シトリックス バーチャルアプリ アンド デスクトップ™ 7 2407

リリースについて

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

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

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

インストールとアップグレードの手順：

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

シトリックス バーチャルアプリ アンド デスクトップ 7 2407

Windows Server 2025 のサポート

Citrix Virtual Apps and DesktopsはWindows Server 2025をサポートするようになりました。Windows Server 2025の詳細については、Microsoftのドキュメント「Windows Server 2025の新機能」を参照してください。

セキュアなデフォルト設定

VDAインストーラーには、よりセキュアな初期設定のために、さまざまな機能のデフォルト設定を有効から無効に変更する新しいオプションが追加されました。詳しくは、「VDAのインストール」を参照してください。

使用状況テレメトリレポートの機能強化

使用状況テレメトリレポート機能が強化され、顧客管理環境に展開されているCitrix®製品、コンポーネント、機能のライセンスがどのように利用されているかに関するデータを収集および処理できるようになりました。この機能強化により、Citrixオンプレミス製品のライセンスコンプライアンスが確保されます。

この機能強化を活用するには、ライセンスサーバーを最新バージョンに更新してください。詳細については、以下を参照してください。

- Citrixライセンステレメトリ
- 必要なライセンスサーバーの更新
- CitrixライセンステレメトリFAQ

ライセンシングテレメトリデータ要素のリストについては、Citrixライセンシングテレメトリデータ要素を参照してください。

仮想ループバックポートの除外

仮想ループバックから特定のポートを除外するオプションが追加されました。これにより、アプリケーションが指定されたポートのループバックアドレスに対して行う呼び出しが、セッション固有のループバックアドレスに変更されなくなります。詳細については、仮想ループバックを参照してください。

シームレスアプリのLogonUIウィンドウのスケーリングの改善

認証パススルーが発生しないシナリオにおいて、**LogonUI**ウィンドウのスケーリングが改善されました。LogonUIウィンドウは、モニターの解像度とDPI設定に基づいてスケーリングされ、LogonUIウィンドウ全体がクリッピングなしで表示されるようになります。 詳細については、公開アプリケーションを開くときにWindows免責事項メッセージをフルサイズで表示するようにLogonUIを変更する方法を参照してください。

公開アプリケーションのサインアウトチェッカーの機能強化

この新機能により、システムに構成されているスタートアップアプリを自動的に検出し、システムプロセスリストに自動的に追加するオプションが追加されました。これにより、最後の公開ア

プリケーションウィンドウが閉じられたときに、これらのアプリケーションがサインアウトをブロックすることがなくなります。 詳細については、公開アプリケーションでのセッションサインアウトの問題のトラブルシューティングを参照してください。

DVCの仮想チャネル許可リスト

DVCの仮想チャネル許可リストを使用して、環境で許可されるカスタム動的仮想チャネルを制御できるようになりました。詳細については、「DVCの仮想チャネル許可リスト」を参照してください。

バーチャル デリバリー エージェント (VDAs) 2407

サードパーティ製VDA展開方法のドキュメント再構成

サードパーティ製VDA展開ページが、追加の詳細な手順を含むように再構成されました。詳細については、「サードパーティ製VDA展開」を参照してください。

MCSでプロビジョニングされていないVDAのトークンベースVDA登録（プレビュー）

この機能により、MCSでプロビジョニングされていないVDAの登録トークンを生成および管理できるようになりました。この実装により、MCSでVDAをプロビジョニングすることなく、WebSocket経由でVDA登録が可能になります。この機能は、Linux Virtual Delivery Agent、macOS用Citrix Virtual Delivery Agent、およびCitrix Virtual Apps and Desktopsを使用するドメイン非参加VDAもサポートします。詳細については、「トークンを使用してMCSでプロビジョニングされていないVDAを登録する」を参照してください。

ウェブスタジオ

依存ポリシーの明確化

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

複数選択ポリシー

複数のポリシーを選択し、以下の機能強化を確認できるようになりました。

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

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

コンテキストに応じたApp Protection

この機能により、管理者はApp Protectionの**画面キャプチャ防止**および**キーロギング防止**制御を、常に有効または常に無効にするのではなく、デバイスおよびユーザーのコンテキストに応じて適用できます。この実装により、必要な場合にのみApp Protectionの画面キャプチャ防止およびキーロギング防止を強制できます。詳細については、「App Protectionの管理」を参照してください。

スマートカード認証のサポート

Web Studioでスマートカード認証がサポートされるようになり、管理者はPIVカードおよびCACカードを使用してWeb Studioにアクセスできるようになりました。詳しくは、「Web Studioのスマートカード認証をセットアップする」および「スマートカード認証を有効にする」を参照してください。

テナント管理

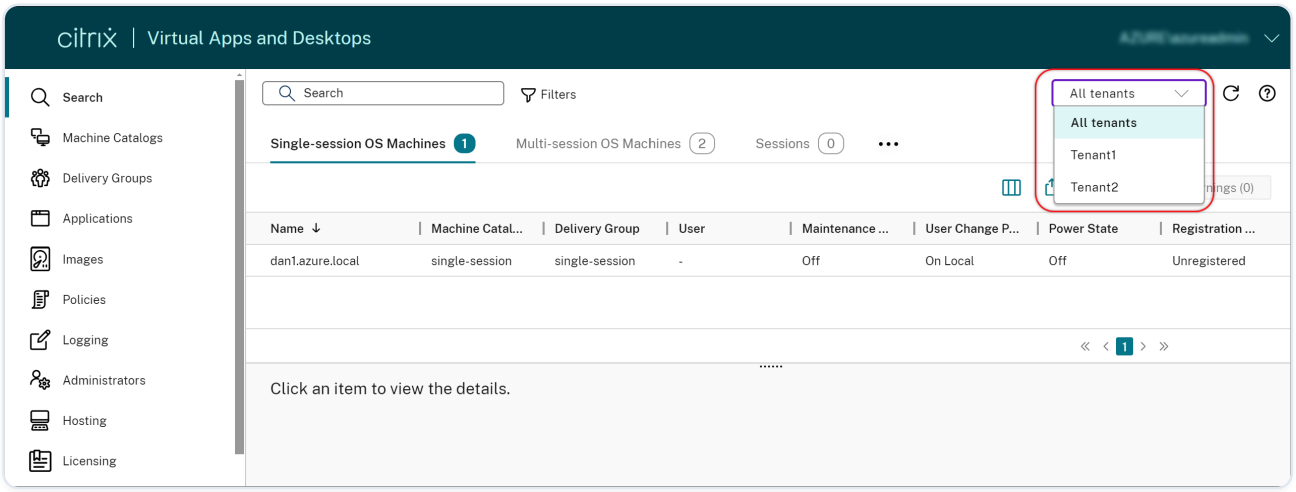
テナント管理を使用すると、単一のCitrix Virtual Apps and Desktopsサイト内に管理パーティションを設定できるようになりました。この機能は、独立した部門や個別のIT管理チームなど、異なる事業サイロで運用している組織に最適です。

テナント管理を設定するには、次の手順に従います。

1. テナントを作成します。 **［管理者］>［スコープ］** に移動し、テナントスコープを作成して、それらのスコープをマシンカタログやデリバリーグループなどの関連リソースおよび構成に関連付けます。

2. テナントの管理者を追加します。**管理者 > 管理者**に移動し、必要に応じてユーザーアカウントにロールとテナントを割り当てます。

テナントへの適切なアクセス権を持つ管理者は、Web Studioの右上隅にある**すべてのテナント**ドロップダウンリストでテナント名を表示および選択できます。その後、そのテナントにのみ関連付けられているリソースと構成を管理します。詳しくは、「テナント管理をセットアップする」を参照してください。



電源管理されたシングルセッションのプールされたVDAでローカルホストキャッシュ（LHC）を有効にする

デフォルトでは、MCSまたはCitrix Provisioningを使用してプロビジョニングされたシングルセッションのプールされたVDAは、LHCモードでは使用できません。Web Studioを使用すると、このデフォルトの動作をデリバリーグループごとに上書きし、LHC中にこれらのVDAを新しい接続で利用できるようにすることができます。詳しくは、「デリバリーグループを作成する」および「デリバリーグループを管理する」を参照してください。

VDA登録トークンの生成と管理

トークンベースのVDA登録により、Cloud Connectorの負荷が軽減され、潜在的な障害点が減少します。Web Studioを使用すると、MCSでプロビジョニングされていないVDAの登録トークンを生成および管理できるようになり、トークンベースの展開が効率化されます。詳しくは、「登録トークンを生成および管理する」を参照してください。

永続的なマルチセッションVMの作成

マルチセッションマシンのカタログを作成する際に、それらを永続的にするかどうかを指定できるようになりました。永続的なマルチセッションマシンについては、ユーザーがデスクトップに加えた変更は保存され、すべての承認済みユーザーがアクセスできることに注意してください。詳しくは、「マシンカタログを作成する」を参照してください。

Peak Autoscale™ 割り当て済み電源オン

永続デスクトップの電源がオンになっているものの使用されていない場合、またはユーザーがログオンしない場合、管理者はアクションなし、一時停止、シャットダウンなどのアクションを実行するまでの待機時間を定義できます。

- 割り当てられたマシンで、電源はオンになっているものの、ピーク時間の開始から設定された時間内にセッションが接続されていない場合、デリバリーグループレベルでポリシーを追加してマシンの電源を切ることができます。
- 割り当てられたマシンで、再開状態にあるものの、ピーク時間の開始から設定された時間内にセッションが接続されていない場合、デリバリーグループレベルでポリシーを追加してマシンを一時停止することができます。

この機能は、PTO中のエンドユーザーやログオンしていないエンドユーザーがいる場合、または会社が長期休暇の場合に役立ちます。待機時間とマシンの切断アクションを設定することで、Azureの消費コストを削減できます。詳細については、「シングルセッションOSランダムデリバリーグループ」および「シングルセッションOS静的デリバリーグループ」を参照してください。

パッケージ化されたアプリケーションをシングルセッション静的デスクトップおよびオフィスPCに配信する

この機能強化により、あらゆる種類のデスクトップにパッケージ化されたアプリケーションを配信できるようになりました。デスクトップにパッケージ化されたアプリケーションを配信するには、次の方法でそれらのアプリケーションをデリバリーグループに追加します。

- デリバリーグループの作成中にアプリケーションを追加します。
- 既存のデリバリーグループにアプリケーションを追加するには、次のいずれかのエントリを使用します: **Delivery Groups > Add Applications > Applications**、**Applications > Properties > Groups**、または **App Packages > Packages > Add Delivery Groups**。

詳細については、「デリバリーグループの作成」、「デリバリーグループの管理」、および「デリバリーグループへのアプリケーションの追加」を参照してください。

デスクトップの表示名を変更する

*シングルセッションOS静的*デリバリーグループ向けの**マシン割り当て**ページを強化し、新しい列「**表示名**」を導入しました。この追加により、ユーザーに割り当てられたマシンのデスクトップ表示名を変更できるようになりました。詳細については、「ユーザー割り当ての管理」を参照してください。

検索ノードのセッションタブからシングルセッションマシンを再起動およびシャットダウンする

検索ノードの**セッション**タブで、不健全な状態のユーザーセッションを検索し、同じタブ内で関連するシングルセッションマシンをシームレスに再起動またはシャットダウンできるようになりました。この機能により効率が向上し、単一のインターフェイス内で特定されたセッションの問題に迅速に対応できるようになります。

ライトバックキャッシュディスクにドライブ文字を割り当てる

以前は、PowerShellコマンドレットを使用してのみ、ライトバックキャッシュディスクに特定のドライブ文字を割り当てることができました。Web Studioを使用すると、同じタスクを実行できるようになりました。詳細については、「Microsoftカタログの作成」を参照してください。

失敗後にカタログの作成を再試行する

カタログの作成に失敗した場合、カタログの作成を再試行できるようになりました。作成を成功させるには、トラブルシューティング情報を確認し、問題を解決してください。この情報には、検出された問題が記述されており、それらを解決するための推奨事項が提供されています。失敗したカタログにはエラーアイコンが表示されます。詳細を表示するには、各カタログの**「トラブルシューティング」**タブに移動します。詳細については、「マシンカタログの管理」を参照してください。

構成ログにクライアントIPを表示

「ログ > イベント」で、ログ内のIPアドレスの詳細を表示できるようになり、アクションの発生源の追跡が容易になりました。メインビューにIPアドレス列を表示するには、ログの右上にある「表示する列」アイコンをクリックし、「クライアントIP」を選択します。

コンテキストヘルプの機能強化

Web Studio内の各ノードにターゲットを絞った情報を提供し、より有益なエクスペリエンスを提供するために、ヘルプパネルを再設計しました。任意のノードでヘルプアイコンをクリックすると、関連機能をよりよく理解するのに役立つ、ワンストップの学習エクスペリエンスを提供することを目的とした包括的なリソースセットにアクセスできるようになりました。

- 選択したノードに特に関連する主要ドキュメントにアクセスします。
- Citrixロードマップ、既知の問題、制限、システム要件、新機能などのサービス更新情報を入手できます。
- Citrixブログ、Citrixコミュニティ、Citrix機能解説、Citrix製品ドキュメント、Citrixサポート、開発者ドキュメントなどの拡張リソースにアクセスします。

検索機能の強化

検索ノードを強化し、以下の新機能を導入しました。

- 精度を高め、使いやすさを向上させるための2つの新しいフィルター、**「ゾーン」と「プロビジョニングの種類」**。
- 2つの新しい列:
  - **「セッション」**タブの「ユーザー表示名」**列。この列を使用すると、特定のユーザーに関連付けられているセッションをすばやく識別できます。
  - 「**デスクトップ表示名**」列が「**シングルセッションOSマシン**」タブと「セッション」タブの両方に表示されます。この列を使用すると、特定のデスクトップに関連付けられているマシンをすばやく特定できます。
- 効率的な検索のための新しいフィルター。これら2つの列の詳細については、「マシンアクションと列」および「セッションアクションと列」を参照してください。
- 「**検索**」および「**マシンカタログ**」ノードの検索パネルにフィルターピンが追加され、頻繁に使用する検索フィルターをページ上でアクセス可能な状態に保つことができます。

アプリケーションノードの機能強化

アプリケーションノードで以下の機能強化を実施しました。

- 表示する列とエクスポートの機能を、アプリケーションタブとアプリケーショングループタブの両方に拡張しました。右上隅に新しく導入されたアイコンを使用すると、アプリケーションとアプリケーショングループのメインビューをカスタマイズし、それらのビューからレコードをCSVファイルにエクスポートできるようになりました。
- アプリケーションの「詳細」ペインに「ゾーン」フィールドを追加し、アプリケーションが存在するゾーンを表示できるようにしました。この情報は、同じ名前を共有しながらも異なるゾーンから提供されるアプリケーションを区別する際に役立ちます。詳細については、「ゾーン」を参照してください。

マシンカタログとホスティングノードのデータキャッシュ

Citrix DaaS™の「**マシンカタログ**」ノードにデータキャッシュを導入しました。この機能強化により、「**マシンカタログ**」ノードに移動する際のページ読み込み時間が大幅に短縮され、全体的なユーザーエクスペリエンスが向上します。

より柔軟なリソースアクセス制御のためのアクセス ポリシー UI の再設計

デリバリーグループのリソースアクセス管理をより柔軟に行えるように、「**デリバリーグループの編集 > アクセスポリシー**」UIを再設計しました。新しい設計で利用できる主な機能は次のとおりです。

- **ポリシー追加のサポート。** ユーザー接続の属性に基づいてリソースアクセスを制限するアクセスポリシーを追加できるようになりました。ポリシーは2種類の基準で構成できます。
  - **包含基準。** デリバリーグループへのアクセスが許可されるユーザー接続を指定できます。
  - **除外基準。** デリバリーグループへのアクセスが禁止されるユーザー接続を指定できます。
- **拡張されたフィルターサポート。** さまざまなSmartAccessフィルターを使用して、包含基準と除外基準を定義できるようになりました。これらのフィルターには、`Citrix.Workspace.UsingDomain`や`Citrix-Via-Workspace`などのWorkspaceフィルター、およびネットワークロケーションベースの適応型アクセス用フィルターが含まれます。
- **含まれる基準に対する「すべて一致」ロジックのサポート。** この新しいロジックにより、デリバリーグループの許可されたユーザー接続を指定する際に、高レベルの精度と制御を実現できます。

詳細については、「」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/delivery-groups-manage.html#restrict-access-to-machines-in-a-delivery-group).

AWSカタログ作成のための高度なイメージフィルタリング

AWSカタログ作成時にマシンのテンプレートを選択する際、以下の検索条件を使用して、ターゲットテンプレートのAWS AMIインベントリをフィルタリングできるようになりました。

- イメージ名
- イメージID
- イメージタグ

マシンテンプレートリストは、リストをスクロールすると動的に読み込まれます。最初は25項目が読み込まれ、スクロールするにつれてさらに読み込まれます。

AWSで休止状態をサポートするVMを作成するためのサポート

AWS環境でVMの休止状態をサポートするマシンカタログを作成できるようになり、展開全体の費用対効果が向上します。関連するマシンプロファイルがこの機能をサポートしている場合、休止

状態に対応したVMを含めるようにカタログを編集することもできます。詳細については、「休止状態」を参照してください。

新しいポリシー検証

追加のポリシー検証が追加されました。その結果、無効なポリシー設定が存在する場合、ポリシーを有効にしたり、インプレースアップグレードを実行したりすると、ポリシーデータが失われる可能性があります。Web Studio以外の方法でポリシーを作成または編集する場合は、最新バージョンのSDKとスナップインを使用することをお勧めします。詳細については、「CTX676686」を参照してください。

ポリシーセット

Web Studio > ポリシーで、ポリシーセットを使用してポリシーをグループ化し、ロールベースのアクセスを簡素化できるようになりました。その後、ポリシーセットにスコープとデリバリーグループを割り当てることで、承認された管理者のみが関連するユーザーとマシンに適用されるポリシーを管理できるようになります。詳細については、「ポリシーセット」を参照してください。

複数選択ポリシー

複数のポリシーを選択し、以下の機能強化をチェックアウトできるようになりました。

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

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

依存ポリシーの明確化

一部の設定は他の設定に依存しています。以前は、ポリシー設定は相互に依存していましたが、設定間の関係が不明確でした。たとえば、子設定が構成されていても、親設定が有効になっていない

場合、構成された子設定は有効になりません。以前は依存関係が明確ではありませんでした。このリリースから、子ポリシーを構成する前に最初に構成する必要がある親ポリシーが明確に示されるようになりました。詳細については、「ポリシー設定」を参照してください。

マシンカタログのサブネット更新を簡素化

以前は、マシンカタログのサブネット設定を変更するには、それを削除して再作成する必要がありました。この機能により、カタログを編集することで同じ機能を実現できるようになりました。カタログの下に作成された新しい仮想マシンのみが、新しく関連付けられたサブネット上に配置されることに注意してください。この機能強化により、カタログの削除と関連タスクの必要性が軽減されます。詳細については、「カタログの編集」を参照してください。

新しいポリシー設定 - セッションメトリック収集

この設定により、Citrix は VDA と Workspace 間のユーザーおよびマシンセッションメトリックを収集し、ユーザーエクスペリエンスを向上させることができます。

Citrix は、オペレーティングシステム、稼働時間、コンピューターシステム情報、ビデオコントローラーの詳細、VDA バージョン、展開タイプ、ドメイン参加ステータスなどのデータを収集します。さらに、製品改善の取り組みを支援するために、いくつかのセッション構成、パフォーマンスおよび信頼性データが収集されます。デフォルトでは、この設定は有効になっています。詳細については、「セッションメトリック収集」を参照してください。

セキュア プライベート アクセスとウェブスタジオの統合

2407 以降、Secure Private Access と Web Studio の統合が強化され、管理者は Web Studio コンソール内で SPA コンソールにアクセスできるようになりました。詳細については、「Secure Private Access と Web Studio の統合」を参照してください。

Citrix Studio

Citrix Studioはメンテナンスモードになりました

本リリースより、Citrix Studioはメンテナンスモードに移行します。今後、新機能の追加は行わず、定期的なバグ修正とセキュリティパッチを通じて、その安定性とセキュリティに注力します。Citrix Studioの次世代版であるWeb Studioへの移行を推奨します。Web Studioは、Citrix Studioと完全に同等の機能を備えたWebベースの管理コンソールであり、最新の管理エクスペリエンス、強化された機能、および強力な新機能を提供します。詳しくは、「Web Studioのインストール」を参照してください。

Citrix Director

ダッシュボードのアプリケーション使用状況監視グラフ

Citrix Directorで、公開アプリケーションの使用状況を監視できるようになりました。この機能はダッシュボードにあり、IT管理者またはアプリケーション管理者が、どのアプリケーションが頻繁に使用されているか、およびその使用状況の程度を把握するのに役立つ厳選されたグラフが含まれています。

これらのグラフは、過去24時間の以下のデータポイントで構成されています。

- 使用中のアプリケーションの総数
- 総ユニークユーザー数による最も使用されているアプリケーション（上位10件）
- アプリケーション起動総数による最も使用されているアプリケーション（上位10件）
- 同時実行アプリケーションインスタンスのピーク上位

この視覚化により、顧客は人気のある公開アプリケーションを可視化し、ソフトウェアライセンスの購入にかかるコストを最適化するために、消費量とエンタイトルメントの分析を実行できます。

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

> アプリケーション監視(/en-us/citrix-virtual-apps-desktops/2407/media/application-monitoring.png)

詳しくは、「ダッシュボードのアプリケーション使用状況監視グラフ」を参照してください。

クラウドおよびオンプレミスユーザー向けの統合検索

以前は、Director でユーザーを検索するトリアージ中に、ユーザーがオンプレミスサイトのユーザーである場合にのみユーザーの詳細が表示されていました。ユーザーがクラウドサイトのユーザーである場合は、Monitor に移動して再度検索する必要がありました。この強化された検索機能により、Director の オプションを使用して、クラウドサイトまたはオンプレミスサイトのユーザーを検索できます。この機能により、問題解決までの平均時間が短縮され、データベースサイズの急激な増加なしに、単一のコンソールでシームレスなエクスペリエンスが提供されます。

統合検索サイト(/en-us/citrix-virtual-apps-desktops/2407/media/unified-search-site.png)

統合検索 - 完了(/en-us/citrix-virtual-apps-desktops/2407/media/unified-search-done.png)

詳しくは、「クラウドおよびオンプレミスユーザー向け統合検索」を参照してください。

セッションログオンビューの改善

-> ページの タブにある、以下のサブセクションを含む新しい オプションは、仮想マシンを異なるフェーズで起動するのにかかった時間の内訳を提供します。

- **電源オン** - 仮想マシンの電源をオンにするのにかかった時間を表示します
- **起動と登録** - 仮想マシンを起動して登録するのにかかった時間を表示します

ページに新しく導入された折りたたみボタンを使用すると、 と のオプションを折りたたんだり展開したりできます。

デフォルトの テーブルオプションである と に加えて、 ページで以下の列を選択することもできます。

- 開始時刻
- 終了時刻
- デリバリーグループの7日間平均 (秒)
- ユーザーの7日間平均 (秒)

上記のデータを.CSVファイルにエクスポートすることもできます。

新しく追加された列 **Power on** および **Boot up and registration** は、**トレンド** -> **ログオンパフォーマンス** > **列の選択** の **ユーザーセッションごとのログオン期間** テーブルに追加できます。**ログオンパフォーマンス** 画面でレポートをエクスポートすることもできます。

この機能強化により、ログオン期間に関連する問題を理解し、簡単にトラブルシューティングできるようになります。詳細については、「ユーザーログオンの問題の診断」を参照してください。

ICA® RTTまたはセッションログオン期間のデータが入力されない場合のトラブルシューティングオプション

以前は、EUEMサービスまたはプロファイル管理サービスが実行に失敗した場合、ICA RTTまたはセッションログオン期間に関連するデータ取得の失敗理由が表示されませんでした。この新機能により、失敗の理由とそれに対応する解決策を確認できます。

詳細については、「ICA RTTまたはセッションログオン期間のデータが入力されない場合のトラブルシューティングオプション」を参照してください。

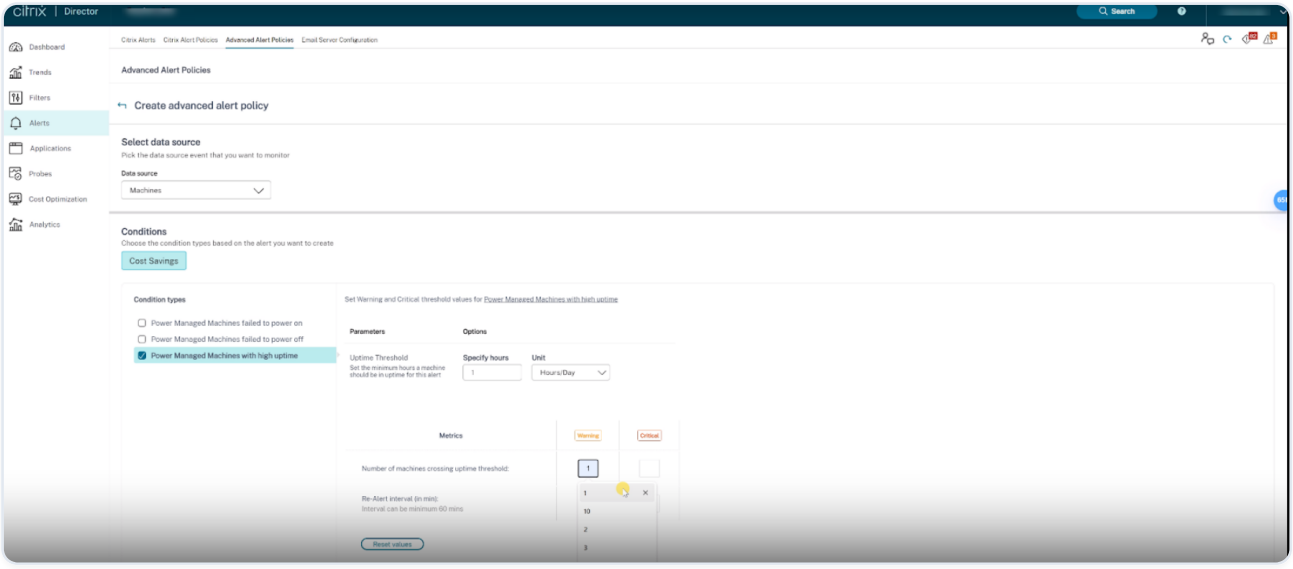
公開デスクトップ名

Citrix DirectorのUIに公開デスクトップ名が表示されるようになりました。この新しいフィールドを使用すると、同じデリバリーグループ内のユーザーグループを区別できます。これらのユーザーグループのカスタムレポートを生成することもできます。この新しいフィールドは、Citrix Director UIの**フィルター**、**カスタムレポート**、または**マシン詳細**セクションに追加されます。

高度なアラートポリシー

Directorのプロアクティブ通知およびアラート機能が強化され、**高度なアラートポリシー**という新しいアラートフレームワークが追加されました。この機能を使用すると、各要素または条件にきめ細かな詳細を含めてアラートを作成できるため、アラートの範囲をより詳細に制御できます。現在、これらのポリシーには、コスト削減とインフラストラクチャに関するアラートが含まれています。

この機能は、過剰なアラートを減らすのに役立ちます。過剰なアラートは、重要な問題への対応の遅延や効果の低下につながる可能性があります。このポリシーは、アラートポリシーの有効性と管理者からのエンゲージメントを測定するのに役立ちます。



詳細については、「高度なアラートポリシー」を参照してください。

アラートコンテンツの機能強化

Directorのアラート機能が強化され、CSV添付ファイルとJSONペイロードが含まれるようになりました。この機能強化により、メールでCSV添付ファイルとして、またはWebhookの場合はJSONペイロードとしてアラートの詳細を取得できます。このCSV添付ファイルとJSONペイロードを使用すると、詳細レベルで豊富なコンテンツを受信でき、問題の迅速な特定と解決に役立ちます。

現在、この機能強化は次のアラートでのみ利用可能です。

- マシンの稼働時間
- 電源オンアクションの失敗
- 電源オフアクションの失敗
- 未登録マシン (%)

詳細については、「アラートコンテンツの機能強化」を参照してください。

セッションタイプと最終起動時間を表示およびフィルターするオプション

Citrix Directorで、**セッションの種類**を新しい列として追加するオプションが提供されるようになりました。利用可能なセッションの種類は、デスクトップとアプリケーションです。**フィルター** > **セッション** > **列の選択**で追加することで、**セッションの種類**を新しい列として追加することもできます。これは、**トレンド > セッション**にも追加されています。

同様に、**フィルター** > **マシン**セクションに、**最終起動時間**を検索する新しいオプションが追加されました。**フィルター** > **マシン** > **列の選択**で追加することで、**最終起動時間**を新しい列として追加することもできます。

セッションとアプリケーションインスタンスで期間別にデータをフィルターするオプション

Citrix Directorで、**フィルター**タブの**セッション**と**アプリケーションインスタンス**に期間フィルターが追加されました。セッションとアプリケーションインスタンスを次の期間でフィルターできるようになりました。

- 過去60分
- 過去24時間
- 過去7日間

また、**フィルター**タブの**セッション**、**接続**、**アプリケーションインスタンス**にカスタム期間オプションが追加されました。

詳細については、「障害トラブルシューティングのためのデータのフィルタリング」(/ja-jp/citrix-virtual-apps-desktops/2407/director/site-analytics/filters-data)を参照してください。

強化されたパフォーマンスメトリックパネル

パフォーマンスメトリックパネルには、履歴データメトリックの視覚化が強化されています。**セッションパフォーマンス**タブをクリックすると、過去15分間のデータに加えて、ICARTTとICA

Latencyの過去24時間分のデータを表示できます。この機能強化により、セッションが過去24時間以内に終了した場合でも管理者が問題をトリアージできるようになり、解決までの平均時間を短縮できます。

詳細については、「パフォーマンスメトリック」(/ja-jp/citrix-virtual-apps-desktops/2407/director/troubleshoot-deployments/user-issues/session-performance#performance-metrics)を参照してください。

セッションパフォーマンスタブの機能強化

セッションパフォーマンスタブの**セッショントポロジ**セクションは、以下を含むように強化されました。

- セッショントポロジビューにおけるコネクタとCitrix Gatewayに関する追加の詳細（エンドポイントIP、エンドポイントOS、エンドポイントホップにおけるCitrix Workspace™アプリのバージョンなど）
- ゲートウェイサービスのPop ID、場所と国、コネクタIP、コネクタ名、リソースの場所
- コネクタとCitrix Gatewayの欠落しているデータ要素に関する詳細と、最新バージョンをダウンロードするためのリンク
- ハイパーバイザーの種類、ホスト接続名、ホスト名などのハイパーバイザーの詳細
- セッション詳細セクションおよびセッショントポロジビューにおけるHDXプロトコルの名前
- Windows版Citrix Workspaceアプリに存在する以下のエンドポイントメトリック：
    - Wi-Fi信号強度
    - スループット（受信および送信）
    - ネットワークインターフェイスタイプ
    - リンク速度

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

ユーザープロファイル読み込みの問題のトリアージに関する機能強化

Citrix Directorは、Citrix Profile ManagementコンテナおよびFSLogixコンテナからのプロファイル読み込み期間とコンテナメトリックの収集をサポートするようになりました。この機能強化により、管理者はユーザーセッションレポートで包括的なプロファイル使用状況とパフォーマンスデータを受け取ることができます。このデータを使用すると、問題をより効率的に特定し、解決できます。

詳細については、「プロファイル読み込み」を参照してください。

コスト最適化

Citrix Directorに、仮想マシンとセッションの使用状況を効果的に分析するのに役立つ「コスト最適化」という新機能が導入されました。この機能は、コストを最適化する方法に関する洞察に満ちた視覚的な表現を提供します。また、不要なマシンを排除し、それによってコストを削減するのにも役立ちます。

コスト最適化ページには、次の機能が含まれています。

- コスト削減
- インフラストラクチャの適正化

コスト削減

コスト削減ページでは、選択した期間に発生したインフラストラクチャの節約額を視覚的に表示し、残りの日数で予想される節約額を予測します。このページでは、マシンの使用状況とセッションを分析することで、達成された節約額とコスト削減の機会を特定するのに役立ちます。このページでは、次の情報を提供します。

- インフラストラクチャコストの最適化に関する洞察
- 節約された金額
- 予測コストを超える可能性のあるさまざまなシナリオに関する情報
- インフラストラクチャコスト削減を実現するための特定と戦略的計画の潜在的な機会

コスト最適化 > **コスト削減**ページには、**推定節約額**と**オートスケール節約レポート**が含まれています。

推定節約額は、インフラストラクチャリソースの効率的な利用を評価するのに役立ちます。推定節約額は、インフラストラクチャリソースの効率的な利用を評価するのに役立ちます。コスト削減額は、ハイパーバイザーの通貨または発生したコストの割合として表示されます。以下の期間の結果を表示できます。

- 7日間
- 30日間
- 3か月
- 6か月
- 12か月

「**推定節約額**」グラフには、以下が表示されます。

- 推定節約額 - 選択した期間にインフラストラクチャで達成された節約額を表示します
- 電源管理されたマシン - 電源管理されたマシンの総数を表示します。
- 予測節約額 - 残りの期間でどれだけのインフラストラクチャの節約が可能かを表示します

オートスケール節約額レポートには、オートスケールが構成および有効化されているデリバリーグループに関する情報が表示されます。このレポートは、電源管理されたマシンにのみ適用されます。

詳細については、「コスト削減」を参照してください。

インフラストラクチャの適正化

「**インフラストラクチャの適正化**」ページでは、リソース使用率に基づいて、デリバリーグループのプロビジョニングとサイジングの側面を分析できます。この分析に基づいて、使用パターンに合わせてマシンのプロビジョニングとサイジングを最適化できます。未使用のリソースへの支出を削減することで、インフラストラクチャコストを最適化できます。リソース使用率がプロビジョニングされたよりも一貫して低い場合は、より低いCPUおよびメモリ仕様のマシンを選択することもできます。リソース使用率が一貫して高く、*ログオンとICARTT*メトリックなどのセッションエクスペリエンスに影響を与えている証拠がある場合は、より高いCPUおよびメモリ仕様のマシンを選択することでパフォーマンスを最適化できます。

インフラストラクチャの適正化は、以下を使用してフィルタリングできます。

- デリバリーグループ - シングルセッションOSまたはマルチセッションOSデリバリーグループでフィルタリングできます
- タグ - タグはマシンに適用されるタグ名です。そのため、同じタグを持つマシンをフィルタリングできます。最大5つのタグを複数選択できます。複数のタグを選択すると、選択されたマシンタグのいずれか1つ以上が適用されているすべてのマシンをフィルタリングできます。
- 期間 - 過去24時間、7日間、30日間のデータをフィルタリングできます。

インフラストラクチャの適正化ページでは、以下を提供します。

- 使用状況の詳細に関する洞察
- リソース使用率の概要
- リソース使用率の傾向

ホーム画面の左側のメニューから**コスト最適化**タブをクリックします。次に、**インフラストラクチャの適正化**タブをクリックして、**インフラストラクチャの適正化**ページにアクセスします。

コスト最適化タブ > **コスト削減**の**インフラストラクチャの詳細**セクションにある**このデリバリーグループを適正化する**リンクをクリックして、**インフラストラクチャの適正化**ページにアクセスすることもできます。

詳細については、「インフラストラクチャの適正化」を参照してください。

最近の電源操作があるマシンを検査する

成功および失敗した電源操作のステータスを持つマシンを検査できるようになりました。この機能は、以下の分析に役立ちます。

- ユーザーの問題を引き起こす電源オンの失敗
- コストを増加させる電源オフの失敗

> **注：**
>
> データは電源管理されたマシンでのみ利用可能です。この機能がサポートされる前に行われた電源操作のデータは利用できません。

> 以下の方法で、マシンの電源操作ステータスを表示できます。

- **フィルター** -> **マシン**タブから。この場合、デフォルトで**電源操作時間**と**電源操作結果**の列が表示されます。表示したい列を選択することもできます。
- **コスト最適化**タブから。この場合、デフォルトのフィルターは**電源操作トリガー元**が**Autoscale**に設定され、**電源操作結果**が**失敗**に設定されています。

この機能により、電源操作制御の詳細を表示できます。たとえば、誰が操作をトリガーしたか、どの操作が電源状態を変更したか、失敗の理由、操作が完了した時刻などを表示できます。これらの詳細をエクスポートすることもできます。

詳細については、「最近の電源操作があるマシンを検査する」を参照してください。

電源オンアクション失敗および電源オフアクション失敗アラート

Directorのプロアクティブ通知およびアラート機能が強化され、デリバリーグループ内で電源管理されたマシンの電源オンまたはオフに失敗した数に基づいて、**電源オン操作の失敗**と**電源オフ操作の失敗**という2つの新しいアラートが追加されました。新しいアラート条件により、デリバリーグループ内で電源オンまたはオフに失敗した電源管理マシンの数をアラートしきい値として構成できます。

詳細については、「電源オン操作の失敗と電源オフ操作の失敗」を参照してください。

マシン稼働時間アラート

Directorのプロアクティブ通知およびアラート機能が強化され、デリバリーグループ内の電源管理されたマシンの稼働時間に基づいて、新しいアラート「マシン稼働時間アラート」が追加されました。しきい値を超えたマシンがあるデリバリーグループごとに、そのデリバリーグループのみの添付ファイルまたはWebhookアラートが届きます。

新しいアラート条件により、デリバリーグループ内でマシンがオンになっている時間数を、1日あたりの時間数、1週間あたりの時間数、または1か月あたりの時間数としてアラートしきい値を構成できます。

詳細については、「マシン稼働時間アラート」を参照してください。

未登録マシンアラート

Directorのプロアクティブ通知およびアラート機能が強化され、デリバリーグループ内の未登録マシンの割合に基づいて、新しいアラート「**未登録 マシン （%）**」が追加されました。この新しいアラート条件により、デリバリーグループ内の未登録マシンの割合として、警告およびクリティカルなしきい値を構成できます。

詳しくは、「未登録マシン」を参照してください。

統合とデータのエクスポート

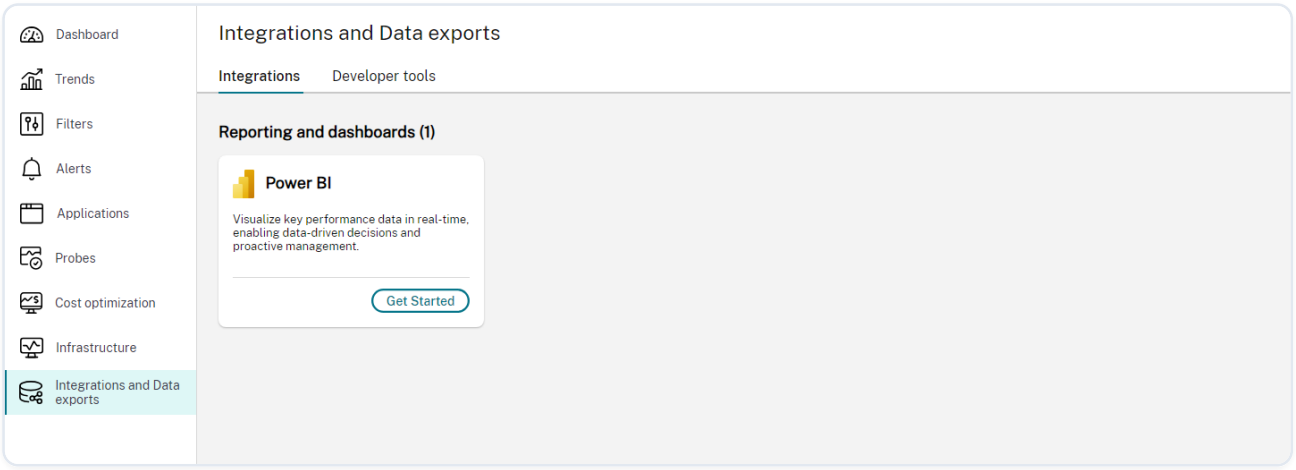
Citrix Director に、統合とデータエクスポートのための新しい UI が追加されました。この機能は、Citrix Director で利用可能なさまざまなインターフェイスとサードパーティ統合の認識を向上させるのに役立ちます。新しく導入された ページには、次のものが表示されます。

- 利用可能な統合
- サポートされている開発者ツール

このページでは、データエクスポートのためのREST APIの設定についても説明し、統合と開発者ツールの使用を開始するためのガイドとドキュメントへの参照リンクを提供します。

現在、Citrix DirectorはPower BIの可観測性と統合されています。この機能を使用すると、REST APIを使用してCitrix DirectorからPower BIにパフォーマンスデータとイベントをエクスポートできます。

左側のナビゲーションメニューから **［統合とデータエクスポート］** をクリックします。 **［統合とデータエクスポート］** ページが表示されます。



詳しくは、「統合とデータエクスポート」を参照してください。

過去のユーザーセッションの診断

Citrix Directorで、アクティブ、切断、または終了状態のセッションの詳細が表示されるようになりました。以前は、アクティブなセッションの詳細のみを表示できました。この機能により、ヘルプデスク管理者は、終了したセッションまたは終了状態のセッションに関する問題をトラブルシューティングできます。セッションの詳細は、過去24時間および過去2日間利用できます。終了したセッションまたは終了状態のセッションについて、次の詳細を表示できます。

- マシン詳細パネル - 選択したセッションが起動されたマシンの利用可能な詳細を表示します。
- セッション詳細パネル - 選択したセッションの利用可能な詳細を表示します。
- セッションログオン期間 - 選択したセッションにかかったログオン期間に関する情報を表示します。ブローカー処理、マシンの起動、HDX接続、認証、GPO、ログオンスクリプト、ディスクへのプロファイル読み込み、および対話型セッションにかかった時間に関するグラフを表示できます。

詳細については、履歴ユーザーセッションの診断を参照してください。

Secure Private Accessセッション用アクティビティマネージャー

Citrix Directorは、Secure Private Accessセッションのアクティビティマネージャービューを提供し、セッションアクティビティの全体像を把握できます。アクティビティマネージャーは、正常に開かれたすべてのアプリとデスクトップ、開くのに失敗したアプリとデスクトップ、およびSecure Private Accessアプリで設定されたポリシーの結果を包括的に表示します。

アクティビティマネージャーには、**利用可能なアプリ**および**起動されたアプリ**の詳細が表示されます。以下のセッション詳細を確認できます。

- 起動時間
- リソース名

- リソースの種類
- アクセスされたリソース
- ステータス
- トランザクションID

また、許可、拒否、エラーなどのアプリケーションステータスで上記の詳細をフィルターすることもできます。上下の矢印で詳細を並べ替えることもできます。

アクティビティマネージャー(/en-us/citrix-virtual-apps-desktops/2407/media/spa-activity-manager.png)

詳細については、Secure Private Accessセッションのアクティビティマネージャーを表示を参照してください。

Secure Private Access アプリのセッショントポロジビュー

Secure Private Access を使用して開かれたアプリのセッショントポロジを表示できます。アクティビティマネージャーから目的のアプリをクリックすると、選択したアプリのセッショントポロジが表示されます。

アクティビティマネージャー(/en-us/citrix-virtual-apps-desktops/2407/media/spa-session-topology.png)

セッショントポロジビューから、Secure Private Access を使用して開かれたアプリ、ポリシー評価のステータス、およびアプリ起動のステータスを表示できます。また、アプリ、ポリシー評価、およびセッションの詳細も確認できます。

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

インフラストラクチャ監視

Citrix Director は、Citrix Virtual Apps and Desktops コンポーネントの運用健全性に関する可視性を提供するようになりました。この機能は、インフラストラクチャに関連する問題を簡単に特定、トラブルシューティング、解決するのに役立ちます。現在、Citrix Provisioning™ (PVS) および StoreFront コンポーネントの健全性が監視されています。

この機能をサポートするために、Citrix Infrastructure Monitor という新しい Windows 実行可能ファイルが導入されました。これは、PVS または StoreFront™ サーバーから Director への関連する健全性メトリックの収集と送信に役立ちます。

この機能は、Director の単一コンソールで、PVS および StoreFront サーバーのシステムメトリックに関する重要な監視データセットとプロアクティブなアラートを取得するのに役立ちます。最新の情報を確保するために、監視コンポーネントから5分ごとにデータが収集されます。

この機能は、プロアクティブな監視、詳細なメトリック、および自動アラートを提供することで、運用効率を向上させ、Citrix インフラストラクチャがスムーズかつ効率的に稼働することを保証することを目的としています。

主な機能

リアルタイム監視:

- Citrix Provisioning (PVS) サーバーや StoreFront などの Citrix インフラストラクチャコンポーネントの継続的な監視。
- システム健全性、リソース使用率、および関連するパフォーマンスメトリックを表示するダッシュボードビュー。

詳細な分析:

- 各コンポーネントの接続ステータス、サービスまたはプロセスステータスなどのシステムヘルス指標に関する詳細な分析を提供します。
- CPU、メモリ、ディスク使用率などのリソース使用率メトリックに関する詳細。

自動アラートと通知:

- きめ細かなスコープを持つさまざまなメトリックと状態に対応するカスタマイズ可能なアラートしきい値。
- メールとWebhookによるリアルタイム通知。

ユースケース

運用効率:

Citrix管理チームがCitrixサーバーとサービスの高可用性とパフォーマンスを維持できるようにします。この機能は、問題が重要なユーザーグループに影響を与える前に、問題を事前に特定して管理者に警告することで、ダウンタイムを最小限に抑えるのにも役立ちます。

チケット解決の高速化:

サーバーの健全性とパフォーマンスに関する主要なメトリックを監視し、仮想アプリケーションとデスクトップのユーザーへの最適な配信を評価します。これらのメトリックを使用して、関連す

るコンポーネントを分析することで、パフォーマンスに関連するユーザーの苦情を診断し、解決します。

詳細については、インフラストラクチャ監視 [プレビュー]セクションを参照してください。

インフラストラクチャ ポリシー

このポリシーは、サポートされているCitrix Virtual Apps and Desktopsコンポーネントの健全性に関連するアラートを作成するために導入されました。

インフラストラクチャ監視のセットアップが完了すると、Directorで利用可能な健全性データを使用して、必要なコンポーネントのアラートを設定できます。管理者は、条件、スコープ、通知媒体を設定して、メールまたはWebhookを介したJSONペイロードで重要なアラートを受信できます。発生したアラートは、分析と管理のために**Citrix Alerts**セクションでも利用できます。

このポリシーの一環として、次の4つの新しいカテゴリが導入されました。

- 到達可能性
- 依存サービス
- 影響
- リソース使用率

重大および**警告**セクションで、必要に応じて異なる条件を設定し、前述のカテゴリの重大度を変更できます。これらのアラートの再アラート間隔をスケジュールすることもできます。

各カテゴリ内の条件は、組織の優先順位に基づいて、重大度を重大および警告に設定できます。これらのアラートの再アラート間隔をスケジュールすることもできます。

詳細については、「インフラストラクチャポリシー (プレビュー)」セクションを参照してください。

シトリックス スカウト

トレースと再現手順の機能強化

以前は、トレースと再現手順で、UI を使用して保存された CDF トレースをインポートできました。

2407 リリース以降、この UI オプションは削除されました。追加のログ収集を有効にすると、Scout はマシンにインストールされている CDC 関連ツールを自動的に検出し、CDC ツール関連のトレースログを zip パッケージに自動収集します。これらの zip ファイルをカスタマイズして

Scout に添付できます。この自動化により、Citrix Scout をより効果的に使用し、問題を迅速に診断できます。

詳細については、「追加のログ収集を有効にする」を参照してください。

マシン作成サービス™ (MCS)

Azure におけるイメージバージョンごとのレプリカ制限の増加

Azure は、ギャラリーイメージの単一バージョンあたりのレプリカの最大数を 100 に増やしました。この制限の増加により、Azure Compute Gallery イメージを使用して MCS マシンカタログを作成する際に、プロパティ `SharedImageGalleryReplicaMaximum` を最大値 100 に設定できるようになりました。詳細については、「Azure Compute Gallery を構成する」を参照してください。

Azure のネストされた仮想化のサポート

この機能を使用すると、ネストされた仮想化が有効になっているマスターVMを構成した場合、そのマスターVMを使用して作成されたMCSマシンカタログ内のすべてのVMでネストされた仮想化が有効になります。この機能は、永続VMと非永続VMの両方に適用されます。既存のMCSマシンカタログと既存のVMをイメージ更新によってネストされた仮想化を有効にするように更新できます。

現在、Dv3およびEv3 VMサイズのみがネストされた仮想化をサポートしています。

ネストされた仮想化の詳細については、Microsoftのブログ「Azureにおけるネストされた仮想化」を参照してください。

休止状態の失敗に関する警告メッセージの取得

MCSでプロビジョニングされた既存の休止状態対応VMの休止状態の失敗が発生した場合に、PowerShellコマンド Get-ProvOperationEvent を使用して警告メッセージを取得できるようになりました。詳細については、「休止状態の失敗に関する警告メッセージの取得」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/power-management/power-manage-azure-vms#get-warnings-messages-for-hibernation-failure) を参照してください。

Azureのホスト接続での権限の検証

以前は、Azure 環境では、Azure への接続を作成するために使用されるホスト接続資格情報 (クライアント ID またはアプリケーション ID) のみを検証できました。

この機能を使用すると、次のことができます。

- ホスト接続資格情報に割り当てられている権限のリストを取得する
- 割り当てられた権限で実行できる操作のリストを取得する
- 必要な権限に関する情報
- 必要な権限を追加する方法に関する情報

これにより、トラブルシューティングを行い、必要な権限を事前に取得できるため、ブロックされることなくタスクを実行できます。詳細については、「ホスト接続での権限の検証」を参照してください。

Azureでのディスク暗号化の変更

この機能により、Azure仮想化環境でディスク暗号化を変更できるようになりました。以下を実行できます。

- マスターイメージのDESとは異なるディスク暗号化セット（DES）を使用してMCSマシンカタログを作成する。
- 既存のMCSマシンカタログおよび既存のVMのディスク暗号化タイプを、あるDESキーから別のDESキーに変更する。
- 以前CMEKが有効になっていなかったMCSマシンカタログとVMを、顧客管理の暗号化キー（CMEK）暗号化（DES）、ホストでのディスク暗号化、または二重暗号化を持つように更新する。
- 以前暗号化されていた既存のMCSマシンカタログとVMを、非暗号化に更新する。
- プライベートエンドポイントを使用したディスク暗号化を有効にします（ProxyHypervisorTrafficThroughConnectorが有効なホスト接続を使用したMCSマシンカタログ）。

詳細については、「ディスク暗号化の変更」を参照してください。

ページファイル設定の変更のサポート

この機能により、マスターイメージを更新することなく、既存のカタログに新しく追加された VM のページファイル設定を変更できます。現在、この機能は Azure 環境のみに適用されます。

ページファイル設定を変更するには、VDAバージョン2311以降が必要です。PowerShellコマンドを使用してページファイル設定を変更できます。ページファイル設定の変更の詳細については、「ページファイル設定の変更」を参照してください。

AWS環境でGP3ボリュームタイプのIDディスクをMCSが作成

これまで、AWS環境では、VMのIDディスク（Identity disks）はGP2ボリュームタイプでした。この機能により、MCSはGP3ボリュームタイプのIDディスクを持つVMをプロビジョニングできるようになりました。GP3ボリュームタイプはAWSが提供する最も安価なオプションであるため、この機能はコストを最小限に抑えます。

この機能は、新しいカタログに追加されたVMと、既存のカタログに追加された新しいVMにのみ適用されます。この機能より前に作成された既存のVMは、IDディスクがリセットされない限り、引き続きGP2ボリュームタイプのIDディスクを持ちます。

AWSでマシンプロファイルソースを使用して追加プロパティをキャプチャするサポート

AWS環境では、この機能強化により、マシンプロファイルベースのカタログを作成または更新して、以下を含めることができるようになりました。

- MCSマシンカタログの作成時に、マシンプロファイルソースからCPUオプション、テナンシータイプ、および休止状態機能を取得します。
- MCSマシンカタログの編集中に、マシンプロファイルソースのテナンシータイプを変更します。この機能は、カタログに追加された新しいVMに適用されます。
- MCSマシンカタログの編集中に、マシンプロファイルソースの休止状態機能を変更します。この機能は、カタログに追加された新しいVMに適用されます。

マシンプロファイルソースは、VMまたは起動テンプレートバージョンにすることができます。この機能は、永続および非永続カタログの両方に適用されます。

詳しくは、「マシンプロファイルを使用してカタログを作成する」を参照してください。

AWSにおけるMCSマシンカタログVMのIDディスクの暗号化のサポート

以前は、AWS環境では、MCSはプロビジョニングされたVMのOSディスクのみの暗号化を許可していました。この機能により、OSディスクに加えてIDディスクも暗号化できるようになりました。この機能を使用すると、AWS KMSキー（カスタマーマネージドキーおよびAWSマネージドキー）を使用して、VMに接続されたディスクに対して暗号化操作を実行できます。

OSディスクとIDディスクの暗号化については、次のいずれかを構成してください。

- 暗号化されたマスターイメージを使用する（例：KMSキーで暗号化されたルートボリュームを含むインスタンスまたはスナップショットから作成されたAMI）

- 暗号化されたルートボリュームを含むマシンプロファイルのソース（VMまたは起動テンプレート）を使用する。

詳しくは、「OSディスクとIDディスクを暗号化する」を参照してください。

AWSにおけるホスト接続の権限の検証

AWS環境では、MCSマシンカタログの作成と管理に関連するタスクを実行するためのホスト接続の権限を検証できるようになりました。この実装により、VMの作成、削除、更新、VMの電源管理、EBS暗号化など、さまざまなシナリオで必要な不足している権限を事前に特定できるため、重要な時期にブロックされることを回避できます。詳しくは、「ホスト接続の権限を検証する」を参照してください。

GCPにおけるマシンプロファイルソースからVMおよびディスクへのラベルの継承のサポート

この機能により、MCSマシンカタログVMおよびディスク（IDディスク、ライトキャッシュバックディスク、およびOSディスク）は、マシンプロファイルソース（GCP VMインスタンスまたはインスタンステンプレート）のラベルを継承できるようになりました。ラベルを使用して、異なるチームが所有するインスタンス（例: team:researchおよびteam:analytics）を区別し、さらにコスト計算や予算編成に利用できます。ラベルの詳細については、GCPドキュメント「ラベルを使用してリソースを整理する」を参照してください。

この機能は、永続的および非永続的な MCS マシンカタログに適用されます。

新しいMCSマシンカタログを作成したり、既存のカタログを更新したり、既存のVMを更新してマシンプロファイルソースからラベルを継承させたりできます。

詳しくは、「継承されたラベルを持つVMとディスク」を参照してください。

XenServer®でMCS PowerShellコマンドを使用してCitrix Provisioningカタログを作成

XenServer環境でMCS PowerShellコマンドを使用してCitrix Provisioningカタログを作成できるようになりました。マシンプロファイルベースと非マシンプロファイルベースの両方のCitrix Provisioningカタログを作成できます。詳しくは、「Citrix StudioでCitrix Provisioningカタログを作成する」を参照してください。

マシンプロファイルからプロビジョニングされたVMへのカスタムタグの継承のサポート

SCVMM VMのカスタムタグを、デフォルトのCitrixProvisioningSchemeIdタグとともにMCSプロビジョニング済みVMに追加できるようになりました。プロビジョニング済みVMにカスタムタグを追加するには、MCSマシンカタログの作成または更新時にSCVMM VMをマシンプロファイルとして使用する必要があります。カタログからVMを削除した場合、CitrixProvisioningSchemeIdのみがタグから削除されます。カスタムタグはVMから削除されません。この機能は、新しいMCSマシンカタログと、既存のカタログに追加された新しいVMに適用されます。詳しくは、「マシンプロファイルを使用してカタログを作成する」を参照してください。

MCSマシンカタログを作成する前に構成を検証する

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

現在、この機能はAzure、GCP、およびVMware仮想化環境に適用されます。詳しくは、「MCSマシンカタログを作成する前に構成を検証する」を参照してください。

AWS、GCP、およびXenServerのアクティブなコンピューターアカウントのID情報を修復する

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

MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てるサポート

以前は、WindowsオペレーティングシステムがMCS I/Oライトバックキャッシュディスクにドライブ文字を自動的に割り当てていました。この機能により、MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てることができるようになりました。この実装は、使用するアプリケーションのドライブ文字とMCS I/Oライトバックキャッシュディスクのドライブ文字との間の競合を回避するのに役立ちます。この機能はWindowsオペレーティングシステムにのみ適用さ

れます。詳しくは、「MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てる」を参照してください。

プロファイル管理

新機能については、別のドキュメントの「新機能」を参照してください。

リナックス VDA

新機能については、別のドキュメントの「新機能」を参照してください。

セッション録画

新機能については、別のドキュメントの「新機能」を参照してください。

ワークスペース環境管理™

新機能については、別のドキュメントの「新機能」を参照してください。

シトリックス プロビジョニング

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

フェデレーション認証サービス

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

修正された問題

Citrix Virtual Apps and Desktops™ 7 2407 には、以下の修正された問題が含まれています。

グラフィック

- 作業中に約10秒間続く断続的な画面のブラックアウトが発生する場合があります。その間、Citrixソフトウェアのグラフィックプロセス (`Ctxgfx.exe`) がリセットされます。`twencode` スレッドでアクセス違反例外が発生し、`ctxExceptionHandler` がミニダンプを記録してこの問題を引き起こします。調査のために完全なダンプを生成するように `ctxExceptionHandler` が設定されています。

マシン作成サービス™

- 一部の2402 LTSR以前のバージョン（バージョン2302、2305、2308、2311を含む）から2402 LTSRにMulti-Delivery Controllerサイトをアップグレードする際に、サイトが部分的にしかアップグレードされていない場合、VMでの電源操作が失敗する可能性があります。詳細については、CTX666299 を参照してください。

シングルセッションOS用VDA

クリップボード

- VDA 2203 LTSR Cu4 を使用し、WebP形式のコンテンツをコピー＆ペーストすると、`WfShell` が動作を停止します。
- 公開されたリモートアプリのクリップボードへのコピーオプションが、CU3 および CU4 バージョンで機能しません。
- Server VDAインスタンスでCitrix Smart Cardサービスにメモリリークの問題が発生し、メモリ消費量が最大100%に達する場合があります。

セッション/接続

- OpenTEXT ETXアプリケーションは、以下のモジュールでアクセス違反が発生するため、開くことができません。

  `C:\Program Files\Citrix\HDX\bin\CtxMFPlugin64.dll`

スマートカード

- Server VDA インスタンスで Citrix Smart Card サービスにメモリリークの問題が発生し、メモリ消費量が最大 100% に達する場合があります。

マルチセッションOS用VDA

クリップボード

- VDA 2203 LTSR Cu4を使用しているときに、WebP形式のコンテンツをコピーして貼り付けると、`WfShell` が動作を停止します。
- 公開されたリモートアプリのクリップボードへのコピーオプションが、CU3 および CU4 バージョンで機能しません。
- Server VDA インスタンスで Citrix Smart Card サービスにメモリリークの問題が発生し、メモリ消費量が最大 100% に達する場合があります。

セッション/接続

- OpenTEXT ETX アプリケーションが、以下のモジュールでアクセス違反が発生するため起動に失敗します。

  `C:\Program Files\Citrix\HDX\bin\CtxMFPlugin64.dll`

スマートカード

- Server VDA インスタンスで Citrix Smart Card サービスにメモリリークの問題が発生し、メモリ消費量が最大 100% に達する場合があります。

既知の問題

Citrix Virtual Apps and Desktops™ 7 2407 には、以下の既知の問題が含まれています。

注

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

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

全般

- Windows Server 2025 を実行しているマシンに Citrix Virtual Apps and Desktops コンポーネントをインストールするためにメタインストーラーを使用すると、`MsiInstall` イベントがイベントログに書き込まれません。
- アプリバーを起動してから、Windows 用 Citrix Workspace™ アプリで接続センターメニューを開くと、アプリバーはそれをホストするサーバーの下に表示されません。
- Windows 用 Citrix Workspace アプリを使用し、アプリバーを垂直位置で起動すると、バーがスタートメニューまたはシステムクロックトレイを覆います。

- ホスト上で既にフォーカスされているコンボボックスをユーザーが選択すると、コンボボックスが正しく表示されない場合があります。回避策として、別の UI 要素を選択してからコンボボックスを選択してください。
- Windows 10 から Windows 11 へのインプレース OS アップグレードを実行した後、Citrix Desktop Service が起動に失敗する場合があります。この問題を解決するには、マシンを再起動してください。
- Windows Server 2022、Windows 10 Enterprise multi-session、および Windows 11 Enterprise multi-session を実行しているセッションホストでは、マルチセッション VDA の **セッション制限** 設定は拒否されます。 回避策として、GPO を介して **RDS セッション時間制限** を構成できます。
- 管理者権限でアプリケーションを実行している場合、FIDO2 に関連付けられた Windows セキュリティダイアログボックスは ICA® セッションウィンドウの前面に表示されません。昇格されたプロセスとして実行されている場合、Windows セキュリティダイアログボックスが ICA セッションウィンドウの背後に隠れるのは、オペレーティングシステムの設計によるものです。
- クライアントから ICA セッションへの 100MB を超えるデータのクリップボードコピーアンドペーストが失敗する場合があります。大きなバッファーのコピーはサポートされていません。
- Windows 10またはWindows 11マルチセッションOSは、Windowsシステム復元をサポートしていません。そのため、UIで復元ポイントを作成するオプションは利用できません。コマンドラインオプション `/EnableRestore` または `/EnableRestoreCleanup` は無視され、「Windows 10/11マルチセッションOSでは現在**システム復元の無効化**はサポートされていません」というメッセージがログに記録されます。
- Citrixは、Citrixが生成したバイナリとサードパーティ製のバイナリの両方に署名します。これは、バイナリがCitrixによって認証されていることを意味します。サードパーティ製バイナリのバージョンは、サードパーティから取得されたものであるため、同じままです。バイナリがすでにインストールされている場合、バージョンが一致するため、VDAアップグレードではバイナリはインストールされません。この制限を回避するには：

  a. バイナリを**許可リスト**に含めます。これにより、バイナリに署名する必要がなくなります。

  b. 古いVDAをアンインストールし、新しいVDAをインストールします。これはVDAの新規インストールに似ており、署名されたバージョンが適用されます。

- いくつかのシナリオで、クライアントIPポリシーフィルターを使用すると、ポリシーの評価に使用されるIPアドレスが正しくありません。

- シングルサインオンに拡張ドメインパススルーを使用している場合、クライアントデバイスまたはセッションホストがWindows 11を実行していると、セッションへのSSOが失敗する可能性があります。
- 無効なポリシー設定でサイトがアップグレードされると、ポリシーデータが失われる可能性があります。この問題が発生した場合は、Citrixサポートポータルを使用してテクニカルサポートケースをオープンしてください。
- VDAWorkstationSetup_2402、VDAServerSetup_2402、または VDAWorkstationCoreSetup_2402 パッケージを使用して Citrix Rendezvous V2 をインストールすると、これらのパッケージに Citrix.Diagnostics.Tracing.dll ファイルがないため、インストールが失敗する可能性があります。回避策：
  - 完全な CVAD Citrix Virtual Apps and Desktops 7 2402 LTSR パッケージまたは Citrix_Virtual_Apps_and_Desktops_7_2402_LTSR.iso から Citrix Rendezvous V2 をインストールします。
  - または、不足している Citrix.Diagnostics.Tracing.dll ファイルを置き換えます。ファイルを置き換えるには：
    a. CVAD Citrix Virtual Apps and Desktops 7 2402 LTSR パッケージまたは ISO の「x64\XenDesktop Setup」フォルダーから Citrix.Diagnostics.Tracing.dll ファイルをコピーします。
    b. 一時フォルダーを作成します。例：「C:\Workaround」。
    c. コマンド：VDAWorkstationSetup_2402.exe /extract "C:\Workaround" を実行して、最小インストーラーパッケージを一時フォルダーに抽出します。
    d. Citrix.Diagnostics.Tracing.dll ファイルを「C:\Workaround\Extract\Image-Full\x64\XenDesktop Setup」フォルダーにコピーします。
    e. 次のコマンドを実行してVDAのインストールを開始します: 「C:\Workaround\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVdaSetup.exe」
- ポリシー設定の更新からサイトサービスでのBLOBの生成まで、5分間の遅延があります。その結果、ポリシーが更新されセッションに反映されるまでに時間がかかる場合があります。

オーディオ

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

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

ウェブスタジオ

Web StudioでGoogle CloudのカタログをCMEK for disksを使用して編集する際、ウィザードのステップをスキップすると、将来マシンを追加する際に失敗する可能性があります。この問題を回避するには、ステップをスキップせずにウィザード全体を完了するか、PowerShell SDKを使用して操作を実行してください。

Web Studioを使用したSecure Private Access

- ユーザーが概要タブ > 「ライセンスサーバーURLを追加」リンクから設定 > 統合ページにリダイレクトされると、ナビゲーションバーが部分的に表示されます。ページを更新してナビゲーションバーを表示してください。
- 誤ったゲートウェイURLが入力されると、空白の警告ポップアップが表示されます。警告アイコンにカーソルを合わせると、警告メッセージが表示されます。
- Day 0統合を実行し、データベースを構成しようとすると、手動モードから自動モードに切り替えた後、警告ポップアップ内のテキストが表示されません。警告アイコンにカーソルを合わせると、メッセージが表示されます。
- コンソールのすべてのタブで垂直スクロールバーが部分的に表示されます。この問題に対する回避策は不要であり、機能やユーザーエクスペリエンスに影響はありません。
- **設定 > 統合**タブで、ブラウザウィンドウが小さい場合、ページ下部に水平スクロールバーが表示されません。ブラウザウィンドウが最大化されている場合、水平スクロールバーは不要です。
- **トラブルシューティング**ログで、ログ詳細ダイアログボックスが開いているときに、ページ下部に垂直スクロールバーが表示されません。この問題に対する回避策は不要であり、機能やユーザーエクスペリエンスに影響はありません。
- 「**概要**」タブは、Secure Private Accessコンソールにログインするとき、またはWSに戻ってSecure Private Accessコンソールに戻るときに強調表示されません。この問題に対する回避策は不要であり、機能やユーザーエクスペリエンスに影響はありません。
- 「**設定 > 統合**」タブでは、エラーメッセージがダイアログボックスの前面ではなく背面に表示されます。この問題に対する回避策は不要であり、機能やユーザーエクスペリエンスに影響はありません。

注:

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

グラフィック

- Theora圧縮を使用して64ビットのウェブカメラアプリでビデオプレビューを開始すると、セッションがクラッシュする可能性があります。
- Skype for desktopアプリで、リモートデスクトップに接続されている余分なウェブカメラに気づく場合があります。これらの余分なウェブカメラのプレビューはセキュリティ上の理由からブロックされ、黒い画面が表示されることがあります。余分なウェブカメラは無視し、エンドポイント用のウェブカメラを引き続き使用できます。

マシン作成サービス™

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

印刷

- 仮想デスクトップで選択されたUniversal Print Serverプリンターは、コントロールパネルの「**デバイスとプリンター**」ウィンドウに表示されません。ただし、ユーザーがアプリケーションで作業しているときは、それらのプリンターを使用できます。この問題はWindows 10でのみ発生します。詳細については、CTX213540を参照してください。
- 印刷ダイアログウィンドウでデフォルトプリンターが正しくマークされない場合があります。この問題は、デフォルトプリンターに送信される印刷ジョブには影響しません。
- Universal Print ServersへのSSL接続が有効になっている場合、ロードバランスされたネットワークプリンターからの印刷ジョブの一部が失敗する可能性があります。これは、印刷ジョブが次々と高速で実行された場合に発生します。
- Microsoftは、Modern Print Dialogを使用する際に印刷ジョブ間で印刷設定が保持されない問題があることを確認しており、現在その解決に取り組んでいます。現在の予測では、2025年前半に解決される見込みです。Modern Print Dialogは、Windows 11やWindows Server 2025などの新しいOSバージョンでデフォルトで有効になっています。OSをレガシー印刷ダイアログを使用するように構成するには、次のアクションを実行します。

1. レジストリエディターを開きます
2. HKEY_CURRENT_USER\Software\Microsoft\Print\UnifiedPrintDialog に移動します

3. 右クリックして、 > を選択します
4. 値の名前を PreferLegacyPrintDialog に変更します
5. PreferLegacyPrintDialog を右クリックして、修正を選択します
6. 値のデータを 1 に設定し、OK をクリックします

サードパーティの問題

- Chrome は、Web ページ上のツールバー、タブ、メニュー、およびボタンに対してのみ UI オートメーションをサポートしています。この Chrome の問題により、タッチデバイス上の Chrome ブラウザでは、自動キーボード表示機能が動作しない場合があります。回避策として、`chrome --force-renderer-accessibility` を実行するか、新しいブラウザタブを開いて `chrome://accessibility` と入力し、特定のページまたはすべてのページで **Native accessibility API** のサポートを有効にすることができます。さらに、シームレスアプリを公開する場合、`--force-renderer-accessibility` スイッチを使用して Chrome を公開できます。
- セッションホストにFSLogix 2201 HF1がインストールされている場合、セッション起動時に黒い画面が表示されることがあります。この問題を解決するには、FSLogixを新しいバージョンにアップグレードする必要があります。

プロファイル管理

- Profile Management 2407 documentation は、このリリースでの更新に関する具体的な情報を提供します。

リナックス VDA

- Linux VDA 2407 documentation は、このリリースでの更新に関する具体的な情報を提供します。

セッション録画

- Session Recording 2407 documentation は、このリリースでの更新に関する具体的な情報を提供します。

ワークスペース環境管理™

- 「Workspace Environment Management 2407 のドキュメント」(/ja-jp/workspace-environment-management/current-release/known-issues.html) には、このリリースでの更新に関する具体的な情報が記載されています。

シトリックス プロビジョニング™

- 「Citrix Provisioning 2407 のドキュメント」(/ja-jp/provisioning/current-release/whats-new/known-issues.html) には、このリリースでの更新に関する具体的な情報が記載されています。

フェデレーション認証サービス

- 「フェデレーション認証サービス 2407 のドキュメント」(/ja-jp/federated-authentication-service/current-release/whats-new/known-issues.html) には、このリリースでの更新に関する具体的な情報が記載されています。

廃止予定

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

非推奨と廃止

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

非推奨

非推奨とは、将来のリリースからその機能または能力を削除する予定であることです。その機能または能力は、正式に削除されるまで引き続き動作し、完全にサポートされます。この非推奨通知は、数か月から数年にわたる場合があります。削除後、その機能または能力は動作しなくなります。この通知は、機能または能力が削除される前に、コードを計画および更新するための十分な時間を提供することを目的としています。非推奨の項目については、可能な限り代替案が提案されます。

項目	非推奨が発表されたバージョン	代替
複数モニターフック	2407	-

項目	非推奨が発表されたバージョン	代替
ドメインパススルー認証	2407	シングルサインオン用の拡張ドメインパススルーを使用してください。
ランデブー V1	2402	Rendezvous V2を使用してください。
セキュア ICA®	2402	-
Windows Server 2016でのVDAサポート	2402	最新のWindows Serverバージョンにアップグレードしてください。
Windows Server 2016でのDelivery Controller™、Web Studio、Citrix Director、Citrix License Server、Citrix StoreFront、シングルセッションOS用Server VDI、マルチセッションOS用VDA、Active Directoryフォレストとドメイン、およびUniversal Print Serverのサポート	2402	最新バージョンのWindows Serverにアップグレードしてください。
サイト構成、構成ログ、および監視データベース用のMicrosoft SQL Server 2016および2017バージョンのサポート	2402	最新バージョンのMicrosoft SQL Serverにアップグレードしてください。
ライトバックキャッシュを、ディスクキャッシュのみを含み、メモリキャッシュを含まないように構成するサポート	2402	メモリキャッシュサイズ構成オプションを使用して、ゼロ以外のサイズを割り当てます。
オンデマンドプロビジョニング機能より前に作成されたAzureカタログ（「レガシー」カタログ）のサポート	2402	Azureレガシーカタログ VMを再作成します。カタログはオンデマンドとしてプロビジョニングされ、ストレージコストを節約します。

項目	非推奨が発表されたバージョン	代替
ターゲット最小フレームレートポリシー	2311	**グラフィックステータスインジケーター**を使用して、ターゲット最小フレームレートを変更します。
System Center Configuration Manager に対応した Citrix Connector 3.1 のサポート	2311	イメージまたはアプリケーションの更新を手動で行います。
カタログが作成されたリージョンとは異なるリージョンでマスターイメージを使用するサポート	2311	Azure Compute Galleryを使用して、マスターイメージを目的のリージョンにレプリケートします。
HDX Graphics ディスプレイメモリ制限設定	2311	クライアントのディスプレイレイアウトが完全に収まるように、必要な最小限のメモリが割り当てられます。
HDX Graphicsでのプログレッシブモードのサポート	2311	Thinwireを使用してください。プログレッシブモードを参照してください。
Internet Explorer 11でのブラウザコンテンツリダイレクトのサポート	2311	Google Chromeベースのブラウザコンテンツリダイレクトを使用してください。
AWSボリュームワーカーのサポートを削除	2311	ダイレクトディスクのアップロードとダウンロードを使用してください。ダイレクトディスクのアップロードとダウンロードを参照してください。
BrokerでのSQL Server 2016のサポート	2308	最新バージョンを使用してください。詳しくは、システム要件を参照してください。
Director での XenApp 5.x のサポート	2308	---

項目	非推奨が発表されたバージョン	代替
Director での XenApp 6.x のサポート	2308	---
Director のアラート用 SCOM Pack	2308	---
Director でのプラグインのサポート	2308	---
WebRTC SDP 形式 (プラン B) のサポート	2308	Citrix Workspace™ アプリをサポートされているバージョンにアップグレードします。
Microsoft Teams Optimization におけるシングルウィンドウモードのサポート	2308	Citrix Workspaceアプリを MultiWindowモードをサポートするバージョンにアップグレードしてください。詳細については、機能マトリックスとバージョンサポートを参照してください。
AWS環境で使用される `AwsCaptureInstanceProperties` のサポート	2308	マシンプロファイルを使用してください。マシンプロファイルを使用してカタログを作成するを参照してください。
`Schedule-ProvVMUpdate` PowerShellコマンド	2305	`Set-ProvVMUpdateTimeWindow` を使用してください。
`Request-ProvVMUpdate` PowerShellコマンド	2305	`-StartsNow` および `-DurationInMinutes -1` パラメーターとともに `Set-ProvVMUpdateTimeWindow` を使用してください。
`Cancel-ProvVMUpdate` PowerShellコマンド	2305	`Clear-ProvVMUpdateTimeWindow` を使用してください。

項目	非推奨が発表されたバージョン	代替
`New-ProvScheme`コマンドで使用される`DedicatedTenancy`パラメーター	2303	`TenancyType`パラメーターを使用してください。
ライセンスサーバー VPX	2206	---
Azure環境でVMをプロビジョニングするためのアンマネージドディスク。	2206	マネージドディスクを使用。
ホストからクライアントへの（URL）リダイレクト	2203	双方向コンテンツリダイレクト。
クラウドおよびオンプレミス環境で使用される4つのAWS固有コマンド（`Revoke-HypSecurityGroupIngress`、`Revoke-HypSecurityGroupEgress`、`Grant-HypSecuritygroupegress`、`Grant-HypSecurityGroupIngress`）のサポート。	2203	---
VDAメタインストーラーからのCitrix Files for WindowsおよびCitrix Files for Outlook。	2203	スタンドアロンインストーラーを使用してください。
VDAメタインストーラーからのWEMエージェントコンポーネント。	2203	---
Remote PC Access用のSCCM統合Wake on LANオプション。	2012	スタンドアロンのWake on LAN機能を使用してください。
XenAppおよびXenDesktop、Provisioning Services、StoreFront用Citrix SCOM	1912	展開の監視と管理にはDirectorを使用してください。SCOMのEOLと代替案の

項目	非推奨が発表されたバージョン	代替
Management Pack。監視可能な製品バージョンについては、Citrix SCOM Management Packのドキュメントを参照してください。		詳細については、https://support.citrix.com/article/CTX266943を参照してください。
モビリティSDK / モバイルSDK（旧シトリックス・ラボ製）	7.16	モバイルエクスペリエンスポリシー設定、およびホスト型デスクトップ/アプリのネイティブエクスペリエンスに置き換えられました。

削除された項目

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

項目	廃止が発表されたバージョン	削除されたバージョン	代替手段
Citrix StudioでのPVSインポートウィザードのサポート	1912 LTSR	2311	以下のいずれかの方法でCitrix Provisioning™マシンをプロビジョニングします • Citrix Provisioning Consoleを使用してマシンをプロビジョニングし、Citrix Provisioning Devices

項目	廃止が発表されたバージョン	削除されたバージョン	代替手段	
			Export Wizardを使用して Citrix Virtual Apps and Desktopsにエクスポートします。詳細については、デバイスエクスポートウィザードを参照してください。 • Web Studioを使用して Citrix Provisioning カタログを作成します。詳細については、Citrix Studio で Citrix Provisioning カタログを作成するを参照してください。	

項目	廃止が発表されたバージョン	削除されたバージョン	代替手段
Windows 用 Citrix Workspace アプリ 1912	---	2402	最新バージョンを使用してください。
HDX Graphics 全画面表示 + テキスト最適化	2311	2311	
HDX 3D Pro を使用した NVIDIA Frame Buffer Capture (NVFBC) のサポート	2308	2311	Desktop Duplication API (DDAPI) を使用してください。
ポリシー設定「インボックスプリンタードライバーの自動インストール」に対する VDA のサポート。	7.16	2311	なし。ポリシー設定は、以前の OS（Windows 7、Windows Server 2012 R2 以前）のVDAでのみサポートされています。
NVIDIA GPU ハードウェアエンコーディング (NVENC) (vGPU 11以前、およびドライバーバージョン466.77以前の場合)。	2305	2305	現在サポートされているNVIDIAドライバーを使用してください: vGPU 13以降、バージョン471.41以降。
VDAメタインストーラーからのCitrixサポートツール	---	2212	---

項目	廃止が発表されたバージョン	削除されたバージョン	代替手段
(SupportabilityTool_x64 .msi)。			
Citrixライセンス管理コンソール (Windows License Server 11.16.3 build 30000に最後に含まれ、Windows License Server v11.16.6 build 31000で削除されました)。	2003	2006	Citrix Licensing Managerを使用してください。
Windows 10 バージョン 1709以前での Citrix Indirect Display Driver (IDD) グラフィックアダプターのサポート。	2003	2003	Citrix Virtual Apps and Desktops 7 1912 LTSR VDAを使用してください。
GRID 9以前のディスプレイドライバーを使用したNVIDIA GPU (NVENC) によるハードウェアエンコーディング。	2003	2003	Citrix Virtual Apps and Desktops 7 2003以降のVDAでGRID 10ディスプレイドライバーを使用するか、Citrix Virtual Apps and Desktops 7 1912 LTSR VDAを使用してください。

項目	廃止が発表されたバージョン	削除されたバージョン	代替手段
セルフサービスパスワードリセット (SSPR) 機能。	2003	2006	---
VDAおよびコアサーバーコンポーネントにおけるバージョン4.8より前のMicrosoft .NET Frameworkバージョンのサポート。Delivery Controller、Studio、Directorを含む。	1912	2003	.NET Framework バージョン 4.8 にアップグレードします。
Windows Server 2012 R2 で動作する VDA。	1912	2003	サポートされているオペレーティングシステムに VDA をインストールします。
Citrix Virtual Apps and Desktops Premium エディションの AppDNA® アプリケーション移行コンポーネント。	1909	2003	---
32 ビット (x86) マシンへの Studio のインストール。	1909	2003	サポートされている x64 オペレーティングシ

項目	廃止が発表されたバージョン	削除されたバージョン	代替手段
			ステムにインストールします。
シームレスアプリケーションでの Excel フックのサポート。これは、Microsoft Excel 2010 の各ワークブックに個別のタスクバーアイコンを作成するために使用されていました。	1909	1909	---
Windows Server 2012 R2 (サービスパックを含む) 上のコアサーバーコンポーネント。含まれるもの: Delivery Controller、Studio、Director。	1906	2003	より新しいサポート対象のオペレーティングシステムにインストールしてください。
Microsoft SQL Serverバージョン2008 R2、2012、2014 (すべてのサービスパックとエディションを含む) 上のサイト構成、構成ログ、および監視データベースのサポート。	1906	2003	サポートされているMicrosoft SQL Server バージョンにデータベースをインストールしてください。

項目	廃止が発表されたバージョン	削除されたバージョン	代替手段
x86プラットフォーム上のWindows 10でのVDAのサポート。	1906	1909*	サポートされているx64オペレーティングシステムにVDAをインストールしてください。*この機能は、Citrix Virtual Apps and Desktops 7 1912 LTSRでは引き続きサポートされています。
Citrix Virtual Apps and Desktopsインストールメディアからの Citrix Smart Tools Agentの削除。	1903	1906	---
Red Hat Enterprise Linux/CentOS 7.5上でのLinux VDAのサポート。	1903	1903	Red Hat Enterprise Linuxのそれ以降のバージョンにLinux VDAをインストールする。
Citrix Virtual Apps and Desktops (旧XenAppおよびXenDesktop) とCitrix Receiver、およびWorkspace Hub間でのTLS	7.17	2203	Citrix Receiverを、TLS 1.2プロトコルをサポートするCitrix Workspaceアプリにアップグレードしてください。Citrix

項目	廃止が発表されたバージョン	削除されたバージョン	代替手段
1.0およびTLS 1.1プロトコルのStoreFrontサポート。			Workspaceアプリの詳細については、https://docs.citrix.com/ja-jp/citrix-workspace-app を参照してください。
ポリシー設定「インボックスプリンタードライバーの自動インストール」のVDAサポート。	7.16	2311	なし。このポリシー設定は、以前のOS (Windows 7、Windows Server 2012 R2以前) のVDAでのみサポートされます。
Framehawkディスプレイリモートテクノロジーのサポート	1811	1903	Thinwire を使用し、adaptive transport を有効にします。
すべてのCitrix Virtual Apps and Desktops (およびXenApp and XenDesktop) バージョンにおけるCitrix Smart Scaleのサポート。この機能は 31 May 2019 にサポート終了となります。	1808	1906	電力管理機能の向上のため、Citrix Cloud上のVirtual Apps and Desktops Service の使用を検討してください。

項目	廃止が発表されたバージョン	削除されたバージョン	代替手段
Citrix StoreFront、Citrix VDA、Citrix Studio、Citrix Director、およびCitrix Delivery Controllerによる Microsoft .NET Frameworkバージョン4.5.1、4.5.2、4.6、4.6.1、4.6.2、および4.7のサポート。	7.18	1808	.NET Frameworkバージョン4.7.1以降にアップグレードしてください。(インストーラーは、まだインストールされていない場合、.NET Framework 4.7.1を自動的にインストールします。)
Red Hat Enterprise Linux 7.3におけるLinux VDAのサポート。	7.18	1808	Red Hat Enterprise Linux の新しいバージョンに Linux VDA をインストールします。
SUSE Linux Enterprise Server 11 Service Pack 4 における Linux VDA のサポート。	7.16	7.16	サポートされているSUSEバージョンにLinux VDAをインストールします。
VDAでのCitrix WDDMドライバーのサポート	7.16	7.16	Citrix WDDMドライバーはVDAとともにインストールされなくなりました。

項目	廃止が発表されたバージョン	削除されたバージョン	代替手段
Windows 10 バージョン 1511 (Threshold 2) およびそれ以前の Windows シングルセッション OS リリース (Windows 8.x および Windows 7 を含む) 上の VDA (<https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/> を参照)。	7.15 LTSR (および 7.12)	7.16	Windows 10 の最小バージョン 1607 (Redstone 1) 以降の半期チャネルにシングルセッション OS VDA をインストールします。1607 LTSB を使用している場合は、7.15 VDA を推奨します。CTX224843 を参照してください。
Windows Server 2008 R2 および Windows Server 2012 (サービスパックを含む) 上の VDA	7.15 LTSR (および 7.12)	7.16	サポートされているオペレーティングシステムにVDAをインストールします。
デスクトップコンポジションリダイレクト (以前はDirectXコマンドリモート処理として知られていました) (DCR)	7.15 LTSR	7.16	Thinwireを使用します。

項目	廃止が発表されたバージョン	削除されたバージョン	代替手段
Windows Server 2012およびWindows Server 2008 R2 (サービスパックを含む) 上のコアコンポーネント。内訳: Delivery Controller、Studio、Director、StoreFront、License Server、Universal Print Server。	7.15 LTSR	7.18	サポートされているオペレーティングシステムにコンポーネントをインストールします。
Windows Server 2012およびWindows Server 2008 R2 (サービスパックを含む) 上のセルフサービスパスワードリセット (SSPR) 機能	7.15 LTSR	7.18	より新しいサポートされているオペレーティングシステムにインストールします。
Windows 7、Windows 8、およびWindows 8.1 (サービスパックを含む) 上のStudio	7.15 LTSR	7.18	サポートされているオペレーティングシステムにStudioをインストールします。
Flashリダイレクト	7.15 LTSR	1912	ビデオコンテンツをHTML5ビデオとして作成します。管理対

項目	廃止が発表されたバージョン	削除されたバージョン	代替手段
			象コンテンツにはHTML5ビデオのリダイレクトを、公開Webサイトにはブラウザコンテンツのリダイレクトを使用します。詳細については、Flashリダイレクトのサポート終了の注記を参照してください。
StoreFrontとのCitrix Online統合（Goto製品）	7.14 (およびStoreFront 3.11)	StoreFront 3.12	---
VDAのインストール中に作成され、VDAマシンのローカル管理者グループに追加されたユーザーアカウントCtxAppVCOMAdminは、作成されなくなりました。基盤となる「COM」メカニズムも削除されました。	7.14	7.14	Windowsサービス CtxAppVServiceは同じ機能を実行します。これは自動的にインストールおよび構成され、ユーザーによる操作は不要です。
ユニバーサルプリントサーバーのUpsServerコンポーネントのWindows	7.14	7.14	より新しいサポート対象のオペレーティングシステムにイン

項目	廃止が発表されたバージョン	削除されたバージョン	代替手段
Server 2008 32ビットでのサポート			ストールしてください。
Internet Explorer 8上で動作するStoreFrontおよびReceiver for Web	7.13	7.13	---
Citrix App-Vコンポーネントのインストールを防止するためのVDAコマンドラインインストールオプション / no_appv	7.13	7.13	コマンドラインインストールオプション / exclude "Citrix Personalization for App-V – VDA" を使用してください。
フルプロダクトインストーラーは、新規インストール時にCitrix.Common.Commandsスナップインをインストールしなくなり、既存のインストールをアップグレードする際に自動的に削除します。	7.13	7.13	Citrix.Common.Commands スナップインによって提供されていた一部のPowerShellコマンドは、XenApp 6.5 SDKで引き続き利用できます。
*-CtxIcon コマンドレットによって提供されていたアイコンデータを操作す	7.13	7.13	現在、Broker Serviceの*-BrokerIcon コマンドレットによって提供されています。

項目	廃止が発表されたバージョン	削除されたバージョン	代替手段
る部分的な機能。			
レガシーThinwireモード	7.12	7.16	(/ja-jp/xenapp-and-xendesktop/current-release/graphics/thinwire.html)を使用してください。Windows Server 2008 R2でレガシーThinwireモードを使用している場合は、Windows Server 2012 R2またはWindows Server 2016に移行し、Thinwireを使用してください。
StoreFront 2.0、2.1、2.5、および2.5.2からのインプレースアップグレード	7.13	7.16	これらのバージョンのいずれかから、サポートされているより新しいバージョンにアップグレードし、その後XenAppおよびXenDesktop 7.16にアップグレードしてください。
XenDesktop 5.6または5.6 FP1	7.12	7.16	XenDesktop 5.6または5.6 FP1

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

項目	廃止が発表されたバージョン	削除されたバージョン	代替手段
CloudPlatform 接続のサポート	7.12	2003	別のサポートされているハイパーバイザーまたはクラウドサービスを使用します。
Azure Classic（別名Azure Service Management）接続のサポート	7.12	2003	Citrix Cloud の Virtual Apps and Desktops Service の使用を検討してください。
AppDisks 機能 (およびそれをサポートする Studio への AppDNA 統合)	7.13	2003	Citrix App Layering を使用してください。
Personal vDisk 機能	7.15	2006†	Citrix App Layering ユーザーレイヤー または ユーザーパーソナライゼーションレイヤー テクノロジーを使用してください。

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

システム要件

はじめに

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

インストールを開始する前に、インストールの準備を確認してください。

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

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

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

ハードウェア要件

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

次の表に、コアコンポーネントの最小要件を示します。

コンポーネント	最小要件
すべてのコアコンポーネントとStoreFront™を1台のサーバーにインストール（評価用のみ、本番環境への展開は不可）	5 GB RAM

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

デスクトップとアプリケーションを提供するVMのサイジング

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

詳細については、以下を参照してください。

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

マイクロソフト ビジュアル C++

Delivery Controller、Virtual Delivery Agent (VDA)、またはUniversal Print Serverをインストールすると、CitrixインストーラーはMicrosoft Visual C++ 2015–2022 再頒布可能パッケージを自動的にインストールします。

- マシンにそのランタイムの以前のバージョン（2015-2019など）が含まれている場合、Citrixインストーラーがそれをアップグレードします。

- マシンに2015年より前のバージョンが含まれている場合、Citrixは新しいバージョンを並行してインストールします。

デリバリーコントローラー

サポートされているオペレーティングシステム：

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

要件：

- Microsoft .NET Framework 4.8がまだインストールされていない場合（またはそれ以降のバージョンがインストールされていない場合）、自動的にインストールされます。
- Windows PowerShell 3.0、4.0、または5.0。
- Microsoft Visual C++ 2015–2022 再頒布可能パッケージ。

データベース

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

- SQL Server 2022、Express、Standard、およびEnterpriseエディション。
  - 新規インストールの場合：既存のサポートされているSQL Serverインストールが検出されない場合、デフォルトで、Controllerのインストール時に累積更新プログラム14が適用されたSQL Server Express 2022がインストールされます。
- SQL Server 2019、Express、Standard、およびEnterpriseエディション。
- SQL Server 2017、Express、Standard、およびEnterpriseエディション。
  - アップグレードの場合、既存のSQL Server Expressバージョンはアップグレードされません。
- SQL Server 2016 SP2、Express、Standard、およびEnterpriseエディション。

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

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

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

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

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

その他のデータベース情報:

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

ウェブ スタジオ

> **注:**
>
> - Citrix Virtual Apps and Desktops™の展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。
> - Web Studioは、オンプレミスのCitrix Virtual Apps and Desktops展開を構成および管理できるWebベースの管理コンソールです。ユーザーエクスペリエンスの向上を目的として

> 設計されており、Windowsベースの管理コンソールであるCitrix Studioよりも一般的に応答が高速です。Web Studioのインストールを参照してください。

> サポートされているオペレーティングシステム:

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

Citrix Director (シトリックス ディレクター)

サポートされているオペレーティングシステム:

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

要件:

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

Citrix プロファイル管理:

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

システムセンター オペレーションズマネージャー (SCOM) 統合要件:

- System Center 2012 R2 オペレーションズマネージャー

Directorを表示するためのサポートされているブラウザ:

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

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

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

サポートされているオペレーティングシステム:

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

要件:

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

リモートPCアクセスでは、物理オフィスPCにインストールするこのVDAを使用します。このVDAは、Windows 11およびWindows 10上のCitrix Virtual Desktops™リモートPCアクセス向けSecure Bootをサポートしています。

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

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

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

Windows 7マシンにVDAをインストールする方法については、Earlier operating systemsを参照してください。

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

サポートされているオペレーティングシステム:

- ウィンドウズ サーバー 2025
- Windows 11 (Citrix DaaS™でのみサポート)
- Windows 10 (x64のみ、Citrix DaaSでのみサポート)、現在メインストリームサポート中のすべてのバージョン。
- ウィンドウズ サーバー 2022
- ウィンドウズ サーバー 2019、スタンダード エディション および データセンター エディション

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

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

Remote Desktop Servicesの役割サービスがまだインストールおよび有効化されていない場合、インストーラーは自動的にそれらをインストールおよび有効化します。

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

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

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

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

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

ホスト / 仮想化リソース

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

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

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

サポートされているハイパーバイザー：

- **ゼノサーバー (旧 シトリックス ハイパーバイザー™)**

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

  詳細については、「XenServer仮想化環境」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/install-prepare/xenserver.html)を参照してください。

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

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

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

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

- **Nutanix アクロポリス**

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

詳細については、Nutanix仮想化環境を参照してください。

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

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

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

  詳細については、VMware仮想化環境を参照してください。

サポートされているパブリッククラウドホスト:

- **アマゾン ウェブ サービス (AWS)**

  AWS を使用した仮想マシンのプロビジョニングについては、「Amazon Web Services 仮想化環境」を参照してください。

- **Google Cloud Platform** 詳細については、「Google Cloud Platform 仮想化環境」および「Google Cloud での Citrix DaaS の概要」を参照してください。
- **マイクロソフト アジュール リソース マネージャー**

  Microsoft Azure Resource Manager を使用した仮想マシンのプロビジョニングについては、「Microsoft Azure Resource Manager 仮想化環境」を参照してください。

- **Nutanix クラウドおよびパートナーソリューション**

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

- **VMware クラウドおよびパートナーソリューション**

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

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

- ハイブリッド権限ライセンスが必要です。ハイブリッド権限ライセンスについては、Transition and Trade-Up (TTU) with Hybrid Rightsを参照してください。ライセンスの追加については、Create a siteを参照してください。
- 情報ソースはCitrix DaaSのドキュメントに誘導します。Citrix DaaS製品のパブリッククラウドホストに慣れている場合でも、オンプレミスバージョンにはいくつかの違いがあります。

- Citrix DaaS では、管理インターフェイスは「Full Configuration」として知られています。オンプレミスの Citrix Virtual Apps and Desktops では、管理インターフェイスは「Web Studio」として知られています。
- Citrix DaaS への更新は、約4週間ごとに展開されます。そのため、Citrix DaaS で利用できる特定の機能がオンプレミスバージョンでは利用できない場合があります。

Active Directoryの機能レベル

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

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

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

HDX

オーディオ

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

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

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

HDX Windows Media の配信

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

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

HDX 3D Pro 機能

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

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

- GPUパススルーは以下で利用可能です。
  - XenServer®
  - ニュータニックス エーエイチブイ
  - VMware vSphereおよびVMware ESX。これらは仮想ダイレクトグラフィックスアクセラレーション（vDGA）と呼ばれます。
- vGPUは以下で利用可能です。
  - XenServer
  - ニュータニックス エーエイチブイ
  - ブイエムウェア ブイスフィア

`<https://docs.citrix.com/ja-jp/citrix-virtual-apps-desktops/2407/graphics/hdx-3d-pro>`を参照してください。

Citrixでは、ホストコンピューターに4GB以上のRAMと、2.3GHz以上のクロック速度を持つ4つの仮想CPUを搭載することを推奨しています。

グラフィックス処理ユニット（GPU）：

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

ユーザーデバイス：

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

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

ユニバーサル プリント サーバー

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

UpsServerコンポーネントは以下でサポートされています。

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

要件:

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

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

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

詳しくは、プリンターのプロビジョニングを参照してください。

その他

Citrix License Server 11.17.2以降のみがサポートされています。詳しくは、ライセンスを参照してください。

バージョン互換性について詳しくは、製品マトリックスを参照してください。

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

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

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

複数のNICがサポートされています。

デフォルトでは、現在のVDAをインストールしてもCitrix Workspaceアプリ for Windowsはインストールされません。詳しくは、Citrix Workspaceアプリ for Windowsのドキュメントを参照してください。

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

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

この製品はPowerShellバージョン3～5をサポートしています。

技術概要

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

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

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

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

主要コンポーネント

Citrix Virtual Apps and Desktops を初めて使用する方にとって、この記事は非常に役立ちます。

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

一般的な展開における主要コンポーネント(/en-us/citrix-virtual-apps-desktops/2407/media/components-new-op.png)

デリバリーコントローラー™

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

- アプリケーションとデスクトップを配信する

- ユーザーアクセスを認証および管理する
- ユーザーと、そのデスクトップおよびアプリケーションとの間の接続を仲介する
- ユーザー接続を最適化する
- 接続をロードバランスする

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

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

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

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

データベース

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

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

仮想配信エージェント (VDA)

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

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

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

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

シトリックス StoreFront™

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

シトリックス Workspace™ アプリ

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

スタジオ

Citrix Virtual Apps and Desktops の展開は、Web Studio (Webベース) と Citrix Studio (Windowsベース) の2つの管理コンソールを使用して管理できます。この製品ドキュメントでは、Web Studio のみを取り扱っています。Citrix Studio の詳細については、「Citrix Virtual Apps and Desktops 7 2212 またはそれ以前のバージョン」を参照してください。

ウェブスタジオ

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

シトリックス スタジオ

Citrix Studio は、Citrix Virtual Apps and Desktops の展開を構成および管理する管理コンソールです。Citrix Studio を使用すると、アプリケーションとデスクトップの配信を管理するための個別の管理コンソールが不要になります。Citrix Studio には、環境のセットアップ、アプリケーションとデスクトップをホストするワークロードの作成、ユーザーへのアプリケーションとデスクトップの割り当てをガイドするウィザードが用意されています。Studio を使用して、サイトの Citrix ライセンスを割り当てたり追跡したりすることもできます。

Citrix Studio は、Controller 内の Broker Service から表示する情報を取得し、TCPポート80を介して通信します。

セキュア プライベート アクセス

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

シトリックス ディレクター

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

Director には以下が表示されます。

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

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

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

Citrixライセンスサーバー

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

ハイパーバイザーまたはその他のサービス

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

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

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

追加コンポーネント

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

Citrix プロビジョニング™

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

シトリックス ゲートウェイ

ユーザーが企業ファイアウォールの外部から接続する場合、Citrix Virtual Apps and Desktops は Citrix Gateway (旧称 Access Gateway および NetScaler® Gateway) テクノロジーを使用して、これらの接続を TLS で保護できます。Citrix Gateway または VPX 仮想アプライアンスは、DMZ (非

武装地帯) に展開される SSL VPN アプライアンスです。これは、企業ファイアウォールを介した単一のセキュアなアクセスポイントを提供します。

シトリックス SD-WAN™

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

一般的な展開の仕組み

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

展開におけるコンポーネント間の通信(/en-us/citrix-virtual-apps-desktops/2407/media/deployment-overview.png)

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

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

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

ユーザー接続の処理方法

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

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

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

ユーザー接続フロー(/en-us/citrix-virtual-apps-desktops/2407/media/user-connections.png)

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

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

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

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

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

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

データアクセスがどのように機能するか

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

展開におけるデータアクセス(/en-us/citrix-virtual-apps-desktops/2407/media/data-access.png)

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

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

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

デスクトップとアプリケーションの配信

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

マシンカタログ

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

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

有効なマシンタイプは次のとおりです。

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

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

デリバリーグループ

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

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

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

詳細については、デリバリーグループの作成を参照してください。

アプリケーショングループ

アプリケーショングループは、より多くのデリバリーグループを使用するよりも、アプリケーション管理とリソース制御の利点を提供します。タグ制限機能を使用すると、既存のマシンを複数の公開タスクに使用できるため、展開とより多くのマシンの管理に関連するコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）するものと考えることができます。アプリケーショングループは、デリバリーグループ内のマシンの一部を分離してトラブルシューティングする場合にも役立ちます。

詳細については、アプリケーショングループの作成を参照してください。

詳細情報

- シトリックス バーチャル アプリケーションズ アンド デスクトップス の図
- ネットワークポート
- データベース
- サポートされるハイパーバイザーおよびその他のサービス

データベース

> **注:**

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

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

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

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

Citrixは、データベースに関して以下を推奨します。

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

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

高可用性

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

- **AlwaysOn可用性グループ (基本可用性グループを含む):** SQL Server 2012で導入されたこのエンタープライズレベルの高可用性および災害復旧ソリューションにより、1つ以上のデータベースの可用性を最大化できます。AlwaysOn可用性グループでは、SQL ServerインスタンスがWindows Server Failover Clustering (WSFC) ノード上に存在する必要があります。詳細については、「SQL ServerでのWindows Serverフェールオーバークラスタリング」を参照してください。

- **SQL Server データベースミラーリング:** データベースをミラーリングすることで、アクティブなデータベースサーバーが失われた場合でも、自動フェイルオーバープロセスが数秒で発生し、ユーザーは通常影響を受けません。この方法は、各データベースサーバーに完全なSQL Serverライセンスが必要となるため、他のソリューションよりも高価です。ミラーリング環境ではSQL Server Express editionを使用できません。
- **SQLクラスタリング:** Microsoft SQLクラスタリングテクノロジーを使用すると、障害が発生した別のサーバーのタスクと責任を、あるサーバーが自動的に引き継ぐことができます。ただし、このソリューションのセットアップはより複雑であり、自動フェイルオーバープロセスは、SQLミラーリングなどの代替手段よりも通常遅くなります。
- **ハイパーバイザーの高可用性機能の使用:** この方法では、データベースを仮想マシンとして展開し、ハイパーバイザーの高可用性機能を使用します。既存のハイパーバイザーソフトウェアを使用し、SQL Server Express editionも使用できるため、このソリューションはミラーリングよりも安価です。ただし、データベース用に新しいマシンが起動するのに時間がかかる場合があり、ユーザーへのサービスが中断される可能性があるため、自動フェイルオーバープロセスは遅くなります。

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

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

SQLクラスタリングまたはSQLミラーリングのインストールにおけるノードへのControllerのインストールはサポートされていません。

データベースソフトウェアのインストール

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

デフォルトのインストールでは、デフォルトのWindowsサービスアカウントと権限が使用されます。Windowsサービスアカウントをsysadminロールに追加することを含め、これらのデフォルトの詳細については、Microsoftのドキュメントを参照してください。この構成では、ControllerはNetwork Serviceアカウントを使用します。Controllerには、追加のSQL Serverロールまたは権限は必要ありません。

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

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

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

SQL Serverを最新の状態に保つには、Windows Updateを使用してください。

サイト作成ウィザードからデータベースをセットアップする

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

「**データベース**」ページには、データベースを設定するための2つのオプションがあります。自動設定とスクリプトを使用した設定です。通常、必要なデータベース権限（Web Studioユーザーおよびcitrix管理者）がある場合は、自動オプションを使用できます。（データベース設定に必要な権限を参照してください。）

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

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

1. SQL Server ソフトウェアを2台のサーバー (AとB) にインストールします。

2. サーバーAで、プリンシパルとして使用するデータベースを作成します。サーバーAのデータベースをバックアップし、サーバーBにコピーします。
3. サーバーBで、バックアップファイルを復元します。
4. サーバーAでミラーリングを開始します。

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

ミラーデータベース環境で後からデリバリーコントローラーを追加、移動、または削除する場合は、デリバリーコントローラーを参照してください。

自動セットアップ

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

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

スクリプトによるセットアップ

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

1. サイト作成ウィザードの**データベース**ページで、**手動でセットアップするためのスクリプトを生成する**を選択します。この操作により、サイト、監視、ログデータベースといった各データベースのプライマリおよびレプリカ用に、次の3種類のスクリプトが生成されます。
    - *名前に「SysAdmin」を含むスクリプト*。データベースとDelivery Controllerのログインを作成するスクリプトです。これらのタスクにはsecurityadmin権限が必要です。
    - *名前に「DbOwner」を含むスクリプト*。データベースにユーザーロールを作成し、ログインを追加し、データベーススキーマを作成するスクリプトです。これらのタスクには `db_owner` 権限が必要です。
    - *名前に「Mixed」を含むスクリプト*。必要な権限に関係なく、すべてのタスクを1つのスクリプトにまとめたものです。

スクリプトの保存場所を指定できます。

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

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

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

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

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

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

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

すべてのスクリプトが正常に完了すると、データベース管理者はCitrix管理者に3つの主要なデータベースアドレスを提供します。

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

データベースのセットアップに必要な権限

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

操作	目的	サーバーロール	データベースロール
データベースの作成	適切な空のデータベースを作成する	`dbcreator`	
スキーマの作成	すべてのサービス固有のスキーマを作成し、最初のControllerをサイトに追加する	`securityadmin` *	`db_owner`
コントローラーを追加	(最初のコントローラー以外の) コントローラーをサイトに追加	`securityadmin` *	`db_owner`
コントローラー (ミラーサーバー) を追加	ミラーデータベースのミラーロールにあるデータベースサーバーにコントローラーログインを追加	`securityadmin` *	
コントローラーを削除	サイトからコントローラーを削除	**	`db_owner`
スキーマを更新	スキーマの更新またはホットフィックスを適用		`db_owner`

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

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

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

優先データベース権限スクリプト

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

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

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

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

詳細については、コマンドレットのヘルプを参照してください。

データベースアドレスの形式

データベースアドレスは、次のいずれかの形式で指定できます。

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

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

データベースの場所を変更する

サイトを作成した後、構成ログデータベースと監視データベースの場所を変更できます。(サイトデータベースの場所は変更できません。)データベースの場所を変更する場合：

- 以前のデータベースのデータは、新しいデータベースにインポートされません。
- ログを取得する際に、両方のデータベースからログを集約することはできません。
- 新しいデータベースの最初のログエントリは、データベースの変更が発生したことを示しますが、以前のデータベースを特定するものではありません。

強制ログが有効になっている場合、構成ログデータベースの場所を変更することはできません。

データベースの場所を変更するには：

1. データベースを配置するサーバーに、サポートされているバージョンのMicrosoft SQL Serverがインストールされていることを確認します。必要に応じて、高可用性機能をセットアップします。
2. Web Studioにサインインし、左ペインで**「設定」**を選択します。
3. **「データベース」タイルを見つけて、「編集」**を選択します。
4. **「データベースの管理」ページで、新しい場所を指定するデータベースを選択し、アクションバーで「データベースの変更」**を選択します。
5. 新しい場所とデータベース名を指定します。
6. Web Studioにデータベースを作成させたい場合で、適切な権限がある場合は、**「完了」をクリックします。プロンプトが表示されたら「完了」**をクリックすると、Web Studioが自動的にデータベースを作成します。Web Studioは、ユーザーの資格情報を使用してデータベースへのアクセスを試行します。失敗した場合は、データベースユーザーの資格情報の入力を求められます。その後、Web Studioはデータベーススキーマをデータベースにアップロードします。資格情報は、データベース作成期間中のみ保持されます。
7. Web Studioにデータベースを作成させたくない場合、または十分な権限がない場合は、**データベーススクリプトの生成**をクリックします。生成されたスクリプトには、必要に応じてデータベースとミラーデータベースを手動で作成するための手順が含まれています。スキーマをアッ

プロードする前に、データベースが空であり、少なくとも1人のユーザーがデータベースにアクセスして変更する権限を持っていることを確認してください。

詳細情報

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

配信方法

Citrix Virtual Apps and Desktops™は、さまざまな配信方法を提供します。1つの配信方法だけでは、すべての要件を満たせない可能性があります。

はじめに

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

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

VDIデスクトップまたはエンドポイントデバイスからホスト型Windowsアプリにシームレスにアクセスでき、アプリがリモートで実行されているという事実を隠します。詳細については、「デリバリーグループの作成」を参照してください。

- **ローカルアプリ:** エンドポイントデバイスに展開されるアプリケーションです。アプリケーションはエンドポイントで実行されますが、そのインターフェイスはユーザーのホスト型VDIセッション内に表示されます。詳細については、「ローカルアプリアクセスとURLリダイレクト」を参照してください。

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

Citrix Virtual Apps™の公開アプリとデスクトップ

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

ユースケース:

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

利点と考慮事項:

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

ユーザーエクスペリエンス:

- ユーザーは、StoreFront™、**スタート**メニュー、または提供されたURLから1つ以上のアプリケーションを要求します。
- アプリケーションは仮想的に配信され、ユーザーデバイス上で高解像度でシームレスに表示されます。

- プロファイル設定に応じて、ユーザーのアプリケーションセッションが終了するとユーザーの変更が保存されます。そうでない場合、変更は削除されます。

アプリケーションの処理、ホスト、および配信:

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

セッション管理と割り当て:

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

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

VMホスト型アプリ

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

ユースケース:

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

利点と考慮事項:

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

ユーザーエクスペリエンス：

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

アプリケーションの処理、ホスト、および配信：

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

セッション管理と割り当て：

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

VDIデスクトップ

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

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

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

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

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

リモートPCアクセス

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

リモートPCアクセスは、仮想デスクトップとアプリケーションを提供するCitrix Virtual Apps and Desktopsと同じコンポーネントを使用します。その結果、リモートPCアクセスの展開と構成の要件およびプロセスは、仮想リソースを提供するためのCitrix Virtual Apps and Desktopsの展開に必要なものと同じです。この一貫性により、一貫性のある統合された管理エクスペリエンスが提供されます。ユーザーは、Citrix HDX™を使用してオフィスPCセッションを配信することで、最高のユーザーエクスペリエンスを得られます。

