロビジョニングされた仮想マシンを保持するかどうかを選択します。PowerShellパラメーター`New-ProvScheme CustomProperties`を使用します。このパラメーターは、プロビジョニングされた仮想マシンが電源サイクル時に永続化するかどうかを決定するために使用される追加のプロパティ`PersistVm`をサポートします。電源オフ時に仮想マシンを永続化するには`PersistVm`プロパティを**true**に設定し、電源オフ時に仮想マシンが保持されないようにするにはプロパティを**false**に設定します。

注:

`PersistVm`プロパティは、`CleanOnBoot`および`UseWriteBackCache`プロパティが有効になっているプロビジョニングスキームにのみ適用されます。非永続的な仮想マシンに対して`PersistVm`プロパティが指定されていない場合、それらは電源がオフになるとAzure環境から削除されます。

電源サイクル時にプロビジョニングされた仮想マシンを保持する

電源サイクル時にプロビジョニングされた仮想マシンを保持するかどうかを選択します。PowerShellパラメーター`New-ProvScheme CustomProperties`を使用します。このパラメーターは、電源サイクル時にプロビジョニングされた仮想マシンが保持されるかどうかを決定するために使用される追加のプロパティ`PersistVm`をサポートします。電源オフ時に仮想マシンを保持するには`PersistVm`プロパティを**true**に設定し、電源オフ時に仮想マシンが保持されないようにするにはプロパティを**false**に設定します。

注:

`PersistVm`プロパティは、`CleanOnBoot`および`UseWriteBackCache`プロパティが有効になっているプロビジョニングスキームにのみ適用されます。非永続仮想マシンに対して`PersistVm`プロパティが指定されていない場合、それらは電源オフ時にAzure環境から削除されます。

「次の例では、`New-ProvScheme CustomProperties`パラメーターは`PersistVm`プロパティを **true** に設定します。」:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
resourcegroup" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />
```

```
</CustomProperties>
```

「次の例では、`New-ProvScheme CustomProperties` パラメーターは、`PersistVM` を **true** に設定することでライトバックキャッシュを保持します。」:

```
 New-ProvScheme

 -AzureAdJoinType "None"

 -CleanOnBoot

 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageType`" Value=`"Standard_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"false`" /
><Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"PersistVm`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"ResourceGroups`" Value=`"demo-resourcegroup`" /><Property
xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Client`" /></CustomProperties>"

 -HostingUnitName "demo"

 -IdentityPoolName "NonPersistent-MCSIO-PersistVM"

 -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-
test.resourcegroup\demo-snapshot.snapshot"

 -NetworkMapping @ {"0"="XDHyp:\HostingUnits\demo\
\virtualprivatecloud.folder\East US.region\virtualprivatecloud.folder\ji-
test.resourcegroup\jitest-vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"

 -ServiceOffering "XDHyp:
\HostingUnits\demo\serviceoffering.folder\Standard_B2ms.serviceoffering"
-UseWriteBackCache

 -WriteBackCacheDiskSize 127
```

```
-WriteBackCacheMemorySize 256
```

ヒント:

`PersistVm`プロパティは、プロビジョニングされた仮想マシンを保持するかどうかを決定します。`PersistOsdisk`プロパティは、OSディスクを永続化するかどうかを決定します。プロビジョニングされた仮想マシンを保持するには、まずOSディスクを保持します。仮想マシンを削除せずにOSディスクを削除しないでください。`PersistVm`パラメーターを指定せずに`PersistOsdisk`プロパティを使用できます。

ストレージタイプの変更失敗時の電源オン動作をカスタマイズする

電源オン時に、Azureでの障害により、管理ディスクのストレージタイプが目的のタイプに変更できない場合があります。このようなシナリオでは、VMはオフのままで、障害メッセージが送信されます。ただし、ストレージが構成されたタイプに復元できない場合でもVMの電源をオンにするか、VMをオフのままにするかを選択できます。

- カスタムプロパティ`FailSafeStorageType`を**true**（デフォルト設定）として構成した場合、または`New-ProvScheme`または`Set-ProvScheme`コマンドで指定しない場合：
  - 電源オン時に、VMは誤ったストレージタイプで電源オンされます。
  - シャットダウン時、VMは誤ったストレージタイプでオフのままになります。
- `New-ProvScheme` または `Set-ProvScheme` コマンドでカスタムプロパティ `FailSafeStorageType` を **false** に構成した場合:
  - 電源オン時に、VMは誤ったストレージタイプでオフのままになります。
  - シャットダウン時、VMは誤ったストレージタイプでオフのままになります。

マシンカタログを作成するには：

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. まだ作成されていない場合は、IDプールを作成します。
4. `New-ProvScheme`にカスタムプロパティを追加します。例：

```
New-ProvScheme -HostingUnitName "Azure-Resources-1" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\Azure-
Resources-1\image.folder\abc.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\Azure-
Resources-1\ght.folder\abc.resourcegroup\abc-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "name"

-ServiceOffering "XDHyp:\HostingUnits\Azure-
Resources-1\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown`"
Value=`"Standard_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"true`" />

</CustomProperties>"
```

5. マシンカタログを作成します。Remote PowerShell SDKを使用してカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

既存のマシンカタログを更新して、`FailSafeStorageType`カスタムプロパティを含めます。この更新は既存のVMには影響しません。

1. `Set-ProvScheme`コマンドでカスタムプロパティを更新します。例：

```
Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "

<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
```

```
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"false`" />

</CustomProperties>"
```

Set-ProvSchemeで行われた変更を既存のVMに適用するには、`-StartsNow`と`-DurationInMinutes -1`のパラメーターを指定して`Set-ProvVMUpdateTimeWindow`コマンドを実行します。

1. `-StartsNow`と`-DurationInMinutes -1`パラメーターコマンドを指定して`Set-ProvVMUpdateTimeWindow`コマンドを実行します。例：

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
   <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
   ```

2. VMを再起動します。

休止状態対応VMの作成

Azure環境では、休止状態をサポートするMCSマシンカタログを作成できます。この機能を使用すると、VMを中断し、ユーザーが再度サインインしたときにVMの以前の状態に再接続できます。

休止状態機能は以下に適用されます。

- シングルセッションOS
- 永続VMと非永続VM
- 静的およびランダム (プールされた) VDI デスクトップ

VDI デスクトップが静的かランダムかに関わらず、VM を休止状態にした後、同じセッションに再開できます。

このセクションでは、以下を参照してください。

- 前提条件

- 制限事項
- 休止状態対応のマシンカタログの作成と管理
- 既存の休止状態対応 VM 用のマシンカタログの作成
- 休止状態プロパティの確認
- VM の電源管理 (手動および自動)

休止状態を使用するための前提条件

休止状態を使用するには、以下のタスクを完了していることを確認してください。

- Windows と Linux の両方のマスターイメージに Azure VM Agent をインストールします。Windows イメージのページファイルは一時ディスクに配置できます。マシンカタログで休止状態が有効になっている場合、MCS はページファイルの場所をベースディスクの C: ドライブに設定します。
- MCS は、生成されたリソースの休止状態プロパティを自動的に設定します。休止状態をサポートするために、マスターリソースのプロパティを構成する必要はありません。
- 休止状態をサポートするサブスクリプション内の VM サイズを使用してください。
- VM が休止状態機能を継承できるように、休止状態対応のマシンプロファイル (VM またはテンプレート仕様) を作成します。VM の作成については、休止状態の開始 を参照してください。

  > **注:**
  >
  > Microsoft によると、OS ディスクから休止状態が有効な VM を展開できます。この機能は現在、特定のリージョンでサポートされており、まもなくすべてのリージョンで利用可能になります。詳細については、「OS ディスクから休止状態が有効な VM を展開する」を参照してください。

  テンプレート仕様を作成するには、次の手順を実行します。

  a. Azure Portal を開きます。テンプレートで使用する構成を持つ VM を選択します。左ペインで を選択します。
  b. チェックボックスをオフにします。コンテキストをコピーし、たとえば `VMExportTemplate.json` のように JSON ファイルとして保存します。
  c. パラメーター `hibernationEnabled` がテンプレートで `true` であることを確認します。パラメーターが `true` でない場合は、使用した VM 構成を確認してください。サポー

トされている VM サイズをテンプレートファイルで指定できます。ただし、カタログの作成時にマシンサイズを指定することもできます。

d. ネットワークインターフェイスリソースのテンプレートを JSON ファイル `VMExportTemplate.json` に追加します。その結果、2つのリソースを持つ ARM テンプレートファイルが作成されます。

e. **> > >** を選択して、このテンプレートファイルを ARM テンプレート仕様としてインポートします。

f. ARM テンプレート仕様が作成されたら、それをマシンプロファイルとして使用できます。

> **注:**
>
> Citrix Studio に同期されるまで数分かかる場合があります。

詳細については、Microsoft ドキュメント「休止状態を使用するための前提条件」を参照してください。

制限事項

- シングルセッション OS マシンカタログ（永続的および非永続的）のみがサポートされています。
- エフェメラル OS ディスクと MCS I/O 機能は、Azure の休止状態をサポートしていません。
- 自動Windowsアップデート中に休止状態が失敗する可能性があります。

詳細については、Microsoftドキュメントを参照してください。

休止状態対応マシンカタログの作成と管理

休止状態対応VMを作成するには、以下を使用して休止状態対応マシンカタログを作成および管理できます。

- Web Studio、または
- PowerShell コマンド

WEB STUDIOを使用してカタログを作成する

1. **マシンカタログの作成**を選択します。カタログ作成ウィザードが開きます。
2. **マシンタイプ**ページで、このカタログの**シングルセッションOS**マシンタイプを選択します。
3. **マシン管理**ページで、次のように設定を選択します。

a. **電源管理されているマシン（仮想マシンやブレードPCなど）**を選択します。

b. **Citrix Machine Creation Services™ (MCS)**を選択します。

4. **デスクトップエクスペリエンス**ページで、必要に応じて、ランダムまたは静的デスクトップエクスペリエンスを選択します。
5. **イメージ**ページで、マスターイメージを選択します。**マシンプロファイルを使用**チェックボックスを選択し、休止状態をサポートするマシンプロファイルを選択します。ツールチップをクリックして、マシンプロファイルが休止状態をサポートしているかどうかを確認します。
6. **ストレージとライセンスの種類**ページで、このカタログに使用するストレージとライセンスを選択します。
7. 「**仮想マシン**」ページで、VM の数、VM サイズ、および可用性ゾーンを選択します。

> 「**注:**」：
>
> ハイバネーションをサポートするマシンサイズのみが選択肢として表示されます。

8. 「**NIC**」ページで、VM が使用する NIC を追加します。
9. 「**ディスク設定**」ページで、ライトバックキャッシュディスクのストレージタイプとサイズを選択します。
10. 「**リソースグループ**」ページで、VM をプロビジョニングするリソースグループを選択します。
11. 「**マシン ID**」ページで、「**新しい Active Directory アカウントを作成**」を選択します。次に、アカウントの命名スキームを指定します。
12. 「**ドメイン資格情報**」ページで、「**資格情報を入力**」をクリックします。ターゲットの Active Directory ドメインでアカウント作成を実行するために、ドメイン資格情報を入力します。
13. 「**概要**」ページで、マシンカタログの名前を入力し、「**完了**」をクリックします。

MCS マシンカタログの作成が完了したら、カタログリストでカタログを見つけ、「**テンプレートプロパティ**」タブをクリックします。パラメーター「**休止状態**」の値は「**サポート対象**」である必要があります。

マシンカタログを編集する場合は、以下の制限事項を考慮してください。

- 現在のマシンカタログが休止状態をサポートしている場合、次のことはできません。
  - VM サイズを休止状態に対応していないものに変更する。

    - マシンプロファイルを休止状態に対応していないものに変更する。

- 現在のマシンカタログが休止状態をサポートしていない場合、次のことはできません。

    - 現在、Web Studioを使用して、マシンプロファイルを休止状態対応のものに変更します。

既存の休止状態対応VMを管理するためのマシンカタログを作成する

既に休止状態対応VMをお持ちで、それらを一時停止および再開したい場合は、電源管理のためにそれらのVMをインポートするマシンカタログを作成します。

> **注:**
>
> 休止状態対応VMと非対応VMの両方を含むマシンカタログを作成できます。ただし、休止状態関連の機能が必要な場合は、休止状態対応VMのみを含むマシンカタログを作成する必要があります。

> Web Studioを使用して既存の休止状態対応VMのカタログを作成するには、画面の指示に従って手順を完了し、次の主要な設定に注意してください。

1. **マシン管理**ページで、**電源管理されているマシン**を選択し、マシンの展開方法として**その他のサービスまたはテクノロジー**を選択します。
2. **仮想マシン**ページで、休止状態対応VMのみを追加またはインポートします。

POWERSHELLコマンドを使用してマシンカタログを作成する

休止状態を使用するためのすべての要件を満たした後、`New-ProvScheme`コマンドを使用して、休止状態対応のマシンカタログを作成できます。Remote PowerShell SDKを使用してカタログを作成する方法については、New-ProvSchemeを参照してください。

カタログの作成中に、次のPowerShellコマンドを使用して、VMサイズとマシンプロファイルが休止状態をサポートしているかどうかを確認できます。

- VMサイズについては、次のコマンドを実行し、プロパティ`supportsHibernation`が**True**であるかどうかを確認します。例：

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath
@("XDHyp:\HostingUnits\ <VirtualNetwork> \serviceoffering.folder") |
select Name, AdditionalData | ConvertTo-Json
```

- マシンプロファイルについては、次のコマンドを実行し、プロパティ`supportsHibernation`が**True**であるかどうかを確認します。例：

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath
@("XDHyp:\HostingUnits\ <VirtualNetwork>
\machineprofile.folder\abc.resourcegroup")|select Name, AdditionalData|
ConvertTo-Json
```

マシンカタログを編集する場合、次の制限事項を考慮してください。

- 現在のマシンカタログが休止状態をサポートしている場合、次のことはできません。
  - VMサイズを休止状態非対応のものに変更する
  - マシンプロファイルを休止状態非対応のものに変更する
- 現在のマシンカタログが休止状態をサポートしていない場合、次のことはできません。
  - 現在、Web Studioを使用してマシンプロファイルを休止状態対応のものに変更します。

Remote PowerShell SDKを使用してカタログのVMサイズとマシンプロファイルを変更する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/>`を参照してください。

休止状態プロパティの確認

PowerShellコマンドを使用して、マシンカタログ、VM、およびブローカーマシンの休止状態プロパティを確認できます。

- プロビジョニングスキームの休止状態プロパティを確認するには、次のPowerShellコマンドを実行します。`HibernationEnabled`パラメーターは`True`である必要があります。

```
(Get-ProvScheme -provisioningSchemeName <YourSchemeName>).VMMetadata
-join "" |  ConvertFrom-Json | Select HibernationEnabled
```

- プロビジョニングVMの休止状態プロパティを確認するには、次のPowerShellコマンドを実行します。`SupportsHibernation`パラメーターは`True`である必要があります。

```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json |
Select SupportsHibernation
```

- ブローカーマシンの休止状態容量を確認するには、次のPowerShellコマンドを実行します。**Suspend** および **Resume** の電源アクションは、休止状態機能を示します。

```
(Get-BrokerMachine -MachineName
<YourMachineName>).SupportedPowerActions
```

休止状態対応VMの電源管理

休止状態対応VMに対して、以下の電源管理操作を実行できます。

- 実行状態からVMを**一時停止**する
- 一時停止状態からVMを**再開**する
- 一時停止状態からVMを**強制シャットダウン**する
- 中断状態のVMを**強制再起動**する

詳細については、以下を参照してください。

- 中断
- 再開

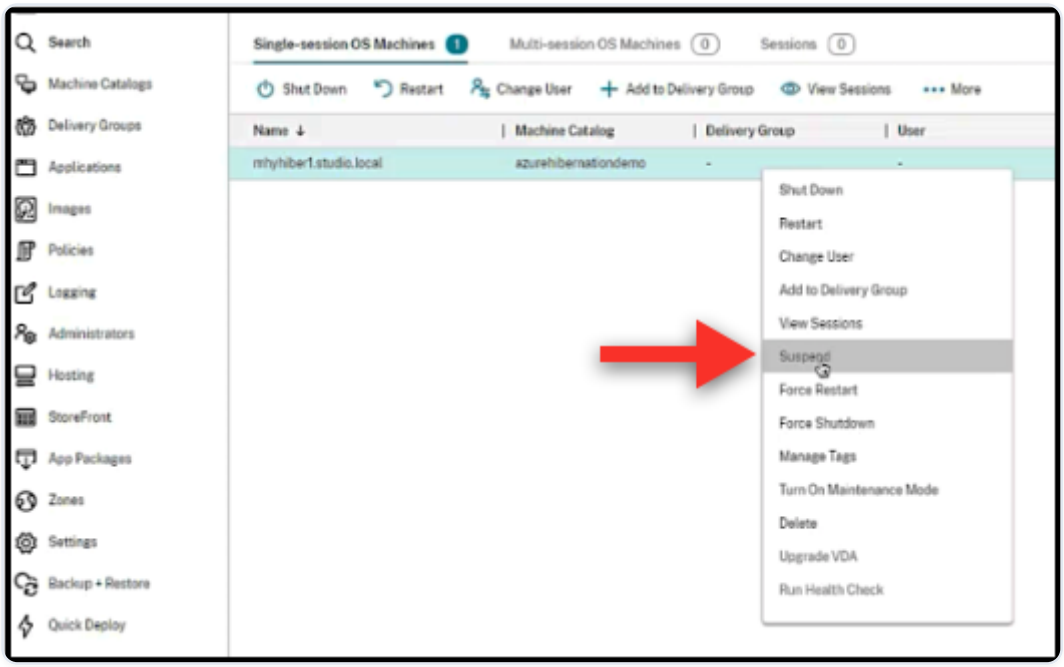
中断

VMを中断するには、次のいずれかの方法を使用できます。

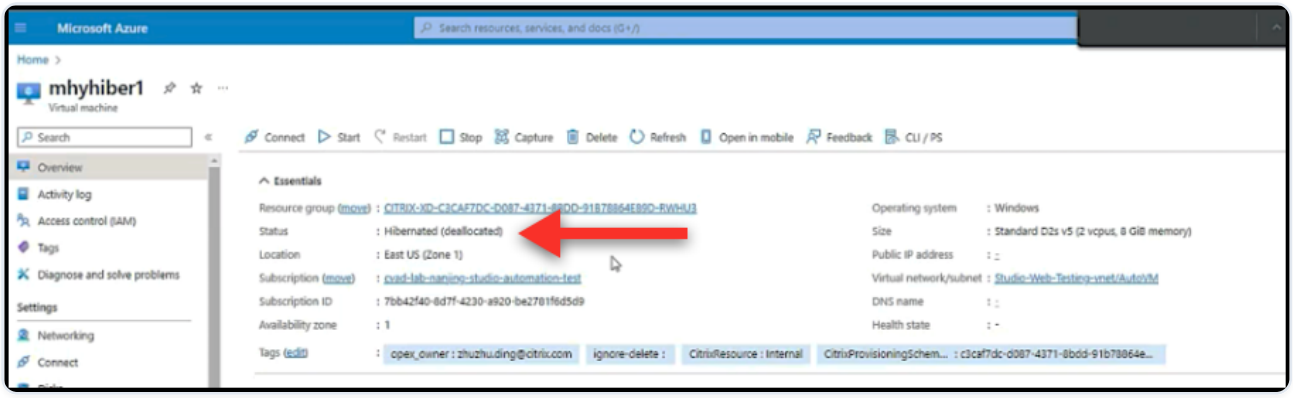
- Web Studioを使用して**手動で**
- タイムアウトポリシーを使用して**自動的に**: 詳細については、その他の設定を参照してください。

VMを手動で中断するには:

1. VMを右クリックし、**中断**を選択します。**はい**をクリックしてアクションを確定します。**電源状態**が**中断中**から**中断済み**に変わります。



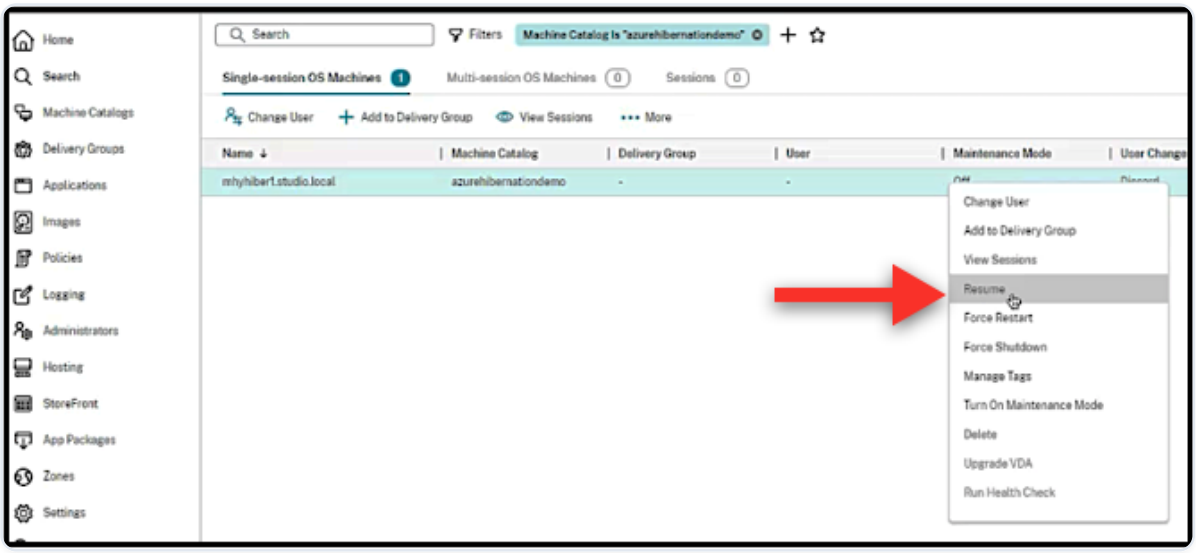
AzureポータルでVMのステータスを確認できます。



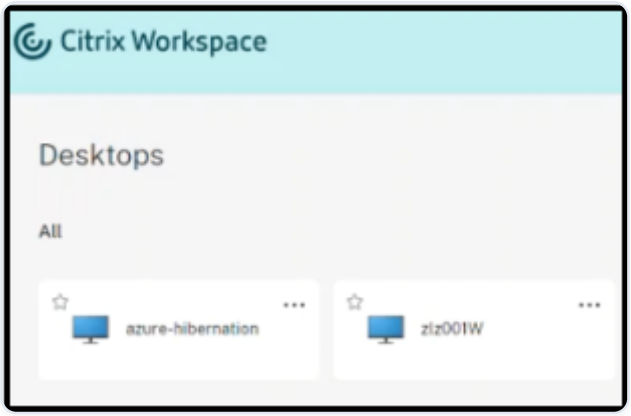
再開

休止状態のVMを再開するには、次のいずれかの方法を使用します:

- **手動で：**
  - 管理者はWeb Studioを使用してVMを再開できます。



- エンドユーザーは、デスクトップアイコンをクリックすると、Citrix Workspace™メニューを使用してVMを起動できます。



- **自動的に：**
  - ピーク時間を正しく設定すると、Autoscale™は休止状態のマシンを自動的に起動できます。タイムスケジュールをクリックすることで、ピーク時間を30分間隔で設定できます。各青い枠は、ピーク時間としてマークされたタイムスロットを表します。ピーク時間には、連続したタイムスロットと非連続のタイムスロットの両方を含めることができます。
    - 連続したタイムスロット

      「連続したピーク時間帯」(/en-us/citrix-virtual-apps-desktops/2411/media/consecutive-peak-time-autoscale.png)
    - 連続しない時間帯

      「連続しないピーク時間帯」(/en-us/citrix-virtual-apps-desktops/2411/media/non-consecutive-peak-time-autoscale.png)

> **注:**
>
> **Autoscaleの管理 > 負荷ベースの設定**で、**アクション**が**中断**として構成されている場合、そのデリバリーグループ内のすべてのVMが休止機能を備えていることを確認してください。そうでない場合、休止できないVMは実行を継続します。

> 「オートスケール負荷ベース設定の管理」(/en-us/citrix-virtual-apps-desktops/2411/media/azure-hibernation-autoscale.png)

休止状態の失敗に関する警告メッセージを取得する

MCSプロビジョニング済みおよび既存の休止状態対応VMの休止状態失敗の場合に、PowerShellコマンド `Get-ProvOperationEvent` を使用して警告メッセージを取得できます。PowerShellコマンドの詳細については、SDKドキュメントのGet-ProvOperationEventを参照してください。

これを行うには：

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*` を実行します。
3. 休止状態の失敗時に警告メッセージを取得するには、`Get-ProvOperationEvent` を実行します。

   ```
   Get-ProvOperationEvent -filter { OperationName -eq "Suspend" }
   ```

   出力:

   ```
   EventAdditionalData : Error code = OperationNotAllowed and Error
   message = The Hibernate-Deallocate Operation cannot be performed on a
   VM that has extension 'AzureHibernateExtension' in failed state. For
   more information, see https://aka.ms/hibernate-resume/errors. Error
   details from the extension : Enabling

                    hibernate failed. Response from the powercfg command.
   Exit Code: 1. Error message:

                    Hibernation failed with the following error: The
   request is not supported.
   ```

```
                  The following items are preventing hibernation on
this system.

                    The current Device Guard configuration has disabled
hibernation.

                    An internal system component has disabled
hibernation.

                            Hypervisor

                  Status: 409

                  ErrorCode: OperationNotAllowed



                  Content:

                  {

                    "error": {

                      "code": "OperationNotAllowed",

                      "message": "The Hibernate-Deallocate Operation
cannot be performed on a VM that has extension
'AzureHibernateExtension' in failed state. For more information, see
https://aka.ms/hibernate-resume/errors. Error details from the
extension : Enabling hibernate failed. Response from the

                  powercfg command. Exit Code: 1. Error message:
\nHibernation failed with the following error: The request is not
supported.\r\r\n\r\nThe following items are preventing hibernation on
this system.\r\n\tThe current Device Guard configuration has disabled
hibernation.\r\n\tAn internal system

                  component has disabled hibernation.
\r\n\t\tHypervisor"

                    }

                  }
```

```
EventCategory       : Warning

EventDateTime       : 1/11/2024 4:18:31 AM

EventId             : 0

EventMessage        : Failed to suspend machine my-resource-group/my-
vm.

EventSeverity       : Important

EventSource         : AzureRmPlugin

EventState          : New

LinkedObjectType    : ProvisioningScheme

LinkedObjectUid     : 589cb600-6e65-479f-9d47-9715c4732366

OperationName       : Suspend

OperationTargetName : my-resource-group/my-vm

OperationTargetType : VirtualMachine

OperationType       : PowerManagement

Recommendation      :
```

休止状態の問題のトラブルシューティング

休止状態と信頼できる起動VM機能の両方を有効にしようとすると、ゲストOSの構成が正しくない場合、次のエラーメッセージが表示されます。

エラーコード	エラーメッセージ
OperationNotAllowed	失敗状態の拡張機能「AzureHibernateExtension」を持つVMでは、休止状態解除操作を実行できません。詳細については、`<https://aka.ms/hibernate-resume/errors/>` を参照してください。拡張機能からのエラー詳細: 休止状態の有効化に失敗しました。powercfgコマンドからの応答。

エラーコード	エラーメッセージ
	終了コード: 1。エラーメッセージ: 次のエラーにより休止状態に失敗しました: 要求はサポートされていません。以下の項目がこのシステムでの休止状態を妨げています。**現在のDevice Guard構成により休止状態が無効になっています。内部システムコンポーネントにより休止状態が無効になっています。**

この問題を解決するには、ゲストVM内で仮想化が有効になっていることを確認してください。たとえば、Windows環境でHyper-Vが有効になっていることを確認します。Microsoft Windowsの制限によると、休止状態は、VMで信頼できる起動が有効になっている場合にのみ、ネストされた仮想化でサポートされます。

警告メッセージの詳細については、MicrosoftドキュメントのVM休止状態のトラブルシューティングを参照してください。

> **注:**
>
> VMの再開失敗に関連するエラーメッセージは、将来のリリースで利用可能になります。

詳細情報

Citrix Azure のハイバネーションに関する詳細については、Citrix Tech Zone の記事 を参照してください。

セキュリティポリシー

この記事では、さまざまなサポート対象クラウドサービスにおけるセキュリティ機能について説明します。セキュリティ機能には以下が含まれます。

- セキュリティグループ(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/security-policies/security-group.html)
- セキュアブート(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/security-policies/secure-boot.html)
- 暗号化機能(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/security-policies/encryption-capabilities.html)

セキュリティグループ

セキュリティグループは、仮想ネットワーク内のリソース間のネットワークトラフィックをフィルタリングするためのセキュリティルールのグループです。セキュリティルールは、いくつかの種類のリソースに対するインバウンドネットワークトラフィックまたはアウトバウンドネットワークトラフィックを許可または拒否します。各ルールは次のプロパティを指定します。

- 名前: ネットワークセキュリティグループ内で一意の名前
- 優先度: ルールは優先度順に処理されます。数値が小さいほど優先度が高いため、数値が小さいルールは数値が大きいルールよりも先に処理されます。
- 送信元または宛先: 任意、または個別のIPアドレス、クラスレスドメイン間ルーティング (CIDR) ブロック (例: 10.0.0.0/24)、サービスタグ、またはアプリケーションセキュリティグループ
- プロトコル: 各セキュリティグループのルールを追加する際の基準となるプロトコル
- 方向: ルールがインバウンドトラフィックまたはアウトバウンドトラフィックのどちらに適用されるか
- ポート範囲: 個別のポートまたはポートの範囲を指定できます
- アクション: 許可または拒否

サポートされているハイパーバイザーの詳細については、以下を参照してください。

- AWS のセキュリティグループ(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/security-policies/security-group.html#security-groups-in-aws)
- Microsoft Azure のセキュリティグループ(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/security-policies/security-group.html#security-groups-in-microsoft-azure)
- Google Cloud Platform のセキュリティグループ(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/security-policies/security-group.html#security-groups-in-google-cloud-platform)

AWS のセキュリティグループ

セキュリティグループは、VPC 内のインスタンスのトラフィックを制御する仮想ファイアウォールとして機能します。パブリックサブネット内のインスタンスがプライベートサブネット内のインスタンスと通信できるようにするルールをセキュリティグループに追加します。これらのセキュリティグループを VPC 内の各インスタンスに関連付けることもできます。インバウンドルールはインスタンスへの受信トラフィックを制御し、アウトバウンドルールはインスタンスからの送信トラフィックを制御します。

イメージ準備中のネットワーク設定の詳細については、イメージ準備中のネットワーク設定を参照してください。

インスタンスを起動するときに、1つ以上のセキュリティグループを指定できます。セキュリティグループを構成するには、セキュリティグループの構成を参照してください。

Microsoft Azure のセキュリティグループ

Citrix Virtual Apps and Desktops は、Azure のネットワークセキュリティグループをサポートしています。ネットワークセキュリティグループは、サブネットに関連付けられることが想定されています。詳細については、ネットワークセキュリティグループを参照してください。

イメージの準備中に作成されるネットワークセキュリティグループの詳細については、「Azure Resource Manager イメージを使用してマシンカタログを作成する」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#create-a-machine-catalog-using-an-azure-resource-manager-image-in-web-studio)を参照してください。

Google Cloud Platform のセキュリティグループ

マシンカタログの準備中に、カタログのマスターイメージシステムディスクとして機能するマシンイメージが準備されます。このプロセスが発生すると、ディスクは一時的に仮想マシンに接続されます。このVMは、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを防止する分離された環境で実行する必要があります。これは、すべてのトラフィックを拒否するファイアウォールルールのペアによって実現されます。詳細については、ファイアウォールルールを参照してください。

セキュアブートとvTPM

セキュアブートは、システムの起動を担当するUnified Extensible Firmware Interface (UEFI) の機能です。これにより、起動プロセス中に信頼できるソフトウェアのみがロードされることが保証されます。

Trusted Platform Module (TPM) は、暗号化キーやその他の機密データを安全に保存するためのハードウェアチップです。Virtual Trusted Platform Module (vTPM) は、TPM と同じ機能を実行しますが、暗号化コプロセッサ機能をソフトウェアで実行します。TPM はセキュリティを強化できますが、Secure Boot の要件ではありません。

サポートされているクラウドサービスの詳細については、以下を参照してください。

- AWS での Secure Boot と NitroTPM
- Google Cloud Platform でのセキュアブートと vTPM
- Microsoft Azure でのセキュアブートと vTPM
- VMware での vTPM

- XenServer 用の Secure Boot と vTPM

AWS でのセキュアブートとNitroTPM

AWS 環境では、NitroTPM および/または UEFI Secure Boot が有効になっているマスターイメージ (AMI) を選択できます。これにより、カタログ内のプロビジョニングされた VM も NitroTPM および/または UEFI Secure Boot が有効になります。この実装により、VM が保護され、信頼できることが保証されます。NitroTPM および UEFI Secure Boot の詳細については、Amazon ドキュメント を参照してください。NitroTPM および UEFI Secure Boot が有効なカタログを作成するには、VM インスタンスの NitroTPM および UEFI Secure Boot を有効にする を参照してください。

Google Cloud Platform でのセキュアブートとvTPM

Google Cloud Platform (GCP) でシールドされた仮想マシンをプロビジョニングできます。シールドされた VM の検証可能な整合性は、次の機能を使用することで実現されます。

- セキュアブート
- vTPM対応メジャーブート
- 整合性監視

シールドされたVMでカタログを作成するためにPowerShellを使用する方法の詳細については、「Using PowerShell to create a catalog with shielded VM」を参照してください。

> **注:**
>
> マスターイメージにWindows 11をインストールする場合、マスターイメージ作成プロセス中にvTPMを有効にする必要があります。また、カタログ作成にマシンプロファイルを使用する場合、マシンプロファイルソース（VMまたはインスタンステンプレート）でvTPMを有効にする必要があります。単一テナントノードでWindows 11 VMを作成する方法については、「Create Windows 11 VMs on the sole-tenant node」を参照してください。

Microsoft Azure での セキュアブートと vTPM

Azure環境では、Trusted Launchが有効なマシンカタログを作成できます。Azureは、第2世代VMのセキュリティを向上させるシームレスな方法としてTrusted Launchを提供します。Trusted Launchは、高度で永続的な攻撃手法から保護します。Trusted Launchを有効にするには、マシンプロファイルベースのカタログ構成を使用します。Trusted Launchの根幹には、VM用のSecure Bootがあります。Trusted Launchは、クラウドによるリモートアテステーションを実行するためにvTPMも使用します。これは、プラットフォームの健全性チェックと信頼に基づく意思決定に使用

されます。Secure BootとvTPMは個別に有効にできます。Trusted Launchを使用してマシンカタログを作成する方法の詳細については、「Machine catalogs with Trusted launch」を参照してください。

VMwareでのvTPM

MCSはvTPMを使用したマシンカタログの作成をサポートしています。マスターイメージにWindows 11がインストールされている場合、マスターイメージでvTPMが有効になっている必要があります。マシンプロファイルベースの構成が使用され、vTPMが有効になっている場合、カタログ内のVMはVMテンプレートから同じvTPMコンテンツを継承します。マシンプロファイルが使用されておらず、マスターイメージでvTPMが有効になっている場合、カタログ内のVMは空のvTPMを持ちます。詳細については、「Create a machine catalog using a machine profile」を参照してください。

XenServer®でのSecure BootとvTPM

XenServer は、サポートされている一部の VM オペレーティングシステムで UEFI セキュアブートを提供します。セキュアブートは、署名されていない、誤って署名された、または変更されたバイナリが起動中に実行されるのを防ぎます。セキュアブートを強制する UEFI 対応 VM では、すべてのドライバーが署名されている必要があります。詳細については、「ゲスト UEFI とセキュアブート」を参照してください。

XenServer 8では、UEFI Secure BootにvTPMは必須ではありません。ただし、vTPMをVMにリンクするには、Secure Bootが有効であるかどうかにかかわらず、そのVMがUEFIで起動されている必要があります。Windows 11 VMにはリンクされたvTPMが必要であり、提供されたテンプレートからWindows 11 VMが作成されるときに自動的に作成されます。他のオペレーティングシステムの場合、vTPMはオプションです。詳細については、「vTPM」を参照してください。

暗号化機能

暗号化機能は、共有仮想マシンホスト上の悪意のあるゲストによる攻撃や、ホスト上のすべての仮想マシンを管理するハイパーバイザー制御ソフトウェアによる攻撃から、仮想マシンのコンテンツを保護します。

サポートされているクラウドサービスの詳細については、以下を参照してください。

- AWS の暗号化機能
- Google Cloud Platform の暗号化機能
- Microsoft Azure の暗号化機能

AWS の暗号化機能

このセクションでは、AWS 仮想化環境における暗号化機能について説明します。

自動暗号化

アカウントで作成された新しい Amazon EBS ボリュームとスナップショットコピーの自動暗号化を有効にできます。詳細については、「自動暗号化」を参照してください。

Google Cloud Platform の暗号化機能

このセクションでは、Google Cloud Platform (GCP) 仮想化環境における暗号化機能について説明します。

Google マネージド暗号化キーが許可するよりもキー操作をより詳細に制御する必要がある場合は、顧客管理の暗号化キーを使用できます。顧客管理の暗号化キーを使用すると、オブジェクトがバケットに保存されるときに Cloud Storage によってキーで暗号化され、リクエスターに提供されるときに Cloud Storage によって自動的に復号化されます。詳細については、「顧客管理の暗号化キー」を参照してください。

MCS カタログに顧客管理の暗号化キー (CMEK) を使用できます。詳細については、「顧客管理の暗号化キー (CMEK) の使用」を参照してください。

Microsoft Azure の暗号化機能

このセクションでは、Azure仮想化環境における暗号化機能について説明します。

Azureサーバー側暗号化

ほとんどのAzureマネージドディスクは、データを保護し、セキュリティおよびコンプライアンスのコミットメントを満たすのに役立つサーバー側暗号化 (SSE) を使用するAzure Storage暗号化で暗号化されています。Citrix Virtual Apps and Desktopsは、Azure Key Vaultを介したAzureマネージドディスクの顧客管理暗号化キーをサポートしています。詳細については、「Azureサーバー側暗号化」を参照してください。

ホストでのAzureディスク暗号化

ホストでの暗号化機能を備えたMCSマシンカタログを作成できます。

この暗号化方法は、Azureストレージを介してデータを暗号化しません。VMをホストするサーバーがデータを暗号化し、その後、暗号化されたデータがAzureストレージサーバーを介して流れます。したがって、この暗号化方法はデータをエンドツーエンドで暗号化します。

ホストでの暗号化機能を持つMCSマシンカタログの作成の詳細については、「ホストでのAzureディスク暗号化」を参照してください。

Azure二重暗号化

二重暗号化は、プラットフォーム側暗号化 (デフォルト) と顧客管理暗号化 (CMEK) です。したがって、暗号化アルゴリズム、実装、または侵害されたキーに関連するリスクを懸念するセキュリティ意識の高いお客様は、この二重暗号化を選択できます。永続的なOSディスクとデータディスク、スナップショット、およびイメージはすべて、二重暗号化によって保存時に暗号化されます。詳細については、「マネージドディスクの二重暗号化」を参照してください。

Azure機密VM

Azure機密コンピューティングVMは、仮想デスクトップがメモリ内で暗号化され、使用中に保護されることを保証します。

MCSを使用して、Azure機密VMを含むカタログを作成できます。そのようなカタログを作成するには、マシンプロファイルワークフローを使用する必要があります。マシンプロファイルの入力として、VMとARMテンプレート仕様の両方を使用できます。

詳細については、「Azure機密VM」を参照してください。

マシンの負荷分散

負荷分散は、組織がクラウドのあらゆる利点を活用しながら、望ましいコストバランスを達成するのに役立ちます。負荷分散はデリバリーグループレベルで構成されます。

> **注:**
>
> 負荷分散は、マルチセッションOSマシンにのみ適用されます。

> 負荷分散には2つのオプションがあります。

- 水平負荷分散
- 垂直負荷分散

デフォルトでは、水平負荷分散が有効になっています。

水平負荷分散: 水平負荷分散モデルでは、受信ユーザーセッションは利用可能な最も負荷の低いマシンに割り当てられます。この例を考えてみましょう。展開環境に2つのVDAがあると仮定します。1つはアクティブなユーザーセッション（ユーザー1）を持ち、2番目のユーザー（ユーザー2）はセッションを待っています。水平負荷分散アルゴリズムは、より有利な負荷インデックスを持つVDA 2にユーザー2を割り当てます。したがって、水平アルゴリズムはすべての利用可能な

VDAにセッションを分散するため、負荷が減少したときにマシンがシャットダウンするのを妨げる可能性があります。

垂直負荷分散: 垂直負荷分散モデルでは、セッションは最も高い負荷インデックスを持つVDAに割り当てられます。これにより、受信ユーザーセッションを他のユーザーがすでに使用しているVDAに統合し、ユーザーセッションのために電源をオンにして準備しておく必要があるVDAの数を減らすことができます。水平負荷分散で述べたのと同じ展開環境を考えてみましょう。ユーザー1はVDA 1に割り当てられ、垂直負荷分散アルゴリズムがユーザー2のセッションに適用されます。負荷インデックスが高いのはVDA 1であるため、ユーザー2はVDA 1に割り当てられます。したがって、すべての受信セッションは、高負荷インデックスのウォーターマークに達するまで、最も負荷の高いVDAに割り当てられます。その後初めて、他のVDAがセッションの受信を開始します。

サイトレベルでの負荷分散設定

すべてのデリバリーグループに対して負荷分散を構成できます（サイト全体の構成）。

Studioからこの機能を構成するには、左ペインで**設定**を選択します。**マシンの負荷分散セッション**の下のオプションを選択します。

または、PowerShellを使用して、サイト全体で垂直負荷分散を有効または無効にすることもできます。`Set-BrokerSite` コマンドレットで `UseVerticalScalingForRdsLaunches` 設定を使用します。`UseVerticalScalingForRdsLaunches` 設定の値を表示するには `Get-BrokerSite` を使用します。詳細については、コマンドレットのヘルプを参照してください。

> **ヒント:**
>
> マシンがホストできるセッションの最大数を指定するには、最大セッション数 ポリシー設定を使用します。

デリバリーグループレベルでの負荷分散設定

ロードバランシングはデリバリーグループレベルで構成でき、サイトレベルから継承されたロードバランシング設定を上書きできます。

これは、デリバリーグループの作成時または既存のデリバリーグループの編集時に構成できます。手順2. 負荷分散を参照してください。

ロード管理

負荷管理は、サーバーの負荷を測定し、現在の環境条件でどのサーバーを選択するかを決定します。この選択は、以下に基づいています。

- **サーバーメンテナンスモードの状態**: マルチセッションOSマシンは、メンテナンスモードがオフの場合にのみ負荷分散の対象となります。
- **サーバー負荷インデックス**: マルチセッションOSマシンを提供するサーバーが接続を受け入れる可能性を決定します。このインデックスは、セッション数やCPU、ディスク、メモリ使用量などのパフォーマンスメトリックの設定といった負荷評価子の組み合わせです。負荷評価子は、負荷管理ポリシー設定で指定されます。デフォルトでは、負荷インデックスは計算にセッション数のみを使用し、CPU、ディスク、メモリは負荷管理ポリシー設定で構成されるまで使用しません。ポリシー設定の詳細については、負荷管理ポリシー設定を参照してください。

  サーバー負荷インデックスが10000の場合、サーバーが完全に負荷されていることを示します。他のサーバーが利用できない場合、ユーザーはセッションを起動したときに、デスクトップまたはアプリケーションが現在利用できないというメッセージを受け取る可能性があります。 負荷インデックスは、Director (Monitor)、Studio検索、およびSDKで監視できます。

  コンソール表示で、**サーバー負荷インデックス**列（デフォルトでは非表示）を表示するには、マシンを選択し、列ヘッダーを右クリックして、**列の選択**を選択します。**マシンカテゴリ**で、**負荷インデックス**を選択します。

  SDKでは、`Get-BrokerMachine` コマンドレットを使用します。詳細については、「CTX202150」を参照してください。

- **同時ログオン許容ポリシー設定**: サーバーへの同時ログオン要求の最大数。（この設定は、XenApp 6.xバージョンでの負荷スロットリングに相当します。）

  すべてのサーバーが同時ログオン許容設定以上の場合、次のログオン要求は保留中のログオンが最も少ないサーバーに割り当てられます。複数のサーバーがこれらの基準を満たす場合、負荷インデックスが最も低いサーバーが選択されます。「同時ログオン許容」を参照してください。

  > **ヒント:**
  >
  > ログオン許容設定を適用し、指定された数を超える同時ログオンを失敗させるには、`Set-BrokerServiceConfigurationData Core.LogonToleranceIsHardLimit -SettingValue $true` を実行できます。

デリバリーグループの作成

> **注:**
>
> Citrix Virtual Apps and Desktops™の展開は、Web Studio (Webベース) と Citrix Studio (Windowsベース) の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> デリバリーグループは、1つ以上のマシンカタログから選択されたマシンの集合です。デリバリーグループは、どのユーザーがそれらのマシンを使用できるか、およびそれらのユーザーが利用できるアプリケーションとデスクトップを指定します。

デリバリーグループの作成は、サイトとマシンカタログを作成した後の展開構成における次のステップです。後で、最初のデリバリーグループの初期設定を変更したり、他のデリバリーグループを作成したりできます。また、デリバリーグループの作成時ではなく、編集時にのみ構成できる機能や設定もあります。

> **注:**
>
> MMCベースのStudioを使用してデリバリーグループを作成またはアップグレードする場合、Autoscale™はデフォルトで有効になります。

> リモートPCアクセスの場合、サイトを作成すると、「Remote PC Access Desktops」という名前のデリバリーグループが自動的に作成されます。

デリバリーグループを作成するには：

1. デリバリーグループなしでサイトとマシンカタログを作成した場合、Web Studioはデリバリーグループを作成するための適切な開始場所に案内します。
2. すでにデリバリーグループを作成しており、別のデリバリーグループを作成したい場合は、次の手順に従ってください。

    a. **デリバリーグループ**を選択します。アクションペインで**デリバリーグループの作成**を選択します。

b. フォルダーを使用してデリバリーグループを整理するには、デフォルトの**デリバリーグループ**フォルダーの下にフォルダーを作成します。詳細については、「フォルダーを作成する」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/delivery-groups-manage.html#create-a-delivery-group-folder)を参照してください。

c. グループを作成したいフォルダーを選択し、**デリバリーグループの作成**をクリックします。グループ作成ウィザードが開きます。

3. ウィザードは**はじめに**ページで起動します。このページは、今後のウィザード起動時に表示しないように設定できます。
4. ウィザードは、次のセクションで説明されているページを案内します。各ページの作業が完了したら、最後のページに到達するまで**次へ**をクリックします。

ステップ1. マシン

ページで、カタログを選択し、そのカタログから使用するマシンの数を選択します。

知っておくと良いこと:

- 選択したカタログでは、少なくとも1台のマシンが未使用のままである必要があります。
- カタログは複数のデリバリーグループで指定できます。マシンは1つのデリバリーグループでのみ使用できます。
- デリバリーグループは複数のカタログのマシンを使用できますが、それらのカタログには同じマシンタイプ（マルチセッションOS、シングルセッションOS、またはRemote PC Access）が含まれている必要があります。つまり、デリバリーグループ内でマシンタイプを混在させることはできません。同様に、展開にWindowsマシンのカタログとLinuxマシンのカタログがある場合、デリバリーグループはどちらかのOSタイプのマシンを含めることができますが、両方を含めることはできません。
- Citrixは、すべてのマシンを最新のVDAバージョンでインストールまたはアップグレードすることを推奨します。必要に応じてカタログとデリバリーグループをアップグレードしてください。デリバリーグループを作成する際に、異なるVDAバージョンがインストールされているマシンを選択した場合、デリバリーグループは最も古いVDAバージョンと互換性があります。これはグループの*機能レベル*と呼ばれます。たとえば、マシンの1つにVDAバージョン7.1がインストールされており、他のマシンに現在のバージョンがインストールされている場合、グループ内のすべてのマシンはVDA 7.1でサポートされていた機能のみを使用できます。これは、より新しいVDAバージョンを必要とする一部の機能がそのデリバリーグループでは利用できない可能性があることを意味します。
- Remote PC Accessカタログ内の各マシンは、デリバリーグループに自動的に関連付けられます。Remote PC Accessサイトを作成すると、「Remote PC Access Machines」という名前の

カタログと「Remote PC Access Desktops」という名前のデリバリーグループが自動的に作成されます。

- 以下の互換性チェックが実行されます。
  - MinimumFunctionalLevelは互換性がある必要があります
  - SessionSupportは互換性がある必要があります
  - AllocationTypeはSingleSessionと互換性がある必要があります
  - ProvisioningTypeは互換性がある必要があります
  - PersistChangesはMCSおよびCitrix Provisioning™と互換性がある必要があります
  - RemotePCカタログはRemote PC Accessカタログとのみ互換性があります
  - AppDisk関連のチェック

ステップ2. 負荷分散

デリバリーグループの作成中に負荷分散設定を構成するには：

1. Web Studioにサインインします。
2. 左側のナビゲーションで、**Delivery Groups**をクリックします。
3. **Delivery Groups**ページで、**Create Delivery Group**をクリックします。
4. **Create Delivery Group**ウィザードで、**Next**をクリックします。**Machine**ウィザードが開きます。
5. **Machines**ウィザードで、必要なマシンカタログを選択し、**Next**をクリックします。**Load Balancing**ウィザードが開きます。
6. **Load Balancing**ウィザードで、**Override site-wide setting**チェックボックスをオンにします。
7. 必要に応じて、**Horizontal load balancing**または**Vertical load balancing**オプションを選択し、**Next**をクリックします。

   デリバリーグループの作成中の負荷分散設定(/en-us/citrix-virtual-apps-desktops/2411/media/load-balance-create-delivery-group.png)

既存のデリバリーグループの編集中に負荷分散設定を構成するには：

1. Web Studioにサインインします。
2. 左ペインで、**デリバリーグループ**をクリックします。

3. リストから**デリバリーグループ**を選択し、**編集**をクリックします。**デリバリーグループの編集**ウィザードが開きます。
4. **デリバリーグループの編集**ページで、**負荷分散**をクリックします。
5. **サイト全体の構成を上書き**チェックボックスをオンにします。
6. 必要に応じて、**水平負荷分散**または**垂直負荷分散**オプションを選択し、**保存**をクリックします。

   デリバリーグループの編集中の負荷分散設定(/en-us/citrix-virtual-apps-desktops/2411/media/load-balance-edit-delivery-group.png)

> **注:**
>
> 垂直負荷分散設定が適用されている場合、**同時ログオン許容数**および**最大セッション数**ポリシーが適切に構成されていることを確認してください。

> デリバリーグループの作成または編集時の垂直負荷分散のポリシー設定(/en-us/citrix-virtual-apps-desktops/2411/media/related-policy-settings-for-vertical-load-balancing-creating-dg.png)

> サイトおよびデリバリーグループレベルでの負荷分散の詳細については、「マシンの負荷分散」を参照してください。

ステップ3. 配信の種類

このページは、静的（割り当て済み）シングルセッションOSマシンを含むカタログを選択した場合にのみ表示されます。

配信の種類ページで、**アプリケーション**または**デスクトップ**のいずれかを選択します。両方を有効にすることはできません。

マルチセッションOSまたはシングルセッションOSランダム（プールされた）カタログからマシンを選択した場合、デリバリーの種類はアプリケーションとデスクトップであると見なされます。アプリケーション、デスクトップ、またはその両方をデリバリーできます。

ステップ4. ユーザー

デリバリーグループ内のアプリケーションとデスクトップを使用できるユーザーとユーザーグループを指定します。

ユーザーリストの指定場所

Active Directoryのユーザーリストは、以下を作成または編集する際に指定します。

- Web Studioでは構成されないサイトのユーザーアクセスリスト。デフォルトでは、アプリケーションエンタイトルメントポリシーのルールにはすべてのユーザーが含まれます。詳細については、PowerShell SDKの`BrokerAppEntitlementPolicyRule`コマンドレットを参照してください。
- アプリケーショングループ（構成されている場合）。
- デリバリーグループ。
- アプリケーション。

StoreFront™を介してアプリケーションにアクセスできるユーザーのリストは、上記のユーザーリストの交差によって形成されます。たとえば、他のグループへのアクセスを不必要に制限することなく、特定の部署にアプリケーションAの使用を構成するには、次の手順を実行します。

- すべてのユーザーを含むデフォルトのアプリケーションエンタイトルメントポリシーのルールを使用します。
- デリバリーグループのユーザーリストを構成して、すべての本社ユーザーがデリバリーグループで指定された任意のアプリケーションを使用できるようにします。
- （アプリケーショングループが構成されている場合）アプリケーショングループのユーザーリストを構成して、管理および財務部門のメンバーがアプリケーションAからLにアクセスできるようにします。
- アプリケーションAのプロパティを構成して、その可視性を管理および財務部門の売掛金担当者のみに制限します。

認証済みユーザーと未認証ユーザー

ユーザーには、認証済みユーザーと未認証ユーザー（未認証は匿名とも呼ばれます）の2種類があります。デリバリーグループでは、これらの種類のいずれかまたは両方を構成できます。

- **認証済み:** アプリケーションとデスクトップにアクセスするには、名前で指定したユーザーとグループメンバーが、スマートカードやユーザー名とパスワードなどの資格情報をStoreFrontまたはCitrix Workspace™アプリに提示する必要があります。シングルセッションOSマシンを含むデリバリーグループの場合、後でデリバリーグループを編集してユーザーデータ（ユーザーリスト）をインポートできます。
- **未認証（匿名）：**マルチセッションOSマシンを含むデリバリーグループの場合、ユーザーはStoreFrontまたはCitrix Workspaceアプリに資格情報を提示することなく、アプリケーションとデスクトップにアクセスできます。たとえば、キオスクではアプリケーションに資格情報が

必要な場合がありますが、Citrixアクセス ポータルとツールは必要ありません。最初のDelivery Controllerをインストールすると、匿名ユーザーグループが作成されます。

認証されていないユーザーにアクセスを許可するには、デリバリーグループ内の各マシンにVDA for Windows Server OS（最小バージョン7.6）がインストールされている必要があります。認証されていないユーザーが有効になっている場合、認証されていないStoreFrontストアが必要です。

認証されていないユーザーアカウントは、セッションが起動されたときにオンデマンドで作成され、Anon*XYZ*という名前が付けられます。ここで*XYZ*は一意の3桁の値です。

認証されていないユーザーセッションには、デフォルトで10分間のアイドルタイムアウトがあり、クライアントが切断されると自動的にログオフされます。再接続、クライアント間のローミング、およびWorkspace Controlはサポートされていません。

次の表は、**ユーザー**ページでの選択肢について説明しています。

アクセスを有効にする対象	ユーザーとユーザーグループを追加/割り当てますか？	「認証されていないユーザーにアクセスを許可する」チェックボックスを有効にしますか？
認証済みユーザーのみ	はい	いいえ
認証されていないユーザーのみ	いいえ	はい
認証済みユーザーと未認証ユーザーの両方	はい	はい

ステップ5. アプリケーション

知っておくと便利な情報:

- デフォルトでは、追加する新しいアプリケーションは「Applications」という名前のフォルダーに配置されます。別のフォルダーを指定することもできます。詳細については、「アプリケーションの管理」の記事を参照してください。
- アプリケーションをデリバリーグループに追加するとき、または後で、そのプロパティを変更できます。詳細については、「アプリケーションの管理」の記事を参照してください。
- アプリケーションを追加しようとしたときに、同じ名前のアプリケーションがそのフォルダーに存在する場合、追加するアプリケーションの名前を変更するよう求められます。拒否した場

合、アプリケーションはそのアプリケーションフォルダー内で一意になるサフィックスを付けて追加されます。

- アプリケーションを複数のデリバリーグループに追加する場合、それらすべてのデリバリーグループでアプリケーションを表示するのに十分な権限がないと、表示の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが追加されたすべてのデリバリーグループを含むようにスコープを拡張してください。
- 同じ名前のアプリケーションを同じユーザーに2つ公開する場合、Web Studioでアプリケーション名（ユーザー向け）プロパティを変更してください。そうしないと、ユーザーはCitrix Workspaceアプリで重複した名前を目にすることになります。
- パッケージ化されたアプリケーションを、シングルセッションの静的およびRemote PC Accessデリバリーグループに追加できます。これらのパッケージは、ユーザーがデスクトップまたはリモートPCにサインインするたびに自動的にマウントされます。

追加をクリックして、アプリケーションソースを表示します。

- **スタートメニューから:** 選択したカタログのマスターイメージから作成されたマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。追加したいアプリケーションを選択し、**OK**をクリックします。
- **手動で:** デリバリーグループ内のVDAまたはネットワーク上の他の場所に存在するアプリケーション。このソースを選択すると、新しいページが開き、次の方法で追加するアプリケーションを指定できます。
  - 実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、および管理者とユーザーの表示名を入力します。
  - デリバリーグループ内のVDAからアプリケーションを選択します。これを行うには、**参照**をクリックし、VDAにアクセスするための資格情報を入力し、VDAへの接続を待ってから、VDAからアプリケーションを選択します。選択したアプリケーションのプロパティが、ページ上のフィールドに自動的に入力されます。
- **既存:** 以前にサイトに追加されたアプリケーション（おそらく別のデリバリーグループ内）。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。アプリケーションを追加し、**OK**をクリックします。
- **アプリケーションパッケージ:** App-V、MSIX、またはMSIXアプリ添付アプリケーションパッケージ内のアプリケーション。このソースを選択すると、新しいページが起動し、そこでソースタイプを選択し、表示された結果から追加したいアプリケーションを選択できます。

アプリケーションソースまたはアプリケーションが利用できないか無効な場合、それは表示されないか、選択できません。たとえば、サイトにアプリケーションが追加されていない場合、**既存**のソースは利用できません。または、アプリケーションが選択されたカタログ内のマシンのサポートされているセッションタイプと互換性がない場合があります。

ステップ 6. デスクトップ

このページのタイトルは、**マシン**ページで選択したカタログによって異なります。

- プールされたマシンを含むカタログを選択した場合、このページは**デスクトップ**というタイトルになります。
- シングルセッションの静的マシンを含むカタログを選択し、**配信タイプ**ページで「デスクトップ」を指定した場合、このページは**デスクトップユーザー割り当て**というタイトルになります。
- シングルセッションの静的マシンを含むカタログを選択し、**配信タイプ**ページで「アプリケーション」を指定した場合、このページは**アプリケーションマシンユーザー割り当て**というタイトルになります。

追加をクリックします。ダイアログボックスで、次のようにします。

- 表示名と説明のフィールドに、Citrix Workspaceアプリに表示する情報を入力します。
- デスクトップにタグ制限を追加するには、**このタグを持つマシンへの起動を制限する**を選択し、ドロップダウンリストからタグを選択します。詳しくは、「タグ」を参照してください。
- ラジオボタンを使用して、デスクトップを起動するか、デスクトップの起動時にマシンを割り当てます。ユーザーは、このデリバリーグループにアクセスできるすべてのユーザー、または特定のユーザーとユーザーグループのいずれかになります。
- グループにシングルセッションの静的マシンが含まれている場合は、ユーザーあたりのデスクトップの最大数を指定します。これは1以上の値である必要があります。
- デスクトップ（プールされたマシン用）またはデスクトップ割り当てルール（シングルセッションの静的マシン用）を有効または無効にします。デスクトップを無効にすると、デスクトップの配信が停止します。デスクトップ割り当てルールを無効にすると、ユーザーへのデスクトップの自動割り当てが停止します。
- ダイアログボックスでの作業が完了したら、**OK**をクリックします。

サイト内のデスクトップの最大インスタンス数（PowerShellのみ）

サイト内のデスクトップの最大インスタンス数を構成するには (PowerShell のみ):

- PowerShell で、適切な BrokerEntitlementPolicyRule コマンドレットを MaxPerEntitlementInstances パラメーターと共に使用します。たとえば、次のコマンドレットは `tsvda-desktop` ルールを変更して、サイトで許可されるデスクトップの最大同時インスタンス数を 2 に設定します。2 つのデスクトップインスタンスが実行されている場合、3 番目のサブスクライバーがデスクトップを起動しようとするとエラーが発生します。

  ```
  Set-BrokerEntitlementPolicyRule -Name tsvda-desktop
  -MaxPerEntitlementInstances 2
  ```

- ガイダンスについては、Get-Help コマンドレットを使用してください。たとえば、`Get-Help Set-BrokerEntitlementPolicyRule-Parameter MaxPerEntitlementInstances`。

ステップ 7: ローカルホストキャッシュ設定

この設定は、電源管理されたシングルセッションのプールされたマシンを含むデリバリーグループでのみ表示されます。

デフォルトでは、これらのマシンはデータ漏洩のリスクがあるため、ローカルホストキャッシュ (LHC) モードでは利用できません。デフォルトの動作を変更し、LHC モードで新しいユーザー接続に利用できるようにするには、**リソースを常に利用可能にする** を選択します。

または、PowerShell コマンドを使用してデフォルトの動作を変更することもできます。詳細については、「アプリケーションとデスクトップのサポート」を参照してください。

> **重要:**
>
> 電源管理されたシングルセッションのプールされたマシンへのアクセスを有効にすると、以前のユーザーセッションのデータと変更が後続のセッションに存在する可能性があります。

ローカルホストキャッシュでの使い捨てプールデスクトップ

ローカルホストキャッシュ (LHC) の停止中、プールされたデスクトップは使い捨てとして使用できます。これは、対応可能な VDA に衛生ブロブを発行し、再起動を開始することによって実現されます。このプロセスにより、停止からの復旧時にデスクトップのクリーンな状態が保証されます。対応できないマシンやレガシーマシンでは、再利用が明示的に有効になっている場合にのみ参加します。 この機能は、可用性をよりシームレスにすることで、停止中の顧客満足度を向上させます。

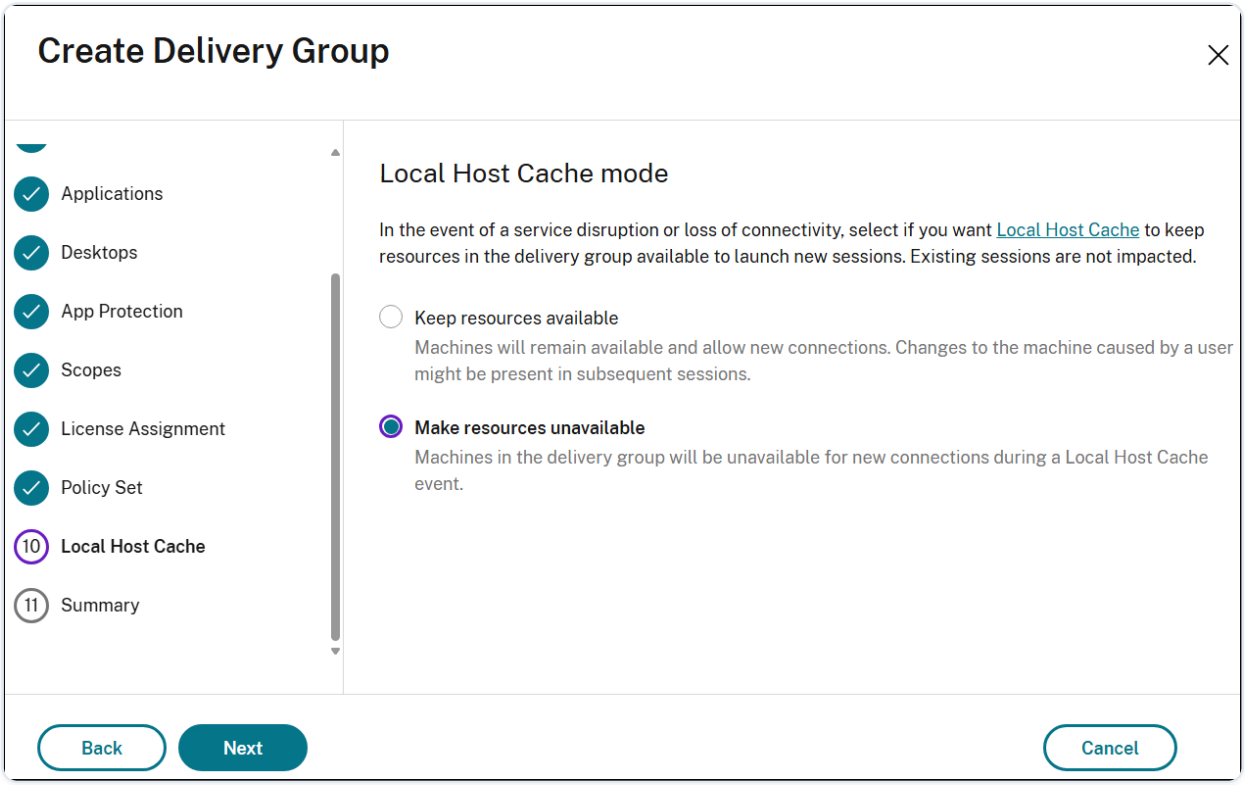
前提条件

- 完全な衛生管理を適用するには、VDA バージョン 2407 以降が必要です。レガシー VDA (VDA バージョン 2407 以前) は、再利用が有効になっている場合にのみ使用できます。これらの VDA は、衛生ブロブや強制再起動を受け取りません。
- シングルセッションマシンを含むマシンカタログ。

プールされたデスクトップの1回限りの使用を構成する

1. VDAビルド2407以降を使用して、シングルセッションマシンを含むMCSカタログを作成します。
2. 対応するデリバリーグループを作成します。Remote PowerShell からデリバリーグループの `ReuseMachinesWithoutShutdownInOutage` デスクトップグループ設定を `false` に設定するか、デリバリーグループの作成時に Web Studio の **［ローカルホストキャッシュモード］** ページで **［リソースを使用不可にする］** を選択します。

```
Set-BrokerDesktopGroup -Name "name"
-ReuseMachinesWithoutShutdownInOutage $false
```



3. 構成が完了すると、LHC停止モード中にマシンは1回限りの使用が可能になります。LHC停止モードが解除されると、汚染されたマシンは再起動され、再度使用できるようになります。

> **注：**

> マシンは、最新の電源投入後にユーザーセッションが開始されると、汚染済みとして分類されます。未汚染のマシンとは、最新の電源投入イベント以降、ユーザーセッションを起動していないマシンを指します。

手順8. 概要

デリバリーグループの名前を入力します。また、Citrix WorkspaceアプリとWeb Studioに表示される説明を（オプションで）入力することもできます。

概要情報を確認し、**「完了」**をクリックします。

デリバリーグループの管理

> **注:**
>
> Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

この記事では、管理コンソールからデリバリーグループを管理する手順について説明します。グループ作成時に指定した設定を変更するだけでなく、デリバリーグループの作成時には利用できないその他の設定を構成することもできます。

手順のカテゴリには、全般、ユーザー、マシン、セッションがあります。一部のタスクは複数のカテゴリにまたがります。たとえば、「ユーザーがマシンに接続できないようにする」はマシンのカテゴリで説明されていますが、ユーザーにも影響します。あるカテゴリでタスクが見つからない場合は、関連するカテゴリを確認してください。

その他の関連情報を含む記事：

- アプリケーションには、デリバリーグループ内のアプリケーションの管理に関する情報が含まれています。
- デリバリーグループの管理には、Delivery Group Administratorの組み込みロール権限が必要です。詳細については、「委任管理」を参照してください。

全般

- グループの詳細を表示
- デリバリーの種類を変更
- StoreFront™アドレスを変更
- 機能レベルを変更
- Remote PC Accessデリバリーグループを管理
- フォルダーを使用してデリバリーグループを整理する
- App Protectionを管理する

グループの詳細を表示

1. 検索機能を使用して特定のデリバリーグループを見つけます。手順については、インスタンスの検索を参照してください。
2. 検索結果から、必要に応じてグループを選択します。
3. グループ列の説明については、次の表を参照してください。
4. このグループの詳細については、下部の詳細ペインのタブをクリックしてください。

列	説明
デリバリーグループ	グループ名とセッションの種類。セッションの種類には、シングルセッションOSとマルチセッションOSが含まれます。
配信内容	このグループから配信されるリソースの種類。可能な値には、アプリケーション、デスクトップ、およびアプリケーションとデスクトップが含まれます。デリバリーグループが専用マシンで構成されている場合、「静的マシン割り当て」が表示されます。
使用中のセッション	設定されているマシンの数と、切断状態にあるマシンの数。
割り当て済み数	デリバリーグループに割り当てられたカタログ内のマシンの数。
フォルダー	**デリバリーグループ**ツリー内のグループの場所。グループが存在するフォルダーの名前（末尾のバックスラッシュを含む）が表示さ

列	説明
	れます。グループがルートレベルにある場合は `-` が表示されます。

デリバリーグループのデリバリーの種類を変更する

デリバリーの種類は、グループが提供できるもの（アプリケーション、デスクトップ、またはその両方）を示します。

アプリケーションのみまたは**デスクトップとアプリケーション**のタイプを**デスクトップのみ**のタイプに変更する前に、グループからすべてのアプリケーションを削除してください。

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. **デリバリータイプ**ページで、目的のデリバリータイプを選択します。
4. 加えた変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

StoreFrontアドレスを変更する

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. **StoreFront**ページで、StoreFront URLを選択または追加します。これらのURLは、デリバリーグループ内の各マシンにインストールされているCitrix Workspace™アプリによって使用されます。
4. 加えた変更を適用してウィンドウを開いたままにするには、「**適用**」をクリックします。変更を適用してウィンドウを閉じるには、「**保存**」をクリックします。

左側のペインで**［StoreFront］**を選択して、StoreFrontサーバーアドレスを指定することもできます。

機能レベルを変更する

デリバリーグループ内のマシン上のVDAと、デリバリーグループで使用されるマシンを含むマシンカタログをアップグレードした後、デリバリーグループの機能レベルを変更します。

開始する前に：

- Citrix Provisioning™（旧Provisioning Services）を使用している場合は、Citrix Provisioningコンソールで VDAバージョンをアップグレードします。

- アップグレードされたVDAを含むマシンを起動して、Delivery Controllerに登録できるようにします。このプロセスにより、デリバリーグループでアップグレードが必要なものがコンソールに通知されます。
- 以前のVDAバージョンを引き続き使用する必要がある場合、新しい製品機能は利用できません。詳しくは、アップグレードのドキュメントを参照してください。

デリバリーグループの機能レベルを変更するには：

1. 左側のペインで、**［デリバリーグループ］**を選択します。
2. グループを選択し、アクションバーの**機能レベルの変更**をクリックします。**機能レベルの変更**アクションは、アップグレードされたVDAが検出された場合にのみ表示されます。
3. **変更**をクリックします。

ディスプレイには、機能レベルに変更できないマシンがある場合、そのマシンと理由が表示されます。その後、変更アクションをキャンセルし、マシンの問題を解決してから、変更アクションを再度実行できます。

変更が完了したら、マシンを以前の状態に戻すことができます。デリバリーグループを選択し、アクションバーで を選択します。

Remote PC Accessデリバリーグループの管理

Remote PC Accessマシンカタログ内のマシンが割り当てられていない場合、そのマシンは一時的にそのカタログに関連付けられたデリバリーグループに割り当てられます。この一時的な割り当てにより、後でマシンをユーザーに割り当てることができます。

デリバリーグループとマシンカタログの関連付けには優先度値があります。優先度は、マシンがシステムに登録されるとき、またはユーザーがマシンの割り当てを必要とするときに、マシンの割り当て済みデリバリーグループを決定します。値が小さいほど優先度が高くなります。Remote PC Access マシンカタログに複数のデリバリーグループ割り当てがある場合、ソフトウェアは最も優先度の高い一致を選択します。この優先度値を設定するには、PowerShell SDK を使用します。

リモートPCアクセス マシンカタログは、最初に作成された際にデリバリーグループと関連付けられます。後からカタログに追加されたマシンアカウントや組織単位も、そのデリバリーグループに追加できます。この関連付けは、有効/無効を切り替えることができます。

Remote PC Accessマシンカタログとデリバリーグループの関連付けを追加または削除するには：

1. 左側のペインで を選択します。
2. Remote PC Access グループを選択します。

3. セクションで、 タブをクリックし、Remote PC Access カタログを選択します。
4. 関連付けを追加または復元するには、 をクリックします。関連付けを削除するには、 をクリックします。

フォルダーを使用したデリバリーグループの整理

デリバリーグループに簡単にアクセスできるように、フォルダーを作成できます。

> **ヒント:**
>
> アクションバーの右上にある アイコンをクリックすると、デリバリーグループノードの優先するデフォルトビュー（フォルダービューまたはリストビュー）を設定できます。

必要な役割

デフォルトでは、デリバリーグループフォルダーを作成および管理するには、Cloud Administrator、Full Administrator、またはDelivery Group Administratorの組み込み役割が必要です。必要に応じて、デリバリーグループフォルダーの作成と管理のための役割をカスタマイズできます。詳しくは、「必要な権限」を参照してください。

デリバリーグループフォルダーを作成する

開始する前に、デリバリーグループの整理方法を計画してください。次の点を考慮してください。

- フォルダーは最大5レベルまでネストできます（デフォルトのルートフォルダーを除く）。
- フォルダーには、デリバリーグループとサブフォルダーを含めることができます。
- Web Studio のすべてのノード（**マシンカタログ**、**デリバリーグループ**、**アプリケーション**、**アプリケーショングループ**など）は、バックエンドで同じフォルダーツリーを共有します。フォルダーの名前変更や移動の際に名前の競合を避けるため、異なるノード間で最上位フォルダーには一意の名前を使用してください。

  `New-BrokerAdminFolder` SDK コマンドレットを使用してフォルダーを作成し、それを **デリバリーグループ** ノードの下に表示させたい場合は、`Set-BrokerAdminFolderMetadata` コマンドレットを使用して `ContainsDeliveryGroups` メタデータを追加する必要があります。

  例:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsDeliveryGroups -Value true
  ```

デリバリーグループフォルダーを作成するには、次の手順に従います。

1. 左ペインで **デリバリーグループ** を選択します。
2. フォルダー階層でフォルダーを選択し、**アクション** バーで **フォルダーの作成** を選択します。
3. 新しいフォルダーの名前を入力し、**完了** をクリックします。

> **ヒント:**
>
> 意図しない場所にフォルダーを作成してしまった場合は、正しい場所にドラッグできます。

デリバリーグループを移動する

デリバリーグループはフォルダー間で移動できます。詳細な手順は次のとおりです。

1. 左ペインで **デリバリーグループ** を選択します。
2. フォルダー別にグループを表示します。フォルダー階層の上にある「**すべて表示**」をオンにすると、すべてのグループを一度に表示することもできます。
3. グループを右クリックし、「**デリバリーグループの移動**」を選択します。
4. グループを移動するフォルダーを選択し、「**完了**」をクリックします。

> **ヒント:**
>
> グループをフォルダーにドラッグできます。

デリバリーグループフォルダーの管理

デリバリーグループフォルダーを削除、名前変更、移動できます。

フォルダーとそのサブフォルダーにデリバリーグループが含まれていない場合にのみ、フォルダーを削除できることに注意してください。

フォルダーを管理するには、次の手順に従います。

1. 左ペインで「**デリバリーグループ**」を選択します。
2. フォルダー階層でフォルダーを選択し、必要に応じて「**アクション**」バーでアクションを選択します。
    - フォルダーの名前を変更するには、「**フォルダー名の変更**」を選択します。

- フォルダーを削除するには、「**フォルダーの削除**」を選択します。
- フォルダーを移動するには、「**フォルダーの移動**」を選択します。

3. 画面の指示に従って、残りの手順を完了してください。

必要な権限

次の表に、デリバリーグループフォルダーに対してアクションを実行するために必要な権限を示します。

アクション	必要な権限
デリバリーグループフォルダーを作成する	デリバリーグループフォルダーの作成
デリバリーグループフォルダーを削除する	デリバリーグループフォルダーの削除
デリバリーグループフォルダーを移動する	デリバリーグループフォルダーの移動
デリバリーグループフォルダーの名前を変更する	デリバリーグループフォルダーの編集
デリバリーグループをフォルダーに移動する	デリバリーグループフォルダーの編集とデリバリーグループプロパティの編集

アプリ保護の管理

以下の情報はApp protectionの補足です。以下の詳細に注意してください。

- 有効なアプリ保護の資格が必要です。アプリ保護機能を購入するには、Citrix の営業担当者にお問い合わせください。
- App ProtectionにはXML信頼が必要です。XML信頼を有効にするには、**設定 > XML信頼を有効にする**に移動します。
- 画面キャプチャ防止について：
  - Windows および macOS では、保護されたコンテンツのウィンドウのみが空白になります。保護されたウィンドウが最小化されていない場合、アプリ保護はアクティブになります。
  - Linux では、キャプチャ全体が空白になります。保護されたウィンドウが最小化されているかどうかにかかわらず、アプリ保護はアクティブになります。

デリバリーグループのアプリ保護方法を選択するには、次の手順に従います。

1. 左ペインで**デリバリーグループ**を選択します。

2. グループを選択し、アクションバーで**編集**を選択します。
3. **App Protection**ページには、次のオプションが表示されます。

オプション	説明
適用しない	設定を適用しない場合は、このオプションを選択します。
このデリバリーグループに適用する	「**アンチキーロギング**」および/または「**アンチキーキャプチャリング**」オプションを選択します。これらの設定のそれぞれにカーソルを合わせると、ツールチップに詳細が表示されます。
コンテキストに応じて適用	この設定を適用するには、「**アクセスポリシー設定**」ページでアクセスポリシーを構成します。
	1. 左ペインで「**アクセスポリシー**」をクリックし、「**追加**」をクリックします。
	1. 「**ポリシーの追加**」ページで、以下を実行します。
	- i. 「**ポリシー名**」を入力し、必要に応じて設定を構成します。
	- ii. 「**フィルター**」および「**値**」フィールドに詳細を入力し、「**完了**」をクリックします。新しいポリシーは「**アプリ保護**」ページに表示されます。このポリシーに必要な設定を有効にします。
	- iii. 「**保存**」をクリックします。

4. 「**デリバリーグループ**」ページで、**デリバリーグループ**を選択し、下部にある「**詳細**」タブをクリックします。適用された新しい**アプリ保護**設定が表示されます。

ユーザー

このセクションでは、次のトピックについて説明します。

- ユーザー設定の変更

- ユーザーの追加または削除
- ユーザー割り当ての管理

デリバリーグループのユーザー設定を変更する

このページの名前は、 または のいずれかで表示されます。

1. 左側のペインで を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. (または) ページで、次の表の設定を変更します。
4. をクリックすると、行った変更が適用され、ウィンドウが開いたままになります。または、 をクリックすると、変更が適用され、ウィンドウが閉じます。

設定	説明
説明	Citrix Workspace (またはStoreFront) が使用し、ユーザーに表示されるテキスト。
デリバリーグループを有効にする	デリバリーグループが有効になっているかどうか。
タイムゾーン	このデリバリーグループのマシンが存在する必要があるタイムゾーン。このオプションには、サイトでサポートされているタイムゾーンが一覧表示されます。**注：**デリバリーグループのタイムゾーンを変更すると、そのデリバリーグループ内のマシンが再起動する可能性があります。これを回避するには、稼働時間外にタイムゾーン設定を変更してください。
Secure ICA®を有効にする	ICAプロトコルを暗号化するSecureICAを使用して、デリバリーグループ内のマシンとの間の通信を保護します。デフォルトのレベルは128ビットです。このレベルはSDKを使用して変更できます。Citrixは、パブリックネットワークを介して通信する場合、TLS暗号化などのより多くの暗号化方法を使用することを推奨します。また、SecureICAはデータ整合性をチェックしません。

デリバリーグループでのユーザーの追加または削除

ユーザーに関する詳細については、「ユーザー」を参照してください。

1. 左側のペインで**［デリバリーグループ］**を選択します。
2. グループを選択し、アクションバーで**［編集］**をクリックします。
3. **［ユーザー］**ページで：
   - ユーザーを追加するには、**［追加］**をクリックし、追加するユーザーを指定します。
   - ユーザーを削除するには、1人以上のユーザーを選択し、**［削除］**をクリックします。
   - 認証されていないユーザーによるアクセスを許可するには、チェックボックスをオンまたはオフにします。
4. 加えた変更を適用してウィンドウを開いたままにするには、**［適用］をクリックします。または、変更を適用してウィンドウを閉じるには、**［保存］**をクリックします。

ユーザーリストのインポートまたはエクスポート

物理的なシングルセッションOSマシンを含むデリバリーグループの場合、デリバリーグループの作成後に.csvファイルからユーザー情報をインポートできます。ユーザー情報を.csvファイルにエクスポートすることもできます。.csvファイルには、以前の製品バージョンのデータを含めることができます。

CSVファイルの最初の行には、コンマで区切られた2つの列ヘッダーが含まれている必要があります。最初のヘッダーが`Machine Account`で、2番目のヘッダーが`User Names`であることを確認してください。（追加のヘッダーを含めることはできますが、サポートされていません。）ファイルの以降の行には、コンマで区切られたデータが含まれます。`Machine Account`エントリは、コンピューターSID、FQDN、またはドメインとコンピューター名のペアにすることができます。

ユーザー情報をインポートまたはエクスポートするには：

1. 左ペインで を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. ページで、 または を選択し、ファイルの場所を参照します。
4. 加えた変更を適用してウィンドウを開いたままにするには、 をクリックします。または、変更を適用してウィンドウを閉じるには、 をクリックします。

ユーザー割り当ての管理

デリバリーグループ内のマシンに対するユーザー割り当てを管理します。デスクトップ割り当てルールがデリバリーグループに構成されている場合、マシンは最初のデスクトップ起動時にユーザーにランダムに割り当てられ、ユーザー割り当てが変更されない限り、ユーザーに割り当てられたままになります。割り当てられていないマシンを特定のユーザーに手動で割り当てる場合、またはマシンの既存のユーザー割り当てを変更する場合は、このトピックで説明されている手順に従って変更を行います。これらの手順を使用すると、ユーザーに割り当てられたマシンのCitrix Workspaceアプリに表示される名前を変更することもできます。

詳細な手順は次のとおりです。

1. コンソールで、左ペインから を選択します。
2. グループを選択し、アクションバーで を選択します。
3. 左ペインで を選択します。グループ内の各マシンの以下の詳細が表示されます。
    - **Machine name:** マシンの名前を表示します。
    - **Display name:** Citrix Workspaceアプリに表示されるマシンの表示名を表示します。
    - **ユーザー：** このマシンに割り当てられているユーザーを表示します。デスクトップ割り当てルールが構成されている場合、マシンは最初のデスクトップ起動時にユーザーにランダムに割り当てられ、ユーザー割り当てが変更されない限り、そのユーザーに割り当てられたままになります。
4. マシンを見つけ、ユーザーを割り当てるか、そのユーザー割り当てを変更します。
    - 「**参照**」をクリックしてユーザーを参照します。
    - 「**ユーザー**」列に、セミコロンで区切られたユーザー名のリストを入力します。
    - 「**CSVファイルからインポート**」をクリックして、CSVファイルを使用して設定の詳細をインポートします。
5. （オプション）マシンがユーザーに割り当てられている場合は、必要に応じて表示名を変更します。

> **注:**
>
> 表示名フィールドは、マシンがユーザーに割り当てられている場合にのみ有効になります。

- デスクトップ割り当てルールに基づいてマシンがユーザーに割り当てられている場合、このフィールドにはそのルールで構成された表示名が表示されます。
- マシンがユーザーに手動で割り当てられており、フィールドが空白のままの場合、デリバリーグループの公開名（指定されている場合）がマシンの表示名として使用されます。公開名が指定されていない場合は、デリバリーグループの名前が使用されます。デリバリーグループの公開名はPowerShellを介してのみ指定できることに注意してください。

6. 「**適用**」を選択して変更を適用し、ウィンドウを開いたままにします。または、「**OK**」を選択して変更を適用し、ウィンドウを閉じます。

マシン

- マシンからユーザーへの割り当てを変更する
- 電源管理されたシングルセッションのプールされたVDAでローカルホストキャッシュを有効にする
- ユーザーあたりの最大マシン数を変更する
- マシンを更新する
- デスクトップのタグ制限を追加、変更、または削除する
- マシンを削除する
- マシンへのアクセスを制限する
- ユーザーがマシンに接続するのを防ぐ（メンテナンスモード）
- マシンをシャットダウンして再起動する
- マシンの再起動スケジュールを作成および管理する
- 1回限りの再起動スケジュールを有効にする
- 管理対象マシンの電源を管理する

デリバリーグループ内のマシンからユーザーへの割り当てを変更する

MCSでプロビジョニングされたシングルセッションOSマシンの割り当てを変更できます。マルチセッションOSマシンまたはCitrix Provisioningでプロビジョニングされたマシンの割り当ては変更できません。

1. 左側のペインで「**デリバリーグループ**」を選択します。
2. グループを選択し、アクションバーで をクリックします。

3. または ページ（ページタイトルはデリバリーグループが使用するマシンカタログの種類によって異なります）で、新しいユーザーを指定します。
4. をクリックして変更を適用し、ウィンドウを開いたままにします。または、 をクリックして変更を適用し、ウィンドウを閉じます。

電源管理されたシングルセッションのプールされたVDAのローカルホストキャッシュを有効にする

デフォルトでは、電源管理されたシングルセッションのプールされたマシンは、ローカルホストキャッシュモードでは利用できません。このデフォルトの動作は、デリバリーグループごとに上書きできます。詳細な手順は次のとおりです。

1. Studioで、左ペインの**デリバリーグループ**を選択します。

   グループリストでは、MCSまたはCitrix Provisioningによってプロビジョニングされたシングルセッションのプールされたマシンを含むグループに警告アイコンが表示されます。
2. 必要に応じてグループを選択し、アクションバーの**編集**を選択します。
3. **ローカルホストキャッシュ**ページで、**リソースを利用可能にする**を選択します。
4. 加えた変更を適用してウィンドウを開いたままにするには、**適用**を選択します。または、変更を適用してウィンドウを閉じるには、**OK**を選択します。

または、PowerShellコマンドを使用してデフォルトの動作を上書きすることもできます。詳細については、「アプリケーションとデスクトップのサポート」を参照してください。

> **重要：**
>
> 電源管理されたシングルセッションのプールされたマシンへのアクセスを有効にすると、以前のユーザーセッションからのデータと変更が後続のセッションに存在する可能性があります。

デリバリーグループ内のユーザーあたりの最大マシン数を変更する

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーの**編集**をクリックします。
3. **デスクトップ割り当てルール**ページで、ユーザーあたりの最大デスクトップ数を設定します。
4. 加えた変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

デリバリーグループ内のマシンを更新する

1. 左ペインで を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. マシンを選択し、アクションバーで をクリックします。

別のイメージを選択するには、 を選択し、スナップショットを選択します。

変更を適用してマシンユーザーに通知するには、 を選択します。次に、以下を指定します。

- マスターイメージを更新するタイミング: 今すぐ、または次回の再起動時
- 再起動の配布時間（グループ内のすべてのマシンの更新を開始するまでの合計時間）
- ユーザーに再起動が通知されるかどうか
- ユーザーが受信するメッセージ

デスクトップのタグ制限を追加、変更、または削除する

タグ制限の追加、変更、削除は、起動対象となるデスクトップに予期せぬ影響を与える可能性があります。タグ の考慮事項と注意事項を確認してください。

1. 左ペインで を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. ページで、デスクトップを選択し、 をクリックします。
4. タグ制限を追加するには、**タグを持つマシンへの起動を制限**を選択し、タグを選択します。
5. タグ制限を変更または削除するには、次のいずれかを実行します。
    - 別のタグを選択します。
    - **このタグを持つマシンへの起動を制限する**のチェックを外して、タグ制限を削除します。
6. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

デリバリーグループからマシンを削除する

マシンを削除すると、デリバリーグループから削除されます。デリバリーグループが使用するマシンカタログからは削除されません。したがって、そのマシンは別のデリバリーグループに割り当てることができます。

マシンは、削除する前にシャットダウンする必要があります。削除中にユーザーがマシンに接続するのを一時的に停止するには、シャットダウンする前にマシンをメンテナンスモードにします。

マシンには個人データが含まれている可能性があるため、別のユーザーにマシンを割り当てる前に注意してください。マシンの再イメージングを検討してください。

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**マシンの表示**をクリックします。
3. マシンがシャットダウンされていることを確認します。
4. マシンを選択し、アクションバーで**デリバリーグループから削除**をクリックします。

マシンが使用する接続を介して、デリバリーグループからマシンを削除することもできます。

デリバリーグループ内のマシンへのアクセスを制限する

デリバリーグループ内のリソースへのアクセスを制限するために行った変更は、使用する方法に関係なく、以前の設定を上書きします。次のことができます。

- **委任管理スコープを使用して管理者へのアクセスを制限する:** 管理者がすべてのアプリケーションにアクセスできるスコープと、特定のアプリケーションのみにアクセスできるスコープを作成して割り当てることができます。詳細については、「委任管理」を参照してください。
- **スマートアクセス ポリシー式を使用してユーザーのアクセスを制限する:** アクセス ポリシー規則を構成して、特定のデリバリーグループへのユーザーアクセスを制御できます。例を次に示します。
    - ユーザーのサブセットへのアクセスを制限し、許可されたユーザーデバイスを指定します。
    - Workspace (StoreFront ではなく) を介して接続しているユーザーへのアクセスを制限します。
    - 特定の Workspace URL を介して接続しているユーザーへのアクセスを制限します。

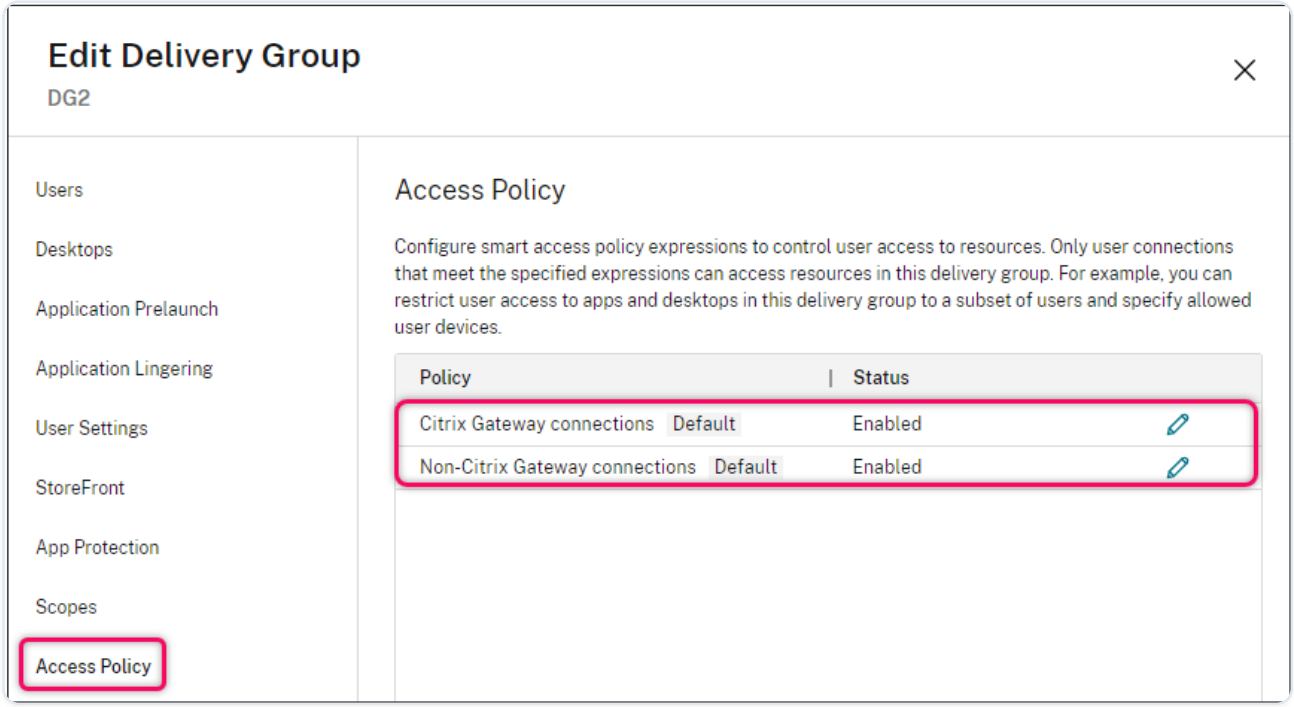
このセクションでは、アクセス ポリシー規則を使用してデリバリーグループへのユーザーアクセスを制限する方法について説明します。

- アクセス ポリシー規則について
- アクセス ポリシー規則の追加
- Web Studio を使用したアクセス ポリシー規則の管理
- PowerShell を使用したポリシー規則の追加と調整

アクセス ポリシー規則について

デリバリーグループに対して複数のアクセス ポリシー規則を構成できます。デリバリーグループ内のアプリとデスクトップは、ユーザーの接続がデリバリーグループに対して定義したアクセスポリシー規則のいずれかに一致する場合に、順序に関係なく、ユーザーの StoreFront または Workspace に表示されます。

各規則は個別に有効または無効にできます。無効な規則は、アクセス ポリシーが評価されるときに無視されます。



Web Studioでは、Access Policyリストには以下のデフォルトのSmartAccessポリシー規則が含まれています。必要に応じて追加できます。

- **Citrix Gateway 接続。** このポリシーでは、Citrix Gateway 経由で行われたユーザー接続のみがデリバリーグループ内のリソースにアクセスできます。デバイスポスチャまたはネットワークロケーション機能が有効になっている場合に Workspace 経由で行われたユーザー接続も、Citrix Gateway 経由の接続と見なされます。
- **Citrix Gateway以外の接続。** このポリシーでは、Citrix Gateway を介さずに行われたユーザー接続のみがデリバリーグループ内のリソースにアクセスできます。

> **注:**

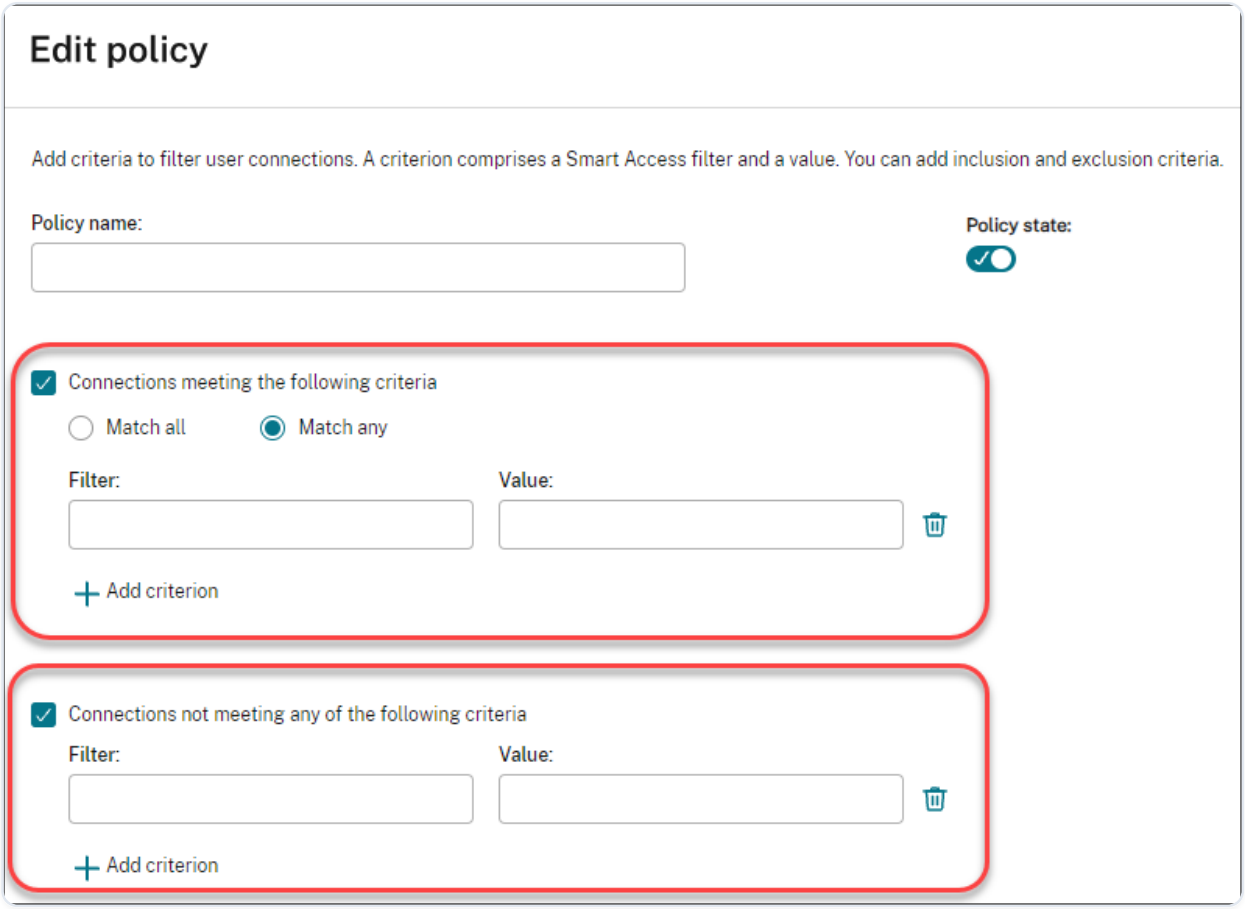
- デフォルトの規則が新しく構成された規則を上書きしないようにするには、デフォルトの規則を無効にするか、新しいポリシーで使用されているフィルターを除外するように調整する必要があります。
- デフォルトのポリシーは削除できませんが、無効にすることはできます。ポリシーを無効にするには、**編集**アイコンをクリックし、**ポリシーの状態**を**無効**に変更します。
- ポリシーリストには、PowerShellコマンドを使用して追加された規則も表示されます。これらのポリシーは削除できますが、Web Studioで編集することはできません。

Web Studioを使用してアクセスポリシー規則を追加する

アクセスポリシー規則は、一連のフィルターで構成されます。フィルターについて詳しくは、この記事を参照してください。アクセスポリシー規則を追加するときは、必要に応じて複数の条件フィルターを規則に追加します。

Web Studio を使用してデリバリーグループのポリシーを追加するには、次の手順に従います。

1. コンソールの左ペインで、**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーの**編集**をクリックします。
3. **Access Policy**ページで、**追加**をクリックします。**Add Policy**ページが表示されます。



4. **ポリシー名**フィールドに、ポリシーのわかりやすい名前を入力します。名前は展開内で一意である必要があります。
5. 許可されるユーザー接続の基準を定義するには、次の手順に従います。
    a. **次の条件を満たす接続**を選択します。
    b. **基準の追加**をクリックします。
    c. **フィルター**フィールドに、使用するフィルターの名前を入力します。**値**フィールドに、フィルターの目的の値を入力します。たとえば、Workspace (StoreFront ではなく) を介して接続されたユーザーのみがこのデリバリーグループのリソースにアクセスできるようにするには、**フィルター**に `Citrix-Via-Workspace`、**値**に `True` と入力します。
    d. さらに基準を追加するには、手順 b～c を繰り返します。
    e. 基準間の関係を選択します。
        - **いずれかに一致**。受信ユーザー接続が構成されたフィルター基準のいずれかを満たす場合にのみアクセスを許可します。
        - **すべてに一致**。受信ユーザー接続が構成されたフィルター基準のすべてを満たす場合にのみアクセスを許可します。
6. 禁止されているユーザー接続の条件を定義するには、次の手順に従います:
    a. **次の条件のいずれも満たさない接続**を選択します。
    b. **基準の追加**をクリックします。
    c. **フィルター**フィールドに、使用するフィルターの名前を入力します。**値**フィールドに、フィルターの目的の値を入力します。たとえば、`example.cloud.com` Workspace URL を介して接続されたユーザーがこのデリバリーグループのリソースにアクセスすることを禁止するには、**フィルター**に `Citrix.Workspace.UsingDomain`、**値**に `example.cloud.com` と入力します。
    d. さらに基準を追加するには、手順 b～c を繰り返します。

    > **注:**
    >
    > 構成された基準のいずれかを満たすユーザー接続は、このデリバリーグループのリソースへのアクセスが禁止されます。

7. **完了**をクリックします。

新しいポリシーがポリシーリストに表示されます。

8. この新しいポリシーでカバーされる接続との意図しない重複を避けるために、デフォルトのポリシー規則を確認し、調整してください。既存のポリシーを調整するには、次の方法を使用します。

   - デフォルトのポリシー規則を無効にします。
   - 新しいポリシーの包含条件に追加した SmartAccess フィルターを除外するように、デフォルトのポリシー規則を構成します。詳しくは、「Web Studio を使用してポリシー規則を管理する」および「PowerShell を使用してアクセスポリシー規則を追加および管理する」を参照してください。

> **重要:**
>
> アクセスポリシー規則についてで説明されているように、ユーザーの接続がデリバリーグループ内の1つ以上のポリシー規則に一致する場合、ユーザーはそのリソースにアクセスできます。したがって、規則を作成した後、新しい規則でカバーされる接続との意図しない重複を避けるために、既存の規則を慎重に確認し、調整する必要があります。

Web Studio を使用してアクセスポリシー規則を管理する

包含条件と除外条件を使用して、デフォルトのポリシーを調整できます。たとえば、それらの接続の一部へのアクセスを制限するには、次の手順に従います。

1. デフォルトのポリシーを編集します。
2. **次のいずれかの条件を満たす接続**を選択します。
3. 許可されたユーザーアクセスシナリオのSmartAccessポリシー式を追加、編集、または削除します。

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

PowerShellを使用したアクセスポリシー規則の追加と管理

デリバリーグループのアクセスポリシー規則を追加および管理するには、次のPowerShellコマンドレットを使用できます。

- New-BrokerAccessPolicyRule
- Get-BrokerAccessPolicyRule
- Set-BrokerAccessPolicyRule
- リネーム-ブローカーアクセス-ポリシー-ルール

- Remove-BrokerAccessPolicyRule

詳細については、Citrix開発者向けドキュメントの関連記事を参照してください。

デリバリーグループ内のマシンへのユーザー接続を防止する（メンテナンスモード）

マシンへの新しい接続を一時的に停止する必要がある場合は、デリバリーグループ内の1台またはすべてのマシンでメンテナンスモードをオンにできます。これは、パッチを適用したり、管理ツールを使用したりする前に行うことがあります。

- マルチセッションOSマシンがメンテナンスモードの場合、ユーザーは既存のセッションに接続できますが、新しいセッションを開始することはできません。
- シングルセッションOSマシン（またはリモートPCアクセスを使用するPC）がメンテナンスモードの場合、ユーザーは接続または再接続できません。現在の接続は、切断またはログオフするまで接続されたままになります。

メンテナンスモードをオンまたはオフにするには：

1. 左ペインで****を選択します。
2. グループを選択します。
3. デリバリーグループ内のすべてのマシンでメンテナンスモードをオンにするには、アクションバーの****をクリックします。

   1台のマシンでメンテナンスモードをオンにするには、アクションバーで**マシンを表示**をクリックします。マシンを選択し、アクションバーで**メンテナンスモードをオンにする**をクリックします。
4. デリバリーグループ内の1台またはすべてのマシンのメンテナンスモードをオフにするには、上記の手順に従い、アクションバーの****をクリックします。

Windows リモートデスクトップ接続 (RDC) の設定も、マルチセッションOSマシンがメンテナンスモードであるかどうかに影響します。以下のいずれかの状況でメンテナンスモードがオンになります。

- 前述のとおり、メンテナンスモードがオンに設定されている。
- RDCが****に設定されている。
- RDCが****に設定されていない。の設定がまたは**のいずれかである。

以下の項目についても、メンテナンスモードをオンまたはオフにできます。

- 接続。その接続を使用しているマシンに影響します。
- マシンカタログ。そのカタログ内のマシンに影響します。

デリバリーグループ内のマシンをシャットダウンして再起動する

この手順は、Remote PC Access マシンではサポートされていません。

1. 左ペインで****を選択します。
2. グループを選択し、アクションバーの****をクリックします。
3. マシンを選択し、アクションバーで以下のいずれかのエントリをクリックします。

    - : マシンの電源を強制的にオフにし、マシンの一覧を更新します。
    - : オペレーティングシステムにシャットダウンと再起動を要求します。オペレーティングシステムがこれに応じられない場合、マシンは現在の状態のままになります。
    - **強制再起動:** オペレーティングシステムを強制的にシャットダウンし、マシンを再起動します。
    - **サスペンド:** マシンをシャットダウンせずに一時停止し、マシンリストを更新します。
    - **シャットダウン:** オペレーティングシステムにシャットダウンを要求します。

強制ではないアクションの場合、マシンが10分以内にシャットダウンしないと、電源がオフになります。シャットダウン中にWindowsが更新プログラムのインストールを試みると、更新が完了する前にマシンの電源がオフになるリスクがあります。

Citrixでは、シングルセッションOSマシンのユーザーがセッション内で**シャットダウン**を選択できないようにすることをお勧めします。詳細については、Microsoftのポリシーに関するドキュメントを参照してください。

接続でマシンをシャットダウンしたり再起動したりすることもできます。

デリバリーグループ内のマシンの再起動スケジュールを作成および管理する

> **注:**

> - Autoscale™が有効なデリバリーグループに再起動スケジュールが適用されると、そのマシンは電源がオフになり、Autoscaleが電源をオンにするまでそのままになります。
> - 再起動スケジュールがランダムなシングルセッションマシンに適用される場合、コストを節約するために、それらのマシンは再起動されるのではなく電源がオフになります。マシンの電源をオンにするには、Autoscaleを使用することをお勧めします。

- デリバリーグループのタイムゾーンを変更すると、そのデリバリーグループ内のマシンが再起動される可能性があります。これを回避するには、稼働時間外にタイムゾーン設定を変更してください。

再起動スケジュールは、デリバリーグループ内のマシンが定期的に再起動されるタイミングを指定します。デリバリーグループに対して1つ以上のスケジュールを作成できます。スケジュールは、次のいずれかに影響を与える可能性があります。

- グループ内のすべてのマシン。
- グループ内の1つまたは複数（ただしすべてではない）のマシン。マシンは、マシンに適用するタグによって識別されます。これはタグ制限と呼ばれます。タグがアクションをそのタグを持つアイテムのみに制限するためです。

たとえば、すべてのマシンが1つのデリバリーグループにあるとします。すべてのマシンを週に1回再起動し、経理チームが使用するマシンを毎日再起動したいとします。これを実現するには、すべてのマシンに対して1つのスケジュールを設定し、経理のマシンのみに対して別のスケジュールを設定します。

スケジュールには、再起動が開始される曜日と時刻、および期間が含まれます。

スケジュールを有効または無効にできます。スケジュールを無効にすることは、テスト中、特別な期間中、またはスケジュールが必要になる前に準備する際に役立ちます。

管理コンソールから自動電源オンまたはシャットダウンにスケジュールを使用することはできません。再起動のみに使用できます。

スケジュールの重複

複数のスケジュールが重複する可能性があります。上記の例では、両方のスケジュールが経理部門のマシンに影響を与えます。これらのマシンは日曜日に2回再起動される可能性があります。スケジューリングコードは、同じマシンが意図したよりも頻繁に再起動されるのを避けるように設計されていますが、保証することはできません。

- スケジュールが開始時刻と期間で正確に一致する場合、マシンが再起動されるのは1回だけである可能性が高くなります。
- スケジュールの開始時刻と期間が異なるほど、複数回の再起動が発生する可能性が高くなります。
- スケジュールによって影響を受けるマシンの数も、重複の可能性に影響します。この例では、すべてのマシンに影響する週次スケジュールは、経理部門のマシンに対する日次スケジュール

よりも早く再起動を開始する可能性があります。これは、それぞれに指定された期間によって異なります。

再起動スケジュールの詳細については、「再起動スケジュールの内部」を参照してください。

再起動スケジュールの表示

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **Restart Schedule**ページを選択します。

ページには、構成されている各スケジュールについて次の情報が表示されます。

- スケジュール名
- タグ制限（使用されている場合）
- マシンの再起動が実行される頻度
- マシンユーザーが通知を受け取るかどうか
- スケジュールが有効になっているかどうか

タグの追加（適用）

タグ制限を使用する再起動スケジュールを構成する場合は、スケジュールが影響するマシンにタグが追加されていることを確認してください。上記の例では、経理チームが使用する各マシンにタグが適用されています。詳細については、「タグ」を参照してください。

1台のマシンに複数のタグを適用できますが、再起動スケジュールで指定できるタグは1つだけです。

1. 左側のペインで を選択します。
2. スケジュールによって制御されるマシンが含まれるグループを選択します。
3. をクリックし、タグを追加するマシンを選択します。
4. アクションバーで をクリックします。
5. タグが存在する場合は、タグ名の横にあるチェックボックスをオンにします。タグが存在しない場合は、 をクリックし、タグの名前を指定します。タグが作成されたら、新しく作成されたタグ名の横にあるチェックボックスをオンにします。
6. 「**タグの管理**」ダイアログで「**保存**」をクリックします。

再起動スケジュールの作成

注:

再起動スケジュールは、電源管理されているすべてのマルチセッションマシンと、電源管理されていないマルチセッションマシンに適用できます。

1. 左側のペインで「**デリバリーグループ**」を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. 「**再起動スケジュール**」ページで、「**追加**」をクリックします。
4. 「**再起動スケジュールの追加**」ページで、次のようにします。
   - スケジュールを有効にするには、「**はい**」を選択します。スケジュールを無効にするには、「**いいえ**」を選択します。
   - スケジュール名と説明を入力します。
   - では、タグの制限を適用します。
   - では、メンテナンスモードのマシンをこのスケジュールに含めるかどうかを選択します。代わりにPowerShellを使用するには、「メンテナンスモードのマシンのスケジュールされた再起動」を参照してください。
   - では、再起動が実行される頻度（毎日、毎週、毎月、または1回）を選択します。 または を選択した場合は、1つ以上の特定の日を指定できます。
   - では、スケジュールを実行する頻度を指定します。
   - では、スケジュールの初回実行の開始日を指定します。
   - では、24時間形式で再起動を開始する時刻を指定します。
   - について:
     - 自然な再起動を使用しない場合は、 または を選択します。
     - 自然な再起動を使用する場合は、**すべてのセッションをドレインした後にすべてのマシンを再起動**を選択します。

       自然な再起動を使用するように構成された再起動スケジュールを開始すると、次のようになります。

       - デリバリーグループに属するすべてのアイドル状態のマシンはすぐに再起動されます
       - 1つ以上の現在アクティブなセッションを持つデリバリーグループに属する各マシンは、すべてのセッションがログオフされたときに再起動されます。

> **注:**
>
> 自然な再起動スケジュールは、電源管理されたマシンのみを再起動できます。

- **ユーザーに通知を送信**で、再起動が始まる前に該当するマシンに通知メッセージを表示するかどうかを選択します。デフォルトでは、メッセージは表示されません。
- 再起動が始まる15分前にメッセージを表示することを選択した場合、最初のメッセージの後に5分ごとにメッセージを繰り返すように（**通知頻度**で）選択できます。デフォルトでは、メッセージは繰り返されません。
- 通知のタイトルとテキストを入力します。デフォルトのテキストはありません。

  メッセージに再起動までのカウントダウンを含める場合は、変数**%m%**を含めます。すべてのマシンを同時に再起動することを選択しない限り、メッセージは再起動前の適切なタイミングで各マシンに表示されます。

5. **完了**をクリックして変更を適用し、**再起動スケジュールの追加**ウィンドウを閉じます。
6. **適用**をクリックして変更を適用し、ウィンドウを開いたままにします。または、**保存**をクリックして変更を適用し、ウィンドウを閉じます。

ドレイン後の再起動

PowerShellを使用してマシン再起動スケジュールを作成または更新する場合（`New-BrokerRebootSchedulev2`または`Set-BrokerRebootSchedulev2`）、別の再起動期間値が利用可能です。

`-UseNaturalReboot <Boolean>`パラメーターでドレイン後の再起動機能を有効にすると、すべてのセッションをドレインした後にすべてのマシンが再起動されます。再起動時刻になると、マシンはドレイン状態になり、すべてのセッションがログオフされた後に再起動されます。

この機能は、シングルセッションまたはマルチセッションマシンを含むデリバリーグループでサポートされています。このオプションは、電源管理されているマシンと電源管理されていないマシンの両方で使用できます。

オンプレミス環境では、この機能は PowerShell を使用する場合にのみサポートされます。この機能は Web Studio では利用できません。

再起動スケジュールの編集、削除、有効化、または無効化

1. 左側のペインで を選択します。

2. グループを選択し、アクションバーで をクリックします。
3. 「**再起動スケジュール**」ページで、スケジュールのチェックボックスを選択します。
    - スケジュールを編集するには、 をクリックします。再起動スケジュールの作成 のガイダンスに従って、スケジュール構成を更新します。
    - スケジュールを有効または無効にするには、**編集**をクリックします。**再起動スケジュールを有効にする**チェックボックスをオンまたはオフにします。
    - スケジュールを削除するには、**削除**をクリックします。削除を確認します。スケジュールを削除しても、影響を受けるマシン内のマシンに適用されているタグには影響しません。

データベースの停止により遅延したスケジュールされた再起動

> **注:**
>
> この機能はPowerShellでのみ利用可能です。

> デリバリーグループ内のマシン（VDA）のスケジュールされた再起動が開始される前にサイトデータベースの停止が発生した場合、停止が終了したときに再起動が開始されます。これは意図しない結果を招く可能性があります。

たとえば、デリバリーグループの再起動を非稼働時間中（03:00開始）に発生するようにスケジュールしたとします。スケジュールされた再起動が開始される1時間前（02:00）にサイトデータベースの停止が発生しました。停止は6時間（08:00まで）続きました。再起動スケジュールは、Delivery Controllerとサイトデータベース間の接続が復元されたときに開始されます。VDAの再起動は元のスケジュールから5時間後に開始され、結果としてVDAが稼働時間中に再起動することになります。

この状況を回避するために、`New-BrokerRebootScheduleV2`および`Set-BrokerRebootScheduleV2`コマンドレットで`MaxOvertimeStartMins`パラメーターを使用できます。この値は、再起動スケジュールが開始できる、スケジュールされた開始時刻を超える最大分数を示します。

- データベース接続がその時間内（スケジュールされた時間 + `MaxOvertimeStartMins`）に復元された場合、VDAの再起動が開始されます。
- データベース接続がその時間内に復元されない場合、VDAの再起動は開始されません。
- このパラメーターが省略されているか、値がゼロの場合、データベースへの接続が復元されると、停止期間に関係なく、スケジュールされた再起動が開始されます。

詳細については、cmdletのヘルプを参照してください。この機能はPowerShellでのみ利用可能です。Web Studioで再起動スケジュールを設定する際には、この値を設定できません。

メンテナンスモードのマシンに対するスケジュールされた再起動

> **注:**
>
> この機能は PowerShell でのみ利用できます。オプション `IgnoreMaintenanceMode` は、Citrix Virtual Apps and Desktops 7 2006 以降でサポートされています。
>
> 再起動スケジュールがメンテナンスモードのマシンに影響するかどうかを示すには、`BrokerRebootScheduleV2` コマンドレットで `IgnoreMaintenanceMode` オプションを使用します。

たとえば、次のコマンドレットは、メンテナンスモードのマシン（メンテナンスモードではないマシンに加えて）を再起動するスケジュールを作成します。

```
New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup> -IgnoreMaintenanceMode $true
```

次のコマンドレットは、既存の再起動スケジュールを変更します。

```
Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode $true
```

詳細については、コマンドレットのヘルプを参照してください。この機能はPowerShellでのみ利用可能です。

1回限りの再起動スケジュールを有効にする

PowerShellを使用して1回限りの再起動スケジュールを有効にするには、次の `BrokerCatalogRebootSchedule` PowerShellコマンドを使用して再起動スケジュールを作成、変更、削除します。

- Get-BrokerCatalogRebootSchedule
- New-BrokerCatalogRebootSchedule
- Set-BrokerCatalogRebootSchedule
- 削除-BrokerCatalogRebootSchedule
- 名前変更-BrokerCatalogRebootSchedule

制限事項:

- タイムゾーンが構成されていないカタログに関連付けられたカタログ再起動スケジュールは作成されますが、開始されません。
- カタログ再起動スケジュールが作成されると、その再起動スケジュールはデリバリーグループに属するカタログVMでのみ実行されます。

例、,

- **BankTellers** という名前のカタログ内のVMの再起動スケジュールを、Feb 3, 2022 の午前2時から午前4時の間に開始するように作成します。

```
C:\PS> New-BrokerCatalogRebootSchedule -Name BankTellers -CatalogName
BankTellers  -StartDate "2022-02-03" -StartTime "02:00" -Enabled $true
-RebootDuration 120
```

- UID 17のカタログ内のVMの再起動スケジュールを、Feb 3, 2022の午前1時から午前5時の間に開始するように作成します。再起動の10分前に、各VMはすべてのユーザーセッションで、タイトルが**WARNING: Reboot pending**、メッセージが**Save your work**というメッセージボックスを表示するように設定されます。

```
C:\PS> New-BrokerCatalogRebootSchedule -Name 'Update reboot'
-CatalogUid 17 -StartDate "2022-02-03" -StartTime "01:00" -Enabled
$true -RebootDuration 240 -WarningTitle "WARNING: Reboot pending"
-WarningMessage "Save your work" -WarningDuration 10
```

- **Old Name** という名前のカタログ再起動スケジュールを **New Name** に変更します。

```
C:\PS> Rename-BrokerCatalogRebootSchedule -Name "Old Name" -NewName
"New Name"
```

- UID 1のすべてのカタログ再起動スケジュールを表示し、その後、UID 1のカタログ再起動スケジュールを**New Name**に名前変更します。

```
C:\PS> Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
```

- **Accounting**という名前のカタログ再起動スケジュールを設定し、各VMの再起動の10分前に、タイトルが**WARNING: Reboot pending, and the message**、メッセージが**Save your work**と

いうメッセージを表示するようにします。このメッセージは、そのVM上のすべてのユーザーセッションに表示されます。

```
C:\PS> Set-BrokerCatalogRebootSchedule -Name Accounting -WarningMessage
"Save your work" -WarningDuration 10 -WarningTitle "WARNING: Reboot
pending"
```

- 無効になっているすべての再起動スケジュールを表示し、その後、無効になっているすべての再起動スケジュールを有効にします。

```
C:\PS> Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
BrokerCatalogRebootSchedule -Enabled $true
```

- カタログの再起動スケジュールをUID 17で設定し、各VMの再起動の15分前、10分前、5分前に「**%m%分後に再起動します**」というメッセージを表示するようにします。

```
C:\PS> Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Rebooting in
%m% minutes." -WarningDuration 15 -WarningRepeatInterval 5
```

- 「**MyCatalog**」という名前のカタログのタイムゾーンを構成します。

```
C:\PS> Set-BrokerCatalog -Name "MyCatalog" -TimeZone &lt;TimeZone>
```

デリバリーグループ内の電源管理対象マシン

電源管理できるのは、仮想シングルセッションOSマシンのみであり、物理マシン（リモートPCアクセス マシンを含む）はできません。GPU機能を備えたシングルセッションOSマシンは一時停止できないため、電源オフ操作は失敗します。マルチセッションOSマシンでは、再起動スケジュールを作成できます。

プールされたマシンを含むデリバリーグループでは、仮想シングルセッションOSマシンは次のいずれかの状態になります。

- ランダムに割り当てられ、使用中
- 未割り当てで未接続

静的マシンを含むデリバリーグループでは、仮想シングルセッションOSマシンは次のようになります。

- 永続的に割り当てられ、使用中
- 永続的に割り当てられ、未接続（ただし準備完了）
- 未割り当てで未接続

通常の使用時、静的デリバリーグループには通常、永続的に割り当てられたマシンと未割り当てのマシンの両方が含まれます。最初は、デリバリーグループ作成時に手動で割り当てられたマシンを除き、すべてのマシンが未割り当てです。ユーザーが接続すると、マシンは永続的に割り当てられます。これらのデリバリーグループ内の未割り当てマシンは完全に電源管理できますが、永続的に割り当てられたマシンは部分的にしか管理できません。

- **プールとバッファー:** プールされたデリバリーグループおよび未割り当てのマシンを持つ静的デリバリーグループの場合、プール（このインスタンスでは）とは、電源オン状態に保たれ、ユーザーが接続する準備ができている、未割り当てまたは一時的に割り当てられたマシンのセットです。ユーザーはログオン直後にマシンを取得します。プールサイズ（電源オン状態に保たれるマシンの数）は、時間帯によって構成可能です。静的デリバリーグループの場合、SDKを使用してプールを構成します。

  バッファーとは、プールのマシン数がしきい値を下回ったときに電源がオンになる、未割り当てマシンの追加のスタンバイセットです。しきい値はデリバリーグループサイズの割合です。大規模なデリバリーグループの場合、しきい値を超えるとかなりの数のマシンが電源オンになる可能性があります。そのため、デリバリーグループのサイズを慎重に計画するか、SDKを使用してデフォルトのバッファーサイズを調整してください。
- **電源状態タイマー:** 電源状態タイマーを使用して、ユーザーが指定された時間切断された後にマシンを一時停止できます。たとえば、ユーザーが10分以上切断されている場合、勤務時間外にマシンは自動的に一時停止します。

  平日と週末、およびピーク時と非ピーク時の間隔でタイマーを構成できます。
- **永続的に割り当てられたマシンの部分的な電源管理:** 永続的に割り当てられたマシンでは、電源状態タイマーを設定できますが、プールやバッファは設定できません。マシンは各ピーク期間の開始時にオンになり、各オフピーク期間の開始時にオフになります。消費されたマシンを補うために利用可能になるマシンの数について、割り当てられていないマシンで行うようなきめ細かな制御はできません。

仮想シングルセッションOSマシンの電源管理

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**デリバリーグループの編集**をクリックします。
3. **電源管理**ページで、**マシンの電源管理**で**平日**を選択します。デフォルトでは、平日は月曜日から金曜日です。

4. ランダムなデリバリーグループの場合、**電源をオンにするマシン**で**編集**をクリックし、平日のプールサイズを指定します。次に、電源をオンにするマシンの数を選択します。
5. **ピーク時間**で、各日のピーク時間とオフピーク時間を設定します。
6. 平日のピーク時間と非ピーク時間の電源状態タイマーを設定します。**ピーク時間中 > 切断時**で、デリバリーグループ内の切断されたマシンをサスペンドするまでの遅延（分単位）を指定し、**サスペンド**を選択します。**オフピーク時間中 > 切断時**で、デリバリーグループ内のログオフされたマシンをシャットダウンするまでの遅延を指定し、**シャットダウン**を選択します。このタイマーは、ランダムなマシンを含むデリバリーグループでは使用できません。
7. **マシンの電源管理**で**週末**を選択し、週末のピーク時間と電源状態タイマーを構成します。
8. **適用**をクリックして変更を適用し、ウィンドウを開いたままにします。または、**保存**をクリックして変更を適用し、ウィンドウを閉じます。

SDKを使用して、次の操作を行います。

- 電源状態タイマーに応じてマシンをサスペンドではなくシャットダウンするか、タイマーを接続解除ではなくログオフに基づいて設定する場合。
- デフォルトの平日と週末の定義を変更します。
- 電源管理を無効にします。CTX217289を参照してください。

切断されたセッションを持つVDIマシンが異なる時間帯に移行する際の電源管理

> **重要:**
>
> この機能強化は、切断されたセッションを持つVDIマシンにのみ適用されます。ログオフされたセッションを持つVDIマシンには適用されません。
>
> 以前のリリースでは、アクション（切断アクション="**Suspend**" または "**Shutdown**"）が必要な時間帯に移行するVDIマシンは、電源がオンのままでした。このシナリオは、アクション（切断アクション="**Nothing**"）が不要な時間帯（ピーク時またはオフピーク時）にマシンが切断された場合に発生しました。

Citrix Virtual Apps and Desktops 7 1909以降、指定された切断時間が経過すると、宛先時間帯に構成されている切断アクションに応じて、マシンは中断または電源オフされます。

たとえば、VDIデリバリーグループに対して次の電源ポリシーを構成します。

- `PeakDisconnectAction` を「何もしない」に設定します。

- `OffPeakDisconnectAction` を「シャットダウン」に設定します。
- `OffPeakDisconnectTimeout` を「10」に設定します。

電源ポリシーにおける切断アクションの詳細については、https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy および https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/ を参照してください。

以前のリリースでは、ピーク時にセッションが切断されたVDIマシンは、ピークからオフピークに移行しても電源がオンのままでした。Citrix Virtual Apps and Desktops 7 1909以降、期間移行時に `OffPeakDisconnectAction` および `OffPeakDisconnectTimeout` ポリシーアクションがVDIマシンに適用されます。その結果、マシンはオフピークに移行してから10分後に電源がオフになります。

以前の動作に戻したい場合（つまり、切断されたセッションを持つマシンがピークからオフピークへ、またはオフピークからピークへ移行しても何もアクションを実行しない場合）、次のいずれかを実行します:

- `LegacyPeakTransitionDisconnectedBehaviour` レジストリ値を `1` に設定します。これは、以前の動作を有効にする *true* と同等です。デフォルトでは、値は `0`、つまり *false* であり、期間移行時に切断電源ポリシーアクションをトリガーします。
  - パス: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer`
  - 名前: `LegacyPeakTransitionDisconnectedBehaviour`
  - 種類: `REG_DWORD`
  - データ: `0x00000001 (1)`
- `Set-BrokerServiceConfigurationData` PowerShellコマンドを使用して設定を構成します。例:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

期間移行時に電源ポリシーアクションを適用する前に、マシンは次の基準を満たす必要があります。

- 切断されたセッションがあること。
- 保留中の電源アクションがないこと。

- 異なる時間帯に移行するVDI（シングルセッション）デリバリーグループに属していること。
- 特定の時間帯（ピーク時またはオフピーク時）にセッションが切断され、電源アクションが割り当てられている時間帯に移行すること。

カタログの電源オン状態のVDAの割合を変更する

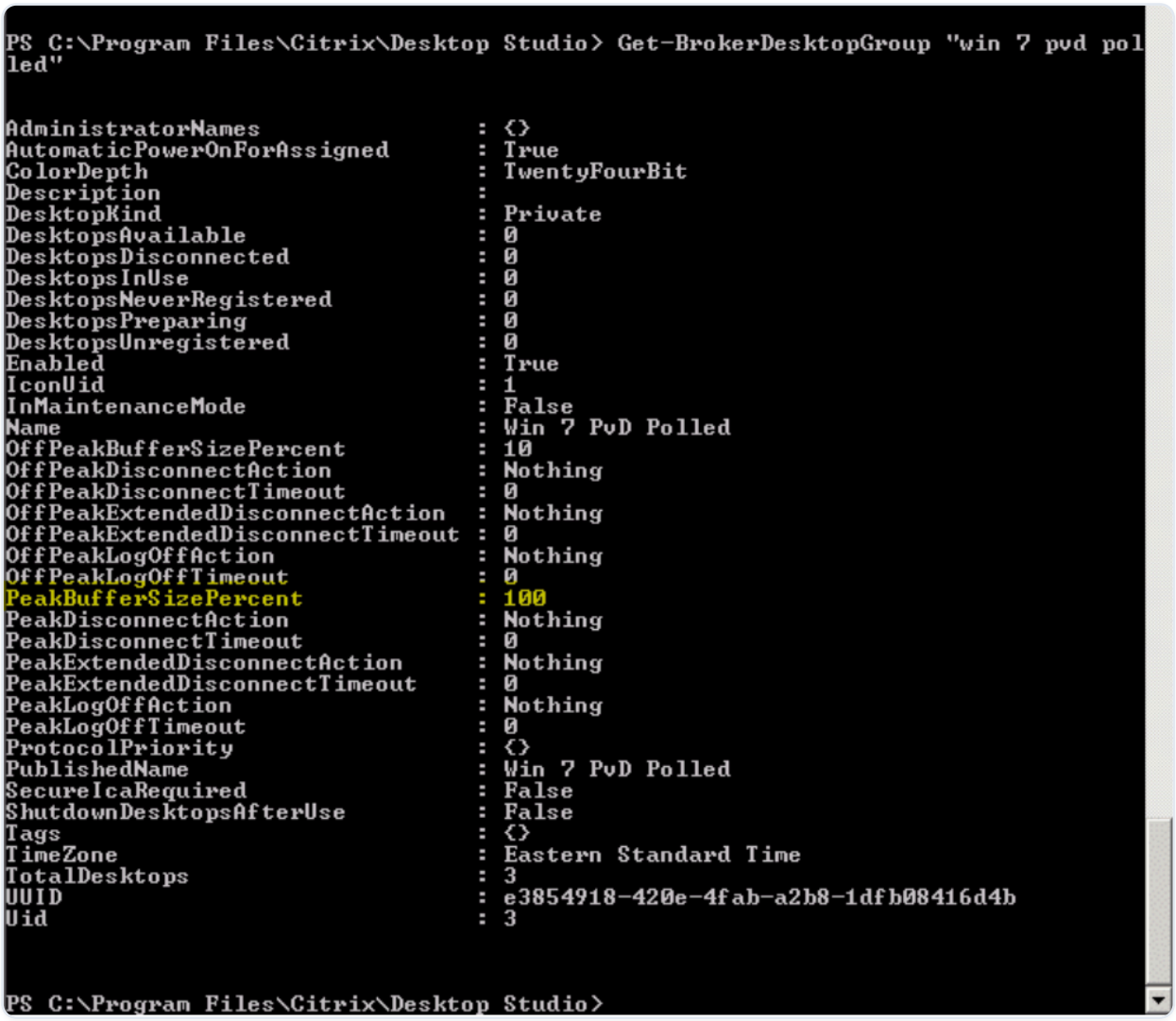
1. デリバリーグループの**電源管理**セクションから、デリバリーグループのピーク時間を調整します。
2. デスクトップグループ名をメモします。
3. 管理者権限でPowerShellを起動し、次のコマンドを実行します。「Desktop Group Name」を、実行中のVDAの割合が変更されたデスクトップグループの名前に置き換えます。

   ```
   asnp Citrix*
   ```

   ```
   # Set-BrokerDesktopGroup "Desktop Group Name" -PeakBufferSizePercent 100
   ```

   「100」という値は、VDAの100%が準備完了状態であることを意味します。
4. 解決策を実行して確認します。

   ```
   #Get-BrokerDesktopGroup "Desktop Group Name"
   ```



変更が有効になるまで最大1時間かかる場合があります。

ユーザーがログオフした後にVDAをシャットダウンするには、次のように入力します。

```
# Set-BrokerDesktopGroup "Desktop Group Name" -ShutDownDesktopsAfterUse $True
```

ピーク時にVDAを再起動して、ユーザーがログオフした後にすぐに使用できるようにするには、次のように入力します。

```
# Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssignedDuringPeak $True
```

セッション

- セッションのログオフまたは切断、またはユーザーへのメッセージ送信
- セッションのプレ起動とセッションの維持を構成する
- メンテナンスモードのマシンから切断された場合のセッション再接続を制御する

- セッションローミングを構成する

セッションのログオフまたは切断

1. 左ペインで**Delivery Groups**を選択します。
2. デリバリーグループを選択し、次にアクションバーで**View Machines**を選択します。
3. 中央ペインでマシンを選択し、アクションバーで**View Sessions**を選択し、次にセッションを選択します。
    - または、中央ペインで**Session**タブを選択し、次にセッションを選択します。
4. セッションからログオフするには、アクションバーで**Log off**を選択します。セッションが閉じられ、ユーザーはログアウトされます。マシンが特定のユーザーに割り当てられていない限り、他のユーザーが利用できるようになります。
5. セッションを切断するには、アクションバーで**Disconnect**を選択します。アプリケーションはセッション内で実行を継続し、マシンはそのユーザーに割り当てられたままになります。ユーザーは同じマシンに再接続できます。

シングルセッションOSマシンに対して電源状態タイマーを構成して、未使用のセッションを自動的に処理できます。詳細については、Power managed machinesを参照してください。

デリバリーグループにメッセージを送信する

1. 左ペインで**Delivery Groups**を選択します。
2. デリバリーグループを選択し、アクションバーで**View Machines**を選択します。
3. 中央ペインで、メッセージを送信するマシンを選択します。
4. アクションバーで、**View Sessions**を選択します。
5. 中央ペインで、すべてのセッションを選択し、次にアクションバーで**Send Message**を選択します。
6. メッセージを入力し、**OK**をクリックします。必要に応じて、重大度レベルを指定できます。オプションには、**Critical**、**Question**、**Warning**、および**Information**が含まれます。

または、Citrix Directorを使用してメッセージを送信することもできます。詳しくは、「ユーザーへのメッセージの送信」を参照してください。

デリバリーグループでセッションの事前起動とセッションの維持を構成する

これらの機能は、マルチセッションOSマシンでのみサポートされています。

セッションの事前起動とセッションの維持機能は、要求される前にセッションを開始すること（セッションの事前起動）と、ユーザーがすべてのアプリケーションを閉じた後もアプリケーションセッションをアクティブに保つこと（セッションの維持）により、指定されたユーザーがアプリケーションにすばやくアクセスできるようにします。

デフォルトでは、セッションの事前起動とセッションの維持は使用されません。セッションは、ユーザーがアプリケーションを起動したときに開始（起動）され、セッション内の最後に開いたアプリケーションが閉じるまでアクティブなままになります。

考慮事項:

- デリバリーグループはアプリケーションをサポートしている必要があり、マシンはマルチセッションOS用のVDA（最小バージョン7.6）を実行している必要があります。
- これらの機能は、Windows向けCitrix Workspaceアプリを使用している場合にのみサポートされており、追加のCitrix Workspaceアプリ構成も必要です。手順については、お使いのWindows向けCitrix Workspaceアプリバージョンの製品ドキュメントで「session prelaunch」を検索してください。
- HTML5向けCitrix Workspaceアプリはサポートされていません。
- セッションの事前起動を使用している場合、ユーザーのマシンがサスペンドモードまたは休止モードになると、事前起動は機能しません（セッションの事前起動設定に関係なく）。ユーザーはマシン/セッションをロックできます。ただし、ユーザーがCitrix Workspaceアプリからログオフすると、セッションは終了し、事前起動は適用されなくなります。
- セッションの事前起動を使用している場合、物理クライアントマシンはサスペンドまたは休止の電源管理機能を使用できません。クライアントマシンのユーザーはセッションをロックできますが、ログオフしてはいけません。
- 事前起動されたセッションと維持されたセッションは、接続されている場合にのみ同時ライセンスを消費します。ユーザー/デバイスライセンスを使用している場合、ライセンスは90日間有効です。デフォルトでは、未使用の事前起動されたセッションと維持されたセッションは15分後に切断されます。この値はPowerShell (`New/Set-BrokerSessionPreLaunch` コマンドレット) で構成できます。
- これらの機能が互いに補完し合うように調整するには、ユーザーのアクティビティパターンを慎重に計画し、監視することが不可欠です。最適な構成は、ユーザーがアプリケーションをより早く利用できるという利点と、ライセンスの使用とリソースの割り当てにかかるコストとのバランスを取ります。
- Citrix Workspaceアプリで、セッションの事前起動を特定の時刻にスケジュールすることもできます。

未使用の事前起動セッションと残存セッションがアクティブなままになる期間

ユーザーがアプリケーションを起動しない場合に、未使用のセッションがアクティブなままになる期間を指定する方法はいくつかあります。構成されたタイムアウトとサーバー負荷のしきい値です。これらすべてを構成できます。最初に発生したイベントにより、未使用のセッションが終了します。

- **タイムアウト:** 設定されたタイムアウトは、未使用のプレローンチセッションまたはリンガーセッションがアクティブな状態を維持する分数、時間、または日数を指定します。タイムアウトを短く設定しすぎると、プレローンチセッションは、アプリケーションへのより迅速なアクセスというユーザーのメリットを提供する前に終了します。タイムアウトを長く設定しすぎると、サーバーに十分なリソースがないため、受信ユーザー接続が拒否される可能性があります。

  このタイムアウトは、SDK (`New/Set-BrokerSessionPreLaunch` コマンドレット) からのみ有効にでき、管理コンソールからは有効にできません。タイムアウトを無効にすると、そのデリバリーグループのコンソール表示や**デリバリーグループの編集**ページには表示されません。

- **しきい値:** サーバーの負荷に基づいてプレローンチセッションとリンガーセッションを自動的に終了すると、サーバーリソースが利用可能である限り、セッションが可能な限り長く開いたままになります。未使用のプレローンチセッションとリンガーセッションは、新しいユーザーセッションにリソースが必要なときに自動的に終了するため、接続拒否の原因にはなりません。

  2つのしきい値を構成できます。デリバリーグループ内のすべてのサーバーの平均負荷率と、グループ内の単一サーバーの最大負荷率です。しきい値を超えると、プレローンチ状態またはリンガー状態であった時間が最も長いセッションが終了します。負荷がしきい値を下回るまで、セッションは1分間隔で1つずつ終了します。しきい値を超えている間は、新しいプレローンチセッションは開始されません。

Controllerに登録されていないVDAを持つサーバーと、メンテナンスモードのサーバーは、完全にロードされていると見なされます。計画外の停止により、容量を解放するために事前起動セッションと残存セッションが自動的に終了します。

セッションの事前起動を有効にするには

1. グループを選択し、アクションバーで**デリバリーグループの編集**をクリックします。
2. **アプリケーションの事前起動**ページで、セッションを起動するタイミングを選択して、セッションの事前起動を有効にします。

   - ユーザーがアプリケーションを起動したとき。これはデフォルト設定です。セッションのプレローンチは無効になっています。

- デリバリーグループ内のいずれかのユーザーがWindows向けCitrix Workspaceアプリにログオンしたとき。
- ユーザーおよびユーザーグループのリスト内のいずれかのユーザーがWindows向けCitrix Workspaceアプリにログオンしたとき。このオプションを選択する場合は、ユーザーまたはユーザーグループも指定してください。

アプリケーションの事前起動セッションページ(/en-us/citrix-virtual-apps-desktops/2411/media/dws-session-2.png)

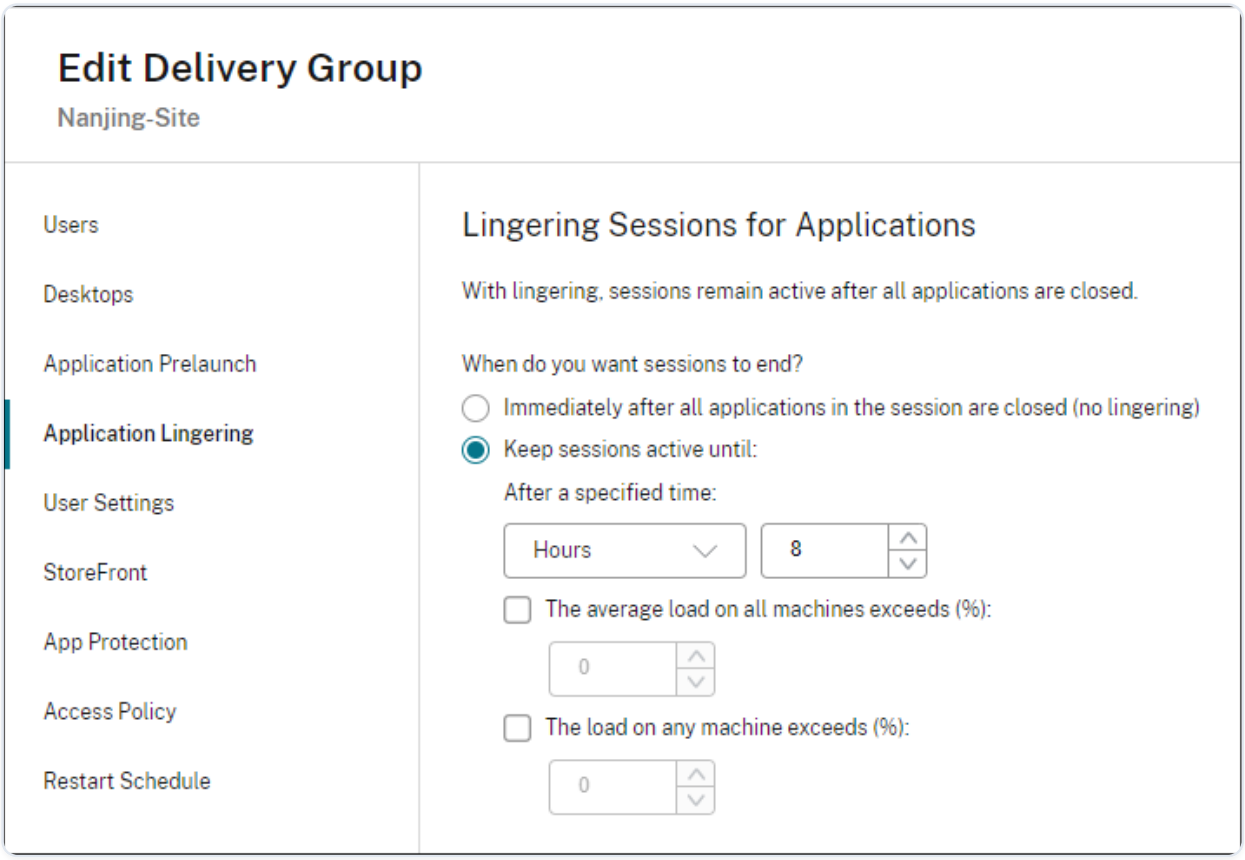
3. ユーザーがアプリケーションを起動すると、プレローンチセッションは通常のセッションに置き換えられます。ユーザーがアプリケーションを起動しない場合（プレローンチセッションが未使用の場合）、以下の設定がそのセッションがアクティブな状態を維持する期間に影響します。

   - 指定された時間間隔が経過したとき。時間間隔は変更できます（1〜99日、1〜2376時間、または1〜142,560分）。
   - デリバリーグループ内のすべてのマシンの平均負荷が指定された割合（1〜99%）を超えたとき。
   - デリバリーグループ内のいずれかのマシンの負荷が指定された割合（1〜99%）を超えたとき。

   まとめ: プレ起動されたセッションは、ユーザーがアプリケーションを起動する、指定された時間が経過する、または指定された負荷しきい値を超える、のいずれかのイベントが発生するまでアクティブなままです。

セッションの維持を有効にするには

1. 左側のペインで を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. ページで、 を選択してセッションの維持を有効にします。



4. ユーザーが別のアプリケーションを起動しない場合、残存セッションがアクティブなままになる期間に影響する設定がいくつかあります。

   - 指定された時間間隔が経過した場合。時間間隔は、1～99日、1～2376時間、または1～142,560分に変更できます。
   - デリバリーグループ内のすべてのマシンの平均負荷が指定された割合（1～99%）を超えた場合。
   - デリバリーグループ内のいずれかのマシンの負荷が指定された割合（1～99%）を超えた場合。

   まとめ：残存セッションは、ユーザーがアプリケーションを起動する、指定された時間が経過する、または指定された負荷しきい値を超える、のいずれかのイベントが発生するまでアクティブなままです。

メンテナンスモードのマシンから切断された場合のセッション再接続を制御する

> **注：**
>
> この機能はPowerShellでのみ利用可能です。

> メンテナンスモードのマシンで切断されたセッションが、デリバリーグループ内のマシンに再接続できるかどうかを制御できます。

バージョン2106より前は、メンテナンスモードのマシンから切断されたシングルセッションのプールされたデスクトップセッションの再接続は許可されていませんでした。バージョン2106以降では、メンテナンスモードのマシンから切断された後、デリバリーグループで再接続を許可または禁止するように構成できます（セッションの種類に関係なく）。

デリバリーグループを作成または編集するとき（`New-BrokerDesktopGroup`、`Set-BrokerDesktopGroup`）、`-AllowReconnectInMaintenanceMode <boolean>`パラメーターを使用して、メンテナンスモードのマシンから切断されたマシンへの再接続を許可または禁止します。

- trueに設定すると、セッションはグループ内のマシンに再接続できます。
- 「false」に設定されている場合、セッションはグループ内のマシンに再接続できません。

デフォルト値:

- シングルセッション: 無効
- マルチセッション: 有効

セッションローミングの構成

デフォルトでは、デリバリーグループでセッションローミングが有効になっています。セッションは、ユーザーとともにクライアントデバイス間をローミングします。ユーザーがセッションを起動し、別のデバイスに移動すると、同じセッションが使用され、アプリケーションは両方のデバイスで同時に利用可能になります。複数のデバイスでアプリケーションを表示できます。アプリケーションは、デバイスや現在のセッションの有無に関係なく追従します。多くの場合、アプリケーションに割り当てられたプリンターやその他のリソースも追従します。または、PowerShellを使用することもできます。詳細については、「セッションローミング」を参照してください。

アプリケーションのセッションローミングの構成

アプリケーションのセッションローミングを構成するには、次の手順に従います。

1. コンソールで、左側のペインの**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**「デリバリーグループの編集」**を選択します。
3. ページで、 チェックボックスをオンにして、セッションローミングを有効にします。

    - 有効にすると、ユーザーがアプリケーションセッションを起動してから別のデバイスに移動した場合、同じセッションが使用され、両方のデバイスで利用可能になります。無効にすると、セッションはデバイス間をローミングしなくなります。

4. 変更を適用してウィンドウを閉じるには、**OK**を選択します。

デスクトップのセッションローミングを構成する

デスクトップのセッションローミングを構成するには、次の手順に従います。

1. コンソールで、左ペインの**Delivery Groups**を選択します。
2. グループを選択し、アクションバーの**Edit**を選択します。
3. **Desktops**ページで、デスクトップを選択し、**Edit**を選択します。
4. **Session roaming**チェックボックスをオンにして、セッションローミングを有効にします。

- 有効にすると、ユーザーがデスクトップを起動してから別のデバイスに移動した場合、同じセッションが使用され、アプリケーションは両方のデバイスで利用可能になります。無効にすると、セッションはデバイス間をローミングしなくなります。

変更を適用してウィンドウを閉じるには、**OK**を選択します。

アプリケーション

デリバリーグループのアプリケーションを表示および追加します。

1. コンソールで、左ペインの**Delivery Groups**を選択します。
2. グループを選択します。このグループにアプリケーションが含まれている場合、アクションバーに**View Applications**が表示されます。
3. **View Applications**を選択します。**Applications**ノードに移動し、このグループで利用可能なすべてのアプリケーションが表示されます。
4. このグループにアプリケーションを追加するには、**デリバリーグループ**ノードに移動し、グループを選択して、アクションバーで**アプリケーションの追加**を選択します。

トラブルシューティング

- Delivery Controllerに登録されていないVDAは、ブローカーセッションの起動時に考慮されません。これにより、利用可能なはずのリソースが十分に活用されないことになります。VDAが登録されない理由はさまざまであり、その多くは管理者がトラブルシューティングできます。詳細表示には、カタログ作成ウィザードと、デリバリーグループにカタログを追加した後のトラブルシューティング情報が表示されます。

  デリバリーグループを作成すると、デリバリーグループの詳細ペインには、登録可能だが登録されていないマシンの数が表示されます。たとえば、1台以上のマシンが電源オンでメンテナンスモードではないにもかかわらず、現在Controllerに登録されていない場合があります。「登

録されていないが、登録されるべき」マシンを表示する際は、詳細ペインの**トラブルシューティング**タブで、考えられる原因と推奨される是正措置を確認してください。

機能レベルに関するメッセージについては、「VDAのバージョンと機能レベル」を参照してください。

VDA登録のトラブルシューティングについては、「CTX136668」を参照してください。

- デリバリーグループの表示では、詳細ペインの**インストールされているVDAバージョン**が、マシンに実際にインストールされているバージョンと異なる場合があります。マシンのWindowsのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- **電源状態不明**ステータスのマシンについては、CTX131267でガイダンスを参照してください。

アプリケーショングループの作成

注:

Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

アプリケーショングループを使用すると、アプリケーションのコレクションを管理できます。異なるデリバリーグループ間で共有されるアプリケーション、またはデリバリーグループ内のユーザーのサブセットによって使用されるアプリケーションに対してアプリケーショングループを作成します。アプリケーショングループはオプションであり、同じアプリケーションを複数のデリバリーグループに追加する代替手段を提供します。デリバリーグループを複数のアプリケーショングループに関連付けたり、アプリケーショングループを複数のデリバリーグループに関連付けたりできます。

アプリケーショングループを使用すると、より多くのデリバリーグループを使用する場合と比較して、アプリケーション管理とリソース制御の利点が得られます。

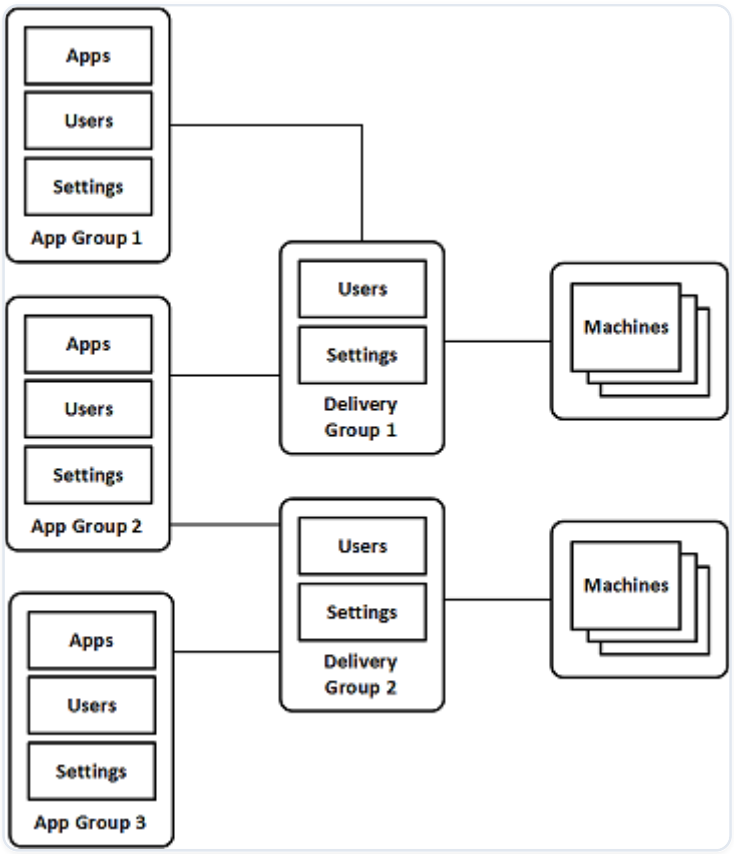
- アプリケーションとその設定を論理的にグループ化することで、それらのアプリケーションを単一の単位として管理できます。たとえば、同じアプリケーションを個々のデリバリーグループに一度に1つずつ追加（公開）する必要はありません。

- アプリケーショングループ間のセッション共有により、リソース消費を節約できます。それ以外の場合、アプリケーショングループ間のセッション共有を無効にすることが有益な場合もあります。
- タグ制限機能を使用すると、選択したデリバリーグループ内のマシンのサブセットのみを考慮して、アプリケーショングループからアプリケーションを公開できます。タグ制限を使用すると、既存のマシンを複数の公開タスクに使用できるため、追加のマシンを展開および管理するコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）するものと考えることができます。タグ制限付きのアプリケーショングループまたはデスクトップを使用すると、デリバリーグループ内のマシンのサブセットを分離してトラブルシューティングする際に役立ちます。

構成例

例 1:

次の図は、アプリケーショングループを含むCitrix Virtual Apps and Desktops展開を示しています。



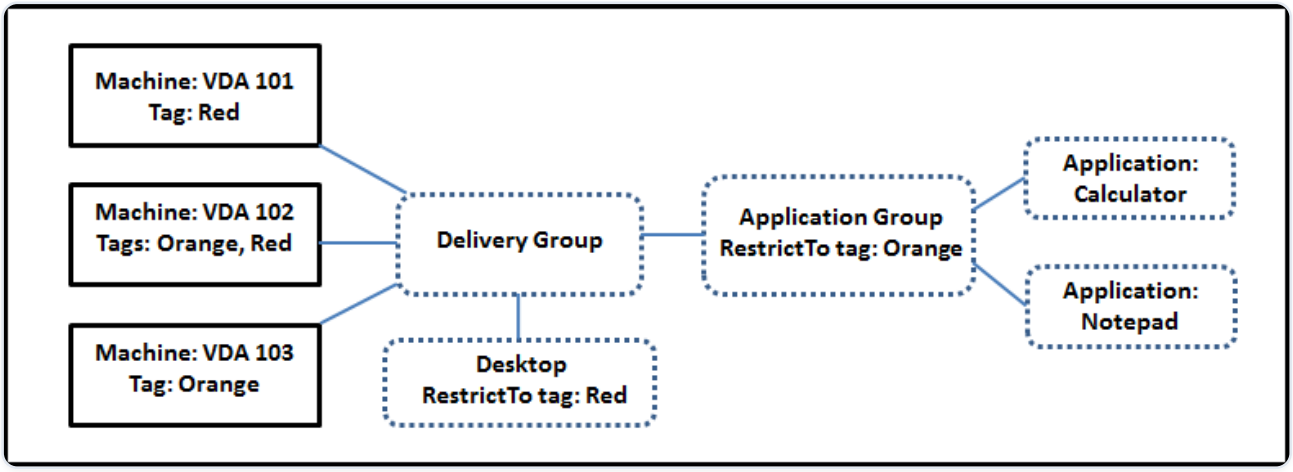
この構成では、アプリケーションはデリバリーグループではなくアプリケーショングループに追加されます。デリバリーグループは、どのマシンが使用されるかを指定します。（図には示されていませんが、マシンはマシンカタログにあります。）

アプリケーショングループ1はデリバリーグループ1に関連付けられています。アプリケーショングループ1で指定されたユーザーによって、アプリケーショングループ1内のアプリケーションにアクセスします。これらのグループは、デリバリーグループ1のユーザーリストにも含まれている場合にのみ表示されます。この構成は、アプリケーショングループのユーザーリストが、関連付けられたデリバリーグループのユーザーリストのサブセット（制限）であるというガイダンスに従っています。アプリケーショングループ1の設定（アプリケーショングループ間のアプリケーションセッション共有、関連付けられたデリバリーグループなど）は、そのグループ内のアプリケーションとユーザーに適用されます。デリバリーグループ1の設定は、アプリケーショングループ1と2のユーザーに適用されます。これは、これらのアプリケーショングループがそのデリバリーグループに関連付けられているためです。

アプリケーショングループ2は、2つのデリバリーグループ（1と2）に関連付けられています。これらのデリバリーグループのそれぞれには、アプリケーショングループ2で優先順位が割り当てられ、アプリケーションが起動される際にデリバリーグループがチェックされる順序を示します。優先順位が同じデリバリーグループは負荷分散されます。アプリケーショングループ2で指定されたユーザーは、アプリケーショングループ2内のアプリケーションにアクセスします。ただし、それらのユーザーはデリバリーグループ1とデリバリーグループ2のユーザーリストにも含まれている必要があります。

例 2:

このシンプルなレイアウトでは、タグ制限を使用して、特定のデスクトップおよびアプリケーションの起動に考慮されるマシンを制限します。このサイトには、1つの共有デリバリーグループ、1つの公開デスクトップ、および2つのアプリケーションで構成された1つのアプリケーショングループがあります。



3台のマシン（VDA 101～103）のそれぞれにタグが追加されています。

アプリケーショングループは「Orange」タグ制限で作成されました。そのアプリケーションはそれぞれ、「Orange」タグを持つデリバリーグループ内のマシン（VDA 102および103）でのみ起動されます。

アプリケーショングループ（およびデスクトップ）でのタグ制限の使用に関するより包括的な例とガイダンスについては、「タグ」を参照してください。

ガイダンスと考慮事項

Citrixでは、アプリケーションをアプリケーショングループまたはデリバリーグループのいずれかに追加することをお勧めします。両方に追加することはお勧めしません。そうしないと、2種類のグループにアプリケーションが存在することによる複雑さが増し、管理が困難になる可能性があります。

デフォルトでは、アプリケーショングループは有効になっています。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

デフォルトでは、アプリケーショングループ間のアプリケーションセッション共有は有効になっています。「アプリケーショングループ間のセッション共有」を参照してください。

Citrixでは、デリバリーグループを現在のバージョンにアップグレードすることをお勧めします。このプロセスには、次のものが必要です。

1. デリバリーグループで使用されるマシン上のVDAのアップグレード。
2. それらのマシンを含むマシンカタログのアップグレード。
3. デリバリーグループのアップグレード。

詳細については、「デリバリーグループの管理」を参照してください。

アプリケーショングループを使用するには、コアコンポーネントが最小バージョン7.9である必要があります。

アプリケーショングループを作成するには、デリバリーグループ管理者組み込みロールの委任管理権限が必要です。詳細については、委任管理を参照してください。

この記事では、アプリケーションを複数のアプリケーショングループに「関連付ける」ことについて言及しています。これは、利用可能なソースからそのアプリケーションのインスタンスを追加するアクションとは区別されます。同様に、デリバリーグループはアプリケーショングループに関連付けられており、互いの追加やコンポーネントではありません。

アプリケーショングループとのセッション共有

アプリケーションセッション共有が有効になっている場合、すべてのアプリケーションは同じアプリケーションセッションで起動します。これにより、より多くのアプリケーションセッションを起動するのにかかるコストが節約され、コピー＆ペースト操作など、クリップボードを使用するアプリケーション機能を利用できるようになります。ただし、状況によってはセッション共有をクリアできます。

アプリケーショングループを使用する場合、デリバリーグループのみを使用する場合に利用できる標準のセッション共有動作を拡張する、次の3つの方法でアプリケーションセッション共有を構成できます。

- アプリケーショングループ間でセッション共有が有効。
- 同じアプリケーショングループ内のアプリケーション間でのみセッション共有が有効。
- セッション共有が無効。

アプリケーショングループ間のセッション共有

アプリケーショングループ間でアプリケーションセッション共有を有効にすることも、または、同じアプリケーショングループ内のアプリケーションにのみアプリケーションセッション共有を制限するために無効にすることもできます。

- **アプリケーショングループ間のセッション共有を有効にすることが役立つ例:**

  アプリケーショングループ1にはWordやExcelなどのMicrosoft Officeアプリケーションが含まれています。アプリケーショングループ2にはメモ帳や電卓などの他のアプリケーションが含まれており、両方のアプリケーショングループは同じデリバリーグループにアタッチされています。両方のアプリケーショングループにアクセスできるユーザーがWordを起動してアプリケーションセッションを開始し、次にメモ帳を起動します。コントローラーが、Wordを実行しているユーザーの既存のセッションがメモ帳の実行に適していると判断した場合、メモ帳は既存のセッション内で起動されます。既存のセッションからメモ帳を実行できない場合（たとえば、タグ制限によってセッションが実行されているマシンが除外される場合など）、セッション共有を使用するのではなく、適切なマシン上に新しいセッションが作成されます。

- **アプリケーショングループ間のセッション共有を無効にすることが役立つ例:**

  同じマシンにインストールされている他のアプリケーションと相互運用性が低いアプリケーションのセットを含む構成。たとえば、同じソフトウェアスイートの2つの異なるバージョンや、同じWebブラウザの2つの異なるバージョンなどです。ユーザーが同じセッションで両方のバージョンを起動することを許可しない方がよいでしょう。

ソフトウェアスイートの各バージョンに対してアプリケーショングループを作成し、各バージョンのアプリケーションを対応するアプリケーショングループに追加します。これらのアプリケーショングループのそれぞれでグループ間のセッション共有が無効になっている場合、それらのグループで指定されたユーザーは、同じセッションで同じバージョンのアプリケーションを実行できます。ユーザーは同時に他のアプリケーションを実行することもできますが、同じセッションでは実行できません。異なるバージョンのアプリケーション、またはアプリケーショングループに含まれていないアプリケーションのいずれかを起動すると、そのアプリケーションは新しいセッションで起動されます。

このアプリケーショングループ間のセッション共有機能は、セキュリティサンドボックス機能ではありません。これは完璧ではなく、ユーザーが他の手段（例えば、Windows Explorer経由など）でセッションにアプリケーションを起動するのを防ぐことはできません。

マシンが容量に達している場合、新しいセッションはそのマシンでは開始されません。必要に応じて、セッション共有を使用して、新しいアプリケーションがそのマシンの既存のセッションで開始されます。

アプリケーションセッション共有が許可されているアプリケーショングループに対してのみ、プリローンチセッションを利用可能にできます。（セッションリンガー機能を使用するセッションは、すべてのアプリケーショングループで利用可能です。）これらの機能は、アプリケーショングループに関連付けられている各デリバリーグループで有効にして構成する必要があります。アプリケーショングループでは構成できません。

デフォルトでは、アプリケーショングループを作成すると、アプリケーショングループ間のアプリケーションセッション共有が有効になります。グループの作成時にこれを変更することはできません。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

アプリケーショングループ内でのセッション共有を無効にする

同じアプリケーショングループ内のアプリケーション間でのアプリケーションセッション共有を防ぐことができます。

- **アプリケーショングループ内でのセッション共有を無効にすることが役立つ例:**

  ユーザーに、別々のモニターでアプリケーションの複数の同時フルスクリーンセッションにアクセスさせたい場合。

  アプリケーショングループを作成し、そこにアプリケーションを追加します。

デフォルトでは、アプリケーショングループを作成すると、アプリケーションセッション共有が有効になります。グループの作成時にこの設定を変更することはできません。アプリケーショング

ループを作成した後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

アプリケーショングループを作成する

アプリケーショングループを作成するには：

1. Web Studioにサインインします。
2. 左ペインで**アプリケーション**を選択し、次に**アプリケーショングループ**タブを選択します。
3. フォルダーを使用してアプリケーショングループを整理するには、**アプリケーショングループ**ルートフォルダーの下にフォルダーを作成します。詳しくは、「フォルダーを使用したアプリケーショングループの整理」を参照してください。
4. グループを作成するフォルダーを選択し、**アプリケーショングループの作成**をクリックします。グループ作成ウィザードが**はじめに**ページで起動します。このページは、このウィザードの今後の起動から削除できます。
5. 以下のページで説明されている設定を構成するには、ウィザードに従います。各ページの作業が完了したら、**概要**ページに到達するまで**次へ**を選択します。

手順1. デリバリーグループ

デリバリーグループページには、すべてのデリバリーグループと、各グループに含まれるマシンの数が一覧表示されます。

- **互換性のあるデリバリーグループ**リストには、選択できるデリバリーグループが含まれています。互換性のあるデリバリーグループには、ランダム（永続的または静的に割り当てられていない）なマルチセッションまたはシングルセッションOSマシンが含まれています。
- **互換性のないデリバリーグループ**リストには、選択できないデリバリーグループが含まれています。各エントリには、静的に割り当てられたマシンが含まれているなど、互換性がない理由が説明されています。

アプリケーショングループは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。

以下の両方の条件が満たされている場合、デスクトップのみを配信する共有マシンを含むデリバリーグループを選択することもできます。

- デリバリーグループに共有マシンが含まれており、XenDesktopバージョン7.9より前のバージョンで作成されていること。
- デリバリーグループの編集権限があること。

アプリケーショングループ作成ウィザードがコミットされると、デリバリーグループの種類は自動的に「デスクトップとアプリケーション」に変換されます。

関連付けられたデリバリーグループがないアプリケーショングループを作成することはできますが（アプリケーションを整理するため、または現在使用されていないアプリケーションのストレージとして機能させるためなど）、少なくとも1つのデリバリーグループを指定するまで、そのアプリケーショングループをアプリケーションの配信に使用することはできません。また、デリバリーグループが指定されていない場合、**スタート**メニューソースからアプリケーショングループにアプリケーションを追加することはできません。

選択したデリバリーグループは、アプリケーションの配信に使用されるマシンを指定します。アプリケーショングループに関連付けるデリバリーグループの横にあるチェックボックスをオンにします。

タグ制限を追加するには、「**タグを持つマシンへの起動を制限する**」を選択し、ドロップダウンリストからタグを選択します。

手順2. ユーザー

アプリケーショングループでアプリケーションユーザーを指定します。前のページで選択したデリバリーグループ内のすべてのユーザーとユーザーグループを許可するか、それらのデリバリーグループから特定のユーザーとユーザーグループを選択します。指定されたユーザーに利用を制限する場合、デリバリーグループで指定されたユーザーのうち、アプリケーショングループで指定されたユーザーのみが、このグループのアプリケーションにアクセスできます。基本的に、アプリケーショングループのユーザーリストは、デリバリーグループのユーザーリストに対するフィルターとして機能します。

認証されていないユーザーによるアプリケーションの使用の有効化または無効化は、アプリケーショングループではなく、デリバリーグループでのみ利用できます。

展開でユーザーリストが指定される場所については、「ユーザーリストが指定される場所」を参照してください。

ステップ3. アプリケーション

知っておくと良いこと:

- デフォルトでは、追加する新しいアプリケーションは**アプリケーション**という名前のフォルダーに配置されます。別のフォルダーを指定することもできます。アプリケーションを追加しようとして、同じ名前のアプリケーションがそのフォルダーに存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。提案された一意の名前に同意すると、その新しい名前でアプリケーションが追加されます。そうでない場合は、追加する前に

自分で名前を変更する必要があります。詳細については、「アプリケーションフォルダーの管理」を参照してください。

- アプリケーションのプロパティ（設定）は、追加時または後で変更できます。「アプリケーションプロパティの変更」を参照してください。同じ名前の2つのアプリケーションを同じユーザーに公開する場合、Web Studioで**アプリケーション名（ユーザー向け）**プロパティを変更してください。そうしないと、ユーザーはCitrix Workspaceアプリで重複した名前を目にすることになります。
- アプリケーションを複数のアプリケーショングループに追加する場合、それらのすべてのグループでアプリケーションを表示する十分な権限がないと、表示の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが追加されたすべてのグループを含むようにスコープを拡張してください。

アプリケーションソースを表示するには、ドロップダウンメニューから「**追加**」をクリックします。

- **スタートメニューから**：選択したデリバリーグループ内のマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、「**OK**」をクリックします。

  以下のいずれかを選択した場合、このソースは選択できません。

  - 関連付けられたデリバリーグループがないアプリケーショングループ。
  - 関連付けられたデリバリーグループにマシンが含まれていないアプリケーショングループ。
  - マシンが含まれていないデリバリーグループ。

- **手動で定義:** サイト内またはネットワーク内の他の場所にあるアプリケーション。このソースを選択すると、実行可能ファイルのパス、作業ディレクトリ、オプションのコマンドライン引数、管理者とユーザーの表示名を入力する新しいページが起動します。この情報を入力したら、**OK**をクリックします。
- **既存**: 以前サイトに追加されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスを選択し、**OK**をクリックします。サイトにアプリケーションがない場合、このソースは選択できません。
- **App-V**: App-Vパッケージ内のアプリケーション。このソースを選択すると、**App-Vサーバー**または**アプリケーションライブラリ**を選択する新しいページが起動します。表示されたリストから、追加するアプリケーションのチェックボックスを選択し、**OK**をクリックします。詳しく

は、「App-Vアプリケーションの展開と配信」を参照してください。サイトでApp-Vが構成されていない場合、このソースは選択できません（または表示されない場合があります）。

前述のとおり、**追加**ドロップダウンメニューの一部のエントリは、その種類の有効なソースがない場合、選択できません。互換性のないソースはまったく表示されません（たとえば、アプリケーショングループにアプリケーショングループを追加することはできないため、アプリケーショングループを作成する際にはそのソースは表示されません）。

ステップ4. スコープ

このページは、以前にカスタムスコープを作成した場合にのみ表示されます。デフォルトでは、**すべて**のスコープが選択されています。詳しくは、「委任管理」を参照してください。

ステップ5. 概要

アプリケーショングループの名前を入力します。また、必要に応じて説明を入力することもできます。

概要情報を確認し、**「完了」**をクリックします。

アプリケーショングループの管理

> **注:**
>
> Citrix Virtual Apps and Desktops™の展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

この記事では、作成したアプリケーショングループを管理する方法について説明します。

アプリケーショングループまたはデリバリーグループでアプリケーションを管理する方法については、アプリケーションを参照してください。これには、次の方法が含まれます。

- アプリケーショングループ内のアプリケーションを追加または削除する。
- アプリケーショングループの関連付けを変更する。

アプリケーショングループの管理には、Delivery Group Administrator組み込みロールの委任管理権限が必要です。詳細については、委任管理を参照してください。

アプリケーショングループを有効または無効にする

アプリケーショングループが有効になっている場合、そのグループに追加されたアプリケーションを配信できます。アプリケーショングループを無効にすると、そのグループ内の各アプリケーションが無効になります。ただし、それらのアプリケーションが他の有効なアプリケーショングループにも関連付けられている場合、それらの他のグループから配信できます。アプリケーションがアプリケーショングループに関連付けられたデリバリーグループに明示的に追加された場合、アプリケーショングループを無効にしても、それらのデリバリーグループ内のアプリケーションには影響しません。

アプリケーショングループは作成時に有効になります。グループ作成時にこの構成を変更することはできません。

1. 左側のペインで を選択し、 タブを選択します。
2. アプリケーショングループを選択し、アクションバーで を選択します。
3. ページで、 チェックボックスをオンまたはオフにします。
4. 「**適用**」をクリックしてウィンドウを開いたままにするか、「**保存**」をクリックして変更を適用し、ウィンドウを閉じます。

アプリケーショングループ間のアプリケーションセッション共有を有効または無効にする

アプリケーショングループ間のセッション共有は、アプリケーショングループの作成時に有効になります。グループの作成時にこの構成を変更することはできません。詳細については、「アプリケーショングループとのセッション共有」を参照してください。

1. 左ペインで「**アプリケーション**」を選択し、次に「**アプリケーショングループ**」タブを選択します。
2. アプリケーショングループを選択し、アクションバーで「**アプリケーショングループの編集**」を選択します。
3. 「**設定**」ページで、「**アプリケーショングループ間のアプリケーションセッション共有を有効にする**」チェックボックスをオンまたはオフにします。
4. 「**適用**」をクリックしてウィンドウを開いたままにするか、「**保存**」をクリックして変更を適用し、ウィンドウを閉じます。

アプリケーショングループ内でのアプリケーションセッション共有を無効にする

同じアプリケーショングループ内のアプリケーション間のセッション共有は、アプリケーショングループの作成時にデフォルトで有効になります。アプリケーショングループ間のアプリケーションセッション共有を無効にしても、同じアプリケーショングループ内のアプリケーション間のセッション共有は有効のままです。

PowerShell SDK を使用して、含まれるアプリケーション間でアプリケーションセッション共有が無効になっているアプリケーショングループを構成できます。特定の状況では、このオプションが望ましい場合があります。たとえば、ユーザーに非シームレスアプリケーションを別々のモニターの全画面アプリケーションウィンドウで起動させたい場合があります。

アプリケーショングループ内でアプリケーションセッション共有を無効にすると、そのグループ内の各アプリケーションは新しいアプリケーションセッションで起動します。同じアプリケーションを実行している適切な切断されたセッションが利用可能な場合、そのセッションは再接続されます。たとえば、メモ帳が実行されている切断されたセッションでメモ帳を起動すると、新しいセッションを作成する代わりにそのセッションが再接続されます。複数の適切な切断されたセッションが利用可能な場合、ランダムではあるが決定論的な方法で、そのうちの1つのセッションが再接続のために選択されます。同じ状況でこの状況が再発生した場合、同じセッションが選択されますが、それ以外の場合、セッションは必ずしも予測可能ではありません。

PowerShell SDK を使用して、既存のアプリケーショングループ内のすべてのアプリケーションのアプリケーションセッション共有を無効にするか、または、アプリケーションセッション共有が無効になっているグループを作成します。

PowerShell コマンドレットの例

セッション共有を無効にするには、Broker PowerShell コマンドレット `New-BrokerApplicationGroup` または `Set-BrokerApplicationGroup` を使用し、パラメーター `SessionSharingEnabled` を `False` に設定し、パラメーター `SingleAppPerSession` を `True` に設定します。

- たとえば、グループ内のすべてのアプリケーションでアプリケーションセッション共有を無効にしたアプリケーショングループを作成するには、次のようにします。

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False
  -SingleAppPerSession $True
  ```

- たとえば、既存のアプリケーショングループ内のすべてのアプリケーション間でアプリケーションセッション共有を無効にするには、次のようにします。

```
Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False
-SingleAppPerSession $True
```

考慮事項

- `SingleAppPerSession`プロパティを有効にするには、`SessionSharingEnabled`プロパティをFalseに設定する必要があります。これら2つのプロパティを同時に有効にすることはできません。`SessionSharingEnabled`パラメーターは、アプリケーショングループ間のセッション共有を指します。
- アプリケーションセッション共有は、アプリケーショングループに関連付けられているが、デリバリーグループには関連付けられていないアプリケーションに対してのみ機能します。デリバリーグループに直接関連付けられているすべてのアプリケーションは、デフォルトでセッションを共有します。
- アプリケーションが複数のアプリケーショングループに割り当てられている場合、グループの設定が競合しないようにしてください。例えば、あるグループのオプションが`True`に設定され、別のグループのオプションが`False`に設定されている場合、予期しない動作が発生します。

アプリケーショングループの名前を変更する

1. 左ペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの名前を変更**を選択します。
3. 新しい一意の名前を指定し、**OK**をクリックします。

アプリケーショングループとのデリバリーグループの関連付けを追加、削除、または優先度を変更する

アプリケーショングループは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。

以下の両方の条件が満たされている場合、デスクトップのみを配信する共有マシンを含むデリバリーグループを選択することもできます。

- デリバリーグループに共有マシンが含まれており、バージョン7.9より前に作成されていること。
- 「デリバリーグループの編集」権限が必要です。

Edit Application Group ダイアログがコミットされると、デリバリーグループの種類は自動的に「デスクトップとアプリケーション」に変換されます。

1. 左ペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **デリバリーグループ**ページを選択します。
4. デリバリーグループを追加するには、**追加**をクリックします。利用可能なデリバリーグループのチェックボックスをオンにします。（互換性のないデリバリーグループは選択できません。）選択が完了したら、**OK**をクリックします。
5. デリバリーグループを削除するには、削除するグループのチェックボックスをオンにしてから、**削除**をクリックします。プロンプトが表示されたら削除を確定します。
6. デリバリーグループの優先度を変更するには、デリバリーグループのチェックボックスをオンにしてから、**優先度の編集**をクリックします。優先度（0 = 最高）を入力し、**OK**をクリックします。
7. 加えた変更を適用してウィンドウを開いたままにするには**適用**をクリックするか、変更を適用してウィンドウを閉じるには**保存**をクリックします。

アプリケーショングループでタグ制限を追加、変更、または削除する

タグ制限の追加、変更、削除は、アプリケーション起動の対象となるマシンに予期せぬ影響を与える可能性があります。タグの考慮事項と注意事項を確認してください。

1. 左側のペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **デリバリーグループ**ページを選択します。
4. タグ制限を追加するには、**タグを持つマシンへの起動を制限する**を選択し、ドロップダウンリストからタグを選択します。
5. タグ制限を変更または削除するには、別のタグを選択するか、**Restrict launches to machines with this tag** のチェックを外してタグ制限を完全に削除します。
6. 加えた変更を適用してウィンドウを開いたままにするには、**Apply** をクリックします。変更を適用してウィンドウを閉じるには、**Save** をクリックします。

アプリケーショングループのユーザーを追加または削除する

ユーザーの詳細については、「アプリケーショングループの作成」を参照してください。

1. 左ペインで **Applications** を選択し、**Application Groups** タブを選択します。

2. アプリケーショングループを選択し、アクションバーで **Edit Application Group** を選択します。
3. **Users** ページを選択します。関連付けられたデリバリーグループ内のすべてのユーザーにアプリケーショングループ内のアプリケーションの使用を許可するか、特定のユーザーとグループのみに許可するかを指定します。ユーザーを追加するには、**Add** をクリックし、追加するユーザーを指定します。ユーザーを削除するには、1人以上のユーザーを選択し、**Remove** をクリックします。
4. 加えた変更を適用してウィンドウを開いたままにするには、**Apply** をクリックします。変更を適用してウィンドウを閉じるには、**Save** をクリックします。

アプリケーショングループでアプリケーションアイコンを追加、変更、または削除する

アプリケーションアイコンを追加、変更、または削除するには、次の手順を実行します。

1. 左ペインで **Applications** を選択します。
2. **Applications** タブで、アプリケーションを選択し、**Properties** を選択します。

   アプリケーショングループレベルで変更を行うには、**Application Groups** タブに移動し、グループ内のアプリケーションを選択して、**Properties** を選択します。
3. **Delivery** ページを選択し、**Change** を選択します。**Select Icon** ウィンドウが表示されます。
4. **Select Icon** ウィンドウで、次のいずれかを実行します。

   - アイコンを追加するには、**Add** を選択し、アイコンを参照します。
   - アイコンを削除するには、アイコンを選択し、**Remove** を選択します。
   - アイコンを変更するには、アプリケーションのアイコンを選択します。

   > **重要:**
   >
   > - サイズが200 KBを超えるアイコンを追加することはできません。
   > - .iconファイルのみを追加できます。
   > - 組み込みアイコンを削除することはできません。
   > - 使用中のアプリケーションのアイコンを削除することはできません。

5. **Save** を選択して変更を適用し、ウィンドウを閉じます。

アプリケーショングループのスコープを変更する

スコープを変更できるのは、スコープを作成した場合のみです（「すべてのスコープ」は編集できません）。詳細については、「委任管理」を参照してください。

1. 左側のペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **スコープ**ページを選択します。スコープの横にあるチェックボックスをオンまたはオフにします。
4. 加えた変更を適用してウィンドウを開いたままにするには**適用**をクリックし、変更を適用してウィンドウを閉じるには**保存**をクリックします。

アプリケーショングループのスコープを変更する

スコープは、作成した場合にのみ変更できます (すべてのスコープは編集できません)。詳細については、「委任管理」を参照してください。

1. 左ペインで**アプリケーション**を選択し、次に**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、次にアクションバーで**アプリケーショングループの編集**を選択します。
3. **スコープ**ページを選択します。変更するスコープの横にあるチェックボックスをオンまたはオフにします。
4. 加えた変更を適用してウィンドウを開いたままにするには、**適用**を選択します。または、変更を適用してウィンドウを閉じるには、**保存**を選択します。

アプリケーショングループを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに関連付けられている必要があります。アプリケーショングループを削除した結果、1つ以上のアプリケーションがどのグループにも属さなくなった場合、そのグループを削除するとそれらのアプリケーションも削除されるという警告が表示されます。その後、削除を確定またはキャンセルできます。

アプリケーションを削除しても、元のソースから削除されるわけではありません。ただし、再度利用可能にする場合は、再度追加する必要があります。

1. 左ペインで**アプリケーション**を選択し、次に**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、次にアクションバーで**グループの削除**を選択します。

3. プロンプトが表示されたら削除を確定します。

フォルダーを使用してアプリケーション グループを整理する

フォルダーを作成してアプリケーション グループを整理し、簡単にアクセスできるようにすることができます。

必要な役割

デフォルトでは、以下の組み込みロールのいずれかを持っている場合、アプリケーション グループのフォルダーを作成および管理できます。

- クラウド管理者
- フル管理者
- アプリケーション グループ管理者

カスタムロールを作成することで、管理アクションを他のユーザーに委任できます。次の表は、各アクションに必要な権限を示しています。

アクション	必要な権限
アプリケーション グループ フォルダーの作成	アプリケーション グループ フォルダーの作成
アプリケーション グループ フォルダーの削除	アプリケーション グループ フォルダーの削除
アプリケーション グループ フォルダーの移動	アプリケーション グループ フォルダーの移動
アプリケーション グループ フォルダーの名前変更	アプリケーション グループ フォルダーの編集
アプリケーショングループをフォルダーに移動する	アプリケーショングループフォルダーの編集、アプリケーショングループプロパティの編集

詳しくは、「役割の作成と管理」を参照してください。

フォルダーの作成と管理

アクションバーまたは右クリックメニューを使用して、アプリケーショングループフォルダーを作成および管理できます。さらに、アプリケーショングループまたはフォルダーをフォルダーツリー内の目的の場所にドラッグすることもできます。

知っておくと良いこと:

- フォルダーは最大5レベルまでネストできます（デフォルトのルートフォルダーを除く）。
- フォルダーにはアプリケーショングループとサブフォルダーを含めることができます。フォルダーとそのサブフォルダーにアプリケーショングループが含まれていない場合にのみ、フォルダーを削除できます。
- Web Studioのすべてのノード（**マシンカタログ**、**デリバリーグループ**、**アプリケーション**、**アプリケーショングループ**など）は、バックエンドで同じフォルダーツリーを共有します。フォルダーの名前変更または移動時に名前の競合を避けるため、異なるノード間で最上位フォルダーに一意の名前を使用してください。

  `New-BrokerAdminFolder` SDKコマンドレットを使用してフォルダーを作成し、それを**アプリケーショングループ**ノードの下に表示したい場合は、`Set-BrokerAdminFolderMetadata` コマンドレットを使用して `ContainsApplicationGroups` メタデータを追加する必要があります。

  例:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsApplicationGroups -Value true
  ```

リモートPCアクセス

注:

Citrix Virtual Apps and Desktops™の展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioの詳細については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

リモートPCアクセスは、Citrix Virtual Apps and Desktopsの機能であり、組織が従業員に企業リソースへのリモートアクセスを安全に簡単に許可できるようにします。Citrixプラットフォームは、ユーザーが物理的なオフィスPCにアクセスできるようにすることで、この安全なアクセスを可能にします。ユーザーがオフィスPCにアクセスできれば、業務に必要なすべてのアプリケーション、データ、リソースにアクセスできます。リモートPCアクセスは、テレワークに対応するために他のツールを導入・提供する必要性を排除します。例えば、仮想

> デスクトップやアプリケーション、およびそれらに関連するインフラストラクチャなどです。

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

この機能は、**リモートPCアクセス**タイプのマシンカタログで構成されており、以下の機能を提供します。

- OUを指定してマシンを追加する機能。この機能により、PCの一括追加が容易になります。
- オフィスWindows PCにログオンするユーザーに基づいた自動ユーザー割り当て。シングルユーザーおよび複数ユーザーの割り当てをサポートしています。デフォルトでは、次に割り当てられていないマシンに複数のユーザーを自動的に割り当てます。自動割り当てをシングルユーザーに制限するには、Web Studioにサインインし、**設定**に移動して、**リモートPCアクセスでの複数ユーザーの自動割り当てを有効にする**設定をオフにします。

Citrix Virtual Apps and Desktopsは、他の種類のマシンカタログを使用することで、物理PCのより多くのユースケースに対応できます。これらのユースケースには、次のものが含まれます。

- 物理Linux PC
- プールされた物理PC（つまり、ランダムに割り当てられ、専用ではないもの）

> **注:**
>
> サポートされているOSバージョンの詳細については、シングルセッションOSおよびLinux VDAのVDAのシステム要件を参照してください。

> オンプレミス展開の場合、リモートPCアクセスはCitrix Virtual Apps and Desktops AdvancedまたはPremiumライセンスでのみ有効です。セッションは、他のCitrix Virtual Desktops™セッションと同じ方法でライセンスを消費します。Citrix Cloudの場合、リモートPCアクセスはCitrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）およびWorkspace Premium Plusで有効です。

考慮事項

Citrix Virtual Apps and Desktops全般に適用されるすべての技術要件と考慮事項はRemote PC Accessにも適用されますが、物理PCの使用事例により関連性が高い、または排他的なものもあります。

> **重要:**
>
> Windows 11物理システム（および一部のWindows 10を実行しているシステム）には、仮想化ベースのセキュリティ機能が含まれており、その結果、VDAソフトウェアがそれらを仮想マシンとして誤って検出します。この問題を軽減するには、以下のオプションがあります。
>
> - VDAコマンドラインインストールの一部として、「/remotepc」オプションとともに「/physicalmachine」オプションを使用する
> - 以前に言及したオプションを使用しなかった場合は、VDAのインストール後に次のレジストリ値を追加します `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
>   - 名前: ForceEnableRemotePC
>   - 種類: DWORD
>   - データ: 1

展開に関する考慮事項

Remote PC Accessの展開を計画する際には、いくつかの一般的な決定を下します。

- 既存のCitrix Virtual Apps and Desktops展開にRemote PC Accessを追加できます。このオプションを選択する前に、次の点を考慮してください。
  - 現在のDelivery ControllerまたはCloud Connectorは、Remote PC Access VDAに関連する追加の負荷をサポートするのに適切なサイズですか？
  - オンプレミスのサイトデータベースとデータベースサーバーは、Remote PC Access VDAに関連する追加の負荷をサポートするのに適切なサイズですか？
  - 既存のVDAと新しいRemote PC Access VDAは、サイトあたりの最大サポートVDA数を超えることになりますか？
- VDAは、自動化されたプロセスを通じてオフィスPCに展開する必要があります。利用可能なオプションは次のとおりです。

  - SCCMなどの電子ソフトウェア配信 (ESD) ツール: SCCMを使用してVDAをインストールする。
  - 展開スクリプト: スクリプトを使用してVDAをインストールする。
- Remote PC Accessのセキュリティに関する考慮事項を確認してください。

注：

Remote PC Accessを設計する際には、リモートPCのGPUに接続されており、現在構成・動作している物理モニターの数を考慮する必要があります。モニターがCitrixセッションで使用されていなくても、GPUによって検出された場合、そのモニターの存在はGPUがサポートする最大モニター数にカウントされます。

マシンカタログに関する考慮事項

必要なマシンカタログの種類は、ユースケースによって異なります。

- Remote PC Accessマシンカタログ
  - Windows専用PC
  - Windows専用マルチユーザーPC。このユースケースは、複数のユーザーが異なるシフトでリモートからアクセスできる物理的なオフィスPCに適用されます。
  - プールされたWindows PC。このユースケースは、コンピューターラボなど、複数の不特定多数のユーザーがアクセスできる物理PCに適用されます。
- シングルセッションOSマシンカタログ
  - 静的 - 専用Linux PC
  - ランダム - プールされたLinux PC

マシンカタログの種類を特定したら、次の点を考慮してください。

- マシンは一度に1つのマシンカタログにのみ割り当てることができます。
- 委任管理を容易にするために、地理的な場所、部門、または各カタログの管理を適切な管理者に委任しやすくするその他のグループに基づいてマシンカタログを作成することを検討してください。
- マシンアカウントが存在するOUを選択する際は、より詳細な粒度を得るために下位レベルのOUを選択してください。そのような粒度が必要ない場合は、上位レベルのOUを選択できま

す。たとえば、Bank/Officers/Tellers の場合、より詳細な粒度を得るには **Tellers** を選択します。それ以外の場合は、要件に基づいて **Officers** または **Bank** を選択できます。

- Remote PC Access マシンカタログに割り当てられた後にOUを移動または削除すると、VDAの関連付けに影響を与え、将来の割り当てで問題が発生します。したがって、マシンカタログのOU割り当て更新がActive Directoryの変更計画に考慮されるように、適切に計画してください。
- OU構造のためにマシンカタログにマシンを追加するOUを選択するのが容易でない場合でも、OUを選択する必要はありません。後でPowerShellを使用してカタログにマシンを追加できます。デスクトップの割り当てがデリバリーグループで正しく構成されていれば、ユーザーの自動割り当ては引き続き機能します。ユーザー割り当てとともにマシンカタログにマシンを追加するサンプルスクリプトは、GitHubで入手できます。
- 統合Wake on LANは、**Remote PC Access**タイプのマシンカタログでのみ利用可能です。

Linux VDAに関する考慮事項

以下の考慮事項は、Linux VDAに固有のものです。

- 物理マシンでは、Linux VDAを非3Dモードでのみ使用してください。NVIDIAドライバーの制限により、HDX 3Dモードが有効になっている場合、PCのローカル画面をブラックアウトできず、セッションのアクティビティが表示されます。この画面を表示することはセキュリティリスクです。
- 物理Linuxマシンには、シングルセッションOSタイプのマシンカタログを使用します。
- 自動ユーザー割り当てはLinuxマシンでは利用できません。
- ユーザーがすでにローカルでPCにログオンしている場合、StoreFront™からPCを起動しようとすると失敗します。
- 省電力オプションはLinuxマシンでは利用できません。

技術要件と考慮事項

このセクションでは、物理PCの技術要件と考慮事項について説明します。

- 以下はサポートされていません。
  - セッションを切断する可能性のあるKVMスイッチまたはその他のコンポーネント。
  - オールインワンPCやNVIDIA Optimus搭載ノートPCおよびPCを含むハイブリッドPC。
  - デュアルブートマシン。

- キーボードとマウスはPCに直接接続してください。モニターや、電源が切れたり切断されたりする可能性のあるその他のコンポーネントに接続すると、これらの周辺機器が使用できなくなることがあります。入力デバイスをモニターなどのコンポーネントに接続する必要がある場合は、それらのコンポーネントの電源を切らないでください。
- PCはActive Directory Domain Servicesドメインに参加している必要があります。
- Secure BootはWindows 10およびWindows 11でのみサポートされています。
- PCにはアクティブなネットワーク接続が必要です。信頼性と帯域幅を向上させるため、有線接続を推奨します。
- Wi-Fiを使用する場合は、以下を実行してください。

  a. ワイヤレスアダプターをオンのままにするように電源設定を行います。

  b. ユーザーがログオンする前にワイヤレスネットワークに自動接続できるように、ワイヤレスアダプターとネットワークプロファイルを構成します。そうしないと、ユーザーがログオンするまでVDAは登録されません。ユーザーがログオンするまで、PCはリモートアクセスに利用できません。

  c. Wi-FiネットワークからDelivery ControllersまたはCloud Connectorsに到達できることを確認します。

- ノートPCでRemote PC Accessを使用できます。ノートPCがバッテリー駆動ではなく、電源に接続されていることを確認してください。ノートPCの電源オプションをデスクトップPCのオプションと一致するように構成します。例：

  a. 休止状態機能を無効にします。

  b. スリープ機能を無効にします。

  c. 蓋を閉じたときの動作を**何もしない**に設定します。

  d. 「電源ボタンを押したときの動作」を**シャットダウン**に設定します。

  e. ビデオカードとNICの省電力機能を無効にします。

- Remote PC Accessは、Windows 10を搭載したSurface Proデバイスでサポートされています。以前に述べたラップトップと同じガイドラインに従ってください。
- ドッキングステーションを使用している場合、ラップトップのドッキング解除と再ドッキングが可能です。ラップトップをドッキング解除すると、VDAはWi-Fi経由でDelivery ControllerまたはCloud Connectorに再登録されます。ただし、ラップトップを再ドッキングしても、ワイヤレスアダプターを切断しない限り、VDAは有線接続に切り替わりません。一部のデバイスには、有線接続が確立されたときにワイヤレスアダプターを切断する組み込み機能が備わっています。その他のデバイスでは、ワイヤレスアダプターを切断するためにカスタムソリューショ

ンまたはサードパーティ製ユーティリティが必要です。以前に述べたWi-Fiに関する考慮事項を確認してください。

Remote PC Accessデバイスのドッキングとドッキング解除を有効にするには、次の手順を実行します。

a. **スタート**メニューで、**設定 > システム > 電源とスリープ**を選択し、**スリープ**を**なし**に設定します。

b. **デバイスマネージャー > ネットワークアダプター > イーサネットアダプター**で、**電源の管理**に移動し、**電力の節約のために、コンピューターでこのデバイスの電源をオフにできるようにする**のチェックを外します。**このデバイスで、コンピューターのスタンバイ状態を解除できるようにする**がオンになっていることを確認します。

- 同じオフィスPCにアクセスできる複数のユーザーは、Citrix Workspaceで同じアイコンを見ます。ユーザーがCitrix Workspaceにログオンしたときに、そのリソースがすでに別のユーザーによって使用されている場合、利用不可として表示されます。
- オフィスPCにアクセスする各クライアントデバイス（例：自宅のPC）にCitrix Workspaceアプリをインストールします。

構成シーケンス

このセクションでは、**Remote PC Access**タイプのマシンカタログを使用する場合にRemote PC Accessを構成する方法の概要を説明します。その他の種類のマシンカタログの作成方法については、マシンカタログの作成を参照してください。

1. オンプレミスサイトのみ - 統合されたWake on LAN機能を使用するには、「Wake on LAN」に概説されている前提条件を構成します。
2. Remote PC Access用に新しいCitrix Virtual Apps and Desktopsサイトが作成された場合：

   a. **Remote PC Access**サイトタイプを選択します。

   b. 「**Power Management**」ページで、デフォルトのRemote PC Accessマシンカタログの電源管理を有効または無効にするかを選択します。この設定は、後でマシンカタログのプロパティを編集して変更できます。Wake on LANの構成の詳細については、「Wake on LAN」を参照してください。

   c. 「**Users**」および「**Machine Accounts**」ページで情報を入力します。

   これらの手順を完了すると、**Remote PC Access Machines**という名前のマシンカタログと、**Remote PC Access Desktops**という名前のデリバリーグループが作成されます。
3. 既存のCitrix Virtual Apps and Desktopsサイトに追加する場合：

a. 種類が「**Remote PC Access**」のマシンカタログを作成します（ウィザードの「Operating System」ページ）。マシンカタログの作成方法の詳細については、「Create machine catalogs」を参照してください。ターゲットPCがRemote PC Accessで使用できるように、正しいOUを割り当てるようにしてください。

b. マシンカタログ内のPCへのユーザーアクセスを提供するためにデリバリーグループを作成します。デリバリーグループの作成方法の詳細については、「Create Delivery Groups」を参照してください。デリバリーグループを、PCへのアクセスを必要とするユーザーを含むActive Directoryグループに割り当てるようにしてください。

4. オフィスPCにVDAを展開します。

- シングルセッションOSコアVDAインストーラー（VDAWorkstationCoreSetup.exe）を使用することをお勧めします。
- シングルセッションのフルVDAインストーラー（VDAWorkstationSetup.exe）を`/remotepc/physicalmachine`オプションとともに使用することもできます。これは、コアVDAインストーラーを使用した場合と同じ結果になります。

> **注：**
>
> RemotePCのインストールでは、特定のユーザーシナリオでVDAが期待どおりに動作するように、`/physicalmachine`引数を`/remotepc`とともに使用します。

- ヘルプデスクチームがCitrix Directorを介してリモートサポートを提供できるように、Windowsリモートアシスタンスを有効にすることを検討してください。そのためには、`/enable_remote_assistance`オプションを使用します。詳細については、「Install using the command line」を参照してください。
- Directorでログオン期間情報を表示できるようにするには、シングルセッションのフルVDAインストーラーを使用し、「**Citrix User Profile Management WMI Plugin**」コンポーネントを含める必要があります。このコンポーネントを含めるには、`/includeadditional`オプションを使用します。詳細については、「Install using the command line」を参照してください。
- SCCMを使用してVDAを展開する方法については、「Install VDAs using SCCM」を参照してください。
- 展開スクリプトを使用してVDAを展開する方法については、「Install VDAs using scripts」を参照してください。

手順2〜4を正常に完了すると、ユーザーがPCにローカルでログオンしたときに、自分のマシンに自動的に割り当てられます。

5. ユーザーには、オフィスPCにリモートでアクセスするために使用する各クライアントデバイスにCitrix Workspaceアプリをダウンロードしてインストールするよう指示してください。Citrix Workspaceアプリは`https://www.citrix.com/downloads/`またはサポートされているモバイルデバイスのアプリケーションストアから入手できます。

レジストリを介して管理される機能

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

複数ユーザーの自動割り当てを無効にする

各Delivery Controller™で、次のレジストリ設定を追加します。

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- 名前: AllowMultipleRemotePCAssignments
- 種類: DWORD
- データ: 0

スリープモード (最小バージョン 7.16)

Remote PC Accessマシンがスリープ状態になることを許可するには、VDAにこのレジストリ設定を追加し、マシンを再起動します。再起動後、オペレーティングシステムの省電力設定が尊重されます。事前設定されたアイドルタイマーが経過すると、マシンはスリープモードに入ります。マシンがウェイクアップすると、Delivery Controllerに再登録されます。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: DisableRemotePCSleepPreventer
- 種類: DWORD
- データ: 1

セッション管理

デフォルトでは、ローカルユーザーがそのマシンでセッションを開始したとき (CTRL+ALT+DEL を押すことによって)、リモートユーザーのセッションは自動的に切断されます。この自動的な動作を防ぐには、オフィスPCに以下のレジストリエントリを追加し、その後、マシンを再起動します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: SasNotification
- 種類: DWORD
- データ: 1

デフォルトでは、タイムアウト期間内に接続メッセージが確認されない場合、リモートユーザーがローカルユーザーよりも優先されます。この動作を設定するには、この設定を使用します:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: RpcaMode
- 種類: DWORD
- データ:
  - 1 - 指定されたタイムアウト期間内にメッセージングUIに応答しない場合、リモートユーザーが常に優先されます。この設定が構成されていない場合、この動作がデフォルトです。
  - 2 - ローカルユーザーが優先されます。

Remote PC Access モードを適用するためのタイムアウトは、デフォルトで30秒です。このタイムアウトは構成できますが、30秒未満に設定しないでください。タイムアウトを構成するには、次のレジストリ設定を使用します。

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: RpcaTimeout
- 種類: DWORD
- データ: タイムアウトの秒数（10進値）

ユーザーが強制的にコンソールアクセスを取得したい場合: ローカルユーザーは、Ctrl+Alt+Delを10秒以内に2回押すことで、リモートセッションのローカル制御を取得し、切断イベントを強制できます。

レジストリ変更とマシンの再起動後、リモートユーザーが使用中にローカルユーザーがCtrl+Alt+Delを押してそのPCにログオンしようとすると、リモートユーザーにプロンプトが表示されます。このプロンプトは、ローカルユーザーの接続を許可するか拒否するかを尋ねます。接続を許可すると、リモートユーザーのセッションは切断されます。

セッション管理のログ記録

Remote PC Access には、アクティブな ICA® セッションを持つPCに誰かがアクセスしようとしたときにログを記録するログ機能が追加されました。これにより、不要なアクティビティや予期しないアクティビティがないか環境を監視し、インシデントを調査する必要がある場合にそのようなイベントを監査できます。

イベントはWindowsイベントビューアーを使用してログに記録され、**アプリケーションとサービス > Citrix > HostCore > ICA Service > 管理** にあります。

Remote PC Access の使用時にログに記録されるイベントは3種類あります。

Ctrl+Alt+Del イベント

このイベントは、アクティブなリモートセッション中にローカルユーザーがコンソールキーボードでCtrl+Alt+Delを押したときに表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベントID: 43, 44, 45
- ソース: ICA サービス

イベント ID 43

このイベントIDは、SasNotification レジストリ値が存在しない場合、またはSasNotification レジストリ値が0の場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to automatically disconnect the
remote session.
```

イベント ID 44

このイベントIDは、SasNotification レジストリ値が1であり、かつRpcaMode レジストリ値が1であるか、またはRpcaMode レジストリ値が存在しない場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user. The user preference is set to remote user.
```

イベント ID 45

このイベントIDは、SasNotification レジストリ値が1であり、かつRpcaMode レジストリ値が2である場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user.

The user preference is set to local user.
```

リモートセッション切断イベント

このイベントは、リモートセッションがさまざまな理由で切断された場合に表示されます。

イベント詳細

- ログ名: アプリケーションとサービス
- イベント ID: 46, 47, 48
- ソース: ICA Service

イベントID 46

このイベントIDは、リモートセッションが切断され、SasNotification レジストリ値が存在しないか、SasNotification レジストリ値が 0 の場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected.
```

イベントID 47

このイベントIDは、リモートユーザーがセッションの切断に同意し、SasNotification レジストリ値が 1 で、RpcaMode レジストリ値が 1 であるか、RpcaMode レジストリ値が 2 であるか、または RpcaMode レジストリ値が存在しない場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected
because the user accepted the request to disconnect the session.
```

イベントID 48

このイベントIDは、リモートユーザーが指定されたタイムアウト期間内に切断要求を拒否せず、SasNotification レジストリ値が 1 で、RpcaMode レジストリ値が 2 の場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected
because the user did not decline the disconnection request within the
configured timeout period (&lt;timeout period>).
```

Ctrl+Alt+Del が2回押されたイベント

このイベントは、Ctrl+Alt+Del が10秒以内に2回押された場合に表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベントID: 49
- ソース: ICA Service

イベントID 49

このイベントIDは、Ctrl+Alt+Delが10秒以内に2回押されたときに表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been forcibly
disconnected.
```

ウェイク・オン・LAN

Remote PC AccessはWake on LANをサポートしており、ユーザーは物理PCをリモートで起動できます。この機能により、ユーザーは使用していないときにオフィスPCの電源を切ったままにして、エネルギーコストを節約できます。また、誤ってマシンの電源が切れてしまった場合でも、リモートアクセスを可能にします。

Wake on LAN機能を使用すると、デリバリーコントローラーからの指示があった場合、PC上で実行されているVDAから、そのPCが存在するサブネットにマジックパケットが直接送信されます。これにより、追加のインフラストラクチャコンポーネントやマジックパケット配信のためのサードパーティソリューションに依存することなく、この機能が動作します。

Wake on LAN機能は、レガシーなSCCMベースのWake on LAN機能とは異なります。SCCMベースのWake on LANの詳細については、「Wake on LAN – SCCM統合」を参照してください。

制限事項

Wake on LAN機能を使用するRemote PC Accessは、ピーク時の自動電源オンをサポートしていません。

システム要件

Wake on LAN機能を使用するためのシステム要件は次のとおりです。

- コントロールプレーン:
  - シトリックス DaaS™
  - シトリックス バーチャル アプリケーションズ アンド デスクトップス 2009以降
- 物理PC:
  - VDAバージョン2009以降
  - Windows 10またはWindows 11。サポートの詳細については、VDAシステム要件を参照してください。
  - BIOS/UEFIでWake on LANが有効になっていること
  - Windows構成内のネットワークアダプターのプロパティでWake on LANが有効になっていること

Wake on LANの構成

Studioを使用したWake on LANの構成

Wake on LAN接続を作成するには:

1. 左側のペインで、**「ホスティング」**ノードを選択します。
2. **接続とリソースの追加**を選択します。
3. ウィザードの**「接続」**ページで、以下を指定します。
    a. 接続の種類: Remote PC Wake on LAN
    b. ゾーン名: Remote PC Accessカタログが存在するゾーンを選択します
    c. 接続名: Wake on LAN接続の名前を入力します
4. 接続とリソースの追加ウィザードの残りの手順を完了します。

Wake on LAN接続をRemote PC Accessマシンカタログに追加するには:

1. 新しいRemote PC Accessマシンカタログを作成している場合は、「マシンカタログセットアップ」ウィザードの**マシンタイプ**ページでドロップダウンリストを使用して接続を追加できます。
2. 既存のマシンカタログにWake on LAN接続を追加する場合：
    a. 左側の**マシンカタログ**ノードに移動します。
    b. 適切なRemote PC Accessマシンカタログを選択します。
    c. マシンカタログを右クリックするか、上部の**その他**メニューを選択します。
    d. **マシンカタログの編集**を選択します。
    e. **電源管理**ページで、**はい**を選択します。
    f. ドロップダウンリストから適切な接続を選択します。
    g. **保存**を選択します。

> **注:**
>
> Studio を介した Wake on LAN の構成は、現時点では Citrix DaaS でのみ利用可能です。

PowerShellを使用したWake on LANの構成

PowerShell を使用して Wake on LAN を構成するには：

1. Remote PC Access マシンカタログがまだない場合は、作成します。
2. Wake on LAN ホスト接続がまだない場合は、作成します。
3. Wake on LAN ホスト接続の一意の識別子を取得します。

4. Wake on LAN ホスト接続をマシンカタログに関連付けます。

Wake on LAN ホスト接続を作成するには：

```
# Load Citrix SnapIns

Add-PSSnapIn -Name "*citrix*"



# Provide the name of the Wake on LAN host connection

[string]$connectionName = "Remote PC Access Wake on LAN"



# Create the hypervisor connection

$hypHc = New-Item -Path xdhyp:\Connections `

                -Name $connectionName `

                -HypervisorAddress "N/A" `

                -UserName "woluser" `

                -Password "wolpwd" `

                -ConnectionType Custom `

                -PluginId VdaWOLMachineManagerFactory `

                -CustomProperties "<CustomProperties></CustomProperties>"
`

                -Persist



$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid
```

```
# Wait for the connection to be ready before trying to use it

while (-not $bhc.IsReady)

{

    Start-Sleep -s 5

    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid

}
```

ホスト接続の準備ができたら、次のコマンドを実行してホスト接続の一意の識別子を取得します。

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"

$hypUid = $bhc.Uid
```

接続の一意の識別子を取得したら、次のコマンドを実行して、その接続をRemote PC Access マシンカタログに関連付けます。

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog
-RemotePCHypervisorConnectionUid $hypUid
```

設計上の考慮事項

Remote PC Access で Wake on LAN を使用する予定がある場合は、次の点を考慮してください。

- 複数のマシンカタログで同じ Wake on LAN ホスト接続を使用できます。
- あるPCが別のPCを起動するには、両方のPCが同じサブネットにあり、同じWake on LANホスト接続を使用している必要があります。PCが同じマシンカタログにあるか、異なるマシンカタログにあるかは関係ありません。
- ホスト接続は特定のゾーンに割り当てられます。展開に複数のゾーンが含まれている場合は、各ゾーンにWake on LANホスト接続が必要です。これはマシンカタログにも当てはまります。
- マジックパケットは、グローバルブロードキャストアドレス255.255.255.255を使用してブロードキャストされます。このアドレスがブロックされていないことを確認してください。

- そのサブネット内のマシンを起動できるようにするには、Wake on LAN接続ごとに、サブネット内で少なくとも1台のPCがオンになっている必要があります。

運用上の考慮事項

「Wake on LAN」機能を使用する際の考慮事項は次のとおりです。

- 統合されたWake on LAN機能を使用してPCを起動するには、VDAが少なくとも一度は登録されている必要があります。
- Wake on LANはPCの起動にのみ使用できます。再起動やシャットダウンなどの他の電源操作はサポートしていません。
- Wake on LAN接続が作成されると、Web Studioに表示されます。ただし、オンプレミスのCitrix Virtual Apps and Desktopsを使用している場合、Web Studio内でそのプロパティを編集することはサポートされていません。
- マジックパケットは次の2つの方法のいずれかで送信されます。

  a. ユーザーがPCへのセッションを起動しようとし、VDAが未登録の場合

  b. 管理者がWeb StudioまたはPowerShellから手動で電源オンコマンドを送信した場合

- デリバリーコントローラーはPCの電源状態を認識しないため、Web Studioでは電源状態の下に**サポートされていません**と表示されます。デリバリーコントローラーは、VDAの登録状態を使用してPCがオンかオフかを判断します。

Wake on LAN – SCCM統合

SCCM統合Wake on LANは、オンプレミスのCitrix Virtual Apps and Desktopsでのみ利用可能な、Remote PC Access用の代替Wake on LANオプションです。

システム要件

SCCM統合Wake on LAN機能を使用するためのシステム要件は次のとおりです。

- Citrix Virtual Apps and Desktops 1912 以降
- 物理PC：
  - VDAバージョン1912以降
  - Windows 10。サポートの詳細については、VDAシステム要件を参照してください。
  - BIOS/UEFIでWake on LANが有効になっていること
  - Windows構成内のネットワークアダプターのプロパティでWake on LANが有効になっていること

- System Center Configuration Manager (SCCM) 2012 R2 以降

SCCM 統合型 Wake on LAN の構成

以下の前提条件を完了してください。

1. 組織内で SCCM 2012 R2、2016、または 2019 を構成します。次に、すべての Remote PC Access マシンに SCCM クライアントを展開し、スケジュールされた SCCM インベントリサイクルが実行されるのを待つか、必要に応じて手動で強制実行します。
2. Wake Proxy のサポートについては、SCCM でオプションを有効にします。Remote PC Access Wake on LAN 機能を使用する PC を含む組織内の各サブネットについて、3 台以上のマシンがセンチネルマシンとして機能できることを確認してください。
3. マジックパケットのサポートについては、サブネット指向ブロードキャストまたはユニキャストのいずれかを使用してマジックパケットを送信できるように、ネットワークルーターとファイアウォールを構成します。
4. 各PCのBIOS/UEFI設定でWake on LANを構成します。
5. まだVDAを展開していない場合は、物理PCにVDAを展開します。

前提条件に対処した後、Delivery Controller が SCCM と通信できるように、次の手順を完了します。

1. SCCMのホスト接続を作成します。詳細については、接続とリソースを参照してください。
    - 接続の種類として**Microsoft Configuration Manager Wake on LAN**を選択します。
    - 入力された資格情報には、スコープ内のコレクションへのアクセス権があり、**Remote Tools Operator**ロールを持っている必要があります。
2. Web Studioで接続を選択し、**接続の編集**を選択して、**詳細設定**をクリックします。
3. Wake on LANの処理に適したオプションを選択します。
    - Wake-upプロキシを使用している場合は、最初のオプションである**Microsoft System Center Configuration Manager Wake-upプロキシ**を選択します。
    - マジックパケットを使用している場合は、2番目のオプションである**Delivery Controllerによって送信されるWake on LANパケット**を選択します。
        - 適切な送信方法（**サブネット指向ブロードキャスト**または**ユニキャスト**）を選択します。

ホスト接続を作成したら、その接続をRemote PC Accessカタログに関連付けます。

- 新しいRemote PC Accessカタログを作成する場合は、カタログ作成ウィザードの**オペレーティングシステム**ページで、カタログの種類として**Remote PC Access**を選択し、ドロップダウンリストから適切な接続を選択します。
- 既存のRemote PC AccessカタログにWake on LANを追加するには：

  a. Web Studioの**マシンカタログ**ノードに移動し、マシンカタログを選択して、**マシンカタログの編集**を選択します。

  b. **電源管理**タブを選択し、マシンカタログの電源管理を有効にするには**はい**を選択します。

  c. ドロップダウンリストから適切な接続を選択し、**OK**をクリックします。

トラブルシューティング

モニターのブランキングが機能しない

アクティブなHDXセッション中にWindows PCのローカルモニターがブランクにならない場合（ローカルモニターにセッションで発生している内容が表示される場合）、GPUベンダーのドライバーに問題がある可能性があります。この問題を解決するには、次のレジストリ値を設定して、Citrix Indirect Displayドライバー（IDD）にグラフィックカードのベンダードライバーよりも高い優先順位を付与します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- 名前: CitrixIDD
- 種類: DWORD
- データ: 3

ディスプレイアダプターの優先順位とモニターの作成に関する詳細については、Knowledge Centerの記事CTX237608を参照してください。

セッション管理通知が有効になっているマシンで Ctrl+Alt+Del を選択すると、セッションが切断されます

SasNotification レジストリ値によって制御されるセッション管理通知は、VDA で Remote PC Access モードが有効になっている場合にのみ機能します。物理 PC で Hyper-V の役割または仮想化ベースのセキュリティ機能が有効になっている場合、その PC は仮想マシンとして報告されます。VDA が仮想マシン上で実行されていることを検出すると、Remote PC Access モードが自動的に無効になります。Remote PC Access モードを有効にするには、次のレジストリ値を追加します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: ForceEnableRemotePC
- 種類: DWORD
- データ: 1

設定を有効にするには、PC を再起動します。

診断情報

Remote PC Access に関する診断情報は、Windows アプリケーションイベントログに書き込まれます。情報メッセージはスロットリングされません。エラーメッセージは、重複するメッセージを破棄することでスロットリングされます。

- 3300（情報）: マシンがカタログに追加されました
- 3301（情報）: マシンがデリバリーグループに追加されました
- 3302（情報）: マシンがユーザーに割り当てられました
- 3303 (エラー): 例外

電源管理

Remote PC Access の電源管理が有効になっている場合、サブネット指向ブロードキャストでは、Controller とは異なるサブネットにあるマシンを起動できない場合があります。サブネット指向ブロードキャストを使用してサブネット間で電源管理が必要で、AMT サポートが利用できない場合は、Wake-up プロキシまたはユニキャスト方式を試してください。これらの設定が電源管理接続の高度なプロパティで有効になっていることを確認してください。

アクティブなリモートセッションはローカルのタッチスクリーン入力を記録します

VDA が Remote PC Access モードを有効にすると、アクティブなセッション中にマシンはローカルのタッチスクリーン入力を無視します。物理 PC に Hyper-V ロールまたは仮想化ベースのセキュリティ機能が有効になっている場合、PC は仮想マシンとして報告されます。VDA が仮想マシン上で実行されていることを検出すると、Remote PC Access モードを自動的に無効にします。Remote PC Access モードを有効にするには、次のレジストリ設定を追加します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: ForceEnableRemotePC
- 種類: DWORD
- データ: 1

設定を有効にするには、PC を再起動してください。

その他のリソース

以下は Remote PC Access に関するその他のリソースです。

- ソリューション設計ガイダンス: Remote PC Access Design Decisions.
- Remote PC Access アーキテクチャの例: Citrix Remote PC Access Solution のリファレンスアーキテクチャ。

スタンドアロンCitrix Secure Ticketing Authority (STA) サービス (プレビュー)

スタンドアロンCitrix Secure Ticketing Authority (STA) サービスを使用すると、環境内のSTAチケットの配信をより詳細に制御できます。

スタンドアロン Citrix STA サービスは、デフォルトでリソースロケーション内のすべてのCloud Connectorにインストールされます。このサービスは、STAチケッティングをCitrix Cloud™チケッティングサービスからCloud Connectorに移行させ、通常モードとLHCモードの両方でチケッティング操作を標準化します。スタンドアロンSTAサービスは、クラウドサービスへの依存を軽減し、LHCモードに入ったときのソリューションのパフォーマンスを向上させます。

スタンドアロンCitrix STAサービスのシナリオ

この表は、スタンドアロンSTAサービスが機能するさまざまなシナリオを示しています。

STOREFRONT™	ゲートウェイ	環境	通常モードでのチケット発行サービス	LHCモードでのチケット発行サービス
シトリックス ワークスペース	オンプレミス Citrix Gateway	クラウド	スタンドアロンSTA サービス	スタンドアロンSTA サービス。STAサービスが利用できない場合のサービス継続性の機能の詳細については、サービス継続性を参照してください。

STOREFRONT™	ゲートウェイ	環境	通常モードでのチケット発行サービス	LHCモードでのチケット発行サービス
シトリックス ワークスペース	オンプレミス Citrix Gateway	オンプレミス	スタンドアロンSTAサービス 注: レジストリキー HKEY_LOCAL_MACHINE\Software\Citrix\XaXdCloudProxyPersist\StandaloneStaServiceForced を 1 に設定します。	スタンドアロンSTAサービス。STAサービスが利用できない場合のサービス継続性の機能の詳細については、サービス継続性を参照してください。
オンプレミス StoreFront	Citrix Gateway サービス	クラウド	スタンドアロンSTAサービス	スタンドアロンSTAサービス
オンプレミス StoreFront	オンプレミス Citrix Gateway	クラウド	スタンドアロン STA サービス	スタンドアロン STA サービス
オンプレミス StoreFront	Citrix Gateway サービス	オンプレミス	スタンドアロン STA サービス	スタンドアロン STA サービス

システム要件

以下のシステム要件が必要です。

- オンプレミス StoreFront: バージョン 2311 以降
- Delivery Controller™: バージョン 2503 以降

オンプレミス環境で必要な構成

オンプレミス環境でCitrix Gatewayサービスとオンプレミスstorefrontを使用しており、スタンドアロンSTAサービスを活用したい場合は、Cloud Connectorをインストールする必要があります。

ステップ1：Citrix Cloudでリソースの場所を作成する

1. Citrix Cloudにオンボードします。詳細については、「Citrix Cloudアカウントを作成する」および「Citrix Cloudに接続する」を参照してください。
2. Citrix Cloudで、Cloud Connectorをインストールし、それらをリソースの場所に関連付けます。詳細については、「Cloud Connectorのインストール」を参照してください。

ステップ2：オンプレミスのDelivery Controllerでゾーンを作成する

オンプレミスのDelivery Controllerで、新しいゾーンを作成し、Citrix Cloudで作成したリソースの場所にマッピングします。

`ZoneMapping.yml`ファイルを手動で更新して、オンプレミスゾーンとクラウドのリソースの場所の正しいマッピングを反映させます。

`ZoneMapping.yml`ファイルは`%HOMEPATH%\Documents\Citrix\AutoConfig`にあります。`.yml`ファイルの内容は、ゾーン名をキー、リソースの場所名を値とする辞書です。

たとえば、「Zone-1」というプライマリゾーンと「Zone-2」というセカンダリゾーンを持つオンプレミスのCitrix Virtual Apps and Desktopsサイトが、「Cloud-RL-1」と「Cloud-RL-2」という2つの新しく作成されたクラウドのリソースの場所を持つCitrix DaaS展開にマッピングされます。この場合、`ZoneMapping.yml`は次のように構成されます。

ゾーン-1: Cloud-RL-1

ゾーン-2: Cloud-RL-2

> **注:**
>
> コロンとリソースの場所名の間にスペースを追加します。ゾーン名またはリソースの場所名にスペースを使用する場合は、名前を引用符で囲みます。

StoreFrontの構成

StoreFrontを構成して、Cloud ConnectorのFQDNをSTAサーバーとして使用します。

1. StoreFront管理コンソールを開きます。

2. **Stores > Manage Citrix Gateways**に移動し、**Add**をクリックします。
3. ルーティングゲートウェイの**表示名**を入力します。
4. ゲートウェイの種類として**Citrix Gateway Service**を選択します。
5. **次へ**をクリックし、**Cloud Connectors**タブに移動します。
6. **追加**をクリックして、クラウドコネクタのURLを追加します。
7. 必要に応じて、**複数のサーバーの負荷を分散**および**セッションの信頼性を有効にする**を有効にします。
8. **OK**をクリックします。

コンテンツの公開

> **注:**
>
> Citrix Virtual Apps and Desktops™ の展開は、Web Studio (Web ベース) と Citrix Studio (Windows ベース) の 2 つの管理コンソールを使用して管理できます。この記事では Web Studio のみを取り上げます。Citrix Studio については、Citrix Virtual Apps and Desktops 7 2212 以前の同等の記事を参照してください。

> Microsoft Word ドキュメントや Web リンクなどのリソースへの URL または UNC パスであるアプリケーションを公開できます。この機能は公開コンテンツとして知られています。コンテンツを公開する機能により、ユーザーにコンテンツを配信する方法に柔軟性が加わります。既存のアクセス制御とアプリケーション管理の恩恵を受けることができます。また、コンテンツを開くためにローカルアプリケーションを使用するか、公開アプリケーションを使用するかを指定することもできます。

公開されたコンテンツは、StoreFront™ および Citrix Workspace™ アプリの他のアプリケーションと同様に表示されます。ユーザーはアプリケーションにアクセスするのと同じ方法でアクセスします。クライアントでは、リソースは通常どおり開きます。

- ローカルにインストールされたアプリケーションが適切な場合、そのアプリケーションが起動されてリソースが開かれます。
- ファイルの種類に関連付けが定義されている場合、公開されたアプリケーションが起動されてリソースが開かれます。

PowerShell SDK を使用してコンテンツを公開します。Web Studio を使用してコンテンツを公開することはできません。ただし、公開後に Web Studio を使用してアプリケーションプロパティを編集することはできます。

構成の概要と準備

コンテンツの公開では、次の主要なプロパティを持つ `New-BrokerApplication` コマンドレットを使用します。(すべてのコマンドレットプロパティの説明については、コマンドレットのヘルプを参照してください。)

```
New-BrokerApplication –ApplicationType PublishedContent
-CommandLineExecutable location -Name app-name -DesktopGroup delivery-
group-name
```

`ApplicationType` プロパティは `PublishedContent` である必要があります。

`CommandLineExecutable` プロパティは、公開コンテンツの場所を指定します。255 文字の制限付きで、次の形式がサポートされています。

- HTML Web サイトアドレス (例: `<http://www.citrix.com>`)
- Web サーバー上のドキュメントファイル (例: `https://www.citrix.com/press/pressrelease.doc`)
- FTP サーバー上のディレクトリ (例: `ftp://ftp.citrix.com/code`)
- FTPサーバー上のドキュメントファイル（例: `ftp://ftp.citrix.com/code/Readme.txt`>）
- UNCディレクトリパス（例: `file://myServer/myShare or \\\\myServer\\myShare`）
- UNCファイルパス（例: `file://myServer/myShare/myFile.asf` または `\\myServer\myShare\myFile.asf`）

正しいSDKがあることを確認してください。

- Citrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）の展開の場合、Citrix Virtual Apps and Desktops Remote PowerShell SDKをダウンロードしてインストールします。
- オンプレミスのCitrix Virtual Apps and Desktops展開の場合、Delivery Controllerとともにインストールされているの PowerShell SDKを使用します。公開コンテンツアプリケーションを追加するには、最低バージョン7.11のDelivery Controllerが必要です。

次の手順では例を使用します。例では次のようになります。

- マシンカタログが作成されています。
- `PublishedContentApps` という名前のデリバリーグループが作成されています。このグループは、カタログからマルチセッションOSマシンを使用します。WordPadアプリケーションがグループに追加されています。
- デリバリーグループ名、`CommandLineExecutable` の場所、およびアプリケーション名が割り当てられます。

はじめに

PowerShell SDKを含むマシンで、PowerShellを開きます。

次のコマンドレットは、適切なPowerShell SDKスナップインを追加し、返されたデリバリーグループレコードを割り当てます。

`Add-PsSnapin Citrix* $dg = Get-BrokerDesktopGroup –Name PublishedContentApps`

Citrix DaaSを使用している場合は、Citrix Cloud™の資格情報を入力して認証します。顧客が複数いる場合は、いずれかを選択します。

URLを公開する

場所とアプリケーション名を割り当てた後、次のコマンドレットは、Citrixのホームページをアプリケーションとして公開します。

```
$citrixUrl = "https://www.citrix.com/"

$appName = "Citrix Home Page"



New-BrokerApplication –ApplicationType PublishedContent –
CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.Uid
```

成功を確認する:

- StoreFrontを開き、PublishedContentAppsデリバリーグループ内のアプリケーションにアクセスできるユーザーとしてログオンします。表示には、デフォルトのアイコンを持つ新しく作成されたアプリケーションが含まれます。アイコンのカスタマイズについては、`<https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/>` を参照してください。

- **Citrix Home Page**アプリケーションをクリックします。URLは、ローカルで実行されているデフォルトブラウザの新しいタブで起動します。

UNCパスにあるリソースを公開する

この例では、管理者は`PublishedResources`という名前の共有をすでに作成しています。場所とアプリケーション名を割り当てた後、以下のコマンドレットはその共有内のRTFファイルとDOCXファイルをリソースとして公開します。

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\\PublishedResources\\PublishedRTF.rtf"

$rtfAppName = "PublishedRTF"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $rtfUNC -Name $rtfAppName

-DesktopGroup $dg.Uid



$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx"

$docxAppName = "PublishedDOCX"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $docxUNC -Name $docxAppName

-DesktopGroup $dg.Uid
```

成功を確認する:

- StoreFrontウィンドウを更新して、新しく公開されたドキュメントを表示します。
- **PublishedRTF**および**PublishedDOCX**アプリケーションをクリックします。各ドキュメントは、ローカルで実行されているWordPadで開きます。

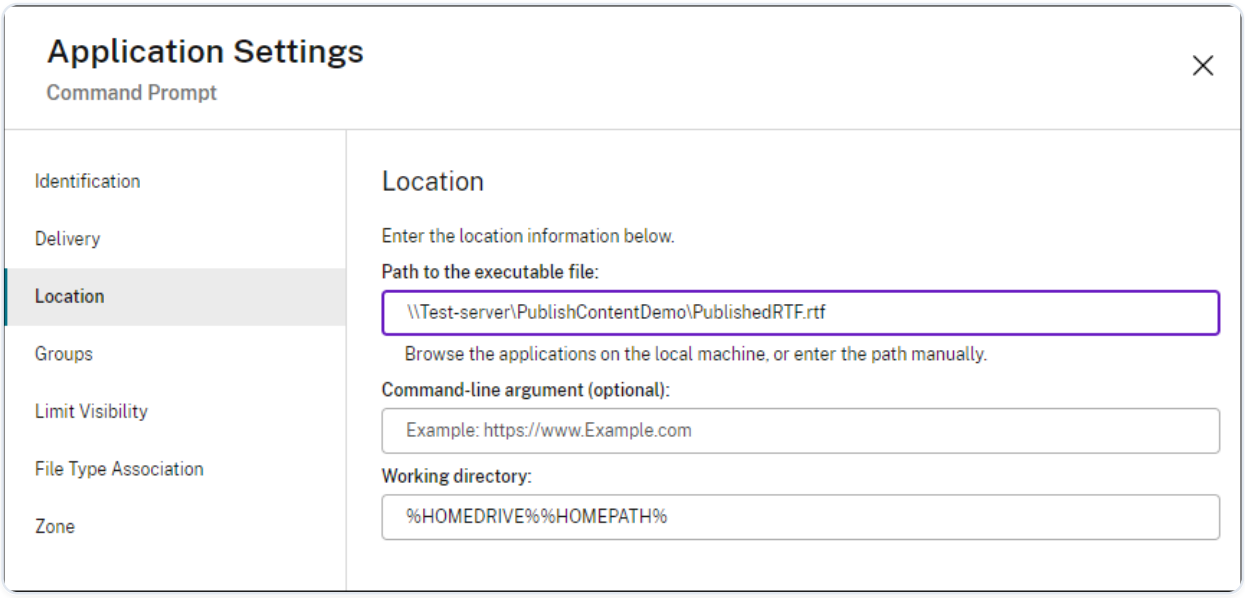
PublishedContentアプリケーションの表示と編集

公開されたコンテンツは、他のアプリケーションタイプに使用するのと同じ方法で管理します。

`PublishedContent`アプリケーションを表示および編集するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**アプリケーション**を選択します。
2. **アプリケーション**タブで、PublishedContentアプリケーションを選択し、**プロパティ**を選択します。

   アプリケーションのプロパティ（ユーザーの可視性、グループの関連付け、ショートカットなど）は公開されたコンテンツに適用されます。ただし、**場所**ページでは、コマンドライン引数または作業ディレクトリのプロパティを変更することはできません。
3. リソースを変更するには、そのページの**実行可能ファイルへのパス**フィールドを変更します。

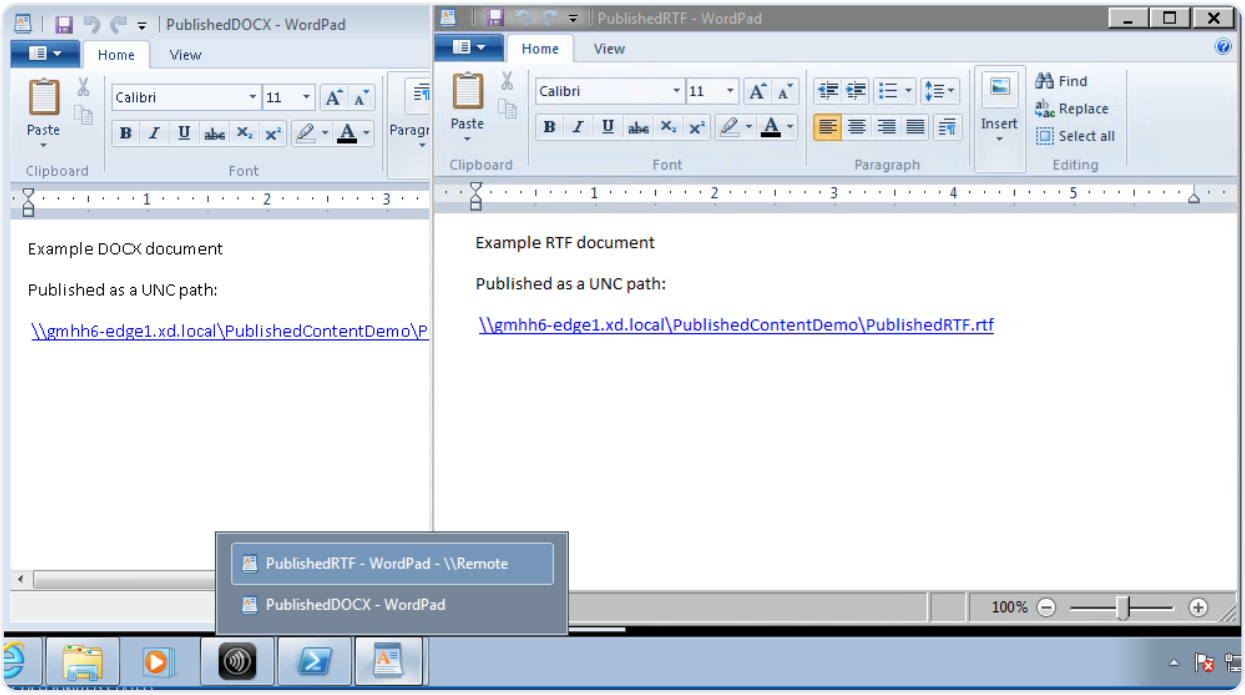


4. 公開アプリケーションを使用して`PublishedContent`アプリケーション（ローカルアプリケーションではなく）を開くには、次の手順に従います。

   この例では、公開されたWordPadアプリケーションが編集され、.rtfファイル用のファイルタイプ関連付けが作成されます。

   a. デリバリーグループのメンテナンスモードをオンにします。
   b. **ファイルタイプ関連付け**プロパティを編集します。
   c. 完了したら、メンテナンスモードをオフにします。
   d. StoreFrontを更新してファイルタイプ関連付けの変更を読み込み、**PublishedRTF**および**PublishedDOCX**アプリケーションをクリックします。違いに注目してください。

PublishedDOCXは引き続きローカルのWordPadで開きます。しかし、**PublishedRTF**はファイルタイプ関連付けにより、公開されたWordPadで開くようになりました。



詳細情報

- マシンカタログを作成する
- デリバリーグループを作成する
- アプリケーションプロパティを変更する

サーバー VDI

Server VDI (Virtual Desktop Infrastructure) 機能を使用して、単一ユーザー向けにサーバーオペレーティングシステムからデスクトップを配信します。

- 企業管理者は、サーバーオペレーティングシステムをVDIデスクトップとして提供できます。これは、エンジニアやデザイナーなどのユーザーにとって価値があります。
- サービスプロバイダーは、クラウドからデスクトップを提供できます。これらのデスクトップは、Microsoft Services Provider License Agreement (SPLA) に準拠しています。

サポート:

- Citrix Virtual Apps and Desktops™ および Citrix DaaS (旧称 Citrix Virtual Apps and Desktops service) の展開では、Server VDI は Windows Server 2022 および Windows Server 2019 でサポートされています。

- すべての Server VDI 展開は、ユーザーパーソナライゼーションレイヤーテクノロジーをサポートします。
- スキャナーなどの TWAIN デバイスで Server VDI を機能させるには、Windows Server デスクトップエクスペリエンス機能をインストールする必要があります。
- 次の機能は Server VDI では使用できません。
  - ホスト型アプリケーション
  - ローカルアプリアクセス
  - 直接 (非ブローカー) デスクトップ接続
  - リモートPCアクセス

Server VDI のインストールと構成

1. Windows サーバーをインストール用に準備します。
   - Windows Server Manager を使用して、リモートデスクトップサービス役割サービスがインストールされていないことを確認します。以前にインストールされていた場合は、削除してください。これらの役割サービスがインストールされていると、VDA のインストールは失敗します。
   - 「**各ユーザーを単一セッションに制限する**」プロパティが有効になっていることを確認します。Windows サーバーで、ターミナルサーバー設定のレジストリを編集します。

     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server`

     `DWORD fSingleSessionPerUser = 1`
2. Citrix Virtual Apps and Desktops インストーラーのコマンドラインインターフェイスを使用して、サポートされているサーバーまたはサーバーマスターイメージに VDA をインストールし、`/servervdi` オプションを指定します。（デフォルトでは、インストーラーのグラフィカルインターフェイスは、サーバーオペレーティングシステム上の Windows シングルセッション OS VDA をブロックします。コマンドラインを使用すると、この動作が上書きされます。）次のいずれかのコマンドを使用します。
   - Citrix Virtual Apps and Desktops展開の場合:
     - `XenDesktopVdaSetup.exe /servervdi`
     - `VDAWorkstationSetup.exe /servervdi`
   - Citrix DaaS™展開の場合:

- `VDAWorkstationSetup.exe /servervdi`

その他のオプション:

- Delivery Controller または Cloud Connector を指定するには、`/controllers` を使用します。
- ファイアウォールを手動で構成する場合を除き、ファイアウォールでポートを開くには `/enable_hdx_ports` を使用します。
- イメージに VDA をインストールし、そのイメージから MCS を使用してサーバー VM を作成する場合は、`/mastermcsimage` (または `/masterimage`) を使用します。
- すべてのオプションの詳細については、「コマンドラインを使用したインストール」を参照してください。

3. Server VDI 用のマシンカタログを作成します。カタログ作成ウィザードで、次のようにします。

   - **オペレーティングシステム**ページで、**シングルセッションOS**を選択します。
   - **概要**ページで、Server VDI であることを明確に識別できるマシンカタログ名と管理者向けの記述を指定します。これは、カタログがServer VDIをサポートしていることをStudioで示す唯一のインジケーターです。

   Studioで検索を使用すると、VDAがマルチセッションマシンにインストールされている場合でも、Server VDIカタログは**シングルセッションOSマシン**タブに表示されます。

4. デリバリーグループを作成し、作成したServer VDIカタログを選択します。

VDAのインストール中にDelivery ControllerまたはCloud Connectorを指定しなかった場合は、後で指定することを忘れないでください。詳細については、「VDA登録」を参照してください。

ユーザーパーソナライゼーションレイヤー

> **注:**
>
> Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioの詳細については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> Citrix Virtual Apps and Desktopsのユーザーパーソナライゼーションレイヤー機能は、非永続マシンカタログの機能を拡張し、セッション間でユーザーのデータとローカルにインストールされたアプリケーションを保持します。基盤となるCitrix App Layeringテクノロジーを搭載したユーザーパーソナライゼーションレイヤー機能は、非永続マシンカタログでCitrix ProvisioningおよびMachine Creation Services™ (MCS) をサポートします。

マスターイメージ内のVirtual Delivery Agentとともに、ユーザーパーソナライゼーションレイヤーコンポーネントをインストールします。VHDファイルは、ユーザーがローカルにインストールしたアプリケーションを保存します。イメージにマウントされたVHDは、ユーザー自身の仮想ハードドライブとして機能します。

重要:

> Citrix Virtual Apps and Desktopsでユーザーパーソナライゼーションレイヤーを展開するか、イメージテンプレートで有効になっているApp Layeringユーザーレイヤーを展開できますが、両方を展開することはできません。App Layering内のレイヤーにユーザーパーソナライゼーションレイヤー機能をインストールしないでください。

> この機能はPersonal vDisk (PvD) に代わるものであり、非永続（プール型）デスクトップ環境のユーザーに永続的なワークスペースエクスペリエンスも提供します。

ユーザーパーソナライゼーションレイヤー機能を展開するには、記事に詳述されている手順を使用してインストールおよび構成します。

アプリケーションのサポート

以下の例外を除き、ユーザーがデスクトップにローカルにインストールするすべてのアプリケーションは、ユーザーパーソナライゼーションレイヤーでサポートされます。

例外

以下のアプリケーションは例外であり、ユーザーパーソナライゼーションレイヤーではサポートされません。

- MS OfficeやVisual Studioなどのエンタープライズアプリケーション。
- ネットワークスタックまたはハードウェアを変更するアプリケーション。例: VPNクライアント。
- ブートレベルドライバーを持つアプリケーション。例：ウイルススキャナー。

- ドライバー ストアを使用するドライバーを持つアプリケーション。例: プリンタードライバー。

> **注:**
>
> Windowsグループポリシーオブジェクト (GPO) を使用してプリンターを利用可能にできます。

サポートされていないアプリケーションをローカルにインストールすることをユーザーに*許可しないでください*。代わりに、これらのアプリケーションはマスターイメージに直接インストールしてください。

ローカルユーザーまたは管理者アカウントを必要とするアプリケーション

ユーザーがアプリケーションをローカルにインストールすると、そのアプリはユーザーレイヤーに格納されます。その後、ユーザーがローカルユーザーまたはグループを追加または編集しても、その変更はセッションを超えて保持されません。

> **重要:**
>
> 必要なローカルユーザーまたはグループは、マスターイメージに追加してください。

要件

ユーザーパーソナライゼーションレイヤー機能には、以下のコンポーネントが必要です。

- シトリックス バーチャルアプリ アンド デスクトップ 7 1909 以降
- Virtual Delivery Agent (VDA) バージョン1912以降
- Citrix Provisioning™ バージョン1909以降
- Windowsファイル共有 (SMB)、またはオンプレミスAD認証が有効なAzure Files

ユーザーパーソナライゼーションレイヤー機能は、OSがシングルセッションとして展開されている場合、以下のWindowsバージョンに展開できます。サポートは、シングルセッション上の単一ユーザーに限定されます。

- ウィンドウズ 11 エンタープライズ x64
- Windows 10 Enterprise x64、バージョン1607以降

- ウィンドウズ サーバー 2019 (Azure Files 対応)
- ウィンドウズ サーバー 2022 (Azure Files 対応)

Citrix Virtual Apps and Desktops 7の場合、ユーザーパーソナライゼーションレイヤーでのAzure Filesの使用は、Windows Server 2022、Windows Server 2019、およびWindows 10クライアントでサポートされています。

> **注:**

> サーバーOSを使用している場合、Server VDIのみがサポートされます。展開の詳細については、Server VDIの記事を参照してください。

> ユーザーパーソナライゼーションレイヤーは、マシンごとに一度に1人のユーザーのみをサポートし、その後、ディスクをリセットするためにマシンを再起動する必要があります。ユーザーパーソナライゼーションレイヤーは、マルチセッションサーバーオペレーティングシステムでは使用できず、シングルセッションサーバーシステムでのみ使用できます。ユーザーパーソナライゼーションレイヤーは、非永続デスクトップのみでサポートされています。

> ユーザーパーソナライゼーションレイヤー機能がインストールされている場合は、アンインストールします。最新リリースをインストールする前に、マスターイメージを再起動します。

ファイル共有を設定する

ユーザーパーソナライゼーションレイヤー機能には、Windows Server Message Block (SMB) ストレージが必要です。Windowsファイル共有を作成するには、使用しているWindowsオペレーティングシステムの通常の手順に従ってください。

Azureベースのカタログでは Azure Filesを使用する方法の詳細については、「ユーザーパーソナライゼーションレイヤー用にAzure Filesストレージを設定する」を参照してください。

推奨事項

ユーザーパーソナライゼーションレイヤーの展開を成功させるには、このセクションの推奨事項に従ってください。

マイクロソフト システムセンター コンフィギュレーションマネージャー (SCCM)

ユーザーパーソナライゼーションレイヤー機能でSCCMを使用している場合は、VDI環境でイメージを準備するためのMicrosoftのガイドラインに従ってください。詳細については、このMicrosoft TechNet記事を参照してください。

ユーザーレイヤーのサイズ

ユーザーレイヤーは、ディスク上のスペースが使用されるにつれて拡張するシンプロビジョニングディスクです。ユーザーレイヤーに許可されるデフォルトサイズは10 GBで、これは推奨される最小値です。

> **注:**
>
> インストール中に値がゼロ (0) に設定されている場合、デフォルトのユーザーレイヤーサイズは10 GBに設定されます。

> ユーザーレイヤーのサイズを変更したい場合は、**User Layer Size** ポリシーに別の値を入力できます。「**オプション: User Layer Size in GBの横にあるをクリックします。**」の下にある「**ステップ5: デリバリーグループのカスタムポリシーを作成する**」を参照してください。

ユーザーレイヤーのサイズを上書きするためのツール (オプション)

Windowsツールを使用してユーザーレイヤーファイル共有にクォータを定義することで、ユーザーレイヤーサイズを上書きできます。

以下のMicrosoftクォータツールのいずれかを使用して、**Users**という名前のユーザーレイヤーディレクトリにハードクォータを設定します。

- ファイルサーバーリソースマネージャー (FSRM)
- クォータマネージャー

> **注:**
>
> クォータを増やすと、新しいユーザーレイヤーに影響し、既存のユーザーレイヤーが拡張されます。クォータを減らすと、新しいユーザーレイヤーのみに影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

ユーザーパーソナライゼーションレイヤーを展開する

ユーザーパーソナライゼーション機能を展開する際、Web Studio内でポリシーを定義します。その後、そのポリシーを、機能が展開されるマシンカタログにバインドされたデリバリーグループに割り当てます。

マスターイメージにユーザーパーソナライゼーションレイヤーの設定がない場合、サービスはアイドル状態のままで、オーサリングアクティビティを妨げません。

マスターイメージでポリシーを設定すると、サービスはマスターイメージ内でユーザーレイヤーを実行およびマウントしようとします。マスターイメージは予期しない動作や不安定性を示します。

ユーザーパーソナライゼーションレイヤー機能を展開するには、以下の手順をこの順序で完了します。

- ステップ1: Citrix Virtual Apps and Desktops環境の可用性を確認します。
- ステップ2: マスターイメージを準備します。
- ステップ3: マシンカタログを作成します。
- ステップ4: デリバリーグループを作成します。
- ステップ5: デリバリーグループのカスタムポリシーを作成します。

> **注:**
>
> イメージ上のWindows 10をアップグレードした後、初めてログインするのに通常よりも時間がかかります。ユーザーのレイヤーが新しいバージョンのWindows 10用に更新される必要があり、その結果、ログオン時間が増加します。

ステップ1: Citrix Virtual Apps and Desktops環境が利用可能であることを確認する

この新機能を使用するために、Citrix Virtual Apps and Desktops 環境が利用可能であることを確認してください。セットアップの詳細については、「Citrix Virtual Apps and Desktops のインストールと構成」を参照してください。

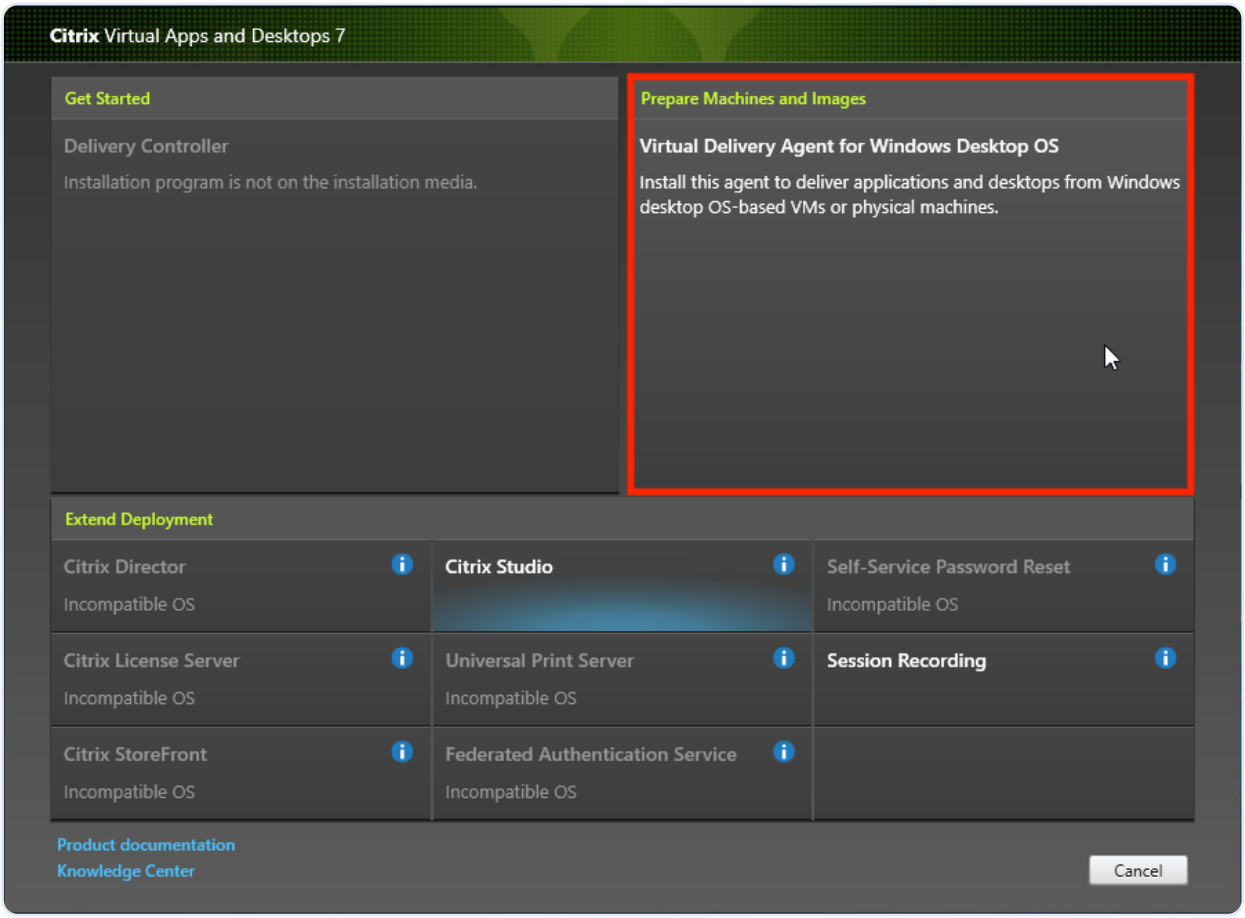
ステップ2: マスターイメージを準備する

マスターイメージを準備するには:

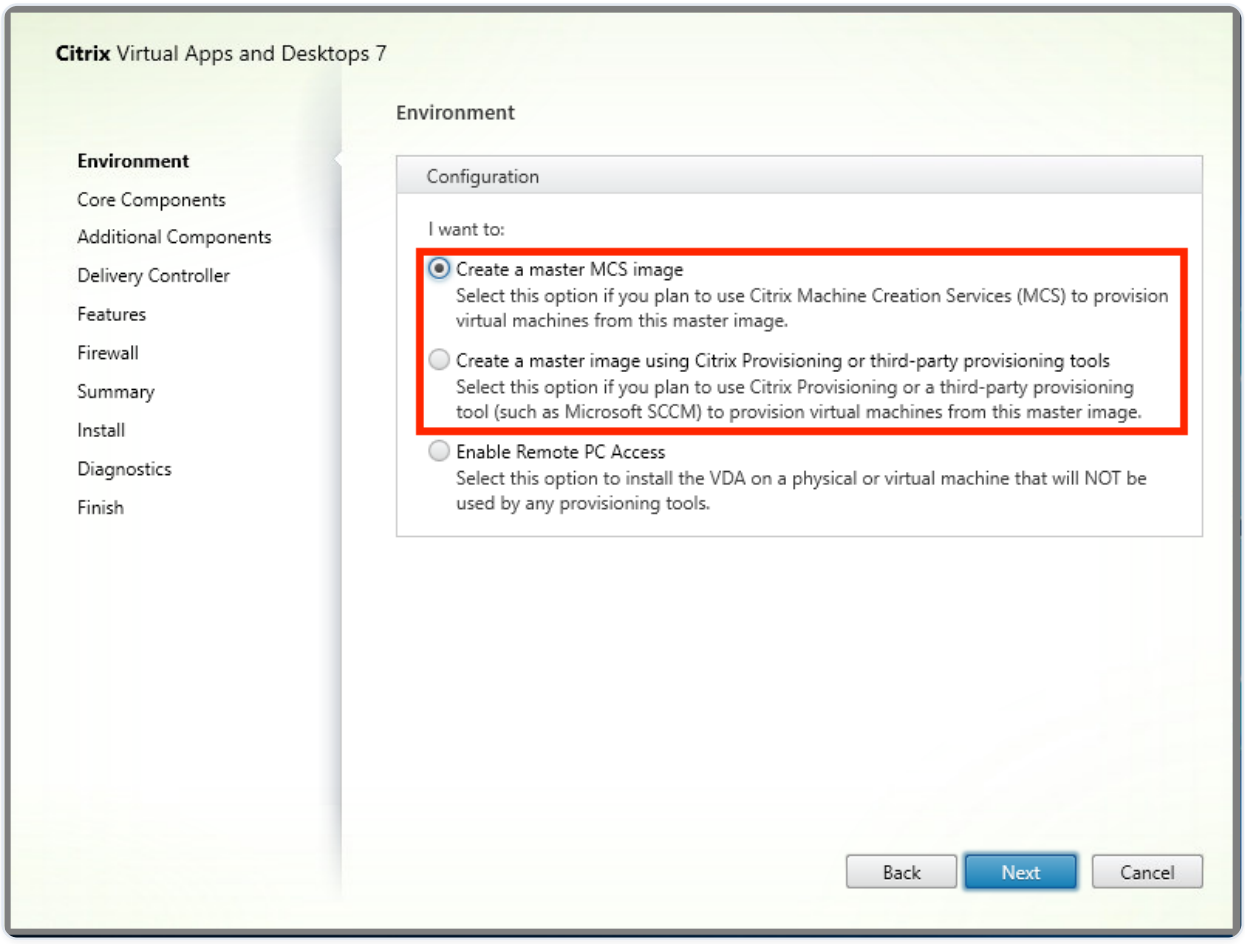
1. マスターイメージを見つけます。組織のエンタープライズアプリケーションと、ユーザーが一般的に役立つと感じるその他のアプリをインストールします。

2. Server VDIを展開する場合は、Server VDIの記事の手順に従ってください。オプションコンポーネントである**ユーザーパーソナライゼーションレイヤー**を必ず含めてください。詳細については、VDAのインストールに関するコマンドラインオプションを参照してください。
3. Windows 10 を使用している場合は、Virtual Delivery Agent (VDA) 1912 以降をインストールします。古いバージョンの VDA がすでにインストールされている場合は、まず古いバージョンをアンインストールしてください。新しいバージョンをインストールする際は、オプションコンポーネントである**Citrix User Personalization Layer**を次のように選択してインストールしてください。

   a. **Virtual Delivery Agent for Windows Desktop OS**タイルをクリックします:

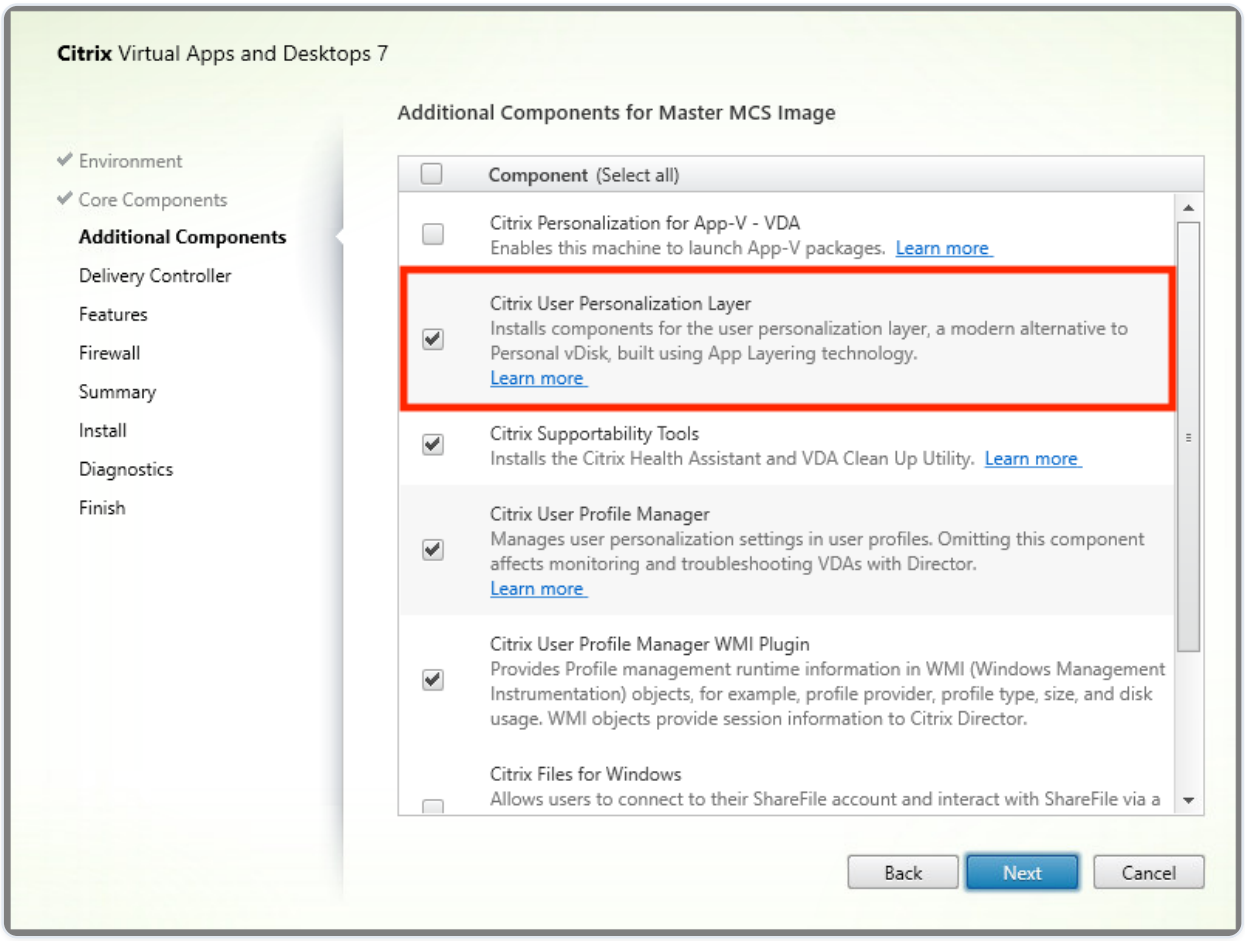


   a. **環境:「マスター MCS イメージを作成する」**または**「Citrix Provisioning またはサードパーティのプロビジョニングツールを使用してマスターイメージを作成する」**のいずれかを選択します。



a. **コアコンポーネント:** 「次へ」をクリックします。

b. **追加コンポーネント:** 「**Citrix User Personalization Layer**」をチェックします。



a. 残りのインストール画面を進み、必要に応じて VDA を構成し、「**インストール**」をクリックします。インストール中にイメージが 1 回以上再起動します。

4. **Windows Update**は無効のままにしてください。ユーザーパーソナライゼーションレイヤーインストーラーは、イメージ上のWindows Updateを無効にします。更新は無効のままにしてください。

イメージをWeb Studioにアップロードする準備ができました。

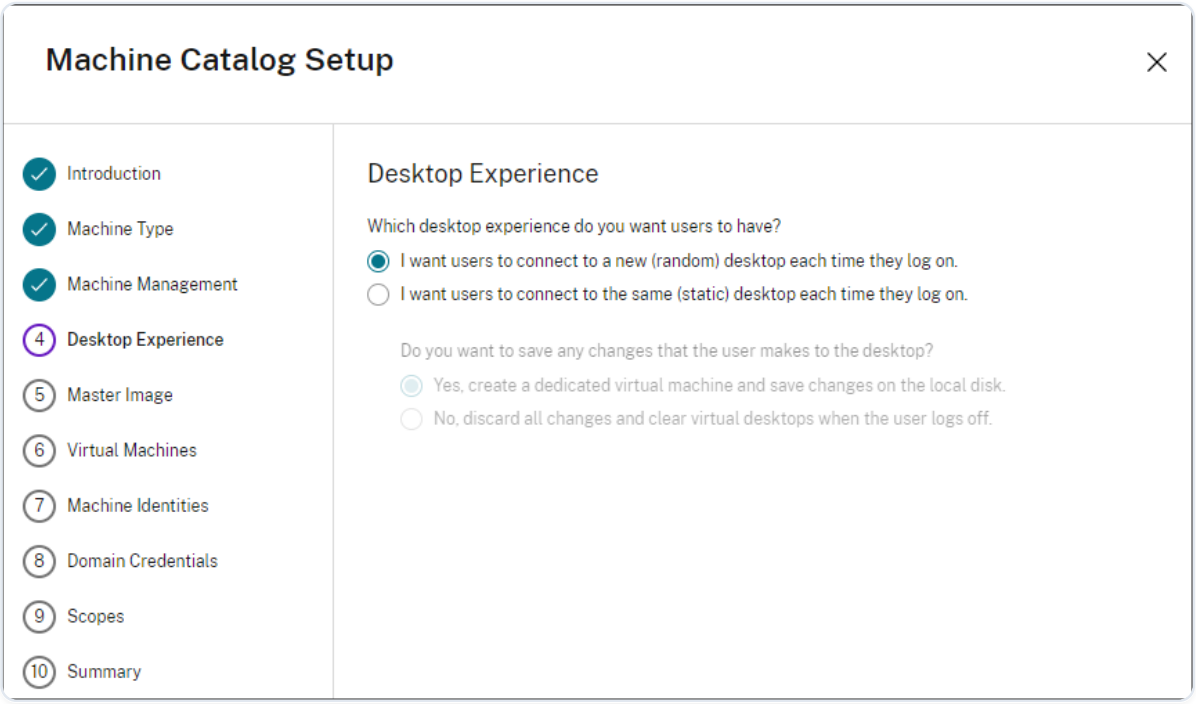
> **注:**
>
> ユーザーパーソナライゼーションレイヤー（UPL）をアップグレードするだけでよい場合は、新しいバージョンのUPLとスタンドアロンパッケージを使用してアップグレードできます。VDAをアップグレードする必要はありません。

ステップ 3: マシンカタログを作成する

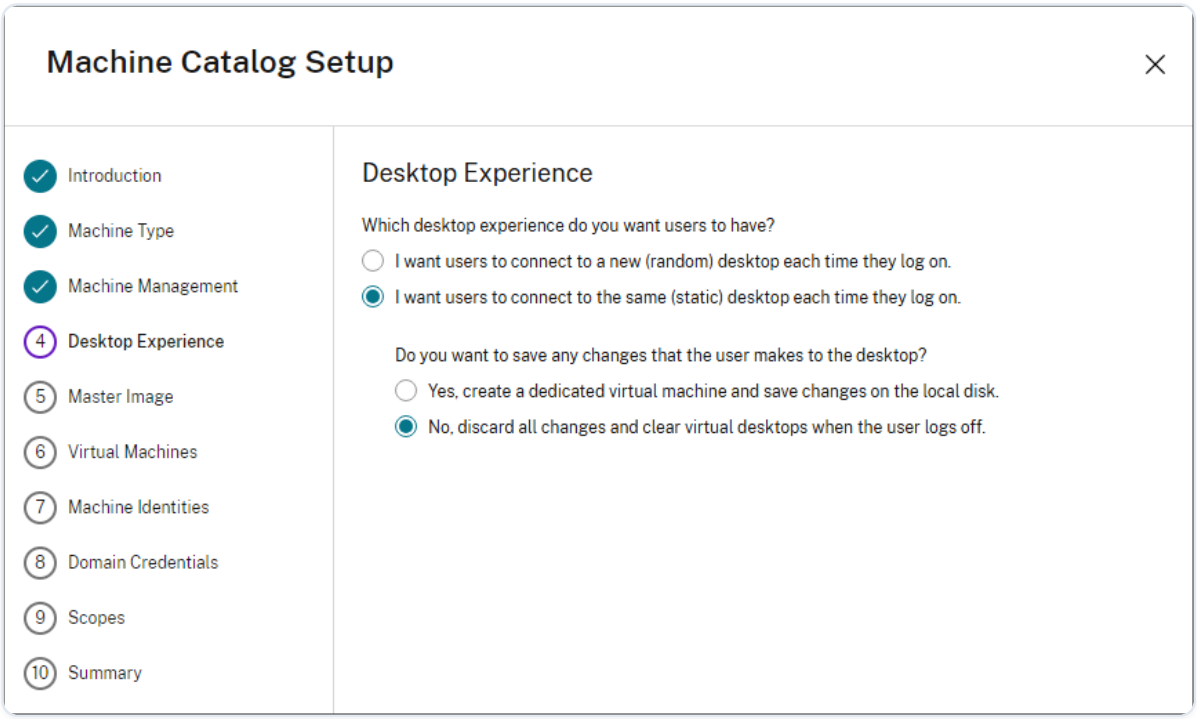
Web Studioで、マシンカタログを作成する手順に従います。カタログ作成時には、以下のオプションを使用します。

1. **オペレーティングシステム**を選択し、**シングルセッションOS**として設定します。
2. **マシン管理**を選択し、**電源管理されているマシン**として設定します。たとえば、仮想マシンやブレードPCなどです。
3. **デスクトップエクスペリエンス**を選択し、以下の例のように、**プールされたランダム**または**プールされた静的**カタログタイプとして設定します:

   - **プールされたランダム:**



   - **プールされた静的:** プールされた静的を選択した場合、次のスクリーンショットに示すように、ユーザーがログオフしたときに、すべての変更を破棄し、仮想デスクトップをクリアするようにデスクトップを構成します:



注:

ユーザーパーソナライゼーションレイヤーは、Citrix Personal vDiskを使用するように構成されている、または専用仮想マシンとして割り当てられているプールされた静的カタログをサポートしていません。

4. MCSを使用している場合は、**イメージ**と、前のセクションで作成したイメージのスナップショットを選択します。
5. 環境に合わせて必要に応じて、残りのカタログプロパティを構成します。

ステップ 4: デリバリーグループを作成する

作成したマシンカタログからのマシンを含めて、**デリバリーグループ**を作成および構成します。詳細については、デリバリーグループの作成を参照してください。

ステップ 5: デリバリーグループのカスタムポリシーを作成する

Virtual Delivery Agent内でユーザーレイヤーのマウントを有効にするには、構成パラメーターを使用して以下を指定します。

- ネットワーク上のどこでユーザーレイヤーにアクセスするか。
- ユーザーレイヤーディスクの拡張をどのくらいのサイズまで許可するか。

Web Studioでパラメーターをカスタムポリシーとして定義し、デリバリーグループに割り当てます。

1. Web Studioにサインインし、左側のペインで**ポリシー**を選択します。

   Studioでポリシーを選択(/en-us/citrix-virtual-apps-desktops/2411/media/upl-studio-select-policies.png)

2. アクションバーで を選択します。 ウィンドウが表示されます。
3. 検索フィールドに `user layer` と入力します。利用可能なポリシーのリストに、次の3つのポリシーが表示されます。

   - ユーザーレイヤーの除外
   - ユーザーレイヤーリポジトリパス
   - ユーザーレイヤーサイズ (GB)

   > **注:**
   >
   > サイズを増やすと、新しいユーザーレイヤーに影響し、既存のユーザーレイヤーが拡張されます。サイズを減らすと、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

   ユーザーレイヤーポリシーの選択(/en-us/citrix-virtual-apps-desktops/2411/media/user-layer-policies.png)

4. **ユーザーレイヤーリポジトリパス**の横にあるチェックボックスをオンにして、**編集**をクリックします。**設定の編集**ウィンドウが表示されます。
5. **値**フィールドにパスを入力し、**保存**をクリックします。

   - **パス形式:** `\\server-name-or-address\share-name\folder`
   - **パスの例:** `\\Server\Share\UPLUsers`
   - **結果のパスの例: CoolCompanyDomainのAlex**という名前のユーザーの場合、パスは次のようになります: `\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`

   リポジトリパス(/en-us/citrix-virtual-apps-desktops/2411/media/upl-user-layer-repo-enter-path-no-variables.png)

`%USERNAME%`と`%USERDOMAIN%`変数、マシン環境変数、およびActive Directory (AD) 属性を使用してパスをカスタマイズできます。これらの変数を展開すると、明示的なパスになります。

環境変数の例:

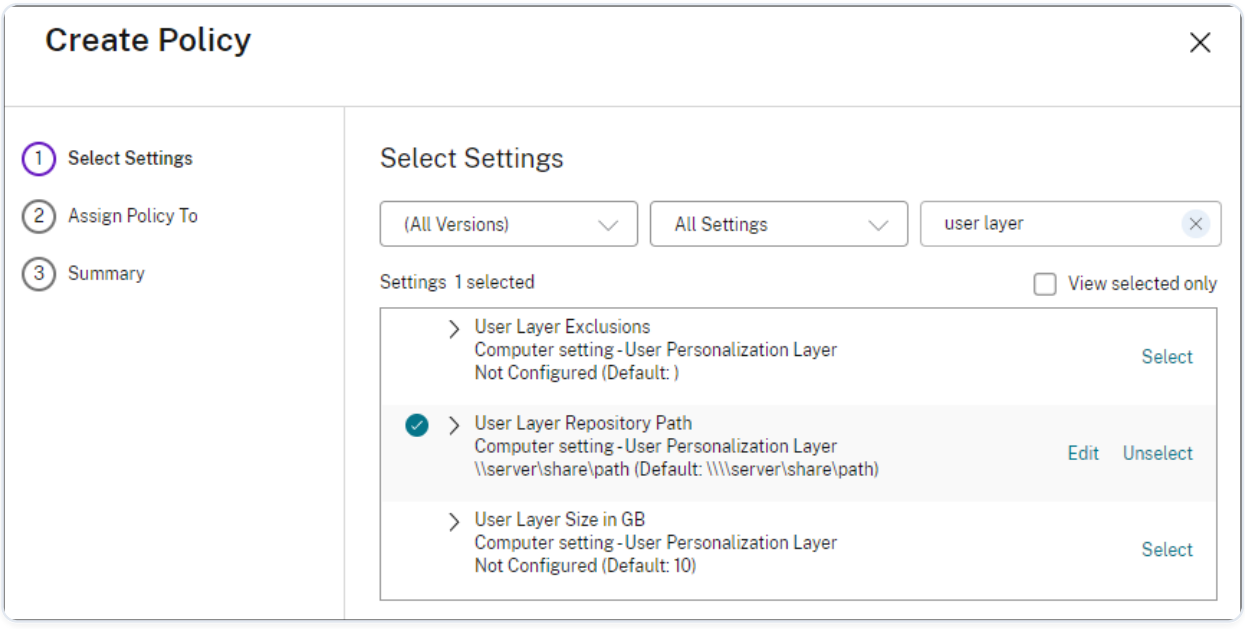
- **パス形式:** `\\Server-name-or-address\share-name\folder-with-environment-variables`
- **パスの例:** `\\Server\Share\UPLUserLayers\%USERNAME%\%USERDOMAIN%`
- **結果のパスの例: CoolCompanyDomainのAlex**という名前のユーザーの場合、パスは次のようになります: `\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`

環境変数を含むリポジトリパス(/en-us/citrix-virtual-apps-desktops/2411/media/upl-user-layer-repo-enter-path-variables.png)

カスタムAD属性の例:

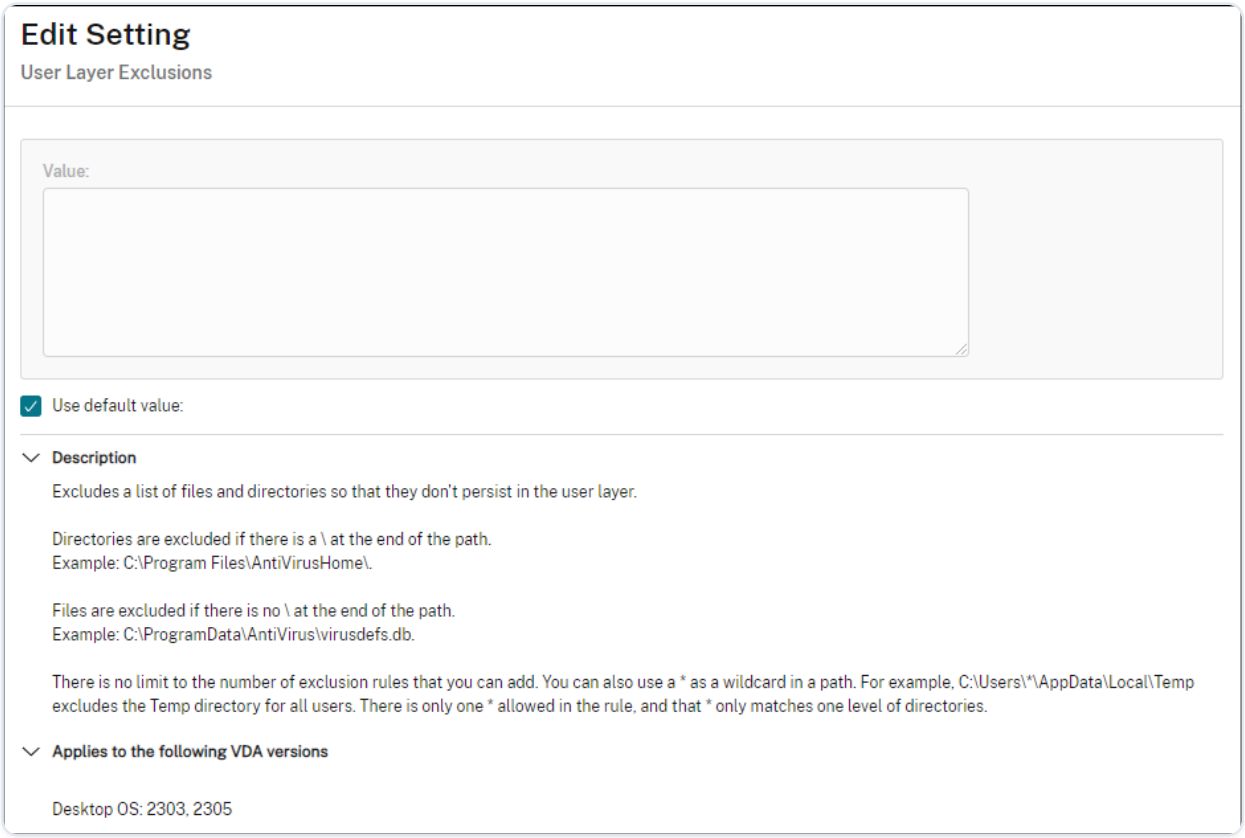
- パス形式: `\\Server-name-or-address\share-name\AD-attribute`
- パスの例: `\\Server\share#sAMAccountName#`
- 結果のパスの例: `\\Server\share\JohnSmith` (現在のユーザーに対して #sAMAccountName# が JohnSmith に解決される場合)

6. オプション: **ユーザーレイヤーサイズ (GB)** の横にあるチェックボックスをオンにして、**編集**をクリックします:

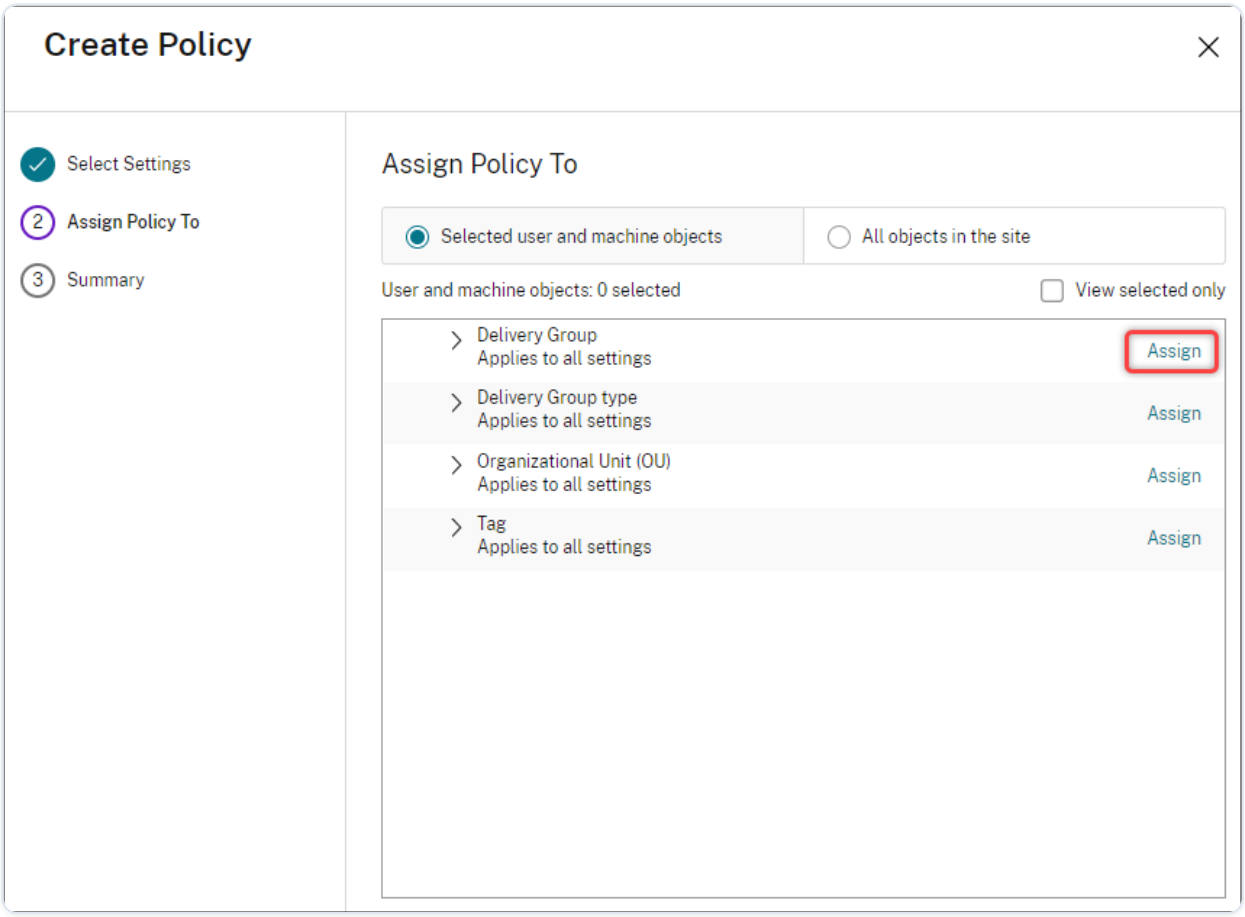


設定の編集ウィンドウが表示されます。

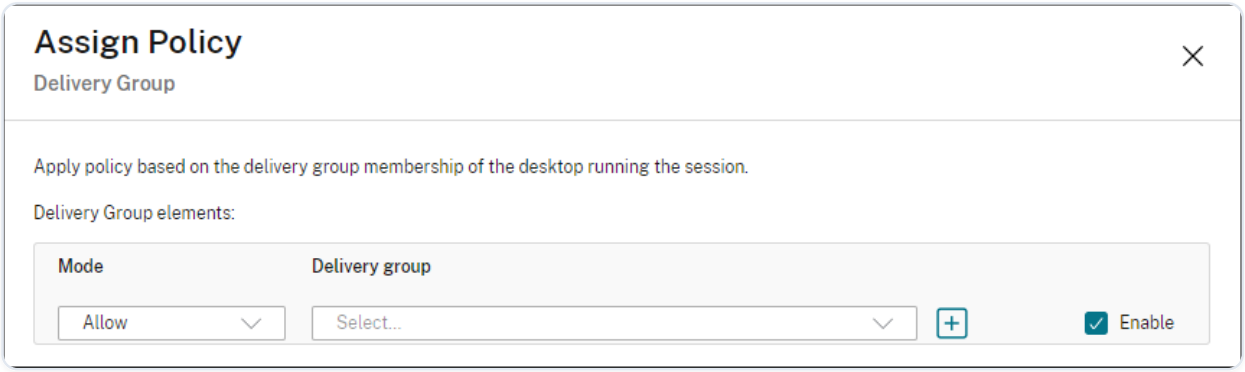
7. オプション: **10 GB** のデフォルト値を、各ユーザーレイヤーが拡張できる最大サイズに変更します。**保存** をクリックします。
8. オプション: **User Layer Exclusions** の横にあるチェックボックスをオンにして、**Edit** をクリックします。



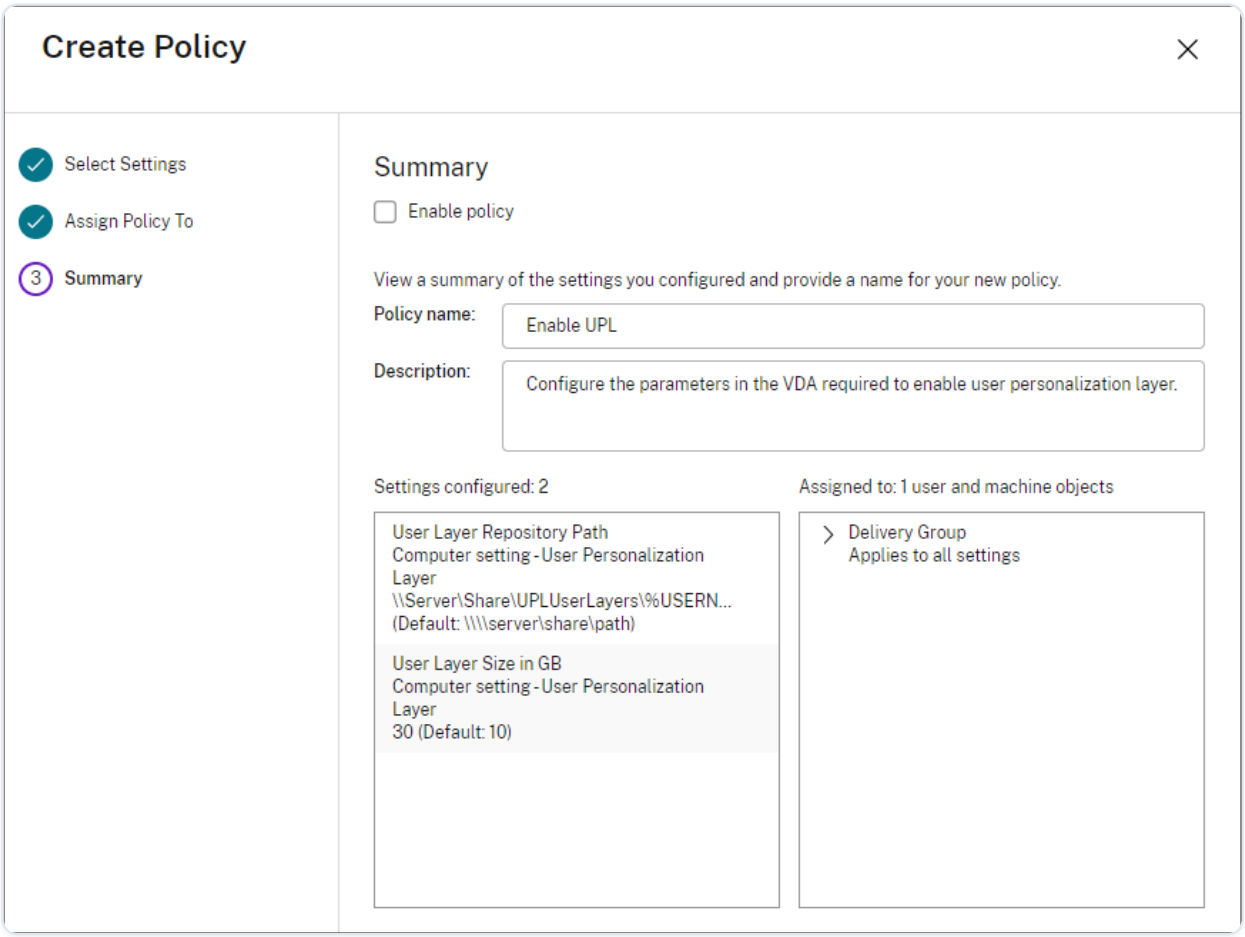
9. オプション: 除外するファイルとフォルダーを指定し、**保存** をクリックします。詳細については、Citrix App Layering のドキュメント を参照してください。
10. 割り当てるユーザーとマシンを構成するには、**次へ** をクリックします。この画像で強調表示されている **デリバリーグループの割り当て** リンクをクリックします:



11. **Delivery Group** メニューで、前のセクションで作成したデリバリーグループを選択します。**OK** をクリックします。



12. ポリシーの名前を入力します。ポリシーを有効にするには、チェックボックスをオンにして、**Finish** をクリックします。



ユーザーレイヤーフォルダーのセキュリティ設定を構成する

ドメイン管理者として、ユーザーレイヤーのストレージ場所を複数指定できます。各ストレージ場所（デフォルトの場所を含む）に`\Users`サブフォルダーを作成します。以下の設定を使用して、各場所を保護します。

設定名	値	適用先	
作成者/所有者	変更	サブフォルダーとファイルのみ	
所有者の権限	変更	サブフォルダーとファイルのみ	
ユーザーまたはグループ	フォルダーの作成/データの追加; フォルダーの横断/ファイルの実行; フォルダーの一覧表示/データの読み取り; 属性の読み取り	選択したフォルダーのみ	

設定名	値	適用先	
システム	フルコントロール	選択されたフォルダー、サブフォルダー、およびファイル	
ドメイン管理者、および選択された管理者グループ	フルコントロール	選択されたフォルダー、サブフォルダー、およびファイル	

ユーザーレイヤーメッセージ

ユーザーがユーザーレイヤーにアクセスできない場合、次のいずれかの通知メッセージが表示されます。

- **ユーザーレイヤーが使用中です**

  `We were unable to attach your user layer because it is in use. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **ユーザーレイヤーが利用できません**

  `We were unable to attach your user layer. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **ユーザーサインアウト後にシステムがリセットされませんでした**

  `This system was not shut down properly. Please log off immediately and contact your system administrator.`.

トラブルシューティング時に使用するログファイル

ログファイル ulayersvc.log には、変更がログに記録されるユーザーパーソナライゼーションレイヤーソフトウェアの出力が含まれています。

```
C:\ProgramData\Unidesk\Logs\ulayersvc.log
```

ユーザーレイヤー/UPL領域の再利用

ユーザーがログオフするたびにVHDXファイルを自動的に圧縮するには、**User Layer/UPL space reclamation**を使用できます。 詳細については、User Layer/UPL space reclamationを参照してください。

制限事項

ユーザーパーソナライゼーションレイヤー機能をインストールして使用する際は、以下の制限事項に留意してください。

- App Layering内のレイヤーにユーザーパーソナライゼーションレイヤーソフトウェアを展開しようとしないでください。Citrix Virtual Apps and Desktopsでユーザーパーソナライゼーションレイヤーを展開するか、App Layeringイメージテンプレートでユーザーレイヤーを有効にするかのいずれかであり、両方ではありません。どちらのプロセスでも、必要なユーザーレイヤーが生成されます。
- 永続的なマシンカタログでユーザーパーソナライゼーションレイヤー機能を構成しないでください。
- 「セッションホスト」は使用しないでください。
- 新しいOSインストール（Windows 10の同じバージョンであっても）を実行しているイメージでマシンカタログを更新しないでください。ベストプラクティスは、マシンカタログの作成時に使用した同じマスターイメージ内でOSに更新を適用することです。
- ブート時ドライバーやその他の初期ブートパーソナライゼーションは使用しないでください。
- PvDデータをユーザーパーソナライゼーションレイヤー機能に移行しないでください。
- 既存のユーザーレイヤーを完全なApp Layering製品からユーザーパーソナライゼーションレイヤー機能に移行しないでください。
- 異なるマスターOSイメージを使用して作成されたユーザーレイヤーにアクセスするために、ユーザーレイヤーのSMBパスを変更しないでください。
- ユーザーがセッションからログアウトし、再度ログインすると、新しいセッションはプール内の別のマシンで実行されます。VDI環境では、Microsoft Software Centerは最初のマシンではアプリケーションを**Installed**と表示しますが、2番目のマシンでは**Unavailable**と表示します。

  アプリケーションの実際のステータスを確認するには、ユーザーにSoftware Centerでアプリケーションを選択し、**Install**をクリックするように指示します。すると、SCCMがステータスを実際の値に更新します。
- ユーザーパーソナライゼーションレイヤー機能が有効になっているVDA内でSoftware Centerを起動すると、すぐに停止することがあります。この問題を回避するには、Implementing SCCM

in a XenDesktop VDI environmentに関するMicrosoftの推奨事項に従ってください。また、Software Centerを起動する前に、`ccmexec`サービスが実行されていることを確認してください。

- グループポリシー（コンピューターの構成）では、ユーザーレイヤーの設定がマスターイメージに適用された設定を上書きします。そのため、GPOを使用してコンピューターの構成で行った変更は、次回のセッションログイン時にユーザーに常に適用されるとは限りません。

  この問題を回避するには、次のコマンドを発行するユーザーログオンスクリプトを作成します。

  ```
  gpupdate /force
  ```

  例えば、あるお客様は、各ユーザーログイン時に次のコマンドを実行するように設定しました。

  ```
  gpudate /Target:Computer /force
  ```

  最良の結果を得るには、ユーザーがログインした後で、コンピューター設定への変更をユーザーレイヤーに直接適用します。
- ドメインユーザーアカウントは、マスターイメージに最後にログインしたユーザーであってはなりません。そうしないと、そのイメージからプロビジョニングされたマシンで問題が発生する可能性があります。
- 純粋なAzure AD環境でUPLが有効になっている場合、Azure上で実行されているWindowsの根本的な問題が原因で、カスタム証明書は永続化しません。Microsoftが将来の機能強化でこの問題を修正した場合、この記事を更新します。

コンポーネントの削除

コンポーネントを削除するには、プログラムの削除または変更を行うWindows機能を使用することをお勧めします。または、コマンドラインまたはインストールメディア上のスクリプトを使用してコンポーネントを削除することもできます。

コンポーネントを削除しても、前提条件は削除されず、ファイアウォール設定も変更されません。たとえば、Delivery Controller™を削除しても、SQL Serverソフトウェアとデータベースは削除されません。

Web Interfaceを含む以前の展開からControllerをアップグレードした場合は、Web Interfaceコンポーネントを個別に削除する必要があります。インストーラーを使用してWeb Interfaceを削除することはできません。

以下に記載されていない機能の削除については、その機能のドキュメントを参照してください。

準備

Controllerを削除する前に、サイトから削除してください。詳しくは、「Controllerを削除する」を参照してください。

StudioとDirectorを削除する前に、それらを閉じます。

Windowsのプログラムの削除または変更機能を使用してコンポーネントを削除する

Windowsのプログラムの削除または変更機能から：

- Controller、Studio、Director、License Server、またはStoreFrontを削除するには、**Citrix Virtual Apps *version*** または **Citrix Virtual Apps and Desktops™ *version*** を右クリックして、**アンインストール**を選択します。インストーラーが起動します。削除するコンポーネントを選択します。

  または、**Citrix StoreFront**を右クリックして**アンインストール**を選択することで、StoreFront™を削除できます。
- VDAを削除するには、**Citrix Virtual Delivery Agent *version*** を右クリックして、**アンインストール**を選択します。インストーラーが起動し、削除するコンポーネントを選択できます。デフォルトでは、削除後にマシンは自動的に再起動します。
- Universal Print Serverを削除するには、**Citrix Universal™ Print Server**を右クリックして、**アンインストール**を選択します。

コマンドラインを使用してコアコンポーネントを削除する

`\x64\XenDesktop Setup`ディレクトリから、`XenDesktopServerSetup.exe`コマンドを実行します。

- 1つ以上のコンポーネントを削除するには、`/remove`および`/components`オプションを指定します。
- すべてのコンポーネントを削除するには、`/removeall`オプションを指定します。

コマンドとパラメーターの詳細については、コマンドラインを使用したインストールを参照してください。

例えば、次のコマンドはWeb Studioを削除します。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components webstudio
```

アップグレード中に、`\x64\Licensing\CitrixLicensing.exe /quiet`または`\x64\Licensing\CitrixLicensing.exe /quiet /l install.log`コマンドを使用して最初にライセンスサーバーをインストールし、その後コアコンポーネントをインストールした場合は、アンインストールも同じ順序で行ってください。

1. コマンドラインを使用してライセンスサーバーをアンインストールします:

   ```
   CitrixLicensing.exe /quiet /uninstall /l uninstall.log
   ```

2. GUIまたはコマンドラインを使用してコンポーネントをアンインストールします。詳細については、コンポーネントの削除を参照してください。

コマンドライン`XenDesktopServerSetup.exe`または`removeall`を使用してライセンスサーバーとコンポーネントをアンインストールした場合は、レジストリエントリと残りのファイルをクリーンアップしてください。

レジストリエントリをクリーンアップするには:

1. レジストリキー`Citrix Licensing`を検索し、そのエントリを削除します。ほとんどの場合、エントリは次の場所にあります。

   ```
   "Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Cur
   rentVersion\Uninstall\
   ```

2. レジストリキーの**Uninstall String**が指すフォルダーを削除します。

コマンドラインを使用してVDAを削除する

`\x64\XenDesktop Setup`ディレクトリから、`XenDesktopVdaSetup.exe`コマンドを実行します。

- 1つ以上のコンポーネントを削除するには、`/remove`および`/components`オプションを使用します。たとえば、VDA と Citrix Workspace アプリを削除するには、`/remove /components vda,plugin`を使用します。
- `/removeall`オプションは VDA のみを削除します。Citrix Workspace アプリは削除しません。

コマンドとパラメーターの詳細については、コマンドラインを使用したインストール を参照してください。

削除後、デフォルトではマシンが自動的に再起動します。

Active Directory でスクリプトを使用して VDA を削除するには、スクリプトを使用した VDA のインストールまたは削除 を参照してください。

アップグレードと移行

注記：

従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきたファイルベースのライセンスシステムは、April 15, 2026にサポート終了 (EOL) となります。License Activation Service (LAS) は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。LASは、April 15, 2026以降、Citrixオンプレミスコンポーネントをアクティベートおよびライセンス供与する唯一の方法となります。サポートを継続するには、Citrix Virtual Apps and Desktopsの展開がLAS互換バージョンである必要があります。LAS互換の最小要件となるCVADバージョンは次のとおりです。

- CVAD 2203 LTSR CU7
- CVAD 2402 LTSR CU3
- CVAD 2507 LTSR
- CVAD 2411

ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrixは、これらの要件を遵守しない場合、Citrixが法または衡平法上持つ可能性のあるその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止する場合があります。これらの要件は、法律または規制によって禁止されている場合は適用されません。

はじめに

アップグレードすると、新しいマシンやサイトをセットアップすることなく、展開がCitrix Virtual Apps and Desktops™ 7 **Current Release (CR)** に変更されます。これはインプレースアップグレードとして知られています。

アップグレードにより、対象となる最新の機能とテクノロジーにアクセスできるようになります。アップグレードには、以前のバージョンからの修正、明確化、および機能強化も含まれる場合があります。

アップグレードの概要

1. アップグレードを開始する前に、(/ja-jp/citrix-virtual-apps-desktops/2411/upgrade-migrate/upgrade.html)の記事を確認してください。これは、アップグレードの準備方法と実装方法を学ぶための主要な情報源です。
2. 現在のCustomer Success Servicesの有効期限が切れていないことを確認してください。詳細については、(/ja-jp/licensing/current-release/customer-success-services.html#customer-success-services-renewal-licenses)の記事を参照してください。
3. 準備に関するガイダンスを完了してください。
4. コアコンポーネントをアップグレードするためにインストーラーを実行します。
5. システムデータベースとサイトをアップグレードします。
6. イメージ上のVDA（またはマシンに直接）をアップグレードします。
7. その他のコンポーネントをアップグレードします。

各準備およびアップグレード手順の詳細については、展開のアップグレードを参照してください。

アップグレード可能なバージョン

Citrix Virtual Apps and Desktops 2407へは、以下からアップグレードできます。

- Virtual Apps and Desktops 2203 LTSR（CUの有無にかかわらず、CU5までを含む）
- Virtual Apps and Desktops 1912 LTSR（CUの有無にかかわらず、CU9までを含む）
- Citrix Virtual Apps and Desktopsの現在サポートされているCRバージョン

アップグレード可能なCitrix Virtual Apps and Desktops（およびXenApp and XenDesktop）のバージョンの一覧については、https://docs.citrix.com/jp/ja/upgrade.htmlも参照してください。

> 注:
>
> - アップグレードプロセスを開始する前に、Citrix®は、お客様が管理された環境でアップグレードをテストし、特定の要件を満たしていることを確認することを推奨します。さらに、スムーズな移行を確実にするために、非推奨リストや既知の問題を含むすべての関連製品ドキュメントを確認することをお勧めします。このアプローチは、本番システムへの潜在的な中断を軽減し、全体的なアップグレードエクスペリエンスを向上させるのに役立ちます。

- Citrix Virtual Apps and Desktops 1912 LTSRは、まもなくサポート終了フェーズに達します。 サポートされているバージョンの一覧については、製品マトリックスを参照してください。

よくある質問

このセクションでは、Citrix Virtual Apps and Desktops のアップグレードに関するよくある質問に回答します。

- **Virtual Apps and Desktops環境をアップグレードする正しい順序は何ですか？**

  推奨されるアップグレードシーケンスの図と説明については、アップグレードシーケンスおよびアップグレード手順を参照してください。

- **私のサイトには複数のDelivery Controller（異なるゾーンにあります）があります。一部のみをアップグレードした場合、どうなりますか？同じメンテナンス期間中にサイト内のすべてのControllerをアップグレードする必要がありますか？**

  各 Controller 上のさまざまなサービスが相互に通信するため、すべての Delivery Controller を同じメンテナンス期間中にアップグレードすることがベストプラクティスです。異なるバージョンを維持すると、問題が発生する可能性があります。メンテナンス期間中には、Controller の半分をアップグレードし、サイトをアップグレードしてから、残りの Controller をアップグレードすることをお勧めします。詳細については、アップグレード手順 を参照してください。

- **最新バージョンに直接アップグレードできますか、それとも段階的なアップグレードを行う必要がありますか？**

  アップグレード先のバージョンの **新機能** の記事で明示的に記載されていない限り、ほとんどの場合、中間リリースをスキップして最新バージョンにアップグレードできます。

- **お客様はLong Term Service Release (LTSR) 環境からCurrent Releaseにアップグレードできますか？**

  はい。お客様は、長期間にわたってLong Term Service Releaseにとどまる必要はありません。お客様は、ビジネス要件と機能に基づいて、LTSR環境をCurrent Releaseに移行できます。

- **コンポーネントの混在バージョンは許可されていますか？**

  Citrixは、各サイト内で、すべてのコンポーネントを同じバージョンにアップグレードすることを推奨しています。一部のコンポーネントで以前のバージョンを使用することはできますが、最新バージョンのすべての機能が利用できない場合があります。詳細については、「混在環境に関する考慮事項」を参照してください。

- **Current Releaseはどのくらいの頻度でアップグレードする必要がありますか？**

  Current Releaseは、リリース日から6か月後にメンテナンス終了（EOM）に達します。Citrixは、お客様が最新のCurrent Releaseを採用することを推奨しています。Current Releaseは、リリース日から18か月後にサポート終了（EOL）に達します。

- **推奨されるのは、LTSRへのアップグレードですか、それともCRへのアップグレードですか？**

  Current Release（CR）は、最新かつ最も革新的なアプリ、デスクトップ、およびサーバー仮想化の機能を提供します。これにより、最先端のテクノロジーを維持し、競合他社の一歩先を行くことができます。

  長期サービスリリース (LTSR) は、長期間にわたって同じベースバージョンを維持することを好む大規模なエンタープライズ生産環境に最適です。

```
For details, see [Servicing Options]( https://www.citrix.com/support/
citrix-customer-success-services/citrix-virtual-apps-and-desktops-
servicing-options.md).
```

- **ライセンスをアップグレードする必要がありますか？**

  現在のライセンスの有効期限が切れておらず、アップグレードするリリースに対して有効であることを確認してください。CTX111618を参照してください。更新については、カスタマーサクセスサービス更新ライセンスを参照してください。

- **アップグレードにはどのくらい時間がかかりますか？**

  展開のアップグレードにかかる時間は、インフラストラクチャとネットワークによって異なります。そのため、正確な時間をお伝えすることはできません。

- **ベストプラクティスは何ですか？**

  準備ガイドを理解し、それに従っていることを確認してください。

- **サポートされているオペレーティングシステムは何ですか？**

  アップグレードするバージョンのシステム要件の記事に、サポートされているOSが記載されています。

  現在の展開でサポートされなくなったオペレーティングシステムを使用している場合は、以前のオペレーティングシステムを参照してください。

- **サポートされているVMware vSphere (vCenter + ESXi) のバージョンは何ですか？**

CTX131239には、サポートされているホストとバージョン、および既知の問題へのリンクが記載されています。

- **私のバージョンはいつEOLになりますか？**

  製品マトリックスを確認してください。

- **最新リリースにおける既知の問題は何ですか？**

  - シトリックス バーチャル アプリケーションズ アンド デスクトップス
  - 「StoreFront」(/ja-jp/storefront/current-release/whats-new.html)
  - シトリックス プロビジョニング
  - シトリックス ライセンス サーバー
  - Windows向けCitrix Workspaceアプリ

詳細情報

長期サービスリリース (LTSR) 展開の更新には累積更新プログラム (CU) が使用されます。CUはLTSRのベースラインコンポーネントを更新し、各CUには独自のメタインストーラーが含まれています。

各CUには専用のドキュメントがあります。たとえば、2203 LTSRの場合、最新のCUについては、そのLTSRの**「新機能」**ページにあるリンクを確認してください。各CUページには、サポートされているバージョン情報、手順、およびCUダウンロードパッケージへのリンクが含まれています。

移行

クラウドへの移行

Citrix Virtual Apps and Desktopsの自動構成ツールを使用して、オンプレミス展開をクラウドに移行できます。詳しくは、「クラウドへの移行」を参照してください。

レガシー移行

移行とは、以前の展開から新しいバージョンにデータを移動することです。このプロセスには、新しいコンポーネントのインストールと新しいサイトの作成、古いファームからのデータのエクスポート、そして新しいサイトへのデータのインポートが含まれます。

XenAppおよびXenDesktopのバージョン、または以前のCitrix Virtual Apps and Desktopsのバージョンを移行するためのサポートされているツールやスクリプトはありません。この製品ドキュメントで説明されているCitrix Virtual Apps and Desktopsのバージョンについては、*アップグレード*がサポートされています。

以前のXenApp 6.xの移行コンテンツについては、以下を参照してください。スクリプトも記事もサポートまたは保守されていません。

- XenApp 6.x バージョン用のオープンソース移行スクリプトは、`<https://github.com/citrix/xa65migrationtool>` で入手できます。Citrix はこれらの移行スクリプトをサポートまたは保守していません
- 7.x での変更点
- XenApp 6.5 ワーカーを新しい VDA にアップグレードする
- XenApp 6.x を移行する

展開のアップグレード

注:

従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきたファイルベースのライセンスシステムは、April 15, 2026にサポート終了（EOL）となります。License Activation Service (LAS) は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。April 15, 2026以降、LASがCitrixオンプレミスコンポーネントをアクティベートおよびライセンス供与する唯一の方法となります。サポートを継続するには、Citrix Virtual Apps and Desktopsの展開がLAS互換バージョンである必要があります。LAS互換の最小要件となるCVADバージョンは次のとおりです。

- CVAD 2203 LTSR CU7
- CVAD 2402 LTSR CU3
- CVAD 2507 LTSR
- CVAD 2411

ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrixは、これらの要件を遵守しない場合、Citrixが法律上または衡平法上持つ可能性のあるその他の救

> 済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。

はじめに

> **注:**

> この記事では、Web Studioを含む展開のアップグレードについて説明します。Citrix Studioを含むアップグレードについては、Citrix Virtual Apps and Desktops™ 7 2212以前の同等の記事を参照してください。

> 新しいマシンやサイトを最初にセットアップすることなく、特定の展開を新しいバージョンにアップグレードできます。これはインプレースアップグレードと呼ばれます。

アップグレードできるCitrix Virtual Apps and Desktopsのバージョンについては、(/ja-jp/citrix-virtual-apps-desktops/2411/upgrade-migrate.html#versions-you-can-upgrade)を参照してください。

Citrix Virtual Apps and Desktopsのいずれかのリリースにアップグレードする前に、現在のCustomer Success Servicesの有効期限が切れていないことを確認してください。詳細については、(/ja-jp/licensing/current-release/customer-success-services.html#customer-success-services-renewal-licenses)の記事を参照してください。

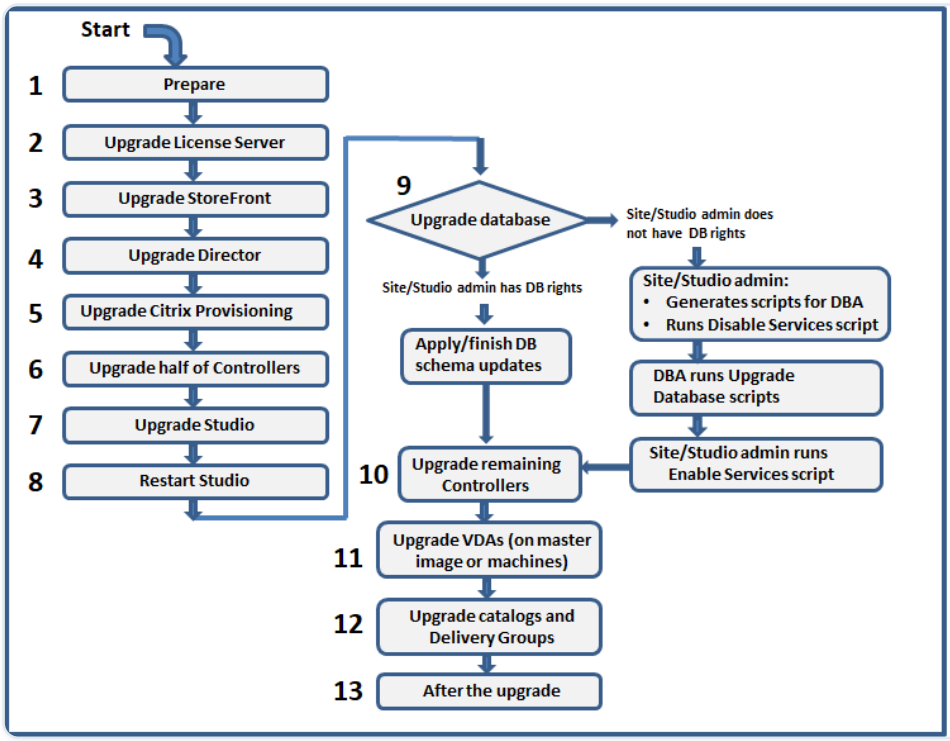
アップグレードを開始するには、新しいバージョンのインストーラーを実行して、以前にインストールされたコアコンポーネント、VDA、および特定のその他のコンポーネントをアップグレードします。次に、データベースとサイトをアップグレードします。

新しいバージョンが提供されている場合、フルプロダクトインストーラー（およびスタンドアロンVDAインストーラー）でインストールできるコンポーネントはすべてアップグレードできます。フルプロダクトインストーラーでインストールされないその他のコンポーネント（Citrix Provisioning™やProfile Managementなど）については、そのコンポーネントのドキュメントを参照してください。ホストのアップグレードについては、適切なドキュメントを参照してください。

アップグレードを開始する前に、この記事のすべての情報を確認してください。

アップグレードシーケンス

次の図は、アップグレードシーケンスの手順を示しています。アップグレード手順には、図の各手順の詳細が含まれています。



注:

障害を回避するため、新しいマシンカタログの作成、マシンカタログの削除、デリバリーグループ内のマシンの更新など、プロビジョニングおよびデリバリーグループ関連のタスクを実行する前に、すべてのDelivery Controllerとデータベースをアップグレードする必要があります。

ハイブリッド権限ライセンス

ハイブリッドライツライセンスは、顧客が永続ライセンスからクラウドサービスサブスクリプションに移行またはアップグレードする際に、クラウドサービスサブスクリプションに加えて提供される期間ベースのサブスクリプションライセンスです。DaaSサブスクリプションでハイブリッドライツアドオンを購入することもできます。

SaaS属性を持つハイブリッドライツライセンスをお持ちの場合、Citrix Virtual Apps and Desktops LTSR 2203以降にアップグレードすると、Citrix Virtual Apps and Desktops LTSR 1912では利用できなかった機能にアクセスできるようになります。これらの機能には、Microsoft Azure、AWS EC2、Google Cloudなどのパブリッククラウドでのワークロードのプロビジョニングとホスティングが含まれます。新しいライセンスファイルを展開する前に、License Serverを最新バージョンに更新してください。

SaaS属性のないハイブリッドライツライセンスにアクセスできる場合は、次の手順に従ってSaaS属性を持つ新しいハイブリッドライツライセンスにアクセスしてください。

注:

- 新しいライセンスコードが記載されたメールが届きます。詳細については、ライセンスアクセスコードの使用を参照してください。
- 既存のライセンスは取り消されます。取り消されたライセンスは、ライセンスサーバーから削除し、その後新しいライセンスをインストールする必要があります。詳細については、ライセンスファイルの削除を参照してください。

1. citrix.comのライセンス管理ポータルにアクセスし、クラウドプロビジョニング権限が有効になっている（SaaS属性を持つ）新しいハイブリッドライツライセンスファイルをダウンロードします。詳細については、ライセンスのダウンロードを参照してください。次の画像は、インクリメントセクションにSaaS属性を持つハイブリッドライツライセンスファイルを示しています。

   「ライセンスファイルのSaaS属性」(/en-us/citrix-virtual-apps-desktops/2411/media/lic-file-hybrid-rights.png)
2. ハイブリッド権限ライセンスファイルをライセンスサーバーにインストールします。詳細については、「ライセンスのインストール」を参照してください。
3. ライセンスのエディションまたはモデルに変更がある場合は、brokerコマンドを実行してエディションとモデルを設定し、インプレースアップグレードを開始してください。Brokerコマンドの詳細については、「Broker PowerShell SDK」セクションを参照してください。

Citrix Virtual Apps and DesktopsのCurrent ReleasesおよびLong Term Service Releasesでのパブリッククラウドサポートの詳細については、「CTX270373」を参照してください。

アップグレード手順

主要な製品コンポーネントのほとんどは、コンポーネントを含むマシンで製品インストーラーを実行することでアップグレードできます。

1台のマシンに複数のコンポーネント（StudioやLicense Serverなど）が含まれている場合、製品メディアにそれらのソフトウェアの新しいバージョンが含まれていれば、そのマシン上のすべてのコンポーネントがアップグレードされます。

インストーラーを使用するには：

- フル製品インストーラーのグラフィカルインターフェイスを実行するには、マシンにログオンし、メディアを挿入するか、新しいリリースのISOドライブをマウントします。「**AutoSelect**」をダブルクリックします。
- コマンドラインインターフェイスを使用するには、適切なコマンドを発行します。「コマンドラインを使用したインストール」を参照してください。

ステップ1：準備

アップグレードを開始する前に、準備が整っていることを確認してください。必要なタスクを読み、完了してください。

- 「PVD、AppDisks™、およびサポートされていないホストの削除」
- 「PvDまたはAppDiskコンポーネントを持つVDA」
- 「制限事項」
- 混在環境に関する考慮事項
- 以前のオペレーティングシステム
- 準備
- サイトの事前テスト
- SQL Serverのバージョンチェック

手順2：ライセンスサーバーのアップグレード

インストールに新しいバージョンのCitrix License Serverソフトウェアが含まれている場合は、他のコンポーネントよりも先にこのコンポーネントをアップグレードしてください。

まだライセンスサーバーが新しいバージョンと互換性があるかどうかを判断していない場合は、他のコアコンポーネントをアップグレードする前に、ライセンスサーバーでインストーラーを実行することが不可欠です。

手順3：StoreFront™のアップグレード

インストールメディアにStoreFrontソフトウェアの新しいバージョンが含まれている場合は、StoreFrontサーバーがインストールされているマシンでインストーラーを実行します。

- グラフィカルインターフェイスで、 セクションから を選択します。
- コマンドラインから、Citrix Virtual Apps and Desktopsインストールメディアの`x64`フォルダーにある`CitrixStoreFront-x64.exe`を実行します。

手順4：Directorのアップグレード

インストールメディアにDirectorソフトウェアの新しいバージョンが含まれている場合は、Directorがインストールされているマシンでインストーラーを実行します。

手順5：Citrix Provisioningのアップグレード

Citrix Provisioningのインストールメディアは、Citrix Virtual Apps and Desktopsのインストールメディアとは別に提供されています。Citrix Provisioningサーバーおよびターゲットデバイスソフトウェアのインストールとアップグレードの方法については、Citrix Provisioning製品ドキュメントを参照してください。

ステップ6：Delivery Controllerの半分をアップグレードする

たとえば、サイトに4つのControllerがある場合、そのうちの2つでインストーラーを実行します。

Controller の半分をアクティブなままにしておくことで、ユーザーはサイトにアクセスできます。VDA は残りの Controller に登録できます。Controller の数が少ないため、サイトの容量が低下する場合があります。アップグレードは、最終的なデータベースアップグレード手順中に新しいクライアント接続を確立する際に、一時的な中断を引き起こすだけです。アップグレードされた Controller は、サイト全体がアップグレードされるまで要求を処理できません。

サイトに Controller が1つしかない場合、アップグレード中は動作しません。

実際のアップグレードが開始される前に、最初の Controller で予備サイトテストが実行されます。詳細については、予備サイトテストを参照してください。

ステップ7：Studioのアップグレード

Web Studio をまだアップグレードしていない場合（別のコンポーネントと同じマシンにあったため）、Studio が含まれているマシンでインストーラーを実行します。

> **注:**
>
> Web Studio をアップグレードした後、バージョン情報がすぐに更新されない場合があります。Web Studio がすでに最新の状態であっても、アップグレードを促されることがあります。この問題に対処するには、Web Studio サーバーに移動し、Internet Information Services (IIS) マネージャーを開き、 > > に移動して、 ペインで を選択します。

ステップ8：Studioの再起動

アップグレードされた Web Studio を再起動します。アップグレードプロセスが自動的に再開されます。

ステップ9：データベースとサイトのアップグレード

> **注:**
>
> 障害を回避するには、新しいマシンカタログの作成、マシンカタログの削除、デリバリーグループ内のマシンの更新など、プロビジョニングおよびデリバリーグループ関連のタスクを実行する前に、すべての Delivery Controller とデータベースをアップグレードする必要があります。

> SQL Server データベースのスキーマを更新するために必要な権限については、準備 を確認してください。

- SQL Server データベーススキーマを更新する十分な権限がある場合は、データベースの自動アップグレードを開始できます。データベースとサイトを自動的にアップグレードする に進みます。
- データベースの権限が不十分な場合は、スクリプトを使用する手動アップグレードを開始し、データベース管理者（必要な権限を持つユーザー）の助けを借りて続行できます。手動アップグレードの場合、Studio ユーザーがスクリプトを生成し、サービスを有効化および無効化するスクリプトを実行します。データベース管理者は、SQLCMD ユーティリティまたは SQLCMD モードの SQL Server Management Studio を使用して、データベーススキーマを更新する他のスクリプトを実行します。データベースとサイトを手動でアップグレードする に進みます。
- マルチゾーン展開でデータベースとサイトを自動的にアップグレードする場合は、サイトの SQL Server データベースをホストするのと同じゾーンで dbschema アップグレードを実行することを Citrix は推奨します。そうしないと、データベースとサイトの自動アップグレードが失敗する可能性があります。

Citrix は、アップグレード前にデータベースをバックアップすることを強く推奨します。CTX135207 を参照してください。データベースのアップグレード中は、製品サービスが無効になります。その間、Controller はサイトの新しい接続を仲介できないため、慎重に計画してください。

データベースとサイトを自動的にアップグレードする

1. 新しくアップグレードされた Studio を起動します。

2. サイトのアップグレードを自動的に開始することを示し、準備ができたことを確認します。

データベースとサイトのアップグレードが進行します。

データベースとサイトを手動でアップグレードする

1. 新しくアップグレードされた Studio を起動します。
2. サイトを手動でアップグレードすることを示します。ウィザードはライセンスサーバーの互換性を確認し、確認を求めます。
3. データベースをバックアップしたことを確認します。

   ウィザードは、スクリプトとアップグレード手順のチェックリストを生成して表示します。アップグレード対象の製品バージョン以降、データベースのスキーマが変更されていない場合、そのスクリプトは生成されません。たとえば、ログデータベースのスキーマが変更されない場合、`UpgradeLoggingDatabase.sql` スクリプトは生成されません。
4. 次のスクリプトを、表示されている順序で実行します。

   - `DisableServices.ps1`: Studioユーザーは、製品サービスを無効にするために、ControllerでこのPowerShellスクリプトを実行します。
   - `UpgradeSiteDatabase.sql`: データベース管理者は、サイトデータベースを含むサーバーでこのSQLスクリプトを実行します
   - `UpgradeMonitorDatabase.sql`: データベース管理者は、監視データベースを含むサーバーでこのSQLスクリプトを実行します。
   - `UpgradeLoggingDatabase.sql`: データベース管理者は、構成ログデータベースを含むサーバーでこのSQLスクリプトを実行します。このスクリプトは、このデータベースが変更された場合（たとえば、修正プログラムを適用した後など）にのみ実行してください。
   - `EnableServices.ps1`: Studioユーザーは、製品サービスを有効にするために、ControllerでこのPowerShellスクリプトを実行します。

   データベースのアップグレードが完了し、製品サービスが有効になると、Studioは環境と構成を自動的にテストし、HTMLレポートを生成します。問題が特定された場合は、データベースのバックアップを復元できます。問題を解決した後、データベースを再度アップグレードできます。
5. チェックリストのタスクを完了したら、**Finish upgrade**をクリックします。

ステップ10：残りのDelivery Controllerをアップグレードする

新しくアップグレードされたStudioから、ナビゲーションペインで**Citrix Studio** *サイト名*を選択します。**Common Tasks**タブで、**Upgrade remaining Delivery Controllers**を選択します。

注:

Upgrade remaining Delivery Controllersを利用できるようにするには、サイト用に少なくとも1つのマシンカタログと1つのデリバリーグループを作成します。

アップグレードを完了し、完了を確認したら、Studioを閉じてから再度開きます。Studioは、Controllerのサービスをサイトに登録するため、またはゾーンIDが存在しない場合にゾーンIDを作成するために、追加のサイトアップグレードを促すことがあります。

ステップ11：VDAをアップグレードする

重要:

VDAをバージョン1912以降にアップグレードする場合は、「VDAを1912以降にアップグレードする」を参照してください。

VDAsを含むマシンで製品インストーラーを実行します。

Machine Creation Services™とマスターイメージを使用してマシンを作成した場合は、ホストに移動してマスターイメージ上のVDAをアップグレードします。利用可能なVDAインストーラーのいずれかを使用できます。

- グラフィックインターフェイスのガイダンスについては、VDAsのインストールを参照してください。
- コマンドラインのガイダンスについては、コマンドラインを使用したインストールを参照してください。

Citrix Provisioningを使用してマシンを作成した場合は、アップグレードのガイダンスについてCitrix Provisioning製品ドキュメントを参照してください。

ステップ12：マシンカタログとデリバリーグループを更新する

- アップグレードされたVDAを使用するマシンを含むカタログを更新する。
- アップグレードされたVDAを使用するマシンを含むカタログをアップグレードする。
- アップグレードされたVDAを使用するマシンを含むデリバリーグループをアップグレードする。

ステップ13：アップグレード後

展開内の他のコンポーネントをアップグレードします。ガイダンスについては、以下の製品ドキュメントを参照してください。

- StoreFront
- AppDNA
- Citrix アプリケーション レイヤリング
- HDX リアルタイム最適化パック
- 「プロファイル管理」(/ja-jp/profile-management/current-release/upgrade-and-migrate.html)
- シトリックス プロビジョニング
- 「セッション録画」(/ja-jp/session-recording/current-release/install-upgrade-uninstall.html#upgrade-session-recording)
- ワークスペース環境管理

Microsoft SQL Server Express LocalDBソフトウェアを以降のバージョンに置換する必要がある場合は、「SQL Server Express LocalDBの置換」(#replace-sql-server-express-localdb)を参照してください。

Dbschemaのアップグレード

展開を更新すると、複数のデータベーススキーマをアップグレードできます。次の表に、そのプロセスでアップグレードされるデータベーススキーマを示します。

From\To	1912 CU1	1912 CU2	1912 CU3	1912 CU4	1912 CU5	2203
7.15 RTM or 7.15 CU releases	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 RTM	Config	Site, Config	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU1		Site	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU2			Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU3				Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU4					Site, Config	Site; Monitor; Config; Logging
1912 CU5						Site; Monitor; Config; Logging
2112						Site; Monitor; Config

用語の定義:

- サイト: サイトデータストア。Dbschemaの更新はサイトデータストアに対して行われます。
- モニター: モニターデータストア。Dbschemaの更新はモニターデータストアに対して行われます。
- 構成: 構成テーブル。構成テーブルでは、Desktop Studioのバージョン、ライセンス情報、またはその両方が更新されます。
- ロギング: ロギングデータストア。Dbschemaの更新はロギングデータストアに対して行われます。

VDAを2203以降にアップグレードする

Personal vDisk (PvD)コンポーネントがVDAにインストールされていた場合、そのVDAはバージョン2203以降にアップグレードできません。新しいVDAを使用するには、現在のVDAをアンインストールしてから、新しいVDAをインストールする必要があります。

この指示は、PvDを一度も使用したことがない場合でも適用されます。

以前のバージョンで PvD コンポーネントがインストールされた可能性のある方法は次のとおりです。

- VDA インストーラーのグラフィックインターフェイスでは、PvD は ページのオプションでした。
- コマンドラインでは、`/baseimage` オプションで PvD がインストールされました。このオプションを指定した場合、またはこのオプションを含むスクリプトを使用した場合は、PvD がインストールされました。

VDA に PvD がインストールされているかどうかわからない場合は、マシンまたはイメージで新しい VDA (2203 以降) のインストーラーを実行します。

- PvD がインストールされている場合、互換性のないコンポーネントがあることを示すメッセージが表示されます。
  - グラフィックインターフェイスから、メッセージを含むページで をクリックし、インストーラーを閉じたいことを確認します。
  - CLI からは、コマンドは表示されたメッセージとともに単に失敗します。
- PvD がインストールされていない場合、アップグレードが続行されます。

対処法

VDAにPvDがインストールされていない場合は、通常のアップグレード手順に従ってください。

VDAにPvDがインストールされている場合：

1. 現在のVDAをアンインストールします。
2. 新しいVDAをインストールします。

Windows 10 (1607 以前、更新なし) マシンで PvD の使用を継続したい場合は、VDA 7.15 LTSR がサポートされる最新バージョンです。

> **注記:**

> *XenApp and XenDesktop 7.15 LTSR で Windows 7 デスクトップと Personal vDisk を使用できますか？*

> Citrix は、2016年1月に発表された XenApp and XenDesktop 7.6 LTSR から Personal vDisk (PvD) を除外しました。さらに、Citrix は PvD テクノロジの非推奨を発表し、今後 Citrix App Layering の使用を開始するようお客様に推奨しています。Citrix App Layering (バージョン 4.4 以降) は、XenApp and XenDesktop 7.15 LTSR の互換性のあるコンポーネントです。ただし、Windows 7 上で既存の PvD 展開を使用しているお客様が Citrix App Layering テクノロジに移行できるよう、Citrix は XenApp and XenDesktop 7.15 LTSR 累積更新プログラム (CU) を通じて Windows 7 デスクトップ用の PvD 展開に対する期間限定のサポートを Jan 14, 2020 まで提供することを決定しました。PvD コンポーネントは LTSR CU から削除され、Jan 14, 2020 以降はサポートされません。また、Jan 14, 2020 以降に Windows 7 で PvD を使用すると、LTSR サイトは非準拠になります。また、Windows 10 用の PvD は 7.15 LTSR から引き続き除外されます。したがって、お客様は 7.15 LTSR サイトでこれを使用しないでください。

PvD、AppDisks、およびサポートされていないホストを削除する

Citrix Virtual Apps and Desktops 7 Current Release の展開では、以下のテクノロジとホストの種類はサポートされていません。

- **Personal vDisks (PvD)**。カタログ内のユーザーの VM の隣にデータを保存するためのものです。ユーザーパーソナライゼーションレイヤー機能が、ユーザーの永続性を処理するようになりました。
- **AppDisks**。デリバリーグループで使用されるアプリケーションを管理するためのものです。
- **ホストの種類:** Azure Classic、CloudPlatform (元の Citrix 製品)。
  - このリリースでサポートされているホストの種類については、システム要件を参照してください。
  - ARM と AWS を引き続き使用できる代替方法については、CTX270373を参照してください。

現在の展開で PvD または AppDisks を使用している場合、またはサポートされていないホストの種類 (Microsoft Azure Classic など) への接続がある場合、それらのテクノロジを使用する項目を削除した後にのみ、バージョン 2006 (またはそれ以降のサポートされているバージョン) にアップグレードできます。現在の展開でパブリッククラウドホスト接続 (AWS など) を使用している場合は、アップグレードする前にハイブリッド権限ライセンスがあることを確認してください。インストーラーがサポートされていないテクノロジまたはハイブリッド権限ライセンスのないホスト

接続を 1 つ以上検出すると、アップグレードは一時停止または停止し、説明メッセージが表示されます。インストーラーログに詳細が含まれています。

アップグレードを確実に成功させるために、サポートされていない項目を削除するための該当するガイダンスを確認し、それに従ってください。

- PvD を削除する
- AppDisks を削除する
- サポートされていないホスト項目を削除する

展開でPvDまたはAppDisksを使用していなかった場合でも、関連するMSIが以前のVDAインストールまたはアップグレードに含まれていた可能性があります。VDAをバージョン2006（またはそれ以降のサポートされているバージョン）にアップグレードする前に、たとえ一度も使用していなかったとしても、そのソフトウェアを削除する必要があります。グラフィカルインターフェイスを使用する場合、その削除は自動的に行われるか、CLIを使用する際に削除オプションを含めることができます。詳細については、「PvDまたはAppDisksコンポーネントを持つVDAのアップグレード」を参照してください。

PvDを削除する

PvDを使用するように構成されているすべてのマシンを削除するまで、展開のアップグレードは成功しません。これはカタログとデリバリーグループに影響します。

グループおよびカタログからPvDを削除するには：

1. Studioで、デリバリーグループにPvDを使用するカタログのマシンが含まれている場合は、それらのマシンをグループから削除します。
2. Studioで、PvDを使用するマシンを含むすべてのカタログを削除します。

VDAのアップグレード： 展開のアップグレードでは、VDAにAppDiskまたはPvDコンポーネントがインストールされているかどうかは検出されません。ただし、VDAインストーラーは検出します。詳細については、「PvDまたはAppDisksコンポーネントを持つVDA」を参照してください。

PvDの代わりにApp Layeringを使用する予定がある場合は、データの移行に関する情報について「PvDからApp Layeringへの移行」を参照してください。

AppDisksを削除する

AppDisksを使用するすべてのデリバリーグループからAppDisksを削除し、その後AppDisks自体を削除するまで、展開のアップグレードは続行できません。

1. Studioのナビゲーションペインで**［デリバリーグループ］**を選択します。

2. グループを選択し、アクションペインで**［AppDiskの管理］**をクリックします。
3. グループからAppDiskを削除するアクションをクリックします。
4. AppDisksを使用する各デリバリーグループに対して、手順2と3を繰り返します。
5. Studioのナビゲーションペインで、 を選択します。
6. AppDisk を選択し、AppDisk を削除するアクションをクリックします。
7. 各 AppDisk について、手順 5 と 6 を繰り返します。

VDA のアップグレード: 展開のアップグレードでは、VDA に AppDisk または PvD コンポーネントがインストールされているかどうかは検出されません。ただし、VDA インストーラーは検出します。詳細については、「PvD または AppDisk コンポーネントがインストールされている VDA」を参照してください。

サポートされていないホストアイテムを削除する

サイトが Citrix CloudPlatform や Microsoft Azure Classic などのサポートされていないホストタイプに接続している場合、バージョン 2006 (またはそれ以降のサポートされているバージョン) への展開のアップグレードは続行できません。アップグレードを試みる前に、次のタスクを完了してください。

Studio から:

- サポートされていないホストへのすべての接続を削除します。
- デリバリーグループに、サポートされていないホストのマスターイメージで作成されたカタログのマシンが含まれている場合は、それらのマシンをグループから削除します。
- サポートされていないホストのマスターイメージを使用して作成されたすべてのカタログを削除します。

PvD または AppDisk コンポーネントがインストールされている VDA

PvD および AppDisk テクノロジーを有効にするコンポーネントが VDA にインストールされている場合、それらのコンポーネントが削除されるまで、その VDA はアップグレードできません。

> **注:**
>
> バージョン 1912 にアップグレードする場合、現在の VDA をアンインストールしてから新しい VDA をインストールする必要がありました。このバージョンでは、Citrix がコンポーネントを削除してアップグレードを続行するかどうかを尋ねられます。

> AppDisk および PvD コンポーネントは、それらのテクノロジーを一度も使用していなくても、以前の VDA バージョンでインストールされている可能性があります。

- グラフィカルインターフェイス: VDA インストーラーの ページには、 オプションが含まれていました。7.15 LTSR およびそれ以前の 7.x リリースでは、このオプションがデフォルトで有効になっていました。したがって、デフォルトを受け入れた場合 (または、このオプションが提供されているリリースで明示的に有効にした場合)、そのコンポーネントがインストールされました。
- CLI: `/baseimage`オプションを指定すると、コンポーネントがインストールされます。

実行すること

VDAインストーラーが現在インストールされているVDAでAppDisksまたはPvDコンポーネントを検出しない場合、アップグレードは通常どおり続行されます。

インストーラーが現在インストールされているVDAでAppDisksまたはPvDコンポーネントを検出した場合：

- グラフィカルインターフェイス：アップグレードが一時停止します。サポートされていないコンポーネントを自動的に削除するかどうかを尋ねるメッセージが表示されます。**OK**をクリックすると、コンポーネントは自動的に削除され、アップグレードが続行されます。
- CLI：コマンドの失敗を避けるため、コマンドに次のオプションを含めます。
  - `/remove_appdisk_ack`
  - `/remove_pvd_ack`

制限事項

アップグレードには次の制限が適用されます。

- **コンポーネントの選択的インストール：** 新しいバージョンにコンポーネントをインストールまたはアップグレードしても、アップグレードが必要な他のコンポーネント（別のマシン上）をアップグレードしないことを選択した場合、Studioが通知します。たとえば、アップグレードにControllerとStudioの新しいバージョンが含まれているとします。Controllerはアップグレードしますが、Studioがインストールされているマシンでインストーラーを実行しません。Studioをアップグレードするまで、Studioはサイトの管理を続行できません。

  VDAをアップグレードする必要はありませんが、利用可能なすべての機能を使用できるように、すべてのVDAをアップグレードすることをCitrixは推奨します。
- **早期リリースまたはテクノロジープレビューバージョン：** 早期リリース、テクノロジープレビュー、またはプレビューバージョンからアップグレードすることはできません。

- **以前のオペレーティングシステム上のコンポーネント：** MicrosoftまたはCitrixによってサポートされなくなったオペレーティングシステムに現在のVDAをインストールすることはできません。詳細については、「以前のオペレーティングシステム」を参照してください。
- **混在環境/サイト：** 以前のバージョンのサイトと現在のバージョンのサイトを継続して実行する必要がある場合は、「混在環境に関する考慮事項」を参照してください。
- **製品の選択:** 以前のバージョンからアップグレードする場合、インストール時に設定された製品 (Citrix Virtual Apps または Citrix Virtual Apps and Desktops) を選択または指定することはありません。

混在環境に関する考慮事項

アップグレードする際は、エディションとバージョンに含まれるすべての新規機能および強化された機能にアクセスできるように、すべてのコンポーネントとVDAをアップグレードすることをお勧めします。

たとえば、以前のControllerバージョンを含む展開で現在のVDAを使用することはできますが、現在のリリースの一部の新機能は利用できない場合があります。また、最新ではないバージョンを使用している場合、VDA登録の問題が発生することもあります。

一部の環境では、すべてのVDAを最新バージョンにアップグレードできない場合があります。その場合、マシンカタログを作成する際に、マシンにインストールされているVDAバージョンを指定できます。(これは機能レベルと呼ばれます。) デフォルトでは、この設定は推奨される最小VDAバージョンを指定します。ほとんどの展開では、デフォルト値で十分です。カタログにデフォルトよりも古いVDAが含まれている場合にのみ、設定を以前のバージョンに変更することを検討してください。マシンカタログ内でVDAバージョンを混在させることは推奨されません。

カタログがデフォルトの最小VDAバージョン設定で作成され、1つ以上のマシンがデフォルトバージョンよりも古いVDAを持っている場合、それらのマシンはControllerに登録できず、機能しません。

詳細については、VDAバージョンと機能レベルを参照してください。

異なるバージョンを持つ複数のサイト

環境に異なる製品バージョン (たとえば、XenDesktop 7.18サイトとCitrix Virtual Apps and Desktops 1909サイト) のサイトが含まれている場合、CitrixではStoreFrontを使用して異なる製品バージョンのアプリケーションとデスクトップを集約することをお勧めします。詳細については、StoreFrontのドキュメントを参照してください。

混在環境では、各リリースに対応するStudioおよびDirectorのバージョンを引き続き使用しますが、異なるバージョンは別々のマシンにインストールされていることを確認してください。

以前のオペレーティングシステム

サポートされているオペレーティングシステム (OS) バージョンを実行しているマシンに、以前のバージョンのコンポーネントをインストールしたとします。現在、より新しいコンポーネントバージョンを使用したいと考えていますが、そのOSは現在のコンポーネントバージョンではサポートされていません。

たとえば、Windows Server 2016マシンにサーバーVDAをインストールしたとします。現在、そのVDAを現在のリリースにアップグレードしたいが、アップグレード先の現在のリリースではWindows Server 2016がサポートされていません。

許可されていないオペレーティングシステムにコンポーネントをインストールまたはアップグレードしようとすると、「このオペレーティングシステムにはインストールできません」などのエラーメッセージが表示されます。

これらの考慮事項は、Current ReleaseおよびLong Term Service Releaseバージョンのアップグレードに適用されます。(LTSRバージョンにCUを適用することには影響しません。)

サポートされているOSについては、以下のリンクを参照してください。

- Citrix Virtual Apps and Desktops (最新リリース):
  - デリバリーコントローラー、スタジオ、ディレクター、VDA、ユニバーサルプリントサーバー
  - フェデレーテッド認証サービス
  - StoreFront、Self-Service Password Reset、およびSession Recordingについては、最新リリースのシステム要件の記事を参照してください。
- LTSRについては、お使いのLTSRバージョンとCUのコンポーネントリストを参照してください。（メインのCitrix Virtual Apps and Desktops製品ドキュメントページから、お使いのLTSRバージョンを選択してください。）

無効なオペレーティングシステム

次の表に、現在のリリースでコンポーネントのインストール/アップグレードに無効な以前のオペレーティングシステムを示します。各OSでサポートされている最新の有効なコンポーネントバージョンと、インストールおよびアップグレードが無効になったコンポーネントバージョンを示します。

表のオペレーティングシステムには、サービスパックと更新プログラムが含まれます。

オペレーティングシステム	コンポーネント/機能	最新の有効なバージョン	インストール/アップグレードが不可能になったバージョン
Windows 7およびWindows 8	VDA	7.15 LTSR	7.16
Windows 7 およびWindows 8	その他のインストーラーコンポーネント	7.17	7.18
1607より前のWindows 10バージョン	VDA	7.15 LTSR	7.16
Windows 10 x86バージョン	VDA	1906.2.0	1909
ウィンドウズ サーバー 2008 R2	VDA	7.15 LTSR	7.16
ウィンドウズ サーバー 2008 R2	その他のインストーラーコンポーネント	7.17	7.18
ウィンドウズ サーバー 2012	VDA	7.15 LTSR	7.16
ウィンドウズ サーバー 2012	その他のインストーラーコンポーネント	7.17	7.18
ウィンドウズ サーバー 2012 R2	その他のインストーラーコンポーネント *	1912 LTSR	2003
ウィンドウズ サーバー 2012 R2	サーバーVDI	7.15 LTSR	7.16
Windows サーバー 2016	サーバーVDI	7.15 LTSR	7.16

Windows XPおよびWindows Vistaは、7.xのコンポーネントまたはテクノロジーでは無効です。

* Delivery Controller、Studio、Director、およびVDAに適用されます。

実行できること

選択肢があります。次のことができます。

- 現在のOSを使い続ける(#continue-with-the-current-os)
- マシンを再イメージ化またはアップグレードする(#reimage-or-upgrade-the-machine)
- 新しいマシンを追加し、古いマシンを削除する(#add-new-machines-and-then-remove-old-machines)

現在のOSを使い続ける

これらの方法はVDAで実行可能です。以前のOSを搭載したマシンを使い続けたい場合は、次のいずれかを選択できます。

- インストールされているコンポーネントバージョンを使い続ける。
- 最新の有効なコンポーネントバージョンをダウンロードし、そのバージョンにコンポーネントをアップグレードする。（これは、最新の有効なコンポーネントバージョンがまだインストールされていないことを前提としています。）

たとえば、Windows 7 SP1マシンに7.14 VDAがインストールされているとします。Windows 7 OSマシンで有効な最新のVDAバージョンは、XenApp and XenDesktop 7.15 LTSRです。7.14を使い続けるか、7.15 LTSR VDAをダウンロードしてVDAをそのバージョンにアップグレードすることができます。これらの以前のVDAバージョンは、より新しいバージョンのDelivery Controllerを含む展開で動作します。たとえば、7.15 LTSR VDAはCitrix Virtual Apps and Desktops 7 1808 Controllerに接続できます。

マシンの再イメージ化またはアップグレード

これらの方法は、VDAや、コアコンポーネント（Delivery Controllerなど）がインストールされていない他のマシンで実行可能です。次のいずれかを選択してください。

- マシンをサービスから外し（メンテナンスモードをオンにしてすべてのセッションを閉じさせてから）、サポートされているWindows OSバージョンに再イメージ化し、コンポーネントの最新バージョンをインストールできます。
- 再イメージ化せずにVDAマシンでOSをアップグレードするには、まずアップグレード先のOSでサポートされているVDAバージョンをインストールするか、OSのアップグレード後にVDAをアップグレードする必要があります。そうしないと、Citrixソフトウェアはサポートされません。VDAをアンインストールせずにインプレースアップグレードを実行する場合、次の最小OSバージョンにアップグレードできます。
    - 2023-07 Cumulative Update for Windows 11 (KB5028185)以降がインストールされているWindows 11（ビルド22621.1992以降）。

  - 2023-07 Dynamic Update for Windows 10 (KB5028311)がインストールされている Windows 10。

- アップグレードを計画しているWindowsのバージョンが上記のガイドラインに合致しない場合は、OSをアップグレードする前にVDAをアンインストールし、OSのアップグレードが完了した後にサポートされているVDAバージョンをインストールする必要があります。

新しいマシンを追加し、古いマシンを削除する

この方法は、Delivery Controller™ またはその他のコアコンポーネントを含むマシンの OS をアップグレードする必要がある場合に実行可能です。

Citrixは、サイト内のすべてのControllerが同じOSを持つことを推奨します。以下のアップグレードシーケンスは、異なるControllerが異なるOSを持つ期間を最小限に抑えます。

1. サイト内のすべての Delivery Controller のスナップショットを取得し、サイトデータベースをバックアップします。
2. サポートされているオペレーティングシステムを搭載したクリーンなサーバーに新しい Delivery Controllerをインストールします。
3. 新しいControllerをサイトに追加します。
4. 現在のリリースで有効でないオペレーティングシステムで実行されているControllerを削除します。Delivery ControllersのController削除に関する推奨事項に従ってください。

準備

アップグレードを開始する前に、以下の情報を確認し、必要なタスクを完了してください。

> **注:**
>
> VDA のアップグレードは アップグレードシーケンス の後半で行われますが、アップグレードを開始する前にインストーラーを選択し、手順を確認して、何が予想されるかを知っておくことをお勧めします。

インストーラーとインターフェースを選択する

製品ISOからフルプロダクトインストーラーを使用してコンポーネントをアップグレードします。VDAは、フルプロダクトインストーラーまたはスタンドアロンVDAインストーラーのいずれかを使用してアップグレードできます。すべてのインストーラーは、グラフィカルインターフェースとコマンドラインインターフェースを提供します。

詳細については、インストーラー を参照してください。

「**インストールの詳細:** 準備作業を完了し、インストーラーを起動する準備が整ったら、インストールの記事には、表示される内容 (グラフィカルインターフェイスを使用している場合) または入力する内容 (コマンドラインインターフェイスを使用している場合) が示されます。」.

- 「グラフィカルインターフェイスを使用したコアコンポーネントのインストール/アップグレード」
- 「コマンドラインを使用したコアコンポーネントのインストール/アップグレード」
- 「グラフィカルインターフェイスを使用したVDAのインストール/アップグレード」
- 「コマンドラインを使用したVDAのインストール/アップグレード」

「シングルセッションVDAを`VDAWorkstationCoreSetup.exe`インストーラーで最初にインストールした場合、Citrixはそのインストーラーを使用してアップグレードすることを推奨します。フルプロダクトVDAインストーラーまたは`VDAWorkstationSetup.exe`インストーラーを使用してVDAをアップグレードすると、アップグレードから明示的に除外しない限り、元々除外されていたコンポーネントがインストールされる可能性があります。」.

「VDAを現在のリリースにアップグレードする際、アップグレードプロセス中にマシンの再起動が発生します。(この要件は7.17リリースから始まりました。) これは回避できません。再起動後、アップグレードは自動的に再開されます (コマンドラインで`/noresume`を指定しない限り)。」.

「データベース操作」

「サイト、監視、および構成ログデータベースをバックアップします。CTX135207の指示に従ってください。アップグレード後に問題が発見された場合、バックアップを復元できます。」.

「サポートされなくなったSQL Serverバージョンのアップグレードについては、SQL Serverバージョンチェックを参照してください。(これは、サイト、モニター、および構成ログデータベースに使用されるSQL Serverを指します。)」

「Microsoft SQL Server Express LocalDBは、ローカルホストキャッシュで使用するために自動的にインストールされます。以前のバージョンを置き換える必要がある場合、新しいバージョンはSQL Server Express LocalDB 2019である必要があります。コンポーネントとサイトをアップグレードした後、SQL Server Express LocalDBを新しいバージョンに置き換える方法の詳細については、SQL Server Express LocalDBの置き換えを参照してください。」.

「Citrixライセンスが最新であることを確認する」

「Citrixライセンスの管理に関する包括的な情報については、Citrixライセンスのアクティブ化、アップグレード、および管理を参照してください。」.

「フルプロダクトインストーラーを使用してライセンスサーバーをアップグレードできます。または、ライセンスコンポーネントを個別にダウンロードしてアップグレードすることもできます。アップグレードを参照してください。」.

「アップグレードする前に、Customer Success Services / Software Maintenance / Subscription Advantageの日付が新しい製品バージョンに対して有効であることを確認してください。日付は2021.11.15以降である必要があります。」.