詳細については、リモートPCアクセス。

ネットワークポート

Communication Ports Used by Citrix Technologiesに、ネットワークポートの完全な情報が記載されています。

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

ポート情報が必要になる場合があります。

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

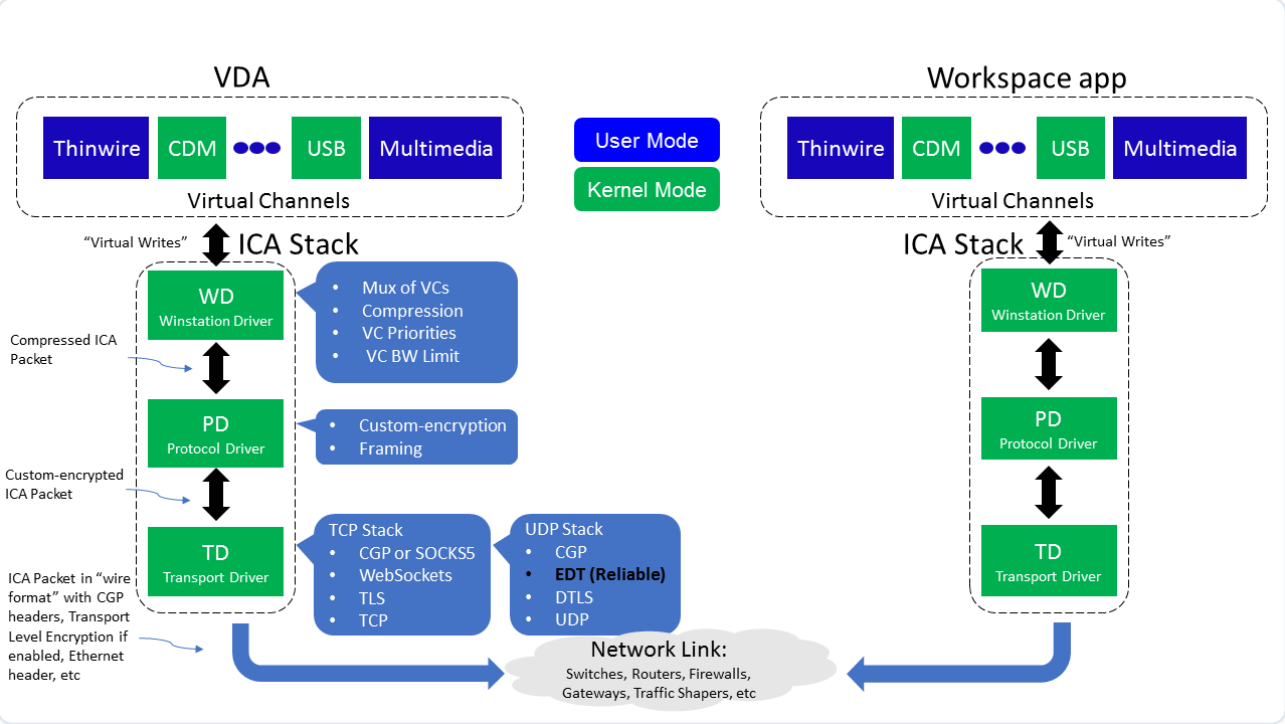
一部のポートは、Internet Assigned Numbers Authority (IANA) に登録されています。これらの割り当てに関する詳細は `<http://www.iana.org/assignments/port-numbers>` で確認できます。ただし、IANAが保持する説明情報は、必ずしも今日の使用状況を反映しているわけではありません。

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

HDX™

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

Citrix HDXは、あらゆるデバイスで、あらゆるネットワーク経由で、一元化されたアプリケーションおよびデスクトップのユーザーに高精細なエクスペリエンスを提供する幅広いテクノロジーの集合体です。

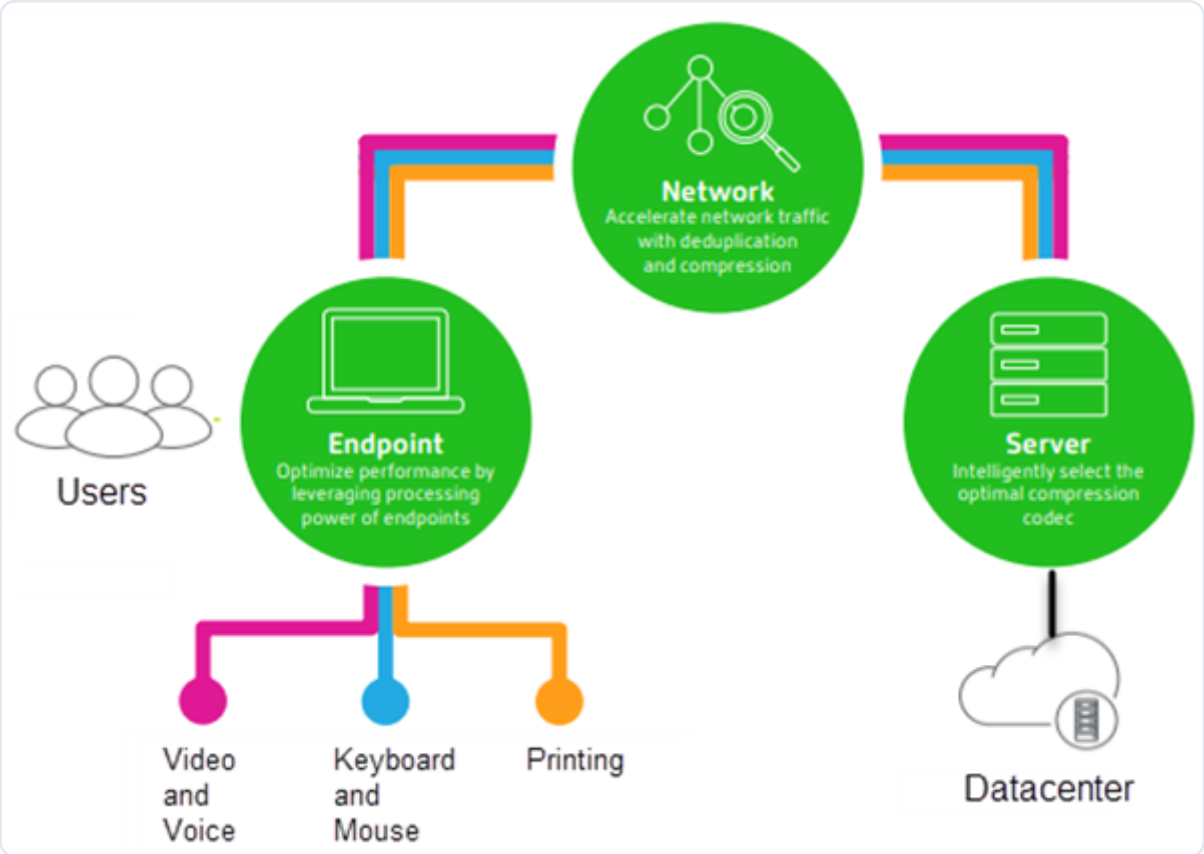


HDXは、次の3つの技術原則に基づいて設計されています。

- インテリジェントなリダイレクト
- 適応型圧縮
- データ重複排除

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

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



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

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

デバイス上での動作

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

ネットワーク上

HDXには、低帯域幅および高遅延のWAN接続を含むあらゆるネットワークで最高のパフォーマンスを提供するための高度な最適化および高速化機能が組み込まれています。

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

データセンター内

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

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

HDX インサイト

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

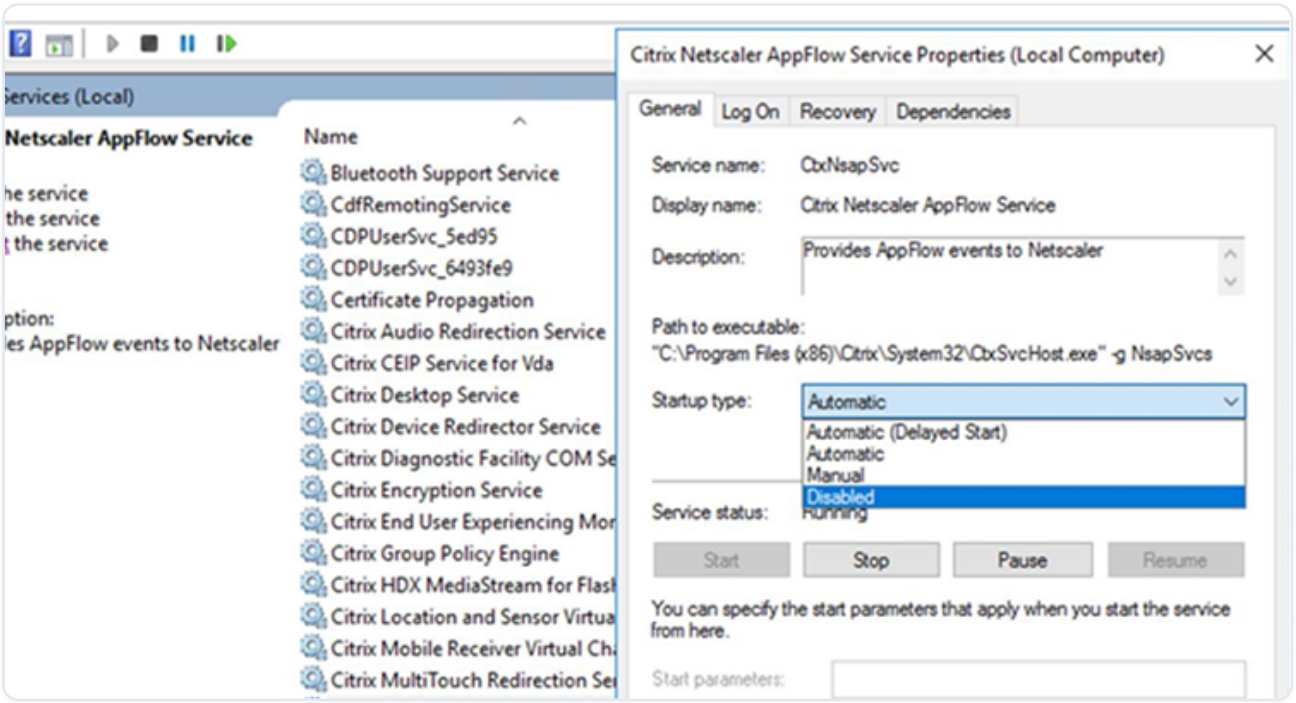
NetScalerを有効にしてHDX Insight仮想チャネルを使用すると、必要なすべてのデータポイントを非圧縮形式で移動できます。この機能を無効にすると、NetScalerデバイスは、さまざまな仮想チャネルに分散されたICA®トラフィックを復号化および解凍します。単一の仮想チャネルを使用すると、複雑さが軽減され、スケーラビリティが向上し、費用対効果が高まります。

最小要件:

- NetScalerバージョン12.0 Build 57.x
- Citrix Workspace™ アプリ Windows 1808 向け
- Citrix レシーバー for Windows 4.10
- Mac用Citrix Workspaceアプリ 1808
- Mac用シトリックス レシーバー 12.8

HDX Insight仮想チャネルの有効化または無効化

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



仮想デスクトップからHDX機能を利用する

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

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

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

- HDXが高品位オーディオをどのように配信するかを確認するには：

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

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

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

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

知っておくと良いこと:

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

自動クライアント再接続とセッションの信頼性

ホストされたアプリケーションやデスクトップにアクセスする際、ネットワークの中断が発生する可能性があります。よりスムーズな再接続を体験していただくために、自動クライアント再接続とセッションの信頼性を提供しています。デフォルト設定では、セッションの信頼性が開始され、その後自動クライアント再接続が続きます。

自動クライアント再接続:

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

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

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

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

自動クライアント再接続のデフォルト設定：

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

詳細については、自動クライアント再接続ポリシー設定を参照してください。

セッションの信頼性:

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

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

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

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

デフォルトのセッションの信頼性設定

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

詳細については、「セッションの信頼性ポリシー設定」を参照してください。

NetScalerと自動クライアント再接続およびセッションの信頼性:

サーバーでマルチストリームポリシーとマルチポートポリシーが有効になっており、以下の条件のいずれかまたはすべてが当てはまる場合、自動クライアント再接続は機能しません。

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

HDXアダプティブスループット

HDXアダプティブスループットは、出力バッファーを調整することで、ICAセッションのピークスループットをインテリジェントに微調整します。出力バッファーの数は、初期値として高い値に設定されます。この高い値により、特に高遅延ネットワークにおいて、データがより迅速かつ効率的にクライアントに送信されます。これにより、インタラクティブ性の向上、ファイル転送の高速化、ビデオ再生のスムーズ化、フレームレートと解像度の向上を実現し、ユーザーエクスペリエンスが強化されます。

ICAセッション内のデータストリームがインタラクティブ性に悪影響を与えていないか、セッションのインタラクティブ性が常に測定されます。そのような状況が発生した場合、セッションに対する大量のデータストリームの影響を軽減し、インタラクティブ性を回復させるためにスループットが低下します。

重要:

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

この機能には、次の要件があります。

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

ユーザーデバイスに送信される画質の向上

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

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

注:

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

ビデオ会議のパフォーマンスを向上させる

いくつかの一般的なビデオ会議アプリケーションは、マルチメディアリダイレクトを介したCitrix Virtual Apps and Desktopsからの配信向けに最適化されています（例: HDX RealTime Optimization Packを参照）。最適化されていないアプリケーションの場合、HDXウェブカメラビデオ圧縮は、

セッション中のビデオ会議におけるウェブカメラの帯域幅効率と遅延耐性を向上させます。このテクノロジーは、専用のマルチメディア仮想チャネルを介してウェブカメラトラフィックをストリーミングします。このテクノロジーは、アイソクロナスなHDX Plug-n-Play USBリダイレクトサポートと比較して帯域幅の使用量が少なく、WAN接続でもうまく機能します。

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

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

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

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

ネットワークトラフィックの優先順位

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

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

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

Windows 10、Windows 8、Windows 7マシンにインストールされているVirtual Delivery Agent（VDA）では、マルチチャネルストリーミング接続がサポートされています。ネットワーク管理

者に協力して、**マルチポートポリシー**設定で構成されているCommon Gateway Protocol（CGP）ポートがネットワークルーターに正しく割り当てられていることを確認してください。

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

警告:

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

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

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

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

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

リモート言語バーの表示/非表示

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

VDAから言語バー機能のクライアント制御を無効にするには：

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

Unicodeキーボードマッピング

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

Unicodeキーボードレイアウトマッピングの有効化または無効化

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

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名前: EnableKlMap

種類: DWORD

値: 1

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

Unicode キーボードレイアウトマッピング互換モードを有効にする

デフォルトでは、Unicode キーボードレイアウトマッピングは、サーバー側でキーボードレイアウトを変更したときに、新しい Unicode キーボードレイアウトマップを再ロードするために一部の Windows API を自動的にフックします。一部のアプリケーションはフックできません。互換性を維持するために、この機能を互換モードに変更して、これらのフックできないアプリケーションをサポートできます。次のレジストリキーを追加します。

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名前: DisableWindowHook

種類: DWORD

値: 1

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

Citrix ICA® 仮想チャネル

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

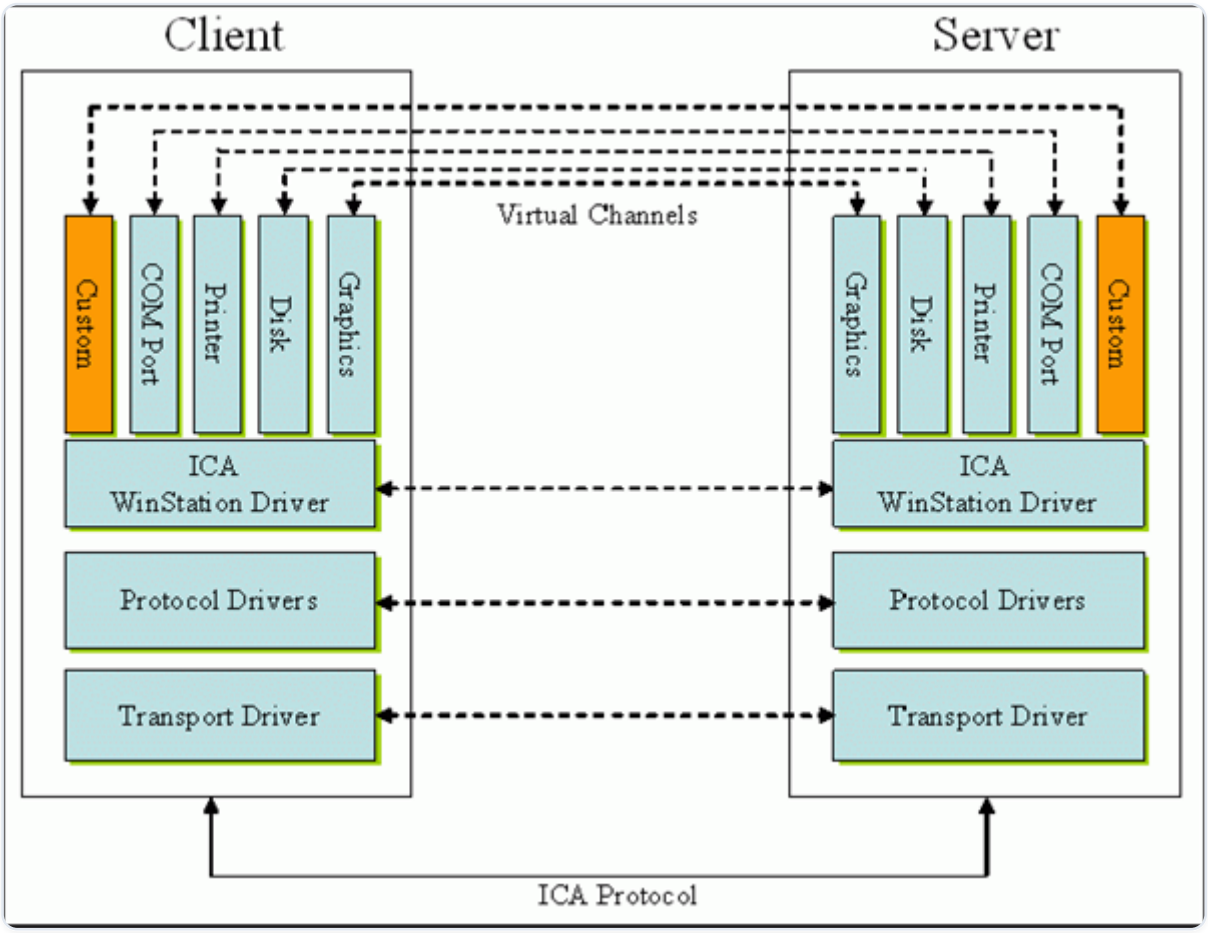
ICA仮想チャネルとは?

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

- オーディオ
- COMポート
- ディスク

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

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



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

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

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

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

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

または

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

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

> **注:**

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

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

- vd3dn.dll – デスクトップコンポジションリダイレクトに使用されるDirect3D仮想チャネル
- vdcamN.dll – 双方向オーディオ
- vdcdm30n.dll – クライアントドライブマッピング
- vdcom30N.dll - クライアントCOMポートマッピング
- vdcpm30N.dll – クライアントプリンターマッピング
- vdctln.dll – ICAコントロールチャネル
- vddvc0n.dll – 動的仮想チャネル
- vdeuemn.dll - エンドユーザーエクスペリエンス監視
- vdgusbn.dll – 汎用USB仮想チャネル
- vdkbhook.dll – 透明キーパススルー
- vdlfpn.dll – UDPライクなトランスポートを介したFramehawkディスプレイチャネル
- vdmmn.dll – マルチメディアサポート
- vdmrvc.dll – モバイルReceiver仮想チャネル
- vdmtchn.dll - マルチタッチサポート
- vdscardn.dll – スマートカードサポート
- vdsens.dll – センサー仮想チャネル
- vdspl30n.dll – クライアントUPD
- vdsspin.dll – ケルベロス
- vdtuin.dll – 透明UI
- vdtw30n.dll – クライアント Thinwire
- vdtwin.dll – シームレス
- vdtwn.dll – トゥエイン

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

64ビット互換性

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

- brapi64.dll
- confmgr.dll
- ctxlogging.dll
- ctxmui.dll
- icaconf.exe
- icaconfs.dll
- icafile.dll
- pnipcn64.dll
- pnsson.dll
- ssoncom.exe
- ssonstub.dll
- vdkbhook64.dll

汎用USB仮想チャネル

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

- ctxusbm.sys
- ctxusbr.sys

ICA仮想チャネルの仕組み

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

シェルによってロードされる仮想チャネルモジュール（例）：

- EUEM

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

一部はカーネルモードとしてロードされます。例:

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

サーバー側のグラフィック仮想チャネル

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

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

Windowsサービスでの特殊チャネルのホスティング

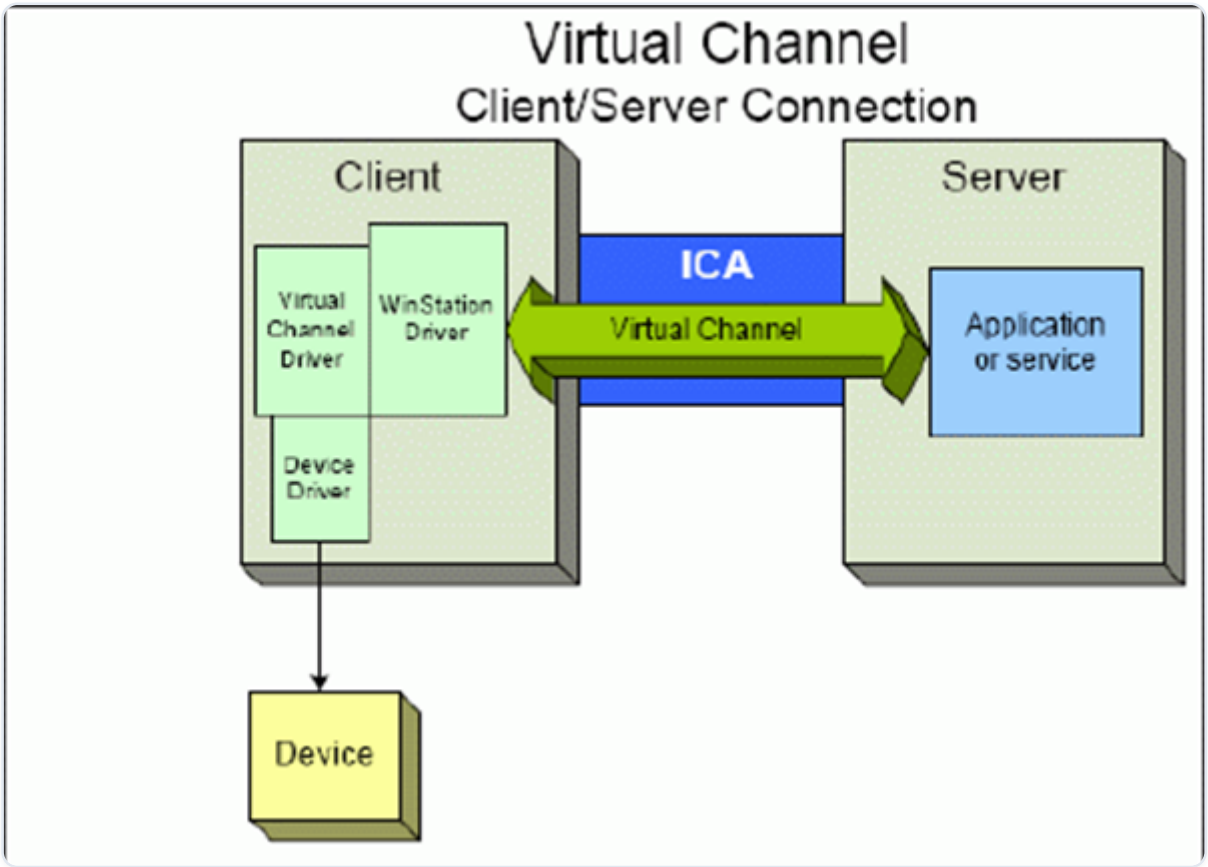
Citrix Virtual Apps and Desktops サーバーでは、さまざまなチャネルが Windows サービスとしてホストされます。このようなホスティングは、セッション内の複数のアプリケーションとサーバー上の複数のセッションに対して、1対多のセマンティクスを提供します。このようなサービスの例は次のとおりです。

- Citrix デバイスリダイレクターサービス
- Citrix ダイナミック仮想チャネルサービス
- Citrix エンドユーザーエクスペリエンス監視サービス
- Citrix ロケーションおよびセンサー仮想チャネルサービス
- Citrix マルチタッチリダイレクトサービス
- Citrix 印刷マネージャーサービス

- Citrix スマートカードサービス
- Citrix オーディオリダイレクトサービス (Citrix Virtual Desktops™ のみ)
- Citrix ICA ステータスチャネルサービス

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

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



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

1. クライアントはCitrix Virtual Apps and Desktopsサーバーに接続します。クライアントは、サポートする仮想チャネルに関する情報をサーバーに渡します。
2. サーバー側アプリケーションが起動し、仮想チャネルへのハンドルを取得し、オプションでチャネルに関する追加情報を照会します。
3. クライアント仮想ドライバーとサーバー側アプリケーションは、次の2つの方法を使用してデータを渡します。

- サーバーアプリケーションがクライアントに送信するデータを持っている場合、そのデータはすぐにクライアントに送信されます。クライアントがデータを受信すると、WinStationドライバーはICAストリームから仮想チャネルデータを逆多重化し、すぐにクライアント仮想ドライバーに渡します。
- クライアント仮想ドライバーがサーバーに送信するデータを持っている場合、そのデータはWinStationドライバーが次にポーリングするときに送信されます。サーバーがデータを受信すると、仮想チャネルアプリケーションがそれを読み取るまでキューに入れられます。データが受信されたことをサーバー仮想チャネルアプリケーションに通知する方法はありません。

4. サーバー仮想チャネルアプリケーションが完了すると、仮想チャネルを閉じ、割り当てられたリソースを解放します。

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

注:

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

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

注:

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

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

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

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

仮想チャネルのパススルー機能

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

次の機能は、シングルホップまたはマルチホップで同じように動作します。

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

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

- 双方向オーディオ

- ファイル転送
- 汎用USBリダイレクト
- シームレス
- シンワイヤー

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

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

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

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

以下の従来の仮想チャネルとその機能がサポートされています。

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

セキュリティとICA仮想チャネル

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

ベストプラクティス

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

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

仮想チャネルの命名:

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

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

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

ダブルホップサポート:

仮想チャネル	ダブルホップはサポートされていますか？
オーディオ	いいえ
ブラウザコンテンツリダイレクション	いいえ
CDM	はい
CEIP	いいえ
クリップボード	はい

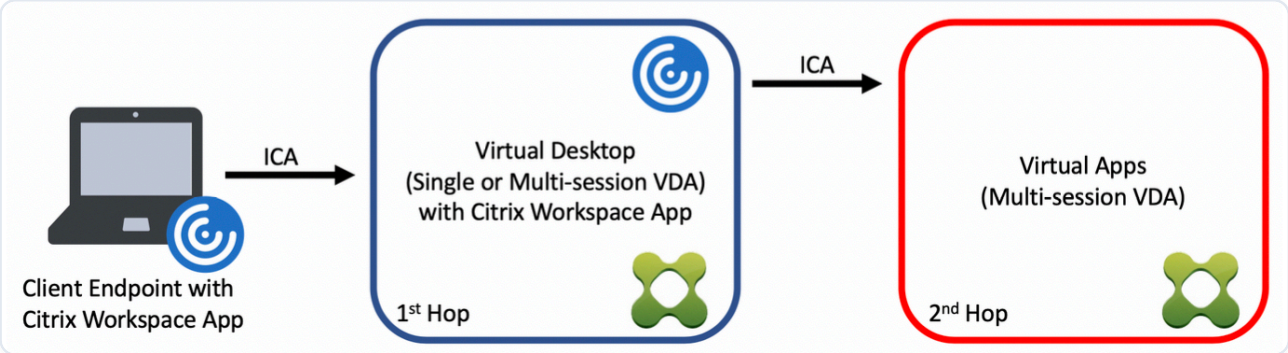
仮想チャネル	ダブルホップはサポートされていますか？
コンティニュアム (MRVC)	いいえ
コントロール VC	はい
HTML5ビデオのリダイレクト (v1)	はい
キーボード、マウス	はい
マルチタッチ	いいえ
NSAPVC	いいえ
印刷	はい
SensVC	いいえ
スマートカード	はい
ツイン	はい
USB VC	はい
WAYCOM デバイス - K2M (USB VC を使用)	はい
Webカメラビデオ圧縮	はい
Windows Mediaリダイレクト	はい

参照

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

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

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



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

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

システム要件

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

最初のホップでは、シングルセッションまたはマルチセッションOS VDAとCitrix Workspaceアプリのサポートされているバージョンを使用する必要があります。2番目のホップでは、マルチセッションOS VDAのサポートされているバージョンを使用する必要があります。サポートされているバージョンについては、製品マトリックスページを参照してください。

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

最初のホップが、Citrix Virtual Appsセッションと組み合わされたサードパーティ製（Citrix以外）の仮想デスクトップソリューションを含む環境では、サポートはCitrix Virtual Apps環境に限定されます。サードパーティ製仮想デスクトップに関連する問題（Citrix Workspace™アプリの互換性、ハードウェアデバイスのリダイレクト、セッションパフォーマンスなどを含むがこれらに限

定されない）が発生した場合、Citrixは限定的な範囲で技術サポートを提供できます。トラブルシューティングの一環として、最初のホップにCitrix Virtual Desktopが必要になる場合があります。

HDX™のダブルホップにおける展開に関する考慮事項

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

グラフィック

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

レイテンシー

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

マルチメディア

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

USBデバイスリダイレクト

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

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

注:

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

サポートの例外

ダブルホップセッションは、以下のものを除き、ほとんどのHDX機能と能力をサポートします。

- ブラウザコンテンツリダイレクト
- ローカルアプリアクセス
- Skype for Business 用 リアルタイム オプティマイゼーション パック
- Microsoft Teamsの最適化

インストールと構成

展開を開始する前に、参照されている記事を確認し、展開中に表示される内容や指定する内容について学習してください。

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

準備

インストールの準備 を確認し、必要なタスクを完了してください。

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

コアコンポーネントのインストール

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

サイトの作成

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

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

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

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

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

オプションコンポーネントのインストール

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

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

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

必要に応じて、追加のCitrixコンポーネントをCitrix Virtual Apps and Desktops展開に統合します。

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

マシンカタログを作成する

Studioでサイトを作成した後、マシンカタログの作成に誘導されます。

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

デリバリーグループを作成する

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

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

アプリケーショングループの作成（オプション）

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

既知の制限

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

マシンID

各マシンは、コンピューターアカウントとも呼ばれる一意のマシンIDを持つ必要があります。マシンIDは、マシン上でローカルに、またはオンプレミスのActive Directory (AD) やAzure ADなどのディレクトリで作成および管理できます。Citrix®は、Active Directoryに参加済み、Azure Active Directoryに参加済み、ハイブリッドAzure Active Directoryに参加済み、またはドメインに参加していないマシンでの仮想アプリケーションおよびデスクトップのホスティングをサポートしています。

マシンIDの種類

以下のマシンIDの種類がサポートされています。

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

マシンIDの種類	説明
	期されます。プロビジョニングされたマシンはオンプレミスのActive Directoryに参加します。その後、マシンはハイブリッドAzure ADに参加します。ハイブリッドAzure AD参加済みVMをインポートする場合、Citrix Virtual Apps and Desktopsでは、そのVMはActive Directory参加済みVMとして扱われます。
ドメイン非参加	IDはマシン上でローカルに作成および管理されます。Citrix Virtual Apps and DesktopsへのVMのインポートはサポートされていません。

サポートされる構成

以下は、各シナリオでサポートされる構成の詳細です。

サポートされるインフラストラクチャ

マシンID	シトリックス バーチャルアプリとデスクトップ™	シトリックス ワークスペース™	シトリックス ストアフロント	シトリックス ゲートウェイ サービス	CITRIX GATEWAY (シトリックス ゲートウェイ)
AD参加済み	はい	はい	はい	はい	はい
Azure AD参加済み	いいえ	はい	いいえ	はい	いいえ
ハイブリッド Azure AD 参加済み	はい	はい	はい	はい	はい
ドメイン非参加	はい	はい	いいえ	はい	いいえ

サポートされているワークスペース認証IDプロバイダー

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

Active Directory 参加済み

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

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

この製品は以下をサポートします。

- **ユーザーアカウントとコンピューターアカウントが単一のActive Directoryフォレスト内のドメインに存在する展開。** ユーザーアカウントとコンピューターアカウントは、単一フォレスト

内の任意のドメインに存在できます。この種類の展開では、すべてのドメイン機能レベルとフォレスト機能レベルがサポートされます。

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

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

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

複数のActive Directoryフォレスト環境での展開

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

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

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

> **注意:**

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

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

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

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

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

DNS名前空間がActive Directoryのものと異なる場合、逆引きDNS構成が必要になることがあります。

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

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

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

このレジストリキーは、双方向の信頼関係にある複数フォレスト環境でDDCルックアップを実行し、初期登録プロセス中にNTLMベースの認証を削除できるようにします。

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

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

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

外部信頼が設定されている場合は、VDAで次の変更を行います。

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

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

次の表に、サポートされている信頼の種類を示します。

信頼の種類	推移性	方向	このリリースでサポートされています
親と子	推移的	双方向	はい

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

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

ハイブリッド Azure Active Directory 参加済み

注:

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

この記事では、システム要件のセクションで概説されている要件に加えて、ハイブリッド Azure Active Directory (HAAD) 参加済みカタログを作成するための要件について説明します。

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

注:

ハイブリッド Azure AD 参加済み VM は、フェデレーションおよびマネージド ID インフラストラクチャの両方でサポートされています。

要件

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

制限事項

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

考慮事項

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

  a. `gpedit.msc` を実行します。

  b. **コンピューターの構成 > 管理用テンプレート > Windows コンポーネント > デバイス登録** に移動します。

  c. **ドメイン参加済みコンピューターをデバイスとして登録する**を**無効**に設定します。

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

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

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

$MaxCount = 60



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

{

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

  {

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

    if ($provider -eq 'Citrix')

    {

        break;

    }



    if ($provider -eq 1)

    {

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

```
-Value "Citrix" -Force

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

        Start-Sleep 5

        dsregcmd /join

        break

    }

  }



  Start-Sleep 1

}
```

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

次のステップ

ハイブリッドAzure Active Directory参加済みカタログの作成に関する詳細については、ハイブリッドAzure Active Directory参加済みカタログの作成を参照してください。

ドメイン非参加

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

要件

- コントロールプレーン: サポートされる構成を参照
- VDAの種類: シングルセッション（デスクトップのみ）またはマルチセッション（アプリとデスクトップ）
- VDAバージョン: 2311以降
- プロビジョニングの種類: Machine Creation Services™ (MCS)、永続および非永続

- 割り当ての種類: 専用およびプール
- ホスティングプラットフォーム: MCSでサポートされているすべてのプラットフォーム
- Rendezvous V2を有効にする必要があります

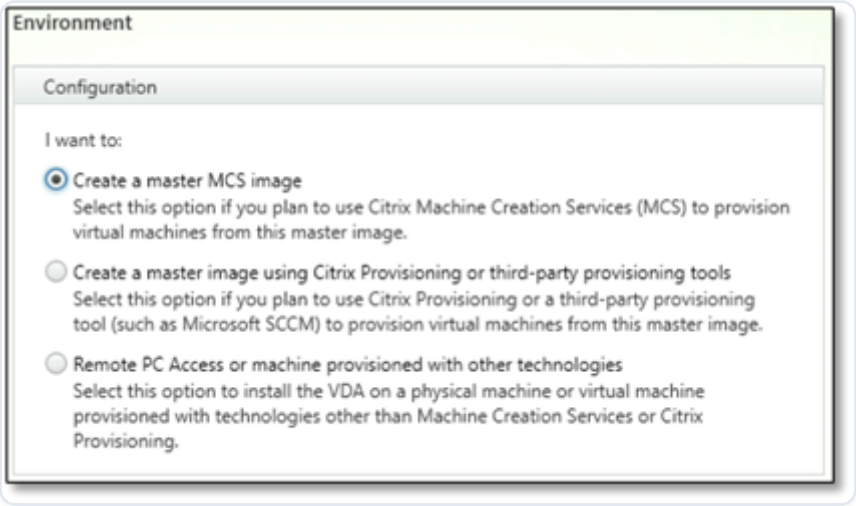
制限事項

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

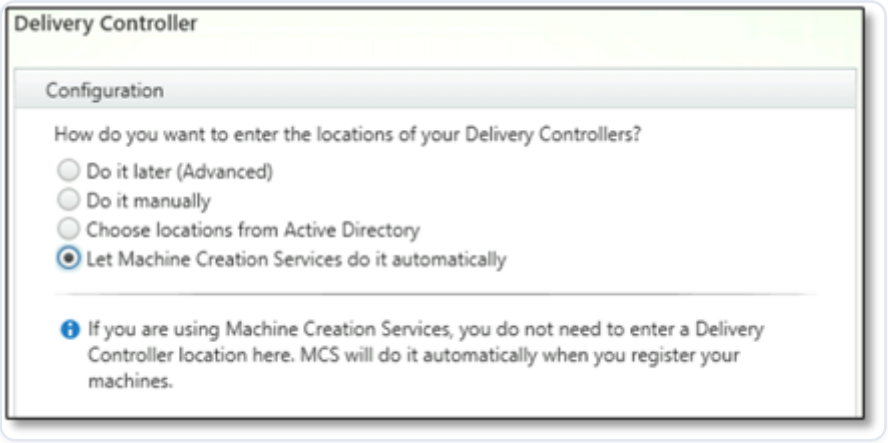
VDAのインストールと構成

VDAをインストールする手順は次のとおりです。

1. インストールウィザードで以下のオプションを選択していることを確認してください。
    - 環境ページで、**マスターMCSイメージを作成**を選択します。



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



次のステップ

リソースの場所とホスティング接続が利用可能になったら、マシンカタログの作成に進みます。ドメインに参加していないマシンカタログの作成の詳細については、ドメインに参加していないカタログの作成を参照してください。

インストール準備

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

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

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

注:

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

- Microsoft **Volume Shadow Copy** および **Microsoft Software Shadow Copy Provider** サービスが実行されていること。詳細については、「Volume Shadow Copy Service」を参照してください。
- **MS-Defender** のバージョンは4.18.2105.5より高い必要があります。詳細については、「Microsoft Defender Antivirus security intelligence and product updates」を参照してください。

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

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

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

インストール前に確認する情報

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

コンポーネントのインストール場所

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

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

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

  他のサーバーに他のコンポーネントをインストールする前に、Citrix License Serverとライセンスをインストールしてください。
- Server CoreOS (Delivery Controllerなど) にサポートされているコンポーネントをインストールするには、(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/install-command.html)コマンドラインを使用する必要があります。このOSタイプにはグラフィカルインターフェイスがないため、Studioやその他のツールは別の場所にインストールし、それらをControllerサーバーにポイントしてください。

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

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

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

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

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

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

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

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

コンポーネントをインストールしてはならない場所:

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

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

権限とActive Directoryの要件

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

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

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

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

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

詳細については、以下を参照してください。

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

インストールのガイダンス、考慮事項、およびベストプラクティス

コンポーネントのインストール中

- フルプロダクトメディアからDelivery Controller、Studio、License Server、またはDirectorをインストールまたはアップグレードする際に、Citrixインストーラーが以前のWindowsインストールによる再起動が保留中であることを検出すると、インストーラーは終了/リターンコード9で停止します。マシンの再起動を促すメッセージが表示されます。

  これはCitrixによって強制される再起動ではありません。以前にマシンにインストールされた他のコンポーネントが原因です。この問題が発生した場合は、マシンを再起動してから、Citrixインストーラーを再度起動してください。

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

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

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

VDAのインストール中

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

  制限を承諾するか、Media Foundationのインストール後にVDAのインストールを終了して後で再開することができます。グラフィカルインターフェイスでは、この選択肢はメッセージで表示されます。コマンドラインでは、`/no_mediafoundation_ack` オプションを使用して制限を承諾できます。
- VDAをインストールすると、**Direct Access Users**という新しいローカルユーザーグループが自動的に作成されます。シングルセッションOS用VDAでは、このグループはRDP接続にのみ

適用されます。マルチセッションOS用VDAでは、このグループはICA®およびRDP接続に適用されます。

- VDAは、通信するための有効なControllerアドレスを持っている必要があります。そうでない場合、セッションを確立できません。ControllerアドレスはVDAのインストール時または後で指定できます。これは必ず行う必要があります。詳細については、VDA登録を参照してください。

VDAインストール後およびインストール中の再起動

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

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

VDAインストール中に必要な再起動の回数を最小限に抑えるには：

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

VDAをインストールする前にこれらの前提条件をインストールしない場合：

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

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

インストールまたはアップグレードの失敗時の復元

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

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

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

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

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

この機能は、デフォルトで無効になっています。

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

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

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

- VDAインストーラーのグラフィカルインターフェイスを使用する場合（**Autostart** または復元オプションやサイレントオプションなしで `XenDesktopVDASetup.exe` コマンドを使用する

場合など）は、**Summary** ページで **Enable automatic restore if update fails** チェックボックスをオンにします。

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

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

インストーラー

フルプロダクトインストーラー

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

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

> **注:**
>
> Workspace Environment Management™ Agentインストーラーはローカライズされていません。英語のみで提供されます。

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

スタンドアロン VDA インストーラー

スタンドアロンVDAインストーラーは、Citrixダウンロードページで入手できます。（製品のインストールメディアからは入手できません。）スタンドアロンVDAインストーラーは、フルプロダクトISOよりもはるかに小さく、次のような展開に容易に対応できます。

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

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

ダウンロード可能なスタンドアロンVDAインストーラーは3つあります。

VDAServerSetup.exe:

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

VDAWorkstationSetup.exe:

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

VDAWorkstationCoreSetup.exe:

Remote PC Access展開またはコアVDIインストール用に最適化されたシングルセッションOS用のVDAをインストールします。Remote PC Accessは物理マシンを使用します。コアVDIインストールは、イメージとして使用されていないVMです。このような展開に必要なVDA接続のコアサービスのみをインストールします。したがって、フルプロダクトインストーラーまたは`VDAWorkstationSetup.exe`インストーラーで有効なオプションのサブセットのみをサポートします。

このインストーラーは、以下の目的で使用されるコンポーネントをインストールまたは含みません。

- アップブイ。
- Profile Management。Citrix Profile Managementをインストールから除外すると、Citrix Directorの表示に影響します。詳細については、「VDAのインストール」を参照してください。
- マシンIDサービス。
- Citrixサポートツール。
- Windows 用 Citrix ファイル。
- アウトルック用シトリックス ファイルズ。

`VDAWorkstationCoreSetup.exe`インストーラーは、Windows向けCitrix Workspaceアプリをインストールまたは含んでいません。

`VDAWorkstationCoreSetup.exe`を使用することは、フルプロダクトまたは`VDAWorkstationSetup`インストーラーを使用してシングルセッションOS VDAをインストールすることと同等であり、以下のいずれかの方法でインストールします。

- グラフィカルインターフェイスで、 ページでRemote PC Accessオプションを選択します。
- コマンドラインインターフェイスで: `/remotepc` オプションを指定する。
- コマンドラインインターフェイスで: `/components vda` と、有効な追加コンポーネント名をすべてリストする `/exclude` オプションを指定する。

省略されたコンポーネント/機能は、後でフルプロダクトインストーラーを実行してインストールできます。この操作により、不足しているすべてのコンポーネントをインストールできます。

`VDAWorkstationCoreSetup.exe` インストーラーは、Browser Content Redirection MSI を自動的にインストールします。この自動インストールは、VDA リリース 2003 以降のサポート対象リリースに適用されます。

Citrix インストールリターンコード

インストールログには、コンポーネントインストールの結果が Microsoft の値ではなく、Citrix のリターンコードとして含まれています。

- 0 = 成功
- 1 = 失敗
- 2 = 部分的な成功

- 3 = 部分的な成功と再起動が必要
- 4 = 失敗と再起動が必要
- 5 = ユーザーによってキャンセルされました
- 6 = 不正なコマンドライン引数
- 7 = 新しいバージョンが見つかりました
- 8 = 成功と再起動が必要
- 9 = ファイルロック再起動
- 10 = 中止
- 11 = メディア失敗
- 12 = ライセンス失敗
- 13 = 事前チェック失敗
- 14 = 再起動保留チェック中止

例えば、Microsoft System Center Configuration Managerなどのツールを使用する場合、インストールログにリターンコード3が含まれていると、スクリプトによるVDAインストールが失敗したように見えることがあります。これは、VDAインストーラーがユーザーが開始する必要のある再起動を待機している場合に発生する可能性があります (例えば、サーバーへのRDSロールの前提条件のインストール後など)。VDAインストールは、すべての前提条件と選択されたコンポーネントがインストールされ、インストール後にマシンが再起動されて初めて成功と見なされます。

あるいは、インストールをCMDスクリプト（Microsoftの終了コードを返す）でラップするか、Configuration Managerパッケージの成功コードを変更することもできます。

Windows Serverワークロード向けにMicrosoft RDSライセンスサーバーを構成する

この製品は、Windows 2016などのWindows Serverワークロードを提供するときに、Windows Serverのリモートセッション機能にアクセスします。これには通常、リモートデスクトップサービス クライアントアクセスライセンス (RDS CAL) が必要です。VDAは、RDS CALを要求するためにRDSライセンスサーバーに接続できる必要があります。ライセンスサーバーをインストールしてアクティブ化します。詳細については、Microsoftドキュメント「リモートデスクトップサービスライセンスサーバーをアクティブ化する」を参照してください。概念実証環境では、Microsoftが提供する猶予期間を使用できます。

この方法を使用すると、このサービスにライセンスサーバー設定を適用させることができます。イメージ上のRDSコンソールで、ライセンスサーバーとユーザーごとのモードを構成できます。Microsoftグループポリシー設定を使用してライセンスサーバーを構成することもできます。詳細に

ついては、Microsoftドキュメント「クライアントアクセスライセンス (CAL) を使用してRDS展開をライセンスする」を参照してください。

グループポリシー設定を使用してRDSライセンスサーバーを構成するには:

1. 利用可能なマシンにリモートデスクトップサービスライセンスサーバーをインストールします。そのマシンは常に利用可能である必要があります。Citrix製品のワークロードは、このライセンスサーバーに到達できる必要があります。
2. Microsoftグループポリシーを使用して、ライセンスサーバーのアドレスとユーザーごとのライセンスモードを指定します。詳細については、Microsoftドキュメント「RDセッションホストサーバーのリモートデスクトップライセンスモードを指定する」を参照してください。

Windows 10ワークロードには、適切なWindows 10ライセンスのアクティベーションが必要です。Windows 10ワークロードをアクティブ化するには、Microsoftのドキュメントに従うことをお勧めします。

詳細情報

特定のホストタイプのリソースロケーションを設定する場合：

- AWSクラウド環境
- XenServer仮想化環境
- Google Cloud環境
- Microsoft Azure Resource Managerクラウド環境
- マイクロソフト システム センター コンフィギュレーション マネージャー 環境
- マイクロソフト システム センター バーチャル マシン マネージャー 仮想化環境
- Nutanix 仮想化環境(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/install-prepare/nutanix.html)
- Nutanix クラウドおよびパートナーソリューション(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/install-prepare/nutanix-cloud-patrner-solutions.html)
- VMware 仮想化環境(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/install-prepare/vmware.html)
- VMware クラウドおよびパートナーソリューション(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/install-prepare/vmware-cloud-partner-solutions.html)

AWSクラウド環境

この記事では、Citrix Virtual Apps and Desktops で使用できるリソースの場所として AWS アカウントを設定する手順を説明します。このリソースの場所には、概念実証や、複数のアベイラビリティゾーンにリソースを分散させる必要のないその他の展開に最適な、基本的なコンポーネントセットが含まれています。これらのタスクを完了すると、VDA のインストール、マシンのプロビジョニング、マシンカタログの作成、およびデリバリーグループの作成を行うことができます。

この記事のタスクを完了すると、リソースロケーションには次のコンポーネントが含まれます。

- 単一のアベイラビリティゾーン内にパブリックサブネットとプライベートサブネットを持つ仮想プライベートクラウド (VPC)。
- VPC のプライベートサブネットに配置され、Active Directory ドメインコントローラーと DNS サーバーの両方として実行されるインスタンス。
- VPC のパブリックサブネットで踏み台ホストとして機能するインスタンス。このインスタンスは、管理目的でプライベートサブネット内のインスタンスへの RDP 接続を開始するために使用されます。リソースの場所の設定が完了したら、このインスタンスをシャットダウンして、簡単にアクセスできないようにすることができます。VDA インスタンスなど、プライベートサブネット内の他のインスタンスを管理する必要がある場合は、踏み台ホストインスタンスを再起動できます。

タスクの概要

パブリックサブネットとプライベートサブネットを持つ仮想プライベートクラウド (VPC) をセットアップします。このタスクを完了すると、AWS はパブリックサブネットに Elastic IP アドレスを持つ NAT ゲートウェイを展開します。このアクションにより、プライベートサブネット内のインスタンスがインターネットにアクセスできるようになります。パブリックサブネット内のインスタンスは受信パブリックトラフィックにアクセスできますが、プライベートサブネット内のインスタンスはアクセスできません。

セキュリティグループを構成します。セキュリティグループは、VPC 内のインスタンスのトラフィックを制御する仮想ファイアウォールとして機能します。パブリックサブネット内のインスタンスがプライベートサブネット内のインスタンスと通信できるようにするルールをセキュリティグループに追加します。また、これらのセキュリティグループを VPC 内の各インスタンスに関連付けます。

DHCP オプションセットを作成します。Amazon VPC では、DHCP および DNS サービスがデフォルトで提供されるため、Active Directory ドメインコントローラーで DNS を構成する方法に影響します。Amazon の DHCP は無効にできず、Amazon の DNS はパブリック DNS 解決にのみ使用でき、Active Directory 名解決には使用できません。DHCP を介してインスタンスに渡される

ドメインとネームサーバーを指定するには、DHCP オプションセットを作成します。このセットは、Active Directory ドメインサフィックスを割り当て、VPC 内のすべてのインスタンスの DNS サーバーを指定します。インスタンスがドメインに参加したときにホスト (A) および逆引き (PTR) レコードが自動的に登録されるようにするには、プライベートサブネットに追加する各インスタンスのネットワークアダプタープロパティを構成します。

踏み台ホストとドメインコントローラーを VPC に追加します。踏み台ホストを介して、プライベートサブネット内のインスタンスにログオンし、ドメインを設定してインスタンスをドメインに参加させることができます。

タスク1：VPCをセットアップする

1. AWS マネジメントコンソールから、 を選択します。
2. VPC ダッシュボードから、 を選択します。
3. を選択します。
4. NATゲートウェイ ($) で、「**1 AZ内**」または「**AZごとに1つ**」を選択します。
5. DNSオプションで、「**DNSホスト名を有効にする**」を選択したままにします。
6. 「**VPCを作成**」を選択します。AWSは、パブリックサブネットとプライベートサブネット、インターネットゲートウェイ、ルートテーブル、およびデフォルトのセキュリティグループを作成します。

タスク 2: セキュリティグループの構成

このタスクでは、VPC 用に次のセキュリティグループを作成および構成します:

- パブリックサブネット内のインスタンスに関連付けるためのパブリックセキュリティグループ。
- プライベートサブネット内のインスタンスに関連付けるためのプライベートセキュリティグループ。

セキュリティグループを作成するには:

1. VPC ダッシュボードで、「**Security Groups**」を選択します。
2. パブリックセキュリティグループ用のセキュリティグループを作成します。「**Create Security Group**」を選択し、グループの名前タグと説明を入力します。VPC で、以前に作成した VPC を選択します。「**Yes, Create**」を選択します。

パブリックセキュリティグループの構成

1. セキュリティグループのリストから、パブリックセキュリティグループを選択します。

2. **［Inbound Rules］タブを選択し、［Edit］**を選択して、次のルールを作成します。

タイプ	送信元
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	パブリックセキュリティグループを選択します。
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (セッションの信頼性)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. 完了したら、**保存**を選択します。
4. **アウトバウンドルール**タブを選択し、**編集**を選択して、次のルールを作成します。

タイプ	宛先
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	0.0.0.0/0
ICMP	0.0.0.0/0

5. 完了したら、**保存**を選択します。

プライベートセキュリティグループを構成する

1. セキュリティグループリストから、プライベートセキュリティグループを選択します。

2. パブリックセキュリティグループからのトラフィックを設定していない場合は、TCPポートを設定する必要があります。**Inbound Rules**タブを選択し、**Edit**を選択して、次のルールを作成します。

タイプ	送信元
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	パブリックセキュリティグループを選択します。
ICMP	パブリックセキュリティグループを選択します。
TCP 53 (DNS)	パブリックセキュリティグループを選択します。
UDP 53 (DNS)	パブリックセキュリティグループを選択します。
80 (HTTP)	「パブリックセキュリティグループ」を選択します。
TCP 135	「パブリックセキュリティグループ」を選択します。
TCP 389	「パブリックセキュリティグループ」を選択します。
UDP 389	「パブリックセキュリティグループ」を選択します。
443 (HTTPS)	「パブリックセキュリティグループ」を選択します。
TCP 1494 (ICA/HDX)	「パブリックセキュリティグループ」を選択します。
TCP 2598 (セッションの信頼性)	「パブリックセキュリティグループ」を選択します。

タイプ	送信元
3389 (RDP)	「パブリックセキュリティグループ」を選択します。
TCP 49152–65535	パブリックセキュリティグループを選択します。

3. 完了したら、**保存**を選択します。
4. **［Outbound Rules］**タブを選択し、［Edit］**を選択して、次のルールを作成します。

タイプ	宛先
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

5. 完了したら、**保存**を選択します。

タスク3：インスタンスの起動

次の手順を実行して、2つのEC2インスタンスを作成し、Amazonが生成するデフォルトの管理者パスワードを復号します。

1. AWS管理コンソールから、**EC2**を選択します。
2. EC2ダッシュボードから、**インスタンスの起動**を選択します。
3. Windows Serverマシンイメージとインスタンスタイプを選択します。
4. **インスタンスの詳細の設定**ページで、インスタンスの名前を入力し、以前に設定したVPCを選択します。
5. **サブネット**で、各インスタンスに対して次の選択を行います。
   - Bastionホスト：パブリックサブネットを選択します
   - ドメインコントローラー：プライベートサブネットを選択します
6. **パブリックIPの自動割り当て**で、各インスタンスに対して次の選択を行います。

- 踏み台ホスト：**［Enable］**を選択します。
- ドメインコントローラー：**［Use default setting］**または**［Disable］**を選択します。

7. **ネットワークインターフェイス**で、ドメインコントローラー用にプライベートサブネットのIP範囲内のプライマリIPアドレスを入力します。
8. 必要に応じて、**ストレージの追加**ページでディスクサイズを変更します。
9. **インスタンスのタグ付け**ページで、各インスタンスにわかりやすい名前を入力します。
10. 「**セキュリティグループの設定**」ページで、「**既存のセキュリティグループを選択**」を選択し、各インスタンスについて以下の選択を行います。
    - バスティオンホスト: パブリックセキュリティグループを選択します。
    - ドメインコントローラー: プライベートセキュリティグループを選択します。
11. 選択内容を確認し、次に「**起動**」を選択します。
12. 新しいキーペアを作成するか、既存のキーペアを選択します。新しいキーペアを作成する場合は、プライベートキー (.pem) ファイルをダウンロードし、安全な場所に保管してください。インスタンスのデフォルトの管理者パスワードを取得する際に、プライベートキーを提供する必要があります。
13. 「**インスタンスの起動**」を選択します。「**インスタンスの表示**」を選択して、インスタンスのリストを表示します。新しく起動したインスタンスがすべてのステータスチェックに合格するまで待ってからアクセスしてください。
14. 各インスタンスのデフォルトの管理者パスワードを取得します。
    a. インスタンスリストからインスタンスを選択し、次に「**接続**」を選択します。
    b. 「**RDPクライアント**」タブに移動し、「**パスワードの取得**」を選択し、プロンプトが表示されたらプライベートキー (`.pem`) ファイルをアップロードします。
    c. 「**パスワードの復号**」を選択し、人間が読めるパスワードを取得します。AWSがデフォルトパスワードを表示します。
15. 手順2から手順を繰り返して、2つのインスタンスを作成します。
    - パブリックサブネットに1つの踏み台ホストインスタンス
    - ドメインコントローラーとして使用する、プライベートサブネットに1つのインスタンス。

タスク4：DHCPオプションセットを作成する

1. VPCダッシュボードから、「**DHCPオプションセット**」を選択します。
2. 次の情報を入力します。

- 名前タグ: セットのわかりやすい名前を入力します。
- ドメイン名: ドメインコントローラーインスタンスを構成するときに使用する完全修飾ドメイン名を入力します。
- ドメインネームサーバー: ドメインコントローラーインスタンスに割り当てたプライベートIPアドレスと、コンマで区切られた文字列 **AmazonProvidedDNS** を入力します。
- NTPサーバー: このフィールドは空白のままにします。
- NetBIOSネームサーバー: ドメインコントローラーインスタンスのプライベートIPアドレスを入力します。
- NetBIOSノードタイプ: **2** を入力します。

3. **はい、作成**を選択します。
4. 新しいセットをVPCに関連付けます。

   a. VPCダッシュボードから、**Your VPCs** を選択し、以前に設定したVPCを選択します。

   b. **アクション > DHCPオプションセットの編集** を選択します。

   c. プロンプトが表示されたら、作成した新しいセットを選択し、**保存** を選択します。

タスク5：インスタンスを構成する

1. RDPクライアントを使用して、踏み台ホストインスタンスのパブリックIPアドレスに接続します。プロンプトが表示されたら、管理者アカウントの資格情報を入力します。
2. 踏み台ホストインスタンスからリモートデスクトップ接続を起動し、構成するインスタンスのプライベートIPアドレスに接続します。プロンプトが表示されたら、そのインスタンスの管理者資格情報を入力します。
3. プライベートサブネット内のすべてのインスタンスについて、DNS設定を構成します。

   a. **> > > >** を選択します。表示されているネットワーク接続をダブルクリックします。

   b. **> >** を選択します。

   c. **>** を選択します。次の設定が有効になっていることを確認し、 を選択します。

      - この接続のアドレスをDNSに登録する
      - この接続のDNSサフィックスをDNS登録で使用する

4. ドメインコントローラーを構成するには:

   a. Server Manager を使用して、Active Directory ドメインサービス の役割をすべてのデフォルト機能とともに追加します。

b. インスタンスをドメインコントローラーに昇格させます。昇格中にDNSを有効にし、DHCPオプションセットを作成したときに指定したドメイン名を使用します。プロンプトが表示されたらインスタンスを再起動します。

次のステップ

- コアコンポーネントをインストールする
- VDAのインストール
- サイトの作成
- AWSでの接続の作成と管理については、「AWSへの接続」を参照してください。

詳細情報

- 接続とリソースを作成および管理する
- マシンカタログを作成する

XenServer® 仮想化環境

XenServer は、運用管理を簡素化し、負荷の高いワークロードに対して高精細なユーザーエクスペリエンスを保証します。

XenServer をセットアップするには、「インストール準備」を参照してください。

次に行うこと

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- XenServer で接続を作成および管理するには、「XenServer への接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Google Cloud環境

Citrix Virtual Apps and Desktops™ を使用すると、Google Cloud 上でマシンをプロビジョニングおよび管理できます。

要件

- Citrix Cloud™ アカウント。この記事で説明されている機能は、Citrix Cloud でのみ利用できます。
- Google Cloud プロジェクト。このプロジェクトには、マシンカタログに関連付けられているすべてのコンピューティングリソースが保存されます。既存のプロジェクトでも新規のプロジェクトでもかまいません。
- Google Cloud プロジェクトで4つのAPIを有効にします。詳細については、「Google Cloud APIを有効にする」を参照してください。
- Google Cloud サービスアカウント。サービスアカウントはGoogle Cloudに対して認証を行い、プロジェクトへのアクセスを有効にします。詳細については、「サービスアカウントの構成と更新」を参照してください。
- Googleプライベートアクセスを有効にします。詳細については、「プライベートGoogleアクセスを有効にする」を参照してください。

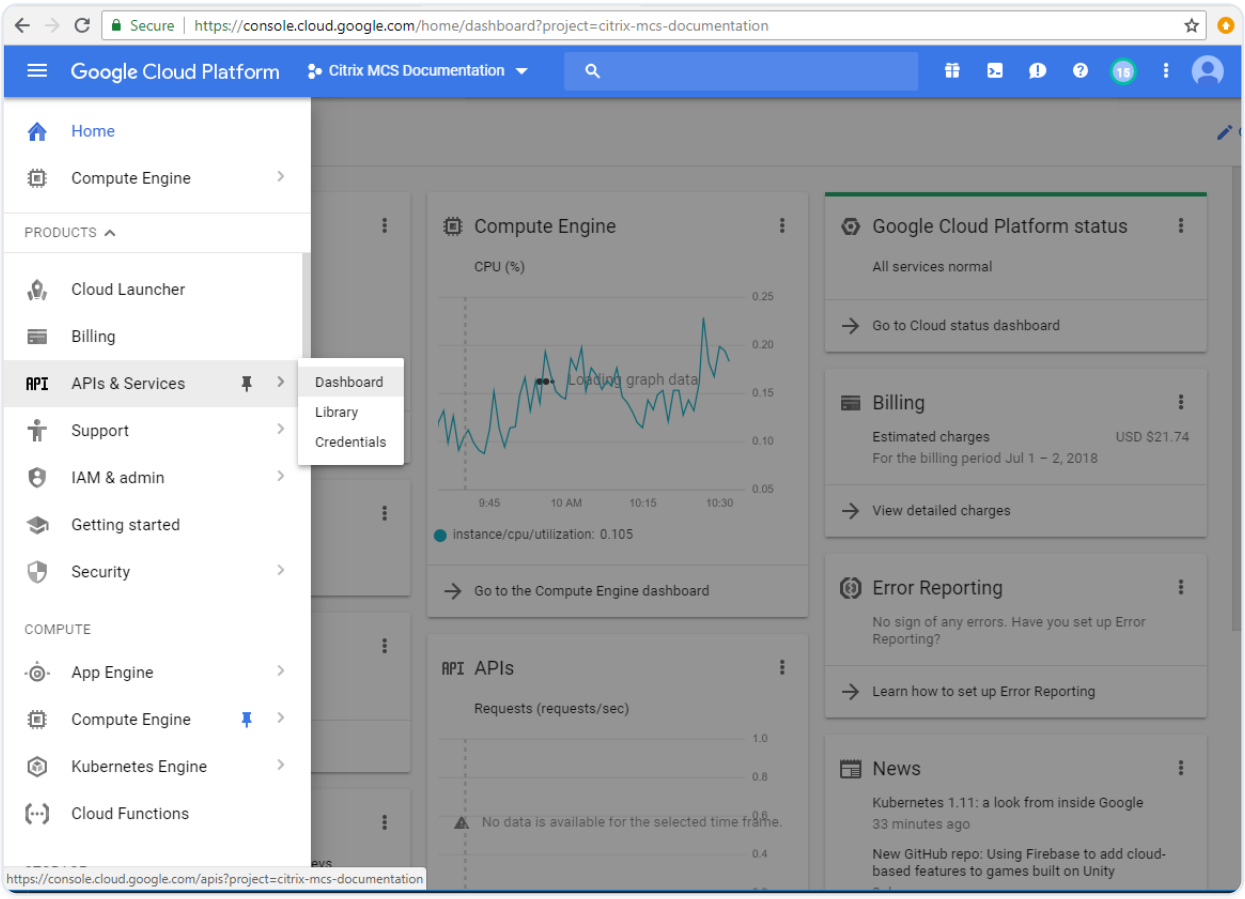
Google Cloud APIを有効にする

Web Studio を介して Google Cloud の機能を使用するには、Google Cloud プロジェクトで次の API を有効にします。

- コンピューティング エンジン API
- クラウド リソース マネージャー API
- ID およびアクセス管理 (IAM) API
- クラウドビルド API
- クラウド キー管理サービス (KMS)

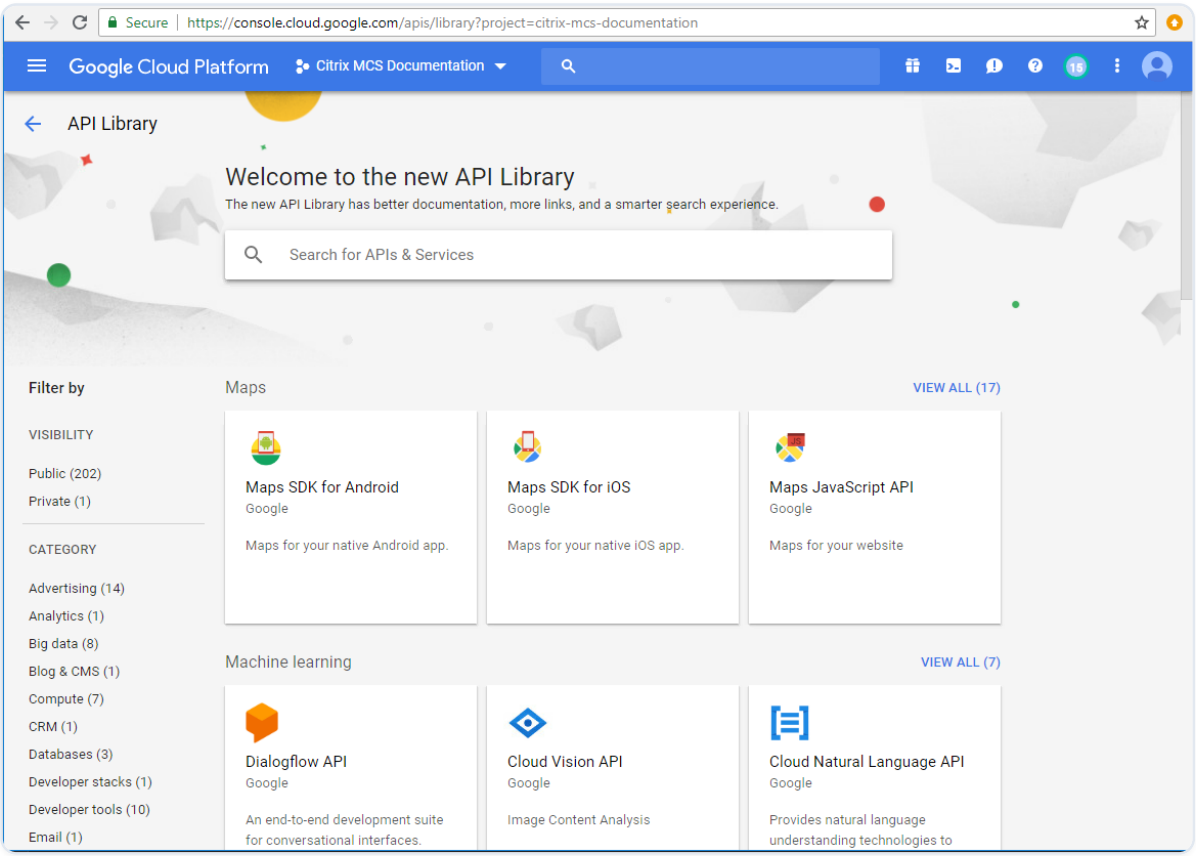
Google Cloudコンソールから、次の手順を実行します。

1. 左上のメニューで、**「APIとサービス」>「ダッシュボード」**を選択します。



2. **ダッシュボード**画面で、Compute Engine APIが有効になっていることを確認します。 有効になっていない場合は、次の手順に従ってください。

   a. 「**APIとサービス > ライブラリ**」に移動します。



b. 検索ボックスに「*Compute Engine*」と入力します。

c. 検索結果から「**Compute Engine API**」を選択します。

d. 「**Compute Engine API**」ページで、「**有効にする**」を選択します。

3. Cloud Resource Manager APIを有効にします。

a. 「**APIとサービス > ライブラリ**」に移動します。

b. 検索ボックスに「*Cloud Resource Manager*」と入力します。

c. 検索結果から「**Cloud Resource Manager API**」を選択します。

d. 「**Cloud Resource Manager API**」ページで、「**有効にする**」を選択します。APIのステータスが表示されます。

4. 同様に、**Identity and Access Management (IAM) API**と**Cloud Build API**を有効にします。

Google Cloud Shellを使用してAPIを有効にすることもできます。これを行うには：

1. Googleコンソールを開き、Cloud Shellをロードします。
2. Cloud Shellで次の4つのコマンドを実行します。

- gcloud services enable compute.googleapis.com
- gcloud services enable cloudresourcemanager.googleapis.com

- gcloud services enable iam.googleapis.com
- gcloud サービス イネーブル cloudbuild.googleapis.com

3. Cloud Shellがプロンプトを表示した場合、「**承認**」をクリックします。

サービスアカウントの構成と更新

> **注:**
>
> GCP は、Cloud Build Service のデフォルトの動作とサービスアカウントの使用に関して、April 29, 2024 以降に変更を導入します。詳細については、「Cloud Build Service Account Change」を参照してください。April 29, 2024 より前に Cloud Build API が有効になっている既存の Google プロジェクトは、この変更の影響を受けません。ただし、April 29 以降も既存の Cloud Build Service の動作を維持したい場合は、Cloud Build API を有効にする前に、組織ポリシーを作成または適用して制約の適用を無効にすることができます。その結果、以下のコンテンツは「Before April 29, 2024」と「After April 29, 2024」の 2 つに分かれています。新しい組織ポリシーを設定する場合は、「Before April 29, 2024」のセクションに従ってください。

April 29, 2024より前

Citrix Cloudは、Google Cloudプロジェクト内で3つの個別のサービスアカウントを使用します。

- *Citrix Cloud Service Account*：このサービスアカウントにより、Citrix Cloud は Google プロジェクトにアクセスし、マシンのプロビジョニングと管理を行うことができます。このサービスアカウントは、Google Cloud によって生成されたキーを使用して Google Cloud に対して認証を行います。

  このサービスアカウントは、ここに記載されているとおりに手動で作成する必要があります。詳細については、「Citrix Cloud Service Account の作成」を参照してください。

  このサービスアカウントはメールアドレスで識別できます。例えば、`<my-service-account>@<project-id>.iam.gserviceaccount.com`。
- *Cloud Build サービスアカウント*: このサービスアカウントは、Google Cloud API を有効にするで言及されているすべての API を有効にすると、自動的にプロビジョニングされます。自動的に作成されたすべてのサービスアカウントを表示するには、**Google Cloud** コンソールで **IAM と管理 > IAM** に移動し、**Google 提供のロール付与を含める** チェックボックスを選択します。

このサービスアカウントは、**プロジェクト ID** と **cloudbuild** という単語で始まるメールアドレスで識別できます。例えば、`<project-id>@cloudbuild.gserviceaccount.com`

サービスアカウントに以下のロールが付与されていることを確認します。ロールを追加する必要がある場合は、Cloud Build サービスアカウントにロールを追加するに記載されている手順に従ってください。

- Cloud Build サービスアカウント
- Compute Instance 管理者
- サービスアカウントユーザー

- *Cloud Compute サービスアカウント*: このサービスアカウントは、Compute API がアクティブ化されると、Google Cloud によって Google Cloud で作成されたインスタンスに追加されます。このアカウントには、操作を実行するための IAM 基本エディターロールがあります。ただし、より詳細な制御を行うためにデフォルトの権限を削除した場合、以下の権限を必要とする **Storage Admin** ロールを追加する必要があります。
  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

このサービスアカウントは、**プロジェクト ID** と **compute** という単語で始まるメールアドレスで識別できます。例えば、`<project-id>-compute@developer.gserviceaccount.com`。

CITRIX CLOUD サービスアカウントを作成する

Citrix Cloud サービスアカウントを作成するには、次の手順に従います。

1. Google Cloud コンソールで、**IAM と管理 > サービスアカウント** に移動します。
2. **サービスアカウント** ページで、**サービスアカウントを作成** を選択します。
3. **サービスアカウントの作成** ページで、必要な情報を入力し、**作成して続行** を選択します。
4. **このサービスアカウントにプロジェクトへのアクセス権を付与** ページで、**ロールを選択** ドロップダウンメニューをクリックし、必要なロールを選択します。さらにロールを追加する場合は、**+別のロールを追加** をクリックします。

   各アカウント（個人またはサービス）には、プロジェクトの管理を定義するさまざまなロールがあります。このサービスアカウントには、以下のロールを付与してください。

   - Compute 管理者

- Storage管理者
- Cloud Build編集者
- サービスアカウントユーザー
- クラウド データストア ユーザー
- Cloud KMS 暗号化オペレーター

Cloud KMS 暗号化オペレーターには、次の権限が必要です。

- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.get
- cloudkms.keyRings.list

> **注：**
>
> 新しいサービスアカウントを作成する際に利用可能な役割の完全なリストを取得するには、すべてのAPIを有効にしてください。

5. **CONTINUE**をクリックします
6. **Grant users access to this service account**ページで、ユーザーまたはグループを追加して、このサービスアカウントでアクションを実行するアクセス権を付与します。
7. **DONE**をクリックします。
8. IAMメインコンソールに移動します。
9. 作成されたサービスアカウントを特定します。
10. 役割が正常に割り当てられていることを検証します。

考慮事項：

サービスアカウントを作成する際は、以下を考慮してください。

- **Grant this service account access to project**および**Grant users access to this service account**の手順はオプションです。これらのオプションの構成手順をスキップすることを選択した場合、新しく作成されたサービスアカウントは**IAM & Admin > IAM**ページに表示されません。

- サービスアカウントに関連付けられた役割を表示するには、オプションの手順をスキップせずに役割を追加します。このプロセスにより、構成されたサービスアカウントに役割が表示されるようになります。

CITRIX CLOUDサービスアカウントキー

Citrix Cloudサービスアカウントキーは、Citrix DaaSで接続を作成するために必要です。キーは資格情報ファイル（.json）に含まれています。キーを作成すると、ファイルは自動的にダウンロードされ、**Downloads**フォルダーに保存されます。キーを作成する際は、キータイプをJSONに設定してください。そうしないと、Web Studioが解析できません。

サービスアカウントキーを作成するには、**IAM と管理 > サービスアカウント**に移動し、Citrix Cloudサービスアカウントのメールアドレスをクリックします。**キー**タブに切り替え、**キーを追加 > 新しいキーを作成**を選択します。キーの種類として**JSON**が選択されていることを確認してください。

> **ヒント:**
>
> Google Cloudコンソールの**サービスアカウント**ページを使用してキーを作成します。セキュリティ上の理由から、キーを定期的に変更することをお勧めします。既存のGoogle Cloud接続を編集することで、Citrix Virtual Apps and Desktopsアプリケーションに新しいキーを提供できます。

CITRIX CLOUD サービスアカウントにロールを追加する

Citrix Cloud サービスアカウントにロールを追加するには、次の手順を実行します。

1. Google Cloudコンソールで、**IAM と管理 > IAM**に移動します。
2. **IAM > 権限**ページで、作成したサービスアカウント（メールアドレスで識別可能）を見つけます。

   例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. 鉛筆アイコンを選択して、サービスアカウントのプリンシパルへのアクセスを編集します。
4. 選択したプリンシパルオプションの**「project-id」へのアクセスを編集**ページで、**別のロールを追加**を選択して、必要なロールをサービスアカウントに1つずつ追加し、**保存**を選択します。

CLOUD BUILD サービスアカウントにロールを追加する

Cloud Build サービスアカウントにロールを追加するには、次の手順を実行します。

1. Google Cloudコンソールで、**IAM と管理 > IAM**に移動します。
2. **IAM**ページで、**プロジェクトID**と**cloudbuild**という単語で始まるメールアドレスで識別できるCloud Buildサービスアカウントを見つけます。

   例：`<project-id>@cloudbuild.gserviceaccount.com`
3. 鉛筆アイコンを選択して、Cloud Build アカウントの役割を編集します。
4. 選択したプリンシパルオプションの「**"project-id" へのアクセスを編集**」ページで、「**別の役割を追加**」を選択して、必要な役割を Cloud Build サービスアカウントに1つずつ追加し、その後「**保存**」を選択します。

   > **注:**
   >
   > すべての API を有効にして、役割の完全なリストを取得します。

April 29, 2024 以降

Citrix Cloud は、Google Cloud プロジェクト内で2つの異なるサービスアカウントを使用します。

- *Citrix Cloud サービスアカウント*: このサービスアカウントにより、Citrix Cloud は Google プロジェクトにアクセスし、マシンをプロビジョニングおよび管理できます。このサービスアカウントは、Google Cloud によって生成されたキーを使用して Google Cloud に対して認証を行います。

  このサービスアカウントは手動で作成する必要があります。

  このサービスアカウントは、メールアドレスで識別できます。例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`。
- *Cloud Compute サービスアカウント*: このサービスアカウントは、Google Cloud API を有効にするで言及されているすべての API を有効にした後に自動的にプロビジョニングされます。自動的に作成されたすべてのサービスアカウントを表示するには、**Google Cloud** コンソールで「**IAM と管理 > IAM**」に移動し、「**Google 提供の役割付与を含める**」チェックボックスを選択します。このアカウントには、操作を実行するための IAM 基本編集者ロールがあります。ただし、より詳細な制御を行うためにデフォルトの権限を削除した場合、次の権限を必要とする**ストレージ管理者**ロールを追加する必要があります。
  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get

- storage.objects.list

このサービスアカウントは、**プロジェクト ID** と「**compute**」という単語で始まるメールアドレスで識別できます。例: `<project-id>-compute@developer.gserviceaccount.com.`.

サービスアカウントに次のロールが付与されていることを確認します。

- Cloud Build サービスアカウント
- Compute Instance 管理者
- サービスアカウントユーザー

CITRIX CLOUD サービスアカウントを作成する

Citrix Cloud サービスアカウントを作成するには、以下の手順に従います。

1. Google Cloud コンソールで、**IAM と管理 > サービスアカウント**に移動します。
2. **サービスアカウント**ページで、**サービスアカウントを作成**を選択します。
3. **サービスアカウントの作成**ページで、必要な情報を入力し、**作成して続行**を選択します。
4. 「**このサービスアカウントにプロジェクトへのアクセスを許可する**」ページで、「**ロールを選択**」ドロップダウンメニューをクリックし、必要なロールを選択します。さらにロールを追加する場合は、「**+別のロールを追加**」をクリックします。

   各アカウント（個人またはサービス）には、プロジェクトの管理を定義するさまざまなロールがあります。このサービスアカウントには、以下のロールを付与してください。

   - Compute 管理者
   - Storage管理者
   - Cloud Build編集者
   - サービスアカウントユーザー
   - クラウド データストア ユーザー
   - Cloud KMS Crypto オペレーター

   Cloud KMS Crypto オペレーターには、次の権限が必要です。

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list

> **注：**
>
> 新しいサービスアカウントを作成する際に利用可能なロールの完全なリストを取得するには、すべてのAPIを有効にします。

5. をクリックします。
6. ページで、ユーザーまたはグループを追加して、このサービスアカウントでアクションを実行するアクセス権を付与します。
7. をクリックします。
8. IAMメインコンソールに移動します。
9. 作成されたサービスアカウントを特定します。
10. ロールが正常に割り当てられていることを検証します。

留意事項:

サービスアカウントを作成する際は、以下の点に留意してください。

- **このサービスアカウントにプロジェクトへのアクセスを許可する**および**ユーザーにこのサービスアカウントへのアクセスを許可する**の手順はオプションです。これらのオプションの構成手順をスキップすることを選択した場合、新しく作成されたサービスアカウントは、**IAM と管理 > IAM** ページに表示されません。
- サービスアカウントに関連付けられたロールを表示するには、オプションの手順をスキップせずにロールを追加してください。このプロセスにより、構成されたサービスアカウントにロールが表示されるようになります。

CITRIX CLOUDサービスアカウントキー

Citrix DaaSで接続を作成するには、Citrix Cloudサービスアカウントキーが必要です。キーは資格情報ファイル（.json）に含まれています。キーを作成すると、ファイルは自動的にダウンロードされ、**ダウンロード**フォルダーに保存されます。キーを作成する際は、キータイプをJSONに設定してください。そうしないと、Web Studioはそれを解析できません。

サービスアカウントキーを作成するには、**IAM と管理 > サービスアカウント**に移動し、Citrix Cloudサービスアカウントのメールアドレスをクリックします。**キー**タブに切り替え、**キーを追加 > 新しいキーを作成**を選択します。キータイプとして**JSON**を必ず選択してください。

> **ヒント:**

Google Cloudコンソールの**サービスアカウント**ページを使用してキーを作成します。セキュリティ上の理由から、キーを定期的に変更することをお勧めします。既存のGoogle Cloud接続を編集することで、新しいキーをCitrix Virtual Apps and Desktopsアプリケーションに提供できます。

CITRIX CLOUD サービスアカウントにロールを追加する

Citrix Cloudサービスアカウントにロールを追加するには、次の手順を実行します。

1. Google Cloudコンソールで、**IAM と管理 > IAM**に移動します。
2. **IAM > 権限**ページで、メールアドレスで識別できる、作成したサービスアカウントを見つけます。

   例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. 鉛筆アイコンを選択して、サービスアカウントのプリンシパルへのアクセスを編集します。
4. 選択したプリンシパルオプションの「**Edit access to "project-id"**」ページで、「**ADD ANOTHER ROLE**」を選択して、必要なロールをサービスアカウントに1つずつ追加し、その後「**SAVE**」を選択します。

CLOUD COMPUTE サービスアカウントにロールを追加する

Cloud Compute サービスアカウントにロールを追加するには：

1. Google Cloud コンソールで、**IAM & Admin > IAM** に移動します。
2. 「**IAM**」ページで、**プロジェクトID**と「**compute**」という単語で始まるメールアドレスで識別できるCloud Compute サービスアカウントを探します。

   例：`<project-id>-compute@developer.gserviceaccount.com`
3. 鉛筆アイコンを選択して、Cloud Build アカウントのロールを編集します。
4. 選択したプリンシパルオプションの「**Edit access to "project-id" page**」で、「**ADD ANOTHER ROLE**」を選択して、必要なロールをCloud Build サービスアカウントに1つずつ追加し、その後「**SAVE**」を選択します。

注:

ロールの完全なリストを取得するには、すべてのAPIを有効にします。

ストレージの権限とバケット管理

Citrix Virtual Apps and Desktops は、Google Cloud サービスのクラウドビルドの失敗を報告するプロセスを改善します。このサービスはGoogle Cloud上でビルドを実行します。Citrix Virtual Apps and Desktops は、Google Cloud サービスがビルドログ情報をキャプチャする`citrix-mcs-cloud-build-logs-{region}-{5 random characters}`という名前のストレージバケットを作成します。このバケットには、30日後にコンテンツを削除するオプションが設定されています。このプロセスでは、接続に使用されるサービスアカウントに`storage.buckets.update`に設定されたGoogle Cloud の権限が必要です。サービスアカウントにこの権限がない場合、Citrix Virtual Apps and Desktops はエラーを無視し、カタログ作成プロセスを続行します。この権限がないと、ビルドログのサイズが増加し、手動でのクリーンアップが必要になります。

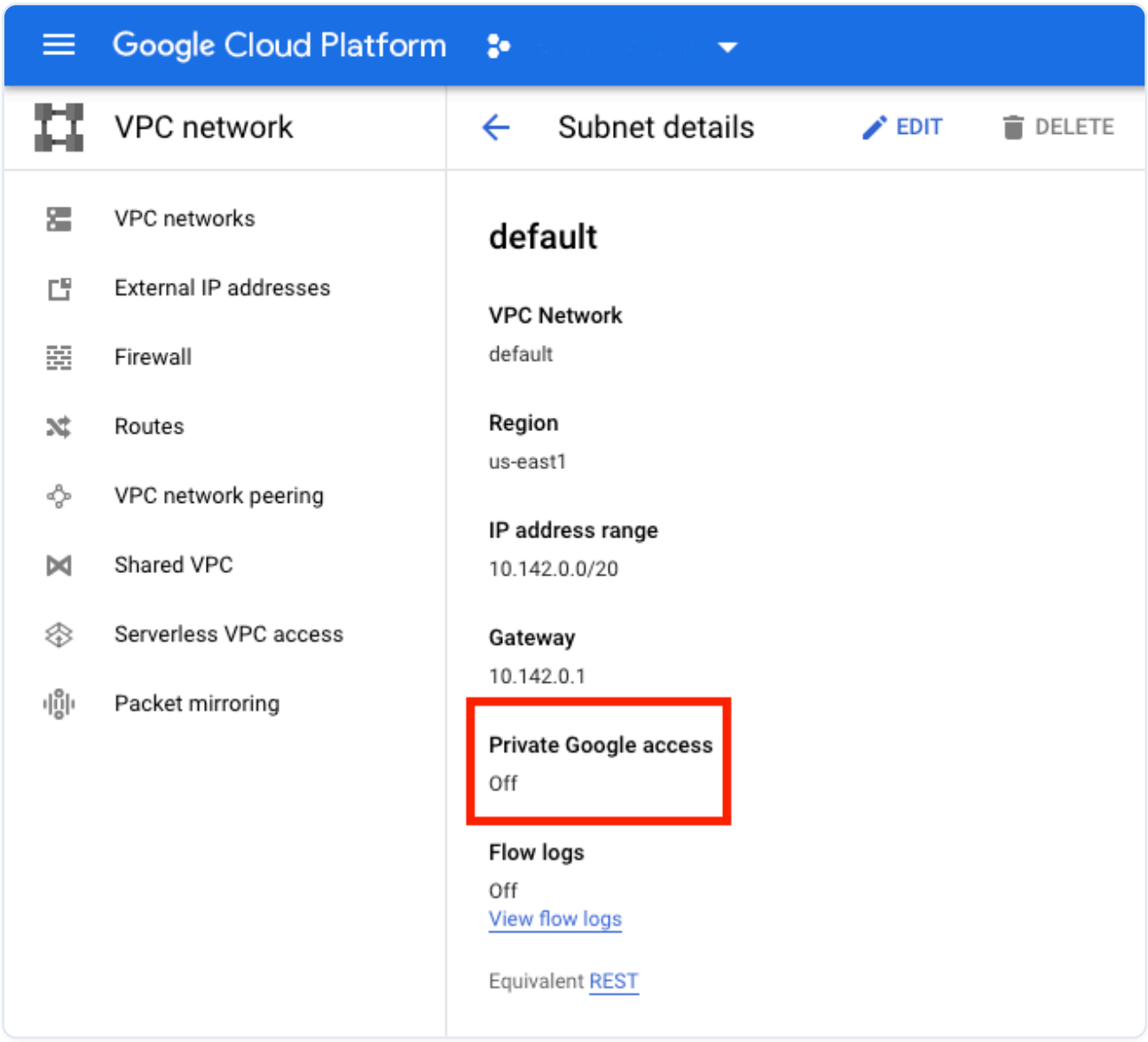
プライベート Google アクセスを有効にする

VMのネットワークインターフェースに外部IPアドレスが割り当てられていない場合、パケットは他の内部IPアドレスの宛先にのみ送信されます。プライベートアクセスを有効にすると、VMはGoogle APIおよび関連サービスで使用される外部IPアドレスのセットに接続します。

> **注:**
>
> プライベート Google アクセスが有効になっているかどうかにかかわらず、パブリック IP アドレスを持つ VM と持たない VM の両方が、特にサードパーティのネットワークアプライアンスが環境にインストールされている場合、Google Public API にアクセスできる必要があります。

MCSプロビジョニングのために、サブネット内のVMがパブリックIPアドレスなしでGoogle APIにアクセスできるようにするには、次の手順を実行します。

1. Google Cloudで、**VPC network configuration**にアクセスします。
2. サブネットの詳細画面で、「**Private Googleアクセス**」をオンにします。



詳細については、「Configuring Private Google Access」を参照してください。

重要:

ネットワークがVMのインターネットアクセスを防止するように構成されている場合、VMが接続されているサブネットに対してPrivate Googleアクセスを有効にすることに関連するリスクを組織が負うことを確認してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成

- Google Cloud 環境での接続の作成と管理については、「Google Cloud 環境への接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログを作成(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html)

HPE Moonshot 仮想化環境

Citrix Virtual Apps and Desktops™ は、Citrix が管理する HPE Moonshot プラグインを介して HPE Moonshot ワークロードを管理します。このプラグインを使用すると、HPE Moonshot シャーシへの接続を作成し、カタログを作成し、カタログ内のマシンの電源を管理できます。

要件

Citrix が管理する HPE Moonshot プラグインを Delivery Controller にインストールします。

> **注:**
>
> - Citrix が管理する HPE Moonshot プラグインと HPE が管理する HPE Moonshot プラグインの両方がインストールされている場合、Delivery Controller は Citrix が管理する HPE Moonshot プラグインを使用します。
> - Citrix が管理する HPE Moonshot プラグインと HPE が管理する HPE Moonshot プラグインの両方がインストールされており、HPE が管理する Moonshot プラグインを使用したい場合は、Citrix が管理する HPE Moonshot プラグインをアンインストールし、`RegisterPlugin` キャッシュを更新してください。

Citrix が管理する HPE Moonshot プラグインをインストールする

Citrix が管理する HPE Moonshot プラグインをインストールするには、次の手順を実行します。

1. `E:\x64\Citrix Desktop Delivery Controller\MoonshotPlugin`.msi をインストールします。`E:\` は ISO です。
2. PowerShell を管理者として開き、次のコマンドを実行します。

```
C:\Program Files\Common Files\Citrix\HCLPlugins> .\RegisterPlugins.exe
-pluginsroot .\CitrixMachineCreation\v1.0.0.0\
```

3. プラグインの登録が成功したら、**タスクマネージャー**から次のサービスを再起動します。
    a. CitrixBrokerService
    b. CitrixHostService
    c. CitrixMachineCreationService
4. `Get-HypHypervisorPlugins`を実行して、デリバリーコントローラーにプラグインがインストールされているか確認します。出力の**DisplayName**フィールドには、**HPE Moonshot**と表示される必要があります。

Citrix管理のHPE Moonshotプラグインをアンインストールし、RegisterPluginキャッシュを更新する

Citrix管理とHPE管理の両方のHPE Moonshotプラグインがインストールされており、HPE管理のMoonshotプラグインを使用したい場合は、Citrix管理のHPE Moonshotプラグインをアンインストールし、`RegisterPlugin`キャッシュを更新する必要があります。その方法は次のとおりです。

1. Citrix管理のHPE Moonshotプラグインをアンインストールします。
2. PowerShellを管理者として開き、次のコマンドを実行します。

```
cd `C:\Program Files\Common Files\Citrix\HCLPlugins\`

C:\Program Files\Common Files\Citrix\HCLPlugins> .\RegisterPlugins.exe
-PluginsRoot ` C:\Program Files\Common
Files\Citrix\HCLPlugins\ManagedMachine\v2.5.0.0\`
```

3. プラグインの登録が成功したら、**タスクマネージャー**から次のサービスを再起動します。
    a. CitrixBrokerService
    b. CitrixHostService
    c. CitrixMachineCreationService
4. `Get-HypHypervisorPlugins`を実行して、デリバリーコントローラーにプラグインがインストールされているか確認します。出力の**DisplayName**フィールドには、**HPE Moonshot Machine Manager**と表示される必要があります。

主な手順

1. HPE 環境をセットアップします。
2. HPE Moonshot シャーシへの接続を作成します。

3. マシンカタログを作成します。

> **注:**
>
> カタログを作成する前に、1 つ以上の HPE Moonshot カートリッジノードがあることを確認し、それらのノードに VDA をインストールしてください。HPE Moonshot シャーシをハイパーバイザー、カートリッジノードを VM と考えることができます。

4. デリバリーグループを作成します。
5. 管理されていない残りの HPE Moonshot ノードを、管理対象のカタログまたはデリバリーグループに移行します。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- HPE Moonshotで接続を作成および管理する方法については、「HPE Moonshotへの接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

マイクロソフト システムセンター バーチャル マシン マネージャー 仮想化環境

仮想マシンを提供するために、Hyper-V と Microsoft System Center Virtual Machine Manager (VMM) を使用する場合は、このガイダンスに従ってください。

このリリースでは、システム要件 に記載されている VMM バージョンがサポートされています。

> **注:**
>
> 混在 Hyper-V クラスター（異なる Hyper-V バージョンを実行しているサーバーを含む）はサポートされていません。

Citrix Provisioning (旧 Provisioning Services) および Machine Creation Services™ を使用して、以下をプロビジョニングできます。

- 第1世代でサポートされているデスクトップまたはサーバーOSのVM。
- セキュアブートのサポートを含む、第2世代でサポートされているデスクトップまたはサーバーOSのVM。

ハイパーバイザーのインストールと構成

重要:

すべてのDelivery Controllerは、VMMサーバーと同じフォレスト内にある必要があります。

1. Microsoft Hyper-VサーバーとVMMをサーバーにインストールします。
2. すべてのControllerにSystem Center Virtual Machine Managerコンソールをインストールします。コンソールのバージョンは管理サーバーのバージョンと一致している必要があります。以前のコンソールでも管理サーバーに接続できますが、バージョンが異なる場合、VDAのプロビジョニングは失敗します。
3. 次のアカウント情報を確認します。

   Studioでホストを指定するために使用するアカウントは、関連するHyper-Vマシンに対するVMM管理者またはVMM委任管理者である必要があります。このアカウントがVMMで委任管理者ロールのみを持っている場合、ホスト作成プロセス中にStudioにストレージデータが表示されません。

   Studio統合に使用されるユーザーアカウントは、各Hyper-Vサーバーの管理者ローカルセキュリティグループのメンバーである必要もあります。この構成は、VMの作成、更新、削除などのVMライフサイクル管理をサポートします。

   Hyper-Vを実行しているサーバーにControllerをインストールすることはサポートされていません。

単一のSCVMMが異なるデータセンター内の複数のクラスターを管理する大規模な展開では、委任管理者のホストグループのスコープを制限できます。

ホストグループのスコープを制限するには、Microsoft System Center Virtual Machine Manager (VMM) コンソールで「委任された管理者」ロールを使用します。

1. **ユーザーロールの作成ウィザード**で、ユーザーロールとして「Fabric Administrator (Delegated Administrator)」を選択します。
2. **メンバー**で、委任された管理者として使用するActive Directoryのユーザーアカウントを追加します。
3. **スコープ**で、委任された管理者がアクセスできるようにするホストグループを選択します。
4. 委任された管理者のユーザー資格情報を使用して、新しい**実行アカウント**を作成します。これらの資格情報を使用して、後でハイパーバイザー接続を作成します。メインの管理者ロールアカウントは使用しないでください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- SCVMMでの接続の作成と管理については、Microsoft System Center Virtual Machine Managerへの接続を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログを作成する

Nutanix仮想化環境

このガイダンスに従って、Nutanix Acropolis を使用して Citrix Virtual Apps and Desktops™ 展開環境で仮想マシンを提供してください。セットアッププロセスには、次のタスクが含まれます。

- Citrix Virtual Apps and Desktops 環境に Nutanix プラグインをインストールして登録します。
- Nutanix Acropolis ハイパーバイザーへの接続を作成します。
- Nutanix ハイパーバイザーで作成したマスターイメージのスナップショットを使用するマシンカタログを作成します。

詳細については、Nutanix Support Portal で入手できる Nutanix Acropolis MCS プラグインインストールガイドを参照してください。

Nutanixプラグインのインストールと登録

すべての Delivery Controller に Nutanix プラグインをインストールして登録するには、次の手順を完了します。Citrix Studio を使用して Nutanix への接続を作成します。次に、Nutanix 環境で作成したマスターイメージのスナップショットを使用するマシンカタログを作成します。

> **ヒント:**
>
> Nutanix プラグインをインストールまたは更新する際は、Citrix Host Service、Citrix Broker Service、および Machine Creation Services™ を停止してから再起動することをお勧めします。
>
> Nutanix プラグインのインストールについては、Nutanix Documentation site を参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- Nutanix環境で接続を作成および管理するには、「Nutanixへの接続」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections/connection-nutanix.html)

詳細情報

- 接続とリソースの作成および管理(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections.html)
- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html)

Nutanix クラウドおよびパートナーソリューション

Citrix Virtual Apps and Desktops™ は、以下の Nutanix クラウドおよびパートナーソリューションをサポートしています。

- AWS 上のニュータニックス・クラウド・クラスター

AWS 上のニュータニックス・クラウド・クラスター

Citrix Virtual Apps and Desktops は、AWS 上の Nutanix Cloud Clusters をサポートしています。Nutanix クラスターは、プライベートクラウドまたは複数のパブリッククラウドでアプリケーションを実行する方法を簡素化します。AWS 上の Nutanix Cloud Clusters の詳細については、Nutanix Cloud Clusters on AWS Deployment and User Guide を参照してください。

> **ヒント:**
>
> このサポートは、Nutanix オンプレミス クラスターと同じ機能を提供します。サポートされるクラスターは、*Prism Element* の 1 つだけです。詳細については、こちら を参照してください。

要件

AWS で Nutanix クラスターを使用するには、以下が必要です。

- Nutanix アカウント。
- 次の権限を持つ AWS アカウント:
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

Nutanix クラスターを作成する

Nutanix Clusterを作成するには:

1. Nutanixアカウントにログインします。
2. **Nutanix cluster**オプションを見つけて、**Launch**をクリックします。**Nutanix Console**が開きます。詳細については、「Get Started with Nutanix Cluster on AWS」を参照してください。
3. **new VPC**を作成することを選択します。

クラスター作成プロセスは、以下のエラーで失敗する可能性があります:

- クラスターは指定された時間内に作成できませんでした。クラスターを削除しています。
- ホスト Nutanix クラスター - ノード `XXXXXXXXXX: Instance i-xxxxxxxxxxxxx: disable network interface source/dest check error.`.
- ホスト Nutanix クラスター - ノード `XXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxx network interface info.`.