Citrix License Server の互換性を確認する

Citrix License Server が新しいバージョンと互換性があることを確認してください。これには2つの方法があります。

- 他のCitrixコンポーネントをアップグレードする前に、Delivery Controller を含むマシンでISOレイアウトから `XenDesktopServerSetup.exe` インストーラーを実行します。互換性の問題がある場合、インストーラーは推奨される解決手順とともにそれを報告します。
- インストールメディアの `XenDesktop Setup` ディレクトリから、コマンド `.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v` を実行します。表示により、License Server が互換性があるかどうかが示されます。License Server に互換性がない場合は、ライセンスサーバーをアップグレードしてください。

StoreFront の変更をバックアップする

アップグレードを開始する前に、`C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data` 内のファイル（例: *default.ica* や *usernamepassword.tfrm*）を変更している場合は、各ストア用にそれらをバックアップしてください。アップグレード後に、変更を元に戻すためにそれらを復元できます。

アプリケーションとコンソールを閉じる

アップグレードを開始する前に、管理コンソールやPowerShellセッションなど、ファイルロックを引き起こす可能性のあるすべてのプログラムを閉じます。

マシンを再起動すると、ファイルロックがすべて解除され、保留中のWindowsアップデートがないことが保証されます。

アップグレードを開始する前に、サードパーティの監視エージェントサービスをすべて停止し、無効にします。

適切な権限があることを確認する

ドメインユーザーであることに加えて、製品コンポーネントをアップグレードするマシンではローカル管理者である必要があります。

サイトデータベースとサイトは、自動または手動でアップグレードできます。自動データベースアップグレードの場合、Studioユーザーの権限には、SQL Serverデータベーススキーマを更新する機能（たとえば、`db_securityadmin` または `db_owner` データベースロール）が含まれている必要があります。詳細については、データベース を参照してください。

Studioユーザーがこれらの権限を持っていない場合、手動データベースアップグレードを開始すると、スクリプトが生成されます。Studioユーザーは、Studioから一部のスクリプトを実行します。データベース管理者は、SQL Server Management Studioなどのツールを使用して、他のスクリプトを実行します。

その他の準備タスク

- 必要に応じて、テンプレートをバックアップし、ハイパーバイザーをアップグレードします
- 事業継続計画で定められているその他の準備タスクを完了します。

サイトの事前テスト

Delivery Controllerとサイトをアップグレードする際、実際のアップグレードが開始される前に事前サイトテストが実行されます。これらのテストでは、以下を確認します。

- サイトデータベースにアクセスでき、バックアップされていること
- 重要なCitrixサービスへの接続が正しく機能していること
- Citrixライセンスサーバーのアドレスが利用可能であること
- 構成ログデータベースに到達可能であること
- パブリッククラウドホスト接続（例：AWS）を追加する場合は、Hybrid Rights Licenseがあることを確認してください。そうでない場合、事前サイトテストは一時停止または停止し、説明メッセージが表示されます。

テストの実行後、結果のレポートを表示できます。検出された問題を修正し、テストを再度実行できます。予備サイトテストを実行せず、問題を解決しないと、サイトの動作に影響を与える可能性があります。

テスト結果を含むレポートは、インストールログと同じディレクトリにあるHTMLファイル（`PreliminarySiteTestResult.html`）です。そのファイルが存在しない場合は作成されます。ファイルが存在する場合は、その内容が上書きされます。

テストの実行

- インストーラーのグラフィカルインターフェイスを使用してアップグレードする場合、ウィザードにはテストを開始してレポートを表示できるページが含まれています。テストが実行さ

れ、レポートを確認し、見つかった問題を解決した後、テストを再実行できます。テストが正常に完了したら、「次へ」をクリックしてウィザードを続行します。

- コマンドラインインターフェイスを使用してアップグレードする場合、テストは自動的に実行されます。デフォルトでは、テストが失敗した場合、アップグレードは実行されません。レポートを確認し、問題を解決した後、コマンドを再実行してください。

Citrixは、Controllerとサイトのアップグレードを続行する前に、常に事前サイトテストを実行し、問題を解決することを推奨します。テストを実行するわずかな時間で得られる潜在的なメリットは十分にあります。ただし、この推奨されるアクションを上書きすることもできます。

- グラフィカルインターフェイスを使用してアップグレードする場合、テストをスキップしてアップグレードを続行することを選択できます。
- コマンドラインからアップグレードする場合、テストをスキップすることはできません。デフォルトでは、サイトテストが失敗すると、アップグレードを実行せずにインストーラーが失敗します。通常、`/ignore_site_test_failure` オプションを含めると、テストの失敗は無視され、アップグレードが続行されます。（例外については、SQL Server のバージョンチェック を参照してください。）

複数のControllerをアップグレードする場合

あるControllerでアップグレードを開始し、その後、同じサイト内の別のControllerでアップグレードを開始した場合（最初のアップグレードが完了する前）：

- 最初のControllerで予備サイトテストが完了している場合、他のControllerのウィザードには予備サイトテストページは表示されません。
- 最初のControllerでのテストが進行中に他のControllerでアップグレードを開始した場合、他のControllerのウィザードにサイトテストページが表示されます。ただし、最初のControllerでのテストが完了すると、最初のControllerからのテスト結果のみが保持されます。

サイトの健全性に関連しないテストの失敗

- 予備サイトテストがメモリ不足で失敗した場合は、より多くのメモリを確保してからテストを再実行してください。
- アップグレードの権限はあるが、サイトテストを実行する権限がない場合、予備サイトテストは失敗します。これを解決するには、テストを実行する権限を持つユーザーアカウントでインストーラーを再実行してください。

SQL Serverバージョンの確認

Citrix Virtual Apps and Desktopsの展開を成功させるには、サイト、モニター、および構成ログデータベース用にサポートされているバージョンのMicrosoft SQL Serverが必要です。サポートされなくなったSQL ServerバージョンでCitrix展開をアップグレードすると、機能上の問題が発生する可能性があり、サイトはサポート対象外となります。

アップグレード先のCitrixリリースでサポートされているSQL Serverのバージョンについては、そのリリースのシステム要件 の記事を参照してください。

Controllerをアップグレードする際、Citrixインストーラーは、サイト、モニター、および構成ログデータベースに使用されている現在インストールされているSQL Serverのバージョンをチェックします。

- チェックの結果、現在インストールされているSQL Serverのバージョンが、アップグレード先のCitrixリリースでサポートされているバージョンではないと判断された場合：
  - グラフィカルインターフェイス：アップグレードはメッセージとともに停止します。「**了解**」をクリックし、次に「**キャンセル**」をクリックしてCitrixインストーラーを閉じます。（アップグレードを続行することはできません。）
  - コマンドラインインターフェイス: コマンドは失敗します (コマンドに `/ignore_db_check_failure` オプションを含めた場合でも)。

  SQL Server のバージョンをアップグレードしてから、Citrix のアップグレードを再度開始します。
- チェックで現在インストールされている SQL Server のバージョンを特定できない場合は、現在インストールされているバージョンがアップグレード先のバージョンでサポートされているかどうかを確認してください (システム要件)。
  - グラフィカルインターフェイス: アップグレードがメッセージとともに停止します。
    - 現在インストールされている SQL Server のバージョンがサポートされている場合は、 をクリックしてメッセージを閉じ、 をクリックして Citrix のアップグレードを続行します。
    - 現在インストールされている SQL Server のバージョンがサポートされていない場合は、 をクリックしてメッセージを閉じ、 をクリックして Citrix のアップグレードを終了します。SQL Server をサポートされているバージョンにアップグレードしてから、Citrix のアップグレードを再度開始します。
  - コマンドラインインターフェイス: コマンドがメッセージとともに失敗します。メッセージを閉じた後:

- 現在インストールされている SQL Server のバージョンがサポートされている場合は、`/ignore_db_check_failure` オプションを指定してコマンドを再度実行します。
- 現在インストールされている SQL Server のバージョンがサポートされていない場合は、SQL Server をサポートされているバージョンにアップグレードします。コマンドを再度実行して Citrix のアップグレードを開始します。

SQL Server のアップグレード

新しい SQL Server を起動してサイトデータベースを移行する場合は、接続文字列を更新する必要があります。

サイトが現在、サイトデータベースに SQL Server Express (Citrix がサイト作成時に自動的にインストールしたもの) を使用している場合:

1. 最新の SQL Server Express バージョンをインストールします。
2. データベースをデタッチします。
3. データベースを新しい SQL Server Express にアタッチします。
4. 接続文字列を移行します。

詳細については、「接続文字列の構成」およびMicrosoft SQL Serverの製品ドキュメントを参照してください。

SQL Server Express LocalDBを置き換える

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

CitrixはSQL Server Express LocalDBを自動的に更新しません。SQL Server Express LocalDBのバージョンを更新するには、このセクションのガイダンスに従ってください。

- Delivery ControllerをCitrix Virtual Apps and Desktopsバージョン2203 LTSR以降のバージョンにアップグレードする場合、サポートされるバージョンはSQL Server Express LocalDB 2019またはSQL Server Express LocalDB 2022です。

必要なもの:

- Citrix Virtual Apps and Desktopsのインストールメディア。
- Windows SysinternalsツールボックスのPsExecツール。

手順:

1. Citrix Virtual Apps and Desktopsのコンポーネント、データベース、およびサイトのアップグレードを完了します。（これらのデータベースアップグレードは、サイト、監視、および構成ログデータベースに影響します。SQL Server Express LocalDBを使用するローカルホストキャッシュデータベースには影響しません。）
2. SQL Server Express LocalDBを更新したいDelivery Controllerにログオンします。
3. MicrosoftからPsExecをダウンロードし、そのDelivery Controller上のアクセスしやすい場所（例: C:\Temp）に配置します。
4. Windowsシステムサービスから、Delivery Controller上のCitrix High Availability Serviceを停止します。
5. Delivery Controllerでコマンドプロンプトを開き、PsExecがある場所（例: `C:\Temp`）に移動して、次のコマンドを実行し、Network Serviceアカウントでコマンドプロンプトを昇格させます。

   ```
   psexec -i -u "NT AUTHORITY\NETWORKSERVICE" cmd
   ```

6. `whoami`を実行して、コマンドプロンプトがNetwork Serviceアカウントとして実行されていることを確認します。次の出力が表示されるはずです: `nt authority\networkservice`。
7. コマンドプロンプトを使用して、SQL LocalDBインスタンスに移動します:

   - SQL LocalDB 2014からアップグレードする場合:

     ```
     cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
     ```

   - SQL LocalDB 2017からアップグレードする場合:

     ```
     cd "C:\Program Files\Microsoft SQL Server\140\Tools\Binn"
     ```

   - SQL LocalDB 2019からアップグレードする場合:

     ```
     cd "C:\Program Files\Microsoft SQL Server\150\Tools\Binn"
     ```

8. SQL LocalDBインスタンスを停止して削除します: `CitrixHA`。

   ```
   SqlLocalDB stop CitrixHA
   ```

```
SqlLocalDB delete CitrixHA
```

9. Delivery Controllerから以下のファイルを削除します:

```
C:\Windows\ServiceProfiles\NetworkService\HADatabaseName.*

C:\Windows\ServiceProfiles\NetworkService\HADatabaseName_log.*

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName.* (if
exists)

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName_log.*
(if exists)
```

10. プログラムを削除するためのWindowsのネイティブ機能を使用して、既存のSQL LocalDB SQL Server ExpressをDelivery Controllerからアンインストールします。
11. アンインストールが完了したら、Delivery Controllerを再起動します。
12. Windowsシステムサービスから、Delivery Controller上のCitrix High Availability Serviceを停止します。
13. Citrix Virtual Apps and Desktopsインストールメディアを Delivery Controllerにマウントします。
14. Delivery ControllerにSQL Server Express LocalDB 2022を管理者としてインストールします。
    a. Citrix Virtual Apps and Desktopsインストールメディアの `Support > SQLLocalDB` フォルダーにある `sqllocaldb.msi` ファイルを使用します。たとえば、インストールメディアが `E drive` ドライブにマウントされている場合、ファイルは `E:\Support\SQLLocalDB\sqllocaldb.msi` にあります。インストールを完了するには再起動が必要です。
    b. 新しいSQL LocalDBは `C:\Program Files\Microsoft SQL Server\160\Tools\Binn` にある必要があります。
15. Windowsシステムサービスから、Delivery Controller上のCitrix High Availability Serviceを開始します。
16. Delivery Controller のコマンドプロンプトで、`C:\Program Files\Microsoft SQL Server\160\Tools\Binn` に移動し、`SqlLocalDB i` を実行して、CitrixHA インスタンスが

作成されたことを確認します。返されたインスタンスのリストに `CitrixHA` が含まれている必要があります。

> **注記：**
>
> Citrix High Availability Service の開始後、CitrixHA データベースが作成されるまでに最大15分かかる場合があります。

17. ローカルホストキャッシュデータベースファイルが作成されていることを確認し、必要に応じて高可用性サービス（セカンダリブローカー）が引き継ぐことができることを確認します。
    a. Delivery Controller で、`C:\Windows\ServiceProfiles\NetworkService` に移動します。
    b. `HaDatabaseName.mdf` と `HaDatabaseName_log.ldf` が作成されていることを確認します。
18. 残りの Delivery Controller で手順を繰り返します。

VDAアップグレードエージェントのプロキシサポート

VDAアップグレードエージェントのプロキシサポートは、2311 VDAで追加されました。

2311 VDA (バージョン: 7.40) のVDAアップグレードエージェントは、プロキシを介してトラフィックを認識し、送信できます。

VDAアップグレードエージェント (VUA) は、Hostname:Port (IP:Port) およびPACファイルの形式でプロキシをサポートしています。

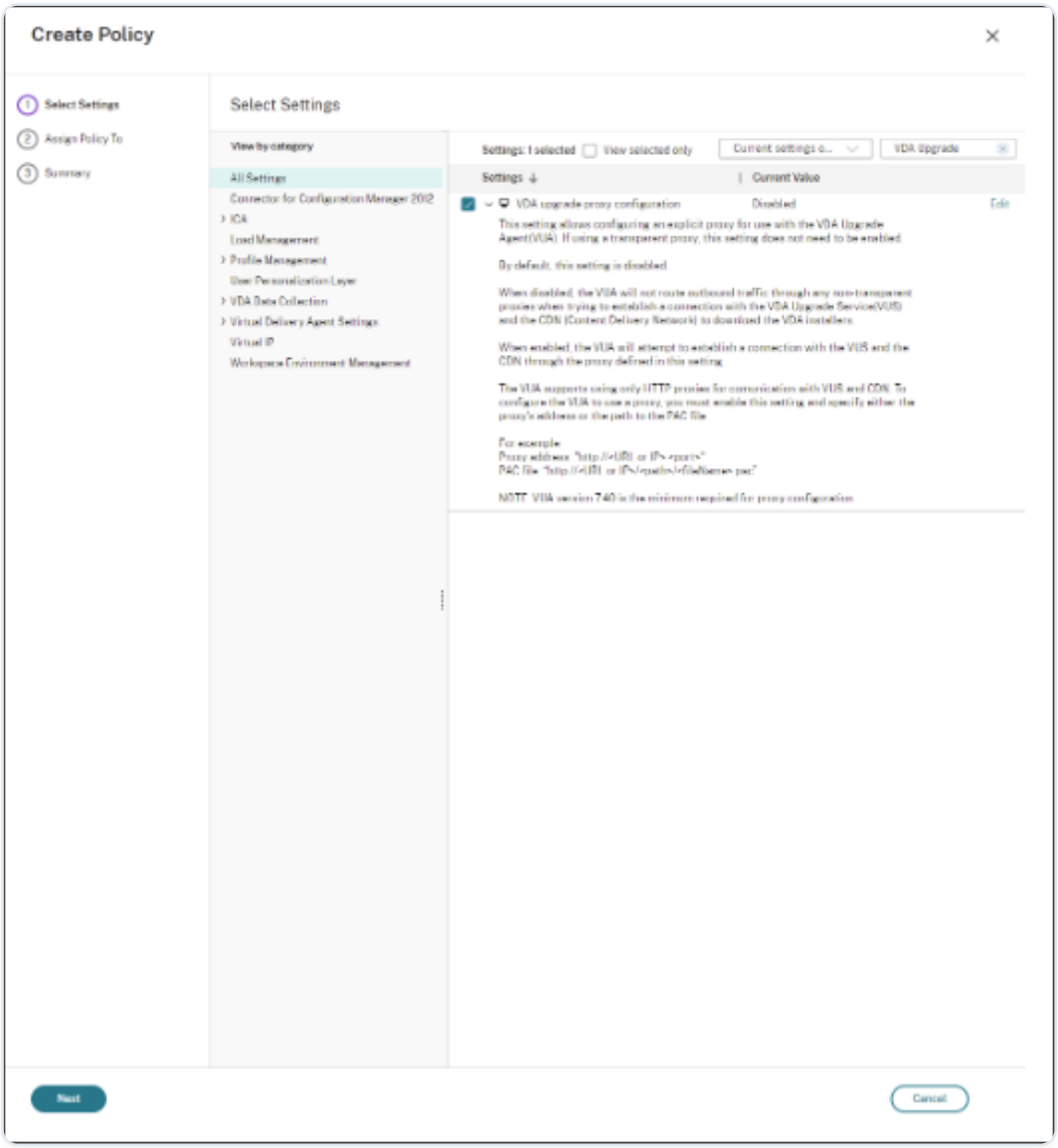
HTTPプロキシのみがサポートされています。 パケットの復号化と検査はサポートされていません。

プロキシ認証はサポートされていません。 SOCKS5はサポートされていません。

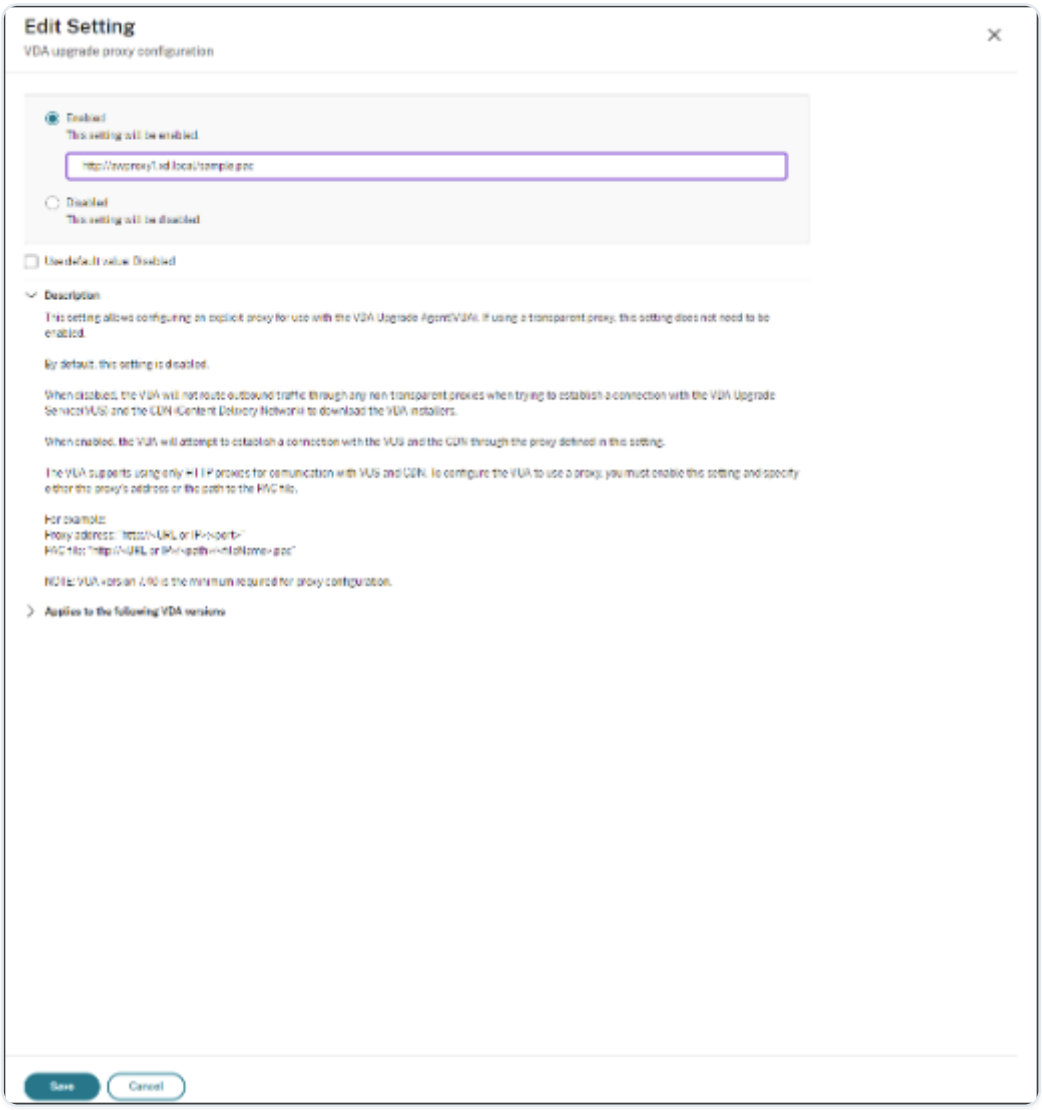
VDAアップグレードエージェントプロキシの構成

VDAアップグレードエージェントプロキシは、次の2つの方法で構成できます。

1. **Webstudioポリシー**を使用した**VDAアップグレードエージェントポリシーの構成**。
2. **ポリシーの作成**ページで、**設定**から**VDAアップグレードプロキシ構成**を選択します。



3. この設定を有効にします。デフォルトでは、この設定は無効になっています。



4. レジストリキーを使用したVDAアップグレードエージェントの構成。

   レジストリキーは、VDAインストール中にMeta-Installerに設定されます。

   レジストリ:

   キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`

   値の型: 文字列

   値の名前: ProxySettings

   値のデータ: プロキシアドレスまたはPACファイルへのパス。

   例:

   a. プロキシアドレス: `http://<URL or IP>:<port>`
   b. PACファイル: `http://<URL or IP>/<path/<filename>.pac`

セキュリティ

Citrix Virtual Apps and Desktops™ は、セキュリティニーズに合わせて環境を調整できる、設計段階から安全なソリューションを提供します。

IT部門がモバイルワーカーに関して直面するセキュリティ上の懸念の1つは、データの紛失または盗難です。Citrix Virtual Apps and Desktopsは、アプリケーションとデスクトップをホストすることで、すべてのデータをデータセンターに保持し、機密データと知的財産をエンドポイントデバイスから安全に分離します。データ転送を許可するポリシーが有効になっている場合、すべてのデータは暗号化されます。

Citrix Virtual Apps and Desktops のデータセンターは、一元化された監視および管理サービスにより、インシデント対応も容易にします。Director を使用すると、IT部門はネットワーク全体でアクセスされているデータを監視および分析でき、Studio を使用すると、IT部門は各エンドユーザーデバイスでローカルに問題を修正する代わりに、データセンター内のほとんどの脆弱性にパッチを適用して対処できます。

Citrix Virtual Apps and Desktops は、監査と規制コンプライアンスも簡素化します。調査官は、一元化された監査証跡を使用して、誰がどのアプリケーションとデータにアクセスしたかを判断できるためです。Director は、構成ログと OData API にアクセスすることで、システムへの更新とユーザーデータ使用に関する履歴データを収集します。

委任管理を使用すると、Citrix Virtual Apps and Desktops へのアクセスをきめ細かく制御するための管理者ロールを設定できます。これにより、組織内で柔軟性が生まれ、特定の管理者にタスク、操作、スコープへのフルアクセスを許可し、他の管理者には制限されたアクセスを許可できます。

Citrix Virtual Apps and Desktops は、ネットワークのさまざまなレベル（ローカルレベルから組織単位レベルまで）でポリシーを適用することにより、管理者にユーザーに対するきめ細かな制御を提供します。このポリシー制御により、ユーザー、デバイス、またはユーザーとデバイスのグループが接続、印刷、コピー/貼り付け、またはローカルドライブのマッピングを行えるかどうかが決定され、サードパーティの臨時作業者に関するセキュリティ上の懸念を最小限に抑えることができます。管理者は、デスクトップロック機能も使用して、エンドユーザーが仮想デスクトップのみを使用できるようにし、エンドユーザーデバイスのローカルオペレーティングシステムへのアクセスを防止できます。

管理者は、サイトを構成して、Controller の Transport Layer Security (TLS) プロトコル、またはエンドユーザーと Virtual Delivery Agents (VDA) 間の TLS プロトコルを使用するようにすることで、Citrix Virtual Apps または Citrix Virtual Desktops のセキュリティを強化できます。このプロトコルは、TCP/IP 接続のサーバー認証、データストリーム暗号化、およびメッセージ整合性チェックを提供するために、サイトで有効にすることもできます。

Citrix Virtual Apps and Desktops は、Windows または特定のアプリケーションの多要素認証もサポートしています。多要素認証は、Citrix Virtual Apps and Desktops によって提供されるすべてのリソースを管理するためにも使用できます。これらの方法には以下が含まれます。

- トークン
- スマートカード
- RADIUS
- ケルベロス
- 生体認証

Citrix Virtual Desktops は、ID管理からウイルス対策ソフトウェアまで、多くのサードパーティ製セキュリティソリューションと統合できます。サポートされている製品のリストは `<http://www.citrix.com/ready>` で確認できます。

Citrix Virtual Apps and Desktops の特定のリリースは、Common Criteria 標準の認定を受けています。これらの標準のリストについては、`<https://www.commoncriteriaportal.org/cc/>` にアクセスしてください。

FIDO2認証

FIDO2およびWebAuthnを使用したローカル認証と仮想認証

ユーザーは、FIDO2 セキュリティキーと、TPM 2.0 および Windows Hello を搭載した統合生体認証デバイスを使用して、仮想セッション内で FIDO2 または WebAuthn を利用するアプリケーションに認証できます。

FIDO2の詳細については、「FIDO2: WebAuthn & CTAP」を参照してください。

この機能の使用方法については、「FIDO2 リダイレクト」を参照してください。

> **注**

この機能は、WebAuthnまたはFIDO2を使用した仮想セッションへのログオンをサポートしていません。この機能は、仮想セッション内のアプリケーションでこれらの認証方法を使用することのみを許可します。

この機能は、ダブルホップシナリオではサポートされていません。

サポートマトリックス

セッションホストオペレーティングシステム	WEBアプリケーション認証	UWPアプリケーション認証
ウィンドウズ サーバー 2016	USB リダイレクト経由でサポート	サポートされていません
ウィンドウズ サーバー 2019	サポートされています	サポートされていません
ウィンドウズ サーバー 2022	サポートされています	サポートされています
ウィンドウズ 10	サポートされています	サポートされています
ウィンドウズ 11	サポートされています	サポートされています

詳細については、以下の要件を確認してください。

Webアプリケーション認証

要件

WebアプリケーションでFIDO2およびWebAuthn認証を使用するための要件は次のとおりです。

Citrix® コントロールプレーン

- Citrix Virtual Apps and Desktops™ 2009以降のバージョン

セッションホスト

- オペレーティングシステム
  - Windows 10 1809以降
  - Windows Server 2019以降のバージョン
- VDA

- Windows: バージョン2009以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Linux: Workspace app for Linuxのシステム要件を参照してください。
- Workspaceアプリ
  - Windows: バージョン2009.1以降
  - Linux: 2303以降

Webブラウザーの要件

- 32ビットおよび64ビットブラウザ

サポートされる認証方法

- FIDO2セキュリティキー
- ウィンドウズ ハロー
  - TPM 2.0
  - 統合生体認証
    - 顔認識
    - 指紋スキャナー
  - WebAuthn

UWPアプリケーション認証

Citrix Virtual Apps and Desktops 2112のリリースにより、CitrixはUWPアプリケーションでのWebAuthnおよびFIDO2認証をサポートします。

Microsoft Teams、Microsoft Outlook for Office 365、OneDriveなどのアプリケーションは、Azure Active Directoryへのリンクとして認証にUWPアプリケーションを使用します。Citrixは現在、これらのアプリケーションの認証にFIDO2を使用することをサポートしています。

要件

UWPアプリケーションでFIDO2およびWebAuthn認証を使用するための要件は次のとおりです。

Citrixコントロールプレーン

- シトリックス バーチャル アプリ アンド デスクトップ 2112 以降

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ サーバー 2022 以降
- VDA
  - Windows: バージョン2112以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Linux: Workspace app for Linuxのシステム要件を参照してください。
- Workspaceアプリ
  - Windows: バージョン2009.1以降
  - Linux: 2303以降

UWPアプリケーションの要件

- 32 ビットおよび 64 ビットアプリケーション

サポートされる認証方法

- FIDO2セキュリティキー
- Windows ハロー
  - TPM 2.0
  - 統合生体認証
    - 顔認識
    - 指紋スキャナー
  - WebAuthn

注：

クライアント、VDA、またはオペレーティングシステムで機能がサポートされていないためにFIDO2リダイレクトが利用できないシナリオでは、USBベースのFIDO2キーをUSBリダイレクトを使用してリダイレクトできます。 FIDO2リダイレクトが利用可能なシナリオでも、USBリダイレクトを使用してUSBベースのFIDO2キーをリダイレクトできます。この場合、FIDO2リダイレクトを無効にし、適切なUSBリダイレクトルールを構成する必要があります。 USBリダイレクトルールを使用してFIDO2キーを構成する方法の詳細については、USBリダイレクトデバイスルールのドキュメントを参照してください。

msedgewebview2.exeベースのアプリケーションの高度な構成

注：

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

msedgewebview2.exeベースのWebアプリケーションを使用している企業の場合、HDXセッション内でFIDO2リダイレクトを機能させるには、VDAに追加のレジストリ値を追加する必要があります。

AllowProcesses レジストリ値に msedgewebview2.exe のフルパスを追加します。

- キー: HKLM\SOFTWARE\Citrix\WebAuthnAllowedProcesses
- 値の名前: AllowProcesses
- 値の型: REG_MULTISZ
- 値のデータ: `<add full path of the msedgewebview2.exe here >`

64ビットアプリケーションの場合、以下の値を設定する必要があります。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\msedgewebview2
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook

- 値の名前: FilePathName
- 値の型: REG_SZ
- 値のデータ: C:\Program Files\Citrix\HDX\bin\CtxWebAuthnHook.dll
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: Flag
- 値の型: DWORD
- 値のデータ: 00000002

32ビットアプリケーションの場合、以下の値を設定する必要があります。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: FilePathName
- 値の型: REG_SZ
- 値のデータ: C:\Program Files\Citrix\HDX\bin\CtxWebAuthnHook.dll
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: Flag
- 値の型: DWORD
- 値のデータ: 00000002

msedgewebview2.exeベースのアプリケーションでFIDO2リダイレクトを有効にするには、レジストリ値を設定した後、VDAを再起動します。

シトリックス バーチャル アプリケーションズ アンド デスクトップ™ と シトリックス ゲートウェイ を統合する

StoreFront™ サーバーは、公開されたリソースとデータへのアクセスを管理するために展開および構成されます。リモートアクセスの場合、StoreFront の前に Citrix Gateway を追加することをお勧めします。

> **注:**

> Citrix Virtual Apps and Desktops と Citrix Gateway を統合する方法の詳細な構成手順については、StoreFront ドキュメントを参照してください。

> 次の図は、Citrix Gateway を含む簡素化された Citrix 展開の例を示しています。Citrix Gateway は StoreFront と通信し、Citrix Virtual Apps and Desktops によって提供されるアプリとデータを保護します。ユーザーデバイスは Citrix Workspace™ アプリを実行して、安全な接続を作成し、アプリ、デスクトップ、ファイルにアクセスします。

Citrix Gateway を含む簡素化された Citrix 展開(/en-us/citrix-virtual-apps-desktops/2411/media/sample-deployment-overview.png)

ユーザーは Citrix Gateway を使用してログオンし、認証します。Citrix Gateway は DMZ に展開され、保護されています。2 要素認証が構成されています。ユーザー資格情報に基づいて、ユーザーには関連するリソースとアプリケーションが提供されます。アプリケーションとデータは適切なサーバー上にあります（図には示されていません）。セキュリティ上機密性の高いアプリケーションとデータには、個別のサーバーが使用されます。

セキュリティに関する考慮事項とベストプラクティス

> **注:**
>
> 組織は、規制要件を満たすために特定のセキュリティ標準に準拠する必要がある場合があります。このようなセキュリティ標準は時間とともに変化するため、このドキュメントではこの主題については扱いません。セキュリティ標準とCitrix製品に関する最新情報については、Citrix Trust Centerを参照してください。

ファイアウォール

環境内のすべてのマシンを、必要に応じてエンクレーブ境界を含め、境界ファイアウォールで保護します。

環境内のすべてのマシンは、パーソナルファイアウォールによって保護されている必要があります。コアコンポーネントとVDAをインストールする際、Windowsファイアウォールサービスが検出された場合（ファイアウォールが有効になっていない場合でも）、コンポーネントと機能の通信に必要なポートを自動的に開くように選択できます。これらのファイアウォールポートを手動で構成することもできます。別のファイアウォールを使用する場合は、手動で構成する必要があ

ります。必要なポートの詳細については、Tech Paper: Communication Ports Used by Citrix Technologiesを参照してください。

従来の環境をこのリリースに移行する場合、既存の境界ファイアウォールの再配置や新しい境界ファイアウォールの追加が必要になる場合があります。たとえば、データセンター内の従来のクライアントとデータベースサーバーの間に境界ファイアウォールがあるとします。このリリースを使用する場合、その境界ファイアウォールは、仮想デスクトップとユーザーデバイスが一方にあり、データセンター内のデータベースサーバーとDelivery Controllerがもう一方にあるように配置する必要があります。したがって、データセンター内にデータベースサーバーとControllerを収容するためのエンクレーブを作成することを検討してください。また、ユーザーデバイスと仮想デスクトップ間の保護も検討してください。

> **注:**
>
> TCPポート1494と2598はICAとCGPに使用されるため、データセンター外のユーザーがアクセスできるようにファイアウォールで開かれている可能性が高いです。Citrixは、管理インターフェイスが意図せず攻撃に対して開かれたままになる可能性を避けるため、これらのポートを他の目的で使用しないことを推奨します。ポート1494と2598は、Internet Assigned Number Authority (http://www.iana.org/) に正式に登録されています。

Delivery Controller™とのセキュアな通信

HTTPSを使用した通信の暗号化

StoreFrontとNetScaler Gatewayは、配信コントローラーで実行されているXMLサービスとHTTPまたはHTTPS経由で通信します。構成によっては、VDAはWebSocketを使用して配信コントローラーと通信する場合があります。Directorは、ODataを使用してHTTPまたはHTTPS経由で監視データと通信します。HTTPSを有効にし、HTTPを無効にすることをお勧めします。これには、Delivery ControllerでTLSを有効にする必要があります。

- StoreFrontをHTTPSを使用して接続するように構成するには、(/ja-jp/storefront/current-release/configure-manage-stores/manage-controllers#add-resource-feeds-for-citrix-virtual-apps-and-desktops)および(/ja-jp/storefront/current-release/integrate-with-citrix-gateway-and-citrix-adc/configure-citrix-gateway#add-citrix-gateway-appliance)を参照してください。
- NetScaler GatewayをHTTPSを使用してDelivery Controllerに接続するように構成するには、NetScaler GatewayでのSecure Ticket Authorityの構成を参照してください。

セキュリティキー

承認されたStoreFrontサーバーとNetScalerサーバーのみがクラウドコネクタ経由でDaaSに接続できるように、セキュリティキーを使用できます。これは、XML信頼を有効にしている場合に特に重要です。

XML信頼

デフォルトでは、StoreFrontが列挙や起動などのアクションのためにデリバリーコントローラーに接続する場合、DaaSがユーザーを認証し、ユーザーのグループメンバーシップを確認できるように、StoreFrontはユーザーのActive Directory資格情報を渡す必要があります。ただし、ドメインパススルー、スマートカード、SAMLなどの他の認証方法を使用する場合、StoreFrontはActive Directoryパスワードを持っていません。この場合、「XML信頼」を有効にする必要があります。XML信頼が有効になっている場合、Citrix Virtual Apps and Desktopsは、ユーザーのパスワードを検証することなく、アプリケーションの列挙や起動など、ユーザーに代わってStoreFrontがアクションを実行することを許可します。XML信頼を有効にする前に、セキュリティキーまたはファイアウォールやIPsecなどの別のメカニズムを使用して、信頼できるStoreFrontサーバーのみがデリバリーコントローラーに接続できるようにしてください。

XML信頼設定を確認、有効化、または無効化するには、Citrix Virtual Apps and Desktops PowerShell SDKを使用します。

- XML信頼設定の現在の値を確認するには、`Get-BrokerSite`を実行し、`TrustRequestsSentToTheXMLServicePort`の値を調べます。
- XML信頼を有効または無効にするには、パラメーター`TrustRequestsSentToTheXmlServicePort`を指定して`Set-BrokerSite`を実行します。

VDAとDelivery Controller間の通信

VDAがコントローラーと通信するためのメカニズムは2つあります。

- ウィンドウズ コミュニケーション ファンデーション

  Windows Communication Foundation (WCF) のメッセージレベル保護は、デリバリーコントローラーとVDA間の通信を保護します。これにより、TLSを使用した追加のトランスポートレベル保護の必要がなくなります。VDAとデリバリーコントローラー間の通信に使用されるデフォルトポートは80です。ただし、ポートをカスタマイズできます。詳細については、VDAのカスタマイズを参照してください。

  WCFにおけるメッセージセキュリティの詳細については、MicrosoftドキュメントWCFにおけるメッセージセキュリティを参照してください。

WCF構成では、ControllerとVDA間の相互認証にKerberosを使用します。暗号化には256ビットキーのCBCモードでAESを使用します。メッセージの整合性にはSHA-1を使用します。

Microsoftによると、WCFで使用されるセキュリティプロトコルは、WS-SecurityPolicy 1.2を含むOASIS（Organization for the Advancement of Structured Information Standards）の標準に準拠しています。また、Microsoftは、WCFがSecurity Policy 1.2に記載されているすべてのアルゴリズムスイートをサポートしていると述べています。

コントローラーとVDA間の通信には、前述のアルゴリズムを使用するbasic256アルゴリズムスイートが使用されます。

WCF構成では、メッセージレベルのセキュリティ暗号化とともに、SOAP over HTTPプロトコルを使用します。

- WebSockets

  これはWCFの最新の代替手段です。VDAからDelivery Controllerへの通信にはTLSポート443のみを使用するという利点があります。現在、MCSでプロビジョニングされたマシンでのみ利用可能です。詳細については、「VDAとDelivery Controller間のWebSocket通信」を参照してください。

Delivery ControllerとLicense Server間のセキュアな通信

Delivery ControllerはHTTPS経由でLicense Serverと通信します。デフォルトでは自己署名証明書を使用しますが、これをエンタープライズまたは公開証明機関によって発行された証明書に置き換えることをお勧めします。詳細については、「Citrix Licensing ManagerおよびWeb Services for Licensingで使用される証明書を手動でインストールする」を参照してください。

WebブラウザとWeb StudioおよびDirector間の通信を保護する

Web StudioとDirectorは、Delivery Controllerと同じマシン、または別のマシンにインストールできます。ユーザーはWebブラウザを使用してWeb StudioとDirectorに接続します。デフォルトでは、Web Studioは自己署名証明書を使用してHTTPSを有効にしますが、スタンドアロンでインストールされたDirectorはHTTPSを構成しません。適切な証明書を使用して、Web StudioおよびDirectorでTLSを有効にすることをお勧めします。

ICA®通信の保護

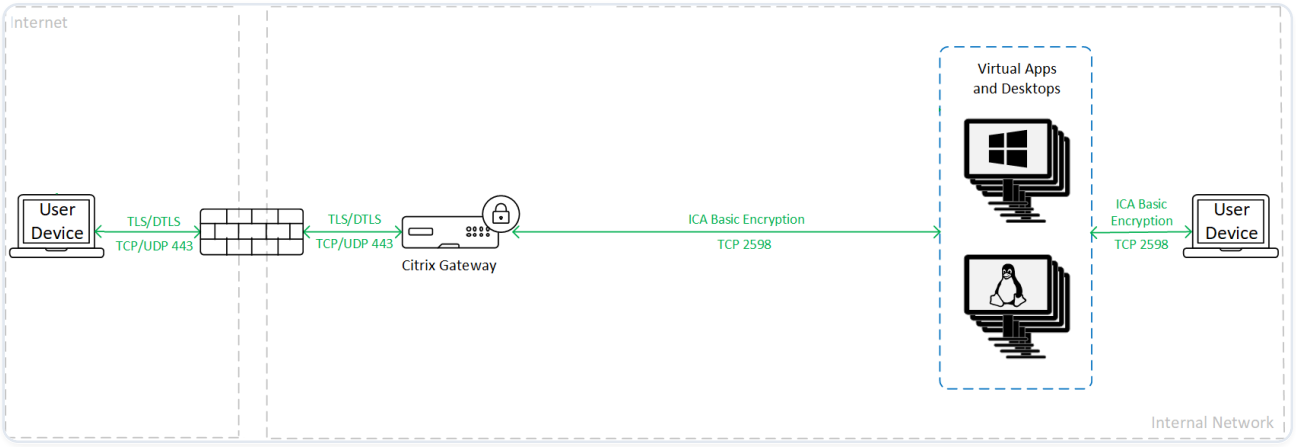
Citrix Virtual Apps and Desktops™は、クライアントとVDA間のICAトラフィックを保護するためのいくつかのオプションを提供します。利用可能なオプションは次のとおりです。

- **基本暗号化:** デフォルト設定です。

- **SecureICA:** RC5 (128ビット) 暗号化を使用してセッションデータを暗号化できます。
- **VDA TLS/DTLS:** TLS/DTLSを使用してネットワークレベルの暗号化を可能にします。

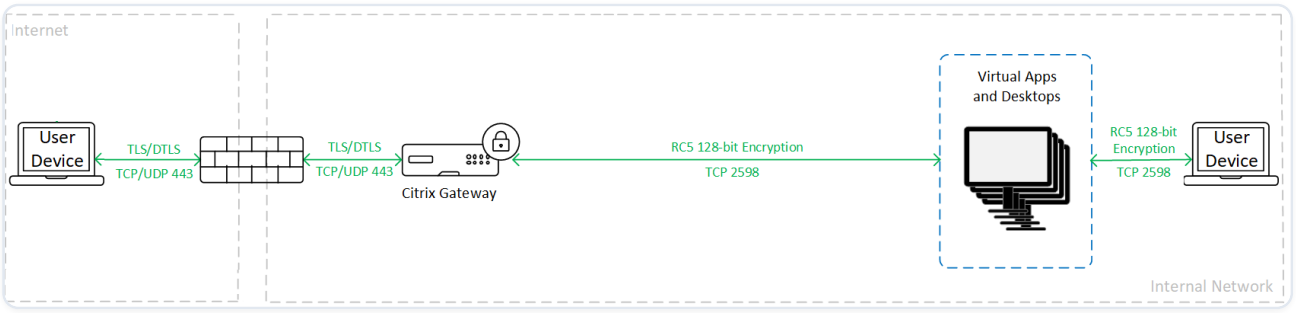
基本暗号化

基本暗号化を使用する場合、トラフィックは次の図に示すように暗号化されます。



SecureICA

SecureICAを使用する場合、トラフィックは次の図に示すように暗号化されます。



詳細については、「セキュリティポリシー設定」を参照してください(/ja-jp/citrix-virtual-apps-desktops/2411/policies/reference/ica-policy-settings/security-policy-settings.html)。

> **注1：**

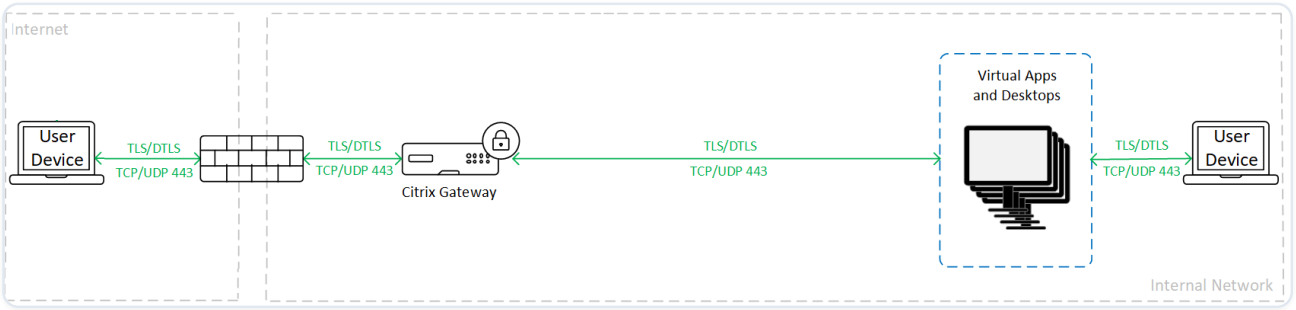
> SecureICAは、Workspace app for HTML5ではサポートされていません。

> **注2：**

> Citrix SecureICAはICA/HDXプロトコルの一部ですが、Transport Layer Security (TLS) のような標準準拠のネットワークセキュリティプロトコルではありません。

VDA TLS/DTLS

VDA TLS/DTLS暗号化を使用する場合、トラフィックは次の図に示すように暗号化されます。



VDA TLS/DTLSを構成するには、「VDA上のTLS設定」を参照してください(/ja-jp/citrix-virtual-apps-desktops/2411/secure/tls-vda)。

仮想チャネル

環境で許可されるCitrix以外の仮想チャネルを制御するには、「仮想チャネル許可リスト」を使用します(/ja-jp/citrix-virtual-apps-desktops/2411/secure/virtual-channel-security)。

印刷サーバーとの安全な通信

Virtual Delivery Agent (VDA) とUniversal Print Server間のTCPベースの接続にTLSを有効にできます。詳細については、「Universal Print ServerでのTransport Layer Security (TLS)」を参照してください(/ja-jp/citrix-virtual-apps-desktops/2411/secure/tls-ups)。

サイトデータベースとのセキュアな通信

サイトデータベースへのTLSの有効化については、「CTX137556」を参照してください。

VDAマシンのセキュリティ

一般的な推奨事項

VDAを最新のオペレーティングセキュリティ更新プログラムとウイルス対策で常に最新の状態に保つようにしてください。

アプリケーションのセキュリティ

管理者以外のユーザーが悪意のある操作を実行するのを防ぐため、Citrix®は、VDAホスト上のインストーラー、アプリケーション、実行可能ファイル、およびスクリプトに対してWindows AppLockerルールを構成することを推奨します。

8.3形式のファイル名

VDAで8.3形式のファイル名を無効にできます。Microsoft fsutil documentationを参照してください。

データストレージに関する考慮事項

デスクトップ環境は、プールされたデスクトップや専用デスクトップなど、さまざまな種類のデスクトップで構成されている場合があります。ユーザーは、プールされたデスクトップなど、ユーザー間で共有されるデスクトップにデータを保存してはなりません。ユーザーが専用デスクトップにデータを保存した場合、そのデスクトップが後で他のユーザーに利用可能になった場合は、そのデータを削除する必要があります。

ユーザーアカウント管理

アカウント管理にはWindowsのベストプラクティスを適用してください。Machine Creation ServicesまたはProvisioning Servicesによって複製される前に、テンプレートまたはイメージ上にアカウントを作成しないでください。保存された特権ドメインアカウントを使用してタスクをスケジュールしないでください。共有Active Directoryマシンアカウントを手動で作成しないでください。これらの慣行は、マシン攻撃がローカルの永続的なアカウントパスワードを取得し、それらを使用して他のユーザーに属するMCS/PVS共有イメージにログオンするのを防ぐのに役立ちます。

ユーザーには、必要な機能のみを付与してください。Microsoft Windowsの特権は、通常の方法でデスクトップに引き続き適用されます。つまり、ユーザー権利の割り当てを通じて特権を構成し、グループポリシーを通じてグループメンバーシップを構成します。このリリースの一つの利点は、デスクトップが保存されているコンピューターに対する物理的な制御を付与することなく、ユーザーにデスクトップへの管理者権限を付与できることです。

デスクトップの特権を計画する際には、次の点に注意してください。

- デフォルトでは、非特権ユーザーがデスクトップに接続すると、自身のユーザーデバイスのタイムゾーンではなく、デスクトップを実行しているシステムのタイムゾーンが表示されます。ユーザーがデスクトップを使用する際にローカルタイムを表示できるようにする方法については、「デリバリーグループの管理」の記事を参照してください。
- デスクトップの管理者であるユーザーは、そのデスクトップを完全に制御できます。デスクトップが専用デスクトップではなくプールされたデスクトップである場合、そのユーザーは、将来のユーザーを含むそのデスクトップの他のすべてのユーザーに対して信頼されなければなりません。デスクトップのすべてのユーザーは、この状況によってデータセキュリティに潜在的に永続的なリスクがあることを認識する必要があります。この考慮事項は、単一のユーザー

のみが使用する専用デスクトップには適用されません。そのユーザーは、他のどのデスクトップでも管理者であってはなりません。

- デスクトップの管理者であるユーザーは、悪意のある可能性のあるソフトウェアを含め、そのデスクトップにソフトウェアを一般的にインストールできます。また、そのユーザーは、デスクトップに接続されている任意のネットワーク上のトラフィックを監視または制御できる可能性もあります。

ログオン権限を管理する

ログオン権限は、ユーザーアカウントとコンピューターアカウントの両方に必要です。Microsoft Windowsの特権と同様に、ログオン権限は通常の方法でデスクトップに適用され続けます。ユーザー権利の割り当てを通じてログオン権限を構成し、グループポリシーを通じてグループメンバーシップを構成します。

Windowsのログオン権限は、ローカルログオン、リモートデスクトップサービス経由のログオン、ネットワーク経由のログオン（ネットワークからこのコンピューターにアクセス）、バッチジョブとしてログオン、サービスとしてログオンです。

コンピューターアカウントの場合、コンピューターが必要とするログオン権限のみを付与します。ログオン権限「ネットワークからこのコンピューターにアクセス」は、デリバリーコントローラーのコンピューターアカウントに必要です。

ユーザーアカウントの場合、ユーザーには必要なログオン権限のみを付与します。

Microsoftによると、デフォルトではRemote Desktop Usersグループにログオン権限「リモートデスクトップサービス経由のログオンを許可」が付与されています（ドメインコントローラーを除く）。

組織のセキュリティポリシーによっては、このグループをそのログオン権限から削除すべきであると明示的に規定している場合があります。次のアプローチを検討してください。

- マルチセッションOS用Virtual Delivery Agent (VDA)は、Microsoft Remote Desktop Servicesを使用します。Remote Desktop Usersグループを制限付きグループとして構成し、Active Directoryグループポリシーを介してグループのメンバーシップを制御できます。詳細については、Microsoftのドキュメントを参照してください。
- シングルセッションOS用VDAを含むCitrix Virtual Apps and Desktopsの他のコンポーネントでは、Remote Desktop Usersグループは不要です。したがって、これらのコンポーネントでは、Remote Desktop Usersグループにログオン権限「リモートデスクトップサービス経由のログオンを許可」は不要であり、削除できます。さらに、次の点に注意してください。

- リモートデスクトップサービスを介してそれらのコンピューターを管理する場合、そのようなすべての管理者がすでにAdministratorsグループのメンバーであることを確認してください。
- リモートデスクトップサービスを介してそれらのコンピューターを管理しない場合、それらのコンピューターでリモートデスクトップサービス自体を無効にすることを検討してください。

ログオン権限「リモートデスクトップサービス経由のログオンを拒否」にユーザーとグループを追加することは可能ですが、拒否ログオン権限の使用は一般的に推奨されません。詳細については、Microsoftのドキュメントを参照してください。

Delivery Controllerのセキュリティ

Delivery Controller上のWindowsサービス

Delivery Controllerのインストールにより、以下のWindowsサービスが作成されます。

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService): VM 用の Microsoft Active Directory コンピューターアカウントを管理します。
- Citrix Analytics (NT SERVICE\CitrixAnalytics): サイト管理者によってこの収集が承認されている場合、Citrix が使用するサイト構成の使用状況情報を収集します。その後、製品の改善に役立てるため、この情報を Citrix に送信します。
- Citrix App Library (NT SERVICE\CitrixAppLibrary): AppDisk の管理とプロビジョニング、AppDNA 統合、および App-V の管理をサポートします。
- Citrix Broker Service (NT SERVICE\CitrixBrokerService): ユーザーが利用できる仮想デスクトップまたはアプリケーションを選択します。
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging): 管理者によってサイトに対して行われたすべての構成変更およびその他の状態変更を記録します。
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService): 共有構成用のサイト全体のレポジトリ。
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin): 管理者に付与された権限を管理します。
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest): 他の Delivery Controller サービスの自己テストを管理します。
- Citrix Host Service (NT SERVICE\CitrixHostService): Citrix Virtual Apps または Citrix Virtual Desktops 展開で使用されるハイパーバイザーインフラストラクチャに関する情報を格納し、

コンソールがハイパーバイザープール内のリソースを列挙するために使用する機能も提供します。

- Citrix Machine Creation Services (NT SERVICE\CitrixMachineCreationService): デスクトップ VM の作成をオーケストレーションします。
- Citrix Monitor Service (NT SERVICE\CitrixMonitor): Citrix Virtual Apps または Citrix Virtual Desktops のメトリックを収集し、履歴情報を格納し、トラブルシューティングツールとレポートツール用のクエリインターフェイスを提供します。
- Citrix StoreFront Service (NT SERVICE\ CitrixStorefront): StoreFront の管理をサポートします。(StoreFront コンポーネント自体の一部ではありません。)
- Citrix StoreFront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService): StoreFrontの特権管理操作をサポートします。(StoreFrontコンポーネント自体の一部ではありません。)
- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService): メインサイトデータベースからローカルホストキャッシュに構成データを伝播します。
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService): メインサイトデータベースが利用できない場合に、ユーザーが利用できる仮想デスクトップまたはアプリケーションを選択します。

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これらは、他のCitrixコンポーネントと一緒にインストールされた場合にも作成されます。

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc): Citrixサポートが使用する診断情報の収集をサポートします。
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService): Citrixによる分析のために診断情報を収集し、管理者が分析結果と推奨事項を表示してサイトの問題の診断に役立てられるようにします。

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これは現在使用されていません。有効になっている場合は、無効にしてください。

- Citrix リモート ブローカー プロバイダー (NT SERVICE\XaXdCloudProxy)

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これらは現在使用されていませんが、有効にする必要があります。無効にしないでください。

- Citrix オーケストレーション サービス (NT SERVICE\CitrixOrchestration)
- Citrix トラスト サービス (NT SERVICE\CitrixTrust)

Citrix StoreFront™ Privileged Administration Serviceを除き、これらのサービスには「サービスとしてログオン」のログオン権限と、「プロセスのメモリクォータの調整」、「セキュリティ監査の生成」、「プロセスレベルトークンの置き換え」の特権が付与されています。これらのユーザー権限を変更する必要はありません。これらの特権はDelivery Controllerでは使用されず、自動的に無効になります。

Citrix StoreFront Privileged AdministrationサービスとCitrix Telemetry Serviceを除き、前述のDelivery Controller WindowsサービスはNETWORK SERVICE IDとしてログオンするように構成されています。これらのサービス設定を変更しないでください。

Citrix Config Synchronizer Service は、Delivery Controller 上のローカル管理者グループに NETWORK SERVICE アカウントが属している必要があります。これにより、ローカルホストキャッシュが正しく機能します。

Citrix StoreFront Privileged Administration サービスは、ローカルシステム (NT AUTHORITY\SYSTEM) としてログオンするように構成されています。これは、通常サービスでは利用できない Delivery Controller StoreFront の操作 (Microsoft IIS サイトの作成を含む) に必要です。サービス設定を変更しないでください。

Citrix Telemetry Service は、サービス固有の ID としてログオンするように構成されています。

Citrix Telemetry Service は無効にできます。このサービスと、すでに無効になっているサービスを除き、これらの Delivery Controller Windows サービスの他のサービスを無効にしないでください。

ログオン権限の管理

VDAのコンピューターアカウントには、「ネットワークからこのコンピューターにアクセス」のログオン権限が必要です。(/ja-jp/advanced-concepts/implementation-guides/ad-ou-controller-discovery.html)を参照してください。

クライアントアクセス

クライアントアクセスは通常、(/ja-jp/storefront)を展開することで提供されます。StoreFrontのセキュリティ保護について詳しくは、(/ja-jp/storefront/current-release/install-standard/secure)を参照してください。

リモートユーザーが StoreFront および VDA に安全に接続できるようにするには、NetScaler® Gateway を展開します。

Citrixでは、クライアントがCitrix Workspaceアプリを使用してStoreFrontに接続することを推奨しています。詳しくは、各オペレーティングシステム用のCitrix Workspaceアプリの(/ja-jp/citrix-workspace-app.html)のセキュリティに関するセクションを参照してください。または、ユーザーはWebブラウザーを使用してStoreFrontにアクセスすることもできます。

ユーザーがCitrix Workspace™アプリ以外のアプリケーションを実行する能力が制限されているシンクライアントをユーザーに提供することを検討してください。デバイスが組織によって管理されている場合は、オペレーティングシステムのセキュリティ更新プログラムとウイルス対策ソフトウェアの展開を確実にするためのポリシーを設定する必要があります。ただし、多くの場合、ユーザーは組織の管理外にある管理されていないデバイスから接続できる必要があります。次の機能の使用を検討してください。

- Endpoint Analysisは、オペレーティングシステムやウイルス対策などのセキュリティ情報についてエンドポイントをスキャンし、セキュリティ要件を満たさないクライアントへのアクセスを拒否します。
- (/ja-jp/citrix-workspace-app/app-protection.html)は、キーロガーと画面キャプチャをブロックします。

混在バージョン環境

VDAがDelivery Controllerとは異なるバージョンである場合など、混在バージョン環境は一部のアップグレード中に避けられません。ベストプラクティスに従い、異なるバージョンのCitrixコンポーネントが共存する時間を最小限に抑えてください。混在バージョン環境では、たとえばセキュリティポリシーが一律に適用されない場合があります。

> **注:**
>
> これは他のソフトウェア製品にも共通しています。以前のバージョンの Active Directory を使用すると、後のバージョンの Windows ではグループポリシーが部分的にしか適用されません。

以下のシナリオでは、特定の混在バージョンCitrix環境で発生する可能性のあるセキュリティ問題について説明します。Citrix Receiver 1.7を使用して、XenAppおよびXenDesktop 7.6 Feature Pack 2のVDAを実行している仮想デスクトップに接続する場合、ポリシー設定 **デスクトップとクライアント間のファイル転送を許可する** はサイトで有効になっていますが、XenAppおよびXenDesktop 7.1を実行しているDelivery Controllerでは無効にできません。これは、製品の後のバージョンでリリースされたポリシー設定を認識しないためです。このポリシー設定により、ユーザーはファイルを仮想デスクトップにアップロードおよびダウン

ロードできますが、これがセキュリティ問題です。この問題を回避するには、Delivery Controller（またはStudioのスタンドアロンインスタンス）をバージョン7.6 Feature Pack 2にアップグレードし、グループポリシーを使用してポリシー設定を無効にします。または、影響を受けるすべての仮想デスクトップでローカルポリシーを使用します。

Remote PC Accessのセキュリティに関する考慮事項

Remote PC Accessは、次のセキュリティ機能を実装しています。

- スマートカードの使用がサポートされています。
- リモートセッションが接続されると、オフィスのPCのモニターは空白で表示されます。
- Remote PC Accessは、CTRL+ALT+DELおよびUSB対応のスマートカードと生体認証デバイスを除く、すべてのキーボードおよびマウス入力をリモートセッションにリダイレクトします。
- SmoothRoamingは単一ユーザーのみがサポートされます。
- ユーザーがオフィスPCにリモートセッションを接続している場合、そのユーザーのみがオフィスPCのローカルアクセスを再開できます。ローカルアクセスを再開するには、ユーザーはローカルPCでCtrl-Alt-Delを押し、リモートセッションで使用したのと同じ資格情報でログオンします。システムに適切なサードパーティのCredential Provider統合がある場合、ユーザーはスマートカードを挿入するか、生体認証を利用してローカルアクセスを再開することもできます。このデフォルトの動作は、グループポリシーオブジェクト（GPO）を介してFast User Switchingを有効にするか、レジストリを編集することで上書きできます。

注:

Citrixは、VDA管理者権限を一般セッションユーザーに割り当てないことを推奨します。

自動割り当て

デフォルトでは、Remote PC Accessは複数のユーザーのVDAへの自動割り当てをサポートしています。XenDesktop 5.6 Feature Pack 1では、管理者はRemotePCAccess.ps1 PowerShellスクリプトを使用してこの動作を上書きできます。このリリースでは、複数の自動リモートPC割り当てを許可または禁止するためにレジストリエントリを使用します。この設定はサイト全体に適用されます。

注意:

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

> 自動割り当てを単一ユーザーに制限するには：

Site内の各Controllerで、次のレジストリエントリを設定します。

```
HKEY_LOCAL_MACHINE\Software\Citrix|DesktopServer

Name: AllowMultipleRemotePCAssignments

Type: REG_DWORD

Data: 0 = Disable multiple user assignment, 1 = (Default) Enable multiple
user assignment.
```

既存のユーザー割り当てがある場合は、VDAが単一の自動割り当ての対象となるように、SDKコマンドを使用してそれらを削除します。

- VDAから割り当て済みのすべてのユーザーを削除します: `$machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine`
- デリバリーグループからVDAを削除します: `$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`

物理的なオフィスPCを再起動します。

証明書を管理する

TLSは、2つの当事者間の信頼を確立するために証明書を使用します。サービスを提供する各サーバーに適切な証明書をインストールし、そのサーバーに接続するマシンがその証明書を信頼するようにする必要があります。証明書に署名するためのオプションは次のとおりです。

- 自己署名証明書。これらは推奨されません。この証明書を信頼する必要がある他のマシンに手動でコピーする必要があるため、管理が困難です。
- エンタープライズ認証局。既存のPKIが導入されている場合、これは通常、内部デバイス間で使用する証明書に署名するための最も簡単なオプションです。

- 公開認証局。これには、ドメインの所有権を認証局に証明する必要があります。管理されていないクライアントデバイスは、通常、主要な公開認証局からの証明書を信頼するように事前設定されているという利点があります。

新しい証明書を作成する

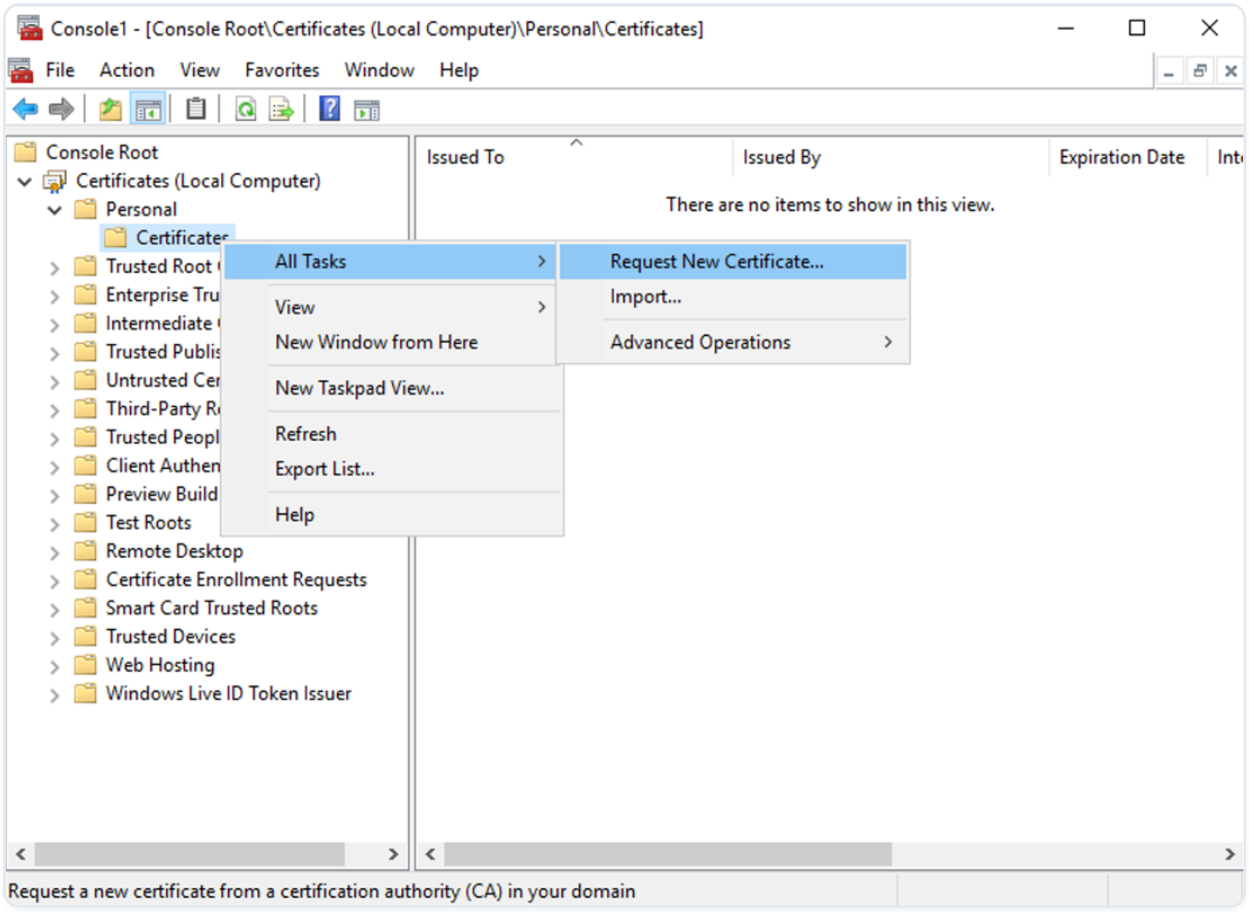
証明書を作成するための組織のポリシーと手順に従ってください。

Microsoft 証明機関を使用して証明書を作成する

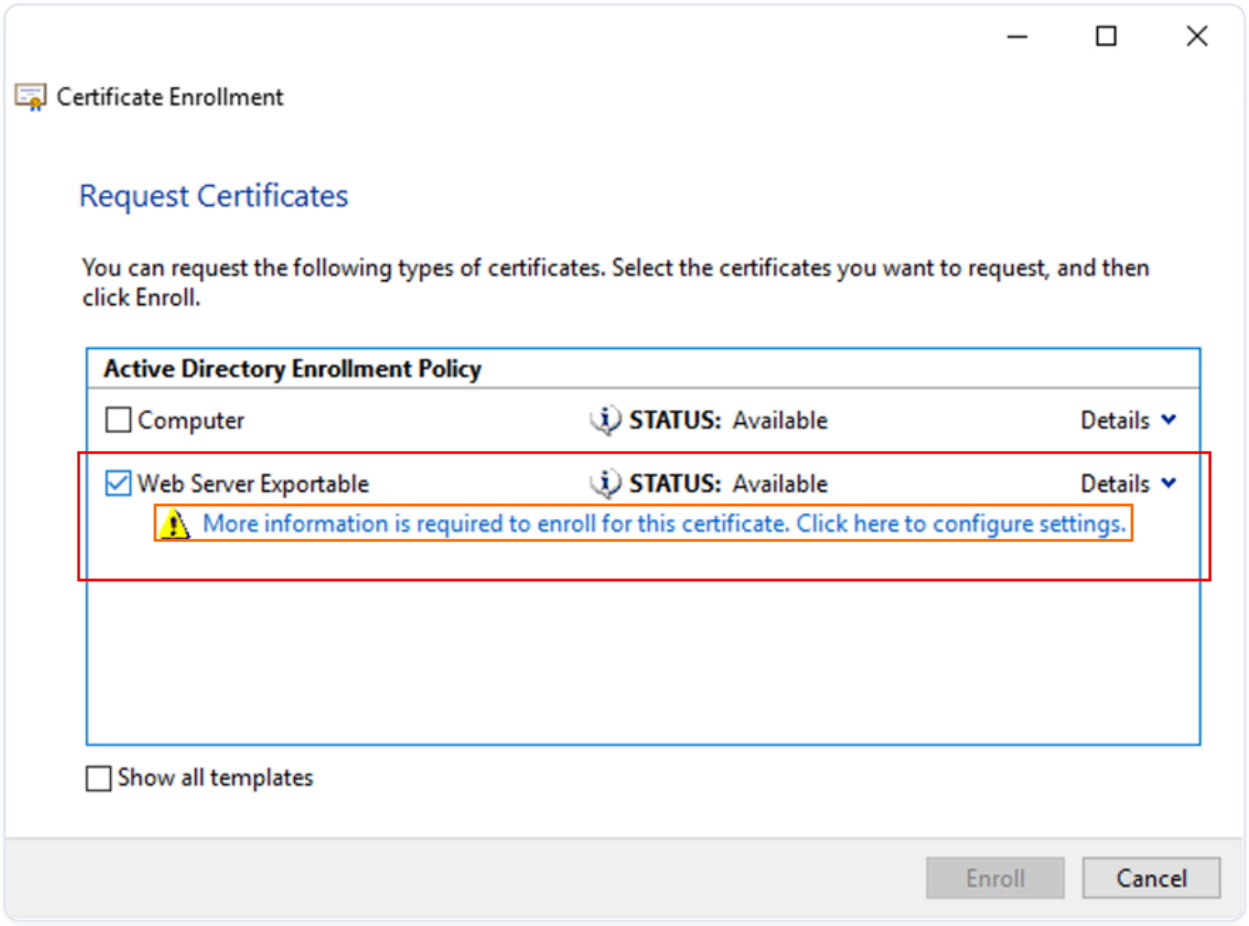
Microsoft 証明機関が Active Directory ドメインまたは Delivery Controller が参加している信頼されたフォレストに統合されている場合、証明書 MMC スナップインの証明書登録ウィザードから証明書を取得できます。Microsoft 証明機関は、Web サーバーでの使用に適した証明書テンプレートを公開している必要があります。

ルート証明書は、グループポリシーを使用してドメイン上の他のマシンに自動的に展開されます。したがって、ドメイン上の他のすべてのマシンは、Microsoft証明機関を使用して作成された証明書を信頼します。ドメイン上にないマシンがある場合は、ルート認証局証明書をエクスポートして、それらのマシンにインポートする必要があります。

1. サーバーで、MMCコンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、コンピューターアカウントを選択します。
2. **個人 > 証明書**を展開し、**すべてのタスク > 新しい証明書の要求**コンテキストメニューコマンドを使用します。



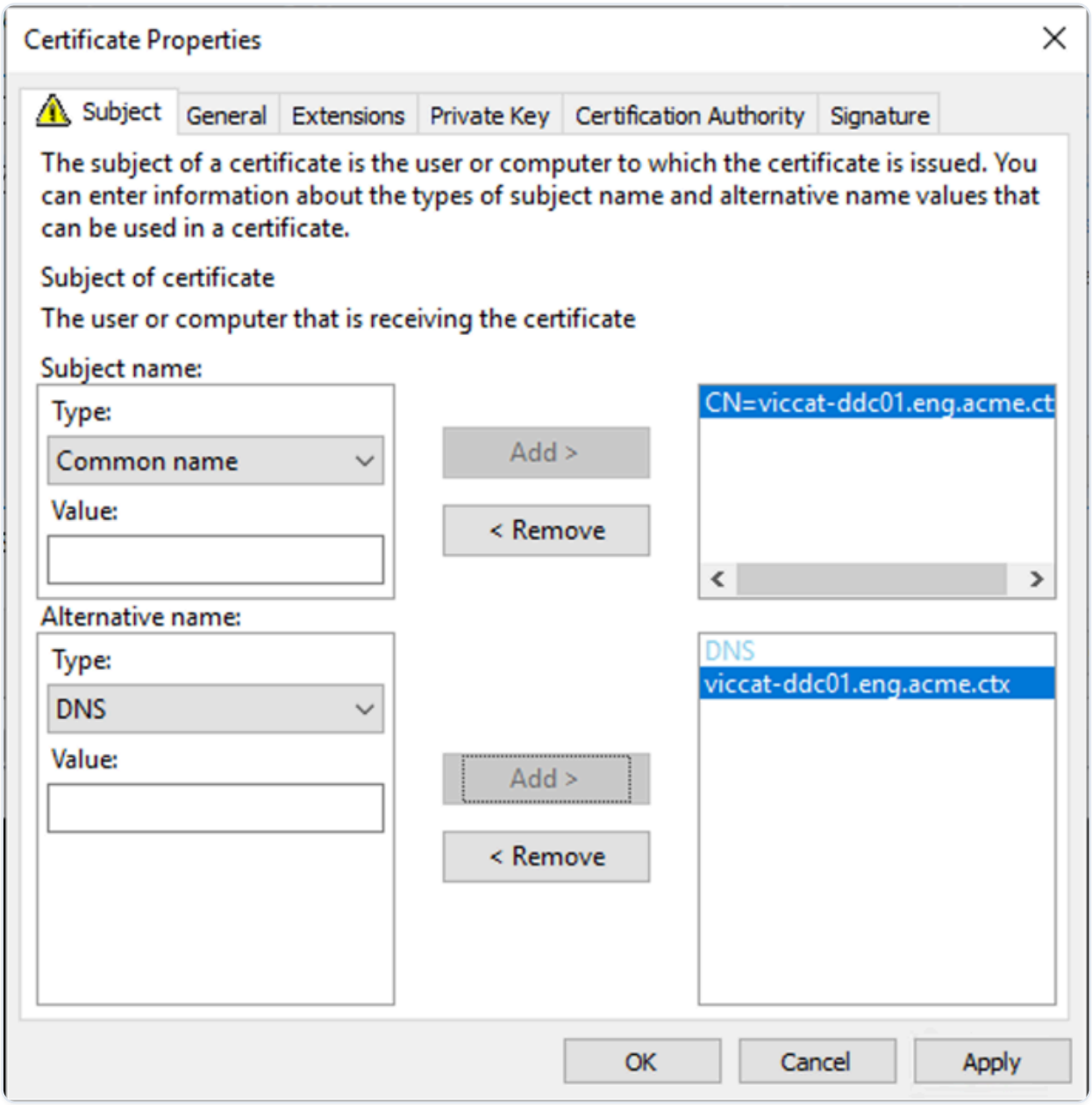
3. **次へ**をクリックして開始し、**次へ**をクリックして、Active Directory登録から証明書を取得することを確認します。
4. **Webサーバーエクスポート可能**などの適切なテンプレートを選択します。テンプレートがSubjectの値を自動的に提供するように設定されている場合は、詳細を提供せずに**登録**をクリックできます。それ以外の場合は、**この証明書を登録するにはさらに情報が必要です。ここをクリックして設定を構成してください。**をクリックします。



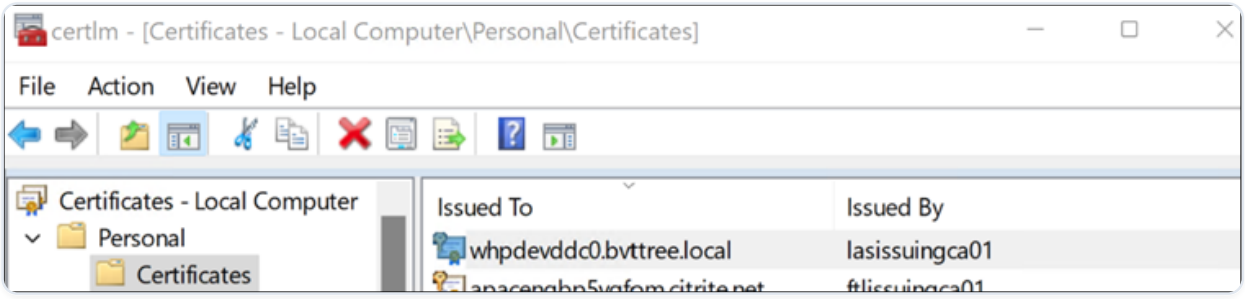
5. 証明書テンプレートの詳細を指定するには、**詳細**の矢印ボタンをクリックし、以下を構成します。

   サブジェクト名: を選択し、サーバーの FQDN を追加します。

   代替名: を選択し、サーバーの FQDN を追加します。



6. **OK**を押します。
7. **Enroll** を押して証明書を作成します。証明書の一覧に表示されます。

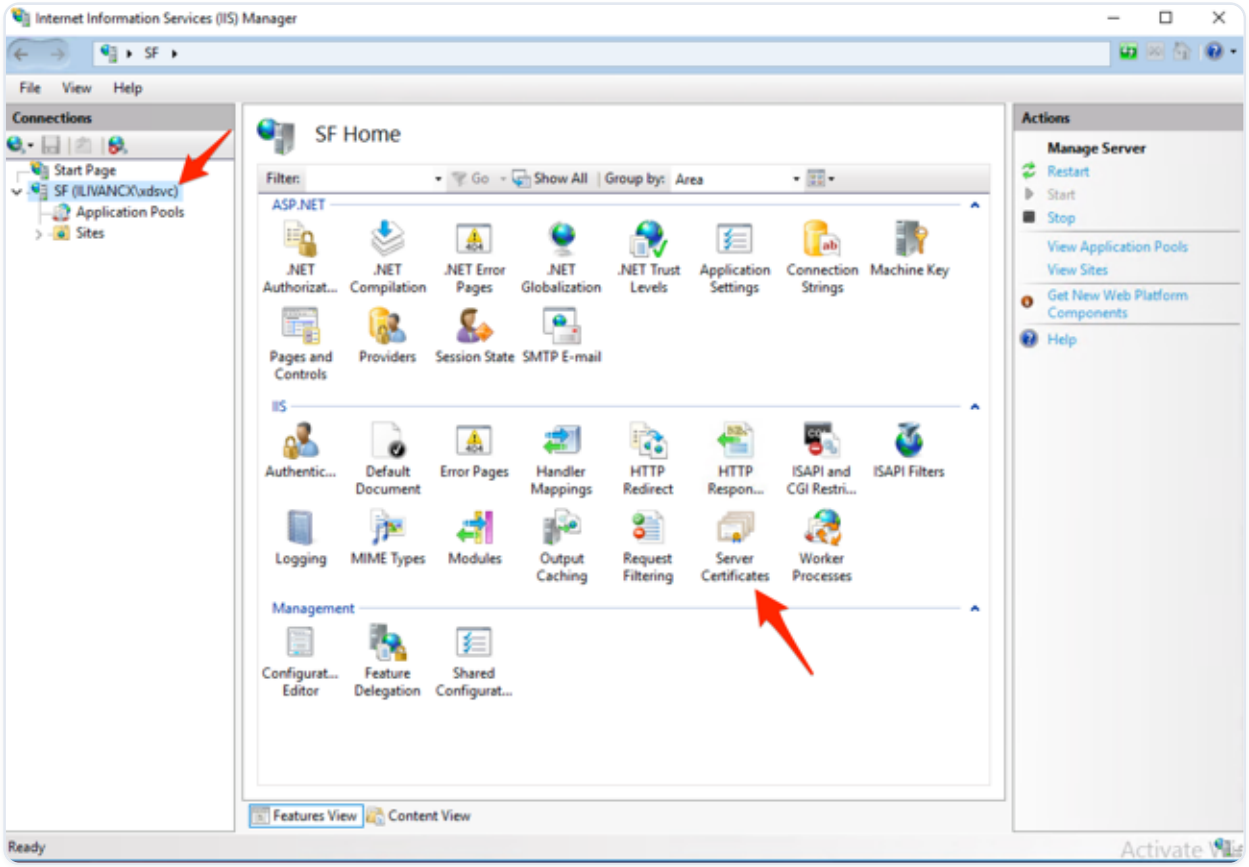


IIS を使用して証明書要求を作成する

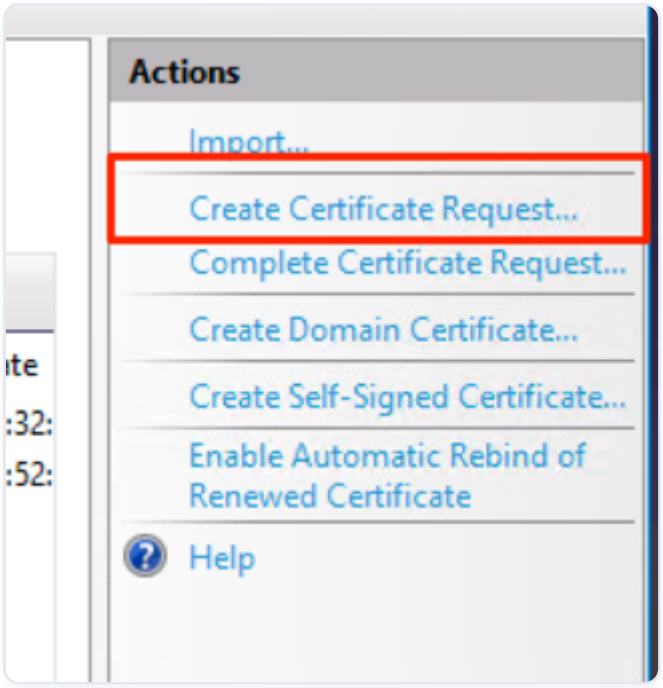
IIS がサーバーにインストールされている場合は、次の手順を実行します。

1. **インターネットインフォメーションサービス（IIS）マネージャー**を開きます。

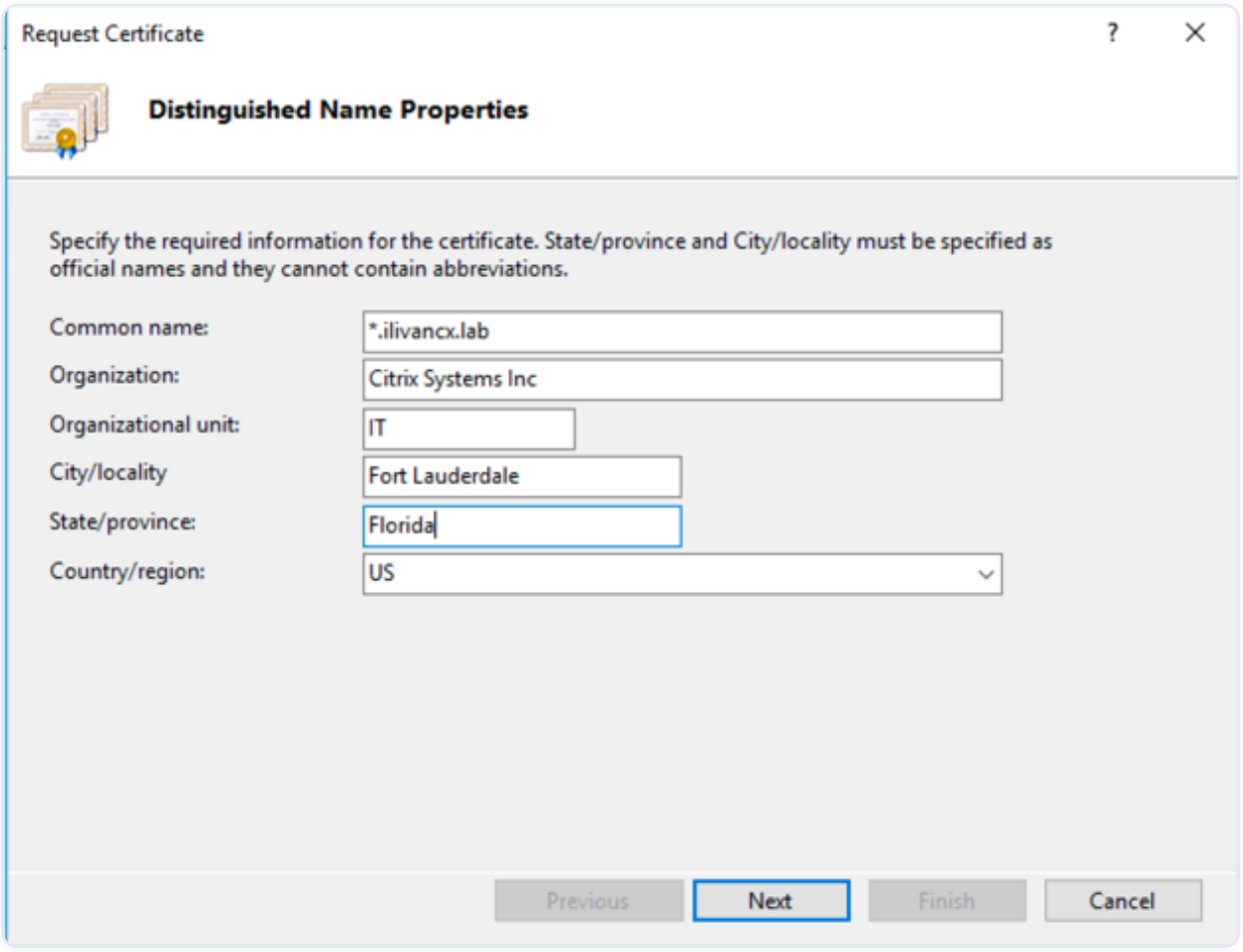
2. 接続リストでサーバーノードを選択します。
3. **サーバー証明書**を開きます。



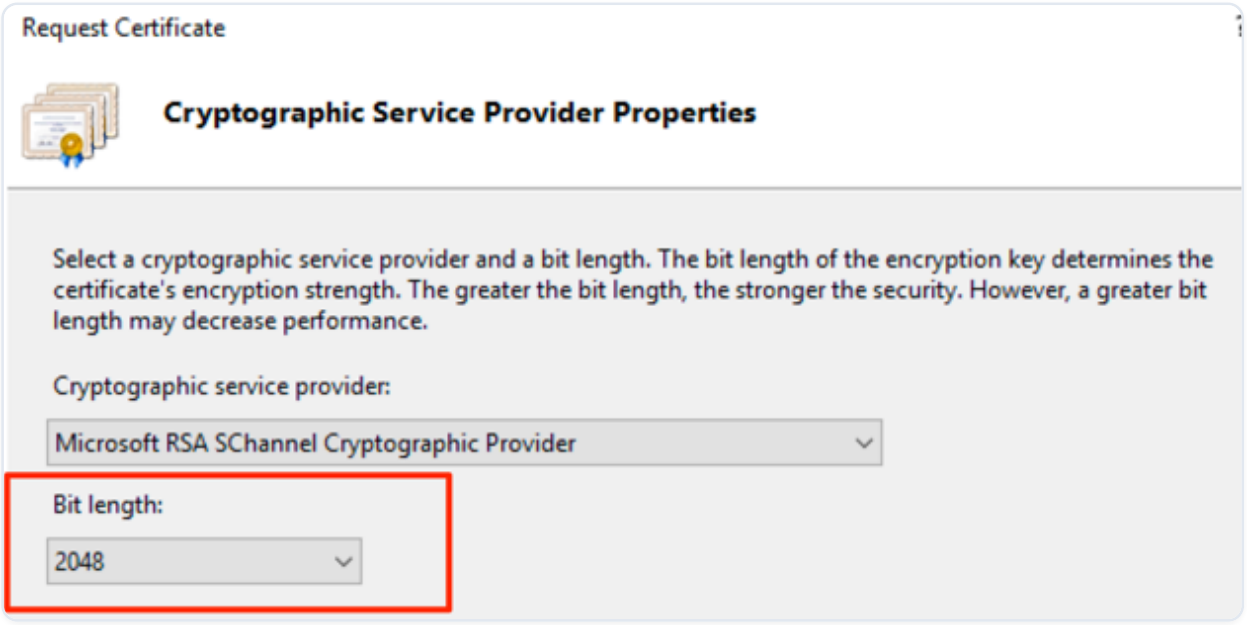
4. **操作**ペインから、**証明書要求の作成...**を選択します。



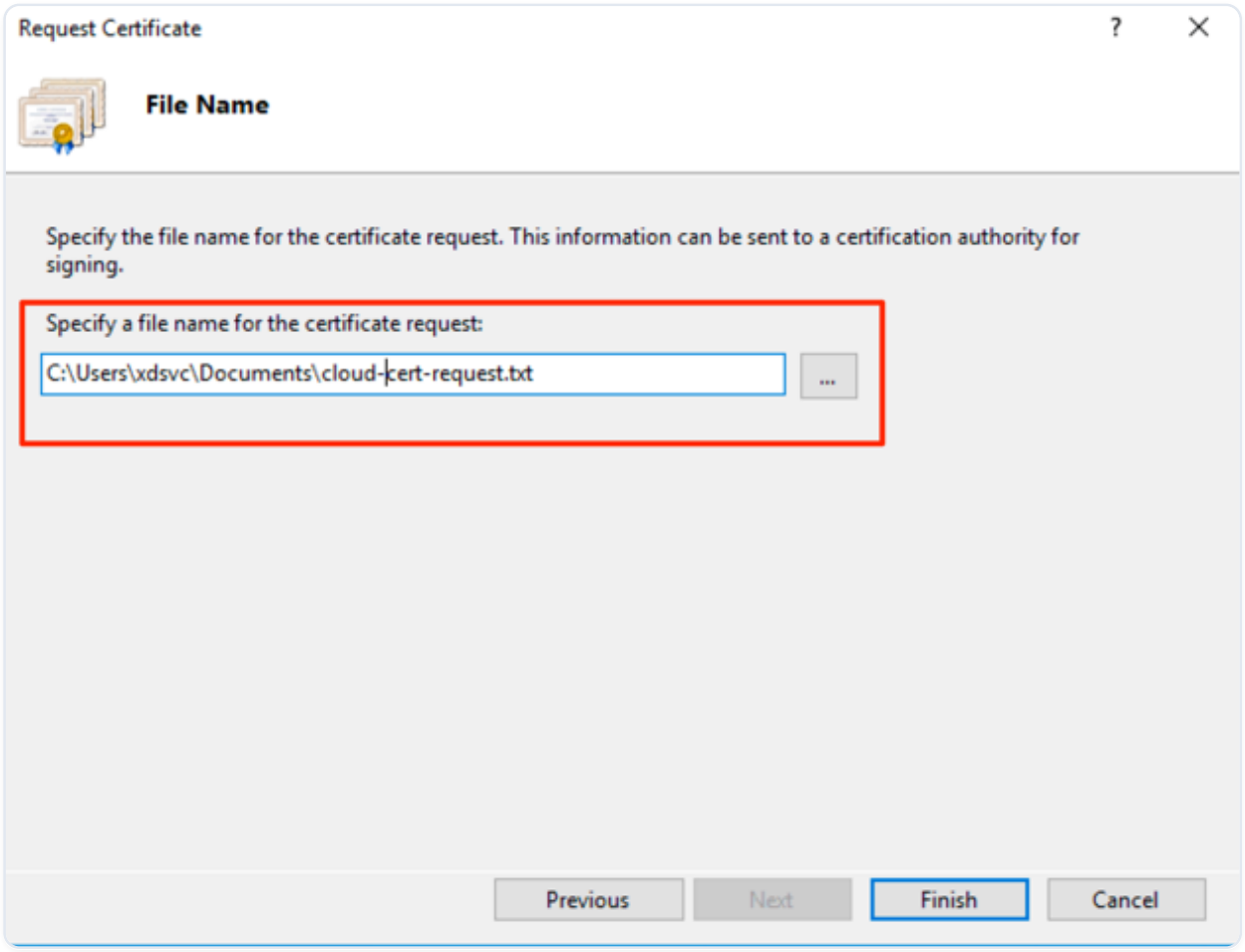
5. **識別名プロパティ**を入力します。



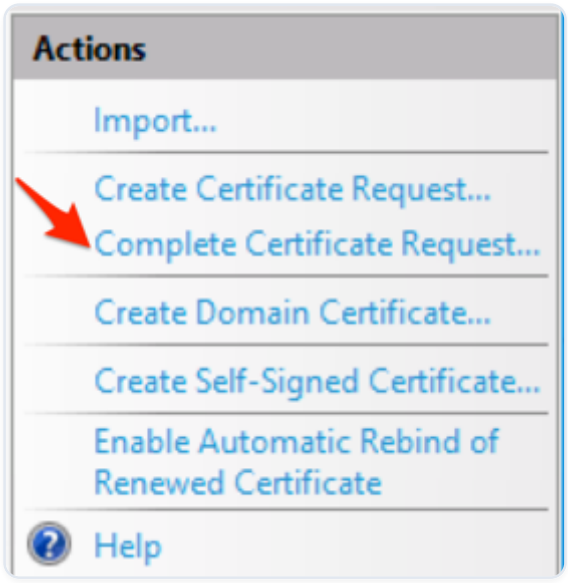
6. 「**暗号化サービスプロバイダーのプロパティ**」画面で、「**暗号化サービスプロバイダー**」をデフォルトのままにします。キーサイズは「**2048**」以上に設定します。



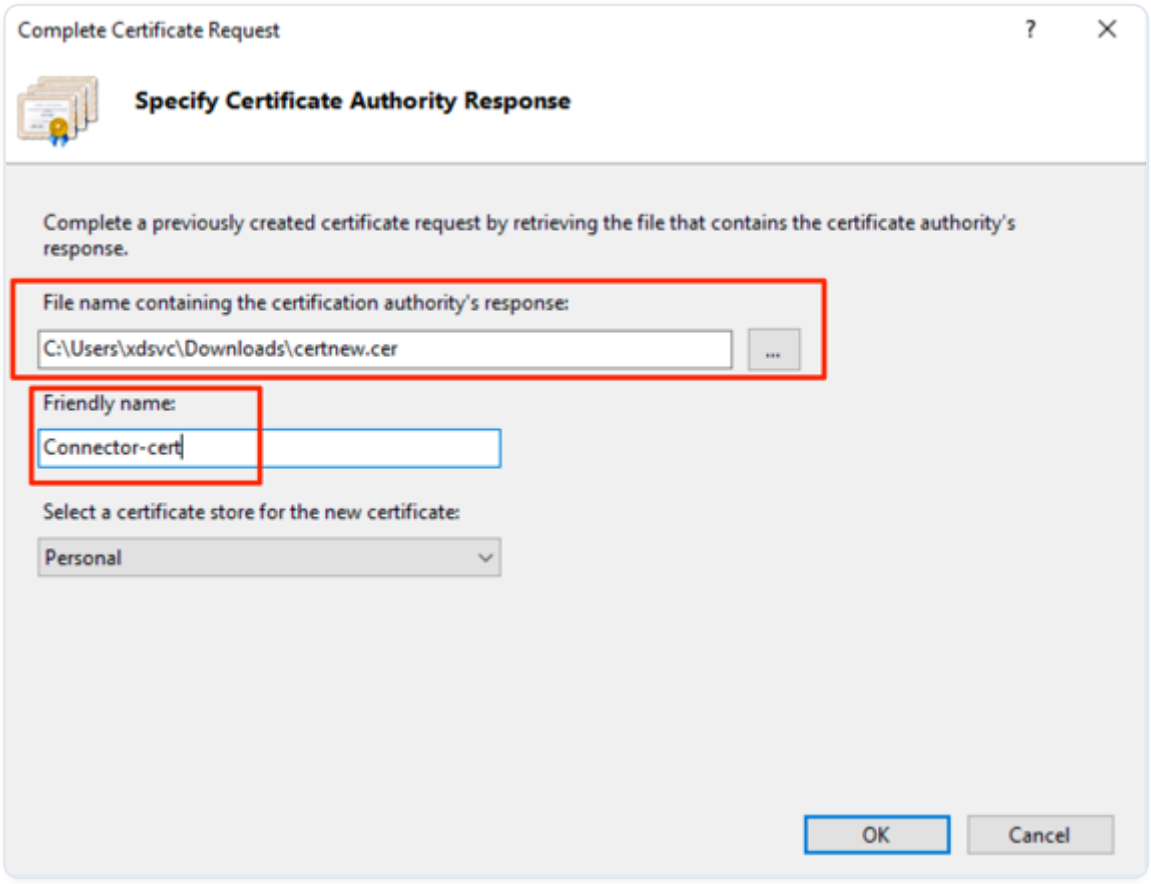
7. ファイル名を選択し、「**完了**」を押します。



8. CSRを証明機関にアップロードします。
9. 証明書を受け取ったら、「**操作**」ペインから「**証明書要求の完了...**」を選択します。



10. 証明書を選択し、「**フレンドリ名**」を指定して「**OK**」を押します。



サブジェクトの別名を設定する方法はありません。そのため、証明書は共通名を使用して指定されたサーバーに限定されます。

証明書スナップインから証明書署名要求を作成する

証明書MMCスナップイン内から、証明書署名要求を作成できます。これにより、証明書を提供する認証局に送信できるファイルが生成されます。その後、証明書をインポートして、ローカルの秘密鍵と結合する必要があります。

1. サーバーで、MMCコンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、を選択します。
2. **個人** > **証明書**を展開します。
3. **すべてのタスク** > **高度な操作** > **カスタム要求の作成**を選択します。
4. **開始する前に**で、**次へ**を選択します。
5. **証明書登録ポリシーの選択**画面で、適切な既存のポリシーを選択するか、**登録ポリシーなしで続行**を選択します。
6. **カスタム要求**画面で、登録ポリシーを使用している場合は、利用可能な場合は**Web Server Exportable**などの適切なテンプレートを選択します。
7. **証明書情報**画面で、**詳細**を展開し、**プロパティ**を選択します。

8. **証明書のプロパティ**ウィンドウの**全般**タブで、適切なフレンドリ名を入力します。
9. **サブジェクト**タブで、次のようにします。
    a. **サブジェクト名**の下で、**共通名**を選択し、サーバーのFQDNを入力します。ワイルドカードを入力できます。**追加**を選択します。
    b. **サブジェクト名**の下で、組織、組織単位、地域、都道府県、国に適切な値を追加します。
    c. **代替名**の下で、**DNS**を選択します。サーバーのFQDNを追加します。複数のサーバーFQDNまたはワイルドカードFQDNを追加できます。
10. **拡張機能**タブで、次のようにします。
    - **キー使用法**の下で、**デジタル署名**と**キーの暗号化**を追加します。
    - 「**拡張キー使用法 (アプリケーションポリシー)**」で、「**サーバー認証**」と「**クライアント認証**」を追加します。
11. 「**秘密キー**」タブで。
    - 「**暗号化サービスプロバイダー (CSP) の選択**」の下で、適切なプロバイダーを選択します。
    - 「**キーオプション**」の下で、適切なキーサイズを選択します。RSAプロバイダーの場合、最小で2048のキーサイズを使用します。セキュリティを強化するために4096を選択することもできますが、パフォーマンスにわずかな影響があります。
    - 「**キーオプション**」の下で、「**秘密キーをエクスポート可能にする**」を選択します。
12. 「**OK**」を選択します。
13. 「**次へ**」を選択します。
14. 「**参照**」を選択し、要求を保存します。
15. 「**完了**」を選択します。
16. CSR を認証局にアップロードします。
17. 証明書を受け取ったら、同じサーバーで(#import-existing-certificate)インポートして、秘密鍵にリンクさせます。

新しい自己署名証明書を作成する

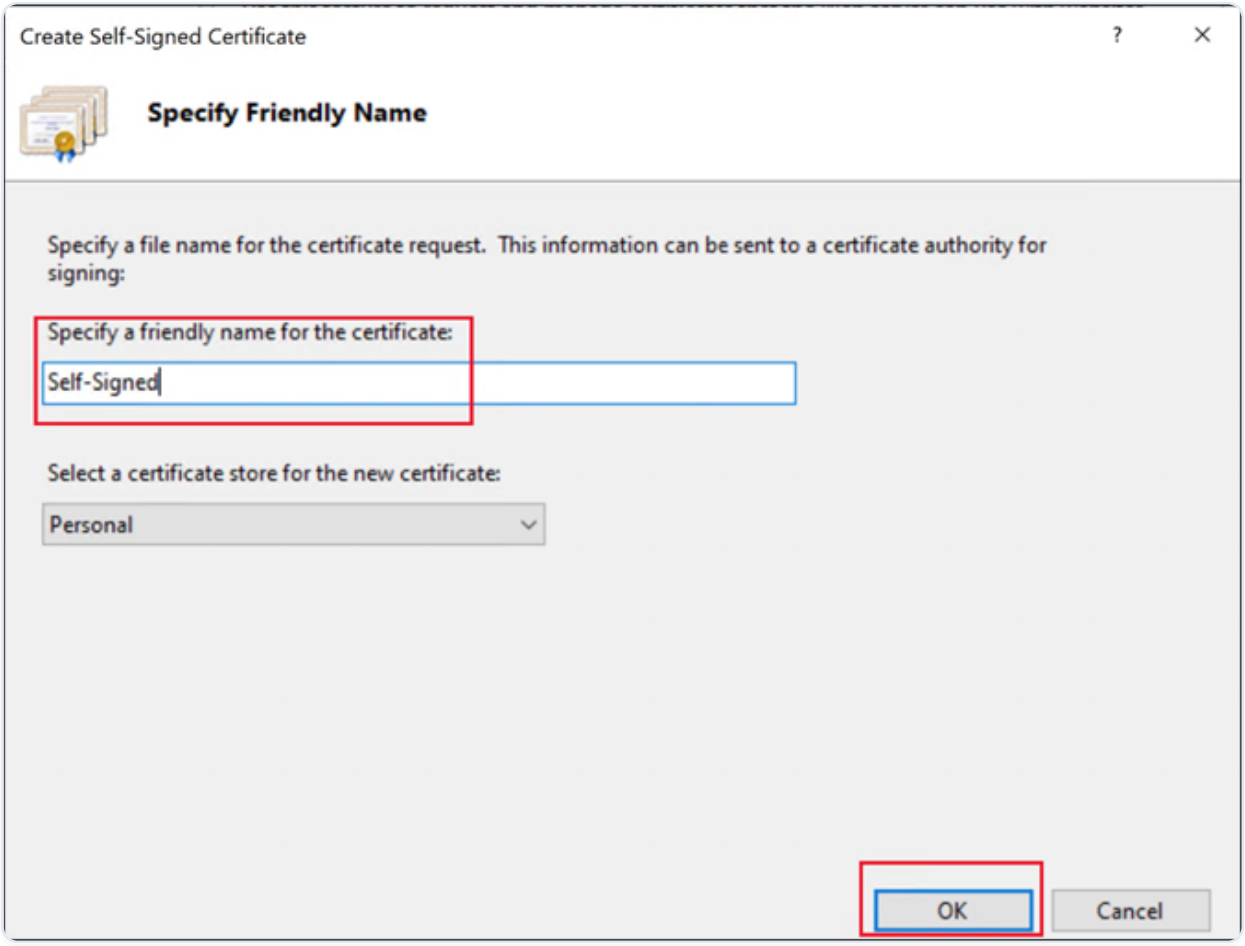
自己署名証明書は、delivery controller™ と web studio のインストール中に作成されます。新しい自己署名証明書を生成し、既存のものと置き換えることができます。

IIS マネージャーを使用する

IIS がサーバーにインストールされている場合は、次の手順を実行できます。

1. 管理者としてサーバーにログオンします。
2. IIS マネージャーを開きます。
3. 「**サーバー証明書**」を開きます。
4. 「**操作**」ペインで、「**自己署名証明書の作成**」を選択します。

   サーバー証明書(/en-us/citrix-virtual-apps-desktops/2411/media/server-certificates.png)
5. 「**自己署名証明書の作成**」で、証明書の名前を入力し、「**OK**」をクリックします。自己署名証明書が作成されます。



PowerShell を使用する

PowerShellを使用して自己署名証明書を作成できます。

```
$certSubject = "CN=myddc.example.com" # The FQDN of the server.

$friendlyName = "Self-Signed-3"
```

```
$expireYears = 5



## Create new self-signed certificate under LocalMachine\My

$certificate = New-SelfSignedCertificate -Subject $certSubject
-CertStoreLocation "Cert:\LocalMachine\My\" -KeyExportPolicy Exportable
-KeySpec Signature -KeyLength 2048 -KeyAlgorithm RSA -HashAlgorithm SHA256
-FriendlyName $friendlyName -NotAfter $
([System.DateTime]::Now.AddYears($expireYears))



# Add to trusted root certificates

$rootCertStore = Get-Item "Cert:\LocalMachine\Root\"

$rootCertStore.Open([System.Security.Cryptography.X509Certificates.OpenFla
gs]::ReadWrite)

$rootCertStore.Add($certificate)
```

既存の証明書をインポートする

以下のいずれかの方法を使用して、既存の証明書をサーバーにインポートできます。

証明書のインポートウィザード

1. PFX ファイルをダブルクリックするか、ファイルを右クリックして **PFX のインストール** を選択します。これにより、**証明書のインポートウィザード** が開きます。
2. **ストアの場所** には、**ローカルコンピューター** を選択します。

   証明書のインポートウィザードのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2411/media/certificate-import-wizard.png)
3. 必要に応じてパスワードを入力します。

   証明書のインポートウィザード、秘密キーの保護手順のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2411/media/key-protection.png)

4. **証明書ストア** を選択します。サーバー証明書の場合は、**個人** を選択します。このマシンから信頼したいルート証明書または自己署名証明書の場合は、**信頼されたルート証明機関** を選択します。

   証明書のインポートウィザード、証明書ストアの手順のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2411/media/certificate-store.png)

コンピューター証明書の管理コンソールを使用する

1. コンピューター証明書の管理コンソールを開き、適切な証明書ストアに移動します。サーバー証明書の場合、通常は **個人** > **証明書** です。ルート証明書または自己署名証明書を信頼するには、**信頼されたルート証明機関** > **証明書** を選択します。
2. 証明書を右クリックし、「**すべてのタスク**」>「**インポート...**」を選択します。

   コンピューター証明書の管理コンソール(/en-us/citrix-virtual-apps-desktops/2411/media/manage-computer-certificates-console.png)

3. **参照...** を選択し、ファイルを選択します。
4. 必要に応じてパスワードを入力します。

PowerShell を使用する

証明書をインポートするには、PowerShell コマンドレット Import-PfxCertificate を使用します。たとえば、パスワード `123456` を使用して証明書 `certificate.pfx` を個人証明書ストアにインポートするには、次のコマンドを実行します。

```
Import-PfxCertificate -Password $(ConvertTo-SecureString -String "123456"
-AsPlainText -Force) -CertStoreLocation Cert:\LocalMachine\My\ -FilePath .
\Desktop\certificate.pfx
```

信頼されたルート証明書をインポートするには、`CertStoreLocation` を `Cert:\LocalMachine\Root\` に設定します。

秘密キーなしで証明書をエクスポートする

証明書を他のデバイスにインポートして信頼できるように証明書をエクスポートするには、秘密キーを除外する必要があります。

1. コンピューター証明書の管理を開きます。**個人** > **証明書** に移動し、エクスポートする証明書を選択します。
2. **操作** メニューから、**すべてのタスク**、次に **エクスポート** を選択します。

エクスポートメニューを含む証明書管理のスクリーンショット](/en-us/citrix-virtual-apps-desktops/2411/media/certificate-export.png)

3. **いいえ、秘密キーをエクスポートしません** を選択し、**次へ** を押します。

   証明書のエクスポート](/en-us/citrix-virtual-apps-desktops/2411/media/certificate-export-no-private-key.png)

4. 形式 **DER encoded binary X.509 (.CER)** (既定) を選択し、**次へ** を押します。
5. ファイル名を入力し、**次へ** を押します。

   証明書のエクスポートウィザード、ファイル名のスクリーンショット](/en-us/citrix-virtual-apps-desktops/2411/media/certificate-export-file.png)

6. 「**完了**」を選択します。

   「証明書のエクスポートウィザード、エクスポート成功」のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2411/media/certificate-export-complete.png)

秘密キーを含む証明書のエクスポート

証明書を他のサーバーで使用できるようにエクスポートするには、秘密キーを含める必要があります。

1. コンピューター証明書の管理を開きます。**個人** > **証明書** に移動し、エクスポートする証明書を選択します。
2. **操作** メニューから、**すべてのタスク**、次に**エクスポート**を選択します。

   エクスポートメニューを含む証明書管理のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2411/media/certificate-export.png)

3. 「**はい、秘密キーをエクスポートします**」を選択し、「**次へ**」を選択します。

   「証明書のエクスポート」(/en-us/citrix-virtual-apps-desktops/2411/media/certificate-export-private-key.png)

4. **セキュリティ** タブで、パスワードを入力し、「**次へ**」を選択します。

   「証明書のエクスポートウィザード、セキュリティ手順」のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2411/media/certificate-export-password.png)

5. ファイル名を入力し、「**次へ**」を選択します。

   「証明書のエクスポートウィザード、ファイル名」のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2411/media/certificate-export-file.png)

6. 「**完了**」を選択します。

   証明書のエクスポートウィザード、エクスポート成功のスクリーンショット](/en-us/citrix-virtual-apps-desktops/2411/media/certificate-export-complete.png)

証明書をPEM形式に変換する

デフォルトでは、Windowsは秘密鍵を含む.pfxファイルとして、PKCS#12形式で証明書をエクスポートします。NetScaler® Gatewayまたはライセンスサーバーで証明書を使用するには、証明書と秘密鍵をPEM形式の別々のファイルに抽出する必要があります。これはopensslを使用して実行できます。

証明書をPEM形式でエクスポートするには、以下を実行します。

```
openssl pkcs12 -in name.pfx -clcerts -nokeys -out name.cer
```

既存のパスワードと新しいパスフレーズの入力を求められます

キーをPEM形式でエクスポートするには、以下を実行します。

```
openssl pkcs12 -in name.pfx -nocerts -out name.key
```

証明書の信頼

- 公開認証局の証明書を使用する場合、デバイスには通常、ルート証明書が事前に構成されています。
- エンタープライズ認証局を使用する場合、その証明書を信頼する必要があるすべてのデバイスにルート証明書を展開する必要があります。Active Directory証明書サービスを使用している場合、ルート証明書はグループポリシーを使用してドメイン上のすべてのマシンにも展開されます。NetScaler Gatewayなどのドメインに参加していないマシンや、他のドメイン上のマシンには、ルート証明書を手動でインポートする必要があります。
- 自己署名証明書を使用している場合、証明書を信頼する必要があるすべてのマシンに手動でインストールする必要があります。

Windowsから自己署名証明書または信頼されたルート証明書をエクスポートするには、秘密鍵なしで証明書をエクスポートするを参照してください。

Windowsが証明書を信頼するには、**信頼されたルート証明機関**ストアに証明書をインポートする必要があります。PowerShellを使用する場合は、ストア**Cert:\\LocalMachine\Root**を入力します。

NetScalerが証明書を信頼するようにするには、まず証明書をPEM形式に変換する、次にルート証明書をインストールする必要があります。

スマートカード

スマートカードおよび同等のテクノロジーは、この記事で説明されているガイドライン内でサポートされています。Citrix Virtual AppsまたはCitrix Virtual Desktops™でスマートカードを使用するには、次の手順を実行します。

- スマートカードの使用に関する組織のセキュリティポリシーを理解します。これらのポリシーには、たとえば、スマートカードの発行方法やユーザーがスマートカードを保護する方法が記載されている場合があります。これらのポリシーの一部は、Citrix Virtual Apps™またはCitrix Virtual Desktops環境で再評価する必要がある場合があります。
- スマートカードで使用するユーザーデバイスの種類、オペレーティングシステム、および公開アプリケーションを決定します。
- スマートカードテクノロジーと、選択したスマートカードベンダーのハードウェアおよびソフトウェアに精通してください。
- 分散環境でデジタル証明書を展開する方法を理解します。

> **注記：**
>
> スマートカード登録は、高速スマートカードではサポートされていません。高速スマートカードが無効になっている場合、スマートカード登録は機能する可能性がありますが、スマートカードとミドルウェアの種類によって異なります。Citrix Virtual Apps and Desktopsとの統合、および仮想セッションを介したスマートカード登録のサポートについては、スマートカードおよびミドルウェアベンダーにお問い合わせください。

スマートカードの種類

企業向けスマートカードと消費者向けスマートカードは、同じ寸法、電気コネクタを持ち、同じスマートカードリーダーに適合します。

エンタープライズ用途のスマートカードには、デジタル証明書が含まれています。これらのスマートカードはWindowsログオンをサポートし、ドキュメントやメールのデジタル署名および暗号化のためのアプリケーションでも使用できます。Citrix Virtual Apps and Desktops™はこれらの用途をサポートしています。

コンシューマー用途のスマートカードにはデジタル証明書は含まれていません。共有シークレットが含まれています。これらのスマートカードは、支払い（チップと署名、またはチップとPINのクレジットカードなど）をサポートできます。Windowsログオンや一般的なWindowsアプリケーションはサポートしていません。これらのスマートカードを使用するには、特殊なWindowsアプリケーションと適切なソフトウェアインフラストラクチャ（たとえば、決済カードネットワークへの接続を含む）が必要です。Citrix Virtual AppsまたはCitrix Virtual Desktopsでこれらの特殊なアプリケーションをサポートする方法については、Citrix担当者にお問い合わせください。

企業向けスマートカードには、同様の方法で使用できる互換性のある同等品があります。

- スマートカードと同等のUSBトークンは、USBポートに直接接続します。これらのUSBトークンは通常、USBフラッシュドライブと同じサイズですが、携帯電話で使用されるSIMカードと同じくらい小さい場合もあります。これらは、スマートカードとUSBスマートカードリーダーの組み合わせとして表示されます。
- Windows Trusted Platform Module (TPM) を使用する仮想スマートカードは、スマートカードとして表示されます。これらの仮想スマートカードは、Citrix Workspaceアプリ（最小バージョンCitrix Receiver 4.3）を使用して、Windows 8およびWindows 10でサポートされています。
    - XenAppおよびXenDesktop 7.6 FP3より前のバージョンのCitrix Virtual Apps and Desktops（旧XenAppおよびXenDesktop）は、仮想スマートカードをサポートしていません。
    - 仮想スマートカードの詳細については、「仮想スマートカードの概要」を参照してください。

    注: 「仮想スマートカード」という用語は、ユーザーコンピューターに保存されているデジタル証明書を指す場合もあります。これらのデジタル証明書は、厳密にはスマートカードと同等ではありません。

Citrix Virtual Apps and Desktopsのスマートカードサポートは、Microsoft Personal Computer/Smart Card (PC/SC) 標準仕様に基づいています。最低要件として、スマートカードおよびスマートカードデバイスは、基盤となるWindowsオペレーティングシステムでサポートされ、Microsoft Windows Hardware Quality Labs (WHQL) によって認定されたWindowsオペレーティングシステムを実行するコンピューターで使用するために承認されている必要があります。ハードウェアのPC/SC準拠に関する追加情報については、Microsoftのドキュメントを参照してください。他の種類のユーザーデバイスもPS/SC標準に準拠している場合があります。詳細については、「Citrix Readyプログラム」を参照してください。

通常、各ベンダーのスマートカードまたは同等のものには、個別のデバイスドライバーが必要です。ただし、スマートカードがNIST Personal Identity Verification (PIV) 標準などの標準に準拠している場合、さまざまなスマートカードに単一のデバイスドライバーを使用できる可能性がありま

す。デバイスドライバーは、ユーザーデバイスとVirtual Delivery Agent (VDA) の両方にインストールする必要があります。デバイスドライバーは、Citrixパートナーから入手できるスマートカードミドルウェアパッケージの一部として提供されることが多く、このスマートカードミドルウェアパッケージは高度な機能を提供します。デバイスドライバーは、Cryptographic Service Provider (CSP)、Key Storage Provider (KSP)、またはミニドライバーとも呼ばれることがあります。

Windowsシステム向けの以下のスマートカードとミドルウェアの組み合わせは、Citrixによってそのタイプの代表的な例としてテストされています。ただし、他のスマートカードとミドルウェアも使用できます。Citrix互換のスマートカードとミドルウェアの詳細については、`<http://www.citrix.com/ready>`を参照してください。

ミドルウェア	対応カード
Gemalto .NETカード用ミニドライバー	Gemalto .NET v2以降

他の種類のデバイスでのスマートカードの使用に関する情報については、そのデバイスのCitrix Workspace™アプリのドキュメントを参照してください。

リモートPCアクセス

スマートカードは、Windows 10、Windows 8、またはWindows 7を実行している物理的なオフィスPCへのリモートアクセスでのみサポートされます。

Remote PC Accessでテストされたスマートカードは次のとおりです。

ミドルウェア	一致するカード
Gemalto .NET ミニドライバー	ジェムアルト .NET v2+

高速スマートカード

高速スマートカードは、既存のHDX PC/SCベースのスマートカードリダイレクトを改善したものです。これは、スマートカードが高遅延のWAN環境で使用される場合のパフォーマンスを向上させます。遅延が高い場合、パフォーマンスの向上は著しいものになります（たとえば、Windowsの高速スマートカードログオンでは15秒、PC/SCベースのスマートカードリダイレクトでは1分以上）。

高速スマートカードは、現在サポートされているWindows VDAを搭載したホストマシンでデフォルトで有効になっています。ホスト側で高速スマートカードを無効にするには（診断目的など）、レジストリ設定「Disable Cryptographic Redirection」をゼロ以外の値に設定します。

```
HKLM\SOFTWARE\Citrix\SmartCard

CryptographicRedirectionDisable (DWORD)
```

クライアント側で高速スマートカードを有効にするには、関連するStoreFrontサイトの *default.ica* ファイルにSmartCardCryptographicRedirection ICAパラメーターを含めます。

```
[WFClient]

SmartCardCryptographicRedirection=On
```

さらに、クライアント側では、以下のレジストリ設定を使用して、高速スマートカードを強制的に有効または無効にすることができます（診断目的など）。

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceEnableCryptographicRedirection (ゼロ以外のDWORDとして)

または

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceDisableCryptographicRedirection (ゼロ以外のDWORDとして)

クライアントマシンが64ビットの場合、32ビットレジストリハイブを指定する必要があります（`WOW6432Node`を使用）。

制限事項：

- Citrix Workspaceアプリ for Windowsのみが高速スマートカードをサポートしています。default.icaファイルで高速スマートカードを設定した場合でも、Windows用ではないCitrix Workspaceアプリは既存のPC/SCリダイレクトを使用します。
- 高速スマートカードがサポートする唯一のダブルホップシナリオは、両方のホップで高速スマートカードが有効になっているICA® > ICAです。高速スマートカードはICA > RDPダブルホップシナリオをサポートしていないため、これらのシナリオは機能しません。
- 高速スマートカードはCryptography Next Generationをサポートしていません。そのため、高速スマートカードは楕円曲線暗号 (ECC) スマートカードをサポートしていません。
- 高速スマートカードは、読み取り専用のキーコンテナ操作のみをサポートしています。
- 高速スマートカードは、スマートカードPINの変更をサポートしていません。

VDAバージョン2203およびWindows版Citrix Workspaceアプリバージョン2202（またはそれ以降）以降、高速スマートカードはCryptography Next Generation (CNG) と互換性があります。さらに、楕円曲線暗号 (ECC) スマートカードは、ECDSAとECDHの両方で、P-256、P-384、P-521ビットの以下の曲線に対応しています。

VDAバージョン2203以降、高速スマートカードは、同じユーザーのログオンセッション内のアプリケーション間でスマートカードPINをキャッシュする機能を追加しました。たとえば、**セッションPINキャッシュ**が有効になっており、エンドユーザーが以前にOutlookにスマートカードPINを提供した場合、Wordでドキュメントに署名する際に、WordはすでにキャッシュされているスマートカードPIN（Outlookに送信されたもの）を使用します。**セッションPINキャッシュ**は、ユーザーがスマートカードPINを入力する回数を減らすことで、ユーザーエクスペリエンスを向上させます。さらに、スマートカードを使用してVDAにログオンする場合、Windowsスマートカードログオン PINをオプションで**セッションPINキャッシュ**に保存できます。これにより、ユーザーエクスペリエンスがさらに向上します。

セッションPINキャッシュはデフォルトで無効になっています。VDA上の以下のレジストリ設定で有効化および制御できます。

HKLM\SOFTWARE\Citrix\SmartCard: で:

- `EnablePinSessionCache` をDWORDとして（有効にするにはゼロ以外）
- `EnableLogonPinSessionCache` をDWORDとして（有効にするにはゼロ以外）
- `PinSessionCacheEntryStaleTimeout` をDWORDとして（エントリが古くなるまでの秒数、デフォルトは1時間）

スマートカードリーダーの種類

スマートカードリーダーは、ユーザーデバイスに内蔵されている場合もあれば、ユーザーデバイスに別途接続されている場合もあります（通常はUSBまたはBluetooth経由）。USB Chip/Smart Card Interface Devices (CCID) 仕様に準拠した接触型カードリーダーがサポートされています。これらには、ユーザーがスマートカードを挿入するためのスロットまたはスワイプ機能があります。Deutsche Kreditwirtschaft (DK) 規格は、接触型カードリーダーを4つのクラスに定義しています。

- クラス1スマートカードリーダーは最も一般的で、通常はスロットを備えています。クラス1スマートカードリーダーはサポートされており、通常はオペレーティングシステムに付属の標準CCIDデバイスドライバーで使用できます。
- クラス2スマートカードリーダーには、ユーザーデバイスからアクセスできないセキュアキーパッドも含まれています。クラス2スマートカードリーダーは、セキュアキーパッドが統合さ

れたキーボードに組み込まれている場合があります。クラス2スマートカードリーダーについては、Citrix担当者にお問い合わせください。セキュアキーパッド機能を有効にするには、リーダー固有のデバイスドライバーが必要になる場合があります。

- クラス3スマートカードリーダーには、セキュアディスプレイも含まれています。クラス3スマートカードリーダーはサポートされていません。
- クラス4のスマートカードリーダーには、セキュアトランザクションモジュールも含まれています。クラス4のスマートカードリーダーはサポートされていません。

注:

スマートカードリーダーのクラスは、USBデバイスクラスとは関係ありません。

スマートカードリーダーは、ユーザーデバイスに適切なデバイスドライバーをインストールする必要があります。

サポートされているスマートカードリーダーについては、使用しているCitrix Workspaceアプリのドキュメントを参照してください。Citrix Workspaceアプリのドキュメントでは、サポートされているバージョンはスマートカードの記事またはシステム要件の記事に記載されています。

ユーザーエクスペリエンス

スマートカードのサポートは、Citrix Virtual Apps and Desktopsに統合されており、特定のICA/HDXスマートカード仮想チャネルを使用します。これはデフォルトで有効になっています。

重要：スマートカードリーダーに汎用USBリダイレクトを使用しないでください。これはスマートカードリーダーではデフォルトで無効になっており、有効にした場合でもサポートされません。

同じユーザーデバイスで複数のスマートカードと複数のリーダーを使用できますが、パススルー認証を使用している場合は、ユーザーが仮想デスクトップまたはアプリケーションを起動するときに、スマートカードを1枚だけ挿入する必要があります。アプリケーション内でスマートカードを使用する場合（デジタル署名や暗号化機能など）、スマートカードの挿入やPINの入力が求められることがあります。これは、複数のスマートカードが同時に挿入されている場合に発生する可能性があります。

- スマートカードがリーダーに挿入されているにもかかわらず、スマートカードの挿入を求められた場合、ユーザーはキャンセルを選択する必要があります。
- ユーザーがPINの入力を求められた場合、PINを再度入力する必要があります。

PINは、カード管理システムまたはベンダーユーティリティを使用してリセットできます。

重要:

Citrix Virtual AppsまたはCitrix Virtual Desktopsセッション内で、Microsoftリモートデスクトップ接続アプリケーションとスマートカードを使用することはサポートされていません。これは「ダブルホップ」の使用と呼ばれることがあります。

スマートカードを展開する前に

- スマートカードリーダー用のデバイスドライバーを入手し、ユーザーデバイスにインストールします。多くのスマートカードリーダーは、Microsoftが提供するCCIDデバイスドライバーを使用できます。
- スマートカードベンダーからデバイスドライバーと暗号化サービスプロバイダー (CSP) ソフトウェアを入手し、ユーザーデバイスと仮想デスクトップの両方にインストールします。ドライバーとCSPソフトウェアはCitrix Virtual Apps and Desktopsと互換性がある必要があります。互換性についてはベンダーのドキュメントを確認してください。ミニドライバーモデルをサポートおよび使用するスマートカードを使用する仮想デスクトップの場合、スマートカードミニドライバーは自動的にダウンロードされますが、(http://catalog.update.microsoft.com/) またはベンダーから入手することもできます。また、PKCS#11ミドルウェアが必要な場合は、カードベンダーから入手してください。
- 重要: Citrixソフトウェアをインストールする前に、物理コンピューターにドライバーとCSPソフトウェアをインストールしてテストすることをお勧めします。
- Windows 10でInternet Explorerを使用してスマートカードを使用するユーザーのために、Citrix Receiver™ for WebのURLを信頼済みサイトリストに追加します。Windows 10では、Internet Explorerは信頼済みサイトに対してデフォルトで保護モードで実行されません。
- 公開鍵インフラストラクチャ (PKI) が適切に構成されていることを確認します。これには、Active Directory環境で証明書とアカウントのマッピングが正しく構成されており、ユーザー証明書の検証が正常に実行できることを確認することが含まれます。
- 展開が、Citrix WorkspaceアプリやStoreFrontなど、スマートカードで使用される他のCitrixコンポーネントのシステム要件を満たしていることを確認します。
- サイト内の以下のサーバーへのアクセスを確保します。
    - スマートカード上のログオン証明書に関連付けられているユーザーアカウントのActive Directoryドメインコントローラー

- デリバリーコントローラー™
- Citrix ストアフロント
- Citrix ゲートウェイ/Citrix アクセスゲートウェイ 10.x
- VDA
- (Remote PC Access の場合、オプション): Microsoft Exchange Server

スマートカードの使用を有効にする

ステップ1. カード発行ポリシーに従って、ユーザーにスマートカードを発行します。

ステップ2. (オプション) リモートPCアクセスを有効にするために、スマートカードを設定します。

ステップ3. スマートカードのリモーティング用に、Delivery ControllerとStoreFrontをインストールして構成します (まだインストールされていない場合)。

ステップ4. スマートカードの使用のためにStoreFrontを有効にします。詳細については、StoreFrontのドキュメントの「スマートカード認証の構成」を参照してください。

ステップ5. スマートカードの使用のためにCitrix Gateway/Access Gatewayを有効にします。詳細については、NetScalerのドキュメントの「認証と承認の構成」および「Webインターフェイスでのスマートカードアクセスの構成」を参照してください。

ステップ6. スマートカードの使用のためにVDAを有効にします。

- VDAに必要なアプリケーションと更新プログラムがあることを確認します。
- ミドルウェアをインストールします。
- スマートカードのリモーティングを設定し、ユーザーデバイス上のCitrix Workspaceアプリと仮想デスクトップセッション間のスマートカードデータの通信を有効にします。

ステップ7. スマートカードの使用のためにユーザーデバイス (ドメイン参加済みまたは非ドメイン参加済みのマシンを含む) を有効にします。詳細については、StoreFrontのドキュメントの「スマートカード認証の構成」を参照してください。

- 証明機関のルート証明書と発行証明機関の証明書をデバイスのキーストアにインポートします。
- ベンダーのスマートカードミドルウェアをインストールします。

- Windows用Citrix Workspaceアプリをインストールして構成します。その際、グループポリシー管理コンソールを使用してicaclient.admをインポートし、スマートカード認証を有効にしてください。

ステップ8. 展開をテストします。テストユーザーのスマートカードを使用して仮想デスクトップを起動し、展開が正しく構成されていることを確認します。可能なすべてのアクセスメカニズム (たとえば、Internet ExplorerおよびCitrix Workspaceアプリを介したデスクトップへのアクセス) をテストします。

スマートカードリーダーの挿入回数を追跡する

スマートカードのリモーティングを使用すると、SCardGetStatusChange関数を使用して、スマートカードがリーダーに挿入または取り外された回数を追跡できます。この関数は、監視するリーダーごとに1つずつ、SCARD_READERSTATEデータ構造の配列を更新します。各SCARD_READERSTATEのdwEventStateフィールドの上位ワード (16ビット) には、リーダーカウントが含まれています。詳細については、Microsoftの記事「SCardGetStatusChangeA function」および「SCARD_READERSTATEA structure」を参照してください。

リーダー挿入回数レポート設定は、デフォルトで無効になっています。追跡を有効にするには、次のレジストリキーを追加します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

名前: EnableReaderInsertCountReporting

種類: DWORD

値: ゼロ以外の任意の値

セッションが切断されると、カウントはゼロにリセットされます。

リーダー挿入回数レポートは、サードパーティのスマートカードミドルウェアと互換性があります。

スマートカードの展開

この製品バージョンおよびこのバージョンを含む混在環境では、以下の種類のスマートカード展開がサポートされています。その他の構成も動作する可能性がありますが、サポートされていません。

タイプ	STOREFRONT™ 接続
ローカルのドメイン参加済みコンピューター	直接接続
ドメイン参加済みコンピューターからのリモートアクセス	Citrix Gateway 経由で接続
ドメインに参加していないコンピューター	直接接続
ドメインに参加していないコンピューターからのリモートアクセス	Citrix Gateway経由で接続
ドメインに参加していないコンピューターおよびシンクライアントがDesktop Applianceサイトにアクセスする場合	Desktop Applianceサイト経由で接続
ドメイン参加済みコンピューターおよびシンクライアントがXenApp® Services URL経由でStoreFrontにアクセスする場合	XenApp Services URL経由で接続

展開タイプは、スマートカードリーダーが接続されているユーザーデバイスの特性によって定義されます。

- デバイスがドメイン参加済みか、ドメイン非参加か。
- デバイスがStoreFrontにどのように接続されているか。
- 仮想デスクトップとアプリケーションの表示にどのソフトウェアが使用されているか。

さらに、Microsoft WordやMicrosoft Excelなどのスマートカード対応アプリケーションをこれらの展開で使用できます。これらのアプリケーションを使用すると、ユーザーはドキュメントにデジタル署名したり、暗号化したりできます。

バイモーダル認証

これらの展開のそれぞれにおいて、可能な場合、Receiverはスマートカードの使用とユーザー名およびパスワードの入力の選択肢をユーザーに提供することで、バイモーダル認証をサポートします。これは、スマートカードが使用できない場合（たとえば、ユーザーが自宅に忘れた場合やログオン証明書の有効期限が切れた場合）に役立ちます。

ドメイン非参加デバイスのユーザーはReceiver for Windowsに直接ログオンするため、明示的な認証にフォールバックできるようにすることができます。バイモーダル認証を構成すると、ユーザー

は最初にスマートカードとPINを使用してログオンするように求められますが、スマートカードに問題が発生した場合は、明示的な認証を選択するオプションがあります。

Citrix Gatewayを展開する場合、ユーザーはデバイスにログオンし、Receiver for WindowsによってCitrix Gatewayへの認証を求められます。これは、ドメイン参加済みデバイスとドメイン非参加デバイスの両方に適用されます。ユーザーは、スマートカードとPIN、または明示的な資格情報のいずれかを使用してCitrix Gatewayにログオンできます。これにより、Citrix Gatewayログオンにバイモーダル認証をユーザーに提供できます。Citrix GatewayからStoreFrontへのパススルー認証を構成し、スマートカードユーザーの資格情報検証をCitrix Gatewayに委任することで、ユーザーはStoreFrontにサイレント認証されます。

複数のActive Directoryフォレストに関する考慮事項

Citrix環境では、スマートカードは単一のフォレスト内でサポートされます。フォレストをまたがるスマートカードログオンには、すべてのユーザーアカウントへの直接的な双方向フォレスト信頼が必要です。スマートカードを含むより複雑なマルチフォレスト展開（つまり、信頼が一方通行であるか、異なるタイプである場合）はサポートされていません。

リモートデスクトップを含むCitrix環境でスマートカードを使用できます。この機能は、ローカル（スマートカードが接続されているユーザーデバイス上）またはリモート（ユーザーデバイスが接続するリモートデスクトップ上）にインストールできます。

スマートカード取り外しポリシー

製品に設定されているスマートカード取り外しポリシーは、セッション中にリーダーからスマートカードを取り外した場合に何が起こるかを決定します。スマートカード取り外しポリシーは、Windowsオペレーティングシステムを介して構成および処理されます。

ポリシー設定	デスクトップの動作
アクションなし	アクションなし。
ワークステーションをロック	デスクトップセッションが切断され、仮想デスクトップがロックされます。
強制ログオフ	ユーザーは強制的にログオフされます。ネットワーク接続が失われ、この設定が有効になっている場合、セッションがログオフされ、ユーザーはデータを失う可能性があります。
リモートターミナルサービスセッションの場合に切断	セッションが切断され、仮想デスクトップがロックされます。

証明書失効チェック

証明書失効チェックが有効になっていて、ユーザーが無効な証明書を含むスマートカードをカードリーダーに挿入した場合、ユーザーは認証できず、その証明書に関連するデスクトップまたはアプリケーションにアクセスできません。たとえば、無効な証明書がメールの復号化に使用されている場合、メールは暗号化されたままになります。認証に使用されるものなど、カード上の他の証明書がまだ有効な場合、それらの機能はアクティブなままです。

展開例：ドメイン参加済みコンピューター

この展開では、Desktop Viewer を実行し、StoreFront に直接接続するドメイン参加済みユーザーデバイスを使用します。

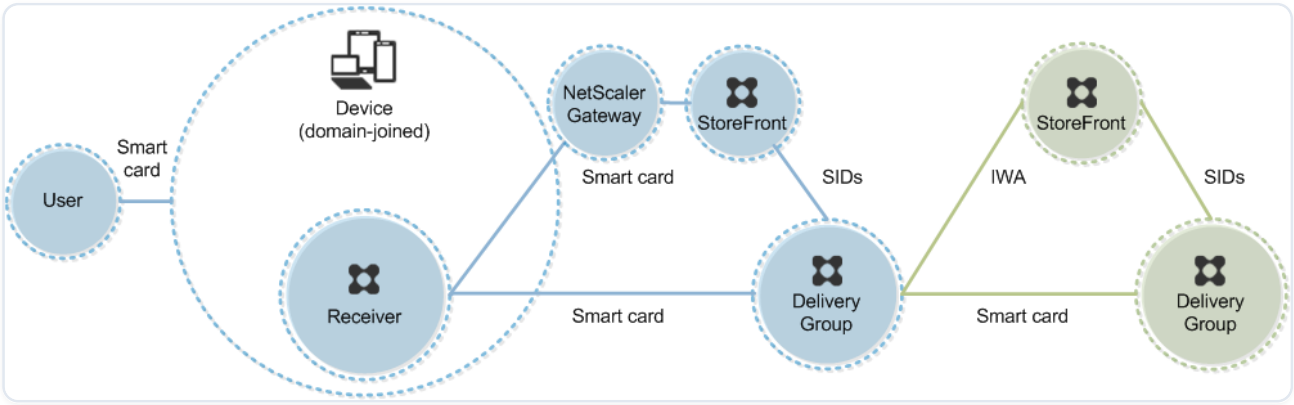
展開例：ドメイン参加済みコンピューター(/en-us/citrix-virtual-apps-desktops/2411/media/smartcard1_1.png)

ユーザーはスマートカードとPINを使用してデバイスにログオンします。Receiverは、統合Windows認証 (IWA) を使用して、ユーザーをStoreFrontサーバーに認証します。StoreFrontは、ユーザーセキュリティ識別子 (SID) をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、Receiverでシングルサインオン機能が構成されているため、PINの入力を再度求められることはありません。

この展開は、2つ目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2つ目のStoreFrontサーバーに対して認証を行います。この2つ目の接続には、任意の認証方法を使用できます。最初のホップで示されている構成は、2つ目のホップで再利用することも、2つ目のホップでのみ使用することもできます。

展開例: ドメイン参加済みコンピューターからのリモートアクセス

この展開では、Desktop Viewer を実行し、Citrix Gateway/Access Gateway を介して StoreFront に接続するドメイン参加済みユーザーデバイスが関与します。



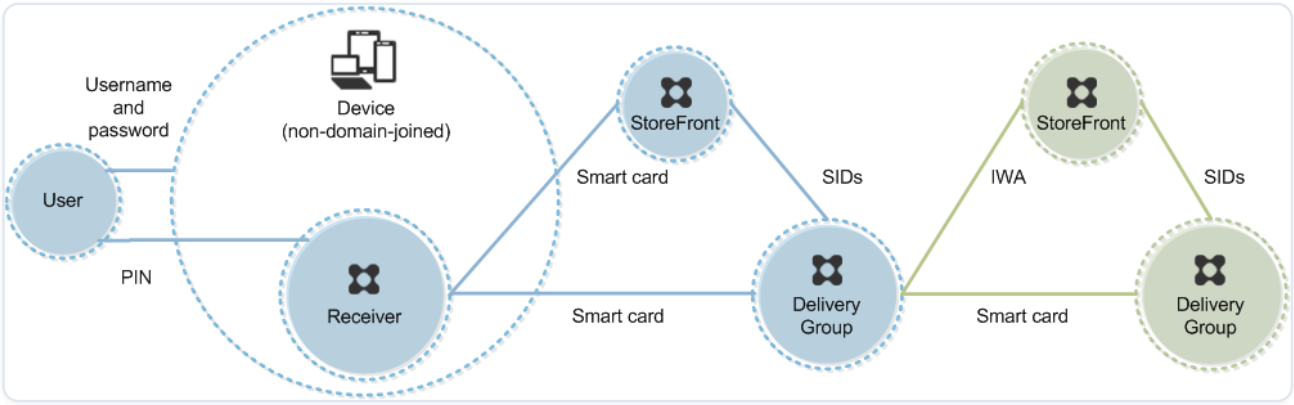
ユーザーはスマートカードとPINを使用してデバイスにログオンし、その後、Citrix Gateway/Access Gatewayに再度ログオンします。この2回目のログオンは、この展開ではReceiverがバイモーダル認証を許可しているため、スマートカードとPIN、またはユーザー名とパスワードのいずれかを使用できます。

ユーザーはStoreFrontに自動的にログオンします。StoreFrontは、ユーザーセキュリティ識別子 (SID) をCitrix Virtual Apps™またはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、Receiverでシングルサインオン機能が構成されているため、PINの入力を再度求められることはありません。

この展開は、2つ目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2つ目のStoreFrontサーバーに対して認証を行います。この2つ目の接続には、任意の認証方法を使用できます。最初のホップで示されている構成は、2つ目のホップで再利用することも、2つ目のホップでのみ使用することもできます。

展開例: ドメインに参加していないコンピューター

この展開には、Desktop Viewerを実行し、StoreFrontに直接接続するドメインに参加していないユーザーデバイスが含まれます。



ユーザーはデバイスにログオンします。通常、ユーザーはユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンの資格情報はオプションです。この展開ではバイモーダル認証が可能であるため、Receiverはユーザーにスマートカードと PIN、またはユーザー名とパスワードのいずれかを要求します。その後、ReceiverはStoreFrontに対して認証を行います。

StoreFrontは、ユーザーセキュリティ識別子 (SID) をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、この展開ではシングルサインオン機能が利用できないため、PINの入力を再度求められます。

この展開は、2つ目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2つ目のStoreFront

サーバーに対して認証を行います。この2つ目の接続には、任意の認証方法を使用できます。最初のホップで示されている構成は、2つ目のホップで再利用することも、2つ目のホップでのみ使用することもできます。

展開例: ドメインに参加していないコンピューターからのリモートアクセス

この展開では、Desktop Viewer を実行し、StoreFront に直接接続するドメイン非参加のユーザーデバイスが関与します。

展開例: ドメイン非参加コンピューターからのリモートアクセス(/en-us/citrix-virtual-apps-desktops/2411/media/smartcard4_1.png)

ユーザーはデバイスにログオンします。通常、ユーザーはユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンの資格情報はオプションです。この展開ではバイモーダル認証が可能であるため、Receiver はユーザーにスマートカードとPIN、またはユーザー名とパスワードのいずれかを要求します。その後、Receiver はStoreFrontに対して認証を行います。

StoreFront はユーザーセキュリティ識別子 (SID) を Citrix Virtual Apps または Citrix Virtual Desktops に渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、この展開ではシングルサインオン機能が利用できないため、ユーザーは再度PINの入力を求められます。

この展開は、2台目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2台目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示された構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: Desktop Appliance サイトにアクセスするドメイン非参加コンピューターとシンクライアント

この展開では、Desktop Lock を実行し、Desktop Appliance サイトを通じてStoreFrontに接続する可能性のあるドメイン非参加のユーザーデバイスが関与します。

Desktop Lock は、Citrix Virtual Apps、Citrix Virtual Desktops、および VDI-in-a-Box とともにリリースされる別のコンポーネントです。これは Desktop Viewer の代替であり、主に再利用された Windows コンピューターおよび Windows シンクライアント向けに設計されています。Desktop Lock は、これらのユーザーデバイスの Windows シェルとタスクマネージャーを置き換え、ユーザーが基盤となるデバイスにアクセスするのを防ぎます。Desktop Lock を使用すると、ユーザー

は Windows Server Machine デスクトップおよび Windows Desktop Machine デスクトップにアクセスできます。Desktop Lock のインストールはオプションです。

展開例: Desktop Appliance サイトにアクセスするドメイン非参加コンピューターとシンクライアント(/en-us/citrix-virtual-apps-desktops/2411/media/smartcard5_1.png)

ユーザーはスマートカードを使用してデバイスにログオンします。デバイスで Desktop Lock が実行されている場合、デバイスはキオスクモードで実行されている Internet Explorer を介して Desktop Appliance サイトを起動するように構成されます。サイト上の ActiveX コントロールがユーザーにPINを要求し、それをStoreFrontに送信します。StoreFront はユーザーセキュリティ識別子 (SID) を Citrix Virtual Apps または Citrix Virtual Desktops に渡します。割り当てられたデスクトップグループのアルファベット順リストで最初に利用可能なデスクトップが起動します。

この展開は、2台目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2台目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示された構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: XenApp Services URL を介して StoreFront にアクセスするドメイン参加コンピューターとシンクライアント

この展開では、Desktop Lock を実行し、XenApp Services URL を介して StoreFront に接続するドメイン参加のユーザーデバイスが関与します。

Desktop Lock は、Citrix Virtual Apps、Citrix Virtual Desktops、および VDI-in-a-Box とともにリリースされる別のコンポーネントです。これは Desktop Viewer の代替であり、主に再利用された Windows コンピューターおよび Windows シンクライアント向けに設計されています。Desktop Lock は、これらのユーザーデバイスの Windows シェルとタスクマネージャーを置き換え、ユーザーが基盤となるデバイスにアクセスするのを防ぎます。Desktop Lock を使用すると、ユーザーは Windows Server Machine デスクトップおよび Windows Desktop Machine デスクトップにアクセスできます。Desktop Lock のインストールはオプションです。

展開例: XenApp Services URL を介して StoreFront にアクセスするドメイン参加コンピューターとシンクライアント(/en-us/citrix-virtual-apps-desktops/2411/media/smartcard6.png)

ユーザーはスマートカードとPINを使用してデバイスにログオンします。デバイスでDesktop Lockが実行されている場合、統合Windows認証 (IWA) を使用してユーザーをStoreFrontサーバーに認証します。StoreFrontは、ユーザーセキュリティ識別子 (SID) をCitrix Virtual AppsまたはCitrix Virtual

Desktopsに渡します。ユーザーが仮想デスクトップを起動すると、Receiverでシングルサインオン機能が構成されているため、PINの再入力を求められることはありません。

この展開は、2つ目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2つ目のStoreFrontサーバーに認証します。この2つ目の接続には、任意の認証方法を使用できます。最初のホップで示された構成は、2つ目のホップで再利用することも、2つ目のホップでのみ使用することもできます。

スマートカードによるパススルー認証とシングルサインオン

パススルー認証

スマートカードによる仮想デスクトップへのパススルー認証は、Windows 10、Windows 8、およびWindows 7 SP1 Enterprise/Professional Editionを実行しているユーザーデバイスでサポートされています。

スマートカードによるホスト型アプリケーションへのパススルー認証は、Windows Server 2012およびWindows Server 2008 R2 SP1を実行しているサーバーでサポートされています。

スマートカードホスト型アプリケーションでパススルー認証を使用するには、サイトの認証方法としてスマートカードによるパススルーを構成する際に、Kerberosの使用を有効にしてください。

注：スマートカードによるパススルー認証の利用可能性は、以下を含む（ただしこれらに限定されない）多くの要因に依存します。

- パススルー認証に関する組織のセキュリティポリシー。
- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアのPINキャッシュポリシー。

スマートカードによるパススルー認証はCitrix StoreFrontで構成されます。詳細については、StoreFrontのドキュメントを参照してください。

シングルサインオン

シングルサインオンは、仮想デスクトップおよびアプリケーションの起動時にパススルー認証を実装するCitrixの機能です。この機能は、ドメイン参加済み、StoreFrontへの直接接続、およびドメイン参加済み、NetScalerからStoreFrontへのスマートカード展開で使用でき、ユーザーがPINを

入力する回数を減らすことができます。これらの展開タイプでシングルサインオンを使用するには、StoreFrontサーバーにあるdefault.icaファイルで以下のパラメーターを編集します。

- ドメイン参加済み、StoreFrontへの直接接続スマートカード展開 — DisableCtrlAltDelをOffに設定
- ドメイン参加済み、NetScalerからStoreFrontへのスマートカード展開 — UseLocalUserAndPasswordをOnに設定

これらのパラメーターの設定に関する詳細な手順については、StoreFrontまたはCitrix Gatewayのドキュメントを参照してください。

シングルサインオン機能の可用性は、以下を含む（ただしこれらに限定されない）多くの要因に依存します。

- シングルサインオンに関する組織のセキュリティポリシー。
- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアのPINキャッシュポリシー。

注：

ユーザーがスマートカードリーダーが接続されたマシン上のVirtual Delivery Agent (VDA)にログオンすると、スマートカードやパスワードなど、以前に成功した認証モードを表すWindowsタイルが表示されることがあります。その結果、シングルサインオンが有効になっている場合、シングルサインオンタイルが表示されることがあります。ログオンするには、シングルサインオンタイルは機能しないため、ユーザーは別のタイルを選択するために**ユーザーの切り替え**を選択する必要があります。

デリバリーコントローラーで TLS を有効にする

デフォルトでは、HTTP と HTTPS の両方が有効になっています。HTTPS は、サーバーの FQDN を共通名として使用する自己署名証明書を使用しますが、StoreFront™ や Web ブラウザーからは信頼されません。

delivery controller™ で TLS を有効にするには、次の操作を行う必要があります。

- すべてのデリバリーコントローラーでサーバー証明書を取得、インストール、および登録します。詳細については、「証明書の要求とインストール」を参照してください。

- TLS 証明書を使用してポートを構成します。詳細については、「証明書のインストール」を参照してください。
- モニターサービスで HTTPS を有効にする。
- HTTP を無効にして HTTPS トラフィックを強制します。詳細については、「HTTPS トラフィックのみを強制する」を参照してください。
- 必要に応じて、Controller が HTTP および HTTPS トラフィックをリッスンするために使用するポートを変更できます。詳細については、「HTTP または HTTPS ポートの変更」を参照してください。

証明書の要求とインストール

TLS を使用するには、共通名またはサブジェクトの別名がサーバーの FQDN と一致する証明書をインストールする必要があります。delivery controller の前にロードバランサーを使用している場合は、サーバーとロードバランサーの両方の FQDN をサブジェクトの別名として含めます。詳細については、「証明書」を参照してください。StoreFront が delivery controller に接続するには、RSA デジタル署名アルゴリズムを使用する必要があります。StoreFront は ECDSA アルゴリズムを使用する証明書をサポートしていません。

SSL/TLS リスナーポートの構成

Web Studio および Director の一部としてインストールされる IIS Windows コンポーネントが同じサーバーにインストールされている場合は、IIS を使用して TLS を構成できます。詳細については、「Web Studio および Director で TLS を有効にする」を参照してください。それ以外の場合は、PowerShell を使用して証明書を構成するには、次の手順を実行します。

1. 既存の証明書がバインドされているかを確認するには、コマンドプロンプトを開き、`netsh http show sslcert` を実行します。

   ```
   netsh http show sslcert
   ```

2. 既存のバインドがある場合は、それを削除します。

   ```
   netsh http delete sslcert ipport=0.0.0.0:443
   ```

   既存のバインドで特定の IP アドレスとポートが指定されていた場合は、`0.0.0.0:443` をその IP アドレスとポートに置き換えます。

3. 以前にインストールした証明書のサムプリントを見つけます。サムプリントを表示するには、**コンピューター証明書の管理**を開き、証明書を参照して開き、**詳細**タブに移動します。

サムプリントを示す証明書のプロパティのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2411/media/certificate-thumbprint.png)

または、PowerShellを使用することもできます。たとえば、次のスクリプトは、サーバーのホスト名と共通名が一致する証明書を検索し、サムネイルを出力します。

```
$HostName =
([System.Net.Dns]::GetHostByName(($env:computerName))).Hostname

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.Subject -match ("CN=" + $HostName)}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $
($Thumbprint)" -Foreground Yellow
```

証明書の共通名がホスト名と一致しない場合、これは失敗します。ホスト名に対して複数の証明書がある場合、これは連結された複数のサムプリントを返し、適切なサムプリントを選択する必要があります。

次の例では、フレンドリ名で証明書を検索します。

```
$friendlyName = "My certificate name"

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.FriendlyName -eq $friendlyNam}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $friendlyName: $
($Thumbprint)" -Foreground Yellow
```

指定されたフレンドリ名を持つ証明書が複数ある場合、これは連結された複数のサムプリントを返し、適切なサムプリントを選択する必要があります。

4. 証明書をポートにバインドするには、`netsh http add sslcert`コマンドを使用します。

```
netsh http add sslcert ipport=[IP address]:443 certhash=[certificate
hash] appid=[application GUID] disablelegacytls=enable
```

- `ipport`: IPアドレスとポート。0.0.0.0:443を使用すると、すべてのIPアドレスに適用されます。代わりに特定のIPアドレスを指定することもできます。
- `certhash`: 前の手順で特定した証明書のサムプリント。

- `appid`: シトリックス ブローカー サービスのGUID。

  > **注:**
  >
  > 証明書を更新または再バインドする際は、任意のGUIDではなく、Broker Serviceに関連付けられた特定の`appid`を使用してください。

  Citrix Broker Serviceの正しい`appid`を見つけるには：

  a. 管理者としてPowerShellコマンドウィンドウを開き、次のコマンドを実行します。

  ```
  Get-WmiObject -Class Win32_Product | Select-String -Pattern
  "broker"
  ```

  b. 出力でCitrix Broker ServiceのIdentifyingNumber (GUID) を見つけます (例: `{D333C884-187F-447C-8C67-463F33989C8F}`)。このGUIDを`appid`パラメーターに使用します。

- `disablelegacytls=enable`: レガシーバージョンのTLSを無効にします。このパラメーターはWindows 2022以降で利用可能です。Windows 2022ではTLS 1.0および1.1を無効にします。Windows 2025では、TLS 1.0および1.1がデフォルトで無効になっているため、これは不要です。

たとえば、次のコマンドを実行して、サムプリント`bc96f958848639fd101a793b87915d5f2829b0b6`の証明書をすべてのIPアドレスのポート`443`にバインドします。

```
netsh http add sslcert ipport=0.0.0.0:443
certhash=bc96f958848639fd101a793b87915d5f2829b0b6 appid={91fe7386-
e0c2-471b-a252-1e0a805febac} disablelegacytls=enable
```

HTTPSを有効にしたら、StoreFront展開 とNetscaler Gatewayを、デリバリーコントローラーへの接続にHTTPではなくHTTPSを使用するように構成する必要があります。

HTTPS 用のモニターサービス OData API を構成する

モニターサービスは、Citrix®およびサードパーティアプリケーションがデータを照会できるように、OData v3およびv4 APIを提供します。DirectorはOData API V3を使用して監視サービスに接続します。HTTPS用にモニターOData APIを構成するには、次の手順を実行します。

1. 次のPowerShellを実行します。

```
$serviceGroup = Get-ConfigRegisteredServiceInstance -ServiceType
Monitor | Select -First 1 ServiceGroupUid

Remove-ConfigServiceGroup -ServiceGroupUid
$serviceGroup.ServiceGroupUid

& 'C:\Program Files\Citrix\Monitor\Service\citrix.monitor.exe'
-ConfigureFirewall -RequireODataTls –OdataPort 443 -RequireODataSdkTls
–OdataSdkPort 443

get-MonitorServiceInstance | register-ConfigServiceInstance

Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-
MonitorServiceGroupMembership
```

2. テキストエディターでファイル `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` を開きます。要素 `<add key="owin:baseAddress" value="http://localhost/citrix/monitor/odata/v4" />` を見つけて、`<add key="owin:baseAddress" value="https://localhost/citrix/monitor/odata/v4" />` に変更します。

暗号スイートを構成する

暗号スイートの順序リストには、`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` または `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` の暗号スイート（またはその両方）を含める必要があります。また、これらの暗号スイートは、`TLS_DHE_` の暗号スイートよりも前に配置する必要があります。

1. Microsoftグループポリシーエディターを使用して、**コンピューターの構成 > 管理用テンプレート > ネットワーク > SSL構成設定** に移動します。
2. 「SSL暗号スイートの順序」ポリシーを編集します。デフォルトでは、このポリシーは「未構成」に設定されています。このポリシーを「有効」に設定します。
3. スイートを正しい順序に並べ替えます。使用したくない暗号スイートは削除します。

`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` または `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` のいずれかが、`TLS_DHE_` の暗号スイートよりも前に来るようにしてください。

Microsoft Learn で、TLS 暗号スイートの順序の構成 も参照してください。

HTTPS トラフィックのみを強制する

XML ServiceをHTTPトラフィックを無視するように構成することをお勧めします。

1. `regedit` を実行します。
2. `HKLM\Software\Citrix\DesktopServer\` を開く
3. `XmlServicesEnableNonSsl` という名前の新しいDWORD値を作成し、0に設定します。
4. Broker Serviceを再起動します。

HTTPSトラフィックを無視するために作成できる対応するレジストリDWORD値 `XmlServicesEnableSsl` があります。これが0に設定されていないことを確認してください。

HTTPまたはHTTPSポートを変更する

デフォルトでは、Controller上のXML Serviceは、HTTPトラフィックにはポート80を、HTTPSトラフィックにはポート443をリッスンします。デフォルト以外のポートを使用することもできますが、Controllerを信頼できないネットワークに公開することによるセキュリティリスクに注意してください。デフォルトを変更するよりも、スタンドアロンのStoreFrontサーバーを展開する方が望ましいです。

Controllerで使用されるデフォルトのHTTPまたはHTTPSポートを変更するには、Studioから次のコマンドを実行します。

```
BrokerService.exe -StoreFrontPort <http-port> -StoreFrontTlsPort <https-port>
```

ここで、`<http-port>` はHTTPトラフィックのポート番号、`<https-port>` はHTTPSトラフィックのポート番号です。

> **注：**
>
> ポートを変更した後、Studioはライセンスの互換性とアップグレードに関するメッセージを表示する場合があります。この問題を解決するには、次のPowerShellコマンドレットシーケンスを使用してサービスインスタンスを再登録します。

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS
|

Unregister-ConfigRegisteredServiceInstance

Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |

Register-ConfigServiceInstance
```

Web StudioとDirectorでTLSを有効にする

Web StudioおよびDirectorへの接続をHTTPSを有効にして保護するために、常にTLSを使用することをお勧めします。この記事では、Web StudioおよびDirectorを信頼された証明書を使用するように構成し、HTTPS経由で安全なアクセスを確保する方法について説明します。

デフォルトの動作

Web Studioをインストールすると、インストーラーは自己署名証明書を作成し、現在のサーバーのポート443にバインドします。ローカルサーバー上のWebブラウザーからHTTPS経由でWeb StudioおよびDirectorにアクセスできます。

ただし、別のマシンからHTTPS経由でWeb StudioまたはDirectorにアクセスしようとすると、ブラウザーは証明書を信頼しないため、セキュリティエラーを表示します。

> **注：**

> Web StudioなしでDirectorをインストールした場合、インストーラーは自己署名証明書を作成しません。

HTTPS経由で安全なアクセスを有効にする

Web Studioサーバー以外のマシンからHTTPS経由でWeb StudioまたはDirectorへのアクセスを許可するには、次の手順に従います。

1. 信頼された証明書を作成またはインポートする。
2. IISで証明書をポート443にバインドする。
3. (オプション) HTTP Strict Transport Security (HSTS) を有効にする。

4. Web Studioがプロキシとして構成されていない場合（クライアントマシンがWeb StudioとDelivery Controllerの両方に接続する場合）、Delivery ControllerでTLSを有効にする。

> **注：**
>
> 自己署名証明書の使用は、各マシンでの手動構成が必要なため、推奨されません。詳細については、「自己署名証明書を使用する」を参照してください。

信頼された証明書を作成またはインポートする

サーバーに接続するマシンによって信頼されている、エンタープライズまたはパブリック認証局からの証明書を使用することをお勧めします。

詳細については、「新しい証明書の作成」および「既存の証明書のインポート」を参照してください。証明書の共通名またはサブジェクトの別名は、ユーザーがWeb StudioまたはDirectorに接続するために使用するFQDNと一致している必要があります。サーバーの前にロードバランサーが展開されている場合は、ロードバランサーのFQDNを使用します。

証明書をポート443にバインドする

信頼された証明書を作成またはインポートした後、IISでポート `443` にバインドします。これは、インストール前またはインストール後に行うことができます。ポート `443` の証明書バインドがすでに構成されている場合、インストーラーは変更を行いません。

> **注:**
>
> デフォルトでは、Web StudioとDirectorはセキュアなHTTPSアクセスにポート443を使用します。必要に応じてポート番号を変更できます。詳細については、デフォルトのポート番号の変更 を参照してください。

> 証明書をポート `443` にバインドするには、次の手順に従います。

1. 管理者としてサーバーにログオンします。
2. IISマネージャーを開き、**サイト > 既定のWebサイト > バインド**に移動します。
3. 種類が**https**の既存のバインドがある場合は、それを選択して**編集...**をクリックします。**https**バインドがない場合は、**追加**をクリックします。

サイトバインドの開き方を強調表示するスクリーンショット(/en-us/citrix-virtual-apps-desktops/2411/media/site-bindings.png)

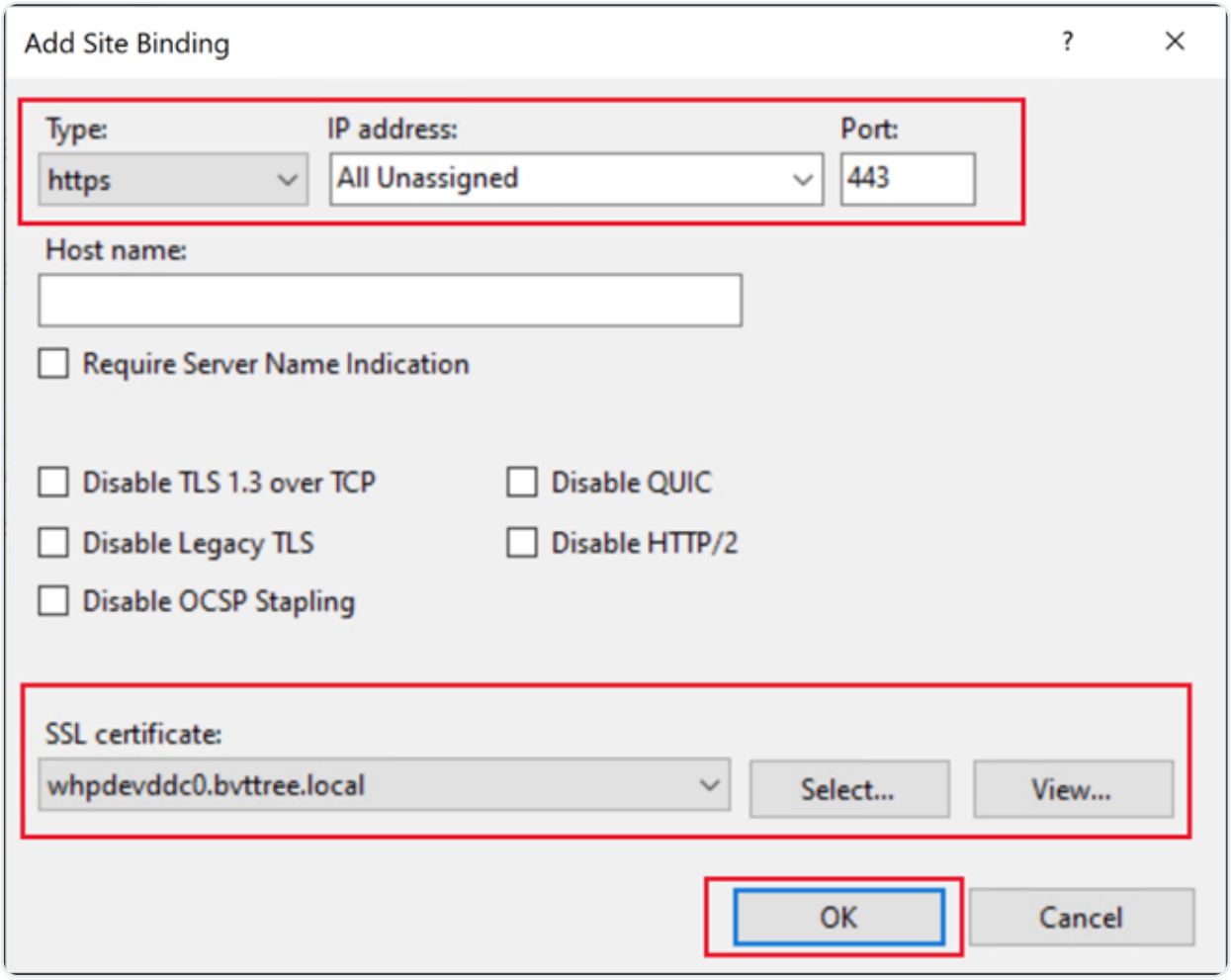
4. サイトバインドを作成または編集します。

   a. 新しいバインドの場合、種類を **https** に、ポートを `443` に設定します。

   b. 適切なSSL証明書を選択します。

   c. Windows Server 2022以降では、必要に応じて、**レガシーTLSを無効にする**を選択して、ユーザーが最新のTLSバージョンのみを使用して接続できるようにします。

   d. **OK**をクリックします。



または、PowerShellを使用して証明書を変更することもできます。たとえば、次のスクリプトは、指定された共通名を持つ証明書を検索し、それをすべてのIPアドレス、ポート443にバインドし、レガシーTLSバージョンを無効にします。

```
$certSName = 'CN=whpdevddc0.bvttree.local'  # The subject name of the
certificate

$certificate = Get-ChildItem -Path Cert:\LocalMachine\My\ | ? {$_.Subject
```

```
-eq $certSName}

netsh http add sslcert ipport=0.0.0.0:443 certhash=$
($certificate.Thumbprint) certstorename=My appid="{91fe7386-e0c2-471b-
a252-1e0a805febac}" disablelegacytls=enable
```

なお、`appid` は、どのアプリケーションが証明書を追加したかを識別するために使用できる任意の GUID です。

自己署名証明書を使用する

既存の自己署名証明書を使用できますが、サーバーにアクセスする各マシンを手動で構成する必要があるため、推奨されません。

Web Studio に接続する必要があるマシンに自己署名証明書をインストールするには、次の手順を実行します。

1. Web StudioおよびDelivery Controllerサーバーから既存の自己署名証明書をエクスポートします。
2. サーバーにアクセスする必要があるマシンの**信頼されたルート証明書**ストアに証明書をインポートします。

(オプション) HTTP Strict Transport Security (HSTS) を有効にする

HTTP Strict Transport Security (HSTS)は、サイトにアクセスする際にHTTPSのみを使用するようにWebブラウザに指示します。ユーザーがHTTPを使用してURLにアクセスしようとすると、ブラウザは自動的にHTTPSに切り替わります。この設定により、クライアント側とサーバー側の両方で安全な接続検証が保証されます。ブラウザは、構成された期間、この検証を維持します。

Windows Server 2019 以降では、IIS で HSTS を構成できます。

1. **インターネットインフォメーションサービス (IIS) マネージャー**を開きます。
2. **既定のWebサイト** (または適切なWebサイト) を選択します。
3. 右側の**「操作」ペインで、「HSTS...」**を選択します。
4. **「有効にする」**を選択し、最大有効期間を入力します (例: 1年間で31536000)。
5. **「HttpをHttpsにリダイレクト」**を選択します。

> **注:**

> Web Studioは、Studio Webサイトにアクセスする際にHTTPをHTTPSにリダイレクトする**URL書き換え**ルールを自動的に構成します。ただし、このオプションはDirectorおよびIISサイト上の他のすべてのアプリケーションにも適用されます。

6. **「OK」**をクリックします。

HSTS設定のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2411/media/iis-hsts.png)

(オプション) デフォルトのポート番号を変更する

デフォルトでは、Web StudioとDirectorはセキュアなHTTPSアクセスにポート443を使用します。このポート番号を変更するには、以下の手順に従って`Default Web Site`で目的のポートのサイトバインディングを作成します。

手順:

1. Web Studioをホストしているサーバーで、**インターネットインフォメーションサービス (IIS) マネージャー**を開きます。
2. **「接続」ペインで、サーバーノードを展開し、「サイト」の下にある「Default Web Site」**を選択します。
3. 右側の**「操作」ペインで、「バインディング」**をクリックします。

新しいポートを設定(/en-us/citrix-virtual-apps-desktops/2411/media/web-studio-new-port.png)

4. **「サイトバインディング」ウィンドウで、「追加」**をクリックします。
5. 「サイトバインドの追加」ウィンドウで、新しいバインドに対して以下を設定します。
   a. **種類**: **https** を選択します。
   b. **IPアドレス**: 適切なIPアドレスを選択するか、該当する場合は「未割り当てのIPすべて」のままにします。
   c. **ポート**: 目的のポート番号を入力します（例: 444）。
   d. **SSL証明書**: セキュアな通信のために適切なSSL証明書を選択します。

> **注:**
>
> Delivery Controller™とWeb Studioが別々のマシンにインストールされており、サーバーに他のサービスやWebサイトが展開されていない場合は、ポート443を削除できます。そ

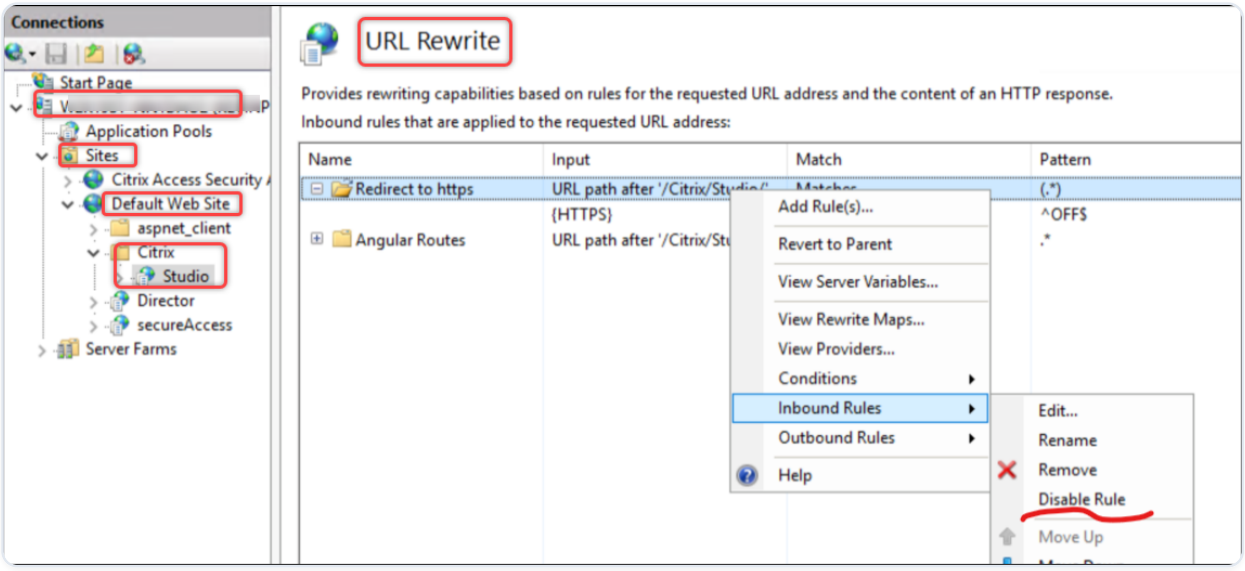
> うでない場合は、オーケストレーションサービスや他のFMAサービスとの通信問題を避けるために、このポートを維持してください。

6. **OK** をクリックしてバインドを保存し、**サイトバインド** ウィンドウを閉じます。
7. **IISマネージャー** でサーバーノードをクリックし、**操作** ペインで **再起動** をクリックして新しいバインドを適用します。

（オプション）HTTPS リダイレクトを無効にする

Web Studio をインストールすると、デフォルトでHTTPアクセスはHTTPSに自動的にリダイレクトされます。このリダイレクトを無効にしてHTTPアクセスを許可することも可能です。この方法は、HTTPアクセスをブロックするための他の対策を講じている場合にのみ推奨されます。Web Studio の前にTLS終端ロードバランサーがある場合でも、ロードバランサーと Web Studio の間ではHTTPSを使用することをお勧めします。

1. Web Studioサーバーにログオンします。
2. **インターネットインフォメーションサービス (IIS) マネージャー** を開き、*Server_name* **> サイト > Default Web Site > URL Rewrite** に移動します。
3. 次のスクリーンショットに示すように、**httpsへのリダイレクト** の **受信規則** を無効にします。



IISでHSTSを有効にしている場合は、**Redirect Http to Https**もクリアする必要があります。

VDA で TLS を有効にする

Citrix Workspace™ アプリと Virtual Delivery Agent (VDA) 間の TLS 接続を有効にするには、次のタスクを完了します。

- VDA に証明書をインストールします。詳細については、「証明書のリクエストとインストール」を参照してください。
- VDA がインストールされているマシンで TLS を構成します。(便宜上、VDA がインストールされているマシンは、以降「VDA」と呼びます。) TLS/DTLS の構成には、Citrix が提供する PowerShell スクリプトを使用することを強くお勧めします。詳細については、「PowerShell スクリプトを使用して VDA で TLS を構成する」を参照してください。ただし、TLS/DTLS を手動で構成する場合は、「VDA で TLS を手動で構成する」を参照してください。
- Studio で一連の PowerShell コマンドレットを実行して、VDA を含むデリバリーグループで TLS を構成します。詳細については、「デリバリーグループで TLS を構成する」を参照してください。

要件と考慮事項:

- コンポーネントのインストール、サイトの作成、マシンカタログの作成、およびデリバリーグループの作成が完了した後で、デリバリーグループと VDA で TLS を構成します。
- デリバリーグループで TLS を構成するには、Controller アクセスルールを変更する権限が必要です。この権限は、フル管理者 (Full Administrator) が持っています。
- VDA で TLS を構成するには、VDA がインストールされているマシンで Windows 管理者である必要があります。
- Machine Creation Services™ または Provisioning Services によってプロビジョニングされたプールされた VDA では、再起動時に VDA マシンイメージがリセットされ、以前の TLS 設定が失われます。VDA が再起動されるたびに PowerShell スクリプトを実行して、TLS 設定を再構成してください。

デリバリーグループには、TLS が構成されている VDA と、TLS が構成されていない VDA を混在させることはできません。デリバリーグループの TLS を構成する前に、そのデリバリーグループ内のすべての VDA に対して TLS がすでに構成されていることを確認してください。

VDA で TLS を構成すると、インストールされている TLS 証明書の権限が変更され、ICA® Service に証明書の秘密キーへの読み取りアクセス権が付与され、ICA Service に次の情報が通知されます。

- TLS に使用する証明書ストア内の証明書。
- TLS 接続に使用する TCP ポート番号。

  Windows ファイアウォール (有効な場合) は、この TCP ポートでの受信接続を許可するように構成する必要があります。この構成は、PowerShell スクリプトを使用すると自動的に行われます。

- 許可するTLSプロトコルのバージョン。

  > **重要:**
  >
  > Citrixでは、TLS 1.2以降の使用を推奨しています。SSLおよびそれ以前のバージョンのTLSは非推奨です。
  >
  > サポートされている TLS プロトコルバージョンは、階層（最低から最高）に従います: SSL 3.0、TLS 1.0、TLS 1.1、TLS 1.2、および TLS 1.3。許可される最小バージョンを指定します。そのバージョンまたはそれより高いバージョンを使用するすべてのプロトコル接続が許可されます。

  たとえば、TLS 1.1を最小バージョンとして指定した場合、TLS 1.1、TLS 1.2、TLS 1.3プロトコル接続が許可されます。SSL 3.0を最小バージョンとして指定した場合、サポートされているすべてのバージョンの接続が許可されます。TLS 1.3を最小バージョンとして指定した場合、TLS 1.3接続のみが許可されます。

- 許可するTLS暗号スイート。

  暗号スイートは、接続に使用される暗号化を選択します。クライアントとVDAは、異なる暗号スイートのセットをサポートできます。クライアント（Citrix Workspaceアプリ）が接続してサポートされているTLS暗号スイートのリストを送信すると、VDAはクライアントの暗号スイートの1つを、構成されている暗号スイートの独自のリスト内の暗号スイートの1つと照合し、接続を受け入れます。一致する暗号スイートがない場合、VDAは接続を拒否します。

  VDAは、3つの暗号スイートセット（コンプライアンスモードとも呼ばれます）をサポートしています：GOV（政府）、COM（商用）、およびALL。許容される暗号スイートは、Windows FIPSモードにも依存します。Windows FIPSモードの詳細については、`<http://support.microsoft.com/kb/811833>`を参照してください。次の表に、各セットの暗号スイートを示します。

暗号スイート	すべて	COM	GOV	すべて	COM	GOV
FIPSモード	オフ	オフ	オフ	オン	オン	オン
TLS_AES_256_G	X		X	X		X

暗号スイート	すべて	COM	GOV	すべて	COM	GOV
CM_SHA384						
TLS_AES_128_GCM_SHA256	X			X		X
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	X	X		X	X	

注:

VDAはDHE暗号スイート（例：TLS_DHE_RSA_WITH_AES_256_GCM_SHA384、TLS_DHE_RSA_WITH_AES_256_CBC_SHA、TLS_DHE_RSA_WITH_AES_128_GCM_SHA256、TLS_DHE_RSA_WITH_AES_128_CBC_SHA）をサポートしていません。Windowsによって選択された場合、接続は失敗します。

> NetScaler Gatewayを使用している場合は、バックエンド通信の暗号スイートサポートに関する情報についてNetScalerのドキュメントを参照してください。TLS暗号スイートのサポートについては、「Citrix ADCアプライアンスで利用可能な暗号」を参照してください。DTLS暗号スイートのサポートについては、「DTLS暗号のサポート」を参照してください。

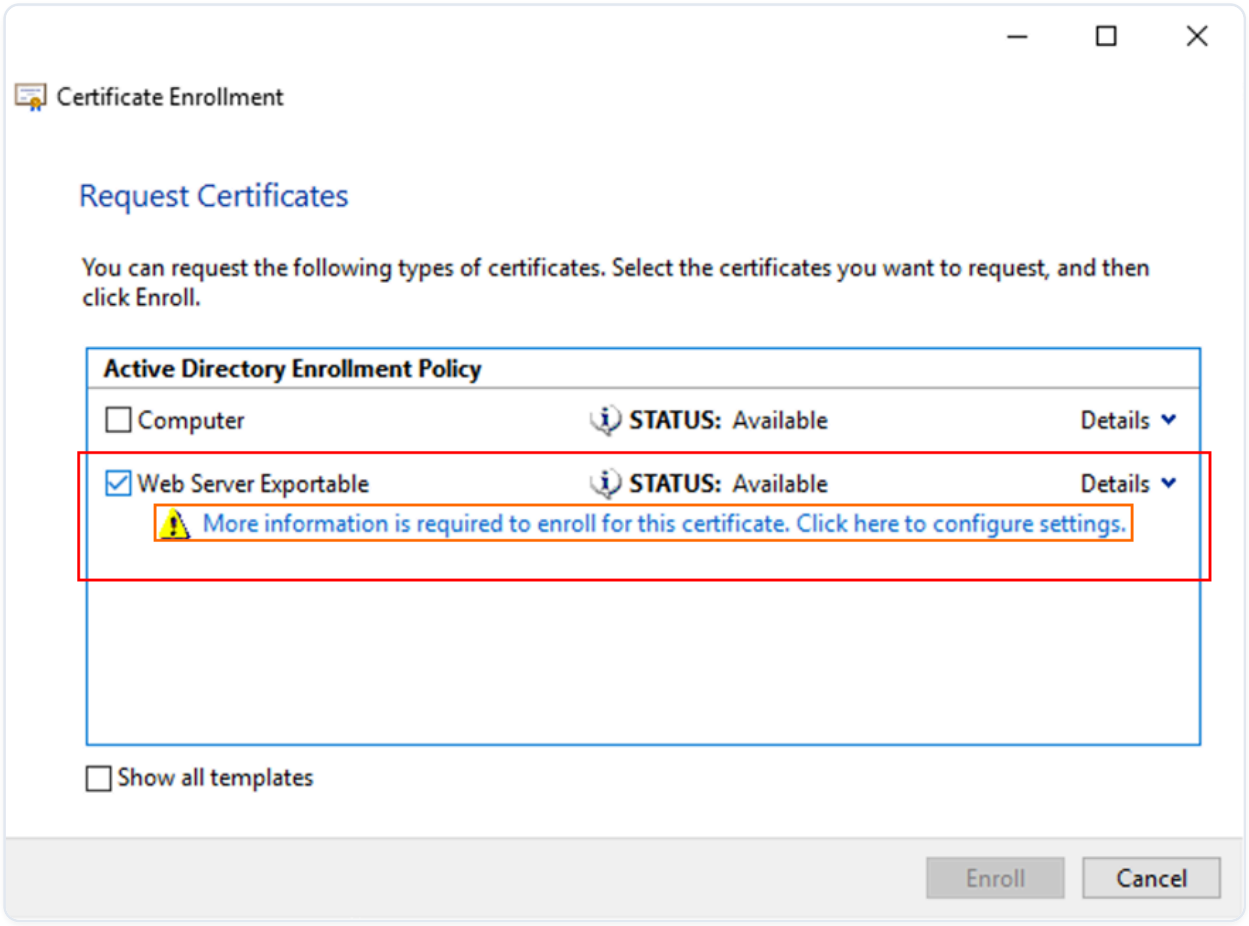
証明書のリクエストとインストール

TLSを使用するには、代替名にVDAのFQDNが含まれる証明書をインストールする必要があります。この証明書は、VDAに直接接続する（Citrix Gatewayを介さない）すべてのクライアントによって信頼されている必要があります。証明書を簡単に展開できない管理対象外のデバイスがVDAに接続できるようにするには、NetScaler® Gatewayの展開を検討してください。

Microsoft証明機関を使用して証明書を作成する

クライアントとVDAが信頼されたフォレストにあり、Microsoft証明機関がある場合、証明書MMCスナップインの証明書登録ウィザードから証明書を取得できます。

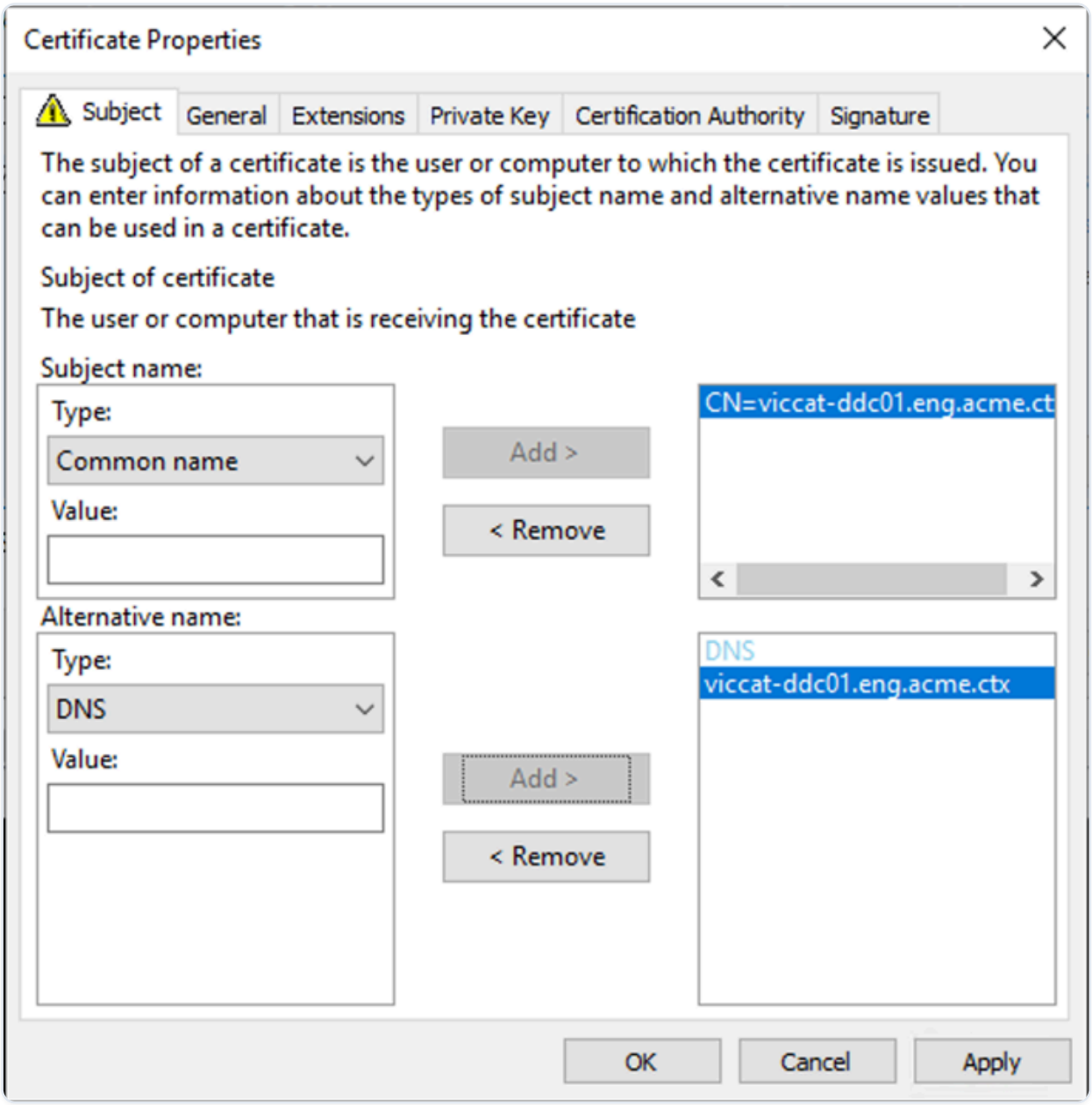
1. VDAで、MMCコンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、コンピューターアカウントを選択します。
2. **個人 > 証明書**を展開し、コンテキストメニューコマンド**すべてのタスク > 新しい証明書のリクエスト**を使用します。
3. 開始するには**次へ**をクリックし、Active Directory登録から証明書を取得することを確認するには**次へ**をクリックします。
4. サーバー認証証明書のテンプレートを選択します。デフォルトのWindowsの**コンピューター**または**Webサーバー（エクスポート可能）**のいずれも使用できます。テンプレートが件名の値を自動的に提供するように設定されている場合は、詳細を指定せずに登録をクリックします。



5. 証明書テンプレートの詳細を指定するには、**詳細**をクリックして以下を構成します。

   サブジェクト名 — 種類として**共通名**を選択し、VDAのFQDNを追加します。

   代替名 — タイプを**DNS**に選択し、VDAのFQDNを追加します



注:

Active Directory証明書サービス証明書の自動登録を使用して、VDAへの証明書の発行と展開を自動化します。これについては、証明書の自動登録を有効にする)で説明しています。

ワイルドカード証明書を使用して、単一の証明書で複数の VDA を保護できます。

サブジェクト名 — タイプを**共通名**に選択し、VDAの*.primary.domainを入力します

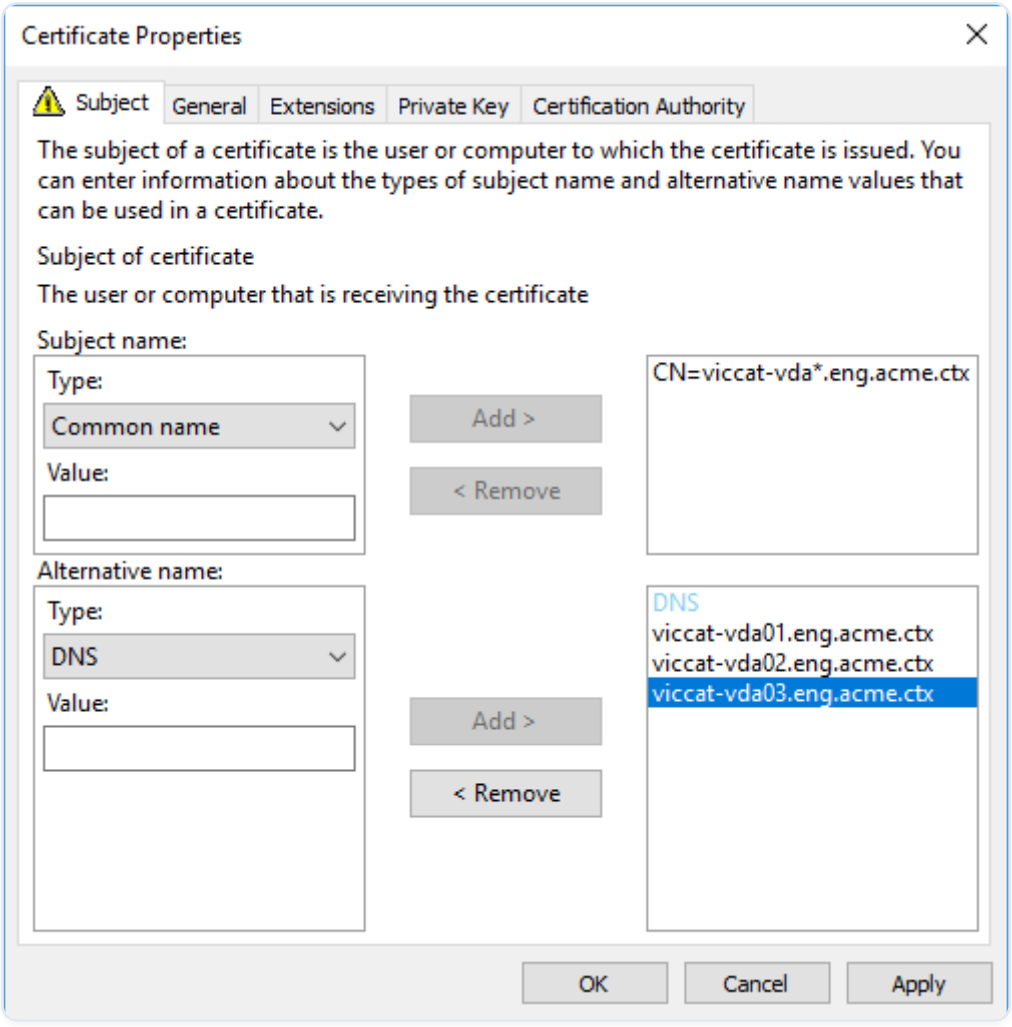
代替名 — タイプを**DNS**に選択し、VDAの*.primary.domainを追加します

ワイルドカード証明書要求ダイアログ(/en-us/citrix-virtual-apps-desktops/2411/media/tls-request-certificates-wildcard.png)

SAN 証明書を使用して、単一の証明書で複数の特定の VDA を保護できます。

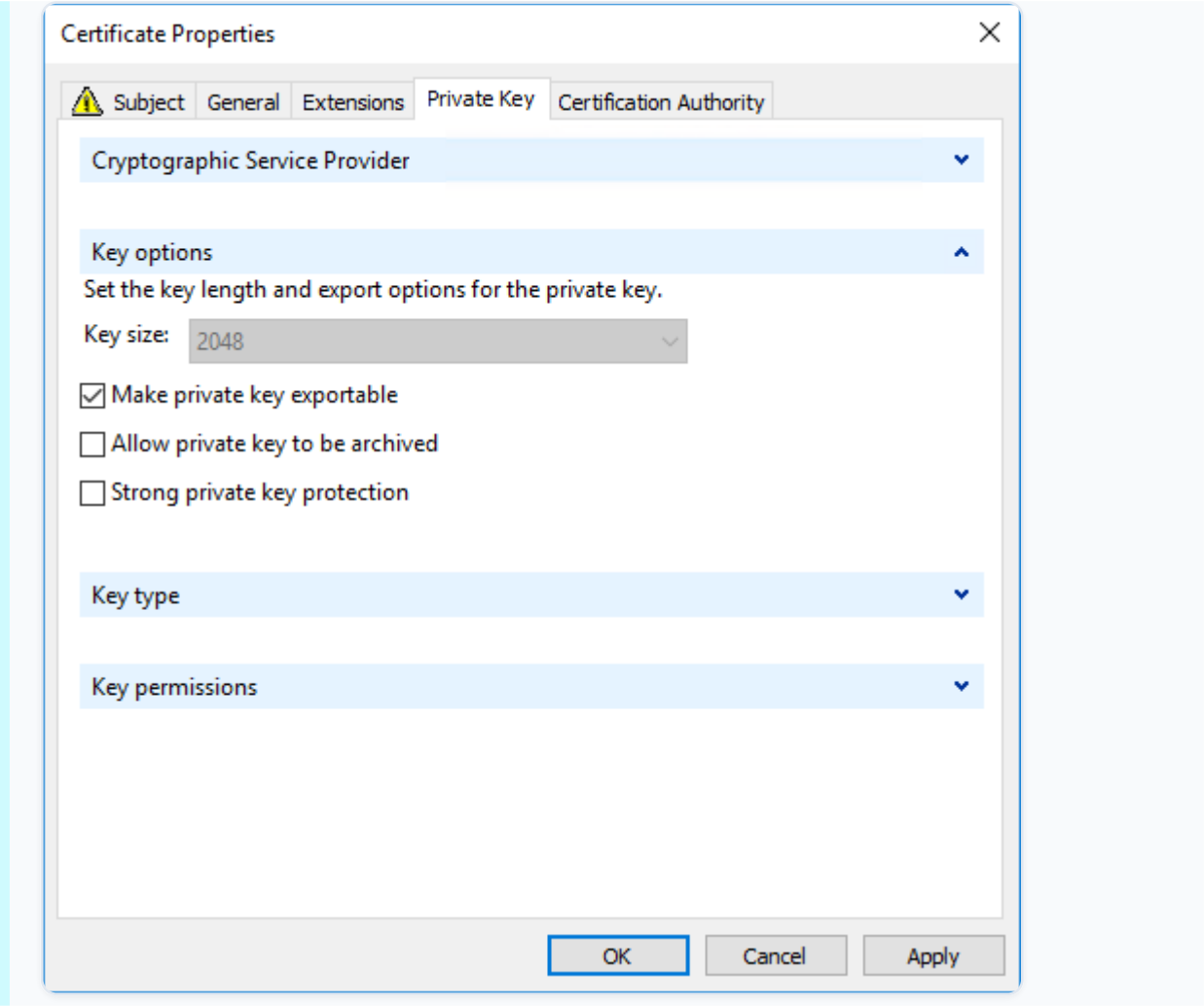
サブジェクト名 — タイプを**共通名**に選択し、証明書の使用状況を識別するのに役立つ文字列を入力します

代替名 — タイプを**DNS**に選択し、各VDAのFQDNのエントリを追加します。最適なTLSネゴシエーションを確保するために、代替名の数を最小限に抑えてください。



注:

ワイルドカード証明書とSAN証明書の両方で、タブで**秘密鍵をエクスポート可能にする**を選択する必要があります。



PowerShellスクリプトを使用してVDAでTLSを構成する

証明書ストアの［ローカルコンピューター］>［個人］>［証明書］領域にTLS証明書をインストールします。その場所に複数の証明書がある場合は、証明書のサムプリントをPowerShellスクリプトに指定します。

> **注:**
>
> XenAppおよびXenDesktop 7.15 LTSR以降、PowerShellスクリプトはVDAのFQDNに基づいて正しい証明書を検索します。VDAのFQDNに対して単一の証明書のみが存在する場合、サムプリントを指定する必要はありません。

Enable-VdaSSL.ps1スクリプトは、VDAでTLSリスナーを有効または無効にします。このスクリプトは、インストールメディアの*Support* > *Tools* > *SslSupport*フォルダーにあります。

TLSを有効にすると、DHE暗号スイートは無効になります。ECDHE暗号スイートは影響を受けません。

TLSを有効にすると、スクリプトは指定されたTCPポートの既存のWindowsファイアウォール規則をすべて無効にします。次に、ICAサービスがTLS TCPポートとUDPポートでのみ受信接続を受け入れることを許可する新しい規則を追加します。また、次のWindowsファイアウォール規則も無効にします。

- Citrix ICA (デフォルト: 1494)
- Citrix CGP (デフォルト: 2598)
- Citrix WebSocket (デフォルト: 8008)

その結果、ユーザーはTLSまたはDTLSを使用してのみ接続できます。TLSまたはDTLSなしでは、ICA/HDX、セッションの信頼性を備えたICA/HDX、またはWebSocket経由のHDXを使用できません。

> **注:**
>
> DTLSは、UDPリアルタイムトランスポート経由のICA/HDXオーディオ、またはICA/HDX Framehawkではサポートされていません。
>
> 「ネットワークポート」(/ja-jp/tech-zone/build/tech-papers/citrix-communication-ports.html#citrix-virtual-apps-and-desktops)を参照してください。

このスクリプトには、以下の構文の説明と追加の例が含まれています。この情報はNotepad++などのツールを使用して確認できます。

> **重要:**
>
> EnableまたはDisableパラメーター、およびCertificateThumbPrintパラメーターを指定します。その他のパラメーターはオプションです。

構文

```
Enable-VdaSSL {-Enable | -Disable} -CertificateThumbPrint "<thumbprint>" [-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"\<suite>"]
```

パラメーター	説明
有効化	VDAにTLSリスナーをインストールして有効にします。このパラメーターまたはDisableパラメーターのいずれかが必要です。
無効化	VDA上のTLSリスナーを無効にします。このパラメーターまたはEnableパラメーターのいずれかが必要です。このパラメーターを指定した場合、他のパラメーターは無効になります。
証明書サムプリント "<thumbprint>"	証明書ストア内のTLS証明書のサムプリントで、引用符で囲みます。スクリプトは、指定されたサムプリントを使用して、使用する証明書を選択します。このパラメーターを省略すると、誤った証明書が選択されます。
SSLポート <port>	TLSポート。デフォルト: 443
SSL最小バージョン "<version>"	引用符で囲まれた最小のTLSプロトコルバージョン。有効な値: `SSL_3.0`、`TLS_1.0` (デフォルト)、`TLS_1.1`、`TLS_1.2`、および `TLS_1.3`。`TLS_1.3` には、Windows 11またはWindows Server 2022以降が必要です。
SSL暗号スイート "<suite>"	引用符で囲まれたTLS暗号スイート。有効な値: 「GOV」、「COM」、および「ALL」（デフォルト）。

例

次のスクリプトは、TLSプロトコルバージョン値をインストールして有効にします。サムプリント (この例では「12345678987654321」と表記) は、使用する証明書を選択するために使用されます。

```
Enable-VdaSSL -Enable -CertificateThumbPrint "12345678987654321"
```

次のスクリプトは、TLSリスナーをインストールして有効にし、TLSポート400、GOV暗号スイート、および最小TLS 1.2プロトコル値を指定します。サムプリント (この例では「12345678987654321」と表記) は、使用する証明書を選択するために使用されます。

```
Enable-VdaSSL -Enable

-CertificateThumbPrint "12345678987654321"

-SSLPort 400 -SSLMinVersion "TLS_1.2"

-SSLCipherSuite "All"
```

次のスクリプトは、VDA上のTLSリスナーを無効にします。

```
Enable-VdaSSL -Disable
```

VDAでTLSを手動で構成する

VDAでTLSを手動で構成する場合、各VDA上の適切なサービスに対して、TLS証明書の秘密キーへの一般的な読み取りアクセスを許可します。WindowsシングルセッションOS用VDAの場合はNT SERVICE\PorticaService、またはWindowsマルチセッションOS用VDAの場合はNT SERVICE\TermServiceです。VDAがインストールされているマシンで:

ステップ 1。Microsoft管理コンソール（MMC）を起動します: > > 。

ステップ 2。MMCに証明書スナップインを追加します。

1. > を選択します。
2. を選択し、 をクリックします。
3. 「このスナップインは常に次の証明書を管理します:」というプロンプトが表示されたら、「コンピューターアカウント」を選択し、 をクリックします。
4. 「このスナップインで管理するコンピューターを選択してください」というプロンプトが表示されたら、「ローカルコンピューター」を選択し、 をクリックします。

手順 3. 証明書 (ローカル コンピューター) > 個人 > 証明書 の下で、証明書を右クリックし、 > を選択します。

手順 4. アクセス制御リストエディターに「(FriendlyName) の秘密キーのアクセス許可」が表示されます。(FriendlyName) は TLS 証明書の名前です。次のいずれかのサービスを追加し、読み取りアクセス権を付与します。

- Windows シングルセッションOS 用 VDA の場合、「PORTICASERVICE」
- Windows マルチセッションOS 用 VDA の場合、「TERMSERVICE」

手順 5. インストールされている TLS 証明書をダブルクリックします。証明書ダイアログで、 タブを選択し、一番下までスクロールします。 をクリックします。

手順 6. regedit を実行し、HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd に移動します。

1. SSL Thumbprint キーを編集し、TLS 証明書の拇印の値をこのバイナリ値にコピーします。 ダイアログボックスの不明な項目（「0000」や特殊文字など）は無視して問題ありません。
2. SSLEnabled キーを編集し、DWORD 値を 1 に変更します。（後で SSL を無効にするには、DWORD 値を 0 に変更します。）
3. デフォルト設定を変更する場合（オプション）は、同じレジストリパスで以下を使用します。

   SSLPort DWORD – SSL ポート番号。デフォルト: 443。

   SSLMinVersion DWORD – 1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.2, 5 = TLS 1.3。デフォルト: 2 (TLS 1.0)。

   SSLCipherSuite DWORD – 1 = GOV、2 = COM、3 = ALL。デフォルト: 3 (ALL)。

手順 7. TLS の TCP および UDP ポートがデフォルトの 443 ではない場合、Windows ファイアウォールで開いていることを確認します。（Windows ファイアウォールで受信規則を作成する際は、そのプロパティで「接続を許可する」と「有効」のエントリが選択されていることを確認してください。）

手順 8. 他のアプリケーションやサービス（IIS など）が TLS TCP ポートを使用していないことを確認します。

手順 9. マルチセッション VDA の場合、変更を有効にするためにマシンを再起動します。（シングルセッション VDA マシンを再起動する必要はありません。）

ステップ10. 接続の問題を回避するために、VDAでサポートされている暗号スイートが最高の優先順位を持つように、Windowsの暗号スイートの優先順位を変更します。

> **重要:**

> 以下に概説するグループポリシーの変更は、システムを再起動した後にのみ有効になります。

> MCSまたはPVSでプロビジョニングされた非永続的なセッションホストを使用している場合、これらの設定をマスターイメージに適用する必要があります。

オプション1:

グループポリシーエディターを使用して、コンピューターの構成 > ポリシー > 管理用テンプレート > ネットワーク > SSL構成設定 > SSL暗号スイートの順序に移動します。次の暗号スイートがリストの最上位にあることを確認してください。

```
TLS_AES_256_GCM_SHA384_P384

TLS_AES_256_GCM_SHA384_P256

TLS_AES_128_GCM_SHA256_P384

TLS_AES_128_GCM_SHA256_P256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

注:

TLS_AES_256_GCM_SHA384およびTLS_AES_128_GCM_SHA256は、Windows 11およびWindows Server 2022以降にのみ適用されます。古いオペレーティングシステムを使用している場合は、これらの暗号スイートをリストに含めないでください。

リストされている暗号スイートは、楕円曲線（P384またはP256）も指定しており、「curve25519」が選択されないようにしていることに注意してください。FIPSモードは「curve25519」の使用を妨げません。

リストから暗号スイートを削除する必要はありません。これらの設定はシステム全体に適用されるため、暗号スイートを削除する場合は、セッションホストで実行されているアプリケーションやサービスによってそれらが必要とされていないことを確認する必要があります。

オプション2:

グループポリシーエディターを使用して、コンピューターの構成 > ポリシー > 管理用テンプレート > ネットワーク > SSL構成設定 > SSL暗号スイートの順序に移動します。次の暗号スイートがリストの最上位にあることを確認してください。

```
TLS_AES_256_GCM_SHA384

TLS_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
```

注: TLS_AES_256_GCM_SHA384およびTLS_AES_128_GCM_SHA256は、Windows 11およびWindows Server 2022以降にのみ適用されます。古いオペレーティングシステムを使用している場合は、これらの暗号スイートをリストに含めないでください。

リストから暗号スイートを削除する必要はありません。これらの設定はシステム全体に適用されるため、暗号スイートを削除する場合は、セッションホストで実行されているアプリケーションやサービスによってそれらが必要とされていないことを確認する必要があります。

グループポリシーエディターを使用して、コンピューターの構成 > ポリシー > 管理用テンプレート > ネットワーク > SSL構成設定 > ECC曲線の順序に移動します。設定を有効にし、次の曲線をリストに含めます。

```
NistP384

NistP256
```

注:

これにより、「curve25519」が選択されないようにします。FIPSモードは「curve25519」の使用を妨げません。

VDAは、グループポリシーリストと、選択されたコンプライアンスモード（COM、GOV、またはALL）のリストの両方に表示される場合にのみ、暗号スイートを選択します。暗号スイートは、クライアント（Citrix Workspaceアプリ）から送信されたリストにも表示されている必要があります。

デリバリーグループでのTLSの構成

TLS接続用に構成したVDAを含む各デリバリーグループに対して、この手順を完了してください。

1. StudioからPowerShellコンソールを開きます。
2. **Get-BrokerAccessPolicyRule -DesktopGroupName '\<*delivery-group-name*>' \| Set-BrokerAccessPolicyRule -HdxSslEnabled $true** を実行します。
3. **Set-BrokerSite -DnsResolutionEnabled $true** を実行します。

自動登録を使用したプールされたVDAのSSL有効化

プールされたVDAを使用する場合、マスターイメージに証明書を追加すると、すべてのVDAが同じイメージを共有します。ワイルドカード証明書を使用できますが、欠点は、いずれかのVDAが侵害された場合、この強力な証明書により、すべてのVDAに属するHDX™接続が危険にさらされることです。

代わりに、より安全な代替策として、Microsoft Active Directory証明書サービスを活用して、グループポリシーを使用して証明書を自動的にプロビジョニングする方法があります。VDA上でスタートアップスクリプトを使用して、新しい証明書を動的にプロビジョニングし、VDAでSSLを有効にすることができます。

このアプローチは、シングルセッションのデスクトップVDAでのみ機能することに注意してください。マルチセッションVDAの場合、証明書が自動的にプロビジョニングされる前に、ブートプロセス中にICAリスナーが早すぎる段階で起動されます。

Active Directory証明書サービスは内部のエンタープライズ証明機関を使用するため、すべてのWindowsインストールによって自動的に信頼されるわけではありません。クライアントが企業によって管理され、ドメインフォレストの一部である場合、信頼されたCA証明書はグループポリシーを使用して自動的に配布できます。BYODやその他のドメインに参加していないデバイスの場合、信頼されたCA証明書を別のメカニズム（ダウンロードリンクの提供など）でユーザーに配布するか、NetScaler Gatewayを使用する必要があります。

証明書の自動登録を有効にする

まず、VDAドメインフォレスト内のサーバーにActive Directory証明書サービスロールがインストールされており、エンタープライズCAが提供されていることを確認してください。そうでない場合、自動登録はできません。

VDAsが起動ごとに証明書要求を送信するため、これはEnterprise CAに通常よりもかなり高い負荷をかける可能性があります。負荷に対処するために、CAサーバーに十分なCPUとメモリを割り当て、本番環境に移行する前に、常にラボ環境で展開のスケーラビリティをテストしてください。

グループポリシー管理エディターで、SSLが有効なプールされたVDAを含む組織単位に適用される新しいポリシーを次のように作成します。

1. コンピューターの構成 -> ポリシー -> Windowsの設定 -> セキュリティの設定 -> 公開キーのポリシー を展開します
2. 「証明書サービス クライアント – 自動登録ポリシー」オブジェクトのプロパティを編集します
3. 以下のスクリーンショットに示すように構成します。
4. 自動証明書要求コンテナを右クリックし、「新規 -> 自動証明書要求...」を選択します。
5. 自動証明書要求セットアップウィザードで、「次へ」をクリックします。
6. コンピューター証明書テンプレートが選択されていることを確認し、「次へ」をクリックします。
7. 「完了」をクリックします。

登録ポリシーのスクリーンショット (/en-us/citrix-virtual-apps-desktops/2411/media/ssltask-autoenrollment-policy.png)

Windowsマスターイメージの準備

Enable-VdaSsl.ps1スクリプトを、製品インストールメディアの `Support\Tools\SslSupport` フォルダーからVDAマスターイメージにコピーします。マスターイメージには、HDX SSL接続に使用する証明書を含めないでください。証明書は、MCSまたはPVSマシンカタログが作成される

ときにプロビジョニングされます。次に、次のように新しいスケジュールされたタスクを作成します（このスケジュールされたタスクは今すぐ実行しないでください）。

1. タスクスケジューラを開きます。
2. **操作**ペインで、**タスクの作成...**を押します。
3. 全般タブで:

   - 「**名前**」を`Enable VDA SSL`のように入力します。
   - 「**ユーザーまたはグループの変更...**」をクリックし、「ユーザーまたはグループの選択」ダイアログボックスに`SYSTEM`と入力して、「**OK**」をクリックします。

   タスクの作成「操作」タブのスクリーンショット (/en-us/citrix-virtual-apps-desktops/2411/media/ssltask-general.png)
4. 「トリガー」タブを選択します。
5. 「**新規...**」をクリックします。「**新しいトリガー**」ダイアログで:

   a. 「**タスクの開始**」を「**イベント時**」に設定します。

   b. 「**ログ**」を「**Microsoft-Windows-CertificateServicesClient-Lifecycle-System/Operational**」に設定します。

   c. 「**ソース**」を「**Microsoft-Windows-CertificateServicesClient-Lifecycle-System**」に設定します。

   d. 「**イベントID**」を`1006`に設定します。

   e. 「**OK**」をクリックしてトリガーを保存します。

   新しいトリガーウィンドウのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2411/media/ssltask-trigger.png)
6. 「**アクション**」タブを選択します。
7. 「**新規...**」をクリックします。
8. 「**新しいアクション**」ダイアログで:

   a. 「**アクション**」を「**プログラムの開始**」に設定します。

   b. 「プログラム/スクリプト」フィールドに、`powershell.exe`と入力します。

   c. 「引数の追加」フィールドに、PowerShellスクリプトへのパスを含めて`-ExecutionPolicy RemoteSigned Enable-VdaSsl.ps1 -Enable -Confirm:$False`を入力します。

   d. 「**OK**」を押してアクションを保存します。

新しいアクションウィンドウのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2411/media/ssltask-action.png)

9. 「**OK**」を押してタスクを保存します。

トラブルシューティング

接続エラーが発生した場合は、VDAのシステムイベントログを確認してください。

Windows向けCitrix Workspaceアプリを使用しているときに、TLSエラーを示す接続エラーが発生した場合は、Desktop Viewerを無効にしてから、もう一度接続を試してください。接続は引き続き失敗しますが、基になるTLSの問題の説明が提供される場合があります。（たとえば、証明機関に証明書を要求する際に誤ったテンプレートを指定した場合などです。）

HDX Adaptive Transport を使用するほとんどの構成は、Citrix Workspace app、Citrix Gateway、および VDA の最新バージョンを使用するものを含め、DTLS で正常に動作します。Citrix Workspace app と Citrix Gateway の間で DTLS を使用し、かつ Citrix Gateway と VDA の間で DTLS を使用する一部の構成では、追加のアクションが必要です。

次の場合、追加の操作が必要です。

- Citrix ReceiverのバージョンがHDX Adaptive TransportおよびDTLSをサポートしている場合：Receiver for Windows (4.7, 4.8, 4.9)、Receiver for Mac (12.5, 12.6, 12.7)、Receiver for iOS (7.2, 7.3.x) またはReceiver for Linux (13.7)

以下のいずれかに該当する場合も同様です。

- Citrix GatewayのバージョンはVDAへのDTLSをサポートしているが、VDAのバージョンはDTLSをサポートしていない（バージョン7.15以前）。
- VDAのバージョンはDTLSをサポートしている（バージョン7.16以降）が、Citrix GatewayのバージョンはVDAへのDTLSをサポートしていない。

Citrix Receiver™ からの接続が失敗するのを避けるには、次のいずれかを実行します。

- Citrix Receiverを、Receiver for Windowsバージョン4.10以降、Receiver for Mac 12.8以降、またはReceiver for iOSバージョン7.5以降に更新する。または、,
- Citrix Gatewayを、VDAへのDTLSをサポートするバージョンに更新する。または、,
- VDAをバージョン7.16以降に更新する。または、,
- VDAでDTLSを無効にする。または、,
- HDX Adaptive Transportを無効にする。

注:

Receiver for Linuxの適切なアップデートはまだ利用できません。Receiver for Android（バージョン3.12.3）は、Citrix Gateway経由のHDX Adaptive TransportおよびDTLSをサポートしていないため、影響を受けません。

VDAでDTLSを無効にするには、VDAファイアウォール構成を変更してUDPポート443を無効にします。(/ja-jp/tech-zone/build/tech-papers/citrix-communication-ports.html#citrix-virtual-apps-and-desktops)を参照してください。

TLSとHTML5ビデオリダイレクト、およびブラウザコンテンツリダイレクト

HTML5ビデオリダイレクトとブラウザコンテンツリダイレクトを使用して、HTTPS Webサイトをリダイレクトできます。これらのWebサイトに挿入されるJavaScriptは、VDAで実行されているCitrix HDX HTML5ビデオリダイレクトサービスへのTLS接続を確立する必要があります。これを実現するために、HTML5ビデオリダイレクトサービスは、VDA上の証明書ストアに2つのカスタム証明書を生成します。サービスを停止すると、証明書は削除されます。

HTML5ビデオリダイレクトポリシーは、デフォルトで無効になっています。

ブラウザコンテンツリダイレクトは、デフォルトで有効になっています。

HTML5ビデオリダイレクトの詳細については、(/ja-jp/citrix-virtual-apps-desktops/2411/policies/reference/ica-policy-settings/multimedia-policy-settings.html#html5-video-redirection)を参照してください。

Universal Print Server で TLS を有効にする

トランスポート層セキュリティ (TLS) プロトコルは、Virtual Delivery Agent (VDA) と Universal Print Server 間の TCP ベースの接続でサポートされています。

警告:

Windows レジストリでの作業を含むタスクの場合、レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になる深刻な問題が発生する可能性があります。Citrix® は、レジストリエディターの誤った使用によって生じる問題が解決されることを

> 保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

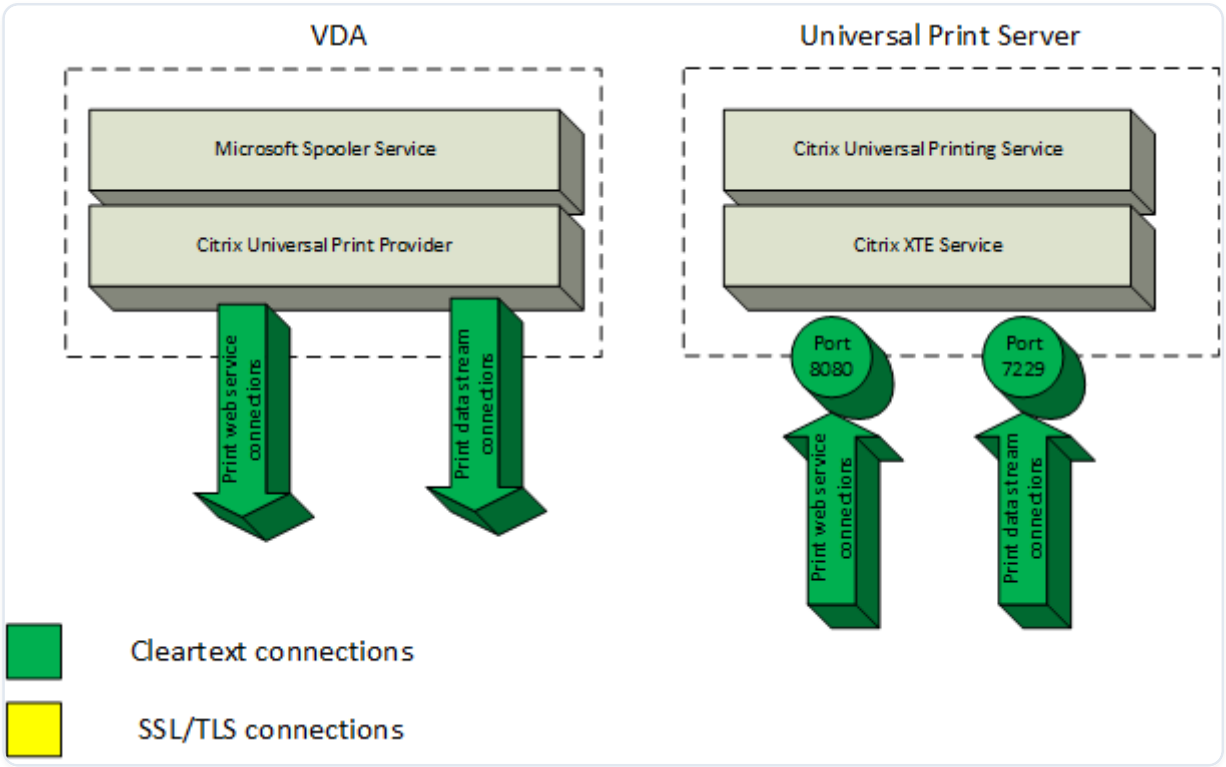
VDA と Universal Print Server 間の印刷接続の種類

クリアテキスト接続

以下の印刷関連の接続は VDA から発信され、Universal Print Server 上のポートに接続します。これらの接続は、**SSL enabled** ポリシー設定が **Disabled** (デフォルト) に設定されている場合にのみ行われます。

- クリアテキスト印刷 Web サービス接続 (TCP ポート 8080)
- クリアテキスト印刷データストリーム (CGP) 接続 (TCP ポート 7229)

Microsoft のサポート記事 Service overview and network port requirements for Windows には、Microsoft Windows Print Spooler サービスが使用するポートが記載されています。このドキュメントの SSL/TLS 設定は、Windows Print Spooler サービスによって行われる NetBIOS および RPC 接続には適用されません。**Universal Print Server enable** ポリシー設定が **Enabled with fallback to Windows' native remote printing** に設定されている場合、VDA は Windows Network Print Provider (win32spl.dll) をフォールバックとして使用します。



暗号化された接続

これらの印刷関連の SSL/TLS 接続は VDA から発信され、Universal Print Server 上のポートに接続します。これらの接続は、**SSL enabled** ポリシー設定が **Enabled** に設定されている場合にのみ行われます。

- 暗号化された印刷 Web サービス接続 (TCP ポート 8443)
- 暗号化された印刷データストリーム (CGP) 接続 (TCP ポート 443)

ユニバーサルプリントサーバーのセキュリティ 2(/en-us/citrix-virtual-apps-desktops/2411/media/universal-print-server-secure-2.png)

SSL/TLS クライアント構成

VDA は SSL/TLS クライアントとして機能します。

Microsoftグループポリシーとレジストリを使用して、暗号化された印刷Webサービス接続（TCPポート8443）のためにMicrosoft SCHANNEL SSPを構成します。Microsoftサポート記事TLSレジストリ設定には、Microsoft SCHANNEL SSPのレジストリ設定が記載されています。

VDA上でグループポリシーエディターを使用し、**コンピューターの構成 > 管理用テンプレート > ネットワーク > SSL構成設定 > SSL暗号スイートの順序**に移動します。TLS 1.3が設定されている場合は、次の順序を選択します。

TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256

TLS 1.2 が設定されている場合は、次の順序を選択します。

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

> **注:**
>
> このグループポリシー設定が構成されている場合、VDAは、暗号化された印刷Webサービス接続（デフォルトポート: 8443）に対して、接続が両方のSSL暗号スイートリストに表示されている場合にのみ、暗号スイートを選択します。

- グループポリシー SSL 暗号スイート順序リスト
- 選択した SSL 暗号スイートポリシー設定 (COM、GOV、または ALL) に対応するリスト

このグループポリシー構成は、VDA上の他のTLSアプリケーションおよびサービスにも影響します。アプリケーションが特定の暗号スイートを必要とする場合は、このグループポリシー暗号スイート順序リストに追加する必要があるかもしれません。

重要:

TLS構成のグループポリシーの変更は、オペレーティングシステムの再起動後にのみ有効になります。

Citrixポリシーを使用して、暗号化された印刷データストリーム (CGP) 接続 (TCPポート443) のSSL/TLS設定を構成します。

SSL/TLSサーバーの構成

Universal Print Server は SSL/TLS サーバーとして機能します。

SSL/TLS設定を構成するには、`Enable-UpsSsl.ps1` PowerShellスクリプトを使用します。

Universal Print ServerにTLS証明書をインストールする

HTTPSの場合、VDAによって信頼されているSSLサーバー証明書をUniversal Print Serverにインストールする必要があります。Microsoft Active Directory証明書サービスまたは別の認証機関を使用して、Universal Print Serverの証明書を要求します。

マイクロソフト Active Directory 証明書サービスを使用して証明書を登録/要求する際は、以下の考慮事項に留意してください。

1. 証明書をローカルコンピューターの**個人**証明書ストアに配置します。
2. 証明書のサブジェクト識別名 (Subject DN) の**共通名**属性を、Universal Print Serverの完全修飾ドメイン名 (FQDN) に設定します。これは証明書テンプレートで指定します。
3. 証明書要求と秘密キーの生成に使用される暗号化サービスプロバイダー (CSP) を**Microsoft Enhanced RSA and AES Cryptographic Provider (Encryption)**に設定します。これは証明書テンプレートで指定します。
4. キーサイズを2048ビット以上に設定します。これは証明書テンプレートで指定します。

証明書の作成とインストールについて詳しくは、「証明書の管理」を参照してください。

Universal Print ServerでのSSLの構成

Universal Print Server上のXTEサービスは、受信接続をリッスンします。SSLが有効な場合、SSLサーバーとして機能します。受信接続には、印刷コマンドを含む印刷Webサービス接続と、印刷ジョブを含む印刷データストリーム接続の2種類があります。これらの接続でSSLを有効にできます。SSLはこれらの接続の機密性と整合性を保護します。デフォルトでは、SSLは無効になっています。

SSLの構成に使用されるPowerShellスクリプトは、インストールメディアにあり、ファイル名は次のとおりです: `\Support\Tools\SslSupport\Enable-UpsSsl.ps1.`.

Universal Print Server でのリスニングポート番号の構成

これらは XTE Service のデフォルトポートです。

- クリアテキスト印刷 Web サービス (HTTP) TCP ポート: 8080
- クリアテキスト印刷データストリーム (CGP) TCP ポート: 7229
- 暗号化された印刷 Web サービス (HTTPS) TCP ポート: 8443
- 暗号化された印刷データストリーム (CGP) TCP ポート: 443

Universal Print Server で XTE Service が使用するポートを変更するには、管理者として PowerShell で次のコマンドを実行します (Enable-UpsSsl.ps1 PowerShell スクリプトの使用に関する注意点については、後のセクションを参照してください)。

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` または `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`
3. `Start-Service CitrixXTEServer`

ユニバーサル プリント サーバーの TLS 設定

負荷分散構成で複数の Universal Print Server を使用している場合は、すべての Universal Print Server で **TLS** 設定が一貫して構成されていることを確認してください。

Universal Print Server で TLS を構成すると、インストールされている TLS 証明書のアクセス許可が変更され、Universal Printing Service に証明書の秘密キーへの読み取りアクセス権が付与され、Universal Printing Service に次の情報が通知されます。

- TLS に使用する証明書ストア内の証明書。

- TLS 接続に使用する TCP ポート番号。

Windows ファイアウォールが有効な場合、これらの TCP ポートで受信接続を許可するように構成する必要があります。この構成は、Enable-UpsSsl.ps1 PowerShell スクリプトを使用すると自動的に行われます。

- 許可する TLS プロトコルのバージョン。

Universal Print Server は TLS プロトコルバージョン 1.3 および 1.2 をサポートしています。許可される最小バージョンを指定します。

デフォルトの TLS プロトコルバージョンは 1.2 です。

> **注：**
>
> Citrix Virtual Apps and Desktops バージョン 2311 以降、TLS 1.1 および 1.0 はサポートされなくなりました。

- 許可する TLS 暗号スイート。

暗号スイートは、接続に使用される暗号化アルゴリズムを選択します。VDA と Universal Print Server は、異なる暗号スイートのセットをサポートできます。VDA が接続してサポートされている TLS 暗号スイートのリストを送信すると、Universal Print Server はクライアントの暗号スイートの 1 つを、自身の構成済み暗号スイートのリストにある暗号スイートの 1 つと照合し、接続を受け入れます。一致する暗号スイートがない場合、Universal Print Server は接続を拒否します。

Universal Print Server は、OPEN、FIPS、および SP800-52 ネイティブ Crypto Kit モード用に、GOV(ernment)、COM(mercial)、および ALL という名前の以下の暗号スイートセットをサポートしています。許容される暗号スイートは、**SSL FIPS Mode** ポリシー設定と Windows FIPS モードにも依存します。Windows FIPS モードの詳細については、この Microsoft サポート記事 を参照してください。

暗号スイート（優先順位の降順）	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_AES256_GCM_SHA384	X		X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA384	X		X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA	X	X		X	X		X	X	

PowerShellスクリプトを使用してUniversal Print ServerでTLSを構成する

証明書ストアの**ローカルコンピューター > 個人 > 証明書**領域にTLS証明書をインストールします。その場所に複数の証明書がある場合は、証明書のサムプリントを`Enable-UpsSsl.ps1` PowerShellスクリプトに指定します。

> **注:**
>
> PowerShellスクリプトは、Universal Print ServerのFQDNに基づいて正しい証明書を見つけます。Universal Print ServerのFQDNに対して証明書が1つしかない場合は、証明書のサムプリントを指定する必要はありません。

> `Enable-UpsSsl.ps1`スクリプトは、VDAからUniversal Print ServerへのTLS接続を有効または無効にします。このスクリプトは、インストールメディアの**Support > Tools > SslSupport**フォルダーにあります。

TLSを有効にすると、スクリプトはUniversal Print ServerのTCPポートに対する既存のWindowsファイアウォール規則をすべて無効にします。その後、XTEサービスがTLS TCPおよびUDPポートでのみ受信接続を受け入れることを許可する新しい規則を追加します。また、以下のWindowsファイアウォール規則も無効にします。

- クリアテキスト印刷Webサービス接続（デフォルト：8080）
- クリアテキスト印刷データストリーム（CGP）接続（デフォルト：7229）

その結果、VDAはTLSを使用している場合にのみこれらの接続を行うことができます。

> **注:**
>
> TLSを有効にしても、VDAからUniversal Print ServerへのWindows Print Spooler RPC/SMB接続には影響しません。

> **重要:**
>
> 最初のパラメーターとして**Enable**または**Disable**のいずれかを指定します。ローカルコンピューターの個人証明書ストアにUniversal Print ServerのFQDNを持つ証明書が1つしかない場合、CertificateThumbprintパラメーターはオプションです。その他のパラメーターもオプションです。

構文

```
Enable-UpsSSL.ps1 -Enable [-HTTPPort &lt;port>] [-CGPPort &lt;port>] [-
HTTPSPort &lt;port>] [-CGPSSLPort &lt;port>] [-SSLMinVersion &lt;version>]
[-SSLCipherSuite &lt;name>] [-CertificateThumbprint &lt;thumbprint>] [-
FIPSMode &lt;Boolean>] [-ComplianceMode &lt;mode>]

Enable-UpsSSL.ps1 -Disable [-HTTPPort &lt;portnum>] [-CGPPort
&lt;portnum>]
```

パラメーター	説明
有効にする	XTEサーバーでSSL/TLSを有効にします。このパラメーターまたはDisableパラメーターのいずれかが必要です。
無効にする	XTEサーバーでSSL/TLSを無効にします。このパラメーターまたはEnableパラメーターのいずれかが必要です。
証明書サムプリント `"<thumbprint>"`	ローカルコンピューターの個人証明書ストアにあるTLS証明書のサムプリントを引用符で囲みます。スクリプトは指定されたサムプリントを使用して、使用する証明書を選択します。
HTTPポート `<port>`	クリアテキスト印刷Webサービス（HTTP/SOAP）ポート。デフォルト: 8080
CGPポート `<port>`	クリアテキスト印刷データストリーム（CGP）ポート。デフォルト: 7229
HTTPSポート `<port>`	暗号化された印刷Webサービス（HTTPS/SOAP）ポート。デフォルト: 8443
CGP SSLポート `<port>`	暗号化された印刷データストリーム（CGP）ポート。デフォルト: 443
SSL最小バージョン `"<version>"`	最小TLSプロトコルバージョンを引用符で囲みます。有効な値: 「TLS_1.2」および「TLS_1.3」。デフォルト: TLS_1.2。

パラメーター	説明
SSL暗号スイート `"<name>"`	TLS暗号スイートパッケージの名前を引用符で囲みます。有効な値: 「GOV」、「COM」、および「ALL」（デフォルト）。
FIPSモード `<Boolean>`	XTE ServerでFIPS 140モードを有効または無効にします。有効な値: FIPS 140モードを有効にする場合は$true、FIPS 140モードを無効にする場合は$false。

例

次のスクリプトはTLSを有効にします。サムプリント（この例では「12345678987654321」として表されています）は、使用する証明書を選択するために使用されます。

```
Enable-UpsSsl.ps1 –Enable -CertificateThumbprint "12345678987654321"
```

次のスクリプトはTLSを無効にします。

```
Enable-UpsSsl.ps1 –Disable
```

FIPSモードの構成

米国連邦情報処理標準（FIPS）モードを有効にすると、Universal Print Serverの暗号化された接続にはFIPS 140準拠の暗号化のみが使用されるようになります。

クライアントでFIPSモードを構成する前に、サーバーでFIPSモードを構成してください。

Windows FIPS モードの有効化/無効化については、Microsoft のドキュメントサイトを参照してください。

クライアントでのFIPSモードの有効化

Delivery Controller™でWeb Studioを実行し、**UPS FIPS Mode** Citrixポリシー設定を**Enabled**に設定します。Citrixポリシーを有効にします。

各VDAで以下を実行します。

1. Windows FIPSモードを有効にします。
2. VDAを再起動します。

サーバーでのFIPSモードの有効化

各Universal Print Serverでこれを実行します。

1. Windows FIPSモードを有効にします。
2. 管理者として次のPowerShellコマンドを実行します: `stop-service CitrixXTEServer, UpSvc`
3. `-Enable -FIPSMode $true` パラメーターを指定して `Enable-UpsSsl.ps1` スクリプトを実行します。
4. Universal Print Serverを再起動します。

クライアントでのFIPSモードの無効化

Web Studioで、Citrixポリシー設定の**UPS FIPS Mode**を**Disabled**に設定します。Citrixポリシーを有効にします。**UPS FIPS Mode** Citrixポリシー設定を削除することもできます。

各VDAでこれを実行します。

1. Windows FIPSモードを無効にします。
2. VDAを再起動します。

サーバーでのFIPSモードの無効化

各Universal Print Serverでこれを実行します。

1. Windows FIPSモードを無効にします。
2. 管理者として次のPowerShellコマンドを実行します: `stop-service CitrixXTEServer, UpSvc`
3. `Enable-UpsSsl.ps1` スクリプトを `-Enable -FIPSMode $false` パラメーターで実行します。
4. Universal Print Serverを再起動します。

> **注:**
>
> SSLプロトコルバージョンがTLS 1.3に設定されている場合、FIPSモードはサポートされません。

SSL/TLSプロトコルバージョンの構成

デフォルトのSSL/TLSプロトコルバージョンはTLS 1.2です。TLS 1.2とTLS 1.3は、本番環境での使用が推奨されるSSL/TLSプロトコルバージョンです。トラブルシューティングのために、非本番環境でSSL/TLSプロトコルバージョンを一時的に変更する必要がある場合があります。

Universal Print Serverでは、SSL 2.0およびSSL 3.0はサポートされていません。

サーバーでのSSL/TLSプロトコルバージョンの設定

各Universal Print Serverで以下を実行します。

1. 管理者としてこのPowerShellコマンドを実行します: `stop-service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1`スクリプトを`-Enable -SSLMinVersion`バージョンパラメーターで実行します。テストが完了したら、これをTLS 1.2またはTLS 1.3に戻すことを忘れないでください。
3. Universal Print Serverを再起動します。

クライアントでのSSL/TLSプロトコルバージョンの設定

Studioで、**SSL Protocol Version**ポリシー設定を目的のプロトコルバージョンに設定し、ポリシーを有効にします。

VDAのオペレーティングシステムが選択したTLSバージョンをサポートしていることを確認してください。Windowsでサポートされ ているTLSバージョンについては、[Microsoft Learn - TLS protocol version support}(https://learn.microsoft.com/ja-jp/windows-server/security/tls/tls-registry-settings?tabs=diffie-hellman#tls-dtls-and-ssl-protocol-version-settings)を参照してください。デフォルトを上書きするようにレジストリを構成するには、Microsoft Learn - TLS, DTLS, and SSL protocol version settingsを参照してください。

トラブルシューティング

接続エラーが発生した場合は、Universal Print Server の C:\Program Files (x86)\Citrix\XTE\logs\error.log ファイルを確認してください。

SSL/TLSハンドシェイクが失敗した場合、このログファイルにエラーメッセージ **SSL handshake from client failed** が表示されます。このような失敗は、VDAとUniversal Print ServerのSSL/TLSプロトコルバージョンが一致しない場合に発生する可能性があります。

Universal Print Serverのホスト名を含む以下のポリシー設定で、Universal Print ServerのFQDNを使用してください。

- セッションプリンター
- プリンターの割り当て
- 負荷分散のためのUniversal Print Server

Universal Print ServerとVDAのシステムクロック（日付、時刻、タイムゾーン）が正しいことを確認してください。

仮想チャネル許可リスト

仮想チャネル許可リストは、Citrix以外の仮想チャネルのうち、どのチャネルを環境で許可するかを制御できる機能です。デフォルトでは、仮想チャネル許可リスト機能は有効になっています。その結果、Citrix Virtual Apps and Desktops™セッションでは、Citrix仮想チャネルのみが開くことが許可されます。自社製またはサードパーティ製のカスタム仮想チャネルを使用する必要がある場合は、それらを明示的に許可リストに追加する必要があります。

構成

仮想チャネル許可リストはデフォルトで有効になっています。この機能は、Citrixポリシーの以下の設定を使用して構成できます。

- **仮想チャネル許可リスト**: この機能を有効または無効にし、仮想チャネルをリストに追加します。
- **仮想チャネル許可リストログのスロットリング**: 仮想チャネル許可リストのイベントログのスロットリング期間を設定します。
- **仮想チャネル許可リストのログ記録**: 仮想チャネル許可リストのログレベルを設定します。

許可リストへの仮想チャネルの追加

仮想チャネルを許可リストに追加するには、以下の情報が必要です。

1. コードで定義されている仮想チャネル名。最大7文字です。例: `CTXCVC1`。
2. VDAマシン上で仮想チャネルを開くプロセスのパス。例: `C:\Program Files\Application\run.exe`。

必要な情報が揃ったら、仮想チャネル許可リストポリシー設定を使用して、仮想チャネルを許可リストに追加する必要があります。リストに仮想チャネルを追加するには、仮想チャネル名の後にコンマを入力し、次に仮想チャネルにアクセスするプロセスのパスを入力します。複数のプロセスがある場合は、各プロセスをコンマで区切って追加できます。

単一プロセスの場合

前の例を使用して、以下のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe
```

複数のプロセスの場合

複数のプロセスがある場合は、次のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

ワイルドカードの使用

ワイルドカード (*) の使用がサポートされています。アプリケーションのバージョンに基づいてディレクトリ名または実行可能ファイル名が変更される場合、またはサードパーティコンポーネントがユーザープロファイルにインストールされている場合に、ワイルドカードを使用できます。

次のシナリオでワイルドカードを使用できます。

- 完全なディレクトリ名を置き換える場合。 例: `C:\Program Files\Application*\run1.exe`
- ディレクトリ名の一部を置き換える場合。 例: `C:\Program Files\Application\v*\run1.exe`
- 実行可能ファイル名を置き換える場合。 例: `C:\Program Files\Application\v1.2*.exe`
- 実行可能ファイル名の一部を置き換える場合。 例: `C:\Program Files\Application\v1.2\run*.exe`

次の制限が適用されます。

- ワイルドカードは、単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルが `C:\Program Files\Application\v1.2\run1.exe` にある場合
  - 許可: `C:\Program Files\Application*\run1.exe`
  - 不許可: `C:\Program Files*\run1.exe`
- エントリにはファイル名拡張子を含める必要があります。
  - 許可: `C:\Program Files\Application\v1.2*.exe`
  - 許可されていません: `C:\Program Files\Application\v1.2*`

- すべてのパスはローカルである必要があります。

> **注:**
>
> - ネットワークパスは許可されていません。
> - ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2206から利用可能です。
> - ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2203 LTSRのCU2以降で利用可能です。

システム環境変数の使用

許可リスト内の信頼されたプロセスの定義を簡素化するために、システム環境変数を使用できます。`%programfiles%`、`%programfiles(x86)%`、`%systemdrive%`、`%systemroot%`などの、標準で用意されている変数を使用できます。

カスタム環境変数も使用できます。ただし、システムレベルで定義されている必要があります。

以下の例は、標準で用意されている環境変数を示しています:

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

以下の例は、カスタムシステム環境変数を示しています。

- カスタム変数名: `app`
- カスタム変数値: `%programfiles%\Application\`
- 許可リストエントリ: `CTXCVC1,%app%\run.exe`

> **注:**
>
> ユーザー環境変数はサポートされていません。

> 環境変数のサポートは、Citrix Virtual Apps and Desktopsバージョン2209以降で利用可能です。

仮想チャネル名とプロセスを取得する

VDAマシン上で仮想チャネルを開くプロセスと仮想チャネルの名前を取得する最も簡単な方法は、仮想チャネルを提供した開発者またはサードパーティベンダーから情報を入手することです。

または、機能のログを適用し、以下の手順に従って情報を取得することもできます。

1. カスタム仮想チャネルのクライアントコンポーネントとサーバーコンポーネントが配置されたら、仮想アプリケーションまたは仮想デスクトップを起動します。
2. VDAマシンのシステムイベントログで、カスタム仮想チャネルの名前と、それを開こうとしたプロセスを探します。利用可能なイベントの詳細については、「イベントログ」を参照してください。
3. セッションからログアウトします。
4. 特定された仮想チャネルとプロセスについて、仮想チャネル許可リストポリシー設定にエントリを追加します。
5. マシンを再起動します。
6. VDAが登録されたら、仮想アプリケーションまたは仮想デスクトップを実行して、カスタム仮想チャネルが正常に開くことを検証します。

Citrix仮想チャネルに関する考慮事項

すべての組み込みCitrix仮想チャネルは信頼されており、追加設定なしで開くことができます。ただし、以下の2つの機能は、外部依存関係のため、許可リストに明示的なエントリが必要です。

- マルチメディアリダイレクト
- スカイプ フォー ビジネス向けHDX リアルタイム最適化パック

マルチメディアリダイレクト

システムのメディアプレーヤーとしてWindows Media Player以外のメディアプレーヤーを使用する場合、それを信頼されたプロセスとして許可リストに追加する必要があります。許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXMM`
- プロセス: VDAマシンで使用されるメディアプレーヤーへのパス。例: `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`。
- 許可リストエントリ: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

スカイプ フォー ビジネス向けHDX リアルタイム最適化パック

許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXRMEP`
- プロセス: VDAマシン内のSkype for Business実行可能ファイルへのパス。これはSkype for Businessのバージョンや、カスタムインストールパスを使用したかどうかによって異なる場合があります。例: `C:\Program Files\Microsoft Office\root\Office16\lync.exe.`.
- 許可リストエントリ: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

VDA と Delivery Controller™ 間の WebSocket 通信

この記事では、WCF 通信の代替として、VDA と Delivery Controller 間の通信に WebSocket 接続をセットアップする方法について説明します。これにより、VDA から Delivery Controller への通信に TLS ポート 443 のみが使用されるという利点があります。

現在、これは MCS でプロビジョニングされたマシンでのみ利用可能です。手動でプロビジョニングされたマシンはテクニカルプレビュー段階です。詳細については、「トークンを使用して非 MCS プロビジョニング VDA を登録する (プレビュー)」を参照してください。

動作の仕組み

次のセクションでは、Delivery Controller と VDA 間の WebSocket 接続のワークフローについて説明します。

1. Citrix Virtual Apps and Desktops™ 管理者は、Machine Creation Service (MCS) を使用して VDA をプロビジョニングすることでプロセスを開始します。
2. MCS プロビジョニングプロセス中に、MCS は各 VDA の公開鍵と秘密鍵のペアを生成し、公開鍵を Delivery Controller 上の FMA 信頼サービスに登録します。MCS は、公開鍵と秘密鍵のペアを VDA の ID ディスクの下にファイルとして保存します。
3. VDA マシンが起動すると、VDA マシンにインストールされている MCS エージェントは ID ディスクからキーペアを読み取り、この情報を VDA レジストリの場所に書き込みます。
4. VDA にインストールされているブローカーエージェントは、レジストリからキーペアを読み取り、秘密鍵で署名されたサービスキーを含む SSL 対応の WebSocket リクエストを Delivery Controller に生成します。
5. Delivery Controller は、FMA 信頼サービスからの公開鍵を使用して、署名されたサービスキー認証ヘッダーを検証します。

6. 検証が完了すると、システムは VDA と Delivery Controller 間の WebSocket 接続を確立します。

WebSocket のサポート

開始する前に

1. サイトを構成します。詳細については、「サイトの作成」を参照してください。
2. Delivery Controller に TLS 証明書をインストールします。詳細については、「Controller に TLS サーバー証明書をインストールする」を参照してください。
3. Delivery Controller を信頼するために、VDA にルート CA と中間 CA をインストールします。

手順

WebSocket 接続を設定するには、次の手順に従います。

1. Delivery Controller で WebSocket 接続を有効にします。サイトにある各 Delivery Controller で次のコマンドを実行します。

   `New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy" -Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -Force`

   > **注：**
   >
   > WebSocket を有効にした後、Delivery Controller を再起動してください。

2. MCS プロビジョニングを使用して、AD 参加済み VDA 用のマシンカタログを作成します。詳しくは、「マシンカタログの作成」を参照してください。
3. デリバリーグループを作成し、VDA を追加します。詳しくは、「デリバリーグループの作成」を参照してください。
4. VDA で WebSocket 接続を有効にします。VDA で次の PowerShell コマンドを実行します。

   ```
   New-ItemProperty
   "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAgent
   \WebSocket" -Name "Enabled" -PropertyType "DWord" -Value 1 -Force
   ```

   - WebSocket が有効になっているか確認するには、次のレジストリキーの値をチェックします。`Enabled` の値は 1 である必要があります。

キー：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAgent\WebSocket
```

名前：Enabled

種類：REG_DWORD

値：1

HDX™ 接続性

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

HDXは、次の3つの技術原則に基づいて設計されています。

- インテリジェントなリダイレクト
- 適応型圧縮
- データ重複排除

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

HDX の提供機能では、独自のプロプライエタリなトランスポートプロトコルを介して接続し、セッション確立時に最大伝送ユニットを利用し、Citrix SD-WAN を使用して接続を最適化できます。

アダプティブトランスポート

アダプティブトランスポートは、Citrix Virtual Apps and Desktops™のメカニズムであり、優先トランスポートプロトコルを使用してHDXセッションの接続を確立し、優先プロトコルでの接続が利用できない場合はTCPにフォールバックできるようにします。

以下のトランスポートプロトコルがサポートされています。

- 高度なデータ転送 (EDT)
- 伝送制御プロトコル (TCP)

構成

アダプティブトランスポートはデフォルトで有効になっています。アダプティブトランスポートは、以下のモードで動作するように構成できます。

- **優先**：（デフォルト）クライアントは優先プロトコルで接続を試行し、優先プロトコルでの接続が利用できない場合はTCPにフォールバックします。

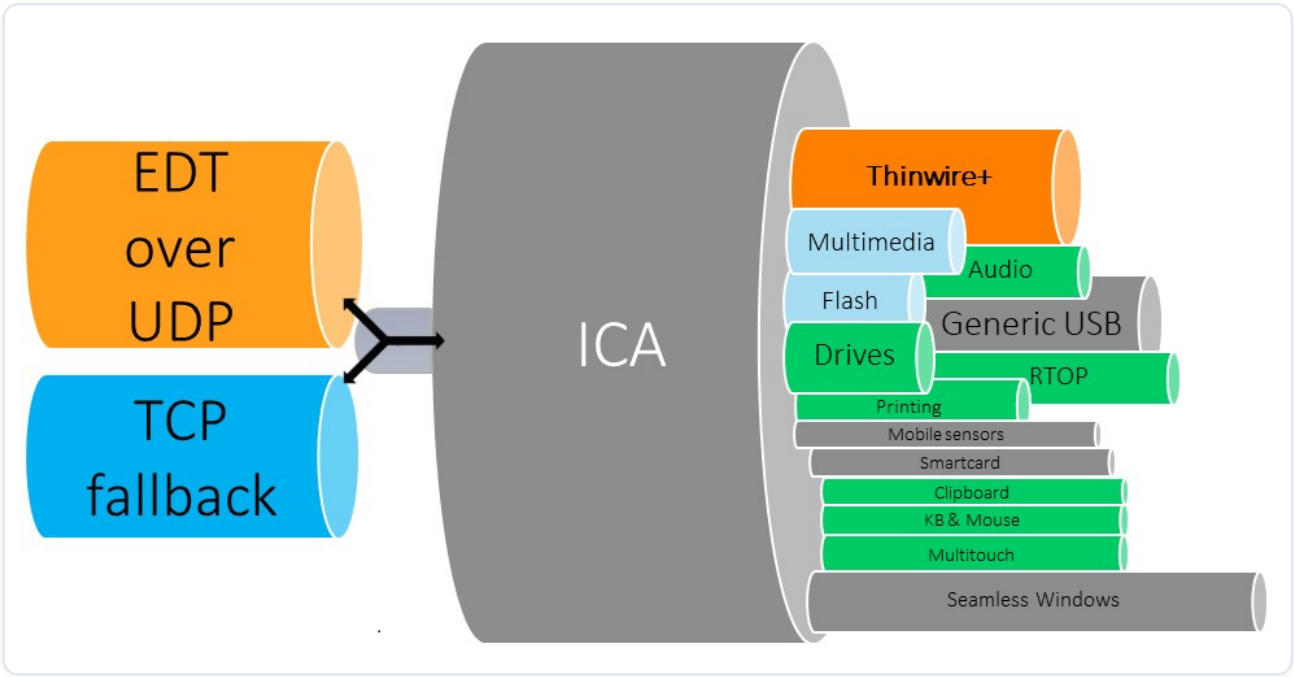
- **診断モード**：クライアントは優先プロトコルのみを使用して接続を試行します。TCPへのフォールバックは無効になります。
- **オフ**：クライアントはTCPのみを使用して接続を試行します。

仕組み

アダプティブトランスポートが`Preferred`に設定されている場合、クライアントは優先プロトコルとTCPの両方でセッションへの接続を並行して試行します。これにより、優先プロトコルで接続できない場合にクライアントがTCPを使用するようにフォールバックする必要がある場合でも、接続時間を最適化できます。TCPを使用して接続が確立された場合、クライアントは5分ごとにバックグラウンドで優先プロトコルでの接続を試行します。

アダプティブトランスポートが`Diagnostic mode`に設定されている場合、クライアントは優先プロトコルのみを使用してセッションに接続します。クライアントが優先プロトコルを使用して接続を確立できない場合、TCPへのフォールバックは行われず、接続は失敗します。

アダプティブトランスポートが`Off`に設定されている場合、**アダプティブトランスポート**は無効になり、クライアントはTCPのみを使用してセッションに接続します。



アダプティブトランスポート(/en-us/citrix-virtual-apps-desktops/2411/media/adaptive-transport.png)

システム要件

アダプティブトランスポートとEDTを使用するための要件は次のとおりです。

- コントロールプレーン

  - シトリックス DaaS（旧シトリックス バーチャル アプリケーションズ アンド デスクトップ サービス）
  - Citrix Virtual Apps and Desktops: 現在サポートされているバージョン
- バーチャル デリバリー エージェント
  - Windows: 現在サポートされているバージョン（2402以降を推奨）
  - Linux: 現在サポートされているバージョン（2402以降を推奨）
- Citrix Workspace™アプリ
  - Windows: 現在サポートされているバージョン（2402以降を推奨）
  - Linux: 現在サポートされているバージョン（2402以降を推奨）
  - Mac: 現在サポートされているバージョン（2402以降を推奨）
  - iOS: Apple App Storeで入手可能な最新バージョン
  - Android: Google Playで入手可能な最新バージョン
- Citrix NetScaler® ゲートウェイ
  - 14.1.12.30以降 (推奨)
  - 13.1.17.42以降 (13.1-52.19以降を推奨)

> **注記:**
>
> Linux VDAの詳細については、Linux Virtual Delivery Agentのドキュメントを参照してください。

ネットワーク要件

以下は、アダプティブトランスポートでEDTを使用するためのネットワーク要件です。

セッションホスト

セッションホストにWindows Defender ファイアウォールなどのファイアウォールがある場合は、内部接続に対して以下の受信トラフィックを許可する必要があります。

説明	送信元	プロトコル	ポート
内部接続 - セッションの信頼性が有効	クライアント	UDP	2598
内部接続 - セッションの信頼性が無効			1494
内部接続 - HDX™ DirectまたはVDA SSL			443

注：

VDAインストーラーは、Windows Defender ファイアウォールに適切な受信規則を追加します。別のファイアウォールを使用している場合は、上記の規則を追加する必要があります。

内部ネットワーク

以下の表は、ネットワークでEDTを使用するために必要なファイアウォール規則を示しています。

説明	プロトコル	送信元	宛先	宛先ポート
直接内部接続 - セッションの信頼性が有効	UDP	クライアントネットワーク	VDAネットワーク	2598
直接内部接続 - セッションの信頼性が無効				1494
直接内部接続 - HDX DirectまたはVDA SSL				443
ネットスケーラー ゲートウェイ		NetScaler SNIP		2598

説明	プロトコル	送信元	宛先	宛先ポート
ネットスケーラー ゲートウェイ - VDA SSL				443

注:

Citrix Gateway Serviceを使用している場合、EDTをトランスポートプロトコルとして使用するには、**Rendezvous**を有効にする必要があります。システムおよびネットワーク要件については、Rendezvousのドキュメントを参照してください。

クライアントネットワーク

以下の表は、クライアントデバイスの接続要件を示しています。

説明	プロトコル	送信元	宛先	宛先ポート
内部接続 - セッションの信頼性が有効	UDP	クライアントIP	VDAネットワーク	2598
内部接続 - セッションの信頼性が無効				1494
内部接続 - HDX Direct または SSL VDA				443
外部接続 - NetScaler Gateway			NetScaler Gateway パブリックIPアドレス	443
外部接続 - Citrix Gateway Service			シトリックス ゲートウェイ サービス	443

注記:

Citrix Gateway Serviceを使用している場合、クライアントは`<https://*.*.nssvc.net>`に到達できる必要があります。`<https://*.*.nssvc.net>`を使用してすべてのサブドメインを許可できない場合は、代わりに`<https://*.c.nssvc.net>`と`<https://*.g.nssvc.net>`を使用できます。詳細については、Knowledge Centerの記事CTX270584を参照してください。

HDX™ ダイレクト

Citrix提供のリソースにアクセスする際、HDX Directは、直接通信が可能な場合、内部および外部のクライアントデバイスがセッションホストと安全な直接接続を確立できるようにします。

重要:

外部ユーザー向けのHDX Directは現在プレビュー中です。この機能はサポートなしで提供されており、本番環境での使用はまだ推奨されていません。フィードバックを送信したり、問題を報告したりするには、こちらのフォームを使用してください。

システム要件

HDX Directを使用するためのシステム要件は以下のとおりです。

- コントロールプレーン
  - シトリックス DaaS™
  - シトリックス バーチャルアプリおよびデスクトップ™ 2411 以降
- 仮想配信エージェント (VDA)
  - Windows: バージョン 2411以降
- Workspaceアプリ
  - Windows: バージョン 2409以降
  - Linux: バージョン 2411以降
  - Mac: バージョン 2411以降

- アクセス層
  - Citrix Gateway Service と共に使用する Citrix Workspace™
  - NetScaler® Gateway を使用する Citrix Workspace
- その他
  - 外部からの直接接続には、アダプティブトランスポートを有効にする必要があります。

ネットワーク要件

HDX Direct を使用するためのネットワーク要件は次のとおりです。

セッションホスト

セッションホストに Windows Defender ファイアウォールなどのファイアウォールがある場合は、内部接続に対して次の受信トラフィックを許可する必要があります。

説明	送信元	プロトコル	ポート
直接内部接続	クライアント	TCP	443
直接内部接続	クライアント	UDP	443

> 注:
>
> VDAインストーラーは、Windows Defender ファイアウォールに適切な受信規則を追加します。別のファイアウォールを使用している場合は、上記の規則を追加する必要があります。

クライアントネットワーク

以下の表は、内部および外部ユーザー向けのクライアントネットワークについて説明しています。

内部ユーザー

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
直接内部接続	TCP	クライアントネットワーク	1024–65535	VDAネットワーク	443

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
直接内部接続	UDP	クライアントネットワーク	1024–65535	VDAネットワーク	443

外部ユーザー

説明	プロトコル	送信元	送信元ポート	宛先	宛先ポート
STUN (外部ユーザーのみ)	UDP	クライアントネットワーク	1024–65535	インターネット (下記の注記を参照)	3478, 19302
外部ユーザー接続	UDP	クライアントネットワーク	1024–65535	データセンターのパブリックIPアドレス	1024–65535

データセンターネットワーク

次の表は、内部ユーザーと外部ユーザー向けのデータセンターネットワークについて説明しています。

内部ユーザー

説明	プロトコル	ソース	送信元ポート	宛先	宛先ポート
直接内部接続	TCP	クライアントネットワーク	1024–65535	VDAネットワーク	443
直接内部接続	UDP	クライアントネットワーク	1024–65535	VDAネットワーク	443

外部ユーザー

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
STUN (外部ユーザーのみ)	UDP	VDAネットワーク	1024–65535	インターネット (下記の注記を参照)	3478, 19302
外部ユーザー接続	UDP	DMZ / 内部ネットワーク	1024–65535	VDAネットワーク	55000–55250
外部ユーザー接続	UDP	VDAネットワーク	55000–55250	クライアントのパブリックIP	1024–65535

注:

VDAとWorkspaceアプリの両方が、次のサーバーに同じ順序でSTUNリクエストを送信しようとします。

- stun.cloud.com:3478
- stun.cloudflare.com:3478
- stun.l.google.com:19302

HDX Directポート範囲ポリシー設定を使用して外部ユーザー接続のデフォルトポート範囲を変更した場合、対応するファイアウォールルールはカスタムポート範囲と一致する必要があります。

構成

HDX Directはデフォルトで無効になっています。この機能は、Citrixポリシーの**HDX Direct**設定を使用して構成できます。

- **HDX Direct**: 機能を有効または無効にするため。

- **HDX Directモード**: **HDX Direct**が内部クライアントのみに利用可能か、内部クライアントと外部クライアントの両方に利用可能かを決定します。
- **HDX Directポート範囲**: VDAが外部クライアントからの接続に使用するポート範囲を定義します。

考慮事項

HDX Directを使用する際の考慮事項は次のとおりです。

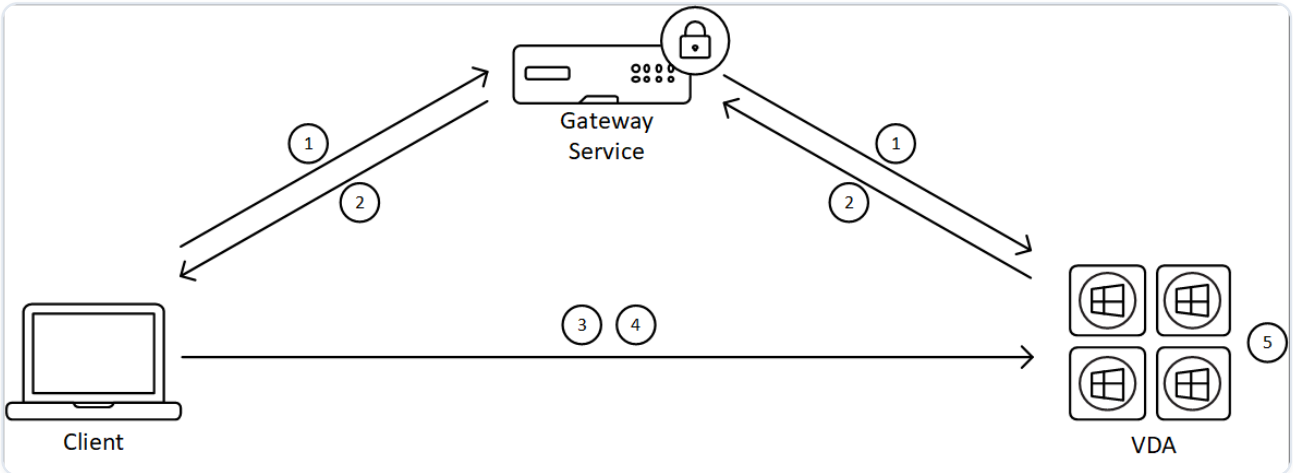
- 外部ユーザー向けのHDX Directは、トランスポートプロトコルとしてEDT (UDP) を使用する場合にのみ利用可能です。そのため、**アダプティブトランスポート**を有効にする必要があります。
- **HDX Insight**を使用している場合、**HDX Direct**を使用すると、セッションがNetScaler Gatewayを介してプロキシされなくなるため、HDX Insightのデータ収集が妨げられることに注意してください。
- 仮想アプリおよびデスクトップに非永続マシンを使用する場合、Citrixは、各マシンが独自の証明書を生成するように、マスター/テンプレートイメージではなくセッションホストで**HDX Direct**を有効にすることを推奨します。
- HDX Directで独自の証明書を使用することは現在サポートされていません。

動作の仕組み

HDX Directを使用すると、直接通信が可能な場合にクライアントがセッションホストへの直接接続を確立できます。HDX Directを使用して直接接続が行われる場合、ネットワークレベルの暗号化 (TLS/DTLS) を使用して直接接続を保護するために、自己署名証明書が使用されます。

内部ユーザー

次の図は、内部ユーザーのHDX Direct接続プロセスの概要を示しています。

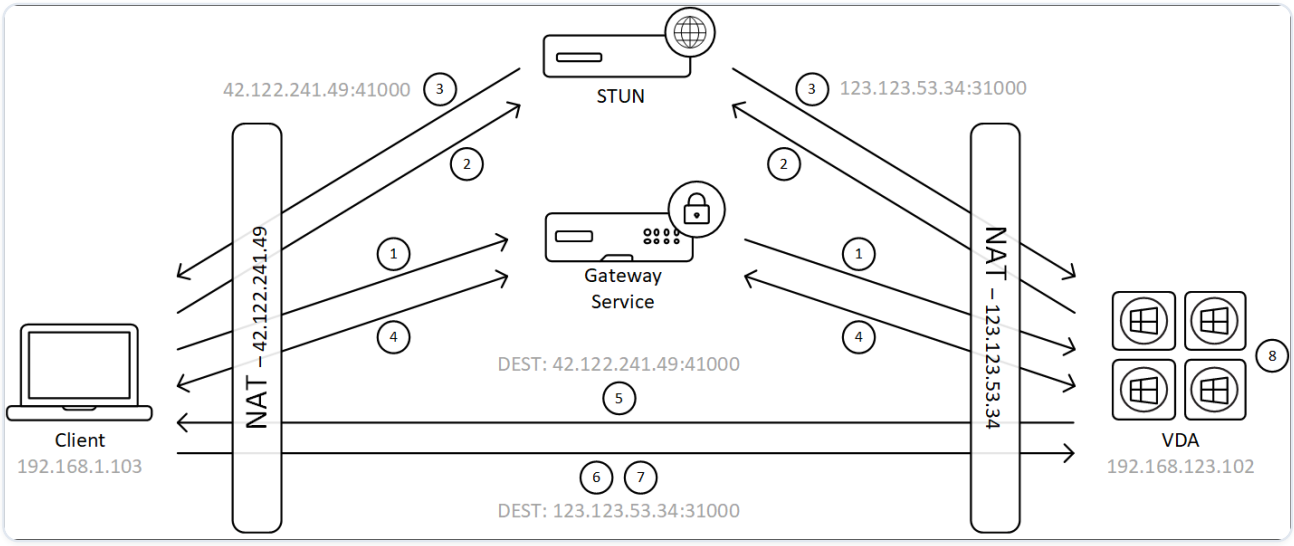


1. クライアントはGateway Serviceを介してHDXセッションを確立します。
2. 接続が成功すると、VDAはHDX接続を介して、VDAマシンのFQDN、そのIPアドレスのリスト、およびVDAマシンの証明書をクライアントに送信します。
3. クライアントはIPアドレスをプローブして、VDAに直接到達できるかどうかを確認します。
4. クライアントが共有されたいずれかのIPアドレスでVDAに直接到達できる場合、クライアントはVDAとの直接接続を確立し、ステップ (2) で交換された証明書と一致する証明書を使用して(D)TLSで保護します。
5. 直接接続が正常に確立されると、セッションは新しい接続に転送され、Gateway Serviceへの接続は終了します。

> **注:**
>
> 上記のステップ2で接続が確立された後、セッションはアクティブになります。その後の手順は、ユーザーが仮想アプリケーションまたはデスクトップを使用する能力を遅らせたり、妨げたりすることはありません。その後の手順のいずれかが失敗した場合でも、ユーザーのセッションを中断することなく、Gateway経由の接続は維持されます。

外部ユーザー

次の図は、外部ユーザー向けのHDX Direct接続プロセスの概要を示しています。



1. クライアントはGateway Serviceを介してHDXセッションを確立します。
2. 接続が成功すると、クライアントとVDAの両方がSTUNリクエストを送信して、それぞれのパブリックIPアドレスとポートを検出します。

3. STUNサーバーは、クライアントとVDAにそれぞれのパブリックIPアドレスとポートで応答します。
4. HDX接続を介して、クライアントとVDAはそれぞれのパブリックIPアドレスとUDPポートを交換し、VDAはクライアントに証明書を送信します。
5. VDAはクライアントのパブリックIPアドレスとUDPポートにUDPパケットを送信します。クライアントはVDAのパブリックIPアドレスとUDPポートにUDPパケットを送信します。
6. VDAからのメッセージを受信すると、クライアントはセキュアな接続要求で応答します。
7. DTLSハンドシェイク中に、クライアントは証明書がステップ(4)で交換された証明書と一致することを確認します。検証後、クライアントは認証トークンを送信します。これでセキュアな直接接続が確立されます。
8. 直接接続が正常に確立されると、セッションは新しい接続に転送され、Gateway Serviceへの接続は終了します。

> **注:**
>
> 上記のステップ2で接続が確立された後、セッションはアクティブになります。その後のステップは、ユーザーが仮想アプリケーションまたはデスクトップを使用する能力を遅らせたり、妨げたりすることはありません。その後のステップのいずれかが失敗した場合でも、ユーザーのセッションを中断することなく、Gatewayを介した接続は維持されます。

証明書管理

セッションホスト

VDAマシン上の以下の2つのサービスは、証明書の作成と管理を処理します。どちらもマシンの起動時に自動的に実行されるように設定されています。

- Citrix ClxMtp Service：CA証明書キーの生成とローテーションを担当します。
- Citrix Certificate Manager Service：自己署名ルートCA証明書とマシン証明書の生成および管理を担当します。

以下の手順は、証明書管理プロセスを示しています。

1. サービスはマシンの起動時に開始されます。
2. `Citrix ClxMtp Service`は、まだキーが作成されていない場合にキーを作成します。

3. Citrix Certificate Manager Serviceは、**HDX Direct**が有効になっているかを確認します。有効でない場合、サービスは停止します。
4. **HDX Direct**が有効になっている場合、Citrix Certificate Manager Serviceは自己署名ルートCA証明書が存在するかを確認します。存在しない場合、自己署名ルート証明書が作成されます。
5. ルートCA証明書が利用可能になると、Citrix Certificate Manager Serviceは自己署名マシン証明書が存在するかを確認します。存在しない場合、サービスはキーを生成し、マシンのFQDNを使用して新しい証明書を作成します。
6. Citrix Certificate Manager Serviceによって作成された既存のマシン証明書があり、そのサブジェクト名がマシンのFQDNと一致しない場合、新しい証明書が生成されます。

> **注：**
>
> Citrix Certificate Manager Serviceは、2048ビットキーを活用するRSA証明書を生成します。

クライアントデバイス

安全な**HDX Direct**接続を正常に確立するには、クライアントはセッションの保護に使用される証明書を信頼する必要があります。これを容易にするため、クライアントはICA®ファイル（Workspaceによって提供される）を介してセッションのCA証明書を受け取るため、CA証明書をクライアントデバイスの証明書ストアに配布する必要はありません。

NAT互換性

外部ユーザーデバイスとセッションホスト間の直接接続を確立するために、HDX™ DirectはNATトラバーサルのためにホールパンチングを利用し、クライアントデバイスとセッションホストのパブリックIPアドレスおよびポートマッピングの交換を容易にするためにSTUNを利用します。これは、VoIP、ユニファイドコミュニケーション、P2Pソリューションの仕組みに似ています。

ファイアウォールやその他のネットワークコンポーネントが、STUNリクエストおよびHDXセッションのUDPトラフィックを許可するように構成されている限り、外部ユーザー向けのHDX Directは機能すると予想されます。ただし、ユーザーおよびセッションホストネットワークのNATタイプが互換性のない組み合わせとなり、HDX Directが失敗する特定のシナリオがあります。

検証

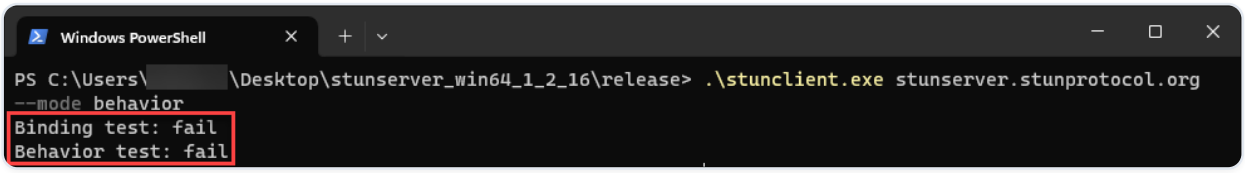
クライアントとセッションホストのNATタイプとフィルタリングは、STUNTMANのSTUNクライアントユーティリティを使用して検証できます。

1. stunprotocol.orgから、ターゲットプラットフォームに適したパッケージをダウンロードし、その内容を抽出します。
2. ターミナルプロンプトを開き、内容が抽出されたディレクトリに移動します。
3. 次のコマンドを実行します。`.\stunclient.exe stunserver2024.stunprotocol.org --mode behavior`
4. 出力を記録します。

   バインディングテストと動作テストが成功した場合、**バインディングテスト**と**動作テスト**の両方が成功を報告し、NAT動作が指定されます。

   テストが失敗した場合、**バインディングテスト**および/または**動作テスト**が失敗を報告します。

5. 次のコマンドを実行します: `.\stunclient.exe stunserver2024.stunprotocol.org --mode filtering`
6. 出力を記録します。

クライアントとセッションホストの両方のテスト結果に基づいて、外部ユーザー向けのHDX Directが動作すると期待されるかどうかを判断するには、以下の表を参照してください。

クライアントNATの動作	クライアントNATのフィルタリング	セッションホストNATの動作	セッションホストNATのフィルタリング	動作すると期待されますか？
エンドポイント独立マッピング	任意	エンドポイント独立マッピング	任意	はい
エンドポイント独立マッピング	エンドポイント独立フィルタリング	アドレス依存マッピング	任意	はい
エンドポイント独立マッピング	アドレス依存フィルタリング	アドレス依存マッピング	任意	いいえ

クライアントNATの動作	クライアントNATのフィルタリング	セッションホストNATの動作	セッションホストNATのフィルタリング	動作すると期待されますか？
エンドポイント独立マッピング	アドレスおよびポート依存フィルタリング	アドレス依存マッピング	任意	いいえ
エンドポイント独立マッピング	エンドポイント独立フィルタリング	アドレスおよびポート依存マッピング	エンドポイント独立フィルタリング	はい
エンドポイント独立マッピング	アドレス依存フィルタリング	アドレス依存マッピング	任意	いいえ
エンドポイント独立マッピング	アドレスおよびポート依存フィルタリング	アドレス依存マッピング	任意	いいえ
アドレス依存マッピング	任意	エンドポイント独立マッピング	エンドポイント独立フィルタリング	はい
アドレス依存マッピング	任意	エンドポイント独立マッピング	アドレス依存フィルタリング	いいえ
アドレス依存マッピング	任意	エンドポイント独立マッピング	アドレスおよびポート依存フィルタリング	いいえ
アドレス依存マッピング	任意	アドレス依存マッピング	任意	いいえ
アドレス依存マッピング	任意	アドレスおよびポート依存マッピング	任意	いいえ
アドレスおよびポート依存マッピング	任意	エンドポイント独立マッピング	エンドポイント独立フィルタリング	はい

クライアントNATの動作	クライアントNATのフィルタリング	セッションホストNATの動作	セッションホストNATのフィルタリング	動作すると期待されますか？
アドレスおよびポート依存マッピング	任意	エンドポイント独立マッピング	アドレス依存フィルタリング	なし
アドレスおよびポート依存マッピング	任意	エンドポイント独立マッピング	アドレスおよびポート依存フィルタリング	なし
アドレスおよびポート依存マッピング	任意	アドレス依存マッピング	任意	なし
アドレスおよびポート依存マッピング	任意	アドレスおよびポート依存マッピング	任意	いいえ
失敗	任意	任意	任意	いいえ
任意	任意	失敗	任意	いいえ
失敗	任意	失敗	任意	いいえ

トラブルシューティング

HDX Direct が直接接続を正常に確立したことを確認するには、VDA マシンで `CtxSession.exe` ユーティリティを使用できます。

`CtxSession.exe` ユーティリティを使用するには、セッション内でコマンドプロンプトまたは PowerShell を起動し、`ctxsession.exe -v` を実行します。**HDX Direct** 接続が正常に確立されている場合、**HDX Direct Status** は `Connected` です。

HDX Direct のトラブルシューティング(/en-us/citrix-virtual-apps-desktops/2411/media/hdx-direct-troubleshooting.png)

セッションホストのイベントログで、HDX™ Direct 接続が正常に確立されたか、失敗したかに関する情報を確認することもできます。詳細については、「**イベントログ**」セクションを参照してください。

> 注:
>
> 環境およびセッションホストで利用可能な IP アドレスの数によっては、HDX Direct 接続が確立されるまでに最大 5 分かかる場合があります。

HDX Direct が直接接続を確立できない場合

HDX Direct が直接接続を確立できない場合は、次の手順を確認してください。

1. 使用している VDA バージョンと Workspace アプリバージョンが、システム要件に従ってこの機能をサポートしていることを確認します。
2. HDX Direct を有効にするポリシーが VDA に適用されており、この機能を無効にする優先度の高い他のポリシーがないことを確認します。
3. 目的の HDX Direct モードを設定するポリシーが VDA に適用されており、この構成を上書きする優先度の高い他のポリシーがないことを確認します。
4. Citrix ClxMtp Service がセッションホストで実行されていることを確認します。
5. Citrix Certificate Manager Service がセッションホストで実行されていることを確認します。実行されていない場合は、手動で起動してみてください。HDX Direct が無効になっている場合、このサービスは自動的に停止します。
6. セッションホストに自己署名ルート CA 証明書があるか確認します。
    a. 発行先: `CA-<hostname>` (例: CA-FTLW11-001)
    b. 発行元: `CA-<hostname>` (例: CA-FTLW11-001)
    c. 発行者情報: 組織はCitrix Systems, Inc.です。
7. セッションホストに自己署名サーバー証明書があるか確認します。
    a. 発行先: `<host FQDN>` (例: FTLW11-001.ctxlab.net)
    b. 発行元: `CA-<hostname>` (例: CA-FTLW11-001)
    c. 発行者情報: 組織はCitrix Systems, Inc.です。
8. 証明書が見つからない場合は、Citrixテクニカルサポートにお問い合わせください。
9. 証明書が存在する場合:
    a. セッションホストでCitrix Certificate Manager Serviceを停止します。
    b. 自己署名ルートCA証明書と自己署名サーバー証明書の両方を削除します。

c. セッションホストでCitrix Certificate Manager Serviceを開始します。サービスは開始されると新しい証明書を作成します。

10. 内部ユーザーの場合:

a. セッションホストのファイアウォールが、HDX over EDTおよびHDX over TCPの場合に、UDP 443またはTCP 443でのインバウンドトラフィックをブロックしていないことを確認します。

b. ネットワークファイアウォールが、クライアントネットワークとセッションホストネットワークの間でUDP 443およびTCP 443のトラフィックをブロックしていないことを確認します。

11. 外部ユーザーの場合:

a. クライアントとセッションホストのNATタイプを確認し、その組み合わせが動作すると期待されることを確認します。詳細については、「NAT互換性」セクションを参照してください。

b. クライアントまたはセッションホストのいずれかでNATテストが失敗した場合:

i. システムでファイアウォールが実行されている場合は、UDP 3478での送信トラフィックをブロックしていないことを確認してください。

ii. ネットワークファイアウォールがUDP 3478での送信トラフィックをブロックしていないことを確認してください。

iii. ファイアウォールがSTUNサーバーの応答をブロックしていないことを確認してください。

c. ネットワークファイアウォールに、必要なすべてのトラフィックを許可するように適切なルールが構成されていることを確認してください。詳細については、「ネットワーク要件」セクションを参照してください。

d. HDX Directポート範囲ポリシー設定を使用してデフォルトのポート範囲を変更する場合は、ファイアウォールルールがカスタムポート範囲に設定されていることを確認してください。

イベントログ

次のイベントがVDAマシンのイベントログに記録されます。

ログ	ID	送信元	レベル	説明
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/操作	1	HDX ダイレクト	情報	内部ユーザー `<username>` のHDX Direct接続が確立されました。
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/操作	2	HDX ダイレクト	情報	外部ユーザー `<username>` のHDX Direct接続が確立されました。
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/操作	3	HDX ダイレクト	情報	ユーザー `<username>` のHDX Direct接続に失敗しました。

既知の問題

すでに **HDX Direct** が有効になっているマシンで VDA のインプレースアップグレードを実行すると、HDX Direct が動作しなくなる場合があります。 この問題を解決するには、次の手順を実行します。

1. セッションホストで Citrix Certificate Manager Service を停止します。
2. 自己署名ルートCA証明書と自己署名サーバー証明書を削除します。
3. レジストリを開きます。
4. `HKLM\Software\Citrix\HDX-Direct` キーを削除します。
5. `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd` にアクセスします。
6. **SSLEnabled** の値を `0` に設定します。
7. **SSLThumbprint** の値の内容を削除します。
8. **Citrix Certificate Manager Service** を開始します。

Secure HDX™ (プレビュー)

Secure HDX は、トラフィックパス内のネットワーク要素がHDXトラフィックを検査できないようにするアプリケーションレベル暗号化 (ALE) ソリューションです。これは、Citrix Workspace™ アプリ (クライアント) とVDA (セッションホスト) の間でAES-256-GCM暗号化を使用して、アプリケーションレベルで真のエンドツーエンド暗号化 (E2EE) を提供することで実現されます。

> **重要:**
>
> Secure HDX は現在プレビュー中です。この機能はサポートなしで提供されており、本番環境での使用はまだ推奨されていません。フィードバックを送信したり、問題を報告したりするには、このフォームを使用してください。

システム要件

次の一覧は、Secure HDX を使用するためのシステム要件を示しています。

- コントロールプレーン
  - シトリックス DaaS™
  - シトリックス バーチャル アプリケーションズ アンド デスクトップ™ 2402 以降
- セッションホスト
  - オペレーティングシステム
    - Windows 10 バージョン 22H2
    - Windows 11 22H2 以降
    - Windows Server 2019 以降のバージョン
  - 仮想配信エージェント (VDA)
    - Windows: バージョン 2402 以降
    - Linux: バージョン 2407 以降
- Workspace アプリ
  - Windows: バージョン 2402 以降
  - Linux: バージョン 2408 以降
  - Mac: バージョン 2409 以降

  - Chrome OS: バージョン 2409 以降
  - HTML5: バージョン 2408 以降

- アクセス層
  - シトリックス ワークスペース
  - Citrix StoreFront™ 2402 以降

> **注:**
>
> Linux VDA で Secure HDX を構成する方法の詳細については、Linux VDA のドキュメントを参照してください。

構成

Secure HDX はデフォルトで無効になっています。この機能は、Citrix ポリシーの Secure HDX 設定を使用して構成できます。

Secure HDX: 機能をすべてのセッションで有効にするか、直接接続のみで有効にするか、または無効にするかを定義します。

考慮事項

Secure HDX を使用する際の考慮事項は以下のとおりです。

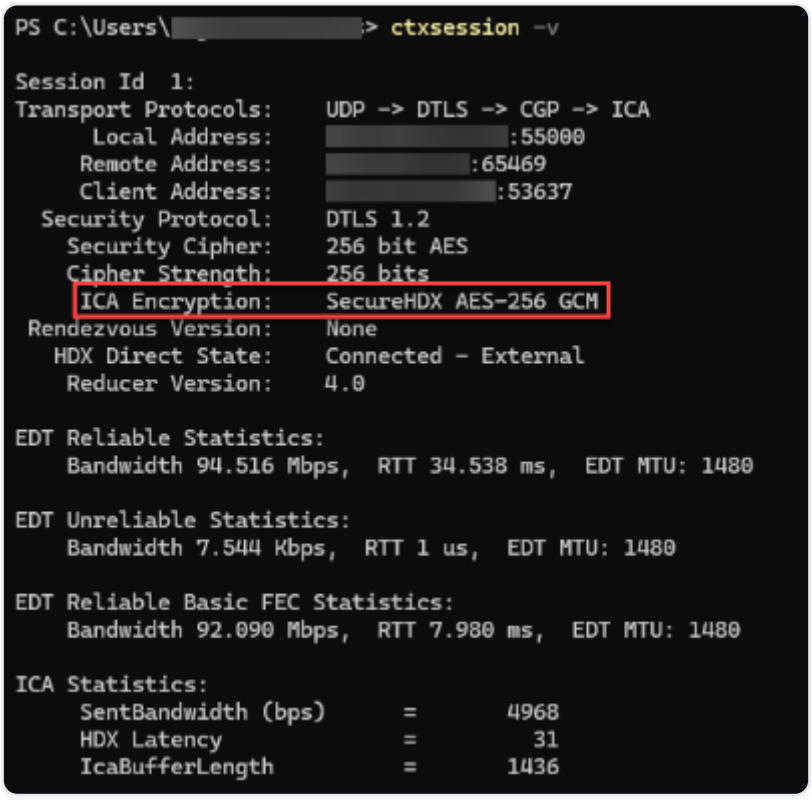
- Secure HDX が有効になっているセッションホストに、その機能をサポートしていないクライアントを使用してユーザーが接続しようとすると、接続は拒否されます。
- Service Continuity is not currently supported with Secure HDX. If you have Service Continuity enabled in your Citrix Cloud™ environment, you will not be able to any session hosts that have Secure HDX enabled if there is a Cloud service outage.
- If you use HDX Insight, note that using Secure HDX prevents HDX Insight data collection as the NetScaler® is not able to inspect the encrypted HDX traffic. If you must use HDX Insight, you can set Secure HDX to be enabled only for direct connections.
- If you use SmartControl, note that using Secure HDX prevents SmartControl from working as the NetScaler is unable to inspect the encrypted HDX traffic. If you must use SmartControl, you can set Secure HDX to be enabled only for direct connections.
- Secure HDX が有効になっている場合、Multi-Stream ICA® はサポートされません。

- HDX トラフィックの検査に依存するサードパーティソリューションを使用している場合、Secure HDX を有効にすると HDX トラフィックが暗号化されるため、それらのソリューションは機能しなくなります。
- Secure HDX を有効にするデリバリーグループで Secure ICA が有効になっている場合は、まず Secure ICA を無効にする必要があります（デリバリーグループの編集 > ユーザー設定）。

トラブルシューティング

Secure HDXがアクティブであることを確認するには、VDAマシンで`ctxsession.exe`ユーティリティを使用できます。

`CtxSession.exe` ユーティリティを使用するには、セッション内でコマンドプロンプトまたは PowerShell を開き、`ctxsession.exe -v` を実行します。Secure HDX が使用されている場合、ICA 暗号化は `SecureHDX AES-256 GCM` と表示されます。



セッションで Secure HDX が有効にならない場合

- 使用中のVDAバージョンがシステム要件に従ってこの機能をサポートしていることを確認してください。
- Secure HDXを有効にするポリシーがVDAに適用されており、この機能を無効にする優先度の高い他のポリシーがないことを確認してください。

- クライアントデバイスが NetScaler Gateway または Gateway Service を介して接続している場合、Secure HDX が「直接接続のみ」に設定されていないことを確認してください。
- Secure HDXを構成したときにセッションホストがすでに実行されていた場合は、変更が有効になるようにマシンを再起動してください。

仮想チャネル許可リスト

仮想チャネル許可リストは、環境内で許可されるCitrix以外の仮想チャネルを制御できる機能です。既定では、仮想チャネル許可リスト機能は有効になっています。その結果、Citrix Virtual Apps and Desktops™セッションで開くことが許可されるのはCitrix仮想チャネルのみです。自社開発またはサードパーティ製のカスタム仮想チャネルを使用する必要がある場合は、これらを明示的に許可リストに追加する必要があります。

構成

仮想チャネル許可リストは既定で有効になっています。この機能は、Citrixポリシーの次の設定を使用して構成できます。

- **仮想チャネル許可リスト**: この機能を有効または無効にし、仮想チャネルをリストに追加します。
- **仮想チャネル許可リストログのスロットリング**: 仮想チャネル許可リストのイベントログのスロットリング期間を設定します。
- **仮想チャネル許可リストのログ記録**: 仮想チャネル許可リストのログレベルを設定します。

仮想チャネルを許可リストに追加する

仮想チャネルを許可リストに追加するには、次の情報が必要です。

1. コードで定義されている仮想チャネル名（最大7文字）。例: `CTXCVC1`。
2. VDAマシン上で仮想チャネルを開くプロセスのパス。例: `C:\Program Files\Application\run.exe`。

必要な情報が揃ったら、仮想チャネル許可リストポリシー設定を使用して、仮想チャネルを許可リストに追加する必要があります。仮想チャネルをリストに追加するには、仮想チャネル名の後にコンマを入力し、次に仮想チャネルにアクセスするプロセスのパスを入力します。複数のプロセスがある場合は、各プロセスをコンマで区切って追加できます。

単一のプロセスの場合

前の例を使用して、次のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe
```

複数のプロセスの場合

複数のプロセスがある場合は、次のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

ワイルドカードの使用

ワイルドカード (*) の使用がサポートされています。アプリケーションのバージョンに基づいてディレクトリ名または実行可能ファイル名が変更される場合、またはサードパーティコンポーネントがユーザープロファイルにインストールされている場合に、ワイルドカードを使用できます。

次のシナリオでワイルドカードを使用できます。

- ディレクトリ名を完全に置き換える場合。 例: `C:\Program Files\Application*\run1.exe`
- ディレクトリ名の一部を置き換える場合。 例: `C:\Program Files\Application\v*\run1.exe`
- 実行可能ファイル名を置き換える場合。 例: `C:\Program Files\Application\v1.2*.exe`
- 実行可能ファイル名の一部を置き換える場合。 例: `C:\Program Files\Application\v1.2\run*.exe`

次の制限が適用されます。

- ワイルドカードは、単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルが `C:\Program Files\Application\v1.2\run1.exe` にある場合
  - 許可: `C:\Program Files\Application*\run1.exe`
  - 不許可: `C:\Program Files*\run1.exe`
- エントリにはファイル名拡張子を含める必要があります。
  - 許可: `C:\Program Files\Application\v1.2*.exe`
  - 不許可: `C:\Program Files\Application\v1.2*`
- すべてのパスはローカルである必要があります。

> **注:**
>
> - ネットワークパスは許可されていません。
> - ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2206から利用可能です。
> - ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2203 LTSRのCU2から利用可能です。

システム環境変数の使用

許可リスト内の信頼されたプロセスの定義を簡素化するために、システム環境変数を使用できます。`%programfiles%`、`%programfiles(x86)%`、`%systemdrive%`、`%systemroot%`など、すぐに使用できる任意の変数を使用できます。

カスタム環境変数も、システムレベルで定義されている限り使用できます。

以下の例は、標準の環境変数を示しています。

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

以下の例は、カスタムシステム環境変数を示しています。

- カスタム変数名: `app`
- カスタム変数値: `%programfiles%\Application\`
- 許可リストエントリ: `CTXCVC1,%app%\run.exe`

> **注:**
>
> ユーザー環境変数はサポートされていません。

> 環境変数サポートは、Citrix Virtual Apps and Desktops バージョン 2209 から利用可能です。

仮想チャネル名とプロセスの取得

VDAマシン上で仮想チャネル名とそれを開くプロセスを取得する最も簡単な方法は、仮想チャネルを提供した開発者またはサードパーティベンダーから情報を入手することです。

または、機能のログを適用し、以下の手順に従って情報を取得することもできます。

1. カスタム仮想チャネルのクライアントおよびサーバーコンポーネントが配置されたら、仮想アプリケーションまたは仮想デスクトップを起動します。
2. VDAマシンのシステムイベントログで、カスタム仮想チャネル名とそれを開こうとしたプロセスを探します。利用可能なイベントの詳細については、イベントログを参照してください。
3. セッションからログアウトします。
4. 識別された仮想チャネルとプロセスに対して、仮想チャネル許可リストポリシー設定にエントリを追加します。
5. マシンを再起動します。
6. VDAが登録されたら、仮想アプリケーションまたは仮想デスクトップを実行して、カスタム仮想チャネルが正常に開くことを検証します。

Citrix仮想チャネルに関する考慮事項

すべての組み込みCitrix仮想チャネルは信頼されており、追加設定なしで開くことができます。ただし、以下の2つの機能は、外部依存関係のため、許可リストに明示的なエントリが必要です。

- マルチメディアリダイレクト
- スカイプ・フォー・ビジネス用 HDX RealTime Optimization Pack

マルチメディアリダイレクト

システムのメディアプレーヤーとしてWindows Media Player以外のメディアプレーヤーを使用する場合、それを信頼されたプロセスとして許可リストに追加する必要があります。許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXMM`
- プロセス: VDAマシンで使用されるメディアプレーヤーへのパス。例: `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`。
- 許可リストエントリ: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

スカイプ・フォー・ビジネス用 HDX RealTime Optimization Pack

許可リストエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXRMEP`
- プロセス: VDAマシン内のSkype for Business実行可能ファイルへのパス。これはSkype for Businessのバージョンやカスタムインストールパスの使用によって異なる場合があります。例: `C:\Program Files\Microsoft Office\root\Office16\lync.exe.`.
- 許可リストエントリ: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

トラブルシューティング

カスタム仮想チャネルが開かない場合は、次の手順を確認してください。

1. 正しいVDAバージョンを使用していることを確認してください。
2. 仮想チャネル許可リストにカスタム仮想チャネルを含むポリシーがVDAに適用されており、この構成を上書きする優先度の高い他のポリシーがないことを確認してください。
3. VDAのイベントログを確認し、報告されている仮想チャネル名が許可リストで定義されているものと一致することを確認してください。

    a. 複数のプロセスがある場合は、仮想チャネルを許可リストに追加するで説明されているように、これらが適切に定義されていることを確認してください。

    b. 定義されたプロセスパスでワイルドカードを使用している場合は、ワイルドカードの使用のガイドラインに従っていることを確認してください。

    c. 定義されたプロセスパスで環境変数を使用している場合は、システム環境変数の使用のガイドラインに従っていることを確認してください。

イベントログ

次のイベントがVDAマシンのイベントログに記録されます。

シングルセッションVDA

次のイベントがシングルセッションVDAマシンのイベントログに記録されます。

ログ名	ID	送信元	レベル	説明
システム	2001	`Picadd`	情報	カスタム仮想チャネル `<vcName>` はプロセス

ログ名	ID	送信元	レベル	説明
				`<processName>` によって開かれました
システム	2002	`Picadd`	警告	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開くことができません
システム	2003	`Picadd`	情報	`<username>` がカスタム仮想チャネル `<vcName>` を開きました
システム	2004	`Picadd`	警告	`<username>` がカスタム仮想チャネル `<vcName>` を開こうとしました
システム	2005	`Picadd`	エラー	ポリシー `<pathInPolicy>` で指定されたパスはプロセスパスに解決できません
システム	2007	`Picadd`	情報	ロードされたプロセスパスは `<processPath>` です
システム	2008	`Picadd`	エラー	VCポリシーパス内の環境変数

ログ名	ID	送信元	レベル	説明
				`<varName>` が見つかりません

マルチセッションVDA

マルチセッションVDAマシンのイベントログに、以下のイベントが記録されます。

ログ名	ID	送信元	レベル	説明
システム	13	`Rpm`	情報	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開かれました
システム	14	`Rpm`	警告	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開けません
システム	15	`Rpm`	情報	`<username>` がカスタム仮想チャネル `<vcName>` を開きました
システム	16	`Rpm`	警告	`<username>` がカスタム仮想チャネル `<vcName>` を開こうとしました
システム	17	`Rpm`	エラー	ポリシー `<pathInPolicy>` で指定され

ログ名	ID	送信元	レベル	説明
				たパスは、プロセスパスに解決できません
システム	18	`Rpm`	情報	ロードされたプロセスパスは `<processPath>` です
システム	19	`Rpm`	エラー	VCポリシーパス内で環境変数 `<varName>` が見つかりません

既知のサードパーティ仮想チャネル

以下は、カスタムCitrix®仮想チャネルを使用する既知のサードパーティソリューションです。このリストには、カスタムCitrix仮想チャネルを使用するすべてのソリューションが含まれているわけではありません。

- カーナー
- ControlUp
- シスコ ウェブエックス チームズ
- シスコ ウェブエックス ミーティングス バーチャルデスクトップ ソフトウェア
- deviceTrust
- エピック ワープドライブ
- エピック スリングショット
- インプリバタ ワンサイン
- ミッドマーク IQPath クライアント拡張機能
- ニュアンス PowerMic クライアント拡張機能
- ニュアンス ドラゴン メディカル ネットワーク エディション 360 vSync
- ズーム ミーティングス for VDI
- アルティマ IA-Connect

関連する仮想チャネルを許可リストに追加するための詳細については、ソリューションのベンダーにお問い合わせください。または、仮想チャネル名とプロセスの取得セクションに記載されている手順に従ってください。

DVC用仮想チャネル許可リスト

DVC用仮想チャネル許可リストを使用して、環境で許可されるカスタム動的仮想チャネルを制御できます。デフォルトでは、動的仮想チャネルは許可されていません。動的仮想チャネルが必要な場合は、明示的に許可リストに追加する必要があります。

構成

DVC用仮想チャネル許可リストはデフォルトで有効になっています。この機能は、Citrix®ポリシーの以下の設定を使用して構成できます。

- DVC用仮想チャネル許可リスト: 機能を有効または無効にし、動的仮想チャネルをリストに追加します。
- 仮想チャネル許可リストログスロットリング: 仮想チャネル許可リストイベントログのスロットリング期間を設定します。
- 仮想チャネル許可リストログ記録: 仮想チャネル許可リストのログレベルを設定します。

許可リストへの動的仮想チャネルの追加

動的仮想チャネルを許可リストに追加するには、以下の情報が必要です。

1. クライアント上のDVCプラグインの名前。例: `DvcPlugin1.dll`。
2. DVCリスナーの名前。例: `ListenerName1`。
3. VDAマシン上で動的仮想チャネルにアクセスするプロセスのパス。例: `C:\Program Files\Application\run.exe`。

必要な情報が揃ったら、DVC用仮想チャネル許可リストポリシー設定を使用して、動的仮想チャネルを許可リストに追加する必要があります。リストに動的仮想チャネルを追加するには、セッションホストでDVCにアクセスするプロセスのパスを入力し、その後にコンマ、クライアント側プラグイン名、コンマ、およびプラグインが使用するリスナー名を入力します。複数のリスナー名はコンマで区切って追加できます。

単一リスナーの場合

前の例を使用して、以下のエントリをリストに追加します。 `C:\Program Files\App\run1.exe,DvcPlugin1,ListenerName1`

複数リスナーの場合

複数のリスナーがある場合は、リストに次のエントリを追加します。 `C:\Program Files\App\run1.exe,DvcPlugin1,ListenerName1,ListenerName2`

ワイルドカードの使用

ワイルドカード（*）の使用がサポートされています。ワイルドカードは、ディレクトリ名や実行可能ファイル名がアプリケーションのバージョンによって変更される場合、またはサードパーティコンポーネントがユーザープロファイルにインストールされている場合に使用できます。

ワイルドカードは次のシナリオで使用できます。

- ディレクトリ名を完全に置き換える場合。例: `C:\Program Files\App*\run1.exe`
- ディレクトリ名の一部を置き換える場合。例: `C:\Program Files\App\v*\run1.exe`
- 実行可能ファイル名を置き換える場合。例: `C:\Program Files\App\v1.2*.exe`
- 実行可能ファイル名の一部を置き換える場合。例: `C:\Program Files\App\v1.2\run*.exe`

次の制限が適用されます。

- ワイルドカードは、単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルが `C:\Program Files\App\v1.2\run1.exe` にある場合
  - 許可: `C:\Program Files\App*\run1.exe`
  - 許可されていません: `C:\Program Files*\run1.exe`
- エントリにはファイル名拡張子を含める必要があります。
  - 許可: `C:\Program Files\App\v1.2*.exe`
  - 不許可: `C:\Program Files\App\v1.2*`
- すべてのパスはローカルである必要があります。

デバイス

HDX™は、あらゆる場所のあらゆるデバイスで高精細なユーザーエクスペリエンスを提供します。デバイスセクションの記事では、以下のデバイスについて説明しています。

- スキャン
- 汎用USBデバイス
- クライアントドライブマッピング
- モバイルおよびタッチスクリーンデバイス
- シリアルデバイス
- 特殊キーボード
- Webカメラ

最適化されたUSBデバイスと汎用USBデバイス

最適化されたUSBデバイスとは、Citrix Workspace™アプリが特定のサポートを提供しているデバイスです。たとえば、HDXマルチメディア仮想チャネルを使用してWebカメラをリダイレクトする機能などです。汎用デバイスとは、Citrix Workspaceアプリで特定のサポートがないUSBデバイスです。

デフォルトでは、汎用USBリダイレクトは、汎用モードに設定しない限り、最適化された仮想チャネルサポートを持つUSBデバイスをリダイレクトできません。

一般的に、USBデバイスは汎用モードよりも最適化モードの方がパフォーマンスが向上します。ただし、最適化モードではUSBデバイスが完全な機能を発揮しない場合があります。その機能に完全にアクセスするには、汎用モードに切り替える必要があるかもしれません。

USBマスストレージデバイスでは、Citrix®ポリシーによって制御されるクライアントドライブマッピング、汎用USBリダイレクト、またはその両方を使用できます。主な違いは次のとおりです。

汎用USBリダイレクトとクライアントドライブマッピングの両方のポリシーが有効になっており、セッション開始前または開始後にマスストレージデバイスが挿入された場合、そのデバイスはクライアントドライブマッピングを使用してリダイレクトされます。

これらの条件が真の場合、マスストレージデバイスは汎用USBリダイレクトを使用してリダイレクトされます。

- 汎用USBリダイレクトとクライアントドライブマッピングポリシーの両方が有効になっています。
- デバイスが自動リダイレクト用に構成されています。
- マスストレージデバイスがセッション開始前または開始後に挿入されます。

詳細については、`<http://support.citrix.com/article/CTX123015>`を参照してください。

機能	クライアントドライブマッピング	汎用USBリダイレクト
デフォルトで有効	はい	いいえ
読み取り専用アクセス設定可能	はい	いいえ
暗号化されたデバイスアクセス	はい、仮想セッションでデバイスがアクセスされる前に暗号化が解除されている場合。	Citrix Virtual Desktops™ のみに適用

スキャン

TWAINリダイレクト

はじめに

ユーザーは、クライアントエンドポイントに接続されたTWAIN準拠のスキャナーを使用して、Citrix HDX™セッション内の32ビットアプリケーションからドキュメントをスキャンできます。Citrixスキャンモジュールは、スキャン要求をクライアントエンドポイントにリダイレクトして処理します。完了すると、スキャンされた情報はVDAホストに送り返されます。

要件

Citrixコントロールプレーン

- シトリックス Virtual Apps and Desktops™ 1912 以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ 11
  - Windows Server 2022 またはそれ以降のバージョン
- VDA
  - バージョン1912以降
- アプリケーション
  - 32ビットアプリケーション

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ 11
- Workspaceアプリ
  - Windows: バージョン1912以降
- スキャナー
  - TWAIN準拠スキャナー
  - クライアントエンドポイントにTWAINドライバーをインストールする

構成

TWAINリダイレクトはデフォルトで有効になっています。TWAINリダイレクトを構成し、スキャンエクスペリエンスを最適化するために、以下のポリシー設定が利用可能です。

- **クライアントTWAINデバイスリダイレクト:** TWAINリダイレクトを有効または無効にする。
- **TWAIN圧縮レベル:** クライアントからVDAに転送される画像の圧縮レベルを設定する。

詳細については、「TWAINデバイスのポリシー設定」を参照してください。

トラブルシューティング

TWAINリダイレクト機能は、公開されているテストアプリTwackerを使用してテストできます。このアプリは、次のURLからダウンロードできます。

HDXセッション内でTWAIN機能を検証するには、次の手順に従います。

1. VDAホストに**Twacker**をインストールします。
2. **Twacker** (32ビット版) を起動します。
3. **File > Select Source**をクリックし、リストからスキャナーを選択します。
4. **File > Acquire**をクリックします。
5. **Scan button**をクリックして、スキャナーをテストします。

Twacker が正常にスキャンできる場合、それは、**Citrix Virtual Apps and Desktops** のセットアップが次のとおりであることを確認します。

- TWAINリダイレクトを使用するように正しく構成されている
- すべてのローカルクライアントデバイス要件を満たしている

特定のアプリケーション内でスキャンに関する問題が引き続き発生する場合は、ソフトウェアの問題である可能性が高いです。

WIA デバイス

要件

- スキャナーはWIA準拠である必要があります。
- WIAドライバーをローカルデバイスにインストールします。サーバーには必要ありません。
- スキャナーをローカルに接続します（例：USB経由）。
- スキャナーがローカルのWindows Image Acquisitionサービスを使用しており、TWAINドライバーを使用していないことを確認してください。
- テストに使用されるユーザーアカウントに、ICA®セッション内の帯域幅を制限するポリシーが適用されていないことを確認してください。たとえば、クライアントUSBリダイレクト帯域幅制限などです。

Windows イメージ取得アプリケーション許可リスト

許可リストを使用すると、VDA上のどのアプリケーションがWindows Image Acquisitionスキャナーリダイレクトにアクセスできるかを制御できます。レジストリエディターは、Windows

Image Acquisitionを含む各VDAの許可リスト設定からの入力を使用します。デフォルトでは、どのアプリケーションもWindows Image Acquisitionにアクセスできません。

VDA上のアプリケーションのWindowsイメージ取得を調整するには、レジストリを介して管理される機能のリストにあるWindowsイメージ取得アプリケーションの許可リスト設定を参照してください。

ポリシー設定の詳細については、WIAデバイスのポリシー設定を参照してください。

SANEリダイレクト

はじめに

ユーザーは、ChromeOSエンドポイントからCitrix®セッション内のTWAINアプリケーションからドキュメントをスキャンできます。ユーザーがアプリケーションからドキュメントをスキャンしようとすると、Citrixスキャンモジュールは要求をクライアントエンドポイントにリダイレクトしてスキャナーからのスキャンを実行し、スキャンが完了するとファイルはVDAに送信されます。

要件

Citrixコントロールプレーン

- シトリックス バーチャルアプリおよびデスクトップ™ 2411 以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ 11
  - ウィンドウズ サーバー 2019 以降
- VDA
  - バージョン2411以降

クライアントデバイス

- オペレーティングシステム
  - ChromeOS v129以降
- Workspaceアプリ

- ChromeOS: バージョン2409以降

- スキャナー
  - スキャナーはChrome OSでサポートされている必要があります。
  - サポートされているデバイス: Fujitsu FI-7160、FI-8170

    注:

    上記に記載されている以外のスキャナーは、Chrome OSでサポートされている場合、Native Twain UIを使用して使用できます。

  - USB経由でクライアントエンドポイントにローカルに接続されている必要があります。

構成

この機能を有効にするための追加設定は不要です。この機能はデフォルトで有効になっています。

注:

この機能を無効にするには、Web Studio/DaaSコンソールを開きます。SANEスキャナーリダイレクトポリシー設定を「禁止」に設定します。

トラブルシューティング

イベントログ

管理者は、スキャン関連のさまざまなイベントメッセージを表示できます。

以下に、さまざまなスキャン関連操作のためにVDAホストのイベントビューアーに記録されるイベントメッセージを示します。これらは、Windowsログの「アプリケーション」セクションで、イベントソースとしてHDX™ Scannerを使用して表示できます。

イベントID	イベントテキスト	説明
2	AllowScannerSANERedirectionポリシーが無効になっています。スキャナーはリダイレクトされません。	SaneRedirectionポリシーが無効になっていることを示します。

イベントID	イベントテキスト	説明
3	スキャン詳細: ページ - '[pages]'、アプリケーション - '[application]'、スキャナー - '[scanner]'、ユーザー - '[user]'、1ページあたりの平均時間 - '[time]'ミリ秒。	スキャンが完了したときに生成されます。
101	スキャンするページが見つかりません。	ドキュメントが検出されなかったときに生成されます。
102	スキャン失敗 - デバイスのドキュメントフィーダーが詰まっています。	スキャナーのドキュメントフィーダーでの紙詰まりによりスキャンが失敗した場合に生成されます。
103	スキャン失敗 - 「[failure]」。スキャナーアプリケーションを閉じて再起動してください。	サポートされていない操作、ファイル終端エラー、アクセス拒否エラーなどのエラーによりスキャンが失敗した場合に生成されます。
104	アプリケーションでのメモリ障害。アプリケーションを再起動してください。	メモリ不足によりスキャンが失敗した場合に生成されます。
201	ユーザーによってスキャン操作がキャンセルされました。	ユーザーによってスキャン操作がキャンセルされた場合に生成されます。
202	スキャン中にセッションが切断されました。	スキャン中にHDXセッションが切断された場合に生成されます。
203	'[capability]' の TWAIN と SANE 間の変換はサポートされていません。スキャナー/アプリケーションがサポートされているか確認してください。	指定された機能の TWAIN と SANE 間の変換がサポートされていないことを示します。

イベントID	イベントテキスト	説明
205	スキャナー '[scanner]' をアクティブに設定できませんでした。スキャナーの電源が入っていて接続されているか確認してください。	スキャナーへの接続が開けなかった場合に生成されます。
206	スキャナーが見つかりません。スキャナーの電源が入っていて接続されているか確認してください。	クライアントエンドポイントでスキャナーが検出されなかった場合に生成されます。

既知の制限事項

1. ネットワーク認証されたスキャナーはサポートされていません。
2. VDA 上の Fujitsu Paperstream アプリケーションなど、一部の独自のスキャンアプリケーションは、リダイレクトされたスキャナーをサポート対象として表示しない場合があります。
3. ネイティブ UI を使用する場合、ページ幅、ページ高さ、用紙サイズ、明るさ、コントラストなど、一部のスキャナー設定は、サードパーティ API の制限により適用されない場合があります。

USBデバイス

はじめに

汎用USBリダイレクト機能により、USBデバイスをクライアントマシンからHDX™セッションにリダイレクトでき、エンドユーザーはHDXセッションで幅広い汎用USBデバイスを操作できます。これは、最適化されたサポートがない、または不適切な特殊デバイスを使用する必要があるシナリオで役立ちます。

> **注：** 仮想チャネルサポート用に最適化されていないUSBデバイスは、汎用USB仮想チャネルにフォールバックし、生のUSBリダイレクトを使用します。

仕組み?

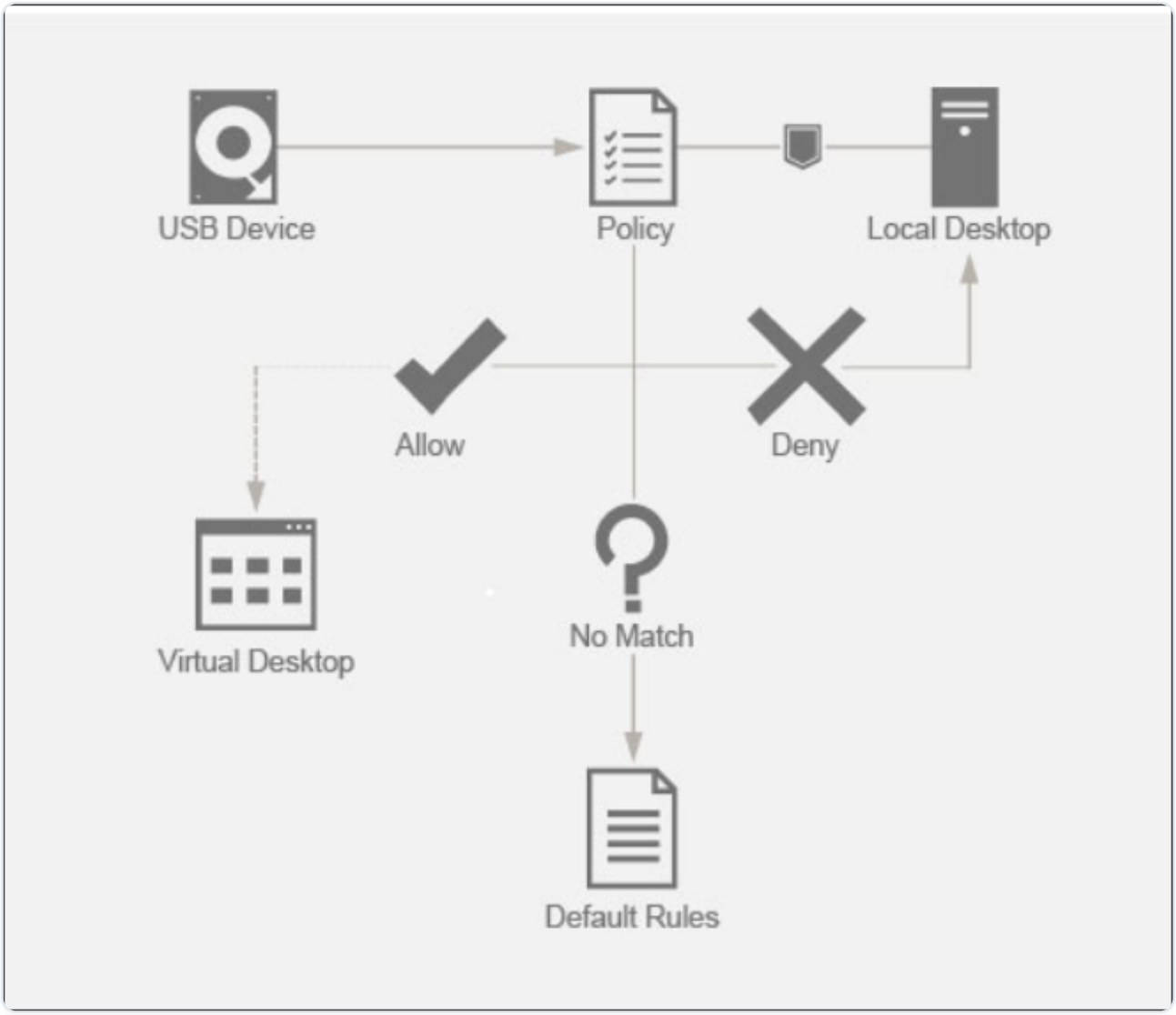
汎用USBリダイレクトは低レベルで機能し、クライアントマシンとXenDesktop®仮想デスクトップ間でUSB要求および応答メッセージをリダイレクトします。

クライアントマシンに互換性のあるデバイスドライバーが必要なくなり、ドライバーは仮想デスクトップでのみサポートされることが期待されます。USBリダイレクトポリシー規則は、DDCポリシー規則が評価および適用された後、クライアント側のポリシーとデフォルト規則が尊重されるように、特定の優先順位に従います。これにより、Citrix管理者は、不正なデバイスや偽装されたデバイスがセッション内にリダイレクトされるのを防ぐことができます。

さらに、リモートセッションへのアクセスを試みる不正なデバイスのイベントログを監査およびフラグ付けでき、管理者はデータ漏洩を防ぐための追加措置を講じることができます。

ユーザーがUSBデバイスを接続すると、セッションホストは一致が見つかるまで各ポリシー規則と照合してチェックします。任意のデバイスに対する最初の一致が最終的なものと見なされます。

- 最初の一致が許可規則である場合、デバイスは仮想デスクトップにリダイレクトされます。
- 最初の一致が拒否規則である場合、デバイスはセッションにリダイレクトされず、ローカルユーザーデバイスでのみ使用できます。一致が見つからない場合は、デフォルト規則が使用されます。



汎用USBリダイレクトとの互換性

以下のCitrix Workspace™アプリは、汎用USBリダイレクトをサポートしています:

- Windows向けCitrix Workspaceアプリ。詳しくは、Windows向けCitrix Workspaceアプリを参照してください。
- Citrix Workspace app for Macについては、Citrix Workspace app for Macを参照してください。
- Citrix Workspace app for Linuxについては、Citrix Workspace app for Linuxを参照してください。
- Citrix Workspace app for Chrome OSについては、Citrix Workspace app for Chromeを参照してください。

Citrix Workspaceアプリのバージョンについては、Citrix Workspaceアプリの機能マトリックスを参照してください。

構成

USBリダイレクトはデフォルトで無効になっています。Citrix®ポリシーで以下の設定を使用して、汎用USBリダイレクトを構成できます。

- **クライアントUSBデバイスリダイレクト**: USBリダイレクトを有効または無効にする
- **クライアントUSBデバイスリダイレクト規則**: 特定のデバイスアクション、つまり特定のデバイスへのアクセスを許可または拒否するように指定する
- **クライアントUSBデバイスリダイレクト規則（バージョン2）**: USBデバイスのフィルタリング、分割、自動接続の規則を指定する
- **クライアントUSBデバイス最適化規則**: 最適化を無効にするか、最適化モードを変更する
- **既存のUSBデバイスの自動接続を許可する**: HDX™セッションの開始時にクライアントエンドポイントに接続されている既存のUSBデバイスの自動接続を許可または防止する
- **新しく接続されたUSBデバイスの自動検出を許可する**: HDXセッション中にクライアントエンドポイントに接続されているUSBデバイスの自動接続を許可または防止する

詳細は、USBポリシー設定を参照してください。

USBリダイレクトの構成方法

デフォルトでは、USBリダイレクト構成は無効になっています。使用するには、USBリダイレクトポリシーと特定のリダイレクト規則をDDCで有効にして構成する必要があります。

> **注:**

> バージョン2212より前のコンポーネントを使用している場合、またはLinux/Mac版Workspaceアプリを使用している場合は、USBリダイレクトの構成方法の詳細について「レガシーUSBリダイレクト構成」を参照してください。

汎用USBリダイレクトの有効化

1. **Citrix Web Studio™ポリシー**を開き、**［ポリシー］**タブをクリックします。
2. **［ポリシーの作成］をクリックし、［ICA®］>［USBデバイスポリシー］**を展開します。
3. **クライアントUSBデバイスリダイレクトポリシー**を編集します。
4. 「**許可**」を選択し、「**保存**」をクリックします。

USBリダイレクトポリシー規則の作成

ユーザーがUSBデバイスを仮想デスクトップにリダイレクトしようとすると、一致が見つかるまで各USBポリシー規則に対して順にチェックされます。いずれかのデバイスに対する最初の一致が最終と見なされます。最初の一致が**許可**規則である場合、一致したデバイスは仮想デスクトップにリダイレクトが許可されます。最初の一致が**拒否**規則である場合、一致したデバイスはローカルデスクトップでのみ利用可能です。一致が見つからない場合は、デフォルト規則が使用されます。

デバイス規則

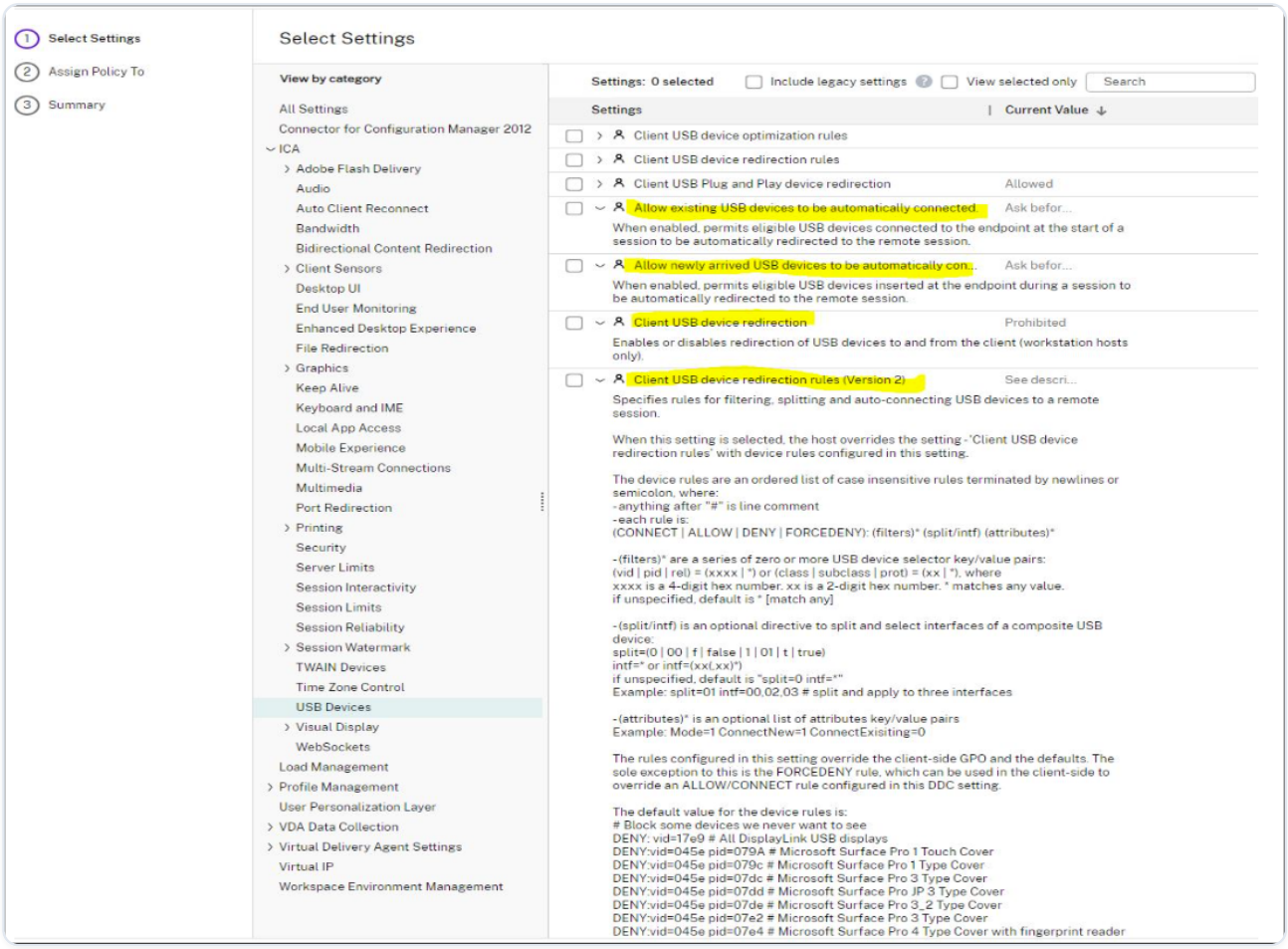
通常のUSBデバイスと同様に、ポリシーまたはエンドポイント上のクライアントCitrix Workspace™アプリの構成で設定されたデバイス規則により、転送するデバイスが選択されます。Citrix Workspaceアプリはこれらの規則を使用して、どのUSBデバイスのリモートセッションへの転送を許可または防止するかを決定します。

各規則は、アクションキーワード（**Allow、Connect、またはDeny**）、コロン（:）、およびエンドポイントのUSBサブシステムにある実際のデバイスと一致するゼロ個以上のフィルターパラメーターで構成されます。これらのフィルターパラメーターは、すべてのUSBデバイスが自身を識別するために使用するUSBデバイス記述子メタデータに対応しています。

デバイス規則はクリアテキストであり、各規則は1行に記述され、#文字の後にオプションのコメントが続きます。規則は上から下へ（優先順位の降順で）照合されます。デバイスまたは子インターフェースに一致する最初の規則が適用されます。同じデバイスまたはインターフェースを選択する後続の規則は無視されます。

例: 許可 VID=1050 PID=0421 #Device1 **例:** 接続 VID=xxxx PID=yyyy Class=03 #Device2

キーワード	説明
CONNECT	このキーワードを使用して、USB仮想チャネル経由でのデバイスのリダイレクトを許可し、セッション起動時および挿入時の自動リダイレクトを有効にします。
ALLOW	このキーワードを使用して、USB仮想チャネル経由でデバイスのリダイレクトを許可します
拒否	このキーワードを使用して、USB仮想チャネル経由でデバイスがリダイレクトされるのを拒否します



DDC でポリシーを設定する:

1. **Citrix Web Studio ポリシー**」を開き、「**ポリシー**」タブをクリックします。
2. **ポリシーの作成**」をクリックし、「**ICA > USB デバイス ポリシー**」を展開します。
3. **クライアント USB デバイス リダイレクト規則**」を編集します (「**バージョン 2**」)。

4. リダイレクトする必要がある各 USB デバイスの説明に記載されている例に基づいて値を設定し、「保存」をクリックします。

   例：許可：VID=056A PID=00A4 #STU-430 拒否：Class=08 subclass=05 # Mass Storage

   > **注:**
   >
   > Citrix 管理者が「**既定値を使用**」をオンにして「**保存**」をクリックすると、既定の規則は VDA の次のレジストリにあります。
   >
   > **注意!**
   >
   > レジストリエディターを使用する前に、この記事の最後にある免責事項を参照してください。
   >
   > `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

> **注:**
>
> グループポリシーデバイスルールを使用してクライアントデバイスにポリシーを設定することは可能ですが、CVADおよびCWAの新しいバージョンでは不要になりました。

USB デバイスのレガシー構成については、「レガシー USB リダイレクト構成」を参照してください。

USBデバイスの自動リダイレクトを構成する（オプション）

USBサポートが有効になっている場合、USBデバイスは自動的にリダイレクトされます。また、USBユーザー設定はUSBデバイスを自動的に接続するように設定されています。すべてのUSBデバイスをリダイレクトすることが常に最適とは限りません。ユーザーは、自動的にリダイレクトされないUSBデバイスリストからデバイスを明示的にリダイレクトできます。USBデバイスが一覧表示されたりリダイレクトされたりするのを防ぐには、クライアントエンドポイントまたはDDCポリシーのいずれかでDeviceRulesを使用します。 このポリシーは、DDC、GPOを使用したクライアント、Citrix Workspace Preferences、またはCDViewerのタブのいずれかで設定できます。これらのすべての方法は以下で説明されています。

DDCでポリシーを設定する:

USB デバイスの自動リダイレクトを許可するように設定できる DDC 上のポリシーは 2 つあります。

- 既存のUSBデバイスの自動接続を許可する
- 新しく接続されたUSBデバイスの自動接続を許可する

a. 「**Citrix Web Studioポリシー**」を開き、「**ポリシー**」タブをクリックします。
b. 「**ポリシーの作成**」をクリックし、「**ICA > USBデバイスポリシー**」を展開します。
c. 設定「**既存のUSBデバイスの自動接続を許可する**」を編集します。
d. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択して、「**保存**」をクリックします。
e. 設定「**新しく接続されたUSBデバイスの自動接続を許可する**」を編集します。
f. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択して、「**保存**」をクリックします。

複合デバイスとデバイス分割

複合USBデバイスは、コンピューターに接続された複数の独立したUSBデバイスのように機能する単一のデバイスです。単一のUSBコネクタを持ちますが、それぞれ独自の機能セットを持つ複数のインターフェイスをコンピューターに公開できます。ユーザーが複合USBデバイスを接続すると、ホストデバイスはすべての機能（インターフェイス）を各ポリシー規則と照合して確認します。いずれかの機能（インターフェイス）に対する最初の照合が拒否規則である場合、その規則は複合デバイスに対して最終的なものと見なされ、デバイスは拒否されます。機能（インターフェイス）に対する最初の照合が許可規則である場合、ホストデバイスは次の機能（インターフェイス）に対して規則の照合を続行します。複合デバイスは、ポリシー規則によって機能（インターフェイス）が拒否されない場合に許可されます。複合デバイスに対する最終的な照合が拒否規則である場合、デバイスはローカルデスクトップでのみ利用可能になり、それ以外の場合は仮想デスクトップにリモート接続されます。一致が見つからない場合は、デフォルト規則が使用されます。

デバイス分割の図(/en-us/citrix-virtual-apps-desktops/2411/media/device-splitting.png)

複合デバイスの特定の機能のみを許可するために、デバイスリダイレクト規則（バージョン2）ポリシーで適切な規則を使用して複合デバイスを分割できます。たとえば、FIDO2キーのHID機能の

みを使用し、スマートカード機能は使用したくない場合があります。その場合、以下に示すように規則を設定します。

1. Connect: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikeyシリーズ5のFIDO2 HID機能は許可されています。
2. Deny: VID=1050 PID=0407 split=01 intf=02 # Yubikeyシリーズ5のスマートカード機能はブロックされています。

> **ヒント:**
>
> 新しいポリシー規則を作成する際は、USB Webサイトで入手可能なUSBクラスコードを参照してください。

署名パッドの構成

1. VDAホストに適切なデバイスドライバーをインストールします。
2. **Citrix Web Studio™**で**クライアントUSBデバイスリダイレクト**ポリシー設定を有効にします。
3. **クライアントUSBデバイスリダイレクト規則（バージョン2）**ポリシー設定を編集します。
    a. リダイレクトする必要がある署名パッドの**VID**および**PID**情報を設定し、**保存**をクリックします。例：**Connect**: VID=06A8 PID=0057 class=03 #Topaz HSB
4. **クライアントUSBデバイス最適化規則**ポリシー設定を編集します。
    a. その他のデバイス情報とともにモードを設定します。例：Mode=00000004 VID=06A8 PID=0057 class=03 #キャプチャモードで動作する入力デバイス
5. ポリシー設定**既存のUSBデバイスの自動接続を許可する**を編集します。
6. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクトする**を選択して、**保存**をクリックします。
7. ポリシー設定**新しく接続されたUSBデバイスの自動接続を許可する**を編集します。
8. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクトする**を選択して、**保存**をクリックします。

これらの設定が構成されると、以降のセッション起動ではデバイスが自動的にリダイレクトされ、エンドユーザーによる追加のアクションは不要になります。

> **注：**
>
> VIDとPIDを、リダイレクトするデバイスの実際のVIDとPIDに置き換えます。

USBリダイレクトを使用したBloombergキーボードの構成

1. **Citrix Web Studio**で**クライアントUSBデバイスリダイレクト**ポリシー設定を有効にします。
2. Bloomberg 5キーボードは、**クライアントUSBデバイスリダイレクト規則（バージョン2）**ポリシー設定でデフォルトで設定されており、追加の管理者アクションは不要です。
3. ポリシー設定**既存のUSBデバイスの自動接続を許可する**を編集します。
4. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクトする**を選択して、**保存**をクリックします。
5. ポリシー設定**新しく接続されたUSBデバイスの自動接続を許可する**を編集します。
6. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクトする**を選択して、**保存**をクリックします。

これらの設定が構成されると、Bloombergキーは以降のHDX™セッションで自動的に表示され、エンドユーザーによる追加のアクションは不要になります。

USBリダイレクトを使用したFIDO2キーの構成

Citrixでは、HDXセッションでFIDO2キーを使用するためにFIDO2リダイレクトを使用することを推奨しています。ただし、代わりにUSBリダイレクトを使用してFIDO2キーをリダイレクトする必要がある状況もあります。これには、クライアント、VDA、またはオペレーティングシステム（例：Windows Server 2016）で機能がサポートされていないため、FIDO2リダイレクトが利用できないシナリオが含まれます。

また、キーに複数のモードが有効になっている場合でも、HDXセッションではその一部のみを許可したいという状況も考えられます。たとえば、FIDO2とOTPは許可するが、スマートカードはブロックしたい場合などです。

次の手順は、USBリダイレクトを使用してFIDO2キー（Yubikey vid=1050, pid=0407）を構成する方法を示しています。

1. **Citrix Web Studio**で**クライアントUSBデバイスリダイレクト**ポリシー設定を有効にします。
2. **クライアントUSBデバイスリダイレクトルール（バージョン2）**ポリシー設定を編集します。

a. セッションでリダイレクトするFIDO2キーの**VID**と**PID**情報、および分割デバイス構成を設定し、**保存**をクリックします。

b. **接続**: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikeyシリーズ5で許可されるFIDO2 HID機能。

c. **拒否**: VID=1050 PID=0407 split=01 intf=02 # Yubikeyシリーズ5のスマートカード機能はブロックされました。

3. ポリシー設定**既存のUSBデバイスの自動接続を許可する**を編集します。
4. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクト**を選択して、**保存**をクリックします。
5. ポリシー設定**新しく接続されたUSBデバイスの自動接続を許可する**を編集します。
6. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクト**を選択して、**保存**をクリックします。

これらの設定が構成されると、FIDO2キーボードは以降のHDXセッションで自動的に表示され、エンドユーザーによる追加の操作は不要になります。

USBリダイレクトを使用した3Dマウスの構成

現在、3dConnexionスペースマウスドライバーはワークステーションOS (Win 10およびWin11) でのみサポートされています。サーバーOSでは動作しません。以下は、ワークステーションOS (vid=046D, pid=C016) でSpaceMouse Enterpriseを構成する手順です。

1. VDAホストに最新のWindowsドライバーをインストールします。
2. 「**Citrix Web Studio**」で「**クライアントUSBデバイスリダイレクト**」ポリシー設定を有効にします。
3. **クライアントUSBデバイスリダイレクトルール (バージョン2)** ポリシー設定を編集します。

   a. リダイレクトする必要がある署名パッドの**VID**と**PID**情報を追加し、**保存**をクリックします。例: **接続**: VID=046D PID=C016 #SpaceMouse Enterprise

4. ポリシー設定**クライアントUSBデバイス最適化ルール**を編集します。

   a. 他のデバイス情報とともにモードを設定します。例: Mode=00000004 VID=046D PID=C016 class=03 #Input device operating in capture mode

5. ポリシー設定**既存のUSBデバイスの自動接続を許可する**を編集します。
6. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクトする**を選択して**保存**をクリックします。

7. ポリシー設定**新しく接続されたUSBデバイスの自動接続を許可する**を編集します。
8. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクトする**を選択して**保存**をクリックします。

異なるデバイスルールでUSBリダイレクトを使用して2つ以上のデバイスを構成する

複数のデバイスを異なるデバイスルールでHDXセッション内にリダイレクトできます。管理者は、一方のデバイスを自動的にリダイレクトし、もう一方のデバイスをエンドユーザーがリダイレクトするオプションを提供したい場合があります。以下は、異なるルールで2つのデバイスを構成する手順です。

1. **Citrix Web Studio**で**クライアントUSBデバイスリダイレクト**ポリシー設定を有効にします。
2. **クライアントUSBデバイスリダイレクトルール (バージョン2)** ポリシー設定を編集します。
    a. セッション内の適切なデバイス規則を使用してリダイレクトする2つのデバイスの**VID**と**PID**の情報を追加し、**保存**をクリックします。
    b. **許可**: VID=0911 PID=0c1c #Phillips スピーチマイク.
    c. **接続**: VID=06A8 PID=0043 class=03 # Topaz HSB 署名パッド
3. ポリシー設定「**既存のUSBデバイスの自動接続を許可する**」を編集します。
4. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクトする**を選択して、**保存**をクリックします。
5. 「**新しく接続されたUSBデバイスの自動接続を許可する**」ポリシー設定を編集します。
6. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクトする**を選択して、**保存**をクリックします。

これらの設定が構成されると、Topaz HSB 署名パッドは、以降のHDXセッションで自動的に表示され、追加のエンドユーザー操作は不要になります。一方、Phillips スピーチマイクは、エンドユーザーがConnection CenterまたはCDViewerのタブでリダイレクトを有効にする必要があります。

トラブルシューティング

USBリダイレクト関連の問題をトリアージするには、次の手順に従ってください。

1. USBリダイレクトのシステム要件が満たされていることを確認します。これには、正しいCVADおよびCWAバージョン、サポートされているデバイス、および検討中のOSプラットフォーム上のデバイスドライバーが含まれます。

2. お使いの環境で使用されているコンポーネントのバージョンとプラットフォームに基づいて、構成が適切であることを確認してください。(/ja-jp/citrix-virtual-apps-desktops/2411/devices/usb-devices/legacy-usb-redirection-configuration.html)を必要とするコンポーネントの詳細については、「レガシーUSBリダイレクト構成」の注記を参照してください。
3. デバイスがクライアントによって列挙されたデバイスの下にリストされていることを確認します。

    a. Workspace Preferencesツールバー: WorkspaceアプリのPreferencesツールバーのタブに列挙されているデバイスを確認します（**CWAアイコン > Connection Center > Preferences**を右クリック… **デバイス**タブをクリック）。

    b. `CtxUsbDiagnostics.exe`（推奨）：このツールをコマンドプロンプトウィンドウで実行します。出力には、特定のセッションのデバイス固有の情報が表示されます。デバイスがリダイレクトされているかどうか、またデバイスルールセットがデバイスのリダイレクトを妨げているかどうかがわかります。詳細については、診断ツールを参照してください。

    c. USBViewまたはその他のサードパーティツール: エンドポイント/クライアントマシンでUSBViewのようなサードパーティツールを実行し、デバイスがエンドポイントで検出されていることを確認します。

4. デバイスが列挙されている場合：

    a. 特定のデバイスに対してCtxUsbDiagnosticsツールの出力に拒否ルールが表示される場合は、Studioで構成されているポリシーを確認し、バージョン2ポリシーでルールが正しく設定されていることを確認します。拒否ルールがStudioポリシーに表示されない場合は、クライアント側ポリシー、そして最後にクライアント側デフォルトの順に確認して、一致する拒否ルールを見つけます。

    b. CtxUsbDiagnosticsの出力に拒否ルールがない場合、CWAはPreferencesウィンドウのデバイスタブ（デバイス > デバイスの管理）で適切なボタンをチェック/クリックすることでデバイスのリダイレクトを許可します。一度リダイレクトされたデバイスはセッションで利用可能になります。これは、HDXセッションでデバイスマネージャー/USBViewまたは同様のアプリケーションをチェックすることで確認できます。

5. セッション内にデバイスが表示されない場合：

    a. VDAホストに正しいデバイスドライバーが正しくインストールされていない可能性があります。VDAホストに最新バージョンのデバイスドライバーが正しくインストールされていることを確認してください。一部のデバイスドライバーはターミナルサーバーマシンではサポートされていないため、リダイレクトしようとしているデバイスがそうでないことを確認してください。

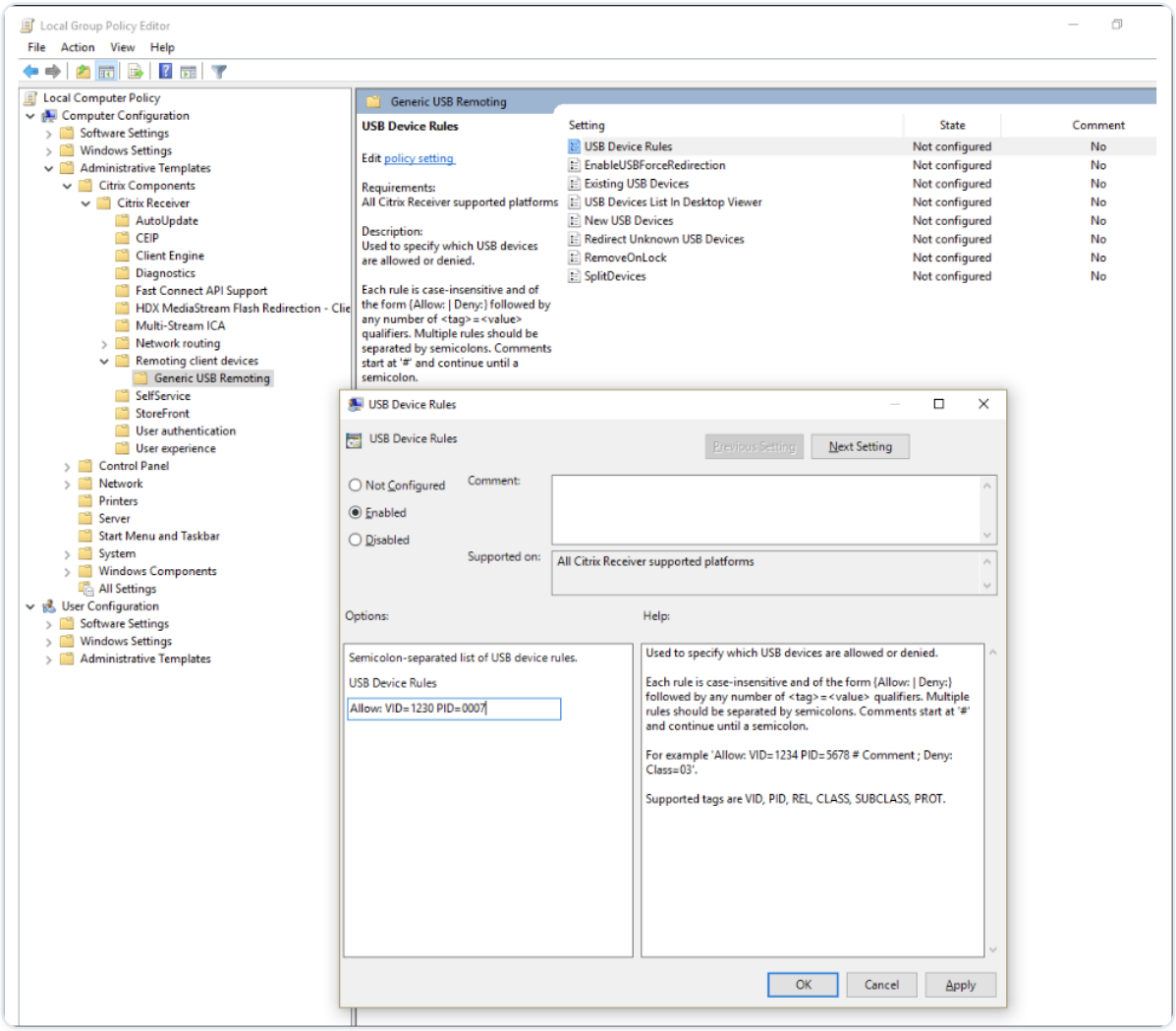
b. デバイスがクライアントエンドポイントで使用されていないことを確認してください。一部のデバイスはクライアントエンドポイントにもドライバーのインストールが必要であり、これがセッションでのリダイレクトを妨げる可能性があります。

6. クライアントエンドポイントでUSB関連のルールが正しく設定されていることを確認します。

   a. **ウィンドウズ用 CWA：**

      i. クライアントのグループポリシー（これに関する詳細とSSを追加）が適切に設定されており、Studioで設定されたルールと競合しないことを確認します。

      ii. クライアントのレジストリ内のデフォルトのルールを確認します。



`(HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules) are appropriately set and not in conflict with the rules set in Studio and client group policy.`.

b. CWA for Linux - CWA for Linux の問題をトリアージするには、CWA for Linux のUSBドキュメントを参照してください。

c. CWA for Mac - CWA for Mac の問題のトリアージについては、CWA for Mac を参照してください。

注：

- TSVDAでは、オーディオデバイスは、デフォルトでUSBリダイレクトの使用がブロックされています。これらのデバイスを使用する推奨される方法は、最適化されたオーディオVCを使用することです。
- 場合によっては、デバイスを分割するための正しいデバイスリダイレクトルールが設定されていても、USB複合デバイスが自動的に分割されないことがあります。この問題は、デバイスが低電力モードになっているために発生します。このような場合、低電力モードになった子デバイスがデバイスリストに表示されないことがあります。この問題を解決するには、次の回避策を使用できます。
  - セッションを切断し、USBデバイスを挿入し、セッションに再接続します。
  - USBデバイスを抜き差しします。この操作により、デバイスは低電力モードから復帰します。
- 場合によっては、バッテリー寿命を最適化するために、USBバッテリーセーバー設定が有効になっていることがあります。クライアントエンドポイントがスリープ状態になると、USBデバイスが切断されることがあります。このようなシナリオでは、セッションでデバイスを再度表示するために、デバイスを一度切断してから再接続する必要がある場合があります。

イベントログ

管理者は、ユーザーがリダイレクトしようとする不正なデバイスを監視し、適切な措置を講じることができます。以下に、VDAホストのイベントビューアーに記録されるイベントメッセージの一部を示します。これは、リダイレクトが許可されているデバイスと許可されていないデバイスに関するものです。

Id	1000
Name	UsbEventAcceptDevice
Severity	Informational
Facility	System
Text	The Citrix USB Service allows the USB Device with Product ID: %2, Vendor ID: %3, and Device ID: %4 to be remoted.
Comment	This message logs the device info of a device redirected in an HDX session

Id	1001
Name	UsbEventPolicyRejectsDeviceV1
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the legacy “Client USB device redirection rules” policy rule.
Arguments	

Id	1002
Name	UsbEventPolicyRejectsDeviceV2
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules (Version 2)" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the "Client USB device redirection rules (Version 2)" policy rule. For instance, if the studio policy rule allows an approved set of devices and denies all other devices and an end user tries to create a new rule on the client endpoint via group policy, this event will get logged. This message would be indicative of an unauthorized device redirection attempt.
Arguments	

USB診断ツール

`CtxUsbDiagnostics.exe` は、VDA 上のコマンドラインツールであり、Citrix 管理者がクライアントで発生するUSBデバイスのリダイレクト問題を迅速に診断し、解決するのに役立ちます。このユーティリティツールは、HDXセッション内でリダイレクトに失敗しているクライアントに接続されたUSBデバイスに関連する構成の問題をトリアージするために必要な重要な情報を収集します。