クラスターの作成に失敗した場合：

- 別のリージョンで再作成してみてください。
- 再試行する前に、Nutanix CloudFormation Stack (CFS) を削除してください。

他のリソースに加えて、Nutanix CFSは以下を作成します:

- *Nutanix Cluster xxxxxxxxxxxx* 10.0.0.0/16 という名前の1つのVPC
- 2つのサブネット 10.0.128.0/24 および 10.0.129.0/24
- 1つのインターネットゲートウェイ
- 1 NATゲートウェイ

クラスターが作成されたら、**Nutanix Prism**のアドレスを取得します。

1. **Nutanix Console**に移動します。
2. コンソールの右上にある**Launch Prism Element**リンクにマウスオーバーし、URLをコピーします。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- Nutanixクラウドおよびパートナーソリューションの接続を作成および管理するには、「Nutanixクラウドおよびパートナーソリューションへの接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

VMware クラウドおよびパートナーソリューション

Citrix Virtual Apps and Desktops™ は、以下の VMware クラウドおよびパートナーソリューションをサポートしています。

- Azure VMware ソリューション (AVS)
- Google Cloud VMware エンジン
- アマゾン ウェブ サービス (AWS) 上の VMware クラウド(#vmware-cloud-on-amazon-web-services-aws)

Azure VMware ソリューション (AVS) の統合

Citrix Virtual Apps and Desktop サービスは AVS をサポートしています。AVS は、Azure インフラストラクチャによって作成された vSphere クラスターを含むクラウドインフラストラクチャを提供します。Citrix Virtual Apps and Desktop サービスを活用して、オンプレミス環境で vSphere を使用する場合と同じ方法で、AVS を使用して VDA ワークロードをプロビジョニングします。

AVS クラスターのセットアップ

Citrix Virtual Apps™ and Desktop サービスで AVS を使用できるようにするには、Azure で次の手順を実行します。

- ホストクォータを要求する
- Microsoft.AVS リソース プロバイダーを登録する
- ネットワークチェックリスト
- Azure VMware Solution プライベートクラウドを作成する
- Azure VMware Solution プライベートクラウドにアクセスする
- AzureでVMwareプライベートクラウドのネットワークを構成する
- Azure VMware Solution の DHCP を構成する
- Azure VMware Solution にネットワークセグメントを追加する
- Azure VMware Solution 環境を確認する

AZURE ENTERPRISE AGREEMENT のお客様向けホストクォータを要求する

Azure ポータルの**ヘルプとサポート**ページで、**新しいサポートリクエスト**を選択し、以下の情報を含めます。

- 問題の種類: 技術
- サブスクリプション: サブスクリプションを選択してください
- サービス: すべてのサービス > Azure VMware Solution
- リソース: 一般的な質問
- 概要: 容量が必要
- 問題の種類: 容量管理の問題
- 問題のサブタイプ: 追加ホストクォータ/容量に関するお客様からのリクエスト

サポートチケットの に、 タブで次の情報を含めます。

- POC または本番環境
- リージョン名

- ホスト数
- その他の詳細

> **注:**
>
> AVSは最低3つのホストを必要とし、N+1ホストの冗長性を使用することを推奨します。

> サポートチケットの詳細を指定した後、**Review + Create** を選択してAzureにリクエストを送信します。

MICROSOFT.AVS リソース プロバイダーを登録する

ホスト クォータを要求した後、リソース プロバイダーを登録します。

1. Azure portal にサインインします。
2. Azure portal メニューで、 を選択します。
3. メニューで、サブスクリプションを入力し、 を選択します。
4. サブスクリプション リストからサブスクリプションを選択します。
5. を選択し、検索バーに **Microsoft.AVS** と入力します。
6. リソース プロバイダーが登録されていない場合は、 を選択します。

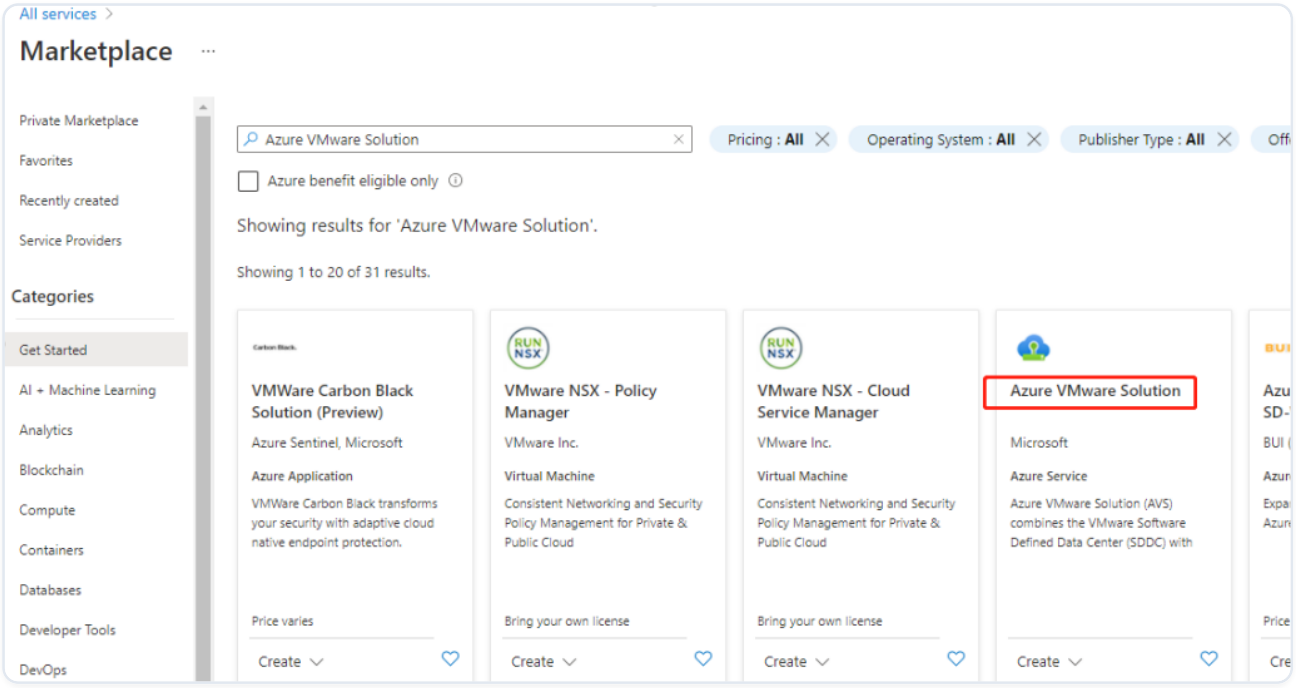
ネットワークに関する考慮事項

AVSは、特定のネットワークアドレス範囲とファイアウォールポートを必要とするネットワークサービスを提供します。詳細については、Azure VMware Solution のネットワーク計画チェックリストを参照してください。

AZURE VMWARE SOLUTION プライベートクラウドを作成する

環境のネットワーク要件を考慮した後、AVS プライベートクラウドを作成します。

1. Azureポータルにサインインします。
2. **新しいリソースの作成**を選択します。
3. **Marketplace の検索**テキストボックスに、*Azure VMware Solution*と入力し、リストから**Azure VMware Solution**を選択します。



image

Azure VMware Solutionウィンドウで、:

1. **作成**を選択します。
2. タブをクリックします。
3. 以下の表の情報を使用して、フィールドに値を入力します。

フィールド	値
サブスクリプション	デプロイに使用するサブスクリプションを選択します。Azure サブスクリプション内のすべてのリソースはまとめて課金されます。
リソースグループ	プライベートクラウドのリソースグループを選択します。Azure リソースグループは、Azure リソースがデプロイおよび管理される論理コンテナです。または、プライベートクラウド用に新しいリソースグループを作成することもできます。
場所	east us などの場所を選択します。これは、計画フェーズで定義したリージョンです。
リソース名	Azure VMware Solution プライベートクラウドの名前を指定します。

フィールド	値
SKU	AV36 を選択します。
ホスト	プライベートクラウドクラスターに割り当てられたホストの数を表示します。デフォルト値は3で、デプロイ後に増減できます。
アドレスブロック	プライベートクラウドの IP アドレスブロックを指定します。CIDR はプライベートクラウド管理ネットワークを表し、vCenter Server や NSX-T Manager などのクラスター管理サービスに使用されます。たとえば、10.175.0.0/22 のように /22 アドレス空間を使用します。このアドレスは一意であり、他の Azure 仮想ネットワークやオンプレミスネットワークと重複しないようにする必要があります。
仮想ネットワーク	Azure VMware Solution ExpressRoute 回線はデプロイ後の手順として確立されるため、このフィールドは空白のままにします。

「**プライベートクラウドの作成**」画面で、次のようにします。

1. 「**場所**」フィールドで、AVS が存在するリージョンを選択します。リソースグループのリージョンは AVS リージョンと同じです。
2. 「**SKU**」フィールドで、「**AV36 Node**」を選択します。
3. 「**Address Block**」フィールドにIPアドレスを指定します。例: 10.15.0.0/22。
4. 「**Review + Create**」を選択します。
5. 情報を確認したら、「**Create**」をクリックします。

Azure ASV プライベートクラウドの作成(/en-us/citrix-virtual-apps-desktops/2407/media/azure-avs-create-private-cloud.png)

> **ヒント:**
>
> プライベートクラウドの作成には3〜4時間かかる場合があります。クラスターに単一のホストを追加するには30〜45分かかる場合があります。

> 展開が成功したことを確認します。作成したリソースグループに移動し、プライベートクラウドを選択します。**Status**が「**Succeeded**」になったら、展開は完了です。

Azure ASV 接続の確認(/en-us/citrix-virtual-apps-desktops/2407/media/azure-avs-verify-connection.png)

AZURE VMWARE SOLUTION プライベートクラウドへのアクセス

プライベートクラウドを作成したら、Windows VMを作成し、プライベートクラウドのローカルvCenterに接続します。
新しいWindows仮想マシンの作成

1. リソースグループで「**+ Add**」を選択し、「**Microsoft Windows 10/2016/2019**」を検索して選択します。
2. 「**Create**」をクリックします。
3. 必要な情報を入力し、「**Review + Create**」を選択します。
4. 検証が成功したら、「**作成**」を選択して仮想マシンの作成プロセスを開始します。

プライベートクラウドのローカルvCenterに接続する

1. クラウド管理者として **vSphere Client with VMware vCenter SSO** にサインインします。

   Azure ASV vSphere ログイン(/en-us/citrix-virtual-apps-desktops/2407/media/azure-avs-vsphere-login.png)
2. Azureポータルでプライベートクラウドを選択し、次に「**管理 > ID**」を選択します。

プライベートクラウドのvCenterとNSX-T ManagerのURLとユーザー資格情報が表示されます。

Azure ASV セットアップ vCenter(/en-us/citrix-virtual-apps-desktops/2407/media/azure-avs-setup-vcenter.png)

URLとユーザー資格情報を確認後:

1. 前の手順で作成したVMに移動し、仮想マシンに接続します。
2. Windows VMでブラウザを開き、2つのブラウザタブでvCenterとNSX-T ManagerのURLに移動します。vCenterタブで、前のステップで取得した*cloudadmin@vmcp.local*ユーザー資格情報を入力します。

AZUREでVMWAREプライベートクラウドのネットワークを構成する

ASVプライベートクラウドにアクセスした後、仮想ネットワークとゲートウェイを作成してネットワークを構成します。
仮想ネットワークを作成する

1. Azureポータルにサインインします。
2. 以前に作成したリソースグループに移動します。
3. 新しいリソースを定義するには、 を選択します。
4. テキストボックスに「*仮想ネットワーク*」と入力します。仮想ネットワークリソースを見つけて選択します。
5. 「**仮想ネットワーク**」ページで、「**作成**」を選択してプライベートクラウドの仮想ネットワークを設定します。
6. 「**仮想ネットワークの作成**」ページで、仮想ネットワークの詳細を入力します。
7. 「**基本**」タブで、仮想ネットワークの名前を入力し、適切なリージョンを選択して、「**次へ：IPアドレス**」をクリックします。
8. 「**IPアドレス**」タブのIPv4アドレス空間で、以前に作成したアドレスを入力します。

> 「**重要:**」:

> プライベートクラウドを作成したときに使用したアドレス空間と重複しないアドレスを使用してください。

> アドレス空間を入力した後:

1. 「**+ サブネットの追加**」を選択します。
2. 「**サブネットの追加**」ページで、サブネットに名前と適切なアドレス範囲を割り当てます。
3. 「**追加**」をクリックします。
4. 「**確認 + 作成**」を選択します。
5. 情報を確認し、「**作成**」をクリックします。デプロイが完了すると、仮想ネットワークがリソースグループに表示されます。

仮想ネットワークゲートウェイを作成する
仮想ネットワークを作成した後、仮想ネットワークゲートウェイを作成します。

1. リソースグループで、「**+ 追加**」を選択して新しいリソースを追加します。
2. 「**Search the Marketplace**」テキストボックスに「*virtual network gateway*」と入力します。仮想ネットワークリソースを見つけて選択します。
3. 「**Virtual Network gateway**」ページで、「**Create**」をクリックします。

4. 「**Create virtual network gateway**」ページの「**Basics**」タブで、フィールドに値を入力します。
5. 「**Review + create**」をクリックします。

Azure ASV セットアップ vCenter(/en-us/citrix-virtual-apps-desktops/2407/media/azure-avs-create-virtual-gateway.png)

仮想ネットワークゲートウェイの構成を確認したら、**作成**をクリックして仮想ネットワークゲートウェイを展開します。 展開が完了したら、**ExpressRoute**接続をAzure AVSプライベートクラウドを含む仮想ネットワークゲートウェイに接続します。

EXPRESSROUTEを仮想ネットワークゲートウェイに接続する

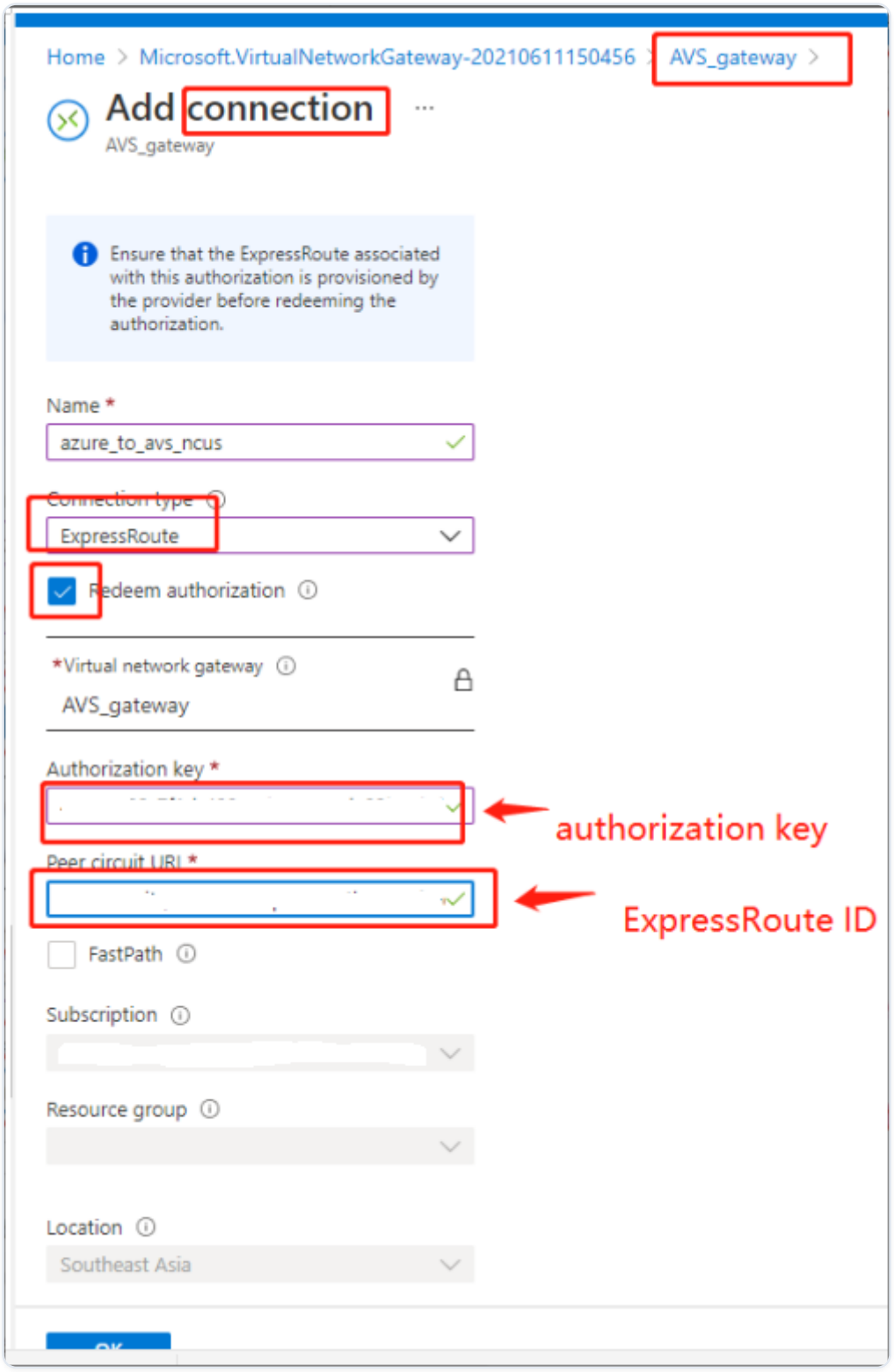
仮想ネットワークゲートウェイを展開した後、それとAzure AVSプライベートクラウドの間に接続を追加します。

1. ExpressRoute承認キーを要求します。
2. Azureポータルで、**Azure VMware Solution private cloud**に移動します。「**Manage> Connectivity > ExpressRoute**」を選択し、次に「**+ Request an authorization key**」を選択します。

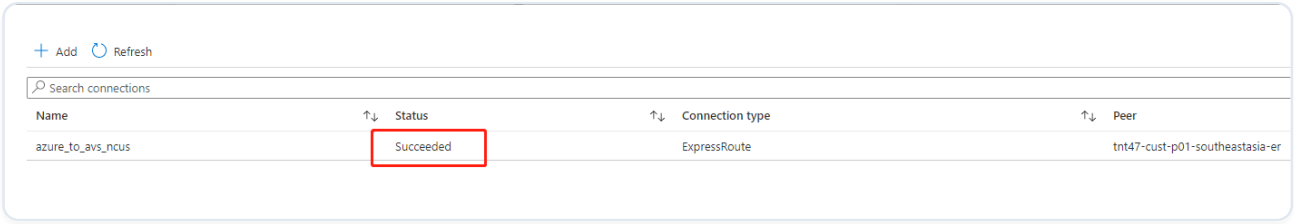
Azure ASV 承認キーの要求(/en-us/citrix-virtual-apps-desktops/2407/media/azure-avs-expressroute.png)

承認キーを要求した後：

1. キーの名前を入力し、**作成**をクリックします。キーの作成には約30秒かかる場合があります。作成されると、新しいキーはプライベートクラウドの承認キーのリストに表示されます。
2. 「**承認キー**」と「**ExpressRoute ID**」をコピーします。これらはピアリングプロセスを完了するために必要です。承認キーはしばらくすると消えるため、表示されたらすぐにコピーしてください。
3. 使用する予定の**仮想ネットワークゲートウェイ**に移動し、「**接続 > + 追加**」を選択します。
4. 「**接続の追加**」ページで、フィールドに値を入力し、「**OK**」を選択します。



接続は、ExpressRoute 回線と仮想ネットワークの間に確立されます。



AZURE VMWARE SOLUTION の DHCP を構成する

ExpressRouteを仮想ゲートウェイに接続した後、DHCPを構成します。
NSX-T を使用して DHCP サーバーをホストする
NSX-T マネージャーで:

1. 「**ネットワーク > DHCP**」を選択し、「**サーバーの追加**」を選択します。
2. 「**サーバーの種類**」に「**DHCP**」を選択し、サーバー名と IP アドレスを入力します。
3. 「**保存**」をクリックします。
4. 「**Tier 1 ゲートウェイ**」を選択し、Tier-1 ゲートウェイの縦の省略記号を選択してから、「**編集**」を選択します。
5. サブネットを追加するには、「**IP 割り当てなし**」を選択します。
6. 「**タイプ**」には「**DHCP Local Server**」を選択します。
7. 「**DHCP Server**」には「**Default DHCP**」を選択し、「**Save**」をクリックします。
8. もう一度「**Save**」をクリックし、「**Close Editing**」を選択します。

Azure ASV NSX-Tサーバーの追加(/en-us/citrix-virtual-apps-desktops/2407/media/azure-avs-nsx-t-add-server.png)

AZURE VMWARE SOLUTIONでネットワークセグメントを追加する

DHCPを設定した後、ネットワークセグメントを追加します。

ネットワークセグメントを追加するには、NSX-T Managerで**Networking> Segments**を選択し、**Add Segment**をクリックします。

Azure ASV NSX-Tセグメントの追加(/en-us/citrix-virtual-apps-desktops/2407/media/azure-avs-nsx-t-add-segment.png)

Segments profile画面で：

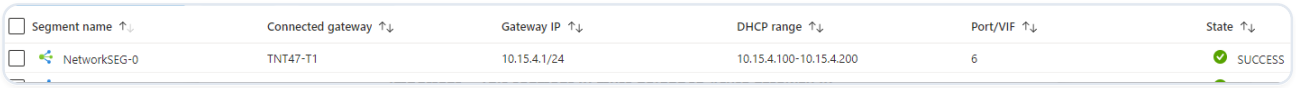
1. セグメントの「**名前**」を入力します。
2. 「**Connected Gateway**」として「**Tier-1 Gateway (TNTxx-T1)**」を選択し、「**Type**」は「**Flexible**」のままにします。
3. 事前構成されたオーバーレイ「**Transport Zone(TNTxx-OVERLAY-TZ)**」を選択します。
4. 「**Set Subnets**」をクリックします。

Azure ASV NSX-Tセグメントプロファイルの追加(/en-us/citrix-virtual-apps-desktops/2407/media/azure-avs-nsx-t-segment-profiles.png)

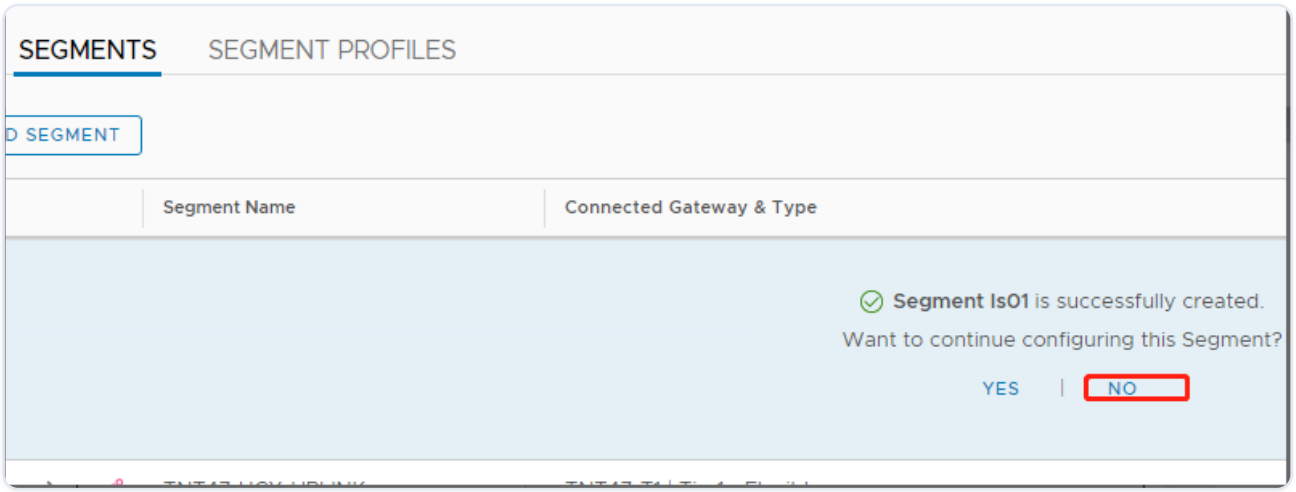
Subnetsセクションで：

1. ゲートウェイIPアドレスを入力します。
2. **Add**を選択します。

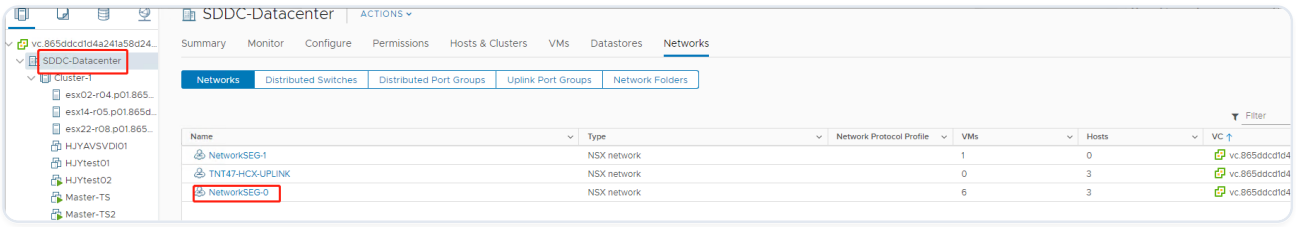
> **重要:**
>
> このセグメントのIPアドレスは、Azureゲートウェイ IPアドレス (10.15.0.0/22) に属している必要があります。
>
> DHCP範囲はセグメントIPアドレスに属している必要があります。



セグメントの構成を続行するオプションを拒否するには、 を選択します:

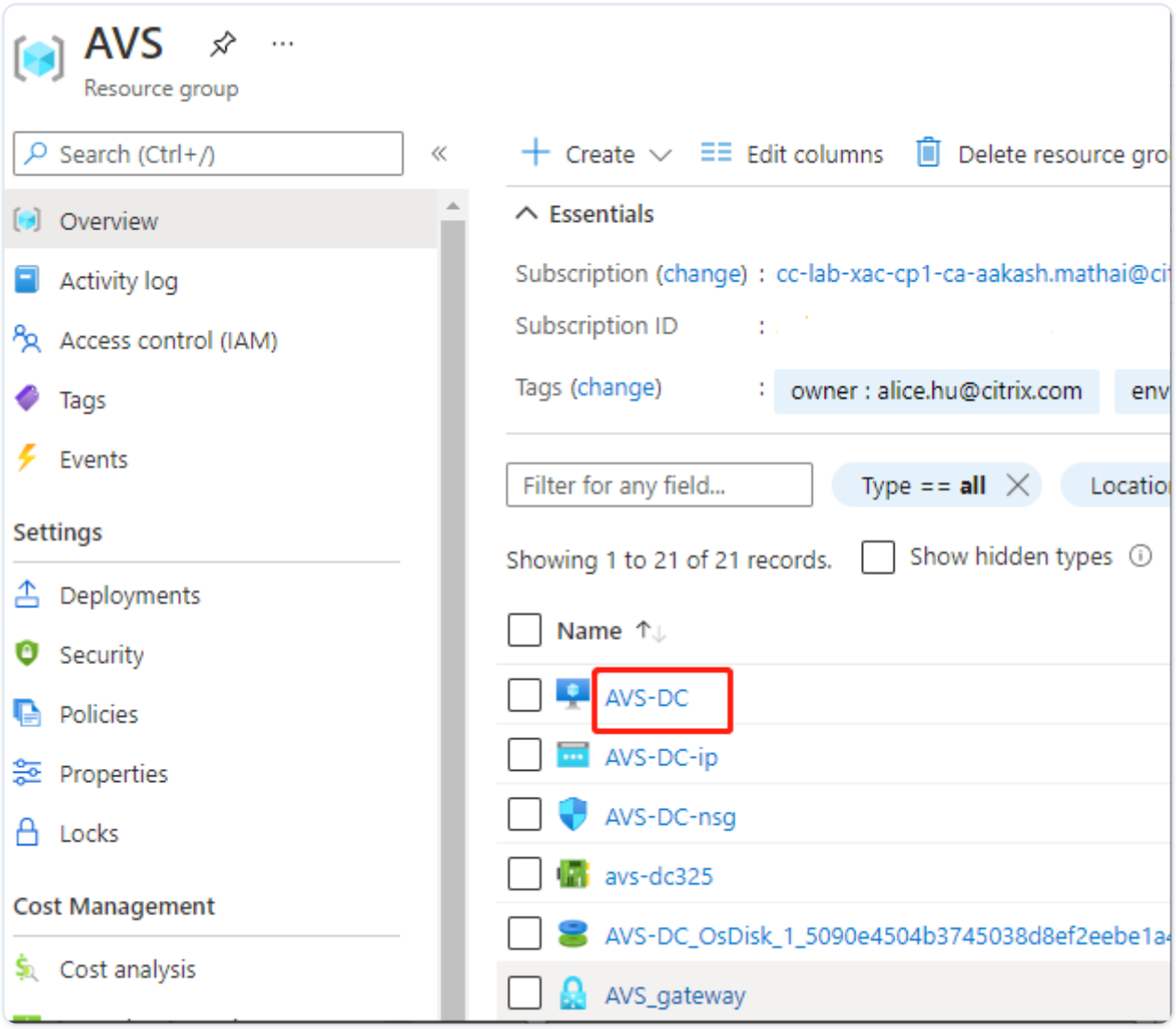


vCenterで、 **>** を選択します:

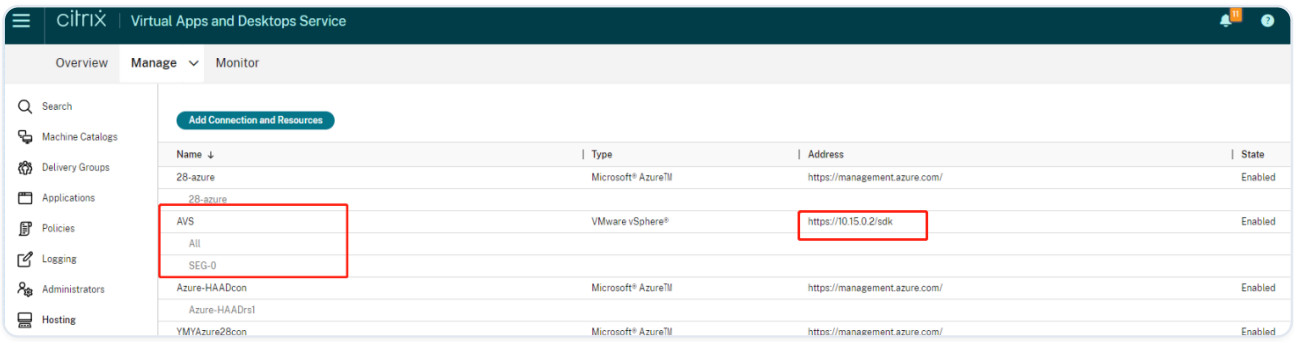


AZURE AVS環境の検証

Azureリソースグループで直接接続とコネクタを設定します。



vCenterの資格情報で接続を確認します。



グーグル クラウド ヴイエムウェア エンジン

Citrix Virtual Apps and Desktopsを使用すると、VMwareベースのオンプレミスCitrixワークロードをGoogle Cloud VMware Engineに移行できます。

Google Cloud VMware Engineを構成する

次の手順では、Google Cloud VMware Engine上にクラスターを取得してセットアップする方法について説明します。

VMWARE ENGINEポータルにアクセスする

1. **Google Cloud Console**で、ナビゲーションメニューをクリックします。
2. **Compute**セクションで、**VMware Engine**をクリックして、新しいブラウザータブでVMware Engineを開きます。

最初のプライベートクラウドを作成するための要件

Google Cloud VMware Engineへのアクセス、利用可能なVMware Engineノードクォータ、および適切なIAMロールが必要です。プライベートクラウドの作成を続行する前に、以下の要件を準備してください。

1. APIアクセスとノードクォータを要求します。詳細については、「APIアクセスとクォータの要求」を参照してください。
2. VMware管理アプライアンスとHCX展開ネットワークに使用するアドレス範囲をメモします。詳細については、「ネットワーク要件」を参照してください。
3. VMware Engine Service Admin IAMロールを取得します。

最初のプライベートクラウドを作成する

1. VMware Engineポータルにアクセスします。
2. VMware Engineのホームページで、**Create a private cloud**をクリックします。ホスティングの場所とハードウェアノードの種類が一覧表示されます。
3. プライベートクラウドのノード数を選択します。最低3つのノードが必要です。
4. VMware管理ネットワークのクラスレス・インタードメイン・ルーティング (CIDR) 範囲を入力します。
5. HCX展開ネットワークのCIDR範囲を入力します。

> **重要:**
>
> CIDR範囲は、オンプレミスまたはクラウドのサブネットと重複してはなりません。CIDR範囲は/27以上である必要があります。

6. を選択します。
7. 設定を確認します。設定を変更するには、 をクリックします。
8. をクリックして、プライベートクラウドの作成を開始します。

VMware Engineが新しいプライベートクラウドを作成すると、いくつかのVMwareコンポーネントが展開され、プライベートクラウド内のクラスターの初期Autoscale™ポリシーが設定されます。

プライベートクラウドの作成には30分から2時間かかる場合があります。プロビジョニングが完了すると、メールが届きます。

GOOGLE CLOUD VMWARE ENGINE VPNゲートウェイを設定する

Google Cloud VMware Engineへの初期接続を確立するには、VPNゲートウェイを使用できます。これはOpenVPNベースのクライアントVPNであり、これを使用してVMware Software Defined Data Center (SDDC) vCenterに接続し、必要な初期構成を行うことができます。

VPNゲートウェイを展開する前に、SDDCが展開されているリージョンの**Edge Services**範囲を構成します。これを行うには：

1. **Google Cloud VMware Engine**ポータルにログオンし、 **>** に移動します。 をクリックします。
2. SDDCが展開されているリージョンを選択し、 と を有効にします。
3. 計画中にメモしたEdge Services範囲を入力し、 をクリックします。これらのサービスを有効にするには10〜15分かかります。

   完了すると、リージョン設定ページでEdge Servicesが**** と表示されます。これらの設定を有効にすると、SDDCにパブリックIPを割り当てることができ、これはVPNゲートウェイを展開するための要件です。

VPNゲートウェイを展開するには：

1. **Google Cloud VMware Engine**ポータルで、**ネットワーク > VPNゲートウェイ**に移動します。**新しいVPNゲートウェイを作成**をクリックします。
2. VPNゲートウェイの名前と、計画中に予約したクライアントサブネットを入力します。**次へ**をクリックします。
3. VPNアクセスを許可するユーザーを選択します。**次へ**をクリックします。
4. VPN経由でアクセス可能にする必要があるネットワークを指定します。**次へ**をクリックします。
5. 概要画面が表示されます。選択内容を確認し、**送信**をクリックしてVPNゲートウェイを作成します。VPNゲートウェイページには、新しいVPNゲートウェイのステータスが**作成中**と表示されます。
6. ステータスが**稼働中**に変わったら、新しいVPNゲートウェイをクリックします。
7. **VPN構成をダウンロード**をクリックして、VPNゲートウェイ用の事前設定済みOpenVPNプロファイルを含むZIPファイルをダウンロードします。UDP/1194およびTCP/443経由で接続するためのプロファイルが利用可能です。好みのものを選択してOpen VPNにインポートし、接続します。

8. **リソース**に移動し、SDDCを選択します。

VPNを接続する

1. VPNゲートウェイの設定を通じて、オンプレミスネットワークとプライベートクラウド間のポイントツーサイト接続を確立します。Google Cloud VMware Engine VPNゲートウェイを設定するを参照してください。
2. Google Cloud VMware Engine VPNゲートウェイを設定するでダウンロードしたVPN構成をアップロードします。
3. VPNクライアント（例：OpenVPN Connect）にインポートします。

詳細については、VPNを使用した接続を参照してください。

最初のサブネットを作成する

VMware EngineポータルからNSX-T Managerにアクセスする
サブネットの作成プロセスはNSX-Tで行われ、VMware Engineを介してアクセスします。NSX-T Managerにアクセスするには、次の手順を実行します。

1. **Google Cloud VMware Engine**ポータルにログオンします。
2. メインナビゲーションから、**リソース**に移動します。
3. サブネットを作成するプライベートクラウドに対応する**プライベートクラウド名**をクリックします。
4. プライベートクラウドの詳細ページで、**vSphere Management Network**タブをクリックします。
5. NSX-T Managerに対応する**FQDN**をクリックします。
6. プロンプトが表示されたら、サインイン資格情報を入力します。vIDMを設定し、Active DirectoryなどのIDソースに接続している場合は、代わりにIDソースの資格情報を使用します。

> **注意：**
>
> 生成された資格情報は、プライベートクラウドの詳細ページから取得できます。

サブネットのDHCPサービスを設定する
サブネットを作成する前に、DHCPサービスを設定します。

NSX-T マネージャーで：

1. **ネットワーク > DHCP**に移動します。ネットワークダッシュボードには、DHCPサービスが1つのTier-0と1つのTier-1ゲートウェイを作成することが示されます。
2. DHCPサーバーのプロビジョニングを開始するには、「**Add Server**」をクリックします。
3. 「**Server Type**」で「**DHCP**」を選択し、サーバー名とIPアドレスを入力します。
4. DHCPサービスを作成するには、「**Save**」をクリックします。

このDHCPサービスを関連するTier-1ゲートウェイにアタッチするには、次の手順を実行します。デフォルトのTier-1ゲートウェイは、DHCPサービスによってすでにプロビジョニングされています。

1. 「**Tier 1 Gateways**」を選択し、Tier-1ゲートウェイの縦の省略記号を選択してから、「**Edit**」を選択します。
2. 「**IP Address Management**」フィールドで、「**No IP Allocation Set**」を選択します。
3. 「**Type**」で「**DHCP Local Server**」を選択します。
4. 「**DHCP Server**」で、作成したDHCPサーバーを選択します。
5. 「**Save**」をクリックします。
6. 「**Close Editing**」をクリックします。

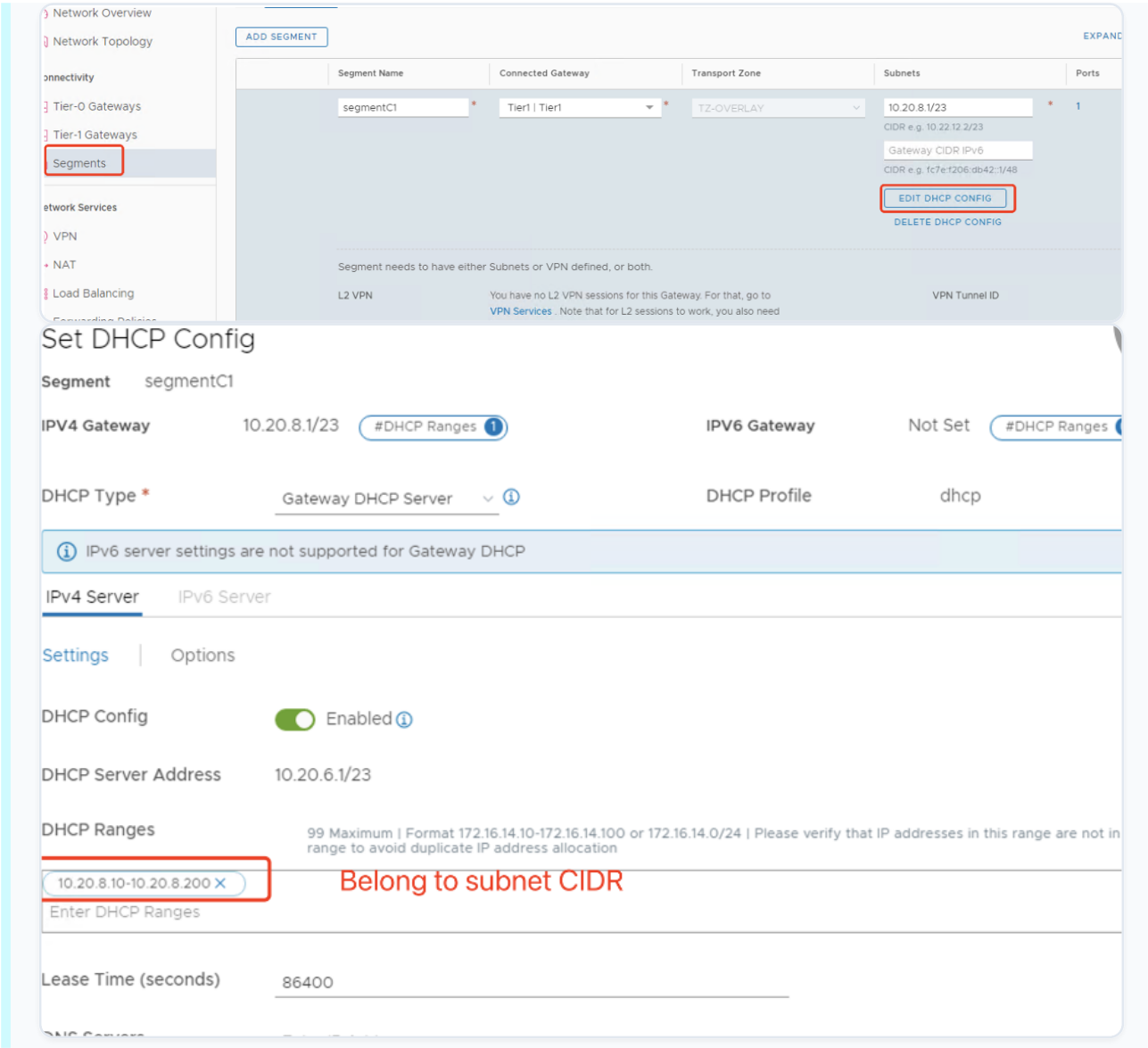
これで、NSX-T でネットワークセグメントを作成できます。NSX-T の DHCP の詳細については、DHCP に関する VMware ドキュメントを参照してください。
NSX-T でネットワークセグメントを作成する
ワークロード VM の場合、プライベートクラウドの NSX-T ネットワークセグメントとしてサブネットを作成します。

1. NSX-T Managerで、「**Networking > Segments**」に移動します。
2. 「**Add Segment**」をクリックします。
3. セグメントの名前を入力します。
4. **Connected Gateway**として**Tier-1**を選択し、Typeは**Flexible**のままにします。
5. **Set Subnets**をクリックします。
6. **Add Subnets**をクリックします。
7. **Gateway IP/Prefix Length**にサブネット範囲を入力します。最後のオクテットを**.1**としてサブネット範囲を指定します。例: **10.12.2.1/24**。
8. DHCP範囲を指定し、**ADD**をクリックします。
9. 「**Transport Zone**」で、ドロップダウンリストから「**TZ-OVERLAY**」を選択します。

10. **Save**をクリックします。これで、VMの作成時にvCenterでこのネットワークセグメントを選択できるようになります。

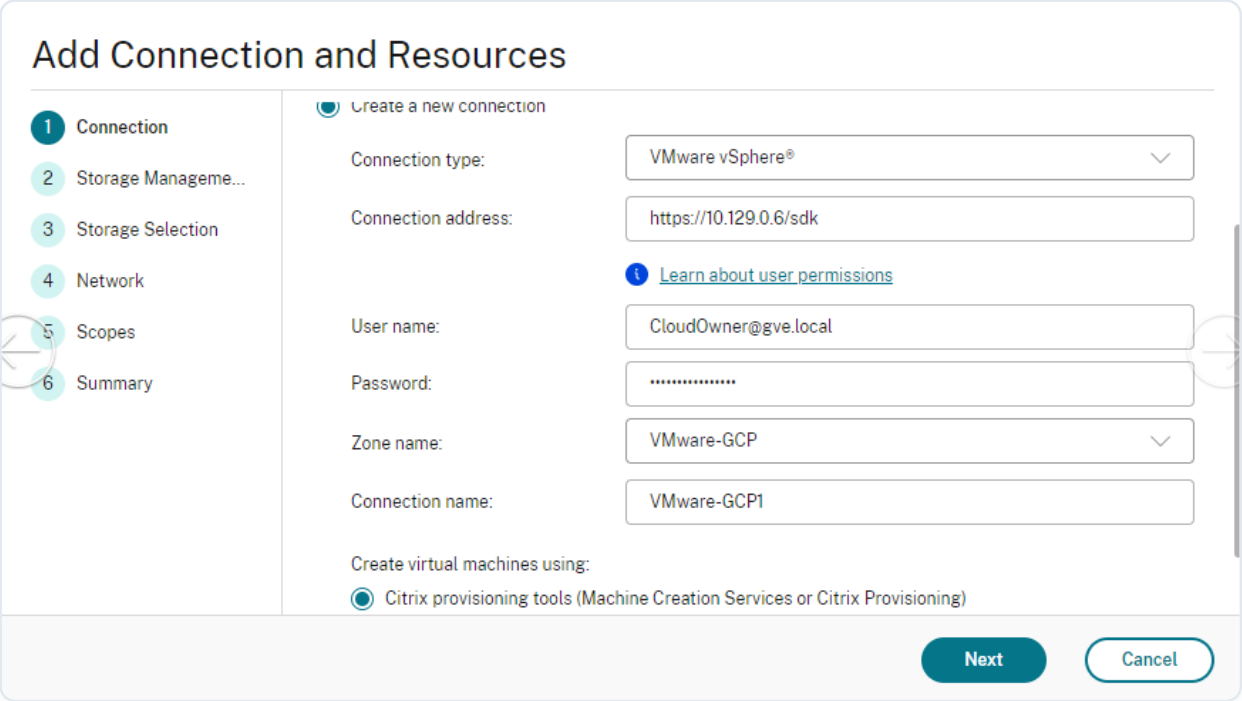
特定のリージョンでは、プライベートサービスアクセスを使用して、VMware EngineからVPCネットワークへの一意のルートを最大100個設定できます。これには、たとえば、プライベートクラウド管理IPアドレス範囲、NSX-Tワークロードネットワークセグメント、およびHCXネットワークIPアドレス範囲が含まれます。この制限には、リージョン内のすべてのプライベートクラウドが含まれます。

> **注：**
>
> Google Cloudの構成の問題により、DHCP範囲設定を複数回構成する必要があります。したがって、Google Cloudの構成後にDHCP範囲設定を構成するようにしてください。DHCP範囲を構成するには、**EDIT DHCP CONFIG**をクリックします。



CITRIX STUDIOでGOOGLE CLOUD VMWARE接続を作成する

1. vCenterでマシンを作成します。
2. Citrix Studioを起動します。
3. ホスティングノードを選択し、**接続とリソースの追加**をクリックします。
4. **接続**画面で、**新しい接続の作成**を選択し、以下の詳細を入力します。



a. 「**Connection type**」として「**VMware vSphere**」を選択します。

b. 「**接続アドレス**」にvCenterのプライベートIPアドレスを入力します。

c. vCenterの資格情報を入力します。

d. 接続名を入力します。

e. 仮想マシンを作成するツールを選択します。

5. **ネットワーク**画面で、NSX-Tサーバーで作成されたサブネットを選択します。
6. ウィザードを完了します。

Amazon Web Services (AWS) 上のVMware クラウド

Amazon Web Services (AWS) 上のVMware Cloudを使用すると、VMwareベースのオンプレミスCitrixワークロードをAWS Cloudに移行できます。

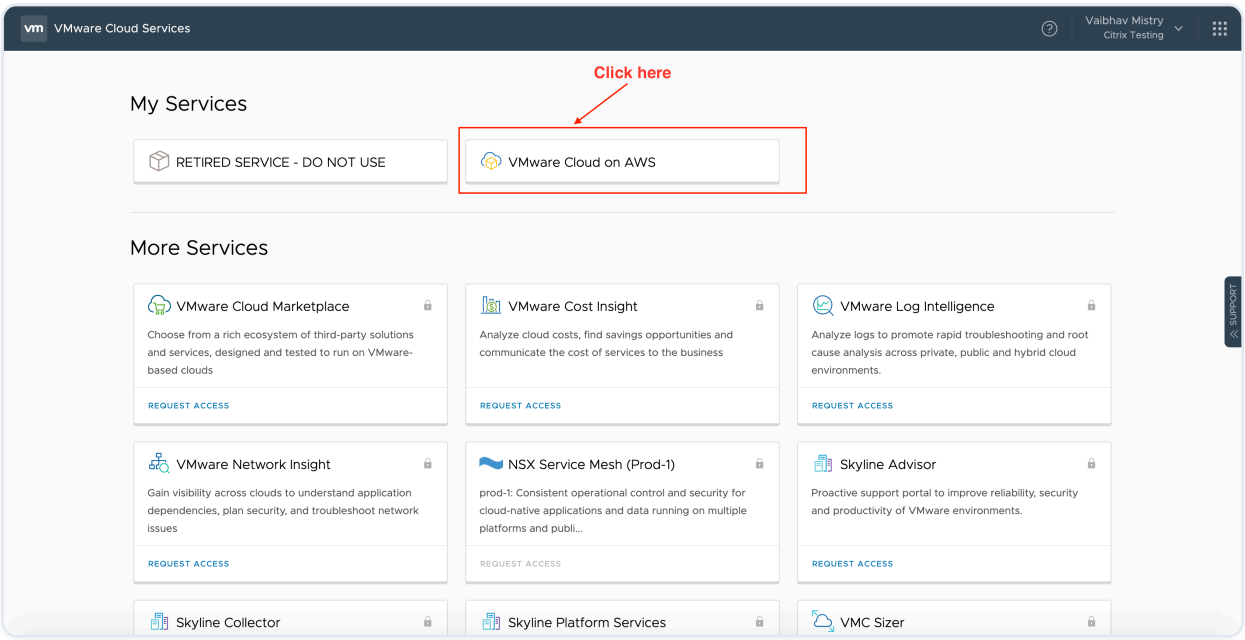
この記事では、AWS上にVMware Cloudをセットアップする手順について説明します。

VMware Cloud環境にアクセスする

1. URL `<https://console.cloud.vmware.com/>` を使用してVMware Cloudサービスにログインします。

   VMware クラウドサービスログイン(/en-us/citrix-virtual-apps-desktops/2407/media/vmc-login.png)

2. **VMware Cloud on AWS** をクリックします。Software-Defined Data Centers (SDDC) ページが表示されます。



3. **OPEN VCENTER** をクリックし、次に **SHOW CREDENTIALS** をクリックします。後で使用するために資格情報をメモしておきます。

   vCenter を開く(/en-us/citrix-virtual-apps-desktops/2407/media/vmc-sddc.png)

   資格情報を表示(/en-us/citrix-virtual-apps-desktops/2407/media/show-credentials-vmc.png)

4. Webブラウザを開き、vSphere Web Client のURLを入力します。
5. メモした資格情報を入力し、**Login** をクリックします。vSphere クライアントのWebページは、オンプレミス環境のものと似ています。

   vSphere クライアントのWebページ(/en-us/citrix-virtual-apps-desktops/2407/media/vcenter-page.png)

VMware クラウド環境について

vSphere クライアントのWebページには、4つのビューがあります。

- ホストとクラスタービュー: 新しいクラスターを作成することはできませんが、クラウド管理者は複数のリソースプールを作成できます。

  ホストとクラスタービュー(/en-us/citrix-virtual-apps-desktops/2407/media/host-cluster-view.png)

- VMとテンプレートビュー: クラウド管理者は多くのフォルダーを作成できます。

  VMとテンプレートビュー(/en-us/citrix-virtual-apps-desktops/2407/media/vm-template-view.png)

- ストレージビュー: Citrix Studioでホスティングユニットを追加する際、**WorkloadDatastore**ストレージを選択してください。Workload Datastoreにのみアクセスできるためです。

  「ストレージビュー」(/en-us/citrix-virtual-apps-desktops/2407/media/storage-view.png)

- ネットワークビュー: VMwareクラウドネットワークと不透明なネットワークでは、アイコンが異なります。

  「ネットワークビュー」(/en-us/citrix-virtual-apps-desktops/2407/media/network-view.png)

クラスターをセットアップした後、接続とリソースを追加するには、VMware仮想化環境を参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- 接続の作成と管理については、「VMware CloudおよびパートナーソリューションへのConnecting」を参照してください。

詳細情報

- 接続とリソースを作成および管理する
- マシンカタログを作成する

コアコンポーネントをインストールする

> **重要:**

> Citrix は、ライセンスコンプライアンスを含む正当な利益のために、基本的なライセンスデータを収集します。詳細については、「Citrix Licensing Data」(/ja-jp/licensing/current-release/license-server/licensing-data-collection-programs.html)を参照してください。

> コアコンポーネントは、Citrix Delivery Controller™、Citrix Studio、Web Studio、Citrix Director、および Citrix License Server です。

> **注:**

> Citrix Studio は、オンプレミスの Citrix Virtual Apps and Desktops 展開を構成および管理できる Windows ベースの管理コンソールです。Web Studio は Citrix Studio の次世代版であり、Citrix Studio と完全に同等の機能を備えた Web ベースの管理コンソールです。Web Studio の詳細については、「Web Studio のインストール」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/install-core/install-web-studio.html)を参照してください。

> (2003 より前のバージョンでは、コアコンポーネントに Citrix StoreFront が含まれていました。**Citrix StoreFront** タイルをクリックするか、インストールメディアで利用可能なコマンドを実行することで、StoreFront をインストールできます。)

インストールを開始する前に、この記事と「インストール準備」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/install-prepare.html)を確認してください。

この記事では、コアコンポーネントをインストールする際のインストールウィザードのシーケンスについて説明します。コマンドラインの同等機能も提供されています。詳細については、「コマンドラインを使用したインストール」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/install-command.html)を参照してください。

ステップ 1. 製品ソフトウェアをダウンロードしてウィザードを起動する

Citrix アカウントの資格情報を使用して、Citrix Virtual Apps and Desktops™ のダウンロードページにアクセスします。製品の ISO ファイルをダウンロードします。

ファイルを解凍します。必要に応じて、ISO ファイルを DVD に書き込みます。

コアコンポーネントをインストールするマシンに、ローカル管理者アカウントを使用してログオンします。

DVD をドライブに挿入するか、ISO ファイルをマウントします。インストーラーが自動的に起動しない場合は、**AutoSelect** アプリケーションまたはマウントされたドライブをダブルクリックします。

ステップ 2. インストールする製品を選択する



インストールする製品（Virtual AppsまたはVirtual Apps and Desktops）の横にある**開始**をクリックします。

(マシンにCitrix Virtual Apps and Desktopsコンポーネントがすでにインストールされている場合、このページは表示されません。)

コマンドラインオプション: Citrix Virtual Appsをインストールするには`/xenapp`。オプションを省略すると、Citrix Virtual Apps and Desktopsがインストールされます。

ステップ3. インストールするコンポーネントを選択する

コンポーネントインストーラーのコンポーネント選択ページ(/en-us/citrix-virtual-apps-desktops/2407/media/what-to-install-2.png)

初めての場合は、**Delivery Controller**を選択します。（後のページで、このマシンにインストールする特定のコンポーネントを選択します。）

すでにControllerをインストールしている場合（このマシンまたは別のマシンに）、別のコンポーネントをインストールするには、**展開の拡張**セクションからコンポーネントを選択します。

コマンドラインオプション: `/components`

ステップ4. ライセンス契約を読んで同意する

コンポーネントインストーラーのライセンス契約ページ(/en-us/citrix-virtual-apps-desktops/2407/media/core-license-75.png)

ライセンス契約ページで、ライセンス契約を読んだ後、それを読んで同意したことを示します。次に、**次へ**をクリックします。

ステップ5. インストールするコンポーネントとインストール場所を選択する

コンポーネントインストーラーのコアコンポーネントページ(/en-us/citrix-virtual-apps-desktops/2407/media/core-components-75.png)

コアコンポーネントページで、:

- **場所:** デフォルトでは、コンポーネントは`C:\Program Files\Citrix`にインストールされます。ほとんどの展開では、デフォルトで問題ありません。別の場所を指定する場合、その場所にはネットワークサービスに対する実行権限が必要です。
- **コンポーネント:** デフォルトでは、すべてのコアコンポーネントのチェックボックスが選択されています。概念実証、テスト、または小規模な本番展開では、すべてのコアコンポーネントを1台のサーバーにインストールしても問題ありません。大規模な本番環境では、CitrixはDirector、StoreFront、Secure Private Access、およびLicense Serverを別々のサーバーにインストールすることを推奨しています。

> **注:**
>
> 複数のサーバーにコンポーネントをインストールする場合は、他のサーバーに他のコンポーネントをインストールする前に、Citrix License Server とライセンスを最初にインストールしてください。ガイダンスについては、Citrix Virtual Apps and Desktops のライセンスガイド の「自動インストール」セクションを参照してください。

> このマシンに必須のコアコンポーネントをインストールしないことを選択した場合、アイコンで警告が表示されます。この警告は、そのコンポーネントをインストールする必要があることを通知しますが、必ずしもこのマシンにインストールする必要があるわけではありません。

Nextをクリックします。

コマンドラインオプション: `/installdir`、`/components`、`/exclude`

ハードウェアチェック

Delivery Controller をインストールまたはアップグレードすると、ハードウェアがチェックされます。マシンに推奨される RAM 容量 (5 GB) より少ない場合、インストーラーは警告を表示します。これはサイトの安定性に影響を与える可能性があります。詳細については、「ハードウェア要件」を参照してください。

グラフィカルインターフェイス: ダイアログボックスが表示されます。

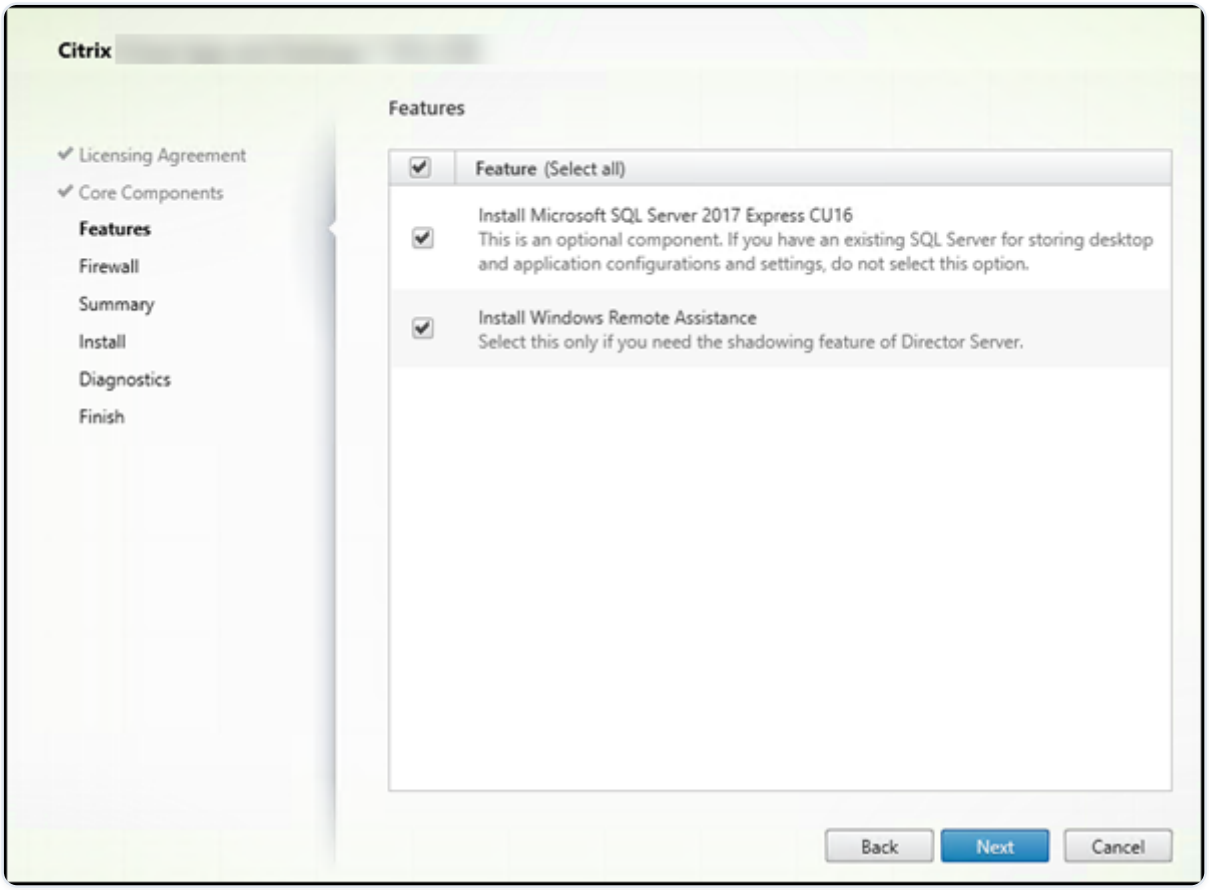
- 推奨: **キャンセル**をクリックしてインストールを停止します。マシンにRAMを追加してから、再度インストールを開始してください。
- または、**次へ**をクリックしてインストールを続行します。サイトの安定性に問題が生じる可能性があります。

コマンドラインインターフェイス: インストール/アップグレードが終了します。インストールログには、検出された内容と利用可能なオプションを説明するメッセージが含まれています。

- 推奨: マシンにRAMを追加してから、再度コマンドを実行してください。
- または、`/ignore_hw_check_failure`オプションを指定してコマンドを再度実行し、警告を上書きします。サイトの安定性に問題が生じる可能性があります。

アップグレード時に、OSまたはSQL Serverのバージョンがサポートされなくなった場合も通知されます。「展開のアップグレード」を参照してください(/ja-jp/citrix-virtual-apps-desktops/2407/upgrade-migrate/upgrade.html)。

手順 6. 機能の有効化または無効化



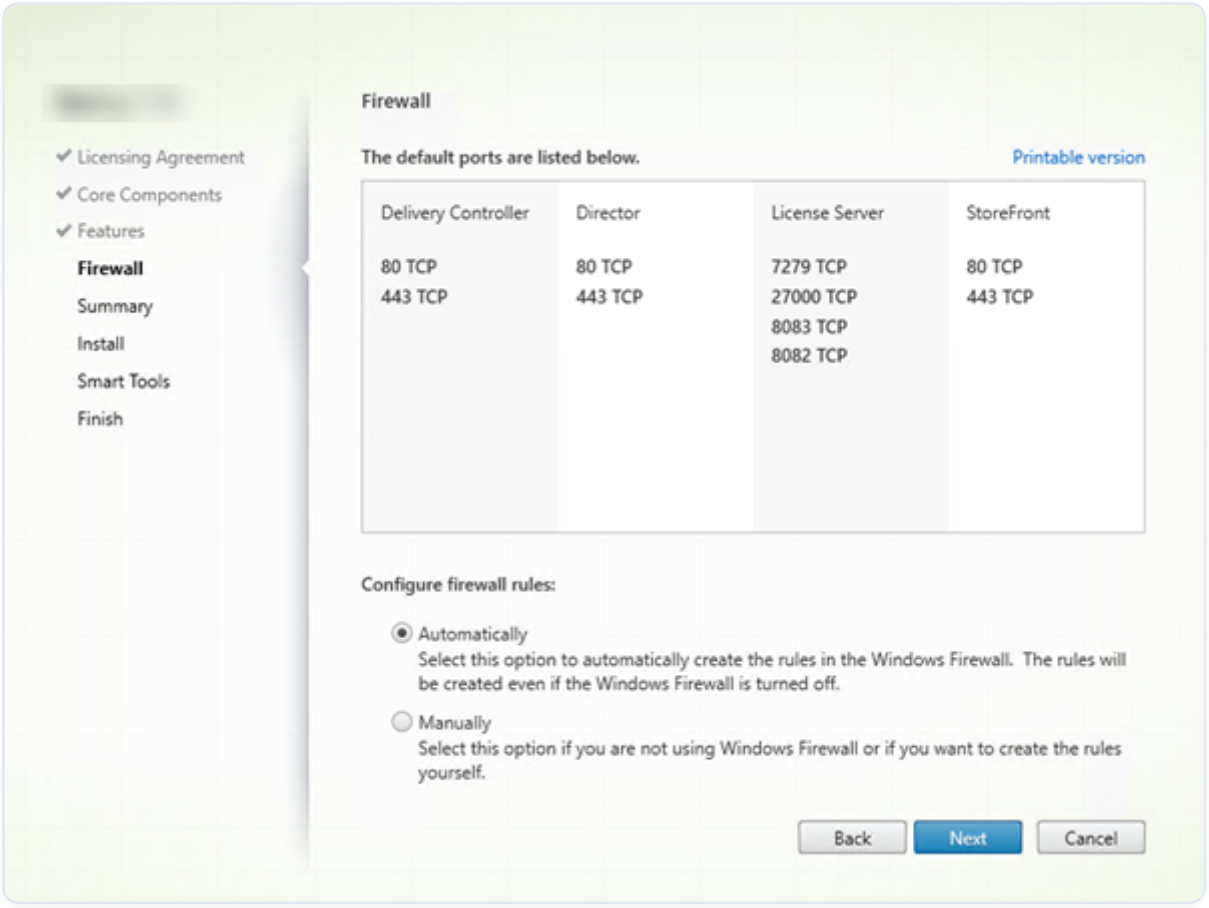
ページで:

- サイトデータベースとして使用するためにMicrosoft SQL Server Expressをインストールするかどうかを選択します。デフォルトでは、この選択は有効になっています。Citrix Virtual Apps and Desktopsデータベースに慣れていない場合は、「データベース」を参照してください(/ja-jp/citrix-virtual-apps-desktops/2407/technical-overview/databases.html)。
- Directorをインストールすると、Windowsリモートアシスタンスが自動的にインストールされます。Directorのユーザーシャドウイングで使用するために、Windowsリモートアシスタンスでシャドウイングを有効にするかどうかを選択します。シャドウイングを有効にすると、TCPポート3389が開きます。デフォルトでは、この機能は有効になっています。ほとんどの展開では、デフォルト設定で問題ありません。この機能は、Directorをインストールしている場合にのみ表示されます。

をクリックします。

コマンドラインオプション: `/nosql` (インストールを防止するため)、`/no_remote_assistance` (有効化を防止するため)

手順7. Windowsファイアウォールポートを開く



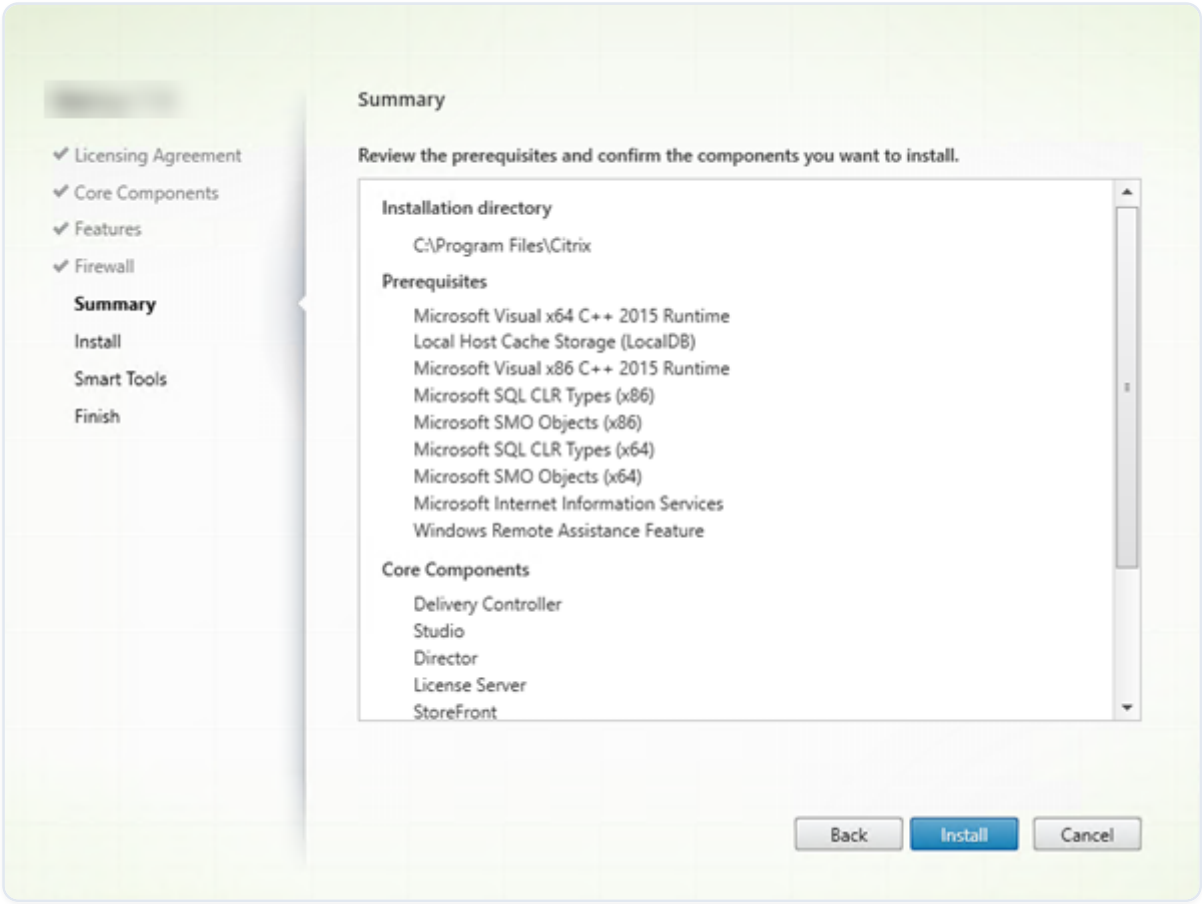
デフォルトでは、Windowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても、 ページのポートは自動的に開かれます。ほとんどの展開では、デフォルト設定で問題ありません。ポート情報については、「ネットワークポート」を参照してください(/ja-jp/tech-zone/build/tech-papers/citrix-communication-ports.html#citrix-virtual-apps-and-desktops)。

をクリックします。

(このグラフィックは、このマシンにすべてのコアコンポーネントをインストールしたときのポートリストを示しています。この種のインストールは、通常、テスト展開のみを対象としています。)

コマンドラインオプション: `/configure_firewall`

手順8. 前提条件を確認し、インストールを確定する



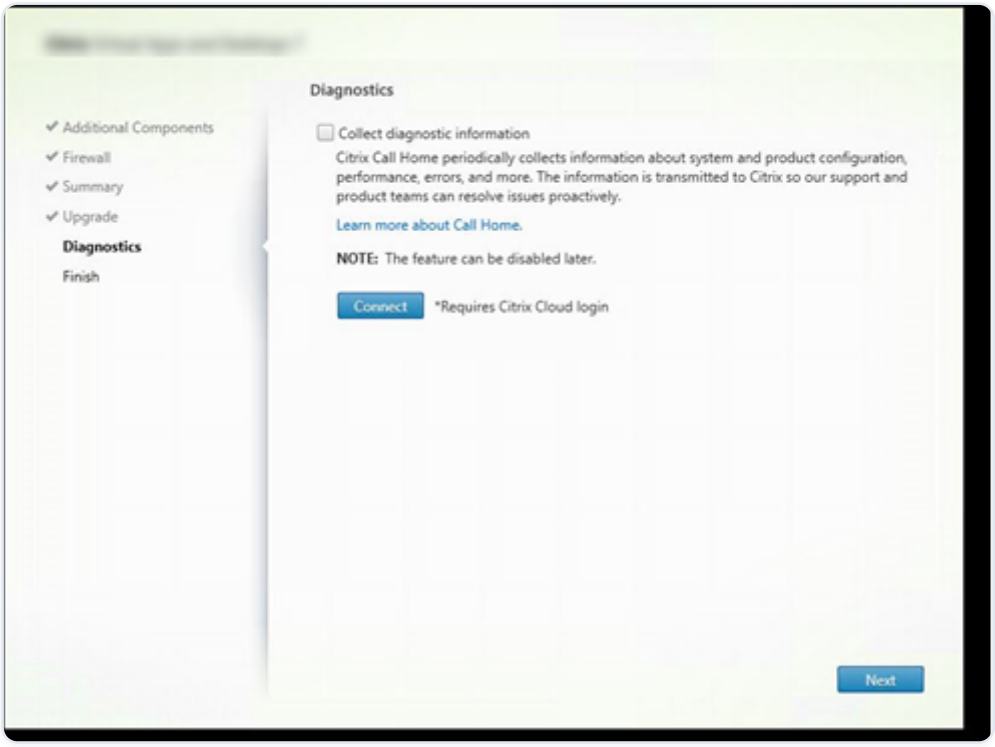
「**概要**」ページには、インストールされるものが表示されます。「**戻る**」ボタンを使用して、必要に応じて以前のウィザードページに戻り、選択を変更します。

準備ができたら、「**インストール**」をクリックします。

ディスプレイにはインストールの進行状況が表示されます。

コンポーネントのインストール中の進行状況表示(/en-us/citrix-virtual-apps-desktops/2407/media/core-during-install-75.png)

ステップ9. 診断情報をCloud Software Groupと共有する



「**診断**」ページで、Citrix Call Homeに参加するかどうかを選択します。

このページは、グラフィカルインターフェイスを使用してDelivery Controllerをインストールするときに表示されます。StoreFrontをインストールする場合（Controllerではない場合）、ウィザードはこのページを表示します。他のコアコンポーネントをインストールする場合（ControllerまたはStoreFrontではない場合）、ウィザードはこのページを表示しません。

アップグレード中に、Call Homeがすでに有効になっている場合、またはインストーラーがCitrix Telemetry Serviceに関連するエラーを検出した場合、このページは表示されません。

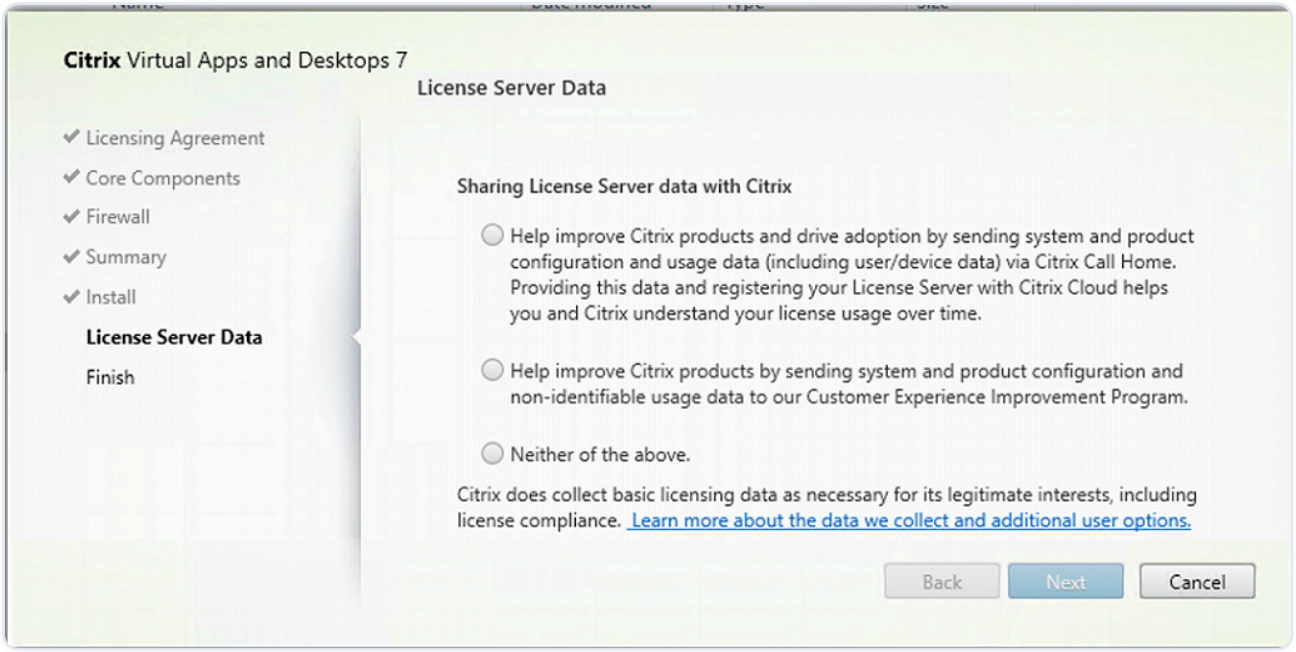
参加することを選択した場合（デフォルト）、**接続**をクリックします。プロンプトが表示されたら、Citrixアカウントの資格情報を入力します。登録の選択は、インストール後に変更できます。

資格情報が検証された後（または参加しないことを選択した場合）、「**次へ**」をクリックします。

「**診断**」ページで、最初に「**診断情報の収集**」を選択せずに「**接続**」をクリックすると、「**Connect to Citrix Insight Services**」ダイアログを閉じた後、「**次へ**」ボタンが無効になります。次のページに進むことはできません。「**次へ**」ボタンを再度有効にするには、「**診断情報の収集**」を選択し、すぐに選択を解除します。

詳細については、「Call Home」を参照してください。

ステップ10. ライセンスサーバーデータをCloud Software Groupと共有する



ライセンスサーバーデータ ページでは、弊社を支援するために、Call Home データまたはカスタマーエクスペリエンス向上プログラム (CEIP) データのいずれかを共有するようお願いしています。さらに、Cloud Software Group は、正当な利益のために必要に応じて、ライセンスコンプライアンスを含む基本的なライセンスデータの収集も要求します。

ライセンスサーバーデータ ページは、License Server をインストールすると表示されます。

- スタンドアロンとして。
- Delivery Controllerのインストール中に、コアコンポーネントとして。

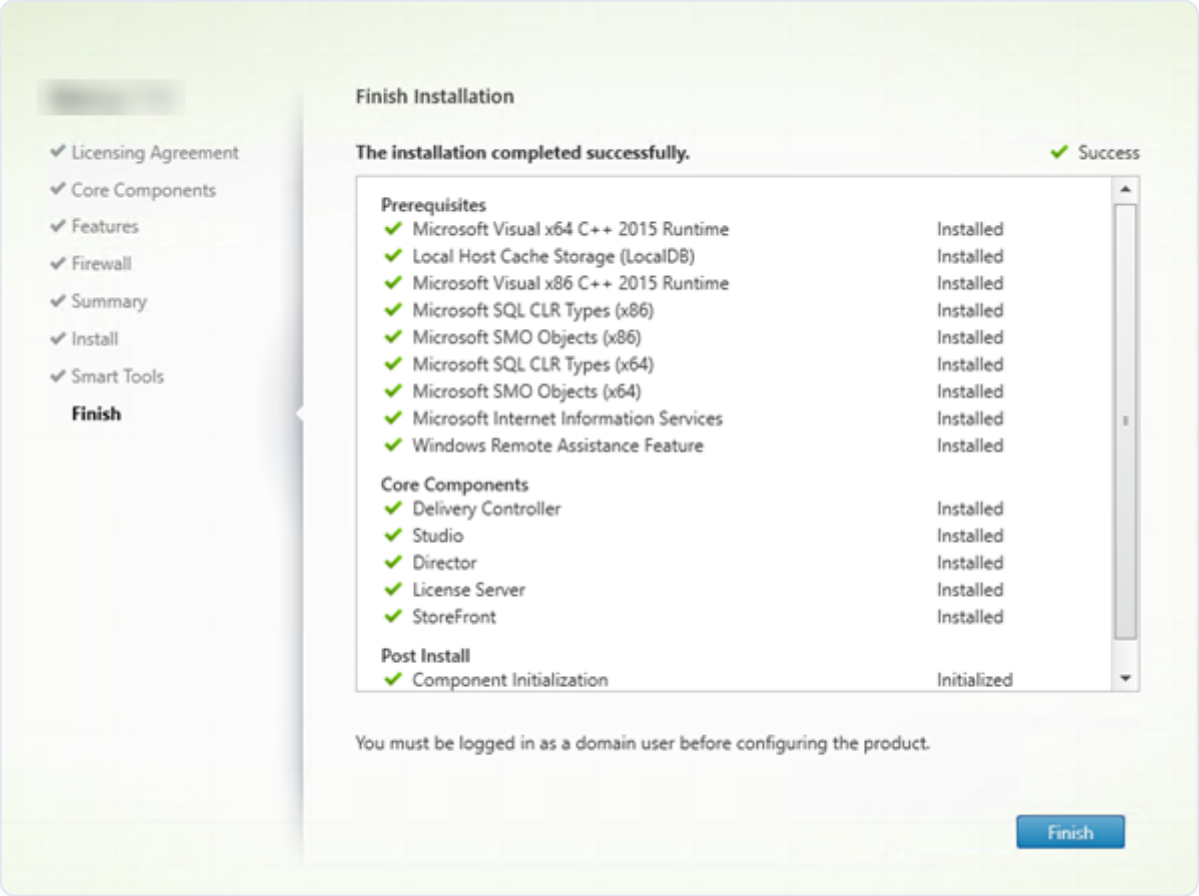
アップグレード中、構成がすでに `/CITRIX.opt:` ファイルで設定されている場合、このページは表示されません。

License Server は、ライセンスデータ、Call Home データ、CEIP データなど、いくつかの種類のユーザーデータを監視します。Call Home データと CEIP データの収集を有効にするには、参加を選択 (オプトイン) する必要があります。

コマンドラインを使用してインストールする際の Call Home および CEIP データ収集を有効にする方法の詳細については、「コアコンポーネントをインストールするためのコマンドラインオプション」を参照してください。

Cloud Software Groupのライセンスデータ収集の詳細については、「Citrixライセンスデータ収集プログラム」を参照してください。

手順 11. このインストールを完了する



完了 ページには、正常にインストールおよび初期化されたすべての前提条件とコンポーネントに対して緑色のチェックマークが表示されます。

完了 をクリックします。

手順 12. 残りのコアコンポーネントを他のマシンにインストールする

すべてのコアコンポーネントを 1 台のマシンにインストールした場合は、「次の手順」に進みます。そうでない場合は、他のマシンでインストーラーを実行して他のコンポーネントをインストールします。他のサーバーにさらに Controller をインストールすることもできます。

次のステップ

必要なすべてのコンポーネントをインストールした後、Studio を使用してサイトを作成(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/site-create.html)します。

サイトを作成した後、VDA をインストール(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/install-vdas.html)します。

いつでも、フルプロダクトインストーラーを使用して、以下のコンポーネントで展開を拡張できます。

- **Universal Print Serverサーバーコンポーネント:** プリントサーバーでインストーラーを起動します。

  a. **展開の拡張**セクションで**Universal Print Server**を選択します。

  b. ライセンス契約に同意します。

  c. **ファイアウォール**ページで、デフォルトでは、Windows ファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても、TCPポート7229と8080がファイアウォールで開かれます。ポートを手動で開きたい場合は、このデフォルトのアクションを無効にできます。

  コマンドラインからこのコンポーネントをインストールするには、「Universal Print Serverをインストールするためのコマンドラインオプション(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/install-command.html#command-line-options-for-installing-a-universal-print-server)」を参照してください。

- フェデレーション認証サービス(/ja-jp/federated-authentication-service.html)。
- セッション録画(/ja-jp/session-recording.html)。
- ワークスペース環境管理。

コマンドラインを使用したインストール

> **重要:**
>
> - アップグレードする場合で、現在のバージョンがPersonal vDiskまたはAppDisksソフトウェアを使用しているか、インストールされている場合は、「PvD、AppDisks、およびサポートされていないホストの削除」を参照してください。
> - Citrixは、ライセンスコンプライアンスを含む正当な利益のために、必要に応じて基本的なライセンスデータを収集します。詳細については、「Citrixライセンスデータ」を参照してください。

はじめに

この記事は、Windowsオペレーティングシステムを搭載したマシンにコンポーネントをインストールする場合に適用されます。Linuxオペレーティングシステム用VDAについては、「Linux Virtual Delivery Agents」を参照してください。

この記事では、製品のインストールコマンドを発行する方法について説明します。インストールを開始する前に、「インストールの準備」を確認してください。この記事には、利用可能なインストーラーの説明が含まれています。

コマンドの実行状況と戻り値を確認するには、元の管理者であるか、**管理者として実行**を使用する必要があります。詳細については、Microsoftのコマンドドキュメントを参照してください。

インストールコマンドを直接使用することに加えて、Active Directory内のマシンにVDAをインストール、アップグレード、または削除するサンプルスクリプトが製品ISOに用意されています。詳細については、「スクリプトを使用したVDAのインストール」を参照してください。

このCitrix Virtual Apps and Desktopsのバージョンでサポートされていないバージョンにインストールまたはアップグレードしようとすると、オプションに関する情報を示すメッセージが表示されます。「以前のオペレーティングシステム」を参照してください。

Citrixがコンポーネントのインストール結果を報告する方法については、「Citrixインストールの戻りコード」を参照してください。

フル製品インストーラーを使用する

フル製品インストーラーのコマンドラインインターフェイスにアクセスするには：

1. Citrixから製品パッケージをダウンロードします。ダウンロードサイトにアクセスするには、Citrixアカウントの資格情報が必要です。
2. ファイルを解凍します。必要に応じて、ISOファイルをDVDに書き込みます。
3. コンポーネントをインストールするサーバーに、ローカル管理者アカウントを使用してログオンします。
4. DVDをドライブに挿入するか、ISOファイルをマウントします。
5. メディアの `\x64\XenDesktop Setup` ディレクトリから、適切なコマンドを実行します。

   コアコンポーネントをインストールするには: `XenDesktopServerSetup.exe` を実行します。オプションについては、コアコンポーネントのインストール用コマンドラインオプション を参照してください。

   VDAをインストールするには: `XenDesktopVDASetup.exe` を実行します。オプションについては、VDAのインストール用コマンドラインオプション を参照してください。

   StoreFrontをインストールするには: インストールメディアの `x64 > StoreFront` フォルダーで `CitrixStoreFront-x64.exe` を実行します。

Universal Print Serverをインストールするには: Universal Print Serverのインストール用コマンドラインオプション のガイダンスに従ってください。

Federated Authentication Serviceをインストールするには： Citrixでは、グラフィカルインターフェイスを使用することをお勧めします。

Session Recordingをインストールするには: Session Recording のガイダンスに従ってください。

Workspace Environment Managementをインストールするには： Workspace Environment Managementのガイダンスに従ってください。

Secure Private Accessをインストールするには： インストールメディアの `x64 > XenDesktop` Setupフォルダーで `XenDesktopSPASetup.exe` を実行します。Secure Private Accessのインストールに関するコマンドラインオプションのガイダンスに従ってください。

コアコンポーネントのインストール用コマンドラインオプション

`XenDesktopServerSetup.exe` コマンドを使用してコアコンポーネントをインストールする場合、以下のパラメーターオプションが有効です。オプションの詳細については、コアコンポーネントのインストールを参照してください。

注:

- コアコンポーネントをインストールするためのコマンドラインオプションを使用している間は、`/exclude` を使用しないでください。
- `/components` を使用して1つのコンポーネントをアップグレードすると、他のコンポーネントもアップグレードされる場合があります。これは、異なるコンポーネント間の潜在的な互換性の問題を回避するためです。
- 1つのコンポーネントのみをアップグレードする場合は、そのコンポーネントの個別のインストーラーを使用してください。展開のアップグレード を参照してください。

- ***/ceipoptin*** *CEIPオプトイン設定 ...*

  Call Homeデータおよびカスタマーエクスペリエンス向上プログラム (CEIP) データの収集を有効にします。有効な値は次のとおりです。

  - `DIAGNOSTIC`: Citrix LicensingがCall Homeデータを収集できるようにするには、この値を選択します。

- `ANONYMOUS`: Citrix Licensingが未識別のCEIPデータ (ユーザーを特定しないデータ) を収集できるようにするには、この値を選択します。
- `NONE`: Citrix LicensingによるCEIPデータの収集を無効にするには、この値を選択します。

Call Homeデータ収集の詳細については、Citrix Licensing Call Home を参照してください。

CEIPデータ収集の詳細については、Citrix Licensing Customer Experience Improvement Program を参照してください。

CEIPデータの詳細については、Citrix Licensing CEIPデータ要素 を参照してください。

License Serverライセンスデータの詳細については、Citrix Licensing Data を参照してください。

- **/components** *コンポーネント ...*

  インストールまたは削除するコンポーネントのコンマ区切りリスト。有効な値は次のとおりです。

  - `CONTROLLER`: コントローラー
  - `DESKTOPSTUDIO`: スタジオ
  - `WEBSTUDIO`: ウェブスタジオ
  - `DESKTOPDIRECTOR`: ディレクター
  - `LICENSESERVER`: Citrix ライセンスサーバー
  - `SECUREPRIVATEACCESS`: セキュアプライベートアクセス

  このオプションを省略した場合、すべてのコンポーネントがインストールされます (`/remove` オプションも指定されている場合は、削除されます)。

  (2003年より前のリリースでは、有効な値には`STOREFRONT`が含まれていました。2003年以降のバージョンでは、Use the full-product installerに記載されている専用のStoreFrontインストールコマンドを使用してください)。

- **/onlyprereqs** オプション

  選択したコンポーネントの前提条件のみがインストールされます。Citrix製品コンポーネントはインストールされません。

- **/configure_firewall**

Windows Firewallサービスが実行されている場合、ファイアウォールが有効になっていなくても、インストールされるコンポーネントが使用するWindowsファイアウォール内のすべてのポートを開きます。サードパーティ製ファイアウォールまたはファイアウォールを使用していない場合は、手動でポートを開く必要があります。

- **/disableexperiencemetrics** オプション

  インストール、アップグレード、または削除中に収集された分析データがCitrixに自動的にアップロードされるのを防ぎます。

- **/help** または **/h**

  コマンドのヘルプを表示します。

- **/ignore_hw_check_failure**

  ハードウェアチェックが失敗した場合（例えば、RAM不足のため）でも、Delivery Controllerのインストールまたはアップグレードを続行できます。詳細については、ハードウェアチェックを参照してください。

- **/ignore_site_test_failure**

  Controllerのアップグレード中にのみ有効です。通常、サイトテストの失敗は無視され、アップグレードは続行されます。省略された場合（またはfalseに設定された場合）、サイトテストの失敗があると、アップグレードを実行せずにインストーラーが失敗します。デフォルト = false

  アップグレード中に、サポートされていないSQL Serverバージョンが検出された場合、このオプションは無視されます。詳細については、SQL Serverバージョンチェックを参照してください。

- **/installdir** *ディレクトリ*

  コンポーネントがインストールされる既存の空のディレクトリ。デフォルト = `c:\Program Files\Citrix`。

- **/logpath** *パス*

  ログファイルの場所。指定されたフォルダーは存在している必要があります。インストーラーは作成しません。デフォルト = `TEMP%\Citrix\XenDesktop Installer`

- **/no_remote_assistance**

  Directorのインストール時にのみ有効です。Windowsリモートアシスタンスを使用するユーザーシャドウイング機能を無効にします。

- **再起動なし**

インストール後の再起動を防止します。（ほとんどのコアコンポーネントでは、再起動はデフォルトで有効になっていません。）

- **再開しない**

  デフォルトでは、インストール中にマシンの再起動が必要な場合、再起動が完了するとインストーラーは自動的に再開します。デフォルトを上書きするには、`/noresume`を指定します。これは、メディアを再マウントする必要がある場合や、自動インストール中に情報を取得したい場合に役立ちます。

- **ノースキューエル**

  コントローラーをインストールするサーバーへのMicrosoft SQL Server Expressのインストールを防止します。このオプションを省略すると、SQL Server Expressがサイトデータベースとして使用するためにインストールされます。

  このオプションは、ローカルホストキャッシュに使用されるSQL Server Express LocalDBのインストールには影響しません。

- **サイレント** または **パッシブ**

  インストール中にユーザーインターフェイスは表示されません。インストールプロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **/削除**

  `/components`オプションで指定されたコアコンポーネントを削除します。

- **/すべて削除**

  インストールされているすべてのコアコンポーネントを削除します。

- **/SKIPHDXDRIVERCHECK**

  VDAメタインストーラーへのHDX™ ドライバーのチェックをスキップします。

- **/エクスペリエンスメトリックを送信**

  インストール、アップグレード、または削除中に収集された分析データをCitrixに自動的に送信します。このオプションを省略した場合（または`/disableexperiencemetrics`が指定されている場合）、分析データはローカルで収集されますが、自動的には送信されません。

- **一時ディレクトリ** *directory*

  インストール中に一時ファイルを保持するディレクトリ。デフォルト = `c:\Windows\Temp`。

- **ゼナップ**

Citrix Virtual Apps をインストールします。このオプションを省略すると、Citrix Virtual Apps and Desktops™ がインストールされます。

コアコンポーネントのインストール例

次のコマンドは、サーバーに Delivery Controller™、Studio、Citrix Licensing、および SQL Server Express をインストールします。コンポーネント間の通信に必要なファイアウォールポートは自動的に開かれます。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver /configure_firewall
```

次のコマンドは、サーバーに Citrix Virtual Apps™ Controller、Studio、および SQL Server Express をインストールします。コンポーネント間の通信に必要なファイアウォールポートは自動的に開かれます。

```
\x64\XenDesktop Setup\\XenDesktopServerSetup.exe /xenapp /components controller,desktopstudio /configure_firewall
```

次のコマンドは、サーバーに Delivery Controller、Secure Private Access、および SQL Server Express をインストールします。コンポーネント間の通信に必要なファイアウォールポートは自動的に開かれます。

```
\x64\XenDesktop Setup XenDesktopServerSetup.exe /xenapp /components controller,secureprivateaccess /configure_firewall
```

スタンドアロンVDAインストーラーを使用する

ダウンロードサイトにアクセスするには、Citrixアカウントの資格情報が必要です。インストールを開始する前に、管理者特権を昇格させるか、**管理者として実行**を使用する必要があります。

1. Citrixから適切なパッケージをダウンロードします。
   - マルチセッションOS Virtual Delivery Agent: `VDAServerSetup_xxxx.exe`
   - シングルセッションOS Virtual Delivery Agent: `VDAWorkstationSetup_xxxx.exe`
   - シングルセッションOSコアサービスVirtual Delivery Agent: `VDAWorkstationCoreSetup_xxxx.exe`
2. まずパッケージから既存のディレクトリにファイルを抽出し、その後インストールコマンドを実行するか、単にパッケージを実行します。

ファイルをインストールする前に抽出するには、絶対パスを指定して`/extract`を使用します（例: `C:\YourExtractFolder\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`）。ディレクトリが存在している必要があります。存在しない場合、抽出は失敗します。その後、別のコマンドで、この記事に記載されている有効なオプションを使用して、適切なコマンドを実行します。

- `VDAServerSetup_XXXX.exe` の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe` を実行します
- `VDAWorkstationCoreSetup_XXXX.exe` の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe` を実行します
- `VDAWorkstationSetup_XXXX.exe` の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe` を実行します

ダウンロードしたパッケージを実行するには、その名前（`VDAServerSetup.exe`、`VDAWorkstationSetup.exe`、または`VDAWorkstationCoreSetup.exe`）を実行します。この記事に記載されている有効なオプションを使用してください。

フル製品インストーラーに慣れている場合：

- スタンドアロンの`VDAServerSetup.exe`または`VDAWorkstationSetup.exe`インストーラーを、名前以外はすべて`XenDesktopVdaSetup.exe`コマンドであるかのように実行します。
- `VDAWorkstationCoreSetup.exe` インストーラーは、他のインストーラーで利用できるオプションのサブセットをサポートしているため、異なります。

VDA をインストールするためのコマンドラインオプション

以下のオプションは、次の1つ以上のコマンド（インストーラー）で有効です: `VDAServerSetup_xxxx.exe`、`VDAWorkstationSetup_xxxx.exe`、および`VDAWorkstationCoreSetup_xxxx.exe`。

オプションの詳細については、「VDA のインストール」を参照してください。

- **/コンポーネント** *コンポーネント*\[,*コンポーネント*\]

  インストールまたは削除するコンポーネントのコンマ区切りリスト。有効な値は次のとおりです。

  - `VDA`: バーチャル デリバリー エージェント
  - `PLUGINS`: Citrix Workspace™ アプリ (Windows用)

VDAとCitrix Workspaceアプリ for Windowsをインストールするには、`/components vda,plugins`を指定するか、コンポーネントをまったく指定しないでください。コンポーネントが指定されていない場合、デフォルトではVDAのみがインストールされます。

VDA のみをインストールし、Citrix Workspace アプリのインストールを除外するには、`/components vda` を指定します。

このオプションは、`VDAWorkstationCoreSetup_xxxx.exe` インストーラーを使用する場合は無効です。そのインストーラーでは Citrix Workspace app をインストールできません。

- **前提条件のみ**

  選択したコンポーネントの前提条件のみがインストールされます。Citrix 製品コンポーネントはインストールされません。

- **コントローラー** "*controller* \[*controller*\]"

  VDA が通信できるコントローラーのスペース区切りの FQDN を、引用符で囲んで指定します。`/site_guid` オプションと `/controllers` オプションの両方を指定しないでください。

- **/ディスエーブルエクスペリエンスメトリクス**

  インストール、アップグレード、または削除中に収集された分析データがCitrixに自動的にアップロードされるのを防ぎます。

- **/enable_hdx_ports**

  Windowsファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、VDAと有効な機能（Windowsリモートアシスタンスを除く）に必要なWindowsファイアウォールのポートを開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、ネットワークポートを参照してください。

  HDX アダプティブトランスポートが使用する UDP ポートを開くには、この `/enable_hdx_ports` オプションに加えて、`/enable_hdx_udp_ports` オプションを指定します。

- **/enable_hdx_udp_ports**

  Windowsファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、HDXアダプティブトランスポートが使用するWindowsファイアウォールのUDPポートを開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用して

いない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、ネットワークポートを参照してください。

VDAが使用する追加ポートを開くには、この`/enable_hdx_udp_ports`オプションに加えて、`/enable_hdx_ports`オプションを指定します。

- **/enable_hdx_tls_dtls**

  HDX Direct V1用にTCPおよびUDPポート443を開きます。

- **/enable_real_time_transport**

  オーディオパケットにUDPを使用するかどうかを有効または無効にします（オーディオ用のRealTime Audio Transport）。この機能を有効にすると、オーディオパフォーマンスが向上する可能性があります。Windowsファイアウォールサービスが検出されたときにUDPポートを自動的に開く場合は、`/enable_hdx_ports`オプションを含めます。

- **/enable_remote_assistance**

  Directorで使用するために、Windowsリモートアシスタンスのシャドウイング機能を有効にします。このオプションを指定すると、Windowsリモートアシスタンスはファイアウォールで動的ポートを開きます。

- **/enablerestore** または **/enablerestorecleanup**

  （シングルセッションVDAにのみ有効）VDAのインストールまたはアップグレードが失敗した場合に、復元ポイントへの自動復帰を有効にします。

  インストール/アップグレードが正常に完了した場合：

  - `/enablerestorecleanup`は、インストーラーに復元ポイントを削除するよう指示します。
  - `/enablerestore`は、使用されなかった場合でも、インストーラーに復元ポイントを保持するように指示します。

  詳細については、インストールまたはアップグレードの失敗時の復元を参照してください。

- **/ENABLE_SECURE_DEFAULTS**

  より安全な初期設定のために、さまざまな機能のデフォルト設定を有効から無効に変更します。関連する機能は、クライアントドライブリダイレクト、特殊フォルダーリダイレクト、ドラッグアンドドロップ、クライアントTWAINデバイスリダイレクト、クライアントUSBプラグアンドプレイデバイスリダイレクト、クライアントプリンターリダイレクト、クライアントクリップボードリダイレクト、およびクライアントマイクリダイレクトです。

- **/enable_ss_ports**

  Windows ファイアウォール サービスが検出された場合、ファイアウォールが有効になっていなくても、画面共有に必要なポートを Windows ファイアウォールで開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。

- **/exclude** "*コンポーネント*"\[,"*コンポーネント*"\]

  1つ以上のコンマ区切りのオプションコンポーネント（それぞれをストレート引用符で囲む）のインストールを防止します。たとえば、MCSで管理されていないイメージにVDAをインストールまたはアップグレードする場合、Machine Identity Serviceコンポーネントは不要です。有効な値は次のとおりです。

マルチセッションOS	シングルセッションOS	シングルセッションOSコアサービス
`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`
`Citrix Backup and Restore`	`Citrix Backup and Restore`	`Citrix Browser Content Redirection`
`Citrix Browser Content Redirection`	`Citrix Browser Content Redirection`	`Citrix Personalization for App-V - VDA`
`Citrix MCS IODriver`	`Citrix MCS IODriver`	`Citrix Telemetry Service`
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`	`Citrix Universal Print Client`
`Citrix Profile Management`	`Citrix Profile Management`	`Citrix Vda Log Capture Service`
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`	`CSE Component`
`Citrix Rendezvous V2`	`Citrix Rendezvous V2`	`Director VDA Plug-in`
`Citrix Telemetry Service`	`Citrix Telemetry Service`	`Machine Management Provider`

マルチセッションOS	シングルセッションOS	シングルセッションOSコアサービス
`Citrix Universal Print Client`	`Citrix Universal Print Client`	`VDA Monitor Plug-in`
`Citrix Vda Log Capture Service`	`Citrix Vda Log Capture Service`	`VDA WMI Proxy Plug-in`
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`	
`CSE Component`	`CSE Component`	
`Director VDA Plug-in`	`Director VDA Plug-in`	
`Machine Identity Service`	`Machine Identity Service`	
`Machine Management Provider`	`Machine Management Provider`	
`VDA Monitor Plug-in`	`User Personalization Layer`	
`VDA WMI Proxy Plug-in`	`VDA Monitor Plug-in`	
	`VDA WMI Proxy Plug-in`	
`Citrix App Protection Component`	`Citrix App Protection Component`	`Citrix App Protection Component`
`Citrix HyperV Filter Driver`	`Citrix HyperV Filter Driver`	
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`

Citrix Profile Management をインストールから除外する (`/exclude "Citrix Profile Management"`) と、Citrix Director を使用した VDA の監視とトラブルシューティングに影響します。**ユーザーの詳細**ページと**エンドポイント**ページでは、パーソナライズパネルとログオン期間パネルが機能しません。**ダッシュボード**ページと**傾向**ページでは、平均ログオン期間パネ

ルに、Profile Management がインストールされているマシンに関するデータのみが表示されます。

サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrix Profile Management Service をインストールして実行することをお勧めします。Citrix Profile Management Service を有効にする必要はありません。

同じコンポーネント名で `/exclude` と `/includeadditional` の両方を指定した場合、そのコンポーネントはインストールされません。

このオプションは、`VDAWorkstationCoreSetup.exe` インストーラーを使用する場合は無効です。そのインストーラーは、これらの項目の多くを自動的に除外します。

- **/h** または **/help**

  コマンドのヘルプを表示します。

- **/includeadditional** "*コンポーネント*"\[,"*コンポーネント*"\]

  1つ以上のコンマ区切りのオプションコンポーネント（それぞれをストレート引用符で囲む）のインストールを含めます。このオプションは、リモート PC アクセス展開を作成していて、デフォルトで含まれていない他のコンポーネントをインストールしたい場合に役立ちます。有効な値は次のとおりです。

マルチセッションOS	シングルセッションOS
`Citrix Backup and Restore`	`Citrix Backup and Restore`
`Citrix MCS IODriver`	`Citrix MCS IODriver`
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`
`Citrix Profile Management`	`Citrix Profile Management`
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`
`Citrix Rendezvous V2`	`Citrix Rendezvous V2`
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`
`Citrix Web Socket Vda Registration Tool`	`Citrix Web Socket Vda Registration Tool`

マルチセッションOS	シングルセッションOS
`Machine Identity Service`	`Machine Identity Service`
	`User Personalization Layer`

同じコンポーネント名で`/exclude`と`/includeadditional`の両方を指定した場合、そのコンポーネントはインストールされません。

- **/installdir** *ディレクトリ*

  コンポーネントがインストールされる既存の空のディレクトリ。デフォルト = `c:\Program Files\Citrix`。

- **/install_mcsio_driver**

  使用しないでください。代わりに、`/includeadditional "Citrix MCS IODriver"`または`/exclude "Citrix MCS IODriver"`を使用してください。

- **/logpath** *パス*

  ログファイルの場所。指定されたフォルダーは存在している必要があります。インストーラーは作成しません。デフォルト = 「`%TEMP%\Citrix\XenDesktop Installer`」

  このオプションはグラフィカルインターフェイスでは利用できません。

- **/マスターイメージ**

  VMにVDAをインストールする場合にのみ有効です。VDAを他のマシンを作成するために使用するイメージとして設定します。このオプションは`/mastermcsimage`と同等です。

  このオプションは、`VDAWorkstationCoreSetup_xxxx.exe`インストーラーを使用している場合は無効です。

- **/マスターMCSイメージ**

  このマシンがMachine Creation Servicesのイメージとして使用されることを指定します。このオプションは`/masterimage`と同等です。

- **/マスターPVSイメージ**

  このマシンが、Citrix Provisioning™ またはサードパーティのプロビジョニングツール（Microsoft System Center Configuration Managerなど）を使用してVMをプロビジョニングするためのイメージとして使用されることを指定します。

- **/websockettoken** *WebSocketトークン*

Web Socket VDAを作成します。WebSocketTokenは、必要なトークン用です。

- **/websockettokenfile** *WebSockトークンを含むファイル*

  Web Socket VDAを作成します。*FileContainingWebSockToken* は、必要なトークンを含むファイル用です。

- **ウェブソケットトークン標準入力** *<ウェブソケットトークン>*

  Web Socket VDAを作成します。*<WebSocketToken* は、STDINによって渡される必要なトークン用です。

- **/no_mediafoundation_ack**

  Microsoft Media Foundationがインストールされていないことを確認し、いくつかのHDXマルチメディア機能がインストールされず、動作しないことを承認します。このオプションが省略され、Media Foundationがインストールされていない場合、前提条件が満たされていないため、VDAのインストールは終了します。ほとんどのサポートされているWindowsエディションには、Nエディションを除き、Media Foundationがすでにインストールされています。Windowsの機能 > メディア機能 を *手動* で 有効にした場合、Citrix Meta Installerが検索するレジストリキーに値が設定されていない可能性があります。インストールプロセスを開始する前に、`SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\Windows-Features\WindowsMediaVersion` レジストリキーをチェックして、値が存在し、空ではないことを確認してください。

- **/nodesktopexperience** (デスクトップエクスペリエンスなし)

  拡張デスクトップエクスペリエンス機能は利用できなくなりました。このオプション（およびポリシー設定）は、指定されても無視されます。

  マルチセッションOS用VDAのインストール時にのみ有効です。拡張デスクトップエクスペリエンス機能の有効化を防止します。この機能は、拡張デスクトップエクスペリエンスCitrixポリシー設定でも制御されます。

- **/noreboot** (再起動なし)

  インストール後の再起動を防止します。VDAは再起動するまで使用できません。

- **/noresume** (再開なし)

  デフォルトでは、インストール中にマシンの再起動が必要な場合、再起動が完了するとインストーラーは自動的に再開します。デフォルトを上書きするには、`/noresume` を指定します。これは、メディアを再マウントする必要がある場合や、自動インストール中に情報を取得したい場合に役立ちます。

- **物理マシン**

  RemotePC インストールの場合、この引数を `/remotepc` とともに使用します。そうしないと、特定のユーザーシナリオで VDA が予期したとおりに動作しない可能性があります。

- **/ポート番号** *ポート*

  `/reconfig`オプションが指定されている場合にのみ有効です。VDAとController間の通信を有効にするポート番号。以前に構成されたポートは、ポート80でない限り無効になります。

- **/プロキシ構成** *"アドレスまたはPACファイルのパス"*

  環境で Gateway Service などのサービスと Rendezvous プロトコルを使用する予定があり、ネットワークにアウトバウンド接続用の非透過型プロキシがある場合は、ここでプロキシを指定します。HTTP プロキシのみがサポートされています。Rendezvous プロトコルで使用するプロキシのアドレスまたは PAC ファイルパス。このコマンドラインは、/includeadditional "Citrix Rendezvous V2" が使用されたかのように、Citrix Rendezvous V2 を自動的にインストールします。機能の詳細については、Rendezvous プロトコル を参照してください。

  - プロキシアドレスの形式: `http://<url-or-ip>:<port>`
  - PACファイルの形式: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **/サイレント** または **/パッシブ**

  インストール中にユーザーインターフェイスは表示されません。インストールと構成プロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **/再構成**

  `/portnumber`、`/controllers`、または`/enable_hdx_ports`オプションと組み合わせて使用すると、以前に構成されたVDA設定をカスタマイズします。このオプションを`/quiet`オプションも指定せずに指定すると、VDAをカスタマイズするためのグラフィカルインターフェイスが起動します。

- **/リモートPC**

  Remote PC Access 展開 (シングルセッション OS) または仲介接続 (マルチセッション OS) の場合にのみ有効です。追加コンポーネントのインストールは除外されます (`/exclude` および `/includeadditional` オプションのコンポーネントリストを参照)。

  このオプションは、`VDAWorkstationCoreSetup.exe`インストーラーを使用する場合は無効です。そのインストーラーは、これらのコンポーネントのインストールを自動的に除外します。

`/remotepc` は `/servervdi` オプションと互換性がありません。

- **/削除**

  `/components`オプションで指定されたコンポーネントを削除します。

- **/remove_appdisk_ack**

  AppDisks™ VDAプラグインがインストールされている場合、VDAインストーラーがそれをアンインストールすることを承認します。

- **/remove_pvd_ack**

  Personal vDiskがインストールされている場合、VDAインストーラーがそれをアンインストールすることを承認します。

- **/すべて削除**

  VDAを削除します。Citrix Workspaceアプリ（インストールされている場合）は削除しません。

- **/REMOVEALLWITHCWA**

  VDA とともに CWA を削除します。

- **/エクスペリエンスメトリックを送信**

  インストール、アップグレード、または削除中に収集された分析データをCitrixに自動的に送信します。このオプションが省略された場合（または`/disableexperiencemetrics`オプションが指定された場合）、分析データはローカルで収集されますが、自動的には送信されません。

- **/サーバーVDI**

  サポートされているWindowsマルチセッションマシンにシングルセッションOS用VDAをインストールします。Windowsマルチセッションマシンにマルチセッション OS用VDAをインストールする場合は、このオプションを省略してください。

  このオプションを使用する前に、サーバーVDI を参照してください。

  このオプションは、フルプロダクトVDAインストーラーでのみ使用してください。

- **/site_guid** *グイッド*

  サイトのActive Directory組織単位 (OU) のグローバル一意識別子。これは、Active Directoryを検出に使用している場合に、仮想デスクトップをサイトに関連付けます（自動更新が推奨され

るデフォルトの検出方法です）。サイトGUIDは、Studioに表示されるサイトプロパティです。`/site_guid`オプションと`/controllers`オプションの両方を指定しないでください。

- **一時ディレクトリ** *directory*

  インストール中に一時ファイルを保持するディレクトリ。デフォルト = `c:\Windows\Temp`。

  このオプションはグラフィカルインターフェイスでは利用できません。

- **仮想マシン**

  VMにVDAをインストールする場合にのみ有効です。インストーラーによる物理マシンの検出を上書きします。VMに渡されるBIOS情報により、VMが物理マシンとして表示される場合があるためです。

  このオプションはグラフィカルインターフェイスでは利用できません。

- **XenDesktopクラウド**

  VDAがCitrix DaaS (Citrix Cloud™) 展開にインストールされていることを示します。

VDAのインストール例

フルプロダクトインストーラーでVDAをインストールする：

以下のコマンドは、シングルセッションOS用VDAとCitrix Workspaceアプリを VMのデフォルトの場所にインストールします。このVDAはイメージとして使用され、MCSを使用してVMをプロビジョニングします。VDAは、`mydomain`ドメイン内の`Contr-Main`という名前のサーバー上のControllerに最初に登録されます。VDAはユーザーパーソナライゼーションレイヤーとWindowsリモートアシスタンスを使用します。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins /
controllers "Contr-Main.mydomain.local" /enable_hdx_ports /includeadditional
"user personalization layer" /mastermcsimage /enable_remote_assistance
```

VDAWorkstationCoreSetupスタンドアロンインストーラーを使用してシングルセッションOS VDAをインストールする:

以下のコマンドは、リモートPCアクセスまたはVDI展開で使用するために、シングルセッションOSにコアサービスVDAをインストールします。Citrix Workspaceアプリおよびその他の非コアサービスはインストールされません。Controllerのアドレスが指定され、Windowsファイアウォールサービス内のポートは自動的に開かれます。管理者が再起動を処理します。

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.com" /
enable_hdx_ports /noreboot
```

VDAをカスタマイズする

VDAをインストールした後、いくつかの設定をカスタマイズできます。製品メディアの `\x64\XenDesktop Setup` ディレクトリから、VDAのインストール用コマンドラインオプションで説明されている以下のオプションを1つ以上使用して、`XenDesktopVdaSetup.exe` を実行します。

- `/reconfigure` (VDAをカスタマイズする際に必須)
- `/h` または `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

VDAのトラブルシューティング

- デリバリーグループのStudio表示で、**詳細**ペインの**インストール済みVDAバージョン**エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンのWindowsのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされた後、Delivery Controllerに登録されるまで、ユーザーにアプリやデスクトップを配信できません。

  VDAの登録方法と登録の問題のトラブルシューティングについては、VDAの登録を参照してください。

Universal Print Serverをインストールするためのコマンドラインオプション

次のオプションは、`XenDesktopPrintServerSetup.exe` コマンドで有効です。

- **/enable_upsserver_port**

このオプションが指定されていない場合、インストーラーはグラフィカルインターフェイスから「**ファイアウォール**」ページを表示します。インストーラーにWindowsファイアウォールルールを自動的に追加させるには「**自動**」を選択するか、管理者がファイアウォールを手動で構成できるように「**手動**」を選択します。

印刷サーバーにソフトウェアをインストールした後、(/ja-jp/citrix-virtual-apps-desktops/2407/printing/printing-provision-printers.html)のガイダンスを使用してUniversal Print Serverを構成します。

Secure Private Accessをインストールするためのコマンドラインオプション

以下のオプションは、両方で有効です。

1. CVADインストーラー: `XenDesktopSPASetup.exe`
2. SPAオンプレミスインストーラー: `SecurePrivateAccessSetup_XXXX.exe`

- **/enable_spa_ports**

  Windowsファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、Secure Private Accessに必要なWindowsファイアウォールのポートを開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、「ネットワークポート」を参照してください。

- **ノーSQL**

  Secure Private Accessをインストールしているサーバーに Microsoft SQL Server Expressがインストールされるのを防止します。このオプションを省略すると、SQL Server Expressがサイトデータベースとして使用するためにインストールされます。

- **/help または /h または /?**

  コマンドのヘルプを表示します

- **/noreboot** (再起動なし)

  インストール後の再起動を防止します。再起動するまでSecure Private Accessは使用できません。

- **/quiet または /passive**

  インストール中にユーザーインターフェイスは表示されません。インストールと構成プロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **/remove** (削除)

  Secure Private Accessを削除します。

オプションの詳細については、Secure Private Access installerを参照してください。

詳細情報

Citrixがコンポーネントインストールの結果を報告する方法については、Citrix installation return codesを参照してください。

Web Studio のインストール

はじめに

Citrix Studio は、Citrix Virtual Apps and Desktops の展開を構成および管理できる Windows ベースの管理コンソールです。Web Studio は、Citrix Studio の次世代版であり、Citrix Studio と完全に同等の機能を備えた Web ベースの管理コンソールです。(/ja-jp/citrix-daas/overview#studio) と同じルックアンドフィールで、Web Studio はネイティブの Web エクスペリエンスを提供することで、管理エクスペリエンスを最新化します。

Web Studio は、Internet Information Service (IIS) がインストールされている任意の Windows サーバーに展開できます。展開オプションは次の 2 つです。

- 専用サーバーにインストールする:

  パフォーマンスと拡張性が重要な大規模環境では、Web Studio を専用サーバーにインストールすることをお勧めします。このサーバーは、オプションで Director もホストできます。

- Delivery Controller™ と統合する:

  迅速な展開やシンプルな環境では、Web Studio を Delivery Controller に直接インストールします。このアプローチは、管理オーバーヘッドを最小限に抑えることが優先される小規模な展開に最適です。

次の図は、Web Studio のアーキテクチャを示しています。

Web Studio のアーキテクチャ(/en-us/citrix-virtual-apps-desktops/2407/media/web-studio-architecture.png)

Web Studio を稼働させるための一般的なワークフローは次のとおりです。

1. Web Studio をインストールする。
2. (#set-up-a-site)。
3. 管理のために Delivery Controller を Web Studio に追加する。
4. Web Studio にログオンする。

ロードバランスされたWeb Studio展開をセットアップするには、(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/install-core/load-balance-studio)を参照してください。

Web Studioで利用可能な新機能

(/ja-jp/citrix-virtual-apps-desktops/2407/whats-new#web-studio)記事を参照してください。

システム要件

サポートされているオペレーティングシステム:

- ウィンドウズ サーバー 2022
- Windows Server 2019、StandardおよびDatacenterエディション、Server Coreオプション付き
- Windows Server 2016、StandardおよびDatacenterエディション、Server Coreオプション付き

サポートされているブラウザー:

- マイクロソフト エッジ 92
- Firefox ESR (延長サポート版) 90
- グーグルクローム 92
- サファリ 14

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

前提条件

このWeb Studioリリースは、Citrix Virtual Apps and Desktops™ 2212以降の展開と互換性があります。

2212より前の展開の場合、まず2212にアップグレードしてからWeb Studioをインストールしてください。

既知の制限事項

Web StudioとCitrix Studioを相互に利用する場合、次の制限事項を考慮してください。Web Studioで作成されたテンプレートはCitrix Studioには表示されず、その逆も同様です。これは、Web StudioがテンプレートをCitrix Studioとは異なるデータベースを使用しているためです。回避策として、Web Studioでテンプレートからポリシーを作成し、次にCitrix Studioでこのポリシーからテンプレートを作成し、その逆も同様に行います。

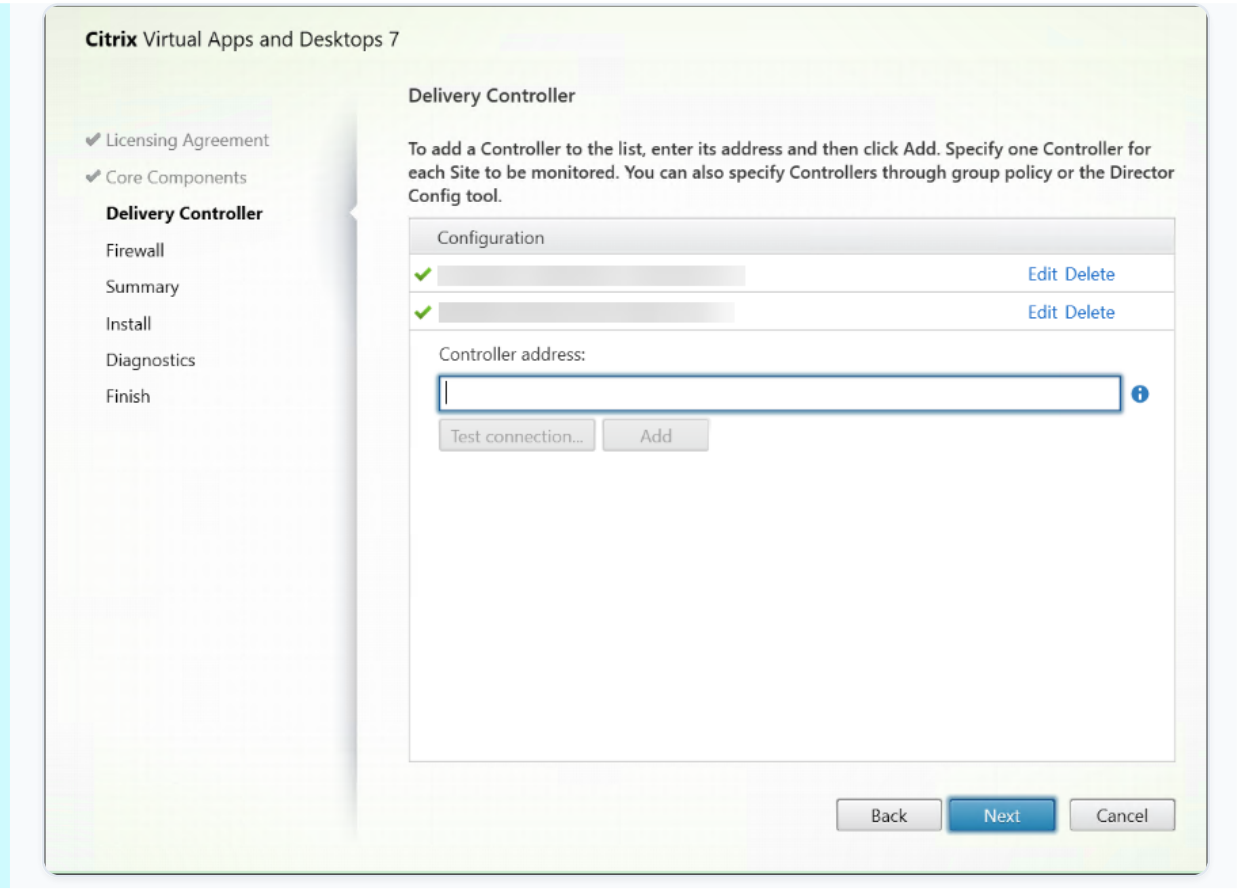
- Web Studioのインストールを成功させるには、Internet Information Services (IIS) マネージャーでデフォルトのサイト名 (**Default Web Site**) を変更しないでください。デフォルトのサイト名を変更すると、インストールが失敗します。

Web Studioのインストール

以下の情報は、コアコンポーネントのインストールのガイダンスを補足するものです。Web Studioをインストールするには：

- Citrix Virtual Apps and Desktopsのフル製品ISOインストーラーを使用してWeb Studioをインストールします。ISOインストーラーは、前提条件を確認し、不足しているコンポーネントをインストールし、Web Studio Webサイトをセットアップし（Delivery Controllerのインストールに含まれている場合はDelivery Controller上に）、基本的な構成を実行します。
- インストール時にWeb Studioが含まれていなかった場合は、インストーラーを使用してWeb Studioを追加します。
- Web Studioをインストールする際、Delivery Controllerのアドレスを入力するよう求められます。

> **注:**
>
> - 複数のDelivery Controllerを追加できます。Web Studioはランダムな順序でそれらに接続を試みます。Web Studioが接続しようとしているDelivery Controllerに到達できない場合、Web Studioは自動的に他のDelivery Controllerにフォールバックします。
> - **コアコンポーネント**でDirectorが選択されインストールされている場合、ここで追加するDelivery ControllerはWeb StudioとDirectorの両方で使用されます。
> - 外部の公開信頼証明書が構成されておらず、エンタープライズCAから証明書を要求したくない場合は、Delivery ControllerのFQDNを構成するだけで済みます。
> - 外部の公開信頼証明書があり、Delivery ControllerのパブリックDNSを構成できる場合は、DNS名をDelivery Controllerアドレスとして入力できます。
> - 企業CAから証明書を要求でき、個人DNSを指定できる場合は、個人DNSをDelivery Controllerアドレスとして追加できます。



- ブラウザとWebサーバー間、およびブラウザとDelivery Controller間の通信を保護するには、Web StudioをホストするIIS WebサイトとDelivery ControllerでTLS暗号化を有効にする必要があります。Delivery ControllerにTLS証明書が構成されていない場合、インストーラーはDelivery ControllerのFQDNとlocalhostをDNS名証明書として使用する自己署名証明書を作成します。TLS証明書が構成されている場合、インストーラーは何も変更しません。TLS暗号化の詳細については、「Web Studio展開を保護する（オプション）」を参照してください。
- **完了**ページでは、**サイトマネージャーを起動**チェックボックスがデフォルトで選択されており、Citrix Site Managerが自動的に開きます。後で起動するには、デスクトップのスタートメニューを開き、**Citrix > Citrix Site Manager**を選択します。Web Studioを起動する前に、Citrix Site Managerを使用してサイトを作成するか、既存のサイトに参加する必要があります。詳細については、「サイトのセットアップ」を参照してください。

  サイトマネージャーを起動(/en-us/citrix-virtual-apps-desktops/2407/media/launch-site-manager.png)

> **注:**
>
> コマンドラインを使用してWeb Studioをインストールすることもできます。例：`.\XenDesktopServerSetup.exe /components webstudio /controllers`

> `"ddc1.studio.local" /configure_firewall /quiet`。詳細については、「コマンドラインを使用したインストール」を参照してください。

サイトをセットアップする

Citrix Virtual Apps and Desktops 展開（サイトとも呼ばれます）をセットアップするには、Citrix Site Manager ツールを使用します。このツールは、Delivery Controller とともに自動的にインストールされます。

サイトをセットアップするには、次の手順に従います。

1. Delivery Controller で、デスクトップのスタートメニューを開き、**Citrix > Citrix Site Manager** を選択します。
2. Citrix Site Manager で、**Create a site** を選択します。サイトセットアップウィザードが表示されます。
3. サイトを作成し、その設定を次のように構成します。
   - **はじめに**ページで、サイトの名前を入力します。
   - **データベース**ページには、サイト、監視、および構成ログデータベースを設定するための選択肢が含まれています。詳細については、「ステップ3. データベース」を参照してください。
   - 「**ライセンス**」ページで、ライセンスサーバーのアドレスを指定し、使用する（インストールする）ライセンスを示します。詳細については、「ステップ4. ライセンス」を参照してください。
4. **Summary** ページで、すべての設定を確認し、**Submit** をクリックします。

   このコントローラーのIPアドレスは、サイトに自動的に追加されます。

> **注:**
>
> サイトを作成したユーザーは、そのサイトのフル管理者になります。詳細については、「委任管理」を参照してください。

サイト作成後に新しいコントローラーをインストールする場合、そのコントローラーをサイトに追加する必要があります。詳細な手順は次のとおりです。

1. この新しいコントローラーでCitrix Site Managerを実行します。

2. 「**既存のサイトに参加**」を選択します。
3. サイトにすでに追加されているコントローラーのアドレスを入力します。
4. 「**送信**」をクリックします。

管理のためにWeb StudioにDelivery Controllerを追加する

Studio構成ツールを使用して、管理のためにDelivery ControllerをWeb Studioに追加します。このツールはWeb Studioのインストールフォルダーにあります。

デフォルトでは、このツールは次のデフォルトフォルダーにインストールされます。

- `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`

Web Studioで管理するサイトに対して、次の2つのDelivery Controller（`ddc1.studio.local`と`ddc2.studio.local`）を構成するとします。次のPowerShellコマンドを実行します。

- `.\StudioConfig.exe --server "ddc1.studio.local,ddc2.studio.local"`

> **注:**
>
> - ツールにはコンピューターの管理者権限が必要です。
> - IISサーバーのキャッシュ設定により、Delivery Controllerの構成変更がすぐに反映されない場合があります。すぐに反映させるには、Web Studioサーバーに移動し、インターネットインフォメーションサービス (IIS) マネージャーを開き、 > > に移動して、 ペインで を選択します。
> - サポートされているすべてのパラメーターを表示するには、`StudioConfig.exe --help` を実行します。

Web StudioをDelivery Controllerのプロキシとして構成する（オプション）

デフォルトでは、Web Studioコンソールを使用して展開を管理する場合、Webブラウザーを介してWeb StudioサーバーとDelivery Controllerの両方に接続します。Web StudioサーバーをDelivery Controllerのプロキシとして構成するオプションを提供します。その結果、展開を管理する際にはWeb Studioサーバーにのみ接続することになります。

このセクションでは、Web StudioサーバーをDelivery Controllerのプロキシとして構成する方法を説明します。Web StudioとDelivery Controllerが異なるサーバーにインストールされていることを前提としています。

開始する前に、展開に必要なすべてのコアコンポーネントがインストールされていることを確認してください。詳細については、「コアコンポーネントのインストール」を参照してください。

Web Studio のプロキシモードを有効にするには、次の手順に従います。

1. Web Studio サーバーで、Windows PowerShell を管理者として実行します。
2. 次のコマンドを実行します。`fqdn_of_webstudio_machine` は Web Studio サーバーの FQDN に置き換えてください。

   ```
   & "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --enableproxy --proxyserver "fqdn_of_webstudio_machine"
   ```

   > **注:**
   >
   > ロードバランスされたWeb Studio展開がある場合は、`fqdn_of_webstudio_machine` をロードバランサーサーバー（仮想サーバーとも呼ばれます）のFQDNに置き換えてください。詳細については、「ロードバランスされたWeb Studio展開のセットアップ」を参照してください。

Web Studio のプロキシモードを無効にするには、この PowerShell コマンドを実行します。