```
> **Note :**

>

> Running Command Prompt or Powershell as an administrator is required to
```

```
ensure the tool has the necessary permissions to perform system-level
operations.
```

要件

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
  - ウィンドウズ サーバー 2016 以降
- VDA
  - Windows版: Citrix Virtual Apps and Desktops™ バージョン 2311 以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809以降
- Workspaceアプリ
  - Windows: バージョン 2311以降

このツールは何をしますか?

このツールは現在、以下を提供します。

- SessionID
- VDAデバイスポリシー（Studioで設定されたデバイスルール）
- クライアントデバイスとクライアントデバイスポリシー（デバイスルール）
- デバイスのリスト、それらのリダイレクト状態、および許可または拒否された理由

> **注：**
>
> 管理者は、すべてのアクティブなセッションのデバイス情報を確認できます。

表示される情報

- **シトリックス スタジオ ルール - バージョン1/2**
  - DDCルールは、Studioでのレガシーな「**クライアントUSBデバイスリダイレクトルール**」または「**クライアントUSBデバイスリダイレクトルール（バージョン2）**」ポリシーの使用を示します。このセクションに記載されている情報は、Citrix®管理者が構成したすべてのルールをリストします。



- **クライアントのデフォルトデバイスルール**
  - このセクションには、クライアントのレジストリに設定されているルールがリストされます。



- **デバイス最適化ルール**
  - このセクションには、「クライアントUSBデバイス最適化ルール」で設定されているデバイス最適化ルールが一覧表示されます。



デバイスリスト

このセクションには、クライアントエンドポイントに接続されている各デバイスに関する貴重な情報（ハードウェア情報、リダイレクトされているかどうか、正しいデバイスリダイレクトルールが設定されているかどうかなど）が一覧表示されます。

タグ名	説明
displayName	デバイスの一般的な名前を一覧表示します。
ベンダーID	ベンダーID
プロダクトID	製品ID
インターフェース	複合デバイスが複数の子デバイスに分割されている場合、このサブセクションにはすべてのインターフェイスが一覧表示されます。
InterfaceNum	インターフェイス記述子のインデックスを示します

タグ名	説明
クラス	クラスコード
サブクラス	サブクラスコード
プロトコル	プロトコル
redirectionState	**Local** は、デバイスがICA®セッションでリダイレクトされていないことを示します。**ThisSession** は、デバイスがICAセッションでリダイレクトされていることを示します。**OtherSession** は、デバイスが別のICAセッションでリダイレクトされていることを示します。
optiEnabled	**true** は、デバイスが最適化されていることを示します。**false** は、デバイスが最適化されておらず、データ転送がUSB仮想チャネル経由で行われることを示します。
deviceType	**generic** は、デバイスに最適化された仮想チャネルがなく、トラフィックがUSB仮想チャネルを介して流れていることを示します。**optimized** は、デバイスに関連付けられたデータ転送が専用の仮想チャネルを介して行われていることを意味します。
isDenied	**true** は、管理者が設定したポリシー規則によりデバイスがリダイレクトされないことを示します。`false` は、適用されたポリシーによりデバイスがリダイレクトされることを示します。
denyRule	このフィールドは、**isDenied** が `true` に設定されている場合に役立ちます。これは、デバイスがリダイレクトされない原因となっている、ポリシーで設定された特定の規則を管理者に伝えます。

レガシーUSBリダイレクトの構成

バージョン2212より古いコンポーネントを使用している場合、またはLinux版CWAを使用している場合は、このガイドに従って環境でUSBリダイレクトを構成してください。

汎用USBリダイレクトの有効化

1. **Citrix Web Studio™ポリシー**を開き、**ポリシー**タブをクリックします。
2. **ポリシーの作成**をクリックし、**ICA® > USBデバイスポリシー**を展開します。
3. **クライアントUSBデバイスリダイレクト**ポリシー設定を編集します。
4. **許可**を選択し、**保存**をクリックします。

USBリダイレクトポリシー規則の作成

ユーザーがUSBデバイスをVirtual Desktopにリダイレクトしようとすると、一致が見つかるまで各USBポリシー規則に対して順番にチェックされます。いずれかのデバイスに対する最初の一致が最終と見なされます。最初の一致が許可規則である場合、一致したデバイスは仮想デスクトップにリダイレクトが許可されます。最初の一致が拒否規則である場合、一致したデバイスはローカルデスクトップでのみ利用可能です。一致が見つからない場合は、デフォルトの規則が使用されます。

Studioコンソールで適切なデバイス規則を設定する:

1. **Citrix Web Studioポリシー**を開き、**ポリシー**タブをクリックします。
2. **ポリシーの作成**をクリックし、**ICA > USBデバイスポリシー**を展開します。
3. **クライアントUSBデバイスリダイレクト規則**ポリシー設定を編集します。
4. リダイレクトする必要がある各USBデバイスについて、説明に記載されている例に基づいて値を設定し、をクリックします。 例： Allow: VID=056A PID=00A4 #STU-430 Deny: Class=08 subclass=05 # Mass Storage

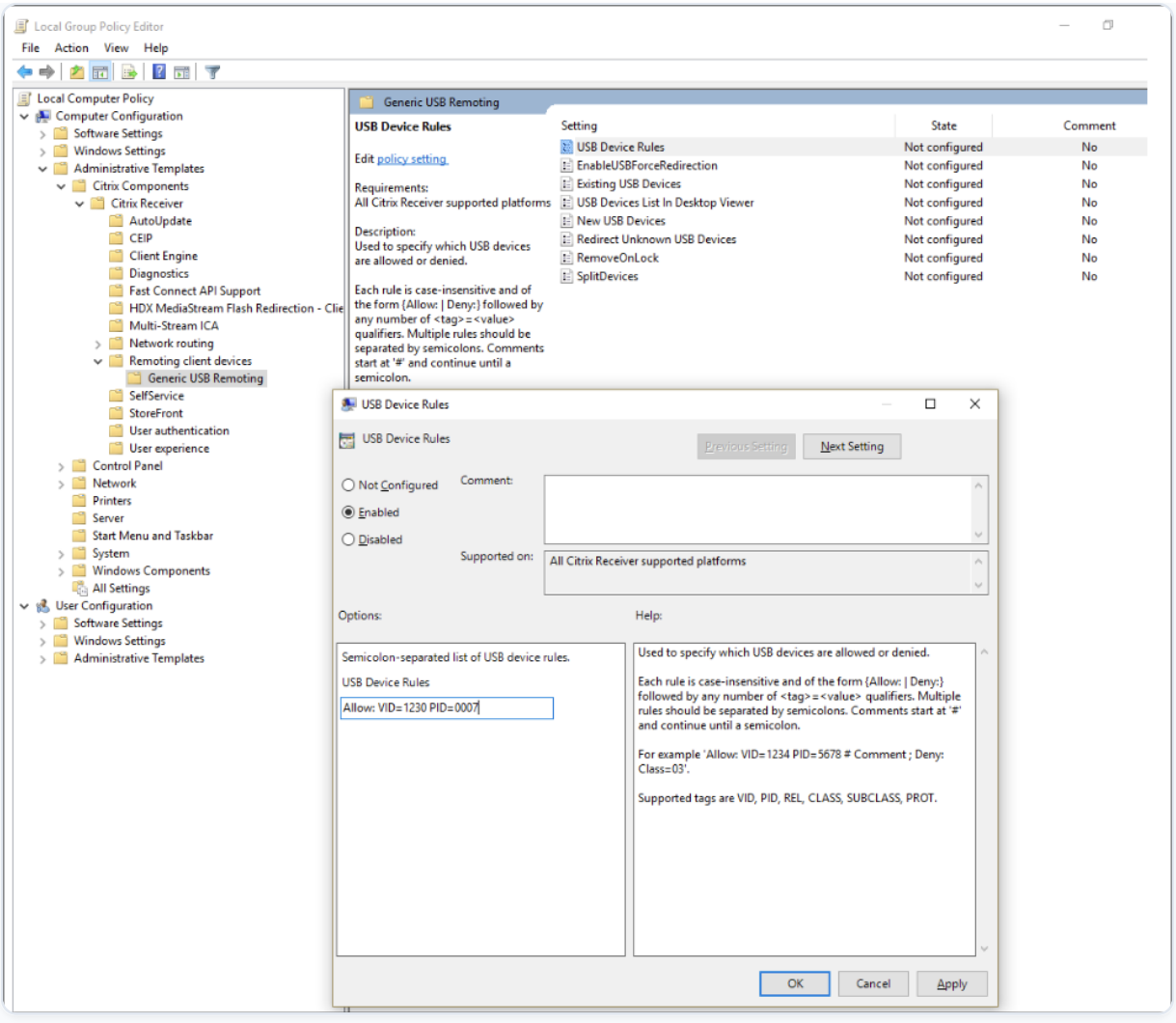
> **注:**
>
> Citrix®管理者が「既定値を使用」をチェックして「保存」をクリックすると、既定のルールはVDAの次のレジストリで見つけることができます。
>
> **注意:**

> レジストリエディターを使用する前に、この記事の最後にある免責事項を参照してください。 `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

クライアントで適切なGPOを設定する:

1. **ローカル グループ ポリシー エディター**を開き、**管理用テンプレート > Citrix Components > Citrix Receiver™ > Remoting client devices > Generic USB Remoting**に移動します。
2. **USBデバイスルール**設定を開き、**有効**に設定します。次の例のようにUSBデバイスルールを追加します。 Allow: VID=1230 PID=0007ルールは、ベンダーID 1230および製品ID 0007のデバイスを許可します。

> **注:**
>
> 特定のデバイスをデバイスルールリストの最上位に配置する必要がある場合は、Allow: VID=xxxx PID=xxxxルールを使用します。



> **注:**
>
> USBViewやConnectionツールバーなどのツールを使用して、VIDやPIDなどのデバイスの詳細を特定できます。

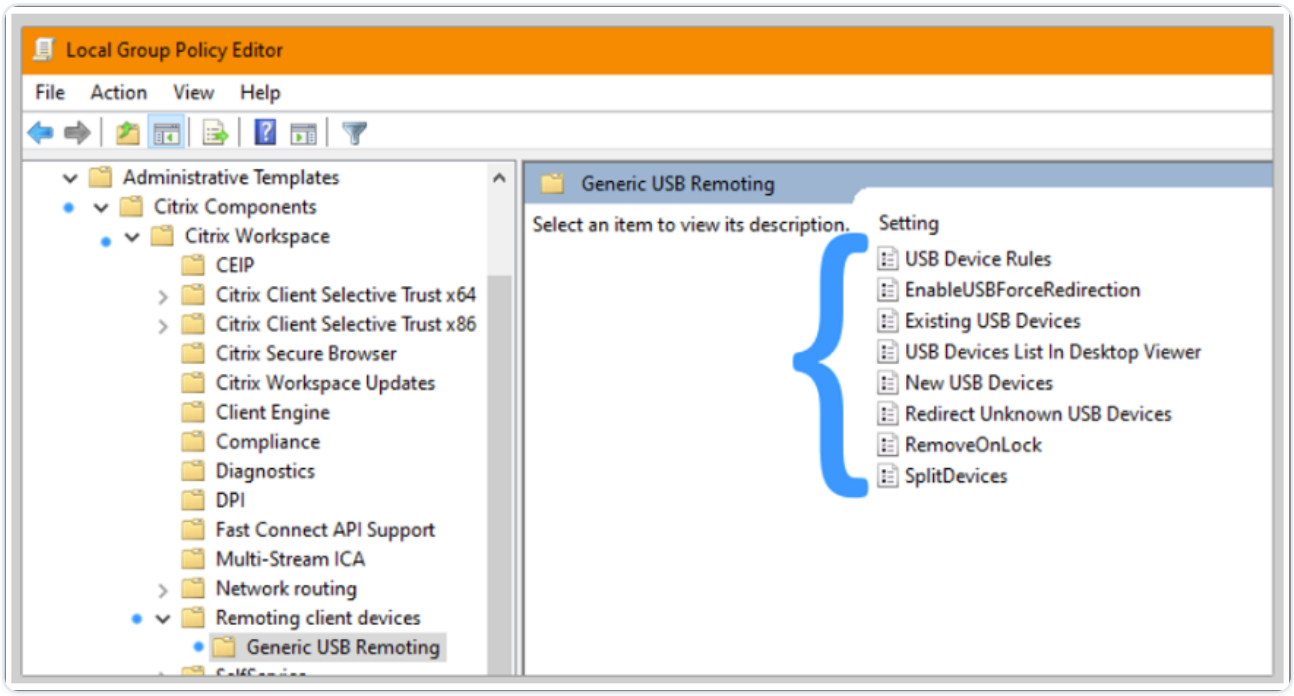
USBデバイスの自動リダイレクトを構成する

USBサポートが有効になっている場合、USBデバイスは自動的にリダイレクトされます。また、USBユーザー設定はUSBデバイスを自動的に接続するように設定されています。すべてのUSBデバイスをリダイレクトすることが常に最善とは限りません。ユーザーは、自動的にリダイレクトされないUSBデバイスリストからデバイスを明示的にリダイレクトできます。USBデバイスがリストされたりリダイレクトされたりするのを防ぐには、クライアントエンドポイントでDeviceRulesポリシー設定を使用します。

このポリシーは、GPO、クライアント側レジストリ、Citrix Workspace™ Preferences、またはCDViewerのタブを使用してクライアントで設定できます。これらの方法はすべて以下に説明されています。

クライアントでGPOを使用する:

1. 「**ローカル グループ ポリシー エディター**」を開き、「**管理用テンプレート > Citrix コンポーネント > Citrix Receiver > クライアント デバイスのリモート処理 > 汎用 USB リモート処理**」に移動します。
2. 「**新しい USB デバイス**」を開き、「**有効**」を選択して「**OK**」をクリックします。
3. 「**既存の USB デバイス**」を開き、「**有効**」を選択して「**OK**」をクリックします。

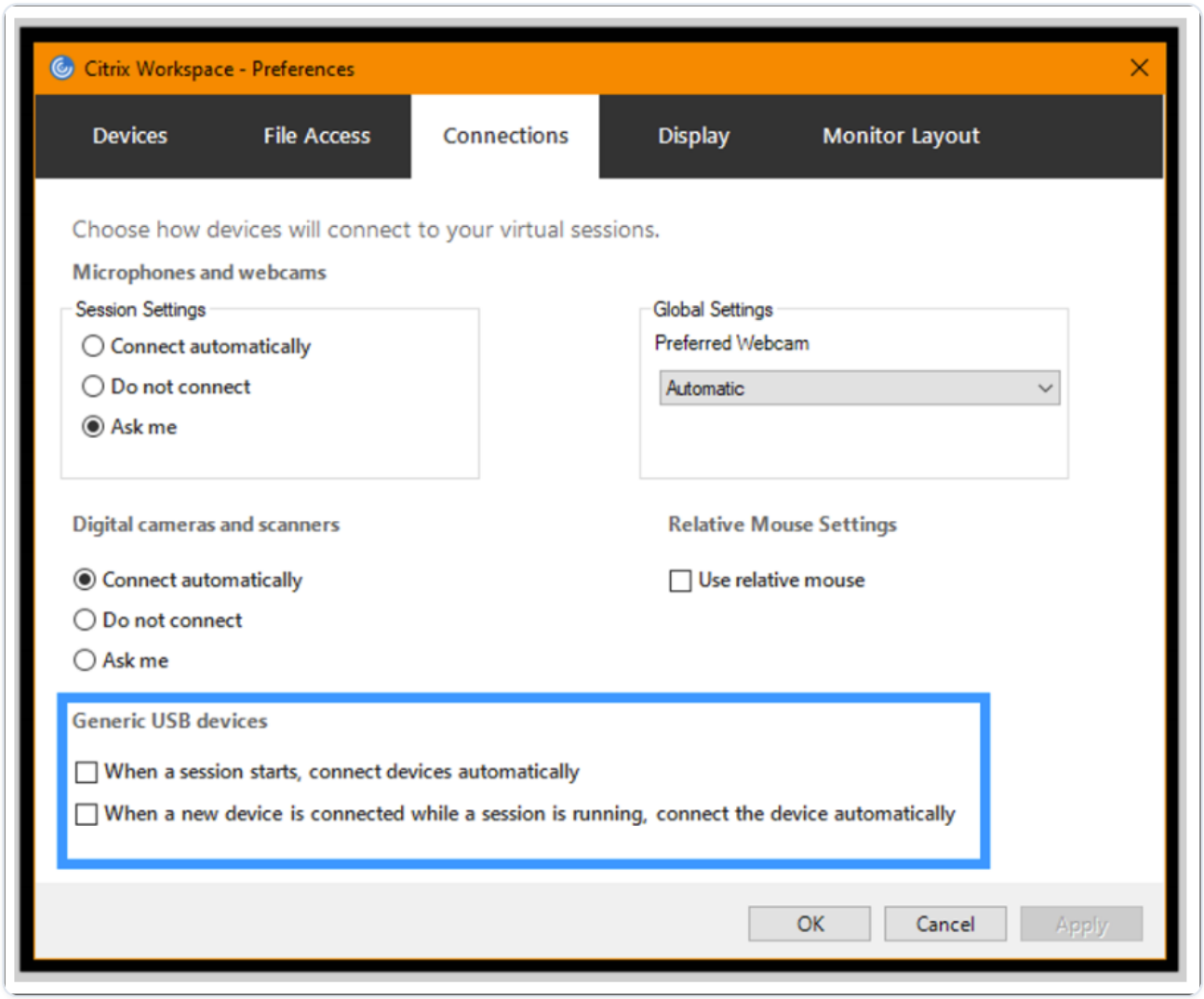


Citrix Connection Center を使用する:

1. Citrix Workspace の**設定 > 接続** に移動します。
2. 次のオプションが選択されていることを確認します。
    a. セッション開始時にデバイスを自動的に接続する
    b. セッション実行中に新しいデバイスが接続された場合、そのデバイスを自動的に接続する。
3. 「**OK**」をクリックします。

「**CDViewer 接続ツールバーの使用:**」:

1. セッション開始後、「**CDViewer**」ドロップダウンをクリックし、「**Citrix Workspace Preferences > Connections**」タブを選択します。
2. 次のオプションが選択されていることを確認します。
    a. セッション開始時にデバイスを自動的に接続する
    b. セッション実行中に新しいデバイスが接続された場合、そのデバイスを自動的に接続する。
3. 「**適用**」と「**OK**」をクリックしてポリシーを保存します。



クライアントベースの構成の場合、レジストリキーは次の場所にあるクライアントデバイスに設定されます。

> **注意：**
>
> レジストリエディターを使用する前に、この記事の最後にある免責事項を参照してください。 `HKLM\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB`

異なるデバイスルールを持つUSBリダイレクトを使用して2つ以上のデバイスを構成する

複数のデバイスを異なるデバイスルールでHDX™セッション内にリダイレクトできます。管理者は、あるデバイスを自動的にリダイレクトし、別のデバイスをエンドユーザーがリダイレクトするオプションを提供したい場合があります。以下に、異なるルールで2つのデバイスを構成する手順を示します。

1. **Citrix Web Studio**で**クライアントUSBデバイスリダイレクト**ポリシー設定を有効にします。

2. クライアント側のGPOで**USBデバイスルール**設定を編集します。

    a. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrixコンポーネント > Citrix Receiver > クライアントデバイスのリモート処理 > Generic USB Remoting**に移動します。

    b. **USBデバイスルール設定**を開き、この設定を有効にします。この例のようにUSBデバイスルールを追加します。**Allow: VID=0911 PID=0c1c**ルールは、**ベンダーID 0911**および**製品ID 0c1c**を持つデバイスを許可しますが、自動的にはリダイレクトされません。**Connect: VID=06A8 PID=0043**ルールは、ステップ3で述べられている自動リダイレクトポリシーが設定されている場合、**ベンダーID 06A8**および**製品ID 0043**を持つデバイスを自動的にリダイレクトします。

    c. **Allow**: VID=0911 PID=0c1c #Phillips スピーチマイク.

    d. **Connect**: VID=06A8 PID=0043 class=03 # Topaz HSB シグネチャパッド

3. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrixコンポーネント > Citrix Receiver > クライアントデバイスのリモート処理 > Generic USB Remoting**に移動します。
4. **新しいUSBデバイス**を開き、**有効**を選択して、**OK**をクリックします。
5. 「**既存のUSBデバイス**」を開き、「**有効**」を選択して、「**OK**」をクリックします。

これらの設定が構成されると、Topaz署名パッドはHDXセッション内に自動的にリダイレクトされ、Phillipsスピーチマイクをセッションにリダイレクトするには、追加のエンドユーザー操作（接続センターまたはCD Viewerのデバイスタブでリダイレクトオプションを選択）が必要になります。

> **注:**
>
> 上記の手順2と3の設定は、クライアント側のレジストリ値 **DeviceRules** (GenericUSBキー (HKLM\SOFTWARE\Wow6432Citrix\ICA Client\GenericUSB) の下) に直接適用できますが、これは推奨される方法ではありません。

汎用USBリダイレクトとクライアントドライブに関する考慮事項

HDX™テクノロジーは、ほとんどの一般的なUSBデバイスに対して**最適化されたサポート**を提供します。最適化されたサポートは、WAN経由でパフォーマンスと帯域幅の効率を向上させ、ユー

ザーエクスペリエンスを改善します。最適化されたサポートは、特に高遅延またはセキュリティに敏感な環境において、通常は最良の選択肢です。

HDXテクノロジーは、最適化されたサポートがない、または不適切な特殊なデバイスに対して**汎用USBリダイレクト**を提供します。例を次に示します。

- USBデバイスに、マウスやWebカメラのボタンが多いなど、最適化されたサポートに含まれない高度な機能がある場合。
- ユーザーが最適化されたサポートに含まれない機能を必要とする場合。
- USBデバイスが、テストおよび測定機器や産業用コントローラーなどの特殊なデバイスである場合。
- アプリケーションがUSBデバイスとしてデバイスに直接アクセスする必要がある場合。
- USBデバイスにWindowsドライバーしか利用できない場合。たとえば、スマートカードリーダーには、Android版Citrix Workspace™アプリ用のドライバーがない場合があります。
- Citrix Workspaceアプリのバージョンが、この種類のUSBデバイスに対して最適化されたサポートを提供しない場合。

汎用USBリダイレクトでは：

- ユーザーはユーザーデバイスにデバイスドライバーをインストールする必要がありません。
- USBクライアントドライバーはVDAマシンにインストールされます。

重要:

- 汎用USBリダイレクトは、最適化されたサポートと組み合わせて使用できます。汎用USBリダイレクトを有効にする場合は、汎用USBリダイレクトと最適化されたサポートの両方について、CitrixのUSBデバイスポリシー設定を構成してください。
- クライアントUSBデバイス最適化ルールのCitrixポリシー設定は、特定のUSBデバイスに対する汎用USBリダイレクトの特定のポリシー設定です。ここで説明されている最適化されたサポートには適用されません。

USBデバイスのパフォーマンスに関する考慮事項

ネットワークの遅延と帯域幅は、一部の種類のUSBデバイスで汎用USBリダイレクトを使用する場合、ユーザーエクスペリエンスとUSBデバイスの動作に影響を与える可能性があります。たとえ

ば、タイミングに敏感なデバイスは、高遅延で低帯域幅のリンクでは正しく動作しない場合があります。可能な場合は、代わりに最適化されたサポートを使用してください。

一部のUSBデバイスは、使用可能にするために高帯域幅を必要とします。たとえば、3Dマウス（通常、高帯域幅を必要とする3Dアプリで使用）などです。帯域幅を増やすことができない場合は、帯域幅ポリシー設定を使用して他のコンポーネントの帯域幅使用量を調整することで、問題を軽減できる場合があります。詳細については、「クライアントUSBデバイスリダイレクトの帯域幅ポリシー設定」および「マルチストリーム接続ポリシー設定」を参照してください。

USBデバイスのセキュリティに関する考慮事項

一部のUSBデバイスは、スマートカードリーダー、指紋リーダー、署名パッドなど、本質的にセキュリティに敏感です。USBストレージデバイスなどの他のUSBデバイスは、機密データである可能性のあるデータを送信するために使用できます。

USBデバイスはマルウェアを配布するためによく使用されます。Citrix WorkspaceアプリおよびCitrix Virtual Apps and Desktops™の設定により、これらのUSBデバイスからのリスクを軽減できますが、排除することはできません。この状況は、汎用USBリダイレクトが使用されているか、最適化されたサポートが使用されているかに関わらず適用されます。

重要:

セキュリティに敏感なデバイスとデータについては、常にHDX接続を保護してください。クライアントとVDA間の通信を参照してください。

必要なUSBデバイスのサポートのみを有効にしてください。このニーズを満たすように、汎用USBリダイレクトと最適化されたサポートの両方を構成してください。

USBデバイスを安全に使用するためのガイダンスをユーザーに提供してください。

- 信頼できる情報源から入手したUSBデバイスのみを使用してください。
- インターネットカフェなど、開かれた環境でUSBデバイスを放置しないでください。
- 複数のコンピューターでUSBデバイスを使用するリスクを説明してください。

USBマスストレージデバイスのセキュリティ制御

USBマスストレージデバイスには、最適化されたサポートが提供されます。このサポートは、Citrix Virtual Apps and Desktopsのクライアントドライブマッピングの一部です。ユーザーがログオンすると、ユーザーデバイス上のドライブが仮想デスクトップ上のドライブ文字に自動的にマッピングされます。ドライブは、マッピングされたドライブ文字を持つ共有フォルダーとして表示されます。クライアントドライブマッピングを構成するには、**クライアントリムーバブルドライブ**設定を使用します。この設定は、ICAポリシー設定のファイルリダイレクトポリシー設定セクションにあります。

USB大容量記憶装置では、クライアントドライブマッピングまたは汎用USBリダイレクト、あるいはその両方を使用できます。Citrix®ポリシーを使用してこれらを制御します。主な違いは次のとおりです。

機能	クライアントドライブマッピング	汎用USBリダイレクト
デフォルトで有効	はい	いいえ
読み取り専用アクセスを構成可能	はい	いいえ

注:

USBリダイレクトは、たとえば50 Kbpsのような低帯域幅接続でもサポートされています。ただし、大きなファイルのコピーは機能しません。

クライアントドライブマッピング

クライアントドライブマッピングにより、クライアントエンドポイント上のストレージドライブがCitrix HDX™セッション内で利用可能になり、ファイルやフォルダーをクライアントからセッションホストへ、またはその逆に転送できます。この機能は、読み取りおよび書き込みの両方の権限でデフォルトで有効になっています。ユーザーがマップされたクライアントデバイス上のファイルやフォルダーを追加または変更できないようにするには、**読み取り専用クライアントドライブアクセス**ポリシー設定を有効にします。この設定をポリシーに追加する際は、**クライアントドライブリダイレクト**設定が**許可**に設定されており、ポリシーにも追加されていることを確認してください。

セキュリティ上の予防措置として、エンドポイントドライブはデフォルトで実行権限なしでマップされます。ユーザーがマップされたクライアントドライブから直接実行可能ファイルを実行できるようにするには、セッションホストで**ExecuteFromMappedDrive**レジストリ値を編集します。詳細については、**レジストリで管理されるHDX機能**セクションのマップされたクライアントドライブを参照してください。

要件

CDMを使用するための要件は次のとおりです。

Citrix コントロールプレーン

- シトリックス バーチャル アプリケーションズ アンド デスクトップ™ 1912以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1809以降
  - Windows Server 2016 以降のバージョン
  - Linux: Linux VDAのシステム要件を参照してください
- VDA
  - Windows: Citrix Virtual Apps and Desktops 1912 以降のバージョン
  - Linux: Linux VDAのドキュメントを参照してください。

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Linux: Workspace app for Linuxのシステム要件を参照してください。

関連ポリシー

CDM設定については、ポリシー設定リファレンスセクションを参照してください。

ダブルホップシナリオ

CDMはダブルホップシナリオでサポートされています。デフォルトでは、クライアントエンドポイントのドライブはセカンドホップセッションにマップされ、ファーストホップのドライブは利用できません。ただし、クライアントエンドポイントのドライブの代わりに、ファーストホップのドライブがセカンドホップセッションにマップされるように設定することも可能です。

この機能を構成するには、以下のレジストリ値を編集します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientDrive\
- 値の名前: NativeDriveMapping
- 値の型: REG_SZ
- 値のデータ:
  - True - ファーストホップセッションのドライブをセカンドホップセッションにマップします
  - 無効 - セカンドホップセッションでクライアントエンドポイントのドライブをマップします

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

モバイルデバイスとタッチスクリーンデバイス

Citrix Virtual Apps and Desktops™ を使用すると、ユーザーは公開されたアプリケーションやデスクトップにモバイルおよびタッチスクリーンクライアントデバイスからアクセスできます。

要件

Citrix® コントロールプレーン

- シトリックス バーチャルアプリおよびデスクトップ 1912 以降

- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1903 以降
  - Windows 11 21H2 以降
- VDA
  - Windows 環境では、Citrix Virtual Apps and Desktops バージョン 7.15 以降が必要です。

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
- Windows 用 Citrix Workspace™ アプリ バージョン 1808 以降

Windows Continuum を使用したタッチスクリーンデバイスのタブレットモード

Continuum は、クライアントデバイスの使用方法に適応する Windows 10 の機能です。VDA は、タッチ対応クライアントでキーボードまたはマウスの存在を検出すると、クライアントをデスクトップモードにします。キーボードまたはマウスが存在しない場合、VDA はクライアントをタブレット/モバイルモードにします。この検出は、セッションの接続時および再接続時、ならびにセッション中にキーボードまたはマウスが接続または切断されたときに発生します。

この機能はデフォルトで有効になっています。この機能を無効にするには、ポリシー設定 タブレットモード切り替えポリシー設定を構成します。

上記のタッチスクリーンデバイスの要件に加えて、Windows Continuumには以下が必要です。

XenServer (旧製品名: Citrix Hypervisor™)

- Citrix Hypervisor 8.2 またはそれ以降
- ラップトップ/タブレットの切り替えを許可するには、XenServer CLI コマンドを実行します。
  xe vm-param-set uuid=\<VM_UUID\> platform:acpi_laptop_slate=1

> **重要:**

> メタデータ設定を変更した後に既存のマシンカタログのベースイメージを更新しても、以前にプロビジョニングされた VM には影響しません。XenServer VM のベースイメージを変更した後、カタログを作成し、ベースイメージを選択して、新しい Machine Creation Services™ (MCS) マシンをプロビジョニングします。

セッションホスト

- オペレーティングシステム
  - Windows 10 1903 以降
  - Windows 11 21H2 以降
- VDA
  - Windows: バージョン 7.16 以降
  - **現在のオペレーティングシステム構成の制限により、ユーザーは最初のICA®セッションを開始してVDAを再起動した後、ドロップダウンメニューから以下のオプションを設定する必要があります。**
    - **設定 > システム > タブレットモード**
      - 自分のハードウェアに適したモードを使用する
      - 確認せずに常に切り替える



タブレットモードは、タッチスクリーンにより適したユーザーインターフェースを提供します。

- わずかに大きいボタン。
- スタート画面と起動するすべてのアプリが全画面で開きます。
- タスクバーに「戻る」ボタンが含まれています。
- タスクバーからアイコンが削除されます。

ファイルエクスプローラーにアクセスできます。



Windows 10は、この更新されたBIOSに基づいてターゲット仮想マシンにGPIOドライバーをロードします。これは、仮想マシン内でタブレットモードとデスクトップモードを切り替えるために使用されます。

Citrix Workspaceアプリ for HTML5は、Windows Continuum機能をサポートしていません。

デスクトップモードは、PCとキーボード、マウスを使用するのと同じ方法で操作できる、従来のユーザーインターフェイスを提供します。

マイクロソフト Surface Pro および Surface Book ペン

Windows Inkベースのアプリケーションで標準のペン機能をサポートしています。サポートには、ポインティング、消去、筆圧、Bluetooth信号、およびオペレーティングシステムのファームウェアとペンモデルに応じたその他の機能が含まれます。たとえば、筆圧は最大4096レベルに達することができます。この機能はデフォルトで有効になっています。

ペン機能のサポートに関する要件は次のとおりです。

Citrixコントロールプレーン

- シトリックス Virtual Apps and Desktops 1903以降
- シトリックス DaaS

セッションホスト

- オペレーティングシステム
  - Windows 10 1809以降
  - Windows 11 21H2 以降
- VDA
  - Windows 環境では、Citrix Virtual Apps and Desktops 1903 以降が必要です。

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809以降
  - Windows 11 21H2以降
- Windows向けCitrix Workspaceアプリ バージョン1902以降

Windows Ink とペンの機能のデモンストレーションについては、このグラフィックをクリックしてください。



この機能を無効または有効にするには、レジストリで管理される機能の一覧にあるMicrosoft Surface ProおよびSurface Bookペンを参照してください。

既知の問題

ペンサポートに関する既知の問題は次のとおりです。

- Windows Server 2k22のOSの制限により、2k22サーバーアプリケーションまたはデスクトップに接続している場合、ユーザーはコントロールパネルでペンのショートカットを設定したり、ペン/インクの設定を調整したりすることはできません。
- OSの制限により、ペン対応のWindows 11クライアントからペンのショートカットが認識されません。

シリアルポート

ほとんどの新しいPCには、内蔵のシリアル（COM）ポートがありません。USBコンバーターを使用すると、ポートを簡単に追加できます。シリアルポートに適したアプリケーションには、センサー、コントローラー、古いチェックリーダー、パッドなどがよく含まれます。一部のUSB仮想COMポートデバイスは、Windowsが提供するドライバー（usbser.sys）の代わりに、ベンダー固有のドライバーを使用します。これらのドライバーを使用すると、USBデバイスの仮想COMポートを強制的に設定できるため、異なるUSBソケットに接続しても変更されません。これは、**デバイスマネージャー > ポート (COM と LPT) > プロパティ**から、またはデバイスを制御するアプリケーションから行うことができます。

クライアントCOMポートマッピングを使用すると、ユーザーのエンドポイントのCOMポートに接続されたデバイスを仮想セッション中に使用できます。これらのマッピングは、他のネットワークマッピングと同様に使用できます。

各COMポートには、オペレーティングシステム内のドライバーがCOM1やCOM2などのシンボリックリンク名を割り当てます。アプリケーションは、そのリンクを使用してポートにアクセスします。

> **重要:**
>
> デバイスがUSBを直接使用してエンドポイントに接続できるからといって、汎用USBリダイレクトを使用してリダイレクトできるとは限りません。一部のUSBデバイスは仮想COMポートとして機能し、アプリケーションは物理シリアルポートと同じ方法でアクセスできます。オペレーティングシステムはCOMポートを抽象化し、ファイル共有のように扱うことができます。仮想COMの2つの一般的なプロトコルは、CDC ACMまたはMCTです。RS-485ポート

を介して接続すると、アプリケーションがまったく機能しない場合があります。RS-485をCOMポートとして使用するには、RS-485-to-RS232コンバーターを入手してください。 **重要:**

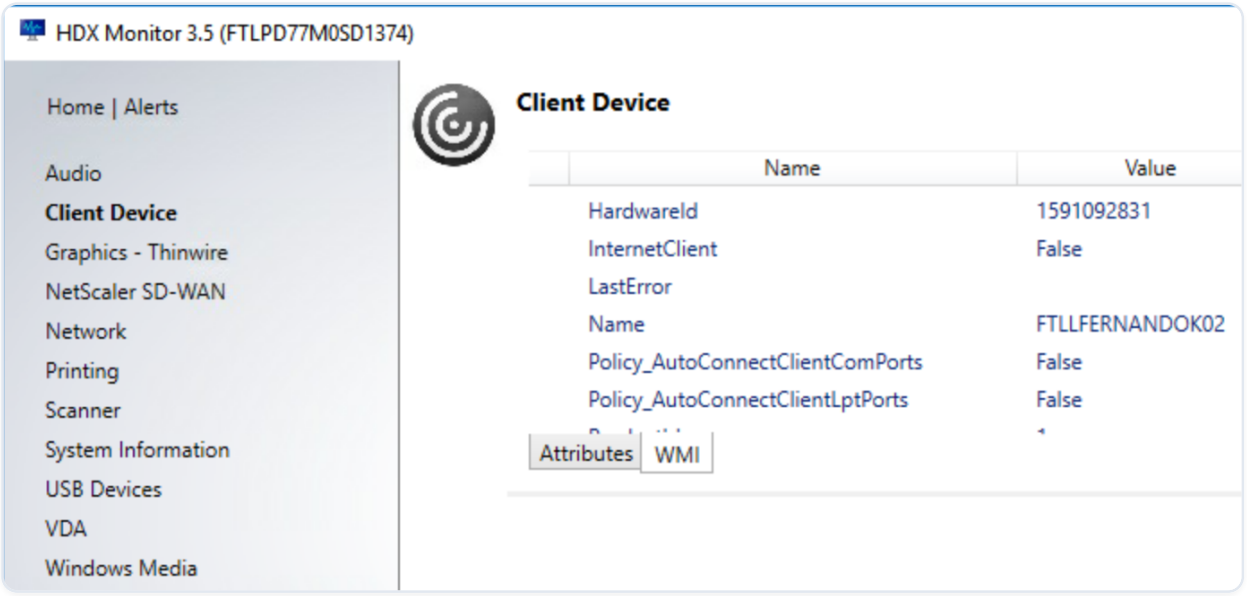
一部のアプリケーションは、デバイス（署名パッドなど）がクライアントワークステーションのCOM1またはCOM2に接続されている場合にのみ、一貫して認識します。

クライアントCOMポートをサーバーCOMポートにマッピングする

クライアントCOMポートをCitrix®セッションにマッピングするには、次の3つの方法があります。

- Studioポリシー。ポリシーの詳細については、「ポートリダイレクトポリシー設定」を参照してください。
- VDAコマンドプロンプト。
- リモートデスクトップ（ターミナルサービス）構成ツール。

1. **クライアントCOMポートリダイレクト**および**クライアントCOMポートの自動接続Studio**ポリシーを有効にします。適用後、一部の情報はHDX™ Monitorで利用できます。



2. **クライアントCOMポートの自動接続**がポートのマッピングに失敗した場合は、手動でポートをマッピングするか、ログオンスクリプトを使用できます。VDAにログオンし、コマンドプロンプトウィンドウで次のように入力します。

   NET USE COMX: `\CLIENT\COMZ`:

   または

NET USE COMX: `\CLIENT\CLIENTPORT:COMZ`:

X は VDA 上の COM ポートの番号です (ポート 1 から 9 までがマッピングに利用可能です)。**Z** はマッピングするクライアント COM ポートの番号です。

操作が成功したことを確認するには、VDA コマンドプロンプトで **NET USE** と入力します。表示されるリストには、マップされたドライブ、LPT ポート、およびマップされた COM ポートが含まれます。

Net use コマンドの画像(/en-us/citrix-virtual-apps-desktops/2411/media/net-use-command.png)

3. 仮想デスクトップまたはアプリケーションでこの COM ポートを使用するには、ユーザーデバイスアプリケーションをインストールし、マップされた COM ポート名を指定します。たとえば、クライアント上の COM1 をサーバー上の COM3 にマップする場合、VDA に COM ポートデバイスアプリケーションをインストールし、セッション中に COM3 を指定します。このマップされた COM ポートは、ユーザーデバイス上の COM ポートと同様に使用します。

重要:

COM ポートマッピングは TAPI と互換性がありません。Windows Telephony Application Programming Interface (TAPI) デバイスをクライアント COM ポートにマップすることはできません。TAPI は、アプリケーションがデータ、FAX、音声通話の電話機能を制御するための標準的な方法を定義します。TAPI は、ダイヤル、応答、通話終了などのシグナリングを管理します。また、保留、転送、会議通話などの付加サービスも管理します。

トラブルシューティング

1. Citrix をバイパスして、エンドポイントからデバイスに直接アクセスできることを確認してください。ポートが VDA にマップされていない間は、Citrix セッションに接続されていません。デバイスに付属のトラブルシューティング手順に従い、まずローカルで動作することを確認してください。 デバイスがシリアル COM ポートに接続されている場合、ここに示されているハイブにレジストリキーが作成されます: トラブルシューティングの画像(/en-us/citrix-virtual-apps-desktops/2411/media/troubleshoot2.png)

   この情報は、コマンドプロンプトで **chgport /query** を実行することでも確認できます。

   コマンドプロンプトからのトラブルシューティングの画像(/en-us/citrix-virtual-apps-desktops/2411/media/troubleshoot1.png)

デバイスのトラブルシューティング手順が利用できない場合は、PuTTY セッションを開いてみてください。**Session** を選択し、**Serial line** で COM ポートを指定します。

PuTTY セッションによるトラブルシューティングの画像(/en-us/citrix-virtual-apps-desktops/2411/media/troubleshoot3.png)

ローカルコマンドウィンドウで **MODE** を実行できます。出力には、使用中のCOMポートと、PuTTYセッションで必要となるBaud/Parity/Data Bits/Stop Bitsが表示される場合があります。PuTTY接続が成功した場合は、**Enter** を押してデバイスからのフィードバックを確認します。入力した文字が画面に繰り返されたり、応答されたりする場合があります。この手順が失敗した場合、仮想セッションからデバイスにアクセスすることはできません。

2. ローカルCOMポートをVDAにマップし（ポリシーまたは **NET USE COMX: \\\CLIENT\COMZ:** を使用）、前の手順と同じPuTTY手順を繰り返しますが、今回はVDA PuTTYから実行します。PuTTYがエラー **Unable to open connection to COM1. Unable to open serial port** を表示しない場合、別のデバイスがCOM1を使用している可能性があります。
3. **chgport /query** を実行します。VDA上の組み込みWindowsシリアルドライバーが \Device\Serial0をVDAのCOM1ポートに自動割り当てしている場合は、次の手順を実行します。 A. VDAでCMDを開き、**NET USE.** と入力します。

   B. VDA上の既存のマッピング（例: COM1）を削除します。

   NET USE COM1 /DELETE

   C. デバイスをVDAにマッピングします。

   NET USE COM1: `\CLIENT\COM3` :

   D. VDA上のアプリケーションをCOM3に指定します。

   最後に、ローカルCOMポート（例: COM3）をVDA上の別のCOMポート（COM1以外、例: COM3）にマップしてみてください。アプリケーションがそれを指していることを確認してください: **NET USE COM3: \\\CLIENT\COM3**
4. ポートがマップされていることが確認でき、PuTTYは動作しているもののデータが通過しない場合、それは競合状態である可能性があります。アプリケーションがマップされる前にポートに接続して開いてしまい、マップできないようにロックしている可能性があります。次のいずれかを試してください。

   - 同じサーバーで公開されている2番目のアプリケーションを開きます。ポートがマップされるまで数秒待ってから、ポートを使用しようとする実際のアプリケーションを開きます。

- Studioではなく、Active Directoryのグループポリシーエディターから COMポートリダイレクトポリシーを有効にします。これらのポリシーは **Client COM port redirection** と **Auto connect client COM ports** です。この方法で適用されたポリシーは、Studioポリシーよりも前に処理され、COMポートが確実にマップされるようにします。CitrixポリシーはVDAにプッシュされ、次の場所に保存されます: `HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`
- ユーザーにこのログオンスクリプトを使用するか、アプリケーションを公開する代わりに、まずVDA上のマッピングを削除し、仮想COMポートを再マッピングしてからアプリケーションを起動する.batスクリプトを公開します。

@echo off NET USE COM1 /delete NET USE COM2 /delete NET USE COM1: `\CLIENT\COM1`: NET USE COM2: `\CLIENT\COM2`: MODE COM1: BAUD=1200 (または必要な値を指定) MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (または必要な値を指定) START `C:\Program Files\<Your Software Path>\<your_software.exe>`

5. SysinternalsのProcess Monitorは、最後の手段となるツールです。VDAでこのツールを実行する際、COM3、picaser.sys、CdmRedirectorなどのオブジェクト、特に\<your_app\>.exeを見つけてフィルターします。エラーは「Access Denied」または類似の形で表示される場合があります。

特殊キーボード

Bloombergキーボード

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

Citrix Virtual Apps and Desktops™は、Bloombergモデル5、モデル4 Starboardキーボード（およびそれ以前のモデル3）をサポートしています。このキーボードにより、金融業界のお客様は、キーボードの特殊機能を使用して金融市場データにアクセスし、迅速に取引を行うことができます。

重要：

Bloombergキーボードは1つのセッションでのみ使用することをお勧めします。複数の同時セッション（1つのクライアントから複数のセッション）でキーボードを使用することはお勧めしません。

Bloombergキーボードは、複数のUSBデバイスを1つの物理シェルに収めたUSB複合デバイスです。

- キーボード。
- 指紋リーダー。
- 音量を上げ下げしたり、スピーカーとマイクをミュートしたりするキーを備えたオーディオデバイス。このデバイスには、オンボードスピーカー、マイク、およびマイクとヘッドセット用のジャックが含まれています。
- これらすべてのデバイスをシステムに接続するためのUSBハブ。

要件：

- Citrix Workspace™ app for Windowsが接続するセッションは、USBデバイスをサポートしている必要があります。
- Bloombergキーボードモデル5をサポートするには、Linux版Citrix Workspace app 2207以降が必要です。
- Bloomberg キーボード モデル 5 をサポートするには、Windows 用 Citrix Workspace アプリ 2109 以降が必要です。
- Bloomberg キーボード モデル 3 および 4 をサポートするには、Windows 用 Citrix Workspace アプリ 1808 以降、または Windows 用 Citrix Receiver 4.8 以降が必要です。
- モデル 4 で KVM モード (KVM を介してルーティングされる 1 本を含む 2 本の USB ケーブル) を使用するには、Windows 用 Citrix Workspace アプリ 1808 以降、または Windows 用 Citrix Receiver 4.12 以降が必要です。

Citrix Workspace app for WindowsでのBloombergキーボードの構成については、Bloombergキーボードの構成を参照してください。

Bloombergキーボードのサポートを有効にするには、レジストリを介して管理される機能のリストでBloombergキーボードを参照してください。

サポートを確認する:

Citrix WorkspaceアプリでBloombergキーボードのサポートが有効になっているかを確認するには、Desktop ViewerがBloombergキーボードのデバイスを正しく報告しているかを確認します。

デスクトップのシナリオ:

Desktop Viewer を開きます。Bloomberg キーボードのサポートが有効になっている場合、Desktop Viewer の USB アイコンの下に 3 つのデバイスが表示されます。

Bloomberg 5キーボードの場合:

- Bloomberg LP Bloomberg 生体認証モジュール
- Bloomberg LP Keyboard (2 つのインターフェイスを持つ複合デバイス)
- Bloomberg LP Keyboard Audio (3 つのインターフェイスを持つ複合デバイス)

Bloomberg 3および4キーボードの場合:

- Bloomberg 指紋スキャナー
- Bloomberg キーボードの機能
- Bloomberg LP キーボード 2013

シームレスアプリケーションのみのシナリオ:

Citrix Workspaceアプリの通知領域アイコンから**接続センター**メニューを開きます。Bloombergキーボードのサポートが有効になっている場合、3つのデバイスが**デバイス**メニューに表示されます。

これらの各デバイスのチェックマークは、それらがセッションにリモート接続されていることを示します。

Windows VDAでのダブルホップにおけるキーイベントシーケンス処理のサポート

この機能により、クライアントデバイスが非WindowsでUnicodeモードで動作している場合、Windows Virtual Desktop Agent (VDA) でキーイベントが順次送信されるようになります。これにより、以下のような特定の入力関連の問題が解決されます。

1. RDPをセカンドホップとするダブルホップシナリオ。

    - ドイツ語キーボードレイアウトを使用している場合、**AltGr**キーを押しながら**q**を押すと、出力として**@**が生成されるはずです。しかし、この機能がない場合、実際の出力は**q**になります。

2. キーショートカット機能

    - Android版Citrix Workspace™ App (CWA) を使用している場合、Windows VDAで**Alt+Tab**ショートカットが常に機能しないことがあります。

この機能を有効にすることで、これらの入力の不整合が解決されます。これにより、正確なキーイベント処理とユーザビリティの向上が保証されます。

この機能はデフォルトで無効になっています。この機能の切り替えは、レジストリ設定の`EnableSendUnicodeKeyQueue`です。

新しいレジストリ`HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\icawd\EnableSendUnicodeKeyQueue` DWORD = 0/1 が使用され、値が1の場合に新しい実装に切り替わります。

デフォルトでは、値は0です。

Windows - キーボードおよびIMEサポートツール

これは、キーボードと入力方式エディターに関する関連する問題を診断できるセルフサービスのコマンドラインツールです。

さまざまなユーザー要件を満たし、プラットフォームの汎用性を提供し、ユーザーにパーソナライズされたニーズを提供するために、キーボードと入力方式エディター (IME) の機能は、VDA と Citrix Workspace™ アプリケーションにおいてさまざまな構成と機能に依存しています。

VDA またはクライアント側での誤った設定は、予期しない入力動作を引き起こす可能性があります。

しかし、Citrix® はいくつかの一般的な使用シナリオに対して推奨設定を提供しており、これらの推奨事項は診断結果にも含まれています。

このツールを使用すると、以下のカテゴリの問題を特定できます。

- **キーボードタイプの不整合:** VDA キーボードタイプとクライアントキーボードタイプをチェックし、不整合があるかどうかを確認します。例えば、VDA が 101 英語キーボードを使用しているのに、クライアントが日本語 106 キーボードを使用している場合などです。この診断は、JP 106/109 キーボードおよび KO 103/106 キーボードの使用事例を対象としています。
- **キーボードレイアウト同期モードの不整合:** キーボードレイアウト同期設定、レジストリ設定、グループポリシーをチェックし、特定の環境における同期モード構成の問題を解決します。

- **クライアントキーボードレイアウトと VDA キーボードレイアウトの不整合:** クライアントキーボードレイアウトが VDA キーボードレイアウトと同じであるかどうかをチェックします。
- **アプリケーションセッションでリモート言語バーが表示されない:** エンドユーザーがアプリケーションセッションを起動し、複数のキーボードレイアウトを使用している場合に、リモート言語バーが表示されているかどうかをチェックします。

このコマンドラインツールは Windows VDA - `CtxKbImeDiagnostics.exe` にホストされています。 コマンドラインインターフェイスは以下のとおりです。

インターフェイス	説明	注
`CtxKbimeDiagnostics`	現在のICA®セッションのみの診断結果を表示	ユーザーが管理者権限を持っている場合、すべてのアクティブなICAセッションの診断を表示します。ユーザーが管理者権限を持っていない場合、現在のユーザーのICAセッションの診断を表示します。
`CtxKbimeDiagnostics [-v]`	現在のセッションの設定情報と診断結果を表示	ユーザーが管理者権限を持っている場合、すべてのアクティブなICAセッションの診断を表示します。
`CtxKbimeDiagnostics [-v] [-s Session_Id]`	このセッションの設定情報と診断結果を表示	
`CtxKbimeDiagnostics [-s Session_Id]`	セッションを指定し、そのセッションの診断結果を表示します	管理者権限は他のICAセッションを照会できます/通常ユーザーは自身のICAセッションのみを照会できます
`CtxKbimeDiagnostics [-s Session_Id] [-v]`	セッションを指定し、そのセッションのすべての設定情報と診断結果を表示します	管理者権限は他のICAセッションを照会できます。通常ユーザーは自身のICAセッションのみを照会できます。
`CtxKbimeDiagnostics [-h]`	サポートされている引数/パラメーターと例を表示	「ヘルプ」インターフェース

インターフェイス	説明	注
`CtxKbimeDiagnostics [-V]`	現在のツールバージョンを表示	

> **注:**
>
> このバージョンでは、クライアントとしてCWA Windowsのみがサポートされています。

Webカメラ

高解像度Webカメラストリーミング

ウェブカメラは、仮想セッション内で実行されているビデオ会議アプリケーションで使用できます。サーバー上のアプリケーションは、サポートされているフォーマットタイプに基づいてウェブカメラのフォーマットと解像度を選択します。セッションが開始されると、クライアントはウェブカメラ情報をサーバーに送信します。ビデオ会議アプリケーションからウェブカメラを選択します。ウェブカメラとアプリケーションの両方が高解像度レンダリングをサポートしている場合、アプリケーションは高解像度を使用します。ウェブカメラの解像度は最大1920x1080までサポートしています。

この機能には、Citrix Receiver for Windowsバージョン4.10以降が必要です。HDXウェブカメラリダイレクトをサポートするCitrix Workspaceアプリプラットフォームのリストについては、Citrix Workspaceアプリの機能マトリックスを参照してください。

高解像度ウェブカメラストリーミングの詳細については、HDXビデオ会議とウェブカメラビデオ圧縮を参照してください。

レジストリキーを使用してこの機能を無効または有効にし、特定の解像度を設定できます。詳細については、レジストリで管理される機能のリストにある高解像度ウェブカメラストリーミングと高解像度ウェブカメラの解像度を参照してください。

グラフィックス

Citrix HDXグラフィックスには、Citrix Virtual Apps and Desktopsからのリッチグラフィックスアプリケーションの配信を最適化する、広範なグラフィックスアクセラレーションおよびエンコーディングテクノロジーが含まれています。これらのグラフィックテクノロジーは、グラフィックスを多用する仮想アプリケーションをリモートで操作する際に、物理デスクトップを使用するのと同じエクスペリエンスを提供します。

グラフィックスレンダリングには、ソフトウェアまたはハードウェアを使用できます。ソフトウェアレンダリングには、ソフトウェアラスタライザーと呼ばれるサードパーティ製ライブラリが必要です。たとえば、WindowsにはDirectXベースのグラフィックス用のWARPラスタライザーが含まれています。場合によっては、代替のソフトウェアレンダラーを使用したいと思うかもしれません。ハードウェアレンダリング（ハードウェアアクセラレーション）には、グラフィックスプロセッサ（GPU）が必要です。

HDX™ Graphicsは、最も一般的なユースケース向けに最適化されたデフォルトのエンコーディング構成を提供します。Citrixポリシーを使用することで、IT管理者はさまざまなグラフィックス関連設定を構成して、さまざまな要件を満たし、望ましいユーザーエクスペリエンスを提供することもできます。

シンワイヤー

Thinwireは、Citrix Virtual Apps and Desktopsで使用されるCitrixのデフォルトのディスプレイリモート処理テクノロジーです。

ディスプレイリモート処理テクノロジーにより、あるマシンで生成されたグラフィックスを、通常はネットワーク経由で別のマシンに送信して表示できます。グラフィックスは、キーボード入力やマウス操作などのユーザー入力の結果として生成されます。

HDX 3D プロ

Citrix Virtual Apps and DesktopsのHDX 3D Pro機能を使用すると、ハードウェアアクセラレーションにグラフィックス処理ユニット（GPU）を使用して最高のパフォーマンスを発揮するデスクトップとアプリケーションを配信できます。これらのアプリケーションには、OpenGLおよびDirectXベースの3Dプロフェッショナルグラフィックスアプリケーションが含まれます。標準VDAはDirectXのGPUアクセラレーションのみをサポートします。

WindowsシングルセッションOS向けGPUアクセラレーション

HDX 3D Proを使用すると、グラフィックスを多用するアプリケーションを、ホストされたデスクトップまたはシングルセッションOSマシン上のアプリケーションの一部として配信できます。HDX 3D Proは、物理ホストコンピューター（デスクトップ、ブレード、ラックワークステーションを含む）と、XenServer®、vSphere、Hyper-V（パススルーのみ）ハイパーバイザーが提供するGPUパススルーおよびGPU仮想化テクノロジーをサポートします。

GPUパススルーを使用すると、専用のグラフィックス処理ハードウェアに排他的にアクセスできるVMを作成できます。ハイパーバイザーに複数のGPUをインストールし、これらのGPUのそれぞれにVMを1対1で割り当てることができます。

GPU仮想化を使用すると、複数の仮想マシンが単一の物理GPUのグラフィックス処理能力に直接アクセスできます。

WindowsマルチセッションOS向けGPUアクセラレーション

HDX 3D Proを使用すると、WindowsマルチセッションOSセッションで実行されているグラフィックを多用するアプリケーションを、サーバーグラフィックス処理ユニット（GPU）でレンダリングできます。OpenGL、DirectX、Direct3D、およびWindows Presentation Foundation（WPF）のレンダリングをサーバーGPUに移行することで、グラフィックスレンダリングがサーバーCPUの速度を低下させることはありません。また、ワークロードがCPUとGPUに分割されるため、サーバーはより多くのグラフィックスを処理できます。

フレームホーク

> **重要:**
>
> Citrix Virtual Apps and Desktops 7 1903以降、Framehawkはサポートされなくなりました。代わりに、Thinwireをアダプティブトランスポートを有効にして使用してください。

> Framehawkは、ブロードバンドワイヤレス接続（Wi-Fiおよび4G/LTEセルラーネットワーク）を使用するモバイルワーカー向けのディスプレイリモートテクノロジーです。Framehawkは、スペクトル干渉とマルチパス伝播の課題を克服し、仮想アプリおよびデスクトップのユーザーに、スムーズでインタラクティブなユーザーエクスペリエンスを提供します。

テキストベースのセッションウォーターマーク

テキストベースのセッションウォーターマークは、データ盗難を抑止し、追跡を可能にするのに役立ちます。この追跡可能な情報は、写真やスクリーンキャプチャを使用してデータを盗む者への抑止力として、セッションデスクトップに表示されます。テキストのレイヤーであるウォーターマークを指定できます。ウォーターマークは、元のドキュメントの内容を変更することなく、セッション画面全体に表示できます。テキストベースのセッションウォーターマークには、VDAのサポートが必要です。

アダプティブ リフレッシュ レート

新しいスケーラビリティの改善により、HDXは、仮想モニターのリフレッシュレートを、設定されたターゲットFPSポリシーに一致させます。アダプティブ リフレッシュ レート（ARR）は、シングルセッションVDAとマルチセッションVDAの両方で利用でき、GPUアクセラレーションシナリオと非GPUシナリオの両方で機能します。

ロス許容モード

損失許容モードは徹底的に再設計され、パケット損失が検出された場合でもセッションがインタラクティブな状態を維持するようにします。

関連情報

- HDX スリーディー プロ
- WindowsシングルセッションOSのGPUアクセラレーション
- WindowsマルチセッションOSのGPUアクセラレーション
- フレームホーク
- シンワイヤー
- テキストベースのセッションウォーターマーク(/ja-jp/citrix-virtual-apps-desktops/2411/graphics/session-watermark.html)

10ビットハイダイナミックレンジ (HDR)

10ビットハイダイナミックレンジ (HDR) 仮想デスクトップセッションでは、拡張されたエンコードおよびデコード機能を使用して、より広い色域、より高いコントラストと輝度で高品質の画像やビデオをレンダリングできます。また、ユーザーエクスペリエンスを向上させるために、白色輝度レベル、Extended Display Identification Data (EDID)、および視覚品質をカスタマイズできます。

システム要件

エンドポイント:

- NVIDIA GPU 向け Windows 版 Citrix Workspace™ アプリ 2209 以降
- エンドポイントで10ビットHEVC (H.265) 444デコードをサポートするNVIDIA GPU
- 10ビットHDR対応モニター。ディスプレイ設定を使用して、すべてのモニターで10ビットHDRを有効にする必要があります。

サーバー:

- NVIDIA GPU 用 Windows シングルセッションOS VDA 2209 以降、および Intel GPU 用 VDA 2308 以降
- VDAで10ビットHEVC 444エンコードをサポートするNVIDIA GPU

必要なポリシー

エンドポイント:

- グラフィックのH.265デコードを有効にする

サーバー:

- 3Dグラフィックワークロード向けに最適化
- グラフィックステータスインジケーター (オプション)

サーバー構成

10ビットHDR対応のエンドポイントモニターでCitrix®セッションを起動すると、HDRセッションがデフォルトで有効になります。マルチモニターHDRセッションでは、すべてのエンドポイントモニターで10ビットHDRが有効になっている必要があります。HDRセッションは、ウィンドウモードと全画面モードの両方でサポートされます。

リファレンスホワイトレベル

この設定は、ニット値によって白色輝度レベルを定義します。セッション内の相対的なHDR画面の明るさを制御します。デフォルト値は80ニットです。異なるニット値を定義するには、次のレジストリキーを設定します。

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- 種類: REG_DWORD
- 名前: RefWhiteLevel

設定を有効にするには、セッションのサイズを変更するか、セッションを切断して再起動する必要があります。

EDIDのオーバーライド

HDRセッションでエンドポイントモニターのEDIDを使用するようにVDAを構成できます。これにより、色域と輝度範囲を一致させることで、モニターの表示機能を最大限に活用できます。デフォルトでは、HDRセッションはHDR1000対応のディスプレイを想定しています。 NVIDIAまたはその他のツールを使用してエンドポイントモニターのEDIDをエクスポートできます。次のレジストリキーを使用してVDAに適用します。

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- 種類: REG_BINARY
- 名前: EDIDOverride

EDIDをレジストリに保存する際、コンマ、スペース、または特殊文字を含めてはなりません。オーバーライドEDIDを有効にするには、サインアウトして新しいセッションを起動します。

視覚的にロスレスなエクスペリエンス

視覚的にロスレスなエクスペリエンスを実現するには、次のポリシーを有効にします。

- 視覚的にロスレスな圧縮を許可
- 視覚品質: 常にロスレスまたはロスレスに構築

ポリシーが設定された後、グラフィックスステータスインジケーターを使用して、イメージ品質スライダーを使用するか、ピクセルパーフェクトモードに切り替えることで、HDRセッションの品質を制御できます。

Windows画面ロックを許可

このポリシーを使用すると、画面ロックを含むすべてのWindowsディスプレイタイムアウトを、ワークステーションOS上のCitrix Virtual Desktopセッションに適用できます。この設定は、Citrix StudioのCitrixグループポリシーオブジェクトを使用して設定できます。

デフォルトでは、この設定が有効になっていない場合、アクティブなセッション中にCitrix Virtual Desktopは、セッションロック、スクリーンセーバー、またはディスプレイオフのタイムアウトに応答しません。

ワークステーションVDAでパスワード保護されたスクリーンセーバーが構成されている場合、スクリーンセーバーのタイムアウトに達したときにCitrix Virtual Desktopセッションが自動的にロックされるようにするには、この設定を有効にする必要があります。

VDAでディスプレイオフタイムアウトが構成されているときにこの設定を有効にすると、そのタイムアウトの期限切れにより、ユーザーがセッションとの対話を再開するまで更新されないセッションになります。たとえば、表示されている時間は更新されず、新しい通知も表示されません。

その他の考慮事項

- 仮想GPU上で最大4台のモニターで10ビットHDRセッションを起動できます。
- 次の場合、Citrixセッションは8ビットの非HDRモードに戻ります。
  - いずれかのエンドポイントモニターで10ビットHDRが有効になっていない場合
  - 画面共有を有効にする。
  - VDA上で仮想ディスプレイレイアウトを設定する。
  - 「**視覚的にロスレスな圧縮を許可**」ポリシーを設定せずに、ピクセルパーフェクトモードに切り替える。

HDX™ 3D プロ

Citrix Virtual Apps and Desktops™のHDX 3D Pro機能を使用すると、ハードウェアアクセラレーションのためにグラフィック処理ユニット（GPU）を使用すると最高のパフォーマンスを発揮するデスクトップとアプリケーションを提供できます。これらのアプリケーションには、OpenGLおよびDirectXベースの3Dプロフェッショナルグラフィックアプリケーションが含まれます。標準VDAは、DirectXのGPUアクセラレーションのみをサポートします。

HDX 3D Proポリシー設定については、「3Dグラフィックスワークロードの最適化」を参照してください。

サポートされているすべてのCitrix Workspaceアプリは3Dグラフィックスで使用できます。複雑な3Dワークロード、高解像度モニター、マルチモニター構成、および高フレームレートアプリケーションで最高のパフォーマンスを得るには、Citrix Workspace app for WindowsおよびCitrix Workspace app for Linuxの最新バージョンをお勧めします。サポートされているCitrix Workspaceアプリのバージョンに関する詳細については、「Citrix Workspaceアプリのライフサイクルマイルストーン」を参照してください。

3Dプロフェッショナルアプリケーションの例は次のとおりです。

- コンピューター支援設計、製造、エンジニアリング (CAD/CAM/CAE) アプリケーション
- 地理情報システム (GIS) ソフトウェア
- 医用画像処理通信システム (PACS)

- 最新のOpenGL、DirectX、NVIDIA CUDA、OpenCL、およびWebGLバージョンを使用するアプリケーション
- 並列コンピューティングにNVIDIA Compute Unified Device Architecture (CUDA) GPUを使用する、計算集約型の非グラフィカルアプリケーション

HDX 3D Proは、あらゆる帯域幅で最高のユーザーエクスペリエンスを提供します。

- WAN接続の場合：1.5 Mbpsという低い帯域幅のWAN接続でも、インタラクティブなユーザーエクスペリエンスを提供します。
- LAN接続の場合: LAN接続では、ローカルデスクトップと同等のユーザーエクスペリエンスを提供します。

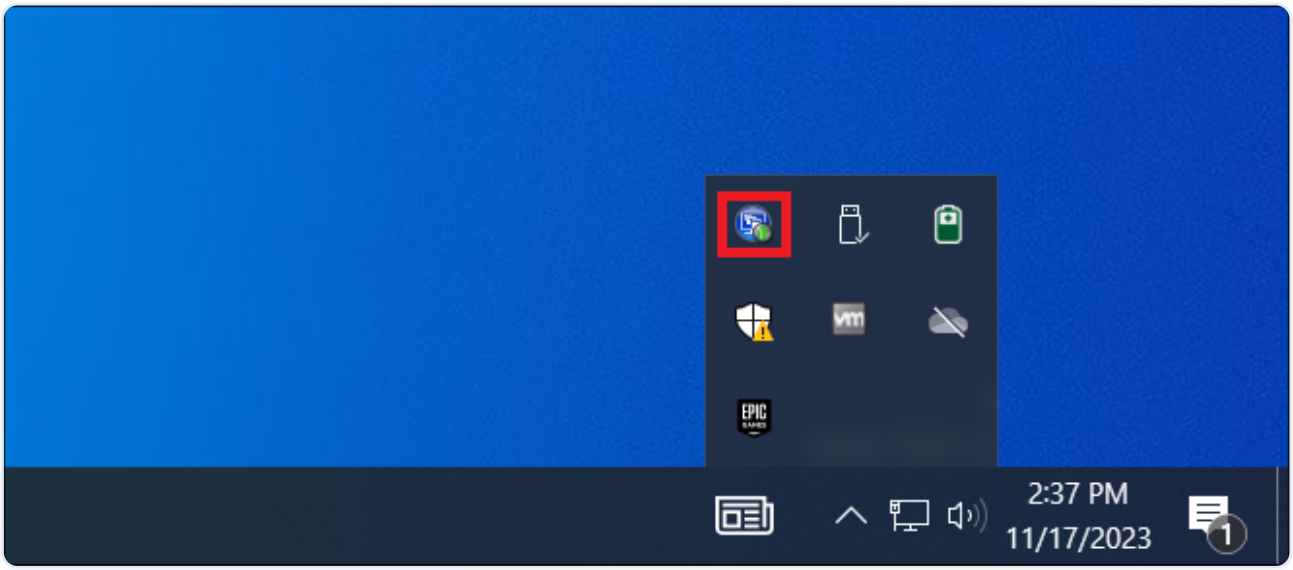
  複雑で高価なワークステーションを、グラフィック処理をデータセンターに移動して一元管理することで、よりシンプルなユーザーデバイスに置き換えることができます。

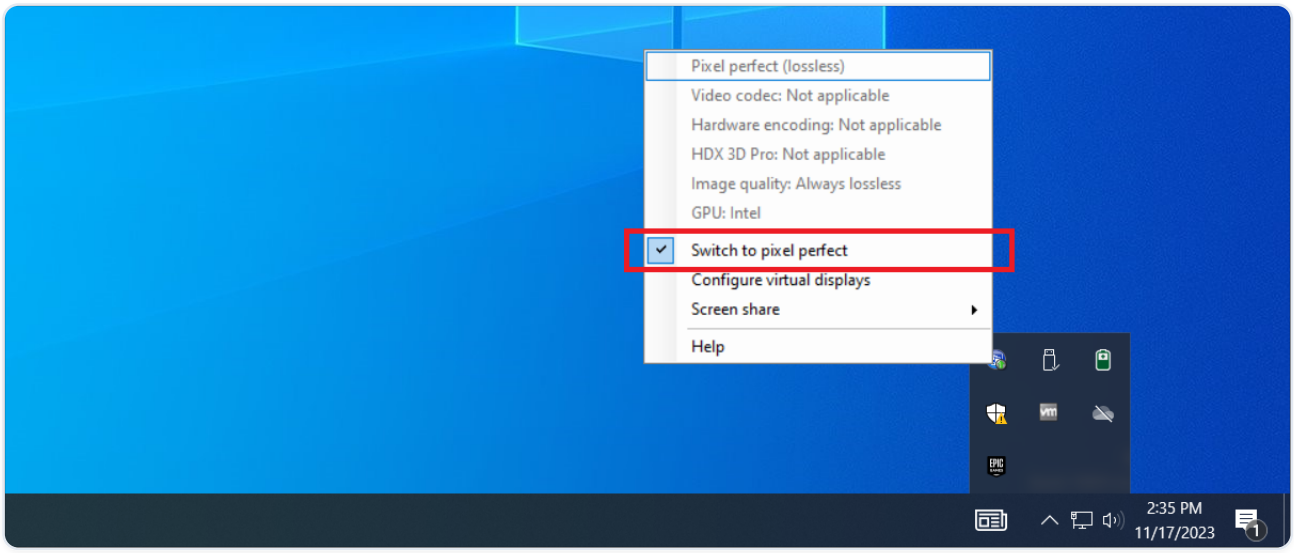
特殊なユースケース向けのロスレス圧縮オプション

HDX 3D Proは、医用画像処理など、ピクセルパーフェクトなグラフィックが必要なアプリケーションをサポートするために、CPUベースのロスレスコーデックも提供します。真のロスレス圧縮は、より多くのネットワークリソースと処理リソースを消費するため、特殊なユースケースでのみ推奨されます。

ロスレス圧縮を使用する場合：

- グラフィックステータスインジケーター（通知領域アイコン）のロスレスインジケーターは、表示されている画面がロッシーフレームかロスレスフレームかをユーザーに通知します。このアイコンは、**視覚品質**ポリシー設定で**ロスレスにビルド**が指定されている場合に役立ちます。送信されたフレームがロスレスの場合、ロスレスインジケーターは緑色に変わります。





- ロスレススイッチを使用すると、セッション中にいつでも**常にロスレス**モードに変更できます。セッション内で**ロスレス**を選択または解除するには、アイコンを右クリックして**ピクセルパーフェクトに切り替え**をクリックするか、ショートカットALT+SHIFT+1を使用します。
  - ロスレス圧縮の場合：HDX 3D Proは、ポリシーで選択されたコーデックに関係なく、ロスレスコーデックを圧縮に使用します。
  - ロッシー圧縮の場合：HDX 3D Proは、デフォルトまたはポリシーで選択された元のコーデックを使用します。 ロスレススイッチの設定は、以降のセッションでは保持されません。すべての接続でロスレスコーデックを使用するには、**視覚品質ポリシー**設定で**常にロスレス**を選択します。

セッション内でロスレスを選択または解除するためのデフォルトのショートカットALT+SHIFT+1を上書きできます。`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator`で新しいレジストリ設定を構成します。

- 名前：HKEY_LOCAL_MACHINE_HotKey、種類：String
- ショートカットの組み合わせを構成する形式はC=0|1, A=0|1, S=0|1, W=0|1, K=valです。キーはコンマ「,」で区切る必要があります。キーの順序は関係ありません。
- A、C、S、W、Kはキーであり、ここでC=Control、A=ALT、S=SHIFT、W=Win、K=有効なキーです。Kに許可される値は0～9、a～z、および任意の仮想キーコードです。
- 例： F10の場合、K=0x79を設定 Ctrl + F10の場合、C=1, K=0x79を設定 Alt + Aの場合、A=1, K=aまたはA=1, K=AまたはK=A, A=1を設定 Ctrl + Alt + 5の場合、C=1, A=1, K=5またはA=1, K=5, C=1を設定 Ctrl + Shift + F5の場合、A=1, S=1, K=0x74を設定

HDX 3D Proのユーザーエクスペリエンスを最適化する

複数のユーザーが帯域幅の制限された接続（たとえば、支店など）を共有している場合、各ユーザーが利用できる帯域幅を制限するために、全体セッション帯域幅制限ポリシー設定を使用することをお勧めします。この設定を使用すると、ユーザーがログオンおよびログオフしても、利用可能な帯域幅が大きく変動しないようにすることができます。HDX 3D Proは利用可能なすべての帯域幅を使用するように自動的に調整されるため、ユーザーセッション全体で利用可能な帯域幅が大きく変動すると、パフォーマンスに悪影響を及ぼす可能性があります。 たとえば、20人のユーザーが60 Mbpsの接続を共有している場合、各ユーザーが利用できる帯域幅は、同時ユーザー数に応じて3 Mbpsから60 Mbpsの間で変動する可能性があります。このシナリオでユーザーエクスペリエンスを最適化するには、ピーク時にユーザーごとに必要な帯域幅を決定し、常にその量にユーザーを制限します。 3Dマウスのユーザーの場合、汎用USBリダイレクト仮想チャネルの優先度を0に上げることをお勧めします。仮想チャネルの優先度を変更する方法については、Knowledge Centerの記事CTX128190を参照してください。 HDX Monitorツールを使用して、HDX視覚化テクノロジーの動作と構成を検証し、HDXの問題を診断およびトラブルシューティングします。このツールは、Citrix Virtual Apps and DesktopsのインストールメディアのSupportフォルダーにあります。

WindowsマルチセッションOS向けGPUアクセラレーション

Citrix Virtual Apps and Desktops™は、WindowsマルチセッションOSセッションで実行されるグラフィック負荷の高いアプリケーションが、サーバーのグラフィック処理ユニット (GPU) でレンダリングされることをサポートします。OpenGL、DirectX、Direct3D、およびWindows Presentation Foundation (WPF) のレンダリングをサーバーのGPUに移行することで、サーバーのCPUをより効率的に使用できます。

Windows Server はマルチユーザーオペレーティングシステムであるため、複数のユーザーが GPU 仮想化 (vGPU) を必要とせずに Citrix Virtual Apps™ によってアクセスされる GPU を共有できます。

レジストリの編集を伴う手順については、注意してください。レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題を引き起こす可能性があります。Citrix® は、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。編集する前にレジストリをバックアップしてください。

GPU 共有

GPU 共有により、リモートデスクトップセッションで OpenGL および DirectX アプリケーションの GPU ハードウェアレンダリングが可能になります。次の特性があります。

- アプリケーションのスケーラビリティとパフォーマンスを向上させるために、ベアメタルまたは仮想マシンで使用できます。
- 複数の同時セッションで GPU リソースを共有できます (ほとんどのユーザーは専用 GPU のレンダリングパフォーマンスを必要としません)。
- 特別な設定は必要ありません。

GPU は、ハイパーバイザーおよび GPU ベンダーの要件に従って、フルパススルーモードまたは仮想 GPU (vGPU) モードのいずれかで Windows Server 仮想マシンに割り当てることができます。物理 Windows Server マシンへのベアメタル展開もサポートされています。

GPU 共有は、特定のグラフィックカードに依存しません。

- 仮想マシンの場合、使用しているハイパーバイザーと互換性のあるグラフィックカードを選択してください。XenServerのハードウェア互換性リストについては、ハイパーバイザーハードウェア互換性リストを参照してください。
- ベアメタルで実行する場合、オペレーティングシステムによって有効化された単一のディスプレイアダプターを使用することをお勧めします。複数のGPUがハードウェアにインストールされている場合は、デバイスマネージャーを使用して1つを除くすべてを無効にしてください。

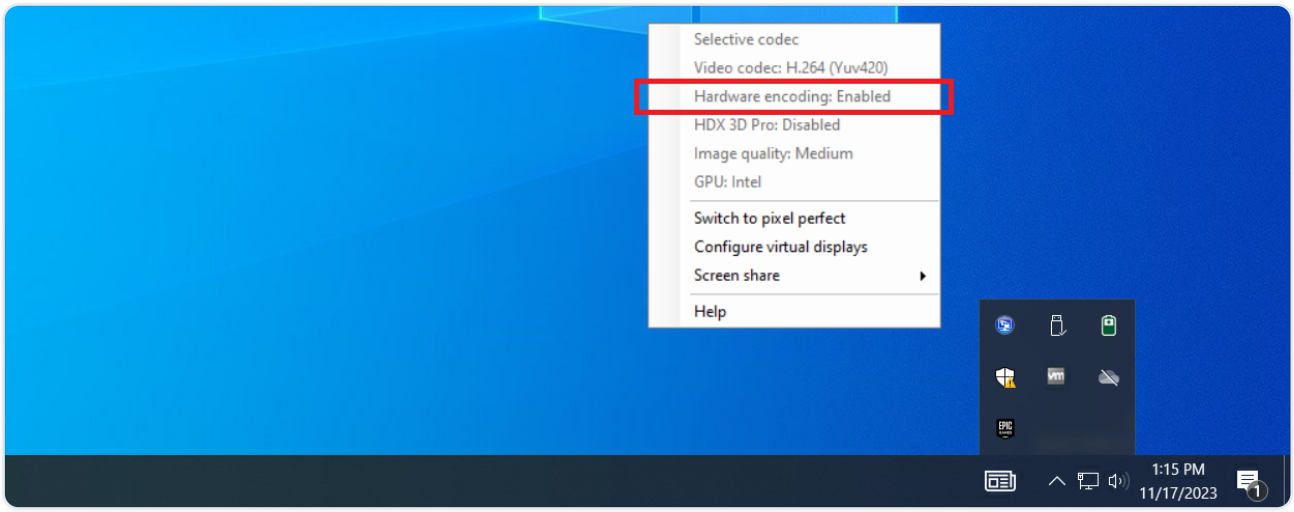
GPU Sharing を使用したスケーラビリティは、いくつかの要因によって異なります。

- 実行されているアプリケーション
- 消費するビデオ RAM の量
- グラフィックカードの処理能力

一部のアプリケーションは、他のアプリケーションよりもビデオRAMの不足にうまく対処します。ハードウェアが過負荷になると、グラフィックカードドライバーの不安定化やクラッシュが発生する可能性があります。このような問題を避けるために、同時ユーザー数を制限してください。

- NVIDIA GPU および Intel Iris Pro グラフィックプロセッサ用の高性能ビデオエンコーダーへのアクセス。ポリシー設定（デフォルトで有効）がこの機能を制御し、H.264 エンコード（利用可能な場合）にハードウェアエンコードの使用を許可します。このようなハードウェアが利用できない場合、VDA はソフトウェアビデオコーデックを使用した CPU ベースのエンコードにフォールバックします。詳しくは、「グラフィックポリシー設定」を参照してください。

GPU アクセラレーションが機能していることを確認するには、グラフィックステータスインジケーターを使用できます。



DirectX、Direct3D、および WPF レンダリング

DirectX、Direct3D、およびWPFレンダリングは、ディスプレイドライバーインターフェイス（DDI）バージョン9ex、10、または11をサポートするGPUを搭載したサーバーでのみ利用できます。

- Windows Server 2016以降では、RDセッションホストサーバー上のRemote Desktop Services（RDS）セッションは、Microsoft Basic Render Driverをデフォルトのアダプターとして使用します。Windows Server 2016以降のRDSセッションでGPUを使用するには、グループポリシーの**ローカルコンピューターポリシー** \> **コンピューターの構成** \> **管理用テンプレート** \> **Windowsコンポーネント** \> **Remote Desktop Services** \> **リモートデスクトップセッションホスト** \> **リモートセッション環境**で、**すべてのRemote Desktop Servicesセッションにハードウェアの既定のグラフィックアダプターを使用する**設定を有効にします。
- WPFアプリケーションがサーバーのGPUを使用してレンダリングできるようにするには、WindowsマルチセッションOSセッションを実行しているサーバーのレジストリに設定を作成します。レジストリ設定の詳細については、レジストリで管理される機能のリストにある「Windows Presentation Foundation (WPF) レンダリング」を参照してください。

CUDAまたはOpenCLアプリケーションのGPUアクセラレーション

ユーザーセッションで実行されているCUDAおよびOpenCLアプリケーションのGPUアクセラレーションは、デフォルトで無効になっています。

CUDA アクセラレーション機能を使用するには、レジストリ設定を有効にします。詳細については、レジストリで管理される機能のリストにある「CUDA または OpenCL アプリケーションの GPU アクセラレーション」を参照してください。

WindowsシングルセッションOSのGPUアクセラレーション

HDX 3D Proを使用すると、グラフィックを多用するアプリケーションを、ホストされたデスクトップまたはシングルセッションOSマシン上のアプリケーションの一部として配信できます。HDX 3D Proは、物理ホストコンピューター（デスクトップ、ブレード、ラックワークステーションを含む）と、XenServer®、vSphere、Nutanix、Hyper-V（パススルーのみ）ハイパーバイザーが提供するGPUパススルーおよびGPU仮想化テクノロジーをサポートします。

HDX™ 3D Proは、次の機能を提供します。

- 最適なWANおよびワイヤレスパフォーマンスのための、適応型H.264ベースまたはH.265ベースのディープ圧縮。HDX 3D Proは、エンコードのデフォルトの圧縮技術として、CPUベースのフルスクリーンH.264圧縮を使用します。H.264によるハードウェアエンコードは、NVENCをサポートするNVIDIA、Intel、AMDのカードで使用されます。H.265によるハードウェアエンコードは、NVENCをサポートするNVIDIAのカードで使用されます。
- 特殊なユースケース向けのロスレス圧縮オプション。HDX 3D Proは、医療画像処理など、ピクセルパーフェクトなグラフィックが必要なアプリケーションをサポートするために、CPUベースのロスレスコーデックも提供します。真のロスレス圧縮は、より多くのネットワークリソースと処理リソースを消費するため、特殊なユースケースでのみ推奨されます。

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

- マルチモニターおよび高解像度モニターのサポート。シングルセッションOSマシンでは、最大8台の4Kモニターがサポートされます。ユーザーはモニターを任意の構成で配置でき、異なる解像度と向きのモニターを混在させることができます。モニターの数は、ホストコンピューターのGPU、ユーザーデバイス、および利用可能な帯域幅の機能によって制限されます。HDX 3D Proはすべてのモニター解像度をサポートし、ホストコンピューターのGPUの機能によってのみ制限されます。
- 動的解像度。仮想デスクトップまたはアプリケーションウィンドウのサイズを任意の解像度に変更できます。**注：** 解像度を変更する唯一のサポートされている方法は、VDAセッションウィンドウのサイズを変更することです。VDAセッション内から解像度を変更する（**コント**

ロールパネル > デザインと**パーソナル設定 > ディスプレイ > 画面の解像度**を使用する）ことはサポートされていません。

- NVIDIA vGPUアーキテクチャのサポート。HDX 3D ProはNVIDIA vGPUカードをサポートしています。詳細については、GPUパススルーとGPU共有に関するNVIDIA vGPUを参照してください。NVIDIA vGPUを使用すると、非仮想化オペレーティングシステムに展開されているものと同じNVIDIAグラフィックドライバーを使用して、複数のVMが単一の物理GPUに同時に直接アクセスできます。
- Virtual Direct Graphics Acceleration (vDGA) を使用したVMware vSphereおよびVMware ESXのサポート - HDX 3D ProをvDGAと組み合わせて、RDSおよびVDIワークロードの両方で使用できます。
- VMware vSphere/ESX のサポート。
- Windows Server 2016のDiscrete Device Assignmentを使用したMicrosoft HyperVのサポート。
- Intel Xeon Processor E3 FamilyおよびIntel Data Center GPU Flex Seriesによるデータセンターグラフィックスのサポート。詳細については、`<https://www.intel.com/content/www/us/en/products/details/discrete-gpus/data-center-gpu/flex-series.html>`を参照してください。
- AMD GPUのサポート。

> 注:
>
> AMD MxGPU (GPU仮想化) のサポートは、VMware vSphere vGPUでのみ機能します。Citrix HypervisorおよびHyper-Vは、GPUパススルーでサポートされています。詳しくは、`<https://www.amd.com/en/graphics/workstation-virtual-graphics>`を参照してください。

- NVIDIA GPU、AMD GPU、およびIntel GPU用の高性能ビデオエンコーダーへのアクセス。この機能は、ポリシー設定（デフォルトで有効）によって制御されます。この機能により、H.264、H.265、またはAV1エンコード（利用可能な場合）にハードウェアエンコードを使用できます。このようなハードウェアが利用できない場合、VDAはソフトウェアビデオコーデックを使用してCPUベースのエンコードにフォールバックします。詳しくは、グラフィックポリシー設定を参照してください。

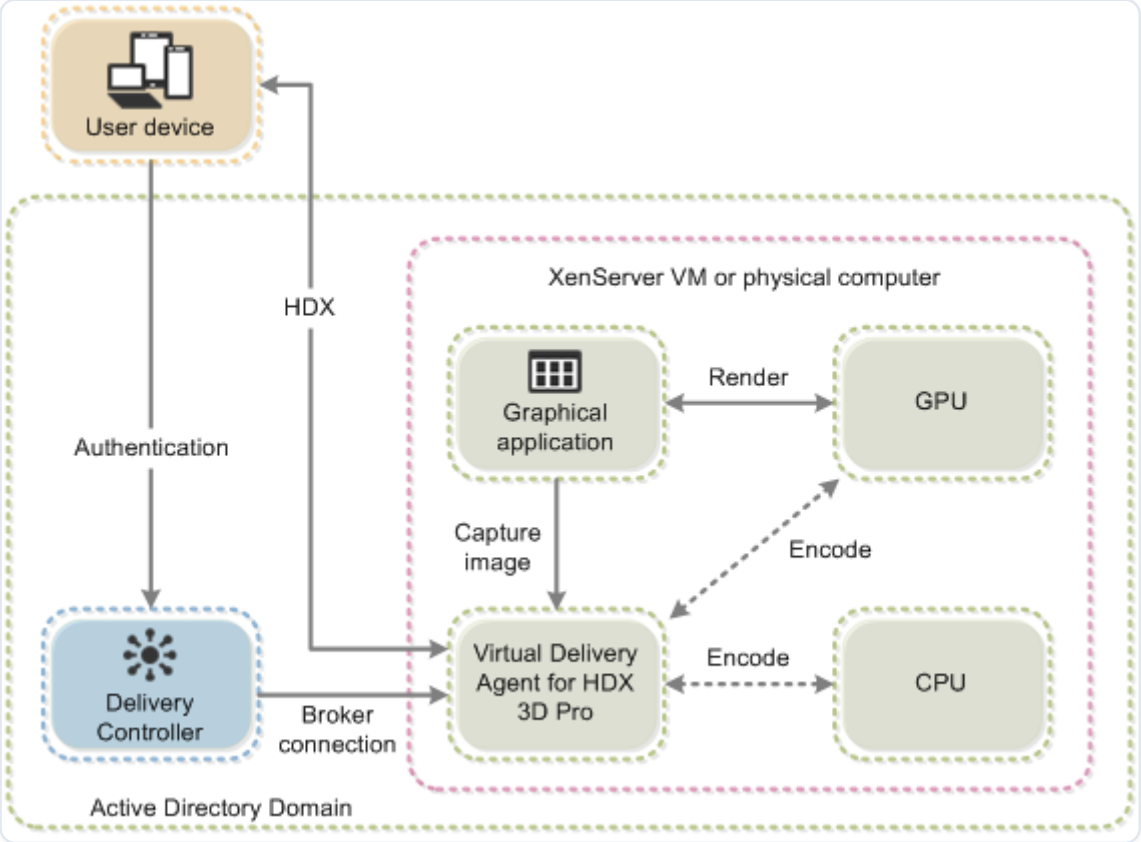
次の図に示すように、:

- ユーザーがCitrix Workspace™ appにログオンして仮想アプリケーションまたはデスクトップにアクセスすると、Controllerがユーザーを認証します。その後、ControllerはHDX 3D Pro用

VDAに接続し、グラフィックアプリケーションをホストするコンピューターへの接続を仲介します。

HDX 3D Pro用VDAは、ホスト上の適切なハードウェアを使用して、デスクトップ全体またはグラフィックアプリケーションのみのビューを圧縮します。

- デスクトップまたはアプリケーションのビューと、それらに対するユーザーの操作は、ホストコンピューターとユーザーデバイス間で転送されます。この転送は、Citrix Workspace appとHDX 3D Pro用VDA間の直接HDX接続を介して行われます。



HDX 3D Proのユーザーエクスペリエンスを最適化する

帯域幅が制限された接続（たとえば、支店など）を複数のユーザーが共有している場合、各ユーザーが利用できる帯域幅を制限するために、**全体のセッション帯域幅制限**ポリシー設定を使用することをお勧めします。この設定を使用すると、ユーザーがログオンおよびログオフしても、利用可能な帯域幅が大きく変動しないようにできます。HDX 3D Proは利用可能なすべての帯域幅を使用するように自動的に調整されるため、ユーザーセッション中に利用可能な帯域幅が大きく変動すると、パフォーマンスに悪影響を及ぼす可能性があります。

たとえば、20人のユーザーが60 Mbpsの接続を共有している場合、各ユーザーが利用できる帯域幅は、同時接続ユーザー数に応じて3 Mbpsから60 Mbpsの間で変動する可能性があります。この

シナリオでユーザーエクスペリエンスを最適化するには、ピーク時にユーザーごとに必要な帯域幅を決定し、常にその量にユーザーを制限します。

3Dマウスのユーザーの場合、Generic USB Redirection仮想チャネルの優先度を0に上げることをお勧めします。仮想チャネルの優先度を変更する方法については、Knowledge Centerの記事CTX128190を参照してください。

ロスレス圧縮

ロスレス圧縮を使用する場合：

- ロスレスインジケーター（通知領域アイコン）は、表示されている画面がロッシーフレームかロスレスフレームかをユーザーに通知します。このアイコンは、**視覚品質**ポリシー設定で**ロスレスにビルド**が指定されている場合に役立ちます。送信されるフレームがロスレスの場合、ロスレスインジケーターは緑色に変わります。
- ロスレススイッチを使用すると、セッション中いつでもユーザーが**常にロスレス**モードに変更できます。セッション中いつでもロスレスを選択または選択解除するには、アイコンを右クリックして**ピクセルパーフェクトに切り替える**をクリックするか、ショートカット**ALT+SHIFT+1**を使用します。
- ロスレス圧縮の場合: HDX 3D Proは、ポリシーで選択されたコーデックに関係なく、圧縮にロスレスコーデックを使用します。
- 非可逆圧縮の場合: HDX 3D Proは、デフォルトまたはポリシーで選択された元のコーデックを使用します。
- ロスレススイッチの設定は、以降のセッションでは保持されません。すべての接続でロスレスコーデックを使用するには、**視覚品質**ポリシー設定で**常にロスレス**を選択します。

ロスレスホットキー

デフォルトのショートカット**ALT+SHIFT+1**を使用することで、セッション中いつでもホットキーを使用して**ロスレス**を選択またはクリアできます。

Windowsレジストリで、デフォルトのショートカット**ALT+SHIFT+1**を上書きできます。 新しいレジストリ設定を構成するには、次のレジストリ値を設定します。

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\Graphics`
- **名前**: `HKLM_HotKey`
- **種類**: `String`

ショートカットの組み合わせを構成する形式は`C=0|1, A=0|1, S=0|1, W=0|1, K=val`です。キーはスペースなしでコンマ「,」で区切る必要があります。キーの順序は関係ありません。

A、C、S、W、Kはキーであり、C=Control、A=ALT、S=SHIFT、W=Win、K=有効なキーで、Kに許可される値は0～9、a～z、および任意の仮想キーコードです。

例:

- **F10**の場合、K=0x79を設定します
- **Ctrl + F10**の場合、C=1、K=0x79を設定します
- 「**Alt + A**」については、A=1,K=a または A=1,K=A または K=A,A=1 を設定します。
- 「**Ctrl + Alt + 5**」については、C=1, A=1,K=5 または A=1,K=5,C=1 を設定します。
- 「**Ctrl + Shift + F5**」については、A=1,S=1,K=0x74 を設定します。

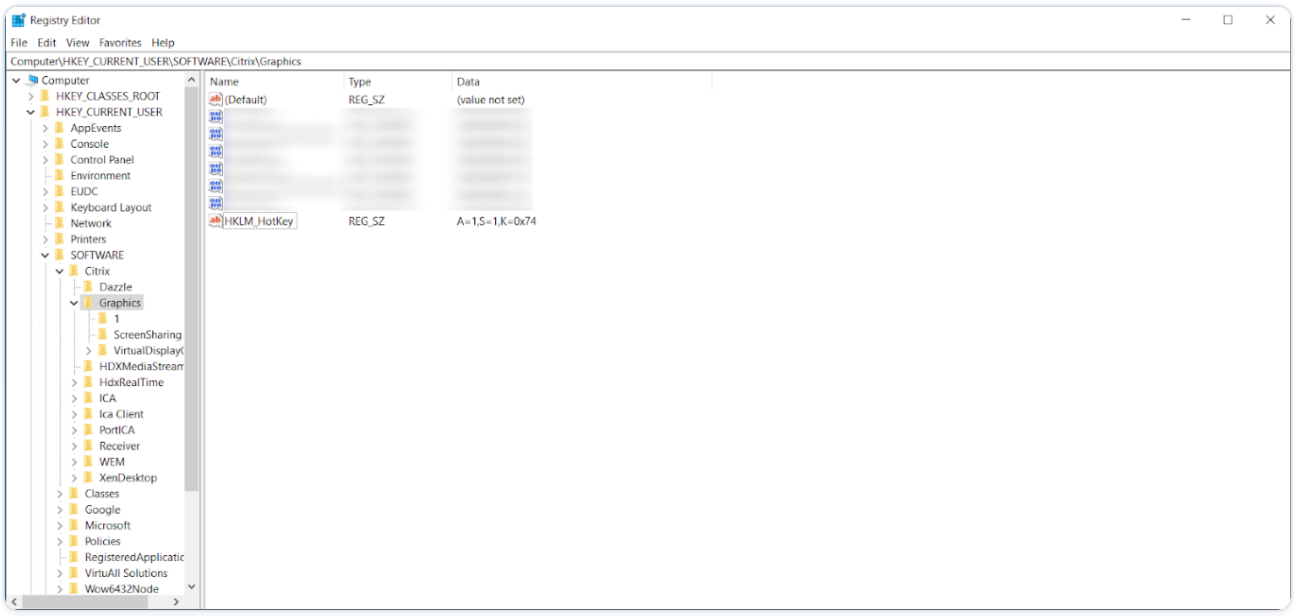
次の表は、仮想キーコードの例のリストを示しています。

キー	値
F1	0x70
F2	0x71
F3	0x72
F4	0x73
F5	0x74
F6	0x75
F7	0x76
F8	0x77
F9	0x78
F10	0x79
F11	0x7A
F12	0x7B
PAGE UP キー	0x21
PAGE DOWN キー	0x22

キー	値
END キー	0x23
HOME キー	0x24
左矢印キー	0x25
上矢印キー	0x26
右矢印キー	0x27
下矢印キー	0x28

ショートカットの組み合わせの間にスペースがないことを確認してください。例:

正しい: C=1,K=0x74 誤り: C=1, K=0x74



注意:

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

シンワイヤー

はじめに

Thinwireは、Citrix HDXテクノロジーの一部であり、Citrix Virtual Apps and Desktopsで使用されるCitrixのデフォルトのディスプレイリモートテクノロジーです。

ディスプレイリモートテクノロジーにより、あるマシンで生成されたグラフィックを、通常はネットワーク経由で別のマシンに送信して表示することができます。

成功したディスプレイリモートソリューションは、ローカルPCと同様の、高度にインタラクティブなユーザーエクスペリエンスを提供します。Thinwireは、複雑で効率的なさまざまな画像分析および圧縮技術を使用することで、このエクスペリエンスを実現します。Thinwireは、サーバーのスケーラビリティを最大化し、他のディスプレイリモートテクノロジーよりも少ない帯域幅で動作します。

このバランスにより、Thinwireはほとんどの一般的なビジネスユースケースに対応し、Citrix Virtual Apps and Desktopsのデフォルトのディスプレイリモートテクノロジーとして使用されています。

エイチディーエックス™ スリーディー プロ

デフォルト構成では、Thinwireは3Dグラフィックまたは高度にインタラクティブなグラフィックを配信し、グラフィック処理ユニット（GPU）が存在する場合はそれを使用できます。ただし、GPUが存在するシナリオでは、**3Dグラフィックワークロード向けに最適化**または**視覚品質 > ロスレスビルド**ポリシーを使用してHDX 3D Proモードを有効にすることをお勧めします。これらのポリシーは、GPUが存在する場合に、Thinwireがビデオコーデック（H.264、H.265、またはAV1）を使用してハードウェアアクセラレーションで画面全体をエンコードするように構成します。これにより、3Dプロフェッショナルグラフィックのよりスムーズなエクスペリエンスが提供されます。詳しくは、H.264 Build to lossless、HDX 3D Pro、およびGPU acceleration for Windows Single-session OSを参照してください。

要件

Thinwireは、Windows Server 2022、Windows Server 2019、Windows 10、Windows 7などの最新のオペレーティングシステム向けに最適化されています。Windows Server 2008 R2では、レガシーグラフィックモードが推奨されます。これらのユースケースに対してCitrixが推奨するポリシー設定の組み合わせを提供するには、組み込みのCitrix policy templates、High Server Scalability-Legacy OS、およびOptimized for WAN-Legacy OSを使用してください。

- Thinwireの動作を制御するポリシー設定である**圧縮にビデオコーデックを使用**は、Citrix Virtual Apps and Desktops 7 1808以降およびXenApp and XenDesktop 7.6 FP3以降のVDAバージョンで利用できます。**優先時にビデオコーデックを使用**オプションは、Citrix Virtual Apps and Desktops 7 1808以降およびXenApp and XenDesktop 7.9以降のVDAバージョンでデフォルト設定です。
- すべてのCitrix Workspace™アプリはThinwireをサポートしています。一部のCitrix Workspaceアプリは、帯域幅使用量を削減するための8ビットまたは16ビットグラフィックなど、他のアプリがサポートしないThinwireの機能をサポートする場合があります。このような機能のサポートは、Citrix Workspaceアプリによって自動的にネゴシエートされます。
- Thinwireは、マルチモニターおよび高解像度のシナリオで、より多くのサーバーリソース（CPU、メモリ）を使用します。Thinwireが使用するリソースの量を調整することは可能ですが、その結果、帯域幅の使用量が増加する可能性があります。
- 低帯域幅または高遅延のシナリオでは、インタラクティブ性を向上させるために8ビットまたは16ビットグラフィックを有効にすることを検討してください。特に8ビットの色深度では、視覚品質が影響を受ける可能性があります。

エンコード方法

Thinwireは、ポリシーとクライアントの機能に応じて、2つの異なるエンコードモードで動作できます。

- アダプティブJPEGを使用したThinwire **圧縮にビデオコーデックを使用する**ポリシー設定: **ビデオコーデックを使用しない**
- 選択的H.264、H.265、またはAV1を使用したThinwire **圧縮にビデオコーデックを使用する**ポリシー設定: **優先される場合はビデオコーデックを使用する** または **アクティブに変化する領域の場合**
- 全画面H.264、H.265、またはAV1を使用したThinwire **圧縮にビデオコーデックを使用する**ポリシー設定: **画面全体の場合**

H.265

High Efficiency Video Coding (HEVC) はH.265としても知られ、H.264の後継です。 H.265ビデオコーデックによるハードウェアエンコードは、以下のGPUでサポートされています。

- NVIDIA Maxwellベース以降のGPU
- Intel 第6世代以降のGPU
- AMD Ravenベース以降のGPU

AV1

CitrixはAV1ビデオコーデックのサポートを追加しました。AV1の利点は、H.264およびH.265と比較して、優れた画像圧縮、より良い画質、および低い帯域幅使用量を持つことです。

AV1の以下の要件を満たす必要があります。

- NVIDIA GPUの場合はVDA 2305以降、または
- Intel GPUの場合はVDA 2308以降

以下のGPUはエンコーディングに対応しています。

- NVIDIA Ada LovelaceベースのGPU
- インテル ARC または インテル データセンター GPU Flex Series GPU

NVIDIAのAda Lovelace GPUの詳細については、ADAアーキテクチャを参照してください。

IntelのARCワークステーションおよびデータセンターFlexシリーズGPUの詳細については、Flexシリーズおよび概要を参照してください。

自動ビデオコーデック選択

圧縮ポリシーの**ビデオコーデックを使用**が有効になっている場合、またはVDAで3Dグラフィックワークロードの最適化が有効になっている場合に、最適なビデオコーデックを自動的に検出できます。Citrix Workspaceアプリfor Windowsのインストール中に、エンドポイントのデコード機能が評価されます。この情報に基づいて、Citrix Workspaceアプリfor Windowsは、接続時にVDAと使用する最適なコーデックをネゴシエートします。ビデオコーデックが評価される順序は次のとおりです。

- AV1
- H.265
- H.264

自動選択は、これらのコーデックの4:2:0バリアントにのみ適用されます。**視覚品質**設定が「Build-to-Lossless」または「Always Lossless」に設定されており、視覚的にロスレスを許可が「有効」に設定されている場合、ビデオコーデックの自動選択は無効になります。

リソースに接続すると、Citrix WorkspaceアプリはエンドポイントのH.265およびAV1のデコード機能をテストし、その機能をレジストリに保存します。その後、Citrix Workspaceアプリは使用する最適なビデオコーデックを自動的に選択し、VDAとネゴシエートします。VDAとクライアントの両方がH.265とAV1を使用できる場合、AV1がビデオコーデックとして選択されます。AV1が

VDAまたはクライアントのいずれかで利用できない場合、H.265がネゴシエートされます。H.265もどちらかで利用できない場合、セッションはH.264をビデオコーデックとして使用します。

> **注:**
>
> この機能はデフォルトで有効になっています。この動作は、新しいクライアント側のレジストリ設定`DisableDecoderCaps`を設定することで変更できます。

> ビデオコーデックの自動選択を無効にするには、「DisableDecoderCaps」を`HKLM\Software\WOW6432Node\Policies\Citrix\ICA Client\Graphics Engine DWORD DisableDecoderCaps = 1`または`HKCU\Software\Policies\Citrix\ICA Client\Graphics Engine DWORD DisableDecoderCaps = 1`に設定します。

これらの値のいずれかが1に設定されている場合、ビデオコーデックの自動選択は使用されません。 グラフィックステータスインジケーターとHDXモニターでビデオコーデックを監視できます。

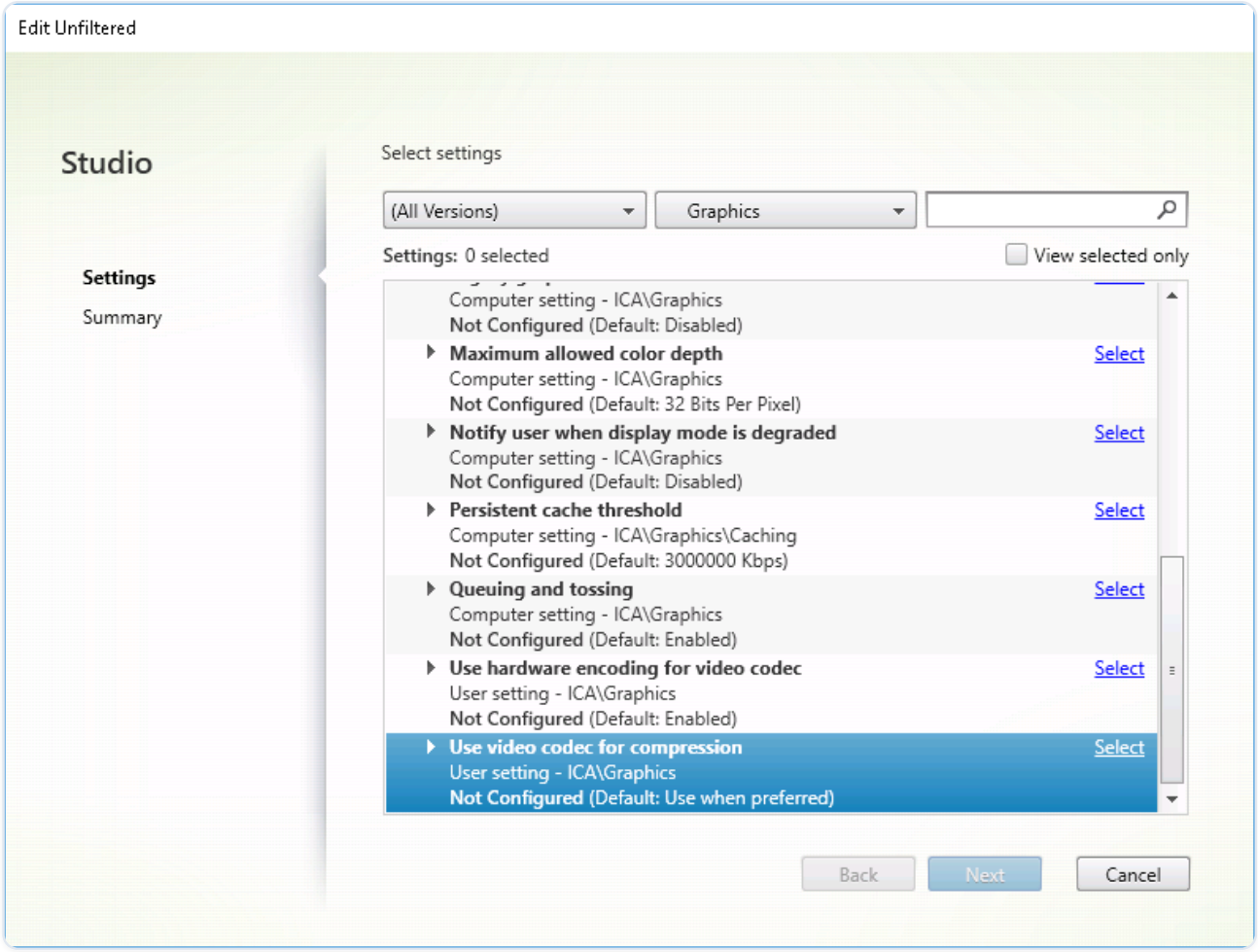
構成

Thinwire は、デフォルトのディスプレイリモート処理テクノロジーです。

以下のグラフィックポリシー設定は、デフォルトを設定し、さまざまなユースケースの代替手段を提供します。

- 圧縮にビデオコーデックを使用
  - **優先する場合はビデオコーデックを使用**。これがデフォルト設定です。追加の構成は不要です。この設定をデフォルトのままにすることで、すべての Citrix 接続で Thinwire が選択され、一般的なデスクトップワークロードのスケーラビリティ、帯域幅、および優れた画質のために最適化されます。これは、**アクティブに変更される領域の場合**と機能的に同等です。
- このポリシー設定の他のオプションは、さまざまなユースケースで他のテクノロジーと組み合わせて Thinwire を引き続き使用します。例：
  - **アクティブに変更される領域の場合**。Thinwire のアダプティブディスプレイテクノロジーは、動いている画像（ビデオ、モーション内の 3D）を識別し、画像が動いている画面の部分でのみ H.264、H.265、または AV1 を使用します。

- **画面全体の場合**。H.264、H.265、または AV1 を使用したフルスクリーンで Thinwire を提供し、3D グラフィックを多用する場合のユーザーエクスペリエンスと帯域幅の向上を最適化します。H.264 4:2:0 の場合（**視覚的にロスレス**ポリシーが無効になっている場合）、最終画像はピクセルパーフェクト（ロスレス）ではなく、特定のシナリオには適さない可能性があります。そのような場合は、代わりに H.264 Build to lossless または H.265 Build to lossless の使用を検討してください。



以下の視覚表示ポリシー設定を含む、さまざまな他のポリシー設定を使用して、ディスプレイリモート処理テクノロジーのパフォーマンスを微調整できます。Thinwire はそれらすべてをサポートしています。

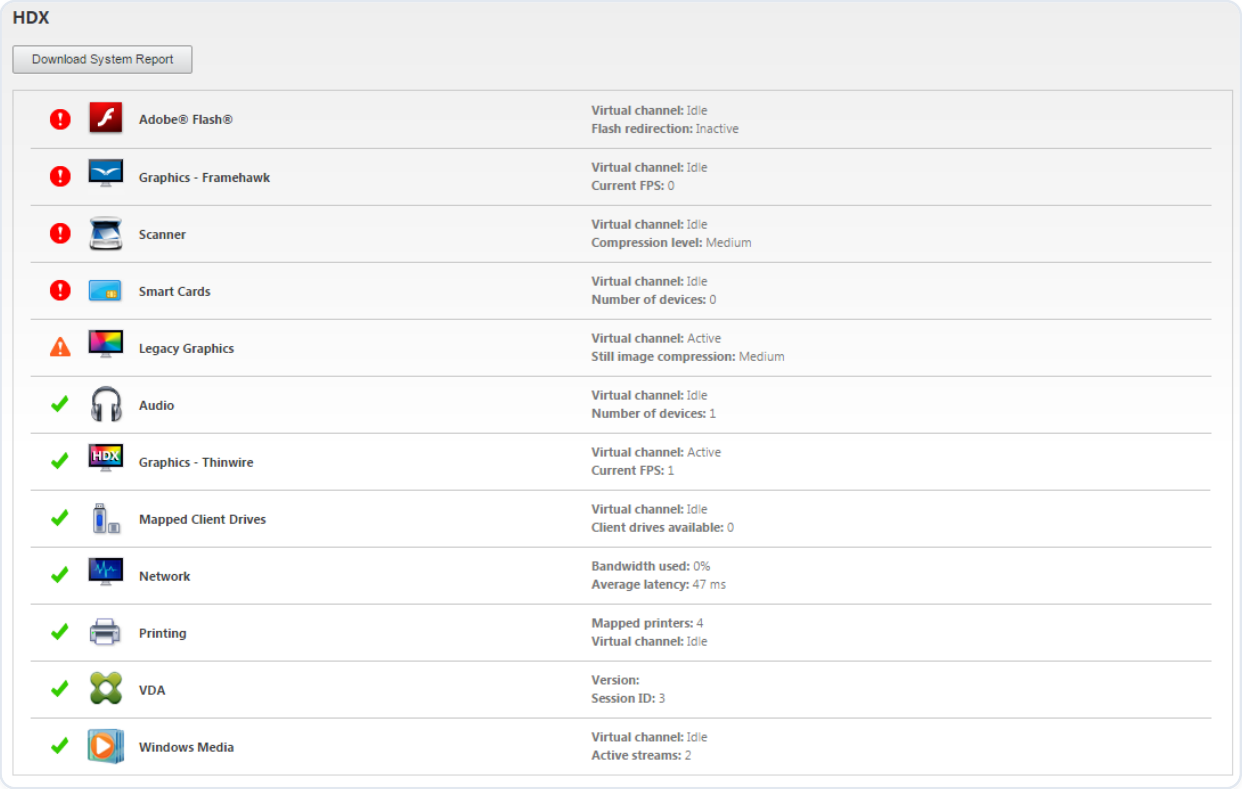
- 単純なグラフィックの優先色深度
- ターゲットフレームレート
- 視覚的品質

さまざまなビジネスユースケースに対応する Citrix 推奨のポリシー設定の組み合わせを取得するには、組み込みの Citrix ポリシーテンプレート を使用します。**高サーバー拡張性**および**超高精細ユーザーエクスペリエンス**テンプレートは、組織の優先順位とユーザーの期待に最適なポリシー設定の組み合わせで Thinwire を使用します。

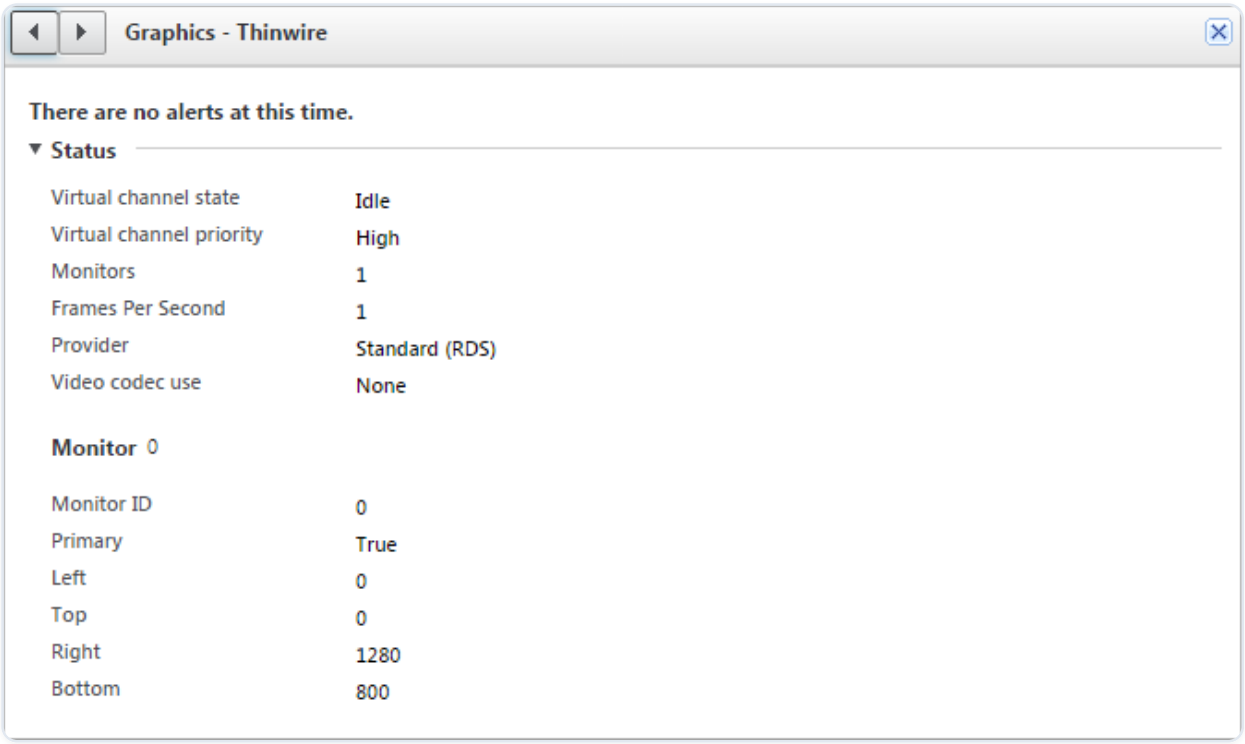
Thinwire の監視

Citrix DirectorからThinwireの使用状況とパフォーマンスを監視できます。HDX仮想チャネルの詳細ビューには、任意のセッションでThinwireのトラブルシューティングと監視に役立つ情報が含まれています。Thinwire関連のメトリックを表示するには：

1. Directorで、ユーザー、マシン、またはエンドポイントを検索し、アクティブなセッションを開いて**Details**をクリックします。または、**Filters** > **Sessions** > **All Sessions**を選択し、アクティブなセッションを開いて**Details**をクリックすることもできます。
2. **HDX**パネルまでスクロールします。



3. **Graphics - Thinwire**を選択します。



ロスレス圧縮コーデック（MDRLE）

一般的なデスクトップセッションでは、ほとんどの画像は単純なグラフィックまたはテキスト領域です。Thinwireはこれらの領域を特定し、2DRLEコーデックを使用してロスレスエンコーディングのためにこれらの領域を選択します。Citrix Workspaceアプリクライアント側では、これらの要素はセッション表示のためにCitrix Workspaceアプリ側の2DRLEデコーダーを使用してデコードされます。

XenApp and XenDesktop 7.17 では、2DRLE コーデックよりも一般的なデスクトップセッションで消費帯域幅が少ない、より高い圧縮率の MDRLE コーデックを追加しました。この新しいコーデックは、サーバーのスケーラビリティに影響を与えません。

帯域幅が低いということは、通常、セッションの対話性が向上し（特に共有リンクや制約のあるリンクの場合）、コストが削減されることを意味します。

MDRLE コーデックの構成は不要です。Citrix Workspace アプリが MDRLE デコードをサポートしている場合、VDA は VDA MDRLE エンコードと Citrix Workspace アプリ MDRLE デコードを使用します。Citrix Workspace アプリが MDRLE デコードをサポートしていない場合、VDA は自動的に 2DRLE エンコードにフォールバックします。

MDRLE の要件:

- Citrix Virtual Apps and Desktopsの最小バージョン7 1808 VDA
- XenAppおよびXenDesktopの最小バージョン7.17 VDA

- Windows向けCitrix Workspaceアプリの最小バージョン1808
- Citrix Receiver for Windows の最小バージョン 4.11

プログレッシブモード

Citrix Virtual Apps and Desktops 1808 では、プログレッシブモードが導入され、デフォルトで有効になりました。ネットワーク条件が制限されている場合（デフォルト：帯域幅 < 2 Mbps、または遅延 > 200 ms）、Thinwire は画面アクティビティ中のインタラクティブ性を向上させるために、テキストと静止画像の圧縮を強化しました。高圧縮されたテキストと画像は、画面アクティビティが停止すると、ランダムなブロック形式で段階的にシャープ化されます。このように圧縮とシャープ化を行うことで、全体的なインタラクティブ性は向上しますが、キャッシュ効率が低下し、帯域幅の使用量が増加します。

Citrix Virtual Apps and Desktops 1906 以降、プログレッシブモードはデフォルトで無効になっています。現在、当社は異なるアプローチを使用しています。静止画の品質はネットワーク条件に基づいており、各**視覚品質**設定の事前定義された最小値と最大値の間で変動します。明示的なシャープ化ステップがないため、Thinwire は画像配信を最適化し、キャッシュ効率を維持しながら、プログレッシブモードのほぼすべての利点を提供します。

プログレッシブモードの動作の変更

レジストリキーを使用してプログレッシブモードの状態を変更できます。詳細については、レジストリを介して管理される機能のリストにあるプログレッシブモードを参照してください。

ビルド・トゥ・ロスレス

ビルド・トゥ・ロスレスは、インタラクティブ性と最終的な画質のためにグラフィック配信を最適化する特別なThinwire構成です。この設定は、**視覚品質**ポリシーを**ビルド・トゥ・ロスレス**に設定することで有効にできます。

ビルド・トゥ・ロスレスは、画面アクティビティ中にH.264、H.265、またはAV1を使用して画面を圧縮し、アクティビティが停止するとピクセルパーフェクト（ロスレス）にシャープ化します。非可逆の画質は、利用可能なリソースに適応して、可能な限り最高のフレームレートを維持します。シャープ化ステップは段階的に実行されます。たとえば、モデルを選択して回転させる場合などです。

ビルド・トゥ・ロスレスは、ハードウェアアクセラレーションを含む画面全体にビデオコーデックを使用するすべての利点を提供しますが、最終的に保証されたロスレス画面という追加の利点があります。これは、最終的なピクセルパーフェクトな画像を必要とする3Dタイプのワークロードにとって重要です。たとえば、医療画像の操作などです。また、H.264 **ビルド・トゥ・ロスレス**は、フルスクリーンH.264 4:4:4よりも少ないリソースを使用します。その結果、**ビルド・トゥ・**

ロスレスを使用すると、通常、視覚的にロスレスなH.264 4:4:4よりも高いフレームレートが得られます。

> **注:**
>
> ビルド・トゥ・ロスレスを使用している場合、ビデオコーデックの使用を無効にできます。**ビデオコーデックの使用**ポリシーを`Do not use video codec`に設定するだけです。これにより、動画は代わりにアダプティブJPEGでエンコードされます。

視覚的にロスレスなエンコーディング

視覚的にロスレスなエンコーディングは、ビデオコーデック圧縮にクロマサブサンプリングされたYUV 4:2:0カラースペースではなく、YUV 4:4:4カラースペースを使用します。これにより、カラースペース変換中に色情報が失われることがなく、デコード後には元のRGB画像と視覚的に区別できなくなります。

次の例を考えてみましょう。ビデオコーデックを使用して画面全体を圧縮する場合、4:2:0の色圧縮はテキストのような高コントラストの詳細を劣化させ、ぼやけて読みにくくする可能性があります。対照的に、4:4:4はほぼすべての色情報を保持し、視覚的に認識できる劣化を示しません。

ロスレスグラフィックス(/en-us/citrix-virtual-apps-desktops/2411/media/lossless-image-graphics.png)

ピクセルパーフェクトな品質や正確な色表示を必要とするワークロードは、視覚的にロスレスなエンコーディングの恩恵を受けることができます。

視覚的にロスレスなエンコーディングは、H.264とH.265の両方で利用可能です。H.264 4:4:4エンコーディングは純粋なソフトウェアベースのソリューションであるため、VDAとクライアントの両方でCPU使用率に大きな影響を与える可能性があります。これにより、フレームレートにも影響が出る場合があります。

H.265 4:4:4のサポートはCitrix Workspaceアプリ2305のリリースで追加され、ThinwireがH.265 4:4:4エンコーディングのためにVDAとクライアントの両方でGPUを使用できるようになり、パフォーマンスが大幅に向上しました。

視覚的にロスレスな4:4:4エンコーディングを許可するには、2つのポリシーを有効にする必要があります。

- **Visual Quality**: `Build to Lossless`または`Always Lossless`に設定
- **視覚的ロスレスを許可**: `Enabled`に設定

注:

「**視覚的にロスレスを許可**」が有効になっていない場合、Thinwireエンコーダーは`Build to lossless`または`Always Lossless`に切り替わります。

H.265 4:4:4視覚的にロスレスには、追加の要件があります。

- NVIDIA GPUにはVDAバージョン2209以降が必要
- Intel GPUにはVDAバージョン2308以降が必要

H.265 4:4:4でサポートされているGPUは次のとおりです。

- NVIDIA Pascal世代以降のGPU
- Intel 第10世代以降のGPU

クライアントには、Citrix Workspaceアプリ for Windows バージョン2305が必要です（バージョン2309.1を推奨）。

H.265 4:4:4 のハードウェアデコードは、以下のクライアントデバイスの GPU で可能です。

- NVIDIA Turing世代以降のGPU
- Intel 第10世代以降のGPU

テキストベースのセッションウォーターマーク

テキストベースのセッションウォーターマークは、データ盗難を抑止し、追跡を可能にするのに役立ちます。この追跡可能な情報は、写真やスクリーンキャプチャを使用してデータを盗む者への抑止力として、セッションデスクトップに表示されます。元のドキュメントの内容を変更することなく、セッション画面全体に表示されるテキストのレイヤーであるウォーターマークを指定できます。テキストベースのセッションウォーターマークにはVDAのサポートが必要です。

重要:

テキストベースのセッションウォーターマークはセキュリティ機能ではありません。このソリューションはデータ盗難を完全に防ぐものではありませんが、ある程度の抑止力と追跡可能性を提供します。この機能を使用しても情報の完全な追跡可能性を保証するものではあり

> ませんが、必要に応じて他のセキュリティソリューションと組み合わせて使用することをお勧めします。

> セッションウォーターマークはテキストであり、ユーザーに配信されるセッションに適用されます。セッションウォーターマークには、データ盗難を追跡するための情報が含まれています。最も重要なデータは、スクリーンイメージが取得された現在のセッションのログオンユーザーのIDです。データ漏洩をより効果的に追跡するには、サーバーまたはクライアントのインターネットプロトコルアドレスや接続時間などの他の情報を含めます。

ユーザーエクスペリエンスを調整するには、セッションウォーターマークポリシー設定 を使用して、画面上の配置とウォーターマークの外観を構成します。

要件:

仮想配信エージェント:

マルチセッションOS 7.17 シングルセッションOS 7.17

制限事項:

- ローカルアプリアクセス、Windowsメディアリダイレクト、MediaStream、ブラウザコンテンツリダイレクト、およびHTML5ビデオリダイレクトが使用されているセッションでは、セッションウォーターマークはサポートされていません。セッションウォーターマークを使用するには、これらの機能が無効になっていることを確認してください。
- セッションが全画面ハードウェアアクセラレーションモード（全画面H.264またはH.265エンコーディング）で実行されている場合、セッションウォーターマークはサポートされず、表示されません。
- これらのHDX™ポリシーを設定すると、ウォーターマーク設定は有効にならず、セッション表示にウォーターマークは表示されません。

ビデオコーデックにハードウェアエンコーディングを使用 を **有効 圧縮にビデオコーデックを使用** を **画面全体**

- これらのHDXポリシーを設定すると、動作は未定義となり、ウォーターマークが表示されない場合があります。

  ビデオコーデックにハードウェアエンコーディングを使用する を **有効 圧縮にビデオコーデックを使用する** を **優先する場合にビデオコーデックを使用する**

ウォーターマークが表示されるようにするには、**ビデオコーデックにハードウェアエンコーディングを使用する** を **無効** に設定するか、**圧縮にビデオコーデックを使用する** を **アクティブに変化する領域の場合** または **ビデオコーデックを使用しない** に設定します。

- セッションウォーターマークは、Thinwireグラフィックモードのみをサポートします。
- セッション録画を使用している場合、録画されたセッションにはウォーターマークは含まれません。
- Windowsリモートアシスタンスを使用している場合、ウォーターマークは表示されません。
- ユーザーが画面をキャプチャするために**Print Screen**キーを押した場合、VDA側でキャプチャされた画面にはウォーターマークは含まれません。キャプチャされた画像がコピーされないように対策を講じることをお勧めします。

画面共有

画面共有により、ユーザーはCitrix Virtual Desktopセッションを、画面コンテンツ、キーボード、マウスコントロールを含めて他のユーザーと共有できます。

システム要件

- Windows: シングルセッションまたはマルチセッションOS VDA
- Linux: Linuxセッションの共有に関する詳細については、Linux VDAドキュメントを参照してください。
- 共有できるのはデスクトップセッションのみです。
- セッションをホストするVDAと、共有セッションに接続するマシンとの間にネットワーク接続が必要です。ネットワークポート要件は、使用中のICAポート（TCP/UDP 1494または2598）と、画面共有ポリシーの構成（デフォルトでTCP 52525〜52625）に基づいています。

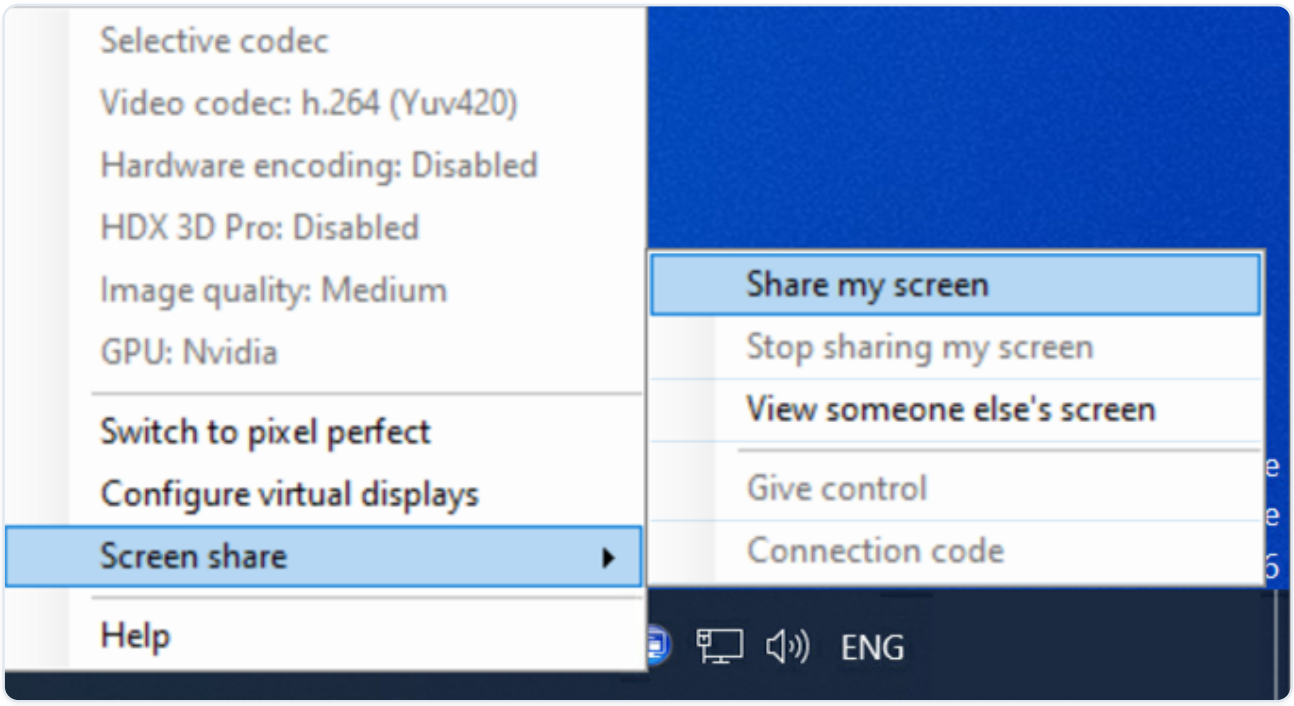
構成

画面共有はCitrixポリシーを使用して有効にする必要があります。画面共有はデフォルトで無効になっています。screen sharing policyを構成して、この機能を有効または無効にし、使用可能なネットワークポート範囲を割り当てます。

セッションの共有と接続のためのコントロールを含むユーザーインターフェイスを表示するには、グラフィックステータスインジケーターポリシーを有効にします。

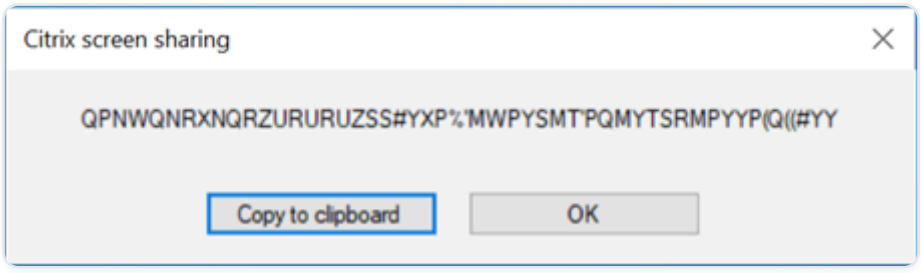
セッションの共有

セッションを共有するには、Windowsの通知領域にあるHDX™グラフィックステータスインジケーターアイコンを探します。アイコンを右クリックしてメニューを表示し、**画面共有 > 自分の画面を共有**を選択します。



クリップボードにコピーをクリックするか、ダイアログボックスに表示されている文字列全体を手動で選択してコピーします。この文字列は、電子メールやIMクライアントなど、選択したアプリケーションに貼り付けて、他のユーザーに配布できます。

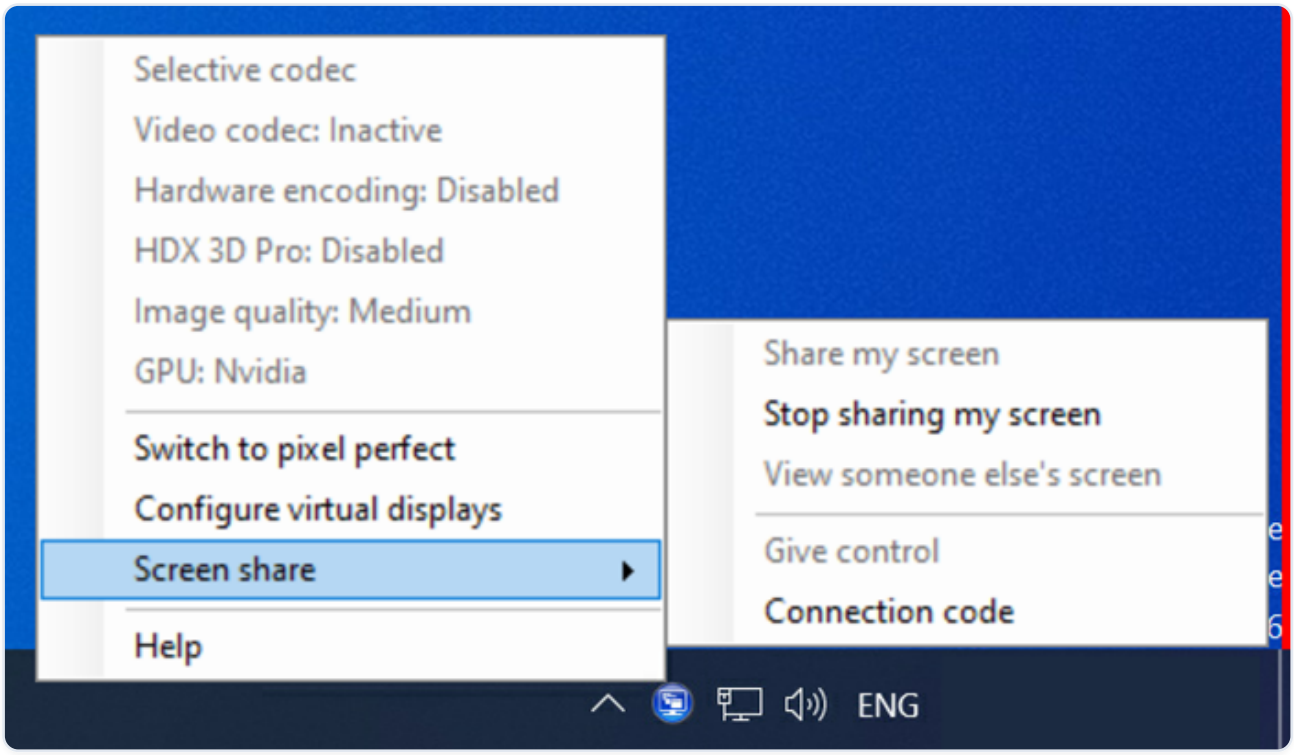
OKまたは**x**をクリックしてダイアログボックスを閉じます。セッションが共有されている間はいつでも、**Screen share > Connection code**メニューオプションから接続コードを取得できます。



セッションが共有されており、他のユーザーから表示されていることを示す赤い枠線が画面の周囲に表示されます。

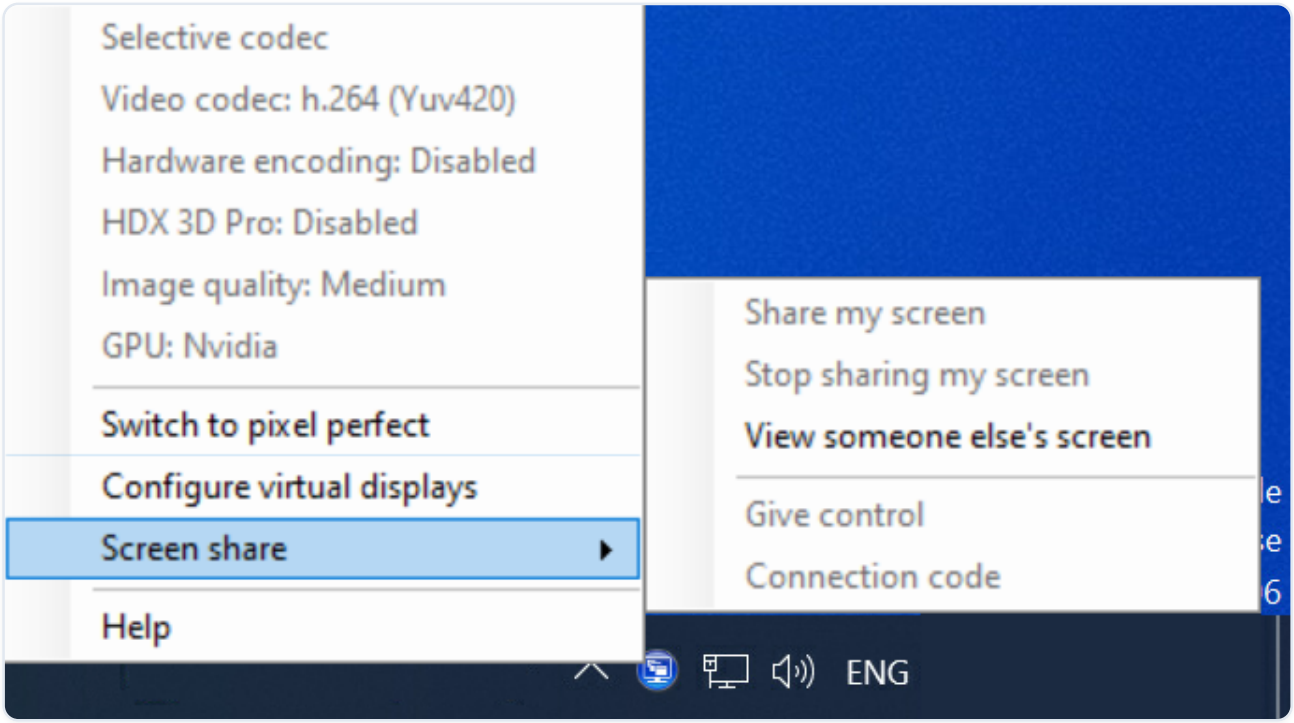
キーボードとマウスのコントロールも、**画面共有 > 制御を付与** メニューオプションを使用して他のユーザーと共有できます。

セッションの共有を停止し、すべてのユーザーを切断するには、**画面共有 > 自分の画面の共有を停止** メニューオプションを使用します。



共有セッションへの接続

他のユーザーのセッションに接続するには、Windowsの通知領域にあるHDXグラフィックステータスインジケーターアイコンを探します。それを右クリックしてメニューを表示し、**画面共有 > 他のユーザーの画面を表示**を選択します。



セッションを共有しているユーザーから提供された接続文字列をテキストボックスに入力または貼り付けます。**接続**をクリックして接続を確立します。

画面共有 5(/en-us/citrix-virtual-apps-desktops/2411/media/screen-sharing-5.png)

HDX 画面共有ビューア ウィンドウの左上隅にあるマウスアイコンをクリックすると、キーボードとマウスのコントロールを要求できます。

いつでも共有セッションから切断するには、**HDX画面共有ビューア**ウィンドウを閉じます。

画面共有 6(/en-us/citrix-virtual-apps-desktops/2411/media/screen-sharing-6.png)

その他の考慮事項

- 画面共有ビューアアプリケーションは、VDA に *C:\Program Files\Citrix\HDX\bin\TwPlayer.exe* として含まれており、Virtual Apps Server を使用して公開アプリケーションとして展開される場合があります。この代替展開モデルにより、仮想デスクトップにアクセスできないユーザーとのコラボレーションが可能になります。
- 共有セッションに接続できるユーザー数は、画面共有ポリシーのネットワークポート範囲を使用して制限できます。ユーザーごとに1つのポートが必要です。デフォルトの範囲では、最大100人のユーザーが許可されます。
- セッションに接続されているすべてのモニターが共有されます。個々のモニターを選択することはできません。
- H.265ビデオコーデックはサポートされていません。

アダプティブ リフレッシュレート

新しいスケーラビリティの向上により、HDX™ は仮想モニターのリフレッシュ レートを、設定されたターゲット FPS ポリシーに合わせて調整します。アダプティブ リフレッシュ レート (ARR) は、シングルセッション VDA とマルチセッション VDA の両方で利用でき、GPU アクセラレーションが有効なシナリオとそうでないシナリオの両方で機能します。

ターゲットフレームレート(/en-us/citrix-virtual-apps-desktops/2411/media/targetframerate_60.png)

DirectX診断ツール(/en-us/citrix-virtual-apps-desktops/2411/media/directx-diagnostic-tool.png)

> **注**
>
> アダプティブ リフレッシュレートは、Citrix Indirect DisplayまたはIDDが使用されている場合（Citrix Virtual Apps and Desktops™のデフォルトによる）にのみ利用可能であり、ベンダー提供のディスプレイアダプターを使用している場合は利用できません。

ロス許容モード

グラフィックのロストレラントモードは、パケットロスが検出されたときにセッションがインタラクティブな状態を維持するように、徹底的に再設計されました。ネットワークの状態が、事前に定義された帯域幅、遅延、およびパケットロスのしきい値を超えて悪化すると、Citrix®グラフィックエンコーダーは、パケットロスの影響を克服するため、自動的にパケット配信のより積極的なモードに切り替わります。その結果、帯域幅の使用量はパケットロスの量に比例して増加します。その後、状況が改善すると、Citrixグラフィックエンコーダーはシームレスに元に戻ります。しきい値はポリシーを介して構成でき、デフォルトは300ミリ秒の遅延と5%のパケットロスです。

現在、Windows 2311向けCitrix Workspace™アプリがサポートされています。他のプラットフォームのサポートは、今後のCitrix Workspaceアプリリリースで追加される予定です。この機能の以前のバージョンと同様に、この機能が動作するには、HDX™ Adaptive Transport (EDT) を有効にする必要があります。さらに、Citrix Gateway Service経由で接続する場合、グラフィックのロストレラントモードもGatewayで有効にする必要があります。

マルチメディア

HDX™ テクノロジースタックは、2つの補完的なアプローチを通じてマルチメディアアプリケーションの配信をサポートします。

- サーバー側レンダリングによるマルチメディア配信
- クライアント側レンダリングによるマルチメディアリダイレクト

この戦略により、優れたユーザーエクスペリエンスで幅広いマルチメディア形式を配信できると同時に、サーバーのスケーラビリティを最大化してユーザーあたりのコストを削減できます。

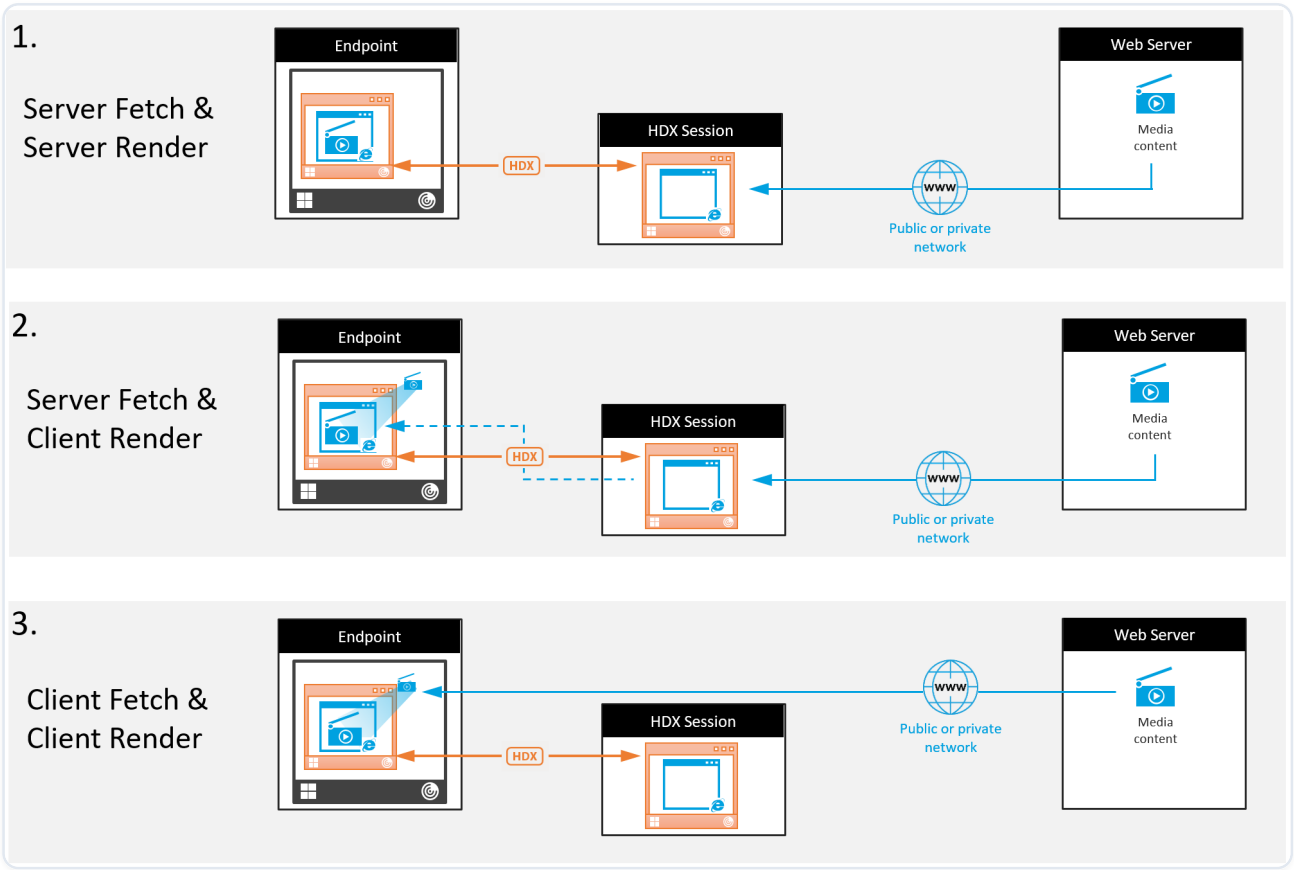
サーバーレンダリングによるマルチメディア配信では、オーディオおよびビデオコンテンツは、アプリケーションによってCitrix Virtual Apps and Desktopsサーバー上でデコードおよびレンダリングされます。その後、コンテンツは圧縮され、ICAプロトコルを使用してユーザーデバイス上のCitrix Workspaceアプリに配信されます。この方法により、さまざまなアプリケーションおよびメディア形式との互換性が最高レベルで提供されます。ビデオ処理は計算負荷が高いため、サーバーレンダリングによるマルチメディア配信は、オンボードのハードウェアアクセラレーションから大きな恩恵を受けます。たとえば、DirectX Video Acceleration (DXVA) のサポートにより、H.264デコードを別のハードウェアで実行することでCPUの負荷が軽減されます。Intel Quick Sync、AMD RapidFire、NVIDIA NVENCテクノロジーは、ハードウェアアクセラレーションによるH.264エンコーディングを提供します。

ほとんどのサーバーはビデオ圧縮用のハードウェアアクセラレーションを提供しないため、すべてのビデオ処理がサーバーCPUで行われると、サーバーのスケーラビリティに悪影響が及びます。多くのマルチメディア形式をローカルレンダリングのためにユーザーデバイスにリダイレクトすることで、高いサーバーのスケーラビリティを維持できます。

- Windows Mediaリダイレクトは、通常Windows Media Playerに関連付けられているさまざまなメディア形式について、サーバーの負荷を軽減します。
- HTML5ビデオは普及しており、Citrix®はこの種のコンテンツ向けにリダイレクトテクノロジーを導入しました。HTML5、HLS、DASH、またはWebRTCを使用するWebサイトには、ブラウザコンテンツリダイレクトをお勧めします。
- 一般的なコンテンツリダイレクトテクノロジーであるホストからクライアントへのリダイレクトとローカルアプリアクセスをマルチメディアコンテンツに適用できます。

これらのテクノロジーをまとめると、リダイレクトを構成しない場合、HDXはサーバー側レンダリングを実行します。 リダイレクトを構成すると、HDXはサーバーフェッチとクライアントレンダリング、またはクライアントフェッチとクライアントレンダリングのいずれかを使用します。これらの方法が失敗した場合、HDXは必要に応じてサーバー側レンダリングにフォールバックし、フォールバック防止ポリシーの対象となります。

シナリオ例



シナリオ1. (サーバーフェッチとサーバーレンダリング):

1. サーバーはソースからメディアファイルを取得し、デコードしてから、オーディオデバイスまたはディスプレイデバイスにコンテンツを提示します。
2. サーバーは、表示デバイスまたはオーディオデバイスから、それぞれ提示された画像またはサウンドを抽出します。
3. サーバーはオプションでそれを圧縮し、クライアントに送信します。

このアプローチでは、高いCPUコスト、高い帯域幅コスト（抽出された画像/音声が効率的に圧縮されていない場合）、および低いサーバー拡張性が発生します。

Thinwireおよびオーディオ仮想チャネルがこのアプローチを処理します。このアプローチの利点は、クライアントのハードウェアおよびソフトウェア要件を削減できることです。このアプローチ

を使用すると、デコードはサーバーで行われ、より幅広い種類のデバイスとフォーマットで動作します。

シナリオ2。（サーバーフェッチとクライアントレンダリング）：

このアプローチは、メディアコンテンツがデコードされてオーディオまたはディスプレイデバイスに提示される前に、それを傍受できることに依存しています。圧縮されたオーディオ/ビデオコンテンツは代わりにクライアントに送信され、そこでデコードされてローカルで提示されます。このアプローチの利点は、処理がクライアントデバイスにオフロードされ、サーバーのCPUサイクルを節約できることです。

しかし、これはクライアントに追加のハードウェアおよびソフトウェア要件も導入します。クライアントは、受信する可能性のある各フォーマットをデコードできる必要があります。

シナリオ3。（クライアントフェッチとクライアントレンダリング）：

このアプローチは、メディアコンテンツのURLがソースからフェッチされる前にそれを傍受できることに依存しています。URLはクライアントに送信され、そこでメディアコンテンツがフェッチ、デコード、およびローカルで提示されます。このアプローチは概念的にシンプルです。その利点は、サーバーが制御コマンドのみを送信するため、サーバーのCPUサイクルと帯域幅の両方を節約できることです。ただし、メディアコンテンツが常にクライアントからアクセスできるとは限りません。

フレームワークとプラットフォーム：

シングルセッションオペレーティングシステム（Windows、Mac OS X、Linux）は、マルチメディアアプリケーションのより迅速な開発を可能にするマルチメディアフレームワークを提供します。この表は、より一般的なマルチメディアフレームワークの一部をリストしています。各フレームワークは、メディア処理をいくつかの段階に分け、パイプラインベースのアーキテクチャを使用します。

フレームワーク	プラットフォーム
DirectShow	Windows (98以降)
メディアファンデーション	ウィンドウズ (ビスタ以降)
Gストリーマー	リナックス
クイックタイム	マック オーエス テン

メディアリダイレクト技術によるダブルホップサポート

オーディオリダイレクト	いいえ
ブラウザコンテンツリダイレクト	いいえ
HDX Webカメラリダイレクト	はい
HTML5ビデオのリダイレクト	はい
Windows Mediaリダイレクト	はい

オーディオ機能

HDXオーディオ機能を最適化するポリシーに、以下のCitrixポリシー設定を構成して追加できます。使用方法の詳細、および他のポリシー設定との関係と依存関係については、「オーディオポリシー設定」、「帯域幅ポリシー設定」、および「マルチストリーム接続ポリシー設定」を参照してください。

アダプティブオーディオ

アダプティブオーディオを使用すると、VDAでオーディオ品質ポリシーを手動で構成する必要がありません。アダプティブオーディオは、環境に合わせて設定を最適化し、古いオーディオ圧縮形式を置き換えて、優れたユーザーエクスペリエンスを提供します。

アダプティブオーディオはデフォルトで有効になっています。アダプティブオーディオを無効にするには、「オーディオポリシー設定」を参照してください。

重要:

リアルタイムオーディオアプリケーションが必要な場合、Citrix®はTCPではなくUser Datagram Protocol (UDP) を使用してオーディオを配信することを推奨します。UDP経由で利用できるオーディオトランスポートオプションは次のとおりです。

- UDP経由のオーディオ
- HDX™アダプティブトランスポート (Enlightened Data Transport)

DTLSを使用したUDPオーディオ暗号化は、Citrix GatewayとCitrix Workspace™アプリの間でのみ利用可能です。そのため、TCPトランスポートを使用する方が望ましい場合があります。TCPは、VDAからCitrix Workspaceアプリへのエンドツーエンドの TLS暗号化をサポートしています。

アダプティブオーディオとUDPオーディオの詳細については、「UDP経由のリアルタイムオーディオトランスポートとオーディオUDPポート範囲」を参照してください。

オーディオの損失許容モード

損失許容モードはオーディオをサポートします。この機能は、リアルタイムストリーミングのユーザーエクスペリエンスを向上させ、高遅延およびパケット損失のあるネットワーク経由でユーザーが接続している場合に、EDT経由のオーディオ品質を改善します。この機能はデフォルトで無効になっています。

注:

この機能が動作するには、**HDXアダプティブトランスポート (EDT)** と**オーディオの損失許容モード**の両方のポリシーを有効にする必要があります。

システム要件

以下の製品が、損失許容モードをサポートする最小バージョンであることを確認してください。

- シトリックス バーチャル デリバリー エージェント (VDA) 2308
- Citrix Workspace アプリ Windows用 2309

さらに、以下の機能を有効にする必要があります。

- HDX Adaptive Transportポリシー。
- (オプション) リモート接続の場合、Citrix Gateway Service が必要です。

注:

上記の条件が満たされない場合、オーディオはEDT Reliableトランスポート経由で送信されます。

追加情報

損失許容モードは、マルチメディアコンテンツを再送信することなく伝送中のパケット損失を許容する損失許容トランスポートプロトコルであり、ユーザーによりリアルタイムなエクスペリエンスをもたらします。

Enlightened Data Transport (EDT) は、Citrix 独自のトランスポートプロトコルであり、サーバーのスケーラビリティを維持しながら、困難な長距離接続で優れたユーザーエクスペリエンスを提供します。損失許容モードは、ネットワークの混雑時でも安定した接続を維持するために、損失許容モードをトランスポートプロトコルとして使用するCitrix Gatewayサービスの機能です。これにより、リモートワーカーに一貫した安定したエクスペリエンスが保証されます。通常の状態では、EDTと損失許容モードの両方が同様の結果を提供します。ただし、パケット損失のあるネットワーク状況では、損失許容モードはEDTと比較してより優れたオーディオエクスペリエンスを提供します。これにより、リアルタイムマルチメディアに依存するリモートワーカーにとって不可欠な機能となります。

オーディオ品質

一般的に、音質が高いほど、より多くのオーディオデータをユーザーデバイスに送信するため、より多くの帯域幅とサーバーCPU使用率を消費します。サウンド圧縮を使用すると、音質とセッション全体のパフォーマンスのバランスを取ることができます。Citrixポリシー設定を使用して、サウンドファイルに適用する圧縮レベルを構成します。

デフォルトでは、TCPトランスポートが使用される場合、**オーディオ品質ポリシー**設定は「高 - 高精細オーディオ」に設定されています。UDPトランスポート（推奨）が使用される場合、ポリシーは「中 - 音声に最適化」に設定されます。**高精細オーディオ**設定は、高忠実度のステレオオーディオを提供しますが、他の品質設定よりも多くの帯域幅を消費します。最適化されていないボイスチャットまたはビデオチャットアプリケーション（ソフトフォンなど）には、このオーディオ品質を使用しないでください。その理由は、リアルタイム通信に適さない遅延をオーディオパスに導入する可能性があるためです。選択されたトランスポートプロトコルに関係なく、リアルタイムオーディオには音声に最適化されたポリシー設定を推奨します。

帯域幅が制限されている場合（衛星接続やダイヤルアップ接続など）は、オーディオ品質を**低**に下げると、消費される帯域幅が最小限になります。この状況では、高帯域幅接続のユーザーが悪影響を受けないように、低帯域幅接続のユーザーに対して個別のポリシーを作成してください。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでClient audio settingsを有効にすることを忘れないでください。

オーディオ再生と録音の帯域幅ガイドライン：

- アダプティブオーディオ（デフォルト）
  - ビットレート: 可変アダプティブ
  - チャンネル数: 再生用2（ステレオ）、マイクキャプチャ用1（モノラル）
  - 周波数: 48000 Hz
  - ビット深度: 16ビット
- 高音質
  - ビットレート: 再生用約100 kbps（最小75、最大175 kbps）/ マイクキャプチャ用約70 kbps
  - チャンネル数: 再生用2（ステレオ）、マイクキャプチャ用1（モノラル）
  - 周波数: 44100 Hz
  - ビット深度: 16ビット
- 中音質（VoIPに推奨）
  - ビットレート: 再生用約16 kbps（最小20、最大40 kbps）、マイクキャプチャ用約16 kbps
  - チャンネル数: 再生とキャプチャの両方で1 (モノラル)
  - 周波数: 16000 Hz (広帯域)
  - ビット深度: 16ビット
- 低品質
  - ビットレート: 再生で約11 kbps (最小10; 最大25 kbps)、マイクキャプチャで約11 kbps
  - チャンネル数: 再生とキャプチャの両方で1 (モノラル)
  - 周波数: 8000 Hz (狭帯域)
  - ビット深度: 16ビット

クライアントオーディオリダイレクト

ユーザーがサーバー上のアプリケーションからのオーディオを、ユーザーデバイスのスピーカーまたはその他のサウンドデバイスを介して受信できるようにするには、**クライアントオーディオリダイレクト**設定を**許可**のままにします。これがデフォルトです。

クライアントオーディオマッピングは、サーバーとネットワークに余分な負荷をかけます。ただし、クライアントオーディオリダイレクトを禁止すると、すべてのHDXオーディオ機能が無効になります。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

クライアントマイクのリダイレクト

ユーザーがユーザーデバイス上のマイクなどの入力デバイスを使用してオーディオを録音できるようにするには、**クライアントマイクのリダイレクト**設定をデフォルト（許可）のままにします。

セキュリティのため、ユーザーデバイスは、信頼できないサーバーがマイクへのアクセスを試みた場合に、ユーザーに警告します。ユーザーはマイクを使用する前に、アクセスを許可するか拒否するかを選択できます。ユーザーはCitrix Workspaceアプリでこの警告を無効にできます。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

オーディオプラグアンドプレイ

オーディオプラグアンドプレイポリシー設定は、複数のオーディオデバイスを使用してサウンドを録音および再生することを許可または禁止します。この設定は、デフォルトで**有効**になっています。オーディオプラグアンドプレイにより、オーディオデバイスが認識されるようになります。デバイスは、ユーザーセッションが開始された後に接続されていなくても認識されます。

この設定は、WindowsマルチセッションOSマシンにのみ適用されます。

設定の詳細については、「オーディオポリシー設定」を参照してください。

オーディオリダイレクト帯域幅制限とオーディオリダイレクト帯域幅制限の割合

オーディオリダイレクト帯域幅制限ポリシー設定は、セッションでのオーディオの再生と録音の最大帯域幅（キロビット/秒）を指定します。

オーディオリダイレクト帯域幅制限の割合設定は、オーディオリダイレクトの最大帯域幅を、利用可能な総帯域幅の割合として指定します。

デフォルトでは、両方の設定でゼロ（最大なし）が指定されています。両方の設定が構成されている場合、帯域幅制限が最も低い方が使用されます。

設定の詳細については、「帯域幅ポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

UDPリアルタイムトランスポート経由のオーディオとオーディオUDPポート範囲

デフォルトでは、ユーザーデータグラムプロトコル（UDP）リアルタイムトランスポート経由のオーディオは許可されています（インストール時に選択した場合）。これにより、UDPリアルタイムトランスポート経由のオーディオを使用する接続のために、サーバー上にUDPポートが開かれます。ネットワークの混雑やパケット損失がある場合は、可能な限り最高のユーザーエクスペリエンスを確保するために、オーディオにUDP/RTPを構成することをお勧めします。ソフトフォンアプリケーションなどのリアルタイムオーディオの場合、UDPオーディオはEDTよりも推奨されます。UDPは再送信なしでパケット損失を許容するため、パケット損失が多い接続で遅延が追加されないようにします。

重要:

Citrix Gatewayが経路にない場合、UDPで送信されるオーディオデータは暗号化されません。Citrix GatewayがCitrix Virtual Apps and Desktops™リソースにアクセスするように構成されている場合、エンドポイントデバイスとCitrix Gateway間のオーディオトラフィックはDTLSプロトコルを使用して保護されます。

オーディオUDPポート範囲は、Windows VDAがユーザーデバイスとオーディオパケットデータを交換するために使用するポート番号の範囲を指定します。

デフォルトでは、範囲は16500から16509です。

注:

アダプティブオーディオにAudio over UDP Real-time Transportが不要な場合、Citrixはポリシー設定を「無効」に構成することを推奨します。これにより、Citrix Workspaceアプリクライアントがオープンな UDP接続を要求したり、不要なCitrix Workspaceアプリクライアントのファイアウォール構成ダイアログウィンドウが表示されたりするのを防ぐことができます。

Audio over UDP Real-time Transportの設定の詳細については、「オーディオポリシー設定」を参照してください。オーディオUDPポート範囲の詳細については、「マルチストリーム接続ポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

Audio over UDPにはWindows VDAが必要です。Linux VDAでサポートされているポリシーについては、「ポリシーサポートリスト」を参照してください。

ユーザーデバイスのオーディオ設定ポリシー

1. 「グループポリシーオブジェクト管理用テンプレートの構成」に従って、グループポリシーテンプレートをロードします。
2. グループポリシーエディターで、**管理用テンプレート > Citrixコンポーネント > Citrix Workspace > ユーザーエクスペリエンス**を展開します。
3. **クライアントオーディオ設定**で、**未構成**、**有効**、または**無効**を選択します。
   - **未構成**。デフォルトでは、オーディオリダイレクトは高品質オーディオまたは以前に構成されたカスタムオーディオ設定を使用して有効になります。
   - **有効**。選択したオプションを使用してオーディオリダイレクトを有効にします。
   - **無効**。オーディオリダイレクトを無効にします。
4. **有効**を選択した場合、音質を選択します。UDPオーディオの場合は、**中**（デフォルト）を使用します。
5. UDPオーディオの場合のみ、**リアルタイムトランスポートを有効にする**を選択し、ローカルのWindowsファイアウォールで開く受信ポートの範囲を設定します。
6. Citrix GatewayでUDPオーディオを使用するには、**ゲートウェイ経由のリアルタイムトランスポートを許可する**を選択します。Citrix GatewayをDTLSで構成します。詳細については、「こちらの記事」を参照してください。

管理者として、これらの変更を行うためのエンドポイントデバイスを制御できない場合は、StoreFront の default.ica 属性を使用して UDP オーディオを有効にします。たとえば、BYOD (個人所有デバイス) や自宅のコンピューターの場合などです。

1. StoreFront マシンで、C:\inetpub\wwwroot\Citrix\\\<Store Name>\App_Data\default.ica をメモ帳などのエディターで開きます。
2. セクションの下に、次のエントリを作成します。

   ; このテキストはリアルタイムトランスポートを有効にします

   RTPオーディオを有効にする=true

   ; このテキストはゲートウェイ経由のリアルタイムトランスポートを許可します

   ゲートウェイ経由のUDPを有効にする=true

; このテキストはオーディオ品質を「中」に設定します

AudioBandwidthLimit=1

; UDP ポート範囲

RtpAudioLowestPort=16500

RtpAudioHighestPort=16509

default.ica を編集してユーザーデータグラムプロトコル (UDP) オーディオを有効にすると、そのストアを使用しているすべてのユーザーに対して UDP オーディオが有効になります。

マルチメディア会議中のエコーを回避する

オーディオ会議やビデオ会議の参加者はエコーを聞くことがあります。エコーは通常、スピーカーとマイクが互いに近すぎるときに発生します。そのため、オーディオ会議やビデオ会議にはヘッドセットの使用をお勧めします。

HDX は、エコーを最小限に抑えるエコーキャンセルオプション (デフォルトで有効) を提供します。エコーキャンセルの有効性は、スピーカーとマイクの間の距離に影響されます。デバイスが互いに近すぎたり遠すぎたりしないようにしてください。

レジストリ設定を変更して、エコーキャンセルを無効にできます。詳細については、レジストリで管理される機能のリストにある マルチメディア会議中のエコーを回避する を参照してください。

ソフトフォン

ソフトフォンは、電話インターフェースとして機能するソフトウェアです。ソフトフォンを使用して、コンピューターやその他のスマートデバイスからインターネット経由で電話をかけます。ソフトフォンを使用すると、画面を使って電話番号をダイヤルしたり、その他の電話関連機能を実行したりできます。

Citrix Virtual Apps and Desktops は、ソフトフォンを配信するためのいくつかの代替手段をサポートしています。

- **制御モード**。ホストされているソフトフォンが物理的な電話機を制御します。このモードでは、Citrix Virtual Apps and Desktops サーバーを介してオーディオトラフィックは流れません。
- **HDX RealTime 最適化ソフトフォンサポート (推奨)**。メディアエンジンはユーザーデバイス上で実行され、Voice over Internet Protocol トラフィックはピアツーピアで流れます。例については、以下を参照してください。

  - Microsoft Teams 向け HDX 最適化
  - Microsoft Skype for Business の配信を最適化する HDX RealTime Optimization Pack
  - Cisco Jabber Softphone for VDI (以前はVXMEとして知られていました)
  - VDI 用 シスコ Webex Meetings
  - Avaya VDI Equinox (以前はVDI Communicatorとして知られていました)
  - Zoom VDI プラグイン
  - ジェネシス ピュアエンゲージ クラウド
  - Nuance Dragon PowerMic ディクテーションデバイス

- **ローカルアプリアクセス**。ソフトフォンなどのアプリケーションをWindowsユーザーデバイス上でローカルに実行しながら、仮想/公開デスクトップとシームレスに統合されているように見せるCitrix Virtual Apps and Desktopsの機能です。この機能は、すべてのオーディオ処理をユーザーデバイスにオフロードします。詳細については、「ローカルアプリアクセスとURLリダイレクト」を参照してください。
- **HDX RealTime汎用ソフトフォンサポート。** ICA経由のVoice over Internet Protocol。

汎用ソフトフォンサポート

汎用ソフトフォンサポートにより、データセンターのXenAppまたはXenDesktopで、変更されていないソフトフォンをホストできます。オーディオトラフィックは、Citrix ICAプロトコル（できればUDP/RTPを使用）を介して、Citrix Workspaceアプリを実行しているユーザーデバイスに送信されます。

汎用ソフトフォンサポートは、HDX RealTimeの機能です。このソフトフォン配信アプローチは、特に次のような場合に役立ちます。

- ソフトフォンを配信するための最適化されたソリューションが利用できず、ユーザーがローカルアプリアクセスを使用できるWindowsデバイスを使用していない場合。
- ソフトフォンの最適化された配信に必要なメディアエンジンがユーザーデバイスにインストールされていないか、ユーザーデバイスで実行されているオペレーティングシステムのバージョンで利用できない場合。このシナリオでは、汎用HDX RealTimeが貴重なフォールバックソリューションを提供します。

Citrix Virtual Apps and Desktopsを使用する際のソフトフォン配信には、次の2つの考慮事項があります。

- ソフトフォンアプリケーションが仮想/公開デスクトップにどのように配信されるか。

- オーディオがユーザーのヘッドセット、マイク、スピーカー、またはUSB電話機にどのように配信され、そこからどのように送信されるか。

Citrix Virtual Apps and Desktopsには、汎用ソフトフォン配信をサポートするための多数のテクノロジーが含まれています。

- リアルタイムオーディオの高速エンコードと帯域幅効率のための、音声に最適化されたコーデック。
- 低遅延オーディオスタック。
- ネットワーク遅延が変動したときにオーディオをスムーズにするサーバー側のジッターバッファ。
- Quality of Serviceのためのパケットタグ付け（DSCPおよびWMM）。
    - RTPパケットのDSCPタグ付け (レイヤー3)
    - Wi-FiのWMMタグ付け

Windows、Linux、Chrome、Mac版のCitrix WorkspaceアプリもVoice over Internet Protocolに対応しています。Windows版Citrix Workspaceアプリには、以下の機能があります。

- クライアント側ジッターバッファ - ネットワーク遅延が変動しても、スムーズなオーディオを保証します。
- エコーキャンセル - ヘッドセットを使用しない作業者向けに、マイクとスピーカー間の距離の許容範囲を広げます。
- オーディオプラグアンドプレイ - セッションを開始する前にオーディオデバイスを接続する必要はありません。いつでも接続できます。
- オーディオデバイスルーティング - ユーザーは着信音をスピーカーに、音声パスをヘッドセットに送ることができます。
- マルチストリームICA - ネットワーク上で柔軟なQuality of Serviceベースのルーティングを可能にします。
- ICAは4つのTCPストリームと2つのUDPストリームをサポートします。UDPストリームの1つは、RTP経由のリアルタイムオーディオをサポートします。

Citrix Workspaceアプリの機能の概要については、「Citrix Receiver Feature Matrix」を参照してください。

システム構成の推奨事項

クライアントハードウェアとソフトウェア: 最適なオーディオ品質を得るには、最新バージョンのCitrix Workspaceアプリと、音響エコーキャンセル（AEC）機能を備えた高品質のヘッドセットをお勧めします。Windows、Linux、Mac版のCitrix WorkspaceアプリはVoice over Internet Protocolをサポートしています。また、Dell WyseはThinOS（WTOS）向けにVoice over Internet Protocolをサポートしています。

CPUに関する考慮事項: 各仮想マシンに2つの仮想CPUを割り当てる必要があるかどうかを判断するために、VDA上のCPU使用率を監視してください。リアルタイムの音声とビデオはデータ集約型です。2つの仮想CPUを構成すると、スレッド切り替えの遅延が減少します。したがって、Citrix Virtual Desktops™ VDI環境では2つのvCPUを構成することをお勧めします。

2つの仮想CPUを持つことは、物理CPUの数を2倍にすることを必ずしも意味しません。物理CPUはセッション間で共有できるためです。

セッションの信頼性機能に使用されるCitrix Gateway Protocol (CGP)もCPU消費を増加させます。高品質のネットワーク接続では、この機能を無効にしてVDA上のCPU消費を削減できます。強力なサーバーでは、上記のいずれのステップも必要ない場合があります。

UDPオーディオ: UDP経由のオーディオは、ネットワークの輻輳とパケット損失に対して優れた耐性を提供します。利用可能な場合は、TCPの代わりにこれをお勧めします。

LAN/WAN構成: 適切なネットワーク構成は、良好なリアルタイムオーディオ品質にとって重要です。通常、過剰なブロードキャストパケットがジッターを引き起こす可能性があるため、仮想LAN（VLAN）を構成する必要があります。IPv6対応デバイスは多くのブロードキャストパケットを生成する可能性があります。IPv6サポートが不要な場合は、それらのデバイスでIPv6を無効にできます。Quality of Serviceをサポートするように構成してください。

WAN接続の使用設定: LANおよびWAN接続を介してボイスチャットを使用できます。WAN接続では、オーディオ品質は接続の遅延、パケット損失、およびジッターに依存します。WAN接続のユーザーにソフトフォンを配信する場合、データセンターとリモートオフィス間でNetScaler® SD-WANを使用することをお勧めします。これにより、高いQuality of Serviceが維持されます。NetScaler SD-WANは、UDPを含むMulti-Stream ICAをサポートしています。また、単一のTCPストリームの場合、さまざまなICA仮想チャネルの優先度を区別して、高優先度のリアルタイムオーディオデータが優先的に処理されるようにすることが可能です。

DirectorまたはHDX Monitorを使用して、HDX構成を検証します。

リモートユーザー接続: Citrix Gatewayは、UDP/RTPトラフィックをネイティブに（TCPでのカプセル化なしで）配信するためにDTLSをサポートしています。 ポート443経由のUDPトラフィックに対して、ファイアウォールを双方向に開きます。

コーデックの選択と帯域幅の消費: ユーザーデバイスとデータセンター内のVDA間では、**Optimized-for-Speech**コーデック設定（ミディアム品質オーディオとも呼ばれる）を使用することをお勧めします。VDAプラットフォームとIP-PBX間では、ソフトフォンは構成またはネゴシエートされたコーデックを使用します。例：

- G711は良好な音声品質を提供しますが、1通話あたり80キロビット/秒から100キロビット/秒の帯域幅要件があります（ネットワークレイヤー2のオーバーヘッドによって異なります）。
- G729は良好な音声品質を提供し、1通話あたり30キロビット/秒から40キロビット/秒の低い帯域幅要件があります（ネットワークレイヤー2のオーバーヘッドによって異なります）。

仮想デスクトップへのソフトフォンアプリケーションの配信

XenDesktop®仮想デスクトップにソフトフォンを配信するには、2つの方法があります。

- アプリケーションは仮想デスクトップイメージにインストールできます。
- アプリケーションはMicrosoft App-Vを使用して仮想デスクトップにストリーミングできます。このアプローチは、仮想デスクトップイメージが整理された状態に保たれるため、管理上の利点があります。仮想デスクトップにストリーミングされた後、アプリケーションは通常の方法でインストールされたかのようにその環境で実行されます。すべてのアプリケーションがApp-Vと互換性があるわけではありません。

ユーザーデバイスとの間のオーディオ配信

汎用HDX RealTimeは、ユーザーデバイスとの間でオーディオを配信する2つの方法をサポートしています。

- **Citrix Audio Virtual Channel**。Citrix Audio Virtual Channelはオーディオ転送専用に設計されているため、一般的にこれをお勧めします。
- **汎用USBリダイレクト**。ユーザーデバイスがCitrix Virtual Apps and Desktopsサーバーへの LANまたはLANに類似した接続上にある場合、ボタンまたはディスプレイ（あるいはその両方）を備えたオーディオデバイス、ヒューマンインターフェースデバイス（HID）をサポートします。

Citrixオーディオ仮想チャネル

双方向のCitrixオーディオ仮想チャネル（CTXCAM）により、オーディオをネットワーク経由で効率的に配信できます。汎用HDX RealTimeは、ユーザーのヘッドセットまたはマイクからのオーディオを取得し、圧縮します。その後、ICA経由で仮想デスクトップ上のソフトフォンアプリケーションに送信します。同様に、ソフトフォンのオーディオ出力は圧縮され、ユーザーのヘッドセットまたはスピーカーに逆方向に送信されます。この圧縮は、ソフトフォン自体が使用する圧縮（G.729やG.711など）とは独立しています。これは、Optimized-for-Speechコーデック（中品

質）を使用して行われます。その特性は、Voice over Internet Protocolに最適です。エンコード時間が短く、ネットワーク帯域幅はピーク時で約56キロビット/秒（各方向28 Kbps）しか消費しません。このコーデックはデフォルトのオーディオコーデックではないため、Studioコンソールで明示的に選択する必要があります。デフォルトはHDオーディオコーデック（高品質）です。このコーデックは高忠実度ステレオサウンドトラックに優れていますが、Optimized-for-Speechコーデックと比較してエンコードが遅くなります。

汎用USBリダイレクト

Citrix汎用USBリダイレクトテクノロジー（CTXGUSB仮想チャネル）は、複合デバイス（オーディオとHID）およびアイソクロナスUSBデバイスを含むUSBデバイスをリモートで利用するための汎用的な手段を提供します。このアプローチは、LAN接続されたユーザーに限定されます。その理由は、USBプロトコルがネットワーク遅延に敏感であり、かなりのネットワーク帯域幅を必要とする傾向があるためです。アイソクロナスUSBリダイレクトは、一部のソフトフォンを使用する場合にうまく機能します。このリダイレクトは、優れた音声品質と低遅延を提供します。ただし、Citrixオーディオ仮想チャネルはオーディオトラフィックに最適化されているため、こちらが推奨されます。主な例外は、ボタン付きのオーディオデバイスを使用する場合です。例えば、データセンターにLAN接続されたユーザーデバイスに接続されたUSB電話などです。この場合、汎用USBリダイレクトは、ソフトフォンに信号を送り返すことで機能を制御する電話機またはヘッドセットのボタンをサポートします。デバイス上でローカルに機能するボタンには問題ありません。

オーディオ診断コマンドラインツール

VDA上のオーディオ診断コマンドラインツールは、オーディオポリシー、構成、およびデータ転送に関連するセッションデータを照会するために使用できます。

使用方法

コマンドプロンプトを開き、`C:\Program Files\Citrix\HDX\bin`フォルダーから`CtxAudio.exe`を実行します。

- 管理者としてツールを実行すると、すべてのアクティブなICAセッションのオーディオ情報が表示されます。
- 非管理者としてツールを実行すると、現在ユーザーのICAセッションオーディオ情報が表示されます。

出力

このツールは、セッション内のオーディオ関連の問題の診断に役立つさまざまな構成設定を出力します。

セクション	説明
ポリシー情報	現在のセッションに適用されているオーディオポリシー。
設定情報	レジストリに保存されているオーディオ関連の構成設定。
状態情報	現在のセッションに適用されているオーディオの状態、バージョン、コーデック、およびトランスポート。
デバイス情報	セッションで使用されているデバイス名、その役割、およびステータス。

注:

出力は、ツールをマルチセッション (TS) VDA で実行するか、シングルセッション VDA (WSVDA) で実行するかによって異なります。

制限事項

クライアントにオーディオデバイスをインストールし、オーディオリダイレクトを有効にしてRDSセッションを開始すると、オーディオファイルが再生に失敗し、エラーメッセージが表示されることがあります。

回避策として、RDSマシンにレジストリキーを追加し、マシンを再起動します。詳細については、レジストリを介して管理される機能のリストにあるオーディオの制限を参照してください。

ブラウザコンテンツリダイレクト

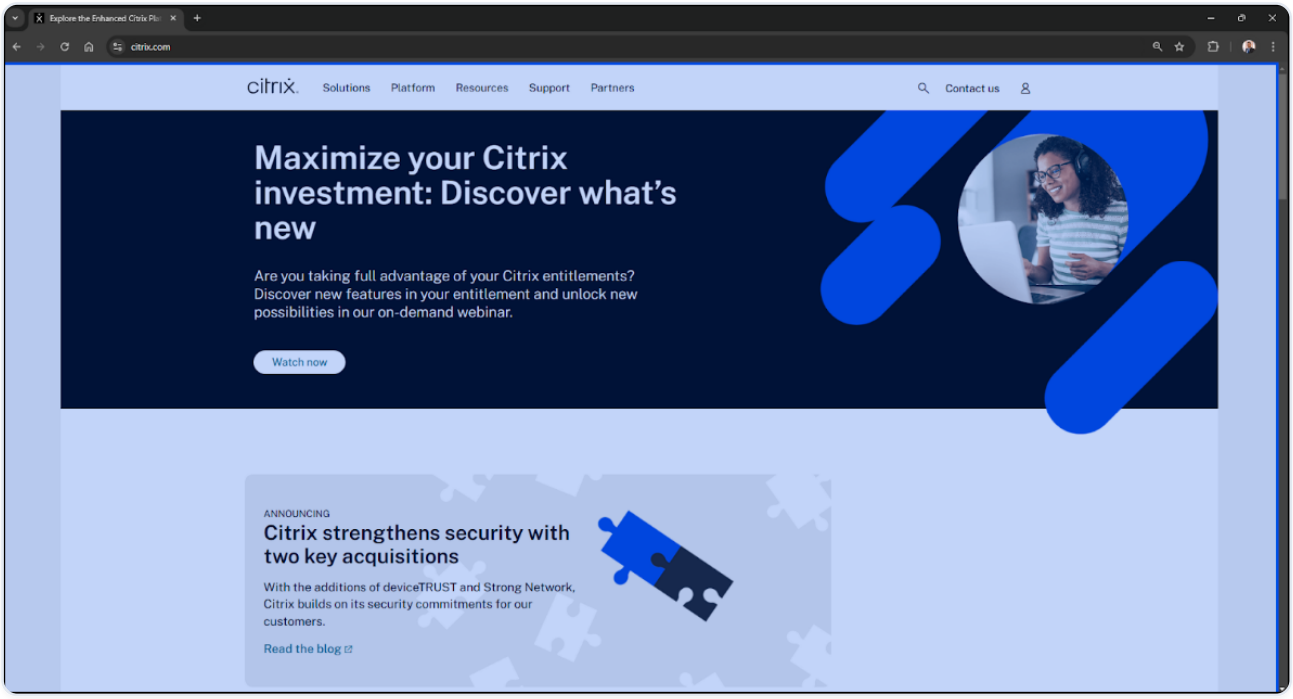
はじめに

ブラウザコンテンツリダイレクト (BCR) は、Citrix Virtual Apps and Desktops™ 環境でのWebブラウジングのユーザーエクスペリエンスを向上させます。Webページのレンダリングをユーザーのローカルマシンにオフロードすることで、BCRはサーバーの負荷を軽減し、特に複雑なWebサイトやリソースを大量に消費するWebサイトのパフォーマンスを向上させます。

動作の仕組み

BCRは、Citrix Workspace™ アプリを利用して、ユーザーデバイス上に安全なブラウジング環境を作成します。ユーザーが許可されたWebページにアクセスすると、ブラウザウィンドウのビューポートがクライアントにリダイレクトされます。その後、クライアント側のブラウザエンジンはローカルマシンのリソースを活用してページをレンダリングし、読み込み時間の短縮とスムーズな操作を実現します。

ブラウザのビューポートのみがリダイレクトされることに注意してください。ビューポートとは、ブラウザでコンテンツが表示される長方形の領域です。ビューポートには、アドレスバー、お気に入りツールバー、ステータスバーなどは含まれません。これらの項目はユーザーインターフェイスにあり、VDA内のブラウザで引き続き実行されます。



主な利点

ブラウザコンテンツリダイレクトは、Webトラフィックをインテリジェントに管理し、インフラストラクチャへの負担を軽減しながら、ユーザーに優れたエクスペリエンスを提供します。

組織にとってのメリットは次のとおりです。

- **コスト削減:** リソースを大量に消費するウェブページをユーザーデバイスにオフロードすることで、貴重なサーバーリソースを解放し、帯域幅の消費を削減します。これにより、ハードウェアコストとネットワークコストが削減されます。
- **ユーザーエクスペリエンスの向上:** グラフィックを多用するWebサイトでも、よりスムーズで応答性の高いブラウジングエクスペリエンスをユーザーに提供します。ネイティブのようなパフォーマンスを提供し、遅延をなくし、生産性を向上させます。

- **セキュリティの向上:** 内部リソースと外部リソースの両方へのアクセスを許可しながら、安全な環境を維持します。
- **柔軟性の向上:** 基本的なWebブラウジングから、プロキシトラバーサルやSSO認証を必要とする複雑なWebアプリケーションまで、幅広いユースケースをサポートします。Citrix Web Studio™ の詳細なポリシーコントロールにより、リダイレクト設定を簡単に管理できます。

システム要件

サーバー側コンポーネント

シトリックス バーチャル アプリケーションズ アンド デスクトップ

- 長期サービスリリース
  - 最小要件 - サポート終了していないLTSR Citrix Virtual Apps and Desktopsリリース
  - 推奨 - シトリックス バーチャル アプリケーションズ アンド デスクトップ 2402以降
- 現在のリリース
  - 最小要件 - サポート終了していないCR Citrix Virtual Apps and Desktopsリリース
  - 推奨 - 最新のCitrix Virtual Apps and Desktopsリリース

ブラウザコンポーネント

- ブラウザ
  - マイクロソフト エッジ
  - グーグル クローム
- ブラウザリダイレクト拡張機能
  - Google Chromeストア
  - マイクロソフト エッジ ストア
- 最高の体験のために、最新バージョンのブラウザを使用することをお勧めします。

> **注:**

> ブラウザコンテンツリダイレクトまたは双方向コンテンツリダイレクトを有効にするには、Microsoft Edgeアドオンストアからブラウザリダイレクト拡張機能を使用する予定がある場合、Virtual Delivery Agent (VDA) バージョン2503があることを確認してください。古いVDA

バージョンでは、Microsoft Edgeブラウザ内でChromeウェブストアから拡張機能をインストールすることで、同じ機能を実現できます。

上記で提供されている拡張機能リンクは一般提供 (GA) されており、実稼働レベルの展開に関連しています。GA拡張機能に加えて、CitrixはGoogle Chromeストアでベータ版 (GA + 1) 拡張機能も特別に公開しています。

Citrixは、今後のアップデートがテストされ、問題が早期に報告されるように、お客様がベータ版でテストユーザーを持つことを推奨しています。これにより、GA拡張機能が正式に展開される際にスムーズなプロセスが保証されます。

拡張機能のリリースは通常、Citrix Workspaceアプリのリリースと一致します。

クライアント側コンポーネント

ウィンドウズ

- Windows 10 または 11
- Citrix Workspaceアプリ
  - 最小要件 - サポート終了していないCitrix Workspaceアプリ
  - 推奨
    - 長期サービスリリース - Citrix Workspace App 2402 最新 CU
    - 現在のリリース - Citrix Workspace App 2405 以降

注:

- ブラウザコンテンツリダイレクトは、Citrix Workspace App Windows LTSRリリース1912および2203.1ではサポートされていません。
- ブラウザコンテンツリダイレクトに必要なクライアント側ブラウザエンジンは、Citrix Workspace Appの現行リリースではデフォルトでインストールされます。
- ブラウザコンテンツリダイレクトに必要なクライアント側ブラウザエンジンは、Citrix Workspace App 2402 LTSR リリースにはデフォルトでインストールされませ

ん。管理者は ADDLOCAL スイッチを利用して、Citrix Workspace App に BCR ブラウザコンポーネントを追加インストールできます。

- Windows 用 Citrix Workspace アプリ 2507 以降、ブラウザコンテンツリダイレクト (BCR) はモジュールコンポーネントとして管理されますが、引き続き Citrix Workspace アプリにパッケージ化されています。BCR コンポーネントは、LTSR バージョンにもデフォルトでインストールされるようになり、CR と LTSR の一貫性が確保されます。さらに、通常の Citrix Workspace アプリのリリースサイクル外で独立した更新や暫定パッチが必要な状況のために、スタンドアロンの BCR パッケージが公開されます。詳細については、Citrix Workspace App Windows ドキュメントを参照してください。

Linux

- Citrix Workspace アプリ
  - 最小要件 - サポート終了 (EOL) ではない任意の Citrix Workspace App
  - 推奨 - Citrix Workspace App 2408 以降 詳細については、Citrix Workspace App Linuxドキュメントを参照してください。

注:

Linux 用 Citrix Workspace アプリ 2601 以降、ブラウザコンテンツリダイレクト (BCR) はモジュールコンポーネントとして管理されます。BCR コンポーネントは、引き続き Linux 用 Citrix Workspace アプリにデフォルトでパッケージ化およびインストールされ、一貫したユーザーエクスペリエンスを保証します。さらに、通常の Citrix Workspace アプリのリリースサイクル外で独立した更新や暫定パッチが必要な状況のために、スタンドアロンの BCR パッケージが公開されます。詳細については、Citrix Workspace App Linux ドキュメントを参照してください。

ChromeOS

- Citrix Workspace アプリ
  - Chrome Web Store からの最新バージョン

MacOS

- macOS 11 ビッグサー

- macOS 12 モンタレー
- macOS 13 ベンチュラ
- macOS 14 Sonoma (14.2.1まで)
- Citrix Workspaceアプリ
    - 最小要件 - Citrix Workspaceアプリ 2411以降

注:

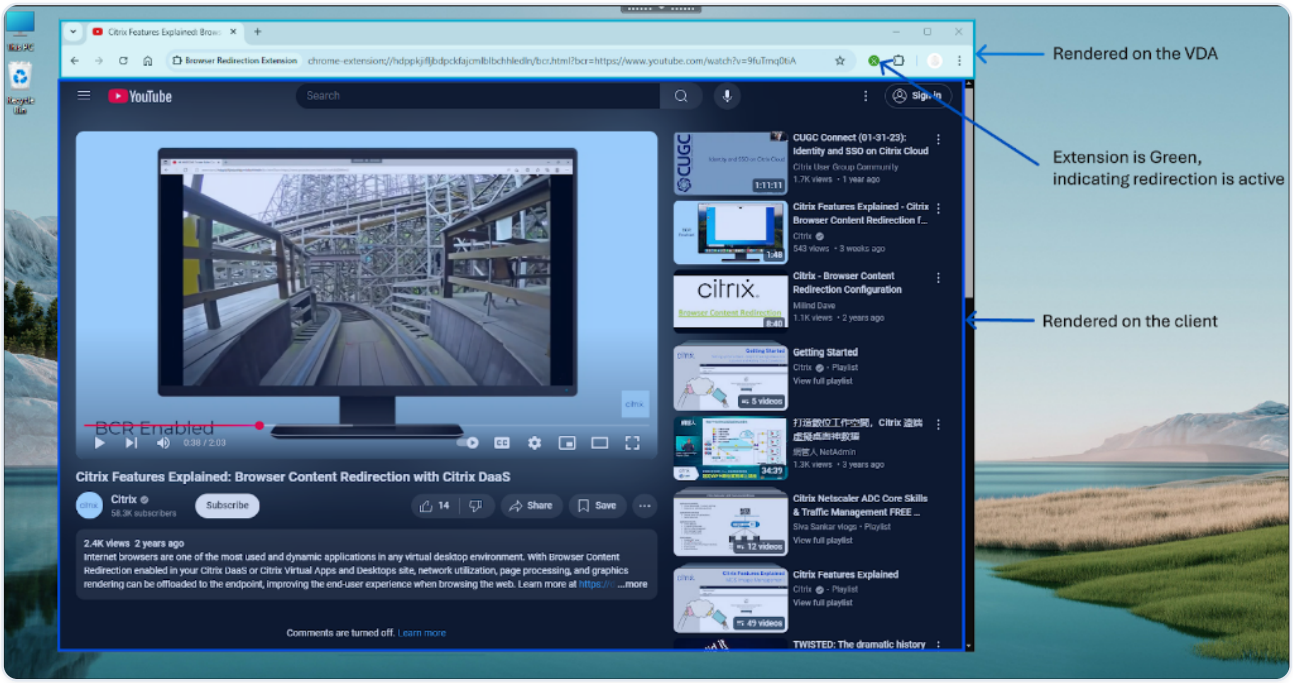
- macOSの場合、ブラウザコンテンツリダイレクトパッケージはCitrix Workspaceアプリとは独立しており、常に最新バージョンです。したがって、このパッケージは、指定された最小バージョンより新しい複数のCWAバージョンと互換性があります。
- Citrix Workspaceアプリ Macへの依存関係がないため、ブラウザコンテンツリダイレクトのバージョン番号はCitrix Workspaceアプリ Macのバージョンとは一致しません。
- クライアント側のブラウザエンジンはCitrix Workspaceアプリ Macにはパッケージされていません。Mac用のクライアント側はCitrix Downloadsからダウンロードしてインストールしてください。
- IntelパッケージとARMパッケージは別々です。そのため、macOSエンドポイントに適したバージョンをインストールする必要があります。
- Mac用Citrix Workspaceアプリ 2511.1以降、モジュラーBCRコンポーネントはデフォルトでインストールされますが、Citrix Workspaceアプリにはパッケージされていません。これにより、Citrix Downloadsからコンポーネントを手動でダウンロードしてインストールする必要がなくなります。スタンドアロンBCRパッケージは、通常のCitrix Workspaceアプリのリリースサイクル外で独立した更新や暫定パッチが必要な状況のために公開されます。詳細については、Citrix Workspaceアプリ Macのドキュメントを参照してください。

構成手順

1. システム要件に従って、クライアント側およびサーバー側コンポーネントをインストールします。
    - 拡張機能の展開の詳細については、「拡張機能の展開」セクションを参照してください。
2. スタジオポリシーを構成します。

- Web Studioポリシーは、さまざまなユースケースに合わせてブラウザコンテンツリダイレクトを構成するためのきめ細かな方法を提供します。
- 基本的なポリシーにより、管理者はブラウザコンテンツリダイレクトで許可/不許可にする必要があるURLを構成できます。
- URLはワイルドカードを使用して構成できます。

3. サポートされているWebブラウザを開き、許可されているURLに移動します。
   - 許可リストで一致が見つかった場合、Webサイトはクライアントにリダイレクトされます。
   - Citrix Workspaceアプリは、ビューポートをVDA側のブラウザにブレンドし、シームレスなエクスペリエンスを実現します。
4. 拡張機能のロゴの色は、コンテンツリダイレクトのステータスを示します。
   - 緑: アクティブで接続済み
   - 灰色: 現在のタブで非アクティブ/アイドル状態
   - 赤: 破損/動作していません



> **注:**
>
> - HTML5ビデオのリダイレクトとブラウザコンテンツのリダイレクトは、独立した機能です。この機能が動作するためにHTML5ビデオのリダイレクトポリシーは必要ありませ

ん。ただし、Citrix HDX™ HTML5ビデオのリダイレクトサービスは、ブラウザコンテンツのリダイレクトに使用されます。

- すべての構成は、レジストリキーではなくWeb Studioを介して行うことをお勧めします。

構成オプション

ブラウザコンテンツリダイレクトは、さまざまな顧客環境のユースケースに合わせて構成するためのさまざまな方法を提供します。ポリシー設定の詳細については、「ブラウザコンテンツリダイレクトポリシー設定」(https://docs.citrix.com/ja-jp/citrix-virtual-apps-desktops/2411/policies/reference/ica-policy-settings/browser-content-redirection-policy-settings)を参照してください。

リダイレクトメカニズム

クライアントフェッチクライアントレンダー

デフォルトでは、ブラウザコンテンツリダイレクトはこのモードで動作します。つまり、クライアント側のブラウザエンジンがWebページに直接アクセスします。これには、クライアントネットワークからWebページへの必要なアクセスが必要です。クライアントフェッチクライアントレンダーのシナリオでは、Citrix VDAからクライアントへ、ネットワーク、CPU、RAMの使用量をすべてオフロードし、ブラウザコンテンツリダイレクトを設定する最も最適な方法です。

ポリシー設定オプション

- ブラウザコンテンツリダイレクト：許可
- ブラウザコンテンツリダイレクトACL構成
  - リダイレクトする必要があるURLを指定します。デフォルトでは、YouTubeのみがリダイレクト用に構成されているウェブサイトです。
- ブラウザコンテンツリダイレクトブロックリスト構成
  - 特定のURLまたはサブURLのリダイレクトをブロックするためのオプション設定です。上記とこのオプションを組み合わせて、最大限のカスタマイズを実現します。

サーバーフェッチクライアントレンダリング

この場合、クライアント側のブラウザエンジンは、仮想チャネルを使用してVDAを介してWebサーバーからコンテンツにアクセスし、取得します。このオプションは、クライアントがインターネットアクセスを持たない場合（シンクライアントなど）に役立ちます。VDAでのCPUとRAMの消費は低いですが、ICA®仮想チャネルで帯域幅が消費されます。

このシナリオには3つの動作モードがあります。「プロキシ」という用語は、VDAがインターネットアクセスを取得するためにアクセスするプロキシデバイスを指します。

ポリシー設定オプション

- クライアントフェッチクライアントレンダーセクションで指定されたポリシーに加えて、以下を設定します。
- ブラウザコンテンツリダイレクトプロキシ構成
  - **直接または透過:** サーバーフェッチクライアントレンダリングを活用したい場合で、VDAからウェブページへの直接アクセスまたは透過プロキシアクセスがある場合は、これを構成します。ポリシーには「DIRECT」というキーワードを設定する必要があります。
  - **明示的プロキシ:** サーバーフェッチクライアントレンダリングを活用したい場合で、VDAからウェブページへの明示的プロキシアクセスがある場合は、これを構成します。
  - **PACファイル:** PACファイルに依存している場合、VDA内のブラウザが指定されたURLを取得するための適切なプロキシサーバーを自動的に選択できるように、これを構成します。

フォールバックモード

BCRリダイレクト(/en-us/citrix-virtual-apps-desktops/2411/media/bcr-redirection.png)

クライアントリダイレクトが失敗する場合があります。たとえば、クライアントマシンがインターネットに直接アクセスできない場合、エラー応答がVDAに戻されることがあります。そのような場合、VDA上のブラウザはページを再読み込みし、サーバー上でレンダリングできます。

認証の処理

認証サイト

Browser Content Redirectionの現在の実装では、リダイレクトメカニズムに関係なく、ウェブサイトへのログインをBrowser Content Redirectionが処理できるように、認証サイトを構成する必要があります。

例:

1. ブラウザコンテンツリダイレクトのACL設定で`<https://www.youtube.com/>`*のみが構成されており、認証サイトが設定されていない場合、ウェブサイトへのサインイン時にBCRはサーバー側レンダリングにフォールバックし、そこで処理を続行します。
2. この場合、BCRが認証サイトを処理できるように、`<https://www.accounts.google.com/>`*や、必要に応じてIdPウェブサイトなどの他の認証サイトを構成します。各ウェブサイトのサインインは異なる動作をするため、必ずリストしてください

3. 構成されている場合、BCRが認証を処理します。たとえば、クライアントフェッチクライアントレンダリングの場合、認証もクライアント側のブラウザエンジンから行われ、シームレスなサインインエクスペリエンスが実現します。

ポリシー構成オプション

「リダイレクトメカニズム」セクションで言及されているポリシーに加えて、「ブラウザコンテンツリダイレクト認証サイト」ポリシーを構成します。

> **注:**
>
> - BCRクライアント側のブラウザは、リダイレクトされたウィンドウが閉じられた後、Cookie（認証を含む）を保持しません。これは、BCRウィンドウが完全に閉じられて再度開かれたときに、Webサイトに再ログインする必要があるという形で現れます。
> - BCRクライアント側のブラウザは、VDA側のブラウザからCookieを読み取りません。そのため、ユーザーのパーソナライズと設定はVDAブラウザと同期されません。

統合Windows認証

ブラウザコンテンツリダイレクトは、VDAと同じドメイン内で統合Windows認証（IWA）が構成されている場合、Webサイトへのシームレスな認証方法を提供できます。

ポリシー構成オプション

- Browser Content Redirection統合Windows認証サポートポリシーを構成します。

シングルサインオンを有効にする前に、以下を完了してください。

- ホスト名から構築されたサービスプリンシパル名（SPN）のチケットを発行するようにKerberosインフラストラクチャを構成します。例：HTTP/serverhostname.com。
- サーバーフェッチクライアントレンダリングの場合: サーバーフェッチモードでブラウザコンテンツリダイレクトを使用する場合は、VDAでDNSが適切に構成されていることを確認してください。
- クライアントフェッチクライアントレンダーの場合：クライアントフェッチモードでブラウザコンテンツリダイレクトを使用する場合、クライアントデバイスでDNSが適切に構成されており、オーバーレイからWebサーバーのIPアドレスへのTCP接続を許可していることを確認してください。

プロキシ認証

ブラウザコンテンツリダイレクトは、サーバーからコンテンツをフェッチする際に、Webプロキシへのシームレスな認証方法を提供できます。有効にすると、ブラウザコンテンツリダイレクトは、Kerberosサービスチケットを自動的に取得して使用し、プロキシで認証します。

ポリシー構成オプション

- ブラウザコンテンツリダイレクトのサーバーフェッチプロキシ認証ポリシーを構成します。

サーバーフェッチプロキシ認証ポリシーを有効にする前に、以下を完了してください。

- PACファイルを構成して、ダウンストリームWebプロキシ経由でトラフィックをルーティングし、プロキシがKerberos認証を使用するように設定する必要があります。

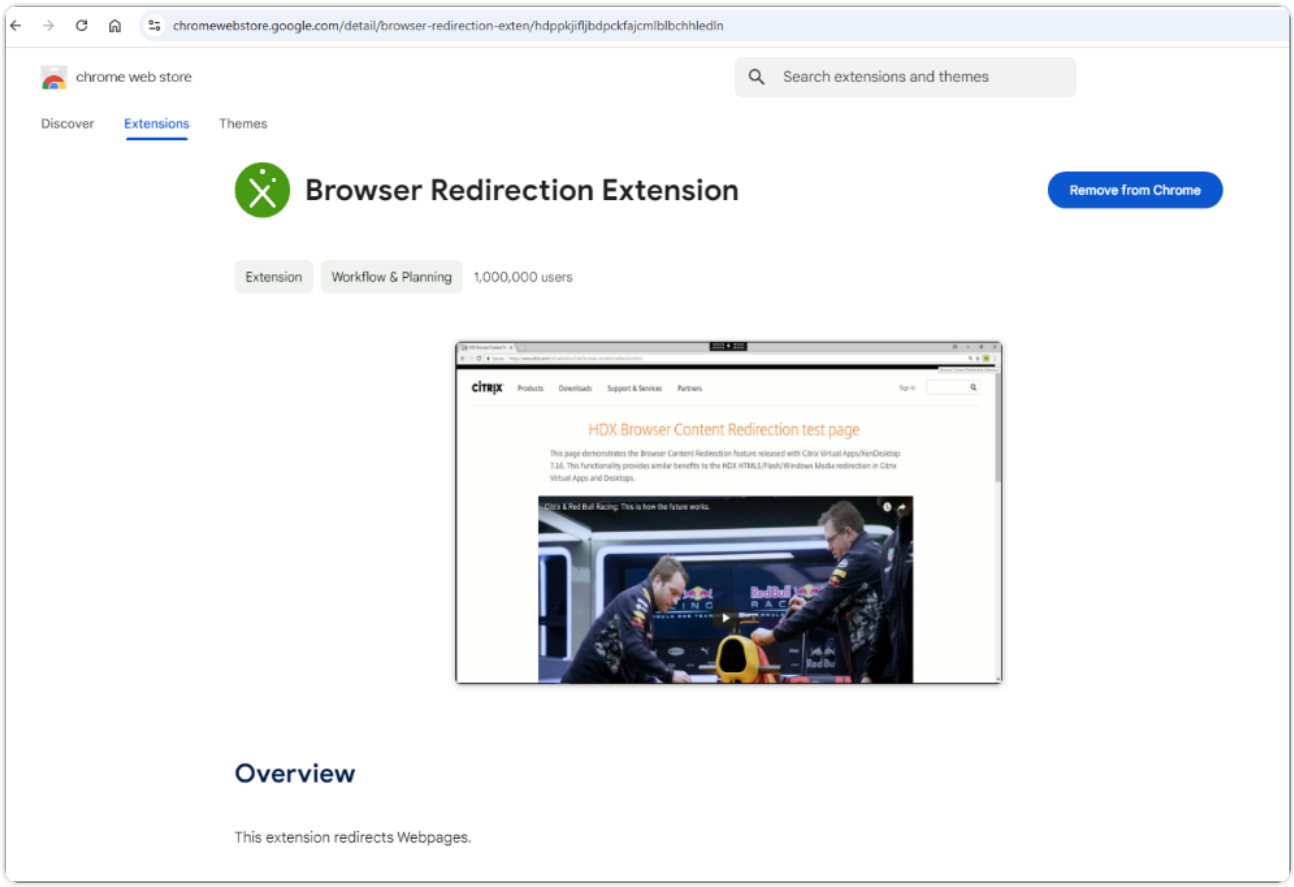
ユースケース

ブラウザコンテンツリダイレクト (BCR) は、特にリソースを大量に消費し、企業が頻繁にアクセスする幅広いWebサイトで利用できます。これには、YouTubeのようなビデオストリーミングプラットフォームが含まれ、レンダリングをエンドポイントデバイスにオフロードすることで、サーバー負荷を大幅に軽減し、コストを節約できます。さらに、BCRは、ビデオ会議やコラボレーションツール (Google Meet、Teams Web、Zoom Web) などのユニファイドコミュニケーションアプリケーションや、コンタクトセンターアプリケーション (Genesys Cloud) に最適であり、スムーズなパフォーマンスと強化されたユーザーエクスペリエンスを保証します。BCRを活用することで、企業はリソースを最適化し、さまざまなWebベースのアプリケーションで効率を向上させることができます。特定のWebサイトの構成方法については、CTX238236を参照してください。

拡張機能の展開

手動で展開

ブラウザリダイレクト拡張機能は、ChromeおよびEdgeのWebストアで公開されています。この拡張機能はVDA上のブラウザにのみ必要であり、クライアント側には必要ありません。拡張機能をインストールするには、Chrome / Edge Webストアに移動し、ブラウザリダイレクト拡張機能を検索して、それぞれのブラウザに追加します。この方法は個々のユーザーに有効です。多数のユーザーに拡張機能を展開するには、グループポリシーを使用して拡張機能を展開します。



グループポリシーを使用した展開

前提条件

- **アクセス:** グループポリシーを構成するマシンまたはActive Directory環境で管理者権限が必要です。
- **ADMXファイル:** お使いのChromeのバージョンに対応するGoogle Chrome ADMXファイル（管理用テンプレート）をダウンロードします。これらはGoogle Chrome Enterprise Helpページで見つけることができます。
- **Edgeテンプレート:** Microsoft Edge Enterprise landingページからMicrosoft Edgeの管理用テンプレート（ADMXファイル）をダウンロードします。
- **拡張機能IDと更新URL:** Citrix Browser Content Redirection拡張機能の拡張機能IDと更新URL。

GOOGLE CHROMEの手順

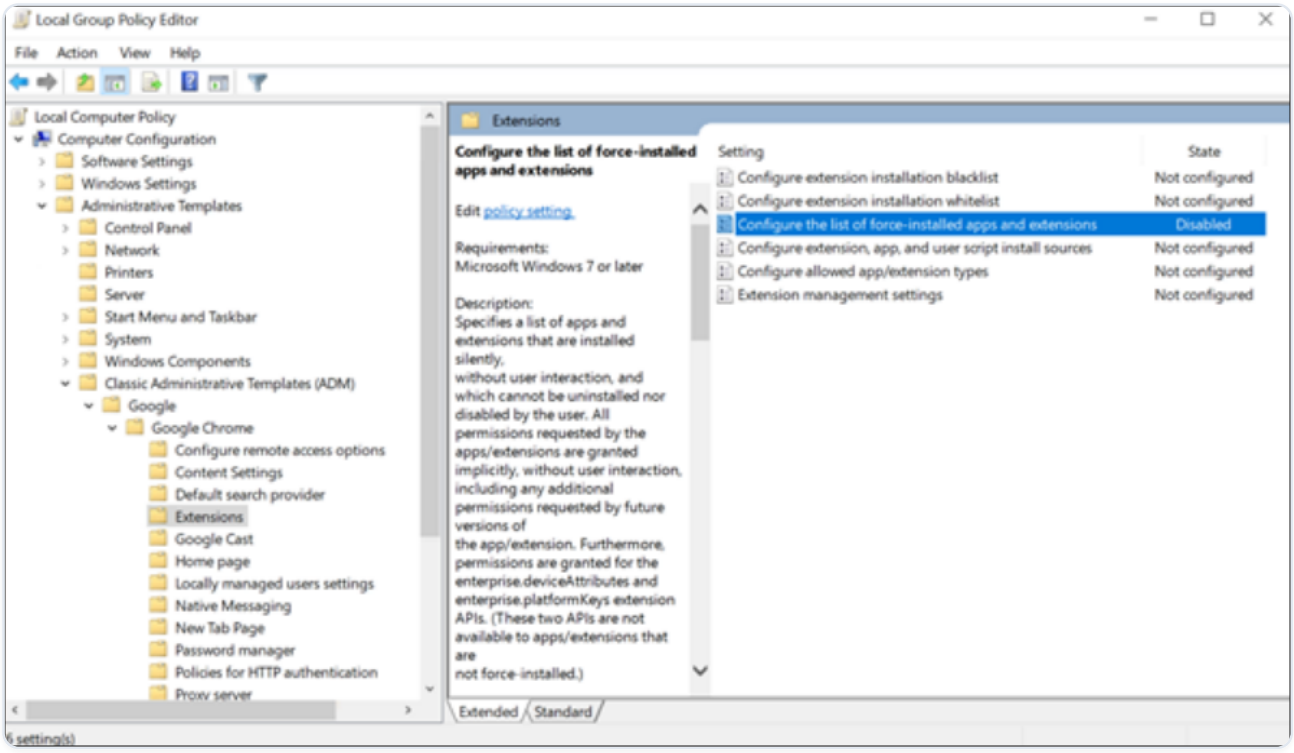
1. ADMXファイルのインポート:
    - Chrome ADMX ファイルを管理用テンプレートの中央ストアにコピーします。これは通常、ドメインコントローラー上の %SystemRoot%\PolicyDefinitions です。
2. グループポリシー管理を開く:
    - グループポリシー管理コンソール (gpmc.msc) を起動します。

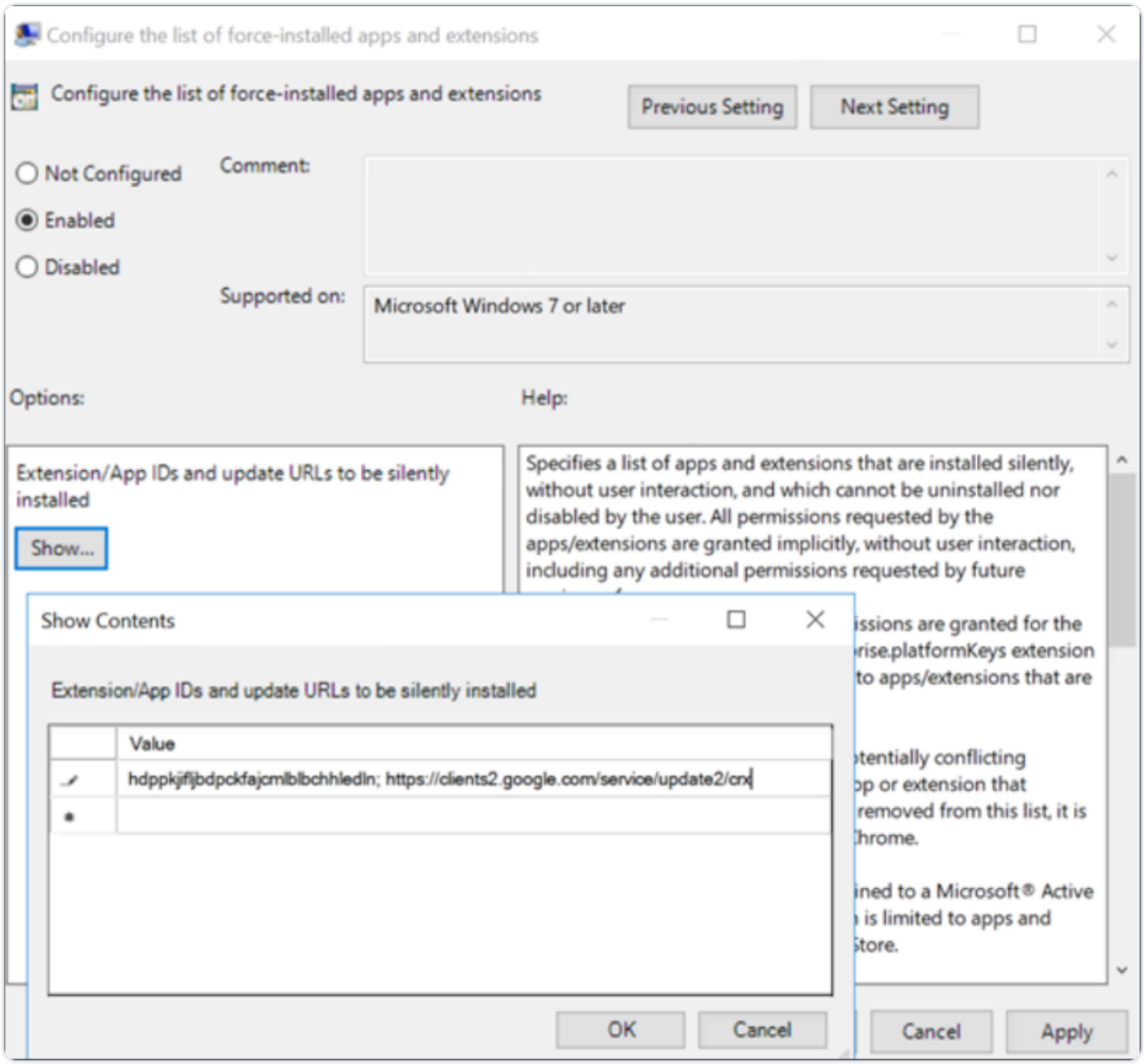
3. GPO の作成または編集:
    - 新しいグループポリシーオブジェクト (GPO) を作成するか、拡張機能を展開するユーザーまたはコンピューターに適用される既存の GPO を編集します。
4. 拡張機能の設定に移動:
    - GPO エディターで、以下に移動します。
        - ユーザーの構成 > 管理用テンプレート > 従来の管理用テンプレート (ADM) > Google > Google Chrome > 拡張機能
5. 「強制インストールされたアプリと拡張機能のリストを構成する」を有効にする:
    - このポリシー設定をダブルクリックし、「有効」を選択します。
    - 「強制インストールされたアプリと拡張機能のリストを構成する」設定が無効に設定されている場合、拡張機能はすべてのユーザーに対して Chrome から自動的に削除されます。
6. 拡張機能 ID と更新 URL を追加する:
    - 「表示」ボタンをクリックします。
    - 拡張機能IDと更新URLを次の形式で入力します: <extension_id>;<update_url>
    - 値: hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx (更新URL)
7. GPOを適用する:
    - Active Directory構造内の適切な組織単位 (OU) にGPOをリンクします。
8. グループポリシーを更新する:
    - ターゲットマシンで、gpupdate /force を実行してポリシーをすぐに適用するか、ポリシーが自動的に更新されるのを待ちます。

MICROSOFT EDGE の手順

1. ADMXファイルをインポートする:
    - Edge ADMXファイルを、管理用テンプレートの中央ストア (%SystemRoot%\PolicyDefinitions) にコピーします。
2. グループポリシー管理を開く:
    - グループポリシー管理コンソール (gpmc.msc) を起動します。

3. GPOを作成または編集します。
    - 新しいGPOを作成するか、既存のGPOを編集します。
4. 拡張機能の設定に移動します。
    - GPOエディターで、以下に移動します。
        - コンピューターの構成 > ポリシー > 管理用テンプレート > Microsoft Edge > 拡張機能
5. 「サイレントインストールされる拡張機能を制御する」を有効にする:
    - このポリシー設定をダブルクリックし、「有効」を選択します。
6. 拡張機能IDと更新URLを追加します。
    - 「表示」ボタンをクリックします。
    - 拡張機能IDと更新URLを次の形式で入力します: <extension_id>;<update_url>
    - 値: hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx (更新URL)
7. GPOを適用する:
    - Active Directory構造内の適切な組織単位 (OU) にGPOをリンクします。
8. グループポリシーを更新:
    - ターゲットマシンで、gpupdate /forceを実行するか、自動更新を待ちます。


Local Group Policy Editor
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
Control Panel
Network
Printers
Server
Start Menu and Taskbar
System
Windows Components
Classic Administrative Templates (ADM)
Google
Google Chrome
Configure remote access options
Content Settings
Default search provider
Extensions
Google Cast
Home page
Locally managed users settings
Native Messaging
New Tab Page
Password manager
Policies for HTTP authentication
Proxy server
Extensions
Configure the list of force-installed apps and extensions
Edit policy setting.
Requirements:
Microsoft Windows 7 or later
Description:
Specifies a list of apps and extensions that are installed silently,
without user interaction, and which cannot be uninstalled nor disabled by the user. All permissions requested by the apps/extensions are granted implicitly, without user interaction, including any additional permissions requested by future versions of
the app/extension. Furthermore, permissions are granted for the enterprise.deviceAttributes and enterprise.platformKeys extension APIs. (These two APIs are not available to apps/extensions that are
not force-installed.)
Setting
State
Configure extension installation blacklist
Not configured
Configure extension installation whitelist
Not configured
Configure the list of force-installed apps and extensions
Disabled
Configure extension, app, and user script install sources
Not configured
Configure allowed app/extension types
Not configured
Extension management settings
Not configured
Extended
Standard
6 setting(s)



トラブルシューティング

トラブルシューティング情報については、ナレッジセンターの記事「ブラウザコンテンツリダイレクトのトラブルシューティング方法」を参照してください。

ブラウザコンテンツリダイレクトの制限事項

サーバー側の制限事項 (VDA)

ブラウザコンテンツリダイレクトは、以下のユースケースをサポートできません。記載されているシナリオまたは新しいシナリオで機能強化が必要な場合は、Citrix製品チームにお問い合わせください。

- ポップアップウィンドウは、ブラウザコンテンツリダイレクトではサポートされていません。
- セッションクッキーの永続性はサポートされていません。

- ブラウザコンテンツリダイレクトを使用している場合、HTML5ビデオリダイレクトポリシーは無効にする必要があります。
- セッションの切断/再接続のシナリオでは、BCRを再度有効にするためにVDAブラウザウィンドウを更新する必要があります。
- BCR化されたウィンドウからの印刷およびファイルのダウンロードはサポートされていません。
- シークレットモードまたはプライベートブラウジングモードは、ブラウザコンテンツリダイレクトではサポートされていません。

クライアント側の制限 (CWA)

- ブラウザコンテンツリダイレクトはARMhfフレームワークではサポートされていません。

HDX™ ビデオ会議およびWebカメラビデオ圧縮

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

> ウェブカメラは、HDXウェブカメラビデオ圧縮またはHDXプラグアンドプレイ汎用USBリダイレクトを使用して、仮想セッション内で実行されているアプリケーションによって使用できます。モードを切り替えるには、**Citrix Workspace™アプリ > 環境設定 > デバイス**を使用します。Citrixは、可能な限り常にHDXウェブカメラビデオ圧縮を使用することを推奨します。HDX汎用USBリダイレクトは、HDXビデオ圧縮とのアプリケーション互換性の問題がある場合、またはウェブカメラの高度なネイティブ機能が必要な場合にのみ推奨されます。パフォーマンスを向上させるには、Virtual Delivery Agentに少なくとも2つの仮想CPUを搭載することをCitrixは推奨します。

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

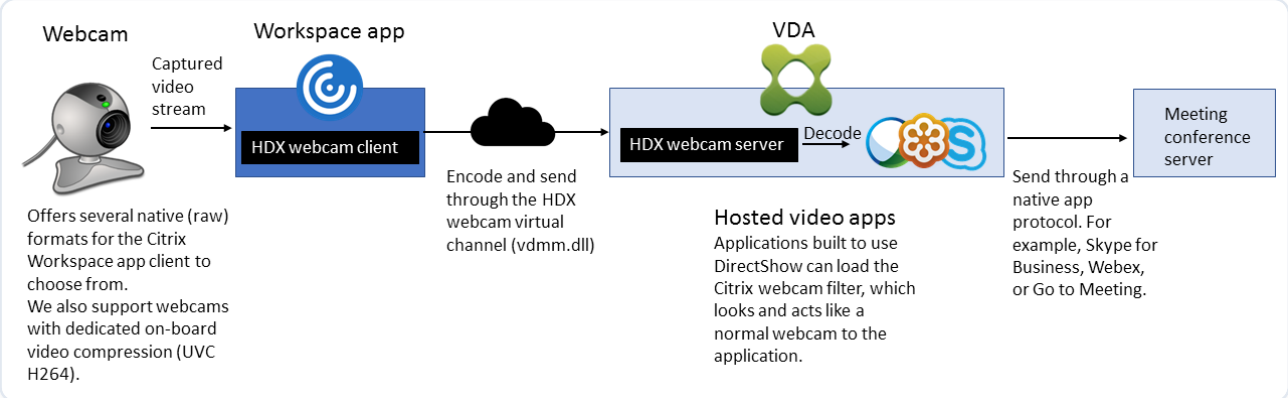
HDXウェブカメラビデオ圧縮

HDXウェブカメラビデオ圧縮は、**最適化された**ウェブカメラモードとも呼ばれます。この種類のウェブカメラビデオ圧縮は、H.264ビデオを仮想セッションで実行されているビデオ会議アプリケーションに直接送信します。VDAリソースを最適化するため、HDXウェブカメラ圧縮はウェブカメラビデオのエンコード、トランスコード、デコードを行いません。この機能はデフォルトで有効になっています。

サーバーからビデオ会議アプリへの直接ビデオストリーミングを無効にするには、VDAでレジストリキーを0に設定します。詳細については、レジストリを通じて管理される機能のリストにあるウェブカメラビデオ圧縮を参照してください。

ビデオリソースをストリーミングするためのデフォルト機能を無効にすると、HDXウェブカメラビデオ圧縮は、クライアントオペレーティングシステムの一部であるマルチメディアフレームワークテクノロジーを使用して、キャプチャデバイスからのビデオをインターセプトし、トランスコードして圧縮します。キャプチャデバイスの製造元は、OSカーネルストリーミングアーキテクチャに接続するドライバーを提供します。

クライアントはウェブカメラとの通信を処理します。その後、クライアントはビデオを適切に表示できるサーバーにのみ送信します。サーバーはウェブカメラを直接処理しませんが、その統合によりデスクトップで同じエクスペリエンスが得られます。Workspaceアプリは、帯域幅を節約し、WANシナリオでの回復性を向上させるためにビデオを圧縮します。



HDXウェブカメラビデオ圧縮には、**マルチメディア会議**ポリシーを有効にする必要があります。このポリシーはデフォルトで有効になっています。

ウェブカメラがハードウェアエンコーディングをサポートしている場合、HDXビデオ圧縮はデフォルトでハードウェアエンコーディングを使用します。ハードウェアエンコーディングは、ソフトウェアエンコーディングよりも多くの帯域幅を消費する可能性があります。ソフトウェア圧縮を強制するには、クライアントでレジストリキーを編集します。詳細については、レジストリを通じて管理される機能のリストにあるウェブカメラソフトウェア圧縮を参照してください。

HDXウェブカメラビデオ圧縮の要件

HDXウェブカメラビデオ圧縮は、Citrix Workspaceアプリの以下のバージョンをサポートしています。

プラットフォーム	プロセッサ
Citrix Workspace アプリ Windows用	Citrix Workspaceアプリ for Windowsは、XenAppおよびXenDesktop 7.17以降で32ビットおよび64ビットアプリのWebカメラビデオ圧縮をサポートしています。それ以前のバージョンでは、Citrix Workspaceアプリ for Windowsは32ビットアプリのみをサポートしています。
Citrix Workspace アプリ Mac用	Citrix Workspaceアプリ for Mac 2006以降は、XenAppおよびXenDesktop 7.17以降で64ビットアプリのWebカメラビデオ圧縮をサポートしています。それ以前のバージョンでは、Citrix Workspaceアプリ for Macは32ビットアプリのみをサポートしています。
Linux向けCitrix Workspaceアプリ	Citrix Workspaceアプリ for Linuxは、仮想デスクトップ上で32ビットおよび64ビットの両方のアプリをサポートしています。
Chrome向けCitrix Workspaceアプリ	一部のARM ChromebookはH.264エンコーディングをサポートしていないため、32ビットアプリのみが最適化されたHDX Webカメラビデオ圧縮を使用できます。

Media Foundationベースのビデオアプリケーションは、Windows 10以降およびWindows Server 2019以降でHDX Webカメラビデオ圧縮をサポートしています。詳細については、Knowledge Centerの記事CTX132764を参照してください。

その他のユーザーデバイス要件:

- サウンドを生成するための適切なハードウェア。
- DirectShow互換のWebカメラ (Webカメラのデフォルト設定を使用)。ハードウェアエンコーディングが可能なWebカメラは、クライアント側のCPU使用率を削減します。

- HDX Webカメラビデオ圧縮の場合、可能であればカメラメーカーから入手したWebカメラドライバーをクライアントにインストールします。デバイスドライバーのインストールはサーバー上では不要です。

Webカメラによってフレームレート、明るさ、コントラストのレベルが異なります。Webカメラのコントラストを調整すると、アップストリームトラフィックを大幅に削減できます。Citrixは、初期機能検証のために以下のWebカメラを使用しています:

- Microsoft LifeCam VXモデル（2000、3000、5000、7000）
- クリエイティブ ライブ！カム オプティア プロ
- ロジクール クイックカム メッセンジャー
- ロジクール C600、C920
- HP デラックス ウェブカメラ

優先するビデオフレームレートを調整するには、クライアントでレジストリキーを編集します。詳細については、レジストリで管理される機能のリストにあるWebカメラビデオ圧縮フレームレートを参照してください。

高解像度Webカメラストリーミング

サーバー上のビデオ会議アプリケーションは、サポートされているフォーマットタイプに基づいてWebカメラのフォーマットと解像度を選択します。セッションが開始されると、クライアントはWebカメラ情報をサーバーに送信します。アプリケーションからWebカメラを選択します。Webカメラとビデオ会議アプリケーションが高解像度レンダリングをサポートしている場合、アプリケーションは高解像度を使用します。すべてのWebカメラの解像度をサポートしています。

この機能には、Citrix Workspaceアプリ for Windows バージョン1808以降、またはCitrix Receiver for Windows バージョン4.10以降が必要です。

レジストリキーを使用して、この機能を無効または有効にできます。詳細については、レジストリで管理される機能のリストにある高解像度Webカメラストリーミングを参照してください。

メディアタイプのネゴシエーションが失敗した場合、HDXはデフォルトのVGA解像度（640 x 480 ピクセル）にフォールバックします。クライアントのレジストリキーを使用して、デフォルトの解像度を構成できます。カメラが指定された解像度をサポートしていることを確認してください。詳細については、レジストリで管理される機能のリストにある高解像度Webカメラ解像度を参照してください。

HDX Webカメラビデオ圧縮は、プラグアンドプレイの汎用USBリダイレクトと比較して帯域幅を大幅に少なく使用し、WAN接続でも良好に機能します。帯域幅を調整するには、クライアントで

レジストリキーを設定します。詳細については、レジストリで管理される機能のリストにある高解像度Webカメラ帯域幅を参照してください。

ビット/秒単位で値を入力します。帯域幅を指定しない場合、ビデオ会議アプリケーションはデフォルトで350000 bpsを使用します。

HDXプラグアンドプレイ汎用USBリダイレクト

HDX プラグアンドプレイ汎用USBリダイレクト（アイソクロナス）は、**汎用**ウェブカメラモードとも呼ばれます。HDX プラグアンドプレイ汎用USBリダイレクトの利点は、シンクライアント/エンドポイントにドライバーをインストールする必要がないことです。USBスタックは仮想化されており、ローカルクライアントに接続したものはすべてリモートVMに送信されます。リモートデスクトップは、ネイティブに接続したかのように動作します。Windowsデスクトップはハードウェアとのすべてのやり取りを処理し、正しいドライバーを見つけるためにプラグアンドプレイロジックを実行します。ほとんどのウェブカメラは、ドライバーがサーバーに存在すれば動作し、ICA経由で動作できます。汎用ウェブカメラモードは、ネットワーク経由でUSBプロトコルを使用して非圧縮ビデオを送信するため、はるかに多くの帯域幅（毎秒数メガビット）を使用します。

HTML5 マルチメディア リダイレクト

HTML5 マルチメディア リダイレクトは、HDX™ MediaStream のマルチメディア リダイレクト機能を拡張し、HTML5 のオーディオとビデオを含めます。特にモバイルデバイスへのマルチメディアコンテンツのオンライン配信の増加により、ブラウザ業界はオーディオとビデオを提示するためのより効率的な方法を開発してきました。

Flash は標準でしたが、プラグインが必要で、すべてのデバイスで動作せず、モバイルデバイスでのバッテリー消費量が多くなります。YouTube、Netflix、および Mozilla、Google、Microsoft の新しいブラウザバージョンなどの企業は HTML5 に移行しており、それが新しい標準となっています。

HTML5 ベースのマルチメディアには、独自のプラグインに比べて多くの利点があります。以下はその一部です。

- 企業に依存しない標準 (W3C)
- 簡素化されたデジタル著作権管理 (DRM) ワークフロー
- プラグインによって引き起こされるセキュリティ問題なしに、より良いパフォーマンス

HTTP プログレッシブダウンロード

HTTP プログレッシブダウンロードは、HTML5 をサポートする HTTP ベースの疑似ストリーミング方式です。プログレッシブダウンロードでは、HTTP Web サーバーからダウンロード中に、ブラウザが単一のファイル (単一の品質でエンコードされたもの) を再生します。ビデオは受信時にドライブに保存され、ドライブから再生されます。ビデオを再視聴する場合、ブラウザはキャッシュからビデオを読み込むことができます。

プログレッシブダウンロードの例については、HTML5 ビデオ リダイレクト テスト ページ を参照してください。Web ページ内のビデオ要素を検査し、HTML5 ビデオタグ内のソース (mp4 コンテナ形式) を見つけるには、ブラウザの開発者ツールを使用します。

HTML5 と Flash の比較

機能	HTML5	フラッシュ
独自のプレーヤーが必要	いいえ	はい
モバイルデバイスで実行	はい	一部
さまざまなプラットフォームでの実行速度	高	低速
iOSでサポート	はい	いいえ
リソース使用量	少ない	多い
より速くロード	はい	いいえ

要件

mp4形式のプログレッシブダウンロードのリダイレクトのみをサポートしています。WebMやDASH/HLSのようなアダプティブビットレートストリーミング技術はサポートしていません。

以下をサポートしており、ポリシーを使用して制御します。詳細については、「マルチメディアポリシー設定」を参照してください。

- サーバー側レンダリング
- サーバーフェッチクライアントレンダリング
- クライアント側フェッチとレンダリング

Citrix Workspace™アプリおよびCitrix Receiver™の最小バージョン:

- Windows向けCitrix Workspaceアプリ1808
- Windows向けシトリックス レシーバー 4.5
- Linux向けCitrix Workspaceアプリ1808
- Linux向けシトリックス レシーバー 13.5

最小VDAブラウザーバージョン	ウィンドウズ OS バージョン/ビルド/SP
インターネット エクスプローラー 11.0	Windows 10 の x86 (1607 RS1) および x64 (1607 RS1) 版; Windows 7 の x86 および x64 版; Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2
Firefox 47 Firefox証明書ストアに証明書を手動で追加するか、Windowsの信頼された証明書ストアから証明書を検索するようにFirefoxを設定します。詳細については、`https://wiki.mozilla.org/CA:AddRootToFirefox`を参照してください。	Windows 10 の x86 (1607 RS1) および x64 (1607 RS1) 版; Windows 7 の x86 および x64 版; Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2
クローム 51	ウィンドウズ 10 x86 (1607 RS1) および x64 (1607 RS1); ウィンドウズ 7 x86 および x64; ウィンドウズ サーバー 2016 RTM 14393 (1607); ウィンドウズ サーバー 2012 R2

HTML5ビデオリダイレクトソリューションのコンポーネント

- **HdxVideo.js** - Webサイト上のビデオコマンドを傍受するJavaScriptフック。HdxVideo.jsは、セキュアWebSocket (SSL/TLS) を使用してWebSocketServiceと通信します。
- **WebSocket SSL証明書**
  - CA（ルート）の場合：**Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX In-Product CA) 場所：**証明書（ローカルコンピューター） > 信頼されたルート証明機関 > 証明書**。
  - エンドエンティティ（リーフ）の場合：**Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX Service) 場所：**証明書（ローカルコンピューター） > 個人 > 証明書**。

- **WebSocketService.exe** - ローカルシステム上で実行され、SSL終端とユーザーセッションマッピングを実行します。127.0.0.1ポート9001でTLSセキュアWebSocketがリッスンしています。
- **WebSocketAgent.exe** - ユーザーセッション上で実行され、WebSocketServiceコマンドの指示に従ってビデオをレンダリングします。

HTML5ビデオのリダイレクトを有効にするにはどうすればよいですか?

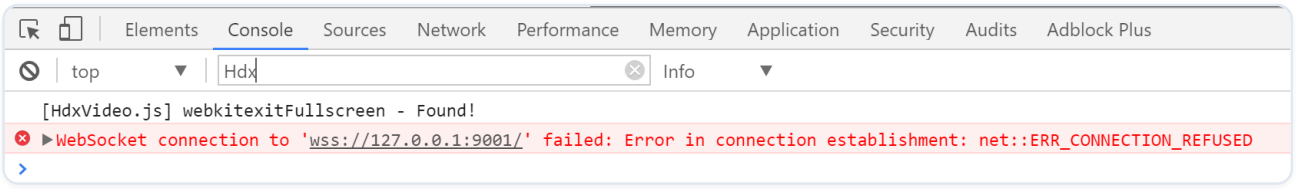
このリリースでは、この機能は管理されたWebページでのみ利用可能です。HTML5マルチメディアコンテンツが利用可能なWebページに、HdxVideo.js JavaScript（Citrix Virtual Apps and Desktopsインストールメディアに含まれています）を追加する必要があります。例えば、社内トレーニングサイトのビデオなどです。

youtube.comのような、アダプティブビットレート技術（例：HTTPライブストリーミング（HLS）やHTTP経由のダイナミックアダプティブストリーミング（DASH））に基づいたウェブサイトはサポートされていません。

詳細については、*マルチメディアポリシー設定*を参照してください。

トラブルシューティングのヒント

ウェブページがHdxVideo.jsを実行しようとすると、エラーが発生する可能性があります。JavaScriptの読み込みに失敗すると、HTML5リダイレクトメカニズムも失敗します。ブラウザの開発者ツールウィンドウでコンソールを検査し、HdxVideo.jsに関連するエラーがないことを確認してください。例：



Microsoft Teams の最適化 (新規)

Citrix® は、VDI 環境で Microsoft Teams のオーディオとビデオを最適化する 2 つの方法をサポートしています。Citrix HDX™ Optimization と、Microsoft が提供する Teams 向け新しい VDI ソリューションです。Classic Teams はサポート終了に達したため、このページで説明されている最適化アプローチは現在の Microsoft Teams クライアントに適用されます。

> **注:**

Microsoft は、Windows エンドポイントにおける WebRTC ベースの Microsoft Teams 向け Citrix HDX Optimization の非推奨を発表しました。以下の 2 つのマイルストーンが適用されます。

- October 1, 2026 - サポート終了: Microsoft または Citrix による公式サポートは終了します。
- April 1, 2027 - 提供終了: WebRTC ベースの最適化は機能しなくなります。レガシー最適化のための Citrix Studio ポリシーは適用されなくなります。

お客様は Teams 向け新しい VDI ソリューションへの移行をお勧めします。この変更は Windows エンドポイントのみに影響します。macOS、Linux、ChromeOS、および HTML5 エンドポイントは影響を受けません。詳細については、Microsoft Blog を参照してください。

最適化アプローチ

- **Citrix HDX Optimization (MTOP)**: Citrix と Microsoft の共同ソリューションで、Citrix が所有する仮想チャネル (CTXMTOP) を使用します。メディアオフロードは、Citrix Workspace™ アプリの `HdxRtcEngine` によって処理されます。このソリューションは従来 MTOP と呼ばれています。
- **Teams 向け新しい VDI ソリューション**: Microsoft が所有および管理する新しい最適化で、Microsoft が所有する仮想チャネル (MSTEAMS、MSTEAM1、MSTEAM2) を使用します。Windows および Mac エンドポイントで利用できます。詳細については、Microsoft ドキュメントの Teams 向け新しい VDI ソリューション を参照してください。

主な違い

CITRIX HDX 最適化	TEAMS 用の新しい VDI ソリューション
最適化は Citrix と Microsoft の共同ソリューションであり、Citrix が所有する仮想チャネル (CTXMTOP) を使用します。	最適化ソリューションは Microsoft が所有および管理しており、Microsoft が所有する仮想チャネル (MSTEAMS、MSTEAM1、MSTEAM2) を使用します。
メディアオフロードは、Citrix Workspaceアプリ内にある`HdxRtcEngine`によって処理されます。	メディアオフロードは、WindowsおよびMacエンドポイント上のSlimCoreメディアエンジンによって処理されます。

CITRIX HDX 最適化	TEAMS 用の新しい VDI ソリューション
Citrix Workspaceアプリのインストールを除き、エンドポイントに追加のコンポーネントは必要ありません。	追加コンポーネントである**Teams VDI Plugin**は、さまざまな方法でエンドポイントに展開する必要があります。このプラグインは、SlimCoreメディアエンジンのダウンロードと更新を管理します。
エンドポイントプラットフォーム（Windows、macOS、Linux、ChromeOS）で利用可能です。	エンドポイントプラットフォーム（WindowsおよびMac）で利用可能です。
新機能は、CitrixとMicrosoftが連携して管理します。	新機能はMicrosoftによって管理されます。ユーザーは、Citrix HDX Optimizationでは利用できない一部の新機能にアクセスできます。
関連するコンポーネントに応じて、CitrixとMicrosoftの両方でサポートされます。お客様はCitrixまたはMicrosoftのいずれかにケースをオープンでき、必要に応じて適切なチームにリダイレクトされます。	Microsoftが所有およびサポートしています。Citrixは、Citrix Workspaceアプリ、仮想チャネル許可リスト、プラグイン展開メカニズムなど、関連するCitrixコンポーネントをサポートします。

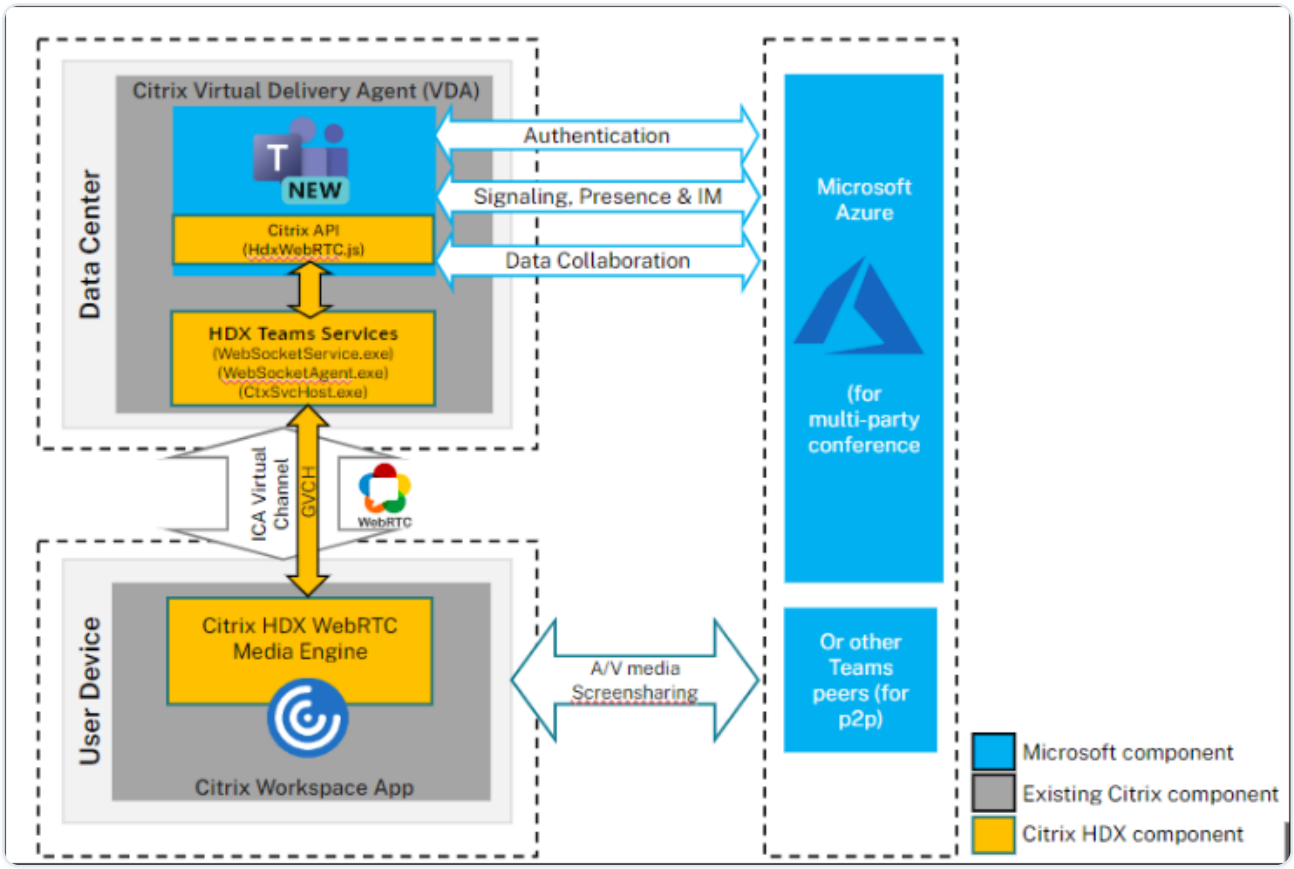
相互運用性とローミング

Citrix HDX OptimizationとTeams向けの新VDIソリューションは並行して存在できますが、Teamsクライアントは一度にいずれか一方のみを使用します。

- Teamsアプリの起動時に、次の順序で最適化が選択されます: Teams向けの新VDIソリューション、次にCitrix HDX Optimization (WebRTC)、次に標準のオーディオ/ビデオリダイレクト。
- Teams向けの新VDIソリューションが失敗した場合、TeamsはWebRTCではなく、標準のオーディオ/ビデオリダイレクトに直接フォールバックします。選択を再実行し、適切な最適化を選択するには、Teamsアプリの再起動が必要です。
- エンドポイント間のローミングはシームレスであり、Teamsアプリの再起動は必要ありません。これには、ユーザーがTeams向けの新VDIソリューションをサポートするエンドポイントとサポートしないエンドポイントの間をローミングする場合も含まれます。

Citrix HDX™ 最適化

Citrix HDX (WebRTC Optimization) では、オフロードされたメディアの処理を担当するエンドポイント上のメディアエンジン (HdxRtcEngine) は Citrix Workspace™ アプリに組み込まれており、Citrix Workspace アプリをインストールすると、エンジンも自動的にインストールされます。



システム要件

このセクションでは、新しい Teams クライアントをサポートするために必要な最小バージョンと推奨バージョンを示します。最小バージョンでは、一部の重要なバグ修正や最新機能が利用できない場合があることに注意してください。最新の修正と機能で最高の体験を得るには、推奨バージョンを展開してください。

VDI オペレーティングシステム

詳細については、Microsoft ドキュメントに記載されている推奨事項を参照してください。

注:

- Windows Server 2016 はサポートされていません。Citrix は、それに応じてアップグレードを計画することをお勧めします。
- バージョンは頻繁に更新されるため、ここに記載されているバージョンはサポート終了となる可能性があります。したがって、さまざまなコンポーネントのサポートされているバージョンを使用していることを確認するために、Citrix Workspace app および Citrix Virtual Apps and Desktops の製品ライフサイクルページを参照してください。

- Citrix Virtual Apps and Desktops™ 1912 LTSR を使用している場合、2024 年 12 月にサポート終了となるため、Citrix はアップグレードを計画することをお勧めします。

仮想デリバリーエージェント (VDA)

最小バージョン	推奨バージョン
1912 LTSR CU8+; 2203 LTSR (任意の CU); 2212 CR	2203 LTSR CU5+ (または) 2402 LTSR およびそれ以降のすべてのCRバージョン

Citrix Workspaceアプリ

最小バージョン	推奨バージョン
ウィンドウズ 2203 LTSR (最新CU); ウィンドウズ 2302 CR; リナックス 2207; Mac 2302; クローム/HTML5 2301	ウィンドウズ 2402 LTSR; ウィンドウズ 2405 CR; リナックス 2405; Mac 2405; ChromeOS/HTML5 2405

展開

1. VDIに新しいTeamsクライアントをインストールします。詳細については、VDI向け新しいTeamsの展開を参照してください。
2. 新しいTeamsを最適化するために、VDAで以下のレジストリキーを構成します。
   - **場所**: `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`
   - **キー (REG_Multi_SZ)**: `ProcessWhitelist`
   - **値**: `msedgewebview2.exe`

   > **注:**
   >
   > Citrix Virtual Apps and Desktops 2402 LTSR (または) Citrix Virtual Apps and Desktops 2203 LTSR CU5+ 以降では、`msedgewebview2.exe` レジストリエントリはデフォルトで許可リストに含まれているため、手動で構成する必要はありません。

3. Microsoft Teamsリダイレクトポリシーが有効になっていることを確認してください。このポリシーはデフォルトで有効になっています。
4. クライアント側で追加の設定は不要です。Citrix Workspaceアプリをインストールするには、ウィザードの指示に従ってください。

App レイヤリング

新しいMicrosoft Teamsはインストール方法が変更され、C:\Program Files\WindowsAppsにインストールされるようになりました。この変更をサポートするには、App Layeringバージョン2403.2以降を実行する必要があります。この修正を含むアップグレードディスクは、App Layering downloadsページからダウンロードできます。

詳細については、App Layering ドキュメントを参照してください。

Citrix プロファイル管理

New Microsoft Teams のローミングを有効にする方法については、Citrix Profile Management のドキュメントを参照してください。Citrix Profile Management の現在の最小バージョンガイダンスは 2402 LTSR (または) 2203 LTSR CU5+ です。

ネットワークに関する考慮事項

New Teams のネットワーク要件は Classic Teams と変わりません。したがって、Classic Teams ドキュメントのネットワーク要件セクションを参照してください。

機能マトリックスとバージョンサポート

バージョンは頻繁に更新されるため、ここで言及されている一部の古いバージョンはサポート終了となる可能性があります。したがって、さまざまなコンポーネントのサポートされているバージョンを使用していることを確認するために、Citrix Workspace App および Citrix Virtual Apps and Desktops の製品ライフサイクルページを参照してください。

> **注:**
>
> - ここで言及されているバージョンは、特定の機能がサポートされる最小バージョン、または新しいTeamsがサポートされる最小バージョンのうち、いずれか高い方です。
> - 最小バージョンセクションに記載されているCitrix Virtual Apps and Desktops 1912 LTSR CU8+は、2024年12月にサポート終了となるため、以下の表には記載されていません。ただし、それまでは引き続きサポートされるバージョンです。
> - 最小Citrix Virtual Apps and Desktopsバージョンが `N/A` である機能は、VDA側からの変更が一切なかったことを意味します。

機能	VDA (最小バージョン)	WINDOWS 用 CITRIX WORKSPACE アプリ (最小バージョン)	MAC 向け CITRIX WORKSPACE アプリ (最小バージョン)	LINUX 向け CITRIX WORKSPACE アプリ (最小バージョン)	CHROMEOS 用 CITRIX WORKSPACE アプリ (最小バージョン)
オーディオ/ビデオ (P2Pおよび会議)	2203 LTSR (任意の CU), 2212 CR	2203 LTSR 最新CU, 2302 CR	2302	2207	2301
画面共有	2203 LTSR (任意の CU), 2212 CR	2203 LTSR 最新CU, 2302 CR	2302	2207	2301
i. 画面インジケーターの赤い枠線	2203 LTSR (任意の CU), 2212 CR	2203 LTSR 最新CU, 2302 CR	2302	2207	いいえ
ii. キャプチャを Desktop Viewerに制限	2203 LTSR (任意の CU), 2212 CR	2203 LTSR 最新CU, 2302 CR	2302	2207	いいえ
iii. マルチモニター	2203 LTSR (任意の CU), 2212 CR	2203 LTSR 最新CU, 2302 CR	2302	2207	なし
DTMF	N/A	2203 LTSR 最新CU, 2302 CR	2302	2207	2301
プロキシサーバーのサポート	N/A	2203 LTSR 最新CU, 2302 CR	2302	2207	2305

機能	VDA (最小バージョン)	WINDOWS 用 CITRIX WORKSPACE アプリ (最小バージョン)	MAC 向け CITRIX WORKSPACE アプリ (最小バージョン)	LINUX 向け CITRIX WORKSPACE アプリ (最小バージョン)	CHROMEOS 用 CITRIX WORKSPACE アプリ (最小バージョン)
アプリ共有	2203 LTSR (任意の CU), 2212 CR	2203 LTSR 最新CU, 2302 CR	2302	2209	なし
ライブキャプション	N/A	2203 LTSR 最新CU, 2302 CR	2302	2207	2303
ダイナミックe911	N/A	2203 LTSR 最新 CU、2302 CR	2302	2207	2301
制御を付与	N/A	2203 LTSR 最新 CU、2302 CR	2302	2207	いいえ
制御を要求	N/A	2203 LTSR 最新 CU、2302 CR	2302	2207	2303
マルチウィンドウ	2203 LTSR (任意の CU), 2212 CR	2203 LTSR 最新CU, 2302 CR	2302	2207	2303
会議の文字起こし	2203 LTSR (任意の CU), 2212 CR	2203 LTSR 最新CU, 2302 CR	2302	2207	2303
背景のぼかし	2203 LTSR (任意の	2203 LTSR 最新のCU, 2302 CR	2302	2212	2303

機能	VDA (最小バージョン)	WINDOWS 用 CITRIX WORKSPACE アプリ (最小バージョン)	MAC 向け CITRIX WORKSPACE アプリ (最小バージョン)	LINUX 向け CITRIX WORKSPACE アプリ (最小バージョン)	CHROMEOS 用 CITRIX WORKSPACE アプリ (最小バージョン)
	CU), 2212 CR				
画面共有 (アプリ保護機能付き)	2203 LTSR (任意の CU), 2212 CR	2402 LTSR, 2309.1 CR	2308	2311	なし
シマルキャスト	2203 LTSR (任意の CU), 2212 CR	2402 LTSR, 2305 CR	2305	2305	2312
セカンダリリンガー	2203 LTSR (任意の CU)、2212 CR	2402 LTSR、2307.1 CR	2308	2308	2312
システムオーディオを共有	2203 LTSR (任意の CU)、2212 CR	2402 LTSR、2403 CR	2405	2402	なし

トラブルシューティングとその他の考慮事項

New Teams については、CTX253754 および Microsoft Teams のトラブルシューティング を参照してください。New Teams に関連する最新情報については、CTX585013 を参照してください。

既知の制限事項

Citrix Workspaceアプリの制限事項

- HID サポート - 通話の応答と終了はサポートされていません。音量の上げ下げはサポートされています。

- ユーザーは、VDA でスニッピングツールを使用している間は、Microsoft Teams のコンテンツのスクリーンショットを撮ることができません。ただし、クライアント側でスニッピングツールを使用すると、コンテンツをキャプチャできます。
- システムオーディオ共有の制限事項
  - RAVE および BCR でリダイレクトされたアプリまたはタブと画面を共有している場合、この機能を使用してオーディオを共有することはできません。
  - この機能は、公開デスクトップでのみサポートされています

VDA の制限事項

- 公開された（シームレスな）アプリケーションとしての New Teams はサポートされていません
  - CVAD 2402 LTSR、2203 LTSR CU5 以降で修正済み
- Citrix WorkspaceアプリのHigh DPI設定を「はい」に構成すると、リダイレクトされたビデオウィンドウがずれて表示されます。この制限は、モニターのDPIスケーリング係数が100%を超えて設定されている場合に発生します。
- Microsoft Teams 2.1 は、一度に 1 つの Web カメラのリダイレクトのみをサポートしています。ただし、シングルセッション VDA では、複数の Web カメラのリダイレクトやプラグアンドプレイ (PnP) Web カメラのリダイレクトはサポートしていません。

Citrix WorkspaceアプリとVDAに関する制限事項

- 最適化された通話の音量は、VDA ではなく、クライアントマシンの音量バーを使用してのみ制御できます。

Microsoftからの制限事項の詳細については、「VDIでサポートされていない機能」を参照してください。

Teams向け新しいVDIソリューション

> **注:**
>
> Teams 向け新しい VDI ソリューションは、Citrix® 上の Windows および Mac エンドポイント向けに現在一般提供されています。このソリューションには、最小限の Microsoft Teams バージョンが必要です。「システム要件」を参照してください(#system-requirements)。

Teams向け新しいVDIソリューションでは、MicrosoftはCitrix Virtual Channel SDKを使用してカスタム仮想チャネルを構築します。エンドポイントでは、メディアは`HdxRtcEngine`ではなく、Microsoftメディアエンジン (SlimCore) にオフロードされます。カスタム仮想チャネルは、VDA上のTeamsとエンドポイント上のメディアエンジン間の通信を伝送します。

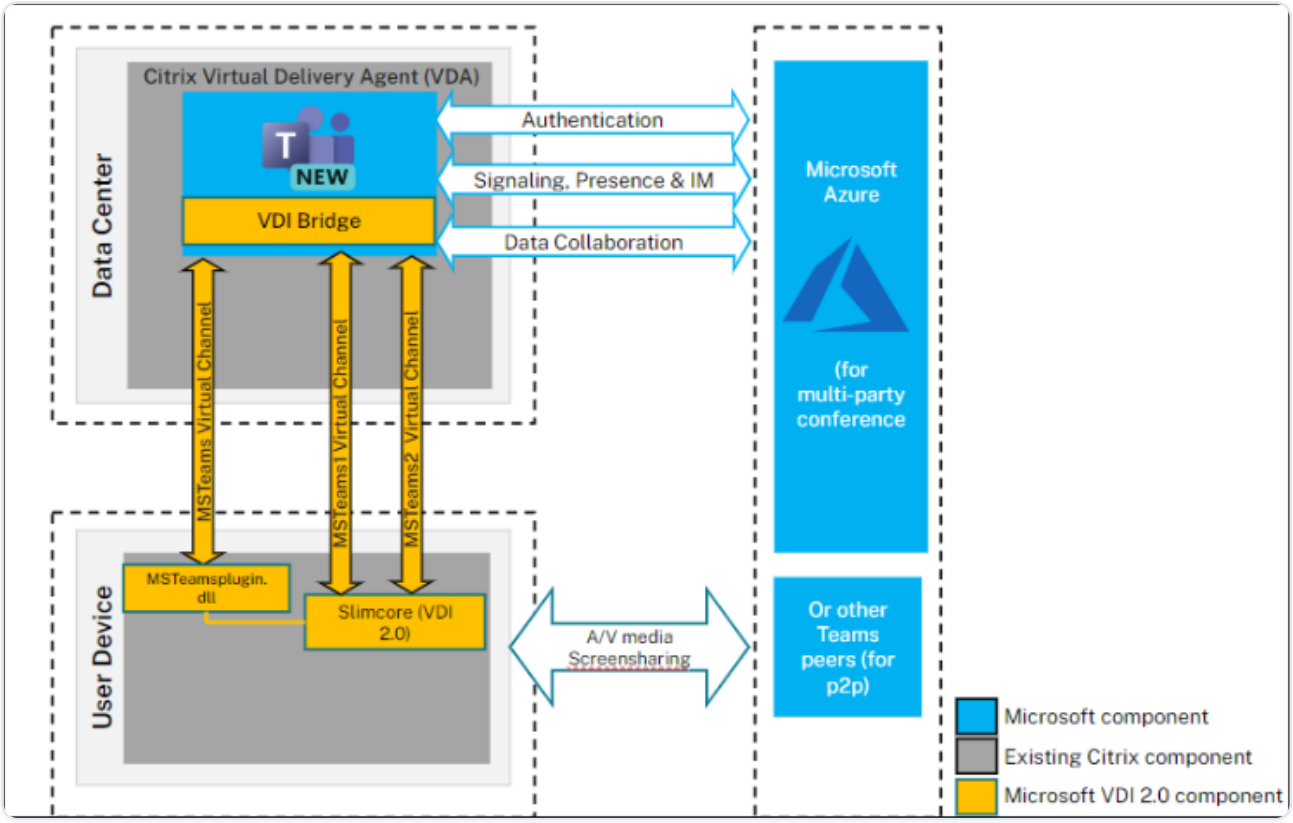
注:

Microsoft は、Windows エンドポイントにおける WebRTC ベースの Citrix HDX™ Optimization for Microsoft Teams の廃止を発表しました。2つのマイルストーンが適用されます。

- October 1, 2026 - サポート終了: MicrosoftまたはCitrixによって公式にサポートされなくなります。
- April 1, 2027 - 提供終了: WebRTCベースの最適化は機能しなくなります。レガシー最適化用のCitrix Studioポリシーは適用されなくなります。

お客様は Teams 向け新しい VDI ソリューションへの移行が推奨されます。この変更は Windows エンドポイントのみに影響します。macOS、Linux、ChromeOS、および HTML5 エンドポイントは影響を受けません。詳細については、Microsoft Blog を参照してください。

このソリューションはMicrosoftが所有および管理しています。Citrixは、関連するCitrixコンポーネント（Citrix Workspace™アプリ、仮想チャネル許可リスト、およびこのページで説明されているプラグイン展開メカニズム）をサポートします。Microsoftが所有するアーキテクチャと詳細については、MicrosoftドキュメントのTeams向け新しいVDIソリューションを参照してください。



システム要件

このセクションでは、Teams 向け新しい VDI ソリューションをサポートするために必要な最小バージョンと推奨バージョンを一覧表示します。最小バージョンでは、一部の重要なバグ修正や最新機能が利用できない場合があります。最高の体験を得るには、推奨バージョンを展開してください。

仮想配信エージェント (VDA)

注:

2203 LTSR CU2以前、または2303 CR以前をご利用の場合は、これらのバージョンの制限事項を理解し、アップグレードを計画するためにCTX682593を参照してください。

最小バージョン	推奨バージョン
2203 LTSR CU3; 2305 CR	2203 LTSR CU5以降; 2402 LTSRおよびそれ以降のCR

Windows用Citrix Workspaceアプリ

最小バージョン	推奨バージョン
2203 LTSR (最新 CU); 2302 CR	2402 LTSR; 2405 CR またはそれ以降

Mac用Citrix Workspaceアプリ

最小バージョン	推奨バージョン
2508.10	2607 またはそれ以降

MacエンドポイントにはmacOS 14、15、または26が必要です。macOS 26には、Citrix Workspaceアプリ2511以降が必要です。Citrix Workspaceアプリ for Mac 2508.10では、プラグインを手動でインストールする必要があります。Citrix Workspaceアプリ、クライアントアプリ管理、または仮想チャネルプラグインマネージャーを介してプラグインをインストールするオプションは、Citrix Workspaceアプリ for Mac 2603以降で利用できます。

Microsoft Teamsの最小バージョン、エンドポイントOS要件、およびハードウェア要件については、Microsoftのドキュメントを参照してください。

コンポーネント

- 新しいTeams `vdiBridge`: Teamsにバンドルされているサーバー側の仮想チャネルモジュール。
- カスタム仮想チャネル（VC）: Microsoft Teamsが所有するカスタムVC。
- プラグイン: クライアント側のVC DLL。メディアエンジンのダウンロードとクリーンアップを担当します。
- メディアエンジン（SlimCore）: MicrosoftがMSIXパッケージとして提供する、オペレーティングシステム固有のメディアエンジン。

展開

1. 前提条件に記載されているMicrosoft Teamsのバージョンがあることを確認してください。
2. Microsoft Teamsの仮想チャネルを許可するように、**仮想チャネル許可リスト**ポリシーを構成します。これらのチャネルにより、Teamsクライアントはクライアント側のプラグインに接続できます。詳細については、「仮想チャネルのセキュリティ」を参照してください。

   このソリューションには、3つのカスタム仮想チャネルが必要です。ワイルドカードを使用して、`ms-teams.exe`実行可能ファイルとカスタム仮想チャネルを許可します。

```
MSTEAMS,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

MSTEAM1,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

MSTEAM2,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe
```

注:

- VDA 2603以降では、これら3つの仮想チャネルがデフォルトで許可されます。これらのバージョンでは、Studioポリシーの構成は不要です。
- 仮想チャネル許可リストポリシーのワイルドカードは、CVAD 2203 LTSR CU2以降、またはCitrix Virtual Apps and Desktops™ 2206 CR以降で利用できます。
- ポリシーを有効にするには、VDAマシンを再起動する必要があります。
- MSTeams のインストールパスは MSIX アプリケーションであるため変更されるため、ワイルドカードが必要です。上記に示されている正確な行を許可してください。

3. このソリューションは、Citrix ポリシーではなく、Microsoft Teams 側のポリシーによって制御されます。デフォルトで有効になっています。特定のユーザーグループに対して有効または無効にするには、Microsoft ドキュメントを参照してください。
4. エンドポイントにTeamsプラグインを展開します。Teamsプラグインをインストールするオプションを参照してください。
5. メディアエンジンのステージングと登録、および MSIX のインストールをブロックできるグループポリシーについては、Microsoft ドキュメントを参照してください。

Teamsプラグインをインストールするオプション

インストール方法に関係なく、プラグインはエンドポイントの Citrix Workspace アプリの場所に配置されます。

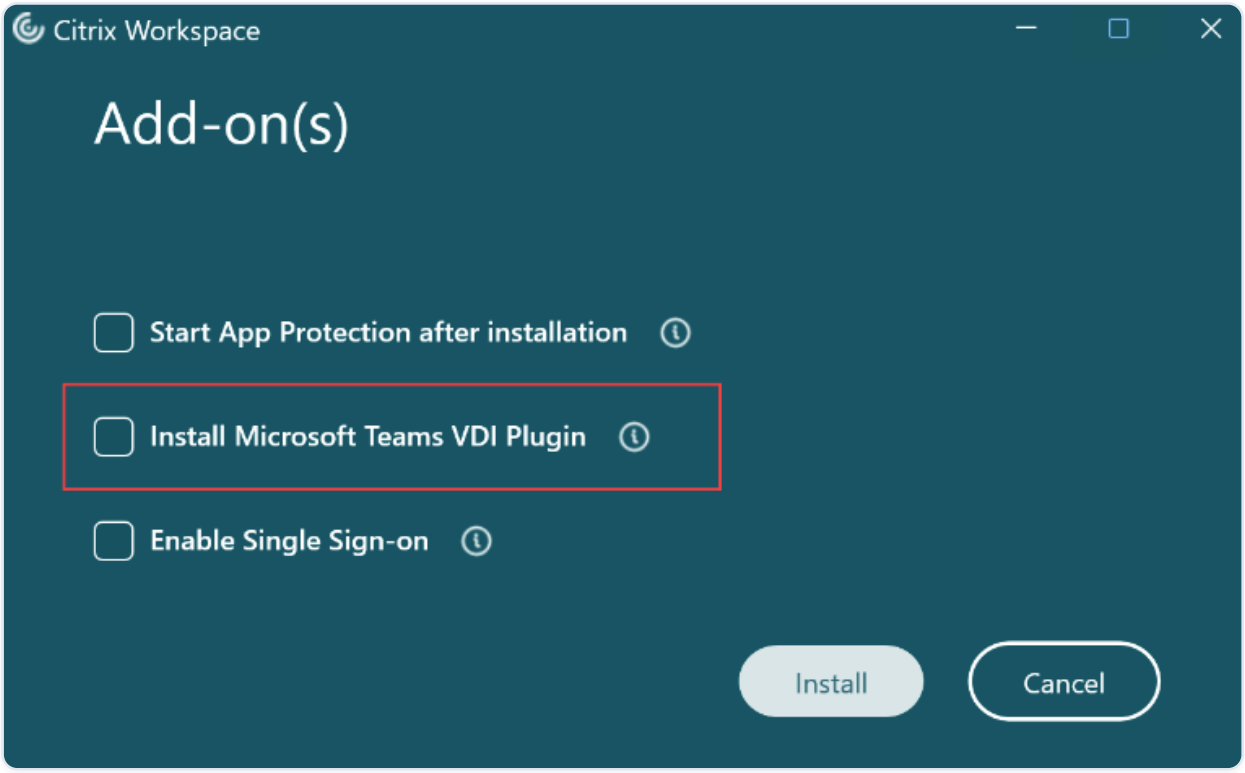
- Windows (`MsTeamsPluginCitrix.dll`): 64 ビット `C:\Program Files (x86)\Citrix\ICA Client`; 32 ビット `C:\Program Files\Citrix\ICA Client`
- Mac: `/Applications/Utilities/MsTeamsVdi.Plugin.app`

注:

- Windows では、仮想チャネルが正しく開くように、Citrix Workspace アプリを管理者モードでインストールします。Citrix Workspace アプリのユーザーごとのインストールはサポートされていません。
- Citrix Workspace アプリが Microsoft Store からインストールされている場合、Microsoft Teams VDI プラグインはサポートされません。
- エンドポイントに Citrix Workspace アプリが見つからない場合、プラグインのインストールは停止します。
- Windows では、プラグインと Citrix Workspace アプリは同じアーキテクチャである必要があります。32 ビットの Citrix Workspace アプリは 64 ビットのプラグインをロードできません。
- プラグインはアップグレードまたは修復できますが、ダウングレードはできません。また、アクティブなセッションがない場合にのみ可能です。

オプション 1: Citrix Workspace アプリのインストールによる方法

- **Windows:** 新規インストールまたは手動アップグレード中に、**アドオン**ページで**Microsoft Teams VDI Pluginをインストール**を選択します。Citrix Workspaceアプリ for Windows 2508以降では、このオプションはデフォルトで選択されています。インストールをスキップするには、このチェックを外します。アップグレードでは、以前の選択が記憶されます。



`/InstallMSTeamsPlugin`スイッチを使用してコマンドラインからインストールすることもできます。たとえば、`CitrixWorkspaceApp.exe /InstallMSTeamsPlugin=Y`はプラグインをインストールし、`/InstallMSTeamsPlugin=N`はインストールを防止します。

新規インストールの場合、最小要件はCitrix Workspaceアプリ for Windows 2402 LTSRです。インプレースアップグレードの場合、最小要件はCitrix Workspaceアプリ for Windows 2405 CRです。最新の詳細については、サードパーティ製プラグインのインストールを参照してください。

- **Mac:** Citrix Workspaceアプリのインストール中にプラグインをインストールするオプションは、Citrix Workspaceアプリ for Mac 2603以降で利用可能であり、ユーザーによる操作が必要です。Citrix Workspaceアプリ for Mac 2607では、プラグインがデフォルトで自動的にインストールされます。Citrix Workspaceアプリ for Mac 2508.10では、プラグインを手動でインストールします。「オプション2：プラグインを直接ダウンロードする」を参照してください。

オプション2: プラグインを直接ダウンロードする

- **Windows:** MSIをダウンロードし、SCCMやIntuneなどのツールを使用して、サポートされている任意のCitrix Workspaceアプリのバージョンに展開します。
  - 32ビットCitrix Workspaceアプリ：aka.ms/plugin
  - 64ビットCitrix Workspaceアプリ：aka.ms/plugin_x64
  - ArmベースのCitrix Workspaceアプリ：aka.ms/plugin_arm64
- **Mac:** aka.ms/macpluginからプラグインをダウンロードし、JAMFなどのツールを使用して展開します。

オプション3: クライアントアプリ管理 (旧Global App Configurationサービス)

クライアントアプリ管理（旧グローバルアプリ構成サービス、またはGACS）は、管理対象および非管理対象のエンドポイントのアプリ設定を管理し、エンドポイント全体にTeamsプラグインを展開できます。Macでは、Citrix Workspaceアプリ for Mac 2603以降が必要です。「Microsoft Teams VDIプラグイン管理」を参照してください。

オプション4: 仮想チャネルプラグインマネージャー

仮想チャネルプラグインマネージャーは、エンドポイントコンポーネントを必要とするアプリケーション（Teams向け新規VDIソリューションを含む）のプラグインをクライアントエンドポイント全体に展開します。VDAで実行されているアプリケーションを検出し、エンドポイントにプラグインをインストールするようにユーザーに促します。管理者はBYODシナリオでこれを使用できます。Macでは、Citrix Workspaceアプリ for Mac 2603以降が必要です。「仮想チャネルプラグインマネージャー」を参照してください。

プラグインの更新シナリオ

プラグインがオプション1、3、または4を通じてインストールされている場合、CitrixはTeamsプラグインの更新をシームレスに処理します。プラグインが手動でインストールされている場合 (オプション2)、Citrixは更新を処理しません。

- プラグインの自動更新のために、Citrix Workspaceアプリの自動更新がオンになっていることを確認してください。
- 少なくともCitrix Workspaceアプリ for Windows 2405以降であることを確認してください。Citrix Workspaceアプリ for Windows 2508以降では、Citrix Workspaceアプリが自動更新されるとプラグインが自動的にインストールされます。
- Citrixはプラグインのアンインストールを処理しません。必要に応じて、プラグインを個別にアンインストールしてください。

> **注:**
>
> CitrixはTeamsプラグインの更新を処理しますが、メディアエンジンは処理しません。Microsoftがメディアエンジンを提供し、更新します。

Citrix公開アプリとしてのTeams

Citrix Virtual Appsアプリケーションとして公開されたTeamsは、必要なすべてのコンポーネントが最小バージョンを満たしている場合、このソリューションで最適化できます。必要なバージョンと既知の制限については、Microsoftドキュメントを参照してください。

相互運用性とローミング

Teams向けの新VDIソリューションとCitrix HDX最適化の相互運用性、およびローミングの動作については、Microsoft Teamsの最適化 を参照してください。

ネットワークに関する考慮事項

Microsoftドキュメントのネットワークに関する考慮事項 を参照してください。

機能サポート

機能セットと実装はMicrosoftが所有しています。Microsoftドキュメントの機能リスト を参照してください。

トラブルシューティング

Microsoft Teamsクライアントは最適化ステータスを報告し、最適化が失敗した場合はエラーコードを報告します。これらのステータスインジケーターとエラーコードはMicrosoftによって定義されています。完全なリストとエンドツーエンドのトラブルシューティングについては、Microsoftドキュメントの Troubleshooting the New VDI solution for Teamsを参照してください。

Citrix Monitorは、このソリューションの最適化状態を可視化します。セッションの詳細では、セッション トポロジ ビューに、アプリケーションが最適化されているかどうか、およびプラグイン マネージャー、プラグインとそのバージョン、仮想チャネルの状態、仮想チャネル許可リストのステータスなど、不足しているコンポーネントが示されます。詳細については、Real-time communications optimization visibilityを参照してください。

一部のMicrosoftエラーコードは、Citrix側の構成を示しています。一般的なCitrixの確認事項:

- Teamsクライアントがカスタム仮想チャネルがブロックされていると報告した場合 (Microsoftエラー2003)、仮想チャネル許可リストにMSTEAMS、MSTEAM1、MSTEAM2が含まれていることを確認してください。
- Teamsクライアントがプラグインが検出されないと報告した場合 (Microsoftエラー2000)、プラグインがインストールされ、ロードされていることを確認してください。Process Explorerで `wfica32.exe` を選択し、下部ペインを表示して、DLLタブで `MsTeamsPluginCitrix.dll` を確認します。
- TeamsクライアントがサポートされていないCitrix Workspaceアプリのバージョンを報告した場合 (Microsoftエラー2004)、サポートされているバージョンにアップグレードしてください。System requirementsを参照してください。

既知の制限事項

機能と実装はMicrosoftが所有しています。MicrosoftドキュメントのKnown issuesを参照してください。

Microsoft Teams (Classic) の最適化

> **注:**
>
> 新しいMicrosoft Teams 2.1は、VDAで一般提供されるようになりました。このMicrosoft Teamsのバージョンは、WebRTC (VDI 1.0) を使用したCitrix Microsoft Teams最適化と互換性があります。

> Citrix Virtual Apps and Desktops 2402以降、`msedgewebview2.exe` レジストリエントリはデフォルトで許可リストに含まれるため、手動で構成する必要はありません。

> 公開アプリケーションは、新しいMicrosoft Teamsでサポートされるようになりました。

> Citrixは、Citrix Virtual Apps and Desktops™およびCitrix Workspace™アプリを使用して、デスクトップベースのMicrosoft Teamsの最適化を提供します。デフォルトでは、必要なすべてのコンポーネントがCitrix WorkspaceアプリとVirtual Delivery Agent (VDA) にバンドルされています。

Microsoft Teamsの最適化には、VDA側のHDX™サービスと、Microsoft Teamsホスト型アプリと連携してコマンドを受信するAPIが含まれます。これらのコンポーネントは、制御仮想チャネル (CTXMTOP) をCitrix Workspaceアプリ側のメディアエンジンに開きます。エンドポイントはマルチメディアをローカルでデコードして提供し、Citrix Workspaceアプリウィンドウをホストされた Microsoft Teamsアプリに戻します。

認証とシグナリングは、他のMicrosoft Teamsサービス（チャットやコラボレーションなど）と同様に、Microsoft Teamsホスト型アプリでネイティブに行われます。オーディオ/ビデオのリダイレクトはこれらに影響しません。

`CTXMTOP` はコマンドおよび制御仮想チャネルです。これは、Citrix WorkspaceアプリとVDAの間でメディアが交換されないことを意味します。

クライアントフェッチ/クライアントレンダリングのみが利用可能です。

このビデオデモンストレーションでは、Citrix仮想環境でMicrosoft Teamsがどのように機能するかを理解できます。

Microsoft Teamsのインストール

CitrixとMicrosoftは、最新バージョンのMicrosoft Teamsを使用し、常に最新の状態に保つことを推奨しています。 現在のバージョンのリリース日から90日以上前のリリース日のMicrosoft Teamsデスクトップアプリバージョンはサポートされていません。 サポートされていないMicrosoft Teamsデスクトップアプリバージョンでは、ユーザーにブロックページが表示され、アプリの更新が要求されます。

最新バージョンについては、「Microsoft Teamsアプリの更新履歴 (デスクトップおよびMac)」を参照してください。

Microsoft Teams のマシン全体へのインストールに関するガイドライン に従うことをお勧めします。`AppData` に Microsoft Teams をインストールする .exe インストーラーの使用は避けてください。代わりに、コマンドラインから `ALLUSER=1` フラグを使用して `C:\Program Files (x86)\Microsoft\Teams` にインストールしてください。

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1 ALLUSERS=1
```

この例では、`ALLUSERS=1` パラメーターも使用しています。このパラメーターを設定すると、Microsoft Teams Machine-Wide Installer が **コントロールパネル** の **プログラムと機能** に表示されます。また、コンピューターのすべてのユーザーの Windows 設定の **アプリと機能** にも表示されます。これにより、管理者資格情報を持つすべてのユーザーが Microsoft Teams をアンインストールできます。

`ALLUSERS=1` と `ALLUSER=1` の違いを理解することが重要です。`ALLUSERS=1` パラメーターは、非 VDI 環境と VDI 環境の両方で使用できます。`ALLUSER=1` パラメーターは、マシンごとのインストールを指定するために VDI 環境でのみ使用してください。

`ALLUSER=1` モードでは、新しいバージョンがリリースされても Microsoft Teams アプリケーションは自動更新されません。このモードは、Windows Server または Windows 10 のランダム/プールされたカタログから提供されるホスト型共有アプリやデスクトップなど、非永続的な環境に推奨されます。詳細については、MSI を使用した Microsoft Teams のインストール (VDI インストールセクション) を参照してください。

Windows 10 の専用永続 VDI 環境があるとします。Microsoft Teams アプリケーションを自動更新し、Microsoft Teams を `Appdata/Local` の下にユーザーごとにインストールしたい場合は、`.exe` インストーラーまたは `ALLUSER=1` なしの MSI を使用してください。

注記：

Citrix では、ゴールデンイメージに Microsoft Teams をインストールする前に VDA をインストールすることをお勧めします。このインストール順序は、`ALLUSER=1` フラグを有効にするために必要です。VDA をインストールする前に仮想マシンに Microsoft Teams をインストールした場合は、Microsoft Teams をアンインストールして再インストールしてください。

Remote PC Accessの場合

Citrix では、VDA のインストール後に Microsoft Teams バージョン 1.4.00.22472 以降をインストールすることをお勧めします。そうしないと、Microsoft Teams が VDA を期待どおりに検出するために、サインアウトして再度サインインする必要があります。バージョン 1.4.00.22472 以降には、VDA 検出のために Microsoft Teams の起動時およびサインイン時に実行される拡張ロジックが含まれています。これらのバージョンには、アクティブなセッションタイプ識別 (HDX、RDP、またはクライアントマシンへのローカル接続) も含まれています。ローカルに接続されている場合、以前のバージョンの Microsoft Teams は、ブレイクアウトルーム、会議やチャットのポップアウトウィンドウ、会議のリアクションなど、特定の機能や UI 要素の検出と無効化に失敗する可能性があります。

> **重要：**
>
> ローカルセッションから HDX セッションにローミングし、Microsoft Teams がバックグラウンドで開いたまま実行されている場合、HDX で正しく最適化するには、Microsoft Teams を終了して再起動する必要があります。 逆に、最適化された HDX セッションを介して Microsoft Teams をリモートで使用している場合、HDX セッションを切断し、デバイスで同じ Windows セッションにローカルで再接続します。オフィスで作業している場合は、Microsoft Teams が Remote PC Access の状態 (HDX またはローカル) を正しく検出できるように、Microsoft Teams を再起動する必要があります。これは、Microsoft Teams が VDI モードをアプリの起動時にのみ評価でき、すでにバックグラウンドで実行されている間は評価できないためです。再起動しないと、Microsoft Teams はポップアウトウィンドウ、ブレイクアウトルーム、会議のリアクションなどの機能の読み込みに失敗する可能性があります。

App Layeringの場合

Citrix App Layering を使用して VDA と Microsoft Teams のインストールを異なるレイヤーで管理する場合、コマンドラインから `ALLUSER=1` フラグを使用して Microsoft Teams をインストールする前に、Windows VDA にレジストリキーを作成する必要があります。詳細については、Multimedia の「*Citrix App Layering を使用した Microsoft Teams の最適化*」セクションを参照してください。

プロファイル管理の推奨事項

Windows Server およびプール型 VDI Windows 10 環境向けに、マシン全体インストーラーを使用することをお勧めします。

コマンドラインから MSI に **ALLUSER=1** フラグが渡されると (マシン全体インストーラーの場合)、Microsoft Teams アプリは `C:\Program Files (x86)` (~300 MB) にインストールされます。このアプリは、ログに `AppData\Local\Microsoft\TeamsMeetingAddin` を、ユーザー固有の構成、ユーザーインターフェイスの要素のキャッシュなどに `AppData\Roaming\Microsoft\Teams` (~600〜700 MB) を使用します。

> **重要:**
>
> **ALLUSER=1** フラグを渡さない場合、MSI は Teams.exe インストーラーと `setup.json` を `C:\Program Files (x86)\Teams Installer` に配置します。レジストリキー (TeamsMachineInstaller) が `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run` に追加されます。
>
> その後のユーザーログオンで、代わりに **AppData** に最終インストールがトリガーされます。

マシン全体インストーラー

以下は、任意の Windows Server 64 ビット VM に Microsoft Teams マシン全体インストーラーをインストールすることによって作成されるフォルダー、デスクトップショートカット、およびレジストリの例です。

フォルダー:

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

デスクトップショートカット:

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

レジストリ:

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- 名前: `Teams`

- 種類: `REG_SZ`
- 値: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> **注:**
>
> レジストリの場所は、基盤となるオペレーティングシステムとビット数によって異なります。

推奨事項

- Microsoft Teams のレジストリキーを削除して、自動起動を無効にすることをお勧めします。これにより、同時に発生する多数のログオン（たとえば、勤務開始時など）による VM の CPU スパイクを防ぐことができます。
- 仮想デスクトップに GPU/vGPU がない場合は、パフォーマンスを向上させるために、Microsoft Teams の で を設定することをお勧めします。この設定 (`"disableGpu":true`) は、`desktop-config.json` の `%Appdata%\Microsoft\Teams` に保存されます。ログオンスクリプトを使用してそのファイルを編集し、値を `true` に設定できます。
- Citrix Workspace Environment Management™ (WEM) を使用している場合は、Microsoft Teams のプロセッサ消費を管理するために を有効にします。

ユーザーごとのインストーラー

`.exe` インストーラーを使用する場合、インストールプロセスは異なります。すべてのファイルは AppData に配置されます。

フォルダー:

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

デスクトップショートカット:

`C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe"`

レジストリ:

`HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

ベストプラクティス

ベストプラクティスに関する推奨事項は、ユースケースのシナリオに基づいています。 非永続的なセットアップでMicrosoft Teamsを使用する場合、効率的なMicrosoft Teamsのランタイムデータ同期のためにプロファイルキャッシュマネージャーが必要です。プロファイルキャッシュマネージャーを使用すると、ユーザーセッション中に適切なユーザー固有の情報がキャッシュされます。たとえば、ユーザー固有の情報には、ユーザーデータ、プロファイル、設定が含まれます。これら2つのフォルダーのデータを同期します。

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

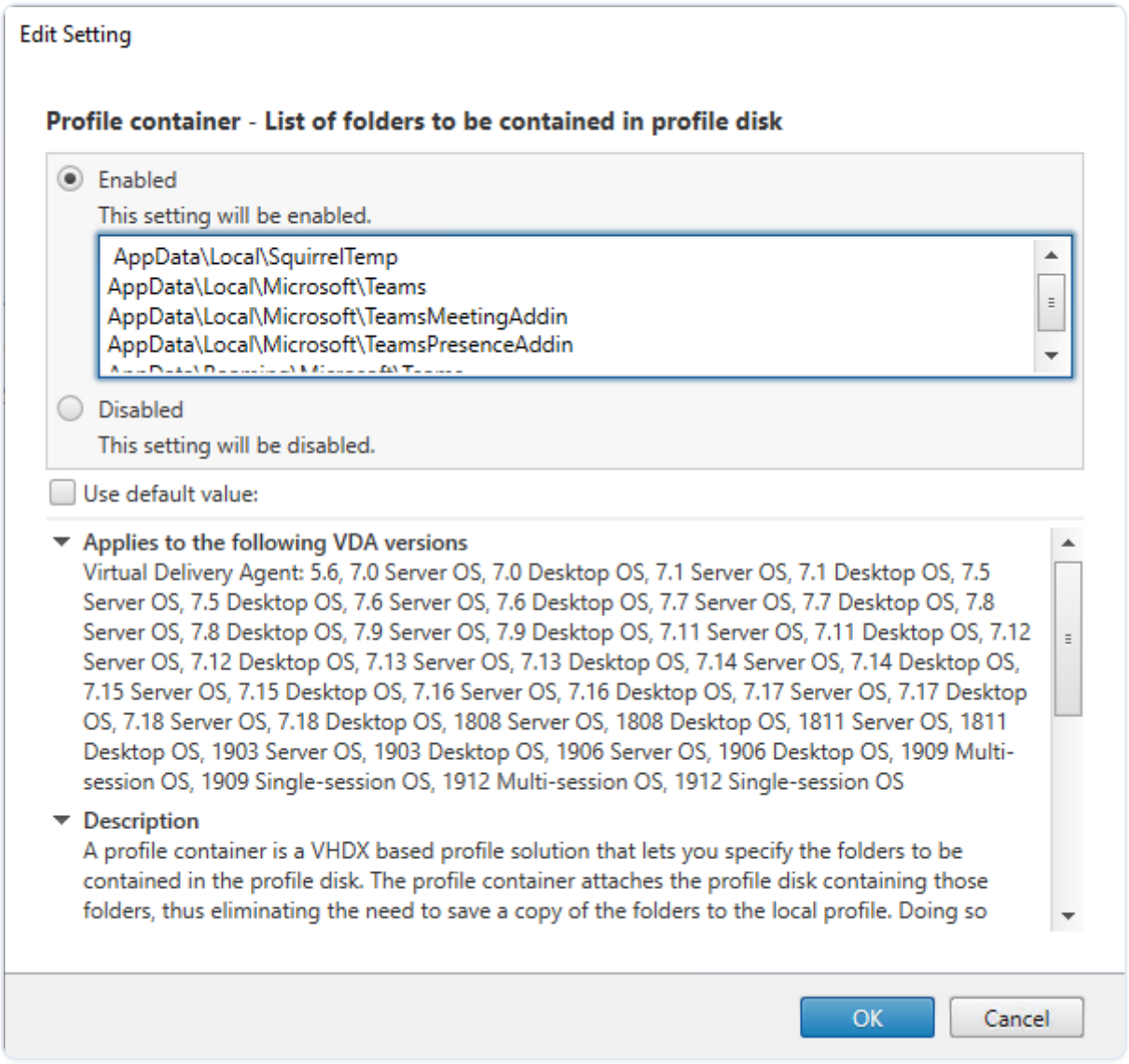
非永続的セットアップ向けの Microsoft Teams キャッシュコンテンツ除外リスト

Microsoftのドキュメントに記載されているように、Microsoft Teamsのキャッシュフォルダーからファイルとディレクトリを除外します。この操作は、ユーザーのキャッシュサイズを削減し、非永続的なセットアップをさらに最適化するのに役立ちます。

ユースケース: シングルセッションシナリオ

このシナリオでは、エンドユーザーは一度に1つの場所でMicrosoft Teamsを使用します。2つのWindowsセッションで同時にMicrosoft Teamsを実行する必要はありません。一般的な仮想デスクトップ展開では、各ユーザーに1つのデスクトップが割り当てられ、Microsoft Teamsは仮想デスクトップに1つのアプリケーションとして展開されます。 Citrix Profileコンテナを有効にし、Per-user installerに記載されているユーザーごとのディレクトリをコンテナにリダイレクトすることをお勧めします。

1. ゴールデンイメージにMicrosoft Teamsのコンピューター全体インストーラー (**ALLUSER=1**) を展開します。
2. Citrix Profile Managementを有効にし、適切な権限でユーザープロファイルストアを設定します。
3. 次のProfile Managementポリシー設定を有効にします: **ファイルシステム > 同期 > プロファイルコンテナ – プロファイルディスクに含めるフォルダーのリスト。**



この構成におけるすべてのユーザーごとのディレクトリをリストします。これらの設定は、Citrix Workspace Environment Management (WEM) サービスを使用して構成することもできます。

4. 設定を適切なデリバリーグループに適用します。
5. ログインして展開を検証します。

システム要件

推奨される最小バージョン - Delivery Controller (DDCs) 1906.2

以前のバージョンを使用している場合は、Microsoft Teamsの最適化を有効にするを参照してください:

サポートされているオペレーティングシステム:

- Windows Server 2022、2019、2016、2012R2 StandardおよびDatacenterエディション、ならびにServer Coreオプション

最小バージョン - Virtual Delivery Agents (VDA) 1906.2

サポートされているオペレーティングシステム:

- ウィンドウズ 11
- Windows 10 64ビット、バージョン1607以降。VMホスト型アプリは、Citrix Workspaceアプリ for Windows 2109.1以降でサポートされています。
- Windows Server 2022, 2019, 2016, および 2012 R2 (Standard および Datacenter エディション)

要件:

- BCR_x64.msi - Microsoft Teamsの最適化コードを含むMSIで、GUIから自動的に起動します。VDAインストールのコマンドラインインターフェイスを使用している場合でも、除外しないでください。

推奨バージョン – Citrix Workspaceアプリ for Windows 最新CR、最小バージョン – Citrix Workspaceアプリ 1907 for Windows

- ウィンドウズ 11。
- Windows 10 (32ビットおよび64ビットエディション、Embeddedエディションを含む) (Windows 7のサポートはバージョン2006で終了) (Windows 8.1のサポートはバージョン2204.1で終了)。
- ウィンドウズ 10 IoT エンタープライズ 2016 LTSB (v1607) および 2019 LTSC (v1809)。
- サポートされるプロセッサ (CPU) アーキテクチャ: x86およびx64 (ARMはサポートされていません)。
- エンドポイント要件: ピアツーピアのビデオ会議中に720p HD解像度をサポートできる、約2.2～2.4 GHzのデュアルコアCPU。
- デュアルコアまたはクアッドコアCPUで、ベース速度が低く（約1.5 GHz）、Intel Turbo BoostまたはAMD Turbo Coreを搭載し、少なくとも2.4 GHzまでブーストできるもの。
- 動作確認済みHPシンクライアント: t630/t640、t730/t740、mt44/mt45。
- 動作確認済みDellシンクライアント: 5070、5470 Mobile TCおよびAIO。
- 動作確認済み10ZiGシンクライアント: 4510および5810q。
- 動作確認済みエンドポイントの完全なリストについては、「シンクライアント」を参照してください。
- Citrix Workspaceアプリには、最低600 MBの空きディスク容量と1 GBのRAMが必要です。

- Microsoft .NET Frameworkの最小要件はバージョン4.8です。Citrix Workspaceアプリは、システムに.NET Frameworkが存在しない場合、自動的にダウンロードしてインストールします。

管理者は、Microsoft Teams最適化ポリシーを変更することで、最適化モードでMicrosoft Teamsを有効/無効にできます。Citrix Workspaceアプリで最適化モードで起動するユーザーは、Microsoft Teamsを無効にできません。

最小バージョン - Linux用Citrix Workspaceアプリ2006

詳しくは、Citrix WorkspaceアプリfoLinuxのドキュメントにあるMicrosoft Teamsの最適化を参照してください。

ソフトウェア:

- `GStreamer` 1.0以降またはCairo 2
- `libc++-9.0` 以降
- `libgdk` 3.22 以降
- OpenSSL 1.1.1d
- `libnsl`
- Ubuntu 20.04 以降

認証の強化:

- Libsecretライブラリ
- libunwind-12ライブラリ。詳しくは、llvm-12のlibunwind-12ライブラリ依存関係の追加を参照してください。

ハードウェア:

- ピアツーピアのビデオ会議通話中に720p HD解像度をサポートできる、最小1.8 GHzデュアルコアCPU
- ベース速度1.8 GHz、Intel Turbo Boostの高速が2.9 GHz以上のデュアルコアまたはクアッドコアCPU

検証済みエンドポイントの完全なリストについては、シンクライアントを参照してください。

詳細については、Citrix Workspaceアプリのインストール要件を参照してください。

`/opt/Citrix/ICAClient/config/module.ini`ファイルで**VDWEBRTC**フィールドの値をOffに更新することで、Microsoft Teamsの最適化を無効にできます。デフォルトはVDWEBRTC=Onです。更新が完了したら、セッションを再起動してください。(ルート権限が必要です)。

最小バージョン - Mac用Citrix Workspaceアプリ2012

サポートされているオペレーティングシステム:

- マックオーエス カタリナ (10.15)。
- macOS Big Sur 11.0.1以降。
- マックオーエス モントレー。

サポートされる機能:

- オーディオ
- ビデオ
- 画面共有の最適化 (送受信)

> **注:**
>
> Citrix Viewerアプリが画面共有を機能させるには、macOSの「セキュリティとプライバシー」設定へのアクセスが必要です。ユーザーは、**Appleメニュー > システム設定 > セキュリティとプライバシー > プライバシー > 画面収録**でこの設定を構成し、**Citrix Viewer**を選択します。

> Microsoft Teamsの最適化は、Citrix Workspaceアプリ2012以降およびmacOS 10.15でデフォルトで機能します。

Microsoft Teamsの最適化を無効にする場合は、ターミナルでこのコマンドを実行し、Citrix Workspaceアプリを再起動してください。

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

最小バージョン - ChromeOSの最新バージョンで実行されているChromeOS用Citrix Workspaceアプリの最新バージョン

ハードウェア:

- Intel i3、クアッドコア2.4 GHzと同等以上の性能を持つプロセッサ。

サポートされている機能:

- オーディオ
- ビデオ

- 画面共有の最適化（送受信） - デフォルトでは無効です。有効にする方法については、これらの設定を参照してください。

シングルサーバのスケーラビリティ

このセクションでは、単一の物理ホストでサポートできるユーザー数または仮想マシン（VM）数を推定するための推奨事項とガイダンスを提供します。これは一般に、Citrix Virtual Apps and Desktopsのシングルサーバのスケーラビリティ（SSS）と呼ばれます。Citrix Virtual Apps（CVA）またはセッション仮想化のコンテキストでは、ユーザー密度としても一般的に知られています。その目的は、主要なハイパーバイザーを実行している単一のハードウェアで、いくつのユーザーまたはVMを実行できるかを明らかにすることです。

注:

このセクションには、SSS を推定するためのガイダンスが含まれています。このガイダンスは一般的なものであり、お客様固有の状況や環境に必ずしも特化したものではない場合があります。Citrix Virtual Apps and Desktops の SSS を真に理解する唯一の方法は、Login VSI のようなスケーラビリティまたはロードテストツールを使用することです。Citrix は、SSS を迅速に推定するためだけに、このガイダンスとこれらの簡単なルールを使用することを推奨します。ただし、特にハードウェアを購入したり、財務上の決定を下したりする前に、結果を検証するために Login VSI または選択したロードテストツールを使用することを Citrix は推奨します。

ハードウェア (テスト対象システム)

- デル パワーエッジ R740
- Intel Xeon (Gold) 6126 @ 2.60 GHz (最大ターボ 3.70 GHz)、ソケットあたり 12 コア、Hyperthreading 有効のデュアルソケット
- 382 GB の RAM
- ローカル SSD RAID 0 ストレージ (11 ディスク) 6 TB

ソフトウェア

Citrix Virtual Apps and Desktops 2106 を実行する Windows 2019 (TSVDA) を搭載した単一の仮想マシン (40 論理プロセッサ) VMware ESXi 6.7

用語

- ナレッジワーカーのワークロード: Acrobat Reader、Freemind/Java、Photo viewer、Edge、および Excel、Outlook、PowerPoint、Word などの MS Office アプリが含まれます。
- ベースライン: ナレッジワーカーのワークロード (Microsoft Teams なし) で実行されるサーバーのスケーラビリティテスト。
- Microsoft Teams ワークロード: ナレッジワーカーの一般的なワークロード + Microsoft Teams。

Microsoft Teams のストレステスト方法

- Microsoft Teams は HDX で最適化されています。そのため、すべてのマルチメディア処理はエンドポイントまたはクライアントにオフロードされ、測定には含まれません。
- ワークロードが開始される前に、すべてのMicrosoft Teamsプロセスが停止または終了されます。
- Microsoft Teams を開く（コールドスタート）。
- Microsoft Teams がロードされ、Microsoft Teams のプライマリウィンドウがフォーカスを取得するまでにかかる時間を測定します。
- キーボードショートカットを使用してチャットウィンドウに切り替える。
- キーボードショートカットを使用してカレンダーウィンドウに切り替える。
- キーボードショートカットを使用して、特定のユーザーにチャットメッセージを送信します。
- キーボードショートカットを使用してMicrosoft Teamsウィンドウに切り替えます。

結果

- Microsoft Teams ワークロード（81ユーザー）では、ベースライン（137ユーザー）と比較して、スケーラビリティに40%の影響があります。
- サーバー容量を約40%（CPUで）増やすと、ベースラインワークロードの場合と同様にユーザー数が回復します。
- Microsoft Teams ワークロードでは、ベースラインと比較して20%の追加メモリが必要です。
- ユーザーあたりのストレージサイズを512〜1024 MB増やします。
- IOPS書き込みが約50%増加し、IOPS読み取りが約100%増加します。Microsoft Teamsは、ストレージが遅い環境では大きな影響を与える可能性があります。

機能マトリックスとバージョンサポート

機能	MICROSOFT TEAMS (最小バージョン)	VDA (最小バージョン)	WINDOWS CR 向け CITRIX WORKSPACE アプリ (最小バージョン)	MAC 向け CITRIX WORKSPACE アプリ (最小バージョン)	LINUX 向け CITRIX WORKSPACE アプリ (最小バージョン)	CHROME OS 向け CITRIX WORKSPACE アプリ (最小バージョン)
オーディオ/ビデオ (P2P および会議)	現在のバージョンから90日前	1906	1907	2009	2004	2105.5
画面共有	現在のバージョンから90日前	1906	1907	2012	2006	2105.5
i. 画面インジケーターの赤い枠線	現在のバージョンから90日を引いたもの	1906	2002	2012	2006	いいえ
ii. キャプチャを Desktop Viewerに制限	現在のバージョンから90日を引いたもの	1906	2009.5	2012	2006	いいえ
iii. マルチモニター	現在のバージョンから90日前	1912 CU6+	2106 (1)	2106	2106	いいえ
DTMF	現在のバージョンから90日前	N/A	2102	2101	2101	2111.1

機能	MICROSOFT TEAMS (最小バージョン)	VDA (最小バージョン)	WINDOWS CR 向け CITRIX WORKSPACE アプリ (最小バージョン)	MAC 向け CITRIX WORKSPACE アプリ (最小バージョン)	LINUX 向け CITRIX WORKSPACE アプリ (最小バージョン)	CHROME OS 向け CITRIX WORKSPACE アプリ (最小バージョン)
プロキシサーバーのサポート	現在のバージョンから90日前	N/A	2012 (2)	2104 (3)	2101 (3)	2305
アプリ共有	現在のバージョンから90日前	2109	2109.1	2203.1	2209	なし
ライブキャプション	現在のバージョンから90日前	N/A (4)	2109.1	2109	2109	2303
動的e911	現在のバージョンから90日前	N/A	2112.1	2112	2112	2112
制御を付与	現在のバージョンから90日前	N/A	2112.1	2203.1	いいえ	いいえ
制御を要求	現在のバージョンから90日前	N/A	2112.1	2203.1	2203	2303
マルチウィンドウ	1.5.00.11865	2112, 1912 CU6 (5)	2112.1	2203.1	2203	2303

機能	MICROSOFT TEAMS (最小バージョン)	VDA (最小バージョン)	WINDOWS CR 向け CITRIX WORKSPACE アプリ (最小バージョン)	MAC 向け CITRIX WORKSPACE アプリ (最小バージョン)	LINUX 向け CITRIX WORKSPACE アプリ (最小バージョン)	CHROME OS 向け CITRIX WORKSPACE アプリ (最小バージョン)
会議の文字起こし	現在のバージョンから90日前	2112.1, 1912 CU6+	2112	2203.1	2203	2303
背景ぼかし	現在のバージョンから90日前	2112, 1912 CU6+	2207	2301	2212	2303

1. CD Viewerは全画面モードのみ。SHIFT+F2はサポートされていません。
2. Negotiate/Kerberos、NTLM、Basic、およびDigest。`Pac`ファイルもサポートされています。
3. 匿名のみ。
4. VDAが2112以降の場合、ライブキャプションは、Citrix Workspaceアプリのバージョンが MACの場合は2203.1、Linuxの場合は2203、Windowsの場合は2112である場合にのみ機能します。これは、Microsoft Teamsがシングルウィンドウ UIモードまたはマルチウィンドウモードの場合、ライブキャプションの動作が異なるためです。
5. MultiWindowは2112 VDAで導入されましたが、VDA 1912 LTSR CU6リリースにバックポートされました。

注:

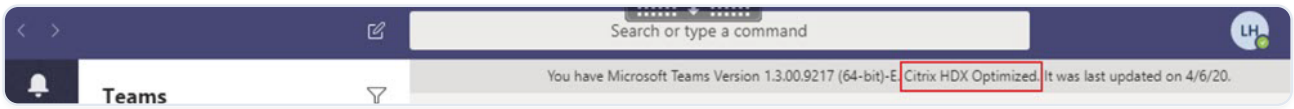
- **Citrix Workspace app for Windows 1912 CU6 (またはそれ以降)**に記載されているすべての機能は、Citrix Workspace app for Windows 2203.1 LTSR CU1に適用されます。
- MicrosoftはMicrosoft Teamsでのシングルウィンドウモードのサポートを非推奨にしました。これに対応するため、VDAを1912 CU6+ LTSRに、Citrix Workspaceアプリを2203 CU2+以降にアップグレードする必要があります。これらはMultiWindowモードをサポートしています。

Microsoft Teamsの最適化を有効にする

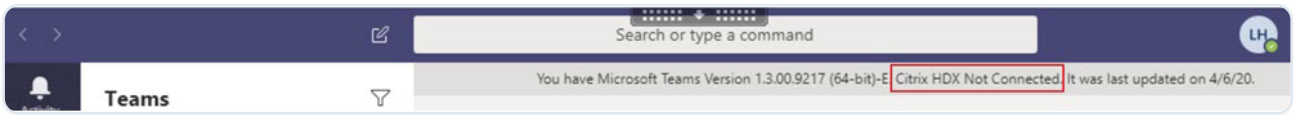
Microsoft Teamsの最適化を有効にするには、Microsoft Teams redirectionポリシーで説明されている管理ポリシーを使用します。このポリシーはデフォルトで**ON**になっています。このポリシーが有効になっていることに加えて、HDXはCitrix Workspaceアプリのバージョンが最低要件を満たしていることを確認します。ポリシーを有効にし、Citrix Workspaceアプリのバージョンがサポートされている場合、VDA上の**HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport**は自動的に**1**に設定されます。Microsoft Teamsは、VDIモードでロードするためにこのキーを読み取ります。

> **注:**
>
> バージョン1906.2以降のVDAを使用している場合、またはManageコンソール（Studio）でポリシーが利用できない古いコントローラーバージョン（バージョン7.15など）を使用している場合でも、VDAは最適化できます。Microsoft TeamsのHDX最適化は、VDAでデフォルトで有効になっています。

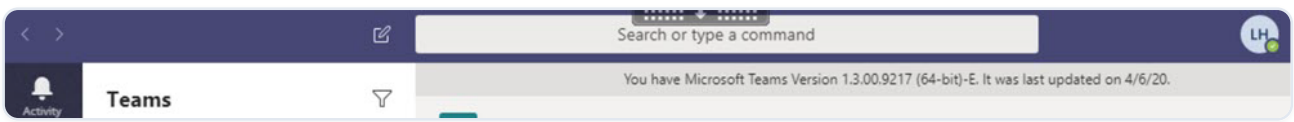
About > Versionをクリックすると、**Citrix HDX Optimized**の凡例が表示されます。



Citrix HDX Not Connectedと表示される場合、Citrix APIはMicrosoft Teamsにロードされています。APIのロードはリダイレクトへの最初のステップです。しかし、スタックの後続の部分でエラーが発生しています。エラーはVDAサービスまたはCitrix Workspaceアプリにある可能性が最も高いです。



凡例が表示されない場合、Microsoft TeamsはCitrix APIのロードに失敗しました。通知領域のアイコンを右クリックしてMicrosoft Teamsを終了し、再起動してください。Manageポリシーが**Prohibited**に設定されておらず、Citrix Workspaceアプリのバージョンがサポートされていることを確認してください。



> **重要: セッションの再接続**

- 接続が変更された場合、HDX最適化セッションを取得するためにMicrosoft Teamsを再起動する必要がある場合があります。たとえば、サポートされていないエンドポイント（iOS、Android、または古いバージョンのWindows/Linux/Mac用Workspaceアプリ）からサポートされているエンドポイント（Windows/Linux/Mac/ChromeOS/HTML5用Workspaceアプリ）にローミングする場合、またはその逆の場合です。
- VDAにMicrosoft Teamsの.exeインストーラーを使用してアプリをインストールした場合も、Microsoft Teamsの再起動が必要です。.exeインストーラーは、永続VDI展開に推奨されます。このような場合、HDXセッションが切断状態のときにMicrosoft Teamsが自動更新されることがあります。そのため、HDXセッションに再接続したユーザーは、Microsoft Teamsが最適化されて実行されていないことに気づきます。
- ローカルセッションからHDXセッションにローミングする場合、HDXで最適化するためにMicrosoft Teamsを再起動する必要があります。この操作は、リモートPCアクセスシナリオで必要です。

ネットワーク要件

Microsoft Teamsは、会議や多人数通話のためにMicrosoft 365のメディアプロセッササーバーに依存しています。また、Microsoft Teamsは、以下のシナリオでMicrosoft 365トランスポートリレーに依存しています。

- ポイントツーポイント通話の2つのピアが直接接続できない場合
- 参加者はメディアプロセッサに直接接続できません。

したがって、ピアとMicrosoft 365クラウド間のネットワークの状態が通話のパフォーマンスを決定します。ネットワーク計画に関する詳細なガイドラインについては、Microsoft 365 network connectivity principlesを参照してください。

クラウド音声およびビデオの全体的な展開に影響を与える可能性のあるリスクと要件を特定するために、環境を評価することをお勧めします。 ネットワークがMicrosoft Teamsに対応しているかどうかをテストするには、Skype for Business Network Assessment Toolを使用してください。サポート情報については、Supportを参照してください。

Real Time Protocol (RTP) トラフィックに関する主要なネットワーク推奨事項の概要

- 支社からMicrosoft 365ネットワークにできるだけ直接接続します。
- 支社で十分な帯域幅を計画し、提供します。
- 各支社のネットワーク接続と品質を確認します。

- 支社で以下のいずれかを使用する必要がある場合は、RTP/UDPトラフィック (Citrix WorkspaceアプリのHdxRtcEngine.exeによって処理されます) が妨げられないことを確認してください。
  - プロキシサーバーのバイパス
  - ネットワークSSLインターセプト
  - ディープパケットインスペクションデバイス
  - VPNヘアピン (可能であればスプリットトンネリングを使用)

> **重要: VPNスプリットトンネル構成**

> HdxRtcEngine.exeトラフィックはVPNトンネルから迂回させ、ユーザーのローカルインターネット接続を使用してサービスに直接接続できるようにする必要があります。これを実現する方法は、使用するVPN製品とマシンプラットフォームによって異なりますが、ほとんどのVPNソリューションでは、このロジックを適用するためのポリシーの簡単な構成が可能です。VPNプラットフォーム固有のスプリットトンネルガイダンスの詳細については、this Microsoft articleを参照してください。

> Workspaceアプリ (HdxRtcEngine.exe) のWebRTCメディアエンジンは、クライアントにオフロードされるマルチメディアストリームにSecure Real-time Transport Protocol (SRTP) を使用します。SRTPは、RTPに機密性と認証を提供します。この機能では、対称鍵 (DTLSでネゴシエート) を使用して、AES暗号化方式でメディアと制御メッセージを暗号化します。

良好なユーザーエクスペリエンスのために、以下のメトリックが推奨されます。

メトリック	エンドポイントからMICROSOFT 365まで
遅延 (片道)	< 50 ミリ秒
遅延 (RTT)	< 100 ミリ秒
パケット損失	15秒間隔で1%未満
パケット到着間隔ジッター	15秒間隔で30ミリ秒未満

詳細については、Microsoft Teams 用に組織のネットワークを準備するを参照してください。

帯域幅要件については、Microsoft Teams の最適化では、オーディオ (OPUS/G.722/PCM G711) およびビデオ (H264) 用にさまざまなコーデックを使用できます。

ピアは、セッション記述プロトコル (SDP) Offer/Answer を使用して、通話確立プロセス中にこれらのコーデックをネゴシエートします。 Citrix のユーザーあたりの最小推奨事項は次のとおりです。

タイプ	帯域幅	コーデック
音声 (双方向)	約 90 kbps	G.722
音声 (双方向)	約 60 kbps	オーパス*
ビデオ (双方向)	約 700 kbps	H264 360p、30フレーム/秒、16:9
画面共有	約 300 kbps	H264 1080p、15フレーム/秒

* Opus は、6 kbpsから510 kbpsまでの定ビットレートおよび可変ビットレートエンコーディングをサポートします。

OpusとH264は、ピアツーピアおよび電話会議に推奨されるコーデックです。

重要:

パフォーマンスに関して、クライアントマシンでのCPU使用率では、デコードよりもエンコードの方がコストがかかります。LinuxおよびWindows版のCitrix Workspaceアプリで、最大エンコード解像度をハードコードできます。エンコーダーのパフォーマンス見積もりおよびMicrosoft Teamsの最適化を参照してください。

プロキシサーバー

プロキシの場所に応じて、以下を考慮してください。

- VDAでのプロキシ構成:

  VDAで明示的なプロキシサーバーを構成し、localhostへの接続をプロキシ経由でルーティングすると、リダイレクトは失敗します。プロキシを正しく構成するには、 **>>>** で 設定を選択し、 `127.0.0.1:9002` をバイパスする必要があります。

PACファイルを使用する場合、PACファイルからのVDAプロキシ構成スクリプトは、`wss://127.0.0.1:9002`に対して **DIRECT** を返す必要があります。そうでない場合、最適化は失敗します。スクリプトが **DIRECT** を返すことを確認するには、`shExpMatch(url, "wss://127.0.0.1:9002/*")`を使用します。

- Citrix Workspaceアプリでのプロキシ構成:

  支社がプロキシ経由でインターネットにアクセスするように構成されている場合、以下のバージョンがプロキシサーバーをサポートします。

  - Windows版Citrix Workspaceアプリバージョン2012 (Negotiate/Kerberos、NTLM、Basic、Digest。`Pac`ファイルもサポートされています)
  - Windows版Citrix Workspaceアプリバージョン1912 CU5 (Negotiate/Kerberos、NTLM、Basic、Digest。`Pac`ファイルもサポートされています)
  - Linux版Citrix Workspaceアプリバージョン2101 (匿名認証)
  - Mac版Citrix Workspaceアプリバージョン2104 (匿名認証)

以前のバージョンのCitrix Workspaceアプリを使用しているクライアントデバイスは、プロキシ構成を読み取ることができません。これらのデバイスは、トラフィックをMicrosoft 365 TURNサーバーに直接送信します。

重要:

- クライアントデバイスがDNS解決を行うためにDNSサーバーに接続できることを確認します。クライアントデバイスは、以下のMicrosoft Teamsリレーサーバーの FQDNを解決できる必要があります。
  - `worldaz.relay.teams.microsoft.com`
  - `inaz.relay.teams.microsoft.com`
  - `uaeaz.relay.teams.microsoft.com`
  - `euaz.relay.teams.microsoft.com`
  - `usaz.relay.teams.microsoft.com`
  - `turn.dod.teams.microsoft.us`
  - `turn.gov.teams.microsoft.us`

DNS要求が失敗した場合、外部ユーザーとのP2P通話およびメディア確立を伴う会議通話は失敗します。

- 会議サーバーの場所は、最初の参加者の仮想デスクトップの場所に基づいて選択されます（クライアントではありません）。

通話の確立とメディアフローパス

可能な場合、Citrix WorkspaceアプリのHDX WebRTCメディアエンジン (HdxRtcEngine.exe) は、ピアツーピア通話でUser Datagram Protocol (UDP) を介した直接のネットワークSecure Real-time Transport Protocol (SRTP) 接続を確立しようとします。UDPハイポートがブロックされている場合、メディアエンジンはTCP/TLS 443にフォールバックします。

HDXメディアエンジンは、候補の検出と接続の確立のために、ICE、NAT用セッショントラバーサルユーティリティ（STUN）、およびNAT周辺リレーを使用したトラバーサル（TURN）をサポートしています。このサポートは、エンドポイントがDNS解決を実行できる必要があることを意味します。

2つのピア間、またはピアと会議サーバー間に直接パスがなく、多人数通話または会議に参加しているシナリオを考えてみましょう。HdxRtcEngine.exeは、Microsoft 365のMicrosoft Teamsトランスポートリレーサーバーを使用して、他のピアまたは会議がホストされているメディアプロセッサに到達します。クライアントマシンは、3つのMicrosoft 365サブネットIPアドレス範囲と4つのUDPポート（UDPがブロックされている場合はフォールバックとしてTCP/TLS 443）にアクセスできる必要があります。詳細については、通話設定 および Office 365のURLとIPアドレス範囲ID 11 のアーキテクチャ図を参照してください。

ID	カテゴリ	アドレス	宛先ポート
11	最適化が必要	13.107.64.0/18, 52.112.0.0/14, 52.122.0.0/15	**UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (フォールバック)

これらの範囲には、Azure Load Balancer によってフロントエンド化されたトランスポートリレーとメディアプロセッサの両方が含まれます。 Microsoft Teams トランスポートリレーは STUN および TURN 機能を提供しますが、ICE エンドポイントではありません。また、Microsoft Teams トランスポートリレーは、メディア、TLS を終端したり、トランスコーディングを行ったりしませ

ん。他のピアまたはメディアプロセッサにトラフィックを転送する際に、TCP (HdxRtcEngine.exe が TCP を使用する場合) を UDP にブリッジできます。

Workspace app WebRTC メディアエンジンは、Microsoft 365 クラウド内で最も近い Microsoft Teams トランスポートリレーに接続します。メディアエンジンは、エニーキャスト IP とポート 3478～3481 UDP (ワークロードごとに異なる UDP ポートですが、多重化が発生する可能性があります)、またはフォールバック用に 443 TCP/TLS を使用します。通話品質は、基盤となるネットワークプロトコルに依存します。UDP は常に TCP よりも推奨されるため、ブランチオフィスで UDP トラフィックに対応できるようにネットワークを設計することをお勧めします。

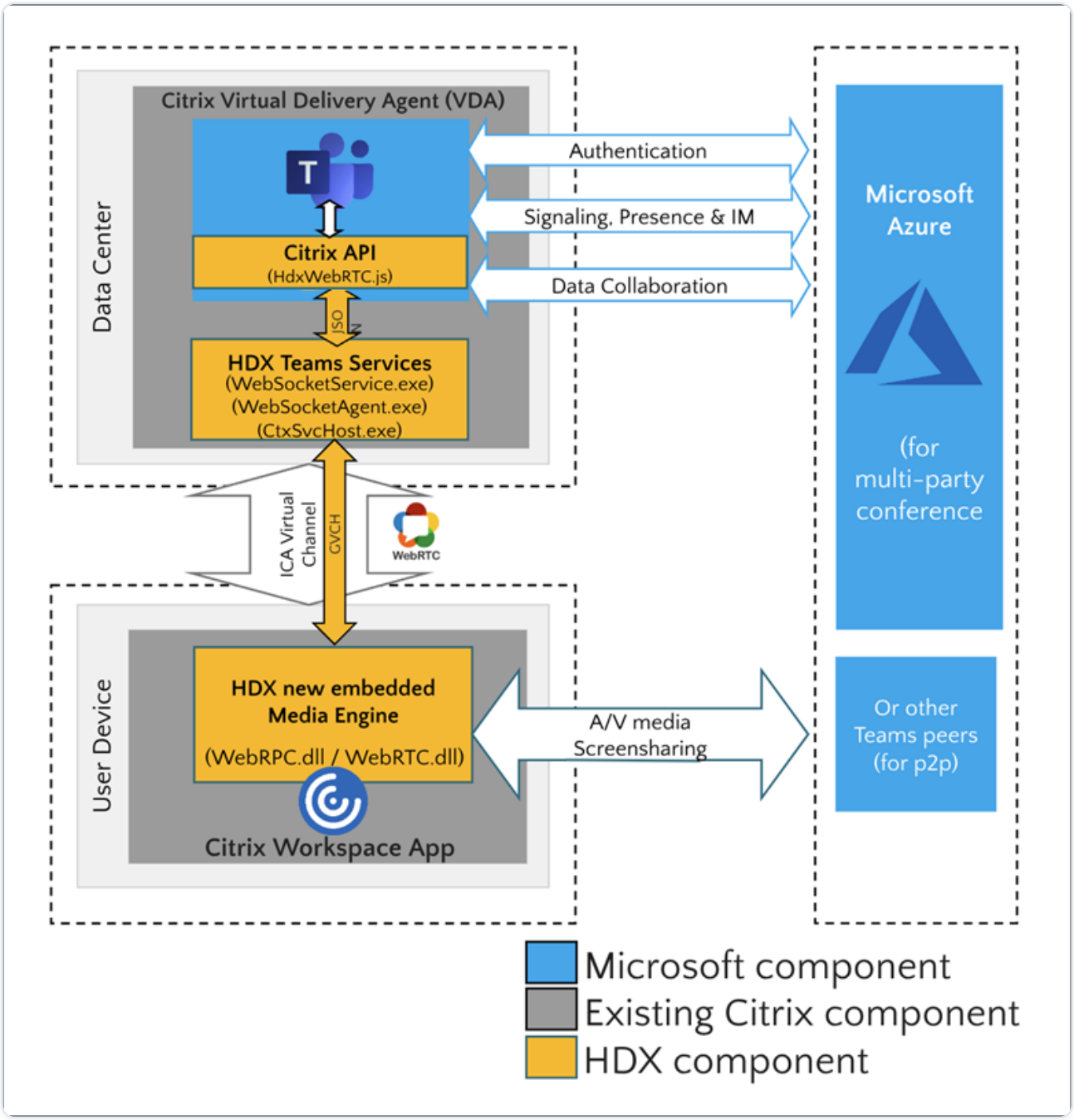
Microsoft Teams が最適化モードでロードされ、HdxRtcEngine.exe がエンドポイントで実行されている場合、ICE の障害により、通話設定の失敗や、音声/ビデオが片方向のみになる可能性があります。通話が完了できない場合や、メディアストリームが全二重でない場合は、まずエンドポイントの **Wireshark トレース**を確認してください。ICE 候補収集プロセスに関する詳細については、「サポート」セクションの「ログの収集」を参照してください。

> **注:**
>
> エンドポイントがインターネットにアクセスできない場合でも、両方のユーザーが同じ LAN 上にあれば、ピアツーピア通話を行うことができる場合があります。会議は失敗します。この場合、通話設定が開始されるまでに 30 秒のタイムアウトがあります。

通話設定

このアーキテクチャ図を、通話フローシーケンスの視覚的な参照として使用してください。対応する手順は図に示されています。

アーキテクチャ



1. Microsoft Teams を起動します。
2. Microsoft Teams は O365 に対して認証を行います。テナントポリシーは Microsoft Teams クライアントにプッシュダウンされ、関連する TURN およびシグナリングチャネル情報がアプリに中継されます。
3. Microsoft Teams は VDA で実行されていることを検出し、Citrix JavaScript API に API 呼び出しを行います。
4. Microsoft Teams 内の Citrix JavaScript は、VDA で実行されている WebSocketService.exe へのセキュアな WebSocket 接続を開き、これによりユーザーセッション内で WebSocketAgent.exe が起動します。

5. WebSocketAgent.exe は、Citrix HDX Microsoft Teams Redirection Service (CtxSvcHost.exe) を呼び出すことにより、汎用仮想チャネルをインスタンス化します。
6. Citrix Workspace アプリの wfica32.exe (HDX エンジン) は、HdxRtcEngine.exe と呼ばれる新しいプロセスを起動します。これは、Microsoft Teams の最適化に使用される新しい WebRTC エンジンです。
7. Citrix メディアエンジンと Teams.exe は双方向の仮想チャネルパスを持ち、マルチメディア要求の処理を開始できます。

   -----ユーザー通話------

8. **ピア A** が **通話** ボタンをクリックします。Teams.exe は Microsoft 365 の Microsoft Teams サービスと通信し、**ピア B** とのエンドツーエンドのシグナリングパスを確立します。Microsoft Teams は HdxRtcEngine に一連のサポートされている通話パラメーター (コーデック、解像度など。これらは Session Description Protocol (SDP) オファーとして知られています) を要求します。これらの通話パラメーターは、シグナリングパスを使用して Microsoft 365 の Microsoft Teams サービスに中継され、そこからもう一方のピアに中継されます。
9. SDP オファー/アンサー (シングルパスネゴシエーション) はシグナリングチャネルを介して行われ、ICE 接続チェック (STUN バインド要求を使用した NAT およびファイアウォールトラバーサル) が完了します。その後、Secure Real-time Transport Protocol (SRTP) メディアは HdxRtcEngine.exe ともう一方のピアの間で直接流れます (会議の場合は Microsoft 365 会議サーバー)。

マイクロソフト フォン システム

Phone System は、Microsoft Teams を使用して Microsoft 365 クラウドで通話制御と PBX を可能にする Microsoft のテクノロジーです。Microsoft Teams の最適化は、Microsoft 365 Calling Plans または Direct Routing を使用して Phone System をサポートします。Direct Routing を使用すると、追加のオンプレミスソフトウェアなしで、サポートされている独自のセッションボーダーコントローラーを Microsoft Phone System に直接接続できます。 通話キュー、転送、フォワード、保留、ミュート、通話の再開がサポートされています。

DTMF

デュアルトーン多周波（DTMF）機能は、以下のバージョンのCitrix Workspaceアプリ（およびそれ以降）でサポートされています。

- Citrix Workspace アプリ for Windows バージョン 2102
- Citrix Workspaceアプリ Windows版 LTSR 1912 CU5 (Windows 10 OSのみ)
- Citrix Workspaceアプリ for Linux バージョン 2101

- Citrix Workspaceアプリ for Mac バージョン 2101
- ChromeOS向けCitrix Workspaceアプリ バージョン2111.1

動的e911のサポート

バージョン2112以降、Citrix Workspaceアプリは動的緊急通報をサポートしています。Microsoft Calling Plans、Operator Connect、およびDirect Routingで使用する場合、以下のことが可能になります。

- 緊急通報の設定とルーティング。
- セキュリティ担当者への通知。

通知は、VDAで実行されているMicrosoft Teamsクライアントではなく、エンドポイントで実行されているCitrix Workspaceアプリの現在の場所に基づいて提供されます。

Ray Baum法では、911通報者の派遣可能な位置情報を適切な公共安全応答拠点（PSAP）に送信することが義務付けられています。HDXによるMicrosoft Teamsの最適化は、以下のバージョンのCitrix Workspaceアプリで使用する場合、Ray Baum法に準拠しています。

- Citrix Workspaceアプリ for Windows バージョン 2112.1 以降
- Citrix Workspaceアプリ for Linux バージョン 2112 以降
- Citrix Workspaceアプリ for Mac バージョン 2112 以降
- ChromeOS版Citrix Workspaceアプリ バージョン2112以降

動的緊急通報を有効にするには、管理者はMicrosoft Teams管理センターを使用して、ネットワークまたは緊急ロケーションマップを作成するために以下を構成する必要があります。

- ネットワーク設定
- ロケーション情報サービス (LIS)

動的緊急通報の詳細については、Microsoftのドキュメントを参照してください。

Citrix WorkspaceアプリがMicrosoft Teamsに中継するディスパッチ可能な位置情報は次のとおりです。

- イーサネット/スイッチ接続用のリンク層検出プロトコル (LLDP) を使用したシャーシID / ポートID。イーサネット/スイッチ (LLDP) は以下でサポートされています。
  - Windows バージョン 8.1 および 10

    - LLDP有効化ソフトウェアを必要とするmacOS。LLDP有効化ソフトウェアをダウンロードするには、`www.microsoft.com`にアクセスしてLLDP有効化ソフトウェアを検索してください。
    - Linux。シンクライアントのオペレーティングシステム (OS) ディストリビューションにLLDPライブラリを含める必要があります。

- Citrix Workspaceアプリがインストールされているエンドポイントの{WLAN BBSIDおよびIPv4-IPv6; サブネット; MACアドレス}。
    - サブネットおよびWiFiベースのロケーションは、Windows、Linux、およびMac版のWorkspaceアプリでサポートされています。
- Citrix Workspaceアプリがインストールされ、OSレベルでユーザー権限が付与されている場合 (権限がHDX RTC Engineに設定されている場合) の緯度と経度。
    - すべてのWorkspaceアプリプラットフォームでサポートされています。ただし、Citrix Workspace for Linuxの場合、シンクライアントのOSディストリビューションに`libgps`ライブラリを含める必要があります (>sudo apt-get install libgps23 gpsd lldpd)。

ファイアウォールの考慮事項

ユーザーがMicrosoft Teamsクライアントを使用して最適化された通話を初めて開始するときに、**Windows ファイアウォール**の設定に関する警告が表示されることがあります。この警告は、HdxTeams.exeまたはHdxRtcEngine.exe (HDX Overlay Microsoft Teams) の通信を許可するようユーザーに求めます。

ファイアウォールの警告](/en-us/citrix-virtual-apps-desktops/2411/media/firewall1.png)

Windows Defender Firewall > Advanced Securityコンソールの**受信の規則**に、次の4つのエントリが追加されます。必要に応じて、より制限の厳しい規則を適用できます。

ファイアウォールの受信規則](/en-us/citrix-virtual-apps-desktops/2411/media/firewall2.png)

Microsoft Teams と Skype for Business の共存について

Microsoft Teams と Skype for Business は、機能が重複する2つの個別のソリューションとして並行して展開できます。 詳しくは、「Understand Microsoft Teams and Skype for Business coexistence and interoperability」を参照してください。

Citrix RealTime Optimization PackおよびMicrosoft Teamsマルチメディアエンジン用のHDX最適化は、環境で設定された構成を尊重します。例としては、アイランドモードや、Microsoft Teamsと

のSkype for Businessコラボレーションが挙げられます。また、Microsoft TeamsとのSkype for Businessコラボレーションおよび会議も含まれます。

周辺機器へのアクセスは、一度に1つのアプリケーションにのみ許可できます。たとえば、通話中にRealTime Media EngineがWebカメラにアクセスすると、通話中はイメージングデバイスがロックされます。デバイスが解放されると、Microsoft Teamsで利用できるようになります。

Microsoft TeamsとSkypeの共存](/en-us/citrix-virtual-apps-desktops/2411/media/teams-coexist.png)

Citrix SD-WAN™: Microsoft Teams向けに最適化されたネットワーク接続

最適なオーディオおよびビデオ品質には、低遅延、低ジッター、低パケット損失のMicrosoft 365クラウドへのネットワーク接続が必要です。支店拠点のCitrix Workspaceアプリユーザーからの Microsoft Teamsオーディオビデオ RTPトラフィックを、インターネットに接続する前にデータセンターにバックホールすると、過度の遅延が発生する可能性があります。また、WANリンクで輻輳を引き起こす可能性もあります。Citrix SD-WANは、Microsoft 365ネットワーク接続の原則に従ってMicrosoft Teamsの接続を最適化します。Citrix SD-WANは、Microsoft RESTベースの Microsoft 365 IPアドレスとWebサービス、および近接DNSを使用して、Microsoft Teamsトラフィックを識別、分類、および誘導します。

多くの地域で、ビジネスブロードバンドインターネット接続は、断続的なパケット損失、過剰なジッター期間、および停止に悩まされています。

Citrix SD-WANは、ネットワークの状態が不安定または劣化している場合に、Microsoft Teamsのオーディオビデオ品質を維持するための2つのソリューションを提供します。

- Microsoft Azureを使用している場合、Azure VNETに展開されたCitrix SD-WAN仮想アプライアンス（VPX）は、高度な接続最適化を提供します。これらの最適化には、シームレスなリンクフェイルオーバーとオーディオパケットレーシングが含まれます。
- Citrix SD-WANのお客様は、Citrix Cloud™ Directサービスを介してMicrosoft 365に接続できます。このサービスは、すべてのインターネット向けトラフィックに対して信頼性の高い安全な配信を提供します。

ブランチオフィスのインターネット接続の品質が問題にならない場合は、遅延を最小限に抑えるだけで十分な場合があります。遅延を最小限に抑えるために、Microsoft Teamsのトラフィックを Citrix SD-WANブランチアプライアンスから最寄りのMicrosoft 365フロントドアに直接誘導します。詳細については、「Citrix SD-WAN Office 365の最適化」を参照してください。

シトリックス SD-WAN](/en-us/citrix-virtual-apps-desktops/2411/media/sd-wan.png)

複数ウィンドウの会議とチャット

Windowsでは、Microsoft Teamsで複数の会議またはチャットウィンドウを使用できます。ポップアウト機能の詳細については、Microsoft 365サイトの「Microsoft Teamsのチャットと会議用ポップアウトウィンドウ」を参照してください。

> **注:**
>
> この機能は、Citrix Workspaceアプリ for Windows 2112.1、Mac 2203、Linux 2203、ChromeOS 2303でサポートされています。VDA 2112以降が必要で、1912 CU6+ LTSRにバックポートされました。

背景のぼかしと背景効果

Citrix Workspaceアプリ for Windows、Mac、Linux、およびChromeOS/HTML5は、HDXによるMicrosoft Teamsの最適化で背景のぼかしと背景効果をサポートしています。

背景をぼかしたり、デフォルトの画像に置き換えたりすることで、会話がシルエット（体と顔）に集中できるようにし、予期せぬ邪魔を避けることができます。この機能はP2Pまたは電話会議で使用できます。

> **注:**
>
> この機能はMicrosoft TeamsのUI/ボタンと統合されています。MultiWindowのサポートは前提条件であり、VDAを2112以降に更新する必要があります。詳細については、「複数ウィンドウの会議とチャット」を参照してください。

> 背景のぼかしと効果に関するMicrosoft Teams UIコントロールには、以下の最小バージョンが必要です。

- Citrix Workspace アプリ Windows 用 2207
- Citrix Workspace アプリ Mac 用 2301
- Citrix Workspace アプリ Linux 2307向け
- ChromeOS 2303 用 Citrix Workspace アプリ

制限事項:

- 背景画像を Microsoft Teams のデフォルト画像に置き換える間、クライアントはインターネットに接続されている必要があります。
- 管理者およびユーザー定義の背景画像の置き換えは、Microsoft Teams UI ではサポートされていません。カスタム背景画像は、画像がクライアントにも保存されている場合、クライアントの構成設定を使用して構成できます。

カスタム背景画像の設定

以下のレジストリキーは、Microsoft Teams UI を使用して機能を制御する予定がない場合、または管理者がデフォルトの動作を上書きしたい場合にのみ必要です。たとえば、エンドポイントの性能が十分でないため、背景のぼかしを無効にする場合などです。

Windows の場合

カスタム背景画像を設定するには、管理者またはエンドユーザーがクライアントまたはエンドポイントで以下のレジストリキーを構成する必要があります。

場所: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- 名前: VideoBackgroundEffect
- 種類: DWORD
- 値: 0 (無効)、1 (有効)、2 (背景画像の置き換え)

値が 1 に設定されている場合、背景がぼかされます。エンドユーザーまたは管理者がこの値を設定できます。

値が 2 に設定されている場合、**VideoBackgroundImage** キーも存在する必要があります。この値は管理者のみが設定できます。以下のキーは、背景画像を置き換えたい場合のみ必要であり、ぼかしには必要ありません。

- 名前: VideoBackgroundImage
- 種類: REG_SZ
- 値: my_image_name.jpeg

ビデオの背景画像は、`C:\Program Files (x86)\Citrix\ICA Client`ディレクトリに存在する必要があります。

このレジストリ構成は、Microsoft TeamsのUIセレクターなしで、Citrix Workspaceアプリ2206での背景のぼかしまたは画像の置き換えを有効にするためにも使用できます。言い換えれば、環境またはVDAがマルチウィンドウをサポートしていない場合でも、Citrix Workspaceアプリ2206以降

でHKCUレジストリの回避策を適用して同様の結果を達成できますが、ユーザーはHDXセッションまたはMicrosoft Teams通話中にその機能を制御することはできません。

レジストリキーの変更は、HDXセッションが接続したときにのみ有効になります。

Macの場合

ユーザーがダウンロードした画像の場所: */Users/username/Downloads/any_image.png*

次のコマンドを実行して、カスタム画像をデフォルト画像として設定します。

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2
```

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "/Users/username/Downloads/any_image.png"
```

Linuxの場合

ユーザーがダウンロードした画像の場所: */home/username/Downloads/any_image.jpg*

ファイル */var/.config/citrix/hdx_rtc_engine/config.json* を作成し、以下の構成キーをJSON形式で追加します。例：

```
{


"VideoBackgroundEffect":2,


"VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"


}
```

HTML5の場合

1. **HTML5Client** フォルダー内の **configuration.js** ファイルに移動します。
2. 属性 **backgroundEffects** を追加し、属性を **true** に設定します。例:

```
'features' : {

    'msTeamsOptimization' :

    {

        'backgroundEffects' : true

    }

}
```

3. 変更を保存します。

クライアントCPU消費に関する考慮事項

ぼかし機能はCPUへの負荷が低いですが、消費量の増加が予想されます。たとえば、4コア、1.5 GHz Intel® Pentium® Silverチップ（TurboBoostで最大2.8 GHz）を搭載したシンクライアントでは、背景のぼかしによりCPU使用率が約2%増加します。平均CPU使用率は20%未満です。

Microsoft Teamsのギャラリービューとアクティブスピーカー

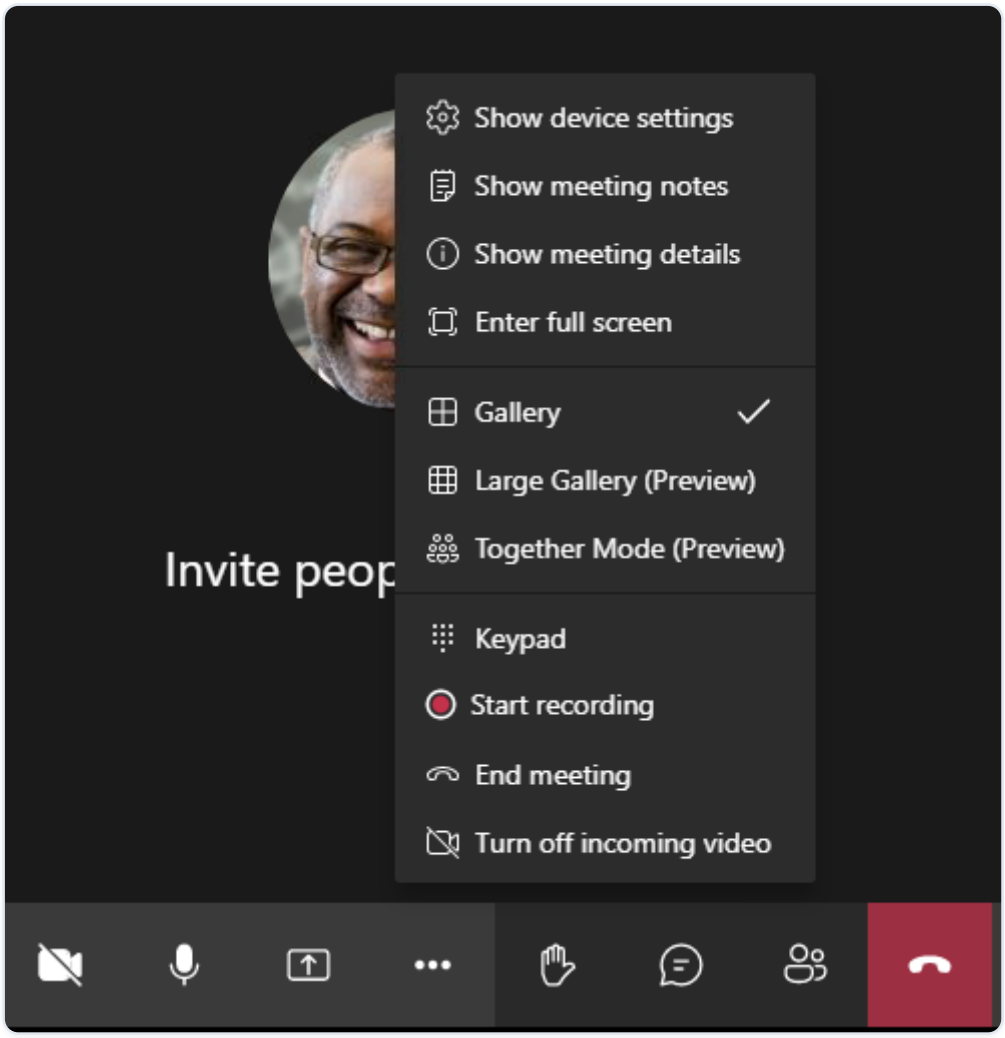
Microsoft Teamsは、**ギャラリー**、**大規模ギャラリー**、および**Togetherモード**のレイアウトをサポートしています。

Microsoft Teamsは、4人の参加者のビデオストリームを2x2のグリッドで表示します（**ギャラリー**として知られています）。この場合、Microsoft Teamsは4つのビデオストリームをクライアントデバイスに送信してデコードします。4人を超える参加者がビデオを共有している場合、画面には最後に最もアクティブだった4人の話者のみが表示されます。

Microsoft Teamsは、最大7x7のグリッドを持つ大規模ギャラリービューも提供します。その結果、Microsoft Teams会議サーバーは単一のビデオフィードを合成し、それをクライアントデバイスに送信してデコードするため、CPU消費量が削減されます。この単一のマトリックス形式のフィードには、ユーザーのセルフプレビュービデオも含まれる場合があります。

最後に、Microsoft Teamsは新しい会議エクスペリエンスの一部である**Togetherモード**をサポートしています。AIセグメンテーションテクノロジーを使用して参加者を共有背景にデジタル配置することで、Microsoft Teamsはすべての参加者を同じ講堂に配置します。

ユーザーは、会議中に省略記号メニューで**ギャラリー**、**大規模ギャラリー**、または**Togetherモード**のレイアウトを選択することで、これらのモードを制御できます。



ビデオアスペクト比の制約のサポート（Citrix Workspace app for Windows 2102、Citrix Workspace app for Linux 2106、Citrix Workspace app for MAC 2106以降）：

- **フレームに合わせる**オプションは、ギャラリー/大規模ギャラリービューで利用できます。このオプションは、サブウィンドウに収まるようにビデオサイズをトリミングします。一方、**フレームにフィット**は、ビデオの側面に黒いバー（レターボックス）を表示するため、トリミングは行われません。

次の表は、ギャラリーレイアウトと大規模ギャラリーレイアウトの比較を示しています。

	ギャラリービュー 2X2 (デフォルト)	ラージギャラリービュー
レイアウト / グリッド	4人の参加者のビデオストリームを含む2x2グリッドを表示します。画面には直近で最もアクティブな4人の発言者のみが表示され、他の参加	49人の参加者のビデオストリームを含む7x7グリッドを表示します。

	ギャラリービュー 2X2 (デフォルト)	ラージギャラリービュー
	者はグリッドに表示されません。	
ミキシング技術	メディアルーターは、各参加者からの個別のストリームをすべてのユーザーに転送します。	中央会議サーバーは、すべてのオーディオまたはビデオをミキシングおよびトランスコードして、各参加者向けに調整された複合レイアウトを作成します。この処理により、追加の遅延が発生する場合があります。
アクティブスピーカー	新しいアクティブスピーカーは、グリッド内で最もアクティブでないスピーカーと入れ替わります。	アクティブか非アクティブかに関わらず、すべての参加者を表示します。
エンドポイントでのエンコード	Simulcastが有効になっている場合、1つ以上のビデオストリームがエンドポイントでエンコードされることがあります。Simulcastのサポートの詳細については、Simulcastを参照してください。	Simulcastが有効になっている場合、1つ以上のビデオストリームがエンドポイントでエンコードされることがあります。Simulcastのサポートの詳細については、Simulcastを参照してください。
エンドポイントでのデコード	各参加者は最大4つの個別のメディアストリームを受信します。これにより、HdxRtcEngine.exeによるエンドポイントでのCPU消費量が増加します（デコード/レンダリングのため）。	各参加者は、オーディオとビデオの単一ストリームのみを受け取ります。この設定により、エンドポイントでのCPU消費が削減されます。
最大解像度	720p。4人の参加者がビデオを共有している場合、ビデオフィードあたりの最大解像度は360pです。4人未満の参加者がビデオを共有している場合、ビデオフィードあたりの	複合レイアウトまたはミキシングの場合は720p。複合レイアウトでは、参加者ごとに高品質のビデオストリームは必要ありません。この条件により、各送信者は解像度または

	ギャラリービュー 2X2 (デフォルト)	ラージギャラリービュー
	解像度は高くなる可能性があります。	アップロードビットレートを削減します。
「低速ユーザー」の問題	送信者は、各モダリティ（オーディオ/ビデオ/画面共有）の品質を、参加者間の最低共通ネットワーク品質に調整します。このマルチメディアストリームは、その後、他のすべての参加者に転送されます。その結果、ネットワーク状態の悪い参加者が、通話中の他の全員の品質に影響を与えます。	最低共通ネットワーク品質のシナリオの影響を受けにくい。会議サーバーは、個々の参加者のネットワーク状態に基づいて異なる品質を提供します。
セルフプレビュー	リアルタイムで自分を小さなサムネイルで表示します。	自分をサムネイルで表示し、残りのビデオフィードと混合します。その結果、メインのビデオレイアウトに自分が含まれているのが、多少の遅延を伴って表示される場合があります。

Microsoft Teamsでの画面共有

Microsoft Teamsは、ビデオベースの画面共有（VBSS）に依存しており、H264などのビデオコーデックで共有されているデスクトップを効果的にエンコードし、高解像度ストリームを作成します。HDX最適化により、受信画面共有はビデオストリームとして扱われます。

Windows、Linux、Mac向けのCitrix Workspaceアプリ2109以降、およびChromeOS向けのCitrix Workspaceアプリ2303以降では、ユーザーは画面とビデオカメラを同時に共有できます。

以前のバージョンでは、ビデオ通話中に相手がデスクトップの共有を開始すると、元のカメラビデオフィードは一時停止されます。代わりに、画面共有ビデオフィードが表示されます。その後、相手は手動でカメラ共有を再開する必要があります。

> **PowerPoint Liveに関する注意**

PowerPoint Liveからコンテンツを共有している場合、この制限はありません。その場合、他のピアは引き続きあなたのウェブカメラとコンテンツを見ることができ、他のスライドを確認するために前後に移動できます。このシナリオでは、スライドはVDAでレンダリングされます。PowerPoint Liveのスライドデッキにアクセスするには、「共有トレイ」ボタンをクリックして、提案されたPowerPointスライドのいずれかを選択するか、「参照」をクリックして、コンピューターまたはOneDrive上のPowerPointファイルを見つけます。

送信画面共有も最適化され、Citrix Workspaceアプリにオフロードされます。この場合、メディアエンジンは、赤い枠線が描かれたCitrix Desktop Viewer (CDViewer.exe) ウィンドウのみをキャプチャして送信します。Desktop Viewerと重なっているローカルアプリケーションはキャプチャされません。

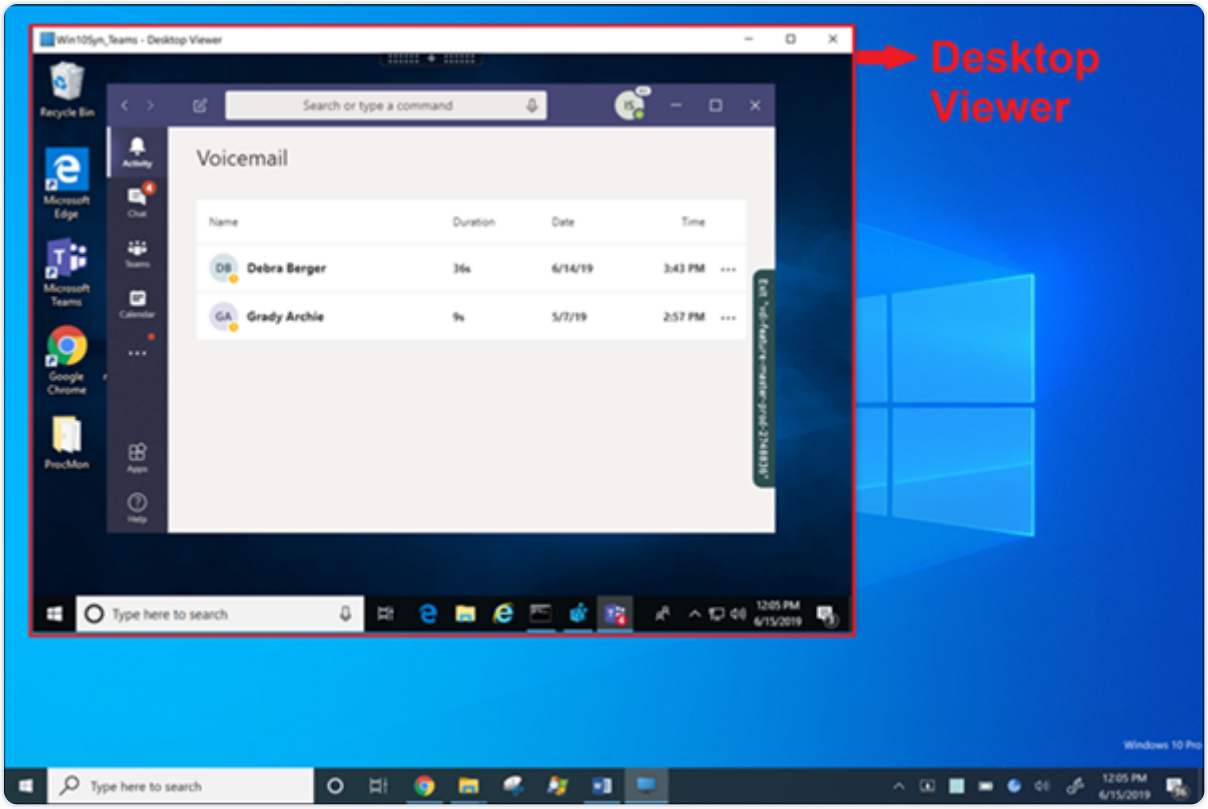
注

画面共有を有効にするには、Mac版Citrix Workspaceアプリで特定の権限を設定します。詳細については、システム要件を参照してください。

既知の制限:

- Desktop Viewerが無効になっている場合、またはDesktop Lockが使用されている場合、Microsoft Teamsの画面ピッカーでマルチモニター選択は利用できません。Desktop Viewerは、`.ICA`ファイルテンプレートを編集するか、`StoreFront web.config`によって無効にされることがあります。SHIFT+F2ホットキーはマルチモニター画面共有と互換性がありません。
- Workspaceアプリのバージョン2106より古い場合、プライマリモニターのみが共有されます。通話中の他のピアに見せるには、仮想デスクトップ内のアプリケーションをプライマリモニターにドラッグしてください。
- Citrix Workspaceアプリを仮想モニターレイアウト機能（単一の物理モニターの論理パーティション）で構成している場合、マルチモニター画面共有が機能しないことがあります。この場合、すべての仮想モニターは複合画像として共有されます。
- Windows版Citrix Workspaceアプリの古いバージョン（1907から2008まで）では、クライアントマシンで実行されているローカルアプリケーションも共有されます。この共有は、ローカルアプリがDesktop Viewerの上に重ねて表示されている場合にのみ可能です。この動作は、2009.6以降および1912 CU5以降で削除されました。

- 画面共有中に、ウィンドウモードから全画面表示に切り替えると、画面共有が停止します。画面共有を機能させるには、一度停止してから再度共有する必要があります。
- 最適化されたMicrosoft Teamsでは、共有コントロールを特定の場所にピン留めすることはできません。
- 最小化されたアプリを共有すると、そのアプリのタイトルバーも共有されることがあります。



シームレスアプリケーションからの画面共有:

Microsoft Teamsをスタンドアロンのシームレスアプリケーションとして公開している場合、画面共有は物理エンドポイントのローカルデスクトップをキャプチャします。Citrix Workspaceアプリの最小バージョン1909が必要です。

アプリ共有

Citrix Workspaceアプリ for Windows 2112.1およびVDA 2112以降、Microsoft Teamsはアプリ共有をサポートしています。

Citrix Workspaceアプリ for Windows 2109、Mac 2203、Linux 2209およびVDA 2109以降、Microsoft Teamsは仮想セッションで実行されている特定のアプリの画面共有をサポートします。最適化されたMicrosoft Teamsを使用して、Javaなどのカスタム社内アプリケーションを共有することもできます。特定のアプリを共有するには：

1. リモートセッション内でMicrosoft Teamsアプリに移動します。
2. Microsoft Teams UIで**コンテンツを共有**をクリックします。

3. 会議で共有するアプリを選択します。選択したアプリの周囲に赤い枠が表示され、通話中のピアは共有されたアプリを見ることができます。

別のアプリを共有するには、もう一度**コンテンツを共有**をクリックして、新しいアプリを選択します。

アプリ共有を無効にする場合は、VDAの`HKLM\SOFTWARE\Citrix\Graphics`に次のレジストリキーを作成します。 名前: `UseWsProvider` 種類: `DWORD` 値: 0

> **注:**
>
> - アプリを最小化すると、Microsoft Teamsは共有アプリの最後の画像を表示します。画面共有を再開するには、ウィンドウを最大化できます。
> - 画面共有は、VDA側でのウィンドウのキャプチャに依存します。コンテンツは最大レートでCitrix Workspaceアプリに中継されます。最大レートは1秒あたり30フレームです。Citrix Workspaceアプリは、コンテンツをピアまたは会議サーバーに転送します。

> Microsoft Teamsのアプリ共有](/en-us/citrix-virtual-apps-desktops/2411/media/ms-teams-app-sharing.png)

特定のアプリの画面共有に関する既知の制限：

- アプリを画面共有している場合、マウス ポインターは表示されません。
- アプリを共有中に最小化すると、画面ピッカーにはアプリのアイコンのみが表示されます。アプリのサムネイルは画面ピッカーにプレビューされません。アプリを最大化するまで、コンテンツを共有できず、赤い枠も表示されません。
- LAAアプリは、VDAの最適化されたMicrosoft Teamsでデスクトップアプリと共有できるアプリのリストを表示します。ただし、リストからアプリを選択しても、期待どおりの結果にならない場合があります。

アプリ保護との互換性 特定のアプリの画面共有は、HDX最適化されたMicrosoft Teamsのアプリ保護機能と互換性があります。アプリ保護が有効になっているデリバリーグループからアプリまたはデスクトップを起動した場合、特定のアプリを画面共有できます。

Microsoft Teams UIで**コンテンツを共有**をクリックすると、画面ピッカーから**デスクトップ**オプションが削除されます。開いているアプリを共有するには、**ウィンドウ**オプションのみを選択できます。

注:

アプリ保護が有効になっているデリバリーグループからアプリまたはデスクトップを起動した場合、Citrix Workspace app for Windows 2202以前を使用していると、受信ビデオまたは画面共有を表示できません。

Microsoft Teamsでの制御の付与と要求

この機能は、Citrix Workspaceアプリの以下のバージョンでサポートされています（VDAバージョン、オペレーティングシステム、シングルセッション、マルチセッションには依存しません）。

- Citrix Workspace app for Windowsバージョン2112.1以降
- Citrix Workspace app for Macバージョン2203.1以降
- Citrix Workspace app for Linuxバージョン2203以降
- Citrix Workspace app for ChromeOSバージョン2303以降

参加者が画面を共有しているMicrosoft Teams通話中に、制御を要求できます。制御を取得すると、共有画面に対して選択、編集、その他のキーボードおよびマウス操作を行うことができます。

画面が共有されているときに制御を取得するには、Microsoft Teams UIの**制御を要求**ボタンをクリックします。画面を共有している会議参加者は、要求を許可または拒否できます。

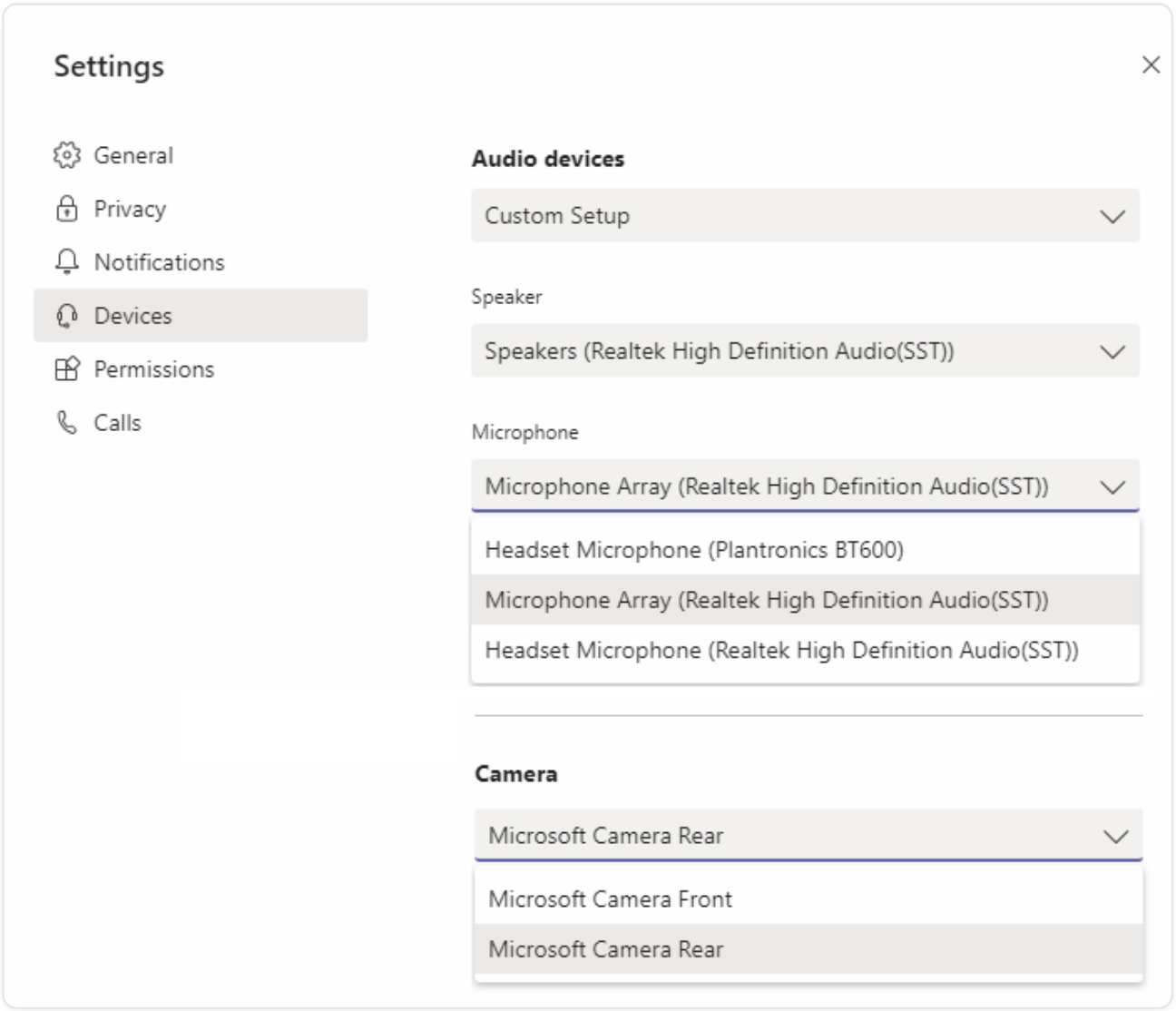
制御中は、共有画面に対して選択、編集、その他の変更を行うことができます。これらの操作には、キーボードとマウスの両方を使用できます。完了したら、**制御を要求**をクリックします。

制限事項:

- ユーザーが単一のアプリを共有している場合 (アプリ共有とも呼ばれます)、制御の付与と要求は利用できません。デスクトップ全体またはモニターを共有する必要があります。
- コントロールバーを特定の場所にピン留めする機能は利用できません。

Microsoft Teamsの周辺機器

Microsoft Teamsの最適化が有効な場合、Citrix Workspaceアプリは周辺機器 (ヘッドセット、マイク、カメラ、スピーカーなど) にアクセスします。その後、周辺機器はMicrosoft Teams UI (**設定 > デバイス**) に適切に表示されます。



Microsoft Teamsはデバイスに直接アクセスしません。代わりに、メディアの取得、キャプチャ、処理のためにWorkspaceアプリのWebRTCメディアエンジンに依存します。Microsoft Teamsは、ユーザーが選択できるようにデバイスを一覧表示します。

Microsoft Teamsがアクティブなときに挿入された周辺機器は、デフォルトでは選択されません。Microsoft Teams UIの **設定** > **デバイス** 画面から周辺機器を手動で選択する必要があります。周辺機器が選択されると、Microsoft Teamsはその周辺機器の情報をキャッシュします。その結果、同じエンドポイントからセッションに再接続すると、周辺機器が自動的に選択されます。

推奨事項:

- エコーキャンセレーション内蔵のMicrosoft Teams認定ヘッドセット。マイクとスピーカーが別々のデバイスにある追加の周辺機器を使用するセットアップでは、エコーが発生する可能性があります。例としては、マイク内蔵のWebカメラとスピーカー付きのモニターがあります。外部スピーカーを使用する場合は、マイクからできるだけ離して配置してください。また、音をマイクに屈折させる可能性のある表面から離して配置してください。詳細については、

`www.microsoft.com` にアクセスし、Microsoft Teams認定ヘッドセットを検索してください。

- Microsoft Teams認定カメラ。ただし、Skype for Business認定周辺機器はMicrosoft Teamsと互換性があります。詳細については、<www.microsoft.com> にアクセスし、Microsoft Teams認定カメラとSkype for Business認定周辺機器を検索してください。
- Citrix Workspaceアプリのメディアエンジンは、オンボードH.264エンコーディング (UVC 1.1および1.5) を実行するWebカメラではCPUオフロードを利用できません。

注:

Windows用Workspaceアプリ2009.6は、24ビットのオーディオ形式または96 kHzを超える周波数で周辺機器を取得できるようになりました。

HdxTeams.exe (Windows用Citrix Workspaceアプリ2009以前) は、これらの特定のオーディオデバイス形式 (チャネル、ビット深度、およびサンプルレート) のみをサポートしています。

- 再生デバイス: 最大2チャネル、16ビット、最大96,000 Hzの周波数
- 録音デバイス：最大4チャンネル、16ビット、最大96,000 Hzの周波数

スピーカーまたはマイクのいずれかが予期される設定と一致しない場合でも、Microsoft Teamsでのデバイス列挙は失敗し、**設定 > デバイス**の下に**なし**と表示されます。

HdxTeams.exeの**Webrpc**ログには、この種類の情報が表示されます。

`Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing...`.

`Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't create audio module!` !

回避策として、特定のデバイスを無効にするか、次のいずれかを実行します。

1. **サウンドコントロールパネル** (mmsys.cpl) を開きます。
2. 再生または録音デバイスを選択します。
3. **プロパティ > 詳細**に移動し、設定をサポートされているモードに変更します。

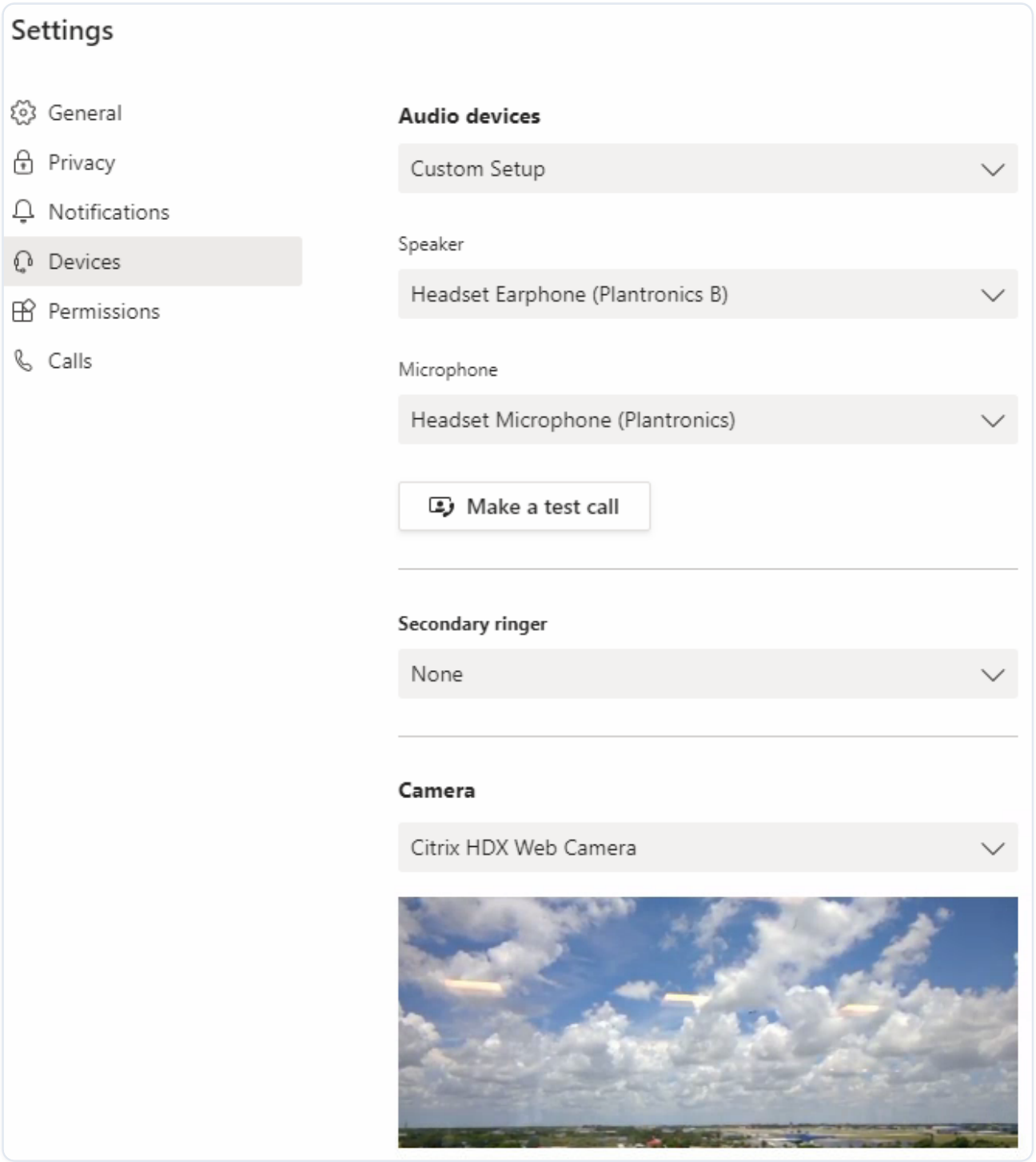
フォールバックモード

Microsoft Teamsが最適化されたVDIモード（Microsoft Teams/バージョン情報/バージョンで「Citrix HDX Not Connected」）でロードに失敗した場合、VDAはレガシーHDXテクノロジーにフォールバックします。レガシーHDXテクノロジーには、Webカメラリダイレクト、クライアントオーディオ、およびマイクリダイレクトが含まれる場合があります。Microsoft Teamsの最適化をサポートしないWorkspaceアプリのバージョン/プラットフォームOSを使用している場合、フォールバックレジストリキーは適用されません。 フォールバックモードでは、周辺機器はVDAにマッピングされます。周辺機器は、仮想デスクトップにローカルで接続されているかのようにMicrosoft Teamsアプリに表示されます。

VDA でレジストリキーを設定することで、フォールバックメカニズムをきめ細かく制御できるようになりました。詳細については、レジストリで管理される機能のリストにある Microsoft Teams フォールバックモード を参照してください。

この機能には、Microsoft Teamsバージョン1.3.0.13565以降が必要です。

Microsoft Teamsアプリの**設定 > デバイス**タブで、最適化モードか非最適化モードかを判断するには、カメラ名が主な違いとなります。Microsoft Teamsが非最適化モードでロードされると、レガシーHDXテクノロジーが起動します。Webカメラ名には、次の図に示すように**Citrix HDX**のサフィックスが付いています。スピーカーとマイクのデバイス名は、最適化モードと比較してわずかに異なる（または切り詰められている）場合があります。



従来のHDXテクノロジーを使用する場合、Microsoft Teamsはオーディオ、ビデオ、画面共有の処理をエンドポイントのCitrix WorkspaceアプリWebRTCメディアエンジンにオフロードしません。代わりに、HDXテクノロジーはサーバー側レンダリングを使用します。ビデオをオンにすると、VDAで高いCPU消費が予想されます。リアルタイムオーディオのパフォーマンスが最適ではない可能性があります。

既知の制限事項

Citrixの制限事項

Citrix Workspaceアプリの制限事項：

- HIDボタン - 通話の応答と終了はサポートされていません。音量アップとダウンはサポートされています。
- Microsoft Teamsの管理センターのQoS設定は、VDIユーザーには適用されません。
- ユーザーは、VDAでSnipping Toolを使用している間、Microsoft Teamsコンテンツのスクリーンショットを撮ることはできません。ただし、クライアント側でSnipping Toolが使用された場合、コンテンツをキャプチャできます。

VDAの制限事項：

- 「**Citrix Workspaceアプリの高DPI**」設定を`Yes`に構成すると、リダイレクトされたビデオウィンドウがずれて表示されます。この制限は、モニターのDPIスケーリング係数が100%を超えて設定されている場合に発生します。

Citrix Workspace アプリと VDA の制限事項:

- 最適化された通話の音量は、VDA上ではなく、クライアントマシンの音量バーを使用してのみ制御できます。

サイマルキャスト

Simulcastのサポートは、WindowsおよびMac上の最適化されたMicrosoft Teamsビデオ会議通話で有効になっています。Linuxについては、シンクライアントベンダーにお問い合わせください。Simulcastを使用すると、すべての発信者にとって最高の通話エクスペリエンスを実現するために適切な解像度に適合させることで、さまざまなエンドポイントでのビデオ会議通話の品質とエクスペリエンスが向上します。

この改善されたエクスペリエンスにより、各ユーザーは、エンドポイントの機能、ネットワークの状態など、いくつかの要因に応じて、異なる解像度（例：720p、360pなど）で複数のビデオストリームを配信する可能性があります。受信側エンドポイントは、処理できる最大品質の解像度を要求し、それにより、すべてのユーザーに最適なビデオエクスペリエンスを提供します。

> **注:**
>
> この機能は、Microsoft Teamsからのアップデートが展開された後にのみ利用可能です。ETAについては、`<https://www.microsoft.com/>`にアクセスし、Microsoft 365ロードマップ

を検索してください。Microsoftによってアップデートが展開されたら、ドキュメントの更新と発表についてはCTX253754 を確認してください。

Microsoftの制限事項

- 3x3ギャラリービューはサポートされていません。Microsoft Teamsの依存関係 – 3x3グリッドがいつ提供されるかについてはMicrosoftにお問い合わせください。
- Skype for Businessとの相互運用性は音声通話に限定されており、ビデオモダリティはありません。
- 送受信ビデオストリームの最大解像度は720pです。
- PSTN通話の呼び出し音はサポートされていません。
- ダイレクトルーティングのメディアバイパスはサポートされていません。
- ブロードキャストおよびライブイベントのプロデューサーおよびプレゼンターの役割はサポートされていません。出席者の役割はサポートされていますが、最適化されていません（代わりにVDAでレンダリングされます）。
- Microsoft Teamsのズームインおよびズームアウト機能はサポートされていません。
- ロケーションベースルーティングとメディアバイパスはサポートされていません。
- 通話のマージはサポートされていません（ユーザーインターフェイスにオプションが表示されません）。

CitrixとMicrosoftの制限事項

- 画面共有を行う際、**システムオーディオを含める**オプションは利用できません。
- SimulcastはChromeOSではサポートされていません。

今後のMicrosoft Teamsシングルウィンドウの EOL

January 31, 2024に、MicrosoftはVDI Microsoft Teams最適化を使用する際のシングルウィンドウUIに対するMicrosoft Teamsのサポートを終了し、マルチウィンドウエクスペリエンスのみをサポートします。Microsoftは9/8/2023にM365管理者センター（投稿ID: MC674419）でこの非推奨化について通知しました。 マルチウィンドウ機能に関する公開されている詳細は、Tech Communityの記事「New Meeting and Calling Experience in Microsoft Teams」で確認できます。

注:

Citrixは、ビデオおよび画面共有のために最適化されたモードでMicrosoft Teamsを引き続き使用するには、VDAとCitrix Workspaceアプリをサポートされているバージョンにアップグレードすることを推奨します。インフラストラクチャとエンドポイントをマルチウィンドウをサポートするようにアップグレードしない場合、通話、ビデオ通話、および画面共有は最適化されなくなります。これにより、通話品質の問題、レイテンシーの増加、およびサーバーへの負荷の増加が発生する可能性があります。

次の表は、Citrix VDIでMicrosoft Teamsの最適化された通話を引き続き使用するために必要なVDAおよびCitrix Workspaceアプリの最小バージョン、LTSRバージョン、および推奨バージョンを示しています。

コンポーネント	最小バージョン (1)	LTSRサポートバージョン (2)	推奨バージョン (3)
マイクロソフトTeams	1.5.00.11865	該当なし	最新
VDA	1912 CU6 LTSR, 2109 CR, 2203 LTSR	1912 CU8+, 2203 LTSR CU2+ (4)	2308 CR+
Windows向けCitrix Workspaceアプリ	2112.1 CR	2203 CU2+ (4)	2309 CR+
Mac向けCitrix Workspaceアプリ	2203 CR	該当なし	2308 CR+
Linux向けCitrix Workspaceアプリ	2202 CR	該当なし	2308 CR+
ChromeOSまたはHTML5向けCitrix Workspaceアプリ	2303 CR	該当なし	2309 CR+

注:

1. 最小バージョン: これは、マルチウィンドウが最初に導入されたバージョンです。ここに記載されている一部の最小バージョンは、サポート終了となっている場合があります。

2. LTSRサポートバージョン: これは、Citrixがマルチウィンドウ向けにサポートしているLTSRバージョンです。これらのLTSRリリースの古いバージョンは動作する可能性がありますが、新しいLTSR CUバージョンがリリースされると、それらのバージョンに対するサポートは利用できなくなります。LTSRサポートポリシーの詳細については、`<https://support.citrix.com/article/CTX205549/faq-citrix-virtual-apps-and-desktops-and-citrix-hypervisor-long-term-service-release-ltsr>`を参照してください。
3. 推奨バージョン: これは、ユーザー/顧客がソフトウェアのアップグレードを選択した場合にCitrixが推奨するソフトウェアのバージョンです。これらはすべてCRバージョンです。
4. VDAおよびCWAベースバージョンのバージョン2203 LTSRには、マルチウィンドウ機能が含まれています。これらのバージョンは、正式にサポートされている最新のCUに置き換えられています。お客様は、自己の判断でこれらのサポートされていないバージョンを引き続き使用できます。Citrixは、LTSRリリースをご利用のお客様に最新のCUへのアップグレードを推奨します。

WebRTCからのSDP形式（プランB）の非推奨のお知らせ

Citrixは、今後のリリースでWebRTCからの現在のSDP形式 (プランB) のサポートを非推奨にする予定です。最適化されたMicrosoft Teamsの機能に対応するには、WebRTCでUnified Planを使用する必要があります。

影響を受ける製品

Citrix Workspaceアプリケーションの今後のリリースでは、Citrix Workspaceアプリの次期リリースを搭載したエンドポイントと、Citrix Workspaceアプリ2108以前のバージョンを搭載したエンドポイント間の通話はサポートされません。この通話の非互換性には、1912 LTSR Citrix Workspaceアプリクライアント (CWA) が含まれます。影響を受けるCWAクライアントは次のとおりです。

- Windows向けCitrix Workspaceアプリ
- Linux向けCitrix Workspaceアプリ
- Mac向けCitrix Workspaceアプリ
- Chrome向けCitrix Workspaceアプリ

プランBの代替

Citrix Workspaceアプリのバージョン2109より古いものを使用している場合、サポートされているバージョン（できれば最新のCRリリース）にアップグレードする必要があります。そうしないと、将来のリリースまたは新しいエンドポイントとの通話は接続に失敗します。将来のリリースとフェデレーション通信パートナー間の通話も、フェデレーションパートナーがCitrix Workspaceをアップグレードしていない場合、完了に失敗する可能性があります。

Citrix Workspaceアプリバージョン2108は、2023年3月にサポート期限が終了しており、より新しいバージョンにアップグレードする必要があります。詳細については、Citrix Workspaceアプリのバージョンサポートに関するWorkspace Appを参照してください。

Plan Bの非推奨に関する詳細については、WebRTCのドキュメントを参照してください。

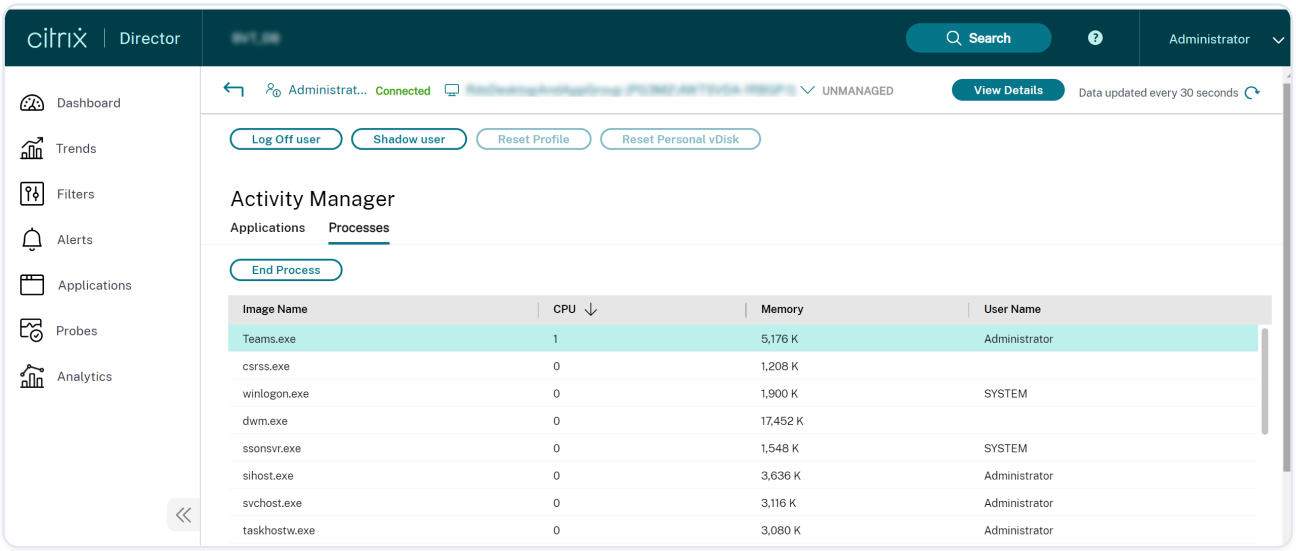
追加情報

- Microsoft Teams の監視、トラブルシューティング、サポート
- VM への Microsoft Teams デスクトップアプリの展開
- MSI を使用した Microsoft Teams のインストール (VDI インストールセクション)
- シンクライアント
- Skype for Business ネットワーク評価ツール
- Microsoft Teams と Skype for Business の共存と相互運用性を理解する

Microsoft Teamsの監視、トラブルシューティング、サポート

Teamsの監視

このセクションでは、HDX を使用した Microsoft Teams の最適化を監視するためのガイドラインを示します。 最適化モードで実行しており、`HdxRtcEngine.exe` がクライアントマシンで実行されている場合、VDA 上で `WebSocketAgent.exe` というプロセスがセッションで実行されます。アプリケーションを表示するには、Director の **Activity Manager** を使用します。



Microsoft Teams の最適化ステータスは、Director の **User Details** ページ > **Session Details** パネル > **MS Teams Optimization** フィールドで確認できます。Microsoft Teams が最適化されていることは、クリアなオーディオとビデオなど、より良いユーザーエクスペリエンスのために不可欠です。この機能は VDA バージョン 2311 以降で利用可能です。サポートされている Citrix Workspace™ app のバージョンは、「Optimization for Microsoft Teams」に記載されています。Director は、Microsoft Teams が公開アプリケーションまたは公開デスクトップ内で実行されている場合にのみ、Microsoft Teams の最適化ステータスを表示します。 詳細については、「Microsoft Teams optimization status」を参照してください。

VDA の最小バージョン 1912 以降では、Citrix HDX Monitor (最小バージョン 3.11) を使用してアクティブな Teams 通話を監視できます。Citrix Virtual Apps and Desktops 製品 ISO には、フォルダー `layout\image-full\Support\HDX Monitor` に最新の `hdxmonitor.msi` が含まれています。 VDA の最小バージョン 1912 以降では、Citrix HDX Monitor (最小バージョン 3.11) を使用してアクティブな Microsoft Teams 通話を監視できます。Citrix Virtual Apps and Desktops 製品 ISO には、フォルダー `layout\image-full\Support\HDX Monitor` に最新の `hdxmonitor.msi` が含まれています。

詳細については、Knowledge Center の記事 CTX253754 の「*Monitoring*」を参照してください。

トラブルシューティング

このセクションでは、Microsoft Teams の最適化を使用する際に発生する可能性のある問題のトラブルシューティングのヒントを提供します。詳細については、CTX253754 を参照してください。

バーチャル デリバリー エージェント上で

BCR_x64.msi によって4つのサービスがインストールされます。そのうち2つだけが、VDA での Microsoft Teams リダイレクトを担当します。

ブラウザコンテンツリダイレクトによってインストールされる4つのサービス (/en-us/citrix-virtual-apps-desktops/2411/media/team-services.png)

- **Citrix HDX Teams Redirection Service**は、Microsoft Teamsで使用される仮想チャネルを確立します。このサービスはCtxSvcHost.exeに依存しています。
- **Citrix HDX HTML5 Video Redirection Service** は、127.0.0.1:9002 TCP でリッスンする WebSocketService.exe として実行されます。WebSocketService.exe は主に2つの機能を実行します。

  i. **セキュアな WebSocket のための TLS 終端** は、Microsoft Teams アプリ内のコンポーネントである vdiCitrixPeerConnection.js からセキュアな WebSocket 接続を受信します。Process Monitor でこれを追跡できます。証明書の詳細については、セクション (TLS および HTML5 ビデオリダイレクト、ブラウザコンテンツリダイレクト) を参照してください。

  一部のアンチウイルスソフトウェアやデスクトップセキュリティソフトウェアは、`WebSocketService.exe`とその証明書の適切な機能を妨げます。Citrix HDX HTML5ビデオリダイレクトサービスが`services.msc`コンソールで実行されている場合でも、netstatで確認できるように、localhost `127.0.0.1:9002` TCPソケットはリスニングモードになっていません。サービスを再起動しようとするとハングします（「停止中...」）。
  `WebSocketService.exe`プロセスに適切な除外を適用していることを確認してください。

  「プロセスモニター」(/en-us/citrix-virtual-apps-desktops/2411/media/team-process-monitor.png)

  ii. **ユーザーセッションマッピング。** Microsoft Teamsアプリケーションが起動すると、WebSocketService.exeはVDAのユーザーセッションでWebSocketAgent.exeプロセスを開始します。WebSocketService.exeはLocalSystemアカウントとしてセッション0で実行されます。

  「WebSocketAgent.exeサービス」(/en-us/citrix-virtual-apps-desktops/2411/media/websocketservice-websocketagent.png)

  `netstat`を使用して、WebSocketService.exeサービスがVDAでアクティブなリスニング状態にあるかどうかを確認できます。

  管理者として実行しているコマンドプロンプトウィンドウから`netstat -anob -p tcp`を実行します。

```
 TCP    127.0.0.1:9001         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
 TCP    127.0.0.1:9002         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
```

  接続が成功すると、状態はESTABLISHEDに変わります。

「netstatの成功例」(/en-us/citrix-virtual-apps-desktops/2411/media/teams-netstat-success.png)

重要:

WebSocketService.exeは、127.0.0.1:9001と127.0.0.1:9002の2つのTCPソケットでリッスンします。ポート9001はブラウザコンテンツリダイレクトとHTML5ビデオのリダイレクトに使用されます。ポート9002はMicrosoft Teamsのリダイレクトに使用されます。Teams.exeとWebSocketService.exe間の直接通信を妨げる可能性のあるプロキシ構成がVDAのWindows OSにないことを確認してください。Internet Explorer 11で明示的なプロキシを構成すると（**インターネットオプション > 接続 > LANの設定 > プロキシサーバー**）、接続が割り当てられたプロキシサーバーを経由する場合があります。手動および明示的なプロキシ設定を使用する場合は、**ローカルアドレスにはプロキシサーバーを使用しない**がチェックされていることを確認してください。

サービスの位置と説明

サービス	WINDOWS SERVER OSの実行可能ファイルへのパス	ログオンアカウント	説明
Citrix HTML5ビデオリダイレクトサービス	"C:\Program Files (x86)\Citrix\System32\WebSocketService.exe" /service	ローカルシステムアカウント	仮想デスクトップとエンドポイントデバイス間でメディアリダイレクトを実行するために必要な初期フレームワークを、複数のHDXマルチメディアサービスに提供します。
Citrix HDX ブラウザリダイレクトサービス	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g BrowserRedirSvcs	このアカウント (ローカルサービス)	エンドポイントデバイスと仮想デスクトップ間でブラウザコンテンツリダイレクトを提供します。
Citrix ポートフォワーディングサービス	"C:\Program Files (x86)\Citrix\System3	このアカウント (ローカルサービス)	ブラウザコンテンツリダイレクトのために、エンドポイントデバイスと仮想デス

サービス	WINDOWS SERVER OSの実行可能ファイルへのパス	ログオンアカウント	説明
	2\CtxSvcHost.exe" -g PortFwdSvcs		クトップ間でポート転送を提供します。
Citrix HDX Teams リダイレクトサービス	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g TeamsSvcs	ローカルシステムアカウント	エンドポイントデバイスと仮想デスクトップ間でMicrosoft Teamsのリダイレクトを提供します。

シトリックス ワークスペース アプリ

ユーザーのエンドポイントでは、Windows版Citrix WorkspaceアプリがHdxTeams.exeまたはHdxRtcEngine.exeという新しいサービスをインスタンス化します。これは、VDAでMicrosoft Teamsが起動し、ユーザーがセルフプレビューで通話しようとしたり、周辺機器にアクセスしようとしたりするときに行われます。このサービスが表示されない場合は、以下を確認してください。

1. Windows 用 Workspace アプリ バージョン 1905 以降がインストールされていることを確認します。Workspace アプリのインストールパスに HdxTeams.exe または HdxRtcEngine.exe と webrpc.dll バイナリが表示されますか？
2. 手順1を確認したら、HdxTeams.exe または HdxRtcEngine.exe が起動しているかどうかを確認するために、次の操作を行います。
    a. VDA 上の Microsoft Teams を終了します。
    b. VDA で services.msc を起動します。
    c. Citrix HDX Teams Redirection Service を停止します。
    d. ICA® セッションを切断します。
    e. ICA セッションを接続します。
    f. Citrix HDX Teams Redirection Service を開始します。
    g. Citrix HDX HTML5 Video Redirection Service を再起動します。
    h. VDA 上で Microsoft Teams を起動します。
3. クライアントエンドポイントで HdxTeams.exe または HdxRtcEngine.exe が起動しない場合は、次の操作を行います。
    a. VDA を再起動します。

b. クライアントエンドポイントを再起動します。

サポート

CitrixとMicrosoftは、Microsoft Teamsの最適化を使用して、Citrix Virtual Apps and Desktops™からのMicrosoft Teamsの提供を共同でサポートしています。この共同サポートは、両社間の緊密な連携の結果です。有効なサポート契約があり、このソリューションで問題が発生した場合は、問題の原因となっていると思われるコードのベンダーにサポートチケットをオープンしてください。つまり、TeamsについてはMicrosoft、最適化コンポーネントについてはCitrixです。 CitrixまたはMicrosoftがチケットを受け取り、問題をトリアージし、必要に応じてエスカレートします。各社のサポートチームに連絡する必要はありません。

問題が発生した場合は、Teams UI で **>** をクリックすることをお勧めします。VDA 側のログは、技術的な問題をより迅速に解決するために、Citrix と Microsoft の間で自動的に共有されます。

ログの収集

HDXメディアエンジンログは、ユーザーのマシン（VDA上ではない）で見つけることができます。問題が発生した場合は、必ずサポートケースにログを添付してください。

Windowsログ：

Windowsログは、**HDXTeams**フォルダー内の%TEMP%にあります（AppData/Local/Temp/HDXTeamsまたはAppData/Local/Temp/HdxRtcEngine）。webrpc_Day_Month_timestamp_Year.txtという名前の.txtファイルを探してください。Citrix Workspaceアプリの新しいバージョン（Citrix Workspaceアプリ2009.5以降など）を使用している場合は、ログをAppData\Local\Temp\HdxRtcEngineに保存します。

各セッションはログ用の個別のフォルダーを作成します。

Macログ：

1. VDWEBRTCログ - 仮想チャネルの実行を記録します。

   場所：`/Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt`

2. HdxRtcEngineログ - HdxRtcEngine上のプロセスの実行を記録します。

   場所: `$TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log`

   HdxRtcEngineログはデフォルトで有効になっています。

3. Webrpcログ - webrtcライブラリのラップアップの実行を記録する最も重要なログです。

場所: `/Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log`

Linuxログ：

Linuxログは`/tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/`フォルダーにあります。 Webrtcログ：`/tmp/webrpc/<current date>/webrtc.log` カーネルログ：`/var/log/syslog`

ICE/STUN/TURN/ログ：

通話の確立時には、次の4つの ICE フェーズが必要です。

- 候補の収集
- 候補の交換
- 接続性チェック (STUN バインド要求)
- 候補の昇格

HdxRtcEngine.exe ログには、関連する Interactive Connectivity Establishment (ICE) エントリが含まれています。これらのエントリは、通話設定が成功するために必要です。収集段階のサンプルスニペットを次に示します。

```
RPCStubs Info: -> device id = \\?
\display#int3470#4&1835d135&0&uid13424#{65e8773d-8f56-11d0-
a3b9-00a0c9223196}\{bf89b5a5-61f7-4127-a279-e187013d7caf} label =
Microsoft Camera Front groupId =



webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1

webrtcapi.RTCPeerConnection Info: setLocalDescription.

>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveLocalOffer
```

```
webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Gathering



[…]

>>> begin:sdp

candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
generation 0 ufrag oVk6 network-id 1

<<< end:sdp

[…]

>>> begin:sdp

candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay raddr
73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1 network-cost
10

<<< end:sdp

[…]

>>> begin:sdp

candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx raddr
10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id 1

<<< end:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Complete
webrtcapi.RTCPeerConnection Info: setRemoteDescription.

>>> begin:sdp

[…]
```

```
webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveRemotelOffer
```

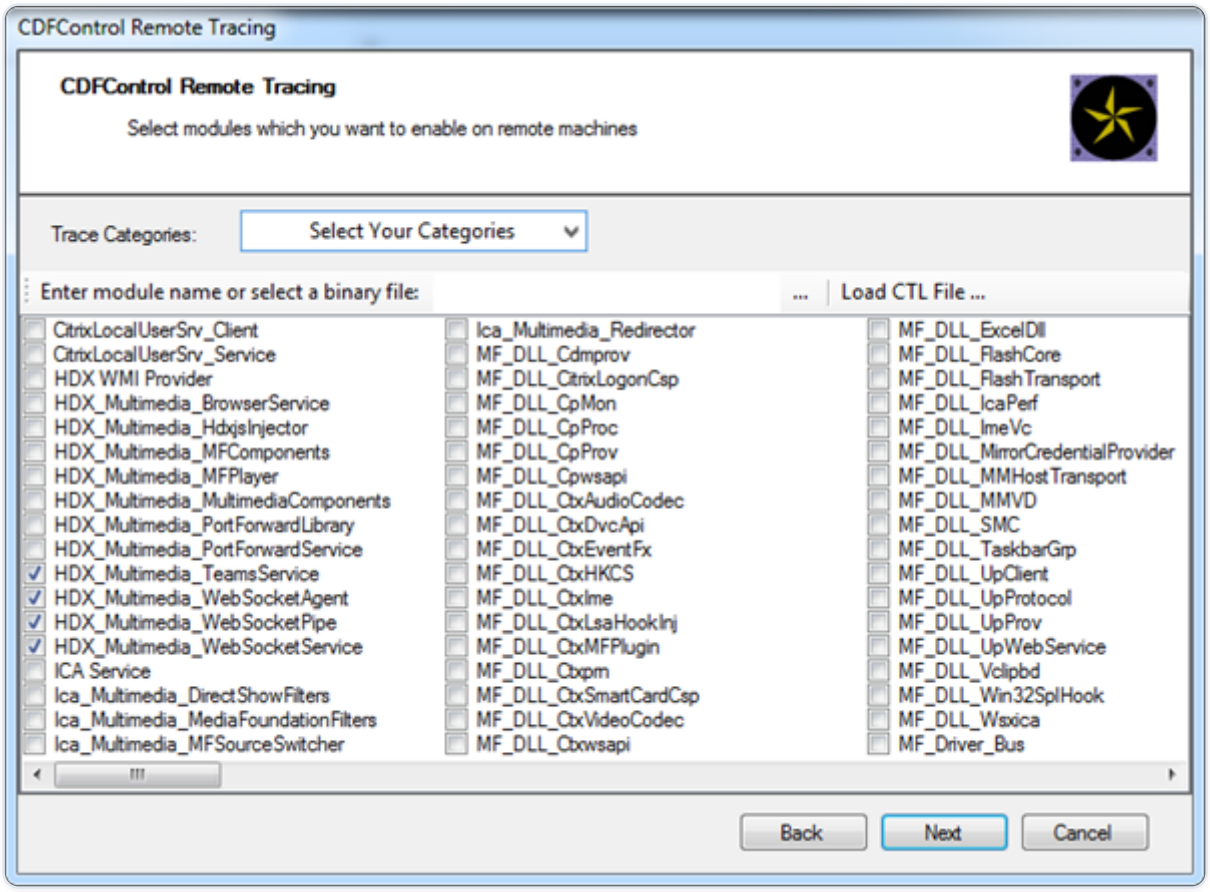
複数の ICE 候補がある場合、優先順位は次のとおりです。

1. ホスト
2. ピア反射型
3. サーバー反射型
4. トランスポートリレー

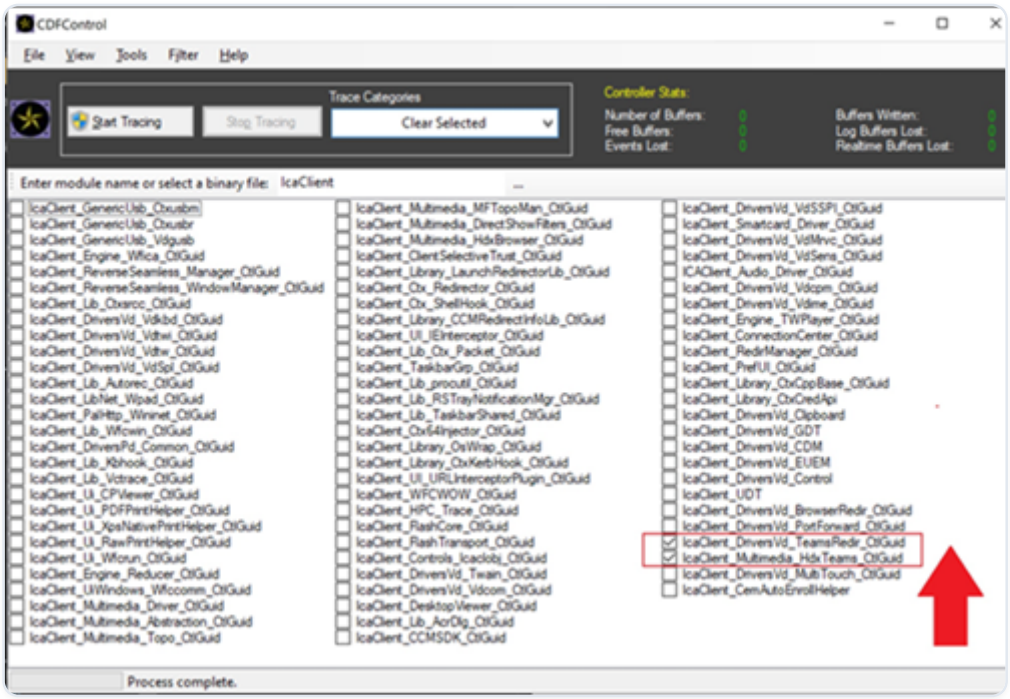
問題が発生し、それを一貫して再現できる場合は、Microsoft Teams で **ヘルプ > 問題の報告** をクリックすることをお勧めします。Microsoft にケースを登録した場合、技術的な問題を解決するためにログが Citrix と Microsoft の間で共有されます。 Citrix Support に問い合わせる前に CDF トレースをキャプチャすることも役立ちます。詳細については、Knowledge Center の記事 CDFcontrol を参照してください。

CDF トレースを収集するための推奨事項については、Knowledge Center の記事 Recommendations for Collecting the CDF Traces を参照してください。

VDA側のCDFトレース - 次のCDFトレースプロバイダーを有効にします。



Workspaceアプリ側のCDFトレース - 次のCDFトレースプロバイダーを有効にします。



- IcaClient_DriversVd_TeamsRedir (オプション)
- IcaClient_Multimedia_HdxTeams (Citrix Workspaceアプリ2012以降が必要)

Windows Media リダイレクト

Windows Media リダイレクトは、サーバーがストリーミングオーディオとビデオをユーザーに配信する方法を制御し、最適化します。メディアのランタイムファイルをサーバーではなくクライアントデバイスで再生することで、Windows Media リダイレクトは、マルチメディアファイルの再生に必要な帯域幅を削減します。Windows Media リダイレクトは、仮想Windowsデスクトップで実行されているWindows Media Playerおよび互換性のあるプレーヤーのパフォーマンスを向上させます。

Windows Media のクライアント側コンテンツフェッチの要件が満たされない場合、メディア配信は自動的にサーバー側フェッチを使用します。この方法はユーザーには透過的です。Citrix Scout を使用して、HostMMTransport.dll から Citrix Diagnosis Facility (CDF) トレースを実行し、使用されている方法を特定できます。詳細については、Citrix Scout を参照してください。

Windows Media リダイレクトは、ホストサーバーでメディアパイプラインを傍受し、メディアデータをネイティブの圧縮形式でキャプチャし、コンテンツをクライアントデバイスにリダイレクトします。その後、クライアントデバイスはメディアパイプラインを再構築して、ホストサーバーから受信したメディアデータを解凍およびレンダリングします。Windows Media リダイレクトは、Windows オペレーティングシステムを実行しているクライアントデバイスでうまく機能します。これらのデバイスには、ホストサーバーに存在していたメディアパイプラインを再構築するために必要なマルチメディアフレームワークがあります。Linux クライアントは、同様のオープンソースメディアフレームワークを使用してメディアパイプラインを再構築します。

ポリシー設定の**Windows Media Redirection**は、この機能を制御し、デフォルトで**Allowed**になっています。通常、この設定により、サーバーからレンダリングされるオーディオおよびビデオの品質が、クライアントデバイスでローカルに再生されるコンテンツに匹敵するレベルに向上します。まれに、Windows Media リダイレクトを使用して再生されるメディアが、基本的なICA®圧縮と通常のオーディオを使用してレンダリングされるメディアよりも悪く見えることがあります。この機能を無効にするには、ポリシーに**Windows Media Redirection**設定を追加し、その値を**Prohibited**に設定します。

ポリシー設定について詳しくは、「マルチメディアポリシー設定」(/ja-jp/citrix-virtual-apps-desktops/2411/policies/reference/ica-policy-settings/multimedia-policy-settings.html)を参照してください。

制限事項:

セッション内でWindows Media PlayerとRemote Audio & Video Extensions (RAVE) を有効にしている場合、黒い画面が表示されることがあります。この黒い画面は、ビデオコンテンツを右クリックして**常に手前に表示**を選択した場合に表示されることがあります。

仮想チャネルプラグインマネージャー

はじめに

仮想チャネルプラグインマネージャーは、特定のアプリケーション向けにクライアントエンドポイント全体にプラグインを展開するように設計されています。プラグインマネージャーは、VDA上で実行されている特定のアプリケーションを検出し、アプリケーション実行時に最適なエクスペリエンスを実現するために、エンドポイントにプラグインをインストールするようユーザーに促します。

ユーザーはプラグインのインストールを選択、スキップ、または拒否できます。プラグインマネージャーは、管理対象か非管理対象かを問わず、すべてのエンドポイントでプラグインを管理する柔軟性を提供します。

例: Microsoft Teams は新しいアーキテクチャ (SlimCore Optimization) を採用しており、最適化を機能させるにはエンドポイントにプラグインをインストールする必要があります。仮想チャネルプラグインマネージャーは、エンドポイント全体にプラグインを展開できます。詳細については、Teams 向け新しい VDI ソリューション を参照してください。

システム要件

仮想チャネルプラグインマネージャーの最小要件は以下のとおりです。

- 仮想デスクトップエージェント (VDA)
  - 2411 CR
- DDC
  - Cloud 121 リリース
  - 2407 CR
- Citrix Workspace™ アプリ (Citrix Workspace アプリ)
  - Citrix Workspace アプリ Windows 2409 用

> **注:**
>
> この機能は現在、Windowsエンドポイントに適用されます。

サポートされるアプリケーション

- 現在サポートされているアプリケーションは以下のとおりです：
    - Microsoft Teams - Teams の新しい VDI ソリューション を参照してください

仮想チャネルプラグインマネージャーの概要

機能の理解

Citrix® は、お客様の環境が複雑になる可能性があり、管理対象および非管理対象のエンドポイントにプラグインを展開するにはかなりの労力が必要であることを理解しています。この機能は、そのプロセスを簡素化するように設計されています。

この機能には2つのコンポーネントが含まれています。1つはVDA側（検出プロセス）にあり、もう1つはCitrix Workspace™ App側（インストーラープロセス）にあります。管理者が、ポリシーの有効化、レジストリエントリの作成、監視するアプリケーションの指定など、上記の前提条件を満たすと、次のようになります。

- VDA側の検出プロセスは、エンドユーザーが仮想デスクトップにログオンすると、アプリケーションの起動を監視します
- 検出プロセスはCitrix Workspace App側に通知し、指定されたアプリケーションを最適化するために必要なプラグインをインストールするようユーザーに促します
- ユーザーは、プラグインに関する簡単な詳細情報が表示されたポップアップを画面に受け取ります。ユーザーは、プラグインをインストールするか、スキップするか、またはインストールしないことを選択できます
    - ユーザーがインストールプロセスをスキップした場合、そのセッションではポップアップが再度表示されることはありません。インストールプロンプトはセッションの再接続時に表示されます。
    - ユーザーがプラグインをインストールしないことを選択した場合、その選択はユーザープロファイルに記録され、管理者が確認できるようになります。
- ユーザーがプラグインのインストールを選択した場合、Citrix Workspace App側がエンドポイントにプラグインをダウンロードしてインストールします。
    - インストールが成功すると、プラグインを有効にするためにセッションを再接続するよう促すメッセージがユーザーに表示されます。ユーザーはすぐに再接続するか、成功メッセージを閉じて後で再接続するかを選択できます。
    - インストールが失敗した場合、ユーザーにはエラーメッセージが表示され、失敗は管理者が確認できるように記録されます。

仮想チャネルプラグインマネージャーの構成

展開

1. Microsoft Teamsリダイレクトポリシーが有効になっているか確認します。詳細については、Microsoft Teams redirection policyを参照してください。

   このポリシーは、監視対象のアプリケーションに関わらず有効にする必要があります。将来的に、より多くのアプリケーションがサポートされ、Microsoft Teamsの代わりにそれらのアプリケーションを監視したい場合でも、このポリシーは有効にしておく必要があります。このポリシーはデフォルトで有効になっています。

2. 仮想チャネルプラグインマネージャーポリシーを有効にする必要があります。ポリシーを有効にする方法の詳細については、Virtual channel plugin manager policy settingsを参照してください。

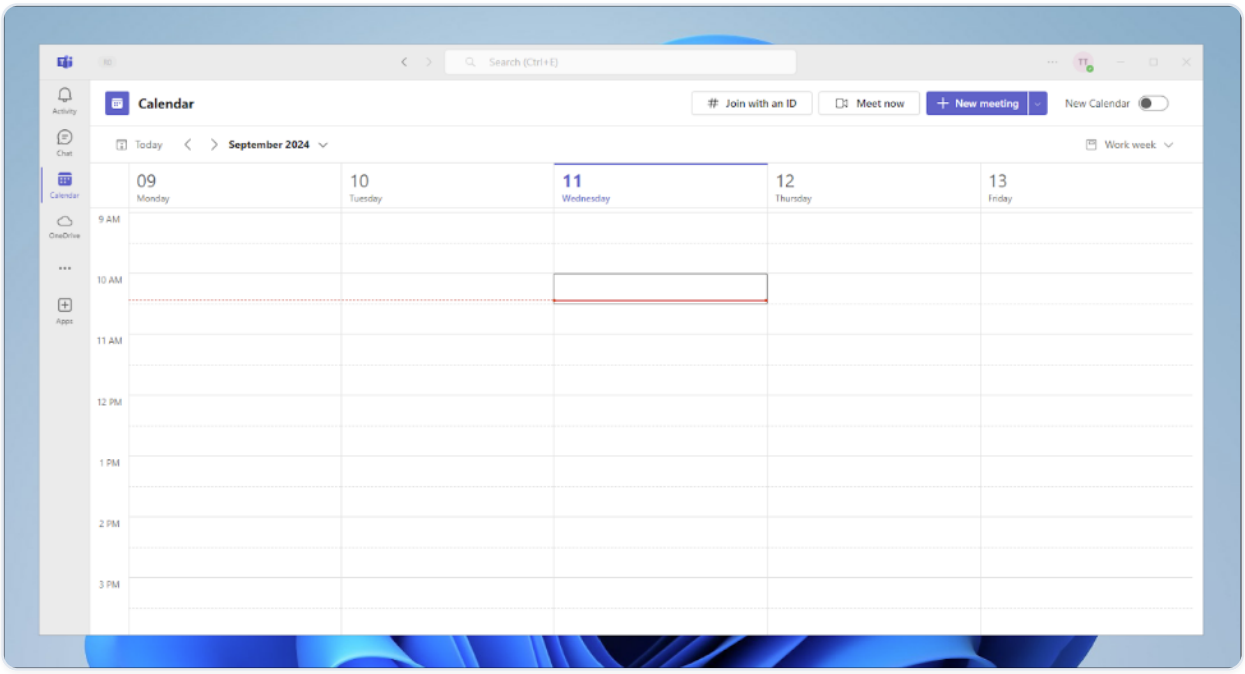
   このポリシーは、Citrix Studioのマルチメディアポリシー設定で利用できます。このポリシーを有効にすると、監視するアプリケーション名（例: 「Microsoft Teams」）を指定できます。このポリシーはデフォルトで無効になっています。

3. Citrix Workspace™アプリは、システムワイドモードでインストールする必要があります。

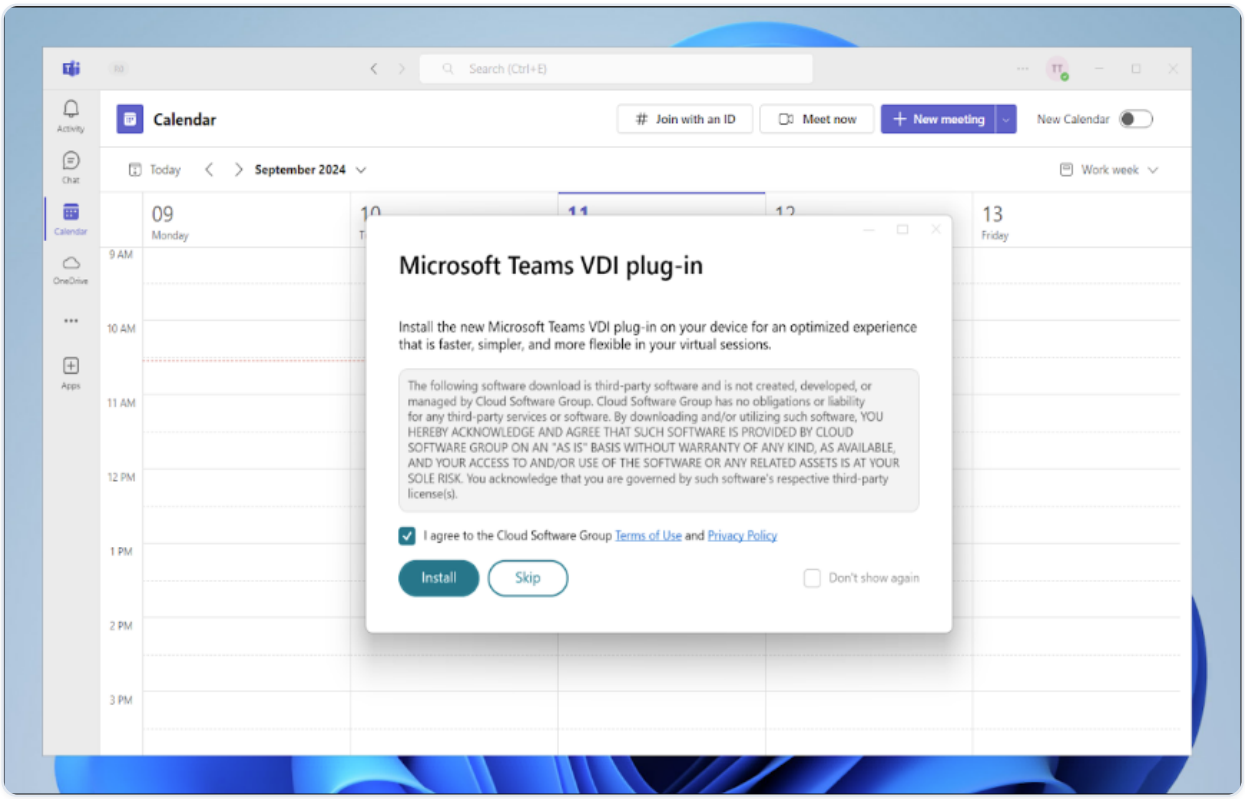
> **注:**
>
> プラグインは、サードパーティのCDNからエンドポイントにダウンロードされます。たとえば、Microsoft Teamsを選択した場合、プラグインはMicrosoft CDNからダウンロードされます。したがって、エンドポイントはサードパーティのCDNにアクセスできる必要があります。そうでない場合、プラグインのインストールは失敗します。

手順

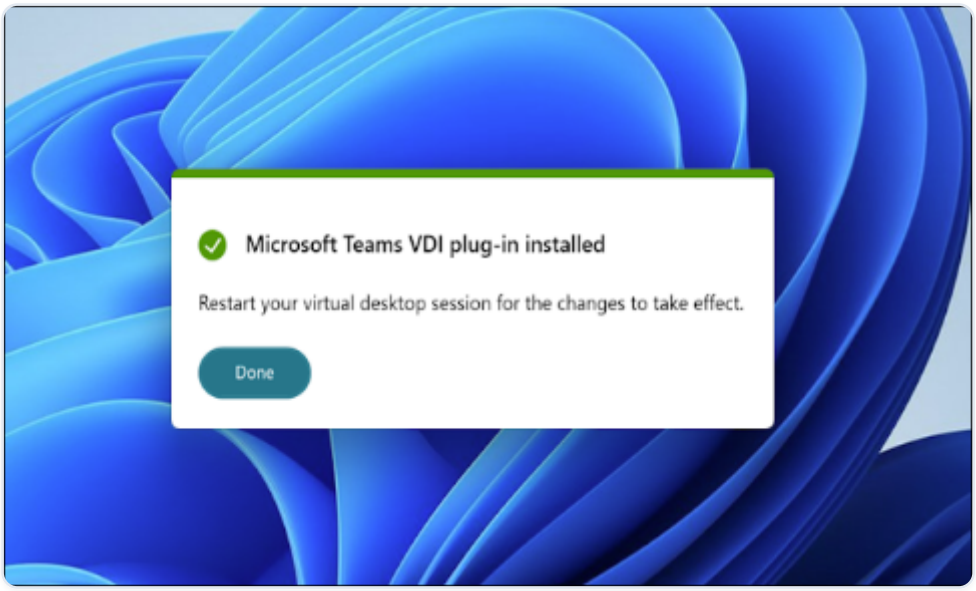
1. ユーザーはCitrixセッションでアプリケーションを起動します。例: Microsoft Teams。



2. ユーザーは、より良いエクスペリエンスのために、エンドポイントにTeams VDIプラグインをインストールするためのポップアップを受け取ります。プラグインはエンドポイントにインストールされるため、ポップアップはセッション内ではなく、セッションの上に表示されます。



3. ユーザーがインストールボタンをクリックすると、プラグインがインストールされます。変更を有効にするには、仮想デスクトップセッションを再起動する必要があります。



既知の問題と制限事項

- 2407 VDAでは、機能を有効にするために、ポリシーに加えてVDAで以下のレジストリ設定を1に設定する必要があります。このレジストリ設定は、2411 VDA以降では自動的に許可され、構成する必要はありません。

  `HKLM\SOFTWARE\Citrix\HDXMediaStream

  Name: EnableAppDetector Type: DWORD`
- その他の制限事項は追って追加されます

一般的なコンテンツリダイレクト

クライアントフォルダーリダイレクト

クライアントフォルダーリダイレクトは、ホスト側セッションでクライアント側ファイルにアクセスする方法を変更します。サーバーでクライアントドライブマッピングのみを有効にすると、クライアント側の完全なボリュームは、Universal Naming Convention (UNC) リンクとしてセッションに自動的にマッピングされます。サーバーでクライアントフォルダーリダイレクトを有効にし、ユーザーがユーザーデバイスでそれを構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

ユーザーが指定したフォルダーのみが、セッション内でUNCリンクとして表示されます。つまり、ユーザーデバイス上の完全なファイルシステムではなく、ユーザーが指定したフォルダーのみが表示されます。レジストリを介してUNCリンクを無効にすると、クライアントフォルダーはセッション内でマップされたドライブとして表示されます。

クライアントフォルダーリダイレクトは、WindowsシングルセッションOSマシンでのみサポートされています。

外部USBドライブのクライアントフォルダーリダイレクトは、デバイスの取り外しと再接続時に保存されません。

サーバーでクライアントフォルダーリダイレクトを有効にします。次に、クライアントデバイスで、リダイレクトするフォルダーを指定します。クライアントフォルダーオプションを指定するために使用するアプリケーション (CtxCFRUI.exe) は、このリリースに付属のCitrix Workspaceアプリに含まれています。

要件:

サーバーの場合:

- ウィンドウズ サーバー 2022
- Windows Server 2019、スタンダードおよびデータセンターエディション

クライアントの場合:

- ウィンドウズ 10

- ウィンドウズ 11

サーバーでクライアントフォルダーリダイレクトを有効にするには、レジストリを介して管理される機能のリストにあるクライアントフォルダーリダイレクトを参照してください。

ユーザーデバイスで、リダイレクトするフォルダーを指定します:

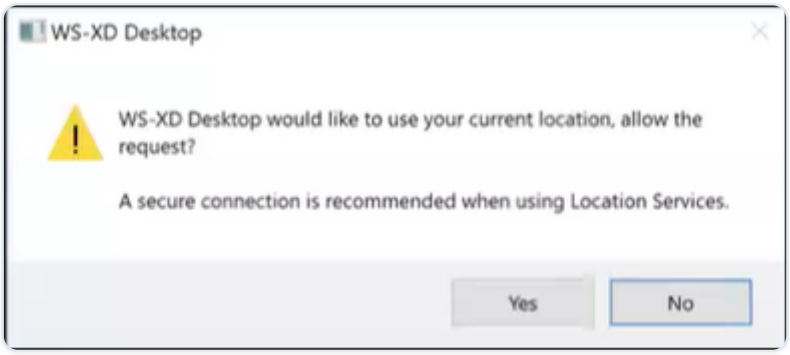
1. Citrix Workspace™アプリの最新バージョンがインストールされていることを確認してください。
2. Citrix Workspaceアプリのインストールディレクトリから、CtxCFRUI.exe **(..\Citrix\ICA Client\CtxCFRUI.exe)** を起動します。
3. **Custom** ラジオボタンを選択し、フォルダーを追加、編集、または削除します。
4. 設定を有効にするには、セッションを切断して再接続します。

クライアント位置情報リダイレクト

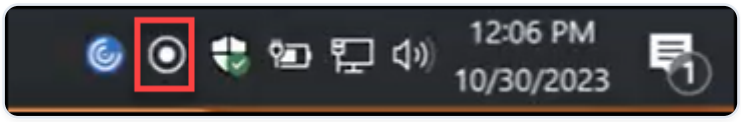
クライアント位置情報リダイレクトを有効にすると、VDAでホストされているアプリとデスクトップセッションがクライアントの現在地へシームレスにアクセスできるようになります。マルチセッションオペレーティングシステム（TS VDAまたはマルチセッションWS VDA）では、各セッションは接続されたクライアントによって提供される独自の場所を持ちます。この機能を使用すると、位置情報に依存するVDA上のアプリケーションは、クライアントの正確な位置情報を取得できます。

詳細については、Microsoftのドキュメントを参照してください。

クライアント位置情報リダイレクトが有効になり、サーバー側とクライアント側の両方で位置情報へのアクセスが許可されると、位置情報にアクセスするアプリケーションまたはデスクトップを起動したときに、クライアントは次のダイアログボックスで現在地を共有するように求めます。



クライアント位置情報リダイレクトを有効にすると、VDAでホストされているアプリまたはデスクトップが現在地情報を照会したときに、クライアントのタスクバーに次のアイコンが表示されます。



システム要件

サーバーの場合：

- シングルセッション (Win10/11) またはマルチセッション (Win 11 22H2 および Server 2022 23H2 以降) OS VDA
- Citrix Workspace™ アプリ for Windows、iOS、または Android

構成

この機能が動作するには、Citrix®ポリシーを使用してクライアント位置情報リダイレクトを有効にする必要があります。クライアント位置情報リダイレクトはデフォルトで無効になっています。

クライアント位置情報リダイレクトを有効にするには、次の手順を実行します。

Windows VDAおよびクライアント側で：

1. **設定 > プライバシー > 位置情報**で、次のオプションを有効にします。
    - **このデバイスの位置情報へのアクセスを許可する**
    - **アプリが位置情報にアクセスすることを許可する**
    - **デスクトップアプリが位置情報にアクセスすることを許可する**
2. マルチセッションOSの場合、「**位置情報のオーバーライド**」設定を有効にします。

コントローラー/DDC側で：

Studio > ポリシー > 位置情報 > 設定 > アプリケーションがクライアントデバイスの物理的な位置情報を使用することを許可するポリシーを有効にします。 詳細については、クライアントセンサーポリシー設定を参照してください。

双方向コンテンツリダイレクト

双方向コンテンツリダイレクトにより、Webブラウザ内、またはアプリケーションに埋め込まれたHTTPまたはHTTPS URLを、Citrix VDAセッションとクライアントエンドポイント間で双方向に転送できます。Citrixセッションで実行されているブラウザに入力されたURLは、クライアントのデフォルトブラウザを使用して開くことができます。逆に、クライアントで実行されているブラウザに入力されたURLは、公開アプリケーションまたはデスクトップを使用してCitrixセッションで

開くことができます。双方向コンテンツリダイレクトの一般的なユースケースには、次のものがあります。

- 開始ブラウザがソースへのネットワークアクセスを持たない場合のWeb URLのリダイレクト。
- ブラウザの互換性とセキュリティ上の理由によるWeb URLのリダイレクト。
- CitrixセッションまたはクライアントでWebブラウザを実行したくない場合に、アプリケーションに埋め込まれたWeb URLのリダイレクト。

システム要件

- シングルセッションまたはマルチセッションOS VDA
- Citrix Workspace™ アプリ for Windows 2311 以降
- Citrix Workspace™ アプリ for Linux 2503 以降
- Citrix Workspace™ アプリ for Mac 2607 以降

ブラウザー：

- Citrix ブラウザリダイレクション拡張機能を搭載した Google Chrome
  - Google Chrome拡張機能
- Citrix ブラウザリダイレクション拡張機能を搭載した Microsoft Edge
  - Microsoft Edge拡張機能

構成

Citrix Virtual Apps and Desktops™ バージョン 2311 以降、双方向コンテンツリダイレクトはCitrix Studioのみで構成されます。以前のリリースでは、クライアントエンドポイントとStudioの両方でポリシー設定が構成されていました。双方向コンテンツリダイレクトはデフォルトで無効になっています。

VDAの構成については、**ICAポリシー**設定の「双方向コンテンツリダイレクト」(/ja-jp/citrix-virtual-apps-desktops/2411/policies/reference/ica-policy-settings/bidirectional-content-redirection.html) を参照してください。

ブラウザリダイレクトを機能させるには、表示されているコマンドを使用して、ブラウザ拡張機能を元のブラウザ（URLがリダイレクトされる元となるブラウザ）に登録する必要があります。使用しているブラウザに基づいて、必要に応じてVDAとクライアントでコマンドを実行してください。

ブラウザ	VDA	クライアント
グーグル クローム	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regChrome	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regChrome
マイクロソフト エッジ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regEdge	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regEdge
すべての利用可能なブラウザ	コマンド: "%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regall	コマンド: "%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regall

ブラウザ拡張機能を登録解除するには：

ブラウザ	VDA	クライアント
グーグル クローム	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregChrome	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregChrome
マイクロソフト エッジ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregEdge	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregEdge
利用可能なすべてのブラウザ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregall	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregall

注:

- これらのコマンドを管理者権限でコマンドプロンプト (CMD) ウィンドウで実行します。

- registerコマンドを実行すると、ChromeおよびEdgeブラウザーは、初回起動時にCitrix Browser Redirection Extensionを有効にするようユーザーに促します。
- registrationコマンドは、Browser Redirection Extensionをネイティブメッセージングホストにリンクさせ、これにより拡張機能がネイティブコードと通信できるようになります。これがないと、ブラウザーは通信をブロックします。
- ブラウザー拡張機能は、Google Chrome Web Storeから手動でインストールすることもできます。Microsoft EdgeアドオンストアからBrowser Redirection Extensionを使用するには、Virtual Delivery Agent (VDA) バージョン2503以降が必要です。古いVDAバージョンの場合は、Microsoft Edgeブラウザー内でGoogle Chrome Web Storeから拡張機能をインストールしてください（Chrome Web StoreからMicrosoft Edgeに拡張機能を追加するを参照）。
- システム要件に記載されているCitrix Workspaceアプリのバージョンは、双方向コンテンツリダイレクトとOAuthリダイレクトの両方をサポートするために必要な最小バージョンです。
- Macの場合：公証済みアプリケーションに対するmacOSのセキュリティ要件のため、カスタムOAuthコールバックURLスキームはCitrixに事前登録されている必要があり、インストール後に動的に変更することはできません。デフォルトでは`citrix-oauth-redir`のみがサポートされています。URLスキームを登録するには、Citrix製品チームにお問い合わせください。

Citrix VDAからクライアントへのワイルドカードリダイレクト

双方向コンテンツリダイレクトは、リダイレクトするURLを定義する際にワイルドカードの使用をサポートします。双方向コンテンツリダイレクトを構成するには、構成の手順を参照してください。

VDAからクライアントへのカスタムプロトコルリダイレクト

双方向コンテンツリダイレクトは、Citrix VDAからクライアントへのカスタムプロトコルのリダイレクトをサポートします。HTTPまたはHTTPS以外のプロトコルがサポートされています。双方向コンテンツリダイレクトを構成するには、構成の手順を参照してください。

Web Studioで、**双方向コンテンツリダイレクト**のカスタムプロトコルを設定します。

注:

- これらのコマンドを実行するには、管理者権限が必要です。
- クライアントは、プロトコルを処理するために登録されたアプリケーションを持っている必要があります。そうでない場合、URLはクライアントにリダイレクトされますが、起動に失敗します。
- ChromeおよびEdgeブラウザーで入力または起動するカスタムプロトコルURLはサポートされておらず、リダイレクトされません。
- 以下のプロトコルはサポートされていません: `rtsp://, rtspu://, pnm://, mms://`.

その他の考慮事項

- ブラウザの要件と構成は、リダイレクトを開始するブラウザにのみ適用されます。リダイレクトが成功した後にURLが開かれる宛先ブラウザは、サポートの対象とはなりません。VDAからクライアントにURLをリダイレクトする場合、サポートされるブラウザ構成はVDA上でのみ必要です。逆に、クライアントからVDAにURLをリダイレクトする場合、サポートされるブラウザ構成はクライアント上でのみ必要です。リダイレクトされたURLは、方向に応じて、クライアントまたはVDAのいずれかの宛先マシンで構成されているデフォルトのブラウザに渡されます。VDAとクライアントで同じブラウザタイプを使用する必要はありません。
- リダイレクトルールがループ構成にならないことを確認してください。たとえば、VDAポリシーが`https://www.citrix.com`をリダイレクトするように設定され、クライアントポリシーが同じURLをリダイレクトするように設定されている場合、無限ループが発生します。
- URL短縮サービスはサポートされていません。
- クライアントからVDAへのリダイレクトには、Windowsクライアントを管理者権限でインストールする必要があります。
- 宛先ブラウザがすでに開いている場合、リダイレクトされたURLは新しいタブで開きます。そうでない場合、URLは新しいブラウザウィンドウで開きます。
- ローカルアプリアクセス (LAA) が有効になっている場合、双方向コンテンツリダイレクトは機能しません。

ホストからクライアントへのリダイレクト

ホストからクライアントへのリダイレクトにより、Citrix®セッションで実行されているアプリケーションにハイパーリンクとして埋め込まれたURLを、ユーザーのエンドポイントデバイス上の対応するアプリケーションを使用して開くことができます。ホストからクライアントへのリダイレクトの一般的なユースケースには、次のようなものがあります。

- Citrixサーバーがソースへのインターネットまたはネットワークアクセスを持たない場合のWebサイトのリダイレクト。
- セキュリティ、パフォーマンス、互換性、またはスケーラビリティの理由から、Citrixセッション内でWebブラウザを実行することが望ましくない場合のWebサイトのリダイレクト。
- URLを開くために必要なアプリケーションがCitrixサーバーにインストールされていない場合の特定のURLタイプのリダイレクト。

ホストからクライアントへのリダイレクトは、Webページでアクセスしたり、Citrixセッションで実行されているWebブラウザのアドレスバーに入力したりするURLを対象としていません。Webブラウザでの URLのリダイレクトについては、「双方向URLリダイレクト」または「ブラウザコンテンツリダイレクト」を参照してください。

システム要件

- マルチセッションOS VDA
- サポートされているクライアント：
  - Windows向けCitrix Workspace™アプリ
  - Mac向けCitrix Workspaceアプリ
  - Linux向け Citrix Workspace アプリ
  - HTML5向けCitrix Workspaceアプリ
  - Chrome向けCitrix Workspaceアプリ

クライアントデバイスには、URLタイプのリダイレクトを処理するためのアプリケーションがインストールされ、構成されている必要があります。

構成

ホストからクライアントへのリダイレクト Citrixポリシーを使用して、この機能を有効にします。**ホストからクライアントへのリダイレクト**は、デフォルトで無効になっています。ホストからクライアントへのリダイレクトポリシーを有効にすると、Citrix LauncherアプリケーションはWindowsサーバーに登録され、URLを傍受してクライアントデバイスに送信できるようになります。

次に、Windowsグループポリシーを設定して、必要なURLタイプのデフォルトアプリケーションとしてCitrix Launcherを使用するようにします。CitrixサーバーVDAで、ServerFTAdefaultPolicy.xmlファイルを作成し、次のXMLコードを挿入します。

```
<?xml version="1.0" encoding="UTF-8"?>



<DefaultAssociations>



<Association Identifier="http" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



<Association Identifier="https" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



</DefaultAssociations>
```

グループポリシー管理コンソールから、**コンピューターの構成 > 管理用テンプレート > Windows コンポーネント > エクスプローラー > 既定の関連付け構成ファイルの設定**に移動し、ServerFTAdefaultPolicy.xmlファイルを保存します。

注:

Citrixサーバーにグループポリシー設定がない場合、WindowsはURLを開くためのアプリケーションを選択するようユーザーに促します。

デフォルトでは、以下のURLタイプのリダイレクトをサポートしています。

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

リダイレクトのリストに、追加の標準またはカスタムURLタイプを含めるには、前述のServerFTAdefaultPolicy.xmlファイルに新しい**関連付け識別子**の行を作成します。例:

```
<Association Identifier="ftp" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />

<Association Identifier="mailto" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />

<Association Identifier="customtype1" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />

<Association Identifier="customtype2" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

リストにURLタイプを追加するには、クライアント構成も必要です。Windowsクライアントで以下のレジストリキーと値を作成します。

> **注:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような重大な問題を引き起こす可能性があります。レジストリエディターの誤った使用によって生じた問題が解決されることをCitrixは保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- 値の名前: ExtraURLProtocols
- 値の型: REG_SZ
- 値のデータ: 必要なURLタイプをセミコロンで区切って指定します。URLのオーソリティ部分より前のすべてを含めます。例: `ftp://;mailto:;customtype1://;custometype2://`

URLの種類はWindowsクライアントにのみ追加できます。上記のレジストリ設定がないクライアントは、Citrixセッションへのリダイレクトを拒否します。クライアントには、指定されたURLの種類を処理するようにインストールおよび構成されたアプリケーションが必要です。

デフォルトのリダイレクトリストからURLタイプを削除するには、サーバーVDAで以下のレジストリキーと値を作成します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA

- 値の名前: DisableServerFTA
- 値の型: DWORD
- 値のデータ: 1
- 値の名前: NoRedirectClasses
- 値の型: REG_MULTI_SZ
- 値のデータ: 次の値の任意の組み合わせを指定します: `http`、`https`、`rtsp`、`rtspu`、`pnm`、または `mms`。複数の値を別々の行に入力します。例:

`http`

`https`

`rtsp`

特定のWebサイトのセットに対してホストからクライアントへのリダイレクトを有効にするには、サーバーVDAにレジストリキーと値を作成します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前: ValidSites
- 値の型: REG_MULTI_SZ
- 値のデータ: 完全修飾ドメイン名（FQDN）の任意の組み合わせを指定します。複数のFQDNを別々の行に入力します。プロトコル（`http://` または `https://`）を含めず、FQDNのみを含めます。FQDNには、アスタリスク（`*`）をワイルドカード文字として左端の位置にのみ含めることができます。このワイルドカードは、RFC 6125のルールと一致する単一レベルのドメインに一致します。例:

`www.exmaple.com`

`*.example.com`

> **注:**
>
> **ValidSites** キーを **DisableServerFTA** および **NoRedirectClasses** キーと併用することはできません。

サーバーVDAのデフォルトブラウザ構成

このセクションで参照されているホストからクライアントへのリダイレクトを有効にすると、サーバーVDA上の以前のデフォルトブラウザ構成がすべて上書きされます。Web URLがリダイレクトされない場合、Citrix Launcherは、`command_backup` レジストリキーで構成されているブラウザにURLを渡します。このキーはデフォルトでInternet Explorerを指していますが、別のブラウザへのパスを含むように変更できます。詳細については、レジストリで管理される機能のリストにあるサーバーVDAのデフォルトブラウザ構成を参照してください。

ローカルアプリアクセスとURLリダイレクト

はじめに

Local App Accessは、ローカルにインストールされたWindowsアプリケーションを、デスクトップを切り替えることなくホストされたデスクトップ環境にシームレスに統合します。Local App Accessを使用すると、次のことが可能になります。

- 物理的なラップトップ、PC、またはその他のデバイスにローカルにインストールされているアプリケーションに、仮想デスクトップから直接アクセスできます。
- 柔軟なアプリケーション配信ソリューションを提供します。ユーザーが仮想化できない、またはIT部門が保守していないローカルアプリケーションを持っている場合でも、それらのアプリケーションは仮想デスクトップにインストールされているかのように動作します。
- アプリケーションが仮想デスクトップとは別にホストされている場合のダブルホップの遅延を排除します。そのためには、公開アプリケーションへのショートカットをユーザーのWindowsデバイスに配置します。
- 次のようなアプリケーションを使用できます。
    - GoToMeetingなどのビデオ会議ソフトウェア。
    - まだ仮想化されていない特殊なアプリケーションまたはニッチなアプリケーション。
    - ユーザーデバイスからサーバーへ、そしてユーザーデバイスへ戻すという大量のデータ転送を伴うアプリケーションや周辺機器。例えば、DVDバーナーやTVチューナーなど。

Citrix Virtual Apps and Desktops™では、ホストされたデスクトップセッションはURLリダイレクトを使用してローカルアプリアクセスアプリケーションを起動します。URLリダイレクトにより、アプリケーションは複数のURLアドレスで利用可能になります。デスクトップセッション内のブラウザで埋め込みリンクを選択すると、ローカルブラウザ（ブラウザのURLブロックリストに基づいて）が起動します。ブロックリストにないURLに移動すると、そのURLはデスクトップセッションで再度開かれます。

URLリダイレクトはデスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。アプリケーションセッションで使用できる唯一のリダイレクト機能は、ホストからクライアントへのコンテンツリダイレクトです。これは、サーバーFTA（ファイルタイプ関連付け）リダイレクトの一種です。このFTAは、HTTP、HTTPS、RTSP、MMSなどの特定のプロトコルをクライアントにリダイレクトします。例えば、HTTPで埋め込みリンクを開く場合、リンクはクライアントアプリケーションで直接開かれます。URLブロックリストまたは許可リストのサポートはありません。

ローカルアプリアクセスが有効になっている場合、ローカルで実行されているアプリケーションから、ユーザーがホストするアプリケーションから、またはデスクトップ上のショートカットとしてユーザーにリンクとして表示されるURLは、次のいずれかの方法でリダイレクトされます。

- ユーザーのコンピューターからホストされたデスクトップへ
- Citrix Virtual Apps and Desktopsサーバーからユーザーのコンピューターへ
- 起動された環境でレンダリングされます（リダイレクトされません）

特定のWebサイトからのコンテンツのリダイレクトパスを指定するには、Virtual Delivery AgentでURL許可リストとURLブロックリストを構成します。これらのリストには、URLリダイレクトポリシー設定を指定する複数文字列のレジストリキーが含まれています。詳細については、「ローカルアプリアクセス ポリシー設定」を参照してください。

URLは、以下の例外を除き、VDAでレンダリングできます。

- 地域/ロケール情報 — msn.comやnews.google.comなど、ロケール情報を必要とするWebサイト（地域に基づいて国固有のページを開きます）。たとえば、VDAが英国のデータセンターからプロビジョニングされ、クライアントがインドから接続している場合、ユーザーはin.msn.comが表示されることを期待しますが、実際にはuk.msn.comが表示されます。
- マルチメディアコンテンツ — リッチメディアコンテンツを含むWebサイトは、クライアントデバイスでレンダリングされると、エンドユーザーにネイティブなエクスペリエンスを提供し、高遅延ネットワークでも帯域幅を節約します。この機能は、Silverlightなどの他のメディアタイプを含むサイトをリダイレクトします。このプロセスはセキュアな環境で行われます。つまり、管理者が承認したURLはクライアントで実行され、それ以外のURLはVDAにリダイレクトされます。

URLリダイレクトに加えて、FTAリダイレクトを使用できます。FTAは、セッション内でファイルが検出されたときにローカルアプリケーションを起動します。ローカルアプリが起動された場合、そのローカルアプリはファイルを開くためにファイルへのアクセス権を持っている必要があります。したがって、ローカルアプリケーションを使用して開くことができるファイルは、ネットワーク共有上にあるファイルか、クライアントドライブ上にあるファイル（クライアントドライ

ブマッピングを使用）に限られます。たとえば、PDFファイルを開く際に、PDFリーダーがローカルアプリである場合、そのPDFリーダーを使用してファイルが開かれます。ローカルアプリはファイルに直接アクセスできるため、ファイルを開くためのICA®を介したファイルのネットワーク転送は発生しません。

要件、考慮事項、および制限事項

WindowsマルチセッションOS用VDAおよびWindowsシングルセッションOS用VDAの有効なオペレーティングシステムで、ローカルアプリアクセスをサポートしています。ローカルアプリアクセスには、Citrix Workspaceアプリ for Windowsバージョン4.1（最小）が必要です。以下のブラウザーがサポートされています。

- Edge、最新バージョン
- Firefox、最新バージョンおよび延長サポートリリース
- Chrome、最新バージョン

ローカルアプリアクセスとURLリダイレクトを使用する際の以下の考慮事項と制限事項を確認してください。

- ローカルアプリアクセスは、すべてのモニターにまたがる全画面の仮想デスクトップ向けに設計されています。
    - ウィンドウモードで実行される仮想デスクトップや、すべてのモニターをカバーしない仮想デスクトップでローカルアプリアクセスを使用すると、ユーザーエクスペリエンスが混乱する可能性があります。
    - 複数モニター — 1つのモニターが最大化されると、そのセッションで起動されたすべてのアプリケーションのデフォルトデスクトップになります。このデフォルトは、後続のアプリケーションが通常別のモニターで起動される場合でも発生します。
    - この機能は1つのVDAをサポートします。複数の同時VDAとの統合はありません。
- 一部のアプリケーションは予期しない動作をする可能性があり、ユーザーに影響を与えます。
    - ドライブ文字は、たとえば仮想デスクトップのC:ドライブではなくローカルのC:ドライブなど、ユーザーを混乱させる可能性があります。
    - 仮想デスクトップで利用可能なプリンターは、ローカルアプリケーションでは利用できません。
    - 昇格された権限を必要とするアプリケーションは、クライアントホスト型アプリケーションとして起動できません。

  - シングルインスタンスアプリケーション（例：Windows Media Player）に対して特別な処理はありません。
  - ローカルアプリケーションは、ローカルマシンのWindowsテーマで表示されます。
  - 全画面表示アプリケーションはサポートされていません。これらのアプリケーションには、PowerPointのスライドショーやデスクトップ全体を覆うフォトビューアなど、全画面で開くアプリケーションが含まれます。
  - ローカルアプリアクセスは、ローカルアプリケーションのプロパティ（クライアントのデスクトップやスタートメニューのショートカットなど）をVDA上にコピーします。ただし、ショートカットキーや読み取り専用属性などの他のプロパティはコピーしません。
  - 重なり合うウィンドウの順序の処理方法をカスタマイズするアプリケーションは、予測できない結果になる可能性があります。たとえば、一部のウィンドウが非表示になることがあります。
  - ショートカットはサポートされていません。マイコンピューター、ごみ箱、コントロールパネル、ネットワークドライブのショートカット、フォルダーのショートカットなどが含まれます。
  - 次のファイルの種類とファイルはサポートされていません：カスタムファイルの種類、関連付けられたプログラムがないファイル、zipファイル、隠しファイル。
  - 32ビットと64ビットが混在するクライアントホスト型またはVDAアプリケーションの場合、タスクバーのグループ化はサポートされていません。つまり、32ビットのローカルアプリケーションと64ビットのVDAアプリケーションをグループ化することです。
  - COMを使用してアプリケーションを起動することはできません。たとえば、Officeアプリケーション内から埋め込みOfficeドキュメントをクリックした場合、プロセスの開始を検出できず、ローカルアプリケーションの統合は失敗します。

- ユーザーが別の仮想デスクトップセッション内から仮想デスクトップを起動するようなダブルホップシナリオはサポートされていません。
- URLリダイレクトは、明示的なURLのみをサポートします（つまり、ブラウザのアドレスバーに表示されるURL、またはブラウザ内ナビゲーションを使用して見つかるURLのみをサポートします。これはブラウザによって異なります）。
- URLリダイレクトは、デスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。
- VDAセッションのローカルデスクトップフォルダーでは、ユーザーはファイルを作成できません。
- ローカルで実行されているアプリケーションの複数のインスタンスは、仮想デスクトップ用に設定されたタスクバーの設定に従って動作します。ただし、ローカルで実行されているアプリ

ケーションへのショートカットは、それらのアプリケーションの実行中のインスタンスとグループ化されません。また、ホストされているアプリケーションの実行中のインスタンスや、ホストされているアプリケーションへのピン留めされたショートカットともグループ化されません。ユーザーは、タスクバーからローカルで実行されているアプリケーションのウィンドウのみを閉じることができます。ユーザーはローカルアプリケーションウィンドウをデスクトップのタスクバーとスタートメニューにピン留めできますが、これらのショートカットを使用してもアプリケーションが常に起動するとは限りません。

- **Allow Local App Access**ポリシー設定を**Enabled**に設定した場合、ブラウザコンテンツリダイレクトはサポートされません。デフォルトでは、Local App Accessは禁止されています。

Windowsとの対話

Local App AccessとWindowsとの対話には、次の動作が含まれます。

- Windows 8およびWindows Server 2012のショートカットの動作
  - クライアントにインストールされているWindowsストアアプリケーションは、ローカルアプリアクセスのショートカットの一部として列挙されません。
  - 画像ファイルとビデオファイルは、デフォルトでWindowsストアアプリケーションを使用して開かれます。ただし、ローカルアプリアクセスはWindowsストアアプリケーションを列挙し、デスクトップアプリケーションでショートカットを開きます。
- ローカルプログラム
  - Windows 7の場合、フォルダーはスタートメニューで利用できます。
  - Windows 8の場合、Local Programsは、ユーザーがスタート画面からカテゴリとして**All Apps**を選択した場合にのみ利用できます。すべてのサブフォルダーがLocal Programsに表示されるわけではありません。
- アプリケーション向けのWindows 8グラフィック機能
  - デスクトップアプリケーションはデスクトップ領域に制限されており、スタート画面およびWindows 8スタイルのアプリケーションによって覆われます。
  - ローカルアプリアクセスアプリケーションは、マルチモニターモードではデスクトップアプリケーションのように動作しません。マルチモニターモードでは、スタート画面とデスクトップが異なるモニターに表示されます。
- Windows 8とローカルアプリアクセスURLリダイレクト
  - Windows 8のInternet Explorerではアドオンが有効になっていないため、デスクトップ版のInternet Explorerを使用してURLリダイレクトを有効にします。

- Windows Server 2012では、Internet Explorerはデフォルトでアドオンを無効にします。URLリダイレクトを実装するには、Internet Explorerの拡張構成を無効にします。その後、Internet Explorerのオプションをリセットして再起動し、標準ユーザー向けにアドオンが有効になっていることを確認します。

ローカルアプリアクセスとURLリダイレクトの構成

Citrix Workspace™アプリでローカルアプリアクセスとURLリダイレクトを使用するには:

- ローカルクライアントマシンにCitrix Workspaceアプリをインストールします。Citrix Workspaceアプリのインストール中に両方の機能を有効にするか、グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にできます。
- **ローカルアプリアクセスを許可**ポリシー設定を**有効**に設定します。URLリダイレクトのURL許可リストおよびブロックリストポリシー設定も構成できます。詳しくは、「ローカルアプリアクセスポリシー設定」を参照してください。

ローカルアプリアクセスとURLリダイレクトを有効にする

すべてのローカルアプリケーションでローカルアプリアクセスを有効にするには、次の手順に従います:

1. Web Studioにサインインし、左側のペインで**ポリシー**をクリックします。
2. アクションバーで、**ポリシーの作成**をクリックします。
3. ポリシーの作成ウィンドウで、検索ボックスに「Allow Local App Access」と入力し、**選択**をクリックします。
4. 設定の編集ウィンドウで、**許可**を選択します。デフォルトでは、**ローカルアプリアクセスを許可**ポリシーは禁止されています。この設定が許可されている場合、VDAは公開アプリケーションとローカルアプリアクセスのショートカットをセッションで有効にするかどうかをエンドユーザーが決定できるようにします。(この設定が禁止されている場合、公開アプリケーションとローカルアプリアクセスのショートカットの両方がVDAで機能しません。)このポリシー設定は、マシン全体とURLリダイレクトポリシーに適用されます。
5. ポリシーの作成ウィンドウで、検索ボックスに「URL redirection allow list」と入力し、**選択**をクリックします。URLリダイレクト許可リストは、リモートセッションのデフォルトブラウザで開くURLを指定します。
6. 「設定の編集」ウィンドウで、「**追加**」をクリックしてURLを追加し、「**OK**」をクリックします。

7. 「ポリシーの作成」ウィンドウで、検索ボックスに「URL redirection block list」と入力し、「**選択**」をクリックします。URLリダイレクトブロックリストは、エンドポイントで実行されているデフォルトのブラウザーにリダイレクトされるURLを指定します。
8. 「設定の編集」ウィンドウで、「**追加**」をクリックしてURLを追加し、「**OK**」をクリックします。
9. 「設定」ページで、「**次へ**」をクリックします。
10. 「ユーザーとマシン」ページで、該当するデリバリーグループにポリシーを割り当て、「**次へ**」をクリックします。
11. 「概要」ページで設定を確認し、「**完了**」をクリックします。

Citrix Workspaceアプリのインストール中にすべてのローカルアプリケーションでURLリダイレクトを有効にするには、次の手順に従います。

1. マシン上のすべてのユーザーに対してCitrix Workspaceアプリをインストールするときに、URLリダイレクトを有効にします。これにより、URLリダイレクトに必要なブラウザーアドオンも登録されます。
2. コマンドプロンプトから、次のいずれかのオプションを使用してCitrix Workspaceアプリをインストールするための適切なコマンドを実行します。
   - CitrixReceiver.exeの場合は、`/ALLOW_CLIENTHOSTEDAPPSURL=1`を使用します。
   - CitrixReceiverWeb.exeの場合は、`/ALLOW_CLIENTHOSTEDAPPSURL=1`を使用します。

グループポリシーエディターを使用してローカルアプリアクセス テンプレートを有効にする

注:

- グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にする前に、receiver.admx/admlテンプレートファイルをローカルGPOに追加します。
- Windows向けCitrix Workspaceアプリのテンプレートファイルは、CitrixBase.admx/CitrixBase.admlを%systemroot%\policyDefinitionsフォルダーに追加した場合にのみ、ローカルGPOの「**管理用テンプレート > Citrixコンポーネント > Citrix Workspace**」フォルダーで使用できます。

> グループポリシーエディターを使用してローカルアプリアクセス テンプレート を有効にするには、次の手順に従います。

1. **gpedit.msc**を実行します。
2. **コンピューターの構成 > 管理用テンプレート > クラシック管理用テンプレート (ADM) > Citrix Components > Citrix Workspace > ユーザーエクスペリエンス**に移動します。
3. **ローカルアプリアクセス設定**をクリックします。
4. **有効**を選択し、次に**URLリダイレクトを許可**を選択します。URLリダイレクトの場合、この記事の後半にある「*ブラウザーアドオンの登録*」セクションで説明されているコマンドラインを使用して、ブラウザーアドオンを登録します。

公開アプリケーションにのみアクセスを許可する

レジストリエディターまたはPowerShell SDKを使用して、公開アプリケーションへのアクセスを提供できます。

レジストリエディターについては、レジストリを介して管理される機能のリストにある「公開アプリケーションのローカルアプリアクセス」を参照してください。

PowerShell SDKを使用するには:

1. Delivery Controller™が実行されているマシンでPowerShellを開きます。
2. 次のコマンドを入力します: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`。

クラウドサービス展開で**ローカルアプリアクセスアプリケーションの追加**にアクセスするには、Citrix DaaS Remote PowerShell SDKを使用します。詳しくは、「Citrix DaaS Remote PowerShell SDK」を参照してください。

1. インストーラーをダウンロードします:

   `<https://download.apps.cloud.com/CitrixPoshSdk.exe>`
2. これらのコマンドを実行します:

   a. `asnp citrix.*`.

   b. `Get-XdAuthentication`
3. 次のコマンドを入力します: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`。

該当する上記の手順を完了したら、以下の手順に従って続行します。

1. Web Studioにサインインし、左側のペインで**アプリケーション**を選択します。
2. 上部中央のペインで、空白の領域を右クリックし、コンテキストメニューから**ローカルアプリアクセスアプリケーションの追加**を選択します。アクションバーで**ローカルアプリアクセスアプリケーションの追加**をクリックすることもできます。アクションバーにローカルアプリアクセスアプリケーションの追加オプションを表示するには、**更新**をクリックします。
3. ローカルアプリアクセスアプリケーションを公開します。

    - ローカルアプリケーションアクセスウィザードが起動し、概要ページが表示されます。このページは、今後のウィザードの起動時に表示しないように設定できます。
    - ウィザードは、以下に説明するグループ、場所、識別、配信、概要の各ページを案内します。各ページの作業が完了したら、概要ページに到達するまで**次へ**をクリックします。
    - グループページで、新しいアプリケーションを追加するデリバリーグループを1つ以上選択し、**次へ**をクリックします。
    - 場所ページで、ユーザーのローカルマシン上のアプリケーションの完全な実行可能パスを入力し、アプリケーションが配置されているフォルダーへのパスを入力します。Citrixでは、システム環境変数パスを使用することをお勧めします。例: %ProgramFiles(x86)%\Internet Explorer\iexplore.exe。
    - 識別ページで、デフォルト値を受け入れるか、必要な情報を入力してから**次へ**をクリックします。
    - 配信ページで、このアプリケーションをユーザーに配信する方法を設定し、**次へ**をクリックします。選択したアプリケーションのアイコンを指定できます。また、仮想デスクトップ上のローカルアプリケーションへのショートカットを、スタートメニュー、デスクトップ、またはその両方に表示するかどうかを指定することもできます。
    - 概要ページで設定を確認し、**完了**をクリックしてローカルアプリケーションアクセスウィザードを終了します。

ブラウザアドオンを登録する

> **注:**
>
> URLリダイレクトに必要なブラウザアドオンは、Citrix Workspaceアプリをコマンドラインから/ALLOW_CLIENTHOSTEDAPPSURL=1オプションを使用してインストールする際に自動的に登録されます。

次のコマンドを使用して、1つまたはすべてのアドオンを登録および登録解除できます。

- クライアントデバイスにアドオンを登録するには：\<*client-installation-folder*>\redirector.exe /reg\<*browser*>
- クライアントデバイスのアドオンを登録解除するには：\<*client-installation-folder*>\redirector.exe /unreg\<*browser*>
- VDAにアドオンを登録するには：\<*VDAinstallation-folder*>\VDARedirector.exe /reg\<*browser*>
- VDAのアドオンを登録解除するには：\<*VDAinstallation-folder*>\VDARedirector.exe /unreg\<*browser*>

ここで、\<*browser*>はInternet Explorer、Firefox、Chrome、またはAllです。

たとえば、次のコマンドは、Citrix Workspaceアプリを実行しているデバイスにInternet Explorerアドオンを登録します。

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

次のコマンドは、WindowsマルチセッションOS VDA上のすべてのアドオンを登録します。

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

ブラウザ間でのURLインターセプト

- デフォルトでは、Internet Explorerは指定されたURLをリダイレクトします。URLがブロックリストにないが、ブラウザまたはWebサイトが別のURLにリダイレクトする場合、最終的なURLはリダイレクトされません。ブロックリストにある場合でもリダイレクトされません。

URLリダイレクトが正しく機能するためには、ブラウザからプロンプトが表示されたときにアドオンを有効にしてください。インターネットオプションを使用しているアドオン、またはプロンプト内のアドオンが無効になっている場合、URLリダイレクトは正しく機能しません。

- Firefoxのアドオンは常にURLをリダイレクトします。

アドオンがインストールされると、Firefoxは新しいタブページにアドオンをインストールすることを許可するか、または阻止するかを促します。機能が動作するようにアドオンを許可してください。

- Chromeアドオンは、入力されたURLではなく、ナビゲートされた最終URLを常にリダイレクトします。

拡張機能は外部からインストールされています。拡張機能を無効にすると、ChromeではURLリダイレクト機能が動作しません。シークレットモードでURLリダイレクトが必要な場合は、ブラウザ設定でそのモードで拡張機能が実行されることを許可してください。

ログオフ時および切断時のローカルアプリケーションの動作を構成する

注記:

これらの手順に従って設定を構成しない場合、デフォルトでは、ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは実行を継続します。再接続後、ローカルアプリケーションが仮想デスクトップで利用可能な場合、それらは再統合されます。

ログオフ時および切断時のローカルアプリケーションの動作を構成するには、レジストリを介して管理される機能のリストにある「ログオフ時および切断時のローカルアプリケーションの動作」(/ja-jp/citrix-virtual-apps-desktops/2411/policies/reference/hdx-registry-settings.html)を参照してください。

印刷

環境内のプリンターの管理は、多段階のプロセスです。

1. まだ慣れていない場合は、印刷の概念に慣れてください。
2. 印刷アーキテクチャを計画します。これには、ビジネスニーズ、既存の印刷インフラストラクチャ、ユーザーとアプリケーションが現在印刷とどのようにやり取りしているか、およびどの印刷管理モデルが環境に最適であるかを分析することが含まれます。
3. プリンタープロビジョニング方法を選択し、印刷設計を展開するためのポリシーを作成して、印刷環境を構成します。新しい従業員やサーバーが追加されたときにポリシーを更新します。
4. ユーザーに展開する前に、パイロット印刷構成をテストします。
5. プリンタードライバーを管理し、印刷パフォーマンスを最適化することで、Citrix® 印刷環境を維持します。
6. 発生する可能性のある問題をトラブルシューティングします。

印刷の概念

展開の計画を開始する前に、印刷に関する以下の主要な概念を理解していることを確認してください。

- 利用可能なプリンタープロビジョニングの種類
- 印刷ジョブがどのようにルーティングされるか
- プリンタードライバー管理の基本

印刷の概念は、Windowsの印刷の概念に基づいています。環境で印刷を構成し、正常に管理するには、Windowsのネットワーク印刷とクライアント印刷がどのように機能するか、そしてそれがこの環境での印刷動作にどのように変換されるかを理解する必要があります。

印刷プロセス

この環境では、すべての印刷は、アプリケーションをホストするマシン上で（ユーザーによって）開始されます。印刷ジョブは、ネットワーク印刷サーバーまたはユーザーデバイスを介して印刷デバイスにリダイレクトされます。

仮想デスクトップおよびアプリケーションのユーザーには、永続的なワークスペースはありません。セッションが終了すると、ユーザーのワークスペースは削除されるため、すべての設定は各セッションの開始時に再構築される必要があります。その結果、ユーザーが新しいセッションを開始するたびに、システムはユーザーのワークスペースを再構築する必要があります。

ユーザーが印刷する場合：

- ユーザーに提供するプリンターを決定します。これはプリンタープロビジョニングとして知られています。
- ユーザーの印刷設定を復元します。
- セッションの既定のプリンターを決定します。

プリンタープロビジョニング、印刷ジョブのルーティング、プリンタープロパティの保持、およびドライバー管理のオプションを構成することで、これらのタスクを実行する方法をカスタマイズできます。さまざまなオプション設定が、環境での印刷パフォーマンスとユーザーエクスペリエンスにどのように影響するかを評価するようにしてください。

プリンタープロビジョニング

セッションでプリンターを利用可能にするプロセスは、プロビジョニングとして知られています。プリンタープロビジョニングは通常、動的に処理されます。つまり、セッションに表示されるプリンターは、事前に決定されて保存されるわけではありません。代わりに、ログオン時および再接続時にセッションが構築される際に、ポリシーに基づいてプリンターが組み立てられます。その結果、ポリシーに反映されていれば、プリンターはポリシー、ユーザーの場所、およびネットワークの変更に応じて変化する可能性があります。したがって、別の場所に移動するユーザーは、ワークスペースの変更を確認する場合があります。

システムはまた、クライアント側のプリンターを監視し、クライアント側のプリンターへの追加、削除、変更に基づいて、セッション内で自動作成されたプリンターを動的に調整します。この動的なプリンター検出は、さまざまなデバイスから接続するモバイルユーザーにメリットをもたらします。

プリンタープロビジョニングの最も一般的な方法は次のとおりです。

- **Universal Print Server** - Citrix Universal Print Serverは、ネットワークプリンターのユニバーサル印刷をサポートします。Universal Print Serverは、ユニバーサル印刷ドライバーを使用します。このソリューションにより、マルチセッションOSマシンで単一のドライバーを使用して、任意のデバイスからネットワーク印刷を可能にすることができます。

Citrixは、リモート印刷サーバーのシナリオにCitrix Universal™ Print Serverを推奨しています。Universal Print Serverは、最適化され圧縮された形式で印刷ジョブをネットワーク経由で転送するため、ネットワークの使用量を最小限に抑え、ユーザーエクスペリエンスを向上させます。

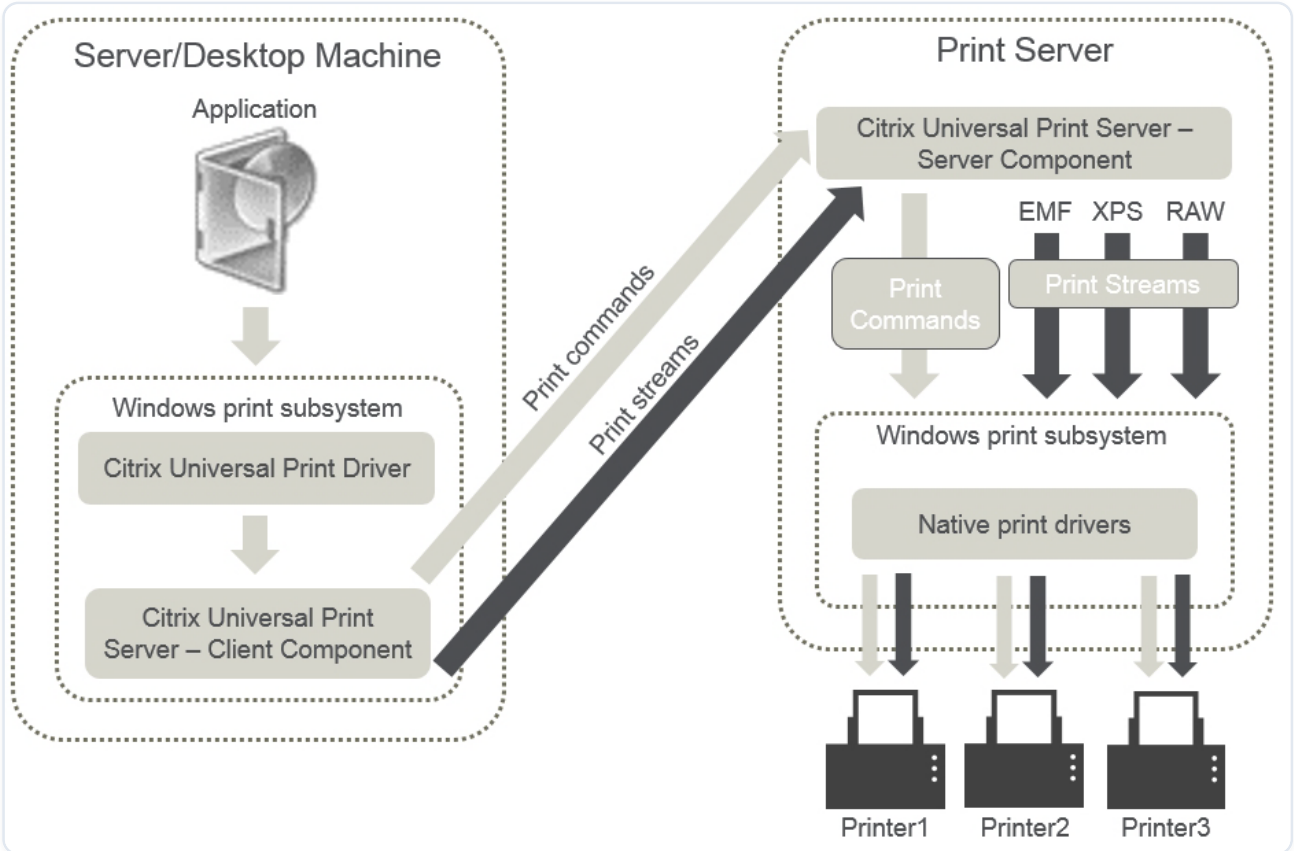
Universal Print Serverの機能は次のとおりです:

クライアントコンポーネント、**UPClient** - セッションネットワークプリンターをプロビジョニングし、ユニバーサル印刷ドライバーを使用する各マルチセッションOSマシンでUPClientを有効にします。

サーバーコンポーネント、**UPServer** - セッションネットワークプリンターをプロビジョニングし、セッションプリンター（セッションプリンターが集中管理されているかどうかにかかわらず）にユニバーサル印刷ドライバーを使用する各印刷サーバーにUPServerをインストールします。

Universal Print Server の要件とセットアップの詳細については、システム要件とインストールの記事を参照してください。

次の図は、Universal Print Server を使用する環境におけるネットワークベースのプリンターの一般的なワークフローを示しています。



Citrix Universal Print Server を有効にすると、接続されているすべてのネットワークプリンターが自動検出によって自動的にそれを利用します。

- **自動作成** - *自動作成*とは、各セッションの開始時に自動的に作成されるプリンターを指します。リモートネットワークプリンターとローカルに接続されたクライアントプリンターの両方を自動作成できます。ユーザーあたりのプリンター数が多い環境では、デフォルトのクライアントプリンターのみを自動作成することを検討してください。プリンターの自動作成数を減らすと、マルチセッションOSマシンでのオーバーヘッド（メモリとCPU）が少なくなります。自動作成されるプリンターを最小限に抑えることで、ユーザーのログオン時間を短縮することもできます。

  自動作成されたプリンターは、以下に基づいています。

  - ユーザーデバイスにインストールされているプリンター。
  - セッションに適用されるポリシー。

    自動作成ポリシー設定を使用すると、自動作成されるプリンターの数または種類を制限できます。デフォルトでは、ローカル接続プリンターとネットワークプリンターを含む、ユーザーデバイス上のすべてのプリンターを自動的に構成すると、プリンターはセッションで利用可能になります。

  ユーザーがセッションを終了すると、そのセッションのプリンターは削除されます。

  クライアントおよびネットワークプリンターの自動作成には、関連するメンテナンスが必要です。たとえば、プリンターを追加するには、次の操作が必要です。

  - セッションプリンターポリシー設定を更新します。
  - プリンタードライバーマッピングと互換性ポリシー設定を使用して、すべてのマルチセッションOSマシンにドライバーを追加します。

印刷ジョブのルーティング

印刷経路という用語は、印刷ジョブがルーティングされるパスと、印刷ジョブがスプールされる場所の両方を指します。この概念の両方の側面が重要です。ルーティングはネットワークトラフィックに影響します。スプールは、ジョブを処理するデバイス上のローカルリソースの利用に影響します。

この環境では、印刷ジョブは印刷デバイスへの2つのパスを取ることができます。クライアント経由またはネットワークプリントサーバー経由です。これらのパスは、クライアント印刷経路およびネットワーク印刷経路と呼ばれます。どちらのパスがデフォルトで選択されるかは、使用されるプリンターの種類によって異なります。

ローカル接続プリンター

システムは、Multi-session OSマシンからクライアント経由で、ローカル接続プリンターにジョブをルーティングし、その後印刷デバイスにルーティングします。ICA®プロトコルは、印刷ジョブトラフィックを最適化および圧縮します。印刷デバイスがユーザーデバイスにローカルに接続されている場合、印刷ジョブはICA仮想チャネル経由でルーティングされます。

ローカル接続プリンターへの印刷ジョブのルーティング図(/en-us/citrix-virtual-apps-desktops/2411/media/cds-print-local-attached.png)

ネットワークベースのプリンター

デフォルトでは、ネットワークプリンター宛てのすべての印刷ジョブは、Multi-session OSマシンからネットワーク経由で直接プリントサーバーにルーティングされます。ただし、次の状況では、印刷ジョブはICA接続経由で自動的にルーティングされます。

- 仮想デスクトップまたはアプリケーションがプリントサーバーに接続できない場合。
- Multi-session OSマシンでネイティブプリンタードライバーが利用できない場合。

Universal Print Serverが有効になっていない場合、ネットワーク印刷用のクライアント印刷経路を構成することは、広域ネットワークなどの低帯域幅接続に役立ちます。これらの接続は、ICA接続経由でジョブを送信することによって得られる最適化とトラフィック圧縮の恩恵を受けることができます。

クライアント印刷経路を使用すると、印刷ジョブに割り当てられるトラフィックを制限したり、帯域幅を制限したりすることもできます。印刷機能のないシンクライアントなど、ユーザーデバイス経由でジョブをルーティングできない場合、ICA/HDXトラフィックを優先し、良好なセッション内ユーザーエクスペリエンスを確保するために、Quality of Serviceを構成する必要があります。

ネットワーク接続プリンターへの印刷ジョブのルーティング図(/en-us/citrix-virtual-apps-desktops/2411/media/cds-print-network-attached.png)

印刷ドライバー管理

Citrix Universal Printer Driver (UPD) は、デバイスに依存しない印刷ドライバーであり、ほとんどのプリンターと互換性があります。Citrix UPDは2つのコンポーネントで構成されています。

サーバーコンポーネント。Citrix UPDは、Citrix Virtual Apps and Desktops™ VDAのインストールの一部としてインストールされます。VDAは、Citrix UPDとともに次のドライバーをインストールします。「Citrix Universal Printer」（EMFドライバー）と「Citrix XPS Universal Printer」（XPSドライバー）。

印刷ドライバー(/en-us/citrix-virtual-apps-desktops/2411/media/print-drivers.png)

VDAインストーラーは、Universal Print Server PDFプリンタードライバーのインストールを制御するオプションを提供しなくなりました。PDFプリンタードライバーは常に自動的にインストールされるようになりました。7.17 VDA（またはそれ以降のサポートされるバージョン）にアップグレードすると、以前にインストールされていたCitrix PDFプリンタードライバーは自動的に削除され、最新バージョンに置き換えられます。

印刷ジョブが開始されると、ドライバーはアプリケーションの出力を記録し、変更せずにエンドポイントデバイスに送信します。

クライアントコンポーネント。Citrix UPDは、Citrix Workspace™アプリのインストールの一部としてインストールされます。Citrix Virtual Apps and Desktopsセッションの受信印刷ストリームを取得します。その後、印刷ストリームをローカル印刷サブシステムに転送し、そこでデバイス固有のプリンタードライバーを使用して印刷ジョブがレンダリングされます。

Citrix UPDは、以下の印刷形式をサポートしています。

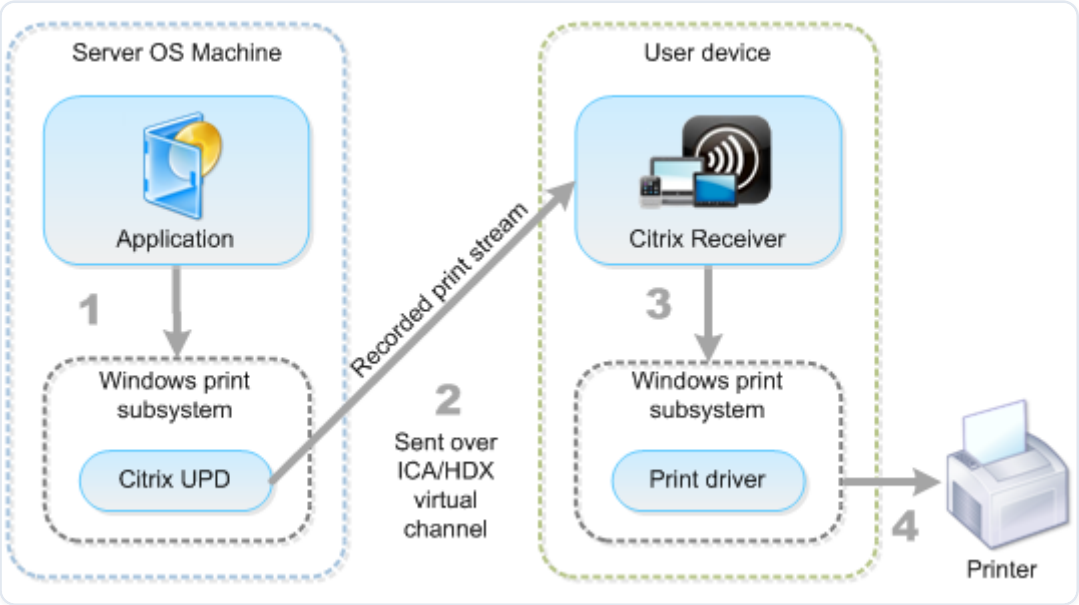
- 拡張メタファイル形式（**EMF**）、デフォルト。EMFは、Windowsメタファイル（WMF）形式の32ビットバージョンです。EMFドライバーは、Windowsベースのクライアントのみが使用できます。
- XML Paper Specification（**XPS**）。XPSドライバーはXMLを使用して、Adobe PDF形式に似たプラットフォームに依存しない「電子ペーパー」を作成します。
- プリンターコマンド言語（**PCL5c**および**PCL4**）。PCLは、元々ヒューレット・パッカードがインクジェットプリンター用に開発した印刷プロトコルです。基本的なテキストとグラフィックの印刷に使用され、HP LaserJetおよび多機能周辺機器で広くサポートされています。
- PostScript（**PS**）。PostScriptは、テキストやベクターグラフィックの印刷に使用できるコンピューター言語です。このドライバーは、低コストのプリンターや多機能周辺機器で広く使用されています。

PCLおよびPSドライバーは、MacやUNIXクライアントなどのWindows以外のデバイスを使用する場合に最適です。Citrix UPDがドライバーを使用しようとする順序は、ユニバーサルドライバーの優先順位ポリシー設定を使用して変更できます。

Citrix UPD（EMFおよびXPSドライバー）は、ステープルや給紙トレイの選択などの高度な印刷機能をサポートしています。これらの機能は、ネイティブドライバーがMicrosoft Print Capabilityテクノロジーを使用して利用可能にする場合に利用できます。ネイティブドライバーは、Print Capabilities XMLで標準化されたPrint Schema Keywordsを使用する必要があります。標準以外の

キーワードが使用されている場合、Citrix Universal Print Driverでは高度な印刷機能は利用できません。

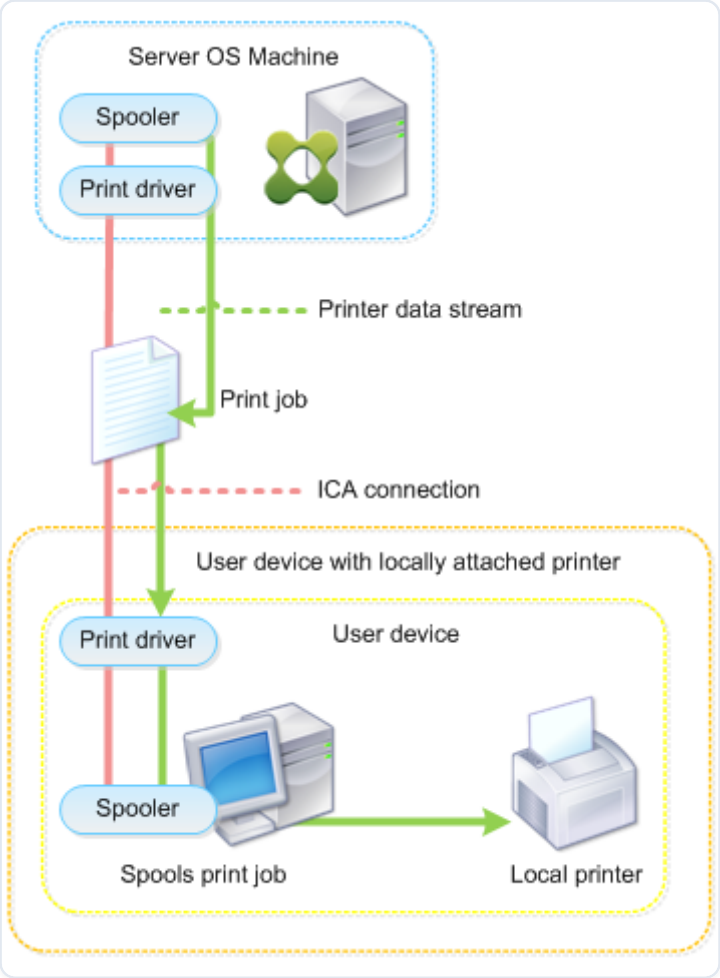
次の図は、ユニバーサルプリンタードライバーのコンポーネントと、デバイスにローカル接続されたプリンターの一般的なワークフローを示しています。



ドライバー管理戦略を計画する際には、ユニバーサルプリンタードライバー、デバイス固有のドライバー、またはその両方をサポートするかどうかを決定します。標準ドライバーをサポートする場合は、以下を決定する必要があります。

プリンターの自動作成中に、システムがユーザーデバイスに接続された新しいローカルプリンターを検出した場合、必要なプリンタードライバーをMulti-session OSマシンで確認します。デフォルトでは、Windowsネイティブドライバーが利用できない場合、システムはユニバーサルプリンタードライバーを使用します。

マルチセッションOSマシン上のプリンタードライバーとユーザーデバイス上のドライバーは、印刷を成功させるために一致している必要があります。以下の図は、クライアント印刷でプリンタードライバーが2か所でどのように使用されるかを示しています。



- サポートするドライバーの種類。
- マルチセッションOSマシンにプリンタードライバーがない場合に、自動的にインストールするかどうか。
- ドライバー互換性リストを作成するかどうか。

関連コンテンツ

- 印刷構成の例
- ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作
- 印刷ポリシーと設定
- プリンターのプロビジョニング
- 印刷環境の維持

印刷構成の例

ニーズと環境に最も適した印刷構成オプションを選択することで、管理を簡素化できます。デフォルトの印刷構成では、ほとんどの環境でユーザーが印刷できますが、そのデフォルト設定では、期待されるユーザーエクスペリエンスや、環境に最適なネットワーク使用量と管理オーバーヘッドが得られない場合があります。

印刷構成は、以下によって異なります。

- ビジネスニーズと既存の印刷インフラストラクチャ。

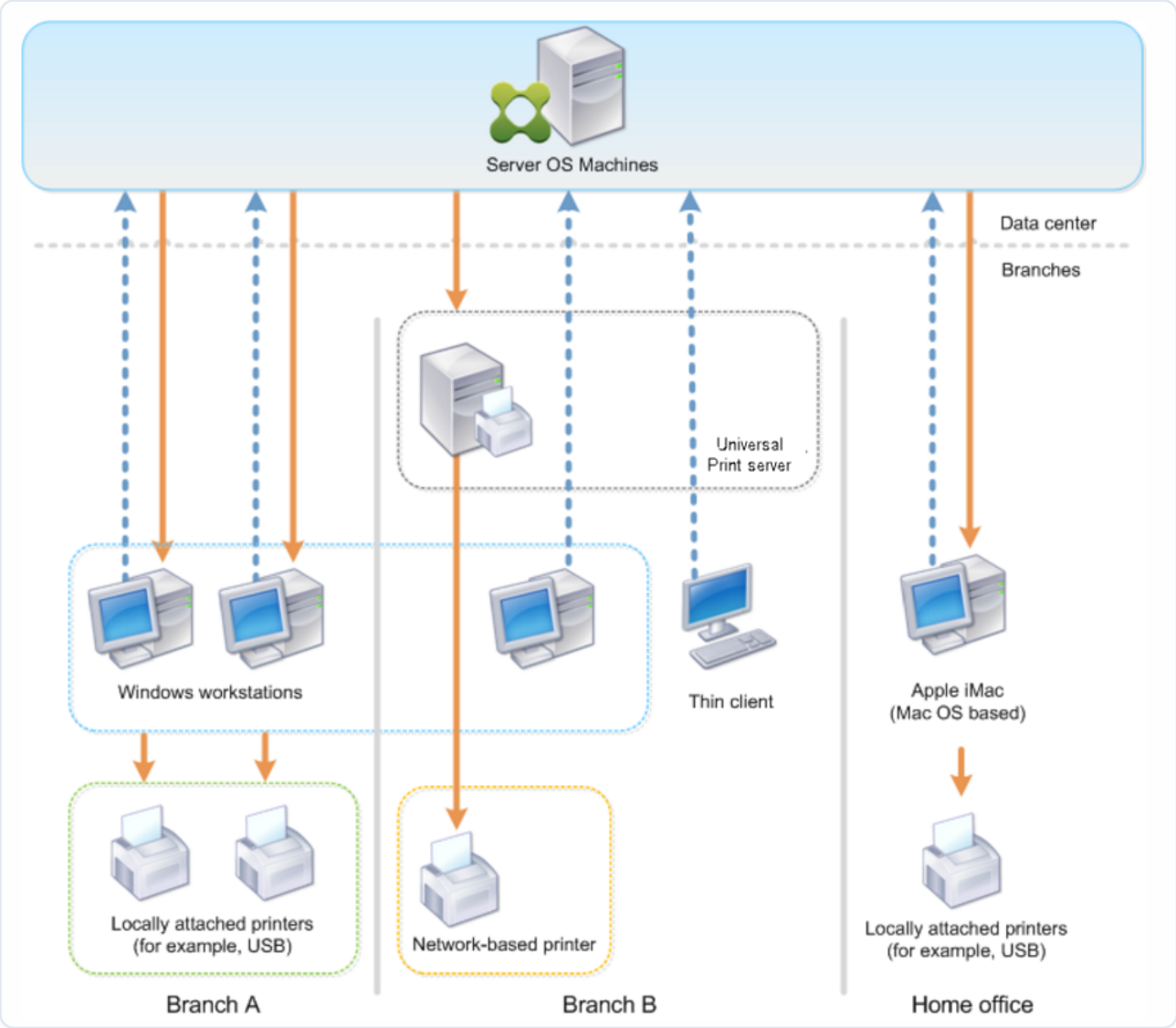
  組織のニーズに合わせて印刷構成を設計します。既存の印刷実装（ユーザーがプリンターを追加できるかどうか、どのユーザーがどのプリンターにアクセスできるかなど）は、印刷構成を定義する際の有用なガイドとなる場合があります。
- 組織に、特定のユーザー（人事部や給与計算用のプリンターなど）のためにプリンターを予約するセキュリティポリシーがあるかどうか。
- ユーザーが、ワークステーション間を移動する従業員や出張中の従業員のように、主要な作業場所から離れているときに印刷する必要があるかどうか。

印刷構成を設計する際は、ローカルユーザーデバイスから印刷する場合と同じエクスペリエンスをセッション内でユーザーに提供するようにしてください。

印刷展開の例

次の図は、これらのユースケースの印刷展開を示しています。

- **支店A** - 数台のWindowsワークステーションがある小規模な海外支店。各ユーザーワークステーションには、ローカルに接続されたプライベートプリンターがあります。
- **支店B** - シンクライアントとWindowsベースのワークステーションがある大規模な支店。効率を高めるため、この支店のユーザーはネットワークベースのプリンター（フロアごとに1台）を共有しています。支店内に設置されたWindowsベースのプリントサーバーが印刷キューを管理します。
- **ホームオフィス** - 会社のCitrix®インフラストラクチャにアクセスするMac OSベースのユーザーデバイスがあるホームオフィス。ユーザーデバイスにはローカルに接続されたプリンターがあります。



以下のセクションでは、環境の複雑さを最小限に抑え、管理を簡素化する構成について説明します。

自動作成されたクライアントプリンターとCitrix Universal™プリンタードライバー

支店Aでは、すべてのユーザーがWindowsベースのワークステーションで作業するため、自動作成されたクライアントプリンターとUniversalプリンタードライバーが使用されます。これらのテクノロジーは、以下の利点を提供します。

- パフォーマンス - 印刷ジョブはICA®印刷チャネルを介して配信されるため、印刷データを圧縮して帯域幅を節約できます。

  大容量のドキュメントを印刷する単一のユーザーが他のユーザーのセッションパフォーマンスを低下させないように、Citrixポリシーが最大印刷帯域幅を指定するように構成されています。

代替ソリューションとして、マルチストリームICA接続を活用する方法があります。この接続では、印刷トラフィックが個別の低優先度TCP接続内で転送されます。マルチストリームICAは、WAN接続でQuality of Service (QoS) が実装されていない場合の選択肢です。

- 柔軟性 - Citrix Universalプリンタードライバーを使用することで、クライアントに接続されたすべてのプリンターを、データセンターに新しいプリンタードライバーを統合することなく、仮想デスクトップまたはアプリケーションセッションから使用できます。

Citrix ユニバーサル プリント サーバー

支店Bでは、すべてのプリンターがネットワークベースであり、そのキューはWindowsプリントサーバーで管理されているため、Citrix Universal Print Serverが最も効率的な構成となります。

必要なすべてのプリンタードライバーは、ローカル管理者によってプリントサーバーにインストールおよび管理されます。仮想デスクトップまたはアプリケーションセッションへのプリンターのマッピングは、次のように機能します。

- Windowsベースのワークステーションの場合 - ローカルITチームは、ユーザーが適切なネットワークベースのプリンターをWindowsワークステーションに接続するのを支援します。これにより、ユーザーはローカルにインストールされたアプリケーションから印刷できるようになります。

  仮想デスクトップまたはアプリケーションセッション中、ローカルで構成されたプリンターは自動作成によって列挙されます。その後、仮想デスクトップまたはアプリケーションは、可能であれば直接ネットワーク接続としてプリントサーバーに接続します。

  Citrix Universal Print Serverコンポーネントがインストールされ有効になっているため、ネイティブプリンタードライバーは不要です。ドライバーが更新されたり、プリンターキューが変更されたりしても、データセンターでの追加構成は必要ありません。
- シンクライアントの場合 - シンクライアントユーザーの場合、プリンターは仮想デスクトップまたはアプリケーションセッション内で接続する必要があります。ユーザーに最もシンプルな印刷エクスペリエンスを提供するために、管理者はフロアごとに単一のCitrixセッションプリンターポリシーを構成し、そのフロアのプリンターをデフォルトプリンターとして接続します。

  ユーザーがフロア間を移動しても正しいプリンターが接続されるように、ポリシーはサブネットまたはシンクライアントの名前に基づいてフィルタリングされます。この構成は近接印刷と呼ばれ、ローカルプリンタードライバーのメンテナンスを可能にします（委任された管理モデルに従って）。

  プリンターキューを変更または追加する必要がある場合、Citrix管理者は環境内の該当するセッションプリンターポリシーを変更する必要があります。

ネットワーク印刷トラフィックはICA仮想チャネルの外部で送信されるため、QoSが実装されます。ICA/HDXトラフィックで使用されるポートでのインバウンドおよびアウトバウンドのネットワークトラフィックは、他のすべてのネットワークトラフィックよりも優先されます。この構成により、大規模な印刷ジョブによってユーザーセッションが影響を受けることはありません。

自動作成されたクライアントプリンターとCitrixユニバーサルプリンタードライバー

ユーザーが標準外のワークステーションで作業し、管理されていない印刷デバイスを使用するホームオフィスの場合、最も簡単な方法は、自動作成されたクライアントプリンターとユニバーサルプリンタードライバーを使用することです。

展開の概要

要約すると、サンプル展開は次のように構成されています。

- マルチセッションOSマシンにはプリンタードライバーはインストールされません。Citrixユニバーサルプリンタードライバーのみが使用されます。ネイティブ印刷へのフォールバックとプリンタードライバーの自動インストールは無効になっています。
- すべてのユーザーに対してすべてのクライアントプリンターを自動作成するようにポリシーが構成されています。マルチセッションOSマシンは、デフォルトで印刷サーバーに直接接続します。必要な構成は、ユニバーサルプリントサーバーコンポーネントを有効にすることだけです。
- ブランチBの各フロアにセッションプリンターポリシーが構成され、それぞれのフロアのすべてのシンクライアントに適用されます。
- 優れたユーザーエクスペリエンスを確保するために、ブランチBにQoSが実装されています。

ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作

ベストプラクティス

特定の環境に最適な印刷ソリューションを決定する要因は多数あります。これらのベストプラクティスの一部は、お客様のサイトには適用されない場合があります。

- Citrix Universal™ Print Serverを使用します。
- ユニバーサルプリンタードライバーまたはWindowsネイティブドライバーを使用します。
- マルチセッションOSマシンにインストールするプリンタードライバーの数を最小限に抑えます。

- ネイティブドライバーへのドライバーマッピングを使用します。
- テストされていないプリンタードライバーを実稼働サイトにインストールしないでください。
- ドライバーの更新は避けてください。常にドライバーをアンインストールし、プリントサーバーを再起動してから、交換用ドライバーをインストールするようにしてください。
- 使用されていないドライバーをアンインストールするか、プリンタードライバーマッピングおよび互換性ポリシーを使用して、そのドライバーでプリンターが作成されないようにします。
- バージョン2のカーネルモードドライバーの使用は避けてください。
- プリンターモデルがサポートされているかどうかを確認するには、製造元に問い合わせるか、www.citrix.com/readyでCitrix Ready製品ガイドを参照してください。

  一般的に、Microsoftが提供するすべてのプリンタードライバーはターミナルサービスでテストされており、Citrixで動作することが保証されています。ただし、サードパーティ製プリンタードライバーを使用する前に、そのドライバーがWindows Hardware Quality Labs (WHQL) プログラムによってターミナルサービス向けに認定されているかどうかをプリンタードライバーベンダーに確認してください。Citrixはプリンタードライバーを認定していません。

セキュリティに関する考慮事項

Citrixの印刷ソリューションは、設計上安全です。

- Citrix Print Manager Serviceは、ログオンとログオフ、切断、再接続、セッション終了などのセッションイベントを常に監視し、対応します。実際のセッションユーザーになりすましてサービス要求を処理します。
- Citrix印刷は、各プリンターにセッション内で一意の名前空間を割り当てます。
- Citrix印刷は、自動作成されたプリンターのデフォルトのセキュリティ記述子を設定し、あるセッションで自動作成されたクライアントプリンターが、他のセッションで実行されているユーザーからアクセスできないようにします。デフォルトでは、管理ユーザーは、他のセッションのクライアントプリンターを見たり、手動でアクセス許可を調整したりできる場合でも、誤って印刷することはできません。

デフォルトの印刷操作

デフォルトでは、ポリシー規則を構成しない場合、印刷動作は次のとおりです。

- ユニバーサルプリントサーバーは無効になっています。
- ユーザーデバイスで構成されているすべてのプリンターは、各セッションの開始時に自動的に作成されます。

この動作は、Citrixポリシー設定「クライアントプリンターを自動作成」を「すべてのクライアントプリンターを自動作成」オプションで構成することと同等です。

- システムは、ユーザーデバイスにローカルに接続されたプリンターにキューに入れられたすべての印刷ジョブをクライアント印刷ジョブとしてルーティングします（つまり、ICA®チャネルを介してユーザーデバイス経由で）。
- システムは、ネットワークプリンターにキューに入れられたすべての印刷ジョブを、Multi-session OSマシンから直接ルーティングします。システムがネットワーク経由でジョブをルーティングできない場合、リダイレクトされたクライアント印刷ジョブとしてユーザーデバイス経由でルーティングします。

  この動作は、Citrixポリシー設定「プリントサーバーへの直接接続」を無効にすることと同等です。
- システムは、ユーザーの印刷設定と印刷デバイス固有の設定の組み合わせである印刷プロパティをユーザーデバイスに保存しようとします。クライアントがこの操作をサポートしない場合、システムは印刷プロパティをMulti-session OSマシンのユーザープロファイルに保存します。

  この動作は、Citrixポリシー設定「プリンタープロパティの保持」を「クライアントに保存されていない場合のみプロファイルに保持」オプションで構成することと同等です。
- VDAバージョン7.16以降では、Windows 8以降のWindowsオペレーティングシステムバージョンでは、V3インボックスプリンタードライバーがオペレーティングシステムに含まれていないため、Citrixポリシー設定「インボックスプリンタードライバーの自動インストール」は効果がありません。
- 7.16より前のVDAでは、Multi-session OSマシンで利用可能な場合、システムはプリンタードライバーのWindowsバージョンを使用します。プリンタードライバーが利用できない場合、システムはWindowsオペレーティングシステムからドライバーをインストールしようとします。ドライバーがWindowsで利用できない場合、Citrixユニバーサルプリンタードライバーを使用します。

  この動作は、Citrixポリシー設定「インボックスプリンタードライバーの自動インストール」を有効にし、ユニバーサル印刷設定を「要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用する」で構成することと同等です。

  「インボックスプリンタードライバーの自動インストール」を有効にすると、多数のネイティブプリンタードライバーがインストールされる可能性があります。

> **注:**

> 印刷の出荷時デフォルトが何であるか不明な場合は、新しいポリシーを作成し、すべての印刷ポリシー規則を「有効」に設定して表示します。表示されるオプションがデフォルトです。

常時オンのログ記録

VDA上のプリントサーバーおよび印刷サブシステムで、常時オンのログ記録機能を利用できます。

ログをZIPファイルとしてまとめてメールで送信したり、Citrix Insight Servicesに自動的にアップロードしたりするには、**Start-TelemetryUpload** PowerShellコマンドレットを使用します。

プリンターのプロビジョニング

Citrix Universal™ プリントサーバー

環境に最適な印刷ソリューションを決定する際には、次の点を考慮してください。

- Universal Print Serverは、Windows Print Providerでは利用できない機能（イメージとフォントのキャッシュ、高度な圧縮、最適化、QoSサポート）を提供します。
- Universal Print Driverは、Microsoftが定義するパブリックなデバイス非依存設定をサポートします。ユーザーが特定のプリンタードライバーメーカーに固有のデバイス設定にアクセスする必要がある場合、Universal Print ServerとWindowsネイティブドライバーの組み合わせが最適なソリューションとなる可能性があります。この構成により、Universal Print Serverの利点を維持しつつ、ユーザーに特殊なプリンター機能へのアクセスを提供できます。考慮すべきトレードオフとして、Windowsネイティブドライバーにはメンテナンスが必要です。
- Citrix Universal Print Serverは、ネットワークプリンターのユニバーサル印刷をサポートします。Universal Print Serverは、Multi-session OSマシン上の単一ドライバーであるUniversal Print Driverを使用し、シンクライアントやタブレットを含むあらゆるデバイスからのローカルまたはネットワーク印刷を可能にします。

WindowsネイティブドライバーでUniversal Print Serverを使用するには、Universal Print Serverを有効にします。デフォルトでは、Windowsネイティブドライバーが利用可能な場合はそれが使用されます。そうでない場合は、Universal Print Driverが使用されます。Windowsネイティブドライバーのみを使用するか、Universal Print Driverのみを使用するかなど、その動作の変更を指定するには、Universal Print Driverの使用ポリシー設定を更新します。

Universal Print Serverのインストール

Universal Print Serverを使用するには、インストールドキュメントに記載されているとおり、プリントサーバーにUpsServerコンポーネントをインストールして構成します。詳細については、「コアコンポーネントのインストール」および「コマンドラインを使用したインストール」を参照してください。

UPClientコンポーネントを個別に展開したい環境（例: **XenApp 6.5**を使用する場合）では、次の手順を実行します。

1. Windows Single-session OSまたはWindows Multi-session OS用のCitrix Virtual Apps and Desktops™ Virtual Delivery Agent (VDA) スタンドアロンパッケージをダウンロードします。
2. 「コマンドラインを使用したインストール」に記載されているコマンドラインの手順を使用してVDAを抽出します。
3. \\Image-Full\\Support\\VcRedist_2013_RTM から前提条件をインストールします。
    - Vcredist_x64 / vcredist_x86
        - 32ビット展開の場合はx86を、64ビット展開の場合は両方を実行します。
4. \\Image-Full\\x64\\Virtual Desktop Components または \\Image-Full\\x86\\Virtual Desktop Components からcdfの前提条件をインストールします。
    - Cdf_x64 / Cdf_x86
        - x86は32ビット用、x64は64ビット用
5. \\Image-Full\\x64\\Virtual Desktop Components または \\Image-Full\\x86\\Virtual Desktop Components でUPClientコンポーネントを見つけます。
6. UPClientコンポーネントを抽出し、そのMSIを起動してインストールします。
7. UPClientコンポーネントのインストール後、再起動が必要です。

Universal Print ServerのCEIPをオプトアウトする

Universal Print Serverをインストールすると、Citrix Customer Experience Improvement Program (CEIP) に自動的に登録されます。データの初回アップロードは、インストール日時から7日後に行われます。

CEIPをオプトアウトするには、レジストリキー **HKLM\\Software\\Citrix\\Universal Print Server\\CEIPEnabled** を編集し、**DWORD** 値を **0** に設定します。

再度オプトインするには、DWORD値を1に設定します。

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

詳細については、Citrix Insight Servicesを参照してください。

Universal Print Serverを構成する

Universal Print Serverを構成するには、以下のCitrixポリシー設定を使用します。詳細については、画面上のポリシー設定ヘルプを参照してください。

- **Universal Print Serverを有効にする**。Universal Print Serverはデフォルトで無効になっています。Universal Print Serverを有効にすると、Universal Print Serverが利用できない場合にWindows Print Providerを使用するかどうかを選択します。Universal Print Serverを有効にすると、ユーザーはWindows Print ProviderおよびCitrix Providerインターフェイスを介してネットワークプリンターを追加および列挙できます。
- **Universal Print Server印刷データストリーム (CGP) ポート**。Universal Print Server印刷データストリームCGP (Common Gateway Protocol) リスナーが使用するTCPポート番号を指定します。デフォルトは**7229**です。
- **ユニバーサルプリントサーバー Webサービス (HTTP/SOAP) ポート**。Universal Print Serverリスナーが受信HTTP/SOAP要求に使用するTCPポート番号を指定します。デフォルトは**8080**です。

Citrix Virtual Apps and Desktops VDAへのUniversal Print Server通信のデフォルトポートであるHTTP 8080を変更するには、Universal Print Serverコンピューターで以下のレジストリを作成し、ポート番号の値を変更する必要があります。

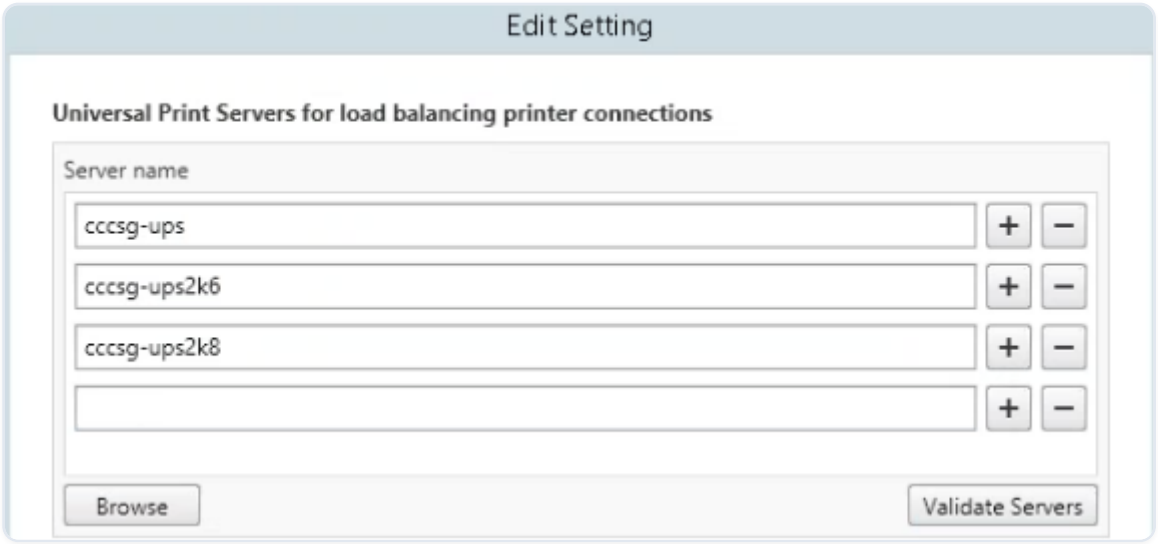
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies`

"UpsHttpPort"=DWORD:\<portnumber\>

このポート番号は、StudioのHDXポリシーであるUniversal Print Server Webサービス (HTTP/SOAP) ポートと一致している必要があります。

- **Universal Print Server印刷ストリーム入力帯域幅制限 (kbps)**。各印刷ジョブからCGPを使用してUniversal Print Serverに配信される印刷データの転送速度の上限 (キロビット/秒) を指定します。デフォルトは0 (無制限) です。
- **負荷分散用のUniversal Print Server**。この設定では、他のCitrix印刷ポリシー設定を評価した後、セッション起動時に確立されたプリンター接続の負荷分散に使用するUniversal Print

Serverを一覧表示します。プリンター作成時間を最適化するために、Citrixはすべての印刷サーバーが同じ共有プリンターのセットを持つことを推奨します。



- **Universal Print Serverサービス停止しきい値**。ロードバランサーが、利用できない印刷サーバーが回復するまで待機する時間を指定します。この時間を過ぎると、サーバーが永続的にオフラインであると判断され、その負荷が他の利用可能な印刷サーバーに再分散されます。デフォルトは180 (秒) です。

Delivery Controller™で印刷ポリシーが変更されると、ポリシーの変更がVDAに適用されるまでに数分かかる場合があります。

他のポリシー設定との相互作用 - Universal Print Serverは、他のCitrix印刷ポリシー設定を尊重し、以下の表に示すようにそれらと相互作用します。提供される情報は、Universal Print Serverポリシー設定が有効になっており、Universal Print Serverコンポーネントがインストールされ、ポリシー設定が適用されていることを前提としています。

ポリシー設定	**相互作用**
クライアントプリンターリダイレクト、クライアントプリンターの自動作成	Universal Print Serverが有効になると、クライアントネットワークプリンターはネイティブドライバーではなくUniversal Print Driverを使用して作成されます。ユーザーは以前と同じプリンター名を確認できます。
セッションプリンター	Citrix Universal Print Serverソリューションを使用する場合、ユニバーサルプリントドライバーのポリシー設定が適用されます。

プリントサーバーへの直接接続	Universal Print Serverが有効で、ユニバーサルプリントドライバーの使用ポリシー設定がユニバーサル印刷のみを使用するように構成されている場合、ユニバーサルプリントドライバーを使用して、プリントサーバーへの直接ネットワークプリンター接続を作成できます。
UPDの優先設定	EMFおよびXPSドライバーをサポートします。

ユーザーインターフェイスへの影響 - Universal Print Serverで使用されるCitrix Universal Print Driverは、以下のユーザーインターフェイスコントロールを無効にします。

- プリンターのプロパティダイアログボックスの「ローカルプリンター設定」ボタン
- ドキュメントのプロパティダイアログボックスの「ローカルプリンター設定」および「クライアントでプレビュー」ボタン

Citrix Universal Print Driver（EMFおよびXPSドライバー）は、ステープルや給紙元などの高度な印刷機能をサポートしています。セッション内でUPDにマップされているクライアントまたはネットワークプリンターがこれらの機能をサポートしている場合、ユーザーはカスタムUPD印刷ダイアログからステープルまたは給紙元のオプションを選択できます。

カスタムUPD印刷ダイアログ(/en-us/citrix-virtual-apps-desktops/2411/media/custom-upd-print-dialog.png)

ステープルやセキュアPINなどの非標準のプリンター設定を行うには、Citrix UPD EMFまたはXPSドライバーを使用するクライアントマッププリンターのカスタムUPD印刷ダイアログで**ローカル設定**を選択します。マップされたプリンターの**印刷設定**ダイアログがセッション外のクライアントに表示され、ユーザーは任意のプリンターオプションを変更できます。変更されたプリンター設定は、そのドキュメントを印刷する際にアクティブなセッションで使用されます。

これらの機能は、ネイティブドライバーがMicrosoft Print Capabilityテクノロジーを使用して利用可能にしている場合に利用できます。ネイティブドライバーは、Print Capabilities XMLで標準化されたPrint Schema Keywordsを使用する必要があります。非標準のキーワードが使用されている場合、Citrix Universal Print Driverを使用して高度な印刷機能を利用することはできません。

Universal Print Serverを使用する場合、Citrix Print Providerのプリンターの追加ウィザードは、Windows Print Providerのプリンターの追加ウィザードと同じですが、以下の例外があります。

- 名前またはアドレスでプリンターを追加する場合、プリントサーバーのHTTP/SOAPポート番号を指定できます。そのポート番号はプリンター名の一部となり、表示されます。
- Citrixユニバーサルプリンタードライバーの使用ポリシー設定でユニバーサル印刷を使用する必要があると指定されている場合、プリンターを選択する際に、ユニバーサルプリンタードライバー名が表示されます。Windows Print Providerはユニバーサルプリンタードライバーを使用できません。

Citrix Print Providerはクライアント側レンダリングをサポートしていません。

Universal Print Serverの詳細については、CTX200328を参照してください。

自動作成されたクライアントプリンター

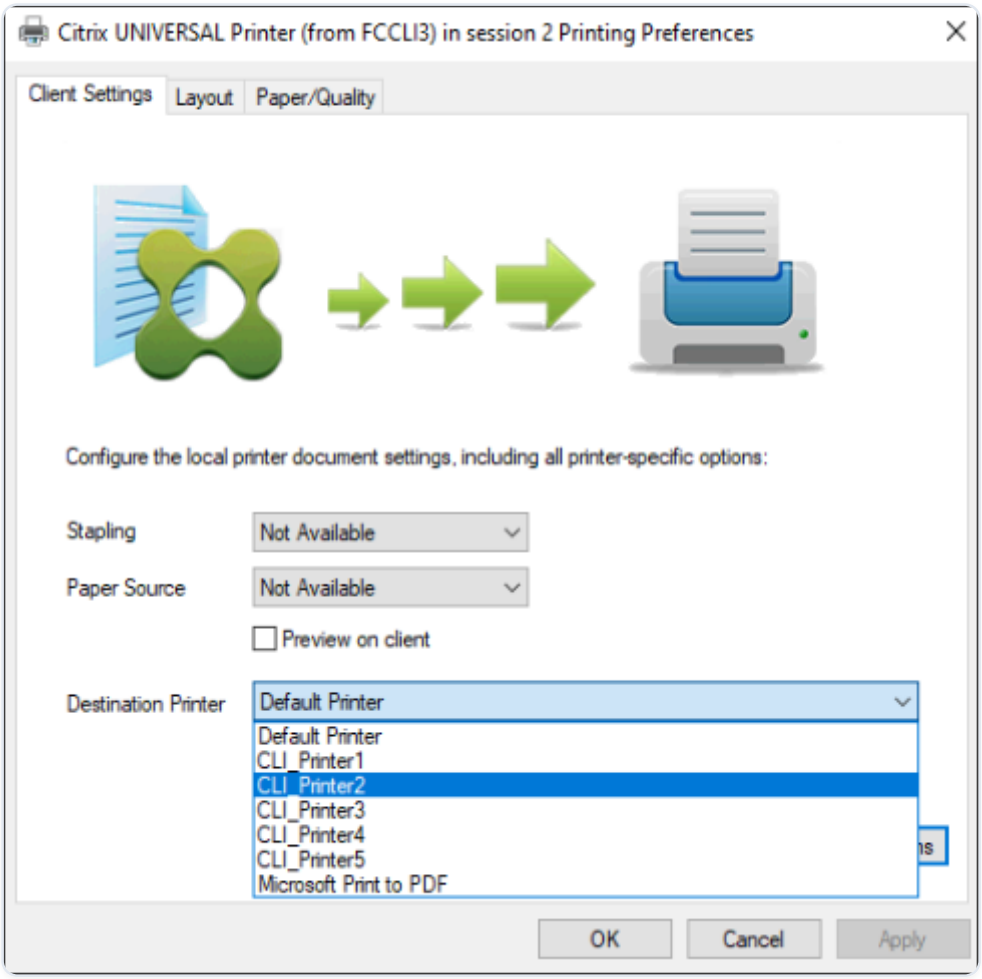
クライアントプリンターには、以下のユニバーサル印刷ソリューションが提供されます。

- **Citrix Universal Printer** - セッションの開始時に作成される汎用プリンターで、印刷デバイスに縛られません。Citrix Universal Printerのみを自動作成して使用すると、リソース使用量が削減され、ユーザーのサインイン時間が短縮される可能性があります。Universal Printerは、任意のクライアント側印刷デバイスに印刷できます。

  Citrix Universal Printerは、環境内のすべてのユーザーデバイスまたはCitrix Workspace™アプリで動作しない場合があります。Citrix Universal PrinterはWindows環境を必要とし、Citrix Offline Plug-inまたはクライアントにストリーミングされるアプリケーションをサポートしていません。このような環境では、自動作成されたクライアントプリンターとユニバーサルプリンタードライバーの使用を検討してください。

  非Windows版Citrix Workspaceアプリでユニバーサル印刷ソリューションを使用するには、PostscriptまたはPCLベースの他のユニバーサルプリンタードライバーのいずれかを使用してください。

  Citrix Universal Printerを使用すると、クライアントのデフォルトプリンターまたは特定のクライアントプリンターを印刷先として選択できます。印刷ジョブに特定のプリンターを選択するには、**Printing Preferences**ダイアログボックスを開きます。**Destination Printer**ドロップダウンを選択します。**Default Printer**オプションは、印刷ジョブをクライアントのデフォルトプリンターに送信します。セッションを実行しているエンドポイントに接続されているクライアントリダイレクトプリンターも一覧表示されます。選択したプリンターは、今後の印刷ジョブの宛先プリンターとして保存されます。



- **Citrix Universal Print Driver** - デバイスに依存しないプリンタードライバーです。Citrix Universal Print Driverを構成すると、システムはデフォルトでEMFベースのUniversal Print Driverを使用します。

  Citrix Universal Print Driverは、古いまたは高度でないプリンタードライバーよりも小さい印刷ジョブを作成する可能性があります。ただし、特殊なプリンターの印刷ジョブを最適化するには、デバイス固有のドライバーが必要になる場合があります。

ユニバーサル印刷の構成 - ユニバーサル印刷を構成するには、以下のCitrixポリシー設定を使用します。詳細については、画面上のポリシー設定ヘルプを参照してください。

- ユニバーサルプリンタードライバーの使用。ユニバーサル印刷を使用するタイミングを指定します。
- 汎用ユニバーサルプリンターの自動作成。ユニバーサル印刷と互換性のあるユーザーデバイスが使用されている場合に、セッション用の汎用Citrix Universal Printerオブジェクトの自動作成を有効または無効にします。デフォルトでは、汎用Universal Printerオブジェクトは自動作成されません。

- ユニバーサルドライバーの優先順位。システムがユニバーサルプリントドライバーを使用しようとする順序を、リストの最初のエントリから指定します。ドライバーの追加、編集、削除、およびリスト内のドライバーの順序変更が可能です。
- ユニバーサル印刷プレビューの優先順位。自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して印刷プレビュー機能を使用するかどうかを指定します。
- ユニバーサル印刷EMF処理モード。Windowsユーザーデバイス上のEMFスプールファイルの処理方法を制御します。デフォルトでは、EMFレコードはプリンターに直接スプールされます。プリンターに直接スプールすることで、スプーラーはレコードをより速く処理し、CPUリソースの使用量を削減できます。

その他のポリシーについては、「印刷パフォーマンスの最適化」を参照してください。用紙サイズ、印刷品質、色、両面印刷、部数などの設定のデフォルトを変更するには、「CTX113148」を参照してください。

ユーザーデバイスからのプリンターの自動作成 - セッションの開始時に、システムはデフォルトでユーザーデバイス上のすべてのプリンターを自動作成します。ユーザーにプロビジョニングされるプリンターの種類を制御したり、自動作成を防止したりできます。

Citrixポリシー設定 クライアントプリンターの自動作成を使用して、自動作成を制御します。次のように指定できます。

- ネットワークプリンターとローカル接続プリンターを含む、ユーザーデバイスに表示されるすべてのプリンターが、各セッションの開始時に自動的に作成される（デフォルト）
- ユーザーデバイスに物理的に接続されているすべてのローカルプリンターが自動的に作成される
- ユーザーデバイスのデフォルトプリンターのみが自動的に作成される
- すべてのクライアントプリンターで自動作成が無効になる

「クライアントプリンターの自動作成」設定では、「クライアントプリンターのリダイレクト」設定が「許可」（デフォルト）である必要があります。

ユーザーへのネットワークプリンターの割り当て

デフォルトでは、ユーザーデバイス上のネットワークプリンターはセッションの開始時に自動的に作成されます。システムでは、各セッション内で作成するネットワークプリンターを指定することで、列挙およびマップされるネットワークプリンターの数を減らすことができます。このようなプリンターはセッションプリンターと呼ばれます。

IPアドレスでセッションプリンターポリシーをフィルター処理して、近接印刷を提供できます。近接印刷により、指定されたIPアドレス範囲内のユーザーは、その同じ範囲内に存在するネットワーク印刷デバイスに自動的にアクセスできます。近接印刷はCitrix Universal Print Serverによって提供され、このセクションで説明されている構成は必要ありません。

近接印刷には、次のシナリオが含まれる場合があります。

- 会社の内部ネットワークは、DHCPサーバーによって運用されており、ユーザーにIPアドレスを自動的に割り当てます。
- 社内のすべての部署には、一意に割り当てられたIPアドレス範囲があります。
- 各部署のIPアドレス範囲内にネットワークプリンターが存在します。

近接印刷が構成されており、従業員がある部署から別の部署に移動した場合、追加の印刷デバイス構成は不要です。ユーザーデバイスが新しい部署のIPアドレス範囲内で認識されると、その範囲内のすべてのネットワークプリンターにアクセスできるようになります。

セッションでリダイレクトする特定のプリンターを構成する - 管理者によって割り当てられたプリンターを作成するには、Citrixポリシー設定の「セッションプリンター」を構成します。次のいずれかの方法を使用して、そのポリシーにネットワークプリンターを追加します。

- `\\servername\printername`の形式を使用して、プリンターのUNCパスを入力します。
- ネットワーク上のプリンターの場所を参照します。
- 特定のサーバー上のプリンターを参照します。サーバー名を「\\servername」の形式で入力し、「参照」をクリックします。

重要: サーバーは、適用されているすべてのポリシーの有効なセッションプリンター設定を、最も高い優先度から最も低い優先度までマージします。複数のポリシーオブジェクトでプリンターが構成されている場合、カスタムのデフォルト設定は、そのプリンターが構成されている最も優先度の高いポリシーオブジェクトからのみ取得されます。

セッションプリンター設定で作成されたネットワークプリンターは、サブネットなどのオブジェクトでフィルタリングすることにより、セッションが開始された場所に応じて異なる場合があります。

セッションのデフォルトのネットワークプリンターを指定する - デフォルトでは、ユーザーのメインプリンターがセッションのデフォルトプリンターとして使用されます。Citrixポリシー設定の「デフォルトプリンター」を使用して、セッションでユーザーデバイスのデフォルトプリンターがどのように確立されるかを変更します。

1. 「デフォルトプリンター設定」ページで、「クライアントのデフォルトプリンターを選択」の設定を選択します。

    - ネットワークプリンター名。セッションプリンターポリシー設定で追加されたプリンターがこのメニューに表示されます。このポリシーのデフォルトとして使用するネットワークプリンターを選択します。
    - ユーザーのデフォルトプリンターを調整しない。デフォルトプリンターには、現在のターミナルサービスまたはWindowsユーザープロファイル設定を使用します。詳細については、画面上のポリシー設定ヘルプを参照してください。

2. 影響を与えたいユーザーグループ（またはその他のフィルターされたオブジェクト）にポリシーを適用します。

近接印刷の構成 - 近接印刷はCitrix Universal Print Serverによっても提供され、ここに記載されている構成は必要ありません。

1. 各サブネットに対して個別のポリシーを作成します（またはプリンターの場所に合わせる）。
2. 各ポリシーで、そのサブネットの地理的な場所にあるプリンターをセッションプリンター設定に追加します。
3. デフォルトプリンター設定を「ユーザーのデフォルトプリンターを調整しない」に設定します。
4. クライアントIPアドレスでポリシーをフィルターします。DHCP IPアドレス範囲の変更を反映するように、これらのポリシーを必ず更新してください。

印刷環境の維持

印刷環境の維持には以下が含まれます。

- プリンタードライバーの管理
- 印刷パフォーマンスの最適化
- プリンターの表示と印刷キューの管理

プリンタードライバーの管理

管理オーバーヘッドと印刷ドライバーの問題の可能性を最小限に抑えるため、Citrix は Citrix Universal™ 印刷ドライバーの使用を推奨します。

自動作成が失敗した場合、既定では、システムは Windows に付属の Windows ネイティブプリンタードライバーをインストールします。ドライバーが利用できない場合、システムは Universal 印

刷ドライバーにフォールバックします。プリンタードライバーの既定値の詳細については、ベストプラクティス、セキュリティに関する考慮事項、および既定の操作を参照してください。

Citrix Universal 印刷ドライバーがすべてのシナリオで選択肢とならない場合、Multi-session OS マシンにインストールされるドライバーの量を最小限に抑えるために、プリンタードライバーをマッピングします。さらに、プリンタードライバーをマッピングすることで、次のことが可能になります。

- 指定されたプリンターが Citrix Universal 印刷ドライバーのみを使用できるようにする
- 指定されたドライバーでプリンターが作成されることを許可または防止する
- 古くなったドライバーや破損したドライバーを適切なプリンタードライバーに置き換える
- クライアントドライバー名に対して、Windows サーバーで利用可能なドライバーを置き換える

プリンタードライバーの自動インストールを防止する - Multi-session OS マシン全体で一貫性を確保するために、印刷ドライバーの自動インストールを無効にする必要があります。これは、Citrix® ポリシー、Microsoft ポリシー、またはその両方を通じて実現できます。Windows ネイティブプリンタードライバーの自動インストールを防止するには、Citrix ポリシー設定「インボックスプリンタードライバーの自動インストール」を無効にします。

クライアントプリンタードライバーをマッピングする - 各クライアントは、ログオン時にプリンタードライバー名を含むクライアント側のプリンターに関する情報を提供します。クライアントプリンターの自動作成中、クライアントによって提供されるプリンターモデル名に対応するWindowsサーバーのプリンタードライバー名が選択されます。その後、自動作成プロセスは、識別された利用可能なプリンタードライバーを使用して、リダイレクトされたクライアント印刷キューを構築します。

マップされたクライアントプリンタードライバーのドライバー置換ルールを定義し、印刷設定を編集するための一般的なプロセスは次のとおりです。

1. 自動作成されたクライアントプリンターのドライバー置換ルールを指定するには、Citrixポリシー設定の「Printer driver mapping and compatibility」を構成します。これには、クライアントプリンタードライバー名を追加し、「Find printer driver」メニューから、そのクライアントプリンタードライバーの代わりに適用するサーバードライバーを選択します。この設定ではワイルドカードを使用できます。たとえば、すべてのHPプリンターに特定のドライバーを使用させるには、ポリシー設定で「HP*」と指定します。
2. プリンタードライバーを禁止するには、ドライバー名を選択し、「Do not create」設定を選択します。
3. 必要に応じて、既存のマッピングを編集したり、マッピングを削除したり、リスト内のドライバーエントリの順序を変更したりします。

4. マップされたクライアントプリンタードライバーの印刷設定を編集するには、プリンタードライバーを選択し、「設定」をクリックして、印刷品質、向き、色などの設定を指定します。プリンタードライバーがサポートしない印刷オプションを指定した場合、そのオプションは無効になります。この設定は、ユーザーが以前のセッションで設定した保持されているプリンター設定を上書きします。
5. 特定のドライバーでのみ利用可能なプリンター機能もあるため、Citrixではドライバーをマッピングした後、プリンターの動作を詳細にテストすることをお勧めします。

ユーザーがログオンすると、システムはクライアントプリンターを設定する前に、クライアントプリンタードライバーの互換性リストをチェックします。

印刷パフォーマンスの最適化

印刷パフォーマンスを最適化するには、Universal Print ServerとUniversal Print Driverを使用します。以下のポリシーは、印刷の最適化と圧縮を制御します。

- ユニバーサル印刷の最適化のデフォルト。セッション用にユニバーサルプリンターが作成される際のデフォルト設定を指定します。
    - 希望する画質は、ユニバーサル印刷に適用されるデフォルトの画像圧縮制限を指定します。デフォルトでは、標準品質が有効になっており、ユーザーは標準または低品質の圧縮を使用してのみ画像を印刷できます。
    - ヘビーウェイト圧縮を有効にするは、希望する画質で設定された圧縮レベルを超えて帯域幅を削減するかどうかを有効または無効にします。これにより、画質が低下することはありません。デフォルトでは、ヘビーウェイト圧縮は無効になっています。
    - 画像とフォントのキャッシュ設定は、印刷ストリームに複数回出現する画像とフォントをキャッシュするかどうかを指定し、各固有の画像またはフォントがプリンターに一度だけ送信されるようにします。デフォルトでは、埋め込み画像とフォントはキャッシュされます。
    - 管理者以外のユーザーによるこれらの設定の変更を許可するは、ユーザーがセッション内でデフォルトの印刷最適化設定を変更できるかどうかを指定します。デフォルトでは、ユーザーはデフォルトの印刷最適化設定を変更できません。
- ユニバーサル印刷の画像圧縮制限。ユニバーサルプリントドライバーで印刷される画像に利用可能な最大品質と最小圧縮レベルを定義します。デフォルトでは、画像圧縮制限は最高品質（ロスレス圧縮）に設定されます。
- ユニバーサル印刷の印刷品質制限。セッションで印刷出力を生成するために利用できる最大ドット/インチ (dpi) を指定します。デフォルトでは、制限は指定されていません。

デフォルトでは、ネットワークプリンター宛てのすべての印刷ジョブは、マルチセッションOSマシンからネットワーク経由で直接印刷サーバーにルーティングされます。ネットワークにかなりの遅延や帯域幅の制限がある場合は、ICA®接続経由で印刷ジョブをルーティングすることを検討してください。そのためには、Citrixポリシー設定「印刷サーバーへの直接接続」を無効にします。ICA接続経由で送信されるデータは圧縮されるため、WANを介してデータが転送される際に消費される帯域幅が少なくなります。

印刷帯域幅を制限してセッションパフォーマンスを向上させる - マルチセッションOSマシンからユーザープリンターにファイルを印刷している間、特にユーザーが低速ネットワーク経由でサーバーにアクセスしている場合、帯域幅の競合により、他の仮想チャネル（ビデオなど）のパフォーマンスが低下する可能性があります。このような劣化を防ぐために、ユーザー印刷で使用される帯域幅を制限できます。印刷のデータ転送速度を制限することで、HDX™データストリーム内でビデオ、キーストローク、マウスデータの転送により多くの帯域幅を利用できるようになります。

> **重要:**
>
> プリンターの帯域幅制限は、他のチャネルが使用されていない場合でも常に適用されます。

> 印刷帯域幅セッション制限を構成するには、以下のCitrixポリシーの帯域幅プリンター設定を使用します。サイトの制限を設定するには、Studioを使用してこのタスクを実行します。
> 個々のサーバーの制限を設定するには、各マルチセッションOSマシンでWindowsのグループポリシー管理コンソールを使用してこのタスクを実行します。

- 「プリンターリダイレクト帯域幅制限」設定は、印刷に利用できる帯域幅をキロビット/秒 (kbps) で指定します。
- 「プリンターリダイレクト帯域幅制限（パーセント）」設定は、印刷に利用できる帯域幅を、利用可能な全体帯域幅のパーセンテージに制限します。

  注：「プリンターリダイレクト帯域幅制限（パーセント）」設定を使用して帯域幅をパーセンテージで指定するには、「セッション全体の帯域幅制限」も有効にする必要があります。

  両方の設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

印刷帯域幅に関するリアルタイム情報を取得するには、Citrix Directorを使用します。

ユニバーサルプリントサーバーの負荷分散

ユニバーサル印刷サーバーソリューションは、負荷分散ソリューションに印刷サーバーを追加することで拡張できます。各VDAには独自のロードバランサーがあり、印刷負荷をすべての印刷サーバーに分散するため、単一障害点はありません。

負荷分散ソリューション内のすべての印刷サーバーに印刷負荷を分散するには、ポリシー設定のUniversal Print Servers for load balancingとUniversal Print Servers out-of-service thresholdを使用します。

印刷サーバーに予期せぬ障害が発生した場合、各VDAのロードバランサーのフェイルオーバーメカニズムは、障害が発生した印刷サーバーに割り当てられていたプリンター接続を他の利用可能な印刷サーバーに自動的に再分散します。これにより、既存および新規のすべてのセッションがユーザーエクスペリエンスに影響を与えることなく、また管理者の即時介入を必要とせずに正常に機能します。

管理者は、一連のパフォーマンスカウンターを使用して、VDA上でロードバランスされたプリントサーバーのアクティビティを監視できます。

- VDA上のロードバランスされたプリントサーバーのリストとその状態（利用可能、利用不可）
- 各プリントサーバーによって受け入れられたプリンター接続数
- 各プリントサーバーで失敗したプリンター接続数
- 各プリントサーバー上のアクティブなプリンター接続数
- 各プリントサーバー上の保留中のプリンター接続数

印刷キューの表示と管理

次の表は、環境内でプリンターを表示し、印刷キューを管理できる場所をまとめたものです。

	印刷経路	場所
クライアントプリンター（ユーザーデバイスに接続されたプリンター）	クライアント印刷経路	UAC有効時: Microsoft Management Consoleにある印刷の管理スナップイン; UAC無効時: Windows 8より前: コントロールパネル, Windows 8: 印刷の管理スナップイン

	印刷経路	場所
ネットワークプリンター（ネットワークプリントサーバー上のプリンター）	ネットワーク印刷経路	UAC有効時: 印刷サーバー \> Microsoft Management Consoleにある印刷の管理スナップイン; UAC無効時: 印刷サーバー \> コントロールパネル
ネットワークプリンター (ネットワーク印刷サーバー上のプリンター)	クライアント印刷経路	UAC有効時: 印刷サーバー \> Microsoft Management Consoleにある印刷の管理スナップイン; UAC無効時: Windows 8より前: コントロールパネル, Windows 8: 印刷の管理スナップイン
ローカルネットワークサーバープリンター (マルチセッションOSマシンに追加されたネットワーク印刷サーバーからのプリンター)	ネットワーク印刷経路	UAC有効時: 印刷サーバー \> コントロールパネル; UAC無効時: 印刷サーバー \> コントロールパネル

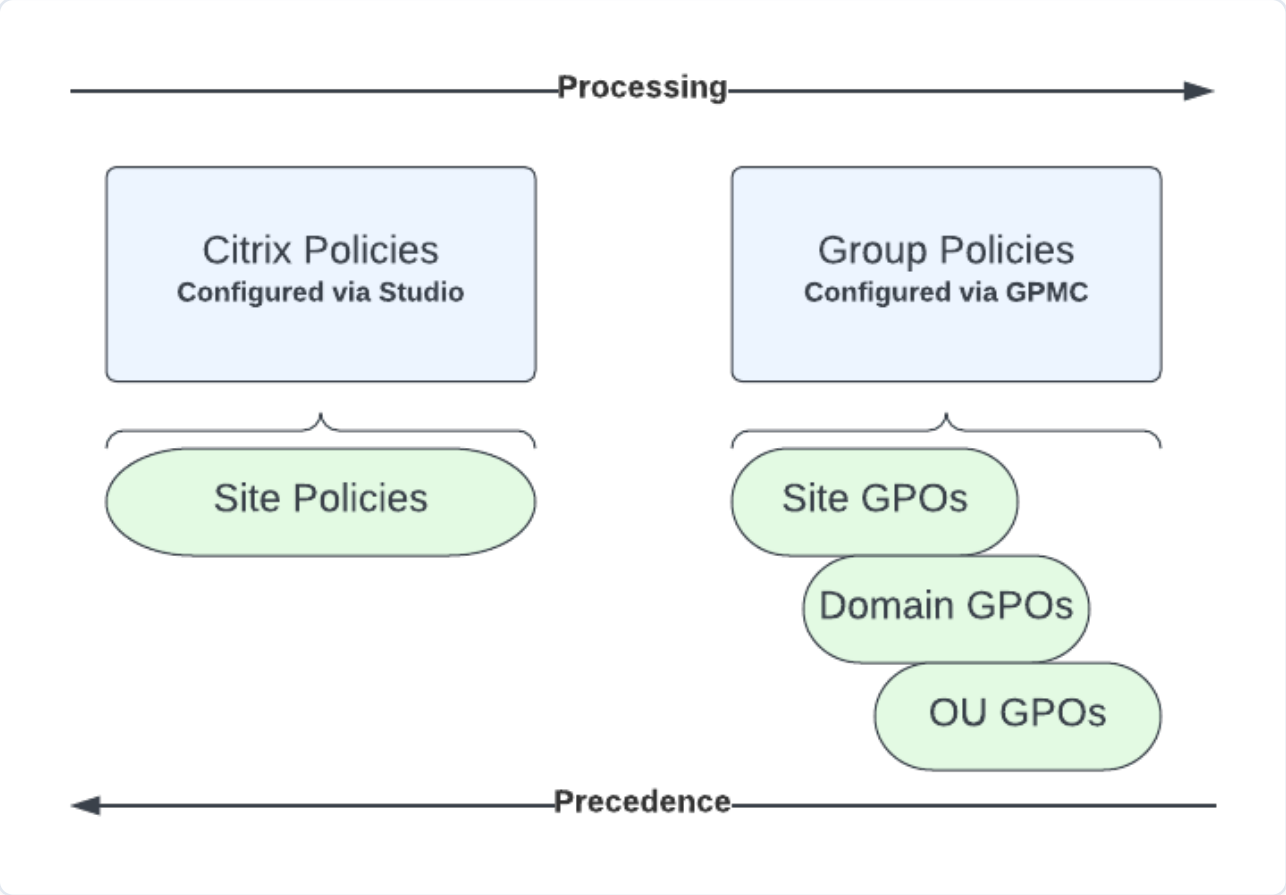
注:

ネットワーク印刷経路を使用するネットワークプリンターの印刷キューはプライベートであり、システムを通じて管理できません。

ポリシー

ポリシーとは、ユーザー、デバイス、または接続タイプのグループに対して、セッション、帯域幅、セキュリティがどのように管理されるかを定義する設定の集合です。

ポリシー設定は、物理マシンおよび仮想マシン、またはユーザーに適用できます。設定は、ローカルレベルの個々のユーザー、またはActive Directoryのセキュリティグループに適用できます。構成は特定の基準とルールを定義します。ポリシーを明示的に割り当てない場合、設定はすべての接続に適用されます。



ポリシーはネットワークの異なるレベルに適用できます。組織単位GPOレベルに配置されたポリシー設定は、ネットワーク上で最も高い優先順位を持ちます。ドメインGPOレベルのポリシーは、サイトグループポリシーオブジェクトレベルのポリシーを上書きします。サイトグループポリシーオブジェクトレベルは、MicrosoftおよびCitrixローカルポリシーレベルの両方における競合するポリシーを上書きします。

すべてのCitrixローカルポリシーは、Web Studioコンソールで作成および管理され、サイトデータベースに保存されます。グループポリシーは、Microsoftグループポリシー管理コンソール (GPMC) を使用して作成および管理され、Active Directoryに保存されます。Microsoftローカルポリシーは、Windowsオペレーティングシステムで作成され、レジストリに保存されます。

Studioはモデリングウィザードを使用して、管理者がテンプレートとポリシー内の構成設定を比較し、競合する設定や冗長な設定を排除するのに役立ちます。管理者はGPMCを使用してGPOを設定し、設定を構成できます。また、それらをネットワークの異なるレベルのターゲットユーザーセットに適用することもできます。

これらのGPOはActive Directoryに保存されます。これらの設定の管理へのアクセスは、セキュリティ上の理由からほとんどのIT担当者に対して制限されています。

設定は、優先度とその条件に従ってマージされます。無効な設定は、下位の有効な設定を上書きします。未構成のポリシー設定は無視され、下位の設定を上書きしません。

ローカルポリシーは、Active Directoryのグループポリシーと競合する可能性もあり、状況によっては互いに上書きし合う可能性があります。

すべてのポリシーは次の順序で処理されます。

1. エンドユーザーはドメイン資格情報を使用してマシンにログオンします。
2. 資格情報はドメインコントローラーに送信されます。
3. Active Directoryはすべてのポリシー (エンドユーザー、エンドポイント、組織単位、ドメイン) を適用します。
4. エンドユーザーはCitrix Workspace™アプリにログオンし、アプリケーションまたはデスクトップにアクセスします。
5. CitrixおよびMicrosoftのポリシーは、エンドユーザーおよびリソースをホストするマシンに対して処理されます。
6. Active Directoryは、ポリシー設定の優先順位を決定します。その後、それらをエンドポイントデバイスのレジストリと、リソースをホストするマシンに適用します。
7. エンドユーザーがリソースからログオフします。エンドユーザーおよびエンドポイントデバイスに対するCitrixポリシーは、アクティブではなくなります。
8. エンドユーザーがユーザーデバイスからログオフすると、GPOユーザーポリシーが解放されます。
9. エンドユーザーがデバイスの電源を切ると、GPOマシンポリシーが解放されます。

ユーザー、デバイス、およびマシンのグループに対してポリシーを作成する場合、一部のメンバーは異なる要件を持つ可能性があり、一部のポリシー設定に対して例外が必要になる場合があります。例外は、ポリシーが誰または何に影響するかを決定するStudioおよびGPMCのフィルターによって作成されます。

> **注:**
>
> 同じGPOでWindowsポリシーとCitrixポリシーを混在させることはサポートしていません。

ポリシーの操作

> **注:**
>
> Citrix Virtual Apps and Desktops™展開は、Web Studio (Webベース) とCitrix Studio (Windowsベース) の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の対応する記事を参照してください。

ユーザーアクセスとセッション環境を制御するためにCitrixポリシーを構成します。Citrixポリシーは、接続、セキュリティ、帯域幅の設定を制御する最も効率的な方法です。特定のユーザーグループ、デバイス、または接続タイプに対してポリシーを作成できます。各ポリシーには複数の設定を含めることができます。

Citrixポリシーを操作するためのツール

Citrixポリシーでは、以下のツールを使用できます。

- **Web Studio。** グループポリシーを管理する権限のないCitrix管理者の場合は、Web Studioを使用してサイトのポリシーを作成します。Web Studioを使用して作成されたポリシーはサイトデータベースに保存され、更新はVDAがブローカーに登録されたとき、またはユーザーがそのVDAに接続したときにVDAにプッシュされます。
- **ローカルグループポリシーエディター** (Microsoft管理コンソールスナップイン)。ネットワーク環境でActive Directoryを使用しており、グループポリシーを管理する権限がある場合は、ローカルグループポリシーエディターを使用してサイトのポリシーを作成できます。構成した設定は、グループポリシー管理コンソールで指定したグループポリシーオブジェクト (GPO) に影響します。

重要:

一部のポリシー設定を構成するには、ローカルグループポリシーエディターを使用することをお勧めします。例としては、VDAをコントローラーに登録する設定や、Microsoft App-Vサーバーに関連する設定などがあります。 追加のポリシー検証が追加されます。その結果、無効なポリシー設定が存在する場合、インプレースアップグレードを行うとポリシーデータが失われる可能性があります。Web Studio以外の方法でポリシーを作成または編集する場合は、最新バージョンのSDKとスナップインを使用することをお勧めします。

ポリシーの処理順序と優先順位

グループポリシー設定は、次の順序で処理されます。

1. ローカルGPO
2. Virtual Apps and DesktopsサイトGPO (サイトデータベースに保存)
3. サイトレベルGPO
4. ドメインレベルGPO
5. 組織単位

ただし、競合が発生した場合、最後に処理されたポリシー設定が以前に処理された設定を上書きします。ポリシー設定の優先順位は次のとおりです。

1. 組織単位
2. ドメインレベルGPO
3. サイトレベルGPO
4. Virtual Apps and DesktopsサイトGPO（サイトデータベースに保存）
5. ローカルGPO

例えば、Citrix管理者はWeb Studioを使用して、会社の営業担当者向けにクライアントファイルリダイレクトを有効にするポリシー（ポリシーA）を作成します。一方、別の管理者はグループポリシーエディターを使用して、営業担当者向けにクライアントファイルリダイレクトを無効にするポリシー（ポリシーB）を作成します。営業担当者が仮想デスクトップにログオンすると、ポリシーBが適用され、ポリシーAは無視されます。その理由は、ポリシーBがドメインレベルで処理され、ポリシーAがVirtual Apps and DesktopsサイトGPOレベルで処理されたためです。

ただし、ユーザーがICA®またはリモートデスクトッププロトコル（RDP）セッションを起動すると、Citrixセッション設定は、Active Directoryポリシーで構成された、またはリモートデスクトップセッションホスト構成を使用して構成された同じ設定を上書きします。この設定には、一般的なRDPクライアント接続設定に関連する設定が含まれます。RDPクライアント接続設定の例としては、デスクトップの壁紙、メニューアニメーション、ドラッグ中のウィンドウコンテンツの表示などがあります。

複数のポリシーを使用する場合、競合する設定を含むポリシーに優先順位を付けることができます。詳しくは、「ポリシーの比較、優先順位付け、モデル化、トラブルシューティング」を参照してください。

Citrixポリシーのワークフロー

ポリシーを構成するプロセスは次のとおりです。

1. ポリシーを作成します。
2. ポリシー設定を構成します。
3. ポリシーをマシンオブジェクトとユーザーオブジェクトに割り当てます。
4. ポリシーに優先順位を付けます。
5. Citrixグループポリシーモデリングウィザードを実行して、有効なポリシーを確認します。

> **注:**
>
> Citrixグループポリシーモデリングウィザードを開くには、**［ポリシー］>［モデリング］**タブに移動し、アクションバーで［モデリングウィザードの起動］をクリックします。［モデリング］**タブは、お客様の要望に応じてWeb Studioで利用できます。

Citrixポリシーと設定のナビゲート

ローカルグループポリシーエディターでは、ポリシーと設定は「コンピューターの構成」と「ユーザーの構成」の2つのカテゴリに表示されます。各カテゴリにはCitrixポリシーノードがあります。このスナップインのナビゲートと使用の詳細については、Microsoftのドキュメントを参照してください。

Web Studioでは、ポリシー設定は、影響を与える機能または特徴に基づいてカテゴリに分類されます。たとえば、**［プロファイル管理］**セクションには、プロファイル管理のポリシー設定が含まれています。

- コンピューター設定（マシンに適用されるポリシー設定）は、仮想デスクトップの動作を定義し、仮想デスクトップの起動時に適用されます。これらの設定は、仮想デスクトップでアクティブなユーザーセッションがない場合でも適用されます。
- ユーザー設定は、ICAを使用して接続する際のユーザーエクスペリエンスを定義します。ユーザーポリシーは、ユーザーがICAを使用して接続または再接続するときに適用されます。ユーザーがRDPを使用して接続したり、コンソールに直接ログオンしたりする場合は、ユーザーポリシーは適用されません。

  ポリシー、設定、またはテンプレートにアクセスするには、Web Studioの左ペインで**［ポリシー］**を選択します。

  - **［ポリシー］**タブにはすべてのポリシーが一覧表示されます。ポリシーを選択すると、下部に次のタブが表示されます。
    - 概要 - 名前、優先度、有効/無効の状態、および説明を一覧表示
    - 設定 - 構成されているすべての設定を一覧表示
    - 割り当て先 - ポリシーが割り当てられているユーザーオブジェクトとマシンオブジェクトを一覧表示します。 詳しくは、「ポリシーの作成」を参照してください。
  - 「**テンプレート**」タブには、作成したCitrix提供のテンプレートとカスタムテンプレートが一覧表示されます。テンプレートを選択すると、下部にタブが表示されます。
    - 説明 (テンプレートを使用する理由)
    - 設定 (構成された設定のリスト)。詳細については、「ポリシーテンプレート」を参照してください。
  - 「**比較**」タブでは、ポリシーまたはテンプレートの設定を、他のポリシーまたはテンプレートの設定と比較できます。たとえば、ベストプラクティスへの準拠を確実にするために、設定値を検証したい場合があります。詳細については、「ポリシーの比較、優先順位付け、モデル化、トラブルシューティング」を参照してください。

  ポリシーまたはテンプレートで設定を検索するには：

  a. ポリシーまたはテンプレートを選択します。
  b. アクションバーで**ポリシーの編集**または**テンプレートの編集**を選択します。
  c. **設定**ページで、**検索**フィールドに設定の名前を入力します。

     検索を絞り込むには、以下を選択します。

     - 特定の製品バージョン

    - カテゴリ（例：帯域幅）
    - 設定名に含まれるキーワード
    - **選択済みのみ表示**チェックボックス
    - 選択したポリシーに追加された設定のみを検索する場合。

  フィルターなしで検索するには、**すべての設定**を選択します。

- ポリシー内の設定を検索するには：

  a. ポリシーを選択します。

  b. **設定**タブを選択し、設定名を入力します。

特定の製品バージョンを選択するか、カテゴリを選択することで検索を絞り込むことができます。フィルターなしで検索するには、**すべての設定**を選択します。

ポリシーは、一度作成されると、使用されたテンプレートとは独立します。新しいポリシーの**説明**フィールドを使用して、使用されたソーステンプレートを追跡できます。

グループポリシーエディターでは、コンピューター設定とユーザー設定は、両方の種類の設定を含むテンプレートから作成された場合でも、個別に適用する必要があります。この例では、コンピューターの構成で「非常に高精細なユーザーエクスペリエンス」を使用することを選択しています。

- レガシーグラフィックモードは、このテンプレートから作成されたポリシーで使用されるコンピューター設定です。
- グレー表示されているユーザー設定は、このテンプレートから作成されたポリシーでは使用されません。

ローカルグループポリシーエディター(/en-us/citrix-virtual-apps-desktops/2411/media/group-policy-editor-template-example.png)

ポリシーテンプレート

> **注:**
>
> Citrix Virtual Apps and Desktops™展開は、Web Studio (Webベース) と Citrix Studio (Windowsベース) の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> テンプレートは、特定の成果を達成するためのポリシー作成に使用することが推奨される設定の集合です。たとえば、エンドユーザーに高精細なユーザーエクスペリエンスを提供するためのポリシーを作成する場合、Very High Definition User Experienceテンプレートで定義されている設定を、そのようなポリシーを作成するための参照点および開始点として使用できます。

テンプレートはポリシーではありません。テンプレートはCitrixポリシー設定の補足ドキュメントです。これらは、特定のユーザー関連設定の集合的な機能を示します。

テンプレートの使用は任意です。管理者はテンプレートを使用せずにポリシーを作成できます。テンプレートは、サイトをどのように構成すべきかについて大まかなアイデアは持っているものの、目的の構成を達成するためにどの設定を使用すべきか確信が持てない管理者にとって役立ちます。

管理者は、既存のテンプレート、既存のポリシー、またはゼロからテンプレートを作成できます。

ADMX/ADML

ここで説明するCitrixグループポリシーテンプレートは、Windowsポリシーテンプレートとは関係ありません。ここで説明するテンプレートとWindowsポリシーテンプレートは、2つの異なる概念です。CitrixグループポリシーテンプレートはADMXファイルではありません。

組み込みのCitrixテンプレート

次のポリシーテンプレートが利用可能です。

- **Very High Definition User Experience**。このテンプレートは、ユーザーエクスペリエンスを最大化するデフォルト設定を適用します。複数のポリシーが優先順位に従って処理されるシナリオでこのテンプレートを使用します。
- **High Server Scalability**。このテンプレートを適用して、サーバーリソースを節約します。このテンプレートは、ユーザーエクスペリエンスとサーバーのスケーラビリティのバランスを取ります。単一サーバーでホストできるユーザー数を増やしながら、優れたユーザーエクスペリエンスを提供します。このテンプレートは、グラフィックの圧縮にビデオコーデックを使用せず、サーバー側のマルチメディアレンダリングを防止します。
- **High Server Scalability-Legacy OS**。このHigh Server Scalabilityテンプレートは、Windows Server 2008 R2またはWindows 7以前を実行しているVDAにのみ適用されます。このテンプレートは、これらのオペレーティングシステムにより効率的なレガシーグラフィックモードに依存しています。

- **NetScaler SD-WAN向けに最適化**。Citrix Virtual Desktopsの配信を最適化するために、NetScaler SD-WANを使用している支社から作業するユーザーにこのテンプレートを適用します。(NetScaler SD-WANはCloudBridgeの新しい名称です)。
- **WAN向けに最適化**。このテンプレートは、共有WAN接続を使用するブランチオフィスのタスクワーカーや、グラフィックがシンプルでマルチメディアコンテンツが少ないユーザーインターフェイスを持つアプリケーションにアクセスする低帯域幅接続のリモートロケーション向けです。このテンプレートは、ビデオ再生エクスペリエンスと一部のサーバー拡張性を犠牲にして、帯域幅効率を最適化します。
- **WAN向け最適化 - レガシーOS**。この*WAN向け最適化*テンプレートは、Windows Server 2008 R2またはWindows 7以前を実行しているVDAにのみ適用されます。このテンプレートは、これらのオペレーティングシステムにより効率的なレガシーグラフィックモードに依存しています。
- **セキュリティと制御**。このテンプレートは、リスク許容度が低い環境で使用し、Citrix Virtual Apps and Desktopsでデフォルトで有効になっている機能を最小限に抑えます。このテンプレートには、ユーザーデバイスでの印刷、クリップボード、周辺機器、ドライブマッピング、ポートリダイレクト、Flashアクセラレーションへのアクセスを無効にする設定が含まれています。このテンプレートを適用すると、より多くの帯域幅を使用し、サーバーあたりのユーザー密度を低下させる可能性があります。

組み込みのCitrixテンプレートをデフォルト設定で使用することをお勧めしますが、特定の推奨値がない設定もあります。たとえば、WAN向け最適化テンプレートに含まれる**セッション全体の帯域幅制限**などです。この場合、管理者がこの設定がシナリオに適用される可能性が高いことを理解できるように、テンプレートが設定を公開しています。

テンプレートのデフォルト設定画像(/en-us/citrix-virtual-apps-desktops/2411/media/template-default-settings.png)

XenAppおよびXenDesktop 7.6 FP3より前の展開（ポリシー管理およびVDA）を使用しており、高サーバー拡張性およびWAN向け最適化テンプレートが必要な場合は、該当する場合にこれらのテンプレートのレガシーOSバージョンを使用してください。

> **注:**
>
> Citrixは組み込みテンプレートを作成および更新します。これらのテンプレートは変更または削除できません。

Web Studioを使用したテンプレートの作成と管理

テンプレートに基づいてテンプレートを作成するには:

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。
2. **テンプレート**タブを選択し、テンプレートを作成する元のテンプレートを選択します。
3. **テンプレートの作成**タブを選択します。**設定の選択**画面が表示されます。
4. テンプレートに含めるポリシー設定を選択して構成します。
5. 「**次へ**」をクリックします。「**概要**」画面が表示されます。
6. テンプレートの名前を入力します。
7. **完了**をクリックします。新しいテンプレートが**テンプレート**タブに表示されます。

ポリシーに基づいてテンプレートを作成するには：

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。
2. **ポリシー**タブを選択し、テンプレートを作成する元のポリシーを選択します。
3. **その他**タブをクリックします。
4. 「**テンプレートとして保存**」を選択します。「**設定の選択**」画面が表示されます。
5. テンプレートに含める新しいポリシー設定を選択して構成します。
6. 「**次へ**」をクリックします。「**概要**」画面が表示されます。
7. テンプレートの名前と説明を入力し、「**完了**」をクリックします。

テンプレートと委任管理

Web Studioのテンプレートはサイトデータベースに保存されますが、Citrix Studioのテンプレートは現在の管理者のユーザープロファイルフォルダーに`.gpt`拡張子を持つファイルとして保存されます。ある管理者が作成したCitrix Studioテンプレートは、他の管理者や、別のマシン上の同じ管理者には表示されません。Web Studioテンプレートは、権限と委任管理の対象となるすべての管理者から参照できます。

ポリシーを作成する

> **注:**
>
> Citrix Virtual Apps and Desktops™展開は、Web Studio (Webベース) と Citrix Studio (Windowsベース) の2つの管理コンソールを使用して管理できます。この記事ではWeb

> Studioのみを扱います。Citrix Studioの詳細については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> ポリシーを作成する前に、それが影響を与える可能性のあるユーザーまたはデバイスのグループを決定します。ユーザーの職務、接続の種類、ユーザーデバイス、または地理的な場所に基づいてポリシーを作成することもできます。Windows Active Directoryグループポリシーで使用するのと同じ基準を使用することもできます。

既にグループに適用されるポリシーを作成している場合は、別のポリシーを作成するのではなく、そのポリシーを編集することを検討してください。ポリシーを編集した後、適切な設定を構成します。特定の設定を有効にするためだけ、または特定のユーザーにポリシーが適用されないようにするためだけにポリシーを作成することは避けてください。

ポリシーを作成する際、ポリシーテンプレートの設定に基づいて作成し、必要に応じて設定をカスタマイズできます。テンプレートを使用せずに、必要なすべての設定を追加して作成することもできます。

Web Studioでは、**ポリシーを有効にする**チェックボックスが明示的にオンにされていない限り、新しく作成されたポリシーは無効に設定されます。

ポリシー作成時および設定構成時に、システムは設定タイプを表示するオプションを提供します。次の設定タイプを表示できます。

- すべての設定 - すべてのVDAバージョンに適用されるすべてを表示
- 現在の設定のみ - 現在のVDAバージョンに固有の設定を表示
- レガシー設定のみ - 非推奨のVDAバージョンにのみ適用される設定を表示

設定を構成しながら設定を表示するには：

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。
2. **ポリシー**タブで、**ポリシーの作成**をクリックします。
3. **設定の選択**テーブルで、**設定**の横にあるドロップダウンをクリックします。
4. ドロップダウンから次のいずれかのオプションを選択します。

- すべての設定 - すべてのVDAバージョンのすべての設定を表示します。
- 現在の設定のみ - 現在のVDAバージョンの設定のみを表示します。
- レガシー設定のみ - 非推奨のVDAバージョンの設定のみを表示します。

1. 「**設定**」テーブルには、前の手順に基づいて利用可能な設定が一覧表示されます。

ポリシー設定

ポリシー設定は、有効、無効、または未構成にできます。デフォルトでは、ポリシー設定は構成されていません。つまり、ポリシーに追加されていません。設定は、ポリシーに追加された場合にのみ適用されます。

ポリシー設定が強化され、依存するポリシー間の明確性が向上しました。この機能により、子ポリシー設定が構成されたときに有効になるように、親ポリシーが最初に構成されることが保証されます。

ポリシー設定を構成するには：

1. 「**ポリシーの作成**」ページで、「**設定の選択**」の下にある「overall」を検索します。 **セッション全体の帯域幅制限**に関連するすべてのポリシー（親と子）が一覧表示されます。
2. 子ポリシーにカーソルを合わせると、ツールヒントが表示され、**セッション全体の帯域幅制限**の親ポリシーが構成されるまで、子ポリシーは構成できないことが示されます。
3. 親ポリシー設定を構成し、次に子ポリシー設定を構成して、**保存**をクリックします。
4. **設定**列と**現在の値**列には、**ポリシーの作成/編集**テーブルで構成された値が表示されます。このテーブルには、構成された設定を変更するための**編集**オプションが表示されます。

依存ポリシー設定(/en-us/citrix-daas/media/dependent-policy-settings.png)

> **注**:
>
> - 親ポリシーが構成されるまで、子ポリシーは選択できません。
> - 親ポリシーのチェックを外すと、関連付けられている子ポリシーもチェックが外れるか、選択解除されることを指示するポップアップメッセージが表示されます。

次の表に、親ポリシーとそれに対応する依存ポリシーまたは子ポリシーのリストを示します。

親ポリシー	依存子ポリシー
セッション全体の帯域幅制限	オーディオリダイレクトの帯域幅制限（パーセント）
	クリップボードリダイレクトの帯域幅制限（パーセント）

親ポリシー	依存子ポリシー
	COMポートリダイレクトの帯域幅制限（パーセント）
	ファイルリダイレクトの帯域幅制限（パーセント）
	HDX™ MediaStream マルチメディアアクセラレーションの帯域幅制限（パーセント）
	LPTポートリダイレクト帯域幅制限（パーセント）
	プリンターリダイレクト帯域幅制限（パーセント）
	クライアントUSBデバイスリダイレクト帯域幅制限（パーセント）
	TWAINデバイスリダイレクト帯域幅制限（パーセント）
双方向コンテンツリダイレクトを許可	クライアントにリダイレクトされる許可されたURL
	VDAにリダイレクトされる許可されたURL
CPU使用率	CPU使用率から除外されるプロセスの優先度
レガシーグラフィックモード	プログレッシブ圧縮レベル
セッションウォーターマークを有効にする	ウォーターマークのカスタムテキスト
	セッションウォーターマークのスタイル
	ウォーターマークの透明度
HDXアダプティブトランスポート	オーディオの損失許容モード

一部のポリシー設定は、次のいずれかの状態になります。

- 許可または禁止は、設定によって制御されるアクションを許可または禁止します。セッション内でユーザーが設定のアクションを管理することを許可または禁止する場合があります。たと

えば、メニューアニメーション設定が「許可」に設定されている場合、ユーザーはクライアント環境でメニューアニメーションを制御できます。

- 有効または無効は、設定をオンまたはオフにします。設定を無効にすると、下位のポリシーでは有効になりません。

さらに、一部の設定は、依存する設定の有効性を制御します。たとえば、クライアントドライブリダイレクトは、ユーザーがデバイス上のドライブにアクセスできるかどうかを制御します。ユーザーがネットワークドライブにアクセスできるようにするには、この設定と**クライアントネットワークドライブ**設定の両方をポリシーに追加する必要があります。**クライアントドライブリダイレクト**設定が無効になっている場合、**クライアントネットワークドライブ**設定が有効になっていても、ユーザーはネットワークドライブにアクセスできません。

一般に、マシンに影響を与えるポリシー設定の変更は、仮想デスクトップが再起動したとき、またはユーザーがログオンしたときに有効になります。ユーザーに影響を与えるポリシー設定の変更は、ユーザーが次回ログオンしたときに有効になります。Active Directoryを使用している場合、ポリシー設定はActive Directoryが90分間隔でポリシーを再評価するときに更新されます。そして、ポリシー設定は、仮想デスクトップが再起動したとき、またはユーザーがログオンしたときに適用されます。

一部のポリシー設定では、設定をポリシーに追加するときに値を入力または選択できます。「デフォルト値を使用」を選択することで、設定の構成を制限できます。この選択により、設定の構成が無効になり、ポリシーが適用されるときに設定のデフォルト値のみが使用されるようになります。この選択は、「デフォルト値を使用」を選択する前に入力された値とは関係ありません。

セキュアデフォルト設定が有効になっている場合、VDAインストール中に、ポリシー設定の優先順位は次のように影響を受けます。

- カスタマイズされた設定が最優先されます
- セキュアなデフォルト設定が2番目の優先順位になります
- デフォルト設定が最も低い優先順位になります

ポリシーのセキュアデフォルト設定を表示するには：

1. Web Studioにログオンします。
2. 左側のナビゲーションで、「**ポリシー**」をクリックします。
3. 「**ポリシー**」タブで、「**ポリシーの作成**」をクリックします。
4. 「**設定の選択**」テーブルで、現在の値が「**許可済み ?**」である設定にマウスカーソルを合わせると、「**セキュリティ保護されたデフォルト値: 禁止**」が表示されます。



ベストプラクティスとして：

- 個々のユーザーではなく、グループにポリシーを割り当てます。グループにポリシーを割り当てると、グループへのユーザーの追加または削除時に割り当てが自動的に更新されます。
- リモートデスクトップセッションホスト構成で、競合する設定や重複する設定を有効にしないでください。リモートデスクトップセッションホスト構成は、Citrixポリシー設定と同様の機能を提供することがあります。トラブルシューティングを容易にするため、可能な限りすべての設定を一貫した状態（有効または無効）に保ってください。
- 未使用のポリシーは無効にします。設定が追加されていないポリシーは、不要な処理を発生させます。

ポリシーの割り当て

ポリシーを作成する際、特定のユーザーとマシンオブジェクトに割り当てます。そのポリシーは、特定の基準またはルールに従って接続に適用されます。一般的に、基準の組み合わせに基づいて、ポリシーに好きなだけ多くの割り当てを追加できます。

割り当てを指定しない場合、または割り当てを指定しても無効にした場合、ポリシーは**すべて**の接続に適用されます。

> **注：**
>
> ポリシーの割り当ては、ポリシーフィルターとも呼ばれます。詳細については、以下のトピックを参照してください。
>
> - ポリシーのフィルターを作成、変更、または削除する
> - フィルターはどのように適用されますか？
>
> 次の表に、利用可能な割り当てを示します。

割り当て名	ポリシーの適用基準
アクセス制御	クライアントが接続する際のアクセス制御条件。*接続タイプ*- NetScaler® Gatewayを使用しているかどうかにかかわ

割り当て名	ポリシーの適用基準
	らず、ポリシーを接続に適用するかどうか。*NetScaler Gatewayファーム名* - NetScaler Gateway仮想サーバーの名前。*アクセス条件* - 使用するエンドポイント分析ポリシーまたはセッションポリシーの名前。
NetScaler SD-WAN	ユーザーセッションがNetScaler SD-WANを介して起動されるかどうか。**注：** ポリシーには、NetScaler SD-WANの割り当てを1つだけ追加できます。
クライアントIPアドレス	クライアントが接続しているIPアドレス。これは、クライアントがセッションに接続する方法によって異なります。 • 直接内部ネットワーク接続：IPアドレスはクライアントのプライベートIPアドレスになります。 • NetScaler Gateway接続：IPアドレスはNetScalerのサブネットIPアドレスになります。 • ゲートウェイサービス接続。 ◦ Rendezvousが無効になっている場合、IPアドレスはCloud Connectorのいずれ

割り当て名	ポリシーの適用基準
	かのIPアドレスになります。 ◦ Rendezvousが有効になっている場合、IPアドレスはGateway Serviceのパブリックアドレスになります。 IPv4の例: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24; IPv6の例: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54
クライアント名	ユーザーデバイスの名前。完全一致: ClientABCName。ワイルドカードを使用: Client*Name。
デリバリーグループ	デリバリーグループのメンバーシップ。
デリバリーグループの種類	デスクトップまたはアプリケーションの種類: プライベートデスクトップ、共有デスクトップ、プライベートアプリケーション、または共有アプリケーション。**注：**プライベートデスクトップと共有デスクトップのフィルターオプションは、Citrix Virtual Apps and Desktops 7.xでのみ利用可能です。詳しくは、

割り当て名	ポリシーの適用基準
	CTX219153を参照してください。
組織単位 (OU)	組織単位。
タグ	タグ。**注：**このポリシーは、タグ付けされたすべてのマシンに適用されます。アプリケーションタグは含まれません。
ユーザーまたはグループ	ユーザーまたはグループ名。

ユーザーがログオンすると、接続の割り当てに一致するすべてのポリシーが特定されます。これらのポリシーは優先順位順に並べ替えられ、設定の複数のインスタンスが比較されます。各設定は、ポリシーの優先順位に従って適用されます。無効になっているポリシー設定は、有効になっている下位ランクの設定よりも優先されます。構成されていないポリシー設定は無視されます。

重要：

グループポリシー管理コンソールを使用してActive DirectoryポリシーとCitrixポリシーの両方を構成する場合、割り当てと設定が期待どおりに適用されないことがあります。詳しくは、CTX127461を参照してください。

「Unfiltered」という名前のポリシーがデフォルトで提供されます。

- Web Studioを使用してCitrixポリシーを管理する場合、Unfilteredポリシーに追加した設定は、Site内のすべてのサーバー、デスクトップ、および接続に適用されます。
- ローカルグループポリシーエディターを使用してCitrixポリシーを管理する場合、Unfilteredポリシーに追加した設定は、すべてのSiteと接続に適用されます。Siteと接続は、ポリシーを含むグループポリシーオブジェクト (GPO) のスコープ内にある必要があります。たとえば、Sales OUには、米国の営業チームのすべてのメンバーを含むSales-USというGPOが含まれています。Sales-US GPOは、いくつかのユーザーポリシー設定を含むUnfilteredポリシーで構成されています。米国の営業マネージャーがSiteにログオンすると、Unfilteredポリシーの設定がセッションに自動的に適用されます。この構成は、ユーザーがSales-US GPOのメンバーであるためです。

割り当てのモードは、ポリシーがすべての割り当て条件に一致する接続にのみ適用されるかどうかを決定します。モードが「許可 (Allow)」(デフォルト) に設定されている場合、ポリシーは割り当て条件に一致する接続にのみ適用されます。モードが「拒否 (Deny)」に設定されている場合、ポリシーは接続が割り当て条件に一致しない場合に適用されます。以下の例は、複数の割り当てが存在する場合に割り当てモードがCitrixポリシーにどのように影響するかを示しています。

- **例: モードが異なる同種の割り当て** - 同じ種類の2つの割り当てがあり、一方が「許可 (Allow)」に設定され、もう一方が「拒否 (Deny)」に設定されているポリシーでは、接続が両方の割り当てを満たす場合、「拒否 (Deny)」に設定された割り当てが優先されます。例:

  ポリシー1には、以下の割り当てが含まれています。

  - 割り当てAは営業グループを指定します。モードは「許可 (Allow)」に設定されています。
  - 割り当てBは営業マネージャーのアカウントを指定します。モードは「拒否 (Deny)」に設定されています。

  割り当てBのモードが「拒否 (Deny)」に設定されているため、営業マネージャーがサイトにログオンしても、そのユーザーが営業グループのメンバーであっても、ポリシーは適用されません。

- **例: モードが同じで異なる種類の割り当て** - 種類が異なる2つ以上の割り当てがあり、「許可 (Allow)」に設定されているポリシーでは、ポリシーが適用されるためには、接続が各種類の割り当ての少なくとも1つを満たす必要があります。例:

  ポリシー2には、以下の割り当てが含まれています。

  - 割り当てCは、営業グループを指定するユーザー割り当てです。モードは「許可 (Allow)」に設定されています。
  - 割り当てDは、10.8.169.* (企業ネットワーク) を指定するクライアントIPアドレス割り当てです。モードは「許可 (Allow)」に設定されています。

  営業マネージャーがオフィスからサイトにログオンすると、接続が両方の割り当てを満たすため、ポリシーが適用されます。

  ポリシー3には、以下の割り当てが含まれています。

  - 割り当てEは、営業グループを指定するユーザー割り当てです。モードは「許可 (Allow)」に設定されています。
  - 割り当てFは、NetScaler Gatewayの接続条件を指定するアクセスコントロール割り当てです。モードは「許可 (Allow)」に設定されています。

営業マネージャーがオフィスからサイトにログオンしても、接続が割り当てFを満たさないため、ポリシーは適用されません。

Web Studioを使用して、テンプレートに基づいてポリシーを作成する

1. Web Studioにサインインし、左側のペインで**ポリシー**を選択します。
2. **テンプレート**タブを選択し、テンプレートを選択します。
3. アクションバーで**テンプレートからポリシーを作成**を選択します。
4. デフォルトでは、新しいポリシーはテンプレート内のすべてのデフォルト設定を使用します。この場合、**テンプレートのデフォルト設定（推奨）**が選択されています。設定を変更する場合は、**デフォルト設定を変更して追加**を選択し、設定を追加または削除します。
5. 次のいずれかを選択して、ポリシーの適用方法を指定します。

   - **選択したユーザーおよびマシンオブジェクト**。ポリシーを選択したユーザーおよびマシンオブジェクトに適用するには、**割り当て**をクリックして、ポリシーを適用する必要があるユーザーおよびマシンオブジェクトを選択します。
   - **サイト内のすべてのオブジェクト**。ポリシーをサイト内のすべてのユーザーおよびマシンオブジェクトに適用します。

6. ポリシーの名前を入力します。ポリシーが影響する対象（例：経理部、リモートユーザーなど）に基づいて名前を付けることを検討してください。必要に応じて、説明を追加します。

   ポリシーはデフォルトで無効になっています。有効にすることができます。ポリシーを有効にすると、ログオンするユーザーにすぐに適用されます。無効にすると、ポリシーが適用されなくなります。ポリシーの優先順位を付けたり、後で設定を追加したりする必要がある場合は、適用する準備ができるまでポリシーを無効にしておくことを検討してください。

Web Studioを使用してポリシーを作成する

1. Web Studioにサインインし、左側のペインで**ポリシー**を選択します。
2. **ポリシー**タブを選択します。
3. アクションバーで**ポリシーを作成**を選択します。
4. ポリシー設定を追加および構成します。
5. 次のいずれかを選択して、ポリシーを適用する方法を指定します。

   - 選択したユーザーオブジェクトとマシンオブジェクトに割り当て、ポリシーを適用するユーザーオブジェクトとマシンオブジェクトを選択します。

- サイト内のすべてのオブジェクトに割り当てて、サイト内のすべてのユーザーオブジェクトとマシンオブジェクトにポリシーを適用します。

6. ポリシーの名前を入力するか、デフォルトを受け入れます。ポリシーが影響する対象（例: 経理部、リモートユーザー）に基づいて名前を付けることを検討してください。必要に応じて、説明を追加します。

   ポリシーはデフォルトで有効になっていますが、無効にすることもできます。ポリシーを有効にすると、ログオンするユーザーにすぐに適用されます。無効にすると、ポリシーは適用されません。ポリシーの優先順位を付けたり、後で設定を追加したりする必要がある場合は、適用する準備ができるまでポリシーを無効にしておくことを検討してください。

グループポリシーエディターを使用してポリシーを作成および管理する

グループポリシーエディターで、**コンピューターの構成**または**ユーザーの構成**を展開します。**ポリシー**ノードを展開し、次に**Citrixポリシー**を選択します。適切なアクションを選択します。

タスク	手順
ポリシーを作成する	**ポリシー**タブで、**新規**をクリックします。
既存のポリシーを編集する	**ポリシー**タブで、ポリシーを選択し、**編集**をクリックします。
既存のポリシーの優先順位を変更する	**ポリシー**タブで、ポリシーを選択し、**上位**または**下位**をクリックします。
ポリシーの概要情報を表示	**ポリシー**タブでポリシーを選択し、**概要**タブをクリックします。
ポリシー設定の表示と変更	**ポリシー**タブでポリシーを選択し、**設定**タブをクリックします。
ポリシーフィルターの表示と変更	**ポリシー**タブでポリシーを選択し、**フィルター**タブをクリックします。ポリシーに複数のフィルターを追加する場合、ポリシーが適用されるにはすべてのフィルター条件を満たす必要があります。
ポリシーの有効化または無効化	**ポリシー**タブでポリシーを選択し、**アクション > 有効化**または**アクション > 無効化**のいずれかを選択します。

タスク	手順
既存のテンプレートからポリシーを作成	**テンプレート**タブでテンプレートを選択し、**新しいポリシー**をクリックします。

ポリシーセット

ポリシーセットは、Citrix Virtual Apps and Desktops™ のオブジェクトであり、ポリシーを集約して、簡素化されたロールベースのアクセスと容易な管理を可能にします。管理者チームや会社の論理的な区分を反映するようにポリシーセットを作成できます。たとえば、地理的な地域ごと、事業部門ごと、または特定のユースケースごとにポリシーセットを作成できます。作成後、スコープとデリバリーグループがポリシーセットに割り当てられ、承認された管理者のみが関連するユーザーとマシンに適用されるポリシーを管理できるようになります。

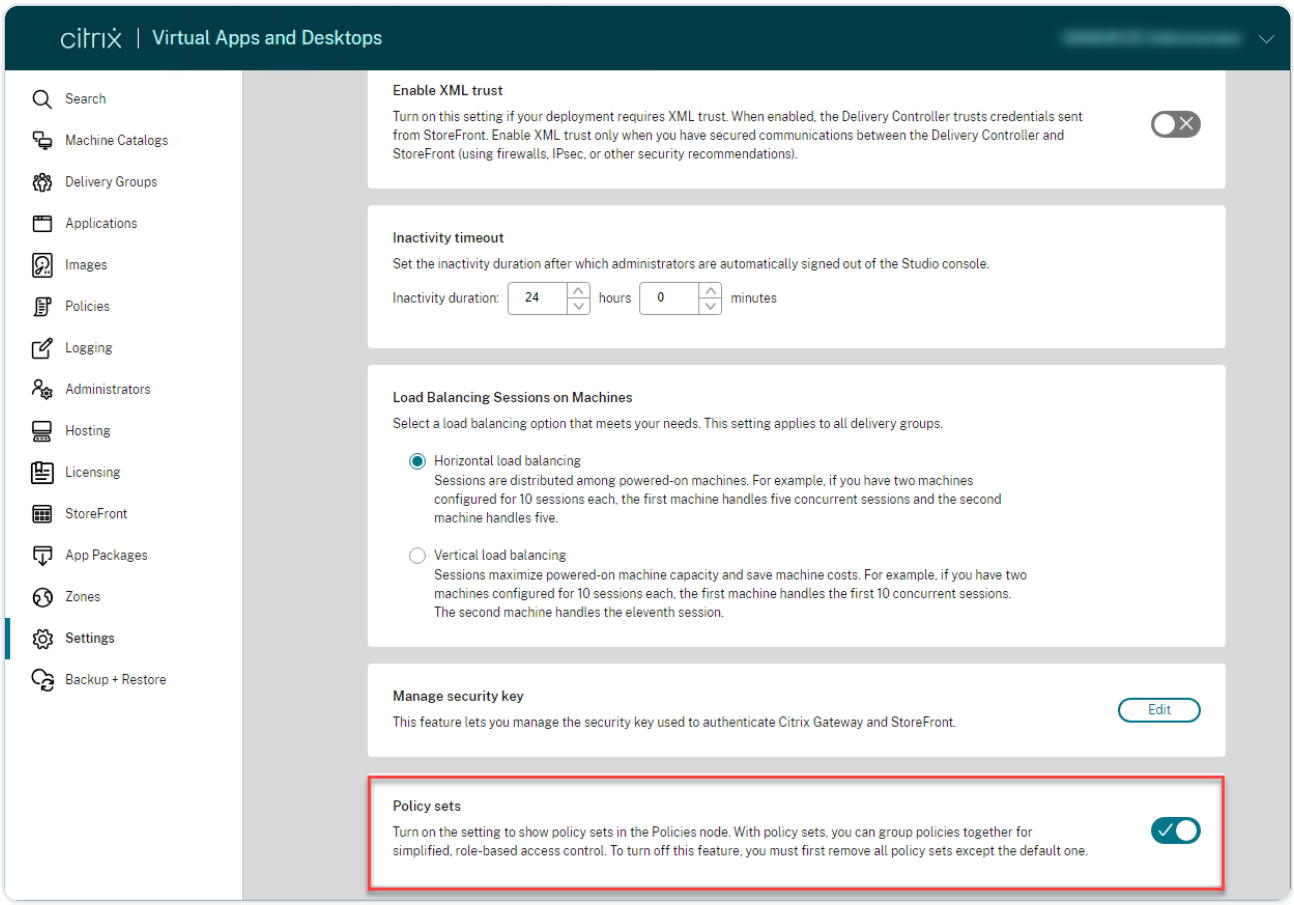
> **注:**
>
> ポリシーセットを有効にする前に、Citrix® は以下の点に注意することをお勧めします。
>
> - 追加のポリシー検証が追加されます。その結果、無効なポリシー設定が存在する場合、インプレースアップグレードを行うとポリシーデータが失われる可能性があります。
> - 無効なデータを検出するには、GPOスキャナーツール を使用し、アップグレード前に必要な編集を行ってください。詳細については、CTX676686 を参照してください。
> - 今後のすべてのアップグレードでは、最新のSDKを使用することをお勧めします。古いSDKを使用してポリシーを更新すると、ポリシー設定に無効なデータが追加される可能性があり、ポリシーデータが失われるリスクにつながる可能性があります。

利点

- 分散型管理者チーム向けのロールベースのアクセス制御
- 合併、買収、統合の簡素化
- 制限された障害ドメイン
- ポリシーのマルチテナントサポート

ポリシーセットを有効にする

Virtual Apps and Desktops の タブから に移動し、 設定をオンにします。



注:

ポリシーセットを作成する前に、ポリシーセットを有効にする必要があります。

機能比較

ポリシーセットを適用する前	ポリシーセットを適用した後
サイト全体に対するポリシー、設定、フィルター、およびポリシーの優先順位は、Citrix Studio内で一箇所で構成されます。	ポリシー、設定、フィルター、およびポリシーの優先順位は、各ポリシーセットに対して個別に構成されます。
1つのポリシーを管理する場合、すべてのポリシーを管理する必要があります。	フル管理者は、特定のポリシーセットを個別に管理する機能を下位レベルの管理者に委任できます。
大規模で分散された環境におけるポリシーは、複雑になり管理が困難になります。	大規模で分散された環境におけるポリシーは、分割して簡単に管理できます。

ポリシーセットの仕組み?

概要

- ポリシーセットはデリバリーグループに割り当てられます
- ポリシーセットは1つまたは複数のスコープを持ちます
- ポリシーセットが割り当てられていないデリバリーグループは、デフォルトのポリシーセットを受け取ります。
- デリバリーグループには、1つのポリシーセットのみを割り当てることができます。
- 複数のデリバリーグループで同じポリシーセットを使用できます。
- ポリシーセットがデリバリーグループに割り当てられていても、ポリシーはフィルターを維持します。

詳細については、「フィルターはどのように適用されますか？」を参照してください。ポリシーセットに対するポリシーの割り当てやポリシーフィルターの動作方法に変更はありません。つまり、ポリシーの場合と同じように機能します。

デフォルトのポリシーセット

- ポリシーセット設定がオンの場合、既存のすべてのポリシーはデフォルトのポリシーセット内にグループ化されます。
- 管理者チームがポリシーセットを作成してデリバリーグループに割り当てない限り、すべてのデリバリーグループはデフォルトのポリシーセットを受け取ります。
- デリバリーグループに別のポリシーセットが割り当てられると、デフォルトのポリシーセットからポリシーを受け取らなくなります。

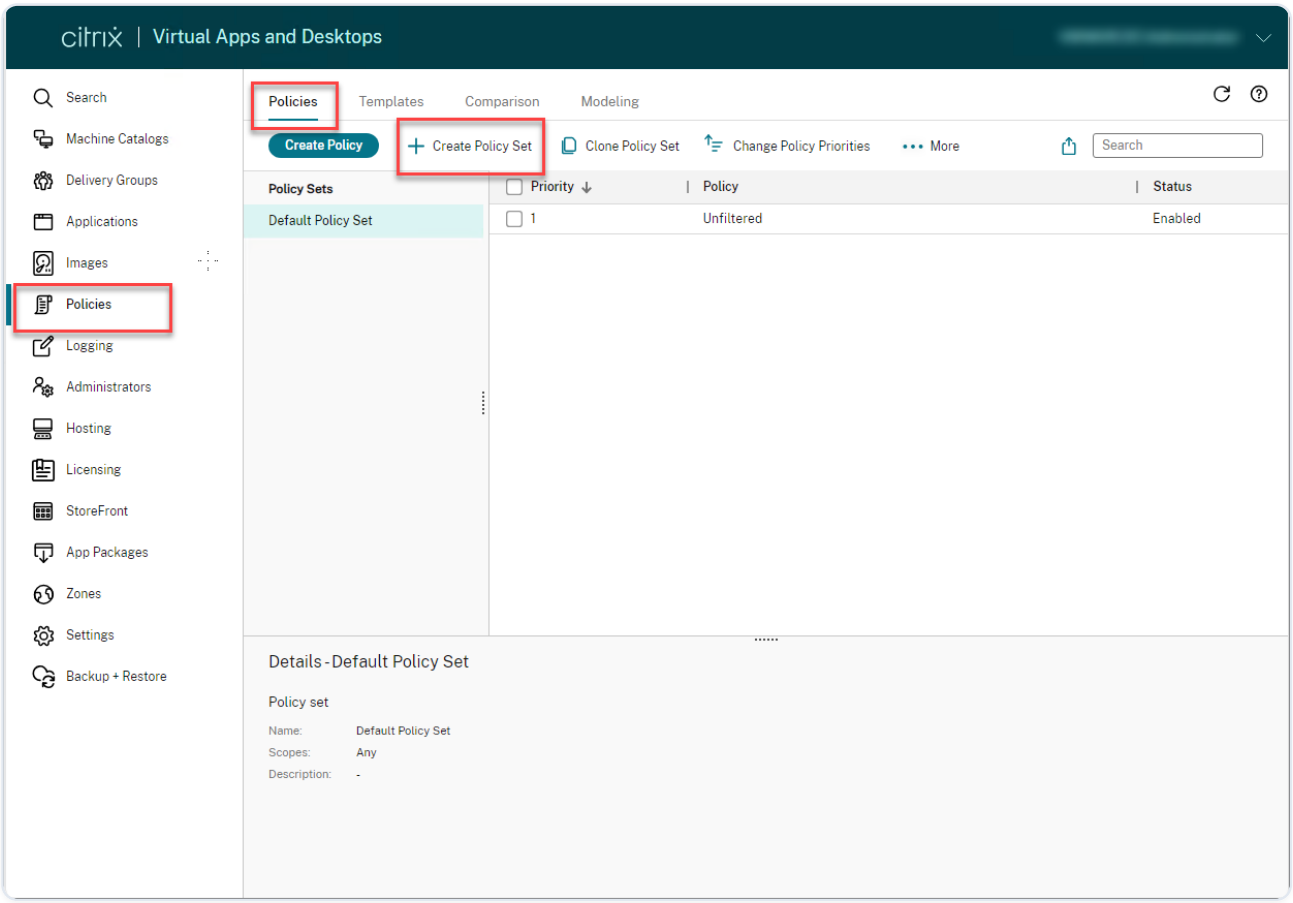
ポリシーセットの作成

ポリシーセットは、次の2つの方法で作成できます。

- ポリシーセットの作成 - このアクションは空のポリシーセットを作成します。
- ポリシーセットのクローン作成 - このアクションは既存のポリシーセットに基づいてポリシーセットを作成します。

ポリシーセットを作成する

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。



1. 「**ポリシーセットの作成**」を選択します。「**はじめに**」タブが表示されます。
2. 「**次へ**」をクリックするか、「**名前と説明**」タブをクリックします。
3. ポリシーセットの名前と説明を入力します。
4. 「**次へ**」をクリックするか、「**割り当て**」タブをクリックします。
5. ポリシーセットを割り当てる1つ以上のデリバリーグループを選択します。
6. 「**次へ**」をクリックするか、「**スコープ**」タブをクリックします。
7. ポリシーセットのスコープを選択します。
8. 「**作成**」をクリックします。定義された割り当てとスコープでポリシーセットが作成されます。

ポリシーセットの複製

1. Web Studioにサインインし、左側のペインで「**ポリシー**」を選択します。
2. 「**ポリシーセットの複製**」を選択します。
3. ポリシーセットの名前を変更します。
4. ポリシーセットの割り当てを変更または作成し、「**次へ**」をクリックします。
5. 複製されたポリシーセットに含めるポリシーを選択または選択解除します。

6. ポリシーのスコープを変更します。
7. **作成**をクリックします。ポリシーセットが作成されます。

ポリシーセットを編集する

1. Web Studioにサインインし、左側のペインで**ポリシー**を選択します。
2. **ポリシーセットの編集**を選択します。
3. ポリシーセットの名前を変更し、**次へ**をクリックします。
4. ポリシーセットの割り当てを変更または作成し、**次へ**をクリックします。
5. ポリシーのスコープを変更します。
6. 「**作成**」をクリックします。ポリシーセットが作成されます。

ポリシーセットの編集

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。
2. 「**ポリシーセットの編集**」を選択します。
3. ポリシーセットの名前を変更し、「**次へ**」をクリックします。
4. ポリシーセットの割り当てを変更または作成し、「**次へ**」をクリックします。
5. ポリシーのスコープを変更します。
6. **Create** をクリックします。

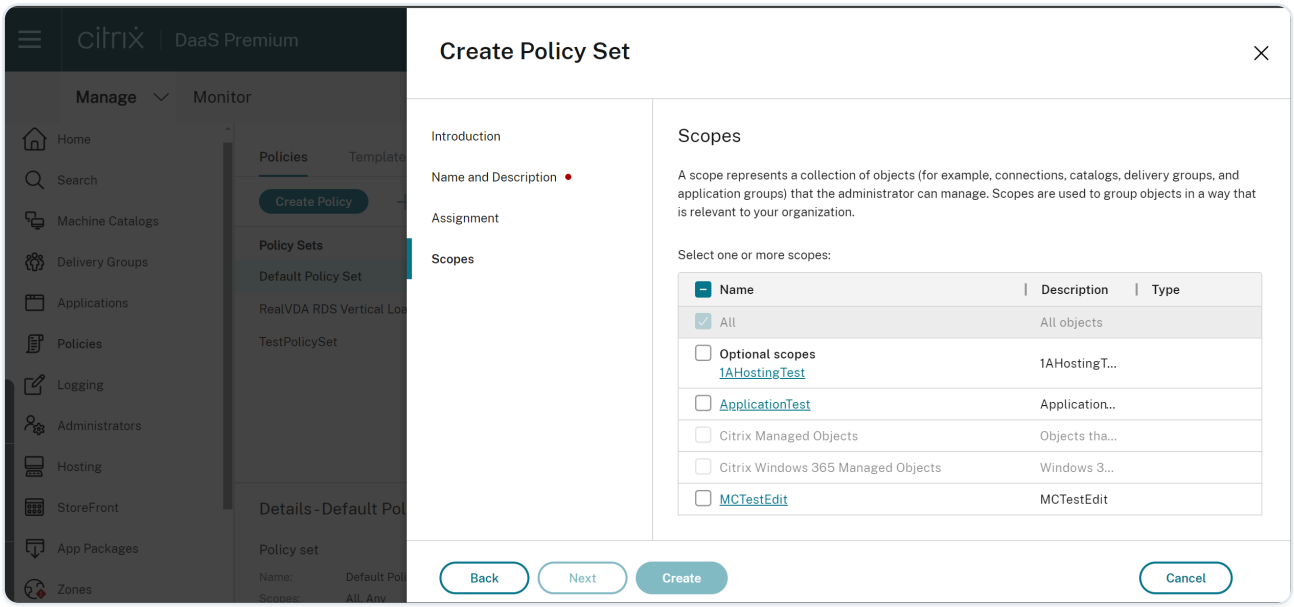
ポリシーセットの割り当て

ポリシーセットはデリバリーグループに割り当てられます。ポリシーセットの作成時または編集時に割り当てを構成できます。また、デリバリーグループの作成時または編集時にも割り当てを構成できます。

ポリシーセットのスコープ

管理者はポリシーセットのスコープを定義して、承認された管理者のみがそれを表示または編集できるようにすることができます。ポリシーセットの作成時または編集時にスコープを構成できます。

ポリシーセットの導入により、APIを使用してCitrixポリシーを作成および管理することもできます。詳細については、「Citrix DaaSでポリシーセットを作成する方法」を参照してください。



ポリシーの比較、優先順位付け、モデル化、トラブルシューティング

注:

Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

複数のポリシーを使用して、ユーザーの職務、地理的な場所、または接続の種類に基づいて、ユーザーのニーズを満たすように環境をカスタマイズできます。たとえば、セキュリティを強化するために、機密データを定期的に扱うユーザーグループに制限を設けることができます。

また、ユーザーが機密ファイルをローカルクライアントドライブに保存できないようにするポリシーを作成することもできます。ただし、ユーザーグループ内の一部のユーザーがローカルドライブへのアクセスを必要とする場合は、それらのユーザー専用の別のポリシーを作成できます。その後、どちらが優先されるかを制御するために、2つのポリシーをランク付けまたは優先順位付けします。複数のポリシーを使用する場合、次のことを決定する必要があります。

- ポリシーの優先順位付け方法
- 例外の作成方法

- ポリシーが競合する場合に有効なポリシーを表示する方法。

一般に、ポリシーは、サイト全体、特定のDelivery Controller、またはユーザーデバイスに構成された同様の設定を上書きします。この原則の例外はセキュリティです。環境内で最も高い暗号化設定は、常に他の設定やポリシーを上書きします。最も高い暗号化設定には、オペレーティングシステムと最も制限の厳しいシャドウイング設定が含まれます。

Citrixポリシーは、オペレーティングシステムで設定したポリシーと相互作用します。Citrix環境では、Citrix設定は、Active Directoryポリシーで構成された、またはリモートデスクトップセッションホスト構成を使用して構成された同じ設定を上書きします。この設定には、一般的なリモートデスクトッププロトコル（RDP）クライアント接続設定に関連する設定が含まれます。一般的なRDP設定には、デスクトップの壁紙、メニューアニメーション、ドラッグ中のウィンドウコンテンツの表示などの設定が含まれます。

Secure ICA®などの一部のポリシー設定は、オペレーティングシステムの設定と一致している必要があります。より優先度の高い暗号化レベルが他の場所で設定されている場合、ポリシーで、またはアプリケーションとデスクトップを配信するときに指定する**Secure ICAポリシー**の設定は上書きされる可能性があります。

たとえば、デリバリーグループを作成するときに指定する暗号化設定は、環境全体で指定した暗号化設定と同じレベルである必要があります。

> **注:**
>
> ダブルホップシナリオの2番目のホップでは、シングルセッションOS VDAがマルチセッションOS VDAに接続することを考慮してください。この場合、Citrixポリシーは、シングルセッションOS VDAをユーザーデバイスであるかのように扱います。たとえば、ユーザーデバイスに画像をキャッシュするようにポリシーが設定されているとします。この例では、ダブルホップシナリオの2番目のホップ用にキャッシュされた画像は、シングルセッションOS VDAマシンにキャッシュされます。

ポリシーモデリングウィザードの使用

ポリシーモデリングは、計画およびテスト目的で、フィルター付きの有効なポリシーをシミュレートするのに役立ちます。フィルター付きの有効なポリシーのみがモデル化されます。無効なポリシーは適用されず、フィルターなしの有効なポリシーは常に適用されます。

ポリシーモデリングウィザードを開くには、次の手順を実行します。

1. 左側のナビゲーションから**ポリシー**を選択します。
2. **モデリング**タブを選択します。
3. アクションバーで**ポリシーモデリング**を選択します。
4. **はじめに**ページを読み、**次へ**をクリックします。
5. ユーザーまたはコンピューターを選択します。コンテナー、または特定のユーザーやコンピューターを参照できます。**次へ**をクリックします。
6. フィルターの証拠を選択します。オプションで、**デリバリーグループ**、**タグ**、**クライアントIPアドレス**などの追加の詳細を入力することで、シミュレーションをより詳細にすることができます。**次へ**をクリックします。
7. 選択内容の概要を確認し、**実行**をクリックします。

「実行」 をクリックすると、ウィザードによってモデリング結果のレポートが生成されます。このレポートを表示している間は、次のことができます。

- ドロップダウンメニューで、**「すべての設定」**、**「コンピューター設定」**、または **「ユーザー設定」** のいずれを表示するかを選択します。
- 検索バーを使用して、特定の設定を検索します。
- 特定の設定をクリックして、その設定の詳細を表示します。たとえば、特定のポリシーに対してすべてのユーザー設定が適用されなかった場合、**詳細**ペインには設定が適用されなかった理由が表示されます。
- **エクスポート**をクリックして、モデリング結果をJSON形式、HTML形式、またはその両方でエクスポートします。

ポリシーモデリングを実行すると、さらに多くのオプションが利用可能になります。次のことができます。

- **モデリングレポートの表示**：これにより、上記のモデリングレポートが開き、再度表示したりエクスポートしたりできます。
- **ポリシーモデリングの再実行**：これにより、以前に選択したのと同じ基準セットでポリシーモデリングを再実行し、新しいモデリング結果を生成できます。これは、一部のポリシーが変更され、それらの変更が現在のモデルにどのように影響するかを確認したい場合に役立ちます。
- **モデリングレポートの削除**：これにより、現在のモデリングレポートが削除されます。

ポリシーとテンプレートの比較

ポリシーまたはテンプレートの設定を、他のポリシーまたはテンプレートの設定と比較できます。たとえば、ベストプラクティスへの準拠を維持するために、設定値を検証する必要がある場合があります。また、ポリシーまたはテンプレートの設定を、Citrixが提供するデフォルト設定と比較することもできます。

1. Web Studio にサインインし、左側のペインで を選択します。
2. タブをクリックし、 をクリックします。
3. 比較するポリシーまたはテンプレートを選択します。比較にデフォルト値を含めるには、チェックボックスをオンにします。
4. をクリックすると、構成された設定が列に表示されます。
5. すべての設定を表示するには、 を選択します。デフォルトビューに戻るには、 を選択します。

ポリシーの優先順位付け

ポリシーの優先順位付けにより、競合する設定が含まれる場合にポリシーの優先順位を定義できます。ユーザーがログオンすると、接続の割り当てに一致するすべてのポリシーが識別されます。これらのポリシーは優先順位順に並べ替えられ、任意の設定の複数のインスタンスが比較されます。各設定は、ポリシーの優先順位に従って適用されます。

ポリシーには異なる優先順位番号を割り当てることで、優先順位を付けます。デフォルトでは、新しいポリシーには最も低い優先順位が与えられます。ポリシー設定が競合する場合、優先順位が高いポリシー（優先順位番号1が最高）は、優先順位が低いポリシーを上書きします。設定は、優先順位と設定の条件（たとえば、設定が無効か有効か）に従ってマージされます。無効な設定は、有効な下位の設定を上書きします。構成されていないポリシー設定は無視され、下位の設定を上書きしません。

1. 左側のペインで を選択します。 タブが選択されていることを確認します。
2. タブで、アクションバーの を選択します。 ページが表示されます。
3. 優先順位リストで、ポリシーの優先順位を変更するには、次のいずれかの方法を使用します。
    - ポリシーを目的の位置にドラッグします。
    - 1つ上または下に移動するには、それぞれ上矢印または下矢印アイコンをクリックします。
    - リストの先頭または末尾に移動するには、それぞれ先頭または末尾の矢印アイコンをクリックします。

- 優先順位番号を変更するには、**編集**アイコンをクリックし、必要に応じて番号を入力して、**保存**をクリックします。

4. 「**保存**」をクリックします。

例外

ユーザー、ユーザーデバイス、またはマシンのグループに対してポリシーを作成する場合、グループの一部のメンバーが特定のポリシー設定の例外を必要とすることがあります。例外を作成するには、次の方法があります。

- 例外を必要とするグループメンバーのみにポリシーを作成し、そのポリシーをグループ全体のポリシーよりも上位にランク付けする
- ポリシーに追加された割り当てに対して拒否モードを使用する

モードが拒否に設定された割り当ては、割り当て基準に一致しない接続にのみポリシーを適用します。たとえば、ポリシーには次の割り当てが含まれます。

- 割り当てAは、範囲208.77.88.*を指定するクライアントIPアドレスの割り当てです。モードは許可に設定されています。
- 割り当てBは、特定のユーザーアカウントを指定するユーザーの割り当てです。モードは拒否に設定されています。

このポリシーは、割り当てAで指定された範囲のIPアドレスを使用してサイトにログオンするすべてのユーザーに適用されます。ただし、割り当てBで指定されたユーザーアカウントを使用してサイトにログオンするユーザーには適用されません。

接続に適用されるポリシーを決定する

複数のポリシーが適用されるため、接続が期待どおりに応答しない場合があります。優先度の高いポリシーが接続に適用される場合、元のポリシーで構成した設定が上書きされることがあります。結果ポリシーセットを計算し、接続に対して最終的なポリシー設定がどのように結合されるかを判断できます。

結果ポリシーセットは、次の方法で計算できます。

- **Citrix Group Policy Modeling**ウィザードを使用して接続シナリオをシミュレートし、Citrixポリシーがどのように適用されるかを識別します。接続シナリオの条件を次のように指定できます。
    - ドメインコントローラー
    - ユーザー

    - Citrixポリシー割り当ての証拠値
    - 低速ネットワーク接続などのシミュレートされた環境設定 ウィザードが生成するレポートには、そのシナリオで有効になるCitrixポリシーが一覧表示されます。ドメインユーザーとしてControllerにログオンするため、ウィザードはサイトポリシー設定とActive Directoryグループポリシーオブジェクト（GPO）の両方を使用して結果を計算します。

- **グループポリシーの結果**を使用して、特定のユーザーとコントローラーに適用されるCitrixポリシーを記述したレポートを生成します。グループポリシーの結果ツールは、環境内のGPOの現在の状態を評価し、レポートを生成するのに役立ちます。生成されたレポートには、Citrixポリシーを含むこれらのオブジェクトが、特定のユーザーとコントローラーに現在どのように適用されているかが記述されています。

Web StudioでCitrix Group Policy Modelingウィザードを起動できます。または、Windowsのグループポリシー管理コンソールからグループポリシーの結果ツールを起動することもできます。

Web Studioを使用して作成されたサイトポリシー設定は、次の場合、結果ポリシーセットには含まれません。

- グループポリシー管理コンソールからCitrix Group Policy Modelingウィザードを実行する場合
- グループポリシー管理コンソールからグループポリシーの結果ツールを実行する場合

最も包括的な結果ポリシーセットを取得することを確認するには、グループポリシー管理コンソールのみを使用してポリシーを作成する場合を除き、CitrixはWeb StudioからCitrix Group Policy Modelingウィザードを起動することを推奨します。

ポリシーのトラブルシューティング

ユーザー、IPアドレス、およびその他の割り当てられたオブジェクトには、同時に適用される複数のポリシーが存在する場合があります。このシナリオでは、ポリシーが期待どおりに動作しない競合が発生する可能性があります。Citrix Group Policy Modelingウィザードまたはグループポリシーの結果ツールを実行すると、ユーザー接続にポリシーが適用されていないことが判明する場合があります。このようなシナリオでは、ポリシー評価基準に一致する条件下でアプリケーションやデスクトップに接続するユーザーには、ポリシー設定が適用されません。この状況は次の場合に発生します。

- ポリシー評価基準に一致する割り当てを持つポリシーがない場合。
- 割り当てに一致するポリシーに設定が構成されていない場合。
- 割り当てに一致するポリシーが無効になっている。

指定された基準を満たす接続にポリシー設定を適用する場合は、次のことを確認してください。

- それらの接続に適用するポリシーが有効になっていること。
- 適用するポリシーに適切な設定が構成されていること。

デフォルトのポリシー設定

以下の表に、ポリシー設定、そのデフォルト値、およびそれらが適用されるVirtual Delivery Agent (VDA) のバージョンを示します。

ICA®

名前	デフォルト設定	VDA
アダプティブトランスポート	オフ。優先される場合に使用します	VDA 7.13～7.15、VDA 7.16以降
クライアントクリップボードリダイレクト	許可	すべてのVDAバージョン
クライアントクリップボード書き込み許可形式	形式は指定されていません	VDA 7.6 以降
デスクトップの起動	禁止	マルチセッションOS用VDA 7以降
ICAリスナーポート番号	1494	すべてのVDAバージョン
クライアント接続中の非公開プログラムの起動	禁止	マルチセッションOS用VDA 7以降
クリップボードのクライアントからセッションへの転送サイズを制限	無効	VDA 2009
クリップボードのセッションからクライアントへの転送サイズを制限	無効	VDA 2009
損失許容モード	許可	VDA 2003。注：損失許容モードはまだ利用できません。このバージョンのVDAは、利用可能になったときにそれをサポートします。

名前	デフォルト設定	VDA
損失許容しきい値	損失許容モードが利用可能な場合：パケット損失：5%、遅延：300 ms (RTT)	VDA 2003から現在まで
ランデブープロトコル	無効	Citrix Cloudを介して確立されたHDXセッションにのみ適用されます。
クライアントクリップボードへの書き込みを制限	禁止	VDA 7.6から現在まで
セッションクリップボードへの書き込みを制限	禁止	VDA 7.6から現在まで
セッションクリップボード書き込み許可形式	形式は指定されていません	VDA 7.6以降
タブレットモードの切り替え	有効	VDA 7.16以降。VDA 7.14および7.15 LTSRの場合は、レジストリを使用してこの設定を構成します。
仮想チャネル許可リスト	有効	VDA 2109以降
セッションメトリック収集	許可	7.42以降

ICA/Adobe Flash 配信/Flash リダイレクト

名前	デフォルト設定	VDA
Flashビデオのフォールバック防止	未構成	VDA 7.6 FP3 から現在まで
Flashビデオのフォールバック防止エラー *.swf	VDA 7.6 FP3 から現在まで	

ICA/オーディオ

名前	デフォルト設定	VDA
アダプティブオーディオ	有効	Citrix Virtual Apps and Desktops™ 2109以降を使用するVDAの、シングルセッションOSおよびマルチセッションOSの両方のセッションに適用されます。
UDPリアルタイムトランスポート経由のオーディオ	許可	すべてのVDAバージョン
オーディオプラグアンドプレイ	許可	マルチセッションOS用VDA 7 から現在まで
オーディオ品質	高 - 高精細オーディオ	すべてのVDAバージョン
クライアントオーディオリダイレクト	許可	すべてのVDAバージョン
クライアントマイクのリダイレクト	許可	すべてのVDAバージョン
オーディオのロス許容モード	禁止	VDA バージョン 2411 以前

ICA/自動クライアント再接続

名前	既定の設定	VDA
自動クライアント再接続	許可	すべての VDA バージョン
自動クライアント再接続認証	認証を要求しない	すべての VDA バージョン
自動クライアント再接続ログ	自動再接続イベントをログに記録しない	すべての VDA バージョン
自動クライアント再接続タイムアウト	120 秒	VDA 7.13 から現在まで
再接続UIの透過レベル	80%	VDA 7.13 から現在まで

ICA/帯域幅

名前	デフォルト設定	VDA
オーディオリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
オーディオリダイレクト帯域幅制限の割合	0	すべてのVDAバージョン
クライアントUSBデバイスリダイレクト帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
クライアントUSBデバイスリダイレクト帯域幅制限率	0	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
クリップボードリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
クリップボードリダイレクト帯域幅制限率	0	すべてのVDAバージョン
COMポートリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン。VDA 7.0〜7.8の場合、この設定はレジストリを使用して構成します。
COMポートリダイレクト帯域幅制限率	0	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します
ファイルリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
ファイルリダイレクト帯域幅制限率	0	すべてのVDAバージョン

名前	デフォルト設定	VDA
HDX MediaStreamマルチメディアアクセラレーション帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7およびシングルセッションOS用VDA 7から現在のマルチセッションOS用VDAおよびシングルセッションOS用VDAまで
HDX MediaStreamマルチメディアアクセラレーション帯域幅制限率	0	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
LPTポートリダイレクトの帯域幅制限	0 ケービーピーエス	すべてのVDAバージョン。VDA 7.0から7.8の場合、この設定はレジストリを使用して構成します。
LPTポートリダイレクトの帯域幅制限の割合	0	すべてのVDAバージョン。VDA 7.0から7.8の場合、この設定はレジストリを使用して構成します。
セッション全体の帯域幅制限	0 ケービーピーエス	すべてのVDAバージョン
プリンターリダイレクトの帯域幅制限	0 ケービーピーエス	すべてのVDAバージョン
プリンターリダイレクトの帯域幅制限の割合	0	すべてのVDAバージョン
TWAINデバイスリダイレクト帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
TWAINデバイスリダイレクト帯域幅制限の割合	0	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/双方向コンテンツリダイレクト

名前	デフォルト設定	VDA
双方向コンテンツリダイレクトを許可する	禁止	VDA 7.13以降
クライアントにリダイレクトを許可するURL	空	VDA 7.13 以降
VDAにリダイレクトされるURLを許可	空	VDA 7.13 以降
双方向コンテンツリダイレクト構成	無効	VDA 2311 以降

ICA/ブラウザコンテンツリダイレクト

名前	デフォルト設定	VDA
ブラウザコンテンツリダイレクト	許可	VDA 7.16 以降
ブラウザコンテンツリダイレクトACL構成	`https://www.youtube.com/*`	VDA 7.16 以降
ブラウザコンテンツリダイレクト 統合Windows認証サポート	禁止	VDA 2106 以降
ブラウザコンテンツリダイレクト プロキシ構成	空	VDA 7.16 以降
ブラウザコンテンツリダイレクト サーバーフェッチ Web プロキシ認証	禁止	VDA 2012 以降

ICA/クライアントセンサー

名前	デフォルト設定	VDA
アプリケーションがクライアントデバイスの物理的な位置	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シ

名前	デフォルト設定	VDA
情報を使用することを許可する		ングルセッションOS用VDA 7以降

ICA/デスクトップUI

名前	デフォルト設定	VDA
デスクトップコンポジションリダイレクト	無効 (7.6 FP3以降); 有効 (5.6から7.6 FP2まで)	VDA 5.6、シングルセッションOS用VDA 7から7.15まで
デスクトップコンポジションリダイレクトのグラフィック品質	中	VDA 5.6、シングルセッションOS用VDA 7から7.15まで
デスクトップの壁紙	許可	すべてのVDAバージョン
メニューアニメーション	許可	すべてのVDAバージョン
ドラッグ中にウィンドウの内容を表示	許可	すべてのVDAバージョン

ICA/エンドユーザー監視

名前	デフォルト設定	VDA
ICAラウンドトリップ計算	有効	すべてのVDAバージョン
ICAラウンドトリップ計算間隔	15秒	すべてのVDAバージョン
アイドル接続のICAラウンドトリップ計算	無効	すべてのVDAバージョン

ICA/強化されたデスクトップエクスペリエンス

名前	デフォルト設定	VDA
強化されたデスクトップエクスペリエンス	許可	マルチセッションOS 7から現在までのVDA

ICA/ファイルリダイレクト

名前	デフォルト設定	VDA
クライアントドライブの自動接続	許可	すべてのVDAバージョン
クライアントドライブのリダイレクト	許可	すべてのVDAバージョン
クライアント固定ドライブ	許可	すべてのVDAバージョン
クライアントフロッピードライブ	許可	すべてのVDAバージョン
クライアントネットワークドライブ	許可	すべてのVDAバージョン
クライアントの光学ドライブ	許可	すべてのVDAバージョン
クライアントのリムーバブルドライブ	許可	すべてのVDAバージョン
ホストからクライアントへのリダイレクト	無効	マルチセッションOS用VDA 7から現在まで
クライアントドライブ文字の保持	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7から現在まで
読み取り専用クライアントドライブアクセス	無効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
特殊フォルダーのリダイレクト	許可	Web Interface展開のみ。マルチセッションOS用VDA 7以降
非同期書き込みの使用	無効	すべてのVDAバージョン

ICA/グラフィック

名前	デフォルト設定	VDA
視覚的にロスレスな圧縮を許可する	無効	VDA 7.6以降
表示メモリ制限	65,536 Kb	VDA 5、5.5、5.6 FP1、シングルセッションOS向けVDA 7以降
ディスプレイモードの劣化設定	最初に色深度を劣化させる	すべてのVDAバージョン
動的ウィンドウプレビュー	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
グラフィックステータスインジケーター	無効	VDA 7.16以降
イメージキャッシュ	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
レガシーグラフィックモード	無効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
最大許容色深度	32ビット/ピクセル	すべてのVDAバージョン
表示モードが低下したときにユーザーに通知する	無効	マルチセッションOS用VDA 7以降
3Dグラフィックワークロード向けに最適化する	無効	VDA 7.17以降
キューイングと破棄	有効	すべてのVDAバージョン
画面共有	無効	VDA 2112

名前	デフォルト設定	VDA
圧縮にビデオコーデックを使用	優先される場合にビデオコーデックを使用	VDA 7.6 FP3から現在まで
ビデオコーデックにハードウェアエンコーディングを使用	有効	VDA 7.11から現在まで

ICA/グラフィック/キャッシュ

名前	デフォルト設定	VDA
永続キャッシュしきい値	300万 bps	マルチセッションOS用VDA 7から現在まで

ICA/グラフィック/Framehawk

名前	デフォルト設定	VDA
Framehawk表示チャネル	無効	VDA 7.6 FP2から現在まで
Framehawk表示チャネルポート範囲	3224,3324	VDA 7.6 FP2から現在まで

ICA/キープアライブ

名前	デフォルト設定	VDA
ICAキープアライブタイムアウト	60秒	すべてのVDAバージョン
ICAキープアライブ	ICAキープアライブメッセージを送信しない	すべてのVDAバージョン

ICA/キーボードおよびIME

名前	デフォルト設定	VDA
クライアントキーボードレイアウト同期とIMEの改善	無効	1912 LTSR CU2以降にのみ適用されます。

名前	デフォルト設定	VDA
Unicodeキーボードレイアウトマッピングを有効にする	許可 (2407から現在まで); 禁止 (以前のバージョン)	1912 LTSR CU2以降にのみ適用されます。
キーボードレイアウト切り替えポップアップメッセージボックスを非表示にする	禁止	1912 LTSR CU2以降にのみ適用されます。

ICA/ローカルアプリアクセス

名前	デフォルト設定	VDA
ローカルアプリアクセスを許可	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
URLリダイレクトブロックリスト	サイトは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
URLリダイレクト許可リスト	サイトは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/モバイルエクスペリエンス

名前	デフォルト設定	VDA
キーボードの自動表示	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
タッチ最適化デスクトップの起動	許可	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降。この設定は無効になっており、Windows 10およびWindows Server 2016マシンでは利用できません。

名前	デフォルト設定	VDA
コンボボックスのリモート化	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/マルチメディア

名前	デフォルト設定	VDA
HTML5ビデオリダイレクト	禁止	VDA 7.12以降
ビデオ品質の制限	未構成	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
Microsoft Teamsリダイレクト	許可	マルチセッションOS用VDA 1906以降、シングルセッションOS用VDA 1906以降。
マルチメディア会議	許可	すべてのVDAバージョン
WAN経由のWindows Media マルチメディアリダイレクトの最適化	許可	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
WAN経由のWindows Media マルチメディアリダイレクトの最適化にGPUを使用	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
Windows Mediaフォールバックの防止	未構成	VDA 7.6 FP3以降
Windows Mediaクライアント側コンテンツフェッチ	許可	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
Windows Mediaリダイレクト	許可	すべてのVDAバージョン
Windows Mediaリダイレクトバッファサイズ	5秒	VDA 5、5.5、5.6 FP1から現在まで

名前	デフォルト設定	VDA
Windows Mediaリダイレクトバッファサイズの使用	無効	VDA 5、5.5、5.6 FP1から現在まで

ICA/マルチストリーム接続

名前	デフォルト設定	VDA
UDP経由のオーディオ	許可	マルチセッションOS用VDA 7から現在まで
オーディオUDPポート範囲	16500、16509	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
マルチポートポリシー	プライマリポート (2598) は高優先度です	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
マルチストリームコンピューター設定	無効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
マルチストリームユーザー設定	無効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
マルチストリーム仮想チャネルストリーム割り当て設定	デフォルトのストリーム割り当てについては、マルチストリーム仮想チャネル割り当て設定を参照してください	VDA 2003

ICA/ポートリダイレクト

名前	デフォルト設定	VDA
クライアントCOMポートの自動接続	無効	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します
クライアントLPTポートの自動接続	無効	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します
クライアントCOMポートリダイレクト	禁止	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します
クライアントLPTポートリダイレクト	禁止	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します

ICA/印刷

名前	デフォルト設定	VDA
クライアントプリンターリダイレクト	許可	すべてのVDAバージョン
デフォルトプリンター	デフォルトプリンターをクライアントのメインプリンターに設定する	すべてのVDAバージョン
プリンターの割り当て	ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます	すべてのVDAバージョン
プリンターの自動作成イベントログの優先順位	エラーと警告をログに記録	すべてのVDAバージョン

名前	デフォルト設定	VDA
セッションプリンター	プリンターが指定されていません	すべてのVDAバージョン
プリンターが作成されるまで待機する (デスクトップ)	無効	すべてのVDAバージョン

ICA/印刷/クライアントプリンター

名前	デフォルト設定	VDA
クライアントプリンターを自動作成	すべてのクライアントプリンターを自動作成	すべてのVDAバージョン
汎用ユニバーサルプリンターを自動作成	無効	すべてのVDAバージョン
クライアントプリンター名	標準プリンター名	VDA 5.6
プリントサーバーへの直接接続	有効	すべてのVDAバージョン
プリンタードライバーのマッピングと互換性	ルールは指定されていません	すべてのVDAバージョン
プリンタープロパティの保持	クライアントに保存されていない場合にのみプロファイルに保持	すべてのVDAバージョン
保持および復元されたクライアントプリンター	許可	VDA 5、5,5、5.6 FP1

ICA/Printing/Drivers

名前	デフォルト設定	VDA
インボックスプリンタードライバーの自動インストール	有効	すべてのVDAバージョン
ユニバーサルドライバーの優先順位	EMF; XPS; PCL5c; PCL4; PS	すべてのVDAバージョン

名前	デフォルト設定	VDA
ユニバーサルプリンタードライバーの使用	要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用する	すべてのVDAバージョン

ICA/印刷/ユニバーサルプリントサーバー

名前	デフォルト設定	VDA
ユニバーサルプリントサーバーを有効にする	無効	すべてのVDAバージョン
ユニバーサルプリントサーバー印刷データストリーム (CGP) ポート	7229	すべてのVDAバージョン
ユニバーサルプリントサーバー印刷ストリーム入力帯域幅制限 (kbps)	0	すべてのVDAバージョン
ユニバーサルプリントサーバーWebサービス (HTTP/SOAP) ポート	8080	すべてのVDAバージョン
負荷分散用のUniversal Print Server	VDA バージョン 7.9 から現在まで	
ユニバーサルプリントサーバーのサービス停止しきい値	180 (秒)	VDA バージョン 7.9 から現在まで

ICA/印刷/ユニバーサル印刷

名前	デフォルト設定	VDA
ユニバーサル印刷 EMF 処理モード	プリンターに直接スプール	すべての VDA バージョン
ユニバーサル印刷画像圧縮制限	最高品質 (ロスレス圧縮)	すべての VDA バージョン

名前	デフォルト設定	VDA
ユニバーサル印刷の最適化の既定値	画像圧縮: 希望する画質 = 標準品質、ヘビーウェイト圧縮を有効にする = False; 画像とフォントのキャッシュ: 埋め込み画像のキャッシュを許可する = True; 管理者以外のユーザーがこれらの設定を変更することを許可する = False;	すべてのVDAバージョン
ユニバーサル印刷プレビューの優先設定	自動作成されたプリンターまたは汎用ユニバーサルプリンターには印刷プレビューを使用しない	すべてのVDAバージョン
ユニバーサル印刷の印刷品質制限	制限なし	すべてのVDAバージョン

ICA/セキュリティ

名前	既定の設定	VDA
SecureICAの最小暗号化レベル	基本	マルチセッションOS用VDA 7以降

ICA/サーバー制限

名前	デフォルト設定	VDA
サーバーアイドルタイマー間隔	0ミリ秒	マルチセッションOS用VDA 7以降

ICA/セッション制限

名前	デフォルト設定	VDA
切断されたセッションタイマー	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
リモートPCアクセス切断セッションタイマー	無効	シングルセッションOS用VDA 7以降
切断セッションタイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッション接続タイマー	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッション接続タイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッションアイドルタイマー	有効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッションアイドルタイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降

ICA/セッションの信頼性

名前	デフォルト設定	VDA
セッションの信頼性接続	許可	すべてのVDAバージョン
セッションの信頼性ポート番号	2598	すべてのVDAバージョン
セッションの信頼性タイムアウト	180秒	すべてのVDAバージョン

ICA/タイムゾーン制御

名前	デフォルト設定	VDA
レガシークライアントのローカル時間を推定	有効	マルチセッションOS 7以降のVDA
セッション切断またはログオフ時にシングルセッションOSのタイムゾーンを復元	有効	現在のVDAバージョン
クライアントのローカル時間を使用	サーバーのタイムゾーンを使用	すべてのVDAバージョン

ICA/TWAINデバイス

名前	デフォルト設定	VDA
クライアントTWAINデバイスリダイレクト	許可	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
TWAIN圧縮レベル	中	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/USBデバイス

名前	デフォルト設定	VDA
クライアントUSBデバイス最適化規則	有効 (VDA 7.6 FP3以降); 無効 (VDA 7.11以降); デフォルトでは、規則は指定されていません	VDA 7.6 FP3 以降
クライアントUSBデバイスリダイレクト	禁止	すべてのVDAバージョン
クライアントUSBデバイスリダイレクト規則	規則は指定されていません	すべてのVDAバージョン

名前	デフォルト設定	VDA
クライアントUSBプラグアンドプレイデバイスリダイレクト	許可	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/ビジュアルディスプレイ

名前	デフォルト設定	VDA
単純なグラフィックの優先色深度	24ビット/ピクセル	VDA 7.6 FP3 以降
ターゲットフレームレート	30 フレーム/秒	すべてのVDAバージョン
画質	中	マルチセッションOS 用 VDA 7 以降、シングルセッションOS 用 VDA 7 以降

ICA/ビジュアルディスプレイ/動画

名前	デフォルト設定	VDA
最小画質	標準	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
動画圧縮	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
プログレッシブ圧縮レベル	なし	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
プログレッシブ圧縮しきい値	2,147,483,647 キロビット/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
ターゲット最小フレームレート	10 フレーム/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

注:

「**目標最小フレームレート**」ポリシーは廃止されました。

ICA/視覚表示/静止画像

名前	デフォルト設定	VDA
追加の色圧縮	無効	すべてのVDAバージョン
追加の色圧縮しきい値	8,192 キロビット/秒	すべてのVDAバージョン
高負荷圧縮	無効	すべてのVDAバージョン
非可逆圧縮レベル	中	すべてのVDAバージョン
非可逆圧縮しきい値	2,147,483,647 ケービーピーエス	すべてのVDAバージョン

ICA/WebSockets

名前	デフォルト設定	VDA
WebSockets接続	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
WebSocketsポート番号	8008	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
WebSockets信頼済みオリジンサーバーリスト	ワイルドカード「*」は、すべてのReceiver for Web URLを信頼するために使用されます	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

負荷管理

名前	デフォルト設定	VDA
同時ログオン許容数	2	マルチセッションOS用VDA 7以降
CPU使用率	無効	マルチセッションOS用VDA 7以降
CPU使用率除外プロセス優先度	通常以下または低	マルチセッションOS用VDA 7以降
ディスク使用率	無効	マルチセッションOS用VDA 7以降
セッションの最大数	250	マルチセッションOS用VDA 7以降
メモリ使用量	無効	マルチセッションOS用VDA 7以降
メモリ使用量のベース負荷	ゼロ負荷: 768 MB	マルチセッションOS用VDA 7以降

プロファイル管理/詳細設定

名前	デフォルト設定	VDA
自動構成を無効にする	無効	すべてのVDAバージョン
問題が発生した場合にユーザーをログオフする	無効	すべてのVDAバージョン

名前	デフォルト設定	VDA
ロックされたファイルへのアクセス時の再試行回数	5	すべてのVDAバージョン
ログオフ時にインターネットCookieファイルを処理する	無効	すべてのVDAバージョン

プロファイル管理/基本設定

名前	デフォルト設定	VDA
アクティブライトバック	無効	すべてのVDAバージョン
プロファイル管理を有効にする	無効	すべてのVDAバージョン
除外グループ	無効。すべてのユーザーグループのメンバーが処理されます。	すべてのVDAバージョン
オフラインプロファイルのサポート	無効	すべてのVDAバージョン
ユーザーストアへのパス	ウィンドウズ	すべてのVDAバージョン
ローカル管理者によるログオンの処理	無効	すべてのVDAバージョン
処理されるグループ	無効。すべてのユーザーグループのメンバーが処理されます。	すべてのVDAバージョン

プロファイル管理/クロスプラットフォーム設定

名前	デフォルト設定	VDA
クロスプラットフォーム設定ユーザーグループ	無効。処理済みグループで指定されたすべてのユーザーグループが処理されます	すべてのVDAバージョン

名前	デフォルト設定	VDA
クロスプラットフォーム設定を有効にする	無効	すべてのVDAバージョン
クロスプラットフォーム定義へのパス	無効。パスは指定されていません。	すべてのVDAバージョン
クロスプラットフォーム設定ストアへのパス	無効。Windows\PM_CMが使用されます。	すべてのVDAバージョン
クロスプラットフォーム設定の作成元	無効	すべてのVDAバージョン

プロファイル管理/ファイルシステム/除外

名前	デフォルト設定	VDA
除外リスト - ディレクトリ	無効。ユーザープロファイル内のすべてのフォルダーが同期されます。	すべてのVDAバージョン
除外リスト - ファイル	無効。ユーザープロファイル内のすべてのファイルが同期されます。	すべてのVDAバージョン

プロファイル管理/ファイルシステム/同期

名前	デフォルト設定	VDA
同期するディレクトリ	無効。除外されていないフォルダーのみが同期されます。	すべてのVDAバージョン
同期するファイル	無効。除外されていないファイルのみが同期されます。	すべてのVDAバージョン
ミラーリングするフォルダー	無効。フォルダーはミラーリングされません。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト

名前	デフォルト設定	VDA
管理者アクセスを許可	無効	すべてのVDAバージョン
ドメイン名を含める	無効	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/AppData(Roaming)

名前	デフォルト設定	VDA
AppData(Roaming)パス	無効。場所は指定されていません。	すべてのVDAバージョン
AppData(Roaming)のリダイレクト設定	コンテンツは、AppData(Roaming)パスのポリシー設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/連絡先

名前	デフォルト設定	VDA
連絡先パス	無効。場所は指定されていません。	すべてのVDAバージョン
連絡先のリダイレクト設定	コンテンツは、**連絡先パスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/デスクトップ

名前	デフォルト設定	VDA
デスクトップパス	無効。場所は指定されていません。	すべてのVDAバージョン
デスクトップのリダイレクト設定	コンテンツは、**デスクトップパスポリシー**設定で指定され	すべてのVDAバージョン

名前	デフォルト設定	VDA
	たUNCパスにリダイレクトされます。	

プロファイル管理/フォルダーリダイレクト/ドキュメント

名前	デフォルト設定	VDA
ドキュメントパス	無効。場所は指定されていません。	すべてのVDAバージョン
ドキュメントのリダイレクト設定	コンテンツは、**ドキュメントパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ダウンロード

名前	デフォルト設定	VDA
ダウンロードパス	無効。場所は指定されていません。	すべてのVDAバージョン
ダウンロードのリダイレクト設定	コンテンツは、**ダウンロードパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/お気に入り

名前	デフォルト設定	VDA
お気に入りパス	無効。場所は指定されていません。	すべてのVDAバージョン
お気に入りのリダイレクト設定	コンテンツは、**お気に入りパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/リンク

名前	デフォルト設定	VDA
リンクパス	無効。場所は指定されていません。	すべてのVDAバージョン
リンクのリダイレクト設定	コンテンツは、**リンクパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ミュージック

名前	デフォルト設定	VDA
ミュージックパス	無効。場所は指定されていません。	すべてのVDAバージョン
音楽のリダイレクト設定	コンテンツは、**音楽パスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/画像

名前	デフォルト設定	VDA
画像パス	無効。場所は指定されていません。	すべてのVDAバージョン
画像のリダイレクト設定	コンテンツは、**画像パスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/保存されたゲーム

名前	デフォルト設定	VDA
保存されたゲームパス	無効。場所は指定されていません。	すべてのVDAバージョン
保存されたゲームのリダイレクト設定	コンテンツは、「**保存されたゲームパスポリシー**」設定で	すべてのVDAバージョン

名前	デフォルト設定	VDA
	指定されたUNCパスにリダイレクトされます	

プロファイル管理/フォルダーリダイレクト/検索

名前	デフォルト設定	VDA
検索パス	無効。場所は指定されていません。	すべてのVDAバージョン
検索のリダイレクト設定	コンテンツは、**検索パスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/スタートメニュー

名前	デフォルト設定	VDA
スタートメニューパス	無効。場所は指定されていません。	すべてのVDAバージョン
スタートメニューのリダイレクト設定	コンテンツは、スタートメニューパスポリシー設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ビデオ

名前	デフォルト設定	VDA
ビデオパス	無効。場所は指定されていません。	すべてのVDAバージョン
ビデオのリダイレクト設定	コンテンツは、**ビデオパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/ログ設定

名前	デフォルト設定	VDA
Active Directory のアクション	無効	すべてのVDAバージョン
一般情報	無効	すべてのVDAバージョン
一般的な警告	無効	すべてのVDAバージョン
ログの有効化	無効	すべてのVDAバージョン
ファイルシステムのアクション	無効	すべてのVDAバージョン
ファイルシステム通知	無効	すべてのVDAバージョン
ログオフ	無効	すべてのVDAバージョン
ログオン	無効	すべてのVDAバージョン
ログファイルの最大サイズ	1048576	すべてのVDAバージョン
ログファイルへのパス	無効。ログファイルはデフォルトの場所 (%SystemRoot%\System32\Logfiles\UserProfileManager) に保存されます。	すべてのVDAバージョン
パーソナライズされたユーザー情報	無効	すべてのVDAバージョン
ログオン時とログオフ時のポリシー値	無効	すべてのVDAバージョン
レジストリアクション	無効	すべてのVDAバージョン
ログオフ時のレジストリの相違点	無効	すべてのVDAバージョン

プロファイル管理/プロファイルの処理

名前	デフォルト設定	VDA
キャッシュされたプロファイルを削除するまでの遅延	0	すべてのVDAバージョン
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効	すべてのVDAバージョン
ローカルプロファイルの競合処理	ローカルプロファイルを使用する	すべてのVDAバージョン
既存のプロファイルの移行	ローカルおよびローミング	すべてのVDAバージョン
テンプレートプロファイルへのパス	無効。新しいユーザープロファイルは、ユーザーが最初にログオンするデバイスのデフォルトユーザープロファイルから作成されます。	すべてのVDAバージョン
テンプレートプロファイルがローカルプロファイルを上書きする	無効	すべてのVDAバージョン
テンプレートプロファイルが移動プロファイルを上書きする	無効	すべてのVDAバージョン
テンプレートプロファイルは、すべてのログオンでCitrix®必須プロファイルとして使用される	無効	すべてのVDAバージョン

プロファイル管理/レジストリ

名前	デフォルト設定	VDA
除外リスト	無効。ユーザーがログオフすると、HKCUハイブ内のすべてのレジストリキーが処理されます。	すべてのVDAバージョン

名前	デフォルト設定	VDA
インクルージョンリスト	無効。ユーザーがログオフすると、HKCUハイブ内のすべてのレジストリキーが処理されます。	すべてのVDAバージョン

プロファイル管理/ストリーム配信ユーザープロファイル

名前	デフォルト設定	VDA
常にキャッシュ	無効	すべてのVDAバージョン
常にキャッシュサイズ	0 MB	すべてのVDAバージョン
プロファイルストリーミング	無効	すべてのVDAバージョン
ストリーミングされたユーザープロファイルグループ	無効。OU内のすべてのユーザープロファイルは通常どおり処理されます。	すべてのVDAバージョン
保留中のエリアロックファイルのタイムアウト (日数)	1日	すべてのVDAバージョン

レシーバー

名前	デフォルト設定	VDA
StoreFront™アカウントリスト	ストアは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ユーザーパーソナライゼーションレイヤー

名前	デフォルト設定	VDA
ユーザーレイヤーリポジトリパス	無効。パスは指定されていません。	VDA 19.12以降のバージョン
ユーザーレイヤーサイズ (GB)	10 GB。ユーザーレイヤーは、設定されたサイズまで拡張するシンプロビジョニング	VDA 19.12以降のバージョン

名前	デフォルト設定	VDA
	ディスクです。ユーザーレイヤーのサイズが小さくなることはありません。	

仮想デリバリーエージェント

名前	デフォルト設定	VDA
コントローラー登録IPv6ネットマスク	ネットマスクは指定されていません	VDA for マルチセッションOS 7以降、VDA for シングルセッションOS 7以降
コントローラ登録ポート	80	すべてのVDAバージョン
コントローラSID	SIDは指定されていません	すべてのVDAバージョン
コントローラ	コントローラは指定されていません	すべてのVDAバージョン
コントローラの自動更新を有効にする	有効	VDA for マルチセッションOS 7以降、VDA for シングルセッションOS 7以降
IPv6コントローラ登録のみを使用する	無効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
サイトGUID	GUIDは指定されていません	すべてのVDAバージョン

仮想デリバリーエージェント/HDX 3D Pro

名前	デフォルト設定	VDA
ロスレスを有効にする	有効	VDA 5.5、5.6 FP1
HDX 3D Pro品質設定	VDA 5.5、5.6 FP1	

仮想配信エージェント/監視

名前	既定の設定	VDA
プロセス監視を有効にする	無効	VDA 7.11以降
リソース監視を有効にする	有効	VDA 7.11以降

仮想IP

名前	既定の設定	VDA
仮想IPループバックのサポート	無効	VDA 7.6から現在まで
仮想IP仮想ループバックプログラムリスト	なし	VDA 7.6 から現在まで

ポリシー設定リファレンス

ポリシーには、ポリシーが適用される際に適用される設定が含まれています。このセクションの説明では、機能を有効にするためにより多くの設定が必要かどうか、または設定と類似しているかどうかも示されています。

クイックリファレンス

以下の表に、ポリシー内で構成できる設定を示します。左の列で完了したいタスクを見つけ、右の列で対応する設定を見つけてください。

.CHM (コンパイル済みHTML) 形式および .CSV 形式で、すべてのポリシー設定の完全なリストが利用可能です。これらのファイルは、ブローカー (デリバリーコントローラー) がインストールされているサーバーの `\program files\citrix\grouppolicy` フォルダーにあります。ポリシー設定の最新バージョンは、こちらをクリックしてダウンロードすることもできます。

オーディオ

このタスクの場合	このポリシー設定を使用する
複数のオーディオデバイスの使用を許可するかどうかを制御する	オーディオプラグアンドプレイ

このタスクの場合	このポリシー設定を使用する
ユーザーデバイスのマイクからのオーディオ入力を許可するかどうかを制御する	クライアントマイクのリダイレクト
ユーザーデバイスのオーディオ品質を制御する	オーディオ品質
ユーザーデバイスのスピーカーへのオーディオマッピングを制御する	クライアントオーディオリダイレクト

ユーザーデバイスの帯域幅

～に使用される帯域幅を制限するには	このポリシー設定を使用します
クライアントオーディオマッピング	オーディオリダイレクト帯域幅制限またはオーディオリダイレクト帯域幅制限パーセント
ローカルクリップボードを使用したカットアンドペースト	クリップボードリダイレクト帯域幅制限またはクリップボードリダイレクト帯域幅制限パーセント
セッションでのローカルクライアントドライブへのアクセス	ファイルリダイレクト帯域幅制限またはファイルリダイレクト帯域幅制限パーセント
HDX™ MediaStreamマルチメディアアクセラレーション	HDX MediaStreamマルチメディアアクセラレーション帯域幅制限またはHDX MediaStreamマルチメディアアクセラレーション帯域幅制限パーセント
クライアントセッション	全体的なセッション帯域幅制限
印刷	プリンターリダイレクト帯域幅制限 または プリンターリダイレクト帯域幅制限率
TWAINデバイス (カメラやスキャナーなど)	TWAINデバイスリダイレクト帯域幅制限 または TWAINデバイスリダイレクト帯域幅制限率
USBデバイス	クライアントUSBデバイスリダイレクト帯域幅制限 または クライアントUSBデバイスリダイレクト帯域幅制限率

クライアントドライブとユーザーデバイスのリダイレクト

このタスクの場合	このポリシー設定を使用する
ユーザーがサーバーにログオンしたときに、ユーザーデバイス上のドライブを接続するかどうかを制御します	クライアントドライブの自動接続
サーバーとローカルクリップボード間のカットアンドペーストデータ転送を制御します	クライアントクリップボードリダイレクト
ユーザーデバイスからドライブがどのようにマップされるかを制御します	クライアントドライブリダイレクト
ユーザーのローカルハードドライブがセッションで利用可能かどうかを制御します	クライアント固定ドライブとクライアントドライブのリダイレクト
ユーザーのローカルフロッピーディスクドライブがセッションで利用可能かどうかを制御します	クライアントフロッピーディスクドライブとクライアントドライブのリダイレクト
ユーザーのネットワークドライブがセッションで利用可能かどうかを制御します	クライアントネットワークドライブとクライアントドライブのリダイレクト
ユーザーのローカルCD、DVD、またはBlu-rayドライブがセッションで利用可能かどうかを制御します	クライアント光学ドライブとクライアントドライブのリダイレクト
ユーザーのローカルリムーバブルドライブがセッションで利用可能かどうかを制御します	クライアントリムーバブルドライブとクライアントドライブのリダイレクト
ユーザーのスキャナーやカメラなどのTWAINデバイスがセッションで利用可能かどうか、および画像データ転送の圧縮を制御します	クライアントTWAINデバイスのリダイレクト。TWAIN圧縮のリダイレクト
USBデバイスがセッションで利用可能かどうかを制御します	クライアントUSBデバイスのリダイレクトとクライアントUSBデバイスのリダイレクト規則
WAN経由でクライアントディスクへのファイルの書き込みとコピーの速度を向上させます	非同期書き込みを使用します

コンテンツリダイレクト

このタスクの場合	このポリシー設定を使用
サーバーからユーザーデバイスへのコンテンツリダイレクトを使用するかどうかを制御します	ホストからクライアントへのリダイレクト

デスクトップUI

このタスクの場合	このポリシー設定を使用
ユーザーセッションでデスクトップの壁紙を使用するかどうかを制御します	デスクトップの壁紙
ウィンドウのドラッグ中にウィンドウの内容を表示	ドラッグ中のウィンドウの内容を表示

グラフィックとマルチメディア

重要:

Flashポリシーは、古いVDAを使用しているお客様が新しいコントローラー（バージョン1912コントローラーなど）を使用し、引き続きFlashを使用できるようにするためにのみ残されています。このVDAバージョンはFlashをサポートしていません。

このタスクの場合	このポリシー設定を使用します
仮想デスクトップからユーザーデバイスに送信される1秒あたりの最大フレーム数を制御します	ターゲットフレームレート
ユーザーデバイスに表示される画像の視覚品質を制御します	視覚品質
セッションでアクセスされたときにWebサイトがFlashコンテンツを表示できるかどうかを制御します	Flashサーバー側コンテンツ取得URLリスト。Flash URL互換性リスト。Flashビデオフォールバック防止ポリシー設定。Flashビデオフォールバック防止エラー *.swf

このタスクの場合	このポリシー設定を使用します
サーバーでレンダリングされたビデオの圧縮を制御します	圧縮にビデオコーデックを使用する。ビデオコーデックにハードウェアエンコードを使用する
HTML5マルチメディアWebコンテンツのユーザーへの配信を制御します	HTML5ビデオのリダイレクト

マルチストリームネットワークトラフィックの優先順位付け

このタスクの場合	このポリシー設定を使用します
複数の接続にわたるICA®トラフィックのポートを指定し、ネットワークの優先順位を確立します。	マルチポートポリシー
サーバーとユーザーデバイス間のマルチストリーム接続のサポートを有効にします。	マルチストリーム (コンピューターとユーザーの設定)

印刷

このタスクの場合	このポリシー設定を使用
ユーザーデバイスでのクライアントプリンターの作成を制御する	クライアントプリンターの自動作成とクライアントプリンターのリダイレクト
プリンタープロパティが保存される場所を制御する	プリンタープロパティの保持
クライアントまたはサーバーのどちらが印刷要求を処理するかを制御する	印刷サーバーへの直接接続
ユーザーが自分のユーザーデバイスに接続されているプリンターにアクセスできるかどうかを制御する	クライアントプリンターのリダイレクト
クライアントプリンターとネットワークプリンターを自動作成する際のネイティブWindowsドライバーのインストールを制御する	インボックスプリンタードライバーの自動インストール

このタスクの場合	このポリシー設定を使用
ユニバーサルプリンタードライバーを使用するタイミングを制御する	ユニバーサルプリントドライバーの使用状況
ローミングユーザーセッション情報に基づいてプリンターを選択する	デフォルトプリンター
ユニバーサルプリントサーバーの負荷分散とフェイルオーバーしきい値の設定	負荷分散のためのユニバーサルプリントサーバー。ユニバーサルプリントサーバーのサービス停止しきい値

注：

デスクトップまたはアプリケーションセッションでスクリーンセーバーを有効にするためにポリシーを使用することはできません。スクリーンセーバーを必要とするユーザーの場合、スクリーンセーバーはユーザーデバイスに実装できます。

ICA® ポリシー設定

注:

このページでは、ICAポリシー設定の説明とサポートされている構成値を提供します。ポリシーの操作に関する詳細については、「ポリシーの操作」セクションを参照してください。

アダプティブトランスポート

この設定により、EDTをプライマリ、TCPをフォールバックとしてデータ転送を許可または防止します。

デフォルトでは、アダプティブトランスポートは有効（**優先**）になっており、可能な場合はEDTが使用され、TCPにフォールバックします。必要に応じて設定を変更できます。

- **優先**。可能な場合はEDT経由のアダプティブトランスポートが使用され、TCPにフォールバックします。
- **診断モード**。EDTが強制的にオンになり、TCPへのフォールバックは無効になります。この設定はトラブルシューティングにのみ推奨されます。

- **オフ**。TCPが強制的にオンになり、EDTは無効になります。

詳細については、「アダプティブトランスポート」を参照してください。

ドラッグアンドドロップ設定

この設定により、クライアントと仮想アプリケーションまたはデスクトップ間でのファイルのドラッグを許可または防止します。デフォルトでは、ドラッグアンドドロップポリシーは無効になっています。必要に応じて、このポリシーを有効にできます。

アプリケーション起動待機タイムアウト

この設定は、セッションが最初のアプリケーションの起動を待機するミリ秒単位の待機タイムアウト値を指定します。アプリケーションの起動がこの期間を超えると、セッションは終了します。

デフォルトの時間（10,000ミリ秒）を選択するか、ミリ秒単位の数値を指定できます。

クライアントクリップボードリダイレクト

この設定により、ユーザーデバイス上のクリップボードがサーバー上のクリップボードにマッピングされることを許可または禁止します。

デフォルトでは、クリップボードのリダイレクトは許可されています。

セッションとローカルクリップボード間のコピー＆ペーストデータ転送を禁止するには、**禁止**を選択します。ユーザーは、セッション内で実行されているアプリケーション間では引き続きデータをコピー＆ペーストできます。

この設定を許可した後、クライアント接続でクリップボードが消費できる最大許容帯域幅を構成します。**クリップボードリダイレクト帯域幅制限**または**クリップボードリダイレクト帯域幅制限率**の設定を使用します。

クライアントクリップボード書き込み許可形式

クライアントクリップボード書き込みの制限設定が**有効**の場合、ホストクリップボードデータはクライアントエンドポイントと共有できません。この設定を使用して、特定のデータ形式をクライアントエンドポイントクリップボードと共有することを許可できます。この設定を使用するには、これを有効にして、許可する特定の形式を追加します。

次のクリップボード形式はシステム定義です。

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT

- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

XenApp and XenDesktopおよびCitrix Virtual Apps and Desktops™には、以下のカスタム形式が事前定義されています。

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- CFX_FILE

HTML形式はデフォルトで無効になっています。この機能を有効にするには:

- **クライアントクリップボードリダイレクト**が**許可**に設定されていることを確認します。
- **クライアントクリップボード書き込みの制限**が**有効**に設定されていることを確認します。

- **クライアントクリップボード書き込み許可形式**に**CF_HTML**（およびサポートしたいその他の形式）のエントリを追加します。

カスタム形式をさらに追加できます。カスタム形式名は、システムに登録される形式と一致している必要があります。形式名は大文字と小文字を区別します。

この設定は、**クライアントクリップボードリダイレクト**ポリシーが**禁止**に設定されている場合、または**クライアントクリップボード書き込みの制限**ポリシーが**無効**に設定されている場合には適用されません。

> **注:**
>
> HTML形式のクリップボードコピーサポート（CF_HTML）を有効にすると、コピーされたコンテンツのソースから宛先にスクリプトがコピーされます。コピーを進める前に、ソースを信頼できることを確認してください。スクリプトを含むコンテンツをコピーした場合、それらは宛先ファイルをHTMLファイルとして保存して実行した場合にのみ有効になります。

クリップボードのクライアントからセッションへの転送サイズを制限する

この設定は、ユーザーが単一のコピー＆ペースト操作中にクライアントエンドポイントから仮想セッションに転送できるクリップボードデータの最大サイズを指定します。

クリップボード転送サイズを制限するには、**Limit clipboard client to session transfer size** 設定を有効にします。次に、**Size Limit** フィールドにキロバイト単位の値を入力して、ローカルクリップボードとセッション間のデータ転送サイズを定義します。

既定では、この設定は無効になっており、クライアントからセッションへの転送に制限はありません。

HDX™ ダイレクト

HDX Direct を使用すると、直接通信が可能な場合に、クライアントがセッションホストとの直接接続を自動的に確立できます。接続は、ネットワークレベルの暗号化を使用して安全に確立されます。

HDX Direct モード

HDX Directは、内部クライアントおよび外部クライアントのセッションホストとの直接接続を確立するために使用できます。この設定は、HDX Directが内部クライアントのみに利用可能か、内部クライアントと外部クライアントの両方に利用可能かを決定します。

内部のみに設定されている場合、HDX Direct は内部ネットワーク内のクライアントに対してのみ直接接続を確立しようとします。

Internal および **external** に設定されている場合、HDX Directは内部クライアントと外部クライアントの両方に対して直接接続を確立しようとします。

既定では、HDX Direct は内部クライアントのみに設定されています。

HDX Direct ポート範囲

外部ユーザーからの接続に HDX Direct が使用するポートの範囲です。 既定では、HDX Direct はポート範囲 55000～55250 を使用します。

クリップボードセッションからクライアントへの転送サイズを制限する

この設定は、ユーザーが単一のコピー＆ペースト操作中に仮想セッションからクライアントエンドポイントに転送できるクリップボードデータの最大サイズを指定します。

クリップボード転送サイズを制限するには、**Limit clipboard session to client transfer size** 設定を有効にします。次に、**Size Limit** フィールドにキロバイト単位の値を入力して、セッションとローカルクリップボード間のデータ転送サイズを定義します。

既定では、この設定は無効になっており、セッションからクライアントへの転送に制限はありません。

クライアントクリップボードへの書き込みを制限する

この設定が**有効**になっている場合、ホストのクリップボードデータはクライアントエンドポイントと共有できません。**クライアントクリップボードへの書き込み許可形式**設定を有効にすることで、特定の形式を許可できます。

デフォルトでは、この設定は**無効**です。

セッションクリップボードへの書き込みを制限する

この設定が**有効**になっている場合、クライアントのクリップボードデータはセッションアプリケーションと共有できません。**セッションクリップボードへの書き込み許可形式**設定を有効にすることで、特定の形式を許可できます。

デフォルトでは、この設定は**無効**です。

セッションクリップボード書き込み許可形式

セッションクリップボードへの書き込みを制限する設定が**有効**になっている場合、クライアントのクリップボードデータはセッションアプリケーションと共有できません。この設定を使用して、特定のデータ形式をセッションクリップボードと共有することを許可できます。

以下のクリップボード形式はシステム定義です。

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

XenAppおよびXenDesktop、Citrix Virtual Apps and Desktopsでは、以下のカスタム形式が事前定義されています。

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

HTML形式はデフォルトで無効になっています。この機能を有効にするには：

- **クライアントクリップボードリダイレクト**が**許可**に設定されていることを確認します。
- **セッションクリップボード書き込みの制限**が**有効**に設定されていることを確認します。
- **セッションクリップボード書き込み許可形式**に**CF_HTML**（およびサポートしたいその他の形式）のエントリを追加します。

カスタム形式を追加できます。カスタム形式名は、システムに登録される形式と一致している必要があります。形式名は大文字と小文字を区別します。

この設定は、**クライアントクリップボードリダイレクト**ポリシーが**禁止**に設定されている場合、または**セッションクリップボード書き込みの制限**ポリシーが**無効**に設定されている場合には適用されません。

> **注:**
>
> HTML形式のクリップボードコピーサポート（CF_HTML）を有効にすると、コピーされたコンテンツのソースから宛先にスクリプトがコピーされます。コピーを続行する前に、ソースを信頼できることを確認してください。スクリプトを含むコンテンツをコピーした場合、それらは宛先ファイルをHTMLファイルとして保存して実行した場合にのみ有効になります。

デスクトップの起動

この設定は、VDA Direct Access Usersグループの非管理者ユーザーがICA接続を使用してそのVDA上のセッションに接続することを許可または禁止します。

デフォルトでは、非管理者ユーザーはこれらのセッションに接続できません。

この設定は、RDP接続を使用しているVDA Direct Access Usersグループの非管理者ユーザーには影響しません。これらのユーザーは、この設定が有効または無効になっている場合でもVDAに接続できます。この設定は、VDA Direct Access Usersグループに属していない非管理者ユーザーには影響しません。これらのユーザーは、この設定が有効または無効になっている場合でもVDAに接続できません。

FIDO2リダイレクト

この設定は、FIDO2リダイレクトを有効または無効にします。FIDO2リダイレクトにより、ユーザーは仮想マシン内のローカルエンドポイントFIDO2コンポーネントを利用できます。ユーザー

は、TPM 2.0とWindows Helloを搭載したデバイスで、FIDO2セキュリティキーまたは統合された生体認証を介して仮想セッションを認証できます。

この設定が**許可**されている場合、ユーザーはローカルエンドポイント機能を使用してFIDO2認証を行うことができます。デフォルトでは、この設定は**許可**されています。

ICAリスナー接続タイムアウト

この設定は、ICAプロトコルを使用した接続が完了するまでの最大待機時間を指定します。

デフォルトでは、最大待機時間は120,000ミリ秒、つまり2分です。

ICAリスナーポート番号

この設定は、サーバー上でICAプロトコルが使用するTCP/IPポート番号を指定します。

デフォルトでは、ポート番号は1494に設定されています。

有効なポート番号は0～65535の範囲で、他の既知のポート番号と競合してはなりません。ポート番号を変更した場合は、新しい値を有効にするためにサーバーを再起動してください。サーバーのポート番号を変更した場合は、そのサーバーに接続するすべてのCitrix Workspace™アプリまたはプラグインでも変更する必要があります。

キーボードと入力方式エディター (IME)

この設定は、次の項目を有効または無効にします。

- 動的キーボードレイアウト同期
- 入力方式エディター (IME)
- Unicode キーボードレイアウトマッピング
- キーボードレイアウト切り替え通知ダイアログメッセージを非表示または表示します

1. Web Studioで、**キーボードとIME**を選択します。
2. VDAでの動的なキーボードレイアウト同期と汎用クライアント入力方式エディター (IME) 機能を制御するには、**クライアントキーボードレイアウトの同期とIMEの改善**を選択します。設定できる項目は次のとおりです。

   無効 - 動的なキーボードレイアウト同期と汎用クライアント入力方式エディター (IME)。

   動的なクライアントキーボードレイアウト同期をサポート - 動的なキーボードレイアウト同期を有効にします。

動的クライアントキーボードレイアウト同期とIMEの改善をサポート - 動的キーボードレイアウト同期と汎用クライアント入力方式エディター (IME) の両方を有効にします。

3. **Unicodeキーボードレイアウトマッピングを有効にする**を選択して、Unicodeキーボードマッピングを有効または無効にします。
4. **キーボードレイアウト切り替えポップアップメッセージボックスを非表示にする**を選択して、ユーザーがクライアントキーボードレイアウトを変更したときに、キーボードレイアウトが同期中であることを示すメッセージを表示するかどうかを制御します。メッセージが表示されないようにすると、ユーザーは誤った文字入力にならないように、入力する前に数秒待つ必要があります。

デフォルト設定：

- **クライアントキーボードレイアウト同期とIMEの改善**
  - Windows Server 2016およびWindows Server 2019では無効です。
  - 動的なクライアントキーボードレイアウトの同期と、Windows Server 2012 および Windows 2010 でのIMEの改善をサポートします。
- **Unicodeキーボードレイアウトマッピングを無効にする**
- **キーボードレイアウト切り替えポップアップメッセージボックスを表示する**

このポリシーは、ポリシー設定の**説明**セクションに記載されているレジストリ設定を置き換えます。

ログオフチェッカーの起動遅延

この設定は、ログオフチェッカーの起動を遅延させる期間を指定します。このポリシーを使用して、クライアントセッションがセッションを切断するまでに待機する時間（秒単位）を設定します。

この設定は、ユーザーがサーバーからログオフするのにかかる時間も増加させます。

ロス耐性モード

> **重要:**
>
> - この機能には、Windows 用 Citrix Workspace アプリ 2002 以降が必要です。VDA のこのバージョンは、利用可能になった時点でこれをサポートします。

- グラフィックのロス耐性モードは、Citrix Gateway および Citrix Gateway Service でサポートされています。このモードは、直接接続でのみ利用可能です。

この設定は、グラフィックのロス耐性モードを有効または無効にします。

デフォルトでは、グラフィックのロス耐性モードは**許可**されています。

許可されている場合、パケット損失と遅延がしきい値を超えると、このモードに入ります。ロス耐性しきい値ポリシーを使用して、しきい値を設定できます。

ロス耐性しきい値

ロストレラントモードが利用可能な場合、この設定は、グラフィックのロストレラントモードにセッションが切り替わるネットワークメトリックのしきい値を指定します。

デフォルトのしきい値は次のとおりです。

- パケット損失: 5%
- 遅延: 300 ms (RTT)

詳細については、ロストレラントモードを参照してください。

オーディオのロストレラントモード

この設定は、オーディオのロストレラントモードを有効または無効にします。

有効にすると、オーディオはロストレラントモードで送信されます。

デフォルトでは、オーディオのロストレラントモードは**禁止**されています。

ポリシーを有効にするには、オーディオポリシーのロストレラントモードのレジストリを**許可**に編集します。

オーディオのロストレラントモードを有効にするには、EDTトランスポートが必要です。

Rendezvous プロトコル

この設定は、Citrix Gateway Serviceを使用する際のHDXセッションのプロキシ方法を変更します。有効にすると、HDXトラフィックはCitrix Cloud Connectorを経由しなくなります。代わりに、VDAはCitrix Gateway Serviceに直接アウトバウンド接続を確立します（Cloud Connectorのスケーラビリティが向上します）。

重要:

Citrix Cloud™の機能トグルとHDXポリシー設定がこの機能を制御します。Citrix Cloudの機能トグルはデフォルトで有効になっていますが、HDX設定はデフォルトで無効になっています。HDX設定は、Citrix Gateway Serviceを介して確立されたHDXセッションにのみ影響します。この設定は、クライアントとVDA間で直接確立されたセッションや、オンプレミスのCitrix Gatewayを介して確立されたセッションには影響しません。

詳細については、Rendezvous protocolを参照してください。

Rendezvousプロキシの構成

この設定では、Rendezvousプロトコルで使用する明示的なプロキシを構成できます。透過プロキシを使用している場合、この設定を有効にする必要はありません。

デフォルトでは、この設定は無効になっています。

無効にすると、VDAはGateway ServiceとのRendezvous接続を確立しようとするときに、非透過プロキシを介して送信トラフィックをルーティングしません。

有効にすると、VDAは、この設定で定義されたプロキシを介してGateway ServiceとのRendezvous接続を確立しようとします。

VDAは、Rendezvous接続にHTTPおよびSOCKS5プロキシの使用をサポートしています。Rendezvous接続にプロキシを使用するようにVDAを構成するには、この設定を有効にする必要があります。また、プロキシのアドレスまたはPACファイルへのパスを指定します。例：

- プロキシアドレス：`http://<URL or IP>:<port>` または `socks5://<URL or IP>:<port>`
- PACファイル：`http://<URL or IP>/<path>/<filename>.pac`

  VDAバージョン2103は、PACファイルを使用したプロキシ構成でサポートされる最小バージョンです。SOCKS5プロキシのPACファイルスキーマの詳細については、Proxy configurationを参照してください。

注：

SOCKS5プロキシのみがEDTを介したデータ転送をサポートします。HTTPプロキシの場合、ICAのトランスポートプロトコルとしてTCPを使用します。

> 詳細については、Rendezvous protocolを参照してください。

クライアント接続中の公開されていないプログラムの起動

この設定は、サーバー上でRDPを介して初期アプリケーションの起動を許可するかどうかを指定します。

既定では、サーバー上のRDPを介した初期アプリケーションの起動は許可されていません。

セッションメトリックの収集

この設定により、Citrix は VDA と Workspace 間のユーザーおよびマシンセッションメトリックを収集し、ユーザーエクスペリエンスを向上させることができます。

オペレーティングシステム、稼働時間、コンピューターシステム情報、ビデオコントローラーの詳細、VDA バージョン、展開タイプ、ドメイン参加ステータスなどのデータが収集されます。さらに、製品改善の取り組みを支援するために、いくつかのセッション構成、パフォーマンスおよび信頼性データを収集できます。カスタマーエクスペリエンス向上プログラムの詳細については、以下を参照してください。

- `<https://more.citrix.com/XD-CEIP>`
- `<https://docs.citrix.com/ja-jp/linux-virtual-delivery-agent/current-release/configure/administration/linux-vda-data-collection-program>`
- `<https://docs.citrix.com/ja-jp/mac-vda/configure/session/supportability-service>`

デフォルトでは、この設定は有効になっています。

タブレットモード切り替えポリシー設定

タブレットモード切り替えは、VDA上のストアアプリ、Win32アプリ、およびWindowsシェルンの外観と動作を最適化します。これは、電話やタブレットなどの小型フォームファクターデバイス、または任意のタッチ対応デバイスから接続する際に、仮想デスクトップを自動的にタブレットモードに切り替えることによって行われます。

このポリシーが無効になっている場合、VDAはユーザーが設定したモードになり、クライアントの種類に関係なく、そのモードを維持します。

自動クライアント再接続ポリシー設定

自動クライアント再接続セクションには、セッションの自動再接続を制御するためのポリシー設定が含まれています。

自動クライアント再接続

この設定は、接続が中断された後に同じクライアントによる自動再接続を許可または防止します。

Citrix Receiver for Windows 4.7以降およびCitrix Workspaceアプリ1808以降では、自動クライアント再接続はCitrix Studioのポリシー設定のみを使用します。Studioでこれらのポリシーを更新すると、自動クライアント再接続がサーバーからクライアントに同期されます。以前のバージョンのCitrix Receiver for Windowsで自動クライアント再接続を構成するには、Studioポリシーを使用し、レジストリまたはdefault.icaファイルを変更します。

自動クライアント再接続を許可すると、接続が切断されたときに中断された場所からユーザーが作業を再開できるようになります。自動再接続は、切断された接続を検出し、ユーザーをセッションに再接続します。

セッションIDと資格情報へのキーを含むCitrix Workspace™アプリのCookieが使用されない場合、自動再接続によって新しいセッションが開始される可能性があります。つまり、既存のセッションに再接続するのではなく、新しいセッションが開始されます。Cookieは、有効期限が切れている場合は使用されません。たとえば、再接続の遅延や、資格情報の再入力が必要な場合などにCookieの有効期限が切れることがあります。ユーザーが意図的に切断した場合、自動クライアント再接続はトリガーされません。

再接続が進行中の場合、セッションウィンドウはグレー表示されます。カウントダウンタイマーは、セッションが再接続されるまでの残り時間を表示します。セッションがタイムアウトすると、切断されます。

アプリケーションセッションの場合、自動再接続が許可されていると、通知領域にカウントダウンタイマーが表示されます。このタイマーは、セッションが再接続されるまでの残り時間を指定します。Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルするまで、セッションへの再接続を試みます。

ユーザーセッションの場合、自動再接続が許可されていると、Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルしない限り、指定された期間セッションへの再接続を試みます。デフォルトでは、この期間は2分です。この期間を変更するには、ポリシーを編集します。

デフォルトでは、自動クライアント再接続は許可されています。ポリシーを**禁止**に設定することで無効にできます。

自動クライアント再接続認証

この設定は、自動クライアント再接続に認証が必要かどうかを指定します。

ユーザーが最初にログオンすると、資格情報は暗号化され、メモリに保存され、暗号化キーを含むCookieが作成されます。CookieはCitrix Workspaceアプリに送信されます。この設定が構成されている場合、Cookieは使用されません。代わりに、Citrix Workspaceアプリが自動的に再接続を試みるときに、資格情報を要求するダイアログボックスがユーザーに表示されます。

デフォルトでは、認証は不要です。

自動クライアント再接続ログ

この設定は、イベントログへの自動クライアント再接続の記録を有効または無効にします。

ログ記録が有効な場合、サーバーのシステムログは、成功および失敗した自動再接続イベントに関する情報をキャプチャします。サイトは、すべてのサーバーの再接続イベントの結合されたログを提供しません。

デフォルトでは、ログ記録は無効です。

自動クライアント再接続のタイムアウト

デフォルトでは、自動クライアント再接続のタイムアウトは120秒に設定されており、自動クライアント再接続のタイムアウトの最大設定可能値は300秒です。このポリシーを使用してタイムアウト値を設定します。

再接続UIの透明度レベル

この設定により、セッションの信頼性再接続中にXenAppまたはXenDesktop®セッションウィンドウに適用される不透明度レベルを指定できます。

デフォルトでは、再接続UIの透明度は80%に設定されています。

オーディオポリシー設定

オーディオセクションには、パフォーマンスを低下させることなく、ユーザーデバイスがセッションでオーディオを送受信できるようにするポリシー設定が含まれています。

アダプティブオーディオ

この設定は、アダプティブオーディオを有効または無効にします。このポリシーを有効にすると、最高のユーザーエクスペリエンスを提供するためにオーディオ品質設定が動的に調整されます。この設定は、Citrix Virtual Apps and Desktops™ 2109以降を使用するVDAのシングルセッションOSおよびマルチセッションOSセッションの両方に適用されます。

この設定が禁止されている場合、オーディオ品質ポリシーが適用されます。詳細については、「オーディオ品質」を参照してください。

デフォルトでは、アダプティブオーディオポリシーは有効になっています。

UDPリアルタイムトランスポート経由のオーディオ

この設定は、User Datagram Protocol (UDP) を使用してRTP経由でVDAとユーザーデバイス間でオーディオを送受信することを許可または禁止します。この設定が無効になっている場合、オーディオはTCP経由で送受信されます。

デフォルトでは、UDP経由のオーディオは許可されています。

オーディオプラグアンドプレイ

この設定は、複数のオーディオデバイスを使用してサウンドを録音および再生することを許可または禁止します。

デフォルトでは、複数のオーディオデバイスの使用は許可されています。

この設定は、WindowsマルチセッションOSマシンにのみ適用されます。

オーディオ品質

この設定は、ユーザーセッションで受信されるサウンドの品質レベルを指定します。

デフォルトでは、音質は高 - 高精細オーディオに設定されています。

サウンド品質を制御するには、次のいずれかのオプションを選択します。

- 低 - 低帯域幅接続の低速接続用に選択します。ユーザーデバイスに送信されるサウンドは最大16 Kbpsに圧縮されます。この圧縮により、音質が大幅に低下します。しかし、低帯域幅接続でも妥当なパフォーマンスを可能にします。
- 中 - 音声に最適化されており、Voice over Internet Protocolアプリケーションを提供します。この設定は、512 Kbps未満の回線、または著しい輻輳やパケット損失があるような困難なネットワーク接続でメディアアプリケーションを配信します。このコーデックはエンコード時間が高速であるため、サーバー側のメディア処理が必要な場合にソフトフォンやユニファイドコミュニケーションアプリケーションでの使用に最適です。

  ユーザーデバイスに送信されるオーディオは、最大64 Kbpsに圧縮されます。この圧縮により、ユーザーデバイスで再生されるオーディオの品質は中程度に低下しますが、低遅延で低帯域幅の消費を実現します。Voice over Internet Protocolの品質が不十分な場合は、「Audio over UDP Real-time Transport」ポリシー設定が「許可」に設定されていることを確認してください。

現在、UDP経由のリアルタイムトランスポート（RTP）は、このオーディオ品質が選択されている場合にのみサポートされます。低速（512 Kbps未満）回線のような困難なネットワーク接続でメディアアプリケーションを配信する場合でも、このオーディオ品質を使用してください。また、ネットワークに輻輳やパケット損失がある場合も同様です。

- 高 - 帯域幅が豊富で音質が重要な接続には、高精細オーディオを選択します。クライアントはネイティブレートでサウンドを再生できます。サウンドはCD品質まで維持される高音質レベルで圧縮され、最大112 Kbpsの帯域幅を使用します。この量のデータを送信すると、CPU使用率の増加やネットワーク輻輳が発生する可能性があります。

帯域幅は、オーディオの録音中または再生中にのみ消費されます。両方が同時に発生する場合、帯域幅の消費量は2倍になります。

最大帯域幅を指定するには、**オーディオリダイレクト帯域幅制限**または**オーディオリダイレクト帯域幅制限パーセント**設定を構成します。

クライアントオーディオリダイレクト

この設定は、サーバーでホストされているアプリケーションが、ユーザーデバイスにインストールされているサウンドデバイスを介してサウンドを再生できるかどうかを指定します。この設定は、ユーザーがオーディオ入力を録音できるかどうかも指定します。

デフォルトでは、オーディオリダイレクトは許可されています。

この設定を許可した後、オーディオの再生または録音によって消費される帯域幅を制限できます。オーディオによって消費される帯域幅の量を制限すると、アプリケーションのパフォーマンスが向上する可能性がありますが、オーディオ品質が低下する可能性もあります。帯域幅は、オーディオの録音中または再生中にのみ消費されます。両方が同時に発生する場合、帯域幅の消費量は2倍になります。最大帯域幅を指定するには、**オーディオリダイレクト帯域幅制限**または**オーディオリダイレクト帯域幅制限パーセント**設定を構成します。

WindowsマルチセッションOSマシンでは、複数のオーディオデバイスをサポートするために、**オーディオプラグアンドプレイ**設定が有効になっていることを確認してください。

重要：クライアントオーディオリダイレクトを禁止すると、すべてのHDX™オーディオ機能が無効になります。

クライアントマイクのリダイレクト

この設定は、クライアントマイクのリダイレクトを有効または無効にします。有効にすると、ユーザーはセッションでマイクを使用してオーディオ入力を録音できます。

デフォルトでは、マイクのリダイレクトは許可されています。

セキュリティのため、信頼されていないサーバーがデバイスを介してマイクにアクセスしようとすると、ユーザーに警告が表示されます。ユーザーはアクセスを許可するかどうかを選択できます。ユーザーはCitrix Workspace™アプリでこの警告を無効にできます。

WindowsマルチセッションOSマシンでは、複数のオーディオデバイスをサポートするために、オーディオプラグアンドプレイ設定が有効になっていることを確認してください。

ユーザーデバイスで**クライアントオーディオリダイレクト**設定が無効になっている場合、このルールは無効になります。

帯域幅ポリシー設定

「**帯域幅**」セクションには、クライアントセッションの帯域幅使用に関連するパフォーマンスの問題を回避するためのポリシー設定が含まれています。

重要: これらのポリシー設定を**マルチストリームポリシー**設定と組み合わせて使用すると、予期しない結果が生じる可能性があります。ポリシーでマルチストリーム設定を使用する場合は、これらの帯域幅制限ポリシー設定が含まれていないことを確認してください。

オーディオリダイレクト帯域幅制限

この設定は、ユーザーセッションでオーディオを再生または録音するために許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**オーディオリダイレクト帯域幅制限（パーセント）**設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

オーディオリダイレクト帯域幅制限（パーセント）

この設定は、オーディオの再生または録音のために許可される最大帯域幅制限を、総セッション帯域幅のパーセンテージとして指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**オーディオリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

クライアントUSBデバイスリダイレクト帯域幅制限

この設定は、クライアントとの間でUSBデバイスをリダイレクトするために許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**クライアントUSBデバイスリダイレクト帯域幅制限（パーセント）**設定の両方に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

クライアントUSBデバイスリダイレクトの帯域幅制限（パーセント）

この設定は、クライアントとの間でUSBデバイスをリダイレクトするために許可される最大帯域幅を、総セッション帯域幅のパーセンテージとして指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**クライアントUSBデバイスリダイレクト帯域幅制限**設定の両方に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

クリップボードリダイレクト帯域幅制限

この設定は、セッションとローカルクリップボード間のデータ転送に許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**クリップボードリダイレクト帯域幅制限（パーセント）**設定の両方に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

クリップボードリダイレクトの帯域幅制限（パーセント）

この設定は、セッションとローカルクリップボード間のデータ転送に許可される最大帯域幅を、総セッション帯域幅のパーセンテージとして指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**クリップボードリダイレクト帯域幅制限**設定の両方に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

COMポートリダイレクトの帯域幅制限

> **注:**
>
> Virtual Delivery Agent 7.0～7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、クライアント接続でCOMポートにアクセスするために許可される最大帯域幅を1秒あたりのキロビット単位で指定します。この設定の値と、**COMポートリダイレクト帯域幅制限（パーセント）**設定の値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

COMポートリダイレクトの帯域幅制限（パーセント）

注：Virtual Delivery Agent 7.0～7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、クライアント接続でCOMポートにアクセスするために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定の値と、**COMポートリダイレクト帯域幅制限**設定の値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合は、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

ファイルリダイレクト帯域幅制限

この設定は、ユーザーセッションでクライアントドライブにアクセスするために許可される最大帯域幅を指定します。許可される最大帯域幅は、1秒あたりのキロビット単位で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定の値と、**ファイルリダイレクト帯域幅制限（パーセント）**設定の値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

ファイルリダイレクトの帯域幅制限（パーセント）

この設定は、クライアントドライブへのアクセスに許可される最大帯域幅制限を、セッション全体の帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**ファイルリダイレクト帯域幅制限**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

HDX™ MediaStream マルチメディアアクセラレーション帯域幅制限

この設定は、HDX MediaStream マルチメディアアクセラレーションを使用してストリーミングオーディオおよびビデオを配信するために許可される最大帯域幅制限を指定します。許可される最大帯域幅はキロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**HDX MediaStream マルチメディアアクセラレーション帯域幅制限の割合**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

HDX MediaStream マルチメディアアクセラレーション帯域幅制限の割合

この設定は、HDX MediaStream マルチメディアアクセラレーションを使用してストリーミングオーディオおよびビデオを配信するために許可される最大帯域幅を、セッション全体の帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**HDX MediaStream マルチメディアアクセラレーション帯域幅制限**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

LPTポートリダイレクト帯域幅制限

注：Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、単一ユーザーセッションでLPTポートを使用する印刷ジョブに許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と、**LPTポートリダイレクト帯域幅制限の割合**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

LPTポートリダイレクト帯域幅制限の割合

注：Virtual Delivery Agent 7.0から7.8では、レジストリを使用してこの設定を構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、単一のクライアントセッションでLPTポートを使用する印刷ジョブの帯域幅制限を、セッション全体の帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と、**LPTポートリダイレクト帯域幅制限**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

セッション全体の帯域幅制限

この設定は、ユーザーセッションで利用可能な総帯域幅を、1秒あたりのキロビット単位で指定します。

強制可能な最大帯域幅は20 Mbps（20,000 Kbps）です。デフォルトでは、最大値（ゼロ）は指定されていません。

クライアント接続によって消費される帯域幅の量を制限すると、クライアント接続外の他のアプリケーションが限られた帯域幅を競合している場合に、パフォーマンスが向上する可能性があります。

プリンターリダイレクト帯域幅制限

この設定は、ユーザーセッションでクライアントプリンターにアクセスするために許可される最大帯域幅を指定します。許可される最大帯域幅は、1秒あたりのキロビット単位で指定されます。

デフォルトでは、最大値 (ゼロ) は指定されていません。

この設定に値を入力し、**プリンターリダイレクト帯域幅制限の割合**設定にも値を入力した場合、最も制限の厳しい設定 (値が小さい方) が適用されます。

プリンターリダイレクトの帯域幅制限（パーセント）

この設定は、クライアントプリンターにアクセスするために許可される最大帯域幅を、総セッション帯域幅の割合として指定します。

デフォルトでは、最大値 (ゼロ) は指定されていません。

この設定に値を入力し、**プリンターリダイレクト帯域幅制限**設定にも値を入力した場合、最も制限の厳しい設定 (値が小さい方) が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

TWAINデバイスリダイレクト帯域幅制限

この設定は、公開アプリケーションからTWAINイメージングデバイスを制御するために許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値 (ゼロ) は指定されていません。

この設定に値を入力し、**TWAINデバイスリダイレクト帯域幅制限の割合**設定にも値を入力した場合、最も制限の厳しい設定 (値が小さい方) が適用されます。

TWAINデバイスリダイレクト帯域幅制限の割合

この設定は、公開アプリケーションからTWAINイメージングデバイスを制御するために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値 (ゼロ) は指定されていません。

この設定に値を入力し、**TWAINデバイスリダイレクト帯域幅制限**設定にも値を入力した場合、最も制限の厳しい設定 (値が小さい方) が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**Overall session bandwidth limit** 設定も構成する必要があります。

双方向コンテンツリダイレクトポリシー設定

「**双方向コンテンツリダイレクト**」セクションには、クライアントからVDAへのURLリダイレクトとVDAからクライアントへのURLリダイレクトを有効または無効にするポリシー設定があります。

サーバーポリシーはWeb Studioで設定されます。Citrix Workspace™ appバージョン2311以降、この設定は、Web Studioで非推奨となった以下の3つのレガシー設定に代わるものです。

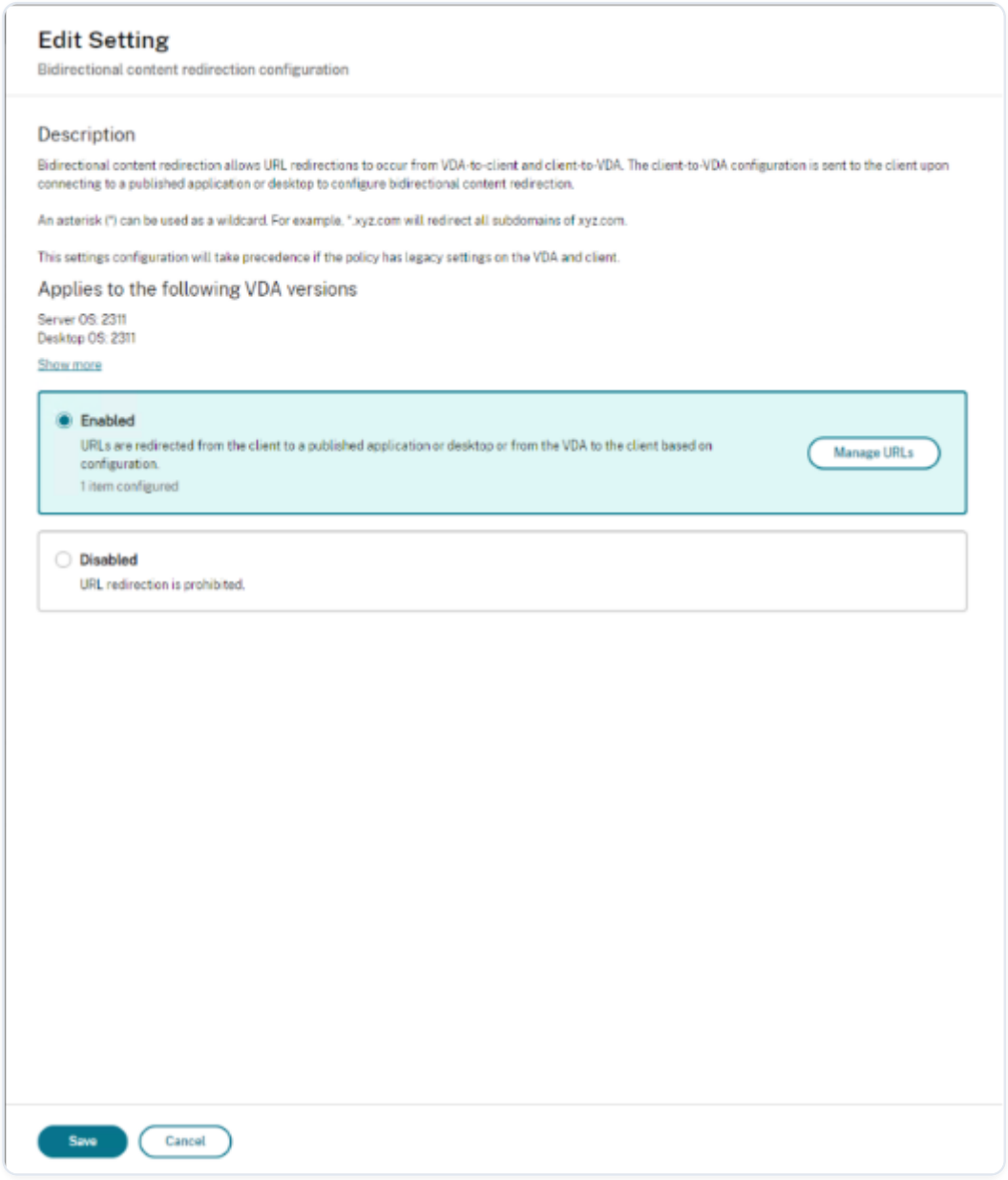
- 双方向コンテンツリダイレクトを許可する

- VDAにリダイレクトされる許可されたURL
- クライアントにリダイレクトされる許可されたURL

また、Windowsクライアント上の以下の3つのローカルGroup Policy Object (GPO) 設定も置き換えます。

- 双方向コンテンツリダイレクト
- 双方向コンテンツリダイレクトのオーバーライド
- OAuthリダイレクト

この設定が有効になっている場合、公開アプリケーションまたはデスクトップへの接続時に、双方向コンテンツリダイレクトを構成するためのクライアントからVDAへの設定がクライアントに送信されます。



この設定が構成されている場合、Web Studioおよびクライアントのレガシー設定よりも優先されます。Citrix®は、予期しない動作を避けるために、新しいポリシー設定のみを使用し、レガシー設定を削除することを推奨します。

VDAとDDCがバージョン2311以降を実行している場合、クライアントポリシーを設定してはなりません。そうでない場合、クライアントポリシーはCitrix Workspace appグループポリシーオブジェクト管理テンプレートから設定されます。

Citrixは、クライアントからURLへのリダイレクトのために、ホストからクライアントへのリダイレクトとローカルアプリアクセスを提供しています。ただし、Citrixは、ドメイン参加済みWindowsクライアントには双方向コンテンツリダイレクトを使用することを推奨します。

Citrix は、Desktop Studio の代わりに Web Studio の新しい UI を使用して機能を構成することを推奨します。

ワイルドカードリダイレクト

双方向コンテンツリダイレクトは、リダイレクトする URL を定義する際にワイルドカードの使用をサポートします。詳細および双方向コンテンツリダイレクトの構成については、構成 の手順を参照してください。 Web Studio で、`hostToClientUrls` 配列または `clientToHostUrls` 配列内の `url` キーの値として JSON 文字列を編集して、ワイルドカード URL を設定します。

> **注:**
>
> - 無限ループを避けるため、`hostToClientUrls` と `clientToHostUrls` に同じ URL を設定しないでください。
> - トップレベルドメインはサポートされていません。たとえば、`<https://www.citrix.*>` や `<http://www.citrix.co*>` はリダイレクトされません。

双方向コンテンツリダイレクトの構成

このポリシーを `Enabled` に設定して機能の構成を開始し、**URL の管理** をクリックします。次の構成を設定します:

- **VDA からクライアントへのリダイレクト**
- **クライアントから VDA へのリダイレクト**

VDA からクライアントへのリダイレクト

VDA からクライアントに URL をリダイレクトするには、1 行に 1 つの URL を入力します。ワイルドカードが許可されます。 OAuth リダイレクトを使用すると、クライアントエンドポイント上のブラウザを使用して認証を実行し、トークンを VDA に送り返すことができます。

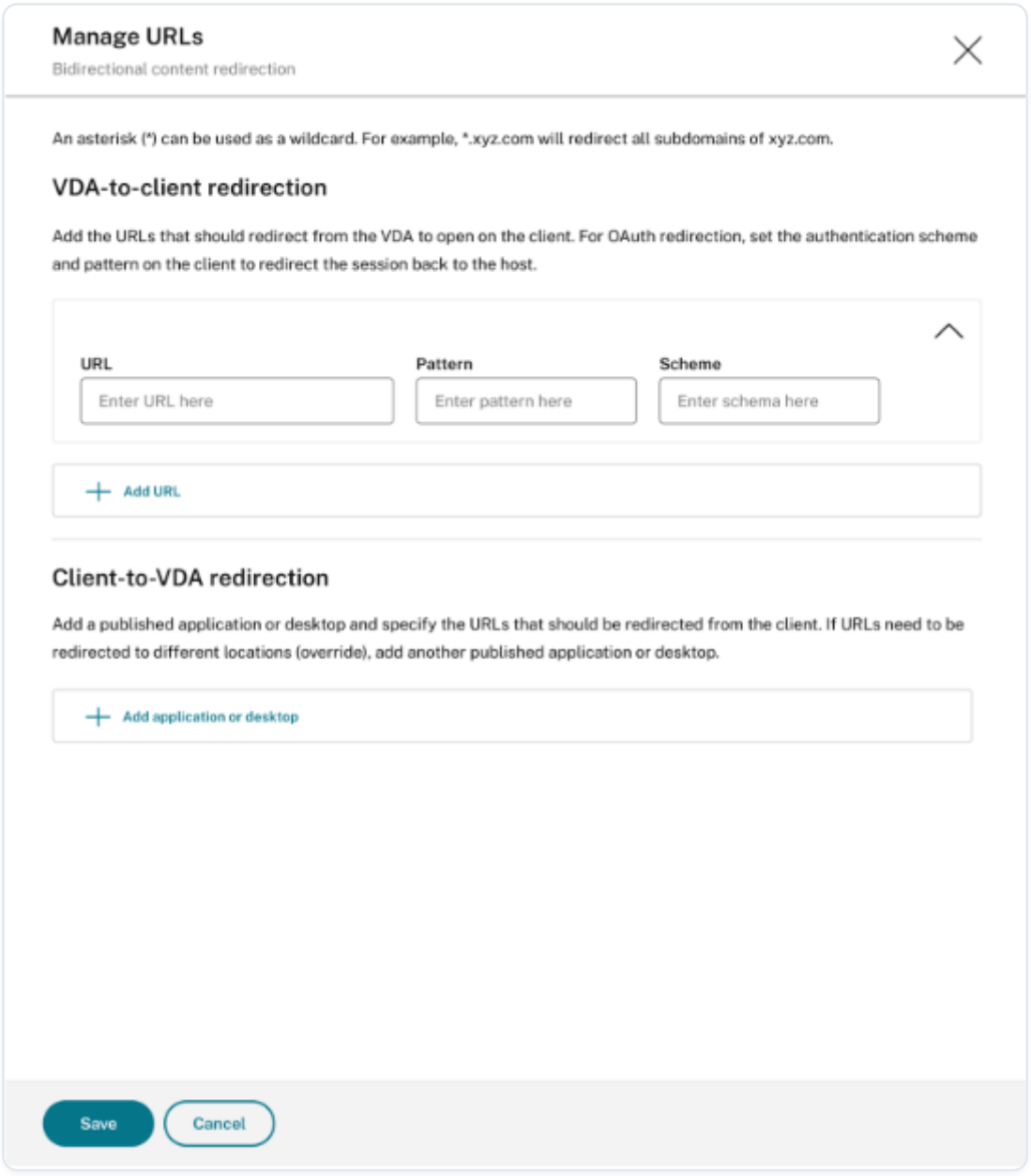
利点:

- ホストされた環境にこれらの資格情報を保存することを避けることができます。
- VDA ではなく、エンドポイントで利用可能な生体認証機能を使用できます。

構成：

URL の VDA からクライアントへのリダイレクトを構成するには、以下を指定します:

- **URL** (必須) VDA からクライアントで開くようにリダイレクトする必要がある URL を追加します。**OAuth リダイレクト**の場合、セッションをホストにリダイレクトするために、クライアントで認証スキームとパターンを設定します。
- **パターン**: (オプション) VDA からクライアントへの URL リダイレクトを介してクライアントにリダイレクトされたときに、OAuth 認証フローが開始されたかのように追跡され、フローが完了したとき（結果のスキームまたはリダイレクト URL パターンが開かれたことによって検出される）、その結果の URL がそのフローを開始したホスト VDA にリダイレクトされる URL 正規表現。
- **スキーム**: (オプション) **スキーム**が指定されている場合、終了 URL は `<scheme>`:// `<something>` の形式であると想定されます。スキームが指定されていない（空である）とします。その場合、元の結果の URL パターンは、正規表現キャプチャグループ（パターンで指定する必要がある）を介してパターンから抽出され、元の URL は `citrix-oauth-redir://` リダイレクト URL を使用するように書き換えられます。フローが完了すると、元のリダイレクト URL はホスト (VDA) にリダイレクトされます。この場合、OAuth 認証サーバーは `citrix-oauth-redir://byIndex/1 (2, 3, ... N)` リダイレクト URL を許可するように構成する必要があります。



注:

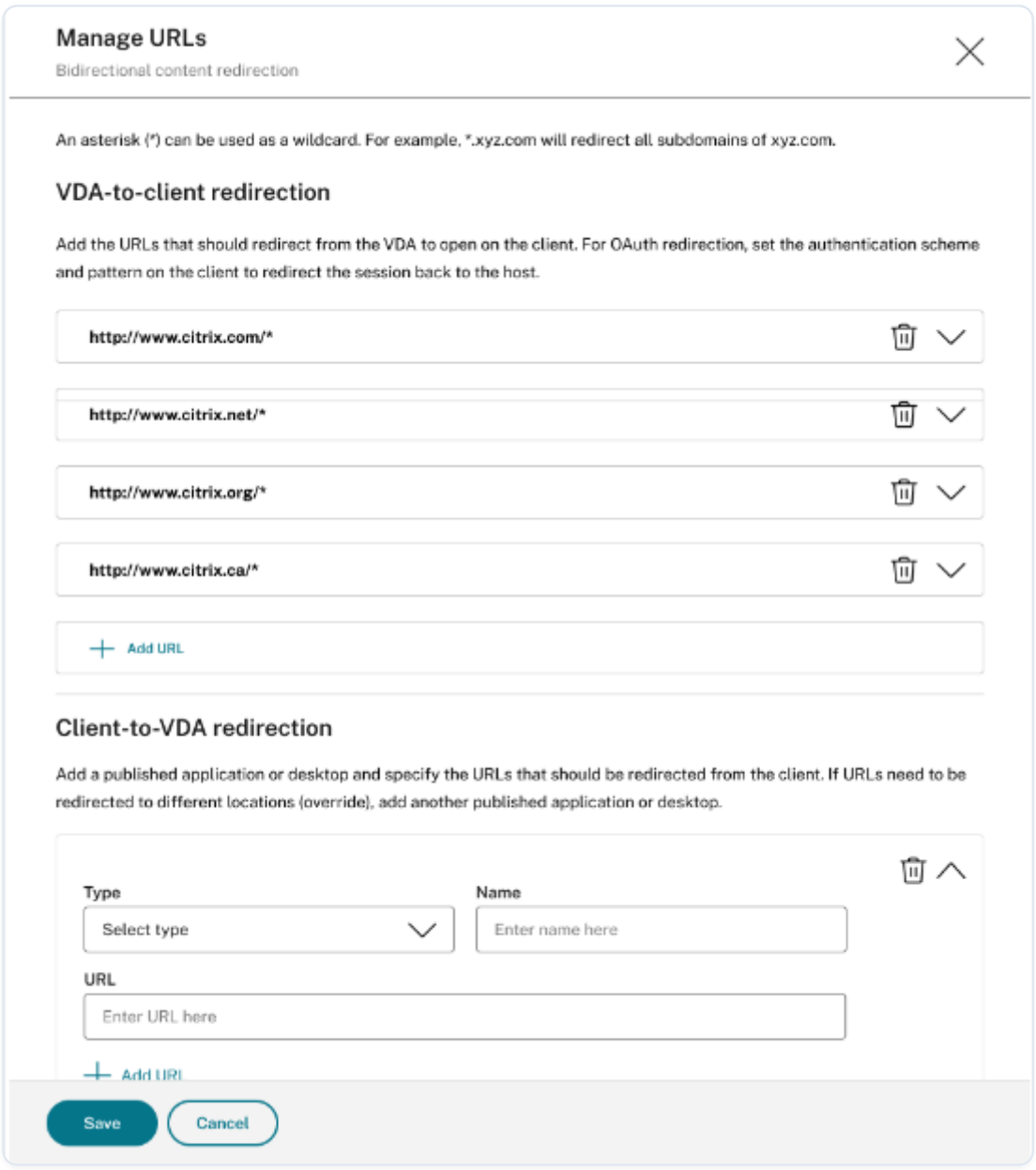
パターンと**スキーム**はどちらもオプションですが、**パターン**が指定されている場合は、**スキーム**も指定する必要があります。

クライアントからVDAへのリダイレクト

クライアントから VDA に URL をリダイレクトするには、次の手順を実行します:

1. クライアントURLの宛先を構成します。
2. 公開アプリケーションまたは公開デスクトップのいずれかを選択します。
3. そのリソースの名前を指定します。

4. そのリソースにリダイレクトする必要があるすべてのURLを追加します。 新しいアプリケーションまたはデスクトップを追加し、そのリソースにリダイレクトするURLを指定することで、このデフォルトのリソースを上書きできます。



デスクトップスタジオ

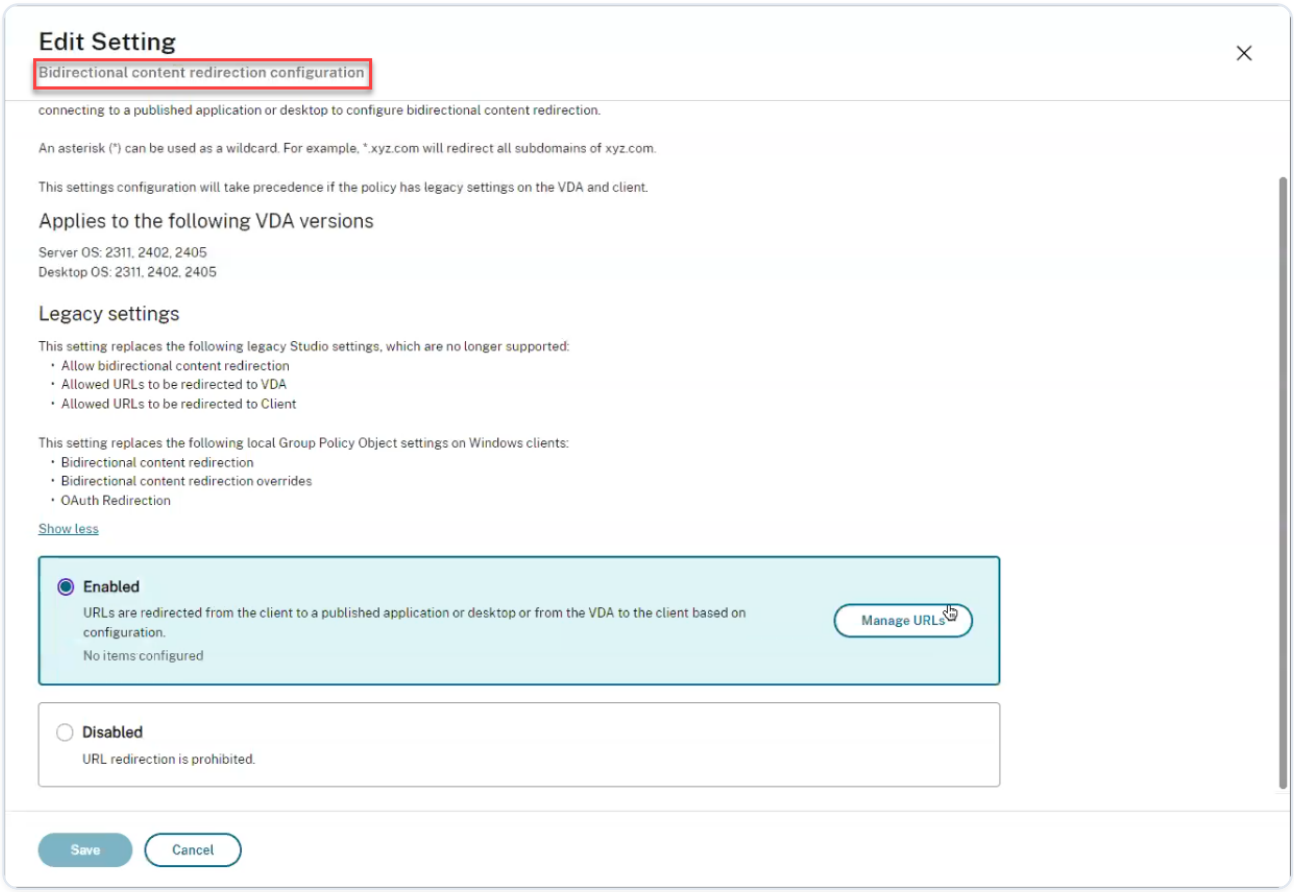
注:

Citrix Virtual Apps and Desktops™ バージョン 2402 以降では、Web Studio を使用してこの機能を構成することをお勧めします。

2311 の双方向コンテンツリダイレクトを構成するには、次の形式で JSON 文字列を作成します。

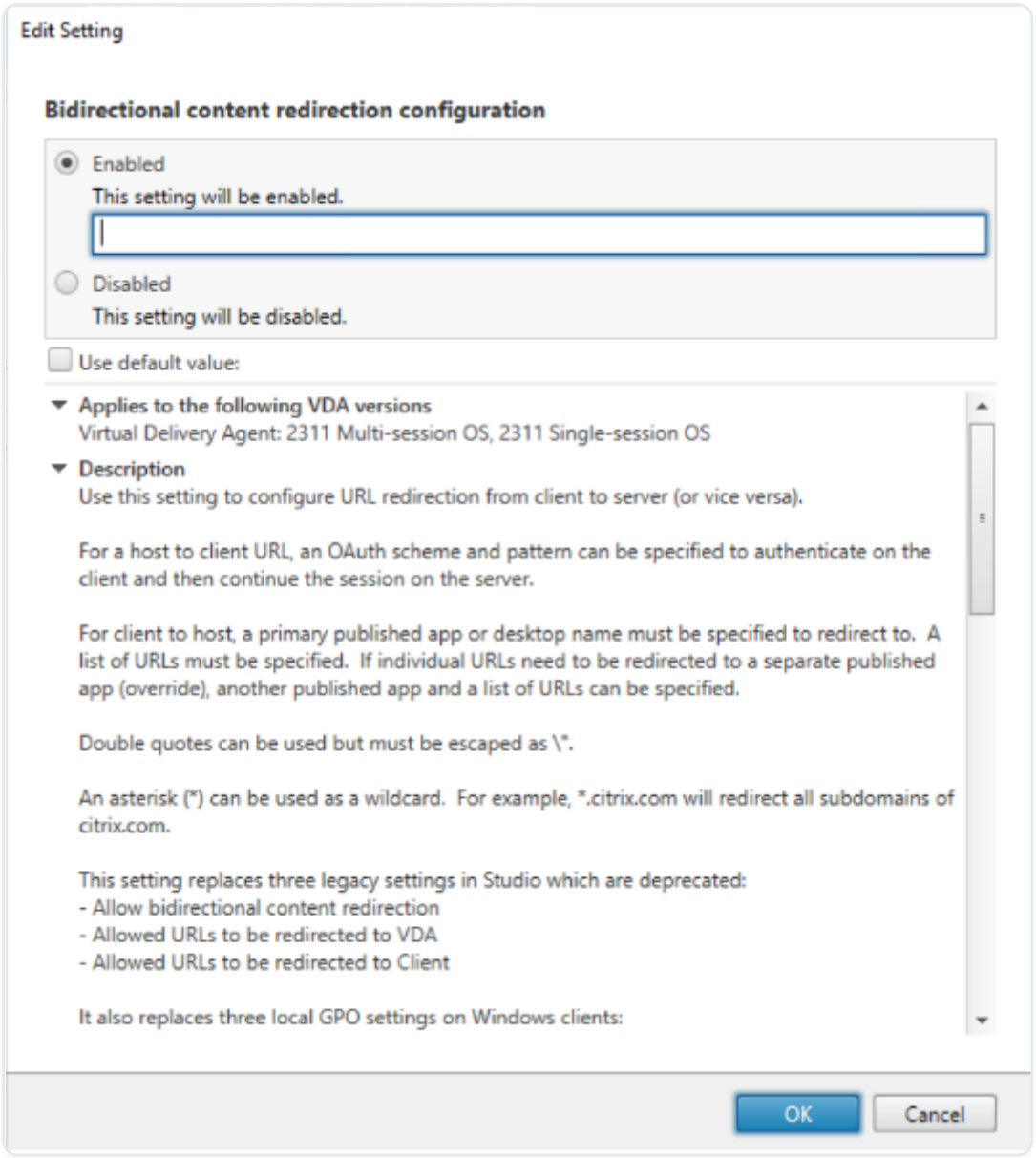
```
{
  "version": 1,
  "hostToClientConfig": [
    {
      "hostToClientUrls": [
        {
          "url": "http://www.citrix.com/*"
        },
        {
          "url": "www.example.com"
        },
        {
          "url": "https://login.example.org/*",
          "oAuthRedirectionPattern": "https://login.example.org/
oauth2?.*",
          "oAuthScheme": "idm.desktop-authentication"
        }
      ]
    }
  ],
  "clientToHostConfig": [
```

```
    {
      "publishedAppOrDesktopNameType": "Desktop",
      "publishedAppOrDesktopName": "Win11Desktop",
      "clientToHostUrls": [
        "https://www.example.net",
        "https://*.citrix.example"
      ]
    },
    {
      "publishedAppOrDesktopNameType": "Application",
      "publishedAppOrDesktopName": "Chrome",
      "clientToHostUrls": [
        "https://tibco.example"
      ]
    }
  ]
}
```



次のパラメーターを設定する必要があります。

- **version**: (必須) 1 に設定します。
- VDA からクライアントへの URL リダイレクトの場合、単一の `hostToClientConfig` を作成します。
- **hostToClientUrls**: (必須) ホスト (VDA) からクライアントにリダイレクトされる URL のリスト。ワイルドカードが許可されます。'*' が指定されている場合、`clientToHostConfig` は `publishedAppOrDesktopNameType`、空の `publishedAppOrDesktopName`、および空の `clientToHostUrls` とともに指定する必要があります。



OAuth リダイレクト

OAuth リダイレクトを使用すると、クライアントエンドポイントブラウザを使用して認証し、トークンを VDA に送り返すことができます。

利点:

- これらの資格情報をホストされた環境に保存することを回避できます。
- エンドポイントで利用可能で、VDA では利用できない生体認証機能を使用できます。

URLのOAuthリダイレクトを構成するには、次のパラメーターを指定します。

- **oAuthRedirectionPattern**: (オプション) VDAからクライアントへのURLリダイレクトを介してクライアントにリダイレクトされたときに、OAuth認証フローが開始されたかのように追跡され、フローが完了したとき（結果のスキームまたはリダイレクトURLパターンが開かれたこ

とによって検出される）、その結果のURLがそのフローを開始したホストVDAにリダイレクトされるURL正規表現。

- **oAuthScheme**: (オプション) スキームが指定されている場合、終了URLは`<scheme>`://`<something>`の形式であると想定されます。スキームが指定されていない（空である）とします。その場合、元の結果URLパターンは、正規表現キャプチャグループ（パターンで指定する必要がある）を介してパターンから抽出され、元のURLは`citrix-oauth-redir://`リダイレクトURLを使用するように書き換えられます。フローが完了すると、元のリダイレクトURLはホスト（VDA）にリダイレクトされます。この場合、OAuth認証サーバーは`citrix-oauth-redir://byIndex/1 (2, 3, ... N)`リダイレクトURLを許可するように構成する必要があります。

クライアントからVDAへのリダイレクトの場合、リダイレクトするリソースごとに**clientToHostConfig**を作成します。 各リソースには、次のパラメーターを含めます。

- **publishedAppOrDesktopNameType**: (必須) Web Studioで構成された公開デスクトップ（「Desktop」）または公開アプリケーション（「Application」）のいずれか。リソースが無効な場合、リダイレクトは正しく機能しません。
- **publishedAppOrDesktopName**: (必須) Web Studioで構成されたリソース名。
- **clientToHostUrls**: (必須) クライアントからホスト（VDA）にリダイレクトされるURLのリスト。ワイルドカードが許可されます。

既知の制限

PowerShellを使用してカスタムURLスキーム（HTTPまたはHTTPSではない）でブラウザーを起動すると、カスタムURLはクライアントにリダイレクトされません。

クライアントセンサーポリシー設定

クライアントセンサーセクションには、ユーザーセッションでモバイルデバイスのセンサー情報を処理する方法を制御するためのポリシー設定が含まれています。

アプリケーションによるクライアントデバイスの物理的な位置情報の使用を許可する

この設定は、モバイルデバイス上のセッションで実行されているアプリケーションが、ユーザーデバイスの物理的な位置情報を使用できるかどうかを決定します。

デフォルトでは、位置情報の使用は禁止されています。

この設定が禁止されている場合、アプリケーションが位置情報を取得しようとすると、「アクセス拒否」の値が返されます。

この設定が許可されている場合、ユーザーはCitrix Workspace™ appからの位置情報へのアクセス要求を拒否することで、位置情報の使用を禁止できます。AndroidおよびiOSデバイスは、各セッションで位置情報が最初に要求されたときにプロンプトを表示します。

「アプリケーションによるクライアントデバイスの物理的な位置情報の使用を許可する」設定を使用するホスト型アプリケーションを開発する際は、以下を考慮してください。

- 位置情報が有効なアプリケーションが位置情報に依存しないようにしてください。その理由は次のとおりです。
  - ユーザーが位置情報へのアクセスを許可しない場合があります。
  - アプリケーションの実行中に位置情報が利用できない場合や、変更される場合があります。
  - ユーザーが位置情報をサポートしない別のデバイスからアプリケーションセッションに接続する場合があります。
- 位置情報が有効なアプリケーションは、次の条件を満たす必要があります。
  - 位置情報機能をデフォルトでオフにする。
  - アプリケーションの実行中に、ユーザーが機能を許可または禁止するオプションを提供する。
  - アプリケーションがキャッシュする位置情報をクリアするオプションをユーザーに提供します。(Citrix Workspaceアプリは位置情報をキャッシュしません。)
- 位置情報対応アプリケーションは、位置情報の粒度を管理する必要があります。この管理により、取得されたデータがアプリケーションの目的に適切であることが保証されます。また、関連するすべての管轄区域の規制に準拠します。
- 位置情報サービスを使用する際は、安全な接続（TLSやVPNの使用など）を強制します。Citrix Workspaceアプリを信頼できるサーバーに接続します。
- 位置情報サービスの使用に関して、法的助言を得ることを検討してください。

デスクトップUIポリシー設定

デスクトップUIセクションには、デスクトップの壁紙、メニューアニメーション、ドラッグイメージなどの視覚効果を制御するポリシー設定が含まれています。これらのポリシー設定は、クライアント接続で使用される帯域幅の管理に役立ちます。帯域幅の使用を制限することで、WANでのアプリケーションパフォーマンスを向上させることができます。

> **重要:**

このリリースでは、レガシーグラフィックモードおよびデスクトップコンポジションリダイレクト (DCR) はサポートされていません。このポリシーは、以下を使用する場合の旧バージョンとの互換性のためだけに含められています。

- XenApp 7.15 LTSR
- XenDesktop 7.15 LTSR
- Windows 7およびWindows 2008 R2を搭載した以前のVDAリリース。

デスクトップコンポジションリダイレクト

この設定は、ユーザーによりスムーズなWindowsデスクトップエクスペリエンスを提供するために、ローカルDirectXグラフィックレンダリングに以下の処理機能を使用するかどうかを指定します。

- ユーザーデバイス上のグラフィック処理ユニット（GPU）
- または、,
- ユーザーデバイス上の統合グラフィックプロセッサ（IGP）

有効にすると、**デスクトップコンポジションリダイレクト**は、サーバーの高いスケーラビリティを維持しながら、応答性の高いWindowsエクスペリエンスを提供します。

デフォルトでは、**デスクトップコンポジションリダイレクト**は無効になっています。

デスクトップコンポジションリダイレクトの選択を解除し、ユーザーセッションで必要な帯域幅を削減するには、この設定をポリシーに追加する際に**無効**を選択します。

デスクトップコンポジションリダイレクトのグラフィック品質

この設定は、デスクトップコンポジションリダイレクトに使用されるグラフィックの品質を指定します。

デフォルトは「高」です。

「高」、「中」、「低」、または「ロスレス」品質から選択します。

デスクトップの壁紙

この設定は、ユーザーセッションでの壁紙の表示を許可または禁止します。

デフォルトでは、ユーザーセッションで壁紙を表示できます。

デスクトップの壁紙を非表示にし、ユーザーセッションで必要な帯域幅を削減するには、この設定をポリシーに追加するときに**禁止**を選択します。

メニューアニメーション

この設定は、ユーザーセッションでのメニューアニメーションを許可または禁止します。

デフォルトでは、メニューアニメーションは許可されています。

メニューアニメーションは、アクセシビリティのためのMicrosoftの個人設定です。有効にすると、短い遅延の後、スクロールまたはフェードインによってメニューが表示されます。メニューの下部には矢印アイコンが表示されます。その矢印をポイントするとメニューが表示されます。

メニューアニメーションは、このポリシー設定が**許可**に設定され、メニューアニメーションのMicrosoft個人設定が有効になっている場合に、デスクトップで有効になります。

> **注:**
>
> メニューアニメーションのMicrosoft個人設定への変更は、デスクトップに影響を与えます。セッション終了時に変更を破棄するようにデスクトップを設定している場合を考慮してください。この場合、メニューアニメーションを有効にしているユーザーは、その後のセッションでメニューアニメーションを利用できない可能性があります。メニューアニメーションを必要とするユーザーに対しては、デスクトップのメインイメージでMicrosoft設定を有効にするか、デスクトップがユーザーの変更を保持するようにしてください。

ドラッグ中のウィンドウコンテンツの表示

この設定は、画面上でウィンドウをドラッグする際に、ウィンドウコンテンツの表示を許可または禁止します。

デフォルトでは、ウィンドウコンテンツの表示は許可されています。

許可に設定すると、ウィンドウをドラッグしたときにウィンドウ全体が移動するように見えます。**禁止**に設定すると、ドロップするまでウィンドウのアウトラインのみが移動するように見えます。

エンドユーザー監視ポリシー設定

「**エンドユーザー監視**」セクションには、セッショントラフィックを測定するためのポリシー設定が含まれています。

ICA®ラウンドトリップ計算

この設定は、アクティブな接続に対してICAラウンドトリップ計算が実行されるかどうかを決定します。

デフォルトでは、アクティブな接続の計算は有効になっています。

デフォルトでは、各ICAラウンドトリップ測定の開始は遅延されます。この遅延は、ユーザーインタラクションを示すトラフィックが発生するまで続きます。この遅延は無期限に続く可能性があり、ICAラウンドトリップ測定がICAトラフィックの唯一の原因となるのを防ぐように設計されています。

ICAラウンドトリップ計算間隔

この設定は、ICAラウンドトリップ計算が実行される頻度を秒単位で指定します。

デフォルトでは、ICAラウンドトリップは15秒ごとに計算されます。

アイドル接続のICAラウンドトリップ計算

この設定は、アイドル接続に対してICAラウンドトリップ計算が実行されるかどうかを決定します。

デフォルトでは、アイドル接続に対して計算は実行されません。

デフォルトでは、各ICAラウンドトリップ測定の開始は遅延されます。この遅延は、ユーザーインタラクションを示すトラフィックが発生するまで続きます。この遅延は無期限に続く可能性があり、ICAラウンドトリップ測定がICAトラフィックの唯一の原因となるのを防ぐように設計されています。

ファイルリダイレクトポリシー設定

ファイルリダイレクトセクションには、クライアントドライブマッピングとクライアントドライブ最適化に関連するポリシー設定が含まれています。

クライアントドライブの自動接続

この設定は、ユーザーがログオンしたときのクライアントドライブの自動接続を許可または禁止します。

デフォルトでは、自動接続は許可されています。

この設定をポリシーに追加するときは、自動接続するドライブの種類の設定を有効にしてください。たとえば、ユーザーのCD-ROMドライブの自動接続を許可するには、この設定と**クライアント光学ドライブ**設定を構成します。

関連するポリシー設定は次のとおりです。

- **クライアントドライブのリダイレクト**
- **クライアントフロッピーディスクドライブ**
- **クライアント光学ドライブ**
- **クライアント固定ドライブ**
- **クライアントネットワークドライブ**
- **クライアントリムーバブルドライブ**

クライアントドライブのリダイレクト

この設定は、ユーザーデバイス上のドライブとの間でファイルリダイレクトを有効または無効にします。

デフォルトでは、ファイルリダイレクトは有効になっています。

> **注:**
>
> クライアントドライブリダイレクトポリシー設定は、汎用USBリダイレクトを使用してセッションにマップされたドライブには適用されません。

> 有効にすると、ユーザーはすべてのクライアントドライブにファイルを保存できます。無効にすると、すべてのファイルリダイレクトが防止されます。この構成は、個々のファイルリダイレクト設定の状態に関係なく適用されます。個々のファイルリダイレクト設定には、クライアントフロッピードライブとクライアントネットワークドライブが含まれます。

以下のポリシー設定が関連しています。

- **クライアントフロッピードライブ**
- **クライアント光学ドライブ**
- **クライアント固定ドライブ**
- **クライアントネットワークドライブ**
- **クライアントリムーバブルドライブ**

クライアント固定ドライブ

この設定により、ユーザーはユーザーデバイス上の固定ドライブへのファイルアクセスまたは保存を許可または禁止されます。

デフォルトでは、クライアント固定ドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合は、**クライアントドライブリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。これらの設定が無効になっている場合、クライアント固定ドライブはマップされず、**クライアント固定ドライブ**設定の状態に関係なく、ユーザーはこれらのドライブに手動でアクセスできません。

ユーザーがログオンしたときに固定ドライブが自動的に接続されるように、**クライアントドライブの自動接続**設定を構成します。

クライアントフロッピードライブ

この設定では、ユーザーがユーザーデバイス上のフロッピーディスクドライブにアクセスしたり、ファイルを保存したりすることを許可または禁止します。

デフォルトでは、クライアントフロッピードライブへのアクセスは許可されています。

この設定をポリシーに追加するときは、**クライアントドライブのリダイレクト**設定が存在し、許可に設定されていることを確認してください。これらの設定が無効になっている場合、**クライアントフロッピーディスクドライブ**設定の状態に関係なく、クライアントフロッピーディスクドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。

ユーザーのログオン時にフロッピーディスクドライブが自動的に接続されるようにするには、**クライアントドライブの自動接続**設定を構成します。

クライアントネットワークドライブ

この設定では、ユーザーがユーザーデバイスを介してネットワーク（リモート）ドライブにアクセスしたり、ファイルを保存したりすることを許可または禁止します。

デフォルトでは、クライアントネットワークドライブへのアクセスは許可されています。

この設定をポリシーに追加するときは、**クライアントドライブのリダイレクト**設定が存在し、許可に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントネットワークドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、**クライアントネットワークドライブ**設定の状態に関係なく適用されます。

ユーザーのログオン時にネットワークドライブが自動的に接続されるようにするには、**クライアントドライブの自動接続**設定を構成します。

クライアント光学ドライブ

この設定では、ユーザーが以下にアクセスしたり、ファイルを保存したりすることを許可または禁止します。

- ユーザーデバイス上のCD-ROM
- ユーザーデバイス上のDVD-ROM
- ユーザーデバイス上のBD-ROMドライブ。

デフォルトでは、クライアントの光学ドライブへのアクセスは許可されています。

この設定をポリシーに追加する際は、**クライアントドライブのリダイレクト**設定が存在し、**許可**に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントの光学ドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、**クライアント光学ドライブ**設定の状態に関係なく適用されます。

ユーザーがログオンしたときに光学ドライブが自動的に接続されるようにするには、「**クライアントドライブの自動接続**」設定を構成します。

クライアントリムーバブルドライブ

この設定は、ユーザーがユーザーデバイス上のUSBドライブにアクセスしたりファイルを保存したりすることを許可または禁止します。

デフォルトでは、クライアントのリムーバブルドライブへのアクセスは許可されています。

この設定をポリシーに追加する際は、**クライアントドライブのリダイレクト**設定が存在し、許可に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントのリムーバブルドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、**クライアントリムーバブルドライブ**設定の状態に関係なく適用されます。

ユーザーがログオンしたときにリムーバブルドライブが自動的に接続されるように、**クライアントドライブの自動接続**設定を構成します。

ホストからクライアントへのリダイレクト

この設定は、URLおよび一部のメディアコンテンツのファイルタイプ関連付けを有効または無効にし、ユーザーデバイスで開かれるようにします。無効にすると、コンテンツはサーバーで開かれます。

デフォルトでは、ファイルタイプ関連付けは無効になっています。

この設定を有効にすると、以下のURLタイプがローカルで開かれます。

- HTTP
- HTTPS
- リアルプレイヤーおよびクイックタイム (RTSP)

- Real Player および QuickTime (RTSPU)
- レガシー Real Player (PNM)
- マイクロソフト メディア サーバー (MMS)

クライアントドライブ文字の保持

この設定により、クライアントドライブをセッション内で同じドライブ文字にマップすることを有効または無効にします。

デフォルトでは、クライアントドライブ文字は保持されません。

この設定をポリシーに追加する場合は、**クライアントドライブのリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。

読み取り専用クライアントドライブアクセス

この設定は、ユーザーとアプリケーションが以下のことを行うことを許可または防止します。

- マップされたクライアントドライブ上でのファイルの作成
- マップされたクライアントドライブ上でのファイルの変更
- マップされたクライアントドライブ上でのフォルダーの変更

デフォルトでは、マップされたクライアントドライブ上のファイルとフォルダーは変更できます。

「有効」に設定されている場合、ファイルとフォルダーは読み取り専用のアクセス許可でアクセスできます。

この設定をポリシーに追加する場合は、**クライアントドライブのリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。

特殊フォルダーのリダイレクト

この設定により、Citrix Workspace™アプリおよびWeb Interfaceユーザーがセッションからローカルのドキュメントおよびデスクトップの特殊フォルダーを表示することが許可または禁止されます。

デフォルトでは、特殊フォルダーのリダイレクトは許可されています。

この設定は、他の場所に存在する設定に関係なく、ポリシーによってフィルター処理されたオブジェクトが特殊フォルダーのリダイレクトを持つことを防止します。この設定が禁止されている場合、StoreFront™、Web Interface、またはCitrix Workspaceアプリに指定された関連設定はすべて無視されます。

どのユーザーが特殊フォルダーのリダイレクトを持つことができるかを定義するには、**許可**を選択し、この機能を有効にしたいユーザーにフィルター処理されたポリシーにこの設定を含めます。この設定は、他のすべての特殊フォルダーのリダイレクト設定を上書きします。

ユーザーがローカルハードドライブにファイルにアクセスしたり保存したりすることを防止するポリシー設定は、特殊フォルダーのリダイレクトが機能することも防止します。この状況は、特殊フォルダーのリダイレクトがユーザーデバイスと対話する必要があるために発生します。

この設定をポリシーに追加する際は、**クライアント固定ドライブ**設定が存在し、「許可」に設定されていることを確認してください。

ファイル転送ポリシー

デフォルトでは、ファイル転送は有効になっています。これらのポリシーを変更するにはWeb Studioを使用します。これらは**ユーザー設定 - ICA\ファイルリダイレクト**の下にあります。ファイル転送ポリシーを使用する際は、以下を考慮してください。

- **Chrome OS/HTML5向けCitrix Workspaceアプリのファイル転送** - ユーザーがCitrix Virtual Apps and Desktopsセッションとデバイス間でファイルを転送することを許可または禁止します。
- **Chrome OS/HTML5向けCitrix Workspaceアプリのファイルアップロード** - ユーザーがデバイスからCitrix Virtual Apps and Desktopsセッションにファイルをアップロードすることを許可または禁止します。
- **Chrome OS/HTML5向けCitrix Workspaceアプリのファイルダウンロード** - ユーザーがCitrix Virtual Apps and Desktopsセッションからデバイスにファイルをダウンロードすることを許可または禁止します。

> **注:**
>
> ファイル転送ポリシーは、HTML5向けCitrix WorkspaceアプリおよびChrome OS向けCitrix Workspaceアプリにのみ適用されます。

非同期書き込みの使用

この設定は、非同期ディスク書き込みを有効または無効にします。

デフォルトでは、非同期書き込みは無効になっています。

非同期ディスク書き込みは、比較的高い帯域幅と高い遅延が特徴であるWAN経由でのファイル転送速度とクライアントディスクへの書き込み速度を向上させることができます。ただし、接続また

はディスクに障害が発生した場合、書き込み中のクライアントファイルが未定義の状態になる可能性があります。この未定義の状態が発生した場合、ポップアップウィンドウで影響を受けるファイルがユーザーに通知されます。ユーザーは、再接続時またはディスク障害が修正されたときに中断されたファイル転送を再開するなどの修復措置を講じることができます。

Citrix®は、良好なファイルアクセス速度を持つリモート接続を必要とし、接続またはディスク障害が発生した場合に失われたファイルやデータを簡単に回復できるユーザーに対してのみ、非同期ディスク書き込みを有効にすることを推奨します。

この設定をポリシーに追加する際は、**クライアントドライブリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。この設定が無効になっている場合、非同期書き込みは行われません。

グラフィックポリシー設定

グラフィックセクションには、ユーザーセッションで画像がどのように処理されるかを制御するためのポリシー設定が含まれています。

視覚的にロスレスな圧縮を許可する

この設定により、グラフィックに真のロスレス圧縮の代わりに視覚的にロスレスな圧縮を使用できます。視覚的にロスレスな圧縮は、真のロスレス圧縮よりもパフォーマンスが向上しますが、目には気づかない程度のわずかな損失があります。この設定は、視覚品質設定の値の使用方法を変更します。

デフォルトでは、この設定は無効になっています。

グラフィックステータスインジケーター

この設定は、ユーザーセッションでグラフィックステータスインジケーターを実行するように構成します。このツールを使用すると、ユーザーはアクティブなグラフィックモードに関する情報を確認できます。情報には、ビデオコーデック、ハードウェアエンコード、画質、およびセッションで使用されているモニターに関する詳細が含まれます。グラフィックステータスインジケーターを使用すると、ユーザーはピクセルパーフェクトモードを有効または無効にすることもできます。

Citrix Virtual Apps and Desktops™ 2103以降のリリースには、画質とインタラクティブ性の適切なバランスを見つけるのに役立つ画質スライダーが含まれています。

Citrix Virtual Apps and Desktops 2109以降のリリースには、グラフィックステータスインジケーターを使用して起動されるユーザーインターフェイスを介して仮想ディスプレイレイアウトを構成する機能が含まれています。

グラフィックステータスインジケーターは、以前のバージョンのロスレスインジケーターツールを置き換えます。このポリシーは、Citrix Virtual Apps and Desktopsバージョン7.16から1809までででロスレスインジケーターを有効にします。

画面共有

この設定により、ユーザーは画面コンテンツ、キーボード、マウスを含むセッションを他のユーザーと共有できます。

デフォルトでは、この設定は無効になっています。

VDAは、TCPポート範囲のポートを使用してデータを交換しようとします。最低ポートから開始し、後続の接続ごとに増分します。このポートは、インバウンドトラフィックとアウトバウンドトラフィックの両方を処理します。

既定では、TCPポート範囲は52525〜52625に設定されています。

画面共有に使用されるポートは、ファイアウォールの例外リストに追加する必要があります。このオプションは、VDAのインストール時にチェックボックスとして表示されます。既定では、このオプションはチェックされていません。

ディスプレイメモリ制限

この設定は、セッションの最大ビデオバッファサイズをキロバイト単位で指定します。

VDAバージョン2308以前の場合、128から4,194,303までのキロバイト単位の量を指定します。指定しない場合、設定は既定で65,536キロバイトになります。

VDAバージョン2311以降の場合、任意のキロバイト単位の量を指定します。指定しない場合、または0として指定した場合、設定は既定で最大値なしになります。

> **注:**
>
> VDAバージョン2311以降の場合、Citrix®は、この設定をデフォルトのままにすることを推奨しています。
>
> 接続に高解像度と複数のモニターを使用すると、より多くのメモリが必要になります。HDX™は各セッションに必要なディスプレイメモリの量のみを割り当てるため、常に環境内の構成の上位層に基づいて必要なビデオメモリの量を計算してください。したがって、一部のユーザーのみが既定値よりも多くを必要とする場合でも、ディスプレイメモリ制限を増やすことによるスケーラビリティへの悪影響はありません。

必要なビデオメモリの量は、次の式を使用して計算されます。

合計ビデオメモリ = ((32 / 8) x Σ)

例1

次の例では、2台のモニターを使用するセッションを想定します。1台は1920x1080の解像度、もう1台は1280x720の解像度です。

1. 解像度の積の合計を計算します。
    - (1080 x 1920) + (720 x 1280)
    - = 2073600 + 921600
    - = 2995200
2. 合計ビデオメモリの計算:
    - ((32 / 8) x 2995200)
    - = (4 x 2995200)
    - = 11,980,800 バイトまたは 11,700 キロバイト

この例では、これら2つのモニター構成を持つセッションをサポートするために、11,700キロバイトのビデオメモリが必要になります。

例2

4Kモニターを4台使用する場合、上記の式を使用すると、これらのセッションには最低129,600キロバイトのビデオメモリが必要になります。

どちらの例でも、VDAバージョン2311以降を使用する場合、Citrixはディスプレイメモリ制限をデフォルトのままにすることを推奨しています。

表示モードの劣化優先順位

> **注:**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

セッションのディスプレイメモリ制限に達した場合、この設定は、色深度と解像度のどちらが先に劣化するかを指定します。

デフォルトでは、色深度が先に劣化します。

セッションメモリ制限に達すると、表示される画像の品質を低下させることができます。この品質は、色深度と解像度のどちらを先に劣化させるかを選択することで低下させることができます。色深度が先に劣化する場合、表示される画像はより少ない色を使用します。解像度が先に劣化する場合、表示される画像は1インチあたりのピクセル数が少なくなります。

カラー深度または解像度が低下した場合にユーザーに通知するには、「ディスプレイモードが低下したときにユーザーに通知」設定を構成します。

動的ウィンドウプレビュー

この設定は、シームレスウィンドウの表示を有効または無効にします。

- フリップ-
- フリップ 3D
- タスクバープレビュー
- Windows ピーク

WINDOWS AERO プレビューオプション	説明
タスクバープレビュー	ユーザーがウィンドウのタスクバーアイコンにマウスカーソルを合わせると、そのウィンドウの画像がタスクバーの上に表示されます。
Windows ピーク	ユーザーがタスクバープレビュー画像にマウスカーソルを合わせると、ウィンドウのフルサイズの画像が画面に表示されます。
フリップ	ユーザーがALT+TABを押すと、開いている各ウィンドウの小さなプレビューアイコンが表示されます。
フリップ 3D	ユーザーがTAB+Windowsロゴキーを押すと、開いているウィンドウの大きな画像が画面全体にカスケード表示されます。

デフォルトでは、この設定は有効になっています。

画像キャッシュ

> **注:**

> Virtual Delivery Agent 7.x の場合、このポリシー設定は、レガシーグラフィックモードのポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、セッション内の画像のセクションのキャッシュと取得を有効または無効にします。画像をセクションにキャッシュし、必要に応じてこれらのセクションを取得することで、次のことが可能になります。

- ユーザーデバイス上でのスクロールがよりスムーズに
- ユーザーデバイス上でネットワーク経由で送信されるデータ量を削減します
- ユーザーデバイス上で必要な処理を削減します

デフォルトでは、画像キャッシュ設定は有効になっています。

> **注:**

> 画像キャッシュ設定は、画像がどのようにキャッシュされ、取得されるかを制御します。この設定は、画像がキャッシュされるかどうかを制御するものではありません。レガシーグラフィックモード設定が有効になっている場合、画像はキャッシュされます。

レガシーグラフィックモード - サポートされていません。下位互換性のためのみ

> **重要:**

> このリリースでは、レガシーグラフィックモードとデスクトップコンポジションリダイレクト (DCR) はサポートされていません。このポリシーは、XenApp 7.15 LTSR、XenDesktop 7.15 LTSR、およびWindows 7とWindows 2008 R2を使用する以前のVDAリリースとの下位互換性のためだけに含められています。

> この設定は、リッチグラフィックエクスペリエンスを無効にします。この設定を使用してレガシーグラフィックエクスペリエンスに戻し、WANまたはモバイル接続での帯域幅消費を削減します。XenAppおよびXenDesktop 7.13で導入された帯域幅の削減により、このモードは廃止されました。

デフォルトでは、この設定は無効になっており、ユーザーにはリッチグラフィックエクスペリエンスが提供されます。

レガシーグラフィックモードは以下でサポートされています。

- ウィンドウズ 7
- Windows Server 2008 R2 を実行しているVDA.

レガシーグラフィックモードは以下ではサポートされていません。

- Windows 8.xおよび10
- Windows Server 2012、2012 R2、および2016。

XenAppおよびXenDesktop 7.6 FP3以降でのグラフィックモードとポリシーの最適化について詳しくは、CTX202687を参照してください。

許可される最大色深度

> **注:**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、セッションで許可される最大色深度を指定します。

デフォルトでは、許可される最大色深度は1ピクセルあたり32ビットです。

この設定は、Thinwireドライバーと接続にのみ適用されます。プライマリディスプレイドライバーとしてThinWire以外のドライバーを使用するVDAには適用されません。これらのVDAは、プライマリディスプレイドライバーとしてWindows Display Driver Model (WDDM) ドライバーを使用するVDAです。Windows 8などのWDDMドライバーをプライマリディスプレイドライバーとして使用するシングルセッションOS VDAの場合、この設定は効果がありません。Windows Server 2019などのWDDMドライバーを使用するWindowsマルチセッションOS VDAの場合、この設定によりユーザーがVDAに接続できなくなる可能性があります。

高い色深度を設定すると、より多くのメモリが必要になります。メモリ制限に達したときに色深度を低下させるには、**表示モードの低下設定**を構成します。色深度が低下すると、表示される画像はより少ない色を使用します。

表示モードが低下したときにユーザーに通知する

> **注:**

> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、色深度または解像度が低下したときに、ユーザーに簡単な説明を表示します。

デフォルトでは、ユーザーへの通知は無効になっています。

3Dグラフィックワークロード向けに最適化する

この設定は、グラフィックを多用するワークロードに最適なデフォルト設定を構成します。グラフィックを多用するアプリケーションに重点を置くユーザーに対して、この設定を有効にします。このポリシーは、セッションでGPUが利用可能な場合にのみ適用してください。このポリシーによって設定されたデフォルト設定を明示的に上書きするその他の設定が優先されます。

デフォルトでは、3Dグラフィックワークロード向けに最適化する設定は無効になっています。

キューイングとトッシング

> **注:**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、別の画像に置き換えられたキュー内の画像を破棄します。

デフォルトでは、キューイングとトッシングは有効になっています。

この設定は、グラフィックがユーザーデバイスに送信される際の応答を改善します。この設定を構成すると、フレームがドロップされるため、アニメーションが途切れることがあります。

圧縮にビデオコーデックを使用する

エンドポイントでビデオデコードが利用可能な場合、グラフィックの圧縮にビデオコーデックの使用を許可します。**画面全体**が選択されている場合、ビデオコーデックはすべてにデフォルトのコーデックとして適用されます。**アクティブに変化する領域**が選択されている場合、ビデオコーデックは画面上で常に変化する領域に使用され、その他のデータは静止画圧縮とビットマップキャッシュを使用します。エンドポイントでビデオデコードが利用できない場合、または**ビデオコーデックを使用しない**を指定した場合、静止画圧縮とビットマップキャッシュの組み合わせが使用されます。**推奨時に使用**が選択されている場合、システムはさまざまな要因に基づいて選択します。選択方法が強化されるにつれて、結果はバージョン間で異なる場合があります。

推奨時に使用を選択すると、システムが現在のシナリオに最適な設定を選択するために最大限の努力をすることができます。

画面全体を選択すると、特にサーバーレンダリングされたビデオや3Dグラフィックを多用する場合に、ユーザーエクスペリエンスと帯域幅の向上に最適化されます。

アクティブに変化する領域を選択すると、特に低帯域幅でビデオパフォーマンスが向上するように最適化され、静的およびゆっくりと変化するコンテンツのスケーラビリティを維持できます。この設定は、マルチモニター展開でサポートされています。

ビデオコーデックを使用しないを選択すると、サーバーのCPU負荷を最適化し、多数のサーバーレンダリングされたビデオやその他のグラフィックを多用するアプリケーションがない場合に最適化されます。

デフォルトは「**推奨時に使用**」です。

ビデオにハードウェアエンコーディングを使用する

この設定により、利用可能な場合、グラフィックハードウェアを使用してビデオコーデックで画面要素を圧縮できます。そのようなハードウェアが利用できない場合、VDAはソフトウェアビデオコーデックを使用したCPUベースのエンコーディングにフォールバックします。

このポリシー設定のデフォルトオプションは「**有効**」です。

複数のモニターがサポートされています。

ビデオデコードをサポートするCitrix Workspace™アプリは、ハードウェアエンコードで使用できます。

NVIDIA

NVIDIA GRID GPUの場合、マルチセッションOSおよびシングルセッションOS用のVDAでハードウェアエンコーディングがサポートされています。

NVIDIA GPUはNVENCハードウェアエンコードをサポートしている必要があります。サポートされているGPUのリストについては、NVIDIA video codec SDKを参照してください。

NVIDIA GRIDにはドライバーバージョン3.1以降が必要です。NVIDIA Quadroにはドライバーバージョン362.56以降が必要です。CitrixはNVIDIA Release R361ブランチのドライバーを推奨しています。

ロスレステキストはNVENCハードウェアエンコードと互換性がありません。ロスレステキストを有効にした場合、ロスレステキストがNVENCハードウェアエンコードよりも優先されます。

活発に変化する領域に対するH.264ハードウェアコーデックの選択的な使用がサポートされています。

視覚的にロスレス（YUV 4:4:4）圧縮がサポートされています。視覚的にロスレス（グラフィックポリシー設定、Allow visually lossless compression)には、Citrix Workspaceアプリ1808以降またはCitrix Receiver for Windows 4.5以降が必要です。

インテル

Intel Iris Proグラフィックプロセッサの場合、ハードウェアエンコードはシングルセッションOSおよびマルチセッションOS用のVDAでサポートされています。

Intel Broadwell processor family以降のIntel Iris Proグラフィックプロセッサがサポートされています。Intel Remote Displays SDKバージョン1.0が必要で、IntelのWebサイトからダウンロードできます: Remote Displays SDK。

ロスレステキストは、ビデオコーデックポリシーが画面全体に設定されており、**3Dグラフィックワークロード向けに最適化**ポリシーが無効になっている場合にのみサポートされます。

視覚的にロスレス（YUV 4:4:4）はサポートされていません。

Intelエンコーダーは、最大8つのエンコードセッション（たとえば、1人のユーザーが8台のモニターを使用する場合、または8人のユーザーがそれぞれ1台のモニターを使用する場合）で良好なユーザーエクスペリエンスを提供します。8つ以上のエンコードセッションが必要な場合は、仮想マシンが接続するモニターの数を確認してください。管理者は、良好なユーザーエクスペリエンスを維持するために、このポリシー設定をユーザーごとまたはマシンごとに構成するかどうかを決定します。

AMD

AMDの場合、シングルセッションOS用VDAでハードウェアエンコードがサポートされています。

AMD GPUはRapidFire SDKをサポートする必要があります。例えば、AMD Radeon ProまたはFirePro GPUなどです。

エンコードを機能させるには、最新のAMDドライバーをインストールしてください。これらのドライバーは`<https://www.amd.com/en/support>`からダウンロードできます。

ロスレステキストはAMDハードウェアエンコードと互換性がありません。ロスレステキストを有効にしている場合、ロスレステキストがAMDハードウェアエンコードよりも優先されます。

積極的に変化する領域に対するH.264ハードウェアコーデックの選択的な使用がサポートされています。

キャッシュポリシー設定

このセクションには、クライアント接続の帯域幅が制限されている場合に、ユーザーデバイスで画像データをキャッシュすることを可能にするポリシー設定が含まれています。

永続キャッシュしきい値

注: Virtual Delivery Agent 7.xの場合、このポリシー設定は、**レガシーグラフィックモード**ポリシー設定が有効になっている場合にのみ適用されます。

この設定は、ユーザーデバイスのハードドライブにビットマップをキャッシュし、以前のセッションからの大規模で頻繁に使用される画像を再利用できるようにします。

デフォルトでは、しきい値は1秒あたり3000000ビットです。

しきい値は、永続キャッシュ機能が有効になるポイントを表します。たとえば、デフォルト値を使用すると、帯域幅が3000000 bpsを下回ったときに、ビットマップがユーザーデバイスのハードドライブにキャッシュされます。

キープアライブ ポリシー設定

「**キープアライブ**」セクションには、ICA® キープアライブメッセージを管理するためのポリシー設定が含まれています。

ICA キープアライブ タイムアウト

この設定は、連続するICAキープアライブメッセージ間の秒数を指定します。

デフォルトでは、キープアライブメッセージ間の間隔は60秒です。

ICAキープアライブメッセージを送信する間隔を1～3600秒で指定します。ネットワーク監視ソフトウェアが非アクティブな接続を閉じる役割を担っている場合は、この設定を構成しないでください。

ICA キープアライブメッセージ

この設定は、ICAキープアライブメッセージを定期的に送信するかどうかを有効または無効にします。

デフォルトでは、キープアライブメッセージは送信されません。

この設定を有効にすると、切断された接続が切断されなくなります。サーバーがアクティビティを検出しない場合、この設定はリモートデスクトップサービス (RDS) がセッションを切断するのを防ぎます。サーバーは数秒ごとにキープアライブメッセージを送信して、セッションがアクティブ

であるかどうかを検出します。セッションがアクティブでなくなった場合、サーバーはセッションを切断済みとしてマークします。

セッションの信頼性を使用している場合、ICAキープアライブは機能しません。ICAキープアライブは、セッションの信頼性を使用していない接続に対してのみ構成してください。

関連するポリシー設定: セッションの信頼性接続。

マルチメディアポリシー設定

マルチメディアセクションには、ユーザーセッションでのストリーミングHTML5およびWindowsオーディオとビデオを管理するためのポリシー設定が含まれています。

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

マルチメディアポリシー

デフォルトでは、Delivery Controller™で設定されたすべてのマルチメディアポリシーは、以下のレジストリに保存されます。

マシンポリシー:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies

ユーザーポリシー:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix{ユーザーセッションID}\User\MultimediaPolicies

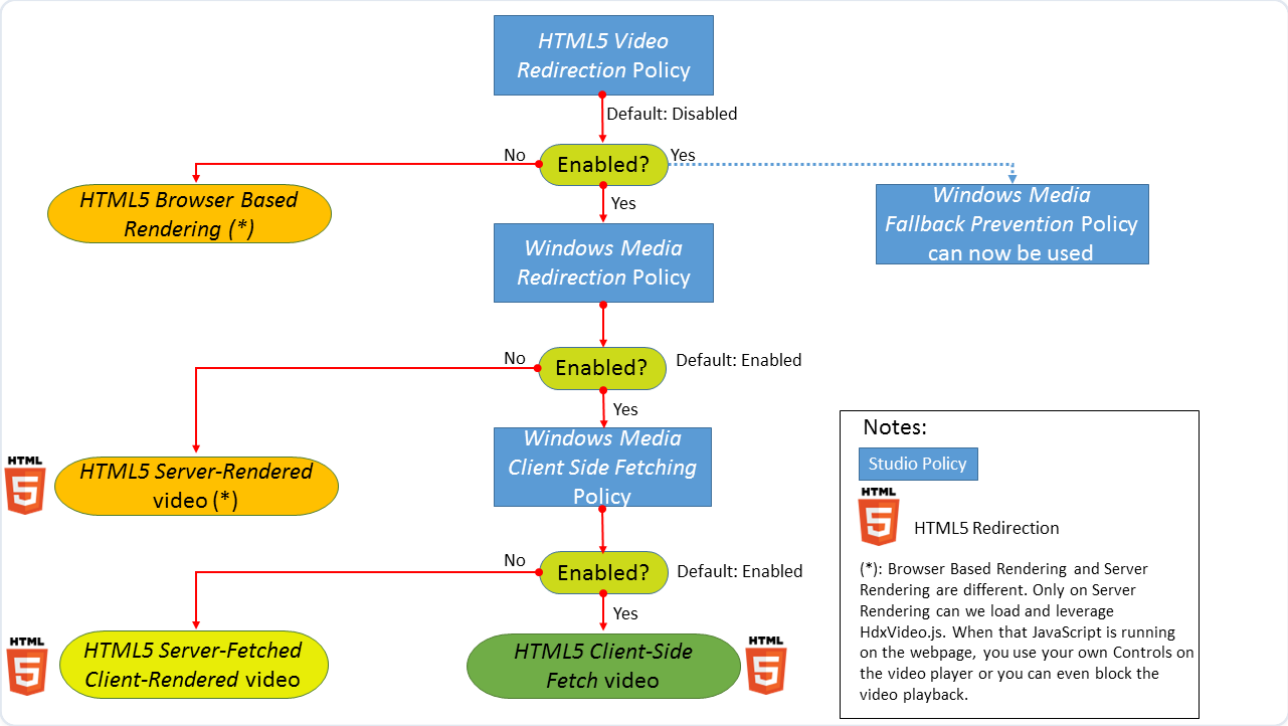
現在のユーザーセッションIDを特定するには、Windowsコマンドラインで**qwinsta**コマンドを発行します。

HTML5ビデオリダイレクト

Citrix Virtual Apps and Desktops™サーバーがHTML5マルチメディアWebコンテンツをユーザーに配信する方法を制御し、最適化します。

デフォルトでは、この設定は無効になっています。

HTML5リダイレクトのグラフィックイメージ



このリリースでは、この機能は制御されたWebページでのみ利用できます。HTML5マルチメディアコンテンツが利用可能なWebページ（例：社内トレーニングサイトのビデオ）にJavaScriptを追加する必要があります。

HTML5ビデオリダイレクトを構成するには:

1. VDAインストール上の%Program Files%/Citrix/ICA Service/HTML5 Video Redirectionから、ファイル **HdxVideo.js** を社内Webページの場所にコピーします。
2. この行をWebページに挿入します（Webページに他のスクリプトがある場合は、それらのスクリプトの前に **HdxVideo.js** を含めます）。 `<script src="HdxVideo.js" type="text/javascript"\></script>`

注： HdxVideo.jsがWebページと同じ場所にない場合は、**src** 属性を使用してそのフルパスを指定します。

JavaScriptが制御されたWebページに追加されておらず、ユーザーがHTML5ビデオを再生する場合を考えてみましょう。この場合、Citrix Virtual Apps and Desktopsはサーバー側レンダリングにデフォルト設定されます。

HTML5ビデオのリダイレクトを機能させるには、***Windows Media Redirection***を許可します。このポリシーは、Server Fetch Client Renderには必須であり、Client Side Fetchingには必要です。Client Side Fetchingは、さらに*Windows Media client-side content fetching*が許可されていることも必要とします。

Microsoft Edgeはこの機能をサポートしていません。

HdxVideo.jsは、ブラウザのHTML5プレーヤーコントロールを独自のコントロールに置き換えます。特定のWebサイトでHTML5ビデオリダイレクトポリシーが有効になっていることを確認するには、プレーヤーコントロールを、**HTML5ビデオリダイレクト**ポリシーが禁止されているシナリオと比較します。

（ポリシーが許可されている場合のCitrixカスタムコントロール）



（ポリシーが禁止されているか、構成されていない場合のネイティブWebページコントロール）



以下のビデオコントロールがサポートされています。

- 再生
- 一時停止
- シーク
- 繰り返し
- オーディオ
- 全画面表示

HTML5ビデオリダイレクトテストページを表示できます。

TLS、HTML5ビデオリダイレクト、およびブラウザーコンテンツリダイレクト

HTML5ビデオリダイレクトは、次の目的で使用できます。

- HTTPS Webサイトからのビデオのリダイレクト
- または
- Webサイト全体をリダイレクトするためのブラウザーコンテンツリダイレクト

これらのWebサイトに挿入されたJavaScriptは、VDAで実行されているCitrix HDX HTML5ビデオリダイレクトサービス (WebSocketService.exe) へのTLS接続を確立する必要があります。VDAの証明書ストアにあるCitrix HDX HTML5ビデオリダイレクトサービスは、次の目的で2つのカスタム証明書を生成します。

- ビデオのリダイレクトを実現する
- WebページのTLS整合性を維持する

HdxVideo.jsは、Secure WebSocketsを使用して、VDAで実行されているWebSocketService.exeと通信します。このプロセスはローカルシステムアカウントとして実行され、SSL終端とユーザーセッションマッピングを行います。

WebSocketService.exeは、127.0.0.1ポート9001でリッスンしています。

ビデオ品質の制限

この設定は Windows Media にのみ適用され、HTML5 には適用されません。これには、**WAN 経由の Windows Media マルチメディアリダイレクトの最適化**を有効にする必要があります。

この設定は、HDX™接続で許可される最大ビデオ品質レベルを指定します。設定すると、最大ビデオ品質は指定された値に制限され、環境内でマルチメディアのサービス品質 (QoS) が維持されます。

デフォルトでは、この設定は構成されていません。

許可される最大ビデオ品質レベルを制限するには、次のいずれかのオプションを選択します。

- 1080p/8.5Mbps
- 720p/4.0Mbps
- 480p/720Kbps
- 380p/400Kbps
- 240p/200Kbps

同じサーバーで複数のビデオを同時に再生すると、大量のリソースが消費され、サーバーのスケーラビリティに影響を与える可能性があります。

Microsoft Teams リダイレクト

この設定は、HDXテクノロジーに基づいてMicrosoft Teamsの最適化を有効にします。

このポリシーが有効で、サポートされているバージョンのCitrix Workspace™アプリを使用している場合、このレジストリキーはVDA上で**1**に設定されます。Microsoft Teamsアプリケーションは、VDIモードでロードするためにこのキーを読み取ります。 レジストリキーを手動で設定する必要はありません。

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

名前: MSTeamsRedirSupport

値: DWORD (1 - オン, 0 - オフ)

注:

Web Studioでポリシーが利用できない古いバージョンのController（バージョン7.15など）で、バージョン1906.2以降のVDAを使用しているとします。この場合、HDX最適化はVDAでデフォルトで有効になっています。Workspaceアプリのバージョンが1907以降の場合、Microsoft Teamsは最適化モードで起動します。7.15 LTSR ControllerとCR VDAを混在させる場合の注意点については、Knowledge Centerの記事CTX205549を参照してください。

この場合、特定のユーザーに対して機能を無効にするには、レジストリ設定を上書きできます。グループポリシーを使用してユーザーの組織単位にログオンスクリプトを適用することで、レジストリ設定を上書きします。

デフォルトでは、Microsoft Teamsリダイレクトは有効になっています。

マルチメディア会議

この設定により、ビデオ会議アプリケーションによる最適化されたWebカメラリダイレクト技術の使用を許可または禁止します。

デフォルトでは、ビデオ会議サポートは許可されています。

この設定をポリシーに追加する場合は、**Windows Mediaリダイレクト**設定が存在し、**許可**（デフォルト）に設定されていることを確認してください。

マルチメディア会議を使用する場合は、次の条件が満たされていることを確認してください。

- マルチメディア会議に使用するWebカメラのメーカー提供ドライバーがクライアントにインストールされていること。
- ビデオ会議セッションを開始する前に、Webカメラをユーザーデバイスに接続します。サーバーは、一度に1つのインストールされたWebカメラのみを使用します。ユーザーデバイスに複数のWebカメラがインストールされている場合、サーバーは各Webカメラを順番に試行します。この試行は、ビデオ会議セッションが正常に作成されるまで続行されます。

汎用USBリダイレクトを使用してWebカメラをリダイレクトする場合、このポリシーは必要ありません。その場合は、WebカメラドライバーをVDAにインストールしてください。

WAN経由のWindows Mediaマルチメディアリダイレクトの最適化

この設定はWindows Mediaにのみ適用され、HTML5には適用されません。この設定により、以下が可能になります。

- リアルタイムマルチメディアトランスコーディング
- 劣化したネットワーク経由でのモバイルデバイスへのオーディオおよびビデオメディアストリーミングを許可
- WAN経由でWindows Mediaコンテンツが配信される方法を改善することで、ユーザーエクスペリエンスを向上させます。

デフォルトでは、WAN経由でのWindows Mediaコンテンツの配信は最適化されています。

この設定をポリシーに追加する際は、**Windows Media Redirection**設定が存在し、**Allowed**に設定されていることを確認してください。

この設定が有効になっている場合、メディアストリーミングを可能にするために、必要に応じてリアルタイムのマルチメディアトランスコーディングが自動的に展開されます。また、極端なネットワーク条件下でもシームレスなユーザーエクスペリエンスを提供します。

WAN経由でのWindows Mediaマルチメディアリダイレクトの最適化にGPUを使用する

この設定はWindows Mediaにのみ適用され、Virtual Delivery Agent (VDA) のグラフィック処理ユニット (GPU) でリアルタイムマルチメディアトランスコーディングを実行できるようにします。これにより、サーバーのスケーラビリティが向上します。GPUトランスコーディングは、VDAがハードウェアアクセラレーションに対応したGPUを搭載している場合にのみ利用可能です。それ以外の場合、トランスコーディングはCPUにフォールバックします。

注: GPUトランスコーディングはNVIDIA GPUでのみサポートされています。

デフォルトでは、WAN経由でのWindows Mediaコンテンツの配信を最適化するためにVDA上のGPUを使用することは禁止されています。

この設定をポリシーに追加する際は、以下の設定が存在し、Allowedに設定されていることを確認してください。

- **Windows Mediaリダイレクト**
- **WAN経由でのWindows Mediaマルチメディアリダイレクト設定の最適化**

Windows Mediaフォールバック防止

この設定は、browser content redirection、HTML5、およびWindows Mediaに適用されます。HTML5をサポートするには、**HTML5 video redirection**ポリシーを**Allowed**に設定します。

管理者は、**Windows Media fallback prevention**ポリシー設定を使用して、ストリーミングコンテンツをユーザーに配信するために試行される方法を指定できます。

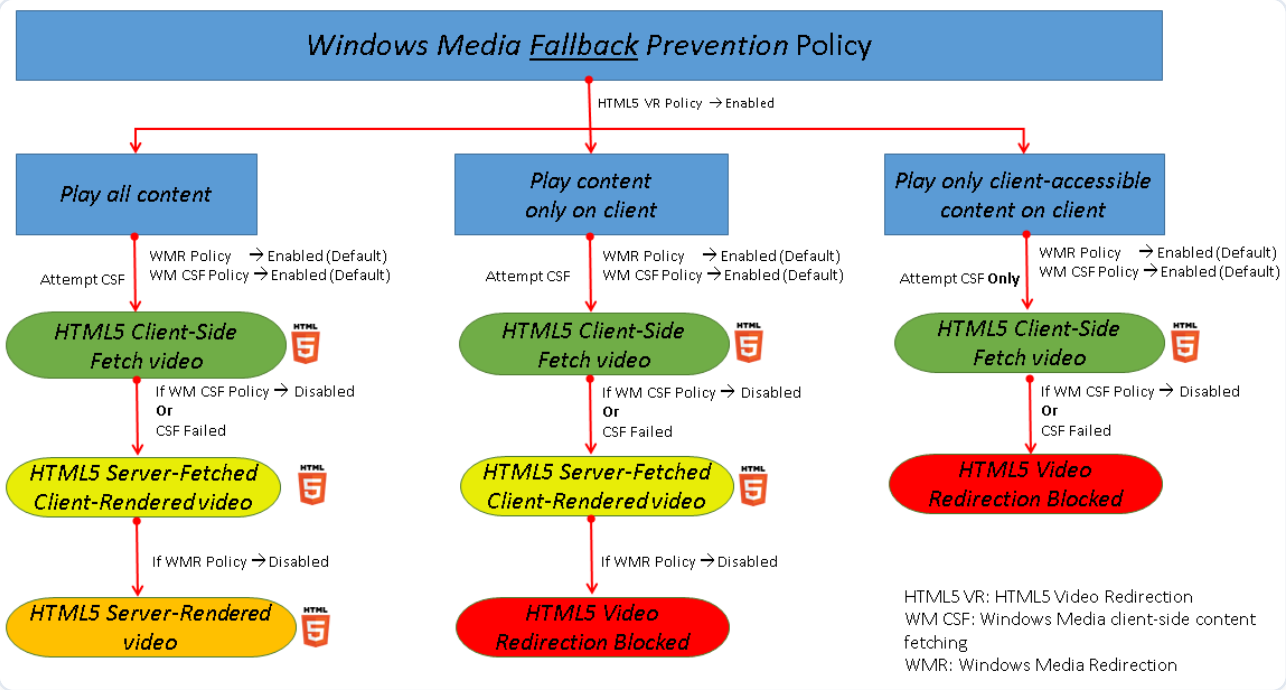
デフォルトでは、この設定は構成されていません。設定が「Not Configured」の場合、動作は**Play all content**と同じです。

この設定を構成するには、次のいずれかのオプションを選択します。

- **Play all content**。クライアント側でのコンテンツ取得を試行し、次にWindows Media Redirectionを試行します。失敗した場合は、サーバーでコンテンツを再生します。
- **Play all content only on client**。クライアント側での取得を試行し、次にWindows Media Redirectionを試行します。失敗した場合、コンテンツは再生されません。
- **Play only client-accessible content on client**。クライアント側での取得のみを試行します。失敗した場合、コンテンツは再生されません。

コンテンツが再生されない場合、プレーヤーウィンドウに次のエラーメッセージが表示されます（デフォルトの表示時間は5秒）。

「リソース不足のため、会社はビデオをブロックしました」



このエラーメッセージの表示時間は、VDA上の次のレジストリキーでカスタマイズできます。レジストリエントリが存在しない場合、表示時間はデフォルトで5秒になります。

レジストリパスは、VDAのアーキテクチャによって異なります。

`\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream`

または

\HKLM\SOFTWARE\Citrix\HdxMediastream

レジストリキー：

名前: VideoLoadManagementErrDuration

種類: DWORD

範囲: 1 - DWORDの制限まで (デフォルト = 5)

単位: 秒

Windows Mediaクライアント側コンテンツ取得

この設定は、HTML5とWindows Mediaの両方に適用されます。この設定により、ユーザーデバイスは、XenAppまたはXenDesktop®ホストサーバーを介するのではなく、インターネットまたはイントラネット上のソースプロバイダーからマルチメディアファイルを直接ストリーミングできるようになります。

デフォルトでは、この設定は**許可**されています。この設定を許可すると、ネットワーク使用率とサーバーのスケーラビリティが向上します。この改善は、メディアに関する処理をホストサーバーからユーザーデバイスに移動することで実現されます。また、Microsoft DirectShowやMedia Foundationなどの高度なマルチメディアフレームワークがユーザーデバイスにインストールされているという要件もなくなります。ユーザーデバイスには、URLからファイルを再生する機能のみが必要です。

この設定をポリシーに追加する場合は、**Windows Media Redirection**設定が存在し、**許可**に設定されていることを確認してください。**Windows Media Redirection**が無効になっている場合、ソースプロバイダーからユーザーデバイスへのマルチメディアファイルの直接ストリーミングも無効になります。

Windows Mediaリダイレクト

この設定は、HTML5とWindows Mediaの両方に適用され、サーバーがストリーミングオーディオとビデオをユーザーに配信する方法を制御および最適化します。

デフォルトでは、この設定は**許可**されています。HTML5の場合、ポリシー**HTML5ビデオのリダイレクト**が**禁止**されている場合、この設定は有効になりません。

この設定が有効になっている場合、サーバーからレンダリングされるオーディオとビデオの品質は、ユーザーデバイスでローカルに再生されるオーディオとビデオに匹敵するレベルに向上します。サーバーはマルチメディアを元の圧縮形式でクライアントにストリーミングし、ユーザーデバイスがメディアを解凍してレンダリングできるようにします。

Windows Media リダイレクトは、Microsoft DirectShow、DirectX Media Objects (DMO)、および Media Foundationの標準に準拠するコーデックでエンコードされたマルチメディアファイルを最適化します。特定のマルチメディアファイルを再生するには、そのマルチメディアファイルのエンコード形式と互換性のあるコーデックがユーザーデバイスに存在する必要があります。

デフォルトでは、Citrix Workspaceアプリでオーディオは無効になっています。ユーザーがICA®セッションでマルチメディアアプリケーションを実行できるようにするには、オーディオをオンにするか、Citrix Workspaceアプリインターフェイスでオーディオをオンにする権限をユーザーに付与します。

Windows Mediaリダイレクトを使用してメディアを再生したときの表示が、基本的なICA圧縮と通常のオーディオを使用してレンダリングした場合よりも劣る場合にのみ、**禁止**を選択してください。この状況はまれですが、低帯域幅の条件下（たとえば、キーフレームの頻度が低いメディアの場合）で発生する可能性があります。

Windows Mediaリダイレクトのバッファサイズ

この設定はレガシーであり、HTML5には適用されません。

この設定は、マルチメディアアクセラレーションのバッファサイズを1～10秒で指定します。

デフォルトでは、バッファサイズは5秒です。

Windows Mediaリダイレクトのバッファサイズの使用

この設定はレガシーであり、HTML5には適用されません。

この設定は、**Windows Mediaリダイレクトのバッファサイズ**設定で指定されたバッファサイズの使用を有効または無効にします。

デフォルトでは、指定されたバッファサイズは使用されません。

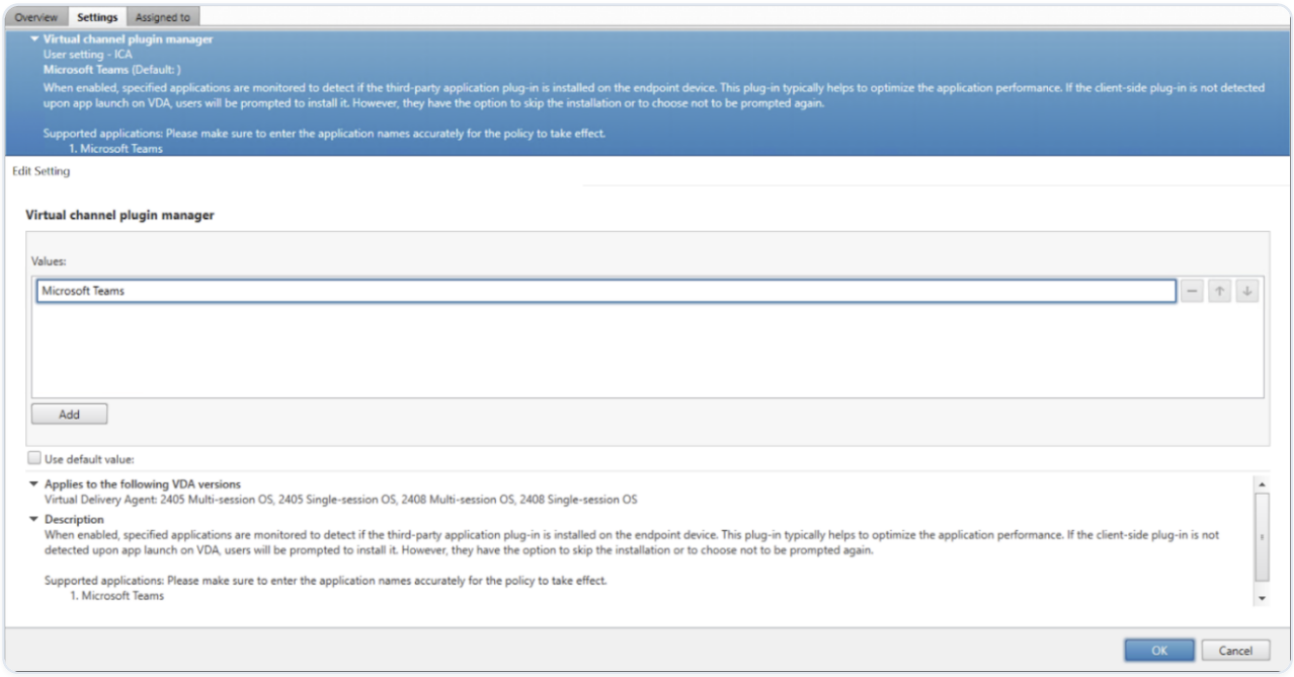
この設定が無効になっている場合、または**Windows Mediaリダイレクトのバッファサイズ**設定が構成されていない場合、サーバーはデフォルトのバッファサイズ値（5秒）を使用します。

仮想チャネルプラグインマネージャーポリシー

仮想チャネルプラグインマネージャーセクションには、この機能を構成するためのポリシー設定が含まれています。

仮想チャネルプラグインマネージャーは、特定の指定されたアプリケーションに対してクライアントエンドポイント全体にプラグインを展開するように設計されています。プラグインマネージャーは、VDAで実行されている特定のアプリケーションを検出し、アプリケーションの実行時に最高

のエクスペリエンスを得るために、エンドポイントにプラグインをインストールするようユーザーに促します。



- 管理者は、ポリシーを使用して、エンドポイント全体にプラグインをインストールする必要があるアプリケーションを指定できます。
- アプリケーション名は、ポリシーの説明の「サポートされているアプリケーション」に記載されている名前と同じである必要があります。
- デフォルトでは、このポリシーは無効になっています。
- 現在サポートされているアプリケーション
  - “マイクロソフト Teams”
- 今後、さらに多くのアプリケーションがサポートされる予定です。

マルチストリーム接続ポリシー設定

「**マルチストリーム接続**」セクションには、セッション内の複数のICA®接続のサービス品質の優先順位付けを管理するためのポリシー設定が含まれています。

> **注:**
>
> マルチストリーム接続ポリシーが有効になっている場合、MTU検出はサポートされません。

UDP経由のオーディオ

この設定は、サーバーでのUDP経由のオーディオを許可または禁止します。

デフォルトでは、サーバーでのUDP経由のオーディオは許可されています。

有効にすると、この設定はサーバー上にUDPポートを開き、UDP経由のオーディオリアルタイムトランスポートを使用するように構成されたすべての接続をサポートします。

オーディオUDPポート範囲

この設定は、Virtual Delivery Agent (VDA) が使用するポート番号の範囲（最小ポート番号、最大ポート番号）を指定します。この指定は、ユーザーデバイスとの間でオーディオパケットデータを交換するのに役立ちます。VDAは、ユーザーデバイスとのデータ交換のために、各UDPポートペアを最小値から開始し、以降の試行ごとに2ずつ増やしながら使用しようとします。各ポートは、インバウンドトラフィックとアウトバウンドトラフィックの両方を処理します。

デフォルトでは、この範囲は16500,16509に設定されています。

マルチポートポリシー

この設定は、ICAトラフィックに使用するTCPポートを指定し、各ポートのネットワーク優先度を確立します。

デフォルトでは、プライマリポート（2598）は高優先度です。

ポートを構成する際、次の優先度を割り当てることができます。

- **最高:** ウェブカメラ会議などのリアルタイムアクティビティ向け
- **高:** 画面、キーボード、マウスなどのインタラクティブ要素向け
- **中:** クライアントドライブマッピングなどのバルク処理向け
- **低:** 印刷などのバックグラウンドアクティビティ向け

各ポートには一意の優先順位が必要です。たとえば、CGPポート1とCGPポート3の両方に「最高」の優先順位を割り当てることはできません。

ポートを優先順位付けから削除するには、ポート番号を0に設定します。プライマリポートを削除することはできません。また、その優先順位レベルを変更することもできません。

この設定を構成するときは、サーバーを再起動してください。この設定は、**Multi-Stream computer**設定ポリシー設定が有効になっている場合にのみ有効になります。

マルチストリームコンピューター設定

この設定は、サーバー上のマルチストリームを有効または無効にします。

デフォルトでは、マルチストリームは無効になっています。Citrix SD-WAN™ またはサードパーティ製ルーターを使用して目的のサービス品質を実現する場合は、マルチストリームコンピューターポリシー設定を構成してください。

マルチストリームが有効になっている場合、アダプティブトランスポートの機能であるMTU検出はサポートされません。

この設定を構成するときは、サーバーを再起動して変更が適用されるようにしてください。

> **重要:**
>
> このポリシー設定を「セッション全体の帯域幅制限」などの帯域幅制限ポリシー設定と組み合わせて使用すると、予期しない結果が生じる可能性があります。この設定をポリシーに含める場合は、帯域幅制限設定が含まれていないことを確認してください。

マルチストリームユーザー設定

この設定は、ユーザーデバイス上でMulti-Streamを有効または無効にします。

デフォルトでは、Multi-Streamはすべてのユーザーに対して無効になっています。Citrix SD-WANまたはサードパーティ製ルーターを使用して目的のQuality of Serviceを実現する場合は、Multi-Stream user設定を構成してください。

この設定は、**マルチストリームコンピューター**設定ポリシー設定が有効になっているホストでのみ有効になります。

> **重要：**
>
> このポリシー設定を、全体的なセッション帯域幅制限などの帯域幅制限ポリシー設定と併用すると、予期しない結果が生じる可能性があります。この設定をポリシーに含める場合は、帯域幅制限設定を含めないようにしてください。

マルチストリーム仮想チャネル割り当て設定

この設定は、マルチストリームが使用されている場合に仮想チャネルが割り当てられるICAストリームを指定します。

これらの設定を構成しない場合、仮想チャネルはデフォルトのストリームに保持されます。仮想チャネルをICAストリームに割り当てるには、仮想チャネル名の横にある**ストリーム番号**リストから目的のストリーム番号（0、1、2、3）を選択します。

環境でカスタム仮想チャネルが使用されている場合は、**追加**をクリックし、**仮想チャネル**の下のテキストボックスに仮想チャネル名を指定し、その横にある**ストリーム番号**リストから目的のストリーム番号を選択します。指定する名前は、フレンドリ名ではなく、実際の仮想チャネル名である必要があります。たとえば、Citrix Browser AccelerationではなくCTXSBRなどです。

これらの設定は、マルチストリームコンピューター設定を有効にした場合にのみ有効になります。

デフォルトでは、仮想チャネルとそのストリーム割り当ては次のとおりです。

- AppFlow®: 2
- オーディオ: 0
- ブラウザコンテンツリダイレクト: 2
- クライアントCOMポートマッピング: 3
- クライアントドライブマッピング: 2
- クライアントプリンターマッピング: 3
- クリップボード: 2
- CTXDND: 1 (**注:** これはCitrixセッションとローカルエンドポイント間でのファイルのドラッグアンドドロップをサポートします。)
- DVCプラグイン (DVCプラグインのフレンドリ名から自動生成される静的VC名、または管理者割り当て): 2
- エンドユーザーエクスペリエンス監視: 1
- ファイル転送 (HTML5 Receiver): 2
- 汎用データ転送: 2
- ICA制御: 1
- 入力メソッドエディター: 1
- レガシー クライアント プリンター マッピング (COM1): 1, 3
- レガシー クライアント プリンター マッピング (COM2): 2, 3
- レガシー クライアント プリンター マッピング (LPT1): 1, 3
- レガシー クライアント プリンター マッピング (LPT2): 2, 3

- ライセンス管理: 1
- Microsoft Teams/WebRTC リダイレクト: 1
- モバイルレシーバー: 1
- マルチタッチ: 1
- ポートフォワーディング: 2
- リモートオーディオおよびビデオ拡張機能 (RAVE): 2
- シームレス (透過ウィンドウ統合): 1
- センサーと位置情報: 1
- スマートカード: 1
- Thinwire グラフィック: 1
- 透明UI統合/ログオンステータス: 2
- TWAIN リダイレクト: 2
- USB: 2
- ゼロ遅延フォントおよびキーボード: 2
- ゼロ遅延データチャネル: 2

仮想チャネルの割り当てと優先順位の詳細については、Knowledge Center の記事 CTX131001 を参照してください。

ポートリダイレクトポリシー設定

ポートリダイレクトセクションには、クライアントLPTおよびCOMポートマッピングのポリシー設定が含まれています。

Virtual Delivery Agentのバージョンが**7.0より前**の場合、ポートリダイレクトを構成するには以下のポリシー設定を使用します。VDAバージョン**7.0から7.8**の場合、これらの設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。VDAバージョン**7.9**の場合、以下のポリシー設定を使用します。

クライアントCOMポートの自動接続

この設定は、ユーザーがサイトにログオンしたときに、ユーザーデバイス上のCOMポートの自動接続を有効または無効にします。

デフォルトでは、クライアントCOMポートは自動的に接続されません。

クライアントLPTポートの自動接続

この設定は、ユーザーがサイトにログオンしたときに、ユーザーデバイス上のLPTポートの自動接続を有効または無効にします。

デフォルトでは、クライアントLPTポートは自動的に接続されません。

クライアントCOMポートリダイレクト

この設定は、ユーザーデバイス上のCOMポートへのアクセスを許可または禁止します。

デフォルトでは、COMポートリダイレクトは禁止されています。

以下のポリシー設定が関連しています。

- COMポートリダイレクトの帯域幅制限
- COMポートリダイレクトの帯域幅制限（パーセント）

クライアントLPTポートリダイレクト

この設定により、ユーザーデバイス上のLPTポートへのアクセスを許可または禁止します。

デフォルトでは、LPTポートリダイレクトは禁止されています。

LPTポートは、印刷ジョブをLPTポートに送信するレガシーアプリケーションでのみ使用されます。これらのポートは、印刷ジョブをユーザーデバイス上の印刷オブジェクトに送信するレガシーアプリケーションでは使用されません。今日のほとんどのアプリケーションは、印刷ジョブをプリンターオブジェクトに送信できます。このポリシー設定は、LPTポートに印刷するレガシーアプリケーションをホストするサーバーにのみ必要です。

注：クライアントCOMポートリダイレクトは双方向ですが、LPTポートリダイレクトは出力のみで、ICAセッション内では\\\client\LPT1および\\\client\LPT2に制限されます。

以下のポリシー設定は関連しています。

- LPTポートリダイレクト帯域幅制限
- LPTポートリダイレクトの帯域幅制限（パーセント）

印刷ポリシー設定

印刷セクションには、クライアント印刷を管理するためのポリシー設定が含まれています。

クライアントプリンターリダイレクト

この設定は、ユーザーがセッションにログオンしたときに、クライアントプリンターがサーバーにマップされるかどうかを制御します。

デフォルトでは、クライアントプリンターのマッピングは許可されています。この設定が無効になっている場合、セッション用のPDFプリンターは自動作成されません。

関連するポリシー設定: クライアントプリンターの自動作成

デフォルトプリンター

この設定は、ユーザーデバイス上のデフォルトプリンターがセッションでどのように確立されるかを指定します。

デフォルトでは、ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます。

デフォルトプリンターに現在のRemote Desktop ServicesまたはWindowsユーザープロファイル設定を使用するには、「ユーザーのデフォルトプリンターを調整しない」を選択します。このオプションを選択した場合、デフォルトプリンターはプロファイルに保存されず、他のセッションまたはクライアントプロパティに従って変更されることもありません。セッション内のデフォルトプリンターは、セッションで最初に自動作成されたプリンターであり、次のいずれかです。

- **コントロールパネル > デバイス**と**プリンター**でWindowsサーバーにローカルに追加された最初のプリンター。
- サーバーにローカルに追加されたプリンターがない場合、最初に自動作成されたプリンター。

このオプションを使用すると、プロファイル設定を通じてユーザーに最も近いプリンターを提示できます（近接印刷として知られています）。

プリンターの割り当て

この設定は、デフォルトプリンターとセッションプリンターの設定の代替手段を提供します。個別のデフォルトプリンターとセッションプリンターの設定を使用して、サイト、大規模グループ、または組織単位の動作を構成します。**プリンター割り当て**設定を使用して、多数のプリンターを複数のユーザーに割り当てます。

この設定は、一覧表示されたユーザーデバイスのデフォルトプリンターがセッション内でどのように確立されるかを指定します。

デフォルトでは、ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます。

各ユーザーデバイスのセッションで自動作成されるネットワークプリンターも指定します。デフォルトでは、プリンターは指定されていません。

- デフォルトプリンターの値を設定する場合：

ユーザーデバイスの現在のデフォルトプリンターを使用するには、「Do not adjust」を選択します。

デフォルトプリンターに現在のRemote Desktop ServicesまたはWindowsユーザープロファイル設定を使用するには、「調整しない」を選択します。このオプションを選択すると、デフォルトプリンターはプロファイルに保存されず、他のセッションまたはクライアントのプロパティに応じて変更されません。セッションのデフォルトプリンターは、セッションで最初に自動作成されたプリンターであり、次のいずれかです。

- **コントロールパネル > デバイスとプリンター**でWindowsサーバーにローカルで追加された最初のプリンター。
- サーバーにローカルで追加されたプリンターがない場合、最初に自動作成されたプリンター。

- **セッションプリンターの値: プリンターを追加する**を設定する場合、自動作成するプリンターのUNCパスを入力します。または、**参照**をクリックして、ネットワーク全体からプリンターを検索します。プリンターサーバーのFQDNまたはNetBIOS名を入力してプリンターを参照することもできます。詳細については、セッションプリンターを参照してください。プリンターを追加した後、ログオンごとに現在のセッションにカスタマイズされた設定を適用できます。

プリンターの自動作成イベントログ設定

この設定は、プリンターの自動作成プロセス中にログに記録されるイベントを指定します。エラーや警告をログに記録しない、エラーのみをログに記録する、またはエラーと警告をログに記録する、のいずれかを選択できます。

デフォルトでは、エラーと警告がログに記録されます。

警告の例としては、プリンターのネイティブドライバーをインストールできず、代わりにUniversal print driverがインストールされるイベントがあります。このシナリオでUniversal print driverを使用するには、Universal print driverの使用設定を「Use universal printing only」または「Use universal printing only if the requested driver is unavailable」に構成します。

セッションプリンター

この設定は、セッションで自動作成されるネットワークプリンターを指定します。ICA/HDXセッション内では、Citrix Print Managerサービス（CpSvc.exe）が、**セッションプリンター**ポリシー設定で指定された各ネットワークプリンターに対して、セッションログオン中にネットワークプリンター接続を作成します。セッションログオフ中にプリンターを削除します。デフォルトでは、プリンターは指定されていません。

セッションプリンターポリシー設定では、ネットワークプリンターはWindows Print ServerまたはCitrix Universal™ Print Server上に存在できます。

- **Windowsプリントサーバー:** 1つ以上のネットワークプリンターを共有します。また、ネットワークプリンターを使用するために必要なネイティブプリンタードライバーも備えています。
- **Universal Print Server:** Citrix Universal Print ServerソフトウェアがインストールされているWindowsプリントサーバーです。

Windowsプリントサーバーを使用する場合、Citrix Print Managerサービスは、ネイティブプリンタードライバーを使用してネットワークプリンター接続を作成します。Citrix Virtual Apps™サーバーには、ネイティブプリンタードライバーがインストールされている必要があります。

Citrix Universal Print Serverを使用する場合、Citrix Print Managerサービスは、ネイティブプリンタードライバー、Citrix Universal Printer Driver、またはCitrix Universal XPS Printer Driverのいずれかを使用してネットワークプリンター接続を作成します。使用するドライバーは、Universal Print Driver使用ポリシー設定によって制御されます。

すべてのWindowsプリンタードライバーは現在、v3またはv4ドライバーバージョンに分類されます。詳細については、「Microsoft V3およびV4プリンタードライバーアーキテクチャのサポート」を参照してください。

セッションプリンターを追加し、それらがセッションに表示されることを確認するには、次の手順を実行します。

1. Web Studioにサインインし、左ペインで**ポリシー**を選択し、次に**ポリシー**タブをクリックします。
2. ポリシーを選択し、 をクリックします。
3. **設定の編集**ページで、**デフォルト値を使用**チェックボックスをオフにし、次の手順に従ってプリンターを追加するには、**追加**をクリックします。

    a. プリンターのUNCパスを`\\<FQDN of the printer server>\<printer name>.`の形式で入力します。または、**参照**をクリックしてネットワーク全体からプリンターを検索します。プリンターサーバーのFQDNまたはNetBIOS名を入力してプリンターを参照することもできます。

    > **注：**

> **参照**を使用して特定のプリンターを検索できるようにするには、プリンターを構成する際に、**プリンター設定 > プリンターのプロパティ > 共有**の下にある**ディレクトリに一覧表示**オプションが選択されていることを確認してください。

b. デフォルトでは、プリンターサーバーを参照するためにユーザー名とパスワードが使用されます。異なるドメイン資格情報が必要な場合は、**参照に別のドメイン資格情報を使用**を選択し、必要なユーザー名とパスワードを入力して、**参照**をクリックします。

c. **完了**をクリックします。

4. ポリシーが設定された後、公開アプリケーションにセッションプリンターが表示されない場合があります。この問題は、Citrix Virtual Appsサーバーにプリンタードライバーがないか、ポリシーが作成されたものの有効になっていないために発生する可能性があります。

> **注:**
>
> セッションプリンターにネイティブプリンタードライバーが必要で、そのネイティブプリンタードライバーがVDAにインストールされていない場合、セッションプリンターはセッション内に作成されない可能性があります。

5. 公開デスクトップを起動し、**デバイスとプリンター > コントロールパネル**でセッションプリンターを手動で追加します。
6. これが失敗した場合は、Citrix Virtual Apps サーバーとプリントサーバー間の通信を調査します。RDP を使用してテストを実行することを検討してください。

プリンターが作成されるのを待つ

Delivery Controller のポリシーを使用して、Citrix Virtual Desktops でこの機能を有効にします。

プリンターが作成されるまで待機 (サーバーデスクトップ):

この設定により、セッションへの接続を遅延させ、クライアントリダイレクトされたプリンターが自動作成されるようにすることができます。

デフォルトでは、接続遅延は発生しません。

プリンターが作成されるまで待機 (Citrix Virtual Apps):

次のPowerShellコマンドレットを実行すると、マルチセッションホストで実行されている仮想アプリへの接続を遅延させ、アプリケーションが開かれる前にクライアントリダイレクトされたプリンターが自動作成されるようにすることができます。

```
Set-BrokerApplication -Name <VirtualAppName> -WaitForPrinterCreation $true
```

デフォルトでは、接続遅延は発生しません。

クライアントプリンターポリシー設定

クライアントプリンターセクションには、クライアントプリンターのポリシー設定が含まれています。これには、クライアントプリンターの自動作成、プリンタープロパティの保持、およびプリントサーバーへの接続に関する設定が含まれます。

クライアントプリンターの自動作成

この設定は、自動作成されるクライアントプリンターを指定します。この設定は、デフォルトのクライアントプリンター自動作成設定を上書きします。

デフォルトでは、すべてのクライアントプリンターが自動作成されます。

この設定は、**クライアントプリンターリダイレクト**設定が存在し、**許可**に設定されている場合にのみ有効になります。

この設定をポリシーに追加するときは、オプションを選択してください。

- **すべてのクライアントプリンターを自動作成**すると、ユーザーデバイス上のすべてのプリンターが自動的に作成されます。
- **クライアントのデフォルトプリンターのみを自動作成**すると、ユーザーデバイスでデフォルトプリンターとして選択されているプリンターのみが自動的に作成されます。
- **ローカル（非ネットワーク）クライアントプリンターのみを自動作成**すると、LPT、COM、USB、TCP/IP、またはその他のローカルポートを介してユーザーデバイスに直接接続されているプリンターのみが自動的に作成されます。
- **クライアントプリンターを自動作成しない**は、ユーザーがログオンしたときにすべてのクライアントプリンターの自動作成をオフにします。このオプションを選択すると、クライアントプリンターの自動作成に関するRemote Desktop Services (RDS) の設定が、優先度の低いポリシーでこの設定を上書きするようになります。

汎用ユニバーサルプリンターの自動作成

この設定は、セッション用の汎用Citrix Universal™ Printerオブジェクトの自動作成を有効または無効にします。これらのセッションには、ユニバーサル印刷と互換性のあるユーザーデバイスが使用されているセッションのみが含まれます。

デフォルトでは、汎用ユニバーサルプリンターオブジェクトは自動作成されません。

関連するポリシー設定は次のとおりです。

- ユニバーサルプリントドライバーの使用状況
- ユニバーサルドライバーの優先順位

PDFユニバーサルプリンターの自動作成

この設定は、以下のセッションでCitrix PDFプリンターの自動作成を有効または無効にします。

- Windows向けCitrix Workspaceアプリ（VDA 7.19以降）
- Linux向けCitrix Workspace™アプリ
- macOS向けCitrix Workspaceアプリ
- HTML5向けCitrix Workspaceアプリ
- Chrome向けCitrix Workspaceアプリ

デフォルトでは、Citrix PDFプリンターは自動作成されません。

クライアントプリンター名

この設定は、自動作成されたクライアントプリンターの名前付け規則を選択します。

デフォルトでは、標準のプリンター名が使用されます。

「**標準プリンター名**」を選択すると、「HPLaserJet 4 from client name in session 3」のようなプリンター名が使用されます。

「**レガシープリンター名**」を選択すると、旧式のクライアントプリンター名が使用され、製品のXenDesktopバージョンに存在するレガシープリンター名との下位互換性が維持されます。このオプションは、現在のCitrix Virtual Apps and Desktopsバージョンの製品でも使用できます。レガシープリンター名の例は「Client/clientname#/HPLaserJet 4」です。このオプションはセキュリティが低くなります。

Citrix Workspace app for HTML5 から起動されたセッションで Citrix PDF プリンターを使用する場合、**クライアントプリンター名**の設定をデフォルトにするか、**標準プリンター名**を選択します。**レガシープリンター名**を選択した場合、Citrix Workspace app for HTML5 は Citrix PDF プリンターオプションをサポートしません。

プリントサーバーへの直接接続

この設定は、仮想デスクトップまたはサーバーホスティングアプリケーションからクライアントプリンター用のプリントサーバーへの直接接続を有効または無効にします。ここで、クライアントプリンターはアクセス可能なネットワーク共有上にホストされます。

デフォルトでは、直接接続が有効になっています。

ネットワークプリントサーバーが仮想デスクトップまたはサーバーホスティングアプリケーションからWANを介していない場合は、直接接続を有効にします。ネットワークプリントサーバーと仮想デスクトップまたはサーバーホスティングアプリケーションが同じLAN上にある場合、直接通信により印刷が高速化されます。

ネットワークがWANを介している場合、または大幅な遅延や帯域幅の制限がある場合は、直接接続を無効にします。印刷ジョブはユーザーデバイスを介してルーティングされ、そこでネットワークプリントサーバーにリダイレクトされます。ユーザーデバイスに送信されるデータは圧縮されるため、WANを介してデータが転送される際の帯域幅の消費が少なくなります。

2つのネットワークプリンターが同じ名前を持つ場合、ユーザーデバイスと同じネットワーク上のプリンターが使用されます。

プリンタードライバーのマッピングと互換性

この設定は、自動作成されたクライアントプリンターのドライバー置換ルールを指定します。

この設定は、自動作成されたクライアントプリンターのリストからMicrosoft OneNoteとXPS Document Writerを除外するように構成されています。

ドライバー置換ルールを定義する際、指定されたドライバーでプリンターが作成されることを許可または防止できます。また、作成されたプリンターがユニバーサルプリントドライバーのみを使用することを許可できます。ドライバー置換は、ユーザーデバイスが提供するプリンタードライバー名を上書きまたはマッピングし、サーバー上の同等のドライバーに置き換えます。これらのルールにより、サーバーアプリケーションは、サーバーと同じドライバーを持つがドライバー名が異なるクライアントプリンターにアクセスできるようになります。

以下を実行できます。

- ドライバーマッピングを追加する
- 既存のマッピングを編集する
- マッピングのカスタム設定を上書きする
- マッピングを削除する
- リスト内のドライバーエントリの順序を変更する

マッピングを追加する際は、クライアントプリンタードライバー名を入力し、置き換えたいサーバードライバーを選択します。

プリンタープロパティの保持

この設定は、プリンタープロパティを保存するかどうか、および保存場所を指定します。

デフォルトでは、システムはプリンタープロパティがユーザーデバイスで利用可能な場合はユーザーデバイスに保存されるか、またはユーザープロファイルに保存されるかを決定します。

この設定をポリシーに追加するときは、オプションを選択してください。

- クライアントデバイスのみに保存は、保存されない強制プロファイルまたは移動プロファイルを持つユーザーデバイス用です。
- ユーザープロファイルのみに保持は、帯域幅によって制約される（このオプションはネットワークトラフィックを削減します）ユーザーデバイスやログオン速度が遅いユーザー、またはレガシープラグインを使用するユーザー向けです。このオプションは、プリンタープロパティをサーバー上のユーザープロファイルに保存し、ユーザーデバイスとのプロパティ交換を防止します。このオプションは、リモートデスクトップサービス (RDS) の移動プロファイルが使用されている場合にのみ適用されます。
- クライアントに保存されていない場合のみプロファイルに保持は、システムがプリンタープロパティの保存場所を決定できるようにします。プリンタープロパティは、利用可能な場合はユーザーデバイスに、またはユーザープロファイルに保存されます。このオプションは最も柔軟ですが、ログオン時間を遅くしたり、システムチェックのために余分な帯域幅を使用したりする可能性があります。
- プリンタープロパティを保持しないは、プリンタープロパティの保存を防止します。

保持および復元されたクライアントプリンター

この設定は、ユーザーデバイス上のプリンターの保持と再作成を有効または無効にします。デフォルトでは、クライアントプリンターは自動的に保持および復元されます。

保持されたプリンターは、次回のセッション開始時に再度作成される、または記憶されるユーザー作成のプリンターです。Citrix Virtual Apps™ が保持されたプリンターを再作成する場合、**クライアントプリンターの自動作成**設定を除くすべてのポリシー設定が考慮されます。

復元されたプリンターとは、管理者が完全にカスタマイズし、クライアントポートに永続的にアタッチされた保存状態を持つプリンターです。

CITRIX PDFユニバーサルプリンタードライバー

Citrix PDF ユニバーサルプリンタードライバーを使用すると、ユーザーはホストされたアプリケーションまたはCitrix Virtual Apps and Desktopsによって提供される仮想デスクトップで実行されているアプリケーションで開いたドキュメントを印刷できます。ユーザーが**Citrix PDF プリンター**オプションを選択すると、ドライバーはファイルをPDFに変換し、PDFをローカルデバイスに転送します。その後、PDFはローカルに接続されたプリンターから表示および印刷するために開かれます。PDFは、Citrixユニバーサルプリンティングでサポートされている形式の1つです（EMFおよびXPSに加えて）。 PDFプリンターは、Citrixポリシーを使用して有効化、構成、およびデフォ

ルトとして設定できます。**Citrix PDF プリンター**オプションは、Windows、Linux、macOS、Chrome、およびHTML5版のCitrix Workspaceアプリのユーザーが利用できます。

> **注:**
>
> WindowsエンドポイントにはPDFビューアーが必要です。クライアントには、PDFファイルを開くためにWindowsにファイルタイプ関連付けが登録されているアプリケーションが必要です。

ドライバーポリシー設定

「**ドライバー**」セクションには、プリンタードライバーに関連するポリシー設定が含まれています。

インボックスプリンタードライバーの自動インストール

> **注**
>
> このポリシーは、このリリースではVDAをサポートしていません。

> この設定では、以下のプリンタードライバーの自動インストールを有効または無効にします。

- Windowsインボックスドライバーセット
- `pnputil.exe /a` を使用してホストにステージングされたドライバーパッケージ

デフォルトでは、これらのドライバーは必要に応じてインストールされます。

ユニバーサルドライバーの優先順位

この設定では、ユニバーサルプリンタードライバーが使用される順序を、リストの最初のエントリから指定します。

デフォルトでは、優先順位は次のとおりです。

- EMF
- XPS
- PCL5c (ピーシーエルファイブシー)
- PCL4

- PS

ドライバーを追加、編集、削除したり、リスト内のドライバーの順序を変更したりできます。

ユニバーサルプリントドライバーの使用

この設定は、ユニバーサル印刷を使用するタイミングを指定します。

デフォルトでは、要求されたドライバーが利用できない場合にのみ、ユニバーサル印刷が使用されます。

ユニバーサル印刷は、標準のモデル固有のドライバーの代わりに汎用プリンタードライバーを使用するため、ホストコンピューターでのドライバー管理の負担を軽減できる可能性があります。ユニバーサルプリントドライバーの可用性は、ユーザーデバイス、ホスト、およびプリントサーバーソフトウェアの機能に依存します。特定の構成では、ユニバーサル印刷が利用できない場合があります。

この設定をポリシーに追加するときは、次の表からオプションを選択してください。

オプション	説明
プリンターモデル固有のドライバーのみを使用する	クライアントプリンターが、サインイン時に自動作成される標準のモデル固有のドライバーのみを使用することを指定します。要求されたドライバーが利用できない場合、クライアントプリンターは自動作成できません。
ユニバーサル印刷のみを使用する	標準のモデル固有のドライバーは使用しないことを指定します。プリンターの作成にはユニバーサルプリントドライバーのみが使用されます。
要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用する	利用可能な場合、プリンター作成に標準のモデル固有ドライバーを使用します。ドライバーがサーバーで利用できない場合、クライアントプリンターは適切なユニバーサルドライバーで自動的に作成されます。
ユニバーサル印刷が利用できない場合にのみ、プリンターモデル固有のドライバーを使用する	利用可能な場合、ユニバーサルプリントドライバーを使用します。ドライバーがサーバーで利用できない場合、クライアントプリンターは適切なモデル固有のプリンタードライバーで自動的に作成されます。

ユニバーサルプリントサーバーポリシー設定

ユニバーサルプリントサーバーセクションには、ユニバーサルプリントサーバーを処理するためのポリシー設定が含まれています。

SSL暗号スイート

この設定は、暗号化された印刷データストリーム（CGP）接続のためにUniversal Print Clientで使用されるSSL/TLS暗号スイートのセットを指定します。

暗号化された印刷Webサービス（HTTPS/SOAP）接続のためにUniversal Print Clientで使用される暗号スイートパッケージを制御するには、を参照してください。

デフォルト値: ALL

この設定には、ALL、COM、GOVのいずれかの値があります。

各値に対応する暗号スイートは次のとおりです:

ALL:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

COM:

TLS_ECDHE_RSA_AES128_CBC_SHA

GOV:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

SSL準拠モード

この設定は、暗号化された印刷データストリーム（CGP）接続にUniversal Print Clientが使用するNIST Special Publication 800-52への準拠レベルを指定します。

デフォルト値：なし。

この設定には次の値があります:

なし。

暗号化された印刷データストリーム（CGP）接続は、デフォルトの準拠モードを使用します。

SP800-52。

暗号化された印刷データストリーム（CGP）接続は、NIST Special Publication 800-52準拠モードを使用します。

SSL有効

この設定は、Universal Print Clientが以下の目的でSSL/TLSを使用するかどうかを指定します:

- 印刷データストリーム（CGP）接続
- Webサービス（HTTP/SOAP）接続

Universal Print Serverを有効にするを**Windowsのネイティブリモート印刷へのフォールバックを有効にする**に設定すると、Microsoft Windows Network Print Providerによってフォールバック接続が行われます。この設定は、これらのフォールバック接続には影響しません。

既定値: 無効

この設定は次の値をとります。

有効。

ユニバーサルプリントクライアントは、Universal Print Serverへの接続にSSL/TLSを使用します。

無効。

ユニバーサルプリントクライアントは、Universal Print Serverへの接続にSSL/TLSを使用します。

SSL FIPSモード

この設定は、Universal Print Clientが印刷データストリーム（CGP）接続のために使用するSSL/TLS暗号化モジュールがFIPSモードで実行されるかどうかを指定します。

既定値: 無効

この設定は次の値をとります。

有効。

FIPSモードがオンになります。

無効。

FIPSモードがオフになります。

SSLプロトコルバージョン

この設定は、Universal Print Client が使用する SSL/TLS プロトコルバージョンを指定します。

デフォルト値: ALL

この設定には、次の値があります。

ALL。

TLS バージョン 1.0、1.1、または 1.2 を使用します。

ティーエルエスブイワン.

TLS バージョン 1.0 を使用します。

TLSv1.1。

TLS バージョン 1.1 を使用します。

TLSv1.2。

TLS バージョン 1.2 を使用します。

SSL UNIVERSAL PRINT SERVER 暗号化印刷データストリーム (CGP) ポート

この設定は、Universal Print Server 暗号化印刷データストリーム (CGP) ポートの TCP ポート番号を指定します。このポートは、印刷ジョブのデータを受信します。

デフォルト値: 443

SSL UNIVERSAL PRINT SERVER 暗号化 WEB サービス (HTTPS/SOAP) ポート

この設定は、Universal Print Serverの暗号化されたWebサービス（HTTPS/SOAP）ポートのTCPポート番号を指定します。このポートは印刷コマンドのデータを受信します。

デフォルト値: 8443

UNIVERSAL PRINT SERVERの有効化

このポリシーは、Citrix Universal Print Server (UPS) の使用を有効または無効にします。このポリシー設定は、仮想デスクトップまたはサーバーホスティングアプリケーションを含む組織単位 (OU) に適用します。このポリシー設定には、Citrix UPSコンポーネントが要求されたプリントサーバーにインストールされていないか、利用できない場合に、ネイティブのWindowsリモート印刷サービスを使用してプリントサーバーへの接続を許可するフォールバックオプションが含まれています。このポリシーへの変更は、VDAが再起動された後にのみ適用されます。

デフォルトでは、Universal Print Serverは無効になっています。

この設定をポリシーに追加するときは、次のいずれかのオプションを選択します。

- **Windowsネイティブのリモート印刷へのフォールバックを有効にする**: 可能な場合、Universal Print Serverはネットワークプリンター接続を処理します。Universal Print Serverが利用できない場合、Windows Print Providerが使用されます。Windows Print Providerは、以前にWindows Print Providerで作成されたすべてのプリンターを引き続き処理します。
- **Windowsネイティブのリモート印刷へのフォールバックなしで有効にする**: Universal Print Serverは、ネットワークプリンター接続を排他的に処理します。Universal Print Serverが利用できない場合、ネットワークプリンター接続は失敗します。この設定は、Windows Print Providerを介したネットワーク印刷を実質的に無効にします。この設定を含むポリシーがアクティブな間は、以前にWindows Print Providerで作成されたプリンターは作成されません。
- **無効**: Universal Print Server機能は無効です。UNC名を持つネットワークプリンターに接続する際、Universal Print Serverへの接続は試行されません。リモートプリンターへの接続は、引き続きWindowsネイティブのリモート印刷機能を使用します。

UNIVERSAL PRINT SERVER印刷データストリーム (CGP) ポート

この設定は、Universal Print Server印刷データストリームのCommon Gateway Protocol (CGP) リスナーが使用するTCPポート番号を指定します。このポリシー設定は、プリントサーバーを含むOUにのみ適用します。

デフォルトでは、ポート番号は7229に設定されています。

有効なポート番号は1～65535の範囲である必要があります。

UNIVERSAL PRINT SERVER印刷ストリーム入力帯域幅制限 (KBPS)

この設定は、印刷データの転送速度の上限（キロビット/秒）を指定します。転送速度は、各印刷ジョブからCGPを使用してUniversal Print Serverに配信される印刷データに対して計算されます。このポリシー設定は、仮想デスクトップまたはサーバーホスティングアプリケーションを含むOUに適用します。

デフォルトでは、値は0であり、上限がないことを指定します。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) ポート

この設定は、Universal Print ServerのWebサービス (HTTP/SOAP) リスナーが使用するTCPポート番号を指定します。Universal Print Serverは、ネットワーク印刷シナリオでCitrixユニバーサル印刷ドライバーの使用を可能にするオプションコンポーネントです。

Universal Print Serverが使用される場合、印刷コマンドはCitrix Virtual Apps and Desktopsホストから Universal Print ServerにHTTP経由のSOAPで送信されます。この設定は、Universal Print Serverが受信HTTP/SOAPリクエストをリッスンするデフォルトのTCPポートを変更します。

ホストとプリントサーバーのHTTPポートは両方とも同じように構成する必要があります。ポートを同じように構成しない場合、ホストソフトウェアはUniversal Print Serverに接続しません。この設定は、Citrix Virtual Apps and Desktops上のVDAを変更します。さらに、Universal Print Serverのデフォルトポートも変更する必要があります。

デフォルトでは、ポート番号は8080に設定されています。

有効なポート番号は0～65535の範囲内である必要があります。

負荷分散用のUNIVERSAL PRINT SERVER

この設定は、他のCitrix®印刷ポリシー設定を評価した後、セッション起動時に確立されたプリンター接続の負荷分散に使用されるUniversal Print Serverを一覧表示します。プリンター作成時間を最適化するために、Citrixはすべての印刷サーバーが同じ共有プリンターのセットを持つことを推奨します。負荷分散のために追加できる印刷サーバーの数に上限はありません。

この設定は、プリントサーバーのフェイルオーバー検出とプリンター接続の回復も実装します。プリントサーバーは定期的に可用性がチェックされます。サーバー障害が検出された場合、そのサーバーは負荷分散スキームから削除されます。また、そのサーバー上のプリンター接続は、他の利用可能なプリントサーバーに再配布されます。障害が発生したプリントサーバーが回復すると、負荷分散スキームに戻されます。

Validate Servers をクリックして、各サーバーが印刷サーバーであること、サーバーリストに重複するサーバー名が含まれていないこと、およびすべてのサーバーに同一の共有プリンターセットがインストールされていることを確認します。この操作には時間がかかる場合があります。

UNIVERSAL PRINT SERVERサービス停止しきい値

この設定は、ロードバランサーが利用できないプリントサーバーが回復するのをどのくらいの期間待つかを指定します。この期間が過ぎると、サーバーは永続的にオフラインであると判断され、その負荷は他の利用可能なプリントサーバーに再配布されます。

デフォルトでは、しきい値は180（秒）に設定されています。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) 接続タイムアウト

この設定は、Universal Print Client が Universal Print Server Web サービスの connect() 操作がタイムアウトするまで待機する秒数を指定します。この設定には次の値があります。これらの値はすべて数値であり、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- 既定値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Client は操作が完了するまで指定された時間待機します。この操作は、TCPソケットの接続操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Client はオペレーティングシステムによって定義された既定のタイムアウトを使用します。この構成は、この変更前のUniversal Print Client の以前のバージョンに存在した利用可能な構成でした。

Universal Print Client は、Universal Print Server と通信するVirtual Delivery Agent (VDA) のコンポーネントです。

> **注：**
>
> このポリシー設定は、VDAバージョン7.35以降に適用されます。

UNIVERSAL PRINT SERVER WEB サービス (HTTP/SOAP) 受信タイムアウト

この設定は、Universal Print Client が Universal Print Server Web サービスの recv() 操作がタイムアウトするまで待機する秒数を指定します。この設定には次の値があり、これらの値はすべて数値であり、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- 既定値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Client は操作が完了するまで指定された時間待機します。この操作は、TCPソケットの受信操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが 0 の場合、Universal Print Client はオペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この設定は、この変更前の Universal Print Client の以前のバージョンで利用可能だった設定でした。

Universal Print Client は、Universal Print Server と通信する Virtual Delivery Agent (VDA) のコンポーネントです。

> **注:**
>
> このポリシー設定は、VDA バージョン 7.35 以降に適用されます。

UNIVERSAL PRINT SERVER WEB サービス (HTTP/SOAP) 送信タイムアウト

この設定は、Universal Print Client が Universal Print Server Web サービスの send() 操作がタイムアウトするまで待機する秒数を指定します。この設定には、次の値があります。これらの値はすべて数値であり、単位 (時間) は秒です。

- 最小値は 0 です。
- 最大値は 60 です。
- デフォルト値は 10 です。

タイムアウトが 1 から 60 (両端を含む) の場合、Universal Print Client は操作が完了するまで指定された時間待機します。この操作は、TCP ソケット送信操作です。ソケットは、TCP/IP ネットワークを介したプロセス間通信を可能にする Windows オペレーティングシステムの機能です。

タイムアウトが 0 の場合、Universal Print Client はオペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この設定は、この変更前の Universal Print Client の以前のバージョンで利用可能だった設定でした。

Universal Print Client は、Universal Print Server と通信する VDA のコンポーネントです。

> **注:**
>
> このポリシー設定は、VDA バージョン 7.35 以降に適用されます。

ユニバーサル印刷ポリシー設定

「**ユニバーサル印刷**」セクションには、ユニバーサル印刷を管理するためのポリシー設定が含まれています。

ユニバーサル印刷EMF処理モード

この設定は、Windowsユーザーデバイス上のEMFスプールファイルの処理方法を制御します。

デフォルトでは、EMFレコードはプリンターに直接スプールされます。

この設定をポリシーに追加するときは、オプションを選択します。

- プリンター用のEMFを再処理すると、EMFスプールファイルが再処理され、ユーザーデバイス上のGDIサブシステムを介して送信されます。この設定は、EMFの再処理を必要とするが、セッションで自動的に選択されない可能性のあるドライバーに使用できます。

- Citrix Universal™印刷ドライバーと併用すると、プリンターに直接スプールすることで、EMFレコードがスプールされ、処理のためにユーザーデバイスに配信されます。通常、これらのEMFスプールファイルはクライアントのスプールキューに直接挿入されます。EMF形式と互換性のあるプリンターおよびドライバーの場合、これが最速の印刷方法です。

ユニバーサル印刷の画像圧縮制限

この設定は以下を指定します:

- Citrix Universal印刷ドライバーで印刷される画像に利用可能な最大品質
- Citrix Universal印刷ドライバーで印刷される画像に利用可能な最小圧縮レベル

デフォルトでは、画像圧縮制限は「最高品質（ロスレス圧縮）」に設定されています。

「圧縮なし」が選択されている場合、EMF印刷の場合にのみ圧縮が無効になります。

この設定をポリシーに追加するときは、オプションを選択します。

- 圧縮なし
- 最高品質 (ロスレス圧縮)
- 高音質
- 標準品質
- 低品質 (最大圧縮)

この設定を**ユニバーサル印刷最適化のデフォルト**設定を含むポリシーに追加する場合は、次の点に注意してください。

- **ユニバーサル印刷イメージ圧縮制限**設定の圧縮レベルが、**ユニバーサル印刷最適化のデフォルト**設定で定義されているレベルよりも低い場合を考慮してください。この場合、画像はユニバーサル印刷イメージ圧縮制限設定で定義されているレベルで圧縮されます。
- 圧縮が無効になっている場合、ユニバーサル印刷最適化のデフォルト設定の「希望する画質」および「ヘビーウェイト圧縮を有効にする」オプションは、ポリシーに影響を与えません。

ユニバーサル印刷最適化のデフォルト

この設定は、セッション用にユニバーサル印刷ドライバーが作成される際の印刷最適化のデフォルト値を指定します。

- 希望する画質は、ユニバーサル印刷に適用されるデフォルトの画像圧縮制限を指定します。デフォルトでは、標準品質が有効になっており、ユーザーは標準または低品質の圧縮を使用してのみ画像を印刷できます。

- ヘビーウェイト圧縮を有効にするは、希望する画質で設定された圧縮レベルを超えて帯域幅を削減するかどうかを有効または無効にします。画質は低下しません。デフォルトでは、ヘビーウェイト圧縮は無効になっています。
- イメージとフォントのキャッシュ設定は、印刷ストリームに複数回出現するイメージとフォントをキャッシュするかどうかを指定します。この設定により、各固有のイメージまたはフォントがプリンターに一度だけ送信されることが保証されます。デフォルトでは、埋め込みイメージとフォントはキャッシュされます。これらの設定は、ユーザーデバイスがこの動作をサポートしている場合にのみ適用されます。
- 非管理者によるこれらの設定の変更を許可するは、ユーザーがセッション内でデフォルトの印刷最適化設定を変更できるかどうかを指定します。デフォルトでは、ユーザーはデフォルトの印刷最適化設定を変更できません。

注: これらのオプションはすべてEMF印刷でサポートされています。XPS印刷では、「希望する画質」オプションのみがサポートされます。

この設定を、**ユニバーサル印刷イメージ圧縮制限**設定を含むポリシーに追加する場合は、次の点に注意してください。

- **ユニバーサル印刷イメージ圧縮制限**設定の圧縮レベルが、**ユニバーサル印刷最適化のデフォルト**設定で定義されているレベルよりも低い場合を考慮してください。この場合、画像はユニバーサル印刷イメージ圧縮制限設定で定義されているレベルで圧縮されます。
- 圧縮が無効になっている場合、ユニバーサル印刷最適化のデフォルト設定の「希望する画質」および「ヘビーウェイト圧縮を有効にする」オプションは、ポリシーに影響しません。

ユニバーサル印刷プレビュー設定

この設定は、自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して印刷プレビュー機能を使用するかどうかを指定します。

デフォルトでは、自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して印刷プレビューは使用されません。

この設定をポリシーに追加するときは、オプションを選択します。

- 自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して印刷プレビューを使用しない
- 自動作成されたプリンターに対してのみ印刷プレビューを使用する
- 汎用ユニバーサルプリンターに対してのみ印刷プレビューを使用する
- 自動作成されたプリンターと汎用ユニバーサルプリンターの両方に対して印刷プレビューを使用する

ユニバーサル印刷の印刷品質制限

この設定は、セッションで印刷出力を生成するために利用できる最大ドット/インチ (dpi) を指定します。

デフォルトでは、「制限なし」が有効になっており、ユーザーは接続先のプリンターで許可されている最高の印刷品質を選択できます。

この設定が構成されている場合、出力解像度の観点から、ユーザーが利用できる最大の印刷品質が制限されます。印刷品質自体と、ユーザーが接続するプリンターの印刷品質機能の両方が、構成された設定に制限されます。

例えば、中解像度 (600 DPI) に設定されている場合、ユーザーは最大 600 DPI の品質で出力物を印刷できます。また、**ユニバーサルプリンター**ダイアログボックスの**詳細設定**タブにある**印刷品質**設定には、中品質 (600 DPI) までの解像度設定のみが表示されます。

この設定をポリシーに追加するときは、オプションを選択します。

- 下書き (150 DPI)
- 低解像度 (300 DPI)
- 中解像度 (600 DPI)
- 高解像度 (1200 DPI)
- 制限なし

セキュリティポリシー設定

セキュリティセクションには、セッション暗号化とログオンデータの暗号化を構成するためのポリシー設定が含まれています。

SecureICA の最小暗号化レベル

この設定は、サーバーとユーザーデバイス間で送信されるセッションデータを暗号化する最小レベルを指定します。

重要: Virtual Delivery Agent 7.x の場合、このポリシー設定は、RC5 128ビット暗号化によるログオンデータの暗号化を有効にするためにのみ使用できます。その他の設定は、Citrix Virtual Apps and Desktops のレガシーバージョンとの下位互換性のためにのみ提供されています。

VDA 7.x の場合、セッションデータの暗号化は、VDA のデリバリーグループの基本設定を使用して設定されます。デリバリーグループでSecure ICAを有効にするが選択されている場合、セッションデータはRC5（128ビット）暗号化を使用して暗号化されます。デリバリーグループで

Secure ICAを有効にするが選択されていない場合、セッションデータは基本暗号化で暗号化されます。

この設定をポリシーに追加するときは、オプションを選択します。

- Basic は、非RC5アルゴリズムを使用してクライアント接続を暗号化します。データストリームが直接読み取られるのを防ぎますが、復号化される可能性があります。デフォルトでは、サーバーはクライアント-サーバー間のトラフィックにBasic暗号化を使用します。
- RC5 (128 bit) logon only は、RC5 128ビット暗号化を使用してログオンデータのみを暗号化し、Basic暗号化を使用してクライアント接続を暗号化します。
- RC5 (40 bit) は、RC5 40ビット暗号化を使用してクライアント接続を暗号化します。
- RC5 (56 bit) は、RC5 56ビット暗号化を使用してクライアント接続を暗号化します。
- RC5 (128 bit) は、RC5 128ビット暗号化を使用してクライアント接続を暗号化します。

クライアント-サーバー間の暗号化に指定する設定は、環境内の他の暗号化設定やWindowsオペレーティングシステムと相互作用する可能性があります。サーバーまたはユーザーデバイスのいずれかで、より高い優先度の暗号化レベルが設定されている場合を考慮してください。この場合、公開リソースに指定した設定が上書きされる可能性があります。

特定のユーザーの通信とメッセージの整合性をさらに保護するために、暗号化レベルを上げることができます。ポリシーでより高い暗号化レベルが必要な場合、より低い暗号化レベルを使用しているCitrix Receiversは接続を拒否されます。

SecureICAは認証を実行したり、データの整合性をチェックしたりしません。サイトにエンドツーエンドの暗号化を提供するには、SecureICAをTLS暗号化と組み合わせて使用します。

SecureICAはFIPS準拠のアルゴリズムを使用しません。この設定が問題となる場合は、SecureICAを使用しないようにサーバーとCitrix Receiverを構成してください。

SecureICAは、機密保持のためにRFC 2040で説明されているRC5ブロック暗号を使用します。ブロックサイズは64ビット（32ビットワード単位の倍数）です。キー長は128ビットです。ラウンド数は12です。

RC5 ブロック暗号のキーは、セッションが作成されるときにネゴシエートされます。ネゴシエーションは Diffie-Hellman アルゴリズムを使用して実行されます。このネゴシエーションでは、Diffie-Hellman の公開パラメーターが使用されます。これらのパラメーターは、Virtual Delivery Agent がインストールされるときに Windows レジストリに保存されます。公開パラメーターは秘密ではありません。Diffie-Hellman ネゴシエーションの結果は秘密キーであり、そこから RC5 ブロック暗号のセッションキーが導出されます。ユーザーログオンとデータ転送には、個別のセッションキーが使用されます。また、Virtual Delivery Agent との間のトラフィックにも個別のセッ

ションキーが使用されます。したがって、各セッションには 4 つのセッションキーがあります。秘密キーとセッションキーは保存されません。RC5 ブロック暗号の初期化ベクトルも秘密キーから導出されます。

セッション制限ポリシー設定

セッション制限セクションには、セッションが強制的にログオフされるまでに接続を維持する期間を制御するポリシー設定が含まれています。

切断されたセッションタイマー

この設定は、切断されロックされたデスクトップが、セッションがログオフされるまでにロックされたままになる期間を指定するタイマーを有効または無効にします。

このタイマーが有効になっている場合、タイマーの期限が切れると、切断されたセッションはログオフされます。

デフォルトでは、切断されたセッションはログオフされません。

Remote PC Accessの切断されたセッションタイマー

この設定は、タイマーの期限が切れた後に切断されたユーザーセッションをログオフするタイマーを有効または無効にします。この設定を有効にする場合は、**切断されたセッションタイマー間隔**設定を使用して、ユーザーセッションがログオフされるまでに切断されたデスクトップがロックされたままになる期間を分単位で指定します。

デフォルトでは、この設定は無効になっています。

切断されたセッションタイマー間隔

この設定は、切断されロックされたデスクトップが、セッションがログオフされるまでにロックされたままになる期間を分単位で指定します。

デフォルトでは、期間は1,440分（24時間）です。

切断されたセッションタイマー – マルチセッション

この設定は、切断されたRDSセッションがログオフされるまでにどのくらいの期間持続できるかを決定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっており、切断されたセッションはログオフされません。

切断されたセッションタイマー間隔 – マルチセッション

この設定は、切断されたRDSセッションがログオフされるまでにどのくらいの期間（分単位）持続できるかを決定します。デフォルトでは、期間は1440分（24時間）です。

セッション接続タイマー

この設定は、ユーザーデバイスとデスクトップ間の途切れない接続の最大期間を指定するタイマーを有効または無効にします。このタイマーが有効になっている場合、タイマーの期限が切れるとセッションは切断されるかログオフされます。Microsoftの**時間制限に達したときにセッションを終了する**設定が、セッションの次の状態を決定します。

デフォルトでは、このタイマーは無効になっています。

セッション接続タイマー間隔

この設定は、ユーザーデバイスとデスクトップ間の途切れない接続の最大分数を示します。

デフォルトでは、最大継続時間は1,440分（24時間）です。

セッション接続タイマー – マルチセッション

この設定は、ユーザーデバイスとターミナルサーバー間の途切れない接続の最大継続時間を指定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっています。

セッション接続タイマー間隔 – マルチセッション

この設定は、ユーザーデバイスとRDSセッション間の途切れない接続の最大分数を示します。デフォルトでは、最大期間は1440分（24時間）です。

セッションアイドルタイマー

ユーザーが何も入力しない場合、この設定は以下を有効または無効にするために使用されます。

- デスクトップへの途切れないユーザーデバイス接続が維持される期間を指定するタイマー。

このタイマーの期限が切れると、セッションは切断状態になり、「**切断されたセッションタイマー**」が適用されます。「**切断されたセッションタイマー**」が無効になっている場合、セッションはログオフされません。

デフォルトでは、このタイマーは有効になっています。

セッションアイドルタイマー間隔

ユーザーからの入力がない場合、この設定は以下を指定するために使用されます。

- デスクトップへのユーザーデバイスの途切れない接続が維持される分数。

デフォルトでは、アイドル状態の接続は1,440分（24時間）維持されます。

セッションアイドルタイマー – マルチセッション

この設定は、ユーザーデバイスとターミナルサーバー間のアイドル接続の最大継続時間を決定するタイマーを有効または無効にします。既定では、このタイマーは無効になっています。

セッションアイドルタイマー間隔 – マルチセッション

この設定は、ユーザーデバイスとRDSセッション間のアイドル接続が何分間維持されるかを指定します。既定では、最大継続時間は1440分（24時間）です。

> **注:**
>
> Citrix®ポリシーを使用して構成されたマルチセッションマシンのタイマー設定は、Microsoftグループポリシーを通じて構成されたタイマー設定を上書きすることが想定されています。予期しない動作を避けるため、いずれかの方法を使用してタイマー設定を構成することをお勧めします。

セッションウォーターマークポリシー設定

「**セッションウォーターマーク**」セクションには、この機能を構成するためのポリシー設定が含まれています。 この機能を有効にすると、VDAマシンのネットワーク帯域幅とCPU使用率が大幅に増加します。利用可能なハードウェアリソースに基づいて、選択したVDAマシンにセッションウォーターマークを設定することをお勧めします。

> **重要**
>
> 他のウォーターマークポリシー設定を有効にするには、セッションウォーターマークを有効にします。より良いユーザーエクスペリエンスを実現するために、2つを超えるウォーターマークテキスト項目を有効にしないでください。

セッションウォーターマークを有効にする

この設定を有効にすると、セッション表示にセッション固有の情報を表示する不透明なテキストウォーターマークが表示されます。他のウォーターマーク設定は、この設定が有効になっているかどうかに依存します。

デフォルトでは、セッションウォーターマークは無効になっています。

クライアントIPアドレスを含める

この設定を有効にすると、セッションは現在のクライアントIPアドレスをウォーターマークとして表示します。

デフォルトでは、クライアントIPアドレスを含めるは無効になっています。

接続時間を含める

この設定を有効にすると、セッションウォーターマークに接続時間が表示されます。形式はyyyy/mm/dd hh:mmです。表示される時刻は、システムクロックとタイムゾーンに基づいています。

デフォルトでは、接続時間を含めるは無効になっています。

ログオンユーザー名を含める

この設定を有効にすると、セッションは現在のログオンユーザー名をウォーターマークとして表示します。表示形式はUSERNAME@DOMAINNAMEです。ユーザー名は最大20文字にすることをお勧めします。ユーザー名が20文字を超えると、文字フォントが過度に小さくなったり、切り捨てられたりして、ウォーターマークの効果が低下する可能性があります。

デフォルトでは、ログオンユーザー名を含めるは有効になっています。

VDAホスト名を含める

この設定を有効にすると、セッションは現在のICA®セッションのVDAホスト名をウォーターマークとして表示します。

デフォルトでは、VDAホスト名を含める設定が有効になっています。

VDA IPアドレスを含める

この設定を有効にすると、セッションは現在のICAセッションのVDA IPアドレスをウォーターマークとして表示します。

デフォルトでは、VDA IPアドレスは無効になっています。

セッションウォーターマークのスタイル

この設定は、単一のウォーターマークテキストラベルを表示するか、複数のラベルを表示するかを制御します。「**値**」ドロップダウンメニューから「**複数**」または「**単一**」を選択します。

「**複数**」は、セッションに5つのウォーターマークラベルを表示します。中央に1つ、四隅に4つです。

「**単一**」は、セッションの中央に単一のウォーターマークラベルを表示します。

デフォルトでは、セッションウォーターマークスタイルは複数です。

ウォーターマークのカスタムテキスト

この設定を使用すると、カスタムテキスト（たとえば、会社名）をセッションウォーターマークに表示できます。空でない文字列を構成すると、ウォーターマークで有効になっている他の情報を

追加して、新しい行にテキストが表示されます。ウォーターマークカスタムテキストは25 Unicode文字に制限されています。より長い文字列を構成した場合、25文字に切り詰められます。

デフォルトのテキストはありません。

Citrix Virtual Apps and Desktops™ 7 2206以降、テキストにカスタムタグを使用してさらにカスタマイズを追加できます。その結果、カスタムテキストの最大文字数は1024に増加しました。

ウォーターマーク設定で利用可能なタグは、次の表に記載されています。

タグ	説明	例
`<font=value>`	ウォーターマークテキストのフォントを変更できます。値はVDAで利用可能なフォントの名前です。	`<font=Courier New>`
`<fontzoom=value>`	フォントのズーム係数のパーセンテージを設定できます。ウォーターマークテキストの200%ズームの場合、値は200です。	`<fontzoom=200>`
`<position=value>`	ウォーターマークテキストの位置を変更できます。値は `center`、`topleft`、`topright`、`bottomleft`、および `bottomright` です。このタグはシングルスタイルでのみ適用可能です。	`<position=topright>`
`<rotation=value>`	ウォーターマークテキストを回転できます。値は度数で指定され、範囲は-360から360です。	`<rotation=45>`
`<style=value>`	表示スタイルを変更できます。このタグはセッションウォーターマークスタイルポリシーを上書きします。	`<style=single>`

利用可能なウォーターマークスタイルは次のとおりです。

- シングルスタイル - セッションの中央に単一のウォーターマークテキストラベルが表示されます。位置タグを使用して場所を変更できます。
- xスタイルまたは複数 - セッションに5つのウォーターマークラベルが表示されます。中央に1つ、各隅に1つずつです。
- タイル - セッションに複数のラベルが表示されます。ウォーターマークテキストは画面全体に均等に配置されます。

ウォーターマークテキストを変更するために利用できるタグは、次の表に記載されています。

タグ	説明
`<clientip>`	エンドポイントのIPアドレス。
`<date>`	セッションが確立された日付。
`<domain>`	ログインしているユーザーアカウントのドメイン名。
`<hostname>`	VDAのマシン名。
`<newline>`	追加の行を作成します。
`<serverip>`	VDAのIPアドレス。
`<time>`	セッションが確立された時刻。
`<username>`	ユーザーの名前。

注:

- **ウォーターマークカスタムテキスト**ポリシーは、**セッションウォーターマークを有効にする**ポリシーが有効になっている場合にのみ適用されます。デフォルト値は*無効*です。
- ウォーターマークテキストを変更するためにタグを使用する場合、**セッションウォーターマークを有効にする**を除く他のすべてのセッションウォーターマークポリシーは無視されます。ウォーターマークテキスト設定にタグを使用する場合、他のすべてのウォーターマークポリシーを使用できます。

透かしの透明度

ウォーターマークの不透明度を0から100まで指定できます。指定する値が大きいほど、ウォーターマークは不透明になります。

デフォルトでは、値は17です。

TWAINデバイスのポリシー設定

TWAINデバイスセクションには、以下のポリシー設定が含まれています。

- デジタルカメラやスキャナーなどのクライアントTWAINデバイスのマッピング
- サーバーからクライアントへの画像転送の最適化

> **注:**
>
> Citrix Receiver for Windows 4.5では、TWAIN 2.0がサポートされています。

クライアントTWAINデバイスのリダイレクト

TWAINデバイスは、TWAINプロトコルを使用して、サーバーでホストされている画像処理アプリケーションと通信します。

この設定では、ユーザーデバイス上のTWAINデバイスへのユーザーのアクセスを許可または禁止します。デフォルトでは、TWAINデバイスリダイレクトは許可されています。

関連するポリシー設定は次のとおりです。

- TWAIN圧縮レベル
- TWAINデバイスのリダイレクト帯域幅制限
- TWAINデバイスリダイレクト帯域幅制限の割合

TWAIN圧縮レベル

この設定は、クライアントからサーバーへの画像転送の圧縮レベルを指定します。最良の画質には「低」、良好な画質には「中」、低い画質には「高」を使用します。デフォルトでは、中程度の圧縮が適用されます。

USBデバイスのポリシー設定

USBデバイスセクションには、USBデバイスのファイルリダイレクトを管理するためのポリシー設定が含まれています。

クライアントUSBデバイスの最適化ルール

クライアントUSBデバイスの最適化ルールは、最適化を無効にするため、または最適化モードを変更するためにデバイスに適用できます。

ユーザーがUSB入力デバイスを接続すると、ホストは**USBポリシー**設定がそのデバイスを許可するかどうかを確認します。デバイスが許可されている場合、ホストはデバイスの**クライアントUSBデバイス最適化ルール**を確認します。ルールが指定されていない場合、デバイスは最適化されません。キャプチャモード (04) は、署名デバイスに推奨されるモードです。高遅延によってパフォーマンスが低下する他のデバイスの場合、管理者はインタラクティブモード (02) を有効にできます。この記事の表で利用可能なモードの説明を参照してください。

知っておくとよいこと

- Wacomの署名パッドとタブレットを使用する場合は、スクリーンセーバーを無効にすることをお勧めします。スクリーンセーバーを無効にする手順は、このセクションの最後にあります。
- Wacom STU署名パッドおよびタブレットシリーズ製品の最適化のサポートは、Citrix Virtual Apps and Desktops™ポリシーのインストール時に事前設定されています。
- 署名デバイスはCitrix Virtual Apps and Desktops全体で機能し、署名デバイスとして使用するためにドライバーを必要としません。Wacomには、デバイスをさらにカスタマイズするためにインストールできる追加のソフトウェアがあります。`<http://www.wacom.com/>`を参照してください。
- 描画タブレット。特定の描画入力デバイスは、PCI/ACPIバス上でHIDデバイスとして表示される場合があり、サポートされていません。これらのデバイスは、クライアント上のUSBホストコントローラーに接続して、Citrix Virtual Desktopsセッション内にリダイレクトしてください。

ポリシールールは、空白で区切られたtag=value式の形式を取ります。以下のタグがサポートされています。

タグ名	説明
モード	最適化モードは、class=**03**の入力デバイスでサポートされています。サポートされているモードは次のとおりです。最適化なし - 値**01**。インタラクティブモード - 値**02**。ペンタブレットや3D Proマウスなどのデバイスに推奨されます。キャプチャモード - 値**04**。署名パッドなどのデバイスに推奨されます。

タグ名	説明
VID	デバイス記述子からのベンダーID。4桁の16進数として。
PID	デバイス記述子からのプロダクトID。4桁の16進数として。
REV	デバイス記述子からのリビジョンID。4桁の16進数として。
クラス	デバイス記述子またはインターフェース記述子のいずれかからのクラス。
サブクラス	デバイス記述子またはインターフェース記述子のいずれかからのサブクラス。
保護	デバイス記述子またはインターフェース記述子のいずれかからのプロトコル。

例

Mode=00000004 VID=067B PID=1230 class=03 #キャプチャモードで動作する入力デバイス

Mode=00000002 VID=067B PID=1230 class=03 #対話モードで動作する入力デバイス (デフォルト)

Mode=00000001 VID=067B PID=1230 class=03 #最適化なしで動作する入力デバイス

Mode=00000100 VID=067B PID=1230 #デバイスセットアップの最適化が無効（デフォルト）

Mode=00000200 VID=067B PID=1230 #デバイスセットアップの最適化が有効

Wacom署名パッドデバイスのスクリーンセーバーを無効にする

Wacom署名パッドおよびタブレットを使用するには、Citrix®はスクリーンセーバーを次のように無効にすることをお勧めします。

1. デバイスをリダイレクトした後、**Wacom-STU-Driver**をインストールします。
2. 署名パッドのコントロールパネルにアクセスするには、**Wacom-STU-Display MSI**をインストールします。
3. **コントロールパネル > Wacom STU Display > STU430** または **STU530** に移動し、お使いのモデルのタブを選択します。

4. 「**変更**」を選択し、UACセキュリティウィンドウが表示されたら「**はい**」を選択します。
5. 「**スライドショーを無効にする**」を選択し、「**適用**」を選択します。

1つの署名パッドモデルに対して設定が行われると、その設定はすべてのモデルに適用されます。

クライアントUSBデバイスのリダイレクト

この設定により、USBデバイスのユーザーデバイスへのリダイレクトおよびユーザーデバイスからのリダイレクトを許可または禁止します。

デフォルトでは、USBデバイスはリダイレクトされません。

クライアントUSBデバイスリダイレクト規則

この設定は、USBデバイスのリダイレクトルールを指定します。

デフォルトでは、ルールは指定されていません。

ユーザーがUSBデバイスを接続すると、ホストデバイスは一致が見つかるまで各ポリシー規則と照合します。任意のデバイスに対する最初の一致が決定的なものと見なされます。最初の一致が許可ルールである場合、デバイスは仮想デスクトップにリモート接続されます。最初の一致が拒否ルールである場合、デバイスはローカルデスクトップでのみ利用可能です。一致が見つからない場合は、デフォルトのルールが使用されます。

ポリシー規則は、{Allow:|Deny:} の形式で、その後に空白で区切られたタグ=値の式が続きます。以下のタグがサポートされています。

タグ名	説明
VID	デバイス記述子からのベンダーID
PID	デバイス記述子からの製品ID
REL	デバイス記述子からのリリースID
クラス	デバイス記述子またはインターフェイス記述子のいずれかからのクラス
サブクラス	デバイス記述子またはインターフェイス記述子のいずれかからのサブクラス
プロトコル	デバイス記述子またはインターフェイス記述子のいずれかからのプロトコル

ポリシー規則を作成する際は、次の点に注意してください。

- ルールでは大文字と小文字は区別されません。
- ルールには、# で始まるオプションのコメントを末尾に含めることができます。
- 空行およびコメントのみの行は無視されます。
- タグは一致演算子 = を使用する必要があります（例：VID=067B_）。
- 各ルールは新しい行から開始するか、セミコロンで区切られたリストの一部である必要があります。
- USB Implementers Forum, Inc. のWebサイトで入手可能なUSBクラスコードを参照してください。

管理者定義の USB ポリシールールの例:

- 許可: VID=067B PID=0007 # その他の産業、その他のフラッシュドライブ
- 拒否: Class=08 subclass=05 # マスストレージ
- すべての USB デバイスを拒否するルールを作成するには、他のタグなしで「DENY:」を使用します。

クライアントUSBプラグアンドプレイデバイスリダイレクト

この設定により、カメラやPOS (point-of-sale) デバイスなどのプラグアンドプレイデバイスのクライアントセッションでの使用を許可または禁止できます。

デフォルトでは、プラグアンドプレイデバイスのリダイレクトは許可されています。「許可」に設定すると、特定のユーザーまたはグループのすべてのプラグアンドプレイデバイスがリダイレクトされます。「禁止」に設定すると、どのデバイスもリダイレクトされません。

USB デバイスの自動リダイレクトを構成する

USB サポートが有効になっている場合、USB デバイスは自動的にリダイレクトされます。また、USB ユーザー設定は USB デバイスを自動的に接続するように設定されています。

> **注:**
>
> Receiver for Windows 4.2では、デスクトップアプライアンスモードで動作している場合もUSBデバイスは自動的にリダイレクトされます。また、接続バーは表示されません。以前のバージョンのCitrix Receiver for Windowsでは、USBデバイスは以下のモードで動作している場合も自動リダイレクトされます。

- デスクトップアプライアンスモード
- 仮想マシン (VM) ホスト型アプリケーション

すべてのUSBデバイスをリダイレクトすることが常に最適とは限りません。ユーザーは、自動的にリダイレクトされないUSBデバイスリストからデバイスを明示的にリダイレクトできます。USBデバイスが一覧表示されたりリダイレクトされたりするのを防ぐには、クライアントエンドポイントまたはDDCポリシーのいずれかでDeviceRulesを使用します。詳細については、管理ガイドを参照してください。

注意:

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

USBデバイスの自動リダイレクトに関するユーザー設定

ポリシー:

1. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrix Components > Citrix Receiver™ > クライアントデバイスのリモート処理 > Generic USB Remoting**に移動します。
2. **新しいUSBデバイス**を開き、**有効**を選択して**OK**をクリックします。
3. 「**既存のUSBデバイス**」を開き、「**有効**」を選択して、「**OK**」をクリックします。

シトリックス レシーバー:

1. **シトリックス レシーバー 環境設定 > 接続** に移動します。
2. 次のオプションが選択されていることを確認します。
   - セッション開始時にデバイスを自動的に接続する
   - セッション実行中に新しいデバイスが接続された場合、そのデバイスを自動的に接続する。
3. 「**OK**」をクリックします。

すべてのレジストリキーとポリシーの変更は、Windowsクライアントデバイスに適用されます。

通常のUSBプリンターのリダイレクト

通常のUSBプリンターに最適なソリューションは、専用のユニバーサルプリンタードライバーと仮想チャネルを使用して印刷を実行することです。デフォルトでは、通常のUSBプリンターは自動的にリダイレクトされません。

通常のプリンターはヒューリスティックを使用して検出されます。また、例えばスキャン機能を備えた高度なプリンターは、完全に機能させるにはUSBサポートを使用してリダイレクトする必要がある場合があります。

通常のプリンターが自動的にリダイレクトされるかどうかを構成するには、このレジストリを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectPrinters

種類: DWORD

データ: 00000000

デフォルト値は0です（自動的にリダイレクトしません）。値を0より大きい任意の数値に変更すると、USBサポートが有効になり、通常のUSBプリンターがリダイレクトされます。

このレジストリキーにActive Directoryポリシーを展開することもでき、両方が存在する場合は非ポリシー値を上書きします。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectPrinters

種類: DWORD

データ: 00000000

通常のオーディオデバイスのリダイレクト

通常のプリンターと同様に、通常のオーディオデバイスからオーディオデータを送信するには、ICA®の専用オーディオ仮想チャネルを使用することで最高のユーザーエクスペリエンスが得られます。ただし、USBサポートを使用して一部の特殊なデバイスをリダイレクトする必要がある場合があります。どのデバイスが通常のオーディオデバイスであるかを判断するためにヒューリスティックが使用されます。

クライアントエンドポイントでこのレジストリを使用して、通常のオーディオデバイスが自動的にリダイレクトされるかどうかを構成します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectAudio

種類: DWORD

データ: 00000000

デフォルトは0に設定されています（自動的にリダイレクトしません）。値をゼロ以外に変更すると、USBサポートにより通常のUSBオーディオデバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値をレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectAudio

種類: DWORD

データ: 00000000

通常のストレージデバイス（マスストレージデバイス）のリダイレクト

通常のストレージデバイスの場合、最適化も実行するクライアントドライブマッピングなどの専用仮想チャネルを使用することで、最高のユーザーエクスペリエンスを実現できます。ファイルの単純な読み書きに加えて、CD/DVD の書き込みや暗号化されたファイルシステムデバイスへのアクセスなどの特定の特殊なタスクを実行するには、汎用 USB サポートを使用してデバイスをリダイレクトする必要がある場合があります。

ヒューリスティックを使用して、どのデバイスが通常のストレージデバイスであるかを判断します。このレジストリキーを使用して、通常のストレージデバイスを自動的にリダイレクトするかどうかを構成します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectStorage

種類: DWORD

データ: 00000000

デフォルトは 0 (自動的にリダイレクトしない) に設定されています。値をゼロ以外に変更すると、汎用 USB サポートを使用して通常の USB ストレージデバイスがリダイレクトされます。

Active Directory ポリシーを使用して、この値を次のレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きすることもできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectStorage

種類: DWORD

データ: 00000000

> **注記:**
>
> 汎用USBサポートを使用している場合、通常のストレージデバイスへの読み取り専用アクセスは構成できませんが、CDMを使用している場合は構成できます。

ハードウェア暗号化機能付きUSBフラッシュドライブのリダイレクト

ハードウェア暗号化機能付きUSBフラッシュドライブは通常、暗号化されたストレージパーティションと、暗号化されたパーティションのロックを解除するためのユーティリティが含まれる2つ目のユーティリティパーティションで構成されています。USBフラッシュドライブデバイスの場合、最適化も実行する専用のクライアントドライブマッピング/動的サムドライブマッピングHDX仮想チャネルを使用することで、最高のユーザーエクスペリエンスを実現できます。

汎用USBリダイレクトは、以下の場合に必要です。

- Windows以外のクライアント (例: Linuxクライアント)
- 顧客がクライアント上のローカル機能へのユーザーアクセスを制限 (ロックダウン) しているクライアント

汎用USBリダイレクトは、ハードウェア暗号化なしで任意のUSBストレージデバイスをシングルセッションOSおよびマルチセッションOS VDAセッションの両方にリダイレクトできます。

Citrix Virtual Apps and Desktops 7 1808より前は、ハードウェア暗号化機能付きUSBフラッシュドライブをシングルセッションOSまたはマルチセッションOS VDAセッションにリダイレクトする有効な方法はありませんでした。Citrix Virtual Apps and Desktops 7 1808で導入された新機能の強化により、ハードウェア暗号化機能付きUSBフラッシュドライブの汎用USBリダイレクトがシングルセッションOSおよびマルチセッションOS VDAセッションでサポートされます。 デバイスが

リダイレクトされた後、そのドライブはローカルクライアントに表示されません。そのため、ドライブのロック解除が必要な場合は、セッション内で実行してください。この機能にはWindows Update KB4074590が必要です。

通常の静止画像デバイス (スキャナーおよびデジタルカメラ)

通常の静止画像デバイスの場合、最適化も実行する専用の仮想チャネル (TWAIN仮想チャネルなど) を使用することで、最高のユーザーエクスペリエンスを実現できます。これらのデバイスは業界標準に準拠している必要があります。デバイスが非準拠であるか、本来の意図どおりに使用されていないと見なされる場合、汎用USBリダイレクトがデバイスを使用する唯一の方法となる可能性があります。どのデバイスが通常の静止画像デバイスであるかを判断するためにヒューリスティックが使用されます。

このレジストリキーを使用して、通常の静止画像デバイスが自動的にリダイレクトされるかどうかを構成します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectImage

種類: DWORD

データ: 00000000

デフォルトは0に設定されています（自動的にリダイレクトされません）。値を0以外に変更すると、汎用USBのプレーンなUSB静止画デバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値をこのレジストリキーに展開することもでき、両方が存在する場合は非ポリシー値を上書きします。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectImage

種類: DWORD

データ: 00000000

デバイス固有の設定

Citrix最適化可能デバイスを選択するために使用されるヒューリスティックは、必ずしもユーザーの意図と一致するとは限りません。Citrix最適化可能デバイスの例としては、プリンター、オーディオ、ビデオ、ストレージ、静止画デバイスなどがあります。上記にリストされていないデバイ

スの自動リダイレクトを制御したい場合があります。自動リダイレクトはデバイス固有に制御できます。

例として、DemoTech 2,000バーコードリーダーはUSBサポートを使用してリダイレクトする必要はありません。ベンダー識別子12AB、製品識別子5678を持っています。これらの16進数はデバイスマネージャーで見つけることができます。

これが自動的にリダイレクトされるのを防ぐには、このデバイス固有のレジストリキーを作成します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名前: AutoRedirect

種類: DWORD

データ: 00000000

値が0の場合、デバイスは自動的にリダイレクトされません。0以外の値は、デバイスが自動リダイレクトの対象となることを示します（ユーザー設定による）。ベンダー識別子と製品識別子の間には単一のスペース文字があります。

Active Directory ポリシーを使用して、このレジストリキーにこの値を展開することもできます。両方が存在する場合、非ポリシー値が上書きされます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名前: AutoRedirect

種類: DWORD

データ: 00000000

デバイス固有の AutoRedirect 設定は、上記で説明したより一般的な AutoRedirectXXX 値よりも優先されます。Citrix 最適化デバイスのデフォルトのヒューリスティックは、デバイスを汎用として誤解する可能性があります。そのため、デバイスを自動的にリダイレクトするには、デバイス固有の AutoRedirect 値を 1 に設定してください。

既存のUSBデバイスの自動接続を許可する

この設定は、セッション開始時にエンドポイントに接続されている既存の USB デバイスがリモートセッションに自動的に接続されることを許可または禁止します。

この設定をポリシーに追加する場合は、次のいずれかのオプションを選択します。

- 利用可能なUSBデバイスをリダイレクトする前に確認する。
- 利用可能なUSBデバイスを自動的にリダイレクトしない。
- 利用可能なUSBデバイスを自動的にリダイレクトする。

デフォルトでは、**利用可能なUSBデバイスをリダイレクトする前に確認する**オプションが選択されています。選択されたポリシーに基づいて、クライアントの**環境設定** > **デバイス**セクションで選択されたオプションを上書きできます。

> **注:**
>
> 現在、**既存のUSBデバイスの自動接続を許可する**ポリシーは、Citrix Workspace™ app for Windowsにのみ適用されます。

新しく接続されたUSBデバイスの自動接続を許可する

この設定は、セッション中にエンドポイントに挿入されたUSBデバイスをリモートセッションに自動接続することを許可または防止します。

この設定をポリシーに追加するときは、次のいずれかのオプションを選択します。

- 利用可能なUSBデバイスをリダイレクトする前に確認する。
- 利用可能なUSBデバイスを自動的にリダイレクトしない。
- 利用可能なUSBデバイスを自動的にリダイレクトします。

デフォルトでは、**利用可能なUSBデバイスをリダイレクトする前に確認する**オプションが選択されています。選択されたポリシーに基づいて、クライアントの**基本設定** > **デバイス**セクションで選択されたオプションが上書きされる場合があります。

> **注:**
>
> 現在、**新しく接続されたUSBデバイスの自動接続を許可する**ポリシーは、Citrix Workspace アプリ for Windowsにのみ適用されます。

クライアントUSBデバイスリダイレクト規則 (バージョン2)

この設定は、USBデバイスをリモートセッションにフィルタリング、分割、および自動接続するための規則を指定します。

この設定が選択されている場合、ホストは *クライアントUSBデバイスリダイレクト規則* 設定を、この設定で構成されたデバイス規則で上書きします。

詳しくは、「複合USBデバイスリダイレクトの構成」を参照してください。

仮想チャネル許可リストポリシー設定

仮想チャネル許可リストポリシー設定は、ICA®セッションで開くことが許可されている仮想チャネルを指定する許可リストの使用を有効にします。

無効にすると、すべての仮想チャネルが許可されます。

有効にすると、Citrix®仮想チャネルのみが許可されます。

カスタムまたはサードパーティの仮想チャネルを使用するには、仮想チャネルをリストに追加します。仮想チャネルをリストに追加するには：

1. 仮想チャネル名の後にコンマを入力します。
2. 仮想チャネルにアクセスするプロセスのパスを入力します。

複数の実行可能パスをリストでき、パスはコンマで区切られます。

例:

```
CTXCVC1,C:\VC1\vchost.exe
```

```
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```

Citrix Virtual Apps and Desktops 7 2109以降、仮想チャネル許可リストはデフォルトで有効になっています。許可リストに仮想チャネルを追加する方法の詳細については、「許可リストへの仮想チャネルの追加」を参照してください。

Skype for Business 用 HDX RealTime Optimization Pack を使用している場合は、仮想チャネルを許可リストに追加します。詳細については、「HDX RealTime Optimization Pack ドキュメント」を参照してください。

> **重要:**
>
> 設定を有効にするには、VDAマシンを再起動する必要があります。

> 仮想チャネルの詳細については、「ICA仮想チャネル」を参照してください。

仮想チャネル許可リストのログ記録

このポリシー設定を使用して、仮想チャネル許可リストのログ記録レベルを構成できます。

次のオプションが利用可能です。

オプション	説明
無効	すべてのログイベントを無効にします。
警告のみをログに記録	許可リストに含まれていない、開こうとするカスタム仮想チャネルに対してのみイベントがログに記録されます。
すべてのイベントをログに記録	すべてのイベントがログに記録されます

仮想チャネル許可リストのログスロットリング

このポリシー設定を使用して、アクティブなセッションのイベントログ記録の頻度を構成できます。

各仮想チャネルのすべてのイベントは、最初に発生したときにログに記録されます。セッションがアクティブな間、スロットリング期間中は繰り返し発生するイベントは抑制されます。セッションが切断された場合、スロットリング期間はリセットされます。

DVCの仮想チャネル許可リスト

ICAセッションで開くことを許可されている動的仮想チャネルを指定する許可リストの使用を有効にします。

無効にすると、すべての動的仮想チャネルが許可されます。

有効にすると、動的仮想チャネルは許可されません。この機能で動的仮想チャネル（DVC）を使用するには、DVCをリストに追加する必要があります。DVCをリストに追加するには、セッションホストでDVCにアクセスするプロセスのパスを入力し、その後にコンマ、クライアント側プラグイン名、コンマ、プラグインが使用するリスナーの名前を入力します。複数のリスナー名はコンマで区切って追加できます。

ワイルドカードを使用して、プラグインがサポートするすべてのリスナーを許可できます。

ワイルドカードを使用して、プロセスパス内の単一のディレクトリ名を置き換えたり、プロセスパス内のディレクトリ名の一部を置き換えたり、実行可能ファイル名を置き換えたり、実行可能ファイル名の一部を置き換えたりすることもできます。

この設定への変更は、セッションホストを再起動した後にのみ適用されます。

例: クライアント側プラグイン: `DvcPlugin1.dll`, `DvcPlugin2.dll`, `DvcPlugin3.dll`

許可リストエントリ: `C:\Program Files\App\run1.2.exe,DvcPlugin1,` ListenerName1 `C:\Program Files*\run*.exe,DvcPlugin2,ListenerName1,ListenerName2` `C:\Program Files\App\run1.2.exe,DvcPlugin3,*`

視覚表示ポリシー設定

視覚表示セクションには、仮想デスクトップからユーザーデバイスに送信される画像の品質を制御するためのポリシー設定が含まれています。

簡易グラフィックの優先色深度

このポリシー設定は、VDAバージョン7.6 FP3以降で利用可能です。8ビットオプションは、VDAバージョン7.12以降で利用可能です。

この設定により、簡易グラフィックがネットワーク経由で送信される際の色深度を下げることができます。ピクセルあたり8ビットまたは16ビットに下げることで、低帯域幅接続での応答性が向上する可能性があります。ただし、この操作により画質がわずかに低下する場合があります。8ビットの色深度は、圧縮にビデオコーデックを使用ポリシー設定が**画面全体**に設定されている場合はサポートされません。

デフォルトの優先色深度はピクセルあたり24ビットです。

8ビット設定がVDAバージョン7.11以前に適用された場合、VDAは24ビット（デフォルト）の色深度にフォールバックします。

ターゲットフレームレート

この設定は、仮想デスクトップからユーザーデバイスに送信される1秒あたりの最大フレーム数を指定します。

デフォルトでは、最大は1秒あたり30フレームです。

1秒あたりのフレーム数を高く設定する（例：30）と、ユーザーエクスペリエンスは向上しますが、より多くの帯域幅が必要になります。1秒あたりのフレーム数を減らす（例：10）と、ユーザーエクスペリエンスを犠牲にしてサーバーのスケーラビリティが最大化されます。CPUが遅いユーザーデバイスの場合、ユーザーエクスペリエンスを向上させるために低い値を指定してください。

1秒あたりの最大サポートフレームレートは60です。

視覚品質

この設定は、ユーザーデバイスに表示される画像の希望する視覚品質を指定します。

デフォルトでは、この設定は「中」です。

画像の品質を指定するには、次のいずれかのオプションを選択します。

- **低** - 帯域幅が制限されたネットワークで、対話性のために視覚的な品質を犠牲にできる場合に推奨されます。
- **中** - ほとんどのユースケースで最高のパフォーマンスと帯域幅効率を提供します。
- **高** - 視覚的にロスレスな画質が必要な場合に推奨されます。
- **ロスレスにビルド** - ネットワークアクティビティが高い期間はロッシー画像をユーザーデバイスに送信し、ネットワークアクティビティが低下した後はロスレス画像を送信します。この設定により、帯域幅が制限されたネットワーク接続でのパフォーマンスが向上します。
- **常にロスレス** - 画像データの保持が不可欠な場合は、「**常にロスレス**」を選択して、ロッシーデータがユーザーデバイスに送信されないようにします。たとえば、画質の低下が許されないX線画像を表示する場合などです。

動きのある画像ポリシー設定

動きのある画像セクションには、動的な画像の圧縮を削除または変更できる設定が含まれています。

最小画像品質

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、アダプティブディスプレイの許容される最小画像品質を指定します。圧縮が少ないほど、表示される画像の品質は高くなります。超高、非常に高、高、標準、低の圧縮から選択します。

デフォルトでは、これは標準に設定されています。

動きのある画像の圧縮

この設定は、アダプティブディスプレイが有効になっているかどうかを指定します。アダプティブディスプレイは、利用可能な帯域幅に基づいて、スライドショーのビデオやトランジションスライドの画質を自動的に調整します。アダプティブディスプレイが有効になっている場合、ユーザーは品質の低下なしにスムーズなプレゼンテーションを見ることができます。

デフォルトでは、アダプティブディスプレイは有効になっています。

VDAバージョン7.0から7.6の場合、この設定はレガシーグラフィックモードが有効になっている場合にのみ適用されます。VDAバージョン7.6 FP1以降の場合、この設定はレガシーグラフィック

モードが有効になっている場合、またはレガシーグラフィックモードが無効でビデオコーデックがグラフィックの圧縮に使用されていない場合に適用されます。

レガシーグラフィックモードが有効になっている場合、ポリシーの変更を有効にするにはセッションを再起動する必要があります。アダプティブディスプレイはプログレッシブディスプレイと相互排他的です。アダプティブディスプレイを有効にするとプログレッシブディスプレイが無効になり、その逆も同様です。ただし、プログレッシブディスプレイとアダプティブディスプレイの両方を同時に無効にすることができます。プログレッシブディスプレイはレガシー機能であるため、XenAppまたはXenDesktopには推奨されません。プログレッシブしきい値レベルを設定すると、アダプティブディスプレイが無効になります。

プログレッシブ圧縮レベル

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、詳細度は低いものの、より高速な画像の初期表示を提供します。

デフォルトでは、プログレッシブ圧縮は適用されません。

通常の非可逆圧縮設定で定義された、より詳細な画像は、利用可能になったときに表示されます。写真などの帯域幅を多く消費するグラフィックの表示を改善するには、非常に高い圧縮または超高圧縮を使用します。

プログレッシブ圧縮を効果的にするには、その圧縮レベルが非可逆圧縮レベル設定よりも高くなければなりません。

注：プログレッシブ圧縮に関連する圧縮レベルの増加は、クライアント接続を介した動的画像の対話性も向上させます。回転する3Dモデルのような動的画像の品質は、画像が動きを停止するまで一時的に低下し、その時点で通常の非可逆圧縮設定が適用されます。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮しきい値
- プログレッシブヘビーウェイト圧縮

プログレッシブ圧縮しきい値

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、プログレッシブ圧縮が適用される接続の最大帯域幅を1秒あたりのキロビットで表します。これは、この帯域幅以下のクライアント接続にのみ適用されます。

デフォルトでは、しきい値は1秒あたり2147483647キロビットです。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮しきい値
- プログレッシブヘビーウェイト圧縮

目標最小フレームレート

この設定は、低帯域幅の条件下で、動的画像に対してシステムが維持しようとする1秒あたりの最小フレームレートを指定します。

デフォルトでは、これは10fpsに設定されています。

VDAバージョン7.0から7.6では、この設定はレガシーグラフィックモードが有効な場合にのみ適用されます。VDAバージョン7.6 FP1以降では、この設定はレガシーグラフィックモードが無効または有効のどちらの場合でも適用されます。

> **注:**
>
> 目標最小フレームレートポリシーは非推奨となり、10 fpsに設定されています。これは、グラフィックステータスインジケーターの品質スライダーを使用してエンドユーザーが変更できます。

静止画像ポリシー設定

静止画像セクションには、静止画像の圧縮を削除または変更できる設定が含まれています。

追加の色圧縮

この設定は、帯域幅が制限されているクライアント接続を介して配信される画像に対する追加の色圧縮の使用を有効または無効にします。これにより、表示される画像の品質を低下させることで応答性が向上します。

デフォルトでは、追加の色圧縮は無効になっています。

有効にすると、追加の色圧縮は、クライアント接続の帯域幅が「追加の色圧縮しきい値」を下回っている場合にのみ適用されます。クライアント接続の帯域幅がしきい値を超えている場合、または「無効」が選択されている場合、追加の色圧縮は適用されません。

追加の色圧縮しきい値

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、追加の色圧縮が適用される接続の最大帯域幅（キロビット/秒）を表します。クライアント接続の帯域幅が設定値を下回ると、有効になっている場合、追加の色圧縮が適用されます。

デフォルトでは、しきい値は8192キロビット/秒です。

ヘビーウェイト圧縮

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、より高度でCPU負荷の高いグラフィックアルゴリズムを使用することで、画質を損なうことなくプログレッシブ圧縮を超えて帯域幅を削減することを有効または無効にします。

デフォルトでは、ヘビーウェイト圧縮は無効になっています。

有効にすると、ヘビーウェイト圧縮はすべての非可逆圧縮設定に適用されます。Citrix Workspace™アプリでサポートされていますが、他のプラグインには影響しません。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮レベル
- プログレッシブ圧縮しきい値

非可逆圧縮レベル

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、帯域幅が制限されているクライアント接続を介して配信される画像に使用される非可逆圧縮の度合いを制御します。このような場合、圧縮なしで画像を表示すると遅くなることがあります。

デフォルトでは、中程度の圧縮が選択されています。

帯域幅を多く消費する画像の応答性を向上させるには、高圧縮を使用します。画質の劣化が許容されないX線画像を表示する場合など、画像データの保持が不可欠な場合は、非可逆圧縮を使用しない方がよいでしょう。

関連ポリシー設定：非可逆圧縮しきい値

非可逆圧縮しきい値

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、非可逆圧縮が適用される接続の最大帯域幅を1秒あたりのキロビット数で表します。

デフォルトでは、しきい値は1秒あたり2147483647キロビットです。

ポリシーに非可逆圧縮レベル設定を追加し、しきい値を指定しないことで、LAN経由での写真などの高精細ビットマップの表示速度を向上させることができます。

関連ポリシー設定：非可逆圧縮レベル

WebSocketsポリシー設定

WebSocketsセクションには、HTML5向けCitrix Workspace™アプリを使用して仮想デスクトップおよびホスト型アプリケーションにアクセスするためのポリシー設定が含まれています。WebSockets機能は、ブラウザーベースのアプリケーションとサーバー間の双方向通信を行うことで、セキュリティを向上させ、オーバーヘッドを削減します。この機能は、複数のHTTP接続を開くことなくこれを実現します。

WebSockets接続

この設定では、WebSockets接続を許可または禁止します。

デフォルトでは、WebSocket接続は禁止されています。

WebSocketsポート番号

この設定では、受信WebSocket接続のポートを識別します。

デフォルトでは、値は8008です。

WebSockets信頼済みオリジンサーバーリスト

この設定は、信頼されたオリジンサーバーのコンマ区切りのリストを提供します。これらは通常、Web向けCitrix Workspaceアプリであり、URLとして表現されます。サーバーは、これらのアドレスのいずれかから発信されたWebSockets接続のみを受け入れます。

既定では、ワイルドカード * は、すべてのCitrix WorkspaceアプリWeb URLを信頼するために使用されます。

リストにアドレスを入力する場合は、次の構文を使用します。

\<protocol>://\<ホストの完全修飾ドメイン名>:

プロトコルはHTTPまたはHTTPSである必要があります。ポートが指定されていない場合、HTTPにはポート80が、HTTPSにはポート443が使用されます。

ワイルドカード `*` は、IPアドレスの一部として使用する場合を除き (`10.105.*.*`)、URL内で使用できます。

レジストリで管理される HDX™ 機能

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

> レジストリエディターを開くには、サーバーで `regedit.exe` を実行します。次に、設定を追加または編集するためにレジストリキーに移動します。

デバイス

Bloomberg キーボード

Citrix Virtual Apps and Desktops™ は、Bloomberg モデル 4 およびモデル 3 のスターボードキーボードをサポートしています。デフォルトでは、拡張 Bloomberg キーボードのサポートは無効になっています。

Bloomberg キーボードのサポートを有効にするには、接続を開始する前に、クライアントマシンで以下のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB`
- **値の名前**: `EnableBloombergHID`
- **値の型**: `DWORD`
- **値のデータ**:
  - `0` - 無効
  - `1` - 有効

詳細については、Bloomberg キーボード を参照してください。

マップされたクライアントドライブ

セキュリティ上の予防措置として、ユーザーがCitrix Virtual Apps and Desktopsにログオンすると、デフォルトでサーバーはユーザーの実行権限なしでクライアントドライブをマップします。

マップされたクライアントドライブにある実行可能ファイルをユーザーが実行できるようにするには、サーバー上のレジストリを編集してこのデフォルト設定を上書きします。

アクセスを許可するには、以下のレジストリ値を編集します（**CDMSettings**が存在しない場合は作成します）。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\CDMSettings`
- **値の名前**: `ExecuteFromMappedDrive`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 権限を許可
  - `0` - マップされたドライブでの権限を拒否

この変更は、レジストリを編集した後に接続されたセッションに適用されます。

Citrix Virtual Apps and Desktops 7 2006は、このレジストリの場所を含む最初のバージョンです。以前のバージョンのCitrix Virtual Apps and Desktopsでは、異なるレジストリの場所が使用されていました。

詳しくは、「クライアントドライブマッピング」を参照してください。

マイクロソフト サーフェス プロ および サーフェス ブック のペン

Citrix Virtual Apps and Desktopsは、Windows Inkベースのアプリケーションで標準のペン機能をサポートしています。デフォルトでは、この機能は有効になっています。

この機能を無効または有効にするには、以下のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent\PenApi`
- **値の名前**: `DisablePen`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 無効にする
  - `0` - 有効にする

詳しくは、Microsoft Surface Pro and Surface Book pensを参照してください。

Windows Image Acquisitionアプリケーション許可リスト

この設定により、VDA上のどのアプリケーションがWindows Image Acquisitionスキャナーリダイレクトにアクセスできるかを制御できます。

デフォルトでは、どのアプリケーションもWindows Image Acquisitionにアクセスできません。

VDA上のアプリケーションのWindows Image Acquisitionを調整するには、次のレジストリ設定を作成します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`
- **値の名前**: `WIAAllowedProcesses`

  WIAAllowedProcessesを選択して右クリックします。「**新規 > 複数行文字列値**」を選択し、新しい値を「**AllowProcesses**」に名前変更します。
- 値のデータ: Windows Image Acquisitionにアクセスできる各アプリケーションの完全なパスとプロセス名を入力します。各アプリケーションは新しい行に入力してください。

この設定への変更は、次回 VDA でセッションを起動したときに有効になります。

全般

HDX リデューサー

セッションホストで使用するHDX圧縮アルゴリズム（Reducer）のバージョンを構成できます。

シングルセッションVDAでReducer V4を有効にするには、次のレジストリ値を設定します。

キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\WDSettings` **値の名前**: `ReducerOverrideMask` **値の型**: `DWORD` **値のデータ**: `23` (10進数)

マルチセッションVDAでReducer V4を有効にするには、次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **値の名前**: `ReducerOverrideMask`
- **値の型**: `DWORD`
- **値のデータ**: `23` (10進数)

EDTタイムアウトの構成

VDAでEDTタイムアウトを5秒から25秒の任意の値に構成できます。デフォルトのEDTタイムアウト値は25秒です。

- **キー**: `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\Tds\udp\UDPStackParameters`
- **値の型**: `DWORD`
- **値の名前**: `edtConnectionTimeout`
- **値のデータ**: 5〜25秒の時間 (10進数)

Windows向けCitrix Workspace™アプリのタイムアウトも構成できます:

- **キー**: `HKLM\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\EDT`
- **値の型**: `String / REG_SZ`
- **値の名前**: `edtConnectionTimeout`
- **値のデータ**: 5〜25秒の時間 (10進数)

Rendezvousバージョンの構成

使用するRendezvousのバージョンを構成するには、次のレジストリ値を設定します:

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`
- **値の型**: `DWORD`
- **値の名前**: `GctRegistration`
- **値のデータ**:
  - `1` - V2を有効にするには
  - `0` - V1を有効にするには

VDAへの自動ログオンを構成する

この設定により、Windows 10シングルセッションOSおよびマルチセッションOS VDAで、Microsoftポリシー設定「**常にパスワードの入力を求める**」を有効または無効にできます。

「**常にパスワードの入力を求める**」が有効になっている場合、ユーザーはリモートセッションを開始するときにVDAで資格情報を入力する必要があります。この設定が無効になっている場合、ユーザーはVDAで資格情報を入力することなく、自動的にリモートセッションに接続します。

デフォルトでは、Microsoftポリシー設定は無効になっています。「**常にパスワードの入力を求める**」設定を有効または無効にするには、VDAで以下のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Portica`
- **値の名前**: `AutoLogon`

- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - Microsoftポリシー設定を無効にし、ユーザーがリモートセッションに自動的にサインインできるようにします。
  - `0` – Microsoftポリシー設定を有効にし、ユーザーがリモートセッションを起動するときに資格情報の入力を求めます。

タイムアウト警告を無効にする

デフォルトでは、非アクティブまたはアイドル状態のセッションを持つユーザーは、セッションが自動的に切断される2分前に警告メッセージを受け取ります。

この設定は、以下の環境でアイドルセッションのタイムアウト制限に達したユーザーに対する警告メッセージを無効にし、削除します。

- ウィンドウズ サーバー 2004
- Windows 10マルチセッション2004以降のマルチセッションOS

警告を削除するには、VDA で次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\ICA-CGP`
- **値の名前**: `fEnableTimeoutWarning`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 警告メッセージを無効にする
  - `0` - 警告メッセージを有効にする

警告メッセージを表示するには、レジストリ値を削除するか、`0` に設定します。

EDT MTU検出

MTU検出により、EDTはセッション確立時に最大転送単位（MTU）を自動的に決定できます。これにより、パフォーマンスの低下やセッション確立の失敗につながる可能性のあるEDTパケットの断片化を防ぎます。

この設定はデフォルトで有効になっています。EDT MTU検出を無効にするには、次のレジストリ値を構成し、VDAを再起動します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **値の名前**: `MtuDiscovery`
- **値の型**: `DWORD`
- **値のデータ**: `0`

この設定はマシン全体に適用され、サポートされているクライアントから接続するすべてのセッションに影響します。

一般的なコンテンツリダイレクト

ホストからクライアントへのリダイレクトにURLタイプを追加する

デフォルトでは、HTTP、HTTPS、RTSP、RTSPU、PNM、MMSのURLタイプのリダイレクトをサポートしています。Windowsクライアントで以下のレジストリキーと値を作成することで、URLタイプをリストに追加できます。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA`
- **値の名前**: `ExtraURLProtocols`
- **値の型**: `REG_SZ`
- **値のデータ**: 必要なURLタイプをセミコロンで区切って指定します。URLの権限部分より前のすべてを含めます。例: `ftp://;mailto:;customtype1://;custometype2://`

URLタイプはWindowsクライアントにのみ追加できます。このレジストリ設定がないクライアントは、Citrixセッションへのリダイレクトを拒否します。クライアントには、指定されたURLタイプを処理するようにインストールおよび構成されたアプリケーションが必要です。

詳しくは、「ホストからクライアントへのリダイレクト」を参照してください。

クライアントフォルダーリダイレクト

クライアントフォルダーリダイレクトは、クライアント側のファイルがホスト側のセッションでアクセス可能になる方法を変更します。サーバーでクライアントフォルダーリダイレクトを有効にし、ユーザーがユーザーデバイスでそれを構成するとします。この場合、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

サーバーでクライアントフォルダーリダイレクトを有効にするには、次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection`

- **値の名前**: `CFROnlyModeAvailable`
- **値の型**: `DWORD`
- **値のデータ**: `1`

詳細については、クライアントフォルダーリダイレクトを参照してください。

特定のWebサイトセットのホストからクライアントへのリダイレクト

特定のWebサイトセットのホストからクライアントへのリダイレクトを有効にするには、サーバーVDAで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- **値の名前**: `ValidSites`
- **値の型**: `REG_MULTI_SZ`
- **値のデータ**: 任意の組み合わせの完全修飾ドメイン名（FQDN）を指定します。複数のFQDNは別々の行に入力します。プロトコル（`http://`または`https://`）なしでFQDNのみを含めます。FQDNには、最も左の位置にのみワイルドカード文字としてアスタリスク（`*`）を含めることができます。このワイルドカードは、RFC 6125の規則に準拠した単一レベルのドメインに一致します。例：

`www.example.com`

`*.example.com`

詳細については、ホストからクライアントへのリダイレクトを参照してください。

ログオフ時および切断時のローカルアプリケーションの動作

デフォルトでは、ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは実行を継続します。再接続後、ローカルアプリケーションが仮想デスクトップで利用可能な場合、それらは再統合されます。ログオフ時および切断時のローカルアプリケーションの動作を構成するには、ホストされたデスクトップで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies`
- **値の名前**: `Session State`
- **値の型**: `DWORD`
- **値のデータ**:

- `1` - ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは引き続き実行されます。再接続すると、ローカルアプリケーションが仮想デスクトップで利用可能な場合、再統合されます。
- `3` - ユーザーが仮想デスクトップからログオフまたは切断すると、ローカルアプリケーションは閉じます。

詳細については、「ローカルアプリアクセスとURLリダイレクト」を参照してください。

ホストからクライアントへのリダイレクトのデフォルトリストからURLタイプを削除する

デフォルトのリダイレクトリストからURLタイプを削除するには、サーバーVDAで以下のレジストリキーと値を作成します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- **値の名前**: `DisableServerFTA`
- **値の型**: `DWORD`
- **値のデータ**: `1`
- **値の名前**: `NoRedirectClasses`
- **値の型**: `REG_MULTI_SZ`
- **値のデータ**: `http`、`https`、`rtsp`、`rtspu`、`pnm`、または`mms`のいずれかの組み合わせを指定します。複数の値を別々の行に入力します。例:

`http`

`https`

`rtsp`

詳細については、ホストからクライアントへのリダイレクトを参照してください。

サーバーVDAのデフォルトブラウザ構成

ホストからクライアントへのリダイレクトを有効にすると、Server VDA のデフォルトのブラウザ設定を上書きできます。Web URL がリダイレクトされない場合、Citrix ランチャーは `command_backup` レジストリキーで構成されているブラウザに URL を渡します。このキーはデフォルトで Internet Explorer を指していますが、別のブラウザへのパスを含むように変更できます。

- Internet Explorer (デフォルト)
  - **キー**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`

  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"c:\program files\internet explorer\iexplore.exe" "%1"`
  - **キー**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"c:\program files\internet explorer\iexplore.exe" "%1"`

- グーグル クローム
  - **キー**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "%1"`
  - **キー**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "%1"`

- マイクロソフト エッジ
  - **キー**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "%1"`
  - **キー**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "%1"`

公開アプリケーションのローカルアプリアクセス

ローカルアプリアクセスは、ローカルにインストールされたWindowsアプリケーションを、デスクトップを切り替えることなくホストされたデスクトップ環境にシームレスに統合します。公開アプリケーションへのアクセスを提供するには、サーバーで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio`
- **値の名前**: `ClientHostedAppsEnabled`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 有効にする
  - `0` - 無効にする

詳細については、ローカルアプリアクセスとURLリダイレクトを参照してください。

グラフィック

CUDAまたはOpenCLアプリケーションのGPUアクセラレーション

ユーザーセッションで実行されているCUDAおよびOpenCLアプリケーションのGPUアクセラレーションは、デフォルトで無効になっています。

CUDAアクセラレーションのPOC機能を使用するには、次のレジストリ設定を有効にします。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- **値の名前**: `CUDA`
- **値の型**: `DWORD`
- **値のデータ**: `00000001`

OpenCLアクセラレーションのPOC機能を使用するには、次のレジストリ設定を有効にします。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- **値の名前**: `OpenCL`
- **値の型**: `DWORD`
- **値のデータ**: `00000001`

詳細については、WindowsマルチセッションOSのGPUアクセラレーションを参照してください。

プログレッシブモード

プログレッシブモードはデフォルトで無効になっています。次のレジストリ値でプログレッシブモードの状態を変更できます。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics`
- **値の型**: `REG_DWORD`
- **値の名前**: `ProgressiveDisplay`
- **値のデータ**:
  - `0` - 常にオフ (プログレッシブモードを無効にします。この値がデフォルトです。)
  - `1` - 自動 (ネットワークの状態に基づいて切り替えます。)
  - 2 = 常にオン

詳細については、プログレッシブモードを参照してください。

> **注:**
>
> プログレッシブモードは非推奨になりました。Thinwireは、プログレッシブモードのほぼすべての利点を提供しながら、画像配信を最適化し、キャッシュ効率を維持する代替オプションです。

Windows Presentation Foundation (WPF) レンダリング

HDX 3D Proを使用すると、Windows Multi-session OSセッションで実行されているグラフィックを多用するアプリケーションを、サーバーのグラフィック処理ユニット (GPU) でレンダリングできます。Windows Presentation Foundation (WPF) レンダリングをサーバーのGPUに移行することで、グラフィックレンダリングがサーバーのCPUを遅くすることはありません。

サーバーのGPUを使用してWPFアプリケーションのレンダリングを有効にするには、WindowsマルチセッションOSを実行しているサーバーのレジストリに次の設定を作成します。

1. VDAでレジストリエディターを開き、次のキーに移動します。

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper`

2. 次のレジストリ値を作成または編集します。

   - AdapterHandle = 0x00000001

- DevicePath = 0x00000001
- フラグ = 0x00000412
- WPF = 0x00000001

3. WPFアプリの実行可能ファイル名でサブキーを作成します。たとえば、アプリが「mywpfapp.exe」という名前の場合、次のキーを作成します。

```
HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper\mywpfapp.exe
```

4. 設定を有効にするには、サーバーを再起動します。

詳細については、WindowsマルチセッションOS向けGPUアクセラレーション およびブログ記事 WindowsマルチセッションOSでWPFアプリを最大限に活用する を参照してください。

マルチメディア

マルチメディア会議中のエコーを回避する

Citrix Virtual Apps and Desktopsには、エコーを最小限に抑えるエコーキャンセルオプションが用意されています。この機能はデフォルトで有効になっています。エコーキャンセルを無効にするには、次のいずれかのレジストリ設定を変更できます。

- **キー**:
  - 32ビット: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
  - 64ビット: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
- **値の名前**: `EchoCancellation`
- **値の型**: `String/REG_SZ`
- **値のデータ**: `False`

詳細については、「オーディオ機能」を参照してください。

オーディオの制限

クライアントにオーディオデバイスをインストールし、オーディオリダイレクトを有効にしてRDSセッションを開始した後、オーディオファイルが再生されない場合があります。回避策として、RDSマシンに次のレジストリキーを追加し、マシンを再起動してください。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig`
- **値の名前**: `EnableSvchostMitigationPolicy`

- **値の型**: `DWORD`
- **値のデータ**: `0`

詳細については、「オーディオ機能」を参照してください。

高解像度Webカメラの解像度

メディアタイプのネゴシエーションが失敗した場合、HDXはデフォルトのVGA解像度（640 x 480 ピクセル）にフォールバックします。クライアントのレジストリキーを使用して、デフォルトの解像度を構成できます。以下のレジストリキーを設定する前に、カメラが指定された解像度をサポートしていることを確認してください。

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- 幅
  - **値の名前**: `DefaultWidth`
  - **値の型**: `DWORD`
  - **値のデータ**: 目的の幅を10進数で (例: 1280)
- 高さ
  - **値の名前**: `DefaultHeight`
  - **値の型**: `DWORD`
  - **値のデータ**: 目的の高さを10進数で (例: 720)

Microsoft Teams フォールバックモード

Microsoft Teamsが最適化されたVDIモードでロードに失敗した場合 (Teams/バージョン情報/バージョンで「Citrix HDX未接続」と表示される場合)、VDAはウェブカメラのリダイレクトやクライアントのオーディオおよびマイクのリダイレクトなど、レガシーHDXテクノロジーにフォールバックします。Microsoft Teamsの最適化をサポートしないWorkspaceアプリのバージョン/プラットフォームOSを使用している場合、フォールバックレジストリキーは適用されません。

フォールバックメカニズムを制御するには、VDAで以下のいずれかのレジストリ値を設定します。

- **キー** (いずれか1つのみ必要):
  - **コンピューター設定:** `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams`
  - **ユーザー設定:** `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Teams`
- **値の名前**: `DisableFallback`

- **値の型**: `DWORD`
- 値のデータ:
  - `1` - フォールバックモードを無効にする
  - `2` - オーディオのみを有効にする

値が存在しないか0に設定されている場合、フォールバックモードが有効になります。この機能には、Microsoft Teamsバージョン1.3.0.13565以降が必要です。詳細については、「Microsoft Teamsの最適化」を参照してください。

Citrix App Layering™を使用したMicrosoft Teamsの最適化

Citrix App Layering を使用して VDA と Microsoft Teams のインストールを異なるレイヤーで管理している場合は、コマンドラインから `ALLUSER=1` フラグを使用して Microsoft Teams をインストールする前に、Windows 上に **PortICA** という名前の空のレジストリキーを作成します。既定の値の名前、種類、およびデータは変更しないでください。

- レジストリエディターの 32 ビット版のキー:
  `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA`
- レジストリエディターの 64 ビット版のキー:
  `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

詳細については、「Microsoft Teamsの最適化」を参照してください。

Web カメラのソフトウェア圧縮

Web カメラがハードウェアエンコーディングをサポートしている場合、HDX ビデオ圧縮は既定でハードウェアエンコーディングを使用します。ハードウェアエンコーディングは、ソフトウェアエンコーディングよりも多くの帯域幅を消費する可能性があります。ソフトウェア圧縮を強制するには、クライアントに次の値を追加します。

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HdxRealTime`
- **値の名前**: `DeepCompress_ForceSWEncode`
- **値の型**: `DWORD`
- **値のデータ**: `1`

詳細については、「HDX Web カメラのビデオ圧縮」を参照してください。

Web カメラのビデオ圧縮

HDX Webカメラビデオ圧縮は、H.264ビデオを仮想セッションで実行されているビデオ会議アプリケーションに直接送信します。VDAリソースを最適化するために、HDX Webカメラ圧縮はWebカメラビデオのエンコード、トランスコード、デコードを行いません。この機能はデフォルトで有効になっています。

サーバーからビデオ会議アプリへの直接ビデオストリーミングを無効にするには、VDAで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime`
- **値の名前**: `OfferH264ToApp`
- **値の型**: `DWORD`
- **値のデータ**: `0`

詳細については、HDX webcam video compressionを参照してください。

Webカメラビデオ圧縮フレームレート

優先ビデオフレームレートを調整するには、クライアントで次のレジストリ値を編集します。

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- **値の名前**: `FramesPerSecond`
- **値の型**: `DWORD`
- **値のデータ**: `15`

ウェブカメラが指定されたフレームレートをサポートしていない場合、アプリケーションはデフォルトで15 FPSを使用します。

詳細については、HDXウェブカメラビデオ圧縮を参照してください。

負荷管理ポリシー設定

「**負荷管理**」セクションには、WindowsマルチセッションOSマシンを提供するサーバー間の負荷管理を有効化および構成するためのポリシー設定が含まれています。

負荷評価インデックスの計算については、CTX202150を参照してください。

同時ログオン許容数

この設定は、サーバーが受け入れ可能な同時ログオンの最大数を指定します。

デフォルトでは、この値は2に設定されています。

この設定が有効な場合、負荷分散は、指定された数を超えるログオンが同時にServer VDAでアクティブにならないように試みます。ただし、この制限は厳密には適用されません。制限を適用し（指定された数を超える同時ログオンを失敗させるには）、次のレジストリキーを作成します。

> HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit 種類: DWORD 値: 1

CPU使用率

この設定は、サーバーがフルロードを報告するCPU使用率のレベルをパーセンテージで指定します。有効にすると、サーバーがフルロードを報告するデフォルト値は90%です。

デフォルトでは、この設定は無効になっており、CPU使用率は負荷計算から除外されます。

CPU使用率から除外されるプロセスの優先度

> **注：**
>
> Workspace Environment Managementがマシンを管理するシナリオでは、この設定をCPU優先度設定と併用すると、意図しない結果が生じる可能性があります。CPU優先度設定を使用する場合は、この設定を無効にすることをお勧めします。

> この設定は、プロセスのCPU使用率がCPU使用率負荷インデックスから除外される優先度レベルを指定します。

デフォルトでは、この値は**標準以下**または**低**に設定されています。

ディスク使用量

この設定は、サーバーが75%のフルロードを報告するディスクキューの長さを指定します。有効にすると、ディスクキューの長さのデフォルト値は8です。

デフォルトでは、この設定は無効になっており、ディスク使用率は負荷計算から除外されます。

セッションの最大数

この設定は、サーバーがホストできる最大セッション数を指定します。有効にすると、サーバーがホストできる最大セッション数のデフォルト設定は250です。

デフォルトでは、この設定は有効になっています。

メモリ使用量

この設定は、サーバーがフルロードを報告するメモリ使用量のレベルをパーセンテージで指定します。有効にすると、サーバーがフルロードを報告するデフォルト値は90%です。

デフォルトでは、この設定は無効になっており、メモリ使用量は負荷計算から除外されます。

メモリ使用量のベースロード

この設定は、ベースオペレーティングシステムのメモリ使用量の近似値を指定します。また、サーバーがゼロロードと見なされるメモリ使用量をMB単位で定義します。

デフォルトでは、この値は768 MBに設定されています。

プロファイル管理ポリシー設定

このセクションには、プロファイル管理を有効化および構成するためのポリシー設定が含まれています。

以下のその他の情報については、「プロファイル管理ポリシー」を参照してください。

- 対応する.iniファイル設定の名前
- ポリシー設定に必要なプロファイル管理のバージョン

高度なポリシー設定

ロックされたファイルへのアクセス時の再試行回数

ロックされたファイルへのアクセス時の再試行回数を設定します。

このポリシーが無効になっている場合、デフォルト値の5回の再試行が使用されます。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、デフォルト値が使用されます。

ログオフ時にインターネットCookieファイルを処理する

一部の展開では、`Index.dat`が参照しない余分なインターネットCookieが残されます。継続的なブラウジングの後、ファイルシステムに残された余分なCookieは、プロファイルの肥大化につながる可能性があります。このポリシーを使用すると、Profile Managementを有効にして、Index.datの処理を強制し、余分なCookieを削除できます。このポリシーはログオフ時間を増加させるため、この問題が発生した場合にのみ有効にしてください。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。

2. ここで、または.iniファイルでこのポリシーが構成されていない場合、Index.datの処理は行われません。

自動構成を無効にする

Profile Managementは、Citrix Virtual Desktops™環境（パーソナルvDiskの有無など）を検査し、それに応じてグループポリシーを構成します。「未構成」状態のProfile Managementポリシーのみが調整されるため、行ったカスタマイズはすべて保持されます。

このポリシーにより、展開を高速化し、最適化を簡素化できます。このポリシーを構成する必要はありません。ただし、次のいずれかの操作を行う場合は、自動構成を無効にできます。

- 以前のバージョンからの設定を保持するためのアップグレード
- トラブルシューティング

自動構成は、実行時に環境に応じてデフォルトのポリシー設定を自動的に構成する動的な構成チェッカーと見なすことができます。これにより、設定を手動で構成する必要がなくなります。実行時環境には以下が含まれます。

- Windows オペレーティングシステム
- Windows OS のバージョン
- シトリックス バーチャル デスクトップの有無
- パーソナルvDisk の有無

環境が変更された場合、自動構成によって以下のポリシーが変更される可能性があります。

- アクティブライトバック
- 常にキャッシュ
- ログオフ時にローカルにキャッシュされたプロファイルを削除
- キャッシュされたプロファイルを削除するまでの遅延
- プロファイルストリーミング

異なる OS でのポリシーのデフォルトの状態については、次の表を参照してください。

	マルチセッションOS	シングルセッションOS
アクティブライトバック	有効	Personal vDisk が使用されている場合は *無効*。それ以外の場合は有効。

	マルチセッションOS	シングルセッションOS
常にキャッシュ	無効	Personal vDisk が使用されている場合は *無効*。それ以外の場合は有効。
ログオフ時にローカルにキャッシュされたプロファイルを削除	有効	以下のいずれかの状況が発生した場合: Personal vDisk が使用されている場合、Citrix Virtual Desktops が割り当てられている場合、または Citrix Virtual Desktops がインストールされていない場合、*無効*になります。それ以外の場合は有効です。
キャッシュされたプロファイルを削除するまでの遅延	0 秒	ユーザーの変更が永続的でない場合は 60 秒。それ以外の場合は 0 秒。
プロファイルストリーミング	有効	Personal vDisk が使用されている場合は *無効*。それ以外の場合は有効。

ただし、自動構成が無効になっている場合、上記のすべてのポリシーはデフォルトで **無効** になります。

> **重要:**

> Personal vDisk は非推奨です。詳細については、「PVD、AppDisks、およびサポートされていないホストの削除」(/ja-jp/citrix-virtual-apps-desktops/2411/upgrade-migrate/upgrade.html#remove-pvd-appdisks-and-unsupported-hosts)を参照してください。

> Profile Management 1909以降、Windows 10 (バージョン1607以降) のスタートメニューで改善されたエクスペリエンスを得ることができます。この改善は、以下のポリシーの自動構成によって実現されます。

- **ミラーリングするフォルダー**に `Appdata\Local\Microsoft\Windows\Caches` と `Appdata\Local\Packages` を追加します。

- **同期するファイル**に`Appdata\Local\Microsoft\Windows\UsrClass.Dat*`を追加します。

構成の優先順位:

1. この設定がここで構成されていない場合、.iniファイルの値が使用されます。
2. この設定がここまたは.iniファイルで構成されていない場合、自動構成が有効になります。この場合、環境が変更されるとProfile Managementの設定も変更される可能性があります。

問題が発生した場合にユーザーをログオフする

問題が発生した場合にProfile Managementがユーザーをログオフするかどうかを指定できます。

このポリシーが無効になっているか、構成されていない場合、問題が発生するとProfile Managementはユーザーに一時プロファイルを提供します。たとえば、ユーザーストアが利用できない場合などです。

有効になっている場合、エラーメッセージが表示され、ユーザーはログオフされます。この設定により、問題のトラブルシューティングが簡素化されます。

構成の優先順位:

1. この設定がここで構成されていない場合、.iniファイルの値が使用されます。
2. この設定がここまたは.iniファイルで構成されていない場合、一時プロファイルが提供されます。

カスタマー エクスペリエンス向上プログラム

デフォルトでは、カスタマー エクスペリエンス向上プログラムが有効になっており、匿名統計と使用状況データを収集することで、Citrix® 製品の品質とパフォーマンスの向上に役立てています。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

Outlook の検索インデックス ローミングを有効にする

ユーザープロファイルとともに Outlook 検索データを自動的にローミングすることで、ユーザーベースの Outlook 検索エクスペリエンスを許可します。この機能には、Outlook の検索インデックスを保存するために、ユーザー ストアに追加のスペースが必要です。

このポリシーを有効にするには、ログオフしてから再度ログオンしてください。

Outlook 検索インデックス データベース – バックアップと復元

Outlook の検索インデックス ローミングを有効にするポリシーが有効になっている場合に、ログオン中に Profile Management が何を行うかを指定できます。

このポリシーが有効になっている場合、Profile Managementは、ログオン時にデータベースが正常にマウントされるたびに検索インデックスデータベースをバックアップします。Profile Managementは、そのバックアップを検索インデックスデータベースの正常なコピーとして扱います。データベースの破損により検索インデックスデータベースのマウントが失敗した場合、Profile Managementは検索インデックスデータベースを最後に認識された正常なコピーに戻します。

> 注:
>
> 新しいバックアップが正常に保存されると、Profile Managementは以前に保存されたバックアップを削除します。バックアップは利用可能なVHDXストレージを消費します。

OUTLOOK検索データローミングの同時セッションサポートを有効にする

Profile Managementにより、同じユーザーの同時セッションでネイティブのOutlook検索エクスペリエンスが提供されます。このポリシーは、Outlookの検索インデックスローミングポリシーと併用してください。

このポリシーが有効な場合、各同時セッションは個別のOutlook OSTファイルを使用します。

デフォルトでは、Outlook OSTファイルを保存するために使用できるVHDXディスクは2つだけです（ディスクごとに1ファイル）。ユーザーがさらにセッションを開始すると、そのOutlook OSTファイルはローカルユーザープロファイルに保存されます。Outlook OSTファイルを保存するためのVHDXディスクの最大数を指定できます。

ONEDRIVE コンテナを有効にする

OneDriveフォルダーをユーザーとともにローミングできるようにします。

OneDriveコンテナは、VHDXベースのフォルダーローミングソリューションです。Profile Managementは、ファイル共有上にユーザーごとにVHDXファイルを作成し、ユーザーのOneDriveフォルダーをVHDXファイルに保存します。VHDXファイルは、ユーザーがログオンするときにアタッチされ、ログオフするときにデタッチされます。

UWPアプリのローミング

UWP (Universal Windows Platform) アプリをユーザーとともにローミングできるようにします。その結果、ユーザーは異なるデバイスから同じUWPアプリにアクセスできます。

このポリシーを有効にすると、Profile ManagementはUWPアプリを個別のVHDXディスクに保存することで、ユーザーと共にローミングできるようにします。これらのディスクは、ユーザーのログオン中にアタッチされ、ログオフ中にデタッチされます。

構成の優先順位:

1. この設定がここで構成されていない場合、.iniファイルの値が使用されます。
2. この設定がここでも.iniファイルでも構成されていない場合、この機能は無効になります。

UWPアプリの読み込み高速化を有効にする

UWPアプリの読み込み高速化を有効にします。これにより、UWPアプリの読み込みを高速化し、非永続環境での一貫性を向上させることができます。デフォルトでは、WindowsはUWPアプリの登録情報を各マシンにローカルに保存しますが、非永続環境では再起動時に失われる可能性があります。このポリシーを有効にすると、Profile Managementは各マシン用にVHDXコンテナを作成してUWPアプリの登録データを保存し、ユーザーログオンを高速化し、再起動時のデータ損失を防ぎます。

構成の優先順位:

1. この設定がGPO、Studio、またはWorkspace Experience Management (WEM) を使用して構成されていない場合、.iniファイルの値が使用されます。
2. この設定がどこにも構成されていない場合、この機能は無効になります。

ログオン時のユーザーグループポリシーの非同期処理を有効にする

Windowsは、ユーザーグループポリシーに同期モードと非同期モードの2つの処理モードを提供します。Windowsは、次のユーザーログオンの処理モードを決定するためにレジストリ値を使用します。レジストリ値が存在しない場合、同期モードが適用されます。レジストリ値はマシンレベルの設定であり、ユーザーとともにローミングされません。したがって、ユーザーが次の場合、非同期モードは期待どおりに適用されません。

- 異なるマシンにログオンします。
- ログオフ時にローカルにキャッシュされたプロファイルを削除するポリシーが有効になっている同じマシンにログオンします。

このポリシーを有効にすると、レジストリ値はユーザーとともにローミングされます。その結果、ユーザーがログオンするたびに処理モードが適用されます。

VHDディスクの圧縮をトリガーする空き領域の比率

VHDディスクの圧縮を有効にする が有効な場合に適用されます。VHDディスクの圧縮をトリガーする空き領域の比率を指定できます。ユーザーがログオフするときに空き領域の比率が指定された値を超えると、ディスクの圧縮がトリガーされます。

空き領域の比率 = (現在のVHDファイルサイズ – 必要な最小VHDファイルサイズ*) ÷ 現在のVHDファイルサイズ

* Microsoft Windowsオペレーティングシステムの`MSFT_Partition`クラスのGetSupportedSizeメソッドを使用して取得されます。

VHDディスクの圧縮をトリガーするログオフ回数

VHDディスクの圧縮を有効にする が有効な場合に適用されます。VHDディスクの圧縮をトリガーするユーザーログオフ回数を指定できます。

最後の圧縮以降のログオフ回数が指定された値に達すると、ディスク圧縮が再度トリガーされます。

VHDディスクの圧縮におけるデフラグを無効にする

VHDディスクの圧縮を有効にする が有効な場合に適用されます。VHDディスクの圧縮におけるファイルのデフラグを無効にするかどうかを指定できます。

VHDディスク圧縮が有効な場合、VHDディスクファイルはまずWindowsに組み込まれている`defrag`ツールを使用して自動的にデフラグされ、その後圧縮されます。VHDディスクのデフラグはより良い圧縮結果をもたらしますが、無効にするとシステムリソースを節約できます。

プロファイルコンテナのマルチセッションライトバックを有効にする

マルチセッションシナリオでプロファイルコンテナのライトバックを有効にします。有効にすると、すべてのセッションでの変更がプロファイルコンテナに書き戻されます。そうでない場合、プロファイルコンテナでは最初のセッションのみが読み取り/書き込みモードであるため、最初のセッションでの変更のみが保存されます。Citrix Profile Managementプロファイルコンテナは Citrix Profile Management 2103以降でサポートされています。FSLogix Profile ContainerはCitrix Profile Management 2003以降でサポートされています。

FSLogix Profile Containerでこのポリシーを使用するには、以下の前提条件が満たされていることを確認してください。

- FSLogix Profile Container機能がインストールされ、有効になっていること。
- FSLogixでプロファイルタイプが**読み書きプロファイルを試行し、読み取り専用にフォールバックする**に設定されていること。

ユーザーストアのレプリケート

ログオンおよびログオフのたびに、リモートユーザープロファイルストアを複数のパスにレプリケートできます。これにより、Profile Managementはユーザーログオンのプロファイル冗長性を提供します。

このポリシーを有効にすると、システムI/Oが増加し、ログオフ時間が長くなる可能性があります。

注:

この機能は、ファイルベースとコンテナベースの両方のプロファイルソリューションで利用できます。

ユーザーストアへの資格情報ベースのアクセスを有効にする

デフォルトでは、Citrix Profile Managementは現在のユーザーを偽装してユーザーストアにアクセスします。Profile Managementがユーザーストアにアクセスする際に現在のユーザーを偽装しないようにしたい場合は、この機能を有効にしてください。現在のユーザーがアクセス権を持たないストレージリポジトリ（例：Azure Files）にユーザーストアを配置できます。

To ensure that Profile Management can access user stores, save the profile storage server's credentials in Workspace Environment Management™ (WEM) or Windows Credential Manager. We recommend you use Workspace Environment Management to eliminate the need of configuring the same credentials for each machine where Profile Management runs. If you use the Windows Credential Manager, use the Local System account to securely save the credentials.