```
`& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --disableproxy`
```

> **注：**
>
> ベストプラクティスとして、外部の公開信頼証明書またはエンタープライズ証明機関 (CA) の証明書を使用して、Web Studio の展開を保護することをお勧めします。詳細については、「Web Studio の展開を保護する」を参照してください。

Web Studioにログオンする

Web StudioのWebサイトは `https://<address of the server hosting Web Studio>/Citrix/Studio` にあります。

Web Studio にログオンするには、デスクトップの メニューを開き、 > を選択します。Web Studio の権限を持つ管理者は、Active Directory ドメインユーザーである必要があります。Web Studio にログオンする際は、次のシナリオを考慮してください。

- サイトのDelivery Controllerをまだ指定していない場合。Delivery Controllerを指定するよう求められ、Web Studioへの一時的なアクセスが提供されます。
- 指定された Delivery Controller に現在到達できない場合、Web Studio にログオンできません。接続をテストして、それらの Delivery Controller に到達可能であることを確認してください。または、代替の Delivery Controller を指定して、Web Studio への一時的なアクセスを提供します。

次のステップ

1. VDA をインストールする
2. Web Studioを使用して、次の方法で仮想アプリとデスクトップをユーザーに配信します。
    a. マシンカタログを作成する
    b. デリバリーグループを作成する
    c. アプリケーショングループを作成する（オプション）

VDAをインストールする

> **重要:**

> - アップグレード中で、現在のバージョンにPersonal vDiskまたはAppDisksソフトウェアがインストールされている場合は、「PvD、AppDisks、およびサポートされていないホストの削除」を参照してください。
> - Citrix®が配布するバイナリは署名されています。署名されたバイナリは、Citrixが生成した証明書または信頼できるサードパーティの証明書によって検証されていることを示します。

> Windowsマシン用のVDAには、マルチセッションOS用VDAとシングルセッションOS用VDAの2種類があります。(Linuxマシン用VDAについては、Linux Virtual Delivery Agentドキュメントを参照してください。)

インストールを開始する前に、インストールの準備を確認し、すべての準備タスクを完了してください。

VDAをインストールする前に、コアコンポーネントをインストールします。VDAをインストールする前にサイトを作成することもできます。

この記事では、VDAをインストールする際のインストールウィザードのシーケンスについて説明します。コマンドラインの同等機能も提供されています。詳細については、「コマンドラインを使用したインストール」を参照してください。

ステップ1. 製品ソフトウェアをダウンロードしてウィザードを起動する

フル製品インストーラーを使用している場合:

1. 製品ISOをまだダウンロードしていない場合：
    - Citrixアカウントの資格情報を使用して、Citrix Virtual Apps and Desktops™ダウンロードページにアクセスします。製品ISOファイルをダウンロードします。
    - ファイルを解凍します。必要に応じて、ISOファイルをDVDに書き込みます。
2. VDAをインストールするイメージまたはマシンでローカル管理者アカウントを使用します。DVDをドライブに挿入するか、ISOファイルをマウントします。インストーラーが自動的に起動しない場合は、マウントされたドライブ上の**AutoSelect**アプリケーションをダブルクリックします。

    インストールウィザードが起動します。

スタンドアロンパッケージを使用している場合:

1. Citrixアカウントの資格情報を使用して、Citrix Virtual Apps and Desktopsのダウンロードページにアクセスします。適切なパッケージをダウンロードします。
    - `VDAServerSetup_2308.exe`: マルチセッションOS VDA *バージョン*
    - `VDAWorkstationSetup_2308.exe`: シングルセッションOS VDA *バージョン*
    - `VDAWorkstationCoreSetup_2308.exe`: シングルセッションOSコアサービスVDA *バージョン*
2. パッケージを右クリックし、**管理者として実行**を選択します。

    インストールウィザードが起動します。

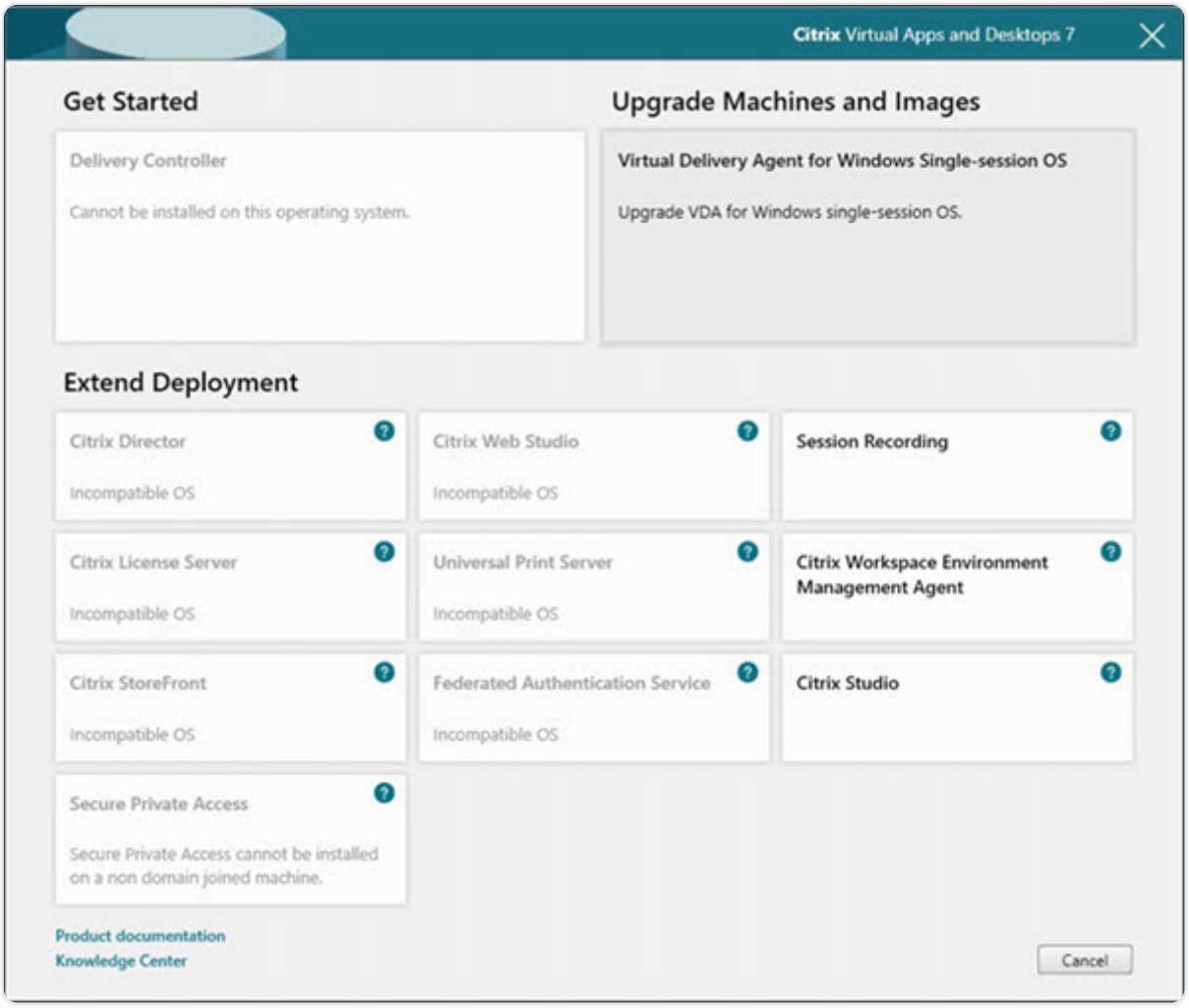
ステップ2. インストールする製品を選択する



インストールする製品（Citrix Virtual AppsまたはCitrix Virtual Desktops）の横にある**開始**をクリックします。（マシンにCitrix Virtual AppsまたはCitrix Virtual Desktopsコンポーネントがすでにインストールされている場合、このページは表示されません。）

コマンドラインオプション: Citrix Virtual Appsをインストールするための`/xenapp`。このオプションが省略された場合、Citrix Virtual Desktopsがインストールされます。

ステップ3. VDAを選択する



Virtual Delivery Agentエントリを選択します。インストーラーは、シングルセッションOSまたはマルチセッションOSのどちらで実行されているかを認識しているため、適切なVDAタイプのみを提供します。

例えば、Windows Server 2019マシンでインストーラーを実行すると、マルチセッションOS用VDAオプションが利用可能です。シングルセッションOS用VDAオプションは提供されません。

このCitrix Virtual Apps and Desktopsバージョンでサポートされていないオペレーティングシステムに Windows VDA をインストール（またはアップグレード）しようとすると、オプションに関する情報を示すメッセージが表示されます。

ステップ4. VDAの使用方法を指定する

VDAインストーラーの環境ページ(/en-us/citrix-virtual-apps-desktops/2407/media/vda-ss-environment.png)

ページで、VDAの使用方法を指定します。このマシンをイメージとして使用して、さらに多くのマシンをプロビジョニングするかどうかを示します。

選択したオプションは、Citrix Provisioning™ツールが自動的にインストールされるかどうか（インストールされる場合）、およびVDAインストーラーのページのデフォルト値に影響します。

VDAをインストールすると、複数のMSI（プロビジョニング用およびその他）が自動的にインストールされます。これらのインストールを防止する唯一の方法は、コマンドラインインストールで`/exclude`オプションを使用することです。

次のいずれかを選択します。

- **マスターMCSイメージを作成する:** Machine Creation Services™を使用してVMをプロビジョニングする予定がある場合は、このオプションを選択してVDAをVMイメージにインストールします。このオプションは、Machine Identity Serviceをインストールします。これはデフォルトのオプションです。

  コマンドラインオプション: `/mastermcsimage` または `/masterimage`

> **重要:**
>
> インストールメディアまたはISOイメージはローカルにマウントする必要があります。ソフトウェアのインストールを目的として、ネットワークドライブからISOイメージをマウントすることはサポートされていません。

- **Citrix Provisioningまたはサードパーティのプロビジョニングツールを使用してマスターイメージを作成する:** Citrix Provisioningまたはサードパーティのプロビジョニングツール（Microsoft System Center Configuration Managerなど）を使用してVMをプロビジョニングする予定がある場合は、このオプションを選択してVDAをVMイメージにインストールします。

  コマンドラインオプション: `/masterpvsimage`

- （マルチセッションOSマシンでのみ表示）**サーバーへの仲介接続を有効にする:** このオプションを選択して、他のマシンをプロビジョニングするためのイメージとして使用されない物理マシンまたは仮想マシンにVDAをインストールします。

  コマンドラインオプション: `/remotepc`

- (シングルセッションOSマシンでのみ表示) **Remote PC Accessを有効にする:** 物理マシンにVDAをインストールしてRemote PC Accessで使用するには、このオプションを選択します。

  コマンドラインオプション: `/remotepc`

Nextをクリックします。

このページは表示されません。

- VDAをアップグレードする場合
- `VDAWorkstationCoreSetup_2308.exe`、`VDAServerSetup_2308.exe`、または`VDAWorkstationSetup_2308.exe`インストーラーを使用している場合

ステップ5. インストールするコンポーネントとインストール場所を選択します

VDAインストーラーのコアコンポーネントページ(/en-us/citrix-virtual-apps-desktops/2407/media/vda-ss-core-components.png)

コアコンポーネントページで:

- **場所:** デフォルトでは、コンポーネントは`C:\Program Files\Citrix`にインストールされます。ほとんどの展開では、このデフォルトで問題ありません。別の場所を指定する場合、その場所にはネットワークサービスに対して`execute`権限が必要です。
- **コンポーネント:** デフォルトでは、Citrix Workspace App for WindowsはVDAと一緒にインストールされません。`VDAWorkstationCoreSetup.exe`インストーラーを使用している場合、Citrix Workspace App for Windowsはインストールされないため、このチェックボックスは表示されません。

Nextをクリックします。

コマンドラインオプション: VDAとCitrix Workspace App for Windowsをインストールするには`/installdir`、`/components vda,plugin`

> **注:**
>
> 以下のシナリオでは、VDAのインストール、アップグレード、またはアンインストール中にCitrix Workspace™ Appをインストール、アップグレード、またはアンインストールすることを選択できます。

> - VDAのインストール中に、Citrix Workspaceアプリをインストールすることを選択できます。デフォルトでは、VDAのインストール中にCitrix Workspaceアプリはインストールされません。

- VDAのアップグレード中に、Citrix WorkspaceアプリがVDAにまだインストールされていない場合、Citrix Workspaceアプリをインストールすることを選択できます。
- VDAのアップグレード中に、Citrix Workspaceアプリのバージョンをアップグレードできる場合、Citrix Workspaceアプリをアップグレードするオプションが表示されます。
- VDA のアンインストール中に、Citrix Workspace App をアンインストールしないことを選択できます。デフォルトでは、VDA のアンインストール中に Citrix Workspace App もアンインストールされます。

ステップ6. 追加コンポーネントをインストールします

VDAインストーラーの追加コンポーネントページ(/en-us/citrix-virtual-apps-desktops/2407/media/vda-ss-addtnl-components.png)

「**追加コンポーネント**」ページには、VDA とともに他の機能やテクノロジーのインストールを有効または無効にするためのチェックボックスが含まれています。コマンドラインインストールでは、`/exclude` または `/includeadditional` オプションを使用して、利用可能なコンポーネントを明示的に除外または含めることができます。

- **/includeadditional** "*コンポーネント*"\[,"*コンポーネント*"\] ...
- **/exclude** "*コンポーネント*"\[,"*コンポーネント*"\] ...

次の表は、このページの項目のデフォルト設定を示しています。デフォルト設定は、「**環境**」ページで選択したオプションによって異なります。

追加コンポーネントページ	環境ページ：「MCS を使用したマスターイメージ」または「CITRIX PROVISIONING を使用したマスターイメージ」が選択されている場合	環境ページ：「サーバーへの仲介接続を有効にする」（マルチセッションOSの場合）または「リモートPCアクセス」（シングルセッションOSの場合）が選択されている場合
App-V用Citrixパーソナライゼーション - VDA	選択されていません	選択されていません
ユーザーパーソナライゼーションレイヤー	選択されていません	このユースケースでは無効なため表示されません。
Citrix プロファイル管理	選択済み	選択されていません

追加コンポーネントページ	環境ページ：「MCS を使用したマスターイメージ」または「CITRIX PROVISIONING を使用したマスターイメージ」が選択されている場合	環境ページ：「サーバーへの仲介接続を有効にする」（マルチセッションOSの場合）または「リモートPCアクセス」（シングルセッションOSの場合）が選択されている場合
Citrix Profile Management WMI プラグイン	選択済み	選択されていません
Citrix VDA アップグレードエージェント	選択されていません	選択されていません
Citrix バックアップと復元	選択されていません	選択されていません
シトリックス MCS I/O ドライバー	選択されていません	選択されていません
シトリックス ランデブー V2	選択されていません	選択されていません

このページは、次の場合には表示されません。

- `VDAWorkstationCoreSetup.exe` インストーラーを使用している場合。また、追加コンポーネントのコマンドラインオプションは、そのインストーラーでは無効です。
- VDA をアップグレードしていて、すべての追加コンポーネントがすでにインストールされている場合。一部の追加コンポーネントがすでにインストールされている場合、そのページにはインストールされていないコンポーネントのみが表示されます。

次のチェックボックスをオンまたはオフにします。(コンポーネントはインストーラーで異なる順序で表示される場合があります。)

- **Citrix Personalization for App-V:** Microsoft App-Vパッケージのアプリケーションを使用する場合は、このコンポーネントをインストールします。詳細については、「App-Vアプリケーションの展開と配信」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Personalization for App-V – VDA"`、コンポーネントのインストールを防止するには `/exclude "Citrix Personalization for App-V – VDA"`。
- **Citrixユーザーパーソナライゼーションレイヤー:** ユーザーパーソナライゼーションレイヤー用のMSIをインストールします。詳細については、「ユーザーパーソナライゼーションレイヤー」を参照してください。

このコンポーネントは、シングルセッションのWindows 10マシンにVDAをインストールする場合にのみ表示されます。

コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "User Personalization Layer"`、コンポーネントのインストールを防止するには `/exclude "User Personalization Layer"`。

- **Citrix Profile Management:** このコンポーネントは、ユーザープロファイル内のユーザー個人設定を管理します。詳細については、「Profile Management」を参照してください。

  Citrix Profile Managementをインストールから除外すると、Citrix DirectorによるVDAの監視とトラブルシューティングに影響します。**User details**ページと**End Point**ページでは、**Personalization**パネルと**Logon Duration**パネルが機能しません。**Dashboard**ページと**Trends**ページでは、**Average Logon Duration**パネルはProfile Managementがインストールされているマシンのみのデータを表示します。

  サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrixは Citrix Profile Management Serviceをインストールして実行することをお勧めします。Citrix Profile Management Serviceを有効にする必要はありません。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Profile Management"`、コンポーネントのインストールを防止するには `/exclude "Citrix Profile Management"`。

- **Citrix Profile Management WMIプラグイン:** このプラグインは、WMI（Windows Management Instrumentation）オブジェクト（プロファイルプロバイダー、プロファイルタイプ、サイズ、ディスク使用量など）でProfile Managementのランタイム情報を提供します。WMIオブジェクトは、Directorにセッション情報を提供します。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Profile Management WMI Plug-in"`、コンポーネントのインストールを防止するには `/exclude "Citrix Profile Management WMI Plug-in"`。

- **VDA Upgrade Agent:** Citrix DaaS（旧称Citrix Virtual Apps and Desktopsサービス）展開にのみ適用されます。VDAがVDA Upgrade機能に参加できるようにします。この機能を使用すると、管理コンソールから、即時またはスケジュールされた時間にカタログのVDAをアップグレードできます。このエージェントがインストールされていない場合、VDAインストーラーをマシンで実行することでVDAをアップグレードできます。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix VDA Upgrade Agent"`、コンポーネントのインストールを防止するには `/exclude "Citrix VDA Upgrade Agent"`。

- **ストレージ最適化のためのMCSIO書き込みキャッシュ:** Citrix MCS I/Oドライバーをインストールします。詳細については、「ハイパーバイザーで共有されるストレージ」および「一時データ用のキャッシュの構成」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix MCS IODriver"`、コンポーネントのインストールを防止するには `/exclude "Citrix MCS IODriver"`。

- **プロキシ構成:** 環境でGateway Service、VDA Upgrade ServiceなどとともにRendezvousプロトコルを使用する予定があり、アウトバウンド接続用にネットワークに非透過型プロキシがある場合は、ここでプロキシを指定します。HTTPプロキシのみがサポートされています。

  このコンポーネントをインストールする場合は、**Rendezvous Proxy Configuration**ページでプロキシのアドレスまたはPACファイルのパスを指定します。機能の詳細については、「Rendezvousプロトコル」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Rendezvous V2"`、コンポーネントのインストールを防止するには `/exclude "Citrix Rendezvous V2"`。

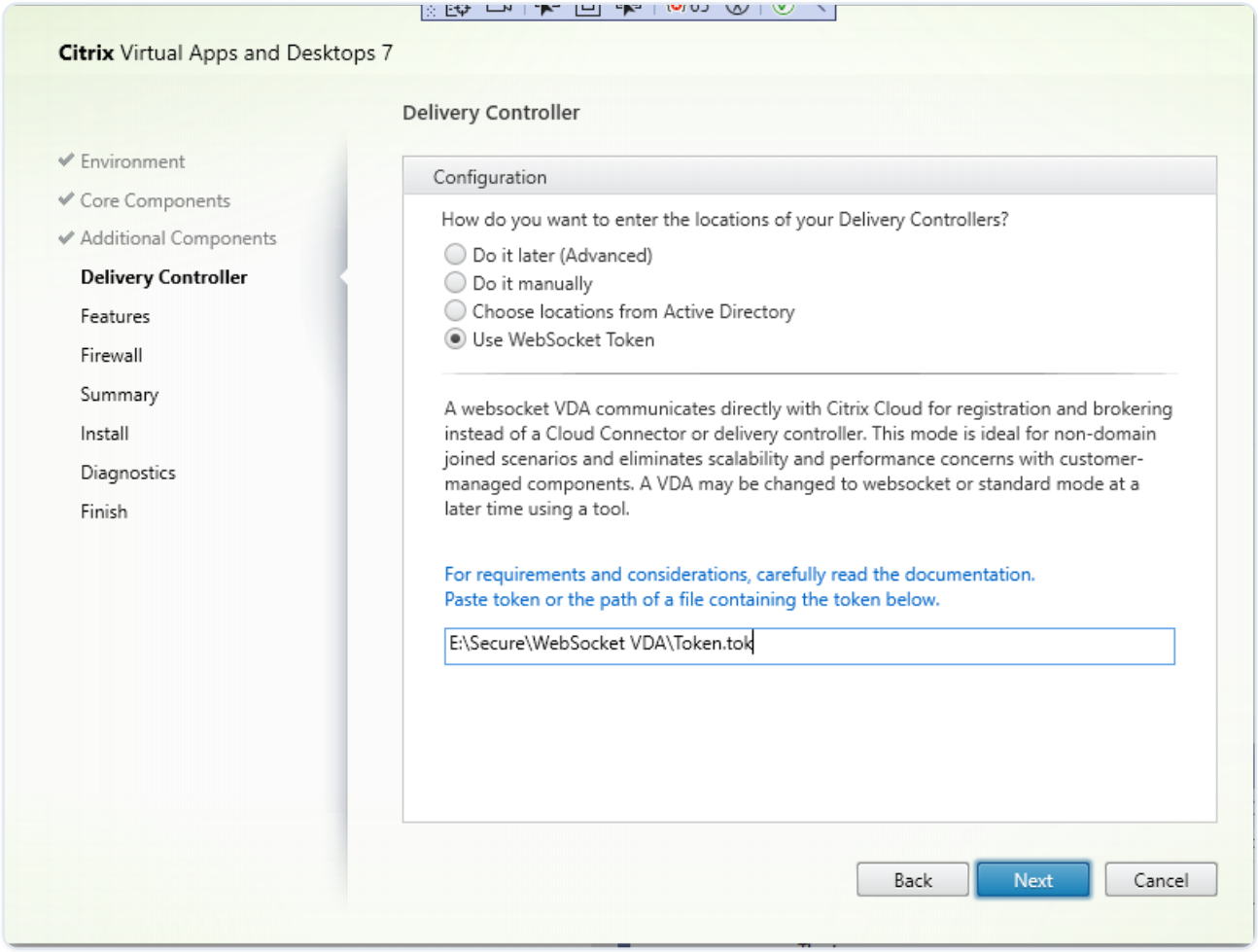
- **Citrix Backup and Restore:** VDAのインストールまたはアップグレードが失敗した場合、このコンポーネントはマシンをインストールまたはアップグレード前のバックアップ状態に戻すことができます。

  「インストール準備」に記載されているように、Microsoft の前提条件が満たされていることを確認してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Backup and Restore"`、コンポーネントのインストールを防止するには `/exclude "Citrix Backup and Restore"`。

> **注:**
>
> MCS ストレージ最適化が有効になっている場合、Windows サーバーまたはデスクトップオペレーティングシステムのバックアップまたは復元が失敗する可能性があります。これを解決するには、メタインストーラーで MCS ストレージ最適化オプションを無効にします。

ステップ 7. Delivery Controller™ アドレス



Delivery Controller ページで、インストールされている Controller のアドレスを入力する方法を選択します。Citrix では、VDA のインストール中にアドレスを指定することをお勧めします (**手動で実行**)。VDA はこの情報がないと Controller に登録できません。VDA が登録できない場合、ユーザーはその VDA 上のアプリケーションやデスクトップにアクセスできません。

- **手動で実行:** (デフォルト) インストールされている Controller の FQDN を入力し、**追加** をクリックします。複数の Controller をインストールしている場合は、それらのアドレスを追加します。
- **後で実行 (詳細):** このオプションを選択すると、ウィザードは続行する前に、その操作を実行することを確認するよう求めます。アドレスを後で指定するには、インストーラーを再実行するか、Citrix グループポリシーを使用します。ウィザードは **概要** ページでも通知します。
- **Active Directory から場所を選択:** マシンがドメインに参加しており、ユーザーがドメインユーザーである場合にのみ有効です。
- **WebSocket トークンを使用 (テクニカルプレビュー):** WebSocket VDA を作成します。WebSocketToken は、必要なトークン用です。

- **Machine Creation Services に自動的に実行させる:** MCS を使用してマシンをプロビジョニングする場合にのみ有効です。

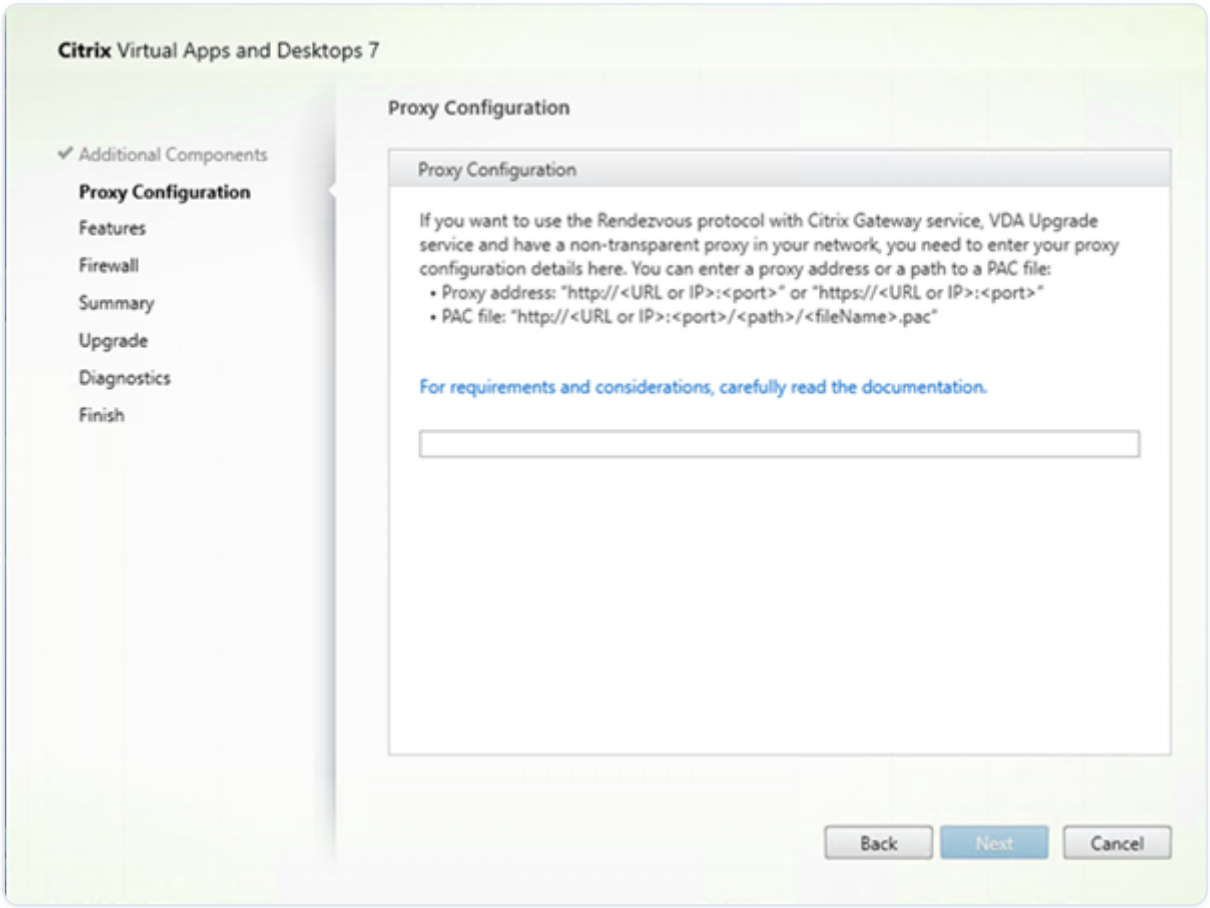
次へ をクリックします。**後で実行 (詳細)** を選択した場合、Controller アドレスを後で指定することを確認するよう求められます。

その他の考慮事項:

- アドレスには英数字以外の文字を含めることはできません。
- VDAインストール時およびグループポリシーでアドレスを指定した場合、ポリシー設定がインストール時に指定された設定を上書きします。
- VDA登録を成功させるには、Controllerとの通信に使用されるファイアウォールポートが開いている必要があります。このアクションは、ウィザードの**ファイアウォール**ページでデフォルトで有効になっています。
- Controllerの場所を指定した後（VDAインストール中またはインストール後）、Controllerが追加または削除されたときにVDAを更新するために自動更新機能を使用できます。VDAがControllerを検出して登録する方法の詳細については、VDA登録を参照してください。

コマンドラインオプション: `/controllers`

ステップ8. プロキシ構成



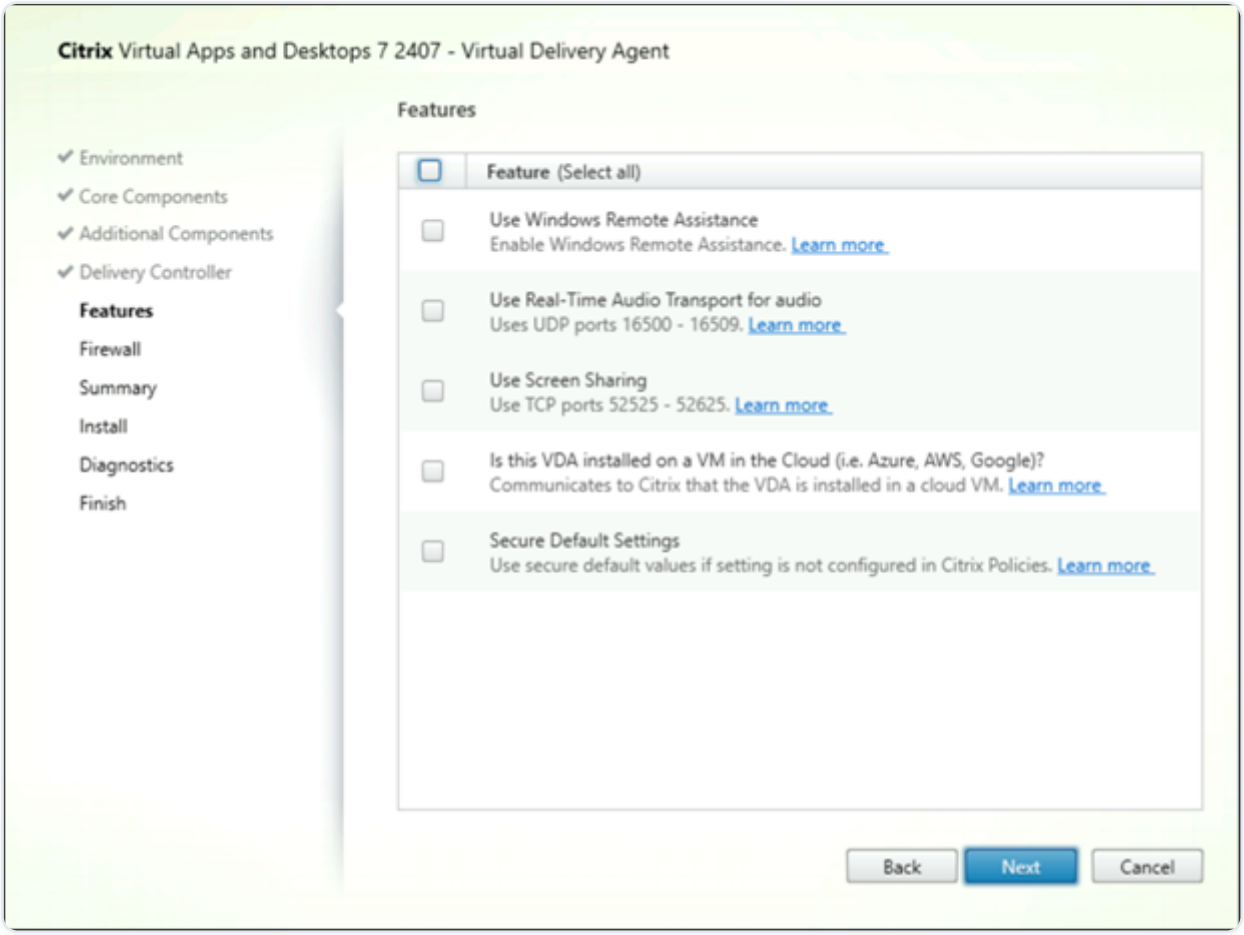
プロキシ構成ページは、**追加コンポーネント**ページで**プロキシ構成**チェックボックスを有効にした場合にのみ表示されます。

1. プロキシソースをプロキシアドレスで指定するか、PACファイルパスで指定するかを選択します。
2. プロキシアドレスまたはPACファイルパスを指定します。
   - プロキシアドレスの形式: `http://<url-or-ip>:<port>`
   - PACファイルの形式: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

接続テストを成功させるには、プロキシポートのファイアウォールが開いている必要があります。プロキシへの接続ができない場合でも、VDAのインストールを続行するかどうかを選択できます。

コマンドラインオプション: `/proxyconfig`

ステップ9. 機能の有効化または無効化



機能ページで、チェックボックスを使用して、使用する機能を有効または無効にします。

- **Windows リモートアシスタンスを使用する:** この機能を有効にすると、Director のユーザーシャドウ機能で Windows リモートアシスタンスが使用されます。Windows リモートアシスタンスは、ファイアウォールで動的ポートを開きます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_remote_assistance`

- **オーディオにリアルタイムオーディオトランスポートを使用する:** ネットワークで Voice-over-IP が広く使用されている場合は、この機能を有効にします。この機能は、遅延を減らし、損失の多いネットワークでのオーディオの回復力を向上させます。RTP over UDP トランスポートを使用してオーディオデータを送信できます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_real_time_transport`

- **画面共有を使用する:** 有効にすると、画面共有で使用されるポートが Windows ファイアウォールで開かれます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_ss_ports`

- **この VDA はクラウドの VM にインストールされていますか:** この設定は、Citrix がテレメトリ目的でオンプレミスおよびサービス (Citrix Cloud™) VDA 展開のリソースの場所を正しく識別するのに役立ちます。この機能は、顧客側の利用には影響しません。展開で Citrix DaaS を使用している場合は、この設定を有効にします。(デフォルト = 無効).

  コマンドラインオプション: `/xendesktopcloud`

- **セキュアなデフォルト設定:** このオプションは、より安全な初期設定のために、さまざまな機能のデフォルト設定を有効から無効に変更します。関連する機能は次のとおりです: クライアントドライブリダイレクト、特殊フォルダーリダイレクト、ドラッグアンドドロップ、クライアント TWAIN デバイスリダイレクト、クライアント USB プラグアンドプレイデバイスリダイレクト、クライアントプリンターリダイレクト、クライアントクリップボードリダイレクト、クライアントマイクのリダイレクト。

コマンドラインオプション: `/ENABLE_SECURE_DEFAULTS`

Nextをクリックします。

手順 10. ファイアウォールポート

VDA インストーラーのファイアウォールページ(/en-us/citrix-virtual-apps-desktops/2407/media/vda-ss-firewall.png)

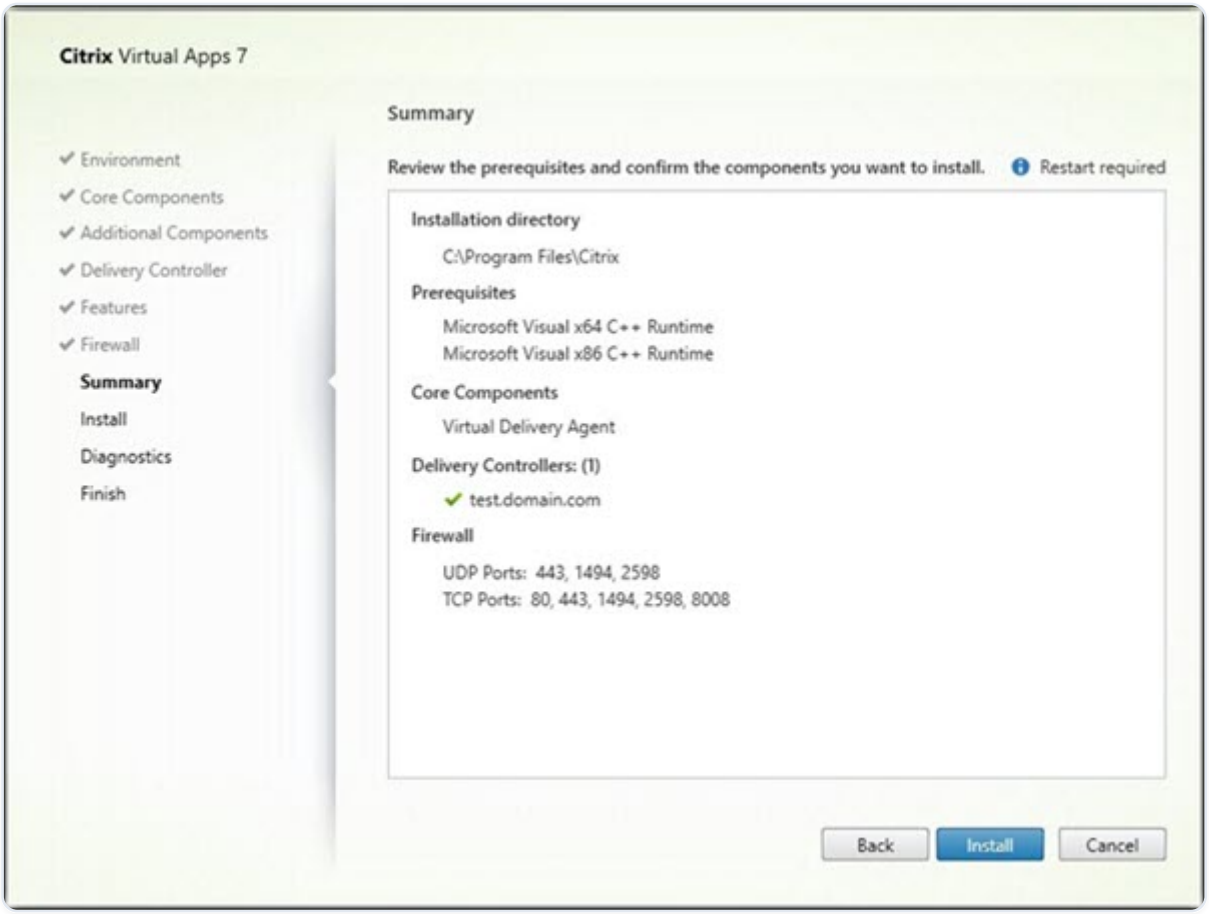
「**ファイアウォール**」ページでは、デフォルトで、Windows ファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくてもポートは自動的に開かれます。このデ

フォルト設定は、ほとんどの展開で問題ありません。ポート情報については、「ネットワークポート」を参照してください。

Nextをクリックします。

コマンドラインオプション: `/enable_hdx_ports`

手順 11. 前提条件を確認し、インストールを確定する

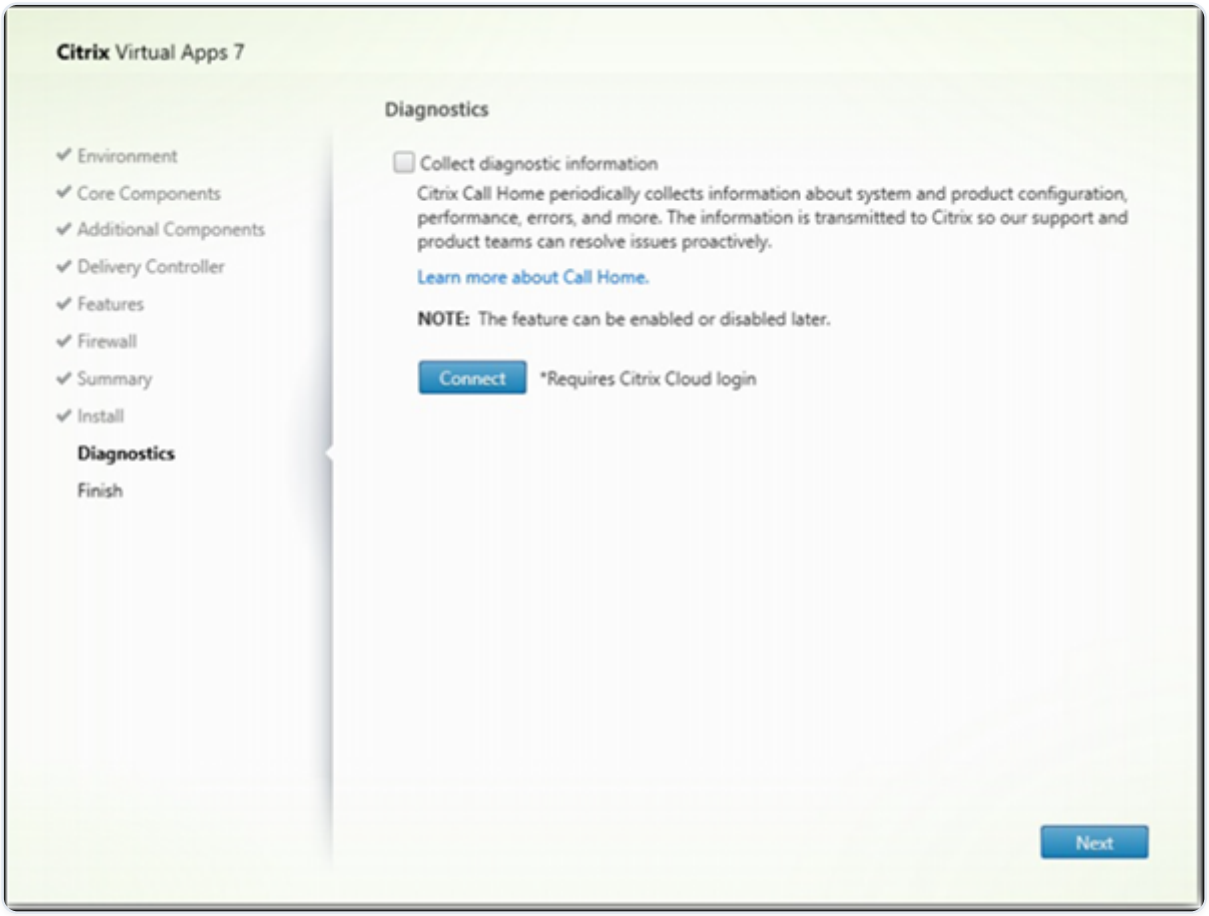


概要ページには、インストールされるものが表示されます。**戻る**ボタンを使用して、以前のウィザードページに戻り、選択を変更します。

準備ができたら、**インストール**をクリックします。

前提条件がまだインストールまたは有効になっていない場合、マシンは1回以上再起動する可能性があります。インストールの準備を参照してください。

ステップ12. 診断



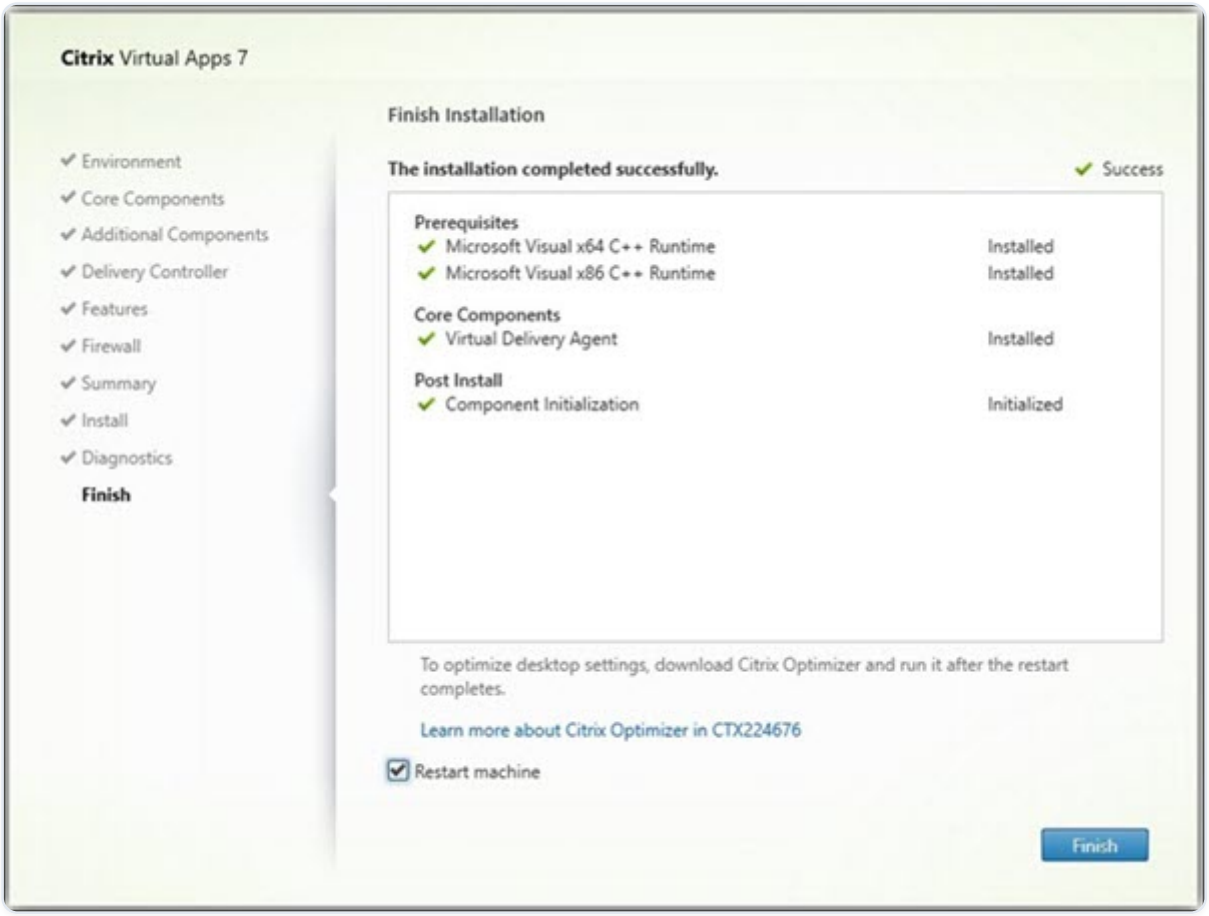
診断ページで、Citrix Call Homeに参加するかどうかを選択します。参加することを選択した場合（デフォルト）、**接続**をクリックします。プロンプトが表示されたら、Citrixアカウントの資格情報を入力します。

資格情報が検証された後（または参加しないことを選択した場合）、**次へ**をクリックします。

フル製品インストーラーを使用している場合、**診断**ページで、最初に**診断情報の収集**を選択せずに**接続**をクリックすると、**Citrix Insight Servicesへの接続**ダイアログを閉じると、**次へ**ボタンが無効になります。次のページに進むことはできません。**次へ**ボタンを再度有効にするには、**診断情報の収集**を選択し、すぐに選択を解除します。

詳細については、Call Homeを参照してください。

ステップ13. このインストールを完了する



完了ページには、正常にインストールおよび初期化されたすべての前提条件とコンポーネントの緑色のチェックマークが表示されます。

完了をクリックします。デフォルトでは、マシンは自動的に再起動します。この自動再起動を無効にすることはできますが、マシンが再起動するまでVDAは使用できません。

次のステップ

必要に応じて、上記のプロシージャを繰り返して、他のマシンまたはイメージにVDAをインストールします。

すべてのVDAをインストールしたら、Studioを起動します。まだサイトを作成していない場合、Studioはそのタスクに自動的に誘導します。それが完了すると、Studioはマシンカタログとデリバリーグループの作成に誘導します。参照：

- サイトの作成(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/site-create.html)
- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html)
- デリバリーグループの作成(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/delivery-groups-create.html)

シトリックス オプティマイザー

Citrix Optimizerは、Citrix管理者がさまざまなコンポーネントを削除および最適化することでVDAを最適化するのに役立つWindows OS用のツールです。

VDAをインストールし、最終的な再起動を完了した後、Citrix Optimizerをダウンロードしてインストールします。CTX224676を参照してください。CTX記事には、ダウンロードパッケージと、Citrix Optimizerのインストールおよび使用に関する手順が含まれています。

VDAをカスタマイズする

インストール済みのVDAをカスタマイズするには：

1. プログラムの削除または変更のためのWindows機能から、「**Citrix Virtual Delivery Agent**」または「**Citrix Remote PC Access/VDI Core Services VDA**」を選択します。次に右クリックして「**変更**」を選択します。
2. 「**Virtual Delivery Agent設定のカスタマイズ**」を選択します。インストーラーが起動すると、以下を変更できます。

    - Controllerアドレス
    - Controllerに登録するTCP/IPポート（デフォルト = 80）
    - Windowsファイアウォールポートを自動的に開くかどうか

トラブルシューティング

- Citrixがコンポーネントインストールの結果を報告する方法については、Citrixインストールのリターンコードを参照してください。
- デリバリーグループのStudio表示で、**詳細**ペインの**インストール済みVDAバージョン**エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンのWindowsのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされても、Delivery Controllerに登録されるまでは、ユーザーにアプリやデスクトップを提供できません。

    VDAの登録方法と登録の問題のトラブルシューティングについては、VDA登録を参照してください。

既知の制限事項

Citrix Workspace app for Windowsバージョン1912以前を使用すると、しばらくするとセッションが切断されます。この問題は、Citrix Workspace appの新しいLTSRおよびCRバージョンで修正さ

れています。 サポートされているリリースバージョンの詳細については、Citrix Workspace app for Windows / Citrix Receiver for Windows Long Term Service Releasesを参照してください。

スクリプトを使用してVDAをインストールする

> **注:**
>
> Citrixは、お客様の運用環境に合わせて変更されたスクリプトによって引き起こされる問題について責任を負いません。インストール関連のCitrixの問題については、Citrixサポートポータルを使用して、関連するインストールログとともにテクニカルサポートケースをオープンしてください。

> この記事は、Windowsオペレーティングシステムを搭載したマシンへのVDAのインストールに適用されます。Linuxオペレーティングシステム用VDAの詳細については、Linux Virtual Delivery Agentのドキュメントを参照してください。

インストールメディアには、Active Directory内のマシンにVirtual Delivery Agent（VDA）をインストール、アップグレード、または削除するサンプルスクリプトが含まれています。これらのスクリプトは、Machine Creation Services™およびCitrix Provisioning（旧Provisioning Services）で使用されるマスターイメージの保守にも使用できます。

必要なアクセス権:

- スクリプトには、VDAインストールコマンドが配置されているネットワーク共有へのEveryone読み取りアクセス権が必要です。インストールコマンドは、完全な製品ISOでは `XenDesktopVdaSetup.exe`、スタンドアロンインストーラーでは `VDAWorkstationSetup.exe` または `VDAServerSetup.exe` です。
- ログの詳細は各ローカルマシンに保存されます。レビューと分析のために結果を一元的にログに記録するには、スクリプトに適切なネットワーク共有へのEveryone読み取りおよび書き込みアクセス権が必要です。

スクリプトの実行結果を確認するには、中央ログ共有を調べます。キャプチャされたログには、スクリプトログ、インストーラーログ、およびMSIインストールログが含まれます。各インストールまたは削除の試行は、タイムスタンプ付きのフォルダーに記録されます。フォルダーのタイトルは、PASSまたはFAILのプレフィックスで操作結果を示します。標準のディレクトリ検索ツールを使用して、中央ログ共有で失敗したインストールまたは削除を見つけることができます。これらのツールは、ターゲットマシンでローカルに検索する代替手段を提供します。

インストールを開始する前に、インストールの準備のタスクを読み、完了してください。

スクリプトを使用してVDAをインストールまたはアップグレードする

1. インストールメディアの\\Support\\AdDeploy\\からサンプルスクリプト**InstallVDA.bat**を入手します。Citrixは、スクリプトをカスタマイズする前に元のスクリプトのバックアップを作成することをお勧めします。
2. スクリプトを編集します。
   - インストールするVDAのバージョンを指定します: `SET DESIREDVERSION`。完全な値は、インストールメディアのProductVersion.txtファイルで確認できます。ただし、完全な一致は必須ではありません。
   - インストーラーが呼び出されるネットワーク共有を指定します。レイアウトのルート（ツリーの最上位）を指します。スクリプトの実行時に、インストーラーの適切なバージョン（32ビットまたは64ビット）が自動的に呼び出されます。例: `SET DEPLOYSHARE=\\fileserver1\share1`。
   - 任意で、一元化されたログを保存するためのネットワーク共有の場所を指定します。例: `SET LOGSHARE=\\fileserver1\log1)`。
   - コマンドラインを使用したインストールで説明されているように、VDA構成オプションを指定します。`/quiet`および`/noreboot`オプションは、スクリプトにデフォルトで含まれており、必須です: `SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT /NORESUME`。
3. グループポリシーのスタートアップスクリプトを使用して、マシンを含むOUにスクリプトを割り当てます。このOUには、VDAをインストールするマシンのみを含める必要があります。そのOU内のマシンが再起動されると、スクリプトはすべてのマシンで実行されます。サポートされているオペレーティングシステムを持つ各マシンにVDAがインストールされます。

スクリプトを使用してVDAを削除する

1. インストールメディアの\\Support\\AdDeploy\\からサンプルスクリプトUninstallVDA.batを取得します。Citrixでは、元のスクリプトをカスタマイズする前にバックアップを作成することをお勧めします。
2. スクリプトを編集します。
   - 削除するVDAのバージョンを指定します: `SET CHECK\_VDA\_VERSION`。完全な値は、インストールメディアのProductVersion.txtファイル（例: 7.0.0.3018）にあります。ただし、完全一致は必須ではありません。
   - 任意で、一元化されたログを保存するためのネットワーク共有の場所を指定します。

3. グループポリシーのスタートアップスクリプトを使用して、マシンを含むOUにスクリプトを割り当てます。このOUには、VDAを削除するマシンのみを含める必要があります。OU内のマシンが再起動されると、スクリプトはすべてのマシンで実行されます。各マシンからVDAが削除されます。

トラブルシューティング

- スクリプトは、スクリプトの実行状況を記述する内部ログファイルを生成します。スクリプトは、展開の開始から数秒以内に`Kickoff_VDA_Startup_Script`ログを中央ログ共有にコピーします。全体的なプロセスが機能していることを確認できます。このログが期待どおりに中央ログ共有にコピーされない場合は、ローカルマシンを検査してさらにトラブルシューティングを行ってください。スクリプトは、各マシンの`%temp%`フォルダーに2つのデバッグログファイルを配置します:

  - `Kickoff_VDA_Startup_Script_<DateTimeStamp>.log`
  - `VDA_Install_ProcessLog_<DateTimeStamp>.log`

  スクリプトが次の状態であることを確認するために、これらのログを確認します。

  - 期待どおりに実行されている。
  - ターゲットオペレーティングシステムを適切に検出する。
  - `DEPLOYSHARE`共有の`ROOT`を指すように正しく構成されていること（`AutoSelect.exe`という名前のファイルが含まれています）。
  - `DEPLOYSHARE`と`LOG`の両方の共有に対して認証できること。

- コンポーネントのインストール結果がCitrixによってどのように報告されるかについては、「Citrixインストールリターンコード」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/install-prepare.html#citrix-installation-return-codes)を参照してください。
- デリバリーグループのStudio表示では、**詳細**ペインの**インストール済みVDAバージョン**エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされても、Delivery Controllerに登録されるまでは、ユーザーにアプリやデスクトップを配信できません。

  VDA登録方法と登録問題のトラブルシューティングについては、「VDA登録」(/ja-jp/citrix-virtual-apps-desktops/2407/manage-deployment/vda-registration.html)を参照してください。

サードパーティ製VDAの展開方法

Microsoft System Center Configuration Manager (SCCM) または Ansible や Microsoft Intunes などの同様のソフトウェア配布ツールを使用して Virtual Delivery Agent (VDA) を正常に展開するには、Citrix® はVDAインストーラーを段階的な手順で使用することをお勧めします。

> **注:**
>
> 以下の記事では、Citrix が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、お客様のニーズに合わせてカスタマイズできます。Citrix は、お客様のニーズに合わせてこれに必要な更新や調整について責任を負いません。

- SCCM を使用した VDA のインストール
- Ansible を使用した VDA のインストール
- Microsoft Intune を使用した VDA のインストール

SCCM を使用した VDA のインストール

概要

以前は System Center Configuration Manager (SCCM) と呼ばれていた Microsoft Endpoint Configuration Manager は、企業全体のデバイスとアプリケーションの管理、展開、セキュリティを可能にする Windows 製品です。

> **注:**
>
> 以下の記事では、Citrix® が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、必要に応じてカスタマイズできます。Citrix は、顧客のニーズに合わせてこれに必要な更新や調整について責任を負いません。

推奨事項

- SCCM または同様のソフトウェア配布ツールを使用して Virtual Delivery Agent (VDA) を正常に展開するには、Citrix は VDA インストーラーを段階的に使用することを推奨します。
- Citrix は、VDA のインストールまたはアップグレードの一部として VDA Cleanup Utility を使用することを推奨しません。VDA インストーラーが以前に失敗した場合にのみ、VDA Cleanup Utility を使用してください。

開始する前に

VDA のインストール中に必要な再起動の回数は、環境によって異なります。例:

- 以前のソフトウェアインストールによる保留中の更新または再起動のために、再起動が必要になる場合があります。
- 他のプロセスによって以前にロックされていたファイルは更新が必要になる場合があり、追加の再起動を強制します。
- VDA インストーラーの一部のオプションコンポーネント（Citrix Profile Management や Citrix Files など）は、再起動が必要になる場合があります。
- VDA をアップグレードする場合、それがインストールされているマシンは、セッションがないメンテナンスモードである必要があります。
- マシンで VDA のインストールが初めて実行されると、使用されている VDA インストーラーがそのマシンにコピーされます。 VDA のインストールに関する詳細については、「インストーラー」を参照してください。

SCCM タスク シーケンサーは、必要なすべての再起動を管理します。

SCCM を使用して VDA を展開するための主要な手順

次の手順では、仮想マシン上で SCCM を使用して VDA を展開する方法について説明します。

1. VDA をインストールする。
2. 組織単位 (OU) を作成する。
3. マシンを検証する。
4. VDA を使用してコンテンツを配布する。

ステップ 1: VDA をインストールする

すべての前提条件を特定した後、**SCCM タスク シーケンサー**を使用して次のタスクを完了します。

1. インストールメディアのアクセス可能なコピーから、またはVDAスタンドアロンインストーラーのいずれかからVDAをインストールします。

   - `VDAWorkstationSetup_XXXX.exe`
   - `VDAServerSetup_XXXX.exe`
   - `VDAWorkstationCoreSetup_XXXX.exe`

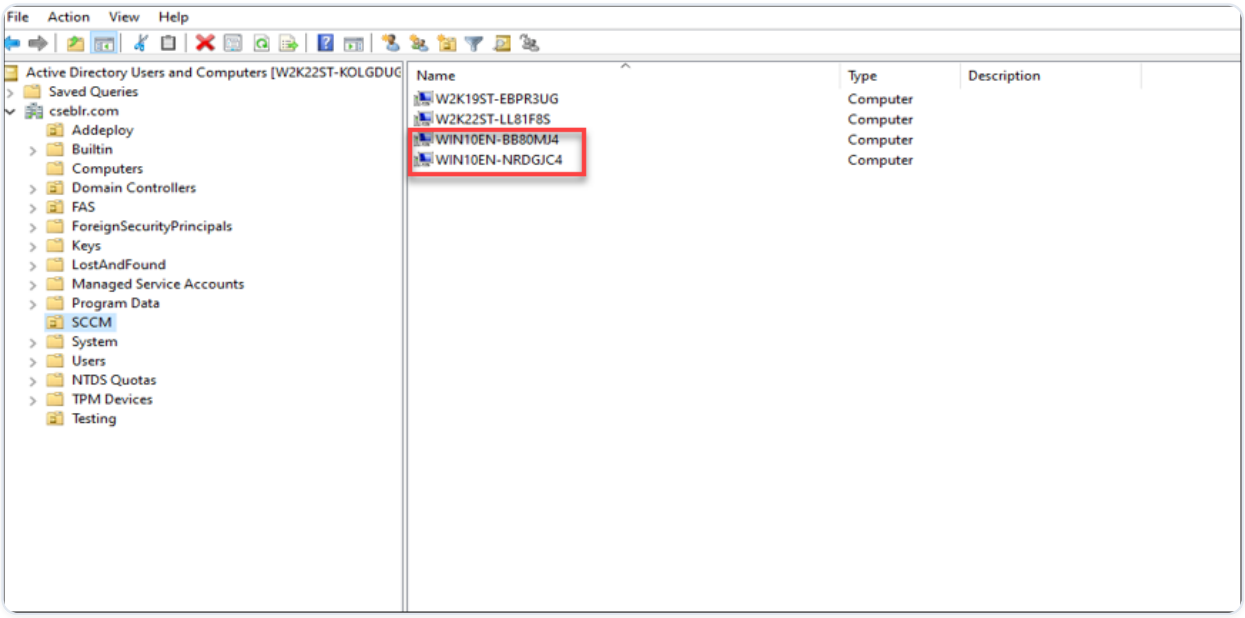
   VDAインストーラーの詳細については、「インストーラー」を参照してください。

> **注:**
>
> VDAをアップグレードする場合、VDAがインストールされているマシンは、セッションがないメンテナンスモードである必要があります。

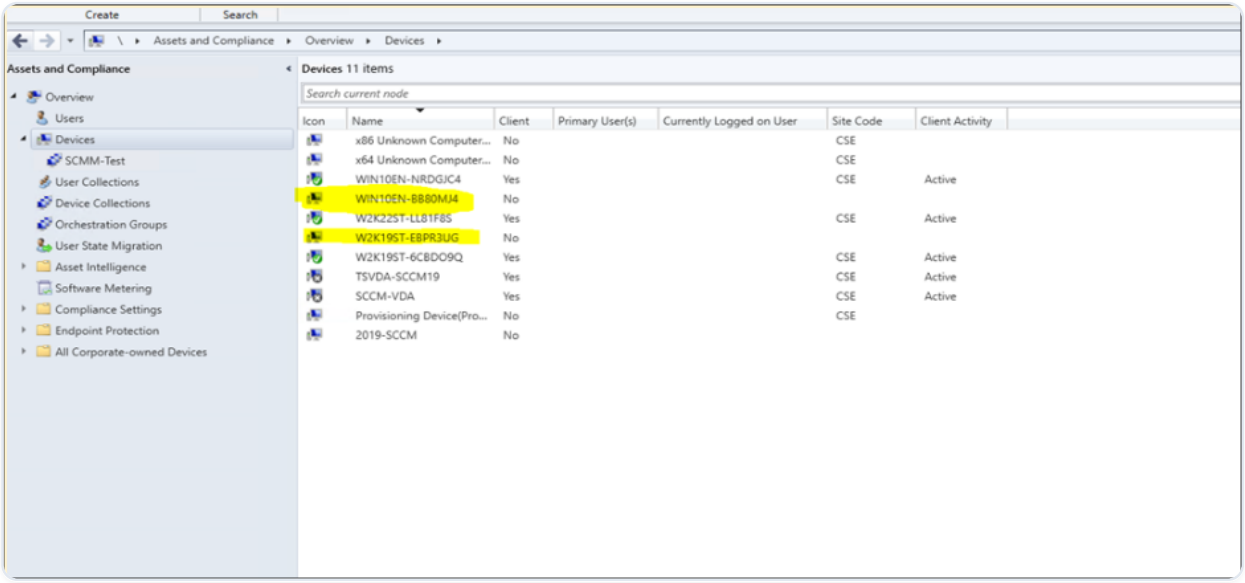
2. マシンでVDAのインストールが初めて実行されると、使用されているVDAインストーラーがそのマシンにコピーされます。
   - `VDAWorkstationCoreSetup_XXXX.exe`以外のVDAインストーラーを使用すると、VDAインストーラーは`%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe`にコピーされます。
   - `VDAWorkstationCoreSetup_XXXX.exe`を使用すると、VDAインストーラーは`%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe.`にコピーされます。
3. VDAインストーラーのディレクトリの場所は、レジストリ`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall”“MetaInstallerInstallLocation”`にも保存されます。
4. コマンドラインオプションに`/NOREBOOT`、`/NORESUME`、および`/QUIET`を追加します。
   - `/QUIET`: インストール中にユーザーインターフェイスを表示しないようにします。これにより、SCCMがインストールプロセスを制御できます。
   - `/NOREBOOT`: VDAインストーラーが自動的に再起動するのを抑制します。SCCMは必要に応じて再起動をトリガーします。
   - `/NORESUME`: 通常、インストール中に再起動が必要な場合、VDAインストーラーはrunonceレジストリキー(`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`)を設定します。Windowsはこのキーを使用して、マシンが再起動したときにVDAインストーラーを開きます。これはSCCMにとって問題となります。なぜなら、SCCMはインストールを監視して終了コードをキャプチャできないからです。

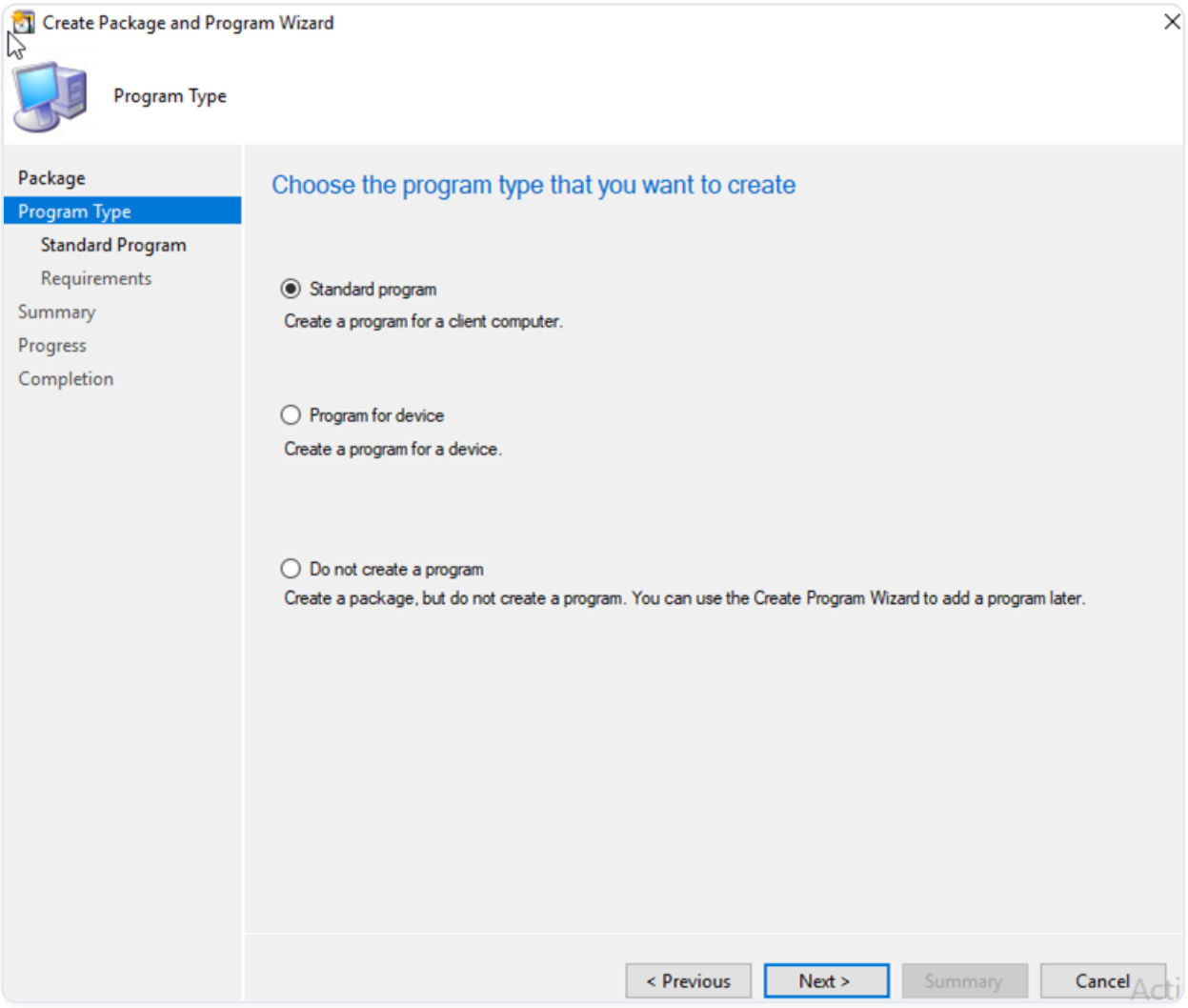
ステップ2: 組織単位 (OU) を作成する

1. OUに追加するドメイン参加済み仮想マシンを2台作成します。仮想マシンが最初に作成されたとき、それらは**Computers**フォルダーにあります。仮想マシンを**SCCM**フォルダーに移動します。 例: WIN10EN-BB80MJ4.cseblr.com W2K19ST-EBPR3UG.cseblr.com

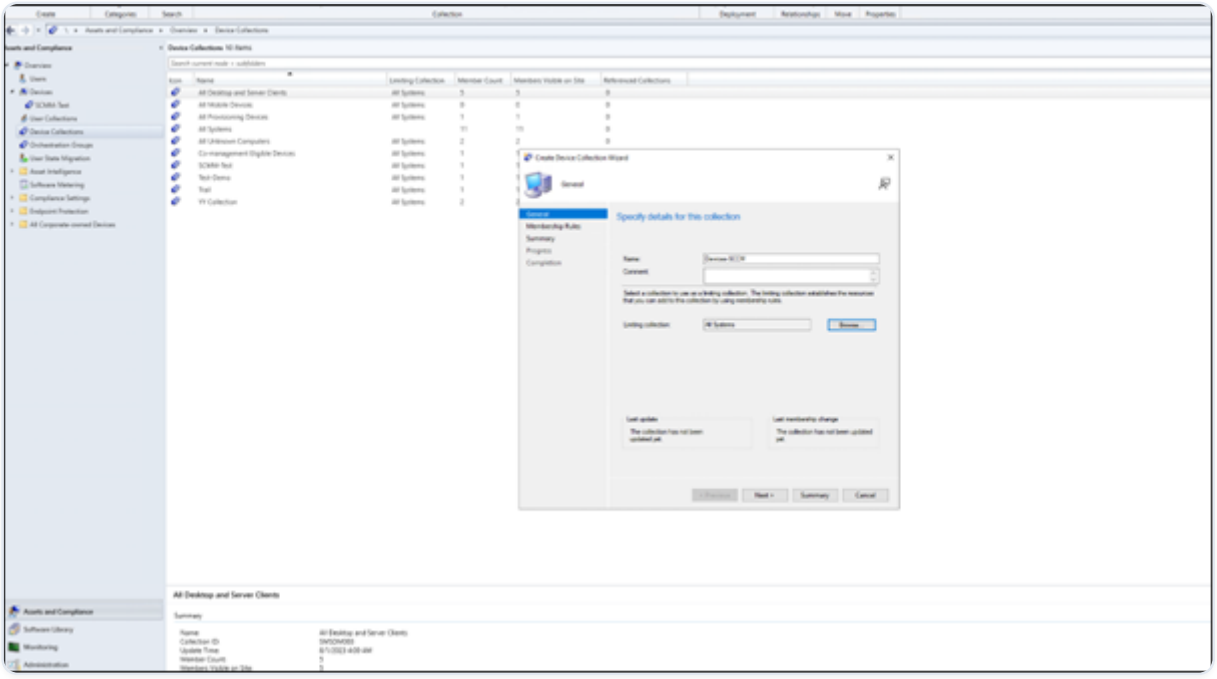


2. Microsoft Configuration Manager で、`\Administration\Overview\Hierarchy Configuration\Discovery Methods\` に移動します。
3. **Active Directory システム検出**をクリックし、**Active Directory システム検出を有効にする**チェックボックスを選択して、新しく作成された仮想マシンの自動検出を有効にします。
4.  アイコンをクリックして、新しいコンテナーを選択します。
5. **場所**セクションで、SCCM 仮想マシンが配置されている**パス**を追加します。
6. `\Administration\Overview\Site Configuration\Sites` に移動し、SCCM VDA を右クリックします。
7. **クライアントインストール設定 > クライアントプッシュインストール**を選択します。**クライアントプッシュインストールのプロパティ**ウィンドウが開きます。
8. VM が `Enabled` に設定されると、以下の画像に示すように VM のリストが表示されます。





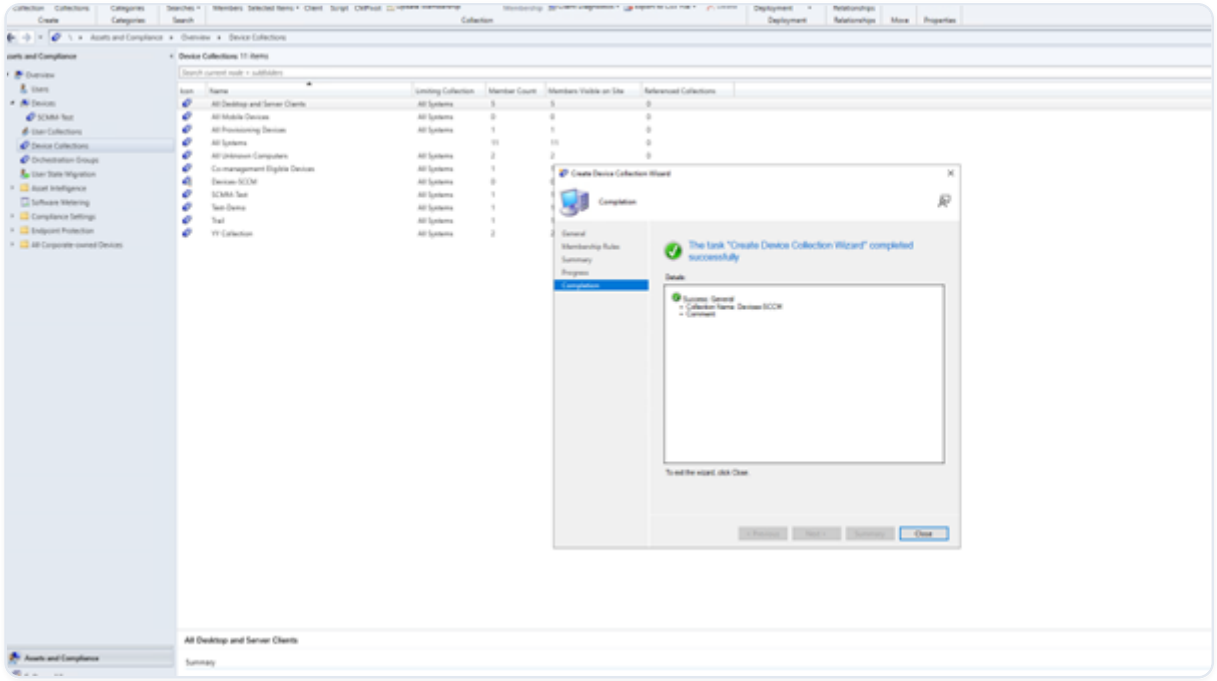
9. OU を作成するために**デバイスコレクション**を作成します。コレクション名の**名前**を入力します。



10. ウィザードの指示に従います。

メンバーシップルール(/en-us/citrix-virtual-apps-desktops/2407/media/sccm-membership-rules.png)

OUが作成されます。



11. 作成したVMを、新しく作成したデバイスコレクションに追加します。

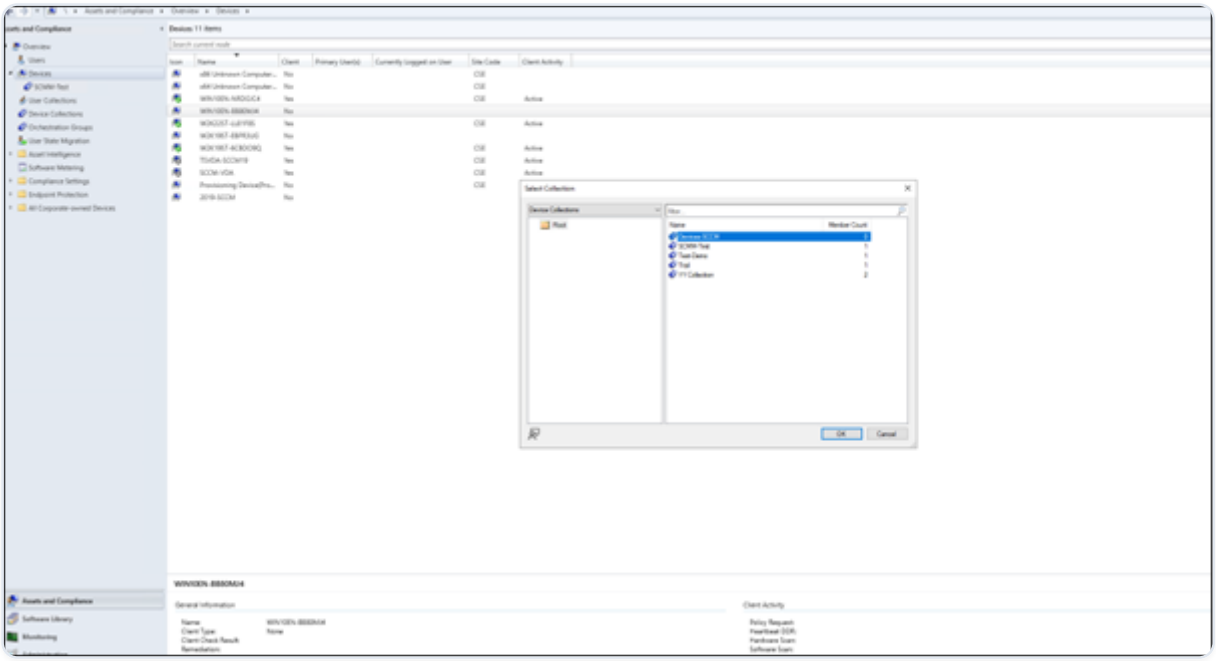
    a. VM を右クリックします。「**選択した項目を追加 > 選択した項目を既存のデバイスコレクションに追加**」を選択します。

    項目の追加(/en-us/citrix-virtual-apps-desktops/2407/media/sccm-add-item-to-device-collection.png)

    b. 「**コレクションの選択**」ウィンドウで、必要なデバイス名を選択します。この例では、`Devices-SCCM`です。

    デバイスリスト(/en-us/citrix-virtual-apps-desktops/2407/media/sccm-list.png)

`Devices-SCCM`は、**資産とコンプライアンス > 概要 > デバイスコレクション**に表示されます。



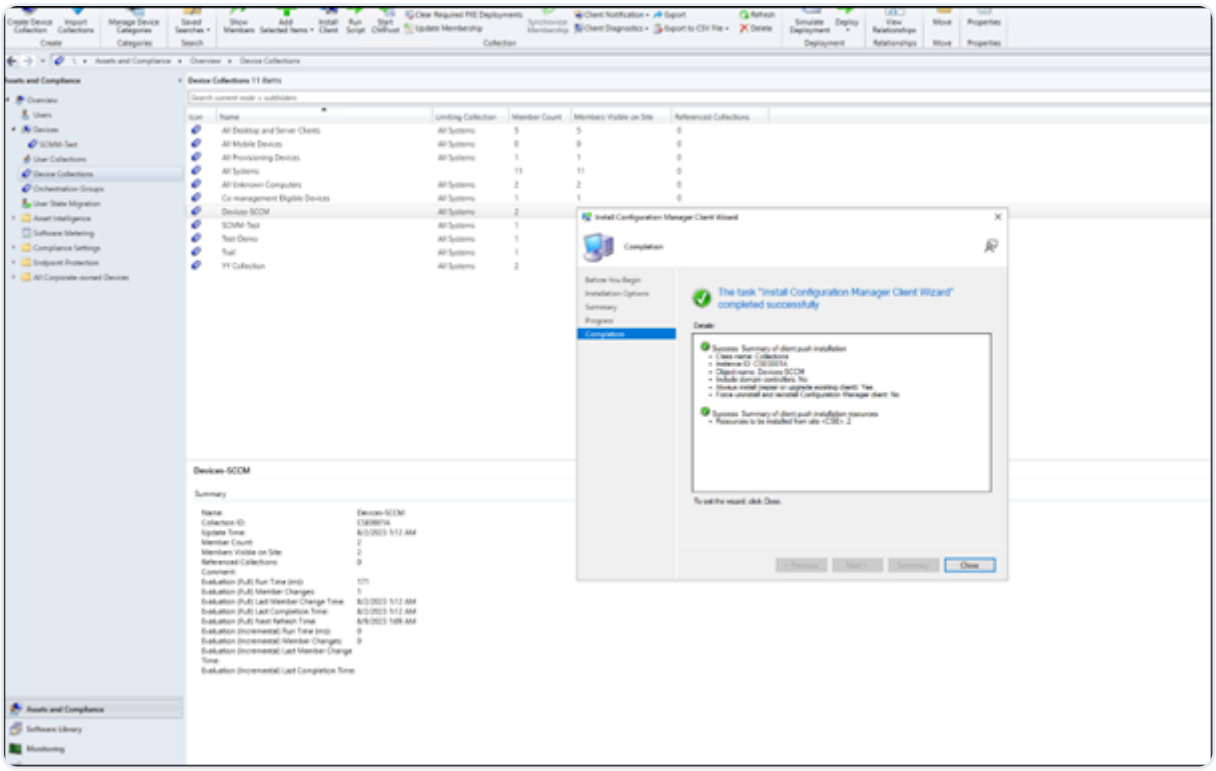
12. デバイスコレクターで「**クライアントのインストール**」を選択します。

    クライアントのインストール(/en-us/citrix-virtual-apps-desktops/2407/media/sccm-install-client.png)

13. 必要なインストール**サイト**を選択します。

    サイトのインストール(/en-us/citrix-virtual-apps-desktops/2407/media/sccm-install-client-1.png)

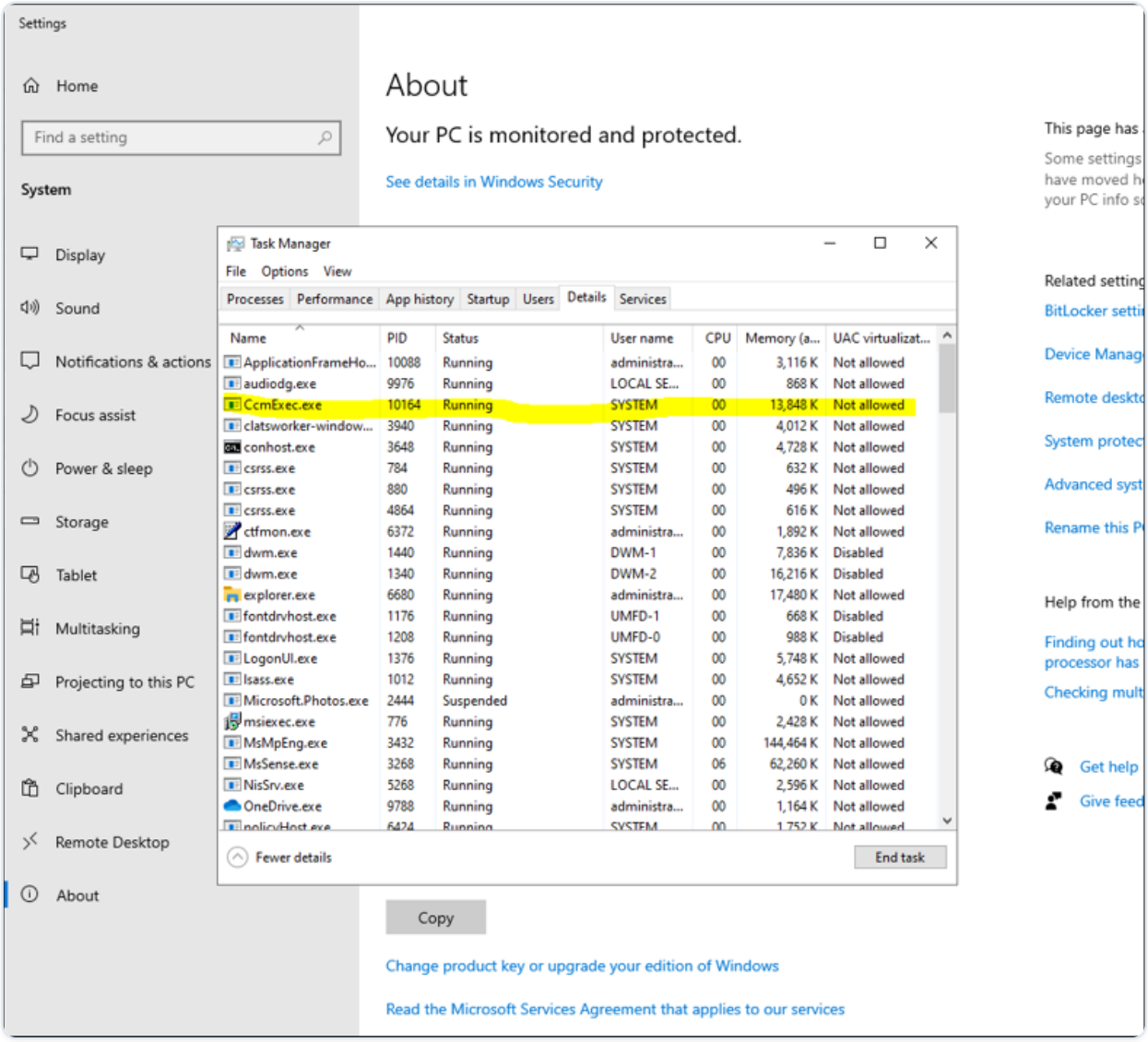
14. ウィザードの指示に従います。「**Configuration Manager クライアントのインストールウィザード**」が正常に完了しました。



詳細については、Microsoft ドキュメントの「コレクションの管理」を参照してください。

ステップ3：マシンの確認

1. クライアントマシンで、`CCMExec`プロセスが実行されていることを確認して、クライアントがインストールされていることを検証します。



2. SCCM上のVMでクライアントが実行されていることを確認します。

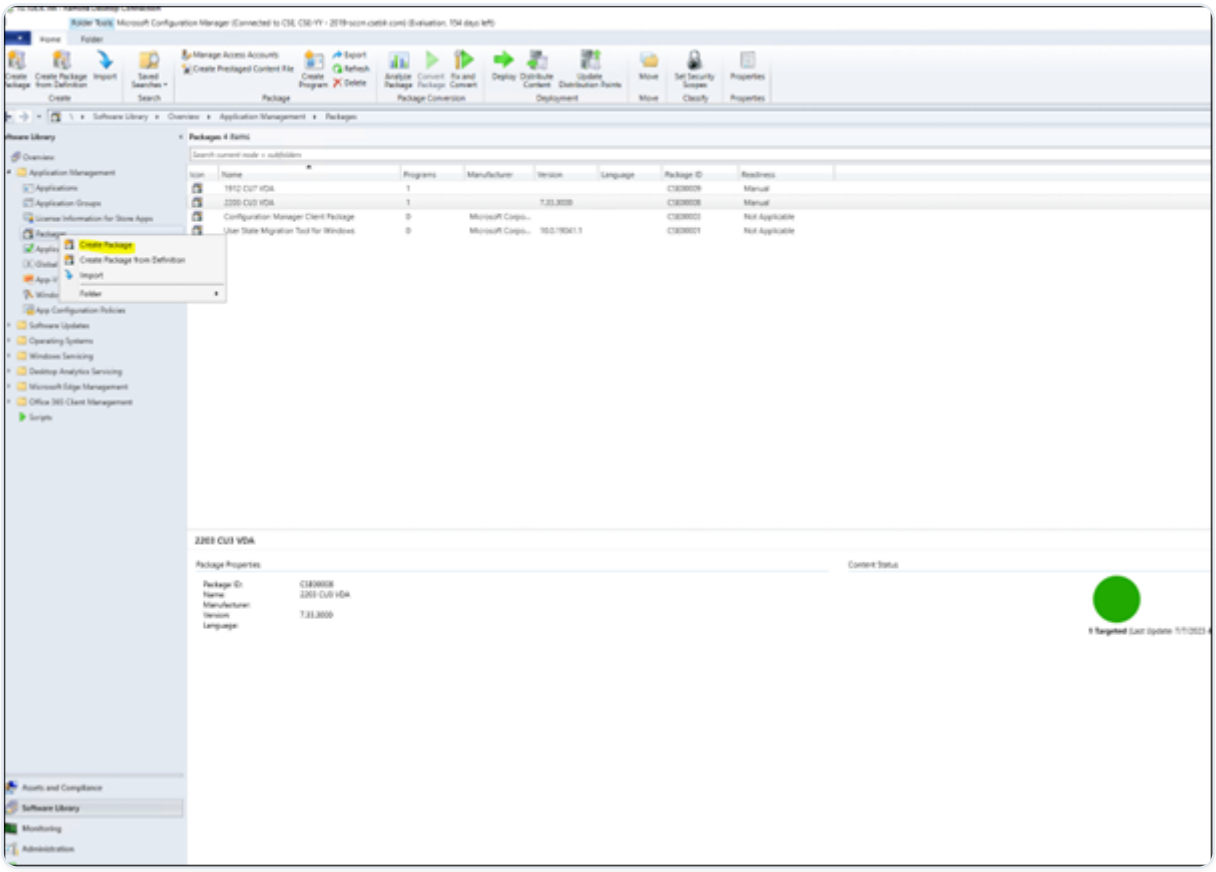
ステップ 4: VDA を使用してコンテンツを配布する

以下の手順では、展開されたVDAを使用して、関連する仮想マシンにコンテンツを配布する方法について説明します。

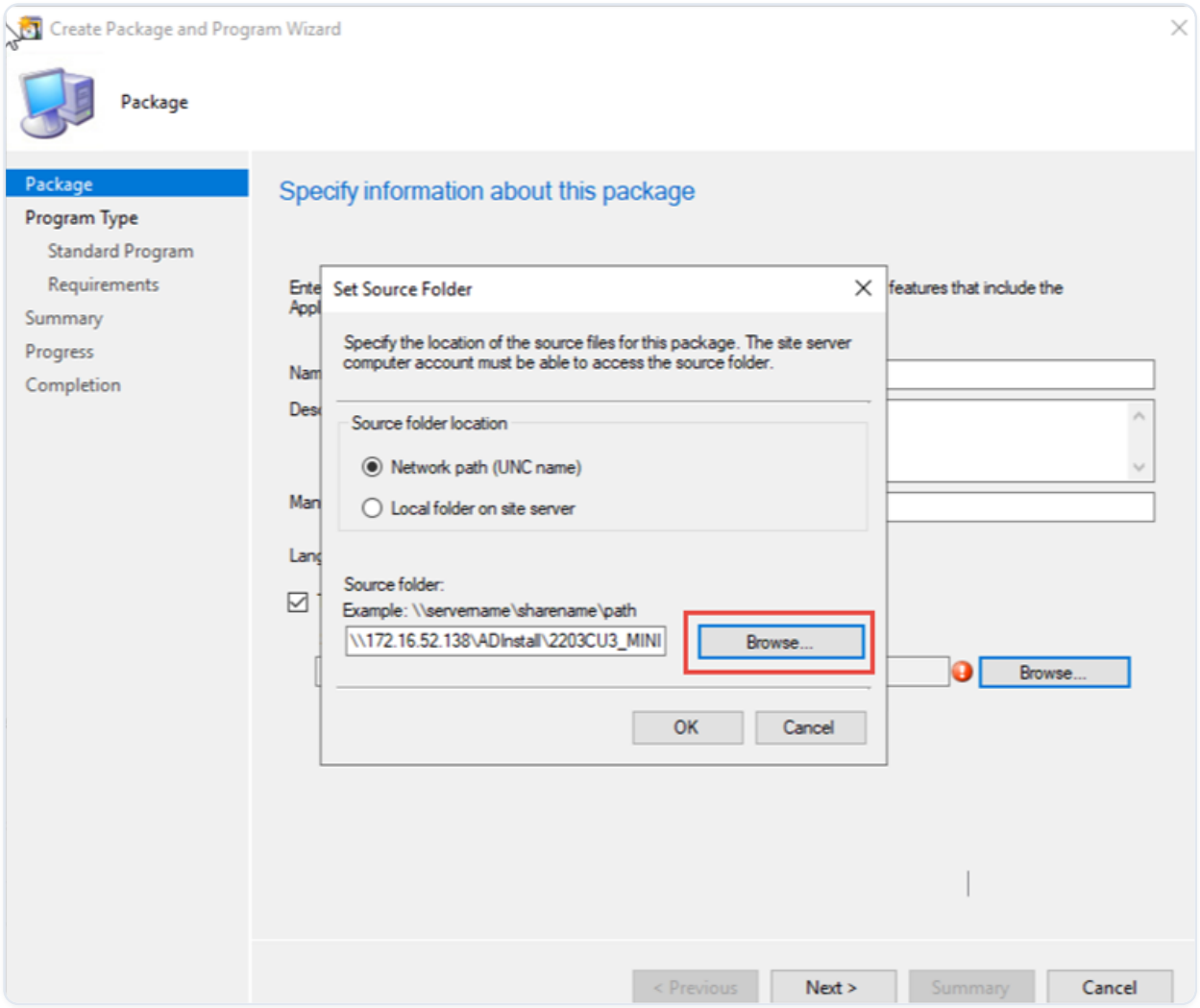
1. パッケージの作成
2. コンテンツの配布

パッケージの作成

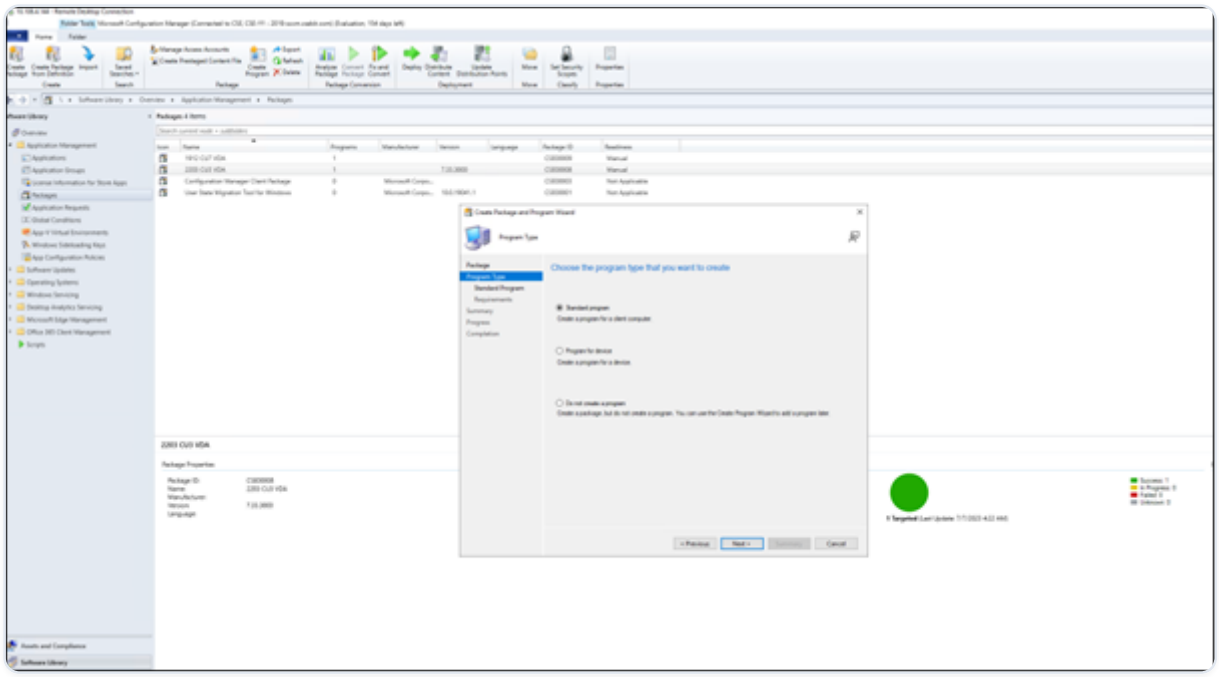
1. パッケージを作成するには、目的のVDAを右クリックし、**「パッケージの作成」**をクリックします。



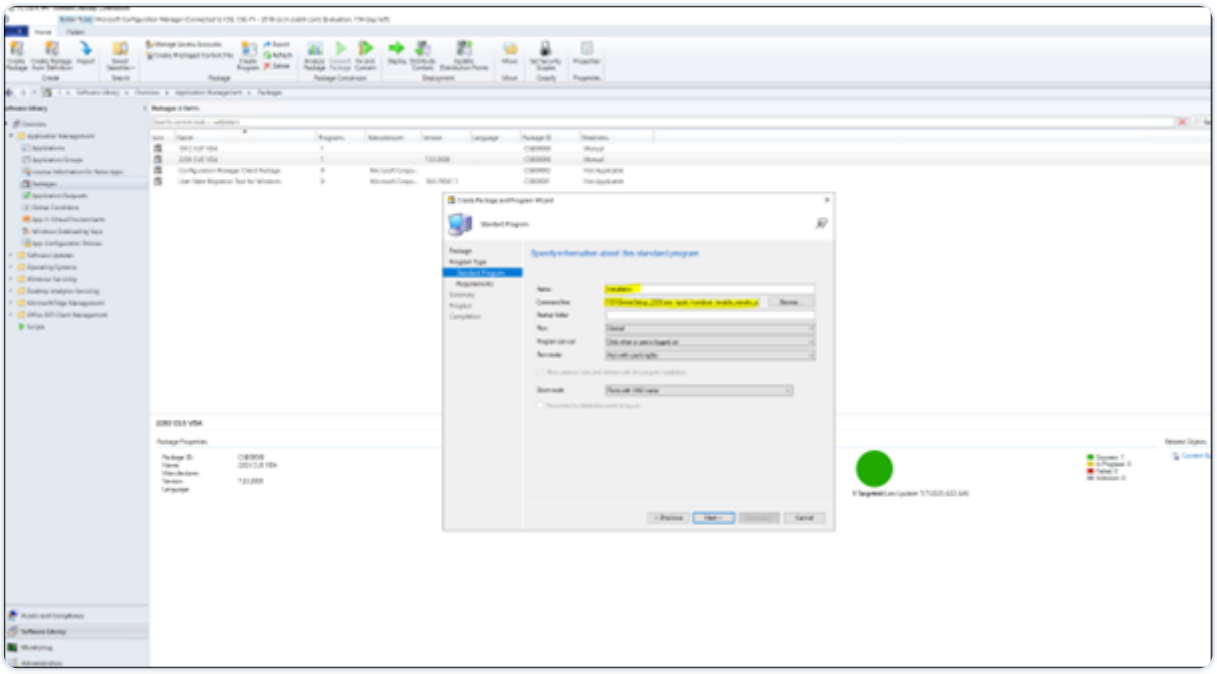
2. **「参照」**をクリックして、このパッケージのソースファイルの場所を指定します。



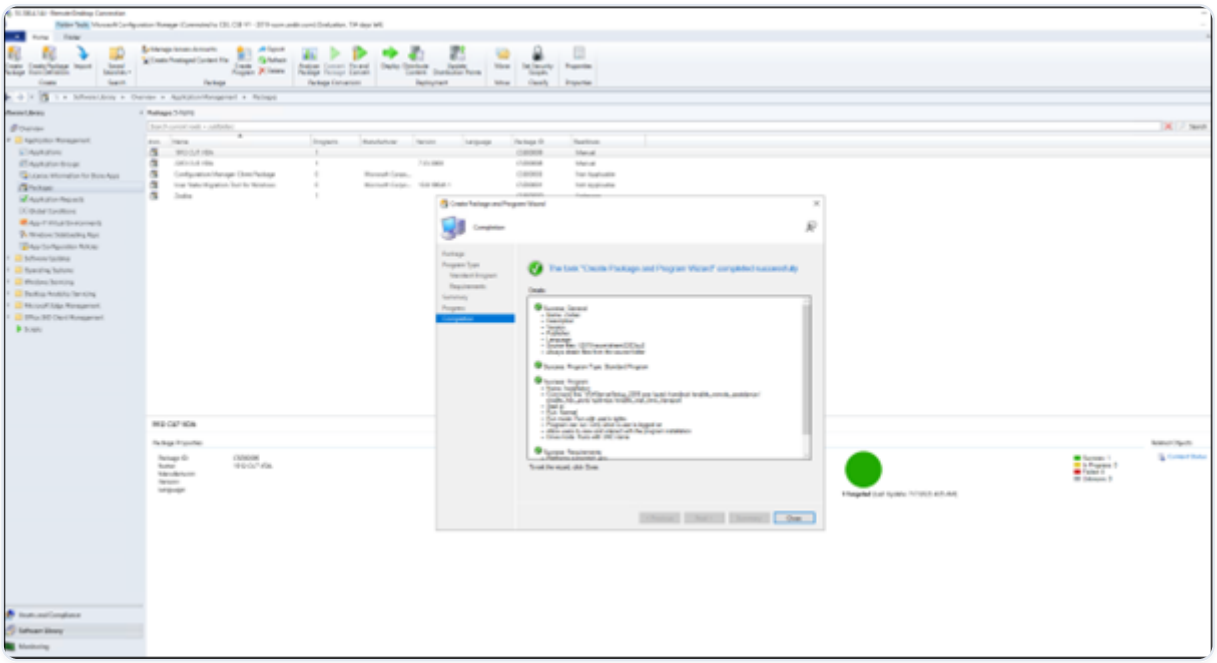
3. 必要なパッケージの種類を選択します。



4. パッケージの**名前**と**コマンドライン**を入力します。



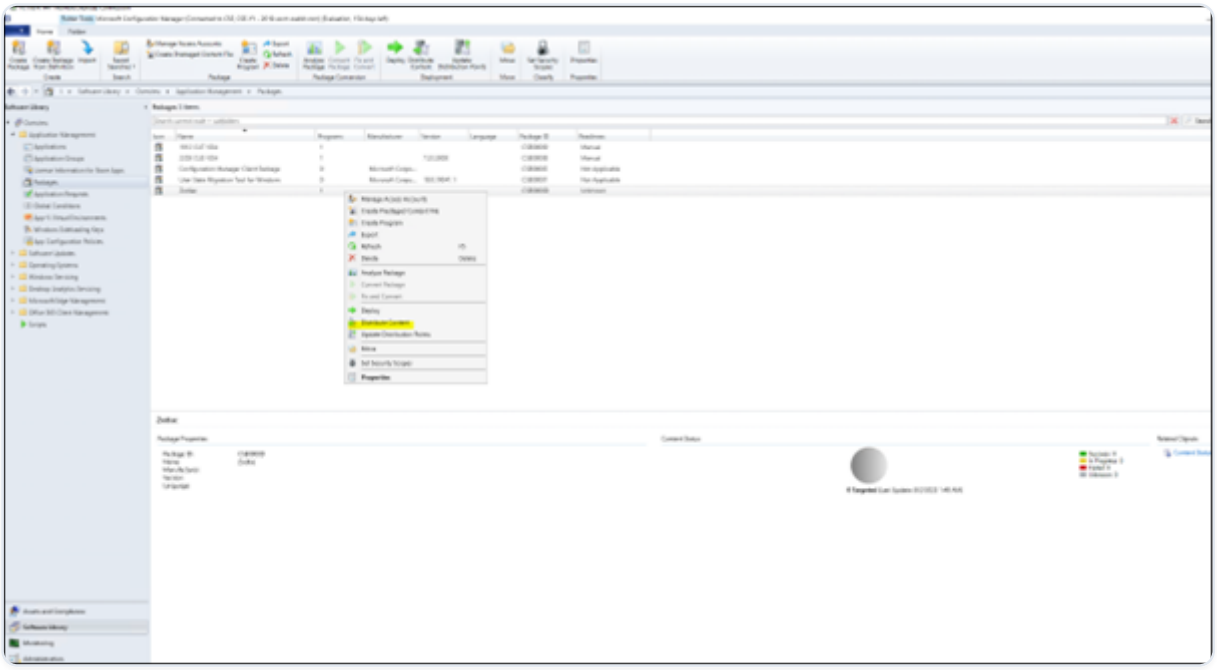
5. **「次へ」**をクリックします。



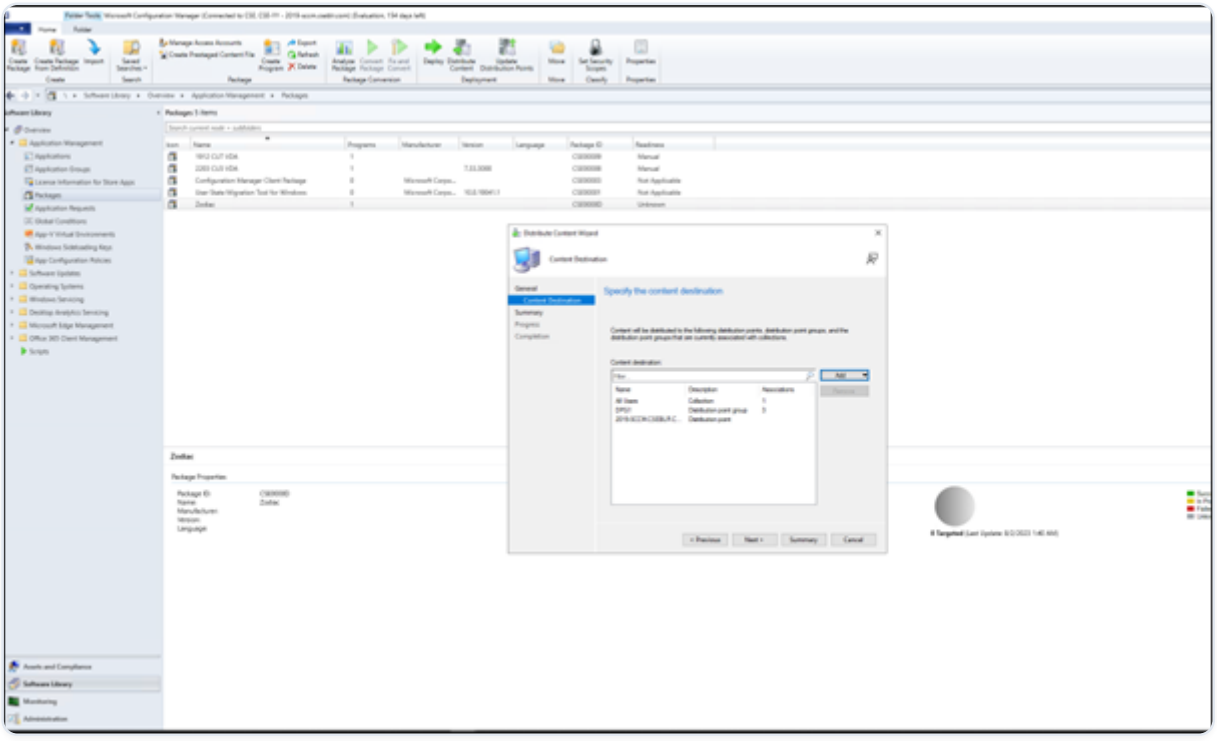
詳細については、Microsoft ドキュメントの Configuration Manager のパッケージとプログラム を参照してください。

コンテンツの配布

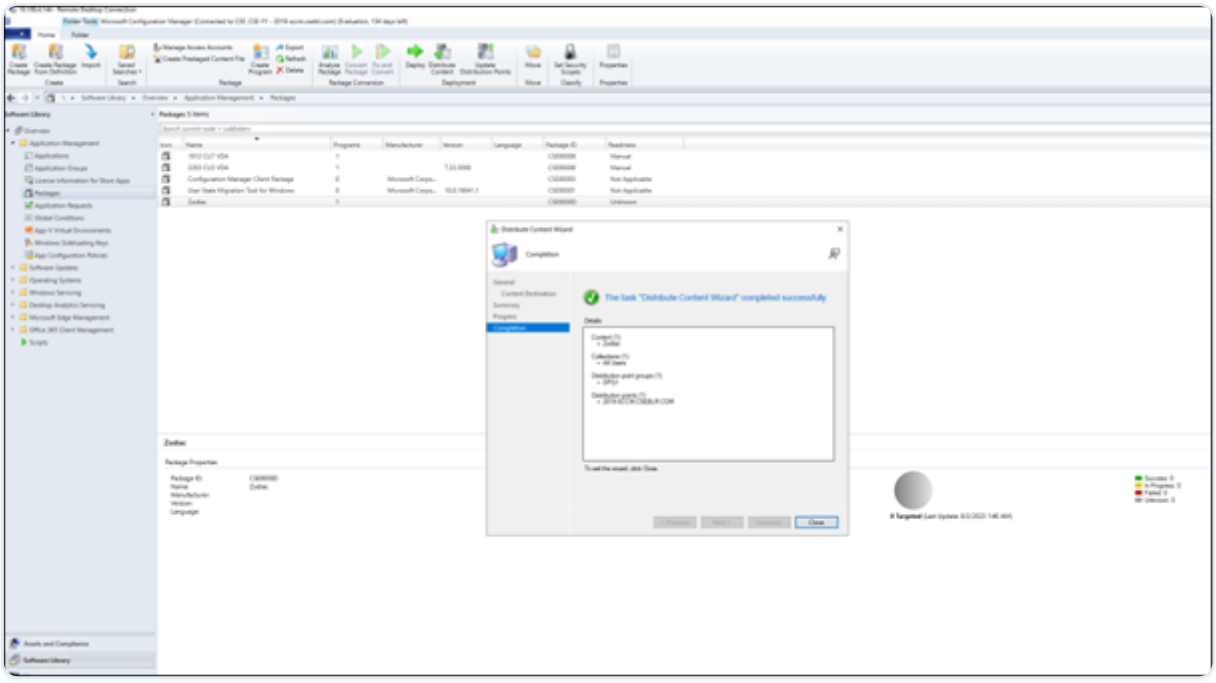
1. 作成したパッケージ名を右クリックします。
2. **コンテンツの配布**を選択します。



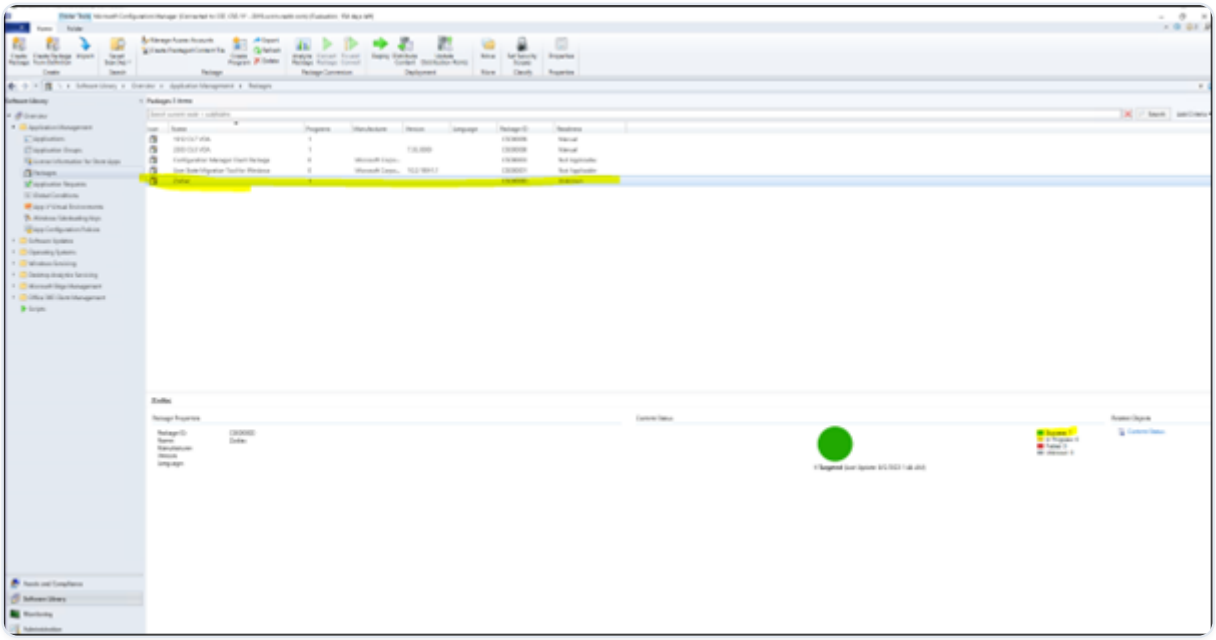
3. **コンテンツ配布ウィザード**ウィンドウで、作成したパッケージのソースファイルの場所を選択します。この例では、`2019-SCCM` です。**次へ**をクリックします。



4. パッケージ（この例では `Zodiac`）が展開可能であることを確認します。



次の図は、パッケージが展開可能であることを示しています。

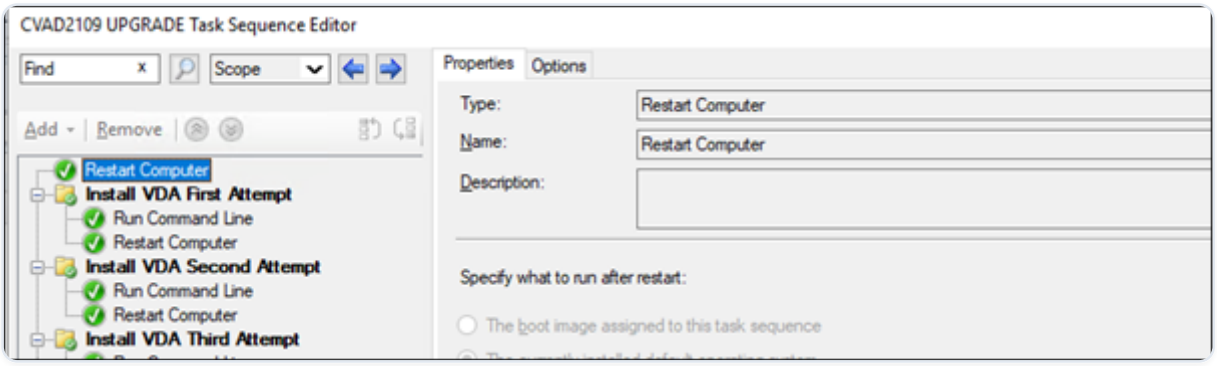


詳細については、Microsoft ドキュメントの Configuration Manager のコンテンツの展開と管理 を参照してください。

SCCM を使用したインストールシーケンスの例

次の例は、インストールシーケンスを示しています。

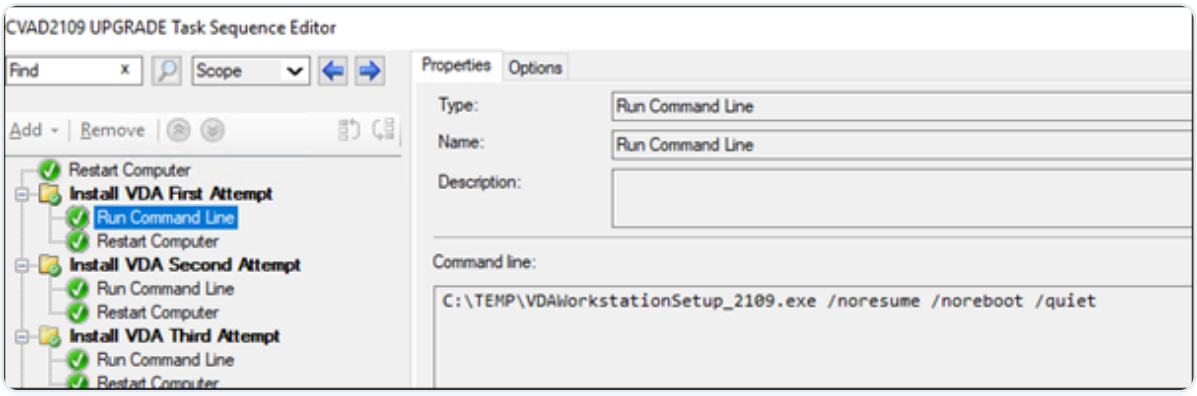
1. **コンピューターの再起動:** マシンを再起動して準備します。



2. **VDA のインストール (初回試行):** VDA のインストールを開始します。

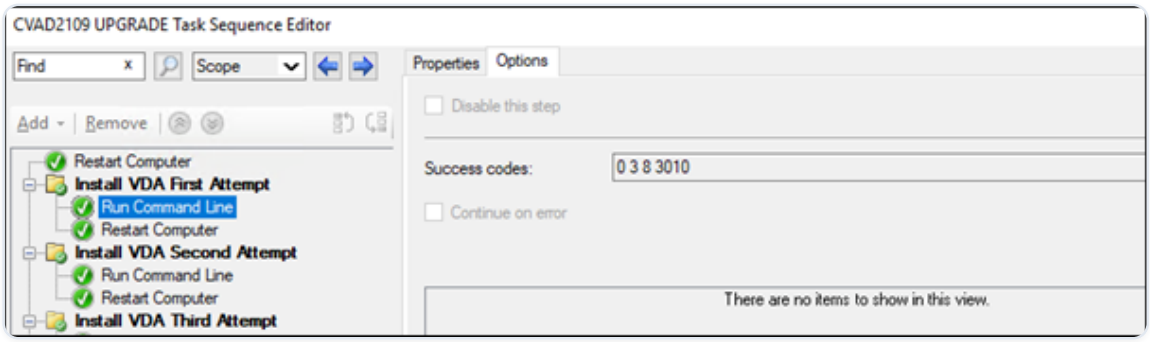
   a. コマンドラインオプションに `/quiet`、`/noreboot`、および `/noresume` オプションを追加します。

   b. 選択した VDA インストーラー (ローカルイメージまたは最小インストーラーのいずれか) を実行します。

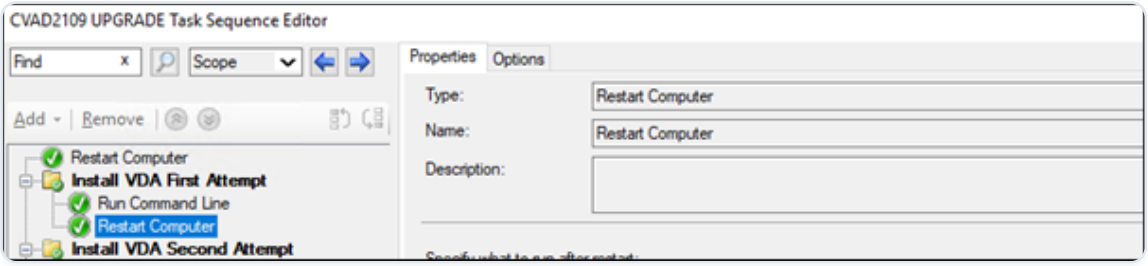


   c. SCCM はリターンコードをキャプチャする必要があります。

   - リターンコードが 0 または 8 の場合、インストールは完了しており、再起動が必要です。



   - リターンコードが3の場合、マシンを再起動してから、**VDAのインストール（2回目試行）**に制御を渡します。



3. **VDAの2回目のインストール:** VDAのインストールを続行します。

   a. **VDAの1回目のインストール**の後、ファイル `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` が存在する場合、インストールは完了しておらず、再起動が完了した後に続行する必要があります。



   b. **VDAの2回目のインストール**は、ファイル `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` が存在しなくなるか、0または8以外のリターンコードが返されるまで繰り返されます。その他のリターンコードはエラーとして扱い、VDAの2回目のインストールはエラーを報告して停止する必要があります。

   c. 適切なVDAインストーラー（ほとんどの場合 `XenDesktopVdaSetup.exe`、または `VDAWorkstationCoreSetup_XXXX.exe` が使用された場合は `XenDesktopRemotePCSetup.exe`）をファイル `%programdata%\Citrix\XenDesktopSetup\` ディレクトリからコマンドラインパラメーターなしで実行して、VDAのインストールを再開します。(VDAインストーラーは、インストーラーの初回実行時に保存したパラメーターを使用します。)

      タスクシーケンスエディターのアップグレード(/en-us/citrix-virtual-apps-desktops/2407/media/upgrade-task-sequence-editor.png)

   d. VDAインストーラーからのリターンコードを確認してください。

      - 0または8：成功、インストール完了、再起動が必要です。

        インストール成功(/en-us/citrix-virtual-apps-desktops/2407/media/success-installation-complete.png)

- 3: インストールは完了していません。マシンを再起動し、ファイル`%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml`が存在しなくなるか、0または8が返されるまでINSTALL VDA SECOND ATTEMPTを繰り返してください。その他のリターンコードはエラーとして扱い、INSTALL VDA SECOND ATTEMPTはエラーを報告して終了する必要があります。

リターンコードの詳細については、Citrixインストールのリターンコードを参照してください。

VDAインストールコマンドの例

利用可能なインストールオプションは、使用するインストーラーによって異なります。コマンドラインオプションの詳細については、以下の記事を参照してください。

- VDAのインストール
- コマンドラインを使用したインストール

REMOTE PC ACCESSのインストールコマンド

- 次のコマンドは、シングルセッションコア VDA インストーラー（`VDAWorkstationCoreSetup.exe`）を使用します。

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

- 次のコマンドは、シングルセッションフル VDA インストーラー（`VDAWorkstationSetup.exe`）を使用します。

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /physicalmachine /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

専用 VDI のインストールコマンド

- 次のコマンドは、シングルセッションフル VDA インストーラー（`VDAWorkstationSetup.exe`）を使用します。