注:

このポリシーは、ファイルベースとVHDXベースの両方のユーザーストアで利用できます。Profile Managementバージョン2212より前のバージョンでは、このポリシーはVHDXベースのユーザーストアでのみ利用できます。

構成の優先順位：

1. ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。
2. ここで、または .ini ファイルでこの設定が構成されていない場合、デフォルトで無効になります。

VHDX ファイルのストレージ パスをカスタマイズする

Profile Managementは、以下のVHDXベースのポリシーを提供します: プロファイルコンテナ、Outlookの検索インデックスローミング、およびフォルダミラーリングの高速化。デフォルトでは、VHDXファイルはユーザーストアに保存されます。このポリシーを使用すると、それらを保存するための別のパスを指定できます。

VHD コンテナーのデフォルト容量

VHDコンテナのデフォルトストレージ容量（GB単位）を指定できます。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。
2. ここで、または .ini ファイルでこのポリシーが構成されていない場合、デフォルトは 50 (GB) です。

セッションで VHDX ディスクを自動的に再アタッチする

このポリシーを有効にすると、Profile Management は VHDX ベースのポリシーの高い安定性を確保します。デフォルトでは、このポリシーは有効になっています。

このポリシーが有効になっている場合、Profile Management は VHDX ベースのポリシーで使用されている VHDX ディスクを監視します。いずれかのディスクがデタッチされた場合、Profile Management はそのディスクを自動的に再アタッチします。

プロファイルコンテナの自動拡張しきい値

プロファイルコンテナが自動拡張をトリガーするストレージ容量の使用率を指定できます。

構成の優先順位:

- このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここまたは.iniファイルで構成されていない場合、デフォルトはストレージ容量の90%です。

プロファイルコンテナの自動拡張増分

自動拡張がトリガーされたときに、プロファイルコンテナが自動的に拡張するストレージ容量（GB単位）を指定できます。

構成の優先順位:

- このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここで、または.iniファイルで構成されていない場合、デフォルトは10 (GB) です。

プロファイルコンテナの自動拡張制限

自動拡張がトリガーされたときに、プロファイルコンテナが自動的に拡張できる最大ストレージ容量（GB単位）を指定できます。

構成の優先順位:

- このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここで、または.iniファイルで構成されていない場合、デフォルトは80 (GB) です。

ユーザーレベルのポリシー設定を有効にする

このポリシーを有効にすると、マシンレベルのポリシー設定がユーザーレベルで機能し、ユーザーレベルの設定がマシンレベルの設定を上書きします。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
2. ここででも.iniファイルでもこのポリシーが構成されていない場合、無効になります。

ユーザーグループの優先順位を設定する

ユーザーグループの優先順位を指定できます。この順序は、ユーザーが異なるポリシー設定を持つ複数のグループに属している場合に、どのグループが優先されるかを決定します。

ユーザーが競合するポリシー設定を持つ複数のグループに属している場合、以下を考慮してください:

- ユーザーがこのポリシーで定義されている1つ以上のグループに属している場合、最も優先順位の高いグループが優先されます。
- ユーザーがこのポリシーで定義されているどのグループにも属していない場合、アルファベット順で最初にリストされているSIDを持つグループが優先されます。

ユーザーストアの選択方法

複数のユーザーストアが利用可能な場合に、ユーザーストアの選択方法を指定できます。オプションは次のとおりです:

- **構成順序。** Profile Managementは、最初に構成されたストアを選択します。
- **アクセスパフォーマンス。** Profile Managementは、最高のアクセスパフォーマンスを持つストアを選択します。

構成の優先順位:

1. ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。
2. ここでも .ini ファイルでもこの設定が構成されていない場合、**構成順序**が使用されます。

ユーザーストア間でのセッション内プロファイルコンテナフェールオーバーを有効にする

デフォルトでは、複数のユーザーストアが展開されている場合、プロファイルコンテナのフェールオーバーはユーザーログオン時にのみ発生します。その結果、プロファイルの冗長性はユーザーログオン時にのみ利用可能です。このポリシーにより、フェールオーバーの範囲をセッション全体に拡大し、セッション全体でプロファイルの冗長性を確保できます。このポリシーが有効になっている場合、Profile Managementがセッション中にアクティブなプロファイルコンテナへの接続を失うと、自動的に別の利用可能なコンテナに切り替わります。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、設定は無効になります。

プロファイルサイズがクォータを超過した場合にユーザーに通知する

ユーザープロファイルにクォータを設定し、プロファイルサイズがそれを超えたときにユーザーに通知できます。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、設定は無効になります。

プロファイルサイズがクォータを超過した場合の通知メッセージ

プロファイルサイズがクォータを超過した場合にユーザーに通知するポリシーが有効な場合に適用されます。ユーザーが受け取る通知メッセージを設定できます。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、設定は無効になります。

基本的なポリシー設定

このセクションには、Profile Management の基本的な構成に関連するポリシー設定が含まれています。

Profile Management を有効にする

既定では、展開を容易にするため、Profile Management はログオンまたはログオフを処理しません。Profile Management は、他のすべてのセットアップタスクを実行し、Citrix® ユーザープロファイルが環境でどのように動作するかをテストした後にのみ有効にしてください。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、Profile Management は Windows ユーザープロファイルを一切処理しません。

処理されるグループ

コンピューターローカルグループとドメイングループ（ローカル、グローバル、ユニバーサル）の両方を使用できます。ドメイングループは「DOMAIN NAME\GROUP NAME」の形式で指定する必要があります。

このポリシーがここで構成されている場合、Profile Management はこれらのユーザーグループのメンバーのみを処理します。このポリシーが無効になっている場合、Profile Management はすべてのユーザーを処理します。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、すべてのユーザーグループのメンバーが処理されます。

除外されるグループ

コンピューターローカルグループとドメイングループ（ローカル、グローバル、ユニバーサル）を使用して、特定のユーザープロファイルが処理されないようにすることができます。ドメイングループは「DOMAIN NAME\ GROUP NAME」の形式で指定します。

この設定がここで構成されている場合、Profile Management はこれらのユーザーグループのメンバーを除外します。この設定が無効になっている場合、Profile Management はどのユーザーも除外しません。この設定がここで構成されていない場合、.ini ファイルの値が使用されます。この設定がここでも .ini ファイルでも構成されていない場合、どのグループのメンバーも除外されません。

ローカル管理者によるログオンを処理する

BUILTIN\Administrators グループのメンバーによるログオンを処理するかどうかを指定します。Citrix Virtual Apps 環境などのマルチセッションオペレーティングシステムでは、このポリシーが無効になっているか、構成されていないと見なされます。この場合、Profile Management は、ローカル管理者ではなくドメインユーザーによるログオンが処理される必要があると想定します。シングルセッションオペレーティングシステム（Citrix Virtual Desktops 環境など）では、ローカル管理者によるログオンが処理されます。このポリシーにより、ローカル管理者権限を持つドメインユーザー（通常は割り当てられた仮想デスクトップを持つ Citrix Virtual Desktops ユーザー）は、次のことが可能になります。

- 処理をバイパスする
- ログオンする
- Profile Managementでデスクトップの問題をトラブルシューティングする

注：ドメインユーザーのログオンは、通常、製品ライセンスへの準拠を確実にするために、グループメンバーシップによって課される制限の対象となる場合があります。 このポリシーが無効になっている場合、Profile Managementはローカル管理者によるログオンを処理しません。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、管理者は処理されません。

ユーザーストアへのパス

ユーザー設定（レジストリの変更と同期されたファイル）が保存されるディレクトリ（ユーザーストア）へのパスを設定します。

パスは次のいずれかです。

- 相対パス。ホームディレクトリ（通常、Active Directoryのユーザーの#homeDirectory#属性として構成されます）に対する相対パスである必要があります。
- UNCパス。通常、サーバー共有またはDFS名前空間を指定します。
- 無効または未構成。この場合、#homeDirectory#\Windowsの値が想定されます。

このポリシーでは、次の種類の変数を使用できます。

- パーセント記号で囲まれたシステム環境変数（例：%ProfVer%）。システム環境変数は通常、追加のセットアップが必要です。
- ハッシュで囲まれたActive Directoryユーザーオブジェクトの属性（例：#sAMAccountName#）。
- Profile Management変数。詳しくは、Profile Management変数の製品ドキュメントを参照してください。

`%username%`と`%userdomain%`を除き、ユーザー環境変数は使用できません。場所やユーザーなどを完全に定義するために、カスタム属性を作成することもできます。属性は大文字と小文字を区別します。

例:

- \\server\share#sAMAccountName# は、ユーザー設定をUNCパス \\server\share\JohnSmith に保存します（現在のユーザーに対して #sAMAccountName# が JohnSmith に解決される場合）。
- \\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS! は \\server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64 に展開される場合があります

重要: どの属性または変数を使用する場合でも、このポリシーが NTUSER.DAT を含むフォルダーの 1 レベル上のフォルダーに展開されることを確認してください。たとえば、このファイルが \\server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile に含まれている場合、ユーザー ストアへのパスは \\server\profiles$\JohnSmith.Finance\Win8x64 に設定します (\UPM_Profile サブフォルダーではありません)。

ユーザー ストアへのパスを指定する際に変数を使用する方法について詳しくは、次のトピックを参照してください。

- 複数のファイルサーバーで Citrix ユーザープロファイルを共有する
- OU 内および OU 間でプロファイルを管理する
- Profile Management を使用した高可用性と災害復旧

「ユーザー ストアへのパス」が無効になっている場合、ユーザー設定はホームディレクトリの Windows サブディレクトリに保存されます。

このポリシーが無効になっている場合、ユーザー設定はホームディレクトリの Windows サブディレクトリに保存されます。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ホームドライブの Windows ディレクトリが使用されます。

ユーザーストアの移行

ユーザー設定（レジストリの変更と同期されたファイル）が以前に保存されていたフォルダーへのパス（以前使用していたユーザーストアパス）を指定します。

この設定が構成されている場合、以前のユーザー ストアに保存されているユーザー設定は、「ユーザー ストアへのパス」ポリシーで指定された現在のユーザー ストアに移行されます。

パスは、絶対 UNC パスまたはホームディレクトリに対する相対パスのいずれかです。

どちらの場合でも、以下の種類の変数を使用できます。

- パーセント記号で囲まれたシステム環境変数
- ハッシュ記号で囲まれた Active Directory ユーザーオブジェクトの属性

例:

- `Windows\%ProfileVer%` フォルダーは、ユーザー設定をユーザー ストアの `Windows\W2K3` というサブフォルダーに保存します（%ProfileVer% が W2K3 に解決されるシステム環境変数である場合）。

- `\\server\share#SAMAccountName#` は、ユーザー設定を UNC パス `\\server\share\<JohnSmith>` に保存します（`#SAMAccountName#` が現在のユーザーに対して JohnSmith に解決される場合）。

パスでは、`%username%` および `%userdomain%` を除くユーザー環境変数を使用できます。

この設定が無効になっている場合、ユーザー設定は現在のユーザーストアに保存されます。

ここでこの設定が構成されていない場合、.ini ファイルの対応する設定が使用されます。

ここで、または .ini ファイルでこの設定が構成されていない場合、ユーザー設定は現在のユーザーストアに保存されます。

アクティブライトバック

変更されたファイルとフォルダー（レジストリ エントリは除く）は、セッション中に、ログオフ前にユーザー ストアに同期できます。

ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。ここで、または .ini ファイルでこのポリシーが構成されていない場合、このポリシーは有効になります。

オフラインプロファイルのサポート

このポリシーにより、プロファイルは可能な限り早い機会にユーザー ストアと同期できます。これは、ローミングするラップトップまたはモバイルデバイスのユーザーを対象としています。ネットワーク接続が切断された場合でも、再起動または休止状態の後でも、プロファイルはラップトップまたはデバイス上でそのまま維持されます。モバイルユーザーが作業すると、プロファイルはローカルで更新されます。また、ネットワーク接続が再確立されると、最終的にユーザー ストアと同期されます。

ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。ここで、または .ini ファイルでこのポリシーが構成されていない場合、オフラインプロファイルは無効になります。

アクティブライトバックレジストリ

このポリシーは、「アクティブライトバック」と併用してください。変更されたレジストリ エントリは、セッション中にユーザー ストアに同期できます。

ここでこの設定を構成しない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定を構成しない場合、アクティブライトバックレジストリは無効になります。

セッションロックおよび切断時のアクティブライトバック

このポリシーと**アクティブライトバック**ポリシーの両方が有効になっている場合、プロファイルファイルとフォルダーは、セッションがロックまたは切断されたときにのみ書き戻されます。

このポリシーと**アクティブライトバック**および**アクティブライトバックレジストリ**ポリシーの両方が有効になっている場合、レジストリエントリは、セッションがロックまたは切断されたときにのみ書き戻されます。

オフラインプロファイルのサポート

オフラインプロファイル機能を有効にします。この機能は、ネットワークから頻繁に切断されるコンピューター向けです。たとえば、サーバーやデスクトップではなく、ラップトップやモバイルデバイスなどです。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定が構成されていない場合、オフラインプロファイルのサポートは無効になります。

クロスプラットフォームポリシー設定

このセクションには、**Profile Management cross-platform** 設定機能の構成に関連するポリシー設定が含まれています。

クロスプラットフォーム設定を有効にする

デフォルトでは、展開を容易にするため、クロスプラットフォーム設定は無効になっています。この機能を十分に計画しテストした後にのみ、このポリシーを有効にして処理をオンにしてください。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、クロスプラットフォーム設定は適用されません。

クロスプラットフォーム設定ユーザーグループ

1つ以上のWindowsユーザーグループを入力します。たとえば、このポリシーを使用して、テストユーザーグループのプロファイルのみを処理することができます。このポリシーが構成されている場合、Profile Managementのクロスプラットフォーム設定機能は、これらのユーザーグループのメンバーのみを処理します。このポリシーが無効になっている場合、この機能は「処理済みグループ」ポリシーで指定されたすべてのユーザーを処理します。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、すべてのユーザーグループが処理されます。

クロスプラットフォーム定義へのパス

ダウンロードパッケージからコピーした定義ファイルのネットワーク上の場所を識別します。このパスはUNCパスである必要があります。ユーザーはこの場所への読み取りアクセス権を持ち、管理者は書き込みアクセス権を持つ必要があります。この場所は、Server Message Block (SMB) または Common Internet File System (CIFS) ファイル共有である必要があります。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、クロスプラットフォーム設定は適用されません。

クロスプラットフォーム設定ストアへのパス

ユーザーのクロスプラットフォーム設定が保存されるフォルダーである、クロスプラットフォーム設定ストアへのパスを設定します。ユーザーはこの領域への書き込みアクセス権を持つ必要があります。パスは絶対UNCパスまたはホームディレクトリに対する相対パスにすることができます。

この領域は、複数のプラットフォームで共有されるプロファイルデータが配置されるユーザーストアの共通領域です。ユーザーはこの領域への書き込みアクセス権を持つ必要があります。パスは絶対UNCパスまたはホームディレクトリに対する相対パスにすることができます。**ユーザーストアへのパス**と同じ変数を使用できます。

このポリシーが無効になっている場合、パス Windows\PM_CP が使用されます。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、デフォルト値が使用されます。

クロスプラットフォーム設定を作成するためのソース

このポリシーがそのプラットフォームのOUで有効になっている場合、プラットフォームをベースプラットフォームとして指定します。このポリシーは、ベースプラットフォームのプロファイルからクロスプラットフォーム設定ストアにデータを移行します。

各プラットフォーム独自のプロファイルセットは、別々のOUに保存されます。クロスプラットフォーム設定ストアをシードするために、どのプラットフォームのプロファイルデータを使用するかを決定する必要があります。これはベースプラットフォームと呼ばれます。クロスプラットフォーム設定ストアにデータのない定義ファイルが含まれている場合、または単一プラットフォームプロファイルのキャッシュデータがストア内の定義データよりも新しい場合を考えてみ

ましょう。この場合、このポリシーを無効にしない限り、Profile Managementは単一プラットフォームプロファイルからストアにデータを移行します。

> **重要:**
>
> このポリシーが複数のOU、または複数のユーザーオブジェクトやマシンオブジェクトで有効になっている場合、最初にユーザーがログオンしたプラットフォームがベースプロファイルになります。 デフォルトでは、このポリシーは有効になっています。

ファイルシステム ポリシー設定

このセクションには、以下の設定を行うポリシーが含まれています。

- ユーザープロファイル内のどのファイルが、プロファイルがインストールされているシステムとユーザー ストアの間で同期されるか
- ユーザープロファイル内のどのディレクトリが、プロファイルがインストールされているシステムとユーザー ストアの間で同期されるか

除外ポリシー設定

このセクションでは、ユーザープロファイル内のどのファイルとディレクトリを同期プロセスから除外するかを設定するためのポリシー設定について説明します。

除外リスト - ファイル

同期中に無視されるファイルのリスト。ファイル名はユーザープロファイル (%USERPROFILE%) に対する相対パスである必要があります。ワイルドカードはファイル名とフォルダー名でサポートされていますが、ファイル名のワイルドカードのみが再帰的に適用されます。

例:

- `Desktop\Desktop.ini` は、`Desktop` フォルダー内のファイル `Desktop.ini` を無視します。
- `%USERPROFILE%*.tmp` は、プロファイル全体で拡張子 `.tmp` を持つすべてのファイルを無視します。
- `AppData\Roaming\MyApp*.tmp` は、プロファイルの一部で拡張子 `.tmp` を持つすべてのファイルを無視します。
- `Downloads*\a.txt` は、`Downloads` フォルダーの直下のサブフォルダーにある `a.txt` を無視します。

このポリシーが無効になっている場合、ファイルは除外されません。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここで、または .ini ファイルで構成されていない場合、ファイルは除外されません。

デフォルトの除外リストを有効にする - ディレクトリ

同期中に無視されるディレクトリのデフォルトリスト。このポリシーを使用して、手動で入力することなく GPO 除外ディレクトリを指定します。

このポリシーを無効にすると、Profile Management はデフォルトでどのディレクトリも除外しません。

このポリシーをここで構成しない場合、Profile Management は .ini ファイルの値を使用します。このポリシーをここで、または .ini ファイルで構成しない場合、Profile Management はデフォルトでどのディレクトリも除外しません。

除外リスト - ディレクトリ

同期中に無視されるフォルダーのリスト。フォルダー名はユーザープロファイル (%USERPROFILE%) に対する相対パスとして指定する必要があります。フォルダー名でのワイルドカードはサポートされていますが、再帰的には適用されません。

例:

- `Desktop` はユーザープロファイル内の `Desktop` フォルダーを無視します

このポリシーが無効になっている場合、フォルダーは除外されません。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、フォルダーは除外されません。

ログオン時の除外チェック

この設定は、ユーザーストア内のプロファイルに除外されたファイルまたはフォルダーが含まれている場合に、Profile Managementが何を行うかを構成します。可能なポリシー設定と対応するアクションを次の表に示します。

ポリシー設定	アクション
設定が無効になっているか、「ログオン時に除外されたファイルまたはフォルダーを同期する」の値がデフォルトに設定されている	ユーザーがログオンすると、Profile Management はユーザー ストアからローカル プロファイルに除外されたファイルまたはフォルダーを同期します。

ポリシー設定	アクション
設定が「ログオン時に除外されたファイルまたはフォルダーを無視する」に設定されている	ユーザーがログオンすると、Profile Management はユーザー ストア内の除外されたファイルまたはフォルダーを無視します。
設定が「ログオン時に除外されたファイルまたはフォルダーを削除する」に設定されている	ユーザーがログオンすると、Profile Management はユーザー ストア内の除外されたファイルまたはフォルダーを削除します。
設定がWeb Studioで構成されていない	.ini ファイルの値が使用されます
Web Studio または .ini ファイルで設定が構成されていません	除外されたファイルまたはフォルダーは、ユーザーがログオンしたときにユーザー ストアからローカル プロファイルに同期されます。

大容量ファイルの処理 - シンボリックリンクとして作成されるファイル

ログオンパフォーマンスを向上させ、サイズの大きいファイルを処理するために、Profile Management はこのリスト内のファイルをコピーする代わりにシンボリックリンクを作成します。

ファイルを参照するポリシーではワイルドカードを使用できます。例: `!ctx_localappdata!\Microsoft\Outlook*.OST`。

Microsoft Outlook のオフラインフォルダーファイル (`*.ost`) を処理するには、**Outlook** フォルダーが Profile Management の対象から除外されていないことを確認してください。

これらのファイルは、複数のセッションで同時にアクセスすることはできません。

同期ポリシー設定

同期セクションでは、ユーザープロファイル内のどのファイルとフォルダーを、プロファイルがインストールされているシステムとユーザー ストアの間で同期するかを指定するポリシー設定について説明します。

同期するディレクトリ

デフォルトでは、Profile Management は、ユーザープロファイルがインストールされているシステムとユーザー ストアの間でユーザープロファイルを同期します。フォルダーを同期から除外した場合、このポリシーを使用すると、除外されたフォルダーのサブフォルダーを同期に含めることができます。

このリストのパスは、ユーザープロファイルに対する相対パスである必要があります。フォルダー名でのワイルドカードはサポートされていますが、再帰的には適用されません。

このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、ユーザープロファイル内の除外されていないフォルダーのみが同期されます。

同期するファイル

デフォルトでは、Profile Management は、ユーザープロファイルがインストールされているシステムとユーザー ストアの間でユーザープロファイルを同期します。フォルダーを同期から除外した場合、このポリシーを使用すると、除外されたフォルダー内のファイルを同期に含めることができます。

このリストのパスは、ユーザープロファイルに対する相対パスである必要があります。ワイルドカードはファイル名とフォルダー名でサポートされていますが、ファイル名のワイルドカードのみが再帰的に適用されます。ワイルドカードをネストすることはできません。

例:

- `AppData\Local\Microsoft\Office\Access.qat` は、デフォルト構成で除外されているフォルダーの下のファイルを指定します
- `AppData\Local\MyApp*.cfg` は、プロファイルフォルダー `AppData\Local\MyApp` およびそのサブフォルダー内の拡張子 `.cfg` を持つすべてのファイルを指定します

このポリシーを無効にすると、有効にして空のリストを構成した場合と同じ効果があります。

このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、ユーザープロファイル内の除外されていないファイルのみが同期されます。

ミラーリングするフォルダー

このポリシーを使用すると、トランザクションフォルダー（参照フォルダーとも呼ばれます）に関連する問題を解決できます。そのフォルダーには、相互に依存するファイルが含まれており、あるファイルが別のファイルを参照しています。

フォルダーのミラーリングにより、プロファイル管理はトランザクションフォルダーとその内容を単一のエンティティとして処理し、プロファイルの肥大化を防ぐことができます。たとえば、**Internet Explorer の Cookie** フォルダーをミラーリングして、Index.dat がインデックス化する Cookie と同期されるようにすることができます。このような状況では、「最後の書き込みが優先

されます」。そのため、複数のセッションで変更されたミラーリングされたフォルダー内のファイルは、最後の更新によって上書きされ、プロファイル変更が失われます。

たとえば、次の表は、ユーザーがインターネットを閲覧している間に Index.dat が Cookie をどのように参照するかを示しています。

シナリオ	INDEX.DAT が COOKIE を参照する方法	
ユーザーは2つのInternet Explorerセッションを持っており、それぞれ異なるサーバー上にあり、各セッションで異なるサイトを訪問します。	各サイトからのCookieは、適切なサーバーに追加されます。	各サイトからのCookieは、適切なサーバーに追加されます。
ユーザーが最初のセッションからログオフするか、セッションの途中でログオフします（アクティブな書き戻し機能が構成されている場合）。	2番目のセッションからのCookieは、最初のセッションからのCookieを置き換える必要があります。	
最初のセッションと2番目のセッションがマージされ、Index.dat内のCookieへの参照が古くなります。	新しいセッションでのさらなるブラウジングは、繰り返しのマージと肥大化したCookieフォルダーにつながります。	

Cookie フォルダーをミラーリングすることで、この問題が解決されます。この場合、ユーザーがログオフするたびに、Cookie は最後のセッションからの Cookie で上書きされます。これにより、Index.dat は常に最新の状態に保たれます。

ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。ここで、または .ini ファイルでこのポリシーが構成されていない場合、フォルダーはミラーリングされません。

フォルダーのミラーリングを高速化する

このポリシーと**ミラーリングするフォルダー**ポリシーの両方を有効にすると、**Profile Management は、ミラーリングされた**フォルダーを VHDX ベースの仮想ディスクに保存します。仮想ディスクはログオン時にアタッチされ、ログオフ時にデタッチされます。このポリシーを有効にすると、ユーザー ストアとローカル プロファイルの間でフォルダーをコピーする必要がなくなり、フォルダーのミラーリングが高速化されます。

フォルダーリダイレクトポリシー設定

このセクションには、プロファイルに一般的に表示されるフォルダーを共有ネットワークの場所にリダイレクトするかどうかを指定するポリシー設定が含まれています。

管理者アクセス権の付与

この設定により、管理者はユーザーのリダイレクトされたフォルダーのコンテンツにアクセスできるようになります。

> **注：**
>
> この設定は、ドメインへの完全かつ無制限のアクセス権を持つ管理者に対して権限を付与します。

デフォルトでは、この設定は無効になっており、ユーザーにはリダイレクトされたフォルダーのコンテンツへの排他的アクセス権が付与されます。

ドメイン名を含める

この設定により、UNC パスの一部として `%userdomain%` 環境変数を含めることができます。この UNC パスは、リダイレクトされたフォルダーに指定されます。

デフォルトでは、この設定は無効になっています。また、リダイレクトされたフォルダーに指定された UNC パスの一部として `%userdomain%` 環境変数は含まれません。

AppData(Roaming) ポリシー設定

このセクションには、**AppData(Roaming)** フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

APPDATA(ROAMING) パス

この設定は、**AppData(Roaming)** フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

APPDATA(ROAMING) のリダイレクト設定

この設定は、**AppData(Roaming)** フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。詳細については、ユーザー ストアへのパス セクションを参照してください。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

お気に入りポリシー設定

このセクションには、「**お気に入り**」フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

お気に入りパス

この設定は、「**お気に入り**」フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

この設定がここで構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

お気に入りのリダイレクト設定

この設定は、「**お気に入り**」フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

この設定がここで構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

音楽ポリシー設定

このセクションには、**Music**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

音楽パス

この設定は、**Music**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

この設定がここで構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

音楽のリダイレクト設定

この設定は、**Music**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

Musicフォルダーのコンテンツをリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次のUNCパスにリダイレクトします。ミュージックパスポリシー設定で指定されたUNCパスにコンテンツをリダイレクトします。
- ドキュメントフォルダーを基準にリダイレクトします。ドキュメントフォルダーを基準としたフォルダーにコンテンツをリダイレクトします。

Documentsフォルダーを基準としたフォルダーにコンテンツをリダイレクトするには、**Documents path**設定を有効にする必要があります。

この設定がここで構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

画像ポリシー設定

このセクションには、「**ピクチャ**」フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

画像パス

この設定は、「**ピクチャ**」フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

画像のリダイレクト設定

この設定は、「**ピクチャ**」フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

「**ピクチャ**」フォルダーのコンテンツをリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次の UNC パスにリダイレクトします。「ピクチャ」パスのポリシー設定で指定された UNC パスにコンテンツをリダイレクトします。
- ドキュメントフォルダーを基準にリダイレクトします。コンテンツをドキュメントフォルダーを基準としたフォルダーにリダイレクトします。

「**ドキュメント**」フォルダーを基準としたフォルダーにコンテンツをリダイレクトするには、「**ドキュメントパス**」設定を有効にする必要があります。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

保存されたゲームのポリシー設定

このセクションには、**保存されたゲーム**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

保存されたゲームのリダイレクト設定

この設定は、**保存されたゲーム**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

保存されたゲームのパス

この設定は、**保存されたゲーム**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

Searchesポリシー設定

このセクションには、「**Searches**」フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

SEARCHESのリダイレクト設定

この設定は、「**Searches**」フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

SEARCHESパス

この設定は、「**Searches**」フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ビデオポリシー設定

このセクションには、**ビデオ**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ビデオのリダイレクト設定

この設定は、**ビデオ**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ビデオフォルダーのコンテンツをリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次のUNCパスにリダイレクトします。コンテンツを、ビデオパスポリシー設定で指定されたUNCパスにリダイレクトします。
- ドキュメントフォルダーを基準にリダイレクトします。コンテンツを、ドキュメントフォルダーを基準としたフォルダーにリダイレクトします。

ドキュメントフォルダーを基準としたフォルダーにコンテンツをリダイレクトするには、**ドキュメントパス**設定を有効にする必要があります。

この設定がここで構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

ビデオパス

この設定は、**ビデオ**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

この設定がここで構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

ログポリシー設定

このセクションには、Profile Management のログ記録を構成するポリシー設定が含まれています。

Active Directory のアクション

この設定は、Active Directory で実行されるアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定が Web Studio で構成されていない場合、.ini ファイルの値が使用されます。

この設定が Web Studio または .ini ファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

一般的な情報

この設定は、一般的な情報の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

一般的な警告

この設定は、一般的な警告の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログの有効化**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー

- 一般情報

ログの有効化

この設定は、デバッグ（詳細ログ）モードでのProfile Managementログを有効または無効にします。デバッグモードでは、"%SystemRoot%\System32\Logfiles\UserProfileManager" にあるログファイルに詳細なステータス情報が記録されます。

デフォルトでは、この設定は無効になっており、エラーのみがログに記録されます。

Citrix®は、Profile Managementのトラブルシューティングを行う場合にのみ、この設定を有効にすることをお勧めします。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、エラーのみがログに記録されます。

ファイルシステムのアクション

この設定は、ファイルシステムで実行されたアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログの有効化**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ファイルシステム通知

この設定は、ファイルシステム通知の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログの有効化**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオフ

この設定は、ユーザーのログオフの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオン

この設定は、ユーザーのログオンの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログファイルの最大サイズ

この設定は、Profile Managementログファイルの最大許容サイズをバイト単位で指定します。

デフォルトでは、この値は1048576バイト（1 MB）に設定されています。

十分なディスク容量がある場合、Citrixはこのファイルのサイズを5 MB以上に増やすことを推奨します。ログファイルが最大サイズを超えて増加した場合：

- 既存のファイルのバックアップ（.bak）が削除されます
- ログファイルは.bakに名前が変更されます
- 新しいログファイルが作成されます

ログファイルは %SystemRoot%\\System32\\Logfiles\\UserProfileManager に作成されます。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がここで、または.iniファイルで構成されていない場合、デフォルト値が使用されます。

ログファイルへのパス

この設定は、Profile Managementログファイルを保存するための代替パスを指定します。

デフォルトでは、この設定は無効になっており、ログファイルはデフォルトの場所である%SystemRoot%\System32\Logfiles\UserProfileManagerに保存されます。

パスはローカルドライブまたはリモートネットワークベースのドライブ（UNCパス）を指すことができます。リモートパスは大規模な分散環境で役立つ場合がありますが、かなりのネットワークトラフィックを生成する可能性があり、ログファイルには不適切な場合があります。永続的なハードドライブを持つプロビジョニングされた仮想マシンでは、そのドライブへのローカルパスを設定します。この設定により、マシンの再起動時にログファイルが保持されます。永続的なハードドライブを持たない仮想マシンでは、UNCパスを設定することでログファイルを保持できます。ただし、マシンのシステムアカウントにはUNC共有への書き込みアクセス権が必要です。オフラインプロファイル機能によって管理されるラップトップには、ローカルパスを使用してください。

ログファイルにUNCパスを使用する場合、Citrixはログファイルフォルダーに適切なアクセス制御リストを適用することを推奨します。この設定により、承認されたユーザーまたはコンピューターアカウントのみが保存されたファイルにアクセスできるようになります。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

ここまたは .ini ファイルでこの設定が構成されていない場合、デフォルトの場所 %SystemRoot%\System32\Logfiles\UserProfileManager が使用されます。

パーソナライズされたユーザー情報

この設定は、パーソナライズされたユーザー情報の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合、**ログの有効化**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオン時とログオフ時のポリシー値

この設定は、ユーザーがログオンおよびログオフするときのポリシー値の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合、**ログの有効化**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

レジストリアクション

この設定は、レジストリで実行されたアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオフ時のレジストリの相違点

この設定は、ユーザーがログオンおよびログオフする際のポリシー値の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー

- 一般情報

レジストリアクション

この設定は、レジストリで実行されたアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオフ時のレジストリの差異

この設定は、ユーザーがログオフしたときのレジストリの差異に関する詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

プロファイル処理ポリシー設定

このセクションには、Profile Management がユーザープロファイルを処理する方法を指定するポリシー設定が含まれています。

キャッシュされたプロファイルを削除するまでの遅延

この設定は、Profile Management がログオフ時にローカルにキャッシュされたプロファイルを削除するまでの遅延を、分単位で任意に延長する時間を指定します。

値を0にすると、ログオフプロセスの終了時にプロファイルがすぐに削除されます。Profile Management は1分ごとにログオフをチェックします。その結果、値を60にすると、ユーザーがログオフしてから1〜2分後にプロファイルが削除されることが保証されます。このアクションは、最後のチェックがいつ行われたかによって異なります。ログオフ中にプロセスがファイルまたはユーザーレジストリハイブを開いたままにしていることがわかっている場合、遅延を延長することは役立ちます。大規模なプロファイルの場合、このプロセスはログオフを高速化することもできます。

デフォルトでは、この値は0に設定されており、Profile Management はローカルにキャッシュされたプロファイルをすぐに削除します。

この設定を有効にする場合は、「ログオフ時にローカルにキャッシュされたプロファイルを削除する」も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、プロファイルはすぐに削除されます。

ログオフ時にローカルにキャッシュされたプロファイルを削除する

この設定は、ユーザーがログオフした後にローカルにキャッシュされたプロファイルが削除されるかどうかを指定します。

この設定が有効になっている場合、ユーザーがログオフした後にローカルプロファイルキャッシュが削除されます。Citrix® は、ターミナルサーバーに対してこの設定を有効にすることをお勧めします。

デフォルトでは、この設定は無効になっており、ユーザーがログオフした後もローカルプロファイルキャッシュは保持されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、キャッシュされたプロファイルは削除されません。

ローカルプロファイルの競合処理

この設定は、ユーザープロファイルが以下の両方に存在する場合のProfile Managementの動作を構成します。

- ユーザー ストア
- ローカルWindowsユーザープロファイル（Citrixユーザープロファイルではない）

デフォルトでは、Profile Management はローカルの Windows プロファイルを使用しますが、それを一切変更しません。

Profile Management の動作を制御するには、次のいずれかのオプションを選択します。

- ローカルプロファイルを使用する。Profile Managementはローカルプロファイルを使用しますが、それを一切変更しません。
- ローカルプロファイルを削除する。Profile ManagementはローカルWindowsユーザープロファイルを削除し、その後、ユーザー ストアからCitrixユーザープロファイルをインポートします。
- ローカルプロファイルの名前を変更する。Profile ManagementはローカルWindowsユーザープロファイルの名前を変更し（バックアップ目的で）、その後、ユーザー ストアからCitrixユーザープロファイルをインポートします。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がここで、または .ini ファイルで構成されていない場合、既存のローカルプロファイルが使用されます。

既存プロファイルの移行

この設定は、ユーザーがユーザー ストアに現在のプロファイルを持っていない場合に、ログオン中にユーザー ストアに移行されるプロファイルの種類を指定します。

ユーザーがユーザー ストアにプロファイルを持っていない場合、Profile Managementはログオン中に既存のプロファイルを「オンザフライ」で移行できます。その後、ユーザー ストアのプロファイルは、以下の両方でProfile Managementによって使用されます。

- 現在のセッション
- 同じユーザー ストアへのパスで構成されたその他のセッション

デフォルトでは、ログオン時にローカルプロファイルと移動プロファイルの両方がユーザー ストアに移行されます。

ログオン中にユーザー ストアに移行されるプロファイルの種類を指定するには、次のいずれかのオプションを選択します。

- ローカルプロファイルと移動プロファイル
- ローカル
- ローミング
- なし (無効)

なしを選択すると、Profile Managementがインストールされていない環境であるかのように、システムは既存のWindowsメカニズムを使用してプロファイルを作成します。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、既存のローカルプロファイルとローミングプロファイルが移行されます。

既存のアプリケーションプロファイルの自動移行

この設定は、異なるオペレーティングシステム間で既存のアプリケーションプロファイルを自動的に移行するかどうかを有効または無効にします。アプリケーションプロファイルには、`AppData`フォルダー内のアプリケーションデータと、`HKEY_CURRENT_USER\SOFTWARE`の下のレジストリエントリの両方が含まれます。この設定は、異なるオペレーティングシステム間でアプリケーションプロファイルを移行したい場合に役立ちます。

たとえば、オペレーティングシステム（OS）をWindows 10バージョン1803からWindows 10バージョン1809にアップグレードするとします。この設定が有効になっている場合、各ユーザーが最初にログオンするときに、Profile Managementは既存のアプリケーション設定をWindows 10バージョン1809に自動的に移行します。その結果、`AppData`フォルダー内のアプリケーションデータとHKEY_CURRENT_USER\SOFTWAREの下のレジストリエントリが移行されます。

複数の既存のアプリケーションプロファイルがある場合、Profile Managementは次の優先順位で移行を実行します。

1. 同じOSタイプのプロファイル (シングルセッションOSからシングルセッションOS、マルチセッションOSからマルチセッションOS)。
2. 同じWindows OSファミリーのプロファイル。例: Windows 10からWindows 10、またはWindows Server 2016からWindows Server 2016。
3. 以前のバージョンのOSのプロファイル。例: Windows 7からWindows 10、またはWindows Server 2012からWindows 2016。
4. 最も近いOSのプロファイル。

注： ユーザーストアパスに変数「!CTX_OSNAME!」を含めることで、OSの短い名前を指定する必要があります。これにより、Profile Managementは既存のアプリケーションプロファイルを特定できます。

ここでこの設定が構成されていない場合、.iniファイルの設定が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、デフォルトで無効になります。

テンプレートプロファイルへのパス

この設定は、Profile Managementがユーザープロファイルを作成するためのテンプレートとして使用するプロファイルへのパスを指定します。

指定されたパスは、NTUSER.DATレジストリファイルと、テンプレートプロファイルに必要なその他のフォルダーおよびファイルを含むフォルダーへの完全なパスである必要があります。

注: パスにNTUSER.DATを含めないでください。たとえば、ファイル \\ \myservername\myprofiles\template\ntuser.dat の場合、場所は \\ \myservername\myprofiles\template と設定します。

絶対パスを使用します。これはUNCパスまたはローカルマシン上のパスのいずれかです。後者を使用すると、たとえば、Citrix Provisioning™ Servicesイメージ上にテンプレートプロファイルを永続的に指定できます。相対パスはサポートされていません。

注: この設定は、Active Directory属性、システム環境変数、または`%USERNAME%`および`%USERDOMAIN%`変数の展開をサポートしていません。

デフォルトでは、この設定は無効になっており、新しいユーザープロファイルは、ユーザーが最初にログオンするデバイスのデフォルトユーザープロファイルから作成されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、テンプレートは使用されません。

テンプレートプロファイルがローカルプロファイルを上書きする

この設定により、ユーザープロファイルの作成時にテンプレートプロファイルがローカルプロファイルを上書きできるようになります。

ユーザーがCitrixユーザープロファイルを持たず、ローカルのWindowsユーザープロファイルを持っている場合を考えます。この場合、この値が有効になっていると、デフォルトでローカルプロファイルが使用され、ユーザーストアに移行されます。このポリシー設定を有効にすると、ユーザープロファイルの作成時に使用されるローカルプロファイルをテンプレートプロファイルが上書きできるようになります。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、テンプレートは使用されません。

テンプレートプロファイルが移動プロファイルを上書きする

この設定により、ユーザープロファイルの作成時にテンプレートプロファイルが移動プロファイルを上書きできるようになります。

ユーザーがCitrixユーザープロファイルを持たず、移動Windowsユーザープロファイルを持っている場合を考えます。この場合、この値が有効になっていると、デフォルトで移動プロファイルが使用され、ユーザーストアに移行されます。このポリシー設定を有効にすると、ユーザープロファイルの作成時に使用される移動プロファイルをテンプレートプロファイルが上書きできるようになります。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、テンプレートは使用されません。

すべてのログオンでCitrix必須プロファイルとして使用されるテンプレートプロファイル

この設定により、Profile Managementはテンプレートプロファイルをすべてのユーザープロファイルを作成するためのデフォルトプロファイルとして使用できるようになります。

デフォルトでは、この設定は無効になっており、新しいユーザープロファイルは、ユーザーが最初にログオンするデバイスのデフォルトユーザープロファイルから作成されます。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、テンプレートは使用されません。

レジストリポリシー設定

このセクションには、Profile Management の処理から含める、または除外するレジストリキーを指定するポリシー設定が含まれています。

除外リスト

ログオフ時に無視される HKCU ハイブ内のレジストリキーのリスト。

例: Software\Policies

このポリシーが無効になっている場合、レジストリキーは除外されません。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、レジストリキーは除外されません。

含めるリスト

ログオフ時に処理される HKCU ハイブ内のレジストリキーのリスト。

例: Software\Adobe。

このポリシーが有効になっている場合、このリストにあるキーのみが処理されます。このポリシーが無効になっている場合、HKCU ハイブ全体が処理されます。ここでこのポリシーが構成さ

れていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、HKCU のすべてが処理されます。

デフォルトの除外リストを有効にする - Profile Management 5.5

HKCU ハイブ内のレジストリキーのデフォルトリストで、ユーザープロファイルに同期されません。このポリシーを使用して、GPO 除外ファイルを手動で入力することなく指定できます。

このポリシーを無効にすると、Profile Management はデフォルトでレジストリキーを除外しません。ここでこのポリシーを構成しない場合、Profile Management は .ini ファイルの値を使用します。ここで、または .ini ファイルでこのポリシーを構成しない場合、Profile Management はデフォルトでレジストリキーを除外しません。

NTUSER.DATのバックアップ

NTUSER.DATの最後に正常だったコピーのバックアップを有効にし、破損がある場合にロールバックします。

ここでこのポリシーを構成しない場合、Profile Management は .ini ファイルの値を使用します。ここで、または .ini ファイルでこのポリシーを構成しない場合、Profile Management は NTUSER.DAT をバックアップしません。

ストリーム配信ユーザープロファイルポリシー設定

このセクションには、Profile Management がストリーム配信ユーザープロファイルを処理する方法を指定するポリシー設定が含まれています。

常にキャッシュ

この設定は、ユーザーのログオン後、Profile Management がストリーム配信ファイルをできるだけ早くキャッシュするかどうかを指定します。ユーザーのログオン後にファイルをキャッシュすると、ネットワーク帯域幅が節約され、ユーザーエクスペリエンスが向上します。

この設定は、**プロファイルストリーミング**設定と組み合わせて使用します。

デフォルトでは、この設定は無効になっており、ユーザーのログオン後、ストリーム配信ファイルはできるだけ早くキャッシュされません。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、無効になります。

常にキャッシュするサイズ

この設定は、ストリーミングされるファイルのサイズの下限を MB 単位で指定します。Profile Management は、ユーザーがログオンした直後に、このサイズ以上のファイルをキャッシュします。

デフォルトでは、値は 0 (ゼロ) に設定されており、プロファイル全体をキャッシュする機能が使用されます。プロファイル全体をキャッシュする機能が有効になっている場合、Profile Management は、ユーザーがログオンした後、バックグラウンドタスクとしてユーザーストア内のすべてのプロファイルコンテンツを取得します。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、無効になります。

プロファイルストリーミング

この設定は、Citrix® ストリーム配信ユーザープロファイル機能を有効または無効にします。有効にすると、プロファイルファイルとフォルダーは、ユーザーがログオン後にアクセスした場合にのみ、ユーザーストアからローカルコンピューターにフェッチされます。レジストリエントリと保留領域のファイルはすぐにフェッチされます。

デフォルトでは、プロファイルストリーミングは無効になっています。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、無効になります。

ストリーミングユーザープロファイルグループ

この設定は、Windows ユーザーグループに基づいて、OU 内のどのユーザープロファイルをストリーム配信するかを指定します。

有効にすると、指定されたユーザーグループ内のユーザープロファイルのみがストリーミングされます。その他のすべてのユーザープロファイルは通常どおり処理されます。

デフォルトでは、この設定は無効になっており、OU内のすべてのユーザープロファイルは通常どおり処理されます。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、すべてのユーザープロファイルが処理されます。

プロファイルストリーミング除外を有効にする

プロファイルストリーミングの除外が有効になっている場合：

- Profile Managementは、除外リスト内のフォルダーをストリーミングしません
- ユーザーがログオンすると、すべてのフォルダーがユーザーストアからローカルコンピューターにすぐにフェッチされます

詳細については、「ユーザープロファイルのストリーム」を参照してください。

ペンディングエリアロックファイルのタイムアウト

この設定は、ストレージサーバーが応答しなくなったときにユーザープロファイルストアがロックされたままの場合、保留領域からユーザープロファイルストアにユーザーのファイルが書き戻されるまでの日数を指定します。この動作により、保留領域の肥大化が防止され、ユーザープロファイルストアに常に最新のファイルが含まれるようになります。

デフォルトでは、この設定は1日（one day）に設定されています。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、デフォルト値が使用されます。

ペンディングエリアのプロファイルストリーミングを有効にする

ペンディングエリア内のファイルとフォルダーに対してプロファイルストリーミング機能を有効にできます。

保留領域は、プロファイルストリーミングが有効になっている間、プロファイルの一貫性を確保するために使用されます。同時セッションで変更されたプロファイルファイルとフォルダーを一時的に保存します。

既定では、このポリシーは無効になっており、ログオン時に保留領域内のすべてのファイルとフォルダーがローカルプロファイルにフェッチされます。このポリシーを有効にすると、保留領域内のファイルは要求されたときにのみローカルプロファイルにフェッチされます。このポリシーをプロファイルストリーミングポリシーと組み合わせて使用すると、同時セッションシナリオで最適なログオンエクスペリエンスを確保できます。

このポリシーは、「フォルダーのプロファイルストリーミングを有効にする」ポリシーが有効になっている場合、保留領域内のフォルダーに適用されます。

ユーザーパーソナライゼーションポリシー設定

Virtual Delivery Agent 内でユーザーレイヤーのマウントを有効にするには、構成パラメーターを使用して以下を指定します。

- ネットワーク上のどこからユーザーレイヤーにアクセスするか。
- 新しいユーザーレイヤーディスクがどのくらいのサイズまで拡張できるか。

そのため、次の2つのポリシーが利用可能なポリシーのリストに表示されます。

- ユーザーレイヤーリポジトリパス - 値フィールドに「\\サーバー名またはアドレス\フォルダー名」の形式でパスを入力します。
- ユーザーレイヤーサイズ (GB) - デフォルトのユーザーレイヤーサイズである10 GBは、Citrix® が推奨する最小値です。ユーザーレイヤーは、スペースが使用されるにつれて設定されたサイズに拡張されるシンプロビジョニングディスクです。ユーザーレイヤーのサイズが小さくなることはありません。

> **注:**
>
> ユーザーレイヤーサイズを増やすと、新しいユーザーレイヤーに影響を与え、既存のレイヤーを拡張します。レイヤーサイズを減らすと、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

詳細については、「ユーザーパーソナライゼーションレイヤー」を参照してください。

Virtual Delivery Agent ポリシー設定

Virtual Delivery Agent (VDA) セクションには、サイトの VDA とコントローラー間の通信を制御するポリシー設定が含まれています。

重要: 自動更新機能を使用しない場合、VDA は Delivery Controller™ に登録するために、これらの設定によって提供される情報を必要とします。この情報は登録に必要であるため、VDA のインストール中にこの情報を提供しない限り、グループポリシーエディターを使用して以下の設定を構成する必要があります。

- コントローラー登録 IPv6 ネットマスク
- コントローラー登録ポート
- コントローラー SID
- コントローラー
- IPv6 コントローラー登録のみを使用
- サイト GUID

コントローラー登録 IPv6 ネットマスク

このポリシー設定により、管理者は VDA を優先サブネットのみに制限できます (グローバル IP が登録されている場合でも)。この設定は、VDA が登録する IPv6 アドレスとネットワークを指定します。VDA は、指定されたネットマスクに一致する最初のアドレスにのみ登録します。この設定は、「IPv6 コントローラー登録のみを使用」ポリシー設定が有効になっている場合にのみ有効です。

デフォルトでは、この設定は空白です。

コントローラー登録ポート

この設定は、**コントローラーの自動更新を有効にする** 設定が無効になっている場合にのみ使用してください。

この設定は、VDA がレジストリベースの登録を使用する際に、コントローラーに登録するために使用する TCP/IP ポート番号を指定します。

デフォルトでは、ポート番号は80に設定されています。

コントローラーSID

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用してください。

この設定は、レジストリベースの登録を使用する際にVDAがControllerに登録するために使用する、スペース区切りのコントローラーセキュリティ識別子（SID）のリストを指定します。この設定はオプションであり、登録に使用されるControllerのリストを制限するために**コントローラー**設定と組み合わせて使用される場合があります。

デフォルトでは、この設定は空白です。

コントローラー

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用してください。

この設定は、レジストリベースの登録を使用する際にVDAがControllerに登録するために使用する、スペース区切りのコントローラー完全修飾ドメイン名（FQDN）のリストを指定します。この設定はオプションであり、**コントローラーSID**設定と組み合わせて使用される場合があります。

デフォルトでは、この設定は空白です。

コントローラーの自動更新を有効にする

この設定により、VDAはインストール後にControllerに自動的に登録できるようになります。

VDAが登録されると、登録先のControllerは現在のコントローラーFQDNとSIDのリストをVDAに送信します。VDAはこのリストを永続ストレージに書き込みます。各Controllerは、90分ごとにSiteデータベースをチェックしてController情報を確認します。以下のいずれかの事象が発生した場合、Controllerは登録済みのVDAに更新されたリストを送信します。

- 前回のチェック以降にControllerが追加または削除された場合
- ポリシー変更が発生した場合

VDAは、受信した最新のリストにあるすべてのControllerからの接続を受け入れます。

デフォルトでは、この設定は有効になっています。

IPv6コントローラー登録のみを使用

この設定は、VDAがコントローラーに登録するために使用するアドレス形式を制御します。

- 有効にすると、VDAはマシンのIPv6アドレスを使用してコントローラーに登録します。VDAがコントローラーと通信する場合、次のアドレス順序を使用します：グローバルIPアドレス、ユニークローカルアドレス（ULA）、リンクローカルアドレス（他のIPv6アドレスが利用できない場合）。
- 無効にすると、VDAはマシンのIPv4アドレスを使用してコントローラーに登録し、通信します。

デフォルトでは、この設定は無効になっています。

サイトGUID

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用してください。

この設定は、Active Directoryベースの登録を使用する際に、VDAがコントローラーに登録するために使用するサイトのグローバル一意識別子（GUID）を指定します。

デフォルトでは、この設定は空白です。

HDX™ 3D Pro ポリシー設定

HDX 3D Proセクションには、ユーザー向けに画質構成ツールを有効化および構成するためのポリシー設定が含まれています。このツールを使用すると、ユーザーは利用可能な帯域幅の使用を最適化できます。この最適化のために、画質と応答性のバランスがリアルタイムで調整されます。

ロスレスを有効にする

この設定は、ユーザーが画質構成ツールを使用してロスレス圧縮を有効または無効にできるかどうかを指定します。デフォルトでは、ユーザーにロスレス圧縮を有効にするオプションは提供されません。

ユーザーがロスレス圧縮を有効にしたとします。この場合、画質は画質構成ツールで利用可能な最大値に自動的に設定されます。デフォルトでは、ユーザーデバイスとホストコンピューターの機能に応じて、GPUベースまたはCPUベースの圧縮のいずれかを使用できます。

HDX 3D Pro の画質設定

この設定は、画質構成ツールでユーザーが利用できる最小値と最大値を指定します。これらの値を使用して、画質構成ツールで画質調整の範囲を定義できます。

画質の値は0から100の範囲で指定します（両端を含む）。最大値は最小値以上である必要があります。

監視ポリシー設定

監視セクションには、プロセス、リソース監視、およびアプリケーション障害監視のポリシー設定が含まれています。

これらのポリシーのスコープは、以下に基づいて定義できます。

- サイト
- デリバリーグループ
- デリバリーグループの種類
- 組織単位
- タグ

プロセスおよびリソース監視のポリシー

CPU、メモリ、プロセスの各データポイントはVDAから収集され、監視データベースに保存されます。VDAからデータポイントを送信するとネットワーク帯域幅を消費し、それらを保存すると監視データベースの相当なスペースを消費します。特定のスコープ（たとえば、特定のデリバリーグループや組織単位）に対して、リソースデータ、プロセスデータ、またはその両方を監視したくない場合を考慮してください。この場合、ポリシーを無効にすることをお勧めします。

プロセス監視を有効にする

この設定を有効にすると、VDAがインストールされているマシンで実行されているプロセスの監視が可能になります。CPUやメモリ使用量などの統計情報は、監視サービスに送信されます。これらの統計情報は、Directorでのリアルタイム通知および履歴レポートに使用されます。

この設定のデフォルトは無効です。

リソース監視を有効にする

この設定を有効にすると、VDAがインストールされているマシン上の重要なパフォーマンスカウンターの監視が可能になります。CPUおよびメモリ使用量、IOPS、ディスク遅延データなどの統計情報は、監視サービスに送信されます。これらの統計情報は、Directorでのリアルタイム通知および履歴レポートに使用されます。

この設定のデフォルトは有効です。

スケーラビリティ

CPUとメモリのデータは、各VDAから5分間隔でデータベースにプッシュされます。プロセスデータ（有効な場合）は10分間隔でデータベースにプッシュされます。IOPSとディスクの待機時間データは1時間間隔でデータベースにプッシュされます。

CPUとメモリデータ

CPUとメモリデータは、デフォルトで**有効**です。データ保持期間の値は次のとおりです (Platinumライセンス):

データ粒度	日数
5分間隔のデータ	1日
10分間隔のデータ	7日
1時間間隔のデータ	30日
1日1回（日次）のデータ	90日

IOPSおよびディスク待機時間データ

IOPSおよびディスク待機時間データは、デフォルトで**有効**になっています。データ保持値は次のとおりです（Platinumライセンス）：

データ粒度	日数
時間別データ	3日間
日別データ	90日間

データ保持設定により、1つのVDAに対して1年間、次の情報を保存するために約276 KBのディスク領域が必要になります。

- CPU
- メモリ
- IOPS
- ディスク遅延データ

マシン数	必要なストレージ容量（概算）
1	276 KB
1K	270 MB
40K	10.6 GB

プロセスデータ

プロセスデータはデフォルトで**無効**です。必要に応じて、一部のマシンでプロセスデータを有効にすることをお勧めします。プロセスデータのデフォルトのデータ保持設定は次のとおりです。

データ粒度	日数
10分間データ	1日
時間データ	7日間

プロセスデータがデフォルトの保持設定で有効になっている場合、プロセスデータは、1年間でVDAあたり約1.5 MB、ターミナルサービスVDA (TS VDA) あたり3 MBを消費します。

マシン数	必要なストレージの目安 VDA	必要なストレージの目安 TS VDA
1	1.5 MB	3 MB
1K	1.5 GB	3 GB

注:

以前に提示された数値には、インデックス領域は含まれていません。また、すべての計算は概算であり、展開によって異なります。

オプションの構成

必要に応じて、デフォルトの保持設定を変更できます。ただし、この構成は追加のストレージを消費します。以下の設定を有効にすることで、プロセス使用率データの精度を高めることができます。有効にできる構成は次のとおりです。

ENABLEMINUTELEVELGRANULARITYPROCESSUTILIZATION

ENABLEDAYLEVELGRANULARITYPROCESSUTILIZATION

これらの構成は、監視PowerShellコマンドレットから有効にできます: Set-MonitorConfiguration

アプリケーション障害監視のポリシー

デフォルトでは、**アプリケーション障害**タブには、マルチセッションOS VDAからのアプリケーション障害のみが表示されます。アプリケーション障害監視の設定は、以下の監視ポリシーで変更できます。

アプリケーション障害の監視を有効にする

この設定を使用して、アプリケーション障害監視を構成し、アプリケーションエラーまたは障害（クラッシュおよび未処理の例外）、あるいはその両方を監視します。 **値**を**None**に設定すると、アプリケーション障害監視が無効になります。 この設定のデフォルトは「アプリケーション障害のみ」です。

シングルセッションOS VDAでのアプリケーション障害の監視を有効にする

デフォルトでは、マルチセッションOS VDAでホストされているアプリケーションからの障害のみが監視されます。シングルセッションOS VDAを監視するには、ポリシーを**Allowed**に設定します。 この設定のデフォルトは**Prohibited**です。

障害監視から除外されるアプリケーションのリスト

障害監視の対象としないアプリケーションのリストを指定します。 デフォルトでは、このリストは空です。

Analytics 用データ収集のポリシー

ANALYTICS 用 VDA データ収集

このポリシーを使用して、パフォーマンスおよびセキュリティ分析のために、Monitorサービスが VDAのパフォーマンスおよびセキュリティ関連のメトリックを収集するのを有効または無効にします。デフォルトでは、ポリシーは**Allowed**です。VDAからのデータ収集を停止するには、ポリシーを**Prohibited**に設定します。

セキュリティ監視のためのクリップボード場所メタデータ収集

このポリシーを使用して、セキュリティ監視、監査、およびコンプライアンスのために、Broker サービスによるクリップボード場所メタデータ収集を有効または無効にします。デフォルトで

は、ポリシーは**Enabled**です。VDAからのデータ収集を停止するには、ポリシーを**Disabled**に設定します。

パフォーマンス監視のための診断データ収集

このポリシーを使用して、監視サービスがセッション情報、UPM/EUEM サービスの状態、Microsoft Teams の最適化、接続プロトコルなどの診断データを収集できるようにします。デフォルトでは、ポリシーは**有効**です。VDA からのデータ収集を停止するには、ポリシーを**無効**に設定します。

ストレージ計画のヒント

グループポリシー。リソースデータまたはプロセスデータの監視に関心がない場合は、グループポリシーを使用して、いずれかまたは両方をオフにすることができます。詳細については、「ポリシーの作成」の**グループポリシー**セクションを参照してください。

データグルーミング。デフォルトのデータ保持設定を変更して、データを早期にグルーミングし、ストレージ領域を解放できます。グルーミング設定の詳細については、「API を使用したデータアクセス」の「データの粒度と保持」を参照してください。

レジストリを使用してCOMポートおよびLPTポートリダイレクト設定を構成する

VDAバージョン7.0から7.8では、**COMポートおよびLPTポート**の設定は、レジストリを使用してのみ構成できます。VDAバージョン7.0より前、およびVDAバージョン7.9以降では、これらの設定はWeb Studioで構成できます。詳しくは、ポートリダイレクトポリシー設定および帯域幅ポリシー設定を参照してください。

COMポートおよびLPTポートリダイレクトのポリシー設定は、VDAイメージまたはマシン上のHKLM\Software\Citrix\GroupPolicy\Defaults\Deprecatedにあります。

COMポートおよびLPTポートリダイレクトを有効にするには、次のようにREG_DWORD型の新しいレジストリキーを追加します。

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

レジストリキー	説明	許可される値
AllowComPortRedirection	COMポートリダイレクトを許可または禁止する	1（許可）または0（禁止）

レジストリキー	説明	許可される値
LimitComBw	COMポートリダイレクトチャネルの帯域幅制限	数値
LimitComBWPercent	COMポートリダイレクトチャネルの帯域幅制限（セッションの総帯域幅に対する割合）	0から100までの数値
AutoConnectClientComPorts	ユーザーデバイスからCOMポートを自動的に接続する	1 (許可) または 0 (禁止)
AllowLptPortRedirection	LPTポートリダイレクトを許可または禁止する	1 (許可) または 0 (禁止)
LimitLptBw	LPTポートリダイレクトチャネルの帯域幅制限	数値
LimitLptBwPercent	LPTポートリダイレクトチャネルの帯域幅制限（セッション全体の帯域幅に対する割合）	0から100までの数値
AutoConnectClientLptPorts	ユーザーデバイスからLPTポートを自動的に接続する	1 (許可) または 0 (禁止)

これらの設定を構成した後、マシンカタログを変更して、新しいマスターイメージまたは更新された物理マシンを使用するようにします。デスクトップは、ユーザーが次回ログオフしたときに新しい設定で更新されます。

Configuration Manager 2012 用コネクタのポリシー設定

Configuration Manager 2012 用コネクタのセクションには、Citrix Connector 7.5 エージェントを構成するためのポリシー設定が含まれています。

> **重要:**

> 警告、ログオフ、および再起動メッセージのポリシーは、手動またはProvisioning Servicesによって管理されるマルチセッションOSマシンカタログへの展開にのみ適用されます。これ

> らのマシンカタログの場合、Connectorサービスは、保留中のアプリケーションインストールまたはソフトウェアアップデートがある場合にユーザーに警告します。

> MCSによって管理されるカタログの場合、Web Studioを使用してユーザーに通知します。手動で管理されるシングルセッションOSカタログの場合、Configuration Managerを使用してユーザーに通知します。Provisioning Servicesによって管理されるシングルセッションOSカタログの場合、Provisioning Servicesを使用してユーザーに通知します。

警告頻度間隔

この設定は、ユーザーへの警告メッセージの表示間隔を定義します。

間隔は ddd.hh:mm:ss の形式で設定されます。ここで、:

- ddd は日数（オプションのパラメーター）で、範囲は 0〜999 です。
- hh は時間で、範囲は 0〜23 です。
- mm は分で、範囲は 0〜59 です。
- ss は秒で、範囲は 0〜59 です。

デフォルトでは、間隔設定は 1 時間 (01:00:00) です。

警告メッセージボックスの本文

この設定には、今後のソフトウェアアップデートやログオフが必要なメンテナンスについてユーザーに通知するメッセージの編集可能なテキストが含まれています。

既定では、メッセージは次のとおりです: {TIMESTAMP} 作業を保存してください。サーバーは{TIMELEFT}後にメンテナンスのためオフラインになります。

警告メッセージボックスのタイトル

この設定には、ユーザーへの警告メッセージのタイトルバーの編集可能なテキストが含まれています。

既定では、タイトルは次のとおりです: 今後のメンテナンス

警告期間

この設定は、メンテナンスのどれくらい前に警告メッセージが最初に表示されるかを定義します。

時間は、ddd.hh:mm:ss の形式を使用して設定されます。ここで、:

- dddは日数で、オプションのパラメーターであり、範囲は0～999です。
- hhは時間で、範囲は0～23です。
- mmは分で、範囲は0～59です。
- ssは秒で、範囲は0～59です。

既定では、この設定は 16 時間 (16:00:00) であり、最初の警告メッセージがメンテナンスの約 16 時間前に表示されることを示します。

最終強制ログオフメッセージボックスの本文

この設定には、強制ログオフが開始されたことをユーザーに警告するメッセージの編集可能なテキストが含まれています。

既定では、メッセージは次のとおりです: サーバーは現在、メンテナンスのためオフラインになります

最終強制ログオフメッセージボックスのタイトル

この設定には、最終的な強制ログオフメッセージのタイトルバーの編集可能なテキストが含まれています。

デフォルトでは、タイトルは「ITスタッフからの通知」です。

強制ログオフ猶予期間

この設定は、ユーザーにログオフを通知してから、保留中のメンテナンスを処理するための強制ログオフが実行されるまでの期間を定義します。

時間はddd.hh:mm:ss形式で設定され、ここで:

- dddは日数で、オプションのパラメーターであり、範囲は0～999です。
- hhは時間で、範囲は0～23です。
- mmは分で、範囲は0～59です。
- ssは秒で、範囲は0～59です。

デフォルトでは、強制ログオフ猶予期間の設定は5分（00:05:00）です。

強制ログオフメッセージボックスの本文

この設定には、強制ログオフを開始する前に、作業を保存してログオフするようにユーザーに指示するメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージには次の内容が含まれています: {TIMESTAMP} 作業を保存してログオフしてください。サーバーは{TIMELEFT}後にメンテナンスのためオフラインになります。

強制ログオフメッセージボックスのタイトル

この設定には、強制ログオフメッセージのタイトルバーの編集可能なテキストが含まれています。

既定では、タイトルは「ITスタッフからの通知」です。

イメージ管理モード

コネクタエージェントは、Provisioning ServicesまたはMCSによって管理されているマシンのクローンで実行されているかどうかを自動的に検出します。エージェントは、イメージ管理されたクローンでのConfiguration Managerの更新をブロックし、カタログのマスターイメージに更新を自動的にインストールします。

マスターイメージが更新された後、Web Studioを使用してMCSカタログクローンの再起動を調整します。コネクタエージェントは、Configuration Managerのメンテナンスウィンドウ中にPVSカタログクローンの再起動を自動的に調整します。この動作を上書きして、Configuration Managerによってカタログクローンにソフトウェアがインストールされるようにするには、イメージ管理モードを「無効」に変更します。

再起動メッセージボックスの本文

この設定には、サーバーが再起動されようとしているときにユーザーに通知するメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージは「サーバーは現在、メンテナンスのためにオフラインになります。」です。

エージェントタスクを実行する定期的な時間間隔

この設定は、Citrix Connector™エージェントタスクがどのくらいの頻度で実行されるかを決定します。

時間はddd.hh:mm:ssの形式で設定されます。ここで、:

- dddは日数で、オプションのパラメーターであり、範囲は0～999です。
- hhは時間で、範囲は0～23です。
- mmは分で、範囲は0～59です。
- ssは秒で、範囲は0～59です。

既定では、定期的な時間間隔の設定は5分 (00:05:00) です。

ポリシーの変更

次の表に、Citrix Virtual Apps and Desktops™ 7 2411 のポリシー更新（追加、削除、名前の変更、デフォルト状態の変更を含む）を示します。

ポリシー設定	変更点
一般 - 依存ポリシーに関する明確化	詳細はこちら。
一般 - ポリシーの複数選択機能	詳細はこちら。
プロファイル管理 > 詳細設定 > UWPアプリの読み込み高速化を有効にする	UWPアプリの読み込みを高速化するための新しいポリシーです。詳細はこちら。
プロファイル管理 > 詳細設定 > プロファイルサイズがクォータを超過した場合にユーザーに通知する	ユーザープロファイルサイズを監視し、クォータを超過した場合にユーザーに通知するための新しいポリシーです。詳細はこちら。
プロファイル管理 > 詳細設定 > プロファイルサイズがクォータを超過した場合の通知メッセージ	
クライアントプリンターポリシー設定 > 保持および復元されたクライアントプリンター	2402以降非推奨

注:

アップグレードする前に、すべての非推奨設定を削除してください。非推奨設定が使用されたままの場合、アップグレードはエラーで失敗する可能性があります。

管理

Citrix Virtual Apps and Desktops™サイトの管理には、さまざまな項目とタスクが含まれます。

ライセンス

サイトを作成する際には、Citrix License Serverへの有効な接続が必要です。その後、Studioから、ライセンスの追加、ライセンスの種類やモデルの変更、ライセンス管理者の管理など、いくつかのライセンス関連タスクを実行できます。StudioからLicense Administration Consoleにアクセスすることもできます。

アプリケーション

デリバリーグループ、およびオプションでアプリケーショングループ内のアプリケーションを管理します。

ゾーン

地理的に分散した展開では、ゾーンを使用してアプリケーションとデスクトップをエンドユーザーの近くに配置し、パフォーマンスを向上させることができます。サイトをインストールして構成すると、すべてのController、マシンカタログ、およびホスト接続は1つのプライマリゾーンに配置されます。その後、Studioを使用して、これらの項目を含むサテライトゾーンを作成できます。サイトに複数のゾーンがある場合、新しく作成されたマシンカタログ、ホスト接続、または追加されたControllerをどのゾーンに配置するかを指定できるようになります。ゾーン間で項目を移動することもできます。

接続とリソース

アプリケーションとデスクトップをユーザーに提供するマシンをホストするためにハイパーバイザーまたはその他のサービスを使用している場合、サイトを作成するときに、そのハイパーバイザーまたはその他のサービスへの最初の接続を作成します。その接続のストレージとネットワークの詳細がそのリソースを構成します。その後、その接続とそのリソースを変更したり、さらに接続を作成したりできます。構成済みの接続を使用するマシンを管理することもできます。

ローカルホストキャッシュ

ローカルホストキャッシュを使用すると、Delivery Controller™とサイトデータベース間の接続が失敗した場合でも、サイトでの接続ブローカー操作を続行できます。

仮想IPと仮想ループバック

Microsoftの仮想IPアドレス機能は、公開されたアプリケーションにセッションごとに一意の動的に割り当てられたIPアドレスを提供します。Citrixの仮想ループバック機能を使用すると、localhostとの通信に依存するアプリケーションを、localhost範囲内の一意の仮想ループバックアドレスを使用するように構成できます。

デリバリーコントローラー

この記事では、サイトへのControllerの追加と削除に関する考慮事項と手順について説明します。また、Controllerを別のゾーンまたはサイトに移動する方法、およびVDAを別のサイトに移動する方法についても説明します。

ControllerへのVDA登録

VDAがアプリケーションとデスクトップの配信を支援するには、Controllerに登録（通信を確立）する必要があります。Controllerのアドレスは、この記事で説明されているいくつかの方法で指定できます。サイトでControllerが追加、移動、削除される際に、VDAが最新の情報を保持していることが重要です。

セッション

セッションアクティビティを維持することは、最高のユーザーエクスペリエンスを提供するために不可欠です。いくつかの機能により、セッションの信頼性を最適化し、不便さ、ダウンタイム、生産性の損失を軽減できます。

- セッションの信頼性
- クライアントの自動再接続
- ICA®キープアライブ
- ワークスペースコントロール
- セッションローミング

Studioでの検索の使用

Studioでマシン、セッション、マシンカタログ、アプリケーション、またはデリバリーグループに関する情報を表示したい場合は、柔軟な検索機能を使用します。

タグ

タグを使用して、マシン、アプリケーション、グループ、ポリシーなどのアイテムを識別します。その後、特定のタグを持つアイテムに適用されるように特定の操作を調整できます。

IPv4/IPv6

Citrix Virtual Apps and Desktops は、純粋な IPv4、純粋な IPv6、および IPv4 と IPv6 の重複するネットワークを使用するデュアルスタック展開をサポートしています。この記事では、これらの展開について説明し、図解します。また、IPv4 または IPv6 の使用を制御する Citrix ポリシー設定についても説明します。

ユーザープロファイル

デフォルトでは、VDA をインストールすると Citrix Profile Management が自動的にインストールされます。このプロファイルソリューションを使用する場合は、一般的な情報についてこの記事を確認してください。詳細については、Profile Management のドキュメントを参照してください。

Citrix Diagnostic Facility (CDF) トレースの収集

CDFControl ユーティリティは、さまざまな Citrix トレースプロバイダーから表示される Citrix Diagnostic Facility (CDF) トレースメッセージをキャプチャするためのイベントトレースコントローラーまたはコンシューマーです。これは、複雑な Citrix 関連の問題のトラブルシューティング、フィルターサポートの解析、およびパフォーマンスデータの収集のために作成されています。

シトリックス インサイト サービス

Citrix Insight Services (CIS) は、計測、テレメトリ、およびビジネスインサイト生成のための Citrix プラットフォームです。

シトリックス スカウト

Citrix Scout は、診断情報を収集し、ヘルスチェックを実行します。結果は、Citrix Virtual Apps and Desktops 展開におけるプロアクティブなメンテナンスに利用できます。Citrix は、Citrix Insight Services を通じて、診断コレクションの包括的で自動化された分析を提供します。また、Scout を使用して、単独で、または Citrix サポートのガイダンスを受けて、問題のトラブルシューティングを行うこともできます。

アプリケーション

> **注:**
>
> Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb

> Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の対応する記事を参照してください。

はじめに

展開でデリバリーグループのみを使用している場合（アプリケーショングループは使用しない場合）、アプリケーションはデリバリーグループに追加します。アプリケーショングループも使用している場合は、通常、代わりにアプリケーショングループにアプリケーションを追加します。このガイダンスにより、管理が容易になります。アプリケーションは常に少なくとも1つのデリバリーグループまたはアプリケーショングループに属している必要があります。

アプリケーションの追加ウィザードでは、1つ以上のデリバリーグループ、または1つ以上のアプリケーショングループを選択できますが、両方を選択することはできません。後でアプリケーションのグループ関連付けを変更できますが（たとえば、アプリケーションをアプリケーショングループからデリバリーグループに移動するなど）、ベストプラクティスとしては、そのような複雑さを追加することは推奨されません。アプリケーションは1種類のグループに保持してください。

アプリケーションを複数のグループに関連付けると、それらのすべてのグループでアプリケーションを表示する十分な権限がない場合、可視性の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが関連付けられているすべてのグループを含むようにスコープを拡張してください。

同じ名前の2つのアプリケーション（異なるグループからのものかもしれません）を同じユーザーに公開する場合、Web Studioで`Application name (for user)`プロパティを変更してください。そうしないと、ユーザーはCitrix Workspace™アプリで重複する名前を目にすることになります。

アプリケーションのプロパティ（設定）は、追加時または後で変更できます。アプリケーションが配置されているアプリケーションフォルダーも、アプリケーションの追加時または後で変更できます。

詳細については、以下を参照してください。

- デリバリーグループの作成
- アプリケーショングループの作成
- タグ

アプリケーションの追加

デリバリーグループまたはアプリケーショングループを作成する際に、アプリケーションを追加できます。これらの手順については、デリバリーグループの作成およびアプリケーショングループの作成で詳しく説明されています。次の手順では、グループ作成後にアプリケーションを追加する方法について説明します。

知っておくと良いこと:

- Remote PC Accessデリバリーグループにアプリケーションを追加することはできません。
- アプリケーションの追加ウィザードを使用して、デリバリーグループまたはアプリケーショングループからアプリケーションを削除することはできません。これは別の操作です。

1つ以上のアプリケーションを追加するには：

1. 左ペインで**アプリケーション**を選択し、アクションバーで**アプリケーションの追加**を選択します。
2. アプリケーションの追加ウィザードが**はじめに**ページとともに起動します。このページは、今後のウィザードの起動時に表示しないように設定できます。
3. ウィザードは、**グループ**、**アプリケーション**、**概要**の各ページを案内します。各ページの作業が完了したら、**概要**ページに到達するまで**次へ**をクリックします。

単一のデリバリーグループまたはアプリケーショングループにアプリケーションを追加する場合の、手順1の代替方法：

- **1つのデリバリーグループにのみアプリケーションを追加する場合：** 手順1で、Web Studioの左ペインで**デリバリーグループ**を選択し、中央ペインでデリバリーグループを選択してから、アクションバーで**アプリケーションの追加**を選択します。ウィザードには**グループ**ページは表示されません。
- **1つのアプリケーショングループにのみアプリケーションを追加する場合：** 手順1で、Web Studioの左ペインで**アプリケーション**を選択し、中央ペインでアプリケーショングループを選択してから、アクションバーのアプリケーショングループ名の下にある**アプリケーションの追加**エントリを選択します。ウィザードには**グループ**ページは表示されません。

グループページ

このページには、サイト内のすべてのデリバリーグループが表示されます。アプリケーショングループも作成している場合は、アプリケーショングループとデリバリーグループが一覧表示されます。どちらかのグループを選択できますが、両方のグループを同時に選択することはできません。つまり、アプリケーショングループとデリバリーグループに同時にアプリケーションを追加するこ

とはできません。通常、アプリケーショングループを使用している場合は、デリバリーグループではなくアプリケーショングループにアプリケーションを追加します。

アプリケーションを追加するときは、少なくとも1つのデリバリーグループ（または、利用可能な場合はアプリケーショングループ）の横にあるチェックボックスをオンにします。すべてのアプリケーションは、常に少なくとも1つのグループに関連付けられている必要があります。

アプリケーションページ

アプリケーションソースを表示するには、**追加**をクリックします。

- **スタートメニューから:** 選択したデリバリーグループ内のマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスを選択し、**OK**をクリックします。

  このソースは、(1)関連付けられたデリバリーグループがないアプリケーショングループを選択した場合、(2)関連付けられたデリバリーグループにマシンが含まれていないアプリケーショングループを選択した場合、または(3)マシンが含まれていないデリバリーグループを選択した場合は、選択できません。
- **手動:** デリバリーグループ内のVDAまたはネットワーク上の他の場所にあるアプリケーション。このソースを選択すると、新しいページが開き、次の方法で追加するアプリケーションを指定できます。
  - 実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、および管理者とユーザーの表示名を入力します。
  - デリバリーグループ内のVDAからアプリケーションを選択します。これを行うには、**参照**をクリックし、VDAにアクセスするための資格情報を入力し、VDAへの接続を待ってから、VDAからアプリケーションを選択します。選択したアプリケーションのプロパティが、ページのフィールドに自動的に入力されます。
- **既存:** 以前にサイトに追加されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスを選択し、**OK**をクリックします。

  サイトにアプリケーションがない場合、このソースは選択できません。
- **アプリケーションパッケージ:** App-V、MSIX、MSIX app attach、またはFlexAppアプリケーションパッケージ内のアプリケーション。このソースを選択すると、**パッケージからのアプリケーションの追加**ページが起動します。アプリケーションパッケージのソースを選択し、表示

された結果から追加するアプリケーションを選択し、**OK**を選択します。詳細については、「アプリパッケージの展開と配信」を参照してください。

- **アプリケーショングループ**: アプリケーショングループ。このソースを選択すると、アプリケーショングループのリストが表示された新しいページが起動します。（表示には各グループのアプリケーションもリストされますが、個々のアプリケーションではなくグループのみを選択できます。）選択したグループ内の現在および将来のすべてのアプリケーションが追加されます。追加するアプリケーショングループのチェックボックスを選択し、**OK**をクリックします。

  このソースは、(1)アプリケーショングループがない場合、または(2)選択したデリバリーグループがアプリケーショングループをサポートしていない場合（たとえば、静的に割り当てられたマシンを持つデリバリーグループなど）は、選択できません。

表に示されているように、**追加**リストの一部のソースは、そのタイプの有効なソースがない場合は選択できません。互換性のないソース（たとえば、アプリケーショングループにアプリケーショングループを追加できないなど）はリストに含まれません。選択したグループに既に追加されているアプリケーションは選択できません。

このページまたは後で、アプリケーションのプロパティ（設定）を変更できます。

デフォルトでは、追加されたアプリケーションは`Applications`という名前のアプリケーションフォルダーに配置されます。このページまたは後でアプリケーションを変更できます。アプリケーションを追加しようとしたときに、同じ名前のアプリケーションが同じフォルダーに存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。提示された新しい名前を受け入れるか、拒否してアプリケーションの名前を変更するか、別のフォルダーを選択できます。たとえば、**Applications**フォルダーに`app`が既に存在し、そのフォルダーに`app`という名前の別のアプリケーションを追加しようとすると、新しい名前`app_1`が提示されます。

概要ページ

追加するアプリケーションが10個以下の場合は、その名前が**追加するアプリケーション**にリストされます。10個を超えるアプリケーションを追加する場合は、合計数が指定されます。

概要情報を確認し、**「完了」**をクリックします。

アプリケーションのグループ関連付けを変更する

アプリケーションを追加した後、そのアプリケーションが関連付けられているデリバリーグループとアプリケーショングループを変更できます。

アプリケーションを別のグループにドラッグできます。これは、アクションバーのコマンドを使用する代替手段です。

アプリケーションが複数のデリバリーグループに関連付けられている場合（アプリケーショングループを使用するか直接関連付けられているかに関わらず）、グループの優先順位を使用して、複数のグループが評価される順序を指定できます。グループは、アクセスポリシー、ユーザーリスト、スマートアクセスタグなどの要因に基づいて考慮対象から除外でき、グループから選択される特定のマシンは、ゾーン設定、起動準備状況、タグ制限などの要因によって影響を受ける可能性があります。デフォルトでは、すべてのグループの優先順位は0（最高）です。デリバリーグループの優先順位が同じ場合、アプリケーションの起動には最も負荷の低いデリバリーグループが選択されます。この場合、垂直ロードバランシングは考慮されません。

アプリケーションは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。また、(1) デリバリーグループに共有マシンが含まれており、XenDesktop 7.x バージョン 7.9 より前に作成されたもので、(2) `Edit delivery group` 権限がある場合、デスクトップのみを配信する共有マシンを含むデリバリーグループを選択することもできます。プロパティダイアログがコミットされると、デリバリーグループの種類は自動的に `desktops and applications` に変換されます。

1. Web Studio にサインインし、左ペインで **アプリケーション** を選択し、アプリケーションを選択します。
2. アクションバーで **プロパティ** を選択します。
3. **グループ** ページを選択します。

    - グループを追加するには、**追加** をクリックし、**アプリケーショングループ** または **デリバリーグループ** を選択します。（アプリケーショングループを作成していない場合、唯一の項目は **デリバリーグループ** です。）次に、1つ以上の利用可能なグループを選択します。アプリケーションと互換性のないグループ、またはすでにアプリケーションに関連付けられているグループは選択できません。
    - グループを削除するには、1つ以上のグループを選択し、**削除** をクリックします。グループの関連付けを削除した結果、アプリケーションがどのグループにも関連付けられなくなる場合、アプリケーションが削除されることを警告されます。
    - グループの優先順位を変更するには、グループを選択し、**優先順位の編集** をクリックします。優先順位の値を選択し、**OK** をクリックします。

4. 完了したら、**適用** をクリックして変更を適用しウィンドウを開いたままにするか、**OK** をクリックして変更を適用しウィンドウを閉じます。

アプリケーションの複製、有効化または無効化、名前の変更、または削除

次のアクションが利用可能です。

- **複製:** アプリケーションを複製して、異なるパラメーターやプロパティを持つ別のバージョンを作成したい場合があります。アプリケーションを複製すると、一意のサフィックスで自動的に名前が変更され、元のアプリケーションの隣に配置されます。アプリケーションを複製してから、別のグループに追加したい場合もあります。(複製後、アプリケーションを移動する最も簡単な方法はドラッグすることです。)
- **有効化または無効化:** アプリケーションの有効化と無効化は、デリバリーグループまたはアプリケーショングループの有効化と無効化とは異なるアクションです。
- **名前の変更:** 一度に1つのアプリケーションのみ名前を変更できます。アプリケーションの名前を変更しようとして、同じ名前のアプリケーションが同じフォルダーまたはグループに存在する場合、別の名前を指定するように求められます。
- **削除:** アプリケーションを削除すると、関連付けられていたデリバリーグループおよびアプリケーショングループから削除されますが、元々アプリケーションを追加するために使用されたソースからは削除されません。アプリケーションの削除は、デリバリーグループまたはアプリケーショングループから削除するのとは異なるアクションです。

アプリケーションを複製、有効化、無効化、名前変更、または削除するには：

1. 左側のペインで を選択します。
2. 中央のペインで1つ以上のアプリケーションを選択し、アクションバーで適切なタスクを選択します。
3. プロンプトが表示されたら、アクションを確認します。

デリバリーグループからアプリケーションを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに関連付けられている（属している）必要があります。アプリケーションをデリバリーグループから削除しようとして、そのアプリケーションがどのデリバリーグループまたはアプリケーショングループとの関連付けも失うことになる場合、続行するとアプリケーションが削除されることが通知されます。そのような場合、そのアプリケーションを配信したい場合は、有効なソースから再度追加する必要があります。

1. 左側のペインで を選択します。
2. デリバリーグループを選択します。中央下部のペインで、 タブの削除するアプリケーションを選択します。

3. アクションバーから を選択します。
4. 削除を確認します。

アプリケーショングループからアプリケーションを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに属している必要があります。アプリケーションをアプリケーショングループから削除しようとした結果、そのアプリケーションがどのグループにも属さなくなる場合、続行するとアプリケーションが削除されることが通知されます。そのような場合、そのアプリケーションを配信したい場合は、有効なソースから再度追加する必要があります。

1. 左側のペインで、 を選択します。
2. 中央のペインでアプリケーショングループを選択し、1つまたは複数のアプリケーションを選択します。
3. アクションバーで を選択します。
4. 削除を確認します。

アプリケーションのプロパティを変更する

アプリケーションのプロパティは、一度に1つしか変更できません。

アプリケーションのプロパティを変更するには：

1. 左ペインで**アプリケーション**を選択します。
2. アプリケーションを選択し、アクションバーで**アプリケーションプロパティの編集**を選択します。
3. 変更したいプロパティを含むページを選択します。
4. 完了したら、**適用**をクリックして変更を適用し、ウィンドウを開いたままにするか、**OK**をクリックして変更を適用し、ウィンドウを閉じます。

以下の一覧では、ページが括弧内に示されています。

プロパティ	ページ
Citrix Workspaceアプリにアプリケーションが表示されるカテゴリ/フォルダー	配信
コマンドライン引数。公開アプリケーションにパラメータを渡すを参照	場所

プロパティ	ページ
アプリケーションが利用可能なデリバリーグループとアプリケーショングループ	グループ
説明	識別
ファイル名拡張子とファイルの種類関連付け: アプリケーションが自動的に開く拡張子	ファイルの種類関連付け
アイコン	配信
StoreFront™用キーワード	識別
制限。アプリケーション制限の構成を参照	配信
名前: ユーザーおよび管理者が参照する名前	識別
実行可能ファイルへのパス。「公開アプリケーションにパラメーターを渡す」を参照してください。	場所
ユーザーのデスクトップ上のショートカット: 有効または無効	配信
可視性: Citrix Workspaceアプリでアプリケーションを表示できるユーザーを制限します。非表示のアプリケーションでも起動できます。アプリケーションを使用不可かつ非表示にするには、別のグループに追加します。	可視性の制限
作業ディレクトリ	場所

アプリケーションの変更は、現在のアプリケーションユーザーがセッションからログオフするまで有効にならない場合があります。

アプリケーション制限を構成する

アプリケーションの使用状況を管理するために、アプリケーション制限を構成します。たとえば、アプリケーション制限を使用して、アプリケーションに同時にアクセスするユーザーの数を管理できます。同様に、アプリケーション制限は、リソースを大量に消費するアプリケーションの同時イ

ンスタンスの数を管理するために使用できます。この制限は、サーバーのパフォーマンスを維持し、サービスの劣化を防ぐのに役立ちます。

この機能は、Controllerによって仲介されるアプリケーション起動の数（Citrix Workspaceアプリや StoreFrontなどから）を制限するものであり、他の方法で起動できる実行中のアプリケーションの数を制限するものではありません。これは、アプリケーション制限が同時使用の管理において管理者を支援するものの、すべてのシナリオで強制力を持つわけではないことを意味します。たとえば、Controllerが停止モードの場合、アプリケーション制限は適用できません。

デフォルトでは、同時に実行できるアプリケーションインスタンスの数に制限はありません。アプリケーション制限の設定はいくつかあります。それらのいずれか、またはすべてを構成できます。

- デリバリーグループ内のすべてのユーザーによるアプリケーションの同時実行インスタンスの最大数。
- デリバリーグループ内のユーザーごとのアプリケーションインスタンス数。
- マシンごとのアプリケーションの同時実行インスタンスの最大数 (PowerShell のみ)。

制限が構成されている場合、ユーザーが構成された制限を超えるアプリケーションインスタンスを起動しようとすると、エラーメッセージが生成されます。複数の制限が構成されている場合、最初に到達した制限でエラーが報告されます。

アプリケーションの制限を使用する例：

- **同時インスタンス数の上限:** デリバリーグループで、アプリケーション `Alpha` の同時インスタンスの最大数を 15 に構成します。その後、そのデリバリーグループのユーザーは、そのアプリケーションの 15 個のインスタンスを同時に実行します。そのデリバリーグループのいずれかのユーザーが `Alpha` を起動しようとすると、エラーメッセージが生成されます。構成された同時アプリケーションインスタンスの制限 (15) を超えるため、`Alpha` は起動されません。
- **ユーザーごとのインスタンス数制限:** 別のデリバリーグループで、アプリケーション `Beta` のユーザーごとのインスタンス数オプションを有効にします。ユーザーの Tony はアプリケーション `Beta` を正常に起動します。その日の後半、そのアプリケーションが Tony のセッションでまだ実行されている間に、彼は `Beta` の別のインスタンスを起動しようとします。エラーメッセージが生成され、ユーザーごとのインスタンス数制限を超えるため、`Beta` は起動されません。
- **同時インスタンス数の上限とユーザーごとのインスタンス数制限:** 別のデリバリーグループで、同時インスタンスの最大数を 10 に構成し、アプリケーション `Delta` のユーザーごとのインスタンス数オプションを有効にします。その後、そのデリバリーグループの 10 人のユー

ザーがそれぞれ `Delta` のインスタンスを実行している場合、そのデリバリーグループの他のユーザーが `Delta` を起動しようとすると、エラーメッセージが表示されます。`Delta` は起動されません。現在の 10 人の `Delta` ユーザーのいずれかがそのアプリケーションの 2 番目のインスタンスを起動しようとすると、エラーメッセージが表示され、2 番目のインスタンスは起動されません。

- **マシンごとの同時インスタンス数の上限とタグ制限の使用:** アプリケーション `Charlie` には、特定のサーバーで同時に実行できるインスタンスの数を規定するライセンスとパフォーマンス要件があります。これらの要件は、サイト内のすべてのサーバーで同時に実行できるインスタンスの数も規定します。

  アプリケーションのインスタンス数/マシン制限は、サイト内のすべてのサーバー (特定のデリバリーグループ内のマシンだけでなく) に影響します。サイトに 3 台のサーバーがあるとします。アプリケーション `Charlie` の場合、マシンごとのアプリインスタンス制限を 2 に構成します。したがって、サイト全体でアプリケーション `Charlie` のインスタンスは 6 つまでしか起動できません。(これは、3 台のサーバーそれぞれで Charlie のインスタンスが 2 つという制限です。)

  アプリケーションの使用をデリバリーグループ内の特定のコンピューターのみに制限するには (サイト全体のすべてのコンピューターでのインスタンスを制限することに加えて)：

  - それらのマシンにタグ付け機能を使用します。
  - そのアプリケーションのマシンごとの最大インスタンス数を構成します。

Controller の仲介以外の方法でアプリケーションが起動され (たとえば、Controller が停止モードの場合など)、構成された制限を超過した場合、ユーザーは制限を超過しないように十分なインスタンスを閉じるまで、それ以上のインスタンスを起動できません。制限を超過したインスタンスは強制的にシャットダウンされません。ユーザーが閉じるまで、それらのインスタンスは継続して実行されます。

セッションローミングを無効にする場合は、ユーザーごとのアプリケーションインスタンス数制限を無効にしてください。ユーザーごとのアプリケーションインスタンス数制限を有効にする場合は、新しいデバイスで新しいセッションを許可する2つの値のいずれも構成しないでください。ローミングの詳細については、「セッション」を参照してください。

デリバリーグループごとの最大インスタンス数制限と、ユーザーごとのインスタンス数制限を構成するには：

1. 左ペインで**アプリケーション**を選択し、アプリケーションを選択します。
2. アクションバーで**アプリケーションプロパティの編集**を選択します。

3. **配信**ページで、次のいずれかのオプションを選択します。

    - **アプリケーションの無制限の使用を許可する**。同時に実行されるインスタンスの数に制限はありません。これがデフォルトです。
    - **アプリケーションの制限を設定する**。2種類の制限があります。いずれかまたは両方を指定します。

        - マシンごとに同時に実行できるインスタンスの最大数を指定します
        - ユーザーごとにアプリケーションのインスタンスを1つに制限する

4. **OK**をクリックして変更を適用しダイアログボックスを閉じるか、**適用**をクリックして変更を適用しダイアログボックスを開いたままにします。

マシンごとの最大インスタンス数制限を構成するには（PowerShellのみ）：

- PowerShellで（Citrix Cloud™展開の場合はRemote PowerShell SDKを、オンプレミス展開の場合はPowerShell SDKを使用して）、適切な`BrokerApplication`コマンドレットを`MaxPerMachineInstances`パラメーターとともに指定します。
- ガイダンスについては、`Get-Help`コマンドレットを使用してください。例：

    ```
    Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
    ```

公開アプリケーションにパラメーターを渡す

公開アプリケーションのコマンドラインを入力し、パラメーターを渡すには、アプリケーションのプロパティの**場所**ページを使用します。

公開アプリケーションをファイルの種類に関連付けると、`"%*"`（二重引用符で囲まれたパーセント記号とアスタリスク記号）がアプリケーションのコマンドラインの末尾に追加されます。これらの記号は、ユーザーデバイスに渡されるパラメーターのプレースホルダーとして機能します。

公開アプリケーションが期待どおりに起動しない場合は、そのコマンドラインに正しい記号が含まれていることを確認してください。デフォルトでは、`"%*"`記号が追加されると、ユーザーデバイスから提供されるパラメーターが検証されます。ユーザーデバイスから提供されるカスタマイズされたパラメーターを使用する公開アプリケーションの場合、コマンドライン検証をバイパスするために、`"%**"`記号がコマンドラインに追加されます。これらの記号がアプリケーションのコマンドラインに表示されない場合は、手動で追加してください。

実行可能ファイルへのパスにスペースを含むディレクトリ名（`"C:\Program Files"`など）が含まれている場合は、スペースがコマンドラインに属していることを示すために、アプリケーションのコマンドラインを二重引用符で囲みます。これを行うには、パスを二重引用符で囲み、`%*`記

号を別の二重引用符で囲みます。パスの閉じ引用符と`%*`記号の開始引用符の間にスペースを含めるようにしてください。

たとえば、公開アプリケーションであるWindows Media Playerのコマンドラインは次のとおりです。

```
"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"
```

> **注：**
>
> 公開アプリケーションを起動するためのコマンドラインの最大文字数（引数を含む）は203文字です。

公開アプリケーションでのセッションサインアウトの問題のトラブルシューティング

アプリケーションを公開する場合、公開アプリケーションのメイン実行可能ファイルのみが指定されます。しかし、一部のアプリケーションは、バックグラウンドで実行される追加の（子）プロセスを生成し、メインの公開アプリケーションが閉じられても、対応するメイン実行可能ファイルによって閉じられない場合があります。追加のプロセスは、実行されるスクリプトや、`Run`や`RunOnceKey`のような特定のレジストリキーからも作成されることがあります。これらのアプリケーションは、正常なサインアウトを妨げ、セッションが残存したりハングしたりする原因となり、セッションが閉じられず、ユーザーがサインアウトできない結果となる可能性があります。

この場合、Citrix Director を使用してこれらのセッションをリセットまたは終了する必要があります。

セッションが適切にサインアウトされない問題を特定し、トラブルシューティングするために、Citrix は3つのレジストリエントリを提供しています。これらの問題によりセッションが適切にログオフされないことの特定とトラブルシューティングは、次の3段階のプロセスです。

1. どのセッションが公開アプリケーションによって正常なサインアウトを妨げているかを特定する
2. それらの公開アプリケーションが追加の（子）プロセスを生成するかどうかを特定する
3. これらのプロセスを指定されたレジストリエントリに追加して、サインアウトを妨げないようにする

ステップ2：公開アプリケーションが追加の（子）プロセスを生成するかどうかを特定する

公開アプリケーションが正常なサインアウトを妨げていると特定されたら、次のステップは、このアプリケーションが実行時に追加のプロセスを生成するかどうかを判断することです。

公開アプリケーションが閉じられたときに、`HKCU\Software\CitrixVolatile\Seamless\Sessions\[ID]\LogoffCheckerBlockingProcess` を読んで、どのプロセスが正常なサインアウトをブロックしているかを判断できます。

以下の例では、キー `LogoffCheckerBlockingProcess` に次のエントリが含まれています。

```
PhoneExperienceHost.exe

SkypeApp.exe

SkypeBackgroundHost.exe
```

これらのプロセスが正常なサインアウトを妨げていました。

> **注:**
>
> 確認したいセッションの正しいセッションIDで を置き換えてください。

ステップ3：これらのプロセスを指定されたレジストリエントリに追加して、サインアウトを妨げないようにする

これらのプロセスを次のレジストリキーに追加して、将来のセッションでサインアウトを妨げないようにすることができます。

```
Add the process file name to the following registry key:

Caution! Refer to the Disclaimer at the end of this article before using
the Registry Editor.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

Value Name:LogoffCheckSysModules
```

```
Type:REG_SZ

String:MyAppName.exe
```

`LogoffCheckSysModules` の詳細については、公開アプリケーションからの正常なログオフによりセッションがアクティブ状態になる を参照してください。

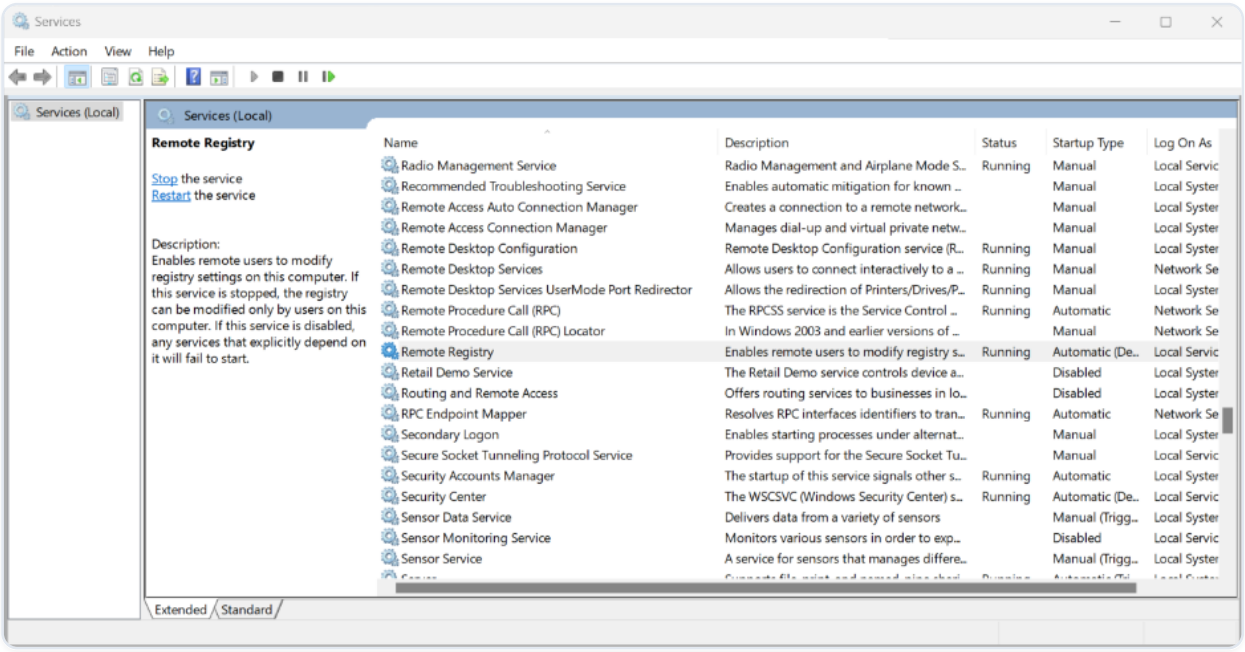
ステップバイステップのトラブルシューティングガイド

1. テスト対象のVDAでリモートレジストリサービスを開始します。

   a. コントロールパネルで、**管理ツール > サービス** を選択します。

   b. **リモートレジストリサービス** を右クリックし、**プロパティ** を選択します。

   c. **スタートアップの種類** で、ドロップダウンメニューから **自動** を選択します。



2. テスト対象のVDAでWindowsファイアウォールをオフにするか、ポート455を有効にする受信ファイアウォール規則を作成します:

   a. コントロールパネルで、**Windows Defender ファイアウォール > 詳細設定**を選択します。

   b. **受信の規則**を右クリックし、**新しい規則**を選択します。

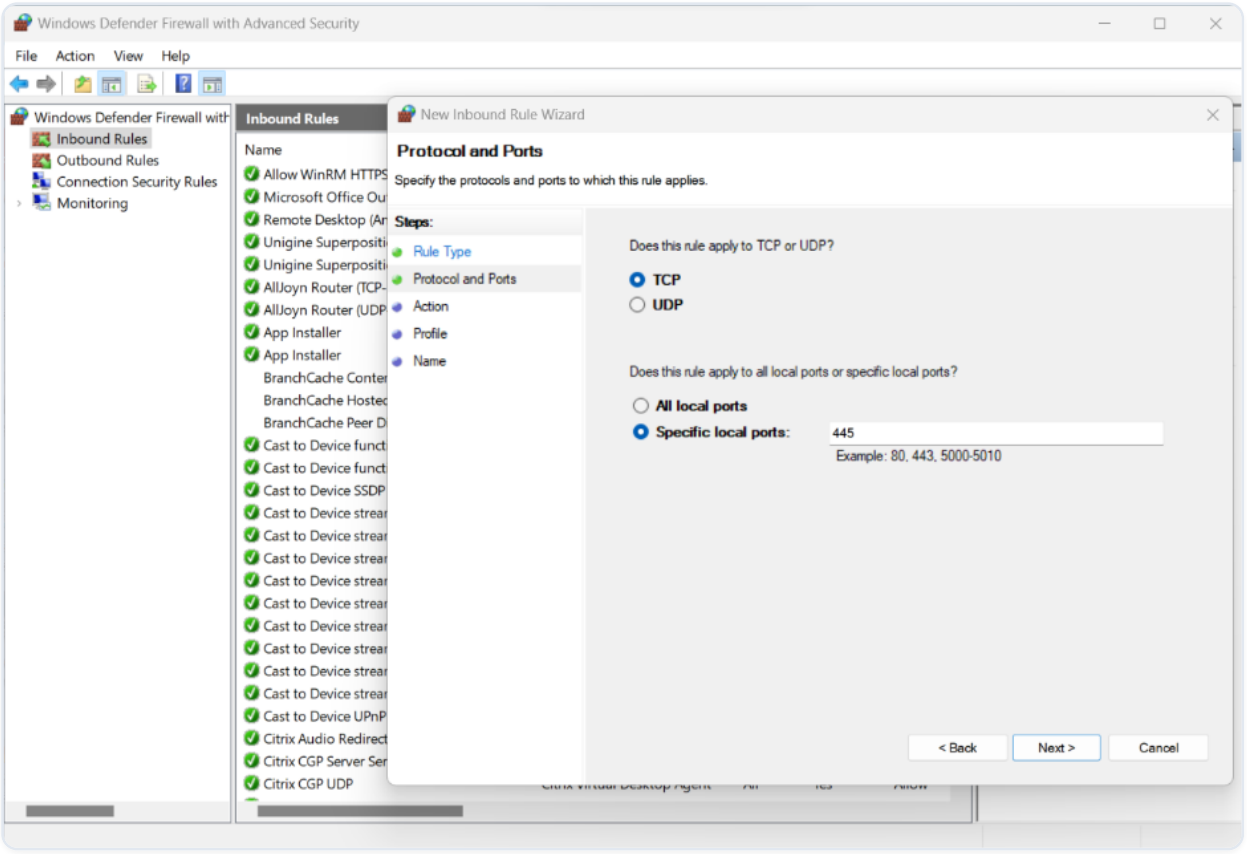
   c. **新しい受信の規則ウィザード**で、**ポート**を選択します。

   d. **プロトコルおよびポート**ページで、**TCP および特定のローカルポート**を選択します。ローカルポートとして `445` を入力します。

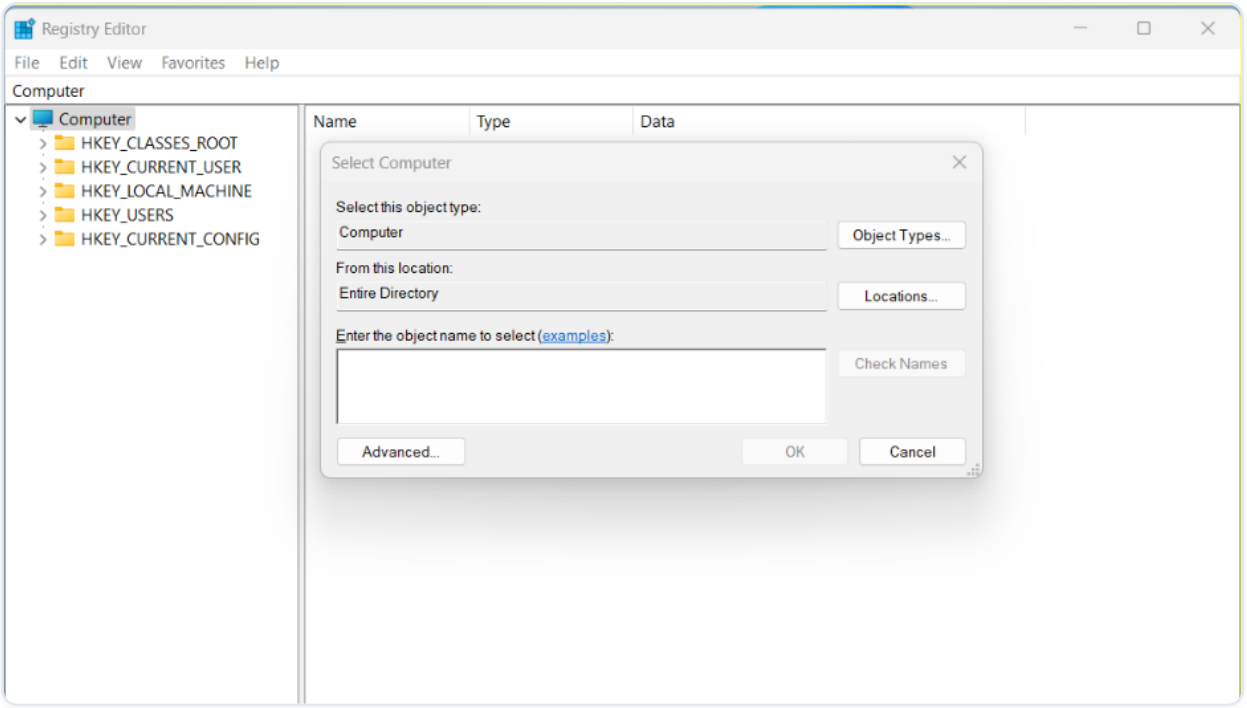
   e. **操作**ページで**接続を許可する**を選択します。

f. 新しい受信規則を適用するファイアウォールプロファイルを選択します。

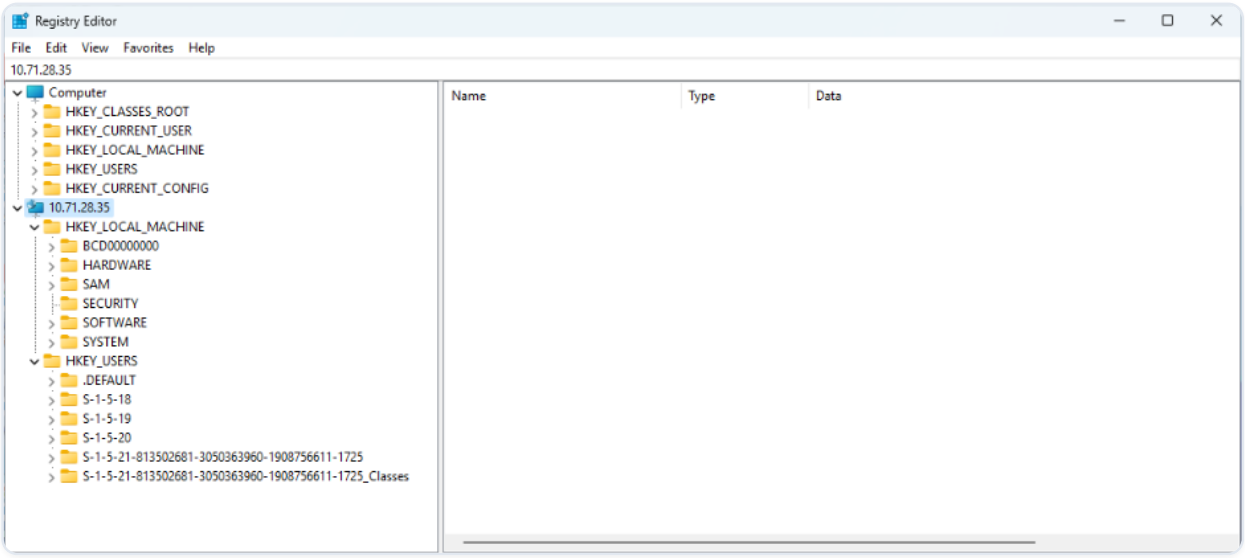
g. ファイアウォール規則に名前を付け、**完了**を選択して**新しい受信の規則ウィザード**を終了します。



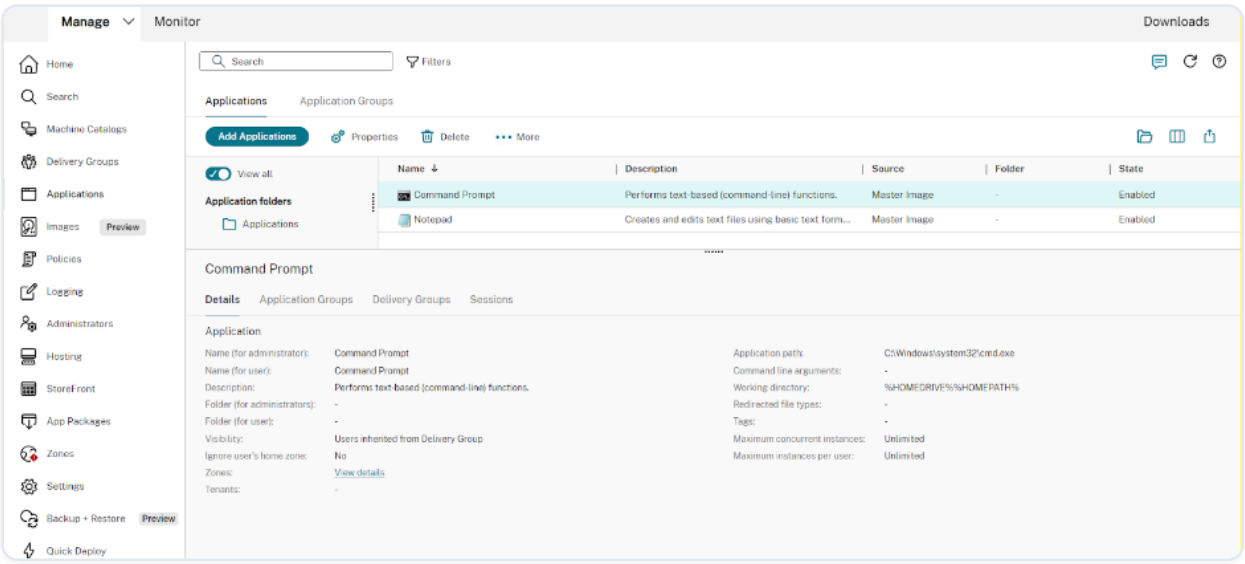
3. 同じドメイン上の別のVM（DC、DDC、または別のVDAでも可）から、`Regedit`を実行し、リモートレジストリに接続します。



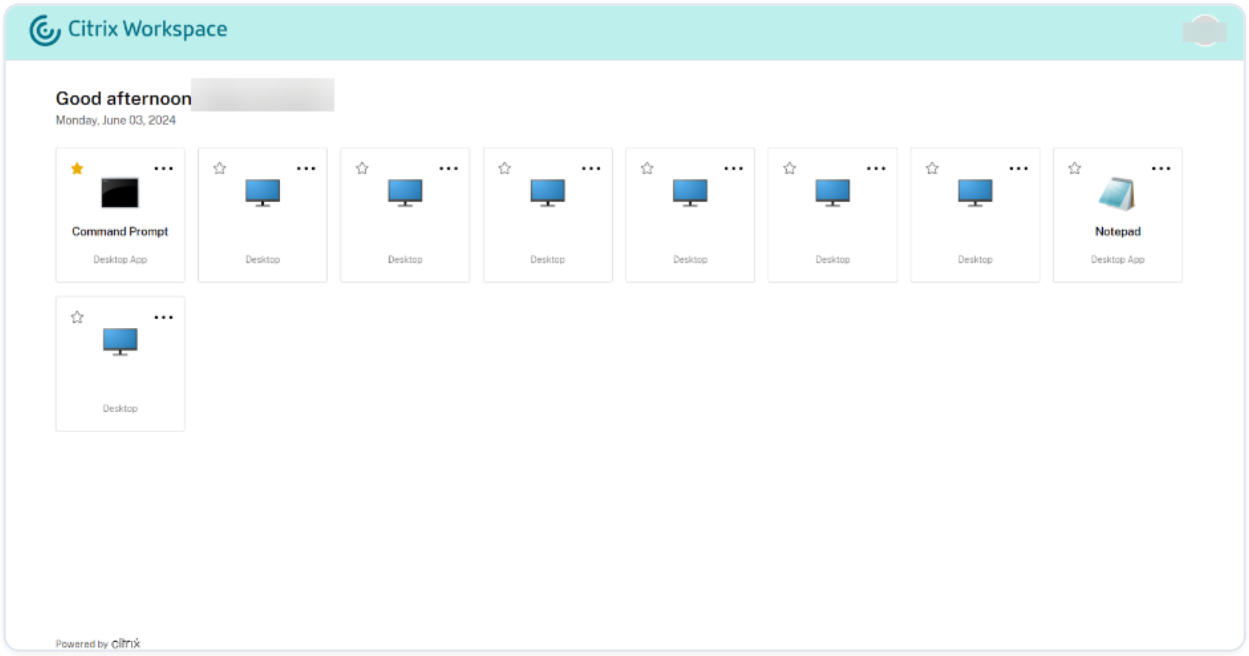
4. テスト対象のVDAのIPアドレスを入力し、**OK**をクリックします。`regedit` ツリーには、テスト対象のVDAのブランチが表示されるはずです。



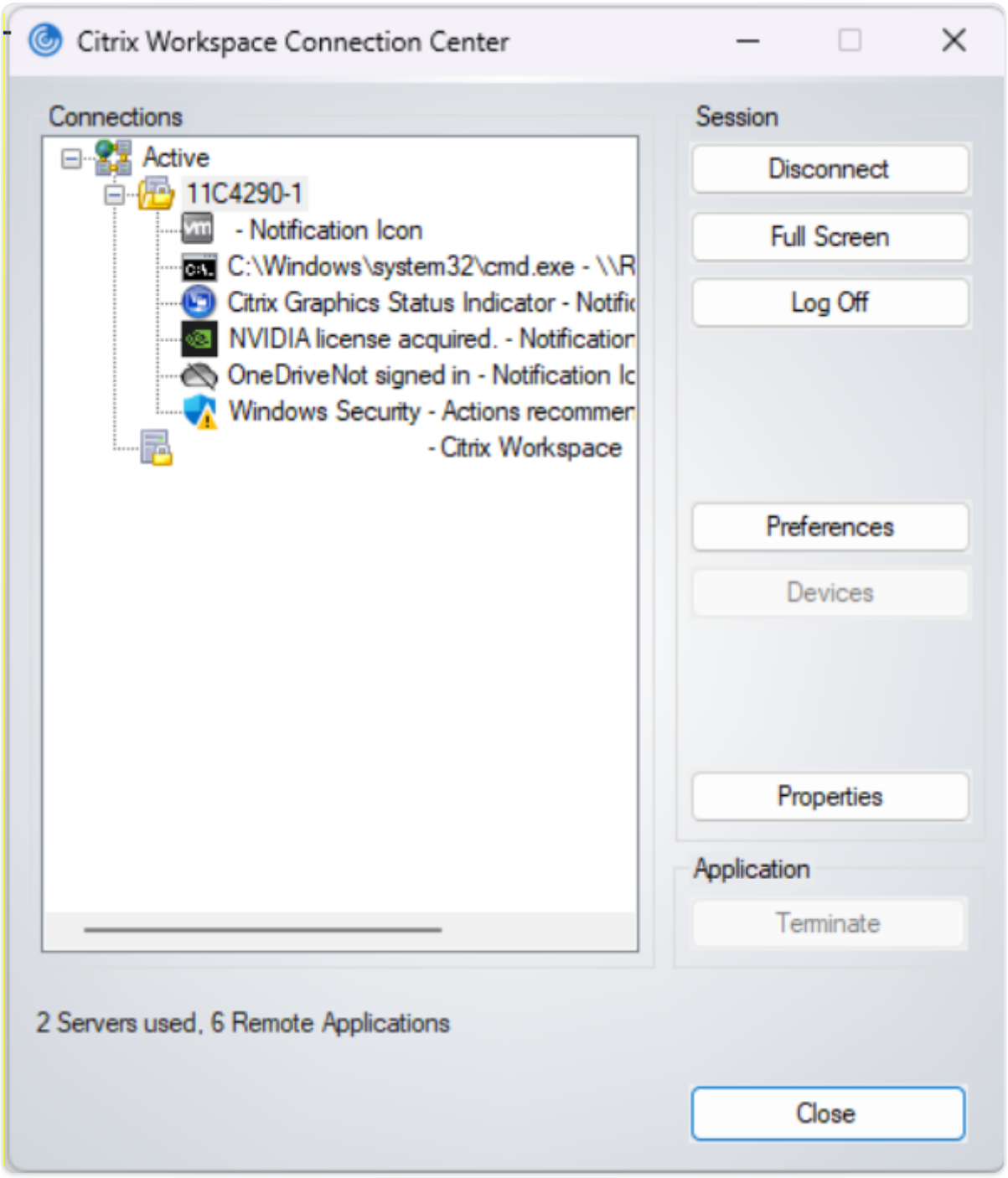
5. **コマンドプロンプト**公開アプリケーションを開きます。



Citrix Workspace に **コマンドプロンプト** アプリが表示されます。



6. クライアントで**接続センター**を開きます。これは、開いているシームレスアプリを閉じた後、セッションがサインアウトされたときに監視するために使用されます。以下の画像で、コマンドプロンプトプロセス`c:\Windows\system32\cmd.exe`がリモートVDIでアクティブになっていることがわかります。



7. **regedit**が実行されているVDAから、次のリモートIPの場所に移動します。

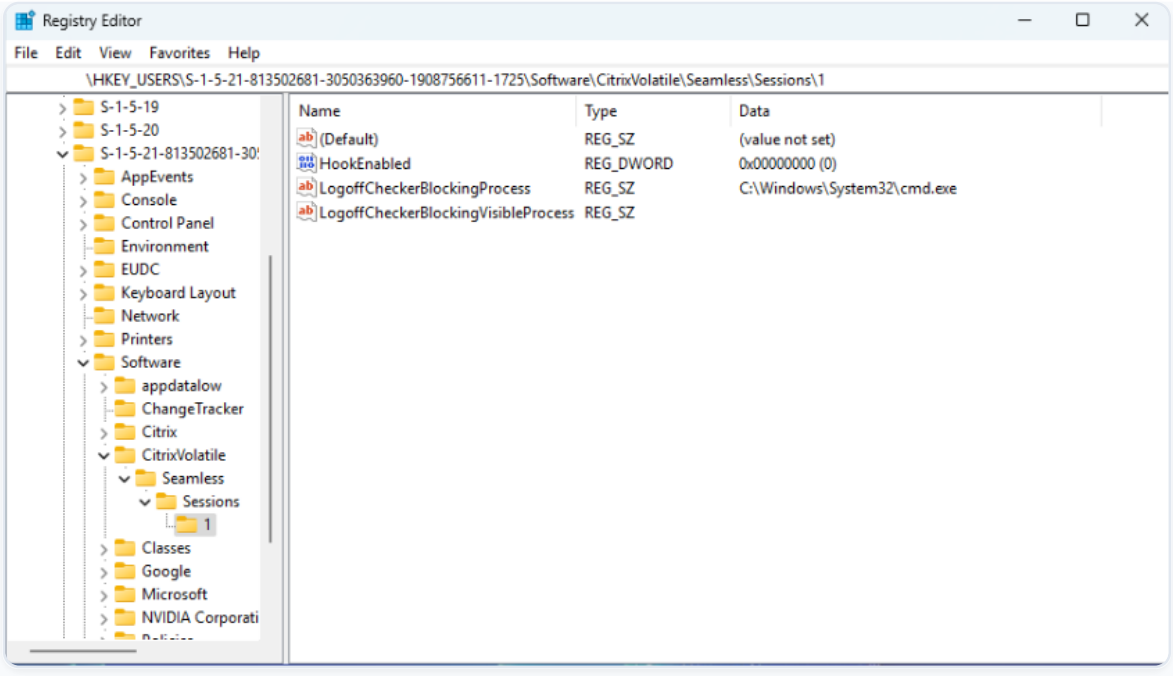
   `HKEY_USERS\S-1-X-XX-XXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXX\SOFTWARE\CitrixVolatile\Seamless\Sessions\X\`

   注：

   新しいセッションを開くたびにこのパスは変更されます。

8. ここで読み取るべきキーは2つあります（ここでは変更しないでください）：**LogoffCheckBlockingProcess**と**LogoffCheckerBlockingVisibleProcess**。これらのキーは、サインアウトをブロックしているプログラムを表示します。最初のキーは、まだ開いていて閉じられていないため、`C:\Windows\System32\cmd.exe`を表示するはずです。

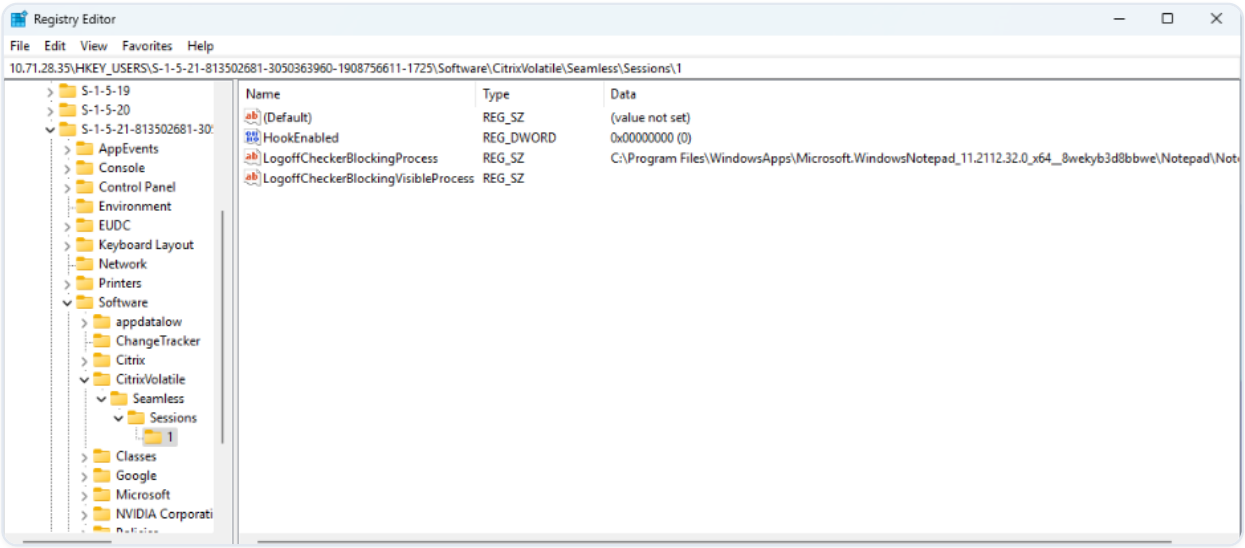
> **注：**
>
> **LogoffCheckBlockingProcess**と**LogoffCheckerBlockingVisibleProcess**は手動で編集してはいけません。これらのレジストリ値を手動で編集すると、セッションが不安定になる可能性があります。



9. 右上隅の **X** をクリックして **Seamless CMD** を終了します。
10. セッションが閉じるかどうか接続センターを確認します。閉じるまでに最大30秒かかる場合があります。閉じた場合、正常なサインアウトを妨げたアプリケーションやプロセスはありません。

    正常なサインアウト(/en-us/citrix-virtual-apps-desktops/2411/media/published-app-bwd.png)
11. セッションが閉じなかった場合は、F5 キーで **regedit** の出力を更新します。
12. **LogoffCheckBlockingProcess**と**LogoffCheckerBlockingVisibleProcess**の内容を再度確認します。CMDは存在しなくなっているはずですが、別のプロセスがリストされているはずです。現在セッションのサインアウトをブロックしているプロセスがここに表示されている必要があります。

このケースでは、コマンドプロンプトが閉じられる前に公開されたコマンドプロンプトから**Notepad.exe**が開かれており、このリモートのメモ帳プロセスが正常なサインアウトを妨げています。



13. この実行可能ファイルのパスと、それが表示されたキーをメモし、リモートツリーの下にある次のレジストリキーに入力します。

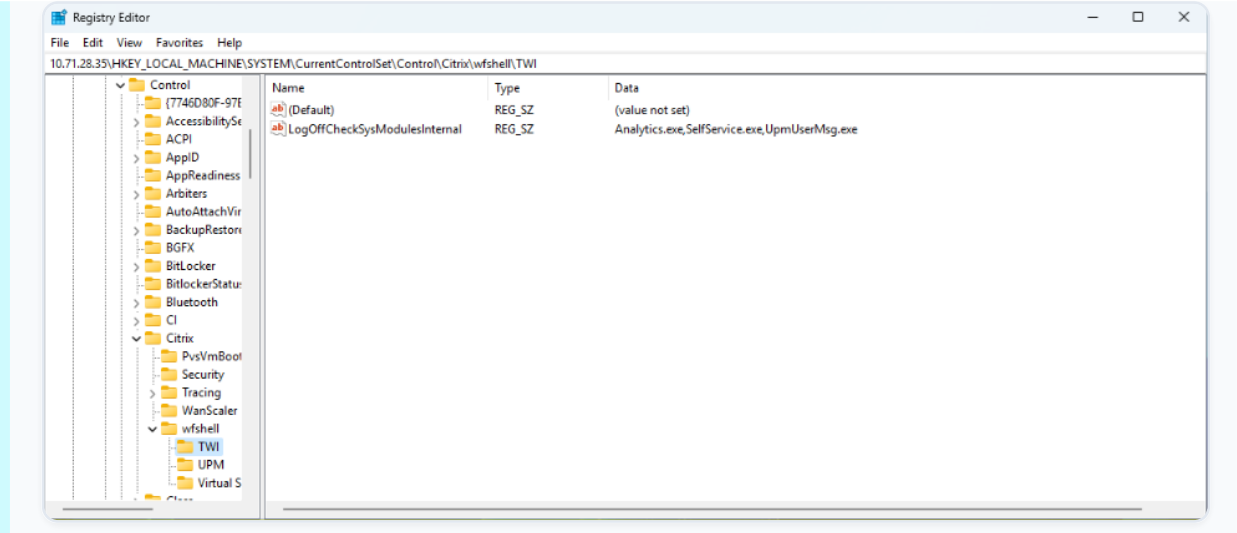
    - **LogoffCheckBlockingProcess** に表示される場合:

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckSysModulesInterna`

    - **LogoffCheckerBlockingVisibleProcess** に表示される場合:

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckVisibleSysModules`

> **注：**
>
> キーにすでに1つ以上のエントリがある場合は、末尾にコンマを追加し、そのコンマの後に新しいエントリを配置します。



14. クライアントの接続センターからセッションをサインアウトし、リモートアプリケーションを再度開きます。
15. リモートアプリケーションを閉じてから30秒以内にセッションが自動的にサインアウトされるまで、手順9〜16を繰り返します。

> **注：**
>
> トラブルシューティング後、必要に応じて、リモートレジストリへのアクセスを許可するための一時的なファイアウォールの変更を元に戻します。

公開アプリケーションを開くときにWindowsの免責事項メッセージを全画面表示で見るためにLogonUIを変更する方法

認証パススルーが発生しないシナリオ向けに、**LogonUI**ウィンドウのスケーリングが改善されました。**LogonUI**ウィンドウは、使用されているモニターの解像度とDPI設定に基づいてスケーリングされ、これにより、完全な**LogonUI**ウィンドウがクリッピングなしで表示されることが保証されます。

ウィンドウのサイズ（ピクセル単位）は、レジストリで手動で設定することもできます。

1. **ファイル名を指定して実行**コマンドで `regedit` を使用して**レジストリエディター**を開きます。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\` にアクセスします。
3. 2つの新しいDWORDキー、**LogonUIWidth** と **LogonUIHeight** を作成します。
4. **LogonUI** ウィンドウに必要な幅と高さ（ピクセル単位）にキーの値を設定します。

LogonUI ウィンドウのサイズを手動で設定すると、自動スケーリングは無効になります。

注:

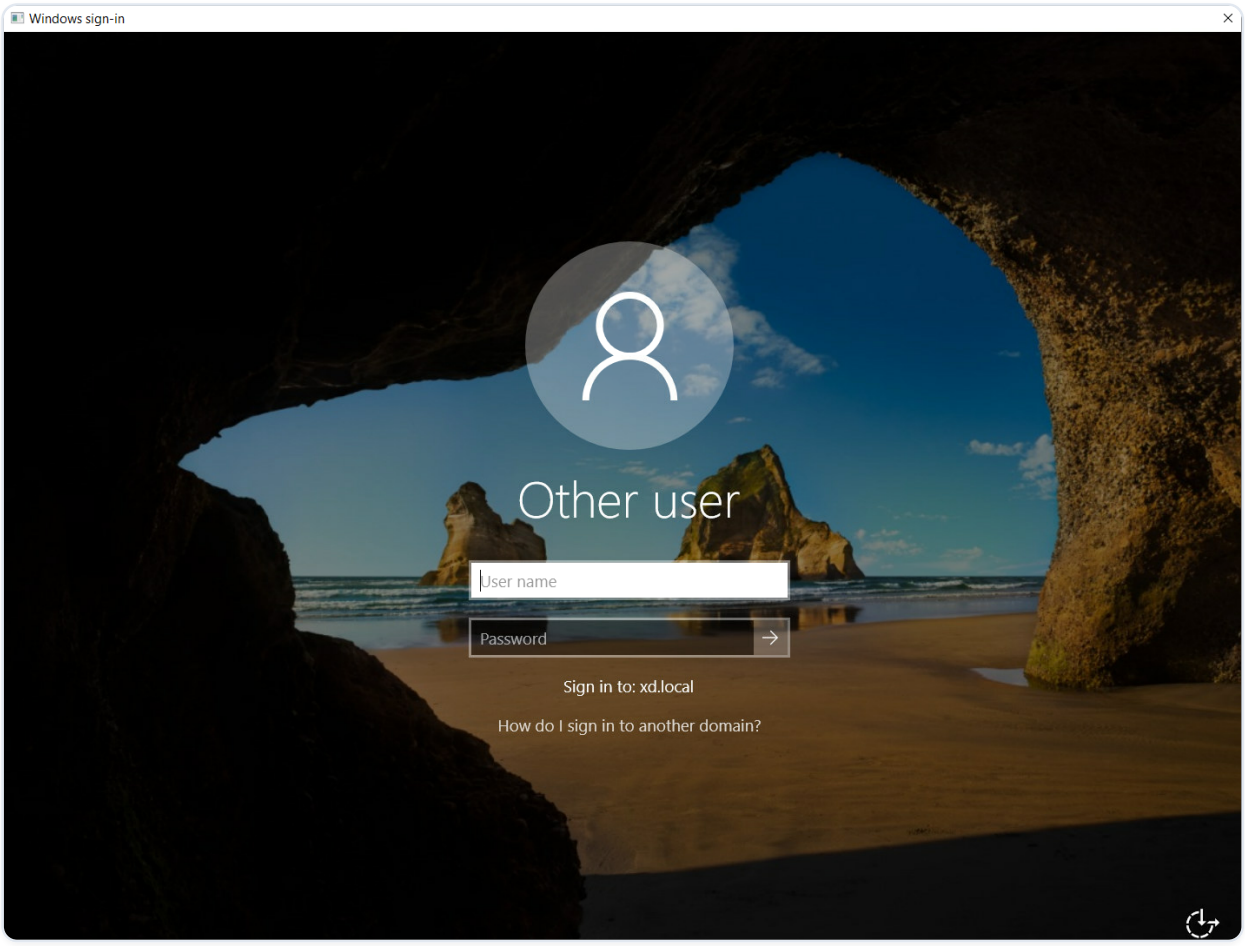
これらのレジストリパスは、2407以降で変更されました。古いレジストリ値は無視され、非推奨です。

デフォルトでは、**LogonUI** ウィンドウには閉じるボタン付きのタイトルバーが含まれており、必要に応じてエンドユーザーがセッションから切断できるようになっています。

タイルバーを無効にする

以下のレジストリキーを使用して、**LogonUI** ウィンドウのタイルバーを無効にできます。

1. **ファイル名を指定して実行** コマンドで `regedit` を使用してレジストリエディターを開きます。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\` にアクセスします。
3. 新しいDWORDキー **LogonUICaption** を作成し、キーの値を `0` に設定します。



アプリケーションフォルダーの管理

デフォルトでは、デリバリーグループに追加する新しいアプリケーションは、「**Applications**」という名前のフォルダーに配置されます。デリバリーグループの作成時、アプリケーションの追加時、または後で別のフォルダーを指定できます。

知っておくと良いこと：

- Applicationsフォルダーの名前を変更したり削除したりすることはできませんが、その中に含まれるすべてのアプリケーションを、作成した他のフォルダーに移動することはできます。
- フォルダー名には1～64文字を含めることができます。スペースも使用できます。
- フォルダーは最大5レベルまでネストできます。
- フォルダーにアプリケーションが含まれている必要はありません。空のフォルダーも許可されます。
- Web Studioでは、フォルダーを移動したり、作成時に別の場所を指定したりしない限り、フォルダーはアルファベット順に表示されます。
- 親フォルダーが異なる限り、同じ名前のフォルダーを複数持つことができます。同様に、異なるフォルダーにある限り、同じ名前のアプリケーションを複数持つことができます。

- フォルダー内のアプリケーションを表示するには`View Applications`権限が必要です。アプリケーションを含むフォルダーを削除、名前変更、または削除するには、そのフォルダー内のすべてのアプリケーションに対して`Edit Application Properties`権限が必要です。
- 以下の手順のほとんどは、Web Studioのアクションバーを使用したアクションを要求します。または、右クリックメニューを使用したり、項目をドラッグしたりすることもできます。たとえば、意図しない場所にフォルダーを作成または移動した場合、ドラッグアンドドロップで正しい場所に移動できます。
- Web Studioのすべてのノード（**Machine Catalogs**、**Delivery Groups**、**Applications**、**Application Groups**など）は、バックエンドで同じフォルダーツリーを共有します。フォルダーの名前変更や移動時に名前の競合を避けるため、異なるノード間で最上位フォルダーに一意の名前を使用してください。

  `New-BrokerAdminFolder` SDK コマンドレットを使用してフォルダーを作成し、それを**アプリケーション**ノードの下に表示させたい場合は、`Set-BrokerAdminFolderMetadata`コマンドレットを使用して`ContainsApplications`メタデータを追加する必要があります。

  例：

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsApplications -Value true
  ```

アプリケーションフォルダーを管理するには、左ペインで**［アプリケーション］**を選択します。以下のリストを参考にしてください。

- **すべてのフォルダーを表示するには（ネストされたフォルダーを除く）：**フォルダーリストの上にある**［すべて表示］**をクリックします。
- **最上位レベルにフォルダーを作成するには（ネストしない）：**［アプリケーション］**フォルダーを選択します。新しいフォルダーを**［アプリケーション］**以外の既存のフォルダーの下に配置するには、そのフォルダーを選択します。次に、アクションバーで**［フォルダーの作成］**を選択します。名前を入力します。
- **フォルダーを移動するには：**フォルダーを選択し、アクションバーで**［フォルダーの移動］**を選択します。フォルダーにネストされたフォルダーが含まれていない限り、一度に1つのフォルダーしか移動できません。（フォルダーを移動する最も簡単な方法は、ドラッグすることです。）
- **フォルダーの名前を変更するには：**フォルダーを選択し、アクションバーで**［フォルダー名の変更］**を選択します。名前を入力します。

- **フォルダーを削除するには：**フォルダーを選択し、アクションバーで**［フォルダーの削除］**を選択します。アプリケーションや他のフォルダーを含むフォルダーを削除すると、それらのオブジェクトも削除されます。アプリケーションを削除すると、デリバリーグループからのアプリケーションの割り当てが削除されます。マシンからは削除されません。
- **アプリケーションをフォルダーに移動するには：**1つまたは複数のアプリケーションを選択します。次に、アクションバーで**［アプリケーションの移動］**を選択します。フォルダーを選択します。

デリバリーグループまたはアプリケーショングループを作成する際に、**［アプリケーション］ページで追加するアプリケーションをフォルダーに配置することもできます。デフォルトでは、追加されたアプリケーションは［アプリケーション］フォルダーに入ります。［変更］**をクリックしてフォルダーを選択または作成します。

公開デスクトップでのアプリケーションのローカル起動を制御する

ユーザーが公開デスクトップ内から公開アプリケーションを起動するときに、そのアプリケーションをデスクトップセッション内で起動するか、公開アプリケーションとして起動するかを制御できます。Citrix Workspaceアプリは、VDAのWindowsレジストリでアプリケーションのインストールパスを検索し、存在する場合はアプリケーションのローカルインスタンスを起動します。それ以外の場合は、アプリケーションのホストされたインスタンスが起動されます。VDAにインストールされていないアプリケーションを起動すると、ホストされたアプリケーションが起動されます。詳細については、「vPrefer起動」を参照してください。

PowerShell（Citrix Cloud展開ではRemote PowerShell SDK、オンプレミス展開ではPowerShell SDKを使用）で、このアクションを変更できます。

`New-Broker` Applicationまたは`Set-BrokerApplication`コマンドレットで、`LocalLaunchDisabled`オプションを使用します。例：

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

デフォルトでは、このオプションの値はfalse（`-LocalLaunchDisabled $false`）です。公開デスクトップ内から公開アプリケーションを起動すると、アプリケーションはそのデスクトップセッション内で起動されます。

オプションの値をtrue（`-LocalLaunchDisabled $true`）に設定すると、公開アプリケーションが起動されます。これにより、公開デスクトップから公開アプリケーションへの個別の追加セッションが（Windows用Citrix Workspaceアプリを使用して）作成されます。

要件と制限事項:

- アプリケーションの`ApplicationType`値は`HostedOnDesktop`である必要があります。
- このオプションは、適切なPowerShell SDKを介してのみ利用できます。現在、Web Studioのグラフィカルインターフェイスでは利用できません。
- このオプションには、StoreFront 3.14、Citrix Receiver for Windows 4.11、およびDelivery Controller 7.17が最低限必要です。

アプリパッケージ

注:

- Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。
- アプリパッケージの展開と配信にWeb StudioとCitrix Studioを相互に利用することはお勧めしません。それぞれ異なるメカニズムを使用しているため、App-Vサーバー情報が一方では正しく表示されるが、もう一方では表示されないといった不一致が生じる可能性があります。

ユーザーにアプリケーションを配信するためのパッケージングテクノロジーには、App-V、MSIX、MSIX app attach、FlexAppなどがあります。この記事では、Citrix Virtual Apps and Desktops環境でこれらのパッケージ化されたアプリケーションを展開および配信する方法について説明します。

- App-Vアプリケーションの展開と配信(#deploy-and-deliver-app-v-applications)
- MSIXおよびMSIX app attachアプリケーションの展開と配信(#deploy-and-deliver-msix-and-msix-app-attach-applications)
- FlexAppアプリケーションの展開と配信(#deploy-and-deliver-flexapp-applications)

App-Vアプリケーションの展開と配信

このセクションでは、次の情報について説明します。

- 概要(#overview)。App-Vパッケージを配信および管理するための管理方法について説明します。
- 手順(#procedures)。これらのパッケージを展開および配信するための手順を提供します。

概要

このセクションでは、App-Vパッケージを配信および管理するための管理方法について説明します。App-Vパッケージアプリケーションを配信する際に操作するコンポーネントと概念の詳細については、Microsoftのドキュメントを参照してください。`<https://docs.microsoft.com/ja-jp/windows/application-management/app-v/appv-for-windows>`。

App-Vパッケージを配信および管理するには、次の方法を使用できます:

- **Dual Admin**。アプリケーションパッケージはApp-Vサーバーで構成および管理されます。Citrix Virtual Apps and DesktopsとApp-Vサーバーが連携してパッケージを配信および管理します。

  この方法では、Citrix Virtual Apps and DesktopsがApp-Vサーバーの状態のスナップショットビューを定期的に更新する必要があります。これにより、ハードウェア、インフラストラクチャ、および管理のオーバーヘッドが発生します。Citrix Virtual Apps and DesktopsとApp-Vサーバーは、特にユーザー権限に関して同期を維持する必要があります。

  Dual Adminは、App-Vと環境が密接に連携している展開で最適に機能します。

  - **App-V管理サーバー**。App-Vパッケージと動的構成ファイルのライフサイクルを公開および管理します。
  - **VDAマシンにインストールされたCitrix Personalizationコンポーネント**。アプリケーションの起動に必要な適切なApp-V公開サーバーの登録を管理します。

  この方法により、App-V公開サーバーが適切なタイミングでユーザーと同期されます。公開サーバーは、ログオン時の更新や接続グループなど、パッケージライフサイクルの他の側面を維持します。
- **シングル管理**。アプリケーションパッケージはネットワーク共有に保存されます。Citrix Virtual Apps and Desktopsは、パッケージを独立して配信および管理します。

  この方法により、展開において App-V サーバーとデータベースインフラストラクチャが不要になるため、オーバーヘッドが削減されます。

  この方法では、App-Vパッケージをネットワーク共有に保存し、その場所からメタデータを環境にアップロードします。VDAマシンにインストールされたCitrix Personalizationコンポーネントは、次のようにアプリケーションを管理および配信します。

  - アプリケーションが起動されたときに、展開構成ファイルとユーザー構成ファイルを処理します。
  - ホストマシン上のパッケージのライフサイクルのすべての側面を管理します。

両方の管理方法を同時に使用できます。つまり、デリバリーグループにアプリケーションを追加する場合、アプリケーションはApp-Vサーバーまたはネットワーク共有に存在するApp-Vパッケージから取得できます。

> **注:**
>
> 両方の管理方法を同時に使用しており、App-Vパッケージが両方の場所に動的構成ファイルを持っている場合、App-Vサーバー上のファイル（デュアル管理）が使用されます。

手順

App-Vアプリケーションの配信をサポートするには、VDAマシンにCitrix Personalizationコンポーネントをインストールする必要があります。詳細については、「VDAマシンへのCitrix Personalizationコンポーネントのインストール」を参照してください。

App-V パッケージ化されたアプリケーションをユーザーに配信するには、次の手順に従います。

1. アプリケーションパッケージをネットワーク共有に保存する。
2. アプリケーションパッケージを環境にアップロードする。
3. デリバリーグループにアプリケーションを追加する。
4. 相互依存するApp-Vパッケージの自動配信を有効にするには、分離グループを作成する。

Citrix Virtual Apps and DesktopsでApp-V動的構成ファイルをシングル管理者方式で認識および適用させるには、このCitrixブログを参照してください。

MSIX および MSIX app attach アプリケーションの展開と配信

このセクションでは、次の情報について説明します。

- 概要。MSIXおよびMSIX app attachパッケージがどのように配信および管理されるかについて説明します。
- 手順。これらのパッケージを展開および配信するための手順を説明します。

概要

Citrix Virtual Apps and Desktopsは、VDAマシンにインストールされているCitrix Personalizationコンポーネントを介して、MSIXおよびMSIX app attachアプリケーションをユーザーに配信します。このコンポーネントは、ホストマシン上のパッケージのライフサイクルのすべての側面を管理します。

MSIX および MSIX app attach の詳細については、Microsoft ドキュメントの `<https://docs.microsoft.com/ja-jp/windows/msix/>` と `<https://docs.microsoft.com/ja-jp/azure/virtual-desktop/what-is-app-attach>` をそれぞれ参照してください。

手順

MSIXおよびMSIX app attachパッケージの配信をサポートするには、次の操作を行う必要があります。

- VDAマシンにCitrix Personalizationコンポーネントをインストールします。詳細については、「VDAマシンへのCitrix Personalizationコンポーネントのインストール」を参照してください。
- SQL Server 2019でサイドローディングを有効にします。

MSIXおよびMSIX app attachパッケージ化されたアプリケーションをユーザーに配信するには、次の手順に従います。

1. アプリケーションパッケージをネットワーク共有に保存する。
2. アプリケーションパッケージを環境にアップロードする。
3. デリバリーグループにアプリケーションを追加する。

FlexAppアプリケーションの展開と配信

このセクションでは、次の情報について説明します。

- 概要。Citrix DaaS™がFlexAppパッケージを配信および管理する方法について説明します。
- 手順。これらのパッケージを展開および配信するための手順を説明します。

概要

Citrix DaaSは、VDAマシンにインストールされているCitrix PersonalizationコンポーネントとFlexApp配信エージェントを介してFlexAppアプリケーションをユーザーに配信します。これら2つのコンポーネントは、ホストマシン上のパッケージのライフサイクルのすべての側面を管理します。

手順

FlexAppアプリケーションの配信をサポートするには、VDAマシンに次のコンポーネントをインストールする必要があります。

- VDAマシン上のCitrix Personalizationコンポーネント。詳細については、「VDAマシンへのCitrix Personalizationコンポーネントのインストール」を参照してください。

- VDA上のFlexApp Agent。詳細については、「FlexApp One Agentのインストール」を参照してください。

以下の手順に従って、FlexAppでパッケージ化されたアプリケーションをユーザーに配信します。

1. アプリケーションパッケージをネットワーク共有に保存する。
2. アプリケーションパッケージを環境にアップロードする。
3. デリバリーグループにアプリケーションを追加する。

FlexApp One Agent をインストールする

1. VDAで管理者コマンドプロンプトを起動します。
2. 任意のFlexApp Onepackageのネットワークパスを見つけます。
3. 次のコマンドを入力します: `\\path\to\any\FlexAppOnePackage.exe --install`
4. 表示されるプロンプトをすべて承認します。

VDAマシンにCitrix Personalizationコンポーネントをインストールする

Citrix Personalizationコンポーネントは、App-V、MSIX、MSIX app attach、およびFlexApp形式のアプリケーションパッケージの公開プロセスを管理します。このコンポーネントは、VDAをインストールする際にはデフォルトではインストールされません。VDAのインストール中またはインストール後にコンポーネントをインストールできます。

VDAのインストール中にコンポーネントをインストールするには、次のいずれかの方法を使用します。

- インストールウィザードで、**追加コンポーネント**ページに移動し、**Citrix Personalization for App-V - VDA**チェックボックスを選択します。
- コマンドラインインターフェイスで、**/includeadditional "Citrix Personalization for App-V – VDA"** オプションを使用します。

VDAのインストール後にコンポーネントをインストールするには、次の手順に従います。

1. VDAマシンで、**コントロールパネル > プログラム > プログラムと機能**に移動し、**Citrix Virtual Delivery Agent**を右クリックして、**変更**を選択します。
2. 表示されるウィザードで、**［追加コンポーネント］ページに進み、［Citrix Personalization for App-V - VDA］**チェックボックスを有効にします。

> **注:**

> Microsoft App-V Desktop Clientは、ユーザーデバイスでApp-Vパッケージから仮想アプリケーションを実行するコンポーネントです。Windows 10 (1607以降) および Windows Server 2019 には、このApp-Vクライアントソフトウェアがすでに含まれています。VDAマシンで有効にするだけで済みます。詳細については、このMicrosoftドキュメント記事を参照してください: `<https://docs.microsoft.com/ja-jp/windows/application-management/app-v/appv-enable-the-app-v-desktop-client>`。

アプリケーションパッケージをネットワーク共有に保存する

インフラストラクチャをセットアップしたら、アプリケーションパッケージを生成し、UNCまたはSMBネットワーク共有、あるいはAzureファイル共有などのネットワークロケーションに保存します。

詳細な手順は次のとおりです。

1. アプリケーションパッケージを生成します。詳細については、Microsoftのドキュメントを参照してください。
2. アプリケーションパッケージをネットワークロケーションに保存します。
   - **App-V Single Admin**の場合: パッケージと対応する動的構成ファイル (App-V) をUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
   - **App-V Dual Admin**の場合: UNCパスからApp-V管理サーバーにパッケージを公開します。(HTTP URLからの公開はサポートされていません。)
   - **MSIXまたはMSIX app attach**の場合: パッケージをUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
   - **FlexApp**の場合: パッケージをUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
3. VDAがパッケージストレージパスに対する読み取り権限を持っていることを確認してください。
   - パッケージをADドメイン内のUNCまたはSMBネットワーク共有に保存する場合、VDAマシンにストレージパスへの読み取り権限を付与します。これを行うには、マシンのADアカウントに共有への読み取り権限を明示的に付与するか、その権限を持つADグループにアカウントを含めます。
   - パッケージをAzureファイル共有に保存する場合、まずAzureのストレージパスに対するユーザーアカウントの読み取り権限を付与します。次に、VDAマシンで実行されている `ctxAppVService` がそのユーザーアカウントを使用してパッケージストレージパスにアク

セスするように構成します。詳細な手順については、次のセクションを参照してください。

ユーザーログオンアカウントの変更

VDAはパッケージストレージパスにアクセスするために`ctxAppVService`を呼び出します。デフォルトでは、`ctxAppVService`はマシンの**ローカルシステムアカウント**を使用してパッケージストレージパスにアクセスします。このタイプのマシン認証はADドメインでは機能します。ただし、ユーザーアカウントベースの認証が必要なADとAzure ADの統合シナリオでは機能しません。

パッケージをAzureファイル共有に保存する場合、`ctxAppVService`のログオンアカウントを、パッケージストレージパスに対する読み取り権限を持つユーザーアカウントに変更します。詳細な手順は次のとおりです。

1. **サービス**を開始し、**ctxAppVService**を右クリックし、**プロパティ**を選択します。
2. **［ログオン］タブで、［このアカウント］**を選択し、パッケージストレージパスへの読み取り権限を持つユーザーアカウントを入力し、ユーザーのパスワードを2回入力します。
3. **OK**をクリックします。

アプリケーションパッケージを環境にアップロードする

必要に応じてアプリケーションパッケージをネットワークの場所に保存した後、配信のために環境にアップロードします。必要に応じて、以下のいずれかの方法を使用します。

- 一括アップロード
- 1つずつアップロード

準備

Citrix Virtual Apps and Desktopsは、パッケージ検出のためにネットワークの場所への接続を設定するためにVDAマシンを使用します。したがって、事前にデリバリーグループを作成し、グループ内の少なくとも1つのVDAが次の要件を満たしていることを確認してください。

- VDAバージョン:
  - App-Vパッケージを検出する場合: 2203以降
  - MSIXおよびMSIXアプリ添付パッケージを検出する場合: 2209以降
  - FlexAppパッケージを検出するには: 2311以降
- Citrix Personalization for App-V コンポーネント: インストール済み
- パッケージの場所に対するアクセス許可: 読み取り (詳細については、「ステップ 2: アプリケーションパッケージをネットワーク共有に保存する」を参照してください。)

- 電源: オン
- 状態: 登録済み

アプリケーションパッケージを一括でアップロードする

ネットワーク上の場所にあるパッケージを環境にアップロードします。アップロードする前に、次の項目が準備されていることを確認してください。

- 準備の要件を満たすデリバリーグループ
- ネットワーク上の場所のパス

パッケージを一括でアップロードするには、次の手順に従います。

1. 左側のペインで、 を選択します。
2. タブで、 ボタンをクリックします。 ページが表示されます。
3. 「**名前**」フィールドに、パッケージソースのわかりやすい名前を入力します。
4. 「**デリバリーグループ**」フィールドで、「**デリバリーグループの選択**」をクリックします。次に、準備に記載されている要件を満たすデリバリーグループを選択し、「**OK**」をクリックします。
5. 「**場所の種類**」フィールドで、パッケージの保存場所に応じて、「**Microsoft App-Vサーバー**」または「**ネットワーク共有**」を選択し、対応する設定を完了します。
   - 「**Microsoft App-Vサーバー**」を選択した場合は、次の情報を入力します。
     - 管理サーバーのURL。例: `http://appv-server.example.com`
     - 管理サーバー管理者のログイン資格情報。
     - 公開サーバーのURLとポート番号。例: `http://appv-server.example.com:3330`
   - **ネットワーク共有**を選択した場合は、次の情報を指定します。
     - ネットワーク共有の UNC パスを入力します。例: `\\Package-Server\apps\`
     - アップロードするパッケージの種類を選択します。オプションには、App-V、MSIX、MSIX app attach、およびFlexAppが含まれます。
     - パッケージのサブフォルダーを検索するかどうかを指定します。
6. **ソースの追加**をクリックします。

   「ソースの追加」ページが閉じ、新しく追加されたソースがソースリストに表示されます。Citrix Virtual Apps and Desktopsは、デリバリーグループ内のVDAを使用してパッケージを環

境にアップロードします。アップロードが完了すると、「ステータス」フィールドに「*インポート成功*」と表示されます。対応するパッケージは「**パッケージ**」タブに表示されます。

> **注:**
>
> ソースの場所でパッケージの更新を確認し、環境にインポートするには、ソースリストで場所を選択し、「**パッケージの更新を確認**」をクリックします。

アプリケーションパッケージを1つずつアップロードする

ネットワーク共有から環境にアプリケーションパッケージをアップロードします。アップロードする前に、次の項目が準備されていることを確認してください。

- 準備に記載されている要件を満たすデリバリーグループ
- ネットワークロケーションパス。

パッケージを環境にアップロードするには、次の手順に従います。

1. 左側のペインで、**App Packages**を選択します。
2. **Packages**タブで、**Add Package**ボタンをクリックします。**Add Package**ページが表示されます。
3. **Delivery group**フィールドで、**Select a delivery group**をクリックします。次に、準備に記載されている要件を満たすデリバリーグループを選択し、**OK**をクリックします。
4. **Package full path**フィールドに、必要に応じてパスを入力します。
   - 複数のパッケージを一度にアップロードするには、それらのフルパスをセミコロンで区切って入力します (`;`)。例: `\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - ネットワーク共有にあるすべてのパッケージをアップロードするには、ストレージパスを入力します。例: \\package-Server\apps\
5. **Add Package**をクリックします。

   アプリケーションパッケージが「**パッケージ**」タブに表示されます。

デリバリーグループにアプリケーションを追加する

アプリケーションパッケージが環境に完全にアップロードされたら、必要に応じてそのアプリケーションを1つ以上のデリバリーグループに追加します。これにより、それらのデリバリーグループに関連付けられたユーザーはアプリケーションにアクセスできるようになります。

注:

- パッケージ化されたアプリケーションは、デリバリーグループを介してシングルセッションVDAおよびマルチセッションVDAに配信できます。
- デフォルトでは、エンドユーザーは、関連付けられているデリバリーグループに割り当てられたすべてのパッケージ化されたアプリケーションに、*シングルセッション*（または*デスクトップ*と呼ばれる）VDAを介してアクセスできます。*デスクトップ*VDA上のパッケージ化されたアプリケーションの可視性を特定のユーザーまたはグループに制限するには、**アプリケーション**ノードに移動し、アプリケーションを選択し、**アプリケーションプロパティの編集 > 可視性の制限**を選択して変更を加えます。

パッケージ内の1つ以上のアプリケーションを複数のデリバリーグループに追加するには、次の手順に従います。

1. 左側のペインで、**アプリパッケージ**を選択します。
2. **パッケージ**タブで、必要に応じてパッケージを選択します。
3. アクションバーで、**デリバリーグループの追加**をクリックします。アプリケーションをデリバリーグループに割り当てるページが表示されます。
4. 必要に応じてパッケージ内の1つまたは複数のアプリケーションを選択し、**次へ**をクリックします。
5. デリバリーグループのリストで、アプリケーションを割り当てるグループを選択し、**次へ**をクリックします。

   注:

   - MSIXまたはMSIXアプリ添付パッケージを選択した場合、機能レベルが2106以降のデリバリーグループのみがリストに表示されます。
   - *FlexApp* パッケージを選択した場合、機能レベルが2206以降のデリバリーグループのみがリストに表示されます。

6. **完了**をクリックします。

さまざまなパッケージのアプリケーションを複数のデリバリーグループに追加するには、次の手順に従います。

1. 左側のペインで、**アプリパッケージ**を選択します。
2. 「**アプリケーション**」タブで、「**アプリケーションの追加**」を選択します。
3. 「**グループ**」ページで、必要に応じて1つ以上のデリバリーグループを選択します。
4. 「**アプリケーション**」ページで、次のように、1つ以上のアプリケーションパッケージを選択します。
    a. 「**追加**」をクリックし、「**アプリケーションパッケージ**」を選択します。
    b. 必要なパッケージソースの種類 (例: App-V Single Admin) を選択します。この種類のすべてのパッケージが表示されます。
    c. 必要に応じて1つ以上のパッケージを選択します。
    d. 「**OK**」をクリックし、「**次へ**」をクリックします。
    e. 別のパッケージタイプのアプリケーションを追加するには、手順aからdを繰り返します。
5. 「**完了**」をクリックします。

次の場合に、パッケージ化されたアプリケーションをデリバリーグループに追加することもできます。

- デリバリーグループを作成する場合。詳細については、「デリバリーグループの作成」を参照してください。
- 既存のデリバリーグループまたはアプリケーショングループを編集する場合。詳細については、「アプリケーションの追加」を参照してください。

（オプション）App-Vパッケージの分離グループを作成する

相互依存するApp-Vパッケージを自動的に配信できるように、分離グループを作成できます。

> **注:**
>
> 隔離グループはApp-Vシングル管理者方式でサポートされています。App-Vデュアル管理者方式を使用している場合、Microsoft App-Vインフラストラクチャで*接続グループ*を作成することで同じ目標を達成できます。詳細については、このMicrosoftドキュメント記事を参照してください: `<https://docs.microsoft.com/ja-jp/windows/application-management/app-v/appv-connection-group-file>`。

隔離グループについて

隔離グループとは、仮想環境を作成するために同じWindows Sandbox内で実行する必要がある、相互依存するアプリケーションパッケージの集合です。Citrix App-Vの隔離グループは、App-Vの接続グループに似ていますが、同一ではありません。隔離グループには、次の2種類のパッケージが含まれます。

- **明示的**アプリケーションパッケージ。特定のライセンス要件を持つアプリケーション。これらのアプリケーションをデリバリーグループに追加することで、特定の範囲のユーザーに制限できます。
- **自動**アプリケーションパッケージ。デリバリーグループに追加されているかどうかに関係なく、常にすべてのユーザーが利用できるアプリケーション。

たとえば、アプリケーション`app-a`の実行にはJRE 1.7が必要です。app-a（*明示的*とマーク）とJRE 1.7（*自動*とマーク）を含む隔離グループを作成できます。次に、`app-a`のApp-Vパッケージを1つ以上のデリバリーグループに追加します。ユーザーがapp-aを起動すると、JRE 1.7が自動的に展開されます。

ユーザーが隔離グループ内で*明示的*とマークされたApp-Vアプリケーションを起動すると、Citrix Virtual Apps and Desktopsはデリバリーグループ内のアプリケーションに対するユーザーのアクセス許可を確認します。ユーザーがアプリケーションへのアクセス許可を持っている場合、同じ隔離グループ内の*自動*アプリケーションパッケージがユーザーに利用可能になります。

*自動*パッケージをどのデリバリーグループにも追加する必要はありません。隔離グループ内に別の*明示的*アプリケーションパッケージがある場合、そのパッケージは同じデリバリーグループ内にある場合にのみユーザーに利用可能になります。

隔離グループの詳細については、このCitrixブログを参照してください。

APP-V隔離グループを作成する

隔離グループを作成し、相互依存するアプリケーションパッケージを追加します。詳細な手順は次のとおりです。

1. **隔離グループ**タブで、**隔離グループの追加**をクリックします。
2. 隔離グループの名前と説明を入力します。環境内のすべてのアプリケーションパッケージが**利用可能なパッケージ**リストに表示されます。
3. **利用可能なパッケージ**リストから必要に応じてアプリケーションを選択し、右矢印をクリックします。選択したアプリケーションが**隔離グループ内のパッケージ**リストに表示されます。
4. **展開**フィールドで、アプリケーションに対して**明示的**または**自動**を選択します。
5. パッケージを追加するには、手順2〜3を繰り返します。

6. リスト内のパッケージの順序を調整するには、上矢印または下矢印をクリックします。
7. 「**保存**」をクリックします。

> **注:**
>
> 分離グループの構成により、VDA上にApp-V接続グループが作成されます。展開シナリオは複雑になる可能性があり、App-Vクライアントは一度に1つのアクティブな接続グループにのみ存在するパッケージをサポートします。同じパッケージを、同じデリバリーグループに追加された2つの異なる分離グループに追加しないことをお勧めします。

パッケージ化されたアプリケーションをシングルセッションまたは共有デスクトップVDAに公開する

App-V、MSIX、およびMSIXアプリのアタッチパッケージを、デリバリーグループを介してシングルセッションまたは共有デスクトップVDAセッションに直接配信できるようになりました。アプリケーションに設定されているアクセシビリティ権限に基づいて、サインイン時にデスクトップVDAでパッケージ化されたアプリケーションにアクセスできます。

利点

- サインイン時にVDAで利用可能で、WorkspaceまたはStoreFrontを介してオンデマンドでステージングされないアプリケーション。
- パッケージ化されたアプリケーションにアクセスする際の起動時間の改善。
- パッケージ化されたアプリケーションのメンテナンスを、VDAのベースイメージとは別に、独立して容易にします。

考慮事項

- このオプションは、適切なPowerShell SDKを介してのみシングルセッションVDAで利用できます。現在、Web Studioワークフローでは利用できません。共有デスクトップへの公開は、PowerShell SDKを使用するか、Web Studioワークフローを介した既存の方法で行うことができます。既存の手順の詳細については、「デリバリーグループへのアプリケーションの追加」を参照してください。
- アプリケーションはデリバリーグループの一部である必要があります。

始める前に

- パッケージ化されたアプリケーションが署名され、ファイル共有またはUNCの場所に利用可能であることを確認します。詳細については、「ネットワーク共有にアプリケーションパッケー

ジを保存する」(/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/applications-manage/app-packages.html#store-application-packages-on-network-shares)を参照してください。

- VDAマシンにCitrix Personalizationコンポーネントをインストールする。

手順

パッケージ化されたアプリケーションをデスクトップVDAに配信するには、次の手順に従います。

1. Web Studioにアプリケーションパッケージをインポートする。
2. パッケージ化されたBrokerApplicationを公開する。
3. Web Studioでのアプリケーションの可視性を制限する。

Web Studioにアプリケーションパッケージをインポートする

1. Webブラウザを開きます。`https://<address of the server hosting Web Studio>/Citrix/Studio`を入力します。
2. デリバリーグループを作成します。詳細については、「デリバリーグループを作成する」(/ja-jp/citrix-virtual-apps-desktops/2411/install-configure/delivery-groups-create)を参照してください。
3. アプリケーションパッケージをWeb Studioにインポートします。詳細については、「アプリケーションパッケージを一括アップロードする」(/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/applications-manage/app-packages#upload-application-packages-in-bulk)を参照してください。

BrokerApplicationでパッケージ化されたアプリケーションを公開する

マルチセッション（共有）VDAまたはシングルセッションアプリケーションVDAに公開する場合、公開手順は変更されません。詳細については、「デリバリーグループにアプリケーションを追加する」(/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/applications-manage/app-packages#add-applications-to-delivery-groups)を参照してください。 シングルセッションデスクトップVDAに公開する場合は、次の操作を行います。

Delivery Controller™上で、以下のPowerShellコマンドを実行します:

1. パッケージ内に存在するコマンドを取得するには：

```
Import-Module "D:
\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
```

> **注記：**
>
> この機能をサポートする`App-V package discovery module`のバージョンは、上記のパスにあるCitrix Virtual Apps and Desktops ISO（2311以降のバージョン）で確認できます。

2. 関連するデリバリーグループIDとパッケージ化されたアプリケーションIDを取得するには:

   `Get-BrokerDesktopGroup | Format-Table Uid, Name` `Get-AppLibAppVApplication | Format-Table Uid, Name`

3. パッケージを公開し、適切なBrokerMachineConfigurationを作成するには:

   `Publish-PackagedApplication -AppLibararyApplicationUid <AppLibararyApplication.Uid > -DesktopGroupUid <DesktopGroup.Uid>`

4. Broker構成を同期するには、これは後でVDA上のBrokerエージェントに送信されます:

   `Update-DesktopGroupMachineConfigurations -DesktopGroupUid <DesktopGroup.Uid>`

> **注記：**
>
> VDA からパッケージ化されたアプリケーションを公開または削除した後、PowerShell コマンド `Update-DesktopGroupMachineConfigurations` を実行してください。

Web Studio でのアプリケーションの可視性を制限する

デフォルトでは、ユーザーはVDAを提供するデリバリーグループに割り当てられているすべてのパッケージ化されたアプリケーションをデスクトップセッションで利用できます。Web Studioで特定のユーザーまたはグループに対してアプリケーションの可視性を設定することにより、デスクトップVDA上のパッケージ化されたアプリケーションの可視性を制御できます。パッケージ化されたアプリケーションの可視性を管理するには、「アプリケーションプロパティの変更」を参照してください。

ユニバーサル Windows プラットフォーム アプリ

ユニバーサル Windows プラットフォーム (UWP) アプリについては、以下の Microsoft ドキュメントを参照してください。

- ユニバーサル Windows プラットフォーム (UWP) アプリとは

- Windows パッケージ マネージャー

要件と制限事項

Citrix Virtual Apps and Desktops™ は、以下の Windows マシン上の VDA で UWP アプリを使用することをサポートしています。

- Windows 10 以降のバージョン
- Windows Server 2016 以降のバージョン

VDA はバージョン 7.11 以降である必要があります。

UWP アプリを使用する場合、以下の Citrix Virtual Apps and Desktops の機能はサポートされていないか、制限があります。

- ファイルの種類のアソシエーションはサポートされていません。
- ローカルアプリアクセスはサポートされていません。
- 動的プレビュー：セッションで実行中のアプリが重なっている場合、プレビューにはデフォルトのアイコンが表示されます。動的プレビューに使用される Win32 API は、UWP アプリではサポートされていません。
- アクションセンターのリモート処理：UWP アプリは、セッション内のメッセージを表示するためにアクションセンターを使用できます。これらのメッセージは現在、ユーザーに表示するためにエンドポイントにリダイレクトされません。

同じサーバーから UWP アプリと非 UWP アプリを起動することはサポートされていません。代わりに、UWP アプリと非 UWP アプリを別々のデリバリーグループまたはアプリケーショングループに配置してください。

マシンにインストールされているすべてのUWPアプリが列挙されるため、Citrix®はWindowsストアへのユーザーアクセスを無効にすることを推奨します。これにより、あるユーザーがインストールしたUWPアプリが別のユーザーによってアクセスされるのを防ぎます。

サイドローディング中、UWPアプリはマシンにインストールされ、他のユーザーが利用できるようになります。別のユーザーがアプリを起動すると、そのアプリがインストールされ、OSはそのユーザーによって「インストール済み」であることを示すようにAppXデータベースを更新します。

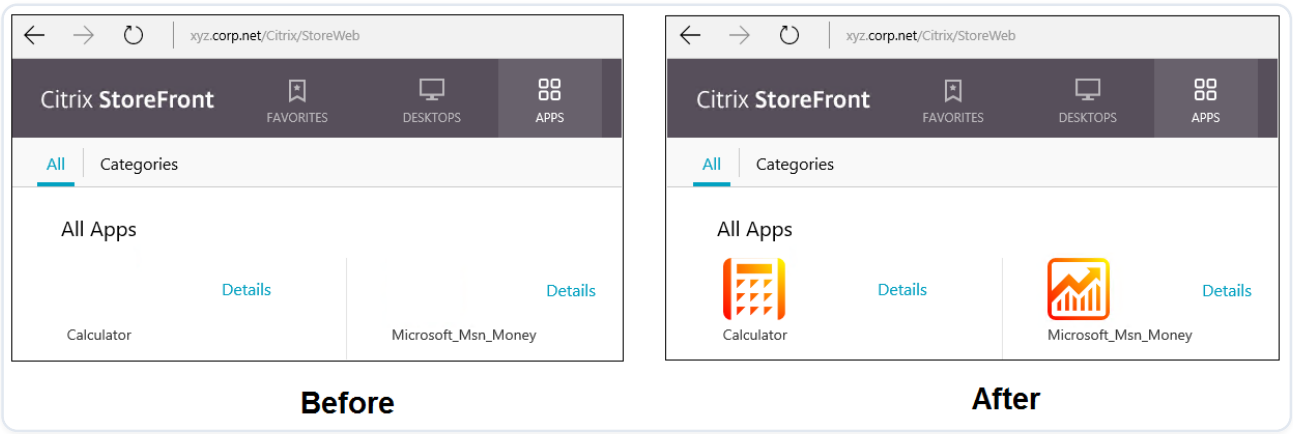
固定ウィンドウまたはシームレスウィンドウで起動された公開UWPアプリから開始された正常なログオフは、VDAセッションが閉じないようにし、ユーザーを強制的にログオフさせる可能性があります。この場合、VDAセッションに残っているいくつかのプロセスが、セッションが適切に閉じないようにします。これを解決するには、VDAセッションの終了を妨げているプロセスを特

定し、CTX891671のガイダンスに従って、「LogoffCheckSysModules」レジストリキー値に追加します。

UWPアプリのアプリケーション表示名と説明が正しくない場合があります。アプリケーションをデリバリーグループに追加する際に、これらのプロパティを編集して修正してください。

その他の問題については、既知の問題を確認してください。

現在、いくつかのUWPアプリは透明度が有効な白いアイコンを使用しており、StoreFront表示の白い背景に対してアイコンが見えなくなることがあります。この問題を回避するには、背景を変更できます。たとえば、StoreFrontマシンでファイル`C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`を編集します。ファイルの最後に`.storeapp-icon {background-image: radial-gradient( circle at top right, yellow, red ); }`を追加します。次の図は、この例の変更前と変更後を示しています。



Windows Server 2016以降のバージョンでは、UWPアプリの起動時にサーバーマネージャーも起動する場合があります。これを防ぐには、`HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon`レジストリキーを使用して、ログオン時にサーバーマネージャーが自動起動しないように無効にできます。詳細については、`<https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/>`を参照してください。

UWPアプリのインストールと公開

UWPアプリのサポートはデフォルトで有効になっています。

VDA（またはマスターイメージ）に1つ以上のUWPアプリをインストールするには、次のいずれかの方法を使用します。

- Windows Store for Businessからオフラインインストールを完了し、Deployment Image Servicing and Management (DISM) などのツールを使用してアプリをデスクトップイメージに展開します。詳細については、Windows Package Managerを参照してください。

- アプリをサイドロードします。詳細については、Windows クライアントデバイスで基幹業務 (LOB) アプリをサイドロードするを参照してください。
- 各対象ユーザー向けに、Windows Store for Businessから直接UWPアプリをインストールします。

Citrix Virtual AppsまたはCitrix Virtual Desktops™で1つ以上のUWPアプリを追加（公開）するには：

1. マシンにUWPアプリがインストールされたら、UWPアプリをデリバリーグループまたはアプリケーショングループに追加します。これは、グループの作成時または後で行うことができます。**アプリケーション**ページで、**追加**メニューから**スタートメニューから**を選択します。
2. アプリケーションリストが表示されたら、公開するUWPアプリを選択します。
3. ウィザードを続行するか、編集ダイアログを閉じます。

VDAでユニバーサルアプリの使用を無効にするには、`HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle`にレジストリ設定**EnableUWASeamlessSupport**を追加し、**0**に設定します。

UWPアプリのアンインストール

`Remove-AppXPackage`のようなコマンドでUWPアプリをアンインストールすると、その項目は管理者に対してのみアンインストールされます。アプリを起動して使用した可能性のあるユーザーのマシンからアプリを削除するには、各マシンで削除コマンドを実行します。1つのコマンドですべてのユーザーのマシンからAppXパッケージをアンインストールすることはできません。

構成のバックアップまたは移行

この機能は、構成のバックアップを取るのに役立ちます。バックアップは、復元機能と合わせて、オンプレミスからクラウドへ、またはあるクラウドサイトから別のクラウドサイトへのサイト情報の移行を容易にします。また、緊急時にはサイトの即時復旧も容易にします。

バックアップを取るには、以下の方法を使用できます。

1. バックアップ + 復元
    a. Web Studioと統合されています。
2. 自動構成ツール (ACT)
    a. PowerShellベースのツールです。使用するにはツールをインストールしてください。「自動構成のダウンロード」を参照してください。

バックアップは以下の目的で使用できます。

1. 復元
2. 移行

Citrix®は、説明されているシナリオに対して以下のツールを推奨します。

バックアップ

環境	ユースケース	推奨ツール	特記事項	リンク
DaaS およびオンプレミス	オンデマンドおよびスケジュールされたバックアップ	バックアップ + 復元	Citrix がバックアップを保持し、必要に応じてユーザーがダウンロードできます	Web Studio を使用したバックアップと復元
DaaS およびオンプレミス	オンデマンドおよびスケジュールされたバックアップ	ACT	ユーザーがバックアップを保持します	Automated Configuration Tool を使用したバックアップと復元

移行

環境	ユースケース	推奨ツール	特別な考慮事項	リンク
オンプレミスからクラウドへ	1つのオンプレミスサイトをDaaSに移行する	ACT		オンプレミスからクラウドへの移行
	複数のオンプレミスサイトを1つのDaaSサイトに統合する	ACT	サイトのマージ	複数のオンプレミスサイトを単一のクラウドサイトにマージする
オンプレミスからオンプレミスへ	1つのオンプレミスサイトを別のオンプレミス	ACT		POC ガイド:自動構成ツール - オンプレミスか

環境	ユースケース	推奨ツール	特別な考慮事項	リンク
	サイトに移行する			らオンプレミスへの移行
同上	複数のオンプレミスサイトを別のオンプレミスサイトに統合する	ACT	サイトのマージ	POC ガイド:自動構成ツール オンプレミスからオンプレミスへの移行
同上	同上	同上	同上	複数のオンプレミスサイトを単一のクラウドサイトにマージする
クラウドからクラウドへ	あるDaaSサイトを別のDaaSサイトに移行する	ACT		クラウドからクラウドへの移行
複数のDaaSサイトを1つのDaaSサイトに統合する	サイトのマージ	ACT		クラウドからクラウドへの移行 (/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/migrate-cloud-to-cloud.html)
				複数のオンプレミスサイトを単一のクラウドサイトに移行する (/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/multi-site-merge)

構成のバックアップと復元

この機能により、管理者はクラウド構成のバックアップを作成できます。これにより、Citrix®構成のコピーが常に利用可能になり、すぐに使用できるようになります。バックアップ機能と復元機能により、オンプレミスからクラウドへ、またはあるクラウドサイトから別のクラウドサイトへのサイト情報の移行が容易になります。誤って変更が発生した場合でも、バックアップを選択して復元を選択するだけで、数回のクリックで再び稼働状態に戻すことができます。特定のコンポーネントをバックアップおよび復元することもできます。

この機能では、以下をバックアップおよび復元できます。

- タグ
- 管理者ロール
- 管理スコープ
- ホスト接続

> **注:**
>
> ホスト接続をバックアップできるようになりました。シークレットは毎回入力する必要があります。インポートまたは更新されるホスト接続に対してのみシークレットを要求するために、インポート前チェックモードが実行されます。

- StoreFront™
- デリバリーグループ
- アプリケーショングループ
- アプリケーション
- AppV分離グループ
- AppLibパッケージ検出
- グループポリシー
- ユーザーゾーン設定
- 手動でプロビジョニングされた、またはPVSでプロビジョニングされたマシンカタログ
- 管理者フォルダー
  - アプリケーションフォルダー
  - デリバリーグループフォルダー

    - マシンカタログフォルダー
- サイト設定

> **重要:**
>
> - 異なるコンポーネントを復元するには、リストの順序に従ってください。例えば、アプリケーション、デリバリーグループ、グループポリシーを復元したい場合は、次の順序に従う必要があります。
>   - デリバリーグループ
>   - アプリケーション
>   - グループポリシー
> - MCS マシンカタログをバックアップまたは復元することはできません。

バックアップの種類

要件に応じてバックアップを実行するには、以下のオプションを使用します。

- **オンデマンド**: サイト構成をリアルタイムでバックアップします。この操作により、現在のCitrix Cloud™サイト構成がバックアップされます。
- **スケジュール済み**: スケジュールされた間隔でサイト構成をバックアップします。これは、指定された間隔で繰り返されます。

> **注:**
>
> フル権限を持つ管理者とクラウド管理者のみが、オンデマンドまたはスケジュールされたバックアップと復元を実行できます。

Web Studio を使用したバックアップと復元

この記事では、コンソールの左ペインにある**バックアップと復元**ノードで実行できる操作について説明します。

バックアップと復元を使用すると、管理者はWeb Studioからバックアップを作成できます。

ストレージの場所を設定する

バックアップを作成する前に、バックアップを保存するストレージの場所を設定する必要があります。

1. Web Studio から、**管理**をクリックします。
2. 左側のメニューから、**バックアップ+復元**を選択します。
3. **バックアップと復元**タブ内で、**ストレージのセットアップ**をクリックします。

   バックアップのストレージの場所を設定する (/en-us/citrix-virtual-apps-desktops/2411/media/first-time-backup-storage-1.png)
4. ドロップダウンリストから、**ストレージの種類** を選択します。ストレージの種類は、ファイルストレージまたはAzureストレージにすることができます。

   > **注:**
   >
   > - その場所は、すべてのDelivery Controllerからアクセスできる必要があります。
   > - フォルダーへのアクセスにユーザー名とパスワードが必要な場合は、企業のパスワードポリシーによってパスワードの有効期間が制限されないようにしてください。

5. 以下を選択します。
   - 最大バックアップ数
   - 最大ピン留めバックアップ
   - 最大自動ピン留めバックアップ
6. ストレージの場所を保存するには **保存** をクリックし、ストレージの場所を保存してバックアップを作成するには **保存してバックアップを作成** をクリックします。

ストレージの場所を設定したら、バックアップを作成できます。

オンデマンドバックアップの作成

1. Web Studio から、**管理** をクリックします。
2. 左側のメニューから、**バックアップと復元** を選択します。
3. ストレージの場所が設定されているがバックアップが存在しない場合は、バックアップを作成するように求められます。

初期バックアップの作成(/en-us/citrix-virtual-apps-desktops/2411/media/backup-after-storage-creation.png)

既存のバックアップがある場合は、**バックアップの作成** をクリックできます。

4. **バックアップの作成** ページで、メモを入力し、**バックアップの作成** をクリックします。

   バックアップをトリガーした管理者の名前でバックアップされているバックアップコンポーネントを示す概要アクティビティが表示されます。

5. バックアップが正常に完了すると、**バックアップと復元** タブの下に項目として表示されます。
6. 特定のバックアップを選択すると、**詳細** タブでそのバックアップに関する詳細情報が表示されます。
7. バックアップを削除するには、バックアップを右クリックして **バックアップの削除** をクリックします。

バックアップをピン留めする

Citrix® は最新の30個のバックアップを保存します。30個を超えるバックアップを作成すると、システムは作成された順序で古いバックアップを削除します。30個のバックアップ制限に加えて新しいバックアップが作成されるたびに、システムは最初に作成されたバックアップを削除します。バックアップのピン留めは、特定のバックアップが自動的に削除されるのを防ぐために使用されます。最大5個のバックアップをピン留めできます。ピン留めされたバックアップがある場合、30個のバックアップに加えてすべてのピン留めされたバックアップを保持します。つまり、最大で35個のバックアップ（ピン留めされていない30個とピン留めされた5個）を保持できます。

1. ピン留めするバックアップを右クリックします。

スケジュールされたバックアップを作成する

バックアップと復元プロセスを自動化するために、組織の要件に合わせたバックアップスケジュールを作成します。バックアップは、選択した頻度（毎日、毎週、毎月、またはその他の適切な頻度）でバックグラウンドで実行されます。

1. スケジュールタブに移動し、**「スケジュールを作成」**を選択します。
2. 「**スケジュールを作成**」ページで、以下を入力します。

   - **このスケジュールを有効にする**: このバックアップスケジュールを有効にするには、**「はい」**を選択します。
   - **名前**: バックアップスケジュールの名前を入力します。
   - **説明**: 説明を入力します。

- **タイムゾーン**: 任意のタイムゾーンを選択します。
- **頻度**: バックアップを実行する頻度を選択します。
- **繰り返し間隔**: スケジュールを繰り返す日数（間隔）を入力します。
- **開始日**: 開始日を入力します。
- **バックアップ開始時刻**: バックアップを開始する時刻を24時間形式で入力します。

3. **完了**を選択します。

スケジュールされたバックアップを制限する

同一のバックアップを避けるため、スケジュールされたバックアップを1日1回に制限できます。

1. **Backup and Restore**ノードの**Settings**タブに移動します。
2. **Scheduled backups**ボックスで「**変更**」をクリックします。
3. トグルを切り替えて、スケジュールされたバックアップを1日1回に制限する機能を有効にします。

スケジュールされたバックアップの自動ピン留め

スケジュールされたバックアップの自動ピン留めは、選択したスケジュールによって作成されたバックアップを自動的にピン留めします。自動ピン留めには、1つのスケジュールのみを選択できます。

スケジュールされたバックアップの自動ピン留めを使用すると、最大6つのスケジュールされたバックアップを保持できます。最大制限に達すると、最も古い自動ピン留めされたバックアップが削除されます。

> **注:**
>
> Citrixは最大6つの自動ピン留めされたバックアップを保存します。システムは、6番目のバックアップ以降に作成された古いバックアップを、作成された順序で削除します。6つのバックアップ制限に加えて新しく作成されるバックアップごとに、システムは最初に作成されたバックアップを削除します。

1. **バックアップと復元**ノードの**設定**タブに移動します。
2. 自動ピン留めするスケジュールされたバックアップを選択します。
3. トグルを切り替えて、自動ピン留めされたスケジュールを有効にします。

4. スケジュールを選択し、「**保存**」をクリックします。

バックアップストレージの編集

バックアップストレージ設定を編集して、ストレージの種類と場所、最大バックアップ数、最大ピン留めバックアップ数、および最大自動ピン留めバックアップ数を変更できます。

1. 「**バックアップと復元**」ノードの「**設定**」タブに移動します。
2. 「**ストレージ**」ボックスで「**変更**」をクリックします。
3. 「**バックアップストレージの編集**」ダイアログでストレージ設定を変更します。

復元

この機能により、管理者はバックアップからサイト構成を復元できます。一度に1つのコンポーネントのみを復元できます。

> **注:**
>
> - 一度に1つのコンポーネントのみを復元することで、コンポーネント間の依存関係による復元中の競合を防ぎます。
> - ホスト接続の復元ワークフローは、ホスト接続を復元しようとするたびにシークレットを入力する必要があるため、他のコンポーネントとは異なります。「**バックアップの復元**」をクリックすると、シークレットを入力するダイアログが表示されます。たとえば、Azureでは、接続の作成に使用した英数字のアプリケーションシークレットを入力します。

1. Web Studioから、「**管理**」をクリックします。
2. 左側のメニューから、「**バックアップと復元**」を選択します。
3. リストから特定のバックアップをクリックします。
4. 「**バックアップの復元**」をクリックします。
5. 「**バックアップの復元**」ウィンドウで、以下を入力します。
   - **コンポーネント**: 復元するコンポーネントを選択します。
   - **フィルター**: 復元するメンバー名をコンマ区切りのリストで指定します。たとえば、*chrome* という単語でフィルターすると、chrome という名前のオブジェクトのみが復元されます。同様に、`chr` というフレーズは、`chr` で始まるオブジェクトを復元します。

コンポーネントメンバーを表示するには、バックアップを選択し、「**詳細 > コンポーネント**」に移動します。コンポーネントを選択し、「**コンポーネントメンバーの表示**」をクリックします。

- **チェックモード**: 実際の復元操作が実行されたときに何を復元する必要があるかを確認するには、**はい**を選択します。このオプションは、実際に復元をトリガーすることなく、復元に必要なすべてを事前に評価します。たとえば、アプリケーションコンポーネントの復元プロセスが実行されたときに復元されるアプリケーションのリストが表示されます。

> **注:**
>
> チェックモードでは、実際の復元は実行されません。このオプションでは、コンポーネント間の依存関係もチェックされません。最適な結果を得るには、一度に1つのコンポーネントでチェックモードを使用することをお勧めします。

- **復元タイプ**: いずれかを選択します。
  - **不足しているもののみ**: この復元タイプを使用して、サイトにコンポーネントとメンバーを追加します。このオプションは、復元されるバックアップの構成が異なっていても、既存のコンポーネントとメンバーを変更しません。
  - **不足しているものと既存のものを更新**: この復元タイプを使用して、サイトにコンポーネントを追加および更新します。このオプションは、既存のコンポーネントとメンバーの構成が異なる場合、バックアップの構成でそれらを更新します。
- **メモ**: メモを入力します。

6. **復元**を選択します。

復元アクションが完了すると、復元結果が**復元**ウィンドウに表示されます。すべての復元アクションは、**履歴**タブに一覧表示されます。

履歴

履歴タブで、すべてのバックアップおよび復元アクションを追跡できます。

アクションの下に、削除されたすべてのバックアップとバックアップ履歴が表示されます。

バックアップの詳細を表示するには：

1. **履歴**タブに移動します。
2. バックアップアクションを選択し、**詳細の表示**をクリックします。

バックアップ結果には、次の詳細が表示されます。

- 期間
- 注
- 管理者名
- バックアップされたコンポーネント

「**履歴**」ページの右上にある検索バーを使用して、特定のバックアップを検索します。たとえば、特定の管理者によって実行されたバックアップや、特定の日に実行されたバックアップを検索できます。

自動構成ツールを使用したバックアップと復元

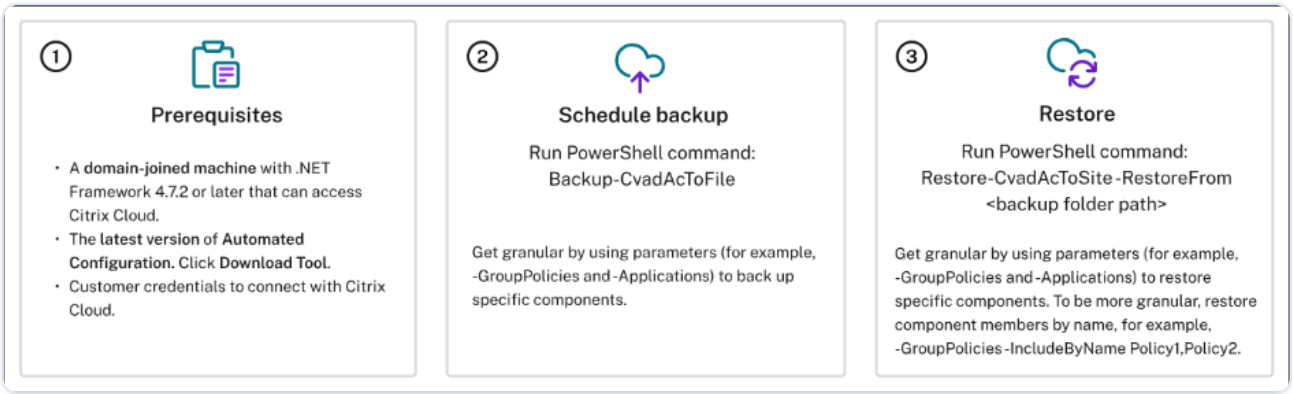
自動構成ツールを使用すると、次の環境でオンデマンドおよびスケジュールされたバックアップを実行できます。

- シトリックス バーチャル アプリ アンド デスクトップ™
- DaaS

自動構成ツールは、次の目的で使用できます。

- バックアップと復元（オンデマンドおよびスケジュールされたバックアップ）
- 移行（オンデマンドバックアップ）

移行用自動構成ツール



シトリックス バーチャル アプリ アンド デスクトップ

構成をバックアップするための前提条件

- Citrix Virtual Apps and Desktopsのすべてのバージョン。
- Auto Configを実行するマシン。このデバイスは次のいずれかです。

- デリバリーコントローラー™
- .NET Framework 4.7.2以降とCitrix PowerShell SDKがインストールされたドメイン参加済みマシン。Citrix PowerShellの場合、Web Studioをインストールする必要があります。

バックアップ

1. Automated Configuration をインストールします。詳細については、「Download Automated Configuration」を参照してください。
2. **Auto-Config** をダブルクリックします。
3. PowerShell ウィンドウで、コマンド `Backup-CvadAcToFile` を実行してすべてのコンポーネントをエクスポートします。オンプレミス構成をエクスポートしても、変更はされません。

コマンドを初めて実行すると、プロセスによって次の場所に `.yml` 構成ファイルを含むフォルダーが作成されます。 `%HOMEPATH%\Documents\Citrix\AutoConfig`。

このフォルダーには、最近エクスポートされたバックアップファイルが含まれており、以前の各バックアップはサブフォルダーに保存されます。

復元

1. **Auto-Config** をダブルクリックします。
2. 復元を実行するには、次のコマンドを実行します。

```
Restore-CvadAcToSite -Environment OnPrem -RestoreFolder <folder path of the backup files>
```

3. コマンドを実行した後、エクスポートの状態を確認し、ログフォルダーが次の場所にあることを確認します: `%HOMEPATH%\Documents\Citrix\AutoConfig`。
4. エラーまたは例外がある場合は、ログファイルの **Fixups** セクションを参照してください。

DaaS

構成をバックアップするための前提条件

- アクティブなリソースの場所とコネクタがインストールされている DaaS 環境。
- Citrix Cloud にアクセスするサイトへの接続。詳細については、「System and Connectivity Requirements」を参照してください。

> **注**

> Automated Configuration を使用して、クラウドから MCS をバックアップすることはできません。

バックアップ

次のファイルをバックアップします。

- 顧客 ID、クライアント ID、およびシークレットキー情報を含む `CustomerInfo.yml` ファイル。顧客 ID、クライアント ID、およびシークレットキーを取得するプロセスについて詳しくは、顧客 ID、クライアント ID、およびシークレットキーの生成 を参照してください。この情報を `CustomerInfo.yml` ファイルに追加する方法については、顧客情報ファイルの入力 を参照してください。
- クラウド内のリソースの場所をマッピングする情報を含む `ZoneMapping.yml` ファイル。ゾーンをマッピングする方法について詳しくは、ゾーンマッピングファイルの入力 を参照してください。
- ホスト接続に関する情報を含む `CvadAcSecurity.yml` ファイル。

1. Automated Configuration をインストールします。詳しくは、Automated Configuration のインストール を参照してください。

> **注**
>
> DaaS バックアップの場合、インターネットアクセスがあり、管理者も直接アクセスできるマシンに Automated Configuration をインストールします。

1. **Auto Config** をダブルクリックします。
2. PowerShell ウィンドウで、バックアップを作成するために次のコマンドを実行します。
   `Export-CvadAcToFile`

初めてコマンドを実行すると、プロセスにより、.yml 構成ファイルを含むフォルダーが次の場所に作成されます。 `%HOMEPATH%\Documents\Citrix\AutoConfig`

このフォルダーには、最近のエクスポートからのバックアップファイルが含まれており、以前の各バックアップはサブフォルダーに保存されます。

復元

1. 「**Auto Config**」をダブルクリックします。
2. PowerShellウィンドウで、リストアを実行するために次のコマンドを実行します。

```
Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
```

3. コマンドを実行した後、エクスポートの状態を確認し、ログフォルダは`%HOMEPATH%\Documents\Citrix\AutoConfig`にあります。
4. エラーまたは例外がある場合は、ログファイルの「**Fixups**」セクションを参照してください。

詳細な移行

> **注**
>
> コンポーネントの移行順序の詳細については、「」を参照してください(/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/migrate#component-migration-order)。

コンポーネント全体をリストアする

コンポーネントをリストアするには、1つ以上のパラメータを選択する必要があります。

たとえば、デリバリーグループとマシンカタログコンポーネント全体をリストアするには、次のコマンドを実行します。

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups
-MachineCatalogs
```

コンポーネントメンバーをリストアする

1つ以上のコンポーネントメンバーをリストアするには、`IncludeByName`機能を使用します。選択したコンポーネントとインクルージョンリストとともに、`Restorefolder`パラメータを指定して`Restore`コマンドレットを呼び出す必要があります。

たとえば、バックアップから2つのグループポリシーをリストアするには：

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -GroupPolicies
-IncludeByName Policy1,Policy2
```

クラウドサイト構成全体をリストアする

すべてのコンポーネントまたはクラウドサイト全体をリストアするには、次のコマンドを実行します。

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

バックアップと復元用の自動構成ツール

Automated Configuration ツールのコマンドは、Web Studio が使用するバックアップおよび復元 API をトリガーします。

`BckRstr` コマンドレットはコンソールにログを記録します。ログ情報を含むフォルダーは `\Documents\Citrix\AutoConfig` に作成されません。

注：

Citrix Virtual Apps and Desktops および Citrix DaaS™ で構成をバックアップするための前提条件は、PowerShell セッションでの自動構成ツールと同じです。

バックアップ

Delivery Controller で新しいバックアップアクションを開始するには、PowerShell ウィンドウで `New-BckRstrBackup` を実行します。

復元

既存のバックアップから単一コンポーネントのメンバーを復元するには、PowerShell ウィンドウで `Restore-BckRstrBackups` を実行します。

コマンドの完全なリストについては、「バックアップと復元のためのAutomated Configuration ツールコマンドレット」を参照してください。

バックアップと復元のベストプラクティス

この記事では、バックアップと復元の計画をより適切に行うのに役立ついくつかの推奨事項を説明します。

カテゴリ	ベストプラクティス
バックアップのスケジュール設定	サイト構成の変更頻度に応じて、日次、週次、または月次で実行できるデフォルトのバックアップスケジュールを設定します。このデフォルトスケジュールは、週末や深夜など、アクティビティの少ない時間帯に設定してくだ

カテゴリ	ベストプラクティス
	さい。スケジュールされたバックアップの詳細については、「スケジュールされたバックアップの作成」を参照してください。
	同じ日に実行される可能性のある複数のバックアップスケジュールが定義されている場合は、**Backup and Restore**ノードの**Settings**タブを使用して、1日あたりのバックアップ制限をリセットします。
バックアップの管理	30個のバックアップ制限に達しても保持されるように、ゴールデンコピーのバックアップを常にピン留めしてください。選択したバックアップをピン留めするには、バックアップを右クリックします。

よくある質問

カスタム管理者はバックアップと復元を実行できますか?

いいえ。バックアップと復元機能は、フル権限を持つ管理者のみに限定されています。

特定のコンポーネントを選択的にバックアップできますか?

いいえ。現在、オンデマンドおよびスケジュールされたバックアップは、サイト構成全体をバックアップします。コンポーネントにはいくつかの依存関係と前提条件があります。これらの依存関係が適切に解決されるように、コンポーネント全体をバックアップできます。ただし、特定のコンポーネントを復元することはできます。

バックアップをダウンロードできますか?

現在、バックアップをダウンロードするにはACTを使用します。ACTはAutomated Configuration for Virtual Apps and Desktopsからダウンロードできます。

MCSカタログをバックアップおよび復元できますか?

現在、MCSカタログをバックアップおよび復元することはできません。ACTを使用してMCSカタログをバックアップし、別のサイトにインポートできます。

構成をCitrix Cloud™に移行する

Automated Configuration Tool (ACT) を使用すると、1つ以上のオンプレミスサイトからCitrix Cloudでホストされているサービス Citrix DaaSへ、Citrix Virtual Apps and Desktops™の構成（ポリシー、

アプリケーション、カタログ、管理者ロール、スコープなど）を移行できます。また、異なるCloudリージョンまたはテナント間で情報を移行するためにも使用できます。

このツールは、1つ以上のオンプレミスサイトを構成ファイルのコレクションとして検出し、エクスポートします。これらのファイルはオプションで編集できます。これらのファイルの構成は、Citrix DaaSにインポートできます。 移行は、ツールを複数回実行することで段階的に行われ、目的の構成状態を簡単に実現できます。

ACTは、一度きりの移行ツールではありません。日常のクラウド運用を管理するために使用できます。例えば、次のとおりです。

- テストまたはステージングクラウドアカウントから本番クラウドアカウントへの転送の自動化
- 構成のバックアップと復元
- 1つのクラウド環境を複数のクラウドに分割する

以下の*2分間の*ビデオでは、自動構成の簡単なツアーを提供します。

<iframe src="https://www.youtube.com/embed/uyQ9o2L1DXQ" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
Automated Configurationに関する追加情報については、Tech Zoneの概念実証: Automated Configuration Toolを参照してください。

展開の移行とオンプレミス構成の移行準備について詳しく知るには、Tech Zoneの展開ガイド: Citrix Virtual Apps and DesktopsをオンプレミスからCitrix Cloudに移行するを参照してください。

既知の制限事項

- Machine Creation Services™を介してプロビジョニングされたマシンカタログには、特別な考慮事項があります。MCSの詳細については、Machine Creation Servicesでプロビジョニングされたカタログの移行についてを参照してください。

構成を移行するための前提条件

Citrix Virtual Apps and Desktopsから構成を*エクスポート*するには、次のものが必要です。

- Citrix Virtual Apps and Desktops: 現在のリリースとその直前のリリース、またはCitrix Virtual Apps and Desktops、XenApp and XenDesktop® LTSRs: すべてのバージョン
- .NET Framework 4.7.2以降とCitrix PowerShell SDKがインストールされたドメイン参加済みマシン。これはDelivery Controllerに自動的にインストールされます。(オンプレミスのDelivery Controller以外のマシンで実行するには、Studioが適切なPowerShellスナップインをインス

トールするため、Citrix Studioをインストールする必要があります。Studioインストーラーは Citrix Virtual Apps and Desktopsのインストールメディアにあります。)

Citrix DaaSに構成を*インポート*するには、以下が必要です。

- Citrix Cloudにアクセスできるマシン。これはDelivery Controller™やドメイン参加済みマシンである必要はありません。
- Citrix DaaSがプロビジョニングされていること。
- Connectorがインストールされ、オンプレミス環境と同じドメインにドメイン参加しているアクティブなリソースロケーション。
- Citrix Cloudにアクセスするサイトへの接続が許可され、利用可能である必要があります。詳細については、システムおよび接続要件を参照してください。

> **注:**
>
> Automated ConfigurationはCloud Connectorシステムにはインストールできません。

主な手順

1. Automated Configuration Toolをダウンロードし、システム要件を確認します。Automated Configurationのダウンロードを参照してください。
2. Citrix Cloudポータルから生成された`CustomerName`、`CustomerID`、および`SecretKey`の値で`CustomerInfo.yml`ファイルを更新します。顧客ID、クライアントID、およびシークレットキーの生成と顧客情報ファイルの入力を参照してください。
3. オンプレミスサイトに複数のゾーンが含まれている場合は、ゾーンをCitrix DaaSリソースロケーションにマッピングするように`ZoneMapping.yml`ファイルを更新します。ゾーンマッピングファイルの入力を参照してください。
4. サイトに複数のホスティング接続が含まれている場合は、Citrix DaaSに移行する各ホストタイプの接続情報で`CvadAcSecurity.yml`ファイルを更新します。ホスト接続が1つだけの場合は、ホスト接続の接続情報で`CvadACSecurity.yml`ファイルを更新します。ホスト接続のセキュリティファイルの更新を参照してください。
5. ACTを開き、`Export-CvadAcToFile`コマンドを使用してオンプレミスサイトをエクスポートします。移行がサポートされているコンポーネントのリストについては、サポートされている移行オブジェクトを参照してください。エクスポートの手順については、オンプレミス構成のエクスポートを参照してください。

6. `Merge-CvadAcToSite`コマンドを使用して、コンポーネントを段階的にインポートします。または、サイト全体を一度に移行することもできます。コンポーネントの移行順序に記載されている順序でコンポーネントを移行してください。インポートの手順については、インポートの実行を参照してください。
7. クラウドサイトをアクティブ化します。サイトのアクティブ化を参照してください。

Automated Configurationをダウンロードする

Citrix DownloadsからAutomated Configurationツールをダウンロードしてインストールします。

Automated Configurationをアップグレードする

機能のエラーを防ぐため、常にACTの最新バージョンを使用してください。

ツールのバージョンを確認するには、次の手順を実行します。

1. **Auto Config**アイコンをダブルクリックします。PowerShellウィンドウが表示されます。
2. バージョン番号を確認するには、次のコマンドを実行します。

```
Get-CvadAcStatus
```

3. Citrix Downloadsに記載されているバージョンとツールのバージョンを比較します。ツールの最新バージョンはそこにあります。
4. ツールの最新バージョンをダウンロードしてインストールします。Automated Configurationをアップグレードするために、古いバージョンをアンインストールする*必要はありません*。

> **注:**
>
> Automated Configurationでクラウドにアクセスするためにコマンドレットを実行すると、ダウンロード可能な新しいバージョンがある場合にツールが通知します。コマンドレットの詳細については、Automated Configurationツールコマンドレットを参照してください。

顧客ID、クライアントID、およびシークレットキーを生成する

オンプレミスサイトをCitrix DaaSに移行するには、Citrix Cloudポータルから顧客ID、クライアントID、およびシークレットキーを使用して`CustomerInfo.yml`ファイルを入力します。

顧客IDを取得するには：

1. Citrix Cloudアカウントにサインインし、顧客を選択します。

2. グリッドアイコンをクリックし、**Identity and Access Management**を選択します。
3. **API access > Secure clients**に移動します。顧客IDがページに表示されます。

クライアントIDとシークレットキーを取得するには：

1. **Secure clients**ページで、ボックスに名前を入力します。この名前は、複数のクライアントIDとシークレットキーを区別するために使用されます。
2. 「Create Client」をクリックして、クライアントIDとシークレットキーを作成します。
3. クライアントIDとシークレットキーを安全な場所にコピーし、この情報を含む`.csv`ファイルをダウンロードします。`.csv`ファイルを使用して`CustomerInfo.yml`ファイルを生成します。

> **注:**
>
> - クライアントIDとシークレットキーには有効期限がありません。これらが侵害された場合は、 アイコンを使用して直ちに削除し、新しいものを作成してください。
> - シークレットキーは、紛失または忘れた場合、取得できません。新しいクライアントIDとシークレットキーを作成する必要があります。

顧客情報ファイルを生成する

`CustomerInfo.yml`ファイルを使用すると、コマンドレットを実行するたびに顧客情報パラメーターを指定する必要がなくなります。顧客情報のいずれかは、コマンドレットパラメーターを使用して上書きできます。

`New-CvadAcCustomerInfoFile`コマンドレットを使用して、`CustomerInfo.yml`ファイルを作成します。

> **重要:**
>
> `CustomerInfo.yml` ファイルを手動で編集しないでください。手動で編集すると、意図しない書式設定エラーが発生する可能性があります。

> `New-CvadAcCustomerInfoFile` コマンドレットには、次の必須パラメーターがあります。

- CustomerId: 顧客のID。

- ClientId: Citrix Cloudで作成された顧客のクライアントID。
- Secret: Citrix Cloudで作成された顧客のシークレット。

例:

```
New-CvadAcCustomerInfoFile -CustomerId markhof123 -ClientId
6813EEA6-46CC-4F8A-BC71-539F2DAC5984 -Secret TwBLaaaaaaaaaaaaaaaaaw==
```

ダウンロードした `security.csv` ファイルを指す `SecurityCsvFileSpec` パラメーターを使用して、`CustomerInfo.yml` を作成することもできます。CustomerId も指定する必要があります。

```
New-CvadAcCustomerInfoFile -SecurityCsvFileSpec C:
\Users\my_user_name\downloads/security.csv -CustomerId markhof123
```

`CustomerInfo.yml` ファイルを更新するには、`Set-CvadAcCustomerInfoFile` コマンドレットを使用します。このコマンドレットはクライアントIDのみを変更します。

```
Set-CvadAcCustomerInfoFile -ClientId C80487EE-7113-49F8-85DD-2CFE30CC398E
```

以下は、CustomerInfo.yml ファイルのサンプルです。

```
# Created/Updated on 2020/01/29 16:46:47

CustomerId: ‘markhof123’

ClientId: ‘6713FEA6-46CC-4F8A-BC71-539F2DDK5384’

Secret: ‘TwBLaaabbbaaaaaaaaaaw==’

Environment: Production

AltRootUrl: ‘’

StopOnError: False

AlternateFolder: ‘’

Locale: ‘en-us’
```

```
Editor: 'C:\Program Files\Notepad++\notepad++.exe'

Confirm: True

DisplayLog: True
```

ゾーンマッピングファイルにデータを入力する

オンプレミスゾーンは、クラウドのリソースの場所と同等です。他のサイトコンポーネントとは異なり、オンプレミスゾーンをクラウドに自動的にインポートすることはできません。代わりに、`ZoneMapping.yml` ファイルを使用して手動でマッピングする必要があります。ゾーン名が既存のリソースの場所名に関連付けられていない場合、インポートが失敗する可能性があります。

オンプレミスサイトにゾーンが1つしかなく、クラウドサイトにリソースの場所が1つしかない場合、自動構成ツールが正しい関連付けを行うため、`ZoneMapping.yml` ファイルを手動で管理する必要はありません。

ただし、オンプレミスサイトに複数のゾーンがある場合、またはクラウドサイトに複数のリソースロケーションがある場合は、`ZoneMapping.yml` ファイルを手動で更新して、オンプレミスゾーンとクラウドのリソースロケーションの正しいマッピングを反映させる必要があります。

`ZoneMapping.yml` ファイルは `%HOMEPATH%\Documents\Citrix\AutoConfig` にあります。`.yml` ファイルの内容は、ゾーン名をキー、リソースの場所名を値とする辞書です。

たとえば、「Zone-1」というプライマリゾーンと「Zone-2」というセカンダリゾーンを持つオンプレミスのCitrix Virtual Apps and Desktopsサイトが、「Cloud-RL-1」と「Cloud-RL-2」という2つの新しく作成されたクラウドのリソースロケーションを持つCitrix DaaS展開に移行されるとします。この場合、ZoneMapping.ymlは次のように構成されます。

```
            Zone-1: Cloud-RL-1



            Zone-2: Cloud-RL-2
```

注:

> コロンとリソースロケーション名の間にスペースを追加します。ゾーン名またはリソースロケーション名にスペースが含まれている場合は、名前を引用符で囲みます。

ホスト接続用のセキュリティファイルを更新する

ホスト接続とその関連ハイパーバイザーは、ACT を使用してエクスポートおよびインポートできます。

ホスト接続にハイパーバイザーを追加するには、ハイパーバイザーの種類に固有のセキュリティ情報が必要です。セキュリティ上の理由から、この情報はオンプレミスサイトからエクスポートできません。自動構成がホスト接続とハイパーバイザーをクラウドサイトに正常にインポートできるように、この情報を手動で提供する必要があります。

エクスポートプロセスでは、特定のハイパーバイザータイプに必要な各セキュリティ項目のプレースホルダーを含む `%HOMEPATH%\Documents\Citrix\AutoConfig` に `CvadAcSecurity.yml` ファイルが作成されます。クラウドサイトにインポートする前に、`CvadAcSecurity.yml` ファイルを更新する必要があります。管理者による更新は、必要に応じて新しいセキュリティプレースホルダーが追加され、複数のエクスポートにわたって保持されます。セキュリティ項目が削除されることはありません。詳細については、「CvadAcSecurity.yml ファイルを手動で更新する」を参照してください。

```
HostConn1:

ConnectionType: XenServer®

UserName: root

PasswordKey: rootPassword

HostCon2:

ConnectionType: AWS

ApiKey: 78AB6083-EF60-4D26-B2L5-BZ35X00DA5CH

SecretKey: TwBLaaaaaaaaaaaaaaaaw==

Region: East
```

ハイパーバイザーごとのセキュリティ情報

各ハイパーバイザータイプに必要なセキュリティ情報を以下に示します。

- ゼンスサーバー、Hyper-V、ヴイエムウェア
  - ユーザー名
  - クリアテキストパスワード
- マイクロソフト アジュール
  - サブスクリプション ID
  - アプリケーション ID
  - アプリケーションシークレット
- AWS
  - サービスアカウントID
  - アプリケーションシークレット
  - 地域

セキュリティに関する特別な考慮事項

すべてのセキュリティ情報はクリアテキストとして入力されます。クリアテキストが推奨されない場合は、ホスト接続と関連するハイパーバイザーを**Studio**を使用して手動で作成できます。ホスト接続とハイパーバイザー名は、オンプレミスの対応するものと正確に一致している必要があります。そうすることで、ホスト接続を使用するマシンカタログを正常にインポートできます。

Citrix Virtual Apps and Desktopsのオンプレミス構成をエクスポートする

`export` PowerShellコマンドを使用して、既存のオンプレミス構成をエクスポートし、必要な`.yml`ファイルを取得できます。これらのファイルは、目的の構成をCitrix Cloudにインポートするために使用されます。

サポートされている移行オブジェクト

自動構成は、以下のコンポーネントの構成の移動をサポートしています。

- タグ
- 委任管理
  - スコープ
  - ロール

- ホスト接続
  - 単一のリソースプール
  - 管理スコープ
- マシンカタログ
  - 管理スコープ
  - マシン
  - リモートPCアクセス、物理、プール、プロビジョニング済み、MCS、割り当て済み
- StoreFront™
- デリバリーグループ
  - アクセス ポリシー
  - 管理スコープの関連付け
  - アプリケーションアクセス ポリシー
  - 割り当てポリシー
  - エンタイトルメント/デスクトップ ポリシー
  - 電源スケジュール
  - セッションの残存
  - セッションの事前起動
  - 再起動スケジュール
  - タグ
- アプリケーション グループ
  - 管理スコープの関連付け
  - デリバリー グループ
  - ユーザーとグループ
- アプリケーション
  - アプリケーション フォルダー
  - アイコン
  - アプリケーション
  - ブローカー構成済みFTA

    - タグ

- グループ ポリシー
- ユーザーゾーンの優先設定

オンプレミス構成のエクスポート

1. **Auto Config** アイコンをダブルクリックします。PowerShell ウィンドウが表示されます。
2. すべてのコンポーネントをエクスポートするには、次のコマンドを実行します。オンプレミス構成をエクスポートしても、その構成が変更されることは*ありません*。

```
Export-CvadAcToFile
```

任意のコマンドレットを初めて実行すると、`.yml` 構成ファイルとログを含むエクスポートフォルダーが作成されます。このフォルダーは `%HOMEPATH%\Documents\Citrix\AutoConfig` にあります。エクスポートを繰り返すたびにサブフォルダーが作成されます。親フォルダー `%HOMEPATH%\Documents\Citrix\AutoConfig` には、常に最新のエクスポートからのエクスポートファイルが含まれています。

> **注:**

> Delivery Controller に Automated Configuration がインストールされていない場合は、PowerShell を介してツールを使用する前に `import-module Citrix.AutoConfig.Commands` を実行します。**Auto Config** アイコンを使用して Automated Configuration を開く場合は、この手順は不要です。

> エラーまたは例外が発生した場合は、ログファイルの **Fixups** セクションを参照してください。

構成を Citrix DaaS にインポートする

> **重要:**

> - オンプレミス展開をクラウドに移行する場合は、Citrix設定を含むドメインおよびOU GPOがクラウドに移行されていることを確認してください。Citrix Web Studio™はGPMCをサポートしていないため、ドメインおよびOU GPOはWeb Studioに表示されま

> せん。Citrixポリシーエンジンは、ドメインおよびOU内のVDAおよびユーザーにドメインおよびOU GPOを適用します。VDAにログインした後、ユーザーはドメインおよびOU GPOからのポリシーがセッションに適用されていることを確認できます。ただし、管理者はこれらのポリシーと設定を確認できないため、混乱を招く可能性があります。

コンポーネントの移行順序

コンポーネントとその依存関係をここに示します。コンポーネントをインポートまたはマージする前に、その依存関係が配置されている必要があります。依存関係が不足している場合、インポートまたはマージコマンドが失敗する可能性があります。インポートまたはマージが失敗した場合、ログファイルの **Fixups** セクションに不足している依存関係が表示されます。

1. タグ
    - 事前依存関係なし
2. 委任された管理者
    - 依存関係なし
3. ホスト接続
    - CvadAcSecurity.yml のセキュリティ情報
4. マシンカタログ
    - Active Directory に存在するマシン
    - ホスト接続
    - タグ
5. StoreFront
6. デリバリーグループ
    - Active Directory に存在するマシン
    - Active Directory に存在するユーザー
    - マシンカタログ
    - タグ
7. アプリケーショングループ
    - デリバリーグループ

- タグ

8. アプリケーション
   - デリバリーグループ
   - アプリケーショングループ
   - タグ
9. グループポリシー
   - デリバリーグループ
   - タグ
10. ユーザーゾーン設定

インポートの実行

1. **Auto Config** アイコンをダブルクリックします。PowerShell ウィンドウが表示されます。
2. すべてのコンポーネントをインポートするには、次のコマンドを実行します。

```
Merge-CvadAcToSite
```

期待される状態と新しい現在の状態を確認します。さまざまなインポートオプションにより、インポート結果がオンプレミスサイトと同一であるか、そのサブセットであるかが制御されます。

コマンドレットを実行すると、`.yml` 構成ファイルとログを含むエクスポートフォルダーが作成されます。フォルダーは `%HOMEPATH%\Documents\Citrix\AutoConfig` にあります。

エラーまたは例外が発生した場合は、ログファイルの **Fixups** セクションを参照してください。

注記：

Delivery ControllerにAutomated Configurationがインストールされていない場合は、PowerShellを介してツールを使用する前に `import-module Citrix.AutoConfig.Commands` を実行します。**Auto Config**アイコンを使用してAutomated Configurationを開く場合は、この手順は不要です。

元のCitrix DaaS構成に戻すには、「Citrix DaaS構成のバックアップ」を参照してください。

インポート操作について

インポートプロセスは、更新を正確に実行し、必要な更新のみを実行し、すべての更新が正しく行われたことを確認するように設計されています。すべてのインポート操作で以下の手順が実行されます。

1. エクスポートされた.ymlファイル（期待される状態）を読み取ります。
2. クラウド（現在の状態）を読み取ります。
3. インポート前のクラウドの状態を.ymlファイルにバックアップします（必要に応じて、事前バックアップを復元できます）。
4. 期待される状態と現在の状態の間の差異を評価します。これにより、実行する更新が決定されます。
5. 更新を実行します。
6. クラウドを再読み込みします（新しい現在の状態）。
7. インポート後のクラウドの状態を.ymlファイルにバックアップします（必要に応じて、事後バックアップを復元できます）。
8. 新しい現在の状態を期待される状態と比較します。
9. 比較結果を報告します。

きめ細かい移行

> **重要:**

> コンポーネントの移行順序の詳細については、コンポーネントの移行順序を参照してください。

> コンポーネントのみ、またはコンポーネント名のみを選択的に移行できます。

- サポートされているコンポーネントパラメーターには、`MachineCatalogs`、`Tags`などがあります。
- サポートされているコンポーネント名パラメーターには、`IncludeByName`および`ExcludeByName`パラメーターなどがあります。

パラメーターとその使用方法の詳細については、詳細な移行パラメーターを参照してください。

サイトをアクティブ化する

オンプレミスサイトとクラウドサイトの両方にあるデリバリーコントローラーは、デスクトップ、アプリケーションの仲介、マシンの再起動などのリソースを制御します。共通のリソースセットが2つ以上のサイトによって制御されると、問題が発生します。このような状況は、オンプレミスサイトからクラウドサイトに移行する際に発生する可能性があります。オンプレミスとクラウドの両方のデリバリーコントローラーが同じリソースセットを管理する可能性があります。このような二重管理は、リソースが利用できなくなり、管理不能になる可能性があり、診断が困難になることがあります。

サイトのアクティブ化により、アクティブなサイトがどこで制御されるかを制御できます。

サイトのアクティブ化は、デリバリーグループのメンテナンスモードを使用して管理されます。サイトが非アクティブの場合、デリバリーグループはメンテナンスモードになります。アクティブなサイトのデリバリーグループからは、メンテナンスモードが解除されます。

サイトのアクティブ化は、VDA登録やマシンカタログに影響を与えたり、管理したりすることはありません。

- `Set-CvadAcSiteActiveStateCloud`
- `Set-CvadAcSiteActiveStateOnPrem`

すべてのコマンドレットは、`IncludeByName`および`ExcludeByName` フィルタリングをサポートしています。このパラメーターを使用すると、メンテナンスモードを変更できるデリバリーグループを選択できます。デリバリーグループは必要に応じて選択的に変更できます。

インポートとクラウドへの制御の移行

オンプレミスサイトからクラウドサイトへ制御をインポートおよび転送する方法の概要を以下に示します。

1. オンプレミスサイトをクラウドにエクスポートおよびインポートします。`-SiteActive` パラメーターがインポートコマンドレットのいずれにも存在しないことを確認してください。オンプレミスサイトはアクティブで、クラウドサイトは非アクティブです。デフォルトでは、クラウドサイトのデリバリーグループはメンテナンスモードになっています。
2. クラウドのコンテンツと構成を確認します。
3. 営業時間外に、オンプレミスサイトを非アクティブに設定します。`-SiteActive` パラメーターは存在しない必要があります。すべてのオンプレミスサイトのデリバリーグループはメンテナンスモードになります。

    - `Set-CvadAcSiteActiveStateOnPrem`

4. クラウドサイトをアクティブに設定します。`-SiteActive` パラメーターが存在している必要があります。クラウドサイトのデリバリーグループはメンテナンスモードになりません。

   - `Set-CvadAcSiteActiveStateCloud -SiteActive`

5. クラウドサイトがアクティブで、オンプレミスサイトが非アクティブであることを確認します。

オンプレミスサイトに制御を戻す

クラウドサイトからオンプレミスサイトに制御を転送するには：

1. 営業時間外に、クラウドサイトを非アクティブに設定します。すべてのクラウドサイトのデリバリーグループはメンテナンスモードになります。

   - `Set-CvadAcSiteActiveStateCloud`

2. オンプレミスサイトをアクティブに設定します。オンプレミスサイトのデリバリーグループはメンテナンスモードになりません。

   - `Set-CvadAcSiteActiveStateOnPrem -SiteActive`

その他のサイトアクティベーション情報

- マシンが電源管理されておらず、再起動スケジュールがない場合（通常、ホスト接続もないことを意味します）、すべてのクラウドデリバリーグループをアクティブとしてインポートできます。インポート後に`-SiteActive`を`Merge-CvadAcToSite`/`Import-CvadAcToSite`に追加するか、`Set-CvadAcSiteActiveStateCloud -SiteActive`を実行します。
- マシンが電源管理されている場合、または再起動スケジュールがある場合は、別のプロセスが必要です。たとえば、この状況でオンプレミスからクラウドに切り替える場合は、`Set-CvadAcSiteActiveStateOnPrem`を使用してオンプレミスサイトを非アクティブに設定します。その後、`Set-CvadAcSiteActiveStateCloud -SiteActive`を使用してクラウドサイトをアクティブに設定します。
- `Set-CvadAcSiteActiveStateCloud`および`Set-CvadAcSiteActiveStateOnPrem`コマンドレットは、プロセスを元に戻すためにも使用されます。たとえば、`-SiteActive`パラメーターなしで`Set-CvadAcSiteActiveStateCloud`を実行し、次に`-SiteActive`パラメーターを指定して`Set-CvadAcSiteActiveStateOnPrem`を実行します。

Machine Creation Servicesでプロビジョニングされたカタログの移行について理解する

> **注:**

> この機能はバージョン3.0以降でのみ利用可能です。Automated Configuration内で `Get-CvadAcStatus` を使用してバージョンを確認してください。

> Machine Creation Services (MCS) カタログは、2種類のカタログを作成します。

- マシンに加えられた変更が失われるか元に戻される場合（一般的にアプリケーションが公開されるサーバーOS） – これはプールされたVDI / マルチセッションのユースケースです
- マシンに加えられた変更が再起動後も保持される場合（一般的に専用ユーザーを持つクライアントOS） – これは静的VDIのユースケースです

カタログの種類は、Citrix Studioのカタログノードでカタログの「User data:」値を確認することで確認できます。

> **注:**
>
> MCSは、Automated Configurationを使用してクラウドからバックアップすることはできません。

プールされたVDI / マルチセッションカタログ

「User data: Discard」のカタログはプールされたVDIカタログであり、メインイメージと構成のみを移行できます。これらのカタログ内の仮想マシンは移行されません。これは、仮想マシンのライフサイクルがインポート元のサイトによって維持されており、マシンが起動されるたびにその状態が変化する可能性があるためです。これにより、仮想マシンのインポートデータがすぐに同期されなくなるため、インポートは不可能になります。

このツールを使用してこれらのカタログを移行する場合、カタログメタデータが作成され、メインイメージの作成が開始されますが、マシンはインポートされません。

メインイメージのサイズに基づいてこのプロセスの作成には時間がかかる場合があるため、ツール内のインポートコマンドはMCSカタログの作成を開始するだけで、完了を待機しません。インポートが完了したら、クラウド展開のStudioを使用してカタログ作成の進行状況を監視してください。

メインイメージが作成されたら、マシンをプロビジョニングできます。オンプレミスでの使用によって容量が消費されるため、容量に関する考慮事項を検討してください。

そのカタログを使用する他のすべてのオブジェクト（デリバリーグループ、アプリケーション、ポリシーなど）はインポートでき、メインイメージの作成を待つ必要はありません。カタログの作

成が完了すると、インポートされたカタログにマシンを追加でき、ユーザーはリソースを起動できます。

> **注:**
>
> カタログおよびその他すべてのオブジェクトを移行するには、ツール内で利用可能な同じコマンドを使用します。

静的VDIカタログ

> **注:**
>
> この操作はデータベースに保存されている低レベルの詳細をインポートするため、このプロセスはデータベースアクセス権を持つマシンから実行する必要があります。

> 静的VDIカタログは、メインイメージ、構成、およびすべての仮想マシンを移行します。プールされたVDIのユースケースとは異なり、イメージを作成する必要はありません。

VDAがクラウドに登録されるように、コネクタを指すように設定する必要があります。

クラウドサイトをアクティブにするには、サイトのアクティブ化セクションを参照してください。これにより、再起動スケジュール、電源管理、その他の項目がクラウドによって制御されます。

移行が完了した後、オンプレミスサイトからこのカタログを削除したい場合は、**VMとADアカウントを残す**を選択する必要があります。そうしないと、それらは削除され、クラウドサイトは削除されたVMを指したままになります。

移行後に孤立したリソースを検出するためにMCSタグを更新する

オンプレミス構成からクラウドサイトへ、またはクラウド構成から別のクラウドサイトへ移行した後、永続VMの場合に孤立したリソースが正しく検出されるように、MCSサイトIDタグを更新する必要があります。これを行うには、PowerShellコマンド`Set-ProvResourceTags`を使用します。現在、この機能はAzureに適用されます。

詳細な手順は次のとおりです。

1. 新しいCitrixサイトからPowerShellコマンド `Set-ProvResourceTags` を使用して、MCSサイトIDタグを更新します。例:

```
Set-ProvResourceTags -ProvisioningSchemeUid xxxxx  [-VMName <String>]
[-VMBatchSize XX] [-ResourceType XX]
```

または、,

```
Set-ProvResourceTags -ProvisioningSchemeName xxxxx  [-VMName <String>]
[-VMBatchSize XX] [-ResourceType XX]
```

パラメーターの詳細は次のとおりです。

- `ProvisioningSchemeUid` または `ProvisioningSchemeName` は必須パラメーターです。
- `VMName` はオプションパラメーターです。`VMName` が指定されていない場合、このマシンカタログのすべてのVMのタグが更新されます。
- `VMBatchSize` は、すべてのVMをバッチに分割するためのオプションパラメーターです。`VMBatchSize` が指定されていない場合、デフォルト値 (10) が適用されます。範囲は1から60です。
- `ResourceType` は次のいずれかです。
  - `MachineCatalog`: マシンカタログリソースのタグを更新する場合。
  - `VirtualMachine`: VM関連リソースのタグを更新する場合。
  - `All`: (デフォルトのResourceType): マシンカタログとVM関連リソースの両方のタグを更新する場合。

複数のサイトを単一のサイトに統合する

Automated Configuration のマルチサイトサポートは、複数のオンプレミスサイトを単一のクラウドサイトに統合する方法を提供します。

マルチサイトサポートは、オンプレミスサイトごとにコンポーネント名に一意のプレフィックスとサフィックスを追加し、複数のオンプレミスサイトが単一のクラウドサイトに統合された後の名前の一意性を確保します。

プレフィックスとサフィックスは、オンプレミスサイトごとに次の各コンポーネントに割り当てることができます。

- `AdminScope`
- `AdminRole`
- `ApplicationAdmin`

- `ApplicationFolder`
- `ApplicationGroup`
- `ApplicationUser`
- `DeliveryGroup`
- `GroupPolicy`
- `HostConnection`
- `MachineCatalog`
- `StoreFront`
- `Tag`

アプリケーションフォルダーは、プレフィックス、サフィックス、および再ルートをサポートします。再ルートにより、アプリケーションの既存のフォルダー構造に最上位のフォルダーが追加されます。

プレフィックスとサフィックスのルール

1. プレフィックスとサフィックスには、次の特殊文字を含めることはできません: `\ , / ; : # . * ? = < > | ( ) " ' { } [ ]`
2. プレフィックスとサフィックスには末尾のスペースを含めることができますが、先頭のスペースを含めることはできません。
3. プレフィックスとサフィックスに末尾のスペースを含めるには、二重引用符で囲む必要があります。
4. プレフィックスとサフィックスは、インポート、マージ、および追加時に適用されます。ソースの.ymlファイルは変更されません。
5. プレフィックスとサフィックスのプロセスは、該当する場合、依存するコンポーネント名に自動的にプレフィックスまたはサフィックスを付けます。たとえば、マシンカタログ名に「East」というプレフィックスが付いている場合、それらを参照するデリバリーグループにも「East」というプレフィックスが付けられます。
6. コンポーネント名がすでにプレフィックスまたはサフィックスで始まっている場合、プレフィックスまたはサフィックスは追加されません。コンポーネント名に同じプレフィックスまたはサフィックスが二重に含まれることはできません。
7. プレフィックスとサフィックスは、個別に、または組み合わせて使用できます。
8. コンポーネントへのプレフィックスまたはサフィックスの使用はオプションです。

> **注:**
>
> Studioはコンポーネントをアルファベット順に表示します。

サイト別にコンポーネントをグループ化する

プレフィックスを使用して、単一サイトのコンポーネントを視覚的にグループ化します。各サイトは独自のグループにリストされ、プレフィックスがアルファベット順に異なるサイトグループの順序を制御します。

名前でコンポーネントをグループ化

複数のサイトから同じ名前のコンポーネントを視覚的にグループ化するには、サフィックスを使用します。異なるサイトの同じ名前のコンポーネントは、視覚的に交互に表示されます。

プレフィックスとサフィックスのマッピングファイル

サイトのプレフィックス付けは、1つ以上のオンプレミスサイトのサイトプレフィックスとサフィックスのマッピングを含むSiteMerging.ymlファイルから始まります。SiteMerging.ymlファイルは手動で管理することも、複数のオンプレミスサイトをマージするコマンドレットセクションに記載されている利用可能なコマンドレットを使用して管理することもできます。

オンプレミスサイトのエクスポート

オンプレミスサイトをエクスポートするまで、マージを開始することはできません。オンプレミスサイトをエクスポートするには、オンプレミス構成のエクスポートを参照してください。

中央エクスポートターゲットフォルダー

このセクションで説明する方法では、複数のサイトのエクスポートを中央のファイル共有場所に配置します。`SiteMerging.yml`ファイル、`CustomerInfo.yml`ファイル、およびすべてのエクスポートファイルはそのファイル共有場所に存在し、オンプレミスサイトとは独立して1つの場所からインポートを実行できます。

クラウドアクセス操作は、オンプレミスサイトやActive Directoryを参照しないため、どこからでもクラウドアクセス操作を実行できます。

これを行うには、2つの方法があります。

- 直接ファイル共有: 直接ファイル共有からインポート、マージ、または追加するには、クラウドアクセス操作を実行するマシンを決定する必要があります。

- `SiteMerging.yml`を使用したファイル共有参照: この方法では、サイトのプレフィックスセットの`SiteRootFolder`メンバーを使用し、エクスポート、インポート、マージ、または追加時に誤ったフォルダーをターゲットにする可能性を低減します。

中央ファイル共有方法を使用しない場合は、個々のDelivery Controllerからインポート、マージ、または追加を実行します。クラウドに移行される各Delivery Controllerで`SiteMerging.yml`ファイルを作成し、複製します。デフォルトの場所は`%HOMEPATH%\Documents\Citrix\AutoConfig`です。正しいサイトプレフィックスを選択するには、`-SiteName`パラメーターを指定する必要があります。

直接ファイル共有

エクスポート、インポート、マージ、および新規/追加操作では、デフォルトのフォルダーである*%HOMEPATH%\Documents\Citrix\AutoConfig*以外のフォルダーをターゲットまたはソースとするパラメーターが提供されます。以下の例では、管理者がすでにアクセス権を持ち、必要に応じて資格情報を提供している`\\share.central.net`にある中央ファイル共有を使用します。

エクスポートをサイト固有のフォルダーにターゲット設定するには、`-TargetFolder`パラメーターを使用します。

イースト デリバリーコントローラー™ から:

```
mkdir \\share.central.net\AutoConfig\SiteEast
```

```
Export-CvadAcToFile -TargetFolder \\share.central.net\AutoConfig\SiteEast
```

ウェスト デリバリーコントローラー から:

```
mkdir \\share.central.net\AutoConfig\SiteWest
```

```
Export-CvadAcToFile -TargetFolder \\share.central.net\AutoConfig\SiteWest
```

エクスポートが完了したら、`CustomerInfo.yml`と`SiteMerging.yml`ファイルを作成し、`\\share.central.net\AutoConfig`に配置します。

> **注:**
>
> この直接ファイル共有参照方法を使用する場合、`SitePrefixes.yml`を作成する際に`SiteRootFolder`パラメーターを使用しないでください。

> 直接ファイル共有からインポート、マージ、または追加するには、どのマシンからクラウドアクセス操作を実行するかを決定する必要があります。オプションは次のとおりです。

- ツールがすでにインストールされているオンプレミスの Delivery Controller のいずれか。
- ファイル共有をホストしているマシン。
- 別のマシン。

クラウドにアクセスするマシンには、Automated Configuration がインストールされている必要があります。オンプレミスの PowerShell SDK、Delivery Controller、Active Directory は使用されないため、クラウドアクセス実行の要件はエクスポートの要件よりも単純です。

East Delivery Controller をクラウドにマージするには:

```
Merge-CvadAcToSite –SiteName East –SourceFolder \
\share.central.net\AutoConfig\SiteEast -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

West Delivery Controller をクラウドにマージするには:

```
Merge-CvadAcToSite –SiteName West –SourceFolder \
\share.central.net\AutoConfig\SiteWest -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

以下は、前の例で使用されたサンプル `SitePrefixes.yml` ファイルです。

```
East:

  SiteRootFolder: "" # Important: leave this empty

  AdminScopePrefix: "East_"

  AdminRolePrefix: "East_"

  ApplicationAdminPrefix: "East_"

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "East"

  ApplicationGroupPrefix: "East_"
```

```
  ApplicationUserPrefix: "East_"
  DeliveryGroupPrefix: "East_"
  GroupPolicyPrefix: "East_"
  HostConnectionPrefix: "East_"
  MachineCatalogPrefix: "East_"
  StoreFrontPrefix: "East_"
  TagPrefix: "East_"
  AdminScopeSuffix: "_east"
  AdminRoleSuffix: "_east"
  ApplicationAdminSuffix: "_east"
  ApplicationFolderSuffix: "_east"
  ApplicationGroupSuffix: "_east"
  ApplicationUserSuffix: "_east"
  DeliveryGroupSuffix: "_east"
  GroupPolicySuffix: "_east"
  HostConnectionSuffix: "_east"
  MachineCatalogSuffix: "_east"
  StoreFrontSuffix: "_east"
  TagSuffix: "_east"
West:
  SiteRootFolder: "" # Important: leave this empty
  AdminScopePrefix: "Western "
```

```
  AdminRolePrefix: "Western "

  ApplicationAdminPrefix: "Western "

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "Western"

  ApplicationGroupPrefix: "Western "

  ApplicationUserPrefix: "Western "

  DeliveryGroupPrefix: "Western "

  GroupPolicyPrefix: "Western "

  HostConnectionPrefix: "Western "

  MachineCatalogPrefix: "Western "

  StoreFrontPrefix: "Western "

  TagPrefix: "Western "

  AdminScopeSuffix: ""

  AdminRoleSuffix: ""

  ApplicationAdminSuffix: ""

  ApplicationFolderSuffix: ""

  ApplicationGroupSuffix: ""

  ApplicationUserSuffix: ""

  DeliveryGroupSuffix: ""

  GroupPolicySuffix: ""

  HostConnectionSuffix: ""
```

```
MachineCatalogSuffix: ""

StoreFrontSuffix: ""

TagSuffix: ""
```

SITEMERGING.YML を使用したファイル共有参照

この方法では、サイトのプレフィックスセットの `SiteRootFolder` メンバーを使用します。直接ファイル共有する方法よりも複雑ですが、この方法を使用すると、エクスポート、インポート、マージ、または追加の際に誤ったフォルダーをターゲットにする可能性が低減されます。

まず、SiteMerging.ymlファイルで各サイトの `SiteRootFolder` を設定します。これは共有場所で行う必要があります。

```
New-CvadAcSiteMergingInfo –SiteName East –SiteRootFolder \
\share.central.net\AutoConfig\SiteEast -SitePrefixesFolder \
\share.central.net\AutoConfig
```

```
New-CvadAcSiteMergingInfo –SiteName West –SiteRootFolder SiteWest
-SitePrefixesFolder \\share.central.net\AutoConfig
```

この例では、Eastは完全修飾フォルダー指定であり、Westは相対フォルダー指定です。

SiteMerging.yml ファイルを使用して、エクスポートをサイト固有のフォルダーにターゲット設定するには:

イースト デリバリー コントローラーから:

```
mkdir \\share.central.net\AutoConfig\SiteEast
```

```
Export-CvadAcToFile -SiteName East -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

ウェスト デリバリーコントローラーから:

```
mkdir \\share.central.net\AutoConfig\SiteWest
```

```
Export-CvadAcToFile -SiteName West -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

エクスポートコマンドレットは、`CustomerInfo.yml`フォルダーの場所を使用して`SiteMerging.yml`ファイルを検索します。Eastの場合、`SiteRootFolder`は完全修飾されています。そのまま使用されます。Westの場合、`SiteRootFolder`は完全修飾されていません。`CustomerInfo.yml`フォルダーの場所と組み合わせて、Westの完全修飾フォルダーの場所を取得します。

East Delivery Controllerをクラウドにマージするには:

```
Merge-CvadAcToSite –SiteName East -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

West Delivery Controllerをクラウドにマージするには:

```
Merge-CvadAcToSite –SiteName West -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

以下は、前の例で使用された`SitePrefixes.yml`ファイルのサンプルです。

```
  East:

  SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteEast"

  AdminScopePrefix: "East_"

  AdminRolePrefix: "East_"

  ApplicationAdminPrefix: "East_"

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "East"

  ApplicationGroupPrefix: "East_"

  ApplicationUserPrefix: "East_"

  DeliveryGroupPrefix: "East_"

  GroupPolicyPrefix: "East_"

  HostConnectionPrefix: "East_"
```

```
  MachineCatalogPrefix: "East_"

  StoreFrontPrefix: "East_"

  TagPrefix: "East_"

  AdminScopeSuffix: "_east"

  AdminRoleSuffix: "_east"

  ApplicationAdminSuffix: "_east"

  ApplicationFolderSuffix: "_east"

  ApplicationGroupSuffix: "_east"

  ApplicationUserSuffix: "_east"

  DeliveryGroupSuffix: "_east"

  GroupPolicySuffix: "_east"

  HostConnectionSuffix: "_east"

  MachineCatalogSuffix: "_east"

  StoreFrontSuffix: "_east"

  TagSuffix: "_east"

West:

  SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteWest"

  AdminScopePrefix: "Western "

  AdminRolePrefix: "Western "

  ApplicationAdminPrefix: "Western "

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead
```

```
ApplicationFolderRoot: "Western"

ApplicationGroupPrefix: "Western "

ApplicationUserPrefix: "Western "

DeliveryGroupPrefix: "Western "

GroupPolicyPrefix: "Western "

HostConnectionPrefix: "Western "

MachineCatalogPrefix: "Western "

StoreFrontPrefix: "Western "

TagPrefix: "Western "

AdminScopeSuffix: ""

AdminRoleSuffix: ""

ApplicationAdminSuffix: ""

ApplicationFolderSuffix: ""

ApplicationGroupSuffix: ""

ApplicationUserSuffix: ""

DeliveryGroupSuffix: ""

GroupPolicySuffix: ""

HostConnectionSuffix: ""

MachineCatalogSuffix: ""

StoreFrontSuffix: ""

TagSuffix: ""
```

中央ファイル共有方式を使用せず、個々のDelivery Controllerからインポート、マージ、または追加を行う場合は、クラウドに移行される各Delivery Controllerで`SiteMerging.yml`ファイルを作成し、複製します。デフォルトの場所は *%HOMEPATH%\Documents\Citrix\AutoConfig* です。正しいサイトプレフィックスを選択するには、`-SiteName`パラメーターを指定する必要があります。

サイトをマージする

Citrix®は、クラウド操作を段階的に実行し、次のクラウド操作を行う前に各結果を完全に確認することを推奨します。たとえば、3つのサイトを単一のクラウドサイトにマージする場合:

1. 適切な`SiteName`値を使用して、最初のサイトをクラウドにマージします。
2. Studioで結果を確認します。
3. 結果が正しくない場合は、問題とその原因を特定し、修正してからマージを再実行します。必要に応じて、クラウドコンポーネントを削除し、選択したコンポーネントとメンバーに`Remove-CvadAcFromSite`を使用して最初からやり直します。結果が正しい場合は、続行します。
4. 最初のマージが正しければ、2番目のサイトを単一のクラウドサイトにマージします。
5. 手順2と3を繰り返します。
6. 2番目のマージが正しければ、3番目のサイトを単一のクラウドサイトにマージします。
7. 手順2と3を繰り返します。
8. ユーザーの視点からリソースを確認し、ビューが目的の状態であることを確認します。

サイトプレフィックスを使用してコンポーネントを削除する

`Remove-CvadAcFromSite` コマンドレットの `-IncludeByName` パラメーターでプレフィックスを使用することにより、単一のサイトコンポーネントを選択的に削除できます。次の例では、West Delivery Controllerのデリバリーグループが正しくありません。Westサイトのデリバリーグループのみを削除するには、次のようにします。

```
Remove-CvadAcFromSite -DeliveryGroups -IncludeByName “Western *”
```

すべてのWestコンポーネントを削除するには、次のコマンドレットを順番に実行します。

1. `Remove-CvadAcFromSite -GroupPolicies -IncludeByName “Western *”`
2. `Remove-CvadAcFromSite -Applications -IncludeByName “Western *”`
3. `Remove-CvadAcFromSite - ApplicationGroups -IncludeByName “Western *”`
4. `Remove-CvadAcFromSite -DeliveryGroups -IncludeByName “Western *”`
5. `Remove-CvadAcFromSite -MachineCatalogs -IncludeByName “Western *”`

6. `Remove-CvadAcFromSite -HostConnections -IncludeByName “Western *”`
7. `Remove-CvadAcFromSite -Tags -IncludeByName “Western *”`

Eastコンポーネントのグループポリシーを削除するには、次のサフィックスを使用します。

```
Remove-CvadAcFromSite -GroupPolicies -IncludeByName “*_east”
```

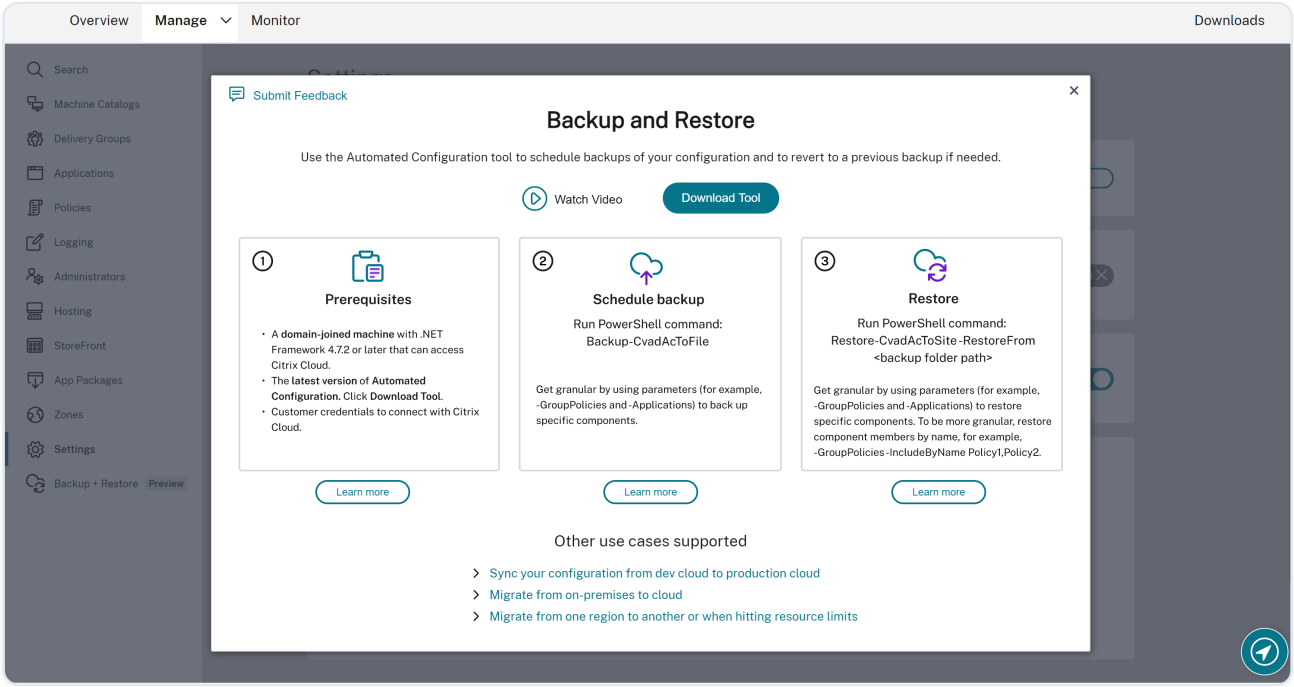
クラウドからクラウドへの移行

自動構成を使用すると、クラウド構成を別のクラウドサイトに移動したり、独自のクラウドサイトを復元したりする作業を自動化できます。

自動構成を使用すると、多くのユースケースを解決できます。

- テストまたはステージング環境から本番環境へのサイトの同期
- 構成のバックアップと復元
- リソース制限への到達
- あるリージョンから別のリージョンへの移行

Citrix Cloud™ のStudioで、自動構成と、それがクラウドからクラウドへの構成の移行にどのように使用できるかについては、ノードを参照してください。



構成を移行するための前提条件

構成をバックアップおよび復元するには、以下が必要です。

- Citrix DaaS™ がプロビジョニングされていること。

- Connector がインストールされたアクティブなリソースの場所。
- Citrix Cloudにアクセスするサイトへの接続が許可され、利用可能である必要があります。詳細については、システムおよび接続要件を参照してください。

> **注:**
>
> MCSは、Automated Configurationを使用してクラウドからバックアップすることはできません。

Citrix DaaS の構成をバックアップする

要件

Citrix DaaS の構成をバックアップする前に、次の操作を実行します。

1. `CustomerInfo.yml` ファイルに、顧客 ID、クライアント ID、および秘密鍵の情報を入力します。顧客 ID、クライアント ID、および秘密鍵の取得方法の詳細については、「顧客 ID、クライアント ID、および秘密鍵を生成する」を参照してください。この情報を `CustomerInfo.yml` ファイルに追加する方法については、「顧客情報ファイルに入力する」を参照してください。

バックアップ コマンドを実行するときは、`CustomerInfo.yml` に、バックアップ元となるソース サイトの顧客の詳細が含まれている必要があります。

復元コマンドを実行するときは、`CustomerInfo.yml` に、構成を復元する宛先サイトの顧客の詳細が含まれている必要があります。

1. `ZoneMapping.yml` ファイルに、クラウド内のリソースの場所をマッピングする情報を入力します。ゾーンのマッピング方法の詳細については、「ゾーンマッピングファイルに入力する」を参照してください。
2. ホスト接続がある場合は、対応する情報を `CvadAcSecurity.yml` ファイルに入力する必要があります。「ホスト接続のセキュリティファイルを更新する」を参照してください。

Citrix DaaS 構成をバックアップする手順

1. Automated Configuration をインストールする。

> **注:**

> クラウド間移行の場合、Automated Configuration は、管理者が直接アクセスできるインターネットにアクセス可能なマシンにインストールできます。

2. **Auto Config** アイコンをダブルクリックします。PowerShell ウィンドウが表示されます。
3. バックアップを実行するには、次のコマンドを実行します。

```
Backup-CvadAcToFile
```

初めてコマンドレットを実行すると、`.yml` 構成ファイルとログを含むエクスポートフォルダーが作成されます。フォルダーは `%HOMEPATH%\Documents\Citrix\AutoConfig` にあります。

エラーまたは例外が発生した場合は、ログファイルの **Fixups** セクションを参照してください。

Citrix DaaS に構成を復元する

1. **Auto Config** アイコンをダブルクリックします。PowerShell ウィンドウが表示されます。
2. 復元を実行するには、次のコマンドを実行します。

```
Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
```

期待される状態と新しい現在の状態を検証します。

コマンドレットを実行すると、`.yml` 構成ファイルとログを含むエクスポートフォルダーが作成されます。フォルダーは *%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。

エラーまたは例外が発生した場合は、ログファイルの **Fixups** セクションを参照してください。

バックアップと復元プロセスは、意図しないクラウドサイト構成の変更や破損から保護します。自動構成は変更が行われるたびにバックアップを作成しますが、このバックアップは変更前のクラウドサイト構成の状態を反映しています。自身を保護するには、クラウドサイト構成を定期的にバックアップし、安全な場所に保存する必要があります。望ましくない変更や破損が発生した場合、バックアップを使用して、きめ細かいレベルまたはサイト構成全体のレベルで変更や破損を修正できます。

詳細な移行

> **重要:**

> コンポーネントの移行順序の詳細については、「コンポーネントの移行順序」を参照してください。

すべてのコンポーネントを復元する

1つのコンポーネントを復元するには、1つ以上のコンポーネントパラメーターを選択します。

復元するには:

- デリバリーグループ全体とマシンカタログコンポーネント
- 完全なクラウドサイト構成

次の例に従います。

```
Restore-CvadAcToSite   -RestoreFolder   %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

コンポーネントメンバーを復元する

1つ以上のコンポーネントメンバーを復元するには、`IncludeByName`機能を使用します。`Restore`コマンドレットは、選択した単一のコンポーネントとインクルージョンリストとともに`RestoreFolder`パラメーターを指定して呼び出されます。

バックアップから2つのグループポリシーを復元するには、次の例に従います。

```
Restore-CvadAcToSite   -RestoreFolder   %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

```
-GroupPolicies -IncludeByName   Policy1,Policy2
```

```
-DeliveryGroups -MachineCatalogs`
```

サイトをアクティブ化する

サイトのアクティブ化により、アクティブなサイトを制御し、リソースを管理できます。詳細については、「サイトをアクティブ化する」を参照してください。

Cloud構成をオンプレミスへ移行する

この記事では、Cloud構成のバックアップとオンプレミスサイトへの移行について説明します。

構成を移行するための前提条件

- Citrix Virtual Apps and Desktops™オンプレミス環境（少なくとも1つの登録済みVDAがあること）。
- Citrix Virtual Apps and Desktopsオンプレミス環境が以下のいずれかのバージョンで実行されていること：
  - 最新の長期サービスリリース（LTSR）バージョン - 2402。
  - 現在のリリース（CR）バージョンのいずれか - 2308、2311。
- Automated Configuration tool (ACT)コマンドを、.Net 4.7.2以降のバージョンがインストールされたドメイン参加済みマシンで実行します。
- Citrix PowerShell SDKがインストールされたマシン。PowerShell SDKは、Citrix Delivery Controller™のインストール可能ファイルに含まれています。

> **注：**
>
> - 別のマシンでACTを実行している場合は、そのマシンがドメインに参加しており、Studioに適切なPowerShellスナップインがインストールされている必要があります。インストーラーを入手するには、Citrix Virtual Apps and DesktopsダウンロードWebサイトにアクセスしてください。
> - オンプレミスサイトでは、Delivery Controller に ACT をインストールすることをお勧めします。ACT はデスクトップアイコンから起動できます。
> - ACTを標準のPowershellウィンドウから使用する場合は、次のコマンドを実行する必要があります: `Import-Module Citrix.AutoConfig.Commands`

> ACTはシステムPowerShellパスの一部ではないため、明示的にインポートする必要があります

主な手順

クラウド構成をオンプレミスに移行するには、以下の手順に従ってください。

1. クラウド構成のバックアップ
2. YMLファイルを変更する
3. オンプレミスに構成をインポートする

クラウド構成のバックアップ

1. **Automated Configuration** をインストールします。
2. **Auto Config** アイコンをダブルクリックします。PowerShell ウィンドウが表示されます。
3. **CustomerInfo.yml** ファイルを作成するには、`New-CvadAcCustomerInfoFile` を実行します。詳細については、「顧客情報ファイルの入力」を参照してください。
4. クラウド構成のバックアップを作成するには、コマンド `Backup-CvadAcToFile` を実行します。

> **注：**
>
> - 初めてコマンドレットを実行すると、.yml 構成ファイルとログを含むエクスポートフォルダーが作成されます。フォルダーは `%HOMEPATH%\Documents\Citrix\AutoConfig` にあります。
> - エラーまたは例外が発生した場合は、ログファイルの**Fixups**セクションを参照してください。
> - Backup-CvadToFileは、パラメーター `IncludeByName` または `ExcludeByName` をサポートしていません。

> **重要:**
>
> Citrixでは、すべてのコンポーネントをまとめてバックアップすることをお勧めします。

YMLファイルを変更する

次の表に示すように、オンプレミスの詳細を含めるには、`%HOMEPATH%\Documents\Citrix\AutoConfig` にある `.yml` ファイルを変更します。

YMLファイル	パラメーター	説明	例
CustomerInfo.yml	環境	環境をOnPremに変更します。環境パラメーターの値は大文字と小文字を区別します。	

YMLファイル	パラメーター	説明	例
ZoneMapping.yml	DaaS:CVAD	クラウドのリソースロケーションをオンプレミスゾーンにマッピングします。	old:newゾーンの形式である必要があります
CvadAcSecurity.yml	ハイパーバイザー: 接続タイプ: ‘ ‘ ユーザー名: ‘ ’ パスワード: ‘ ‘	ハイパーバイザーのユーザー名とパスワードを追加します。	ハイパーバイザーがXenServerの場合、XenServer: ConnectionType: ‘XenServer’ Username: ‘root’ Password: ‘ ‘

オンプレミスに構成をインポートする

1. 要件に基づいて、オンプレミスサイトで次のいずれかのコマンドを実行します。
    a. `Merge-CvadAcToSite` - オンプレミスサイトが実行中で、クラウド構成をそれにマージしたい場合。
    b. `Import-CvadAcToSite -Environment OnPrem` - オンプレミス構成が利用できない場合で、クラウド構成をインポートして新しいものを作成する場合。

> **重要:**
>
> 競合を避けるため、Citrixでは一度に1つのコンポーネントをインポートすることをお勧めします。

オンプレミス構成をオンプレミスサイトに移行する

この記事では、Automated Configuration Tool (ACT) を使用して、オンプレミス構成をあるオンプレミスサイトから別のオンプレミスサイトに移行する手順について説明します。

要件

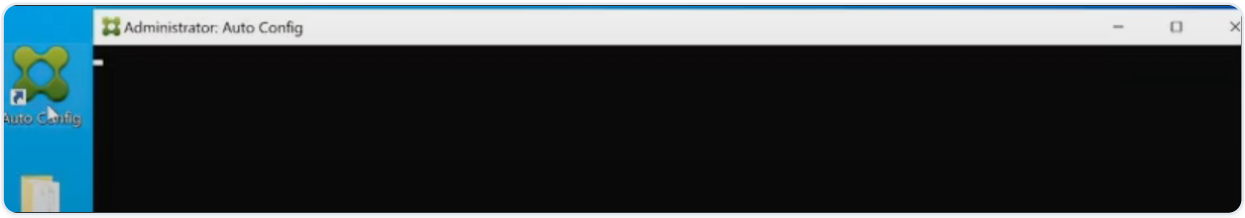
- 両方のオンプレミスサイトが同じドメインに参加している必要があります。
- Citrix Virtual Apps and Desktops™ バージョン 2305 以降を使用してください。

手順

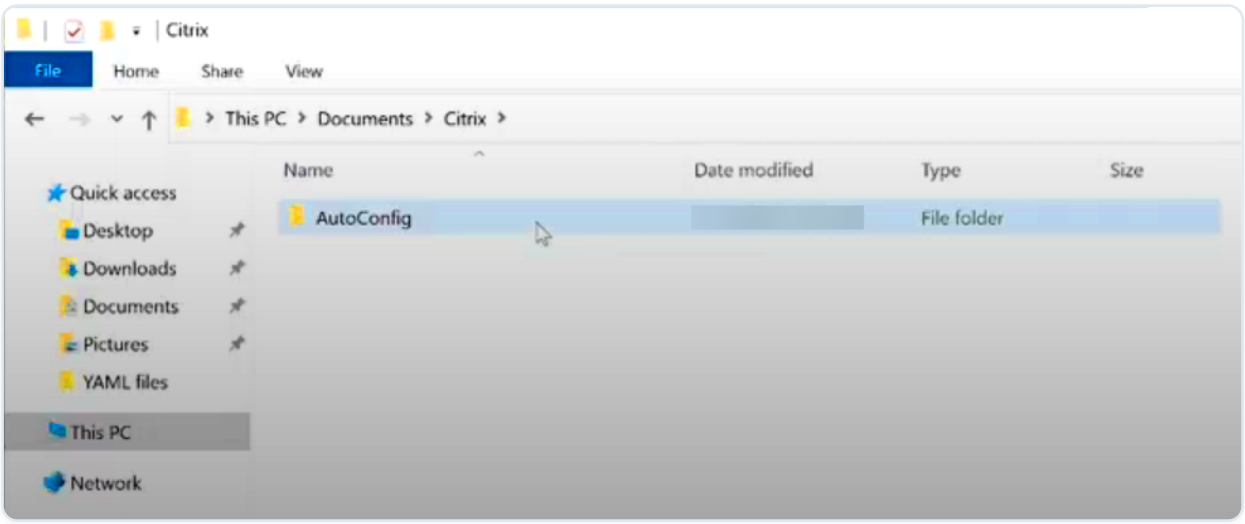
1. Automated Configuration Tool をダウンロードし、システム要件を確認します。「Automated Configuration のダウンロード」を参照してください。
2. ACT を開き、次のコマンドを使用してオンプレミスサイトをエクスポートします。

   ```
   Export-CvadAcToFile
   ```

   移行でサポートされているコンポーネントのリストについては、「サポートされている移行オブジェクト」を参照してください。エクスポートの手順については、「オンプレミス構成のエクスポート」を参照してください。親フォルダー `%HOMEPATH%\\Documents\\Citrix\\AutoConfig` には、常に最新のエクスポートからのエクスポートされたファイルが含まれています。
3. ターゲットサイトで ACT を起動します。`%HOMEPATH%\\Documents\\Citrix` に `AutoConfig` フォルダーが作成されていることを確認する必要があります。

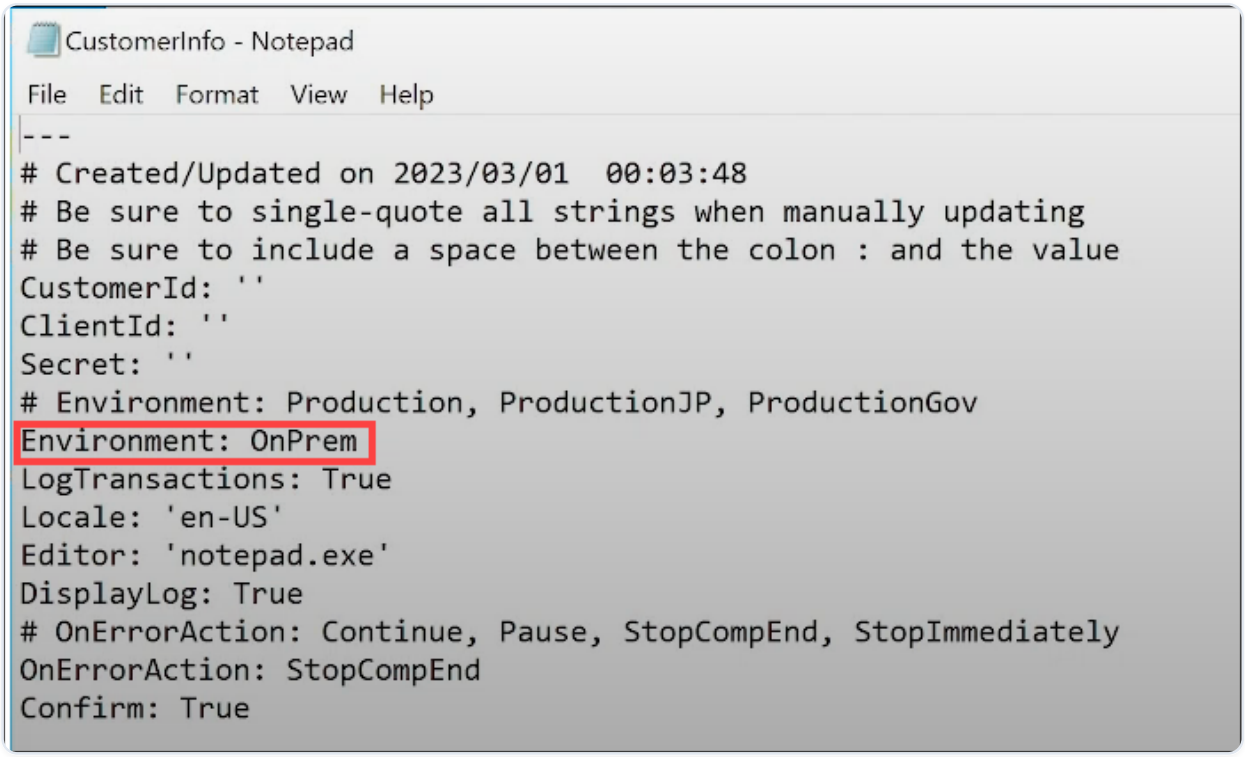
4. ソースサイトの **Export** フォルダーから `.yml` ファイルをターゲットサイトの `%HOMEPATH%\\Documents\\Citrix\\AutoConfig` フォルダーにコピーします。

5. `Set-CvadAcCustomerInfoFile` コマンドを使用して、作業している環境を指定します。例:

   ```
   Set-CvadAcCustomerInfoFile -Environment OnPrem
   ```

このコマンドは、**CustomerInfo** ファイルを環境で更新します。



6. 以下のコマンドを使用して構成ファイルを移行します。

```
Import-CvadAcToFile
```

`AutoConfig` フォルダ以外のフォルダからインポートする場合は、以下を実行します。

```
Import-CvadAcToFile -Sourcefolder PATH
```

注:

ホスト接続を移行する場合は、各ホストタイプの接続情報で `CvadAcSecurity.yml` ファイルを更新します。ホスト接続のセキュリティファイルを更新するを参照してください。

エラーまたは例外が発生した場合は、ログファイルの「Fixups」セクションを参照してください。

7. Web Studioを使用して、構成がターゲットサイトに移行されていることを確認します。

移行のための自動構成ツールコマンドレット

このページには、移行ユースケースのためにツールでサポートされているすべてのコマンドレットとパラメーターがリストされています。

すべてのコマンドレットは、次のいずれかの型のパラメータを受け取ります。

- 文字列
- 文字列のリスト
- ブール値: `$true` または `$false`
- SwitchParameter: パラメーターの存在は `$true` を意味し、パラメーターの不在は `$false` を意味します

注:

SwitchParameter は真偽選択の推奨される方法ですが、レガシーの問題により、ツールでは引き続きブール値が使用されています。

次の表は、すべてのコマンドレットの概要です。各コマンドレットがサポートするパラメータについては、各セクションを参照してください。

カテゴリ	コマンドレット	説明
オンプレミスからクラウドへの移行	`Export-CvadAcToFile`	オンプレミスファイルをYAMLファイルにエクスポートします。
	`Import-CvadAcToSite`	YAMLファイルをクラウドにインポートします。作成、更新、削除の操作をサポートします。
	`Merge-CvadAcToSite`	YAMLファイルをクラウドにインポートします。作成と更新の操作をサポートします。
	`New-CvadAcToSite`	YAMLファイルをクラウドにインポートします。作成と更新の操作をサポートします。

カテゴリ	コマンドレット	説明
	`Sync-CvadAcToSite`	1つのステップでエクスポートとインポートを行います。
	きめ細かな移行 コンポーネントの場合は、上記のコマンドでパラメータを使用します。例: `MachineCatalogs`、`Tags`。コンポーネント名の場合は、上記のコマンドでパラメータを使用します。例: `IncludeByName`、`ExcludeByName`。	コンポーネントまたはコンポーネント名のみを選択的に移行する
クラウドからクラウドへのコマンドレット	`Backup-CvadAcToFile`	クラウドサイトからすべての構成をバックアップします。
	`Restore-CvadAcToSite`	バックアップされたYAMLファイルをクラウドサイトに復元します。このクラウドサイトは、ソースのクラウドサイトと同じでも異なっていてもかまいません。
	`Remove-CvadAcFromSite`	クラウドからコンポーネントメンバーを削除します。
	きめ細かな移行 コンポーネントの場合は、上記のコマンドでパラメーターを使用します。例: `MachineCatalogs`、`Tags`。コンポーネント名の場合は、上記のコマンドでパラメーターを使用します。例: `IncludeByName`、`ExcludeByName`。	コンポーネントまたはコンポーネント名のみを選択的に移行する
その他の基本コマンドレット	`Compare-CvadAcToSite`	オンプレミスの.ymlファイルをクラウド構成と比較します。

カテゴリ	コマンドレット	説明
前提条件関連のコマンドレット	`New-CvadAcCustomerInfoFile`	顧客情報ファイルを作成します。
	`Set-CvadAcCustomerInfoFile`	既存の顧客情報ファイルを更新します。
サポートおよびトラブルシューティングのコマンドレット	`New-CvadAcZipInfoForSupport`	すべてのログファイルと.ymlファイルを単一のzipファイルに圧縮し、サポートのためにCitrix®に送信します。
	`Get-CvadAcStatus`	接続をテストし、すべての前提条件が満たされていることを確認するために使用します。ツールに関する情報（バージョン番号、クラウドとの接続、コネクタの状態など）を返します。
	`Test-CvadAcConnectionWithSite`	クラウドサイトとの接続をテストします。
	`Find-CvadAcConnector`	既存のコネクタを特定し、その実行状態を判断します。
	`Get-CvadAcCustomerSites`	すべての顧客サイトのリストを返します。
	`New-CvadAcTemplateToFile`	選択したコンポーネントのテンプレートファイルを作成します。
	`Show-CvadAcDocument`	このドキュメントをデフォルトのブラウザに表示します。
	`Find-CvadAcInFile`	「ファイル内検索」は、ワイルドカードを含む可能性のある1つ以上の名前に一致するメンバーを探して、コンポーネントのYAMLファイルを検索します。

カテゴリ	コマンドレット	説明
サイトアクティベーションコマンドレット(#site-activation-cmdlets)	`Set-CvadAcSiteActiveStateOnPrem`	オンプレミスサイトの状態をアクティブまたは非アクティブに設定します。
	`Set-CvadAcSiteActiveStateCloud`	クラウドサイトの状態をアクティブまたは非アクティブに設定します。
複数のオンプレミスサイトをマージするコマンドレット(#merging-multiple-on-premises-sites-cmdlets)	`New-CvadAcSiteMergingInfo`	サイトマージのプレフィックス/サフィックス情報セットを作成します。
	`Set-CvadAcSiteMergingInfo`	既存のサイトマージのプレフィックス/サフィックス情報セットを更新します。
	`Remove-CvadAcSiteMergingInfo`	既存のサイトマージのプレフィックス/サフィックス情報セットを削除します。

パラメーターとその使用方法の詳細については、「きめ細かな移行パラメーター」を参照してください。

基本的なコマンドレット

オンプレミスからクラウドへのコマンドレット

- `Export-CvadAcToFile` - オンプレミスファイルをYAMLファイルにエクスポートします。

  オンプレミス設定から構成をエクスポートします。これは、自動構成のデフォルトのエクスポート操作です。オンプレミスサイトの構成には変更が加えられません。エクスポートされたファイルは、一意の名前が付けられた **Export** サブフォルダー内のディレクトリ *%HOMEPATH%\Documents\Citrix\AutoConfig* に配置されます。フォルダー *%HOMEPATH%\Documents\Citrix\AutoConfig* には、常に最新のエクスポートされたオンプレミスサイト構成が含まれています。

  パラメーター:

名前	説明	必須ですか?	タイプ
コンポーネントによる移行	を参照してください(#migrate-by-components)		SwitchParameters
オブジェクト名によるフィルタリング	「オブジェクト名によるフィルタリング」を参照してください(#filtering-by-object-names)		文字列のリスト
`TargetFolder`	エクスポート先のフォルダーを指定します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`AdminAddress`	エクスポートがDelivery Controllerで実行されていない場合に、Delivery ControllerのDNSまたはIPアドレスを指定します。		文字列
`CheckUserAndMachines`	ユーザーとマシンがActive Directoryに存在するかどうかを確認します。Active Directoryに存在しないユーザーとマシンは、インポートの失敗につながる可能性があります。		`$true` または `$false`

名前	説明	必須ですか?	タイプ
`ZipResults`	バックアップされたYAMLファイルを単一のzipファイルに圧縮します。このファイルは、バックアップされたYAMLファイルと同じフォルダーにあり、フォルダーと同じ名前を持ちます。		SwitchParameter

戻り値:

- Cmdlet の戻り値 を参照してください

データをクラウドにインポートする方法は3つあります。特定のコマンドレットを実行すると、クラウドサイトで次の3つのアクションの組み合わせのいずれかが実行されます。

- 追加、更新、および削除
- 追加と更新のみ
- 追加のみ

コマンドレット	追加	更新	削除
インポート	X	X	X
マージ	X	X	
新規	X		

- `Import-CvadAcToSite` - YAMLファイルをクラウドにインポートします。作成、更新、削除操作をサポートします。

  すべてのオンプレミスファイルをクラウドにインポートします。このコマンドは、クラウドの最終状態がオンプレミスの状態と同一であることを保証します。このオプションは、クラウドに存在する変更をすべて削除します。インポートされたサイト構成ファイルは、*%HOMEPATH%\Documents\Citrix\AutoConfig* から取得されます。*注意して使用してください。*

パラメーター:

名前	説明	必須？	種類
コンポーネントごとの移行	コンポーネントごとの移行を参照してください。		SwitchParameters
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリングを参照してください。		文字列のリスト
クラウドアクセスパラメータ	クラウドアクセスパラメーターを参照してください。		SwitchParameters
`SourceFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代替ルートフォルダーを識別します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ出力を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには `$false` に設定します。		`$true` or `$false`
`Merge`	`$true` に設定すると、クラウドサイトにコンポーネントのみを追加します。コンポーネントは削除されません。コン		`$true` or `$false`

名前	説明	必須？	種類
	ポーネントを削除するには`$false`に設定します。		
`AddOnly`	`$true`に設定すると、新しいコンポーネントのみを追加し、既存のコンポーネントを更新または削除しません。更新と削除を許可するには`$false`に設定します。このパラメーターが`$true`の場合、`Merge`は無視されます。		`$true` or `$false`
`MergePolicies`	ポリシー設定とフィルターをマージします。マージは、インポートされるポリシーがクラウドDDCに既に存在する場合にのみ行われます。ポリシーをマージした結果、クラウドDDCポリシーには、既存の設定とフィルターに加えて、インポートされる新しい設定とフィルターが含まれます。設定とフィルターの競合が発生した場合、インポートされた値が優先されることに注意してください。		SwitchParameter

名前	説明	必須？	種類
`OnErrorAction`	OnErrorAction parameterを参照してください。		文字列

戻り値:

- Cmdlet の戻り値 を参照してください

- `Merge-CvadAcToSite` - YAMLファイルをクラウドにインポートします。作成および更新操作をサポートします。

  オンプレミスファイルをクラウドにマージしますが、クラウドまたはオンプレミスサイトのコンポーネントを削除することは*ありません*。これにより、クラウドで既に行われた変更が保持されます。Citrix Cloudに同じ名前のコンポーネントが存在する場合、このコマンドはそのコンポーネントを変更できます。これは、自動構成のデフォルトのインポート操作です。マージされたサイト構成ファイルは、*%HOMEPATH%\Documents\Citrix\AutoConfig*から取得されます。

  パラメーター:

名前	説明	必須ですか？	種類
コンポーネントによる移行	コンポーネントによる移行を参照してください。		スイッチパラメーター
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリングを参照してください。		文字列のリスト
クラウドアクセスパラメーター	クラウドアクセスパラメーターを参照してください。		スイッチパラメーター
`SourceFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代替ルートフォルダーを識別します。		文字列

名前	説明	必須ですか？	種類
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true` または `$false`
`Merge`	`$true` に設定すると、クラウドサイトにコンポーネントを追加するだけです。コンポーネントは削除されません。コンポーネントを削除するには、`$false` に設定します。		`$true` または `$false`
`AddOnly`	`$true` に設定すると、新しいコンポーネントのみを追加し、既存のコンポーネントを更新または削除しません。更新と削除を許可するには、`$false` に設定します。このパラメーターが `$true` の場合、`Merge` は無視されます。		`$true` または `$false`
`MergePolicies`	ポリシー設定とフィルターをマージします。マージは、イン		SwitchParameter

名前	説明	必須ですか？	種類
	ポートされるポリシーがクラウドDDCに既に存在する場合にのみ行われます。ポリシーをマージした結果、クラウドDDCポリシーには、既存の設定とフィルターに加えて、インポートされる新しい設定とフィルターが含まれます。設定とフィルターの競合が発生した場合、インポートされた値が優先されることに注意してください。		
`OnErrorAction`	を参照してください(/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/auto-config-troubleshoot#onerroraction-parameter)。		文字列

戻り値:

- Cmdlet の戻り値を参照してください

- `New-CvadAcToSite` - YAML ファイルをクラウドにインポートします。作成および更新操作をサポートします。

  オンプレミスサイト構成をクラウドにインポートしますが、新しいコンポーネントのみを追加します。既存のクラウドサイトコンポーネントは更新も削除もされません。既存のクラウドサイトコンポーネントを変更しない必要がある場合は、このコマンドを使用してください。

  パラメーター:

名前	説明	必須ですか?	タイプ
コンポーネントによる移行	コンポーネントによる移行を参照してください。		SwitchParameters
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリングを参照してください。		文字列のリスト
クラウドアクセスパラメーター	クラウドアクセスパラメーターを参照してください。		SwitchParameter
`SourceFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代替ルートフォルダーを識別します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true` または `$false`
`OnErrorAction`	を参照してください (/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/auto-config-troubleshoot#onerro		文字列

名前	説明	必須ですか?	タイプ
	raction-parameter)。		

戻り値:

- を参照してください(#cmdlet-return-values)

- `Sync-CvadAcToSite` - 1つのステップでエクスポートとインポートを実行します。

同期は、エクスポートとインポートの両方を1つのステップで実行します。エクスポート/インポートの保存先フォルダーを指定するには、`SourceTargetFolder`パラメーターを使用します。

パラメーター:

名前	説明	必須ですか？	型
コンポーネントによる移行	を参照してください(#migrate-by-components)		SwitchParameters
オブジェクト名によるフィルタリング	「オブジェクト名によるフィルタリング」を参照してください(#filtering-by-object-names)		文字列のリスト
クラウドアクセスパラメータ	「クラウドアクセスパラメータ」を参照してください(#cloud-accessing-parameters)		SwitchParameters
`SourceTargetFolder`	エクスポート/インポートの保存先フォルダーを指定します。		文字列
`Locale`	エクスポート可能な人間が判読できるテ		文字列

名前	説明	必須ですか？	型
	キストの言語を指定します。		
`AdminAddress`	エクスポートがデリバリーコントローラーで実行されていない場合に、デリバリーコントローラーのDNSまたはIPアドレスを指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true` または `$false`
`Merge`	`$true` に設定すると、クラウドサイトにコンポーネントのみを追加します。コンポーネントは削除されません。コンポーネントを削除するには、`$false` に設定します。		`$true` または `$false`
`AddOnly`	`$true` に設定すると、新しいコンポーネントのみを追加し、既存のコンポーネントを更新または削除しません。更新と削除を許可するには、`$false` に設定します。このパラ		`$true` または `$false`

名前	説明	必須ですか？	型
	メーターが `$true` の場合、 `Merge` は無視されます。		
`MergePolicies`	ポリシー設定とフィルターをマージします。マージは、インポートされるポリシーがクラウドDDCに既に存在する場合にのみ行われます。ポリシーをマージした結果、クラウドDDCポリシーには、既存の設定とフィルターに加えて、インポートされる新しい設定とフィルターが含まれます。設定とフィルターの競合が発生した場合、インポートされた値が優先されることに注意してください。		SwitchParameter

戻り値:

- Cmdlet の戻り値を参照してください

クラウドからクラウドへのコマンドレット

- `Backup-CvadAcToFile` - クラウドサイトからすべての構成をバックアップします。

  クラウド構成を.ymlファイルにエクスポートします。このバックアップは、失われたコンポーネントを復元するためのバックアップおよび復元プロセスで使用できます。

  パラメーター:

名前	説明	必須?	種類
コンポーネントによる移行	コンポーネントによる移行を参照してください		SwitchParameters
クラウドアクセスパラメーター	クラウドアクセスパラメーターを参照してください。		SwitchParameters
`TargetFolder`	エクスポート先のフォルダーを指定します。		文字列
`Locale`	エクスポートできる人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ出力を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。`$false`に設定すると、ログの表示が抑制されます。		`$true`または`$false`
`ZipResults`	YAMLファイルのバックアップを単一のzipファイルに圧縮します。このファイルは、バックアップされたYAMLファイルと同じフォルダーにあり、フォルダーと同じ名前です。		SwitchParameter

戻り値:

- Cmdlet の戻り値 を参照してください

- `Restore-CvadAcToSite` - バックアップされたYAMLファイルをクラウドサイトに復元します。このクラウドサイトは、ソースクラウドサイトと同じでも異なっていてもかまいません。

  クラウドサイトを以前の構成に復元します。インポートされるファイルは、`-RestoreFolder` パラメーターを使用して指定されたフォルダーから取得されます。このパラメーターは、クラウドサイトに復元する.ymlファイルを含むフォルダーを識別します。これは完全修飾フォルダー指定である必要があります。このコマンドレットは、以前の構成に戻すため、またはクラウドサイトのバックアップと復元のために使用できます。このコマンドは、クラウドサイトの追加、削除、更新を行うことができます。

  パラメーター:

名前	説明	必須?	種類
コンポーネントによる移行	コンポーネントによる移行を参照してください。		SwitchParameters
オブジェクト名によるフィルタリング	「オブジェクト名によるフィルタリング」を参照してください(#filtering-by-object-names)。		文字列のリスト
クラウドアクセスパラメーター	「クラウドアクセスパラメーター」を参照してください(#cloud-accessing-parameters)。		SwitchParameter
`RestoreFolder`	クラウドサイトに復元する.ymlファイルを含むフォルダーを識別します。これは完全修飾フォルダー指定である必要があります。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列

名前	説明	必須?	種類
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true` または `$false`
`Merge`	`$true` に設定すると、クラウドサイトにコンポーネントのみを追加します。コンポーネントは削除されません。コンポーネントを削除するには、`$false` に設定します。		`$true` または `$false`
`AddOnly`	`$true` に設定すると、新しいコンポーネントのみを追加し、既存のコンポーネントを更新または削除しません。更新と削除を許可するには、`$false` に設定します。このパラメーターが `$true` の場合、`Merge` は無視されます。		`$true` または `$false`
`MergePolicies`	ポリシー設定とフィルターをマージします。マージは、インポートされるポリシーがクラウドDDCに既に存在する場合にのみ行われます。ポリシーを		SwitchParameter

名前	説明	必須?	種類
	マージした結果、クラウドDDCポリシーには、既存の設定とフィルターに加えて、インポートされる新しい設定とフィルターが含まれます。設定とフィルターの競合が発生した場合、インポートされた値が優先されることに注意してください。		
`OnErrorAction`	OnErrorAction パラメーターを参照してください。		文字列

戻り値:

- コマンドレットの戻り値(#cmdlet-return-values)を参照してください

- `Remove-CvadAcFromSite` – クラウドからコンポーネントメンバーを削除します。

  サイト全体をリセットしたり、コンポーネントからメンバー項目を削除したりできます（例：カタログのリストから1つのマシンカタログを削除する）。これは、`IncludeByName` パラメーターと組み合わせて使用することで、特定のメンバーを選択的に削除できます。

  パラメーター:

名前	説明	必須?	種類
コンポーネントによる移行	コンポーネントによる移行(#migrate-by-components)を参照してください		SwitchParameters
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリング(#filtering-by-object-		文字列のリスト

名前	説明	必須?	種類
	names)を参照してください		
クラウドアクセスパラメーター	「クラウドアクセスパラメータ」を参照してください(#cloud-accessing-parameters)		SwitchParameters
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false`に設定します。		`$true` または `$false`

戻り値:

- 「コマンドレットの戻り値」を参照してください(#cmdlet-return-values)

その他の基本コマンドレット

- `Compare-CvadAcToSite` - オンプレミスの.ymlファイルをクラウド構成と比較し、`Import`、`Merge`、または`Restore`コマンドレットによって行われた変更のレポートを作成します。

  パラメータ:

名前	説明	必須ですか？	種類
コンポーネントごとに移行	コンポーネントごとに移行を参照してください。		SwitchParameters
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリングを参照してください。		文字列のリスト

名前	説明	必須ですか？	種類
クラウドアクセスパラメーター	クラウドアクセスパラメーターを参照してください。		SwitchParameters
`SourceFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代替ルートフォルダーを識別します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false`に設定します。		`$true` または `$false`
`Merge`	`$true`に設定すると、クラウドサイトにコンポーネントのみを追加します。コンポーネントは削除されません。コンポーネントを削除するには、`$false`に設定します。		`$true` または `$false`
`AddOnly`	`$true`に設定すると、新しいコンポーネントのみを追加し、既存のコンポーネントを更新または削除しません。更新		`$true` または `$false`

名前	説明	必須ですか？	種類
	と削除を許可するには、`$false`に設定します。このパラメーターが`$true`の場合、`Merge`は無視されます。		
`OnErrorAction`	「OnErrorAction parameter」を参照してください。		文字列

戻り値:

- 「Cmdlet return values」を参照してください

- `Remove-CvadAcFromSite` – クラウドからコンポーネントメンバーを削除します。

  サイト全体をリセットしたり、コンポーネントからメンバー項目を削除したりできます (たとえば、カタログのリストから1つのマシンカタログを削除する場合など)。これは、`IncludeByName`パラメーターと組み合わせて使用すると、特定のメンバーを選択的に削除できます。

サポートするコマンドレットで、以下のコンポーネントを指定できます。コンポーネントパラメーターが指定されていない場合、`All`オプションが自動的に選択されます。エラーを回避するため、コンポーネントを次の順序で移行することをお勧めします。

- `All`
- `Tags`
- `AdminRoles`
- `AdminScopes`
- `HostConnections`
- `MachineCatalogs`
- `StoreFronts`
- `DeliveryGroups`
- `ApplicationGroups`
- `ApplicationFolders`

- `Applications`
- `GroupPolicies`
- `UserZonePreference`

オブジェクト名によるフィルタリング

コンポーネント名による移行

`IncludeByName` および `ExcludeByName` パラメーターを使用すると、名前でコンポーネントメンバーをコマンドレットに含めたり除外したりできます。サポートされているコマンドレットでは、一度に1つのコンポーネント（たとえば、デリバリーグループ）のみを選択できます。コンポーネントメンバーが両方の領域にある場合、除外は他のすべてのパラメーターを上書きし、除外されたコンポーネントとメンバー名を識別するエントリがログ修正リストに作成されます。

`IncludeByName`と`ExcludeByName`は、コンポーネントメンバー名のリストを受け取ります。任意の名前には、1つ以上のワイルドカードを含めることができます。2種類のワイルドカードがサポートされています。メンバー名に特殊文字が含まれている場合、コンポーネントメンバー名のリストは単一引用符で囲む必要があります。

- * 任意の数の文字に一致します
- ？1つの文字に一致します

`IncludeByName` および `ExcludeByName` は、各メンバーが明示的であるかワイルドカードを含むメンバーのリストを含むファイルを受け取ることもできます。ファイルの各行には1つのメンバーを含めることができます。メンバー名から先頭と末尾のスペースはトリミングされます。ファイル名の前には @ 記号を付け、単一引用符で囲む必要があります（@ が再解釈されないようにするための PowerShell の要件）。複数のファイルを、メンバー名と混在させてリストすることもできます。

名前が`DgSite1`で始まり、`Home2`を含むすべてのデリバリーグループをマージする例は、次のように記述されます。

```
Merge-CvadAcToSite –DeliveryGroups –IncludeByName DgSite1*,*Home2*
```

デリバリーグループ名別

`ByDeliveryGroupName` は、アプリケーションおよびアプリケーショングループのデリバリーグループ名でフィルタリングします。このパラメータは、デリバリーグループの関連付けに基づいて含めるメンバーを識別する包含リストです。

`ByDeliveryGroupName` は、デリバリーグループ名のリストを受け取ります。任意の名前には、1つ以上のワイルドカードを含めることができます。2種類のワイルドカードがサポートされています。

- * は任意の数の文字に一致します
- ? は単一の文字に一致します

次の例では、`EastDg` で始まるすべてのデリバリーグループ名を参照するすべてのアプリケーションをマージします。

```
Merge-CvadAcToSite –Applications –ByDeliveryGroupName EastDg*
```

無効なものを除外

`ExcludeDisabled` は、無効になっているすべてのアプリケーションおよびアプリケーショングループをインポート操作から除外します。`ExcludeDisabled` のデフォルトは `false` であり、これは、有効化されているかどうかにかかわらず、すべてのアプリケーションとアプリケーショングループがインポートされることを意味します。

マシン名別

`ByMachineName` は、マシンカタログおよびデリバリーグループのマシン名でフィルタリングします。このパラメータは、マシン名の関連付けに基づいて含めるメンバーを識別する包含リストです。

`ByMachineName` は、マシン名のリストを受け取ります。任意の名前には、1つ以上のワイルドカードを含めることができます。2種類のワイルドカードがサポートされています。

- * は任意の数の文字に一致します
- ? は単一の文字に一致します

エクスポートまたはインポート時に `ByMachineName` を使用し、マシン名フィルターによってマシンカタログまたはデリバリーグループにマシンが存在しない場合、そのマシンカタログまたはデリバリーグループはエクスポートまたはインポートから除外されます。

> **注:**
>
> `ByMachineName` をインポートタイプのコマンドレットで使用すると、`MergeMachines` が `$true` に設定されます。

マシンのマージ

`MergeMachines` を `$true` に設定すると、インポート操作はマシンをマシンカタログまたはデリバリーグループにのみ追加するように指示されます。マシンは削除されないため、増分追加操作が可能です。

`MergeMachines` はデフォルトで false であり、マシンカタログまたはデリバリーグループの .yml ファイルに存在しないマシンは削除されることを意味します。`MergeMachines` は `ByMachineName` が使用されると `$true` に設定されますが、`MergeMachines` を false に設定することで上書きできます。

前提条件関連のコマンドレット

- `New-CvadAcCustomerInfoFile` - 顧客情報ファイルを作成します。デフォルトでは、顧客情報ファイルは *%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。

  パラメーター:

名前	説明	必須？	タイプ
`CustomerId`	顧客ID。	x	文字列
`ClientId`	Citrix Cloud で作成された顧客のクライアント ID。このパラメーターを使用する場合は、CustomerId と Secret を指定する必要があります。	条件付き	文字列
`Secret`	Citrix Cloud で作成された顧客のシークレットキー。このパラメーターを使用する場合は、CustomerId と ClientId を指定する必要があります。	条件付き	文字列
`Environment`	Production、ProductionGov、ま		列挙

名前	説明	必須？	タイプ
	たはProductionJP環境。		
`LogFileName`	ログファイルプレフィックスをCitrixLogから別のものに変更します。		文字列
`AltRootUrl`	Citrixの指示の下でのみ使用してください。		文字列
`StopOnError`	最初のエラーで操作を停止します。		`$true` or `$false`
`TargetFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代わりに、指定されたフォルダーをルートフォルダーとして使用します。		文字列
`Locale`	ツールが実行されているシステムから派生したロケールの代わりに、指定されたロケールを使用します。		文字列
`Editor`	各コマンドレットの完了時にログを表示するために、指定されたエディターを使用します。Notepad.exeがデフォルトのエディターです。このパラメーターには、エディターへの完全修飾ファイル指定を含める必要があり、エ		文字列

名前	説明	必須？	タイプ
	ディターはログファイル指定を唯一のパラメーターとして受け取る必要があります。		
`SecurityCsvFileSpec`	Citrix Identity and Access Management からダウンロードした SecurityClient.csv ファイルを指す完全修飾ファイル指定。このパラメーターを使用する場合は、CustomerId を指定する必要があります。		文字列

戻り値:

- コマンドレットの戻り値を参照してください

- `Set-CvadAcCustomerInfoFile` - 既存の顧客情報ファイルを更新します。コマンドレットで指定されたパラメーターのみが変更されます。CustomerInfo.yml ファイル内の指定されていないパラメーター値はすべて変更されません。

  パラメーター:

名前	説明	必須？	タイプ
`CustomerId`	顧客のID。		文字列
`ClientId`	Citrix Cloud で作成された顧客のクライアントID。		文字列
`Secret`	Citrix Cloudで作成された顧客のシークレットキー。		文字列

名前	説明	必須？	タイプ
`Environment`	Production、ProductionGov、またはProductionJP環境。		列挙
`LogFileName`	ログファイルプレフィックスをCitrixLogから別のものに変更します。		文字列
`StopOnError`	最初のエラーで操作を停止します。		`$true` または `$false`
`TargetFolder`	ルートフォルダーとして、*%HOMEPATH%\Documents\Citrix\AutoConfig* の代わりに指定されたフォルダーを使用します。		文字列
`Locale`	ツールが実行されているシステムから派生したロケールの代わりに、指定されたロケールを使用します。		文字列
`Editor`	各コマンドレットの完了時にログを表示するために、指定されたエディターを使用します。Notepad.exeがデフォルトのエディターです。このパラメーターには、エディターへの完全修飾ファイル指定を含める必要があり、エディターはログファ		文字列

名前	説明	必須？	タイプ
	イル指定を唯一のパラメーターとして受け取る必要があります。		
`SecurityCsvFileSpec`	Citrix Identity and Access Managementからダウンロードされた SecurityClient.csv ファイルを指す完全修飾ファイル指定。このパラメーターを使用する場合、CustomerIdを指定する必要があります。		文字列

戻り値:

- コマンドレットの戻り値を参照してください

前提条件関連のパラメーター

クラウドアクセスパラメーターとともに、前提条件関連のコマンドレットで以下のパラメーターを使用できます。

- `Environment` – ProductionまたはProductionGov環境。
- `LogFileName` – ログファイルプレフィックスをCitrixLogから別のものに変更します。
- `StopOnError` – 最初のエラーで操作を停止します。
- `AlternateRootFolder` – *%HOMEPATH%\Documents\Citrix\AutoConfig* の代わりに、指定されたフォルダーをルートフォルダーとして使用します。
- `Locale` – ツールが実行されているシステムから派生したロケールの代わりに、指定されたロケールを使用します。
- `Editor` – 各コマンドレットの完了時にログを表示するために、指定されたエディターを使用します。Notepad.exe がデフォルトのエディターです。このパラメーターには、エディターへの完全修飾ファイル指定を含める必要があり、エディターはログファイル指定を唯一のパラメーターとして受け取る必要があります。

サポートおよびトラブルシューティングコマンドレット

- `New-CvadAcZipInfoForSupport` - すべてのログファイルと.ymlファイルを1つのzipファイルに圧縮し、サポートのためにCitrixに送信します。顧客の機密情報（CustomerInfo.ymlおよびCvadAcSecurity.yml）はzipに含まれません。Icon.ymlファイルもサイズが大きいため除外されます。zipファイルは *%HOMEPATH%\Documents\Citrix\AutoConfig* に配置され、日付とタイムスタンプに基づいて *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip* という名前が付けられます。このzipファイルはバックアップとしても機能します。

  パラメーター:

名前	説明	必須?	型
`TargetFolder`	zipファイルを作成して保存するターゲットフォルダーを指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter

  戻り値:

  - zipファイル名と場所を含むzipファイルがコマンドプロンプトに表示されます。

- `Get-CvadAcStatus` - 接続をテストし、すべての前提条件が満たされていることを確認するために使用します。ツールに関する情報（バージョン番号、クラウドとの接続、コネクターステータスなど）を返します。

  パラメーター:

名前	説明	必須ですか？	種類
クラウドアクセスパラメータ	クラウドアクセスパラメータを参照してください。		SwitchParameters
`SiteId`	接続先のサイトを識別します。		文字列
`AdminAddress`	これは、管理者のアクセスレベルを確認するために使用され		文字列

名前	説明	必須ですか？	種類
	るオンプレミスのDelivery ControllerのDNSまたはIPアドレスです。ツールがDelivery Controllerで実行されていない場合に必要です。		

戻り値:

- 各項目の結果を表示します。

- `Test-CvadAcConnectionWithSite` – クラウドサイトとの接続をテストし、通信接続が機能していることを確認します。このコマンドレットは、クラウドアクセスパラメータまたはCustomerInfo.ymlファイルを使用して、顧客の接続情報を指定します。

  パラメーター:

名前	説明	必須ですか？	タイプ
クラウドアクセスパラメーター	クラウドアクセスパラメーターを参照してください。		スイッチパラメータ
`Quiet`	コンソールへのログ出力を抑制します。		スイッチパラメータ

  戻り値:

  - テスト結果はコマンドラインに表示されます。

- `Find-CvadAcConnector` - 既存のコネクタを特定し、その実行状態を判断します。このコマンドレットは、CustomerInfo.yml ファイルまたは顧客 ID パラメータからの情報を使用して、顧客のコネクタを特定します。

  パラメータ:

名前	説明	必須?	タイプ
`CustomerInfoFileSpec`	デフォルトの場所と名前を上書きするための顧客情報ファイルを指すファイル指定。このパラメータは、`CustomerId` パラメータが指定されている場合は無視されます。		文字列
`CustomerId`	顧客のID。このパラメーターは、CustomerInfo.yml ファイル内の同じ値を上書きします。		文字列

戻り値:

- 結果はコマンドラインに表示されます。

- `Get-CvadAcCustomerSites` - すべての顧客サイトのリストを返します。このコマンドレットは、クラウドアクセスパラメータまたは CustomerInfo.yml ファイルを使用して、顧客の接続情報を指定します。

  パラメーター:

  - を参照してください(#cloud-accessing-parameters)

  戻り値:

  - 見つかった顧客サイトIDのリストを表示します。

- `New-CvadAcTemplateToFile` – 選択したコンポーネントのテンプレートファイルを作成し、手動でインポートファイルを作成できるようにします。

  パラメーター:

名前	説明	必須？	タイプ
コンポーネントによる移行	コンポーネントによる移行を参照		SwitchParameters

名前	説明	必須？	タイプ
`TargetFolder`	エクスポート先のフォルダーを指定します。		文字列

戻り値:

- コマンドレットの戻り値を参照

- `Show-CvadAcDocument` - このドキュメントをデフォルトのブラウザに表示します。

  パラメーター:

  - なし。

  戻り値:

  - このWebページをデフォルトのWebブラウザに表示します。

- `Find-CvadAcInFile` - ファイル内検索は、ワイルドカードを含む1つ以上の名前に一致するメンバーを検索するために、コンポーネントのYAMLファイルを検索します。結果は、見つかったメンバーのレポートです。ファイル内検索は、一度に1つのコンポーネントしか検索できません。ファイル内検索は、現在のフォルダーとすべてのサブフォルダー内のすべてのYAMLファイルを検索します。検索するファイルの数を制限するには、`FindSourceFolder`を使用します。

  パラメーター:

名前	説明	必須?	種類
コンポーネントによる移行	コンポーネントによる移行を参照してください。注: `-All`の値は無効です。		SwitchParameters
`IncludeByName`	サイトのアクティブ状態をアクティブに設定する際に含めるデリバリーグループの名前を指定するリスト。「*」と「?」のワイルドカードが		文字列のリスト

名前	説明	必須?	種類
	名前にサポートされています。		
`Unique`	一意に見つかったメンバーのみを報告します。		SwitchParameter
`IncludeYaml`	メンバー固有のYAMLを含めます。		SwitchParameter
`FindSourceFolder`	検索を開始するフォルダー。		文字列
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		SwitchParameter
`Quiet`	コンソールへのログ出力を抑制します。		SwitchParameter

戻り値:

- 指定されたコンポーネントの検出されたメンバーを含むレポートを作成します。

サイトアクティベーションコマンドレット

サイトのアクティベーションとこれらのコマンドレットの使用方法の詳細については、「サイトのアクティベーション」を参照してください。

- `Set-CvadAcSiteActiveStateOnPrem` - オンプレミスサイトの状態をアクティブまたは非アクティブに設定します。

  パラメーター:

名前	説明	必須?	タイプ
クラウドアクセスパラメーター	クラウドアクセスパラメーターを参照		スイッチパラメーター

名前	説明	必須?	タイプ
`SiteActive`	存在する場合、オンプレミスサイトをアクティブに設定し、すべてのデリバリーグループからメンテナンスモードを削除します。このパラメーターが存在しない場合、すべてのデリバリーグループでメンテナンスモードが設定されます。		SwitchParameter
`IncludeByName`	サイトのアクティブ状態をアクティブに設定する際に含めるデリバリーグループの名前を指定するリスト。名前に「*」と「?」のワイルドカードがサポートされています。		文字列のリスト
`ExcludeByName`	サイトのアクティブ状態をアクティブに設定する際に除外するデリバリーグループの名前を指定するリスト。「*」と「?」のワイルドカードが名前にサポートされています。		文字列のリスト
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには		`$true or $false`

名前	説明	必須?	タイプ
	`$false` に設定します。		

戻り値:

- コマンドレットの戻り値 を参照してください。

- `Set-CvadAcSiteActiveStateCloud` - クラウドサイトの状態をアクティブまたは非アクティブのいずれかに設定します。

  パラメーター:

名前	説明	必須？	タイプ
クラウドアクセスパラメーター	クラウドアクセスパラメーターを参照		SwitchParameters
`SiteActive`	このパラメーターが存在する場合、クラウドサイトをアクティブに設定し、すべてのデリバリーグループからメンテナンスモードを解除します。このパラメーターが存在しない場合、すべてのデリバリーグループにメンテナンスモードが設定されます。		SwitchParameter
`IncludeByName`	サイトのアクティブ状態をアクティブに設定する際に含めるデリバリーグループの名前を指定するリスト。名前に「*」と「?」のワイルドカードがサポートされています。		文字列のリスト

名前	説明	必須？	タイプ
`ExcludeByName`	サイトのアクティブ状態をアクティブに設定する際に除外するデリバリーグループの名前を指定するリスト。名前に「*」と「?」のワイルドカードがサポートされています。		文字列のリスト
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true or $false`

戻り値:

- コマンドレットの戻り値 を参照してください。

複数のオンプレミスサイトをマージするコマンドレット

サイトのマージとこれらのコマンドレットの使用方法の詳細については、複数のサイトを単一のサイトにマージする を参照してください。

- `New-CvadAcSiteMergingInfo` - サイトマージのプレフィックス/サフィックス情報セットを作成します。最初からすべてのプレフィックスまたはサフィックスを知っている必要はありません。これらは `Set-CvadAcSiteMergingInfo` で、または SiteMerging.yml ファイルを手動で編集することで更新できます。 パラメーター:

名前	説明	必須ですか？	タイプ
`SiteName`	特定のサイトのプレフィックス/サフィックスのセットを識別するために使用される名前。実際	x	文字列

名前	説明	必須ですか？	タイプ
	のサイト名と一致してもよいし、一致しなくてもよい。		
サイト統合パラメータ	サイト統合パラメータを参照してください。		SwitchParameters
`Quiet`	コンソールへのログ出力を抑制します。		SwitchParameter

戻り値:

- なし

- `Set-CvadAcSiteMergingInfo` - 既存のサイト統合プレフィックス/サフィックス情報セットを更新します。

  パラメーター:

名前	説明	必須?	種類
`SiteName`	特定のサイトのプレフィックス/サフィックスのセットを識別するために使用される名前です。実際のサイトの名前と一致してもかまいませんが、一致する必要はありません。	x	文字列
サイトマージパラメータ	を参照してください (#site-merging-parameters)		SwitchParameters
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter

  戻り値:

- なし

- `Remove-CvadAcSiteMergingInfo` - 既存のサイトマージプレフィックス/サフィックス情報セットを削除します。

  パラメーター:

  - `SiteName` – サイトのプレフィックスとサフィックスのセットを識別します。これは文字列であり、必須です。

  戻り値:

  - なし

サイトのマージパラメーター

サイトのマージコマンドレットを実行する際に、以下のパラメーターを使用できます。リストされているすべてのパラメーターは文字列です。

- `SiteName` –特定のサイトのプレフィックス/サフィックスのセットを識別するために使用される名前です。実際のサイト名と一致してもよいですが、必須ではありません。SiteNameは必須パラメーターです。
- `AdminScopedPrefix` – 管理者スコープに適用するプレフィックス。
- `ApplicationPrefix` - アプリケーションに適用するプレフィックス。
- `ApplicationFolderPrefix` – アプリケーションフォルダーに適用するプレフィックス。`ApplicationFolderPrefix`は`ApplicationFolderRoot`と組み合わせることができます。
- `ApplicationFolderRoot` – アプリケーションフォルダーの新しいルートフォルダー。これにより、追加のフォルダー階層が作成されます。`ApplicationFolderRoot`は`ApplicationFolderPrefix`と組み合わせることができます。
- `ApplicationGroupPrefix` – アプリケーショングループのプレフィックス。
- `ApplicationUserPrefix` – ユーザーに表示されるアプリケーション名に適用するプレフィックス。
- `ApplicationAdminPrefix` – 管理者に表示されるアプリケーション名に適用するプレフィックス。
- `DeliveryGroupPrefix` – デリバリーグループに適用するプレフィックス。
- `GroupPolicyPrefix` – ポリシー名に適用するプレフィックス。
- `HostConnectionPrefix` – ホスト接続に適用するプレフィックス。
- `MachineCatalogPrefix` – マシンカタログに適用するプレフィックス。

- `StoreFrontPrefix` – StoreFront™ 名に適用するプレフィックス。
- `TagPrefix` – タグに適用するプレフィックス。
- `AdminScopedSuffix` – 管理者スコープに適用するサフィックス。
- `ApplicationSuffix` - アプリケーションに適用するサフィックス。
- `ApplicationFolderSuffix` – アプリケーションフォルダーに適用するサフィックス。`ApplicationFolderSuffix` は `ApplicationFolderRoot` と組み合わせることができます。
- `ApplicationGroupSuffix` – アプリケーショングループのサフィックス。
- `ApplicationUserSuffix` – ユーザーに表示されるアプリケーション名に適用するサフィックス。
- `ApplicationAdminSuffix` – 管理者に表示されるアプリケーション名に適用するサフィックス。
- `DeliveryGroupSuffix` – デリバリーグループに適用するサフィックス。
- `GroupPolicySuffix` – ポリシー名に適用するサフィックス。
- `HostConnectionSuffix` – ホスト接続に適用するサフィックス。
- `MachineCatalogSuffix` – マシンカタログに適用するサフィックス。
- `StoreFrontSuffix` – StoreFront名に適用するサフィックス。
- `TagSuffix` – タグに適用するサフィックス。
- `SiteRootFolder` – エクスポートおよびインポートに使用する完全修飾フォルダー名。ローカルフォルダーまたはファイル共有にすることができます。

汎用パラメーター

クラウドアクセスパラメーター

クラウドにアクセスするすべてのコマンドレットは、次の追加パラメーターをサポートしています。

> **注:**

> CustomerId、ClientId、および Secret は、CustomerInfo.yml ファイルに配置するか、次のパラメーターを使用してコマンドレットで指定できます。両方の場所で指定されている場合、コマンドレットパラメーターが優先されます。

- `CustomerId` – Rest API で使用される顧客 ID であり、すべての Rest API にアクセスするために必要です。顧客 ID は Citrix Cloud にあります。
- `ClientId` – Citrix Cloud Identity and Access Management Web サイトで作成された clientID。これは、すべての Rest API の認証に必要なベアラートークンを取得するために必要です。
- `Secret` – Citrix Cloud Identity and Access Management Web サイトで作成された秘密鍵。これは、すべての Rest API の認証に必要なベアラートークンを取得するために必要です。
- `CustomerInfoFileSpec` – デフォルトの場所と名前を上書きするための顧客情報ファイルを指すファイル指定。

移行モードパラメーター

クラウドサイト構成を変更するコマンドレット (`Import` 、 `Restore` 、 `Merge` 、 `New` 、および `Sync`) は、さらなる柔軟性を提供するために以下の追加パラメーターをサポートしています。

- `CheckMode` – インポート操作を実行しますが、変更は*行いません*。すべての予期される変更は、インポートが完了する前に報告されます。このコマンドを使用して、インポートが実行される前にテストできます。
- `BackupFirst` – クラウド構成を変更する前に、クラウドコンテンツを.ymlファイルにバックアップします。これはデフォルトで有効になっています。
- `Confirm` – trueの場合、クラウドサイト構成に変更を加えることをユーザーに確認するプロンプトが表示されます。 `Remove` コマンドレットは、その破壊的な性質のためプロンプトを表示します。自動スクリプト内で実行する場合など、プロンプトが不要な場合はfalseに設定します。 `Confirm` はデフォルトでtrueです。
- `SecurityFileFolder` – これは、CustomerInfo.ymlファイルを含む完全修飾フォルダーであり、ローカルフォルダーまたは認証制御下にある可能性のあるネットワーク共有フォルダーを指す場合があります。ツールは資格情報を要求しません。ツールを実行する前に、制御されたリソースへのアクセスを取得する必要があります。
- `SiteName` – インポート時に使用するサイトマージのプレフィックスとサフィックスのセットを指定します。
- `SiteActive` – インポートされたサイトがアクティブか非アクティブかを指定します。デフォルトでは、このパラメーターは `$false` に設定されており、インポートされたサイトが非アクティブであることを意味します。

ログ表示パラメーター

`Export`、`Import`、`Sync`、`Restore`、`Backup`、`Compare`、および`Remove`コマンドレットは、操作が完了するとログファイルを表示します。`-DisplayLog`パラメーターを`$false`に設定することで、表示を抑制できます。ログファイルの表示には、デフォルトでNotepad.exeが使用されます。CustomerInfo.ymlファイルで別のエディターを指定できます。

```
Editor: C:\Program Files\Notepad++\notepad++.exe
```

コマンドレットの戻り値

ActionResult

すべてのコマンドレットは次の値を返します。

```
public class ActionResult

{

    public bool                         Overall_Success;

    public Dictionary&lt;string, string>   Individual_Success;

    public object                       CustomResult;

}
```

`Overall_Success`は、選択されたすべてのコンポーネントにおけるコマンドレット全体の成功を示す単一のブール値を返します。trueは成功、falseは失敗を意味します。

`Individual_Success`は、各主要コンポーネントに対して1つまたは3つの値を返します。コンポーネントの結果は、成功 (Success)、失敗 (Failure)、またはスキップ (Skipped) のいずれかになります。スキップは、そのコンポーネントがコマンドレットによる実行のために選択されなかったことを示します。

`CustomResult`はコマンドレット固有です。

CustomResult

`Import`、`Merge`、`Restore`、`Sync`、`Compare`、`Compare File`、および`Remove`は、`EvaluationResultData`の単一インスタンスに次のカスタム結果情報を返します。

> **注:**

`Export` および `Template` コマンドレットはカスタム結果を返しません。

```
 public class EvaluationResultData

 {

     public Dictionary&lt;string, Dictionary&lt;string, ActionResultValues
>> EvaluationResults;

     public int                  Added;

     public int                  Updated;

     public int                  Deleted;

     public int                  NoChange;

     public int                  TotalChanged;

     public EvaluationResults     OverallResult;

     public string               CloudBackupFolder;

     public string               SourceBackupFolder;

 }

 Where:

 public enum ActionResultValues

{

     Add,

     Update,

     Delete,

     Identical,
```

```
    DoNothing
}
public enum EvaluationResults
{
    Success,
    Failure,
    Skipped
}
```

`EvaluationResults` は、選択されたコンポーネントごとに 1 つのエントリを含むリストを表示します。キーはコンポーネント名で、値は各コンポーネントメンバーのリストと、そのコンポーネントメンバーに対して実行されたアクションです。アクションは `ActionResultValues` のいずれかの値になります。

`Added`、`Updated`、`Deleted`、および `NoChange` は、追加、更新、削除、またはアクションなしのコンポーネントメンバーの総数をこの順序で示します。

`TotalChanged` は、`Added`、`Updated`、および `Deleted` の合計です。

`OverallResult` は、コマンドレットの結果を示す単一のブール値です。True はすべてのコンポーネントでの完全な成功を示し、False は 1 つ以上のコンポーネントの処理の失敗を示します。

`CloudBackupFolder` は、コマンドレットがクラウド変更アクションを実行する前の、クラウドサイト構成バックアップの完全修飾ファイル指定です。

`SourceBackupFolder` は、コマンドレットの完了後に作成されたソースファイルバックアップの完全修飾ファイル指定です。デフォルトでは、これらのファイルは *%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。

PowerShell ヘルプ

各コマンドレットの PowerShell ヘルプが利用可能です。すべてのパラメーターは、コマンドレットの簡単な説明とともに各コマンドレットに文書化されています。任意のコマンドレットのヘルプにアクセスするには、コマンドレットの前に `Get-Help` と入力します。

`Get-Help Import-CvadAcToSite`

バックアップと復元のための自動構成ツール コマンドレット

このページには、Web Studio が使用するバックアップおよび復元 API をトリガーするためにツールがサポートするすべてのコマンドレットとパラメーターがリストされています。

バックアップストレージのコマンドレット

Get-BckRstrStorage

このコマンドレットはオンプレミスのみに適用されます。バックアップが保存されるストレージの詳細を取得します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。

Set-BckRstrStorage

このコマンドレットはオンプレミスのみに適用されます。バックアップが保存される新しいストレージを設定します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティ情報と環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`MaximumBackups`	新しいバックアップが作成されたときに、バックアップクリーンアッププロセスが最も

パラメーター	説明
	古いバックアップを削除するまで保持される、固定されていないバックアップの最大数。
`MaximumPinnedBackups`	保持される固定されたバックアップの最大数。これらのバックアップはクリーンアッププロセスによって削除されません。
`BlobStorageType`	ストレージのタイプ: `FileStorage` または `CustomerAzureStorage`。
`FileStoragefolder`	`BlobStorageType` `FileStorage` オプションの完全修飾フォルダー指定。
`Info1`	`FileStorage` の場合、オプションの `UserName` `CustomerAzureStorage` の場合、Azure SAS URL
`Info2`	`FileStorage` の場合、オプションのパスワード
`Info3` および `Info4`	使用されていません

テスト-BckRstrStorage

このコマンドレットはオンプレミスのみに適用されます。定義されたストレージが有効であることを確認するためにテストします。

`FileStorage`の場合、テストは、そのフォルダーが存在し、書き込み可能であることを確認します。

`CustomerAzureStorage`の場合、テストは、SAS URLが正しい権限を持ち、現在の日付がURLの開始日と終了日の間にあることを確認します。

有効な場合は`true`を返し、無効な場合は`false`を返します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud を参照してください。
`Environment`	本番環境の種類: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。

バックアップ コマンドレット

Get-BckRstrBackups

バックアップまたは復元BLOBストレージの場所に保存されているバックアップを列挙します。Citrix Virtual Apps and Desktops™の場合、この場所は管理者がWebStudioを通じて設定します。DaaSの場合、これは既存の顧客Azureストレージです。各バックアップに関する完全な情報については、`Get-BckRstrBackupsWithDetiails`を使用してください。バックアップの詳細は次のとおりです。

- バックアップ名
- 注
- ピン留め済み（trueまたはfalse）

- バックアップの日時
- 履歴UID
- 関連UID (最後の復元履歴レコードのUID)
- 関連日時
- チェックモードで実行された場合の関連
- 期間（秒）
- 管理者名
- 各コンポーネントと各コンポーネントのメンバー数を列挙した詳細。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud を参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。

Get-BckRstrBackupsMembers

選択したバックアップに保存されている単一のコンポーネントのメンバーを列挙します。メンバー名は単純なリストで返されます。

コンポーネントは次のとおりです。

- タグ
- AdminScopes
- AdminRoles
- AdminAdministrators (オンプレミスのみ)
- HostConnections
- アイコン
- AdminFolders
- MachineCatalogs
- StoreFronts
- DeliveryGroups
- ApplicationGroups
- ApplicationFolders
- アプリケーション
- AppVServers
- AppLibPackageDiscovery
- AppVIsolationGroups
- グループポリシー
- ユーザーゾーン設定
- サイトデータ
- ゾーン (オンプレミスのみ)

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。

パラメーター	説明
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud を参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前です。`.zip` 拡張子はオプションです。
`Component`	バックアップに含めるコンポーネント。

New-BckRstrBackup

Delivery Controller で新しいバックアップアクションを開始します。このアクションは、`New-BckRstrBackup` コマンドレットに対して非同期です。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。

パラメーター	説明
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される、既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud を参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`Notes`	バックアップに関するメモ。
`PollForCompletion`	アクションが完了するまで、Delivery Controllerで実行中のアクションをポーリングするためのパラメーター。`Quite` パラメーターが指定されていない限り、ポーリングは進行状況と完了結果をコンソールにログ記録します。

バックアップをピン留めするコマンドレット

Set-BckRstrPinBackups

Delivery Controllerのバックアップクリーンアッププロセスの一部として削除されないように、バックアップをピン留めします。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。

パラメーター	説明
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Citrix Cloud 用リモート PowerShell SDK v2 を参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip`拡張子はオプションです。

Set-BckRstrUnpinBackups

バックアップのピン留めを解除し、Delivery Controllerのバックアップクリーンアッププロセスで削除できるようにします。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。

パラメーター	説明
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip`拡張子はオプションです。

バックアップコマンドレットの削除

バックアップの削除

1つ以上のバックアップを削除します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。

パラメーター	説明
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`IncludeByName`	リストアの対象とするコンポーネントメンバーを指定するフィルターです。これは、カンマ区切りのフィルター値のリストであり、ワイルドカード文字 `*` および `?` を含めることができます。

スケジュールされたバックアップコマンドレット

Get-BckRstrSchedules

バックアップスケジュールのリストを取得します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。

パラメーター	説明
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、「XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud」を参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip` 拡張子はオプションです。
`Notes`	設定または変更するメモ。

New-BckRstrSchedule

新しいバックアップスケジュールを作成します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。

パラメーター	説明
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`Name`	スケジュール名。
`Frequency`	頻度の種類: 毎日、毎週、または毎月。
`Day`	頻度が毎日の場合。
`DaysInWeek`	頻度が毎週の場合。
`DayInMonth`	頻度が毎月の場合。
`WeekInMonth`	頻度が毎月の場合。
`StartDate`	形式は `M/d/yy` です
`StartTime`	24時間形式で指定された開始時刻。
`FrequencyFactor`	毎日 (値 = 1) または隔日 (値 = 2) のように、n 回ごとに実行します。
`Description`	スケジュールされたバックアップの説明
`Enabled`	このバックアップスケジュールを有効にするパラメーター。有効な場合は `True`、無効な場合は `false`。
`TimeZoneId`	Windows タイムゾーン ID

Set-BckRstrSchedule

既存のバックアップスケジュールを変更します。変更するスケジュールを選択するには、名前または Uid を指定します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud を参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`Name`	スケジュール名。
`Uid`	スケジュール名を変更する場合。
`Frequency`	頻度の種類: 毎日、毎週、または毎月。
`Day`	頻度が毎日の場合。
`DaysInWeek`	頻度が毎週の場合。

パラメーター	説明
`DayInMonth`	頻度が毎月の場合。
`WeekInMonth`	頻度が毎月の場合。
`StartDate`	形式は `M/d/yy` です。
`StartTime`	24時間形式で指定された開始時刻。
`FrequencyFactor`	毎日 (値 = 1) または隔日 (値 = 2) のように、n 回ごとに実行します。
`Description`	スケジュールされたバックアップの説明。
`Enabled`	このバックアップスケジュールを有効にするためのパラメーター。有効な場合は `True`、無効な場合は `false`。
`TimeZoneId`	WindowsタイムゾーンID。

Set-BckRstrScheduleEnabled

既存のバックアップスケジュールを有効にします。有効にするスケジュールを選択するには、名前または Uid を指定します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客 ID。
`CientId`	ベアラートークンを取得するために必要なクライアント ID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。

パラメーター	説明
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud を参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するパラメーター。
`Name`	スケジュール名。
`Uid`	スケジュール名を変更する場合。

Set-BckRstrScheduleDisabled

既存のバックアップスケジュールを無効にします。無効にするスケジュールを選択するには、名前またはUidを指定します。

パラメータ:

パラメータ	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに、既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop:

パラメータ	説明
	Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`Name`	スケジュール名。
`Uid`	スケジュール名を変更する場合。

バックアップの制限コマンドレット

Set-BckRstrOptions

スケジュールされたバックアップを1日1回に制限し、同一のバックアップを回避します。

パラメーター：

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。

パラメーター	説明
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`OneScheduledBackupPerDay`	同一のバックアップを避けるため、スケジュールされたバックアップを1日1回に制限するパラメーター。

復元コマンドレット

バックアップの復元

既存のバックアップから、単一のコンポーネントのメンバーを復元します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーターです。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。

パラメーター	説明
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip`拡張子はオプションです。
`Component`	バックアップに含めるコンポーネント。
`Notes`	バックアップに関するメモ。
`CheckMode`	復元されるコンポーネントメンバーを識別しますが、実際の復元は実行しないパラメーター。
`RestoreType`	復元タイプ: MissingOnly または MissingUpdateExisting
`IncludeByName`	復元対象とするコンポーネントメンバーを指定するフィルター。これは、フィルター値のコンマ区切りリストであり、ワイルドカード文字 `*` および `?` を含めることができます。

履歴コマンドレット

Get-BckRstrHistory

すべてのアクションの履歴詳細のリストを取得します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。

パラメーター	説明
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production, ProductionGov, ProductionJP, OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。

Get-BckRstrSpecificBackupHistory

特定のバックアップの履歴詳細のリストを取得します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp &

パラメーター	説明
	XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip`拡張子はオプションです。

Set-BckRstrNotes

履歴レコード内のメモを設定または変更します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production, ProductionGov, ProductionJP, OnPrem.

パラメーター	説明
`Quiet`	コンソールへの出力を抑制するパラメーター。
`BackupName`	バックアップの名前。`.zip` 拡張子はオプションです。
`Notes`	設定または変更するメモ。

自動構成のトラブルシューティングと追加情報

> **重要:**
>
> 自動構成でよく発生するエラーメッセージとそれに対応する解決策については、Knowledge Center の記事 CTX277730 の *トラブルシューティング FAQ* を参照してください。

自動構成ツールのエラー

自動構成ツールの操作中にエラーが発生することがあります。この場合、たとえばマシンカタログ、デリバリーグループ、グループポリシーなどのコンポーネントの処理中に障害が発生する可能性があります。`OnErrorAction` と継続パラメーターを使用すると、処理中にエラーを捕捉し、解決して、中断したところから再開できます。

デフォルトの `OnErrorAction` 値は `StopCompEnd` です。エラーが発生すると、ツールは現在のコンポーネントの処理を終了します。追加のコンポーネントは処理されず、エラーは下流の依存コンポーネントに引き継がれません。エラーを解決した後、継続パラメーターを適用してコマンドレットを再実行できます。

OnErrorAction パラメーター

移行コマンドで `OnErrorAction` パラメーター値を定義して、コンポーネントの処理中にツールが検出したエラーにどのように応答するかを制御できます。

この表は、パラメーター値とその説明を示しています。

値	説明
`Continue`	すべてのコンポーネントを可能な限り多く処理しようとします。

値	説明
`Pause`	処理の最後に一時停止し、続行するか停止するかを尋ねます。
`StopCompEnd`	コンポーネントを可能な限り処理しようとします。コンポーネントの処理が完了すると停止します。(既定)
`StopImmediately`	エラーが見つかると処理が停止します。

移行cmdlet

次の移行コマンドに `OnErrorAction` パラメーターを適用できます。

- `Compare-CvadAcToSite`
- `Import-CvadAcToSite`
- `Merge-CvadAcToSite`
- `New-CvadAcToSite`
- `Restore-CvadAcToSite`

例: `Merge-CvadAcToSite -OnErrorAction StopImmediately`

再開パラメーター

これらのパラメーターは、エラーが原因で操作が一時停止または停止した後に、ツールがどのように再開するかを定義します。

次の `OnErrorAction` パラメーター値のいずれかを含む移行コマンドレットに、再開パラメーターを適用できます。

- `Pause`
- `StopCompEnd`
- `StopImmediately`

この表は、パラメーター値とその説明を示しています。

値	説明
`-AllRemaining`	開始コンポーネントが必要です。処理は開始コンポーネントから始まり、残りのすべてのコン

値	説明
	ポーネントを処理します。複数のコンポーネントが処理されます。
`-Resume`	`CurrentComponent.txt` からのコンポーネントを開始点として使用します。残りのすべてはtrueに設定されます。複数のコンポーネントが処理されます。
`-Repeat`	`CurrentComponent.txt` からのコンポーネントを開始点として使用します。残りのすべてはfalseに設定されます。1つのコンポーネントのみが処理されます。

最後に処理されたコンポーネントは、AutoConfig フォルダー内の `CurrentComponent.txt` ファイルに保存されます。このファイルの編集は推奨されません。 `-Resume` または `-Repeat` を指定し、`CurrentComponent.txt` が見つからないか無効な場合、処理は停止し、コンポーネントを選択するよう求められます。

CustomerInfo.ymlファイルでのOnErrorActionの設定

`CustomerInfo.yml` ファイルで `OnErrorAction` の値を設定することもできます。次のコマンドレットを使用して値を設定します。

- 新しいファイルの場合: `New-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`
- 既存のファイルの場合: `Set-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`

ログ

いずれかのコマンドレットを実行すると、ログファイルが作成され、メインの履歴ログファイルにエントリが追加されます。すべての操作ログファイルはバックアップフォルダーに配置されます。すべてのログファイル名は `CitrixLog` で始まり、その後、自動構成操作とコマンドレット実行の日付とタイムスタンプが表示されます。ログは自動削除されません。

メインの履歴ログは `*%HOMEPATH%\Documents\Citrix\AutoConfig*` にある **History.Log** というファイルに保存されます。各コマンドレットの実行により、実行の日付、操作、結果、バックアップ、ログファイルの場所を含むメインログエントリが作成されます。

また、`New-CvadAcZipInfoForSupport` コマンドレットを使用して、Citrix サポートに送信するログを収集することもできます。このコマンドレットは、すべてのログファイルと .yml ファイルを単一の zip ファイルに圧縮します。顧客の機密情報 (CustomerInfo.yml および CvadAcSecurity.yml) は zip に含まれません。Icon.yml ファイルもサイズが大きいため除外されます。zip ファイルは *%HOMEPATH%\Documents\Citrix\AutoConfig* に配置され、日付とタイムスタンプに基づいて *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip* という名前が付けられます。この zip ファイルはバックアップとしても機能します。

各ログファイルには以下が含まれます。

- 操作の名前と、チェックモードが有効になっているかどうか
- 開始日時と終了日時
- 各コンポーネントのアクションと成功/失敗通知に関する複数のエントリ
- 作成されたオブジェクトのさまざまな数を含む、実行されたアクションの概要
- 該当する場合の推奨される修正
- 該当する場合のバックアップフォルダーの場所
- メインログの場所
- 期間

診断ファイル

診断ファイルは、問題の特定と解決に役立ちます。以下のファイルは、操作が実行されると作成されます。これらは、*%HOMEPATH%\Documents\Citrix\AutoConfig* の下にあるアクション固有のサブフォルダーに保存されます。問題解決のサポートのために情報を提供する際は、これらのファイルを含めてください。

エクスポート

`PoshSdk_yyyy_mm_dd_hh_mm_ss.ps1`

このファイルには、サイト構成をファイルにエクスポートするために行われたすべてのBroker PowerShell SDK呼び出しがカウントされます。

インポート、マージ、復元、同期、バックアップ、比較

`Transaction_yyyy_mm_dd_hh_mm_ss.txt`

このファイルには、各Rest API呼び出しと関連情報が記録されます。

`RestApiContent_yyyy_mm_dd_hh_mm_ss.txt`

このファイルには、すべての `Add`、`Update`、および `Delete` のRest APIコンテンツが含まれています。

依存関係に起因する問題

インポートとマージは、依存関係の欠落が原因で失敗する可能性があります。一般的な問題は次のとおりです。

1. グループポリシーにデリバリーグループフィルターがありません。通常の原因は、インポートされていないデリバリーグループです。
2. アプリケーションのインポートまたはマージが失敗します。通常の原因は、インポートされていないデリバリーグループまたはアプリケーショングループです。
3. アプリケーショングループにRestrictToTagがありません。通常の原因は、インポートされていないタグです。
4. ホスト接続が失敗します。通常の原因は、CvadAcSecurity.ymlファイルにセキュリティ情報がないことです。
5. マシンカタログが失敗します。通常の原因は、インポートされなかったホスト接続です。
6. マシンカタログとデリバリーグループからマシンが欠落しています。通常の原因は、Active Directoryで見つからなかったマシンです。
7. デリバリーグループからユーザーが欠落しています。通常の原因は、Active Directoryで見つからなかったユーザーです。

推奨事項

- 自動構成のインスタンスを同時に複数実行しないでください。複数のインスタンスを同時に実行すると、クラウドサイトで予期しない結果が生じます。この問題が発生した場合は、自動構成のインスタンスを1つ再実行して、サイトを予期される状態に戻してください。
- 自動構成の実行中にStudioで作業したり、データを変更したりしないでください。
- クラウドサイトが期待どおりであることを確認するために、Studioでマージ、インポート、または復元の結果を常に視覚的に検証してください。

フォルダー

デフォルトのフォルダーのルート場所

すべての自動構成ツール操作は、ルートフォルダーまたはその中のサブフォルダーで行われます。ルートフォルダーは、*%HOMEPATH%\Documents\Citrix\AutoConfig*にあります。

エクスポート

すべてのエクスポートされたファイルは、使いやすさとエクスポート履歴を提供するために、2つのフォルダーの場所に配置されます。エクスポートは常にルートフォルダーに配置されます。コピーは、エクスポートの日時とともに**Export**という名前のサブフォルダーに配置されます。

ルートフォルダーには常に、最新のエクスポートされたオンプレミスサイト構成が含まれています。各**Export**サブフォルダーには、指定された日時に行われたエクスポートが含まれており、エクスポートの履歴が保持されます。任意の**Export**サブフォルダーを使用して、クラウドサイトを構成できます。自動構成は、既存のエクスポートサブフォルダーを削除または変更しません。

インポート/マージ/同期/比較

`Import`、`Merge`、および`Compare`の各操作は、常にルートフォルダーにあるファイルから実行されます。各操作の結果、サブフォルダーが作成され、ルートフォルダー内のファイルがそこにコピーされます。これにより、クラウドサイトの変更履歴ソースファイルが提供されます。

復元

`Restore`操作は、既存のサブフォルダーを使用してクラウドサイトを構成します。ソースフォルダーは、必須の`-RestoreFolder`パラメーターで指定されます。他のコマンドとは異なり、`Restore`操作は既存のサブフォルダーを使用するため、新しいサブフォルダーは作成されません。復元フォルダーはルートフォルダーにすることができますが、それでも`-RestoreFolder`パラメーターで指定する必要があります。

バックアップ

Automated Configurationは、クラウドサイト構成を初期化、更新、およびバックアップします。長期間使用すると、クラウドサイトでさまざまな構成が変更される可能性があります。長期的な使用を容易にし、履歴の変更を保持するために、Automated Configurationは保存スキームを使用して、この変更履歴を保存し、以前の状態を復元する方法を提供します。

クラウドサイト構成のバックアップは、常にバックアップの日時とともに**Backup**という名前のサブフォルダーに作成されます。Automated Configurationは、既存のエクスポートサブフォルダーを削除または変更しません。

バックアップを使用して、特定のコンポーネントまたは構成全体を復元できます。デリバリーグループとマシンカタログコンポーネント全体を復元するには、次のコマンドレットを使用します。

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig/
Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups -MachineCatalogs
```

> **注：**
>
> 上記のコマンドレットのバックアップファイル情報は、ご自身のバックアップに基づいています。

> クラウドサイト構成全体を復元するには、次のコマンドレットを使用します。

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig\Backup_yyyy_mm_dd_hh_mm_ss
```

> **注：**
>
> 上記のコマンドレットのバックアップファイル情報は、ご自身のバックアップに基づいています。

デフォルトのルートフォルダーの変更

`Export`、`Import`、`Merge`、`Sync`、および`Compare`の各操作では、`-AlternateFolder`パラメーターを使用してデフォルトのルートフォルダーを変更できます。操作ごとのサブフォルダーの作成と管理は、前述のとおりです。

サブフォルダーにコピーされるファイル

以下のファイルを除き、拡張子が「.yml」のすべてのファイルは操作サブフォルダーにコピーされます。

- CustomerInfo.yml
- ZoneMapping.yml
- CvadAcSecurity.yml

自動フェールセーフクラウドサイトバックアップ

現在のクラウドサイト構成のバックアップは、構成を変更する操作を実行する前に作成されます。これには、`Import`、`Merge`、`Sync`、および`Restore`パラメーターが含まれます。バックアップは常に、運用サブフォルダーの下のサブフォルダーに保存されます。

`Restore`の場合、バックアップフォルダーは`-RestoreFolder`パラメーターで指定されたフォルダーのサブフォルダーです。

自動化

自動構成ツールコマンドレットは、プロンプトとコマンドレット完了時のログ結果の表示を抑制することで、管理者による介入なしに自動化スクリプトで実行できます。CustomerInfo.ymlファイルを使用して、同じことを行うパラメーターを設定することもできます。

プロンプトの表示を抑制するには、クラウド変更コマンドレットに次のパラメーターを追加します。

```
-Confirm $false
```

コマンドレットの完了時にログの表示を抑制するには、コマンドレットに次のパラメーターを追加します。

```
-DisplayLog $false
```

PowerShellコマンドウィンドウへのログ記録を抑制するために、次のパラメーターをコマンドレットに追加します。

```
-Quiet
```

別の方法として、次のパラメーターをCustomerInfo.ymlファイルに配置できます。

```
Confirm: False
```

```
DisplayLog: False
```

Delivery Controller™以外のPCからのエクスポート

自動構成ツールは、複数のCitrix PowerShell SDKを使用して、オンプレミスサイト構成をファイルにエクスポートします。これらのSDKはDelivery Controllerに自動的にインストールされるため、追加の操作なしでツールをDelivery Controllerで実行できます。Delivery Controller以外のマシンで実行する場合は、ツールに必要なCitrix PowerShell SDKのセットをインストールする必要があります。このSDKセットはCitrix Studioの一部であり、Citrix Virtual Apps and Desktops™インストールメディアからインストールできます。

> **注:**
>
> 自動構成はCloud Connectorでは実行できません。

Citrix Cloud™ GovernmentおよびJapan Control Planeへの移行

Citrix Cloud GovernmentおよびJapan Control Plane環境では、認証およびアクセストークンの割り当てに異なるアクセスポイントを使用します。この固有の要件は、クラウドにアクセスするすべての自動構成ツールに適用されます。これらの環境で自動構成を使用するには、次の手順を実行します。

1. *%HOMEPATH%\Documents\Citrix\AutoConfig*フォルダーで、CustomerInfo.ymlを編集します。
2. 接続する環境に応じて、次のいずれかの行をCustomerInfo.ymlに追加します（または、すでに存在する場合は変更します）。

   ```
   Environment: 'ProductionGov'
   ```

   または

   ```
   Environment: 'ProductionJP'
   ```

これらの環境で自動構成を使用できるようになりました。

Citrix Cloud のデータ収集

Citrix Cloud が収集する情報については、Citrix Cloud Services の顧客コンテンツとログの処理を参照してください。

その他のリソース

ディスカッションフォーラム

自動構成に関するCitrixディスカッションフォーラムにアクセスしてください。

ビデオ

Citrix Virtual Apps and Desktops 用自動構成ツールの内部構造をYouTubeでご覧ください。

トレーニング

Cloud Learning Center には、サービス展開を構築するためのステップバイステップのビデオガイドが含まれており、この記事で説明されているタスクも含まれています。Citrix Virtual Apps and Desktops を Citrix Cloud に移行する学習パスを参照してください。

オートスケール™

> **注:**

> Citrix Virtual Apps and Desktops™の展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この機能はWeb Studioでのみ利用可能です。

> Autoscaleは、マシンをプロアクティブに電力管理するための、一貫性のある高性能なソリューションを提供する機能です。コストとユーザーエクスペリエンスのバランスを取ることを目的としています。

Autoscaleは、デリバリーグループ内の登録されているすべてのシングルセッションおよびマルチセッションOSマシンのプロアクティブな電源管理を可能にします。

Autoscaleの機能は次のとおりです。

- スケジュールベースおよび負荷ベースの設定(/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/autoscale/schedule-based-and-load-based-settings.html)
- 動的セッションタイムアウト(/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/autoscale/dynamic-session-timeout.html)
- Autoscaleタグ付きマシン（クラウドバースト）(/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/autoscale/autoscale-tagged-machines.html)
- ユーザーログオフ通知(/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/autoscale/force-user-logoff.html)

サポートされているVDAホスティングプラットフォーム

Autoscaleは、Citrix Virtual Apps and Desktopsがサポートするすべてのプラットフォームをサポートしています。これには、XenServer、Amazon Web Services、Google Cloud Platform、Microsoft Azure Resource Manager、VMware vSphereなど、さまざまなインフラストラクチャプラットフォームが含まれます。サポートされているプラットフォームの完全なリストについては、Citrix Virtual Apps and Desktopsのシステム要件を参照してください。

> **注:**
>
> パブリッククラウドホスト接続をデプロイに追加する場合、Hybrid Rights Licenseが必要です。Hybrid Rights Licenseの詳細については、Transition and Trade-Up (TTU) with Hybrid Rightsを参照してください。ライセンスの追加については、サイトの作成を参照してください。

サポートされているワークロード

Autoscale は、マルチセッション OS とシングルセッション OS の両方のデリバリーグループをサポートしています。注意すべきユーザーインターフェイスは次の3つです。

- マルチセッション OS デリバリーグループ (旧 RDS デリバリーグループ) 用の Autoscale ユーザーインターフェイス
- シングルセッション OS ランダム (プール型) デリバリーグループ (旧 プール型 VDI デリバリーグループ) 用の Autoscale ユーザーインターフェイス
- シングルセッション OS 静的デリバリーグループ (旧 静的 VDI デリバリーグループ) 用の Autoscale ユーザーインターフェイス

さまざまなデリバリーグループのユーザーインターフェイスの詳細については、「Autoscale ユーザーインターフェイス」を参照してください。

利点

Autoscale 機能には、次の利点があります。

- デリバリーグループ内のマシンを電源管理するための、単一で一貫したメカニズムを提供します。
- 負荷ベースまたはスケジュールベースの電源管理、あるいはその両方を組み合わせてマシンに電力を供給することで、可用性を確保し、コストを管理します。
- コスト削減や容量使用率などのメトリックを監視し、通知を有効にするには、Director を使用します。

2分間のビデオを見る

次のビデオでは、Autoscale の簡単なツアーを提供します。

<iframe src="https://www.youtube.com/embed/5yxERrFZQ68" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

Autoscale™ の使用を開始する

Autoscale は、構成されたスケジュールまたは負荷の要求に基づいてデリバリーグループをプロアクティブにスケーリングする、一貫性のある高性能な電源管理ソリューションを提供する機能です。

Autoscale は、すべての種類のデリバリーグループに適用されます。

- シングルセッション静的 OS

- シングルセッションランダム OS
- マルチセッションランダム OS

この記事では、Autoscale に関連する基本的な概念について説明し、デリバリーグループ向けに Autoscale を有効にして構成する方法に関するガイダンスを提供します。

基本的な概念

開始する前に、Autoscale における次の基本的な概念について学びます。

- キャパシティとマシンの登録
- 複数のマシンカタログにわたるスケーリング
- マシンのプロビジョニングとセッションの需要
- インスタンスサイズの考慮事項
- スケジュール
- ピーク時とオフピーク時
- 電源オフ遅延
- プールサイズ
- 容量バッファ
- ロードインデックス
- Autoscaleとメンテナンスモード
- マシンコスト
- デリバリーグループのスケールアップ
- デリバリーグループのスケールダウン
- ドレイン状態

容量とマシンの登録

Autoscaleは、容量を決定する際に、サイトに登録されているマシンのみを含めます。登録されていない電源オンのマシンはセッション要求を受け入れることができません。その結果、それらはデリバリーグループの全体的な容量には含まれません。

複数のマシンカタログにわたるスケール

一部のサイトでは、複数のマシンカタログが単一のデリバリーグループに関連付けられている場合があります。Autoscaleは、スケジュールまたはセッションの需要要件を満たすために、各カタログからマシンをランダムに電源オンにします。

たとえば、あるデリバリーグループには2つのマシンカタログがあります。カタログAには3台のマシンが電源オンになっており、カタログBには1台のマシンが電源オンになっています。Autoscaleが追加のマシンを電源オンにする必要がある場合、カタログAまたはカタログBのいずれかのマシンを電源オンにする可能性があります。

マシンのプロビジョニングとセッション需要

デリバリーグループに関連付けられているマシンカタログには、需要の増減に応じて電源をオン/オフするのに十分な数のマシンが必要です。セッション需要がデリバリーグループ内の登録済みマシンの総数を超えた場合、Autoscaleはすべての登録済みマシンが電源オンになるようにします。ただし、**Autoscaleは追加のマシンをプロビジョニングしません。**

> **注:**
>
> デリバリーグループに63台のマシンがあり、営業時間外に10%のバッファ容量が設定されている場合、Autoscaleの計算によると、営業時間外には6.3台のマシンが電源オンになっている必要があります。小数値を処理するために、以下のルールが適用されます。
>
> - 最も近い値に丸める：たとえば、値が6.4の場合、6台のマシンがオンになります。値が6.7の場合、7台のマシンがオンになります。
> - 1未満のゼロ以外の値はすべて1に丸める：たとえば、値が0.2または0.9の場合、1台のマシンがオンになります。

インスタンスサイズの考慮事項

パブリッククラウドでインスタンスを適切にサイジングすると、コストを最適化できます。ワークロードのパフォーマンスと容量要件に合致する限り、より小さなインスタンスをプロビジョニングすることをお勧めします。

小さいインスタンスは、大きいインスタンスよりも少ないユーザーセッションをホストします。そのため、最後のユーザーセッションがログオフされるまでの時間が短いため、Autoscaleはマシンをより速くドレイン状態にします。結果として、Autoscaleは小さいインスタンスの電源をより早くオフにし、コストを削減します。

スケジュール

Autoscaleは、設定したスケジュールに基づいて、デリバリーグループ内のマシンの電源をオン/オフします。

スケジュールには、各タイムスロットのアクティブなマシンの数と、ピーク時およびオフピーク時が定義されています。

スケジュールの設定は、デリバリーグループの種類によって異なります。詳細については、以下を参照してください。

- マルチセッションOSデリバリーグループ
- シングルセッションOSランダムデリバリーグループ
- シングルセッションOS静的デリバリーグループ

ピーク時とオフピーク時

ピーク時間とオフピーク時間は、1日の特定の期間にどの容量バッファ値を使用するかを示すために使用されます。ピーク時間を定義し、残りの未定義の時間をオフピーク時間として設定できます。

電源オフ遅延

電源オフ遅延とは、マシンが電源オンになってからAutoscaleがそのマシンの電源をオフにできるようになるまでに経過する必要がある最小分数です。これにより、セッション需要が不安定なときにマシンが頻繁にオン/オフを繰り返すのを防ぎます。デフォルトでは、電源オフ遅延は30分です。0〜60分の範囲で設定できます。

プールサイズ

プールサイズとは、1日の特定の期間に電源オンの状態を維持する必要があるマシンの数です。

容量バッファ

容量バッファは、動的な負荷増加に対応するために、現在の需要に予備容量を追加するために使用されます。注意すべき2つのシナリオがあります。

- マルチセッションOSデリバリーグループの場合、容量バッファは、負荷インデックスの観点から、デリバリーグループの総容量の割合として定義されます。
- シングルセッションOSデリバリーグループの場合、容量バッファは、デリバリーグループ内のマシンの総数の割合として定義されます。

容量バッファはローリングバッファであり、構成されたプールサイズに加えて計算および適用されるのではなく、現在の使用状況に基づいて計算および適用されます。

たとえば、10台のマシンを持つデリバリーグループ、現在の期間のプールサイズが1台のマシン、容量バッファが10%であるとします。スケジュールで定義された1台の電源オンマシンが、10%の容量バッファが満たされなくなるまで負荷がかかると、追加のマシンが電源オンになります。2台

目のマシンの電源をオンにした後で負荷が減少し、10%の容量バッファを満たすのに十分すぎるほどの空き負荷容量がある場合、Autoscaleは1台のマシンの電源オフを準備します。

負荷インデックス

> **重要:**
>
> 負荷インデックスは、マルチセッションデリバリーグループにのみ適用されます。

> ロードインデックスメトリックは、マシンがユーザーログオン要求を受信する可能性を決定します。これは、同時ログオン、セッション、CPU、ディスク、メモリ使用量に対して構成された**Citrix Load Management policy**設定を使用して計算されます。

ロードインデックスは0から10,000の範囲です。デフォルトでは、マシンが250セッションをホストしている場合、フルロードと見なされます。

- 数字の「0」は、アンロードされたマシンを示します。ロードインデックス値が0のマシンは、ベースライン負荷の状態です。
- 数字の「10,000」は、これ以上セッションを実行できない完全にロードされたマシンを示します。

Autoscaleとメンテナンスモード

メンテナンスモードのマシンは、その可用性ステータスに関係なく、全体のプールサイズの計算の一部として考慮されます。したがって、プール内のすべてのマシンがメンテナンスモードになる可能性があります。ただし、これらのマシンは容量バッファの計算から除外され、即座に利用可能であることが保証されます。ユーザー接続のために特定の割合のマシンがアクセス可能であることを保証するには、プールサイズとバッファ値を適切に調整してください。

マシンコスト

マシンインスタンスの1時間あたりのコストは、使用されているコンピューティング容量の1時間あたりのコスト（米ドル）です。この設定は、Autoscale設定のコスト削減を計算するために使用されます。節約額を表示するには、**Monitor > Trends > Machine usage**に移動します。

デリバリーグループのスケールアップ

Autoscaleは、Autoscaleが有効なデリバリーグループで追加のマシンを次のときに電源オンにします。

1. デリバリーグループのAutoscaleスケジュールが、現在の期間により多くのマシンを電源オンにする必要があることを示している場合。
2. デリバリーグループの現在の負荷が容量バッファを超過した場合。

マシンの電源をオンにする条件：

1. メンテナンスモードではないこと。
2. ハイパーバイザーがメンテナンスモードではないこと。
3. 電源がオフで未登録である。
4. スケールアップが必要なデリバリーグループに属している。
5. 保留中の電源操作がない。

デリバリーグループをスケールダウンする

Autoscale は、Autoscale が有効なデリバリーグループ内のマシンの電源を、次の場合にオフにします。

1. Autoscale スケジュールで、現在の期間に設定されたマシン数に合わせるために、マシンの電源をオフにする必要があると指定されている場合。
2. デリバリーグループの現在の負荷が減少し、プールサイズと容量バッファを満たすために必要な数よりも多くの電源オン状態のマシンが存在する場合。

Autoscale は、プールサイズと容量バッファを満たすために必要な数を超える余分なマシンの電源をオフにすることで、デリバリーグループをスケールダウンします。

スケールダウンプロセスには、次の2つのステップがあります。

1. 必要な数のマシンをドレイン状態にします。
2. ドレイン状態のすべてのマシンを電源オフのために選択します。

電源オフの対象となるマシンは、次の条件を満たしている必要があります。

1. メンテナンスモードではない
2. ハイパーバイザーがメンテナンスモードではない
3. 現在電源オンの状態である
4. 利用可能として登録されているか、起動後に登録を待機している
5. ドレイン状態であり、アクティブなセッションがない
6. 保留中の電源操作がない
7. 電源オフ遅延を満たしている

ドレイン状態

Autoscale は、デリバリーグループ内の電源オン状態のマシンの数を、構成されたプールサイズと容量バッファにまでスケールダウンしようとします。

この目標を達成するために、Autoscale はセッション数が最も少ない余分なマシンを「ドレイン状態」にし、すべてのセッションがログオフされたときにそれらの電源をオフにします。この動作は、セッションの需要が減少し、スケジュールで電源オンになっているマシンよりも少ないマシンが必要な場合に発生します。

マシンがドレイン状態になる条件:

1. 電源オンである
2. メンテナンスモードではない
3. ハイパーバイザーがメンテナンスモードではない
4. スケールダウンが必要なデリバリーグループに属している
5. 現在のアクティブセッション数が最も少ない

> **注:**
>
> - 電源オフ遅延で指定された時間以上電源オン状態であったマシンが、ドレインの対象として優先されます。
> - ドレイン状態のマシンは、新しいセッションの起動をホストしなくなり、既存のセッションがログオフされるのを待機します。すべてのセッションがログオフされた場合にのみ、マシンはシャットダウンされます。ただし、セッション起動にすぐに利用できるマシンがない場合、Autoscaleはマシンの電源をオンにするよりも、ドレイン状態のマシンにセッション起動を誘導することを優先します。

> Autoscale は、余分なマシンを「ドレイン状態」に1台ずつ移行します。

- 2台以上のマシンが同じ数のアクティブセッションを持っている場合、Autoscale は、指定された電源オフ遅延の間電源がオンになっていたマシンをドレインします。

  そうすることで、最近電源がオンになったマシンがドレイン状態になるのを回避します。それらのマシンはセッション数が最も少ない可能性が高いからです。
- 2台以上のマシンが指定された電源オフ遅延の間電源がオンになっていた場合、Autoscale はそれらのマシンをランダムに1台ずつドレインします。

ドレイン状態のマシンは、新しいセッションの起動をホストしなくなり、既存のセッションがログオフされるのを待機します。すべてのセッションがログオフされた場合にのみ、マシンはシャットダウンの候補となります。ただし、セッション起動にすぐに利用できるマシンがない場合、Autoscaleはマシンの電源をオンにするよりも、ドレイン状態のマシンにセッション起動を誘導することを優先します。

次のいずれかの条件が満たされた場合、マシンはドレイン状態から解除されます。

- マシンの電源がオフになる。
- マシンが属するデリバリーグループでAutoscaleが無効になっている。
- Autoscaleは、スケジュールまたは負荷需要の要件を満たすためにマシンを使用します。このケースは、スケジュール（スケジュールベースのスケーリング）または現在の需要（負荷ベースのスケーリング）が、現在電源がオンになっているマシンの数よりも多くのマシンを必要とする場合に発生します。

> **重要:**
>
> セッション起動にすぐに利用できるマシンがない場合、Autoscaleは、マシンの電源をオンにするよりも、ドレイン状態のマシンにセッション起動を誘導することを優先します。セッション起動をホストするドレイン状態のマシンは、ドレイン状態のままになります。

どのマシンがドレイン状態にあるかを確認するには、`Get-BrokerMachine` PowerShellコマンドを使用します。例: `Get-BrokerMachine -DrainingUntilShutdown $true`。または、Studioを使用することもできます。「ドレイン状態のマシンを表示」を参照してください。

ドレイン状態のマシンを表示する

> **注:**
>
> この機能は、マルチセッションマシンにのみ適用されます。

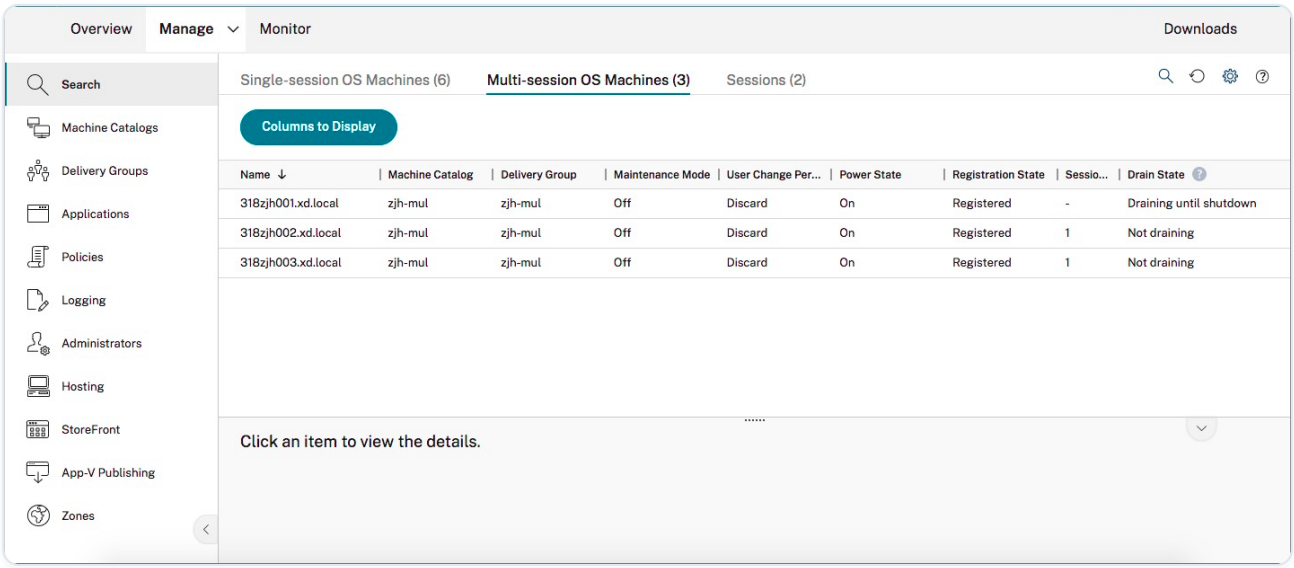
Studioでは、ドレイン状態のマシンを表示して、どのマシンがシャットダウンされようとしているかを知ることができます。次の手順を完了します。

1. **検索**ノードに移動し、**表示する列**をクリックします。

2. **表示する列**ウィンドウで、**ドレイン状態**の横にあるチェックボックスを選択します。
3. **保存**をクリックして、**表示する列**ウィンドウを終了します。

ドレイン状態列には、次の情報が表示されます。

- **シャットダウンまでドレイン中。** マシンがシャットダウンされるまでドレイン状態にある場合に表示されます。
- **ドレイン中ではありません。** マシンがまだドレイン状態にない場合に表示されます。

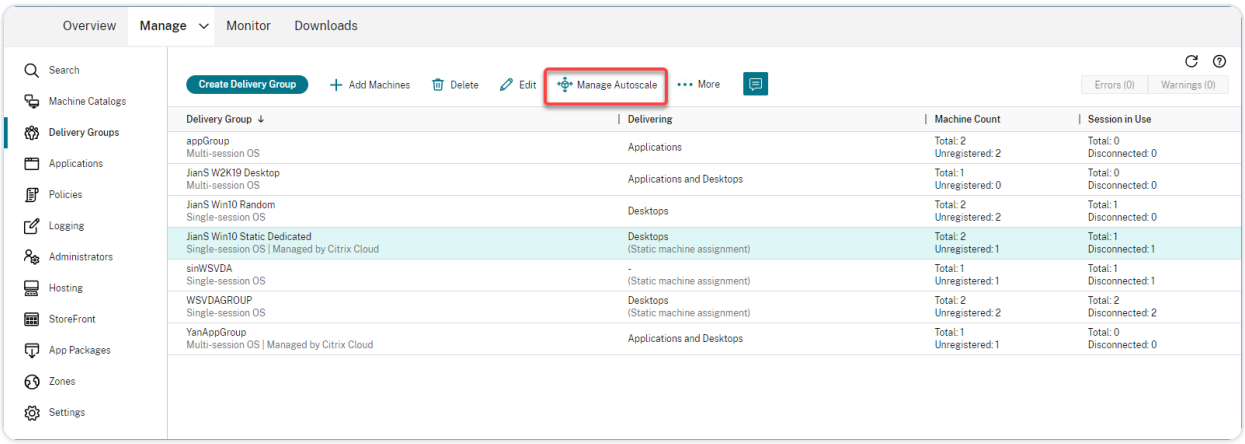


デリバリーグループのAutoscaleを有効にする

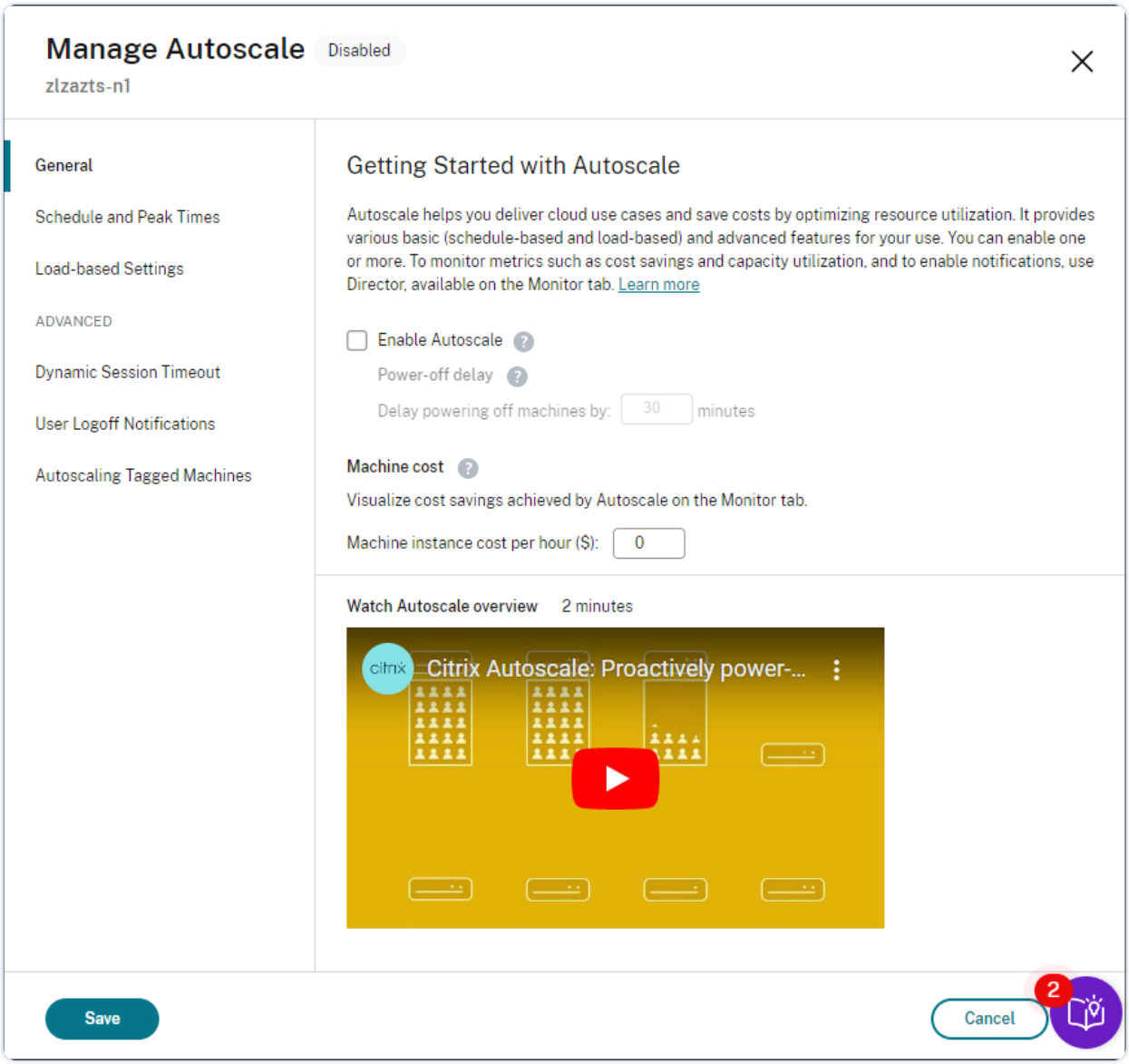
デリバリーグループを作成すると、Autoscaleはデフォルトで無効になります。Web Studioを使用してデリバリーグループのAutoscaleを有効にして構成するには、次の手順に従います。

PowerShellコマンドを使用して、デリバリーグループのAutoscaleを有効にして構成することもできます。詳細については、Broker PowerShell SDKコマンドを参照してください。

1. 左ペインで**デリバリーグループ**を選択します。
2. 管理するデリバリーグループを選択し、**Autoscaleの管理**をクリックします。



3. 「**Autoscaleの管理**」ページで、「**Autoscaleを有効にする**」チェックボックスをオンにしてAutoscaleを有効にします。Autoscaleを有効にすると、ページ上のオプションが有効になります。



4. 組織のニーズに基づいてデフォルト設定を変更するには、次の設定を完了します。

   - スケジュールを設定する
   - 非アクティブなマシンをより効率的に電源オフにするには、動的セッションタイムアウトとユーザーログオフ通知を使用します。
   - デリバリーグループ内のマシンの一部を電源管理するには、タグ付けされたマシンのAutoscalingを使用します。

Autoscaleを無効にするには、「**Autoscale**」チェックボックスをオフにします。ページ上のオプションが灰色表示になり、選択したデリバリーグループでAutoscaleが無効になっていることを示します。

重要:

- Autoscaleを無効にすると、Autoscaleによって管理されていたすべてのマシンは、無効化された時点の状態を維持します。
- Autoscaleを無効にすると、ドレイン状態のマシンはドレイン状態から解除されます。ドレイン状態の詳細については、ドレイン状態を参照してください。

メトリックの監視

デリバリーグループでAutoscaleを有効にすると、DirectorからAutoscaleによって管理されているマシンの次のメトリックを監視できます。

- マシンの使用状況
- 推定節約額
- マシンとセッションのアラート通知
- マシンのステータス
- 負荷評価の傾向

注:

デリバリーグループでAutoscaleを最初に有効にすると、そのデリバリーグループの監視データが表示されるまでに数分かかる場合があります。 Autoscaleが有効になり、その後デリバリーグループで無効になった場合でも、監視データは引き続き利用可能です。Autoscaleは5分間隔で監視データを収集します。

メトリックの詳細については、「Autoscaleで管理されるマシンの監視」を参照してください。

詳細情報

Autoscaleの詳細については、Tech Zoneの「Citrix Autoscale」を参照してください。

スケジュールベースおよび負荷ベースの設定

Autoscale™によるマシンの電源管理方法

Autoscale は、選択されたスケジュールに基づいてマシンの電源をオン/オフします。Autoscale を使用すると、特定の曜日を含む複数のスケジュールを設定し、それらの時間帯に利用可能なマシンの数を調整できます。特定の曜日の特定の時間に一連のユーザーがマシンリソースを消費すると予想される場合、Autoscale は最適化されたエクスペリエンスを提供するのに役立ちます。これらのマシンは、セッションが実行されているかどうかにかかわらず、スケジュール中に電源がオンになることに注意してください。

> **注:**
>
> Autoscaleは、電源管理されているすべてのマシンをサポートします。

> スケジュールは、デリバリーグループの**タイムゾーン**に基づいています。タイムゾーンを変更するには、デリバリーグループのユーザー設定を変更します。詳しくは、「デリバリーグループの管理」を参照してください。

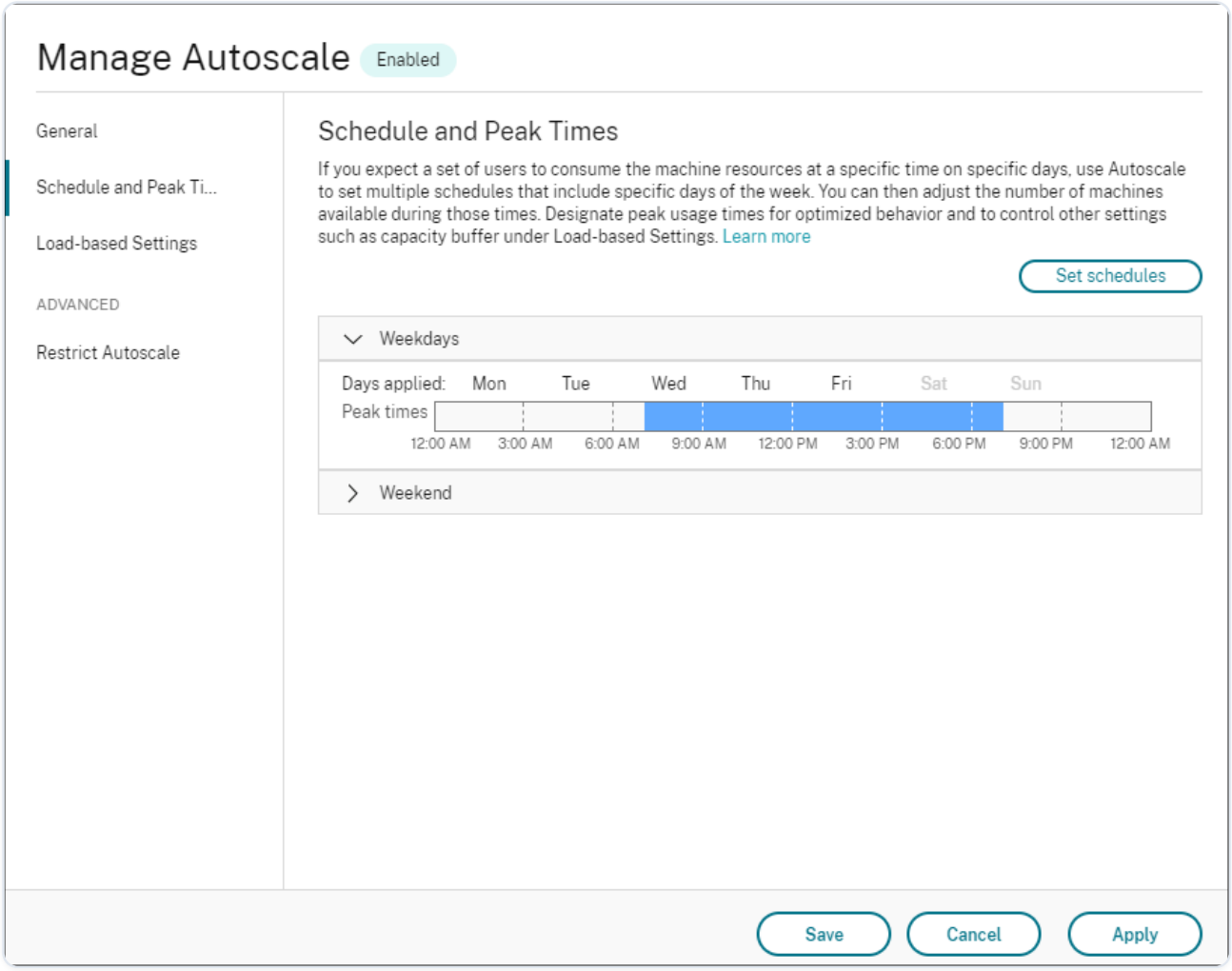
Autoscale には、デフォルトで2つのスケジュールがあります。*平日*（月曜日から金曜日）と*週末*（土曜日と日曜日）です。デフォルトでは、**平日**スケジュールでは、ピーク時に午前7時から午後6時30分まで1台のマシンの電源がオンになり、オフピーク時には電源がオンになりません。デフォルトの容量バッファは、ピーク時とオフピーク時ともに10%に設定されています。デフォルトでは、**週末**スケジュールでは、マシンの電源はオンになりません。

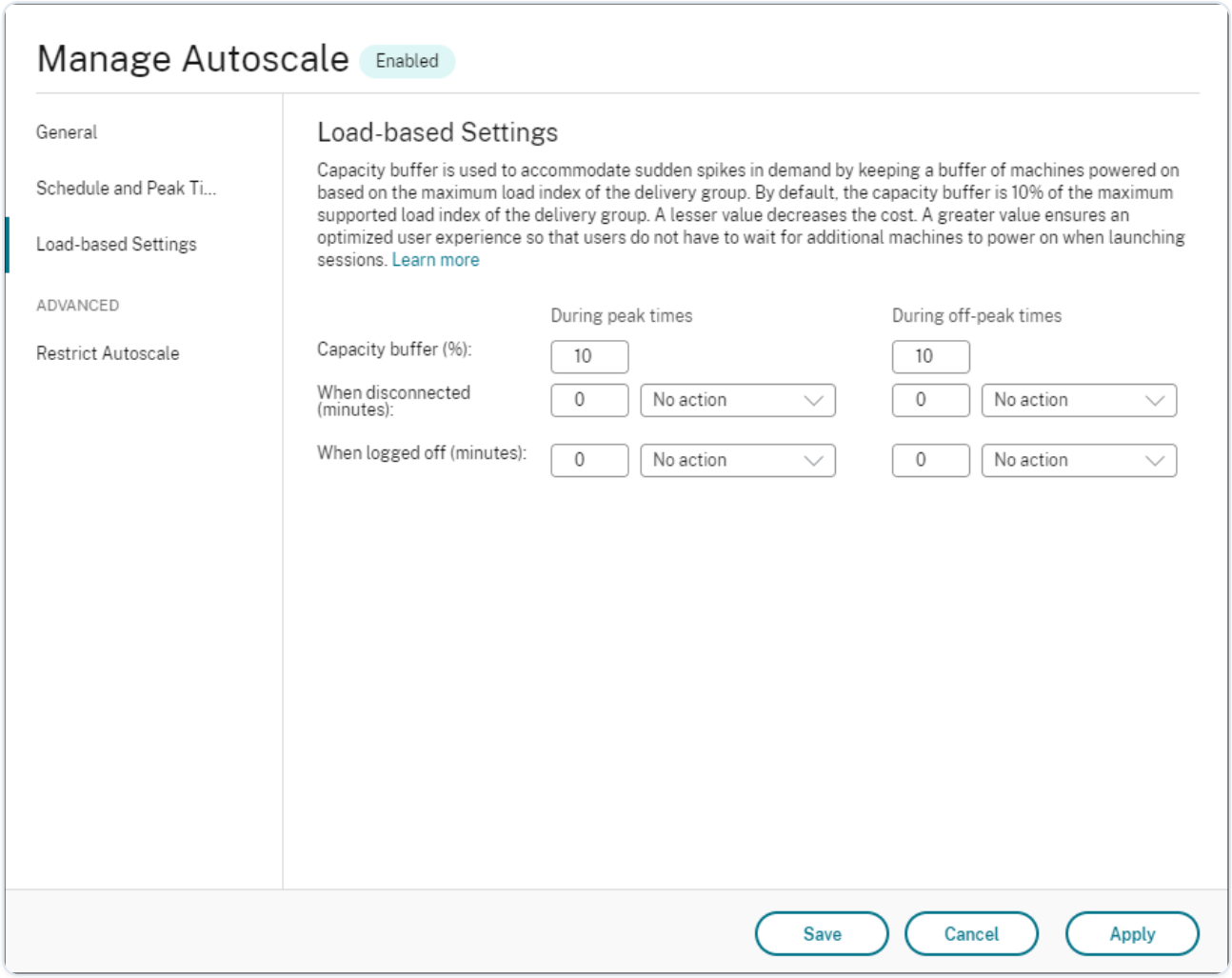
> **注:**
>
> Autoscaleは、サイトに登録されているマシンのみを、計算における利用可能な容量の一部として扱います。「登録済み」とは、マシンが使用可能であるか、すでに使用中であることを意味します。これにより、ユーザーセッションを受け入れられるマシンのみがデリバリーグループの容量に含まれるようになります。

ユーザーインターフェイス

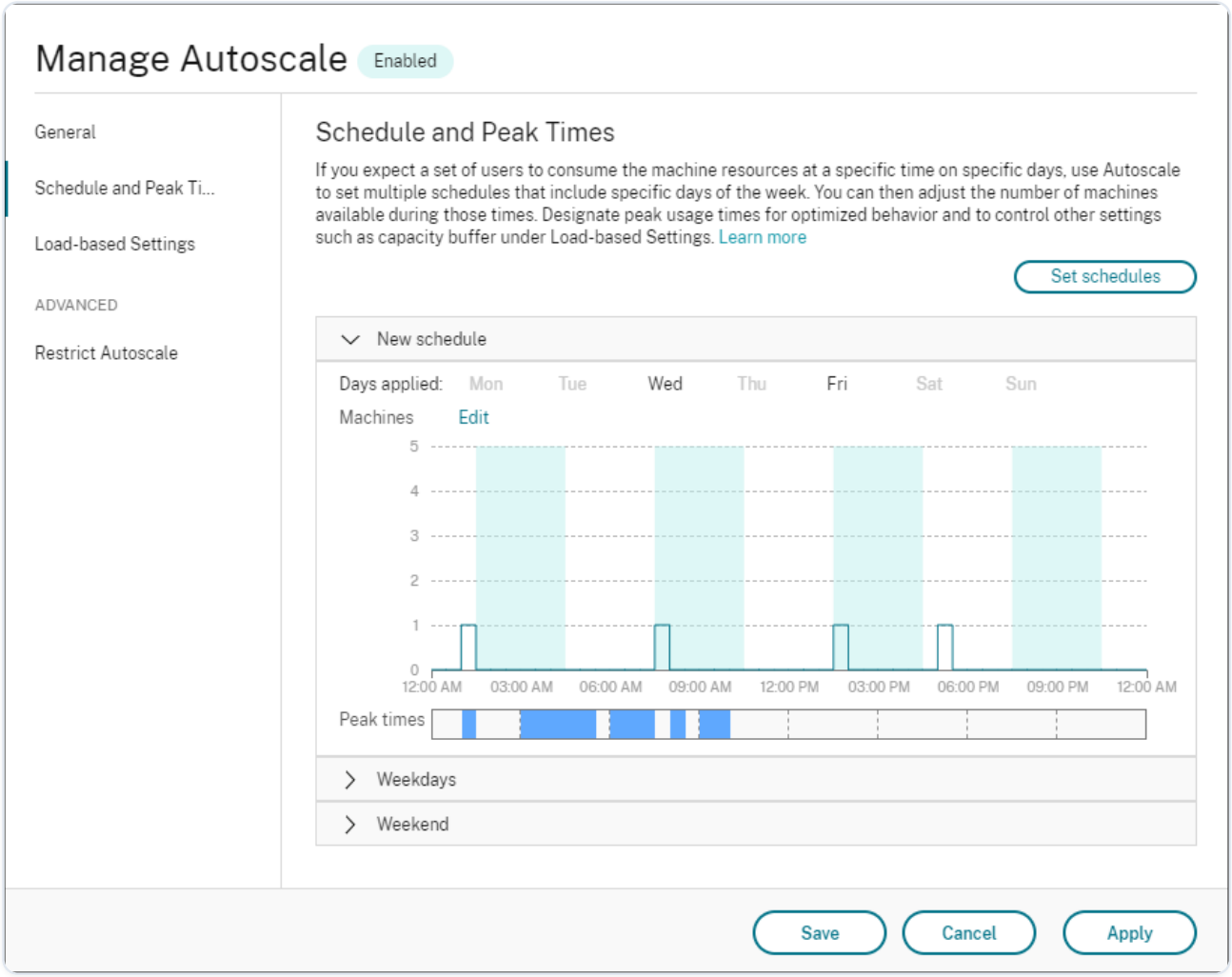
留意すべきユーザーインターフェイスは3種類あります。

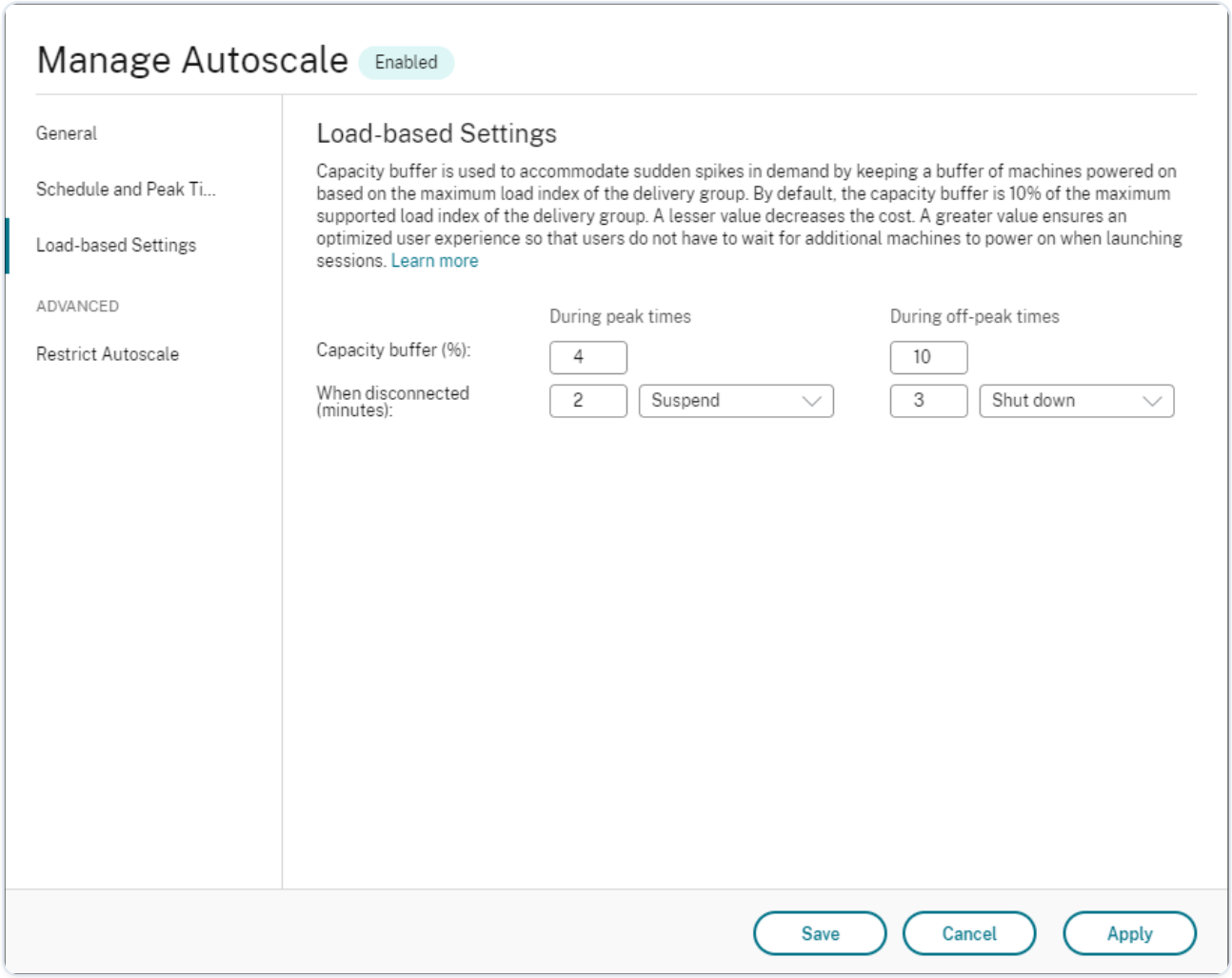
*シングルセッションOS静的デリバリーグループ*のユーザーインターフェイス：


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
Weekdays
Days applied: Mon Tue Wed Thu Fri Sat Sun
Peak times
12:00 AM 3:00 AM 6:00 AM 9:00 AM 12:00 PM 3:00 PM 6:00 PM 9:00 PM 12:00 AM
Weekend
Save
Cancel
Apply

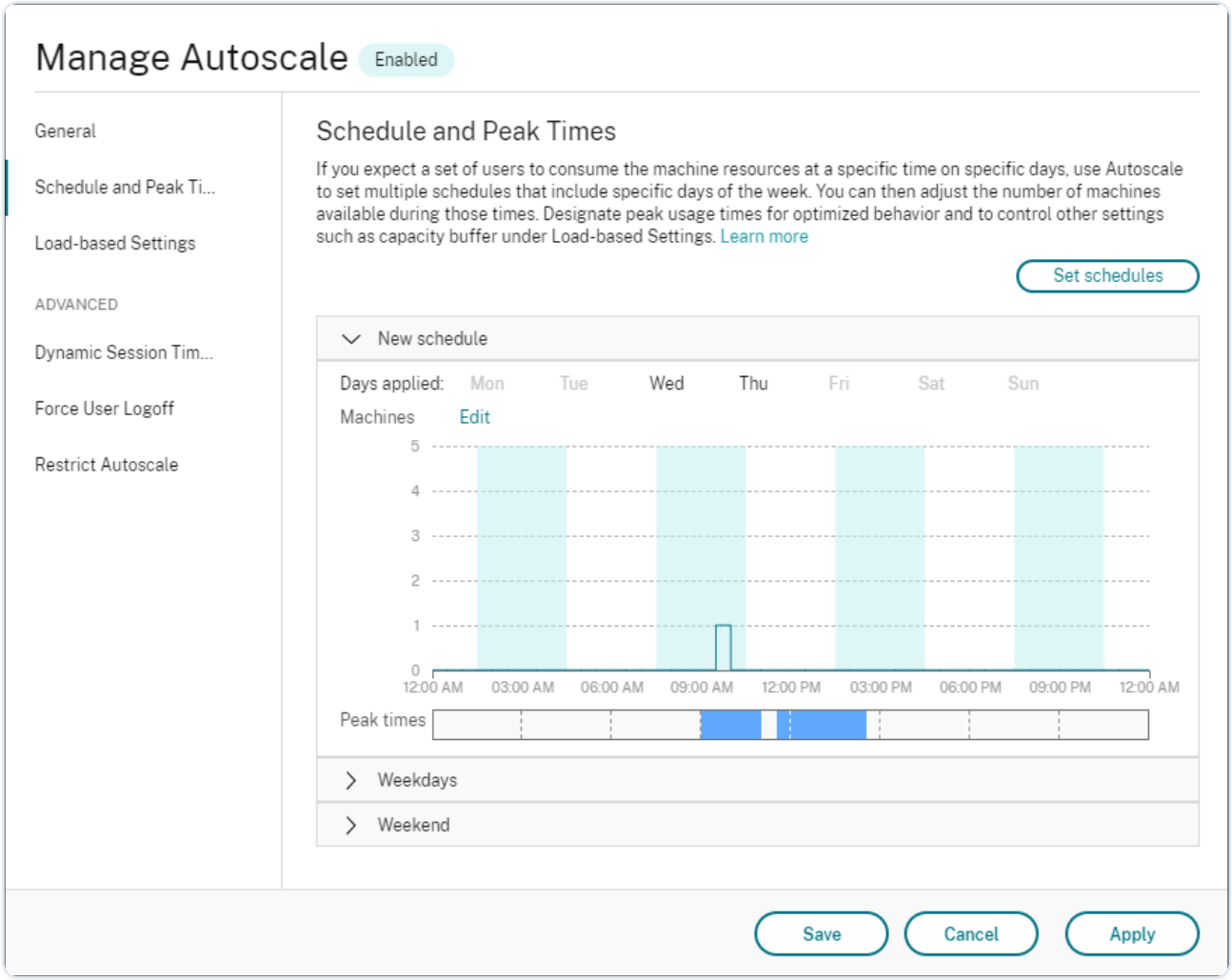


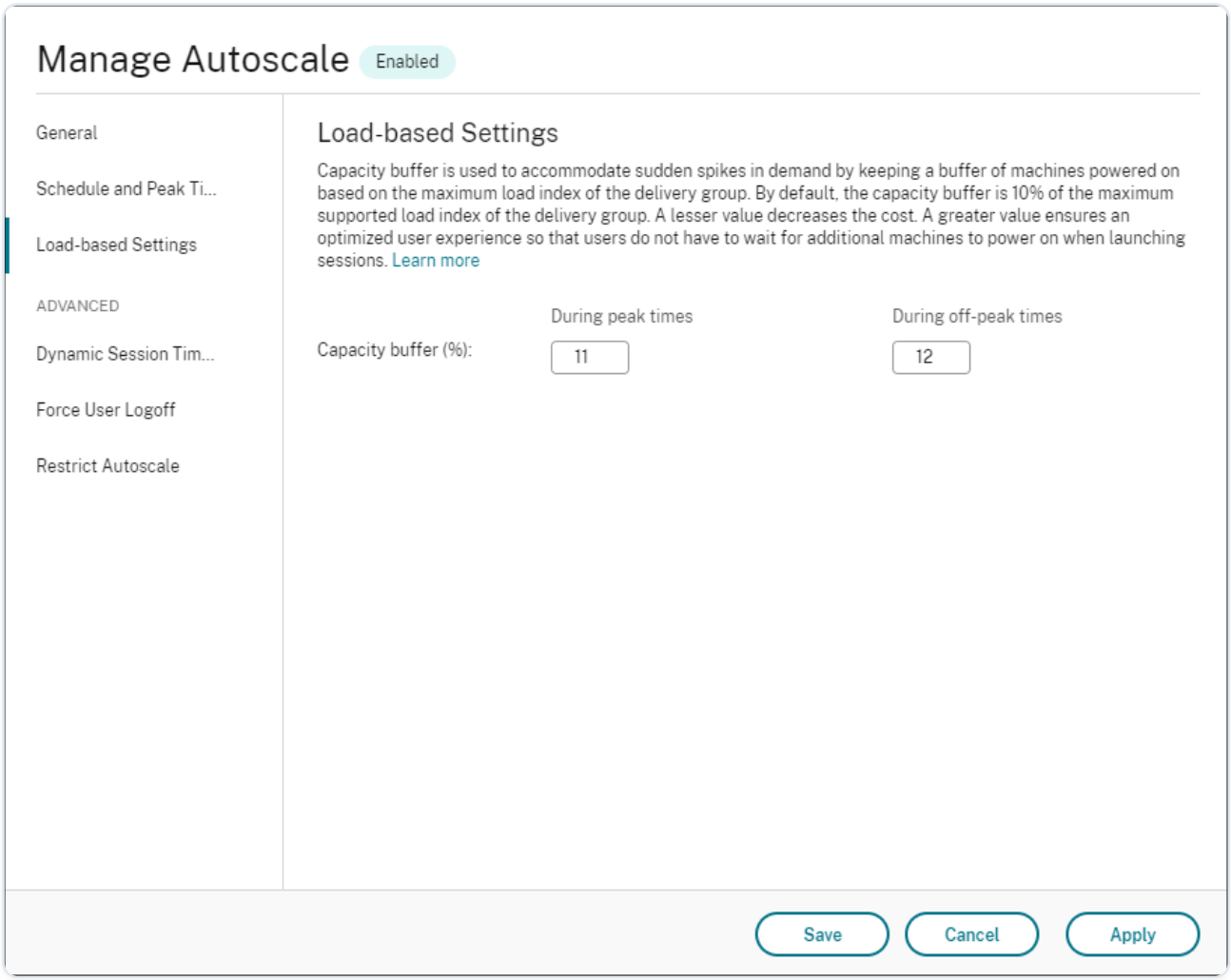
*シングルセッションOSランダムデリバリーグループの*Autoscaleユーザーインターフェイス：


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
New schedule
Days applied: Mon Tue Wed Thu Fri Sat Sun
Machines Edit
5
4
3
2
1
0
12:00 AM 03:00 AM 06:00 AM 09:00 AM 12:00 PM 03:00 PM 06:00 PM 09:00 PM 12:00 AM
Peak times
Weekdays
Weekend
Save
Cancel
Apply



Autoscale ユーザーインターフェイス：*マルチセッションOSデリバリーグループ*:


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Dynamic Session Tim...
Force User Logoff
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
New schedule
Days applied: Mon Tue Wed Thu Fri Sat Sun
Machines Edit
5
4
3
2
1
0
12:00 AM 03:00 AM 06:00 AM 09:00 AM 12:00 PM 03:00 PM 06:00 PM 09:00 PM 12:00 AM
Peak times
Weekdays
Weekend
Save
Cancel
Apply



スケジュールベースの設定

Autoscale スケジュール。スケジュールの追加、編集、選択、削除が可能です。

適用された曜日。選択したスケジュールに適用した曜日を強調表示します。残りの曜日はグレー表示されます。

編集。マシンを1時間ごとまたは30分ごとに割り当てることができます。マシンは数値またはパーセンテージで割り当てることができます。

> **注：**
>
> - このオプションは、マルチセッションOSおよびシングルセッションOSのランダムデリバリーグループ用のAutoscaleユーザーインターフェイスでのみ利用可能です。
> - **編集**の横にあるヒストグラムは、異なるタイムスロットで実行されているマシンの数または割合を示します。

- **ピーク時間**の上にある**編集**をクリックして、各タイムスロットに**マシンを割り当てる**ことができます。**起動するマシン**ウィンドウのメニューから選択したオプションに応じて、マシンを数値またはパーセンテージで割り当てることができます。
- マルチセッションOSデリバリーグループの場合、各日において30分単位で実行中のマシンの最小数を個別に設定できます。シングルセッションOSランダムデリバリーグループの場合、各日において60分単位で実行中のマシンの最小数を個別に設定できます。

独自のスケジュールを定義するには、次の手順に従います。

1. 「**Autoscaleの管理**」ウィンドウの「**スケジュールとピーク時間**」ページで、「**スケジュールを設定**」をクリックします。
2. 「**Autoscaleスケジュールの編集**」ウィンドウで、各スケジュールに適用する日を選択します。必要に応じてスケジュールを削除することもできます。
3. 「**完了**」をクリックしてスケジュールを保存し、「**スケジュールとピーク時間**」ページに戻ります。
4. 該当するスケジュールを選択し、必要に応じて構成します。
5. 「**適用**」をクリックして「**Autoscaleの管理**」ウィンドウを終了するか、他のページで設定を構成します。

重要:

- Autoscaleでは、異なるスケジュールで同じ日が重複することは許可されていません。たとえば、schedule1で月曜日を選択した後、schedule2で月曜日を選択すると、schedule1の月曜日は自動的にクリアされます。
- スケジュール名は大文字と小文字を区別しません。
- スケジュール名は空白にしたり、スペースのみを含めたりすることはできません。
- Autoscaleでは、文字間に空白スペースを入れることができます。
- スケジュール名には、次の文字を含めることはできません: \ / ; : # . * ? = < > \| ( ) { } " ' `.
- Autoscaleは重複するスケジュール名をサポートしていません。各スケジュールに異なる名前を入力してください。
- Autoscaleは空のスケジュールをサポートしていません。つまり、曜日が選択されていないスケジュールは保存されません。

注:

選択したスケジュールに含まれる曜日は強調表示され、含まれない曜日はグレー表示されます。

負荷ベースの設定

ピーク時間。選択したスケジュールに適用した日のピーク時間を定義できます。水平棒グラフを右クリックして定義できます。ピーク時間を定義すると、残りの未定義の時間はデフォルトでオフピーク時間になります。**デフォルト**では、選択したスケジュールに含まれる日の午前7時から午後7時までの時間帯がピーク時間として定義されています。

重要:

- マルチセッションOSデリバリーグループの場合、ピーク時間の棒グラフは容量バッファに使用されます。
- シングルセッションOSデリバリーグループの場合、ピーク時間の棒グラフは容量バッファに使用され、ログオフ後または切断後にトリガーされるアクションを制御します。
- マルチセッションOSおよびシングルセッションOSデリバリーグループの両方で、スケジュールに含まれる日のピーク時間を30分単位で細かく定義できます。または、代わりに`New-BrokerPowerTimeScheme PowerShell`コマンドを使用することもできます。詳細については、「Broker PowerShell SDKコマンド」を参照してください。

キャパシティバッファー。稼働中のマシンのバッファーを維持できます。値が小さいほどコストが削減されます。値が大きいほど、セッション起動時にユーザーが追加のマシンの電源がオンになるのを待つ必要がなくなり、最適化されたユーザーエクスペリエンスが保証されます。デフォルトでは、ピーク時とオフピーク時のキャパシティバッファーは10%です。キャパシティバッファーを0に設定すると、セッション起動時にユーザーが追加のマシンの電源がオンになるのを待つ必要がある場合があります。Autoscaleでは、ピーク時とオフピーク時でキャパシティバッファーを個別に決定できます。

その他の設定

ヒント:

- Broker PowerShell SDKを使用してその他の設定を構成することもできます。詳細については、「Broker PowerShell SDKコマンド」を参照してください。
- 切断時およびログオフ時の設定に関連するSDKコマンドを理解するには、`<https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy>`を参照してください。

切断時。セッション切断後、切断されロックされたマシンがサスペンドまたはシャットダウンされるまで、どのくらいの時間電源がオンのままになるかを指定できます。時間値を指定すると、構成したアクションに応じて、指定された切断時間が経過したときにマシンがサスペンドまたはシャットダウンされます。デフォルトでは、切断されたマシンにはアクションが割り当てられていません。ピーク時間とオフピーク時間でアクションを個別に定義できます。これを行うには、下矢印をクリックし、メニューから次のいずれかのオプションを選択します。

- **アクションなし**。選択すると、セッション切断後もマシンは電源がオンのままになります。Autoscaleはそれに対してアクションを実行しません。
- **サスペンド**。選択すると、指定された切断時間が経過したときに、Autoscaleはマシンをシャットダウンせずに一時停止します。**サスペンド**を選択すると、次のオプションが利用可能になります。
  - **再接続がない場合（分）**。サスペンドされたマシンは、切断されたユーザーが再接続したときに利用可能ですが、新しいユーザーには利用できません。すべてのワークロードを処理するためにマシンを再度利用可能にするには、シャットダウンします。Autoscaleがそれらをシャットダウンするまでのタイムアウトを分単位で指定します。
- **シャットダウン**。選択した場合、指定された切断時間が経過すると、Autoscale はマシンをシャットダウンします。

注:

このオプションは、シングルセッション OS のランダムおよび静的デリバリーグループ向けの Autoscale ユーザーインターフェイスでのみ利用可能です。

ログオフ時。セッションログオフ後、マシンがサスペンドまたはシャットダウンされるまでに、どのくらいの時間電源がオンのままになるかを指定できます。時間値が指定されている場合、設定したアクションに応じて、指定されたログオフ時間が経過するとマシンはサスペ

ンドまたはシャットダウンされます。デフォルトでは、ログオフされたマシンにはアクションが割り当てられていません。ピーク時とオフピーク時でアクションを個別に定義できます。これを行うには、下矢印をクリックし、メニューから次のいずれかのオプションを選択します。

- **アクションなし**。選択した場合、セッションログオフ後のマシンは電源がオンのままになります。Autoscale はそれに対してアクションを実行しません。
- **サスペンド**。選択した場合、指定されたログオフ時間が経過すると、Autoscale はマシンをシャットダウンせずに一時停止します。
- **シャットダウン**。選択した場合、指定されたログオフ時間が経過すると、Autoscale はマシンをシャットダウンします。

注:

このオプションは、シングルセッション OS の静的デリバリーグループ向けの Autoscale ユーザーインターフェイスでのみ利用可能です。

切断されたセッションを持つ、異なる時間帯に移行するシングルセッション OS マシンの電源管理

重要:

- この機能強化は、切断されたセッションを持つシングルセッションOSマシンにのみ適用されます。ログオフされたセッションを持つシングルセッションOSマシンには適用されません。
- この機能強化を有効にするには、該当するデリバリーグループでAutoscaleを有効にする必要があります。そうしないと、期間移行時に切断電源ポリシーアクションはトリガーされません。

以前のリリースでは、アクション (切断アクション = 「**サスペンド**」または「**シャットダウン**」) が必要な時間帯に移行するシングルセッション OS マシンは、電源がオンのままでした。このシナリオは、アクション (切断アクション = 「**何もしない**」) が不要な時間帯 (ピーク時またはオフピーク時) にマシンが切断された場合に発生しました。

このリリースから、Autoscale は、移行先の時間帯に設定された切断アクションに応じて、指定された切断時間が経過するとマシンをサスペンドまたは電源オフにします。

例えば、シングルセッションOSデリバリーグループに対して、以下の電源ポリシーを設定します。

- `PeakDisconnectAction`を「Nothing」に設定します
- `OffPeakDisconnectAction`を「Shutdown」に設定します
- 「OffPeakDisconnectTimeout」を「10」に設定します

> **注:**
>
> 切断アクション電源ポリシーの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy>`および`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>`を参照してください。

> 以前のリリースでは、ピーク時にセッションが切断されたシングルセッションOSマシンは、ピークからオフピークに移行しても電源がオンのままでした。このリリース以降、期間移行時にシングルセッションOSマシンに`OffPeakDisconnectAction`および`OffPeakDisconnectTimeout`ポリシーアクションが適用されます。その結果、マシンはオフピークに移行してから10分後に電源がオフになります。

以前の動作（つまり、切断されたセッションを持つマシンがピークからオフピークへ、またはオフピークからピークへ移行しても何もアクションを実行しない）に戻したい場合は、以下のいずれかを実行します。

- 「LegacyPeakTransitionDisconnectedBehaviour」レジストリ値を1（true; 以前の動作を有効にする）に設定します。デフォルトでは、値は0（false; 期間移行時に切断電源ポリシーアクションをトリガーする）です。
  - パス: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - 名前: LegacyPeakTransitionDisconnectedBehaviour
  - 種類: REG_DWORD
  - データ: 0x00000001 (1)

- `Set-BrokerServiceConfigurationData` PowerShellコマンドを使用して設定を構成します。例:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

マシンは、期間移行時に電源ポリシーアクションが適用される前に、以下の条件を満たしている必要があります。

- 切断されたセッションがある。
- 保留中の電源アクションがない。
- 異なる時間帯に移行するシングルセッションOSデリバリーグループに属している。
- 特定の時間帯（ピーク時またはオフピーク時）に切断され、電源アクションが割り当てられている期間に移行するセッションがある。

容量バッファの仕組み

容量バッファは、動的な負荷増加に対応するために、現在の需要に予備容量を追加するために使用されます。留意すべき2つのシナリオがあります。

- マルチセッションOSデリバリーグループの場合、容量バッファは、ロードインデックスの観点から、デリバリーグループの総容量のパーセンテージとして定義されます。ロードインデックスの詳細については、「ロードインデックス」(/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/autoscale.html#load-index)を参照してください。
- シングルセッションOSデリバリーグループの場合、容量バッファは、マシンの数の観点から、デリバリーグループの総容量のパーセンテージとして定義されます。

> **注:**

> Autoscaleをタグ付けされたマシンに制限するシナリオでは、容量バッファは、ロードインデックスの観点から、デリバリーグループ内のタグ付けされたマシンの総容量のパーセンテージとして定義されます。

> Autoscaleでは、ピーク時とオフピーク時で容量バッファを個別に設定できます。容量バッファフィールドの値が小さいほど、Autoscaleが起動する予備容量が少なくなるため、コストが削減されます。値が大きいほど、ユーザーがセッションを起動する際に追加のマシンが

起動するのを待つ必要がないため、最適化されたユーザーエクスペリエンスが保証されます。デフォルトでは、容量バッファは10%です。

重要：

容量バッファにより、総予備容量がデリバリーグループの総容量の「X」パーセントを下回ると、マシンが起動します。これにより、必要な割合の予備容量が確保されます。

マルチセッションOSデリバリーグループ

マシンはいつ電源オンになりますか?

重要:

容量バッファにより、総予備容量がデリバリーグループの総容量の「X」パーセントを下回るレベルに低下した場合にマシンが起動されます。これにより、必要な割合の予備容量が確保されます。

デリバリーグループ内の電源オン状態のマシンの数が、負荷インデックスの観点からバッファ容量を維持するために必要なバッファを満たせなくなった場合、Autoscale は追加のマシンの電源をオンにします。たとえば、デリバリーグループに 20 台のマシンがあり、スケジュールベースのスケーリングの一部として、容量バッファ 20% で 3 台のマシンの電源がオンになるようにスケジュールされているとします。最終的に、負荷がない場合でも 4 台のマシンが電源オンになります。これは、バッファとして 4 x 10k の負荷インデックスが必要なため、少なくとも 4 台のマシンの電源をオンにする必要があるためです。このケースは、ピーク時、マシンの負荷増加、新しいセッションの起動、およびデリバリーグループに新しいマシンを追加する際に発生する可能性があります。Autoscale は、次の条件を満たすマシンのみの電源をオンにすることに注意してください。

- マシンがメンテナンスモードではない。
- マシンが実行されているハイパーバイザーがメンテナンスモードではない。
- マシンが現在電源オフになっている。
- マシンに保留中の電源操作がない。

マシンはいつ電源オフになりますか?

重要:

- スケジュールが選択されている場合、Autoscale はスケジュールに基づいてマシンの電源をオフにします。
- Autoscale は、スケジュール中に電源オンになるようにスケジュールで構成されたマシンの電源をオフにしません。

デリバリーグループのターゲットとなる電源オン状態のマシン数（バッファを含む）をサポートするのに十分すぎるほどのマシンがある場合、Autoscale は余分なマシンの電源をオフにします。このケースは、オフピーク時、マシンの負荷減少、セッションログオフ、およびデリバリーグループからマシンを削除する際に発生する可能性があります。Autoscale は、次の条件を満たすマシンのみの電源をオフにします。

- マシンと、マシンが実行されているハイパーバイザーがメンテナンスモードではない。
- マシンが現在電源オンになっている。
- マシンは利用可能として登録されているか、起動後に登録を待機しています。
- マシンにアクティブなセッションはありません。
- マシンに保留中の電源操作はありません。
- マシンは指定された電源オフ遅延を満たしています。これは、マシンが少なくとも「X」分間電源オンの状態であったことを意味します。「X」はデリバリーグループに指定された電源オフ遅延です。

例のシナリオ

次のシナリオを想定します。

- **デリバリーグループの構成**。Autoscale で電源管理するデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscale の構成**
  - キャパシティバッファは10%に設定されています。
  - 選択されたスケジュールにはマシンが含まれていません。

シナリオは次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. より多くのユーザーセッションが開始されます。
4. セッション終了により、ユーザーセッションの負荷が減少します。
5. ユーザーセッションの負荷は、セッション負荷がオンプレミスリソースのみで処理されるまでさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかの詳細については、以下を参照してください。

- ユーザー負荷なし (初期状態)
  - 1台のマシン (例: M1) が電源オンになります。マシンは、構成されたキャパシティバッファのために電源オンになります。この場合、10 (マシン数) x 10,000 (負荷インデックス) x 10% (構成されたキャパシティバッファ) は10,000に相当します。したがって、1台のマシンが電源オンになります。
  - 電源オンになったマシン (M1) の負荷インデックス値は、ベースライン負荷 (負荷インデックスは0に相当) にあります。
- 最初のユーザーがログオンします
  - セッションはマシンM1でホストされるように指示されます。
  - 電源オンになったマシンM1の負荷インデックスが増加し、マシンM1はベースライン負荷ではなくなります。
  - Autoscaleは、構成されたキャパシティバッファのために需要を満たすために、追加のマシン (M2) の電源をオンにし始めます。
  - マシンM2の負荷インデックス値はベースライン負荷にあります。
- ユーザーが負荷を増加させます
  - セッションはマシンM1とM2の間で負荷分散されます。その結果、電源オンになったマシン (M1とM2) の負荷インデックスが増加します。
  - 総予備容量は、負荷インデックスの観点からまだ10,000を超えるレベルにあります。
  - マシンM2の負荷インデックス値はベースライン負荷ではなくなります。
- より多くのユーザーセッションが開始されます
  - セッションはマシン (M1 および M2) 間で負荷分散されます。その結果、電源がオンになっているマシン (M1 および M2) の負荷インデックスがさらに増加します。

  - 総予備容量が負荷インデックスで10,000を下回ると、構成された容量バッファにより、Autoscale は需要を満たすため追加のマシン (M3) の電源をオンにし始めます。
  - マシン M3 の負荷インデックス値はベースライン負荷です。
- さらに多くのユーザーセッションが開始されます
  - セッションはマシン (M1 から M3) 間で負荷分散されます。その結果、電源がオンになっているマシン (M1 から M3) の負荷インデックスが増加します。
  - 総予備容量は負荷インデックスで10,000を上回るレベルです。
  - マシン M3 の負荷インデックス値はベースライン負荷ではなくなります。
- セッション終了によりユーザーセッションの負荷が減少します
  - ユーザーがセッションからログオフするか、アイドルセッションがタイムアウトすると、マシン M1 から M3 で解放された容量は、他のユーザーが開始したセッションをホストするために再利用されます。
  - 総予備容量が負荷インデックスで10,000を上回るレベルに増加すると、Autoscale はマシンの1つ (たとえば M3) をドレイン状態にします。その結果、新しい変更が発生しない限り、他のユーザーが開始したセッションはそのマシンに転送されなくなります。たとえば、エンドユーザーの負荷が再び増加したり、他のマシンの負荷が最も低くなったりした場合などです。
- ユーザーセッションの負荷は減少し続けます
  - マシン M3 のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、Autoscale はマシン M3 の電源をオフにします。
  - さらに多くのユーザーがセッションを終了すると、電源がオンになっているマシン (M1 および M2) で解放された容量は、他のユーザーが開始したセッションをホストするために再利用されます。
  - 総予備容量が負荷インデックスで10,000を上回るレベルに増加すると、Autoscale はマシンの1つ (たとえば M2) をドレイン状態にします。その結果、他のユーザーが開始したセッションはそのマシンに転送されなくなります。
- セッションがなくなるまでユーザーセッションの負荷は減少し続けます
  - マシンM2上のすべてのセッションが終了し、指定された電源オフ遅延時間がタイムアウトすると、AutoscaleはマシンM2の電源をオフにします。
  - 電源オン状態のマシン (M1) の負荷インデックス値はベースライン負荷です。構成された容量バッファのため、AutoscaleはマシンM1をドレイン状態にしません。

注：

マルチセッションOSデリバリーグループの場合、ユーザーがセッションからログオフすると、デスクトップへのすべての変更は失われます。ただし、構成されている場合、ユーザー固有の設定はユーザープロファイルとともにローミングされます。

シングルセッションOSランダムデリバリーグループ

容量バッファは、デリバリーグループ内のマシンの総数に基づいて、電源オン状態のマシンのバッファを維持することで、急激な需要の増加に対応するために使用されます。デフォルトでは、容量バッファはデリバリーグループ内のマシンの総数の10%です。

マシンの数（容量バッファを含む）が現在電源オン状態のマシンの総数を超える場合、需要を満たすために追加のマシンが電源オンになります。マシンの数（容量バッファを含む）が現在電源オン状態のマシンの総数よりも少ない場合、余分なマシンは構成したアクションに応じてシャットダウンまたは中断されます。

電源ポリシー

さまざまなシナリオでマシンの電源を管理するポリシーを構成します。各シナリオについて、待機時間（分単位）と、指定された時間が終了した後に実行するアクションを指定できます。電源ポリシーは、シングルセッションOSランダムデリバリーグループおよびシングルセッションOS静的デリバリーグループに適用されます。

電源ポリシーのアクション(/en-us/citrix-virtual-apps-desktops/2411/media/power-policies-actions.png)

切断後、ピーク時とオフピーク時の両方で、以下の設定が適用されます。

- ドロップダウンから、待機時間（分単位）と、アクション（アクションなし、中断、シャットダウンなど）を設定できます。
- 中断アクションを選択した場合、マシンをシャットダウンするための追加の待機時間を構成します。

注：

- ピーク時およびオフピーク時において、シャットダウンアクションの待機時間は中断の待機時間よりも長くする必要があります。

- サスペンドされたマシンは、再接続時に切断されたユーザーのみがアクセスできます。新しいユーザーがサスペンドされたマシンを利用できるようにするには、シャットダウンします。
- サスペンドおよびシャットダウンのフィールドの時刻設定が正しく構成されていない場合、**保存**オプションは無効になり、設定エラーを示す赤い点もナビゲーション項目の横に表示されます。

シングルセッションOSランダムDG電源ポリシー設定(/en-us/citrix-virtual-apps-desktops/2411/media/single-session-os-random-dg-power-policies-settings.png)

例

- 待機時間を12分に設定し、最初の操作を「操作なし」に選択した場合、12分経過後もマシンは電源オンの状態を維持します。
- 待機時間を15分に設定し、最初の操作を「サスペンド」に選択し、2番目の待機時間を20分に設定した場合、15分経過後、マシンはサスペンドされます。2番目の待機時間経過後、マシンはシャットダウンされます。
- 待機時間を18分に設定し、最初の操作を「シャットダウン」に選択した場合、18分経過後、マシンはシャットダウンされます。

例のシナリオ

次のシナリオを想定します。

- **デリバリーグループの構成**。Autoscaleで電源管理するデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscaleの構成**
  - 容量バッファは10%に設定されています。
  - 選択したスケジュールにはマシンが含まれていません。

シナリオは次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. さらに多くのユーザーセッションが開始されます。
4. セッション終了により、ユーザーセッションの負荷が減少します。

5. セッション負荷がオンプレミスリソースのみで処理されるまで、ユーザーセッションの負荷はさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期状態）
  - 1台のマシン（M1）が電源オンになります。このマシンは、設定されたキャパシティバッファのために電源オンになります。この場合、10（マシン数）x 10%（設定されたキャパシティバッファ）は1に等しくなります。したがって、1台のマシンが電源オンになります。
- 最初のユーザーがログオンします
  - ユーザーがデスクトップを使用するために初めてログオンすると、電源オンになっているマシンでホストされているデスクトップのプールからデスクトップが割り当てられます。この場合、ユーザーにはマシンM1からデスクトップが割り当てられます。
  - Autoscaleは、設定されたキャパシティバッファのために需要を満たすために、追加のマシン（M2）の電源をオンにし始めます。
- 2番目のユーザーがログオンします
  - ユーザーにはマシンM2からデスクトップが割り当てられます。
  - Autoscaleは、設定されたキャパシティバッファのために需要を満たすために、追加のマシン（M3）の電源をオンにし始めます。
- 3番目のユーザーがログオンします
  - ユーザーにはマシンM3からデスクトップが割り当てられます。
  - 構成された容量バッファにより、需要を満たすためにAutoscaleが追加のマシン（M4）の電源をオンにし始めます。
- ユーザーがログオフする
  - ユーザーがログオフするか、ユーザーのデスクトップがタイムアウトすると、解放された容量（例：M3）がバッファとして利用可能になります。その結果、容量バッファが10%に設定されているため、AutoscaleはマシンM4の電源をオフにし始めます。
- ユーザーがいなくなるまで、さらに多くのユーザーがログオフする
  - さらに多くのユーザーがログオフした後、Autoscaleはマシン（例：M2またはM3）の電源をオフにします。

- ユーザーが残っていなくても、Autoscaleは残りの1台のマシン（例：M1）の電源をオフにしません。これは、そのマシンが予備容量として予約されているためです。

> **注:**
>
> シングルセッションOSのランダムデリバリーグループの場合、ユーザーがセッションをログオフすると、デスクトップへのすべての変更は失われます。ただし、構成されている場合、ユーザー固有の設定はユーザープロファイルとともにローミングされます。

シングルセッションOSの静的デリバリーグループ

キャパシティバッファは、デリバリーグループ内の未割り当てマシンの総数に基づいて、未割り当てマシンのバッファの電源をオンに保つことで、急な需要の急増に対応するために使用されます。デフォルトでは、キャパシティバッファはデリバリーグループ内の未割り当てマシンの総数の10%です。

> **重要:**
>
> デリバリーグループ内のすべてのマシンが割り当てられた後、容量バッファはマシンの電源オン/オフには影響しません。

> マシン数（容量バッファを含む）が現在電源がオンになっているマシンの総数を超える場合、需要を満たすために追加の未割り当てマシンが電源オンになります。マシン数（容量バッファを含む）が現在電源がオンになっているマシンの総数より少ない場合、設定したアクションに応じて、余分なマシンは電源オフまたは一時停止されます。

シングルセッションOS静的デリバリーグループの場合、Autoscaleは次のようになります。

- 該当するシングルセッションOSデリバリーグループの`AutomaticPowerOnForAssigned`プロパティがtrueに設定されている場合にのみ、ピーク時に割り当て済みマシンの電源をオンにし、オフピーク時に電源をオフにします。
- ピーク時にマシンが電源オフであり、かつそのマシンが属するデリバリーグループの`AutomaticPowerOnForAssignedDuringPeak`プロパティがtrueに設定されている場合、自動的に電源をオンにします。

割り当てられたマシンで容量バッファがどのように機能するかを理解するには、以下を考慮してください。

- 容量バッファは、デリバリーグループに1つ以上の未割り当てマシンがある場合にのみ機能します。
- デリバリーグループに未割り当てのマシンがない場合 (デリバリーグループ内のすべてのマシンが割り当てられている場合)、容量バッファはマシンの電源オン/オフに影響しません。
- `AutomaticPowerOnForAssignedDuringPeak`プロパティは、ピーク時に割り当てられたマシンの電源がオンになるかどうかを決定します。trueに設定されている場合、Autoscaleはピーク時にマシンの電源をオンのままにします。Autoscaleは、電源がオフになっている場合でも、それらの電源をオンにします。

電源ポリシー

さまざまなシナリオでマシンの電源を管理するためのポリシーを構成します。各シナリオについて、待機時間 (分単位) と、指定された時間が終了した後に実行するアクションを指定できます。電源ポリシーは、シングルセッションOSランダムデリバリーグループとシングルセッションOS静的デリバリーグループに適用されます。

シングルセッションOS静的DG電源ポリシー設定(/en-us/citrix-virtual-apps-desktops/2411/media/single-session-os-static-dg-power-policies-settings.png)

切断後および**ログオフ後**の場合、以下の設定はピーク時とオフピーク時の両方に適用されます。ドロップダウンから、待機時間 (分単位) と、アクション (アクションなし、一時停止、シャットダウンなど) を設定できます。

Autoscaleによってマシンの電源がオンになった後、ユーザーがログオンしない場合、以下の設定はピーク時にのみ適用されます。ピーク時に、ドロップダウンから待機時間 (分単位) と、アクション (アクションなし、一時停止、シャットダウンなど) を設定できます。

例のシナリオ

次のシナリオがあるとします。

- **デリバリーグループの構成**。Autoscaleで電源管理するデリバリーグループには、10台のマシン (M1～M10) が含まれています。
- **Autoscaleの構成**
  - マシンM1～M3は割り当て済みで、マシンM4～M10は未割り当てです。
  - ピーク時とオフピーク時でキャパシティバッファを10%に設定。
  - 選択されたスケジュールに従って、Autoscaleは午前9時から午後6時の間、マシンの電源を管理します。

上記のシナリオでAutoscaleがどのように機能するかについては、以下を参照してください。

- スケジュール開始 – 午前9時
  - AutoscaleはマシンM1からM3の電源をオンにします。
  - 設定されたキャパシティバッファにより、Autoscaleは追加のマシン（例: M4）の電源をオンにします。マシンM4は割り当てられていません。
- 最初のユーザーがログオンします
  - ユーザーがデスクトップを使用するために初めてログオンすると、割り当てられていない電源オン状態のマシンでホストされているデスクトップのプールからデスクトップが割り当てられます。この場合、ユーザーにはマシンM4からデスクトップが割り当てられます。そのユーザーによるその後のログオンは、初回使用時に割り当てられたのと同じデスクトップに接続されます。
  - 設定されたキャパシティバッファにより、Autoscaleは需要を満たすため、追加のマシン（例: M5）の電源をオンにし始めます。
- 2番目のユーザーがログオンします
  - ユーザーには、割り当てられていない電源オン状態のマシンからデスクトップが割り当てられます。この場合、ユーザーにはマシンM5からデスクトップが割り当てられます。そのユーザーによるその後のログオンは、初回使用時に割り当てられたのと同じデスクトップに接続されます。
  - 設定されたキャパシティバッファにより、Autoscaleは需要を満たすため、追加のマシン（例: M6）の電源をオンにし始めます。
- ユーザーがログオフします
  - ユーザーがデスクトップからログオフするか、デスクトップがタイムアウトすると、Autoscaleは午前9時から午後6時の間、マシンM1からM5の電源をオンのままにします。これらのユーザーが次回ログオンするときは、初回使用時に割り当てられたのと同じデスクトップに接続されます。
  - 割り当てられていないマシンM6は、受信する割り当てられていないユーザーにデスクトップを提供するのを待機しています。
- スケジュールの終了 – 午後 6 時
  - 午後 6 時、Autoscale はマシン M1 から M5 の電源をオフにします。
  - Autoscale は、構成されたキャパシティバッファのため、割り当てられていないマシン M6 の電源をオンのままにします。そのマシンは、着信する割り当てられていないユーザーにデスクトップを提供するのを待機しています。

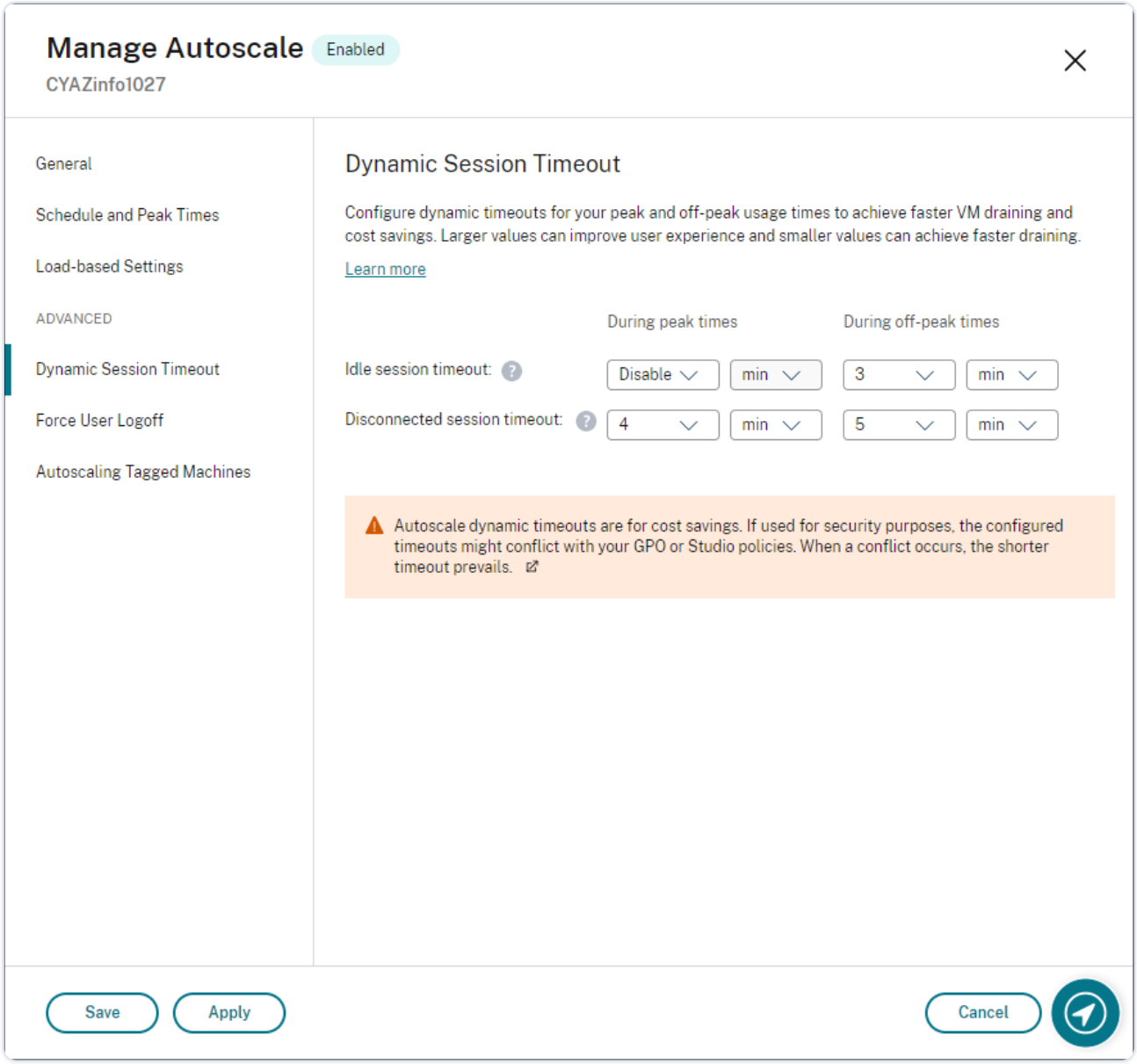
- デリバリーグループでは、マシン M6 から M10 は割り当てられていないマシンです。

動的セッションタイムアウト

この機能を使用すると、ピーク時とオフピーク時の使用時間に合わせて、切断されたセッションとアイドルセッションのタイムアウトを設定し、より迅速なマシンのドレインとコスト削減を実現できます。この機能は以下に適用されます。

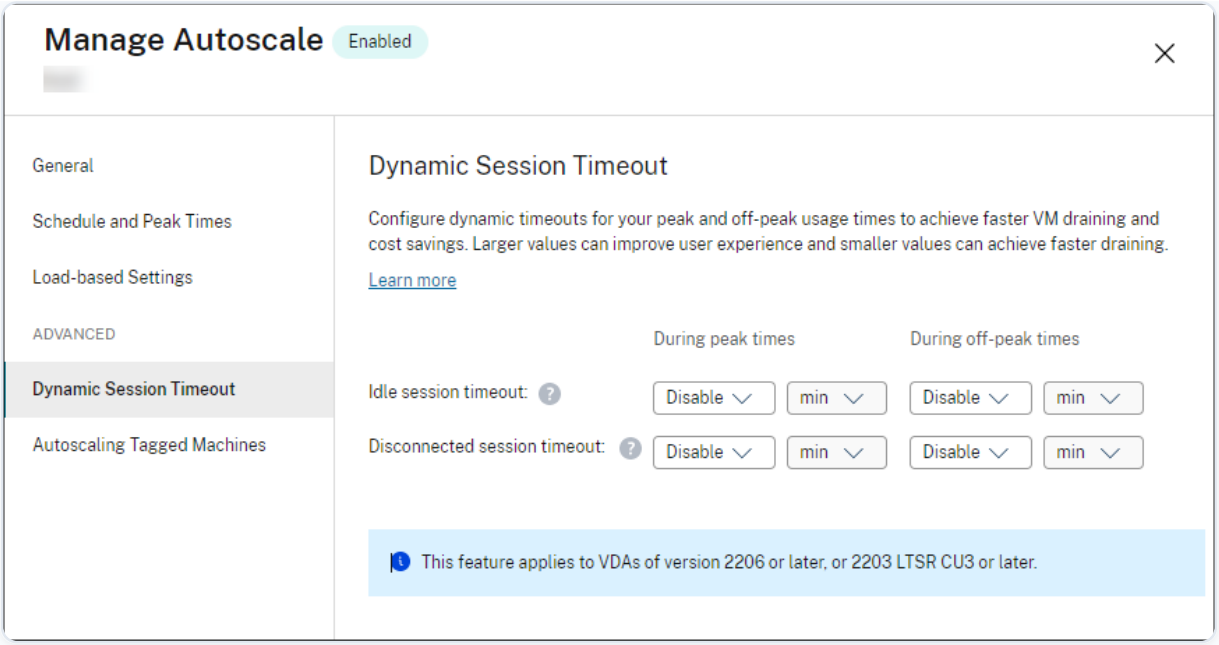
- シングルセッションおよびマルチセッションOSマシン。
- オートスケール用にタグ付けされているかどうかにかかわらず、デリバリーグループ内のすべてのマシン。

VDAは、10分以上アイドル状態になっているセッションのアイドル時間を報告するため、動的セッションタイムアウトは、アイドル状態になってから10分以内にアイドルセッションを切断することはできません。より短い値を設定すると、残存するセッションがより早く削除され、コストが削減されます。



注:

- この機能は、マルチセッションOSデリバリーグループで常に利用可能です。
- シングルセッションOSデリバリーグループの場合、この機能はバージョン2206 CR以降、または2203 LTSR CU3以降のVDAに適用されます。これらのVDAがCitrix Cloud™に少なくとも1回登録されていることを確認してください。利用できない場合、次のユーザーインターフェイスが表示されます。



- Autoscale™の動的タイムアウトはコスト削減を目的としています。セキュリティ目的で使用する場合、設定されたタイムアウトがGPOまたは管理コンソールポリシーと競合する可能性があります。競合が発生した場合、より短いタイムアウトが優先されます。

アイドルセッションタイムアウト。ユーザー入力がない場合に、中断されないユーザー接続が維持される期間を指定するタイマーを有効または無効にします。タイマーが期限切れになると、セッションは切断状態になり、**切断されたセッションタイムアウト**が適用されます。**切断されたセッションタイムアウト**が無効になっている場合、セッションはログオフされません。

重要:

- 10分（600秒）以下の値を指定した場合、Autoscaleは、関連するセッションが10分間アイドル状態になった後に切断します。これは、AutoscaleがVDAが報告するセッションのアイドル時間に依存しているためです。VDAは、10分以上アイドル状態になっているセッションのアイドル時間のみを報告します。
- アイドルセッションは、ユーザーがアイドルセッションタイムアウトに達するまでの最後の5分以内に操作した場合でも、切断状態に移行する可能性があります。

> **切断セッションタイムアウト**。切断されたデスクトップがログオフされるまでロックされたままになる時間を指定するタイマーを有効または無効にします。有効になっている場合、タイマーが期限切れになると切断されたセッションはログオフされます。

FAQ

動的セッションタイムアウト機能は、オートスケール用にタグ付けされたマシンにのみ適用されます?

動的セッションタイムアウト機能は、オートスケール用にタグ付けされているかどうかに関係なく、デリバリーグループ内のすべてのマシンに適用されます。

動的セッションタイムアウトによりセッションがログオフされた場合、タグ付けされていないマシンも、タグ付けされたマシンのオートスケールターゲットに含まれます?

動的セッションタイムアウト機能は、オートスケールのタグ付け機能とは関係ありません。動的セッションタイムアウトによってセッションが終了した場合、マシンがシャットダウンされるまでドレインされていることを条件として、タグ付けされていないマシンもそのプロセス中にシャットダウンされる可能性があります。

タグ付きマシンの自動スケーリング (クラウドバースト)

> **注:**
>
> この機能は以前はAutoscaleの制限でした。

はじめに

Autoscaleは、デリバリーグループ内のマシンの一部のみを電源管理する柔軟性を提供します。これを実現するには、1つ以上のマシンにタグを適用し、その後、Autoscaleを構成してタグ付きマシンのみを電源管理します。

この機能は、クラウドベースのリソースが追加の需要（つまり、バーストワークロード）に対応する前に、オンプレミスリソース（または予約済みのパブリッククラウドインスタンス）を使用してワークロードを処理したいクラウドバーストのユースケースで役立ちます。オンプレミスのマシン（または予約済みインスタンス）に最初にワークロードを処理させるには、タグ制限とゾーン優先度を組み合わせて使用する必要があります。

タグ制限は、Autoscaleによって電源管理されるマシンを指定します。ゾーン優先度は、ユーザー起動要求を処理するために優先ゾーン内のマシンを指定します。詳細については、「タグ」および「ゾーン優先度」を参照してください。

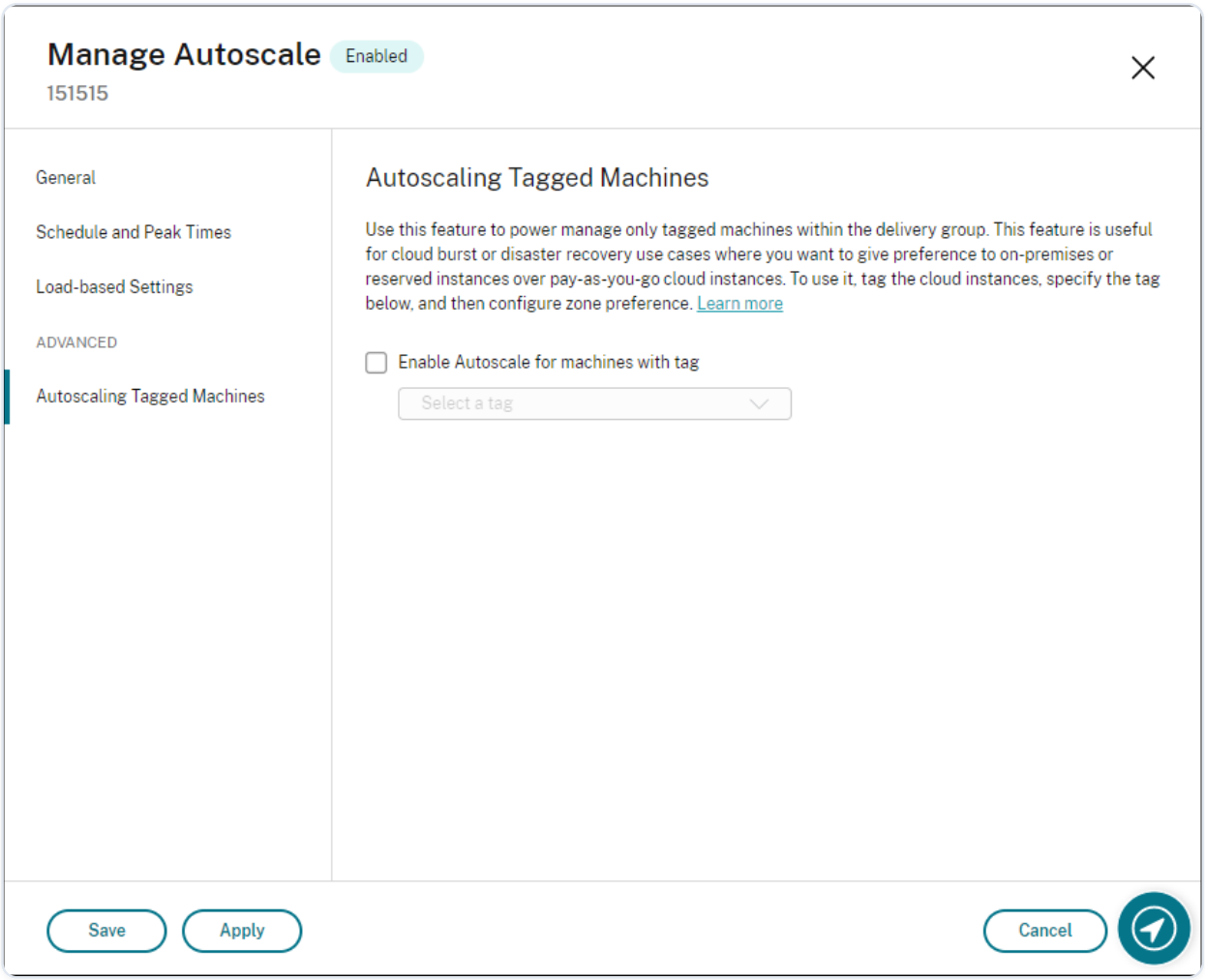
特定のタグ付きマシンを自動スケーリングするには、ManageコンソールまたはPowerShellを使用できます。

Manageコンソールを使用して特定のタグ付きマシンを自動スケーリングする

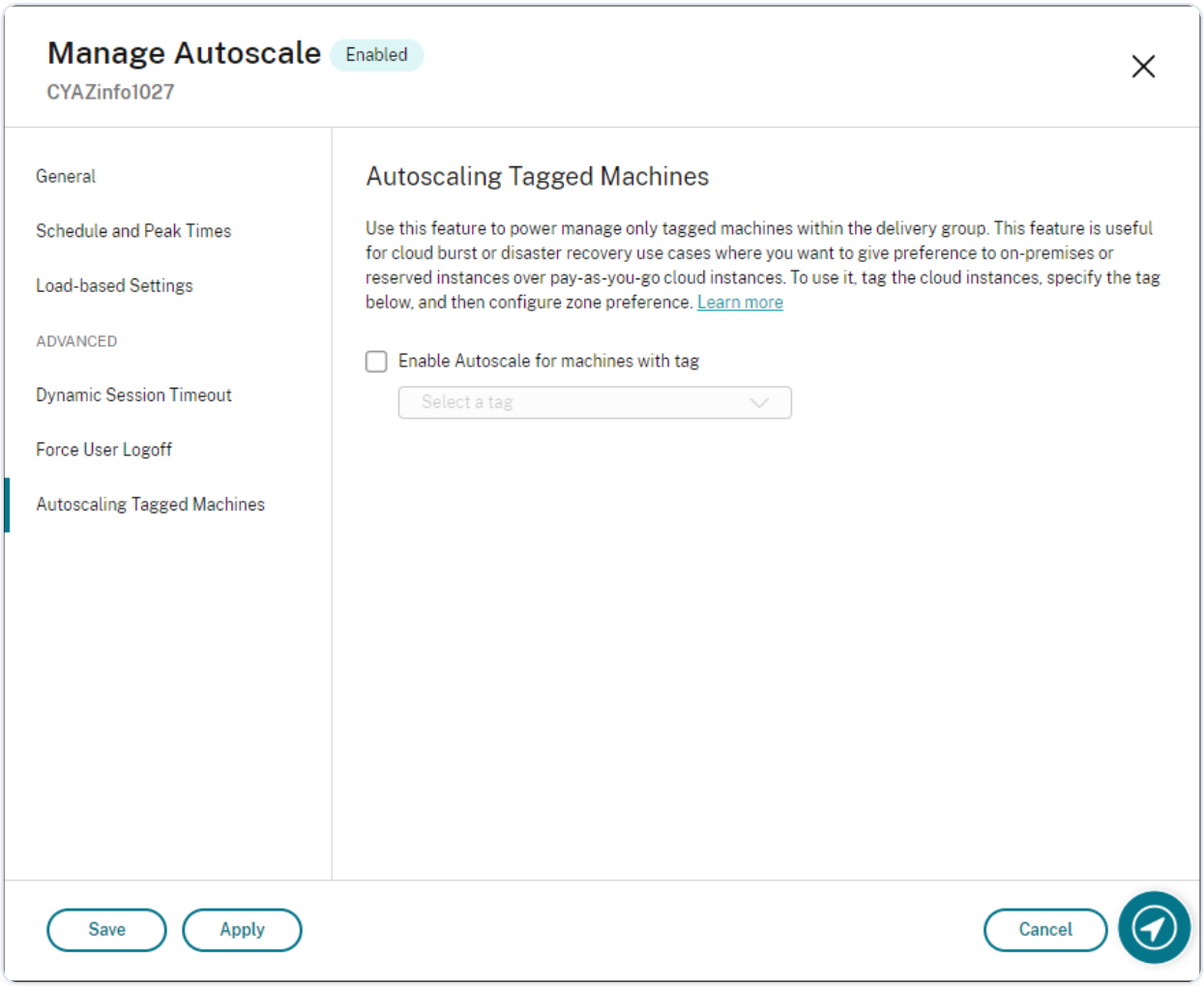
特定のタグ付きマシンを自動スケーリングするには、次の手順を実行します。

1. タグを作成し、そのタグをデリバリーグループ内の該当するマシンに適用します。詳細については、「タグとタグ制限の管理」を参照してください。
2. デリバリーグループを選択し、**Manage Autoscale** ウィザードを開きます。
3. **タグ付きマシンの自動スケーリング**ページで、**タグ付きマシンのAutoscaleを有効にする**を選択し、リストからタグを選択し、**適用**をクリックして変更を保存します。

   シングルセッションOSのユーザーインターフェイス (*静的*および *ランダム*なデリバリーグループ):



マルチセッションOSデリバリーグループのユーザーインターフェイス:



警告:

- 特定のタグを持つマシンのAutoscaleにより、ヒストグラムが自動的に更新され、タグごとのマシン数が反映される可能性があります。「**スケジュールとピーク時間**」ページで、必要に応じて各時間帯にマシンを手動で割り当てることができます。
- タグ付きマシンで使用されているタグは削除できません。タグを削除するには、まずタグの制限を解除する必要があります。

タグの制限を適用した後、後でデリバリーグループから削除したい場合があります。その場合は、「**Autoscaleの管理 > タグ付きマシンのAutoscale**」ページに移動し、「**タグ付きマシンのAutoscaleを有効にする**」のチェックを外します。

警告:

- 「**タグ付きマシンのAutoscaleを有効にする**」のチェックを外さずに、該当するマシンからタグを削除すると、「**Autoscaleの管理**」ウィザードを開いたときに警告が表示されることがあります。マシンからタグを削除すると、Autoscaleで指定したタグが無効になるため、Autoscaleが管理するマシンがなくなる可能性があります。この警告を解決するには、「**タグ付きマシンのAutoscale**」ページに移動し、無効なタグを削除して、「**適用**」をクリックして変更を保存します。

Autoscaleがリソースの電源をオンにするタイミングを制御する

また、タグなしマシンの使用状況に基づいて、Autoscaleがタグ付きマシンの電源をオンにし始めるタイミングを制御することもできます。これにより、タグ付きまたはパブリッククラウドのワークロードの消費をさらに最適化できます。

これを行うには、次の手順を完了します:

1. 「**タグ付きマシンのAutoscale**」ページで、「**Autoscaleがタグ付きマシンの電源をオンにし始めるタイミングを制御する**」を選択します。
2. ピーク時とオフピーク時の両方で達成したいタグなしマシンの使用率を入力し、「**適用**」をクリックします。サポートされる値: 0〜100。

Autoscaleがタグ付けされたマシンの電源をオンにし始めるタイミングを制御する(/en-us/citrix-virtual-apps-desktops/2411/media/autoscale-powers-on-tagged-machines.png)

ヒント:

このパーセンテージは、Autoscale がタグ付きマシンの電源をオンにし始めるタイミングを制御します。パーセンテージがしきい値（デフォルトは10%）を下回ると、Autoscale はタグ付きマシンの電源をオンにし始めます。パーセンテージがしきい値を超えると、Autoscale は電源オフモードに入ります。パーセンテージを入力する際は、次の2つのシナリオを考慮してください。

- シングルセッションOSデリバリーグループの場合：この値は、アイドル状態のタグなしマシンの総数に対する割合として定義されます。例：タグなしのシングルセッションOS

マシンが10台あるとします。セッションがないマシンが1台だけになった場合、Autoscale はタグ付きマシンの電源をオンにし始めます。

- マルチセッションOSデリバリーグループの場合：この値は、利用可能なタグなしマシンの総容量（負荷インデックスの観点から）に対する割合として定義されます。例：タグなしのマルチセッションOSマシンが10台あるとします。それらが90%ロードされた場合、Autoscale はタグ付きマシンの電源をオンにし始めます。

PowerShell を使用して特定のタグ付きマシンを自動スケーリングする

PowerShell SDK を直接使用するには、次の手順を完了します。

1. **タグを作成します。** New-Brokertag PowerShell コマンドを使用してタグを作成します。
   - 例：`$managed = New-BrokerTag Managed`。この場合、タグは「Managed」という名前です。New-Brokertag PowerShell コマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/>` を参照してください。
2. **マシンにタグを適用します。** Get-Brokermachine PowerShell コマンドを使用して、Autoscale で電源管理するカタログ内のマシンにタグを適用します。
   - 例：`Get-BrokerMachine -CatalogName "cloud" | Add-BrokerTag $managed.Name`。この場合、カタログは「cloud」という名前です。
   - Get-Brokermachine PowerShell コマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/>` を参照してください。

   注:

   タグを適用した後で、カタログに新しいマシンを追加する場合があります。そのタグは、それらの新しいマシンには自動的に適用*されません*。

3. **Autoscale で電源管理するデリバリーグループにタグ付きマシンを追加します。** Get-BrokerDesktopGroup PowerShell コマンドを使用して、マシンを含むデリバリーグループにタグ制限を追加します（つまり、「タグXを持つマシンへの起動を制限する」）。

- 例：`Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`。この場合、デリバリーグループのUIDは1です。
- Get-BrokerDesktopGroup PowerShell コマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>` を参照してください。

タグ制限を適用した後、後でデリバリーグループから削除したい場合があります。その場合は、Get-BrokerDesktopGroup PowerShellコマンドを使用します。

例: `Get-BrokerDesktopGroup –Uid 1 | Set-BrokerDesktopGroup –RestrictAutoscaleTagUid $null`。この場合、デリバリーグループのUIDは1です。

> **注:**
>
> タグ付けされていないマシンは、ユーザーが電源を切った後、自動的に再起動します。この動作により、ワークロードをより早く処理できるようになります。これは、`Set-BrokerDesktopGroup` の `AutomaticRestartForUntaggedMachines` プロパティを使用して、デスクトップグループごとに有効または無効にできます。詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>` を参照してください。

例のシナリオ

次のシナリオを想定します。

- **マシンカタログの構成**。2つのマシンカタログ（C1とC2）があります。
  - カタログC1には、オンプレミス展開にローカルな5台のマシン（M1～M5）が含まれています。
  - カタログC2には、クラウド展開にリモートな5台のマシン（M6～M10）が含まれています。
- **タグ制限**。「Cloud」という名前のタグが作成され、カタログC2内のマシンM6～M10に適用されます。
- **ゾーン構成**。2つのゾーン（Z1とZ2）が作成されます。
  - カタログC1を含むゾーンZ1は、オンプレミス展開に対応します。

- カタログC2を含むゾーンZ2は、クラウド展開に対応します。

- **デリバリーグループの構成**
  - デリバリーグループには、10台のマシン（M1～M10）が含まれており、そのうち5台はカタログC1（M1～M5）から、5台はカタログC2（M6～M10）からです。
  - M1からM5までのマシンは手動で電源がオンにされ、スケジュール期間中ずっとオンのままです。

- **Autoscale構成**
  - 容量バッファは10%に設定されています。
  - Autoscaleは「Cloud」タグを持つマシンのみを電源管理します。この場合、Autoscaleはクラウドマシン M6からM10を電源管理します。

- **公開アプリケーションまたはデスクトップ構成**。公開デスクトップ（例）にはゾーン設定が構成されており、ユーザー起動要求ではゾーンZ2よりもゾーンZ1が優先されます。
  - ゾーンZ1は、公開デスクトップの優先ゾーン（ホームゾーン）として構成されています。

このシナリオは、次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. 利用可能なすべてのオンプレミス・マシンが消費されるまで、ユーザーセッションはさらに増加します。
4. さらにユーザーセッションが開始されます。
5. セッション終了によりユーザーセッションが減少します。
6. セッション負荷がオンプレミス・マシンのみで処理されるまで、ユーザーセッションはさらに減少します。

上記シナリオにおけるAutoscaleの動作の詳細については、以下を参照してください。

- ユーザー負荷なし（初期状態）
  - オンプレミス マシン M1 から M5 はすべて電源オンになっています。
  - クラウド内のマシン (例: M6) が 1 台電源オンになっています。このマシンは、構成された容量バッファのために電源オンになっています。この場合、10 (マシン数) x 10,000 (ロードインデックス) x 10% (構成された容量バッファ) は 10,000 になります。したがって、マシンが 1 台電源オンになります。

  - 電源オンになっているすべてのマシン (M1 から M6) のロードインデックス値は、ベースライン負荷 (ロードインデックスは 0) です。

- ユーザーがログオンします
  - セッションは、構成されたゾーン優先度を通じてマシン M1 から M5 でホストされるように指示され、これらのオンプレミス マシン間で負荷分散されます。
  - 電源オンになっているマシン (M1 から M5) のロードインデックス値が増加します。
  - 電源オンになっているマシン M6 のロードインデックス値は、ベースライン負荷です。
- ユーザーが負荷を増やし、すべてのオンプレミス リソースを消費します
  - セッションは、構成されたゾーン優先度を通じてマシン M1 から M5 でホストされるように指示され、これらのオンプレミス マシン間で負荷分散されます。
  - 電源オンになっているすべてのマシン (M1 から M5) のロードインデックス値が 10,000 に達しました。
  - 電源オンになっているマシン M6 のロードインデックス値は、ベースライン負荷のままです。
- もう 1 人のユーザーがログオンします
  - セッションはゾーン優先度を超過し、クラウド マシン M6 でホストされるように指示されます。
  - 電源オンになっているすべてのマシン (M1 から M5) のロードインデックス値が 10,000 に達しました。
  - 電源オンになっているマシン M6 のロードインデックス値が増加し、ベースライン負荷ではなくなります。合計予備容量がロードインデックスで 10,000 を下回るレベルに低下すると、構成された容量バッファのために、Autoscale は需要を満たすために追加のマシン (M7) の電源をオンにし始めます。マシン M7 の電源をオンにするには時間がかかる場合があることに注意してください。そのため、マシン M7 が準備できるまでに遅延が発生する可能性があります。
- さらに多くのユーザーがログオンします
  - セッションはマシンM6でホストされるように指示されます。
  - 起動中のすべてのマシン (M1～M5) のロードインデックス値が10,000に達しました。
  - 起動中のマシンM6のロードインデックス値はさらに増加しますが、ロードインデックスで合計予備容量は10,000を上回るレベルにあります。
  - 起動中のマシンM7のロードインデックス値は、ベースライン負荷のままです。

- さらに多くのユーザーがログオンします
  - マシンM7の準備ができた後、セッションはマシンM6とM7でホストされるように指示され、これらのマシン間で負荷分散されます。
  - 起動中のすべてのマシン (M1～M5) のロードインデックス値が10,000に達しました。
  - マシンM7のロードインデックス値は、ベースライン負荷ではなくなります。
  - 稼働中のマシン (M6 および M7) の負荷インデックス値が増加します。
  - 負荷インデックスの観点から、総予備容量は依然として10,000を超えるレベルにあります。
- セッション終了により、ユーザーセッションの負荷が減少します。
  - ユーザーがセッションからログオフするか、アイドルセッションがタイムアウトすると、マシンM1からM7で解放された容量は、他のユーザーが開始したセッションをホストするために再利用されます。
  - 負荷インデックスの観点から総予備容量が10,000を超えるレベルに増加すると、Autoscaleはクラウドマシン (M6からM7) の1つをドレイン状態にします。その結果、新しい変更が発生しない限り、他のユーザーが開始したセッションはそのマシン (たとえばM7) には転送されなくなります。たとえば、ユーザー負荷が再び増加したり、他のクラウドマシンの負荷が最も低くなったりした場合です。
- 1つ以上のクラウドマシンが不要になるまで、ユーザーセッション負荷はさらに減少します。
  - M7マシン上のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、AutoscaleはM7マシンの電源をオフにします。
  - 電源がオンになっているすべてのマシン（M1からM5）のロードインデックス値は、10,000未満のレベルに低下する可能性があります。
  - 電源がオンになっているマシン（M6）のロードインデックス値は減少します。
- クラウドマシンが不要になるまで、ユーザーセッションはさらに減少します。
  - マシンM6にユーザーセッションがない場合でも、Autoscaleは予備容量として予約されているため、電源をオフにしません。
  - Autoscaleは、構成された容量バッファのため、残りのクラウドマシンM6の電源をオンのままにします。そのマシンは、着信するユーザーにデスクトップを提供するのを待機しています。
  - オンプレミス環境のマシンに利用可能な容量がある限り、セッションはマシンM6でホストされるようには転送されません。

ユーザーログオフ通知

重要:

この機能は、マルチセッションアプリベースのデリバリーグループ向けのAutoscale™ユーザーインターフェイスでのみ利用できます。

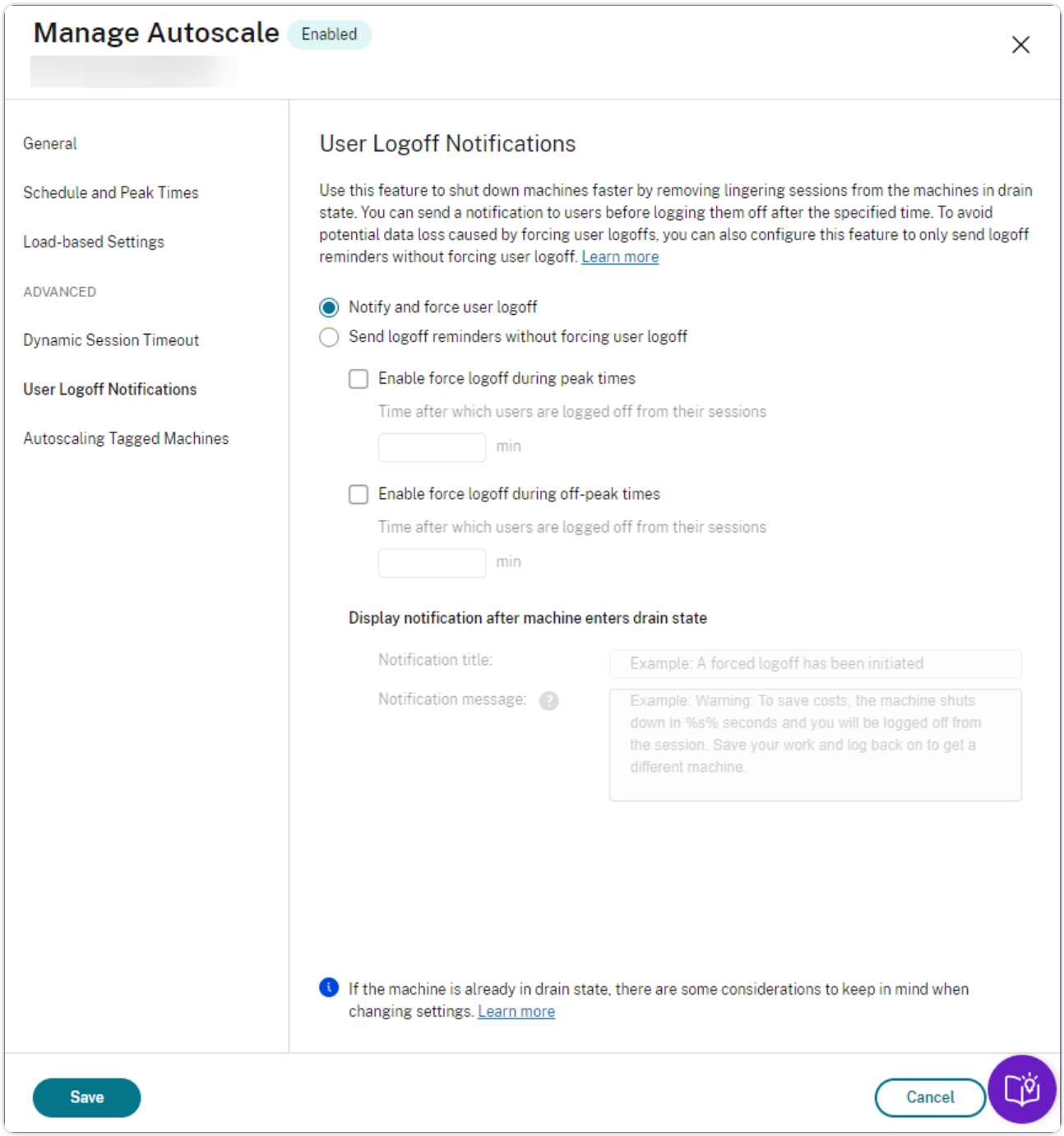
コスト削減をより効果的に実現するため、Autoscaleでは、残存セッションを強制的にログオフできます。これは、ユーザーにカスタム通知を送信し、セッションが強制的にログオフされるまでの猶予期間を指定することで行われます。これは、ドレイン状態のマシンに対してのみ行われ、すべての電源オンのマシンに対して行われるわけではありません。ユーザーの強制ログオフによって発生する可能性のあるデータ損失を回避するため、この機能は、ユーザーのログオフを強制することなく、ログオフのリマインダーのみを送信するように構成することもできます。

以下の2つのオプションがあります。

- **通知してユーザーを強制ログオフする**
- **ユーザーのログオフを強制せずにログオフリマインダーを送信する**

ユーザーに通知してログオフを強制する

選択した場合、Autoscaleは、以下で指定された時間が経過した後、ユーザーをセッションからログオフします。



ピーク時の強制ログオフを有効にする。選択した場合、Autoscaleは、指定された時間が経過すると、ピーク時にそれらのユーザーをセッションからログオフします。

オフピーク時の強制ログオフを有効にする。選択した場合、Autoscaleは、指定された時間が経過すると、オフピーク時にそれらのユーザーをセッションからログオフします。

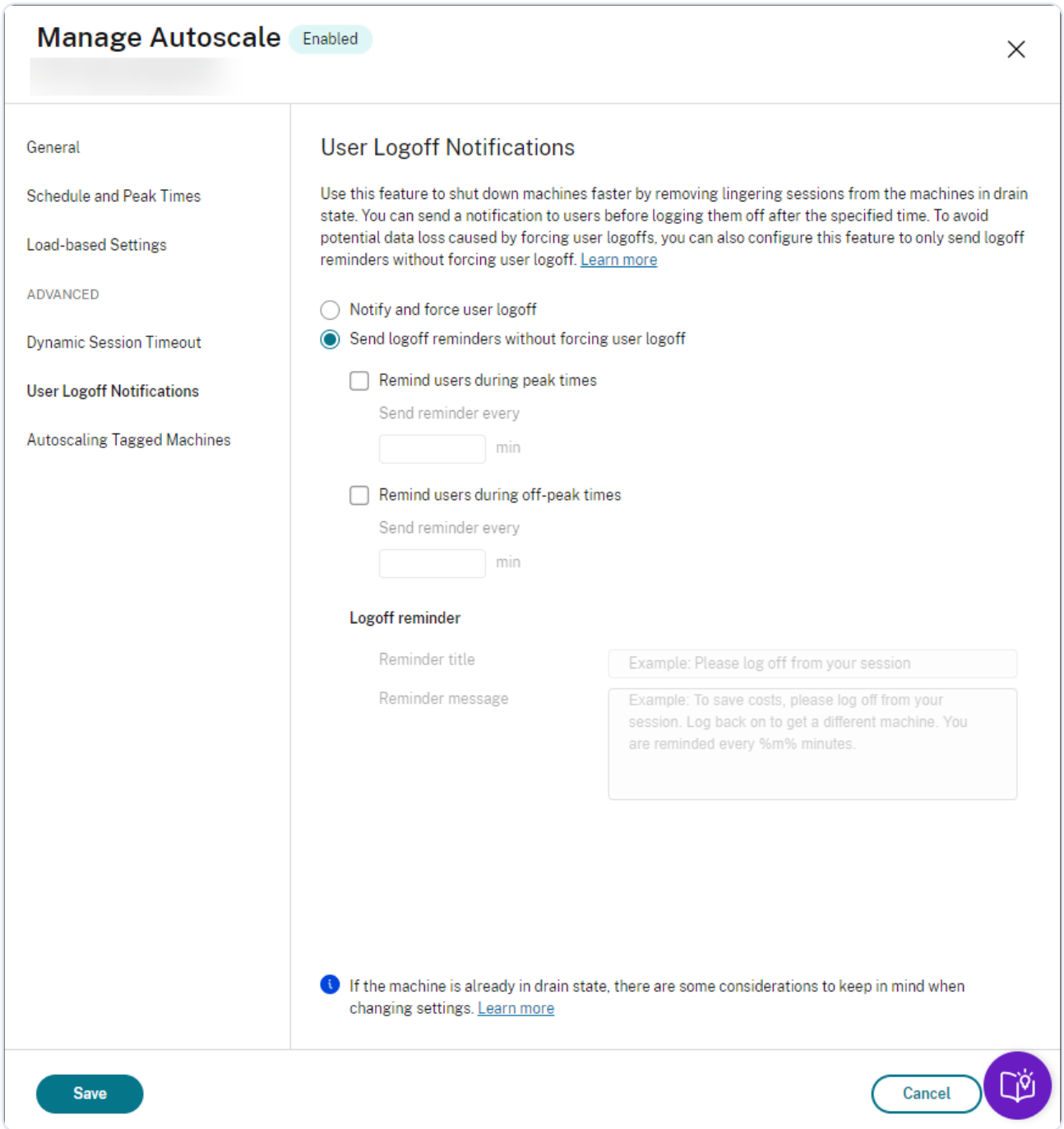
マシンがドレイン状態になった後に通知を表示する。マシンがドレイン状態になった後、ユーザーに通知を送信できます。

- **通知のタイトル。**ユーザーに送信する通知のタイトルを指定できます。例：`A forced logoff has been initiated.`.

- **通知メッセージ**。ユーザーに送信する通知の内容を指定できます。メッセージ内で指定された時間を示す変数として、%s% または %m% を使用できます。時間を秒で表すには、%s% を使用します。時間を分で表すには、%m% を使用します。例：`Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine.`.

ユーザーのログオフを強制せずにログオフのリマインダーを送信する

これを選択すると、マシンがドレイン状態になった後、ユーザーはマシンからログオフするようリマインダーを受け取ります。このリマインダーは、以下で指定された間隔で送信されるように設定できます。



ピーク時にユーザーにリマインダーを送信する。これを選択すると、ユーザーはピーク時にX分ごとにセッションからログオフするようリマインダーを受け取ります（Xは指定された時間を示します）。

オフピーク時にユーザーにリマインダーを送信する。これを選択すると、ユーザーはオフピーク時にX分ごとにセッションからログオフするようリマインダーを受け取ります（Xは指定された時間を示します）。

ログオフリマインダー。マシンがドレイン状態になった後、ユーザーに送信されるリマインダーを設定できます。

- **リマインダーのタイトル**。ユーザーに送信するリマインダーのタイトルを指定できます。例: `Please log off from your session`。
- **リマインダーメッセージ**。ユーザーに送信するメッセージを指定できます。例: `Please log off from your session and log back on to save costs`。

考慮事項

マシンがすでにドレイン状態である場合、設定を変更する際には以下を考慮してください。

- 設定を**ユーザーのログオフを強制せずにログオフのリマインダーを送信する**から**通知してユーザーのログオフを強制する**に変更した場合、新しい設定はすぐに有効になります。
- 設定を**通知してユーザーのログオフを強制する**から**ユーザーのログオフを強制せずにログオフのリマインダーを送信する**に変更した場合、新しい設定はマシンが次にドレイン状態になるまで有効になりません。ユーザーは引き続きログオフを強制されます。

Broker PowerShell SDKコマンド

Broker PowerShell SDKを使用して、デリバリーグループのAutoscaleを構成できます。PowerShellコマンドを使用してAutoscaleを構成するには、PowerShell SDKバージョン7.21.0.12以降を使用する必要があります。PowerShell SDKの詳細については、「SDKとAPI」(/ja-jp/citrix-virtual-apps-desktops/2411/sdk-api.html)を参照してください。

Set-BrokerDesktopGroup

既存の BrokerDesktopGroup を無効または有効にするか、その設定を変更します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>` を参照してください。

例

PowerShellコマンドレットの使用方法の詳細については、以下の例を参照してください。

Autoscale™を有効にする

- 名前が「MyDesktop」であるデリバリーグループに対して Autoscale を有効にしたいとします。`Set-BrokerDesktopGroup` PowerShell コマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -AutoscalingEnabled $true`

ピーク時とオフピーク時で容量バッファを個別に構成する

- 名前が「MyDesktop」であるデリバリーグループに対して、容量バッファをピーク時は 20%、オフピーク時は 10% に設定したいとします。`Set-BrokerDesktopGroup` PowerShell コマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakBufferSizePercent 20 -OffPeakBufferSizePercent 10`

切断時のタイムアウト設定を構成する

- 名前が「MyDesktop」であるデリバリーグループに対して、**切断時のタイムアウト**値をピーク時は 60 分、オフピーク時は 30 分に設定したいとします。`Set-BrokerDesktopGroup` PowerShell コマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakDisconnectTimeout 60 -OffPeakDisconnectTimeout 30`

「**when logged off timeout**」設定を構成する

- 名前が「MyDesktop」であるデリバリーグループに対して、ピーク時には**when logged off timeout**値を60分に、オフピーク時には30分に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例：
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakLogOffTimeout 60 -OffPeakLogOffTimeout 30`

「**power-off delay**」設定を構成する

- 名前が「MyDesktop」であるデリバリーグループに対して、パワーオフ遅延を15分に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例：
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PowerOffDelay 15`

パワーオフ遅延が適用されない期間を構成する

- 名前が「MyDesktop」であるデリバリーグループに対して、パワーオフ遅延が30分経過するまで有効になるようにしたいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例：
  - `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -SettlementPeriodBeforeAutoShutdown 30`.

「**machine instance cost**」設定を構成する

- 名前が「MyDesktop」であるデリバリーグループに対して、マシンインスタンスの1時間あたりのコストを0.2ドルに設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例：
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -MachineCost 0.2`

New-BrokerPowerTimeScheme

デリバリーグループのBrokerPowerTimeSchemeを作成します。詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/>`を参照してください。

例

UID値が3のデリバリーグループに対して電源時間スキームを作成したいとします。新しいスキームは週末、月曜日、火曜日を対象とします。午前8時から午後6時30分までの時間帯は、スキームに含まれる日のピーク時間として定義されます。ピーク時間の場合、プールサイズ（電源がオンのまま維持されるマシンの数）は20です。オフピーク時間の場合、それは5です。`Set-BrokerDesktopGroup` PowerShellコマンドを使用できます。例：

- `PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { 5 } else { 20 } } )`
- `PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { $false } else { $true } } )`
- `PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week' -DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48`

動的セッションタイムアウトのパラメーター

以下のBroker PowerShell SDKコマンドレットは、複数の新しいパラメーターをサポートすることで、動的セッションタイムアウトのために拡張されました。

- Get-BrokerDesktopGroup

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

これらのパラメーターには以下が含まれます。

- **DisconnectPeakIdleSessionAfterSeconds** – ピーク時にアイドル状態のセッションが切断されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、ピーク時の関連動作が無効になっていることを示します。0より大きい値は、ピーク時のみデリバリーグループの動作を有効にします。
- **DisconnectOffPeakIdleSessionAfterSeconds** - オフピーク時にアイドル状態のセッションが切断されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、オフピーク時の関連動作が無効になっていることを示します。0より大きい値は、オフピーク時のみデリバリーグループの関連動作を有効にします。
- **LogoffPeakDisconnectedSessionAfterSeconds** - ピーク時に切断されたセッションが終了されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、ピーク時の関連動作が無効になっていることを示します。0より大きい値は、ピーク時のみデリバリーグループの関連動作を有効にします。
- **LogoffOffPeakDisconnectedSessionAfterSeconds** - オフピーク時に切断されたセッションが終了されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、オフピーク時の関連動作が無効になっていることを示します。0より大きい値は、ピーク時のみデリバリーグループの関連動作を有効にします。

例

「MyDesktop」という名前のデリバリーグループのピーク時に、アイドルセッションタイムアウトを3,600秒に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例：

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -DisconnectOffPeakIdleSessionAfterSeconds 3600`

これにより、「MyDesktop」という名前のデスクトップグループの場合、オフピーク時に1時間以上アイドル状態だったセッションが切断されます。

シトリックス インサイト サービス

Citrix Insight Services (CIS) は、計測、テレメトリー、ビジネスインサイト生成のためのCitrixプラットフォームです。その計測およびテレメトリー機能により、技術ユーザー（顧客、パートナー、エンジニア）は問題を自己診断して修正し、環境を最適化できます。CISの詳細と最新情

報、およびその仕組みについては、`<https://cis.citrix.com>`（Citrixアカウントの資格情報が必要です）を参照してください。

Citrixにアップロードされるすべての情報は、トラブルシューティングと診断の目的、および製品の品質、信頼性、パフォーマンスの向上に使用されます。ただし、以下の条件に従います。

- シトリックス インサイト サービス ポリシー (https://cis.citrix.com/legal)
- Citrixプライバシーポリシー（`<https://www.cloud.com/privacy-policy>`）

このCitrix Virtual Apps and Desktops™リリースは、以下のテクノロジーをサポートしています。

- Citrix Virtual Apps and Desktopsのインストールとアップグレードの分析
- Citrixカスタマーエクスペリエンス向上プログラム（CEIP）
- シトリックス コールホーム
- シトリックス スカウト

CISおよびCitrix Analyticsとは別に、Studioをインストール（またはアップグレード）すると、Google Analyticsが自動的に収集され（その後アップロードされます）。Studioのインストール後、レジストリキー HKLM\\Software\\Citrix\\DesktopStudio\\GAEnabled を使用してこの設定を変更できます。値が1の場合、収集とアップロードが有効になり、0の場合、収集とアップロードが無効になります。

インストールおよびアップグレード分析

フルプロダクトインストーラーを使用してCitrix Virtual Apps and Desktopsコンポーネントを展開またはアップグレードすると、インストールプロセスに関する匿名情報が収集され、コンポーネントをインストール/アップグレードしているマシンに保存されます。このデータは、Citrixが顧客のインストールエクスペリエンスを向上させるのに役立てられます。

情報は、%ProgramData%\\Citrix\\CTQs にローカルに保存されます。

このデータの自動アップロードは、フルプロダクトインストーラーのグラフィカルインターフェイスとコマンドラインインターフェイスの両方で、デフォルトで有効になっています。

- レジストリ設定のデフォルト値を変更できます。インストール/アップグレードの前にレジストリ設定を変更すると、フルプロダクトインストーラーを使用する際にその値が使用されます。
- コマンドラインインターフェイスを使用してインストール/アップグレードする場合、コマンドでオプションを指定することで、デフォルト設定を上書きできます。

自動アップロードの制御:

- インストール/アップグレード分析の自動アップロードを制御するレジストリ設定 (デフォルト = 1):
  - 場所: `HKLM:\Software\Citrix\MetaInstall`
  - 名前: SendExperienceMetrics
  - 値: 0 = 無効、1 = 有効
- PowerShell を使用すると、次のコマンドレットでインストール/アップグレード分析の自動アップロードが無効になります:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
SendExperienceMetrics -PropertyType DWORD -Value 0
```