  ```
  VDAWorkstationSetup.exe /quiet /components vda /controllers “control.domain.com” /enable_hdx_ports /enable_remote_assistance /noresume /noreboot
  ```

Microsoft Intune を使用した VDA のインストール

概要

この記事では、Microsoft Intune を使用して VDA を展開する方法について説明します。詳細については、Microsoft のドキュメントを参照してください。

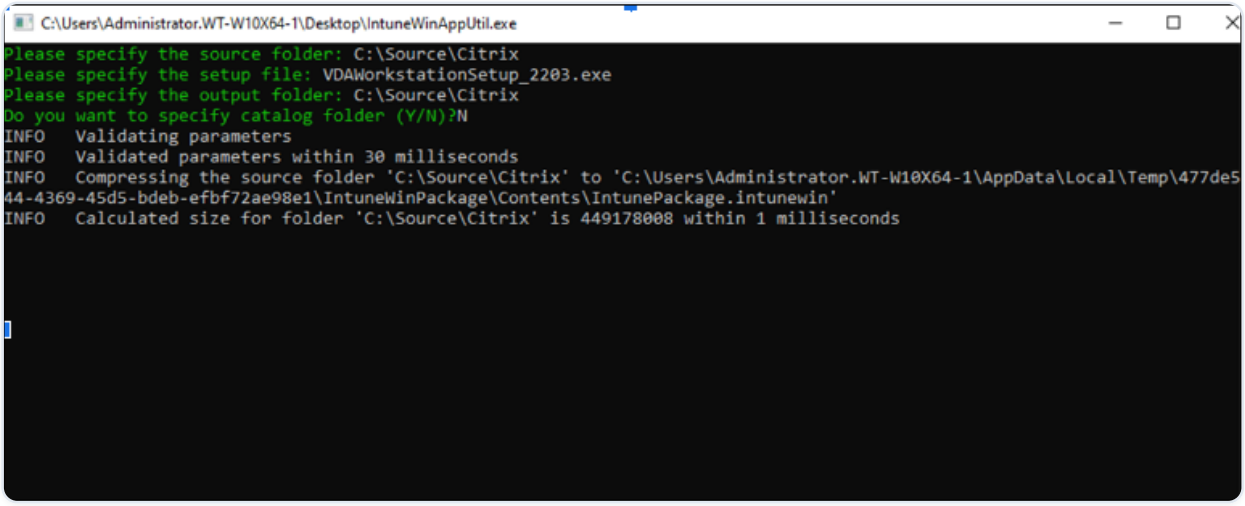
> **注:**
>
> 以下の記事は、Citrix® が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、お客様のニーズに合わせてカスタマイズできます。Citrix は、お客様のニーズに合わせて必要な更新や調整について責任を負いません。

Microsoft Intune を使用して VDA を展開するための主要な手順

1. Citrix VDA のインストールを準備する。
2. Microsoft 365 開発者プログラムサブスクライバーを設定する。
3. アプリを追加して割り当てる。
4. 登録済みデバイスにアプリをインストールする。

ステップ 1: CITRIX VDA のインストールを準備する

1. 更新された IntuneWinAppUtil.exe を GitHub からダウンロードします。
2. **管理者として実行**を使用して `IntuneWinAppUtil.exe` ファイルを実行します。
3. 次のデータを入力します。



a. **ソースフォルダーを指定してください**: アプリケーションのセットアップファイルが含まれるフォルダーを入力します。例: C:\source\Citrix。

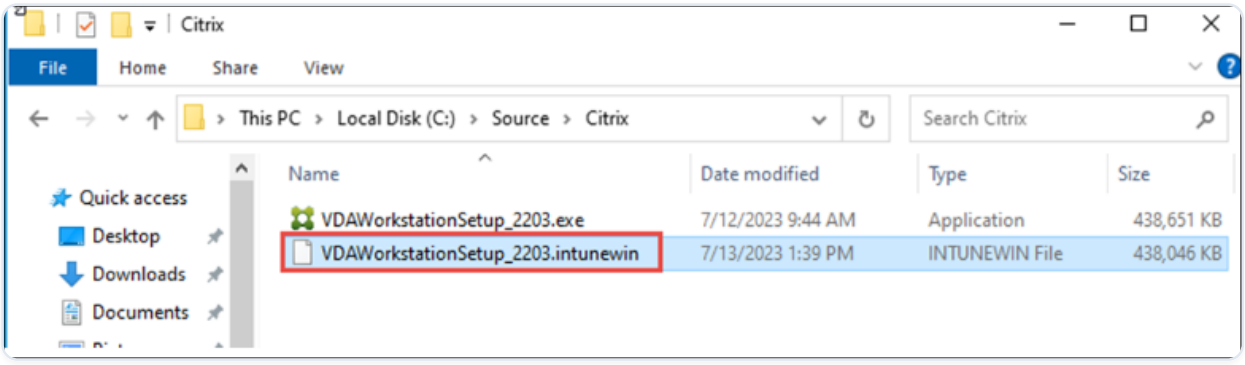
b. **セットアップファイルを指定してください**: セットアップファイル名（setup.exeやsetup.msiなど）を入力します。例: VDAWorkstationSetup_2203.exe。

c. **出力フォルダーを指定してください**: .intunewinファイルを生成するための出力フォルダーのパスを入力します。例: C:\source\Citrix。

d. **カタログフォルダーを指定しますか (Y/N)**: Nと入力します。

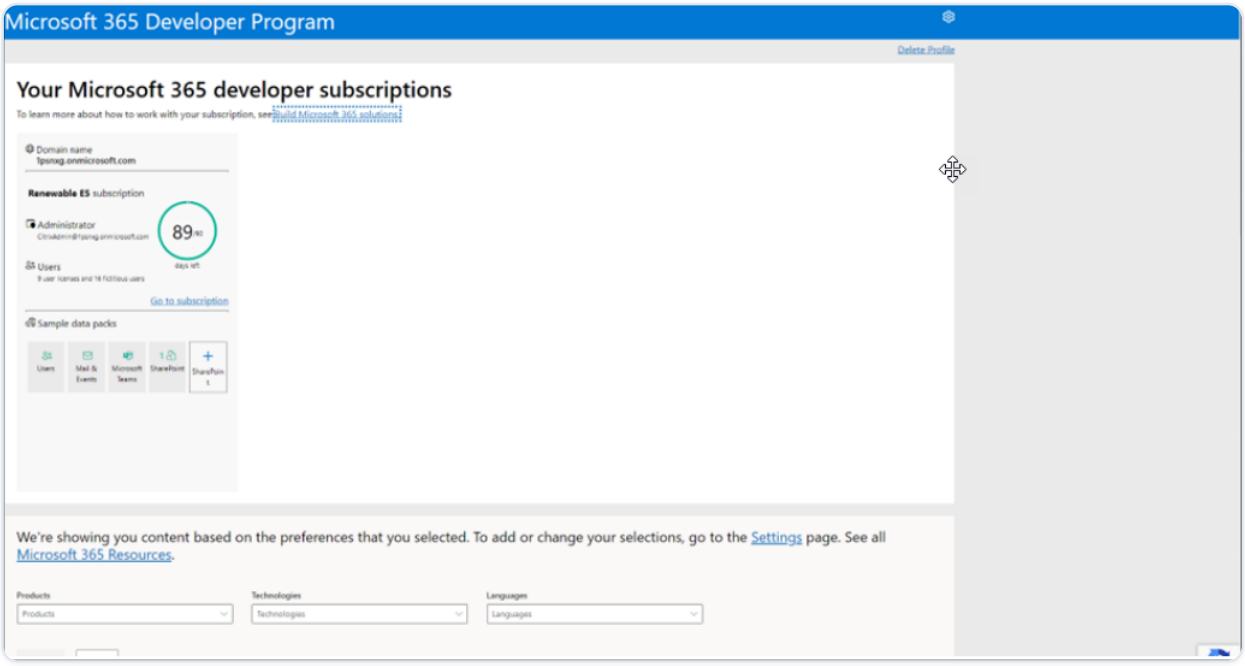
> **注:**
>
> **Win32 Content Prep Tool**が実行されている間、数分間お待ちください。`.intunewin`ファイルが生成されると、コマンドプロンプトの下部にステータスが100%と表示されます。

4. プロセスが完了したら、出力フォルダー（この例では`C:\source\Citrix`）に移動して、Microsoft Intune展開ファイルを取得します。
5. Microsoft Intuneの無料試用版にサインアップします。

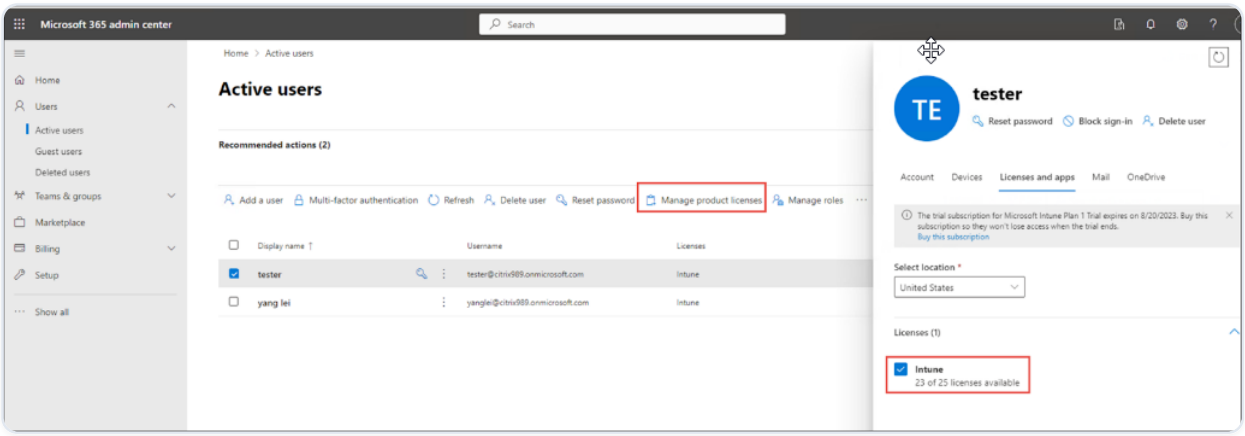


ステップ2: MICROSOFT 365開発者プログラムサブスクライバーのセットアップ

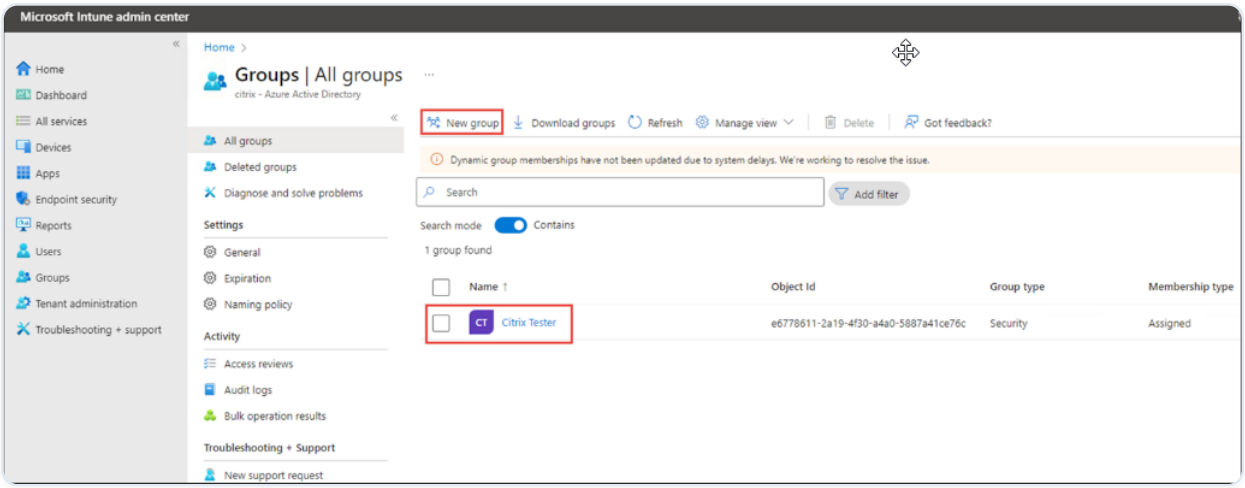
1. サブスクリプションをアクティブ化するために、インスタントサンドボックスを作成します。開発者サンドボックスを取得するには、Microsoft 365開発者プログラムダッシュボードにアクセスし、**Add a new subscription**を選択します。



2. Microsoft 365管理センターでユーザーを作成し、そのユーザーにライセンスを割り当てます。



3. グループを作成します。



4. グループが作成されたら、そのグループにMDM機関を提供する必要があります。自動登録を設定します。アクティブ化には1分ほどかかる場合があります。 または、次の手順を実行して、MDM機関をグループに手動で追加することもできます。

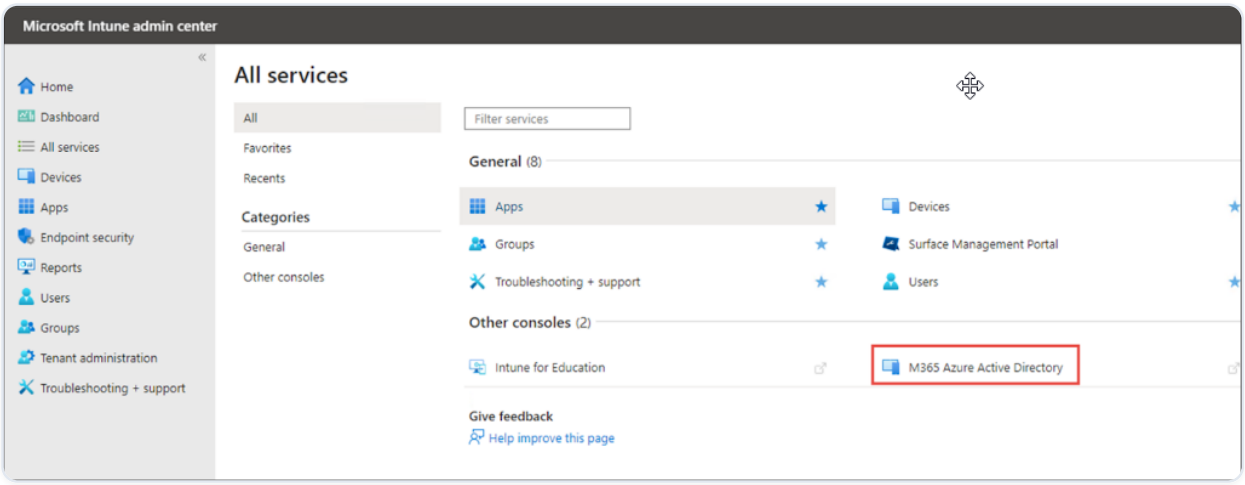
   a. **すべてのサービス > Microsoft Entra** に移動します。

   b. **設定 > モビリティ** に移動し、**Microsoft Intune** を選択します。

   c. 作成したばかりのグループを選択します。これにより、MDMユーザー範囲のページが開きます。

   d. **保存** をクリックします。

5. **すべてのサービス** タブで、**M365 Azure Active Directory** をクリックします。



6. **この機能を使用するには、無料のPremium試用版を入手してください** をクリックします。



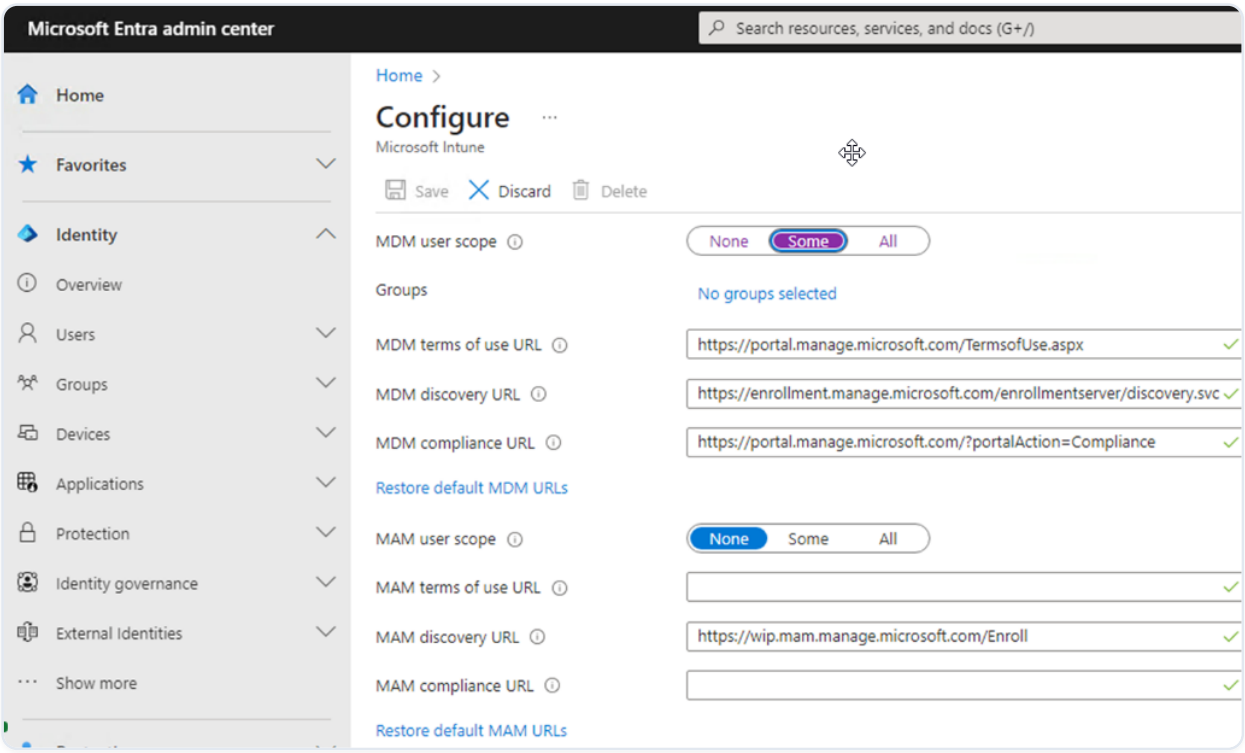
7. **アクティブ化** をクリックします。

「MS Entra センター」(/en-us/citrix-virtual-apps-desktops/2407/media/ms-entra-admin-center.png)

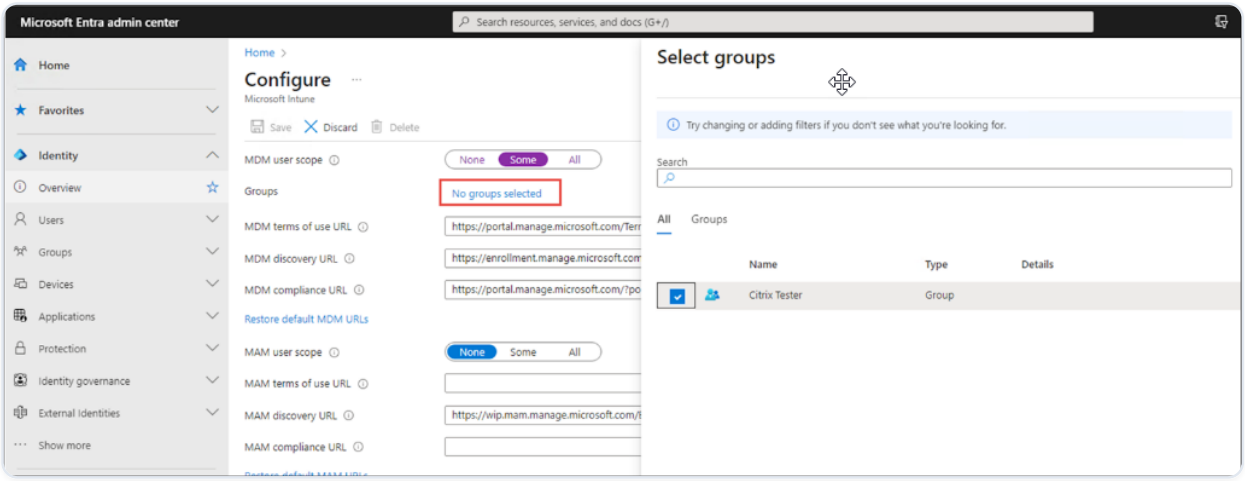
8. 次に、**Microsoft Intune** をクリックします。

「MS Intune の選択」(/en-us/citrix-virtual-apps-desktops/2407/media/select-ms-intune.png)

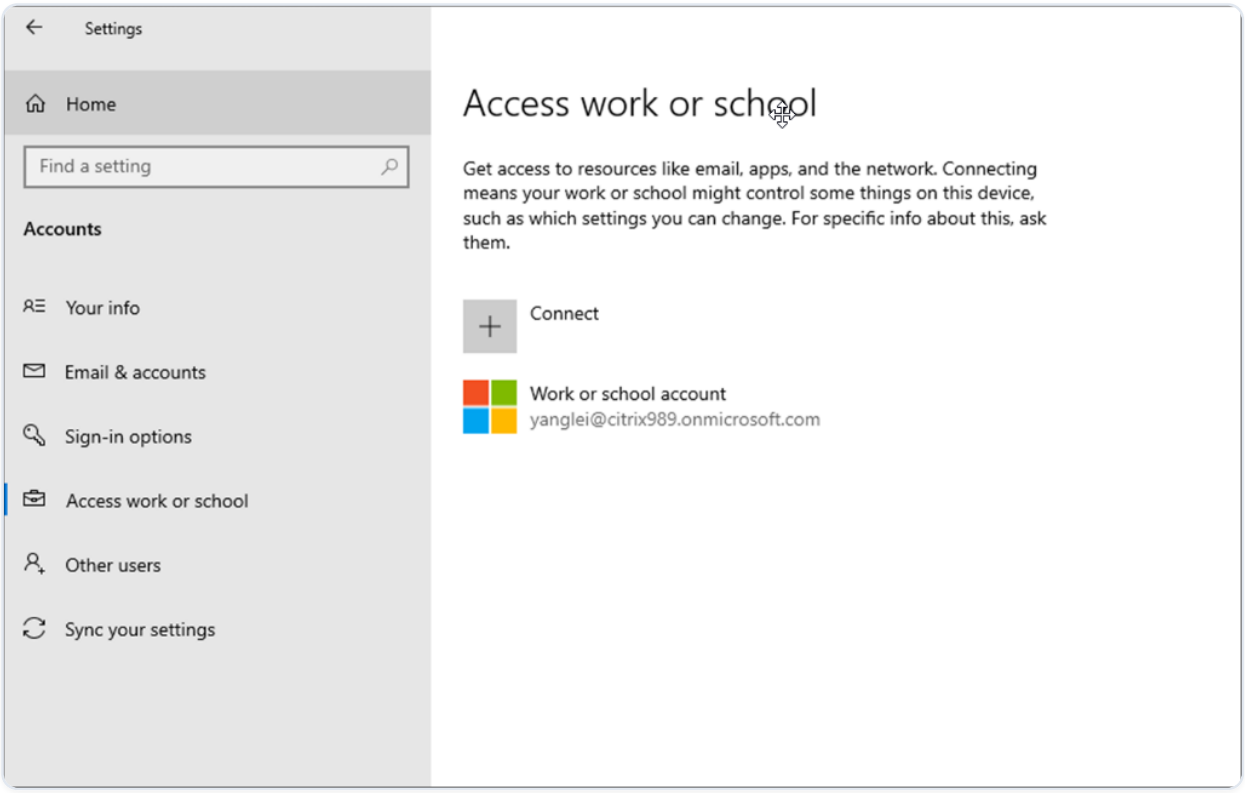
9. **構成** タブで、必要な構成を入力します。



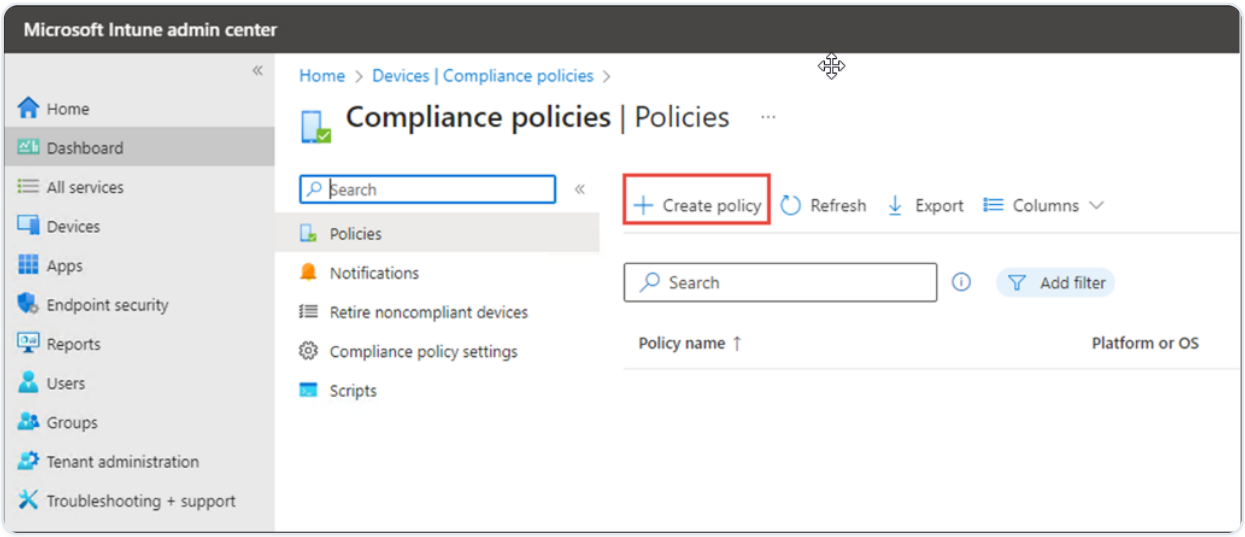
10. グループを追加するには、**グループが選択されていません**をクリックします。



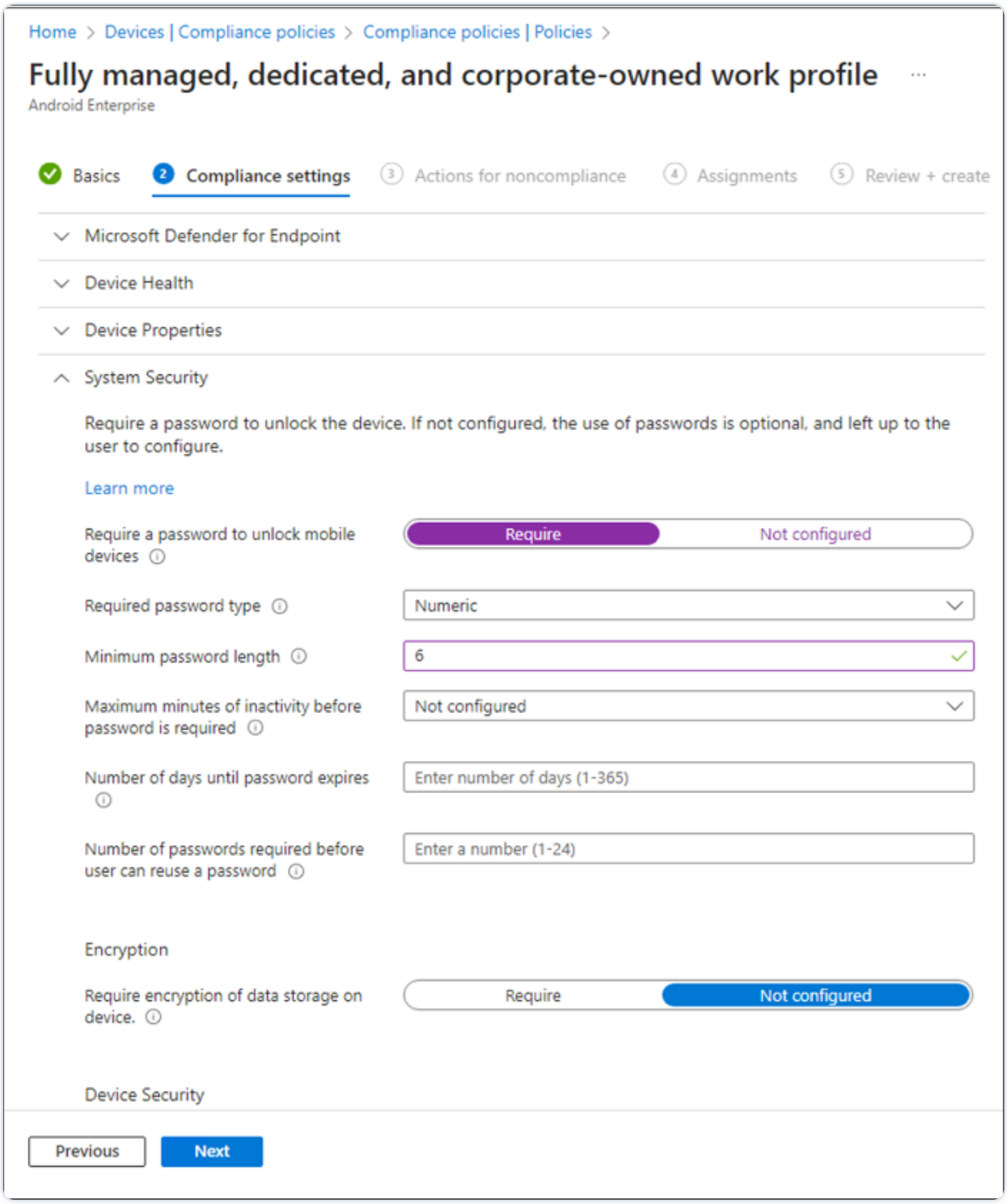
11. デバイスを登録します。



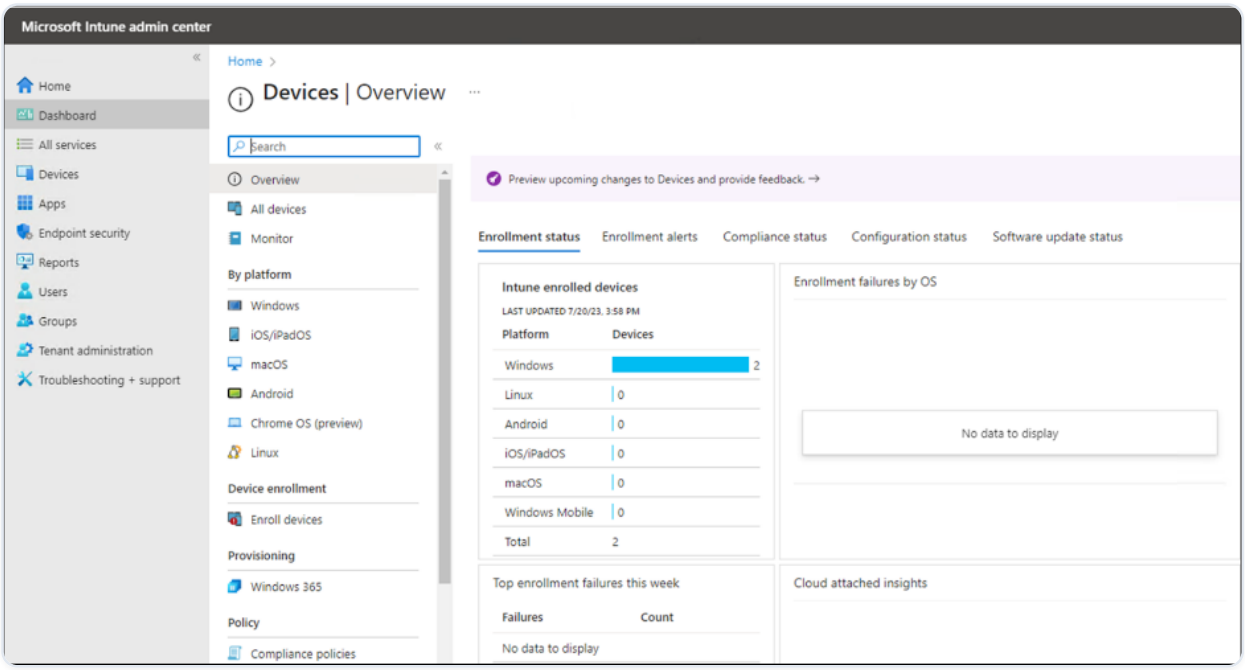
12. 新しく作成したデバイスのコンプライアンスを`Compliant`に変更するためのデバイスコンプライアンスポリシーを作成します。



13. 新しく作成したグループを追加するには、**割り当て**タブに移動します。



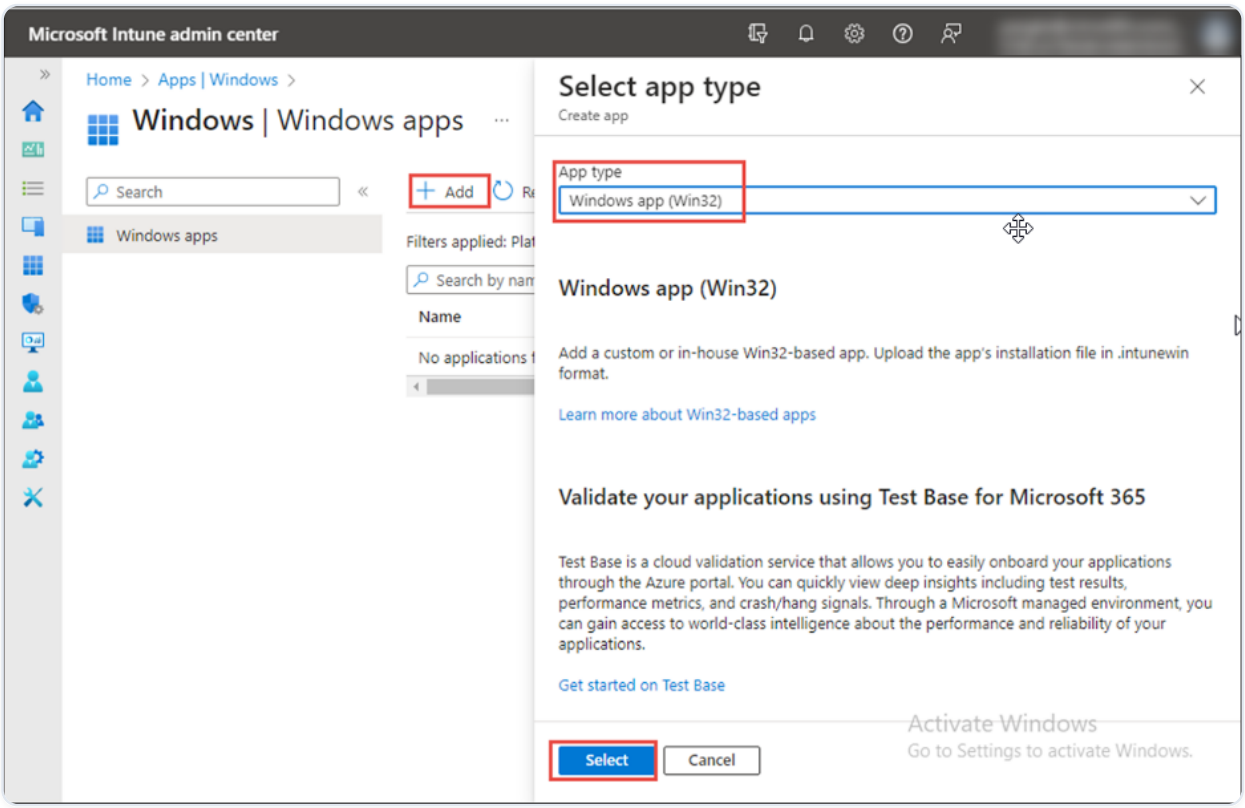
14. デバイスの登録を確認します。



詳細については、Microsoft 365 開発者プログラムを参照してください。

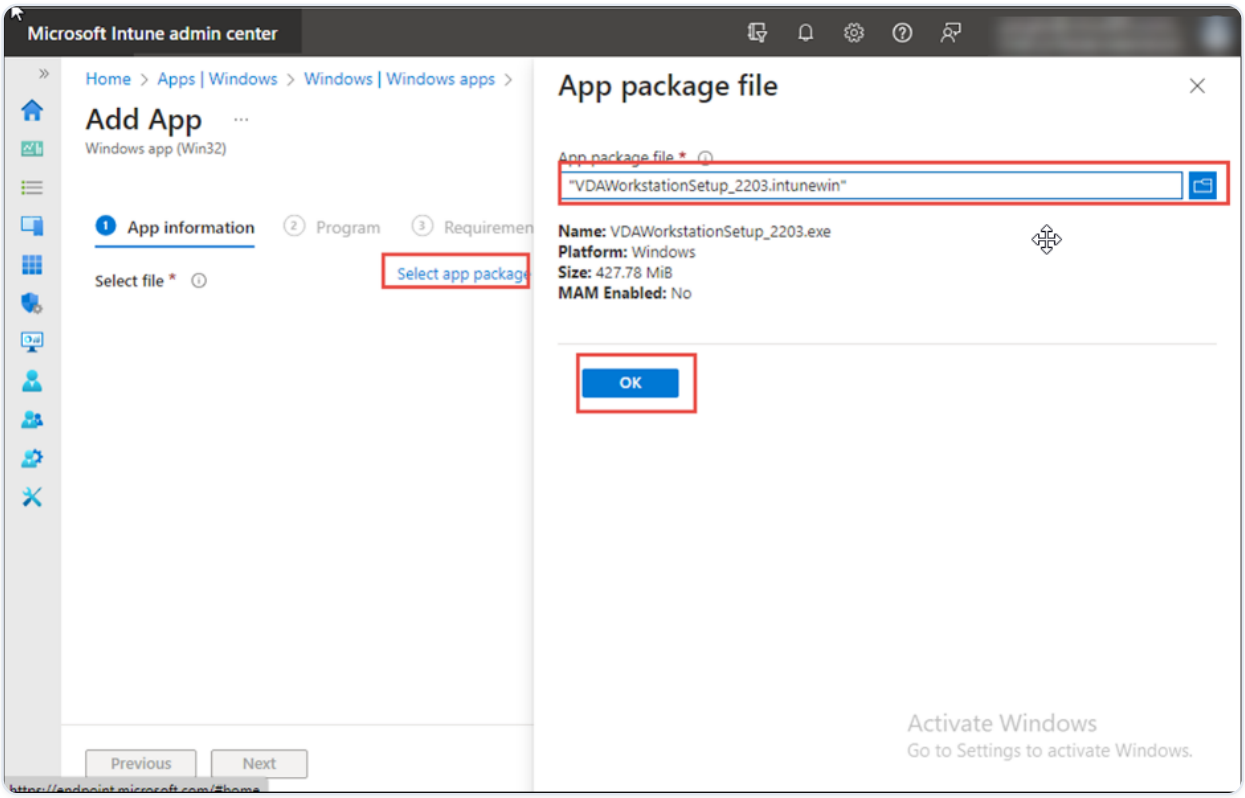
ステップ3：アプリの追加と割り当て

1. Microsoft Intune 管理センターにサインインします。
2. **アプリ > すべてのアプリ > 追加**を選択するか、**アプリ > Windows > Windows アプリ**に移動します。



3. ペインで、 > を選択し、 をクリックします。

4. ペインで、 をクリックします。 をクリックします。
5. 拡張子 `.intunewin` の準備されたファイルを選択します。準備されたファイルは、Citrix VDAのインストールの準備 の手順で作成されます。アプリに関する詳細情報を含むページが表示されます。

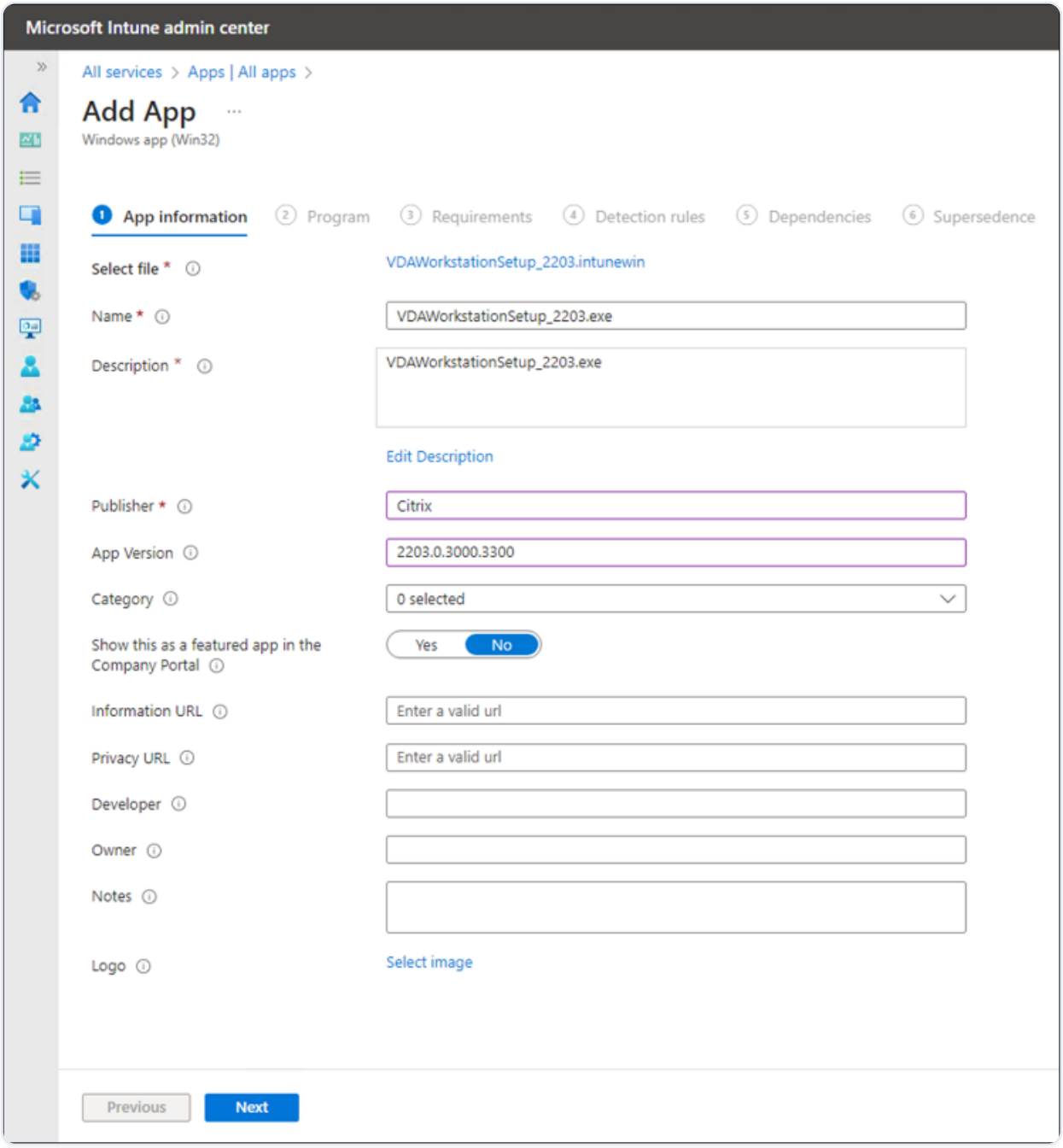


注:

- サーバーコアマシンを使用している場合は、VDAワークステーションコアを使用する必要があります。
- Windows 10デスクトップOSを使用している場合は、VDAワークステーションを使用する必要があります。
- サーバーOS（例: Windows 2022）を使用している場合は、VDAサーバーセットアップを使用する必要があります。
- この例ではバージョン2203を使用していますが、これはすべてのバージョンに適用されます。

6. **App package file**ペインで**OK**をクリックします。

7. 次の画面で、「**アプリ情報**」タブの下にあるアプリの「**名前**」を入力し、Windowsアプリの「**説明**」を入力します。「**発行元**」の名前を `Citrix` と入力し、ここで追加のアプリ情報を指定できます。「**次へ**」をクリックします。



8. 次の画面で、次の値を入力します。

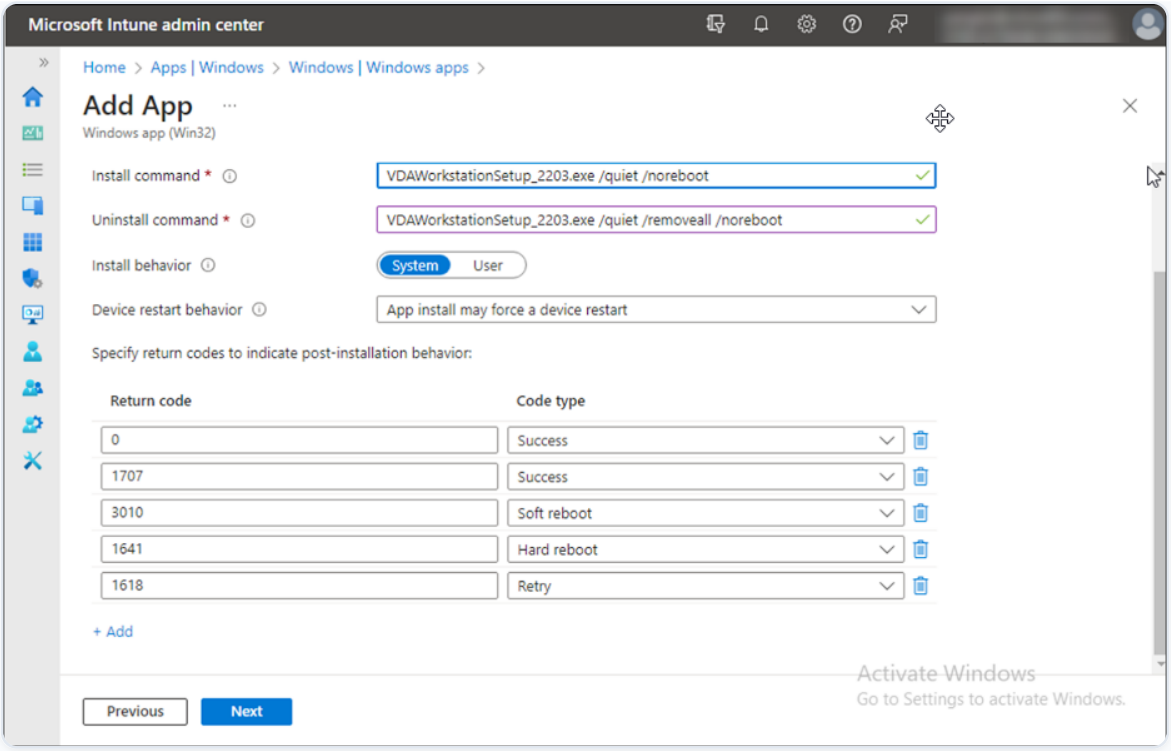
   - **インストールコマンド**: `VDAWorkstationSetup_2203.exe /quiet /noreboot`
   - **アンインストールコマンド**: `VDAWorkstationSetup_2203.exe /quiet /removeall /noreboot`
   - **インストール動作**:

- **システム**: このオプションを選択すると、グループ内のすべてのデバイスにアプリがインストールされます。
- **ユーザー**: このオプションを選択すると、グループ内の特定のユーザーデバイスにのみアプリがインストールされます。

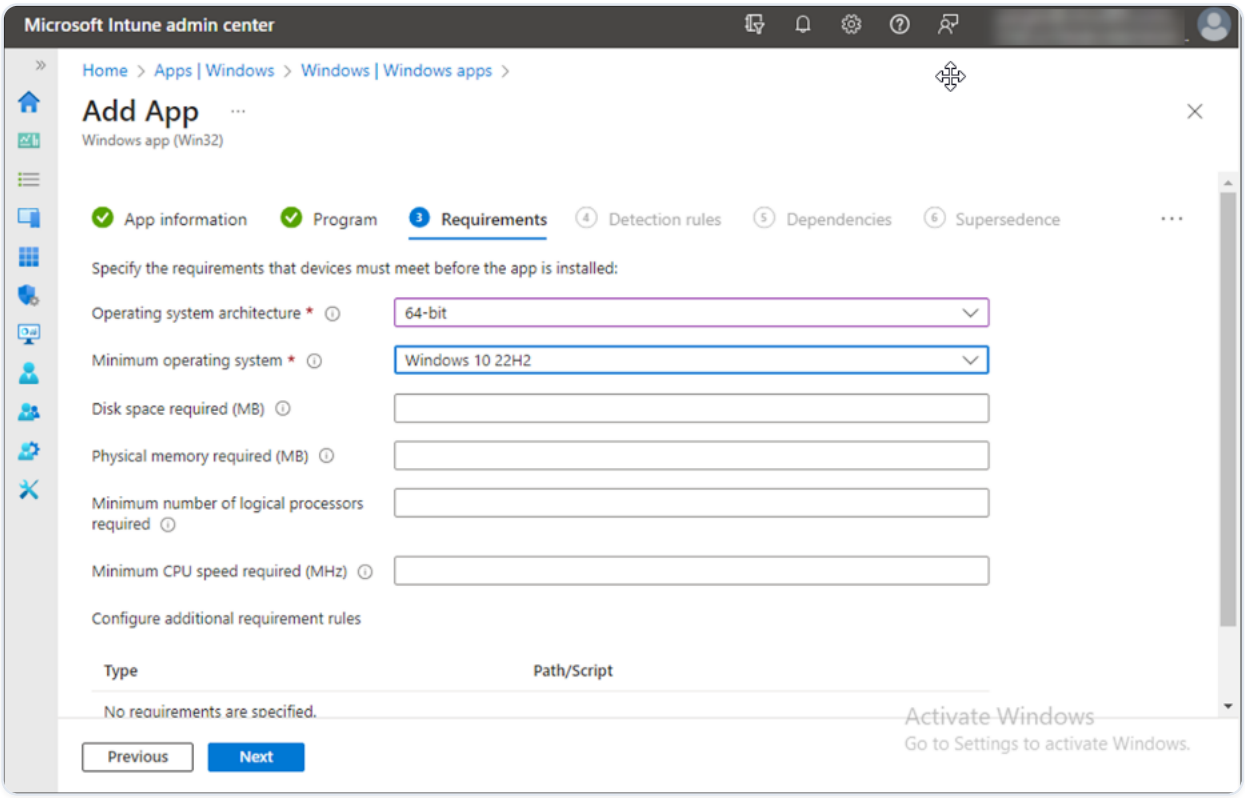
9. **Next**をクリックします。

注:

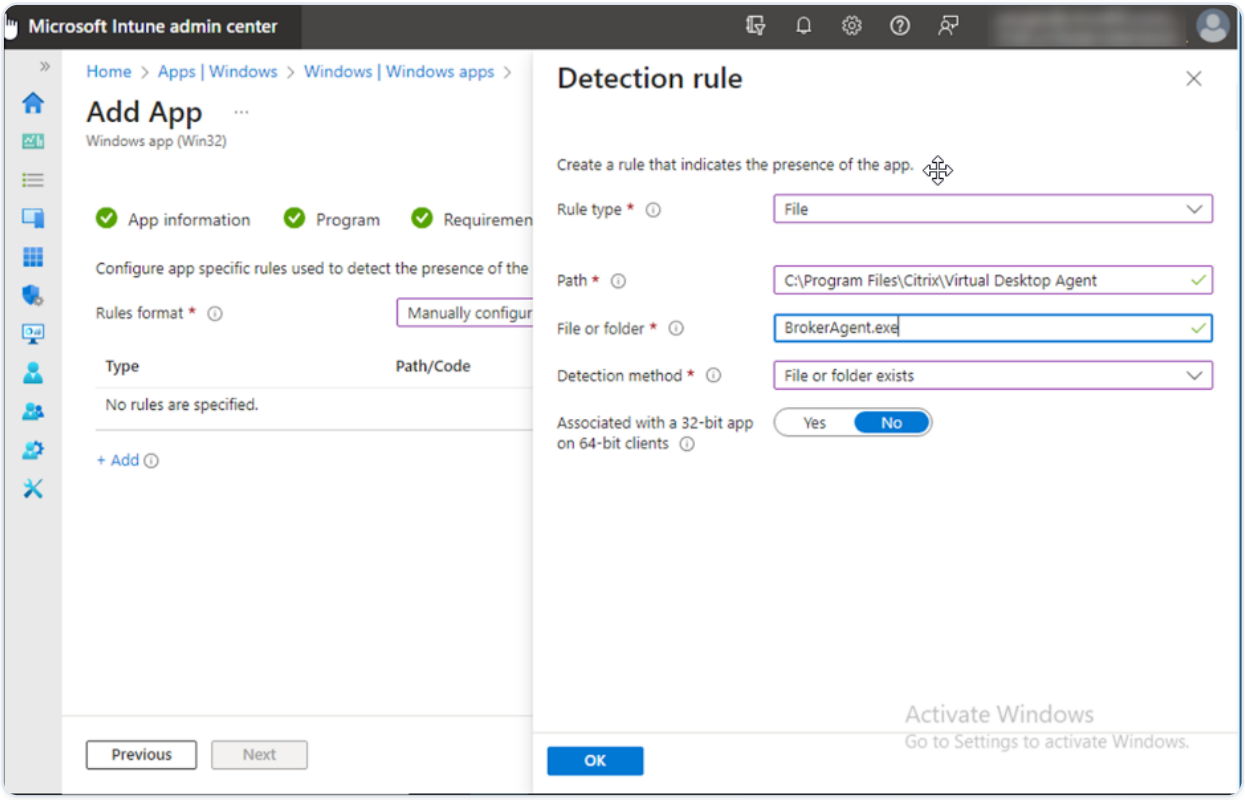
- この例ではバージョン2203を使用していますが、どのバージョンでも使用できます。
- コマンドに`/noreboot`を追加しても、インストールまたは展開中に再起動が発生しないという意味ではなく、強制的な再起動を適用するだけです。 スクリプトの詳細については、VDAのインストール用コマンドラインオプションを参照してください。
- **デバイスの再起動動作**で、**Intuneが強制的にデバイスを再起動します**を選択します。
- **リターンコード**テキストボックスに、インストール後の成功のために`0`、`3`、および`8`を入力します。 その他のリターンコードについては、Citrixインストールリターンコードを参照してください。



10. 次の画面の**要件**タブで、必要な値を入力します。**次へ**をクリックします。



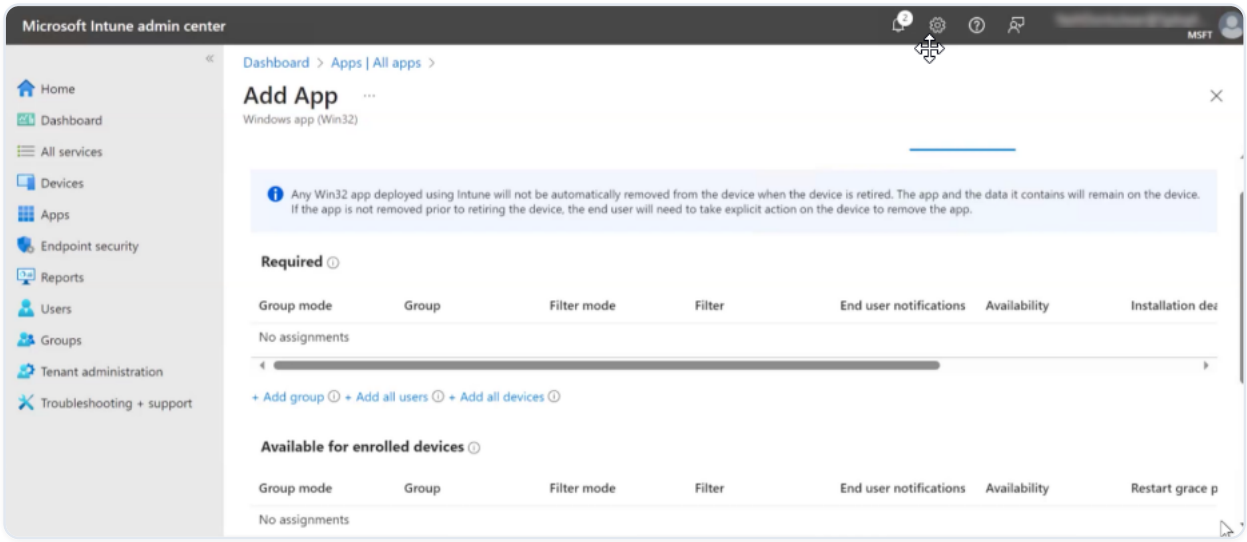
11. 次の画面の**検出ルール**タブで、Brokerエージェントを追加するために**検出ルール**を追加します。**OK**をクリックします。



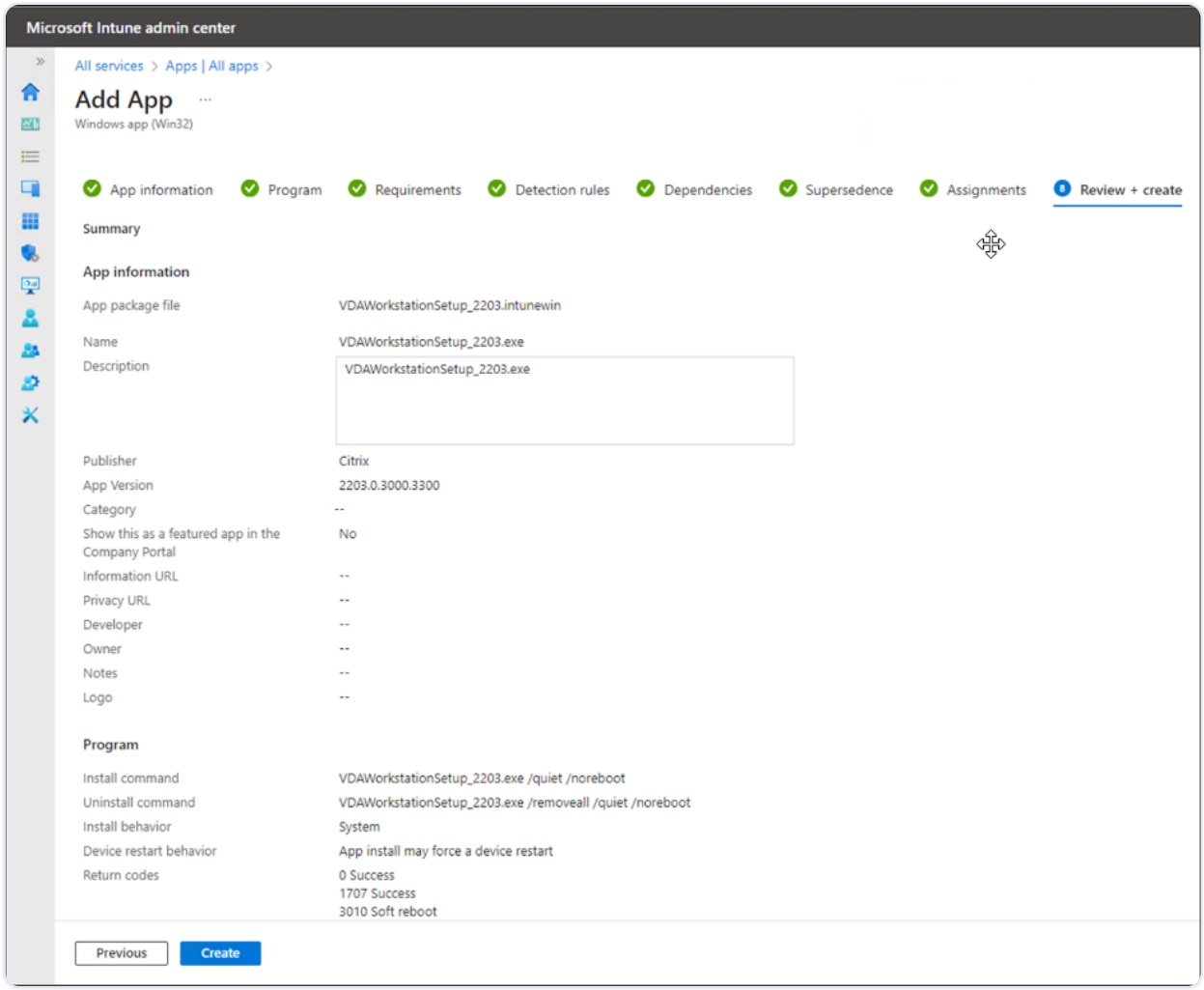
12. 「**割り当て**」タブで、デバイスを次のように追加できます。

- **必須**: 更新が自動的に行われるデバイス。

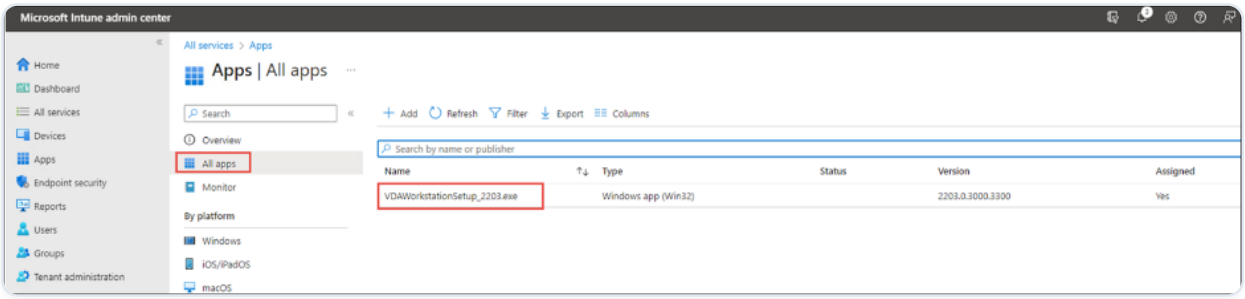
- **登録済みデバイスで利用可能**: 更新が手動で行われるデバイス。



13. 詳細を確認し、「**作成**」をクリックします。



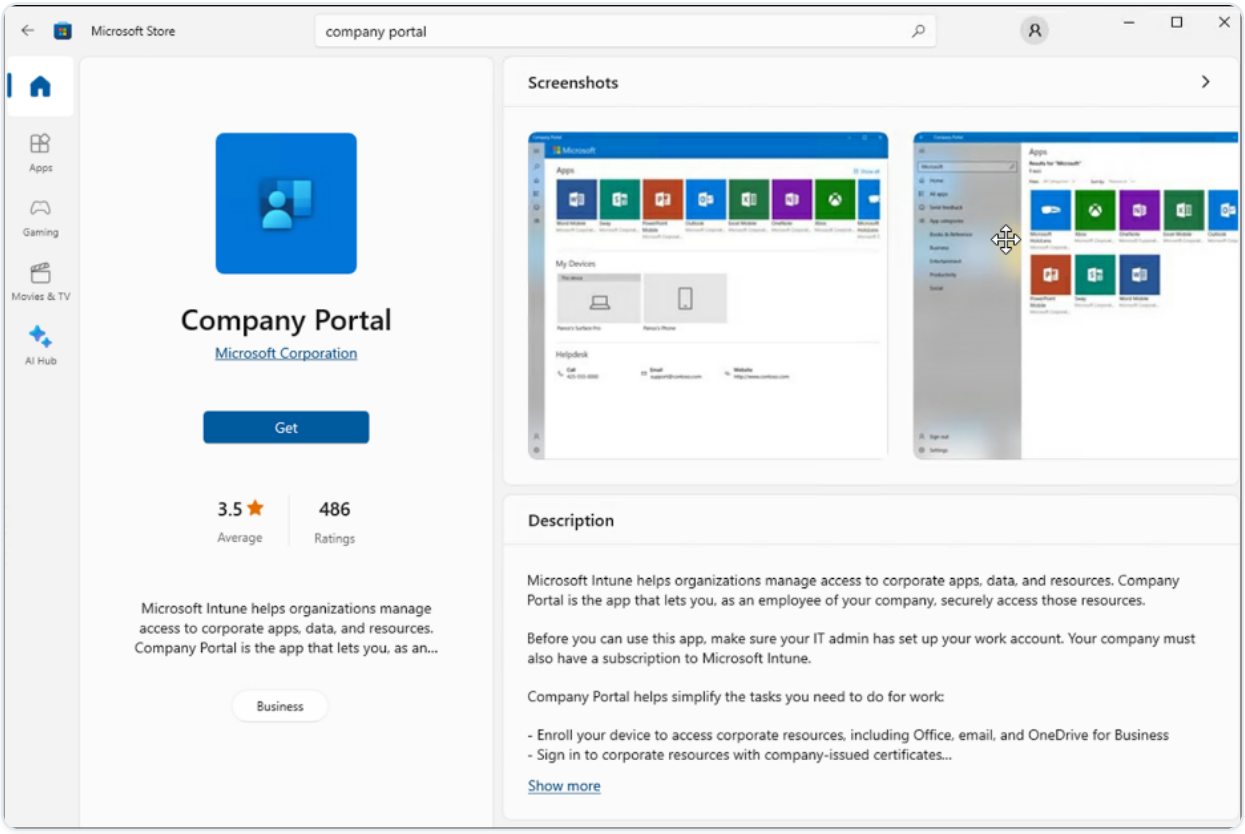
アプリが正常に割り当てられました。



詳細については、「アプリの追加と割り当て」を参照してください。

ステップ 4: 登録済みデバイスにアプリをインストールする

1. 登録済みのWindows 10デスクトップデバイスにサインインします。 デバイスはMicrosoft Intuneに登録されている必要があります。また、アプリに割り当てたグループに含まれるアカウントを使用してデバイスにサインインする必要があります。詳細については、Microsoftのドキュメントを参照してください。
2. 「**スタート**」メニューから「**Microsoft Store**」を開きます。
3. 「**Company Portal**」アプリを検索してインストールします。



4. 「**Company Portal**」アプリを実行します。
5. Microsoft Intuneを使用して追加したアプリをクリックします。 Intuneユーザーにアプリを正常に割り当てなかった場合、次のメッセージが表示されます。 `Your IT administrator did not make any apps available to you.`

6. **Install**をクリックします。

サイトを作成する

> **注:**
>
> サイト作成中に、ハイブリッド権限ライセンスを有効にするライセンスを追加した後、サイト作成が完了するまで、パブリッククラウドホスト（Microsoft Azure、Google Cloud Platform、Amazon Web Servicesなど）は接続の種類リストに表示されません。

> サイトとは、Citrix Virtual Apps and Desktops™展開に付ける名前です。デリバリーコントローラーとその他のコアコンポーネント、Virtual Delivery Agent (VDA)、ホストへの接続、マシンカタログ、およびデリバリーグループで構成されます。コアコンポーネントをインストールした後、最初のマシンカタログとデリバリーグループを作成する前にサイトを作成します。

コントローラーがServer Coreにインストールされている場合は、Citrix Virtual Apps and Desktops SDKのPowerShellコマンドレットを使用してサイトを作成します。

サイトを作成すると、Citrixカスタマーエクスペリエンス向上プログラム（CEIP）に自動的に登録されます。CEIPは匿名の統計情報と使用状況情報を収集し、Citrixに送信します。最初のデータパッケージは、サイト作成後約7日後にCitrixに送信されます。サイト作成後であれば、いつでも登録を変更できます。Web Studioの左ペインで**設定**を選択し、**Citrixカスタマーエクスペリエンス向上プログラム**の設定を見つけます。詳細については、`<http://more.citrix.com/XD-CEIP>`を参照してください。

サイトを作成したユーザーは、フル管理者になります。詳細については、委任管理を参照してください。

サイトを作成する前にこの記事を確認して、何が期待できるかを知っておいてください。

ステップ1. サイト作成ウィザードを開く - Citrix Site Manager

Citrix Site Managerというツールを使用して、Citrix Virtual Apps and Desktops展開（サイトとも呼ばれます）をセットアップします。このツールは、デリバリーコントローラーをインストールすると自動的にインストールされます。

このツールを実行するには、デリバリーコントローラーのデスクトップのスタートメニューを開き、**Citrix > Citrix Site Manager**を選択します。Web Studioのインストールを参照してください。

ステップ2. サイト名

はじめにページで、サイトの名前を入力します。

ステップ3. データベース

データベースページには、サイト、監視、および構成ログデータベースを設定するための選択肢が含まれています。データベースのセットアップの選択肢と要件の詳細については、データベースを参照してください。

> **注:**
>
> SQL Server Always Onリスナーが TLS暗号化用に構成されている場合、データベース作成権限を持つ資格情報の入力を求められることがあります。有効な管理者資格情報を入力しても、データベースの作成は失敗します。SQL Server証明書に、サブジェクトの別名（SAN）にリスナーのDNS名が含まれていることを確認してください。詳細については、`<https://docs.microsoft.com/ja-jp/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover#SSLcertificates>` を参照してください。

> サイトデータベースとしてSQL Server Expressをインストールすることを選択した場合（デフォルト）、そのソフトウェアのインストール後に再起動が発生します。サイトデータベースとしてSQL Server Expressソフトウェアをインストールしないことを選択した場合は、再起動は発生しません。

デフォルトのSQL Server Expressを使用しない場合は、サイトを作成する前に、SQL Serverソフトウェアがマシンにインストールされていることを確認してください。システム要件にサポートされているバージョンが記載されています。

サイトにDelivery Controllerを追加したい場合で、すでに他のサーバーにControllerソフトウェアをインストールしている場合は、このページからそれらのControllerを追加できます。データベースを設定するスクリプトを生成する予定がある場合は、スクリプトを生成する前にControllerを追加してください。

ステップ4. ライセンス

ライセンスページで、ライセンスサーバーのアドレスを指定し、使用する（インストールする）ライセンスを示します。

- ライセンスサーバーのアドレスを`name:[port]`の形式で指定します。*name*はFQDN、NetBIOS、またはIPアドレスである必要があります。FQDNを推奨します。ポート番号を省略した場合、デフォルトは27000です。**接続**をクリックします。ライセンスサーバーへの接続が成功するまで、次のページに進むことはできません。
- 接続が確立されると、デフォルトで**既存のライセンスを使用**が選択されます。表示には、現在インストールされているライセンスに基づいて、この製品が構成できる互換性のある製品がリストされます。
  - この製品をリストされている製品のいずれか（例：Citrix Virtual Apps PremiumまたはCitrix Virtual Desktops™ Premium）として、それらのライセンスのいずれかを使用して構成したい場合は、そのエントリを選択します。
  - この製品で使用するためにライセンスをすでに割り当ててダウンロードしているが（Citrix Manage Licenses Toolを使用して）、まだライセンスをインストールしていない場合：
    - **ライセンスファイルを参照**をクリックします。
    - ファイルエクスプローラーで、ダウンロードしたライセンスを見つけて選択します。関連する製品がサイト作成ウィザードの**ライセンス**ページに表示されます。使用したいエントリを選択します。
  - 目的の製品が表示されない場合、または割り当て済みでダウンロード済みのライセンスがない場合は、ライセンスを割り当て、ダウンロードしてインストールできます。これを行うには、ライセンスサーバーがインターネットにアクセスできる必要があります。目的の製品のライセンスアクセスコードが必要です。Citrixからそのコードがメールで送信されます。
    - **割り当ててダウンロード**をクリックします。
    - 「**ライセンスの割り当て**」ダイアログで、Citrixから送付されたライセンスアクセスコードを入力します。「**ライセンスの割り当て**」をクリックします。
    - 新しいライセンスに関連付けられている製品が、サイト作成ウィザードの「**ライセンス**」ページに表示されます。使用するエントリを選択します。

    または、「**30日間の無料評価版を使用する**」を選択し、後でライセンスをインストールします。詳しくは、ライセンスに関するドキュメントを参照してください。

手順5. 概要

概要ページには、指定した情報が一覧表示されます。変更する場合は、**戻る**ボタンを使用します。完了したら、**完了**をクリックします。

詳細情報

ホスト接続、ネットワーク、およびストレージ

ハイパーバイザーまたはその他のサービス上のVMを使用してアプリケーションとデスクトップを配信している場合、オプションでそのホストへの最初の接続を作成できます。また、その接続のストレージリソースとネットワークリソースを指定することもできます。サイト作成後、この接続とリソースを変更したり、さらに接続を作成したりできます。詳しくは、接続とリソースを参照してください。

- 「**接続**」ページで指定する情報については、接続とリソースを参照してください。
    - ハイパーバイザーまたはその他のサービス上のVMを使用しない場合（またはWeb Studioを使用して専用ブレードPC上のデスクトップを管理する場合）は、接続の種類「**なし**」を選択します。
    - Remote PC Accessサイトを構成していて、Wake on LAN機能を使用する予定がある場合は、「**Microsoft System Center Virtual Machine Manager**」または「**Remote PC Wake on LAN**」の種類を選択します。詳しくは、Wake on LANを参照してください。

  接続の種類に加えて、Citrixツール（Machine Creation Services™など）またはその他のツールを使用してVMを作成するかどうかを指定します。
- 「**ストレージ**」および「**ネットワーク**」ページで指定する情報については、ホストストレージ、ストレージ管理、およびストレージの選択を参照してください。
- ハイブリッド権限ライセンスを所有しており、パブリッククラウドホスト接続（AWSなど）を追加している場合、それらの接続がここに一覧表示されます。これらのパブリッククラウドホスト接続を表示するには、追加後数分経ってからWeb Studioを更新してください。

リモートPCアクセス

リモートPCアクセス展開の詳細については、「リモートPCアクセス」を参照してください(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/remote-pc-access.html)。

Wake on LAN機能を使用する場合は、サイトを作成する前に、Microsoft System Center Configuration Managerで構成手順を完了してください。詳細については、「Configuration ManagerとリモートPCアクセスWake on LAN」を参照してください(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/remote-pc-access.html#wake-on-lan)。

接続とリソースを作成および管理する

> **重要:**

Citrix Virtual Apps and Desktops™ 7 2006以降、現在の展開で以下のいずれかのテクノロジーを使用している場合、それらのテクノロジーを使用するサポート終了（EOL）項目を削除した後にのみ、現在のリリースに展開をアップグレードできます。

- パーソナル vDisk (PvD)
- AppDisks™
- パブリッククラウドホストの種類：Citrix CloudPlatform、Microsoft Azure Classic

詳細については、「PVD、AppDisks、およびサポートされていないホストの削除」を参照してください。

注:

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

展開にパブリッククラウドホスト接続を使用する場合は、新規インストールまたは現在のリリースへのアップグレードを完了するためにHybrid Rights Licenseが必要です。

インストーラーがサポートされていないテクノロジーの1つ以上、またはHybrid Rights Licenseなしのホスト接続を検出すると、アップグレードが一時停止または停止し、説明メッセージが表示されます。インストーラーのログに詳細が含まれています。詳しくは、「展開のアップグレード」を参照してください。

Hybrid Rights Licenseがホスト接続に与える影響

Hybrid Rights Licenseの資格に基づいて、パブリッククラウドホストへのホスト接続が影響を受ける3つのシナリオがあります。

- パブリッククラウドホストへの新しいホスト接続を作成するには、Hybrid Rights Licenseが必要です。

- Hybrid Rights Licenseを所有しているがライセンスの有効期限が切れている場合、パブリッククラウドホストへの既存の接続は資格なしとマークされ、メンテナンスモードに入ります。既存のホスト接続がメンテナンスモードの場合、次の操作はできません。
  - ホスト接続の追加または変更
  - カタログの作成とイメージの更新
  - 電源操作を実行する
- 権限のないホスト接続が権限のあるホスト接続に変更されると、既存のホスティング接続が再度有効になります。

はじめに

サイトを作成する際に、ホスティングリソースへの最初の接続をオプションで作成できます。後で、その接続を変更したり、他の接続を作成したりできます。接続の構成には、サポートされているハイパーバイザーの中から接続タイプを選択すること、およびその接続のリソースから選択するストレージとネットワークが含まれます。

読み取り専用管理者は、接続とリソースの詳細を表示できます。接続とリソースの管理タスクを実行するには、フル管理者である必要があります。詳細については、「委任管理」を参照してください。

接続タイプに関する情報の場所

サポートされている仮想化プラットフォームを使用して、Citrix Virtual AppsまたはCitrix Virtual Desktops環境でマシンをホストおよび管理できます。「システム要件」の記事に、サポートされているタイプが記載されています。

詳細については、以下の情報源を参照してください。

- **XenServer（旧称はCitrix Hypervisor™）：**
  - XenServer仮想化環境。
  - XenServer®ドキュメント。
- **ニュータニックス アクロポリス:**
  - Nutanix仮想化環境。
  - Nutanix ドキュメント。
- **ヴイエムウェア:**

  - VMware仮想化環境。
  - VMware製品ドキュメント。

- **マイクロソフト Hyper-V:**
  - Microsoft System Center Virtual Machine Manager 仮想化環境の記事。
  - Microsoft ドキュメント。

- **パブリッククラウドホスト接続 (AWS、Google Cloud、Microsoft Azure、Nutanix クラウドおよびパートナーソリューション、VMware クラウドおよびパートナーソリューション):** パブリッククラウドホストに関する情報については、「リソースタイプのセットアップ」を参照してください。

> **注:**
>
> 情報源は Citrix DaaS™ ドキュメントに誘導します。Citrix DaaS 製品のパブリッククラウドホストに慣れている場合でも、オンプレミスバージョンにはいくつかの違いがあります。オンプレミスの Virtual Apps and Desktops では、管理インターフェイスは Web Studio と呼ばれます。更新はサービスに約4週間ごとに展開されます。そのため、サービスで利用できる特定の機能がオンプレミスバージョンでは利用できない場合があります。

ホストストレージ

サポートされているハイパーバイザーによって管理されている場合、ストレージ製品はサポートされます。Citrix Supportは、これらのストレージ製品ベンダーが問題のトラブルシューティングと解決を支援し、必要に応じてナレッジセンターにそれらの問題を文書化します。

マシンをプロビジョニングする際、データはタイプ別に分類されます。

- マスターイメージを含むオペレーティングシステム（OS）データ。
- 一時データ。このデータには、MCSプロビジョニングマシンに書き込まれるすべての非永続データ、Windowsページファイル、ユーザープロファイルデータ、およびShareFileと同期されるすべてのデータが含まれます。このデータは、マシンが再起動するたびに破棄されます。

データタイプごとにストレージを分離することで、各ストレージデバイスの負荷を軽減し、パフォーマンスを向上させ、ホストの利用可能なリソースを最大限に活用できます。また、異なる

データタイプに適したストレージを使用できるようになります。一部のデータでは、永続性と回復性が他のデータよりも重要になります。

ストレージは共有（中央に配置され、どのホストからも独立しており、すべてのホストで使用される）することも、ハイパーバイザーにローカルに配置することもできます。たとえば、中央共有ストレージは、1つ以上のWindows Server 2012クラスター化ストレージボリューム（接続されたストレージの有無にかかわらず）、またはストレージベンダーのアプライアンスにすることができます。中央ストレージは、ハイパーバイザーストレージ制御パスやパートナープラグインを介した直接アクセスなど、独自の最適化を提供する場合があります。

一時データをローカルに保存することで、共有ストレージにアクセスするためにネットワークを介する必要がなくなります。また、共有ストレージデバイスの負荷も軽減されます。共有ストレージはより高価になる可能性があるため、データをローカルに保存することで費用を削減できます。これらの利点は、ハイパーバイザーサーバー上の十分なストレージの可用性と比較検討する必要があります。

接続を作成するときは、2つのストレージ管理方法のいずれかを選択します。ハイパーバイザーによって共有されるストレージ、またはハイパーバイザーにローカルなストレージです。

1つ以上のXenServerホストで一時データストレージにローカルストレージを使用する場合は、プール内の各ストレージの場所に一意の名前があることを確認してください。（XenCenter®で名前を変更するには、ストレージを右クリックして名前プロパティを編集します。）

ハイパーバイザーで共有されるストレージ

ハイパーバイザーによって共有されるストレージ方式は、より長期的な永続性が必要なデータを中央に保存し、一元的なバックアップと管理を提供します。そのストレージにはOSディスクが格納されます。

この方法を選択すると、一時的なマシンデータにローカルストレージ（同じハイパーバイザープール内のサーバー上）を使用するかどうかを選択できます。この方法は、共有ストレージ内のデータ（*一時データキャッシュ*と呼ばれる）ほど永続性や回復性を必要としません。ローカルディスクは、メインOSストレージへのトラフィックを削減するのに役立ちます。このディスクは、マシンの再起動ごとにクリアされます。ディスクはライトスルーメモリキャッシュを介してアクセスされます。一時データにローカルストレージを使用する場合、プロビジョニングされたVDAは特定のハイパーバイザーホストに紐付けられます。そのホストが故障すると、VMは起動できません。

例外: Microsoft System Center Virtual Machine Managerでは、クラスター共有ボリューム（CSV）を使用している場合、ローカルストレージ上の一時データキャッシュディスクは許可されません。

一時データをローカルに保存するための接続を作成し、各VMのキャッシュディスクサイズとメモリサイズの非デフォルト値を有効にして構成します。デフォルト値は接続タイプに合わせて調整されており、ほとんどのケースで十分です。詳細については、「マシンカタログの作成」を参照してください。

ハイパーバイザーは、ディスクイメージをローカルで読み取りキャッシュすることにより、最適化テクノロジーを提供することもできます。たとえば、XenServerはIntelliCache™を提供し、中央ストレージへのネットワークトラフィックを削減します。

ハイパーバイザーのローカルストレージ

ハイパーバイザーにローカルなストレージ方式では、データをハイパーバイザーにローカルに保存します。この方式では、マスターイメージやその他のOSデータがサイト内のハイパーバイザーに転送されます。このプロセスは、最初のマシン作成時と将来のイメージ更新時に発生します。このプロセスにより、管理ネットワークでかなりのトラフィックが発生します。イメージ転送には時間がかかり、イメージは各ホストで異なるタイミングで利用可能になります。

接続とリソースの作成

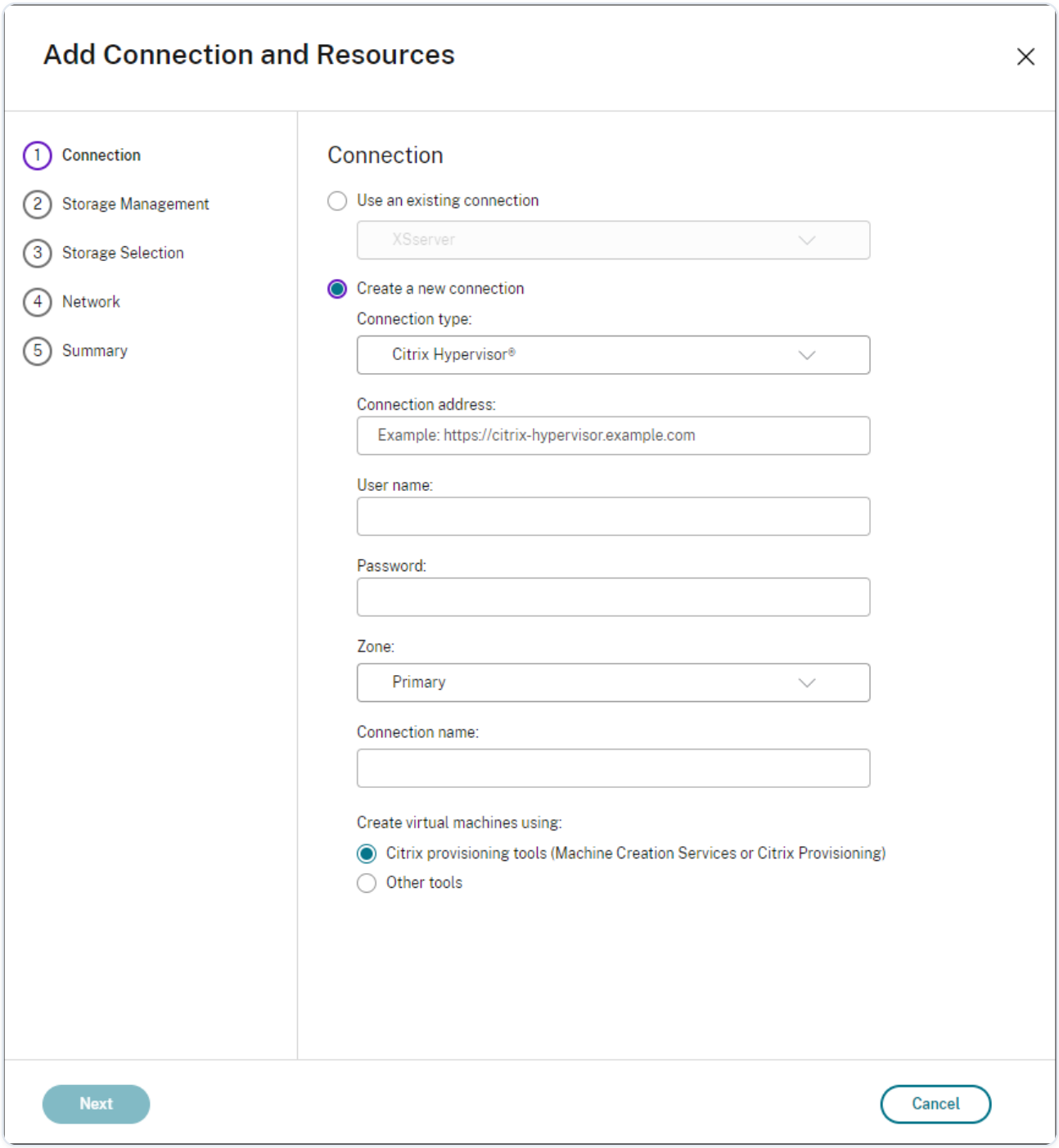
サイトを作成するときに、最初の接続をオプションで作成できます。サイト作成ウィザードには、以下のセクションで説明されている接続関連のページが含まれています。

サイトの作成後に接続を作成する場合は、手順1から開始します。

> **重要:**
>
> 接続を作成する前に、ホストリソース（ストレージとネットワーク）が利用可能である必要があります。

1. Web Studioにサインインします。
2. 左側のペインで**ホスティング**を選択します。
3. アクションバーで**接続とリソースの追加**を選択します。
4. ウィザードは以下のページを案内します（特定のページの内容は、選択した接続タイプによって異なります）。各ページを完了したら、**次へ**をクリックして**概要**ページに進みます。

接続



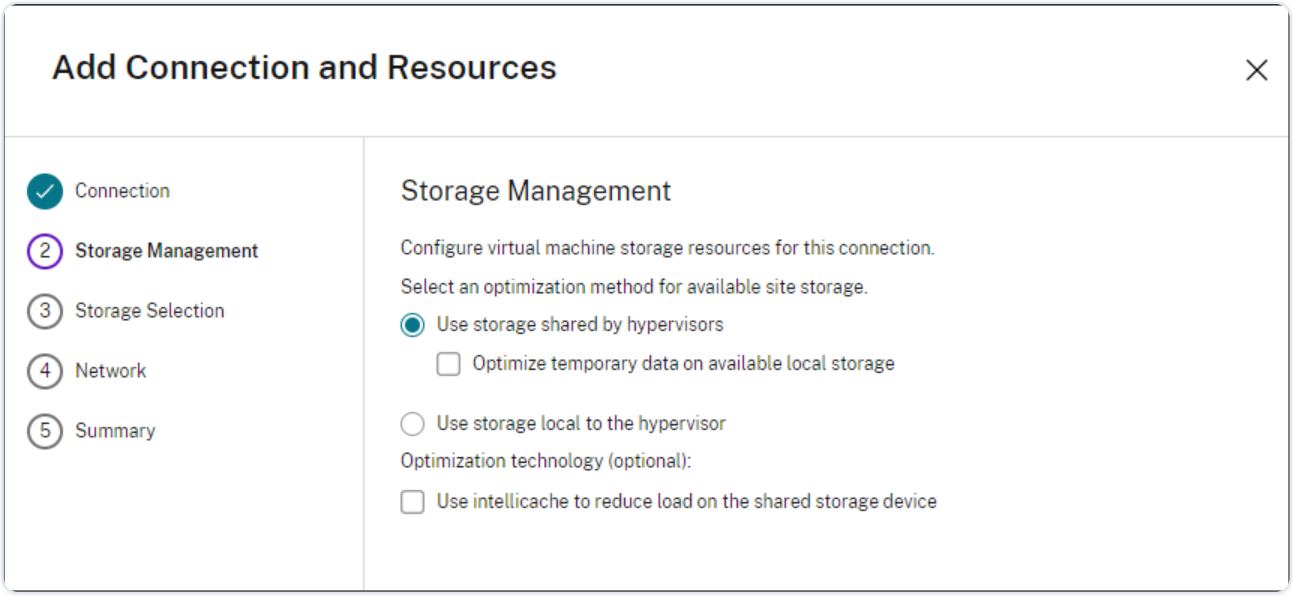
「**接続**」ページで：

- 接続を作成するには、 を選択します。既存の接続と同じホスト構成に基づいて接続を作成するには、 を選択し、関連する接続を選択します。
- フィールドで、使用しているハイパーバイザーを選択します。パブリッククラウドホスト接続は、Hybrid Rights Licenseを使用している場合にのみドロップダウンリストに表示されます。または、PowerShellコマンド `Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false/true を使用して、以下を取得できます。

  - サードパーティ製プラグインを含む、Citrixがサポートするすべてのハイパーバイザープラグインのリスト。
  - ハイパーバイザープラグインの可用性。可用性ステータスが **false** の場合、ハイパーバイザープラグインが正しくインストールされていないか、Hybrid Rights Licenseの資格がないことが考えられます。

- 接続アドレスと資格情報フィールドは、選択した接続タイプによって異なります。要求された情報を入力します。
- 接続名を入力します。この名前はWeb Studioに表示されます。
- 仮想マシンの作成に使用するツールを選択します: Web Studioツール（Machine Creation Services™やCitrix Provisioningなど）またはその他のツール。

ストレージ管理



ストレージ管理の種類と方法については、「ホストストレージ」を参照してください。

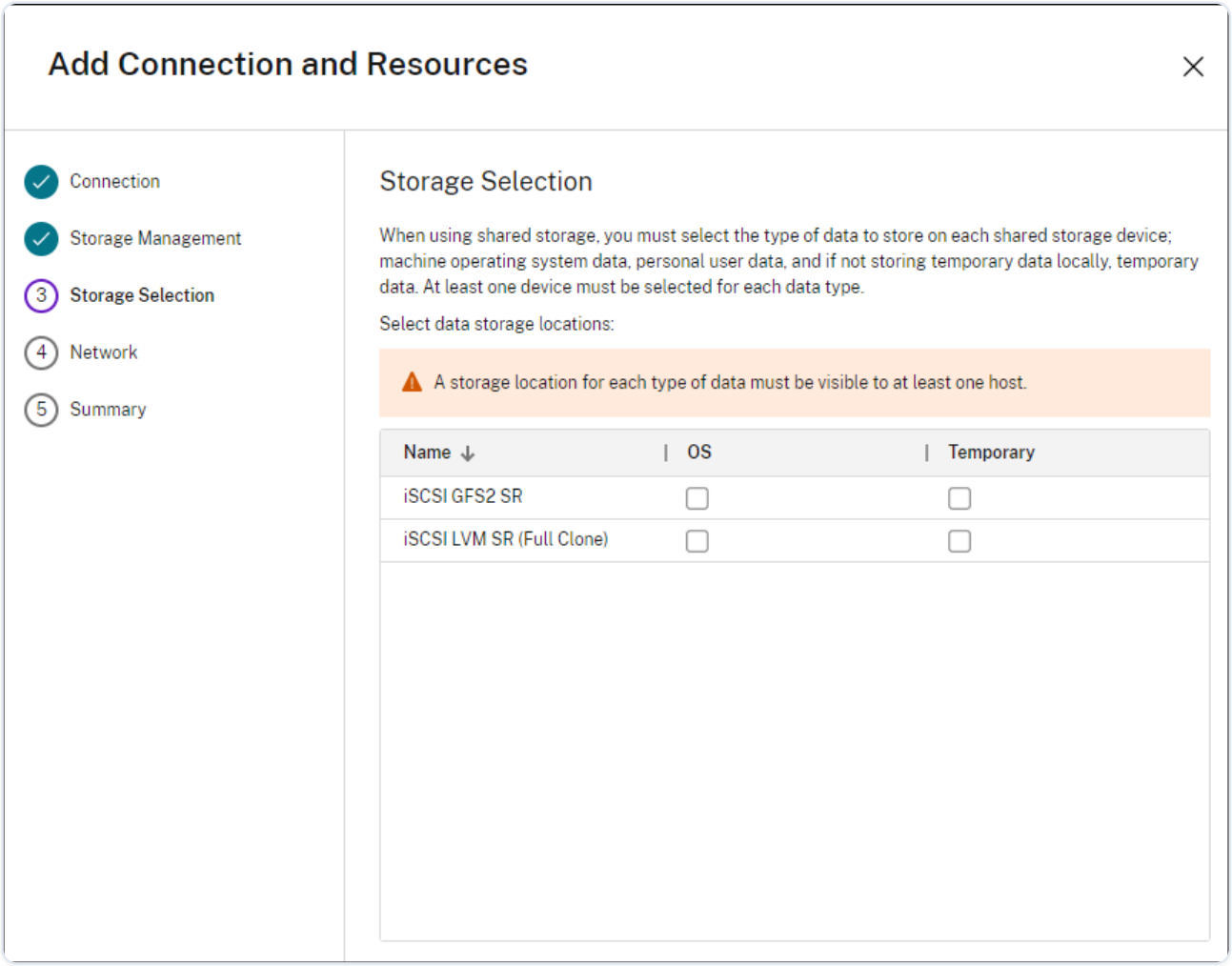
Hyper-V または VMware ホストへの接続を構成している場合は、クラスター名を参照して選択します。その他の接続タイプでは、クラスター名は要求されません。

ストレージ管理方法を選択します: ハイパーバイザー間で共有されるストレージ、またはハイパーバイザーにローカルなストレージ。

- ハイパーバイザー間で共有されるストレージを選択した場合、利用可能なローカルストレージに一時データを保持するかどうかを指定します。（この接続を使用するマシンカタログで、デフォルト以外のテンポラリストレージサイズを指定できます。）**例外:** クラスター共有ボリューム（CSV）を使用する場合、Microsoft System Center Virtual Machine Managerはローカルストレージ上の一時データキャッシュディスクを許可しません。Web Studioでそのストレージ管理設定を構成すると失敗します。

XenServerプールで共有ストレージを使用している場合は、IntelliCacheを使用して共有ストレージデバイスへの負荷を軽減するかどうかを指定します。「XenServer接続にIntelliCacheを使用する」を参照してください。

ストレージの選択



ストレージの選択の詳細については、「ホストストレージ」を参照してください。

利用可能なデータタイプごとに、少なくとも1つのホストストレージデバイスを選択します。前のページで選択したストレージ管理方法によって、このページで選択できるデータタイプが決まります。ウィザードの次のページに進む前に、サポートされているデータタイプごとに少なくとも1つのストレージデバイスを選択してください。

「**ストレージの選択**」ページの下部には、ハイパーバイザー間で共有されるストレージを選択し、前のページで「**利用可能なローカルストレージ上の一時データを最適化**」を有効にした場合に、追加の構成オプションが表示されます。一時データに使用するローカルストレージデバイスを選択できます。

現在選択されているストレージデバイスの数が表示されます（上記の図では「1 storage device selected」）。そのエントリにカーソルを合わせると、選択されたデバイス名が表示されます。

1. 使用するストレージデバイスを変更するには、**選択**をクリックします。
2. **ストレージの選択**ダイアログボックスで、ストレージデバイスのチェックボックスをオンまたはオフにして、**OK**をクリックします。

ネットワーク

ネットワークページで、リソースの名前を入力します。この名前は、接続に関連付けられたストレージとネットワークの組み合わせを識別するためにWeb Studioに表示されます。

仮想マシンが使用するネットワークを1つ以上選択します。

概要

概要ページで、選択内容を確認します。完了したら、**完了**をクリックします。

注意: 一時データをローカルに保存すると、この接続を使用するマシンを含むマシンカタログを作成するときに、一時データストレージのデフォルト以外の値を構成できます。「マシンカタログの作成」を参照してください。

接続設定の編集

この手順を使用して、接続の名前を変更したり、接続を作成したりしないでください。これらの接続は異なる操作です。現在使用中のホストマシンに新しいアドレスがある場合にのみ、アドレスを変更してください。異なるマシンにアドレスを入力すると、接続のマシンカタログが破損します。

このリソースにアクセスするマシンカタログは、適切なGPU固有のマスターイメージを使用する必要があるため、接続の**GPU**設定を変更することはできません。接続を作成してください。

1. Web Studioにサインインします。
2. 左ペインで「**ホスティング**」を選択します。
3. 接続を選択し、アクションバーで「**接続の編集**」を選択します。
4. 接続を編集するときに利用できる設定のガイダンスに従ってください。
5. 完了したら、行った変更を適用してウィンドウを開いたままにするには **適用** をクリックするか、変更を適用してウィンドウを閉じるには **保存** をクリックします。

接続プロパティ ページ:

- 接続アドレスと資格情報を変更するには、**設定の編集...** を選択し、新しい情報を入力します。

- XenServer接続の高可用性サーバーを指定するには、**サーバーの編集...** を選択し、サーバーを選択します。Citrixでは、プールマスターが失敗した場合にXenServerとの通信を可能にするため、プール内のすべてのサーバーを選択することをお勧めします。

  > **注:**
  >
  > HTTPSを使用しており、高可用性サーバーを構成する場合は、プール内のすべてのサーバーにワイルドカード証明書をインストールしないでください。各サーバーに個別の証明書が必要です。

詳細 ページ:

- Remote PC Accessで使用されるMicrosoft System Center Configuration Manager (ConfMgr) Wake on LAN接続タイプの場合、**ConfMgr Wake Proxy**、マジックパケット、およびパケット送信情報を入力します。
- スロットリングしきい値設定を使用すると、接続で許可される電源アクションの最大数を指定できます。これらの設定は、電源管理設定によって同時に起動できるマシンの数が多すぎたり少なすぎたりする場合に役立ちます。各接続タイプには、ほとんどの場合に適切な特定のデフォルト値があり、変更してはなりません。
- **同時アクション（すべてのタイプ）** 設定では、この接続で同時に発生できる最大絶対数と、この接続を使用するすべてのマシンの最大割合の2つの値を指定します。絶対値とパーセンテージ値の両方を指定する必要があります。適用される実際の制限は、これらの値の小さい方です。

  たとえば、34台のマシンがある展開で、**同時アクション（すべてのタイプ）** が絶対値10、パーセンテージ値10に設定されている場合、適用される実際の制限は3です（つまり、34の10パーセントを最も近い整数に丸めたもので、絶対値10台のマシンよりも小さい）。
- **1分あたりの最大新規アクション数** は絶対数です。パーセンテージ値はありません。
- **接続オプション** フィールドには、Citrixサポート担当者の指示または明示的なドキュメントの指示がある場合にのみ情報を入力してください。

共有テナント ページ:

この接続のサブスクリプションとAzure Compute Galleryを共有するテナントとサブスクリプションを追加します。その結果、カタログを作成または更新する際に、それらのテナントとサブスクリプションから共有イメージを選択できます。

- この接続に関連付けられているアプリケーションの**アプリケーションID**と**アプリケーションシークレット**を入力します。この情報を使用して、Azureに認証できます。セキュリティを確保するため、定期的にキーを変更することをお勧めします。
- 共有テナントとサブスクリプションを指定します。最大8つの共有テナントを追加できます。各テナントにつき、最大8つのサブスクリプションを追加できます。
- 完了したら、**保存**と**適用**をクリックします。

「**接続オプション**」フィールドには、Citrixサポート担当者の指示がある場合にのみ情報を入力してください。

ネットワークの編集

接続のネットワークを変更できます。次の手順を実行します。

1. に移動します。
2. 接続の下にあるターゲットリソースを選択し、アクションバーで を選択します。
3. 仮想マシンが使用するネットワークを1つ以上選択します。
4. 変更を保存して終了するには、**保存**をクリックします。

接続のメンテナンスモードをオンまたはオフにする

接続のメンテナンスモードをオンにすると、新しい電源操作が接続に保存されているマシンに影響を与えるのを防ぎます。ユーザーは、マシンがメンテナンスモードの場合、マシンに接続できません。ユーザーがすでに接続している場合、メンテナンスモードはログオフ時に有効になります。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択します。メンテナンスモードをオンにするには、アクションバーで**Turn On Maintenance Mode**を選択します。メンテナンスモードをオフにするには、**Turn Off Maintenance Mode**を選択します。

個々のマシンに対してメンテナンスモードをオンまたはオフにすることもできます。また、マシンカタログまたはデリバリーグループ内のマシンに対してメンテナンスモードをオンまたはオフにすることもできます。

接続を削除する

接続を削除すると、多数のマシンが削除され、データが失われる可能性があります。影響を受けるマシンのユーザーデータがバックアップされているか、または不要であることを確認してください。

接続を削除する前に、以下を確認してください。

- 接続に保存されているすべてのマシンからすべてのユーザーがログオフしていること。
- 切断されたユーザーセッションが実行されていないこと。
- プールされたマシンと専用マシンのメンテナンスモードがオンになっていること。
- 接続で使用されているマシンカタログ内のすべてのマシンは電源がオフになります。

カタログによって参照されている接続を削除すると、マシンカタログは使用できなくなります。この接続がカタログによって参照されている場合、カタログを削除するオプションがあります。カタログを削除する前に、他の接続で使用されていないことを確認してください。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**接続の削除**を選択します。
4. この接続にマシンが保存されている場合、マシンを削除するかどうかを尋ねられます。削除する場合は、関連するActive Directoryコンピューターアカウントをどうするかを指定します。

接続の名前変更またはテスト

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**接続名の変更**または**接続のテスト**を選択します。

接続上のマシンの詳細を表示する

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**マシンの表示**を選択します。

上部のペインには、接続を介してアクセスされるマシンが一覧表示されます。マシンを選択すると、下部のペインにその詳細が表示されます。開いているセッションのセッション詳細も提供されます。

検索機能を使用して、マシンをすばやく見つけます。ウィンドウ上部のリストから保存された検索を選択するか、新しい検索を作成します。マシン名の全部または一部を入力して検索するか、高度な検索に使用する式を作成できます。式を作成するには、**展開**をクリックし、プロパティと演算子のリストから選択します。

接続上のマシンを管理する

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、**アクション**ペインで**マシンの表示**を選択します。
4. アクションバーで次のいずれかを選択します。マシン状態と接続ホストの種類によっては、一部のアクションが利用できない場合があります。

アクション	説明
開始	マシンが電源オフまたは中断状態の場合に、マシンを起動します。
中断	マシンをシャットダウンせずに一時停止し、マシンの一覧を更新します。
シャットダウン	オペレーティングシステムにシャットダウンを要求します。
強制シャットダウン	マシンの電源を強制的にオフにし、マシンの一覧を更新します。
再起動	オペレーティングシステムにシャットダウンと再起動を要求します。オペレーティングシステムがこれに応じられない場合、デスクトップは現在の状態のままになります。
メンテナンスモードを有効にする	マシンへの接続を一時的に停止します。この状態のマシンにはユーザーは接続できません。ユーザーが接続している場合、メンテナンスモードはログオフ時に有効になります。（上記のように、接続を介してアクセスされるすべてのマシンに対してメンテナンスモードをオンまたはオフにすることもできます。）

アクション	説明
デリバリーグループから削除	デリバリーグループからマシンを削除しても、デリバリーグループが使用するマシンカタログから削除されるわけではありません。マシンは、ユーザーが接続していない場合にのみ削除できます。マシンを削除している間、ユーザーが一時的に接続できないようにするには、メンテナンスモードをオンにします。
削除	マシンを削除すると、ユーザーはそのマシンにアクセスできなくなり、マシンはマシンカタログから削除されます。マシンを削除する前に、すべてのユーザーデータがバックアップされているか、不要であることを確認してください。マシンは、どのユーザーも接続していない場合にのみ削除できます。マシンを削除している間、ユーザーが接続できないように、メンテナンスモードをオンにしてください。

マシンのシャットダウンを伴う操作の場合、マシンが10分以内にシャットダウンしないと、電源がオフになります。シャットダウン中にWindowsが更新プログラムのインストールを試みると、更新が完了する前にマシンの電源がオフになるリスクがあります。

ストレージの編集

接続を使用するVMのオペレーティングシステムデータと一時データを保存するために使用されるサーバーのステータスを表示できます。また、各データタイプのストレージにどのサーバーを使用するかを指定することもできます。

1. Web Studioにサインインします。
2. 左ペインで**「ホスティング」**を選択します。
3. 接続を選択し、アクションバーで**「ストレージの編集」**を選択します。
4. 左ペインで、データタイプ（オペレーティングシステムまたは一時）を選択します。
5. 選択したデータタイプに対して、1つ以上のストレージデバイスのチェックボックスをオンまたはオフにします。
6. **「OK」**をクリックします。

リスト内の各ストレージデバイスには、その名前とストレージステータスが含まれます。有効なストレージステータス値は次のとおりです。

- **使用中:** ストレージはマシンの作成に使用されています。
- **廃止済み:** ストレージは既存のマシンにのみ使用されています。このストレージには新しいマシンは追加されません。
- **未使用:** ストレージはマシンの作成に使用されていません。

現在**使用中**のデバイスのチェックボックスをオフにすると、そのステータスは**廃止済み**に変わります。既存のマシンはそのストレージデバイスを引き続き使用し（データを書き込むこともできます）、そのため、マシンの作成に使用されなくなった後でも、その場所がいっぱいになる可能性があります。

リソースの削除、名前変更、またはテスト

1. Web Studioにサインインします。
2. 左側のペインで**ホスティング**を選択します。
3. リソースを選択し、アクションバーで適切なエントリ（**リソースの削除**、**リソース名の変更**、または**リソースのテスト**）を選択します。

孤立したAzureリソースの検出

孤立したリソースは、システム内に存在する使用されていないリソースであり、不要な費用につながる可能性があります。

この機能を使用すると、Citrix Virtual Apps and Desktopsサイトのホストにある孤立したAzureリソースを検出できます。

Web Studioで次の手順を実行します。

1. **管理**から、左側のペインで**ホスティング**を選択します。
2. 接続を選択し、アクションバーで**孤立したリソースの検出**を選択します。**孤立したリソースの検出**ダイアログボックスに、孤立したリソースのレポートが表示されます。
3. 孤立したリソースのレポートを表示するには、**レポートの表示**を選択します。

または、PowerShellを使用して孤立したAzureリソースを検出することもできます。詳しくは、「孤立したリソースのリストを取得する」を参照してください。

孤立したリソースの原因を理解し、その後の対処方法については、「Citrixで孤立したAzureリソースを効率的に管理する」を参照してください。

接続タイマー

ポリシー設定を使用して、3つの接続タイマーを構成できます。

- **最大接続タイマー:** ユーザーデバイスと仮想デスクトップ間の途切れない接続の最大継続時間を決定します。**セッション接続タイマー**および**セッション接続タイマー間隔**ポリシー設定を使用します。
- **接続アイドルタイマー:** ユーザーからの入力がない場合に、仮想デスクトップへの途切れないユーザーデバイス接続が維持される期間を決定します。**セッションアイドルタイマー**および**セッションアイドルタイマー間隔**ポリシー設定を使用します。
- **切断タイマー:** 切断されロックされた仮想デスクトップが、セッションがログオフされるまでロックされたままになる期間を決定します。**切断セッションタイマー**および**切断セッションタイマー間隔**ポリシー設定を使用します。

これらの設定のいずれかを更新する場合は、展開全体で一貫性があることを確認してください。

詳細については、ポリシー設定のドキュメントを参照してください。

孤立したリソースのリストを取得する

MCS によって作成されたものの、MCS によって追跡されなくなった孤立したリソースのリストを取得できます。これは現在、Azure 環境に適用されます。リストを取得するには、PowerShell コマンドを使用できます。接続を使用してフィルタリングできます。

> **注:**
>
> - プロビジョニングまたはイメージの更新が進行中の場合、PowerShellコマンドは拒否されます。
> - すべてのCitrixタグが付けられた顧客管理リソースは、孤立したリソースとして検出されます。ただし、そのリソースに値がtrueの別のタグCitrixDetectIgnoreを追加すると、孤立したリソースの検出中にそのリソースは無視されます。

制限事項

- 組み込みのフル管理者またはクラウド管理者ロールの管理者ユーザーのみが、PowerShellコマンドを実行して孤立リソースのリストを取得できます。
- 孤立したリソースの誤認識を避けるため、孤立したリソースをフィルタリングしている間はVMの電源を入れないでください。
- 負荷が高い可能性がある場合、約2,000件のレコードが孤立として表示されます。

孤立リソースのリストを表示するには：

1. **PowerShell**ウィンドウを開きます。
2. 次のコマンドを実行します。

    a. 接続UIDを取得します。接続UIDは、HypervisorConnectionUid属性の値です。

    ```
    Get-ChildItem xdhyp:\connections | where { $_.PluginId -like
    'Azure*' }"
    ```

    b. 孤立したリソースのリストを取得します。

    ```
    get-provorphanedresource -HypervisorConnectionUid <connection uid>
    ```

サブスクリプションIDから孤立リソースのリストを表示するには：

1. **PowerShell**ウィンドウを開きます。
2. 次のコマンドを実行します。

    a. サブスクリプションIDを使用して接続UIDを見つけます。接続UIDは HypervisorConnectionUid属性の値です。

    ```
    Get-ChildItem xdhyp:\connections | where { $_.CustomProperties
    -match '<subscriptionId>' }
    ```

    b. 孤立リソースのリストを取得します。

    ```
    get-provorphanedresource -HypervisorConnectionUid <connection uid>
    ```

注:

削除する前にリソースを慎重に確認してください。

次のステップ

特定のホストタイプへの接続については、以下を参照してください。

- AWSへの接続
- XenServerへの接続

- Googleクラウド環境への接続(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections/connection-gcp.html)
- Microsoft Azureへの接続(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections/connection-azure-resource-manager.html)
- マイクロソフト システム センター バーチャル マシン マネージャー への接続
- Nutanixへの接続(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections/connection-nutanix.html)
- Nutanixクラウドおよびパートナーソリューションへの接続(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections/connection-nutanix-cloud-and-partner-solutions.html)
- VMwareへの接続(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections/connection-vmware-virtualization-environments.html)
- VMwareクラウドおよびパートナーソリューションへの接続(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections/connection-vmware-cloud-partner-solutions.html)

初期展開プロセス中の場合は、マシンカタログを作成します。

AWSへの接続

接続とリソースの作成と管理(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections.html)は、接続を作成するウィザードについて説明しています。以下の情報は、AWSクラウド環境に固有の詳細を扱っています。

> **注:**
>
> AWSへの接続を作成する前に、まず、AWSアカウントをリソースの場所として設定を完了する必要があります。「AWSクラウド環境(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/install-prepare/aws.html)」を参照してください。

接続を作成する

Web Studioから接続を作成する場合：

- APIキーとシークレットキーの値を指定する必要があります。これらの値を含むキーファイルをAWSからエクスポートし、インポートできます。また、リージョン、アベイラビリティゾーン、VPC名、サブネットアドレス、ドメイン名、セキュリティグループ名、および資格情報も指定する必要があります。

- ルートAWSアカウントの資格情報ファイル（AWSコンソールから取得）は、標準のAWSユーザー向けにダウンロードされた資格情報ファイルと同じ形式ではありません。そのため、Citrix Virtual Apps and Desktops™管理では、このファイルを使用してAPIキーとシークレットキーのフィールドに入力することはできません。AWS Identity Access Management (IAM) 資格情報ファイルを使用していることを確認してください。

> **注:**
>
> 接続を作成した後、APIキーとシークレットキーの更新が失敗する場合があります。この問題を解決するには、プロキシサーバーまたはファイアウォールの制限を確認し、次のアドレスに接続できることを確認してください: `https://*.amazonaws.com`。

ホスト接続のデフォルト値

AWSクラウド環境でホスト接続を作成すると、次のデフォルト値が表示されます。

オプション	絶対値	パーセンテージ
同時実行アクション (すべての種類)	125	100
1分あたりの新規アクションの最大数	125	

MCS は、デフォルトで最大 100 の同時プロビジョニング操作をサポートします。

サービスエンドポイント URL

標準ゾーンサービスエンドポイント URL

MCS を使用すると、API キーと API シークレットを使用して新しい AWS 接続が追加されます。この情報と認証済みアカウントを使用して、MCS は AWS DescribeRegions EC2 API 呼び出しを使用して、サポートされているゾーンを AWS に照会します。クエリは、汎用 EC2 サービスエンドポイント URL `https://ec2.amazonaws.com/` を使用して行われます。MCS を使用して、サポートされているゾーンのリストから接続するゾーンを選択します。優先される AWS サービスエンドポイント URL は、そのゾーンに対して自動的に選択されます。ただし、サービスエンドポイント URL を作成した後は、その URL を設定または変更することはできません。

IAM 権限を定義する

このセクションの情報を使用して、AWS 上の Citrix Virtual Apps and Desktops の IAM 権限を定義します。Amazon の IAM サービスでは、複数のユーザーを持つアカウントが許可されており、それらのユーザーはさらにグループに編成できます。これらのユーザーは、アカウントに関連付けられた操作を実行する能力を制御するために、異なる権限を持つことができます。IAM 権限の詳細については、「IAM JSON ポリシーリファレンス」を参照してください。

IAM 権限ポリシーを新しいユーザーグループに適用するには：

1. AWS マネジメントコンソールにログインし、ドロップダウンリストから **IAM サービス**を選択します。
2. を選択します。
3. 新しいユーザーグループの名前を入力し、 を選択します。
4. **権限**ページで、**カスタムポリシー**を選択します。**選択**をクリックします。
5. **権限ポリシー**の名前を入力します。
6. **ポリシードキュメント**セクションで、関連する権限を入力します。

ポリシー情報を入力したら、**続行**を選択してユーザーグループを完了します。グループ内のユーザーには、Citrix Virtual Apps and Desktopsに必要なアクションのみを実行する権限が付与されます。

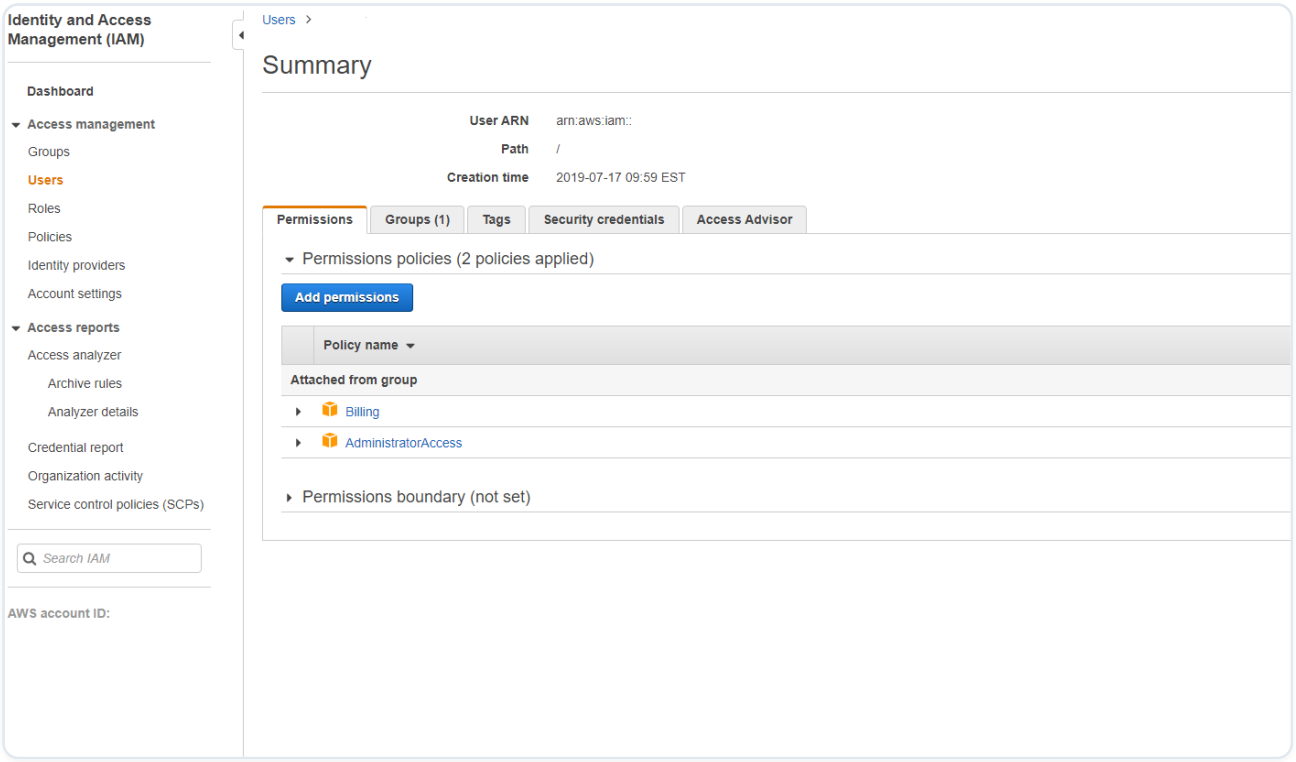
> **重要:**

> 前の例で提供されているポリシーテキストを使用して、Citrix Virtual Apps and DesktopsがAWSアカウント内でアクションを実行するために使用するアクションを、それらのアクションを特定のリソースに制限することなくリストします。Citrixは、テスト目的でこの例を使用することをお勧めします。本番環境では、リソースにさらに制限を追加することを選択できます。

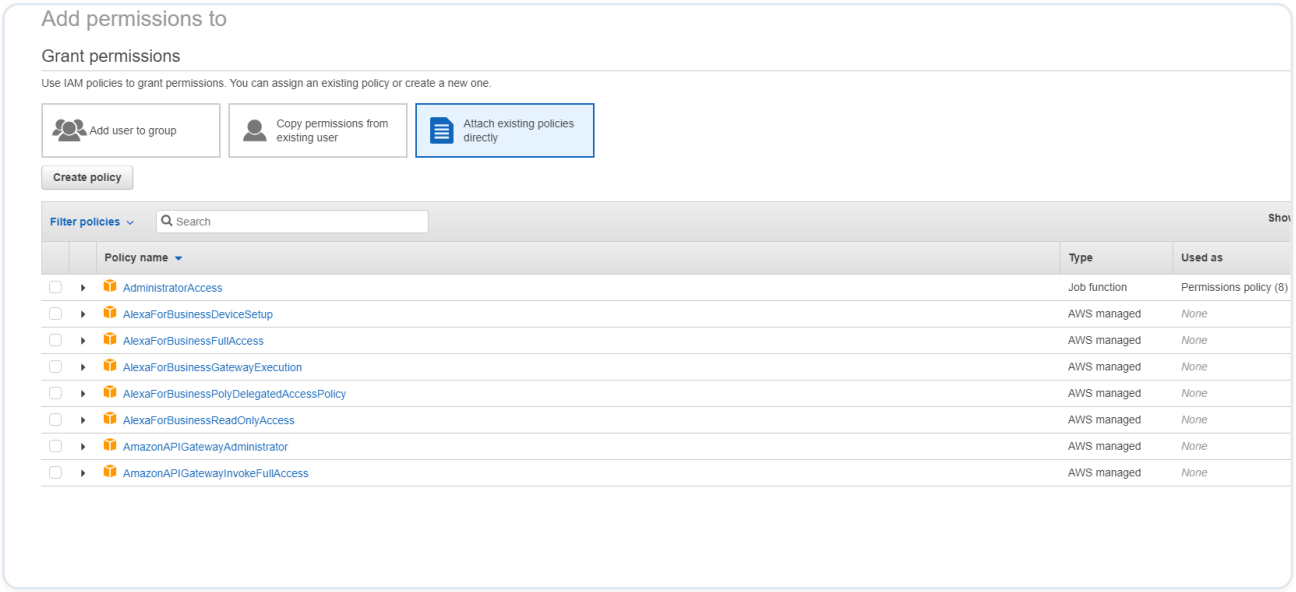
IAM権限を設定する

AWSマネジメントコンソールの**IAM**セクションで権限を設定します。

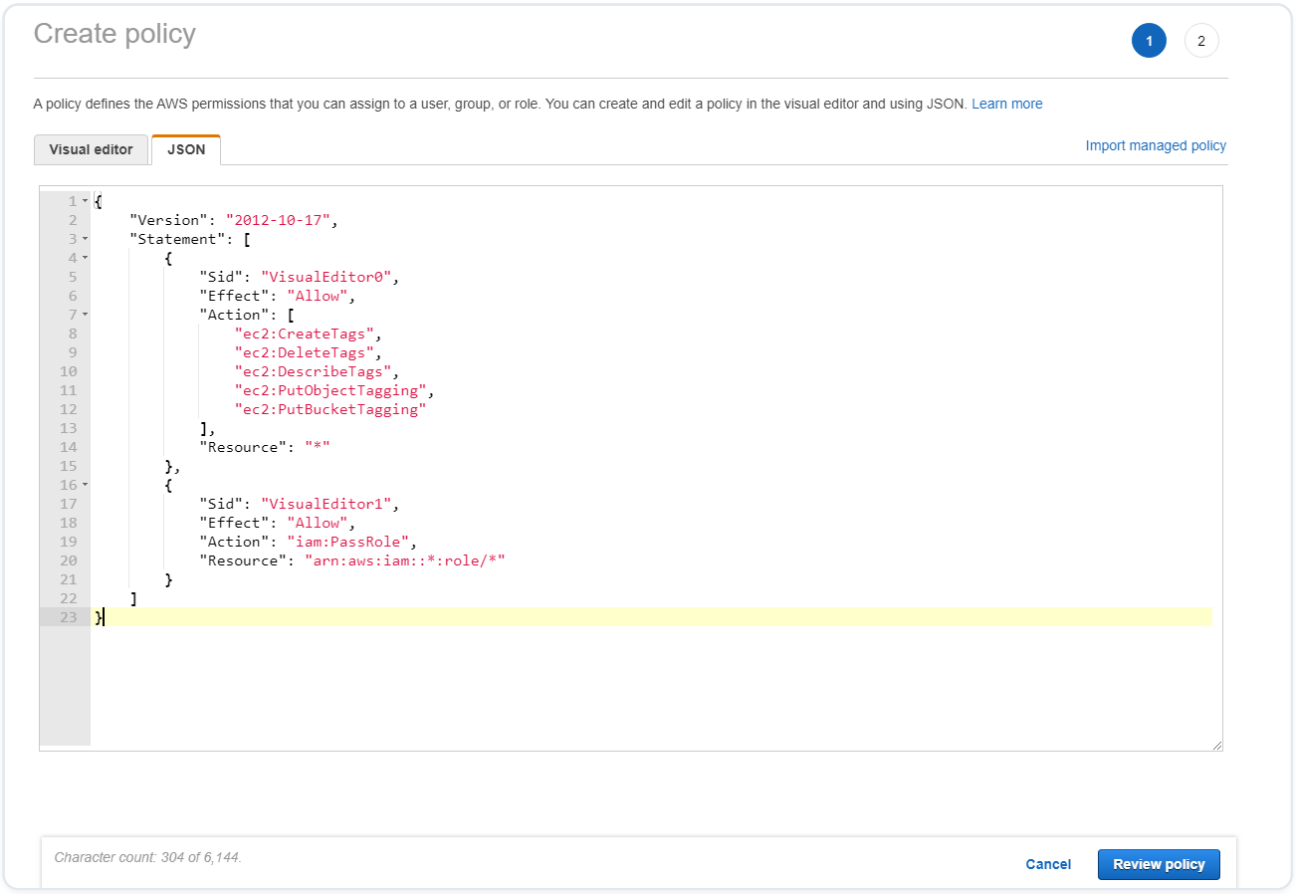
1. **概要**パネルで、**権限**タブを選択します。
2. **権限を追加**を選択します。



権限の追加先画面で、権限を付与します。



JSONタブで、以下を例として使用します。



ヒント:

記載されているJSONの例には、お使いの環境のすべての権限が含まれていない場合があります。詳細については、「AWSでCitrix Virtual Apps and Desktopsを実行するためのIDおよびアクセス管理権限の定義方法」を参照してください。

必要なAWS権限

このセクションには、AWS権限の完全なリストが含まれています。

注:

iam:PassRole 権限は、**role_based_auth** の場合にのみ必要です。

ホスト接続の作成

AWSからの情報を使用して、新しいホスト接続が追加されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs"
                "ec2:DescribeRegions",
                "ec2:DescribeSnapshots",
                "ec2:DescribeLaunchTemplates"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

VM の電源管理

マシンインスタンスの電源はオンまたはオフになります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DetachVolume",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:DescribeInstanceStatus"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

仮想マシンの作成、更新、または削除

AWSインスタンスとしてプロビジョニングされたVMを使用して、マシンカタログが作成、更新、または削除されます。

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "ec2:AttachVolume",

                "ec2:AssociateIamInstanceProfile",

                "ec2:AuthorizeSecurityGroupEgress",

                "ec2:AuthorizeSecurityGroupIngress",

                "ec2:CreateImage",

                "ec2:CreateLaunchTemplate",

                "ec2:CreateSecurityGroup",

                "ec2:CreateTags",

                "ec2:CreateVolume",

                "ec2:DeleteVolume",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",
```

```
                "ec2:DescribeInstanceTypes",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",

                "ec2:DescribeVolumes",

                "ec2:DescribeVpcs",

                "ec2:DetachVolume",

                "ec2:DisassociateIamInstanceProfile",

                "ec2:RunInstances",

                "ec2:StartInstances",

                "ec2:StopInstances",

                "ec2:TerminateInstances"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
```

```
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
```

```
}
```

注:

セキュリティグループに関連するEC2セクションは、カタログ作成時に準備VM用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが完了すると、これらの権限は不要になります。

ディスクの直接アップロードとダウンロード

直接ディスクアップロードにより、マシンカタログのプロビジョニングにおけるボリュームワーカーの要件が不要になり、代わりにAWSが提供するパブリックAPIが使用されます。この機能により、追加のストレージアカウントに関連するコストと、ボリュームワーカー操作の維持に関する複雑さが軽減されます。

注:

ボリュームワーカーのサポートは非推奨になりました。

以下の権限をポリシーに追加する必要があります。

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

重要:

- ボリュームワーカーAMIやボリュームワーカーVMなどのボリュームワーカー操作なしで、既存のマシンカタログにVMを追加できます。
- 以前にボリュームワーカーを使用していた既存のカタログを削除すると、ボリュームワーカー関連を含むすべてのアーティファクトが削除されます。

作成されたボリュームのEBS暗号化

AMIが暗号化されている場合、またはEBSがすべての新しいボリュームを暗号化するように構成されている場合、EBSは新しく作成されたボリュームを自動的に暗号化できます。ただし、この機能を実装するには、IAMポリシーに以下の権限を含める必要があります。

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",

                 "kms:DescribeKey",

                 "kms:GenerateDataKeyWithoutPlainText",

                 "kms:ReEncryptTo",

                 "kms:ReEncryptFrom"

            ],

            "Resource": "*"

        }
```

```
    ]

}
```

注:

権限は、ユーザーの裁量でリソースと条件ブロックを含めることにより、特定のキーに制限できます。例: **条件付きKMS権限**:

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",

                 "kms:DescribeKey",

                 "kms:GenerateDataKeyWithoutPlainText",

                 "kms:ReEncryptTo",

                 "kms:ReEncryptFrom"

            ],

            "Resource": [

                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-
a123-456d-a12b-a123b4cd56ef"
```

```
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

以下のキーポリシーステートメントは、アカウントがIAMポリシーを使用してKMSキーに対するすべてのアクション (kms:*) の権限を委任することを許可するために必要な、KMSキーのデフォルトキーポリシー全体です。

```
{
"Sid": "Enable IAM policies",
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::111122223333:root"
},
"Action": "kms:",
"Resource": ""
}
```

詳細については、「AWS Key Management Service 公式ドキュメント」を参照してください。

IAMロールベース認証

ロールベース認証をサポートするために、以下の権限が追加されます。

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]

}
```

最小限のIAM権限ポリシー

以下のJSONは、現在サポートされているすべての機能に使用できます。このポリシーを使用して、ホスト接続の作成、VMの作成、更新、削除、および電源管理を行うことができます。 このポリシーは、IAM権限の定義セクションで説明されているようにユーザーに適用することも、**role_based_auth**セキュリティキーとシークレットキーを使用してロールベース認証を使用することもできます。

> **重要:**
>
> **role_based_auth** を使用するには、まずサイト内のすべてのDelivery Controllerで目的のIAMロールを構成します。Web Studioを使用してホスティング接続を追加し、認証キーとシークレットに role_based_auth を指定します。これらの設定を持つホスティング接続は、ロールベース認証を使用します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
```

```
                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",

                "ec2:DescribeVolumes",

                "ec2:DescribeVpcs",

                "ec2:DetachVolume",

                "ec2:DisassociateIamInstanceProfile",
```

```
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
```

```
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutBucketAcl",
                "s3:PutObject",
                "s3:PutBucketTagging",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:GenerateDataKey",
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
        }
```

```
    ]
}
```

注:

- SecurityGroupsに関連するEC2セクションは、カタログ作成時に準備VM用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが完了すると、これらの権限は不要になります。
- KMSセクションは、EBSボリューム暗号化を使用する場合にのみ必要です。
- iam:PassRole 権限セクションは、**role_based_auth** の場合にのみ必要です。
- 要件と環境に基づいて、フルアクセスではなく特定のリソースレベルの権限を追加できます。詳細については、AWSドキュメントのDemystifying EC2 Resource-Level Permissions および Access management for AWS resources を参照してください。

ホスト接続での権限の検証

ホスト接続で権限を検証し、MCSマシンカタログの作成と管理に関連するタスクを実行できます。この実装により、VMの作成、削除、更新、VMの電源管理、EBS暗号化など、さまざまなシナリオで必要な不足している権限を事前に特定できるため、重要な時期にブロックされるのを回避できます。

PowerShellコマンド `Test-HypHypervisorConnection` を使用して、ホスト接続の権限を検証できます。コマンドの結果はリストとして取得され、リスト内の各項目は3つのセクションに分かれています。

- カテゴリ: ユーザーがMCSマシンカタログを作成および管理するために実行できるアクションまたはタスク。
- 修正措置: 管理者がユーザーの不足している権限の不一致を解決するために実行する必要がある手順。
- 不足している権限: カテゴリの不足している権限のリスト。

権限を検証するには、次の手順を実行します。

1. AWSへのホスト接続を作成します。
2. Delivery Controller™ホストからPowerShellウィンドウを開きます。

3. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
4. 権限を検索するために必要な権限があるかどうかを確認するには、次のコマンドを実行します。

```
Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\AWSCon"
```

5. 権限を検索するために必要な不足している権限を追加した後、以下のコマンドを実行して、次のカテゴリの権限があるかどうかを確認します。

   - 作成 更新 削除
   - 電源管理
   - EBS暗号化

```
Test-HypHypervisorConnection -LiteralPath "XDHyp:
\Connections\AWSCon" [-SecurePassword -Password] "password" -UserName
"" -CustomProperties ""
```

権限の追加に関する詳細については、「IAM権限の設定」を参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- AWS固有の情報については、AWSカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

XenServer®への接続

「接続とリソースの作成および管理」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections.html)では、接続を作成するウィザードについて説明します。以下の情報は、XenServer仮想化環境に固有の詳細を扱っています。

> **注:**

> XenServerへの接続を作成する前に、まず、XenServerアカウントをリソースの場所として設定を完了する必要があります。XenServer仮想化環境を参照してください。

XenServerへの接続を作成する

XenServer（旧Citrix Hypervisor™）への接続を作成する場合、VM Power Adminまたはそれ以上のレベルのユーザーの資格情報を指定する必要があります。

Citrixでは、XenServerとの通信を保護するためにHTTPSを使用することを推奨しています。HTTPSを使用するには、XenServerにインストールされているデフォルトの SSL証明書を置き換える必要があります。

XenServerサーバーで高可用性が有効になっている場合、それを構成できます。Citrix Virtual Apps and Desktopsのバージョン2507 LTSRより前のバージョンでは、プール内のすべてのサーバーにワイルドカード証明書をインストールすることはできません。各サーバーに個別の証明書が必要です。

XenServerがvGPUをサポートしている場合、GPUの種類とグループを選択するか、パススルーすることができます。選択した項目に専用のGPUリソースがあるかどうかは、表示で示されます。

一つ以上のXenServerホストで一時データストレージにローカルストレージを使用する場合、プール内の各ストレージの場所が一意の名前を持つようにしてください。（XenCenter®で名前を変更するには、ストレージを右クリックして名前プロパティを編集します。）

Citrix Provisioning（旧Provisioning Services）およびMachine Creation Services™（MCS）を使用して、以下をプロビジョニングできます。

- サポートされているデスクトップまたはサーバーOS VM用のレガシーBIOS。
- Secure Bootを含む、サポートされているデスクトップまたはサーバーOS VM用のUEFI。

> **注:**
>
> MCSを構成する際には、プールオペレーター以上の権限が必要です。

XenServer接続にIntelliCache™を使用する

IntelliCacheを使用すると、共有ストレージとローカルストレージの組み合わせを使用できるため、ホスト型VDI展開の費用対効果が高まります。これにより、パフォーマンスが向上し、ネットワークトラフィックが削減されます。ローカルストレージは共有ストレージからマスターイメージをキャッシュするため、共有ストレージへの読み取り回数が減少します。共有デスクトップの場

合、差分ディスクへの書き込みは、共有ストレージではなくホスト上のローカルストレージに書き込まれます。

- IntelliCacheを使用する場合、共有ストレージはNFSである必要があります。
- Citrixでは、可能な限り最速のデータ転送を確保するために、高性能なローカルストレージデバイスを使用することを推奨しています。

IntelliCacheを使用するには、この製品とXenServerの両方で有効にする必要があります。

- XenServerをインストールするときは、**［シンプロビジョニングを有効にする（仮想デスクトップ向けに最適化されたストレージ）］**を選択します。Citrixは、IntelliCacheが有効なサーバーと無効なサーバーが混在するサーバープールをサポートしていません。詳しくは、XenServerのドキュメントを参照してください。
- Citrix Virtual Apps and Desktops™では、IntelliCacheはデフォルトで無効になっています。この設定は、XenServer接続を作成するときにのみ変更できます。後からIntelliCacheを無効にすることはできません。XenServer接続を追加するときは、次の手順を実行します。
  - ストレージの種類として**［共有］**を選択します。
  - **［IntelliCacheを使用する］**チェックボックスをオンにします。

必要なXenServer権限

XenServerの権限はロールベース（RBAC）です。XenServerのロールベースアクセス制御（RBAC）機能を使用すると、ユーザー、ロール、および権限を割り当てて、XenServerへのアクセス権を持つユーザーと、それらのユーザーが実行できるアクションを制御できます。XenServer RBACシステムは、ユーザー（またはユーザーグループ）を定義されたロール（名前付きの権限セット）にマッピングします。ロールには、特定の操作を実行するための関連するXenServer権限があります。

詳細については、「Role-based access control」を参照してください。

権限が昇順のロール階層は次のとおりです：Read-Only → VM Operator → VM Admin → VM Power Admin → Pool Operator → Pool Admin。

次のセクションでは、各プロビジョニングタスクに必要な最小ロールをまとめます。

ホスト接続の作成

タスク	必要な最小限の役割
XenServerから取得した情報を使用してホスト接続を追加する	読み取り専用

タスク	必要な最小限の役割
ユーザーとその割り当てられた役割を表示する	読み取り専用

VMの電源管理

タスク	必要な最小限の役割
VMの電源をオンまたはオフにする	VMオペレーター

VMの作成、更新、または削除

タスク	必要な最小限の役割
既存のスナップショットスケジュールにVMを追加または削除する	VM電源管理者
スナップショットスケジュールを追加、変更、削除する	プールオペレーター
マスターイメージを公開する	プールオペレーター（スイッチポートロックが必要）
マシンカタログを作成する	プールオペレーター：スイッチポートロックが必要
VMを追加または削除する（GPU対応VMではないもの）	VM管理者
VMを追加または削除する（GPU対応VM）	プールオペレーター
仮想ディスクまたはCDデバイスを追加、削除、または構成する	VM管理者
タグを管理する	VMオペレーター

RBACの役割と権限の詳細については、RBACの役割と権限を参照してください。

スイッチポートロックの詳細については、スイッチポートロックの使用を参照してください。

次のステップ

- 初期展開プロセス中の場合は、マシンカタログの作成を参照してください。

- XenServer固有の情報については、XenServerカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

Google Cloud環境への接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明します。以下の情報は、Google Cloud環境に固有の詳細を扱っています。

> **注:**
>
> Google Cloud環境への接続を作成する前に、まずGoogle Cloudアカウントをリソースの場所として設定する必要があります。「Google Cloud環境」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/install-prepare/gcp.html)を参照してください。

接続の追加

「接続とリソースの作成」(/ja-jp/citrix-virtual-apps-desktops/2407/manage-deployment/connections.html)のガイダンスに従ってください。以下の説明では、ホスティング接続の設定について説明します。

1. **管理 > 構成**から、左側のペインで**ホスティング**を選択します。
2. アクションバーで**「接続とリソースの追加」**を選択します。
3. **接続**ページで、**新しい接続の作成**と**Citrix Provisioning™ツール**を選択し、**次へ**を選択します。
    - **接続の種類**。メニューから**Google Cloud**を選択します。
    - **接続名**。接続の名前を入力します。
4. **地域**ページで、メニューからプロジェクト名を選択し、使用するリソースを含む地域を選択して、**次へ**を選択します。
5. **ネットワーク**ページで、リソースの名前を入力し、メニューから仮想ネットワークを選択し、サブセットを選択して、**次へ**を選択します。リソース名は、地域とネットワークの組み合わせを識別するのに役立ちます。名前に*(Shared)*サフィックスが付加された仮想ネットワーク

は、共有VPCを表します。共有VPCのサブネットレベルのIAMロールを構成した場合、共有VPCの特定のサブネットのみがサブネットリストに表示されます。

> **注:**
>
> - リソース名には1～64文字を含めることができ、空白のみ、または文字`\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' )`を含めることはできません。

6. 「**概要**」ページで情報を確認し、「**完了**」を選択して「**接続とリソースの追加**」ウィンドウを終了します。

接続とリソースを作成すると、作成した接続とリソースが一覧表示されます。接続を構成するには、接続を選択し、アクションバーで該当するオプションを選択します。

同様に、接続の下に作成されたリソースを削除、名前変更、またはテストできます。これを行うには、接続の下のリソースを選択し、アクションバーで該当するオプションを選択します。

サービスエンドポイントのURL

次のURLにアクセスできる必要があります。

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`
- `https://compute.googleapis.com`
- `https://storage.googleapis.com`
- `https://cloudbuild.googleapis.com`

Google Cloudプロジェクト

Google Cloudプロジェクトには基本的に2つのタイプがあります。

- プロビジョニングプロジェクト: この場合、現在の管理者アカウントがプロジェクト内のプロビジョニングされたマシンを所有します。このプロジェクトはローカルプロジェクトとも呼ばれます。
- 共有VPCプロジェクト: プロビジョニングプロジェクトで作成されたマシンが、共有VPCプロジェクトのVPCを使用するプロジェクト。プロビジョニングプロジェクトに使用される管理者アカウントは、このプロジェクトで限られた権限、具体的にはVPCを使用する権限のみを持ちます。

GCP管理トラフィックのセキュアな環境を作成する

Google Cloudプロジェクトへのプライベートアクセスを許可できます。この実装により、機密データを処理するためのセキュリティが強化されます。これを実現するには、次のいずれかを実行できます。

- Cloud Build サービスアカウントの VPC サービスコントロールの以下のイングレスルールを含めます。この手順を実行する場合は、GCP マネージドトラフィックのセキュアな環境を作成するための以下の手順に従わないでください。

```
Ingress Rule 1

From:

Identities:

<ProjectID>@cloudbuild.gserviceaccount.com

Source > All sources allowed

To:

Projects =

All projects

Services =

Service name: All services
```

- プライベートワーカープールを使用している場合は、`CustomProperties`に`UsePrivateWorkerPool`を追加します。プライベートワーカープールの詳細については、プライベートプール概要を参照してください。

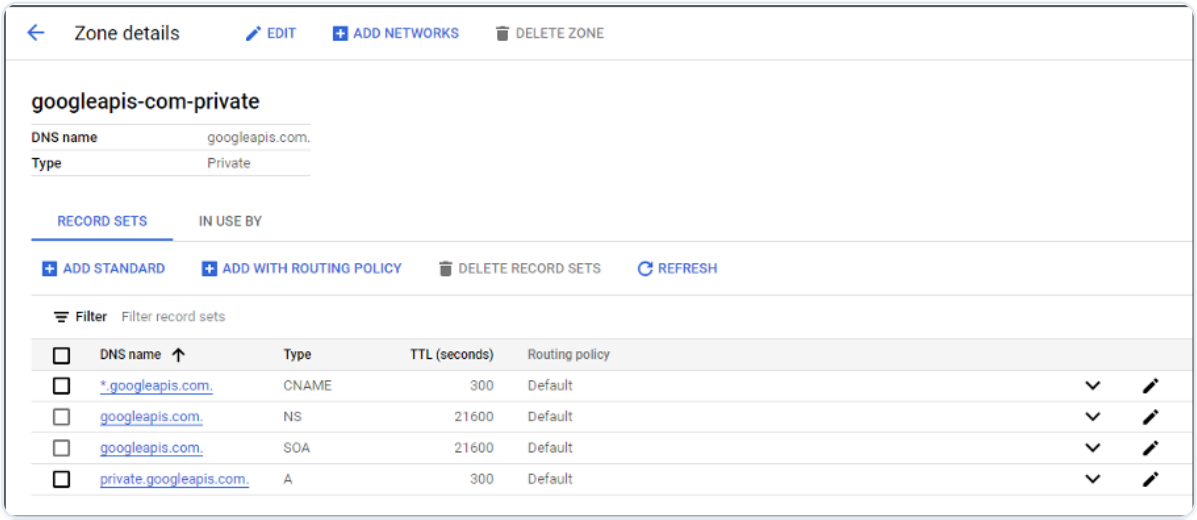
GCP管理トラフィックのセキュアな環境を作成するための要件

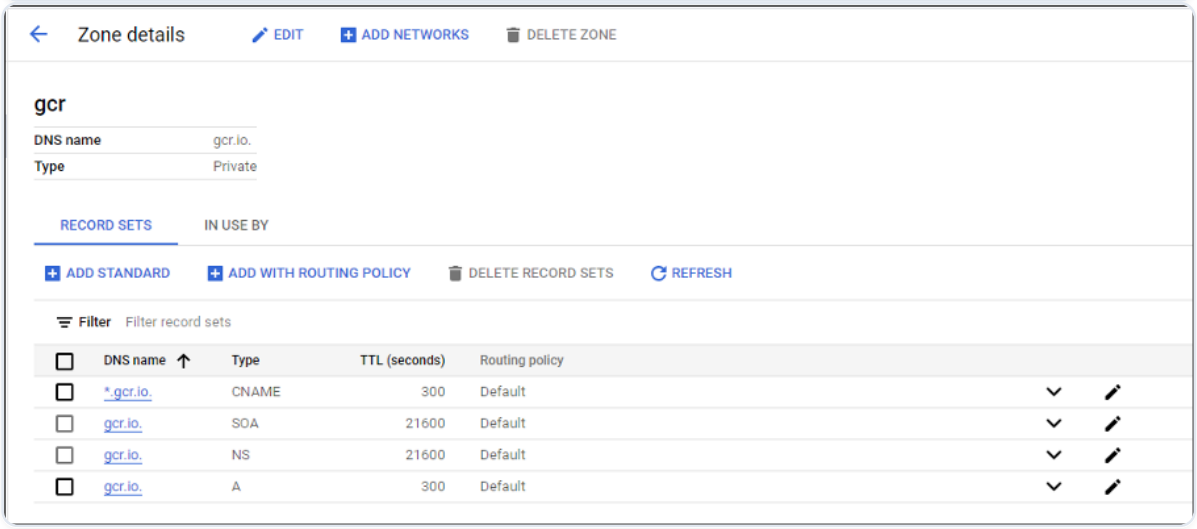
GCP管理トラフィックのセキュアな環境を作成するための要件は次のとおりです。

- カスタムプロパティを更新する際は、ホスティング接続がメンテナンスモードであることを確認してください。
- プライベートワーカープールを使用するには、以下の変更が必要です。
  - Citrix Cloud™ サービスアカウントには、以下の IAM ロールを追加します。

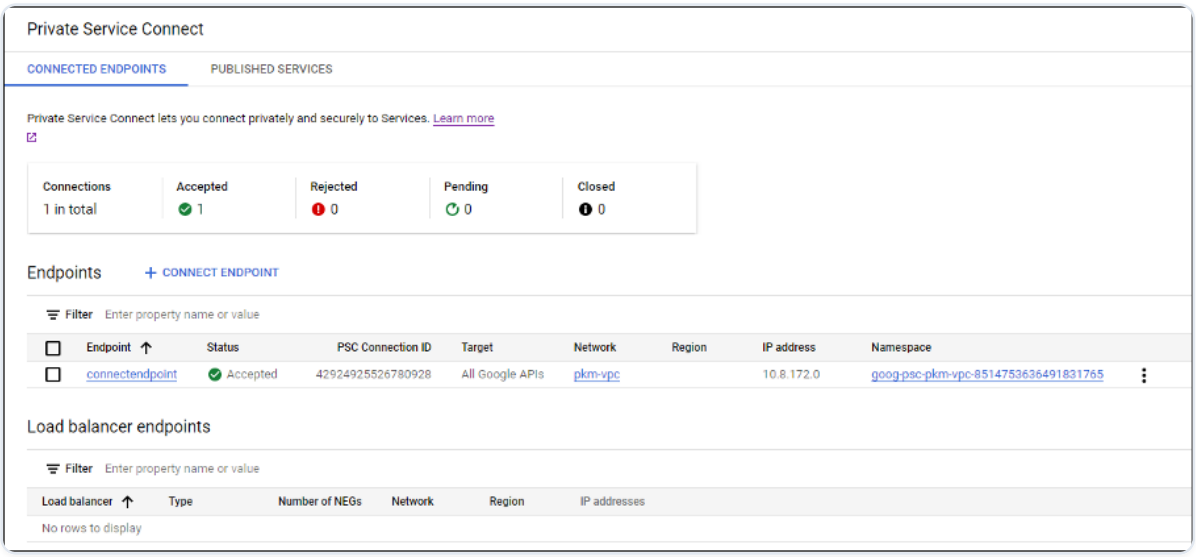
- Cloud Build サービスアカウント
- Compute Instance 管理者
- サービスアカウントユーザー
- サービスアカウントトークン作成者
- Cloud Build WorkerPool 所有者

- ホスティング接続の作成に使用するのと同じプロジェクトに、Citrix Cloud サービスアカウントを作成します。
- DNS 構成で説明されているように、`private.googleapis.com` と `gcr.io` の DNS ゾーンを設定します。

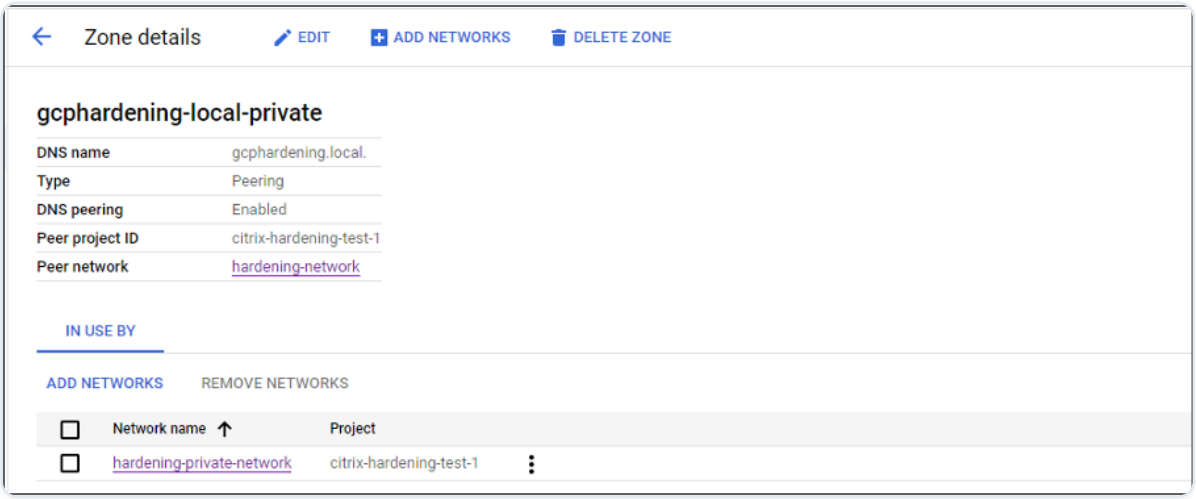




- プライベートネットワークアドレス変換 (NAT) を設定するか、プライベートサービス接続を使用します。詳細については、「エンドポイントを介したGoogle APIへのアクセス」を参照してください。



- ピアリングされたVPCを使用している場合は、ピアリングされたVPCへのCloud DNSゾーンピアリングを作成します。詳細については、「ピアリングゾーンの作成」を参照してください。



- VPCサービスコントロールで、APIとVMがインターネットと通信できるようにエグレスルールを設定します。イングレスルールはオプションです。例：

```
Egress Rule 1

From:

Identities:ANY_IDENTITY

To:

Projects =

All projects
```

```
Service =

Service name: All services
```

プライベートワーカープールを有効にする

プライベートワーカープールを有効にするには、ホスト接続でカスタムプロパティを次のように設定します。

1. Delivery ControllerホストからPowerShellウィンドウを開くか、Remote PowerShell SDKを使用します。Remote PowerShell SDKの詳細については、「SDKとAPI」を参照してください。
2. 次のコマンドを実行します。
   a. `Add-PSSnapin citrix*`
   b. `cd XDHyp:\Connections\`
   c. `dir`
3. 接続から`CustomProperties`をメモ帳にコピーします。
4. プロパティ設定`<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool" Value="True"/>`を追加します。例：

```
```

<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.citrix.com/2014/xd/machinecreation">

<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool"
Value="True"/>

</CustomProperties>

```
```

5. PowerShellウィンドウで、変更されたカスタムプロパティに変数を割り当てます。例: `$customProperty = '<CustomProperties…</CustomProperties>'`。
6. `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"` を実行します。
7. `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"` を実行します。

8. `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force` を実行します。
9. 既存のホスト接続を更新するには、以下を実行します:

```
Set-Item -PassThru -Path @('XDHyp:\\Connections\\<ENTER YOUR CONNECTION
NAME HERE>') -SecurePassword $securePassword -UserName
$gcpServiceAccount -CustomProperties $customProperty
```

必要なGCP権限

このセクションには、GCP権限の完全なリストが含まれています。機能が正しく動作するように、このセクションに記載されている権限の完全なセットを使用してください。

注:

GCPは、April 29, 2024以降、Cloud Build Servicesのデフォルトの動作とサービスアカウントの使用に変更を導入しています。詳細については、Cloud Build Service Account Changeを参照してください。April 29, 2024より前にCloud Build APIが有効になっている既存のGoogleプロジェクトは、この変更の影響を受けません。ただし、April 29以降も既存のCloud Build Serviceの動作を維持したい場合は、APIを有効にする前に、制約の適用を無効にする組織ポリシーを作成または適用できます。新しい組織ポリシーを設定した場合でも、このセクションの既存の権限と、**Before Cloud Build Service Account Change**とマークされている項目に従うことができます。そうでない場合は、既存の権限と、**After Cloud Build Service Account Change**とマークされている項目に従ってください。

ホスト接続の作成

- プロビジョニングプロジェクトにおけるCitrix Cloudサービスアカウントに必要な最小限の権限:

```
compute.instanceTemplates.list

compute.instances.list

compute.networks.list

compute.projects.get

compute.regions.list
```

```
compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- Compute管理者
- クラウド データストア ユーザー

- 共有VPCプロジェクト内のCitrix Cloudサービスアカウントの共有VPCに必要な追加の権限:

```
compute.networks.list

compute.subnetworks.list

resourcemanager.projects.get
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- コンピュート ネットワーク ユーザー

VMの電源管理

電源管理のみのカタログの場合、プロビジョニングプロジェクト内のCitrix Cloudサービスアカウントに必要な最小限の権限:

```
compute.instanceTemplates.list

compute.instances.list

compute.instances.get

compute.instances.reset

compute.instances.resume

compute.instances.start

compute.instances.stop
```

```
compute.instances.suspend

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get

compute.zoneOperations.get
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- Compute 管理者
- クラウド データストア ユーザー

VMの作成、更新、または削除

- プロビジョニングプロジェクト内のCitrix Cloudサービスアカウントに必要な最小限の権限:

```
cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete
```

```
compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create
```

```
compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list
```

```
compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list

iam.serviceAccounts.actAs

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete
```

```
storage.objects.get

storage.objects.list

compute.networks.get

compute.resourcePolicies.use
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- Compute 管理者
- Storage 管理者
- Cloud Build エディター
- サービスアカウントユーザー
- クラウド データストア ユーザー

- Shared VPCプロジェクトのCitrix Cloudサービスアカウントが、Shared VPCプロジェクトのVPCとサブネットワークを使用してホスティングユニットを作成するために必要な追加の権限:

```
compute.firewalls.list

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zones.list

resourcemanager.projects.get
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- コンピュートネットワークユーザー
- クラウド データストア ユーザー

準備指示ディスクをMCSにダウンロードする際に必要な最小限の権限:

- (Cloud Buildサービスアカウントの変更前): これらの権限をプロビジョニングプロジェクトのCloud Buildサービスアカウントに割り当てます。
- (Cloud Buildサービスアカウントの変更後): これらの権限をプロビジョニングプロジェクトのCloud Computeサービスアカウントに割り当てます。

```
compute.disks.create

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.images.get

compute.images.list

compute.images.useReadOnly

compute.instances.create

compute.instances.delete

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.setLabels
```

```
compute.instances.setMetadata

compute.instances.setServiceAccount

compute.machineTypes.list

compute.networks.get

compute.networks.list

compute.projects.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zones.list

iam.serviceAccounts.actAs

logging.logEntries.create

pubsub.topics.publish

resourcemanager.projects.get

source.repos.get

source.repos.list

storage.buckets.create

storage.buckets.get

storage.buckets.list

storage.objects.create

storage.objects.delete
```

```
storage.objects.get

storage.objects.list
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- Cloud Buildサービスアカウント (Cloud Buildサービスアカウントの変更後はCloud Computeサービスアカウント)
- Compute Instance 管理者
- サービスアカウントユーザー

- 準備指示ディスクをMCSにダウンロードする際に、Google Cloud Buildサービスがプロビジョニングプロジェクトの Cloud Computeサービスアカウントに要求する最小限の権限:

```
resourcemanager.projects.get

storage.objects.create

storage.objects.get

storage.objects.list
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- コンピュートネットワークユーザー
- ストレージアカウントユーザー
- Cloud Datastore 利用者

MCSに準備指示ディスクをダウンロードする際に、共有VPCに必要とされる追加の権限:

- (Cloud Buildサービスアカウントの変更前): これらの権限をプロビジョニングプロジェクトのCloud Buildサービスアカウントに割り当てます。
- (Cloud Buildサービスアカウントの変更後): これらの権限をプロビジョニングプロジェクトのCloud Computeサービスアカウントに割り当てます。

```
compute.firewalls.list

compute.networks.list
```

```
compute.subnetworks.list

compute.subnetworks.use

resourcemanager.projects.get
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- Compute Network 利用者
- ストレージアカウントユーザー
- Cloud Datastore 利用者

- プロビジョニングプロジェクトのCitrix CloudサービスアカウントのCloud Key Management Service (KMS) に必要となる追加の権限:

```
cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- Compute KMS 閲覧者

一般的な権限

以下は、MCSでサポートされるすべての機能について、プロビジョニングプロジェクトのCitrix Cloudサービスアカウントに対する権限です。これらの権限は、今後の最適な互換性を提供します:

```
resourcemanager.projects.get

cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list
```

```
compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get
```

```
compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.instances.update

compute.instances.updateAccessConfig

compute.instances.updateDisplayDevice

compute.instances.updateSecurity

compute.instances.updateShieldedInstanceConfig
```

```
compute.instances.updateShieldedVmConfig

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get
```

```
compute.zones.list

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list

compute.disks.list

compute.instances.setServiceAccount

compute.networks.get

compute.networks.use

compute.networks.useExternalIp

iam.serviceAccounts.actAs
```

```
compute.resourcePolicies.use
```

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html)を参照してください。
- Google Cloud Platform (GCP) 固有の情報については、「Google Cloud Platformカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create/create-machine-catalog-gcp.html)を参照してください。

詳細情報

- 接続とリソース(/ja-jp/citrix-virtual-apps-desktops/2407/manage-deployment/connections.html)
- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html)

HPE Moonshotへの接続

(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections.html)では、接続を作成するウィザードについて説明します。以下の情報は、HPE Moonshotに固有の詳細を扱います。

> **注:**

> HPE Moonshotへの接続を作成する前に、まずHPEアカウントの設定を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/install-prepare/hpe-moonshot.html)を参照してください。

接続の作成

HPE Moonshotへの接続は、次の方法で作成できます。

- ウェブスタジオ
- PowerShellコマンド

Web Studioを使用した接続の作成

1. **［接続とリソースの追加］ページで、接続の種類として［HPE Moonshot］**を選択します。
2. Moonshot iLO Chassis Managerの接続アドレスを入力します。アドレスには、IPアドレス、ホスト名、またはFQDNを使用できます。

3. シャーシの管理資格情報と、わかりやすい接続名を入力します。

次のいずれかの状況が発生すると、接続設定が停止します。

- Citrix Virtual Apps and Desktops™が、エラーのある公開CA署名証明書を受信した場合：エラーメッセージが表示されます。画面の指示に従って問題を修正してください。修正しないと、接続の作成に進むことができません。
- Citrix Virtual Apps and Desktopsが、プライベートCA署名証明書を受信した場合：警告ページが表示されます。受信したサムプリントをサーバーの証明書と比較して、証明書の有効性を確認します。有効な場合は、**［証明書を信頼する］を選択し、［OK］**をクリックして接続の作成に進みます。Citrix Virtual Apps and Desktopsは、その証明書を信頼し、将来の検証のためにサムプリントを保存します。

PowerShellコマンドを使用して接続を作成する

PowerShellコマンドを使用して接続を作成する場合、以下の情報を提供します。

- IP: HPEサーバーのIPアドレス
- ユーザー名: HPEユーザー名
- パスワード: HPEパスワード

例:

```
New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata
@{"Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false"} -Path
@("XDHyp:\Connections\$connectionName") -Persist -PluginId
"HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
$UserName -sslthumbprint $SslThumbprint New-BrokerHypervisorConnection
-HypHypervisorConnectionUid $HypervisorConnectionID
```

注:

`sslthumbprint` パラメーターは、プライベートCA署名付き証明書にのみ必要です。

証明書とサムプリントの検証

HPE Moonshotへの接続を正常に作成するには、証明書にエラーがなく、サムプリントが正しい値である必要があります。証明書とサムプリントの検証に関連するユースケースは以下のとおりです。

- パブリックCA署名付き証明書にエラーがあります。接続は正常に作成されません。エラーの詳細を確認し、問題を解決してください。
- エラーのないパブリックCA署名付き証明書。接続は正常に作成され、`SslThumbprints` の値は **Null** です。
- エラーがなく、`sslthumbprint` の値を持つプライベートCA署名付き証明書。接続は正しい `SslThumbprints` の値で正常に作成されます。
- 不正なサムプリント値を持つプライベートCA署名付き証明書。接続は正常に作成されません。
- エラーのないプライベートCA署名付き証明書。接続は正常に作成されます。接続作成時、`SSlThumbprints` は **Null** です。`SSlThumbprints` の値は、サイトサービスによって値に更新されます。

接続の管理

このセクションでは、接続を管理する方法について詳しく説明します。

- Web Studioを使用して証明書の問題を修正する
- PowerShellコマンドを使用してサムプリント値を更新する

証明書の問題を修正する

証明書の問題が発生すると、Citrix Virtual Apps and Desktops は HPE Moonshot 接続をブロックし、関連する HPE Moonshot ノードでのワークロードの配信と管理を妨げます。**ホスト接続**リストの接続の横にエラーアイコンが表示されます。具体的な問題と解決策については、次の表を参照してください。

問題	解決策
公開 CA 署名証明書で証明書エラーが発生する	接続をクリックし、**トラブルシューティング**タブを選択します。エラーの詳細を表示し、問題を解決します。
受信した証明書がプライベート CA 署名であるか、期限切れである。	ホスト接続を編集して、証明書のサムプリントを更新します。詳細な手順は次のとおりです:

問題	解決策	
	1. 接続を選択し、**接続の編集**をクリックします。 2. 「**接続プロパティ**」ページで、「**設定の編集**」をクリックします。 3. HPE Moonshotシャーシに接続するためのパスワードを入力し、「**保存**」をクリックします。 4. 表示される「**警告**」ページで、受信したサムプリントをサーバーのものと比較して、証明書の有効性を確認します。 5. 同じ場合は、「**証明書を信頼する**」を選択し、「**OK**」をクリックします。	

サムプリント値の更新

接続を作成した後、`Set-Item` PowerShellコマンドを使用して接続のサムプリント値を更新できます。たとえば、次のコマンドを実行します。

1. 接続の詳細を取得します。例：

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

2. サムプリント値を更新します。例：

```
Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
Administrator -SslThumbprint xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
```

3. 更新されたサムプリント値を確認します。例：

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

注：

`Set-Item`コマンドで誤ったサムプリント値を指定すると、更新は失敗します。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html)を参照してください。
- AWS固有の情報については、「HPE Moonshotマシンカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create/create-machine-catalog-hpe-moonshot.html)を参照してください。

詳細情報

- 「接続とリソース」(/ja-jp/citrix-virtual-apps-desktops/2407/manage-deployment/connections.html)
- 「マシンカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html)

Microsoft Azure への接続

注:

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

接続とリソースの作成および管理 では、接続を作成するウィザードについて説明します。以下の情報では、Azure Resource Manager クラウド環境に固有の詳細について説明します。

注:

> Microsoft Azure への接続を作成する前に、Azure アカウントをリソースの場所として設定を完了する必要があります。Microsoft Azure Resource Manager クラウド環境 を参照してください。

サービスプリンシパルと接続の作成

接続を作成する前に、接続が Azure リソースにアクセスするために使用するサービスプリンシパルを設定する必要があります。接続は次の 2 つの方法で作成できます。

- Web Studio を使用してサービスプリンシパルと接続を同時に作成する
- 以前に作成したサービスプリンシパルを使用して接続を作成する

このセクションでは、次のタスクを完了する方法について説明します。

- Web Studio を使用してサービスプリンシパルと接続を作成する
- PowerShell を使用してサービスプリンシパルを作成する
- Azure でアプリケーションシークレットを取得する
- 既存のサービスプリンシパルを使用して接続を作成する

考慮事項

- Citrix® は、共同作成者ロールを持つサービスプリンシパルの使用を推奨しています。ただし、最小限の権限のリストについては、(#minimum-permissions)セクションの「最小限の権限」を参照してください。
- 最初の接続を作成する際、Azure は必要な権限を付与するよう求めます。今後の接続では引き続き認証が必要ですが、Azure は以前の同意を記憶しているため、プロンプトは再度表示されません。
- 認証に使用されるアカウントは、Azure RBAC を使用してサブスクリプションでロールを割り当てる権限を持っている必要があります。例として、サブスクリプションの所有者、ロールベースのアクセス制御管理者、またはユーザーアクセス管理者などがあります。
- 認証に使用されるアカウントは、サブスクリプションのディレクトリのメンバーである必要があります。注意すべきアカウントには、「職場または学校」と「個人用 Microsoft アカウント」の2種類があります。詳細については、CTX219211を参照してください。
- 既存の Microsoft アカウントをサブスクリプションのディレクトリのメンバーとして追加して使用することはできますが、ユーザーが以前にディレクトリのリソースのいずれかへのゲストアクセスを許可されていた場合、問題が発生する可能性があります。この場合、ディレクトリ

内に必要な権限を付与しないプレースホルダーエントリが存在し、エラーが返されることがあります。

これを修正するには、ディレクトリからリソースを削除し、明示的に再度追加します。ただし、このオプションは、アカウントがアクセスできる他のリソースに意図しない影響を与える可能性があるため、慎重に実行してください。

- 特定のアカウントが実際にはメンバーであるにもかかわらず、ディレクトリゲストとして検出されるという既知の問題があります。このような構成は、通常、古くから確立されたディレクトリアカウントで発生します。回避策：ディレクトリにアカウントを追加し、適切なメンバーシップ値を取得させます。
- リソースグループは単にリソースのコンテナであり、自身のリージョン以外のリージョンからのリソースを含むことができます。これは、リソースグループのリージョンに表示されているリソースが利用可能であると期待する場合、混乱を招く可能性があります。
- 必要な数のマシンをホストするのに十分な大きさのネットワークとサブネットがあることを確認してください。これにはある程度の先見性が必要ですが、Microsoft はアドレス空間の容量に関するガイダンスを提供し、適切な値を指定するのに役立ちます。

Web Studio を使用してサービスプリンシパルと接続を作成する

> **重要:**
>
> この機能は、Azure China サブスクリプションではまだ利用できません。

> Web Studio を使用すると、単一のワークフローでサービスプリンシパルと接続の両方を作成できます。サービスプリンシパルは、接続に Azure リソースへのアクセスを許可します。サービスプリンシパルを作成するために Azure に認証すると、アプリケーションが Azure に登録されます。登録されたアプリケーションには、秘密鍵 (クライアントシークレットまたはアプリケーションシークレットと呼ばれます) が作成されます。登録されたアプリケーション (この場合は接続) は、クライアントシークレットを使用して Azure AD に認証します。

開始する前に、以下の前提条件を満たしていることを確認してください。

- サブスクリプションのAzure Active Directoryテナントにユーザーアカウントがあること。
- 認証に使用されるアカウントは、Azure RBACを使用してサブスクリプションでロールを割り当てる権限を持っている必要があります。例として、サブスクリプションの所有者、ロールベースのアクセス制御管理者、またはユーザーアクセス管理者などです。

- 認証のために、グローバル管理者、アプリケーション管理者、またはアプリケーション開発者の権限を持っていること。これらの権限は、ホスト接続の作成後に取り消すことができます。ロールの詳細については、Azure AD の組み込みロールを参照してください。

サービスプリンシパルと接続を同時に作成するには、**接続とリソースの追加**ウィザードを使用します。

1. **接続**ページで、**新しい接続の作成**、**Microsoft Azure**接続タイプ、およびAzure環境を選択します。
2. 仮想マシンの作成に使用するツールを選択し、**次へ**を選択します。
3. **接続の詳細**ページで、AzureサブスクリプションIDと接続名を入力します。サブスクリプションIDを入力すると、**新規作成**ボタンが有効になります。

   > **注:**
   >
   > 接続名には 1～64 文字を含めることができ、空白のみ、または文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。

4. を選択し、Azure Active Directory アカウントのユーザー名とパスワードを入力します。
5. **サインイン**を選択します。
6. Citrix Virtual Apps and Desktops™に一覧表示された権限を付与するには、**同意する**を選択します。Citrix Virtual Apps and Desktopsは、指定されたユーザーに代わってAzureリソースを管理できるサービスプリンシパルを作成します。
7. **同意する**を選択すると、ウィザードの**接続**ページに戻ります。

   > **注:**
   >
   > Azureへの認証が成功すると、**新規作成**ボタンと**既存を使用**ボタンは表示されなくなります。緑色のチェックマークとともに**接続成功**というテキストが表示され、Azureサブスクリプションへの接続が成功したことを示します。

8. 「**Connection Details**」ページで、「**Next**」を選択します。

   > 「**注：**」:

> Azureへの認証が正常に完了し、必要な権限の付与に同意するまで、次のページに進むことはできません。

9. 接続のリソースを構成します。リソースは、リージョンとネットワークで構成されます。
   - 「**地域**」ページで、地域を選択します。
   - 「**ネットワーク**」ページで、次の操作を行います。
     - リージョンとネットワークの組み合わせを識別しやすくするために、1〜64文字のリソース名を入力します。リソース名には、空白のみを含めることや、文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。
     - 仮想ネットワーク/リソースグループのペアを選択します。（同じ名前の仮想ネットワークが複数ある場合、ネットワーク名とリソースグループをペアにすることで、一意の組み合わせが提供されます。）前のページで選択したリージョンに仮想ネットワークがない場合は、そのページに戻り、仮想ネットワークがあるリージョンを選択してください。
10. 「**概要**」ページで、設定の概要を確認し、「**完了**」を選択してセットアップを完了します。

アプリケーションIDを表示する

接続を作成した後、その接続がAzureリソースへのアクセスに使用するアプリケーションIDを表示できます。

「**Add Connection and Resources**」リストで、接続を選択して詳細を表示します。「**Details**」タブにはアプリケーションIDが表示されます。

PowerShellを使用してサービスプリンシパルを作成する

PowerShellを使用してサービスプリンシパルを作成するには、Azure Resource Managerサブスクリプションに接続し、以下のセクションで提供されているPowerShellコマンドレットを使用します。

次の項目が準備されていることを確認してください。

- **SubscriptionId:** VDA をプロビジョニングするサブスクリプションの Azure Resource Manager `SubscriptionID`。
- **ActiveDirectoryID**: Azure AD に登録したアプリケーションのテナント ID。
- **ApplicationName:** Azure AD で作成するアプリケーションの名前。

詳細な手順は次のとおりです。

Azure Resource Manager サブスクリプションに接続します。

```
`Connect-AzAccount`
```

1. サービスプリンシパルを作成する Azure Resource Manager サブスクリプションを選択します。

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-AzSubscription
   ```

2. AD テナントにアプリケーションを作成します。

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

3. サービスプリンシパルを作成します。

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

4. サービスプリンシパルにロールを割り当てます。

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

5. PowerShell コンソールの出力ウィンドウから、ApplicationId をメモします。ホスト接続を作成するときに、その ID を指定します。

Azure でアプリケーションシークレットを取得する

既存のサービスプリンシパルを使用して接続を作成するには、まず Azure portal でサービスプリンシパルのアプリケーションIDとシークレットを取得する必要があります。

詳細な手順は次のとおりです。

1. Web StudioまたはPowerShellを使用して、**アプリケーションID**を取得します。
2. Azureポータルにサインインします。
3. Azure で、「**Azure Active Directory**」を選択します。
4. Azure AD の「**App registrations**」から、アプリケーションを選択します。
5. **証明書とシークレット**に移動します。
6. **クライアントシークレット**をクリックします。

既存のサービスプリンシパルを使用して接続を作成する

サービスプリンシパルが既にある場合は、それを使用してWeb Studioで接続を作成できます。

次の項目を準備してください。

- SubscriptionId
- ActiveDirectoryID (テナントID)
- アプリケーションID
- アプリケーションシークレット

  詳細については、「アプリケーションシークレットの取得」を参照してください。
- シークレットの有効期限

詳細な手順は次のとおりです。

接続とリソースの追加ウィザードで、次の手順を実行します。

1. **接続**ページで、**新しい接続の作成**、**Microsoft Azure**接続タイプ、およびAzure環境を選択します。
2. 仮想マシンを作成するために使用するツールを選択し、**次へ**を選択します。
3. 「**接続の詳細**」ページで、Azure サブスクリプション ID と接続の名前を入力します。

   > **注:**
   >
   > 接続名には 1〜64 文字を含めることができ、空白のみ、または文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。

4. **既存のものを使用**を選択します。**既存のサービスプリンシパルの詳細**ウィンドウで、既存のサービスプリンシパルに対して次の設定を入力します。詳細を入力すると、**保存**ボタンが有効になります。**保存**を選択します。有効な詳細情報が提供されるまで、このページから先に進むことはできません。

   - **サブスクリプションID**。AzureサブスクリプションIDを入力します。サブスクリプションIDを取得するには、Azureポータルにサインインし、**サブスクリプション > 概要**に移動します。
   - **Active Directory ID** (テナント ID)。Azure AD に登録したアプリケーションのディレクトリ (テナント) ID を入力します。
   - **アプリケーション ID**。Azure AD に登録したアプリケーションのアプリケーション (クライアント) ID を入力します。
   - **アプリケーションシークレット**。シークレットキー (クライアントシークレット) を作成します。登録済みアプリケーションは、このキーを使用して Azure AD に対して認証を行いま

す。セキュリティ上の理由から、キーを定期的に変更することをお勧めします。キーは後で取得できないため、必ず保存してください。

- **シークレットの有効期限**。アプリケーションシークレットの有効期限が切れる日付を入力します。シークレットキーの有効期限が切れる 14 日前から、「**ホスティング**」ノードの特定のホスト接続に警告アイコンが表示されます。ただし、シークレットキーの有効期限が切れると、エラーが発生します。

  > **注:**
  >
  > セキュリティ上の理由から、有効期限は現在から2年を超えることはできません。

- **認証 URL**。このフィールドは自動的に入力され、編集できません。
- **管理 URL**。このフィールドは自動的に入力され、編集できません。
- **ストレージサフィックス**。このフィールドは自動的に入力され、編集できません。

  AzureでMCSカタログを作成するには、以下のエンドポイントへのアクセスが必要です。これらのエンドポイントへのアクセスにより、ネットワークとAzureポータルおよびそのサービス間の接続が最適化されます。

  - 認証URL: `<https://login.microsoftonline.com/>`
  - 管理URL: `<https://management.azure.com/>`。これはAzure Resource ManagerプロバイダーAPIのリクエストURLです。管理のエンドポイントは環境によって異なります。たとえば、Azure Globalの場合は`<https://management.azure.com/>`、Azure US Governmentの場合は`<https://management.usgovcloudapi.net/>`です。
  - ストレージサフィックス: `<https://*.core.windows.net./>`。これはストレージサフィックスのワイルドカード文字(*)です。例: `https://demo.table.core.windows.net/`。

5. **保存**を選択した後、**接続の詳細**ページに戻ります。次のページに進むには、**次へ**を選択します。
6. 接続のリソースを構成します。リソースはリージョンとネットワークで構成されます。

   - **リージョン**ページで、リージョンを選択します。
   - **ネットワーク**ページで、以下を実行します。

- リージョンとネットワークの組み合わせを識別しやすくするため、1〜64文字のリソース名を入力します。リソース名には、空白のみを含めることや、文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。
- 仮想ネットワーク/リソースグループのペアを選択します。（同じ名前の仮想ネットワークが複数ある場合、ネットワーク名とリソースグループをペアにすることで一意の組み合わせが提供されます。）前のページで選択したリージョンに仮想ネットワークがない場合は、そのページに戻り、仮想ネットワークがあるリージョンを選択してください。

7. 「**概要**」ページで、設定の概要を確認し、「**完了**」を選択してセットアップを完了します。

サービスプリンシパルと接続を管理する

このセクションでは、サービスプリンシパルと接続を管理する方法について詳しく説明します。

- Azureの調整設定を構成する
- Azureでイメージ共有を有効にする
- Web Studioを使用して共有テナントを接続に追加する
- PowerShellを使用してイメージ共有を実装する
- アプリケーションシークレットとシークレットの有効期限を管理する

Azureの調整設定を構成する

Azure Resource Managerは、プロバイダーの特定のニーズに合わせて定義された制限に基づいてトラフィックをルーティングし、サブスクリプションとテナントのリクエストを調整します。詳細については、MicrosoftサイトのResource Managerリクエストの調整を参照してください。サブスクリプションとテナントには制限があり、多数のマシンを管理すると問題が発生する可能性があります。たとえば、多数のマシンを含むサブスクリプションでは、電源操作に関連するパフォーマンスの問題が発生する可能性があります。

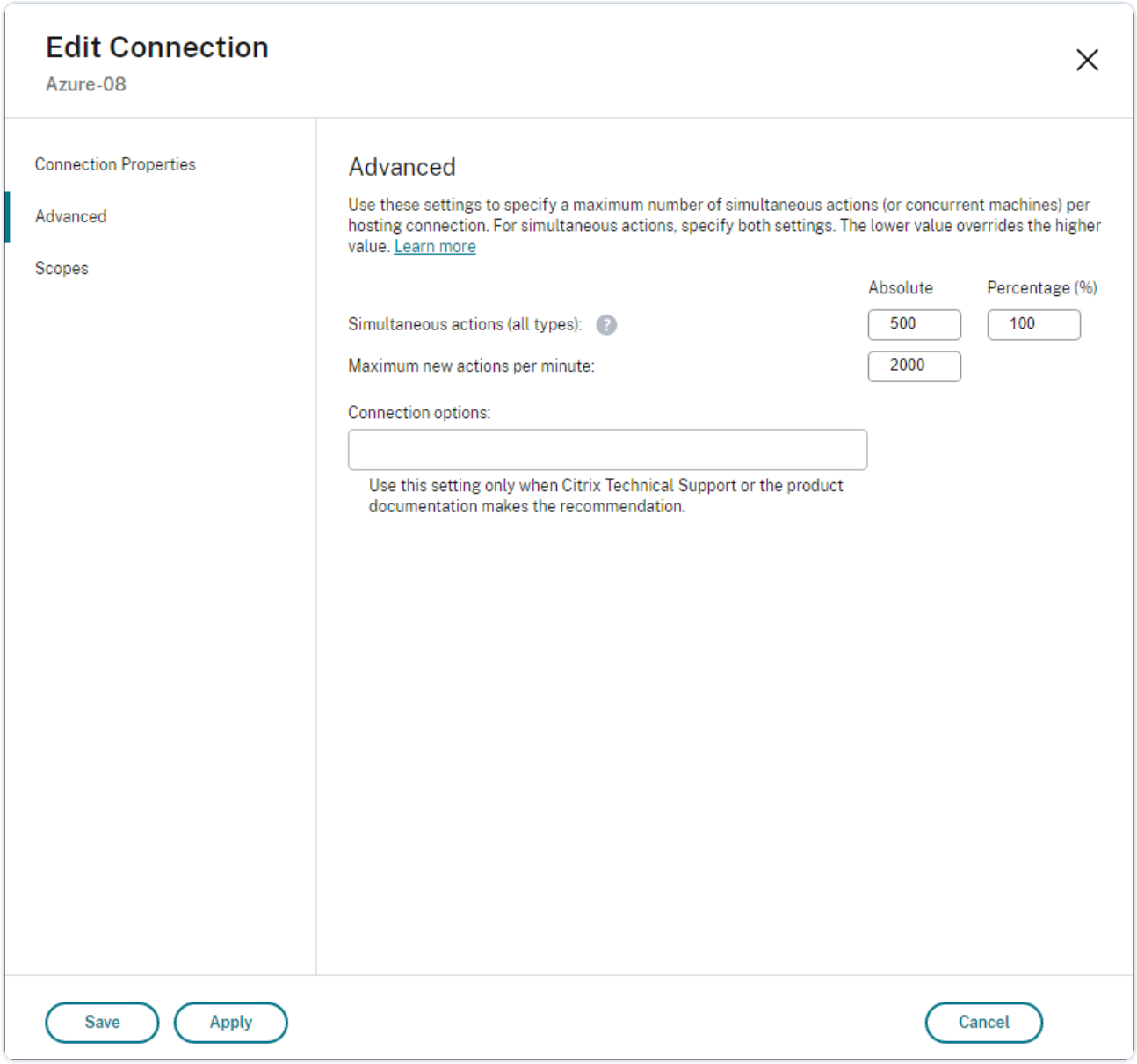
> **ヒント:**
>
> 詳細については、「Machine Creation ServicesによるAzureパフォーマンスの向上」を参照してください。
>
> これらの問題を軽減するために、MCSの内部調整を削除して、Azureから利用可能なリクエストクォータをより多く使用できます。

大規模なサブスクリプション（たとえば、1,000台のVMを含むサブスクリプション）でVMの電源をオンまたはオフにする場合、次の最適な設定をお勧めします。

- 絶対同時操作数: 500
- 1分あたりの最大新規操作数: 2000
- 操作の最大同時実行数: 500

Web Studio を使用して、特定の Azure 接続の Azure 操作を構成します。

1. Web Studioで、左側のペインで**「ホスティング」**を選択します。
2. 接続を選択します。
3. ウィザードで、 を選択します。
4. ページで、構成オプションを使用して、同時アクションの数、1 分あたりの最大新規アクション数、および追加の接続オプションを指定します。



MCS はデフォルトで最大 500 の同時操作をサポートします。または、Remote PowerShell SDK を使用して、同時操作の最大数を設定することもできます。

PowerShellプロパティ `MaximumConcurrentProvisioningOperations` を使用して、Azureプロビジョニング操作の最大同時実行数を指定します。このプロパティを使用する際は、次の点を考慮してください。

- `MaximumConcurrentProvisioningOperations` のデフォルト値は 500 です。
- PowerShell コマンド `Set-item` を使用して、`MaximumConcurrentProvisioningOperations` パラメーターを構成します。

Azureでのイメージ共有を有効にする

マシンカタログを作成または更新する際、異なるAzureテナントおよびサブスクリプション（Azure Compute Galleryを介して共有）から共有イメージを選択できます。テナント内またはテナント間でイメージ共有を有効にするには、Azureで必要な設定を行う必要があります。

- テナント内でのイメージ共有（サブスクリプション間）
- テナント間でのイメージ共有

テナント内でのイメージ共有（サブスクリプション間）

別のサブスクリプションに属するAzure Compute Galleryのイメージを選択するには、そのサブスクリプションのサービスプリンシパル (SPN) とイメージを共有する必要があります。

たとえば、Studioで次のように構成されているサービスプリンシパル (SPN 1) がある場合：

サービスプリンシパル: SPN 1

サブスクリプション: subscription 1

テナント: tenant 1

イメージは別のサブスクリプションにあり、Studio では次のように構成されています。

サブスクリプション: subscription 2

テナント: tenant 1

subscription 2 のイメージを subscription 1 (SPN 1) と共有したい場合は、subscription 2 に移動し、リソースグループを SPN1 と共有します。

イメージは、Azure ロールベースのアクセス制御 (RBAC) を使用して別のSPNと共有する必要があります。Azure RBACは、Azureリソースへのアクセスを管理するために使用される承認システムです。Azure RBACの詳細については、Microsoftドキュメント「Azure ロールベースのアクセス制御 (Azure RBAC) とは」を参照してください。アクセスを許可するには、リソースグループスコープで共同作成者ロールを持つサービスプリンシパルにロールを割り当てます。Azureロールを割り当てるには、ユーザーアクセス管理者や所有者などの `Microsoft.Authorization/roleAssignments/write` 権限が必要です。別のSPNとイメージを共有する方法の詳細については、Microsoftドキュメント「Azure portal を使用して Azure ロールを割り当てる」を参照してください。

PowerShell コマンドを使用して別のサブスクリプションからイメージを選択する方法については、「別のサブスクリプションからイメージを選択する」を参照してください。

テナント間で画像を共有する

Azure Compute Gallery を使用してテナント間でイメージを共有するには、アプリケーション登録を作成します。

例えば、2つのテナント（テナント1とテナント2）があり、テナント1とイメージギャラリーを共有したい場合：

1. テナント1のアプリケーション登録を作成します。詳細については、「アプリ登録の作成」を参照してください。
2. ブラウザを使用してサインインを要求することで、テナント2にアプリケーションへのアクセスを許可します。`Tenant2 ID` をテナント1のテナントIDに置き換えます。`Application (client) ID` を作成したアプリケーション登録のアプリケーションIDに置き換えます。置換が完了したら、URLをブラウザに貼り付け、サインインプロンプトに従ってテナント2にサインインします。例:

   ```
   https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
   client_id=<Application (client)
   ID>&response_type=code&redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
   ```

   詳細については、「テナント2へのアクセスを許可する」を参照してください。
3. アプリケーションにテナント2のリソースグループへのアクセスを許可します。テナント2としてサインインし、ギャラリーイメージがあるリソースグループにアプリケーション登録のアクセスを許可します。詳細については、「テナント間の要求を認証する」を参照してください。

PowerShell コマンドを使用して別のテナントのイメージからカタログを作成するには:

1. 共有テナントIDでホスティング接続のカスタムプロパティを更新する。
2. 別のテナントからイメージを選択する。

Web Studio を使用して共有テナントを接続に追加する

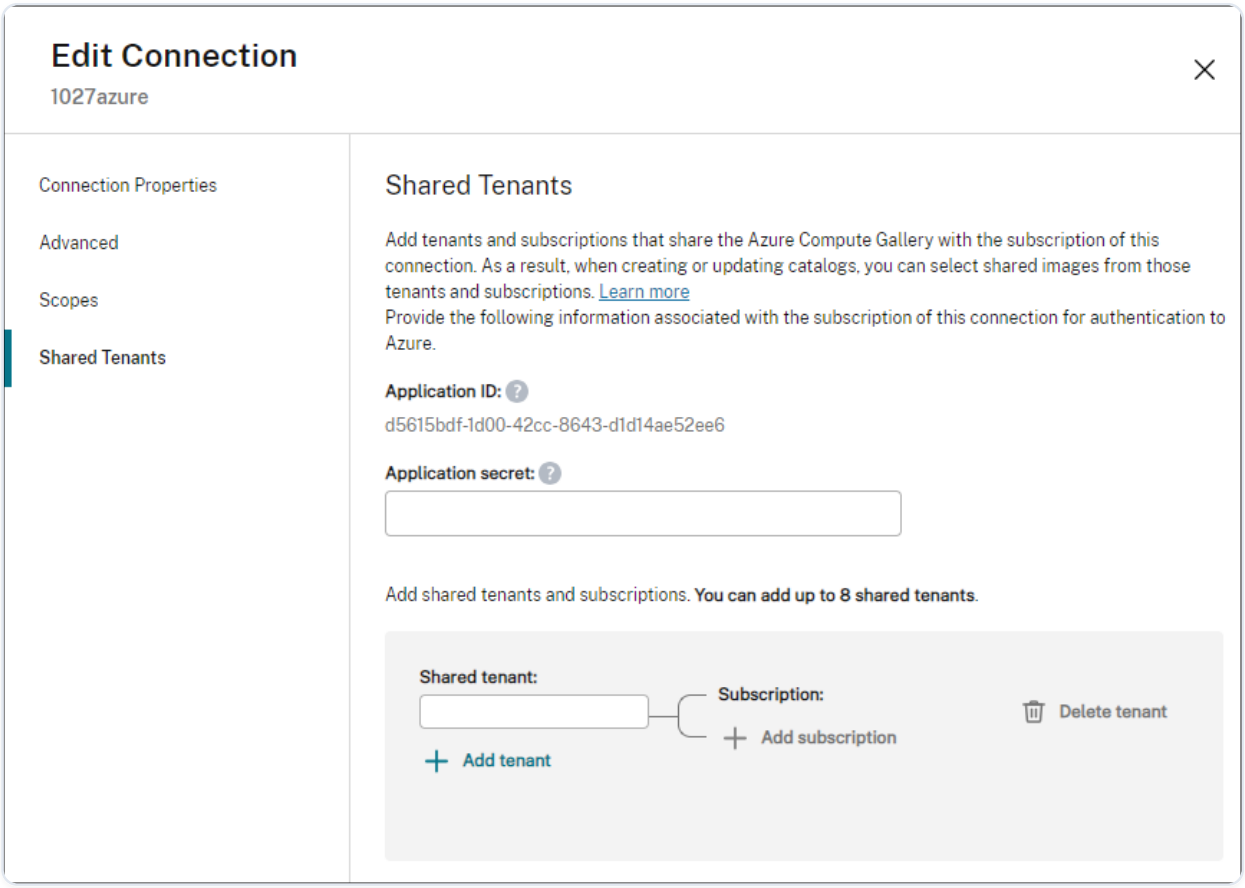
Web Studioでマシンカタログを作成または更新する際、異なるAzureテナントおよびサブスクリプション（Azure Compute Galleryを通じて共有される）から共有イメージを選択できます。この機能では、関連するホスト接続の共有テナントおよびサブスクリプション情報を提供する必要があります。

> **注:**
>
> テナント間でイメージ共有を有効にするために、Azure で必要な設定が構成されていることを確認してください。詳細については、「テナント間で画像を共有する」を参照してください。

接続に対して以下の手順を完了します。

1. Web Studioで、左ペインの**「ホスティング」**を選択します。

2. 接続を選択し、アクションバーで**「接続の編集」**を選択します。



3. **共有テナント**で、次の操作を行います。

   - 接続のサブスクリプションに関連付けられているアプリケーションIDとアプリケーションシークレットを指定します。Citrix Virtual Apps and Desktopsは、この情報を使用してAzure ADに対して認証を行います。
   - 接続のサブスクリプションとAzure Compute Galleryを共有するテナントとサブスクリプションを追加します。各テナントにつき、最大8つの共有テナントと8つのサブスクリプションを追加できます。

4. 完了したら、**適用**を選択して変更を適用し、ウィンドウを開いたままにするか、**OK**を選択して変更を適用してウィンドウを閉じます。

PowerShellを使用したイメージ共有の実装

このセクションでは、PowerShellを使用してイメージを共有するプロセスについて説明します。

- 別のサブスクリプションからイメージを選択する
- 共有テナントIDでホスティング接続のカスタムプロパティを更新する
- 別のテナントからイメージを選択する

別のサブスクリプションからイメージを選択する

PowerShellコマンドを使用してMCSカタログを作成および更新するために、同じAzureテナント内の別の共有サブスクリプションに属するAzure Compute Galleryのイメージを選択できます。

1. ホスティングユニットのルートフォルダーに、Citrixは`sharedsubscription`という新しい共有サブスクリプションフォルダーを作成します。
2. テナント内のすべての共有サブスクリプションを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\sharedsubscription.folder"
```

3. 1つの共有サブスクリプションを選択し、その共有サブスクリプションのすべての共有リソースグループを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription"
```

4. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\
xyz.resourcegroup"
```

5. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\testgallery.gallery"
```

6. 1つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\sigtestdef.imagedefinition"
```

7. 次の要素を使用してMCSカタログを作成および更新します。

   - リソースグループ

- ギャラリー
- ギャラリーイメージ定義
- ギャラリーイメージバージョン

Remote PowerShell SDK を使用したカタログの作成方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>` を参照してください。

共有テナントIDを使用してホスティング接続のカスタムプロパティを更新する

`Set-Item` を使用して、共有テナントIDとサブスクリプションIDでホスティング接続のカスタムプロパティを更新します。`CustomProperties` にプロパティ `SharedTenants` を追加します。`Shared Tenants` の形式は次のとおりです。

```
[{"Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":
["7bb42f40-8d7f-4230-a920-be2781f6d5d9"]},{"Tenant":"50e83564-c4e5-4209-
b43d-815c45659564","Subscriptions":["06ab8944-6a88-47ee-
a975-43dd491a37d0"]}]
```

例:

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
Value=`"123`" />

<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
Value=`"https://management.azure.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
Value=`"https://login.microsoftonline.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`"
Value=`"core.windows.net`" />

<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`" /
>

<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`"
Value=`"`[ { 'Tenant':'123abc', 'Subscriptions':['345', '567'] } ]`"` />
```

```
</CustomProperties>"

-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "advc345"
-SecurePassword

$psd
```

注:

複数のテナントを追加できます。各テナントは複数のサブスクリプションを持つことができます。

別のテナントからイメージを選択する

PowerShellコマンドを使用して、別のAzureテナントに属するAzure Compute Galleryのイメージを選択し、MCSカタログを作成および更新できます。

1. ホスティングユニットのルートフォルダーに、Citrixは`sharedsubscription`という名前の新しい共有サブスクリプションフォルダーを作成します。
2. すべての共有サブスクリプションを一覧表示します。

   ```
   Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
   ```

3. 1つの共有サブスクリプションを選択し、その共有サブスクリプションのすべての共有リソースグループを一覧表示します。

   ```
   Get-ChildItem XDHyp:
   \HostingUnits\azres\image.folder\abc123.sharedsubscription
   ```

4. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

   ```
   Get-ChildItem XDHyp:
   \HostingUnits\azres\image.folder\abc123.sharedsubscription\
   xyz.resourcegroup
   ```

5. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery
```

6. 1つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery\hij.imagedefinition
```

7. 次の要素を使用してMCSカタログを作成および更新します。

   - リソースグループ
   - ギャラリー
   - ギャラリーイメージ定義
   - ギャラリーイメージバージョン

   Remote PowerShell SDKを使用してカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

アプリケーションシークレットとシークレットの有効期限を管理する

シークレットの有効期限が切れる前に、接続のアプリケーションシークレットを必ず変更してください。シークレットキーの有効期限が切れる14日前から、**ホスティング**ノードの特定のホスト接続に警告アイコンが表示されます。ただし、シークレットキーの有効期限が切れると、エラーが発生します。

AZURE でアプリケーションシークレットを作成する

Azure portal を介して、接続用のアプリケーションシークレットを作成できます。

1. **Azure Active Directory** を選択します。
2. Azure AD の **App registrations** から、アプリケーションを選択します。
3. **証明書とシークレット**に移動します。
4. **>** をクリックします。
5. シークレットの説明を入力し、期間を指定します。完了したら、**Add** を選択します。

> **注:**
>
> クライアントシークレットは後で取得できないため、必ず保存してください。

6. クライアントシークレットの値と有効期限をコピーします。
7. Web Studio で、対応する接続を編集し、**Application secret** および **Secret expiration date** フィールドの内容をコピーした値に置き換えます。

シークレットの有効期限を変更する

Web Studio を使用して、使用中のアプリケーションシークレットの有効期限を追加または変更できます。

> **注:**
>
> シークレットキーの有効期限が切れる14日前から、**Hosting** ノードの特定のホスト接続に警告アイコンが表示されます。

1. **接続とリソースの追加**ウィザードで、接続を右クリックし、**接続の編集**をクリックします。
2. **接続プロパティ**ページで、**シークレットの有効期限**をクリックして、使用中のアプリケーションシークレットの有効期限を追加または変更します。

必要なAzure権限

このセクションには、Azure に必要な最小限の一般的な権限が含まれています。

最小限の権限

最小限の権限は、より優れたセキュリティ制御を提供します。ただし、追加の権限を必要とする新機能は、最小限の権限のみを使用しているため失敗します。

ホスト接続の作成

Azure から取得した情報を使用して、新しいホスト接続を追加します。

```
"Microsoft.Network/virtualNetworks/read",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/disks/read",
```

```
"Microsoft.Resources/providers/read",

"Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/tenants/read"
```

VM の電源管理

マシンインスタンスの電源をオンまたはオフにします。

```
"Microsoft.Compute/virtualMachines/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Insights/diagnosticsettings/delete",

"Microsoft.Insights/diagnosticsettings/read",

"Microsoft.Insights/diagnosticsettings/write",
```

仮想マシンの作成、更新、または削除

マシンカタログを作成し、マシンの追加、削除、更新を行い、マシンカタログを削除します。

以下は、マスターイメージがマネージドディスクである場合、またはスナップショットがホスティング接続と同じリージョンにある場合に必要となる最小限の権限のリストです。

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Compute/virtualMachines/read",
```

```
"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
read",

"Microsoft.Compute/skus/read",

"Microsoft.Compute/virtualMachines/extensions/read",

"Microsoft.Compute/virtualMachines/extensions/write",

"Microsoft.Features/providers/features/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/virtualNetworks/subnets/read",
```

```
"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/locations/usages/read",
```

以下の機能については、最小限の権限に加えて、以下の追加権限が必要です。

- マスターイメージがホスティング接続と同じリージョンにあるストレージアカウント内の VHD である場合：

  ```
  "Microsoft.Storage/storageAccounts/read",

  "Microsoft.Storage/storageAccounts/listKeys/action",
  ```

- マスターイメージが共有イメージギャラリーのImageVersionである場合:

  ```
  "Microsoft.Compute/galleries/read",

  "Microsoft.Compute/galleries/images/read",

  "Microsoft.Compute/galleries/images/versions/read",
  ```

- マスターイメージがマネージドディスクである場合、スナップショットまたはVHDがホスティング接続のリージョンとは異なるリージョンにある場合:

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",
```

- Citrix管理のリソースグループを使用する場合:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
```

- マスターイメージを共有テナントまたはサブスクリプションのAzure Compute Gallery (旧共有イメージギャラリー) に配置する場合:

```
"Microsoft.Compute/galleries/write",

"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/images/versions/write",

"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/versions/delete",
```

```
"Microsoft.Resources/subscriptions/read",
```

- Azure専用ホストサポートを使用する場合:

```
"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",

"Microsoft.Compute/hostGroups/hosts/read",
```

- 顧客管理キー (CMK) を使用したサーバー側暗号化 (SSE) を使用する場合:

```
"Microsoft.Compute/diskEncryptionSets/read",
```

- ARM テンプレート (マシンプロファイル) を使用して VM を展開する場合:

```
"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/delete",

"Microsoft.Insights/DataCollectionRuleAssociations/Read",

"Microsoft.Insights/dataCollectionRules/read",
```

- Azure テンプレート仕様をマシンプロファイルとして使用する場合:

```
"Microsoft.Resources/templateSpecs/read",

"Microsoft.Resources/templateSpecs/versions/read",
```

アンマネージドディスクを使用したマシンの作成、更新、および削除

マスターイメージがVHDであり、管理者が提供するリソースグループを使用する場合に必要となる最小限の権限のリストは次のとおりです。

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",
```

```
"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/locations/usages/read",
```

一般的な権限

共同作成者ロールは、すべてのリソースを管理するためのフルアクセス権を持っています。この権限セットは、新しい機能の取得を妨げません。

次の権限セットは、現在の機能セットで必要とされる以上の権限が含まれているものの、今後の最高の互換性を提供します。

```
"Microsoft.Compute/diskEncryptionSets/read",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/delete",

"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/images/versions/write",
```

```
"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/write",

"Microsoft.Compute/hostGroups/hosts/read",

"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
read",

"Microsoft.Compute/skus/read",

"Microsoft.Compute/virtualMachines/extensions/read",

"Microsoft.Compute/virtualMachines/extensions/write",
```

```
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/locations/usages/read",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/delete",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Resources/providers/read",
"Microsoft.Resources/subscriptions/locations/read",
```

```
"Microsoft.Resources/subscriptions/read",

"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Resources/tenants/read",

"Microsoft.Resources/templateSpecs/read",

"Microsoft.Resources/templateSpecs/versions/read",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",