- XenDesktopServerSetup.exe または XenDesktopVDASetup.exe コマンドで自動アップロードを無効にするには、`/disableexperiencemetrics` オプションを含めます。

  XenDesktopServerSetup.exe または XenDesktopVDASetup.exe コマンドで自動アップロードを有効にするには、`/sendexperiencemetrics` オプションを含めます。

Citrixカスタマーエクスペリエンス向上プログラム

Citrixカスタマーエクスペリエンス向上プログラム (CEIP) に参加すると、匿名の統計情報と使用状況情報が Citrix に送信され、Citrix 製品の品質とパフォーマンスの向上に役立てられます。詳細については、https://more.citrix.com/XD-CEIP を参照してください。

サイト作成時またはアップグレード時の登録

サイトを作成すると (最初の Delivery Controller™ をインストールした後)、CEIP に自動的に登録されます。最初のデータアップロードは、サイト作成後約7日で行われます。

サイト作成後、いつでも参加を停止できます。Web Studio の左ペインで ノードを選択し、 設定をオフにします。

Citrix Virtual Apps and Desktops 展開をアップグレードする場合:

- CEIPをサポートしていなかったバージョンからアップグレードする場合、参加を希望するかどうか尋ねられます。
- CEIPをサポートしていたバージョンからアップグレードし、参加が有効になっていた場合、アップグレードされたSiteでCEIPが有効になります。
- CEIPをサポートしていたバージョンからアップグレードし、参加が無効になっていた場合、アップグレードされたSiteでCEIPが無効になります。

- CEIPをサポートしていたバージョンからアップグレードし、参加が不明な場合、参加を希望するかどうか尋ねられます。

収集された情報は匿名であるため、Citrix Insight Servicesにアップロードされた後は閲覧できません。

VDAインストール時の登録

デフォルトでは、Windows VDAをインストールすると、CEIPに自動的に登録されます。このデフォルト設定はレジストリ設定で変更できます。VDAをインストールする前にレジストリ設定を変更した場合、その値が使用されます。

CEIPへの自動登録を制御するレジストリ設定（デフォルト = 1）：

場所: HKLM: `\\Software\Citrix\Telemetry\CEIP` 名前: Enabled 値: 0 = 無効, 1 = 有効

デフォルトでは、`Enabled` プロパティはレジストリで非表示になっています。指定されていない場合、自動アップロード機能が有効になります。

PowerShellを使用すると、次のコマンドレットでCEIPへの登録を無効にできます。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled
-PropertyType DWORD -Value 0
```

収集されたランタイムデータポイントは、定期的にファイルとして出力フォルダー（デフォルト %programdata%/Citrix/VdaCeip）に書き込まれます。

データの初回アップロードは、VDAのインストール後約7日で行われます。

その他の製品およびコンポーネントのインストール時の登録

Citrix Provisioning™、AppDNA、Citrix License Server、Windows 用 Citrix Workspace™ アプリ、Universal Print Server、Session Recording など、関連する Citrix 製品、コンポーネント、テクノロジーをインストールする際にも、CEIP に参加できます。インストールと参加のデフォルト値の詳細については、各製品のドキュメントを参照してください。

Citrix コールホーム

Citrix Virtual Apps and Desktops の特定のコンポーネントと機能をインストールすると、Citrix Call Home に参加する機会が提供されます。Call Home は診断データを収集し、そのデータを含むテレメトリパッケージを分析とトラブルシューティングのために Citrix Insight Services に直接 (デフォルトポート 443 の HTTPS 経由で) 定期的にアップロードします。

Citrix Virtual Apps and Desktops では、Call Home は Citrix Telemetry Service という名前のバックグラウンドサービスとして実行されます。

Call Home のスケジュール機能は Citrix Scout でも利用できます。詳細については、Citrix Scout を参照してください。

収集される情報

Citrix Diagnostic Facility (CDF) トレースは、トラブルシューティングに役立つ情報をログに記録します。Call Home は、VDA 登録やアプリケーション/デスクトップの起動など、一般的な障害のトラブルシューティングに役立つ CDF トレースのサブセットを収集します。このテクノロジーは、常時オンのトレース (AOT) として知られています。AOT ログは、C:\ProgramData\Citrix\TelemetryService\CitrixAOT にディスクに保存されます。

> **注:**
>
> `ProgramData` フォルダーは非表示になっています。表示するには、**表示** > **表示** > **隠し項目** をクリックします。

> Call Home は、その他の Event Tracing for Windows (ETW) 情報を収集せず、またそのように構成することもできません。

Call Home は、次のようなその他の情報も収集します。

- `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix` の下に Citrix Virtual Apps and Desktops によって作成されたレジストリ。
- Citrix 名前空間下の Windows Management Instrumentation (WMI) 情報。
- 実行中のプロセスの一覧。
- %PROGRAM DATA%\\Citrix\\CDF に保存されている Citrix プロセスのクラッシュダンプ。
- インストールおよびアップグレード情報。これには、製品全体のメタインストーラーログ、失敗したMSIログ、MSIログアナライザーからの出力、StoreFront™ログ、ライセンス互換性チェックログ、および予備サイトアップグレードテストの結果が含まれます。

トレース情報は収集時に圧縮されます。Citrix Telemetry Serviceは、最大10 MBの圧縮された最新のトレース情報を、最大8日間の期間保持します。

- データを圧縮することで、Call HomeはVDA上で小さなフットプリントを維持できます。

- プロビジョニングされたマシンでのIOPを回避するために、トレースはメモリに保持されます。
- トレースバッファは、トレースをメモリに保持するために循環メカニズムを使用します。

Call Home は、Call Home の主要データポイント に記載されている主要なデータポイントを収集します。

構成と管理の概要

Call Homeには、製品全体のインストールウィザードを使用しているとき、または後でPowerShellコマンドレットを使用して登録できます。登録すると、診断情報はデフォルトで毎週日曜日の現地時間午前3時頃にCitrixに収集およびアップロードされます。アップロードは、指定された時刻から2時間の範囲でランダム化されます。これは、デフォルトのスケジュールを使用するアップロードが午前3時から午前5時の間に行われることを意味します。

スケジュールに基づいて診断情報をアップロードしたくない場合（またはスケジュールを変更したい場合）は、PowerShellコマンドレットを使用して診断情報を手動で収集してアップロードするか、ローカルに保存できます。

スケジュールされた Call Home アップロードに登録する場合、および診断情報を手動で Citrix にアップロードする場合、Citrix アカウントまたは Citrix Cloud™ の資格情報を提供します。Citrix は、資格情報をアップロードトークンと交換します。このトークンは、顧客を識別し、データをアップロードするために使用されます。資格情報は保存されません。

アップロードが行われると、Citrixアカウントに関連付けられたアドレスに通知がメールで送信されます。

コンポーネントのインストール時に Call Home を有効にした場合、後で無効にできます。

前提条件

- マシンは PowerShell 3.0 以降を実行している必要があります。
- Citrix Telemetry Service がマシン上で実行されている必要があります。
- システム変数 `PSModulePath` は、Telemetryのインストールパス（例: `C:\Program Files\Citrix\Telemetry Service\`）に設定されている必要があります。

コンポーネントのインストール中に Call Home を有効にする

VDAのインストールまたはアップグレード中: フルプロダクトインストーラーのグラフィカルインターフェイスを使用してVirtual Delivery Agentをインストールまたはアップグレードする際、Call Homeへの参加を求められます。2つのオプションがあります。

- Call Home に参加する。
- Call Home に参加しない。

VDAをアップグレードしていて、以前にCall Homeに登録していた場合、そのウィザードページは表示されません。

Controllerのインストールまたはアップグレード中: グラフィカルインターフェイスを使用してDelivery Controllerをインストールまたはアップグレードする際、Call Homeへの参加を求められます。3つのオプションがあります。

Controllerをインストールする際、そのサーバーに「サービスとしてログオン」ポリシー設定が適用されたActive Directory GPOがある場合、インストールウィザードのCall Homeページで情報を構成することはできません。詳細については、CTX218094を参照してください。

Controllerをアップグレードしていて、以前にCall Homeに登録していた場合、参加について尋ねられることはありません。

PowerShellコマンドレット

PowerShellヘルプには、これらの一般的なユースケースでは使用されないコマンドレットとパラメーターの説明を含む、包括的な構文が記載されています。

アップロードにプロキシサーバーを使用するには、プロキシサーバーの構成を参照してください。

- **スケジュールされたアップロードを有効にする:** 診断コレクションはCitrixに自動的にアップロードされます。カスタムスケジュール用の追加のコマンドレットを入力しない場合、デフォルトのスケジュールが使用されます。

  ```
  $cred = Get-Credential

  Enable-CitrixCallHome -Credential $cred
  ```

  スケジュールされたアップロードが有効になっていることを確認するには、`Get-CitrixCallHome`と入力します。有効になっている場合、戻り値は`IsEnabled=True`および`IsMasterImage=False`です。

- **マスターイメージから作成されたマシンに対するスケジュールされたアップロードを有効にする:** マスターイメージでスケジュールされたアップロードを有効にすると、マシンカタログで作成される各マシンを構成する必要がなくなります。

  `Enable-CitrixCallHome -Credential $cred -MasterImage`

スケジュールされたアップロードが有効になっていることを確認するには、**Get-CitrixCallHome**と入力します。有効になっている場合、戻り値は`IsEnabled=True`と`IsMasterImage=True`です。

- **カスタムスケジュールを作成する:** 診断情報の収集とアップロードのために、日次または週次のスケジュールを作成します。

```
$timespan = New-TimeSpan –Hours hours -Minutes minutes

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek day
-UploadFrequency {Daily|Weekly}
```

例:

次のコマンドレットは、毎晩22時20分にデータをバンドルしてアップロードするスケジュールを作成します。Hoursパラメーターは24時間形式を使用します。`UploadFrequency`パラメーターの値がDailyの場合、`DayOfWeek`パラメーターは指定されていても無視されます。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

スケジュールを確認するには、`Get-CitrixCallHomeSchedule`と入力します。前の例では、`StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily`が返されます。

次のコマンドレットは、毎週水曜日の夜22時20分にデータをバンドルしてアップロードするスケジュールを作成します。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed
-UploadFrequency Weekly
```

スケジュールを確認するには、`Get-CitrixCallHomeSchedule`と入力します。前の例では、`StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly`が返されます。

Call Homeを無効にする

PowerShellコマンドレットを使用するか、Citrix Scoutを介してCall Homeを無効にできます。

Call Homeのスケジュールされたアップロードが無効になっている場合でも、AOTログは収集されディスクに保存されます。(スケジュールされたアップロードが無効になっている場合、AOTログはCitrixに自動的にアップロードされません。)AOTログの収集とローカルストレージを無効にできます。

PowerShellでCall Homeを無効にする

次のコマンドレットを実行すると、診断データはCitrixに自動的にアップロードされなくなります。(Citrix ScoutまたはテレメトリPowerShellコマンドレットを使用して、診断データをアップロードすることは引き続き可能です。)

```
Disable-CitrixCallHome
```

Call Homeが無効になっていることを確認するには、`Get-CitrixCallHome`と入力します。無効になっている場合、戻り値は`IsEnabled=False`と`IsMasterImage=False`です。

Citrix Scoutを使用して収集スケジュールを無効にする

Citrix Scout で診断データの収集スケジュールを無効にするには、収集のスケジュール設定 の手順に従います。手順 3 で **オフ** をクリックし、選択したマシンのスケジュールを取り消します。

AOTログの収集を無効にする

次の cmdlet を実行し、`Enabled` フィールドを `false` に設定すると、AOT ログは収集されなくなります。

```
Enable-CitrixTrace -Listen'{"trace":{"enabled":false,"persistDirectory":"C:\Users\Public","maxSizeBytes":1000000, "sliceDurationSeconds":300}}'
```

`Listen` パラメーターには、JSON 形式の引数が含まれます。

Call Home のアップロード用プロキシサーバーを構成する

Call Home が有効になっているマシンで、次の作業を実行します。以下の手順の図では、例としてサーバーアドレスとポート 10.158.139.37:3128 を使用しています。実際の環境の情報は異なります。

1. ブラウザーにプロキシサーバーの情報を追加します。Internet Explorer で **インターネットオプション \> 接続 \> LAN の設定** を選択します。**LAN にプロキシサーバーを使用する** を選択し、プロキシサーバーのアドレスとポート番号を入力します。
2. PowerShell で `netsh winhttp import proxy source=ie` を実行します。

```
PS C:\Users\administrator.JLGXH> netsh winhttp import proxy source=ie

Current WinHTTP proxy settings:

    Proxy Server(s) :  10.108.124.245:8080
    Bypass List     :  (none)
```

3. テキストエディターを使用して、C:\\Program Files\\Citrix\\Telemetry Service にある TelemetryService.exe の構成ファイルを編集します。赤い枠で示されている情報を追加します。

```
TelemetryService.exe - Notepad
File  Edit  Format  View  Help
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <startup>
                <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1" />
    </startup>
    <runtime>
      <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
        <dependentAssembly>
          <assemblyIdentity name="Newtonsoft.Json" culture="neutral" publicKeyToken="30ad4fe6b2a6aeed" />
          <bindingRedirect oldVersion="0.0.0.0-9.0.0.0" newVersion="9.0.0.0" />
        </dependentAssembly>
        <probing privatePath="TelemetryModule" />
      </assemblyBinding>
    </runtime>
<system.net>
<defaultProxy>
<proxy bypassonlocal="false" usesystemdefault="true" proxyaddress="http://10.108.124.245:8080" />
</defaultProxy>
</system.net>

</configuration>
```

4. Telemetry Service を再起動します。

PowerShell で Call Home の cmdlet を実行します。

診断情報を手動で収集してアップロードする

CIS Webサイトを使用して、診断情報バンドルをCISにアップロードできます。PowerShell コマンドレットを使用して、診断情報を収集し、CISにアップロードすることもできます。

CIS Webサイトを使用してバンドルをアップロードするには：

1. Citrixアカウントの資格情報を使用してCitrix Insight Servicesにログオンします。
2. **My Workspace**を選択します。
3. **Healthcheck**を選択し、データの場所に移動します。

CISは、データアップロードを管理するいくつかのPowerShellコマンドレットをサポートしています。このドキュメントでは、2つの一般的なケースのコマンドレットについて説明します。

- `Start-CitrixCallHomeUpload`コマンドレットを使用して、診断情報バンドルを手動で収集し、CISにアップロードします。（バンドルはローカルに保存されません。）

- `Start-CitrixCallHomeUpload`コマンドレットを使用してデータを手動で収集し、診断情報バンドルをローカルに保存します。これにより、データをプレビューできます。その後、`Send-CitrixCallHomeBundle`コマンドレットを使用して、そのバンドルのコピーを手動でCISにアップロードします。（最初に保存したデータはローカルに残ります。）

PowerShellヘルプには、これらの一般的なユースケースでは使用されないコマンドレットとパラメーターの説明を含む、包括的な構文が記載されています。

CISにデータをアップロードするコマンドレットを入力すると、アップロードの確認を求められます。アップロードが完了する前にコマンドレットがタイムアウトした場合は、システムイベントログでアップロードのステータスを確認してください。サービスがすでにアップロードを実行している場合、アップロード要求は拒否される可能性があります。

データの収集とバンドルのCISへのアップロード:

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath string]
[-Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploadHeader string] [-AppendHeaders string] [-Collect string]
[<CommonParameters>]
```

データの収集とローカルへの保存:

```
Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
strings] [<CommonParameters>]
```

次のパラメーターが有効です。

- **Credential:** アップロードをCISに指示します。
- **InputPath:** バンドルに含めるzipファイルの場所。これは、Citrixサポートが要求する追加ファイルである可能性があります。.zip拡張子を含めるようにしてください。
- **OutputPath:** 診断情報が保存される場所。このパラメーターは、Call Homeデータをローカルに保存する場合に必要です。
- **Description and Incident Time:** アップロードに関する自由形式の情報。
- **SRNumber:** Citrixテクニカルサポートのインシデント番号。
- **Name:** バンドルを識別する名前。

- **UploadHeader:** CISにアップロードされるアップロードヘッダーを指定するJSON形式の文字列。
- **AppendHeaders:** CISにアップロードされる追加ヘッダーを指定するJSON形式の文字列。
- **Collect:** 収集または省略するデータを指定するJSON形式の文字列で、{'collector': {'enabled':Boolean}} の形式で、Booleanはtrueまたはfalseです。 有効なコレクター値は次のとおりです。

  - 'WMI'
  - 'プロセス'
  - 'レジストリ'
  - 'クラッシュレポート'
  - 'トレース'
  - 'ファイル'
  - 'MSI'
  - 'ローカルデータ'
  - 'サイトデータ'
  - 'SFB'

  デフォルトでは、「sfb」を除くすべてのコレクターが有効になっています。

  'sfb'コレクターは、Skype for Businessの問題を診断するためにオンデマンドで使用するように設計されています。「'enabled'」パラメーターに加えて、「'sfb'」コレクターはターゲットユーザーを指定するための「'account'」および「'accounts'」パラメーターをサポートしています。次のいずれかの形式を使用してください。

  - "-収集 "`{'sfb':{'account':'domain\\user1'}}`"
  - "-収集 "{'sfb':{'accounts':}}"
- **共通パラメーター:** PowerShellヘルプを参照してください。

以前にローカルに保存されたデータをアップロードする:

```
Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string
[<CommonParameters>]
```

`Path` パラメーターは、以前に保存されたバンドルの場所を指定します。

例:

次のコマンドレットは、Call Homeデータ（WMIコレクターからのデータを除く）をCISにアップロードするよう要求します。このデータは、Citrix Provisioning VDAの登録失敗に関連しており、Citrixサポートケース123456について午後2時30分に記録されました。Call Homeデータに加えて、ファイル「"c:\\Diagnostics\\ExtraData.zip"」がアップロードされたバンドルに組み込まれます。

```
C:\PS\>Start-CitrixCallHomeUpload -InputPath "c:
\Diagnostics\ExtraData.zip" -Description "Registration failures with
Citrix Provisioning VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name
"RegistrationFailure-021812016" -Collect "{'wmi':{'enabled':false}}"
-UploadHeader "{'key1':'value1'}" -AppendHeaders "{'key2':'value2'}"
```

次のコマンドレットは、午前8時15分に記録されたCitrixサポートケース223344に関連するCall Homeデータを保存します。データはネットワーク共有上のファイルmydata.zipに保存されます。Call Homeデータに加えて、ファイル「"c:\\Diagnostics\\ExtraData.zip"」が保存されたバンドルに組み込まれます。

```
C:\PS\>Start-CitrixCallHomeUpload -OutputPath \
\mynetwork\myshare\mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip"
-Description "Diagnostics for incident number 223344" -IncidentTime "8:15"
-SRNumber 223344
```

以下のコマンドレットは、以前に保存したデータバンドルをアップロードします。

```
$cred=Get-Credential

C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \
\mynetwork\myshare\mydata.zip
```

シトリックス スカウト

はじめに

Citrix Scoutは診断情報を収集し、ヘルスチェックを実行します。その結果を使用して、Citrix Virtual Apps and Desktops™展開を保守できます。Citrixは、Citrix Insight Servicesを通じて、診断情報収集の包括的で自動化された分析を提供します。また、Scoutを使用して、単独で、またはCitrixサポートのガイダンスを受けて、問題をトラブルシューティングすることもできます。

収集ファイルをCitrixにアップロードして、Citrixサポートからの分析とガイダンスを受けることができます。または、収集したファイルをローカルに保存して自分で確認し、後でその収集ファイルをCitrixにアップロードして分析することもできます。

Scoutは次の手順を提供します:

- **収集:** サイトで選択したマシンに対して、1回限りの診断情報収集を実行します。その後、ファイルをCitrixにアップロードするか、ローカルに保存できます。
- **トレースと再現:** 選択したマシンで手動トレースを開始します。その後、それらのマシンで問題を再現します。問題を再現した後、トレースは停止されます。その後、Scoutは他の診断情報を収集し、ファイルをCitrixにアップロードするか、ローカルに保存します。
- **スケジュール:** 選択したマシンで、指定した時間に毎日または毎週診断情報収集が実行されるようにスケジュールします。ファイルは自動的にCitrixにアップロードされます。
- **ヘルスチェック:** サイトとそのコンポーネントの正常性と可用性を測定するチェックを実行します。Delivery Controller、Virtual Delivery Agent（VDA）、StoreFront™サーバー、およびCitrix License Serverのヘルスチェックを実行できます。チェック中に問題が見つかった場合、Scoutは詳細なレポートを提供します。Scoutが起動するたびに、更新されたヘルスチェックスクリプトを確認します。新しいバージョンが利用可能な場合、Scoutはそれらを自動的にダウンロードし、次回のヘルスチェック実行時に使用します。

> **注:**
>
> **トレースと再現**、**スケジュール**、および**ヘルスチェック**の手順は現在、Linux VDAでは利用できません。

> この記事で説明されているグラフィカルインターフェイスは、Scoutを使用する主な方法です。あるいは、PowerShellを使用して、1回限りの診断情報収集またはスケジュールされた診断情報収集とアップロードを構成することもできます。「Call Home」を参照してください。

Scoutの実行場所:

- オンプレミス展開では、Delivery Controller™からScoutを実行して、1つ以上のVirtual Delivery Agent（VDA）、Delivery Controller、StoreFrontサーバー、およびLicense Serverで診断情報を取得したり、チェックを実行したりできます。また、VDAからScoutを実行して、ローカル診断情報を収集することもできます。

- Citrix DaaS（旧称Citrix Virtual Apps and Desktopsサービス）を使用するCitrix Cloud環境では、VDAからScoutを実行して、ローカル診断情報を収集します。

Scout アプリケーションのログは `C:\ProgramData\Citrix\TelemetryService\ScoutUI.log` に保存されます。このファイルはトラブルシューティングに使用できます。

収集される情報

Scoutによって収集される診断情報には、Citrix Diagnostic Facility（CDF）トレースログファイルが含まれます。Always-on Tracing（AOT）と呼ばれるCDFトレースのサブセットも含まれます。AOT情報は、VDA登録やアプリケーション/デスクトップの起動などの一般的な問題のトラブルシューティングに役立ちます。その他のEvent Tracing for Windows（ETW）情報は収集されません。

収集される情報には以下が含まれます。

- Citrix Virtual Apps and Desktopsによって `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix` の下に作成されたレジストリエントリ。
- **Citrix名前空間**の下のWindows Management Instrumentation（WMI）情報。
- 実行中のプロセス。
- `%PROGRAMDATA%\Citrix\CDF` に保存されているCitrixプロセスのクラッシュダンプ。
- Citrixポリシー情報（CSV形式）。
- インストールおよびアップグレード情報。収集される情報には、製品の完全なメタインストーラーログ、失敗したMSIログ、MSIログアナライザーからの出力、StoreFrontログ、ライセンス互換性チェックログ、および予備的なサイトアップグレードテストの結果が含まれる場合があります。

トレース情報について:

- トレース情報は収集時に圧縮され、マシン上のフットプリントを小さく保ちます。
- 各マシンでは、Citrix Telemetry Serviceが圧縮された最新のトレース情報を最大8日間保持します。
- Citrix Virtual Apps and Desktops 7 1808以降、AOTトレースはデフォルトでローカルディスクに保存されます。(以前のバージョンでは、トレースはメモリに保持されていました。) デフォルトパス = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`。
- Citrix Virtual Apps and Desktops 7 1811以降、ネットワーク共有に保存されたAOTトレースは、他の診断情報とともに収集されます。

- 最大サイズ (デフォルト = 10 MB) とスライス期間は、`Enable-CitrixTrace` コマンドレットまたは `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen` レジストリ文字列を使用して変更できます。
- トレースは、ファイルが `MaxSize` の 10% に達するまでファイルに追加されます。

Scout が収集するデータポイントのリストについては、「Call Home の主要なデータポイント」を参照してください。

Scout の構成

Scout は Linux VDA で動作するように構成できます。Linux VDA とテレメトリの詳細については、「Citrix Telemetry Service との統合」を参照してください。

Linux VDA は、`ctxtelemetry` ソケットポートまたはテレメトリサービス用のポートを自動的に変更する場合があります。その場合は、ポートを手動で構成する必要があります。

1. C:\Program Files\Citrix\Telemetry Service に移動します。
2. ScoutUI.exe.config ファイルを開きます。
3. LinuxVDATelemetryServicePort または LinuxVDATelemetryWakeupPort の値を、Linux VDA で構成された値に変更します。

- `<add key="LinuxVDATelemetryServicePort" value="7502"/>`
- `<add key="LinuxVDATelemetryWakeupPort" value="7503"/>`

1. 変更を保存してファイルを閉じます。
2. 最新の構成が読み込まれていることを確認するために、Scout を再度開きます。

ヘルスチェックについて

ヘルスチェックデータは、`C:\ProgramData\Citrix\TelemetryService\`の下のフォルダーに保存されます。

サイトのヘルスチェック

サイトヘルスチェックは、FlexCast Management Architecture (FMA) サービスの包括的な評価を提供する環境テストサービスに含まれています。これらのチェックは、サービスの可用性を確認するだけでなく、データベース接続などの他のヘルスインジケーターも探します。

サイトヘルスチェックは、Delivery Controllerで実行されます。サイトの規模によっては、これらのチェックの完了には最大1時間かかる場合があります。

DELIVERY CONTROLLER の構成チェック

サイトの健全性チェックの一環として、Delivery Controller の構成チェックでは、Virtual Apps and Desktops サイトに関する Citrix の推奨事項に基づいて、以下の問題が存在するかどうかを確認します。

- 1 つ以上の Delivery Controller が失敗状態にある。
- サイトに Delivery Controller が 1 つしかない。
- Delivery Controller のバージョンが異なる。

健全性チェックの 権限と要件 を満たすことに加えて、Delivery Controller の構成チェックには以下が必要です。

- 少なくとも 1 つの Controller の電源がオンになっていること。
- Controller 上で Broker Service が実行されていること。
- Controller からサイトデータベースへの接続が機能していること。

VDA の健全性チェック

VDA の健全性チェックは、一般的な VDA 登録、セッション起動、およびタイムゾーンリダイレクトの問題の考えられる原因を特定します。

VDA での登録について、Scout は以下をチェックします。

- VDA ソフトウェアのインストール
- VDA マシンのドメインメンバーシップ
- VDA 通信ポートの可用性
- VDA サービスステータス
- Windows ファイアウォール構成
- Controller との通信
- Controller との時刻同期
- VDA 登録ステータス

VDA でのセッション起動について、Scout は以下を確認します。

- セッション起動通信ポートの可用性
- セッション起動サービスのステータス
- セッション起動 Windows ファイアウォール構成
- VDA リモートデスクトップサービス クライアントアクセスライセンス

- VDA アプリケーション起動パス
- セッション起動レジストリ設定

VDAでのタイムゾーンリダイレクトについて、Scoutは以下をチェックします。

- Windows ホットフィックスのインストール
- Citrix ホットフィックスのインストール
- Microsoft グループポリシー設定
- Citrix グループポリシー設定

VDAでのプロファイル管理について、Scoutは以下をチェックします。

- ハイパーバイザーの検出
- プロビジョニングの検出
- シトリックス バーチャル アプリおよびデスクトップ
- Personal vDiskの構成
- ユーザーストア
- プロファイル管理サービスのステータス検出
- Winlogon.exeフッキングテスト

Profile Management のチェックを実行するには、VDA に Profile Management をインストールして有効にする必要があります。Profile Management の構成チェックの詳細については、Knowledge Center の記事 CTX132805 を参照してください。

StoreFront のヘルスチェック

StoreFront のチェックでは、以下を確認します。

- Citrix Default Domainサービスが実行されていること
- Citrix Credential Walletサービスが実行されていること
- StoreFrontサーバーからActive Directoryポート88への接続
- StoreFrontサーバーからActive Directoryポート389への接続
- ベースURLが有効なFQDNであること
- ベースURLから正しいIPアドレスを取得できること
- IISアプリケーションプールが.NET 4.0を使用していること
- 証明書がホストURLのSSLポートにバインドされているかどうか
- 証明書チェーンが完全であるかどうか

- 証明書の有効期限が切れているかどうか
- 証明書の有効期限が間もなく切れるかどうか（30日以内）

ライセンスサーバーのチェック

ライセンスサーバーのチェックでは、以下を確認します。

- Delivery Controllerからのライセンスサーバー接続
- License Server ファイアウォールのリモートアクセスステータス
- Citrix Licensing サービスのステータス
- License Server のライセンスキャッシュモードの状態
- License Server ポートの接続
- Citrix ベンダーデーモン (CITRIX) が実行中であるかどうか
- システムクロックが同期されているかどうか
- Citrix Licensing サービスがローカルサービスアカウントで実行されているかどうか
- `CITRIX.opt` ファイルの存在
- Customer Success Services の資格取得日
- シトリックス ライセンス サーバー アップデート
- License Server 証明書が Delivery Controller の信頼されたルートストアにあるかどうか

ヘルスチェックの権限と要件を満たすことに加えて、ライセンスサーバーはドメインに参加している必要があります。そうでない場合、ライセンスサーバーは検出されません。

ヘルスチェックの実行

ヘルスチェックの手順は、マシンの選択、チェックの開始、結果レポートの確認で構成されます。

1. Scout を起動します。マシンの メニューから、 **>** を選択します。開いたページで、 をクリックします。
2. マシンを選択します。「**Find machine**」をクリックしてマシンを検出します。「**Select machines**」ページには、サイトで検出されたすべてのVDA、Delivery Controller、およびライセンスサーバーが一覧表示されます。マシン名で表示をフィルターできます。診断を収集する各マシンの横にあるチェックボックスをオンにして、「**Continue**」をクリックします。

   その他のコンポーネントタイプ（StoreFrontサーバーやVDAマシンなど）を追加するには、「Add machines manually」および「Import VDA machines」を参照してください。Citrix Provisioning™サーバーまたはライセンスサーバーを手動で追加することはできません。

Scoutは、選択された各マシンで検証テストを自動的に起動し、「Verification tests」に記載されている基準を満たしていることを確認します。検証に失敗すると、「**Status**」列にメッセージが表示され、そのマシンのチェックボックスがオフになります。次のいずれかを実行できます。

- 問題を解決してから、マシンのチェックボックスを再度オンにします。これにより、検証テストが再試行されます。
- そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンではヘルスチェックは実行されません。

検証テストが完了したら、「**Continue**」をクリックします。

3. 選択したマシンでヘルスチェックを実行します。概要には、テストが実行されるマシン（検証テストに合格した選択済みのマシン）が一覧表示されます。「**Start Checking**」をクリックします。

   チェック中およびチェック後：

   - 「**Status**」列は、マシンの現在のチェック状態を示します。
   - 進行中のすべてのチェックを停止するには、ページ右下隅にある「**Stop Checking**」をクリックします。（単一のマシンのヘルスチェックをキャンセルすることはできず、選択されているすべてのマシンのみをキャンセルできます。チェックが完了したマシンからの情報は保持されます。
   - 選択されたすべてのマシンのチェックが完了すると、右下隅の「**Stop Checking**」ボタンが「**Done**」に変わります。
   - チェックに失敗した場合は、「**Action**」列の「**Retry**」をクリックできます。
   - チェックが問題なく完了した場合、「**Action**」列は空になります。
   - チェックで問題が見つかった場合は、「**View Details**」をクリックして結果を表示します。
   - 選択されたすべてのマシンのチェックが完了した後、「**Back**」をクリックしないでください。（クリックすると、チェック結果が失われます）。

4. チェックが完了したら、**完了**をクリックしてScoutの開始ページに戻ります。

ヘルスチェックの結果

レポートを生成するCitrixチェックの場合、レポートには以下が含まれます。

- 結果レポートが生成された日時
- チェックされたマシン

- ターゲットマシンでチェックが探した条件

権限と要件

権限:

- 診断情報を収集するには:
  - 診断情報を収集する各マシンで、ローカル管理者およびドメインユーザーである必要があります。
  - 各マシンで LocalAppData ディレクトリへの書き込み権限が必要です。
- ヘルスチェックを実行するには:
  - ドメインユーザーグループのメンバーである必要があります。
  - フル管理者であるか、サイトに対する読み取り専用および **Run Environment Tests** 権限を持つカスタムロールを持っている必要があります。
  - スクリプトの実行を許可するには、スクリプト実行ポリシーを少なくとも `RemoteSigned` に設定します。例: `Set-ExecutionPolicy RemoteSigned`。**注:** 他のスクリプト実行権限でも機能する場合があります。
- Scout の起動時には、**管理者として実行**を使用します。

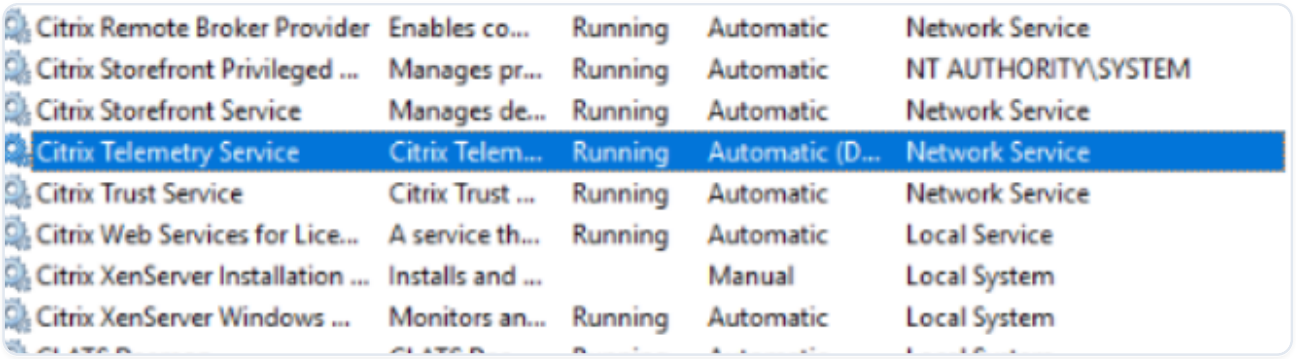
診断情報を収集したり、ヘルスチェックを実行したりする各マシンについては、次のとおりです。

- Scoutがそのマシンと通信できる必要があります。
- ファイルとプリンターの共有が有効になっている必要があります。
- PSRemotingとWinRMが有効になっている必要があります。また、そのマシンではPowerShell 3.0以降が実行されている必要があります。
- Citrix Telemetry Serviceがそのマシンで実行されている必要があります。
- Windows Management Infrastructure (WMI)へのアクセスがそのマシンで有効になっている必要があります。
- 診断情報収集のスケジュールを設定するには、そのマシンで互換性のあるScoutバージョンが実行されている必要があります。

パス名で指定するユーザー名にドル記号 ($) を使用しないでください。診断情報の収集が妨げられます。

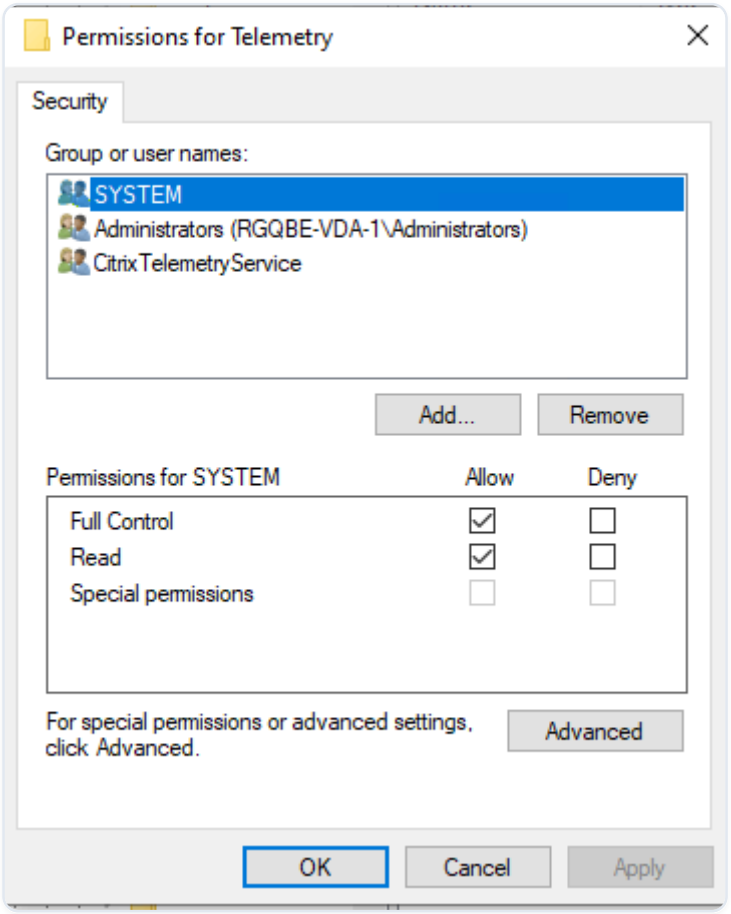
Scoutは、選択したマシンで検証テストを実行し、これらの要件が満たされていることを確認します。

Windows用Telemetry Serviceは、Network Serviceで実行されます。

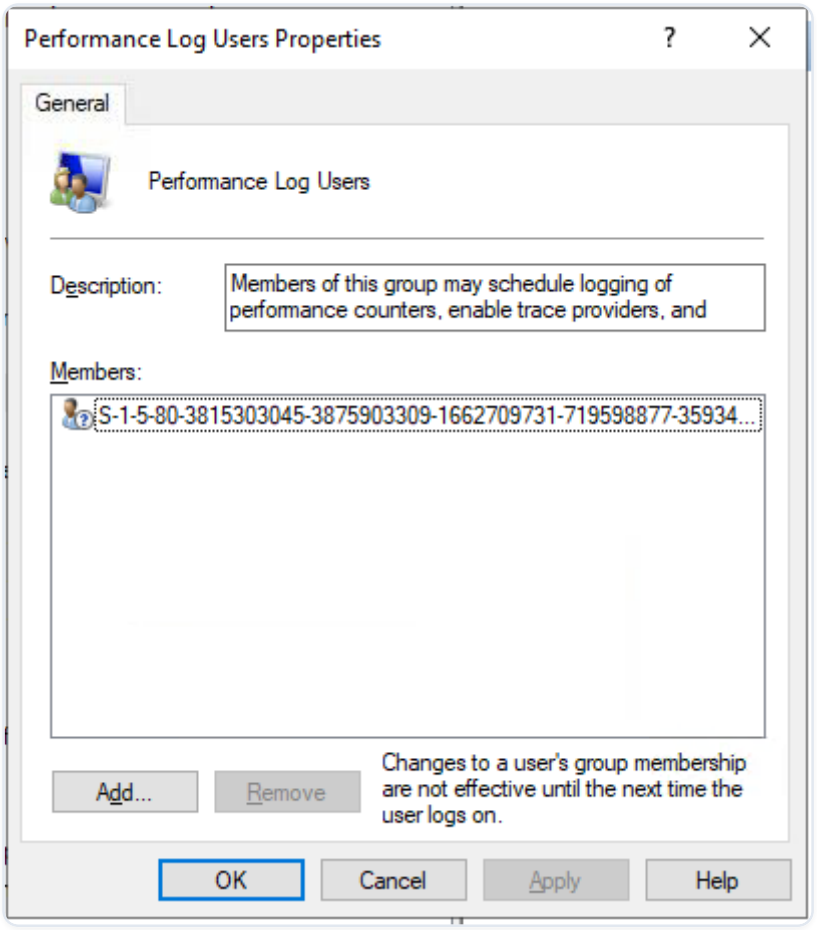


AOTトレースフォルダーは`C:\ProgramData\Citrix\TelemetryService\CitrixAOT`に保存されます。

Administratorグループ、System、およびTelemetry Service SIDのユーザーのみが、`HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry`レジストリにアクセスする権限を持っています。



テレメトリサービスをアンインストールした後も、テレメトリサービスSIDはパフォーマンスログユーザーグループに残りますが、手動で削除できます。



検証テスト

診断コレクションまたはヘルスチェックが開始される前に、選択された各マシンに対して検証テストが自動的に実行されます。これらのテストは、要件が満たされていることを確認します。マシンでテストが失敗した場合、Scoutは推奨される是正措置を含むメッセージを表示します。

- **Scoutがこのマシンに到達できません** - 以下を確認してください:
  - マシンの電源がオンになっていること。
  - ネットワーク接続が正常に機能していること。(これには、ファイアウォールが適切に構成されていることの確認も含まれます。)
  - ファイルとプリンターの共有がオンになっていること。手順については、Microsoftのドキュメントを参照してください。
- **PSRemotingとWinRMを有効にする** - PowerShellリモート処理とWinRMを同時に有効にできます。**管理者として実行**を使用して、`Enable-PSRemoting` コマンドレットを実行します。詳細については、コマンドレットのMicrosoftヘルプを参照してください。
- **ScoutにはPowerShell 3.0（最小）が必要です** - マシンにPowerShell 3.0（またはそれ以降）をインストールし、PowerShellリモート処理を有効にします。

- **このマシン上のLocalAppDataディレクトリにアクセスできません** - アカウントがマシン上のLocalAppDataディレクトリへの書き込み権限を持っていることを確認してください。
- **Citrix Telemetry Serviceが見つかりません** - Citrix Telemetry Serviceがマシンにインストールされ、開始されていることを確認してください。
- **スケジュールを取得できません** - マシンを（最小で）XenAppおよびXenDesktop 7.14にアップグレードしてください。
- **WMIがマシンで実行されていません** - Windows Management Instrumentation (WMI) アクセスが有効になっていることを確認してください。
- **WMI接続がブロックされています** - Windows FirewallサービスでWMIを有効にしてください。
- **Citrix Telemetry Service の新しいバージョンが必要です** - (バージョンは、Collect および Trace & Reproduce のみで確認されます。) マシン上の Telemetry Service のバージョンをアップグレードしてください (インストールとアップグレードを参照)。サービスをアップグレードしない場合、そのマシンは **Collect** または **Trace & Reproduce** アクションに含まれません。
- **Scout がこのマシン上の systemd ソケットに接続できません** - 以下を確認してください。
  - ポート 7503 が開いていることを確認します。`systemd ctxtelemetry.socket` がマシン上のポート 7503 でリッスンしていることを確認します。`ctxtelemetry.socket` ポートが変更されている場合、ポートが異なる可能性があります。ポートを調整するには、Scout の構成を参照してください。
  - ネットワーク接続が正常に機能していることを確認します。(これには、ファイアウォールが適切に構成されていることの確認が含まれる場合があります。)
- **このマシンで Linux VDA Telemetry Service が開始されていません** - 以下を確認してください。
  - ポート 7502 が開いていることを確認します。Linux VDA Telemetry Service がマシンにインストールされ、開始されていることを確認します。テレメトリサービスポートが変更されている場合、ポートが異なる可能性があります。ポートを調整するには、Scout の構成を参照してください。
  - ネットワーク接続が正常に機能していることを確認します。(これには、ファイアウォールが適切に構成されていることの確認が含まれる場合があります。)

バージョン互換性

このバージョンの Scout (3.x) は、Citrix Virtual Apps and Desktops (または XenApp and XenDesktop 7.14 以降) のコントローラーおよび VDA で実行することを目的としています。

| 機能 | スカウト 2.23 | スカウト 3.0 | --- | --- | ---| -- | Citrix Virtual Apps and Desktops (および XenApp and XenDesktop 7.14 ～ 7.18) のサポート | はい | はい XenDesktop 5.x、7.1～7.13をサポート | はい | いいえ XenApp 6.x、7.5～7.13をサポート | はい | いいえ 製品に同梱 | 7.1～7.13 | 7.14以降 CTX記事からダウンロード可能 | はい | いいえ CDFトレースをキャプチャ | はい | はい Always-on-Traces (AOT) をキャプチャ | いいえ | はい 診断データの収集を許可 | 一度に最大10台のマシン（デフォルト） | 無制限（リソースの可用性による） 診断データをCitrixに送信することを許可 | はい | はい 診断データをローカルに保存することを許可 | はい | はい Citrix Cloud™ 資格情報をサポート | いいえ | はい Citrix資格情報のサポート | はい | はい アップロード用プロキシサーバーのサポート | はい | はい スケジュールの調整 | 該当なし | はい スクリプトのサポート | コマンドライン（ローカルControllerのみ） | Call Homeコマンドレットを使用したPowerShell（Telemetry Serviceがインストールされている任意のコンピューター） ヘルスチェック | いいえ | はい データマスキング | いいえ | 3.17以降

インストールとアップグレード

デフォルトでは、VDAまたはControllerをインストールまたはアップグレードすると、Citrix Telemetry Serviceの一部としてScoutが自動的にインストールまたはアップグレードされます。

VDAのインストール時にCitrix Telemetry Serviceを省略した場合、または後でサービスを削除した場合は、Citrix Virtual Apps and Desktopsインストールメディアの`x64\Virtual Desktop Components`または`x86\Virtual Desktop Components`フォルダーから`TelemetryServiceInstaller_xx.msi`を実行します。

Collectまたは**Trace & Reproduce**アクションを選択すると、マシンで古いバージョンのCitrix Telemetry Serviceが実行されている場合に通知されます。Citrixでは、サポートされている最新バージョンを使用することをお勧めします。そのマシンでTelemetry Serviceをアップグレードしない場合、そのマシンは**Collect**または**Trace & Reproduce**アクションに含まれません。Telemetry Serviceをアップグレードするには、インストールと同じ手順を使用します。

アップロードの承認

診断コレクションをCitrixにアップロードする予定がある場合は、CitrixアカウントまたはCitrix Cloudアカウントが必要です。（これらは、Citrixダウンロードにアクセスしたり、Citrix Cloud Control Centerにアクセスしたりするために使用する資格情報です。）アカウントの資格情報が検証されると、トークンが発行されます。

CitrixアカウントまたはCitrix Cloudアカウントで認証する場合、リンクをクリックして、デフォルトのブラウザーでHTTPSを使用してCitrix Cloudにアクセスします。Citrix Cloudの資格情報を入力すると、トークンが表示されます。トークンをコピーしてScoutに貼り付けます。その後、Scoutウィザードを続行できます。

トークンは、Scoutを実行しているマシンにローカルに保存されます。次回**Collect**または**Trace & Reproduce**を実行するときにそのトークンを使用できるようにするには、**Store token and skip this step in the future**チェックボックスをオンにします。

Scoutの開始ページで**Schedule**を選択するたびに、再承認する必要があります。スケジュールを作成または変更する際には、保存されたトークンを使用できません。

アップロードにプロキシを使用する

コレクションをCitrixにアップロードするためにプロキシサーバーを使用したい場合は、Scoutにブラウザーのインターネットプロパティで構成されたプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を指定することもできます。

マシンの検索

Collect、**Trace & Reproduce**、**Schedule** の各手順では、Scout は自動的に検出したコントローラーと VDA を一覧表示します。

Delivery Controller から Scout Health Check を実行するときは、**Find machine** をクリックして、デリバリーコントローラー、VDA、ライセンスサーバー、StoreFrontサーバーなどのマシンを検出します。

Delivery Controller ではないドメイン参加済みマシンから Scout Health Check を実行する場合、Scout はマシンを自動的に検出できません。マシンを手動で追加する か、VDA マシンをインポートする 必要があります。

マシンを手動で追加する

Scout が検出したコントローラーと VDA を一覧表示した後、StoreFrontサーバー、ライセンスサーバー、Citrix Provisioningサーバーなど、展開内の他のマシンを手動で追加できます。

ヘルスチェック の実行時：

- ドメイン内の Citrix ライセンスサーバーは自動的に検出されます。ライセンスサーバーを手動で追加することはできません。
- ヘルスチェックは現在、Citrix Provisioningサーバーをサポートしていません。

検出されたマシンを一覧表示するScoutページで、**+ Add machine** をクリックします。追加するマシンのFQDNを入力し、**Continue** をクリックします。必要に応じて、他のマシンを追加するために繰り返します。(FQDNの代わりにDNSエイリアスを入力しても有効に見えることがありますが、ヘルスチェックが失敗する可能性があります。)

手動で追加されたマシンは、検出されたマシンよりも上に、マシンリストの常に上部に表示されます。

手動で追加されたマシンを識別する簡単な方法は、行の右端にある赤い削除ボタンです。手動で追加されたマシンのみがそのボタンを持っています。検出されたマシンにはありません。

手動で追加されたマシンを削除するには、行の右端にある赤いボタンをクリックします。削除を確認します。他の手動で追加されたマシンを削除するために繰り返します。

Scout は、手動で追加されたマシンを削除するまで記憶しています。Scout を閉じてから再度開くと、手動で追加されたマシンは引き続きリストの上部に表示されます。

StoreFrontサーバーで **Trace & Reproduce** を使用する場合、CDFトレースは収集されません。ただし、他のすべてのトレース情報は収集されます。

VDA マシンをインポートする

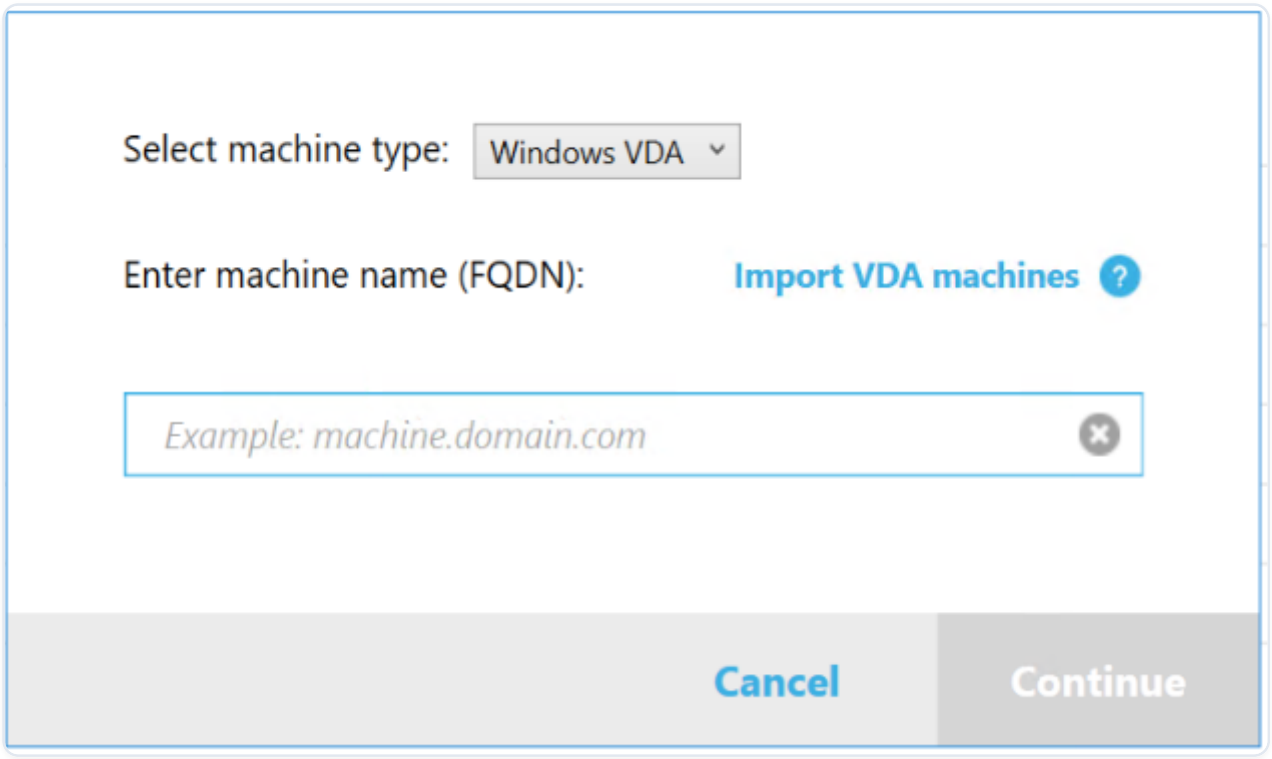
ヘルスチェック の実行時に、展開内の VDA マシンをインポートできます。

1. Delivery Controller または Connector で、PowerShell コマンドを使用してマシンリストファイルを生成します。Connector では、Citrix 資格情報を入力し、ポップアップダイアログで顧客を選択する必要があります。

   ```
   Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList.txt
   ```

2. machineList.txtファイルを、Scout Health Checkを起動するドメイン参加済みマシンにコピーします。
3. Scout Health Checkページで、 をクリックします。
4. マシンタイプを選択します。
5. をクリックします。
6. machineList.txtファイルを選択します。
7. をクリックします。

インポートされた VDA マシンが Scout Health Check ページに一覧表示されます。



診断情報の収集

手順には、マシンの選択、診断情報収集の開始、および収集を含むファイルをCitrixにアップロードするかローカルに保存することが含まれます。

1. Scoutを起動します。マシンの**** メニューから、 > を選択します。開いたページで、 をクリックします。
2. マシンを選択します。

   - Controllerでは、 ページにサイト内のすべてのVDAとControllerが一覧表示されます。表示はマシン名でフィルターできます。他のマシン（StoreFrontやCitrix Provisioningサーバーなど）を手動で追加するには、「Add machines manually」を参照してください。
   - その他のコンポーネント（VDAサーバーなど）では、 ページにはローカルマシンのみが表示されます。マシンの手動追加はサポートされていません。

   診断情報を収集する各マシンの横にあるチェックボックスをオンにして、 をクリックします。

   Scoutは、選択された各マシンで検証テストを自動的に起動し、「Verification tests」に記載されている基準を満たしていることを確認します。検証に失敗すると、 列にメッセージが表示され、そのマシンのチェックボックスはオフになります。次のいずれかを実行できます。

   - 問題を解決してから、マシンのチェックボックスを再度オンにします。これにより、検証テストが再実行されます。

- そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンからは診断情報は収集されません。

検証テストが完了したら、 をクリックします。

3. 診断情報を収集します。概要には、診断情報が収集されるすべてのマシン（選択され、検証テストに合格したマシン）が一覧表示されます。 をクリックします。

   収集中:

   - 列は、マシンの現在の収集状態を示します。
   - 単一マシンでの進行中の収集を停止するには、そのマシンの 列にある をクリックします。
   - 進行中のすべての収集を停止するには、ページの右下隅にある をクリックします。収集が完了したマシンからの診断情報は保持されます。収集を再開するには、各マシンの 列にある をクリックします。
   - 選択したすべてのマシンの収集が完了すると、右下隅にある ボタンが に変わります。
   - 診断情報を再度収集するには、そのマシンの 列にある をクリックします。新しい収集は以前の収集を上書きします。
   - 収集に失敗した場合は、 列にある をクリックできます。成功した収集のみがアップロードまたは保存されます。
   - 選択したすべてのマシンでコレクションが完了したら、**戻る**をクリックしないでください。(クリックすると、コレクションは失われます。)

   コレクションが完了したら、**続行**をクリックします。

4. コレクションを保存またはアップロードします。ファイルをCitrixにアップロードするか、ローカルマシンに保存するかを選択します。

   今すぐファイルをアップロードする場合は、手順5に進みます。

   ファイルをローカルに保存することを選択した場合：

   - Windowsの**保存**ダイアログボックスが表示されます。目的の場所に移動します。
   - ローカル保存が完了すると、ファイルのパス名が表示され、リンクされます。ファイルを表示できます。後でファイルをCitrixにアップロードできます。CTX136396を参照してください。

   完了をクリックしてScoutの開始ページに戻ります。この手順でこれ以上ステップを完了する必要はありません。

5. アップロードの認証を行い、必要に応じてプロキシを指定します。詳細については、アップロードの承認を参照してください。

   - Scoutを通じて認証していない場合は、この手順に進みます。
   - Scoutを通じて認証済みの場合、保存されている認証トークンがデフォルトで使用されます。これを行う場合は、このオプションを選択して**続行**をクリックします。このコレクションの資格情報は要求されません。手順6に進みます。
   - 以前に認証済みで、再認証して新しいトークンを取得したい場合は、**変更/再認証**をクリックしてこの手順に進みます。

   アップロードを認証するためにCitrix資格情報を使用するか、Citrix Cloud資格情報を使用するかを選択します。**続行**をクリックします。資格情報ページは、保存されたトークンを使用していない場合にのみ表示されます。

   資格情報ページで：

   - ファイルアップロードにプロキシサーバーを使用したい場合は、**プロキシの構成**をクリックします。Scoutにブラウザのインターネットプロパティで構成されているプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
   - Citrix Cloudアカウントの場合は、**トークンを生成**をクリックします。デフォルトのブラウザがCitrix Cloudページを起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
   - Citrixアカウントの場合は、資格情報を入力します。

   完了したら、**続行**をクリックします。

6. アップロードに関する情報を入力します。

   - 名前フィールドには、収集された診断ファイルのデフォルト名が含まれています。名前を変更することはできますが、ほとんどのコレクションではこれで十分です。(デフォルト名を削除して名前フィールドを空のままにした場合、デフォルト名が使用されます。)
   - オプションで、8桁のCitrixサポートケース番号を指定します。
   - オプションの**説明**フィールドに、問題について説明し、該当する場合は問題が発生した時期を示します。

   完了したら、**アップロードを開始**をクリックします。

アップロード中、ページの左下部分に、完了したアップロードのパーセンテージが概算で表示されます。進行中のアップロードをキャンセルするには、**アップロードを停止**をクリックします。

アップロードが完了すると、その場所のURLが表示され、リンクされます。リンクをたどってCitrixの場所にアクセスし、アップロードの分析を表示したり、リンクをコピーしたりできます。

完了をクリックしてScoutの開始ページに戻ります。

トレースと再現

トレースと再現の手順は、マシンの選択、トレースの開始、問題の再現、診断コレクションの完了、そしてファイルをCitrixにアップロードするか、ローカルに保存することから構成されます。

この手順は、標準の**収集**手順に似ています。ただし、マシンでトレースを開始し、それらのマシンで問題を再作成することができます。すべての診断コレクションにはAOTトレース情報が含まれています。この手順では、トラブルシューティングに役立つCDFトレースが追加されます。

1. Scoutを起動します。マシンの**スタート**メニューから、**Citrix > Citrix Scout**を選択します。開始ページで、**トレースと再現**をクリックします。
2. マシンを選択します。**Select machines**ページには、サイト内のすべてのVDAとControllerが一覧表示されます。マシン名で表示をフィルタリングできます。トレースと診断を収集する各マシンの横にあるチェックボックスをオンにします。その後、**Continue**をクリックします。

   その他のマシンを手動で追加するには (StoreFrontまたはCitrix Provisioningサーバーなど)、マシンを手動で追加するを参照してください。

   Scoutは、選択した各マシンで検証テストを自動的に起動し、Verification testsに記載されている基準を満たしていることを確認します。マシンの検証が失敗した場合、**Status**列にメッセージが表示され、そのマシンのチェックボックスはオフになります。次のいずれかを実行できます。

   - 問題を解決してから、そのマシンのチェックボックスを再度オンにします。これにより、検証テストが再試行されます。
   - そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンからは診断情報とトレースは収集されません。

   検証テストが完了したら、**Continue**をクリックします。
3. トレースを開始します。概要には、トレースが収集されるすべてのマシンが一覧表示されます。**Start Tracing**をクリックします。

選択した1台以上のマシンで、発生した問題を再現します。その間、トレースの収集は続行されます。問題の再現が完了したら、Scoutで**Continue**をクリックします。これによりトレースが停止します。

トレースを停止した後、トレース中に問題を再現したかどうかを示します。

4. マシンから診断情報を収集します。**Start Collecting**をクリックします。収集中に：

   - **Status**列には、マシンの現在の収集状態が表示されます。
   - 単一マシンで進行中の収集を停止するには、そのマシンの**Action**列にある**Cancel**をクリックします。
   - 進行中のすべての収集を停止するには、ページの右下隅にある**Stop Collection**をクリックします。収集が完了したマシンからの診断情報は保持されます。収集を再開するには、各マシンの**Action**列にある**Retry**をクリックします。
   - 選択したすべてのマシンで収集が完了すると、右下隅にある**Stop Collection**ボタンが**Continue**に変わります。
   - マシンから診断情報を再度収集するには、そのマシンの**Action**列にある**Collect Again**をクリックします。新しい収集は以前の収集を上書きします。
   - コレクションが失敗した場合は、**アクション**列の**再試行**をクリックできます。正常に完了したコレクションのみがアップロードまたは保存されます。
   - 選択したすべてのマシンでコレクションが完了したら、**戻る**をクリックしないでください。(クリックすると、コレクションは失われます。)

   収集が完了したら、**続行**をクリックします。

5. コレクションを保存またはアップロードします。ファイルをCitrixにアップロードするか、ローカルに保存するかを選択します。

   今すぐファイルをアップロードする場合は、手順6に進みます。

   ファイルをローカルに保存する場合は、次の手順を実行します。

   - Windowsの保存ダイアログボックスが表示されます。目的の場所を選択します。
   - ローカル保存が完了すると、ファイルのパス名が表示され、リンクされます。ファイルを表示できます。注意: ファイルは後でCitrixからアップロードできます。Citrix Insight Servicesについては、CTX136396を参照してください。

   完了をクリックしてScoutの開始ページに戻ります。この手順でこれ以上完了する必要のある手順はありません。

6. アップロードの認証を行い、必要に応じてプロキシを指定します。このプロセスの詳細については、アップロードの承認を確認してください。

   - Scoutを介して認証していない場合は、この手順に進みます。
   - Scoutを介して認証した場合、保存されている認証トークンがデフォルトで使用されます。これを行う場合は、このオプションを選択して**続行**をクリックします。このコレクションの資格情報は求められません。手順7に進みます。
   - 以前に認証済みで、再認証して新しいトークンを取得したい場合は、**変更/再認証**をクリックしてこの手順に進みます。

   アップロードを認証するためにCitrix資格情報を使用するか、Citrix Cloud資格情報を使用するかを選択します。**続行**をクリックします。資格情報ページは、保存されたトークンを使用していない場合にのみ表示されます。

   資格情報ページで:

   - ファイルアップロードにプロキシサーバーを使用したい場合は、「**Configure proxy**」をクリックします。Scoutにブラウザのインターネットプロパティで設定されているプロキシ設定を使用するよう指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
   - Citrix Cloudアカウントの場合、「**Generate token**」をクリックします。デフォルトのブラウザがCitrix Cloudページを起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
   - Citrixアカウントの場合、資格情報を入力します。

   完了したら、「**Continue**」をクリックします。

7. アップロードに関する情報を提供します。

   アップロードの詳細を入力します。

   - 名前フィールドには、収集された診断ファイルのデフォルト名が含まれています。ほとんどの収集ではこれで十分ですが、名前を変更することもできます。(デフォルト名を削除して名前フィールドを空にした場合でも、デフォルト名が使用されます。)
   - 必要に応じて、8桁のCitrixサポートケース番号を指定します。
   - オプションの「説明」フィールドに、問題を説明し、該当する場合は問題が発生した時期を示します。

   完了したら、「**Start Upload**」をクリックします。

アップロード中、ページの左下部分に、アップロードの完了率がおおよそ表示されます。進行中のアップロードをキャンセルするには、「**Stop Upload**」をクリックします。

アップロードが完了すると、その場所のURLが表示され、リンクされます。リンクをたどってCitrixの場所に移動し、アップロードの分析を表示したり、リンクをコピーしたりできます。

「**Done**」をクリックしてScoutの開始ページに戻ります。

ScoutはTraceLoggingプロバイダーをサポートします

以前、ScoutはWindowsパフォーマンスプロバイダーのみをサポートしていました。これは追加のデコードファイルを必要とし、同じプロバイダーの単一セッションからのセッションとイベントのみをトレースしていました。

Citrix Virtual Apps and Desktops バージョン 2411 以降、Scout は TraceLogging プロバイダーをサポートします。このプロバイダーは、追加のデコードファイルを必要とせず、同じプロバイダーに対して最大 8 つのトレースセッションからイベントを有効にして受信できます。この機能はデフォルトで有効になっています。

追加のログ収集を有効にする

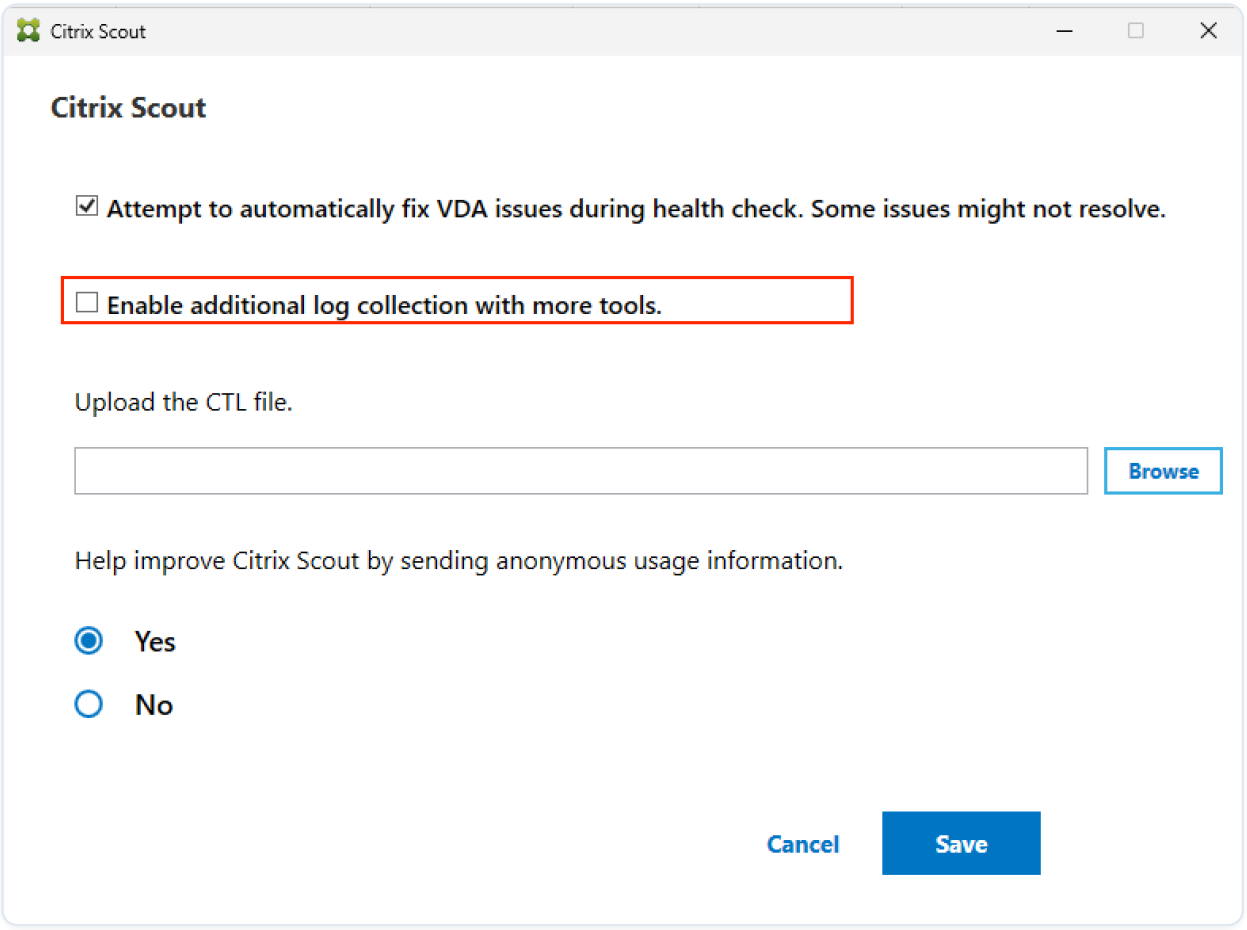
追加のログ収集を有効にする機能を使用すると、perfmon、Netsh、DebugView、Wireshark などのより多くのツールでトレースおよび再現機能を使用できます。

2407 リリース以降、追加のログ収集を有効にすると、Scout はマシンにインストールされている CDC 関連ツールを自動的に検出し、CDC ツール関連のトレースログを zip パッケージに自動収集します。これらの zip ファイルをカスタマイズして Scout に添付できます。この自動化により、Citrix Scout をより効果的に使用でき、問題の迅速な診断に役立ちます。

> **注:**
>
> これはローカルマシンにのみ適用されます。

追加のログ収集を設定するには：

1. Citrix Scout を起動します。
2. **設定**ギアをクリックします。
3. **追加のログ収集をより多くのツールで有効にする**をクリックします。
4. **保存**をクリックします。



追加のログ収集を有効にするには、次の必要なツールがインストールされており、指定された場所にディレクトリが手動で作成されていることを確認してください。

ツールのインストール場所：

- Procdump ログ: Procdump をダウンロードし、%ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\Procdump\procdump.exe に配置します。
- StoreFrontログ: DbgViewをダウンロードし、%ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\DebugView\Dbgview.exeに配置します。
- Procmonログの収集: Process Monitorをダウンロードし、%ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\ProcessMonitor\Procmon.exeに配置します。
- Wiresharkログ: システムにWiresharkを手動でインストールします。

追加のログを収集するには：

1. Scout のホームページで、**トレースと再現**をクリックします。
2. データを収集する **マシンの選択または追加** ページで、ローカルマシンのチェックボックスをオンにします。ステータスは *Verified* と表示されている必要があります。

3. 「**続行**」をクリックし、トレースと再現の手順に従います。
4. 完了後、zip ファイル内のログを確認します。ログは *CDCLogs* フォルダーに圧縮されています。

> **注:**
>
> Procmonツールがトレース用に選択されている場合、Process Monitorログはすぐに大きくなる可能性があります。必要なツールのみを選択するようにしてください。ログのサイズは*%temp%\Scout-CDC-Log*で監視することもできます。

コレクションのスケジュール

> **注:**
>
> 現在、コレクションはスケジュールできますが、ヘルスチェックはスケジュールできません。

> スケジュール手順は、マシンを選択し、スケジュールを設定またはキャンセルすることで構成されます。スケジュールされたコレクションは自動的にCitrixにアップロードされます。（PowerShellインターフェイスを使用して、スケジュールされたコレクションをローカルに保存できます。Citrix Call Homeを参照してください。）

1. Scoutを起動します。マシンのスタートメニューから、**Citrix > Citrix Scout**を選択します。開いたページで、**Schedule**をクリックします。
2. マシンを選択します。サイト内のすべてのVDAとコントローラーが一覧表示されます。マシン名で表示をフィルターできます。

   グラフィカルインターフェイスを使用してVDAとコントローラーをインストールしたときに、Call Homeスケジュールを設定した場合 ((/ja-jp/citrix-virtual-apps-desktops/2411/manage-deployment/cis.html#citrix-call-home)を参照)、Scoutはデフォルトでそれらの設定を表示します。このバージョンのScoutを使用して、スケジュールされたコレクションを初めて開始したり、以前に構成したスケジュールを変更したりできます。

   コンポーネントのインストール中にマシンごとにCall Homeを有効/無効にした場合でも、Scoutで構成されたスケジュールは、選択したすべてのマシンに影響します。

診断情報を収集する各マシンの横にあるチェックボックスをオンにして、「**続行**」をクリックします。

その他のマシン（StoreFrontサーバーやCitrix Provisioningサーバーなど）を手動で追加するには、「Add machines manually」を参照してください。

Scoutは、選択した各マシンで検証テストを自動的に起動し、Verification testsの基準を満たしていることを確認します。マシンの検証に失敗した場合、**「Status」**列にメッセージが表示され、そのマシンのチェックボックスはオフになります。次のいずれかを実行できます。

- 問題を解決してから、マシンのチェックボックスをもう一度選択します。これにより、検証テストが再試行されます。
- そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンからは診断（またはトレース）は収集されません。

検証テストが完了したら、**Continue**をクリックします。

概要ページには、スケジュールが適用されるマシンが一覧表示されます。**Continue**をクリックします。

3. スケジュールを設定します。診断情報を収集するタイミングを指定します。注意：スケジュールは、選択したすべてのマシンに影響します。

   - 選択したマシンの週次スケジュールを構成するには、**「Weekly」**をクリックします。曜日を選択します。収集を開始する時刻（24時間形式）を入力します。
   - 選択したマシンの日次スケジュールを構成するには、**「Daily」**をクリックします。収集を開始する時刻（24時間形式）を入力します。
   - 選択したマシンの既存のスケジュールをキャンセルするには（別のスケジュールに置き換えない場合）、**「Off」**をクリックします。これにより、それらのマシンに対して以前に構成されたスケジュールがすべてキャンセルされます。

   続行をクリックします。

4. アップロードの認証を行い、必要に応じてプロキシを指定します。このプロセスの詳細については、アップロードの承認 を参照してください。注意: Scout スケジュールを使用している場合、保存されたトークンを使用して認証することはできません。

   アップロードの認証に Citrix 資格情報を使用するか、Citrix Cloud 資格情報を使用するかを選択します。 をクリックします。

   資格情報ページで：

- ファイルのアップロードにプロキシサーバーを使用する場合は、 をクリックします。Scout に、ブラウザのインターネットプロパティで構成されているプロキシ設定を使用するように指示できます。または、プロキシサーバーの IP アドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
- Citrix Cloud アカウントの場合は、 をクリックします。デフォルトのブラウザが Citrix Cloud ページを起動し、トークンが表示されます。トークンをコピーし、Scout ページに貼り付けます。
- Citrix アカウントの場合は、資格情報を入力します。

完了したら、 をクリックします。

構成されたスケジュールを確認します。 をクリックして Scout の開始ページに戻ります。

コレクション中、選択された各マシンの Windows アプリケーションログには、コレクションとアップロードに関するエントリが含まれます。

データマスキング

Citrix Scout を使用して収集された診断情報には、セキュリティ上機密性の高い情報が含まれる場合があります。Citrix Scout のデータマスキング機能を使用すると、診断ファイルを Citrix にアップロードする前に、機密データをマスクできます。

Scout のデータマスキングは、IP アドレス、マシン名、ドメイン名、ユーザー名、ハイパーバイザー名、デリバリーグループ名、カタログ名、アプリケーション名、および SID をマスクするように構成されています。

> **注:**
>
> CDF トレースは暗号化されており、マスクできません。
>
> Linux VDA ログは `.tar.gz2` 形式に圧縮されており、マスクできません。

新しい診断情報を収集し、データマスキングを実行する

Citrix Scoutのデータマスキング機能を使用するには、コマンドラインからScoutを起動します。

1. Windowsで、コマンドプロンプトを管理者として開きます。
2. Scoutがインストールされているディレクトリに移動します: `cd C:\Program Files\Citrix\Telemetry Service`。

3. Scoutを起動します: `ScoutUI.exe datamasking`。
4. 診断情報を収集するには、**Collect** または **Trace & Reproduce** をクリックします。
5. 収集が完了したら、**Enable data masking** を選択します。このオプションはデフォルトで有効になっています。
6. データマスクを構成します。デフォルトのルールを使用することも、ルールをカスタマイズすることもできます。
7. 診断情報の収集をアップロードするか保存するかを選択します。

    - **Upload the diagnostics collection to Citrix**を選択した場合、マスクされた診断ファイルはCitrixにアップロードされます。
    - **Save the diagnostics collection on your local machine**を選択した場合、元の診断情報とマスクされた診断情報の両方が指定された場所に保存されます。

既存の診断情報に対してデータマスキングを実行する

1. Windowsで、コマンドプロンプトを管理者として開きます。
2. Scoutがインストールされているディレクトリに移動します: `cd C:\Program Files\Citrix\Telemetry Service`。
3. データマスキングモードでScoutを直接起動します: `ScoutUI.exe datamasking filePath`。
4. ［データマスキングを有効にする］を選択して続行します。このオプションは既定で有効になっています。
5. データマスクを構成します。既定のルールでデータマスキングを実行することも、ルールをカスタマイズすることもできます。
6. 診断データをアップロードするか保存するかを選択します。

    - **診断データを Citrix にアップロード** を選択すると、マスキング済みの診断ファイルが Citrix にアップロードされます。
    - **診断データをローカルマシンに保存** を選択すると、元の診断データとマスキング済みの診断データの両方が指定した場所に保存されます。

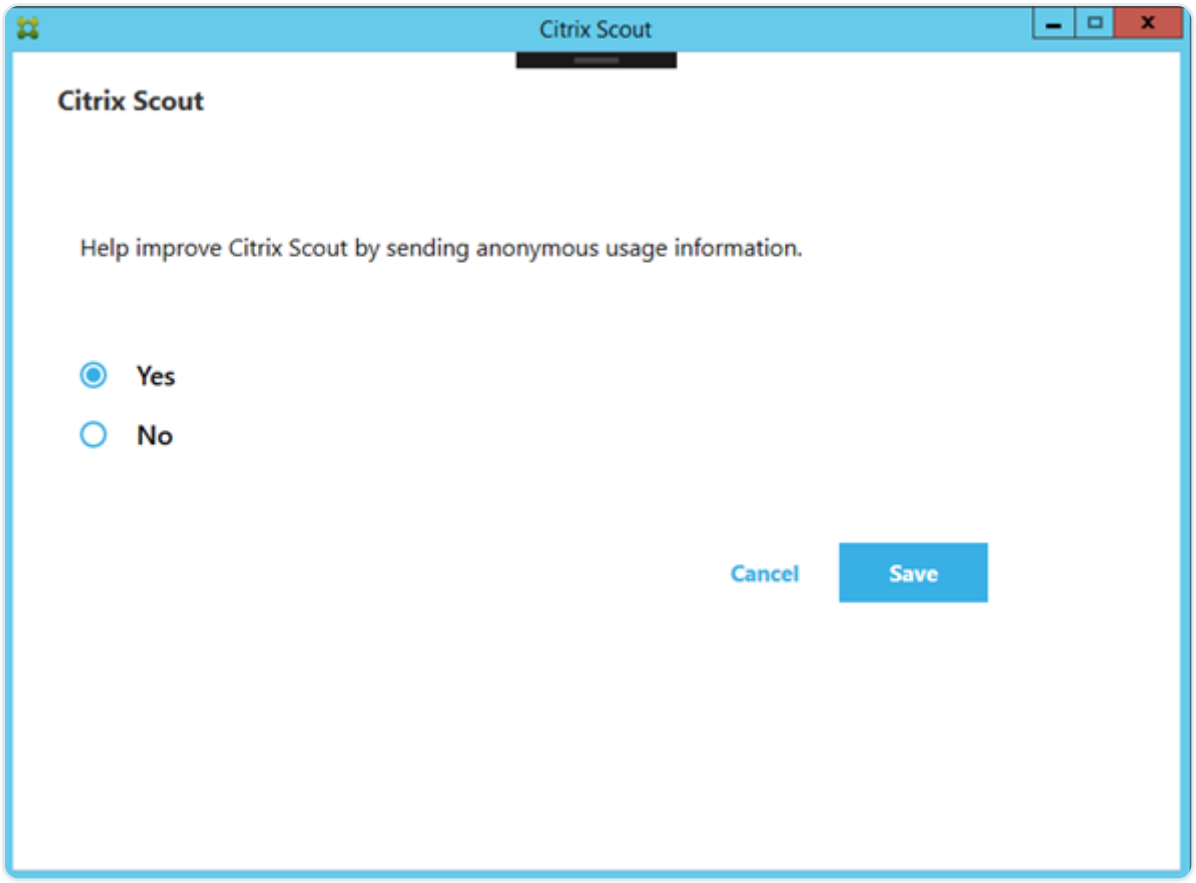
マスキング済みデータファイルとマッピングファイルの場所

診断データをアップロードまたは保存した後、リンクをクリックして元の診断データ、マスキング済み診断データ、およびマッピング情報ファイルを開きます。

使用状況データの収集

Scout の使用時に、Citrix は Google Analytics を使用して匿名の使用状況データを収集し、将来の製品機能や改善に活用します。データ収集は既定で有効になっています。

使用状況データの収集とアップロードを変更するには、Scout UI の **設定** 歯車アイコンをクリックします。**はい** または **いいえ** を選択し、**保存** をクリックして、情報を送信するかどうかを指定できます。



Scout 機能のコマンドラインインターフェイス

Scout の機能をコマンドラインインターフェイスから使用できるため、Scout UI を開かずに必要なログやデータを収集できます。上級ユーザーは、対象のマシンやサイトに対するログ記録やトレースを、ローカルまたはリモートで自動化できます。この機能は既定で有効になっています。

次の機能のコマンドが追加されています。

- ヘルプ
- 診断情報の収集
- トレースを開始
- トレースを停止
- 進行中のトレースセッションを一覧表示

- CDCの開始と停止

注:

リモートトレースセッションを実行する際は、VDAとDDCの両方に新しいテレメトリバージョンをインストールする必要があります。このインストールが必要なのは、Scoutコマンドラインがバージョン2411以降でサポートされており、`TelemetryService`の以前のバージョンではこの機能がサポートされていないためです。

次の表に、新しく追加されたコマンドを示します。

ヘルプ

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe -h`	コンテキストに応じたヘルプを表示します。	`ScoutCLI.exe -h` `ScoutCLI.exe -help`

診断情報を収集するためのコマンド

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe Collect -exclude <collector>`	指定されたコレクター（Windows Management Instrumentation (WMI) プロセス、レジストリ、クラッシュレポート、ヘッダー、トレース、`msi`、`vcu`、ツールテレメトリ、およびローカルデータ）からの診断を除外します。	`ScoutCLI.exe collect -exclude wmi, localdata -output "C:/Logs/mydata.zip"`
`ScoutCLI.exe Collect -output <filename>`	出力ログファイルを、サフィックスとして`.zip`を付けて保存する場所を指定します。	

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe Collect -fqdn <hostname>`	サイト内の指定されたマシンで診断を収集します。	`ScoutCLI.exe collect -fqdn hostname -exclude wmi, localdata -output "C:/Logs/mydata.zip"`

トレースの開始

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe StartTrace -guids <filename (xxx.ctl)>`	指定されたGUIDのターゲットモジュールのログを収集します。	ローカルマシンのトレース開始の例 - `ScoutCLI.exe StartTrace -guids C:\Logs\provider1.ctl -output C:\Logs\xxx.etl -name session1 -level 16 -max 50` ; リモートマシンのトレース開始の例 - `ScoutCLI.exe StartTrace -fqdn hostname -guids C:\Logs\provider1.ctl -output C:\Logs\xxx.etl -name session1 -level 16 -max 50`
`ScoutCLI.exe StartTrace -output <filename>`	出力ログファイルを、.etl をサフィックスとして保存する場所を指定します。	
`ScoutCLI.exe StartTrace -name <session name>`	トレースセッションの名前を定義します。	
`ScoutCLI.exe StartTrace -level <value>`	ターゲット診断の詳細をログに記録するログレベルを選択します。デフォルト値は16です。	
`ScoutCLI.exe StartTrace -max <value>`	最大ログファイルサイズをMB単位で指定します。デフォルト値は50です。	
`ScoutCLI.exe StartTrace -fqdn <hostname>`	サイト内の指定されたマシンでトレースを開始します。	

トレースの停止

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe StopTrace -name <session name>`	指定されたトレースセッションを停止します。	`ScoutCLI.exe StopTrace -name session1`

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe StopTrace -fqdn <hostname>`	サイト内の指定されたマシンでのトレースを停止します。リモートの `.etl` がコピーされるローカルパスを割り当てるには、-o オプションが必要です。	`ScoutCLI.exe StopTrace -fqdn hostname -name session1 -output C:\Logs\xxx.etl`
`ScoutCLI.exe StopTrace -output <filename>`	.etl をサフィックスとして持つ出力ログファイルを保存する場所を指定します。	

進行中のトレースセッションを一覧表示

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe ListSession -name <session name>`	指定されたトレースセッションの詳細を表示します。名前が指定されていない場合は、実行中のすべてのトレースセッションの詳細を表示します。	`ScoutCLI.exe ListSession -name session1`
`ScoutCLI.exe ListSession -fqdn <hostname>`	サイト内の指定されたマシンでトレースの詳細を表示します。	`ScoutCLI.exe ListSession -fqdn hostname -name session1`

CDC の開始と停止

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe StartCDC -config <filename>`	Citrix Diagnostic Collectors (CDC) ツールのパラメーターの JSON 構成ファイルを指定します。	`ScoutCLI.exe StartCDC -config xxx.json -path C:\Logs`
`ScoutCLI.exe StartCDC -path <folder>`	出力ログファイルの保存場所を指定します。	

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe StopCDC`	CDC ツールの収集を停止します。	`ScoutCLI.exe StopCDC`

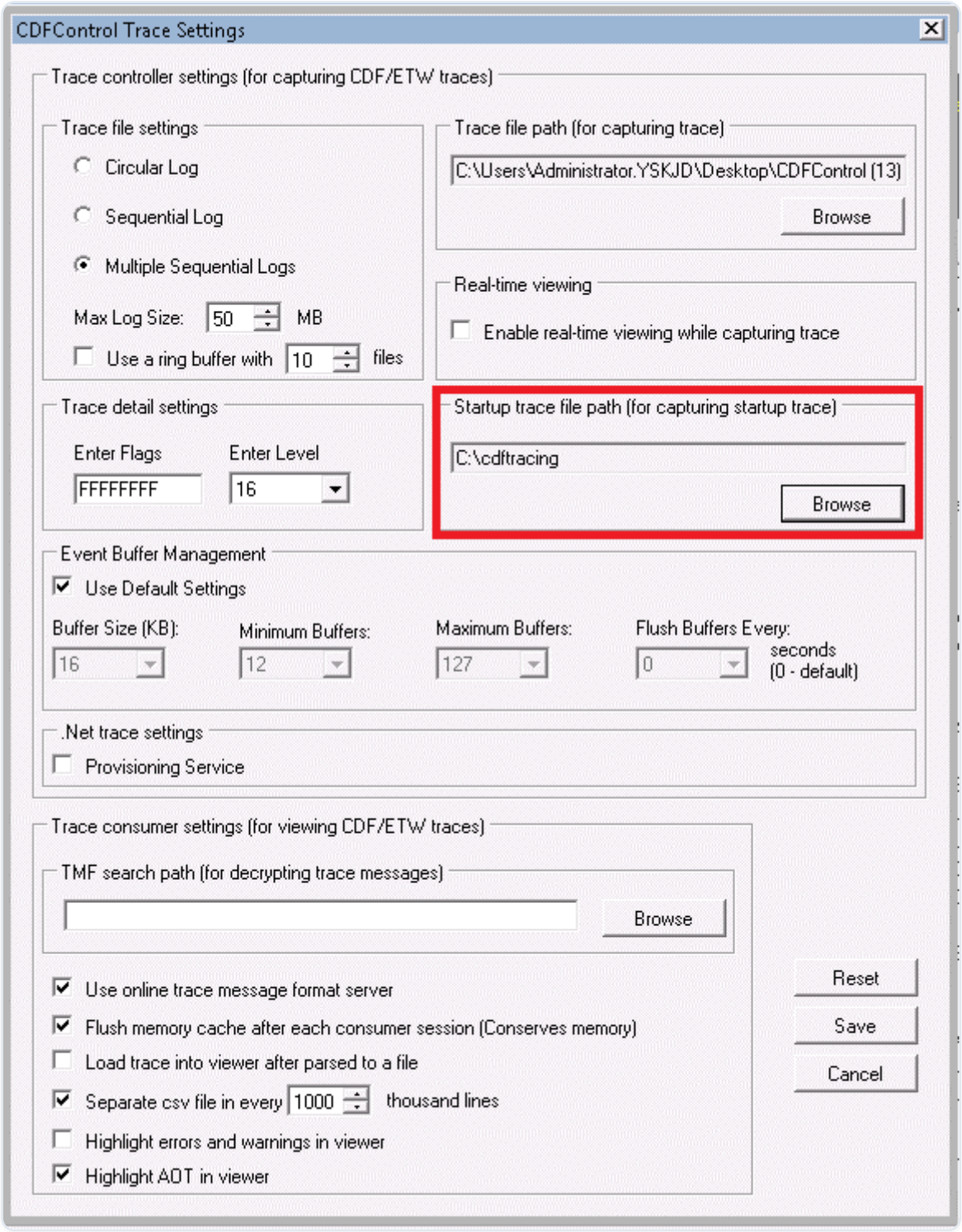
システム起動時にCitrix Diagnostic Facility (CDF) トレースを収集する

CDFControlユーティリティは、さまざまなCitrixトレースプロバイダーから表示されるCitrix Diagnostic Facility (CDF) トレースメッセージをキャプチャするためのイベントトレースコントローラーまたはコンシューマーです。これは、複雑なCitrix関連の問題のトラブルシューティング、解析フィルターのサポート、およびパフォーマンスデータの収集を目的としています。CDFControlユーティリティをダウンロードするには、CTX111961を参照してください。

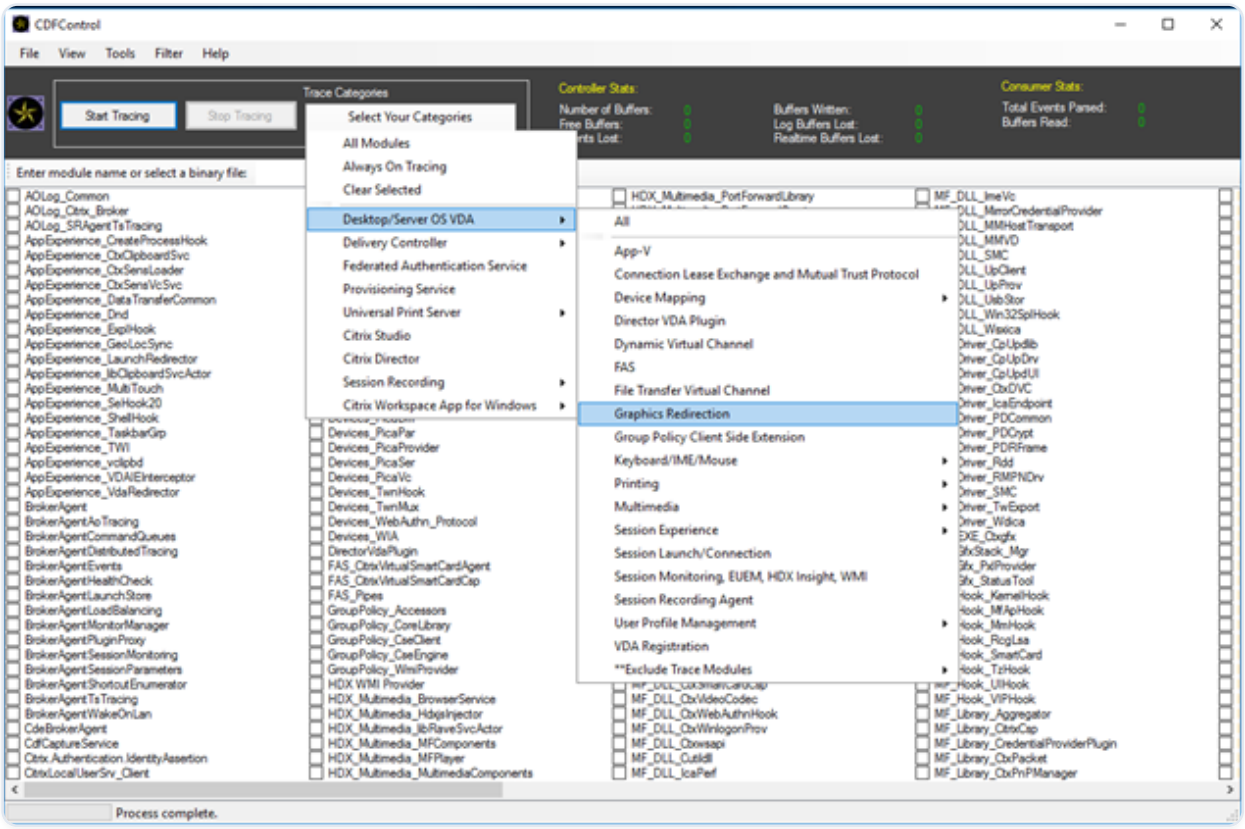
システム起動時にトレースを収集する

システム起動時にCDFトレースを収集するには、次の手順を使用します。管理者権限が必要です。

1. **CDFControl**を起動し、**ツール**メニューから**オプション**を選択します。
2. **起動トレースをキャプチャするための起動トレースファイルパス**セクションでトレースファイルパスを指定します。次に、**保存**をクリックします。



3. Citrixサポートが推奨する**トレースカテゴリ**を選択します。(次の例では、**グラフィックリダイレクト**が選択されています。この選択は単なる例です。トラブルシューティングを行う特定の問題に対してプロバイダーを有効にすることをお勧めします。)



4. **起動トレース**を選択し、**ツール**メニューから**有効にする**を選択します。

   有効にするを選択すると、アニメーションバーがスクロールを開始します。このアクティビティは手順に影響しません。次のステップに進みます。

5. **起動トレース**が有効になったら、**CDFControlユーティリティ**を閉じてシステムを再起動します。

6. **CDFControl**ユーティリティを起動します。システムが再起動し、エラーが表示されたら、**ツール**メニューから**起動トレース**を選択し、**無効にする**をクリックして起動トレースを無効にします。

7. 手順2で指定したトレースファイルパスに移動し、分析のためにトレースログファイル (.etl) を収集します。

委任管理

> **注:**

> Citrix Virtual Apps and Desktops™展開は、Web Studio (Webベース) とCitrix Studio (Windowsベース) の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioの詳細については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

委任管理モデルは、ロールベースおよびオブジェクトベースの制御を使用して、組織が管理アクティビティを委任する方法に合わせた柔軟性を提供します。委任管理はあらゆる規模の展開に対応し、展開の複雑さが増すにつれて、より詳細な権限の粒度を設定できます。委任管理では、管理者、ロール、スコープの3つの概念を使用します。

- **管理者:** 管理者は、Active Directoryアカウントによって識別される個人またはグループを表します。各管理者は、1つ以上のロールとスコープのペアに関連付けられています。
- **ロール:** ロールは職務を表し、それに関連付けられた定義済みの権限を持ちます。たとえば、デリバリーグループ管理者ロールには、「デリバリーグループの作成」や「デリバリーグループからのデスクトップの削除」などの権限があります。管理者はサイトに対して複数のロールを持つことができるため、ある人物がデリバリーグループ管理者とマシンカタログ管理者の両方になることができます。ロールは組み込みまたはカスタムにできます。

  組み込みロールは次のとおりです。

ロール	権限
フル管理者	すべてのタスクと操作を実行できます。フル管理者は常に「すべて」スコープと組み合わされます。
読み取り専用管理者	グローバル情報に加えて、指定されたスコープ内のすべてのオブジェクトを表示できますが、何も変更することはできません。たとえば、Scope=Londonの読み取り専用管理者は、すべてのグローバルオブジェクト（構成ログなど）と、ロンドンにスコープ指定されたオブジェクト（ロンドンデリバリーグループなど）を表示できます。ただし、その管理者はニューヨークスコープ内のオブジェクトを表示できません（ロンドンとニューヨークのスコープが重複しないと仮定した場合）。
ヘルプデスク管理者	デリバリーグループを表示し、それらのグループに関連付けられたセッションとマシンを管理できます。監視対象のデリバリーグループのマシンカタログとホスト情報を表示できます。また、それらのデリバリーグループ内のマシンに対してセッション管理およびマシン電源管理操作を実行できます。

ロール	権限
マシンカタログ管理者	マシンカタログを作成および管理し、それらにマシンをプロビジョニングできます。仮想化インフラストラクチャ、Provisioning Services、および物理マシンからマシンカタログを構築できます。この役割は、ベースイメージを管理し、ソフトウェアをインストールできますが、アプリケーションやデスクトップをユーザーに割り当てることはできません。
デリバリーグループ管理者	アプリケーション、デスクトップ、およびマシンを配信できます。また、関連するセッションを管理することもできます。ポリシーや電源管理設定など、アプリケーションとデスクトップの構成を管理することもできます。
ホスト管理者	ホスト接続とそれに関連するリソース設定を管理できます。マシン、アプリケーション、またはデスクトップをユーザーに配信することはできません。

特定の製品エディションでは、組織の要件に合わせてカスタムロールを作成し、より詳細に権限を委任できます。カスタムロールを使用して、コンソールでのアクションまたはタスクの粒度で権限を割り当てることができます。

- **スコープ:** スコープはオブジェクトの集合を表します。スコープは、組織に関連する方法でオブジェクトをグループ化するために使用されます（たとえば、営業チームが使用するデリバリーグループのセット）。オブジェクトは複数のスコープに属することができます。オブジェクトが1つ以上のスコープでラベル付けされていると考えることができます。組み込みスコープが1つあります。「すべて」で、すべてのオブジェクトが含まれます。フル管理者ロールは常に**すべて**のスコープとペアになります。

例

XYZ社は、部門（経理、営業、倉庫）とデスクトップオペレーティングシステム（Windows 7またはWindows 8）に基づいてアプリケーションとデスクトップを管理することにしました。管理者は5つのスコープを作成し、各デリバリーグループに2つのスコープをラベル付けしました。1つは使用される部門用、もう1つは使用するオペレーティングシステム用です。

次の管理者が作成されました。

管理者	ロール	スコープ
domain/fred	フル管理者	すべて (フル管理者ロールは常に「すべて」スコープを持ちます)
domain/rob	読み取り専用管理者	すべて
domain/heidi	読み取り専用管理者、ヘルプデスク管理者	すべての営業
domain/warehouseadmin	ヘルプデスク管理者	倉庫
domain/peter	デリバリーグループ管理者、マシンカタログ管理者	Win7

- Fred はフル管理者であり、システム内のすべてのオブジェクトを表示、編集、削除できます。
- Robはサイト内のすべてのオブジェクトを表示できますが、編集または削除はできません。
- ハイディはすべてのオブジェクトを表示でき、Salesスコープ内のデリバリーグループに対してヘルプデスクタスクを実行できます。これにより、彼女はそれらのグループに関連付けられたセッションとマシンを管理できますが、マシンの追加や削除など、デリバリーグループに変更を加えることはできません。
- warehouseadmin Active Directoryセキュリティグループのメンバーであるすべてのユーザーは、Warehouseスコープ内のマシンを表示し、ヘルプデスクタスクを実行できます。
- ピーターはWindows 7のスペシャリストであり、どの部署スコープに属しているかに関わらず、すべてのWindows 7マシンカタログを管理し、Windows 7アプリケーション、デスクトップ、およびマシンを提供できます。管理者はピーターをWin7スコープのフル管理者とすることを検討しましたが、フル管理者は「サイト」や「管理者」など、スコープが設定されていないすべてのオブジェクトに対しても完全な権限を持つため、この案は却下しました。

委任管理の使用方法

一般的に、管理者の数とその権限の粒度は、展開の規模と複雑さによって異なります。

- 小規模な展開や概念実証の展開では、1人または数人の管理者がすべての作業を行います。委任は行われません。この場合、各管理者を、すべてのスコープを持つ組み込みのフル管理者ロールで作成します。

- より多くのマシン、アプリケーション、デスクトップを含む大規模な展開では、より多くの委任が必要です。複数の管理者が、より具体的な機能的責任（ロール）を持つ場合があります。たとえば、2人がフル管理者で、他の管理者がヘルプデスク管理者である場合があります。また、管理者はマシンカタログなど、特定のオブジェクトグループ（スコープ）のみを管理する場合があります。この場合、新しいスコープを作成し、組み込みロールのいずれかと適切なスコープを持つ管理者を作成します。
- さらに大規模な展開では、より多くの（またはより具体的な）スコープと、型にはまらないロールを持つ異なる管理者が必要になる場合があります。この場合、スコープを編集または追加作成し、カスタムロールを作成し、既存および新規のスコープに加えて、組み込みまたはカスタムロールを持つ各管理者を作成します。

柔軟性と構成の容易さのために、管理者を作成する際にスコープを作成できます。マシンカタログまたは接続を作成または編集する際にもスコープを指定できます。

管理者の作成と管理

ローカル管理者としてサイトを作成すると、ユーザーアカウントは自動的に、すべてのオブジェクトに対する完全な権限を持つフル管理者になります。サイトが作成された後、ローカル管理者には特別な権限はありません。

フル管理者ロールには常にすべてのスコープが割り当てられます。これは変更できません。

デフォルトでは、管理者は有効になっています。管理者を今作成しても、その人が後で管理業務を開始しない場合は、管理者を無効にする必要があるかもしれません。既存の有効な管理者については、オブジェクト/スコープを再編成している間、一部を無効にし、更新された構成で稼働準備ができたときに再度有効にしたい場合があります。有効なフル管理者がいなくなる場合、フル管理者を無効にすることはできません。有効/無効のチェックボックスは、管理者を作成、コピー、または編集するときに利用できます。

管理者をコピー、編集、または削除する際にロール/スコープのペアを削除すると、その管理者に対するロールとスコープ間の関係のみが削除されます。ロールまたはスコープのいずれも削除されません。また、そのロール/スコープのペアで構成されている他の管理者にも影響しません。

管理者を作成および管理するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで をクリックし、 タブをクリックします。
2. 実行するタスクの手順に従います。

    - **管理者を作成する：** アクションバーで をクリックします。ユーザーアカウント名を入力または参照し、スコープを選択または作成してから、役割を選択します。新しい管理者はデフォルトで有効になっています。これは変更できます。

- **管理者をコピーする：** 管理者を選択し、アクションバーで をクリックします。ユーザーアカウント名を入力または参照します。役割/スコープのペアを選択して編集または削除したり、新しいペアを追加したりできます。新しい管理者はデフォルトで有効になっています。これは変更できます。
- **管理者を編集する：** 管理者を選択し、アクションバーで をクリックします。役割/スコープのペアを編集または削除したり、新しいペアを追加したりできます。
- **管理者を削除する：** 管理者を選択し、アクションバーで をクリックします。有効なフル管理者がいなくなる場合、フル管理者を削除することはできません。

上部のペインには、作成した管理者が表示されます。管理者を選択すると、下部のペインにその詳細が表示されます。 列は、管理者に関連付けられている役割とスコープのペアに、使用できない役割またはスコープが含まれているかどうかを示します。関連付けられている役割とスコープのペアに、使用できない役割またはスコープが含まれている場合、次の警告メッセージが表示されます。

- 関連付けられているロールまたはスコープが使用できません

> **重要：**

> 警告メッセージは、関連付けられている役割とスコープのペアに、使用できない役割、使用できないスコープ、またはその両方が含まれている場合にのみ表示されます。

> 管理者からロールとスコープのペアを削除するには、次のいずれかの手順を実行します。

- 役割とスコープのペアを削除します。
  a. アクションバーで をクリックします。
  b. ウィンドウで、役割とスコープのペアを選択し、 をクリックします。
  c. 「**保存**」をクリックして終了します。
- 管理者を削除します。
  a. アクションバーで、「**管理者削除**」をクリックします。
  b. 確認ウィンドウで、「**削除**」をクリックします。

ロールの作成と管理

管理者がロールを作成または編集する場合、自分自身が持っている権限のみを有効にできます。これにより、管理者が現在持っている権限よりも多くの権限を持つロールを作成し、それを自分自身に割り当てること（またはすでに割り当てられているロールを編集すること）を防ぎます。

ロール名には最大64文字のUnicode文字を含めることができます。ただし、バックスラッシュ、スラッシュ、セミコロン、コロン、ポンド記号、コンマ、アスタリスク、疑問符、等号、左右の矢印、パイプ、左右の角括弧、左右の丸括弧、引用符、アポストロフィは含めることができません。説明には最大256文字のUnicode文字を含めることができます。

組み込みロールを編集または削除することはできません。いずれかの管理者が使用しているカスタムロールを削除することはできません。

> **注:**
>
> 特定の製品エディションのみがカスタムロールをサポートしています。カスタムロールをサポートするエディションのみが、アクションバーに関連エントリを持っています。

ロールを作成および管理するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで「**管理者**」をクリックし、次に「**ロール**」タブをクリックします。
2. 実行したいタスクの手順に従ってください。

   - **ロールの詳細を表示する:** ロールを選択します。下部のペインに、そのロールのオブジェクトタイプと関連する権限が一覧表示されます。下部のペインにある「**管理者**」タブをクリックすると、現在このロールを持つ管理者の一覧が表示されます。
   - **カスタムロールを作成する:** アクションペインで「**ロールの作成**」をクリックします。名前と説明を入力します。オブジェクトタイプと権限を選択します。
   - **役割をコピーする:** 役割を選択し、アクションバーで **役割をコピー** をクリックします。必要に応じて、名前、説明、オブジェクトの種類、および権限を変更します。
   - **カスタム役割を編集する:** 役割を選択し、アクションバーで **役割を編集** をクリックします。必要に応じて、名前、説明、オブジェクトの種類、および権限を変更します。
   - **カスタム役割を削除する:** 役割を選択し、アクションバーで **役割を削除** をクリックします。プロンプトが表示されたら、削除を確認します。

スコープの作成と管理

サイトを作成すると、利用可能なスコープは「すべて」スコープのみであり、これは削除できません。

次の手順でスコープを作成できます。管理者を作成するときにもスコープを作成できます。各管理者は、少なくとも1つのロールとスコープのペアに関連付けられている必要があります。デスクトップ、マシンカタログ、アプリケーション、またはホストを作成または編集するときに、それらを既存のスコープに追加できます。スコープに追加しない場合、それらは「すべて」スコープの一部として残ります。

サイトの作成はスコープ化できず、委任管理オブジェクト（スコープと役割）もスコープ化できません。ただし、スコープ化できないオブジェクトは「すべて」スコープに含まれます。（フル管理者は常に「すべて」スコープを持ちます。）マシン、電源アクション、デスクトップ、およびセッションは直接スコープ化されません。管理者は、関連するマシンカタログまたはデリバリーグループを通じて、これらのオブジェクトに対する権限を割り当てることができます。

スコープの作成と管理に関するルール:

- スコープ名には最大64文字のUnicode文字を含めることができます。スコープ名には、バックスラッシュ、スラッシュ、セミコロン、コロン、ポンド記号、コンマ、アスタリスク、疑問符、等号、左矢印、右矢印、パイプ、左右の角括弧、左右の丸括弧、引用符、アポストロフィを含めることはできません。
- スコープの説明には最大256文字のUnicode文字を含めることができます。
- スコープをコピーまたは編集する際は、スコープからオブジェクトを削除すると、それらのオブジェクトが管理者からアクセスできなくなる可能性があることに注意してください。編集されたスコープが1つ以上の役割とペアになっている場合、スコープの更新によって役割/スコープのペアが使用できなくならないようにしてください。

スコープを作成および管理するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで **管理者** をクリックし、**スコープ** タブをクリックします。
2. 完了したいタスクの手順に従います。

    - **スコープを作成する:** アクションバーで **新しいスコープを作成** をクリックします。名前と説明を入力します。特定の種類のすべてのオブジェクト（例: デリバリーグループ）を含めるには、オブジェクトの種類を選択します。特定のオブジェクトを含めるには、種類を展開してから個々のオブジェクト（例: 営業チームが使用するデリバリーグループ）を選択します。

- **スコープをコピーする:** スコープを選択し、アクションバーで**スコープのコピー**をクリックします。名前と説明を入力します。必要に応じて、オブジェクトの種類とオブジェクトを変更します。
- **スコープを編集する:** スコープを選択し、アクションバーで**スコープの編集**をクリックします。必要に応じて、名前、説明、オブジェクトの種類、およびオブジェクトを変更します。
- **スコープを削除する:** スコープを選択し、アクションバーで**スコープの削除**をクリックします。プロンプトが表示されたら、削除を確認します。

テナント管理を設定する

単一のCitrix Virtual Apps and Desktopsサイト内に管理パーティションを作成するために、テナント管理を設定します。各テナントには、マシンカタログやデリバリーグループなどの分離されたリソースと構成があります。特定のテナントにアクセスできる管理者は、そのテナントに関連付けられたリソースと構成のみを管理できます。使用例としては、単一サイト内に異なるビジネスサイロ（独立した部門または個別のIT管理チーム）を持つ企業が挙げられます。

大まかに言えば、テナント管理を設定するためのワークフローには以下が含まれます。

1. テナントを作成する
2. テナントの管理者を追加する

テナントを作成する

テナントスコープを作成してテナントを作成します。詳細な手順は次のとおりです。

1. Web Studioにサインインし、左ペインで**管理者**をクリックし、次に**スコープ**タブをクリックします。
2. *スコープの作成**をクリックしてテナントの作成を開始します。
3. テナントスコープの以下の詳細を入力します。

    a. スコープのわかりやすい名前を入力します。この名前はテナントの識別子としても機能します。

    b. （オプション）簡単な説明を入力します。

    c. 「**テナントスコープ**」を選択します。

    d. 必要に応じて、テナントに関連付けられているオブジェクトを選択します。オブジェクトの作成時または管理時に、テナントスコープにオブジェクトを追加することもできます。

    e. 「**OK**」をクリックして作成を完了します。

完了後、以下が表示されます。

- 新しいテナントスコープレコードがスコープリストに表示され、「**種類**」列で「**テナント**」として識別されます。
- スコープ名は、Web Studio の右上隅にある「**すべてのテナント**」ドロップダウンリストに表示されます。

テナントスコープを操作する際は、以下の考慮事項に留意してください。

- テナントプロパティは、ホスティング > マシンカタログ > デリバリーグループ > アプリケーションという階層的な割り当て順序に従います。下位レベルのオブジェクトは、上位レベルのオブジェクトからテナントプロパティを継承します。たとえば、テナントスコープのデリバリーグループを選択する場合は、関連するホスティングとマシンカタログも選択していることを確認してください。そうしないと、デリバリーグループはテナントのプロパティを継承できません。
- テナントスコープを作成した後、オブジェクトを変更することでテナントの割り当てを編集できます。テナントの割り当てが変更された場合でも、同じテナントまたはそれらのテナントのサブセットに割り当てられるという制約が適用されます。ただし、テナントの割り当てが変更されても、下位レベルのオブジェクトは再評価されません。テナントの割り当てを変更する際は、オブジェクトが適切に制限されていることを確認してください。たとえば、マシンカタログが `TenantA` と `TenantB` で利用可能な場合、`TenantA` 用と `TenantB` 用のデリバリーグループを作成できます。（`TenantA` と `TenantB` は両方ともそのマシンカタログに関連付けられています。）その後、マシンカタログを `TenantA` のみに関連付けるように変更できます。その結果、`TenantB` に関連付けられているデリバリーグループは無効になります。

テナントの管理者を追加する

管理者ロールとテナントを持つユーザーアカウントを割り当てることで、テナントの管理者を追加します。

テナントの管理者を追加するには、次の手順に従います。

1. Web Studio にサインインし、左側のペインで「**管理者**」をクリックし、次に「**管理者**」タブをクリックします。
2. 「**管理者を追加**」をクリックし、次の手順に従って完了します。
    a. ユーザーアカウント名を入力または参照し、「**次へ**」をクリックします。
    b. 「**カスタムアクセス**」を選択し、必要に応じて1つ以上の役割（例: マシンカタログ管理者）を選択します。

c. 各役割の横にある「**スコープの編集**」をクリックし、スコープを「**すべて**」から目的のテナントスコープに変更して、「**保存**」をクリックします。

3. **Next**をクリックします。
4. 「**確認と確定**」ページで、「**招待状を送信**」をクリックします。

レポートの作成

委任管理レポートには、次の2種類を作成できます。

- 管理者に関連付けられている役割とスコープのペア、および各オブジェクトタイプ（例: デリバリーグループやマシンカタログ）の個々の権限を一覧表示するHTMLレポート。このレポートはWeb Studioから生成します。

  このレポートを作成するには、次の手順に従います。

  a. Web Studioにサインインし、左ペインで「**管理者**」をクリックします。

  b. 管理者を選択し、アクションバーで「**レポートの作成**」をクリックします。

  管理者の作成、コピー、または編集時に、このレポートを要求することもできます。

- すべての組み込み役割とカスタム役割を権限にマッピングするHTMLまたはCSVレポート。このレポートは、OutputPermissionMapping.ps1という名前のPowerShellスクリプトを実行して生成します。

  このスクリプトを実行するには、フル管理者、読み取り専用管理者、または役割の読み取り権限を持つカスタム管理者である必要があります。スクリプトは、Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scriptsにあります。

  構文：

  `OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path string] [-AdminAddress string] [-Show] [CommonParameters]`

パラメーター	説明
`-Help`	スクリプトのヘルプを表示します。
`-Csv`	CSV出力を指定します。デフォルト = HTML
`-Path string`	出力の書き込み先。デフォルト = stdout

パラメーター	説明
`-AdminAddress string`	接続先のDelivery Controller™のIPアドレスまたはホスト名。デフォルト = localhost
`-Show`	(`-Path` パラメーターも指定されている場合にのみ有効) 出力をファイルに書き込むと、`-Show` によって出力がWebブラウザーなどの適切なプログラムで開かれます。
共通パラメーター	`Verbose`、`Debug`、`ErrorAction`、`ErrorVariable`、`WarningAction`、`WarningVariable`、`OutBuffer`、および `OutVariable`。詳細については、Microsoftのドキュメントを参照してください。

次の例では、HTMLテーブルをRoles.htmlという名前のファイルに書き込み、そのテーブルをWebブラウザーで開きます。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

-Path Roles.html –Show
```

次の例では、CSVテーブルをRoles.csvという名前のファイルに書き込みます。テーブルは表示されません。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

–CSV -Path Roles.csv
```

Windowsコマンドプロンプトから、上記の例のコマンドは次のとおりです。

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'
```

```
-CSV -Path Roles.csv"
```

デリバリーコントローラー

注：

Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

デリバリーコントローラーは、ユーザーアクセス管理、接続の仲介と最適化を担当するサーバー側コンポーネントです。コントローラーは、デスクトップおよびサーバーイメージを作成するMachine Creation Services™も提供します。

サイトには少なくとも1つのコントローラーが必要です。最初のコントローラーをインストールした後、サイトの作成時または後でコントローラーを追加できます。サイトに複数のコントローラーを配置することには、主に2つの利点があります。

- **冗長性：** ベストプラクティスとして、本番サイトでは常に異なる物理サーバー上に少なくとも2つのコントローラーを配置してください。1つのコントローラーが故障しても、他のコントローラーが接続を管理し、サイトを管理できます。
- **スケーラビリティ：** サイトのアクティビティが増加すると、コントローラーのCPU使用率とデータベースのアクティビティも増加します。追加のコントローラーにより、より多くのユーザー、アプリケーション、デスクトップ要求を処理できるようになり、全体的な応答性が向上します。

各コントローラーはサイトデータベースと直接通信します。複数のゾーンがあるサイトでは、すべてのゾーンのコントローラーがプライマリゾーンのサイトデータベースと通信します。

重要：

サイトの構成後、コントローラーのコンピューター名またはドメインメンバーシップを変更しないでください。

VDAがControllerに登録する方法

VDAを使用する前に、サイト内のデリバリーコントローラーに登録（通信を確立）する必要があります。VDA登録の詳細については、「VDA registration with Controllers」を参照してください。

コントローラーの追加、削除、または移動

コントローラーを追加、削除、または移動するには、「Databases」の記事に記載されているサーバーロールおよびデータベースロールの権限が必要です。

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

サイトにDelivery Controller™を追加する場合は、高可用性のために使用するレプリカSQL Serverに、そのマシンのログオン資格情報を追加してください。

展開でデータベースミラーリングを使用している場合:

- Controllerを追加、削除、または移動する前に、プリンシパルデータベースとミラーデータベースの両方が実行中であることを確認してください。さらに、SQL Server Management Studioでスクリプトを使用している場合は、スクリプトを実行する前にSQLCMDモードを有効にしてください。
- Controllerの追加、削除、または移動後にミラーリングを確認するには、PowerShell `Get-configdbconnection` コマンドレットを実行します。このコマンドレットにより、接続文字列にミラーへのフェールオーバーパートナーが設定されていることが保証されます。

Controller を追加、削除、または移動した後:

- 自動更新が有効になっている場合、VDAは90分以内に更新されたControllerのリストを受信します。
- 自動更新が有効になっていない場合は、すべてのVDAでControllerポリシー設定またはListOfDDCsレジストリキーが更新されていることを確認してください。Controllerを別のサイトに移動した後、両方のサイトでポリシー設定またはレジストリキーを更新してください。

Controllerを追加する

Controllerは、サイトの作成時および後で追加できます。このソフトウェアの以前のバージョンでインストールされたControllerを、このバージョンで作成されたサイトに追加することはできません。

1. サポートされているオペレーティングシステムを含むサーバーでインストーラーを実行します。Delivery Controllerコンポーネントと、必要なその他のコアコンポーネントをインストールします。インストールウィザードを完了します。
2. まだサイトを作成していない場合は、このControllerでCitrix Site Manager を実行してサイトを作成します。このControllerのIPアドレスは、新しいサイトに自動的に追加されます。

   データベースを初期化するスクリプトを生成する予定がある場合は、スクリプトを生成する前に Controller を追加してください。
3. 既にサイトを作成している場合は、次の手順に従ってください：

   a. このControllerでCitrix Site Manager を実行し、 をクリックして、参加するサイトのControllerのアドレスを入力します。

   b. Studio構成ツール を実行して、ControllerをWeb Studioに追加します。

Controller を削除する

サイトからコントローラーを削除しても、Citrixソフトウェアやその他のコンポーネントはアンインストールされません。この操作により、コントローラーはデータベースから削除され、接続の仲介やその他のタスクに使用できなくなります。コントローラーを削除しても、後で同じサイトまたは別のサイトに再度追加できます。サイトには少なくとも1つのコントローラーが必要なため、Web Studioに表示されている最後のコントローラーを削除することはできません。

サイトからコントローラーを削除しても、データベースサーバーへのコントローラーのログオンは削除されません。これは、同じマシン上の他の製品のサービスで使用されているログオンが誤って削除されるのを防ぐためです。ログオンが不要になった場合は、手動で削除する必要があります。ログオンを削除するには、`securityadmin`サーバーロールの権限が必要です。

コントローラーを削除した後：

- 自動更新を使用しているVDAは、他の利用可能なコントローラーに再登録されます。この再登録は、自動更新メカニズムが有効になっており、VDAが他のコントローラー（削除されたコントローラーと同じセカンダリゾーン、またはオンプレミス展開のプライマリゾーン）に到達できる場合にのみ発生します。
- Citrix StoreFrontでコントローラー情報を更新します。詳細については、「コントローラーの管理」を参照してください。
- Citrix StoreFrontで、Citrix Gatewayを介したリモートアクセス用のSecure Ticket Authority (STA) URLを更新します。詳細については、「Secure Ticket Authority の管理」を参照してください。

- Citrix Gatewayで、仮想サーバーのSTA URLを更新します。詳細については、「Citrix Gateway」を参照してください。

重要：

サイトからコントローラーを削除するまでは、Active Directoryからコントローラーを削除しないでください。

1. Web Studioがロードされ、削除したいコントローラーが表示されるように、コントローラーの電源がオンになっていることを確認してください。
2. Web Studioがコントローラーを完全にロードした後、コントローラー上のすべてのサービスが実行されており、コントローラーの電源がオンのままであることを確認してください。
3. Web Studioにサインインし、左ペインで**［設定］**を選択します。
4. **［Delivery Controller］**タイルを見つけて、**［編集］**をクリックします。
5. **［Delivery Controllerの管理］**ページで、削除したいコントローラーを選択します。
6. **Controllerの削除**を選択します。適切なデータベースロールと権限がない場合は、データベース管理者がControllerを削除できるようにするスクリプトを生成するオプションが提示されます。

   Web Studioは、Controllerを削除する前に事前チェックを実行します。Controllerが電源オフの状態であり、以下のサービスステータスにない場合は、安全に削除できます。

   - 不明
   - 失敗保留中
   - 古いバージョン
   - 新しいバージョン
   - バージョン変更が進行中
   - 必須機能が不足しています

   Controllerが電源オフの状態ではなく、上記のいずれかのサービスステータスにある場合、Web StudioはControllerの電源をオフにするよう促します。
7. データベースサーバーから Controller のマシンアカウントを削除する必要があります。削除する前に、別サービスがそのアカウントを使用していないことを確認してください。

Web Studioを使用してControllerを削除した後、現在のタスクが適切に完了するように、そのControllerへのトラフィックがしばらく残る場合があります。Controllerの削除を短時間で強制したい場合は、Citrixは、Controllerがインストールされていたサーバーをシャットダウンするか、そのサーバーをActive Directoryから削除することを推奨します。その後、サイト上の他のControllerを再起動して、削除されたControllerとの通信がこれ以上行われないようにします。

Controller を別のゾーンに移動する

サイトに複数のゾーンが含まれている場合、Controller を別のゾーンに移動できます。この移動が VDA 登録やその他の操作にどのように影響するかについては、「ゾーン」を参照してください。

1. 左ペインで「**ゾーン**」を選択します。
2. 中央ペインでゾーンを選択し、次にControllerを選択します。
3. アクションバーで**アイテムの移動**を選択します。
4. 表示される**アイテムの移動**ページで、Controllerを移動するゾーンを選択します。
5. **保存**をクリックします。

VDA を別のサイトに移動する

Citrix Provisioning™を使用してVDAがプロビジョニングされた場合、または既存のイメージである場合、アップグレード時、あるいはテストサイトで作成されたVDAイメージを本番サイトに移動する際に、VDAを別のサイト（サイト1からサイト2へ）に移動できます。Machine Creation Services (MCS)を使用してプロビジョニングされたVDAは、あるサイトから別のサイトへ移動できません。MCSは、VDAがControllerに登録するために確認するListOfDDCsの変更をサポートしていません。MCSを使用してプロビジョニングされたVDAは、常に作成されたサイトに関連付けられているListOfDDCsを確認します。

VDAを別のサイトに移動するには、インストーラーを使用する方法とCitrixポリシーを使用する方法の2つがあります。

インストーラー

インストーラーを実行し、サイト2のControllerのFQDN（DNSエントリ）を指定してControllerを追加します。

インストーラーでControllerを指定するのは、Controllerポリシー設定が使用されていない場合のみです。

グループポリシーエディター

次の例では、複数のVDAをサイト間で移動します。

1. サイト1で次の設定を含むポリシーを作成し、そのポリシーをDelivery Groupレベルにフィルターして、サイト間の段階的なVDA移行を開始します。
   - Controller: サイト2の1つ以上のControllerのFQDN（DNSエントリ）を含みます。
   - Controllerの自動更新を有効にする: 無効に設定します。
2. デリバリーグループ内の各VDAは、新しいポリシーが適用されてから90分以内に通知を受けます。VDAは受信したControllerのリストを無視し（自動更新が無効になっているため）、ポリシーで指定されたControllerのいずれかを選択します。このポリシーにはサイト2のControllerがリストされています。
3. VDAがサイト2のControllerに正常に登録されると、サイト2のListOfDDCsとポリシー情報を受け取ります。これはデフォルトで自動更新が有効になっています。サイト1でVDAが登録されていたControllerは、サイト2のControllerから送信されたリストには含まれていません。そのため、VDAはサイト2のリストにあるControllerの中から選択して再登録します。それ以降、VDAはサイト2からの情報で自動的に更新されます。

グループポリシーエディターの使用方法については、Citrixポリシーのドキュメントを参照してください。

IPv4/IPv6 のサポート

このリリースでは、純粋な IPv4、純粋な IPv6、および重複する IPv4 と IPv6 ネットワークを使用するデュアルスタック展開をサポートしています。

次のコンポーネントは IPv4 のみをサポートします。その他すべてのコンポーネントは IPv4 と IPv6 をサポートします。

- XenServer®
- **Only use IPv6 Controller registration**ポリシー設定によって制御されていないVirtual Delivery Agents (VDA)

IPv6 通信は、VDA 接続に関連する2つの Citrix® ポリシー設定によって制御されます。

- **IPv6の使用を強制する主要な設定:** Only use IPv6 Controller registration。

  このポリシー設定は、VDA が Delivery Controller に登録するために使用するアドレス形式を制御します。

  有効にすると、VDAは次の優先順位で選択された単一のIPv6アドレスを使用して、Controllerに登録および通信します。グローバルIPアドレス、Unique Local Address (ULA)、リンクローカルアドレス（他のIPv6アドレスが利用できない場合のみ）。

無効にすると、VDAはマシンのIPv4アドレスを使用してControllerに登録および通信します。これがデフォルト値です。

チームが頻繁にIPv6ネットワークを使用する場合、**Only use IPv6 Controller registration**ポリシー設定が有効になっているイメージまたは組織単位 (OU) に基づいて、それらのユーザーのデスクトップとアプリケーションを公開します。

チームが頻繁にIPv4ネットワークを使用する場合、**Only use IPv6 Controller registration**ポリシー設定が無効になっているイメージまたはOUに基づいて、それらのユーザーのデスクトップとアプリケーションを公開します。

- **IPv6ネットマスクを定義する依存設定:** Controller registration IPv6 netmask。

  マシンは複数の IPv6 アドレスを持つことができます。このポリシー設定により、管理者は、登録されている場合に、VDA をグローバル IP ではなく、優先サブネットのみに制限できます。この設定は、VDA が登録するネットワークを指定します。VDA は、指定されたネットマスクに一致する最初のアドレスにのみ登録します。

  この設定は、**Only use IPv6 Controller registration policy**設定が有効な場合にのみ有効です。デフォルト = 空の文字列

展開に関する考慮事項

環境にIPv4ネットワークとIPv6ネットワークの両方が含まれている場合は、IPv4専用クライアントとIPv6ネットワークにアクセスできるクライアント用に、別々のデリバリーグループ構成を作成します。ユーザーを区別するために、命名規則、手動のActive Directoryグループ割り当て、またはSmartAccessフィルターの使用を検討してください。 接続がIPv6ネットワークで開始され、その後IPv4アクセスのみを持つクライアントから再接続しようとすると、セッションの再接続が失敗する可能性があります。

注記 - DNS解決が有効になっている場合は、これらの考慮事項は適用されません。

Web Studio を使用した Citrix Virtual Apps and Desktops™ のライセンス

> **注:**
>
> - Citrix Virtual Apps and Desktops の展開は、Web Studio (Web ベース) と Citrix Studio (Windows ベース) の 2 つの管理コンソールを使用して管理できます。この記事では Web

Studio のみを取り上げます。Citrix Studio については、Citrix Virtual Apps and Desktops 7 2212 以前の同等の記事を参照してください。

- License Activation Service (LAS) は、従来の Citrix® レガシーライセンスに代わる新しいクラウドベースのライセンスソリューションです。LAS はアクティベーション用の新しいモジュールを導入し、ライセンス管理へのシームレスで最新のアプローチを保証します。詳細については、License Activation Service を参照してください。

Web Studio から、ライセンスサーバーが Web Studio と同じドメイン内にあるか、信頼されたドメイン内にある場合、ライセンスを管理および追跡できます。ライセンスタスクの詳細については、ライセンスドキュメント および マルチタイプライセンス を参照してください。

次の表に、サポートされているエディションとライセンスモデルを示します。

製品	エディション	ライセンスモデル
シトリックス バーチャル アプリ	プレミアム、アドバンスト、スタンダード	同時使用
シトリックス バーチャル デスクトップ	プレミアム、アドバンスト、スタンダード	ユーザー/デバイスおよび同時使用

詳細については、同時使用ライセンスおよびユーザー/デバイスライセンスを参照してください。

サポートされているCurrent Release (CR) およびLong Term Service Release (LTSR) バージョン

Citrixでは、常にCitrix License Serverの最新バージョンを使用し、含まれる可能性のある機能やセキュリティの改善点を利用することを強くお勧めします。

注:

License Server VPXは非推奨となり、今後のメンテナンスやセキュリティ修正は提供されません。License Server VPXのバージョン11.16.6以前を使用しているお客様は、Windows向けLicense Serverの最新バージョンにできるだけ早く移行することをお勧めします。

Citrix製品のライフサイクル日付の詳細については、製品マトリックスを参照してください。

レガシー製品および製品バージョンについては、レガシー製品マトリックスを参照してください。

以下のタスクを完了するには、完全なライセンス管理者である必要があります。Web Studioでライセンス情報を表示するには、管理者は少なくとも「ライセンスの読み取り」委任管理権限を持っている必要があります。組み込みの「完全管理者」および「読み取り専用管理者」の役割には、その権限があります。

Web Studioを使用してCitrixからライセンスをダウンロードしてインストールする

1. Web Studioにサインインし、左側のペインで**［ライセンス］**を選択します。
2. アクションバーで**［ライセンスの割り当て］**を選択します。
3. ライセンスアクセスコードを入力します。このコードは、ライセンスの購入または更新後にCitrixからメールで送付されます。
4. 製品を選択し、**［ライセンスの割り当て］**を選択します。その製品で利用可能なライセンスが割り当てられ、ダウンロードされます。特定のライセンスアクセスコードのすべてのライセンスを割り当ててダウンロードすると、そのライセンスアクセスコードを再利用することはできません。同じコードで他のトランザクションを実行するには、My Accountにログオンしてください。

ローカルコンピューターまたはネットワークに保存されているライセンスを追加する

1. Web Studioにサインインし、左側のペインで**［ライセンス］**を選択します。
2. アクションバーで****を選択します。
3. ライセンスファイルを参照し、ライセンスサーバーに追加します。

ライセンスサーバーを変更する

1. Web Studioにサインインし、左側のペインで****を選択します。
2. アクションバーで****を選択します。
3. ライセンスサーバーのアドレスを*name:port*の形式で入力します。ここで、nameはDNS、NetBIOS、またはIPアドレスです。ポート番号を指定しない場合、デフォルトのポート（27000）が使用されます。

使用するライセンスの種類を選択する

- サイトを構成する際、ライセンスサーバーを指定した後、使用するライセンスの種類を選択するよう求められます。サーバーにライセンスがない場合、ライセンスなしで製品を30日間試用するオプションが自動的に選択されます。
- サーバーにライセンスがある場合、その詳細が表示され、いずれかを選択できます。または、ライセンスファイルをサーバーに追加してから、それを選択することもできます。

製品エディションとライセンスモデルを変更する

1. Web Studioにサインインし、左側のペインで****を選択します。
2. アクションバーで****を選択します。
3. 適切なオプションを更新します。

ライセンス管理コンソールにアクセスするには、アクションバーで****を選択します。コンソールはすぐに表示されるか、ダッシュボードがパスワード保護されている場合は、ライセンス管理コンソールの資格情報を求められます。コンソールの使用方法の詳細については、ライセンスドキュメントを参照してください。

> **注:**

> Web Studioでライセンスを切り替えると、その変更がCitrix Directorに反映されるまでに最大5分かかります。たとえば、AdvancedとPremiumを切り替える場合などです。

ライセンス管理者を追加する

1. Web Studioにサインインし、左側のペインで**［ライセンス］**を選択します。
2. **［ライセンス管理者］**タブを選択します。
3. アクションバーで**［ライセンス管理者の追加］**を選択します。
4. 管理者として追加するユーザーを参照し、アクセス許可を選択します。

ライセンス管理者のアクセス許可を変更またはライセンス管理者を削除する

1. Web Studioにサインインし、左側のペインで**［ライセンス］**を選択します。
2. **［ライセンス管理者］**タブを選択し、管理者を選択します。

3. アクションバーで**ライセンス管理者編集**または**ライセンス管理者削除**のいずれかを選択します。

ライセンス管理者グループを追加する

1. Web Studioにサインインし、左ペインで**ライセンス**を選択します。
2. **ライセンス管理者**タブを選択します。
3. アクションバーで**ライセンス管理者グループの追加**を選択します。
4. ライセンス管理者として機能させたいグループを参照し、権限を選択します。Active Directoryグループを追加すると、そのグループ内のユーザーにライセンス管理者権限が付与されます。

ライセンス管理者グループの権限を変更または削除する

1. Web Studioにサインインし、左ペインで**ライセンス**を選択します。
2. **ライセンス管理者**タブを選択し、管理者グループを選択します。
3. アクションバーで**ライセンス管理者グループの編集**または**ライセンス管理者グループの削除**のいずれかを選択します。

ライセンス情報を表示する

Web Studioにサインインし、左ペインで**［ライセンス］**を選択します。サイトのライセンス使用状況と設定の概要が、指定されたライセンスサーバーに現在インストールされているすべてのライセンスのリストとともに表示されます。

製品タイプ、ライセンスエディション、ライセンスモデルを含むサイトのライセンス設定が、構成済みのライセンスサーバーが使用するライセンスと一致していることを確認してください。一致しない場合は、サイトのライセンス設定に合わせて既存のライセンスをダウンロードまたは割り当てる必要がある場合があります。

次のライセンス情報を取得するには、コマンド`Get-Brokersite`を実行します。

- TotalUniqueLicenseUsers
- PeakConcurrentLicenseUsers
- PeakConcurrentLicensedDevice

> **注:**

> Citrix DaaSで情報を取得するには、クラウドライセンスAPIを使用します。クラウドライセンスAPIの詳細については、「Citrix Cloudライセンスを管理するためのAPI」を参照してください。

ライセンス有効期限アラートを表示する

Web Studioは、Citrix License Serverからライセンスファイルの有効期限を照会します。ライセンスファイルの有効期限が近づいている場合、またはすでに期限切れになっている場合、Web Studioは概要タブで管理者に警告します。

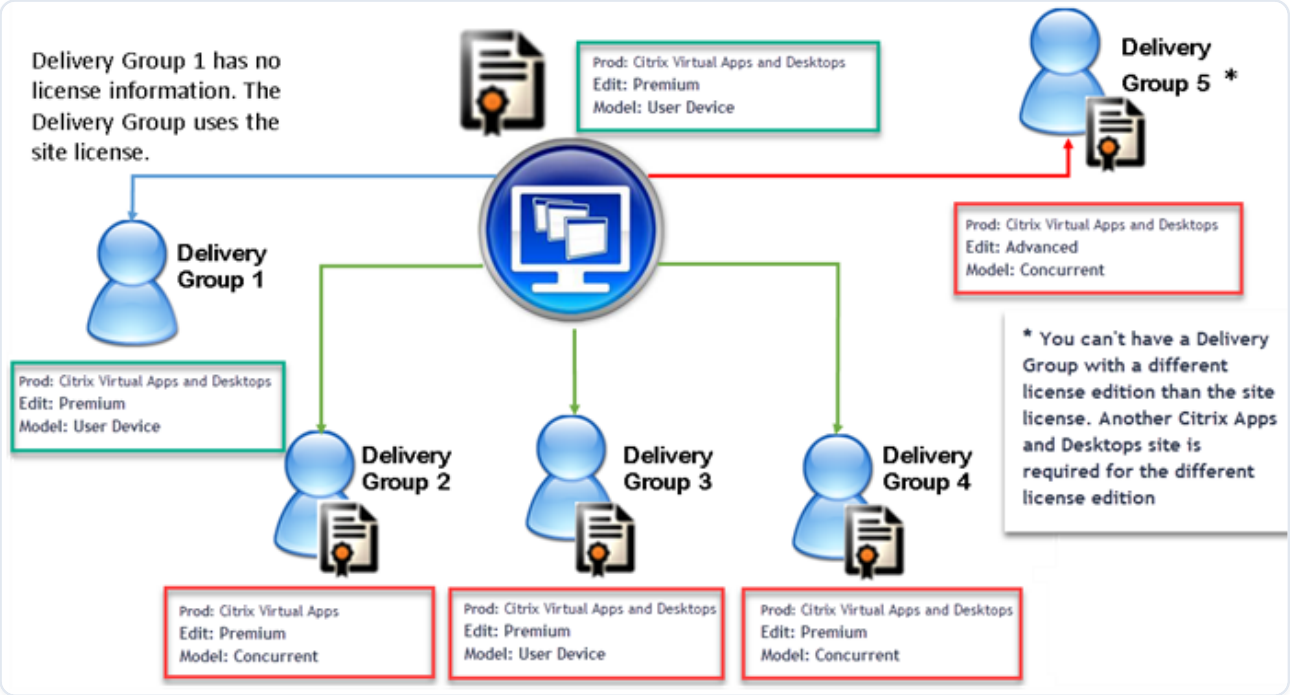
関連リンク

- 「年間および期間ベースの小売ライセンス向けCitrixオンプレミスサブスクリプション」を参照してください(/ja-jp/licensing/current-release/license-types.html#citrix-on-premises-subscription-for-annual-and-term-based-retail-licenses)。
- 「ハイブリッド権限付きの移行およびトレードアップ (TTU)」を参照してください(/ja-jp/licensing/current-release/hybrid-rights-ttu.html)。

マルチタイプライセンス

マルチタイプライセンスは、単一の Citrix Virtual Apps and Desktops サイト上のデリバリーグループに対して、異なるライセンスタイプの消費をサポートします。**タイプ**は、製品ID（XDTまたはMPS）とモデル（UserDeviceまたはConcurrent）の単一の組み合わせです。デリバリーグループは、サイトレベルで構成されているものと同じ製品エディション（PLT/PremiumまたはENT/Advanced）を使用する必要があります。Citrix Virtual Apps and Desktops の展開でマルチタイプライセンスを構成する際は、この記事の最後にある特別な考慮事項 に注意してください。

マルチタイプライセンスが構成されていない場合、異なるライセンスタイプは、個別のサイト用に構成されている場合にのみ使用できます。デリバリーグループはサイトライセンスを使用します。マルチタイプライセンスが構成されている場合の重要な通知の制限については、特別な考慮事項 を参照してください。



異なる種類のライセンスを消費するデリバリーグループを特定するには、以下の Broker PowerShell コマンドレットを使用します。

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

ライセンスをインストールするには、以下を使用します。

- シトリックス スタジオ
- シトリックス ライセンシング マネージャー
- citrix.com

Customer Success Services の日付は、各ライセンスファイル、各製品、およびモデルに固有です。異なる設定のデリバリーグループは、互いに異なる Customer Success Services の日付を持つ場合があります。

特別な考慮事項

マルチタイプライセンスは、通常のCitrix Virtual Apps and Desktops™ライセンスとは異なる機能を持ちます。

サイト構成とは異なるタイプを使用するように構成されたデリバリーグループに対して、DirectorまたはStudioからの警告や通知はありません。

- ライセンス制限に近づいたとき、またはライセンスバーストモードのトリガーや期限切れのときには情報がありません。
- 特定のグループに問題が発生した場合の通知はありません。

マルチタイプライセンス用に構成されたデリバリーグループは、そのライセンスタイプのみを消費し、全て消費されてもサイト構成にフォールバックしません。

Citrix Virtual Apps StandardとCitrix Virtual Desktops™ Standardのライセンスエディション名はどちらもStandardであることを示していますが、これらは同じエディションではありません。マルチタイプライセンスは、Citrix Virtual Apps StandardおよびCitrix Virtual Desktop Standardライセンスでは利用できません。

ライセンス互換性マトリックス

この表は、古い製品名、新しい製品名、および関連する機能名を詳述しています。4つの互換性列は、どの製品とライセンスモデルの組み合わせがマルチタイプライセンスと互換性があるかを指定します。CCUとCCSは同時接続ライセンスを表し、UDはユーザー/デバイスライセンスを表します。

Old Name	New Name	Feature	Multi-type licensing compatibility			
			STD	ADV	ENT	PLT
Citrix XenApp Standard	Citrix XenApp Standard	MPS_STD_CCU	X			
Citrix XenApp Advanced	Citrix Virtual Apps Standard	MPS_ADV_CCU		X		
Citrix XenApp Enterprise	Citrix Virtual Apps Advanced	MPS_ENT_CCU			X	
Citrix XenApp Platinum	Citrix Virtual Apps Premium	MPS_PLT_CCU				X
Citrix XenDesktop VDI Edition (XDT-U)	Citrix Virtual Desktops Standard- Per User/Device	XDT_STD_UD	X			
Citrix XenDesktop VDI Edition (XDT-C)	Citrix Virtual Desktops Standard - Concurrent	XDT_STD_CCS	X			
Citrix XenDesktop Enterprise Edition (XDT-C)	Citrix Virtual Apps and Desktops Advanced - Concurrent	XDT_ENT_CCS			X	
Citrix XenDesktop Enterprise Edition (XDT-U)	Citrix Virtual Apps and Desktops Advanced - Per User/Device	XDT_ENT_UD			X	
Citrix XenDesktop Platinum Edition (XDT-C)	Citrix Virtual Apps and Desktops Premium - Concurrent	XDT_PLT_CCS				X
Citrix XenDesktop Platinum Edition (XDT-U)	Citrix Virtual Apps and Desktops Premium - Per User/Device	XDT_PLT_UD				X

ブローカー PowerShell SDK

DesktopGroupオブジェクトには、関連するNew-BrokerDesktopGroupおよびSet-BrokerDesktopGroupコマンドレットを使用して操作できる、これらの2つのプロパティがあります。

名前	値	制限
LicenseModel	グループのライセンスモデルを指定するパラメーター (Concurrent または UserDevice)。指定されてい	機能トグルが無効になっている場合、プロパティを設定しようとすると失敗します。

名前	値	制限
	ない場合、サイト全体のライセンスモデルが使用されます。	
ProductCode	グループのライセンス製品IDを指定するXDT（Citrix Virtual Desktops用）またはMPS（Citrix Virtual Apps™用）のテキスト文字列。指定されていない場合、サイト全体の製品コードが使用されます。	機能トグルが無効になっている場合、プロパティを設定しようとすると失敗します。

LicenseModelとProductCodeの詳細については、about_Broker_Licensingを参照してください。

New-BrokerDesktopGroup

デスクトップグループの仲介を管理するためのデスクトップグループを作成します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/>`を参照してください。

Set-BrokerDesktopGroup

既存のブローカーデスクトップグループを無効または有効にするか、その設定を変更します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`を参照してください。

Get-BrokerDesktopGroup

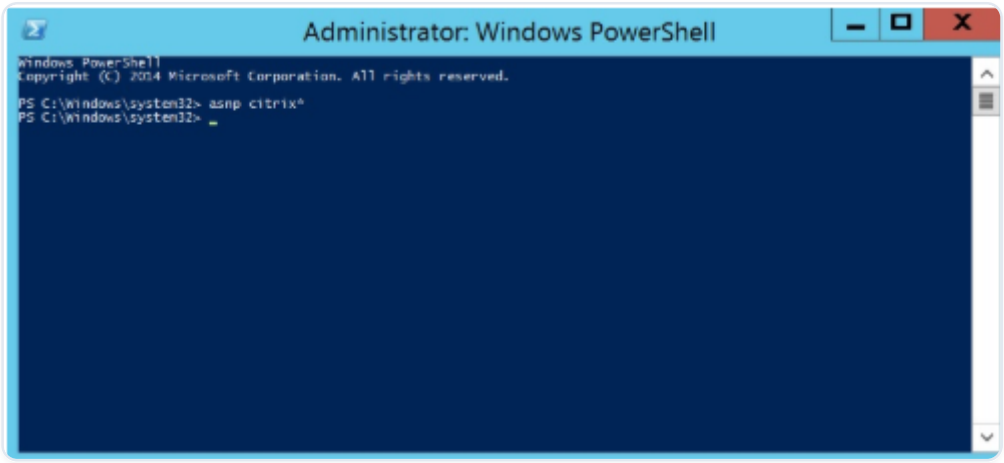
指定された条件に一致するデスクトップグループを取得します。Get-BrokerDesktopGroupコマンドレットの出力には、グループの**ProductCode**および**LicenseModel**プロパティが含まれます。New-BrokerDesktopGroupまたはSet-BrokerDesktopGroupを使用してプロパティが設定されていない場合、null値が返されます。nullの場合、サイト全体のライセンスモデルと製品コードが使用されます。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/>`を参照してください。

デリバリーグループごとに異なるライセンス製品とモデルを構成する

> **注:**

> 単一のデリバリーグループで、2つ以上の異なる種類の製品、エディション、またはライセンスモデルを構成することはできません。異なる種類の製品、エディション、またはライセンスモデルがある場合は、それらを別々のデリバリーグループで構成してください。

1. 管理者権限でPowerShellを開き、Citrixスナップインを追加します。



2. 「**Get-BrokerDesktopGroup –Name “DeliveryGroupName”**」コマンドを実行して、現在のライセンス構成を表示します。「**LicenseModel**」と「**ProductCode**」のパラメーターを見つけてください。これらのパラメーターを以前に構成していない場合、空白になっている可能性があります。

> **注:**
>
> デリバリーグループにライセンス情報が設定されていない場合、デフォルトで「**サイトレベルのサイトライセンス**」になります。
>
> PowerShellコマンド(/en-us/citrix-virtual-apps-desktops/2411/media/license-configuration-2.png)

3. コマンド「**Set-BrokerDesktopGroup –Name “DeliveryGroupName” –LicenseModel LicenseModel**」を実行して、ライセンスモデルを変更します。 PowerShellコマンド(/en-us/citrix-virtual-apps-desktops/2411/media/license-configuration-3.png)
4. コマンド「**Set-BrokerDesktopGroup –Name “DeliveryGroupName” –ProductCode ProductCode**」を実行して、ライセンス製品を変更します。 PowerShellコマンド(/en-us/citrix-virtual-apps-desktops/2411/media/license-configuration-4.png)
5. 変更を検証するには、コマンド「**Get-BrokerDesktopGroup –Name “DeliveryGroupName”**」を入力します。

> **注:**
>
> 同じサイト内でエディションを混在させることはできません。たとえば、Premiumライセンスとライセンスなどです。異なるエディションのライセンスがある場合は、複数のサイトが必要です。

> PowerShellコマンド(/en-us/citrix-virtual-apps-desktops/2411/media/license-configuration-5.png)

6. 前の手順で説明したのと同じ「**Set-BrokerDesktopGroup**」コマンドを実行し、値を「**$null**」に設定して、ライセンス構成を削除します。

> **注:**
>
> Studioでは、各デリバリーグループのライセンス構成は表示されません。現在の構成を表示するには、PowerShellを使用してください。

> PowerShellコマンド(/en-us/citrix-virtual-apps-desktops/2411/media/license-configuration-6.png)

例

このPowerShellコマンドレットの例は、既存の2つのデリバリーグループにマルチタイプライセンスを設定し、3つ目のデリバリーグループを作成して設定する方法を示しています。

デリバリーグループに関連付けられているライセンス製品とライセンスモデルを確認するには、**Get-BrokerDesktopGroup** PowerShellコマンドレットを使用します。

1. 最初のデリバリーグループをXenApp®および同時使用に設定します。

   Set-BrokerDesktopGroup -Name "シトリックス バーチャル アプリ プレミアム コンカレント 用配信グループ" -ProductCode MPS -LicenseModel Concurrent

2. 2番目のデリバリーグループをXenDesktop®および同時使用に設定します。

   Set-BrokerDesktopGroup -Name "シトリックス バーチャル デスクトップ プレミアム コンカレント 用配信グループ" -ProductCode XDT -LicenseModel Concurrent

3. 3番目のデリバリーグループをXenDesktopおよびユーザー/デバイス用に作成して設定します。

New-BrokerDesktopGroup -Name "Citrix Virtual Desktops Premium UserDevice 用デリバリーグループ" -PublishedName "マイデスクトップ" -DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

ライセンスアクティベーションサービス

ライセンスアクティベーションサービス (LAS) は、従来のCitrix®レガシーライセンスに代わる、新しいクラウドベースのライセンスソリューションです。LASはアクティベーションのための新しいモジュールを導入し、ライセンス管理へのシームレスでモダンなアプローチを保証します。

LASはCitrixライセンスのエクスペリエンスを簡素化します。ライセンスサーバーで生成、ダウンロード、またはインストールするライセンスアクセスコードやファイルはもうありません。ライセンスサーバーをアップグレードし、Citrix Cloudに登録するだけで済みます。互換性のある製品がライセンスサーバーを指すように設定されると、自動的にアクティベートされます。

アクティベーション後、ライセンスサーバーはライセンスアクティベーションサービスと定期的に通信し、アクティベーションを最新の状態に保ちます。LASはクラウドテクノロジーで構築されており、パフォーマンスを向上させ、ダウンタイムがないことを保証します。何らかの理由でライセンスサーバーまたはLASに到達できない場合、システムはライセンスキャッシュモードに入ります。これは、システムのライセンスが失われるのを防ぎ、停止を回避するように設計されています。詳細については、「ライセンスキャッシュモード」を参照してください。

LASの詳細については、ライセンスドキュメントの「ライセンスアクティベーションサービス」を参照してください。

前提条件

- ライセンスサーバーをバージョン 11.17.2 ビルド 51000 以降にインストールまたは更新します。
- ライセンスサーバー用の信頼性の高い継続的なインターネット接続。

考慮事項

- Web StudioがアクティベーションをDelivery ControllerはLASと互換性がある必要があります。単一のサイトでは、レガシーライセンスまたはLASのいずれかを使用できます。
- 同じCitrix Cloud ID (CCID) またはOrgIDに複数のライセンスサーバーを登録できます。ただし、サイトは1つのライセンスサーバーのみを指すように構成できます。

制限事項

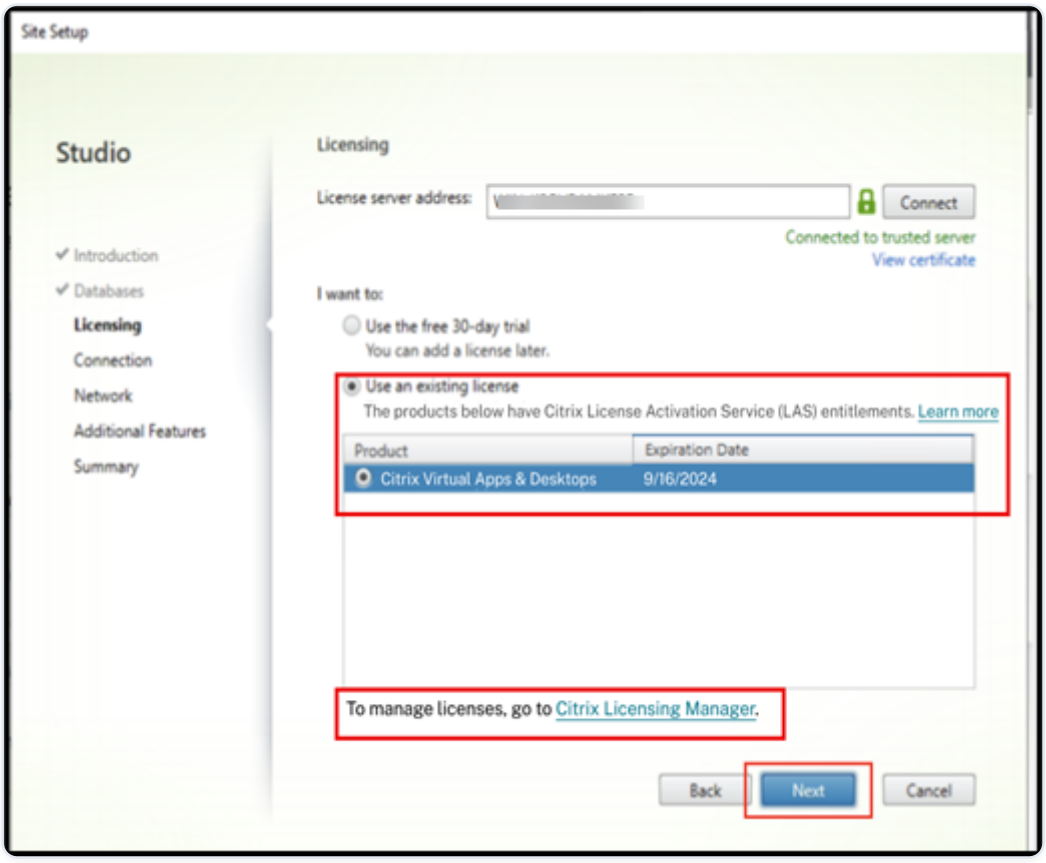
- LASへの移行により、製品エディションは**Premium**に、ライセンスモデルは**Concurrent**に設定されますが、これは将来変更される可能性があります。PowerShellを使用してライセンス構成を変更しないでください。登録とセッション起動に影響を与える可能性があります。
- Web Studioのみを使用して、既存のレガシーライセンスからLASへCitrix Virtual Apps and Desktops™サイトを移行できます。

主な手順

1. License Server をバージョン 11.17.2 ビルド 51000 以降にインストールまたはアップグレードし、License Activation Service 用の License Server の構成方法 に記載されている手順に従って LAS を構成します。
2. Citrix Virtual Apps and Desktops バージョン 2411 以降をインストールします。Citrix Delivery Controller、Citrix Studio、Web Studio、Citrix Director などのコアコンポーネントをインストールします。

   > **注：**
   >
   > Citrix Virtual Apps and Desktopsサイト内のすべてのDelivery Controllerは、LASと互換性がある必要があります。

3. 必要なコンポーネントをインストールしたら、Citrix Site Manager を使用してサイトを作成します。サイトの作成については、サイトの作成 を参照してください。License Server が LAS を使用するように構成されている場合、Metainstaller にエンタイトルメントが表示されます。エンタイトルメントは、対応するライセンスの有効期限とともに提供されます。



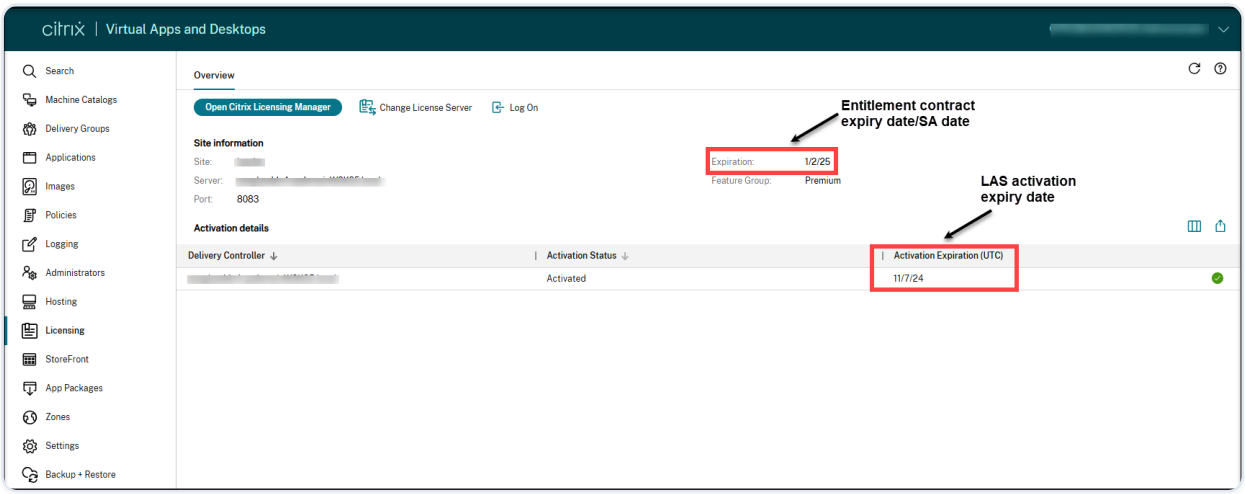
> **注：**
>
> License Serverが最新のLicense Serverバージョンにアップグレードされていない場合、エラーメッセージが表示されます。

4. ライセンスの詳細を確認する。
5. レガシーライセンスを LAS に移行する。

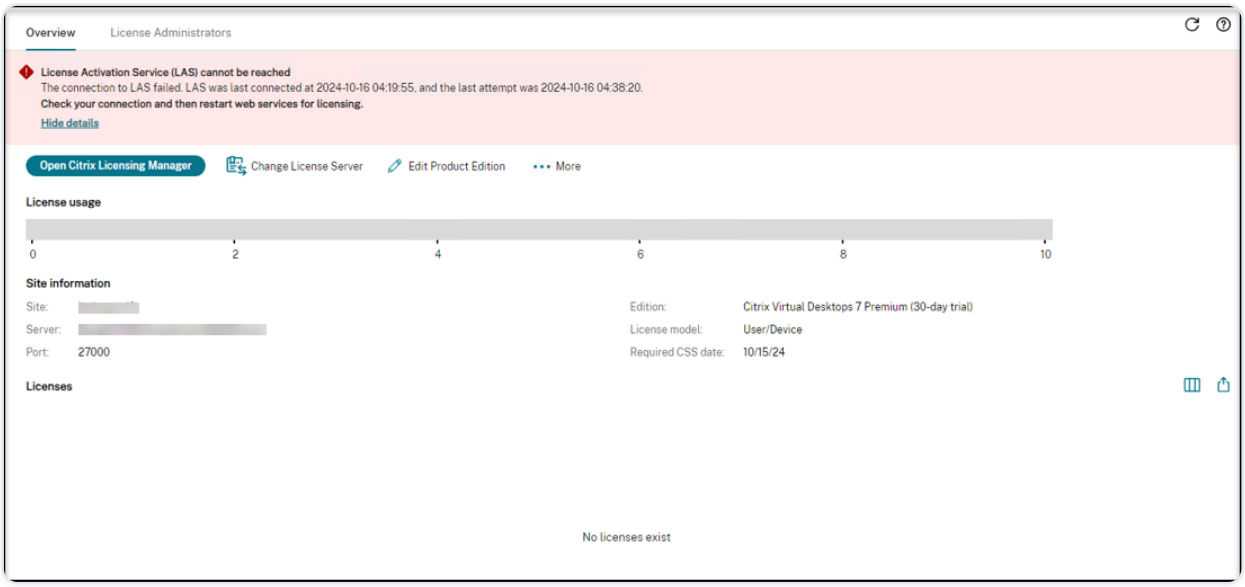
ライセンスの詳細を確認する

サイトを作成したら、Web Studio を使用してライセンスの詳細を確認します。

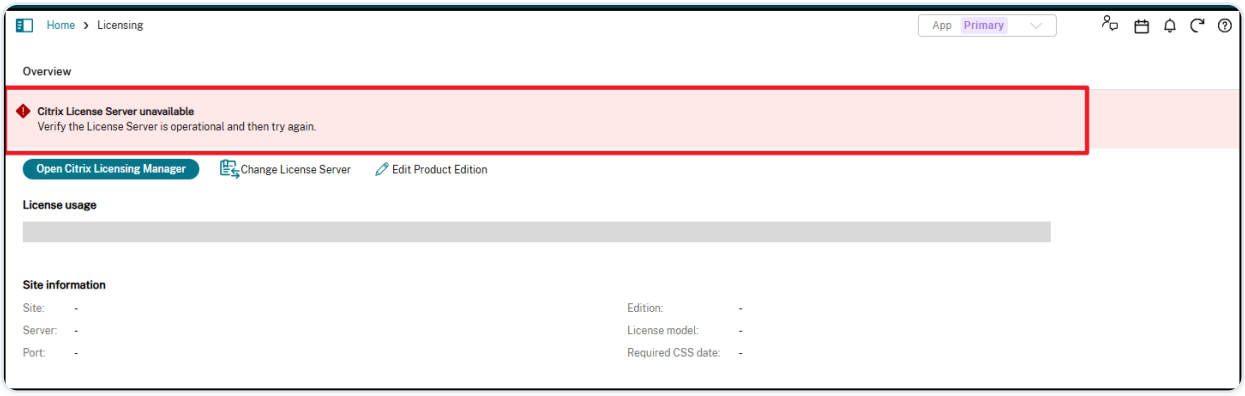
1. Web Studio で、**［ライセンス］**ノードを選択します。
2. **［概要］**タブで、Citrix Virtual Apps and Desktops サイトに適切なライセンスがあるか、または LAS 機能の使用中にライセンスの有効期限が切れていないかを確認します。



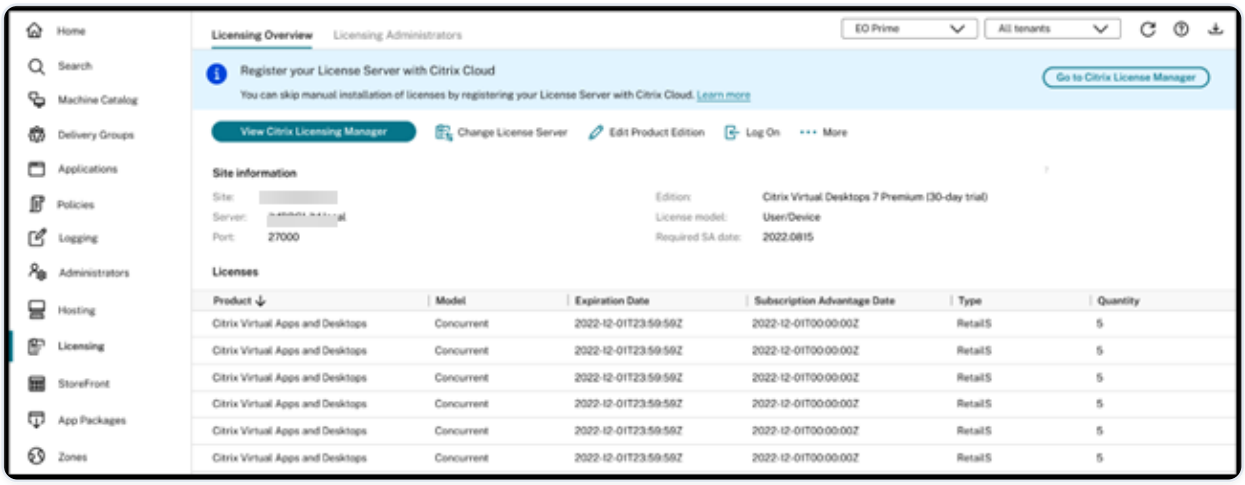
LAS に到達できない場合、エラーメッセージが表示されることがあります。



ライセンスサーバーが利用できない場合、エラーメッセージが表示されることがあります。



ライセンスサーバーが古いレガシーライセンスをまだ使用しており、Citrix Virtual Apps and Desktops サイトが LAS 対応である場合、Web Studio はライセンスサーバーを Citrix Cloud に登録するよう促します。



レガシーライセンスを LAS に移行する

ライセンスサーバーを Citrix Cloud に登録済みで、必要なエンタイトルメントがある場合は、ユーザーセッションに影響を与えることなく、既存の Citrix Virtual Apps and Desktops サイトをレガシーライセンスから LAS に移行するために、以下の特定の手順に従う必要があります。

1. **ライセンスサーバーのアップグレード:** ライセンスサーバーをサポートされている最小バージョンにアップグレードします。
2. **Delivery Controller のアップグレード:** サイト内のすべての Delivery Controller を LAS 対応バージョンにアップグレードします。
3. **デリバリーグループのライセンス割り当てを削除:**
   - **Migrate to LAS** をクリックする前に、サイトレベルより下で設定されているライセンス割り当て（つまり、デリバリーグループレベルのライセンス割り当て）を手動で削除します。
4. **割り当ての確認:** LAS の割り当てが正確であることを確認します。
5. **Migrate to LAS をクリック:**
   - 前の手順が完了したら、**Migrate to LAS** をクリックします。

     レガシーライセンスからLASに移行する(/en-us/citrix-virtual-apps-desktops/2411/media/migrate-to-las.png)
   - LASに移行すると、Citrix Virtual Apps and Desktopsサイトの**ライセンスエディション**は**Citrix Virtual Apps and Desktops Premium**に設定され、**ライセンスモデル**は**同時接続**に構成されます。

LASからレガシーライセンスへのロールバック

LASからレガシーライセンスにロールバックするには、次の手順を実行します。

1. 次のPowerShellコマンドを実行します。

```
Set-ConfigSite -UseLicenseActivationService $false
```

2. Web Studioでレガシーライセンスを構成します。

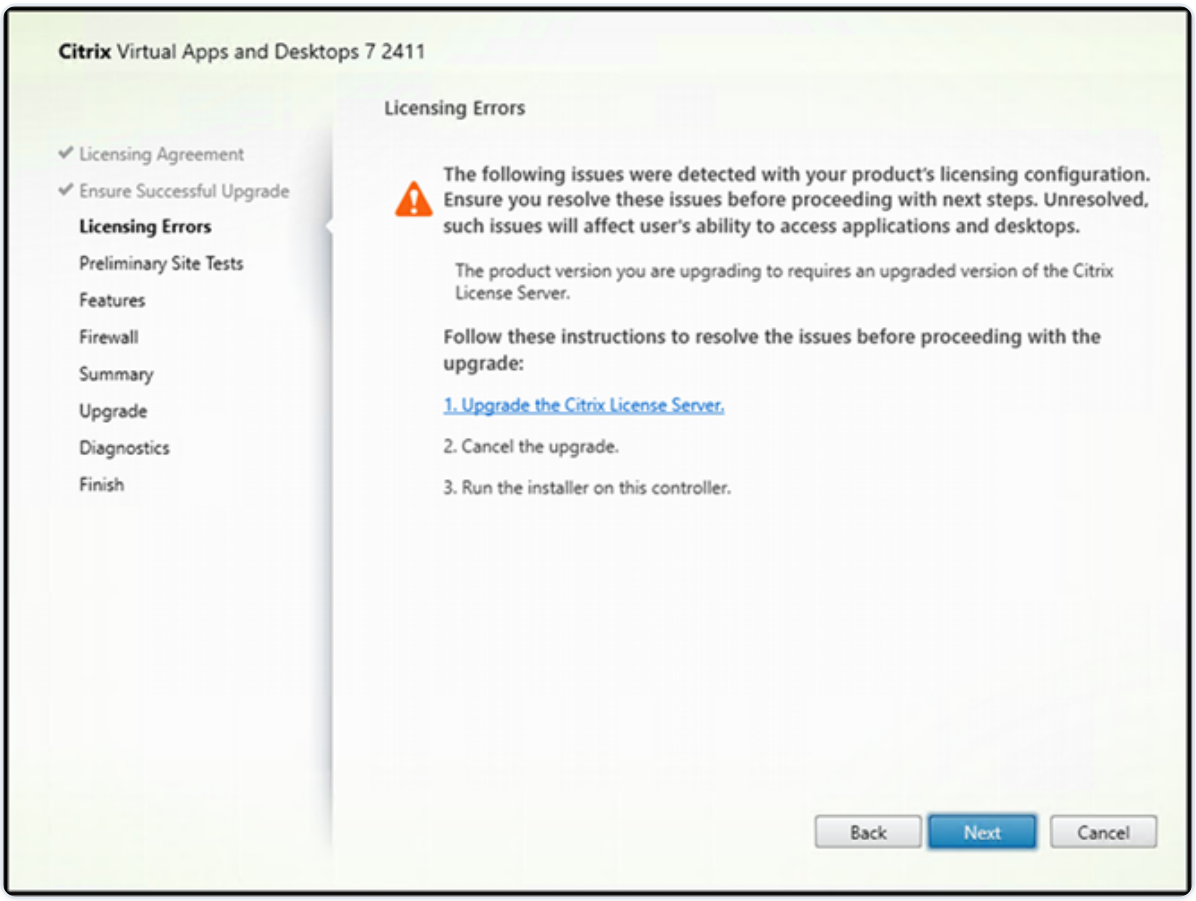
注:

これらの手順は、一時的なトラブルシューティングのみを目的としています。レガシーライセンスファイルは、End of Life (EOL) に近づいており、April 15, 2026 以降は機能しません。中断のないサービスを確保するために、License Activation Service (LAS) への移行をお勧めします。詳細については、お知らせを参照してください。

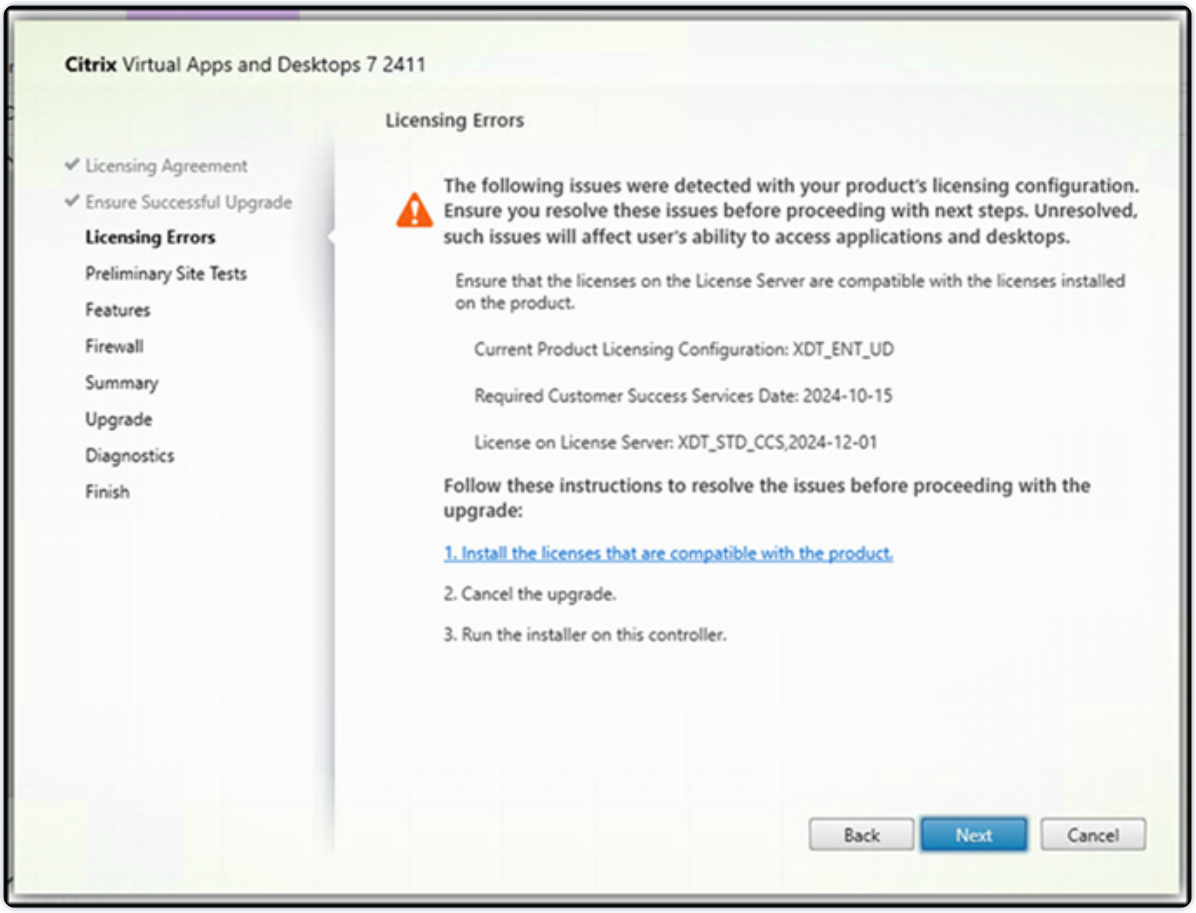
アップグレードに関する重要な考慮事項

以前のCitrix Virtual Apps and Desktopsのバージョンから2411以降にアップグレードする場合、ライセンスサーバーを最新バージョン (バージョン 11.2.17 ビルド 51000 以降) にアップグレードしてください。

- メタインストーラーUIを使用してアップグレードする際に、ライセンスエラーページに次のエラーが表示されます。
  - 最新のLicense Serverバージョンにアップグレードしない場合:



- 古いLicense Serverやライセンスの利用不可など、互換性の問題がある場合:



- コマンドラインを使用してアップグレードする場合、アップグレードの失敗を回避するために次のコマンドを実行します (マウントされたISO内の\x64フォルダーにいると仮定して)。

1. 次を実行します。

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet
   ```

   ライセンスバイナリをローカルドライブのいずれかにコピーしている場合、次のコマンドを実行します：

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet /l install.log
   ```

2. 次を実行します。

   ```
   \x64\XenDesktop Setup\XenDesktopServerSetup.exe  /components
   "CONTROLLER,DESKTOPSTUDIO,DESKTOPDIRECTOR" /CONFIGURE_FIREWALL
   ```

コアコンポーネントのアンインストール

アップグレード中に、`\x64\Licensing\CitrixLicensing.exe /quiet` または `\x64\Licensing\CitrixLicensing.exe /quiet /l install.log` コマンドを使用して最初にライセンスサーバーをインストールし、その後コアコンポーネントをインストールした場合は、アンインストールも同じ順序で行ってください。

1. コマンドラインを使用してライセンスサーバーをアンインストールします。

   ```
   CitrixLicensing.exe /quiet /uninstall /l uninstall.log
   ```

2. GUIまたはコマンドラインを使用してコンポーネントをアンインストールします。詳細については、「コンポーネントの削除」を参照してください。

コマンドライン `XenDesktopServerSetup.exe` または `removeall` を使用してライセンスサーバーとコンポーネントをアンインストールする場合は、レジストリエントリと残りのファイルをクリーンアップします。

レジストリエントリをクリーンアップするには：

1. レジストリキー `Citrix Licensing` を検索し、そのエントリを削除します。ほとんどの場合、エントリは次の場所にあります。

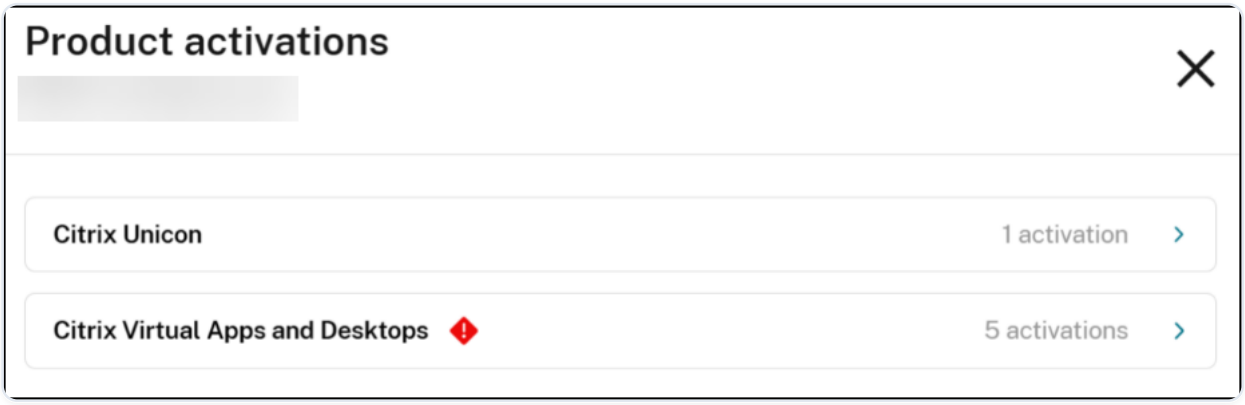
```
"Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\
```

2. レジストリキーの**Uninstall String**が指すフォルダーを削除します。

トラブルシューティング

Citrix Cloudでライセンスサーバーのステータスが緑色以外で表示されている場合は、問題が発生している可能性のあるアクティベーションの詳細を把握するために、次の手順を実行します。

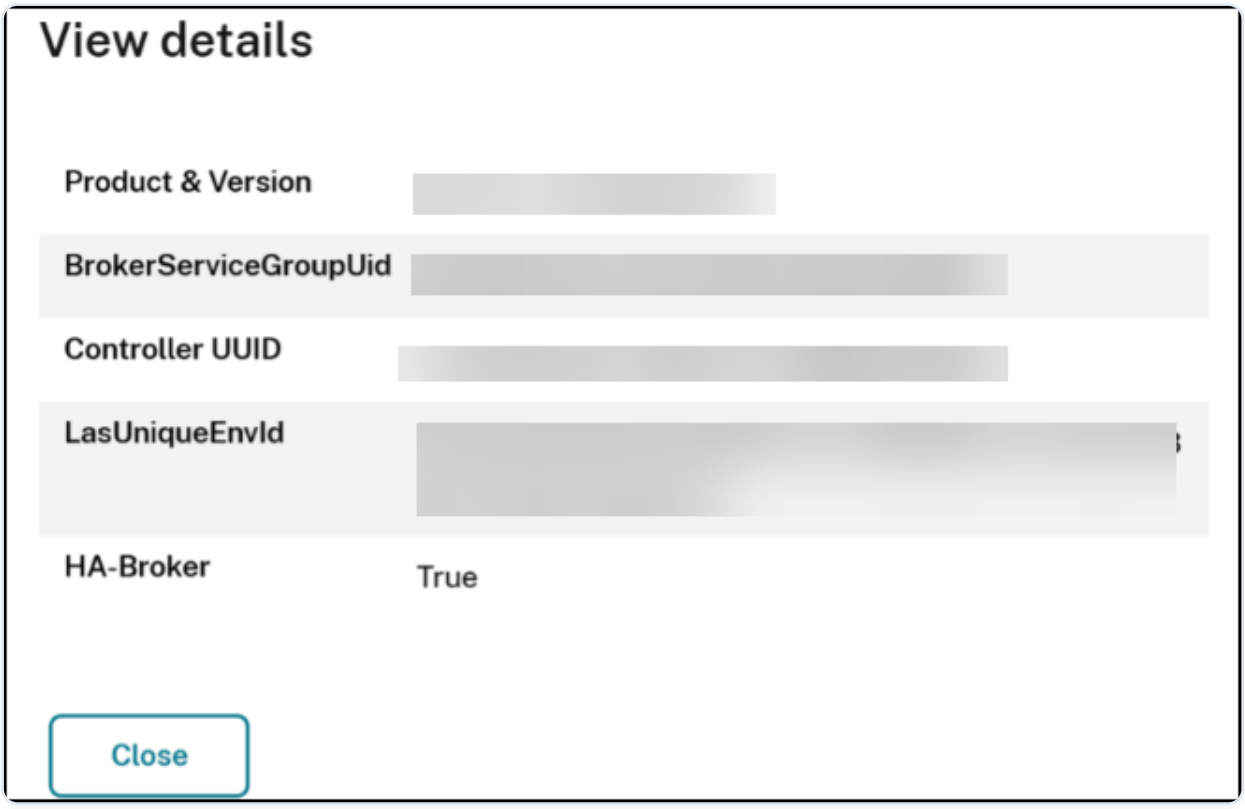
1. Citrix Cloudで、**ライセンス > ライセンス済み展開 > ライセンスサーバー** に移動します。
2. Citrix Virtual Apps and Desktops の展開ボタン **>** をクリックして、アクティブ化された Delivery Controller のリストを表示します。



3. アクティベーションの **詳細表示** をクリックして、詳細な情報を表示します。

   ID は、アクティベーションを識別するための一意の識別子です。

   以下の詳細が提供されます:



- **製品とバージョン**: LAS でアクティブ化する際に製品が使用するように構成されている Product_Edition_Model と Burn In Date。BurnInDate は通常、製品のリリース日です。
- **BrokerServiceGroupUid**: ブローカーサービスグループの UID。
- **コントローラー UUID**: デリバリーコントローラーの UUID。
- **LasUniqueEnvId**: アクティベーションのために LAS によって提供されるインスタンスの一意の ID。
- **HA-Broker**: HA ブローカーかメインブローカーかを示す True または False。

アクティブ化されたホストの詳細を実際のホストにマッピングするには、ホストで次のコマンドを実行します。

- `Get-BrokerSite`: 画面に表示される **BrokerServiceGroupUid** の値をコマンドの `BrokerServiceGroupId` 出力と比較します。
- `Get-BrokerController`: 画面に表示される **Controller UUID** の値をコマンドの UUID 出力と比較します。

ライセンスイベントに関連するイベントビューアーログ

イベントID	説明
1112	Citrix Broker Service は、ユーザーからリソースへの接続を仲介できませんでした。サイト

イベントID	説明
	の製品およびエディションのライセンス構成では、このタイプのリソースは許可されていません。このサイトに正しいライセンスが選択されていることを確認してください。
1150	Citrix Broker Service はライセンスサーバーへの接続に成功しました。
1151	Citrix Broker Service はライセンスサーバーに接続できません。ライセンスサーバーが正しく機能していること、および XenDesktop 構成でライセンスサーバーを識別する詳細が正しいことを確認してください。
1152	この XenDesktop サイトには、ライセンスサーバーに必要な製品ライセンスがありません。License Administration Console を使用して、関連する製品ライセンスをライセンスサーバーに追加してください。
1153	この XenDesktop サイトのライセンスの有効期限が切れました。Citrix Broker Service はライセンスサーバーに新しいライセンスを要求します。
1154	このコントローラーは、ライセンスサーバーに接続できなかったため、ライセンスキャッシュモードに入りました。このコントローラーがデスクトップおよびアプリケーションセッションの提供を停止するまで、残り 2 時間です。
1155	Citrix Broker Service は、デスクトップおよびアプリケーションセッションの提供を停止します。このコントローラーは、ライセンスサーバーとの通信が継続的に失敗したため、ライセンスキャッシュモードになっていないか、ライセンスキャッシュモードに入ることができませんでした。ライセンスサーバーが機能していることを確認し、必要に応じて License Administration Console を使用して、関連する

イベントID	説明
	ライセンスをライセンスサーバーに追加してください。
1156	Citrix Broker Service はライセンスサーバーと正常に通信しています。このコントローラーはライセンスキャッシュモードではなくなりました。
1157	実行中のライセンスサーバーのバージョンは、Citrix Broker Service のバージョンよりも古く、互換性がありません。ライセンスサーバーをアップグレードするか、XenDesktop の構成で正しいバージョンのライセンスサーバーの場所を指定してください。
1158	Citrix Broker Service は、このエディションのライセンスサーバーで、このサイトに利用可能なライセンス数を超過していることを検出しました。ライセンスサーバーは、オーバードラフトライセンスを付与しました。
1159	このサイトにインストールされているライセンスの最大数を超過したため、Citrix Broker Service はデスクトップ接続を拒否しました。このエディションには3つのライセンスがインストールされていますが、このエディションで許可されているライセンスの最大数は2つです。ライセンス制限に準拠するために、ライセンスサーバーから関連するライセンスを削除してください。
1160	Citrix Broker Service は、ライセンスの管理中に内部エラーを検出しました。ライセンスサーバーが正しく機能していること、および XenDesktop の構成でライセンスサーバーを識別する詳細が正しいことを確認してください。Citrix Broker Service を再起動すると、問題が解決する場合もあります。この問題が解決しない場合は、Citrix XenDesktop Controller を再インストールしてください。Citrix

イベントID	説明
	Knowledge Base の記事 CTX126990 を参照してください。
1161	ライセンスの初期化エラー。ライセンスサーバーの接続を確認してください。
1162	ライセンスの停止エラー。ライセンスサーバーの接続を確認してください。
1163	接続ライセンスがありません。解決するには、不要なセッションを閉じてライセンスを解放するか、ライセンスを追加してください。
1164	接続ライセンスのチェックアウト中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1165	接続ライセンスのチェックイン中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1166	ライセンスの可用性確認中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1167	ライセンスの開始に失敗しました。ライセンスサーバーの接続を確認してください。
1168	ライセンスユーザー通知設定の読み取り中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1169	ライセンスサーバーで適切なライセンスが見つからなかったため、このコントローラーは初期設定のライセンスキャッシュモードに入りました。このコントローラーがデスクトップおよびアプリケーションセッションの提供を停止するまで、残り2時間です。
1170	Citrix Broker Service は、ライセンスサーバー上で適切なライセンスを正常に検出しました。このコントローラーは、初期設定のライ

イベントID	説明
	センスキャッシュモードではなくなりました。
1171	ライセンスサーバーが指定されていません。有効なライセンスサーバーが指定されるまで、Citrix Broker Service はユーザーにデスクトップとアプリケーションを提供できません。Citrix Studio または Citrix PowerShell SDK コマンドレット Set-ConfigSite を使用して、ライセンスサーバーを指定できます。
1172	ライセンスサーバーの適合性チェック中にエラーが発生しました。Citrix Broker Service は、マシンがライセンスサーバーとして使用するのに適しているかどうかを確認する際に、予期しない応答を受け取りました。コントローラーからマシンに接続できること、およびマシンのファイアウォールがコントローラーからの接続を許可していることを確認してください。マシンにライセンスサーバーがインストールされている場合は、それが正しく構成され、動作していることを確認してください。
1173	この XenDesktop サイトには、ライセンスサーバーに必要な起動ライセンスがありません。License Administration Console を使用して、関連するライセンスをライセンスサーバーに追加してください。
1174	この XenDesktop サイトに構成されている製品エディションはアプリケーションをサポートしていません。アプリケーションリソースは利用できません。
1176	構成されている製品エディションはマルチセッションマシンをサポートしていません。登録は拒否されました。

イベントID	説明
1177	構成されている製品エディションはシングルセッションマシンをサポートしていません。登録は拒否されました。
1178	構成されている製品エディションはRemotePC をサポートしていません。登録は拒否されました。
1179	設定された製品エディションは、クラウドシステムにプロビジョニングされたマシンをサポートしていません。登録は拒否されました。
1180	このXenDesktopサイト用に設定された製品エディションは、シングルセッション（ワークステーションOS）マシン上のアプリケーションをサポートしていません。アプリケーションリソースの起動は拒否されました。
1181	このXenDesktopサイト用に設定された製品エディションは、マルチセッション（サーバーOS）マシン上のアプリケーションをサポートしていません。アプリケーションリソースの起動は拒否されました。
1182	このXenDesktopサイト用に設定された製品エディションは、シングルセッション（ワークステーションOS）マシン上のデスクトップをサポートしていません。デスクトップリソースの起動は拒否されました。
1183	このXenDesktopサイト用に設定された製品エディションは、マルチセッション（サーバーOS）マシン上のデスクトップをサポートしていません。デスクトップリソースの起動は拒否されました。
1196	このコントローラーは、ライセンスサーバー上の使用可能なすべてのライセンスを使い果たしたため、ライセンスバーストモードに入りました。これを解決するには、さらにライセ

イベントID	説明
	ンスを追加してください。このコントローラーがデスクトップおよびアプリケーションセッションの提供を停止するまで、残り2時間です。
1197	Citrix Broker Serviceは、デスクトップおよびアプリケーションセッションの提供を停止します。このコントローラーは、ライセンスサーバー上のライセンス不足のため、ライセンスバーストモードに入っていないか、入ることができませんでした。関連するライセンスをライセンスサーバーに追加するには、License Administration Consoleを使用してください。
1198	Citrix Broker Serviceは、ライセンスサーバーからライセンスを正常に消費しています。現在の需要を満たすのに十分なライセンスがサーバーにあります。このコントローラーは、ライセンス枯渇によるライセンスバーストモードではなくなりました。
1199	Citrix Broker Serviceは、デスクトップおよびアプリケーションセッションの提供を停止します。ライセンスサーバーにライセンスがインストールされていないため、このコントローラーはライセンスキャッシュモードではなくなったか、ライセンスキャッシュモードに入ることができませんでした。License Administration Consoleを使用して、関連するライセンスをライセンスサーバーに追加してください。
1205	ソフトウェアメンテナンスの有効期限が切れました。お使いのCitrix環境は現在サポートされていません。ライセンスサーバーで期限切れのライセンスを確認し、削除してください。ユーザーが警告メッセージを受け取り始める前に、30日間のライセンスキャッシュモードがあります。

イベントID	説明
1206	ライセンス証明書のハッシュが無効です。お使いのCitrixライセンス証明書のハッシュが無効です。
1300	Citrix Broker Serviceは、デスクトップおよびアプリケーションセッションの提供を停止します。ライセンスサーバーのシステムクロックに問題があります。
1301	ライセンスサーバーのシステムクロックに関する問題が修正されました。Citrix Broker Serviceは通常の操作を再開します。
1302	このコントローラーは、接続ライセンスのチェックインまたはチェックアウトに再度失敗しました。以前に検出された障害はまだ存在します。過剰なイベントログを避けるため、問題が解決されるまで、サービスは関連メッセージ（イベントID 1163、1164、1165）を抑制しています。ライセンス取得の試行は継続されます。
1303	このコントローラーは、関連メッセージ（イベントID 1163、1164、1165）の抑制を停止しました。
1304	Citrix Broker Service は LAS に正常に接続しました。
1305	Citrix Broker Service は LAS に接続できません。LAS が正しく機能していること、および XenDesktop 構成で LAS を識別する詳細が正しいことを確認してください。

詳細情報

サイトの LAS 状態の確認、またはサイトがライセンスキャッシュモードであるかどうかの確認については、以下を参照してください。

- サイトの LAS 状態を確認するにはどうすればよいですか？
- サイトがライセンスキャッシュモードであるかどうかを確認するにはどうすればよいですか？

コマンドの詳細については、以下を参照してください。

- Get-BrokerController
- Get-ConfigSite

Citrix Virtual Apps and Desktops™ テレメトリーデータ要素

ブローカー

使用方法

ヘッダー

キー	説明	例
バージョン	テレメトリーイベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	SendBrokerTelemetryData
st	Brokerでイベントが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
製品	使用状況イベントの発生元となる製品と展開を識別します。	XenDesktop.Broker（クラウド） OnPrem.Broker (OnPrem)
prodVer	Citrix DaaS/Citrix Virtual Apps and	7.25.0.0

キー	説明	例
	Desktopsの製品バージョンを示します。	

ペイロード

フィールド	説明	例
TotalPublishedApps	公開されているアプリケーションの総数を示します。	10
TotalPublishedDesktops	公開されているデスクトップの総数を示します。	10
VDAs.Total	VDA の総数を示します。	10
VDAs.OSTypes	Windows、Linux、Mac などの OS タイプ別の VDA の総数を示します。	10
VDAs.OSVersions	Windows 10、11、2022、2019などのOSバージョンごとの合計数を示します。	10
VDAs.HostingLocations.Azure	Azure、AWS、GCP、Nutanix、VMWare、XenServer、HyperVなどのサポートされている各ホスティングロケーションのVDAの数を示します。	10
VDAs.HostingLocations.AWS		
VDAs.HostingLocations.Nutanix		
VDAs.HostingLocations.VMWare		
VDAs.HostingLocations.XenServer		
VDAs.HostingLocations.HyperV		
VDAs.ProvisionedMethod.MCS	Machine Creation Service (MCS) によってプロビジョニ	10

フィールド	説明	例
	ングされたマシンの数を示します。	
VDAs.ProvisionedMethod.ManualOr3P	手動または3Pでプロビジョニングされたマシンの数を示します。	10
VDAs.SessionSupport.StaticSingle	静的に割り当てられたシングルセッションのマシンの数を示します。	10
VDAs.SessionSupport.DynamicSingle	動的に割り当てられたシングルセッションのマシンの数を示します。	10
VDAs.SessionSupport.Multi	マルチセッションマシンの総数を示します。	10
VDAs.RemotePCAccess.Windows	OSタイプ（Win、Mac、Linux）別のRemote PC Accessマシンの数を示します。	10
VDAs.RemotePCAccess.Linux		
VDAs.RemotePCAccess.MacOS		
VDAs.ActiveSessionRecordingAgents	アクティブなセッション記録エージェントを持つVDAの数を示します。	5
VDAs.Subscriptions	VDAのパブリッククラウドサブスクリプションの数を示します。	2
VDAs.LocationTypes	VDAのロケーションタイプの数を示します。	2
AutoScale.DGWithAutoscaleEnabled	**Autoscale** が有効になっているデリバリーグループの数を示します。	2

フィールド	説明	例
AutoScale.TotalMachinesCtrlByAutoscale	Autoscaleによって制御されるマシンの数を示します。	5
AutoScale.VerticalAutoscaleEnabledByDGandSite	DGとサイト別に**垂直オートスケール**が有効になっているマシンの数を示します。	2
AutoScale.TaggedBasedAutoscaledDG	タグベースで自動スケールされたデリバリーグループの数を示します。	2
DeliveryGroup.TotalRebootSchedulesEnabled	**再起動スケジュール**が有効になっているデリバリーグループの数を示します。	2
DeliveryGroup.Total	デリバリーグループの総数を示します。	10
Policy.TotalPolicySets	ポリシーセットの数を示します。	3
Policy.TotalPolicies	グループポリシーの数を示します。	2
Policy.TotalPolicySettings	グループ設定の数を示します。	2
PublishedPackageApps.AppVSingleAdmin	AppV Single Adminモードで公開されているパッケージアプリの総数を示します。	2
PublishedPackageApps.AppVDualAdmin	AppV Dual Adminモードで公開されているパッケージアプリの総数を示します。	2
PublishedPackageApps.Msix	MSIXモードで公開されているパッケージアプリの総数を示します。	2

フィールド	説明	例
PublishedPackageApps.AppAttach	AppAttachモードで公開されたパッケージ化されたアプリの総数を示します。	2
PublishedPackageApps.FlexApp	FlexAppモードで公開されたパッケージ化されたアプリの総数を示します。	2

セッション

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	Cloud.Licensing
st	Broker でイベントが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
製品	使用状況イベントの発生元の製品と展開を識別します。	XenDesktop.Broker (クラウド) OnPrem.Broker (OnPrem)
prodVer	Citrix DaaS または Citrix Virtual Apps	7.25.0.0

フィールド	説明	例
	and Desktops の製品バージョンを示します。	
ユーザー	セッション起動を開始するユーザーを一意に識別するためのユーザーIDを特定します。**値はスクランブル化されています。**	fullName: C648FE671A44B3F7 **(常にスクランブル化されています)** samName:C758LH671A44B3F7 **(常にスクランブル化されています)** upn: C7948FE671A44B3F7 **(常にスクランブル化されています)** userLicenseId:C265FE671A44B3F7 **(常にスクランブル化されています)** userSid: C097FE671A44B3F7 **(常にスクランブル化されています)**
テナント -> ID	Citrix Cloud™アカウントの顧客IDを示します。オンプレミス展開の場合、このフィールドは適用されず、値はありません。	ジョジイチエムゼロゴキュウハチティージェイ
デバイス -> デバイス ID	セッション起動が開始されたデバイスを一意に識別するため	AE18C4D5

フィールド	説明	例
	のデバイスIDを示します。	
デバイス -> デバイス名	デバイスのフレンドリ名を示します。**値はスクランブル化されています。**	C758LH671A44B3F7 **(常にスクランブル化されています)**

ペイロード

フィールド	説明	例
appProtectionKeyLoggingRequired	セッションがキーロギング保護を有効にして起動されたかどうかを示します。	いいえ
appProtectionScreenCaptureRequired	セッションが画面キャプチャ保護を有効にして起動されたかどうかを示します。	いいえ
cspTenantCustomerId	CSPテナントのCitrix Cloudアカウントの顧客IDを示します。オンプレミス展開の場合、このフィールドは適用されず、値はありません。	6c2vtxgxyftt
isAnonymousUser	認証されていないセッションが起動されたかどうかを示します。	いいえ
licenseActivityTimeStamp	ペイロードが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z

フィールド	説明	例
licenseActivityType	ライセンスイベントの種類を示します。このフィールドは、ライセンスイベントの種類が割り当てアクションかリリースアクションかを示します。	接続
licenseModel	展開のライセンスモデルを示します。	UserDevice
productEdition	展開の製品エディションを示します。	プレミアム
productId	展開内の製品の製品IDを示します。	CAVDS
プロトコル	セッションの起動に使用されたプロトコルを示します。	HDX™
sessionKey	セッションの一意の識別子を示します。	uq390c5fc3-86eb-4df3-bd9a-f4a8fed2c9e2
sessionSupport	セッションサポートの種類を示します。	SingleSession
sessionType	セッションの種類を示します。	アプリケーション
バージョン	ペイロードのバージョンを示します。	1.3
workerSid	セッションに使用されるVDAの一意の識別子を示します。**値はスクランブル化されています。**	1E5LH671A44B3F7 **(常にスクランブル化されています)**

フィールド	説明	例
isWindows365	セッションがWindows 365向けに起動されたかどうかを示します。	真
entitlementType	顧客のライセンスエンタイトルメントタイプを示します。	本番
siteId	サイトの一意の識別子を示します。	a35647d0-901c-4477-87e0-dcd781d455f4
desktopGroupId	デスクトップまたはデリバリーグループの一意の識別子を示します。	e9d859dc-1bfc-4b3e-bad3-41806bb4e694
clientType	Citrix Workspace™アプリのタイプを示します。	ウィンドウズ
clientVersion	Citrix Workspaceアプリのバージョンを示します。	23.5.1.83
workerCloudType	VDAプロビジョニングに使用されるパブリッククラウドの種類を示します。	アジュール
enabledFeatures	セッションで有効になっている機能を示します。たとえば、`AppProtectionScreenCaptureRequired`と`SessionRecording`が有効になっているセッションでは、こ	66

フィールド	説明	例
	のフィールドの値は 66 です。	
launchRequestSource	起動を要求するために使用される製品を記録します。オンプレミスの StoreFront™ または Cloud StoreFront のいずれかです。	0 (StoreFront または 3P) 1 (ワークスペース)
isEvents	{{page.lic}}における重大な障害を示します。	STデータベースを作成できません。
heartBeatTime	CISまたはCitrix Analytic Serviceへのライセンスサーバーのハートビート時間を示します。	1689058813
vdaTelemetry	App Layering、User Personalization Layer、User Profile management、Workspace Environment Management™、およびHDX機能のためにキャプチャされるペイロードを示します。	vdaTelemetry SessionTelemetry CPM機能: 32 HDX1: 66 HDX2: 0 MachineTelemetry AL_productVersion: 23.12.0.1001 UPL_isEnabled: 1 CPM_version: 22.3.4000

フィールド	説明	例
		wem_enableMethod: 1 wem_agentVersion: 2402.1

スタジオ

使用方法

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	8c2e20a5-ca3f-4401-ad69-d037933c40a0
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	Studio.Usage
st	Studio でイベントが生成されたときのタイムスタンプを示します。	2024-03-22T01:32:23.4056195Z
プロダクション	使用状況イベントの発生元の製品と展開を識別します。	XenDesktop.Studio
prodVer	Citrix DaaS/Citrix Virtual Apps and Desktops の製品バージョンを示します	7.42.0.0

ペイロード

フィールド	説明	例
AdminLoginList	一意の管理者 SamAccountName のリストを示します。**値はスクランブルされています。**	{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw= =]}**(常にスクランブルされています)**
TotalApiRequests	オーケストレーションサービスの API リクエストを示します。	{TotalApiRequests: 1000}
BackupCount	Studio 管理者によって操作されたバックアップの数を示します。	{BackupCount: 200}
RestoreCount	Studio 管理者によって操作された復元回数を示します。	{RestoreCount: 20}

ディレクター

使用状況レポート

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	8c2e20a5-ca3f-4401-ad69-d037933c40a0
タイプ	Citrix Analytic Serviceがクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	テレメトリ
st	Studioでイベントが生成されたときのタイムスタンプを示します。	2024-03-22T01:32:23.4056195Z

フィールド	説明	例
製品	使用状況イベントの発生元製品と展開を識別します。	XenApp.Monitor
prodVer	Directorの製品バージョンを示します。	7.42.0.0
dvcName	サーバー名	C758LH671A44B3F7

ペイロード

フィールド	説明	例
AdminLoginCount	これは、管理者のログイン数を提供するペイロードのセクションです。	タイプ: 管理者ログイン 統計 0: 1 1: 7
FeatureUsageCount	このペイロードのこのセクションには、Directorで使用されている主要な機能のカウントが含まれています。	タイプ: FeatureUsage 統計 0: 15 1: 20 5: 10
OdataUsageCount	ペイロードのこのセクションには、Odata APIの使用状況のカウントが含まれています	タイプ: OData_v3 統計 0: 1 2: 7 5: 9 タイプ: OData_v4 統計

フィールド	説明	例
		0: 1 2: 8 6: 7
AppUsage	公開されたアプリケーションの週次使用状況メトリックを示します。	タイプ: AppUsage ヘッダー: applicationName,processName,totalDurationInMinutes 期間: 01/05/24-07/05/24 値: [Calc_AWTSVDA-1907R,calc.exe,0.13, Notepad_AWTSVDA-1907R,notepad.exe,4]
UniqueAppUsers	公開されたアプリケーションについて、月間の合計アプリ起動数と一意のユーザー数を表示します。	タイプ: UniqueAppUsers ヘッダー: applicationName,totalLaunches,totalUniqueUsers 期間: 04/24 値: [Calc_AWTSVDA-1907R,100,10,

フィールド	説明	例
		Notepad_AWTSVDA-1907R,200,20]
DesktopUsage	公開デスクトップの週次使用状況メトリックを示します。	タイプ: DesktopUsage ヘッダー: desktopGroupName,sessionSupport,totalDurationInMinutes 期間: 01/05/24-07/05/24 値: [RdsDesktopAndAppGroup,1,10]
UniqueDesktopUsers	公開されたデスクトップについて、1か月間のユニークユーザー数と総起動回数を表します。	タイプ: UniqueDesktopUsers ヘッダー: desktopGroupName,totalLaunches,totalUniqueUsers 期間: 04/24 値: [RdsDesktopAndAppGroup,10,5]
AvgLogonDuration	平均ログオン期間を示します。	タイプ: AvgLogonDuration ヘッダー: totalUserLogons,

フィールド	説明	例
		avgLogonDurationInSeconds 期間: 01/05/24-07/05/24 値: [200,4]
コスト削減	顧客が1ヶ月で節約したコストを示します。	タイプ: コスト削減 ヘッダー: hypervisor,costSaved,currency 期間: 04/24 値: [1,221.02,1 2,301.02,2]

Storefront 構成

使用方法

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1.0
id	使用イベントの一意の識別子を示します。	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	CAS がクラウド使用状況イベントを識別するために使用するイベントの種類を示します。	構成

フィールド	説明	例
st	StoreFront でイベントが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
本番	使用イベントの発生元の製品と展開を識別します。	OnPrem.StoreFront
prodVer	StoreFront のバージョン (内部) を示します。	3.30.0.0

ペイロード

フィールド	説明	例
serverName	StoreFront が実行されているサービスのホスト名を示します	storefront-01.storefront.local
deploymentId	StoreFront の展開の一意の識別子を示します	f47ac10b-58cc-4372-a567-0e02b2c3d479
installedWithCVAD	StoreFrontがCVADと同時にインストールされたかどうかを示します	偽
cpuCores	CPUコアの総数を示します	4
cpuModel	StoreFrontを実行しているCPUを示します	第12世代 Intel(R) Core(TM) i7-1255U 1.70 GHz
ramGb	RAMの総容量をGB単位で示します	16
numServersInGroup	サーバーグループ内のサーバー数を示します	3
ストア	StoreFrontストア構成JSONブロブを示します。ストアオブジェクトの配列です。**一部の値はスクランブルされています**	例

フィールド	説明	例
rfWebSites	StoreFront RFWeb構成JSONブロブを示します。RFWeb構成オブジェクトの配列です。	例
ゲートウェイ	ゲートウェイ構成オブジェクトをJSONブロブとして示します。ゲートウェイオブジェクトの配列です。	例
authServices	認証サービス構成オブジェクトをJSONブロブとして示します。認証サービスオブジェクトの配列です。	例
IsPiiScrambled	はい	

フィールド STORES の例

```
[{

            "BaseUrl": "baseUrl",

            "StorePath": "/",

            "EnabledFeatures": 21 bit bitmap,

            "ResourceTypeFilteringEnabled": "disabled|
Citrix.MPS.Application;Citrix.MPS.Desktop",

            "DefaultRfWebSite": "/Citrix/StoreWeb",

            "GatewaysUsed": [

                "gatewayId"

            ],

            "VdaLogonDataProvider": "",

            "ResourceFeeds": [
```

```
                {
                    "FeedName": "<resourceFeedName>|scrambled",
                    "Type": "CVAD",
                    "LoadBalancingEnabled": true,
                }
            ],
            "AdvancedAggregation": {
                 "Enabled": true,
                 "GroupingCount": 1,
                 "ControllersPushIdenticalResources": true,
                 "LoadBalanced": true,
                 "AnyPrimaryFarms": true,
                 "AnyBackupFarms": true,
            }
}]
```

ストアが見つからない場合、それは空の配列になります 。

フィールド RFWEBSITES の例

```
[{
    "SiteId": "siteId",
    "BaseUrl": "baseUrl",
    "StorePath": "storePath",
    "UiExperienced": 0,
```

```
"EnabledFeatures": 9 bit,
"AuthMethodsEnabled": [
    "ad"
],
"CanUsersDownloadApps": {
    "Enabled": true,
    "Windows": "exe",
    "MacOS": "dmg"
},
"WorkspaceControl": {
    "Enabled": true,
    "LogoffAction": 0,
    "AutoReconnectAtLogon": true,
    "ShowReconnectButton": true,
    "ShowDisconnectButton": true
},
"MultiClickTimeout": 1,
"UiViews": [
    "apps",
    "desktops"
],
"DefaultTab": 0,
```

```
}]
```

rfWebサイトが見つからない場合、それは空の配列になります 。

フィールド GATEWAYS の例

```
[{
            "GatewayId": "gatewayId",
            "IsCloudGateway": true,
            "LoadBalancingSTAEnabled": true,
            "SessionReliabilityEnabled": true,
            "RequestTicketsFromTwoSTA": true,
            "Version": "1234",
            "LogonType": "domain",
            "SmartCardFallbackEnabled": true
}]
```

ゲートウェイが見つからない場合、それは空の配列になります 。

フィールド AUTHSERVICES の例

```
[{
    "SiteId": "SiteId",
    "Store": "StoreAuth",
    "AuthMethodsEnabled": [
        "ad"
    ],
    "PasswordChangeWhenExpired": 0,
```

```
    "PasswordRemindersForm": 1,

    "DelegateCredentialValidationToCitrix": true,

    "ValidatePasswordsOnDeliveryControllers": true

}]
```

認証サービスが見つからない場合、それは空の配列になります 。

ストアフロントログイン

使用方法

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します	1.0
ID	使用状況イベントの一意の識別子を示します	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	CAS がクラウド使用状況イベントを識別するために使用するイベントの種類を示します	ログイン
st	Broker でイベントが生成されたときのタイムスタンプを示します	2011-08-12T20:17:46.384Z
プロド	使用状況イベントの発生元となる製品と展開を識別します	OnPrem.StoreFront
prodVer	StoreFront バージョン (内部)	3.30.0.0

ペイロード

フィールド	説明	例
ユーザー	起動を開始したユーザー。**値はスクランブルされます**	fullName: C648FE671A44B3F7 **(常にスクランブルされます)** samName:C758LH671A44B3F7 **(常にスクランブルされます)** upn: C7948FE671A44B3F7 **(常にスクランブルされます)** userLicenseId:C265FE671A44B3F7 **(常にスクランブル化されます)** userSid: C097FE671A44B3F7 **(常にスクランブル化されます)**
serverName	StoreFrontが実行されているサービスのホスト名を示します	storefront-01.storefront.local
loginMethodRfWeb	ユーザーがRFWebからStoreFrontにログインするために使用した方法を示します	0
loginMethodAuth	ユーザーがAuthサービスからStoreFrontにログインするために使用した方法を示します	0

フィールド	説明	例
gatewayURL	ログイン時に使用されたNetscaler Gatewayを示します	netscaler-gateway.com
enabledFeatures	有効な機能のビットマスクを示します	12
userAgent	ログインに使用されたクライアントのUserAgentを示します	CitrixReceiver/22.11.0.19 Linux/5.17.15 X1Class CWACapable CWA/22.11.0.19
baseUrl	ユーザーがログインしたストアを示します	storefront-dev.storefront.dev
storePath	ユーザーがログインしたストアを示します	/Citirx/StoreWeb
apiUsed	クライアントがStoreまたはPNAgent APIを使用しているかどうかを示します	0
deviceId	StoreFrontへのログインに使用されたデバイスを示します。**値はスクランブルされています**	ジョン・ドウ
transactionId	単一のトランザクション中に送信/生成されるトランザクションIDを示します。	773aba9e-5b91-4ef9-8782-c4afb75698e7

委任管理

使用方法

ヘッダー

キー	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	8c2e20a5-ca3f-4401-ad69-d037933c40a0
タイプ	Citrix Analytic Serviceがクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	DelegatedAdmin.Usage
st	Delegated Adminでイベントが生成されたときのタイムスタンプを示します。	2024-03-22T01:32:23.4056195Z
製品	使用状況イベントの元の製品と展開を識別します。	XenDesktop.DelegatedAdmin (クラウド)
		OnPrem.DelegatedAdmin (OnPrem)
prodVer	Citrix DaaSまたはCitrix Virtual Apps and Desktopsの製品バージョンを示します。	7.42.0.0

ペイロード

キー	説明	例
TotalCustomScopes	カスタムスコープの総数を示します。	2
TotalCustomRoles	カスタムロールの総数を示します。	4

ライセンステレメトリデータのスクランブル

ライセンス テレメトリで送信される情報の機密性を考慮し、Citrix はデータを難読化するオプションを提供します。

次の表に、難読化できるデータを示します。

フィールド	説明	例
ユーザー	セッション起動を開始するユーザーを一意に識別するためのユーザー ID を特定します。	• fullName: `C648FE671A44B3F7` • samName: `C758LH671A44B3F7` • ユーザープリンシパル名: `C7948FE671A44B3F7` • userLicenseId: `C265FE671A44B3F7` • userSid: `C097FE671A44B3F7`
dvc を dvcName に	デバイスのフレンドリ名を示します。	`C758LH671A44B3F7`
workerSid	セッションに使用されるVDAの一意の識別子を示します。	`1E5LH671A44B3F7`
AdminLoginList	一意の管理者のSamAccountNameのリストを示します。	`{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw= =]}`

フィールド	説明	例
格納	StoreFrontストア構成JSONブロブを示します。Storeオブジェクトの配列です。**一部の値はスクランブルされています**	例
deviceId	StoreFrontへのログオンに使用されるデバイスを示します。	ジョン・ドウ

スクランブルを有効または無効にするには、Delivery Controllerで次のPowerShellコマンドを実行します。

> **注:**
>
> Citrix Service Provider™ (CSP) のお客様の場合、スクランブルは常に無効になっています。CSP のお客様は、PowerShell コマンドを使用してスクランブルを有効にすることはできません。

1. Delivery ControllerホストからPowerShellウィンドウを開きます。
2. コマンド `asnp citrix` を実行して、Citrix固有のPowerShellモジュールをロードします。
3. スクランブルを有効または無効にするには、次のコマンドを実行します。

   デフォルトでは、値は`1`または`true`であり、ライセンステレメトリデータのスクランブルを有効にします。

   無効にするには：

   ```
   Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
   -SettingValue $false
   ```

   スクランブルを無効にした後、次のコマンドを使用して有効にできます。

```
Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
-SettingValue $true
```

ライセンスに関するFAQ

注:

- COVID-19パンデミックに関連する事業継続リソースについては、CTX27055を参照してください。
- 事業継続の維持に関する一般情報については、Business continuity — on demandを参照してください。
- 現在のCitrix License Serverに関する詳細については、Licensingを参照してください。

Citrix®ライセンス

ライセンスファイルはどのように入手できますか?

ライセンスアクセスコードは電子メールで送信されます。ライセンスアクセスコードを使用してライセンスファイルを生成する方法は3つあります。

- `citrix.com`のMyAccountページにある**Manage Licenses**。詳細については、Manage licenses on citrix.comを参照してください。
- Web Studioで購入を割り当てると、ライセンスファイルがCitrix License Serverに自動的にインストールされます。
- Citrix License Server内のCitrix Licensing Managerを使用して購入を割り当て、ライセンスファイルをインストールします。詳細については、Install icensesを参照してください。

MyAccountでライセンスを割り当てる方法?

ライセンスの割り当てを参照してください。

割り当てられたライセンスをライセンスサーバーに追加する方法?

ライセンスの変更を参照してください。

Citrixライセンスはどのポートを使用しますか?

- ライセンスサーバーのポート番号は27000です。

- ベンダーデーモンのポート番号は7279です。
- ライセンス用Webサービスのポートは8083です。

Citrixライセンスサーバーとは何ですか?

Citrixライセンスサーバーは、ネットワーク全体でライセンスを共有できるシステムです。詳しくは、「ライセンス操作の概要」を参照してください。

Citrixライセンスサーバーを仮想化またはクラスター化できますか?

はい。Citrixライセンスサーバーを仮想化またはクラスター化できます。詳しくは、「クラスター化されたライセンスサーバー」を参照してください。

Citrixライセンスサーバーを仮想化すると、どのようなメリットがありますか?

Citrixライセンスサーバーを仮想化することで、冗長なソリューションが提供されます。このソリューションにより、ダウンタイムなしで複数の物理サーバー間を移動できます。

Citrixライセンスサーバーを仮想化する場合、考慮すべき制限はありますか?

いいえ。

Citrixライセンスサーバーは、Citrix Virtual Apps and Desktops™展開のすべてのライセンスを管理しますか?

Citrixライセンスサーバーは、Citrix Virtual Apps™およびDesktop用に受け取るすべてのライセンスを管理しますが、Citrix Gatewayで使用されるPremium Editionのライセンスは除きます。これらのセキュリティ指向のネットワークデバイスに必要な、ネットワークアプライアンスに組み込まれたライセンスサーバーが、それらのライセンスを管理します。

Citrix Licensing Managerとは何ですか?

Citrix Licensing Managerを使用すると、Citrix Licensing Managerをインストールしたライセンスサーバーからライセンスファイルをダウンロードして割り当てることができます。Citrix Licensing Managerは推奨されるライセンスサーバー管理方法であり、これにより以下が可能になります。

- ライセンスサーバーのCitrix Cloud™へのショートコード登録と、登録の簡単な削除。
- ユーザーアカウントとグループアカウントを構成する。
- ダッシュボードを使用して、インストール済み、使用中、期限切れ、利用可能なライセンス、およびCustomer Success Servicesの期日を表示する。
- レポート作成に使用するため、ライセンス使用状況データをエクスポートする。
- 履歴使用状況データの保持期間を構成する。デフォルトのデータ保持期間は180日です。
- ライセンスアクセスコードまたはダウンロードしたファイルを使用して、ライセンスサーバーへのライセンスファイルのインストールを簡素化する。

- ライセンスバーストモードを有効化および無効化する。
- Customer Experience Improvement Program (CEIP) およびCall Homeを構成する。
- Customer Success Servicesの更新ライセンスを自動または手動で確認し、見つかった場合は通知するか、ライセンスをインストールします。
- ライセンスサーバーの状態（起動ライセンスの不足、時間の問題、アップローダーの障害）を通知する。
- これらのポートを変更する:
  - ライセンスサーバー (デフォルト 27000)
  - ベンダーデーモン (デフォルト 7279)
  - ライセンス用Webサービス (デフォルト 8083)

詳細については、「Citrix Licensing Manager」を参照してください。

Citrix License Administration Consoleはどこにありますか?

License Administration Consoleはサポートされなくなり、License Serverバージョン11.16.6から削除されました。Citrix Licensing Managerを使用することをお勧めします。

License ServerがStudioと同じドメイン内、または信頼されたドメイン内にある場合、Studioを使用してライセンスを管理および追跡できます。

詳細については、「Citrix Licensing Manager」を参照してください。

ライセンス割り当て期間とは何ですか?

ライセンス割り当て期間とは、Citrix Virtual Apps and Desktopsライセンスがユーザーまたはデバイスに割り当てられる期間のことです。デフォルトのライセンス割り当て期間は90日です。

組織が購入したライセンスの数を確認するにはどうすればよいですか?

購入したすべてのライセンスは、`<https://www.citrix.com>`の**My Account**ページにある安全な**Manage Licenses**ツールボックスから、いつでも（24時間365日）確認およびアクセスできます。

いつでも使用中のライセンス数を確認するにはどうすればよいですか?

Citrix Licensing ManagerとStudioは、リアルタイムのライセンス使用状況に関する詳細を提供します。

License Serverのディザスターリカバリとメンテナンス

License Serverのディザスターリカバリとメンテナンスについては、Citrix LicensingドキュメントのDisaster recovery and maintenanceを参照してください。

Citrix Virtual Apps and Desktopsのライセンス

Citrix Virtual Apps and Desktopsはどのようにライセンスされますか?

シトリックス バーチャル アプリケーションズ アンド デスクトップス のライセンスは、ユーザー/デバイスライセンスモデルと同時使用ライセンスモデルを提供しています。

ユーザー/デバイス:

柔軟なユーザー/デバイスモデルは、以下と連携します。

- 企業全体のデスクトップ利用。
- 基盤となるMicrosoftデスクトップ仮想化ライセンス。
- 仮想デスクトップとアプリへのアクセスが時々しか必要ないユーザーを持つ顧客向けの同時使用ライセンス。

ユーザー/デバイスライセンスは、ユーザーが無制限のデバイスから仮想デスクトップとアプリにアクセスできるようにします。デバイスライセンスは、無制限のユーザーが単一のデバイスから仮想デスクトップとアプリにアクセスできるようにします。このアプローチにより、最大限の柔軟性が提供され、Microsoftデスクトップ仮想化ライセンスとの連携が向上します。

> **重要:**

> ライセンスをユーザーまたはデバイスに手動で割り当てることはできません。ライセンスサーバーまたはクラウドサービスがライセンスを割り当てます。ユーザー/デバイスライセンスでは、一度割り当てられたライセンスは、90日間非アクティブになるまで別のユーザーに割り当てることはできません。

> **同時使用:**

同時使用ライセンスは、任意のユーザーおよび任意のデバイスに対して、無制限の仮想アプリおよびデスクトップへの1つの接続を許可します。ライセンスはアクティブなセッション中にのみ消費されます。セッションが切断または終了した場合、ライセンスはプールに戻されます。

ユーザー/デバイスライセンスの詳細については、ユーザー/デバイスライセンス を、同時使用ライセンスについては、同時使用ライセンス を参照してください。

ライセンスを購入する前にCitrix Virtual Apps and Desktopsを試用することは可能ですか?

はい、可能です。Citrix Virtual Apps and Desktopsソフトウェアをダウンロードし、試用モードで実行できます。試用モードでは、ライセンスなしで、オンプレミスのCitrix Virtual Apps and Desktopsを30日間、10接続まで使用できます。詳細については、評価ライセンス を参照してください。

Citrix Cloud 向けのCitrix DaaS™ (旧Citrix Virtual Apps and Desktopsサービス) は、承認に基づいて試用サービスとして利用可能です。詳細については、Citrix担当者にお問い合わせください。

Citrix は Citrix Virtual Apps and Desktops の同時接続をどのように定義していますか?

Citrix Virtual Apps and Desktops の同時接続モデルでは、任意のユーザーと任意のデバイスに対して、無制限の数の仮想アプリとデスクトップへの単一の接続を許可します。ライセンスはアクティブなセッション中にのみ消費されます。セッションが切断または終了すると、ライセンスは再発行のためにプールに戻されます。詳細については、「同時接続ライセンス」を参照してください。

共通のライセンスサーバーに Citrix Virtual Apps and Desktops ライセンスの複数のエディションを展開できますか?

はい。ライセンスサーバーは、Citrix Virtual Apps と Citrix Virtual Apps and Desktops の両方のライセンスを同時に管理します。最新のライセンスサーバーバージョンをインストールすることをお勧めします。お使いのライセンスサーバーのバージョンが最新であるか不明な場合は、Citrix ダウンロードサイトの番号とバージョンを比較して確認してください。

単一のサイトで Citrix Virtual Apps と Citrix Virtual Apps and Desktops の両方のライセンスを使用できますか?

バージョンによっては、単一の Citrix Virtual Apps または Citrix Virtual Apps and Desktops サイトで、ユーザー/デバイスまたは同時接続の両方のライセンスモデルをサポートできます。単一の Citrix Virtual Apps または Citrix Virtual Apps and Desktops サイトでサポートできるエディションは 1 つだけです。詳細については、「複数タイプライセンス」を参照してください。

複数タイプライセンスをサポートする最小バージョンは、XenApp および XenDesktop 7.15 Long Term Service Release (LTSR) と Citrix Virtual Apps and Desktops 7 1808 です。

ライセンスサーバーに Citrix Virtual Apps and Desktops のユーザー/デバイスライセンスまたは Citrix Virtual Apps and Desktops の同時接続ライセンスがインストールされている場合、製品モデルとして Citrix Virtual Apps の同時接続を選択できますか?

Citrix Virtual Apps and Desktops Advanced または Premium Edition の機能として Citrix Virtual Apps を使用する場合、そのライセンスモデルは、Advanced または Premium Edition と同じです。Citrix Virtual Apps and Desktops を購入した場合、Citrix Virtual Apps の機能のみを使用する予定であっても、ライセンスは Citrix Virtual Apps and Desktops として構成してください。製品モデ

ルとして Citrix Virtual Apps を選択するのは、ライセンスサーバーにその同時接続スタンドアロンライセンスがインストールされている場合のみです。

各 Citrix Virtual Apps および Citrix Virtual Apps and Desktops エディションには、どのような製品コンポーネントが含まれていますか?

エディションごとの全機能マトリックスについては、「Citrix Virtual Apps and Desktops の機能」を参照してください。

Citrix Virtual Apps and Desktops EULA に準拠して Citrix Virtual Desktops™ 環境のライセンスを付与するにはどうすればよいですか?

Citrix Virtual Apps and Desktops EULA に準拠して、ユーザー/デバイスまたは同時接続ライセンスモデルで Citrix Virtual Apps and Desktops を展開するには、ライセンスファイルをライセンスサーバーに適用します。ライセンスサーバーは、ライセンスコンプライアンスを制御および監視します。購入した製品に基づいて製品を構成することをお勧めします。たとえば、Citrix Virtual Apps and Desktops Premium を購入したが、Citrix Virtual Apps 機能のみを使用したい場合は、コンプライアンスを満たすために製品を Citrix Virtual Apps and Desktops に構成します。詳細については、「製品ライセンスコンプライアンスセンター」を参照してください。

Citrix Virtual Apps EULA に準拠して Citrix Virtual Apps 環境のライセンスを付与するにはどうすればよいですか?

Citrix Virtual Apps EULA に準拠して同時接続ライセンスモデルで Citrix Virtual Apps を展開するには、ライセンスファイルをライセンスサーバーに適用します。ライセンスサーバーは、ライセンスコンプライアンスを制御および監視します。

Citrix Virtual Apps and Desktops サービスオプション（長期サービスリリース (LTSR) または現在のリリース (CR)）にライセンス要件はありますか?

長期サービスリリースなどの Citrix Virtual Apps and Desktops サービスオプションは、Customer Success Services プログラムの特典です。LTSR の特典を受けるには、アクティブな Customer Success Services が必要です。詳細については、「[Citrix Virtual Apps、Citrix Virtual Apps and Desktops、および XenServer サービスオプション」を参照してください。

Remote Browser Isolation (RBI) サービスのプールされた時間はどのように機能します?

サービスを最低 25 ユーザー購入すると、サービスを使用する権利として 5000 時間が付与され、すべてのユーザーで共有されます。その後のユーザー権限の購入によって、プールされた時間の資格が増えることはありません。サービス時間の資格を増やすには、アドオンパックを購入してください。

Remote PC Access を CCU ライセンスで使用できますか?

はい。

Remote PC Access については、「Remote PC Access」を参照してください。

Citrix 環境のソフトウェアメンテナンスの有効期限が切れるとどうなりますか?

ソフトウェアメンテナンス (SWM) またはサブスクリプションの有効期限が切れると、ソフトウェアアップグレードとテクニカルサポートへのアクセスが一時停止されます。また、ライセンスの種類と製品バージョンに応じて、エンドユーザーと管理者は、環境がサポートされていないことを示す特定の警告通知を受け取ります。

これらの通知は、サーバー上のすべてのライセンスの有効期限が切れている場合にのみトリガーされます。

エンドユーザーエクスペリエンス

ユーザーはセッション起動後に警告メッセージを受け取ります。メッセージには次のように表示されます。

```
Citrix Virtual Apps and Desktops warning: Your corporate Citrix
environment is currently unsupported. Please contact your IT department to
resolve.
```

管理者エクスペリエンス

管理者は、Citrix Studio コンソール内で、今後の、または現在有効な期限切れについて警告するアラートを目にします。

ライセンスの種類別の有効期限切れの動作

これらのメッセージのタイミングは、ライセンスの種類とインストールされているCitrix Virtual Apps and Desktopsのバージョンによって異なります。

オンプレミスサブスクリプションライセンス

- エンドユーザー警告: サブスクリプションの有効期限が切れた後、猶予期間中に表示されます。
- 管理者警告: サブスクリプションの有効期限が切れる30日前にStudioに表示されます。
- サポートされているバージョン:
  - 現在のリリース: Citrix Virtual Apps and Desktops 2411以降。
  - LTSR: 2203 CU6、2402 CU1、およびそれ以降のLTSRリリース

サイトのLAS状態を確認するにはどうすればよいですか?

LASアクティベーションの状態とSaaSビットのステータスを確認するには、`Get-configsite`を実行します。

Get-configsiteコマンド(/en-us/citrix-virtual-apps-desktops/2503/media/get-config-site-brk-cmnd.png)

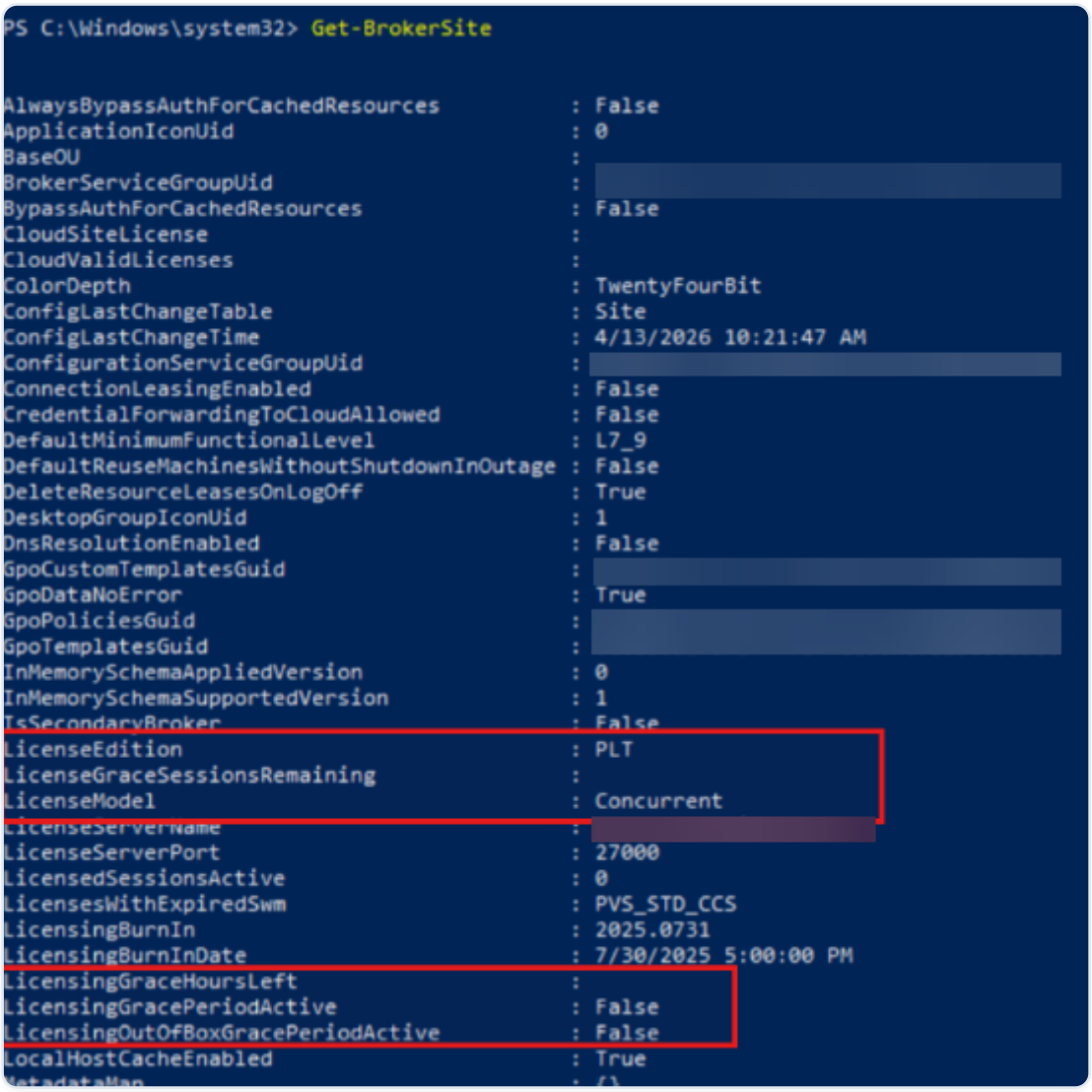
サイトがライセンスキャッシュモードになっているかどうかを確認するにはどうすればよいですか?

キャッシュモードと残り時間の詳細を取得するには、`Get-Brokercontroller`と`Get-brokersite`を実行します。

- `Get-Brokercontroller`の出力:

  Get-Brokercontrollerコマンド(/en-us/citrix-virtual-apps-desktops/2503/media/get-broker-controller-brk-cmnd.png)

- `Get-brokersite`の出力:



コマンドの詳細については、以下を参照してください。

- Get-BrokerController

- Get-ConfigSite

ライセンスに関するDelivery Controllerのイベントビューアーログについては、「ライセンスイベントに関連するイベントビューアーログ」を参照してください。

ユーザーまたはデバイスライセンス

Citrixは、ユーザー/デバイスライセンスモデルでユーザーにライセンスをどのように割り当てますか?

ユーザー/デバイスライセンスモデルでは、ライセンスサーバーは一意のユーザーIDにライセンスを割り当てます。これにより、その単一ユーザーは無制限のデバイスから無制限の接続を行うことができます。ユーザーがデスクトップまたはデバイスに接続する場合、仮想デスクトップまたはアプリケーションにアクセスするには、そのユーザーに割り当てられた1つのライセンスが必要です。ライセンスはライセンスサーバーまたはクラウドサービスによって割り当てられます。これらのライセンスを手動で割り当てることはできません。ライセンスは共有デバイスではなく、ユーザーに割り当てられます。一度ライセンスが割り当てられると、90日間の非アクティブ期間が経過するまで、別のユーザーに割り当てることはできません。詳細については、「ユーザー/デバイスライセンス」を参照してください。

Citrixは、ユーザー/デバイスライセンスモデルでライセンスデバイスをどのように定義しますか?

ライセンスデバイスには、一意のエンドポイントデバイスIDが必要です。ユーザー/デバイスモデルでは、デバイスとは、Citrix Virtual Apps and Desktopsのインスタンスにアクセスするために個人が使用を許可したあらゆる機器を指します。共有デバイスの場合、1つのCitrix Virtual Apps and Desktopsユーザー/デバイスライセンスで、デバイスを共有する複数のユーザーをサポートできます。たとえば、共有デバイスは教室のワークステーションや病院の臨床ワークステーションなどです。

シトリックス バーチャル デスクトップス スタンダード エディション の同時接続ライセンスを、ユーザー/デバイスモデルに変換することは可能ですか?

Citrix Virtual Desktops Standard Editionの同時使用ライセンスをCitrix Virtual Desktops Standard Editionのユーザー/デバイスライセンスに変換することはできません。同様に、Citrix Virtual Desktops Standard Editionのユーザー/デバイスライセンスをCitrix Virtual Desktops Standard Editionの同時使用ライセンスに変換することもできません。

Citrix Virtual Desktops Standard Editionの同時使用ライセンスをお持ちで、ユーザー/デバイスライセンスモデルをご希望の場合は、Citrix Virtual Apps and Desktops AdvancedまたはPremium Editionにアップグレードしてください。

元	STANDARD同時接続へ	STANDARDユーザー/デバイス向け	ADVANCEDユーザー/デバイス向け	PREMIUMユーザー/デバイス向け
Citrix Virtual Desktops Standard Editionの同時接続ライセンス	該当なし	同時接続からユーザー/デバイスへの変換は許可されていません	ライセンスモデルを変換することはできませんが、Citrix Virtual Apps and Desktops AdvancedまたはPremium Editionにアップグレードすることはできます。	ライセンスモデルを変換することはできませんが、Citrix Virtual Apps and Desktops AdvancedまたはPremium Editionにアップグレードすることはできます。
シトリックス バーチャル デスクトップ スタンダード エディション ユーザー/デバイス ライセンス	ユーザー/デバイスから同時接続への変換は許可されていません	該当なし	該当なし	該当なし

同時接続ライセンスとユーザー/デバイスライセンスの違い?

同時接続ライセンスは、デバイスの同時接続数に基づいています。同時接続ライセンスは、デバイスがアクティブな接続を確立している場合にのみ使用されます。接続が終了すると、同時接続ライセンスはすぐに使用できるようライセンスプールに戻されます。このライセンスモデルは、一時的な使用におすすめです。ユーザー/デバイスライセンスは一定期間リースされ、リース期間が終了するまで他のユーザーは利用できません。

ユーザー/デバイスモデル: 同じ企業内でユーザーとデバイスの両方にライセンスを割り当てられるか?

はい。両方のタイプが同じ企業内に存在できます。ライセンスサーバーは、使用状況に基づいてユーザーまたはデバイスにライセンスを最適に割り当てます。これらのライセンスを手動で割り当てることはできません。

ライセンスを付与するユーザーまたはデバイスの数をどのように決定すればよいですか?

ユースケースの要件を評価して、適切なライセンス数を決定します。ユーザー/デバイスライセンスは、無制限の数のデバイスから無制限の仮想デスクトップと仮想アプリへの無制限のアクセス

を可能にします。同時接続ライセンスは、無制限の数のユーザーが使用できる単一のデバイスから無制限の仮想デスクトップと仮想アプリへの無制限のアクセスを可能にします。次の式を考慮してください。

```
(Number of total users) – (number of users that only access exclusively

 with shared devices) + (number shared devices) = total number

 of licenses to buy.



For example, there are 1000 total users at the hospital. If 700 of them
access only

Citrix Virtual Desktops from 300 shared devices in the hospital, the
number of

licenses to purchase is 1000 – 700 + 300 = 600 licenses.
```

ユーザー/デバイスモデルでは、ライセンスを持つユーザーが自分の環境に接続するために使用できるデバイスの最大数はいくつですか?

各ライセンスユーザーは、接続されているかオフラインであるかにかかわらず、無制限のデバイスを使用できます。

ユーザー/デバイスモデルでは、ライセンスを持つデバイスにアクセスできるユーザーの最大数はいくつですか?

各ライセンスデバイスは、組織内で無制限のユーザーにサービスを提供できます。

ユーザー/デバイスモデルでは、ライセンスユーザーが一度に利用できる仮想デスクトップまたはRBI Webアプリケーションの最大数?

各ライセンスユーザーは、無制限の仮想デスクトップまたはWebアプリケーションに接続できます。

既存のCitrix Virtual Apps and Desktops環境で、ライセンスユーザー/デバイスの数を増やすためにCitrix Virtual Apps and Desktopsライセンスを購入できますか?

はい。既存のCitrix Virtual Apps and Desktops環境で、ライセンスユーザー/デバイスの数を増やすためにCitrix Virtual Apps and Desktopsライセンスを購入できます。

承認されたユーザー/デバイスライセンスを解放するにはどうすればよいですか?

承認されたユーザー/デバイスの割り当てを解放するには、EULAの条項に従って`udadmin`ユーティリティを使用します。その後、ライセンスサーバーは次の適切なユーザー/デバイスにライセンスを割り当てます。詳細については、「ユーザーまたはデバイスのライセンスの表示または解放」を参照してください。

購入したユーザー/デバイスライセンス数を超過した場合、どうなりますか?

ユーザー/デバイスライセンスには10%のオーバードラフトが含まれており、これはライセンス生成時に含まれます。オーバードラフトは、インストールされているライセンス数にも含まれます。使用量の急増がオーバードラフトを含むインストール済みライセンス数を超えた場合、追加ユーザーのアクセスは拒否されます。追加ユーザーのアクセスを有効にするには、新しいライセンスを購入して展開してください。

ライセンスオーバードラフトを含め、すべてのライセンスが使用中の場合、ライセンスバーストモードにより、製品への無制限の接続が可能になります。ライセンスバーストモードは、最大ライセンス数を超過した理由を特定し、ユーザーに中断を与えることなく追加のライセンスを購入する時間を与えます。この期間は、15日が経過するか、追加のリテールライセンスをインストールするかのいずれか早い方まで続きます。詳しくは、「ライセンスバーストモード」を参照してください。

Directorはライセンスキャッシュモードの状態を表示します。詳しくは、「Directorダッシュボードのパネル」を参照してください。

ライセンスユーザーが一度に利用できる仮想アプリケーションの最大数はいくつですか?

各ライセンスユーザーは、無制限の数の仮想アプリケーションに接続できます。

ライセンスユーザーが組織を離れた場合、どうなりますか?

既存のライセンスユーザーが組織を離れる場合、Citrixに通知することなく、そのユーザーのライセンスを解放できます。ライセンスを解放するには、`udadmin`ユーティリティを使用します。ライセンスを解放しない場合、ライセンスサーバーは90日間の非アクティブ期間の後、自動的にライセンスを解放します。この情報は、EULAに規定されている条件に従います。

ライセンスユーザーが長期間不在の場合、どうなりますか?

既存のライセンスユーザーが長期間不在の場合、Citrix に通知することなくライセンスを解放し、再割り当てできるようにすることができます。ライセンスを解放するには、`udadmin` ユーティリティを使用します。

組織内のライセンスデバイスを交換した場合、どうなりますか?

既存のライセンスデバイスを交換する場合、Citrix に通知することなくライセンスを解放し、再割り当てできるようにすることができます。ライセンスを解放するには、`udadmin` ユーティリティを使用します。

ライセンスデバイスが長期間サービス停止になった場合、どうなりますか?

既存のライセンスデバイスが長期間サービス停止になった場合、Citrixに通知することなくライセンスを解放し、再割り当てできるようにすることができます。ライセンスを解放するには、`udadmin`ユーティリティを使用します。ライセンスを解放しない場合、ライセンスサーバーは90日間の非アクティブ期間の後、自動的にライセンスを解放します。この情報は、EULAに規定されている条件に従います。

デバイスまたはユーザーにライセンスを割り当てた後で、ユーザーライセンスをデバイスライセンスに、またはその逆に切り替えることはできますか?

はい、この変更は自動的に行われます。ライセンスサーバーは、使用パターンに基づいてライセンスをユーザーまたはデバイスに割り当てます。使用パターンが変更された場合、ライセンスサーバーは新しい使用状況に基づいて割り当てを切り替えることがあります。ライセンスサーバーは常に、お客様にとって最も経済的な方法でライセンスを割り当てます。また、ライセンスサーバーは、90日間の割り当て期間が経過した後に**未使用**のライセンスを特定するためにライセンスを監視します。90日間の割り当て期間後に未使用と識別されたライセンスは、他のユーザーまたはデバイスに再割り当てできます。

同時使用ライセンス

同時使用モデルでは、Citrix Virtual Apps and Desktops のライセンスユーザーが一度に消費できる仮想デスクトップの最大数はいくつですか?

エンドポイントは多数のユーザーにサービスを提供でき、無制限の接続を許可します。

以前のバージョンの Citrix Virtual Apps and Desktops の同時使用ライセンスと、新しいユーザー/デバイスライセンスまたは同時使用ライセンスを、単一のライセンスサーバーに展開できます?

はい。同じライセンスサーバーを使用して、ユーザー/デバイスまたは同時使用ライセンスの展開をサポートし続けることができます。

単一のライセンスサーバーに、同時使用ライセンスとユーザー/デバイスライセンス、または同時使用ライセンスを展開できます?

はい。引き続き同じライセンスサーバーを使用して、同時使用ライセンスとユーザー/デバイスライセンス、または同時使用ライセンスの展開をサポートできます。

Citrix Virtual Apps and Desktops AdvancedおよびPremiumエディションには、Citrix Virtual Appsの同時使用ライセンスが含まれていますか?

Citrix Virtual Apps and Desktops AdvancedおよびPremiumのユーザー/デバイスライセンスには、互換性のためのみにCitrix Virtual Appsの同時使用ライセンスが含まれています。これらの同時使用ライセンスは、ユーザー/デバイスライセンスと互換性のない以前の製品バージョンでのみ使用できます。ユーザー/デバイスライセンスに含まれる同時使用互換ライセンスの使用は、XenApp 6.5より前のバージョンおよびXenDesktop 5.0 Service Pack 1より前のバージョンでのみ許可されます。

購入した同時使用ライセンス数を超過した場合、どうなりますか?

すべてのライセンスが使用中の場合、ライセンスバーストモードにより、製品への無制限の接続が可能になります。ライセンスバーストモードは、最大ライセンス数を超過した理由を特定し、ユーザーを中断することなく追加のライセンスを購入するための時間を提供します。この期間は、15日が経過するか、追加のリテールライセンスをインストールするかのいずれか早い方まで継続します。詳細については、「ライセンスバーストモード」を参照してください。

Directorは猶予期間の状態を表示します。詳細については、「Directorダッシュボードのパネル」を参照してください。

超過ライセンス

オーバードラフトライセンスはどのように入手できますか?

ユーザー/デバイス、ユーザー、またはデバイスライセンスモデルをサポートする製品（Citrix Cloudを除く）には、アクセス拒否を防ぐために限られた数の追加ライセンスを使用できるようにするライセンスオーバードラフト機能が含まれています。オーバードラフト機能は、ライセンスの権利ではなく、便宜のために提供されます。同時使用ライセンスおよびサーバーライセンスにはオーバードラフトは含まれません。使用されたオーバードラフトライセンスは、初回使用から30日以内に購入する必要がありますが、使用期間は30日に限定されません。Citrixは、新しい製品リリースでオーバードラフト機能を削除する権利を留保します。詳細については、「ライセンスオーバードラフト」を参照してください。

ライセンス超過をどのように識別できますか?

Citrix Licensing Managerで、超過しているライセンス数を含む使用状況情報を表示できます。Studioにも超過使用状況情報が含まれています。

超過ライセンスが消費されるとどうなりますか?

Citrix Virtual Apps and Desktops環境へのアクセスを有効にするために、インストールされているライセンスからライセンスが割り当てられます。この超過ライセンスは、他のライセンスと同等のアクセスと機能を提供します。

超過ライセンスが消費されたときにアラートを受け取ることはできますか?

現在、オーバードラフトライセンスが消費されたときに提供される特定の警告はありません。

オーバードラフトライセンスはどのくらいの期間消費できます?

最初に使用してから30日以内に使用されたオーバードラフトライセンスを購入してください。

オーバードラフトライセンスはどのくらいの期間消費できます?

最初に使用してから30日以内に使用されたオーバードラフトライセンスを購入してください。

その他の製品固有のライセンス情報

- シトリックス ADC
- シトリックス クラウド
- シトリックス エンドポイント マネジメント
- シトリックス ゲートウェイ
- XenServer
- シトリックス ライセンシング

ローカルホストキャッシュ

Citrix Virtual Apps and Desktopsサイトデータベースが常に利用可能であることを保証するため、Citrixは、Microsoftの可用性の高いベストプラクティスに従って、フォールトトレラントなSQL Server展開から開始することを推奨します。(サポートされているSQL Serverの高可用性機能については、「データベース」を参照してください。)しかし、ネットワークの問題や中断により、ユーザーがアプリケーションやデスクトップに接続できなくなる可能性があります。

ローカルホストキャッシュ機能により、障害発生時にサイトでの接続仲介操作を継続できます。障害は、オンプレミスのCitrix®環境でDelivery Controller™とサイトデータベース間の接続が失敗したときに発生します。サイトデータベースに90秒間アクセスできない場合、ローカルホストキャッシュが作動します。

XenAppおよびXenDesktop 7.16以降、接続リース機能（以前のリリースにおける先行の高可用性機能）は製品から削除され、利用できなくなりました。

データコンテンツ

ローカルホストキャッシュには、メインデータベースの情報の一部である以下の情報が含まれます。

- サイトから公開されたリソースへの権限が割り当てられているユーザーおよびグループのID。

- サイトから公開されたリソースを現在使用している、または最近使用したユーザーのID。
- サイトで構成されているVDAマシン（リモートPCアクセス マシンを含む）のID。
- 公開リソースへの接続に積極的に使用されているクライアントCitrix Receiver™マシンのID（名前とIPアドレス）。

また、メインデータベースが利用できなかった間に確立された、現在アクティブな接続に関する情報も含まれます。

- Citrix Receiverによって実行されたクライアントマシンのエンドポイント分析の結果。
- サイトに関与しているインフラストラクチャマシン（NetScaler GatewayやStoreFront™サーバーなど）のID。
- ユーザーによる最近のアクティビティの日付、時刻、種類。

仕組み

以下の図は、通常の操作におけるローカルホストキャッシュのコンポーネントと通信パスを示しています。

通常の操作におけるローカルホストキャッシュの通信パスの図(/en-us/citrix-virtual-apps-desktops/2411/media/lhc-normal1.png)

通常の操作時

- Controller上の *プリンシパルブローカー* (Citrix Broker Service) は、StoreFrontからの接続要求を受け入れます。ブローカーはサイトデータベースと通信し、ユーザーをControllerに登録されているVDAに接続します。
- Citrix Config Synchronizer Service (CSS) は、約5分ごとにブローカーに問い合わせて、変更が行われたかどうかを確認します。これらの変更は、管理者によって開始されたもの（デリバリーグループのプロパティの変更など）またはシステムアクション（マシン割り当てなど）である可能性があります。
- 前回のチェック以降に構成変更があった場合、CSSは情報をController上のセカンダリーブローカーに同期（コピー）します。（セカンダリーブローカーはHigh Availability Serviceとも呼ばれます。）

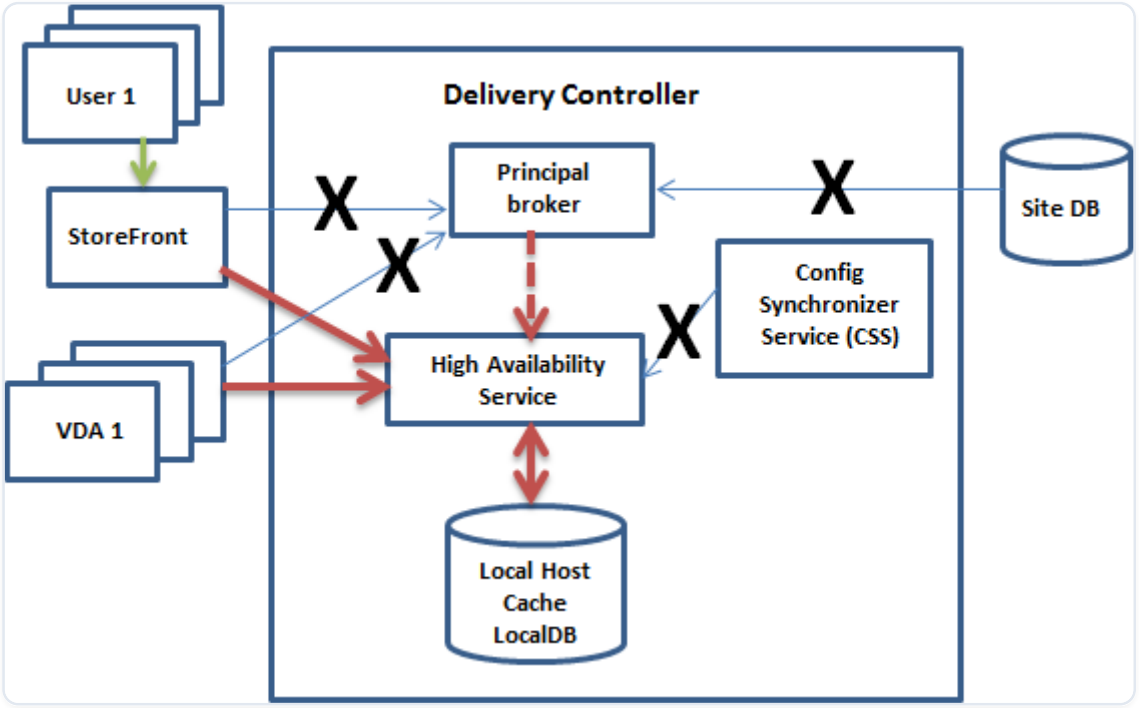
  前回のチェック以降に変更された項目だけでなく、すべての構成データがコピーされます。CSSは構成データをController上のMicrosoft SQL Server Express LocalDBデータベースにインポートします。このデータベースはローカルホストキャッシュデータベースと呼ばれます。CSSは、ローカルホストキャッシュデータベースの情報がサイトデータベースの情報と一致し

ていることを保証します。ローカルホストキャッシュデータベースは、同期が行われるたびに再作成されます。

Microsoft SQL Server Express LocalDB（ローカルホストキャッシュデータベースで使用）は、Controllerをインストールする際に自動的にインストールされます。（コマンドラインからControllerをインストールする際に、このインストールを禁止できます。）ローカルホストキャッシュデータベースは、複数のController間で共有することはできません。ローカルホストキャッシュデータベースをバックアップする必要はありません。構成変更が検出されるたびに再作成されます。

- 前回のチェック以降に変更がない場合、データはコピーされません。

以下の図は、プリンシパルブローカーがサイトデータベースとの接続を失った場合（停止が始まった場合）の通信パスの変化を示しています。



停止中

停止が始まった場合：

- セカンダリーブローカーは接続要求のリッスンと処理を開始します。
- 停止が始まると、セカンダリーブローカーは最新のVDA登録データを持っていませんが、VDAがセカンダリーブローカーと通信すると、登録プロセスがトリガーされます。そのプロセス中に、セカンダリーブローカーはそのVDAに関する現在のセッション情報も取得します。
- セカンダリブローカーが接続を処理している間、ブローカリングプリンシパルは接続の監視を続けます。接続が復元されると、ブローカリングプリンシパルはセカンダリブローカーに接続情報のリスニングを停止するよう指示し、ブローカリングプリンシパルはブローカリング操作

を再開します。VDAが次にブローカリングプリンシパルと通信するときに、登録プロセスがトリガーされます。セカンダリブローカーは、以前の停止から残っているVDA登録をすべて削除します。CSSは、展開で構成変更が発生したことを認識すると、情報の同期を再開します。

同期中に停止が発生するという万が一の事態では、現在のインポートは破棄され、最後に認識された構成が使用されます。

イベントログは、同期と停止に関する情報を提供します。

停止モードでの運用に時間制限はありません。

通常モードと停止モード間の移行は、既存のセッションには影響しません。新しいセッションの起動のみに影響します。

意図的に停止をトリガーすることもできます。その理由と方法の詳細については、「停止の強制」を参照してください。

複数のControllerがあるサイト

CSSは、その他のタスクの中でも、ゾーン内のすべてのコントローラーに関する情報をセカンダリブローカーに定期的に提供します。（展開に複数のゾーンが含まれていない場合、このアクションはサイト内のすべてのコントローラーに影響します。）その情報を持つことで、各セカンダリブローカーは、ゾーン内の他のコントローラーで実行されているすべてのピアセカンダリブローカーについて知っています。

セカンダリブローカーは、別のチャネルで相互に通信します。これらのブローカーは、実行されているマシンのFQDN名のアルファベット順リストを使用して、停止が発生した場合にゾーンでブローカー操作を行うセカンダリブローカーを決定（選出）します。停止中、すべてのVDAは選出されたセカンダリブローカーに登録します。ゾーン内の選出されていないセカンダリブローカーは、受信接続およびVDA登録要求を積極的に拒否します。

停止中に選出されたセカンダリブローカーが失敗した場合、別のセカンダリブローカーが引き継ぐために選出され、VDAは新しく選出されたセカンダリブローカーに登録します。

停止中にControllerが再起動された場合：

- そのコントローラーが選出されたブローカーでない場合、再起動は影響しません。
- そのコントローラーが選出されたブローカーである場合、別のコントローラーが選出され、VDAが登録されます。再起動されたコントローラーが電源オンになった後、自動的にブローカリングを引き継ぎ、これによりVDAが再度登録されます。このシナリオでは、登録中にパフォーマンスが影響を受ける可能性があります。

通常の操作中にControllerの電源をオフにし、停止中に電源をオンにした場合、そのControllerがブローカーとして選出されても、そのControllerではローカルホストキャッシュを使用できません。

イベントログは、選出に関する情報を提供します。

停止中に利用できないもの、およびその他の違い

停止モードでの運用に時間制限はありません。ただし、Citrixは可能な限り迅速に接続を復元することを推奨しています。

停止中：

- Studioを使用できません。
- PowerShell SDKへのアクセスは制限されます。
    - まず、次の操作を行う必要があります。
        - 値が1のレジストリキー `EnableCssTestMode` を追加します: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
        - ポート89を使用します: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ControllerDNSName, DesktopGroupName, RegistrationState`
    - これらのコマンドを実行すると、以下にアクセスできます。
        - すべての `Get-Broker*` コマンドレット。
- ハイパーバイザーの資格情報はホストサービスから取得できません。すべてのマシンは不明な電源状態になり、電源操作は発行できません。ただし、ホスト上で電源が入っているVMは接続要求に使用できます。
- 割り当てられたマシンは、通常の操作中に割り当てが行われた場合にのみ使用できます。停止中に新しい割り当てを行うことはできません。
- リモートPCアクセス マシンの自動登録と構成はできません。ただし、通常の操作中に登録および構成されたマシンは使用可能です。
- リソースが異なるゾーンにある場合、サーバーでホストされているアプリケーションおよびデスクトップのユーザーは、構成されたセッション制限よりも多くのセッションを使用する可能性があります。
- ユーザーは、現在アクティブ/選出されているセカンダリブローカーを含むゾーン内の登録済みVDAからのみアプリケーションとデスクトップを起動できます。ゾーンをまたぐ起動（ある

ゾーンのセカンダリブローカーから別のゾーンのVDAへの起動）は、停止中はサポートされません。

- デリバリーグループ内のVDAのスケジュールされた再起動が開始される前にサイトデータベースの停止が発生した場合、停止が終了したときに再起動が開始されます。これは予期しない結果を招く可能性があります。詳細については、「データベース停止によるスケジュールされた再起動の遅延」を参照してください。
- ゾーンの優先順位は構成できません。構成されている場合、セッション起動時に優先順位は考慮されません。
- タグがゾーンの指定に使用されるタグ制限は、セッション起動ではサポートされていません。このようなタグ制限が構成され、StoreFrontストアの高度なヘルスチェックオプションが有効になっている場合、セッションが断続的に起動に失敗する可能性があります。

アプリケーションとデスクトップのサポート

LHCは、次の種類のVDAと配信モデルをサポートしています。

VDAタイプ	配信モデル	LHCイベント中のVDAの可用性
マルチセッションOS	アプリケーションとデスクトップ	常に利用可能。
シングルセッションOS静的（割り当て済み）	デスクトップ	常に利用可能。
電源管理されたシングルセッションOSランダム（プール）	デスクトップ	デフォルトでは利用できません。プールされたデリバリーグループ内の電源管理されたVDAへのすべてのセッション起動試行は、デフォルトで失敗します。LHCイベント中に新しい接続で利用できるようにすることができます。詳細については、Web Studioを使用した有

VDAタイプ	配信モデル	LHCイベント中のVDAの可用性	
		効化 および PowerShellを使用した有効化 を参照してください。 **重要:** 電源管理されたシングルセッションのプールされたマシンへのアクセスを有効にすると、以前のユーザーセッションからのデータや変更が後続のセッションに存在する可能性があります。	

注:

プールされたデリバリーグループ内の電源管理されたデスクトップVDAへのアクセスを有効にしても、通常の操作中に構成された`ShutdownDesktopsAfterUse`プロパティの動作には影響しません。LHC中にこれらのデスクトップへのアクセスが有効になっている場合、LHCイベントが完了してもVDAは自動的に再起動しません。プールされたデリバリーグループ内の電源管理されたデスクトップVDAは、VDAが再起動するまで以前のセッションからのデータを保持できます。VDAの再起動は、非LHC操作中にユーザーがVDAからログオフした場合、または管理者がVDAを再起動した場合に発生する可能性があります。

Web Studioを使用して、電源管理されたシングルセッションOSプールVDAのLHCを有効にする

Web Studioを使用して、LHCイベント中にデリバリーグループごとに新しい接続でこれらのマシンを利用できるようにすることができます。

- デリバリーグループの作成中にこの機能を有効にするには、デリバリーグループの作成 を参照してください。

- 既存のデリバリーグループでこの機能を有効にするには、デリバリーグループの管理 を参照してください。

> **注:**
>
> この設定は、電源管理されたVDAを提供するプールされたデスクトップデリバリーグループに対してのみ、Web Studioで利用できます。

PowerShellを使用して、電源管理されたシングルセッションOSのプールされたVDAでLHCを有効にする

特定のデリバリーグループ内のVDAでLHCを有効にするには、次の手順に従います。

1. このコマンドを実行して、サイトレベルでこの機能を有効にします。

   ```
   Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
   ```

2. デリバリーグループ名を指定してこのコマンドを実行し、デリバリーグループのLHCを有効にします。

   ```
   Set-BrokerDesktopGroup -Name "name" -ReuseMachinesWithoutShutdownInOutage $true
   ```

新しく作成された電源管理VDAを持つプール型デリバリーグループのデフォルトのLHC可用性を変更するには、次のコマンドを実行します。

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

RAM サイズに関する考慮事項

LocalDBサービスは約1.2 GBのRAMを使用できます（データベースキャッシュに最大1 GB、SQL Server Express LocalDBの実行に200 MB）。セカンダリブローカーは、多数のログオンが発生する長時間の停止（たとえば、10Kユーザーで12時間）が発生した場合、最大1 GBのRAMを使用できます。これらのメモリ要件は、コントローラーの通常のRAM要件に追加されるため、RAM容量の合計を増やす必要がある場合があります。

サイトデータベースにSQL Server Expressインストールを使用している場合、サーバーには2つのsqlserver.exeプロセスがあります。

CPU コアとソケット構成に関する考慮事項

コントローラーのCPU構成、特にSQL Server Express LocalDBで利用可能なコア数は、メモリ割り当てよりもさらに、ローカルホストキャッシュのパフォーマンスに直接影響します。このCPUオーバーヘッドは、データベースに到達できず、セカンダリブローカーがアクティブな障害期間中にのみ観測されます。

LocalDBは複数のコア（最大4つ）を使用できますが、単一のソケットに制限されています。ソケットを追加してもパフォーマンスは向上しません（たとえば、各ソケットに1コアを持つ4つのソケット）。代わりに、Citrixは複数のコアを持つ複数のソケットを使用することを推奨しています。Citrixのテストでは、2x3（2ソケット、3コア）構成が4x1および6x1構成よりも優れたパフォーマンスを提供しました。

ストレージに関する考慮事項

ユーザーが障害中にリソースにアクセスすると、LocalDBは増大します。たとえば、1秒あたり10回のログオンで実行されるログオン/ログオフテスト中に、データベースは2〜3分ごとに1MB増加しました。通常の操作が再開されると、ローカルデータベースは再作成され、領域は解放されます。ただし、障害発生時のデータベースの増大に対応できるよう、LocalDBがインストールされているドライブには十分な空き領域が必要です。ローカルホストキャッシュは、障害発生時により多くのI/Oも発生させます。具体的には、1秒あたり約3MBの書き込みと、数十万回の読み取りが発生します。

パフォーマンスに関する考慮事項

障害発生時には、1つのセカンダリブローカーがすべての接続を処理します。そのため、通常の操作中に複数のController間で負荷分散を行うサイト（またはゾーン）では、選出されたセカンダリブローカーが障害発生時に通常よりもはるかに多くの要求を処理する必要がある場合があります。したがって、CPUの要求は高くなります。障害発生時に選出されるセカンダリブローカーは変更される可能性があるため、サイト（ゾーン）内のすべてのセカンダリブローカーは、ローカルホストキャッシュデータベースと影響を受けるすべてのVDAによって課される追加の負荷を処理できる必要があります。

VDIの制限事項:

- シングルゾーンVDI展開では、障害発生時に最大10,000台のVDAを効果的に処理できます。
- マルチゾーンVDI展開では、障害発生時に各ゾーンで最大10,000台のVDAを効果的に処理でき、サイト全体では最大40,000台のVDAを処理できます。たとえば、以下の各サイトは障害発生時に効果的に処理できます。
    - 4つのゾーンがあり、それぞれに10,000台のVDAが含まれるサイト。

    - 7つのゾーンがあり、1つのゾーンに10,000台のVDA、残りの6つのゾーンにそれぞれ5,000台のVDAが含まれるサイト。

障害発生時には、サイト内の負荷管理が影響を受ける可能性があります。負荷評価機能（特にセッション数ルール）が超過する可能性があります。

すべてのVDAがセカンダリブローカーに登録されるまでの間、そのサービスは現在のセッションに関する完全な情報を持っていない可能性があります。そのため、その期間中のユーザー接続要求は、既存のセッションへの再接続が可能であったとしても、新しいセッションが起動される結果となる可能性があります。この間隔（「新しい」セカンダリブローカーが再登録中にすべてのVDAからセッション情報を取得する間）は避けられません。障害発生時に接続されているセッションは、移行期間中に影響を受けませんが、新しいセッションやセッションの再接続は影響を受ける可能性があります。

この間隔は、VDAが登録する必要がある場合に発生します。

- 障害の開始時: プリンシパルブローカーからセカンダリブローカーに移行する場合。
- 障害発生中のセカンダリブローカーの障害: 障害が発生したセカンダリブローカーから新しく選出されたセカンダリブローカーに移行する場合。
- 障害からの復旧時: 通常の操作が再開され、プリンシパルブローカーが制御を再開する場合。

Citrix Broker Protocolの`HeartbeatPeriodMs`レジストリ値（デフォルト = 600000 ms、つまり10分）を下げることで、間隔を短縮できます。このハートビート値は、VDAがpingに使用する間隔の2倍であるため、デフォルト値では5分ごとにpingが実行されます。

例えば、次のコマンドはハートビートを5分（300000ミリ秒）に変更し、2.5分ごとにpingが実行されるようにします。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name HeartbeatPeriodMs -PropertyType DWORD –Value 300000
```

ハートビート値を変更する際は注意してください。頻度を上げると、通常モードと障害モードの両方でControllerへの負荷が増加します。

VDAがどれだけ迅速に登録されても、この間隔を完全に排除することはできません。

セカンダリブローカー間の同期にかかる時間は、オブジェクト（VDA、アプリケーション、グループなど）の数が増えるにつれて長くなります。たとえば、5000個のVDAを同期するには、10分以上かかる場合があります。

XenApp 6.xリリースとの違い

このローカルホストキャッシュの実装は、XenApp 6.xおよびそれ以前のXenAppリリースにおけるローカルホストキャッシュ機能と同じ名前を共有していますが、大幅な改善が施されています。この実装はより堅牢で、破損の影響を受けません。定期的な`dsmaint`コマンドの必要性を排除するなど、メンテナンス要件が最小限に抑えられています。このローカルホストキャッシュは、技術的には全く異なる実装です。

ローカルホストキャッシュの管理

ローカルホストキャッシュが正しく機能するには、各ControllerのPowerShell実行ポリシーをRemoteSigned、Unrestricted、またはBypassに設定する必要があります。

SQL Server エクスプレス ローカルDB

ローカルホストキャッシュが使用するMicrosoft SQL Server Express LocalDBソフトウェアは、Controllerをインストールするか、7.9より前のバージョンからControllerをアップグレードする際に自動的にインストールされます。セカンダリブローカーのみがこのデータベースと通信します。PowerShellコマンドレットを使用してこのデータベースに関する何も変更することはできません。LocalDBはController間で共有できません。

SQL Server Express LocalDBデータベースソフトウェアは、ローカルホストキャッシュが有効になっているかどうかにかかわらずインストールされます。

そのインストールを防ぐには、`XenDesktopServerSetup.exe`コマンドを使用してControllerをインストールまたはアップグレードし、`/exclude "Local Host Cache Storage (LocalDB)"`オプションを含めます。ただし、ローカルホストキャッシュ機能はデータベースなしでは機能せず、セカンダリブローカーで別のデータベースを使用することはできないことに注意してください。

このLocalDBデータベースのインストールは、サイトデータベースとして使用するためにSQL Server Expressをインストールするかどうかには影響しません。

以前のSQL Server Express LocalDBバージョンを新しいバージョンに置き換える方法については、SQL Server Express LocalDBの置き換えを参照してください。

製品のインストールとアップグレード後のデフォルト設定

Citrix Virtual Apps and Desktopsの新規インストール時（最小バージョン7.16）には、ローカルホストキャッシュが有効になります。

アップグレード後（バージョン7.16以降）、展開全体で10,000未満のVDAがある場合、ローカルホストキャッシュが有効になります。

ローカルホストキャッシュの有効化と無効化

- ローカルホストキャッシュを有効にするには、次のように入力します。

  ```
  Set-BrokerSite -LocalHostCacheEnabled $true
  ```

  ローカルホストキャッシュが有効になっているかどうかを確認するには、`Get-BrokerSite` と入力します。`LocalHostCacheEnabled` プロパティが `True` であることを確認します。

- ローカルホストキャッシュを無効にするには、次のように入力します。

  ```
  Set-BrokerSite -LocalHostCacheEnabled $false
  ```

注意: XenAppおよびXenDesktop 7.16以降、接続リース（バージョン7.6からローカルホストキャッシュに先行していた機能）は製品から削除され、利用できなくなりました。

ローカルホストキャッシュが機能していることを確認する

ローカルホストキャッシュが正しく設定され、機能していることを確認するには：

- 同期インポートが正常に完了していることを確認します。イベントログを確認してください。
- 各Delivery ControllerにSQL Server Express LocalDBデータベースが作成されていることを確認します。これにより、必要に応じてセカンダリブローカーが引き継ぐことができることが確認されます。
  - Delivery Controllerサーバーで、`C:\Windows\ServiceProfiles\NetworkService` を参照します。
  - `HaDatabaseName.mdf` と `HaDatabaseName_log.ldf` が作成されていることを確認します。
- Delivery Controllerで障害を強制的に発生させます。ローカルホストキャッシュが機能することを確認したら、すべてのControllerを通常モードに戻すことを忘れないでください。これには約15分かかる場合があります。

イベントログ

イベントログは、同期と障害が発生した時期を示します。イベントビューアーログでは、障害モードは*HA モード*と呼ばれます。*

コンフィグ シンクロナイザー サービス:

通常操作中、CSSがローカルホストキャッシュブローカーを使用して構成データをローカルホストキャッシュデータベースにインポートすると、次のイベントが発生する可能性があります。

- 503: Citrix Config Sync Serviceが更新された構成を受信しました。このイベントは、同期プロセスの開始を示します。
- 504: Citrix Config Sync Serviceが更新された構成をインポートしました。構成のインポートが正常に完了しました。
- 505: Citrix Config Sync Serviceのインポートに失敗しました。構成のインポートが正常に完了しませんでした。以前に正常な構成が利用可能な場合、障害が発生したときにそれが使用されます。ただし、現在の構成とは異なる古いものになります。以前の構成が利用できない場合、サービスは障害発生時にセッションブローカーに参加できません。この場合、トラブルシューティングセクションを参照し、Citrixサポートに連絡してください。
- 507: システムが障害モードであり、ローカルホストキャッシュブローカーがブローカー処理に使用されているため、Citrix Config Sync Serviceはインポートを中止しました。サービスは新しい構成を受信しましたが、障害が発生したためインポートは中止されました。これは予期される動作です。
- 510: プライマリ構成サービスから構成サービス構成データが受信されませんでした。
- 517: プライマリブローカーとの通信に問題がありました。
- 518: セカンダリブローカー（高可用性サービス）が実行されていないため、Config Syncスクリプトが中止されました。

高可用性サービス:

このサービスは、ローカルホストキャッシュブローカーとも呼ばれます。

- 3502: 停止が発生し、ローカルホストキャッシュブローカーがブローカー操作を実行しています。
- 3503: 停止が解決され、通常の操作が再開されました。
- 3504: どのローカルホストキャッシュブローカーが選出されたか、および選出に関与した他のローカルホストキャッシュブローカーを示します。
- 3507: 選出されたブローカーでローカルホストキャッシュモードがアクティブであることを示す、ローカルホストキャッシュのステータス更新を2分ごとに提供します。停止期間、VDA登録、セッション情報を含む停止の概要が含まれます。
- 3508: 選出されたブローカーでローカルホストキャッシュがアクティブでなくなり、通常の操作が復元されたことを通知します。停止期間、ローカルホストキャッシュイベント中に登録されたマシンの数、LHCイベント中の正常な起動の数を含む停止の概要が含まれます。
- 3509: 非選出ブローカーでローカルホストキャッシュがアクティブであることを通知します。2分ごとの停止期間と、選出されたブローカーを示します。

- 3510: 非選出ブローカーでローカルホストキャッシュがアクティブでなくなり、通常の操作が復元されたことを通知します。停止期間と、選出されたブローカーを示します。

停止を強制する

意図的に停止を強制したい場合があります。

- ネットワークが繰り返し停止したり再開したりする場合。ネットワークの問題が解決されるまで停止を強制することで、通常モードと停止モード間の継続的な移行（およびその結果として頻繁に発生するVDA登録ストーム）を防ぎます。
- ディザスタリカバリ計画をテストするため。
- ローカルホストキャッシュが正しく機能していることを確認するため。
- サイトデータベースサーバーの交換または保守中。

停止を強制するには、Delivery Controller を含む各サーバーのレジストリを編集します。`HKLM\Software\Citrix\DesktopServer\LHC`で、`OutageModeForced`を`REG_DWORD`として`1`に作成して設定します。この設定により、データベースの状態に関係なく、ローカルホストキャッシュブローカーは停止モードに入ります。値を`0`に設定すると、ローカルホストキャッシュブローカーは停止モードを終了します。

イベントを確認するには、`C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityService`にある`Current_HighAvailabilityService`ログファイルを監視します。

トラブルシューティング

ローカルホストキャッシュデータベースへの同期インポートが失敗し、505イベントが投稿された場合、いくつかのトラブルシューティングツールが利用可能です。

CDFトレース: `ConfigSyncServer` および `BrokerLHC` モジュールのオプションが含まれています。これらのオプションは、他のブローカーモジュールとともに、問題の特定に役立つでしょう。

レポート: 同期インポートが失敗した場合、レポートを生成できます。このレポートは、エラーの原因となっているオブジェクトで停止します。このレポート機能は同期速度に影響するため、Citrixは使用しないときは無効にすることを推奨します。

CSSトレースレポートを有効にして生成するには、次のコマンドを入力します。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1
```

HTMLレポートは`C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.htm`に投稿されます。

レポートが生成されたら、次のコマンドを入力してレポート機能を無効にします。

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```

ブローカー構成のエクスポート: デバッグ目的で正確な構成を提供します。

```
Export-BrokerConfiguration | Out-File <file-pathname>
```

例: `Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`。

ローカルホストキャッシュのPowerShellコマンド

PowerShellコマンドを使用して、Delivery Controllerでローカルホストキャッシュ (LHC) を管理できます。

PowerShellモジュールは、Delivery Controllerの次の場所にあります。

```
C:\Program Files\Citrix\Broker\Service\ControlScripts
```

> **重要:**
>
> このモジュールはDelivery Controllerでのみ実行してください。

PowerShell モジュールのインポート

モジュールをインポートするには、Delivery Controllerで次を実行します。

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-Module .\HighAvailabilityServiceControl.psm1
```

LHC を管理するための PowerShell コマンド

次のコマンドは、Delivery ControllerでLHCモードをアクティブ化および管理するのに役立ちます。

コマンドレット	機能
`Enable-LhcForcedOutageMode`	ブローカーをLHCモードにします。`Enable-LhcForcedOutageMode`が正常に機能するには、ConfigSyncサービスによってLHCデータベースファイルが正常に作成されている必要があります。このコマンドレットは、実行されたDelivery ControllerでのみLHCを強制します。LHCをアクティブにするには、このコマンドをゾーン内のすべてのDelivery Controllerで実行する必要があります。
`Disable-LhcForcedOutageMode`	ブローカーをLHCモードから外します。このコマンドレットは、実行されたDelivery ControllerでのみLHCモードを無効にします。`Disable-LhcForcedOutageMode`は、ゾーン内のすべてのDelivery Controllerで実行する必要があります。
`Set-LhcConfigSyncIntervalOverride`	Citrix Config Synchronizer Service (CSS) がサイト内の構成変更をチェックする間隔を設定します。時間間隔は60秒（1分）から3600秒（1時間）まで設定できます。この設定は、実行されたDelivery Controllerにのみ適用されます。Delivery Controller間の一貫性を保つため、このcmdletを各Delivery Controllerで実行することを検討してください。例: `Set-LhcConfigSyncIntervalOverride -Seconds 1200`
`Clear-LhcConfigSyncIntervalOverride`	Citrix Config Synchronizer Service (CSS) がサイト内の構成変更をチェックする間隔を、デフォルト値の300秒（5分）に設定します。この設定は、実行されたDelivery Controllerにのみ適用されます。Delivery Controller間の一貫性を保つため、このcmdletを各Delivery Controllerで実行することを検討してください。
`Enable-LhcHighAvailabilitySDK`	実行されたDelivery Controller内のすべての`Get-Broker*` cmdletへのアクセスを有効にします。

コマンドレット	機能
`Disable-LhcHighAvailabilitySDK`	実行されたDelivery Controller内のBroker cmdletへのアクセスを無効にします。

注:

- Delivery Controllerで `Get-Broker*` cmdletを実行する際は、ポート89を使用してください。例:
  - `Get-BrokerMachine -AdminAddress localhost:89`
- LHC モードでない場合、Delivery Controller 上の LHC Broker は構成情報のみを保持します。
- LHC モード中、選出された Delivery Controller 上の LHC Broker は次の情報を保持します。
  - リソースの状態
  - セッションの詳細
  - VDA登録
  - 構成情報

マシンとセッション

注:

Citrix Virtual Apps and Desktops™の展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

検索機能を使用して、特定の仮想マシン、セッション、マシンカタログ、アプリケーション、またはデリバリーグループに関する情報を表示します。Web Studioで**検索**を選択すると、いくつかのオプションが表示されます。

- タブを使用して、種類別（シングルセッションOSまたはマルチセッションOS）に仮想マシンを一覧表示するか、すべてのセッションを一覧表示します。
- 検索ボックスに名前を入力します。入力すると、クイック検索のためのフィルターが提供されます。
- フィルターを使用して検索を絞り込みます。
    - デフォルトでは、**名前**、**セッション状態**、**障害状態**のフィルターがビューに固定されています。フィルターを選択して式を作成します。フィルターをカスタマイズするには、省略記号をクリックします。表示されるウィンドウで、次の操作を実行できます。
        - フィルターを固定または固定解除します。固定解除されたフィルターは一度限りの使用であり、保存されません。
        - フィルターをクリックしてビューに追加します。
        - フィルターをクリアして、現在のフィルター検索をクリアし、固定解除されたフィルターを削除します。

コールアウト	領域	説明
A	検索バー	複雑な検索条件を定義できるクイック検索とフィルターベースの検索を提供します。詳細については、「インスタンスの検索」を参照してください。
B	タイプタブ	マシンをタイプ別に一覧表示するタブ、またはすべてのセッションを一覧表示するタブが表示されます。インスタンス数はタブ名に表示されます。
C	インスタンスレベルのアクション	*選択したインスタンス* (マシンまたはセッション) に対して実行できるアクションが表示されま

コールアウト	領域	説明
		す。詳細については、マシンアクション および セッションアクション を参照してください。
D	リストレベルのアクション	現在の*リスト*に対して実行できるアクションが表示されます。 • **エクスポート**アイコン: メインビューに表示されているインスタンスのリストをCSVファイルにエクスポートします。 • **表示する列**アイコン: リストのメインビューをカスタマイズします。 • 「**エラー**」ラベル: このラベルを有効にすると、メインビューにエラーのある未登録のマシンのみが表示されます。問題の詳細を表示するには、「**詳細**」ペインの「**トラブルシュー**

コールアウト	領域	説明	
		ティング」タブに移動します。 • 「**警告**」ラベル: このラベルを有効にすると、メインビューに警告のある未登録のマシンのみが表示されます。問題の詳細を表示するには、「**詳細**」ペインの「**トラブルシューティング**」タブに移動します。	
E	メインビュー	インスタンスとそのプロパティを表示します。「**表示する列**」アイコンを選択して、メインビューをカスタマイズできます。利用可能な列の詳細については、「マシン列」と「セッション列」を参照してください。	
F	詳細ペイン	次の詳細が表示されます: • 選択したインスタンス (マシンまたはセッション) の詳細	

コールアウト	領域	説明	
		• 選択したマシンに適用されているタグ • 選択したマシンに関するエラーまたは警告の詳細。問題、考えられる原因、推奨される解決策を含む	

フィルターセットを管理する(/en-us/citrix-virtual-apps-desktops/2411/media/manage-filter-sets.png)

検索機能を使用して、特定のマシンとセッションを見つけます。

検索ボックスに入力すると、プロンプトを含むメニューが表示され、検索をすばやく絞り込むのに役立つさまざまな検索オプションが提供されます。入力したコンテンツが*VM01*であるとします。次のいずれかのプロンプトを選択します。

- VM01 Name。名前で検索します。
- VM01 Machine Catalog。名前で検索します。
- VM01 デリバリーグループ。デリバリーグループ名で検索します。

たとえば、*静的でユーザーに割り当てられている*すべてのシングルセッションOSマシンを見つけるには、次の手順に従います。

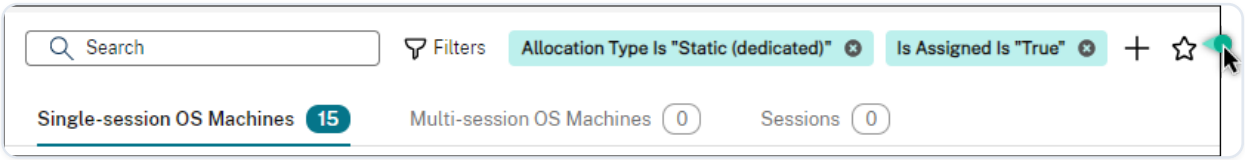
- **名前**。マシン名またはDNS名で検索します。
- **マシンカタログ**。マシンカタログ名で検索します。
- **デリバリーグループ**。デリバリーグループ名で検索します。
- **ユーザー**。セッションユーザー名で検索します。
- **クライアント**。セッションクライアント名で検索します。
- **VM**。ホストされているマシン名で検索します。これは、ハイパーバイザーで使用されるホストされているマシンのフレンドリ名です。
- **ホスティングサーバー名**。ホスティングサーバー名で検索します。

ユーザー、デスクトップグループ、カタログ、マシンなどの特定の項目を検索する場合、一般的な検索は必要な情報を見つけるための便利な方法を提供します。

マシンカタログまたはデリバリーグループを検索する

1. すべてのフィルター条件に一致する結果を検索で返す場合は、**すべて一致**（AND演算子）を選択します。いずれかのフィルター条件に一致する結果を検索で返す場合は、**いずれか一致**（OR演算子）を選択します。
2. **適用**をクリックします。

   フィルターされたリストには、静的でユーザーに割り当てられているすべてのシングルセッションOSマシンが表示されます。



デリバリーグループでは、次のフィルターが利用可能です。

たとえば、静的でユーザーに割り当てられているシングルセッションOSマシンのフィルターセットを将来の使用のために保存するには、次の手順に従います。

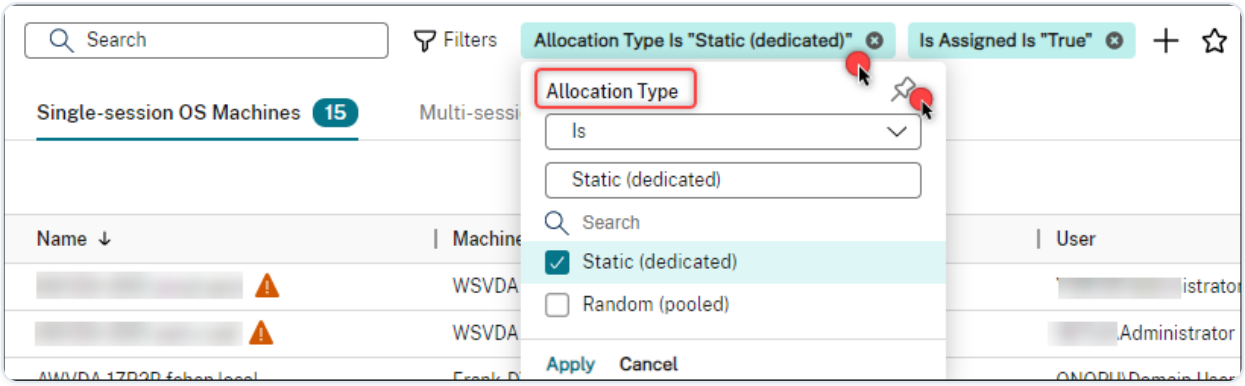
1. フィルターベースの検索を実行した後、前の図に示すように、検索バーの**星**アイコンをクリックします。
2. 表示されるページで、このフィルターセットの名前を入力します（例：*静的および割り当て済みマシン*）。
3. **保存**をクリックします。

- マシンカタログ:
  - 名前: フォルダーパスを含む名前でマシンカタログを検索します。
  - マシンカタログ: 名前でマシンカタログを検索します。
  - 説明: カタログ作成時に指定されたマシンカタログの説明で検索します。
- デリバリーグループ:
  - デリバリーグループ名: 名前でデリバリーグループを検索します。
  - 説明: デリバリーグループ作成時に指定されたデリバリーグループの説明で検索します。

頻繁に使用するフィルター*フィールド*を検索バーにピン留めして、簡単にアクセスできるようにします。たとえば、フィルターベースの検索を実行した後、検索バーに**割り当てタイプ**をピン留めしたいとします。次の手順に従います。

アプリケーショングループに対して、一般的な検索とフィルターベースの検索を実行できます。アプリケーショングループでは、次のフィルターが利用可能です:

1. 表示されるパネルで、**ピン**アイコンをクリックして、検索バーにフィルターフィールド（この例では*割り当てタイプ*）をピン留めします。



クイック検索ボックスを使用した検索

クイック検索ボックスは、名前関連のプロパティまたは保存されたフィルターセットに基づいてインスタンスを検索する便利な方法を提供します。詳細な手順は次のとおりです。

1. 検索ボックスをクリックします。最近の検索と保存されたフィルターセットがドロップダウンリストに表示されます。以前の検索またはフィルターセットをクリックして、クイック検索を実行できます。
2. 新しい検索を開始するには、次のオプションから完全または部分的な名前を入力します。

   - マシン名またはDNS名
   - マシンカタログ名
   - デリバリーグループ名
   - セッションユーザー名
   - セッションクライアント名
   - セッションをホストしているVMのフレンドリ名（ハイパーバイザーで使用されているもの）
   - ホスティングサーバー名

検索を強化するためのヒント

検索機能を使用する際は、以下のヒントを考慮してください。

- 「**検索**」ノードで、任意の列を選択して項目を並べ替えます。

- 検索および並べ替えが可能な表示に含める特性をさらに表示するには、 を選択するか、任意の列をクリックして を選択します。 ウィンドウで、表示する項目の横にあるチェックボックスをオンにし、 を選択して終了します。

> 「**注：**」:
>
> パフォーマンスを低下させる列には、「**パフォーマンスを低下させます**」というラベルが付けられています。

- マシンに接続されているユーザーデバイスを見つけるには、 と を使用し、デバイスのIPアドレスを入力します。
- アクティブなセッションを見つけるには、、、および を使用します。
- デリバリーグループ内のすべてのマシンを一覧表示するには、左側のペインで を選択します。グループを選択し、アクションバーまたはコンテキストメニューから を選択します。

並べ替え操作を実行する際は、以下の考慮事項に留意してください。

- 項目の数が5,000を超えない限り、任意の列をクリックして項目を並べ替えることができます。数が5,000を超えると、名前または現在のユーザー（表示しているタブによって異なります）でのみ並べ替えることができます。並べ替えを有効にするには、フィルターを使用して項目の数を5,000以下に減らします。
- 項目の数が500より大きく5,000以下の場合は、次のようになります。
  - 並べ替えのパフォーマンスを向上させるために、すべてのデータをローカルにキャッシュします。「**シングルセッションOSマシン**」タブと「**マルチセッションOSマシン**」タブでは、列（**名前**列を除く任意の列）を初めてクリックして並べ替えるときにデータをキャッシュします。「**セッション**」タブでは、列（**現在のユーザー**列を除く任意の列）を初めてクリックして並べ替えるときにデータをキャッシュします。その結果、並べ替えの完了に時間がかかります。パフォーマンスを高速化するには、名前または現在のユーザーで並べ替えるか、フィルターを使用して項目の数を減らします。
  - テーブルの下に表示される次のメッセージは、データがキャッシュされていることを示します: 最終更新日時: `<the time when you refreshed the table>`。この場合、並べ替え操作は以前に読み込まれた項目に基づいています。これらの項目は最新ではない可能性があります。最新の状態にするには、更新アイコンをクリックします。

表示する列をカスタマイズする

列をカスタマイズする際、**パフォーマンスが低下します**というラベルが付いた列が表示されることがあります。これらの列を選択すると、コンソールのパフォーマンスが低下する可能性があります。カスタマイズが完了すると、選択した列を表示するためにテーブルが更新されます。これらの列が存在すると、テーブルを更新する際に遅延が発生する可能性があります。

カスタマイズにパフォーマンスを低下させる列が含まれている場合、それらを保持するかどうかを決定するよう求められます。プロンプトは、ブラウザウィンドウを更新するか、コンソールからサインアウトしてサインインした後に表示されます。列を保持することにした場合は、次の考慮事項に注意してください。

> 利用可能な列とその説明の詳細については、[マシン列](studio-search/manage-machines.md#列)および[セッション列](studio-search/manage-sessions.md#列)を参照してください。

検索結果をCSVファイルにエクスポートする

- カスタマイズが完了すると、選択した列を表示するようにテーブルが更新されます。これらの列が存在すると、テーブルを更新する際に遅延が発生する可能性があります。
- ブラウザを更新するか、コンソールからサインアウトして再度サインインすると、それらの列を保持するかどうかを尋ねるメッセージが表示されます。保持することを選択した場合、最適なコンソールパフォーマンスを得るために、1分間に1回を超えるテーブルの更新は制限されます。より頻繁に更新するには、パフォーマンスを低下させる列をすべて削除してください。

検索ノードの各タブでは、エクスポートが進行中に別のエクスポートを実行することはできません。

検索を強化するためのヒント

検索機能を使用する際は、以下のヒントを考慮してください。

- **検索**ノードで、任意の列を選択して項目を並べ替えます。
- 検索および並べ替えが可能な表示に含める特性をさらに表示するには、**表示する列**を選択するか、任意の列をクリックして**表示する列**を選択します。**表示する列**ウィンドウで、表示したい項目の横にあるチェックボックスをオンにし、**保存**を選択して終了します。
- マシンカタログレベル。カタログのマスターイメージの変更、カタログからのマシンの削除、カタログへのマシンの追加など。詳細については、マシンカタログの管理を参照してください。

- デリバリーグループレベル。グループ内のマシンのメンテナンスモードのオン/オフなど。詳細については、デリバリーグループの管理を参照してください。

個々のセッションレベルに加えて、デリバリーグループレベルでもセッションを管理できます。たとえば、デリバリーグループのセッションの事前起動と維持を構成するなどです。詳細については、デリバリーグループの管理を参照してください。

- デリバリーグループ内のすべてのマシンを一覧表示するには、左ペインで**デリバリーグループ**を選択します。グループを選択し、アクションバーまたはコンテキストメニューから**マシンの表示**を選択します。

並べ替え操作を実行する際は、次の考慮事項に留意してください。

1. 「**検索**」ノードで、「**マルチセッションOSマシン**」、「**シングルセッションOSマシン**」、または「**セッション**」タブを選択します。
2. 必要に応じて、1つ以上のインスタンスを選択します。
3. アクションバーまたは右クリックメニューから、それらのインスタンスで発生する問題またはユーザー要求に基づいてアクションを選択します。

   利用可能なアクションとその説明の詳細については、「マシンアクション」と「セッションアクション」を参照してください。

   - ソートパフォーマンスを向上させるため、すべてのデータをローカルにキャッシュします。**シングルセッションOSマシン**タブと**マルチセッションOSマシン**タブでは、ソートのために列（**名前**列を除く任意の列）を初めてクリックしたときにデータをキャッシュします。**セッション**タブでは、ソートのために列（**現在のユーザー**列を除く任意の列）を初めてクリックしたときにデータをキャッシュします。その結果、ソートの完了に時間がかかります。パフォーマンスを向上させるには、名前または現在のユーザーでソートするか、フィルターを使用してアイテム数を減らしてください。
   - テーブルの下に表示される次のメッセージは、データがキャッシュされていることを示します: 最終更新: `<the time when you refreshed the table>`。この場合、ソート操作は以前にロードされたアイテムに基づいています。これらのアイテムは最新ではない可能性があります。最新の状態にするには、更新アイコンをクリックしてください。

マシンのアクションと列

この記事では、参照用にマシンのアクションと列を説明とともに一覧表示します。

アクション

マシンで実行できるアクションとその説明を表示します。

アクション	説明	適用対象
デリバリーグループから削除	デリバリーグループからマシンを削除します。	シングルセッションおよびマルチセッション
デリバリーグループに追加	マシンをデリバリーグループに追加します。	シングルセッションおよびマルチセッション
セッションの表示	マシンで実行中のセッションを表示します	シングルセッションおよびマルチセッション
タグの管理	マシンにタグを追加して管理します。タグの一般的な使用例について詳しくは、「タグ」を参照してください。	シングルセッションおよびマルチセッション
メンテナンスモードをオンにする	パッチを適用する前、またはトラブルシューティングのために、マシンをメンテナンスモードにします。 このモードでは、そのマシンへの新しい接続が防止されます。ユーザーはそのマシン上の既存のセッションに接続できますが、そのマシン上で新しいセッションを開始することはできません。	シングルセッションおよびマルチセッション
メンテナンスモードをオフにする	マシンのメンテナンスモードをオフにします。	シングルセッションおよびマルチセッション
VDAのアップグレード	マシンのVDAをアップグレードします。	特定の要件を満たすシングルセッションまたはマルチセッションOSマシンです。詳細はこちら。
ログオフ	マシンを強制的にログオフする	シングルセッションおよびマルチセッション
削除	マシンカタログからVMを削除しますが、ハイパーバイザーまたはクラウドサービス	シングルセッションおよびマルチセッション

アクション	説明	適用対象
	上ではVMはそのまま残されます。	
ユーザーの変更	特定のユーザーにマシンを割り当てる。	シングルセッションの*静的*マシン。
起動	マシンを起動する。	シングルセッションおよびマルチセッション
シャットダウン	マシンをシャットダウンする。	シングルセッションおよびマルチセッション
再起動	マシンを再起動する	シングルセッションおよびマルチセッション
サスペンド	マシンを休止状態またはサスペンド状態にします。マシンをサスペンドすると、Delivery Controller はマシンのメモリ内容をファイルに保存し、マシンをシャットダウンします。	シングルセッションOSマシン
再開	サスペンドされたマシンを再開します。サスペンドされたマシンを再開すると、Delivery Controller はマシンを起動し、以前の状態に復元します。	シングルセッションOSマシン
強制再起動	マシンを強制的に再起動する。	シングルセッションOSマシン
強制シャットダウン	マシンを強制的にシャットダウンする。	シングルセッションOSマシン

列

マシンのすべての列とその説明を種類別に表示します。

- マシン
- マシンの詳細

- アプリケーション
- ホスティング
- 接続
- 登録
- セッションの詳細
- セッション

マシン

マシンカテゴリの列。

列	説明	適用対象
名前	マシンのDNSホスト名。	シングルセッションおよびマルチセッション
マシンカタログ	マシンが属するカタログの名前。	シングルセッションおよびマルチセッション
デリバリーグループ	マシンが属するデリバリーグループの名前。	シングルセッションおよびマルチセッション
ユーザー表示名	マシンに関連付けられているユーザーのフルネーム (通常、`Firstname Lastname`の形式)。関連付けられているユーザーとは、共有マシンの現在のユーザーと、専用マシンの割り当て済みユーザーです。	シングルセッションおよびマルチセッション
ユーザー	マシンに関連付けられているユーザーのユーザー名 (「domain\user」の形式)。関連付けられ	シングルセッションおよびマルチセッション

列	説明	適用対象
	ているユーザーとは、共有マシンの現在のユーザーと、専用マシンの割り当て済みユーザーです。	
ユーザープリンシパル名	マシンに関連付けられているユーザーのユーザープリンシパル名（「user@domain」の形式）。関連付けられているユーザーとは、共有マシンの現在のユーザーと、専用マシンに割り当てられたユーザーのことです。	シングルセッションおよびマルチセッション
デスクトップ表示名	セッションの起動に元々使用されたマシンの公開名。Citrix Workspace™アプリまたはStoreFrontに表示される名前です。	シングルセッションのみ
	注： デスクトップの表示を変更するには、**マシンの更新を実行**権限が必要です。表示名の変更にはマシンプロパティの更新が含まれるためです。	
デスクトップ条件	マシンの未解決のデスクトップ条件のリスト。可能な値：Unknown、CPU、	シングルセッションおよびマルチセッション

列	説明	適用対象
	ICALatency、および UPMLogonTime。	
割り当てタイプ	マシンの割り当てタイプ：ユーザーに永続的に割り当てられる場合は**永続**。ランダムに割り当てられる場合は**ランダム**。	シングルセッションおよびマルチセッション
メンテナンスモード	マシンがメンテナンスモードであるかどうかを示します。	シングルセッションおよびマルチセッション
Windows接続設定	Windowsによって報告されたログオンモード。	マルチセッションのみ
	指定可能な値: LogonEnabled、Draining、DrainingUntilRestart、および LogonDisabled。	
割り当て済み	専用デスクトップがユーザーまたはクライアント (名前/アドレス) に割り当てられているかどうかを示します。ユーザーは明示的に割り当てることも、マシンの初回使用時に割り当てることもできます。	シングルセッションおよびマルチセッション
物理マシン	マシンが物理マシンであるかどうかを示します。`True` はマシンが物理マシンであることを示し、こ	シングルセッションおよびマルチセッション

列	説明	適用対象	
	れはDelivery Controllerによって電源管理されていないことを意味します。`False` はそうでないことを示します。		
プロビジョニングの種類	マシンがプロビジョニングされた方法。指定可能な値 • 手動: PVSまたはMCSを使用してプロビジョニングされていません。 • PVS: PVSを使用してプロビジョニングされています (物理マシン、ブレードマシン、仮想マシン)。 • MCS: MCSを使用してプロビジョニングされています (VMのみ)。	シングルセッションおよびマルチセッション	
スケジュールされた再起動	マシンのスケジュールされた再起動操作の状態。指定可能な値	シングルセッションおよびマルチセッション	

列	説明	適用対象	
	• なし: 再起動はスケジュールされていません。 • 保留中: 再起動を待機していますが、使用可能です。 • ドレイン中: 再起動を待機しており、新しいセッションには使用できません。ただし、既存の接続への再接続は引き続き許可されます。 • 進行中: スケジュールされた再起動がアクティブに実行されています。 • 自然: 自然な再起動が進行中です。マシンは再起動を待機しています。		
ゾーン	マシンが配置されているゾーンの名前。	シングルセッションおよびマルチセッション	
状態	マシンに関連付けられているデスクトップの全体的な状態。これは、セッション	シングルセッションおよびマルチセッション	

列	説明	適用対象
	状態、登録状態、電源状態など、さまざまな特定の状態から派生しています。	
	可能な状態: オフ、未登録、利用可能、切断済み、使用中、準備中。	
タグ	マシンに関連付けられているタグのリスト。	シングルセッションおよびマルチセッション
VDAアップグレード	VDAパッケージアップグレードアクションのマシン状態。	シングルセッションとマルチセッション
	指定可能な値: MissingUpgradeType、UpgradeScheduled、UpgradeAvailable、UpToDate、および Unknown。	
サスペンド可能	マシンが電源アクション（サスペンドと再開）をサポートしているかどうかを示します。	シングルセッションとマルチセッション
ロードインデックス	現在のロードインデックス。詳細については、詳細情報を参照してください。	マルチセッションのみ
ドレイン状態	マシンがドレイン中で、マシン上のすべてのセッションが終了した後にシャット	マルチセッションのみ

列	説明	適用対象
	ダウンするかどうかを示します。Trueは、電源管理されたマルチセッションマシンにのみ表示されます。	
	注: マシンがメンテナンスモードの場合、シャットダウンしません。メンテナンスモードが解除された後にのみシャットダウンします。	

マシンの詳細

マシンの詳細カテゴリの列。

列	説明	適用対象
エージェントバージョン	マシンにインストールされているCitrix Virtual Delivery Agent (VDA) のバージョン。	シングルセッションおよびマルチセッション
IPアドレス	マシンのIPアドレス。	シングルセッションおよびマルチセッション
割り当て済み	専用デスクトップがユーザーまたはクライアント（名前/アドレス）に割り当てられているかどうかを示します。ユーザーは明示的に割り当てることも、マシンを初めて使用する際に割り当てることもできます。	シングルセッションおよびマルチセッション
OSの種類	マシンで実行されているオペレーティングシステムの種類。	シングルセッションのみ

アプリケーション

アプリケーションカテゴリの列。

列	説明	適用対象
使用中のアプリケーション	マシンで使用中のアプリケーションのリスト（ブラウザ名として表示されます）。	シングルセッションおよびマルチセッション
公開アプリケーション	マシンによって公開されたアプリケーションのリスト（ブラウザ名として表示されます）。	シングルセッションおよびマルチセッション

接続

接続カテゴリの列。

「列」	「説明」	「適用対象」
クライアント (IP)	マシンに接続されているクライアントのIPアドレス。	シングルセッションのみ
クライアント	マシンに接続されているクライアントのホスト名。	シングルセッションのみ
プラグインバージョン	接続されているクライアント上のCitrix Workspaceアプリのバージョン。	シングルセッションのみ
接続元	受信接続のホスト名。通常、ゲートウェイ、ルーター、またはクライアントです。	シングルセッションのみ
接続元 (IP)	受信接続のIPアドレス。通常、ゲートウェイ、ルーター、またはクライアントです。	シングルセッションのみ
接続の種類	セッションに使用されるプロトコル。指定可能な値: HDX、RDP、および Console。注: XenDesktop® 5	シングルセッションのみ

「列」	「説明」	「適用対象」
	VDA上のコンソールセッションの場合、このフィールドは空白になります。	
最終接続時刻 (UTC)	最後に検出された接続試行（失敗または成功）の時刻。	シングルセッションおよびマルチセッション
最終接続ユーザー	マシンへの接続を最後に試行したユーザーのSAM名（「DOMAIN\user」形式）。SAM名が利用できない場合は、SIDが使用されます。	シングルセッションおよびマルチセッション
Secure ICA® アクティブ	現在のセッションでSecureICAがアクティブであるかどうかを示します。マルチセッションマシンでは常にnullです。	シングルセッションおよびマルチセッション

ホスティング

ホスティングカテゴリの列。

列	説明	適用対象
VM	セッションを実行しているホストされたマシンの、ハイパーバイザーによって使用されるフレンドリ名。マシンのDNS名またはAD名と必ずしも一致するわけではありません。	シングルセッションおよびマルチセッション
ホスティングサーバー名	管理対象の場合、マシンをホストしているハイパーバイザーのDNS名。	シングルセッションおよびマルチセッション

列	説明	適用対象
接続	セッションをホストしているマシンに割り当てられているホスト接続の名前。	シングルセッションおよびマルチセッション
保留中の更新	ホストされているマシンのVMイメージが古くなっており、次回の再起動時に新しいイメージに更新される必要があるかどうかを示します。	シングルセッションおよびマルチセッション
ユーザー変更の永続性	ユーザーの変更がどのように処理されるかを示し、変更が永続的であるかどうかを示します: • OnLocal: 永続的。ユーザーの変更はローカルに保存されます。 • Discard: 非永続的。ユーザーの変更は破棄されます。	シングルセッションおよびマルチセッション
保留中の電源操作	マシンに保留中の電源操作があるかどうかを示します。	シングルセッションおよびマルチセッション
電源状態	マシンの電源状態。可能な値：管理対象外、不明、利用不可、オフ、オン、一時停止、起動中、	シングルセッションおよびマルチセッション

列	説明	適用対象
	シャットダウン中、一時停止中、再開中。	
使用後にシャットダウン	電源管理されたシングルセッションマシンにのみ適用されます。マシンが汚染されており、すべてのセッションが終了した後にシャットダウンするかどうかを示します。	シングルセッションのみ
	注： マシンがメンテナンスモードの場合、シャットダウンしません。メンテナンスモードから解除された後にのみシャットダウンします。	

登録

登録カテゴリの列。

列	説明	適用対象
最終登録失敗	マシンがブローカーから最後に登録解除された理由。	シングルセッションおよびマルチセッション
	指定できる値は次のとおりです: AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactabl	

列	説明	適用対象
	e, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError, and BrokerRegistrationLimitReached.	
最終登録失敗時刻 (UTC)	マシンが最後に登録解除された時刻。	シングルセッションおよびマルチセッション

列	説明	適用対象
登録状態	マシンの登録状態。指定できる値: Unregistered, Initializing, Registered, and AgentError.	シングルセッションおよびマルチセッション
障害状態	マシンの現在の障害状態の概要。指定できる値: • なし: 障害なし。マシンは正常です。 • FailedToStart: マシンの前回の電源投入操作が失敗しました。 • StuckOnBoot: 電源投入後、マシンが起動に失敗しました。 • Unregistered: マシンが予期された期間内に登録に失敗したか、登録が拒否されました。 • MaxCapacity: マシンが最大容量に達していると報告しています。	シングルセッションおよびマルチセッション

セッションの詳細

セッションの詳細カテゴリの列。

列	説明	適用対象
起動元	現在のブローカーセッションの起動に使用されたStoreFrontサーバーのホスト名。マルチセッションマシンでは常にnullです。	シングルセッションおよびマルチセッション
起動元 (IP)	現在のブローカーセッションの起動に使用されたStoreFrontサーバーのIPアドレス。マルチセッションマシンでは常にnullです。	シングルセッションおよびマルチセッション
セッション変更時刻 (UTC)	現在のセッションの最後の状態変更時刻。	シングルセッションのみ
SmartAccessフィルター	現在のセッションのSmart Accessタグ。マルチセッションマシンでは常にヌルです。	シングルセッションおよびマルチセッション

セッション

セッションカテゴリの列。

列	説明	適用対象
セッションの状態	現在のセッションの状態。可能な値: Other、PreparingSession、Connected、Active、Disconnected、Reconnecting、NonBrokeredSession、Unknown。	シングルセッションのみ
現在のユーザー	現在のセッションのユーザー名（「DOMAIN\user」の形式）。	シングルセッションのみ

列	説明	適用対象
開始時刻 (UTC)	現在のセッションの開始時刻。	シングルセッションのみ
セッション数	マシン上のセッション数。	マルチセッションのみ

セッションのアクションと列

この記事では、参照用にマシンアクションと列を説明とともに示します。

アクション

セッションで実行できるアクションとその説明を表示します。

アクション	説明	セッションの適用先
ログオフ	セッションからユーザーをログオフします。	シングルセッションOSマシンまたはマルチセッションOSマシン
メッセージを送信	セッションのユーザーにメッセージを送信します。	シングルセッションOSマシンまたはマルチセッションOSマシン
マシンの表示	セッションのホストマシンを表示します。	シングルセッションOSマシンまたはマルチセッションOSマシン
切断	セッションを切断します。セッションが切断されても、セッションはアクティブなままでアプリケーションは実行され続けますが、ユーザーデバイスはDelivery Controllerと通信しなくなります。	シングルセッションOSマシンまたはマルチセッションOSマシン
マシンのシャットダウン	セッションに関連付けられているマシンをシャットダウンします。	シングルセッションOSマシン
マシンの再起動	セッションに関連付けられているマシンを再起動します。	シングルセッションOSマシン

列

セッションの列とその説明を表示します。

列	説明
現在のユーザー	ユーザー名。ユーザーのユーザープリンシパル名 (UPN)。
名前	セッションをホストしているマシンのDNSホスト名。
デリバリーグループ	セッションをホストしているマシンを含むデリバリーグループの名前。
マシンカタログ	セッションをホストしているマシンを含むマシンカタログの名前。
エージェントバージョン	セッションをホストしているマシンにインストールされているCitrix Virtual Delivery Agent (VDA) のバージョン。
使用中のアプリケーション	セッションで使用されているアプリケーションのリスト。管理名で識別されます。
自律的に仲介済み	これは、仲介されずに直接接続によって確立されたHDX™セッションであるかどうか。
仲介時刻 (UTC)	セッションが仲介された時刻。
ブローカーユーザー名	ブローカーユーザーの名前。
クライアント (IP)	セッションに接続されているクライアントのIPアドレス。
クライアント	セッションに接続されているクライアントのホスト名。

列	説明
プラグインバージョン	セッションに接続されているクライアントで実行されているCitrix Workspace™アプリのバージョン。
接続元	受信接続のホスト名。通常はゲートウェイ、ルーター、またはクライアント。
接続元 (IP)	受信接続のIPアドレス。通常はゲートウェイ、ルーター、またはクライアント。
割り当ての種類	セッションが共有か専用か。
非表示	セッションがユーザーから隠されているか、再接続されないように設定されているか。
VM	セッションをホストしているVMの、ハイパーバイザーで使用されているフレンドリ名。これは、マシンのDNS名またはAD名のいずれとも必ずしも一致しません。
ホスティングサーバー名	セッションのホスティングマシンをホストしているハイパーバイザーのDNS名。
接続	セッションをホストしているマシンに割り当てられているホスト接続の名前。
保留中の更新	ホストされているマシンのVMイメージが古く、次回の再起動時に新しいイメージに更新される予定であるかどうか。

列	説明
メンテナンスモード	セッションをホストしているマシンがメンテナンスモードであるかどうか。
IPアドレス	セッションをホストしているマシンのIPアドレス。
物理か	セッションをホストしているマシンが物理であるかどうか。`True` はマシンが物理であることを示し、Delivery Controllerによって電源管理されていないことを意味します。`False` はそうでないことを示します。
起動元	セッションの起動に使用されたStoreFront™サーバーのホスト名。セッションがWorkspace経由で起動された場合は空白。
起動元 (IP)	セッションの起動に使用されたStoreFrontサーバーのIPアドレス。セッションがWorkspace経由で起動された場合は空白。
OSの種類	セッションをホストしているオペレーティングシステムの識別文字列。
ユーザー変更の永続性	ユーザーの変更がどのように処理されるかを示し、変更が永続的であるかどうかを示します:

列	説明
	• OnLocal: 永続的。ユーザーの変更はローカルに保存されます。 • Discard: 非永続的。ユーザーの変更は破棄されます。
接続タイプ	セッションに使用されるプロトコル（HDX、RDP、Consoleなど）。 **注:** XenDesktop® 5 VDA 上のコンソールセッションの場合、このフィールドは空白です。
プロビジョニングの種類	セッションをホストしているマシンがどのようにプロビジョニングされたか • 手動: PVSまたはMCSを使用してプロビジョニングされていません。 • PVS: PVSによってプロビジョニングされています (物理マシン、ブレードマシン、仮想マシン)。 • MCS: MCSによってプロビジョニングされています (VMのみ)。
Secure ICA® アクティブ	セッションでSecureICAがアクティブであるかどうか。

列	説明
セッションの状態	セッションの状態。可能な値: Connected、Active、Disconnected。L7より前の機能レベルのマシン上のセッションでは、PreparingSession、Reconnecting、NonBrokeredSession、Other、Unknownなどの他の状態が発生する場合があります。
セッション変更時刻	セッションの最新の状態変更時刻。
アプリケーションの状態	セッション内のアプリケーションの状態。可能な値: PreLogon、PreLaunched、Active、Desktop、Lingering、およびNoApps。
セッションサポート	セッションをホストしているマシンが、複数セッションをサポートするか単一セッションをサポートするか。
ゾーン	セッションをホストしているマシンが配置されているゾーンの名前。
SmartAccessフィルター	セッションのSmart Accessタグ。
開始時刻 (UTC)	セッションが開始された日時。
状態	マシンの概要状態。可能な値: Unregistered、Disconnected、またはInUse。

列	説明
状態での時間 (UTC)	セッションが現在の状態になってからの時間。
デリバリーコントローラー™	セッションのホストマシンが登録されているコントローラーのDNSホスト名。
ユーザー表示名	ユーザーのフルネーム。
デスクトップ表示名	セッションの起動に元々使用されたマシンの公開名。Citrix Workspaceアプリまたはストアフロントに表示される名前です。アプリケーションセッションの場合、そのアプリケーションが終了していても、セッションで最初に起動されたアプリケーションの名前です。リソースが後で名前変更または削除されても、名前は変更されません。

セキュリティキー

重要:

- この機能は、StoreFront™ 1912 LTSR CU2以降と組み合わせて使用する必要があります。
- Secure XML機能は、Citrix ADCおよびCitrix Gatewayリリース12.1以降でのみサポートされています。

注:

Citrix Virtual Apps and Desktops™の展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb

> Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> この機能を使用すると、承認されたStoreFrontおよびCitrix GatewayマシンのみがDelivery Controllerと通信することを許可できます。この機能を有効にすると、キーを含まないすべての要求はブロックされます。この機能を使用して、セキュリティの追加レイヤーを追加し、内部ネットワークから発信される攻撃から保護します。

この機能を使用するための一般的なワークフローは次のとおりです。

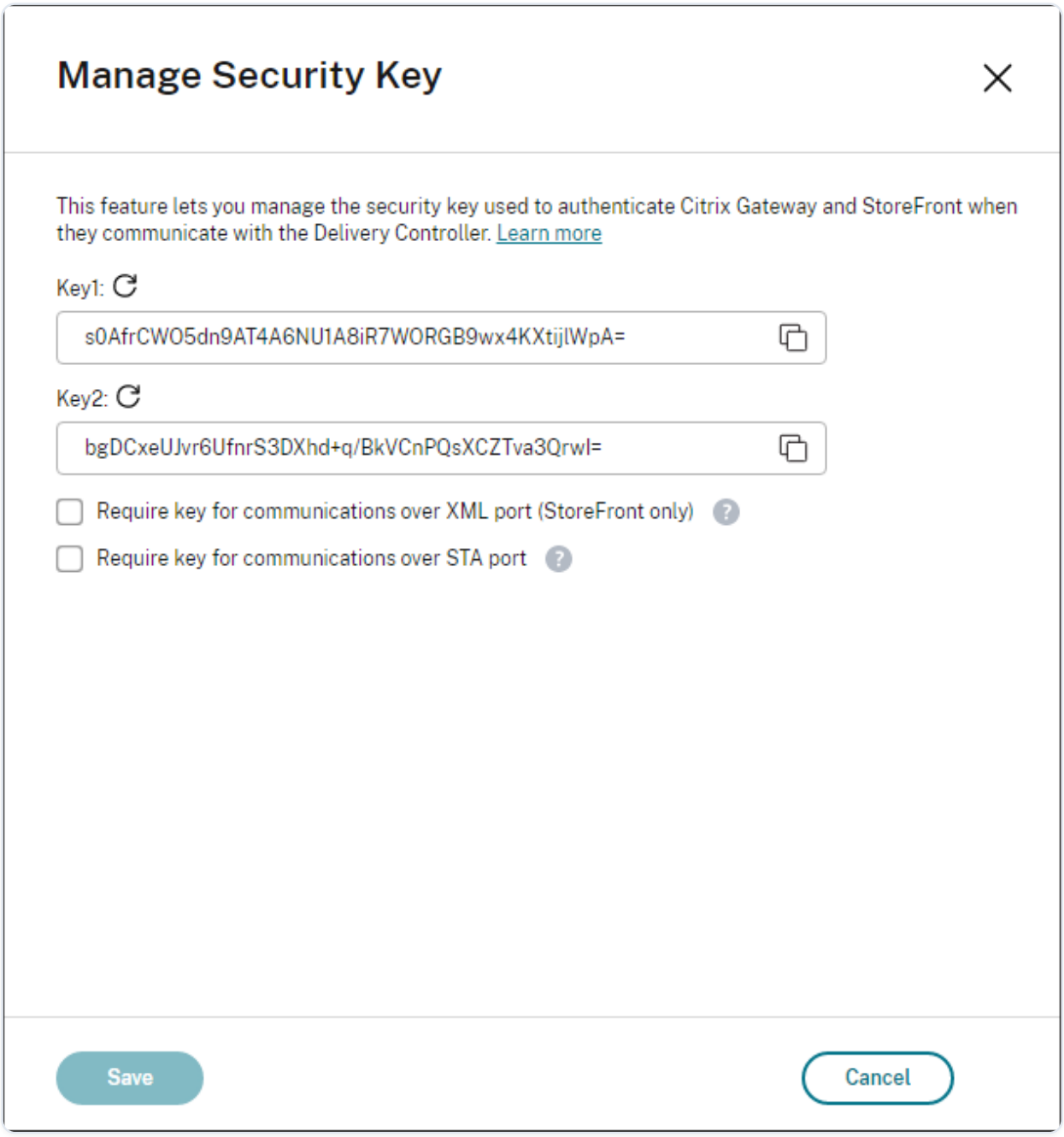
1. Web Studioを有効にして、機能設定を表示します。
2. サイトの設定を構成します。
3. StoreFrontの設定を構成します。
4. Citrix ADCの設定を構成します。

サイトの設定を構成する

Web Studio または PowerShell を使用して、サイトのセキュリティキー設定を構成できます。

Web Studioを使用する

1. Web Studioにサインインし、左ペインで**設定**を選択します。
2. **セキュリティキーの管理**タイルを見つけて**編集**をクリックします。**セキュリティキーの管理**ページが表示されます。



3. 更新アイコンをクリックしてキーを生成します。

重要：

- 使用できるキーは2つあります。XMLポートおよびSTAポートを介した通信には、同じキーまたは異なるキーを使用できます。一度に1つのキーのみを使用することをお勧めします。未使用のキーは、キーのローテーションにのみ使用されます。
- 使用中のキーを更新するために更新アイコンをクリックしないでください。クリックすると、サービスが中断されます。

4. 通信にキーが必要な場所を選択します。

   - **XMLポートを介した通信にキーを要求する（StoreFrontのみ）**。選択すると、XMLポートを介した通信を認証するためにキーが必要になります。StoreFrontはこのポートを介してCitrix Cloudと通信します。XMLポートの変更については、Knowledge Centerの記事CTX127945を参照してください。
   - **STAポートを介した通信にキーを要求する**。選択すると、STAポートを介した通信を認証するためにキーが必要になります。Citrix GatewayとStoreFrontはこのポートを介してCitrix Cloudと通信します。STAポートの変更については、Knowledge Centerの記事CTX101988を参照してください。

5. **保存**をクリックして変更を適用し、ウィンドウを閉じます。

PowerShell を使用する

以下は、Web Studioの操作に相当するPowerShellの手順です。

1. Citrix Virtual Apps and Desktops Remote PowerShell SDK を実行します。
2. コマンドウィンドウで、次のコマンドを実行します。

   - `Add-PSSnapIn Citrix*`

3. キーを生成し、Key1を設定するには、次のコマンドを実行します。

   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`

4. 以下のコマンドを実行してキーを生成し、Key2 をセットアップします。

   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`

5. 通信の認証でキーの使用を有効にするには、次のコマンドのいずれかまたは両方を実行します。

   - XML ポート経由で通信を認証するには:
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - STA ポート経由で通信を認証するには:
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

ガイダンスと構文については、PowerShellコマンドのヘルプを参照してください。

StoreFrontの設定を構成する

サイトの構成が完了したら、PowerShellを使用してStoreFrontの関連設定を構成する必要があります。

StoreFront サーバーで、以下の PowerShell コマンドを実行します。

XMLポートを介した通信用のキーを構成するには、コマンドを使用します。例:

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [secret]
```

次のパラメータに適切な値を入力します。

- `Path to store`
- `Resource feed name`
- `secret`

STAポート経由の通信用にキーを構成するには、`New-STFSecureTicketAuthority`および`Set-STFRoamingGateway`コマンドを使用します。例:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

次のパラメータに適切な値を入力します。

- `Gateway name`

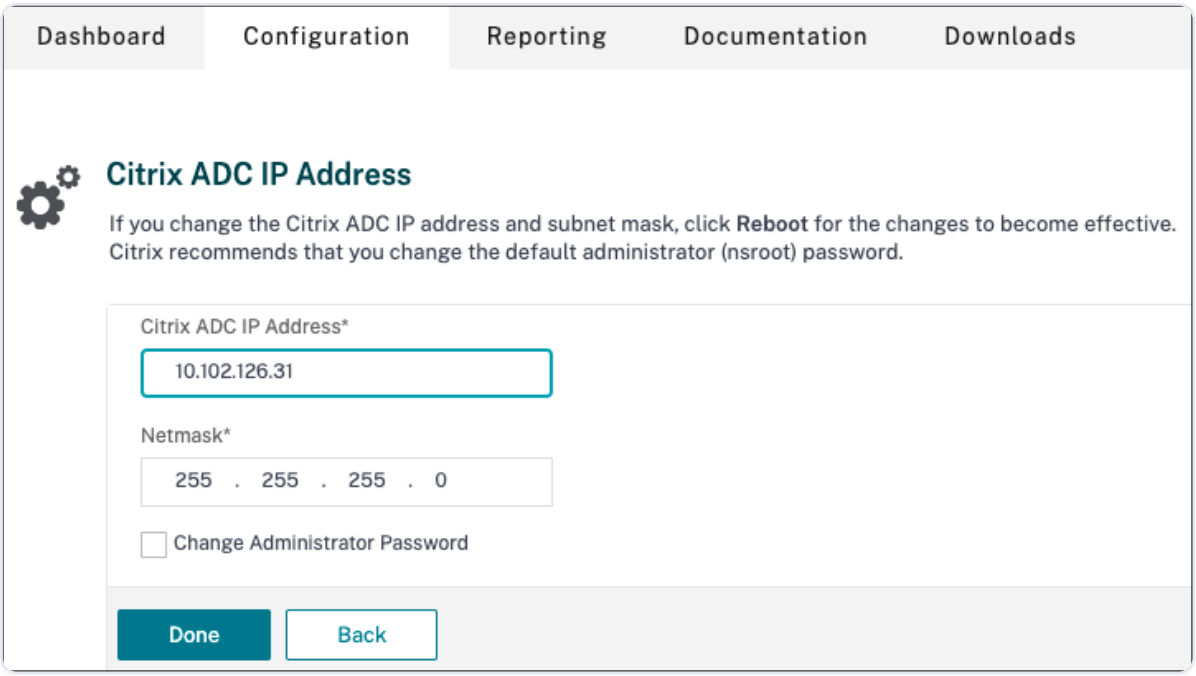
- `STA URL`
- `Secret`

ガイダンスと構文については、PowerShellコマンドのヘルプを参照してください。

Citrix ADCの設定を構成する

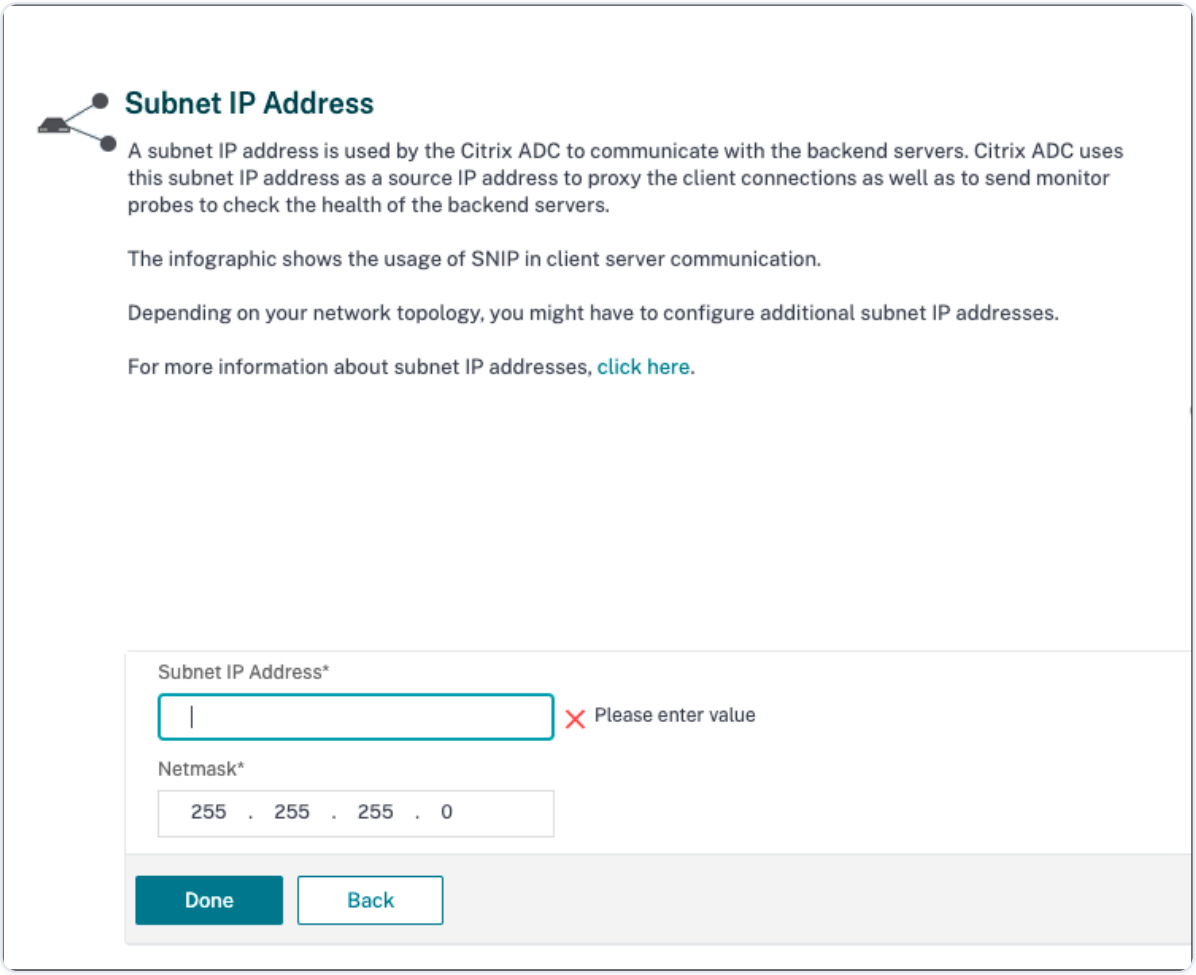
> **注:**
>
> Citrix ADC をゲートウェイとして使用しない限り、Citrix ADC のこの機能を構成する必要はありません。Citrix ADC を使用する場合は、次の手順に従ってください。

1. 以下の前提条件となる構成がすでに設定されていることを確認してください。
   - 次のCitrix ADC関連のIPアドレスが構成されています。
     - Citrix ADCコンソールにアクセスするための Citrix ADC管理IP (NSIP) アドレス。詳細については、「NSIPアドレスの構成」を参照してください。

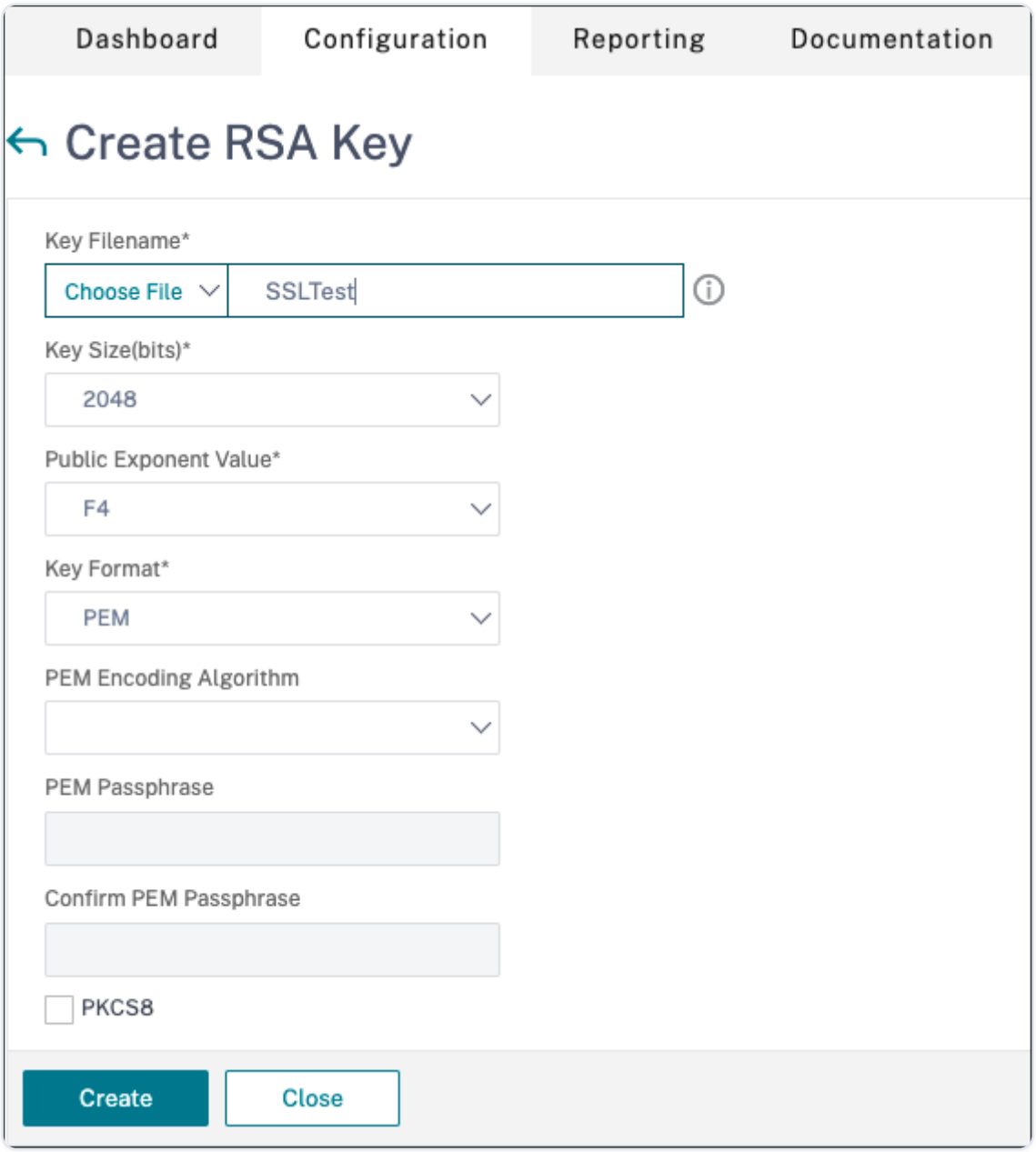


     - Citrix ADCアプライアンスとバックエンドサーバー間の通信を有効にするためのサブネットIP（SNIP）アドレス。詳細については、「サブネットIPアドレスの構成」を参照してください。

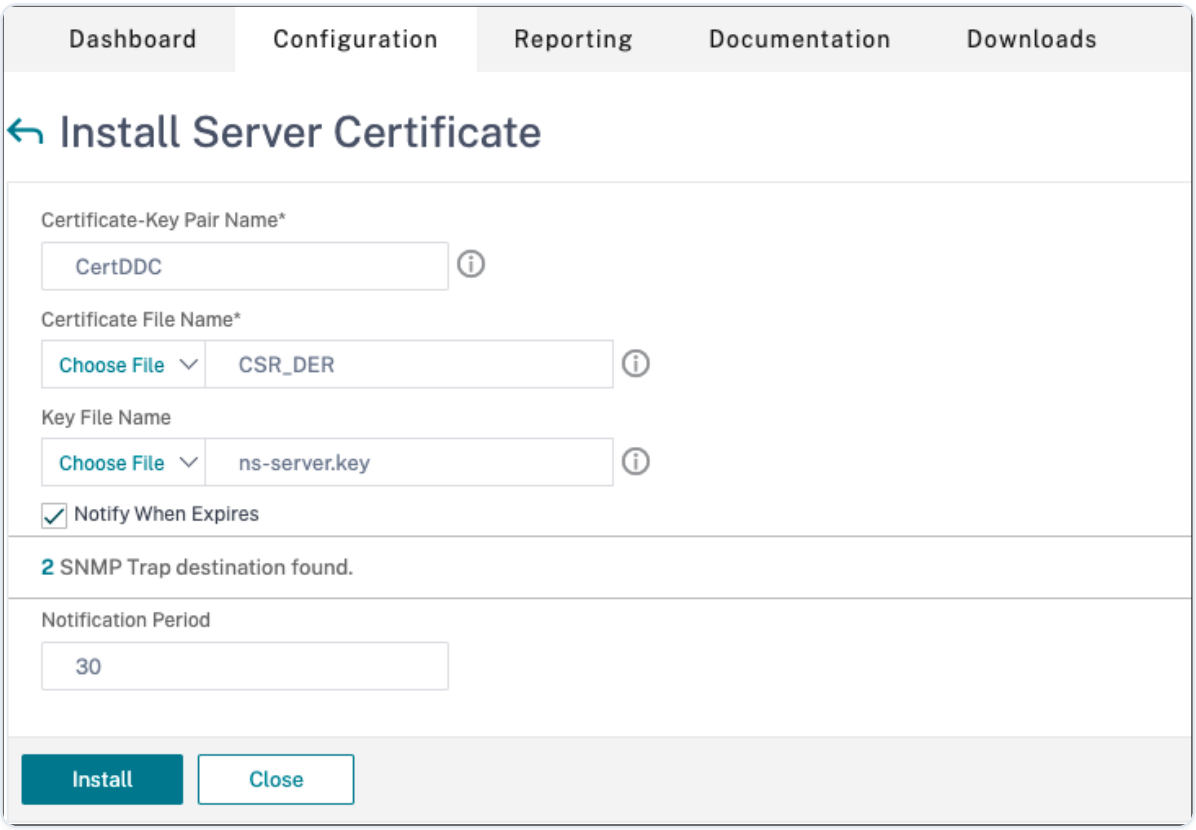
- セッション起動のためにADCアプライアンスにログインするためのCitrix Gateway仮想IPアドレスとロードバランサー仮想IPアドレス。詳細については、「仮想サーバーの作成」を参照してください。



- Citrix ADCアプライアンスで必要なモードと機能が有効になっています。
  - モードを有効にするには、Citrix ADC GUIで **System > Settings > Configure Mode** に移動します。
  - 機能を有効にするには、Citrix ADC GUIで **System > Settings > Configure Basic Features** に移動します。
- 証明書関連の構成が完了しています。
  - 証明書署名要求 (CSR) が作成されています。詳細については、「証明書の作成」を参照してください。



- サーバー証明書、CA証明書、およびルート証明書がインストールされています。詳細については、「インストール、リンク、および更新」を参照してください。



「CA証明書をインストール」(/en-us/citrix-virtual-apps-desktops/2411/media/adc-install-ca-certificate.png)

- Citrix Virtual Desktops 用に Citrix Gateway が作成されました。仮想サーバーがオンラインであることを確認するには、**Test STA Connectivity** ボタンをクリックして接続をテストします。詳細については、「Citrix Virtual Apps and Desktops 用の Citrix ADC のセットアップ」を参照してください。

「仮想デスクトップ用ゲートウェイ」(/en-us/citrix-virtual-apps-desktops/2411/media/xenapp-xendesktop-wizard.gif)

2. リライトアクションを追加します。詳細については、「リライトアクションの構成」を参照してください。

   a. 「**AppExpert > Rewrite > Actions**」に移動します。

   b. 新しい書き換えアクションを追加するには、**追加**をクリックします。アクションの名前は「set Type to INSERT_HTTP_HEADER」にすることができます。

「リライトアクションの追加」(/en-us/citrix-virtual-apps-desktops/2411/media/adc-appexpert-rewrite-action.png)

   a. **Type** で、**INSERT_HTTP_HEADER** を選択します。

   b. **Header Name** に「X-Citrix-XmlServiceKey」と入力します。

c. **Expression** に、引用符付きで `<XmlServiceKey1 value>` を追加します。
XmlServiceKey1 の値は、Desktop Delivery Controller™ の構成からコピーできます。

「XMLサービスキー値」(/en-us/citrix-virtual-apps-desktops/2411/media/xml-service-key-values.png)

3. 書き換えポリシーを追加します。詳細については、「書き換えポリシーの構成」を参照してください。

   a. 「**AppExpert > Rewrite > Policies**」に移動します。
   b. 新しいポリシーを追加するには、**追加**をクリックします。

「リライトポリシーの追加」(/en-us/citrix-virtual-apps-desktops/2411/media/adc-appexpert-rewrite-policy.png)

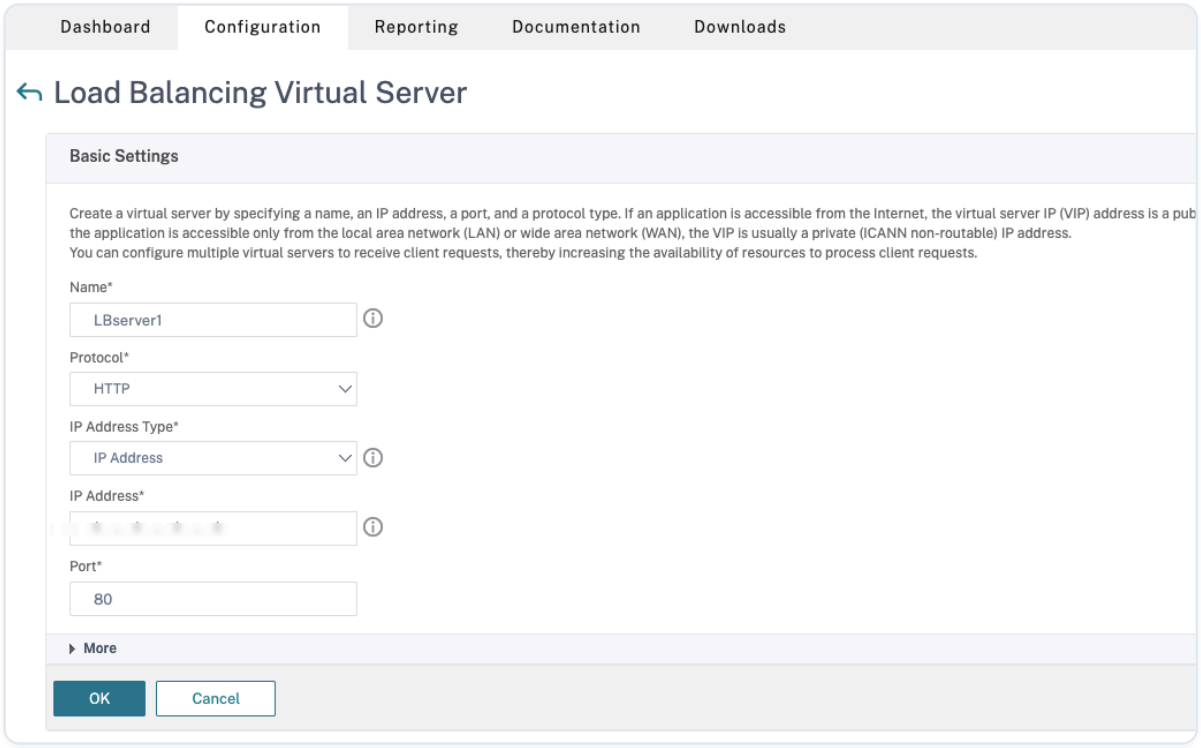
   a. **アクション**で、前の手順で作成したアクションを選択します。
   b. **式**に「HTTP.REQ.IS_VALID」を追加します。
   c. **OK**をクリックします。

4. 負荷分散を設定します。STAサーバーごとに1つの負荷分散仮想サーバーを構成する必要があります。構成しない場合、セッションの起動に失敗します。

   詳細については、基本的な負荷分散のセットアップを参照してください。

   a. 負荷分散仮想サーバーを作成します。

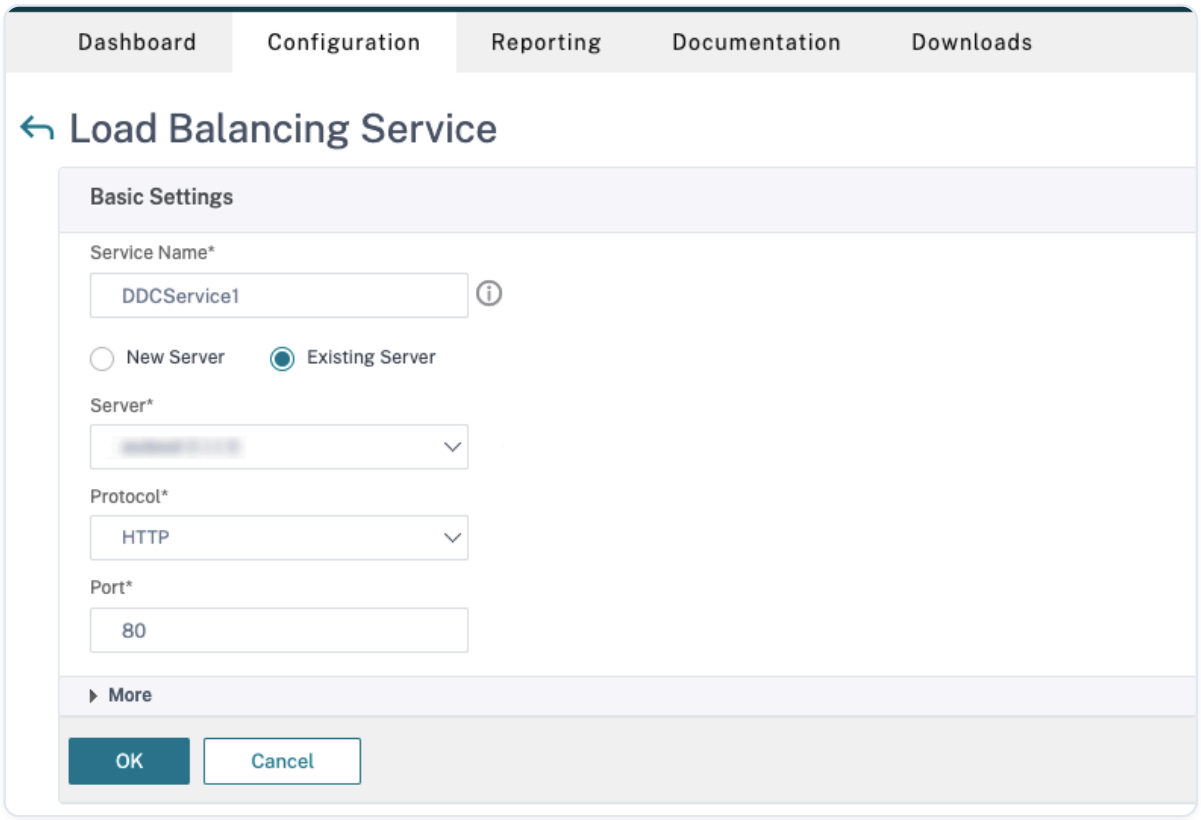
      - **トラフィック管理 > 負荷分散 > サーバー** に移動します。
      - 「**仮想サーバー**」ページで、「**追加**」をクリックします。



- **Protocol**で、**HTTP**を選択します。
- 負荷分散仮想IPアドレスを追加し、**Port**で**80**を選択します。
- **OK**をクリックします。

b. 負荷分散サービスを作成します。

- **トラフィック管理 > 負荷分散 > サービス** に移動します。



- 「**既存のサーバー**」で、前の手順で作成した仮想サーバーを選択します。
- 「**プロトコル**」で「**HTTP**」を選択し、「**ポート**」で「**80**」を選択します。
- 「**OK**」をクリックし、次に「**完了**」をクリックします。

c. サービスを仮想サーバーにバインドします。

- 以前に作成した仮想サーバーを選択し、「**編集**」をクリックします。
- 「**サービスとサービスグループ**」で、「**ロードバランシング仮想サーバーサービスバインディングなし**」をクリックします。

仮想サーバーにサービスをバインド(/en-us/citrix-virtual-apps-desktops/2411/media/adc-bind-service-to-lbvserver.png)

- **Service Binding**で、以前に作成したサービスを選択します。
- **バインド**をクリックします。

d. 以前に作成した書き換えポリシーを仮想サーバーにバインドします。

- 以前に作成した仮想サーバーを選択し、「**編集**」をクリックします。
- 「**詳細設定**」で「**ポリシー**」をクリックし、次に「**ポリシー**」セクションで「**+**」をクリックします。

書き換えポリシーをバインド(/en-us/citrix-virtual-apps-desktops/2411/media/adc-bind-rewrite-policy.png)

- **ポリシーの選択**で**書き換え**を選択し、**タイプの選択**で**要求**を選択します。
- **続行**をクリックします。
- **ポリシーの選択**で、以前に作成した書き換えポリシーを選択します。
- **バインド**をクリックします。
- **完了**をクリックします。

e. 必要に応じて、仮想サーバーの永続性を設定します。

- 以前に作成した仮想サーバーを選択し、**編集**をクリックします。
- **詳細設定**で、**永続性**をクリックします。

永続性の設定(/en-us/citrix-virtual-apps-desktops/2411/media/adc-lb-vserver-persistence.png)

- 永続性の種類として「**その他**」を選択します。

- 「**DESTIP**」を選択して、仮想サーバーによって選択されたサービスのIPアドレス (宛先IPアドレス) に基づいて永続セッションを作成します。
- 「**IPv4ネットマスク**」で、DDCと同じネットワークマスクを追加します。
- 「**OK**」をクリックします。

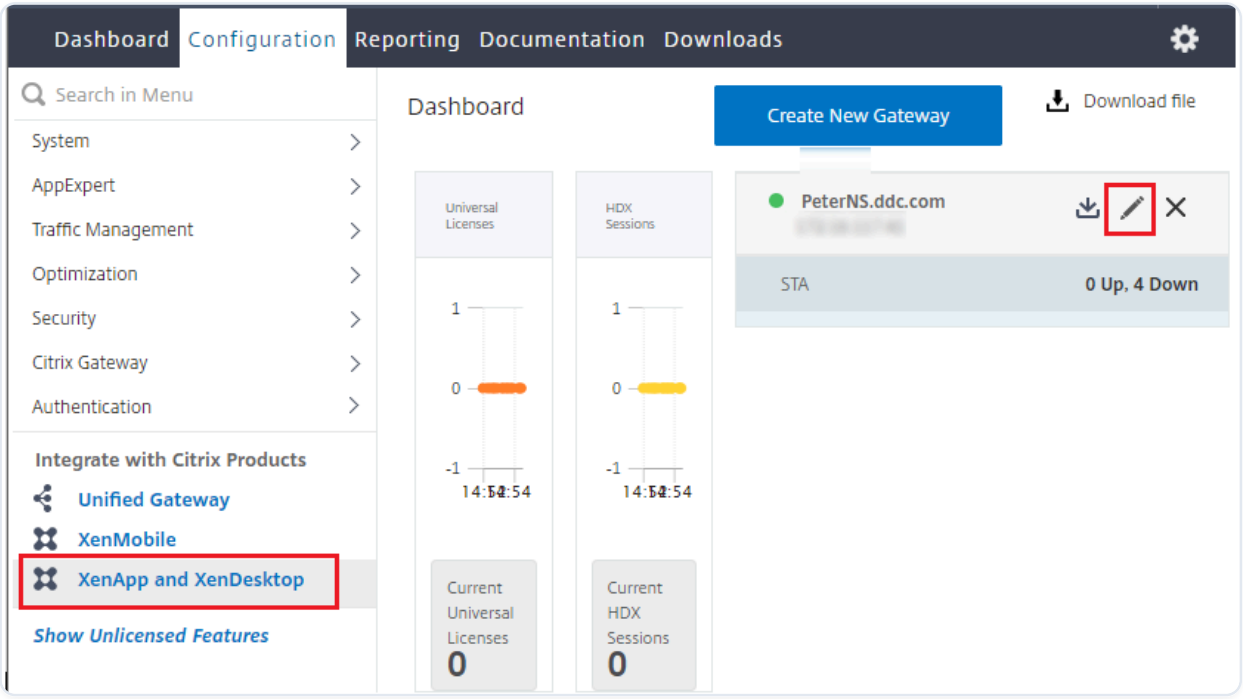
f. 他の仮想サーバーについても、これらの手順を繰り返します。

Citrix ADCアプライアンスがCitrix Virtual Desktops™で既に構成されている場合の構成の変更

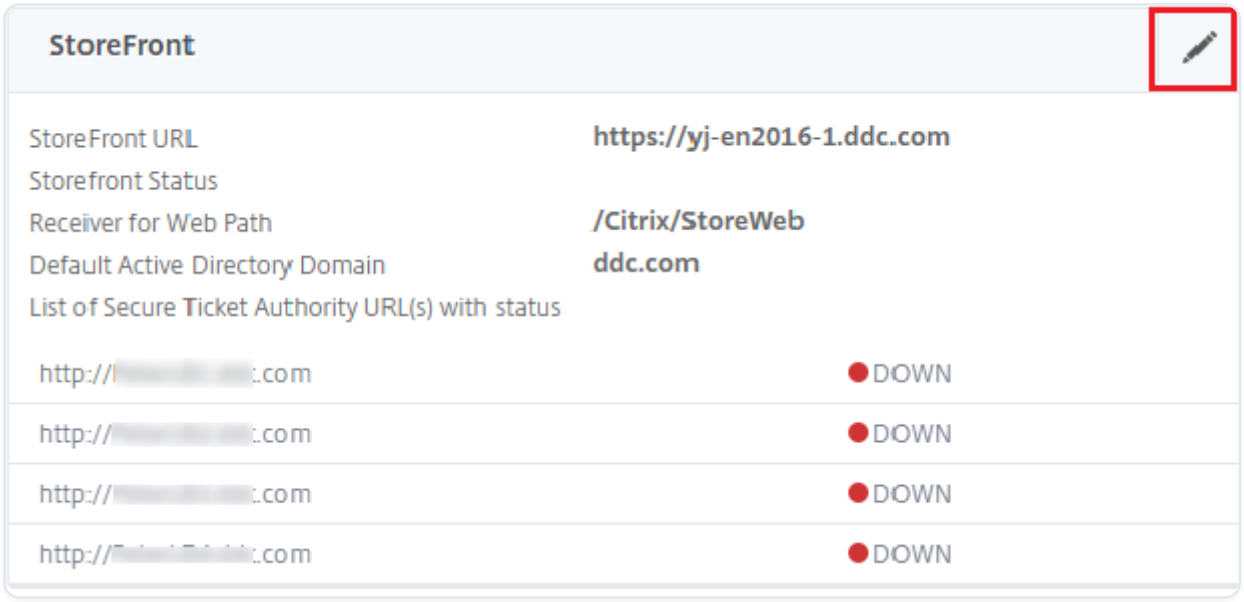
Citrix ADCアプライアンスをCitrix Virtual Desktopsで既に構成している場合、Secure XML機能を使用するには、以下の構成変更を行う必要があります。

- セッション起動前に、ゲートウェイの「**セキュリティチケット機関のURL**」を変更して、負荷分散仮想サーバーのFQDNを使用するようにします。
- `TrustRequestsSentToTheXmlServicePort`パラメーターがFalseに設定されていることを確認します。デフォルトでは、`TrustRequestsSentToTheXmlServicePort`パラメーターはFalseに設定されています。ただし、お客様がCitrix Virtual Desktops用にCitrix ADCをすでに構成している場合、`TrustRequestsSentToTheXmlServicePort`はTrueに設定されます。

1. Citrix ADC GUIで、**［Configuration］>［Integrate with Citrix Products］**の順に選択し、［XenApp and XenDesktop®］**をクリックします。
2. ゲートウェイインスタンスを選択し、編集アイコンをクリックします。

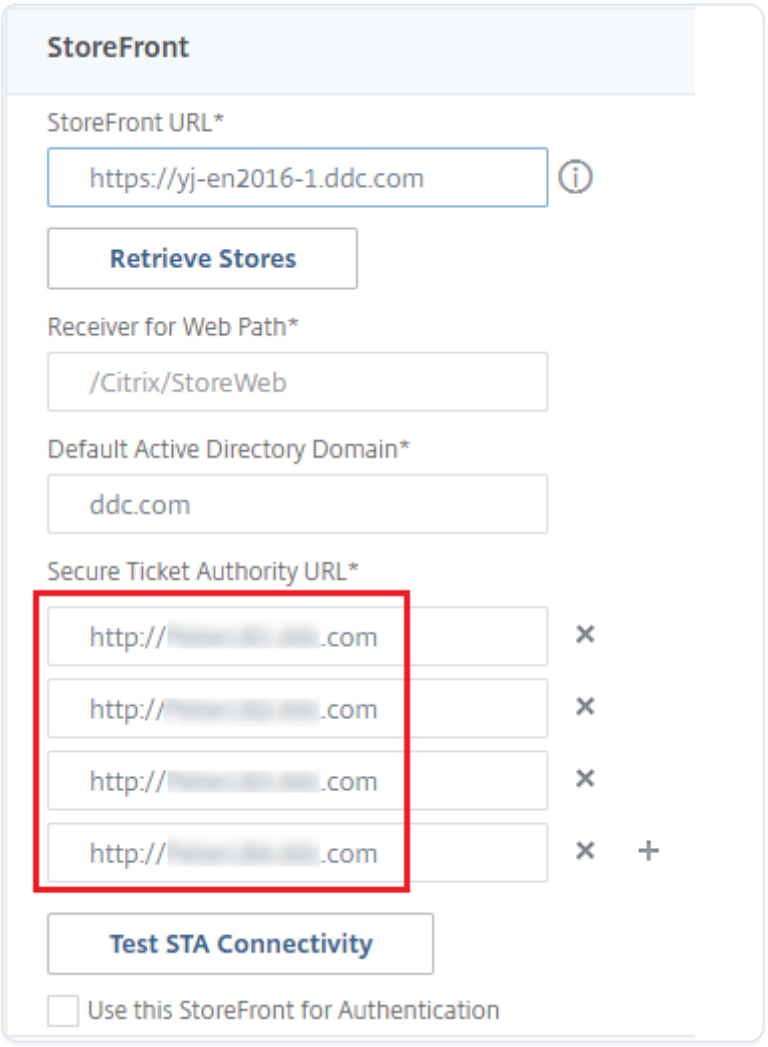


3. StoreFrontペインで、編集アイコンをクリックします。



4. **Secure Ticket Authority URL**を追加します。

   - Secure XML機能が有効になっている場合、STA URLは負荷分散サービスのURLである必要があります。
   - Secure XML機能が無効になっている場合、STA URLはSTAのURL（DDCのアドレス）である必要があり、DDC上の`TrustRequestsSentToTheXmlServicePort`パラメーターはTrueに設定する必要があります。



セッションの回復性設定

セッションアクティビティを維持することは、最高のユーザーエクスペリエンスを提供するために不可欠です。信頼性の低いネットワーク、非常に変動するネットワーク遅延、ワイヤレスデバイスの範囲制限による接続の喪失は、ユーザーの不満につながる可能性があります。デバイス間を素早く移動し、ログオンするたびに同じアプリケーションにアクセスすることは、医療従事者などの多くのモバイルワーカーにとって優先事項です。

この記事で説明する機能は、セッションの信頼性を最適化し、不便さ、ダウンタイム、生産性の損失を軽減します。これらの機能を使用することで、モバイルユーザーはデバイス間を迅速かつ簡単にローミングできます。

セッションの信頼性

セッションの信頼性により、ネットワーク接続が中断されてもセッションがアクティブな状態に保たれ、ユーザーの画面に表示されます。ユーザーは、ネットワーク接続が再開されるまで、使用しているアプリケーションを引き続き見ることができます。

この機能は、ワイヤレス接続を使用するモバイルユーザーにとって特に便利です。たとえば、ワイヤレス接続を使用しているユーザーが鉄道トンネルに入り、一時的に接続が失われたとします。通常、セッションは切断されてユーザーの画面から消え、ユーザーは切断されたセッションに再接続する必要があります。セッションの信頼性を使用すると、セッションはマシン上でアクティブなままになります。接続が失われたことを示すために、ユーザーのディスプレイはフリーズし、カーソルはトンネルの反対側で接続が再開されるまで回転する砂時計に変わります。ユーザーは中断中もディスプレイにアクセスし続け、ネットワーク接続が復元されるとアプリケーションとの対話を再開できます。セッションの信頼性は、再認証のプロンプトなしでユーザーを再接続します。

Citrix Workspace™アプリのユーザーは、Controllerの設定を上書きできません。

セッションの信頼性は、Transport Layer Security (TLS) とともに使用できます。TLS は、ユーザーデバイスと Citrix Gateway 間で送信されるデータのみを暗号化します。

次のポリシー設定でセッションの信頼性を有効にして構成します。

- 「セッションの信頼性接続」ポリシー設定は、セッションの信頼性を許可または禁止します。
- 「セッションの信頼性タイムアウト」ポリシー設定のデフォルトは180秒、つまり3分です。セッションの信頼性がセッションを開いたままにする時間を延長することはできますが、この機能はユーザーの利便性のために設計されています。そのため、ユーザーに再認証を促すことはありません。セッションを開いたままにする時間を延長すると、ユーザーが注意散漫になり、ユーザーデバイスから離れてしまう可能性が高まります。これらの行動により、セッションが不正なユーザーにアクセスされる可能性があります。
- 受信セッションの信頼性接続は、ポート番号を「セッションの信頼性ポート番号」ポリシー設定で変更しない限り、ポート2598を使用します。
- ユーザーが再認証なしで中断されたセッションに再接続するのを防ぐには、自動クライアント再接続機能を使用します。「自動クライアント再接続認証」ポリシー設定を構成して、中断されたセッションに再接続する際にユーザーに再認証を促すことができます。

セッションの信頼性と自動クライアント再接続の両方を使用する場合、これら2つの機能は順次動作します。セッションの信頼性は、「セッションの信頼性タイムアウト」ポリシー設定で指定した時間の経過後、ユーザーセッションを閉じるか、切断します。その後、自動クライアント再接続ポリシー設定が有効になり、ユーザーを切断されたセッションに再接続しようとします。

クライアントの自動再接続

Auto Client Reconnect 機能を使用すると、Citrix Workspace アプリは意図しない ICA® セッションの切断を検出し、影響を受けるセッションにユーザーを自動的に再接続できます。この機能がサーバーで有効になっている場合、ユーザーは手動で再接続することなく作業を続行できます。

アプリケーションセッションの場合、Citrix Workspace アプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルするまで、セッションへの再接続を試行します。

デスクトップセッションの場合、Citrix Workspace アプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルしない限り、指定された期間、セッションへの再接続を試行します。デフォルトでは、この期間は5分です。この期間を変更するには、ユーザーデバイスで次のレジストリ設定を編集します（`seconds` は、セッションの再接続がそれ以上試行されなくなるまでの秒数です）。

`HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>`

次のポリシー設定を使用して、Auto Client Reconnect を有効にして構成します。

- **Auto Client Reconnect:** 接続が中断された後、Citrix Workspace アプリによる自動再接続を有効または無効にします。
- **Auto Client Reconnect 認証:** 自動再接続後のユーザー認証の要件を有効または無効にします。
- **Auto Client Reconnect ログ記録:** イベントログへの再接続イベントのログ記録を有効または無効にします。ログ記録はデフォルトで無効になっています。有効にすると、サーバーのシステムログに、成功および失敗した自動再接続イベントに関する情報が記録されます。各サーバーは、再接続イベントに関する情報を独自のシステムログに保存します。サイトは、すべてのサーバーの再接続イベントの統合ログを提供しません。

注：

再認証なしの Auto Client Reconnect は、パスワード認証でのみサポートされます。フェデレーション認証サービスまたはスマートカード認証を使用している場合、再認証なしの Auto Client Reconnect はサポートされません。そのような場合、ユーザーはログイン画面にリダイレクトされます。

Auto Client Reconnect は、暗号化されたユーザー資格情報に基づく認証メカニズムを組み込んでいます。ユーザーが最初にログオンすると、サーバーはユーザー資格情報を暗号化してメモリに保存します。サーバーはまた、暗号化キーを含む Cookie を作成し、Citrix Workspace アプリに送信します。Citrix Workspace アプリは、再接続のためにキーをサーバーに送信します。サーバーは資格情報を復号化し、認証のために Windows ログオンに送

> 信します。Cookie の有効期限が切れると、ユーザーはセッションに再接続するために再認証する必要があります。

Auto Client Reconnect 認証設定を有効にしている場合、Cookie は使用されません。代わりに、Citrix Workspace アプリが自動的に再接続しようとすると、資格情報を要求するダイアログボックスがユーザーに表示されます。

ユーザー資格情報とセッションを最大限に保護するために、クライアントとサイト間のすべての通信に暗号化を使用してください。

icaclient.adm ファイルを使用して、Windows 向け Citrix Workspace アプリで Auto Client Reconnect を無効にします。詳細については、お使いの Windows 向け Citrix Workspace アプリのバージョンのドキュメントを参照してください。

接続の設定も Auto Client Reconnect に影響します。

- デフォルトでは、前述のとおり、サイトレベルのポリシー設定によって自動クライアント再接続が有効になっています。ユーザーの再認証は不要です。ただし、サーバーのICA TCP接続が、通信リンクが切断されたセッションをリセットするように構成されている場合、自動再接続は行われません。自動クライアント再接続は、サーバーが切断された接続またはタイムアウトした接続でセッションを切断する場合にのみ機能します。このコンテキストでは、ICA TCP接続とは、TCP/IPネットワーク上のセッションに使用されるサーバーの仮想ポート（実際のネットワーク接続ではなく）を指します。
- デフォルトでは、サーバー上のICA TCP接続は、切断された接続またはタイムアウトした接続でセッションを切断するように設定されています。切断されたセッションはシステムメモリにそのまま残り、Citrix Workspaceアプリによる再接続が可能です。
- 接続は、切断された接続またはタイムアウトした接続でセッションをリセットまたはログオフするように構成できます。セッションがリセットされると、再接続を試みると新しいセッションが開始されます。ユーザーが使用中のアプリケーションの同じ場所に戻るのではなく、アプリケーションが再起動されます。
- サーバーがセッションをリセットするように構成されている場合、自動クライアント再接続は新しいセッションを作成します。このプロセスでは、ユーザーがサーバーにログオンするために資格情報を入力する必要があります。
- Citrix Workspaceアプリまたはプラグインが誤った認証情報を送信した場合（攻撃中に発生する可能性あり）、またはサーバーが切断された接続を検出してから時間が経ちすぎたと判断した場合、自動再接続は失敗する可能性があります。

ICA キープアライブ

ICAキープアライブ機能を有効にすると、切断された接続が切断されるのを防ぎます。有効にすると、サーバーがアクティビティを検出しない場合、この機能はリモートデスクトップサービスがそのセッションを切断するのを防ぎます。アクティビティがない例としては、クロックの変更がない、マウスの動きがない、画面の更新がないなどが挙げられます。サーバーは数秒ごとにキープアライブパケットを送信して、セッションがアクティブであるかどうかを検出します。セッションがアクティブでなくなった場合、サーバーはそのセッションを切断済みとしてマークします。

> **重要：**
>
> ICAキープアライブは、セッションの信頼性を使用していない場合にのみ機能します。セッションの信頼性には、切断された接続が切断されるのを防ぐ独自のメカニズムがあります。セッションの信頼性を使用しない接続にのみICAキープアライブを構成してください。

> ICA Keep-Alive設定は、Windowsグループポリシーで構成されているキープアライブ設定を上書きします。

次のポリシー設定を使用して、ICA Keep-Aliveを有効にして構成します。

- **ICAキープアライブタイムアウト：** ICAキープアライブメッセージの送信に使用する間隔（1〜3600秒）を指定します。切断された接続が非常にまれで、ユーザーがセッションに再接続できることが問題にならない環境で、ネットワーク監視ソフトウェアに非アクティブな接続を閉じさせたい場合は、このオプションを構成しないでください。

  デフォルトの間隔は60秒です。ICAキープアライブパケットは60秒ごとにユーザーデバイスに送信されます。ユーザーデバイスが60秒以内に応答しない場合、ICAセッションのステータスは切断済みに変わります。
- **ICAキープアライブ：** ICAキープアライブメッセージを送信するか、送信を防止します。

ワークスペースコントロール

ワークスペースコントロールを使用すると、デスクトップとアプリケーションがユーザーをあるデバイスから別のデバイスへと追跡できます。このローミング機能により、ユーザーはログオンするだけで、どこからでもすべてのデスクトップまたは開いているアプリケーションにアクセスでき、各デバイスでデスクトップやアプリケーションを再起動する必要がありません。たとえば、ワークスペースコントロールは、病院で異なるワークステーション間を迅速に移動し、ログオンするたびに同じアプリケーションセットにアクセスする必要がある医療従事者を支援できます。ワークスペースコントロールオプションを許可するように構成すると、これらの医療従事者は1つのクライ

アントデバイスで複数のアプリケーションから切断し、別のクライアントデバイスで同じアプリケーションに再接続できます。

ワークスペースコントロールは、次のアクティビティに影響します。

- **ログオン:** デフォルトでは、ワークスペースコントロールにより、ユーザーはログオン時に実行中のすべてのデスクトップとアプリケーションに自動的に再接続でき、手動で再開する必要がありません。ワークスペースコントロールを通じて、ユーザーは切断されたデスクトップまたはアプリケーション、および別のクライアントデバイスでアクティブなものを開くことができます。デスクトップまたはアプリケーションから切断すると、それはサーバー上で実行されたままになります。一部のデスクトップまたはアプリケーションを1つのクライアントデバイスで実行したまま、別のクライアントデバイスでデスクトップまたはアプリケーションのサブセットに再接続する必要があるローミングユーザーがいる場合、ログオン再接続動作を、ユーザーが以前に切断したデスクトップまたはアプリケーションのみを開くように構成できます。
- **再接続:** サーバーにログオンした後、ユーザーはいつでも「再接続」をクリックして、すべてのデスクトップまたはアプリケーションに再接続できます。デフォルトでは、「再接続」は切断されたデスクトップまたはアプリケーション、および現在別のクライアントデバイスで実行されているものを開きます。ユーザーが以前に切断したデスクトップまたはアプリケーションのみを開くように「再接続」を構成できます。
- **ログオフ:** StoreFront™を介してデスクトップまたはアプリケーションを開くユーザーの場合、**ログオフ**コマンドを構成して、StoreFrontとすべてのアクティブなセッションからユーザーをログオフするか、StoreFrontのみからログオフすることができます。
- **切断:** ユーザーは、個別に切断する必要なく、実行中のすべてのデスクトップとアプリケーションから一度に切断できます。

ワークスペースコントロールは、Citrix StoreFront接続を介してデスクトップとアプリケーションにアクセスするCitrix Workspaceアプリユーザーのみが利用できます。デフォルトでは、仮想デスクトップセッションではワークスペースコントロールは無効になっていますが、ホスト型アプリケーションでは有効になっています。公開されたデスクトップと、それらのデスクトップ内で実行されている公開されたアプリケーションの間では、デフォルトではセッション共有は行われません。

ユーザーが新しいクライアントデバイスに移動すると、ユーザーポリシー、クライアントドライブマッピング、およびプリンター構成が適切に変更されます。ポリシーとマッピングは、ユーザーがセッションにログオンしているクライアントデバイスに従って適用されます。たとえば、医療従事者が救急治療室のデバイスからログオフし、X線検査室のワークステーションにログオンします。X線検査室でのセッションに適したポリシー、プリンターマッピング、およびクライアントドライブマッピングは、セッション開始時に有効になります。

ユーザーが場所を変更したときに表示されるプリンターをカスタマイズできます。また、ユーザーがローカルプリンターに印刷できるかどうか、ユーザーがリモートで接続したときに消費される帯域幅の量、および印刷エクスペリエンスのその他の側面を制御することもできます。

ユーザーのワークスペースコントロールを有効にして構成する方法については、StoreFrontのドキュメントを参照してください。

セッションローミング

> **注記:**
>
> 以下の情報は、PowerShellを使用してセッションローミングを構成するためのガイドです。代わりにWeb Studioを使用することもできます。詳細については、「デリバリーグループの管理」を参照してください。

> デフォルトでは、セッションはユーザーとともにクライアントデバイス間をローミングします。ユーザーがセッションを起動し、別のデバイスに移動すると、同じセッションが使用され、アプリケーションは両方のデバイスで利用可能になります。アプリケーションは、デバイスや現在のセッションの有無にかかわらず追跡されます。多くの場合、アプリケーションに割り当てられたプリンターやその他のリソースも追跡されます。

このデフォルトの動作には多くの利点がありますが、すべての場合に理想的とは限りません。PowerShell SDKを使用してセッションローミングを防止できます。

例1：医療従事者が2つのデバイスを使用しており、デスクトップPCで保険フォームを完成させ、タブレットで患者情報を閲覧しています。

- セッションローミングが有効になっている場合、両方のアプリケーションが両方のデバイスに表示されます（1つのデバイスで起動されたアプリケーションは、使用中のすべてのデバイスで表示されます）。これはセキュリティ要件を満たさない可能性があります。
- セッションローミングが無効になっている場合、患者記録はデスクトップPCに表示されず、保険フォームはタブレットに表示されません。

例2：生産管理者がオフィスにあるPCでアプリケーションを起動します。デバイス名と場所によって、そのセッションで利用可能なプリンターやその他のリソースが決まります。その日の後半、彼は会議のために隣の建物のオフィスに行き、そこでプリンターを使用する必要があります。

- セッションローミングが有効になっている場合、生産管理者は会議室近くのプリンターにアクセスできない可能性があります。なぜなら、彼がオフィスで以前に起動したアプリケーションによって、その場所近くのプリンターやその他のリソースが割り当てられたためです。
- セッションローミングが無効になっている場合、彼が別のマシンに（同じ資格情報を使用して）ログオンすると、新しいセッションが開始され、近くのプリンターやリソースが利用可能になります。

セッションローミングの構成

セッションローミングを構成するには、「SessionReconnection」プロパティを持つ以下のエンタイトルメントポリシー規則コマンドレットを使用します。オプションで、「LeasingBehavior」プロパティも指定できます。

デスクトップセッションの場合：

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

アプリケーションセッションの場合：

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

`value` には、次のいずれかを指定できます。

- **Always:** クライアントデバイスやセッションが接続されているか切断されているかに関係なく、セッションは常にローミングします。これがデフォルト値です。
- **DisconnectedOnly:** 既に切断されているセッションにのみ再接続します。それ以外の場合は、新しいセッションを起動します。（セッションは、まず切断するか、Workspace Control を使用して明示的にローミングすることで、クライアントデバイス間をローミングできます。）別のクライアントデバイスからのアクティブな接続済みセッションは決して使用されません。代わりに、新しいセッションが起動されます。
- **SameEndpointOnly:** ユーザーは使用するクライアントデバイスごとに一意のセッションを取得します。これにより、ローミングが完全に無効になります。ユーザーは、以前セッションで使用したのと同じデバイスにのみ再接続できます。

"LeasingBehavior" プロパティについては、以下で説明します。

他の設定からの影響:

セッションローミングの無効化は、デリバリーグループのアプリケーションのプロパティにあるアプリケーション制限 **ユーザーごとにアプリケーションのインスタンスを1つのみ許可する** の影響を受けます。

- セッションローミングを無効にする場合は、「アプリケーションのインスタンスを1つのみ許可する...」アプリケーション制限を無効にします。
- 「アプリケーションのインスタンスを1つのみ許可する...」アプリケーション制限を有効にする場合は、新しいデバイスで新しいセッションを許可する2つの値のいずれも構成しないでください。

ログオン間隔

デスクトップVDAを含む仮想マシンがログオンプロセス完了前に閉じられた場合、そのプロセスにより多くの時間を割り当てることができます。バージョン7.6以降のデフォルトは180秒です（バージョン7.0〜7.5のデフォルトは90秒です）。

マシン（またはマシンカタログで使用されるマスターイメージ）で、次のレジストリキーを設定します。

キー: `HKLM\SOFTWARE\Citrix\PortICA`

- 値: `AutoLogonTimeout`
- 種類: `DWORD`
- 0〜3600の範囲で、秒単位の10進数を指定します。

マスターイメージを変更した場合は、カタログを更新します。

この設定は、デスクトップVDAを搭載したVMにのみ適用されます。サーバーVDAを搭載したマシンでのログオンタイムアウトは、Microsoftによって制御されます。

設定

> **注:**
>
> Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> Web Studioを使用して、次の設定を管理できます。

- 認証の管理
- Studioログインページのデフォルトドメイン名を設定する
- Citrixカスタマーエクスペリエンス向上プログラム
- デリバリーコントローラーの削除
- データベースの場所を変更する
- 日付と時刻の設定
- サイト管理の一元化
- リモートPCアクセスでの複数ユーザーの自動割り当てを有効にする
- DNS解決の有効化
- XML信頼の有効化
- セキュリティキーの管理
- Studioコンソールの非アクティビティタイムアウトを設定する(#set-the-inactivity-timeout-for-the-studio-console)

認証の管理

デフォルトでは、ユーザーはドメインのユーザー名とパスワードを使用してWeb Studioにログオンします。スマートカード認証や統合Windows認証など、ユーザーに対して別の認証方法を選択することもできます。

Studioを使用した管理

ユーザーの認証方法を選択するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**設定**を選択します。
2. **認証**タイルを見つけて、**編集**をクリックし、オプションを選択します。

    - **ドメイン資格情報**
    - **ドメイン資格情報または統合 Windows 認証**

      統合 Windows 認証が有効になっている場合、ユーザーは Windows 資格情報 (Kerberos/NTLM) またはクライアント証明書を使用して Web Studio にアクセスできます。

      Web StudioとDelivery Controller™が異なるマシンにインストールされている場合、統合Windows認証を機能させるには、クロスオリジンアクセスを許可を有効にし、Web StudioサーバーのURLを許可リストに追加します。

> **重要**
>
> Web StudioがDelivery Controllerのプロキシとして構成されている場合、統合Windows認証は機能しません。

- **スマートカード認証**
- **ドメイン資格情報またはスマートカード認証**

  スマートカード認証を有効にするには追加の設定が必要です。詳細については、Web Studio 用スマートカード認証のセットアップを参照してください。

PowerShell スクリプトを使用して管理

認証方法は Delivery Controller データベースで構成されます。次の PowerShell スクリプトを使用して認証方法を設定できます。

1. Delivery Controller で次のコマンドを実行して、現在のサイト ID を取得します。

   `Get-ConfigSite | Select SiteGuid`

2. 以下のスクリプトを実行して認証方法を設定します。

```
# Generate a new bearer token

$bearerData = New-TrustBearerToken

# Define the Delivery Controller DNS name and Site ID

$ddc = "ddc.dc.com" # replace this with the Delivery Controller's DNS
name

$siteid = "c68a8f89-42af-4bea-a6e9-c8c936353f49" # replace this with
the site ID you get from step #1

# Define the URL and headers

$url = "https://$ddc/citrix/orchestration/api/CitrixOnPremises/Sites/
$siteid/Settings"

$headers = @{

"Content-Type" = "application/json"
```

```
"Authorization" = "Bearer $($bearerData.Token)"

}

# Define the JSON body

$body = @{

SupportedAuthenticators = "BasicAndSmartCard" # replace this with a
required authentication method: "Basic" for "Domain credentials";
"BasicAndIntegratedWindowsAuthentication" for "Domain credentials or
integrated Windows authentication"; "BasicAndSmartCard" for "Domain
credentials or smart card authentication"; "SmartCard" for "Smart card
authentication"

} | ConvertTo-Json -Depth 10

# Send the PATCH request

Invoke-RestMethod -Uri $url -Method Patch -Headers $headers -Body $body
```

統合Windows認証のためにブラウザを構成する

ドメイン資格情報または統合Windows認証を使用して*統合Windows認証*を有効にすると、ユーザーが次回サインインするときに、自動的にサインインされます。ユーザーとして自動的にサインインできない場合は、以下の手順に従ってWebブラウザを構成し、統合Windows認証を許可してください。

Google Chromeの場合：

1. コントロールパネルから、**インターネットオプション**を選択します。
2. **詳細設定**タブを選択します。
3. **統合Windows認証を有効にする**を選択します。
4. **セキュリティ**タブを選択します。
5. **ローカルイントラネット > サイト > 詳細設定**を選択します。
6. **このWebサイトをゾーンに追加する**ボックスで：
    - Web Studio と Delivery Controller が同じサーバー上にある場合は、Web Studio を実行しているホストの URL を入力します。

- そうでない場合は、ワイルドカードドメインを入力します。例: Delivery Controller が `ddc.domain.com` にある場合、`*.domain.com` と入力します。

7. **追加 > 閉じる** をクリックします。

Mozilla Firefox の場合:

1. ブラウザから、URL ボックスに `about:config` と入力します。
2. **検索** ボックスに `network negotiate` と入力します。
3. **network.negotiate-auth.trusted-uris** を右クリックし、**変更** を選択します。
4. **文字列値を入力** ボックスで:

   - Web Studio と Delivery Controller が同じサーバー上にある場合は、Web Studio をホストしているサーバー名を参照する URL および/またはエイリアスのコンマ区切りリストを追加します。
   - そうでない場合は、次のように URL を追加します。例: Delivery Controller が `ddc.domain.com` にある場合、`*.domain.com` と入力します。

ブラウザを設定したら、サインインページで **Windows 統合サインイン** をクリックして再試行できます。

Web Studio と Delivery Controller が異なるマシンにインストールされている場合、統合 Windows 認証を機能させるには、**クロスオリジンアクセスを許可** を有効にする必要があります。

クロスオリジンアクセスを許可 を有効にするには、次の手順に従います。

1. **クロスオリジンアクセスを許可** チェックボックスをオンにします。
2. Web Studio サーバーの URL を許可リストに追加します。
3. 「**URLを入力**」フィールドにURLを入力します。必要に応じて「**追加**」をクリックしてさらに追加します。

> **注**
>
> - URLは正しい形式 `<scheme>://<hostname>` に従う必要があります。パスや末尾のスラッシュを含まないようにしてください。
> - IPアドレスとFQDNがサポートされています。URLを追加する際は、Web Studioへのアクセス方法に対応していることを確認してください。たとえば、IPアドレスを使用

してWeb Studioにアクセスする場合は、IPアドレスベースのURLをリストに追加します。

- デフォルト以外のポートを使用する場合は、ポート番号を含めるようにしてください。

4. 必要に応じて、「**追加**」をクリックしてさらに追加します。
5. 完了したら、「**完了**」をクリックして保存し、終了します。

Studioログインページのデフォルトドメイン名を設定する

Studioログインページの**ドメイン**フィールドにドメイン名を自動入力するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで設定を選択します。
2. **ドメイン名の構成**タイルで、必要に応じてドメイン名を入力します。
3. **適用**をクリックします。

   管理者がStudioログインページにアクセスすると、「*ドメイン*」フィールドに設定したドメイン名が自動的に入力されます。

タイムゾーンを設定する

日付と時刻の形式を好みに合わせてカスタマイズするには、次の手順に従います。

1. Web Studio にサインインし、左ペインで **設定** を選択します。
2. **日付と時刻** タイルを見つけ、**編集** をクリックして次のオプションを構成します。
   - **時刻形式:**
     - 12時間形式 (例: 午後09:00) または24時間形式 (例: 21:00) で時刻を表示するように選択します。
   - **日付形式:**
     - yyyy/MM/dd のように、好みに合わせて日付形式を構成します。
   - **タイムゾーン:**
     - **UTC:** ユーザーインターフェイス全体で日付と時刻をUTCで表示します。日付と時刻にマウスを合わせると、その情報がローカルタイムゾーンで表示されます。

- **ローカルタイムゾーン:** ユーザーインターフェイス全体で日付と時刻をローカルタイムゾーンで表示します。日付と時刻にマウスを合わせると、その情報がUTCで表示されます。

> **注:**
>
> これらの設定は、各ユーザーアカウントに固有のものです。

DNS解決を有効にする

ICA® ファイルでIPアドレスの代わりにDNS名を表示するには、次の手順に従います。

1. Web Studio にサインインし、左ペインで **設定** を選択します。
2. **DNS解決を有効にする** 設定をオンにします。

Studioコンソールの非アクティブタイムアウトを設定する

管理者がStudioコンソールから自動的にサインアウトされるまでの非アクティビティ期間を設定できます。

1. Web Studioにサインインし、左ペインで**設定**を選択します。
2. 10分から24時間の範囲で期間を入力します。
3. この設定を適用するには、ページを更新するか、サインアウトしてから再度サインインしてください。

サイト管理の一元化

この機能を使用すると、1つのWeb Studioコンソールで複数のCitrix Virtual Apps and Desktopsサイトを管理できます。詳細については、「複数のサイト管理を有効にする」を参照してください。

タグ

> **注:**
>
> Citrix Virtual Apps and Desktops™の展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb

> Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

タグは、マシン、アプリケーション、デスクトップ、デリバリーグループ、アプリケーショングループ、ポリシーなどの項目を識別する文字列です。タグを作成して項目に追加すると、特定のタグを持つ項目にのみ適用されるように特定の操作を調整できます。

- Web Studioでの検索表示を調整します。

  たとえば、テスター向けに最適化されたアプリケーションのみを表示するには、「test」という名前のタグを作成し、それらのアプリケーションに追加（適用）します。これで、Web Studioの検索を「test」タグでフィルタリングできます。

- アプリケーショングループからアプリケーションを公開したり、デリバリーグループから特定のデスクトップを公開したりする際に、選択したデリバリーグループ内のマシンの一部のみを考慮します。これは*タグ制限*と呼ばれます。

  タグ制限を使用すると、既存のマシンを複数の公開タスクに使用できるため、追加のマシンを展開および管理するコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）するものと考えることができます。その機能は、XenApp 7.xより前のリリースにおけるワーカーグループと似ていますが、同一ではありません。

  タグ制限付きのアプリケーショングループまたはデスクトップを使用すると、デリバリーグループ内のマシンの一部を分離してトラブルシューティングする際に役立ちます。

- デリバリーグループ内のマシンの一部に対して定期的な再起動をスケジュールします。

  マシンにタグ制限を使用すると、新しいPowerShellコマンドレットを使用して、デリバリーグループ内のマシンの一部に対して複数の再起動スケジュールを構成できます。例と詳細については、「デリバリーグループの管理」を参照してください。

- Citrixポリシーの適用（割り当て）を、指定されたタグを持つ（または持たない）デリバリーグループ、デリバリーグループの種類、またはOU内のマシンの一部に調整します。

  たとえば、より強力なワークステーションにのみCitrixポリシーを適用したい場合は、それらのマシンに「high power」という名前のタグを追加します。次に、ポリシー作成ウィザードの**［ポリシーの割り当て］**ページで、そのタグと［有効にする］**チェックボックスを選択します。デリバリーグループにタグを追加し、そのグループにCitrixポリシーを適用することもできます。詳細については、「ポリシーの作成」を参照してください。

タグは以下に適用できます。

- マシン
- アプリケーション
- マシンカタログ (PowerShell のみ。(#tags-on-machine-catalogs)を参照)
- デリバリーグループ
- アプリケーショングループ

Web Studio で以下を作成または編集する際に、タグ制限を構成できます。

- 共有デリバリーグループ内のデスクトップ
- アプリケーショングループ

> **重要:**
>
> タグは、明示的にマシンに適用することも、マシンカタログまたはデリバリーグループレベルで明示的に適用することもできます。タグがマシンカタログまたはデリバリーグループレベルで適用されると、そのカタログまたはデリバリーグループ内のすべてのマシンが暗黙的にそのタグを継承します。これらの継承されたタグは、マシンレベルで削除することはできません。タグの効果を削除するには、マシンカタログまたはデリバリーグループレベルからタグを削除する必要があります。

デスクトップまたはアプリケーショングループのタグ制限

タグ制限にはいくつかの手順があります。

- タグを作成し、マシンに追加（適用）します。
- タグ制限付きのグループを作成または編集します（つまり、「タグ x の付いたマシンへの起動を制限する」）。

タグ制限は、ブローカーのマシン選択プロセスを拡張します。ブローカーは、アクセスポリシー、構成されたユーザーリスト、ゾーン設定、起動準備状況、およびタグ制限（存在する場合）に従って、関連付けられたデリバリーグループからマシンを選択します。アプリケーションの場合、ブローカーは優先順位に従って他のデリバリーグループにフォールバックし、検討対象の各デリバリーグループに同じマシン選択ルールを適用します。

例1：シンプルなレイアウト

この例では、タグ制限を使用して、特定のデスクトップおよびアプリケーションの起動に考慮されるマシンを制限するシンプルなレイアウトを紹介します。このサイトには、1つの共有デリバ

リーグループ、1つの公開デスクトップ、および2つのアプリケーションで構成された1つのアプリケーショングループがあります。

シンプルなレイアウトでタグ制限を使用する例。(/en-us/citrix-virtual-apps-desktops/2411/media/tags-example.png)

- 3台の各マシン (VDA 101～103) にタグが追加されています。
- 共有デリバリーグループ内のデスクトップは、「Red」というタグ制限で作成されました。デスクトップは、そのデリバリーグループ内で「Red」タグを持つマシン (VDA 101および102) でのみ起動できます。
- アプリケーショングループは「Orange」タグ制限で作成されたため、その各アプリケーション (CalculatorとNotepad) は、そのデリバリーグループ内で「Orange」タグを持つマシン (VDA 102および103) でのみ起動できます。

マシンVDA 102は両方のタグ (RedとOrange) を持っているため、アプリケーションとデスクトップの起動に考慮されます。

例2：より複雑なレイアウト

この例には、タグ制限付きで作成された複数のアプリケーショングループが含まれています。これにより、デリバリーグループのみを使用した場合に必要となるよりも少ないマシンで、より多くのアプリケーションを配信できるようになります。

例 2 の構成方法 は、この例でタグを作成および適用し、タグ制限を構成するために使用される手順を示しています。

複雑なレイアウトでタグ制限を使用する例。(/en-us/citrix-virtual-apps-desktops/2411/media/tags-example2.png)

この例では、10台のマシン (VDA 101～110)、1つのデリバリーグループ (D01)、および3つのアプリケーショングループ (A100、A200、A300) を使用します。各マシンにタグを適用し、各アプリケーショングループの作成時にタグ制限を指定することで、次のようになります。

- グループ内の経理ユーザーは、5台のマシン (VDA 101～105) で必要なアプリにアクセスできます。
- グループ内のCAD設計者は、5台のマシン (VDA 106～110) で必要なアプリにアクセスできます。
- グループ内でOfficeアプリケーションを必要とするユーザーは、10台のマシン (VDA 101～110) でOfficeアプリにアクセスできます。

使用されるマシンは10台のみで、デリバリーグループは1つだけです。デリバリーグループのみを使用する場合（アプリケーショングループなしの場合）、マシンは1つのデリバリーグループにしか属せないため、2倍の数のマシンが必要になります。

タグとタグ制限の管理

タグは、Web Studioの**［タグの管理］**アクションを通じて、選択したアイテムに対して作成、追加（適用）、編集、削除されます。

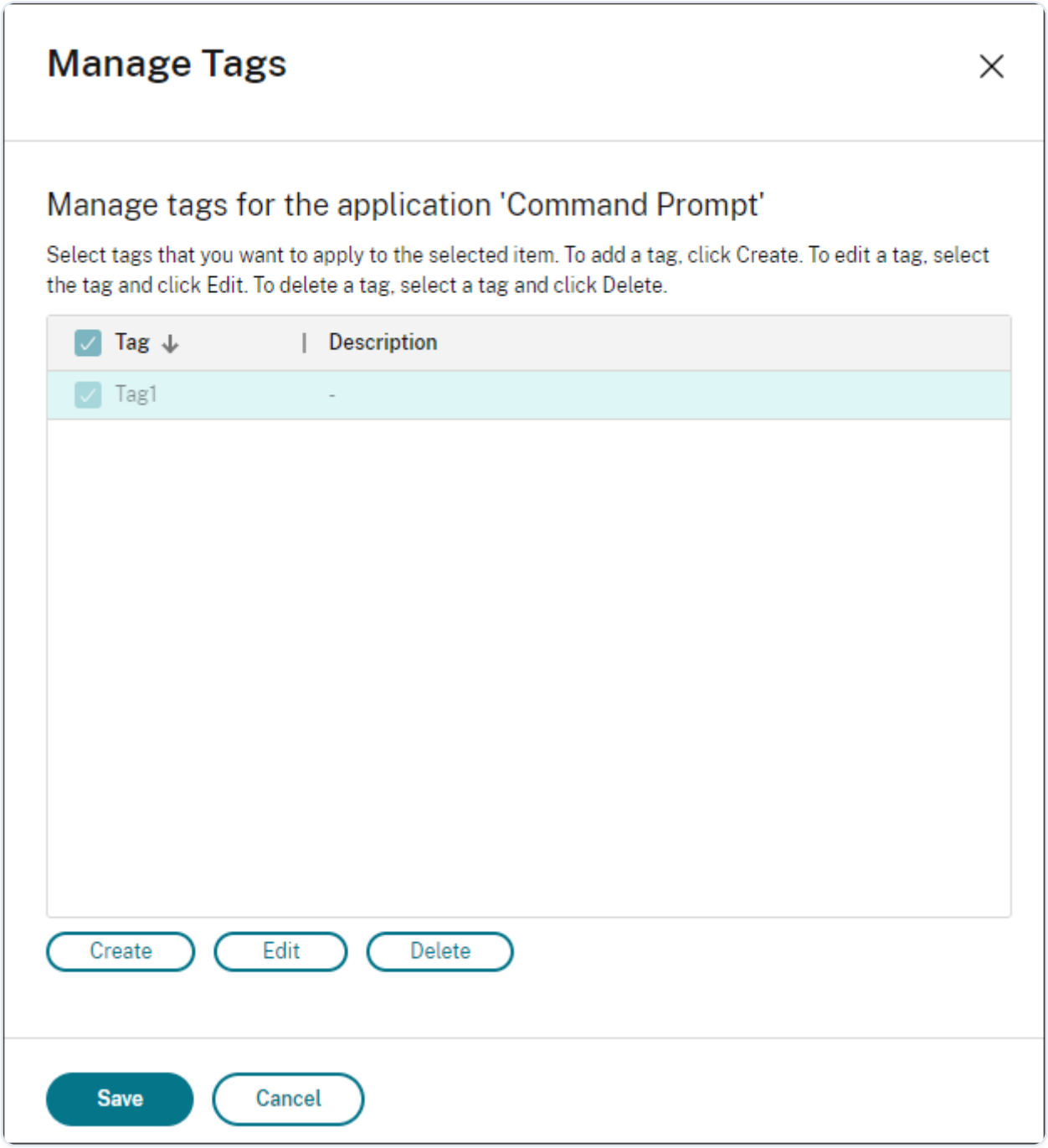
（例外：ポリシー割り当てに使用されるタグは、Web Studioの**［タグの管理］**アクションを通じて作成、編集、削除されます。ただし、タグはポリシーの作成時に適用（割り当て）されます。詳細については、「ポリシーの作成」を参照してください。）

タグ制限は、デリバリーグループでデスクトップを作成または編集するとき、およびアプリケーショングループを作成および編集するときに構成されます。

Web Studioで［タグの管理］ダイアログを使用する

Web Studioで、タグを適用するアイテム（1つまたは複数のマシン、アプリケーション、デスクトップ、デリバリーグループ、またはアプリケーショングループ）を選択し、アクションバーで**タグの管理**を選択します。ダイアログボックスには、選択したアイテムだけでなく、サイトで作成されたすべてのタグが一覧表示されます。

- チェックマークが付いたチェックボックスは、そのタグが選択したアイテムに既に追加されていることを示します。（以下のスクリーンショットでは、選択したマシンに「Tag1」という名前のタグが適用されています。）
- 複数のアイテムを選択した場合、ハイフンが付いたチェックボックスは、選択したアイテムの一部にのみそのタグが追加されていることを示します。



次のアクションは、**［タグの管理］**ダイアログボックスから利用できます。タグの操作に関する注意点を必ず確認してください。

- **タグを作成するには:**

  作成をクリックします。名前と説明を入力します。タグ名は一意である必要があり、大文字と小文字は区別されません。次に、**OK**をクリックします。（タグを作成しても、選択した項目に自動的に適用されるわけではありません。チェックボックスを使用してタグを適用します。）

- **1つ以上のタグを追加（適用）するには:**

タグ名の横にあるチェックボックスを有効にします。複数のアイテムを選択し、タグの横にあるチェックボックスにハイフンが含まれている場合（選択したアイテムの一部にのみタグがすでに適用されていることを示す）、それをチェックマークに変更すると、選択したすべてのマシンに影響します。

1つ以上のマシンにタグを追加しようとしたときに、そのタグがアプリケーショングループで制限として使用されている場合、その操作によってそれらのマシンが起動可能になる可能性があるという警告が表示されます。それが意図した操作であれば、続行してください。

- **1つ以上のタグを削除するには:**

  タグ名の横にあるチェックボックスをオフにします。複数の項目を選択していて、タグの横にあるチェックボックスにハイフンが含まれている場合（選択した項目の一部にのみタグが適用されていることを示す）、チェックボックスをオフにすると、選択したすべてのマシンからタグが削除されます。

  制限としてタグを使用しているマシンからタグを削除しようとすると、その操作によって起動対象となるマシンに影響が出る可能性があるという警告が表示されます。それが意図した操作であれば、続行してください。

- **タグを編集するには:**

  タグを選択し、**編集**をクリックします。新しい名前、説明、またはその両方を入力します。一度に編集できるタグは1つだけです。

- **1つ以上のタグを削除するには:**

  タグを選択し、**削除**をクリックします。「タグの削除」ダイアログボックスには、現在選択されているタグを使用している項目の数（例：「2台のマシン」）が表示されます。項目をクリックすると、詳細情報が表示されます。たとえば、「2台のマシン」項目をクリックすると、そのタグが適用されている2台のマシン名が表示されます。タグを削除するかどうかを確認します。

  Web Studioを使用して、制限として使用されているタグを削除することはできません。まず、アプリケーショングループを編集してタグ制限を削除するか、別のタグを選択してください。

タグの管理ダイアログボックスでの作業が完了したら、**保存**をクリックします。

マシンにタグが適用されているかどうかを確認するには：左ペインで**デリバリーグループ**を選択します。中央ペインでデリバリーグループを選択し、アクションバーで**マシンの表示**を選択します。中央ペインでマシンを選択し、**詳細**ペインで**タグ**タブを選択します。

タグ制限を管理する

タグ制限の構成は複数の手順からなるプロセスです。まずタグを作成し、それをマシンに追加/適用します。次に、アプリケーショングループまたはデスクトップに制限を追加します。

- **タグを作成して適用する：**

  タグを作成し、前述の**タグの管理**アクションを使用して、タグ制限の影響を受けるマシンにタグを追加（適用）します。

- **アプリケーショングループにタグ制限を追加するには:**

  アプリケーショングループを作成または編集します。**デリバリーグループ**ページで、**タグを持つマシンへの起動を制限する**を選択し、リストからタグを選択します。

- **アプリケーショングループのタグ制限を変更または削除するには:**

  グループを編集します。**デリバリーグループ**ページで、リストから別のタグを選択するか、**タグを持つマシンへの起動を制限する**のチェックを外してタグ制限を完全に削除します。

- **デスクトップにタグ制限を追加するには:**

  デリバリーグループを作成または編集します。**デスクトップ**ページで、**追加**または**編集**をクリックします。「デスクトップの追加」ダイアログボックスで、**タグを持つマシンへの起動を制限する**を選択し、メニューからタグを選択します。

- **デリバリーグループのタグ制限を変更または削除するには:**

  グループを編集します。デスクトップページで、**編集**をクリックします。ダイアログボックスで、リストから別のタグを選択するか、**タグを持つマシンへの起動を制限する**のチェックを外してタグ制限を完全に削除します。

タグを使用する際の注意点

アイテムに適用されたタグはさまざまな目的に使用できるため、タグの追加、削除、および消去が意図しない影響を与える可能性があることに留意してください。Web Studioの検索フィールドでマシンの表示を並べ替えるためにタグを使用できます。アプリケーショングループまたはデスクトップを構成する際に、同じタグを制限として使用できます。このタグは、指定されたデリバリーグループ内でそのタグを持つマシンのみに起動の考慮事項を制限します。

デスクトップまたはアプリケーショングループのタグ制限としてタグが構成された後で、そのタグをマシンに追加しようとすると、警告が表示されます。そのタグを追加すると、マシンが追加のアプリケーションやデスクトップの起動に利用可能になる可能性があります。それが意図したものであれば、続行してください。そうでない場合は、操作をキャンセルできます。

たとえば、「Red」タグ制限を持つアプリケーショングループを作成したとします。その後、そのアプリケーショングループで使用されているのと同じデリバリーグループに他のマシンをいくつか追加します。そのマシンに「Red」タグを追加しようとすると、Web Studioは次のようなメッセージを表示します。「タグ「Red」は、以下のアプリケーショングループの制限として使用されています。このタグを追加すると、選択したマシンがこのアプリケーショングループ内のアプリケーションを起動できるようになる可能性があります。」その後、その追加のマシンにそのタグを追加することを確認またはキャンセルできます。

同様に、アプリケーショングループが起動を制限するためにタグを使用している場合、Web Studioは、制限として削除するためにグループを編集するまでタグを削除できないことを警告します。（アプリケーショングループで制限として使用されているタグを削除することが許可された場合、そのアプリケーショングループに関連付けられているデリバリーグループ内のすべてのマシンでアプリケーションの起動が許可される可能性があります。）タグがデスクトップ起動の制限として使用されている場合も、タグの削除に対する同じ禁止が適用されます。そのタグ制限を削除するために、アプリケーショングループまたはデリバリーグループ内のデスクトップを編集した後、タグを削除できます。

すべてのマシンが同じアプリケーションセットを持っているとは限りません。ユーザーは複数のアプリケーショングループに属することができ、それぞれ異なるタグ制限と、デリバリーグループからの異なるまたは重複するマシンセットを持っています。以下の表は、マシンの考慮事項がどのように決定されるかを示しています。

アプリケーションが追加された場合	選択されたデリバリーグループ内のこれらのマシンが起動対象と見なされます
タグ制限のないアプリケーショングループが1つ	任意のマシン。
タグ制限Aのあるアプリケーショングループが1つ	タグAが適用されているマシン。
タグ制限Aのあるアプリケーショングループと、タグ制限Bのあるアプリケーショングループの2つ	タグAとタグBの両方を持つマシン。利用可能なマシンがない場合は、タグAまたはタグBのいずれかを持つマシン。
タグ制限Aのあるアプリケーショングループと、タグ制限のないアプリケーショングループの2つ	タグAを持つマシン。利用可能なマシンがない場合は、任意のマシン。

マシンの再起動スケジュールでタグ制限を使用した場合、タグの適用または制限に影響する変更は、次回のマシン再起動サイクルに影響します。変更が行われている間に進行中の再起動サイクルには影響しません。

例2の構成方法

以下の手順では、タグを作成して適用し、2番目の例で示されているアプリケーショングループのタグ制限を構成する手順を示します。

VDAとアプリケーションはすでにマシンにインストールされており、デリバリーグループも作成されています。

マシンにタグを作成して適用します。

1. Web Studioで、デリバリーグループD01を選択し、アクションバーで**「マシンの表示」**を選択します。
2. VDA 101～105のマシンを選択し、アクションバーで「**タグの管理**」を選択します。
3. 「タグの管理」ダイアログボックスで、「**作成**」をクリックし、`CADApps`という名前のタグを作成します。「**OK**」をクリックします。
4. もう一度「**作成**」をクリックし、OfficeAppsという名前のタグを作成します。「**OK**」をクリックします。
5. 「**タグの管理**」ダイアログボックスを開いたまま、各タグの名前（`CADApps`と`OfficeApps`）の横にあるチェックボックスを有効にして、新しく作成したタグを選択したマシンに追加（適用）します。完了したら、ダイアログボックスを閉じます。
6. 配信グループD01を選択し、アクションバーで「**マシンの表示**」を選択します。
7. VDA 106～110のマシンを選択し、アクションバーで「**タグの管理**」を選択します。
8. 「**タグの管理**」ダイアログボックスで、「**作成**」をクリックします。`AcctgApps`という名前のタグを作成します。「**OK**」をクリックします。
9. 新しく作成した`AcctgApps`タグと`OfficeApps`タグを、各タグ名の横にあるチェックボックスをクリックして選択したマシンに適用し、ダイアログボックスを閉じます。

タグ制限付きのアプリケーショングループを作成します。

1. Web Studioで、左ペインの「**アプリケーション**」を選択し、「**アプリケーショングループ**」タブを選択してから、アクションバーで「**アプリケーショングループの作成**」を選択します。「アプリケーショングループの作成」ウィザードが起動します。
2. ウィザードの「**配信グループ**」ページで、配信グループD01を選択します。「**タグを持つマシンへの起動を制限**」を選択し、リストから`AcctgApps`タグを選択します。

3. ウィザードを完了し、会計ユーザーと会計アプリケーションを指定します。（アプリケーションを追加するときは、`AcctgApps`タグを持つマシンでアプリケーションを検索する「**スタートメニューから**」ソースを選択します。）「**概要**」ページで、グループに`A100`という名前を付けます。
4. 前の手順を繰り返して、`CADApps`タグを持つマシンと、適切なユーザーおよびアプリケーションを指定して、アプリケーショングループ`A200`を作成します。
5. 手順を繰り返して、`OfficeApps`タグを持つマシンと、適切なユーザーおよびアプリケーションを指定して、アプリケーショングループ`A300`を作成します。

マシンカタログのタグ

マシンカタログでタグを使用できます。タグを作成してカタログに適用する全体的な手順は、前述のとおりです。ただし、カタログへのタグの適用はPowerShellインターフェイスを介してのみサポートされています。Web Studioを使用してカタログにタグを適用したり、カタログからタグを削除したりすることはできません。Web Studioのカタログ表示では、タグが適用されているかどうかは示されません。

概要: Web StudioまたはPowerShellを使用して、カタログで使用するタグを作成または削除できます。PowerShellを使用して、タグをカタログに適用します。

カタログでタグを使用する例をいくつか示します。

- デリバリーグループには複数のカタログのマシンが含まれていますが、特定のカタログ内のマシンのみに操作（再起動スケジュールなど）を適用したい場合があります。そのカタログにタグを適用することで、これが実現します。
- アプリケーショングループでは、アプリケーションセッションを特定のカタログ内のマシンに制限したい場合があります。そのカタログにタグを適用することで、これが実現します。

影響を受けるPowerShellコマンドレット:

- `Add-BrokerTag`や`Remove-BrokerTag`などのコマンドレットにカタログオブジェクトを渡すことができます。
- `Get-BrokerTagUsage`は、タグを含むカタログの数を示します。
- `Get-BrokerCatalog`には`Tags`というプロパティがあります。

たとえば、次のコマンドレットは、`acctg`という名前のカタログに`fy2018`という名前のタグを追加します。`Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`。(このタグは、以前にWeb StudioまたはPowerShellを使用して作成されています。)

詳細なガイダンスと構文については、PowerShellコマンドレットのヘルプを参照してください。

自動タグ

自動タグを使用すると、マシン、アプリケーショングループ、アプリケーション、デスクトップグループ、またはデスクトップへのタグの自動追加および削除のルールを定義できます。定義されたルールを満たさない場合、タグも自動的に削除されます。この機能強化により、環境最適化のために定期的に実行されるさまざまなスクリプトを維持する必要がなくなります。

ユースケース

自動タグ付けを使用すると、コスト削減、インフラストラクチャの最適化、消費の促進など、ビジネスドライバーに関連するルールを実装できます。以下にいくつかのユースケースを示します。

- **未使用のVDIを再利用** - 事前設定された日数以上使用されていない専用ワークロードを、利用可能なプールに解放するため。
- **アプリの煩雑さを解消** - 事前設定された日数以上使用されていないアプリケーションを特定することで、アプリケーションの煩雑さを軽減するため。
- **X未満の機能レベルを持つDG** - 特定の機能レベル未満のデリバリーグループを見つけるため。
- **非アクティブユーザー** - 事前設定された日数以上ログオンしていないユーザーのリソースを再利用するため。

> **注:**
>
> 30日以上使用されていないマシンに付与されたタグは、ユーザーが30日後にそのマシンにログインした場合、次回そのマシンが実行されるときに削除されます。

PowerShellコマンド

PowerShellコマンドを使用して自動タグを作成できます。自動タグルールが作成されると、3600秒の頻度で評価されます。詳細については、New-BrokerAutoTagRuleを参照してください。

`New-BrokerAutoTagRule`のパラメーターは次のとおりです。

- 名前: ルールの汎用名
- オブジェクトタイプ: マシン
- ルールテキスト: ルールを定義するフィルター。
- タグUid: 関連付けたいタグID。

例

1. 30日以上使用されていない専用VDIにタグを付けるには:

```
New-BrokerAutoTagRule -Name ‘UnusedVdi’ -ObjectType ‘Machine’ -RuleText
“-AllocationType Static -IsAssigned $true -Filter { SummaryState -ne
`”InUse`” -and ( LastConnectionTime -lt ‘-30’ -or LastConnectionTime
-eq `$null ) }” -TagUid 123
```

ルールが構成された後、タグ **unused-VDI** が付いたマシンは解放されます。

2. X機能レベル未満のデリバリーグループにタグを付けるには (**L7_20** をしきい値機能レベルとして使用):

```
New-BrokerAutoTagRule -Name 'LowFL' -ObjectType 'DesktopGroup'
-RuleText " -Filter { MinimumFunctionalLevel -lt 'L7_20' } " -TagUid
143
```

3. フォルダーなしで公開された、ユーザーに表示されるアプリにタグを付けるには:

```
New-BrokerAutoTagRule -Name 'NoFolder' -ObjectType 'Application'
-RuleText "-Enabled $true -Filter { ClientFolder -eq $null } " -TagUid
153`
```

詳細情報

ブログ投稿: 特定のサーバーにデスクトップを割り当てる方法。

ユーザープロファイル

デフォルトでは、Virtual Delivery Agentをインストールすると、Citrix Profile Managementはマスターイメージにサイレントインストールされますが、プロファイルソリューションとしてProfile Managementを使用する必要はありません。

ユーザーのさまざまなニーズに合わせて、Citrix Virtual Apps and Desktops™ポリシーを使用して、各デリバリーグループのマシンに異なるプロファイル動作を適用できます。たとえば、あるデリバリーグループでは、テンプレートが1つのネットワークロケーションに保存されているCitrix強制プロファイルが必要な場合があります。一方、別のデリバリーグループでは、複数のリダイレクトされたフォルダーとともに別のロケーションに保存されているCitrix移動プロファイルが必要な場合があります。

- 組織内の他の管理者がCitrix Virtual Apps and Desktopsポリシーを担当している場合は、彼らと協力して、デリバリーグループ全体でプロファイル関連のポリシーが設定されていることを確認してください。

- Profile Managementポリシーは、グループポリシー、Profile Management .iniファイル、および個々の仮想マシンでローカルに設定することもできます。プロファイル動作を定義するこれらの複数の方法は、次の順序で読み取られます。

  a. グループポリシー（.admまたは.admxファイル）

  b. ポリシーノードのCitrix Virtual Apps and Desktopsポリシー

  c. ユーザーが接続する仮想マシン上のローカルポリシー

  d. Profile Management .iniファイル

  たとえば、グループポリシーとポリシーノードの両方で同じポリシーを設定した場合、システムはグループポリシーのポリシー設定を読み取り、Citrix Virtual Apps and Desktopsポリシー設定を無視します。

どのプロファイルソリューションを選択しても、Director管理者は診断情報にアクセスし、ユーザープロファイルのトラブルシューティングを行うことができます。詳細については、Directorドキュメントを参照してください。

自動構成

デスクトップの種類は、Virtual Delivery Agentのインストールに基づいて自動的に検出され、Studioで行う構成の選択に加えて、それに応じてProfile Managementのデフォルトを設定します。

Profile Managementが調整するポリシーを次の表に示します。デフォルト以外のポリシー設定は保持され、この機能によって上書きされることはありません。各ポリシーの詳細については、Profile Managementのドキュメントを参照してください。プロファイルを作成するマシンの種類は、調整されるポリシーに影響します。主な要因は、マシンが永続的であるかプロビジョニングされているか、および複数のユーザーで共有されているか、1人のユーザー専用であるかです。

永続システムには何らかのローカルストレージがあり、その内容はシステムがオフになっても保持されることが期待されます。永続システムは、SANなどのストレージテクノロジーを使用して、ローカルディスクのエミュレーションを提供する場合があります。対照的に、プロビジョニングされたシステムは、ベースディスクと何らかのIDディスクから「オンザフライ」で作成されます。ローカルストレージは通常、RAMディスクまたはネットワークディスクによってエミュレートされ、後者は高速リンクを備えたSANによって提供されることがよくあります。プロビジョニングテクノロジーは通常、Citrix ProvisioningまたはMachine Creation Services™（あるいはサードパーティ製の同等品）です。プロビジョニングされたシステムが永続的なローカルストレージを持つ場合もあります。これらは永続的として分類されます。

これら2つの要素を合わせると、以下のマシンタイプが定義されます。

- **永続的かつ専用**。例としては、Machine Creation Servicesで作成された静的割り当てと永続的なローカルストレージを持つシングルセッションOSマシン、物理ワークステーション、ラップトップなどがあります。
- **永続的かつ共有**。例としては、Machine Creation Servicesで作成されたマルチセッションOSマシン、およびCitrix Virtual Appsサーバーなどがあります。
- **プロビジョニング済みかつ専用**。例としては、静的割り当てを持つものの永続ストレージを持たず、Citrix Provisioning Service (Citrix Virtual Desktops™内) で作成されたシングルセッションOSマシンなどがあります。
- **プロビジョニング済みかつ共有**。例としては、ランダム割り当てを持つシングルセッションOSマシンで、Citrix Provisioning™ Service (Citrix Virtual Desktops内) で作成されたもの、およびCitrix Virtual Appsサーバーなどがあります。

以下のProfile Managementポリシー設定は、異なるマシンタイプに対する推奨ガイドラインです。ほとんどの場合にうまく機能しますが、展開の要件に応じてこれらから逸脱することもできます。

> **重要:**
>
> **ログオフ時にローカルにキャッシュされたプロファイルを削除、プロファイルストリーミング**、および**常にキャッシュ**は、自動構成機能によって適用されます。その他のポリシーは手動で調整してください。

永続マシン

ポリシー	永続的かつ専用	永続的かつ共有
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効	有効
プロファイルストリーミング	無効	有効
常にキャッシュ	有効 (注 1)	無効 (注 2)
アクティブライトバック	無効	無効 (注 3)
ローカル管理者のログオンを処理する	有効	無効 (注 4)

プロビジョニング済みマシン

ポリシー	プロビジョニング済みと専用の両方	プロビジョニング済みと共有の両方
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効 (注5)	有効
プロファイルストリーミング	有効	有効
常にキャッシュ	無効 (注6)	無効
アクティブライトバック	有効	有効
ローカル管理者によるログオンを処理する	有効	有効 (注 7)

1. このマシンタイプでは**プロファイルストリーミング**が無効になっているため、**常にキャッシュ**設定は常に無視されます。
2. **常にキャッシュ**を無効にします。ただし、このポリシーを有効にし、ファイルサイズ制限 (MB単位) を定義することで、ログオン後できるだけ早く大きなファイルがプロファイルに読み込まれるようにすることができます。このサイズ以上のファイルは、できるだけ早くローカルにキャッシュされます。
3. Citrix Virtual Appsサーバー間をローミングするユーザーのプロファイルの変更を保存する場合を除き、**アクティブなライトバック**を無効にします。この場合は、このポリシーを有効にします。
4. ホスト型共有デスクトップの場合を除き、**ローカル管理者のログオンを処理**を無効にします。この場合は、このポリシーを有効にします。
5. **ログオフ時にローカルにキャッシュされたプロファイルを削除**を無効にします。この設定は、ローカルにキャッシュされたプロファイルを保持します。マシンはログオフ時にリセットされますが、個々のユーザーに割り当てられるため、プロファイルがキャッシュされているとログオンが速くなります。
6. **常にキャッシュ**を無効にします。ただし、このポリシーを有効にし、ファイルサイズ制限 (MB単位) を定義することで、ログオン後できるだけ早く大きなファイルがプロファイルに読み込まれるようにすることができます。このサイズ以上のファイルは、できるだけ早くローカルにキャッシュされます。

7. Citrix Virtual Apps and Desktopsサーバー間をローミングするユーザーのプロファイルの場合を除き、**ローカル管理者のログオンを処理**を有効にします。この場合は、このポリシーを無効にします。

フォルダーリダイレクト

フォルダーリダイレクトを使用すると、プロファイルが保存されている場所とは異なるネットワーク共有にユーザーデータを保存できます。フォルダーリダイレクトはプロファイルのサイズと読み込み時間を削減しますが、ネットワーク帯域幅に影響を与える可能性があります。フォルダーリダイレクトは、Citrixユーザープロファイルが使用されていることを必要としません。ユーザープロファイルを独自に管理し、フォルダーをリダイレクトすることもできます。

StudioのCitrixポリシーを使用してフォルダーリダイレクトを構成します。

- リダイレクトされたフォルダーのコンテンツを保存するために使用されるネットワークの場所が利用可能であり、正しい権限を持っていることを確認します。場所のプロパティは検証されます。
- リダイレクトされたフォルダーはネットワーク上に設定され、そのコンテンツはログオン時にユーザーの仮想デスクトップから入力されます。

フォルダーリダイレクトは、CitrixポリシーまたはActive Directoryグループポリシーオブジェクトのいずれか一方のみを使用して構成し、両方は使用しないでください。両方のポリシーエンジンを使用してフォルダーリダイレクトを構成すると、予期しない動作が発生する可能性があります。

高度なフォルダーリダイレクト

複数のオペレーティングシステム (OS) を使用する展開環境では、ユーザープロファイルの一部を各OSで共有したい場合があります。プロファイルの残りの部分は共有されず、1つのOSでのみ使用されます。OS間で一貫したユーザーエクスペリエンスを確保するには、各OSで異なる構成、つまり高度なフォルダーリダイレクトが必要です。たとえば、2つのOSで実行されているアプリケーションの異なるバージョンが共有ファイルを読み取ったり編集したりする必要がある場合、両方のバージョンがアクセスできる単一のネットワークロケーションにリダイレクトすることを決定します。あるいは、2つのOSで**スタートメニュー**フォルダーの内容の構造が異なるため、両方ではなく1つのフォルダーのみをリダイレクトすることを決定します。このアプローチにより、各OSで**スタートメニュー**フォルダーとその内容が分離され、ユーザーに一貫したエクスペリエンスが保証されます。

展開環境で高度なフォルダーリダイレクトが必要な場合は、ユーザーのプロファイルデータの構造を理解し、そのどの部分をOS間で共有できるかを判断する必要があります。フォルダーリダイレクトが正しく使用されないと、予期しない動作が発生する可能性があります。

高度な展開環境でフォルダーをリダイレクトするには：

- 各OSに個別のDelivery Groupを使用します。
- 仮想デスクトップ上のものを含む仮想アプリケーションがユーザーデータと設定をどこに保存するか、およびデータがどのように構造化されているかを理解します。
- 安全にローミングできる共有プロファイルデータ（各OSで同じ構造になっているため）については、各Delivery Group内のコンテナフォルダーをリダイレクトします。
- ローミングできない非共有プロファイルデータについては、いずれかのDesktop Groupのコンテナフォルダーのみをリダイレクトします。通常は、最も使用されているOSまたはデータが最も関連性の高いOSのものです。あるいは、OS間でローミングできない非共有データについては、両方のシステムのコンテナフォルダーを別々のネットワークロケーションにリダイレクトします。

高度な展開の例

この展開環境には、Windows 10デスクトップで実行されるMicrosoft OutlookおよびInternet Explorerのバージョンを含むアプリケーションと、Windows Server 2019によって提供されるOutlookおよびInternet Explorerの他のバージョンを含むアプリケーションがあります。2つのOS用に2つのDelivery Groupをすでに設定しています。ユーザーは、両方のアプリケーションのバージョンで同じ**連絡先**と**お気に入り**のセットにアクセスしたいと考えています。

重要： 以下の決定とアドバイスは、説明されているOSと展開環境に有効です。組織では、リダイレクトするフォルダーとそれらを共有するかどうかの決定は、特定の展開環境に固有のさまざまな要因に依存します。

- Delivery Groupに適用されるポリシーを使用して、以下のフォルダーをリダイレクトするように選択します。

フォルダ	WINDOWS 10でリダイレクトされますか？	WINDOWS SERVER 2019でリダイレクトされますか？
マイドキュメント	はい	はい
アプリケーションデータ	いいえ	いいえ
連絡先	はい	はい
デスクトップ	はい	いいえ
ダウンロード	いいえ	いいえ

フォルダ	WINDOWS 10でリダイレクトされますか？	WINDOWS SERVER 2019でリダイレクトされますか？
お気に入り	はい	はい
リンク	はい	いいえ
マイミュージック	はい	はい
マイピクチャ	はい	はい
マイビデオ	はい	はい
検索	はい	いいえ
保存されたゲーム	いいえ	いいえ
スタートメニュー	はい	いいえ

- 共有され、リダイレクトされたフォルダーの場合:
  - OutlookとInternet Explorerの異なるバージョンによって保存されたデータの構造を分析した結果、**連絡先**フォルダーと**お気に入り**フォルダーを共有しても安全であると判断しました。
  - **ドキュメント**、**ミュージック**、**ピクチャ**、**ビデオ**フォルダーの構造はOS間で標準的であることがわかっています。そのため、これらのフォルダーを各デリバリーグループで同じネットワークの場所に保存しても安全です。
- 共有されない、リダイレクトされたフォルダーの場合:
  - Windows Serverデリバリーグループでは、デスクトップ、リンク、検索、または**スタートメニュー**フォルダーをリダイレクトしません。これらのフォルダーのデータは2つのOSで異なる方法で整理されているためです。したがって、共有することはできません。
  - この共有されないデータの予測可能な動作を保証するために、Windows 10デリバリーグループでのみリダイレクトします。Windows 10は、ユーザーが日常業務でより頻繁に使用します。ユーザーは、Windows Serverによって提供されるアプリケーションにはたまにしかアクセスしません。また、この場合、共有されないデータはアプリケーション環境よりもデスクトップ環境により関連性が高くなります。たとえば、デスクトップショートカットは**デスクトップ**フォルダーに保存され、Windows 10マシンから作成されたものであれば役立つ可能性がありますが、Windows Serverマシンから作成されたものでは役立たない場合があります。

- リダイレクトされないフォルダーの場合:
  - ユーザーのダウンロードファイルでサーバーを散らかしたくないため、ダウンロードフォルダーをリダイレクトしないことを選択します
  - 個々のアプリケーションからのデータは互換性やパフォーマンスの問題を引き起こす可能性があるため、アプリケーションデータフォルダーをリダイレクトしないことを決定します

フォルダーリダイレクトの詳細については、「フォルダーリダイレクト、オフラインファイル、および移動ユーザープロファイルの概要」を参照してください。

フォルダーリダイレクトと除外

Citrix Profile Management（ただしStudioではない）では、パフォーマンス強化により、除外を使用してフォルダーが処理されるのを防ぐことができます。この機能を使用する場合、リダイレクトされたフォルダーを除外しないでください。フォルダーリダイレクトと除外機能は連携して動作します。リダイレクトされたフォルダーが除外されないようにすることで、後でリダイレクトしないと決定した場合でも、Profile Managementがそれらをプロファイルフォルダー構造に戻し、データの整合性を維持できます。除外の詳細については、「項目の含める/除外」を参照してください。

VDA登録

はじめに

> **注:**
>
> オンプレミス環境では、VDAはDelivery Controllerに登録します。Citrix Cloudサービス環境では、VDAはCloud Connectorに登録します。ハイブリッド環境では、一部のVDAはDelivery Controllerに登録し、他のVDAはCloud Connectorに登録します。

> VDAを使用する前に、サイト上の1つ以上のControllerまたはCloud Connectorに登録（通信を確立）する必要があります。VDAは、`ListofDDCs`と呼ばれるリストを確認することでControllerまたはConnectorを見つけます。VDA上の`ListOfDDCs`には、そのVDAをサイト上のControllerまたはCloud Connectorにポイントするエントリが含まれています。負荷分散のため、VDAはリスト内のすべてのControllerまたはCloud Connectorに接続を自動的に分散します。

VDA登録がこれほど重要なのはなぜですか？

- セキュリティの観点から見ると、登録は機密性の高い操作です。ControllerまたはCloud ConnectorとVDA間の接続を確立しています。このような機密性の高い操作では、すべてが完璧な状態でない場合、接続を拒否するのが期待される動作です。VDAからControllerまたはCloud Connectorへ、そしてControllerまたはCloud ConnectorからVDAへという、2つの別々の通信チャネルを効果的に確立しています。接続にはKerberosが使用されるため、時刻同期やドメインメンバーシップの問題は許容されません。Kerberosはサービスプリンシパル名（SPN）を使用するため、負荷分散されたIP\\ホスト名を使用することはできません。
- Controller（またはCloud Connector）を追加および削除する際に、VDAが正確で最新のControllerまたはCloud Connector情報を持っていない場合、VDAはリストにないControllerまたはCloud Connectorによって仲介されるセッション起動を拒否する可能性があります。無効なエントリは、仮想デスクトップシステムソフトウェアの起動を遅らせる可能性があります。VDAは、不明で信頼できないControllerまたはCloud Connectorからの接続を受け入れません。

`ListofDDCs`に加えて、`ListOfSIDs`（セキュリティID）は、`ListofDDCs`内のどのマシンが信頼されているかを示します。`ListofSIDs`は、Active Directoryへの負荷を軽減したり、侵害されたDNSサーバーからの潜在的なセキュリティ脅威を回避したりするために使用できます。詳細については、ListOfSIDsを参照してください。

`ListofDDCs`が複数のControllerまたはCloud Connectorを指定している場合、VDAはランダムな順序でそれらに接続しようとします。オンプレミス展開では、`ListofDDCs`にはControllerグループも含まれる場合があります。VDAは、`ListofDDCs`内の他のエントリに移動する前に、グループ内の各Controllerに接続しようとします。

Citrix Virtual Apps and Desktops™は、VDAのインストール中に構成されたControllerまたはCloud Connectorへの接続を自動的にテストします。ControllerまたはCloud Connectorに到達できない場合、エラーが表示されます。ControllerまたはCloud Connectorに接続できないという警告を無視した場合（またはVDAのインストール中にControllerまたはCloud Connectorのアドレスを指定しなかった場合）、メッセージが表示されて通知されます。

ControllerまたはCloud Connectorアドレスを構成する方法

管理者は、VDAが初めて登録するとき（初回登録）に使用する構成方法を選択します。初回登録中に、VDA上に永続的なキャッシュが作成されます。その後の登録では、構成の変更が検出されない限り、VDAはこのローカルキャッシュからControllerまたはCloud Connectorのリストを取得します。

その後の登録でそのリストを取得する最も簡単な方法は、自動更新機能を使用することです。自動更新はデフォルトで有効になっています。詳細については、「自動更新」を参照してください。

VDA上でControllerまたはCloud Connectorアドレスを構成する方法はいくつかあります。

- ポリシーベース (LGPO または GPO)
- レジストリベース (手動、グループポリシー設定 (GPP)、VDA インストール時に指定)
- Active Directory OU ベース (レガシー OU 検出)
- MCS ベース (personality.ini)

VDA をインストールする際に、初期登録方法を指定します。(自動更新を無効にすると、VDA インストール時に選択した方法が以降の登録に使用されます。)

次の図は、VDA インストールウィザードの **Delivery Controller** ページを示しています。

VDA インストールウィザードの Delivery Controller ページを示す図(/en-us/citrix-virtual-apps-desktops/2411/media/vda-install-controllers-all.png)

ポリシーベース (LGPO\\GPO)

Citrix® は、初期 VDA 登録に GPO を使用することを推奨しています。これは最も高い優先順位を持ちます。(自動更新が最も高い優先順位としてリストされていますが、自動更新は初期登録後にのみ使用されます。) ポリシーベースの登録は、構成にグループポリシーを使用することによる一元化の利点を提供します。

この方法を指定するには、以下の両方の手順を完了します。

- VDA インストールウィザードの **Delivery Controller** ページで、**後で実行 (詳細)** を選択します。ウィザードは、VDA インストール中にコントローラーアドレスを指定しない場合でも、コントローラーアドレスを指定するように何度も通知します。(VDA 登録はそれほど重要です。)
- `Virtual Delivery Agent Settings > Controllers` 設定を使用して、Citrix ポリシーを介してポリシーベースの VDA 登録を有効または無効にします。(セキュリティが最優先事項である場合は、`Virtual Delivery Agent Settings > Controller SIDs` 設定を使用してください。)

この設定は `HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)` の下に保存されます。

レジストリベース

この方法を指定するには、以下のいずれかの手順を完了します。

- VDAインストールウィザードの**Delivery Controller**ページで、**手動で実行** を選択します。次に、インストールされているControllerのFQDNを入力し、**追加** をクリックします。複数のControllerをインストールしている場合は、それらのアドレスを追加します。

- コマンドラインVDAインストールの場合、/controllersオプションを使用し、インストールされているControllerまたはCloud ConnectorのFQDNを指定します。

この情報は、レジストリキー`HKLM\Software\Citrix\VirtualDesktopAgent`または`HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent`の下のレジストリ値`ListOfDDCs`に保存されます。

このレジストリキーは手動で構成することも、グループポリシー設定（GPP）を使用することもできます。この方法は、ポリシーベースの方法よりも推奨される場合があります（たとえば、異なるControllerまたはCloud Connectorの条件付き処理が必要な場合など：XDW-001-で始まるコンピューター名にはXDC-001を使用するなど）。

サイト内のすべてのControllerまたはCloud ConnectorのFQDNをリストする`ListOfDDCs`レジストリキーを更新します。（このキーは、Active DirectoryサイトOUに相当します。）

```
HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)
```

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`レジストリの場所に`ListOfDDCs`キーと`FarmGUID`キーの両方が含まれている場合、ControllerまたはCloud Connectorの検出には`ListOfDDCs`が使用されます。`FarmGUID`は、VDAインストール中にサイトOUが指定された場合に存在します。（これはレガシー展開で使用される場合があります。）

必要に応じて、`ListOfSIDs`レジストリキーを更新します（詳細については、ListOfSIDsを参照してください）。

```
HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)
```

注意：Citrixポリシーを通じてポリシーベースのVDA登録も有効にすると、VDAインストール中に指定した設定が上書きされます。これは、ポリシーベースの方法がより優先されるためです。

Active Directory OUベース (レガシー)

この方法は、主に下位互換性のためにサポートされており、推奨されません。まだ使用している場合は、Citrixは別の方法に変更することを推奨します。

この方法を指定するには、以下の両方の手順を完了します。

- VDAインストールウィザードの**Delivery Controller**ページで、**Active Directoryから場所を選択**を選択します。
- `Set-ADControllerDiscovery.ps1`スクリプト（すべてのControllerで利用可能）を使用します。また、各VDAで`FarmGuid`レジストリエントリを構成して、正しいOUを指すようにします。この設定はグループポリシーを使用して構成できます。

MCSベース

MCSを使用してVMをプロビジョニングする場合、MCSはControllerまたはCloud Connectorのリストを設定します。この機能は自動更新と連携します。カタログの作成時に、MCSは初期プロビジョニング中にControllerまたはCloud Connectorのリストを`Personality.ini`ファイルに挿入します。自動更新により、リストは最新の状態に保たれます。

この方法を指定するには、VDAインストールウィザードの **Delivery Controller** ページで、**Machine Creation Services™に任せる** を選択します。

レビューと推奨事項

ベストプラクティスとして:

- 初期登録にはグループポリシー登録方法を使用します。
- 自動更新（デフォルトで有効）を使用して、Controllerのリストを最新の状態に保ちます。
- マルチゾーン展開では、初期構成にグループポリシーを使用します（少なくとも2つのControllerまたはCloud Connectorを使用）。VDAを、そのゾーン内のローカルなControllerまたはCloud Connectorにポイントします。自動更新を使用して、それらを最新の状態に保ちます。自動更新は、サテライトゾーンのVDAの`ListofDDCs`を自動的に最適化します。
- Controllerが利用できない場合の登録の問題を防ぐため、`ListOfDDCs`レジストリキーに複数のControllerをスペースで区切ってリストします。例：

```
DDC7x.xd.local DDC7xHA.xd.local



32-bit: HKEY_LOCAL_MACHINE
\Software\Citrix\VirtualDesktopAgent\ListOfDDCs



HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\ListOfDDCs
(REG_SZ)
```

- `ListofDDCs` の下にリストされているすべての値が有効な完全修飾ドメイン名にマッピングされていることを確認し、起動時の登録遅延を防ぎます。

自動更新

自動更新（XenAppおよびXenDesktop 7.6で導入）はデフォルトで有効になっています。これは、VDA登録を最新の状態に保つための最も効率的な方法です。初期登録には使用されませんが、初期登録時に、自動更新ソフトウェアは`ListofDDCs`をダウンロードし、VDA上の永続キャッシュに保存します。このプロセスは各VDAに対して実行されます。キャッシュにはマシンポリシー情報も保持され、ポリシー設定が再起動後も維持されるようにします。

自動更新は、MCSまたはCitrix Provisioning™を使用してマシンをプロビジョニングする場合にサポートされますが、Citrix Provisioningのサーバー側キャッシュは除きます。自動更新キャッシュ用の永続ストレージがないため、サーバー側キャッシュは一般的なシナリオではありません。

この方法を指定するには:

- `Virtual Delivery Agent Settings > Enable auto update of Controllers`設定を含むCitrixポリシーを介して、自動更新を有効または無効にします。この設定はデフォルトで有効になっています。

仕組み：

- VDAが再登録されるたびに（たとえば、マシンの再起動後など）、キャッシュが更新されます。各ControllerまたはCloud Connectorも90分ごとにサイトデータベースをチェックします。前回のチェック以降にControllerまたはCloud Connectorが追加または削除された場合、またはVDA登録に影響するポリシー変更が発生した場合、ControllerまたはCloud Connectorは更新されたリストを登録済みのVDAに送信し、キャッシュが更新されます。VDAは、最新のキャッシュ済みリストにあるすべてのControllerまたはCloud Connectorからの接続を受け入れます。
- VDAが、登録されているControllerまたはCloud Connectorが含まれていないリストを受信した場合（つまり、そのControllerまたはCloud Connectorがサイトから削除された場合）、VDAは`ListofDDCs`にあるControllerまたはCloud Connectorの中から選択して再登録します。

例：

- 展開には3つのController（A、B、C）があります。VDAはController Bに登録されます（これはVDAのインストール時に指定されました）。
- その後、2つのController（DとE）がサイトに追加されます。90分以内に、VDAは更新されたリストを受信し、Controller A、B、C、D、Eからの接続を受け入れます。（VDAが再起動されるまで、負荷はすべてのControllerに均等に分散されません。）
- さらにその後、Controller Bが別のサイトに移動されます。90分以内に、元のサイトのVDAは更新されたリストを受信します。これは、前回のチェック以降にControllerの変更があったた

めです。Controller Bに最初に登録されていたVDA（リストにはもうありません）は、現在のリスト（A、C、D、E）にあるControllerの中から選択して再登録します。

マルチゾーン展開では、サテライトゾーンの自動更新は、まずすべてのローカルControllerを自動的にキャッシュします。プライマリゾーンのすべてのControllerはバックアップグループにキャッシュされます。サテライトゾーンにローカルControllerが利用できない場合、プライマリゾーンのControllerへの登録が試行されます。

次の例に示すように、キャッシュファイルにはホスト名とセキュリティID（`ListofSIDs`）のリストが含まれています。VDAはSIDを照会しないため、Active Directoryの負荷が軽減されます。

VDAの登録キャッシュファイルの例(/en-us/citrix-virtual-apps-desktops/2411/media/vda-registration-cache-file.png)

WMI呼び出しでキャッシュファイルを取得できます。ただし、SYSTEMアカウントのみが読み取り可能な場所に保存されます。

> **重要：**
>
> この情報は情報提供のみを目的としています。このファイルを変更しないでください。このファイルまたはフォルダーを変更すると、サポートされていない構成になります。

```
Get-WmiObject -Namespace "Root\Citrix\DesktopInformation" -Class "Citrix_VirtualDesktopInfo" -Property "PersistentDataLocation"
```

セキュリティ上の理由で（Active Directoryの負荷軽減とは別に）`ListofSIDs`を手動で構成する必要がある場合、自動更新機能は使用できません。詳細については、ListOfSIDsを参照してください。

自動更新の優先順位の例外

自動更新は通常、すべてのVDA登録方法の中で最も高い優先順位を持ち、他の方法の設定を上書きしますが、例外があります。キャッシュ内の`NonAutoListOfDDCs`要素は、初期VDA構成方法を指定します。自動更新はこの情報を監視します。初期登録方法が変更された場合、登録プロセスは自動更新をスキップし、次に高い優先順位で構成された方法を使用します。このプロセスは、VDAを別のサイトに移動する場合 (たとえば、ディザスターリカバリー中) に役立ちます。

構成に関する考慮事項

一般的なVDA登録構成を表示します。

<iframe src="https://www.youtube.com/embed/MgGMZp4SnZgEq9ieibQc9j" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
VDA登録手順を表示します。

<iframe src="https://www.youtube.com/embed/iwsbajSVY5QvoUTh6m7AjG" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
VDA登録に影響を与える可能性のある項目を構成する際は、次の点を考慮してください。

ControllerまたはCloud Connectorのアドレス

ControllerまたはCloud Connectorを指定するためにどの方法を使用する場合でも、CitrixはFQDNアドレスを使用することを推奨します。IPアドレスは、DNSレコードよりもIPを侵害する方が容易であるため、信頼できる構成とは見なされません。`ListofSIDs`を手動で入力する場合、`ListofDDCs`でIPを使用できます。ただし、FQDNが引き続き推奨されます。

負荷分散

前述のとおり、VDAは `ListofDDCs` 内のすべてのControllerまたはCloud Connectorに接続を自動的に分散します。フェールオーバーと負荷分散機能は、Citrix Brokering Protocol (CBP) に組み込まれています。構成で複数のControllerまたはCloud Connectorを指定した場合、必要に応じて登録はそれらの間で自動的にフェールオーバーします。自動更新により、すべてのVDAで自動フェールオーバーが自動的に発生します。

セキュリティ上の理由から、Citrix ADCなどのネットワークロードバランサーを使用することはできません。VDA登録ではKerberos相互認証を使用します。これは、クライアント（VDA）がサービス（Controller）に対して自身のIDを証明する必要があることを意味します。ただし、ControllerまたはCloud ConnectorもVDAに対して自身のIDを証明する必要があります。これは、VDAとControllerまたはCloud Connectorが同時にサーバーとクライアントとして機能していることを意味します。この記事の冒頭で述べたように、VDAからController/Cloud Connectorへ、およびController/Cloud ConnectorからVDAへの2つの通信チャネルがあります。

このプロセスにおけるコンポーネントの1つは、Active Directoryコンピューターオブジェクトのプロパティとして保存されるサービスプリンシパル名（SPN）と呼ばれます。VDAがControllerまたはCloud Connectorに接続するとき、通信したい相手を指定する必要があります。このアドレスがSPNです。負荷分散されたIPを使用すると、Kerberos相互認証は、そのIPが予期されるControllerまたはCloud Connectorに属していないことを正しく認識します。

詳細については、以下を参照してください。

- Kerberos の概要(https://blogs.technet.microsoft.com/askds/2008/03/06/kerberos-for-the-busy-admin/)

- Kerberos を使用した相互認証(https://docs.microsoft.com/ja-jp/windows-server/security/kerberos/kerberos-authentication-overview)

自動更新による CNAME の置き換え

自動更新機能は、XenApp および XenDesktop の 7.x より前のバージョンからの CNAME (DNS エイリアス) 機能に代わるものです。XenApp および XenDesktop 7 以降、CNAME 機能は無効になっています。CNAME の代わりに自動更新を使用してください。(CNAME を使用する必要がある場合は、CTX137960 を参照してください。DNS エイリアスを常に機能させるには、自動更新と CNAME の両方を同時に使用しないでください。)

Controller/Cloud Connector グループ

特定のシナリオでは、Controller または Cloud Connector をグループで処理したい場合があります。その際、1つのグループを優先し、すべての Controller/Cloud Connector が失敗した場合に別のグループをフェールオーバーに使用します。Controller または Cloud Connector はリストからランダムに選択されることに注意してください。そのため、グループ化は優先的な使用を強制するのに役立ちます。

これらのグループは、単一サイト内での使用を目的としています (複数サイトではありません)。

Controller/Cloud Connector のグループを指定するには、かっこを使用します。たとえば、4つの Controller (プライマリ 2つとバックアップ 2つ) の場合、グループ化は次のようになります。

```
(XDC-001.cdz.lan XDC-002.cdz.lan) (XDC-003.cdz.lan XDC-004.cdz.lan)
```

この例では、最初のグループの Controller (001 と 002) が最初に処理されます。両方が失敗した場合、2番目のグループの Controller (003 と 004) が処理されます。

XenDesktop 7.0 以降の場合、**登録グループ**機能を使用するには、追加の手順を実行する必要があります。Studio から **Controller の自動更新を有効にする**ポリシーを**禁止**する必要があります。

ListOfSIDs

VDA が登録のために連絡できる Controller のリストは `ListofDDCs` です。VDA は、どの Controller を信頼すべきかも知っておく必要があります。VDA は `ListofDDCs` の Controller を自動的に信頼しないためです。`ListofSIDs` (セキュリティ ID) は、信頼できる Controller を識別します。VDA は、信頼できる Controller のみに登録しようとします。

ほとんどの環境では、`ListofSIDs` は `ListofDDCs` から自動的に生成されます。CDF トレースを使用して `ListofSIDs` を読み取ることができます。

通常、`ListofSIDs` を手動で変更する必要はありません。いくつかの例外があります。最初の2つの例外は、新しいテクノロジーが利用可能になったため、もはや有効ではありません。

- **Controllerの役割の分離:** XenAppおよびXenDesktop 7.7でゾーンが導入される前は、登録にControllerのサブセットのみが使用されていた場合、`ListofSIDs` は手動で構成されていました。たとえば、XDC-001とXDC-002をXMLブローカーとして使用し、XDC-003とXDC-004をVDA登録に使用していた場合、すべてのControllerを `ListofSIDs` に、XDC-003とXDC-004を `ListofDDCs` に指定していました。これは一般的または推奨される構成ではありません。新しい環境では使用しないでください。代わりにゾーンを使用してください。
- **Active Directoryの負荷軽減:** XenAppおよびXenDesktop 7.6で自動更新機能が導入される前は、ドメインコントローラーの負荷を軽減するために `ListofSIDs` が使用されていました。`ListofSIDs` を事前に入力することで、DNS名からSIDへの解決をスキップできます。ただし、この永続的なキャッシュにはSIDが含まれているため、自動更新機能によりこの作業は不要になります。Citrixは自動更新機能を有効にしておくことを推奨します。
- **セキュリティ:** 一部の高度に保護された環境では、侵害されたDNSサーバーからの潜在的なセキュリティ脅威を回避するために、信頼されたControllerのSIDが手動で構成されていました。ただし、これを行う場合は、自動更新機能も無効にする必要があります。そうしないと、永続的なキャッシュからの構成が使用されます。

したがって、特別な理由がない限り、`ListofSIDs` を変更しないでください。

`ListofSIDs` を変更する必要がある場合は、`HKLM\Software\Citrix\VirtualDesktopAgent` の下に `ListOfSIDs (REG_SZ)` という名前のレジストリキーを作成します。値は信頼された SID のリストで、複数ある場合はスペースで区切ります。

次の例では、VDA登録には1つのController (`ListofDDCs`) が使用されますが、ブローカー処理には2つのController (List OfSIDs) が使用されます。

登録とブローカー処理に使用される異なるControllerの例(/en-us/citrix-virtual-apps-desktops/2411/media/vda-registration-listofsids.png)

VDA 登録中の Controller 検索

VDAが登録を試みるとき、Broker Agentはまずローカルドメインで DNSルックアップを実行し、指定されたControllerに到達可能であることを確認します。

最初のルックアップで Controller が見つからない場合、Broker Agent は AD でフォールバックのトップダウンクエリを開始できます。このクエリはすべてのドメインを検索し、頻繁に繰り返されます。Controller アドレスが無効な場合 (たとえば、管理者が VDA のインストール時に誤った

FQDN を入力した場合)、そのクエリのアクティビティがドメインコントローラーで分散型サービス拒否 (DDoS) 状態を引き起こす可能性があります。

次のレジストリキーは、Broker Agent が最初の検索中に Controller を見つけられない場合に、フォールバックのトップダウンクエリを使用するかどうかを制御します。

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`

- 名前: `DisableDdcWildcardNameLookup`
- 種類: `DWORD`
- 値: `0` (デフォルト) または任意のゼロ以外の値

`0`に設定すると、フォールバック検索が有効になります。Controllerの初期検索が失敗した場合、フォールバックのトップダウン検索が開始されます。これはデフォルトの動作です。ただし、ゼロ以外の値に設定すると、フォールバック検索は無効になります。Controllerの初期検索が失敗した場合、Broker Agentは検索を停止します。

読み取り専用ドメインコントローラーを使用したVDA登録中のLDAPバインディングのシーケンス

VDAが読み取り専用ドメインコントローラー（RODC）に登録されると、Broker Agentはどの Light Directory Access Protocol (LDAP) バインディングを無視するかを選択する必要があります。この選択を行うには、Broker Agentに適切なレジストリキーが必要です。

レジストリキーが提供されていない場合、またはレジストリキーフィールドが空の場合、元のLDAPバインディングシーケンスをたどる必要があるため、RODCへのVDA登録には時間がかかります。

LDAPバインディングシーケンスを変更するには、レジストリキー`ListofIgnoredBindings`が`HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`に追加されました。`ListofIgnoredBindings`を使用すると、必要に応じてLDAPバインディングシーケンスを変更でき、これによりRODCへのVDA登録を高速化できます。

- 名前: `ListofIgnoredBindings`
- 種類: `REG_SZ`
- 値: `DefaultPath`, `DomainPath`, `PDCPath`

値はバインディングパスオプションのリストで、それぞれコンマで区切られています。レジストリキーは、有効と認識しない値を無視します。

VDA登録の問題のトラブルシューティング

前述のとおり、VDAは、仲介されたセッションを起動する際に考慮されるように、Delivery ControllerまたはCloud Connectorに登録されている必要があります。未登録のVDAは、利用可能なリソースの活用不足につながる可能性があります。VDAが登録されない理由はさまざまであり、その多くは管理者がトラブルシューティングできます。Studioは、カタログ作成ウィザードおよびデリバリーグループ作成後にトラブルシューティング情報を提供します。

- **マシンカタログ作成中の問題の特定:** カタログ作成ウィザードで、既存のマシンを追加した後、コンピューターアカウント名のリストは、各マシンがカタログに追加するのに適しているかどうかを示します。各マシンの横にあるアイコンにカーソルを合わせると、そのマシンに関する情報メッセージが表示されます。

  メッセージが問題のあるマシンを特定した場合、そのマシンを削除する（**削除**ボタンを使用）か、マシンを追加することができます。たとえば、マシンに関する情報が取得されなかった（おそらく登録されたことがないため）ことを示すメッセージが表示された場合でも、マシンを追加することを選択できます。

  カタログの機能レベルは、カタログ内のマシンで利用できる製品機能を制御します。新しい製品バージョンで導入された機能を使用するには、新しいVDAが必要になる場合があります。機能レベルを設定すると、そのバージョンで導入されたすべての機能（および機能レベルが変更されない場合はそれ以降のバージョン）がカタログ内のマシンで利用可能になります。ただし、そのカタログ内の以前のVDAバージョンのマシンは登録できません。
- **デリバリーグループ作成後の問題の特定:** デリバリーグループを作成した後、Studioは、そのグループに関連付けられているマシンの詳細を表示します。

  デリバリーグループの詳細ペインには、登録が必要だが登録されていないマシンの数が表示されます。つまり、電源がオンになっていてメンテナンスモードではないが、現在コントローラーに登録されていないマシンが1台以上存在する可能性があります。「登録されていないが、登録が必要な」マシンを表示している場合は、詳細ペインの**トラブルシューティング**タブで、考えられる原因と推奨される是正措置を確認してください。

VDA登録のトラブルシューティングに関する詳細情報

- 機能レベルの詳細については、「VDAのバージョンと機能レベル」を参照してください。
- VDA登録のトラブルシューティングについて詳しくは、「CTX136668」を参照してください。
- VDA登録とセッション起動のトラブルシューティングには、Citrix Scoutのヘルスチェックも使用できます。詳細については、「ヘルスチェックについて」を参照してください。

仮想IPと仮想ループバック

重要:

- Windows 10 Enterprise マルチセッションは、リモートデスクトップIP仮想化 (仮想IP) をサポートしていません。また、Windows 10 Enterprise マルチセッションでは、リモートデスクトップIP仮想化または仮想ループバックをサポートしていません。
- リモートデスクトップIP仮想化 (仮想IP) は、クラウドホスト型マシンではサポートされていません。 詳細については、Microsoft のドキュメントを参照してください。

リモートデスクトップIP仮想化および仮想ループバック機能は、Windows Server 2016、Windows Server 2019、およびWindows Server 2022マシンでサポートされています。これらの機能は、WindowsデスクトップOSマシンには適用されません。

Microsoftのリモートデスクトップ IP仮想化アドレス機能は、公開アプリケーションにセッションごとに一意の動的に割り当てられたIPアドレスを提供します。Citrix仮想ループバック機能を使用すると、localhost (デフォルトでは127.0.0.1) との通信に依存するアプリケーションを、localhost範囲 (127.*) 内の一意の仮想ループバックアドレスを使用するように構成できます。

CRMやCTI (Computer Telephony Integration) などの特定のアプリケーションは、アドレス指定、ライセンス、識別、または一意のIPアドレスやループバックアドレスを必要とするその他の目的でIPアドレスを使用します。他のアプリケーションは静的ポートにバインドする可能性があり、その場合、マルチユーザー環境でアプリケーションの追加インスタンスを起動しようとすると、ポートが使用中のため失敗します。このようなアプリケーションがCitrix Virtual Apps™環境で正しく機能するには、デバイスごとに一意のIPアドレスが必要です。

Remote Desktop IP Virtualization と仮想ループバックは、互いに独立した機能です。どちらか一方、または両方を使用できます。

管理者アクションの概要:

- Microsoftリモートデスクトップ IP仮想化を使用するには、Windowsサーバーでそれを有効にして構成します。(Citrix®ポリシー設定は不要です。)
- Citrix仮想ループバックを使用するには、Citrixポリシーで2つの設定を構成します。

リモートデスクトップIP仮想化 (仮想IP)

リモートデスクトップIP仮想化がWindowsサーバーで有効化および構成されている場合、セッションで実行されている構成済みの各アプリケーションは、一意のアドレスを持っているように見えます。ユーザーは、他の公開アプリケーションにアクセスするのと同じ方法で、Citrix Virtual Appsサーバー上のこれらのアプリケーションにアクセスします。プロセスがリモートデスクトップIP仮想化を必要とするのは、次のいずれかのケースです。

- プロセスがハードコードされたTCPポート番号を使用している場合
- プロセスがWindowsソケットを使用し、一意のIPアドレスまたは指定されたTCPポート番号を必要とする場合

アプリケーションが Remote Desktop IP Virtualization アドレスを使用する必要があるかどうかを判断するには：

1. Microsoftから**TCPView**ツールを入手します。このツールは、特定のIPアドレスとポートをバインドするすべてのアプリケーションを一覧表示します。TCPViewの詳細については、Microsoftドキュメントを参照してください。
2. ホスト名の代わりにアドレスが表示されるように、**IPアドレスの解決**機能を無効にします。
3. アプリケーションを起動し、**TCPView**を使用して、アプリケーションが開いているIPアドレスとポート、およびこれらのポートを開いているプロセス名を確認します。
4. サーバーのIPアドレス、0.0.0.0、または127.0.0.1を開くプロセスを構成します。
5. アプリケーションが異なるポートで同じ IP アドレスを開かないようにするには、アプリケーションの別のインスタンスを起動します。

Microsoft Remote Desktop (RD) IP仮想化の仕組み

- Microsoftサーバーで仮想IPアドレス指定を有効にする必要があります。

  たとえば、Windows Server 2016 環境では、サーバーマネージャーから **Remote Desktop Services > RD Session Host Connections** を展開して、RD IP Virtualization 機能を有効にし、セッションごとまたはプログラムごとに動的ホスト構成プロトコル (DHCP) サーバーを使用して IP アドレスを動的に割り当てる設定を構成します。Remote Desktop IP Virtualization の構成の詳細については、Microsoft ドキュメント を参照してください。
- 機能を有効にした後、セッション開始時に、サーバーはDHCPサーバーから動的に割り当てられたIPアドレスを要求します。
- The **RD IP Virtualization**機能は、リモートデスクトップ接続にセッションごとまたはプログラムごとにIPアドレスを割り当てます。複数のプログラムにIPアドレスを割り当てる場合、それらはセッションごとのIPアドレスを共有します。

- アドレスがセッションに割り当てられた後、次の呼び出しが行われるたびに、セッションはシステムのプライマリIPアドレスではなく仮想アドレスを使用します:
  `bind`、`closesocket`、`connect`、`WSAConnect`、`WSAAccept`、`getpeername`、`getsockname`、`sendto`、`WSASendTo`、`WSASocketW`、`gethostbyaddr`、`getnameinfo`、`getaddrinfo`。

リモートデスクトップセッションホスティング構成内でMicrosoft IP仮想化機能を使用する場合、アプリケーションとWinsock関数呼び出しの間に「フィルター」コンポーネントを挿入することで、アプリケーションは特定のIPアドレスにバインドされます。これにより、アプリケーションは使用すべき正しいIPアドレスのみを認識します。アプリケーションがTCPまたはUDP通信をリッスンしようとすると、自動的に割り当てられた仮想IPアドレス（またはループバックアドレス）にバインドされます。アプリケーションによって開かれた発信接続はすべて、アプリケーションにバインドされたIPアドレスから発信されます。

アドレスを返す関数（Windowsポリシーが制御する`GetAddrInfo()`など）でローカルホストIPアドレスが要求された場合、リモートデスクトップIP仮想化は返されたIPアドレスを調べ、それをセッションのリモートデスクトップIP仮想化アドレスに変更します。このような名前関数を介してローカルサーバーのIPアドレスを取得しようとするアプリケーションは、そのセッションに割り当てられた一意のリモートデスクトップIP仮想化アドレスのみを認識します。このIPアドレスは、bindやconnectなどの後続のソケット呼び出しでよく使用されます。Windowsポリシーの詳細については、「RDS IP Virtualization in Windows Server」を参照してください。

多くの場合、アプリケーションはアドレス0.0.0.0でリッスンするためにポートへのバインドを要求します。アプリケーションがこれを行い、静的ポートを使用する場合、アプリケーションの複数のインスタンスを起動することはできません。リモートデスクトップIP仮想化アドレス機能は、これらの呼び出しタイプで0.0.0.0も検索します。呼び出しを特定のリモートデスクトップIP仮想化アドレスでリッスンするように変更し、これにより、すべて異なるアドレスでリッスンしているため、同じコンピューター上の同じポートで複数のアプリケーションがリッスンできるようになります。呼び出しは、ICAセッション内であり、リモートデスクトップIP仮想化アドレス機能が有効になっている場合にのみ変更されます。たとえば、異なるセッションで実行されているアプリケーションの2つのインスタンスが両方ともすべてのインターフェイス（0.0.0.0）と特定のポート（9000など）にバインドしようとすると、VIPAddress1:9000とVIPAddress2:9000にバインドされ、競合は発生しません。

仮想ループバック

「**Citrix Remote Desktop IP Virtualization loopback policy**」設定を有効にすると、各セッションが通信用に独自のループバックアドレスを持つことができます。アプリケーションが Winsock 呼び出しで localhost アドレス (デフォルト = 127.0.0.1) を使用すると、仮想ループバック機能は 127.0.0.1 を 127.X.X.X に置き換えます。ここで、X.X.X はセッション ID + 1 を表します。たとえ

ば、セッション ID が 7 の場合、127.0.0.8 となります。セッション ID が第 4 オクテット (255 を超える) を超えるという万が一の場合、アドレスは次のオクテット (127.0.1.0) に繰り上がり、最大 127.255.255.255 となります。

プロセスが仮想ループバックを必要とするのは、次のいずれかのケースです。

- プロセスが Windows ソケットループバック (localhost) アドレス (127.0.0.1) を使用している場合
- プロセスがハードコードされた TCP ポート番号を使用している場合

プロセス間通信にループバックアドレスを使用するアプリケーションには、仮想ループバックポリシー設定を使用します。追加の設定は不要です。仮想ループバックは仮想 IP に依存しないため、Microsoft サーバーを設定する必要はありません。

- 仮想 IP ループバックサポート。有効にすると、このポリシー設定により、各セッションが独自の仮想ループバックアドレスを持つことができます。この設定はデフォルトで無効になっています。この機能は、仮想 IP 仮想ループバックプログラムリストポリシー設定で指定されたアプリケーションにのみ適用されます。
- 仮想 IP 仮想ループバックプログラムリスト。このポリシー設定は、仮想 IP ループバック機能を使用するアプリケーションを指定します。この設定は、仮想 IP ループバックサポートポリシー設定が有効になっている場合にのみ適用されます。
- 仮想 IP ループバックポート除外。アプリケーションがこの設定で指定されたポートでループバックアドレスを呼び出す場合、仮想ループバックは呼び出しをセッション固有のループバックアドレスに変更しません。

関連機能

仮想ループバックが仮想 IP よりも優先されるように、次のレジストリ設定を使用できます。この機能は「優先ループバック」と呼ばれます。ただし、注意して進めてください。

- 仮想 IP と仮想ループバックの両方が有効になっている場合にのみ、優先ループバックを使用してください。そうしないと、意図しない結果が生じる可能性があります。
- レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix は、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

アプリケーションが存在するサーバーで regedit を実行します。

- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP`

- 名前: PreferLoopback, 種類: REG_DWORD, データ: 1
- 名前: PreferLoopbackProcesses, 種類: REG_MULTI_SZ, データ: \<プロセスリスト\>

ゾーン

> **注記：**
>
> Citrix Virtual Apps and Desktops™展開は、Web Studio (Webベース) と Citrix Studio (Windowsベース) の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

WANで接続された広範囲に分散した場所にまたがる展開では、ネットワークの遅延と信頼性により課題が生じる可能性があります。これらの課題を軽減するための2つのオプションがあります。

- 複数のサイトを展開し、それぞれに独自のSQL Serverサイトデータベースを持たせる。

  このオプションは、大規模なエンタープライズ展開に推奨されます。複数のサイトは個別に管理され、それぞれに独自のSQL Serverサイトデータベースが必要です。各サイトは独立したCitrix Virtual Apps™展開です。
- 単一サイト内に複数のゾーンを構成する。

  ゾーンを構成することで、リモート地域のユーザーがWANの大部分を通過することなくリソースに接続できるようになります。ゾーンを使用すると、単一のWeb Studioコンソール、Citrix Director、およびサイトデータベースから効果的なサイト管理が可能になります。これにより、リモートロケーションに個別のデータベースを含むより多くのサイトを展開、人員配置、ライセンス供与、および運用するコストを節約できます。

  ゾーンは、あらゆる規模の展開で役立ちます。ゾーンを使用すると、アプリケーションとデスクトップをエンドユーザーの近くに配置できるため、パフォーマンスが向上します。ゾーンには、冗長性と回復性のために1つ以上のControllerをローカルにインストールできますが、必須ではありません。

  サイトに構成されているControllerの数は、サイト自体に新しいControllerを追加するなどの一部の操作のパフォーマンスに影響を与える可能性があります。これを避けるため、Citrix

Virtual AppsまたはCitrix Virtual Desktops™サイトのゾーン数を50以下に制限することをお勧めします。

ゾーンのネットワーク遅延が250ミリ秒RTTを超える場合は、ゾーンではなく複数のサイトを展開することをお勧めします。

この記事全体を通して、「ローカル」という用語は、議論されているゾーンを指します。たとえば、「VDAがローカルControllerに登録する」とは、VDAがVDAが配置されているゾーン内のControllerに登録することを意味します。

このリリースでのゾーンは、XenAppバージョン6.5以前のゾーンと似ていますが、同一ではありません。たとえば、このゾーンの実装では、データコレクターはありません。サイト内のすべてのControllerは、プライマリゾーンの1つのサイトデータベースと通信します。また、このリリースではフェールオーバーゾーンと優先ゾーンの動作が異なります。

ゾーンの種類

サイトには常に1つのプライマリゾーンがあります。オプションで1つ以上のサテライトゾーンを持つこともできます。サテライトゾーンは、災害復旧、地理的に離れたデータセンター、支社、クラウド、またはクラウド内のアベイラビリティゾーンに使用できます。

プライマリゾーン:

プライマリゾーンのデフォルト名は「Primary」です。このゾーンには、SQL Serverサイトデータベース（および使用されている場合は高可用性SQLサーバー）、Web Studio、Director、Citrix StoreFront™、Citrix License Server、およびCitrix Gatewayが含まれます。サイトデータベースは常にプライマリゾーンに保持してください。

プライマリゾーンには、冗長性のために少なくとも2つのControllerが必要です。プライマリゾーンには、データベースおよびインフラストラクチャと密接に連携するアプリケーションを持つVDAを配置できます。

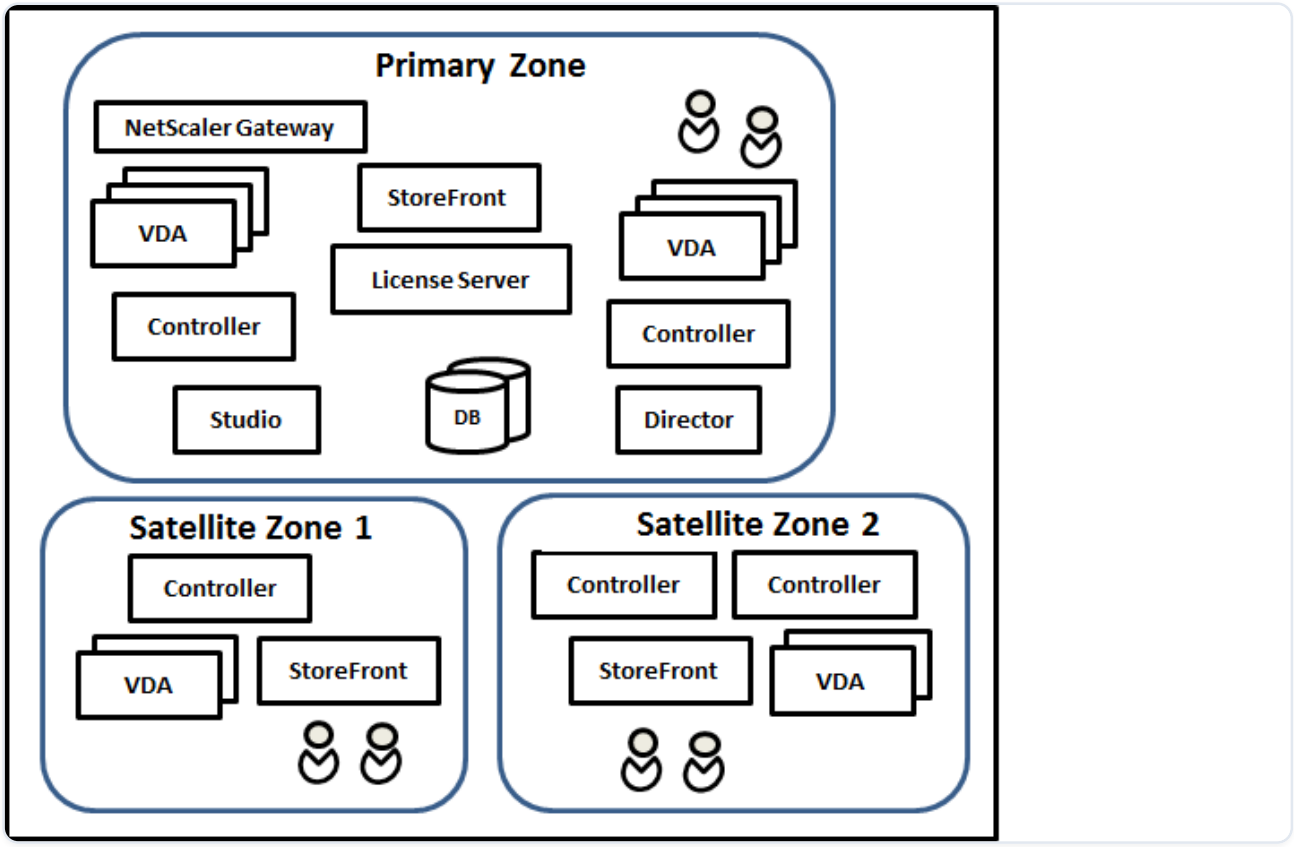
サテライトゾーン:

サテライトゾーンには、1つ以上のVDA、Controller、StoreFrontサーバー、およびCitrix Gatewayサーバーが含まれます。通常の運用では、サテライトゾーンのControllerはプライマリゾーンのデータベースと直接通信します。

サテライトゾーン、特に大規模なゾーンには、そのゾーンのマシンをプロビジョニングおよび保存するために使用されるハイパーバイザーが含まれる場合もあります。サテライトゾーンを構成する

ときは、ハイパーバイザーまたはその他のサービス接続を関連付けることができます。（その接続を使用するカタログがすべて同じゾーンにあることを確認してください。）

サイトには、固有のニーズと環境に基づいて、さまざまな構成のサテライトゾーンを含めることができます。次の図は、プライマリゾーンとサテライトゾーンの例を示しています。



図では、次のようになっています。

- **プライマリゾーン:** 2つのController、Web Studio、Director、StoreFront、License Server、およびサイトデータベース（高可用性SQL Server展開を含む）が含まれます。プライマリゾーンには、複数のVDAとCitrix Gatewayも含まれます。
- **サテライトゾーン1: Controllerを持つVDA:** サテライトゾーン1には、Controller、VDA、およびStoreFrontサーバーが含まれます。このサテライトゾーンのVDAは、ローカルのControllerに登録されます。ローカルのControllerは、プライマリゾーンのサイトデータベースおよびライセンスサーバーと通信します。

  WANに障害が発生した場合、ローカルホストキャッシュ機能により、サテライトゾーンのControllerは、そのゾーンのVDAへの接続の仲介を継続できます。このような展開は、従業員がローカルのStoreFrontサイトとローカルのControllerを使用してローカルリソースにアクセスするオフィスで効果的です。

- **サテライトゾーン2: 冗長Controllerを持つVDA:** サテライトゾーン2には、2つのController、VDA、およびStoreFrontサーバーが含まれます。これは最も回復力のあるゾーンタイプであり、WANとローカルControllerの1つが同時に障害を起こした場合でも保護を提供します。

VDAの登録先とControllerのフェールオーバー先

プライマリゾーンとサテライトゾーンを含むサイトで、VDAが最小バージョン7.7の場合:

- プライマリゾーンのVDAは、プライマリゾーンのControllerに登録します。プライマリゾーンのVDAがサテライトゾーンのControllerに登録しようとすることはありません。
- サテライトゾーンのVDAは、可能であればローカルのControllerに登録します。（これは優先Controllerと見なされます。）ローカルのControllerが利用できない場合（たとえば、これ以上VDA登録を受け入れられない、または障害が発生した場合）、VDAはプライマリゾーンのControllerに登録しようとします。この場合、サテライトゾーンのControllerが再び利用可能になっても、VDAはプライマリゾーンに登録されたままになります。サテライトゾーンのVDAが別のサテライトゾーンのControllerに登録しようとすることはありません。
- ControllerのVDA検出で自動更新が有効になっており、VDAのインストール中にControllerアドレスのリストを指定した場合、初期登録のためにそのリストからControllerがランダムに選択されます（Controllerがどのゾーンにあるかに関係なく）。そのVDAがインストールされているマシンが再起動されると、VDAはローカルゾーンのControllerへの登録を優先するようになります。
- サテライトゾーンのControllerで障害が発生した場合、可能であれば別のローカルControllerにフェールオーバーします。ローカルControllerが利用できない場合は、プライマリゾーンのControllerにフェールオーバーします。
- Controllerをゾーンの内外に移動し、自動更新が有効になっている場合、両方のゾーンのVDAは、どのControllerがローカルで、どのControllerがプライマリゾーンにあるかを示す更新されたリストを受け取ります。これにより、VDAはどのControllerに登録し、どのControllerから接続を受け入れることができるかを知ることができます。
- カタログを別のゾーンに移動すると、そのカタログ内のVDAは、カタログを移動したゾーンのControllerに再登録します。（カタログを別のゾーンに移動するときは、このゾーンと関連するホスト接続があるゾーンが適切に接続されていることを確認してください。帯域幅が制限されている場合や、高遅延の場合は、ホスト接続を関連するマシンカタログを含む同じゾーンに移動してください。）

プライマリゾーンのすべてのControllerで障害が発生した場合：

- Web Studioはサイトに接続できません。
- プライマリゾーンのVDAへの接続はできません。

- プライマリゾーンのControllerが利用可能になるまで、サイトのパフォーマンスが低下します。

VDAバージョン7.7より前のサイトの場合：

- サテライトゾーンのVDAは、ローカルゾーンおよびプライマリゾーンのControllerからの要求を受け入れます。（最小バージョン7.7のVDAは、他のサテライトゾーンのControllerからの要求を受け入れることができます。）
- サテライトゾーンのVDAは、プライマリゾーンまたはローカルゾーンのControllerにランダムに登録します。（最小バージョン7.7のVDAはローカルゾーンを優先します。）

ゾーンの優先順位

ゾーンの優先順位機能を使用するには、StoreFront 3.7およびCitrix Gateway 11.0-65.x以降を使用している必要があります。

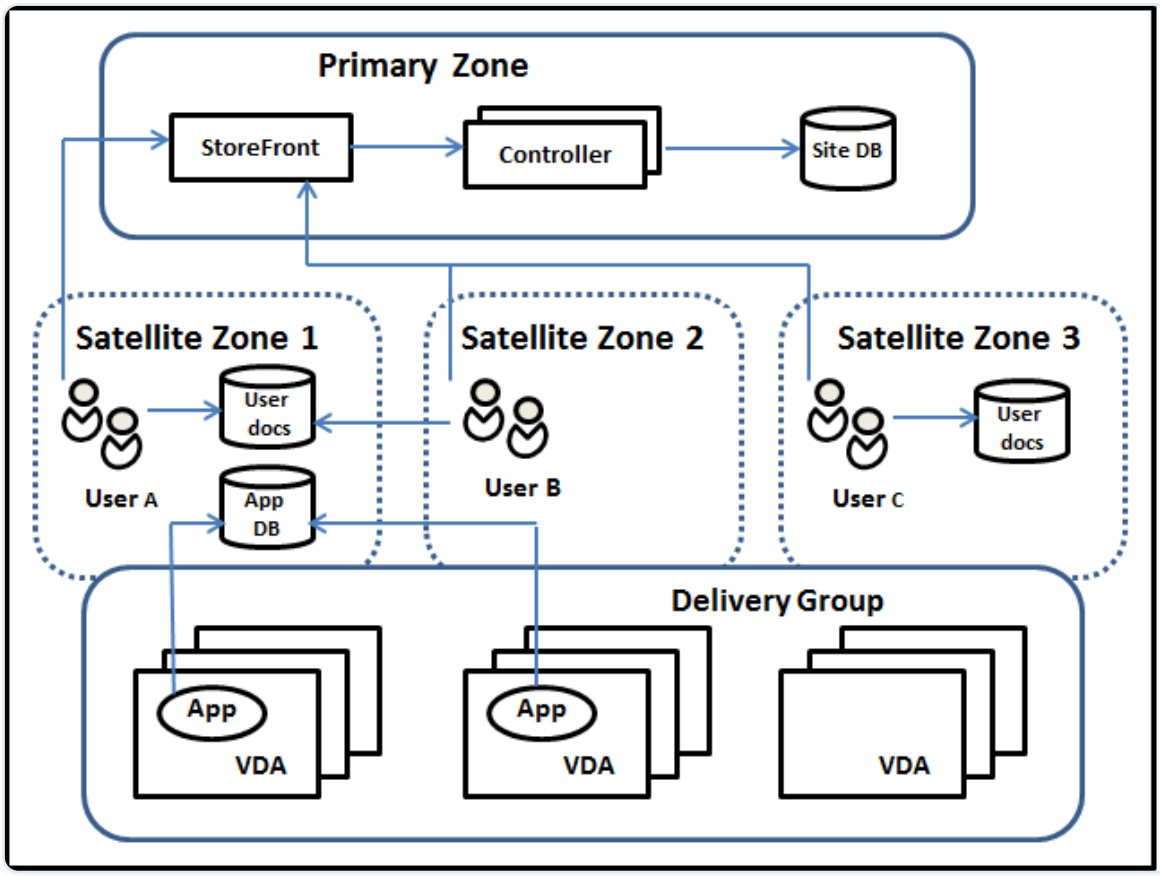
マルチゾーンサイトでは、ゾーン優先機能により、管理者はアプリケーションまたはデスクトップの起動に使用されるVDAをより柔軟に制御できます。

ゾーンの優先順位の仕組み

ゾーン優先機能には3つの形式があります。特定のゾーンのVDAを使用することを好む場合があります。その判断基準は次のとおりです。

- アプリケーションのデータが保存されている場所。これはアプリケーションホームと呼ばれます。
- ユーザーのホームデータ（プロファイルやホーム共有など）の場所。これはユーザーホームと呼ばれます。
- ユーザーの現在の場所（Citrix Workspace™アプリが実行されている場所）。これはユーザーの場所と呼ばれます。

次の図は、マルチゾーン構成の例を示しています。



この例では、VDAは3つのサテライトゾーンに分散していますが、すべて同じデリバリーグループに属しています。そのため、ブローカーはユーザーの起動リクエストに対してどのVDAを使用するかを選択する可能性があります。この例は、ユーザーがCitrix Workspaceアプリのエンドポイントを実行できる場所がいくつかあることを示しています。

- ユーザーAは、サテライトゾーン1でCitrix Workspaceアプリがインストールされたデバイスを使用しています。
- ユーザーBは、サテライトゾーン2でデバイスを使用しています。
- ユーザーのドキュメントはさまざまな場所に保存できます。
  - ユーザーAとBは、サテライトゾーン1にある共有を使用します。
  - ユーザーCは、サテライトゾーンCの共有を使用します。
  - 公開されているアプリケーションの1つは、サテライトゾーン1にあるデータベースを使用します。

ユーザーまたはアプリケーションのホームゾーンを構成することで、ユーザーまたはアプリケーションをゾーンに関連付けます。Delivery Controller™のブローカーは、リソースが利用可能な場合、これらの関連付けを使用してセッションが起動されるゾーンの選択を支援します。次のことができます。

- ユーザーをゾーンに追加して、ユーザーのホームゾーンを構成します。

- アプリケーションのプロパティを編集して、アプリケーションのホームゾーンを構成します。

ユーザーまたはアプリケーションは、一度に1つのホームゾーンしか持つことができません。（ユーザーグループのメンバーシップにより複数のゾーンメンバーシップが発生する場合、ユーザーには例外が発生する可能性があります。「その他の考慮事項」セクションを参照してください。ただし、この場合でも、ブローカーは1つのホームゾーンのみを使用します。）

ユーザーおよびアプリケーションのゾーン設定を構成できますが、ブローカーは起動に優先ゾーンを1つだけ選択します。優先ゾーンを選択するためのデフォルトの優先順位は、アプリケーションホーム \> ユーザーホーム \> ユーザーロケーションです。この順序を制限できます。(#tailoring-zone-preference)「ゾーン設定の調整」を参照してください。ユーザーがアプリケーションを起動すると、次のようになります。

- そのアプリケーションに構成済みのゾーン関連付け（アプリケーションホーム）がある場合、優先ゾーンはそのアプリケーションのホームゾーンになります。
- アプリケーションに構成済みのゾーン関連付けがないが、ユーザーに構成済みのゾーン関連付け（ユーザーホーム）がある場合、優先ゾーンはそのユーザーのホームゾーンになります。
- アプリケーションにもユーザーにも構成済みのゾーン関連付けがない場合、優先ゾーンはユーザーがCitrix Workspaceアプリインスタンスを実行しているゾーン（ユーザーロケーション）になります。そのゾーンが定義されていない場合、ランダムなVDAとゾーンの選択が使用されます。優先ゾーン内のすべてのVDAに負荷分散が適用されます。優先ゾーンがない場合、Delivery Group内のすべてのVDAに負荷分散が適用されます。

ゾーンの優先順位の調整

ユーザーまたはアプリケーションのホームゾーンを構成（または削除）する際、ゾーン設定の使用方法をさらに制限することもできます。

- **必須のユーザーホームゾーンの使用：** Delivery Groupでは、ユーザーのホームゾーン（構成されている場合）でセッションを起動するように指定できます。ホームゾーンに利用可能なリソースがない場合でも、他のゾーンへのフェールオーバーは行われません。この制限は、ゾーン間で大きなプロファイルやデータファイルをコピーするリスクを回避する必要がある場合に役立ちます。つまり、セッションを別のゾーンで起動するよりも、セッションの起動を拒否する方が望ましいということです。
- **必須のアプリケーションホームゾーンの使用：** 同様に、アプリケーションのホームゾーンを構成する際に、そのアプリケーションをそのゾーンでのみ起動し、アプリケーションのホームゾーンにリソースがない場合でも別のゾーンへのフェールオーバーを行わないように指定できます。

- **アプリケーションホームゾーンなし、および構成済みのユーザーホームゾーンを無視：** アプリケーションのホームゾーンを指定しない場合、そのアプリケーションを起動する際に構成済みのユーザーゾーンを考慮しないように指定することもできます。たとえば、一部のユーザーが異なるホームゾーンを持っている場合でも、ユーザーがデバイスの近くのVDAでアプリケーションを実行し、ユーザーロケーションゾーン設定を使用することを好む場合があります。

優先ゾーンがセッションの使用に与える影響

ユーザーがアプリケーションまたはデスクトップを起動すると、ブローカーは既存のセッションを使用するよりも優先ゾーンを使用することを優先します。

アプリケーションまたはデスクトップを起動するユーザーが、起動するリソースに適したセッションをすでに持っている場合（たとえば、アプリケーションのセッション共有を使用できる場合、または起動するリソースがすでに実行されているセッションの場合）、そのセッションがユーザー/アプリケーションの優先ゾーン以外のゾーンにあるVDAで実行されていると、システムは新しいセッションを作成する可能性があります。これにより、そのユーザーのセッション要件にとって優先度の低いゾーンのセッションに再接続するよりも、正しいゾーンでの起動が満たされます（利用可能な容量がある場合）。

到達不能になる孤立したセッションを防ぐため、既存の切断されたセッションへの再接続は、たとえ優先ゾーン以外にあっても許可されます。

起動を満たすためのセッションの望ましさの順序は次のとおりです。

1. 優先ゾーン内の既存のセッションに再接続する。
2. 優先ゾーン以外のゾーンにある、既存の切断されたセッションに再接続する。
3. 優先ゾーンで新しいセッションを開始する。
4. 優先ゾーン以外のゾーンにある、接続済みの既存セッションに再接続する。
5. 優先ゾーン以外のゾーンで新しいセッションを開始する。

その他のゾーン優先度に関する考慮事項

- ユーザーグループ（セキュリティグループなど）にホームゾーンを構成した場合、そのグループのユーザー（直接的または間接的なメンバーシップを通じて）は指定されたゾーンに関連付けられます。ただし、ユーザーは複数のセキュリティグループのメンバーになることができ、その結果、他のグループメンバーシップを通じて異なるホームゾーンが構成される可能性があります。このような場合、そのユーザーのホームゾーンの決定は曖昧になることがあります。

ユーザーがグループメンバーシップを通じて取得したものではない構成済みのホームゾーンを持っている場合、そのゾーンがゾーン優先度に使用されます。グループメンバーシップを通じて取得されたゾーン関連付けはすべて無視されます。

ユーザーがグループメンバーシップのみを通じて取得した複数の異なるゾーン関連付けを持っている場合、ブローカーはゾーンの中からランダムに選択します。ブローカーがこの選択を行うと、そのゾーンは、ユーザーのグループメンバーシップが変更されるまで、その後のセッション起動に使用されます。

- ユーザーロケーションゾーンの優先度には、デバイスが接続しているCitrix GatewayによるエンドポイントデバイスのCitrix Workspaceアプリの検出が必要です。Citrix Gatewayは、IPアドレスの範囲を特定のゾーンに関連付けるように構成する必要があり、検出されたゾーンIDはStoreFrontを介してControllerに渡される必要があります。

ゾーンの優先度について詳しくは、「ゾーンの優先度の内部」を参照してください。

考慮事項、要件、およびベストプラクティス

- ゾーンには、次の項目を配置できます: コントローラー、マシンカタログ、ホスト接続、ユーザー、およびアプリケーション。カタログがホスト接続を使用する場合、カタログと接続が同じゾーンにあることを確認してください。(ただし、低遅延で高帯域幅の接続が利用可能な場合は、異なるゾーンに配置することもできます。)
- サテライトゾーンに項目を配置すると、サイトがそれらの項目や関連する他のオブジェクトとどのようにやり取りするかに影響します。
    - コントローラーがサテライトゾーンに配置されると、それらのマシンは同じゾーン内のハイパーバイザーおよび VDA に対して良好な（ローカル）接続性を持つと想定されます。そのサテライトゾーン内のコントローラーは、それらのハイパーバイザーおよび VDA マシンを処理する際に、プライマリゾーン内のコントローラーよりも優先的に使用されます。
    - ハイパーバイザー接続がサテライトゾーンに配置されると、そのハイパーバイザー接続を介して管理されるすべてのハイパーバイザーもそのサテライトゾーンに存在すると想定されます。そのサテライトゾーン内のコントローラーは、そのハイパーバイザー接続と通信する際に、プライマリゾーン内のコントローラーよりも優先的に使用されます。
    - When a machine catalog is placed into a satellite zone, it is assumed that all the VDA machines in that catalog are in the satellite zone. Local Controllers are used in preference to Controllers in the primary zone when attempting to register with the site, after the Controller list auto-update mechanism has activated after the first registration of each VDA.
    - Citrix Gateway instances can also be associated with zones. This is done as part of the StoreFront Optimal HDX™ Routing configuration rather than, as for the other elements

described here, as part of the site configuration. When a Citrix Gateway is associated with a zone, it is preferred to be used when HDX connections to VDA machines in that zone are used.

- 生産サイトを作成し、最初のカタログとデリバリーグループを作成すると、すべての項目はプライマリゾーンに配置されます。この初期設定が完了するまで、サテライトゾーンを作成することはできません。（空のサイトを作成した場合、プライマリゾーンには最初にコントローラーのみが含まれます。カタログとデリバリーグループを作成する前または後にサテライトゾーンを作成できます。）
- 1つ以上の項目を含む最初のサテライトゾーンを作成すると、サイト内の他のすべての項目はプライマリゾーンに残ります。
- The primary zone is named 'Primary' by default; you can change that name. Although Web Studio indicates which zone is the primary zone, it is best practice to use an easily identifiable name for the primary zone. You can reassign the primary zone (that is, make another zone the primary zone), but it should always contain the site database and any high availability servers.
- Always keep the site database in the primary zone.
- ゾーンを作成した後、後で項目をあるゾーンから別のゾーンに移動できます。この柔軟性により、近接して動作するのが最適な項目を分離できる可能性があります。たとえば、カタログ内のマシンを作成する接続（ホスト）とは異なるゾーンにカタログを移動すると、パフォーマンスに影響を与える可能性があります。ゾーン間で項目を移動する前に、意図しない潜在的な影響を考慮してください。カタログとそれが使用するホスト接続は同じゾーンに、または十分に接続されたゾーン（たとえば、低遅延で高帯域幅のネットワーク経由）に保持してください。
- 最適なパフォーマンスを得るには、Web StudioとDirectorはプライマリゾーンにのみインストールしてください。Web StudioとDirectorはWebアプリケーションであるため、サテライトゾーン（たとえば、プライマリゾーンがアクセス不能になった場合のフェイルオーバーとして使用するコントローラーを含むサテライトゾーン）からアクセスできます。
- Ideally, Citrix Gateway in a satellite zone is used for user connections coming into that zone from other zones or external locations, although you can use it for connections within the zone.
- Remember: To use the zone preference feature, you must be using minimum StoreFront 3.7 and Citrix Gateway 11.0-65.x.

接続品質の制限

サテライトゾーンのControllerは、サイトデータベースと直接SQL対話を行います。これにより、サテライトゾーンとサイトデータベースを含むプライマリゾーン間のリンクの品質にいくつかの制限が課せられます。具体的な制限は、サテライトゾーンに展開されているVDAの数と、それらのVDA上のユーザーセッションの数に比例します。したがって、VDAとセッションが少ないサテラ

イトゾーンは、VDAとセッションが多いサテライトゾーンよりも、データベースへの接続品質が低い場合でも機能できます。

詳しくは、「待機時間とSQLブロッキングクエリの改善」を参照してください。

ブローカリングパフォーマンスに対する待機時間の影響

ゾーンによってユーザーは待機時間の長いリンク上にいても、ローカルブローカーがあれば利用できますが、追加の待機時間は必然的にエンドユーザーエクスペリエンスに影響を与えます。ユーザーが行うほとんどの作業において、サテライトゾーンのControllerとサイトデータベース間のラウンドトリップによって引き起こされる遅延を経験します。

アプリケーションを起動する場合、セッションブローカリングプロセスがセッション起動要求を送信するのに適したVDAを特定する際に、追加の遅延が発生します。

ゾーンの作成と管理

フル管理者であれば、すべてのゾーン作成および管理タスクを実行できます。ただし、ゾーンの作成、編集、削除を許可するカスタムロールを作成することもできます。ゾーン間でアイテムを移動する場合、ゾーン関連の権限（ゾーン読み取り権限を除く）は必要ありませんが、移動するアイテムに対する編集権限が必要です。たとえば、あるゾーンから別のゾーンにカタログを移動するには、そのカタログに対する編集権限が必要です。詳しくは、「委任管理」を参照してください。

Citrix Provisioning™を使用する場合： Citrix Provisioningコンソールはゾーンを認識しないため、Web Studioを使用してサテライトゾーンのカタログを作成することをお勧めします。Web Studioでカタログを作成し、正しいサテライトゾーンを指定します。その後、Citrix Provisioningコンソールを使用して、そのカタログ内のマシンをプロビジョニングします。（Citrix Provisioningウィザードを使用してカタログを作成した場合、カタログはプライマリゾーンに配置されます。後でWeb Studioを使用してサテライトゾーンに移動する必要があります。）

ゾーンの作成

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. アクションバーで を選択します。
4. ゾーンの名前と説明（オプション）を入力します。名前はサイト内で一意である必要があります。
5. 新しいゾーンに配置するアイテムを選択します。選択可能なアイテムのリストをフィルター処理または検索できます。空のゾーンを作成することもできます。その場合は、どのアイテムも選択しないでください。

6. をクリックします。

この方法の代替として、Web Studioで1つ以上の項目を選択し、その後、アクションバーで**ゾーンの作成**を選択できます。

ゾーン名または説明の変更

1. Web Studioにサインインします。
2. 左ペインで**ゾーン**を選択します。
3. 中央ペインでゾーンを選択し、その後、アクションバーで**ゾーンの編集**を選択します。
4. ゾーン名、説明、またはその両方を変更します。プライマリゾーンの名前を変更する場合は、そのゾーンがプライマリゾーンとして容易に識別できる状態を維持するようにしてください。
5. **保存**または**適用**をクリックします。

ゾーン間でアイテムを移動する

1. Web Studioにサインインします。
2. 左ペインで**ゾーン**を選択します。
3. 中央ペインでゾーンを選択し、その後、1つ以上の項目を選択します。
4. 項目を移動先のゾーンにドラッグするか、アクションバーで**項目の移動**を選択し、その後、移動先のゾーンを指定します。

確認メッセージには、選択した項目が一覧表示され、それらすべてを移動してもよいかどうかが尋ねられます。

注意: カタログがハイパーバイザーまたはその他のサービスへのホスト接続を使用する場合、カタログと接続の両方を同じゾーンに配置します。そうしないと、パフォーマンスに影響が出る可能性があります。一方を移動する場合は、もう一方も移動してください。

ゾーンを削除する

ゾーンを削除するには、ゾーンが空である必要があります。プライマリゾーンは削除できません。

1. Web Studioにサインインします。
2. 左ペインで**ゾーン**を選択します。
3. 中央ペインでゾーンを選択します。
4. アクションバーから**ゾーンの削除**を選択します。ゾーンが空でない場合（アイテムが含まれている場合）、それらのアイテムを移動するゾーンを選択するよう求められます。
5. 削除を確認します。

ユーザーのホームゾーンを追加する

ユーザーのホームゾーンを構成することは、*ユーザーをゾーンに追加する*とも呼ばれます。

1. Web Studioにサインインします。
2. 左ペインで**ゾーン**を選択し、中央ペインでゾーンを選択します。
3. アクションバーで**ゾーンにユーザーを追加**を選択します。
4. **ゾーンにユーザーを追加**ダイアログボックスで、**追加**をクリックし、ゾーンに追加するユーザーとユーザーグループを選択します。すでにホームゾーンを持つユーザーを指定した場合、メッセージには2つの選択肢が表示されます:**はい** = ホームゾーンを持たない指定したユーザーのみを追加する、**いいえ** = ユーザー選択ダイアログに戻る。
5. **OK**をクリックします。

ホームゾーンが構成されているユーザーの場合、セッションをそのホームゾーンからのみ起動するように要求できます。

1. デリバリーグループを作成または編集します。
2. 「**ユーザー**」ページで、「**ユーザーのホームゾーンでセッションを起動するよう要求する（構成されている場合）**」チェックボックスをオンにします。

そのデリバリーグループのユーザーが起動するすべてのセッションは、そのユーザーのホームゾーン内のマシンから起動する必要があります。デリバリーグループ内のユーザーにホームゾーンが構成されていない場合、この設定は無効です。

ユーザーのホームゾーンを削除する

この手順は、ゾーンからユーザーを削除することとも呼ばれます。

1. Web Studioにサインインします。
2. 左側のペインで「**ゾーン**」を選択し、中央のペインでゾーンを選択します。
3. アクションバーで「**ゾーンからユーザーを削除**」を選択します。
4. 「**ゾーンにユーザーを追加**」ダイアログボックスで、「**削除**」をクリックし、ゾーンから削除するユーザーとグループを選択します。この操作では、ユーザーはゾーンからのみ削除されます。これらのユーザーは、所属するデリバリーグループおよびアプリケーショングループに残ります。
5. プロンプトが表示されたら削除を確定します。

アプリケーションのホームゾーンを管理する

アプリケーションのホームゾーンを構成することは、アプリケーションをゾーンに追加することとも呼ばれます。デフォルトでは、マルチゾーン環境では、アプリケーションにホームゾーンはありません。

アプリケーションのホームゾーンは、アプリケーションのプロパティで指定されます。アプリケーションをグループに追加するとき、または後でアプリケーションのプロパティを構成できます。

- デリバリーグループを作成する、アプリケーショングループを作成する、または既存のグループにアプリケーションを追加するときに、ウィザードの「**アプリケーション**」ページで「**プロパティ**」を選択します。
- アプリケーションの追加後にアプリケーションのプロパティを変更するには、左側のペインで「**アプリケーション**」を選択します。アプリケーションを選択し、アクションバーで「**アプリケーションプロパティの編集**」を選択します。

アプリケーションのプロパティ/設定の ページで、次の操作を行います。

- アプリケーションにホームゾーンを設定する場合：
  - **選択したゾーンを使用して決定する**ラジオボタンを選択し、ゾーンを選択します。
  - アプリケーションを、選択したゾーンからのみ（他のゾーンからは起動しないように）起動する場合は、ゾーン選択の下にあるチェックボックスをオンにします。
- アプリケーションにホームゾーンを設定しない場合：
  - **ホームゾーンを構成しない**ラジオボタンを選択します。
  - このアプリケーションを起動する際に、ブローカーが構成済みのユーザーゾーンを考慮しないようにする場合は、ラジオボタンの下にあるチェックボックスをオンにします。この場合、アプリケーションのホームゾーンもユーザーのホームゾーンも、このアプリケーションをどこで起動するかを決定するために使用されません。

ゾーンの指定を含むその他のアクション

少なくとも1つのサテライトゾーンを作成した後、ホスト接続を追加するか、カタログを作成する際にゾーンを指定できます。

通常、プライマリゾーンがデフォルトです。Machine Creation Services™を使用してカタログを作成する場合、ホスト接続用に構成されたゾーンが自動的に選択されます。

サイトにサテライトゾーンが含まれていない場合、プライマリゾーンが想定され、ゾーン選択ボックスは表示されません。

モニター

管理者とヘルプデスク担当者は、さまざまな機能とツールを使用してCitrix Virtual Apps and Desktops™サイトを監視できます。これらのツールを使用すると、以下を監視できます。

- ユーザーセッションとセッションの使用状況
- ログオンパフォーマンス
- 接続とマシン（障害を含む）
- 負荷評価
- 履歴トレンド
- インフラストラクチャ

Citrix Director (シトリックス ディレクター)

Directorは、監視とトラブルシューティング、およびエンドユーザーのサポートタスクの実行に使用できるリアルタイムのWebツールです。

詳細については、Director の記事を参照してください。

構成ログ

構成ログを使用すると、管理者はサイトに対する管理上の変更を追跡できます。構成ログは、構成変更が行われた後の問題の診断とトラブルシューティング、変更管理と構成の追跡を支援し、管理アクティビティを報告するのに役立ちます。

Studioからログに記録された情報を表示し、レポートを生成できます。また、Directorのトレンドビューでログに記録された項目を表示し、構成変更の通知を受け取ることもできます。この機能は、Studioにアクセスできない管理者にとって役立ちます。

トレンドビューは、一定期間にわたる構成変更の履歴データを提供します。これにより、管理者はサイトに対してどのような変更がいつ、誰によって行われたかを評価し、問題の原因を特定できます。このビューでは、構成情報が次の3つのカテゴリに分類されます。

- 接続障害
- 失敗したシングルセッションマシン

- 失敗したマルチセッションマシン

構成ログを有効にして構成する方法の詳細については、構成ログを参照してください。Directorの記事では、そのツールからログに記録された情報を表示する方法について説明しています。

イベントログ

Citrix Virtual Apps and Desktops内のサービスは、発生したイベントをログに記録します。イベントログは、操作の監視とトラブルシューティングに使用されます。

詳細については、イベントログを参照してください。個々の機能の記事にもイベント情報が含まれている場合があります。

構成ログ

構成ログは、サイト構成の変更と管理アクティビティをデータベースにキャプチャする機能です。この機能はデフォルトで有効になっています。ログに記録されたコンテンツは、次の目的で使用できます。

- 構成変更後に発生した問題を診断し、トラブルシューティングします。ログは追跡記録を提供します。
- 変更管理を支援し、構成を追跡します。
- 管理アクティビティを報告します。

Citrix Studioから、構成ログ設定の指定、構成ログの表示、HTMLおよびCSVレポートの生成を行うことができます。構成ログの表示は、日付範囲や全文検索結果でフィルターできます。必須ログが有効になっている場合、ログに記録できない構成変更は行えません。適切な権限があれば、構成ログからエントリを削除できます。構成ログ機能を使用してログコンテンツを編集することはできません。

構成ログは、PowerShell SDKと構成ログサービスを使用します。構成ログサービスは、サイト内のすべてのControllerで実行されます。いずれかのControllerで障害が発生した場合、別のController上のサービスがログ要求を自動的に処理します。

デフォルトでは、構成ログ機能は有効になっており、サイト作成時に作成されるデータベース（サイト構成データベース）を使用します。データベースの別の場所を指定することもできます。構成ログデータベースは、サイト構成データベースと同じ高可用性機能をサポートしています。

構成ログへのアクセスは、委任管理を通じて、「ログ設定の編集」および「構成ログの表示」の権限によって制御されます。

構成ログは作成時にローカライズされます。たとえば、英語で作成されたログは、閲覧者のロケールに関係なく英語で読み取られます。

記録される内容

Studio、Director、およびPowerShellスクリプトから開始された構成変更と管理アクティビティが記録されます。記録される構成変更の例には、以下に関する作業（作成、編集、削除、割り当て）が含まれます。

- マシンカタログ
- デリバリーグループ（電源管理設定の変更を含む）
- 管理者ロールとスコープ
- ホストリソースと接続
- Studioを介したCitrixポリシー

ログに記録される管理変更の例は次のとおりです。

- 仮想マシンまたはユーザーデスクトップの電源管理
- StudioまたはDirectorがユーザーにメッセージを送信する

次の操作はログに記録されません。

- 仮想マシンのプール管理による電源投入などの自律的な操作。
- グループポリシー管理コンソール (GPMC) を介して実装されたポリシーアクション。これらのアクションのログを表示するには、Microsoftツールを使用してください。
- レジストリ、データベースへの直接アクセス、またはStudio、Director、PowerShell以外のソースを介して行われた変更。
- 展開が初期化されると、最初の構成ログサービスインスタンスが構成サービスに登録されたときに構成ログが利用可能になります。したがって、構成の初期段階（たとえば、データベーススキーマが取得および適用されたとき、ハイパーバイザーが初期化されたとき）はログに記録されません。

構成ログの管理

デフォルトでは、構成ログはサイトを作成したときに作成されるデータベース（サイト構成データベースとも呼ばれます）を使用します。Citrixは、以下の理由により、構成ログデータベース（および監視データベース）に別の場所を使用することをお勧めします。

- 構成ログデータベースのバックアップ戦略は、サイト構成データベースのバックアップ戦略とは異なる可能性があります。
- 構成ログ（および監視サービス）のために収集されるデータ量が多いと、サイト構成データベースで利用可能な領域に悪影響を及ぼす可能性があります。
- これにより、3つのデータベースの単一障害点が分割されます。

構成ログをサポートしない製品エディションには、Studioにログノードがありません。

構成ログと強制ログの有効化および無効化

デフォルトでは、構成ログは有効になっており、強制ログは無効になっています。

1. Web Studioにサインインし、左ペインで**ログ**を選択します。
2. アクションバーで**設定**を選択します。構成ログダイアログボックスにはデータベース情報が含まれており、構成ログと強制ログが有効か無効かを示します。
3. 目的のアクションを選択します:

   構成ログを有効にするには、**有効**を選択します。これはデフォルト設定です。データベースに書き込めない場合、ログ情報は破棄されますが、操作は続行されます。

   構成ログを無効にするには、**無効**を選択します。以前にログが有効になっていた場合、既存のログはPowerShell SDKで読み取り可能です。

   強制ログを有効にするには、**データベースが利用できない場合にサイト構成の変更を防止する**を選択します。通常ログに記録される構成変更または管理アクティビティは、構成ログデータベースに書き込める場合にのみ許可されます。強制ログは、構成ログが有効になっている場合（**有効**が選択されている場合）にのみ有効にできます。構成ログサービスが失敗し、高可用性が使用されていない場合、強制ログが適用されていると見なされます。そのような場合、通常ログに記録される操作は実行されません。

   強制ログを無効にするには、**Allow changes when to the site configuration when the database is not available** を選択します。構成ログデータベースにアクセスできない場合でも、構成変更と管理アクティビティが許可されます。これはデフォルト設定です。

構成ログデータベースの場所を変更する

強制ログが有効になっている場合、データベースの場所を変更することはできません。なぜなら、場所の変更にはログに記録できない短い切断間隔が含まれるためです。

1. サポートされているSQL Serverバージョンを使用して、データベースサーバーを作成します。
2. Web Studioにサインインし、左ペインで**ログ**を選択します。

3. アクションバーで**設定**を選択します。
4. 「ログ設定」ダイアログボックスで、「**ログデータベースの変更**」を選択します。
5. 「ログデータベースの変更」ダイアログボックスで、新しいデータベースサーバーを含むサーバーの場所を指定します。有効な形式については、「データベースアドレス形式」を参照してください。
6. Studioでデータベースを作成するには、「**OK**」をクリックします。プロンプトが表示されたら「**OK**」をクリックすると、データベースが自動的に作成されます。Studioは、現在のStudioユーザーの資格情報を使用してデータベースにアクセスしようとします。失敗した場合は、データベースユーザーの資格情報の入力を求められます。その後、Studioはデータベーススキーマをデータベースにアップロードします。（資格情報はデータベース作成中のみ保持されます。）
7. データベースを手動で作成するには、「**データベーススクリプトの生成**」をクリックします。生成されたスクリプトには、データベースを手動で作成するための手順が含まれています。スキーマをアップロードする前に、データベースが空であり、少なくとも1人のユーザーがデータベースにアクセスして変更する権限を持っていることを確認してください。

以前のデータベースの構成ログデータは、新しいデータベースにはインポートされません。ログを取得する際に、両方のデータベースからログを集約することはできません。新しい構成ログデータベースの最初のログエントリは、データベースの変更が発生したことを示しますが、以前のデータベースを特定するものではありません。

構成ログコンテンツの表示

構成変更や管理アクティビティを開始すると、StudioおよびDirectorによって作成された上位レベルの操作が、Studioの右上ペインに表示されます。上位レベルの操作は、1つ以上のサービスおよびSDK呼び出し（下位レベルの操作）をもたらします。上位ペインで上位レベルの操作を選択すると、下位ペインに下位レベルの操作が表示されます。

操作が完了する前に失敗した場合、ログ操作がデータベースで完了しない可能性があります。たとえば、開始レコードに対応する停止レコードがない場合があります。そのような場合、ログには情報が不足していることが示されます。時間範囲に基づいてログを表示すると、ログ内のデータが条件に一致する場合、不完全なログが表示されます。たとえば、過去5日間のすべてのログが要求され、過去5日間に開始時刻があるが終了時刻がないログが存在する場合、それは含まれます。

PowerShellコマンドレットを呼び出すスクリプトを使用する場合、親の上位レベルの操作を指定せずに下位レベルの操作を作成すると、構成ログは代理の上位レベルの操作を作成します。

構成ログコンテンツを表示するには、Studioナビゲーションペインで「**ログ**」を選択します。デフォルトでは、中央ペインにログコンテンツが日付ごとに区切られて時系列順（最新のエントリが最初）に表示されます。次のことができます。

- 列ヘッダーで表示を並べ替えます。
- 日付間隔を指定するか、 ボックスにテキストを入力して表示をフィルターします。検索を使用した後に標準表示に戻るには、 ボックスのテキストをクリアします。
- テーブルの右上隅にある アイコンを選択して、表示する列を選択します。たとえば、管理者がWeb Studio へのアクセスに使用する IP アドレスを表示するには、アイコンをクリックして 列を追加します。

レポートを生成する

構成ログデータを含むCSVおよびHTMLレポートを生成できます。

- CSVレポートには、指定された時間間隔のすべてのログデータが含まれています。データベース内の階層データは、単一のCSVテーブルにフラット化されます。データに優先順位はなく、書式設定も使用されず、人間が読み取れることは想定されていません。ファイル（MyReportという名前）には、普遍的に利用可能な形式でデータが含まれています。CSVファイルは、データのアーカイブや、Microsoft Excelなどのレポート作成ツールやデータ操作ツールのデータソースとしてよく使用されます。
- HTMLレポートは、指定された時間間隔のログデータを人間が読み取れる形式で提供します。変更を確認するための構造化されたナビゲート可能なビューを提供します。HTMLレポートは、SummaryとDetailsという2つのファイルで構成されます。Summaryには、各操作がいつ、誰によって行われ、どのような結果になったかなど、高レベルの操作が一覧表示されます。各操作の横にある**詳細**リンクをクリックすると、Detailsファイル内の低レベルの操作に移動し、追加情報が提供されます。

構成ログレポートを生成するには、Studioナビゲーションペインで**Logging**を選択し、アクションバーで**Create custom report**を選択します。

- レポートの日付範囲を選択します。
- レポート形式（CSV、HTML、またはその両方）を選択します。
- レポートを保存する場所を参照します。

構成ログコンテンツを削除する

構成ログを削除するには、特定の委任管理権限とSQL Serverデータベース権限が必要です。

- **委任管理:** 展開構成の読み取りを許可する委任管理ロールが必要です。完全管理者ロールにはこの権限があります。カスタムロールには、カテゴリでまたはが選択されている必要があります。

  構成ログデータを削除する前にバックアップを作成するには、カスタムロールのカテゴリでまたはが選択されている必要もあります。

- **SQL Serverデータベース:** データベースからレコードを削除する権限を持つSQL Serverログインが必要です。これには2つの方法があります。

  - データベースサーバー上のあらゆるアクティビティを実行できるsysadminサーバー役割を持つSQL Serverデータベースログインを使用します。または、`serveradmin`または`setupadmin`サーバー役割を使用すると、削除操作を実行できます。
  - 展開でより高いセキュリティが必要な場合は、データベースからレコードを削除する権限を持つデータベースユーザーにマッピングされた非sysadminデータベースログインを使用します。

    a. SQL Server Management Studioで、「sysadmin」以外のサーバー役割を持つSQL Serverログインを作成します。

    b. ログインをデータベース内のユーザーにマッピングします。SQL Serverは、ログインと同じ名前のユーザーをデータベースに自動的に作成します。

    c. データベースロールメンバーシップで、データベースユーザーのロールメンバーを少なくとも1つ指定します: `ConfigurationLoggingSchema_ROLE` または `dbowner`。

    詳細については、SQL Server Management Studioのドキュメントを参照してください。

構成ログを削除するには:

1. Web Studioにサインインし、左ペインで を選択します。
2. アクションバーで を選択します。
3. ログを削除する前にバックアップを作成するかどうかを尋ねられます。バックアップを作成することを選択した場合、バックアップアーカイブが保存される場所に移動します。バックアップはCSVファイルとして作成されます。

構成ログがクリアされると、ログの削除が、空のログに最初に記録されるアクティビティになります。そのエントリには、誰がいつログを削除したかに関する詳細が記載されています。

APIおよびPowerShellログの表示

現在のセッション中に実行されたAPIリクエストを監視するには、 タブをクリックします。Web Studioからサインアウトすると、APIログはクリアされます。

その日に実行したUIアクションに対応するPowerShellコマンドを表示するには、 タブをクリックします。

構成ログにメタデータを関連付ける

ログレコードに `MetadataMap` と呼ばれる `name-value` ペアを関連付けることで、構成ログにメタデータを添付できます。

> **注:**
>
> - メタデータは、高レベルの操作オブジェクトにのみ添付できます。
> - メタデータは、実行時に既存のレコードに関連付けられます。

メタデータを設定する

ログレコードを `MetadataMap` に関連付けるには、PowerShellコマンド `Set-LogHighLevelOperationMetadata` を実行します。 `Set-LogHighLevelOperationMetadata` は次のパラメーターを受け取ります。

- **Id**: 上位レベルの操作のID。
- **InputObject**: メタデータを追加する上位レベルの操作。これは、上位レベルの操作オブジェクトまたはオブジェクトのリストがPowerShellコマンドに渡される `Id` パラメーターの代替です。
- **Name**: 追加するメタデータのプロパティ名。このプロパティは、指定された上位レベルの操作に対して一意である必要があります。このプロパティには、次の文字を含めることはできません: ()\/;:#.*?=<>|'"。
- **Value**: プロパティの値。
- **Map**: プロパティの(名前、値)ペアの辞書。これは、 `-Name` および `-Value` パラメーターを使用してメタデータを設定する代替手段です。

たとえば、Id 40を持つすべての高レベルログレコードにメタデータを添付するには、次のPowerShellコマンドを実行します。

```
Get-LogHighLevelOperation – Id 40 | Set-LogHighLevelOperationMetadata -Name A -Value B
```

ユーザー `abc@example.com` を持つ上位レベルのレコードにメタデータを添付するには、次のPowerShellコマンドを実行します。

```
Get-LogHighLevelOperation – User `abc@example.com` | Set-
LogHighLevelOperationMetadata -Name C -Value D
```

メタデータを使用して取得する

関連付けられたメタデータを使用してログレコードを取得するには、次のPowerShellコマンドを実行します。

- キーと値で検索:

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- 値で任意のキーを検索:

  ```
  Get-LogHighLevelOperation -Metadata "*:Value"
  ```

- キーと任意の値で検索:

  ```
  Get-LogHighLevelOperation -Metadata "Key:*"
  ```

メタデータを削除する

関連付けられたメタデータを削除するには、PowerShell コマンド `Remove-LogHighLevelOperationMetadata` を実行します。 `Remove-LogHighLevelOperationMetadata` は次のパラメーターを受け入れます:

- **Id**: 高レベル操作のID。
- **InputObject**: メタデータを追加する高レベル操作。これは、高レベル操作オブジェクトまたはオブジェクトのリストがPowerShellコマンドに渡される `Id`` パラメーターの代替です。
- **Name**: 削除するメタデータのプロパティ名。指定されたオブジェクトのすべてのメタデータを削除するには、$null に設定します。
- **Map**: プロパティの (名前、値) ペアの辞書。これは、ハッシュテーブル (@{"name1" = "val1"; "name2" = "val2"} で作成) または文字列辞書 (new-object "System.Collections.Generic.Dictionary" で作成) のいずれかです。マップ内のキーと名前が一致するプロパティは削除されます。

イベントログ

以下の記事では、Citrix Virtual Apps and Desktops 内のサービスによってログに記録される可能性のあるイベントを一覧表示し、説明します。

この情報は網羅的ではありません。追加のイベント情報については、個々の機能記事を確認してください。

- Citrix Broker Service イベント
- Citrix FMA Service SDK イベント
- Citrix コンフィグレーションサービス イベント
- Citrix デリゲート管理サービス イベント

ディレクター

Directorは、Citrix Virtual Apps and Desktops向けの監視およびトラブルシューティングコンソールです。

Directorのアーキテクチャ(/en-us/citrix-virtual-apps-desktops/2411/media/director-architecture.png)

Directorは以下にアクセスできます。

- Analytics、Performance Manager、およびNetwork Inspectorと統合された統合コンソールを使用して、Broker Agentからのリアルタイムデータ。Citrix Virtual Apps™またはDesktops環境におけるネットワークに起因するボトルネックを特定するために、以下の分析はCitrix ADMによって提供されます。
  - 健全性と容量の保証のためのパフォーマンス管理
  - 履歴トレンドとネットワーク分析
- Configuration Loggingデータベースにアクセスするために、Monitorデータベースに保存されている履歴データ。
- Citrix ADMを使用してCitrix GatewayからのICA®データ。
  - Citrix Virtual AppsまたはDesktops向けの仮想アプリケーション、デスクトップ、およびユーザーのエンドユーザーエクスペリエンスの可視性を得る。
  - 効果的なトラブルシューティングのために、ネットワークデータとアプリケーションデータおよびリアルタイムメトリックを関連付ける。
  - Citrix Virtual Desktop 7 Director監視ツールと統合する。

Directorは、Citrix Virtual AppsまたはDesktopsサイトのリアルタイムおよび履歴の健全性監視を提供するトラブルシューティングダッシュボードを使用します。この機能により、リアルタイムで障害を確認でき、エンドユーザーが何を経験しているかをよりよく理解できます。

Director機能とDelivery Controller (DC)、VDA、およびその他の依存コンポーネントとの互換性に関する詳細については、「機能互換性マトリックス」(/ja-jp/citrix-virtual-apps-desktops/2411/director/version-matrix.html)を参照してください。

> **注:**

MeltdownおよびSpectreの投機的実行サイドチャネル脆弱性が開示されたことを受け、Citrixは関連する緩和パッチをインストールすることを推奨します。これらのパッチはSQL Serverのパフォーマンスに影響を与える可能性があります。詳細については、Microsoftサポート記事「Protect SQL Server from attacks on Spectre and Meltdown side-channel vulnerabilities」を参照してください。Citrixは、実稼働環境にパッチを展開する前に、規模をテストし、ワークロードを計画することを推奨します。

Directorは、デフォルトでDelivery Controller上のWebサイトとしてインストールされます。前提条件およびその他の詳細については、本リリースのシステム要件ドキュメントを参照してください。Directorのインストールと構成に関する具体的な情報については、Directorのインストールと構成を参照してください。

Directorにログオンする

Director Webサイトは、httpsまたは`http://<Server FQDN>/Director`にあります。

マルチサイト展開でいずれかのサイトがダウンしている場合、ダウンしているサイトへの接続を試行している間、ログオンに少し時間がかかります。

PIV スマートカード認証での Director の使用

Director は、Personal Identity Verification (PIV) ベースのスマートカード認証によるログオンをサポートするようになりました。この機能は、アクセス制御にスマートカードベースの認証を使用する組織や政府機関にとって役立ちます。 スマートカード認証には、Director サーバーおよび Active Directory での特定の構成が必要です。構成手順については、PIV スマートカード認証の構成に詳しく記載されています。

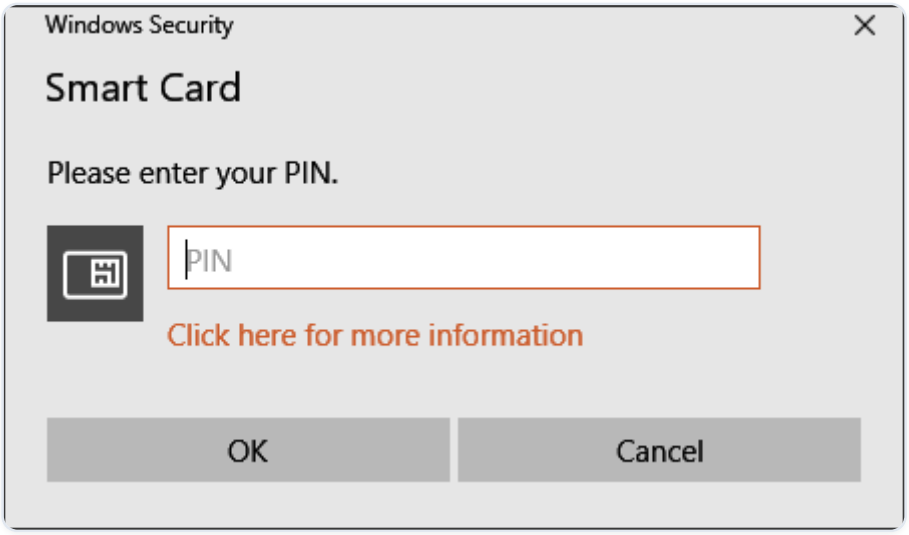
注:

スマートカード認証は、同じ Active Directory ドメインのユーザーのみがサポートされます。

必要な構成を実行した後、スマートカードを使用して Director にログオンできます。

1. スマートカードをスマートカードリーダーに挿入します。
2. ブラウザーを開き、DirectorのURL `https://<directorfqdn>/Director`にアクセスします。

3. 表示されたリストから有効なユーザー証明書を選択します。
4. スマートカードトークンを入力します。



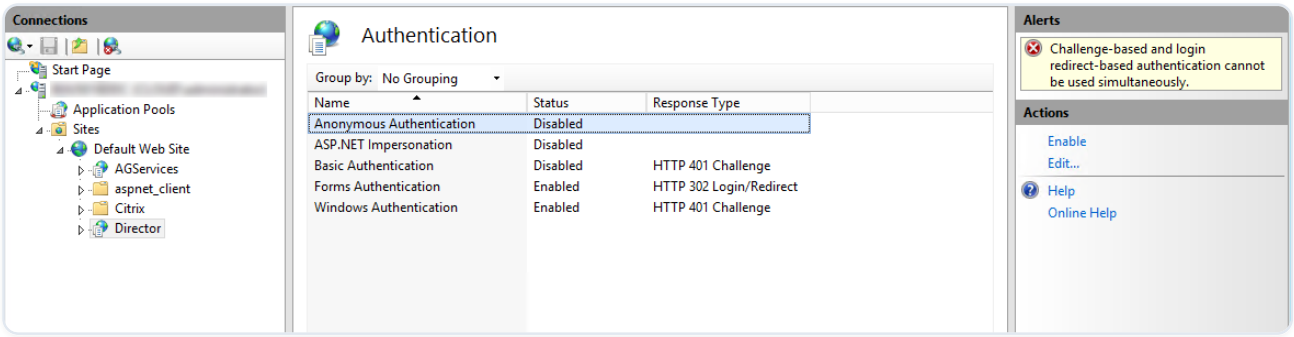
5. 認証後、Directorログオンページで追加の資格情報を入力することなく、Directorにアクセスできます。

統合 Windows 認証での Director の使用

統合Windows認証（IWA）を使用すると、ドメイン参加ユーザーはDirectorログオンページで資格情報を再入力することなく、Directorに直接アクセスできます。統合Windows認証とDirectorを使用するための前提条件は次のとおりです。

- DirectorをホストするIIS Webサイトで統合Windows認証を有効にします。Directorをインストールすると、匿名認証とフォーム認証が有効になります。統合Windows認証とDirectorをサポートするには、匿名認証を無効にし、Windows認証を有効にします。ドメイン以外のユーザーの認証には、フォーム認証を有効のままにしておく必要があります。

  a. IISマネージャーを起動します。
  b. **サイト** \> **既定のWebサイト** \> **Director**に移動します。
  c. **認証**を選択します。
  d. **匿名認証**を右クリックし、**無効**を選択します。
  e. **Windows認証**を右クリックし、**有効**を選択します。



- Directorマシンに対してActive Directoryの委任権限を構成します。構成が必要となるのは、DirectorとDelivery Controller™が別々のマシンにインストールされている場合のみです。

  a. Active Directoryマシンで、Active Directory管理コンソールを開きます。

  b. Active Directory管理コンソールで、**ドメイン名** \> **コンピューター** に移動します。Directorマシンを選択します。

  c. 右クリックして **プロパティ** を選択します。

  d. プロパティで、**委任** タブを選択します。

  e. オプション、**このコンピューターを任意のサービスへの委任のために信頼する (Kerberos のみ)** を選択します。

- Director へのアクセスに使用するブラウザーは、統合 Windows 認証をサポートしている必要があります。Firefox および Chrome では、追加の構成手順が必要になる場合があります。詳細については、ブラウザーのドキュメントを参照してください。
- 監視サービスは、Microsoft .NET Framework 4.5.1 以降の、Director のシステム要件に記載されているサポート対象バージョンを実行している必要があります。詳細については、システム要件を参照してください。

ユーザーが Director からログオフするか、セッションがタイムアウトすると、ログオンページが表示されます。ログオンページから、ユーザーは認証タイプを**自動ログオン**または**ユーザー資格情報**に設定できます。

インターフェイスビュー

Director は、特定の管理者向けに調整されたさまざまなインターフェイスビューを提供します。製品の権限によって、表示される内容と利用可能なコマンドが決まります。

たとえば、ヘルプデスク管理者は、ヘルプデスクタスクに合わせたインターフェイスを参照します。Director を使用すると、ヘルプデスク管理者は、問題を報告しているユーザーを検索し、そのユーザーに関連付けられたアクティビティを表示できます。たとえば、ユーザーのアプリケーションとプロセスのステータスなどです。応答しないアプリケーションやプロセスを終了する、ユー

ザーのマシンで操作をシャドウする、マシンを再起動する、ユーザープロファイルをリセットするなどのアクションを実行することで、問題を迅速に解決できます。

対照的に、完全な管理者はサイト全体を表示および管理し、複数のユーザーとマシンに対してコマンドを実行できます。ダッシュボードは、セッションのステータス、ユーザーログオン、サイトインフラストラクチャなど、展開の主要な側面を概観できます。情報は毎分更新されます。問題が発生した場合、発生した障害の数と種類に関する詳細が自動的に表示されます。

Director におけるさまざまな役割とその権限の詳細については、委任管理とDirectorを参照してください。

Pendoによる使用状況データの収集

Director のインストール後、Director Service は Pendo を使用して使用状況データの収集を開始します。トレンドページの使用状況に関する統計と OData API 呼び出し分析が収集されます。分析収集は、Citrix プライバシーポリシーに準拠しています。Director をインストールすると、データ収集はデフォルトで有効になります。

Pendo のデータ収集をオプトアウトするには、Director がインストールされているマシンでレジストリキーを編集します。レジストリキーが存在しない場合は、作成して目的の値に設定します。レジストリキーの値を変更した後、Director インスタンスを更新します。

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

場所: HKEY_LOCAL_MACHINE\Software\Citrix\Director

名前: DisableGoogleAnalytics

> **注:**
>
> 以前は、DirectorサービスはGoogle Analyticsを使用してデータを収集していました。同じレジストリキーがPendoでも使用されるようになりました。
>
> 値：0 = 有効（デフォルト）、1 = 無効

Pendoによるデータ収集を無効にするには、次のPowerShellコマンドレットを使用できます。

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

新機能ガイド

Directorには、Directorの現在のバージョンでリリースされた新機能に関する洞察を提供するPendoを使用する製品内ガイドがあります。概要と適切な製品内メッセージを組み合わせることで、製品の新機能を理解するのに役立ちます。

この機能をオプトアウトするには、Directorがインストールされているマシンで、以下に説明するようにレジストリキーを編集します。レジストリキーが存在しない場合は、作成して目的の値に設定します。レジストリキーの値を変更した後、Directorインスタンスを更新してください。

注意:

レジストリエディターを誤って使用すると、オペレーティングシステムの再インストールが必要になるような重大な問題を引き起こす可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターの使用は自己責任で行ってください。Citrixは、Windowsレジストリを変更する前にバックアップすることをお勧めします。

場所: HKEY_LOCAL_MACHINE\Software\Citrix\Director

名前: DisableGuidedHelp

値: 0 = 有効（デフォルト）、1 = 無効

製品内ガイドを無効にするには、次のPowerShellコマンドレットを使用できます。

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director
```

```
New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
-PropertyType DWORD -Value 1
```

参照記事

- Citrix DirectorからのMTTRの削減
- Citrix Director - PowerShell を使用してアラートと通知を管理および構成する
- Citrix Virtual Apps and Desktops 開発者向けドキュメント

関連製品の新機能

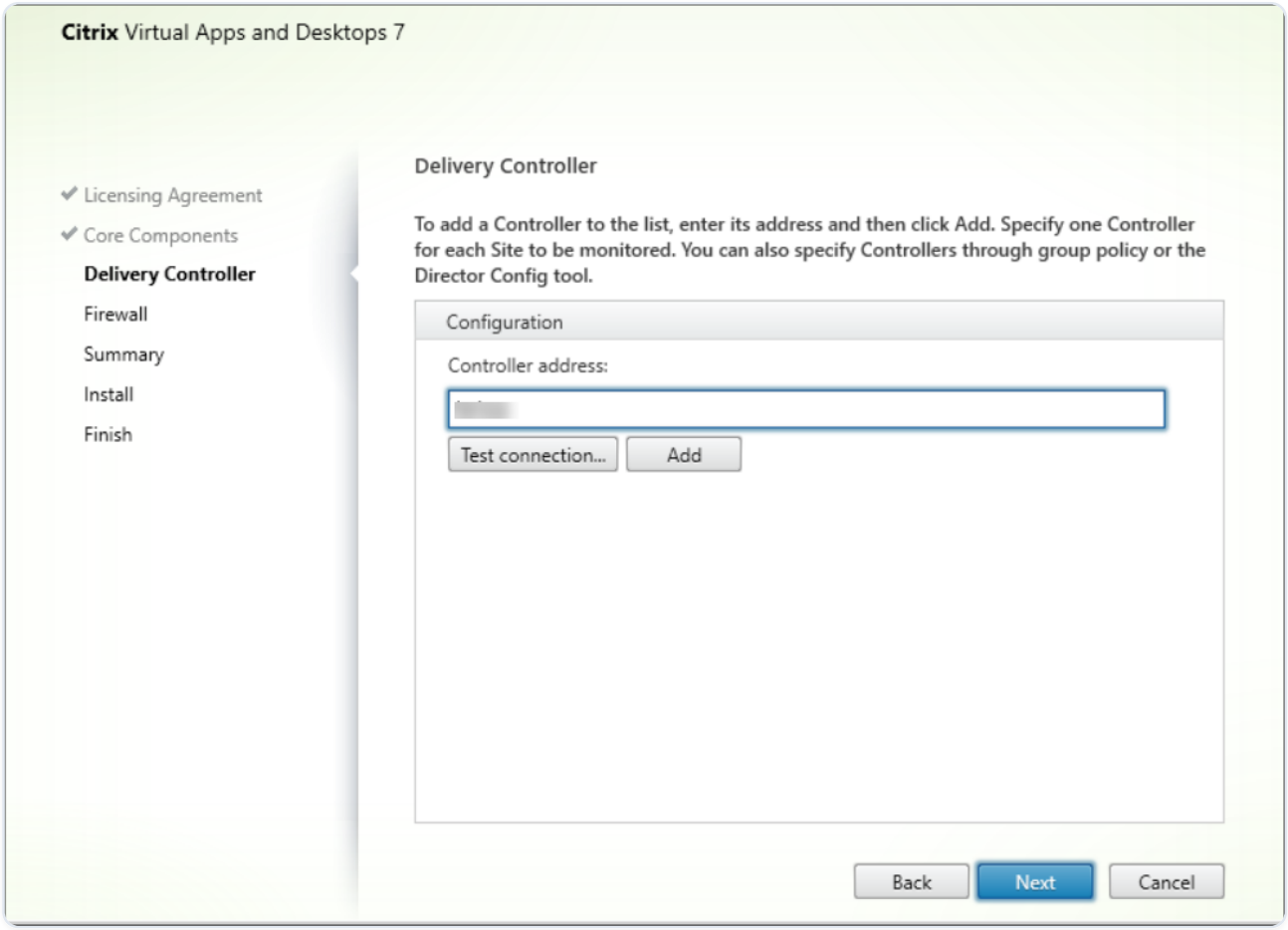
- シトリックス DaaS
- StoreFront
- セキュアプライベートアクセス
- シトリックス エンタープライズブラウザ
- シトリックス ワークスペース
- プロビジョニング

インストールと構成

Directorのインストール

Citrix Virtual Apps and Desktops 用のフル製品ISOインストーラーを使用してDirectorをインストールすると、前提条件の確認、不足しているコンポーネントのインストール、Director Webサイトのセットアップ、および基本的な構成が実行されます。前提条件およびその他の詳細については、このリリースのシステム要件ドキュメントを参照してください。このリリースのDirectorは、Virtual Apps 6.5以前の展開、またはVirtual Desktops 7以前の展開とは互換性がありません。 ISOインストーラーによって提供されるデフォルト構成は、一般的な展開に対応しています。インストール時にDirectorが含まれていなかった場合は、ISOインストーラーを使用してDirectorを追加します。追加のコンポーネントを追加するには、ISOインストーラーを再実行し、インストールするコンポーネントを選択します。ISOインストーラーの使用方法については、インストールドキュメントのコアコンポーネントのインストールを参照してください。Citrixでは、.MSIファイルではなく、フル製品ISOインストーラーのみを使用してインストールすることをお勧めします。

DirectorがControllerにインストールされている場合、サーバーアドレスとしてlocalhostが自動的に構成され、Directorはデフォルトでローカルcontrollerと通信します。Controllerから離れた専用サーバーにDirectorをインストールする場合は、ControllerのFQDNまたはIPアドレスを入力するよう求められます。



注:

追加をクリックして、監視するControllerを追加します。

Directorは、デフォルトで指定されたControllerと通信します。監視するサイトごとに、Controllerアドレスを1つだけ指定します。Directorは、同じサイト内の他のすべてのControllerを自動的に検出し、指定したControllerが失敗した場合は、それらの他のControllerにフォールバックします。

注:

> DirectorはController間で負荷分散を行いません。

> ブラウザーとWebサーバー間の通信を保護するために、Citrix®はDirectorをホストするIIS WebサイトでTLSを実装することを推奨します。手順については、Microsoft IISのドキュメントを参照してください。TLSを有効にするためにDirectorの構成は必要ありません。

Directorの展開と構成

Directorが複数のサイトを含む環境で使用される場合は、Controller、Director、およびその他のコアコンポーネントがインストールされているすべてのサーバーでシステムクロックを同期してください。そうしないと、Directorでサイトが正しく表示されない可能性があります。

> **重要:**
>
> ネットワーク経由でプレーンテキストを使用して送信されるユーザー名とパスワードのセキュリティを保護するため、Director接続にはHTTPではなくHTTPSのみを使用してください。特定のツールは、HTTP（暗号化されていない）ネットワークパケット内のプレーンテキストのユーザー名とパスワードを読み取ることができ、ユーザーにとって潜在的なセキュリティリスクを生じさせる可能性があります。

権限の構成

Directorにログオンするには、Directorの権限を持つ管理者はActive Directoryドメインユーザーであり、以下の権限を持っている必要があります。

- 検索対象となるすべてのActive Directoryフォレストにおける読み取り権限（高度な構成を参照）。
- 構成済みの委任管理者ロール（委任管理とDirectorを参照）。
- ユーザーをシャドウするには、管理者はWindowsリモートアシスタンス用のMicrosoftグループポリシーを使用して構成されている必要があります。さらに：
  - VDAをインストールする際は、すべてのユーザーデバイスでWindowsリモートアシスタンス機能が有効になっていることを確認してください（デフォルトで選択されています）。
  - Directorをサーバーにインストールする際は、Windowsリモートアシスタンスがインストールされていることを確認してください（デフォルトで選択されています）。ただし、サーバーではデフォルトで無効になっています。Directorがエンドユーザーにアシスタンスを提

供するために、この機能を有効にする必要はありません。Citrixは、サーバーのセキュリティを向上させるために、この機能を無効のままにしておくことを推奨します。

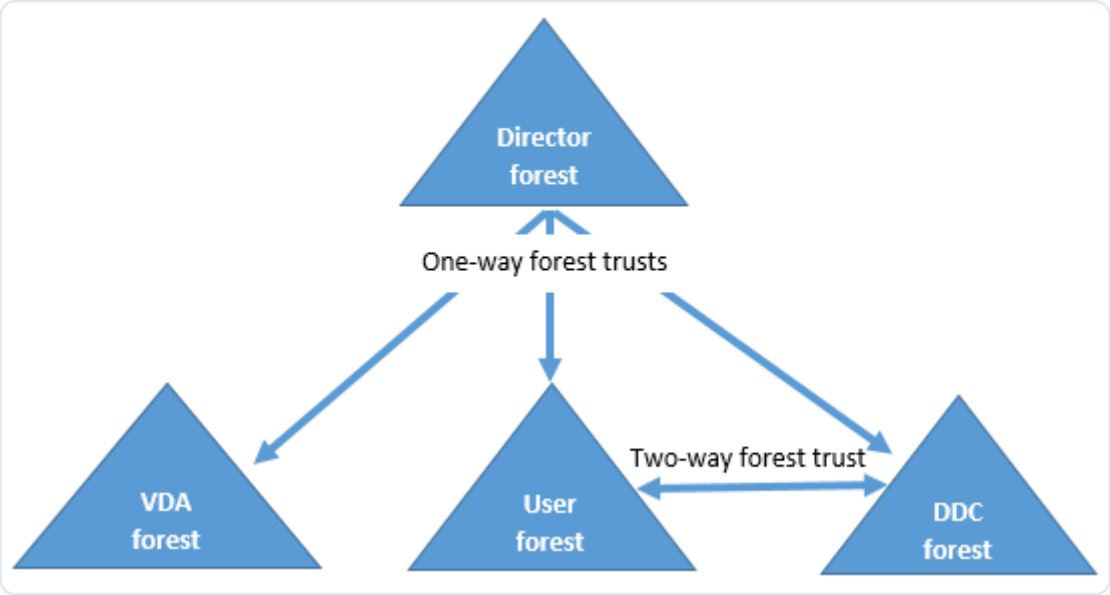
- 管理者がWindowsリモートアシスタンスを開始できるようにするには、リモートアシスタンス用の適切なMicrosoftグループポリシー設定を使用して、必要な権限を付与します。詳細については、CTX127388: How to Enable Remote Assistance for Desktop Directorを参照してください。

高度な構成

Director は、ユーザー、Delivery Controller (DC)、VDA、および Director が異なるフォレストに配置されているフォレスト構成にまたがるマルチフォレスト環境をサポートできます。これには、フォレスト間の信頼関係と構成設定の適切なセットアップが必要です。

マルチフォレスト環境での推奨構成

推奨される構成では、ドメイン全体の認証を持つフォレスト間で、送信および受信フォレスト信頼関係の作成が必要です。



Director からの信頼関係により、異なるフォレストにあるユーザーセッション、VDA、および Delivery Controller の問題をトラブルシューティングできます。

Directorが複数のフォレストをサポートするために必要な高度な構成は、Internet Information Services (IIS) マネージャーで定義された設定によって制御されます。

重要:

> IIS で設定を変更すると、Director サービスは自動的に再起動し、ユーザーをログオフします。

> IISを使用して高度な設定を構成するには：

1. Internet Information Services (IIS) マネージャーコンソールを開きます。
2. デフォルトWebサイトの下にあるDirector Webサイトに移動します。
3. **アプリケーション設定**をダブルクリックします。
4. 設定をダブルクリックして編集します。
5. 新しい設定を追加するには、**追加**をクリックします。

Director は Active Directory を使用してユーザーを検索し、より多くのユーザーおよびマシン情報を参照します。デフォルトでは、Director は次のドメインまたはフォレストを検索します。

- 管理者アカウントがメンバーです。
- Director Webサーバーがメンバーです（異なる場合）。

Director は Active Directory グローバルカタログを使用してフォレストレベルで検索を実行しようとします。フォレストレベルで検索する権限がない場合、ドメインのみが検索されます。

別の Active Directory ドメインまたはフォレストからデータを検索または参照するには、検索するドメインまたはフォレストを明示的に設定する必要があります。IIS マネージャーで Director Web サイトに次のアプリケーション設定を構成します。

```
Connector.ActiveDirectory.Domains = (user),(server)
```

値属性のuserとserverは、それぞれDirectorユーザー（管理者）とDirectorサーバーのドメインを表します。

追加のドメインまたはフォレストからの検索を有効にするには、この例に示すように、ドメイン名をリストに追加します。

```
Connector.ActiveDirectory.Domains = (user),(server),\&lt;domain1\>,
\&lt;domain2\>
```

リスト内の各ドメインについて、Director はフォレストレベルで検索を実行しようとします。フォレストレベルで検索する権限がない場合、ドメインのみが検索されます。

ドメインローカルグループの構成

ほとんどの Citrix Service Providers (CSP) は、インフラストラクチャフォレスト内の VDA、DC、および Director で構成される同様の環境設定を持っています。ユーザーまたはユーザーグループのレコードは顧客フォレストに属します。インフラストラクチャフォレストから顧客フォレストへの一方向の送信信頼が存在します。

CSP管理者は通常、インフラストラクチャフォレストにドメインローカルグループを作成し、カスタマーフォレストのユーザーまたはユーザーグループをこのドメインローカルグループに追加します。

推奨されるマルチフォレストサイト構成(/en-us/citrix-virtual-apps-desktops/2411/media/domainlocalgroup-config.png)

Directorはこのようなマルチフォレスト設定をサポートし、ドメインローカルグループを使用して構成されたユーザーのセッションを監視できます。

1. IIS マネージャーで Director Web サイトに次のアプリケーション設定を追加します。

   ```
   Connector.ActiveDirectory.DomainLocalGroupSearch= true



   DomainLocalGroupSearchDomains= \&lt;domain1\>,\&lt;domain2\>
   ```

   \<domain1\>\<domain2\> は、ドメインローカルグループが存在するフォレストの名前です。
2. Web Studioでドメインローカルグループをデリバリーグループに割り当てます。
3. IISを再起動し、変更を有効にするためにDirectorに再度ログオンします。これで、Directorはこれらのユーザーのセッションを監視し、表示できるようになります。

Directorにサイトを追加する

Directorがすでにインストールされている場合は、複数のサイトで動作するように構成します。構成するには、各DirectorサーバーでIISマネージャーコンソールを使用して、アプリケーション設定のサーバーアドレスリストを更新します。

各サイトのControllerのアドレスを次の設定に追加します。

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
```

SiteAControllerとSiteBControllerは、2つの異なるサイトのDelivery Controllerのアドレスです。

アクティビティマネージャーで実行中のアプリケーションの可視性を無効にする

デフォルトでは、Directorのアクティビティマネージャーは、ユーザーセッションのすべての実行中のアプリケーションのリストを表示します。この情報は、Directorのアクティビティマネージャー機能にアクセスできるすべての管理者が表示できます。委任された管理者ロールの場合、これにはフル管理者、デリバリーグループ管理者、およびヘルプデスク管理者が含まれます。

ユーザーのプライバシーと実行中のアプリケーションを保護するために、実行中のアプリケーションを一覧表示する**アプリケーション**タブを無効にすることができます。

警告:

レジストリを誤って編集すると、オペレーティングシステムを再インストールする必要があるような深刻な問題が発生する可能性があります。Citrix® は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証しません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

1. VDAで、HKEY_LOCAL_MACHINE\\Software\\Citrix\\Director\\TaskManagerDataDisplayedにあるレジストリキーを変更します。デフォルトでは、このキーは1に設定されています。値を0に変更すると、VDAから情報が収集されなくなり、アクティビティマネージャーに表示されなくなります。
2. Directorがインストールされているサーバーで、実行中のアプリケーションの表示を制御する設定を変更します。デフォルトでは、値は「true」であり、アプリケーションタブで実行中のアプリケーションの表示が許可されます。値を「false」に変更すると、表示が無効になります。このオプションは、VDAではなく、Directorのアクティビティマネージャーのみに影響します。 次の設定の値を変更します。 UI.TaskManager.EnableApplications = false

重要:

実行中のアプリケーションの表示を無効にするには、アクティビティマネージャーにデータが表示されないように、両方の変更を行います。

PIV スマートカード認証を構成する

この記事では、スマートカード認証機能を有効にするためにDirectorサーバーおよびActive Directoryで必要な構成について説明します。

> **注記：**
>
> スマートカード認証は、同じActive Directoryドメインのユーザーのみがサポートされます。

Directorサーバーの構成

Directorサーバーで以下の構成手順を実行します。

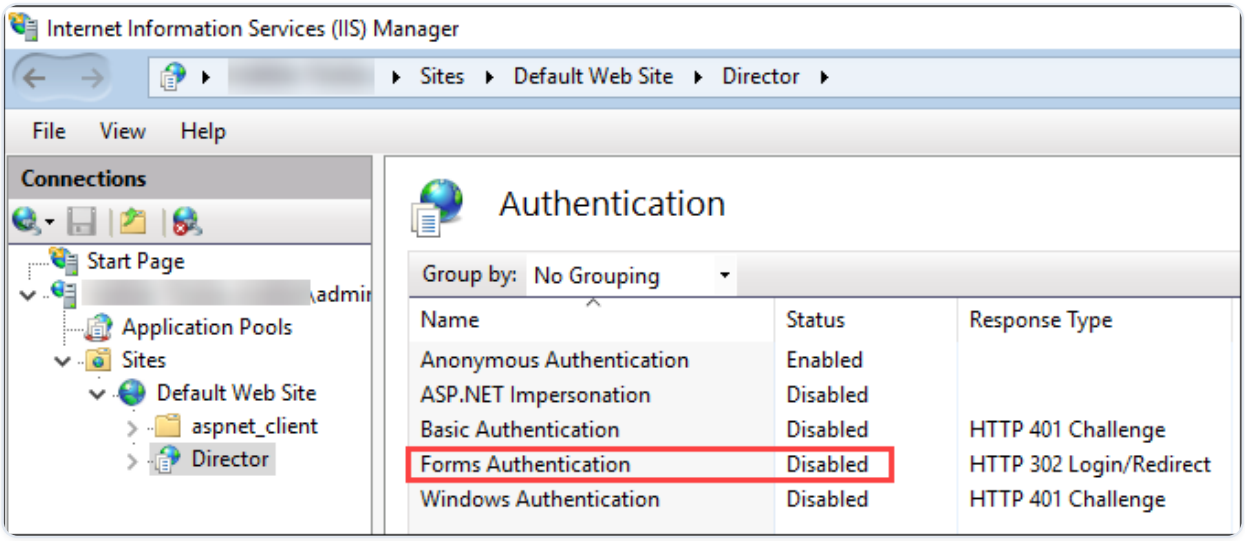
1. クライアント証明書マッピング認証をインストールして有効にします。Microsoftドキュメントのクライアント証明書マッピング認証に記載されている**Active Directoryを使用したクライアント証明書マッピング認証**の手順に従います。
2. Directorサイトでフォーム認証を無効にします。

   IISマネージャーを起動します。

   サイト \> **Default Web Site** \> **Director**に移動します。

   認証を選択します。

   フォーム認証を右クリックして、**無効**を選択します。



3. クライアント証明書認証のために、DirectorのURLをより安全なhttpsプロトコル（HTTPの代わりに）を使用するように構成します。

   a. IISマネージャーを起動します。

b. **サイト** \> **既定のWebサイト** \> **Director** に移動します。

c. 「**SSL Settings**」を選択します。

d. 「**SSLを必須にする**」と「**クライアント証明書**」\>「**必須**」を選択します。

SSL設定(/en-us/citrix-virtual-apps-desktops/2411/media/dir-smartcard-config2.png)

4. web.configを更新します。テキストエディターを使用して、web.configファイル（c:\\inetpub\\wwwroot\\Directorにあります）を開きます。

`<system.webServer>` 親要素の下に、次のスニペットを最初の子要素として追加します。

```
&lt;defaultDocument>

   &lt;files>

       &lt;add value="LogOn.aspx"/>

   &lt;/files>

&lt;/defaultDocument>
```

Active Directory の構成

デフォルトでは、Directorアプリケーションは**アプリケーションプール**のIDプロパティで実行されます。スマートカード認証には委任が必要であり、そのためにはDirectorアプリケーションIDがサービスホスト上でTrusted Computing Base (TCB)権限を持っている必要があります。

Citrixは、アプリケーションプールID用に個別のサービスアカウントを作成することを推奨します。Microsoft MSDNの記事「Protocol Transition with Constrained Delegation Technical Supplement」の指示に従って、サービスアカウントを作成し、TCB権限を割り当ててください。

新しく作成したサービスアカウントを Director アプリケーションプールに割り当てます。次の図は、サンプルサービスアカウント「Domain Pool」のプロパティダイアログを示しています。

サンプルサービスアカウント(/en-us/citrix-virtual-apps-desktops/2411/media/dir-smartcard-config3.png)

このアカウントに対して、次のサービスを構成します:

- Delivery Controller™: ホストサーバー、HTTP
- Director: ホスト、HTTP
- アクティブディレクトリ: GC、LDAP

構成するには、,

1. 「ユーザーアカウントのプロパティ」ダイアログで、「**追加**」をクリックします。
2. **サービスの追加**ダイアログで、またはをクリックします。
3. Delivery Controllerのホスト名を選択します。
4. 「**利用可能なサービス**」リストから、HOSTとHTTPの「**サービスの種類**」を選択します。

サービスを構成する(/en-us/citrix-virtual-apps-desktops/2411/media/dir-smartcard-config4.png)

同様に、**Director**および**Active Directory**ホストのサービスの種類を追加します。

サービスプリンシパル名レコードを作成する

各Directorサーバーと、Directorサーバーのプールにアクセスするために使用される負荷分散された仮想IP (VIP) ごとにサービスアカウントを作成する必要があります。新しく作成されたサービスアカウントへの委任を構成するには、サービスプリンシパル名 (SPN) レコードを作成する必要があります。

- DirectorサーバーのSPNレコードを作成するには、次のコマンドを使用します。

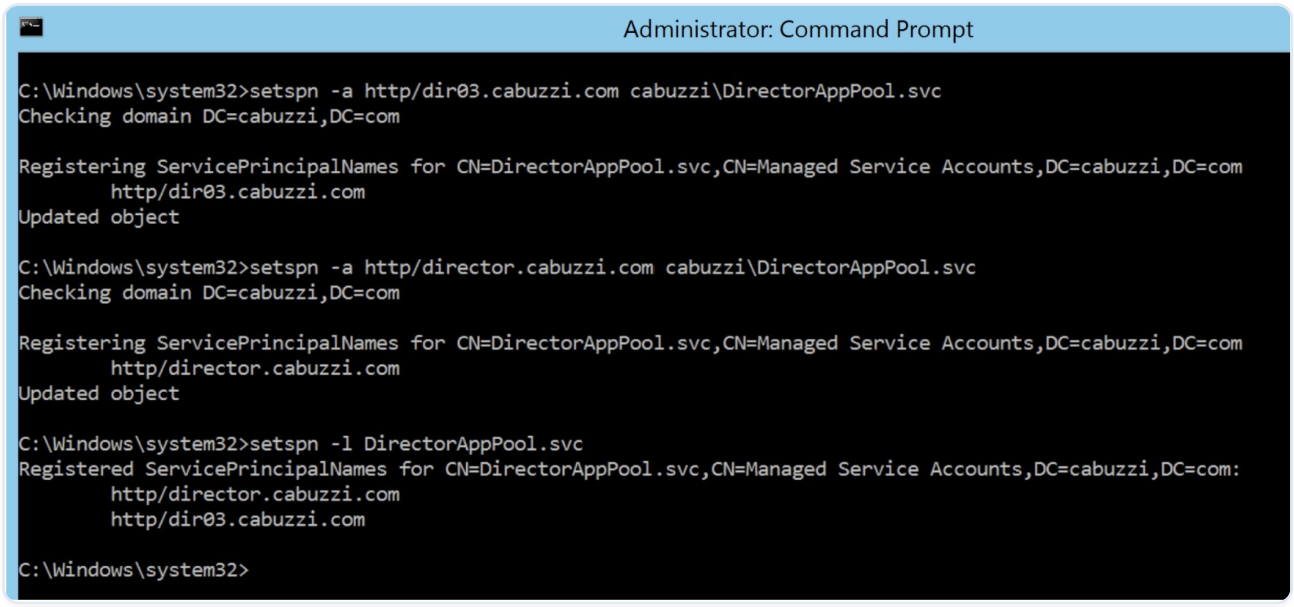
```
  setspn -a http/<directorServer>.<domain_fqdn>
<domain>\<DirectorAppPoolServiceAcct>
```

- 負荷分散されたVIPのSPNレコードを作成するには、次のコマンドを使用します。

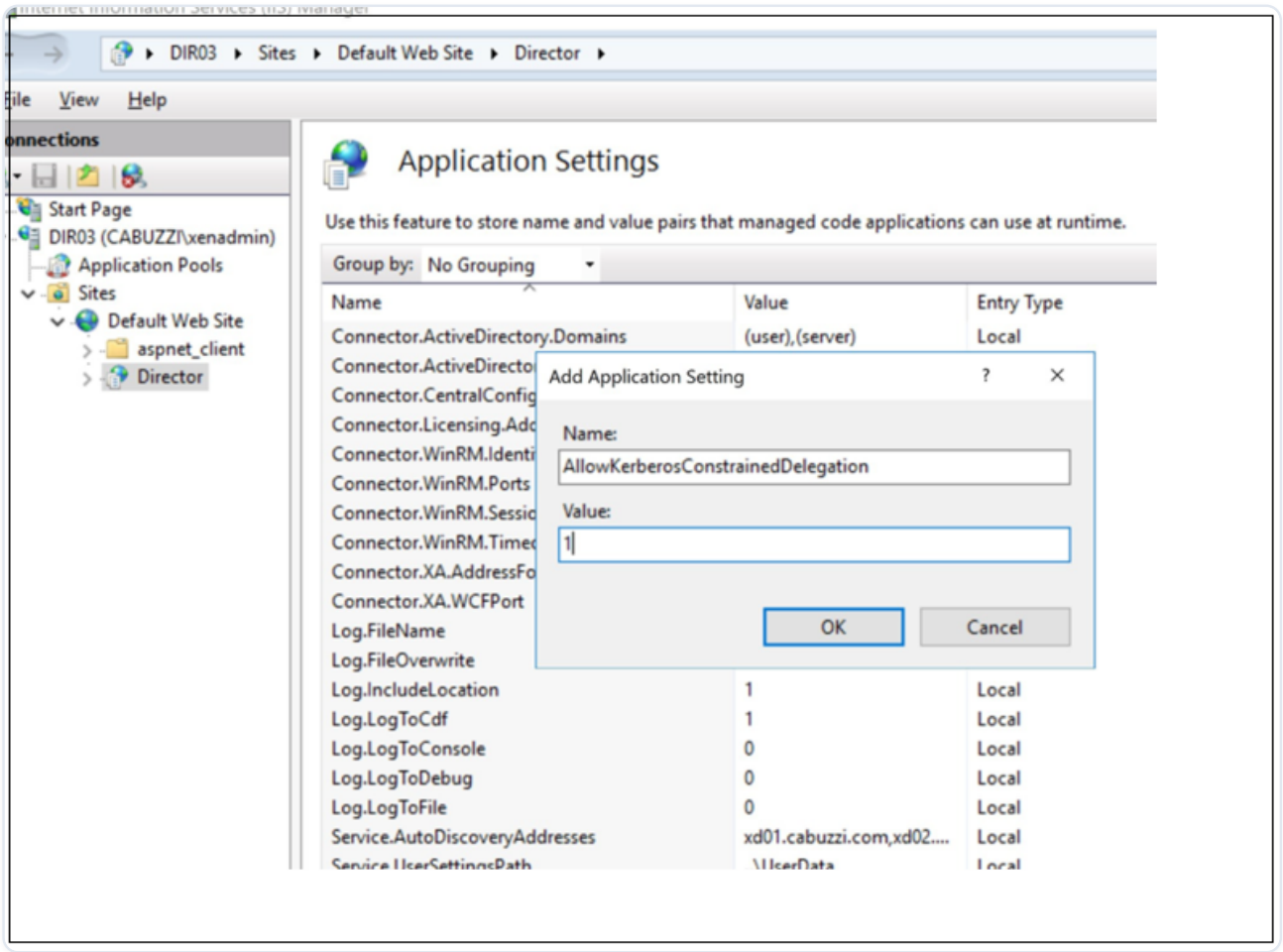
```
  setspn -S http/<DirectorFQDN> <domain>\<DirectorAppPoolServiceAcct>
```

- 作成されたSPNを表示またはテストするには、次のコマンドを使用します。

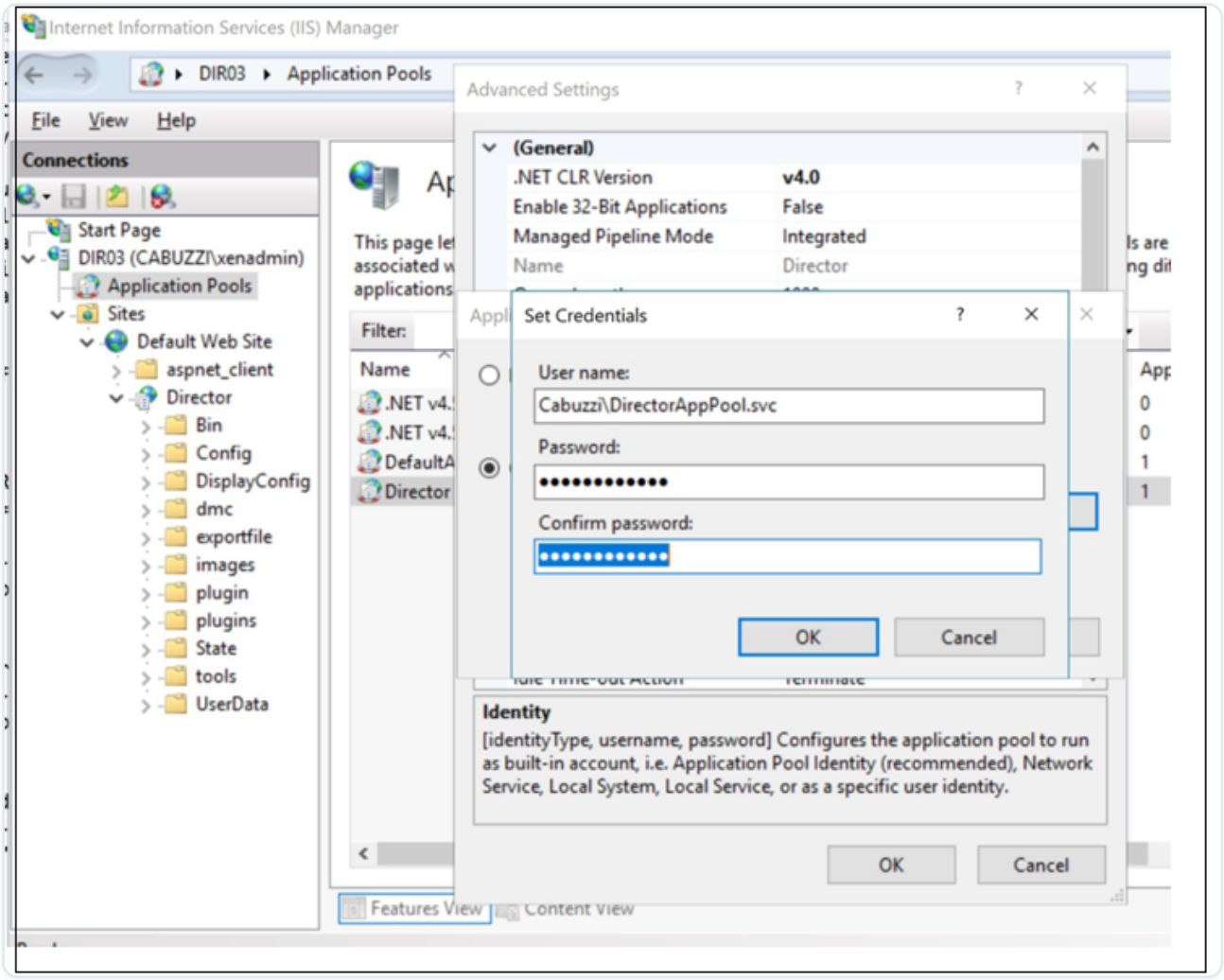
```
 setspn –l <DirectorAppPoolServiceAcct>
```



- 左ペインでDirector仮想ディレクトリを選択し、 をダブルクリックします。 ウィンドウで をクリックし、**AllowKerberosConstrainedDelegation** が1に設定されていることを確認します。



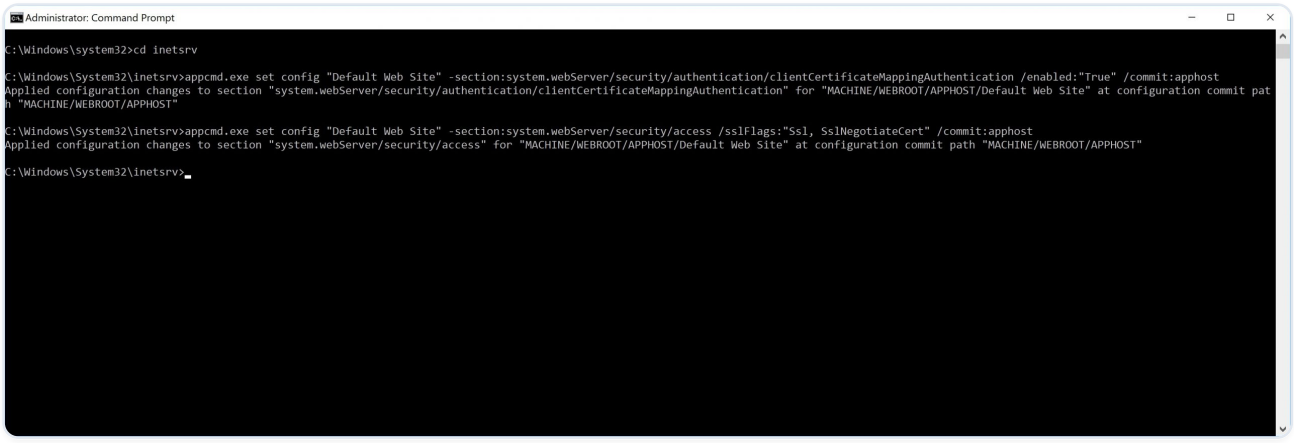
- 左側のペインで を選択し、Directorアプリケーションプールを右クリックして を選択します。
- 「**ID**」を選択し、省略記号（「…」）をクリックして、サービスアカウントのドメイン\ログオンとパスワードの資格情報を入力します。IISコンソールを閉じます。



- 管理者として実行したコマンドプロンプトから、ディレクトリを C:\Windows\System32\inetsrv に変更し、次のコマンドを入力します。

```
   appcmd.exe set config “Default Web Site” -section:system.webServer/
security/authentication/clientCertificateMappingAuthentication /
enabled:”True” /commit:apphost
```

```
    appcmd.exe set config “Default Web Site” -section:system.webServer/
security/access /sslFlags:”Ssl, SslNegotiateCert” /commit:apphost
```



Firefoxブラウザの設定

Firefoxブラウザを使用するには、OpenSC 0.17.0で入手可能なPIVドライバーをインストールします。インストールと構成の手順については、Installing OpenSC PKCS#11 Module in Firefox, Step by Stepを参照してください。 Directorでのスマートカード認証機能の使用方法については、Directorの記事の「Use Director with PIV based smart card authentication」セクションを参照してください。

ネットワーク分析を構成する

> **注：** この機能の利用可否は、組織のライセンスと管理者権限によって異なります。

> DirectorはCitrix ADMと統合され、ネットワーク分析とパフォーマンス管理を提供します。

- ネットワーク分析は、Citrix ADMからのHDX™ Insightレポートを使用して、ネットワークのアプリケーションおよびデスクトップのコンテキストビューを提供します。この機能により、Directorは展開環境におけるICAトラフィックの高度な分析を提供します。
- パフォーマンス管理は、履歴保持と傾向レポートを提供します。リアルタイム評価と比較してデータの履歴保持を行うことで、容量や健全性の傾向を含むトレンドレポートを作成できます。

Directorでこの機能を有効にすると、HDX InsightレポートはDirectorに追加情報を提供します。

- ページの タブには、展開環境全体におけるアプリケーション、デスクトップ、およびユーザーの遅延と帯域幅の影響が表示されます。
- ページには、特定のユーザーセッションに固有の遅延と帯域幅の情報が表示されます。

制限事項:

- ビューでは、バージョン7より前のVDAのHDX接続ログオンデータは収集されません。それ以前のVDAの場合、グラフデータは0と表示されます。

ネットワーク分析を有効にするには、DirectorにCitrix ADMをインストールして構成する必要があります。Directorには、Citrix ADMバージョン11.1ビルド49.16以降が必要です。MASはXenServer上で動作する仮想アプライアンスです。ネットワーク分析を使用すると、Directorは展開環境に関連する情報を通信し、収集します。

詳しくは、Citrix ADM ドキュメントを参照してください。

注:

Citrix NetScaler Insight Centerは、15 May 2018をもってメンテナンス終了日を迎えました。Citrix Product Matrix を参照してください。ネットワーク分析のためにDirectorをCitrix ADMと統合してください。NetScaler Insight CenterをCitrix ADMに移行するには、NetScaler Insight CenterからCitrix ADMへの移行 を参照してください。

1. Directorがインストールされているサーバーで、C:\\inetpub\\wwwroot\\Director\\toolsにあるDirectorConfigコマンドラインツールを見つけ、コマンドプロンプトからパラメーター /confignetscaler を指定して実行します。
2. プロンプトが表示されたら、Citrix ADMマシン名（FQDNまたはIPアドレス）、ユーザー名、パスワード、HTTPS接続タイプ（HTTPよりも推奨）、およびCitrix ADM統合を選択します。
3. 変更を確認するには、ログオフして再度ログオンします。

注:

セキュリティ上の理由から、DirectorとのADM統合のために、HDX Insightへのアクセスのみに十分な権限を持つカスタムロールを作成することをお勧めします。

詳細については、アクセスポリシーの構成を参照してください。

委任管理とDirector

委任管理では、管理者、役割、スコープという3つの概念を使用します。権限は、管理者の役割とその役割のスコープに基づいています。たとえば、管理者はヘルプデスク管理者役割を割り当てられ、そのスコープは1つのサイトのエンドユーザーに対する責任のみを含む場合があります。

委任管理者の作成については、メインの委任管理の記事を参照してください。

管理権限は、管理者に表示されるDirectorインターフェイスと、管理者が実行できるタスクを決定します。権限によって以下が決定されます。

- 管理者がアクセスできるビュー（総称してビューと呼ばれる）。
- 管理者が表示および操作できるデスクトップ、マシン、およびセッション。
- ユーザーセッションのシャドウイングやメンテナンスモードの有効化など、管理者が実行できるコマンド。

組み込みの役割と権限は、管理者がDirectorを使用する方法も決定します。

管理者役割	DIRECTORでの権限
フル管理者	すべてのビューへのフルアクセス権を持ち、ユーザーセッションのシャドウイング、メンテナンスモードの有効化、トレンドデータのエクスポートを含むすべてのコマンドを実行できます。
デリバリーグループ管理者	すべてのビューへのフルアクセス権を持ち、ユーザーセッションのシャドウイング、電源管理とセッション管理、メンテナンスモードの有効化、トレンドデータのエクスポートを含むすべてのコマンドを実行できます。
読み取り専用管理者	すべてのビューにアクセスし、指定されたスコープ内のすべてのオブジェクトとグローバル情報を表示できます。HDX™チャネルからレポートをダウンロードし、トレンドビューの「エクスポート」オプションを使用してトレンドデータをエクスポートできます。その他のコマンドを実行したり、ビュー内の何かを変更したりすることはできません。
ヘルプデスク管理者	ヘルプデスクビューとユーザー詳細ビューのみにアクセスでき、管理者が管理を委任されて

管理者役割	DIRECTORでの権限
	いるオブジェクトのみを表示できます。ユーザーのセッションをシャドウし、そのユーザーに対してコマンドを実行できます。メンテナンスモード操作を実行できます。シングルセッションOSマシンに対して電源制御オプションを使用できます。ダッシュボード、トレンド、アラート、またはフィルタービューにはアクセスできません。マルチセッションOSマシンに対して電源制御オプションを使用することはできません。
マシンカタログ管理者	マシンの詳細ページ（マシンベースの検索）のみにアクセスできます。
ホスト管理者	アクセスできません。この管理者はDirectorではサポートされておらず、データを表示できません。

Director管理者用のカスタム役割を構成する

Studioでは、組織の要件により厳密に一致させ、権限をより柔軟に委任するために、Director固有のカスタム役割を構成することもできます。たとえば、組み込みのヘルプデスク管理者役割を制限して、この管理者がセッションをログオフできないようにすることができます。

Director権限を持つカスタム役割を作成する場合、その役割に他の一般的な権限も付与する必要があります。

- DirectorにログオンするためのDelivery Controller™権限 - 管理者ノードで少なくとも読み取り専用アクセス
- Directorで配信グループに関連するデータを表示するための配信グループへの権限 - 少なくとも読み取り専用アクセス

カスタムロール(/en-us/citrix-virtual-apps-desktops/2411/media/dir_custom_role.png)

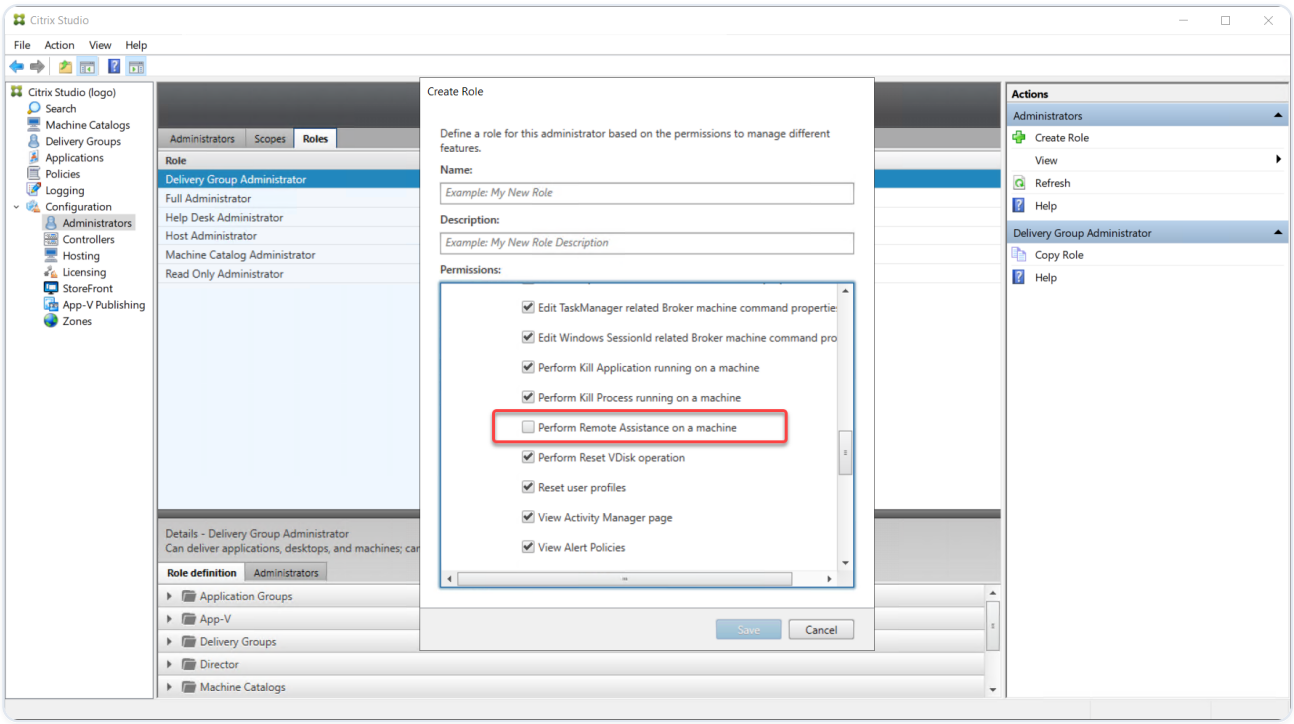
または、既存のロールをコピーして、異なるビューに対する追加の権限を含めることで、カスタムロールを作成できます。たとえば、ヘルプデスクロールをコピーして、ダッシュボードまたはフィルターページを表示する権限を含めることができます。

カスタムロールのDirector権限を選択します。これには以下が含まれます。

- マシン上で実行中のアプリケーションの強制終了を実行する

- マシン上で実行中のプロセスの強制終了を実行する
- マシン上でリモートアシスタンスを実行する
- ユーザープロファイルをリセットする
- クライアント詳細ページを表示
- ダッシュボードページの表示
- フィルターページを表示する
- マシン詳細ページを表示
- トレンドページの表示
- ユーザー詳細ページを表示

この例では、シャドウイング（マシン上でリモートアシスタンスを実行する）が無効になっています。



権限は、UIで適用可能になるために他の権限に依存する場合があります。たとえば、**マシン上で実行中のアプリケーションの強制終了を実行する**権限を選択すると、ロールに権限があるパネルでのみ**アプリケーションの終了**機能が有効になります。次のパネル権限を選択できます。

- フィルターページを表示する
- ユーザー詳細ページを表示する
- マシンの詳細ページを表示
- クライアントの詳細ページを表示

さらに、他のコンポーネントの権限リストから、デリバリーグループの以下の権限を検討してください。

- デリバリーグループのメンバーシップを使用して、マシンのメンテナンスモードを有効/無効にする。
- デリバリーグループのメンバーシップを使用して、Windowsデスクトップマシンで電源操作を実行する。
- デリバリーグループのメンバーシップを使用して、マシンでセッション管理を実行する。

Directorの展開を保護する

この記事では、Directorの展開と構成時にシステムセキュリティに影響を与える可能性のある領域について説明します。

Directorの通信

実稼働環境では、Directorとサーバー間でやり取りされるデータを保護するためにHTTPSプロトコルを使用します。HTTPSは、Transport Layer Security (TLS) プロトコルを使用して、強力なデータ暗号化を提供します。

> **注:**
>
> - Citrix®は、イントラネットネットワーク内でのDirectorコンソールへのアクセスを制限することを強くお勧めします。
> - Citrixは、実稼働環境でDirectorへの保護されていない接続を有効にしないことを強くお勧めします。
> - TLS 1.2以降を使用してください。レガシーTLSまたはSSLは使用しないでください。

> ユーザーのWebブラウザーとDirector間の通信を保護するには、「Web StudioおよびDirectorでTLSを有効にする」を参照してください。

DirectorとCitrix Virtual Apps and Desktopsサーバー間の通信（監視およびレポート用）を保護するには、「オンプレミスMonitor OData APIアクセスを保護する」を参照してください。

DirectorとCitrix ADC間の通信（Citrix Insight用）を保護するには、「ネットワーク分析を構成する」ときに、接続の種類としてHTTPSを選択します。

Microsoft インターネット インフォメーション サービス (IIS) の構成

制限されたIIS構成でDirectorを構成できます。

アプリケーションプールのリサイクル制限

Directorは、**Director**という名前のアプリケーションプールを使用します。アプリケーションプールで次のアプリケーションプールのリサイクル制限を設定できます。

- 仮想メモリ制限: 4,294,967,295
- プライベートメモリ制限: StoreFront™サーバーの物理メモリのサイズ
- リクエスト制限: 4,000,000,000

ファイル名拡張子

インストール中に、Directorは以下の拡張子のみを許可するようにリクエストフィルタリングを構成します。

- .
- .エーエスピーエックス
- .シーエスエス
- .イーオーティー
- .エイチティーエムエル
- .アイシーオー
- .js
- .ピーエヌジー
- .エスブイシー
- .エスブイジー
- .ジフ
- .ジェイソン
- .ウォフ
- .ウォフ2
- .ティーティーエフ

HTTP動詞

インストール中、Directorは以下の動詞のみを許可するようにリクエストフィルタリングを構成します。

- GET
- POST
- HEAD

IIS機能

Directorは以下のIISコンポーネントを必要としません。

- ISAPI拡張機能
- CGIプログラム
- FastCGIプログラム

これらのコンポーネントは削除できます。

.NET信頼レベル

Director では、**.NET 信頼レベル**を**完全信頼**に設定する必要があります。.NET 信頼レベルを他の値に設定しないでください。

ユーザー権限の構成

Directorがインストールされると、そのアプリケーションプールには次の権限が付与されます。

- 「**サービスとしてログオン**」ログオン権限
- 「**プロセスのメモリクォータの調整**」、「**セキュリティ監査の生成**」、「**プロセスレベルトークンの置き換え**」の各特権

言及されている権限と特権は、アプリケーションプールが作成される際の通常のインストール動作です。

これらのユーザー権限を変更する必要はありません。これらの特権は Director では使用されず、自動的に無効になります。

Director のセキュリティ分離

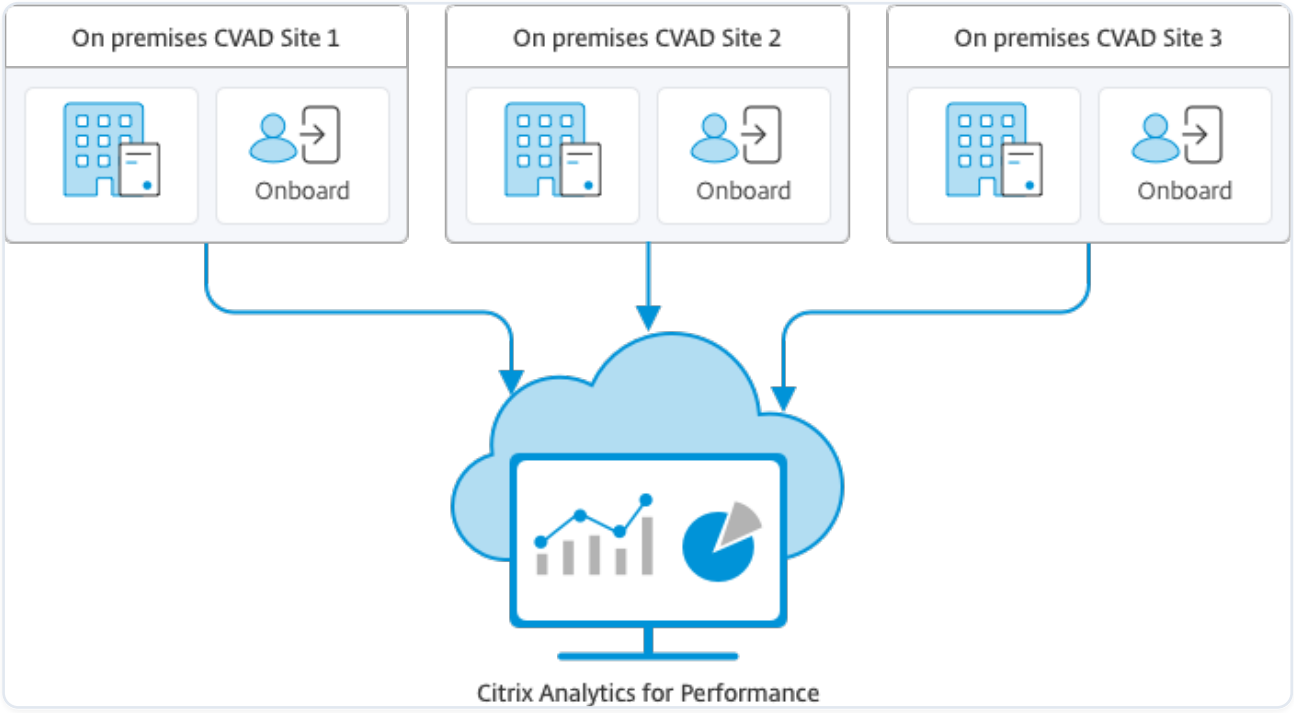
Directorと同じWebドメイン（ドメイン名とポート）に任意のWebアプリケーションを展開できます。ただし、それらのWebアプリケーションにセキュリティリスクがあると、Director展開のセキュリティが低下する可能性があります。より高度なセキュリティ分離が必要な場合は、Directorを別のWebドメインに展開することをCitrixは推奨します。

Citrix Analytics for Performance™ を使用したオンプレミスサイトの構成

Citrix Analytics for Performance (Performance Analytics) は、Citrix Analytics Cloud Service が提供する包括的なパフォーマンス監視ソリューションです。Performance Analytics は、パフォーマンスメトリックに基づいて構築された高度なインサイトと分析を提供します。Performance Analytics を使用すると、組織内の 1 つ以上の Citrix Virtual Apps and Desktops™ サイトの使用状況とパフォーマンスメトリックを監視および表示できます。

Performance Analytics の詳細については、Performance Analytics の記事を参照してください。

サイトから Citrix Cloud™ 上の Citrix Analytics for Performance にパフォーマンスデータを送信して、その高度なパフォーマンス分析機能を活用できます。Performance Analytics を表示および使用するには、まず **Director** の **Analytics** タブから Citrix Analytics for Performance を使用してオンプレミスサイトを構成する必要があります。



Performance Analytics は安全な方法でデータにアクセスし、Citrix Cloud からオンプレミス環境にデータが転送されることはありません。

前提条件

Director から Citrix Analytics for Performance を構成するために、新しいコンポーネントをインストールする必要はありません。次の要件が満たされていることを確認してください。

- Delivery Controller と Director のバージョンが 1912 CU2 以降であること。詳細については、「機能互換性マトリックス」を参照してください。

> **注:**

- Delivery Controller が Microsoft .NET Framework バージョン 4.8 より前のバージョンを実行している場合、Director から Citrix Analytics for Performance を使用してオンプレミスサイトを構成すると失敗する可能性があります。回避策として、Delivery Controller の .NET Framework をバージョン 4.8 にアップグレードしてください。LCM-9255。
- Citrix Virtual Apps and Desktops バージョン 2012 を実行しているオンプレミスサイトを Director から Citrix Analytics for Performance で構成すると、数時間後または Delivery Controller の Citrix Monitor Service の再起動後に構成が失敗する場合があります。この場合、Analytics タブには「未接続」ステータスが表示されます。回避策として、Delivery Controller のレジストリに Encryption フォルダーを作成します。場所: HKEY_LOCAL_MACHINE\Software\Citrix\XDservices\Monitor、フォルダー名: Encryption。CitrixMonitor アカウントが Encryption フォルダーに対してフルコントロールアクセス権を持っていることを確認します。Citrix Monitor Service を再起動します。DIR-14324。

- この構成を実行するための **Analytics** タブへのアクセスは、フル管理者のみが利用できます。
- Performance Analytics がパフォーマンスメトリックにアクセスできるようにするには、すべての Delivery Controller および Director がインストールされているマシンでアウトバウンドインターネットアクセスが利用可能である必要があります。具体的には、次の URL へのアクセスが可能であることを確認してください。
  - Citrix キー登録: `https://*.citrixnetworkapi.net/`
  - シトリックス クラウド: `https://*.citrixworkspacesapi.net/`
  - シトリックス アナリティクス: `https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/` Delivery ControllerとDirectorマシンがイントラネット内にあり、アウトバウンドインターネットアクセスがプロキシサーバー経由である場合、以下を確認してください。
- プロキシサーバーは、上記のURLリストを許可する必要があります。
- Directorのweb.configファイルとcitrix.monitor.exe.configファイルに以下の構成を追加します。この構成は**configuration**タグ内に必ず追加してください。

```
&lt;system.net>

    &lt;defaultProxy>
```

```
        &lt;proxy  usesystemdefault = "false"  proxyaddress = "http://
&lt;your_proxyserver_address>:80" bypassonlocal = "true"  />

    &lt;/defaultProxy>

&lt;/system.net>
```

- Director web.config は、Director がインストールされているマシンの `C:\inetpub\wwwroot\Director\web.config` にあります。
- citrix.monitor.exe.config は、Delivery Controller がインストールされているマシンの `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` にあります。

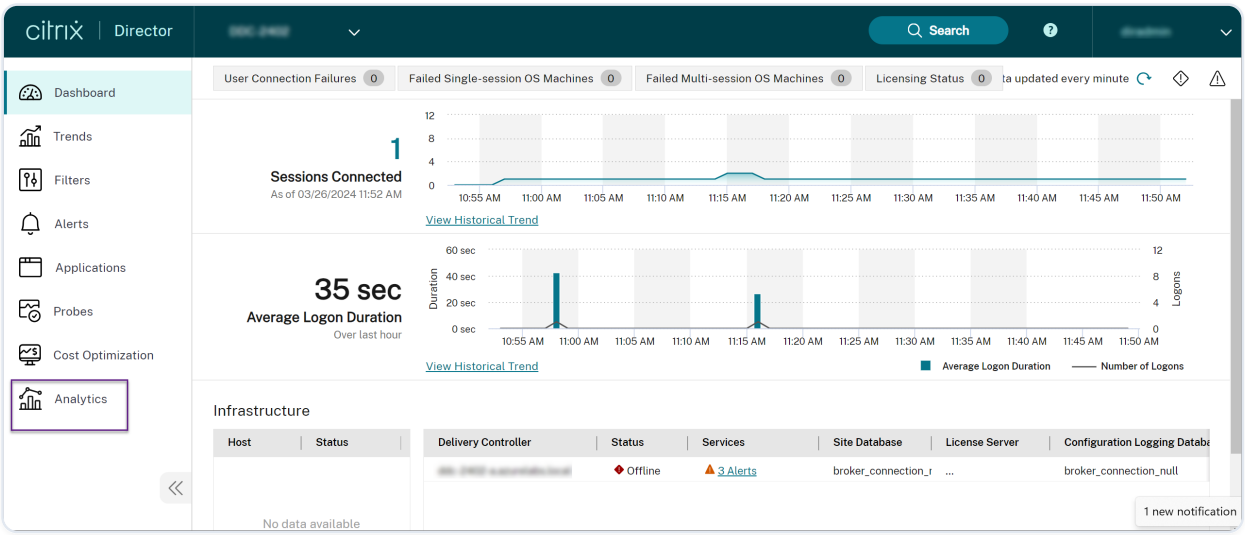
この設定は、IIS上のMicrosoftによって提供されます。詳細については、`https://docs.microsoft.com/ja-jp/dotnet/framework/network-programming/proxy-configuration`を参照してください。 構成ファイルの**defaultproxy**フィールドは、DirectorおよびMonitor Serviceのアウトバウンドアクセスを制御します。Performance Analyticsとの構成および通信には、**defaultproxy**フィールドを**true**に設定する必要があります。適用されているポリシーによっては、このフィールドがfalseに設定されている場合があります。この場合、フィールドを手動でtrueに設定する必要があります。変更を行う前に、構成ファイルのバックアップを取ってください。変更を有効にするには、Delivery Controller™上のMonitoringサービスを再起動してください。

- Citrix Analytics for PerformanceのCitrix Cloudエンタイトルメントがアクティブであること。
- Citrix Cloudアカウントが、製品登録エクスペリエンスに対する権限を持つ管理者アカウントであること。管理者権限の詳細については、「」(/ja-jp/citrix-cloud/citrix-cloud-management/identity-access-management/add-admins.html#modify-administrator-permissions)を参照してください。

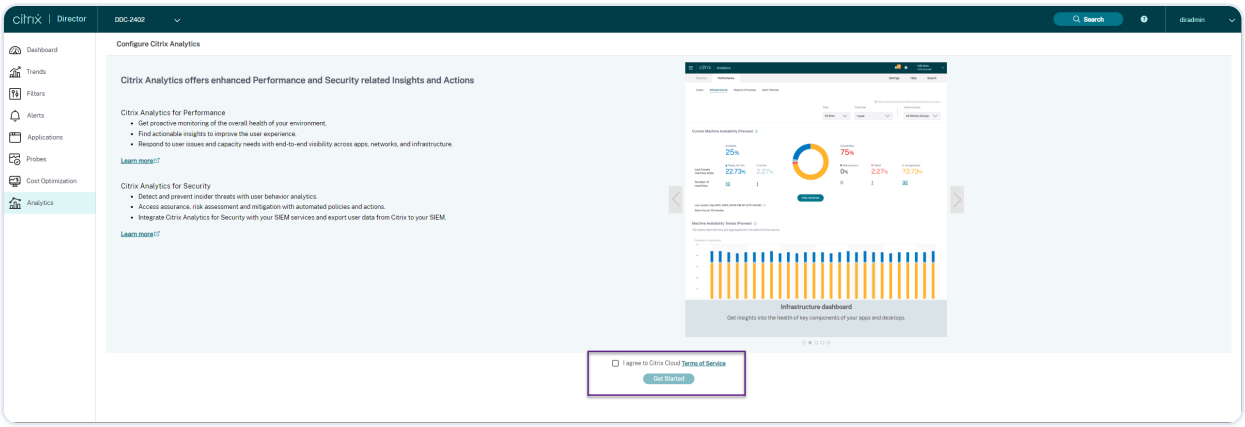
構成手順

前提条件を確認したら、次の手順を実行します。

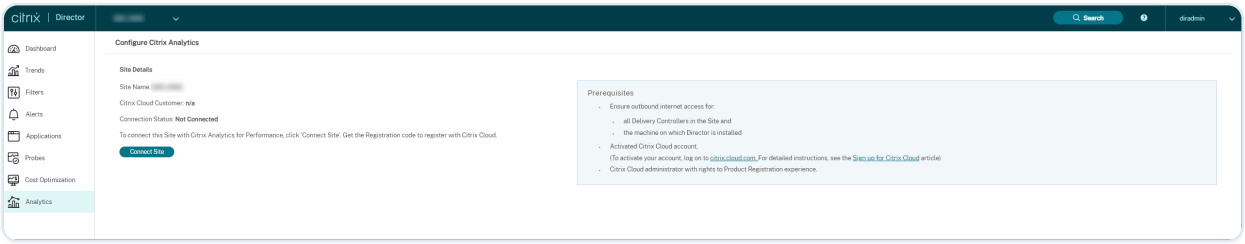
1. Director にフル管理者としてサインインし、Performance Analytics で構成するサイトを選択します。Director ダッシュボードページが表示されます。



2. **Analytics**タブをクリックします。**Citrix Analyticsの構成**ページが表示されます。

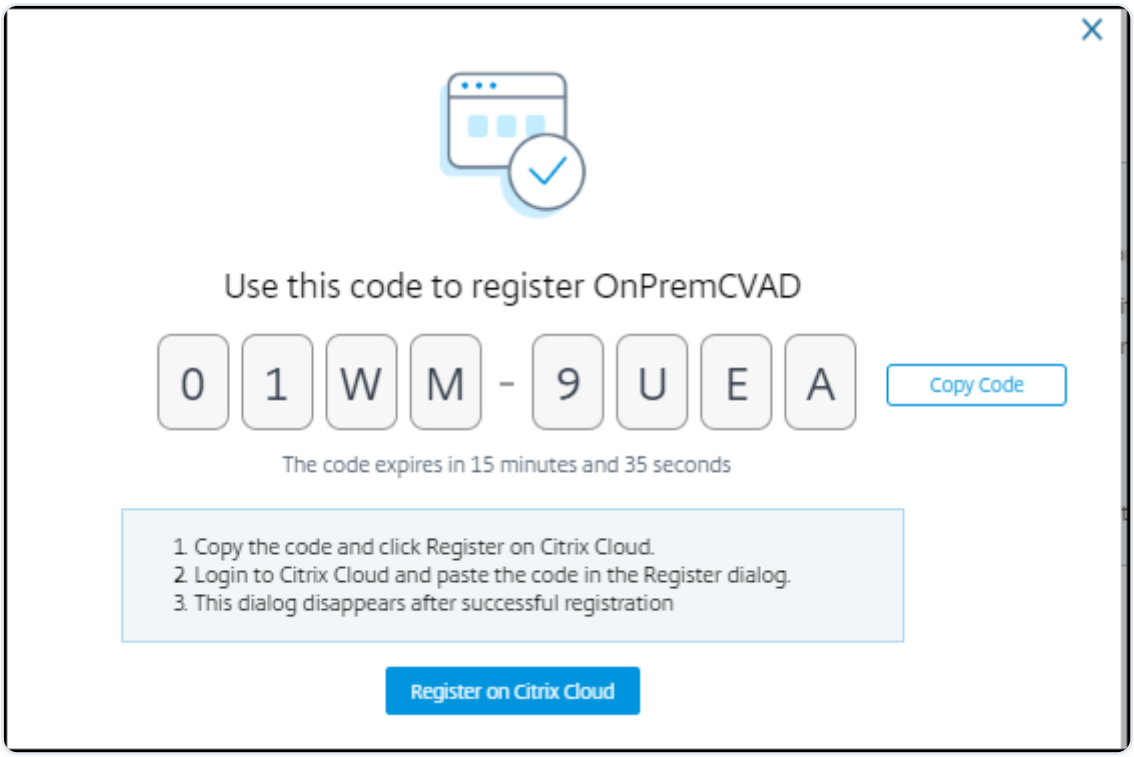


3. 手順を確認し、サービス利用規約を選択してから、**Get Started**をクリックします。**Site Details**ページが表示されます。

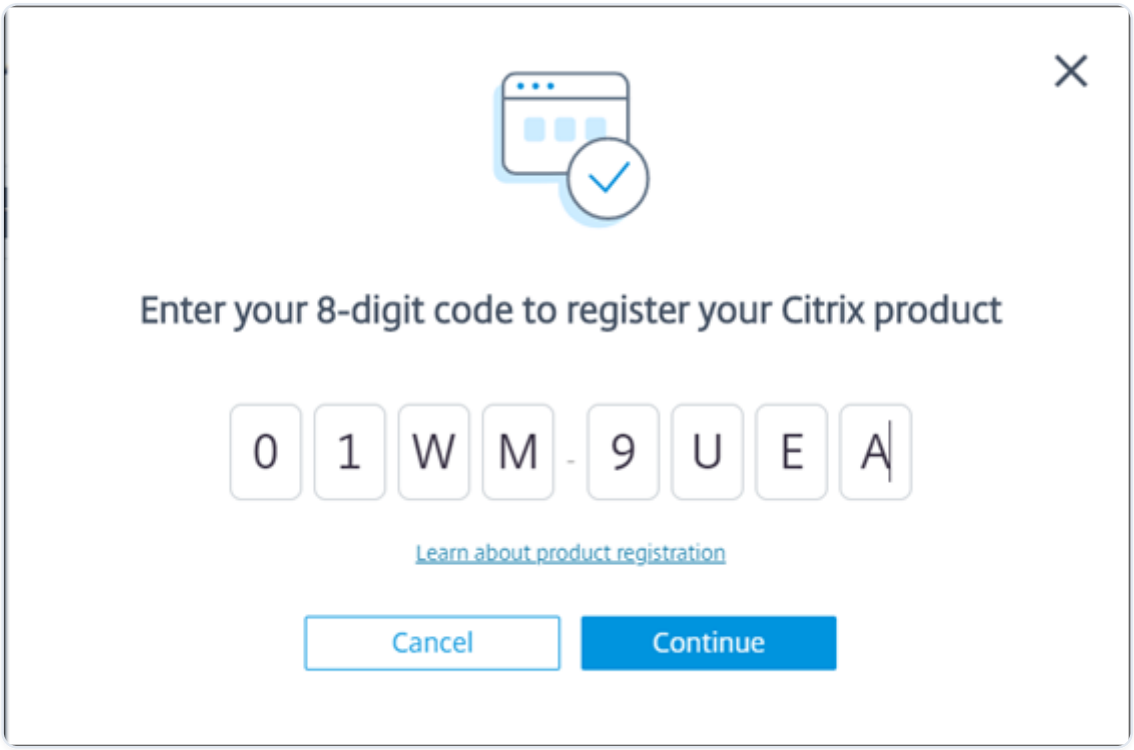


4. 前提条件を確認し、満たされていることを確認します。サイトの詳細を確認します。
5. 構成プロセスを開始するには、**Connect Site**をクリックします。

   このサイトを Citrix Cloud に登録するために使用する、一意の8桁の登録コードが生成されます。



6. コードをコピーするには**Copy Code**をクリックし、その後**Register on Citrix Cloud**をクリックします。Citrix Cloudの登録URLにリダイレクトされます。
7. Citrix Cloudの資格情報でサインインし、顧客を選択します。
8. コピーした登録コードをCitrix Cloudの製品登録ページに貼り付けます。登録するには**Continue**をクリックします。登録の詳細を確認し、**Register**をクリックします。



オンプレミスサイトがCitrix Cloudに登録されます。

9. **Director**の**Analytics**タブで、**Go to Analytics**をクリックします。

Analyticsに移動(/en-us/citrix-virtual-apps-desktops/2411/media/dir-onboarding7.png)

Performance Analyticsがブラウザーの新しいタブで開きます。 Performance Analyticsダッシュボード(/en-us/citrix-virtual-apps-desktops/2411/media/dir-onboarding-pa-dashboard.png)

Citrix Cloudセッションの有効期限が切れている場合、Citrix.comまたはMy Citrixアカウントのログオンページにリダイレクトされることがあります。

10. 複数のサイトをPerformance Analyticsに登録するには、Directorから各サイトについて前述の構成手順を繰り返します。構成されたすべてのサイトのメトリックは、Performance Analyticsダッシュボードに表示されます。

    サイトごとに複数のDirectorインスタンスが実行されている場合は、いずれか1つのDirectorインスタンスから構成します。サイトに接続されている他のすべてのDirectorインスタンスは、構成プロセスの後の次回の更新時に更新されます。

11. サイトをCitrix Cloudから切断するには、 をクリックします。このオプションは、既存の構成を削除します。

> **注:**
>
> サイトを初めて構成する場合、サイトからのイベントの処理には時間がかかる場合があります（約1時間）。これにより、Performance Analyticsダッシュボードにメトリックが表示されるまでに遅延が生じます。その後、イベントは定期的に更新されます。
>
> 切断後、新しいアカウントからのイベントが送信されるまで、古いアカウントからのデータ送信はしばらく継続されます。データ送信が停止してから約1時間、古いアカウントに関連する分析はPerformance Analyticsダッシュボードに表示されたままになります。
>
> Citrix Analyticsサービスへのエンタイトルメントの有効期限が切れると、サイトメトリックがPerformance Analyticsに送信されなくなるまでに最大1日かかります。

LTSR展開用Directorの独立リリース

LTSR展開用Directorの独立リリースにより、互換性のあるLTSR環境でCitrix®環境におけるトラブルシューティングと監視を強化するための最新のDirector機能にアクセスするオプションが提供されるようになりました。この機能により、2402 LTSR展開で最新のDirectorバージョンを使用でき

ます。また、アプリケーション配信インフラストラクチャに影響を与えることなく、LTSR発表後にリリースされた機能にアクセスできます。

スタンドアロンインストーラーには、モニターサービス、Directorサービス、およびモニターSnap-in用の最新の.msiが含まれています。これらの新しい.msiファイルを使用すると、2402 LTSR CU1を現在のリリース機能でアップグレードできます。

2402 LTSRリリース以降の現在のリリースに含まれるDirector機能については、以下を参照してください。

- シトリックス バーチャルアプリおよびデスクトップ 2407 リリース
- シトリックス バーチャルアプリおよびデスクトップ 2411 リリース

VDAの最小バージョンでのDirectorの特定の機能の詳細については、Directorバージョンマトリックスを参照してください。

利点

- **新機能へのアクセス**: 2402 LTSR発表後にリリースされたDirector機能（Citrix Virtual Apps and Desktops™ 2407および2411累積リリース（CR）の機能を含む）にアクセスできます。
- **ターゲットを絞ったアップグレード:** LTSRインフラストラクチャの残りの部分に影響を与えることなく、Directorおよび監視サービスコンポーネントのみをアップグレードします。
- **LTSR互換性**: 最新のDirector機能強化の恩恵を受けながら、LTSR環境を維持します。
- **ロールバックオプション:** 必要に応じて、以前のDirectorバージョンにロールバックする柔軟性があります。

重要な考慮事項

アップグレードされたDirectorコンポーネントはLTSR互換ですが、LTSRコアコンポーネントのサポート対象ではありません。ただし、LTSRインフラストラクチャの残りの部分は、既存のサポートを維持します。

前提条件

1. 「`Director2411.zip`」ファイルをCitrix downloadsページからダウンロードします。
2. インストーラーファイルを解凍すると、以下のインストーラーが見つかります。
    - DesktopDirector.msi
    - Monitor_PowerShellSnapIn.msi
    - Monitor_Service_x64.msi

3. Citrix Virtual Apps and Desktops 2402 LTSR または 2402 LTSR CU1 サイトを使用していることを確認してください。
4. Microsoft SQL Server バージョン 2019 以降を使用していることを確認してください。

概要

Citrix Virtual Apps and Desktops 2402 LTSR CU1 サイトを最新のCurrent Releaseの機能でアップグレードするには、以下の手順に従ってください。

1. **データベースをバックアップする**: アップグレードする前に、監視データベースをバックアップしてください。アップグレードプロセスでデータベースも更新されるため、この手順は非常に重要です。
2. **サイトをアップグレードする**: 現在のリリースで追加された新機能を取り込むために、サイトのアップグレードを進めてください。
3. **ロールバックオプション**: アップグレードされたサイトの使用を継続しないと判断した場合、ロールバック手順を使用して以前のサイトに戻すことができます。

アップグレード手順

1. 監視データベースのバックアップを取ります。
2. 「`Director2411.zip`」ファイルをCitrix downloadsページからダウンロードします。
3. インストーラーファイルを解凍すると、以下のインストーラーが見つかります。
    - DesktopDirector.msi
    - Monitor_PowerShellSnapIn.msi
    - Monitor_Service_x64.msi
4. .msi ファイルの場所に移動します。
5. コマンドラインを使用してモニターサービスをインストールします。

```
msiexec /i Monitor_service_x64 REINSTALLMODE=amus /l*v <logfile path
and name>
```

6. 画面の指示に従ってウィザードを完了します。
7. コマンドラインを使用してDirectorサービスをインストールします。

```
msiexec /i DesktopDirector /l*v <logfile path and name>
```

8. 画面の指示に従ってウィザードを完了します。
9. コマンドラインを使用して次のコマンドを実行します。

```
DirectorConfig.exe /UPGRADE
```

10. コマンドラインを使用してモニター スナップインをインストールします。

```
msiexec /i Monitor_PowershellSnapin_x64.msi
```

11. すべての.msiインストールが完了したら、Program Files内のMonitorサービスに移動し、次のコマンドを実行します。

```
Citrix.Monitor.exe /upgrade /enablefeatures
```

12. Citrix Site Managerを開き、**自動サイトアップグレード**オプションを選択して、アップグレードワークフローを完了します。
13. Directorにサインインして、新機能が利用可能であることを確認します。

ロールバック手順

1. 監視データベースのバックアップを必ず取得してください。
2. dbollback.zipという名前のデータベースロールバックスクリプトをダウンロードして実行します。

> **注：**
>
> DDCにsqlcmdがインストールされている場合、`dbrollback.zip`ファイルに含まれるPowerShellスクリプト (dbrollback.ps1) は、rollback.sqlスクリプトを実行する方法を示しています。

3. コントロールパネルから以下をアンインストールします。
   - **Citrix Monitor Service PowerShell Snap-in- x64** を選択し、**アンインストール**をクリックします。
   - **Citrix Monitor Service - x64** を選択し、**アンインストール**をクリックします。
   - **Citrix Director** を選択し、**アンインストール**をクリックします。

4. 既に取得済みのバックアップから監視データベースを復元します。詳細については、ナレッジ共有記事 CTX135207 を参照してください。
5. Citrix Virtual Apps and Desktopsインストーラーを使用して、Delivery ControllerとDirectorを再インストールします。詳細については、コアコンポーネントのインストール を参照してください。

   ```
   Or,
   ```

   次のコマンドを使用してコンポーネントを再インストールすることもできます。

   ```
   XenDesktopServerSetup.exe /components controller,director /
   configure_firewall /quiet
   ```

6. インストールが完了したら、**Open Citrix Site Manager** チェックボックスを選択します。
7. Citrix Site Manager で推奨されている場合は、サイトのアップグレードを実行します。

サポートとコンプライアンス

サポート

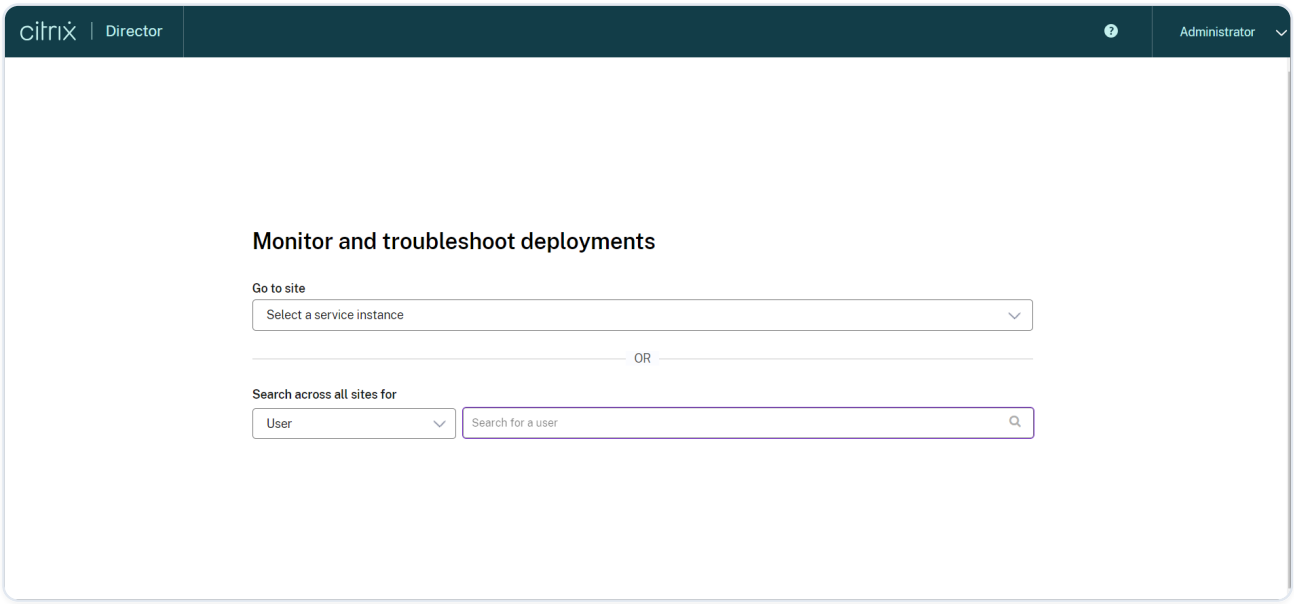
- Director の累積リリース (CR) バージョンは LTSR と互換性がありますが、LTSR に準拠していません。
- アップグレード後、必要なすべてのサポートチケットとバグ修正は、Director の次の累積リリース (CR) に追加されます。
- 変更または修正を含む CR は、次の累積更新プログラム (CU) で利用可能になります。

508/WCAG 2.1

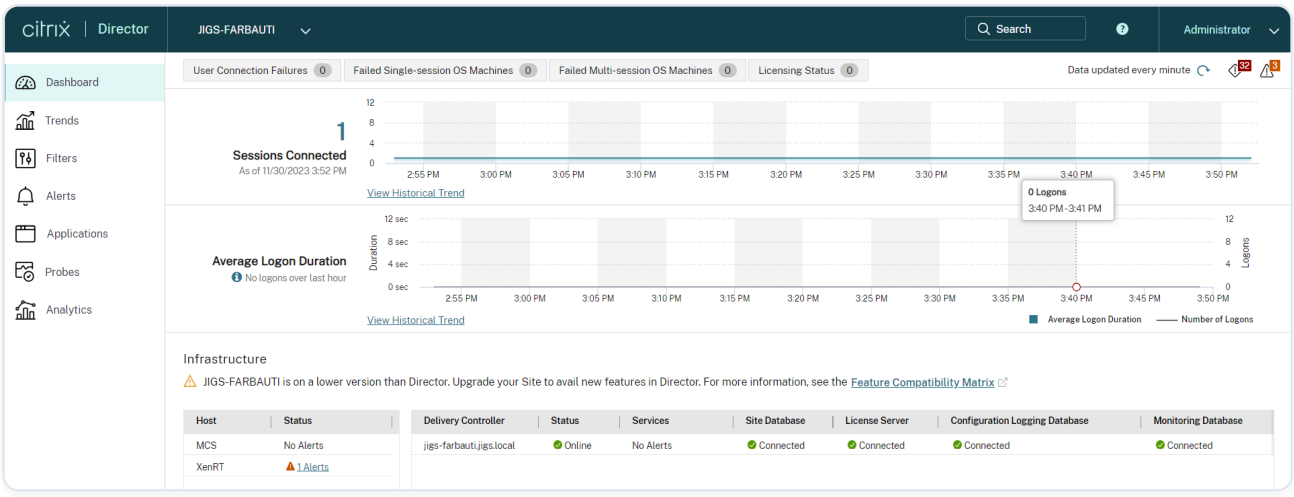
- 508/WCAG 2.1 準拠の義務があるお客様には、すべてのコアコンポーネントの LTSR バージョンを継続して使用することをお勧めします。

サイト分析

Director を使用して、展開の健全性を監視できます。オンボードされたすべてのサイトでユーザー、エンドポイント、またはマシンを検索することで、パフォーマンスの問題をトラブルシューティングできます。



完全な管理者権限があれば、Directorを開くと、ダッシュボードは、サイトの健全性と使用状況を監視するための一元的な場所を提供します。



現在障害がなく、過去60分間に障害が発生していない場合、パネルは折りたたまれたままになります。障害が発生すると、特定の障害パネルが自動的に表示されます。

> **注記：**
>
> 組織のライセンスと管理者権限によっては、一部のオプションまたは機能が利用できない場合があります。

Director ダッシュボードのパネル

ユーザー接続障害

過去60分間の接続障害。合計数の横にあるカテゴリをクリックすると、その種類の障害のメトリックが表示されます。隣接するテーブルでは、その数がデリバリーグループ別に分類されています。接続障害には、アプリケーション制限に達したことによる障害が含まれます。アプリケーション制限の詳細については、「アプリケーション」を参照してください。

失敗したシングルセッションOSマシンまたは失敗したマルチセッションOSマシン

過去 60 分間の合計失敗数をデリバリーグループ別に分類。失敗は、起動失敗、ブートスタック、未登録などの種類別に分類されます。マルチセッション OS マシンの場合、失敗には最大負荷に達したマシンも含まれます。

ライセンスステータス

ライセンスサーバーアラートには、ライセンスサーバーから送信されたアラートと、アラートを解決するために必要なアクションが表示されます。ライセンスサーバーバージョン 11.12.1 以降が必要です。デリバリーコントローラーアラートには、コントローラーから見たライセンス状態の詳細が表示され、コントローラーによって送信されます。XenApp 7.6 または XenDesktop 7.6 以降のコントローラーが必要です。アラートのしきい値は Studio で設定できます。**Delivery Controllers** > **Details** > **Product Editions** > **PLT** に表示されるライセンスステータスは、**Premium** であり、**Platinum** ではありません。

猶予状態

Directorは次のいずれかのグレース状態を表示します。この情報はDelivery Controllerから取得されます。

1. **非アクティブ:** いかなる種類のライセンスキャッシュモードでもありません。通常のライセンス制限が適用されます。
2. **緊急グレース:** ライセンスサーバーに到達できない場合、または接続の仲介中にライセンス情報を取得できない場合に有効になります。ユーザーには影響しません。Directorに表示されるエラーは、ライセンスサーバーに到達可能になるまで閉じることができません。
3. **猶予期間の期限切れ:** 緊急ライセンスキャッシュモードの有効期限が切れました。

詳細については、ライセンスの超過 および ライセンスバーストモード を参照してください。

接続されたセッション

過去60分間のすべてのデリバリーグループにわたる接続済みセッション。

平均ログオン時間

過去60分間のログオンデータ。左側の大きな数字は、1時間あたりの平均ログオン時間です。XenDesktop 7.0より前のVDAのログオンデータは、この平均には含まれません。詳細については、ユーザーログオンの問題の診断 を参照してください。

インフラストラクチャ

サイトのインフラストラクチャ（ホストとコントローラー）を一覧表示します。XenServerまたはVMwareのインフラストラクチャの場合、パフォーマンスアラートを表示できます。たとえば、管理対象サーバーまたは仮想マシンでCPU、ネットワークI/O、またはディスクI/Oの使用率が指定されたしきい値を超えたときに、XenCenterがパフォーマンスアラートを生成するように構成できます。デフォルトでは、アラートの繰り返し間隔は60分ですが、これも構成できます。詳細については、XenServer製品ドキュメント のXenCenterパフォーマンスアラートのセクションを参照してください。

> **注:**
>
> 特定のメトリックにアイコンが表示されない場合、そのメトリックは使用しているホストの種類でサポートされていないことを示します。たとえば、System Center Virtual Machine Manager (SCVMM) ホスト、AWS、およびCloudStackでは、正常性情報は利用できません。

これらのオプションを使用して問題のトラブルシューティングを続行します（以下のセクションに記載されています）：

- ユーザーマシンの電源を制御する
- マシンへの接続を防止する

セッションを監視する

セッションが切断されても、そのセッションはアクティブなままでアプリケーションは実行され続けますが、ユーザーデバイスはサーバーと通信しなくなります。

アクション	説明
ユーザーの現在接続されているマシンまたはセッションを表示する	アクティビティマネージャーおよびユーザー詳細ビューから、ユーザーの現在接続されているマシンまたはセッション、およびこのユーザーがアクセスできるすべてのマシンとセッションのリストを表示します。このリストにア

アクション	説明
	クセスするには、ユーザータイトルバーのセッションスイッチャーアイコンをクリックします。詳しくは、セッションの復元を参照してください。
すべてのデリバリーグループにわたる接続済みセッションの合計数を表示する	ダッシュボードの**Sessions Connected**ペインで、過去60分間のすべてのデリバリーグループにわたる接続済みセッションの合計数を表示します。次に、大きな合計数をクリックすると、フィルタービューが開き、選択したデリバリーグループと範囲、およびデリバリーグループ全体の使用状況に基づいてグラフィカルなセッションデータを表示できます。
アイドルセッションを終了する	セッションフィルタービューには、すべてのアクティブなセッションに関連するデータが表示されます。関連ユーザー、デリバリーグループ、セッション状態、およびしきい値期間を超えるアイドル時間に基づいてセッションをフィルター処理します。フィルター処理されたリストから、ログオフまたは切断するセッションを選択します。詳しくは、アプリケーションのトラブルシューティングを参照してください。
より長期間のデータを表示する	トレンドビューで、**Sessions**タブを選択して、より長期間にわたる接続済みセッションと切断済みセッションのより具体的な使用状況データ（つまり、過去60分より前のセッション合計）をドリルダウンします。この情報を表示するには、**View historical trends**をクリックします。

注:

ユーザーデバイスがレガシーなVirtual Delivery Agent (VDA) (バージョン7より前のVDAやLinux VDAなど) を実行している場合、Directorはセッションに関する完全な情報を表示できません。代わりに、情報が利用できないことを示すメッセージが表示されます。

デスクトップ割り当てルールの制限事項: Web Studioでは、異なるユーザーまたはユーザーグループに対して複数のデスクトップ割り当てルール (DAR) を、デリバリーグループ内の単一のVDAに割り当てることができます。StoreFront™は、ログインユーザーのDARに従って、対応する**表示名**とともに割り当てられたデスクトップを表示します。しかし、DirectorはDARをサポートしておらず、ログインユーザーに関係なく、デリバリーグループ名を使用して割り当てられたデスクトップを表示します。その結果、Directorで特定のデスクトップをマシンにマッピングすることはできません。 StoreFrontに表示される割り当てられたデスクトップを、Directorに表示されるデリバリーグループ名にマッピングするには、次のPowerShellコマンドを使用します。

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq
"\&lt;Name on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property
Name, Uid
```

セッション転送プロトコル

セッションの詳細パネルで、現在のセッションのHDX接続タイプに使用されている転送プロトコルを表示します。この情報は、VDAバージョン7.13以降で起動されたセッションで利用できます。

転送プロトコル(/en-us/citrix-virtual-apps-desktops/2411/media/sessions-transport-protocol.png)

- **HDX™**接続タイプの場合、,
  - HDX接続にEDTが使用されている場合、プロトコルは**UDP**と表示されます。
  - HDX接続にTCPが使用されている場合、プロトコルは**TCP**と表示されます。
- **RDP**接続タイプの場合、プロトコルは**n/a**と表示されます。

アダプティブトランスポートが構成されている場合、セッション転送プロトコルはネットワークの状態に基づいて、EDT (UDP経由) とTCPの間で動的に切り替わります。EDTを使用してHDXセッションを確立できない場合、TCPプロトコルにフォールバックします。

アダプティブトランスポートの構成の詳細については、「アダプティブトランスポート」を参照してください。

レポートのエクスポート

定期的な使用状況および容量管理レポートを生成するために、傾向データをエクスポートできます。エクスポートは、PDF、Excel、CSVのレポート形式をサポートしています。PDFおよびExcel

形式のレポートには、グラフと表で表された傾向が含まれます。CSV形式のレポートには、ビューを生成するために処理できる、またはアーカイブできる表形式のデータが含まれます。

レポートをエクスポートするには：

1. **傾向**タブに移動します。
2. フィルター条件と期間を設定し、**適用**をクリックします。トレンドグラフとテーブルにデータが入力されます。
3. **エクスポート**をクリックし、レポートの名前と形式を入力します。

Director は、選択したフィルター条件に基づいてレポートを生成します。フィルター条件を変更した場合は、**エクスポート**をクリックする前に**適用**をクリックしてください。

> **注:**
>
> 大量のデータをエクスポートすると、Director サーバー、Delivery Controller、および SQL サーバーのメモリと CPU の消費量が大幅に増加します。最適なエクスポートパフォーマンスを実現するために、サポートされる同時エクスポート操作の数とエクスポートできるデータ量は、デフォルトの制限に設定されています。

サポートされるエクスポート制限

エクスポートされた PDF および Excel レポートには、選択されたフィルター条件の完全なグラフが含まれています。ただし、すべてのレポート形式の表形式データは、テーブル内の行数またはレコード数のデフォルト制限を超えると切り捨てられます。サポートされるレコードのデフォルト数は、レポート形式に基づいて定義されます。

Internet Information Services (IIS) で Director アプリケーション設定を構成することで、デフォルトの制限を変更できます。

レポート形式	サポートされるレコードのデフォルト数	DIRECTOR アプリケーション設定のフィールド	サポートされる最大レコード数
PDF	500	UI.ExportPdfDrilldownLimit	5000
エクセル	100,000	UI.ExportExcelDrilldownLimit	100,000

レポート形式	サポートされるレコードのデフォルト数	DIRECTOR アプリケーション設定のフィールド	サポートされる最大レコード数
CSV	100,000 (「**セッション**」タブでは 10,000,000)	UI.ExportCsvDrilldownLimit	100,000

エクスポートできるレコード数の制限を変更するには:

1. IISマネージャーコンソールを開きます。
2. デフォルトのWebサイトの下にあるDirector Webサイトに移動します。
3. 「**アプリケーション設定**」をダブルクリックします。
4. 必要に応じて、UI.ExportPdfDrilldownLimit、UI.ExportExcelDrilldownLimit、または UI.ExportCsvDrilldownLimitフィールドの設定を編集または追加します。

アプリケーション設定でこれらのフィールド値を追加すると、デフォルト値が上書きされます。

> **警告:**
>
> サポートされる最大レコード数を超えるフィールド値を設定すると、エクスポートのパフォーマンスに影響を与える可能性があり、サポートされていません。

エラー処理

このセクションでは、エクスポート操作中に発生する可能性のあるエラーの対処方法について説明します。

- **Director がタイムアウトしました**

このエラーは、ネットワークの問題、Director サーバーまたは Monitor Service でのリソース使用率の高さが原因で発生する可能性があります。

デフォルトのタイムアウト期間は 100 秒です。Director Service のタイムアウト期間を延長するには、Internet Information Services (IIS) の Director アプリケーション設定で **Connector.DataServiceContext.Timeout** フィールドの値を設定します。

1. IIS マネージャーコンソールを開きます。
2. デフォルトの Web サイトの下にある Director Web サイトに移動します。

3. **アプリケーション設定**をダブルクリックします。
4. **Connector.DataServiceContext.Timeout** の値を編集します。

- **Monitor がタイムアウトしました**

このエラーは、ネットワークの問題、Monitor Service または SQL サーバーでのリソース使用率の高さが原因で発生する可能性があります。

Monitor Service のタイムアウト期間を延長するには、Delivery Controller で次の PowerShell コマンドを実行します。

```
asnp Citrix.*

Get-MonitorConfiguration

Set-MonitorConfiguration -MonitorQueryTimeoutSeconds &lt;timeout value>
```

- **同時実行中のエクスポートまたはプレビュー操作の最大数**

Director は、Export または Preview のインスタンスを 1 つサポートしています。「**Max concurrent Export or Preview operations ongoing**」エラーが発生した場合は、次の Export 操作を後でもう一度試してください。

同時実行の Export または Preview 操作の数を増やすことは可能ですが、Director のパフォーマンスに影響を与える可能性があり、サポートされていません。

1. IIS マネージャーコンソールを開きます。
2. デフォルトの Web サイトの下にある Director Web サイトに移動します。
3. **Application Settings** をダブルクリックします。
4. **UI.ConcurrentExportLimit** の値を編集します。

- **Director のディスク容量不足**

各 Export 操作には、Windows Temp フォルダーに最大 2 GB のハードディスク容量が必要です。Director サーバーで空き容量を確保するか、ハードディスク容量を追加してから、Export を再試行してください。

Monitorのホットフィックス

特定のマシン VDA (物理または VM) にインストールされているホットフィックスを表示するには、**Machine Details** ビューを選択します。

ユーザーマシンの電源状態を制御する

Director で選択したマシンの状態を制御するには、電源制御オプションを使用します。これらのオプションは、シングルセッション OS マシンで利用できますが、マルチセッション OS マシンでは利用できない場合があります。

注:

この機能は、物理マシンまたはリモート PC アクセスを使用するマシンでは利用できません。

コマンド	機能
再起動	VMの正常な（ソフト）シャットダウンを実行し、VMを再起動する前に実行中のすべてのプロセスを個別に停止します。たとえば、Directorで「起動に失敗しました」と表示されるマシンを選択し、このコマンドを使用して再起動します。
強制再起動	シャットダウン手順を最初に実行せずにVMを再起動します。このコマンドは、物理サーバーのプラグを抜き、再度差し込んで電源を入れるのと同じように機能します。
シャットダウン	VMの正常な（ソフト）シャットダウンを実行します。実行中のすべてのプロセスは個別に停止されます。
強制シャットダウン	シャットダウン手順を最初に実行せずにVMをシャットダウンします。このコマンドは、物理サーバーのプラグを抜くのと同じように機能します。すべての実行中のプロセスが常にシャットダウンされるとは限らず、この方法でVMをシャットダウンするとデータが失われるリスクがあります。
一時停止	実行中のVMを現在の状態で一時停止し、その状態をデフォルトのストレージリポジトリのファイルに保存します。このオプショ

コマンド	機能
	ンを使用すると、VMのホストサーバーをシャットダウンし、後で再起動した後、VMを再開して元の実行状態に戻すことができます。
再開	一時停止されたVMを再開し、元の実行状態を復元します。
開始	VMがオフのときに起動します（コールドスタートとも呼ばれます）。

電源制御アクションが失敗した場合、アラートにマウスを重ねると、失敗の詳細を示すポップアップメッセージが表示されます。

マシンへの接続を防止する

適切な管理者がイメージのメンテナンス作業を実行している間、メンテナンスモードを使用して一時的に新しい接続を防止します。

マシンでメンテナンスモードを有効にすると、無効にするまで新しい接続は許可されません。ユーザーが現在ログオンしている場合、すべてのユーザーがログオフするとすぐにメンテナンスモードが有効になります。ログオフしないユーザーには、マシンが特定の時間にシャットダウンされることを通知するメッセージを送信し、電源制御を使用してマシンを強制的にシャットダウンします。

1. たとえば、ユーザー詳細ビューからマシンを選択するか、フィルタービューでマシンのグループを選択します。
2. **メンテナンスモード**を選択し、オプションをオンにします。

ユーザーが割り当てられたデスクトップにメンテナンスモード中に接続しようとすると、デスクトップが利用できないことを示すメッセージが表示されます。メンテナンスモードを無効にするまで、新しい接続はできません。

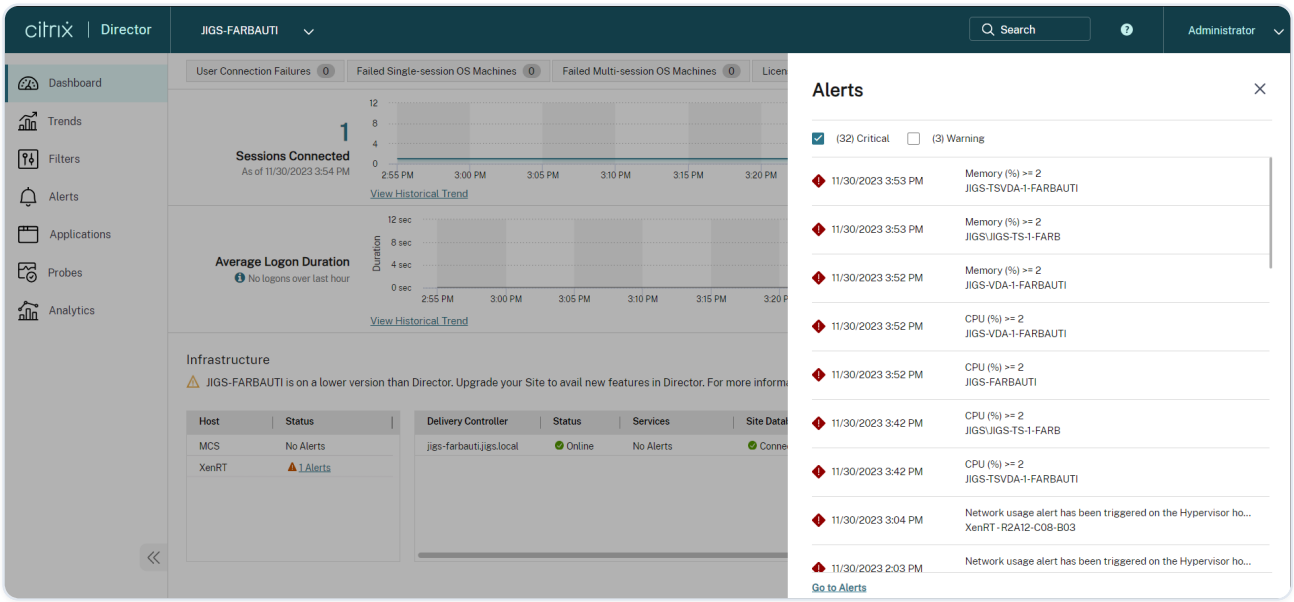
アプリケーション分析

アプリケーションタブには、アプリケーションベースの分析が単一の統合ビューで表示され、アプリケーションのパフォーマンスを効率的に分析および管理するのに役立ちます。サイトに公開されているすべてのアプリケーションの健全性と使用状況に関する貴重な洞察を得ることができます。プローブ結果、アプリケーションごとのインスタンス数、公開されたアプリケーションに関

連する障害やエラーなどのメトリックが表示されます。詳細については、**アプリケーションのトラブルシューティング**のアプリケーション分析セクションを参照してください。

アラートと通知

アラートは、Directorのダッシュボードやその他の概要ビューに、警告および重大なアラートシンボルとともに表示されます。アラートは、**Premium**ライセンスサイトで利用できます。アラートは1分ごとに自動的に更新されます。オンデマンドでアラートを更新することもできます。

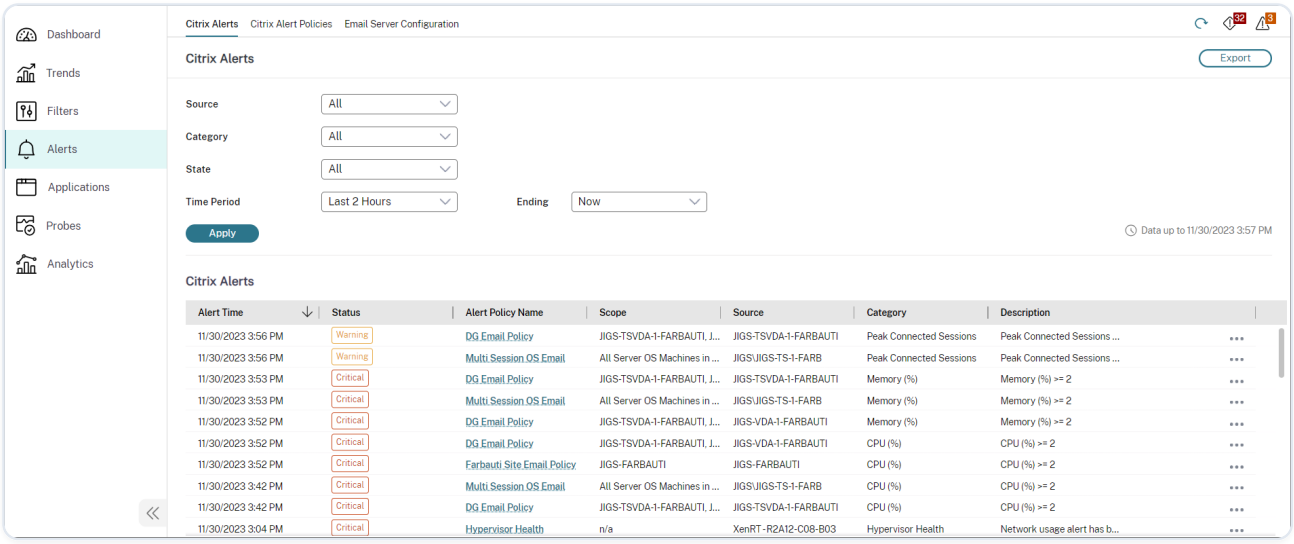


警告アラート（琥珀色の三角形）は、条件の警告しきい値に達したか、それを超えたことを示します。

重大なアラート（赤い円）は、条件の重大なしきい値に達したか、それを超えたことを示します。

アラートに関する詳細情報を表示するには、サイドバーからアラートを選択するか、サイドバーの下部にある**アラートに移動**リンクをクリックするか、Directorページの上部から**アラート**を選択します。

アラートビューでは、アラートをフィルター処理してエクスポートできます。たとえば、過去1か月間の特定のデリバリーグループの失敗したマルチセッションOSマシン、または特定のユーザーのすべてのアラートなどです。詳しくは、「レポートのエクスポート」を参照してください。



Citrix®アラート

Citrixアラートは、Citrixコンポーネントから発生し、Directorで監視されるアラートです。Directorの**アラート** \> **Citrixアラートポリシー**でCitrixアラートを構成できます。構成の一部として、アラートが設定したしきい値を超えたときに、個人やグループにメールで通知を送信するように設定できます。Citrixアラートの設定について詳しくは、「アラートポリシーの作成」を参照してください。

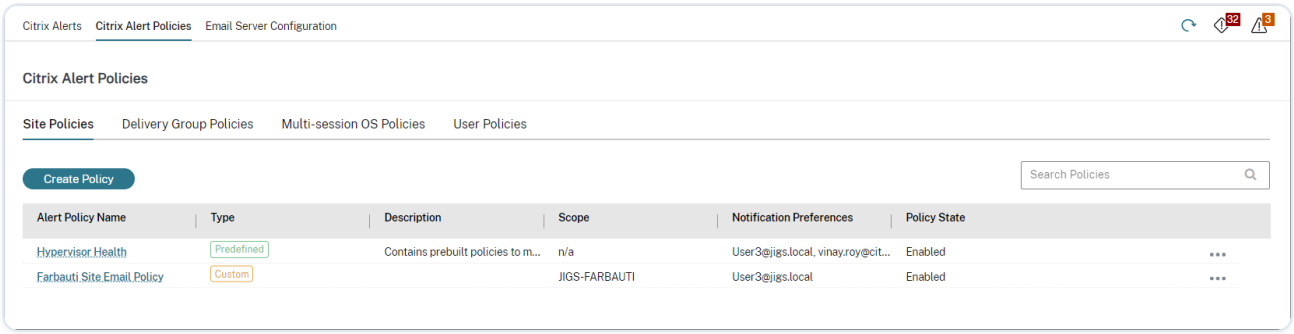
> **注:**
>
> ファイアウォール、プロキシ、またはMicrosoft Exchange Serverがメールアラートをブロックしないことを確認してください。

スマートアラートポリシー

事前定義されたしきい値を持つ一連の組み込みアラートポリシーは、デリバリーグループおよびマルチセッションOS VDAスコープで利用できます。この機能には、Delivery Controllerバージョン7.18以降が必要です。組み込みアラートポリシーのしきい値パラメーターは、**アラート** \> **Citrixアラートポリシー**で変更できます。 これらのポリシーは、サイトで定義されたデリバリーグループまたはマルチセッションOS VDAという少なくとも1つのアラートターゲットがある場合に作成されます。さらに、これらの組み込みアラートは、新しいデリバリーグループまたはマルチセッションOS VDAに自動的に追加されます。

Directorとサイトをアップグレードする場合、以前のDirectorインスタンスのアラートポリシーが引き継がれます。組み込みのアラートポリシーは、Monitorデータベースに対応するアラートルールが存在しない場合にのみ作成されます。

組み込みのアラートポリシーのしきい値については、「アラートポリシーの条件」セクションを参照してください。



高度なアラートポリシー

Director のプロアクティブ通知およびアラート機能が強化され、**高度なアラートポリシー**という新しいアラートフレームワークが追加されました。この機能を使用すると、各要素または条件のきめ細かな詳細を含めてアラートを作成できるため、アラートの範囲に対する制御が強化されます。現在、これらのポリシーには、コスト削減とインフラストラクチャに関するアラートが含まれています。

データソース駆動型アラートである高度なアラートポリシーの導入により、複数条件のスコープフィルタリングを使用できます。

この機能は、過剰なアラートを減らすのに役立ちます。過剰なアラートは、重要な問題への対応の応答性や有効性の低下につながる可能性があります。このポリシーは、アラートポリシーの有効性と管理者からのエンゲージメントを測定するのに役立ちます。

> > ****セクションから高度なアラートポリシーを作成できます。

次のデータソースのいずれかを選択できます。

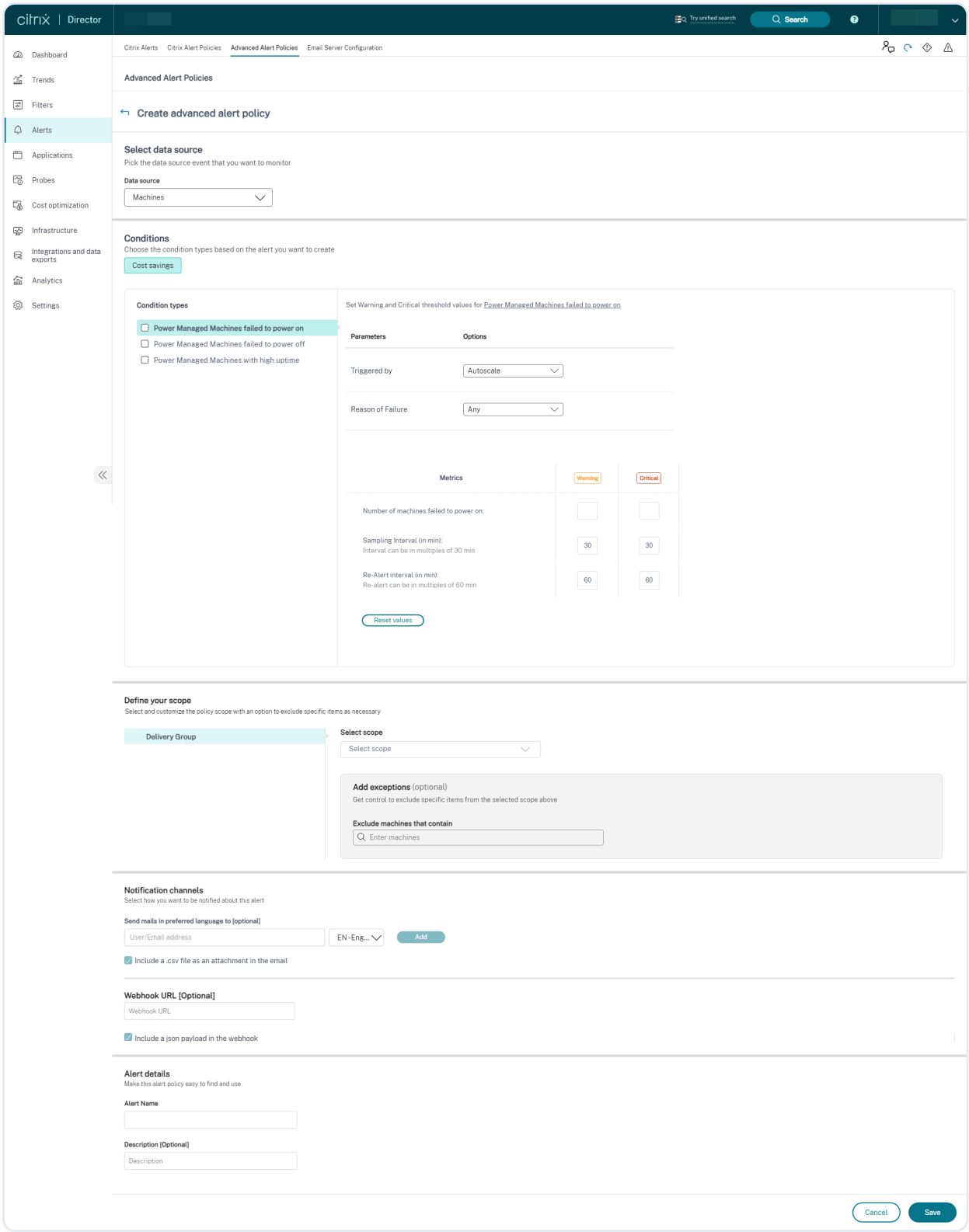
- マシン
- プロビジョニングサービス
- StoreFront™
- デリバリーコントローラー™

コスト削減に関するアラート

コストを最適化するのに役立つコスト削減に関するアラートを作成できます。現在、マシンに関するアラートを作成できます。

マシンに関するアラートを作成するには、次の手順を実行します。

1. 「**アラート**」タブ > 「**高度なアラートポリシー**」をクリックします。「**高度なアラートポリシー**」ページが表示されます。
2. 「**ポリシーの作成**」をクリックします。「**高度なアラートポリシーの作成**」セクションが表示されます。
3. データソースドロップダウンリストから「**マシン**」を選択します。コスト削減条件と、それに対応する条件タイプが表示されます。



4. 必要な条件タイプを以下から選択します。

   - 電源管理されたマシンが起動に失敗しました
   - 電源管理されたマシンがシャットダウンに失敗しました
   - アップタイムが高い電源管理されたマシン

5. 選択した各条件について、特定のパラメーターと対応するオプションを選択します。

6. 選択した条件タイプに対して、警告およびクリティカルのメトリックを設定します。
    - アップタイムが高い電源管理されたマシンについて:
        - アップタイムしきい値を超過したマシンの数
        - 再アラート間隔（分）。間隔は最低60分です。
    - 電源オンに失敗した電源管理マシンおよび電源オフに失敗した電源管理マシンについて:
        - アップタイムしきい値を超過したマシンの数
        - サンプリング間隔（分）は30分の倍数に設定できます
        - 再アラート間隔（分）は60分の倍数に設定できます
7. 必要に応じて、選択したアラートの再アラート間隔をスケジュールします。
8. アラートのスコープを定義します。
9. 通知チャネルを設定します。メールまたはWebhookを選択できます。

    a. 次のチェックボックスを選択できます。

    - Webhookに添付ファイルとしてJSONペイロードを含める
    - メールに添付ファイルとしてCSVファイルを含める

    詳細については、アラートコンテンツの機能強化を参照してください。
10. **アラート名**や**説明**（オプション）などの**アラートの詳細**を入力します。
11. **保存**をクリックします。アラートが作成されます。

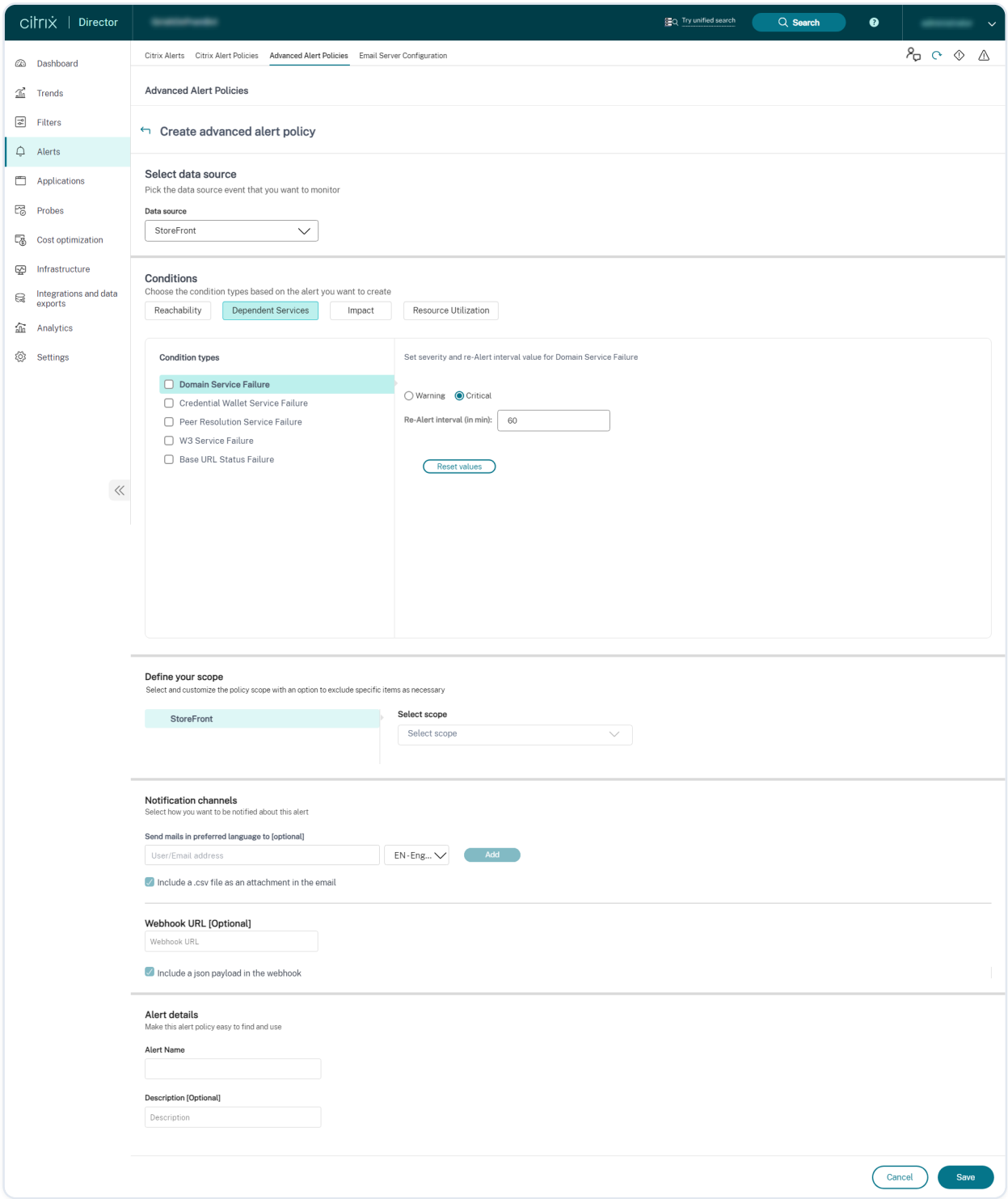
インフラストラクチャ監視のアラート

次のサポートされているCitrix Virtual Apps and Desktops™コンポーネントの健全性を監視するためのアラートを作成できます。

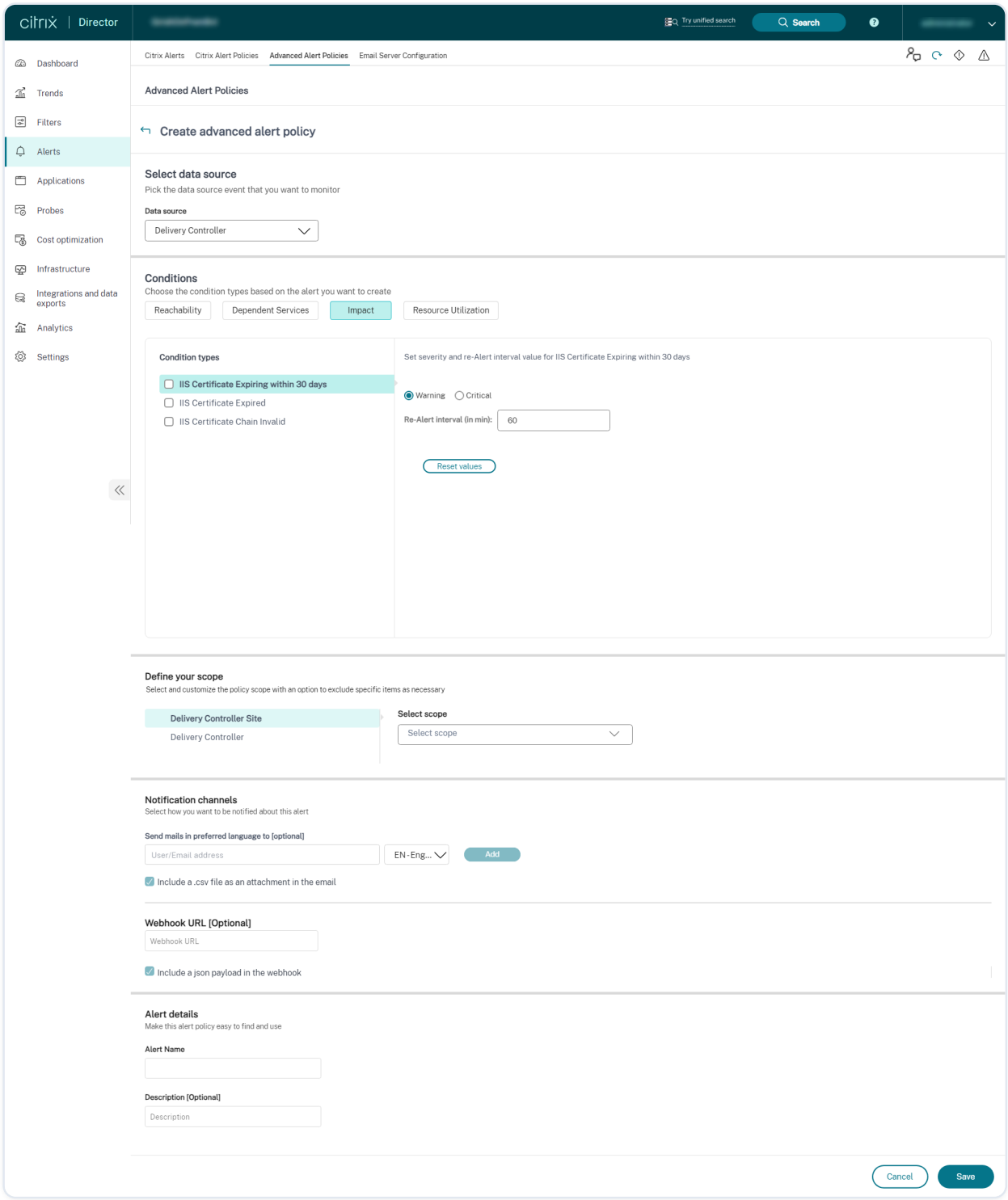
- プロビジョニングサービス

- StoreFront



- デリバリーコントローラー



インフラストラクチャ監視 のセットアップが完了すると、Director で利用可能な健全性データを使用して、必要なコンポーネントのアラートを設定できます。管理者は、条件、スコープ、および通知媒体を設定して、電子メールまたは Webhook を介した JSON ペイロードで重要なアラートを受信できます。発生したアラートは、分析および管理のために **Citrix Alerts** セクションでも利用できます。

新しく導入されたインフラストラクチャポリシーの一部として、アラート条件は次の 4 つのセクションに分類されます。

- 到達可能性
- 依存サービス
- 影響
- リソース使用率

各カテゴリ内の条件は、組織の優先順位に基づいて、**重大** および **警告** の重大度で設定できます。これらのアラートの再アラート間隔をスケジュールすることもできます。

アラート > **Citrix アラートポリシー** セクションからインフラストラクチャポリシーを作成できます。必要なカテゴリを選択し、ポリシーに必要な条件を選択できます。ポリシーの作成方法の詳細については、「アラートポリシーの作成」を参照してください。ポリシーが作成された後、Citrix Alerts ページでポリシーを編集、削除、または無効にできます。

各カテゴリとコンポーネントでサポートされている条件の詳細については、以下を参照してください。

- Provisioning Service の健全性メトリック
- StoreFront の健全性メトリック
- Delivery Controller の正常性メトリック

次のデータは、電子メールまたはCitrixアラートページでアラートとして受信されます。

フィールド	説明
顧客ID	サイトの顧客ID。
アラートレベル	指定できる値は、Critical と Warning です。
ターゲット	アラートがトリガーされたマシンの名前。
時間	アラートがトリガーされた時刻。
スコープ	ポリシーのスコープ。
ポリシー	ポリシーの名前。
説明	アラートがトリガーされる問題の説明。

ポリシーのスコープを定義する

アラートのスコープを定義し、例外を追加できます。アラートは選択したスコープに対してのみ生成され、例外の追加を使用して除外されたサブスコープはアラート生成に含まれません。この機能は、詳細なレベルでアラートを作成するのに役立ちます。

メールまたはWebhook URLを介して通知を作成できます。アラートを受信する希望の言語を選択することもできます。また、メールの場合は.CSVファイル添付として、Webhook URLを介してはJSONペイロードとしてアラートパラメータを受信するオプションを選択することもできます。添付ファイルには、必要なパラメータの詳細が含まれています。詳細については、「アラートコンテンツの機能強化」を参照してください。

次のデータは、メールまたは**Citrix Alerts**ページでアラートとして受信されます。

フィールド	説明
顧客ID	サイトの顧客ID。
アラートレベル	この値は、各アラート条件に設定された事前定義値です。可能な値は「Critical」と「Warning」です。
条件	この値は、ポリシー作成時に設定された条件です。たとえば、未登録のマシンの数が20以上である場合などです。
ターゲット	アラートがトリガーされるデリバリーグループまたはサイトの名前。
サイト	サイトの名前。
スコープ	ポリシーのスコープ。この値にはサブスコープも含まれます。
ポリシー	ポリシーの名前。
説明	アラートがトリガーされる問題の説明。

PowerShellスクリプトを使用して高度なアラートポリシーを作成する方法?

アラートポリシーを作成するためのPowerShellスクリプト:

```
asnp Citrix.Monitor.*

# Add Parameters

$timeSpan = New-TimeSpan -Seconds 30

$alertThreshold = 1

$alarmThreshold = 2

# Add Target UID's

$targetIds = @()

$targetIds += "e9a211b4-a1f3-4f74-b6c7-85225902e997"

# Add email addresses

$emailaddress = @()

$emailaddress += "loki@abc.com"

# Create new policy

$policy = New-MonitorNotificationPolicy -Name
"FailedMachinePercentageAlertCreationViaPowershell" -Description "Policy
created to test urm" -Enabled $true
```

次の行をFAILEDMACHINEPERCENTAGEの正しい条件に置き換えます

```
Add-MonitorNotificationPolicyCondition -Uid $policy.Uid -ConditionType
FailedMachinePercentage -AlertThreshold $alertThreshold -AlarmThreshold
$alarmThreshold -AlertRenotification $timeSpan -AlarmRenotification
$timeSpan

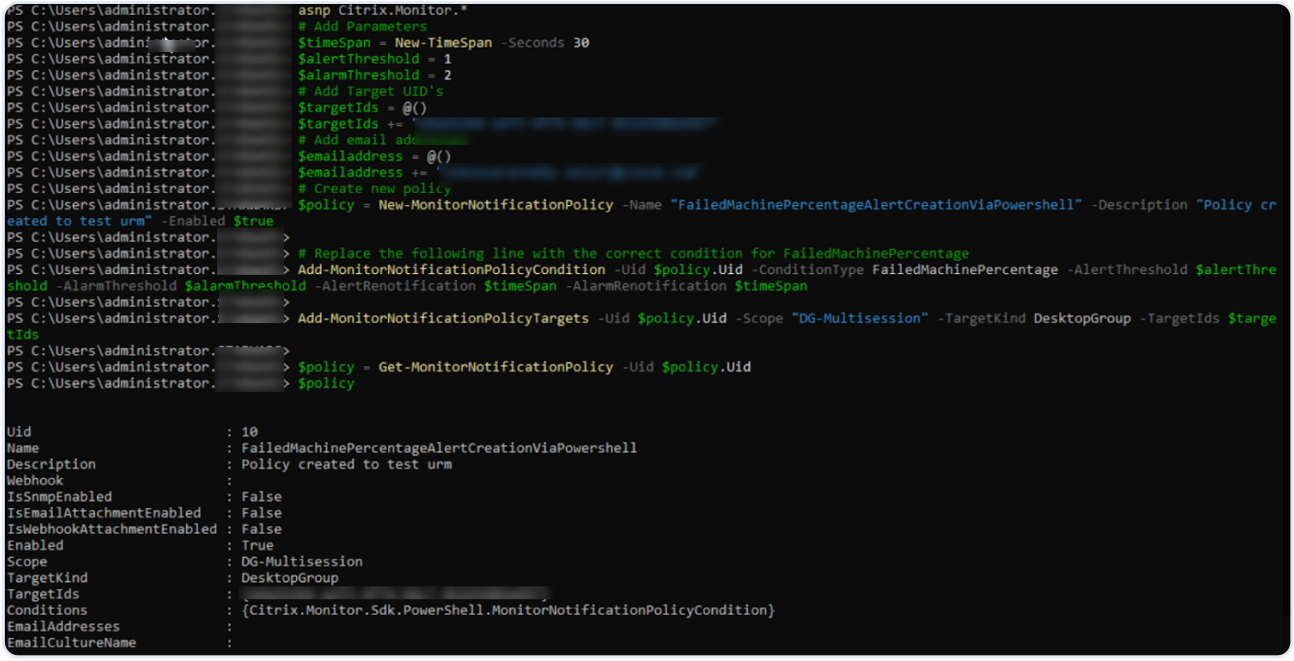


Add-MonitorNotificationPolicyTargets -Uid $policy.Uid -Scope "DG-
Multisession" -TargetKind DesktopGroup -TargetIds $targetIds



$policy = Get-MonitorNotificationPolicy -Uid $policy.Uid
```

```
$policy
```



上記の画像から、ポリシーが作成され、Uidが10であることがわかります。

構成にメールを追加するには

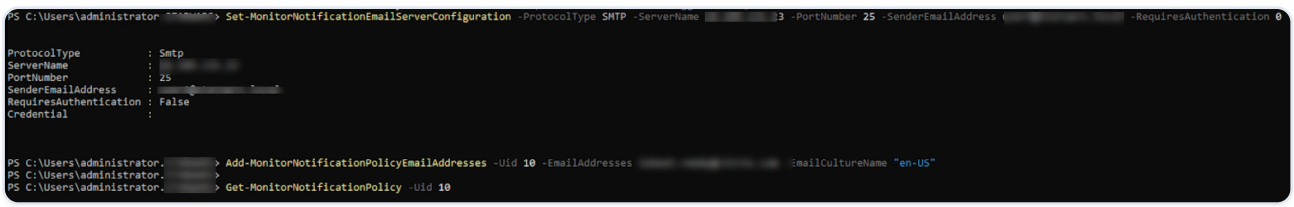
```
Set-MonitorNotificationEmailServerConfiguration -ProtocolType SMTP
-ServerName NameOfTheSMTPServerOrIPAddress -PortNumber 80
-SenderEmailAddress loki@abc.com -RequiresAuthentication 0
```

ポリシーにメールを追加するには

```
Add-MonitorNotificationPolicyEmailAddresses -Uid $policy.Uid
-EmailAddresses $emailaddress -EmailCultureName "en-US"
```

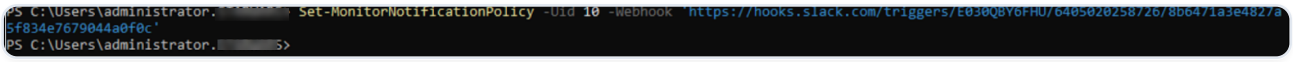
メールを追加するためのサンプルスクリプト:

```
Add-MonitorNotificationPolicyEmailAddresses -Uid 10 -EmailAddresses
$emailaddress -EmailCultureName "en-US"
```



ポリシーにWEBHOOK URLを追加するには

```
Set-MonitorNotificationPolicy –Uid $polcy.Uid –Webhook 'URL'
```

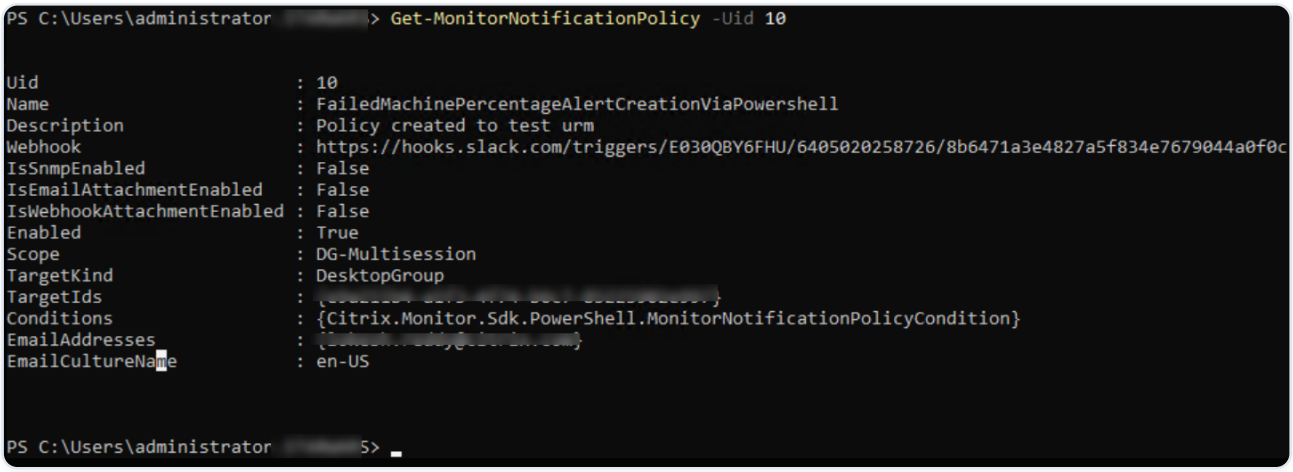


Webhook URLを追加するためのサンプルスクリプト:

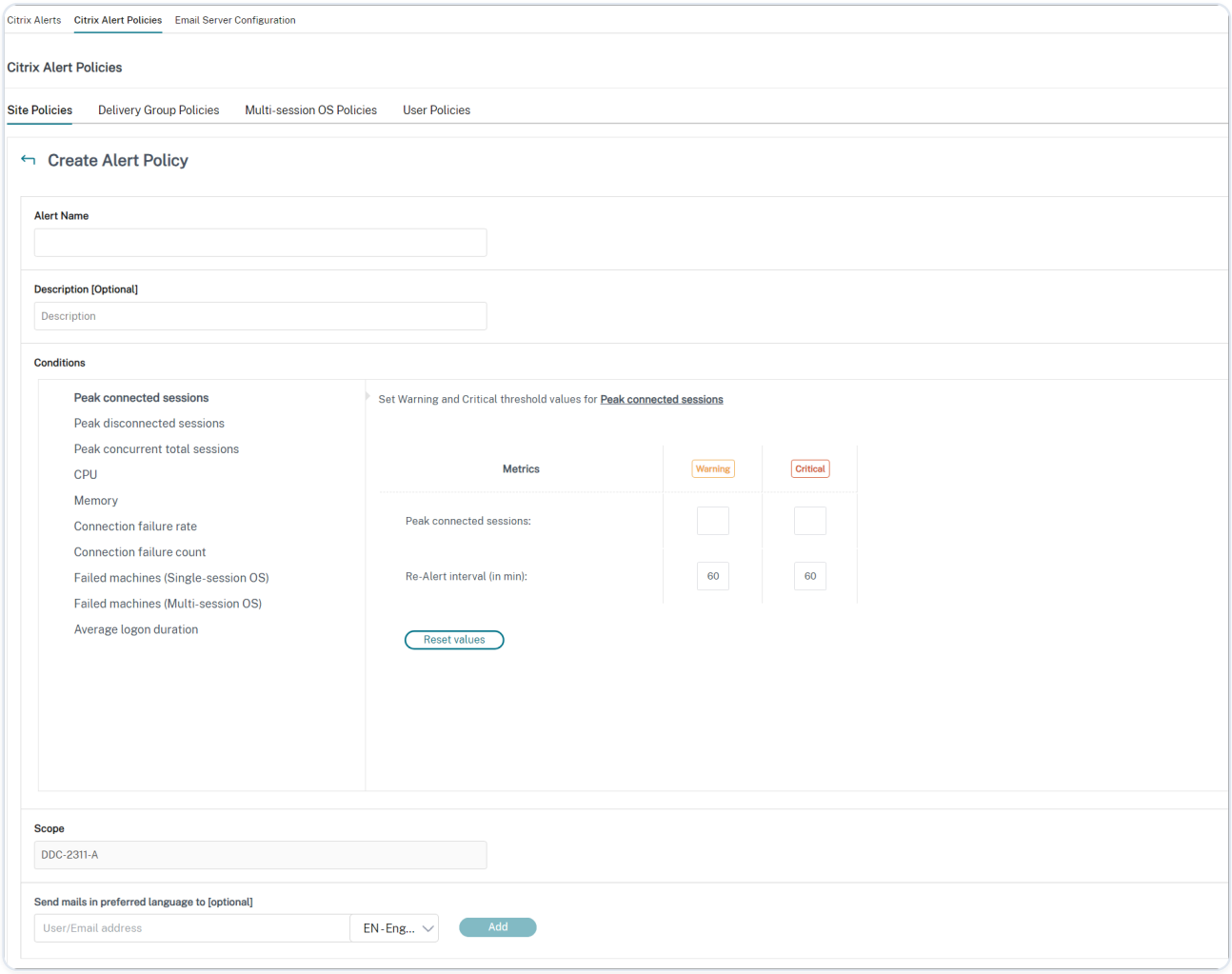
```
Set-MonitorNotificationPolicy –Uid 10  –Webhook  'https://hooks.slack.com/
triggers/E030QBY6FHU/6405020258726/8b6471a3e4827a5f834e7679022a1f1c'
```

作成されたポリシーの詳細を取得

```
Get-MonitorNotificationPolicy -Uid 10
```



アラートポリシーを作成する



たとえば、特定のセッション数条件が満たされたときにアラートを生成するアラートポリシーを作成するには、次の手順を実行します。

1. **アラート** > **Citrixアラートポリシー** に移動し、たとえば、マルチセッションOSポリシーを選択します。
2. **作成** をクリックします。
3. ポリシーに名前を付けて説明し、アラートがトリガーされるために満たす必要がある条件を設定します。たとえば、ピーク接続セッション、ピーク切断セッション、およびピーク同時合計セッションの警告数と重大数を指定します。警告値は重大値より大きくしてはいけません。詳細については、アラートポリシーの条件を参照してください。
4. 再アラート間隔を設定します。アラートの条件が引き続き満たされている場合、この時間間隔でアラートが再度トリガーされ、アラートポリシーで設定されている場合はメール通知が生成されます。却下されたアラートは、再アラート間隔でメール通知を生成しません。
5. スコープを設定します。たとえば、特定のデリバリーグループに設定します。

6. 通知設定で、アラートがトリガーされたときにメールで通知する必要があるユーザーを指定します。アラートポリシーでメール通知設定を行うには、**メールサーバー構成**タブでメールサーバーを指定する必要があります。

   a. アラートコンテンツを.CSV添付ファイルまたはJSONペイロードを介して受信することもできます。そのためには、次のチェックボックスを選択します。

      - **Webhookにjsonペイロードを添付として含める**
      - **メールにcsvファイルを添付として含める**

> **注:**
>
> .CSV添付ファイルおよびJSONペイロードを介してアラートコンテンツを受信するオプションは、現在、一部のアラートでのみ利用可能です。詳細については、「アラートコンテンツの機能強化」を参照してください。

7. 「**保存**」をクリックします。

スコープに20以上のデリバリーグループが定義されたポリシーを作成すると、構成の完了に約30秒かかる場合があります。この間、スピナーが表示されます。

最大20のユニークなデリバリーグループ（合計1000のデリバリーグループターゲット）に対して50を超えるポリシーを作成すると、応答時間が増加する可能性があります（5秒以上）。

アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、マシンパラメーターを使用して定義された誤ったデリバリーグループアラートがトリガーされる可能性があります。

> **注:**
>
> アラートポリシーを削除した後、そのポリシーによって生成されたアラート通知が停止するまでに最大30分かかる場合があります。

アラートコンテンツの機能強化

Directorの警告機能が強化され、CSV添付ファイルとJSONペイロードが含まれるようになりました。この強化により、メールでCSV添付ファイルとして、またはWebhookがある場合はJSONペイロードとして、アラートの詳細を取得できます。このCSV添付ファイルまたはJSONペイロードを

使用すると、詳細なレベルで豊富なコンテンツを受け取ることができ、問題の迅速な特定と解決に役立ちます。

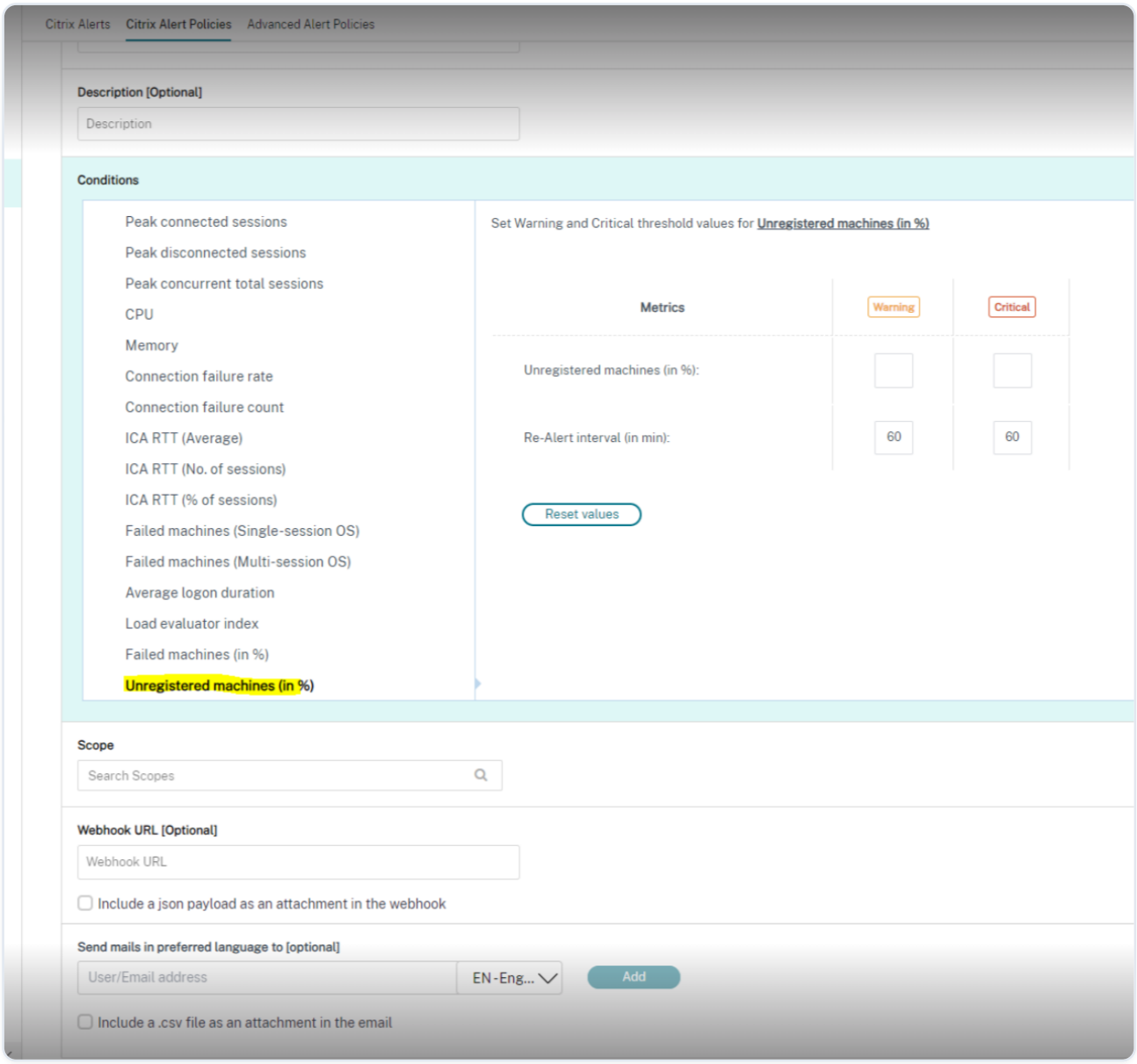
現在、この機能強化は以下の警告でのみ利用可能です。

- マシンの稼働時間
- 電源オンアクションの失敗
- 電源オフアクションの失敗
- 未登録マシン (%)

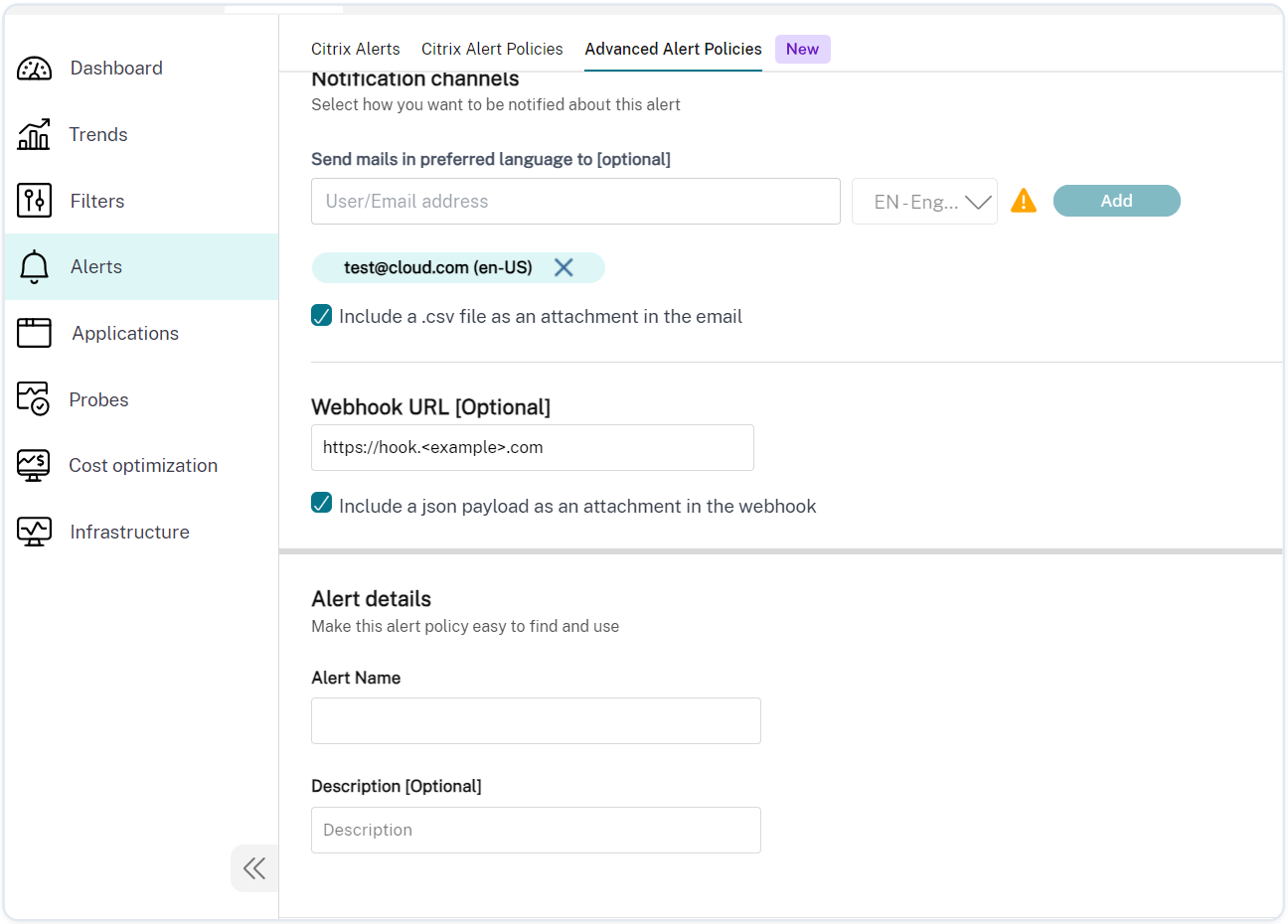
この機能を使用するには、警告に移動し、次のチェックボックスを選択します。

- **WebhookにJSONペイロードを添付ファイルとして含める**
- **メールにCSVファイルを添付ファイルとして含める**

以下は、**Citrix Alert Policies**セクションのスクリーンショットです。



以下は、**Advanced Alert Policies**セクションのスクリーンショットです。



CSV添付ファイル

次の表は、サポートされているすべての警告の.CSV添付ファイルの列を示しています。

列	適用されるアラート
マシン名、IPアドレス、およびデリバリーグループ名	マシンの稼働時間、電源オフ失敗アクションと電源オン失敗アクション、および未登録マシン (%)
現在の登録状態、失敗日、障害状態、およびライフサイクル状態	未登録マシン (%)
最終電源アクション失敗理由、最終電源アクショントリガー元、最終電源アクションタイプ、および最終電源アクション完了日	電源オフ失敗アクションと電源オン失敗アクション
電源状態、電源オン日、および合計稼働時間 (分)	マシンの稼働時間

WEBHOOKペイロード

未登録マシンの割合アラート

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Unregistered machines (in %)\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"CurrentRegistrationState\":\"Unregistered\",
\"FailureDate\":\"<Date of Failure>\",\"FaultState\":\"<Fault State of the
Machine>\",\"LifecycleState\":\"<Lifecycle state of the Machine>\"},
{\"MachineName\":\"<Name of the Machine>\",\"IPAddress\":\"<IP Address>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",
\"CurrentRegistrationState\":\"Unregistered\",\"FailureDate\":\"<Date of
Failure>\",\"FaultState\":\"<Fault State of the Machine>\",
\"LifecycleState\":\"<Lifecycle state of the Machine>\"}]}"

}
```

電源オン失敗アクションアラート

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Failure To PowerOn Action\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure, HypervisorRateLimitExceeded, UnknownError,
Power Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-User,
Administrator, Auto-Scale, Schedule>\",\"LastPowerActionType\":\"<PowerOn/
PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"},{\"MachineName\":\"<Name of the Machine>\",
\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of the
DeliveryGroup>\",\"LastPowerActionFailureReason\":
```

```
\"<HypervisorReportedFailure, HypervisorRateLimitExceeded, UnknownError,
Power Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-User,
Administrator, Auto-Scale, Schedule>\",\"LastPowerActionType\":\"<PowerOn/
PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"}]}"

}
```

電源オフ失敗アクションアラート

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Failure To PowerOff Action\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IPV4 Address of the Machine>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",
\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Powe
r Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-
User,Administrator,Auto-Scale,Schedule>\",\"LastPowerActionType\":
\"<PowerOn/PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"},{\"MachineName\":\"<Name of the Machine>\",
\"IPAddress\":\"<IPV4 Address of the Machine>\",\"DeliveryGroupName\":
\"<Name of the DeliveryGroup>\",\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Powe
r Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-
User,Administrator,Auto-Scale,Schedule>\",\"LastPowerActionType\":
\"<PowerOn/PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"}]}"

}
```

マシンの稼働時間アラート

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Machine Uptime Alert\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"PowerState\":\"<On/Off>\",\"PoweredOnDate\":
\"2024-05-15T15:04:27.723\",\"TotalUptimeInMinutes\":180},
{\"MachineName\":\"<Name of the Machine>\",\"IPAddress\":\"<IP Address>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",\"PowerState\":
\"<ON/OFF>\",\"PoweredOnDate\":\"2024-05-15T15:04:27.723\",
\"TotalUptimeInMinutes\":\"<Uptime Duration>\"}]}"

}
```


アラートポリシーの条件

以下に、アラートカテゴリ、アラートを軽減するための推奨アクション、および定義されている場合は組み込みポリシー条件を示します。組み込みのアラートポリシーは、アラートおよび再アラートの間隔が60分に設定されています。

ピーク接続セッション

- Directorのセッショントレンドビューで、接続済みセッションのピークを確認します。
- セッション負荷に対応する十分な容量があることを確認してください。
- 必要に応じて新しいマシンを追加する

ピーク切断セッション

- Directorのセッショントレンドビューで、ピーク時の切断済みセッションを確認します。
- セッション負荷に対応する十分な容量があることを確認します。
- 必要に応じて新しいマシンを追加します。
- 必要に応じて切断されたセッションをログオフします。

ピーク時の同時合計セッション数

- DirectorのDirectorセッショントレンドビューで、ピーク時の同時セッションを確認します。
- セッション負荷に対応する十分な容量があることを確認します。
- 必要に応じて新しいマシンを追加します。
- 必要に応じて、切断されたセッションをログオフします。

CPU

CPU 使用率の割合は、プロセスを含む VDA 上の全体的な CPU 消費量を示します。個々のプロセスによる CPU 使用率の詳細については、対応する VDA の ページで確認できます。

- **> >** に移動し、CPU を消費しているプロセスを特定します。プロセスレベルのリソース使用状況統計の収集を開始するには、プロセス監視ポリシーが有効になっていることを確認してください。
- 必要に応じてプロセスを終了します。
- プロセスを終了すると、保存されていないデータが失われます。
- すべてが期待どおりに機能している場合は、将来的に追加のCPUリソースを追加します。

> **注:**
>
> **リソース監視を有効にする**ポリシー設定は、VDAがインストールされているマシンでのCPUおよびメモリのパフォーマンスカウンターの監視に対して、デフォルトで許可されています。このポリシー設定が無効になっている場合、CPUおよびメモリの状態に関するアラートはトリガーされません。詳しくは、「監視ポリシー設定」を参照してください。
>
> **スマートポリシーの条件：**
>
> - **スコープ：** デリバリーグループ、マルチセッションOSスコープ
> - **しきい値:** 警告 - 80%、危険 - 90%

メモリ

メモリ使用率は、VDA上の全体的なメモリ消費量（プロセスによるものを含む）を示します。
個々のプロセスによるメモリ使用量に関する詳細な情報は、対応するVDAの**マシン詳細**ページから取得できます。

- **［マシン詳細］>［履歴使用率の表示］>［上位10プロセス］** に移動し、メモリを消費しているプロセスを特定します。プロセスレベルのリソース使用状況統計の収集を開始するには、プロセス監視ポリシーが有効になっていることを確認してください。
- 必要に応じてプロセスを終了します。
- プロセスを終了すると、保存されていないデータが失われます。
- すべてが期待どおりに機能している場合は、将来的に追加のメモリを追加します。

> **注:**
>
> **リソース監視を有効にする**ポリシー設定は、VDAがインストールされたマシン上のCPUおよびメモリのパフォーマンスカウンターを監視するために、デフォルトで許可されています。このポリシー設定が無効になっている場合、CPUおよびメモリの状態に関するアラートはトリガーされません。詳細については、「監視ポリシー設定」を参照してください。
>
> **スマートポリシー条件:**
>
> - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
> - **しきい値:** 警告 - 80%、重大 - 90%

接続失敗率

過去1時間の接続失敗の割合。

- 試行された接続の総数に対する総失敗数に基づいて計算されます。
- 構成ログから記録されたイベントについては、Directorの接続失敗トレンドビューを確認してください。
- アプリケーションまたはデスクトップに到達可能かどうかを判断します。

接続失敗数

過去1時間の接続失敗数。

- Director接続失敗トレンドビューで、構成ログから記録されたイベントを確認します。
- アプリケーションまたはデスクトップに到達可能かどうかを判断します。

ICA® RTT (平均)

平均ICAラウンドトリップ時間。

- ICA RTTの内訳についてCitrix ADMを確認し、根本原因を特定します。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、DirectorのユーザーDetailビューでICA RTTと遅延を確認し、ネットワークの問題か、アプリケーションまたはデスクトップの問題かを判断します。

ICA RTT (セッション数)

しきい値のICAラウンドトリップ時間を超えるセッション数。

- 高いICA RTTを持つセッション数についてCitrix ADMを確認します。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、ネットワークチームと協力して根本原因を特定します。

  スマートポリシーの条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 5セッション以上で300ミリ秒、重大 - 10セッション以上で400ミリ秒

ICA RTT (セッションの割合)

平均ICAラウンドトリップ時間を超えるセッションの割合。

- ICA RTTが高いセッションの数についてCitrix ADMを確認します。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、ネットワークチームと協力して根本原因を特定してください。

ICA RTT (ユーザー)

指定されたユーザーによって起動されたセッションに適用されるICAラウンドトリップ時間。ICA RTTが少なくとも1つのセッションでしきい値を超えた場合、アラートがトリガーされます。

失敗したマシン（シングルセッションOS）

失敗したシングルセッションOSマシンの数。失敗は、Directorのダッシュボードおよびフィルタービューに示されているように、さまざまな理由で発生する可能性があります。

- Citrix Scout診断を実行して根本原因を特定します。

  スマートポリシー条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 1、重大 - 2

失敗したマシン (マルチセッションOS)

失敗したマルチセッションOSマシンの数。失敗は、Directorのダッシュボードおよびフィルタービューに示されているように、さまざまな理由で発生する可能性があります。

- Citrix Scout診断を実行して根本原因を特定します。

  スマートポリシー条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 1、致命的 - 2

失敗したマシン (割合)

配信グループ内の失敗したシングルセッションおよびマルチセッションOSマシンの割合は、失敗したマシンの数に基づいて計算されます。このアラート条件では、配信グループ内の失敗したマシンの割合としてアラートしきい値を構成でき、30秒ごとに計算されます。 失敗は、Directorのダッシュボードおよびフィルタービューに示されているように、さまざまな理由で発生する可能性があります。Citrix Scout診断を実行して、根本原因を特定してください。詳細については、「ユーザーの問題のトラブルシューティング」を参照してください。

電源オンアクションの失敗と電源オフアクションの失敗

配信グループ内の電源オンアクションの失敗数と電源オフアクションの失敗数は、電源オンまたはオフに失敗した**電源管理対象マシン**の数に基づいて計算されます。このアラート条件では、配信グループ内で電源オンまたはオフに失敗した**電源管理対象マシン**の数としてアラートしきい値を構成でき、30分ごとに計算されます。

管理者は、高度なアラートポリシーでこれらのアラートに対して次のパラメーターを構成できます。

- トリガー元: 電源アクションをトリガーしたもの
- 失敗の理由: アクションが失敗した理由
- しきい値: ポリシーをトリガーするために電源アクションに失敗したマシンのしきい値の数
- サンプリング間隔: 失敗した電源アクションをチェックする必要がある間隔
- 再アラート間隔: アラートを再送信する必要がある時間

失敗は、Directorのダッシュボードおよびフィルタービューに示されているように、さまざまな理由で発生する可能性があります。Citrix Scout診断を実行して、根本原因を特定してください。詳細については、「ユーザーの問題のトラブルシューティング」を参照してください。

未登録マシン (割合)

マシンが再起動によって不安定になった場合、またはデリバリーコントローラーと仮想マシンの間に通信の問題がある場合、マシンは未登録と見なされます。**未登録マシン (割合)** は、未登録のシングルセッションおよびマルチセッションOSマシンの数に基づいて計算される、配信グループ内の未登録マシンの割合です。このアラート条件では、配信グループ内の未登録マシンの割合として、警告および致命的なしきい値を構成できます。再アラートの間隔を設定できます。**未登録マシン (割合)** の条件が満たされたときに通知を受け取るために、メールを追加することもできます。致命的または警告のしきい値を超えると、アラートとメールが生成されます。アラートは **Citrix Alerts**で確認できます。**未登録マシン (割合)** カテゴリと、必要な状態および時間でフィルターできます。

メールがある場合はCSV添付ファイルで、Webhookがある場合はJSONペイロードを介して、アラートの詳細を受け取ることもできます。

> **注記:**
>
> クリティカル値は警告値よりも大きくする必要があります。

> **ポリシー条件:**

- **スコープ**: シングルセッションOS、およびマルチセッションOSデリバリーグループ
- **しきい値**: 警告およびクリティカル

マシン稼働時間アラート

デリバリーグループ内のマシンの稼働時間は、デリバリーグループ内で電源がオンになっているマシンの1日あたりの時間数、1週間あたりの時間数、または1か月あたりの時間数に基づいて計算されます。このアラート条件を使用すると、デリバリーグループ内でマシンがオンになっている時間をアラートしきい値として構成できます。マシンの稼働時間アラートは、次の場合に機能します。

- 1日あたりの時間数 - マシンが1日あたりにオンになる時間数を指定でき、30分ごとに計算されます。設定できる1日あたりの最大時間数は24時間です。
- 1週間あたりの時間数 - マシンが1週間あたりにオンになる時間数を指定でき、6時間ごとに計算されます。設定できる1週間あたりの最大時間数は168時間です。
- 1か月あたりの時間数 - マシンが1か月あたりにオンになる時間数を指定でき、毎日1回計算されます。1か月あたりの最大時間数は720時間です。 設定できる再アラート間隔の最小値は60分です。警告およびクリティカルアラートセクションで、マシンの稼働時間のしきい値を超過するマシンの数を入力できます。任意のマシンに例外を追加することもできます。

たとえば、このアラートに5つのデリバリーグループが追加されており、最初のデリバリーグループと4番目のデリバリーグループでマシンの数が警告またはクリティカルしきい値を超えた場合、最初と4番目のデリバリーグループに対してアラートが個別にトリガーされます。

このアラートは、管理者がマシンの稼働時間を分析するのに役立ち、この分析に基づいて管理者はコストの最適化を支援できます。メールがある場合はCSV添付ファイルで、Webhookがある場合はJSONペイロードを介してアラートの詳細を受け取ることもできます。

平均ログオン時間

過去1時間に発生したログオンの平均ログオン時間。

- Directorダッシュボードでログオン期間に関する最新のメトリックを確認します。短期間に多くのユーザーがログオンすると、ログオン期間が長くなる可能性があります。
- ログオンのベースラインと内訳を確認して、原因を絞り込みます。詳細については、「ユーザーログオンの問題の診断」を参照してください。

  スマートポリシー条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 45秒、重大 - 60秒

ログオン時間（ユーザー）

過去1時間に発生した、指定されたユーザーのログオンのログオン時間。

ロード評価インデックス

過去5分間のロード評価インデックスの値。

- ピーク負荷（最大負荷）が発生している可能性のあるマルチセッションOSマシンについてDirectorを確認します。ダッシュボード（障害）とトレンドのロード評価インデックスレポートの両方を確認してください。

  スマートポリシーの条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 80%、重大 - 90%

Webhook を使用してアラートポリシーを構成する

電子メール通知とは別に、Webhook を使用してアラートポリシーを構成できます。

注: この機能には、Delivery Controllerバージョン7.11以降が必要です。

PowerShell コマンドレットを使用して、HTTP コールバックまたは HTTP POST でアラートポリシーを構成できます。これらは Webhook をサポートするように拡張されています。

新しい Octoblu ワークフローの作成と、対応する Webhook URL の取得については、Octoblu Developer Hub を参照してください。

新しいアラートポリシーまたは既存のポリシーの Webhook URL を構成するには、次の PowerShell コマンドレットを使用します。

Webhook URLを使用して新しいアラートポリシーを作成します:

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -Description
<Policy description> -Enabled $true -Webhook <Webhook URL>
```

既存のアラートポリシーに Webhook URL を追加する:

```
Set-MonitorNotificationPolicy - Uid <Policy id> -Webhook <Webhook URL>
```

PowerShellコマンドに関するヘルプについては、PowerShellヘルプを使用してください。例：

```
Get-Help  <Set-MonitorNotificationPolicy>
```

アラートポリシーから生成された通知は、Webhook URLへのPOST呼び出しでWebhookをトリガーします。POSTメッセージには、通知情報がJSON形式で含まれています。

```
{"NotificationId" : \<Notification Id\>,



"Target" : \<Notification Target Id\>,



"Condition" : \<Condition that was violated\>,



"Value" : \<Threshold value for the Condition\>,



```

```
"Timestamp": \<Time in UTC when notification was generated\>,

"PolicyName": \<Name of the Alert policy\>,

"Description": \<Description of the Alert policy\>,

"Scope" : \<Scope of the Alert policy\>,

"NotificationState": \<Notification state critical, warning, healthy or dismissed\>,

"Site" : \<Site name\>}
```

アラートの一括解除

この機能は、管理者のアラート管理プロセスを最適化し、柔軟性を提供し、アラート疲労を軽減します。管理者は、時間、種類、またはカテゴリに基づいてアラートを一括で解除できるため、メンテナンス中やハイパーバイザーなどの環境を扱う際のアラート管理が簡素化されます。

アラートの一括解除は、管理者がワークロードを効率的に管理し、大量のアラートに圧倒されるのを防ぐのに役立ちます。

アラートを一括解除する手順

1. **アラート** > **Citrixアラート**タブに移動します。アラートが表示されます。

   「一括アラート」(/en-us/citrix-virtual-apps-desktops/2411/media/bulk-alert.png)

2. **ソース**、**カテゴリ**、**状態**、または**期間**からオプションを選択して、解除したいアラートをフィルタリングします。特定のアラートが表示されます。
3. 特定のアラートの横にあるチェックボックス、または上部にあるチェックボックスを選択して、すべてのアラートを選択します。

4. **Dismiss** をクリックします。アラートの解除を確認する通知が表示されます。
5. **Yes** をクリックします。選択したアラートは *解除済み* としてマークされ、アラートのステータスがそれに応じて更新されます。

PowerShell SDK を使用した Webhook の構成

PowerShell SDK を使用した Webhook 構成機能により、管理者は Webhook プロファイルを作成、変更、削除、および一覧表示できます。この機能は、ヘッダー、認証タイプ、コンテンツタイプ、ペイロード、および Webhook URL の指定を可能にすることで、Webhook の構成に柔軟性をもたらします。

> **注：**
>
> サポートされているペイロード形式はテキストであり、エンドユーザーは Webhook でテキストを有効にする必要があります。
>
> 最新のペイロード形式は次のとおりです。

```
{"text": "This is a message from a Webex incoming webhook."}
```

Webhook の作成

Webhook プロファイルを作成するには、次のサンプル PowerShell コマンドを使用できます。

認証ヘッダーなしで Webhook を作成するには：

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")


$payloads = '{ "text": "$PAYLOAD" }'


$url = "<Fill this field with the required URL>"
```

```
Add-MonitorWebhookProfile -Name "profile_slack" -Description "webhook
profile for slack" -Url $url -Headers $headers -PayloadFormat $payloads
```

認証ヘッダー付きで Webhook を作成するには：

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")

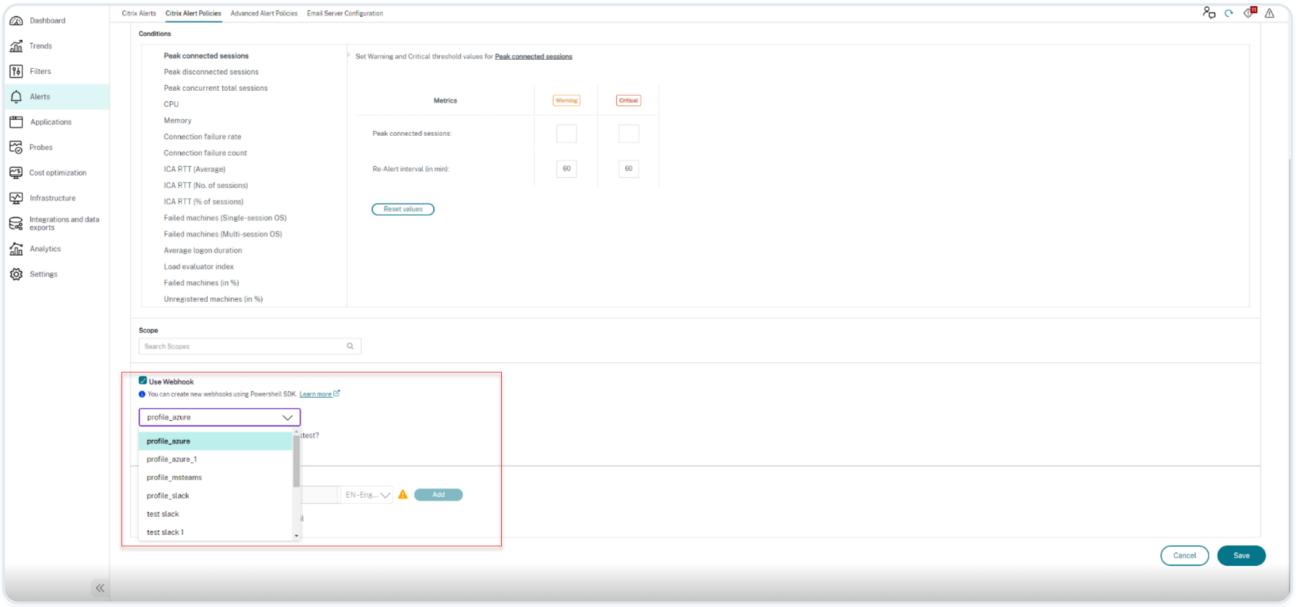

$headers.Add("Authorization", "Basic <Fill this field with the
authorization token>")


$payloads = '{ "text": "$PAYLOAD" }'


$url = "<Fill this field with the required URL>"


Add-MonitorWebhookProfile -Name "profile_azure" -Description "webhook
profile for azure function with Authentication" -Url $url -Headers
$headers -PayloadFormat $payloads
```

プロファイルが作成されたら、データベースで確認できます。また、新しく作成された Webhook プロファイルは、**Citrix Alerts** ページで見つけることができます。



Webhook プロファイルの更新

Webhook プロファイルを更新するには、次のサンプル PowerShell コマンドを使用できます。

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")


$payloads = '{ "text": "$PAYLOAD" }'


$url =  "<Fill this field with the required URL>"


Set-MonitorWebhookProfile -Uid 1  -Name "profile_slack_citrix"
-Description "webhook profile for citrix slack" -Url $url -Headers
$headers -PayloadFormat $payloads
```

すべてのWebhookプロファイルの一覧を取得する

利用可能なすべてのWebhookプロファイルの一覧を取得するには、以下のPowerShellコマンドのサンプルを使用できます。

```
Get-MonitorWebhookProfile



Get-MonitorWebhookProfile -Name 'profile_msteams'



Get-MonitorWebhookProfile -Uid 1
```

Webhookプロファイルを削除する

Webhookプロファイルを削除するには、以下のPowerShellコマンドのサンプルを使用できます。

```
Remove-MonitorWebhookProfile -Uid 1
```

注:

Webhookプロファイルがいずれかのポリシーにマッピングされている場合、削除できません。回避策として、まずポリシーからWebhookマッピングを削除する必要があります。

Webhookプロファイルを含むポリシーを作成する

Webhookプロファイルを含むポリシーを作成するには、以下のPowerShellコマンドのサンプルを使用できます。

```
New-MonitorNotificationPolicy -Name "Policy1" -Description "Policy
Description" -Enabled $true -WebhookProfileId 1
```

Webhookプロファイルを含むポリシーを更新する

Webhookプロファイルを含むポリシーを更新するには、以下のPowerShellコマンドのサンプルを使用できます。

```
$Policy = Set-MonitorNotificationPolicy -Uid 1 -WebhookProfileId 1
```

ポリシーからWebhookマッピングを削除する

ポリシーからWebhookプロファイルを削除するには、以下のPowerShellコマンドのサンプルを使用できます。

```
$Policy = Set-MonitorNotificationPolicy -Uid 1 -WebhookProfileId 0
```

Webhookプロファイルをテストする

Webhookプロファイルをテストするには、以下のPowerShellコマンドのサンプルを使用できます。

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")


$headers.Add("Authorization", "Basic <Fill this with authorization
token>")

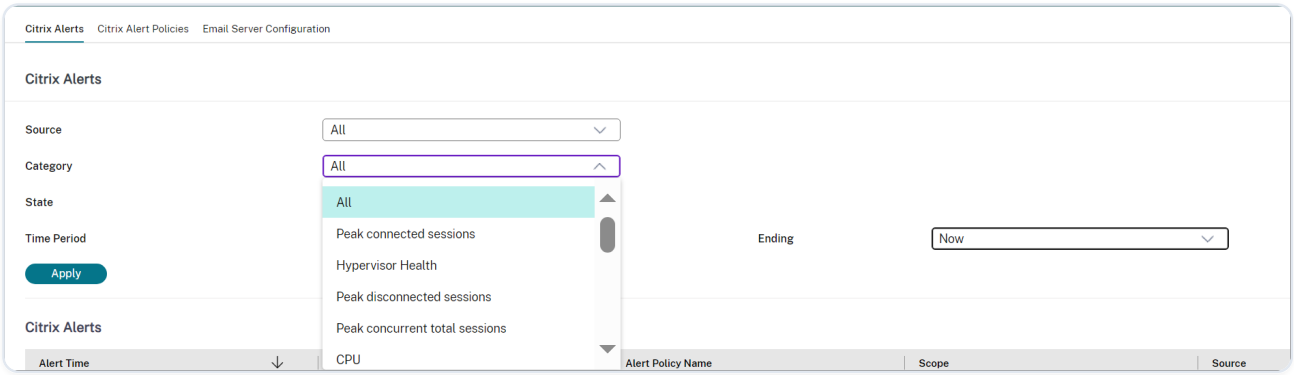

$payloads = '{ "text": "$PAYLOAD" }'


$url ="<Fill this field with the required URL>"


Test-MonitorWebhookProfile -Url $url -Headers $headers -PayloadFormat
$payloads
```

ハイパーバイザーアラートの監視

Directorはハイパーバイザーの健全性を監視するためにアラートを表示します。XenServer®およびVMware vSphereからのアラートは、ハイパーバイザーのパラメーターと状態の監視に役立ちます。ハイパーバイザーへの接続ステータスも監視され、ホストのクラスターまたはプールが再起動されたり利用できなくなったりした場合にアラートが提供されます。



ハイパーバイザーアラートを受信するには、Web Studioでホスティング接続が作成されていることを確認してください。詳細については、接続とリソースを参照してください。これらの接続のみがハイパーバイザーアラートのために監視されます。

これらのアラートは、しきい値に達するか、または超過すると表示されます。ハイパーバイザーアラートは次のとおりです。

- 致命的—ハイパーバイザーアラームポリシーの致命的なしきい値に達したか、または超過した
- 警告—ハイパーバイザーアラームポリシーの警告しきい値に達したか、または超過した
- 却下済み—アラートがアクティブなアラートとして表示されなくなった

ハイパーバイザーアラート表示(/en-us/citrix-virtual-apps-desktops/2411/media/hypervisor_alerts_display.png)

この機能には、Delivery Controllerバージョン7 1811以降が必要です。Directorの古いバージョンをサイト7 1811以降で使用している場合、ハイパーバイザーアラートの数のみが表示されます。アラートを表示するには、Directorをアップグレードする必要があります。

次の表は、ハイパーバイザーアラートのさまざまなパラメーターと状態について説明しています。

アラート	サポートされているハイパーバイザー	トリガー元	条件	構成
CPU使用率	ゼノサーバー、ブイエムウェア ブイスフィア	ハイパーバイザー	CPU使用率アラートのしきい値に達したか、超過した	アラートのしきい値はハイパーバイザーで構成する必要があります。
メモリ使用率	ゼノサーバー、ブイエムウェア ブイスフィア	ハイパーバイザー	メモリ使用率アラートのしきい値に達したか、超過した	アラートのしきい値はハイパーバイザーで構成

アラート	サポートされているハイパーバイザー	トリガー元	条件	構成
				する必要があります。
ネットワーク使用率	ゼノサーバー、ブイエムウェア ブイスフィア	ハイパーバイザー	ネットワーク使用率アラートのしきい値に達したか、超過した	アラートのしきい値はハイパーバイザーで構成する必要があります。
ディスク使用量	ヴイエムウェア vSphere	ハイパーバイザー	ディスク使用量アラートのしきい値に達したか、超過しました	アラートのしきい値はハイパーバイザーで構成する必要があります。
ホスト接続または電源状態	ヴイエムウェア vSphere	ハイパーバイザー	ハイパーバイザーホストが再起動されたか、利用できません	アラートは VMware vSphereに組み込まれています。追加の構成は不要です。
ハイパーバイザー接続が利用できません	XenServer、ヴイエムウェア vSphere	デリバリーコントローラー	ハイパーバイザー（プールまたはクラスター）への接続が失われたか、電源が切られたか、再起動されました。このアラートは、接続が利用できない間、1時間ごとに生成されます。	アラートは Delivery Controllerに組み込まれています。追加の構成は不要です。

注:

アラートの設定に関する詳細については、Citrix XenCenter Alertsを参照するか、VMware vCenter Alertsのドキュメントを確認してください。

メール通知設定は、**Citrix Alerts Policy > Site Policy > Hypervisor Health**で構成できます。ハイパーバイザーアラートポリシーのしきい値条件は、Directorからではなく、ハイパーバイザーからのみ構成、編集、無効化、または削除できます。ただし、メール設定の変更やアラートの解除はDirectorで行うことができます。役割にインフラストラクチャの監視が含まれていない場合は、アラートを無効にできます。

重要:

- ハイパーバイザーによってトリガーされたアラートは、Directorでフェッチされ表示されます。ただし、ハイパーバイザーアラートのライフサイクル/状態の変更はDirectorには反映されません。
- ハイパーバイザーコンソールで正常、解除、または無効化されたアラートは、Directorに表示され続け、明示的に解除する必要があります。
- Directorで解除されたアラートは、ハイパーバイザーコンソールでは自動的に解除されません。

アプリケーション使用状況の監視

現在、Citrix Directorは公開アプリケーションの使用状況を監視するのに役立ちます。この機能はダッシュボードにあり、厳選されたチャートが含まれています。これらのチャートは、IT管理者またはアプリケーション管理者が、どのアプリケーションが頻繁に使用されているか、およびその使用状況の程度を把握するのに役立ちます。

注：

この機能は、プラチナライセンスサイトでのみ利用できます。

この機能を使用すると、管理者はどの公開アプリケーションが最も使用されているかを確認できます。このデータを使用して、管理者は使用状況の程度をより深く掘り下げることがで

きます。管理者は、過去24時間における人気のあるアプリの詳細を、以下のデータポイントで分析できます。

- アプリケーションの総数 - 企業のサイト内のすべてのユーザーが使用しているアプリケーションの総数を特定します。
- 個別ユーザー数による最も使用されているアプリケーション - ユニークユーザーの総数に基づいて上位10のアプリを特定します。
- アプリケーション起動の総数による最も使用されているアプリケーション - アプリケーション起動の総数に基づいて上位10のアプリを特定します。
- ピーク時の同時実行アプリインスタンス数上位 - 各アプリケーションの使用状況における同時実行インスタンスの最大数に基づいて上位10のアプリを特定します。この情報は、リストされているアプリケーションの最大需要を示します。

このチャートはダッシュボードページの下部に表示されます。ただし、画面上部の**Check it out**をクリックすると、直接チャートにアクセスできます。

アプリケーション監視(/en-us/citrix-virtual-apps-desktops/2411/media/application-monitoring.png)

また、**View all app usage**をクリックして、単一のアプリの詳細を表示することもできます。このリンクをクリックすると、**Trends** > **Capacity Management** > **Hosted Application Usage**ページが開きます。

このチャートは、アプリの使用状況を視覚的に表現します。また、グラフにカーソルを合わせると、選択したデータポイントのそれぞれの絶対数が表示されます。チャート上の任意のデータポイントをクリックすると、特定のアプリ名が選択された状態で**Trends** > **Capacity Management** > **Hosted Application Usage**ページが開きます。このデータは、企業のシステムに存在するすべてのアプリに対する比較値を示すものです。データポイントの絶対値も、同じホバー内に個別に記載されています。

使用頻度の低い、および未使用の公開アプリレポート

大規模なCitrix Virtual Apps and Desktops™環境では、利用されていないアプリケーションが多数存在することがよくあります。環境を最適化するために、**Applications**ページでは、組織内のアプリケーション使用パターンを理解し、リソース割り当てとコスト削減を改善するためのデータに基づいた意思決定を行うのに役立つ追加のメトリックが提供されるようになりました。

主な機能

- **詳細な使用状況情報:** 各アプリケーションの過去30日間の個別ユーザー数、合計起動回数、ピーク時の同時実行インスタンス数、および経時的な個別ユーザー数の傾向グラフを表示します。

- **データ重視:** 過去7日間、30日間、または90日間のアプリケーション使用パターンを分析し、アプリケーションの必要性を評価します。90日間のデータは四半期分のデータを提供し、アプリケーションの使用状況が変動するか一貫しているかを観察できるため、90日間のデータを表示することをお勧めします。X軸の日付は、組織のイベントと使用傾向を関連付け、減少が予想されたものかどうかを判断するのに役立ちます。このデータにより、管理者は不要なアプリケーションを排除することで効率的な環境を維持できます。
- **最適化:** 公開されているアプリケーションの総数、ほとんど使用されていないアプリケーション、および未使用のアプリケーションを特定して、Citrix展開を最適化します。
- **実用的なデータ:** データに基づいた意思決定を行い、アプリケーション管理を支援して、リソース割り当てとライセンス管理を最適化します。
- **データのエクスポート:** 詳細な分析のために、データをPDFまたはCSV形式でエクスポートします。

> **注:**
>
> 現在、この機能強化には、公開されているアプリケーション（Citrix Workspace™アプリではデスクトップアプリと呼ばれます）のみが含まれています。

要件

- Delivery Controller バージョン 7.16 以降
- VDA バージョン 7.15 以降

アプリケーション使用状況の詳細の表示

1. ダッシュボードの**セクションにある**リンクをクリックします。

   または、,

   ****タブをクリックします。

   タブ(/en-us/citrix-virtual-apps-desktops/2411/media/dir-app-analytics.png)
2. 目的のデリバリーグループを選択します。
3. 必要な期間を選択します。(注: 最適な分析のため、デフォルトは過去90日間です。)

   次の情報が表示されます。

   - **公開済みアプリケーションの合計:** 公開済みアプリケーションの合計数を表示します。

- **最も使用頻度の低いもの:** 選択した期間でユニークユーザーが最も少ないアプリを表示します。計算は次のように行われます。

  a. **1日のユーザー数:** 各アプリのユニークユーザー数が毎日カウントされます。

  b. **1日のピーク使用量:** 各アプリの1日のユーザー数の最高値が特定されます。

  c. **全体で最も高い使用量:** 選択した期間における各アプリのユーザー数の最高値が決定されます。

  d. **昇順:** アプリは、最も低いユーザー数のアプリから始まり、全体で最も高いユーザー数に基づいて昇順でリストされます。

  > **注:**
  >
  > 分析期間として過去90日間を選択することをお勧めします。この期間は四半期分のデータを提供し、アプリの使用パターンを包括的に把握できます。ただし、7日間および1か月でフィルタリングするオプションも利用できます。

- **未使用:** 使用量がゼロのアプリケーションが、アプリ名、デリバリーグループ、および状態 (有効または無効) とともにリストされます。この情報は、最適化するアプリケーションを特定するのに役立ちます。

4. **最も使用頻度の低い**カテゴリからアプリを選択して、以下を含む詳細な使用状況情報を表示します。

   - **過去30日間のユニークユーザー数:** 過去30日間にアプリにアクセスしたユニークユーザーの数を表示します。7日間でフィルタリングした場合、このメトリックは、選択したアプリのその7日間のユニークユーザー数を表示します。

   > **注：**
   >
   > 90日を選択した場合でも、このメトリックは過去30日間のデータのみを表示します。

   - **合計インスタンス数：** アプリが起動された回数を表示します。
   - **ピーク同時実行インスタンス数：** 同時に実行されているインスタンスの最大数を表示します。

- **トレンドチャート：** 選択したアプリの経時的なユニークユーザー数を示すトレンドチャートを表示します。**詳細を表示**をクリックすると、**キャパシティ管理 > ホスト型アプリケーション使用状況**セクションで詳細情報が表示されます。

トレンドチャートの使用方法

トレンドチャートは使用パターンを示し、選択した期間における傾向や使用量の少ない期間または多い期間を特定するのに役立ちます。X軸は日数を表し、Y軸は経時的なユニークユーザー数を表します。これらのメトリックと使用パターングラフを分析することで、管理者はCitrix Virtual Apps and Desktops環境を自信を持って最適化できます。

トレンドチャートは以下の方法で使用できます。

- **データポイントにカーソルを合わせる：** 選択した期間のユニークユーザー数を表示します。
- **傾向の表示：** 使用パターンを特定し、アプリの使用状況が一貫しているか、一時的な急増にすぎないかを判断します。このチャートは、管理者が従業員の活動を監視し、潜在的な問題や改善領域を特定するのに役立ちます。たとえば、従業員が休暇を取ると、その期間はアプリケーションの使用がない場合があります。従業員が戻ると、アプリケーションの使用量が増加します。期間のデフォルトフィルターは90日で、管理者がこれらの計算を行うのに役立ちます。
- **詳細の表示：** 日付と対応するユニークユーザー数を表示します。
- **フィルターオプション：** 異なる期間フィルターオプションを選択して、対応するデータを表示します。

障害のトラブルシューティングのためにデータをフィルターする

ダッシュボードの数値をクリックするか、フィルターメニューから定義済みフィルターを選択すると、選択したマシンまたは障害タイプに基づいてデータを表示するフィルタービューが開きます。

定義済みフィルターは編集できませんが、定義済みフィルターをカスタムフィルターとして保存し、後で変更できます。また、すべてのデリバリーグループにわたるマシン、接続、セッション、およびアプリケーションインスタンスのカスタムフィルタービューを作成することもできます。

1. ビューを選択します。

    - **マシン**。シングルセッションOSマシンまたはマルチセッションOSマシンを選択します。これらのビューには、構成されているマシンの数が表示されます。マルチセッションOSマシンタブには、パフォーマンスカウンターの分布を示すロード評価インデックスと、リンクにカーソルを合わせると表示されるセッション数のツールヒントも含まれています。

- **セッション**。セッションを、過去60分、過去24時間、過去7日間、またはカスタム期間など、異なる期間でフィルターします。セッションビューからセッション数を確認することもできます。アイドル時間測定を使用して、しきい値期間を超えてアイドル状態になっているセッションを特定します。**関連ユーザー**をクリックすると、そのユーザーのアクティビティマネージャーが開きます。**エンドポイント**名をクリックすると、そのエンドポイントのアクティビティマネージャーが開きます。**詳細の表示**をクリックすると、それぞれ**ユーザーの詳細**ページまたは**エンドポイントの詳細**ページが開きます。詳しくは、「ユーザーの詳細」を参照してください。
- **接続**。接続を、過去60分、過去24時間、過去7日間、またはカスタム期間など、異なる期間でフィルターします。
- **アプリケーションインスタンス**。アプリケーションインスタンスを、過去60分、過去24時間、過去7日間、またはカスタム期間など、異なる期間でフィルターします。このビューには、サーバーおよびシングルセッションOSのVDA上のすべてのアプリケーションインスタンスのプロパティが表示されます。マルチセッションOSのVDA上のアプリケーションインスタンスでは、セッションアイドル時間測定が利用可能です。

> **注：**
>
> Windows 10 1809コンピューターにインストールされているVDAでデスクトップセッションを起動した場合、Directorのアクティビティマネージャーは、Microsoft EdgeとOfficeが実際にはバックグラウンドでのみ実行されているにもかかわらず、アクティブに実行中のアプリケーションとして表示することがあります。

2. **フィルター条件**で、基準を選択します。
3. 必要に応じて、各ビューの追加タブを使用してフィルターを完了します。
4. 必要に応じて、追加の列を選択して、さらにトラブルシューティングを行います。
5. フィルターを保存して名前を付けます。
6. 複数のDirectorサーバーからフィルターにアクセスするには、それらのサーバーからアクセス可能な共有フォルダーにフィルターを保存します。
   - 共有フォルダーには、Directorサーバー上のアカウントに対する変更権限が必要です。
   - Directorサーバーは、共有フォルダーにアクセスするように構成する必要があります。構成するには、**IIS Manager**を実行します。**Sites \> Default Web Site \> Director\ > Application Settings**で、**Service.UserSettingsPath**設定を共有フォルダーのUNCパスを反映するように変更します。

7. 後でフィルターを開くには、**Filters**メニューからフィルターの種類（Machines、Sessions、Connections、またはApplication Instances）を選択し、保存されたフィルターを選択します。
8. **Export**をクリックして、データをCSV形式ファイルにエクスポートします。最大100,000レコードのデータをエクスポートできます。この機能は、Delivery Controller™バージョン1808以降で利用可能です。
9. 必要に応じて、**Machines**または**Connections**ビューでは、フィルターされたリストで選択したすべてのマシンに対して電源制御を使用します。Sessionsビューでは、セッション制御またはメッセージ送信オプションを使用します。
10. **Machines**および**Connections**ビューで、失敗したマシンまたは接続の**Failure Reason**をクリックすると、障害の詳細な説明と、障害のトラブルシューティングに推奨されるアクションが表示されます。マシンおよび接続の障害理由と推奨されるアクションについては、Citrix Director failure reasons and troubleshootingを参照してください。
11. **Machines**ビューで、マシン名のリンクをクリックすると、対応する**Machine Details**ページに移動します。このページには、マシンの詳細が表示され、電源制御が提供され、CPU、メモリ、ディスク監視、およびGPU監視グラフが表示されます。また、**View Historical Utilization**をクリックすると、マシンのリソース使用率の傾向を確認できます。詳細については、Troubleshoot machinesを参照してください。
12. **Application Instances**ビューで、しきい値期間より長い**Idle Time**に基づいて並べ替えまたはフィルター処理を行います。終了するアイドル状態のアプリケーションインスタンスを選択します。アプリケーションインスタンスのログオフまたは切断により、同じセッション内のすべてのアクティブなアプリケーションインスタンスが終了します。詳細については、Troubleshoot applicationsを参照してください。Application Instancesフィルターページと Sessionsフィルターページでのアイドル時間測定は、Director、Delivery Controllers、および VDAがバージョン7.13以降の場合に利用可能です。

注:

Web Studioでは、異なるユーザーまたはユーザーグループに対して複数のDesktop Assignment Rules (DAR) をデリバリーグループ内の単一のVDAに割り当てることができます。StoreFront™は、ログインユーザーのDARに従って、対応する表示名を持つ割り当てられたデスクトップを表示します。ただし、DirectorはDARをサポートしておらず、ログインユーザーに関係なく、デリバリーグループ名を使用して割り当てられたデスクトップを表示します。その結果、Directorで特定のデスクトップをマシンにマッピングすることはできません。StoreFrontに表示される割り当てられたデスクトップをDirectorに表示されるデリバリーグループ名にマッピングするには、次のPowerShellコマンドを使用します。

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq "\<Name
on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property Name, Uid
```

サイト全体の履歴トレンドを監視する

トレンドビューでは、以下のパラメーターについて、各サイトの履歴トレンド情報にアクセスできます。

- セッション
- 接続障害
- マシン障害
- ログオンパフォーマンス
- 負荷評価
- キャパシティ管理
- マシン使用状況
- リソース使用率
- 各サイトのネットワーク分析。

この情報を見つけるには、**トレンド**メニューをクリックします。

ズームイン・ドリルダウン機能を使用すると、期間を拡大表示（グラフのデータポイントをクリック）したり、トレンドに関連する詳細を表示するためにドリルダウンしたりすることで、トレンドチャートをナビゲートできます。この機能により、誰が、または何が影響を受けているかの詳細をよりよく理解できます。

各グラフのデフォルトのスコープを変更するには、データに別のフィルターを適用します。

履歴トレンド情報が必要な期間を選択します。期間の利用可能性は、Directorの展開によって次のように異なります。

- 最大1年間 (365日間) のトレンドレポートは、Premiumライセンスサイトで利用できます。
- 最大1か月間 (31日間) のトレンドレポートは、Advancedライセンスサイトで利用できます。
- 最大7日間のトレンドレポートは、PremiumおよびAdvanced以外のライセンスサイトで利用できます。

注:

- すべてのDirector展開において、期間が「先月」（**現在終了**）以下に設定されている場合、セッション、障害、ログオンパフォーマンスのトレンド情報はグラフとテーブルとして利用できます。期間がカスタム終了日を指定した「先月」または「昨年」として選択されている場合、トレンド情報はグラフとして利用でき、テーブルとしては利用できません。
- Monitor Serviceのグルーミング保持値がトレンドデータの可用性を制御します。デフォルト値はデータ粒度と保持で確認できます。Premiumライセンスサイトのお客様は、グルーミング保持を希望する保持日数に変更できます。
- IIS Managerの以下のパラメーターは、選択可能なカスタム終了日の範囲を制御します。ただし、選択された日付のデータ可用性は、測定対象の特定のメトリックに対するグルーミング保持設定によって異なります。

パラメーター	デフォルト値
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

利用可能なトレンド

セッションの傾向を表示: 「**セッション**」タブから、デリバリーグループと期間を選択して、同時セッション数に関する詳細情報を表示します。

セッションの自動再接続列には、セッション内の自動再接続の数が表示されます。自動再接続は、セッションの信頼性ポリシーまたはクライアント自動再接続ポリシーが有効な場合に有効になります。エンドポイントでネットワークの中断が発生した場合、次のポリシーが適用されます。

- セッションの信頼性が有効になり（デフォルトで3分間）、Citrix Receiver™またはCitrix Workspace™アプリがVDAへの接続を試行します。
- クライアント自動再接続が3分から5分の間に有効になり、クライアントがVDAへの接続を試行します。

両方の再接続がキャプチャされ、ユーザーに表示されます。この情報は、再接続が発生してからDirector UIに表示されるまでに最大5分かかる場合があります。

自動再接続情報は、中断のあるネットワーク接続の表示とトラブルシューティングに役立ちます。また、シームレスなエクスペリエンスを持つネットワークも分析します。フィルターで選択した特定のデリバリーグループまたは期間の再接続数を表示できます。ドリルダウンでは、セッションの信頼性またはクライアント自動再接続、タイムスタンプ、エンドポイントIP、Workspaceアプリがインストールされているマシンのエンドポイント名などの追加情報が提供されます。

デフォルトでは、ログはイベントタイムスタンプの降順でソートされます。この機能は、Windows向けCitrix Workspaceアプリ、Mac向けCitrix Workspaceアプリ、Windows向けCitrix Receiver、およびMac向けCitrix Receiverで利用できます。この機能には、Delivery Controller™ バージョン7 1906以降、およびVDA 1906以降が必要です。

セッションの再接続の詳細については、「セッション」を参照してください。

ポリシーの詳細については、「クライアント自動再接続ポリシー設定」および「セッションの信頼性ポリシー設定」を参照してください。

自動再接続データがDirectorに表示されない場合があります。その理由は次のとおりです。

- WorkspaceアプリがVDAに自動再接続データを送信していません。
- VDAがモニターサービスにデータを送信していません。
- Delivery Controllerは、対応するセッションがない可能性があるため、VDAペイロードを破棄します。

> **注:**
>
> Citrix Gateway の特定のポリシーが設定されている場合、クライアント IP アドレスが正しく取得されないことがあります。

> **接続障害の傾向を表示:** タブから、接続、マシンタイプ、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のユーザー接続障害に関する詳細情報を含むグラフを表示します。

マシン障害の傾向を表示: タブまたは タブから、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のマシン障害に関する詳細情報を含むグラフを表示します。

ログオンパフォーマンスの傾向を表示: タブから、デリバリーグループと期間を選択して、サイト全体のユーザーログオン時間の期間と、ログオン数がパフォーマンスに影響するかどうかに関する詳細情報を含むグラフを表示します。このビューには、ブローカー処理時間や VM 起動時間など、ログオンフェーズの平均期間も表示されます。 このデータはユーザーログオン専用であり、

切断されたセッションから再接続しようとしているユーザーは含まれません。 グラフの下の表には、ユーザーセッションごとのログオン期間が表示されます。表示する列を選択し、任意の列でレポートを並べ替えることができます。これらのレポートを .CSV ファイルにエクスポートすることもできます。詳細については、「ユーザーログオンの問題の診断」を参照してください。

負荷評価の傾向を表示: タブから、マルチセッション OS マシン間で分散される負荷に関する詳細情報を含むグラフを表示します。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のマルチセッション OS マシン、マルチセッション OS マシン (デリバリーグループ内のマルチセッション OS マシンが選択されている場合にのみ利用可能)、および範囲が含まれます。

ホスト型アプリケーションの使用状況を表示: この機能の可用性は、組織のライセンスによって異なります。 タブから、 タブを選択します。デリバリーグループと期間を選択して、ピーク時の同時使用状況を示すグラフと、アプリケーションベースの使用状況を示す表を表示します。 表から、特定のアプリケーションを選択して、詳細と、そのアプリケーションを使用している、または使用したユーザーのリストを表示できます。

シングルセッションおよびマルチセッション OS の使用状況を表示: ビューには、サイト別およびデリバリーグループ別のシングルセッション OS の使用状況が表示されます。 を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、ユーザーごとの使用状況が表示されます。 ビューには、サイト別、デリバリーグループ別、およびマシン別のマルチセッション OS の使用状況も表示されます。 を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、マシンごとおよびユーザーごとの使用状況が表示されます。マシンが選択されている場合、ユーザーごとの使用状況が表示されます。

仮想マシンの使用状況を表示: タブから、 を選択して、VM 使用状況のリアルタイムビューを取得し、サイトのキャパシティニーズを迅速に評価できるようにします。 シングルセッション OS の可用性 - サイト全体または特定のデリバリーグループの可用性別に、シングルセッション OS マシン (VDI) の現在の状態を表示します。 マルチセッション OS の可用性 - サイト全体または特定のデリバリーグループの可用性別に、マルチセッション OS マシンの現在の状態を表示します。

コスト最適化によるマシン使用状況の可視性を高めるには、表示されるバナーの以下のリンクをクリックします。

- 推定節約額 - このリンクをクリックすると、**コスト最適化**ページの**推定節約額**セクションに移動し、すべてのデリバリーグループの詳細が表示されます。
- 節約レポート - このリンクをクリックすると、**コスト最適化**ページの**節約レポート**セクションに移動し、すべてのデリバリーグループの詳細が表示されます。

注:

利用可能なカウンターに表示されるマシンの数には、メンテナンスモードのマシンが含まれます。

リソース使用率の表示: **リソース使用率**タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択すると、CPUとメモリの使用状況、および各VDIマシンのIOPSとディスク待機時間に関する過去の傾向データが得られ、キャパシティプランニングの改善に役立ちます。 この機能には、Delivery ControllerおよびVDA **バージョン 7.11** 以降が必要です。 グラフには、平均CPU、平均メモリ、平均IOPS、ディスク待機時間、およびピーク時の同時セッションのデータが表示されます。マシンにドリルダウンして、CPUを消費している上位10プロセスのデータとグラフを表示できます。

デリバリーグループと期間でフィルターします。CPU、メモリ使用量、およびピーク時の同時セッションのグラフは、過去 2 時間、24 時間、7 日間、月、年で利用できます。平均 IOPS とディスク待機時間のグラフは、過去 24 時間、月、年で利用できます。バナーの リンクをクリックすると、コスト最適化によるマシン使用状況の可視性が向上します。このリンクをクリックすると、 ページの タブに移動し、 タブから選択したデリバリーグループの詳細が表示されます。

注:

- 監視ポリシー設定の は、 ページの テーブルでデータを収集して表示するために に設定する必要があります。このポリシーは、デフォルトで に設定されています。すべてのリソース使用率データはデフォルトで収集されます。これは、 ポリシー設定を使用して無効にできます。グラフの下の表には、マシンごとのリソース使用率データが表示されます。詳しくは、「監視ポリシー設定」を参照してください。
- 平均 IOPS は日次平均を示します。ピーク IOPS は、選択した期間の IOPS 平均の最高値として計算されます（IOPS 平均とは、VDA でその時間に収集された IOPS の時間平均です）。
- マシンのドリルダウンでは、平均 CPU または平均メモリ使用量が 1% を超えるプロセスが一覧表示されます。これは、10 未満のプロセスが一覧表示される場合があることを意味します。

ネットワーク分析データの表示: この機能の可用性は、組織のライセンスと管理者権限によって異なります。この機能には、Delivery Controller **バージョン 7.11** 以降が必要です。

タブから、ネットワーク分析を監視します。これにより、ネットワークのユーザー、アプリケーション、デスクトップのコンテキストビューが提供されます。この機能により、Director は Citrix ADM の HDX Insight レポートを通じて、展開における ICA トラフィックの詳細な分析を提供します。詳しくは、「ネットワーク分析の構成」を参照してください。

アプリケーション障害の表示: タブには、VDA 上で公開されているアプリケーションに関連する障害が表示されます。

この機能には、Delivery Controller および VDA **バージョン 7.15** 以降が必要です。Windows Vista 以降を実行するシングルセッション OS VDA と、Windows Server 2008 以降を実行するマルチセッション OS VDA がサポートされています。 詳しくは、「過去のアプリケーション障害監視」を参照してください。

デフォルトでは、マルチセッション OS VDA からのアプリケーション障害のみが表示されます。監視ポリシーを使用して、アプリケーション障害の監視を設定できます。詳しくは、「監視ポリシー設定」を参照してください。

プローブ結果の表示: タブには、構成ページでプローブ用に構成されたアプリケーションとデスクトップのプローブ結果が表示されます。ここでは、障害が発生した起動の段階が記録されます。

詳しくは、「アプリケーションおよびデスクトップのプローブ」を参照してください。

カスタマイズされたレポートの作成: タブは、監視データベースからのリアルタイムデータと履歴データを含むカスタムレポートを表形式で生成するためのユーザーインターフェイスを提供します。

この機能には、Delivery Controller **バージョン 7.12** 以降が必要です。

以前に保存したカスタムレポートクエリのリストから、**実行してダウンロード**をクリックしてレポートをCSV形式でエクスポートしたり、**ODataをコピー**をクリックして対応するODataクエリをコピーして共有したり、**編集**をクリックしてクエリを編集したりできます。 マシン、接続、セッション、またはアプリケーションインスタンスに基づいてカスタムレポートクエリを作成できます。マシン、デリバリーグループ、期間などのフィールドに基づいてフィルター条件を指定します。カスタムレポートに必要な追加の列を指定します。プレビューには、レポートデータのサンプルが表示されます。カスタムレポートクエリを保存すると、保存されたクエリのリストに追加されます。

コピーしたODataクエリに基づいてカスタムレポートクエリを作成できます。これを行うには、オプションを選択し、コピーしたODataクエリを貼り付けます。結果のクエリは、後で実行するために保存できます。

注:

ODataクエリを使用して生成されたプレビューおよびエクスポートレポートの列名はローカライズされず、英語で表示されます。

グラフ上のフラグアイコンは、特定の時間範囲における重要なイベントまたはアクションを示します。フラグにマウスを合わせ、クリックしてイベントまたはアクションを一覧表示します。

注:

- HDX™接続ログオンデータは、バージョン7より前のVDAでは収集されません。それより前のVDAの場合、チャートデータは0と表示されます。
- Citrix Studioで削除されたデリバリーグループは、関連データが削除されるまでDirectorトレンドフィルターで選択できます。削除されたデリバリーグループを選択すると、保持期間までの利用可能なデータのグラフが表示されます。ただし、テーブルにはデータが表示されません。
- アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、新しいデリバリーグループの**リソース使用率と負荷評価インデックス**テーブルに、古いデリバリーグループと新しいデリバリーグループから統合されたメトリックが表示されます。

Autoscale 管理のマシンを監視する

Autoscale は、デリバリーグループ内の登録済みマルチセッションおよびシングルセッションOSマシンのプロアクティブな電源管理を可能にする電源管理機能です。Web Studio で選択したデリバリーグループに対して Autoscale を構成できます。詳細については、「Autoscale」を参照してください。 Director を使用して、Autoscale が有効なマシンの主要なメトリックを監視できます。

マシン使用状況

マシンの使用状況ページには、選択したデリバリーグループと期間について、電源がオンになっている Autoscale が有効なマルチセッションおよびシングルセッションOSマシンの総数が表示されます。このメトリックは、デリバリーグループ内のマシンの実際の使用状況を示します。 **シング**

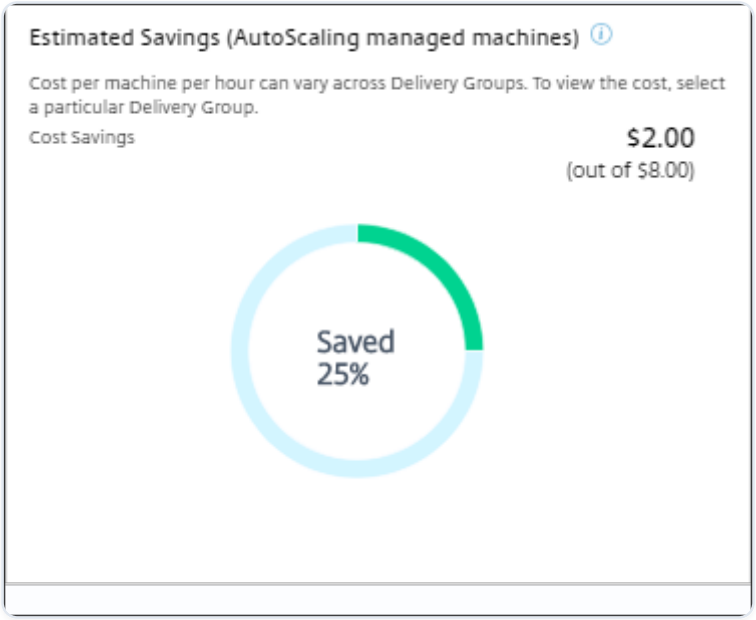
ルセッションOSマシンタブまたは**マルチセッションOSマシン**タブから、デリバリーグループと期間を選択します。

このグラフには、次のメトリックがプロットされます。

- **電源オンのマシン** - 電源がオンになっている Autoscale が有効なマシンの数
- **登録済みマシン** - 登録済みのマルチセッションまたはシングルセッションOSマシンの数
- **メンテナンス中のマシン** - メンテナンスモードがオンになっているマルチセッションまたはシングルセッションOSマシンの数

推定節約額

マシンの使用状況ページには、選択したデリバリーグループでAutoscaleを有効にすることによって達成された推定コスト削減額も表示されます。



推定節約額は、**デリバリーグループの編集** > **Autoscale** で構成されているとおりに、1時間あたりのマシンごとの節約額の割合（米ドル）として計算されます。マシンごとの節約額の構成の詳細については、「Autoscale」を参照してください。

すべてのデリバリーグループを選択すると、すべてのデリバリーグループにおける推定節約額の平均値が表示されます。

推定節約額は、管理者が既存のインフラストラクチャを統合し、最大の節約と利用率を達成するためのキャパシティを計画するのに役立ちます。

マシンとセッションのアラート通知

Directorダッシュボードには、アラート通知が表示されます。これらの通知はさらにドリルダウンできます。アラートの詳細は、**アラート**ページに表示されます。

- デリバリーグループでアラートポリシーを作成するには、**アラート** > **Citrixアラートポリシー** > **デリバリーグループポリシー**に移動します。
- ここでは、次の警告および重大なしきい値を設定できます。
  - 失敗したマシン（シングルセッションOS）および失敗したマシン（マルチセッションOS）、,
  - デリバリーグループ内のピーク接続セッション、ピーク切断セッション、およびピーク同時合計セッション。
- デリバリーグループ内の対応するメトリックがしきい値に達すると、アラートが生成されます。

アラートポリシーの条件と新しいアラートポリシーの作成に関する詳細については、「アラートと通知」を参照してください。

マシンのステータス

- **フィルター** > **マシン**には、すべてのマシンの電源状態が表形式で表示されます。特定のデリバリーグループでフィルターできます。
- **フィルター** > **セッション**には、マシン名でフィルターして、関連するセッションとそのリアルタイムの状態が表示されます。
- **傾向** > **セッション**で、デリバリーグループと期間を選択して、セッションとその関連メトリックの傾向を確認します。

詳細については、「障害トラブルシューティングのためのデータのフィルター」を参照してください。

負荷評価のトレンド

トレンド > **負荷評価インデックス**ページには、マルチセッションOSマシン間で分散される負荷に関する詳細情報を含むグラフが表示されます。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のマルチセッションOSマシン、マルチセッションOSマシン（デリバリーグループ内のマルチセッションOSマシンが選択されている場合にのみ利用可能）、および範囲が含まれます。負荷評価インデックスは、CPU合計、メモリ、ディスク、またはセッションの割合として表示され、最後の間隔での接続ユーザー数と比較して示されます。

展開のトラブルシューティング

ヘルプデスク管理者として、問題を報告しているユーザーを検索し、そのユーザーに関連付けられているセッションまたはアプリケーションの詳細を表示できます。同様に、問題が報告されてい

るマシンまたはエンドポイントを検索します。関連するメトリックを監視し、適切なアクションを実行することで、問題を迅速に解決できます。

利用可能なアクションは次のとおりです。

- 応答しないアプリケーションまたはプロセスを終了する
- ユーザーのマシンでのシャドウ操作
- 応答しないセッションからログオフする
- マシンを再起動する
- マシンをメンテナンスモードにする
- ユーザープロファイルをリセットする

アプリケーションのトラブルシューティング

リアルタイムアプリケーション監視

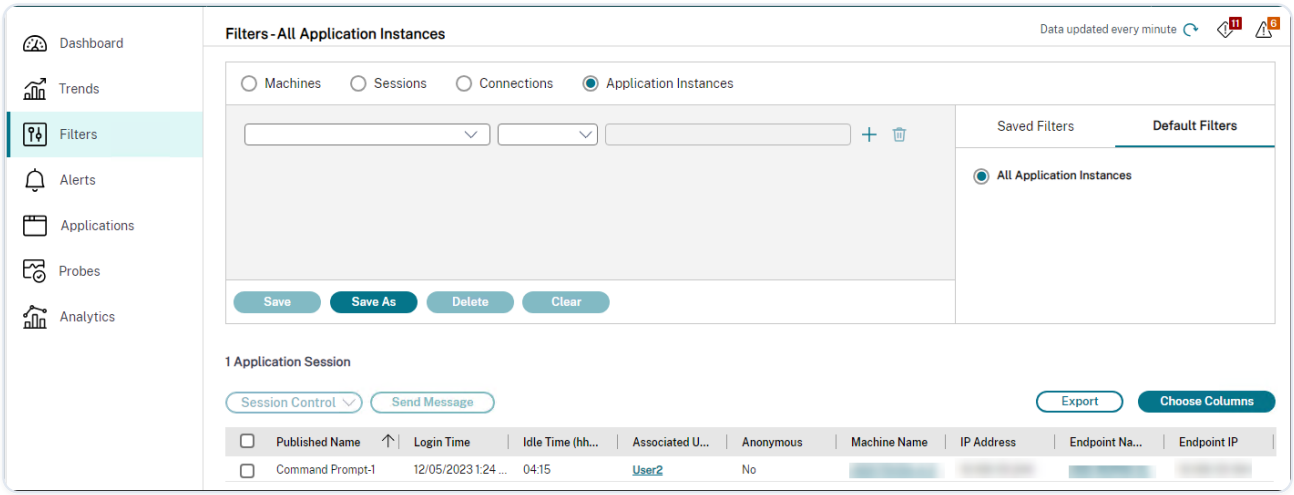
アイドル時間メトリックを使用して、特定の時間制限を超えてアイドル状態になっているインスタンスを特定することで、アプリケーションとセッションのトラブルシューティングを行うことができます。

アプリケーションベースのトラブルシューティングの典型的なユースケースは、従業員がアプリケーションライセンスを共有する医療分野にあります。そこでは、Citrix Virtual Apps and Desktops™ 環境をパージしたり、パフォーマンスの低いサーバーを再構成したり、アプリケーションを保守およびアップグレードしたりするために、アイドル状態のセッションとアプリケーションインスタンスを終了する必要があります。

アプリケーションインスタンスフィルターページには、サーバーおよびシングルセッションOSのVDA上のすべてのアプリケーションインスタンスが一覧表示されます。関連するアイドル時間測定値は、10分以上アイドル状態になっているマルチセッションOSのVDA上のアプリケーションインスタンスに対して表示されます。

> **注:** アプリケーションインスタンスのメトリックは、すべてのライセンスエディションのサイトで利用できます。

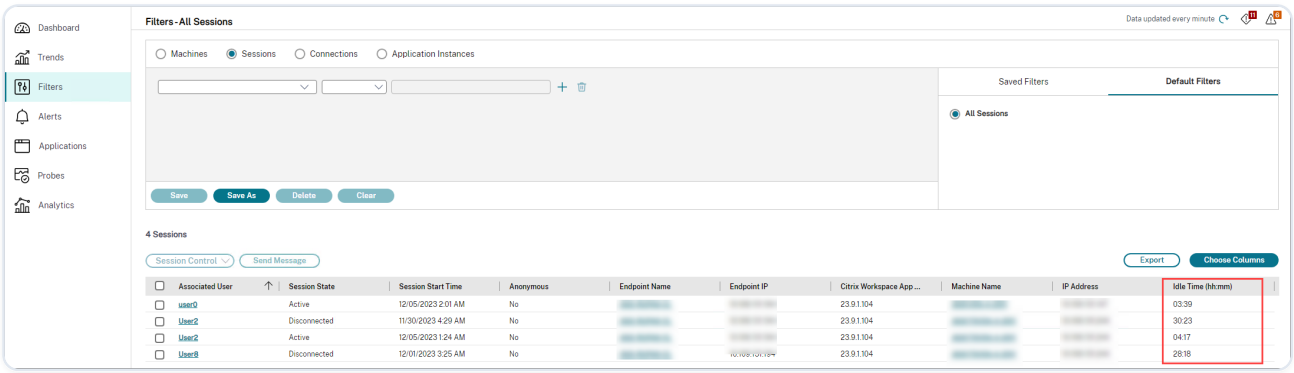
この情報を使用して、特定の期間を超えてアイドル状態になっているアプリケーションインスタンスを特定し、必要に応じてログオフまたは切断します。これを行うには、**フィルター \> アプリケーションインスタンス**を選択し、事前に保存されたフィルターを選択するか、**すべてのアプリケーションインスタンス**を選択して独自のフィルターを作成します。



フィルターの例は次のとおりです。**フィルター条件**として、**公開名**（アプリケーションの）と**アイドル時間**を選択します。次に、**アイドル時間**を特定の時間制限**以上**に設定し、再利用のためにフィルターを保存します。フィルターされたリストから、アプリケーションインスタンスを選択します。メッセージを送信するオプションを選択するか、**セッション制御**ドロップダウンから**ログオフ**または**切断**を選択してインスタンスを終了します。

> **注:** アプリケーションインスタンスからログオフまたは切断すると、現在のセッションがログオフまたは切断され、同じセッションに属するすべてのアプリケーションインスタンスが終了します。

セッションの状態とセッションアイドル時間メトリックを使用して、**セッション**フィルターページからアイドルセッションを特定できます。**アイドル時間**列で並べ替えるか、特定の時間制限を超えてアイドル状態になっているセッションを特定するためのフィルターを定義します。アイドル時間は、10分以上アイドル状態になっているマルチセッションOSのVDA上のセッションに対して一覧表示されます。



セッションまたはアプリケーションインスタンスが次のいずれかの場合、**アイドル時間**は**N/A**と表示されます。

- 10分以上アイドル状態になっていない場合、,
- シングルセッションOSのVDAで起動されている場合、または

- Version 7.12以前のVDAで起動されます。

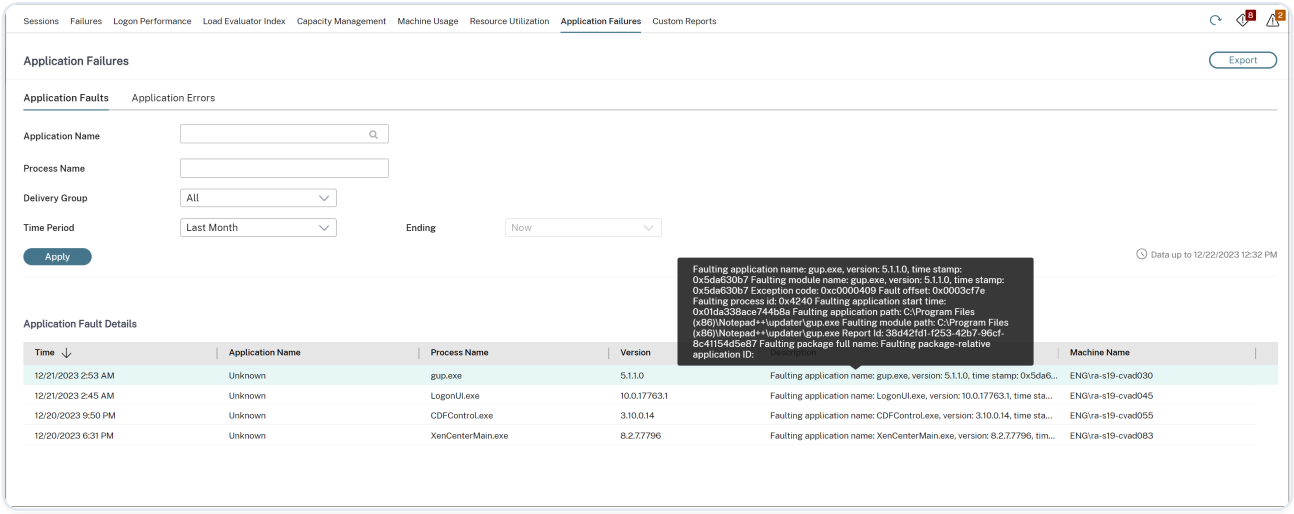
アプリケーション障害の履歴監視

トレンド -\> **アプリケーション障害**タブには、VDA上の公開アプリケーションに関連する障害が表示されます。

アプリケーション障害の傾向は、PremiumおよびAdvancedライセンスサイトでは過去2時間、24時間、7日間、および1か月間利用できます。その他のライセンスタイプでは、過去2時間、24時間、および7日間利用できます。「Application Errors」をソースとしてイベントビューアにログ記録されたアプリケーション障害が監視されます。**エクスポート**をクリックして、CSV、Excel、またはPDF形式でレポートを生成します。

アプリケーション障害監視のグルーミング保持設定であるGroomApplicationErrorsRetentionDaysとGroomApplicationFaultsRetentionDaysは、Premiumおよび非Premiumライセンスサイトの両方で、デフォルトで1日に設定されています。この設定は、PowerShellコマンドを使用して変更できます。

```
Set-MonitorConfiguration -\<setting name\> \<value\>
```



障害は、その重大度に基づいて**アプリケーション障害**または**アプリケーションエラー**として表示されます。アプリケーション障害タブには、機能またはデータの損失に関連する障害が表示されます。アプリケーションエラーは、すぐには関連しない問題を示します。これらは将来問題を引き起こす可能性のある状態を示します。

「**公開アプリケーション名**」、「**プロセス名**」、「**デリバリーグループ**」、および「**期間**」に基づいて障害をフィルタリングできます。テーブルには、障害またはエラーコードと障害の簡単な説明が表示されます。詳細な障害説明はツールチップとして表示されます。

> **注:** 対応するアプリケーション名を導出できない場合、公開アプリケーション名は「不明」と表示されます。これは通常、起動されたアプリケーションがデスクトップセッションで失敗した場合、または依存する実行可能ファイルによって引き起こされた未処理の例外が原因で失敗した場合に発生します。

> デフォルトでは、マルチセッションOS VDAでホストされているアプリケーションの障害のみが監視されます。監視設定は、監視グループポリシー（アプリケーション障害の監視を有効にする、シングルセッションOS VDAでのアプリケーション障害の監視を有効にする、障害監視から除外されるアプリケーションのリスト）を通じて変更できます。詳細については、監視ポリシー設定のアプリケーション障害監視のポリシーを参照してください。

トレンド \> アプリケーションプローブ結果ページには、過去24時間および7日間にサイトで実行されたアプリケーションプローブの結果が表示されます。アプリケーションプローブの構成方法の詳細については、アプリケーションプローブを参照してください。

マシンのトラブルシューティング

> **注:**

> **Citrix Health Assistant**は、未登録VDAの構成に関する問題をトラブルシューティングするためのツールです。このツールは、VDA登録の失敗、セッション起動、タイムゾーンリダイレクト構成に関する問題の考えられる根本原因を特定するために、いくつかのヘルスチェックを自動化します。Knowledge Centerの記事「Citrix Health Assistant - VDA登録とセッション起動のトラブルシューティング」には、**Citrix Health Assistant**ツールのダウンロードと使用方法が記載されています。

> Directorコンソールの**フィルター > マシン**ビューには、サイトで構成されているマシンが表示されます。マルチセッションOSマシンタブには、ロード評価インデックスが含まれており、これはパフォーマンスカウンターの分布と、リンクにカーソルを合わせると表示されるセッション数のツールヒントを示します。

失敗したマシンの**失敗理由**列をクリックすると、失敗の詳細な説明と、その失敗をトラブルシューティングするために推奨されるアクションが表示されます。マシンおよび接続の失敗の理由と推奨されるアクションについては、「Citrix Directorの失敗理由とトラブルシューティング」を参照してください。

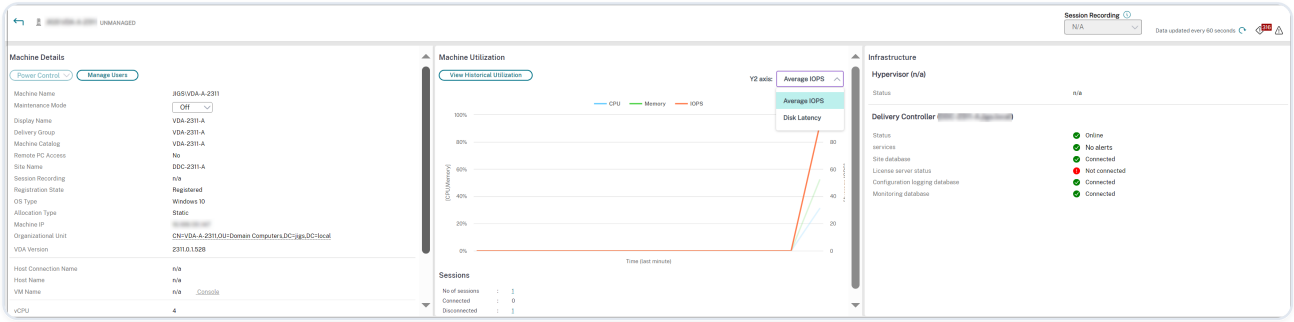
マシン名のリンクをクリックすると、**マシン詳細**ページに移動します。

マシン詳細ページには、マシンの詳細、インフラストラクチャの詳細、およびマシンに適用されているホットフィックスの詳細が一覧表示されます。

マシンベースのリアルタイムリソース使用率

マシン使用率パネルには、CPUとメモリのリアルタイム使用率を示すグラフが表示されます。さらに、Delivery ControllerとVDAのバージョンが**7.14**以降のサイトでは、ディスクとGPUの監視グラフが利用できます。

ディスク監視グラフ、平均IOPS、およびディスク遅延は、VDAディスクに関連する問題を監視およびトラブルシューティングするのに役立つ重要なパフォーマンス測定値です。平均IOPSグラフは、ディスクへの読み取りおよび書き込みの平均数を表示します。**ディスク遅延**を選択すると、データの要求からディスクからの応答までの遅延をミリ秒単位で測定したグラフが表示されます。



GPU使用率

マルチセッションおよびシングルセッションOS VDAでのGPU関連の問題をトラブルシューティングするには、**GPU使用率**を選択して、GPU、GPUメモリ、エンコーダー、およびデコーダーの使用率（パーセンテージ）を確認します。

サポートされているGPUバージョン:

- ディスプレイドライバーバージョン369.17以降を実行しているNVIDIA Tesla M60 GPU。詳細については、「NVIDIA vGPUソフトウェア」を参照してください。
- AMD Radeon Instinct MI25 GPUおよびAMD EPYC 7V12（Rome）CPU。詳細については、「AMD Drivers and Support」を参照してください。

ドライバー:

適切なドライバーまたは拡張機能をVDAにインストールする必要があります。

- NVIDIA GPUの場合、GRIDドライバーを手動で、または拡張機能経由でインストールします。詳細については、「NVIDIA vGPU Software」を参照してください。
    - NVIDIAの場合、GRIDドライバーのみがサポートされています。CUDAドライバーはNVadsA10 v5シリーズでは動作せず、サポートされていません。

  - Azureベースのマシンに拡張機能経由でNVIDIA Grid GPUドライバーをインストールする手順の例については、「NVIDIA GRID drivers. NVIDIA GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines」を参照してください。
  - NVIDIA Grid GPUドライバーを手動でインストールする手順の例については、「Azure N-series NVIDIA GPU driver setup for Windows - Azure Virtual Machines」を参照してください。

- AMD GPUの場合、AMDグラフィックドライバーを手動で、または拡張機能経由でインストールします。詳細については、「AMD Drivers and Support」を参照してください。

  - Azureベースのマシンに拡張機能経由でAMD GPUドライバーをインストールする手順の例については、「AMD GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines」を参照してください。
  - AzureマシンにAMD GPUドライバーを手動でインストールする手順の例については、「Install AMD GPU drivers on N-series VMs running Windows」を参照してください。

使用上の注意:

- GPU使用率グラフは、64ビットWindowsを実行しているVDAでのみ利用可能です。
- GPUアクセラレーションを提供するには、VDAでHDX 3D Proを有効にする必要があります。詳細については、「GPU acceleration for Windows Single-session OS」および「GPU acceleration for Windows Multi-session OS」を参照してください。
- VDAが複数のGPUにアクセスする場合、使用率グラフには個々のGPUから収集されたGPUメトリックの平均が表示されます。GPUメトリックは、個々のプロセスではなく、VDA全体に対して収集されます。
- AMDの場合、エンコーダーとデコーダーの使用は個別にサポートされていません。GPUを使用するエンコード/デコードワークロードは、GPU使用率における一般的な3D負荷として報告されます。
- NVIDIA WMIをインストール時にインストールしてください。このウィンドウは手動インストール時のみ利用可能です。
- ドライバーがインストールされているのにDirectorがGPUを検出しない場合

  - タスクマネージャーを確認してください。ドライバーが正しくインストールされていれば、GPUはタスクマネージャーに表示されるはずです。
  - マシンが登録されているか確認してください。マシンがオンラインとして検出されるまでに時間がかかる場合があります。

- DirectorでGPU使用率にアクティビティが表示されない場合は、実行しているワークロードがGPUを使用していることを確認してください。グラフィックワークロードの場合、これは「設定」>「システム」>「ディスプレイ」>「グラフィック設定」>「優先するアプリを選択」から有効にできます。「高パフォーマンス」をオンにしてください。システムデフォルトまたは省電力に設定されている場合、他の設定に基づいて、Windowsがグラフィックワークロードに CPUを使用するようデフォルトで設定されることがあります。
- データは毎分更新され、**GPU使用率**を選択してから1分以内にデータ視覚化が開始されます。

マシンベースの履歴リソース使用率

マシン使用率パネルで、**履歴使用率の表示**をクリックすると、選択したマシン上のリソースの履歴使用状況が表示されます。 使用率グラフには、CPU、メモリ、ピーク同時セッション、平均IOPS、ディスク遅延の重要なパフォーマンスカウンターが含まれます。

> **注:**
>
> 監視ポリシー設定の**プロセス監視を有効にする**は、履歴マシン使用率ページの「上位10プロセス」テーブルでデータを収集および表示するために、「許可」に設定する必要があります。収集はデフォルトで禁止されています。

> CPUとメモリの使用率、平均IOPS、ディスク遅延のデータはデフォルトで収集されます。**リソース監視を有効にする**ポリシー設定を使用して、収集を無効にできます。



1. **マシン詳細**ビューの**マシン使用率**パネルから、**履歴使用率の表示**を選択します。

2. **履歴マシン使用率**ページで、**期間**を設定して、過去2時間、24時間、7日間、1か月、または1年間の使用状況を表示します。

> **注:**
>
> 平均IOPSとディスク遅延の使用状況データは、現在を終点とする過去24時間、1か月、1年分のみ利用可能です。カスタム終了時刻はサポートされていません。

3. **適用**をクリックし、必要なグラフを選択します。
4. グラフのさまざまなセクションにカーソルを合わせると、選択した期間の詳細情報が表示されます。



たとえば、**過去2時間**を選択した場合、ベースライン期間は選択した時間範囲の前の2時間です。過去2時間とベースライン時間のCPU、メモリ、セッションの傾向を表示します。**先月**を選択した場合、ベースライン期間は前月です。先月とベースライン時間の平均IOPSとディスク遅延を表示するように選択します。

1. **エクスポート**をクリックして、選択した期間のリソース使用状況データをエクスポートします。詳細については、「展開の監視」のレポートのエクスポートセクションを参照してください。
2. グラフの下の表には、CPUまたはメモリ使用率に基づいて上位10個のプロセスが一覧表示されます。選択した時間範囲におけるアプリケーション名、ユーザー名、セッションID、平均CPU、ピークCPU、平均メモリ、ピークメモリを示す任意の列でソートできます。IOPSとディスク遅延の列はソートできません。

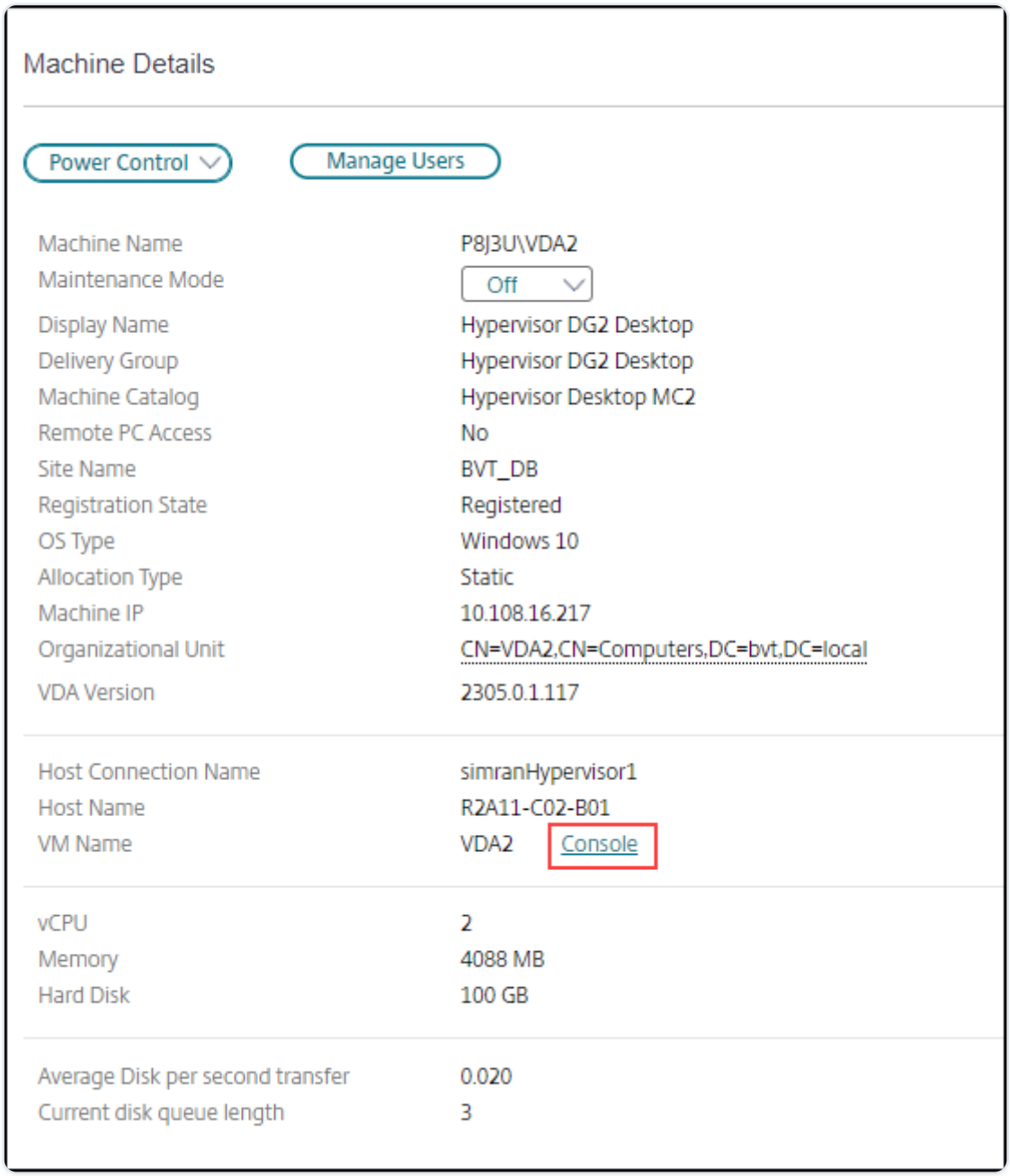
> **注：**
>
> システムプロセスのセッションIDは「0000」と表示されます。

3. 特定のプロセスのリソース消費の履歴傾向を表示するには、上位10個のプロセスのいずれかをドリルダウンします。

マシンコンソールへのアクセス

XenServerバージョン7.3以降でホストされているシングルセッションおよびマルチセッションOSマシンのコンソールには、Directorから直接アクセスできます。これにより、XenServerでホストされているVDAの問題をトラブルシューティングするためにXenCenterは必要ありません。この機能を利用するには：

- バージョン7.16以降のDelivery Controllerが必要です。
- マシンをホストしているXenServerはバージョン7.3以降である必要があり、Director UIからアクセスできる必要があります。



マシンのトラブルシューティングを行うには、対応するマシン詳細パネルの**コンソール**リンクをクリックします。提供されたホスト資格情報が認証されると、WebベースのVNCクライアントであるnoVNCを使用して、マシンコンソールが別のタブで開きます。これで、キーボードとマウスでコンソールにアクセスできます。

注:

- この機能はInternet Explorer 11ではサポートされていません。
- マシンコンソールのマウス ポインターがずれている場合は、問題を解決する手順についてCTX230727を参照してください。

- Directorは新しいタブでコンソールアクセスを起動します。ブラウザの設定でポップアップが許可されていることを確認してください。
- セキュリティ上の理由から、Citrix®はブラウザにSSL証明書をインストールすることを推奨しています。

最近の電源操作があるマシンを検査する

成功および失敗した電源操作のステータスを持つマシンを検査できるようになりました。この機能は、以下の分析に役立ちます。

- ユーザーの問題を引き起こす電源オンの失敗
- コストを増加させる電源オフの失敗

注:

データは電源管理されているマシンでのみ利用可能です。この機能がサポートされる前に実行された電源操作のデータは利用できません。

以下の方法で、マシンの電源操作ステータスを表示できます。

フィルター -> **マシン** タブから。この場合、デフォルトで**電源操作時刻**と**電源操作結果**の列が表示されます。表示したい列を選択することもできます。

コスト最適化タブから。この場合、デフォルトのフィルターは**電源操作のトリガー元**が*Autoscale™*に設定され、**電源操作結果**が*失敗*に設定されています。

この機能により、電源操作制御の詳細を表示できます。たとえば、誰が操作をトリガーしたか、どの操作が電源状態を変更したか、失敗の理由、操作が完了した時刻などを表示できます。これらの詳細をエクスポートすることもできます。

電源操作のステータスを表示するために、以下のフィルターが追加されています。

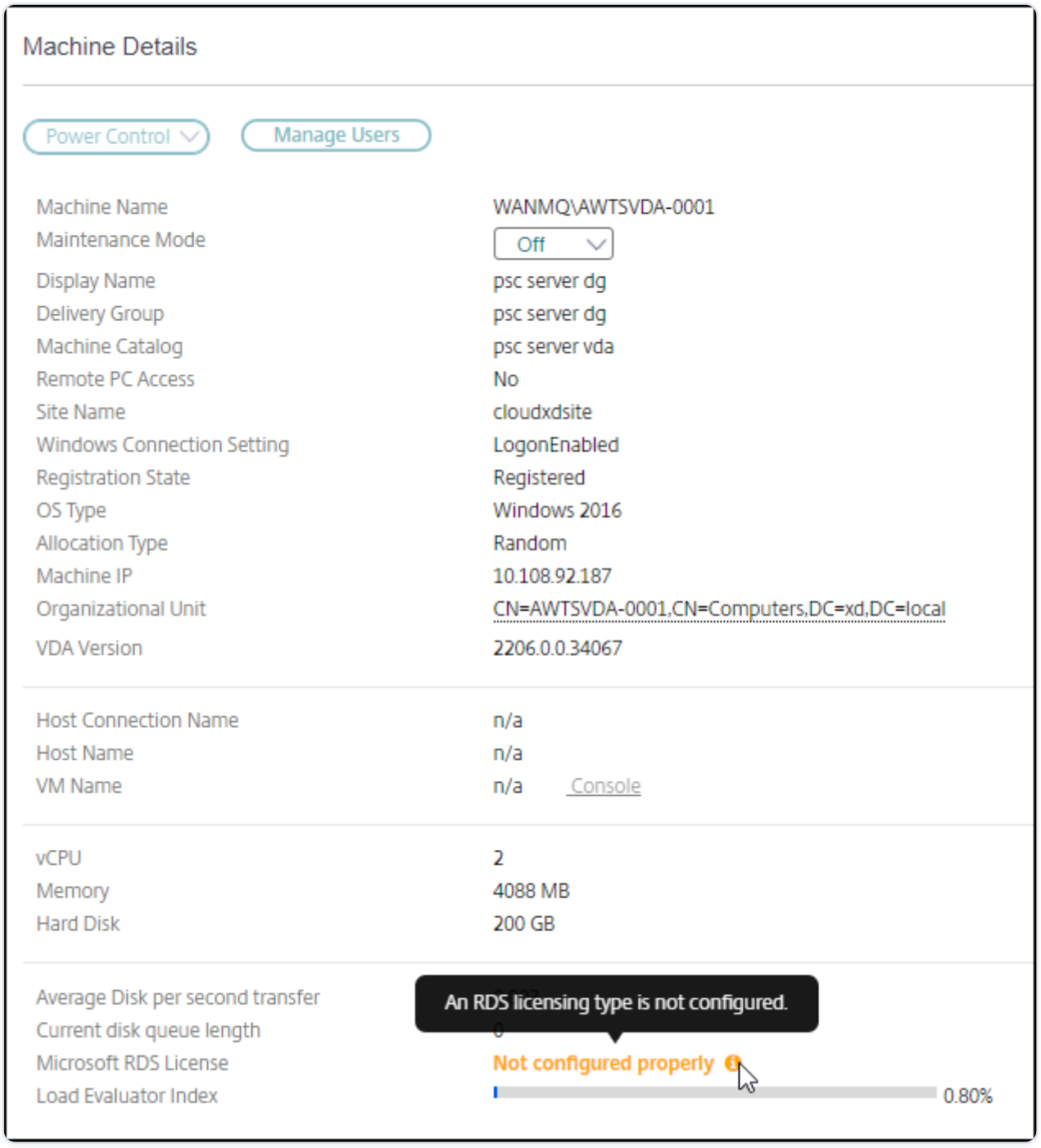
フィルター	説明
電源操作結果	電源操作の結果を表示します。可能なフィルター値は「成功」と「失敗」です。

フィルター	説明
電源操作のトリガー元	電源操作をトリガーしたユーザーまたは内容を表示します。可能なフィルター値は次のとおりです。 • オートスケール - この値は、電源操作が次によってトリガーされた場合に表示されます。 • 管理者がVMのOSディスクを初期状態に戻すためにVMをシャットダウンした場合 • 設定されたポリシーに基づいてVMがシャットダウンまたは中断された場合 • プールサイズまたはバッファサイズの構成に基づいてVMが利用可能になった場合 • 管理者 - この値は、管理者によって電源操作がトリガーされたときに表示されます。考えられる例としては、管理者がVMのシャットダウン、起動、一時停止、再開、再起動、またはリブートを要求した場合などがあります。 • ユーザー - この値は、ユーザーによって電源操作がトリガーされたときに表示されます。例としては、ユーザーがVMをリセット、起動、または作業を再開した場合などがあります。

フィルター	説明
	• その他 - この値は、電源操作がスケジュールされた理由または不明な理由によってトリガーされたときに表示されます。
最終電源操作	マシンで発生した正確な電源操作（電源オン、電源オフ、シャットダウン、再起動、リセット、再開など）を表示します。
電源操作時刻	電源操作が完了した時刻。可能なフィルター値は、過去1分、過去5分、過去30分、過去1時間、今日、過去24時間、昨日です。
電源操作失敗理由	失敗の理由を表示します。可能なフィルター値は、ハイパーバイザー報告の失敗、ハイパーバイザーのレート制限超過、不明なエラー、なしです。操作が成功した場合は「なし」と表示されます。

Microsoft RDSライセンスの健全性

マルチセッションOSマシンについては、**マシン詳細**パネルの**マシン詳細**ページと**ユーザー詳細**ページで、Microsoft RDSライセンスのステータスを表示できます。



次のいずれかのメッセージが表示されます。

- ライセンス利用可能
- 適切に構成されていません（警告）
- ライセンスエラー（エラー）
- 互換性のないVDAバージョン（エラー）

> **注:**

有効なライセンスを持つ猶予期間中のマシンのMicrosoft RDSライセンスの健全性ステータスは、緑色で「**ライセンス利用可能**」メッセージを表示します。ライセンスの有効期限が切れる前に更新してください。

警告メッセージとエラーメッセージについては、情報アイコンにカーソルを合わせると、次の表に示す追加情報が表示されます。

メッセージの種類	DIRECTOR内のメッセージ
エラー	VDAバージョン7.16以降で利用可能です。
エラー	新しいRDS接続は許可されません。
エラー	Microsoft RDSライセンスの猶予期間が過ぎました。
エラー	必要なOSレベルに対して、デバイスごとのクライアントアクセスライセンスの種類でライセンスサーバーが構成されていません。
エラー	構成されているライセンスサーバーは、デバイスごとのクライアントアクセスライセンスの種類でRDSホストOSレベルと互換性がありません。
警告	Personal Terminal Serverは、Citrix Virtual Apps and Desktops™展開において有効なRDSライセンスの種類ではありません。
警告	管理用リモートデスクトップは、Citrix Virtual Apps and Desktops展開において有効なライセンスの種類ではありません。
警告	RDSライセンスの種類が構成されていません。
警告	ユーザーごとのクライアントアクセスRDSライセンスの種類では、ドメインコントローラーまたはライセンスサーバーに到達できません。

メッセージの種類	DIRECTOR内のメッセージ
警告	デバイスごとのクライアントアクセスライセンスの種類では、必要なOSレベルのライセンスサーバーに到達できないため、クライアントデバイスライセンスを特定できません。

注:

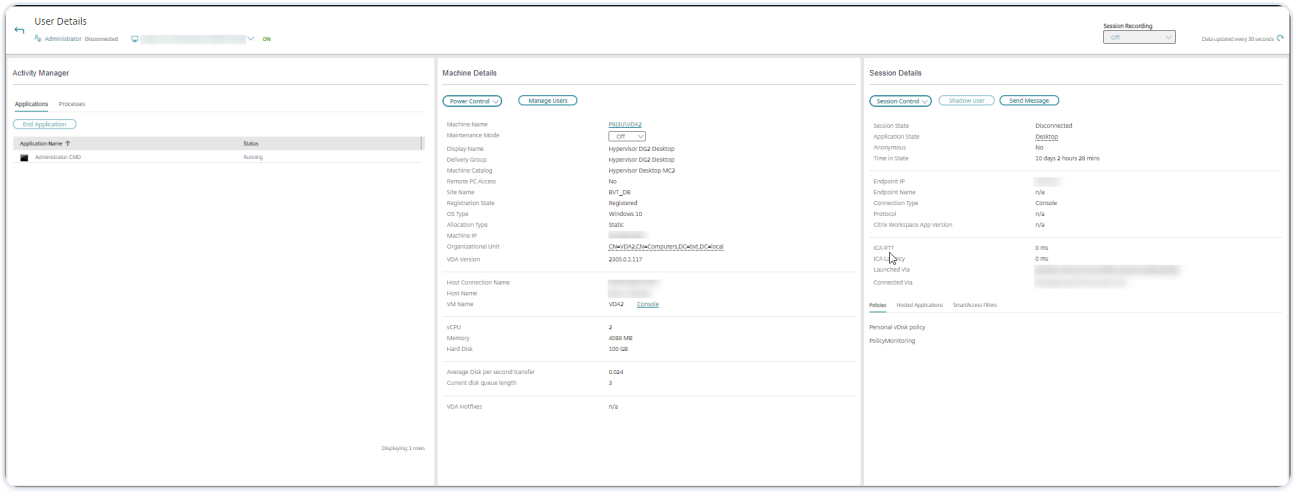
この機能は、Microsoft RDS CAL (クライアントアクセスライセンス) にのみ適用されます。

ユーザーの問題のトラブルシューティング

Directorの**ヘルプデスク**ビュー（**アクティビティマネージャー**ページ）を使用して、ユーザーまたはセッションに関する情報を表示します。

ユーザーの詳細(/en-us/citrix-virtual-apps-desktops/2411/media/dir-user-details-summary.png)

アクティビティマネージャーでユーザーの**詳細の表示**をクリックすると、**ユーザーの詳細**ページが開きます。 アクティビティマネージャーでエンドポイントの**詳細の表示**をクリックすると、**エンドポイントの詳細**ページが開きます。



セッションセレクター

ユーザーが複数のセッションを開始している場合、セッションセレクターはセッションの選択に役立ちます。

セッションセレクター(/en-us/citrix-virtual-apps-desktops/2411/media/dir-session-selector.png)

詳細を表示するセッションを選択します。

- セッション、ユーザーのサインインエクスペリエンス、セッションの起動、接続、およびアプリケーションに関する詳細を確認します。
- ユーザーのマシンをシャドウできます。
- ICA®セッションを記録します。

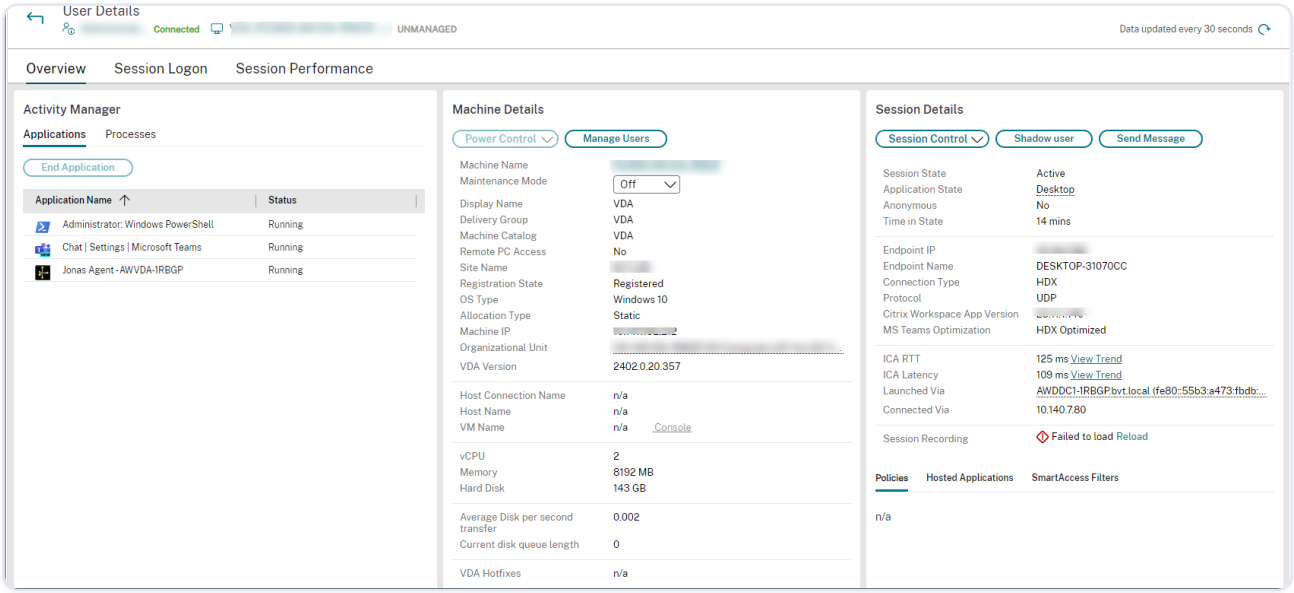
Microsoft Teamsの最適化ステータス

Directorは、**ユーザーの詳細**ページ > **セッションの詳細**パネル > **MS Teamsの最適化**フィールドに、HDX™セッションのMicrosoft Teamsの最適化ステータスを表示します。Microsoft Teamsが最適化されていることは、クリアなオーディオとビデオなど、より良いユーザーエクスペリエンスのために不可欠です。Microsoft Teamsの最適化ステータスの可視性は、チケットの解決にかかる時間を短縮し、管理者がトラブルシューティング中に重要なメトリックを特定するのに役立ちます。

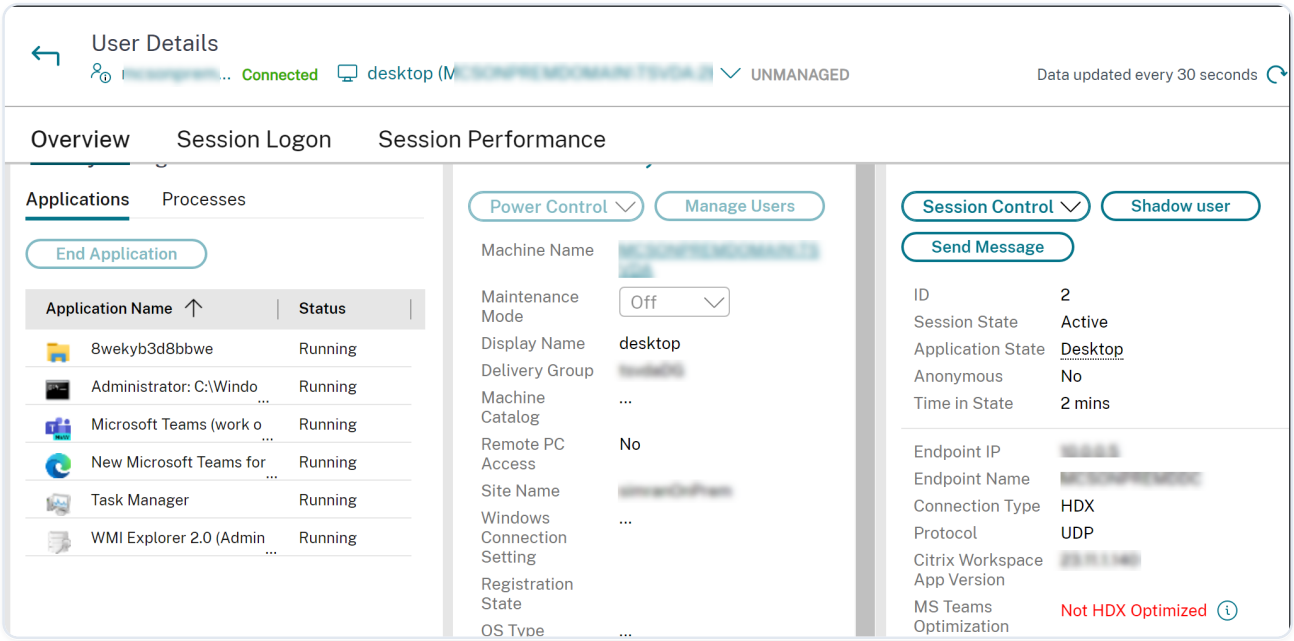
> **注：**
>
> Citrix Directorは、Microsoft Teamsバージョン2.1以前をサポートしています。

> 前提条件:

- VDAはバージョン2311以降を実行しています。
- Citrix Workspace app でサポートされているバージョンは、Microsoft Teams の最適化に記載されています。
- Microsoft Teams は、公開アプリケーションとして、または公開デスクトップ内で実行されます。
- Citrix HDX HTML5 Video Redirection Service などの重要なサービスが実行されています。



Microsoft Teams が最適化されていない場合、ツールヒントには、Microsoft Teams を最適化するためのヒントを含む、HDX からの外部トラブルシューティングライブ記事へのリンクが表示されます。HDX 最適化のトラブルシューティング。



トラブルシューティングのヒント

次の表に記載されている推奨されるアクションで問題をトラブルシューティングし、必要に応じて適切な管理者に問題をエスカレートしてください。

ユーザーの問題	提案
ログオンに時間がかかる、または断続的または繰り返し失敗する	ユーザーログオンの問題を診断する

ユーザーの問題	提案
セッションの起動に時間がかかる、または断続的または繰り返し失敗する	セッション起動の問題を診断する
セッションの応答が遅い、または応答しない	セッションパフォーマンスの問題を診断する
アプリケーションが遅い、または応答しない	アプリケーション障害の解決
接続に失敗しました	デスクトップ接続の復元
セッションが遅い、または応答しない	セッションの復元
セッションを記録する	セッションの記録
ビデオが遅い、または品質が悪い	HDXチャネルシステムレポートの実行

注: マシンがメンテナンスモードになっていないことを確認するには、ユーザー詳細ビューから パネルを確認します。

セッションログオン

「**ユーザー詳細**」ビュー > 「**セッションログオン**」タブには、セッションログオンプロセスの包括的なビューが表示されます。このタブには、さまざまなログオンフェーズがプロットされたログオン期間フェーズチャートが含まれています。このデータを使用して、ユーザーログオンの問題をトラブルシューティングします。詳細については、「ユーザーログオンの問題の診断」を参照してください。

セッションパフォーマンス

セッションパフォーマンスタブには、ユーザーセッション内の問題を特定するためにリアルタイムメトリックを関連付ける機能から始まる、強化されたトラブルシューティングワークフローがあります。**セッショントポロジ**パネルは、接続されたHDXセッションのセッション内パスを視覚的に表現します。**パフォーマンスメトリック**パネルは、ICARTT、ICA遅延、1秒あたりのフレーム数、利用可能な出力帯域幅、消費された出力帯域幅などのセッションメトリックの傾向を提供し、これらのメトリックが時間の経過とともにどのようにパフォーマンスを発揮したかを示します。詳細については、セッションパフォーマンスの問題の診断を参照してください。

検索のヒント

検索フィールドにユーザー名を入力すると、DirectorはDirectorをサポートするように構成されているすべてのサイトのActive Directoryでユーザーを検索します。

検索フィールドにマルチユーザーマシンの名前を入力すると、Director は指定されたマシンのマシン詳細を表示します。

検索フィールドにエンドポイント名を入力すると、Director は特定のEndpointに接続されている認証されていない（匿名）セッションと認証済みセッションを使用します。この検索により、認証されていないセッションのトラブルシューティングが可能になります。認証されていないセッションのトラブルシューティングを可能にするには、エンドポイント名が一意であることを確認してください。

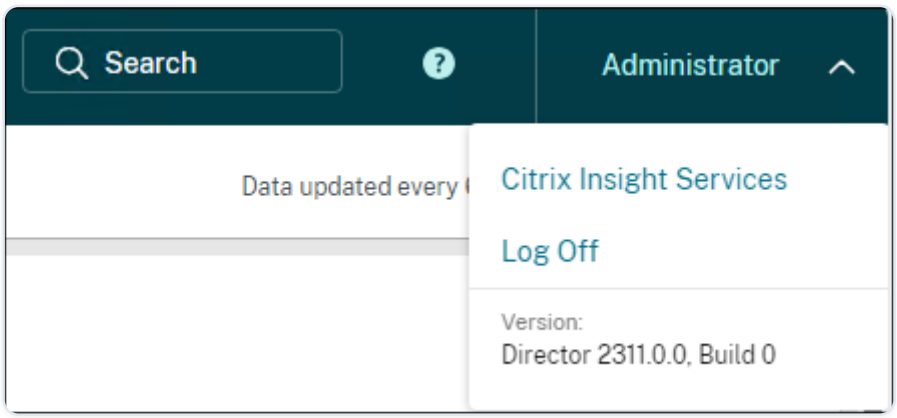
検索結果には、現在マシンを使用していない、またはマシンに割り当てられていないユーザーも含まれます。

- 検索では大文字と小文字は区別されません。
- 部分的な入力では、一致する可能性のあるリストが生成されます。
- スペースで区切られた2つの部分からなる名前の数文字を入力すると、両方の文字列に一致する結果が含まれます。2つの部分からなる名前の例としては、ユーザー名、姓と名、または表示名があります。たとえば、「jo rob」と入力すると、「John Robertson」や「Robert Jones」などの文字列が結果に含まれる場合があります。

ランディングページに戻るには、**Director ロゴ**をクリックします。

Citrix Insight Servicesへのアクセス

Director の ドロップダウンリストから Citrix Insight Services (CIS) にアクセスして、追加の診断情報を取得できます。CIS で利用できるデータは、Call Home や Citrix Scout などのソースから取得されます。



トラブルシューティング情報をCitrixテクニカルサポートにアップロードする

単一のDelivery Controller™またはVDAからCitrix Scoutを実行し、主要なデータポイントとCitrix Diagnostics Facility (CDF)トレースをキャプチャして、選択したコンピューターのトラブルシューティングを行います。Scoutは、データをCISプラットフォームに安全にアップロードする機能を提供し、Citrixテクニカルサポートのトラブルシューティングを支援します。CitrixテクニカルサポートはCISプラットフォームを使用して、顧客から報告された問題の解決にかかる時間を短縮します。

ScoutはCitrix Virtual Apps and Desktops™コンポーネントとともにインストールされます。Windowsのバージョンに応じて、Citrix Virtual Apps and Desktopsをインストールまたはアップグレードすると、Scoutは**Windowsのスタート**メニューまたはスタート画面に表示されます。

Scoutを起動するには、スタートメニューまたはスタート画面から、**Citrix \> Citrix Scout**を選択します。

Scoutの使用方法と構成、およびFAQについては、CTX130147を参照してください。

セッション起動の問題を診断する

ユーザーログオンの問題の診断セクションで述べられているログオンプロセスフェーズに加えて、Directorはセッション起動時間を表示します。これは、**ユーザー詳細**ページと**マシン詳細**ページで、Workspace Appセッション起動時間とVDAセッション起動時間に分けられます。これら2つの期間は、さらに個々のフェーズを含み、その起動時間も表示されます。このデータは、セッション起動時間が長い原因を理解し、トラブルシューティングするのに役立ちます。さらに、セッション起動に関わる各フェーズの時間も、個々のフェーズに関連する問題のトラブルシューティングに役立ちます。たとえば、ドライブマッピング時間が長い場合、GPOまたはスクリプトですべての有効なドライブが正しくマッピングされているかを確認できます。この機能は、Delivery Controllerバージョン7 1906以降およびVDA 1903以降で利用可能です。

前提条件

セッション起動時間のデータが表示されるには、以下の前提条件が満たされていることを確認してください。

- デリバリーコントローラー™ 7 1906 以降。
- VDA 1903以降。
- Citrix End User Experience Monitoring (EUEM) サービスがVDAで実行されている必要があります。

制限事項

Directorがセッション起動時間のデータを表示する際には、以下の制限が適用されます。

- セッション起動時間は、HDX™セッションでのみ利用可能です。
- iOSおよびAndroid OSからのセッション起動の場合、VDA起動時間のみが利用可能です。
- ICA®ファイルダウンロード時間 (IFDCD) は、ブラウザから起動する際にWorkspace Appが検出された場合にのみ利用可能です。
- Mac OSからのセッション起動の場合、IFDCDはWorkspace App 1902以降でのみ利用可能です。
- Windows OSからのセッション起動の場合、IFDCDはWorkspace app 1902以降で利用可能です。それ以前のバージョンでは、IFDCDは、ブラウザから起動し、Workspace appが検出されたアプリ起動の場合にのみ表示されます。

注:

- 前提条件が満たされた後もセッション起動時間の表示に問題がある場合は、CTX130320に記載されているように、DirectorサーバーとVDAのログを確認してください。 共有セッション（同じセッションで複数のアプリケーションが起動される場合）の場合、Workspace Appの起動メトリックは、最新の接続または最新のアプリケーション起動に対して表示されます。
- VDAセッション起動の一部のメトリックは、再接続時には適用されません。そのような場合は、メッセージが表示されます。

セッション起動(/en-us/citrix-virtual-apps-desktops/2411/media/session_startup.png)

Workspace App セッション起動フェーズ

セッション起動クライアント期間 (SSCD)

このメトリックが高い場合、起動時間の長期化を引き起こしているクライアント側の問題を示しています。問題の根本原因を特定するために、後続のメトリックを確認してください。SSCDは、要求（マウスクリック）の時刻にできるだけ近い時刻に開始されます。クライアントデバイスとVDA間のICA接続が確立されたときに終了します。共有セッションの場合、サーバーへの新しい接続の作成に関連するセットアップコストの多くが発生しないため、この期間ははるかに短くなります。次のレベルでは、いくつかの詳細なメトリックが利用可能です。

ICA ファイルダウンロード期間

これは、クライアントがサーバーから ICA ファイルをダウンロードするのにかかる時間です。全体的なプロセスは次のとおりです。

1. ユーザーはWorkspaceアプリケーションでリソース（アプリケーションまたはデスクトップ）をクリックします。
2. ユーザーからの要求は、Citrix Gateway（構成されている場合）を介してStoreFront™に送信され、StoreFront™は要求をDelivery Controllerに送信します。
3. Delivery Controllerは要求に利用可能なマシンを見つけ、マシン情報とその他の詳細をStoreFrontに送信します。また、StoreFrontはSecure Ticket Authorityからワンタイムチケットを要求し、受け取ります。
4. StoreFrontはICAファイルを生成し、Citrix Gateway（構成されている場合）を介してユーザーに送信します。

IFDCDは、完全なプロセス（ステップ1～4）にかかる時間を表します。IFDCD期間は、クライアントがICAファイルを受信したときにカウントを停止します。

LPWD は、プロセスの StoreFront コンポーネントです。

IFDCD が高い (ただし LPWD が正常である) 場合、起動のサーバー側処理は成功しましたが、クライアントデバイスと StoreFront の間に通信の問題がありました。これは、2つのマシン間のネットワークの問題に起因します。したがって、まず潜在的なネットワークの問題をトラブルシューティングできます。

起動ページWEBサーバー所要時間 (LPWD)

これはStoreFrontで起動ページ (launch.aspx) を処理するのにかかる時間です。LPWDが高い場合、StoreFrontでボトルネックが発生している可能性があります。

考えられる原因は次のとおりです。

- StoreFrontの負荷が高い。Internet Information Services (IIS) のログや監視ツール、タスクマネージャー、パフォーマンスモニターなどを確認して、速度低下の原因を特定してください。
- StoreFrontがDelivery Controllerなどの他のコンポーネントとの通信に問題がある。StoreFrontとDelivery Controller間のネットワーク接続が遅いか、一部のDelivery Controllerがダウンしているか、過負荷になっていないかを確認してください。

名前解決WEBサーバー所要時間 (NRWD)

これは、Delivery Controllerが公開アプリケーション/デスクトップの名前をVDAマシンのIPアドレスに解決するのにかかる時間です。

このメトリックが高い場合、Delivery Controllerが公開アプリケーションの名前をIPアドレスに解決するのに時間がかかっていることを示します。

考えられる原因としては、クライアント側の問題、Delivery Controllerの過負荷などのDelivery Controller側の問題、またはそれらの間のネットワークリンクの問題が挙げられます。

チケット応答WEBサーバー所要時間 (TRWD)

この所要時間は、Secure Ticket Authority (STA) サーバーまたはDelivery Controllerからチケットを取得するのにかかる時間を示します (必要な場合)。この所要時間が高い場合、STAサーバーまたはDelivery Controllerが過負荷になっていることを示します。

セッション検索クライアント所要時間 (SLCD)

この所要時間は、要求された公開アプリケーションをホストするためにすべてのセッションを照会するのにかかる時間を表します。既存のセッションがアプリケーション起動要求を処理できるかどうかを判断するために、クライアントでチェックが実行されます。使用される方法は、セッションが新規か共有かによって異なります。

セッション作成クライアント所要時間 (SCCD)

この所要時間は、wfica32.exe (または同様の同等ファイル) が起動されてから接続が確立されるまでの、セッション作成にかかる時間を表します。

VDAセッション起動フェーズ

セッション起動VDA期間 (SSVD)

この期間は、VDAが起動操作全体を実行するのにかかる時間を含む、高レベルのサーバー側接続起動メトリックです。このメトリックが高い場合、セッション起動時間を増加させるVDAの問題があることを示します。これには、VDAで起動操作全体を実行するのに費やされた時間が含まれます。

資格情報取得VDA期間 (COVD)

VDAがユーザー資格情報を取得するのにかかる時間。

ユーザーが時間内に資格情報を提供できない場合、この期間は人為的に増加する可能性があります。そのため、VDA起動期間には含まれません。この時間は、手動ログインが使用され、サーバー側の資格情報ダイアログが表示される場合（またはログイン開始前に法的通知が表示される場合）にのみ重要となる可能性があります。

資格情報認証VDA期間 (CAVD)

これは、VDAが認証プロバイダーに対してユーザーの資格情報を認証するのにかかる時間です。認証プロバイダーは、Kerberos、Active Directory、またはSecurity Support Provider Interface (SSPI) のいずれかです。

グループポリシーVDA期間 (GPVD)

この期間は、ログオン中にグループポリシーオブジェクトを適用するのにかかる時間です。

ログオンスクリプト実行VDA期間 (LSVD)

これは、VDAがユーザーのログオンスクリプトを実行するのにかかる時間です。

ユーザーまたはグループのログオンスクリプトを非同期にすることを検討してください。アプリケーション互換性スクリプトを最適化するか、代わりに環境変数を使用することを検討してください。

プロファイルロードVDA期間 (PLVD)

これは、VDAがユーザープロファイルをロードするのにかかる時間です。

この期間が長い場合は、ユーザープロファイルの設定を検討してください。ローミングプロファイルのサイズと場所は、セッションの起動が遅くなる原因となります。ユーザーがターミナルサービスローミングプロファイルとホームフォルダが有効になっているセッションにログオンすると、ログオン中にローミングプロファイルの内容とそのフォルダへのアクセスがマッピングされます。これには追加のリソースが必要です。場合によっては、CPU使用率の大部分を消費することがあります。この問題を軽減するには、リダイレクトされた個人用フォルダとともに**ターミナルサービスホーム**フォルダを使用することを検討してください。一般に、Citrix環境でユーザープロファイルを管理するには、Citrix Profile Managementの使用を検討してください。Citrix Profile Managementを使用しており、ログオン時間が遅い場合は、アンチウイルスソフトウェアがCitrix Profile Managementツールをブロックしていないか確認してください。

プリンター作成VDA期間（PCVD）

これは、VDAがユーザーのクライアントプリンターを同期的にマッピングするのにかかる時間です。プリンター作成が非同期で実行されるように設定されている場合、セッション起動の完了に影響しないため、PCVDの値は記録されません。

プリンターのマッピングに過剰な時間が費やされるのは、多くの場合、プリンターの自動作成ポリシー設定が原因です。ユーザーのクライアントデバイスにローカルで追加されたプリンターの数と、印刷設定は、セッションの起動時間に直接影響する可能性があります。セッションが開始されると、Citrix Virtual Apps and Desktops™は、クライアントデバイス上のローカルにマッピングされたすべてのプリンターを作成する必要があります。特にユーザーが多くのローカルプリンターを持っている場合は、作成されるプリンターの数を減らすために、印刷ポリシーを再構成することを検討してください。これを行うには、Delivery ControllerとCitrix Virtual Apps and Desktopsでプリンター自動作成ポリシーを編集します。

ドライブマッピングVDA期間（DMVD）

これは、VDAがユーザーのクライアントドライブ、デバイス、ポートをマッピングするのにかかる時間です。

ベースポリシーに、未使用の仮想チャネルを無効にする設定が含まれていることを確認してください。たとえば、オーディオやCOMポートのマッピングなど、ICAプロトコルを最適化し、セッション全体のパフォーマンスを向上させるためです。

アプリケーション/デスクトップ起動VDA期間（ALVD/DLVD）

このフェーズは、UserinitとShellの期間の組み合わせです。ユーザーがWindowsマシンにログオンすると、winlogonがuserinit.exeを実行します。Userinit.exeはログオンスクリプトを実行し、ネットワーク接続を再確立してからExplorer.exeを起動します。Userinitは、userinit.exeの開始から仮想デスクトップまたはアプリケーションのユーザーインターフェイスの開始までの期間を表します。Shell期間は、ユーザーインターフェイスの初期化からユーザーがキーボードとマウスの制御を受け取るまでの時間です。

セッション作成VDA期間（SCVD）

この時間には、VDAでのセッション作成時間におけるその他の遅延が含まれます。

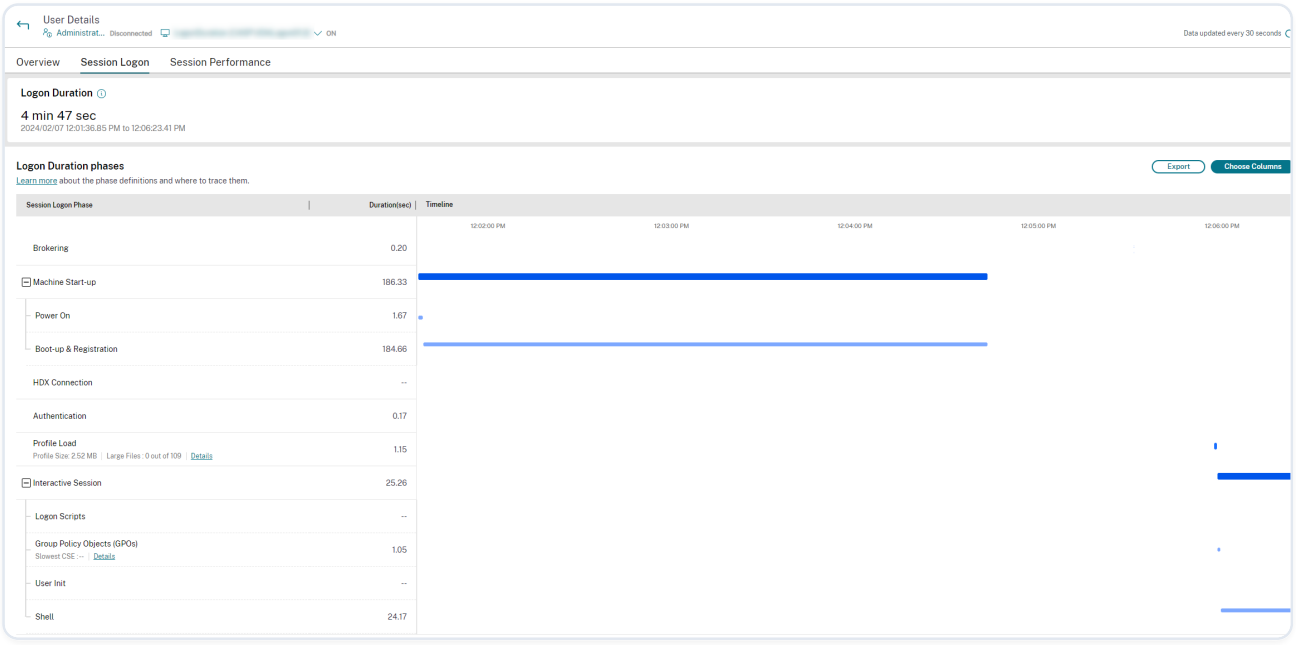
ユーザーログオンの問題を診断する

ユーザー詳細ビュー > **セッションログオン**タブには、セッションログオンプロセスの包括的なビューが表示されます。このデータを使用して、ユーザーログオンの問題をトラブルシューティングします。

ログオン期間は、HDXを使用してデスクトップまたはアプリへの初回接続に対してのみ測定されます。このデータには、リモートデスクトッププロトコルで接続しようとしているユーザーや、切断されたセッションから再接続しているユーザーは含まれません。具体的には、ユーザーが最初に非HDXプロトコルを使用して接続し、HDXを使用して再接続する場合、ログオン期間は測定されません。

ユーザーがCitrix Virtual Apps and Desktops™にログオンすると、Monitor Serviceはログオンプロセスのフェーズを追跡します。フェーズは、ユーザーがCitrix Workspace™アプリから接続した時点から、アプリまたはデスクトップが使用可能になるまでの時間で始まります。

セッションログオンタブには、さまざまなログオンフェーズがプロットされたログオン期間フェーズチャートが含まれています。ログオン期間は、Delivery Controller™から接続を確立してアプリまたはデスクトップを取得するのに費やされた時間と、仮想アプリまたはデスクトップに認証してログオンするのに費やされた時間を表します。期間情報は秒（または秒の端数）で表示されます。



ログオン期間フェーズチャートは、さまざまなログオンフェーズとその開始時刻および終了時刻を明確に示します。このチャートは、個々のログオンフェーズの重複を示しています。合計ログオン時間は、個々のログオンフェーズの期間の合計ではない場合があります。これは、個々のフェーズが重複する可能性があり、すべてのログオンフェーズがこの表現の一部ではないためです。また、特定のフェーズは、ユーザーが仮想アプリまたはデスクトップとの対話を開始した後も延長される可能性があり、この期間は全体のログオン期間の一部として測定されません。

このビューを使用して、セッション起動の遅延を引き起こしている特定のログオンフェーズを特定します。各ログオンフェーズの定義と、情報を追跡できるイベントソースは、さらなるトラブルシューティングに役立ちます。チャートにカーソルを合わせると、現在のセッションのフェーズ期間、ユーザーの7日間平均、およびデリバリーグループの7日間平均を含むツールチップが表示されます。この情報は、現在のセッションログオン期間を7日間平均値と比較するのに役立ちます。GPOおよびプロファイル詳細の場合、サブフェーズ測定にさらにドリルダウンできます。この視覚化は、ログオン期間関連の問題を簡単に理解し、トラブルシューティングするのに役立ちます。

前提条件

ログオン期間データとドリルダウンが表示されるように、次の前提条件が満たされていることを確認してください。

1. VDAに**Citrix User Profile Manager**と**Citrix User Profile Manager WMI Plugin**をインストールします。
2. Citrix Profile Management Serviceが実行されていることを確認します。
3. XenAppおよびXenDesktopサイト7.15以前の場合、GPO設定**レガシー実行リストを処理しない**を無効にします。

4. 対話型セッションのドリルダウンには、監査プロセス追跡を有効にする必要があります。
5. GPO ドリルダウンの場合、グループポリシーの運用ログのサイズを増やします。

> **注:**
>
> - ログオン時間は、デフォルトのWindowsシェル (explorer.exe) でのみサポートされ、カスタムシェルではサポートされません。
> - Remote PC Access のログオン時間は、Remote PC Access のインストール中に **Citrix User Profile Manager** および **Citrix User Profile Manager WMI Plugin** が追加コンポーネントとしてインストールされている場合にのみ利用可能です。詳細については、Remote PC Access の構成とシーケンスに関する考慮事項 のステップ4を参照してください。

ユーザーログオンの問題をトラブルシューティングする手順

1. **ユーザー詳細**ビュー > **セッションログオン**タブから、ログオン時間グラフを使用してログオン状態をトラブルシューティングします。
   - ユーザーがログオン中の場合、ビューにはログオンのプロセスが反映されます。
   - ユーザーがログオンしている場合、ログオン時間パネルには、ユーザーが現在のセッションにログオンするのにかかった時間が表示されます。
2. ログオンプロセスのフェーズを調べます。

ログオンプロセスのフェーズ

ブローカリング

ユーザーに割り当てるデスクトップを決定するのにかかった時間。

マシンの起動

セッションでマシンの起動が必要だった場合、これは仮想マシンの起動にかかった時間です。以下のサブセクションでは、異なるフェーズで仮想マシンを起動するまでにかかった時間の内訳を示します。

- **電源オン** - 仮想マシンの電源をオンにするのにかかった時間を表示します
- **起動と登録** - 仮想マシンを起動して登録するのにかかった時間を表示します

折りたたみボタンを使用して、**マシンの起動**の下にあるオプションを折りたたんだり展開したりできます。

HDX接続

クライアントから仮想マシンへのHDX接続のセットアップに必要な手順を完了するのにかかった時間。

認証

リモートセッションへの認証を完了するのにかかった時間。

GPO

仮想マシンでグループポリシー設定が有効になっている場合、これはログオン中にグループポリシーオブジェクトを適用するのにかかった時間です。GPOバーにカーソルを合わせると、CSE（クライアント側拡張）に従って各ポリシーを適用するのにかかった時間のドリルダウンがツールチップとして表示されます。



詳細をクリックすると、ポリシーの状態と対応するGPO名を示すテーブルが表示されます。ドリルダウンの時間間隔はCSEの処理時間のみを表し、GPOの合計時間には加算されません。ドリルダウンテーブルをコピーして、さらなるトラブルシューティングやレポートに使用できます。ポリシーのGPO時間はイベントビューアーログから取得されます。ログは、運用ログに割り当てられたメモリ（デフォルトサイズは4 MB）に応じて上書きされる可能性があります。運用ログのログサイズを増やす方法の詳細については、Microsoft TechNetの記事イベントログの構成を参照してください。

ログオンスクリプト

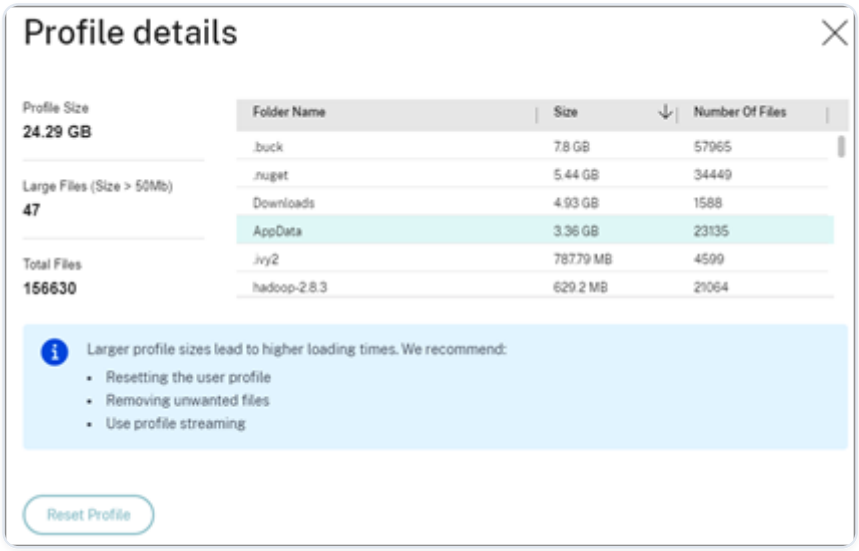
セッションにログオンスクリプトが構成されている場合、これはログオンスクリプトの実行にかかった時間です。

プロファイル読み込み

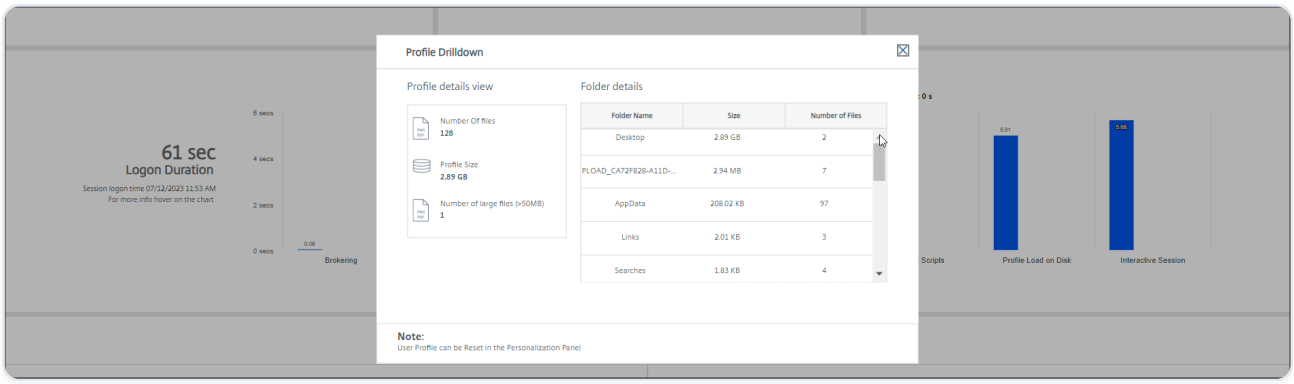
ユーザーまたは仮想マシンにプロファイル設定が構成されている場合、これはプロファイルのロードにかかった時間です。

Citrix Profile ManagementとFSLogixが構成されている場合、プロファイルロードバーには、Citrix Profile ManagementとFSLogixがユーザープロファイルを処理するのにかかった時間が含まれます。この情報は、管理者がプロファイル処理時間の長い問題をトラブルシューティングするのに役立ちます。Profile ManagementとFSLogixが構成されている場合、プロファイルロードバーには増加した期間が表示されます。この増加はこの機能強化によって引き起こされるものであり、パフォーマンスの低下を反映するものではありません。この機能強化は、VDAバージョン2407以降で利用可能です。

プロファイルロードバーにカーソルを合わせると、現在のセッションのユーザープロファイルの詳細を示すツールチップが表示されます。



「**詳細**」をクリックして、プロファイルルートフォルダー（例：C:/Users/username）内の各個別のフォルダーをさらに詳細に分析し、そのサイズとファイル数（ネストされたフォルダー内のファイルを含む）を確認します。



プロファイルのドリルダウンは、Delivery Controllerバージョン7 1811以降およびVDA 1811以降で利用できます。プロファイルのドリルダウン情報を使用すると、プロファイルの読み込み時間が長いことに関する問題を解決できます。次のことができます。

- ユーザープロファイルをリセットする
- 不要な大きなファイルを削除してプロファイルを最適化する

- ネットワーク負荷を軽減するためにファイル数を減らす
- プロファイルストリーミングを使用する

デフォルトでは、プロファイルルート内のすべてのフォルダーがドリルダウンに表示されます。フォルダーの表示を非表示にするには、VDAマシンで次のレジストリ値を編集します。

> **警告:**
>
> レジストリを誤って追加または編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤用によって生じる問題が解決されることを保証しません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

1. VDAで、HKEY_LOCAL_MACHINE\Software\Citrix\Director\ に新しいレジストリ値 **ProfileFoldersNameHidden** を追加します。
2. 値を1に設定します。この値はDWORD（32ビット）値である必要があります。これでフォルダー名の表示が無効になります。
3. フォルダー名を再度表示するには、値を0に設定します。

> **注:**
>
> GPOまたはPowerShellコマンドを使用して、複数のマシンにレジストリ値の変更を適用できます。GPOを使用してレジストリの変更を展開する方法の詳細については、ブログを参照してください。

追加情報

- プロファイルのドリルダウンでは、リダイレクトされたフォルダーは考慮されません。
- ルートフォルダー内のNTUser.datファイルは、エンドユーザーには表示されない場合があります。ただし、これらはプロファイルのドリルダウンに含まれ、**ルートフォルダー**のファイルリストに表示されます。
- AppDataフォルダー内の一部の隠しファイルは、プロファイルのドリルダウンに含まれません。
- ファイル数とプロファイルサイズデータは、特定のWindowsの制限により、パーソナライゼーションパネルのデータと一致しない場合があります。

対話型セッション

対話型セッションとは、ユーザープロファイルがロードされた後、キーボードとマウスの制御をユーザーに「引き渡す」のにかかる時間です。これは通常、ログオンプロセスのすべてのフェーズの中で最も長い期間であり、**対話型セッション期間 = デスクトップ準備完了イベントのタイムスタンプ (VDA上のEventId 1000) - ユーザープロファイルロード済みイベントのタイムスタンプ (VDA上のEventId 2)** として計算されます。対話型セッションには、Pre-userinit、Userinit、Shellの3つのサブフェーズがあります。対話型セッションにカーソルを合わせると、次の情報を示すツールチップが表示されます。

- サブフェーズ
- 各サブフェーズにかかる時間
- これらのサブフェーズ間の累積合計時間遅延

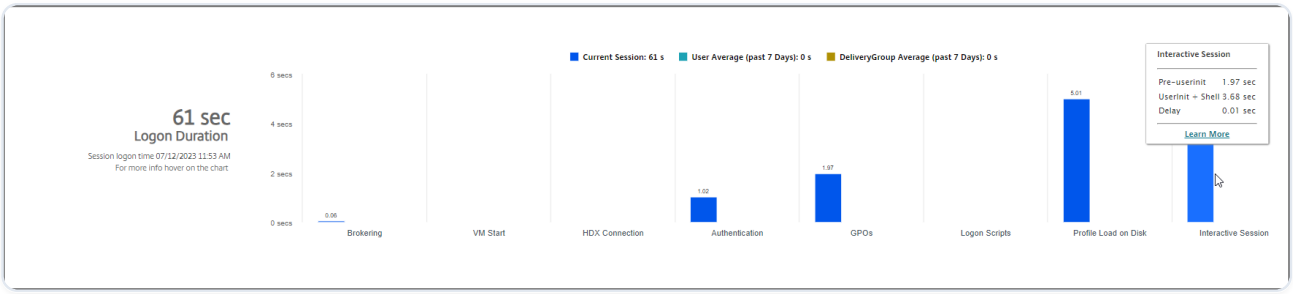
折りたたみボタンを使用して、**Interactive Session**の下にあるオプションを折りたたんだり展開したりできます。

> **注:**
>
> この機能はVDA 1811以降で利用できます。7.18より前のサイトでセッションを起動し、その後7.18以降にアップグレードした場合、「サーバーエラーのためドリルダウンが利用できません」というメッセージが表示されます。ただし、アップグレード後にセッションを起動した場合は、エラーメッセージは表示されません。

> 各サブフェーズの期間を表示するには、VM (VDA) で監査プロセス追跡を有効にします。監査プロセス追跡が無効になっている場合（デフォルト）、Pre-userinitの期間と、UserinitおよびShellの合計期間が表示されます。監査プロセス追跡は、グループポリシーオブジェクト（GPO）を介して次のように有効にできます。

1. GPOを作成し、GPOエディターを使用して編集します。
2. **コンピューターの構成 > Windows の設定 > セキュリティの設定 > ローカル ポリシー > 監査ポリシー** に移動します。
3. 右側のペインで、**プロセスの追跡の監査** をダブルクリックします。
4. **成功** を選択し、OK をクリックします。
5. この GPO を必要な VDA またはグループに適用します。

プロセスの追跡の監査、およびその有効化または無効化の詳細については、Microsoft ドキュメントのプロセスの追跡の監査を参照してください。



ユーザー詳細ビューのログオン期間パネル。

- **対話型セッション – Pre-userinit:** グループポリシーオブジェクトとスクリプトと重複する対話型セッションのセグメントです。このサブフェーズは、GPOとスクリプトを最適化することで短縮できます。
- **対話型セッション – Userinit:** ユーザーがWindowsマシンにログオンすると、Winlogonはuserinit.exeを実行します。Userinit.exeはログオンスクリプトを実行し、ネットワーク接続を再確立し、その後Windowsユーザーインターフェイスであるexplorer.exeを起動します。対話型セッションのこのサブフェーズは、Userinit.exeの開始から仮想デスクトップまたはアプリケーションのユーザーインターフェイスの開始までの期間を表します。
- **対話型セッション – Shell:** 前のフェーズでは、UserinitがWindowsユーザーインターフェイスの初期化を開始します。Shellサブフェーズは、ユーザーインターフェイスの初期化からユーザーがキーボードとマウスの制御を受け取るまでの期間を捕捉します。
- **遅延:** これは、**Pre-userinitとUserinit**サブフェーズ間、および**UserinitとShell**サブフェーズ間の累積時間遅延です。

合計ログオン時間は、これらのフェーズの正確な合計ではありません。たとえば、一部のフェーズは並行して発生し、一部のフェーズでは、合計よりも長いログオン期間になる可能性のあるより多くの処理が発生します。 合計ログオン時間には、ICAファイルのダウンロードからアプリケーションのICAファイル起動までの時間であるICA®アイドル時間は含まれません。 アプリケーション起動時にICAファイルを自動的に開くには、ICAファイルのダウンロード時にICAファイルを自動的に起動するようにブラウザーを設定します。詳細については、CTX804493を参照してください。

> **注:**
>
> ログオン期間グラフは、ログオンフェーズを秒単位で表示します。1秒未満の期間値は、サブ秒値として表示されます。1秒を超える値は、最も近い0.5秒に丸められます。グラフは、y

> 軸の最大値が200秒になるように設計されています。200秒を超える値は、バーの上に実際の値が表示されます。

データのエクスポート

セッションログオンフェーズと期間であるデフォルトのログオン期間フェーズテーブルオプションに加えて、セッションログオンページで次の列を選択することもできます。

- 開始時刻
- 終了時刻
- デリバリーグループ - 7日間平均 (秒)
- ユーザー - 7日間平均 (秒)

以前のデータを.CSVファイルにエクスポートすることもできます。

トラブルシューティングのヒント

グラフ内の異常な値や予期しない値を特定するには、現在のセッションの各フェーズにかかった時間を、このユーザーの過去7日間の平均所要時間と、このデリバリーグループ内の全ユーザーの過去7日間の平均所要時間と比較します。

必要に応じてエスカレートします。たとえば、**マシンの起動**が遅い場合、問題はハイパーバイザーにある可能性があるため、ハイパーバイザー管理者にエスカレートできます。

以下を含む異常な相違点を調べます。

- 不足している（現在の）ログオンバー
- 現在の所要時間とこのユーザーの平均所要時間の間の大きな不一致。原因は次のとおりです。
  - 新しいアプリケーションがインストールされた。
  - オペレーティングシステムのアップデートが行われた。
  - 構成変更が行われた。
  - ユーザーのプロファイルサイズが大きい。この場合、プロファイルロードが高くなります。
- ユーザーのログオン数（現在および平均所要時間）とデリバリーグループの平均所要時間の間に大きな不一致がある。

必要に応じて、「**再起動**」をクリックしてユーザーのログオンプロセスを監視し、**マシンの起動**や**ブローカリング**などの問題をトラブルシューティングします。

セッションパフォーマンスの問題を診断する

ユーザー詳細ページの**セッションパフォーマンス**タブには、HDX™ユーザーセッション内の問題を特定するのに役立つ強化されたトラブルシューティングワークフローがあります。**セッションのトポロジとパフォーマンスメトリック**パネルは、セッションのコンポーネントビューと複数のパフォーマンスメトリックを単一のビューで関連付け、セッションエクスペリエンスの問題解決にかかる平均時間を短縮します。

セッションパフォーマンスビュー(/en-us/citrix-virtual-apps-desktops/2411/media/dir-session-performance.png)

エンドツーエンドのネットワークホップビュー

エンドツーエンドのネットワークホップビューは、セッションパス全体の視覚的な表現を提供することで、トラブルシューティングを強化します。エンドツーエンドのネットワークホップビューを見つけるには、**ユーザー詳細** > **セッションパフォーマンス** > **セッションのトポロジ**をクリックします。このビューには、接続されているHDXセッションのコンポーネント、メタデータ、リンク、公開アプリケーションが表示されます。

このビューは、管理者が次のことを行うのに役立ちます。

- セッションデータフローを理解する。
- 特定のホップでのパフォーマンスボトルネックを特定する。

> **注：**
>
> パフォーマンスメトリックは、接続されているHDXセッションでのみ利用可能です。

セッションパフォーマンスメトリック

次のメトリックは、管理者が特定のセッションのパフォーマンスを理解するのに役立つように、コンテキストに応じて利用できます。ホップビューで利用可能なデータは、UIに示されている間隔で定期的に更新されます。

エンドポイントメトリック：

> **注：**

エンドポイントメトリックは、Citrix Studioポリシーを使用して管理できます。以下のポリシーはデフォルトで*有効*になっており、管理者は要件とコンプライアンスに基づいてこれらを無効にできます。

- **エンドポイント統計間隔** - Wi-Fi信号強度、ネットワークインターフェースタイプ、送受信スループット、リンク速度などのエンドポイントメトリックを管理するために使用します。
- **エンドポイント位置データ収集** - パブリックIPアドレス、国、都市、インターネットサービスプロバイダーなどのエンドポイントメトリックを管理するために使用します。

次の表に、機能、エンドポイントメトリック、およびサポートされている製品バージョンを示します。

機能名	UIパラメーター	VIRTUAL DELIVERY AGENT バージョン	WINDOWS版 CITRIX WORKSPACE™ アプリ	CITRIX WORKSPACE APP FOR MAC のバージョン	CITRIX WORKSPACE APP LINUX 版 バージョン	CITRIX WORKSPACE APP FOR HTML5 バージョン	CITRIX WORKSPACE APP FOR CHROME OS バージョン
エンドポイントネットワークの詳細	ネットワークインターフェースタイプ	2407以降	2405.10以降	2409 以降	2408 以降	2411 以降	2411 以降
	WiFi信号強度	2407 以降	2405.10以降	2409 以降	2408 以降	該当なし	該当なし
	スループット(受信/送信)	2407 以降	2405.10以降	2409 以降	2408 以降	該当なし	該当なし

機能名	UIパラメーター	VIRTUAL DELIVERY AGENT バージョン	WINDOWS版 CITRIX WORKSPACE™ アプリ	CITRIX WORKSPACE APP FOR MAC のバージョン	CITRIX WORKSPACE APP LINUX 版 バージョン	CITRIX WORKSPACE APP FOR HTML5 バージョン	CITRIX WORKSPACE APP FOR CHROME OS バージョン
	リンク速度	2407 以降	2405.10 以降	2409 以降	2408 以降	2411 以降	2411 以降
	パブリック IP アドレス	2411 以降	2409 以降	2409 以降	2408 以降	2411 以降	2411 以降
	場所 (国/都市)	2411 以降	2409 以降	2409 以降	2408 以降	2411 以降	2411 以降
	インターネットサービスプロバイダー	2411以降	2409以降	2409以降	2408以降	2411以降	2411以降
	ワークスペースの種類 (CWAアプリ/ブラウザ)	2411以降	2409以降	2409以降	2408以降	2411以降	2411以降
	アクセスタイプ (Workspace / StoreFr	2411以降	2409以降	2409以降	2408以降	2411以降	2411以降

機能名	UIパラメーター	VIRTUAL DELIVERY AGENTバージョン	WINDOWS版CITRIX WORKSPACE™アプリ	CITRIX WORKSPACE APP FOR MACのバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5バージョン	CITRIX WORKSPACE APP FOR CHROME OSバージョン
	ont 経由)						
	CPU使用率	2411以降	2409以降	2409以降	2408以降	該当なし	2411 以降
	メモリ使用率	2411 以降	2409 以降	2409 以降	2408 以降	該当なし	2411 以降
	GPU使用率	2411 以降	2409 以降	2409 以降	2408 以降	該当なし	該当なし
	ネットワーク遅延	2411 以降	2409 以降	2409 以降	2408 以降	2411 以降	2411 以降

HDXメトリック:

機能名	UIパラメーター	WINDOWS向けCITRIX WORKSPACEアプリのバージョン	VIRTUAL DELIVERY AGENTのバージョン
ICAメトリック	ICA RTT	Citrix Workspaceアプリ for Windows バージョン 2405.10 以降	シトリックス バーチャル アプリ アンド デスクトップ 2407 以降
	ICA® 遅延		

データ定義:

UIパラメーター	説明
ICA RTT	ユーザーのアクションから画面の応答までの時間（ICA遅延、エンドポイント遅延、ホスト遅延を含む）を測定します。
ICA遅延	ネットワーク遅延と潜在的な速度低下を示します。
Wi-Fi信号強度	ワイヤレス信号の品質と強度を表示します。
送受信スループット	ネットワークインターフェイスへのデータ転送速度と、ネットワークインターフェイスからのデータ転送速度を示します。
ネットワークインターフェイスの種類	イーサネット、Wi-Fi、セルラーなどのネットワーク接続の種類を指定します。
リンク速度	ネットワーク接続の最大データ転送速度を表します。
パブリックIPアドレス	インターネットサービスプロバイダーによってデバイスに割り当てられた外部IPアドレスです。
場所（国/都市）	デバイスの地理的な場所（国と都市を含む）です。
インターネットサービスプロバイダー	デバイスにインターネットアクセスを提供する会社です。
ワークスペースの種類（Citrix Workspaceアプリ/ブラウザ）	使用されているワークスペースの種類（Citrix WorkspaceアプリまたはWebブラウザのいずれか）。
アクセスタイプ（Workspace / StoreFront経由）	リソースへのアクセス方法（Citrix WorkspaceまたはStoreFrontのいずれかを通じて）。
CPU使用率	現在使用されているCPUリソースの割合。
メモリ使用率	現在使用されているメモリリソースの割合。
GPU使用率	現在使用されているGPUリソースの割合。

UIパラメーター	説明
ネットワーク遅延	ネットワークで発生する時間遅延（ミリ秒単位で測定）。

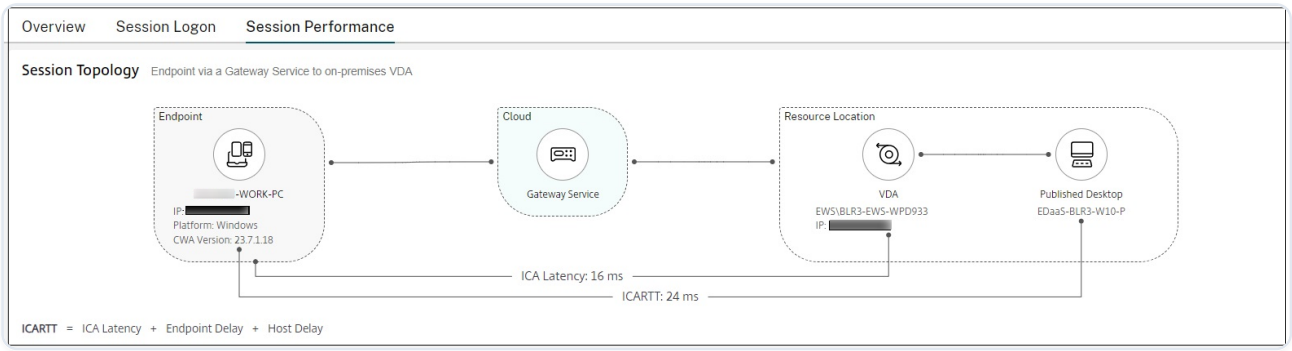
セッショントポロジのシナリオ

サイトの展開シナリオに応じて、セッションに関与するコンポーネントは以下のすべてまたは一部です。

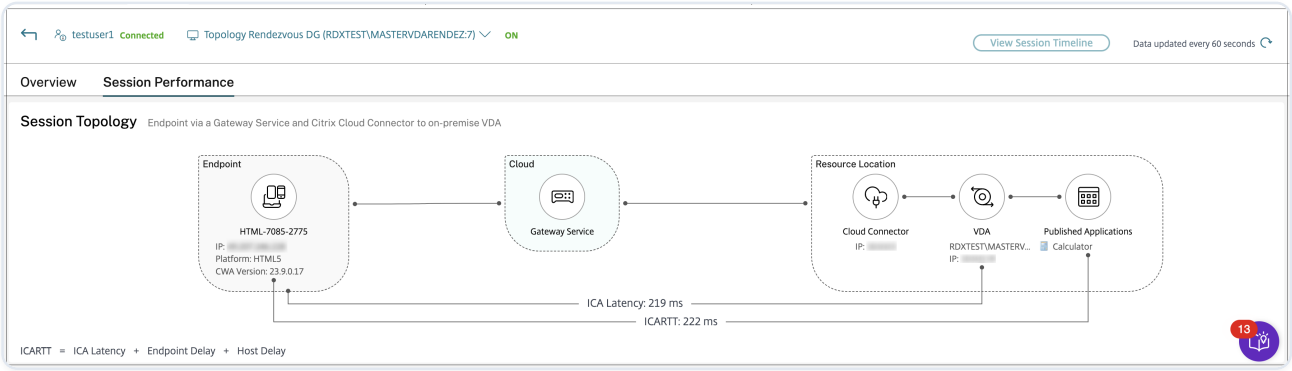
- エンドポイント上のCitrix Workspaceアプリ
- Gatewayサービス / オンプレミスGateway
- Cloud Connector – ハイブリッド接続の場合、Gateway は Cloud Connector を介して DaaS に接続されます。
- VDA

したがって、可能なネットワークトポロジは次のとおりです。

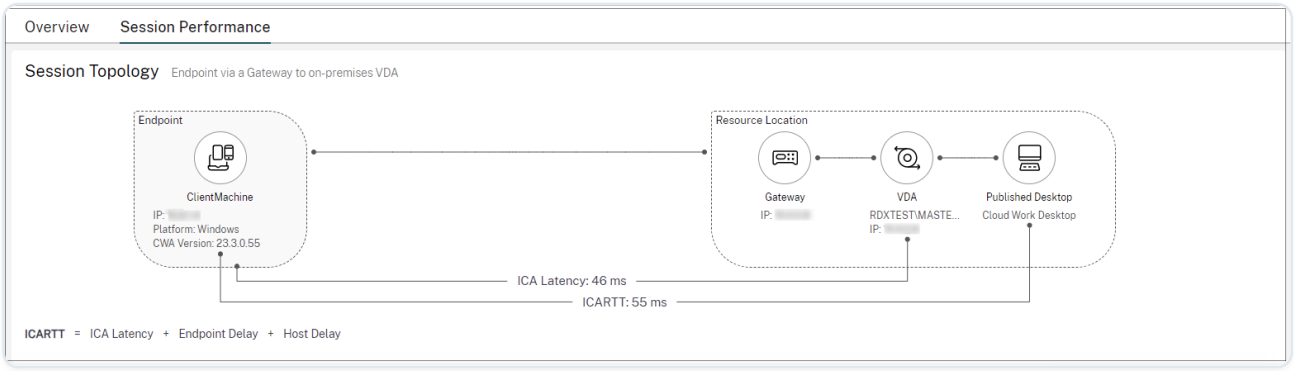
- エンドポイント上の Citrix Workspace アプリは、Citrix Workspace および Gateway Service を介してオンプレミスの VDA に接続します。VDA への接続には Cloud Connector は使用されません。



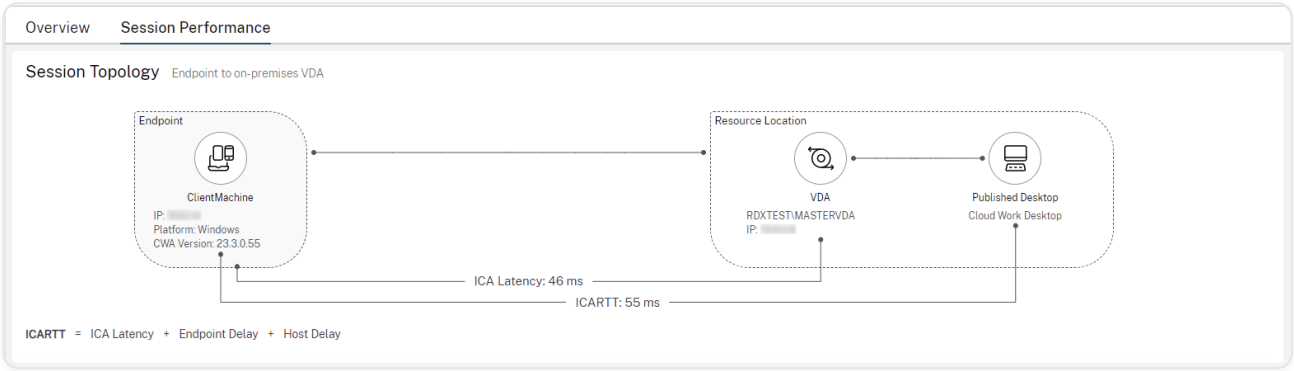
- エンドポイント上の Citrix Workspace アプリは、Citrix Workspace および Gateway Service を介して Cloud Connector 経由でオンプレミスの VDA に接続します。



- エンドポイント上の Citrix Workspace アプリは、StoreFront™ およびオンプレミス Gateway を介してオンプレミスの VDA に接続します。

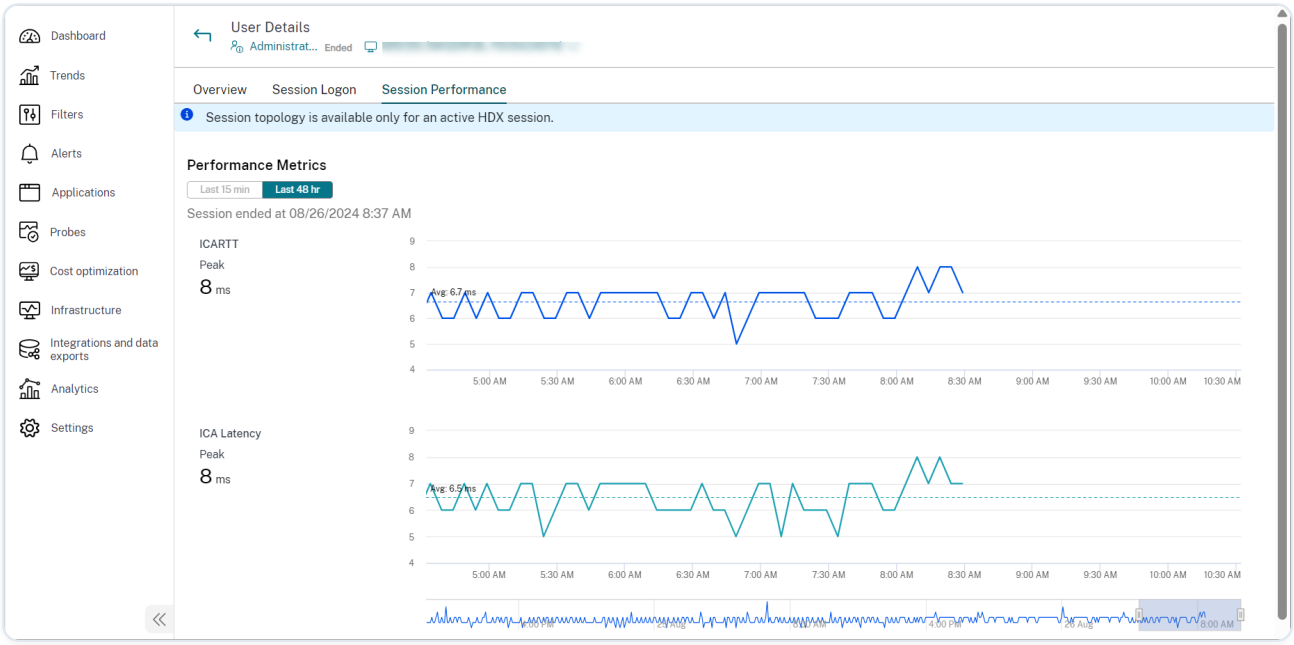


- エンドポイント上の Citrix Workspace アプリは、StoreFront を介してオンプレミスの VDA に接続します。



パフォーマンスメトリック

パフォーマンスメトリックパネルでは、リアルタイムメトリックを関連付けて、ユーザーセッション内の問題を特定できます。セッションメトリックの傾向は、これらのメトリックが時間の経過とともにどのようにパフォーマンスを発揮したかを示すのに役立ちます。**セッションパフォーマンス**タブをクリックすると、リアルタイムデータとともに、過去15分間および48時間のデータを表示できます。プロットは、複数のコンポーネントのパフォーマンスメトリックを単一のビューで関連付けるのに役立ちます。



注:

- 過去15分間のメトリックサポートにより、セッションが接続および切断されている期間のグラフがプロットされます。切断されたセッションのメトリックはゼロ値で表示されます。
- 過去48時間のメトリックサポートにより、ICARTTおよびICA待機時間のプロットは、履歴データメトリックで更新されます。

ICARTTとICA待機時間以外に、リアルタイムおよび過去15分間のメトリックとして、以下のメトリックが利用可能です。

- 1秒あたりのフレーム数 - 1秒あたりのフレーム数は、セッションの応答性を示す重要なメトリックです。
- 利用可能な出力帯域幅 - 利用可能な出力帯域幅は、VDAからエンドポイントにデータを送信するために利用可能な総帯域幅の測定値です。
- 消費された出力帯域幅 - 消費された出力帯域幅は、VDAからエンドポイントに送信され、ユーザーにセッションを表示するために使用された実際のデータ量を示します。

出力帯域幅の利用可能量と出力帯域幅の消費量を分析することで、セッションを提供するために十分な帯域幅が利用可能であるかを確認し、セッションが帯域幅不足の影響を受けているかどうかを検出するのに役立ちます。

ICA RTTまたはセッションログオン期間データが入力されない場合のトラブルシューティング

以前は、EUEMサービスまたはプロファイル管理サービスが実行に失敗した場合、ICA RTTまたはセッションログオン期間に関連するデータ取得の失敗理由が表示されませんでした。この新機能により、失敗の理由とその失敗に対する対応する解決策を取得できます。**詳細**リンクには、以下の表に示すように、ICA RTTおよびセッションログオン期間のエラー、失敗の理由、および解決策が記載されています。

エラーの種類	エラー	エラーメッセージ	解決策
ICA RTTエラー	ICA RTT値が表示されません。	**Citrix End User Experience Monitoring が実行されていません。**	1. サービスコンソールを開きます。このコンソールを開くには、**スタート**をクリックし、**サービス**と入力します。
			2. Citrix End User Experience Monitoring Service が実行されていることを確認してください。
			3. デスクトップセッションを再度開き、試してください。ICA RTT 値が表示されるはずです。
			4. 問題が解決しない場合は、Citrix 管理者にお問い合わせください。
ICA RTT エラー	ICA RTT値が表示されていません。	**Citrix End User Experience Monitoringがインストールされていません。**	1. VDAを再インストールします。
			2. サービスコンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サー

エラーの種類	エラー	エラーメッセージ	解決策
			ビス」と入力します。
			3. Citrix End User Experience Monitoringサービスが実行されていることを確認します。
			4. デスクトップセッションを再度開き、試してください。ICA RTT値が表示されるはずです。
			5. 問題が解決しない場合は、Citrix管理者に連絡してください。
ICA RTTエラー	ICA RTT値が表示されません。	**データ取得エラー。**	1. サービスコンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サービス」と入力します。
			2. **Windows Management Instrumentation サービス**が実行されていることを確認してください。
			3. また、WfShell.exe/ PicaShell.exe プロセスが **アクティビティマネージャー** > **プロセス** タブで実行され

エラーの種類	エラー	エラーメッセージ	解決策
			ていることを確認してください。実行されていない場合は、デスクトップセッションを再度開いてください。
			`4.` 上記の手順で解決しない場合は、Citrix_Euem_RoundTrip インスタンスが存在することを確認するために、次のコマンドを実行してください。`Get-CimInstance -Namespace 'ROOT\Citrix\Euem' -Query "select * from Citrix_Euem_RoundTrip"`
			`5.` Citrix_Euem_RoundTrip インスタンスが存在する場合は、デスクトップセッションを再度開いてください。
			`6.` 問題が解決しない場合は、Citrix 管理者に連絡してください。
セッションログオン期間エラー	グラフが読み込まれません。	**Citrix Profile Managementが実行されていません**	`1.` サービスコンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サー

エラーの種類	エラー	エラーメッセージ	解決策
			ビス」と入力します。
			2. **Citrix Profile Management Service**が実行されていることを確認します。
			3. デスクトップセッションを再度開き、試してください。グラフが表示されるはずです。
			4. 問題が解決しない場合は、Citrix管理者に連絡してください。
セッションログオン期間エラー	グラフが読み込まれていません。	**Citrix Profile Management がインストールされていません。**	1. Citrix Profile Management Service をインストールします。
			2. サービスコンソールを開きます。このコンソールを開くには、**［スタート］**をクリックし、「サービス」と入力します。
			3. **Citrix Profile Management Service** が実行されていることを確認します。
			4. デスクトップセッションを再度開き、試してくださ

エラーの種類	エラー	エラーメッセージ	解決策
			い。グラフが表示されるはずです。 `5.` 問題が解決しない場合は、Citrix管理者に連絡してください。
セッションログオン期間エラー	グラフが読み込まれません。	**データの取得エラー。**	`1.` **サービス**コンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サービス」と入力します。 `2.` **Windows Management Instrumentation サービス**が実行されていることを確認してください。 `3.` 前のサービスがすでに実行されている場合は、次のコマンドを実行して、`LogonTimings instance is present` を確認します: `Get-CimInstance -Namespace 'ROOT\Citrix\Profile\Metrics' -Query "select * from LogonTimings"` `4.` 問題が解決しない場合は、Citrix管理

エラーの種類	エラー	エラーメッセージ	解決策
			者に連絡してください。
ICA RTTエラー	ICA RTT値が表示されません。	コンソールはサポートされていません。	HDXを使用してセッションを開始します。
ICA RTTエラー	ICA RTT値が表示されません。	リモートデスクトッププロトコル (RDP) はサポートされていません。	HDXを使用してセッションを開始します。
ICA RTTエラー	ICA RTT値が表示されません。	詳細なエラー検出を取得し、すべての機能にアクセスするには、VDAをバージョン2402以降にアップグレードしてください。	VDAを2402以降にアップグレードしてください。
セッションログオン期間エラー	グラフがロードされていません。	Citrix Profile Management WMIプラグインがインストールされていません。	Citrix Profile Management WMIプラグインをインストールしてください。

終了したユーザーセッションの診断

Citrix Director は、アクティブ、切断、または終了状態のセッションの詳細を表示するようになりました。以前は、アクティブなセッションの詳細のみを表示できました。この機能により、ヘルプデスク管理者は、終了したセッションまたは終了状態のセッションに関する問題をトラブルシューティングできます。終了したセッションの詳細は、過去24時間および過去2日間利用できます。終了したセッションまたは終了状態のセッションの次の詳細を表示できます。

- マシン詳細パネル - 選択したセッションが起動されたマシンの利用可能な詳細を表示します。
- セッション詳細パネル - 選択したセッションの利用可能な詳細を表示します。
- セッションログオン期間 - 選択したセッションにかかったログオン期間に関する情報を表示します。以下の時間に関するグラフを表示できます。
    - ブローカリング

- マシンの起動
- HDX™ 接続
- 認証
- GPO
- ログオンスクリプト
- ディスク上のプロファイルロード
- インタラクティブセッション

> **注:**
>
> この機能は、Citrix Analytics および Performance の資格を持つ Citrix Director のお客様のみが利用できます。

過去のユーザーセッションを表示するには、次の手順を実行します。

1. **フィルター** > **セッション**ビューをクリックします。
2. 「**関連ユーザー**」をクリックして、ユーザーのActivity Managerを開きます。

   履歴ユーザーセッションのActivity Manager(/en-us/citrix-virtual-apps-desktops/2411/media/dir-his-user-sessions-am.png)
3. 「**終了したセッション**」セクションから必要なセッションを選択します。
4. 「**マシン詳細**」パネルと「**セッション詳細**」パネルを表示します。

   履歴ユーザーセッションの詳細(/en-us/citrix-virtual-apps-desktops/2411/media/dir-his-user-sessions-details.png)
5. 下にスクロールして、終了したセッションの「**セッションログオン期間**」を表示します。

   履歴ユーザーセッションの期間(/en-us/citrix-virtual-apps-desktops/2411/media/dir-his-user-sessions-duration.png)
6. 「**セッションログオン**」タブをクリックして、詳細を表示します。

   終了したユーザーセッションのログオン期間(/en-us/citrix-virtual-apps-desktops/2411/media/session-logon-ended.png)
7. 「**セッションパフォーマンス**」タブをクリックして、詳細を表示します。

終了したユーザーセッションのパフォーマンス(/en-us/citrix-virtual-apps-desktops/2411/media/session-performance-ended.png)

ユーザーのシャドウイング

Directorから、シャドウユーザー機能を使用して、ユーザーの仮想マシンまたはセッションを直接表示または操作できます。Windows VDAとLinux VDAの両方をシャドウできます。シャドウするマシンにユーザーが接続している必要があります。これは、ユーザーのタイトルバーに表示されているマシン名を確認することで検証できます。

Directorは新しいタブでシャドウイングを起動します。DirectorのURLからのポップアップを許可するようにブラウザ設定を更新してください。

シャドウイング機能は、**ユーザーの詳細**ビューからアクセスします。ユーザーセッションを選択し、アクティビティマネージャービューまたはセッションの詳細パネルで**シャドウ**をクリックします。

Linux VDAのシャドウ

シャドウイングは、RHEL7.3またはUbuntuバージョン16.04のLinuxディストリビューションを実行している、バージョン7.16以降のLinux VDAで利用できます。

注:

- シャドウイングが機能するには、VDAがDirector UIからアクセス可能である必要があります。したがって、シャドウイングはDirectorクライアントと同じイントラネット内のLinux VDAでのみ可能です。
- DirectorはFQDNを使用してターゲットLinux VDAに接続します。Directorクライアントが Linux VDAのFQDNを解決できることを確認してください。
- VDAには、python websockifyおよびx11vncパッケージがインストールされている必要があります。
- VDAへのnoVNC接続はWebSocketプロトコルを使用します。デフォルトでは、**ws://** WebSocketプロトコルが使用されます。セキュリティ上の理由から、Citrixは安全な **wss://**プロトコルを使用することを推奨します。各DirectorクライアントとLinux VDAにSSL証明書をインストールしてください。

セッションシャドウイングの指示に従って、シャドウイング用にVDAを構成してください。

1. **シャドウ**をクリックすると、シャドウイング接続が初期化され、ユーザーデバイスに確認プロンプトが表示されます。
2. マシンまたはセッションの共有を開始するには、ユーザーに**はい**をクリックするよう指示します。
3. 管理者はシャドウされたセッションを表示することしかできません。

Windows VDA のシャドウイング

Windows VDA のセッションは、Windows リモートアシスタンスを使用してシャドウイングされます。VDA のインストール時に **Windows リモートアシスタンスを使用する** 機能を有効にします。詳しくは、機能の有効化または無効化 を参照してください。

1. **シャドウ** をクリックすると、シャドウイング接続が初期化され、.msrc インシデントファイルを開くか保存するかを確認するダイアログボックスが表示されます。
2. 既定で選択されていない場合は、リモートアシスタンスビューアーでインシデントファイルを開きます。ユーザーデバイスに確認のプロンプトが表示されます。
3. ユーザーに **はい** をクリックしてもらい、マシンまたはセッションの共有を開始します。
4. より詳細な操作が必要な場合は、キーボードとマウスの制御を共有するようユーザーに依頼します。

シャドウイング用の MICROSOFT INTERNET EXPLORER ブラウザー設定の簡素化

ダウンロードした Microsoft リモートアシスタンス (.msra) ファイルをリモートアシスタンスクライアントで自動的に開くよう、Microsoft Internet Explorer を構成します。

そのためには、グループポリシーエディターで［ファイルのダウンロード時に自動的にダイアログを表示］設定を有効にする必要があります。

コンピューターの構成 \> 管理用テンプレート \> Windows コンポーネント \> Internet Explorer \> インターネットコントロールパネル \> セキュリティページ \> インターネットゾーン \> ファイルのダウンロード時に自動的にダイアログを表示。

既定では、このオプションはローカルイントラネットゾーンのサイトで有効になっています。Director サイトがこのゾーンにない場合は、手動で追加することを検討してください。

ユーザーにメッセージを送信する

Directorから、1台以上のマシンに接続しているユーザーにメッセージを送信します。この機能を使用して、デスクトップのメンテナンスの予定、マシンのログオフと再起動、プロファイルのリセットなど、管理操作に関する即時通知を送信します。

1. アクティビティマネージャービューで、ユーザーを選択し、 をクリックします。

2. ユーザー詳細ビューで、セッション詳細パネルを見つけ、 をクリックします。
3. および フィールドにメッセージ情報を入力し、 をクリックします。

メッセージが正常に送信されると、Directorに確認メッセージが表示されます。メッセージはユーザーのマシンに表示されます。

メッセージが正常に送信されない場合、Directorにエラーメッセージが表示されます。エラーメッセージに従って問題をトラブルシューティングしてください。完了したら、件名とメッセージテキストを再度入力し、 をクリックします。

アプリケーション障害の解決

アクティビティマネージャービューで、タブをクリックします。このユーザーがアクセスできるすべてのマシン上のすべてのアプリケーション（現在接続されているマシンのローカルアプリケーションとホストされたアプリケーションを含む）と、それぞれのステータスを表示できます。

> **注:**
>
> タブがグレー表示されている場合は、そのタブを有効にする権限を持つ管理者に連絡してください。
>
> このリストには、セッション内で起動されたアプリケーションのみが含まれます。

マルチセッションOSマシンおよびシングルセッションOSマシンの場合、アプリケーションは切断されたセッションごとに一覧表示されます。ユーザーが接続されていない場合、アプリケーションは表示されません。

アクション	説明
応答しないアプリケーションを終了する	応答しないアプリケーションを選択し、[アプリケーションの終了]をクリックします。アプリケーションが終了したら、ユーザーに再度起動するよう依頼します。
応答しないプロセスを終了する	必要な権限がある場合は、[プロセス]タブをクリックします。アプリケーションに関連する、または大量のCPUリソースやメモリを使用しているプロセスを選択し、[プロセスの終了]をクリックします。ただし、プロセスを終了する

アクション	説明
	のに必要な権限がない場合、プロセスを終了しようとしても失敗します。
ユーザーのマシンを再起動する	シングルセッションOSマシンのみの場合、選択したセッションで[再起動]をクリックします。または、[マシン詳細]ビューから、電源コントロールを使用してマシンを再起動またはシャットダウンします。アプリケーションを再確認できるように、ユーザーに再度ログオンするよう指示します。マルチセッションOSマシンの場合、再起動オプションは利用できません。代わりに、ユーザーからログオフし、ユーザーに再度ログオンさせます。
マシンをメンテナンスモードにする	マシンのイメージにメンテナンスが必要な場合（パッチやその他の更新など）、そのマシンをメンテナンスモードにします。マシン詳細ビューから、[詳細] をクリックし、メンテナンスモードオプションをオンにします。適切な管理者にエスカレートしてください。

セッションを復元する

セッションが切断されても、セッションはアクティブなままでアプリケーションは実行され続けますが、ユーザーデバイスはサーバーと通信しなくなります。

ユーザー詳細ビューで、**セッションの詳細**パネルのセッション障害をトラブルシューティングします。セッションIDで示される現在のセッションの詳細を表示できます。

アクション	説明
応答しないアプリケーションまたはプロセスを終了する	**アプリケーション**タブをクリックします。応答しないアプリケーションを選択し、**アプリケーションの終了**をクリックします。同様に、応答しない対応するプロセスを選択し、**プロセスの終了**をクリックします。また、異常に大量のメモリまたはCPUリソースを消費しているプロセスも終了します。これにより、CPUが使用不能になる可能性があります。

アクション	説明
Windowsセッションを切断する	**セッション制御**をクリックし、**切断**を選択します。このオプションは、ブローカーされたマルチセッションOSマシンでのみ利用可能です。ブローカーされていないセッションの場合、このオプションは無効になります。
ユーザーのセッションからログオフする	**セッション制御**をクリックし、**ログオフ**を選択します。

セッションをテストするには、ユーザーはセッションに再度ログオンを試みることができます。また、ユーザーをシャドウして、このセッションをより詳細に監視することもできます。

HDX™ チャネルシステムレポートを実行する

「**ユーザーの詳細**」ビューで、ユーザーのマシン上のHDXチャネルのステータスを「**HDX**」パネルで確認します。このパネルは、ユーザーのマシンがHDXを使用して接続されている場合にのみ利用できます。

情報が現在利用できないことを示すメッセージが表示された場合は、ページが更新されるまで1分間待つか、「**更新**」ボタンを選択します。HDXデータは、他のデータよりも更新に少し時間がかかります。

詳細については、エラーまたは警告アイコンをクリックしてください。

> ヒント:
>
> タイトルバーの左隅にある左右の矢印をクリックすると、同じダイアログボックスで他のチャネルに関する情報を表示できます。
>
> HDXチャネルシステムレポートは、主にCitrixサポートがさらなるトラブルシューティングを行うために使用されます。

1. HDXパネルで、をクリックします。
2. .xmlレポートファイルを表示または保存できます。
    - .xmlファイルを表示するには、をクリックします。.xmlファイルは、Directorアプリケーションと同じウィンドウに表示されます。

- .xmlファイルを保存するには、をクリックします。ウィンドウが表示され、Directorマシン上のファイルのダウンロード先を尋ねられます。

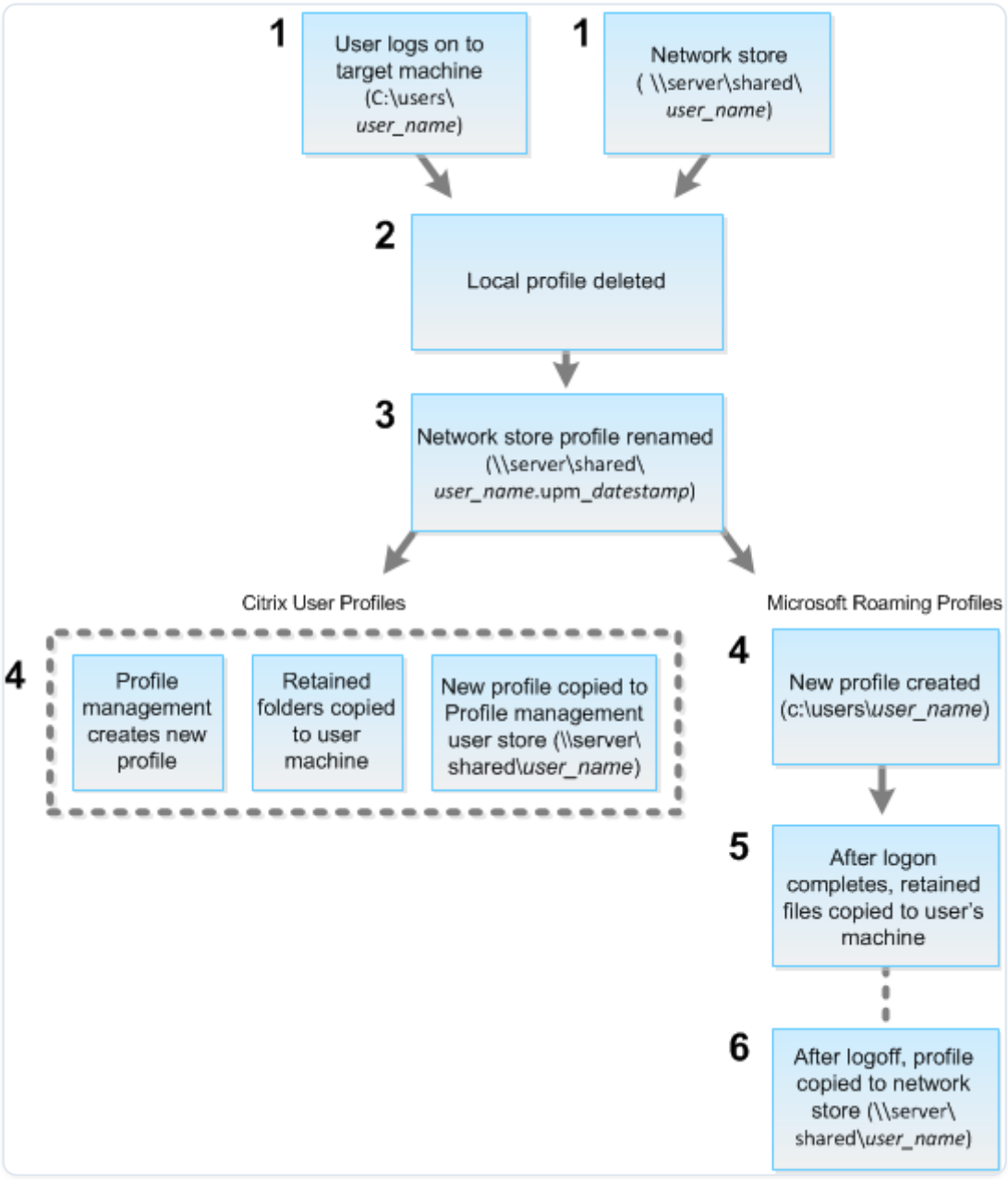
ユーザープロファイルをリセットする

> **注意:**
>
> プロファイルがリセットされると、ユーザーのフォルダーとファイルは保存され、新しいプロファイルにコピーされます。ただし、ほとんどのユーザープロファイルデータは失われます（たとえば、レジストリがリセットされ、アプリケーション設定が削除される可能性があります）。
>
> リセット機能は、ファイルベースとコンテナベースの両方のプロファイルソリューションに適用されます。

リセットされたプロファイルの処理方法

任意のCitrix®ユーザープロファイルまたはMicrosoftローミングプロファイルをリセットできます。ユーザーがログオフし、リセットコマンド（DirectorまたはPowerShell SDKを使用して）を選択すると、Directorはまず使用中のユーザープロファイルを識別し、適切なリセットコマンドを発行します。Directorは、プロファイルサイズ、種類、ログオンタイミングなどの情報をProfile Managementを通じて受け取ります。

この図は、ユーザープロファイルがリセットされた場合の、ユーザーログオン後のプロセスを示しています。



Directorによって発行されるリセットコマンドは、プロファイルの種類を指定します。その後、Profile Managementサービスはその種類のプロファイルをリセットしようとし、適切なネットワーク共有（ユーザーストア）を探します。ユーザーがProfile Managementによって処理されているにもかかわらず、ローミングプロファイルコマンドを受け取った場合、それは拒否されます（またはその逆も同様です）。

1. ローカルプロファイルが存在する場合、それは削除されます。
2. ネットワークプロファイルの名前が変更されます。
3. 次のアクションは、リセットされるプロファイルがCitrixユーザープロファイルかMicrosoftローミングプロファイルかによって異なります。

Citrixユーザープロファイルの場合、新しいプロファイルはProfile Managementのインポートルールを使用して作成されます。フォルダーはネットワークプロファイルにコピーされ、ユーザーは通常どおりログオンできます。リセットにローミングプロファイルが使用される場合、ローミングプロファイル内のレジストリ設定はリセットされたプロファイルに保持されます。必要に応じて、テンプレートプロファイルがローミングプロファイルを上書きするようにProfile Managementを構成できます。

Microsoftローミングプロファイルの場合、Windowsはプロファイルを作成し、ユーザーがログオンすると、フォルダーはユーザーデバイスにコピーされます。ユーザーが再度ログオフすると、新しいプロファイルはネットワークストアにコピーされます。

Directorでユーザープロファイルをリセットするには

Citrix Virtual Desktops™ (Desktop VDA) を使用している場合は、次の操作を行います。

1. **Director** で、プロファイルをリセットするユーザーを検索し、そのユーザーのセッションを選択します。
2. をクリックします。
3. ユーザーにすべてのセッションからログオフするよう指示します。
4. ユーザーに再度ログオンするよう指示します。 ユーザーのプロファイルから保存されたフォルダーとファイルは、新しいプロファイルにコピーされます。

Citrix Virtual Desktops (Server VDA) を使用している場合は、プロファイルのリセットを実行するためにログオンしている必要があります。その後、ユーザーはログオフして再度ログオンし、プロファイルのリセットを完了する必要があります。

> **重要:**

> ユーザーが複数のプラットフォーム（Windows 8やWindows 7など）にプロファイルを持っている場合は、ユーザーが問題として報告したのと同じデスクトップまたはアプリに最初に再度ログオンするよう指示します。このログオン操作により、正しいプロファイルがリセットされます。プロファイルがCitrixユーザープロファイルの場合、ユーザーのデスクトップが表示されるまでにプロファイルはすでにリセットされています。プロファイルがMicrosoftローミングプロファイルの場合、フォルダーの復元が短時間進行中の可能性があります。ユーザーは復元が完了するまでログオンしたままにする必要があります。

> プロファイルが正常にリセットされない場合（たとえば、ユーザーがマシンに正常に再ログオンできない、または一部のファイルが欠落している場合）は、元のプロファイルを手動で復元する必要があります。

次の点に注意してください。

- ユーザープロファイルソリューションとしてユーザーストアが有効になっている場合、新しいプロファイルには元のユーザープロファイルから次の個人用フォルダーが含まれます。
  - デスクトップ
  - クッキー
  - お気に入り
  - ドキュメント
  - 画像
  - 音楽
  - ビデオ
- Citrix Profile Managementバージョン2407以降では、プロファイルコンテナがユーザープロファイルソリューション全体として有効になっている場合、新しいプロファイルは以前の個人用フォルダーを保持します。
- Windows 8以降では、プロファイルがリセットされると、Cookieは新しいプロファイルにコピーされません。

リセットに失敗したプロファイルを手動で復元するには

1. ユーザーにすべてのセッションからログオフするよう指示します。
2. ローカルプロファイルが存在する場合は削除します。
3. フォルダー名に日付と時刻が追加された、.upm_datestamp拡張子を持つフォルダーである、ネットワーク共有上のアーカイブされたフォルダーを見つけます。
4. 現在のプロファイル名を削除します。つまり、upm_datestamp拡張子のないものです。
5. 元のプロファイル名を使用してアーカイブされたフォルダーの名前を変更します。つまり、日付と時刻の拡張子を削除します。これで、プロファイルはリセット前の元の状態に戻りました。

PowerShell SDKを使用してプロファイルをリセットするには

Broker PowerShell SDKを使用してプロファイルをリセットできます。

NEW-BROKERMACHINECOMMAND

特定のユーザー、セッション、またはマシンへの配信のためにキューに入れられたコマンドを作成します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerMachineCommand/>`を参照してください。

例

プロファイルをリセットするためにPowerShellコマンドレットを使用する方法の詳細については、以下の例を参照してください。

Profile Managementプロファイルをリセットする

- user1のプロファイルをリセットするとします。New-BrokerMachineCommand PowerShellコマンドを使用します。例:
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetUpmProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

> **重要:**
>
> `CommandData $byteArray`は次の形式である必要があります: `<SID>[,<backup path>]`。バックアップパスを指定しない場合、Profile Managementは現在の日付と時刻で名前が付けられたバックアップフォルダーを生成します。

Windowsローミングプロファイルをリセットする

- user1のローミングプロファイルをリセットするとします。New-BrokerMachineCommand PowerShellコマンドを使用します。例:
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetRoamingProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

ハイブリッドマルチクラウド展開のための統合検索

以前は、トリアージ中にDirectorでユーザーを検索すると、オンプレミスサイトのユーザーである場合にのみ、ユーザーの詳細が表示されました。ユーザーがクラウドサイトからのものである場合、Monitorに移動して再度検索する必要がありました。

この強化された検索機能により、Directorの**検索**オプションを使用して、クラウドサイトまたはオンプレミスサイトのユーザーを検索できます。この機能は、ハイブリッド展開（クラウドサイトとオンプレミスサイトの両方）を使用している場合や、トリアージ目的でDirectorを使用している場合に利用できます。オンプレミスサイトかクラウドサイトかに関わらず、ユーザーの詳細を取得できます。サイトがDirectorに存在する場合、Directorで選択したセッションのActivity Managerに直接移動できます。サイトがDirectorに存在しない場合、Monitorで選択したセッションのActivity Managerに直接移動できます。その後、トリアージを続行できます。

> **注記:**
>
> Citrix Directorを介して統合検索コンソールを使用できます。
>
> この機能により、問題解決までの平均時間が短縮され、クラウドユーザーとオンプレミスユーザーの両方に単一のコンソールでシームレスなエクスペリエンスを提供します。追加の利点として、Directorにはクラウドサイトの詳細のみが追加されるため、データベースのサイズが急激に増加することはありません。ユーザーの詳細はクラウド自体に保存されます。

> **注記:**
>
> 最大6つ以下のクラウドサイトの場合、3秒以内に検索結果を取得できます。
>
> この機能を有効にするには、クラウドサイトをDirectorに接続する必要があります。

クラウドサイトをDirectorに接続する

前提条件

Citrix Directorで統合検索を構成するために、新しいコンポーネントをインストールする必要はありません。次の要件が満たされていることを確認してください。

- Directorに存在するサイトの1つは2407以降である必要があります。他のサイトは2402以降でも構いません。
- 統合検索の場合、すべてのDelivery ControllerおよびDirectorがインストールされているマシンで、アウトバウンドインターネットアクセスが利用可能である必要があります。具体的には、次のURLへのアクセスが可能であることを確認してください。

  - Citrix キー登録: `<https://*.citrixnetworkapi.net/>`
  - シトリックスクラウド: `<https://*.citrixworkspacesapi.net/>`
  - シトリックス DaaS: `<https://*.cloud.com/>`
  - マイクロソフト アジュール: `<https://*.windows.net/>`

- Delivery ControllerおよびDirectorマシンがイントラネット内にあり、アウトバウンドインターネットアクセスがプロキシサーバーを介している場合は、次のことを確認してください。

  - プロキシサーバーは、上記のURLリストを許可する必要があります。
  - Directorの **web.config** および **citrix.monitor.exe.config** ファイルに以下の構成を追加します。この構成は **configuration** タグ内に必ず追加してください。

```
<system.net>

    <defaultProxy>

        <proxy usesystemdefault="false" proxyaddress="http://
<your_proxyserver_address>:80" bypassonlocal="true" />

    </defaultProxy>

</system.net>
```

  - Directorの **web.config** は、Directorがインストールされているマシンの `C:\inetpub\wwwroot\Director\web.config` にあります。
  - **citrix.monitor.exe.config** は、Delivery Controllerがインストールされているマシンの `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` にあります。

  この設定は、IIS上のMicrosoftによって提供されます。詳細については、「プロキシ構成」を参照してください。構成ファイルの **defaultproxy** フィールドは、DirectorおよびMonitor Serviceのアウトバウンドアクセスを制御します。Citrix DaaSとの構成および通信には、**defaultproxy** フィールドをtrueに設定する必要があります。適用されているポリシーによってこのフィールドがfalseに設定されている可能性があります。この場合、手動でフィールドをtrueに設定する必要があります。変更を行う前に構成ファイルのバックアップを取ってください。変更を有効にするには、Delivery Controllerで監視サービスを再起動してください。

- DaaSのCitrix Cloud™エンタイトルメントがアクティブであること。

- お使いのCitrix Cloudアカウントは、製品登録エクスペリエンスに対する権限を持つ管理者アカウントであること。管理者権限の詳細については、「管理者権限の変更」を参照してください。
- Citrix Directorがインストールされているマシンにインターネットアクセスがあることを確認してください。
- Citrix Cloudサービスを使用するには、HTTPSポート443を介して必要なCitrixアドレスに接続できる必要があります。詳細については、「インターネット接続要件」を参照してください。
- 製品登録を実行するための完全な管理者アクセス権があることを確認してください。

構成手順

1. Directorにフル管理者としてサインインします。Directorダッシュボードページが表示されます。
2. **設定**タブをクリックします。**設定**ページが表示されます。

   統合検索サイト設定(/en-us/citrix-virtual-apps-desktops/2411/media/unified-search-settings.png)
3. **クラウドサイトの追加**をクリックします。次のページが表示されます。

   統合検索サイトの追加(/en-us/citrix-virtual-apps-desktops/2411/media/unified-search-cloud-site.png)
4. 前提条件を確認し、その後、**クラウドサイトの接続**をクリックして構成プロセスを開始します。このサイトをCitrix Cloudに登録するために使用する、一意の8桁の登録コードが生成されます。

   統合検索コード(/en-us/citrix-virtual-apps-desktops/2411/media/unified-search-code.png)
5. コードをコピーするには**コードのコピー**をクリックし、その後、**Citrix Cloudで登録**をクリックします。Citrix Cloudの登録URLにリダイレクトされます。
6. Citrix Cloudの資格情報でサインインし、顧客を選択します。
7. コピーした登録コードをCitrix Cloudの**製品登録**ページに貼り付けます。サイトを登録するには**続行**をクリックします。

   統合検索コードの入力(/en-us/citrix-virtual-apps-desktops/2411/media/unified-search-enter-code.png)
8. **続行**をクリックします。クラウドサイトがCitrix Directorに登録され、次のメッセージが表示されます。

統合検索登録成功(/en-us/citrix-virtual-apps-desktops/2411/media/unified-search-reg-success.png)

9. **閉じる**をクリックします。次の画面が表示されます。

   統合検索接続済み(/en-us/citrix-virtual-apps-desktops/2411/media/unified-search-connected.png)

10. Directorで複数のクラウドサイトを構成するには、Directorから各サイトについて前述の構成手順を繰り返します。

    サイトごとに複数のDirectorインスタンスが実行されている場合は、いずれかのDirectorインスタンスから構成します。構成プロセスが完了したら、管理者はサインアウトし、他のDirectorインスタンスにサインインし直して、接続されているクラウドサイトを確認する必要があります。

> **注:**

> サイトをCitrix Directorから切断するには、**Remove site** をクリックします。このオプションは既存の構成を削除します。

ハイブリッド展開からのユーザー検索

ユーザーを検索するには、次の手順を実行します。

1. 上部のナビゲーションバーで「**検索**」をクリックします。「**展開の監視とトラブルシューティング**」ページが表示されます。

   統合検索サイト(/en-us/citrix-virtual-apps-desktops/2411/media/unified-search-site.png)

2. ドロップダウンリストから「**ユーザー**」を選択し、ユーザー名を入力します。オンプレミスおよびクラウド展開からのアクティブなセッションと失敗したセッションのリストが表示されます。

   統合検索 - 完了(/en-us/citrix-virtual-apps-desktops/2411/media/unified-search-done.png)

3. 検査するセッションを選択します。

- クラウド展開を使用しているセッションの場合、ユーザーコンテキストを含む関連するDaaS Monitor URLが**「アクティビティマネージャー」**ページで開かれ、トラブルシューティングを迅速に開始できます。

- オンプレミス展開を使用しているセッションの場合、「アクティビティマネージャー」ページがすぐに開かれ、トラブルシューティングを開始できます。

インフラストラクチャの監視

Director は現在、Citrix Virtual Apps and Desktops™ コンポーネントの運用状況を可視化します。この機能は、インフラストラクチャに関連する問題を簡単に特定、トラブルシューティング、解決するのに役立ちます。現在、以下のコンポーネントの健全性が監視されています。

- デリバリーコントローラー™
- シトリックス プロビジョニング™ サービス
- StoreFront™

この機能をサポートするために、Citrix コンポーネント向けに `citrixinframonitor.msi` という新しい Windows 実行可能ファイルが導入されました。これにより、Provisioning Service または StoreFront サーバーから Director への関連する健全性メトリックの収集と送信が容易になります。ただし、Delivery Controller の監視には `CitrixInfraMonitor.msi` は必要ありません。Delivery Controller コンポーネントは、Citrix Virtual Apps and Desktops サイトに接続されると、監視のために自動的にオンボーディングされます。

この機能により、Director の単一ダッシュボードで、Delivery Controller、Provisioning Service、StoreFront サーバーに関する重要な監視データセットとプロアクティブなアラートを取得できます。最新の情報を確保するため、監視対象コンポーネントから5分ごとにデータが収集されます。

この機能は、プロアクティブな監視、詳細なメトリック、自動アラートを提供することで運用効率の向上を目指し、Citrix® インフラストラクチャがスムーズかつ効率的に稼働することを保証します。

主な機能

リアルタイム監視:

- Delivery Controller、Citrix Provisioning (Provisioning Service) サーバー、StoreFront などの Citrix インフラストラクチャコンポーネントの継続的な監視。
- システムの状態、リソース使用率、関連するパフォーマンスメトリックを表示するダッシュボードビュー。

詳細な分析:

- 各コンポーネントの接続ステータス、サービスまたはプロセスステータスなどのシステム健全性メトリックに関する詳細な分析を提供します。

- CPU、メモリ、ディスク使用率などのリソース使用率メトリックの詳細。

自動アラートと通知:

- さまざまなメトリックと状態に対して、きめ細かなスコープでカスタマイズ可能なアラートしきい値。
- メールとWebhookによるリアルタイム通知。

ユースケース

運用効率:

Citrix管理者チームがCitrixサーバーとサービスの高可用性とパフォーマンスを維持できるようにします。この機能は、重大なユーザーグループに影響を与える前に問題を事前に特定して管理者に警告することで、ダウンタイムを最小限に抑えるのにも役立ちます。

チケット解決の高速化:

サーバーの健全性とパフォーマンスに関する主要なメトリックを監視し、仮想アプリケーションとデスクトップのユーザーへの最適な配信を評価します。これらのメトリックを使用して、関連するコンポーネントを分析することで、パフォーマンスに関連するユーザーの苦情を診断し、解決します。

前提条件

- Citrix Virtual Apps and Desktopsバージョン2407以降
- Provisioning Serviceの前提条件またはStoreFrontの前提条件が満たされていることを確認してください。
- Citrix Provisioningを監視する場合:
  - **DB接続**と**ライセンスサーバー到達可能性**を監視するために必要な最小バージョンはCitrix Provisioning 2407です。
  - **PXEサービス**、**TFTPサービス**、および**合計再接続数**を監視するために必要な最小バージョンはCitrix Infra Monitor 2411です。
- Citrix Infrastructure Monitorを実行するために必要なユーザーアカウントまたは権限:
  - エンドポイントマシンにCitrix Infrastructure Monitorをインストールするための Windows管理者権限を持つユーザーアカウント。
  - 次のDirector権限を持つフル管理者ユーザーアカウントまたはカスタムロール：

- アラートポリシーの作成\編集\有効化\削除
- アラートメールサーバー構成の作成\編集\削除
- Citrixコンポーネントへの接続の作成\編集\管理 (インフラ監視)
- アラートの無視
- アラートポリシーの表示
- アラートの表示
- ダッシュボードページの表示
- インフラストラクチャモニターページの表示

注：

- 前述の前提条件は、Provisioning ServiceおよびStoreFrontコンポーネントの監視にのみ有効です。
- **アラート**ページにアクセスする権限がない場合、**インフラストラクチャ監視**ページで**アラートの管理**オプションが無効になります。

詳細については、以下を参照してください。

- インフラストラクチャ監視の概要
- 接続の管理
- インフラストラクチャダッシュボード
- 高度なアラートポリシー
- インフラストラクチャポリシー

インフラストラクチャ監視の概要

注：

以下の2つの手順は、Provisioning ServiceおよびStoreFront™コンポーネントの監視にのみ有効です。

ステップ1：Citrix Infrastructure Monitorのインストール

安全なデータ収集のための接続を確立するには、ターゲットコンポーネントへのインストールを完了するために、以下の手順を実行します。

> **注：**
>
> Citrix Infrastructure Monitorをインストールするマシンには、すでにProvisioning ServiceまたはStoreFrontのいずれかがインストールされている必要があります。

ステップ1.1：ターゲットコンポーネントの特定

監視が必要なProvisioning ServiceやStoreFrontサーバーなどのターゲットコンポーネントを特定します。

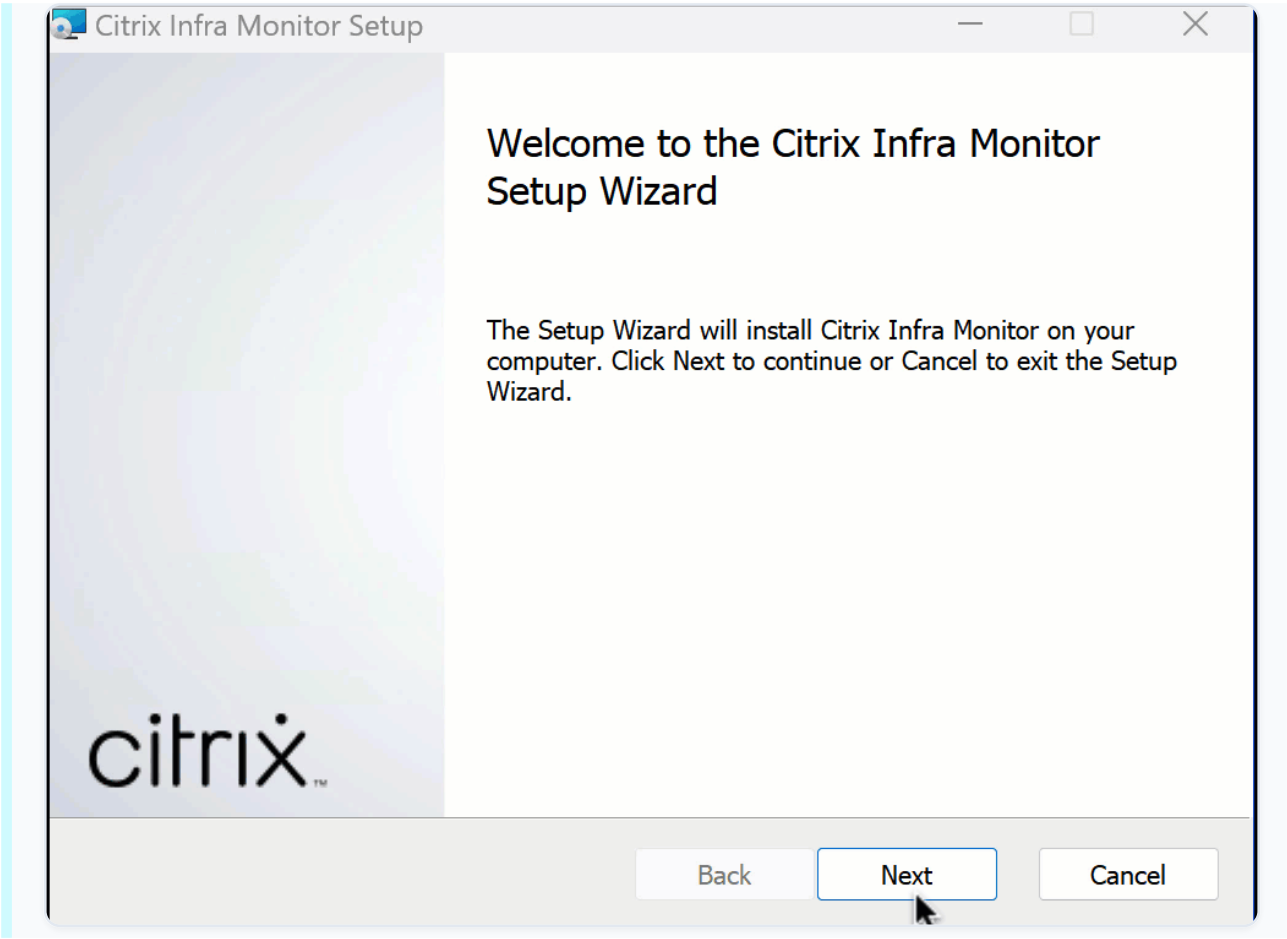
ステップ1.2：Citrix Infrastructure Monitorのダウンロード

ステップ 1.1で特定されたターゲットサーバーのCitrixダウンロードページから `CitrixInfraMonitor.msi` をダウンロードできます。

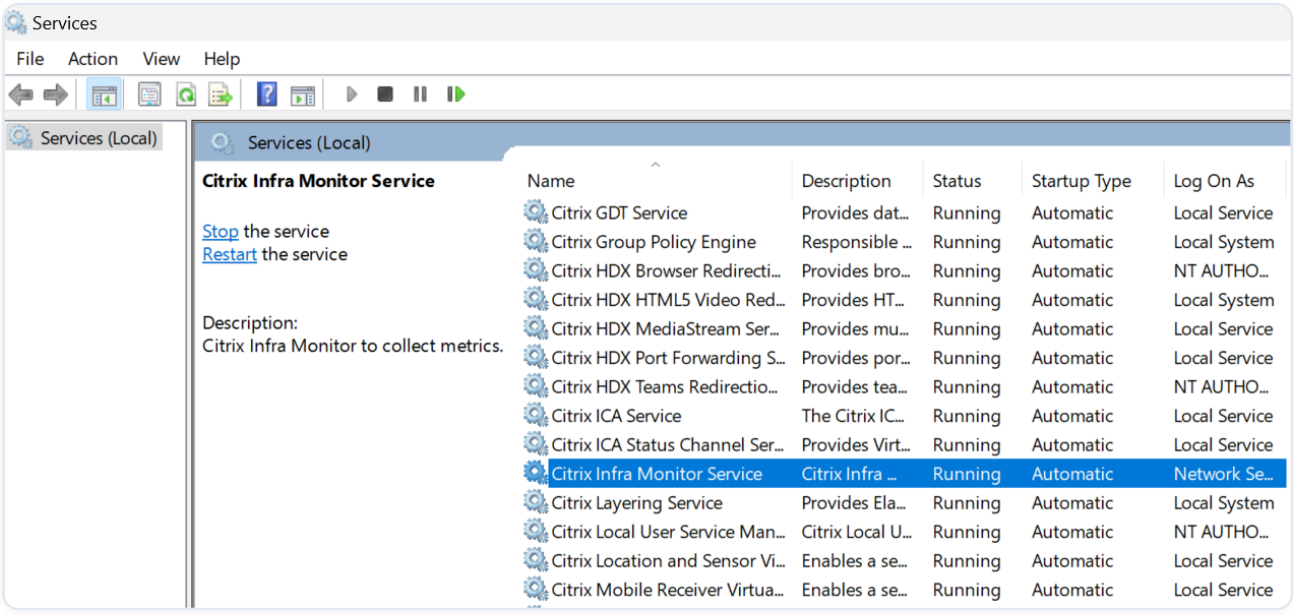
ステップ1.3：Citrix Infrastructure Monitorの実行

インストールウィザードの指示に従って、ターゲットコンポーネントで `CitrixInfraMonitor.msi` インストーラーを実行します。

> **注：**
>
> 管理者権限を持つユーザーは、ターゲットコンポーネントにCitrix Infrastructure Monitorをインストールおよび構成できます。



インストールが正常に完了すると、**サービス**セクションでCitrix Infrastructure Monitor Serviceを表示できます。



ステップ 1.4: 登録トークンを取得する

Citrix Infrastructure Monitorがインストールされているシステムで、`C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt`にある

`RegistrationToken.txt`ファイルで提供されているトークンを取得し、ステップ 2: Citrix Infrastructure Monitorを登録するで使用できるように準備しておきます。

ポート要件

`CitrixInfraMonitor.msi`を正常にインストールすると、インストーラーは9595ポートの例外を作成します。サードパーティのファイアウォールを使用している場合は、Citrix Infrastructure Monitoringサービスを使用するために、このポートのTCP通信を手動で許可する必要がある場合があります。

次の表は、Provisioning ServiceおよびStoreFrontマシンに対するインバウンドポート要件の詳細を示しています。

送信元	宛先	種類	ポート	プロトコル	目的
DDC	Provisioning Serviceまたは StoreFront マシン	TCP	9595	HTTPまたは HTTPS	Provisioning Serviceまたは StoreFront マシンからメトリックを収集するための呼び出し。

注:

Provisioning ServiceおよびStoreFrontマシンは、Infrastructure Monitoringサービスに対してアウトバウンド呼び出しを行いません。

ステップ2：Citrix Infrastructure Monitorを登録する

Citrix Infrastructure Monitorは、以下の方法で登録できます。

- ディレクターユーザーインターフェース
- PowerShell SDK

Director UI から

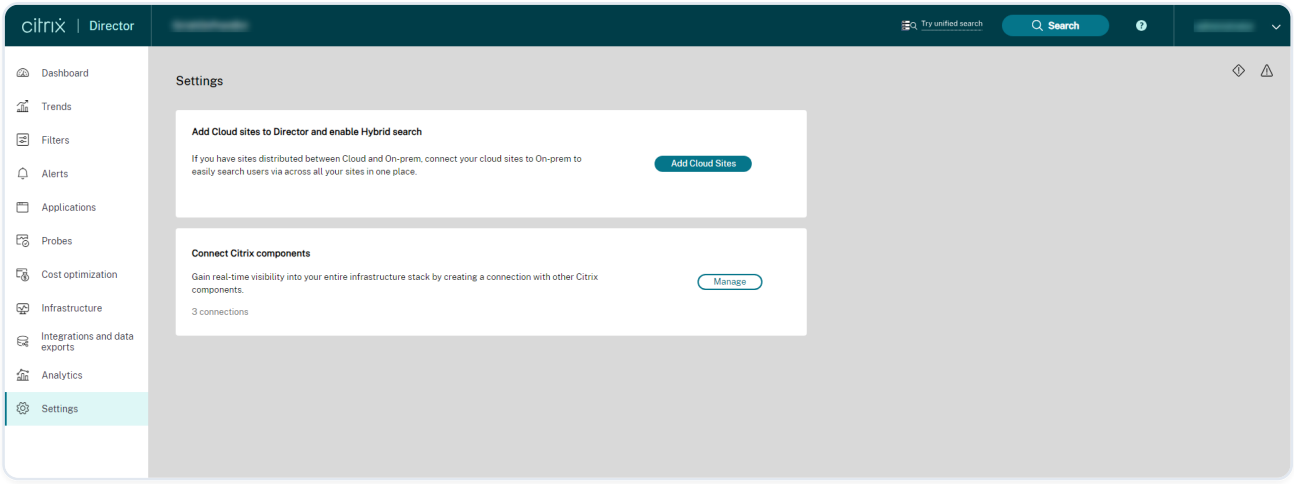
次の手順で Director UI で登録を完了します。

ステップ 2.1: 「CITRIX コンポーネントの接続」ページに移動する

［設定］ > **［Citrix コンポーネントの接続］** > **［管理］** の順にクリックします。

または、,

> をクリックします。



](/en-us/citrix-virtual-apps-desktops/2411/media/connect-citrix-components.png)

ステップ2.2: コンポーネントの詳細を入力する

画面で、 をクリックします。 ウィンドウが表示されます。

](/en-us/citrix-virtual-apps-desktops/2411/media/create-a-connectiOn.png)

`CitrixInfraMonitor.msi` がターゲットにダウンロードされ、インストールされていることを確認します。詳しくは、このドキュメントのステップ1 を参照してください。画面の指示に従い、安全な接続を確立するために必要なコンポーネントの詳細を入力します。

- ドロップダウンリストからコンポーネントの種類を選択します。コンポーネントは Provisioning Service または StoreFront です。
- ホスト名を入力します。
- ドメイン名を入力します。
- Provisioning Service または StoreFront マシンのユーザー名を入力します。
- Provisioning Service または StoreFront マシンのパスワードを入力します。

ステップ2.3: 接続を承認する

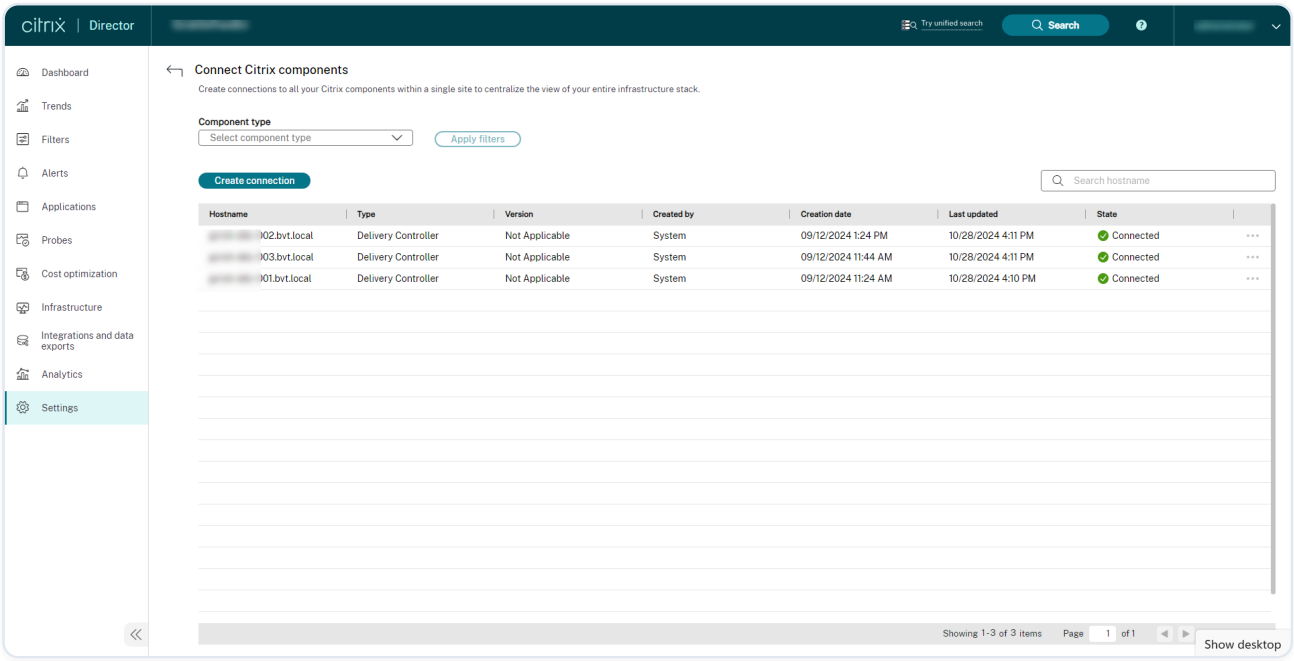
Citrix Infrastructure Monitorがインストールされているシステムの `C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt` にある `RegistrationToken.txt` ファイルからCitrix Infrastructure Monitorトークンを取得します。

取得したトークンの詳細をDirector UIに入力します。このトークンは、サイトとコンポーネント間の接続を認証します。

`RegistrationToken.txt`ファイルに存在するトークンテキストは、Citrix Infrastructure Monitorサービスを再起動すると再生成されます。登録が成功すると、トークンファイルはマシンから削除されます。何らかの理由で新しいトークンファイルを再作成する必要がある場合は、Citrix Infrastructure Monitorサービスを再起動してください。セキュリティ上の理由から、無効なトークンによる登録試行が3回失敗すると、トークンファイルは削除されます。

ステップ 2.4: 接続を作成する

詳細が入力されたら、**作成**をクリックします。作成された接続は、**Citrixコンポーネントの接続**ページにある接続リストで利用可能です。



リモート PowerShell SDK の使用

前提条件：

- Citrix Infrastructure Monitor が StoreFront または PVS マシンにインストールされていることを確認します。

PVSまたはStoreFrontマシンと通信するために、DDCにCitrix Infrastructure Monitorを登録します。この登録は、PVSまたはStoreFrontマシンで収集されたインフラストラクチャの健全性メトリックをDDCに送信するためのものです。

Citrix Infrastructure Monitorに登録するには、Delivery Controller™で以下のPowerShellコマンドを実行します。

```
Add-MonitorDirectorAgent -Fqdn <FQDN of component> -Component <component>
-Domain <domain> -Username <username> -Password <password> -Token <token>
```

注:

ユーザー名とパスワードはオプションのパラメーターです。ただし、これらのパラメーターを指定しない場合、一部のメトリックは利用できません。

上記のコマンドのパラメーターは次のとおりです。

パラメーター	説明
`Fqdn`	PVS または StoreFront サーバーの FQDN。
`Component`	オンボーディングするコンポーネント。例: PVS または SF。PVS は Citrix Provisioning™ を表し、SF は StoreFront を表します。
`Domain`	すべてのコンポーネントが属するドメイン。
`Username`	管理者ユーザーのユーザー名。
`Password`	管理者ユーザーのパスワード。
`Token`	Citrix Infrastructure Monitorがインストールされているシステムで、`C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt` にある `RegistrationToken.txt` ファイルからCitrix Infrastructure Monitorトークンを取得します。

注:

- Citrix Infrastructure Monitorサービスを再起動すると、`RegistrationToken.txt` ファイルに存在するトークンテキストが再生成されます。登録が成功すると、トークンファイ

ルはマシンから削除されます。再登録が必要な場合は、Citrix Infrastructure Monitorサービスを再起動してください。

- セキュリティ上の理由から、無効なトークンによる登録試行が3回失敗すると、トークンファイルは削除されます。

PVSまたはStoreFrontマシンを正常に登録すると、マシン名の詳細が**Director** > **インフラストラクチャ**タブに表示されます。

Citrix Infrastructure Monitorに登録するためのコマンド例は次のとおりです。

インフラモニターを再起動(/en-us/citrix-virtual-apps-desktops/2411/media/sm-sample-comand-im-register-on-prem.png)

Citrix Infrastructure MonitorのHTTPSを構成する手順

注:

Citrix Infrastructure MonitorサービスはHTTPモードでも動作し、この場合、以下の構成は不要です。ただし、HTTPSモードでの使用をお勧めします。Citrix Infrastructure MonitorのHTTPSを構成する必要がある場合にのみ、以下の手順を実行してください。

ステップ1：証明書をマシンにアップロードする

1. Citrix Infrastructure Monitorがインストールされているマシン用の`PFX`証明書を取得します。PFXファイルの生成の詳細については、「PFXファイルの作成方法」を参照してください。

   注:

   パスワードで保護されたPFXファイルも使用できます。

2. 証明書をマシンの任意の場所にアップロードします。

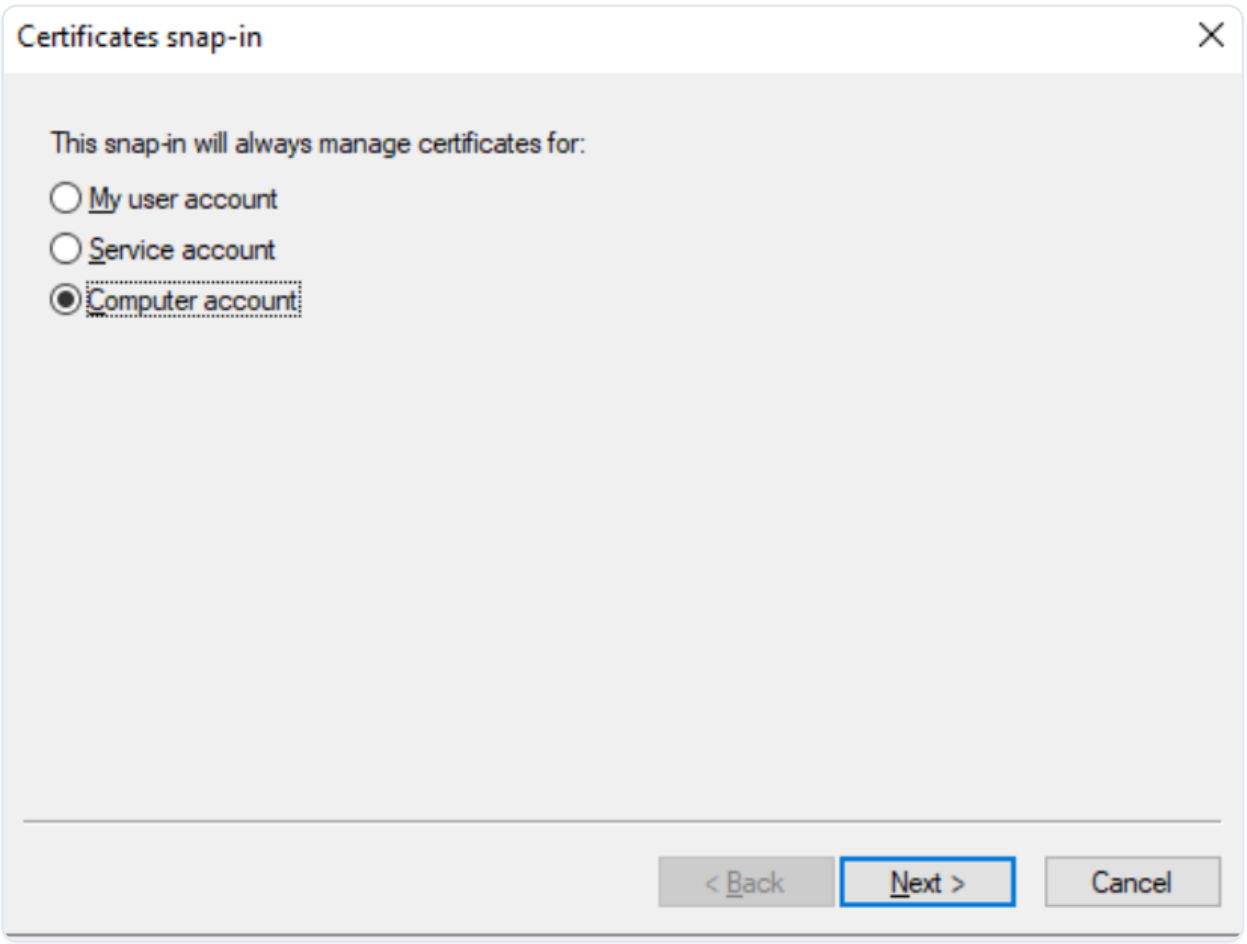
ステップ2：証明書をコンピューター証明書にインポートする

1. **スタート** > **ファイル名を指定して実行**をクリックし、`mmc`と入力して**OK**をクリックします。**コンソール1 - **ウィンドウが表示されます。

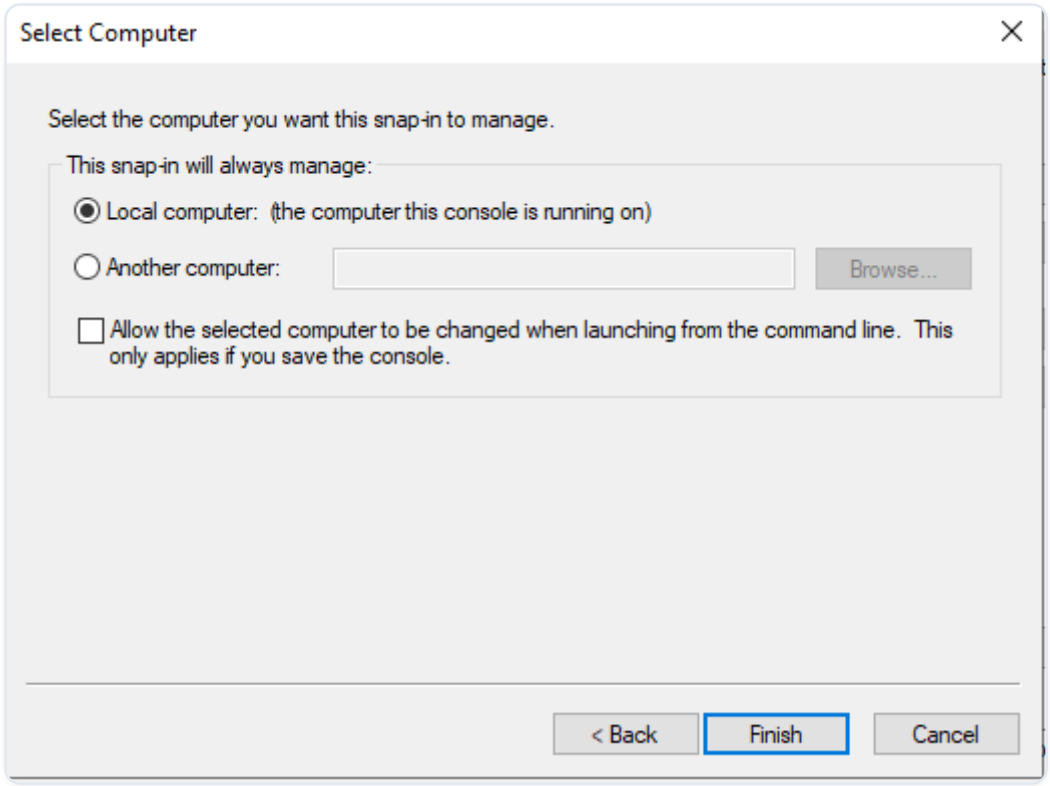
2. **ファイル**メニューで、**スナップインの追加と削除**をクリックします。**スナップインの追加と削除**ウィンドウが表示されます。

   スナップインの追加と削除(/en-us/citrix-virtual-apps-desktops/2411/media/sm-add-or-remove-snap-in.png)

3. 「**スナップイン**」の下にある「**証明書**」をダブルクリックします。「**証明書スナップイン**」ウィンドウが表示されます。

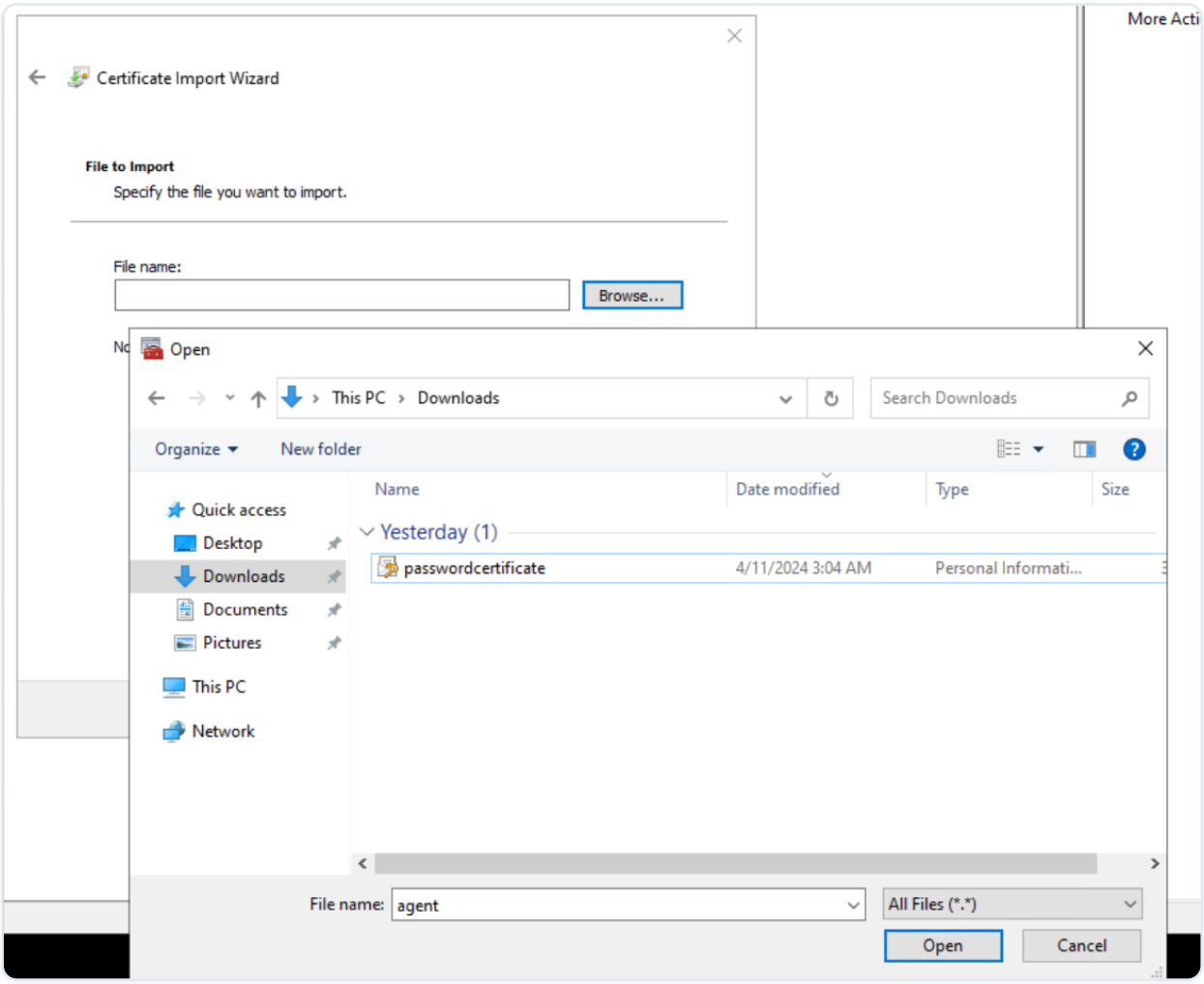


4. 「**コンピューターアカウント**」を選択し、「**次へ**」をクリックします。「**コンピューターの選択**」ウィンドウが表示されます。



5. 「**ローカルコンピューター**」を選択します。
6. 「**完了**」をクリックします。新しいコンソールの選択されたスナップインのリストに、「**証明書 (ローカルコンピューター)**」セクションが表示されます。
7. **OK**をクリックします。
8. 「**証明書**」を展開し、「**個人**」を右クリックして「**すべてのタスク**」>「**インポート**」を選択します。「**証明書のインポートウィザードへようこそ**」が表示されます。

   証明書の展開(/en-us/citrix-virtual-apps-desktops/2411/media/sm-expand-certificate.png)
9. 「**次へ**」>「**ファイルの参照**」を選択します。PFXファイルをアップロードした場所に移動し、ファイルの種類を「**すべてのファイル**」に変更して、該当するPFX証明書を選択します。



10. PFXパスワードを入力します。パスワードがない場合は空白のままにできます。
11. 「**次へ**」をクリックします。
12. 証明書ストアについては、「**すべての証明書を次のストアに配置する**」オプションが選択されており、「**証明書ストア**」が「**個人**」として選択されていることを確認します。

    証明書ストア(/en-us/citrix-virtual-apps-desktops/2411/media/sm-certificate-store.png)
13. **Next**をクリックします。
14. 詳細を確認し、**完了**をクリックします。
15. 確認を待ちます。「*インポートは正常に完了しました*」というメッセージが表示されます。
16. **証明書** > **個人**に移動し、証明書が存在することを確認します。
17. マシンからPFX証明書ファイルを削除します。

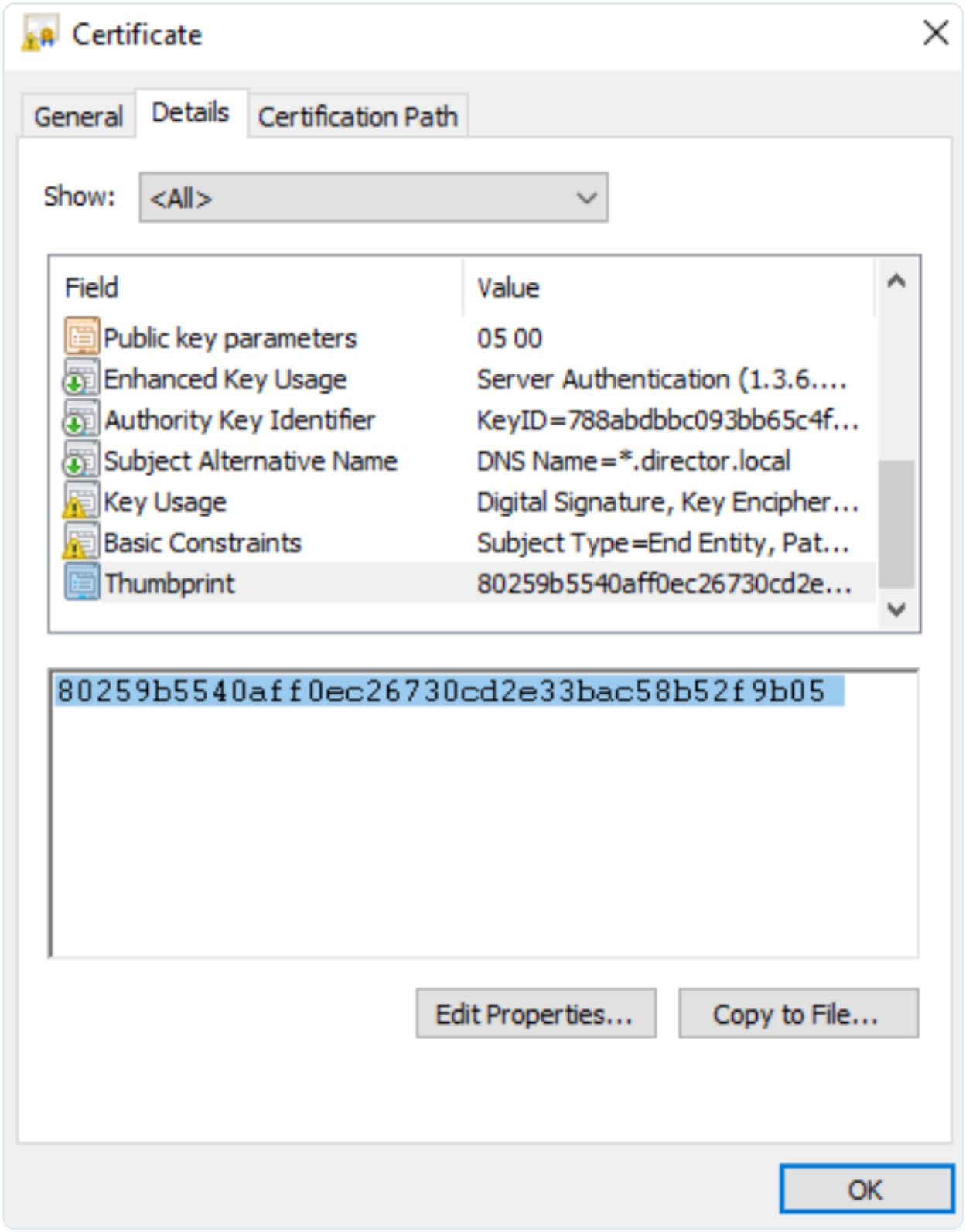
ステップ3: 証明書への読み取りアクセス権を付与する

1. インポートした証明書を右クリックし、**すべてのタスク** > **秘密キーの管理** を選択します。
2. 開いたダイアログで「**追加**」を選択し、「**Network Service**」を検索します。 「**OK**」をクリックします。

3. 「**グループ**または**ユーザー名**」の下にある「**NETWORK SERVICE**」を選択します。
4. 「**NETWORK SERVICEのアクセス許可**」の下にある*読み取り*アクセスを許可します。
5. 「**OK**」をクリックします。

ステップ4: サムプリントを取得する

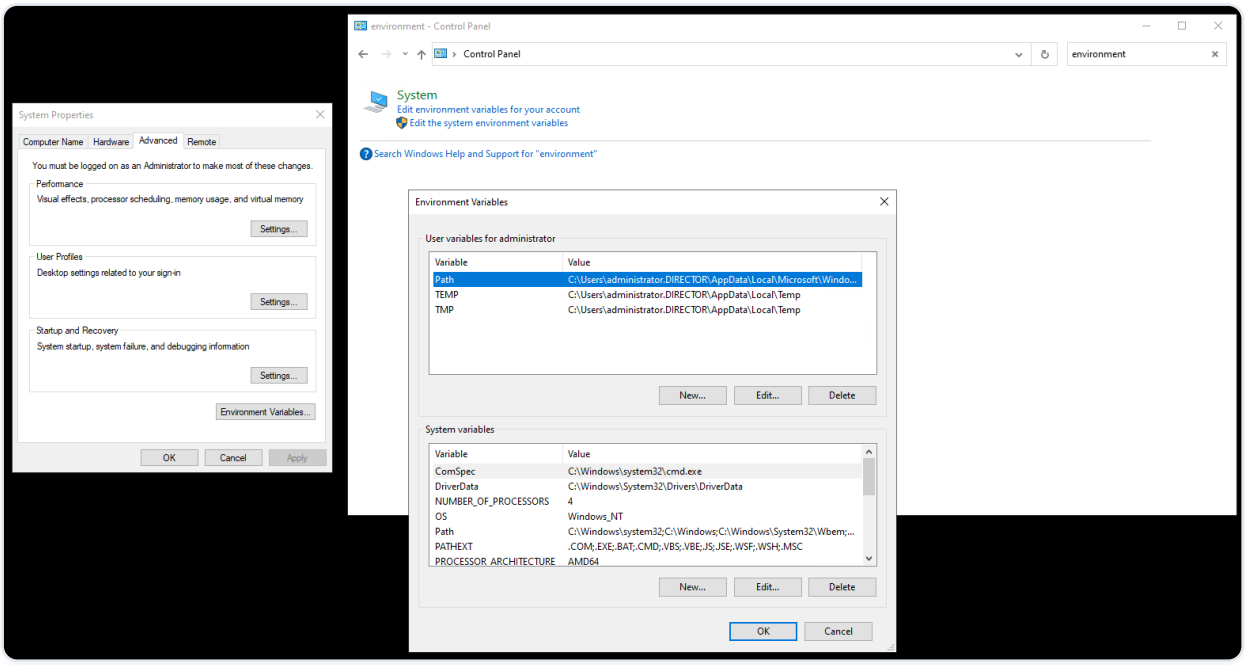
1. インポートした証明書をダブルクリックします。
2. 開いたダイアログで「**詳細**」タブに移動し、一番下までスクロールします。
3. 「**サムプリント**」をクリックします。



4. 値をコピーし、次のステップのために準備しておきます。

ステップ5：環境変数の設定

1. コントロールパネルを開きます。
2. 「環境」を検索し、**システム環境変数の編集**を選択します。
3. **システム変数（すべてのユーザー）の下にある新規**をクリックします。



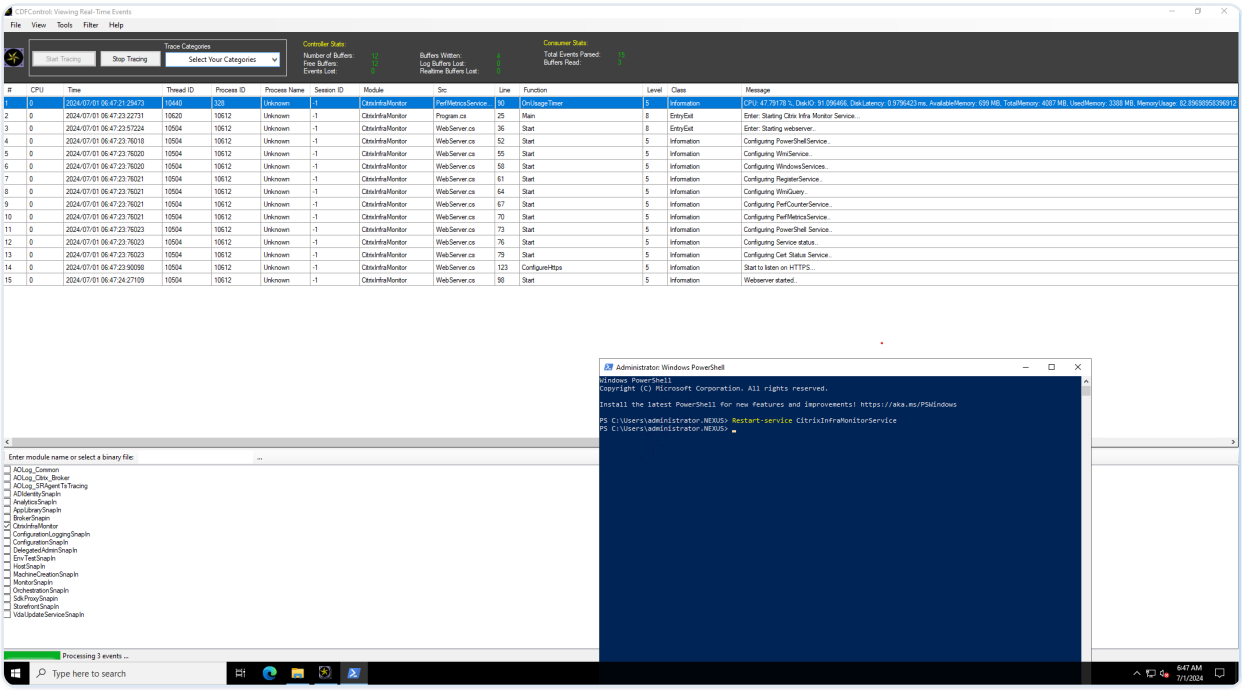
4. **変数**名として*DIRECTOR_AGENT_HTTPS_CERTIFICATE_THUMBPRINT*を指定します。
5. **変数値**に、前のステップで取得したサムプリントを指定します。
6. **OK**をクリックします。

ステップ6：CitrixInfraMonitorServiceの再起動

1. PowerShellを開き、次のコマンドを実行します。

```
Restart-Service CitrixInfraMonitorService
```

2. **CitrixInfraMonitorService**モジュールをキャプチャし、ログ行**Start to listen on HTTPS...**を探して、HTTPSが有効になっていることを確認します。



ステップ 7: モニター構成で HTTPS を有効にする

Delivery Controllerマシンで次のコマンドを実行します。

```
Set-MonitorConfiguration -DirectorAgentEnableHttps $true
```

接続の管理

「**Citrixコンポーネントの接続**」ページで、接続の表示、削除、または編集ができます。

接続の表示

このビューで利用可能な、接続済みおよび切断済みのすべてのコンポーネントの詳細を表示できます。次の表は、「**接続の作成**」ページのさまざまな列について説明しています。

列	説明
ホスト名	サーバーの名前。
種類	接続の種類。Delivery Controller™、Provisioning Service、およびStoreFrontがあります。
バージョン	コンポーネントにインストールされている `CitrixInfraMonitor.msi` のバージョン。このフィールドはDelivery Controllerには適用されません。

列	説明
作成者	接続を作成したユーザーの名前。
作成日	接続が確立された日付。
最終更新日時	接続が最後に更新された日付。
状態	状態には、接続中、接続済み、切断済みがあります。
	接続中: この状態は、新しいコンポーネントのデータが表示されるまでに約5分、リソース使用率のデータが利用可能になるまでに約10分かかる可能性があることを示します。
	接続済み: この状態は、コンポーネントとサイト間の接続が稼働中であることを示します。
	切断済み: この状態は、コンポーネントとサイト間の接続が切断されていることを示します。切断済みの状態になる可能性のある理由としては、サーバーのダウンタイムや、サイトがCitrix Infrastructure Monitorに接続できないことなどが挙げられます。

> **注：**
>
> オンプレミスのCitrix Virtual Apps and Desktops™サイトに接続されている場合、Delivery Controllerの接続はこのビューに自動的に入力されます。

接続の編集

Provisioning ServiceまたはStoreFront™接続を確立するために使用される管理者資格情報を更新するには、接続の編集が必要になる場合があります。

既存の接続を編集するには、次の手順を実行します。

1. **Settings**タブまたは**Infrastructure**タブから、**Connect Citrix Components**ページに移動します。
2. 接続リストテーブルで、目的のコンポーネントの行の末尾にある3つの点をクリックします。

3. **Edit**をクリックし、必要に応じて詳細を更新します。

コンポーネントを削除する

Director UIまたはPowerShellコマンドを使用して、コンポーネントを削除できます。

Director UIの使用

コンポーネントの削除とは、DirectorからProvisioning ServiceまたはStoreFront接続を登録解除するプロセスです。登録解除プロセスが完了すると、選択したコンポーネントの新しいデータ収集は停止します。既存の接続を削除するには：

1. **Settings**タブまたは**Infrastructure**タブから、**Connect Citrix Components**ページに移動します。
2. 接続リストテーブルで、目的のコンポーネントの行の末尾にある3つの点をクリックします。
3. **Remove**をクリックします。接続は登録解除され、Directorから削除されます。

PowerShell SDK の使用

特定のコンポーネントの登録を解除する必要がある場合は、Delivery Controller で次の PowerShell コマンドを実行します。

```
Remove-MonitorDirectorAgent -Fqdn <FQDN of component> -Component
<component>
```

Citrix Infrastructure Monitorの登録を解除するコマンドの例は次のとおりです。

```
Remove-MonitorDirectorAgent -Component PVS -Fqdn [redacted]
```

注:

コンポーネントの登録解除は、特定のコンポーネントからDirectorへのデータフローを停止するだけです。Citrix Infrastructure Monitor をアンインストールする必要がある場合は、「**コントロールパネル**」からアンインストールしてください。

インフラストラクチャダッシュボード

インフラストラクチャ監視ページで、コンポーネントの健全性値を確認できます。これらの結果は、インフラストラクチャに関する問題をプロアクティブに分析し、トラブルシューティングするのに役立ちます。

「**インフラストラクチャ監視**」ページは、以下でフィルタリングできます。

- ホスト名 - ホスト名を選択します
- 到達可能性 - **稼働中**（サーバーに到達可能）または**停止中**（サーバーに到達不能）チェックボックスを選択します
- エラー - 「エラーのある行のみ表示」チェックボックスを選択します。

「**列の管理**」オプションを使用して、ダッシュボードに表示するデータを選択します。

プロビジョニングサービスの健全性メトリック

インフラストラクチャタブをクリックし、**プロビジョニングサービス**を選択します。プロビジョニングサービスのインフラストラクチャダッシュボードが表示されます。

プロビジョニングサービスダッシュボード(/en-us/citrix-virtual-apps-desktops/2411/media/sm-pvs-dashboard.png)

プロビジョニングサービスサーバーについては、以下の詳細が監視されます。

カテゴリ	メトリック	説明
到達可能性	ホスト名	Citrix Infrastructure Monitorがインストールされている Provisioning Serviceマシンの名前。このメトリックは文字列値です。
	Provisioning Serviceサイト名	Provisioning Serviceサイトの名前。このメトリックは文字列値です。
	Provisioning Serviceファーム名	Provisioning Serviceファームの名前。このメトリックは文字列値です。
	プロビジョニングサービス サイトID	Provisioning Serviceサーバーのサイトidを表示します。このメトリックは文字列値です。
	プロビジョニングサービス ファームID	Provisioning Serviceサーバーのファームidを表示します。

カテゴリ	メトリック	説明
		このメトリックは文字列値です。
	サーバーの状態	指定されたサーバーの到達可能性の状態を表示します。可能な値は、*稼働中*、*停止中*、*不明*です。
	最終起動時間	プロビジョニングサービスサーバーが最後に起動された時刻を表示します。
	最終更新日時	プロビジョニングサービスサーバーからデータが収集された時刻を表示します。
依存サービス	ストリーミングサービス	ストリーミングサービスのステータスを表示します。このメトリックは、Windowsサービスのステータスを示します。可能な値は、*実行されていません*、*実行中*、*インストールされていません*、および*該当なし*（ヘルプアイコン付き）です。
	SOAPサービス	Simple Object Access Protocol (SOAP) サービスのステータスを表示します。このメトリックは、Windowsサービスのステータスを示します。可能な値は、*実行されていません*、*実行中*、*インストールされていません*、および*該当なし*（ヘルプアイコン付き）です。
	DB接続	データベース接続のステータスを表示します。Citrix Provisioningサーバーバージョン2402以前を使用している場合、不明なエラーが発生

カテゴリ	メトリック	説明
		する可能性があります。可能な値は、*未接続*、*接続済み*、*不明*、および*該当なし*（ヘルプアイコン付き）です。
	ライセンスサーバー到達可能性	ライセンスサーバーに到達可能かどうかを表示します。Citrix Provisioningサーバーバージョン2402以前を使用している場合、不明なエラーが発生する可能性があります。可能な値は、*未接続*、*接続済み*、*不明*、および*該当なし*（ヘルプアイコン付き）です。
リソース使用率	CPU使用率 %	CPU使用率を折れ線グラフで表示します。表示される値は、過去5分間の終わり時点での最新の値です。
	平均CPU %	過去10分間に集計されたProvisioning Serviceサーバーの平均CPU使用率を表示します。
	ピークCPU %	過去5分間のProvisioning Serviceサーバーのピーク CPU使用率を表示します。
	メモリ使用量 %	スタックチャートを使用して、メモリの使用率を表示します。表示される値は、過去5分間の終わり時点での最新のものです。
	平均メモリ %	過去10分間にわたって集計されたProvisioning Serviceサーバーの平均メモリ使用率を表示します。

カテゴリ	メトリック	説明
	ピークメモリ %	過去5分間のProvisioning Serviceサーバーのピークメモリ使用率を表示します。
	ディスクIOPS	折れ線グラフを使用して、ディスクの入出力値を表示します。
	平均ディスクIOPS %	過去10分間にわたって集計されたProvisioning Serviceサーバーの平均ディスクIOPSを表示します。
	ピークディスクIOPS %	過去10分間のProvisioning Serviceサーバーのピークディスクパーセンテージを表示します。
	ディスク遅延 (ミリ秒)	折れ線グラフを使用してディスクの遅延値を表示します。
	平均ディスク遅延 %	過去10分間に集計されたProvisioning Serviceサーバーの平均ディスク遅延を表示します。
	ピークディスク遅延 %	過去5分間のProvisioning Serviceサーバーのピークディスク遅延パーセンテージを表示します。
影響	拒否されたログインの合計	失敗したログインの合計数を、ログイン試行の合計数で割った値。
	アクティブなデバイス数	Provisioning Serviceサーバー内のアクティブなデバイスの総数を表示します。このメトリックは整数値です。

StoreFront™の健全性メトリック

インフラストラクチャタブをクリックし、**StoreFront**を選択します。StoreFront のインフラストラクチャダッシュボードが表示されます。

Provisioning Serviceダッシュボード(/en-us/citrix-virtual-apps-desktops/2411/media/sm-storefront-dashboard.png)

StoreFrontサーバーでは、以下の詳細が監視されます。

カテゴリ	メトリック	説明
到達可能性	ホスト名	StoreFrontサーバーの名前を表示します。このメトリックは文字列値です。
	サーバーの状態	StoreFrontサーバーの状態を表示します。このメトリックはWindowsサービスのステータスを示します。可能な値は、*実行中ではない*、*実行中*、*インストールされていない*、および*n/a* (ヘルプアイコン付き) です。
	ベースURLステータス	ベースURLの健全性を表示します。HTTPステータスコードが200の場合、ステータスはUPです。それ以外の場合、値はDownです。
	最終起動時刻	StoreFrontサーバーが最後に起動された時刻を表示します。
	最終更新	StoreFrontサーバーからデータが収集された時刻を表示します。
依存サービス	ドメインサービス	ドメインサービスという名前のWindowsサービスの健全性。このメトリックはWindowsサービスのステータスを示します。可能な値は、

カテゴリ	メトリック	説明
		実行中ではない、*実行中*、*インストールされていない*、および*n/a*（ヘルプアイコン付き）です。
	資格情報ウォレットサービス	このサービスは、暗号化されたパスワードを保存するために使用されるWindowsサービスです。可能な値は、*実行中ではない*、*実行中*、*インストールされていない*、および*n/a*（ヘルプアイコン付き）です。
	ピア解決サービス	このサービスは、StoreFrontサーバーのピアメッシュを形成するサーバー間グループネットワーク通信を担当するWindowsサービスです。可能な値は、*実行していません*、*実行中*、*インストールされていません*、および*n/a*（ヘルプアイコン付き）です。
	WWWサービス	このメトリックは、StoreFrontサーバーのWebサービスです。このメトリックは、Windowsサービスのステータスを示します。可能な値は、*実行していません*、*実行中*、*インストールされていません*、および*n/a*（ヘルプアイコン付き）です。
リソース使用率	CPU使用率 %	CPUの使用率を折れ線グラフで表示します。表示される値は、過去5分間の終わり時点での最新の値です。

カテゴリ	メトリック	説明
	平均CPU %	過去10分間にわたって集計されたStoreFrontサーバーの平均CPU使用率を表示します。
	ピークCPU %	過去5分間のStoreFrontサーバーのピークCPU使用率を表示します。この値は、CPUに必要な最大容量を決定するのに役立ちます。
	メモリ使用率 %	スタックチャートを使用して、メモリの使用率をパーセンテージで表示します。表示される値は、過去5分間の終わり時点での最新のものです。
	平均メモリ %	過去10分間にわたって集計されたStoreFrontサーバーの平均メモリ使用率を表示します。
	ピークメモリ %	過去5分間のStoreFrontサーバーのピークメモリ使用率を表示します。
	ディスクIOPS	折れ線グラフを使用して、ディスクの入出力値を表示します。
	平均ディスクIOPS %	浮動小数点数を使用して、StoreFrontサーバーの平均ディスクIOPSを表示します。
	ピークディスクIOPS %	過去10分間のStoreFrontサーバーのピークディスクIOPSパーセンテージを集計して表示します。
	ディスク遅延 (ミリ秒)	ディスクの遅延値を折れ線グラフで表示します。

カテゴリ	メトリック	説明
	平均ディスク遅延 %	過去10分間のStoreFrontサーバーの平均ディスク遅延を集計して表示します。
	ピークディスク遅延 %	過去5分間のStoreFrontサーバーのピークディスク遅延パーセンテージを表示します。
影響	ICA®証明書の有効性	ICA証明書の有効性を表示します。可能な値は、*期限切れ*、*期限切れ間近*、*有効*、*見つかりません* です。
	ICA証明書チェーンの有効性	StoreFront ICA証明書チェーンが有効かどうかを表示します。可能な値は*はい*または*いいえ*です。
	IIS証明書の有効性	IIS証明書の有効性を表示します。可能な値は、*期限切れ*、*期限切れ間近*、*有効*、*見つかりません*です。
	IIS証明書チェーンの有効性	StoreFront IIS証明書チェーンが有効かどうかを表示します。可能な値は*はい*または*いいえ*です。

Delivery Controller™の健全性メトリック

Delivery Controllerコンポーネントは、インフラストラクチャ監視の一部としてデフォルトで追加されます。Citrix Virtual Apps and Desktops™サイトに接続されているDelivery Controllerコンポーネントは、監視のために自動的にオンボーディングされます。

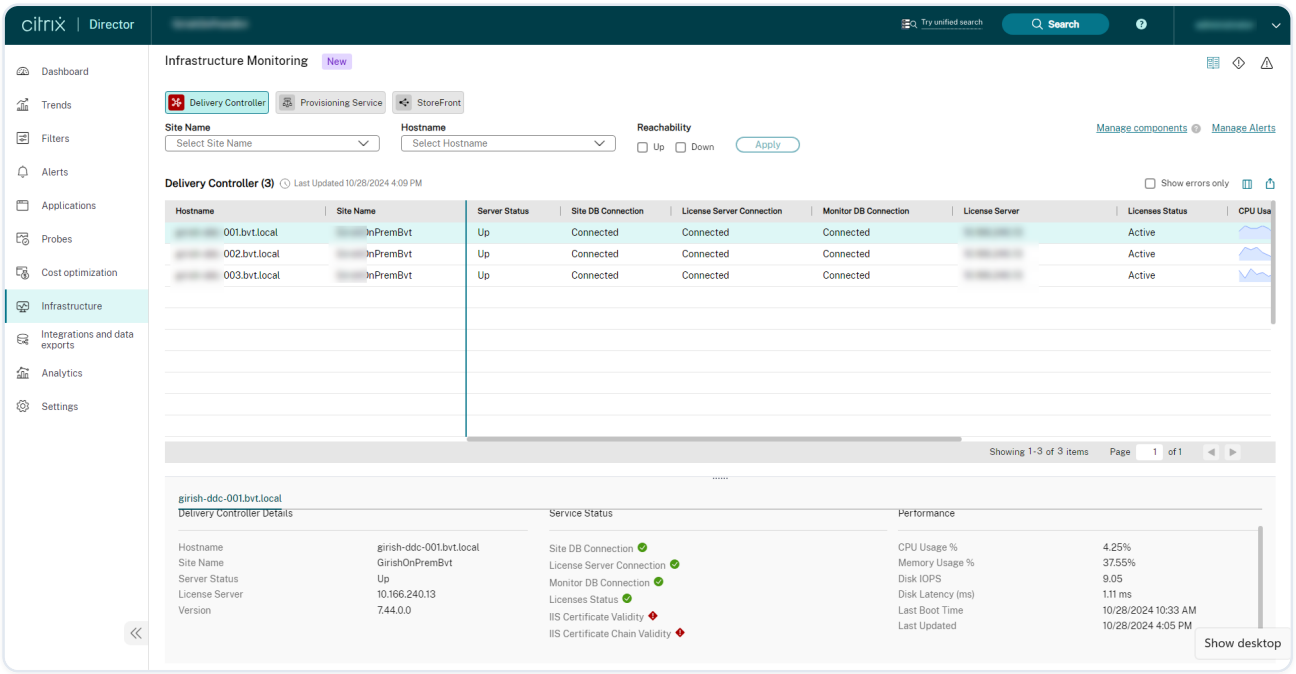
この機能により、お客様はインフラストラクチャ監視ダッシュボードでコントローラーの健全性を監視し、アラートを設定できます。アラート機能により、デリバリーコントローラー用に作成されたポリシーのいずれかがクリティカルまたは警告ステージにある場合、顧客管理者にアラートが通知されます。

必要なサイト名を選択すると、選択したサイト名に応じて詳細が表示されます。また、*稼働中*または*停止中*などの**到達可能性ステータス**を選択することもできます。

注： Delivery Controllerの監視には、`CitrixInfraMonitor.msi`ファイルは必要ありません。

インフラストラクチャの詳細について、シングルサイトとマルチサイトの両方の詳細を監視できます。

インフラストラクチャタブをクリックし、**Delivery Controller**を選択します。Delivery Controllerのインフラストラクチャダッシュボードが表示されます。



Delivery Controllerでは、以下の詳細が監視されます。

カテゴリ	メトリック	説明
到達可能性	サーバーの状態	指定された Delivery Controller の到達可能性の状態を表示します。指定可能な値は、*Up* と *Down* です。
	バージョン	Delivery Controller のバージョン。
	最終起動時刻	Delivery Controller が最後に起動された時刻を表示します。

カテゴリ	メトリック	説明
	最終更新日時	Delivery Controller からデータが収集された時刻を表示します。
依存サービス	サイトDB接続	サイトデータベース接続のステータスを表示します。可能な値は、*未接続*、*接続済み*、*不明*、および *n/a* (ヘルプアイコン付き) です。**不明:** この値は、メトリックが収集されていないか、利用できない場合に表示されます。**n/a:** 該当なし。この値は、サーバーのステータスがダウンしている場合に表示されます。
	ライセンスサーバー接続	ライセンスサーバー接続のステータスを表示します。可能な値は、*未接続*、*接続済み*、*不明*、および *n/a* (ヘルプアイコン付き) です。
	モニターDB接続	モニターデータベース接続のステータスを表示します。可能な値は、*未接続*、*接続済み*、*不明*、および *n/a* (ヘルプアイコン付き) です。
	ライセンスサーバー	ライセンスサーバーに到達可能かどうかを表示します。
	ライセンスステータス	ライセンスのステータスを表示します。
リソース使用率	CPU使用率 %	CPU使用率を折れ線グラフで表示します。表示される値は、過去5分間の終わりの最新の値です。
	平均CPU %	過去10分間に集計されたDelivery Controllerサーバーの

カテゴリ	メトリック	説明
		平均CPU使用率を表示します。
	ピークCPU %	過去5分間のDelivery Controllerサーバーのピーク CPU使用率を表示します。
	メモリ使用率 %	メモリ使用率を積み上げグラフで表示します。表示される値は、過去5分間の終わりの最新の値です。
	平均メモリ使用率 (%)	過去10分間のDelivery Controllerサーバーの平均メモリ使用率を表示します。
	ピークメモリ使用率 (%)	過去5分間のDelivery Controllerサーバーのピークメモリ使用率を表示します。
	ディスクIOPS	ディスクの入出力値を折れ線グラフで表示します。
	平均ディスクIOPS (%)	過去10分間のDelivery Controllerサーバーの平均ディスクIOPSを表示します。
	ピークディスクIOPS (%)	過去10分間のDelivery Controllerサーバーのピークディスクの使用率を表示します。
	ディスク待機時間 (ミリ秒)	ディスクの待機時間値を折れ線グラフで表示します。
	平均ディスク待機時間 %	過去10分間のDelivery Controllerサーバーの平均ディスク待機時間を表示します。
	ピークディスク待機時間 %	過去5分間のDelivery Controllerサーバーのピーク

カテゴリ	メトリック	説明
		ディスク待機時間の割合を表示します。
影響	IIS証明書の有効性	IIS証明書の有効性を表示します。可能な値は、*期限切れ*、*期限切れ間近*、*有効*、*見つかりません*です。
	IIS証明書チェーンの有効性	StoreFront IIS証明書チェーンが有効かどうかを表示します。可能な値は、*はい*または*いいえ*です。

アラートの作成と管理

関心のある条件や範囲をプロアクティブに監視し、アラート疲れを軽減するためにアラートを設定できます。アラートは、重要度、再アラート間隔、通知媒体を設定でき、製品でサポートされているアラートライフサイクルに従います。インフラストラクチャに関連するアラートは、**高度なアラートポリシー**セクションから作成できます。

詳細については、高度なアラートポリシーのページを参照してください。

アプリケーションおよびデスクトップのプロービング

アプリケーションとデスクトップのプロービングは、StoreFront を使用してサイトに公開されているアプリとデスクトップをテスト起動することで、それらの正常性をチェックするプロセスを自動化します。プロービングの結果は Director で確認できます。

要件

- Delivery Controller は、アプリケーションプロービングの場合はバージョン 7.18 以降、デスクトッププロービングの場合はバージョン 1906 以降を実行している必要があります。
- プローブエージェントを実行するエンドポイントマシンは、アプリケーションプロービングの場合は Windows 版 Citrix Workspace™ アプリバージョン 1808 以降、デスクトッププロービングの場合はバージョン 1906 以降がインストールされた Windows マシンである必要があります。Unified Windows Platform (UWP) 用 Workspace アプリはサポートされていません。
- Citrix Probe Agent は、Active Directory 資格情報を使用した StoreFront および Citrix Workspace 経由の認証をサポートしています。エンドポイントデバイスが Citrix Gateway 経由で StoreFront / Workspace に接続されている場合、Citrix Gateway ドメイン資格情報または多

要素認証 (MFA) を使用して認証できます。Citrix Probe Agent は、シングルサインオン (SSO) などの他の認証方法はサポートしていません。

> **注:**
>
> - ユーザーがCitrix Cloud™でサインインポリシーまたは条件付き認証を有効にしている場合、プローブエージェントはStoreFrontまたはCitrix Workspaceアプリにサインインできません。
> - Probe Agent は、Citrix Workspace アプリへの認証に Active Directory 認証のみをサポートしています。

- Citrix Probe Agent は、Citrix Gateway や Citrix ADC のようなプロキシサーバーまたはロードバランサーが展開されていない場合にのみ機能します。
- Probe Agent をインストールするエンドポイントマシンに、Microsoft .NET Framework バージョン 4.7.2 以降がインストールされていることを確認してください。

プロービングの実行に必要なユーザーアカウント/権限：

- 各エンドポイントマシンでプローブを実行するための固有の StoreFront ユーザー。StoreFront ユーザーは管理者である必要はなく、プローブは非管理者コンテキストで実行できます。
- エンドポイントマシンに Citrix Probe Agent をインストールおよび構成するための Windows 管理者権限を持つユーザーアカウント
- プロービングのために既存のユーザーアカウントを再利用すると、ユーザーのアクティブなセッションからログオフする可能性があります。完全な管理者ユーザーアカウント、または以下の権限を持つカスタムロール：
  - デリバリーグループのアクセス許可:
    - 読み取り専用
  - Directorのアクセス許可:
    - アラートメールサーバー構成の作成\\編集\\削除 - メールサーバーがまだ構成されていない場合
    - プローブ構成の作成\\編集\\削除
    - 構成ページの表示
    - 傾向ページの表示

構成

複数の地域で、ピーク時間外にプローブを実行するようにスケジュールできます。包括的なプローブ結果は、ユーザーが問題に遭遇する前に、アプリケーション、ホストマシン、または接続に関連する問題をトラブルシューティングするのに役立ちます。

Citrix Probe Agentバージョン2103以降は、サイト集約をサポートしています。Citrix Probe Agentを構成するときに、Workspace (StoreFront) Site Aggregation Enabledオプションを選択して、集約されたサイトからのアプリケーションとデスクトップの列挙を有効にします。以下のサイトの組み合わせがサポートされています:

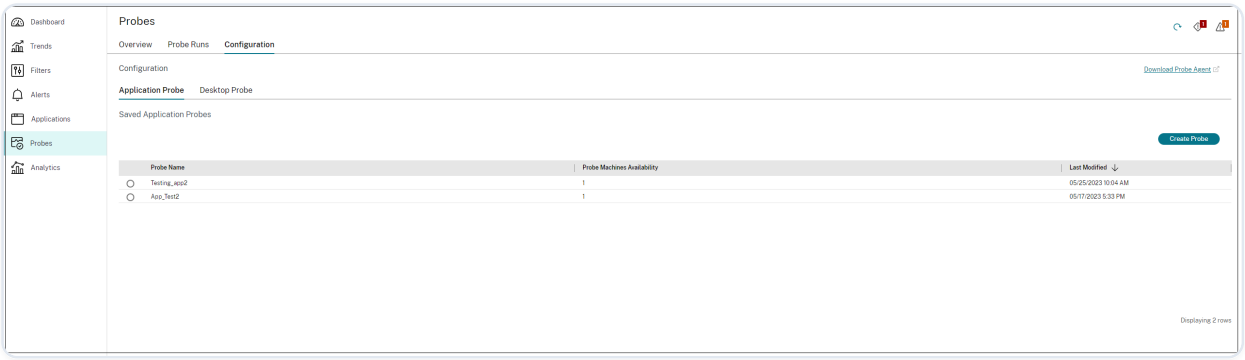
- 1つの StoreFront URL を持つ複数のオンプレミスサイト。
- StoreFront または Workspace URL のいずれかを持つオンプレミスサイトとクラウドサイト。
- 1つの Workspace URL を持つ複数のクラウドサイト。
- Citrix Gateway 経由で StoreFront または Workspace に接続されているオンプレミスサイト。

> **注:**
>
> 1つのサイトのみにアクセスできるプローブを構成するには、個別の管理者またはユーザーを作成する必要があります。

ステップ1：Citrix Probe Agentのインストールと構成

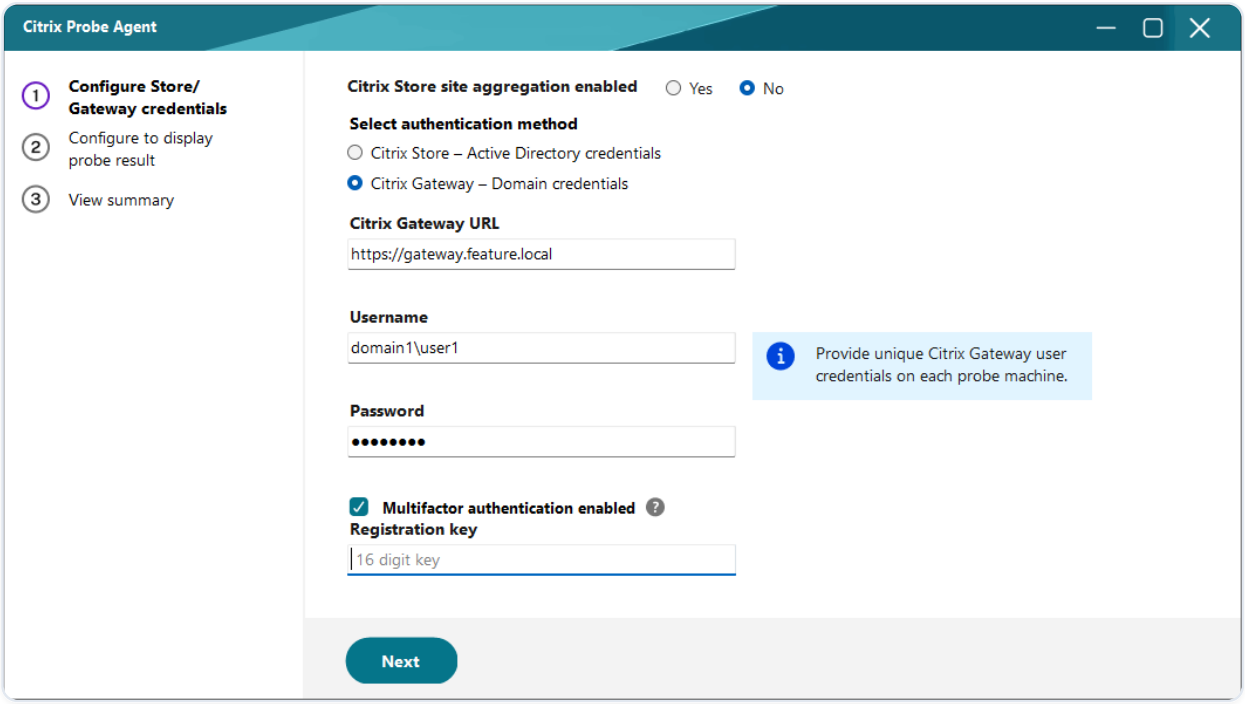
Citrix Probe Agent は、ユーザーが StoreFront を介して実際のアプリケーションまたはデスクトップを起動するのをシミュレートする Windows 実行可能ファイルです。Director で構成された起動をテストし、その結果を Director に報告します。

1. プロービングを実行するエンドポイントマシンを特定します。
2. 管理者権限を持つユーザーは、エンドポイントマシンにCitrix Probe Agentをインストールして構成できます。`<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/edition-software/premium-2411.html>`で入手可能なCitrix Probe Agent実行可能ファイルをダウンロードしてください。ダウンロードリンクは、Directorの**プローブ**タブでも利用できます。

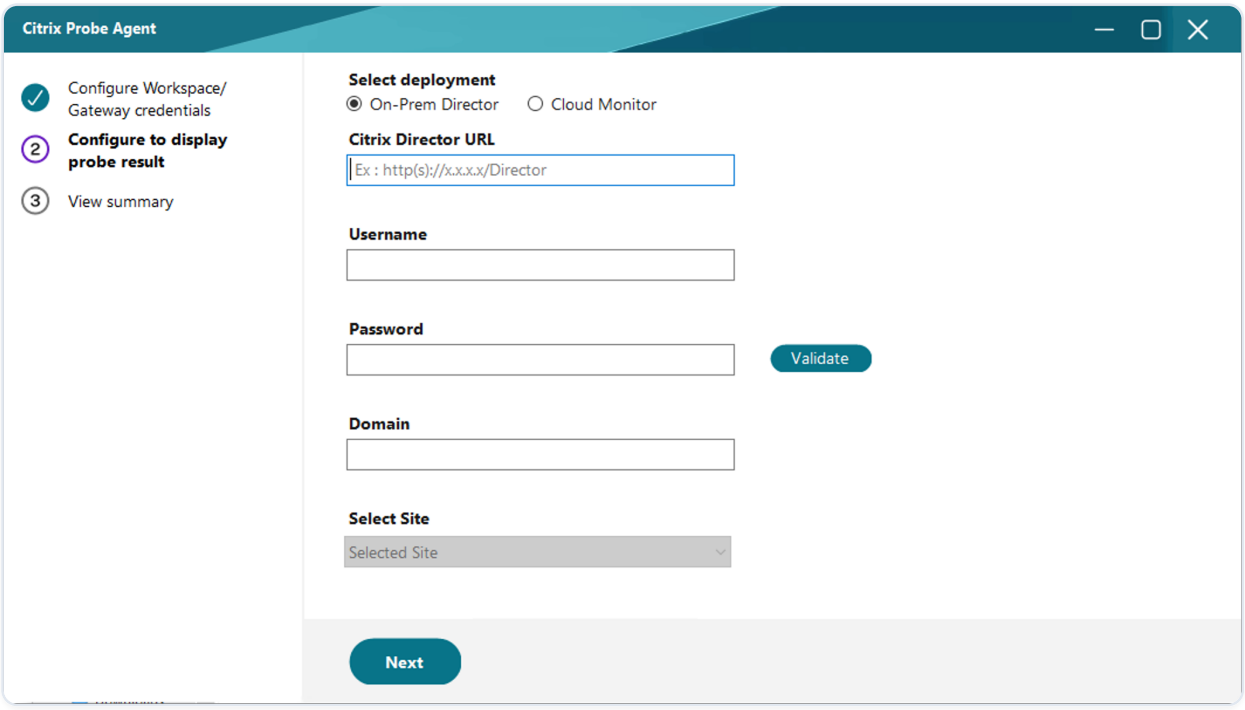


。

3. 集約されたサイトがある場合は、集約されたサイトからのアプリケーションとデスクトップの列挙を有効にするために、Workspace (StoreFront) Site Aggregation Enabled オプションを選択します。
4. 認証方法を選択し、関連する資格情報を入力します。資格情報は暗号化され、安全に保存されます。
5. StoreFront の Active Directory 資格情報で構成します。各エンドポイントマシンで一意の Workspace (StoreFront) ユーザーを構成します。
6. エンドポイントがCitrix Gatewayを介してStoreFrontに接続されている場合は、Citrix Gatewayオプションを選択し、Citrix Gatewayドメインの資格情報で構成します。



7. Gatewayが多要素認証をサポートしている場合は、多要素認証オプションを選択し、16桁の認証キーを入力します。これは、シングルログインスキーマを使用してLDAPおよびネイティブOTPで構成されたCitrix Gatewayでのみ利用可能です。
8. 「**プローブ結果の表示を構成**」タブで、Directorの資格情報を入力し、**検証**をクリックします。



9. サイトを選択し、**次へ**をクリックします。
10. 「**概要の表示**」タブで、設定された詳細が正確であることを確認します。変更が必要な場合は、該当するタブに移動して更新します。

> **注:**
>
> Automating Citrix Probe Agent Installation and Configuration に含まれるPowerShellスクリプトを使用して、Citrix Probe Agentのインストールと構成を自動化できます。

ステップ2：Directorでプロービングを構成する

> **制限事項:**
>
> 対話型ログオンメッセージバナーが有効になっている Windows VDA からアプリケーションまたはデスクトップがテスト起動されると、プロービングは失敗します。これは、対話型ログオンメッセージの承認を待機しているためにタイムアウトが発生するためです。 サーバーVDAでログオンメッセージを無効にするには、 > > > > に移動します。

> 以下のフィールドのテキストを削除し、Microsoftポリシーを更新します。

- 対話型ログオン: ログオンしようとしているユーザーへのメッセージテキスト
- 対話型ログオン: ログオンしようとしているユーザーへのメッセージタイトル

プローブがアプリケーションまたはデスクトップの起動状態を通過できるように、対話型ログオンメッセージバナーが無効になっているこの特定のサーバーVDAにプローブユーザーを割り当てます。

詳細については、`<https://learn.microsoft.com/ja-jp/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>`を参照してください。

1. **プローブ** \> **アプリケーションプローブ** または **デスクトッププローブ** に移動し、**プローブの作成** をクリックします。
2. **プローブの作成** ページで、プローブの名前を入力します。
3. スケジュールを選択します。
    a. プローブを実行する曜日を選択します。
    b. プローブを実行したい開始時刻を入力します。
    c. さらに、**Repeat in a day** オプションを選択できます。プローブを1日の中で繰り返したい終了時刻と間隔を入力します。たとえば、以下の構成は、毎週月曜日、水曜日、木曜日、日曜日に、12時08分から16時34分まで30分ごとに繰り返してアプリケーションプローブを実行するのに役立ちます。
4. 間隔に応じて、プローブするアプリケーションまたはデスクトップの推奨数を選択します。
5. プローブを実行する必要があるエンドポイントマシンを選択します。
6. 失敗したプローブの結果を送信する管理者のメールアドレスを入力します。メールサーバーは、**Alerts** > **Email Server Configuration** で構成します。

Director構成(/en-us/citrix-virtual-apps-desktops/2411/media/dir-probe-config.png)

この構成では、毎週月曜日、水曜日、木曜日、日曜日に、アプリケーションセッションが12:08、12:38、13:08といった具合に16:08まで起動します。

注:

- 構成後、エージェントは次の時間から構成されたプローブを実行します。
- **Repeat in a day** オプションが導入される前に設定されたプローブは、スケジュールされた時間に引き続き実行されます。これらのプローブでは、**Repeat in a day** オプションはデフォルトで無効になっています。
- 重複を防ぐため、各実行に5分間の期間があるようにプローブを構成することをお勧めします。

ステップ3：プローブの実行

エージェントは、Directorから定期的に取得するプローブ構成に従ってプロービングを実行します。

StoreFrontを使用して選択されたアプリケーションを順次起動します。エージェントは、Monitorデータベースを介して結果をDirectorに報告します。障害は5つの特定の段階で報告されます。

- **StoreFrontの到達可能性** - 構成されたStoreFront URLに到達できません。
- **StoreFront認証** - 構成されたStoreFrontの資格情報が無効です。
- **StoreFront列挙** - StoreFrontのアプリケーション列挙リストに、プローブ対象のアプリケーションまたはデスクトップが含まれていません。
- **ICA®ダウンロード** - ICAファイルが利用できません。
- **アプリケーション/デスクトップ起動** – アプリケーションまたはデスクトップを起動できませんでした。

ステップ4：プローブ結果の表示

プローブ結果は**プローブ**で確認できます。プローブビューでは、プローブ結果の包括的な概要が表示されます。これらの結果は、問題をプロアクティブに分析およびトラブルシューティングするのに役立ち、ユーザーのセッション起動エクスペリエンスをよりスムーズにします。

概要タブには、構成されているすべてのプローブの概要が1つのビューに表示されます。

Directorプローブの実行(/en-us/citrix-virtual-apps-desktops/2411/media/dir-probe-metrics-chart.png)

プローブは、期間、プローブの種類、エンドポイント名、アプリケーション名、デスクトップ名、プローブ結果の種類に基づいてフィルターできます。フィルター条件に一致するプローブは、プローブ、アプリケーション/デスクトップ、およびエンドポイントごとに次の詳細とともに表示されます。

プローブメトリックには、スケジュール済み、計画済み、スキップ済み、成功、失敗した実行の数が表示されます。

- 完了した実行 – 完了まで実行されたプローブ実行の数。
- 失敗した実行 – 失敗したプローブ実行の数。
- スキップされた実行 – エンドポイントが非アクティブであるか、サービスが利用できないために完了まで実行されなかった実行の数。
- 成功した実行 – アプリケーション/デスクトップの起動中にどの段階でも失敗することなく正常に完了したプローブの数。

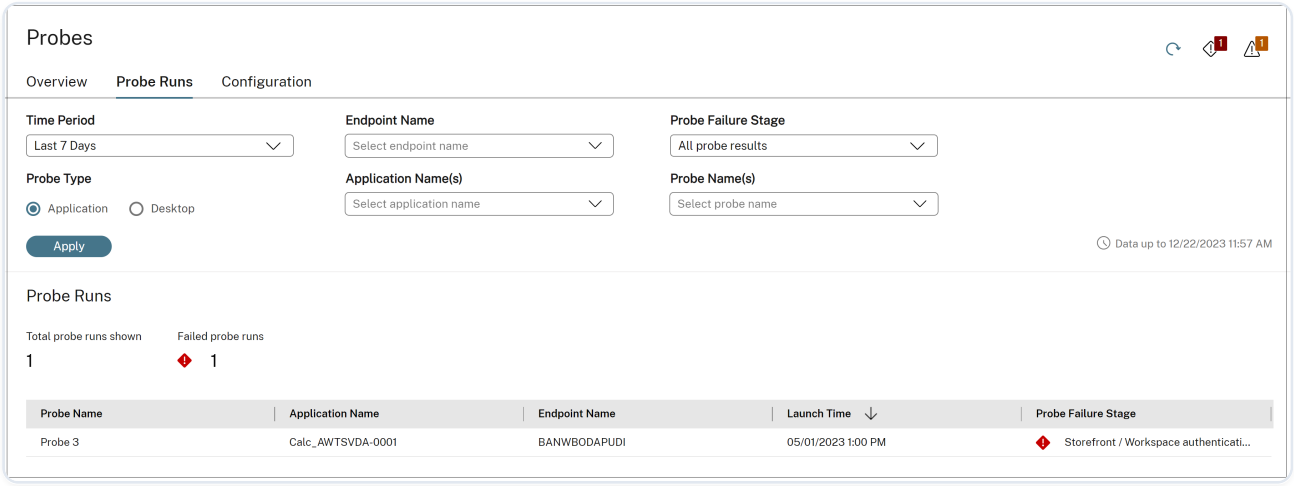
エンドポイントマシンの総数も、アクティブなマシンと非アクティブなマシンの数とともに表示されます。

プローブ失敗ステージは、各失敗グループの失敗分布を視覚的に分類して表示します。ほとんどの失敗が発生したステージを分析することで、プローブ結果の解釈と問題のトラブルシューティングが容易になります。このグラフィック表示は、アプリケーション/デスクトップの起動、ICAファイルのダウンロード、Storefront/Workspaceの列挙、Storefront/Workspaceの到達可能性、Storefront/Workspaceの認証における失敗したプローブ実行の数を示します。

ほとんどの失敗が発生したステージを分析するのに役立ちます。この情報は、プローブ結果を迅速に理解し、トラブルシューティングを行うのに役立ちます。

一部のプローブ実行は、エンドポイントが非アクティブであるか、サービスが利用できないために完了しない場合があります。

プローブ実行タブには、完了したプローブ実行の結果が詳細に表示されます。選択したプローブの個々の実行の詳細を確認するためにドリルダウンできます。重要な分析ポイントに基づいて、さらにフィルタリングおよび分析できます。



プローブ実行は、期間、プローブの種類、エンドポイント名、アプリケーション名、デスクトップ名、およびプローブ失敗ステージに基づいてフィルタリングできます。プローブ失敗ステージは、プローブが失敗したステージを表示します。プローブ名、スケジュールされた実行、失敗した実行、アプリケーション/デスクトップ名のリンクをクリックすると、フィルター条件に一致するプローブ実行のリストが表示されたプローブ実行ページに移動します。

コスト最適化

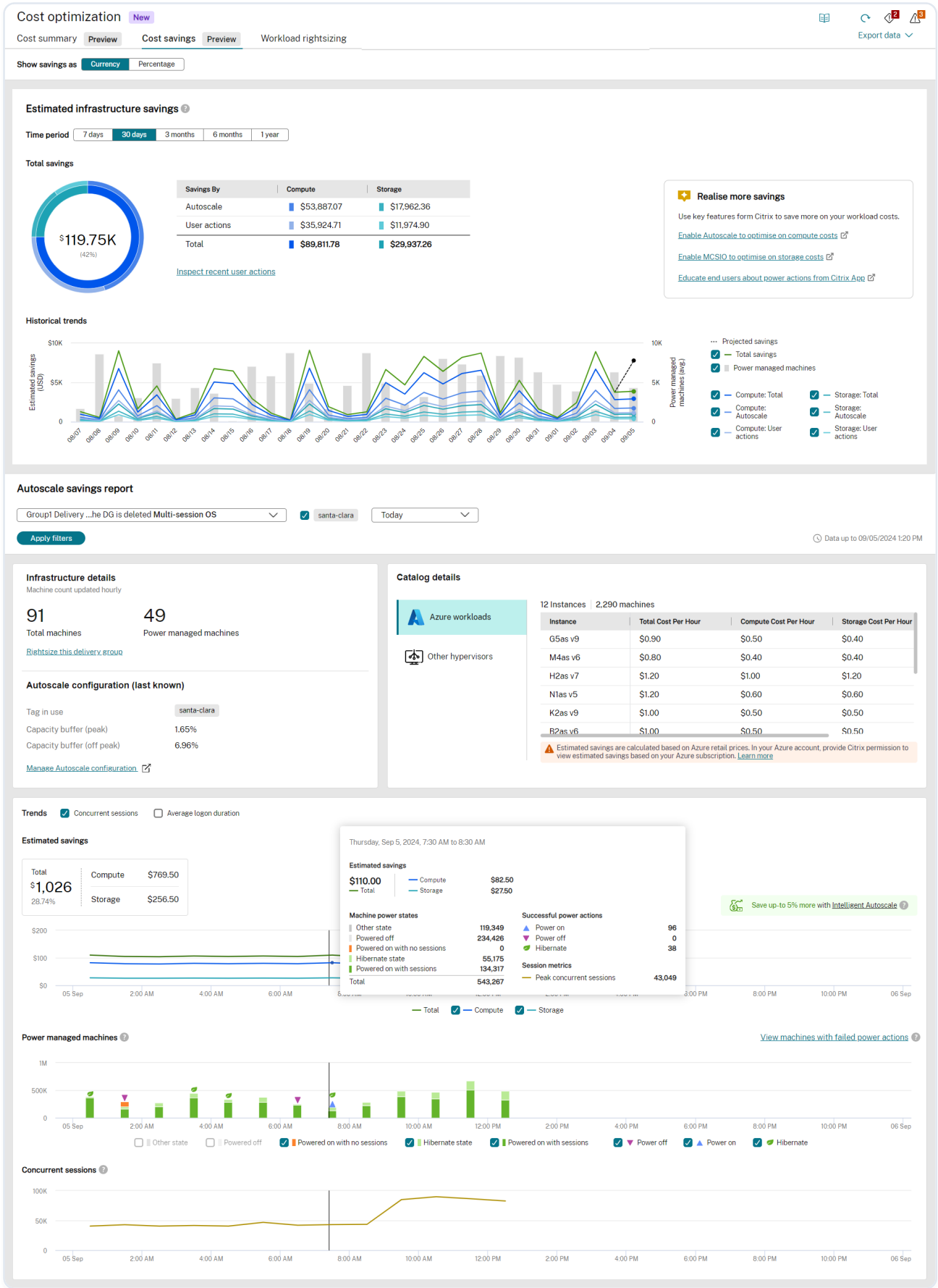
Citrix Director には、仮想マシンとセッションの使用状況を効果的に分析するのに役立つ「コスト最適化」という新機能が導入されました。この機能は、コストを最適化する方法に関する洞察に満ちた視覚的表現を提供します。また、不要なマシンを排除し、それによってコストを削減するのにも役立ちます。

コスト最適化をサポートするために、次のアラートも導入されています。

- 電源オン失敗アクションと電源オフ失敗アクション
- マシンの稼働時間アラート

最近の電源アクションを持つマシンを検査して、ユーザーの問題を引き起こす電源オンの失敗や、コストを増加させる電源オフの失敗を分析することもできます。詳細については、「最近の電源アクションを持つマシンの検査」セクションを参照してください。

ホームページの左側のメニューから**コスト最適化**タブをクリックして、**コスト最適化**ページにアクセスします。



コスト最適化ホームページでは、次のことができます。

- 開始リンク - このリンクにアクセスして、コスト最適化機能について詳しく学びます。

- コスト最適化ページを確認する - **コスト最適化**ページに関するフィードバックを提供できます
- データを更新する。
- アラートを表示する - 重大アラートと警告アラートの両方を表示できます。

コスト最適化ページには、次の機能が含まれています。

- コスト削減
- インフラストラクチャの適正化(/ja-jp/citrix-virtual-apps-desktops/2411/director/cost-optimization/infrastructure-rightsizing)

コスト最適化のためのコストはどのように計算されますか?

マシンあたりの時間あたりのコストは、ハイパーバイザーがサポートする通貨で表示されます。このセクションでは、Azureマシンおよびその他のマシンのコストがどのように計算されるかについて説明します。

Azureマシンのコスト

コスト計算の優先順位は次のとおりです:

1. 'Microsoft.Consumption/pricesheets/read権限が利用可能な場合、有効価格はAzureサブスクリプションで構成されている通貨で表示されます。
2. 権限が利用できない場合、Azureの小売価格が表示されます。詳細については、Azure Retail Prices overviewを参照してください。
3. 有効価格または小売価格が利用できない場合、コストはWeb Studioで管理者が入力したコストに基づいて表示されます。
4. Web Studioでコストが指定されていない場合、デフォルトのコストである1ドルが考慮されます。

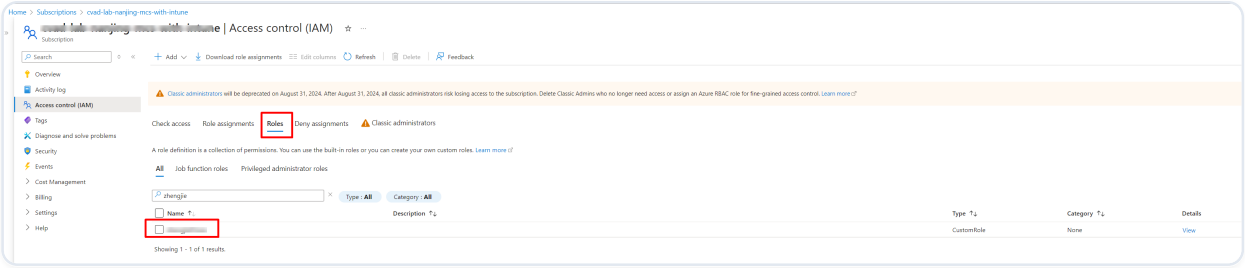
Azureのアカウント詳細を見つけ、有効価格を見つけるために必要な権限を追加するには、次の手順を実行します。

1. Citrix DaaSに移動します。
2. **Hosting**タブをクリックして、ホスティング接続アカウントを見つけます。
3. **Hosting**タブに記載されている**Application ID**を探します。

   ホスティングタブ(/en-us/citrix-virtual-apps-desktops/2411/media/daas-azure-hosting.png)
4. Azure ADに移動し、ステップ3でメモした**Application ID**を探します。

5. **サブスクリプション** > **アクセス制御 (IAM)** に移動し、ホスティング接続SPN用に構成されたカスタムロールを選択します。

   Azure ポータル(/en-us/citrix-virtual-apps-desktops/2411/media/azure-portal.png)



6. ロールに *Microsoft.Consumption/pricesheets/read* 権限を追加します。

Azureの小売価格を確認する方法?

`Microsoft.Consumption/pricesheets/read` が利用できない場合、Azure の小売価格が表示されます。これで、Retail Rates Prices API を使用して、すべての Azure サービスの小売価格を取得できます。以前は、Azure サービスの価格を取得する唯一の方法は、Azure Pricing Calculator を使用するか、Azure portal を使用することでした。詳細については、「Azure Retail Prices の概要」を参照してください。

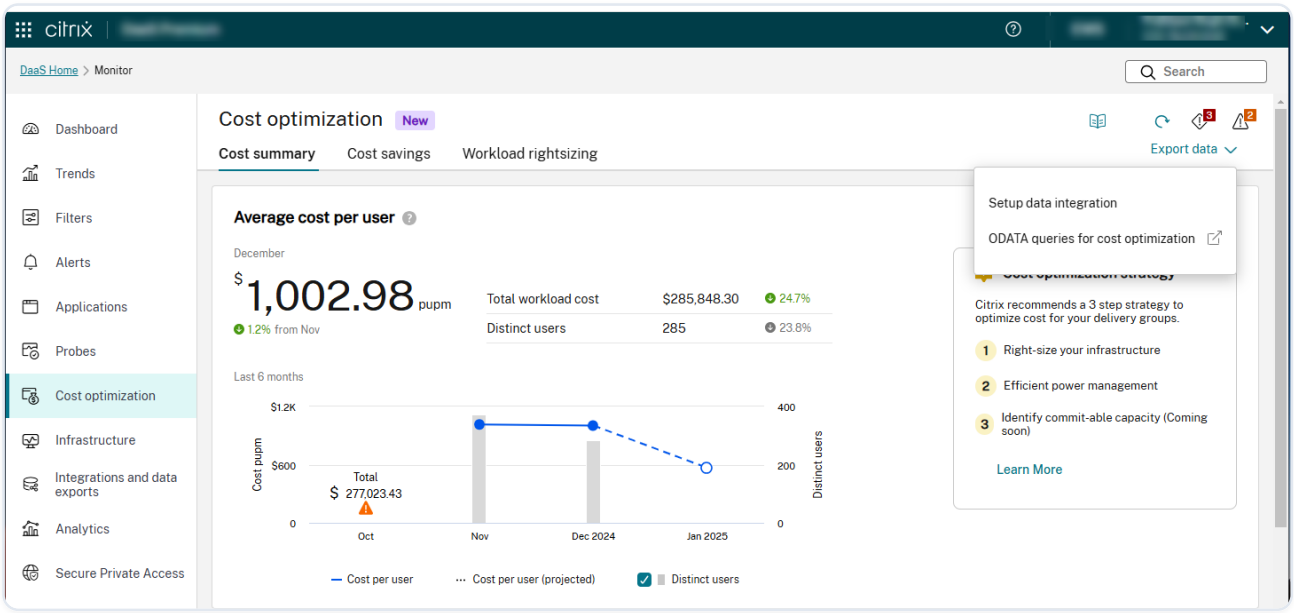
Azure 以外のマシンのコスト計算

その他のマシンの場合、コストは管理者がWeb Studioに入力したコストに基づいて表示されます。Web Studioにコストが記載されていない場合、デフォルトのコストである1ドルが考慮されます。

データのエクスポート

コスト最適化ページで、データ統合とODATAクエリを使用してデータをエクスポートできます。データをエクスポートするには、**コスト最適化**ページで**データのエクスポート**をクリックすると、次のオプションが表示されます。

- データ統合のセットアップ
- コスト最適化のための ODATA クエリ



データ統合のセットアップ

コスト最適化データをMonitor Service APIと統合することで、トラブルシューティングや問題のトリアージのためのデータを収集できます。詳細については、「統合とデータのエクスポート」ページを参照してください。

コスト最適化のためのODATAクエリ

「**コスト最適化**」ページで利用可能なサンプルODATAクエリを使用して、データをエクスポートできます。

ODATAの利用を開始する

以下のリンクは、ODATAの利用を開始するのに役立ちます。

- ODATAの概要
- Citrix CloudのOData v4エンドポイントを使用してCitrix Monitor Serviceデータにアクセスするためのさまざまな方法
- Citrix Monitor ServiceデータでOData V4集計クエリを使用する
- ODataとAPIクライアントを使用してPowerBIをDaaS Monitorに接続する方法
- Postmanを使用してログオン時間が長いユーザーの詳細を取得する
- Monitor Serviceデータにアクセスする方法
- データアクセスプロトコル
- モニターモデル
- モニター通知

サンプルODATAクエリ

未使用のVDAを検索する

未使用のVDAを検索するには、デスクトップグループID、VDAの開始日、および終了日を指定する必要があります。

未使用リソースへの支出を削減するための詳細については、ワークロードの適正化を参照してください。

クエリ例:

```
https://<DDC URL>/monitorodata/ResourceUtilizationSummary?
$apply=filter(DesktopGroupId eq desktop-group-id and granularity eq 1440
and SummaryDate ge startdate and SummaryDate lt enddate)/
groupby((MachineId), aggregate(cast(TotalSessionCount, Edm.Int32) with
average as AvgTotalSessionCount))/filter(AvgTotalSessionCount eq 0.0)/
aggregate($count as UnusedVDACount)
```

1日の平均稼働時間（分）を検索する

1日の平均稼働時間（分）を検索するには、以下を指定する必要があります。

- デスクトップグループID
- 開始日
- 終了日
- 終了日と開始日の間の日数。

未使用リソースへの支出を削減するための詳細については、ワークロードの適正化を参照してください。

クエリ例:

```
https://[<DDC URL>|https://api-us.cloud.com/monitorodata/
ResourceUtilizationSummary?$apply=filter(DesktopGroupId] /monitorodata/
ResourceUtilizationSummary?$apply=filter(desktopGroupId eq desktop-group-
id and granularity eq 1440 and SummaryDate ge startdate and SummaryDate lt
enddate)/groupby((MachineId), aggregate(cast(UptimeInMinutes, Edm.Int32)
div day-difference with sum as TotalUptimeInMinutes))/
aggregate(TotalUptimeInMinutes with average as
DailyAverageUptimeInMinutes)
```

失敗したマシンの電源アクションを確認する

失敗したマシンの電源アクションの詳細については、電源オンアクションの失敗と電源オフアクションの失敗を参照してください。

クエリ例:

```
https:// <DDC URL> /monitorodata/Machines?$filter=LifecycleState eq 0 and
DesktopGroup/SessionSupport eq 1 and
(cast(LastPowerActionReason,'Edm.Int32') eq 6 or
cast(LastPowerActionReason,'Edm.Int32') eq 7 or
cast(LastPowerActionReason,'Edm.Int32') eq 8) and
(cast(LastPowerActionFailureReason,'Edm.Int32') eq 300 or
cast(LastPowerActionFailureReason,'Edm.Int32') eq 402 or
cast(LastPowerActionFailureReason,'Edm.Int32') eq 401) and MachineRole eq
0&$orderby=Name&$skip=0&$top=50&$expand=DesktopGroup($select=Name)&$select
=Sid,Id,Name,IsAssigned,IPAddress,FaultState,LastDeregisteredCode,FailureD
ate,CurrentPowerState,CurrentSessionCount,IsInMaintenanceMode,LastPowerAct
ionFailureReason,LastPowerActionCompletedDate
```

合計節約額を確認する

コスト削減の詳細については、(/ja-jp/citrix-virtual-apps-desktops/2411/director/cost-optimization/cost-savings)の「コスト削減」ページを参照してください。

サンプルクエリ:

```
https://[<DDC URL>|https://api-us.cloud.com/monitorodata/
ResourceUtilizationSummary?$apply=filter(DesktopGroupId] /monitorodata/
MachineCostSavingsSummaries?$apply=aggregate(TotalAmountSaved with sum as
TotalAmountSavedSum)
```

マシンの状態を確認する

コスト削減の詳細については、(/ja-jp/citrix-virtual-apps-desktops/2411/director/cost-optimization/cost-savings)の「コスト削減」ページを参照してください。

サンプルクエリ:

```
https:// <DDC URL> /monitorodata/MachineCostSavingsSummaries?
$filter=SummaryDate eq
2024-08-09T06:00:00Z&$select=TotalMachinesCount,PowerManagedMachinesOff,Po
```

```
werManagedMachinesInHibernate,PowerManagedMachinesOnWithSessions,PowerMana
gedMachinesOnWithoutSessions
```

コスト削減

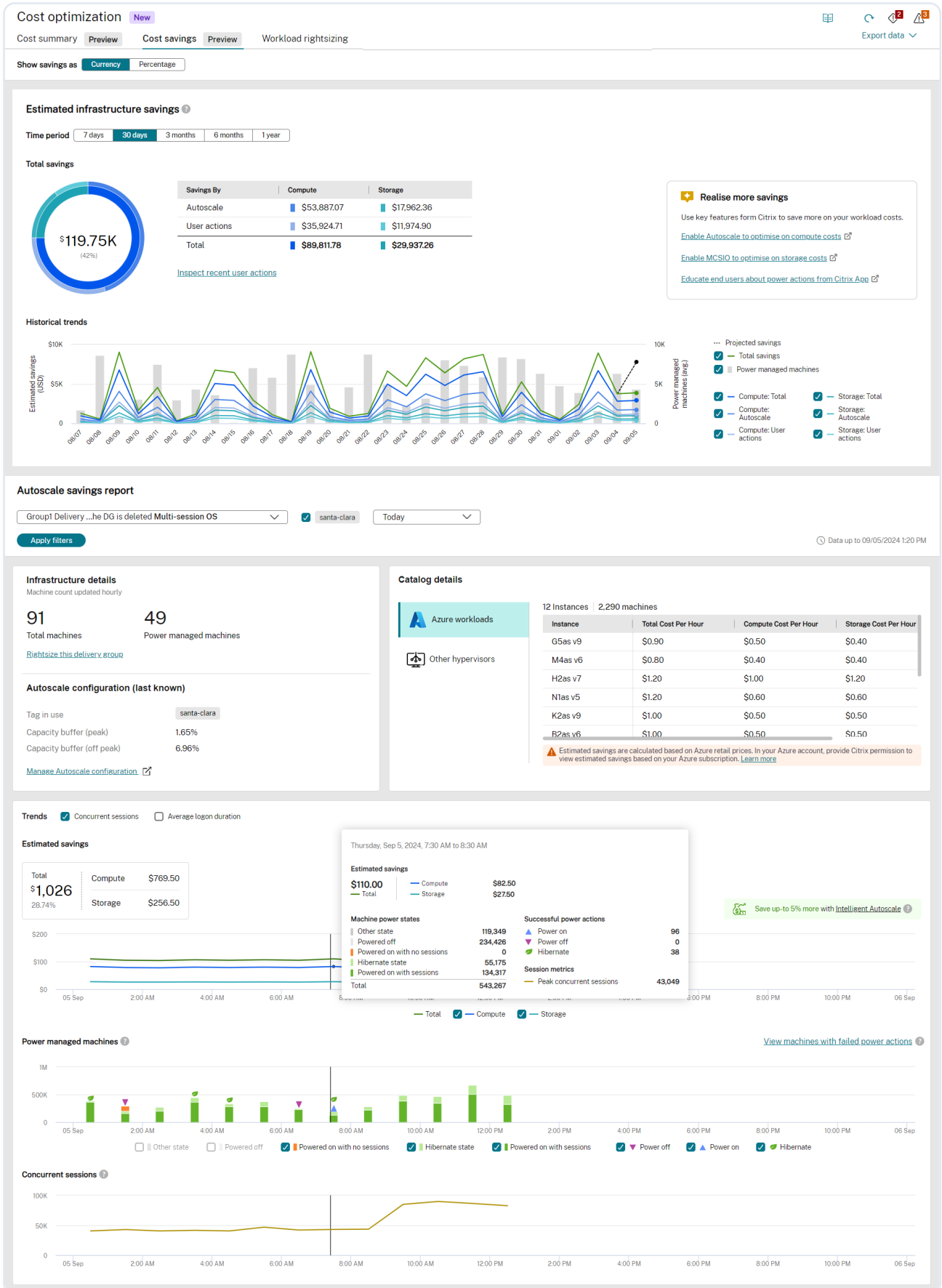
「**コスト削減**」ページでは、選択した期間に発生したインフラストラクチャの節約額を視覚的に表示し、残りの日数で予想される節約額を予測します。このページでは、マシンの使用状況とセッションを分析することで、達成された節約額とコスト削減の機会を特定するのに役立ちます。このページでは、以下を提供します。

- インフラストラクチャコストの最適化に関する洞察
- 節約された金額
- 予測コストを超える可能性のあるさまざまなシナリオに関する情報
- インフラストラクチャコスト削減を実現するための特定と戦略的計画の潜在的な機会

マシンの使用量は通常、ピーク時に増加し、より多くのリソースを必要とします。Autoscale™ 機能は、需要の低い期間に未使用のマシンを自動的に電源オフにすることで、コスト削減に役立ちます。予測される節約額は、この使用パターンに依存します。ただし、未使用のマシンが存在する場合や、Autoscale の電源アクションに障害が発生した場合など、特定の状況下ではコストが予想を超える可能性があります。これらの発生の背後にある理由を特定することは、以前は困難でした。

「**コスト最適化**」ページでは、予想コストを超える可能性のあるさまざまなシナリオに関する詳細情報が提供されます。同様に、たとえば、セッションのないマシンがある場合、さらなるコスト削減の機会が表示されます。

「**ホーム**」ページの左メニューから「**コスト最適化**」タブをクリックして、「**コスト最適化**」ページにアクセスします。



「**コスト最適化**」ページには、「**推定節約額**」と「**Autoscale 節約レポート**」が含まれています。コスト削減額は、ハイパーバイザーの通貨または発生したコストの割合として表示できます。

推定節約額: このグラフ表示は、インフラストラクチャリソースの効率的な利用を評価するのに役立ちます。コスト削減額は、ハイパーバイザーの通貨または発生したコストの割合として表示されます。このグラフは、コンピューティング関連の節約額とストレージの節約額から達成された節約額を示しています。

注:

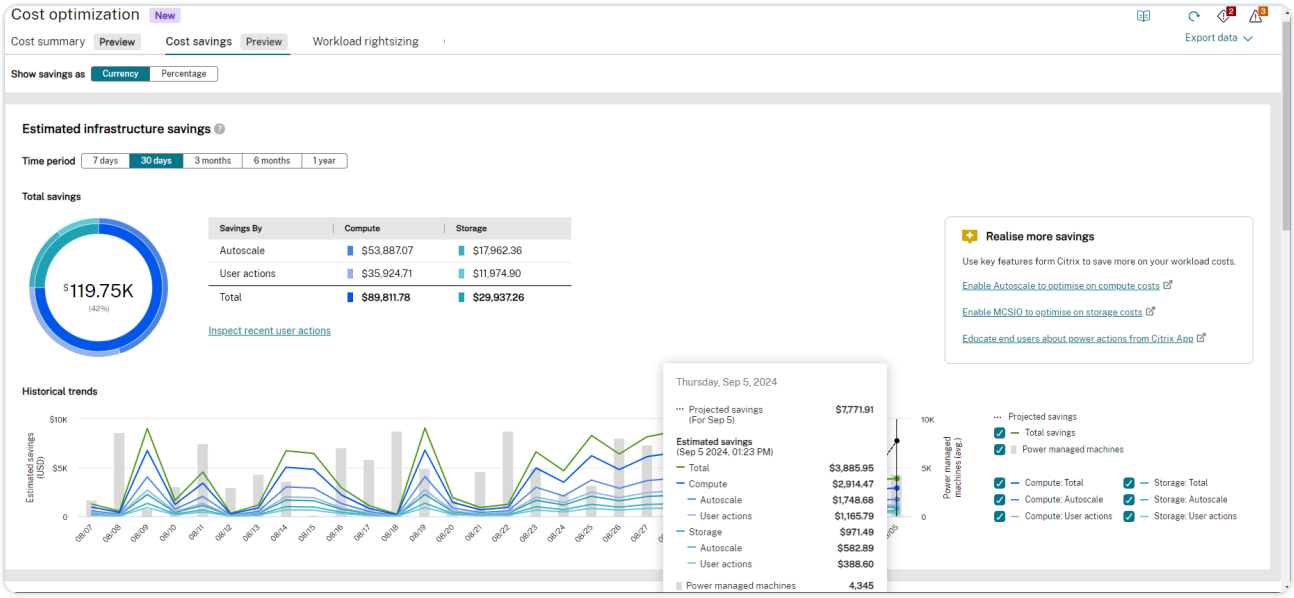
ストレージからの節約額を表示するには:

- コンピューティングコストを最適化するには、Autoscale を有効にする必要があります。詳細については、「Autoscale の使用を開始する」を参照してください。
- VMがシャットダウンされたときにストレージタイプを下位層に変更して、ストレージコストを最適化します。詳細については、VMがシャットダウンされたときにストレージタイプを下位層に変更するドキュメントを参照してください。
- この機能は現在、Azureマシンにのみ適用されます。

以下の期間の結果を表示できます。

- 7日間
- 30日間
- 3か月
- 6か月
- 12か月

次の図は、「推定インフラストラクチャ節約」セクションを示しています。



次の表は、「推定インフラストラクチャの節約」グラフの要素を示しています。

要素	説明
合計節約額	選択した期間にインフラストラクチャで達成された合計節約額を表示します。節約額はさらにストレージコストとコンピューティングコストに分類され、表形式で利用できます。
推定される節約額	選択した期間にインフラストラクチャで達成された節約額を表示します。
電源管理されたマシン	電源管理されたマシンの総数を表示します。
予測される節約額	残りの期間でどれだけのインフラストラクチャの節約が可能かを表示します。
コンピューティング - 合計	コンピューティング関連の節約から達成された合計節約額を表示します。
コンピューティング - オートスケール	オートスケール機能を使用しているコンピューティング関連の節約から達成された合計節約額を表示します。
コンピューティング - ユーザーアクション	ユーザーアクションによるコンピューティング関連の節約から達成された合計節約額を表示します。
ストレージ - 合計	ストレージの節約から達成された合計節約額を表示します。

要素	説明
ストレージ - オートスケール	Autoscale機能を使用しているストレージ節約によって達成された合計節約額を表示します。
ストレージ - ユーザーアクション	ユーザーアクションによるストレージ節約によって達成された合計節約額を表示します。

Autoscale節約レポート: このグラフィカルな表示は、Autoscale機能が構成され有効になっているデリバリーグループの節約レポートを提供します。このレポートは、電源管理されているマシンにのみ適用されます。デリバリーグループを選択し、今日、昨日、先週、来週、今月、または来月のデータを選択できます。グラフにカーソルを合わせると、特定のグラフ値を取得できます。

> **注:**
>
> デリバリーグループが削除された場合、Autoscale節約レポートでデータを取得することはできません。

> デリバリーグループのドロップダウンリストから、以下のオプションにドリルダウンできます。

- **すべて**: インフラストラクチャの詳細には、すべてのデリバリーグループ情報が表示されます。
- **シングルセッション**: シングルセッションマシンであるすべてのデリバリーグループのインフラストラクチャの詳細と、グラフにカーソルを合わせたときに表示されるマシンの電源状態、成功したAutoscale電源アクション、およびセッションのグラフィカルな表示。
- **マルチセッション**: マルチセッションマシンであるすべてのデリバリーグループのインフラストラクチャの詳細と、グラフィカルな表示。

選択した期間のデータが表示されます。**推定節約額**のグラフィカルな表示は、ドロップダウンメニューから選択された実際の節約額です。ピークポイントにカーソルを合わせると、マシンの電源状態、成功したAutoscale電源アクション、およびセッションに関する情報が表示されます。

選択したデリバリーグループに基づいて、次の詳細を表示できます。

- **インフラストラクチャの詳細**
    - 総マシン数と電源管理されているマシン数 - 総マシン数と、そのうち電源管理されているマシンの数を表示します。このデータは、残りの電源管理されていないマシンを電源管理されているマシンに変換し、Autoscale機能を有効にしてより包括的なカバレッジを実現す

る機会を提供します。インフラストラクチャの詳細セクションのデータは、1時間ごとに更新される最新の情報を示します。

- **カタログの詳細**

  ハイパーバイザー（サービスプロバイダー）の名前を表示します。詳細については、サポートされているVDAホスティングプラットフォームを参照してください。カタログの詳細データには、現在の時点で利用可能な最新データ（ライブデータ）が表示されます。

  次の詳細を取得できます。

  - **ハイパーバイザー名** - サイトが接続されているハイパーバイザーの名前を表示します。複数のハイパーバイザーが存在する場合は、利用可能なすべてのハイパーバイザーを表示します。
  - **インスタンス** - インスタンスの名前を表示します。
  - **1時間あたりの合計コスト** - ハイパーバイザーがサポートする通貨で、マシンあたりの1時間あたりのコストを表示します。Azureマシンでは、Microsoft.Consumption/pricesheets/read権限が利用可能な場合、Azureサブスクリプションで構成されている通貨で実効価格が表示されます。権限が利用できない場合は、Azureの小売価格が表示されます。詳細については、Azure小売価格の概要を参照してください。その他のマシンについては、管理者がWeb Studioで入力したコストに基づいてコストが表示されます。Web Studioでコストが記載されていない場合、デフォルトのコストは1ドルです。詳細については、「コスト最適化のコストはどのように計算されますか？」を参照してください。
  - **1時間あたりのコンピューティングコスト** - コンピューティング関連の節約によるコスト削減額を表示します。
  - **1時間あたりのストレージコスト** - ストレージの節約によるコスト削減額を表示します。
  - **マシン** - 選択したインスタンスのマシン数を表示します。

- **Autoscale構成（最新の既知）**

  使用中のタグ - WebStudioのAutoscale設定で構成されているマシンのタグを表示します。タグ付けされたマシンに基づいてデータをフィルタリングすることもできます。この場合、タグ付けされたマシンの概要のみが表示されます。

  容量バッファー（ピーク時） および **容量バッファー（オフピーク時）**

  ピーク時およびオフピーク時のデリバリーグループの最大要件に基づいて、電源がオンになっているマシンのバッファーの割合を表示します。

- **推定節約額**

選択した期間にインフラストラクチャで達成された節約額を表示します。Autoscale機能が有効なAzureマシンについて、コンピューティング関連の節約とストレージ関連の節約による節約額を表示できます。

- **電源管理対象マシン**

  Autoscaleが有効な場合、電源管理されたマシンは使用されていないときにオフになり、コストを最適化します。以下の詳細を確認できます。

  - 電源オフされたマシンの数 - このデータは、電源オフされたマシンの数を分析し、コスト削減に貢献したことを把握するのに役立ちます。
  - 休止状態 - このデータは、休止状態にあるマシンの数を分析するのに役立ちます。
  - セッションなしで稼働中のマシン - このデータは、なぜマシンがセッションなしでアクティブであったかを分析する機会を提供します。このデータは、より効果的なインフラストラクチャの節約戦略を計画する機会を提供します。
  - セッションありで稼働中のマシン - このデータは、電源オンされ、アクティブなセッションを持つマシンの数を分析するのに役立ちます。
  - 電源オフ - このデータは、電源オフまたは中断されたマシンの数と、このアクションがいつ実行されたかを分析するのに役立ちます。このデータを検証し、さらなる変更を加えることで、コスト削減に貢献できます。
  - 電源オン - このデータは、電源オンされたマシンの数と、このアクションがいつ実行されたかを分析するのに役立ちます。このデータを検証し、さらなる変更を加えることで、コスト削減に役立てることができます。

- **同時セッション**

  選択した時点でのセッションの総数を表示します。このデータは、コスト最適化のためにいつマシンを電源オフするかを決定するのに役立ちます。

- **平均ログオン時間**

  選択した期間にわたって、ユーザーがログオンする平均時間を表示します。

ワークロードの適正化

「ワークロードの適正化」（以前は**「インフラストラクチャの適正化」**）ページは、リソース使用率に基づいてデリバリーグループのプロビジョニングとサイジングの側面を分析するのに役立ちます。この分析に基づいて、次のことができます。

- 未使用のリソースへの支出を削減する

- 平均マシン稼働時間と正味無駄時間に基づいて計算される、マシンの正味アクティブ使用量を特定する。
- 特定のデリバリーグループの消費に対するマシンが、過剰、不足、または適正なサイズであるかを特定する
- 使用率が主にパワーユーザーによって推進されているかどうかを特定する（グループの残りのマシンと比較して、上位5パーセンタイルのマシンによる高い使用率によって示される）

ワークロードの適正化は、以下を使用してフィルタリングできます。

- デリバリーグループ - シングルセッションOSまたはマルチセッションOSデリバリーグループでフィルタリングできます
- タグ - タグはマシンに適用されるタグ名です。そのため、同じタグを持つマシンをフィルタリングできます。最大5つまで複数のタグを選択できます。複数のタグを選択すると、選択したマシンタグのいずれか1つ以上が適用されているすべてのマシンをフィルタリングできます。
- 期間 - 過去24時間、7日間、30日間のデータをフィルタリングできます。

ワークロードの適正化ページでは、次の機能が提供されます。

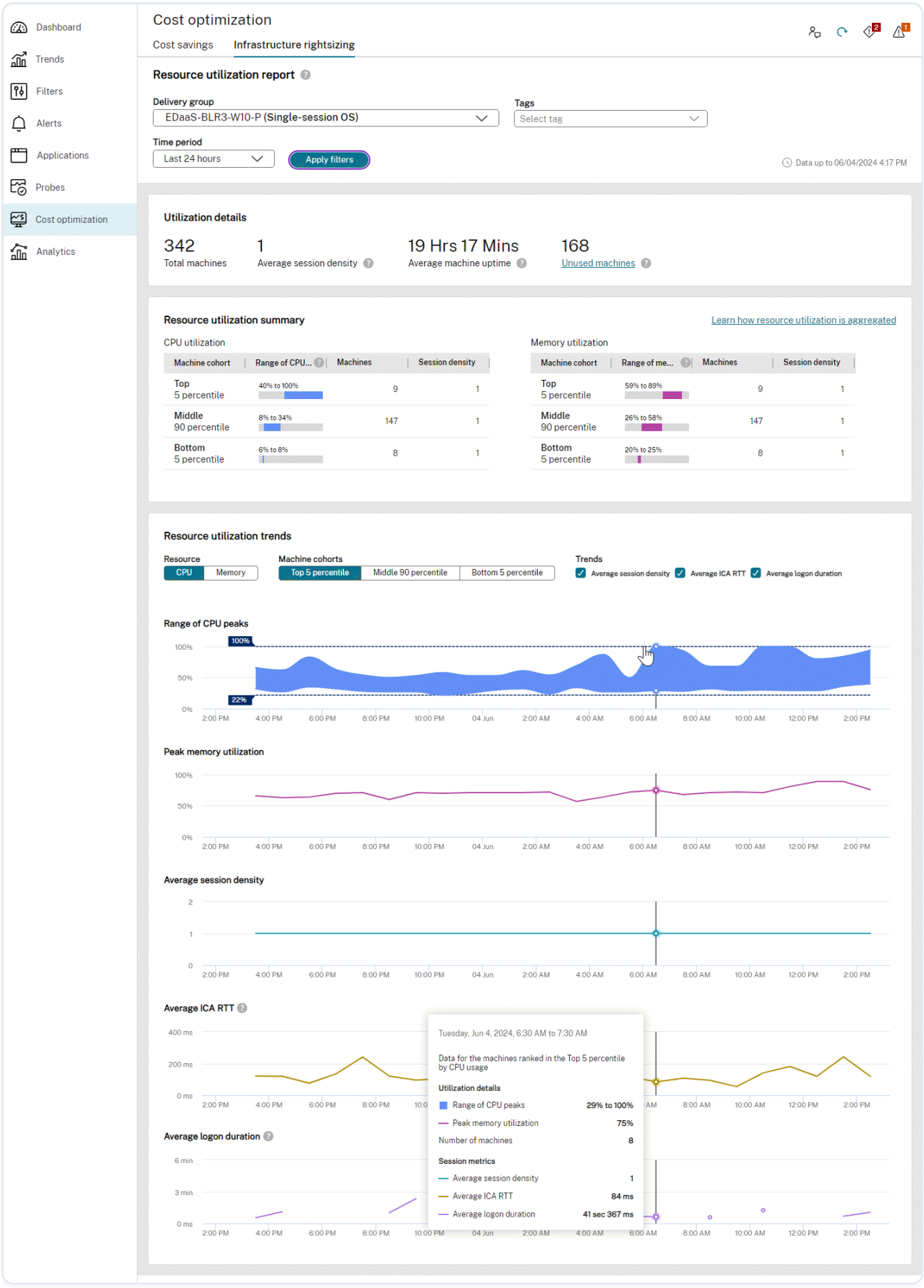
- マシンの正味アクティブ使用率に関する洞察
- 使用率の詳細に関するインサイト
- パワーユーザーの詳細に関する洞察と、これらのデータのエクスポート
- リソース使用率の概要
- リソース使用率の傾向

このページに表示される集計データは、次のように更新されます。

- 「過去24時間」および「過去7日間」フィルターの場合は1時間
- 「過去30日間」フィルターの場合は1日

ホームページの左メニューから「**コスト最適化**」タブをクリックします。次に、「**ワークロードの適正化**」タブをクリックして、「**ワークロードの適正化**」ページにアクセスします。

「**コスト最適化**」タブ > 「**コスト削減**」の「**インフラストラクチャの詳細**」セクションにある「**このデリバリーグループを適正化するリンク**」をクリックして、「**ワークロードの適正化**」ページにアクセスすることもできます。



「**ワークロードの適切なサイジング**」ページには、次のものが含まれます。

- マシンの正味アクティブ使用量

- 使用率の詳細
- リソース使用率の概要
- リソース使用率の傾向

マシンの正味アクティブ使用量:

このセクションには、詳細なマシン使用状況情報が表示され、コストを最適化できます。デリバリーグループ内のマシンの平均正味アクティブ使用時間を理解することで、管理者は節約を最大化するための最適な電源管理および課金戦略を決定できます。正味アクティブ使用量は、平均マシン稼働時間から合計稼働時間の無駄を差し引くことによって計算されます。すべての時間は分単位です。

「**マシンの正味アクティブ使用量**」セクションには、次の情報が表示されます。

- **正味アクティブ使用率:** ユーザーがマシンをアクティブに使用した実際の時間。これは、マシンが電源オンの状態で少なくとも1つのセッションがアクティブだった期間です。
- **平均マシン稼働時間:** マシンの電源がオンになっていた合計時間。
- **セッションなし:** アクティブなセッションがないことによる無駄な稼働時間。
- **アイドル時間:** アイドルセッションによる無駄な稼働時間。これは、マシン上のすべてのセッションがアイドル状態である時間です。
- **切断時間:** 切断されたセッションによる無駄な稼働時間。これは、マシン上のすべてのセッションが切断されている時間です。

使用率の詳細:

このセクションでは、選択したデリバリーグループおよび選択したタグの利用状況に関する詳細情報を提供します。過去24時間、7日間、30日間の詳細を表示できます。**利用状況の詳細**セクションでは、選択した時間フィルターの全期間にわたる詳細情報を提供します。たとえば、7日間が選択されている場合、合計マシン数は、7日間のいずれかの時点で稼働していたマシンの総数です。**利用状況の詳細**セクションでは、以下を提供します。

- **合計マシン** - マシンの総数を表示します。このデータには、選択した期間中に電源がオンになっていたすべてのマシンが含まれます。たとえば、7日間が選択されている場合、合計マシン数は、7日間のいずれかの時点で稼働していたマシンの総数です。
- **平均セッション密度** - このデータは、マシンの数と選択した期間にわたる平均です。セッションに利用可能なリソースに影響を与える、マシン上のセッション負荷の量を指します。
- **平均マシン稼働時間** - 電源管理されているマシンの総稼働時間と選択した期間の比率です。マシンが1日あたり、1台あたりどれくらいの時間稼働していたかを示します。たとえば、1つの

デリバリーグループまたは選択したタグに2台のマシンがあり、1台のマシンが24時間使用され、もう1台のマシンが1時間使用されたとします。平均マシン稼働時間は12時間30分です。この例では、選択されたフィルター値は「過去24時間」です。

- **未使用のマシン** - 選択した期間中にセッションがなかったにもかかわらず、電源がオンになっていたマシンの数を表示します。**未使用のマシン**リンクをクリックすると、**フィルター**タブが開き、現在電源がオンでセッションがない、同じデリバリーグループ内のすべてのマシンを表示できます。

リソース使用状況の概要:

このセクションでは、選択したデリバリーグループと選択したタグのリソースがどのように使用されたかの概要を提供します。最大5つのタグを選択できます。過去24時間、7日間、30日間の詳細を表示できます。マシンは使用状況に基づいてランク付けされます。**リソース使用状況の概要**セクションでは、アクティブなセッションを持つマシンのCPU使用率とメモリ使用率に関する詳細を提供します。このセクションでは、パワーユーザーを特定するオプションも提供し、パワーユーザーデータをエクスポートするのに役立ちます。

- **CPU使用率**:
  - マシンコホート - CPU利用率に基づいて、上位、中間、下位に分類されたマシングループに関する情報を提供します。最も使用頻度の高いマシンの5%は**上位5パーセンタイル**に、最も使用頻度の低いマシンの5%は**下位5パーセンタイル**に分類され、残りの90%は**中間90パーセンタイル**に分類されます。
  - CPUピークの範囲 - マシンコホートに対応するCPUピークの範囲をその使用率に基づいて表示します。
  - マシン - マシンコホートに対応するマシンの数を表示します。
  - セッション密度 - マシンコホートに対応するセッション密度を表示します。
- **メモリ使用率**:
  - マシンコホート - メモリ使用率に基づいて、上位、中間、下位に分類されたマシングループに関する情報を提供します。最も使用されているマシンの5%は**上位5パーセンタイル**に、最も使用されていないマシンの5%は**下位5パーセンタイル**に、残りの90%は**中間90パーセンタイル**に分類されます。
  - メモリピークの範囲 - マシンコホートに対応するメモリピークの範囲をその使用率に基づいて表示します。
  - マシン - マシンコホートに対応するマシンの数を表示します。
  - セッション密度 - マシンコホートに対応するセッション密度を表示します。

- パワーユーザーの特定 - このオプションを使用すると、パワーユーザーの詳細をエクスポートできます。

> **注:**
>
> この機能は、シングルセッションOSデリバリーグループでのみ利用可能です。

エクスポートデータには、**ユーザー名**、**合計セッション数**、**平均セッション期間 (分)**、**CPUピーク使用率 (%)**、および**メモリピーク使用率 (%)**が含まれます。

この機能強化により、リソース使用率に関する貴重な洞察が得られ、ユーザーの行動に基づいて効率的なリソース割り当てを確保することで、インフラストラクチャコストの最適化に役立ちます。

次の表は、**リソース使用率の概要**セクションに表示される値に基づいて実行可能なアクション項目に関する情報を提供します。

シナリオ	アクション項目
CPU使用率が高い	デリバリーグループのCPU仕様を増やします。または、使用率の高いユーザーを特定し、より優れた仕様の別のデリバリーグループに移動します。
CPU使用率が低い	デリバリーグループのCPU仕様を減らします。
メモリ使用率が高い	デリバリーグループのメモリ仕様を増やします。
メモリ使用率が低い	デリバリーグループのメモリ仕様を減らします。

リソース使用率の概要セクションにおけるデータ入力方法?

リソース使用率の概要セクションのデータは、**リソース使用率の傾向**のデータに基づいて入力されます。概要には、アクティブなセッションを持つマシンに関する詳細のみが表示されます。マシンが5台を超える場合、概要はより良い結果を提供します。

選択したデリバリーグループ内のマシンの数に基づいて、最大および最小使用率が計算されます。

たとえば、期間として「過去7日間」を選択し、選択したデリバリーグループに20台のマシンがあるとします。これらの20台のマシンは、さらに**上位5パーセンタイル**、**中間90パーセンタイル**、**下位5パーセンタイル**に分類されます。CPUとメモリの使用率は、アクティブなセッションがある場合に計算されます。たとえば、このケースでは、最初と最後のマシンが上位5パーセンタイルと下位5パーセンタイルに入ります。残りの18台のマシンは中間90パーセンタイルに分類されます。このケースでは、**上位5パーセンタイル**にマシンが1台しかないため、最大値と最小値は同じです。コホート内に複数のマシンがある場合、コホートの最高値と最低値は、そのグループ内の最高ランクのマシンの最大値と、そのグループ内の最低ランクのマシンの最大値にそれぞれ基づきます。

リソースタイプとして**CPU**を選択すると、選択したマシンの**CPUピークの範囲**と**ピークメモリ使用率**が表示されます。

リソースタイプとしてメモリを選択すると、選択したマシンのメモリピークの範囲とピークCPU使用率が表示されます。

リソース使用率の傾向: このセクションでは、CPUピークの範囲、ピークメモリ使用率、平均セッション密度、平均ICA® RTT、および平均ログオン期間のグラフ表示を提供します。

以下の詳細をフィルターできます。

- リソース - CPUとメモリ
- マシンコホート - 上位5パーセンタイル、中央90パーセンタイル、下位5パーセンタイル
- 傾向 - 平均セッション、平均ICA RTT、平均ログオン時間。

次のグラフを表示できます。

- **CPUピークの範囲** - CPUピークの範囲を帯状に表示します。帯の任意のポイントにカーソルを合わせると、帯の上限値と下限値が表示されます。
- **メモリ使用率のピーク** - 選択したマシンと選択した期間のメモリ使用率の最高値をグラフで表示します。
- **平均セッション密度** - 選択したマシンと選択した期間の平均セッション密度をグラフで表示します。
- **平均ICA RTT** - セッションの平均ラウンドトリップタイムを表示します。このグラフは、アクティブなセッションがない場合やセッションが切断されている場合に中断を示します。
- **平均ログオン期間** - 選択したマシンおよび選択した期間の平均ログオン期間をグラフで表示します。このグラフは、選択した期間中に新しいログオンが開始された場合にデータを表示します。

コスト概要

「**コスト概要**」ページでは、Citrix®環境の実行に関連する費用の包括的な概要が提供されます。この機能強化により、以下の情報を可視化できます。

- ユーザーあたりの総コスト
- 選択されたワークロードプロバイダー、デスクトップの種類、およびVMシリーズセットによる仮想化提供のコスト

このページでは、以下を提供します。

- ユーザーに仮想化されたアプリまたはデスクトップを提供するコストに関する洞察
- 節約された金額
- コストと節約に関する情報（カテゴリ別）：
  - プラットフォームプロバイダー
  - OSの種類
  - デスクトップの種類
  - VMシリーズ

> **注：**
>
> 「**コスト概要**」ページは、サイトが月に少なくとも15日間稼働している場合にのみ利用可能です。

> 「**コスト概要**」ページにアクセスするには、「**Director**」>「**コスト最適化**」>「**コスト概要**」をクリックします。「**コスト概要**」ページが表示されます。

コスト概要(/en-us/citrix-virtual-apps-desktops/2411/media/cost-summary.png)

コスト概要ページには、以下が含まれます。

- **ユーザーあたりの平均コスト**

  過去6か月間の月ごとの実際のユーザーあたりのコストと、現在の月の予測コストを表示できます。さらに、ワークロードの総コストとサイト上の個別のユーザー数を確認できます。複数の通貨が関係している場合、USDがそのうちの1つであれば、コストはUSDで表示されます。それ以外の場合は、リストからランダムに選択された通貨でコストが表示されます。先月およ

び先々月と比較したコスト削減額がパーセンテージで表示されます。また、個別のユーザー数の変化も表示されます。グラフィカルな表示では、毎月の傾向が示されます。

ユーザーあたりの平均コストを使用して、使用状況を最適化できます。

- **コストレポート**

  選択したサービスプロバイダー、選択したデリバリーグループ、および選択したタグのコストレポートを表示できます。過去3か月間のレポートを個別に表示することも、過去3か月間のデータを統合して表示することもできます。

- **Citrix を使用したコスト削減**

  AutoscaleやMachine Creation Services™ (MCS)、Storage Optimization (MCSIO)などのCitrix機能を有効にすることで、ユーザーあたりの平均コストをさらに削減できます。また、使用していないときにマシンをシャットダウンするなど、エンドユーザーの行動を促します。

  このデータは、Citrix機能が適用された場合の合計削減額を表示します。また、エンドユーザーの行動による削減額も表示されます。

- **デスクトップタイプ別のコスト**

  以下の種類のデスクトップのコストを表示できます。

  - **静的永続:** ユーザーは毎回同じ仮想デスクトップにサインオンし、デスクトップに加えられた変更は保存されます。
  - **静的非永続:** ユーザーは毎回同じ仮想デスクトップにサインオンしますが、デスクトップに加えられた変更は保存されません。
  - **ランダム永続:** ユーザーにはデスクトッププールから仮想デスクトップが割り当てられ、デスクトップに加えられた変更は保存されます。
  - **ランダム非永続:** ユーザーはデスクトッププールから仮想デスクトップを割り当てられ、デスクトップに加えられた変更は保存されません。

  各マシンタイプについて、個別のユーザー数、マシン数、月間平均稼働時間を表示できます。

  このデータを使用して、ユーザーを異なる種類のデスクトップに移動させることでコスト削減を計画できます。例えば、静的永続デスクトップタイプは、ランダム非永続デスクトップと比較して、より多くのリソース使用量を必要とします。そのため、一部のユーザーを静的永続デスクトップタイプからランダム非永続デスクトップタイプに移動させることを計画できます。

- **OSタイプ別のコスト**

シングルセッションおよびマルチセッションOSタイプのコストを表示できます。マシンのOSタイプ、個別のユーザー数、マシン数、月間平均稼働時間を表示できます。このデータを使用して、ユーザーを異なるOSタイプに移動させることでコスト削減を計画できます。

- **ユーザーあたりの月間最高コスト別ワークロード**

  ユーザーあたりの月間最高コストの詳細（仮想マシンインスタンス、個別のユーザー数、マシンの平均稼働時間を含む）を表示できます。また、マシン数とユーザーあたりのコストも確認できます。

  このデータを使用して、各VM構成タイプのコストを表示し、どの構成をユーザーに割り当てるかを決定します。

機能互換性マトリックス

Citrix Director 7 2411 は以下に対応しています:

- Citrix Virtual AppsおよびDesktops™ 7 2112 以降
- Citrix Virtual AppsおよびDesktops 7 1912 長期サービスリリース

各サイト内で、Director を以前のバージョンの Delivery Controller™ とともに使用することはできますが、Director の最新バージョンのすべての機能が利用できない場合があります。Citrix は、Director、Delivery Controller、および VDA を同じバージョンにすることを推奨しています。

> **注:**

> Delivery Controller をアップグレードした後、Studio を開くと、サイトのアップグレードを促されます。詳細については、展開のアップグレード の「**アップグレードシーケンス**」セクションを参照してください。

> Director のアップグレード後に初めてログインすると、構成済みのサイトでバージョンチェックが実行されます。いずれかのサイトが Director よりも古いバージョンの Controller を実行している場合、Director コンソールにサイトのアップグレードを推奨するメッセージが表示されます。さらに、サイトのバージョンが Director よりも古い間は、この不一致を示すメモが Director ダッシュボードに表示され続けます。

> **注:**

以前のバージョンの Citrix Director では、最近の VDA バージョンで実行されているユーザーセッションに適用されたポリシーは表示されません。Citrix Director 1912 およびそれ以前のバージョンでは、VDA バージョン 2003 以降で実行されているユーザーセッションに適用されたポリシーは表示されません。これらのポリシーを表示するには、Citrix Director バージョン 2003 以降を使用してください。

特定の Director 機能は、Delivery Controller (DC)、VDA、およびその他の必要な依存コンポーネントの最小バージョンと、ライセンスエディションとともに以下に示します。

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2411	アプリケーションページでの、最も使用頻度の低い公開済みアプリと未使用の公開済みアプリのレポート(/ja-jp/citrix-virtual-apps-desktops/2411/director/site-analytics/application-usage-monitoring#least-used-and-unused-published-apps-report)	DDC 7.16、VDA 7.15	プラチナライセンスサイト
2411	アクティビティマネージャーでのTCPまたはUDPアプリの列挙されたアプリケーションの詳細(/ja-jp/citrix-virtual-apps-desktops/2411/director/spa-integration-with-director#session-topology-view-for-secure-private-access-apps.)	VDA 2411およびDDC 2411	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2411	PowerShell SDKを使用したWebhook構成(/ja-jp/citrix-virtual-apps-desktops/2411/director/site-analytics/alerts-notifications#webhook-configuration-using-powershell-sdk)	VDA 2411およびDDC 2411	すべて
2411	一括アラート解除(/ja-jp/citrix-virtual-apps-desktops/2411/director/site-analytics/alerts-notifications#bulk-alert-dismissal)	VDA 2411およびDDC 2411	すべて
2411	ワークロードの適正化ページでのマシンの純アクティブ使用量	なし	すべて
2411	ストレージ使用量を最適化することによるコスト削減 (プレビュー)	なし	すべて
2411	コスト概要 (プレビュー)	なし	すべて
2411	Delivery Controllerの監視 (プレビュー)	VDA 2411	すべて
2411	UI から Citrix コンポーネントを接続する (プレビュー)	VDA 2411	すべて
2407	コスト最適化	なし	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2407	統合とデータのエクスポート	VDA 2407	すべて
2407	過去のユーザーセッションを診断 (プレビュー)	VDA 2407	すべて
2407	Secure Private Accessセッション用アクティビティマネージャー (プレビュー)	VDA 2407	すべて
2407	DirectorをTCPおよびUDPアプリのSecure Private Access統合 (プレビュー)	VDA 2407	すべて
2407	インフラストラクチャ監視 (プレビュー)	VDA 2407	すべて
2407	登録されていないマシンアラート	VDA 2407 および DDC 2407	すべて
2407	マシンの稼働時間アラート	VDA 2407 および DDC 2407	すべて
2407	電源オンアクションの失敗および電源オフアクションの失敗アラート	VDA 2407 および DDC 2407	すべて
2407	アラートメールにCSV添付ファイルを含め、アラートWebhookにJSONペイロードを含める機能	VDA 2407 および DDC 2407	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2407	最近の電源操作を行ったマシンを検査	VDA 2407	すべて
2407	高度なアラートポリシー	VDA 2407およびDDC 2407	すべて
2407	クラウドおよびオンプレミスユーザー向け統合検索	DDC 2407	すべて
2407	ダッシュボード上の公開アプリケーション使用状況監視チャート	VDA 2407およびDDC 2407	Platinumライセンスサイト
2402 LTSR	DirectorによるWebおよびSaaSアプリのSecure Private Access統合（プレビュー）(/ja-jp/citrix-virtual-apps-desktops/2411/2402-ltsr/director/spa-integration-with-director)	VDA 2402 LTSR	すべて
2402 LTSR	Microsoft Teamsバージョン2.1以前のサポート(/ja-jp/citrix-virtual-apps-desktops/2411/2402-ltsr/director/troubleshoot-deployments/user-issues#microsoft-teams-optimization-status)	VDA 2402 LTSR	すべて
2311	ライブセッションと録画セッションの再	VDA 2308およびDDC 2311	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	生(/ja-jp/citrix-virtual-apps-desktops/2411/director/troubleshoot-deployments/user-issues/record-sessions#play-back-live-and-recorded-sessions)		
2311	セッション トポロジとパフォーマンス メトリック(/ja-jp/citrix-virtual-apps-desktops/2411/director/troubleshoot-deployments/user-issues/session-performance#session-topology)	複数バージョン - リンク	すべて
2311	最適な画面解像度	なし	すべて
2311	MS Teams の最適化	VDA 2311 および DDC 最新版	すべて
2311	プローブの概要の機能強化	なし	すべて
2311	刷新されたセッション ログオン期間ビュー(/ja-jp/citrix-virtual-apps-desktops/2411/director/troubleshoot-deployments/user-issues/user-logon)	なし	すべて
2308	プローブの概要とドリルダウン(/ja-jp/citrix-virtual-apps-desktops/2411/	なし	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	director/probes#step-4-view-probe-results)		
2308	Citrix Gateway 多要素認証に対する Citrix Probe Agent のサポート(/ja-jp/citrix-virtual-apps-desktops/2411/director/probes/#step-1-install-and-configure-the-citrix-probe-agent)	シトリックス ゲートウェイ	すべて
2308	ハイパーバイザーアラートの無効化(/ja-jp/citrix-virtual-apps-desktops/2411/director/site-analytics/alerts-notifications#hypervisor-alerts-monitoring)	なし	すべて
2308	セッションエクスペリエンスメトリックの傾向	なし	すべて
2305	Citrix Gateway を介した認証のサポート	なし	すべて
2305	Director での Autoscale 管理	なし	すべて
2303	失敗したマシンのアラート	DC 7 2303	プレミアム
2203	TLS 1.3のサポート	-	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2212	AMD GPUで利用可能なリアルタイムGPU使用率	64ビットWindowsで動作し、HDX 3D Proが有効なDC 7.14およびVDA 7.14	すべて
2212	高度なプローブスケジューリング	DC 7 1906およびシトリックス プローブエージェント 2209	プレミアム
1909	Citrix Analytics for Performance でオンプレミスサイトを構成(/ja-jp/citrix-virtual-apps-desktops/2411/director/install-and-configure/onboarding.html)	DC 7 1906 および VDA 1906	すべて
1906	セッションの自動再接続(/ja-jp/citrix-virtual-apps-desktops/2411/director/site-analytics/trends.html#available-trends)	DC 7 1906 および VDA 1906	すべて
1906	セッションの起動時間(/ja-jp/citrix-virtual-apps-desktops/2411/director/troubleshoot-deployments/user-issues/session-startup.html)	DC 7 1906 および VDA 1903	すべて
1906	デスクトッププロービング(/ja-jp/citrix-virtual-apps-desktops/2411/director/probes.html)	DC 7 1906 および Citrix プローブエージェント 1903	プレミアム

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.9 以降	プロファイル読み込みにおける Citrix Profile Management の期間	VDA 1903	すべて
1811	プロファイルドリルダウン	DC 7 1811 および VDA 1811	すべて
1811	ハイパーバイザーアラートの監視	DC 7 1811	プレミアム
1811	アプリケーションプロービング	DC 7 1811 および Citrix アプリケーションプローブエージェント 1811	プレミアム
1811	Microsoft RDS ライセンスの正常性	DC 7 1811 および VDA 7.16	すべて
1811	主要な RTOP データ表示	DC 7 1811 および VDA 1808	プレミアム
1808	フィルターデータのエクスポート	DC 7 1808	すべて
1808	インタラクティブセッションのドリルダウン	DC 7 1808 および VDA 1808	すべて
1808	GPOドリルダウン	DC 7 1808 および VDA 1808	すべて
1808	OData API を使用して利用可能なマシンの履歴データ	DC 7 1808	すべて
7.18	アプリケーションプロービング	DC 7.18	Premium (旧 プラチナ)

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.18	スマートアラートポリシー	DC 7.18	プレミアム（旧プラチナ）
7.18	Health Assistant リンク	なし	すべて
7.18	対話型セッションのドリルダウン	なし	すべて
7.17	PIV スマートカード認証	なし	すべて
7.16	アプリケーション分析	DC 7.16 および VDA 7.15	すべて
7.16	OData API バージョン 4	DC 7.16	すべて
7.16	Linux VDA シャドウユーザー	VDA 7.16	すべて
7.16	ドメインローカルグループのサポート	なし	すべて
7.16	マシンコンソールアクセス	DC 7.16	すべて
7.15	アプリケーション障害監視	DC 7.15およびVDA 7.15	すべて
7.14	アプリケーション中心のトラブルシューティング	DC 7.13およびVDA 7.13	すべて
7.14	ディスク監視	DC 7.14およびVDA 7.14	すべて
7.14	GPU監視	DC 7.14およびVDA 7.14	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.13	セッション詳細パネルのトランスポートプロトコル	DC 7.x および VDA 7.13	すべて
7.12	ユーザーフレンドリーな接続およびマシン障害の説明	DC 7.12 および VDA 7.x	すべて
7.12	Enterprise editionでの履歴データ可用性の向上(/ja-jp/citrix-virtual-apps-desktops/2411/director/site-analytics/trends.html)	DC 7.12およびVDA 7.x	エンタープライズ
7.12	カスタムレポート(/ja-jp/citrix-virtual-apps-desktops/2411/director/site-analytics/trends.html)	DC 7.12およびVDA 7.x	プレミアム (旧 Platinum)
7.11	リソース使用率レポート(/ja-jp/citrix-virtual-apps-desktops/2411/director/site-analytics/trends.html)	DC 7.11およびVDA 7.11	すべて
7.11	CPU、メモリ、ICA RTT条件に対するアラート機能の拡張(/ja-jp/citrix-virtual-apps-desktops/2411/director/site-analytics/alerts-notifications.html)	DC 7.11およびVDA 7.11	プレミアム (旧 Platinum)
7.11	レポートのエクスポート機能の改善(/	DC 7.11およびVDA 7.x	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	ja-jp/citrix-virtual-apps-desktops/2411/director/site-analytics.html#export-reports)		
7.11	Citrix ADMとの統合(/ja-jp/citrix-virtual-apps-desktops/2411/director/install-and-configure/hdx-insight.html)	DC 7.11、VDA 7.x、およびMASバージョン11.1ビルド49.16	プレミアム (旧プラチナ)
7.9	ログオン期間の内訳(/ja-jp/citrix-virtual-apps-desktops/2411/director/troubleshoot-deployments/user-issues/user-logon.html)	DC 7.9およびVDA 7.x	すべて
7.7	プロアクティブな監視とアラート(/ja-jp/citrix-virtual-apps-desktops/2411/director/site-analytics/alerts-notifications.html)	DC 7.7およびVDA 7.x	プレミアム (旧 プラチナ)
7.7	Windows認証統合	DC 7.x および VDA 7.x	すべて
7.7	シングルセッションおよびマルチセッションOSの使用状況	DC 7.7 および VDA 7.x	プレミアム (旧 プラチナ)
7.6.300	Framehawk仮想チャネルのサポート	DC 7.6 および VDA 7.6	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.6.200	セッション記録の統合	DC 7.6 および VDA 7.x	プレミアム (旧 Platinum)
7	HDX Insight の統合	DC 7.6、VDA 7.x、および Citrix ADM	プレミアム (旧 Platinum)

データ粒度と保持

データ値の集計

Monitor Serviceは、ユーザーセッションの使用状況、ユーザーログオンパフォーマンスの詳細、セッション負荷分散の詳細、接続およびマシン障害情報など、さまざまなデータを収集します。データはカテゴリに応じて異なる方法で集計されます。OData Method APIを使用して提示されるデータ値の集計を理解することは、データを解釈するために不可欠です。例を次に示します。

- 接続されたセッションとマシン障害は一定期間にわたって発生します。したがって、これらは期間中の最大値として公開されます。
- ログオン期間は時間の長さを測定するものであるため、期間中の平均として公開されます。
- ログオン数と接続障害は期間中の発生回数であるため、期間中の合計として公開されます。

同時データ評価

セッションが同時であると見なされるには、重複している必要があります。ただし、時間間隔が1分の場合、その1分間のすべてのセッション（重複しているかどうかに関わらず）は同時であると見なされます。間隔のサイズが非常に小さいため、精度を計算するのにかかるパフォーマンスオーバーヘッドは、追加される価値に見合いません。セッションが同じ時間内であっても、同じ分内でない場合、それらは重複しているとは見なされません。

サマリーテーブルと生データの相関

データモデルは、メトリックを2つの異なる方法で表現します。

- サマリーテーブルは、メトリックの集計ビューを分、時間、日単位の粒度で表します。
- 生データは、セッション、接続、アプリケーション、およびその他のオブジェクトで追跡される個々のイベントまたは現在の状態を表します。

API呼び出し間またはデータモデル自体の中でデータを関連付けようとする場合、以下の概念と制限を理解することが重要です。

- **部分的な間隔のサマリーデータはありません。** メトリックのサマリーは、長期間にわたる履歴トレンドのニーズを満たすように設計されています。これらのメトリックは、完全な間隔についてサマリーテーブルに集計されます。データ収集の開始（利用可能な最も古いデータ）および終了における部分的な間隔のサマリーデータはありません。1日の集計（Interval=1440）を表示する場合、これは最初と最新の不完全な日にはデータがないことを意味します。これらの部分的な間隔には生データが存在する可能性がありますが、集計されることはありません。特定のデータ粒度における最も早い集計間隔と最も遅い集計間隔は、特定のサマリーテーブルから最小および最大のSummaryDateをプルすることで判断できます。SummaryDate列は間隔の開始を表します。Granularity列は集計データの期間の長さを表します。
- **時間による相関。** メトリックは、前述のセクションで説明したように、完全な間隔についてサマリーテーブルに集計されます。これらは履歴トレンドに使用できますが、生イベントはトレンド分析のために集計されたものよりも現在の状態を反映している可能性があります。サマリーと生データの時間ベースの比較を行う場合、発生する可能性のある部分的な間隔や、期間の開始と終了にはサマリーデータがないことを考慮する必要があります。
- **見逃されたイベントと潜在的なイベント。** イベントが見逃されたり、集計期間に対して潜在的であったりすると、サマリーテーブルに集計されるメトリックはわずかに不正確になる可能性があります。モニターサービスは正確な現在の状態を維持しようとしますが、見逃されたイベントや潜在的なイベントのために、サマリーテーブルの集計を再計算するために過去に遡ることはありません。
- **接続の高可用性。** 接続の高可用性中、現在の接続のサマリーデータカウントにはギャップが生じますが、セッションインスタンスは引き続き生データで実行されます。
- **データ保持期間。** サマリーテーブルのデータは、生イベントデータのスケジュールとは異なるグルーミングスケジュールで保持されます。サマリーテーブルまたは生テーブルからグルーミングによってデータが削除されたため、データが欠落している可能性があります。保持期間は、サマリーデータの異なる粒度によっても異なる場合があります。粒度の低いデータ（分）は、粒度の高いデータ（日）よりも早くグルーミングされます。グルーミングによってある粒度からデータが欠落している場合でも、より高い粒度で見つかる可能性があります。API呼び出しは要求された特定の粒度のみを返すため、ある粒度でデータが受信されないからといって、同じ期間のより高い粒度でデータが存在しないという意味ではありません。
- **タイムゾーン。** メトリックはUTCタイムスタンプで保存されます。サマリーテーブルは時間単位のタイムゾーン境界で集計されます。時間単位の境界に該当しないタイムゾーンの場合、データが集計される場所に関して多少の不一致が生じる可能性があります。

粒度と保持

Directorによって取得される集計データの粒度は、要求された時間（T）スパンの関数です。ルールは次のとおりです。

- 0 \< T \<= 1時間 - 分単位の粒度を使用
- 0 \< T \<= 30日 - 時間単位の粒度を使用
- T \> 31日 - 日単位の粒度を使用

集計データから取得されない要求データは、生のセッションおよび接続情報から取得されます。このデータは急速に増加する傾向があるため、独自のグルーミング設定があります。グルーミングは、関連データのみが長期的に保持されることを保証します。グルーミングは、レポートに必要な粒度を維持しながら、より良いパフォーマンスを保証します。Premiumライセンスサイトのお客様は、グルーミング保持を希望する保持日数に変更できます。変更しない場合はデフォルトが使用されます。サイトデータベースとの接続が失われた場合、モニターサービスは以下の表で指定されているPremiumエンタイトルメントのデフォルトの保持日数を使用します。

設定にアクセスするには、Delivery Controller™で次のPowerShellコマンドを実行します。

```
asnp Citrix.*

 Get-MonitorConfiguration

 Set-MonitorConfiguration -<setting name> <value>
```

	設定名	影響を受けるグルーミング	PREMIUMの保持日数	ADVANCEDの保持日数
1	GroomSessionsRetentionDays	セッション終了後のセッションおよび接続レコードの保持	90	31
2	GroomFailuresRetentionDays	MachineFailureLog およびConnectionFailureLog レコード	90	31

	設定名	影響を受けるグルーミング	PREMIUMの保持日数	ADVANCEDの保持日数
3	GroomLoadIndexesRetentionDays	LoadIndex レコード	90	31
4	GroomDeletedRetentionDays	「Deleted」のLifecycleStateを持つMachine、Catalog、DesktopGroup、およびHypervisorエンティティ。この設定は、関連するSession、SessionDetail、Summary、Failure、またはLoadIndexレコードも削除します。	90	31
5	GroomSummariesRetentionDays	DesktopGroupSummary、FailureLogSummary、およびLoadIndexSummaryレコード。集計データ - 日次粒度。	365	31
6	GroomMachineHotfixLogRetentionDays	VDAおよびControllerマシンに適用されたHotfix	90	31
7	GroomMinuteRetentionDays	集計データ - 分単位の粒度	3	3

	設定名	影響を受けるグルーミング	PREMIUMの保持日数	ADVANCEDの保持日数
8	GroomHourlyRetentionDays	集計データ - 時間単位の粒度	32	31
9	GroomApplicationInstanceRetentionDays	アプリケーションインスタンスの履歴	90	該当なし
10	GroomNotificationLogRetentionDays	通知ログレコード	90	該当なし
11	GroomResourceUsageRawDataRetentionDays	リソース使用率データ - 生データ	3	3
12	GroomResourceUsageMinuteDataRetentionDays	リソース使用率サマリーデータ - 分単位の粒度	7	7
13	GroomResourceUsageHourDataRetentionDays	リソース使用率の概要データ - 時間単位	30	30
14	GroomResourceUsageDayDataRetentionDays	リソース使用率の概要データ - 日単位	365	31
15	GroomProcessUsageRawDataRetentionDays	プロセス使用率データ - 生データ	1	1
16	GroomProcessUsageMinuteDataRetentionDays	プロセス使用率データ - 分粒度	3	3

	設定名	影響を受けるグルーミング	PREMIUMの保持日数	ADVANCEDの保持日数
17	GroomProcessUsageHourDataRetentionDays	プロセス使用率データ - 時間粒度	7	7
18	GroomProcessUsageDayDataRetentionDays	プロセス使用率データ - 日粒度	30	30
19	GroomSessionMetricsDataRetentionDays	セッションメトリックデータ	1	1
20	GroomMachineMetricDataRetentionDays	マシンメトリックデータ	3	3
21	GroomMachineMetricDaySummaryDataRetentionDays	マシンメトリック概要データ	365	31
22	GroomApplicationErrorsRetentionDays	アプリケーションエラーデータ	1	1
23	GroomApplicationFaultsRetentionDays	アプリケーション障害データ	1	1

注意：

Monitor Serviceデータベースの値を変更した場合、新しい値を有効にするにはサービスを再起動する必要があります。Monitor Serviceデータベースへの変更は、Citrixサポートの指示の下でのみ行うことをお勧めします。

設定 GroomProcessUsageRawDataRetentionDays、GroomResourceUsageRawDataRetentionDays、および

> GroomSessionMetricsDataRetentionDays はデフォルト値の1に制限されており、GroomProcessUsageMinuteDataRetentionDays はデフォルト値の3に制限されています。プロセス使用状況データは急速に増加する傾向があるため、これらの値を設定するPowerShellコマンドは無効になっています。 また、ライセンスベースの保持設定は次のとおりです。

- **Premiumライセンスサイト -** すべての設定のグルーミング保持期間は1000日（Citrixは365日を推奨）に制限されています。
- **Advancedライセンスサイト -** すべての設定のグルーミング保持期間は31日に制限されています。
- **その他のすべてのサイト -** すべての設定のグルーミング保持期間は7日間に制限されます。

例外:

- GroomApplicationInstanceRetentionDays は、Premiumライセンスサイトでのみ設定できます。
- GroomApplicationErrorsRetentionDays および GroomApplicationFaultsRetentionDays は、Premiumライセンスサイトでは31日間に制限されます。

長期間データを保持すると、テーブルサイズに以下の影響があります:

- **時間単位のデータ。** 時間単位のデータを最大2年間データベースに保持することを許可した場合、1000のデリバリーグループを持つサイトでは、データベースが次のように増加する可能性があります。

  1000のデリバリーグループ x 24時間/日 x 365日/年 x 2年 = 17,520,000行のデータ。集計テーブルにこれほど大量のデータがあると、パフォーマンスへの影響は甚大です。ダッシュボードデータはこのテーブルから取得されるため、データベースサーバーへの要件は大きくなる可能性があります。過度に大量のデータは、パフォーマンスに劇的な影響を与える可能性があります。

- **セッションおよびイベントデータ。** セッションが開始され、接続/再接続が行われるたびに収集されるデータです。大規模なサイト（10万ユーザー）の場合、このデータは急速に増加します。たとえば、これらのテーブルの2年分のデータは1TBを超えるデータとなり、ハイエンドのエンタープライズレベルのデータベースが必要になります。

Citrix Director の障害理由とトラブルシューティング

以下の表は、さまざまな障害カテゴリ、その理由、および問題を解決するために必要なアクションについて説明しています。詳細については、「列挙型、エラーコード、および説明」を参照してください。

接続障害エラー

カテゴリ	理由	問題	アクション
該当なし	[0] 不明。このエラーコードはマッピングされていません。	監視サービスは、ブローカリングサービスから共有された情報から、報告された起動または接続障害の理由を判断できません。	コントローラーでCDFログを収集し、Citrixサポートに連絡してください。
[0] なし	[1] なし	なし	該当なし
[2] マシン障害	[2] セッション準備	デリバリーコントローラーからVDAへのセッション準備要求が失敗しました。考えられる原因: コントローラーとVDA間の通信の問題、準備要求の作成中にBroker Serviceで発生した問題、またはVDAが要求を受け入れない原因となるネットワークの問題。	コントローラーとVDA間の通信の問題を引き起こす一般的な問題については、Knowledge Centerの記事「Citrix Virtual Apps and Desktopsにおけるデリバリーコントローラーへの Virtual Delivery Agent登録のトラブルシューティング」に記載されているトラブルシューティング手順を参照してください。
[2] マシン障害	[3] 登録タイムアウト	VDAは電源がオンになっていましたが、デリバリーコントローラーへの登録を試行中にタイムアウトが発生しました。	デリバリーコントローラーでCitrix Broker Serviceが実行されていること、およびVDAでDesktop Serviceが実行されていることを確認してください。停止している場合は、それぞれを開始してください。

カテゴリ	理由	問題	アクション
[1] クライアント接続失敗	[4] 接続タイムアウト	VDAがセッション起動のために準備された後、クライアントはVDAに接続しませんでした。セッションは正常に仲介されましたが、クライアントがVDAに接続するのを待っている間にタイムアウトが発生しました。考えられる原因: ファイアウォール設定、ネットワークの中断、またはリモート接続を妨げる設定。	Directorコンソールで、クライアントが現在アクティブな接続を持っているかどうかを確認してください。これは、ユーザーに影響がないことを意味します。セッションが存在しない場合は、クライアントとVDAのイベントログでエラーを確認してください。クライアントとVDA間のネットワーク接続に関する問題を解決してください。
[4] 利用可能なライセンスなし	[5] ライセンス	ライセンス要求が失敗しました。考えられる原因: ライセンス数が不足している、またはライセンスサーバーが30日以上ダウンしている。	ライセンスサーバーがオンラインで到達可能であることを確認します。ライセンスサーバーへのネットワーク接続の問題を解決するか、ライセンスサーバーが誤動作しているように見える場合は再起動します。環境内に十分なライセンスがあることを確認し、必要に応じて追加で割り当てます。
[1] ClientConnectionFailure	[6] チケッティング	チケット発行中にエラーが発生しました。これは、VDAへのクライアント接続が仲介された要求と一致しないことを示しています。起動要	デリバリーグループで定義されたユーザーグループに基づいて、ユーザーがアプリケーションまたはデスクトップにアクセスできることを

カテゴリ	理由	問題	アクション
		求チケットはBrokerによって準備され、ICA®ファイルで配信されます。ユーザーがセッションを起動しようとすると、VDAはICAファイル内の起動チケットをBrokerで検証します。考えられる原因：ICAファイルが破損しているか、ユーザーが不正な接続を試みている。	確認します。これが一時的な問題であるかどうかを判断するために、ユーザーにアプリケーションまたはデスクトップを再起動するように指示します。問題が再度発生する場合は、クライアントデバイスのイベントログでエラーを確認します。ユーザーが接続しようとしているVDAが登録されていることを確認します。登録されていない場合は、VDAのイベントログを確認し、登録に関する問題を解決します。
[1] ClientConnectionFailure	[7] その他	クライアントが最初にVDAに接続した後、接続シーケンスを完了する前に、セッションがVDAから終了したと報告されました。	起動前にユーザーによってセッションが終了されなかったことを確認します。セッションの再起動を試み、問題が解決しない場合は、CDFログを収集してCitrixサポートに連絡してください。
[1] ClientConnectionFailure	[8] GeneralFail	セッションの起動に失敗しました。考えられる原因：ブローカーがまだ起動中または初期化中に仲介された起動が要求された、または起動の仲介フェーズ中に内	Citrix Broker Serviceが実行されていることを確認し、セッションの起動を再試行します。

カテゴリ	理由	問題	アクション
		部エラーが発生した。	
[5] 設定	[9] MaintenanceMode	VDA、またはVDAが属するデリバリーグループがメンテナンスモードに設定されています。	メンテナンスモードが必要かどうかを判断します。不要な場合は、該当するデリバリーグループまたはマシンでメンテナンスモードを無効にし、ユーザーに再接続を試みるよう指示します。
[5] 構成	[10] アプリケーション無効	アプリケーションは管理者によって無効にされているため、エンドユーザーはアクセスできません。	アプリケーションが本番環境で使用されることを意図している場合は、アプリケーションを有効にし、ユーザーに再接続するよう指示します。
[4] 利用可能なライセンスなし	[11] ライセンス機能拒否	使用されている機能は、既存のライセンスではカバーされていません。	既存のCitrix Virtual Apps and Desktops™ライセンスのエディションとタイプでカバーされている機能を確認するには、Citrixの営業担当者にお問い合わせください。
[3] 利用可能な容量なし	[13] セッション制限に到達	すべてのVDAが使用中であり、これ以上セッションをホストする容量がありません。考えられる原因：すべてのVDAが使用中である（シングルセッションOS	メンテナンスモードになっているVDAがないか確認します。容量を増やすために不要な場合は、メンテナンスモードを無効にします。Citrixポリシー設定の**最大**

カテゴリ	理由	問題	アクション
		VDAの場合）、またはすべてのVDAが設定された最大同時セッション数に達している（マルチセッションOS VDAの場合）。	**セッション数**の値を増やして、サーバーVDAあたりのセッション数を増やすことを検討してください。マルチセッションOS VDAを追加することを検討してください。シングルセッションOS VDAを追加することを検討してください。
[5] 構成	[14] DisallowedProtocol	ICAおよびRDPプロトコルは許可されていません。	デリバリーコントローラーで**Get-BrokerAccessPolicyRule** PowerShellコマンドを実行し、**AllowedProtocols**の値に目的のプロトコルがすべてリストされていることを確認します。この問題は、構成が誤っている場合にのみ発生します。
[5] 構成	[15] ResourceUnavailable	ユーザーが接続しようとしているアプリケーションまたはデスクトップは利用できません。このアプリケーションまたはデスクトップが存在しないか、実行できるVDAがありません。考えられる原因：アプリケーションまたはデスクトップが非公開になっている、アプリケー	アプリケーションまたはデスクトップがまだ公開されており、VDAがメンテナンスモードではないことを確認します。マルチセッションOS VDAがフルロード状態であるかどうかを判断します。もしそうであれば、さらにマルチセッションOS VDAをプロビジョニングします。接続に

カテゴリ	理由	問題	アクション
		ションまたはデスクトップをホストしているVDAが最大負荷に達している、またはアプリケーションまたはデスクトップがメンテナンスモードに設定されている。	利用可能なシングルセッションOS VDAがあることを確認します。必要に応じて、さらにシングルセッションOS VDAをプロビジョニングします。
[5] 構成	[16] ActiveSessionReconnectDisabled	ICAセッションはアクティブで、別のエンドポイントに接続されています。しかし、**Active Session Reconnection**が無効になっているため、クライアントはアクティブなセッションに接続できません。	デリバリーコントローラーで、**Active Session Reconnection**が有効になっていることを確認します。レジストリの**HKEY_LOCAL_MACHINE\Software\Citrix\Desktop\Server**の下にある**DisableActiveSessionReconnect**の値が0に設定されていることを確認します。
[2] MachineFailure	[17] NoSessionToReconnect	クライアントは特定のセッションに再接続しようとしましたが、セッションは終了しました。	ワークスペースコントロールの再接続を再試行してください。
[2] MachineFailure	[18] SpinUpFailed	セッション起動のためにVDAの電源をオンにできません。これはハイパーバイザーが報告した問題です。	マシンがまだ電源オフの状態である場合は、Citrix Studioからマシンの起動を試みてください。これが失敗した場合は、ハイパーバイザーの接続性と権限を確認してください。VDAが

カテゴリ	理由	問題	アクション
			PVSプロビジョニングされたマシンである場合は、PVSコンソールでマシンが実行中であることを確認してください。実行中でない場合は、マシンにパーソナルvDiskが割り当てられていることを確認し、ハイパーバイザーにログインしてVMをリセットしてください。
[2] MachineFailure	[19] 拒否	デリバリーコントローラーは、エンドユーザーからの接続に備えるようVDAに要求を送信しますが、VDAはこの要求を積極的に拒否します。	pingを使用して、デリバリーコントローラーとVDAが正常に通信できることを確認してください。通信できない場合は、ファイアウォールまたはネットワークルーティングの問題を解決してください。
[2] MachineFailure	[20] 構成セット失敗	デリバリーコントローラーは、セッション起動中にポリシー設定やセッション情報などの必要な構成データをVDAに送信しませんでした。考えられる原因：コントローラーとVDA間の通信の問題、構成セット要求の作成中にブローカーサービスで発生した問題、または	-

カテゴリ	理由	問題	アクション
		VDAが要求を受け入れない原因となるネットワークの問題。	
[3] NoCapacityAvailable	[21] MaxTotalInstancesExceeded	アプリケーションのインスタンスの最大数に達しました。VDA上でアプリケーションの追加インスタンスを開くことはできません。この問題は、アプリケーション制限機能に関連しています。	ライセンスが許す範囲で、アプリケーション設定の「**同時に実行するインスタンスの数を制限する**」をより高い値に増やすことを検討してください。
[3] NoCapacityAvailable	[22] MaxPerUserInstancesExceeded	ユーザーがアプリケーションの複数のインスタンスを開こうとしていますが、アプリケーションはユーザーごとに単一のインスタンスのみを許可するように構成されています。この問題は、アプリケーション制限機能に関連しています。	デフォルトでは、ユーザーごとにアプリケーションのインスタンスは1つのみ許可されます。ユーザーごとに複数のインスタンスが必要な場合は、アプリケーション設定の「**ユーザーごとに1つのインスタンスに制限する**」設定をクリアすることを検討してください。
[1] ClientConnectionFailure	[23] 通信エラー	デリバリーコントローラーがVDAに接続準備の要求などの情報を送信しようとしましたが、通信中にエラーが発生しました。これはネットワーク障害が原因である可能性があります。	既に開始されている場合は、VDA上のDesktopサービスを再起動して登録プロセスを再開し、VDAが正常に登録されることを確認します。アプリケーションイベントログの詳細を通じて、VDA用に構

カテゴリ	理由	問題	アクション
			成されているデリバリーコントローラーが正確であることを確認します。
[3] NoCapacityAvailable	[100] NoMachineAvailable 監視サービスは [12] NoDesktopAvailable をこのエラーコードに変換します。	セッションの起動に割り当てられたVDAが無効な状態であるか、利用できません。考えられる原因：VDAの電源状態が不明または利用できない、前回のユーザーセッション以降VDAが再起動されていない、現在のセッションでセッション共有が有効になっている必要があるのに無効になっている、またはVDAがデリバリーグループまたはサイトから削除された。	VDAがデリバリーグループ内にあることを確認します。ない場合は、適切なデリバリーグループに追加します。ユーザーが要求した公開共有デスクトップまたはアプリケーションを起動できるように、十分なVDAが登録され、準備完了状態であることを確認します。VDAをホストしているハイパーバイザーがメンテナンスモードではないことを確認します。
[2] MachineFailure	[101] MachineNotFunctional. 監視サービスは [12] NoDesktopAvailable をこのエラーコードに変換します。	VDAが動作していません。考えられる原因：VDAがデリバリーグループから削除された、VDAが未登録である、VDAの電源状態が利用できない、またはVDAが内部的な問題を抱えている。	VDAがデリバリーグループに含まれていることを確認します。含まれていない場合は、適切なデリバリーグループに追加します。Citrix StudioでVDAが電源オンとして表示されていることを確認します。複数のマシンの電源状態が不明な場合は、ハイパーバイザーへの接続に関する問題またはホストの障害を解決しま

カテゴリ	理由	問題	アクション
			す。VDAをホストしているハイパーバイザーがメンテナンスモードではないことを確認します。これらの問題が解決されたら、VDAを再起動します。

マシン障害の種類

エラーコード	エラーコードID	問題	アクション
不明	-	-	-
未登録	3	-	-
MaxCapacity (Director上では最大負荷として表示されます)	4	マシンが最大容量に達している、つまり最大負荷インデックスを報告しています。	すべてのハイパーバイザーが電源オンになっていることを確認してください。ハイパーバイザーに容量を追加するか、またはハイパーバイザーを追加することによって、影響を受けるデリバリーグループにマシンを追加します。
StuckOnBoot	2	VMが起動シーケンスを完了せず、ハイパーバイザーと通信していません。	VMがハイパーバイザー上で正常に起動したことを確認してください。OSの問題など、VM上の他のメッセージを確認してください。ハイパーバイザーツールがVMにインストールされていることを確認してください。

エラーコード	エラーコードID	問題	アクション
			VDAがVMにインストールされていることを確認してください。
FailedToStart	1	ハイパーバイザー上で起動しようとしたときに、VMで問題が発生しました。	ハイパーバイザーのログを確認してください。
なし	0	-	-

マシンの登録解除理由 (障害タイプが「未登録」または「不明」の場合に適用)

エラーコード	エラーコード ID	問題	アクション
AgentShutdown	0	VDA が正常にシャットダウンされました。	既存の電源管理ポリシーに基づいて VDA がオフになっていることが予期されない場合は、VDA の電源をオンにします。イベントログでエラーを確認してください。
AgentSuspended	1	VDA は休止状態またはスリープモードです。	VDA を休止状態から復帰させます。電源設定を介して Citrix Virtual Apps and Desktops VDA の休止状態を無効にすることを検討してください。
IncompatibleVersion	100	Citrixプロトコルバージョンの不一致により、VDAはデリバ	VDAとデリバリーコントローラーのバージョンを合わせます。

エラーコード	エラーコード ID	問題	アクション
		リーコントローラーと通信できません。	
AgentAddressResolutionFailed	101	デリバリーコントローラーは、VDAのIPアドレスを解決できませんでした。	VDAマシンアカウントがADに存在することを確認します。存在しない場合は、作成します。DNS内のVDAの名前とIPアドレスが正確であることを確認します。正確でない場合は、修正します。広範囲にわたる場合は、デリバリーコントローラーのDNS設定を検証します。コントローラーから `nslookup` コマンドを実行して、DNS解決を確認します。
[Cloud]:AgentAddressResolutionFailed	101	デリバリーコントローラーは、VDAのIPアドレスを解決できませんでした。	VDAマシンアカウントがADに存在することを確認します。存在しない場合は、作成します。DNS内のVDAの名前とIPアドレスが正確であることを確認します。正確でない場合は、修正します。
AgentNotContactable	102	デリバリーコントローラーとVDA間で通信の問題が発生しました。	pingを使用して、デリバリーコントローラーとVDAが正常に通信できることを確認します。できない場合は、ファイアウォールまたはネットワークの問題を解

エラーコード	エラーコード ID	問題	アクション
			決します。コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。
[Cloud]: AgentNotContactable	102	デリバリーコントローラーとVDAの間で通信の問題が発生しました。	コントローラーとVDA間の通信問題を引き起こす一般的な問題については、ナレッジセンターの記事「Citrix Virtual Apps and Desktopsにおけるデリバリーコントローラーとの Virtual Delivery Agent登録のトラブルシューティング (CTX136668)」(https://support.citrix.com/article/CTX136668)に記載されているトラブルシューティング手順を参照してください。Citrixサポートにお問い合わせください。

エラーコード	エラーコード ID	問題	アクション
AgentWrongActiveDirectoryOU	103	Active Directoryの検出設定に誤りがありました。VDAレジストリで構成されているサイト固有のOU（サイトコントローラー情報がADに保存されている場所）が、別のサイト用です。	Active Directoryの設定が正しいことを確認するか、レジストリ設定を確認してください。
EmptyRegistrationRequest	104	VDAからデリバリーコントローラーに送信された登録要求が空でした。これは、VDAソフトウェアのインストールが破損していることが原因である可能性があります。	VDA上のDesktopサービスを再起動して登録プロセスを再開し、アプリケーションイベントログを介してVDAが正しく登録されていることを確認してください。
MissingRegistrationCapabilities	105	VDAのバージョンがデリバリーコントローラーと互換性がありません。	VDAをアップグレードするか、VDAを削除してから再インストールします。
MissingAgentVersion	106	VDAのバージョンがデリバリーコントローラーと互換性がありません。	問題がすべてのマシンに影響している場合は、VDAソフトウェアを再インストールします。
InconsistentRegistrationCapabilities	107	VDAはBrokerにその機能を通信できません。これは、VDAとデリバリーコントローラーのバージョン間の非互換性が原因である可能性があります。各バージョンで変更される登録	VDAとデリバリーコントローラーのバージョンを合わせます。

エラーコード	エラーコード ID	問題	アクション
		機能は、登録要求と一致しない形式で表現されています。	
NotLicensedForFeature	108	使用しようとしている機能はライセンスされていません。	Citrixライセンスエディションを確認するか、VDAを削除してから再インストールしてください。
[Cloud]: NotLicensedForFeature	108	使用しようとしている機能はライセンスされていません。	Citrixサポートにお問い合わせください。
サポートされていないCredentialSecurityバージョン	109	VDAとデリバリーコントローラーは同じ暗号化メカニズムを使用していません。	VDAとデリバリーコントローラーのバージョンを合わせてください。
InvalidRegistrationRequest	110	VDAはBrokerに登録要求を行いましたが、要求の内容が破損しているか無効です。	コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。
SingleMultiSessionMismatch	111	VDAのオペレーティングシステムの種類は、マシンカタログまたはデリバリーグ	VDAを、同じオペレーティングシステムを持つマシンを含む正しいマシンカタ

エラーコード	エラーコード ID	問題	アクション
		ループと互換性がありません。	ログタイプまたはデリバリーグループに追加してください。
FunctionalLevelTooLowForCatalog	112	マシンカタログが、インストールされているVDAバージョンよりも高いVDA機能レベルに設定されています。	VDAのマシンカタログ機能レベルがVDAの機能レベルと一致していることを確認します。VDAの機能レベルと一致するように、マシンカタログをアップグレードまたはダウングレードします。
FunctionalLevelTooLowForDesktopGroup	113	デリバリーグループが、インストールされているVDAバージョンよりも高いVDA機能レベルに設定されています。	VDAのデリバリーグループ機能レベルがVDAの機能レベルと一致していることを確認します。VDAの機能レベルと一致するように、マシンカタログをアップグレードまたはダウングレードします。
PowerOff	200	VDAが正常にシャットダウンされませんでした。	VDAが電源オンの状態であるべき場合、Citrix StudioからVDAを起動してみて、VDAが正常に起動して登録されることを確認します。起動または登録に関する問題をトラブルシューティングします。VDAが再び起動したら、イベントログを確認し、シャットダウンの根本原因を特

エラーコード	エラーコード ID	問題	アクション
			定するのに役立ててください。
AgentRejectedSettingsUpdate	203	Citrixポリシーなどの設定が変更または更新されましたが、VDAへの更新の送信中にエラーが発生しました。これは、更新がインストールされているVDAバージョンと互換性がない場合に発生する可能性があります。	必要に応じてVDAをアップグレードします。適用された更新がVDAバージョンでサポートされているかどうかを確認します。
SessionPrepareFailure	206	Broker が VDA で実行されているセッションの監査を完了しませんでした。	広範囲にわたる場合は、デリバリーコントローラーで Citrix Broker Service を再起動してください。
[Cloud]: SessionPrepareFailure	206	Broker が VDA で実行されているセッションの監査を完了しませんでした。	Citrix サポートにお問い合わせください。
ContactLost	207	デリバリーコントローラーが VDA との接続を失いました。これはネットワーク障害が原因である可能性があります。	デリバリーコントローラーで Citrix Broker Service が実行されており、VDA で Desktop Service が実行されていることを確認します。停止している場合はそれぞれを起動します。すでに起動している場合は、VDA で Desktop Service を再起動して登録プロセスを再開し、VDA が正常に登録される

エラーコード	エラーコード ID	問題	アクション
			ことを確認します。アプリケーションイベントログの詳細を介して、VDA 用に構成されているデリバリーコントローラーが正確であることを確認します。ping を使用して、デリバリーコントローラーと VDA が正常に通信できることを確認します。通信できない場合は、ファイアウォールまたはネットワークの問題を解決します。
[Cloud]: ContactLost	207	デリバリーコントローラーが VDA との接続を失いました。これはネットワーク障害が原因である可能性があります。	VDA で Desktop サービスが実行されていることを確認します。停止している場合は開始します。
BrokerRegistrationLimitReached	301	デリバリーコントローラーが、同時に登録できる VDA の設定された最大数に達しました。デフォルトでは、デリバリーコントローラーは 10,000 の同時 VDA 登録を許可します。	サイトにデリバリーコントローラーを追加するか、サイトを作成することを検討してください。また、**HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\MaxWorkers** レジストリキーを使用して、デリバリーコントローラーに同時に登録できる VDA の数を増やすことまで

エラーコード	エラーコード ID	問題	アクション
			きます。詳細については、Knowledge Center の記事「Registry Key Entries Used by Citrix Virtual Apps and Desktops (CTX117446)」を参照してください。この数を増やすと、コントローラーにより多くの CPU およびメモリリソースが必要になる場合があります。
SettingsCreationFailure	208	Broker が VDA に送信する設定と構成のセットを構築しませんでした。Broker がデータを収集できない場合、登録は失敗し、VDA は登録解除されます。	デリバリーコントローラーのイベントログでエラーがないか確認します。ログに特定の問題が明らかでない場合は、Broker Service を再起動します。Broker Service の再起動後、影響を受ける VDA で Desktop サービスを再起動し、正常に登録されることを確認します。
[Cloud]: SettingsCreationFailure	208	Broker が VDA に送信する設定と構成のセットを構築しませんでした。Broker がデータを収集できない場合、登録は失敗し、VDA は登録解除されます。	影響を受ける VDA で Desktop サービスを再起動し、正常に登録されることを確認します。Citrix サポートに連絡してください。

エラーコード	エラーコード ID	問題	アクション
SendSettingsFailure	204	BrokerがVDAに設定と構成データを送信しませんでした。Brokerがデータを収集できても送信できない場合、登録は失敗します。	単一のVDAに限定される場合、VDA上のDesktopサービスを再起動して再登録を強制し、アプリケーションイベントログを介してVDAが正常に登録されることを確認します。発生したエラーをトラブルシューティングします。コントローラーとVDA間の通信問題を引き起こす一般的な問題については、ナレッジセンターの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。
AgentRequested	2	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
DesktopRestart	201	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
DesktopRemoved	202	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
SessionAuditFailure	205	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。

エラーコード	エラーコード ID	問題	アクション
UnknownError	300	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
RegistrationStateMismatch	302	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
不明	-	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。

DirectorとのSecure Private Access統合（プレビュー）

DirectorとのSecure Private Access統合により、ヘルプデスク管理者またはフル管理者は、Directorですべてのセッションを監視およびトラブルシューティングできます。この機能をサポートするには、Director、Secure Private Access、Citrix Workspace™アプリ、およびVDAのバージョン2402以降を使用する必要があります。

利用可能なアクションには、以下の詳細の表示が含まれます。

- **Select a Session**ポップアップ > **Sessions**タブ > **Web SaaS and Client/Server Apps**の下にあるユーザーのSecure Private Accessアクティブセッション
- **Select a Session**ポップアップ > **Denied Access**タブの下にあるSecure Private Accessの失敗またはブロックされた列挙、および失敗したアプリの起動
- アクティブおよび失敗したアプリの起動のセッションとアプリケーションの詳細ビュー
- 失敗およびブロックされた列挙のセッションとアプリケーションの詳細ビュー

> **注：**
>
> DirectorとのSecure Private Access統合は、Directorのフォームベース認証でのみサポートされており、統合Windows認証またはスマートカードベース認証ではサポートされていません。

前提条件

1. この機能をサポートするには、以下を使用する必要があります。
    - Director 2402以降のバージョン

- Secure Private Access 2402以降のバージョン
- Citrix Workspaceアプリ 2402以降のバージョン

2. Directorに少なくとも1つのCitrix Virtual Apps and Desktops™サイトが構成されていることを確認してください。
3. 「Secure Private Access をセットアップする」(/ja-jp/citrix-secure-private-access/current-release/spa-onprem-setup-spa.html)。
4. DirectorサーバーがSecure Private Accessサーバーへのネットワーク接続を持っていることを確認してください。

> **注:**
>
> Citrix Directorへの接続を正常に確立するには、信頼された証明書がSecure Private Accessサーバーにインストールされている必要があります。

5. Director管理者ユーザーが以下の権限を持っていることを確認してください。
   a. Secure Private Access管理コンソールでのSecure Private Accessフル管理者または読み取り専用管理者。
   b. Citrix StudioコンソールでのCitrix Virtual Apps™またはDesktopsヘルプデスク、フル管理者、または読み取り専用管理者。

DirectorをSecure Private Accessで構成する

1. Directorがインストールされているマシンで、管理者としてコマンドプロンプトを開きます。
2. 次のコマンドを実行して、`DirectorConfig`ツールのパスに移動します。

```
cd c:\inetpub\wwwroot\Director\tools
```

3. Secure Private Accessを構成するには、次のコマンドを実行します。

```
DirectorConfig.exe /configspa
```

4. Secure Private Accessがインストールされているマシンの FQDNとポート番号を入力します。
5. Secure Private Access（サーバーまたはロードバランサー）への接続が安全であり、信頼された証明書が適用されていることを確認してください。

Director SPA構成ツール(/en-us/citrix-virtual-apps-desktops/2411/media/director-spa-config-tool.png)

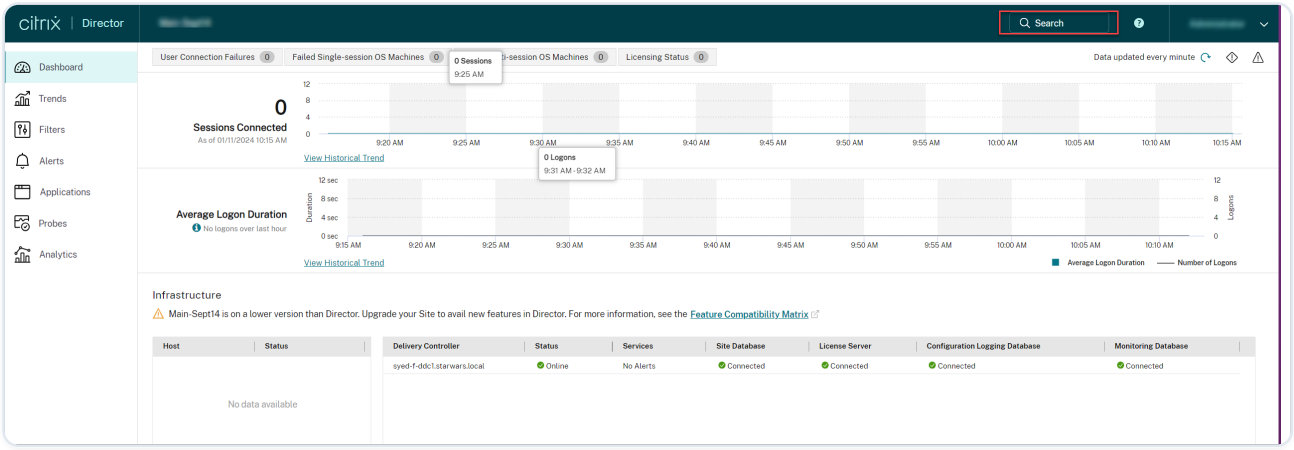
注:

Director で Secure Private Access セッションの詳細を表示するには、管理者を Secure Private Access コンソールに追加する必要があります。詳細については、「管理者の管理」を参照してください。

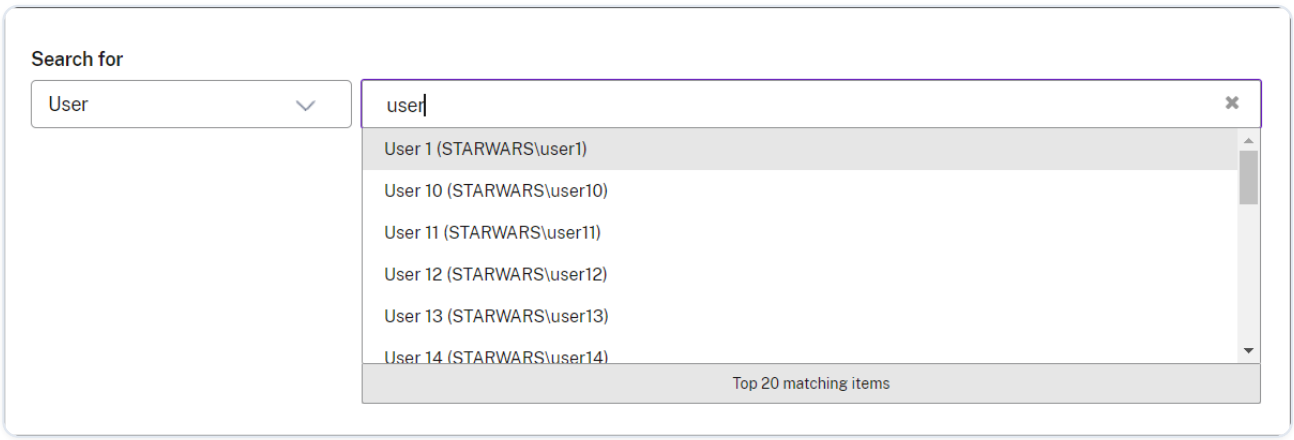
ユーザー別の Secure Private Access セッションの表示

Director ダッシュボードで、 をクリックし、ユーザー名を入力します。 画面が表示されます。

フル管理者:



ヘルプデスク管理者:



Secure Private Access セッションの Activity Manager の表示

Citrix Director は、Secure Private Access セッションの Activity Manager ビューを提供し、セッションアクティビティの全体像を把握できます。Activity Manager は、正常に開かれた、開くのに失敗したすべてのアプリとデスクトップ、および Secure Private Access アプリで設定されたポリシーの結果を包括的に表示します。この機能は、Citrix Virtual Apps and Desktops バージョン 2407 以降で利用できます。

前提条件:

- Director 2407 以降のバージョン
- Secure Private Access 2407 以降のバージョン

Activity Manager には、 と の詳細が表示されます。次のセッションの詳細を確認できます。

- 起動時間
- リソース名
- リソースの種類
- アクセスされたリソース
- ステータス
- トランザクションID

Activity Managerを表示するには、次の手順を実行します。

1. Directorダッシュボードで、**検索**をクリックし、ユーザー名を入力します。「**セッションの選択**」画面が表示されます。
2. Secure Private Accessセッションを使用して開かれたセッションを選択します。選択したセッションのアクティビティマネージャーが表示されます。

   アクティビティマネージャー(/en-us/citrix-virtual-apps-desktops/2411/media/spa-activity-manager.png)
3. **利用可能なアプリ**をクリックして、Citrix Workspaceアプリで利用可能なアプリを表示します。

または、,

起動されたアプリ（セッション）をクリックして、Citrix Workspaceアプリで開かれているアプリを表示します。

Secure Private Accessアプリで設定されたリソースのステータスでリソースをフィルタリングできます。

- 許可 - ユーザーがアクセスを許可されているリソース。このステータスは、Secure Private Accessアプリのポリシーを使用して設定されます。このリソースは、Citrix Workspaceアプリでユーザーに表示されます。
- 拒否 - ユーザーがアクセスを拒否されているリソース。このステータスは、Secure Private Accessアプリのポリシーを使用して設定されます。このリソースは、Citrix Workspaceアプリでユーザーに表示されます。
- エラー - Secure Private Accessアプリでユーザーがアクセスを許可されているリソース。ただし、何らかのエラーにより、Citrix Workspaceアプリでリソースが利用できません。列挙エラーとセッションエラーの2種類のエラーがあります。

利用可能なアプリを表示

Citrix Workspaceアプリで利用可能なWebアプリとSaaSアプリは、**利用可能なアプリ**セクションに表示されます。このセクションには、アプリの最後の列挙試行と、その列挙試行のステータスが表示されます。

以下の詳細を表示できます。

- リソース名
- ステータス
- トランザクションID

アプリケーションステータス（**許可**、**拒否**、**エラー**など）で、上記の詳細をフィルタリングすることもできます。上下矢印を使用して詳細を並べ替えることもできます。

> **注:**
>
> TCP/UDPアプリは、**利用可能なアプリ**セクションには表示されません。

起動されたアプリを表示

Citrix Workspaceアプリで開かれたアプリは、**起動されたアプリ（セッション）**セクションに表示されます。次の詳細を表示できます。

- 起動時間
- リソース名

- リソースの種類
- アクセスされたリソース
- 状態
- トランザクションID

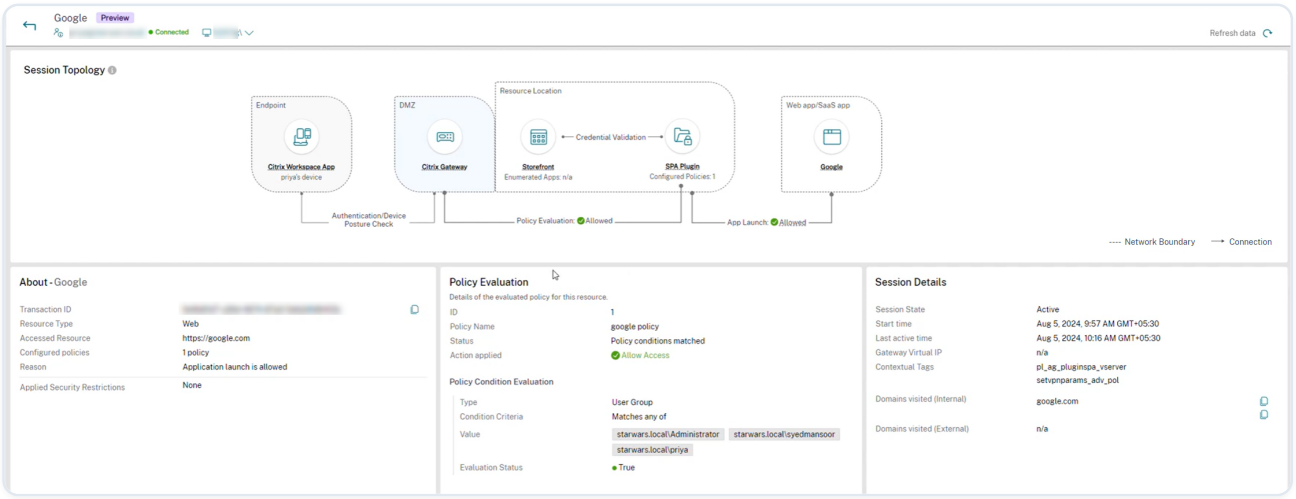
前述の詳細を、**許可**、**拒否**、**エラー**などのアプリケーションステータスでフィルタリングすることもできます。また、上下の矢印を使用して詳細を並べ替えることもできます。

Secure Private Access アプリのセッション トポロジ ビュー

Secure Private Access を使用して開かれたアプリのセッション トポロジを表示できます。選択したアプリのセッション トポロジを表示するには、**アクティビティ マネージャー**から目的のアプリをクリックします。

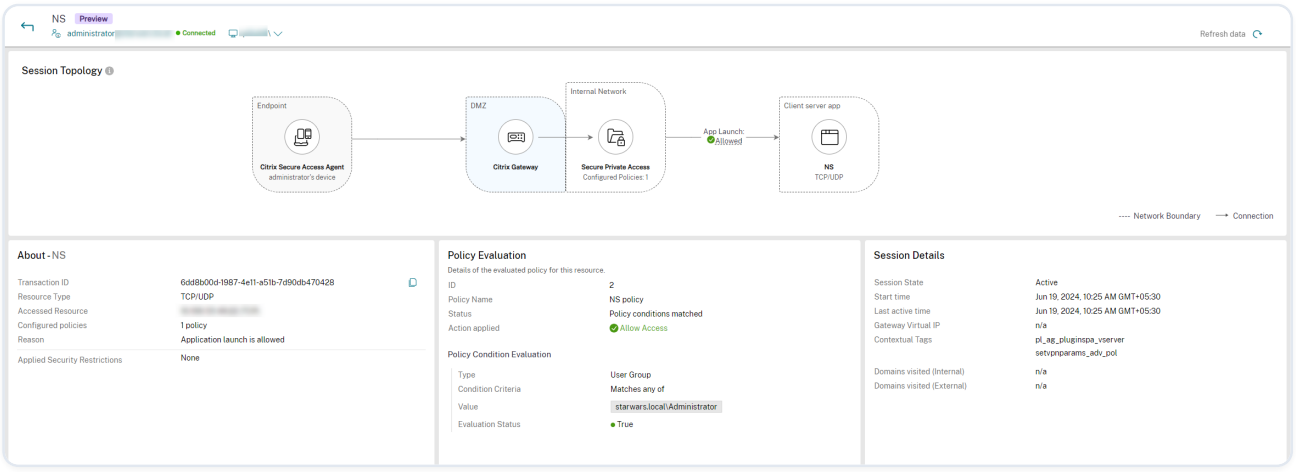
Web/SaaS アプリ:

WebまたはSaaSのセッショントポロジ



TCP/UDP アプリ:

アクティビティマネージャー



セッショントポロジビューは、アプリ起動プロセスのフローを提供します。エンドポイントはCitrix Gatewayに接続し、Citrix GatewayはSecure Private Accessプラグインに接続します。Secure Private Accessプラグインからの情報を使用して、アプリが起動されます。この機能は、Citrix Virtual Apps and Desktopsバージョン2407以降で利用可能です。

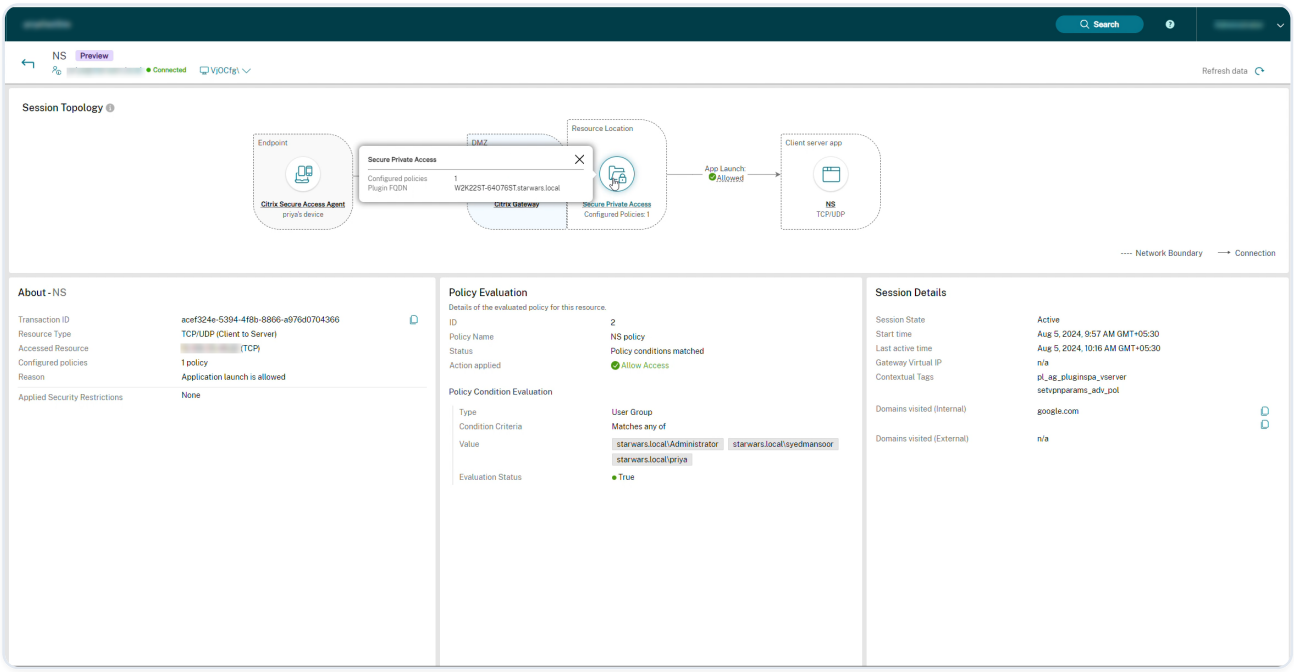
前提条件:

- Director 2407 以降のバージョン
- Secure Private Access 2407 以降のバージョン
- Citrix Secure Access 24.8.1.x 以降のバージョン

以下を表示できます。

- Endpoint - アプリが開かれるエンドポイントを表示します。選択可能なオプションは、Citrix WorkspaceアプリとCitrix Secure Agentです。デバイスIDが表示されます。
- Internal network - 列挙されたアプリの数と構成されたポリシーの数を表示します。
- Policy evaluation - Secure Private Accessアプリに設定されているポリシーの結果を表示します。異なる値は、**許可**、**拒否**、**制限付きアクセス許可**、および**エラー**です。これはWebまたはSaaSアプリにのみ適用されます。
- アプリ起動 - アプリの種類とアプリ起動のステータスを表示します。アプリの種類として可能な値は、Web/SaaSアプリまたはTCP/UDPアプリです。同様に、アプリ起動ステータスとして可能な値は、**許可**、**拒否**、**制限付きアクセス許可**、および**エラー**です。

セキュアプライベートアクセスアプリの**セッショントポロジ**ビューで、以下の追加の詳細を表示できるようになりました。この変更は、TCP/UDPアプリに加えて、ウェブアプリとサースアプリの両方に適用されます。



エンドポイント:

エンドポイント内のリンクをクリックすると、以下が表示されます。

- **エンドポイントの種類:** これは、Secure Access AgentまたはCitrix Workspaceアプリのいずれかです。
- **アクセス詳細:** エンドポイントがStoreFront™またはCitrix Workspaceアプリのどちらを介してアクセスされたかを表示します。
- **エンドポイントOS:** 例: Windows。
- **場所の種類:** 場所が内部か外部かを示します。

リソースの場所:

リソースの場所内のリンクをクリックすると、以下が表示されます。

> **注:** これは Web および SaaS アプリにのみ適用されます。

- **列挙されたアプリケーションの数:** 列挙されたアプリケーションの数とストアURLを表示します。
- **アクセス方法:** エンドポイントがStoreFrontまたはCitrix Workspaceアプリを介してアクセスされるかどうかを示します。

セキュアプライベートアクセス:

- **構成済みポリシー:** 構成済みポリシーの数を表示します。

- **FQDNプラグイン:** リクエストを処理したエージェントのFQDNを表示します。

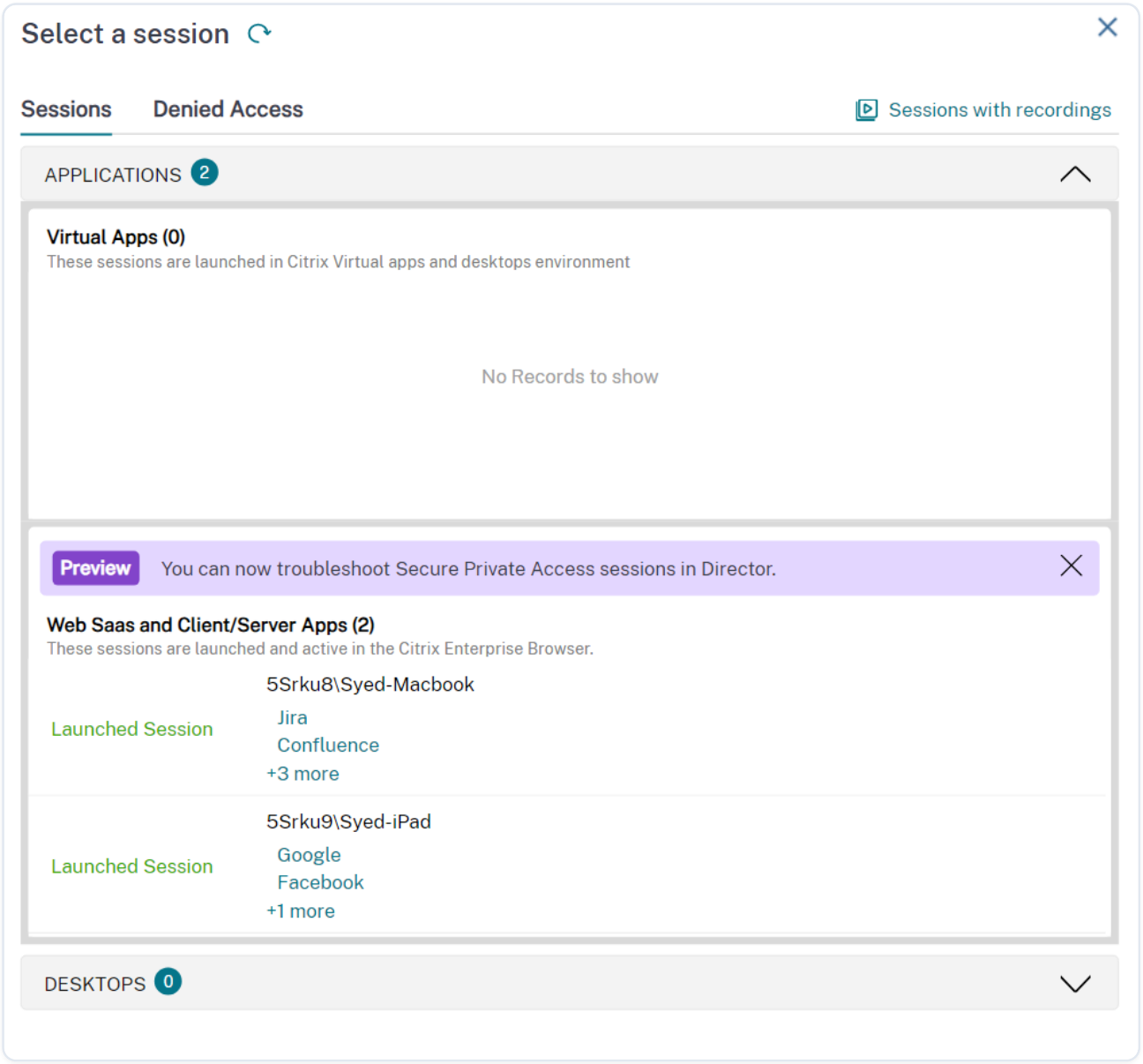
WebおよびSaaSアプリ / クライアントサーバーアプリ (TCP/UDP):

WebおよびSaaSアプリ / クライアントサーバーアプリ内のリンクをクリックすると、以下が表示されます。

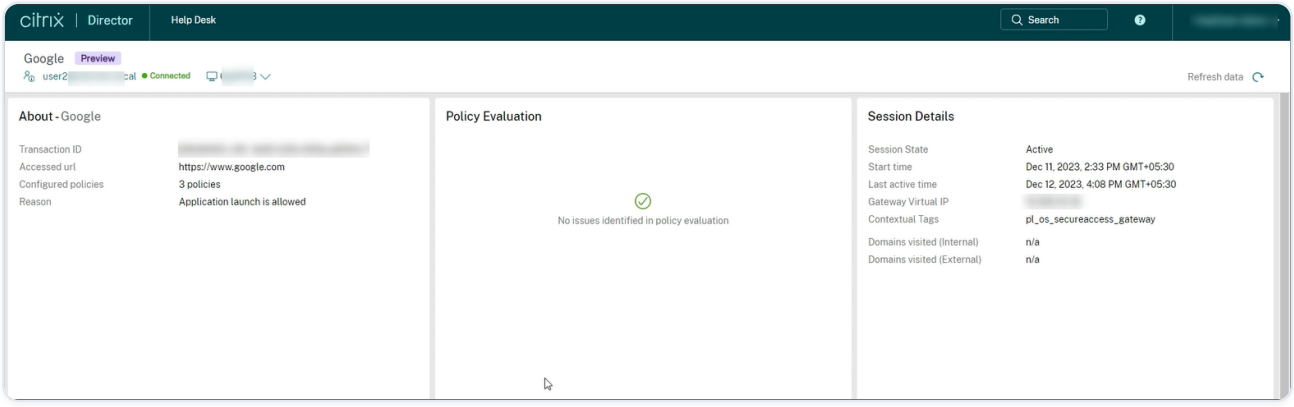
- **アプリ名:** アプリの名前。
- **トップレベルURL:** WebまたはSaaSアプリの場合、公開されたアプリのURLが表示されます。TCP/UDPアプリの場合、アプリのプロトコルIPアドレスが表示されます。
- **アプリの種類:** アプリがWebまたはSaaSアプリであるか、TCP/UDPアプリであるかを示します。
- **アプリの公開タイプ:** アプリが外部公開されているか内部公開されているかを示します。

正常に起動されたWebアプリとSaaSアプリを表示する

正常に起動されたアプリは、**Web SaaSおよびクライアント/サーバーアプリ**セクションに表示されます。



Web SaaSおよびクライアント/サーバーアプリセクションからアプリをクリックすると、詳細が表示されます。



成功コードの詳細については、「Citrix Director関連コード」(/ja-jp/citrix-secure-private-access/current-release/spa-onprem-director-info-codes)を参照してください。

アクセスが拒否されたアプリの詳細を表示する

「**セッションの選択**」画面で「**アクセス詳細の確認**」をクリックします。

Director SPAのアクセス詳細を確認(/en-us/citrix-virtual-apps-desktops/2411/media/director-check-access-details.png)

> **注:**
>
> アクティブなセッションがない場合、「**アクセス詳細の確認**」ボタンが表示されます。
>
> または、,

「**アクセス拒否**」タブをクリックして、アクセスが拒否されたアプリを表示します。

「**アクセス拒否**」タブが開きます。

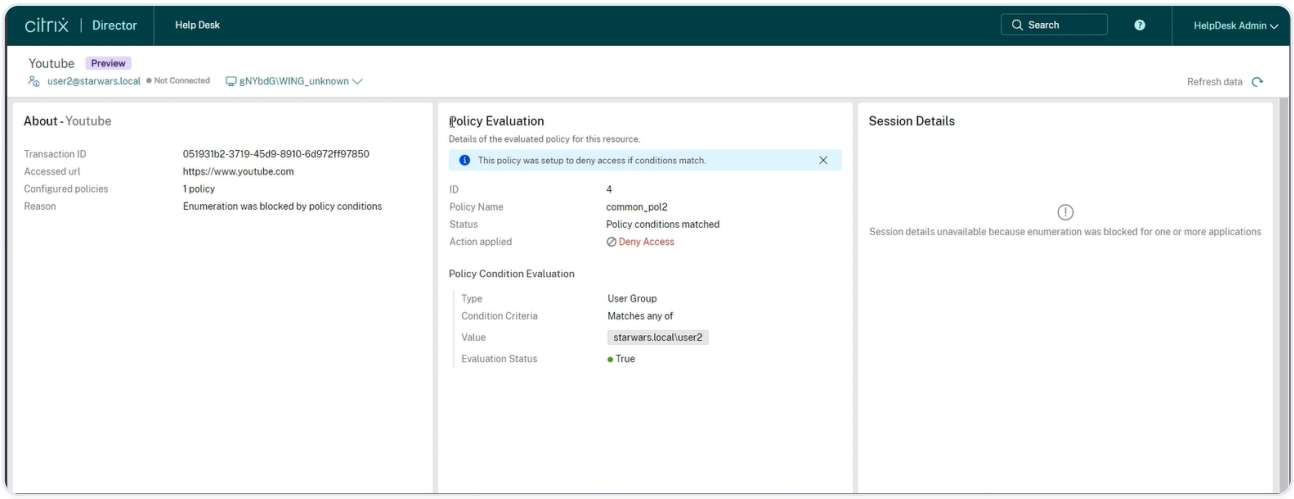
Director SPAのアクセス拒否の詳細(/en-us/citrix-virtual-apps-desktops/2411/media/director-spa-denied-access.png)

時間、リソース、エンドポイント名、失敗の理由などのセッション詳細が表示されます。エラーコードの詳細については、「Citrix Director関連コード」(/ja-jp/citrix-secure-private-access/current-release/spa-onprem-director-info-codes)を参照してください。

現在、以下の問題が特定されています。

- ポリシー条件により列挙が拒否されました
- アプリの起動エラー
- 列挙エラー
- ポリシー条件によりアプリの起動が拒否されました

詳細を表示するには、**Denied Access** タブ > **Resource** 列からアプリを選択します。



成功または失敗したセッションについて、以下の詳細が表示されます。

- アプリについて
- ポリシー評価
- セッションの詳細

アプリについて

成功、失敗、または拒否されたアプリの名前が表示されます。それに加えて、成功または失敗したアプリの以下の詳細が表示されます。

フィールド	説明
トランザクションID	セッション中または列挙中のCitrixトランザクションID。
リソースタイプ	リソースのタイプを表示します。指定可能な値は、Web、SaaS、TCP/UDP (サーバーからクライアントへ)、およびTCP/UDP (クライアントからサーバーへ) です。
アクセスされたリソース	セッションまたは列挙中にアクセスされたリソースのURL。TCPまたはUDPアプリの場合、アクセスされたリソースのタイプがTCPかUDPかを示します。
構成済みポリシー	セッションまたは列挙内で使用されるポリシーの数。
理由	セッションまたは列挙アクティビティの分析。

フィールド	説明
適用されたセキュリティ制限	Secure Private Accessアプリで適用されたセキュリティ制限を表示します。

ポリシー評価

成功したセッションの評価中に問題が検出されなかったことを表示します。失敗したセッションまたは列挙の場合、評価されたポリシーの以下の詳細が表示されます。

フィールド	説明
ID	Citrix トランザクション ID。
ポリシー名	ポリシーの名前。複数のポリシーがある場合、設定された条件に一致する最初のポリシーが表示されます。
ステータス	ポリシーのステータス。
適用されたアクション	ポリシーに適用されたアクション。たとえば、アクセス拒否。
ポリシー条件の評価	
タイプ	ポリシー条件のタイプ。
条件基準	失敗したセッションまたは列挙で適用されたポリシーの条件基準。
値	ポリシーの値。
評価ステータス	ポリシーの評価ステータス。異なる値は、**許可済み**、**拒否済み**、**制限付きでアクセス許可**、および**エラー**です。

セッションの詳細

失敗したセッションの場合、セッション失敗の理由が表示されます。成功したセッションの場合、次の詳細が表示されます。

フィールド	説明
セッションの状態	セッションがアクティブか非アクティブか、その状態を表示します。
開始時刻	セッションの開始時刻を表示します。
最終アクティブ時刻	成功したセッションの最終アクティブ時刻を表示します。
ゲートウェイ仮想IP	正常に接続されたセッションが接続されているゲートウェイの仮想IPアドレスを表示します。
コンテキストタグ	コンテキストタグを表示します。Secure Private Accessプラグインのコンテキストタグは、認証済みユーザーのセッションに適用されるNetScaler® Gatewayポリシー（セッション、事前認証、EPA）の名前です。
アクセスしたドメイン（内部）	成功したセッションを使用してアクセスされた内部ドメインを表示します。
アクセスしたドメイン (外部)	成功したセッションを使用してアクセスされた外部ドメインを表示します。

サードパーティ通知

このCitrix Virtual Apps and Desktops™リリースには、以下のドキュメントに定義されている条件に基づいてライセンス供与されたサードパーティ製ソフトウェアが含まれている場合があります。

- Citrix Virtual Apps and Desktops サードパーティ通知(/ja-jp/citrix-virtual-apps-desktops/2411/downloads/third-party-notices-apps-and-desktops.pdf) (PDFダウンロード)
- FlexNet Publisher 2017 (11.15.0.0) の非商用ソフトウェア開示(/ja-jp/citrix-virtual-apps-desktops/2411/downloads/fnp-licensing-11-15-0-ncsd-summary.pdf) (PDFダウンロード)
- FlexNet Publisher 11.15.0 で使用されている FlexNet Publisher ドキュメント補足 サードパーティおよびオープンソースソフトウェア(/ja-jp/citrix-virtual-apps-desktops/2411/downloads/fnp-licensing-11-15-0-opensource.pdf) (PDFダウンロード)

SDK および API

このリリースでは、いくつかのSDKとAPIが利用可能です。SDKとAPIにアクセスするには、Build anything with Citrixにアクセスしてください。そこから、**Citrix Workspace**を選択して、Citrix Virtual Apps and Desktopsおよび関連コンポーネントのプログラミング情報にアクセスします。

> **注:**
>
> Citrix Virtual Apps and Desktops™ SDKとCitrix Group Policy SDKは、モジュールまたはスナップインとしてインストールできます。いくつかのコンポーネントSDK（Citrix Licensing、Citrix Provisioning、StoreFrontなど）は、スナップインのみを使用してインストールされます。

> この製品はPowerShellバージョン3から5をサポートしています。

Citrix Virtual Apps and Desktops ソフトウェア開発キット

Delivery Controller™またはStudioをインストールすると、このSDKはPowerShellモジュールとして自動的にインストールされます。これにより、スナップインを追加することなく、このSDKのコマンドレットを使用できます。（このSDKをスナップインとしてインストールすることを選択した場合、手順は以下に記載されています。）

権限

Citrix管理権限を持つIDを使用してシェルまたはスクリプトを実行する必要があります。Controller上のローカル管理者グループのメンバーは、Citrix Virtual AppsまたはCitrix Virtual Desktops™をインストールするための完全な管理権限を自動的に持ちますが、Citrixは、通常の運用では、ローカル管理者アカウントを使用するのではなく、適切な権限を持つCitrix管理者を作成することを推奨します。

コマンドレットにアクセスして実行する

1. PowerShellでシェルを起動します。Studioを開き、**PowerShell**タブを選択し、**Launch PowerShell**をクリックします。

2. スクリプト内でSDKコマンドレットを使用するには、PowerShellで実行ポリシーを設定します。PowerShellの実行ポリシーについては、Microsoftのドキュメントを参照してください。
3. モジュールではなくスナップインを使用したい場合は、`Add-PSSnapin`（または`asnp`）コマンドレットを使用してスナップインを追加します。

   V1とV2はスナップインのバージョンを示します。XenDesktop 5のスナップインはバージョン1です。Citrix Virtual Apps and Desktops、およびそれ以前のXenDesktop 7バージョンのスナップインはバージョン2です。例えば、Citrix Virtual Apps and Desktopsスナップインをインストールするには、`Add-PSSnapin Citrix.ADIdentity.Admin.V2`と入力します。すべてのコマンドレットをインポートするには、次のように入力します。`Add-PSSnapin Citrix.*.Admin.V*`

これで、コマンドレットとヘルプファイルを使用できます。

- このSDKのヘルプファイルにアクセスするには、カテゴリリストで製品またはコンポーネントを選択し、次に**Citrix Virtual Apps and Desktops SDK**を選択します。
- PowerShellのガイダンスについては、Windows PowerShell Integrated Scripting Environment (ISE)を参照してください。

グループポリシーSDK

Citrixグループポリシー SDKを使用すると、グループポリシーの設定とフィルターを表示および構成できます。このSDKは、PowerShellプロバイダーを使用して、マシンおよびユーザーの設定とフィルターに対応する仮想ドライブを作成します。プロバイダーは`New-PSDrive`の拡張機能として表示されます。

Group Policy SDKを使用するには、StudioまたはCitrix Virtual Apps and Desktops SDKのいずれかがインストールされている必要があります。

Citrix Group Policy PowerShell プロバイダーは、モジュールまたはスナップインとして利用できます。

- モジュールを使用する場合、追加の作業は不要です。
- スナップインを追加するには、`Add-PSSnapin citrix.common.grouppolicy` と入力します。

ヘルプにアクセスするには、`help New-PSDrive -path localgpo:/`と入力します。

仮想ドライブを作成し、設定をロードするには、`New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>`と入力します。ここで、Controller文字列は、接続して設定をロードするサイト内のControllerの完全修飾ドメイン名です。

シトリックス バーチャル アプリケーションズ アンド デスクトップ REST API

Citrix Virtual Apps and Desktops REST APIを使用すると、Citrix Virtual Apps and Desktops展開内のリソースの管理を自動化できます。

Citrix Virtual Apps and Desktops REST APIは`<https://developer.cloud.com/citrixworkspace/citrix-daas-rest-apis/docs/citrix-virtual-apps-and-desktops-apis>`で利用できます。Citrix Virtual Apps and Desktopsに適用されないAPIは、そのようにマークされています。そこにあるガイダンスに従って、APIサービスへのアクセスを構成し、APIを使用してリソースを管理および最適化してください。

モニターサービス OData

Monitor API を使用すると、OData API のバージョン 3 または 4 を使用して Monitor Service データにアクセスできます。Monitor Service データからクエリされたデータに基づいて、カスタマイズされた監視およびレポートダッシュボードを作成できます。OData V.4 は ASP.NET Web API に基づいており、集計クエリをサポートしています。

詳細については、Monitor Service OData APIを参照してください。

Unicon™ のご紹介

完全に管理可能なエンドポイントOSでCitrix®エクスペリエンスを最大限に活用

Unicon とは?

Uniconは、仮想デスクトップエンドポイント向けのセキュアでリーンなオペレーティングシステムと管理ツールを提供します。eLux® OSとScout管理システムにより、Uniconのソフトウェアは、シンクライアント、デスクトップPC、ラップトップなどのエンドポイントで構成されるオンプレミスおよびクラウドのユースケースに非常に適しています。

eLux OSは、セキュアで軽量、ハードウェアに依存しないLinuxベースのオペレーティングシステムであり、管理対象エンドポイントで使用され、セキュアで一貫したエンドユーザーエクスペリエンスを提供します。一方、ScoutはeLuxデバイスを管理するためのエンドポイント管理ソリューションであり、エンドポイントインフラストラクチャの管理を簡素化します。

買収に関する詳細については、こちらの発表をご覧ください。

はじめに

Uniconとの統合を進めている間、UniconのWebサイトで以下のドキュメントリンクを見つけてください。

- Uniconドキュメントの使用方法: uDocs
- 管理者ガイド
- ショートガイド
- ホワイトペーパー
- 法的通知
- サードパーティソフトウェア
- PDFダウンロード

__index__

サイト全体の履歴トレンドを監視する

トレンドビューでは、以下のパラメーターについて、各サイトの履歴トレンド情報にアクセスできます。

- セッション
- 接続障害
- マシン障害
- ログオンパフォーマンス
- 負荷評価
- キャパシティ管理
- マシン使用状況
- リソース使用率
- 各サイトのネットワーク分析。

この情報を見つけるには、**トレンド**メニューをクリックします。

ズームイン・ドリルダウン機能を使用すると、期間を拡大表示（グラフのデータポイントをクリック）したり、トレンドに関連する詳細を表示するためにドリルダウンしたりすることで、トレンドチャートをナビゲートできます。この機能により、誰が、または何が影響を受けているかの詳細をよりよく理解できます。

各グラフのデフォルトのスコープを変更するには、データに別のフィルターを適用します。

履歴トレンド情報が必要な期間を選択します。期間の利用可能性は、Directorの展開によって次のように異なります。

- 最大1年間 (365日間) のトレンドレポートは、Premiumライセンスサイトで利用できます。
- 最大1か月間 (31日間) のトレンドレポートは、Advancedライセンスサイトで利用できます。
- 最大7日間のトレンドレポートは、PremiumおよびAdvanced以外のライセンスサイトで利用できます。

注:

- すべてのDirector展開において、期間が「先月」（**現在終了**）以下に設定されている場合、セッション、障害、ログオンパフォーマンスのトレンド情報はグラフとテーブルとして利用できます。期間がカスタム終了日を指定した「先月」または「昨年」として選択されている場合、トレンド情報はグラフとして利用でき、テーブルとしては利用できません。
- Monitor Serviceのグルーミング保持値がトレンドデータの可用性を制御します。デフォルト値はデータ粒度と保持で確認できます。Premiumライセンスサイトのお客様は、グルーミング保持を希望する保持日数に変更できます。
- IIS Managerの以下のパラメーターは、選択可能なカスタム終了日の範囲を制御します。ただし、選択された日付のデータ可用性は、測定対象の特定のメトリックに対するグルーミング保持設定によって異なります。

パラメーター	デフォルト値
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

利用可能なトレンド

セッションの傾向を表示: 「**セッション**」タブから、デリバリーグループと期間を選択して、同時セッション数に関する詳細情報を表示します。

セッションの自動再接続列には、セッション内の自動再接続の数が表示されます。自動再接続は、セッションの信頼性ポリシーまたはクライアント自動再接続ポリシーが有効な場合に有効になります。エンドポイントでネットワークの中断が発生した場合、次のポリシーが適用されます。

- セッションの信頼性が有効になり（デフォルトで3分間）、Citrix Receiver™またはCitrix Workspace™アプリがVDAへの接続を試行します。
- クライアント自動再接続が3分から5分の間に有効になり、クライアントがVDAへの接続を試行します。

両方の再接続がキャプチャされ、ユーザーに表示されます。この情報は、再接続が発生してからDirector UIに表示されるまでに最大5分かかる場合があります。

自動再接続情報は、中断のあるネットワーク接続の表示とトラブルシューティングに役立ちます。また、シームレスなエクスペリエンスを持つネットワークも分析します。フィルターで選択した特定のデリバリーグループまたは期間の再接続数を表示できます。ドリルダウンでは、セッションの信頼性またはクライアント自動再接続、タイムスタンプ、エンドポイントIP、Workspaceアプリがインストールされているマシンのエンドポイント名などの追加情報が提供されます。

デフォルトでは、ログはイベントタイムスタンプの降順でソートされます。この機能は、Windows向けCitrix Workspaceアプリ、Mac向けCitrix Workspaceアプリ、Windows向けCitrix Receiver、およびMac向けCitrix Receiverで利用できます。この機能には、Delivery Controller™ バージョン7 1906以降、およびVDA 1906以降が必要です。

セッションの再接続の詳細については、「セッション」を参照してください。

ポリシーの詳細については、「クライアント自動再接続ポリシー設定」および「セッションの信頼性ポリシー設定」を参照してください。

自動再接続データがDirectorに表示されない場合があります。その理由は次のとおりです。

- WorkspaceアプリがVDAに自動再接続データを送信していません。
- VDAがモニターサービスにデータを送信していません。
- Delivery Controllerは、対応するセッションがない可能性があるため、VDAペイロードを破棄します。

> **注:**
>
> Citrix Gateway の特定のポリシーが設定されている場合、クライアント IP アドレスが正しく取得されないことがあります。

> **接続障害の傾向を表示:** タブから、接続、マシンタイプ、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のユーザー接続障害に関する詳細情報を含むグラフを表示します。

マシン障害の傾向を表示: タブまたは タブから、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のマシン障害に関する詳細情報を含むグラフを表示します。

ログオンパフォーマンスの傾向を表示: タブから、デリバリーグループと期間を選択して、サイト全体のユーザーログオン時間の期間と、ログオン数がパフォーマンスに影響するかどうかに関する詳細情報を含むグラフを表示します。このビューには、ブローカー処理時間や VM 起動時間など、ログオンフェーズの平均期間も表示されます。 このデータはユーザーログオン専用であり、切断されたセッションから再接続しようとしているユーザーは含まれません。 グラフの下の表には、ユーザーセッションごとのログオン期間が表示されます。表示する列を選択し、任意の列でレポートを並べ替えることができます。これらのレポートを .CSV ファイルにエクスポートすることもできます。詳細については、「ユーザーログオンの問題の診断」を参照してください。

負荷評価の傾向を表示: タブから、マルチセッション OS マシン間で分散される負荷に関する詳細情報を含むグラフを表示します。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のマルチセッション OS マシン、マルチセッション OS マシン (デリバリーグループ内のマルチセッション OS マシンが選択されている場合にのみ利用可能)、および範囲が含まれます。

ホスト型アプリケーションの使用状況を表示: この機能の可用性は、組織のライセンスによって異なります。 タブから、 タブを選択します。デリバリーグループと期間を選択して、ピーク時の同時使用状況を示すグラフと、アプリケーションベースの使用状況を示す表を表示します。 表から、特定のアプリケーションを選択して、詳細と、そのアプリケーションを使用している、または使用したユーザーのリストを表示できます。

シングルセッションおよびマルチセッション OS の使用状況を表示: ビューには、サイト別およびデリバリーグループ別のシングルセッション OS の使用状況が表示されます。 を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、ユーザーごとの使用状況が表示されます。 ビューには、サイト別、デリバリーグループ別、およびマシン別のマルチセッション OS の使用状況も表示されます。 を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、マシンごとおよびユーザーごとの使用状況が表示されます。マシンが選択されている場合、ユーザーごとの使用状況が表示されます。

仮想マシンの使用状況を表示: タブから、 を選択して、VM 使用状況のリアルタイムビューを取得し、サイトのキャパシティニーズを迅速に評価できるようにします。 シングルセッション OS の可用性 - サイト全体または特定のデリバリーグループの可用性別に、シングルセッション OS マシン (VDI) の現在の状態を表示します。 マルチセッション OS の可用性 - サイト全体または特定のデリバリーグループの可用性別に、マルチセッション OS マシンの現在の状態を表示します。

コスト最適化によるマシン使用状況の可視性を高めるには、表示されるバナーの以下のリンクをクリックします。

- 推定節約額 - このリンクをクリックすると、**コスト最適化**ページの**推定節約額**セクションに移動し、すべてのデリバリーグループの詳細が表示されます。

- 節約レポート - このリンクをクリックすると、**コスト最適化**ページの**節約レポート**セクションに移動し、すべてのデリバリーグループの詳細が表示されます。

注:

利用可能なカウンターに表示されるマシンの数には、メンテナンスモードのマシンが含まれます。

リソース使用率の表示: リソース使用率タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択すると、CPUとメモリの使用状況、および各VDIマシンのIOPSとディスク待機時間に関する過去の傾向データが得られ、キャパシティプランニングの改善に役立ちます。 この機能には、Delivery ControllerおよびVDA **バージョン 7.11** 以降が必要です。 グラフには、平均CPU、平均メモリ、平均IOPS、ディスク待機時間、およびピーク時の同時セッションのデータが表示されます。マシンにドリルダウンして、CPUを消費している上位10プロセスのデータとグラフを表示できます。

デリバリーグループと期間でフィルターします。CPU、メモリ使用量、およびピーク時の同時セッションのグラフは、過去 2 時間、24 時間、7 日間、月、年で利用できます。平均 IOPS とディスク待機時間のグラフは、過去 24 時間、月、年で利用できます。バナーの リンクをクリックすると、コスト最適化によるマシン使用状況の可視性が向上します。このリンクをクリックすると、 ページの タブに移動し、 タブから選択したデリバリーグループの詳細が表示されます。

注:

- 監視ポリシー設定の は、 ページの テーブルでデータを収集して表示するために に設定する必要があります。このポリシーは、デフォルトで に設定されています。すべてのリソース使用率データはデフォルトで収集されます。これは、 ポリシー設定を使用して無効にできます。グラフの下の表には、マシンごとのリソース使用率データが表示されます。詳しくは、「監視ポリシー設定」を参照してください。
- 平均 IOPS は日次平均を示します。ピーク IOPS は、選択した期間の IOPS 平均の最高値として計算されます（IOPS 平均とは、VDA でその時間に収集された IOPS の時間平均です）。
- マシンのドリルダウンでは、平均 CPU または平均メモリ使用量が 1% を超えるプロセスが一覧表示されます。これは、10 未満のプロセスが一覧表示される場合があることを意味します。

> **ネットワーク分析データの表示:** この機能の可用性は、組織のライセンスと管理者権限によって異なります。この機能には、Delivery Controller **バージョン 7.11** 以降が必要です。

タブから、ネットワーク分析を監視します。これにより、ネットワークのユーザー、アプリケーション、デスクトップのコンテキストビューが提供されます。この機能により、Director は Citrix ADM の HDX Insight レポートを通じて、展開における ICA トラフィックの詳細な分析を提供します。詳しくは、「ネットワーク分析の構成」を参照してください。

アプリケーション障害の表示: タブには、VDA 上で公開されているアプリケーションに関連する障害が表示されます。

この機能には、Delivery Controller および VDA **バージョン 7.15** 以降が必要です。Windows Vista 以降を実行するシングルセッション OS VDA と、Windows Server 2008 以降を実行するマルチセッション OS VDA がサポートされています。 詳しくは、「過去のアプリケーション障害監視」を参照してください。

デフォルトでは、マルチセッション OS VDA からのアプリケーション障害のみが表示されます。監視ポリシーを使用して、アプリケーション障害の監視を設定できます。詳しくは、「監視ポリシー設定」を参照してください。

プローブ結果の表示: タブには、構成ページでプローブ用に構成されたアプリケーションとデスクトップのプローブ結果が表示されます。ここでは、障害が発生した起動の段階が記録されます。

詳しくは、「アプリケーションおよびデスクトップのプローブ」を参照してください。

カスタマイズされたレポートの作成: タブは、監視データベースからのリアルタイムデータと履歴データを含むカスタムレポートを表形式で生成するためのユーザーインターフェイスを提供します。

この機能には、Delivery Controller **バージョン 7.12** 以降が必要です。

以前に保存したカスタムレポートクエリのリストから、**実行してダウンロード**をクリックしてレポートをCSV形式でエクスポートしたり、**ODataをコピー**をクリックして対応するODataクエリをコピーして共有したり、**編集**をクリックしてクエリを編集したりできます。 マシン、接続、セッション、またはアプリケーションインスタンスに基づいてカスタムレポートクエリを作成できます。マシン、デリバリーグループ、期間などのフィールドに基づいてフィルター条件を指定します。カスタムレポートに必要な追加の列を指定します。プレビューには、レポートデータのサンプルが表示されます。カスタムレポートクエリを保存すると、保存されたクエリのリストに追加されます。

コピーしたODataクエリに基づいてカスタムレポートクエリを作成できます。これを行うには、オプションを選択し、コピーしたODataクエリを貼り付けます。結果のクエリは、後で実行するために保存できます。

注:

ODataクエリを使用して生成されたプレビューおよびエクスポートレポートの列名はローカライズされず、英語で表示されます。

グラフ上のフラグアイコンは、特定の時間範囲における重要なイベントまたはアクションを示します。フラグにマウスを合わせ、クリックしてイベントまたはアクションを一覧表示します。

注:

- HDX™接続ログオンデータは、バージョン7より前のVDAでは収集されません。それより前のVDAの場合、チャートデータは0と表示されます。
- Citrix Studioで削除されたデリバリーグループは、関連データが削除されるまでDirectorトレンドフィルターで選択できます。削除されたデリバリーグループを選択すると、保持期間までの利用可能なデータのグラフが表示されます。ただし、テーブルにはデータが表示されません。
- アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、新しいデリバリーグループの**リソース使用率と負荷評価インデックス**テーブルに、古いデリバリーグループと新しいデリバリーグループから統合されたメトリックが表示されます。

統合とデータのエクスポート

Citrix Director に、統合とデータのエクスポート用の新しい UI が追加されました。この機能は、Citrix Director で利用可能なさまざまなインターフェイスとサードパーティ統合の認識を高めるのに役立ちます。新しく導入された**統合とデータのエクスポート**ページには、次のものが一覧表示されます。

- 利用可能な統合

- サポートされている開発者ツール

このページでは、データのエクスポート用の REST API の設定についても説明しています。また、統合と開発者ツールの使用を開始するためのガイドやドキュメントへの参照リンクも提供しています。

現在、Citrix DirectorはPower BIの可観測性と統合されています。この機能を使用して、REST API経由でCitrix DirectorからPower BIにパフォーマンスデータとイベントをエクスポートできます。

左側のナビゲーションメニューから をクリックします。 ページが表示されます。

統合とデータのエクスポート(/en-us/citrix-virtual-apps-desktops/2411/media/integrations-and-data-exports.png)

利用可能な統合を表示

統合タブには、Citrix Directorで利用可能な統合が表示されます。現在、Citrix DirectorはPower BIの可観測性と統合されています。

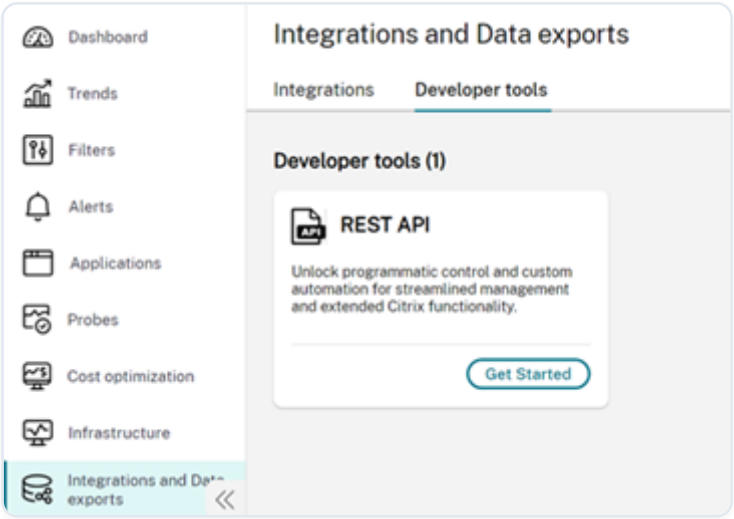
開始をクリックします。**REST API**開発者ツールの詳細ページが表示されます。

REST API (開発者ツール)(/en-us/citrix-virtual-apps-desktops/2411/media/rest-api-developer-tools.png)

このページには、リソースやブログへの参照リンクが記載されています。

サポートされている開発者ツールを表示する

1. **開発者ツール**をクリックして、利用可能な開発者ツールを表示します。



2. 「**開始**」をクリックします。**REST API** 開発者ツールの詳細ページが開きます。リソースやブログへの参照リンクにアクセスできます。

Ansible を使用した VDA のインストール

概要

この記事では、Ansible を使用して VDA を展開する方法について説明します。詳細については、Ansible ドキュメントを参照してください。

> **注:**
>
> この記事では、Citrix® が環境をテストした方法に基づいた推奨事項のみを説明します。これらの手順は、お客様のニーズに合わせてカスタマイズできます。Citrix は、お客様のニーズに合わせて必要な更新や調整について責任を負いません。

Ansible を使用して VDA を展開するための主要な手順

1. 仮想マシン環境の構成。
2. Ansible のインストール
3. Kerberos の構成
    a. Kerberos をインストールする
    b. Kerberos を構成する
4. Ansible を構成する

ステップ 1: 仮想マシン環境を構成する

Windows サーバーで次のコマンドを実行します。

1. PS RemoteSigned を設定します。 `Set-ExecutionPolicy RemoteSigned`
2. WinRM を暗号化なしで使用するように設定します。 `winrm set winrm/config/service '@{AllowUnencrypted="true"}'`

    > **注:**
    >
    > このステップでエラーが発生した場合は、次のコマンドを使用します: `Enable-PSRemoting -Force`

3. ファイアウォールポート5985を開きます。`New-NetFirewallRule -DisplayName "Allow WinRm port 5985" -Direction Inbound -Profile Any -Action Allow -LocalPort 5985 -Protocol tcp`

ステップ2：Ansibleのインストール

Ubuntu 20.4以降でAnsibleをインストールするには、次のコマンドを実行します。

- `sudo apt update`
- `sudo apt install software-properties-common`
- `sudo add-apt-repository --yes --update ppa:ansible/ansible`
- `sudo apt install ansible`
- `sudo apt install python3-pip`

ステップ2i：Kerberosのインストール

Kerberosをインストールするには、次のコマンドを実行します。

`sudo apt install python3-dev libkrb5-dev krb5-user`

ステップ2ii：Kerberosの構成

Kerberosを構成するには、次のコマンドを実行します。

`Edit /etc/krb5.conf`

```
[libdefaults]
        default_realm = [redacted]

# The following krb5.conf variables are only for MIT Kerberos.
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true

# The following encryption type specification will be used by MIT Kerberos
# if uncommented.  In general, the defaults in the MIT Kerberos code are
# correct and overriding these specifications only serves to disable new
# encryption types as they are added, creating interoperability problems.
#
# The only time when you might need to uncomment these lines and change
# the enctypes is if you have local software that will break on ticket
# caches containing ticket encryption types it doesn't know about (such as
# old versions of Sun Java).

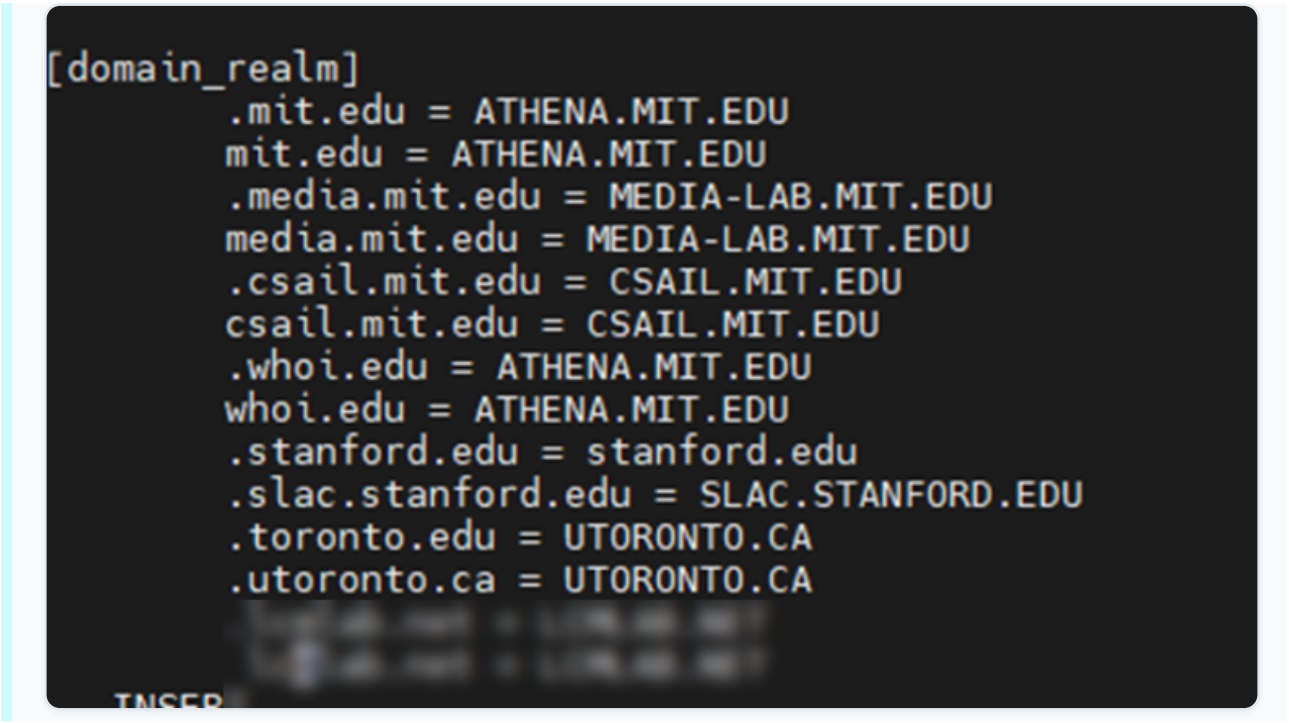
#       default_tgs_enctypes = des3-hmac-sha1
#       default_tkt_enctypes = des3-hmac-sha1
#       permitted_enctypes = des3-hmac-sha1

# The following libdefaults parameters are only for Heimdal Kerberos.
        fcc-mit-ticketflags = true

[realms]
        LTSRLAB.NET = {
                kdc = [redacted]
                admin_server = [redacted]
        }
        ATHENA.MIT.EDU = {
                kdc = [redacted]
```

注：

Kerberosレルム名には大文字を使用します。



ステップ 3：Ansible を構成する

Ansible ホストを構成するには、次の手順を実行します。

1. 次のコマンドを実行します。

   `Edit /etc/ansible/hosts`

2. Delivery Controller `Install.yaml` ファイルを構成します

   `/QUIET /NOREBOOT /NORESUME /OPTIMIZE /VERBOSELOG /COMPONENTS VDA /CONTROLLERS 'MyDDC.xd.local' /ENABLE_HDX_PORTS /ENABLE_REAL_TIME_TRANSPORT`

   「デリバリーコントローラー」(/en-us/citrix-virtual-apps-desktops/2411/media/delivery-controller-yaml-1.png)

   「デリバリーコントローラー」(/en-us/citrix-virtual-apps-desktops/2411/media/delivery-controller-yaml-2.png)

   「デリバリーコントローラー」(/en-us/citrix-virtual-apps-desktops/2411/media/delivery-controller-yaml-3.png)

   「デリバリーコントローラー」(/en-us/citrix-virtual-apps-desktops/2411/media/delivery-controller-yaml-4.png)

3. 以下のコマンドでyamlファイルを実行します。 `sudo ansible-playbook install.yml -vvv` (詳細モード)

4. 設定ファイルで、他の追加設定とともに複数のホストを構成できます。

`Edit /etc/ansible/hosts`

```
[WSVDA]

[TSVDA]

[WSVDA:vars]
ansible_port=
ansible_user =
ansible_password =
ansible_connection = winrm
ansible_winrm_transport = kerberos
ansible_winrm_server_cert_validation = ignore

[TSVDA:vars]
ansible_port=
ansible_user =
ansible_password =
ansible_connection = winrm
ansible_winrm_transport = kerberos
ansible_winrm_server_cert_validation = ignore
```

Call Home の主要データポイント

Call Home は、次の主要なデータポイントを収集します。

(M) = 手動収集時のみ取得されます (PowerShell コマンドレット `Start-CitrixCallHomeUpload`)

ファイル名	カテゴリ	データグループ
		マシン
		エックスディーサイト
		サイト情報
		Broker DB 情報 (M)
		インストールされている DB バージョン (M)
		Broker Service ステータス (M)

		登録済みサービスインスタンス (M)
		ブローカーライセンス テスト (M)
		アクティブな HDX™ セッション (M)
		ブローカー管理者
		ブローカー管理者権限
		RDS構成 (LicensingSettings、SessionSettings、SpecifiedLicenseServers、および RegisteredLicenseServersを含む)
		監視サービス (M) (MonitorConfiguration、MonitorDataStore、MonitorDBConnection、MonitorDBSchemaVersion、MonitorService、MonitorServiceAddedCapability、MonitorServiceInstance、MonitorServiceStatus、およびMonitorInstalledDBVersionを含む)
		構成ログ
		接続ログ
		ハイパーバイザー接続 (M)
		ブローカーハイパーバイザー接続
		ハイパーバイザーアラート

		カタログ
		マルチセッションOSエージェント (M)
		シングルセッションOSエージェント (M)
		公開アプリケーション
		デリバリー グループ
		構成済みデリバリーエージェント

		Citrixインストール済みコンポーネント
		シトリックス ブローカーサービス情報
		Broker Service構成ファイル
		Machine Creation Services™ 構成ファイル
		Host Service構成ファイル
		AD Identity Service構成ファイル
		Configuration Service構成ファイル
		Configuration Logging Service構成ファイル
		Delegated Administration Service構成ファイル
		環境テストサービス構成ファイル

		監視サービス構成ファイル
		Storefront™ サービス構成ファイル
		ワークステーションエージェント構成ファイル
		Citrix VDA情報
		Citrix XD ホットフィックス
		Citrix_VirtualChannel_Graphics_Enum
		Citrix_VirtualChannel_Flash_Enum
		Citrix_VirtualChannel_Printer_Enum

		コンピューター
		BIOS
		メモリ情報
		プロセッサ
		PNP デバイス
		デバイス
		ディスクドライブ
		論理ドライブ
		ページファイル使用状況
		ネットワークアダプター
		ネットワークアダプター構成

		ipConfig
		ビデオコントローラー
		IDE コントローラー
		SCSI コントローラー

		HKLM:\Software\Wow6432Node\Citrix
		HKLM:\System\CurrentControlSet\Control\Citrix
		HKLM:\SOFTWARE\Policies\Citrix
		HKLM:\Software\Microsoft\Cryptography
		HKLM:\Software\Wow6432Node\Microsoft\Cryptography
		HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Windows
		HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
		HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
		HKLM:\Software\Wow6432Node\Mic

		rosoft\Windows\CurrentVersion\Policies\Explorer
		HKLM:\SYSTEM\CurrentControlSet\Control\Print\Environments
		HKLM:\System\CurrentControlSet\Control\セッションマネージャー
		HKLM:\System\CurrentControlSet\Control\ターミナルサーバー
		HKCU:\Control Panel\Desktop
		HKLM:\SOFTWARE\Classes\ShockwaveFlash.ShockwaveFlash\CurVer
		HKLM:\SYSTEM\CurrentControlSet\Control\SystemInformation
		HKLM:\SYSTEM\CurrentControlSet\Control\FileSystem
		HKLM:\SYSTEM\CurrentControlSet\Control\Windows
		HKLM:\SYSTEM\CurrentControlSet\Control\TimeZoneInformation

		ドライバー
		EnvVariables

		OS
		プロセス
		サービス
		サービスパック
		ジーピーリザルト
		Microsoft ホットフィックス
		ネットスタット
		PNP ドライバー

		システムイベントログ
		AOT (常時オンのトレース)
		クラッシュダンプ

		アップタイム
		メモリ
		コンピューターシステム
		プロセッサ
		ビデオコントローラー
		ディスクドライブ
		ブラウザ情報
		再起動回数
		メモリ使用量
		ディスク使用量

		ICAセッション解像度
		ICA色深度
		メタインストーラーCEIPマシンID

		ストア数
		サーバーグループ内のサーバー数
		ストアあたりのDelivery Controller™数
		HTTPS有効
		Citrix Receiver™向けクラシックエクスペリエンスが有効
		Citrix Receiver 向け HTML5 Receiver 設定
		Citrix Receiver向けワークスペースコントロールが有効
		Store向けリモートアクセスが有効
		ゲートウェイ数
		統合されたNetScaler®認証用の明示的なJSONサービス

Teams およびその他のプラットフォーム向け最適化されたコンテンツ共有

この設定は、Citrix Virtual Channel SDK (VCSDK) を利用するMicrosoft Teams、Zoom、Webexなどの最適化されたビデオ会議およびコラボレーションプラットフォーム向けに、コンテンツ共有（アプリケーション共有およびデスクトップ共有）を構成するために設計されています。

この構成により、Citrix Virtual Desktop Infrastructure (VDA) 環境においてセキュリティ制御を維持しながら、シームレスなコンテンツ共有が保証されます。

機能

アプリケーション共有とデスクトップ共有: これらの機能により、Microsoft Teams、Zoom、Webexなどのユニファイドコミュニケーション (UC) アプリケーションのユーザーは、特定のアプリケーションコンテンツまたはデスクトップ全体を会議参加者と共有できます。

要件

- **アプリケーション共有:** Citrix Workspace™ App (Windows、Mac、Linux) でサポートされています。
- **VDA:** 最適な機能のためにVirtual Desktop Agent (VDA) が必要です。

構成

- この設定により、アプリ共有とデスクトップ共有の両方を無効にするオプションがあります。
- デフォルトでは、アプリ共有とデスクトップ共有の両方が有効になっています。
- この設定は、UCアプリケーション（例：Teams、Zoom、Webex）に特化して適用され、CitrixネイティブのHDX™画面共有には影響しません。
- この設定を構成すると、VDA UseWsProviderレジストリキーが上書きされます。

> **注:**
>
> - この設定は、個々のUCアプリケーション（例：Microsoft Teams）内のコンテンツ共有ポリシーとは独立して動作します。
> - この設定は、アプリ保護が有効な場合にのみ適用されます。アプリ保護が無効な場合、このポリシーは効果がありません。

セキュリティに関する考慮事項とバイパスメカニズム

App Protection が有効な場合、Microsoft Teams や Zoom などのアプリケーションは、クライアント側から VDA 画面をキャプチャしようとするため、画面を共有できません。これは制限されています。この問題に対処するため、Teams と Zoom が App Protection をバイパスし、クライアント側から画面共有を有効にできるようにするサポートが導入されました。

ただし、このバイパスを有効にすると、App Protection の制御を回避するため、潜在的なセキュリティリスクが生じます。これを軽減するため、App Protection が有効な場合に、管理者が UC アプリケーションの画面共有を無効にできるようにする新しいポリシーが導入されました。

ポリシーの詳細

- **App Protection が有効な場合:** App Protection が有効な場合、管理者は Zoom や Teams などの UC アプリケーションの画面共有を無効にすることを選択できます。
- **ユーザーエクスペリエンスへの影響:** 画面共有が無効になっている場合、App Protection がアクティブなときに、UC アプリでの会議中にユーザーはアプリケーションまたはデスクトップコンテンツを共有できません。

必要なアクション

- 管理者は、セキュリティ要件に基づいて設定を構成し、UC アプリケーションの画面共有が適切に有効または無効になっていることを確認する必要があります。
- このポリシーを構成する際は、App Protection が有効な環境にのみ影響することに留意してください。

プロファイルコンテナのポリシー設定

プロファイルコンテナ

ユーザープロファイルに関連付けられた大きなフォルダーは、ログオンの遅延を引き起こします。Citrix Profile Managementは、プロファイルディスク（VHDXファイル）に含めるフォルダーを指定できるVHDXベースのプロファイルソリューションを提供します。このソリューションは、指定されたフォルダーをネットワークに保存されているプロファイルディスクにマッピングすることで、ログオン時間を短縮します。プロファイルコンテナは、ログオン時にこれらのフォルダーを含むプロファイルディスクをアタッチするため、フォルダーのコピーをローカルプロファイルに保存する必要がなくなります。これにより、ログオン時間が短縮されます。

プロファイルコンテナのローカルキャッシュを有効にする

このポリシーは、Citrix Profile Managementプロファイルコンテナのローカルキャッシュサポートを有効にします。ポリシーが**有効**に設定されている場合、各ローカルプロファイルは、そのCitrix Profile Managementプロファイルコンテナのローカルキャッシュとして機能します。プロファイルストリーミングが使用されている場合、ローカルにキャッシュされたファイルはオンデマンドで作成されます。そうでない場合は、ユーザーログオン時に作成されます。ローカルキャッシュ機能

を使用するには、ユーザープロファイル全体をCitrix Profile Managementプロファイルコンテナに配置します。

プロファイルコンテナから除外するフォルダー

Citrix Profile Managementプロファイルコンテナから除外するフォルダーのリスト。

プロファイルコンテナに含めるフォルダー

親フォルダーが除外されている場合に、Citrix Profile Managementプロファイルコンテナに保持するフォルダーのリスト。

このリストのフォルダーは、除外されたフォルダーのサブフォルダーである必要があります。そうでない場合、この設定は機能しません。

プロファイルコンテナに含めるファイル

Citrix Profile Managementプロファイルコンテナに含めるファイルのリスト。

このリストのファイルは、除外されたフォルダー内にある必要があります。そうでない場合、この設定は機能しません。

プロファイルコンテナから除外するファイル

Citrix Profile Managementプロファイルコンテナから除外するファイルのリスト。

VHDディスク圧縮を有効にする

Profile Management の VHD ディスク圧縮を有効にします。有効にすると、特定の条件が満たされたときに、ユーザーのログオフ時に VHD ディスクが自動的に圧縮されます。このポリシーにより、プロファイルコンテナ、OneDriveコンテナ、およびミラーフォルダーコンテナが消費するストレージスペースを節約できます。

必要性および利用可能なリソースに応じて、詳細設定にある **VHDディスク圧縮をトリガーする空き領域の比率**、**VHDディスク圧縮をトリガーするログオフ回数**、および **VHDディスク圧縮のデフラグを無効にする** の各ポリシーを使用して、デフォルトのVHD圧縮設定と動作を調整できます。

プロファイルコンテナのVHD自動拡張を有効にする

プロファイルコンテナのVHD自動拡張を有効にするかどうかを指定します。有効にすると、すべてのVHD自動拡張設定がプロファイルコンテナに適用されます。

構成の優先順位：

- ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
- ここでも.iniファイルでもこのポリシーが構成されていない場合、無効になります。

VHDコンテナへの排他的アクセスを有効にする

デフォルトでは、VHDコンテナは同時アクセスを許可します。この設定を有効にすると、一度に1つのアクセスのみが許可されます。この機能は、プロファイルコンテナとOneDriveコンテナに適用されます。

> **注：**
>
> コンテナベースのプロファイルソリューションでプロファイルコンテナに対してこの設定を有効にすると、*プロファイルコンテナのマルチセッションライトバックを有効にする* 設定が自動的に無効になります。

構成の優先順位：

1. ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
2. ここでも.iniファイルでもこのポリシーが構成されていない場合、設定は無効になります。

ログオン時にプロファイルコンテナが利用できない場合にユーザーをログオフする

ユーザーログオン時にプロファイルコンテナが利用できない場合にユーザーを強制的にログオフさせ、(オプションで)ユーザーに表示されるエラーメッセージをカスタマイズできます。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
2. ここでも.iniファイルでもこのポリシーが構成されていない場合、設定は無効になります。

プロファイルコンテナにアクセスするユーザーとグループ

どのADドメインユーザーとグループがプロファイルコンテナに対する`Read & Execute`権限を持つかを指定できます。デフォルトでは、プロファイルコンテナはその所有者のみがアクセスできます。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.iniファイルの設定が使用されます。

2. ここでも.iniファイルでもこのポリシーが構成されていない場合、プロファイルコンテナはその所有者のみがアクセスできます。