"Microsoft.Features/providers/features/read",

"Microsoft.Insights/DataCollectionRuleAssociations/Read",

"Microsoft.Insights/dataCollectionRules/read",

"Microsoft.Insights/diagnosticsettings/delete",

"Microsoft.Insights/diagnosticsettings/read",

"Microsoft.Insights/diagnosticsettings/write",
```

ホスト接続上の権限を検証する

ホスト接続上の権限を検証して、MCSマシンカタログの作成と管理に関連するタスクを実行できます。この実装は、VMの作成、削除、更新、VMの電源管理など、さまざまなシナリオに必要な

不足している権限を事前に見つけるのに役立ち、重要なときにブロックされるのを避けることができます。

ホスト接続の権限は、PowerShellコマンド `Test-HypHypervisorConnection` を使用して検証できます。コマンドの結果はリストとしてキャプチャされ、リスト内の各項目は3つのセクションに分かれています。

- カテゴリ: ユーザーがMCSマシンカタログを作成および管理するために実行できるアクションまたはタスク。
- 修正措置: 管理者がユーザーの不足している権限の不一致を解決するために実行する必要がある手順。
- 不足している権限: カテゴリに対して不足している権限のリスト。

権限を検証するには、次の手順を実行します。

1. Azureへのホスト接続を作成します。
2. Delivery Controller™ホストからPowerShellウィンドウを開きます。
3. Citrix固有のPowerShellモジュールをロードするために `asnp citrix*` を実行します。
4. 接続をテストするために必要な権限があるかどうかを確認するには、次のコマンドを実行します。

   ```
   Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\AzureCon"
   ```

   SPNに必要なロールレベルの権限:

   - Microsoft.Authorization/roleDefinitions/read (サブスクリプションレベル、またはリソースグループが指定されている場合はリソースグループレベル)
   - Microsoft.Authorization/roleAssignments/read (サブスクリプションレベル、またはリソースグループが指定されている場合はリソースグループレベル)

   SPN に必要な API レベルの権限:

   Microsoft.Graph:

   - Application.Read.All
   - Directory.Read.All
   - ServicePrincipalEndpoint.Read.All

5. 権限を検索するために必要な不足している権限を追加した後、さまざまなカテゴリで権限があるかどうかを確認するために、次のコマンドを実行します。

   例:

   より高いレベルの承認が必要なサブスクリプションレベルで接続をテストするには:

   ```
   Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\ AzureCon
   -SecurePassword $password -UserName 922e65d5-38ae-4cf5-xxxx-xxxxxxxxx
   ```

   例:

   高レベルの承認なしでリソースグループレベルで接続をテストするには:

   ```
   Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\testles
   -CustomProperties $customProperties | Format-List
   ```

   注:

   CustomProperties パラメータは、リソースグループが接続固有の情報であるため、リソースグループレベルを提供するために使用されます。

   例:

   リソースグループレベルでより高いレベルの承認を使用して接続をテストするには:

   ```
   Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\testles
   -SecurePassword $password -UserName
   922e65d5-38ae-4cf5-832b-54122196b7dd -CustomProperties
   $customProperties
   ```

権限に関する情報については、必要なAzure権限を参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Azure固有の情報については、「Microsoft Azureカタログの作成」を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

マイクロソフト システムセンター 仮想マシンマネージャー への接続

接続を作成するウィザードについては、接続とリソースの作成および管理を参照してください。以下の情報は、Microsoft System Center Virtual Machine Manager (VMM) に固有の詳細を説明しています。

> **注:**
>
> VMM への接続を作成する前に、まず VMM アカウントをリソースの場所として設定する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/install-prepare/msscvmm.html)を参照してください。

接続を作成する

MCSを使用してVMをプロビジョニングした場合は、接続作成ウィザードで次の操作を行います。

- ホストサーバーの完全修飾ドメイン名としてアドレスを入力します。
- 以前に設定した管理者アカウントの資格情報を入力します。このアカウントには、新しいVMを作成する権限が必要です。
- 「ホストの詳細」ダイアログボックスで、VMの作成時に使用するクラスターまたはスタンドアロンホストを選択します。

  > **重要**
  >
  > 単一の Hyper-V ホスト展開を使用している場合でも、クラスターまたはスタンドアロンホストを参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。

- SMB 3 ファイル共有でMCSを使用してマシンカタログを作成する方法については、(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create/create-machine-catalog-mscvmm.html)を参照してください。

詳細情報

- 接続とリソース(/ja-jp/citrix-virtual-apps-desktops/2407/manage-deployment/connections.html)
- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html)

Nutanixへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報はNutanixに固有の詳細を扱っています。

> **注:**
>
> Nutanixへの接続を作成する前に、まず、リソースの場所としてNutanixアカウントの設定を完了する必要があります。Nutanix仮想化環境を参照してください。

Nutanixへの接続を作成する

以下の情報は、接続とリソースのガイダンスを補足するものです。Nutanix接続を作成するには、その記事の一般的なガイダンスに従い、Nutanixに固有の詳細に注意してください。

接続とリソースの追加ウィザードで、**接続**ページでNutanix接続の種類を選択し、アドレスと資格情報、および接続の名前を指定します。**ネットワーク**ページで、ホスティングユニットのネットワークを選択します。

以下の接続タイプを選択できます：**Nutanix AHV**、**Nutanix AHV DRaaS**、および**Nutanix AHV PC**。

- **Nutanix AHV**の場合、Prism Element（PE）クラスターのアドレスと資格情報を指定します。
- **Nutanix AHV PC**の場合、Prism Central（PC）のアドレスと資格情報を指定します。

> **注:**

> 現在、Nutanix AHV PC接続タイプは、Azure上のNutanix Cloud Cluster (NC2) への接続を作成する場合にのみ使用されます。また、マシンカタログは、Azure接続上のNC2内の単一クラスターにのみホストできます。

- **Nutanix AHV DRaaS**の場合、DRaaSテナントのアドレスとユーザー名を指定します。プライベートおよびパブリックのNutanix DRaaS資格情報ファイル（`.pem`）をインポートします。

ヒント:

Nutanix AHV (Prism Element) をリソースとして使用してマシンを展開する場合、仮想マシンのディスクが存在するコンテナを選択します。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Nutanix固有の情報については、「Nutanixカタログの作成」を参照してください。

詳細情報

- 「接続とリソース」(/ja-jp/citrix-virtual-apps-desktops/2407/manage-deployment/connections.html)
- 「マシンカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html)

Nutanix クラウドおよびパートナーソリューションへの接続

接続を作成するウィザードについては、(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections.html)で説明しています。以下の情報は、Nutanixクラウドおよびパートナーソリューションに固有の詳細を扱っています。

Citrix Virtual Apps and Desktops™ は、以下の Nutanix クラウドおよびパートナーソリューションをサポートしています。

- AWS 上のニュータニックス クラウドクラスター

注:

> Nutanix クラウドおよびパートナーソリューションへの接続を作成する前に、まずそれぞれのアカウントをリソースの場所として設定を完了する必要があります。「Nutanix クラウドおよびパートナーソリューション」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/install-prepare/nutanix-cloud-patrner-solutions.html).

Nutanix Prismへの接続

Nutanix クラスターを作成したら、Nutanix Prism に接続します。

Nutanix Prism に接続するには:

1. 10.0.129.0/24サブネットに踏み台VMを作成します。
2. 踏み台VMにRDP接続し、前のセクションでコピーした**Prism Element**のURLにアクセスします。
3. デフォルトの資格情報 `admin:nutanix/4u` を使用してログインします。パスワードを変更することを忘れないでください。

Nutanixクラスター上にVMを作成する

Nutanix Prismに接続した後、Nutanixクラスター上のVMを作成します。

VMにインターネットアクセスが必要な場合

1. AWSコンソールに移動します。
2. Nutanix CFS によって作成された VPC と同じ VPC 内に、新しいサブネット 10.0.130.0/24 を作成します。
3. このサブネットのルートテーブルにルートを追加して、すべての非ローカルトラフィックを上記のNATゲートウェイにルーティングするようにします。
4. Bastion VMにRDP接続し、前のセクションでコピーした**Prism Element**のURLにアクセスしてログインします。
5. 新しいネットワークを追加します。**Settings>Network Configuration>Create Subnet**に移動します。AWSで使用したのと同じサブネット10.0.130.0/24を使用します。
6. その新しいサブネット内に、すべてのVM (AD、CC、VDAなど) を作成します。

VM がインターネットアクセスを必要としない場合

1. Bastion VMにRDP接続し、前のセクションでコピーした**Prism Element**のURLにアクセスしてログインします。

2. 新しいネットワークを追加します。**Settings>Network Configuration>Create Subnet**に移動します。サブネット10.0.129.0/24を使用します。
3. そのサブネット内に、すべてのVM (AD、CC、VDAなど) を作成します。

> **ヒント:**
>
> VM の時刻とタイムゾーン情報が正しく設定されていることを確認してください。これは特に AD に当てはまります。

ホスト接続を作成します

1. Web Studio を起動します。
2. ホスティングノードを選択し、 をクリックします。
3. **Connection** 画面で、**Create a new Connection** を選択し、**Connection address** に `https://xxx.xxx.xxx.xxx:9440` を入力します。
4. UI に従ってウィザードを完了します。

> **注:**
>
> Web Studio で Nutanix のオプションを表示するには、Nutanix ゾーンで使用されていない場合でも、すべてのコネクタ VM に nutanix プラグインがインストールされている必要があります。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Nutanix 固有の情報については、「Nutanix カタログの作成」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create/create-machine-catalog-nutanix.html)

詳細情報

- 「接続とリソース」
- 「マシンカタログの作成」

VMwareへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報は、VMware仮想化環境に固有の詳細を扱っています。

> **注:**
>
> VMwareへの接続を作成する前に、まずVMwareアカウントをリソースの場所として設定を完了する必要があります。「VMware仮想化環境」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/install-prepare/vmware.html)を参照してください。

接続を作成する

接続作成ウィザードで：

1. VMware接続の種類を選択します。
2. vCenter SDKのアクセスポイントのアドレスを指定します。
3. 以前に設定した、VMを作成する権限を持つVMwareユーザーアカウントの資格情報を指定します。ユーザー名はdomain/usernameの形式で指定します。

VMware SSLサムプリント

VMware SSLサムプリント機能により、VMware vSphereハイパーバイザーへのホスト接続を手動で作成する必要がなくなります。接続を作成する前に、サイト内のDelivery Controllerとハイパーバイザーの証明書との間に信頼関係を手動で作成する必要はなくなりました。

VMware SSLサムプリント機能は、信頼されていない証明書のサムプリントをサイトデータベースに保存します。この構成により、コントローラーによって信頼されていない場合でも、ハイパーバイザーがCitrix Virtual Apps and Desktops™によって継続的に信頼されていると識別されることが保証されます。

StudioでvSphereホスト接続を作成する際、接続先のマシンの証明書を表示できるダイアログボックスが表示されます。その後、それを信頼するかどうかを選択できます。

必要な権限

VMwareユーザーアカウントと、この記事に記載されている権限の一部またはすべてを持つ1つ以上のVMwareロールを作成します。ロールの作成は、ユーザーがいつでもさまざまなCitrix DaaS™操作を要求するために必要な権限の特定の粒度レベルに基づいて行います。ユーザー固有の権限

をいつでも付与するには、**子に伝播**オプションを選択した状態で、少なくともデータセンターレベルでそれぞれのロールに関連付けます。

以下の表は、Citrix Virtual Apps and Desktops の操作と、最低限必要な VMware 権限とのマッピングを示しています。

> **注:**
>
> 権限リストの表示名、特に *User Interface* は、vSphere のバージョンによって異なります。たとえば、vSphere 6.7 では、*User Interface* 権限は、このページに記載されている必要な権限の説明にある **Settings** および **Memory** ではなく、**Change Memory** および **Change Settings** です。

接続とリソースを追加する

SDK	ユーザーインターフェイス
System. 匿名、System. 読み取り、および System. 表示	自動的に追加されます。組み込みの読み取り専用ロールを使用できます。

電源管理

SDK	ユーザーインターフェイス
VirtualMachine.Interact.PowerOff	仮想マシン > インタラクション > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > インタラクション > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > 対話 > リセット
VirtualMachine.Interact.Suspend	仮想マシン > 対話 > 一時停止
Datastore.Browse	データストア > データストアの参照

マシンのプロビジョニング (Machine Creation Services™)

MCS を使用してマシンをプロビジョニングするには、次の権限が必要です。

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	データストア > 領域の割り当て

SDK	ユーザーインターフェイス
Datastore.Browse	データストア > データストアの参照
Datastore.FileManagement	データストア > 低レベルファイル操作
Network.Assign	ネットワーク > ネットワークの割り当て
Resource.AssignVMToPool	リソース > 仮想マシンをリソースプールに割り当てる
VirtualMachine.Config.AddExistingDisk	仮想マシン > 構成 > 既存のディスクを追加
VirtualMachine.Config.AddNewDisk	仮想マシン > 構成 > 新しいディスクを追加
仮想マシン.構成.デバイスの追加または削除	仮想マシン > 構成 > デバイスの追加または削除
VirtualMachine.Config.AdvancedConfig	仮想マシン > 構成 > 詳細設定
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Config.CPUCount	仮想マシン > 構成 > CPU数の変更
VirtualMachine.Config.Memory	仮想マシン > 構成 > メモリの変更
VirtualMachine.Config.Settings	仮想マシン > 構成 > 設定の変更
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > 操作 > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > 操作 > リセット
VirtualMachine.Interact.Suspend	仮想マシン > 操作 > サスペンド
VirtualMachine.Inventory.CreateFromExisting	仮想マシン > インベントリ > 既存から作成
VirtualMachine.Inventory.Create	仮想マシン > インベントリ > 新規作成
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除
VirtualMachine.Provisioning.Clone	仮想マシン > プロビジョニング > 仮想マシンのクローン作成

SDK	ユーザーインターフェイス
VirtualMachine.State.CreateSnapshot	vSphere 5.0、Update 2、vSphere 5.1、Update 1、および vSphere 6.x、Update 1: 仮想マシン > 状態 > スナップショットの作成; vSphere 5.5: 仮想マシン > スナップショット管理 > スナップショットの作成

イメージの更新とロールバック

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	データストア > スペースの割り当て
Datastore.Browse	データストア > データストアの参照
Datastore.FileManagement	データストア > 低レベルファイル操作
Network.Assign	ネットワーク > ネットワークの割り当て
Resource.AssignVMToPool	リソース > 仮想マシンをリソースプールに割り当てる
VirtualMachine.Config.AddExistingDisk	仮想マシン > 構成 > 既存のディスクを追加
VirtualMachine.Config.AddNewDisk	仮想マシン > 構成 > 新しいディスクを追加
VirtualMachine.Config.AdvancedConfig	仮想マシン > 構成 > 詳細設定
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > 操作 > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > 操作 > リセット
VirtualMachine.Inventory.CreateFromExisting	仮想マシン > インベントリ > 既存から作成
VirtualMachine.Inventory.Create	仮想マシン > インベントリ > 新規作成
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除

SDK	ユーザーインターフェイス
VirtualMachine.Provisioning.Clone	仮想マシン > プロビジョニング > 仮想マシンのクローン作成

プロビジョニングされたマシンの削除

SDK	ユーザーインターフェイス
Datastore.Browse	データストア > データストアの参照
Datastore.FileManagement	Datastore > 低レベルファイル操作
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除

ストレージプロファイル (vSAN)

vSAN データストアでのカタログ作成中にストレージポリシーを表示、作成、または削除するには、次の権限が必要です。

SDK	ユーザーインターフェイス
StorageProfile.Update	プロファイル駆動型ストレージ > プロファイル駆動型ストレージの更新。vSphere 8 の場合: VMストレージポリシー > VMストレージポリシーの更新
StorageProfile.View	PROFILE-DRIVEN STORAGE > プロファイル駆動型ストレージビュー。vSphere 8 の場合: VM ストレージポリシー > VM ストレージポリシーの表示

タグとカスタム属性

タグとカスタム属性を使用すると、vSphere インベントリで作成された VM にメタデータを付加し、これらのオブジェクトの検索とフィルタリングを容易にすることができます。タグまたはカテゴリを作成、編集、割り当て、削除するには、次の権限が必須です。

SDK	ユーザーインターフェイス
InventoryService.Tagging.CreateTag	vSphere タグ付け > vSphere タグの作成
InventoryService.Tagging.CreateCategory	vSphere タグ付け > vSphere タグカテゴリの作成
InventoryService.Tagging.EditTag	vSphere タグ付け > vSphere タグの編集
InventoryService.Tagging.EditCategory	vSphere Tagging > vSphereタグカテゴリの編集
InventoryService.Tagging.DeleteTag	vSphere Tagging > vSphereタグの削除
InventoryService.Tagging.DeleteCategory	vSphere Tagging > vSphereタグカテゴリの削除
InventoryService.Tagging.AttachTag	vSphere Tagging > vSphereタグの割り当てまたは割り当て解除
InventoryService.Tagging.ObjectAttachable	vSphere Tagging > オブジェクト上のvSphereタグの割り当てまたは割り当て解除
Global.ManageCustomFields	Global > カスタム属性の管理
Global.SetCustomField	Global > カスタム属性の設定

注：

MCSがマシンカタログを作成すると、ターゲットVMに特別な名前タグを付けます。これらのタグは、マスターイメージをMCSで作成されたVMと区別し、MCSで作成されたVMがイメージ準備に使用されるのを防ぎます。vCenterの `XdProvisioned` 属性の値によって違いを識別できます。MCSがVMを作成した場合、この属性は**True**に設定されます。

暗号化操作

暗号化操作の権限は、誰がどの種類のオブジェクトに対してどの種類の暗号化操作を実行できるかを制御します。vSphere Native Key Providerは `Cryptographer.*` 権限を使用します。暗号化操作には、以下の最小限の権限が必要です。

注:

これらの権限は、vTPM を搭載した VM を使用して MCS マシンカタログを作成するために必要です。

SDK	ユーザーインターフェイス
Cryptographer.Access	権限 > すべての権限 > 暗号化操作 > 直接アクセス
Cryptographer.AddDisk	権限 > すべての権限 > 暗号化操作 > ディスクの追加
Cryptographer.Clone	権限 > すべての権限 > 暗号化操作 > クローン
Cryptographer.Encrypt	権限 > すべての権限 > 暗号化操作 > 暗号化
Cryptographer.EncryptNew	権限 > すべての権限 > 暗号化操作 > 新規暗号化
Cryptographer.Decrypt	権限 > すべての権限 > 暗号化操作 > 復号化
Cryptographer.Migrate	権限 > すべての権限 > 暗号化操作 > 移行
Cryptographer.ReadKeyServersInfo	権限 > すべての権限 > 暗号化操作 > KMS情報の読み取り

マシンのプロビジョニング（Citrix Provisioning™）

テンプレートをクローンして展開するためのこれらの権限は、Citrix Virtual Apps and Desktops セットアップウィザードおよびデバイスのエクスポートウィザードを使用してCitrix Provisioning コンソールを介してVMをプロビジョニングするために必要です。ホスティング接続の作成中に権限を設定します。マシンのプロビジョニング（Machine Creation Services）からのすべての権限と、以下の権限が必要です。

SDK	ユーザーインターフェイス
VirtualMachine.Config.AddRemoveDevice	仮想マシン > 構成 > デバイスの追加または削除

SDK	ユーザーインターフェイス
VirtualMachine.Config.CPUCount	仮想マシン > 構成 > CPU数の変更
VirtualMachine.Config.Memory	仮想マシン > 構成 > メモリ
VirtualMachine.Config.Settings	仮想マシン > 構成 > 設定
VirtualMachine.Provisioning.CloneTemplate	仮想マシン > プロビジョニング > テンプレートのクローン作成
VirtualMachine.Provisioning.DeployTemplate	仮想マシン > プロビジョニング > テンプレートの展開
VApp.Export	vApp > エクスポート

注:

`VApp.Export` は、マシンプロファイルを使用してMCSマシンカタログを作成するために必要です。

証明書の取得とインポート

vSphere通信を保護するため、Citrix®はHTTPではなくHTTPSを使用することを推奨します。

HTTPSにはデジタル証明書が必要です。組織のセキュリティポリシーに準拠した認証局から発行されたデジタル証明書を使用してください。

認証局から発行されたデジタル証明書を使用できない場合は、VMwareがインストールした自己署名証明書を使用できます。この方法は、組織のセキュリティポリシーで許可されている場合にのみ使用してください。VMware vCenter証明書を各Delivery Controllerに追加します。

1. vCenter Serverを実行しているコンピューターの完全修飾ドメイン名（FQDN）を、そのサーバーのhostsファイル（`%SystemRoot%/WINDOWS/system32/Drivers/etc/`）に追加します。この手順は、vCenter Serverを実行しているコンピューターのFQDNがドメインネームシステムにまだ存在しない場合にのみ必要です。
2. 以下の3つのいずれかの方法でvCenter証明書を取得します。

   vCenterサーバーから。

a. vCenterサーバーからrui.crtファイルをDelivery Controllerでアクセス可能な場所にコピーします。

b. Controllerで、エクスポートされた証明書の場所に移動し、rui.crtファイルを開きます。

Webブラウザーを使用して証明書をダウンロードします。 Internet Explorerを使用している場合は、Internet Explorerを右クリックし、**「管理者として実行」**を選択して証明書をダウンロードまたはインストールします。

a. Webブラウザーを開き、vCenterサーバーへのセキュアなWeb接続を行います (例: `<https://server1.domain1.com)>`)。

b. セキュリティ警告を受け入れます。

c. 証明書エラーが表示されているアドレスバーをクリックします。

d. 証明書を表示し、「詳細」タブをクリックします。

e. **「ファイルにコピー」を選択し、.CER形式でエクスポートします。**プロンプトが表示されたら名前を指定します。

f. エクスポートされた証明書を保存します。

g. エクスポートされた証明書の場所に移動し、.CER ファイルを開きます。

管理者として実行している Internet Explorer から直接インポートします。

- Webブラウザーを開き、vCenterサーバーに安全なWeb接続を行います（例：`<https://server1.domain1.com)>`）。
- セキュリティ警告を承認します。
- 証明書エラーが表示されているアドレスバーをクリックします。
- 証明書を表示します。

3. 各Controllerの証明書ストアに証明書をインポートします。

a. **証明書のインストール**オプションをクリックし、**ローカルコンピューター**を選択して、**次へ**をクリックします。

b. **証明書をすべて次のストアに配置する**を選択し、**参照**をクリックします。**信頼された発行元**を選択し、**OK**をクリックします。**次へ**をクリックし、**完了**をクリックします。

インストール後にvSphereサーバーの名前を変更した場合は、新しい証明書をインポートする前に、そのサーバーで新しい自己署名証明書を生成する必要があります。

次のステップ

- 初期展開プロセス中の場合は、マシンカタログの作成を参照してください。
- VMware固有の情報については、VMwareカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

VMware クラウドおよびパートナーソリューションへの接続

Azure VMware Solution (AVS) クラスター、Google Cloud VMware Engine、およびVMware Cloud on AWS を設定した後、接続を作成します。接続の作成については、VMware への接続 を参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- VMware固有の情報については、VMwareカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

イメージ管理 (プレビュー)

はじめに

MCSカタログの作成または更新プロセスには2つのフェーズがあります。

- マスタリング: ソースイメージが公開イメージに変換されます
- クローニング: 公開イメージから新しいVMが作成されます

イメージ管理機能を使用すると、MCSはマスタリングフェーズをプロビジョニングワークフロー全体から分離します。

単一のソースイメージからさまざまなMCSイメージバージョン (準備済みイメージ) を準備し、複数の異なるMCSマシンカタログで利用できます。この実装により、ストレージと時間のコストが大幅に削減され、VMの展開とイメージ更新プロセスが簡素化されます。

このイメージ管理機能を使用する利点は次のとおりです。

- カタログを作成せずに、準備済みイメージを事前に生成します。
- カタログの作成や更新など、複数のシナリオで準備済みイメージを再利用します。
- カタログの作成または更新時間を大幅に削減します。

> **注:**
>
> - この機能は現在、AzureおよびVMware仮想化環境に適用されます。
> - 準備済みイメージを使用せずにMCSマシンカタログを作成できます。その場合、この機能のメリットは得られません。

ユースケース

イメージ管理機能のユースケースの一部を次に示します。

- *バージョン管理*: イメージバージョンを使用すると、次のことができます。
  - 特定のイメージに対する異なるイテレーションや更新を管理する。
  - 異なる目的のためにイメージの複数のバージョンを維持する。
- *論理的なグループ化*: 複数のイメージ定義を作成して、次のことを行えます。
  - プロジェクト、部門、アプリケーション、デスクトップの種類など、さまざまな基準に基づいてイメージのバージョンを論理的にグループ化する。
  - 組織内でイメージをより効率的に管理する。

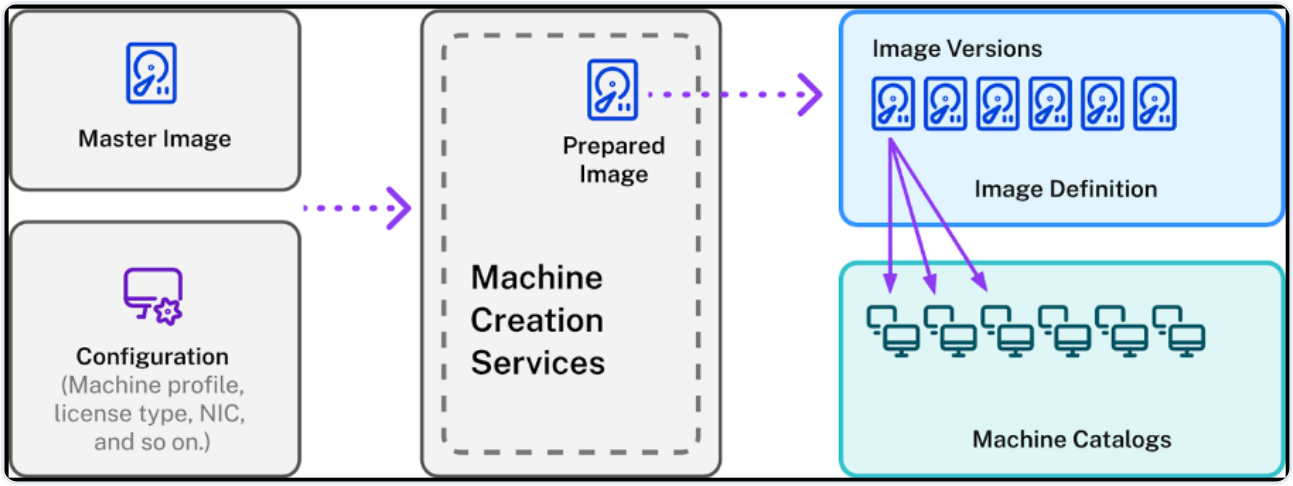
準備されたイメージとは何ですか?

イメージ管理機能により、MCSはマスタリングフェーズをカタログ作成または更新の全体的なワークフローから切り離し、プロセスを2つの段階に分けます。

1. 単一のソースイメージから準備されたイメージを作成する。
2. 準備されたイメージを使用して、MCSマシンカタログを作成または更新する。

準備されたイメージは事前に作成できます。単一の準備されたイメージを使用して、複数のMCSプロビジョニング済みマシンカタログを作成または更新できます。

イメージからWeb Studioを使用する場合に、準備されたイメージが複数のMCSマシンカタログでどのように使用されるかを理解してください。



イメージ定義: イメージ定義は、イメージのバージョンの論理的なグループ化です。イメージ定義には、次の情報が含まれます。

- イメージが作成された理由
- 対象となるOS
- イメージの使用に関するその他の情報。

カタログはイメージ定義から作成されるのではなく、イメージ定義に基づいて作成されたイメージバージョンから作成されます。

イメージバージョン: イメージバージョンは、イメージ定義のバージョン管理を行います。イメージ定義には複数のイメージバージョンを含めることができます。イメージバージョンを準備済みイメージとして使用して、カタログを作成または更新します。

または、PowerShellコマンドを使用してプロビジョニングスキームを作成し、カタログを作成または更新する場合は、環境の必要に応じて、マスターイメージバージョンスペックに基づいて準備済みイメージバージョンスペックを作成する必要があります。

テックプレビューに参加する

テックプレビューへの参加にご興味がある場合は、こちらからご連絡先をご提供ください。

必要に応じて、テスト環境のセットアップを支援し、技術サポートを提供します。

要件

- Windowsマスターイメージの場合、VDAイメージバージョン2311以降のみがサポートされます。MCS/IOコンポーネントは明示的に選択してインストールする必要があります。MCS I/O構

成の有効化または無効化は、デフォルトでは有効になっていないため、マシンカタログの作成または更新時に決定する必要があります。

制限事項

現在、この機能は以下をサポートしていません。

- Azureでの複数のNIC
- 永続データディスク機能
- マルチセッションの休止状態
- イメージタイプの変更

Web Studioを使用したイメージライフサイクル管理

Web Studioを使用する場合のイメージのライフサイクルは次のとおりです。

1. 準備済みイメージの作成: イメージ定義とその初期イメージバージョンを作成します。
2. 初期イメージバージョンからイメージバージョンを作成します。
3. イメージバージョンを準備済みイメージとして使用してカタログを作成します。
4. 別の準備済みイメージでマシンカタログを更新します。
5. イメージ定義とバージョンを管理する: イメージバージョンの名前と説明、およびイメージ定義の説明を編集します。
6. イメージバージョンを削除します。
7. イメージ定義を削除します。

あるいは、PowerShell を使用してイメージを管理することもできます。「PowerShell を使用したイメージライフサイクル管理」を参照してください。

準備済みイメージを使用してカタログを作成または更新する

準備済みイメージを作成し、その準備済みイメージを使用して、次の方法で MCS マシンカタログを作成または更新します。

- ウェブスタジオ
- PowerShell コマンド

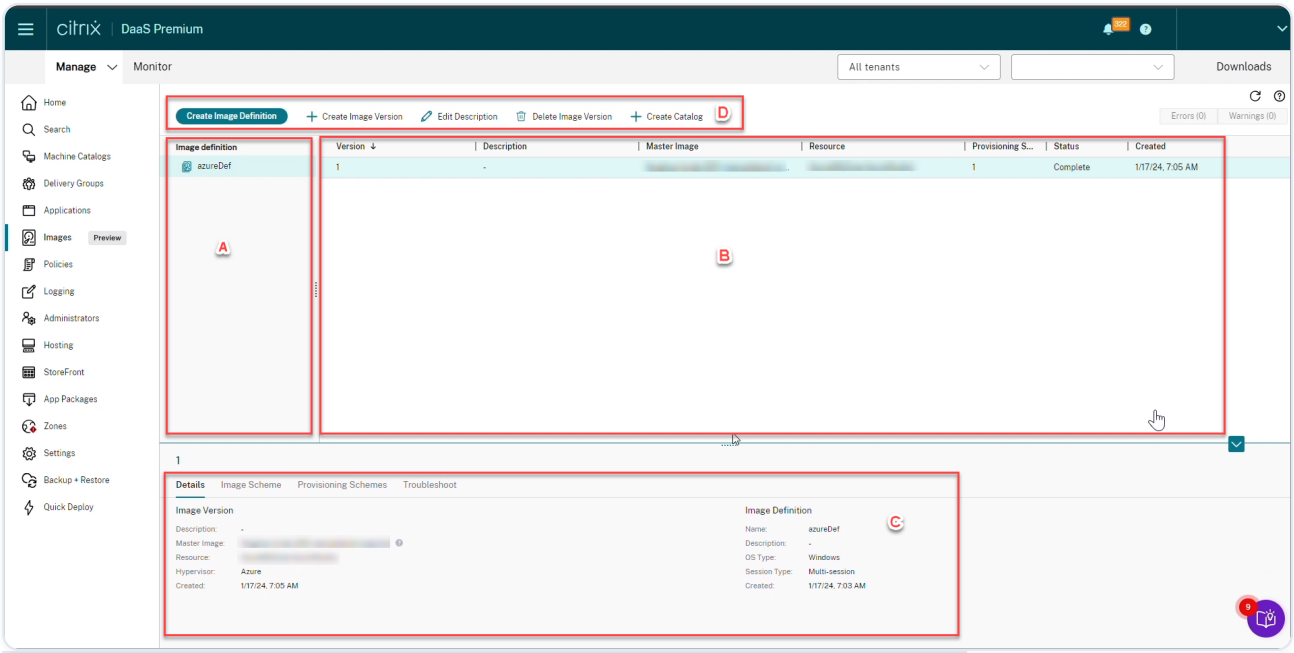
Web Studio の使用

次のトピックを参照してください。

- イメージノードについて理解する
- イメージ定義と初期イメージバージョンを作成する
- イメージバージョンを作成する
- イメージノードからマシンカタログを作成する
- マシンカタログノードからマシンカタログを作成する
- 別の準備済みイメージでマシンカタログを更新する
- イメージ定義とバージョンを管理する

イメージノードについて理解する

イメージノードを使用して、MCSで準備されたイメージを作成および管理します。そのメインビューは4つの部分に分かれています。



ラベル	部分	説明
A	イメージ定義	以前に作成されたイメージ定義を一覧表示します。
B	イメージバージョン	選択したイメージ定義のイメージバージョンを表示します。

ラベル	部分	説明
C	詳細	• **詳細**タブには、選択したイメージ定義またはバージョンに関する詳細情報（マスターイメージ、リソース、ハイパーバイザー、イメージ定義の名前、OSタイプ、セッションタイプなど）が表示されます。 • **イメージスキーム**タブには、ハードディスク、マシンサイズ、ライセンスタイプ、ディスク暗号化セット、マシンプロファイルなど、イメージの準備に使用されるテンプレートに関する情報が表示されます。 • 「**Provisioning Schemes**」タブには、カタログの作成に使用されたプロビジョニングス

ラベル	部分	説明	
		キーム名が表示されます。 • 「**Troubleshoot**」タブには、選択したイメージバージョンのエラー状態が表示されます。	
D	アクションバー	イメージ定義とバージョンに対して実行できるアクション（**Create Image Version**、**Edit Description**、**Delete Image Version**、**Create Catalog**など）を一覧表示します。	

準備されたイメージを使用してマシンカタログを作成する

準備されたイメージを使用してMCSマシンカタログを作成するための主要な手順は次のとおりです。

1. イメージ定義と初期イメージバージョンを作成します。
2. イメージバージョンを準備されたイメージとして使用して、カタログを作成します。

イメージ定義と初期イメージバージョンを作成する

イメージ定義と初期イメージバージョンを作成するには、次の手順を実行します。

1. Web Studioにサインインし、「**Images**」ノードを選択します。「**Introduction**」ページで「**Next**」をクリックします。
2. 「**Image Definition**」ページで、イメージ定義の「**OS type**」と「**Session type**」を指定します。

3. 「**Image**」ページで、「**Resources**」と、イメージバージョン作成のテンプレートとして使用するマスターイメージを選択します。「**Use a machine profile**」チェックボックスを選択し、マシンプロファイルを選択できます。

   > **注：**
   >
   > イメージを選択する前に、マスターイメージにVDA 2311以降がインストールされており、MCSIOドライバーがVDAにインストールされていることを確認してください。

4. (Azureのみ) **Storage and Licenses Types**ページで、イメージ準備プロセスの一部として使用するストレージとライセンスの種類を選択します。

   > **注：**
   >
   > **イメージ**ページでマシンプロファイルを選択すると、プロファイル設定に基づいてマシンプロファイルのライセンスタイプが事前に選択されます。

5. 「**マシン仕様**」ページで：

   - Azureの場合、マシンサイズを選択します。**Image**ページでマシンプロファイルを選択した場合、マシンプロファイルのマシンサイズがデフォルトで選択されます。
   - VMwareの場合、マシンプロファイルを選択すると、マシンプロファイルから派生した仮想CPUカウントが表示され、変更できません。マシンプロファイルを選択しない場合、マスターイメージから派生したメモリサイズのみが表示されます。

6. **NIC**ページで、準備イメージのNICを選択または追加します。各NICについて、関連する仮想ネットワークを選択します。

   VMwareの場合、マシンプロファイルを選択しない場合、マスターイメージに関連付けられているNICがデフォルトで選択されます。マシンプロファイルを選択した場合、NICはマシンプロファイルから派生し、その数は変更できません。

   > **注：**
   >
   > Azureでは複数のNICはサポートされていません。

7. (Azureのみ) 「**Disk Settings**」ページで、顧客管理の暗号化キー (CMEK) を選択します。マシンプロファイルにCMEKがないが、マスターイメージにある場合、マスターイメージからCMEKが事前に選択されます。
8. 「**Version Description**」ページで、作成された初期イメージバージョンの説明を入力します。
9. 「**概要**」ページで、作成されたイメージ定義と初期イメージバージョンの詳細を確認します。イメージ定義の名前と説明を入力します。「**完了**」をクリックします。

イメージバージョンを作成する

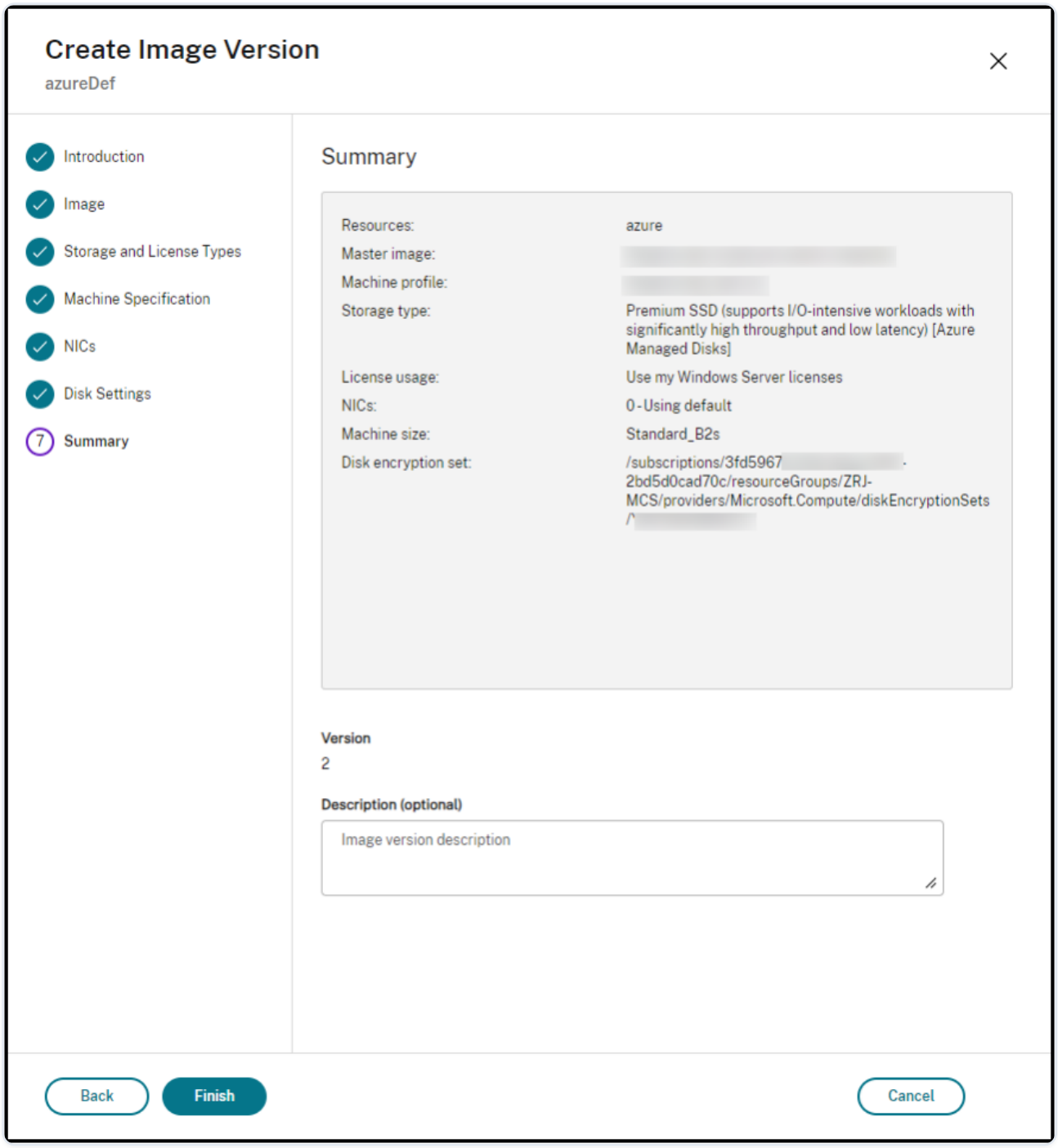
イメージバージョンを使用すると、特定のイメージに対するさまざまなイテレーションや更新を管理できます。この機能により、さまざまな目的のためにイメージの複数のバージョンを維持できます。

初期イメージバージョンからイメージバージョンを作成するには、次の手順を実行します。

> 「**注：**」:

> すべてのイメージバージョンのホスティングユニットは同じである必要があります。

1. 「**イメージ**」ノードに移動し、イメージバージョンを選択して、「**イメージバージョンの作成**」を選択します。
2. イメージバージョンの構成を初期構成済みイメージバージョンと異なるものにしたい場合は、「**イメージバージョンの作成**」ダイアログの「**イメージ**」、「**ストレージとライセンスの種類**」、「**マシン仕様**」、「**NIC**」、「**ディスク設定**」の各ページで設定を構成します。
3. イメージバージョンの説明を追加します。「**完了**」をクリックします。



「イメージ」ノードからマシンカタログを作成する

「**イメージ**」ノードの「**カタログの作成**」オプションを使用して、イメージバージョンでカタログを作成します。

または、**マシンカタログ**ノードでカタログを作成する際にバージョンを選択し、カタログ作成ワークフローで準備済みイメージオプションにリンクできます。「マシンカタログノードからマシンカタログを作成する」を参照してください。(#create-a-machine-catalog-from-the-machine-catalogs-node)

「**イメージ**」ノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. イメージバージョンを選択し、「**カタログの作成**」をクリックします。「**はじめに**」ページで「**次へ**」をクリックします。
2. 「**デスクトップエクスペリエンス**」ページで、必要なデスクトップエクスペリエンスを選択します。
3. 「**イメージ**」ページから「**ディスク設定**」ページまで、設定は選択したイメージバージョンに基づいて事前に選択されています。
4. (Azureの場合) 「**リソースグループ**」ページで、新しいリソースグループを作成するか、既存のリソースグループを使用してこのカタログのリソースを配置するかを選択できます。
5. 以下のページで設定を完了します。
6. 「**概要**」ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。「**完了**」をクリックします。
7. 作成されたマシンカタログを表示するには、「**マシンカタログ**」ノードに移動します。

「マシンカタログ」ノードからマシンカタログを作成する

マシンカタログノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. 左側のナビゲーションペインで「**マシンカタログ**」をクリックします。
2. 「**マシンカタログの作成**」をクリックします。「**マシンカタログのセットアップ**」ページが表示されます。「**はじめに**」、「**マシンタイプ**」、「**マシン管理**」の各ページで「**次へ**」をクリックします。
3. 「**イメージ**」ページで：
   a. 「**準備済みイメージ**」を選択します。
   b. 「**準備済みイメージ**」の下で、イメージ定義のイメージバージョンを選択します。
   c. イメージバージョン名をクリックします。選択したイメージバージョンの詳細を表示するには、下線が引かれているバージョン番号をクリックします。
   d. 選択したイメージバージョンがマシンプロファイルで構成されている場合は、マシンプロファイルを選択します。選択したイメージバージョンがマシンプロファイルで構成されていない場合は、マシンプロファイルを使用することを選択できません。
4. 次のページで設定を構成します。
5. **ディスク設定**ページで、選択した準備済みイメージがディスク暗号化セットを使用している場合、その暗号化セットを削除することはできませんが、キーを別の暗号化キーに変更することはできます。

6. (Azureの場合) **リソースグループ**ページで、新しいリソースグループを作成するか、既存のリソースグループを使用してこのカタログのリソースを配置するかを選択できます。
7. 次のページで設定を完了します。
8. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。

別の準備済みイメージでマシンカタログを更新する

既存のMCSマシンカタログを別の準備済みイメージで更新するには、次の手順を実行します。

1. 左側のナビゲーションペインで をクリックし、更新するマシンカタログを選択します。右クリックして を選択します。
2. **イメージ**ページで、準備済みイメージを選択します。
3. **ロールアウト戦略**ページで、選択した準備済みイメージでこのカタログを更新するタイミングを選択します。
4. ページで詳細を確認します。 をクリックします。

カタログに対して行われたイメージ変更の履歴を確認できます。履歴を表示するには、次の手順を実行します。

1. マシンカタログを選択します。
2. タブの フィールドで、 をクリックします。

イメージの定義とバージョンを管理する

イメージ定義とバージョンを編集および削除して、作成されたさまざまなイメージバージョンと定義の使用を管理できます。

イメージ定義を編集する

イメージ定義の名前と説明を編集できます。

イメージ定義を編集するには、次の手順を実行します。

1. ノードに移動し、イメージ定義を選択して、 を選択します。

イメージバージョンを編集する

イメージバージョンの説明を編集して、そのイメージバージョンの目的を指定できます。

イメージバージョンを編集するには、次の手順を実行します。

1. **イメージ**ノードに移動し、イメージバージョンを選択して、**説明の編集**を選択します。

イメージバージョンを削除する

イメージバージョンを削除するには、次の手順を実行します。

1. **イメージ**ノードに移動し、イメージバージョンを選択して、**イメージバージョンの削除**を選択します。

> **注:**
>
> イメージバージョンがマシンカタログで使用されている場合、そのイメージバージョンを削除することはできません。

イメージ定義を削除する

イメージ定義を削除するには、次の手順を実行します。

1. **イメージ**ノードに移動し、イメージ定義を選択して、**イメージ定義の削除**を選択します。

> **注：**
>
> イメージバージョンが含まれているイメージ定義は削除できません。

PowerShell を使用したイメージライフサイクル管理

PowerShell コマンドを使用してプロビジョニングスキームを作成する場合は、環境の必要に応じて、マスターイメージバージョン仕様に基づいて準備されたイメージバージョン仕様を作成する必要があります。

マスターイメージバージョン仕様: マスターイメージバージョン仕様は、イメージバージョンに追加または作成された特定のイメージです。ハイパーバイザー内の既存のイメージをマスターイメージバージョン仕様として追加するか、環境の必要に応じてマスターイメージバージョン仕様に基づいて準備されたイメージバージョン仕様を作成できます。準備されたイメージバージョン仕様は、複数のプロビジョニングスキームに使用できます。

PowerShell コマンドを使用する場合のイメージのライフサイクルは次のとおりです。

1. イメージを作成する：
    a. イメージ定義を作成します。
    b. イメージバージョンを作成します。

c. マスターイメージバージョン仕様を追加します。

d. 準備済みイメージバージョン仕様を作成します。

2. 準備済みイメージバージョン仕様を使用して MCS マシンカタログを作成する：

a. ブローカーカタログを作成します。

b. IDプールを作成します。

c. `New-ProvScheme`コマンドを使用して、準備済みイメージバージョン仕様Uidのパラメーターを持つプロビジョニングスキームを作成します。

d. ブローカーカタログをプロビジョニングスキームにリンクします。

3. MCSマシンカタログにVMを作成します。

4. `Set-ProvScheme`コマンドを使用して、プロビジョニングスキームの準備済みイメージバージョン仕様を変更します。

5. イメージ定義とバージョンを管理します: イメージバージョンとイメージ定義を編集します。

6. MCSマシンカタログを削除します: 削除順序は、準備済みイメージバージョン仕様 > マスターイメージバージョン仕様 > イメージバージョン > イメージ定義です。イメージバージョン仕様を削除する前に、準備済みイメージバージョン仕様がどのMCSマシンカタログにも関連付けられていないことを確認してください。

PowerShell を使用する

PowerShellコマンドを使用して、以下を実行できます。

- 準備済みイメージを作成する
- 準備済みイメージバージョン仕様を使用してカタログを作成する
- 準備されたイメージバージョン仕様を使用してカタログを更新する
- イメージ定義、イメージバージョン、および準備されたイメージバージョン仕様を削除する
- イメージ定義とイメージバージョンを管理する
- イメージ定義、イメージバージョン、準備済みイメージバージョン仕様、およびプロビジョニングスキームの詳細を取得する

準備済みイメージを作成する

準備済みイメージバージョン仕様を作成するための詳細な PowerShell コマンドは次のとおりです。

1. `Test-ProvImageDefinitionNameAvailable command` を使用して、利用可能なイメージ定義名を確認します。例:

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
```

2. `New-ProvImageDefinition` コマンドを使用してイメージ定義を作成します。例:

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession
```

3. `New-ProvImageVersion` コマンドを使用してイメージバージョンを作成します。例:

```
New-ProvImageVersion -ImageDefinitionName image1 -Description "version
1"
```

4. `Add-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様をイメージバージョンに追加します。例:

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
ImageVersionNumber  1 -HostingUnitName azure -MasterImagePath "XDHyp:
\HostingUnits\azure\image.folder\azureresourcegroup.resourcegroup\win20
22-snapshot.snapshot"
```

注:

ホスティングユニットの1つのイメージバージョンには、マスターイメージバージョン仕様を1つだけ追加できます。

5. `New-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様から準備済みイメージバージョン仕様を作成します。例:

```
New-ProvImageVersionSpec

-SourceImageVersionSpecUid  c6e7384c-b2f8-46d6-9519-29a2c57ed3cb

-NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resou
```

```
rcegroup\azure-vnet-eastus.virtualprivatecloud\dev.network"

-ServiceOffering "XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2ms.serviceofferin
g" -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"></CustomProperties>"
-RunAsynchronously
```

注:

1つのホスティングユニットと準備タイプには、準備済みインスタンスを1つだけ含めることができます。

Azureでイメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を作成するためのPowerShellコマンドの完全なセットの例:

```
$ImageDefintion = New-ProvImageDefinition

-ImageDefinitionName image1 -OsType Windows -VdaSessionSupport
MultiSession

 $ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"

$MasterImagePath = "XDHyp:
\HostingUnits\azure\image.folder\azureresourcegroup.resourcegroup\win2022-
snapshot.snapshot"

$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageVersion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName azure -MasterImagePath
$MasterImagePath

$Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resource
group\azure-vnet-eastus.virtualprivatecloud\dev.network"} -ServiceOffering
"XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2ms.serviceoffering"
```

```
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"></CustomProperties>" -RunAsynchronously

Get-ProvTask -TaskId $Task.TaskId
```

VMwareでイメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を作成するためのPowerShellコマンドの完全なセットの例:

```
$ImageDefintion = New-ProvImageDefinition -ImageDefinitionName image2
-OsType Windows -VdaSessionSupport SingleSession

$ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"

$MasterImagePath = "XDHyp:\HostingUnits\vmware\win10-master.vm\win10-
master-snap.snapshot"

$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageVersion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName vmware -MasterImagePath
$MasterImagePath

$Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vmware\\DSwitch-VM Network.network"} -VMCpuCount 2
-VMMemoryMB 4096 -RunAsynchronously

Get-ProvTask -TaskId $Task.TaskId
```

注:

- イメージ定義内のすべてのイメージバージョン仕様は、同じホスティングユニットに属している必要があります。
- イメージバージョンは、マスターイメージバージョン仕様を1つ、準備済みイメージバージョン仕様を1つしか持つことができません。

- すべてのイメージバージョン仕様は、マシンプロファイルを持つか、またはどのイメージバージョン仕様もマシンプロファイルを持たないかのいずれかである必要があります。
- イメージバージョン仕様の作成中にリソースグループを指定することはできません。

準備済みイメージバージョン仕様を使用してカタログを作成する

`New-ProvScheme`コマンドを使用して、準備済みイメージバージョン仕様からMCSマシンカタログを作成します。例:

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

または、,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

AzureでカタログをするためのPowerShellコマンドの完全なセットの例:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "azurecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"

$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "azure.local"
```

```
-IdentityPoolName "azurecatalog" -IdentityType "ActiveDirectory"  -
NamingScheme "azure##" -NamingSchemeType "Numeric" -Scope @()

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"

$Task = New-ProvScheme -ProvisioningSchemeName azurecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName azure -IdentityPoolName azurecatalog -CleanOnBoot -Scope
@() -SecurityGroup @() -ServiceOffering "XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2s.serviceoffering"
-NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resource
group\azure-vnet-eastus.virtualprivatecloud\dev.network"}
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"StandardSSD_LRS`" /></
CustomProperties>" -RunAsynchronously

Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName azurecatalog

Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

VMwareでカタログを作成するためのPowerShellコマンドの完全なセットの例:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "vmwarecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"

$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain
"vmware.local" -IdentityPoolName "vmwarecatalog" -IdentityType
"ActiveDirectory"  -NamingScheme "vmware##" -NamingSchemeType "Numeric"
-Scope @()

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image2 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"

$Task = New-ProvScheme -ProvisioningSchemeName vmwarecatalog
```

```
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName vmware -IdentityPoolName vmwarecatalog -CleanOnBoot
-Scope @() -SecurityGroup @() -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vmware\\DSwitch-VM Network.network"} -VMCpuCount 2
-VMMemoryMB 4096 -RunAsynchronously

Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName vmwarecatalog

Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

準備されたイメージバージョン仕様を使用してカタログを更新する

`Set-ProvSchemeImage`コマンドを使用してカタログを更新できます。例:

```
Set-ProvSchemeImage -ProvisioningSchemeUid <Guid> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess]
```

または、,

```
Set-ProvSchemeImage -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess]
```

カタログを更新するためのPowerShellコマンドの完全なセットの例:

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 2 -Filter "PreparationType -eq 'Mcs'"

Set-ProvSchemeImage -ProvisioningSchemeName azurecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-RunAsynchronously
```

イメージ定義、イメージバージョン、および準備されたイメージバージョン仕様を削除する

イメージ定義、イメージバージョン、および準備されたイメージバージョン仕様を削除する前に、次の点を考慮してください:

- イメージ定義にイメージバージョンが含まれている場合、そのイメージ定義は削除できません。
- イメージバージョンにイメージバージョン仕様が含まれている場合、そのイメージバージョンは削除できません。
- マスターイメージバージョン仕様が他の準備済みイメージバージョン仕様で使用されている場合、そのマスターイメージバージョン仕様は削除できません。
- 準備済みイメージバージョン仕様がプロビジョニングスキームで使用されている場合、その準備済みイメージバージョン仕様は削除できません。

詳細な手順は次のとおりです。

1. 準備済みイメージバージョン仕様を削除します。例：

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec
-ImageDefinitionName image1 -ImageVersionNumber 1 -Filter
"PreparationType -eq 'Mcs'"

Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
```

> **注：**
>
> マスターイメージバージョン仕様は、関連付けられた準備済みイメージバージョン仕様がない場合にのみ削除できます。

2. マスターイメージバージョン仕様を削除します。例：

```
$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"

Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
```

3. イメージバージョンを削除します。例：

```
Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber
1
```

4. イメージ定義を削除します。例：

```
Remove-ProvImageDefinition -ImageDefinitionName image1
```

PowerShellコマンドの完全なセットの例：

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"

$Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously

$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"

$Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously

Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber 1

Remove-ProvImageDefinition -ImageDefinitionName image1
```

イメージ定義とイメージバージョンの管理

イメージ定義の名前変更と編集、およびイメージバージョンの編集が可能です。

- `Rename-ProvImageDefinition` コマンドを使用してイメージ定義の名前を変更します。例：

  ```
  Rename-ProvImageDefinition -ImageDefinitionUid <Guid>
  -NewImageDefinitionName <string>
  ```

  または、,

  ```
  Rename-ProvImageDefinition -ImageDefinitionName <string>
  -NewImageDefinitionName <string>
  ```

- `Set-ProvImageDefinition` コマンドを使用してイメージ定義を編集します。例：

  ```
  Set-ProvImageDefinition -ImageDefinitionUid <Guid> [-Description
  <string>]
  ```

または、,

```
Set-ProvImageDefinition -ImageDefinitionName <string> [-Description
<string>]
```

- `Set-ProvImageVersion` コマンドを使用してイメージバージョンを編集します。例：

```
Set-ProvImageVersion -ImageVersionUid <Guid> [-Description <string>]
```

または、,

```
Set-ProvImageVersion -ImageDefinitionName <string> -ImageVersionNumber
<int> [-Description <string>]
```

イメージ定義、イメージバージョン、準備済みイメージバージョンスペック、およびプロビジョニングスキームの詳細を取得する

- `Get-ProvImageDefinition` コマンドを使用してイメージ定義の詳細を取得します。例:

```
Get-ProvImageDefinition [-ImageDefinitionName <string>] [-
ImageDefinitionUid <Guid>] [-ReturnTotalRecordCount] [-MaxRecordCount
<int>] [-Skip <int>] [-SortBy <string>] [-Filter <string>]
```

- `Get-ProvImageVersion` コマンドを使用してイメージバージョンの詳細を取得します。例:
  - イメージ定義内のイメージバージョンを一覧表示するには、,

    ```
    Get-ProvImageVersion -ImageDefinitionUid <Guid>
    ```

    または、,

    ```
    Get-ProvImageVersion -ImageDefinitionName <string>
    ```

  - イメージバージョンの詳細を取得するには、,

    ```
    Get-ProvImageVersion -ImageVersionUid <Guid>
    ```

    または、,

```
Get-ProvImageVersion -ImageDefinitionName <string>
-ImageVersionNumber <int>
```

- `Get-ProvImageVersionSpec` コマンドを使用して準備済みイメージバージョンスペックを取得します。例:
  - イメージバージョン内のすべての準備済みイメージバージョンスペックを一覧表示するには、,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid>
```

  - 準備済みイメージバージョンスペック内のマスターイメージバージョンスペックを一覧表示するには、,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "None"'
```

  - マスターイメージに関連付けられているイメージバージョン内の準備済みイメージバージョンスペックを一覧表示するには、,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"'
```

  - イメージバージョン内で正常に準備されたイメージバージョンのスペックを取得するには、,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" -and ImageVersionSpecStatus
-eq "Complete"'
```

  - 準備されたイメージバージョンのスペック詳細を取得するには、,

```
Get-ProvImageVersionSpec -ImageVersionSpecUid <Guid>
```

- `Get-ProvScheme` コマンドを使用してプロビジョニングスキームの詳細を取得します。例:

```
Get-ProvScheme [[-ProvisioningSchemeName] <String>] [-
ProvisioningSchemeUid <Guid>] [-ScopeId <Guid>] [-ScopeName <String>]
[-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-
SortBy <String>] [-Filter <String>] [-FilterScope <Guid>]
```

- `Get-ProvSchemeImageVersionSpecHistory` コマンドを使用してプロビジョニングスキームの準備されたイメージバージョンのスペック履歴を取得します。例:

```
Get-ProvSchemeImageVersionSpecHistory [-ProvisioningSchemeName
<String>] [-ProvisioningSchemeUid <Guid>] [-ImageVersionSpecUid <Guid>]
[-ImageVersionSpecHistoryUid <Guid>] [-ReturnTotalRecordCount] [-
MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter
<String>] [-FilterScope <Guid>]
```

マシンカタログを作成する

重要:

Citrix Virtual Apps and Desktops™ 7 2006以降、現在の展開で以下のいずれかのテクノロジーを使用している場合、それらのテクノロジーを使用するサポート終了（EOL）項目を削除した後にのみ、現在のリリースにアップグレードできます。

- パーソナルvDisk (PvD)
- AppDisks™
- パブリッククラウドホストの種類：Citrix CloudPlatform、Microsoft Azure Classic

詳細については、「PvD、AppDisks、およびサポートされていないホストの削除」を参照してください。

注:

Citrix Virtual Apps and Desktopsの展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb

> Studioのみを扱います。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> 展開にパブリッククラウドホスト接続を使用する場合は、新規インストールまたは現在のリリースへのアップグレードを完了するためにハイブリッド権限ライセンスが必要です。

インストーラーがサポートされていないテクノロジーまたはハイブリッド権限ライセンスのないホスト接続を1つ以上検出すると、アップグレードは一時停止または停止します。説明メッセージが表示されます。インストーラーログには詳細が含まれています。詳細については、「展開のアップグレード」を参照してください。

はじめに

物理マシンまたは仮想マシンのコレクションは、マシンカタログと呼ばれる単一のエンティティとして管理されます。カタログ内のすべてのマシンは、マルチセッションOSまたはシングルセッションOS、およびWindowsまたはLinuxマシンという同じ種類のオペレーティングシステムを持っています。

Web Studioは、サイトを作成した後、最初のマシンカタログを作成するようにガイドします。最初のカタログを作成した後、Web Studioは最初のデリバリーグループを作成するようにガイドします。後で、作成したカタログを変更したり、さらにカタログを作成したりできます。

> **ヒント:**
>
> 既存の展開をアップグレードすると、マシン作成サービス (MCS) ストレージ最適化 (MCS I/O) 機能が有効になり、追加の構成は不要です。Virtual Delivery Agent (VDA) と Delivery Controller のアップグレードによって、MCS I/O のアップグレードが処理されます。

概要

VM のカタログを作成するときは、それらの VM をプロビジョニングする方法を指定します。Machine Creation Services™ (MCS) を使用できます。または、独自のツールを使用してマシンを提供することもできます。

考慮事項:

- MCS は、仮想マシンイメージからの単一のシステムディスクをサポートします。そのイメージに接続されている残りのデータディスクは無視されます。

- MCS を使用して VM をプロビジョニングする場合、カタログに同一の VM を作成するためにマスターイメージ (またはイメージのスナップショット) を提供します。カタログを作成する前に、まずツールを使用してマスターイメージを作成および構成します。このプロセスには、イメージへの Virtual Delivery Agent (VDA) のインストールが含まれます。次に、Web Studio でマシンカタログを作成します。そのイメージ (またはスナップショット) を選択し、カタログに作成する VM の数を指定し、追加情報を構成します。
- マシンがすでに利用可能な場合でも、それらのマシン用に1つ以上のマシンカタログを作成する必要があります。
- PowerShell SDK を直接使用してカタログを作成する場合、イメージまたはスナップショットではなく、ハイパーバイザーテンプレート (**VMTemplates**) を指定できます。
- テンプレートを使用してカタログをプロビジョニングすることは、実験的な機能と見なされます。この方法を使用すると、仮想マシンの準備が失敗する可能性があります。その結果、テンプレートを使用してカタログを公開することはできません。

MCSまたはCitrix Provisioning™を使用して最初のカタログを作成する場合、サイトを作成したときに構成したホスト接続を使用します。後で（最初のカタログとデリバリーグループを作成した後）、その接続に関する情報を変更したり、さらに接続を作成したりできます。

カタログ作成ウィザードを完了すると、正しく構成されていることを確認するためにテストが自動的に実行されます。テストが完了すると、テストレポートを表示できます。Web Studio からいつでもテストを実行できます。

> **注:**
>
> MCS は Windows 10 IoT Core および Windows 10 IoT Enterprise をサポートしていません。詳細については、Microsoft サイト を参照してください。

> Citrix Provisioningツールの技術的な詳細については、Citrix Virtual Apps and Desktops Image Managementを参照してください。

RDS ライセンスチェック

Web Studioは現在、WindowsマルチセッションOSマシンを含むマシンカタログの作成中に、有効なMicrosoft RDSライセンスのチェックを実行しません。Windows **マルチセッションOSマシン**のMicrosoft RDSライセンスのステータスを表示するには、Citrix Directorに移動します。Microsoft RDSライセンスのステータスは、**マシン詳細**パネルで確認できます。このパネルは、**マシン詳細**

とユーザー詳細ページにあります。詳細については、「Microsoft RDSライセンスの健全性」を参照してください。

VDA登録

ブローカーセッションを起動する際には、VDAをDelivery Controller™に登録する必要があります。未登録のVDAは、利用可能なリソースの利用率低下につながる可能性があります。VDAが登録されない理由はさまざまですが、その多くは管理者がトラブルシューティングできます。Web Studioは、カタログ作成ウィザードで、またカタログからデリバリーグループにマシンを追加した後で、トラブルシューティング情報を提供します。

ウィザードを使用して既存のマシンを追加すると、コンピューターアカウント名のリストに、各マシンがカタログに追加するのに適しているかどうかが示されます。各マシンの横にあるアイコンにカーソルを合わせると、そのマシンに関する情報メッセージが表示されます。

メッセージで問題のあるマシンが特定された場合は、そのマシンを削除するか、追加します。たとえば、マシンに関する情報が取得できない可能性があることを示すメッセージが表示された場合でも、そのマシンを追加します。

詳細については、以下を参照してください。

- VDA登録のトラブルシューティングガイダンスについては、CTX136668
- VDAのバージョンと機能レベル
- VDA登録方法

MCSカタログ作成の概要

カタログ作成ウィザードで情報を提供した後の、デフォルトのMCSアクションの概要を以下に示します。

- マスターイメージ（スナップショットではない）を選択した場合、MCSはスナップショットを作成します。
- MCSはスナップショットの完全なコピーを作成し、ホスト接続で定義された各ストレージの場所にそのコピーを配置します。
- MCSはマシンをActive Directoryに追加し、一意のIDを作成します。
- MCSは、ウィザードで指定された数のVMを作成し、各VMに2つのディスクを定義します。VMごとの2つのディスクに加えて、マスターも同じストレージの場所に保存されます。複数のストレージの場所が定義されている場合、それぞれが次のディスクタイプを取得します。
    - 作成されたばかりのVM間で共有される、読み取り専用のスナップショットの完全なコピー。

- 各VMに一意のIDを付与する、16 MBの一意のIDディスク。各VMはIDディスクを1つ取得します。
- VMへの書き込みを保存するための一意の差分ディスク。このディスクはシンプロビジョニングされており（ホストストレージがサポートしている場合）、必要に応じてマスターイメージの最大サイズまで増加します。各VMは差分ディスクを取得します。差分ディスクはセッション中に加えられた変更を保持します。専用デスクトップの場合は永続的です。プールされたデスクトップの場合、デリバリーコントローラーを介した再起動のたびに削除され、新しいものが作成されます。

あるいは、静的デスクトップを配信するためにVMを作成する際、カタログ作成ウィザードの**マシン**ページで、シック（完全コピー）VMクローンを指定できます。完全クローンは、すべてのデータストアにマスターイメージを保持する必要はありません。各VMは独自のファイルを持っています。

MCSストレージに関する考慮事項

MCSのストレージソリューション、構成、容量を決定する際には多くの要因があります。以下の情報は、ストレージ容量に関する適切な考慮事項を提供します。

容量に関する考慮事項:

- ディスク

  DeltaまたはDifferencing (Diff) ディスクは、ほとんどのMCS展開において、各VMで最大のスペースを消費します。MCSによって作成される各VMには、作成時に最低2つのディスクが割り当てられます。

  - Disk0 = 差分ディスク: マスターベースイメージからコピーされたOSを含みます。
  - Disk1 = IDディスク: 16 MB - 各VMのActive Directoryデータを含みます。

  製品が進化するにつれて、特定のユースケースや機能の消費を満たすために、さらに多くのディスクを追加する必要があるかもしれません。例：

  - MCS Storage Optimizationは、各VMにライトキャッシュスタイルのディスクを作成します。
  - MCSは、前のセクションで説明した差分ディスクのシナリオとは対照的に、フルクローンを使用する機能を追加しました。

  ハイパーバイザーの機能も考慮に入れる必要があるかもしれません。例:

  - 「XenServer IntelliCache」(/ja-jp/citrix-hypervisor/storage/intellicache.html)は、各XenServerのローカルストレージにリードディスクを作成します。このオプションにより、

共有ストレージの場所に保持されている可能性のあるマスターイメージに対するIOPSを節約できます。

- ハイパーバイザーのオーバーヘッド

  ハイパーバイザーの種類によって、VMにオーバーヘッドを発生させる特定のファイルが使用されます。ハイパーバイザーは、管理および一般的なログ記録操作にもストレージを使用します。以下のオーバーヘッドを含めるための領域を計算してください。

  - ログファイル
  - ハイパーバイザー固有のファイル。例:
    - VMwareは、**VMストレージ**フォルダーにファイルを追加します。VMwareのベストプラクティスを参照してください。
    - 仮想マシンの合計サイズ要件を計算します。仮想ディスクに20 GB、スワップファイルに16 GB、ログファイルに100 MBを使用し、合計36.1 GBを消費する仮想マシンを考慮してください。
  - XenServerのスナップショット; VMwareのスナップショット。

- プロセスオーバーヘッド

  カタログの作成、マシンの追加、カタログの更新には、それぞれ固有のストレージへの影響があります。例:

  - 初期カタログ作成では、ベースディスクのコピーを各ストレージの場所にコピーする必要があります。
    - また、一時的に準備用VMを作成する必要があります。
  - カタログにマシンを追加しても、ベースディスクを各ストレージの場所にコピーする必要はありません。カタログの作成は、選択された機能によって異なります。
  - カタログを更新すると、各ストレージの場所に余分なベースディスクが作成されます。カタログの更新では、カタログ内の各VMが一定期間2つの差分ディスクを持つため、一時的なストレージピークも発生します。

その他の考慮事項：

- **RAMサイジング：** I/O最適化ディスク、ライトキャッシュ、スナップショットファイルなど、特定のハイパーバイザーファイルとディスクのサイズに影響します。
- **シンプロビジョニング/シックプロビジョニング:** シンプロビジョニング機能があるため、NFSストレージが推奨されます。

Machine Creation Services (MCS) ストレージ最適化

MCS I/Oと呼ばれるMachine Creation Services (MCS) ストレージ最適化機能では、次のようになります。

- ライトキャッシュコンテナはCitrix Provisioningと同じ機能である*ファイルベース*です。たとえば、Citrix Provisioningのライトキャッシュファイル名は`D:\vdiskdif.vhdx`で、MCS I/Oのライトキャッシュファイル名は`D:\mcsdif.vhdx`です。
- ライトキャッシュディスクに書き込まれるWindowsクラッシュダンプファイルのサポートを含めることで、診断の改善を実現します。
- MCS I/Oは、最適な多層ライトキャッシュソリューションを提供するために、*RAMにキャッシュし、ハードディスクにオーバーフローする*テクノロジーを保持しています。この機能により、管理者は各層（RAMとディスク）のコストとパフォーマンスのバランスを取り、目的のワークロードの期待に応えることができます。

書き込みキャッシュ方式を*ディスクベース*から*ファイルベース*に更新するには、次の変更が必要です。

1. MCS I/OはRAMのみのキャッシュをサポートしなくなりました。マシンカタログ作成時にWeb Studioでディスクサイズを指定してください。
2. VMライトキャッシュディスクは、VMを初めて起動するときに自動的に作成およびフォーマットされます。VMが起動すると、ライトキャッシュファイル`mcsdif.vhdx`がフォーマットされたボリューム`MCSWCDisk`に書き込まれます。
3. ページファイルはこのフォーマットされたボリューム`MCSWCDisk`にリダイレクトされます。結果として、このディスクサイズはディスク領域の合計量を考慮します。これには、ディスクサイズと生成されたワークロードの差分に加えて、ページファイルのサイズが含まれます。これは通常、VMのRAMサイズに関連付けられます。

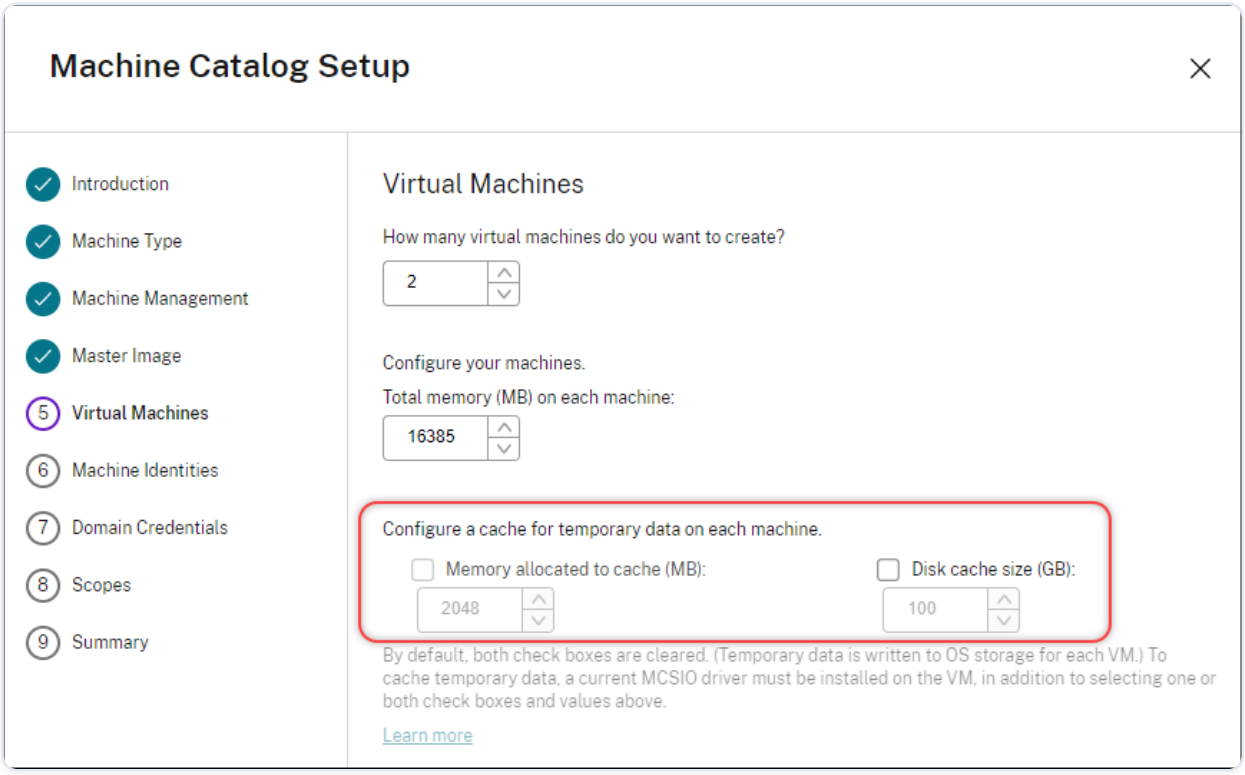
MCSストレージ最適化の更新を有効にする

MCS I/Oストレージ最適化機能を有効にするには、Delivery ControllerとVDAをCitrix Virtual Apps and Desktopsの最新バージョンにアップグレードしてください。

> **注:**
>
> MCS I/Oが有効になっている既存の展開をアップグレードする場合、追加の構成は不要です。VDAとDelivery ControllerのアップグレードがMCS I/Oのアップグレードを処理します。

MCS ストレージ最適化の更新を有効にする際は、次の点を考慮してください。

- マシンカタログを作成する際、管理者は RAM とディスクサイズを構成できます。



- 既存のマシンカタログを、バージョン1903用に構成されたVDAを含む新しいVMスナップショットに更新すると、次の動作が発生します。新しいスナップショットは、既存のカタログのRAMおよびディスクサイズに対するMCS I/O設定を継続して使用します。既存のRAWディスクはフォーマットされます。

重要:

MCSストレージ最適化は、Citrix Virtual Apps and Desktopsバージョン1903で変更されました。このリリースでは、ファイルベースのライトキャッシュテクノロジーがサポートされ、パフォーマンスと安定性が向上しています。MCS I/Oによって提供される新しい機能は、以前のCitrix Virtual Apps and Desktopsリリースと比較して、より高いライトキャッシュストレージ要件を必要とする場合があります。Citrixは、割り当てられたワークフローと追加のページファイルサイズに対して十分なディスク容量があることを確認するために、ディスクサイズを再評価することを推奨します。ページファイルサイズは通常、システムRAMの量に関連しています。既存のカタログディスクサイズが不十分な場合は、マシンカタログを作成し、より大きなライトキャッシュディスクを割り当ててください。

MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てる

MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てることができます。この実装により、使用するアプリケーションのドライブ文字とMCS I/Oライトバックキャッシュディスクのドライブ文字との間の競合を回避できます。MCS I/Oライトバックキャッシュディスクにドライブ文字を割り当てるには、PowerShellコマンドを使用できます。サポートされているハイパーバイザーは、Azure、GCP、VMware、SCVMM、およびXenServerです。

> **注:**
>
> この機能には、VDAバージョン2305以降が必要です。

制限事項

- Windowsオペレーティングシステムのみに適用
- ライトバックキャッシュディスクに適用可能なドライブ文字：`E`から`Z`
- Azure一時ディスクがライトバックキャッシュディスクとして使用されている場合は適用されません
- 新しいマシンカタログを作成する場合にのみ適用されます

ライトバックキャッシュディスクにドライブ文字を割り当てる

ライトバックキャッシュディスクにドライブ文字を割り当てるには：

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. まだ作成されていない場合は、IDプールを作成します。
4. プロパティ`WriteBackCacheDriveLetter`を指定して、`New-ProvScheme`コマンドを使用してプロビジョニングスキームを作成します。例：

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "<name>" `

-IdentityPoolName $schemeName `

-ProvisioningSchemeName $schemeName `
```

```
-InitialBatchSizeHint 1 `

-UseWriteBackCache -WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `

-MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
resources.resourcegroup\MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxxx2130aa
145ec77.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\name\
\virtualprivatecloud.folder\\East US.region\
\virtualprivatecloud.folder\\abcd-resources.resourcegroup\\abcd-
resources-vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.folder\
\Standard_D2s_v5.serviceoffering" `

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS"/>

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk"
Value="false" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
Value="false" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-
```

```
group1" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

5. カタログの作成を完了します。詳細については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

マスターイメージを準備する

接続ホストの作成については、「接続とリソース」を参照してください。

マスターイメージには、オペレーティングシステム、仮想化されていないアプリケーション、VDA、およびその他のソフトウェアが含まれています。

知っておくと良いこと:

- マスターイメージは、クローンイメージ、ゴールデンイメージ、ベースVM、またはベースイメージとも呼ばれることがあります。ホストベンダーは異なる用語を使用します。
- 作成されるマシンの数に対応できる十分なプロセッサ、メモリ、ストレージがホストにあることを確認してください。
- デスクトップおよびアプリケーションに必要なハードディスク容量を正しく構成してください。この値は、後で変更したり、マシンカタログで変更したりすることはできません。
- Remote PC Accessマシンカタログでは、マスターイメージは使用されません。

マスターイメージに以下のソフトウェアをインストールして構成します:

- ハイパーバイザー用の統合ツール（Citrix VM Tools、Hyper-V Integration Services、VMware toolsなど）。この手順を省略すると、アプリケーションやデスクトップが正しく機能しない可能性があります。
- VDA。Citrixは、最新機能にアクセスできるように、最新バージョンをインストールすることを推奨します。マスターイメージにVDAをインストールしないと、カタログ作成が失敗します。
- 必要に応じて、ウイルス対策ソフトウェアや電子ソフトウェア配布エージェントなどのサードパーティツール。ユーザーとマシンタイプに適した設定（更新機能など）でサービスを構成します。

- 仮想化しないサードパーティアプリケーション。Citrixはアプリケーションの仮想化を推奨しています。仮想化により、アプリケーションの追加または再構成後にマスターイメージを更新する必要がなくなるため、コストが削減されます。また、インストールされるアプリケーションが少ないほど、マスターイメージのハードディスクサイズが小さくなり、ストレージコストを節約できます。
- App-Vアプリケーションを公開する予定がある場合は、推奨設定のApp-Vクライアント。App-VクライアントはMicrosoftから入手できます。
- MCSを使用する場合、Microsoft Windowsをローカライズする際は、ロケールと言語パックをインストールしてください。プロビジョニング中にスナップショットが作成されると、プロビジョニングされたVMはインストールされているロケールと言語パックを使用します。

重要:

MCSを使用している場合は、マスターイメージでSysprepを実行しないでください。

マスターイメージを準備するには：

1. ハイパーバイザーの管理ツールを使用してマスターイメージを作成し、オペレーティングシステム、すべてのサービスパック、および更新プログラムをインストールします。vCPUの数を指定します。PowerShellを使用してマシンカタログを作成する場合も、vCPUの値を指定できます。Web Studioを使用してカタログを作成する場合、vCPUの数を指定することはできません。デスクトップとアプリケーションに必要なハードディスク容量を構成します。この値は後で、またはカタログ内で変更することはできません。
2. ハードディスクがデバイスロケーション0に接続されていることを確認します。ほとんどの標準マスターイメージテンプレートではこのロケーションがデフォルトで構成されていますが、一部のカスタムテンプレートではそうでない場合があります。
3. 上記のソフトウェアをマスターイメージにインストールして構成します。
4. MCSを使用しない場合は、アプリケーションとデスクトップが属するドメインにマスターイメージを参加させます。マスターイメージがマシンが作成されるホストで利用可能であることを確認します。MCSを使用している場合、マスターイメージをドメインに参加させる必要はありません。プロビジョニングされたマシンは、カタログ作成ウィザードで指定されたドメインに参加します。
5. Citrixは、マスターイメージのスナップショットを作成して名前を付けることを推奨します。カタログ作成時にスナップショットではなくマスターイメージを指定した場合、Web Studioはスナップショットを作成しますが、名前を付けることはできません。

ボリュームライセンス認証

MCSは、WindowsオペレーティングシステムとMicrosoft Officeのアクティベーションを自動化および管理するためのボリュームライセンス認証をサポートしています。MCSがサポートするボリュームライセンス認証の3つのモデルは次のとおりです。

- キー管理サービス（KMS）
- Active Directoryベースのアクティベーション（ADBA）
- 複数ライセンス認証キー（MAK）

マシンカタログを作成した後で、アクティベーション設定を変更できます。

キー管理サービス（KMS）

KMSは、専用システムを必要とせず、他のサービスを提供するシステムと簡単に共存できる軽量サービスです。この機能は、Citrixがサポートするすべてのバージョンでサポートされています。イメージ準備中に、MCSはMicrosoft WindowsおよびMicrosoft OfficeのKMSリアームを実行します。コマンド `Set-Provserviceconfigurationdata` を実行してリアームをスキップできます。イメージ準備中のMicrosoft Windows KMSリアームおよびMicrosoft Office KMSリアームの詳細については、「Machine Creation Services: Image Preparation Overview and Fault-Finding」を参照してください。KMSアクティベーションの詳細については、「Activate using Key Management Service」を参照してください。

> **注記：**
>
> コマンド `Set-Provserviceconfigurationdata` の実行後に作成されたすべてのマシンカタログは、コマンドで指定されたものと同じ設定になります。

Active Directoryベースのアクティベーション（ADBA）

ADBAを使用すると、ドメイン接続を介してマシンをアクティブ化できます。マシンはドメインに参加するとすぐにアクティブ化されます。これらのマシンは、ドメインに参加し、ドメインと通信している限り、アクティブ化されたままになります。この機能は、Citrixがサポートするすべてのバージョンでサポートされています。Active Directoryベースのアクティベーションの詳細については、「Active Directory-based activation」を使用してアクティベートするを参照してください。

複数ライセンス認証キー（MAK）

MAKは、Microsoftサーバーの助けを借りてボリュームをアクティブ化し、Windowsシステムを認証する方法です。MicrosoftからMAKキーを購入する必要があります。これには、固定されたアクティベーションカウントが割り当てられています。Windowsシステムがアクティブ化されるたびに、アクティベーションカウントが減少します。システムをアクティブ化する方法は2つあります。

- オンラインアクティベーション：アクティブ化したいWindowsシステムがインターネットにアクセスできる場合、プロダクトキーをインストールすると、システムはWindowsを自動的にアクティブ化します。このプロセスにより、対応するMAKのアクティベーションカウントが1減ります。
- オフラインアクティベーション: Windowsシステムがオンラインアクティベーションのためにインターネットに接続できない場合、MCSはMicrosoftサーバーから確認IDとインストールIDを取得してWindowsシステムをアクティベートします。このアクティベーション方法は、非永続的なマシンカタログに役立ちます。

> **注：**
>
> - MCSはMAKを使用したMicrosoft Officeのアクティベーションをサポートしていません。
> - 必要なVDAの最小バージョンは2303です。

主な要件

- Delivery Controllerはインターネットにアクセスできる必要があります。
- 更新する新しいイメージが元のイメージと異なるMAKキーを持っている場合は、新しいカタログを作成します。
- マスターイメージにMAKキーをインストールします。WindowsシステムにMAKキーをインストールする手順については、「MAKアクティベーションの展開」を参照してください。
- イメージ準備を使用しない場合：

  a. `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`の下にレジストリDWORD値`Manual`を追加します。

  b. 値を`1`に設定します。

アクティベーション数

MAKキーの残りのアクティベーション数を確認したり、VMが2つ以上のアクティベーションを消費しているかどうかを確認したりするには、ボリュームアクティベーション管理ツール（VAMT）を使用します。「VAMTのインストール」を参照してください。

MAKを使用してWindowsシステムをアクティベートする

MAKを使用してWindowsシステムをアクティベートするには：

1. マスターイメージにプロダクトキーをインストールします。この手順で1つのアクティベーションカウントが消費されます。
2. MCSマシンカタログを作成します。
3. イメージ準備を使用しない場合：

   a. `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`の下にレジストリDWORD値`Manual`を追加します。

   b. 値を`1`に設定します。

   この方法では、オンラインアクティベーションのオプションが無効になります。
4. マシンカタログにVMを追加します。
5. VMの電源を入れます。
6. オンラインアクティベーションかオフラインアクティベーションかに応じて、Windowsシステムがアクティベートされます。

   - アクティベーションがオンラインの場合、プロダクトキーのインストール後にWindowsシステムがアクティベートされます。
   - アクティベーションがオフラインの場合、MCSはプロビジョニングされたVMと通信してWindowsシステムのアクティベーションステータスを取得します。その後、MCSはMicrosoftサーバーから確認IDとインストール済みIDを取得します。これらのIDはWindowsシステムのアクティベートに使用されます。

トラブルシューティング

プロビジョニングされたVMがインストール済みのMAKキーでアクティベートされていない場合は、PowerShellウィンドウで`Get-ProvVM`または`Get-ProvScheme`コマンドを実行します。

- `Get-ProvScheme`コマンド：最新のマスターイメージからMCSマシンカタログに関連付けられているパラメーター`WindowsActivationType`を参照してください。

- `Get-ProvVM`コマンド。パラメーター`WindowsActivationType`、`WindowsActivationStatus`、`WindowsActivationStatusErrorCode`、および`WindowsActivationStatusError`を参照してください。

エラーを確認し、問題を解決するための手順を検証できます。

Web Studio を使用してマシンカタログを作成する

カタログを作成する前に:

- このセクションを確認して、選択する項目と提供する情報について学習してください。
- マシンをホストするハイパーバイザー、クラウドサービス、およびその他のリソースへの接続が作成されていることを確認してください。
- マシンをプロビジョニングするためのマスターイメージを作成した場合は、そのイメージに VDA がインストールされていることを確認してください。

カタログ作成ウィザードを開始するには：

1. これが最初に作成するカタログである場合、適切な選択肢（「マシンをセットアップし、アプリとデスクトップを実行するためのマシンカタログを作成する」など）に誘導されます。カタログ作成ウィザードが開きます。
2. 既にカタログを作成しており、別のカタログを作成したい場合は、次の手順に従ってください:

    a. Web Studio にサインインし、左側のペインで **Machine Catalogs** を選択し、アクションバーで **Create Machine Catalog** を選択します。

    b. フォルダーを使用してカタログを整理するには、デフォルトの**Machine Catalogs**フォルダーの下にフォルダーを作成します。詳細については、(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-manage.html#create-a-catalog-folder)を参照してください。

    c. カタログを作成したいフォルダーを選択し、**Create Machine Catalog**をクリックします。カタログ作成ウィザードが開きます。

ウィザードは次の項目について説明します。表示されるウィザードページは、選択内容によって異なります。

オペレーティングシステム

各カタログには、1種類のマシンのみが含まれます。1つ選択してください。

- **マルチセッションOS:** マルチセッションOSカタログは、ホストされた共有デスクトップを提供します。マシンは、サポートされているバージョンのWindowsまたはLinuxオペレーティン

グシステムを実行できますが、カタログに両方を含めることはできません。(そのOSの詳細については、Linux VDAのドキュメントを参照してください。)

- **シングルセッションOS:** シングルセッションOSカタログは、さまざまなユーザーに割り当てることができるVDIデスクトップを提供します。
- **Remote PC Access:** Remote PC Accessカタログは、ユーザーに物理的なオフィスデスクトップマシンへのリモートアクセスを提供します。Remote PC Accessは、セキュリティを提供するためにVPNを必要としません。

マシン管理

このページは、リモートPCアクセスカタログを作成する際には表示されません。

マシン管理ページは、マシンがどのように管理され、マシンの展開にどのツールを使用するかを示します。

カタログ内のマシンをWeb Studio経由で電源管理するかどうかを選択します。

- マシンはWeb Studioを介して電源管理されます。たとえば、VMやブレードPCなどです。このオプションは、ホストへの接続をすでに構成している場合にのみ利用可能です。
- マシンはWeb Studioを介して電源管理されません。たとえば、物理マシンなどです。

マシンがWeb Studioを介して電源管理されることを指定した場合は、VMの作成に使用するツールを選択します。

- Citrix Provisioningテクノロジー
  - **Citrix Machine Creation Services (MCS)** MCSを使用してプロビジョニングおよびイメージ化されたVMのカタログを作成します。MCSは、マスターイメージからクローンされたイメージをそれらのVMにコピーします。
  - **Citrix Provisioning Services (PVS)** MCSを使用してプロビジョニングされ、PVSを使用してイメージ化されたVMのカタログを作成します。これらのVMはPVSターゲットデバイスとして機能し、PVSサーバーは単一の共有ディスクイメージをそれらにストリーミングできます。

> **注:**
>
> - このオプションは、Citrix Cloud™に登録されているPVSサイトでのみ利用可能であり、現在、Azureリソースに限定されています。

    - Citrix Provisioningカタログを作成する際、**ターゲットデバイス**ページで、プロビジョニングするマシンのファームとサイトを選択するためのドロップダウンメニューに、存在しないファームとサイトがリストされている場合があります。回避策として、PowerShellコマンド `Unregister-HypPvsSite` を実行して、データベースからファームとサイトを削除できます。PowerShellコマンドの詳細については、Unregister-HypPvsSite を参照してください。

- **その他のサービスまたはテクノロジー** データセンターに既に存在するマシンを管理するツール。Citrixでは、カタログ内のマシンの一貫性を確保するために、Microsoft System Center Configuration Managerまたはその他のサードパーティ製アプリケーションを使用することをお勧めします。

デスクトップの種類（デスクトップエクスペリエンス）

注:

デスクトップエクスペリエンスページに表示されるオプションは、**マシンの種類**ページで選択したマシンの種類によって異なります。

- **マルチセッションOS**マシンでは、ユーザーはログオンするたびにランダムなデスクトップを割り当てられます。次のいずれかのオプションを選択してください。
    - **はい、仮想デスクトップをホストするマシンのローカルディスクに変更を保存します。**（永続的）
    - **いいえ、すべての変更を破棄し、ユーザーがログオフするときに仮想デスクトップをクリアします。**（非永続的）

    注:

    永続的なマルチセッションマシンでは、ユーザーがデスクトップに加えた変更は保存され、すべての承認済みユーザーがアクセスできます。

- **シングルセッションOS**マシンでは、**デスクトップエクスペリエンス**ページで次のオプションが表示されます。

- **ユーザーがログオンするたびに新しい（ランダムな）デスクトップに接続するようにします。**
- **ユーザーがログオンするたびに同じ（静的な）デスクトップに接続するようにします。**

  静的デスクトップの場合、ユーザーが行った変更をログオフ後に保存するか破棄するかをさらに決定できます。

イメージとマシンプロファイル

このページは、MCSを使用してVMを作成している場合にのみ表示されます。

1. マシンカタログのイメージの種類を選択し、イメージを選択します。利用可能なイメージの種類は2つあります。

   - **マスターイメージ。** イメージ準備プロセスがまだ完了していないイメージです。イメージ準備プロセスは、カタログ作成が開始されると自動的に開始されます。

     > **注:**
     >
     > - MCS を使用している場合、マスターイメージで Sysprep を実行しないでください。
     > - スナップショットではなくマスターイメージを指定した場合、Web Studio はスナップショットを作成しますが、名前を付けることはできません。

   - **準備済みイメージ。** イメージ準備プロセスが完了しており、VM 作成に直接使用できるイメージです。カタログ作成時にマスターイメージではなく準備済みイメージを選択すると、マシンカタログの作成がより高速かつ信頼性の高いものになり、イメージのライフサイクル管理も効率化されます。

     > **注:**
     >
     > - 準備されたイメージを使用して作成されたVMは、ハイバネーションをサポートしていません。
     > - 現在、準備されたイメージを使用してカタログを作成することは、AzureおよびVMware環境でのみ利用可能です。

準備済みイメージの作成方法の詳細については、「イメージ管理（プレビュー）」を参照してください。

イメージを選択する際、必要に応じて、選択したイメージにメモを追加できます。

最新の製品機能を使用できるようにするには、マスターイメージに最新のVDAバージョンがインストールされていることを確認してください。デフォルトの最小VDA選択を変更しないでください。ただし、以前のVDAバージョンを使用する必要がある場合は、VDA versions and functional levelsを参照してください。

ウィザードで以前に選択したマシン管理テクノロジーと互換性のないスナップショットまたはVMを選択すると、エラーメッセージが表示されます。

2. 既存のVMをマシンプロファイルとして使用するには、**Use a machine profile**を選択し、その後、VMを選択します。

> **注記:**
>
> 現在、マシンプロファイルの利用はAzure、AWS、GCP、およびVMware VMに限定されています。

> VMware展開の場合、マシンプロファイルを使用してマシンカタログを作成する際、仮想マシンを保持するフォルダーを指定する必要があります。

仮想マシンフォルダーの場所を指定するには、カタログ作成ウィザードで、**仮想マシン**ページに移動し、**マシンを配置するフォルダーを選択**セクションに移動して仮想マシンフォルダーの場所を選択します。指定しない場合、システムは、選択したマシンプロファイルのフォルダーをデフォルトの場所と見なします。

3. カタログの最小機能レベルを選択します。最新の製品機能を使用できるようにするには、マスターイメージに最新のVDAバージョンがインストールされていることを確認してください。

マシン

リモートPCアクセス カタログを作成している場合、このページは表示されません。

このページのタイトルは、**マシン管理**ページで選択した内容によって異なります: **マシン**、**仮想マシン**、または**VMとユーザー**。

MCSを使用する場合：

- 作成する仮想マシンの数を指定します。作成しない場合は**0**（ゼロ）を入力します。後で、**マシンの追加**を実行して、空のカタログにVMを作成できます。
- 各VMが持つメモリ量（MB単位）を選択します。
- 作成された各VMにはハードディスクがあります。そのサイズはマスターイメージで設定されます。カタログでハードディスクのサイズを変更することはできません。
- 展開に複数のゾーンが含まれている場合、カタログのゾーンを選択できます。
- 静的デスクトップVMを作成している場合、仮想マシンコピーモードを選択します。仮想マシンコピーモードを参照してください。
- vDiskを使用しないランダムデスクトップVMを作成している場合、各マシンの一時データに使用するキャッシュを構成できます。一時データ用のキャッシュの構成を参照してください。

その他のツールを使用する場合：

Active Directory マシンアカウント名を追加（またはリストをインポート）します。VM を追加/インポートした後で、その VM の Active Directory アカウント名を変更できます。**Desktop Experience** ページで静的マシンを指定した場合、追加する各 VM の Active Directory ユーザー名をオプションで指定できます。

名前を追加またはインポートした後、このページにいる間は、**削除**ボタンを使用してリストから名前を削除できます。

他のツールを使用する場合（ただしMCSではない場合）：

追加（またはインポート）された各マシンに表示されるアイコンとツールヒントは、カタログに追加できない可能性のあるマシンや、Delivery Controller に登録できない可能性のあるマシンを特定するのに役立ちます。詳細については、「VDA のバージョンと機能レベル」を参照してください。

仮想マシン作成時にSIDを追加する

新しい仮想マシンを作成する際に、マシンを一意に識別するためにパラメータ `ADAccountSid` を追加できるようになりました。

これを行うには：

1. サポートされているIDタイプでカタログを作成します。
2. `NewProvVM` を使用してカタログにマシンを追加します。例：

```
New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID ")  -
RunAsynchronously
```

ただし、次の条件のマシンをプロビジョニングすることはできません。

- カタログIDプールにないADアカウント
- 利用可能な状態ではないADアカウント

仮想マシンのコピーモード

マシンページで指定するコピーモードによって、MCS がマスターイメージからシン（高速コピー）クローンを作成するか、シック（完全コピー）クローンを作成するかが決まります。（デフォルト = シンクローン）

- 高速コピー クローンを使用して、ストレージの使用効率を高め、マシンの作成を高速化します。
- フルコピー クローンを使用して、データ回復と移行のサポートを強化し、マシン作成後のIOPSを削減できる可能性があります。

VDAのバージョンと機能レベル

カタログの機能レベルは、カタログ内のマシンで利用できる製品機能を制御します。新しい製品バージョンで導入された機能を使用するには、新しいVDAが必要です。 ただし、以前のVDAバージョンのマシンは、そのカタログに登録できません。

マシン（または**デバイス**）ページの下部にあるメニューで、最小VDAレベルを選択できます。これにより、カタログの最小機能レベルが設定されます。デフォルトでは、オンプレミス展開の場合、最新の機能レベルが選択されています。Citrixの推奨に従って、VDAとコアコンポーネントを常に最新バージョンにインストールおよびアップグレードする場合は、この選択を変更する必要はありません。ただし、古いVDAバージョンを使い続ける必要がある場合は、正しい値を選択してください。

Citrix Virtual Apps and Desktopsのリリースには、新しいVDAバージョンが含まれていない場合や、新しいVDAが機能レベルに影響を与えない場合があります。そのような場合、機能レベルは、インストールまたはアップグレードされたコンポーネントよりも古いVDAバージョンを示すことがあります。各リリースの新機能の記事には、デフォルトの機能レベルの変更が示されています。

選択された機能レベルは、その上にあるマシンのリストに影響します。リストでは、各エントリの横にあるツールヒントが、その機能レベルでマシンのVDAがカタログと互換性があるかどうかを示します。

各マシンのVDAが選択された最小機能レベルを満たしていないか、超えていない場合、ページにメッセージが表示されます。ウィザードを続行できます。それらのマシンは、後でControllerに登録できない可能性があります。代わりに、次のことができます。

- 古いVDAを含むマシンをリストから削除し、VDAをアップグレードしてから、カタログに再度追加します。
- 最新の製品機能へのアクセスを妨げる、より低い機能レベルを選択します。

マシンタイプが正しくないためにカタログに追加されなかった場合も、メッセージが表示されます。例としては、サーバーをシングルセッションOSカタログに追加しようとしたり、ランダム割り当て用に作成されたシングルセッションOSマシンを静的マシンのカタログに追加したりする場合があります。

> **重要:**
>
> リリース1811で、追加の機能レベル「**1811（またはそれ以降）**」が追加されました。このレベルは、将来のCitrix Virtual Apps and Desktops機能で使用することを目的としています。「**7.9（またはそれ以降）**」の選択はデフォルトのままです。このデフォルトは、現在すべての展開で有効です。

> **1811 (またはそれ以降)**を選択した場合、そのカタログ内の以前のVDAバージョンはControllerに登録できません。ただし、カタログにバージョン1811以降のサポートされているVDAのみが含まれている場合、それらはすべて登録の対象となります。これには、バージョン1903や現在のリリース以前の他の19XXリリースを含む、後のCitrix Virtual Apps and Desktopsリリース用に構成されたVDAを含むカタログも含まれます。

一時データのキャッシュを構成する

カタログ内のランダムな非永続マシンを管理するためにMCSを使用する場合、マシンのI/Oパフォーマンスを向上させるために、ライトバックキャッシュを有効にできます。

ライトバックキャッシュはMCSIOと呼ばれます。詳細については、こちらのブログ記事を参照してください。

前提条件

ライトバックキャッシュを有効にするには、カタログが次の要件を満たしている必要があります。

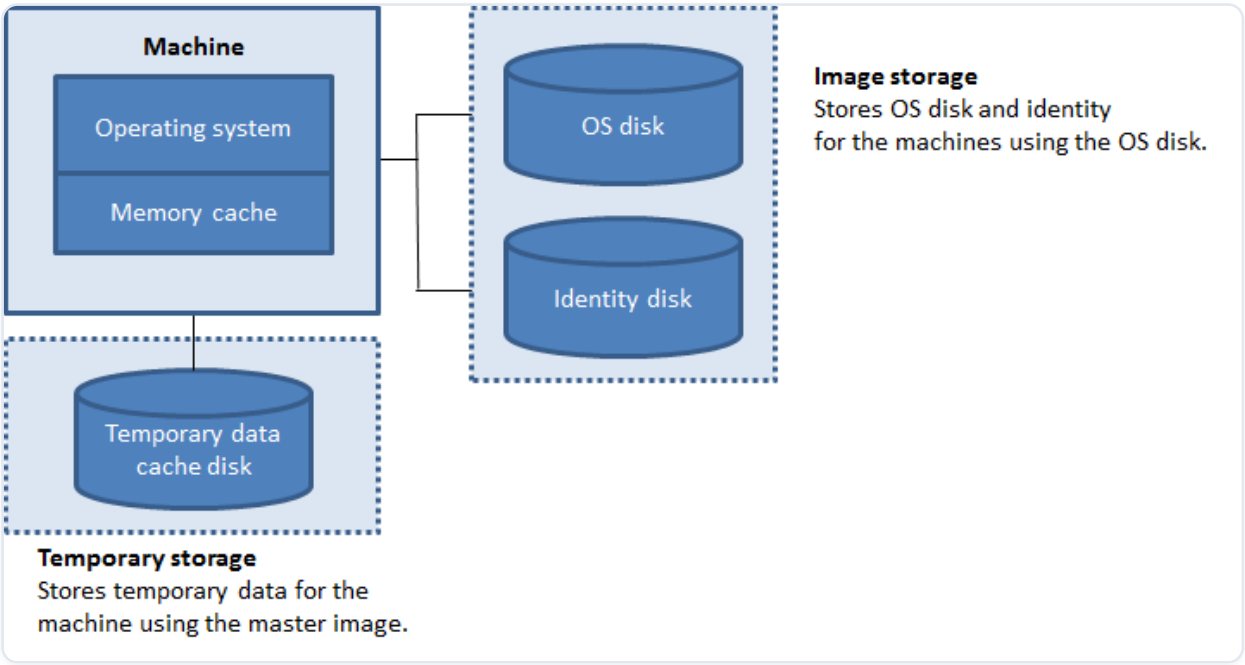
- 一時データ用のストレージを指定する接続を使用していること。詳細については、接続とリソースを参照してください。
- VDAはバージョン7.9以降で、最新のMCSIOドライバーがインストールされている必要があります。

> **注:**
>
> このドライバーのインストールは、VDAをインストールまたはアップグレードする際のオプションです。デフォルトでは、このドライバーはインストールされません。

- ディスクキャッシュのドライブ文字割り当てを有効にするには、VMは次の追加要件を満たしている必要があります。
  - オペレーティングシステム：Windows
  - VDAバージョン：2305以降

考慮事項

- ライトバックキャッシュには、*メモリ*キャッシュと*ディスク*キャッシュがあります。デフォルトでは、接続の種類によってデフォルト値が異なります。通常、デフォルト値はほとんどのケースで十分ですが、次の用途に必要な領域を考慮してください。
  - Windows自体によって作成される一時データファイル（Windowsページファイルを含む）。
  - ユーザープロファイルデータ。
  - ユーザーのセッションに同期されるShareFileデータ。
  - セッションユーザーまたはユーザーがセッション内にインストールする可能性のあるアプリケーションによって作成またはコピーされる可能性のあるデータ。



- ディスクキャッシュのみでメモリキャッシュなしのライトバックキャッシュの構成は非推奨になりました。一時データのキャッシュを有効にするには、**ディスクキャッシュサイズ (GB)** と **キャッシュに割り当てられるメモリ (MB)** を選択し、メモリキャッシュに0より大きいサイズを指定することをお勧めします。一時データは最初にメモリキャッシュに書き込まれます。メモリキャッシュが構成された制限に達すると、最も古いデータは一時データキャッシュディスクに移動されます。
- メモリキャッシュは、各マシンの合計メモリ量の一部です。したがって、**メモリキャッシュサイズ (MB) (推奨)** チェックボックスを有効にする場合は、各マシンの合計メモリ量を増やすことを検討してください。
- **メモリキャッシュサイズ (MB) (推奨)** チェックボックスをオフのままにすると、一時データは最小限のメモリを使用してディスクキャッシュに直接書き込まれます。
- **ディスクキャッシュサイズ (GB)** をデフォルト値から変更すると、パフォーマンスに影響を与える可能性があります。サイズは、ユーザー要件とマシンにかかる負荷に合わせる必要があります。

> **重要:**
>
> ディスクキャッシュの空き容量がなくなると、ユーザーセッションは使用できなくなります。

- **ディスクキャッシュサイズ** チェックボックスをオフにすると、キャッシュディスクは作成されません。この場合、すべての一時データを保持するのに十分な大きさの **キャッシュに割り当て**

られるメモリ の値を指定します。これは、各VMに割り当てるための大量のRAMが利用可能な場合にのみ実現可能です。

- 両方のチェックボックスをオフにすると、一時データはキャッシュされません。各VMの差分ディスク（OSストレージにあります）に書き込まれます。（これは、7.9より前のリリースでのプロビジョニングアクションです。）
- このカタログを使用してAppDiskを作成する予定がある場合は、キャッシュを有効にしないでください。
- マシンカタログ作成後にキャッシュ値を変更することはできません。

NIC

このページは、リモートPCアクセス カタログを作成する際には表示されません。

「**ネットワークインターフェイスカード**」ページで、複数のNICを使用する予定がある場合は、各カードに仮想ネットワークを関連付けます。たとえば、1つのカードを特定のセキュアネットワークへのアクセスに割り当て、別のカードをより一般的に使用されるネットワークへのアクセスに割り当てることができます。このページからNICを追加または削除することもできます。

マシンアカウント

このページは、リモートPCアクセス カタログを作成する場合にのみ表示されます。

「**マシンアカウント**」ページで、ユーザーまたはユーザーグループに対応するActive Directoryマシンアカウントまたは組織単位（OU）を指定します。OU名にスラッシュ（/）を使用しないでください。

OUを追加する際、ドメインがリストに表示されない場合は、次の操作を実行できます。

- 完全一致を使用して検索します。
- すべてのドメインを参照して見つけます。

以前に構成した電源管理接続を選択するか、電源管理を使用しないことを選択できます。電源管理を使用したいが、適切な接続がまだ構成されていない場合は、後でその接続を作成し、マシンカタログを編集して電源管理設定を更新できます。

マシンID

このページは、MCSを使用してVMを作成する場合にのみ表示されます。

カタログ内の各マシンは一意のIDを持つ必要があります。このページでは、カタログ内のマシンのIDを構成できます。マシンはプロビジョニング後にIDに参加します。カタログ作成後にIDタイプを変更することはできません。

このページで設定を構成するための一般的なワークフローは次のとおりです。

1. リストからIDを選択します。
2. アカウントを作成するか既存のアカウントを使用するか、およびそれらのアカウントの場所（ドメイン）を指定します。

次のいずれかのオプションを選択できます。

- **オンプレミスActive Directory**。組織が所有し、その組織に属するActive Directoryアカウントでサインインするマシン。これらはオンプレミスに存在します。
- **ハイブリッドAzure Active Directory参加済み**。組織が所有し、その組織に属するActive Directory Domain Servicesアカウントでサインインするマシン。これらはクラウドとオンプレミスの両方に存在します。要件、制限、考慮事項については、「ハイブリッドAzure Active Directory参加済み」を参照してください。

> **注：**
>
> - ハイブリッドAzure Active Directory参加を使用する前に、Azure環境が前提条件を満たしていることを確認してください。`<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/hybrid-azuread-join-managed-domains>`を参照してください。
> - このオプションでは、マスターイメージがオペレーティングシステムの前提条件を満たしている必要があります。詳細については、Microsoftのドキュメントを参照してください: `<https://learn.microsoft.com/ja-jp/azure/active-directory/devices/concept-azure-ad-join-hybrid>`。

> **重要：**
>
> - IDタイプとして**オンプレミスActive Directory**または**ハイブリッドAzure Active Directory参加済み**を選択した場合、カタログ内の各マシンには対応するActive Directoryコンピューターアカウントが必要です。

> アカウントを作成する場合、マシンが存在するOUにコンピューターアカウントを作成する権限が必要です。カタログ内の各マシンは一意の名前を持つ必要があります。作成するマシンのアカウント命名スキームを指定します。詳細については、「マシンアカウント命名スキーム」を参照してください。

> **注：**
>
> OU名にスラッシュ（`/`）を使用しないようにしてください。

> 既存のアカウントを使用する場合は、アカウントを参照するか、**インポート**をクリックしてアカウント名を含む.csvファイルを指定します。インポートされるファイルの内容は、次の形式を使用する必要があります。

- ADcomputeraccountname.domain

追加するすべてのマシンに対して十分なアカウントがあることを確認してください。Web Studioインターフェイスがそれらのアカウントを管理します。したがって、そのインターフェイスがすべてのアカウントのパスワードをリセットできるようにするか、すべてのアカウントで同じである必要があるアカウントパスワードを指定してください。

物理マシンまたは既存のマシンを含むカタログの場合、既存のアカウントを選択またはインポートし、各マシンをActive Directoryコンピューターアカウントとユーザーアカウントの両方に割り当てます。

マシンアカウント命名スキーム

カタログ内の各マシンには一意の名前が必要です。カタログを作成する際には、マシンアカウントの命名スキームを指定する必要があります。名前の中に現れる連番や文字のプレースホルダーとして、ワイルドカード（ハッシュマーク）を使用します。

命名スキームを指定する際は、以下の規則に注意してください。

- 命名スキームには少なくとも1つのワイルドカードを含める必要があります。すべてのワイルドカードはまとめて配置する必要があります。
- ワイルドカードを含め、名前全体は2文字以上15文字以下である必要があります。少なくとも1つの非数字文字と1つの#（ワイルドカード）文字を含める必要があります。
- 名前にスペースや以下の文字を含めることはできません: `,~!@'$%\^&.()}{\/*?"<>|=+[];:_".`。

- 名前をハイフン (-) で終わらせることはできません。

また、命名スキームを指定する際は、将来の拡張に十分な余裕を持たせてください。次の例を考えてみましょう。「veryverylong#」というスキームで1,000個のマシンアカウントを作成した場合、最後に作成されるアカウント名（veryverylong1000）は16文字になります。したがって、この命名スキームでは、15文字の最大値を超えるマシン名が1つ以上生成されることになります。

連番の値が数字 (0-9) なのか文字 (A-Z) なのかを指定できます。

- **0-9**。選択した場合、指定されたワイルドカードは連番の数字に解決されます。

> **注:**
>
> ワイルドカードが1つの場合、アカウント名は1から始まります。2つの場合、アカウント名は01から始まります。3つの場合、アカウント名は001から始まり、以降同様です。

> **重要:**
>
> - IDの種類として**オンプレミスActive Directory**または**ハイブリッドAzure Active Directory参加済み**を選択した場合、カタログ内の各マシンには対応するActive Directoryコンピューターアカウントが必要です。

アカウントを作成する場合、マシンが存在するOUにコンピューターアカウントを作成する権限が必要です。カタログ内の各マシンは一意の名前を持つ必要があります。作成するマシンのアカウント命名スキームを指定します。詳細については、マシンアカウントの命名スキームを参照してください。

オプションで、アカウント名の開始文字を指定できます。

- **0-9** を選択した場合、アカウントは指定された数字から始まる連番で命名されます。前のフィールドで使用するワイルドカードの数に応じて、1桁以上の数字を入力してください。たとえば、2つのワイルドカードを使用する場合は、2桁以上の数字を入力します。
- **A-Z** を選択した場合、アカウントは指定された文字から始まり、順に命名されます。前のフィールドで使用するワイルドカードの数に応じて、1文字以上の文字を入力します。たとえば、2つのワイルドカードを使用する場合は、2文字以上を入力します。

ドメイン資格情報

資格情報の入力 を選択し、ターゲットのActive Directoryドメインでアカウント操作を実行する権限を持つ管理者の資格情報を入力します。

名前の確認 オプションを使用して、ユーザー名が有効か一意であるかを確認します。このオプションは、たとえば次のような場合に役立ちます。

- 複数のドメインに同じユーザー名が存在する場合。目的のユーザーを選択するよう求められます。
- ドメイン名を思い出せない場合。ドメイン名を指定せずにユーザー名を入力できます。確認が成功すると、ドメイン名が自動的に入力されます。

> **注:**
>
> **マシンID** で選択したIDタイプが **Hybrid Azure Active Directory joined** の場合、入力する資格情報には `Write userCertificate` 権限が付与されている必要があります。

概要、名前、および説明

概要 ページで、指定した設定を確認します。カタログの名前と説明を入力します。この情報はWeb Studioに表示されます。

完了したら、**完了** をクリックしてカタログの作成を開始します。 完了したら、**完了** を選択してカタログの作成を開始します。

マシンカタログ に、新しいカタログがインラインの進行状況バーとともに表示されます。

作成の進行状況の詳細を表示するには：

1. マシンカタログにマウスを合わせます。
2. 表示されるツールチップで、**詳細の表示** をクリックします。

   以下の項目を確認できる段階的な進行状況グラフが表示されます。

   - ステップの履歴
   - 現在のステップの進行状況と実行時間
   - 残りのステップ

MCSの時刻同期

時刻同期は、マスターイメージと、参加しているマシンIDカタログのタイプによって決定されます。マスターイメージとカタログに応じて、次の時刻同期方法が適用されます。

マスターイメージ	カタログ	結果的な時刻同期方法
NDJ	AD またはハイブリッド Azure AD	デフォルトでは NT5DS。マスターイメージのレジストリ設定を使用して、MCS が時刻同期設定を変更するのを無効にできます。
NDJ	NDJ または Azure AD	元の時刻同期設定と同じ
AD またはハイブリッド Azure AD	AD またはハイブリッド Azure AD	元の時刻同期設定と同じ
アジュール AD	アジュール AD	元の時刻同期設定と同じ

注:

元の時刻同期は、以下のレジストリ設定によって制御されており、変更できません。

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config

値: MaxAllowedPhaseOffset, MaxNegPhaseCorrection, and MaxPosPhaseCorrection

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

値: Type

MCSが時刻同期設定を変更しないようにするには、マスターイメージで以下のレジストリ設定の値を設定します。

- `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix`

- 名前: TimeSyncMethodKeep
- 種類: DWORD
- 0 (または、値TimeSyncMethodKeepが構成されていない場合): 元の時刻同期設定を保持しません。
- 1: 元の時刻同期設定とデフォルトのパラメーター値を保持します。

カスタムプロパティの設定に関する重要な考慮事項

カスタムプロパティは、GCP および Azure 環境の `New-ProvScheme` と `Set-ProvScheme` で正しく設定する必要があります。存在しないカスタムプロパティを指定すると、次のエラーメッセージが表示され、コマンドの実行に失敗します。

- Azure の場合: `Invalid property found: <invalid property>. Ensure that the CustomProperties parameter supports the property.`.
- GCP の場合: `Invalid property found: <invalid property>. Ensure that the value supplied for the property is supported in the Hypervisor.`.

トラブルシューティング

> **重要:**

> Web Studio を使用してマシンカタログを作成した後、`Get-ProvTask` PowerShell コマンドを使用してマシンカタログ作成に関連付けられたタスクを取得することはできません。この制限は、カタログが正常に作成されたかどうかにかかわらず、Web Studio がマシンカタログ作成後にそれらのタスクを削除するためです。

> Citrix は、サポートチームがソリューションを提供できるよう、ログを収集することをお勧めします。Citrix Provisioning を使用する場合は、次の手順でログファイルを生成します。

1. マスターイメージで、値 1 (DWORD (32 ビット) 値として) を持つ次のレジストリキーを作成します: `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`。
2. マスターイメージをシャットダウンし、スナップショットを作成します。
3. Delivery Controller で、次の PowerShell コマンドを実行します: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`。
4. そのスナップショットに基づいてカタログを作成します。

5. 準備用VMがハイパーバイザー上に作成されたら、ログインして、C:\のルートから以下のファイルを抽出します: Image-prep.logとPvsVmAgentLog.txt。
6. マシンをシャットダウンすると、その時点で障害が報告されます。
7. イメージ準備マシンの自動シャットダウンを再度有効にするには、次のPowerShellコマンドを実行します: `Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown`。

MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てる

MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てることができます。この実装により、使用するアプリケーションのドライブ文字とMCS I/Oライトバックキャッシュディスクのドライブ文字との競合を回避できます。これを行うには、PowerShellコマンドを使用します。サポートされているハイパーバイザーは、Azure、GCP、VMware、SCVMM、XenServerです。

> **注:**
>
> この機能には、VDAバージョン2305以降が必要です。

制限事項

- Windowsオペレーティングシステムのみに適用
- ライトバックキャッシュディスクに適用可能なドライブ文字: `E`から`Z`
- Azure一時ディスクがライトバックキャッシュディスクとして使用されている場合は適用されません
- 新しいマシンカタログを作成する場合にのみ適用

ライトバックキャッシュディスクにドライブ文字を割り当てる

ライトバックキャッシュディスクにドライブ文字を割り当てるには:

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. まだ作成されていない場合は、IDプールを作成します。詳しくは、カタログの作成を参照してください。

4. `WriteBackCacheDriveLetter` プロパティを持つ `New-ProvScheme` コマンドを使用してプロビジョニングスキームを作成します。例:

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "<name>" `

-IdentityPoolName $schemeName `

-ProvisioningSchemeName $schemeName `

-InitialBatchSizeHint 1 `

-UseWriteBackCache -WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `

-MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
resources.resourcegroup\MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxx2130aa
145ec77.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\name\
\virtualprivatecloud.folder\\East US.region\
\virtualprivatecloud.folder\\abcd-resources.resourcegroup\\abcd-
resources-vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.folder\
\Standard_D2s_v5.serviceoffering" `

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS"/>

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk"
```

```
Value="false" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
Value="false" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-
group1" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

5. カタログの作成を完了します。

MCSマシンカタログを作成する前に構成を検証する

`New-ProvScheme`コマンドの`-validate`パラメーターを使用して、MCSマシンカタログを作成する前に構成設定を検証できます。このPowerShellコマンドをパラメーターと共に実行すると、誤ったパラメーターが使用されている場合や、パラメーターが別のパラメーターと競合している場合に、適切なエラーメッセージが表示されます。その後、エラーメッセージを使用して問題を解決し、PowerShellを使用してMCSマシンカタログを正常に作成できます。現在、この機能はAzure、GCP、およびVMwareの仮想化環境に適用できます。

注:

検証中は、実際のMCSマシンカタログを作成してはなりません。コマンドの結果を使用してエラーを修正し、その後で正常なカタログを作成する必要があります。したがって、`New-ProvScheme`コマンドを実行する際は、架空のIDプール名を使用してください。

構成を検証するには、次の手順を実行します。

1. Delivery ControllerホストからPowerShellウィンドウを開きます。

2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. `New-ProvScheme`コマンドを実行し、`-validate`パラメーターを使用します。コマンドが機能するように、偽のIDプール名を提供します。例:

```
$result =New-ProvScheme  -CleanOnBoot -HostingUnitName "vSanRg"
-IdentityPoolName "mptmpcatalogdemo" -InitialBatchSizeHint 1  -
MasterImageVM "XDHyp:
\HostingUnits\vSanRg\Windows19MasterImage.vm\Citrix_XD_NonMachineProfil
eWin19Machines.snapshot" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vSanRg\\VM Network.network"} -ProvisioningSchemeName
"MachineProfileW10Machines"  -Scope @()

-VMCpuCount 2  -VM

MemoryMB 6143 -MachineProfile "XDHyp:\HostingUnits\vSanRg\TRW-Win11-
tpm-BL-TEMPLATE.template" -TenancyType Shared  -FunctionalLevel "L7_20"
-Validate

$result.TerminatingError | Format-List -Property *
```

エラーメッセージ：

```
ErrorData    : {[[ValidationFailureCount, xxx], [InvalidMemoryValue,
The memory size provided 6143 must be a multiple of 4 MB and must be
greater than or equal to 4 MB.], [InconsistentGuestOsSetting, The
GuestOs setting - windows9_64Guest of the selected machine profile does
not match with the setting - windows2019srv_64Guest of master image.
Please select a machine profile that matches the GuestOs setting of the
master image.], [InconsistentVtpmSetting, The vTPM setting of the
selected machine profile does not match with the selected master image.
Please select a machine profile that matches the vTPM setting of the
master image.], [InconsistentFirmwareSetting, The firmware setting -
efi of the selected machine profile does not match with the setting -
bios of master image. Please select a machine profile that matches the
firmware setting of the master image ErrorId      : ValidationFailure

ErrorMessage : ValidationFailure

Operation    : ValidatingInputs
```

4. 構成設定を検証した後、実際のIDプール名と正しいパラメーターを使用してMCSマシンカタログを作成できます。

次のステップ

特定のクラウドサービスカタログの作成については、以下を参照してください。

- AWSカタログを作成する
- XenServerカタログを作成する
- Google Cloud Platformカタログを作成する
- Microsoft Azureカタログを作成する
- Microsoft System Center Virtual Machine Managerカタログを作成する
- Nutanixカタログを作成する
- VMwareカタログを作成する

これが最初に作成されたカタログである場合、Web Studioはデリバリーグループを作成するように案内します。

設定プロセス全体を確認するには、インストールと構成を参照してください。

Web StudioとPowerShellを使用してCitrix Provisioningカタログを作成できます。 この実装には、次の利点があります。

- MCSとCitrix Provisioningカタログの両方を管理するための単一の統合コンソール。
- ID管理ソリューション、オンデマンドプロビジョニングなど、Citrix Provisioningカタログの新機能があります。

現在、この機能はAzureおよびVMwareワークロードでのみ利用可能です。ただし、VMware環境では、現在PowerShellコマンドのみを使用してカタログを作成できます。詳細については、Citrix StudioでCitrix Provisioningカタログを作成するを参照してください。

詳細情報

- 接続とリソースの作成および管理(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections.html)
- 異なる結合タイプのカタログを作成(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/create-machine-identities-joined-catalogs.html)
- マシンカタログを管理(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-manage.html)

AWSカタログを作成する

マシンカタログの作成では、マシンカタログを作成するウィザードについて説明します。以下の情報では、AWS仮想化環境に固有の詳細について説明します。

> **注:**
>
> AWSカタログを作成する前に、AWSへの接続の作成を完了する必要があります。AWSへの接続を参照してください。

制限事項

Citrix Virtual Apps and Desktops™ 2203 LTSR以降では、MCS AWSプラグインは `DescribeInstanceTypes` AWS APIコールを実行し、それが成功すると、MCSはAPI応答から作成されたインベントリ名を使用します。

したがって、CVAD 1912から2203以降にアップグレードする場合は、AWS上の `DefineInstanceType` 権限を無効にし、`Set-ProvScheme` コマンドを使用して既存のカタログを更新してAWSの命名規則に合わせます。その後、カタログの更新が完了し、サービス提供がAWSの命名規則に一致したら、`DescribeInstanceType` 権限を再度追加します。

イメージ準備中のネットワーク設定

イメージ準備中、元のVMに基づいて準備用仮想マシン（VM）が作成されます。この準備用VMはネットワークから切断されます。準備用VMからネットワークを切断するために、すべてのインバウンドおよびアウトバウンドトラフィックを拒否するネットワークセキュリティグループが作成されます。このネットワークセキュリティグループは永続的に存在し、再利用されます。ネットワークセキュリティグループの名前は `Citrix.XenDesktop.IsolationGroup-GUID` で、GUIDはランダムに生成されます。

AWSテナンシーの構成

AWSは以下のテナンシーオプションを提供します。

- 共有テナンシー（デフォルトタイプ）：異なる顧客の複数のAmazon EC2インスタンスが、同じ物理ハードウェア上に存在する場合があります。
- 専用テナンシー：お客様のEC2インスタンスは、お客様が展開した他のインスタンスと同じハードウェア上でのみ実行されます。他の顧客は同じハードウェアを使用しません。

PowerShellを使用して、MCSでAWS専用ホストをプロビジョニングできます。

PowerShellを使用してAWS専用ホストテナンシーを構成する

PowerShell を介してホストテナンシーが定義されたマシンカタログを作成できます。

Amazon 専用ホストは、 インスタンス容量を持つ物理サーバーであり、完全に専用であるため、既存のソケットごとまたはVMごとのソフトウェアライセンスを使用できます。

専用ホストは、インスタンスタイプに基づいて事前設定された利用率を持っています。たとえば、C4 Large インスタンスタイプの単一の割り当てられた専用ホストは、16 インスタンスの実行に制限されます。詳細については、AWS サイト を参照してください。

AWSホストへのプロビジョニングの要件は次のとおりです。

- インポートされた BYOL (bring your own license) イメージ (AMI)。専用ホストでは、既存のライセンスを使用および管理します。
- プロビジョニング要求を満たすのに十分な利用率を持つ専用ホストの割り当て。
- **自動配置**を有効にします。

PowerShell を使用して AWS の専用ホストにプロビジョニングするには、**New-ProvScheme** コマンドレットでパラメーター `TenancyType` を *Host* に設定して使用します。

詳細については、Citrix Developer Documentation を参照してください。

AMI からマシンプロパティをキャプチャする

AWS で Machine Creation Services (MCS) を使用してマシンをプロビジョニングするためのカタログを作成するときは、そのカタログのマスター/ゴールデンイメージを表す AMI を選択します。その AMI から、MCS はディスクのスナップショットを使用します。以前のリリースでは、マシンにロールやタグを設定したい場合、AWS コンソールを使用して個別に設定していました。この機能はデフォルトで有効になっています。

> **ヒント:**
>
> AWS インスタンスプロパティキャプチャを使用するには、AMI に関連付けられた VM が必要です。

> このプロセスを改善するために、**MCS は** AMI が取得されたインスタンスからプロパティを読み取り、そのマシンの Identity Access Management (IAM) ロールとタグを、特定のカタログ用にプロビジョニングされたマシンに適用します。このオプション機能を使用する場合、カタログ作成プロセスは選択された AMI ソースインスタンスを見つけ、限られたプロパティ

> セットを読み取ります。これらのプロパティは AWS 起動テンプレートに保存され、そのカタログのマシンをプロビジョニングするために使用されます。カタログ内のすべてのマシンは、キャプチャされたインスタンスプロパティを継承します。

キャプチャされるプロパティには以下が含まれます。

- IAM ロール – プロビジョニングされたインスタンスに適用されます。
- タグ - プロビジョニングされたインスタンス、そのディスク、および NIC に適用されます。これらのタグは、S3 バケットとオブジェクト、AMI、スナップショット、起動テンプレートなど、一時的な Citrix® リソースに適用されます。

> **ヒント:**
>
> 一時的な Citrix リソースのタグ付けはオプションであり、カスタムプロパティ `AwsOperationalResourcesTagging` を使用して構成できます。

AWS インスタンスプロパティをキャプチャする

AWS ホスティング接続のプロビジョニングスキームを作成する際に、カスタムプロパティ `AwsCaptureInstanceProperties` を指定することで、この機能を使用できます。

`New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true" …<standard provscheme parameters`

詳細については、Citrix開発者向けドキュメントを参照してください。

> **注:**
>
> `AwsCaptureInstanceProperties` は非推奨です。代わりに、VMのコンピュータープロパティを指定するには、マシンプロファイルを使用することをお勧めします。

マシンプロファイルからマシンプロパティをキャプチャする

MCSを使用してAWSマシンをプロビジョニングするカタログを作成する際、マシンプロファイルを使用して特定のコンピュータープロパティ設定をプリセットできます。

そのためには、次の手順に従います。

1. マシンプロファイルを、このカタログを作成するリソースと同じアベイラビリティゾーンに保存します。
2. カタログ作成ウィザードの**マシンテンプレート**ページで、**マシンプロファイルを使用**を選択します。選択したリソースと同じ利用可能なゾーンにあるマシンプロファイルが表示されます。
3. 必要に応じてマシンプロファイルを選択します。

> **注:**
>
> マシンプロファイルまたはAMIのいずれかを使用して、マシンプロパティをキャプチャできます。Web Studioで**マシンプロファイルを使用**を選択すると、**仮想マシンにマシンテンプレートプロパティを適用**オプションが自動的に非表示になります。

AWS運用リソースにタグを付ける

MCSを使用してAWSにマシンをプロビジョニングするためのカタログを作成する際、IAMロールとタグプロパティをそれらのマシンに適用するかどうかを制御できます。また、マシンタグを運用リソースに適用するかどうかも制御できます。

Amazon Machine Image (AMI) は、Amazon Cloud環境内で仮想マシンを作成するために使用される仮想アプライアンスの一種で、一般にEC2と呼ばれます。AMIを使用して、EC2環境を使用するサービスを展開します。MCS for AWSを使用してマシンをプロビジョニングするためのカタログを作成する際、そのカタログのゴールデンイメージとして機能する**AMI**を選択します。

> **重要:**
>
> インスタンスプロパティと起動テンプレートをキャプチャしてカタログを作成することは、運用リソースのタグ付けを使用するために必要です。

> AWSカタログを作成するには、まずゴールデンイメージとするインスタンスのAMIを作成する必要があります。MCSはそのインスタンスからタグを読み取り、起動テンプレートに組み込みます。その後、起動テンプレートのタグは、AWS環境で作成されたすべてのCitrixリソースに適用されます。これには以下が含まれます。

- 仮想マシン
- VMディスク
- VMネットワークインターフェース

- S3バケット
- S3オブジェクト
- 起動テンプレート
- AMI

運用リソースにタグを付ける

PowerShellを使用してリソースにタグを付けるには：

1. DDCホストからPowerShellウィンドウを開きます。
2. コマンド `asnp citrix` を実行して、Citrix固有のPowerShellモジュールをロードします。

プロビジョニングされたVMのリソースにタグを付けるには、新しいカスタムプロパティ `AwsOperationalResourcesTagging` を使用します。このプロパティの構文は次のとおりです。

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true;
AwsOperationalResourcesTagging,true" …<standard provscheme parameters>
```

VM上のタグをコピーする

マシンプロファイルで指定されたNICおよびディスク（IDディスク、ライトバックキャッシュディスク、OSディスク）のタグを、MCSマシンカタログで新しく作成されたVMにコピーできます。これらのタグは、マシンプロファイルのソース（AWS VMインスタンスまたはAWS起動テンプレートバージョン）のいずれかで指定できます。この機能は、永続および非永続マシンカタログとVMに適用されます。

注:

- AWS EC2コンソールでは、**起動テンプレートバージョンリソースタグ**の下に**ネットワークインターフェースのタグ付け**の値が表示されません。ただし、PowerShellコマンド `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` を実行してタグの仕様を確認できます。
- マシンプロファイルソース（VMまたは起動テンプレートバージョン）に2つのネットワークインターフェース（eni-1とeni-2）があり、eni-1にタグt1、eni-2にタグt2がある場合、VMは両方のネットワークインターフェースのタグを取得します。

マシンプロファイルを使用してカタログを作成する

マシンプロファイルを使用して、EC2インスタンス（VM）または起動テンプレートバージョンからハードウェアプロパティをキャプチャし、プロビジョニングされたマシンに適用できます。キャプチャされるプロパティには、たとえば、EBSボリュームプロパティ、インスタンスタイプ、EBS最適化、CPUオプション、テナンシータイプ、ハイバネーション機能、およびその他のサポートされているAWS構成が含まれます。

AWS EC2インスタンス（VM）またはAWS起動テンプレートバージョンをマシンプロファイルの入力として使用できます。

> **注：**
>
> - EBSボリュームプロパティは、マシンプロファイルからのみ派生します。
> - MCSは、GP3ボリュームタイプのIDディスクを持つVMをプロビジョニングします。GP3ボリュームタイプはAWSが提供する最も安価なオプションであるため、この機能はコストを最小限に抑えます。この実装は、新しいカタログに追加されたVMと、既存のカタログに追加された新しいVMにのみ適用されます。この機能より前に作成された既存のVMは、IDディスクがリセットされない限り、GP2ボリュームタイプのIDディスクを引き続き使用します。

重要な考慮事項

MCSマシンカタログの作成時における重要な考慮事項：

- `New-ProvScheme`および`Set-ProvScheme`コマンドでマシンハードウェアプロパティパラメータを追加した場合、パラメータで指定された値はマシンプロファイル内の値を上書きします。
- `AwsCaptureInstanceProperties`を`true`として設定し、`MachineProfile`プロパティを設定しない場合、IAMロールとタグのみがキャプチャされます。
- `AwsCaptureInstanceProperties`と`MachineProfile`の両方を同時に設定することはできません。

  > **注：
  >
  > `AwsCaptureInstanceProperties`は非推奨です。

- マシンプロファイルが提供されていない場合は、以下のプロパティの値を明示的に指定する必要があります。
  - セキュリティグループ
  - ENI または仮想ネットワーク
- `AwsOperationalResourcesTagging` は、`AwsCaptureInstanceProperties` を有効にするか、マシンプロファイルを指定した場合にのみ有効にできます。

MCSマシンカタログの作成後における重要な考慮事項：

- マシンプロファイルベースのカタログから非マシンプロファイルベースのカタログにカタログを変更することはできません。

マシンプロファイルを使用してマシンカタログを作成する

マシンプロファイルを使用してマシンカタログを作成するには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. まだ作成されていない場合は、IDプールを作成します。例：

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain abcdf -NamingSchemeType Numeric
```

4. New-ProvSchemeコマンドを実行します。例：

```
New-ProvScheme -ProvisioningSchemeName demet-test-1

-HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1

-IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4

-CleanOnBoot

-MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-demet-
ami.0 (ami-0ca813xxxxxx061ef).template'

-MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-
east-1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).vm'
```

5. カタログの作成を完了します。詳しくは、「Citrix PowerShell SDK」を参照してください。

マシンプロファイルを更新する

マシンプロファイルで最初にプロビジョニングされたカタログのマシンプロファイルを更新するには、次の手順を実行します。MCSマシンカタログを編集する際に、マシンプロファイルソースのテナンシータイプとハイバネーション機能を変更することもできます。

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme `

-ProvisioningSchemeUid "<ID" `

-MachineProfile "XDHyp:\HostingUnits\abc\us-
east-1a.availabilityzone\citrix-cvad-machineprofile-instance
(i-0xxxxxxxx).vm"
```

起動テンプレートバージョンでカタログを作成する

起動テンプレートバージョンをマシンプロファイル入力として使用して、MCSマシンカタログを作成できます。また、マシンプロファイルカタログの入力をVMから起動テンプレートバージョンへ、または起動テンプレートバージョンからVMへ更新することもできます。

AWS EC2コンソールでは、起動テンプレートのインスタンス構成情報をバージョン番号とともに提供できます。マシンカタログの作成または更新時に起動テンプレートバージョンをマシンプロファイル入力として指定すると、その起動テンプレートバージョンのプロパティがプロビジョニングされたVDA VMにコピーされます。

以下のプロパティは、マシンプロファイル入力を使用するか、`New-ProvScheme`または`Set-ProvScheme`コマンドで明示的にパラメーターとして提供できます。`New-ProvScheme`または`Set-ProvScheme`コマンドで提供された場合、これらのプロパティのマシンプロファイル値よりも優先されます。

- サービスオファリング
- ネットワーク
- セキュリティグループ
- テナンシータイプ

> **注:**

> マシンプロファイルの起動テンプレートでサービス提供が指定されていない場合、または `New-ProvScheme` コマンドのパラメーターとして指定されていない場合、適切なエラーが発生します。

> 起動テンプレートバージョンをマシンプロファイルの入力として使用してカタログを作成するには:

1. **PowerShell** ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。
3. 起動テンプレートの起動テンプレートバージョンの一覧を取得します。例:

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate> ls |
Select FullPath
```

4. 作成されていない場合は、ID プールを作成します。例:

```
New-AcctIdentityPool `

-IdentityPoolName "abc11" `

-NamingScheme "abc1-##" `

-NamingSchemeType Numeric `

-Domain "citrix-xxxxxx.local" `

-ZoneUid "xxxxxxxx" `
```

5. 起動テンプレートバージョンをマシンプロファイルの入力として使用してプロビジョニングスキームを作成します。例:

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `
```

```
-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-persistent-
vda-win2022 (ami-0axxxxxxxxxx).template" `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

6. プロビジョニングスキームをブローカーカタログとして登録します。例:

```
New-BrokerCatalog -Name "MPLT1" `

-AllocationType Random `

-Description "Machine profile catalog" `

-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `

-ProvisioningType Mcs `

-SessionSupport MultiSession `

-PersistUserChanges Discard
```

7. カタログの作成を完了します。詳細については、「Citrix PowerShell SDK」を参照してください。

マシンプロファイルカタログの入力を、VM から起動テンプレートバージョンへ、または起動テンプレートバージョンから VM へ更新することもできます。例:

- マシンプロファイルカタログの入力をVMから起動テンプレートバージョンへ更新するには：

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxx
(1).launchtemplateversion"
```

- マシンプロファイルカタログの入力を起動テンプレートバージョンからVMへ更新するには：

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-
east-1a.availabilityzone\apollo-non-persistent-vda-win2022-2
(i-08xxxxxxxx).vm"
```

OSディスクとIDディスクを暗号化する

OSディスクとIDディスクの暗号化に使用できるAWS KMSキー（カスタマー管理キーとAWS管理キー）を使用して、永続的および非永続的なVMカタログを作成できます。

- AWS管理キーは毎年自動的にローテーションされます。
- カスタマー管理キーは自動ローテーションのオプションであり、手動で管理できます。

KMSキーの詳細については、以下のAWSドキュメントを参照してください。

- AWS KMSの概念
- 自動キーローテーションの仕組み。

OSディスクとIDディスクの暗号化には、次のいずれかを構成します。

- 暗号化されたマスターイメージを使用します（たとえば、KMSキーで暗号化されたEBSルートボリュームを含むインスタンスまたはスナップショットから作成されたAMI）。
- 暗号化されたEBSルートボリュームを含むマシンプロファイルソース（VMまたは起動テンプレート）を使用します。

制限事項

以下の制限事項を考慮してください。

- MCS は現在、マスターイメージ AMI 上のディスクを 1 つのみサポートしています。
- 既存の暗号化されていない EBS ボリュームまたはスナップショットを直接暗号化したり、既存の暗号化されたボリュームの KMS キーを変更したりすることはできません。これを行うには、次の手順を実行する必要があります。

  a. そのボリュームの新しいスナップショットを作成します。

  b. そのスナップショットから新しいボリュームを作成します。

  c. 新しいボリュームを暗号化します。

以下の AWS ドキュメントを参照してください。

- 暗号化されていないリソースを暗号化する

- EBSボリュームの自動またはデフォルト暗号化の制限：既存および新規のAmazon EBSボリュームを自動的に暗号化する。

ディスク暗号化を使用してカタログを作成する

ディスク暗号化を使用して MCS マシンカタログを作成するには、次の方法があります。

- マスターイメージ
- マシンプロファイル

ディスク暗号化にマシンプロファイル入力を使用する際の考慮事項：

- マシンプロファイル入力のKMSキーは、マスターイメージのKMSキーよりも優先されます。
- マシンプロファイル入力が提供されない場合、マスターイメージAMIのKMSキーがカタログVMのディスクを暗号化するために使用されます。
- マシンプロファイルにブロックデバイスマッピングが存在する場合、マスターイメージテンプレート（AMI）とマシンプロファイルに存在するブロックデバイスは一致する必要があります。たとえば、AMIに`/dev/sda1`で定義されたデバイスがある場合、マシンプロファイルにも`/dev/sda1`で定義されたデバイスが必要です。
- マシンプロファイルソースにキーがなく、マスターイメージが暗号化されていない場合、カタログVMのディスクは暗号化されません。
- マスターイメージが暗号化されている場合、マシンプロファイルソースVMまたは起動テンプレートには、有効な入力と見なされるために暗号化されたルートボリュームが必要です。

既存のカタログを変更する

`Set-ProvScheme`を使用して、既存のカタログを次のように変更できます。

- 新しいKMSキーを含むボリュームを持つマシンプロファイル入力。
- 新しいKMSキーで暗号化されたマスターイメージテンプレートAMI。

重要な考慮事項

- カタログに追加された新しいVMのボリュームは、新しいKMSキーで暗号化されます。
- 既存のマシンプロファイルがある場合に暗号化設定を更新するには、新しいマシンプロファイルで`Set-ProvScheme`を実行します。
- 既存のカタログを、暗号化されたボリュームから暗号化されていないボリュームに変更することはできません。 暗号化されたマスターAMIから暗号化されていないマスターAMIへのイメージ更新はできません。

VMインスタンスのフィルタリング

マシンプロファイルVMとして使用するAWS EC2インスタンスは、マシンカタログが正しく作成され機能するために互換性がある必要があります。マシンプロファイル入力VMとして使用できるAWS EC2インスタンスを一覧表示するには、`Get-HypInventoryItem` コマンドを使用できます。このコマンドは、ホスティングユニットで利用可能なVMのインベントリをページングおよびフィルタリングできます。

ページネーション:

Get-HypInventoryItem は、2つのページネーションモードをサポートしています。

- ページングモードでは、`-MaxRecords` と `-Skip` パラメーターを使用してアイテムのセットを返します。
  - `-MaxRecords`: デフォルトは**1**です。これは、返されるアイテムの数を制御します。
  - `-Skip`: デフォルトは**0**です。これは、ハイパーバイザー内のリストの絶対的な先頭（または絶対的な末尾）からスキップするアイテムの数を制御します。
- スクロールモードでは、レコードのスクロールを可能にするために、`-MaxRecords`、`-ForwardDirection`、および`-ContinuationToken`パラメーターを使用します。
  - `-ForwardDirection`: デフォルトは**True**です。これは、`-MaxRecords`と組み合わせて使用され、一致するレコードの次のセットまたは前のセットのいずれかを返します。
  - `-ContinuationToken`: これは、`ContinuationToken`で指定されたアイテムを含まずに、直後（または`ForwardDirection`が**false**の場合は直前）のアイテムを返します。

ページネーションの例:

- 最も名前の小さいマシンテンプレートの単一レコードを返すには。`AdditionalData`フィールドには`TotalItemsCount`と`TotalFilteredItemsCount`があります:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template
```

- 最も名前の小さいマシンテンプレートのレコードを10件返します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 10 | select Name
```

- 最も名前の大きいレコードで終わるレコードの配列を返します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ForwardDirection $False -MaxRecords 10 | select
Name
```

- 指定された`ContinuationToken`に関連付けられたマシンテンプレートから始まるレコードの配列を返すには:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ContinuationToken "ami-07xxxxxxxxx"
-MaxRecords 10
```

フィルタリング:

フィルタリングには、以下の追加のオプションパラメータがサポートされています。これらのパラメータは、ページネーションオプションと組み合わせることができます。

- `-ContainsName "my_name"`: 指定された文字列がAMI名の一部と一致する場合、そのAMIは`Get`結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -ContainName ‘apollo’ | select
Name
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: AMIにこれらのタグのいずれかが少なくとも1つある場合、そのAMIは`Get`結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -Tags '{"opex owner": "Not
tagged"}' | select Name
```

注:

2つのタグ値がサポートされています。**タグなし**タグ値は、タグのリストに指定されたタグがない項目と一致します。**すべての値**タグ値は、タグの値に関係なく、タグを持つ項目と一致します。それ以外の場合、一致は、項目がタグを持ち、その値がフィルターで指定された値と等しい場合にのみ発生します。

- `-Id "ami-0a2d913927e0352f3"`: AMIが指定されたIDと一致する場合、そのAMIは`Get`結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -Id ami-xxxxxxxxxxxx
```

AdditionalData パラメータでのフィルタリング:

`AdditionalData`フィルターパラメーターは、テンプレートまたはVMを、その機能、サービス提供、またはAdditionalDataにある任意のプロパティに基づいて一覧表示します。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200).AdditionalData
```

互換性のないVMを示す`-Warn`パラメータを追加することもできます。VMには、**Warning**という名前の`AdditionalData`フィールドが含まれます。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-015xxxxxxxx"
-Warn $true).AdditionalData
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成に誘導します。
- 構成プロセス全体を確認するには、インストールと構成を参照してください。
- カタログを管理するには、マシンカタログの管理およびAWSカタログの管理を参照してください。

詳細情報

- 接続とリソースの作成および管理
- AWSへの接続
- マシンカタログの作成

XenServer®カタログを作成する

マシンカタログの作成では、マシンカタログを作成するウィザードについて説明します。以下の情報は、XenServer仮想化環境に固有の詳細を扱います。

> **注：**
>
> XenServerカタログを作成する前に、XenServerへの接続の作成を完了する必要があります。XenServerへの接続を参照してください。

XenServer接続を使用してマシンカタログを作成する

GPU対応マシンには、専用のマスターイメージが必要です。これらのVMには、GPUをサポートするビデオカードドライバーが必要です。GPU対応マシンを構成して、VMがGPUを操作に使用するソフトウェアで動作できるようにします。

1. XenCenter®で、標準VGA、ネットワーク、およびvCPUを備えたVMを作成します。
2. GPUの使用（パススルーまたはvGPUのいずれか）を有効にするようにVM構成を更新します。
3. サポートされているオペレーティングシステムをインストールし、RDPを有効にします。
4. Citrix VM ToolsとNVIDIAドライバーをインストールします。
5. パフォーマンスを最適化するために、Virtual Network Computing (VNC) 管理コンソールをクリアし、VMを再起動します。
6. RDPを使用するように求められます。RDPを使用してVDAをインストールし、VMを再起動します。
7. オプションで、他のGPUマスターイメージのベースラインテンプレートとしてVMのスナップショットを作成します。
8. RDPを使用して、XenCenterで構成され、GPU機能を使用する顧客固有のアプリケーションをインストールします。

制限事項

- Citrix Hypervisor 8.2 Cumulative Update 1上にVMがホストされているCitrix Virtual Apps and Desktops展開で、単一のMCSカタログに複数のGFS2 SRを使用している場合、展開中にカタログ内のVMがVDIにアクセスできません。「VDI is currently in use」というエラーが報告されます。
- Citrix Hypervisor 8.2 Cumulative Update 1は、GFS2 SRを使用したMCSフルクローンVMをサポートしていません。

詳細については、「制約」を参照してください。

これらの制約は、XenServer 8 以降には適用されません。

マシンプロファイルを使用してマシンカタログを作成する

MCSを使用してマシンをプロビジョニングするためのカタログを作成するときに、マシンプロファイルを使用して仮想マシンからハードウェアプロパティをキャプチャし、カタログ内の新しくプロビジョニングされたVMに適用できます。`MachineProfile`パラメーターが使用されていない場合、ハードウェアプロパティはマスターイメージVMまたはスナップショットからキャプチャされます。

> **注:**
>
> 現在、マシンプロファイルの入力として使用できるのは VM のみです。

> 以下のパラメータを明示的に構成して、マシンプロファイルの入力にあるパラメータの値を上書きできます。

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

マシンプロファイルを使用してカタログを作成するには：

1. PowerShellウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. 識別プールを作成します。識別プールは、作成されるVMのActive Directory (AD) アカウントのコンテナです。例:

   ```
   New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -IdentityPoolName
   "ExampleIdentityPool" -NamingScheme "abc1-##" -NamingSchemeType
   "Numeric" -Scope @() -ZoneUid "xxxxxxxx"
   ```

4. 必要なADコンピューターアカウントをActive Directoryに作成します。

   ```
   $password = "password123" | ConvertTo-SecureString -AsPlainText -Force

   New-AcctADAccount -IdentityPoolName "ExampleIdentityPool" -Count 10
   -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
   ```

```
Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
```

5. カタログを作成するために`New-ProvScheme`コマンドを実行します。例:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
-IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

</CustomProperties>'

-MasterImageVM "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleVDA.vm\ExampleVDA.snapshot"
-ProvisioningSchemeName "ExampleCatalog" -Scope @() -SecurityGroup @()

-MachineProfile "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfile.vm"
```

6. プロビジョニングスキームをブローカーカタログとして登録します。例：

```
$ConfigZone = Get-ConfigZone | Where-Object { $_.Name -eq "xxxxxx" }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -Description
"Machine profile catalog" -ProvisioningSchemeId fe7df345-244e-4xxxx-
xxxxxxxxx -ProvisioningType Mcs -SessionSupport MultiSession
-PersistUserChanges Discard -ZoneUid ($ConfigZone.Uid)
```

7. カタログにVMを追加します。

新しいマシンプロファイルでカタログを更新するには：

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -MachineProfile
"XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfileVm.vm\ExampleMach
ineProfileSnapshot.snapshot"
```

Set-ProvSchemeコマンドの詳細については、「Set-ProvScheme」を参照してください。

注:

- この場合、`Set-ProvScheme`コマンドはカタログ内の既存のVMのマシンプロファイルを変更しません。カタログに追加された新しく作成されたVMのみが新しいマシンプロファイルを持ちます。
- マシンプロファイルベースのマシンカタログを、非マシンプロファイルベースのマシンカタログに変換することはできません。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成に誘導します。
- 構成プロセス全体を確認するには、「インストールと構成」を参照してください。
- カタログを管理するには、「マシンカタログの管理」および「XenServerカタログの管理」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- XenServerへの接続
- マシンカタログの作成

Google Cloud Platformカタログを作成する

(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html)では、マシンカタログを作成するウィザードについて説明しています。以下の情報は、Google Cloud環境に固有の詳細を扱っています。

注:

> Google Cloud Platform（GCP）カタログを作成する前に、GCPへの接続の作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections/connection-gcp.html)を参照してください。

マスターVMインスタンスと永続ディスクを準備する

> **ヒント:**

> 永続ディスクは、Google Cloudにおける仮想ディスクの用語です。

> マスターVMインスタンスを準備するには、計画しているマシンカタログ内のクローンVDAインスタンスに求める構成と一致するプロパティを持つVMインスタンスを作成および構成します。この構成は、インスタンスのサイズと種類だけでなく、メタデータ、タグ、GPU割り当て、ネットワークタグ、サービスアカウントのプロパティなどのインスタンス属性も含まれます。

マスタリングプロセスの一環として、MCSはマスターVMインスタンスを使用してGoogle Cloudの*インスタンステンプレート*を作成します。このインスタンステンプレートは、マシンカタログを構成するクローンVDAインスタンスの作成に使用されます。クローンインスタンスは、インスタンステンプレートが作成されたマスターVMインスタンスのプロパティ（VPC、サブネット、永続ディスクのプロパティを除く）を継承します。

マスターVMインスタンスのプロパティを特定の要件に合わせて構成したら、インスタンスを起動し、インスタンスの永続ディスクを準備します。

ディスクのスナップショットを手動で作成することをお勧めします。そうすることで、意味のある命名規則を使用してバージョンを追跡し、マスターイメージの以前のバージョンを管理するためのより多くのオプションが得られ、マシンカタログの作成時間を節約できます。独自のスナップショットを作成しない場合、MCSが一時的なスナップショットを作成します（これはプロビジョニングプロセスの終了時に削除されます）。

マシンカタログを作成する

マシンカタログは、次の2つの方法で作成できます。

- (/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create/create-machine-catalog-gcp.html#create-a-machine-catalog-using-web-studio)

- (/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create/create-machine-catalog-gcp.html#create-a-machine-catalog-using-powershell)

Web Studioを使用してマシンカタログを作成する

> **注:**
>
> マシンカタログを作成する前に、リソースを作成してください。マシンカタログを構成する際は、Google Cloudで確立されている命名規則を使用してください。詳細については、「バケットとオブジェクトの命名ガイドライン」を参照してください。

> 「マシンカタログの作成」のガイダンスに従ってください。以下の説明は、Google Cloudカタログに固有のものです。

1. Web Studioにサインインし、左ペインで を選択します。
2. アクションバーで を選択します。
3. ページで、 を選択し、 を選択します。
   - Citrix Virtual Apps and Desktops™は、シングルセッションOSもサポートしています。
4. ページで、 と オプションを選択し、 を選択します。複数のリソースがある場合は、メニューから1つ選択します。
5. ページで、必要に応じて以下の手順を完了し、 をクリックします。
   a. スナップショットまたはVMをマスターイメージとして選択します。単一テナンシー機能を使用する場合は、ノードグループプロパティが正しく構成されているイメージを選択してください。「ゾーン選択の有効化」を参照してください。
   b. 既存のVMをマシンプロファイルとして使用するには、 を選択し、そのVMを選択します。

      > **注:**
      >
      > 現在、このカタログ内のVMは、ディスク暗号化セットID、マシンサイズ、ストレージタイプ、およびゾーン設定をマシンプロファイルから継承します。

   c. カタログの最小機能レベルを選択します。単一テナンシー機能を使用する場合は、ノードグループプロパティが正しく構成されているイメージを選択してください。

6. 「**ストレージの種類**」ページで、このマシンカタログのオペレーティングシステムを格納するために使用するストレージの種類を選択します。以下の各ストレージオプションには、固有の価格とパフォーマンス特性があります。（IDディスクは常にゾーン標準永続ディスクを使用して作成されます。）

   - 標準永続ディスク
   - バランス永続ディスク
   - SSD永続ディスク

   Google Cloudのストレージオプションの詳細については、`<https://cloud.google.com/compute/docs/disks/>`を参照してください。

7. 「**仮想マシン**」ページで、作成するVMの数を指定し、VMの詳細な仕様を確認してから、「**次へ**」を選択します。マシンカタログに単一テナントノードグループを使用する場合は、予約済みの単一テナントノードが利用可能なゾーンを**のみ**選択するようにしてください。ゾーン選択を有効にするを参照してください。

8. 「**コンピューターアカウント**」ページで、Active Directoryアカウントを選択し、「**次へ**」を選択します。

   - 「**新しいActive Directoryアカウントを作成**」を選択した場合は、ドメインを選択し、Active Directoryで作成されるプロビジョニング済みVMコンピューターアカウントの命名スキームを表す文字のシーケンスを入力します。アカウントの命名スキームは1～64文字で構成でき、空白、非ASCII文字、または特殊文字を含めることはできません。
   - 「**既存のActive Directoryアカウントを使用**」を選択した場合は、「**参照**」を選択して、選択したマシン用の既存のActive Directoryコンピューターアカウントに移動します。

9. 「**ドメイン資格情報**」ページで、「**資格情報を入力**」を選択し、ユーザー名とパスワードを入力して、「**保存**」を選択し、次に「**次へ**」を選択します。

   - 入力する資格情報には、Active Directoryアカウント操作を実行する権限が必要です。

10. 「**概要**」ページで、情報を確認し、カタログの名前を指定して、「**完了**」を選択します。

> **注:**
>
> バージョン2402以降、GCPカタログ名は以下の規則に準拠する必要があります。
>
> - 小文字で始まること。

- 小文字 (a-z)、数字、ハイフンのみを含めること。
- 小文字または数字で終わること。 これらの規則に準拠していない既存のGCPカタログの名前を変更しようとすると、エラーメッセージが表示され、更新された規則に従って名前を変更するように案内されます。

マシンカタログの作成には時間がかかる場合があります。マシンがターゲットノードグループに作成されていることを確認するには、Google Cloudコンソールに移動します。

手動で作成したGoogle Cloudマシンをインポートする

Google Cloudへの*接続を作成*し、その後、Google Cloudマシンを含む*カタログを作成*できます。その後、Citrix Virtual Apps and Desktopsを介してGoogle Cloudマシンを手動で電源サイクルできます。この機能を使用すると、次のことができます。

- 手動で作成したGoogle CloudマルチセッションOSマシンをCitrix Virtual Apps and Desktopsマシンカタログにインポートします。
- 手動で作成したGoogle CloudマルチセッションOSマシンをCitrix Virtual Apps and Desktopsカタログから削除します。
- 既存のCitrix Virtual Apps and Desktopsの電源管理機能を使用して、Google Cloud WindowsマルチセッションOSマシンの電源を管理します。たとえば、これらのマシンの再起動スケジュールを設定します。

この機能は、既存のCitrix Virtual Apps and Desktopsプロビジョニングワークフローの変更や、既存の機能の削除を必要としません。手動で作成したGoogle Cloudマシンをインポートする代わりに、Web StudioでMCSを使用してマシンをプロビジョニングすることをお勧めします。

共有仮想プライベートクラウド

共有Virtual Private Cloud（VPC）は、共有サブネットが利用可能になるホストプロジェクトと、リソースを使用する1つ以上のサービスプロジェクトで構成されます。共有VPCは、共有企業Google Cloudリソースの一元的な制御、使用、管理を提供するため、大規模なインストールに適したオプションです。詳細については、Googleドキュメントサイトを参照してください。

この機能により、Machine Creation Services（MCS）は、共有VPCに展開されたマシンカタログのプロビジョニングと管理をサポートします。このサポートは、ローカルVPCで現在提供されているサポートと機能的に同等ですが、次の2つの点で異なります。

1. ホスト接続の作成に使用されるサービスアカウントに追加の権限を付与する必要があります。このプロセスにより、MCSは共有VPCリソースにアクセスして使用できるようになります。

2. イングレスとエグレス用にそれぞれ1つずつ、2つのファイアウォールルールを作成する必要があります。これらのファイアウォールルールは、イメージマスタリングプロセス中に使用されます。

必要な新しい権限

ホスト接続を作成する際には、特定の権限を持つGoogle Cloudサービスアカウントが必要です。これらの追加権限は、共有VPCベースのホスト接続を作成するために使用されるすべてのサービスアカウントに付与する必要があります。

> **ヒント:**

> これらの追加の権限は、Citrix Virtual Apps and Desktopsにとって新しいものではありません。これらはローカルVPCの実装を容易にするために使用されます。共有VPCでは、これらの追加の権限により、他の共有VPCリソースへのアクセスが可能になります。

> Shared VPCをサポートするために、ホスト接続に関連付けられたサービスアカウントに最大4つの追加権限を付与する必要があります。

1. **compute.firewalls.list** - この権限は必須です。これにより、MCSは共有VPCに存在するファイアウォールルールのリストを取得できます。
2. **compute.networks.list** - この権限は必須です。これにより、MCSはサービスアカウントが利用できる共有VPCネットワークを識別できます。
3. **compute.subnetworks.list** – この権限は、VPCの使用方法によってオプションです。これにより、MCSは可視の共有VPC内のサブネットを識別できます。この権限はローカルVPCを使用する場合にすでに必要ですが、共有VPCホストプロジェクトでも割り当てる必要があります。
4. **compute.subnetworks.use** - この権限は、VPCの使用方法によってオプションです。プロビジョニングされたマシンカタログでサブネットリソースを使用するために必要です。この権限はローカルVPCを使用する場合にすでに必要ですが、共有VPCホストプロジェクトでも割り当てる必要があります。

これらの権限を使用する際には、マシンカタログの作成に使用される権限の種類に基づいて異なるアプローチがあることを考慮してください。

- プロジェクトレベルの権限:
  - ホストプロジェクト内のすべての共有VPCへのアクセスを許可します。
  - 権限 #3 と #4 をサービスアカウントに割り当てる必要があります。

- サブネットレベルの権限:
  - Shared VPC内の特定のサブネットへのアクセスを許可します。
  - 権限 #3 と #4 はサブネットレベルの割り当てに固有のものであるため、サービスアカウントに直接割り当てる必要はありません。

組織のニーズとセキュリティ基準に合ったアプローチを選択してください。

> **ヒント:**
>
> プロジェクトレベルとサブネットレベルの権限の違いの詳細については、Google Cloud のドキュメントを参照してください。

ファイアウォールルール

マシンカタログの準備中に、カタログのマスターイメージシステムディスクとして機能するマシンイメージが準備されます。このプロセスが発生すると、ディスクは一時的に仮想マシンに接続されます。このVMは、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを防止する分離された環境で実行する必要があります。これは、イングレス用とエグレス用の2つのすべて拒否ファイアウォールルールによって実現されます。Google CloudローカルVCPを使用する場合、MCSはこのファイアウォールをローカルネットワークに作成し、マスタリング用のマシンに適用します。マスタリングが完了すると、ファイアウォールルールはイメージから削除されます。

共有VPCを使用するために必要な新しい権限の数を最小限に抑えることをお勧めします。共有VPCはより上位の企業リソースであり、通常、より厳格なセキュリティプロトコルが導入されています。このため、ホストプロジェクトの共有VPCリソースに、イングレス用とエグレス用の2つのファイアウォールルールを作成してください。それらに最高の優先順位を割り当てます。次の値を使用して、これらの各ルールに新しいターゲットタグを適用します。

`citrix-provisioning-quarantine-firewall`

MCSがマシンカタログを作成または更新するとき、このターゲットタグを含むファイアウォールルールを検索します。次に、ルールの正確性を確認し、カタログのマスターイメージを準備するために使用されるマシンに適用します。ファイアウォールルールが見つからない場合、またはルールは見つかったがルールまたはその優先順位が正しくない場合、次のようなメッセージが表示されます。

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules for VPC
<name> in project <project>. " Please ensure you have created 'deny all' firewall
```

`rules with the network tag 'citrix-provisioning-quarantine-firewall' and proper priority." "Refer to Citrix Documentation for details."`

共有 VPC の構成

Web Studioで共有VPCをホスト接続として追加する前に、プロビジョニングするプロジェクトからサービスアカウントを追加するために、次の手順を完了してください。

1. IAMロールを作成します。
2. CVADホスト接続の作成に使用されるサービスアカウントを、共有VPCホストプロジェクトのIAMロールに追加します。
3. プロビジョニングするプロジェクトのCloud Buildサービスアカウントを、共有VPCホストプロジェクトのIAMロールに追加します。
4. ファイアウォールルールを作成します。

IAMロールを作成する

ロールのアクセスレベルを決定します — *プロジェクトレベルアクセス*、またはより制限されたモデルである *サブネットレベルアクセス* を使用します。

IAMロールのプロジェクトレベルアクセス。プロジェクトレベルのIAMロールには、次の権限を含めます。

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

プロジェクトレベルのIAMロールを作成するには：

1. Google Cloudコンソールで、**IAMと管理 > ロール**に移動します。
2. **ロール**ページで、**ロールを作成**を選択します。
3. **ロールの作成**ページで、ロール名を指定します。**権限を追加**を選択します。
    a. **権限の追加**ページで、ロールに権限を個別に追加します。権限を追加するには、**テーブルをフィルタリング**フィールドに権限の名前を入力します。権限を選択し、**追加**を選択します。
    b. **作成**を選択します。

サブネットレベルのIAMロール。このロールは、**ロールを作成**を選択した後に権限`compute.subnetworks.list`と`compute.subnetworks.use`の追加を省略します。このIAMアクセスレベルの場合、権限`compute.firewalls.list`と`compute.networks.list`を新しいロールに適用する必要があります。

サブネットレベルのIAMロールを作成するには：

1. Google Cloudコンソールで、**VPC network** > **Shared VPC**に移動します。**Shared VPC**ページが表示され、ホストプロジェクトに含まれるShared VPCネットワークのサブネットが表示されます。
2. **Shared VPC**ページで、アクセスしたいサブネットを選択します。
3. 右上隅で、サービスアカウントを追加するために**ADD MEMBER**を選択します。
4. **Add members**ページで、次の手順を完了します。
    a. **New members**フィールドにサービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。
    b. **Select a role**フィールドを選択し、次に**Compute Network User**を選択します。
    c. **SAVE**を選択します。
5. Google Cloudコンソールで、**IAM & Admin** > **Roles**に移動します。
6. **Roles**ページで、**CREATE ROLE**を選択します。
7. **Create Role**ページで、ロール名を指定します。**ADD PERMISSIONS**を選択します。
    a. **Add permissions**ページで、ロールに個別に権限を追加します。権限を追加するには、**Filter table**フィールドに権限の名前を入力します。権限を選択し、**ADD**を選択します。
    b. **CREATE**を選択します。

ホストプロジェクトのIAMロールにサービスアカウントを追加する

IAMロールを作成したら、ホストプロジェクトのサービスアカウントを追加するために次の手順を実行します。

1. Google Cloud コンソールで、ホストプロジェクトに移動し、次に **IAM と管理 > IAM** に移動します。
2. **IAM** ページで、サービスアカウントを追加するために **追加** を選択します。
3. **メンバーの追加** ページで:
    a. **新しいメンバー** フィールドに、サービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。

b. ロールフィールドを選択し、作成した IAM ロールを入力し、メニューからそのロールを選択します。

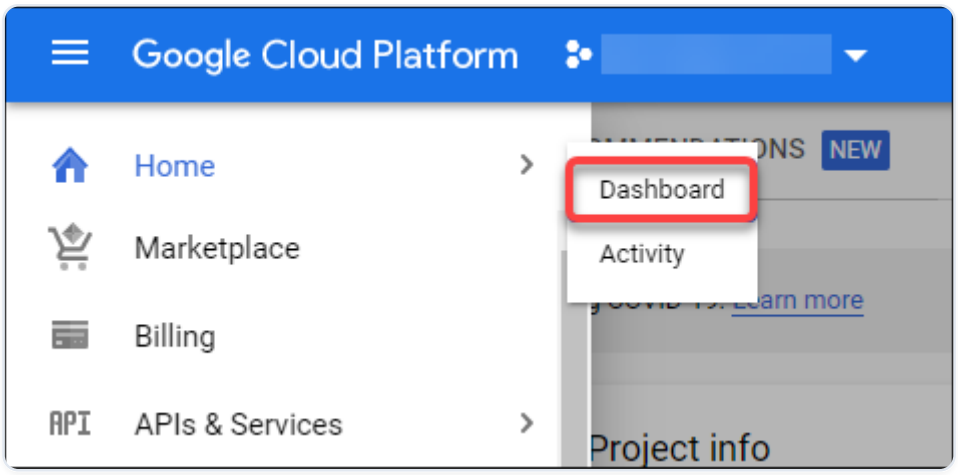
c. **保存** を選択します。

これで、サービスアカウントがホストプロジェクト用に構成されました。

クラウドビルドサービスアカウントを共有 VPC に追加する

すべての Google Cloud サブスクリプションには、プロジェクト ID 番号の後に `cloudbuild.gserviceaccount` が続く名前のサービスアカウントがあります。例: `705794712345@cloudbuild.gserviceaccount`。

Google Cloud コンソールで **ホーム** と **ダッシュボード** を選択すると、プロジェクトのプロジェクト ID 番号を確認できます。



画面の **プロジェクト情報** エリアの下にある **プロジェクト番号** を見つけます。

Cloud Buildサービスアカウントを共有VPCに追加するには、次の手順を実行します。

1. Google Cloud コンソールで、ホストプロジェクトに移動し、次に **IAM と管理** > **IAM** に移動します。
2. **権限** ページで、アカウントを追加するために **追加** を選択します。
3. 「**メンバーの追加**」ページで、次の手順を実行します。

   a. 「**新しいメンバー**」フィールドにCloud Buildサービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。

   b. 「**ロールを選択**」フィールドを選択し、`Computer Network User`と入力して、メニューからロールを選択します。

   c. 「**保存**」を選択します。

ファイアウォールルールを作成する

マスタリングプロセスの一環として、MCSは選択したマシンイメージをコピーし、それを使用してカタログのマスターイメージシステムディスクを準備します。マスタリング中、MCSはディスクを一時的な仮想マシンに接続し、その仮想マシンが準備スクリプトを実行します。このVMは、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを禁止する分離された環境で実行する必要があります。分離された環境を作成するために、MCSは2つの *すべて拒否* ファイアウォールルール（イングレスルールとエグレスルール）を必要とします。したがって、*ホストプロジェクト* に次の2つのファイアウォールルールを作成します。

1. Google Cloudコンソールで、ホストプロジェクトに移動し、次に「**VPCネットワーク > ファイアウォール**」に移動します。
2. 「**ファイアウォール**」ページで、「**ファイアウォールルールを作成**」を選択します。
3. 「**ファイアウォールルールを作成**」ページで、以下を完了します。
   - **名前**。ルールの名前を入力します。
   - **ネットワーク**。イングレスファイアウォールルールが適用される共有 VPC ネットワークを選択します。
   - **優先度**。値が小さいほど、ルールの優先度が高くなります。小さい値（例: 10）をお勧めします。
   - **トラフィックの方向**。「**イングレス**」を選択します。
   - **一致時のアクション**。「**拒否**」を選択します。
   - **ターゲット**。デフォルトの「**指定されたターゲットタグ**」を使用します。
   - 「**ターゲットタグ**」。`citrix-provisioning-quarantine-firewall` と入力します。
   - 「**ソースフィルター**」。デフォルトの「**IP範囲**」を使用します。
   - 「**ソースIP範囲**」。すべてのトラフィックに一致する範囲を入力します。`0.0.0.0/0` と入力します。
   - 「**プロトコルとポート**」。「**すべて拒否**」を選択します。
4. 「**作成**」を選択してルールを作成します。
5. 手順 1〜4 を繰り返して別のルールを作成します。**Direction of traffic** には **Egress** を選択します。

接続の追加

Google Cloud環境への接続を追加します。「接続を追加する」を参照してください。

ゾーン選択を有効にする

Citrix Virtual Apps and Desktopsはゾーン選択をサポートしています。ゾーン選択を使用すると、VMを作成するゾーンを指定できます。ゾーン選択を使用すると、管理者は選択したゾーンに単一テナントノードを配置できます。単一テナンシーを構成するには、Google Cloudで以下を完了する必要があります。

- Google Cloud の単一テナントノードを予約する
- VDA マスターイメージを作成する

Google Cloud の単一テナントノードを予約する

単一テナントノードを予約するには、Google Cloud のドキュメントを参照してください。

> 「**重要:**」:

> ノードテンプレートは、ノードグループに予約されているシステムのパフォーマンス特性を示すために使用されます。これらの特性には、vGPUの数、ノードに割り当てられるメモリ量、およびノード上に作成されるマシンに使用されるマシンタイプが含まれます。詳細については、Google Cloudのドキュメントを参照してください。

VDA マスターイメージの作成

単一テナントノードにマシンを正常に展開するには、マスターVMイメージを作成する際に追加の手順を実行する必要があります。Google Cloud上のマシンインスタンスには、*ノードアフィニティラベル*と呼ばれるプロパティがあります。単一テナントノードに展開されるカタログのマスターイメージとして使用されるインスタンスには、**ターゲットノードグループ**の名前と一致する*ノードアフィニティラベル*が必要です。これを実現するには、次の点に留意してください。

- 新しいインスタンスの場合、インスタンスの作成時にGoogle Cloudコンソールでラベルを設定します。詳細については、「インスタンスの作成時にノードアフィニティラベルを設定する」を参照してください。
- 既存のインスタンスの場合、**gcloud**コマンドラインを使用してラベルを設定します。詳細については、「既存のインスタンスのノードアフィニティラベルを設定する」を参照してください。

> **注:**

> 共有 VPC で単一テナンシーを使用する場合は、共有仮想プライベートクラウドを参照してください。

インスタンスの作成時にノードアフィニティラベルを設定する

ノードアフィニティラベルを設定するには：

1. Google Cloudコンソールで、**Compute Engine > VM instances**に移動します。
2. **VM instances**ページで、**Create instance**を選択します。
3. **Instance creation**ページで、必要な情報を入力または構成し、**management, security, disks, networking, sole tenancy**を選択して設定パネルを開きます。
4. **Sole tenancy**タブで、**Browse**を選択して現在のプロジェクトで利用可能なノードグループを表示します。**Sole-tenant node**ページが表示され、利用可能なノードグループのリストが表示されます。
5. **Sole-tenant node**ページで、リストから該当するノードグループを選択し、**Select**を選択して**Sole tenancy**タブに戻ります。ノードアフィニティラベルフィールドには、選択した情報が入力されます。この設定により、インスタンスから作成されたマシンカタログが選択されたノードグループに展開されることが保証されます。
6. **Create**を選択してインスタンスを作成します。

既存のインスタンスにノードアフィニティラベルを設定する

ノードアフィニティラベルを設定するには：

1. Google Cloud Shellターミナルウィンドウで、*gcloud compute instances*コマンドを使用してノードアフィニティラベルを設定します。**gcloud**コマンドに次の情報を含めます:

   - **VMの名前**。たとえば、`s*2019-vda-base`という名前の既存のVMを使用します。*
   - **ノードグループの名前**。以前に作成したノードグループ名を使用します。たとえば、`mh-sole-tenant-node-group-1`。
   - **インスタンスが存在するゾーン**。たとえば、VMは`*us-east-1b* zone`に存在します。

   たとえば、ターミナルウィンドウで次のコマンドを入力します:

   - `gcloud compute instances set-scheduling "s2019-vda-base" --node-group="mh-sole-tenant-node-group-1" --zone="us-east1-b"`

   *gcloud compute instances*コマンドの詳細については、`<https://cloud.google.com/sdk/gcloud/reference/beta/compute/instances/set-scheduling>`にあるGoogle Developer Toolsのドキュメントを参照してください。

2. インスタンスの**VMインスタンスの詳細**ページに移動し、**ノードアフィニティ**フィールドにラベルが入力されていることを確認します。

マシンカタログを作成する

ノードアフィニティラベルを設定したら、マシンカタログを構成します。

顧客管理の暗号化キー (CMEK)

MCSカタログに顧客管理の暗号化キー (CMEK) を使用できます。この機能を使用する場合、Google Cloud Key Management Service `CryptoKey Encrypter/Decrypter` ロールをCompute Engine Service Agentに割り当てます。Citrix Virtual Apps and Desktopsアカウントは、キーが保存されているプロジェクトで適切な権限を持っている必要があります。詳細については、Cloud KMS キーを使用してリソースを保護するを参照してください。

Compute Engine サービスエージェントは次の形式です: `service-<Project _Number>@compute-system.iam.gserviceaccount.com`。この形式は、デフォルトの Compute Engine サービスアカウントとは異なります。

> **注:**
>
> この Compute Engine サービスアカウントは、Google Console の「**IAM 権限**」表示に表示されない場合があります。そのような場合は、Cloud KMS キーを使用してリソースを保護する で説明されているように、`gcloud` コマンドを使用してください。

Citrix Virtual Apps and Desktops アカウントに権限を割り当てる

Google Cloud KMS の権限はさまざまな方法で構成できます。*プロジェクトレベル*の KMS 権限または*リソースレベル*の KMS 権限のいずれかを付与できます。詳細については、権限とロール を参照してください。

プロジェクトレベルの権限

1つのオプションは、Citrix Virtual Apps and Desktopsアカウントに、Cloud KMSリソースを参照するためのプロジェクトレベルの権限を付与することです。これを行うには、カスタムロールを作成し、次の権限を追加します。

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

このカスタムロールをCitrix Virtual Apps and Desktopsに割り当てます。これにより、インベントリ内の関連プロジェクトでリージョンキーを参照できるようになります。

リソースレベルの権限

もう1つのオプションであるリソースレベルの権限の場合、Google Cloud コンソールで、MCS プロビジョニングに使用する `cryptoKey` を参照します。Citrix Virtual Apps and Desktops アカウントを、カタログプロビジョニングに使用するキーリングまたはキーに追加します。

> **ヒント:**
>
> このオプションでは、Citrix Virtual Apps and DesktopsアカウントがCloud KMSリソースに対するプロジェクトレベルのリスト権限を持っていないため、インベントリでプロジェクトのリージョンキーを参照することはできません。ただし、以下で説明するように、`ProvScheme`カスタムプロパティで正しい`cryptoKeyId`を指定することで、CMEKを使用してカタログをプロビジョニングすることは可能です。

カスタムプロパティを使用した CMEK でのプロビジョニング

PowerShell を使用してプロビジョニングスキームを作成する 場合は、`ProvScheme` `CustomProperties` で `CryptoKeyId` プロパティを指定します。例:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId"
Value="<yourCryptoKeyId>" />

</CustomProperties>'
```

`cryptoKeyId` は次の形式で指定する必要があります。

`projectId:location:keyRingName:cryptoKeyName`

たとえば、リージョン `us-east1` のキーリング `my-example-key-ring` にあるキー `my-example-key` と、ID `my-example-project-1` のプロジェクトを使用する場合、`ProvScheme` のカスタム設定は次のようになります。

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
example-project-1:us-east1:my-example-key-ring:my-example-key" />

</CustomProperties>'
```

このプロビジョニングスキームに関連するすべてのMCSプロビジョニング済みディスクとイメージは、この顧客管理暗号化キーを使用します。

ヒント:

グローバルキーを使用する場合、顧客プロパティの場所は `global` と記述する必要があり、上記の例の **us-east1** のような**リージョン**名ではありません。例: `<Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-example-project-1:global:my-example-key-ring:my-example-key" />`。

顧客管理キーのローテーション

Google Cloud は、既存の永続ディスクまたはイメージでのキーのローテーションをサポートしていません。マシンがプロビジョニングされると、作成時に使用されていたキーのバージョンに紐付けられます。ただし、新しいバージョンのキーを作成でき、その新しいキーは、新しくプロビジョニングされたマシンや、新しいマスターイメージでカタログが更新されたときに作成されるリソースに使用されます。

キーリングに関する重要な考慮事項

キーリングの名前変更や削除はできません。また、キーリングを構成する際に予期せぬ料金が発生する可能性があります。キーリングを削除または削除すると、Google Cloud はエラーメッセージを表示します。

```
Sorry, you can't delete or rename keys or key rings. We were concerned
about the security implications of allowing multiple keys or key versions
over time to have the same resource name, so we decided to make names
immutable. (And you can't delete them, because we wouldn't be able to do a
true deletion--there would still have to be a tombstone tracking that this
name had been used and couldn't be reused).

We're aware that this can make things untidy, but we have no immediate
```

```
plans to change this.

If you want to avoid getting billed for a key or otherwise make it
unavailable, you can do so by deleting all the key versions; neither keys
nor key rings are billed for, just the active key versions within the
keys.
```

ヒント:

詳細については、コンソールからキーリングを編集または削除する を参照してください。

均一なバケットレベルのアクセス互換性

Citrix Virtual Apps and Desktops は、Google Cloud の均一なバケットレベルのアクセス制御ポリシーと互換性があります。この機能は、ストレージバケットを含むリソースの操作を許可するためにサービスアカウントに権限を付与する IAM ポリシーの使用を強化します。均一なバケットレベルのアクセス制御により、Citrix Virtual Apps and Desktops では、アクセス制御リスト (ACL) を使用して、ストレージバケットまたはそこに保存されているオブジェクトへのアクセスを制御できます。Google Cloud の均一なバケットレベルのアクセスに関する概要情報については、均一なバケットレベルのアクセス を参照してください。構成情報については、均一なバケットレベルのアクセスを要求する を参照してください。

PowerShell を使用してマシンカタログを作成する

このセクションでは、PowerShell を使用してカタログを作成する方法について詳しく説明します。

- 永続的なライトバックキャッシュディスクを持つカタログを作成する
- MCSIO で起動パフォーマンスを向上させる
- マシンプロファイルを使用してマシンカタログを作成する
- インスタンステンプレートとしてマシンプロファイルを持つマシンカタログを作成する
- PowerShell を使用してシールドされた VM を持つカタログを作成する
- 単一テナントノードに Windows 11 VM を作成する

永続的なライトバックキャッシュディスクを持つカタログを作成する

永続的なライトバックキャッシュディスクを持つカタログを構成するには、PowerShell パラメーター `New-ProvScheme` `CustomProperties` を使用します。

ヒント:

ここでは、クラウドベースのホスティング接続にのみ PowerShell パラメーターを使用してください。オンプレミスソリューション (XenServer® など) の永続的なライトバックキャッシュディスクを使用してマシンをプロビジョニングする場合、ディスクは自動的に永続化されるため、PowerShell は必要ありません。

このパラメーターは、MCS プロビジョニングされたマシンのライトバックキャッシュディスクがどのように永続化されるかを決定するために使用される追加のプロパティ `PersistWBC` をサポートします。`PersistWBC` プロパティは、`UseWriteBackCache` パラメーターが指定され、`WriteBackCacheDiskSize` パラメーターがディスクが作成されることを示すように設定されている場合にのみ使用されます。

注:

この動作は、Azure と GCP の両方に適用され、電源を入れ直すとデフォルトの MCSIO ライトバックキャッシュディスクが削除され、再作成されます。ディスクを永続化することで、MCSIO ライトバックキャッシュディスクの削除と再作成を回避できます。

`PersistWBC` プロパティを `true` に設定すると、Citrix Virtual Apps and Desktops 管理者が管理インターフェイスからマシンをシャットダウンしても、ライトバックキャッシュディスクは削除されません。

`PersistWBC` プロパティを `false` に設定すると、Citrix Virtual Apps and Desktops 管理者が管理インターフェイスからマシンをシャットダウンしたときに、ライトバックキャッシュディスクが削除されます。

注:

`PersistWBC` プロパティが省略された場合、プロパティはデフォルトで `false` になり、管理インターフェイスからマシンがシャットダウンされるとライトバックキャッシュは削除されます。

たとえば、CustomProperties パラメーターを使用して `PersistWBC` を `true` に設定する場合：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

注:

`PersistWBC` プロパティは、`New-ProvScheme` PowerShell コマンドレットを使用してのみ設定できます。プロビジョニングスキームの `CustomProperties` を作成後に変更しようとしても、マシンカタログや、マシンがシャットダウンされたときのライトバックキャッシュディスクの永続性には影響しません。

たとえば、`New-ProvScheme` を使用してライトバックキャッシュを使用するように設定し、`PersistWBC` プロパティを `true` に設定します。

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
```

```
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

MCSIO で起動パフォーマンスを向上させる

MCSIO が有効になっている場合、Azure および GCP マネージドディスクの起動パフォーマンスを向上させることができます。この機能を構成するには、`New-ProvScheme` コマンドで PowerShell の `PersistOSDisk` カスタムプロパティを使用します。`New-ProvScheme` に関連するオプションは次のとおりです。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->
```

```
````````Groups" Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```

この機能を有効にするには、`PersistOSDisk` カスタムプロパティを `true` に設定します。例：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127
```
```

```
-WriteBackCacheMemorySize 256
```

マシンプロファイルを使用してマシンカタログを作成する

Machine Creation Services (MCS) を使用してマシンをプロビジョニングするカタログを作成する場合、マシンプロファイルを使用して仮想マシンからハードウェアプロパティをキャプチャし、カタログ内の新しくプロビジョニングされた VM に適用できます。`MachineProfile` パラメーターが使用されない場合、ハードウェアプロパティはマスターイメージ VM またはスナップショットからキャプチャされます。 たとえば、`StorageType`、`CatalogZones`、`CryptoKeyIs` など、明示的に定義する一部のプロパティは、マシンプロファイルから無視されます。

- マシンプロファイルを使用してカタログを作成するには、`New-ProvScheme` コマンドを使用します。たとえば、`New-ProvScheme –MachineProfile "path to VM"` です。`MachineProfile` パラメーターを指定しない場合、ハードウェアプロパティはマスターイメージ VM からキャプチャされます。
- 新しいマシンプロファイルでカタログを更新するには、`Set-ProvScheme` コマンドを使用します。例えば、`Set-ProvScheme –MachineProfile "path to new VM"`。このコマンドは、カタログ内の既存のVMのマシンプロファイルを変更しません。カタログに追加された新しく作成されたVMのみが新しいマシンプロファイルを持ちます。
- マスターイメージを更新することもできますが、マスターイメージを更新してもハードウェアプロパティは更新されません。ハードウェアプロパティを更新したい場合は、`Set-ProvScheme` コマンドを使用してマシンプロファイルを更新する必要があります。これらの変更は、カタログ内の新しいマシンにのみ適用されます。既存のマシンのハードウェアプロパティを更新するには、`-StartsNow` および `-DurationInMinutes -1` パラメータを指定して `Set-ProvVMUpdateTimeWindow` コマンドを使用できます。

  注:

  - `StartsNow` は、スケジュールされた開始時刻が現在の時刻であることを示します。
  - 負の数（例：–1）を指定した `DurationInMinutes` は、スケジュールの時間枠に上限がないことを示します。

マシンプロファイルをインスタンステンプレートとして使用してマシンカタログを作成する

マシンプロファイルの入力としてGCPインスタンステンプレートを選択できます。インスタンステンプレートはGCPの軽量リソースであるため、非常に費用対効果が高いです。

マシンプロファイルをインスタンステンプレートとして使用して新しいマシンカタログを作成する

1. PowerShellウィンドウを開きます。
2. `asnp citrix*`を実行して、Citrix固有のPowerShellモジュールをロードします。
3. 次のコマンドを使用して、GCPプロジェクトでインスタンステンプレートを見つけます。

   ```
   cd XDHyp:\HostingUnits\<HostingUnitName>\instanceTemplates.folder
   ```

4. NewProvSchemeコマンドを使用して、インスタンステンプレートをマシンプロファイルとして使用する新しいマシンカタログを作成します。

   ```
   New-ProvScheme -ProvisioningSchemeName <CatalogName>  -HostingUnitName
   <HostingUnitName> -IdentityPoolName <identity pool name> -MasterImageVM

   XDHyp:\HostingUnits\<HostingUnitName> \Base.vm\Base.snapshot
   -MachineProfile XDHyp:
   \HostingUnits\<HostingUnitName>\instanceTemplates.folder\mytemplate.tem
   plate
   ```

   New-ProvSchemeコマンドの詳細については、https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/を参照してください。

5. PowerShell コマンドを使用してマシンカタログの作成を完了します。Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/ を参照してください。

既存のマシンカタログのマシンプロファイルをインスタンステンプレートに変更する

既存のマシンカタログのマシンプロファイルをインスタンステンプレートに変更する詳細な手順は次のとおりです。

1. PowerShell ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. 次のコマンドを実行します。

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -MachineProfile
XDHyp:
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\<TemplateName>
.template
```

Set-ProvSchemeコマンドの詳細については、https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/を参照してください。

PowerShell を使用して、シールドされたVMでカタログを作成する

シールドされたVMプロパティを持つMCSマシンカタログを作成できます。シールドされた仮想マシンは、セキュアブート、仮想トラステッドプラットフォームモジュール、UEFIファームウェア、整合性監視などの高度なプラットフォームセキュリティ機能を使用して、Compute Engineインスタンスの検証可能な整合性を提供する一連のセキュリティ制御によって強化されています。

MCSは、マシンプロファイルワークフローを使用してカタログを作成することをサポートしています。マシンプロファイルワークフローを使用する場合、VMインスタンスのシールドされたVMプロパティを有効にする必要があります。その後、このVMインスタンスをマシンプロファイルの入力として使用できます。

マシンプロファイルワークフローを使用して、シールドされたVMでMCSマシンカタログを作成するには。

1. Google Cloud コンソールでVMインスタンスのシールドされたVMオプションを有効にします。クイックスタート: シールドされたVMオプションを有効にするを参照してください。
2. VMインスタンスを使用して、マシンプロファイルワークフローでMCSマシンカタログを作成します。
    a. PowerShell ウィンドウを開きます。
    b. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
    c. まだ作成されていない場合は、IDプールを作成します。
    d. `New-ProvScheme`コマンドを実行します。例：

```
New-ProvScheme -ProvisioningSchemeName <catalog-name>

-HostingUnitName gcp-hostint-unit

-MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-vda.vm
```

```
-MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
machine.vm
```

3. マシンカタログの作成を完了します。

新しいマシンプロファイルでマシンカタログを更新するには:

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme -ProvisioningSchemeName <catalog-name>

-MasterImageVM XDHyp:\HostingUnits\<hostin-unit>\catalog-vda.vm

-MachineProfile "DHyp:\HostingUnits\<hostin-unit>\catalog-machine.vm
```

`Set-ProvScheme` で行った変更を既存のVMに適用するには、`Set-ProvVMUpdateTimeWindow` コマンドを実行します。

1. `Set-ProvVMUpdateTimeWindow` コマンドを実行します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

2. VMを再起動します。

単一テナントノードにWindows 11 VMを作成する

GCPでWindows 11 VMを作成できます。ただし、マスターイメージにWindows 11をインストールする場合は、マスターイメージ作成プロセス中にvTPMを有効にする必要があります。また、マシンプロファイルソース（VMまたはインスタンステンプレート）でvTPMを有効にする必要があります。

単一テナントノードにWindows 11 VMを作成するための主要な手順は次のとおりです。

1. Google Cloud仮想化環境をセットアップします。詳しくは、「Google Cloud environments」を参照してください。
2. VDAをインストールします。「Install VDAs」を参照してください。
3. Google Cloud環境への接続を作成します。詳しくは、「Connection to Google cloud environments」を参照してください。

4. Windows 11 Bring Your Own License (BYOL) マスターイメージを作成し、そのイメージをGoogle Cloudにインポートします。「Create a Windows 11 BYOL master image」を参照してください。
5. マシンプロファイルソースを作成します。単一テナントノードにVMをプロビジョニングし、ソースマシンプロファイルのvTPMを有効にします。「Provision VM on sole-tenant node」を参照してください。
6. vTPMが有効なWindows 11マシンプロファイルソースを使用してMCSマシンカタログを作成します。マシンプロファイルソースは、単一テナントノードで説明されているものと同じインスタンスタイプである必要があります。「Create an MCS machine catalog using the Windows 11 machine profile source」を参照してください。

Windows 11 BYOLマスターイメージを作成する

Windows 11 BYOLマスターイメージを作成し、そのマスターイメージをGoogle Cloudにインポートするには、2つのオプションがあります。

- Google Cloud Cloud Build Tools を使用する
- 他のハイパーバイザーでマスターイメージを作成する

GOOGLE CLOUD CLOUD BUILD TOOLS を使用する

1. Windows 11 ISO、GCP SDK、.NET Framework、および PowerShell インストーラーファイルを GCP ストレージバケットにアップロードします。
2. クラウドビルド `.yaml` ファイル内のファイルパスをパラメーターとして指定します。
3. コマンドラインから以下の Cloud Build を実行して、最終的な Windows 11 イメージをビルドします。GCP は、GCP の Daisy ワークフローを使用して、選択したプロジェクトでマスターイメージをブートストラップして作成し、マスターイメージは GCP にインポートされます。

```
gcloud compute instances import INSTANCE-NAME--source-uri=gs://BUCKET/
IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
machine-type=MACHINE-TYPE --zone=ZONE
```

> **注：**
>
> すべての大文字のテキストを実際のリソースの詳細に置き換えます。

詳細については、「カスタムWindows BYOLイメージを作成する」を参照してください。

他のハイパーバイザーでマスターイメージを作成する

1. 他のハイパーバイザーを使用して Windows 11 マスターイメージを作成します。
2. マスターイメージを OVF 形式でローカルマシンにエクスポートします。
3. ローカルの gcloud CLI を使用して、OVF ファイルを GCP ストレージバケットにアップロードします。

   ```
   gsutil cp LOCAL_IMAGE_PATH_OVF_FILES gs://BUCKET_NAME/
   ```

4. コマンドラインから以下の Cloud Build を実行して、最終的な Windows 11 イメージをビルドします。GCP は、GCP の Daisy ワークフローを使用して、選択したプロジェクトでマスターイメージをブートストラップして作成し、マスターイメージは GCP にインポートされます。

   ```
   gcloud compute instances import INSTANCE-NAME --source-uri=gs://BUCKET/
   IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
   machine-type=MACHINE-TYPE --zone=ZONE
   ```

   注:

   すべての大文字のテキストを実際のリソースの詳細に置き換えてください。

シングルテナントノードにVMをプロビジョニングする

シングルテナントノードを使用すると、VMを他のプロジェクトのVMから物理的に分離したり、同じホストハードウェア上にVMをグループ化したりできます。シングルテナントノードの詳細については、GCPドキュメント「シングルテナンシーの概要」を参照してください。

シングルテナントノードにVM（マシンプロファイルソース）をプロビジョニングする方法については、GCPドキュメント「シングルテナントノードにVMをプロビジョニングする」を参照してください。

注:

- ノードグループと同じインスタンスタイプとリージョンを選択します。
- Shielded VMセクションでvTPMを有効にします。詳細については、「クイックスタート：Shielded VMオプションを有効にする」を参照してください。

- ソースVMでBitlockerを無効にします。

Windows 11のマシンプロファイルソースを使用してMCSマシンカタログを作成する

Web StudioまたはPowerShellコマンドを使用して、Windows 11 VMを作成するためのMCSマシンカタログを作成できます。

注:

- マスターイメージには、Windows 11のスナップショットまたはVMを選択します。
- マシンプロファイルソースには、Windows 11 VMをマシンプロファイルとして選択します。マシンプロファイルソースは、シングルテナントノードで説明されているものと同じインスタンスタイプである必要があります。

Web Studio の使用方法については、Web Studio を使用したマシンカタログの作成 を参照してください。

PowerShell コマンドについては、マシンプロファイルを使用したマシンカタログの作成 を参照してください。

カタログを作成し、VM の電源をオンにすると、Google Cloud コンソールで単一テナントノード上で実行されている Windows 11 VM を確認できます。

継承されたラベルを持つ VM とディスク

MCS マシンカタログのVMとディスク（Identity Disk、Write-cache Back Disk、およびOSディスク）は、マシンプロファイルソース（GCP VMインスタンスまたはインスタンステンプレート）のラベルを継承できます。これらのラベルを使用して、異なるチームが所有するインスタンス（例：team:research および team:analytics）を区別し、さらにコスト計算や予算編成に利用できます。ラベルの詳細については、GCPドキュメントのラベルを使用したリソースの整理 を参照してください。

マシンプロファイルソースを使用して、新しいカタログの作成、既存のカタログの更新、および既存のVMの更新を行い、ラベルを継承させることができます。

この機能は、永続的および非永続的な MCS マシンカタログに適用されます。

次のことができます。

- 継承されたラベルを持つカタログを作成する
- 継承されたラベルを持つ既存のカタログを更新する
- 継承されたラベルを持つ既存のVMを更新する
- VMおよびブートディスクのラベル情報を取得する
- VMを削除する

継承されたラベルを持つカタログを作成する

VM とディスクがマシンプロファイルソースからラベルを継承する MCS マシンカタログを作成するには、次の手順を実行します。

1. ラベル付きのマシンプロファイルソース（VMインスタンスまたはインスタンステンプレート）を作成します。ラベル付きVMの作成については、GCPドキュメント「Create resources with labels」を参照してください。インスタンステンプレートはVMから作成され、VMで定義されたラベルを引き継ぎます。
2. Web StudioまたはPowerShellコマンドを使用してMCSカタログを作成します。
3. Web Studioを使用している場合は、**イメージ**ページで**マシンプロファイルを使用**を選択し、VMまたはテンプレートを選択します。
4. PowerShellコマンドを使用する場合は、次の手順を実行します。

    a. PowerShellウィンドウを開きます。

    b. asnp citrix* を実行します。

    c. IDプールを作成します。IDプールは、作成されるVMのActive Directory (AD) アカウントのコンテナです。

    d. Active Directoryで必要なADコンピューターアカウントを作成します。

    e. カタログを作成するには、`New-ProvScheme`コマンドを実行します。例:

    マシンプロファイル入力としてテンプレートを使用するNew-ProvScheme（永続カタログ）：

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `
```

```
-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `
```

マシンプロファイル入力としてインスタンステンプレートを使用するNew-ProvScheme（非永続カタログ）：

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `

-CleanOnBoot
```

マシンプロファイル入力としてVMインスタンスを使用するNew-ProvScheme（永続カタログ）：

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

マシンプロファイル入力としてVMインスタンスを使用するNew-ProvScheme（非永続カタログ）：

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-CleanOnBoot
```

f. プロビジョニングスキームをブローカーカタログとして登録します。

g. カタログにVMを追加します。

継承されたラベルで既存のカタログを更新する

既存のカタログを新しいマシンプロファイルを持つように更新するには、Set-ProvSchemeコマンドを実行します。コマンドを実行すると、カタログに追加されたすべての新しいVMは、新しいマシンプロファイルソースのラベルを持つようになります。非永続カタログは、次回の電源投入時に更新されます。

例:

インスタンステンプレートをマシンプロファイル入力として使用するSet-ProvScheme:

```
Set-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `
```

VMインスタンスをマシンプロファイル入力として使用するSet-ProvScheme:

```
Set-ProvScheme `

-ProvisioningSchemeName "catalog-name" `
```

```
-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

継承されたラベルで既存のVMを更新する

更新されたマシンプロファイルソースで既存のVMを更新するには、次のコマンドを実行します。

1. `Set-ProvScheme`
2. `Set-ProvVMUpdateTimeWindow`。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

3. VMを再起動します。

VMおよびブートディスクラベルの情報を取得する

VMを作成した後、`AdditionalData`パラメーターを指定して`Get-Item`コマンドを使用すると、VMおよびブートディスクラベルの情報を取得できます。

VMラベルの情報を取得するには、次のコマンドを実行します。

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-
name\vm_name.vm).AdditionalData.Tags
```

ブートディスクラベルの情報を取得するには、次のコマンドを実行します。

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-name\vm_name.vm\bootdisk-
name.attacheddisk).AdditionalData.Tags
```

注:

さまざまなハイパーバイザー間で一貫性を保つため、GCPラベルを表示するために「タグ」という用語を使用しています。

VMを削除する

カタログからVMを削除するが、GCPからVMを削除しないことを選択できます。この場合、Citrixラベルのみがから削除されます。その他の追加されたラベルはすべてVMから削除されません。Web StudioまたはPowerShellコマンドを使用してVMを削除できます。

WEB STUDIOの使用

1. VMを選択して右クリックします。
2. をクリックします。
3. を選択します。

POWERSHELLコマンドの使用

`ForgetVM`パラメーターを指定して`Remove-ProvVM`を実行します。詳細については、SDKドキュメントのRemove-ProvVMを参照してください。

Google Cloud マーケットプレイス

Citrixが**Google Cloud Marketplace**で提供するイメージを参照して選択し、マシンカタログを作成できます。現在、MCSはこの機能に対してマシンプロファイルワークフローのみをサポートしています。

Google Cloud Marketplaceを通じてCitrix VDA VM製品を検索するには、https://console.cloud.google.com/marketplaceにアクセスしてください。

カスタムイメージまたはCitrix ready®イメージを**Google Cloud Marketplace**で使用して、マシンカタログのイメージを更新できます。

> **注:**
>
> マシンプロファイルにストレージタイプ情報が含まれていない場合、値はカスタムプロパティから派生します。

> サポートされているGoogle Cloud Marketplaceイメージは次のとおりです。

- Windows 2019シングルセッション
- Windows 2019 マルチセッション
- ウブントゥ

マシンカタログ作成のソースとしてCitrix対応イメージを使用する例：

```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \

-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \

-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
```

```
win2019-single-vda-v20220819.publicimage \

-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループを作成するようにガイドします。
- 構成プロセス全体を確認するには、インストールと構成を参照してください。
- カタログを管理するには、マシンカタログの管理とGoogle Cloud Platformカタログの管理を参照してください。

詳細情報

- 接続とリソースを作成および管理する
- Google Cloud環境への接続
- マシンカタログを作成する

HPE Moonshot マシンカタログを作成する

マシンカタログの作成 では、マシンカタログを作成するウィザードについて説明します。以下の情報は、HPE Moonshot 環境に固有の詳細を扱っています。

注記：

- HPE Moonshot への接続を作成する
- 1つ以上の HPE Moonshot ノードが利用可能であることを確認し、それらのノードに VDA をインストールします。
- 初期の HPE Moonshot カートリッジイメージの作成については、「OS Deployment on Moonshot User Guide」を参照してください。

HPE Moonshot マシンカタログは、以下を使用して作成できます。

- ウェブスタジオ
- PowerShell コマンド

Web Studio を使用してマシンカタログを作成する

マシンカタログのセットアップウィザードで、次の手順を実行します。

1. **オペレーティングシステム**ページで、**マルチセッションOS**または**シングルセッションOS**を選択します。
2. **マシン管理**ページで、**電源管理されているマシン**と**別のサービスまたはテクノロジ**を選択します。
3. **仮想マシン**ページで、マシンとその Active Directory マシンアカウントを追加します。次のいずれかを実行できます。
   - **マシンの追加**をクリックして、マシンを手動で追加します。**VM の選択**ウィンドウが表示されます。以前に作成した HPE Moonshot シャーシ接続を展開し、追加するノード（VM）を選択します。次に、関連付けられたマシンアカウント名を追加します。
   - マシンを一括追加するには、「**CSVファイルの追加**」をクリックします。CSVファイルを使用してマシンを追加する方法については、「CSVファイルを使用してマシンをカタログに一括追加する」を参照してください。

スコープページと**概要**ページには、HPE Moonshot固有の情報は含まれていません。

PowerShellコマンドを使用してマシンカタログを作成する

ブローカーカタログを作成し、マシンをブローカーカタログにインポートするには、`New-BrokerCatalog`および`New-BrokerMachine` PowerShellコマンドを実行します。

例:

```
New-BrokerCatalog  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -AllocationType "Random" -IsRemotePC $False
-MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "BurMC"
-PersistUserChanges "OnLocal" -ProvisioningType "Manual" -Scope @()
-SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc-4578-bc07-
bcf2a82d1463"

New-BrokerMachine  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -CatalogUid 3 -HostedMachineId "c10n1"
-HypervisorConnectionUid 4 -IsReserved $False -MachineName
"S-1-5-21-2589939477-3963209805-1860259709-1121"
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、「インストールと構成」を参照してください。
- カタログを管理するには、「マシンカタログの管理」および「HPE Moonshotカタログの管理」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- HPE Moonshotへの接続
- マシンカタログの作成

Microsoft Azure カタログを作成する

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

マシンカタログの作成では、マシンカタログを作成するウィザードについて説明しています。以下の情報は、Microsoft Azure Resource Managerクラウド環境に固有の詳細を扱っています。

> **注:**
>
> Microsoft Azureカタログを作成する前に、Microsoft Azureへの接続の作成を完了する必要があります。Microsoft Azureへの接続を参照してください。

マシンカタログの作成

マシンカタログは、次の2つの方法で作成できます。

- Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#create-a-machine-catalog-using-an-azure-resource-manager-image-in-web-studio)
- PowerShellを使用してマシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#create-a-machine-catalog-using-powershell)

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

イメージは、ディスク、スナップショット、またはAzure Compute Gallery内のイメージ定義のイメージバージョンであり、マシンカタログ内のVMを作成するために使用されます。マシンカタログを作成する前に、Azure Resource Managerでイメージを作成します。イメージに関する一般情報については、マシンカタログの作成を参照してください。

> **注:**
>
> ホスト接続で構成されているリージョンとは異なるリージョンからマスターイメージを使用するサポートは非推奨です。Azure Compute Galleryを使用して、マスターイメージを目的のリージョンにレプリケートしてください。

> MCSマシンカタログを作成する際、DHCPの有効化やライセンスの再アクティブ化などの準備タスクを実行するために、元のVMに基づいて一時的なVMが作成されます。この一時的なVMは準備VMと呼ばれます。この準備VMの名前は**Preparati-84x9n**という形式に従い、最後の5文字は重複を避けるためにランダムに生成されます。この準備VMの命名規則は固定されており、カスタマイズできません。準備タスクが完了すると、準備VMは破棄されます。

準備VMからネットワークを切断するために、すべてのインバウンドおよびアウトバウンドトラフィックを拒否するネットワークセキュリティグループが作成されます。ネットワークセキュリティグループは、カタログごとに1回自動的に作成されます。ネットワークセキュリティグループの名前は`Citrix-Deny-All-a3pgu-GUID`で、GUIDはランダムに生成されます。例: `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`。

マシンカタログ作成ウィザードで:

- 「**マシンタイプ**」および「**マシン管理**」ページには、Azure固有の情報は含まれていません。マシンカタログの作成の記事のガイダンスに従ってください。

- **イメージ**ページで、このカタログにマシンを作成するためのテンプレートとして使用するイメージを選択します。

  使用するイメージの種類として**マスターイメージ**を選択する場合は、**イメージの選択**をクリックし、必要に応じてマスターイメージを選択するために次の手順に従います。

  a. (テナント内またはテナント間で共有イメージが構成されている接続にのみ適用) イメージが存在するサブスクリプションを選択します。

  b. リソースグループを選択します。

  c. Azure VHD、Azure Compute Gallery、またはAzureイメージバージョンに移動します。必要に応じて、選択したイメージにメモを追加します。

  イメージを選択する際は、次の点を考慮してください。

  - イメージにCitrix VDAがインストールされていることを確認します。
  - VMに接続されているVHDを選択する場合は、次の手順に進む前にVMをシャットダウンする必要があります。

> **注:**
>
> - カタログ内のマシンを作成した接続（ホスト）に対応するサブスクリプションは、緑色の点で示されます。その他のサブスクリプションは、Azure Compute Galleryがそのサブスクリプションと共有されているものです。これらのサブスクリプションでは、共有ギャラリーのみが表示されます。共有サブスクリプションの構成方法については、テナント内でイメージを共有する（サブスクリプション間）およびテナント間でイメージを共有するを参照してください。
> - 信頼された起動が有効になっているイメージまたはスナップショットを選択する場合、**セキュリティの種類**として信頼された起動を持つマシンプロファイルを使用することが必須です。その後、マシンプロファイルでSecureBootとvTPMの値を指定することで、それらを有効または無効にできます。信頼された起動は、Shared Image Galleryではサポートされていません。Azureの信頼された起動の詳細については、`<https://docs.microsoft.com/ja-jp/azure/virtual-machines/trusted-launch>`を参照してください。
> - 信頼された起動が有効なWindowsでエフェメラルOSディスクを使用してプロビジョニングスキームを作成できます。信頼された起動が有効なイメージを選択する場合、vTPMが有効な信頼された起動を持つマシンプロファイルを選択する必要がありま

す。エフェメラルOSディスクを使用してマシンカタログを作成する方法については、エフェメラルOSディスクを使用してマシンを作成する方法を参照してください。

- イメージのレプリケーションが進行中の場合でも、続行してそのイメージをマスターイメージとして選択し、セットアップを完了できます。ただし、イメージのレプリケーション中にカタログ作成の完了に時間がかかる場合があります。MCSでは、カタログ作成から1時間以内にレプリケーションを完了する必要があります。レプリケーションがタイムアウトすると、カタログ作成は失敗します。Azureでレプリケーションステータスを確認できます。レプリケーションがまだ保留中の場合、またはレプリケーションが完了した後に、もう一度試してください。
- Azureでマシンカタログのマスターイメージを選択すると、MCSは、選択したマスターイメージとマシンプロファイルに基づいてOSの種類を識別します。MCSが識別できない場合は、マスターイメージと一致するOSの種類を選択してください。
- Gen2イメージを使用してGen2 VMカタログをプロビジョニングすることで、起動時間のパフォーマンスを向上させることができます。ただし、Gen1イメージを使用してGen2マシンカタログを作成することはサポートされていません。同様に、Gen2イメージを使用してGen1マシンカタログを作成することもサポートされていません。また、世代情報を持たない古いイメージはすべてGen1イメージです。

使用するイメージの種類として**準備済みイメージ**を選択した場合、**イメージの選択**をクリックし、必要に応じて準備済みイメージを選択します。

VMの作成を成功させるには、イメージにCitrix VDA 2311以降がインストールされており、VDAにMCSIOが存在することを確認してください。

イメージを選択すると、**マシンプロファイルを使用（Azure Active Directoryに必須）**チェックボックスが自動的に選択されます。**マシンプロファイルの選択**をクリックして、リソースグループのリストからVMまたはARMテンプレート仕様を参照します。カタログ内のVMは、選択したマシンプロファイルから構成を継承できます。

ARMテンプレート仕様がマシンカタログを作成するためのマシンプロファイルとして使用できることを確認するために検証します。ARMテンプレート仕様を検証する方法は2つあります。

- リソースグループリストからARMテンプレート仕様を選択した後、**次へ**をクリックします。ARMテンプレート仕様にエラーがある場合、エラーメッセージが表示されます。
- 次のPowerShellコマンドのいずれかを実行します。

- `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
- `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

VMがマシンプロファイルから継承できる構成の例は次のとおりです。

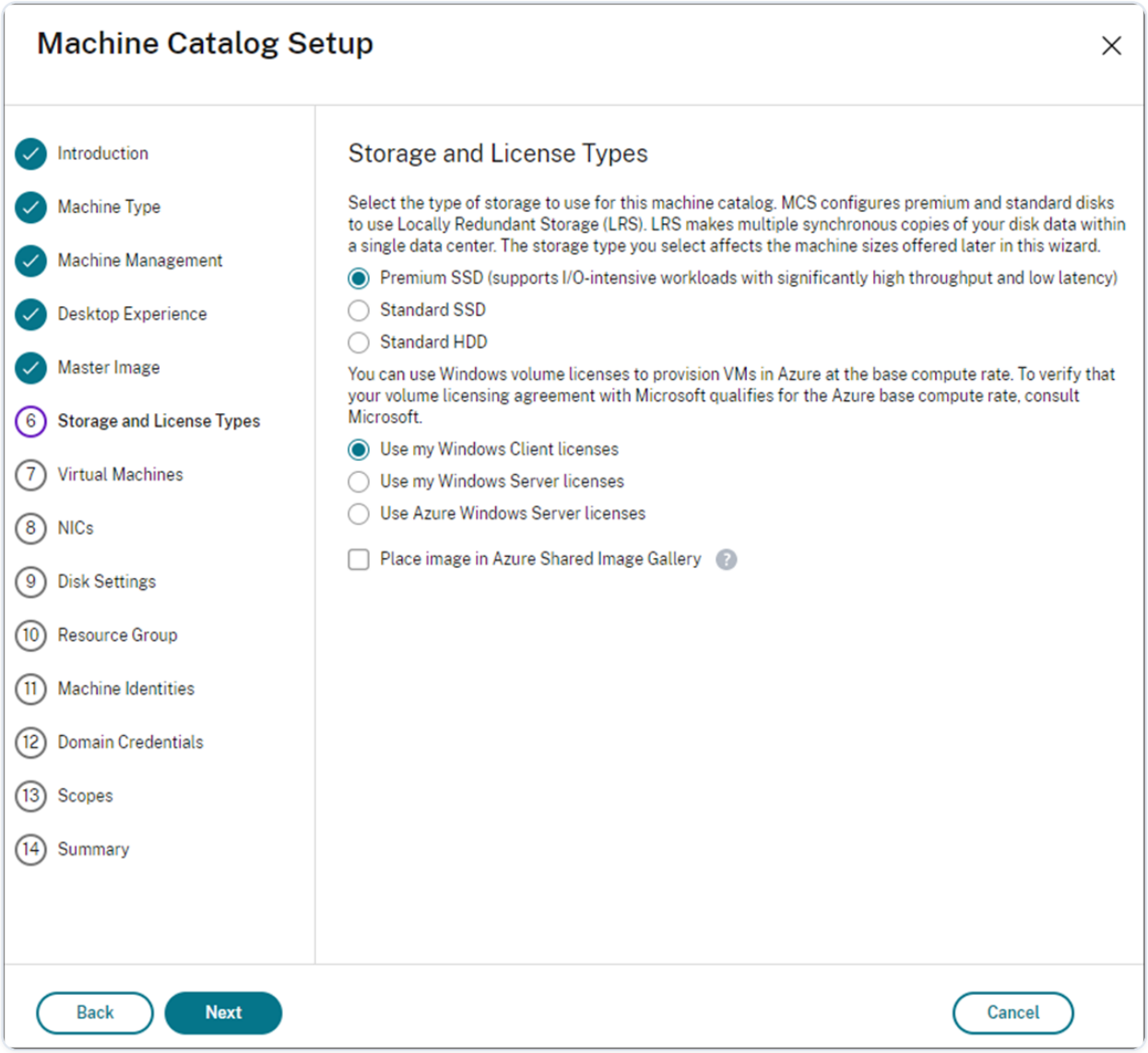
- アクセラレーテッドネットワーク
- ブート診断
- ホストディスクキャッシュ（OSおよびMCSIOディスクに関連）
- マシンサイズ（特に指定がない場合）
- VMに配置されたタグ

カタログを作成した後、イメージがマシンプロファイルから継承する構成を表示できます。**マシンカタログ**ノードで、カタログを選択して下部ペインに詳細を表示します。次に、**テンプレートプロパティ**タブをクリックして、マシンプロファイルのプロパティを表示します。**タグ**セクションには、最大3つのタグが表示されます。VMに配置されているすべてのタグを表示するには、**すべて表示**をクリックします。

MCSでAzure専用ホストにVMをプロビジョニングする場合は、**専用ホストグループを使用する**チェックボックスを有効にしてから、リストからホストグループを選択します。ホストグループは、専用ホストのコレクションを表すリソースです。専用ホストは、1つ以上のVMをホストする物理サーバーを提供するサービスです。サーバーはAzureサブスクリプション専用であり、他のサブスクライバーと共有されません。専用ホストを使用すると、AzureはVMがそのホストで実行されている唯一のマシンであることを保証します。この機能は、規制要件または内部セキュリティ要件を満たす必要があるシナリオに適しています。ホストグループとそれらを使用する際の考慮事項の詳細については、「Azure 専用ホスト」を参照してください。

> **重要：**
>
> - Azureの自動配置が有効になっているホストグループのみが表示されます。
> - ホストグループを使用すると、ウィザードの後半で表示される**仮想マシン**ページが変更されます。そのページには、選択したホストグループに含まれるマシンサイズのみが表示されます。また、可用性ゾーンは自動的に選択され、選択できません。

- **ストレージとライセンスの種類**ページは、Azure Resource Managerイメージを使用している場合にのみ表示されます。



マシンカタログで使用できるストレージの種類は次のとおりです。

- I/O負荷の高いワークロードを持つVMに適した、高性能で低遅延のディスクストレージオプションとして、「**Premium SSD**」を提供します。
- **Standard SSD**。低いIOPSレベルで一貫したパフォーマンスを必要とするワークロードに適した、費用対効果の高いストレージオプションを提供します。
- **Standard HDD**。遅延に影響されないワークロードを実行するVMに適した、信頼性が高く低コストのディスクストレージオプションを提供します。
- **Azure ephemeral OS disk**。VMのローカルディスクを再利用してオペレーティングシステムディスクをホストする、費用対効果の高いストレージオプションを提供します。または、PowerShellを使用してエフェメラルOSディスクを使用するマシンを作成することもできます。詳細については、「Azure エフェメラルディスク」を参照してください。エフェメラルOSディスクを使用する際は、以下の考慮事項に注意してください。
  - AzureエフェメラルOSディスクとMCS I/Oは同時に有効にできません。

- エフェメラルOSディスクを使用するマシンを更新するには、VMのキャッシュディスクまたは一時ディスクのサイズを超えないイメージを選択する必要があります。
- ウィザードの後半で提示される**電源サイクル中にVMとシステムディスクを保持する**オプションは使用できません。

> **注:**
>
> IDディスクは、選択したストレージタイプに関係なく、常にStandard SSDを使用して作成されます。

> ストレージタイプによって、ウィザードの**仮想マシン**ページで提供されるマシンサイズが決まります。MCSは、プレミアムディスクと標準ディスクをローカル冗長ストレージ（LRS）を使用するように構成します。LRSは、単一のデータセンター内でディスクデータの複数の同期コピーを作成します。AzureエフェメラルOSディスクは、VMのローカルディスクを使用してオペレーティングシステムを保存します。Azureストレージタイプとストレージレプリケーションの詳細については、以下を参照してください。

- `<https://docs.microsoft.com/ja-jp/azure/storage/common/storage-introduction/>`
- `<https://docs.microsoft.com/ja-jp/azure/virtual-machines/premium-storage-performance/>`
- `<https://docs.microsoft.com/ja-jp/azure/storage/common/storage-redundancy/>`

既存のWindowsライセンスまたはLinuxライセンスを使用するかどうかを選択します。

- Windowsライセンス：Windowsイメージ（Azureプラットフォームサポートイメージまたはカスタムイメージ）とともにWindowsライセンスを使用すると、AzureでWindows VMを低コストで実行できます。ライセンスには2つのタイプがあります。
  - **Windows Serverライセンス**。Windows ServerまたはAzure Windows Serverライセンスを使用でき、Azureハイブリッド特典を利用できます。詳細については、`<https://azure.microsoft.com/ja-jp/pricing/hybrid-benefit/>`を参照してください。Azureハイブリッド特典は、AzureでのVM実行コストを基本コンピューティング料金に削減し、Azureギャラリーからの追加のWindows Serverライセンスのコストを免除します。

- **Windowsクライアントライセンス**。Windows 10およびWindows 11ライセンスをAzureに持ち込むことができ、追加のライセンスなしでAzureでWindows 10およびWindows 11 VMを実行できます。詳細については、「クライアントアクセスライセンスと管理ライセンス」を参照してください。

プロビジョニングされたVMがライセンス特典を使用しているかどうかは、次のPowerShellコマンドを実行して確認できます: `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`。

- Windows Serverライセンスタイプの場合、ライセンスタイプが**Windows_Server**であることを確認してください。詳細な手順は`<https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/hybrid-use-benefit-licensing/>`で入手できます。
- Windowsクライアントライセンスタイプの場合、ライセンスタイプが**Windows_Client**であることを確認してください。詳細な手順は`<https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/>`で入手できます。

あるいは、`Get-Provscheme` PowerShell SDK を使用して検証を行うこともできます。例: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`。このコマンドレットの詳細については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/>`を参照してください。

- Linux ライセンス: BYOS (bring-your-own-subscription) Linux ライセンスを使用する場合、ソフトウェアの料金を支払う必要はありません。BYOS の料金には、コンピューティングハードウェア料金のみが含まれます。ライセンスには次の2種類があります。
  - **RHEL_BYOS**: RHEL_BYOS タイプを正常に使用するには、Azure サブスクリプションで Red Hat Cloud Access を有効にします。
  - **SLES_BYOS**: SLES の BYOS バージョンには、SUSE からのサポートが含まれています。

  `New-ProvScheme` および `Set-ProvScheme` で LicenseType の値を Linux オプションに設定できます。

  `New-ProvScheme` で LicenseType を RHEL_BYOS に設定する例:

  ```
  New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "azureCatalog"
  -RunAsynchronously -Scope @() -SecurityGroup @() -CustomProperties
  '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  ```

```
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" /><Property xsi:type="StringProperty"
Name="StorageAccountType" Value="StandardSSD_LRS" /><Property
xsi:type="StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /
><Property xsi:type="StringProperty" Name="OsType" Value="Linux" /
><Property xsi:type="StringProperty" Name="LicenseType"
Value="RHEL_BYOS" /></CustomProperties>'
```

`Set-ProvScheme` で LicenseType を SLES_BYOS に設定する例:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog"
-CustomProperties '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"><Property
xsi:type="StringProperty" Name="UseManagedDisks" Value="true" /
><Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" /><Property xsi:type="StringProperty"
Name="ResourceGroups" Value="hu-dev-mcs" /><Property
xsi:type="StringProperty" Name="OsType" Value="Linux" /><Property
xsi:type="StringProperty" Name="LicenseType" Value="SLES_BYOS" /></
CustomProperties>'
```

注:

`LicenseType` の値が空の場合、デフォルト値は OsType の値に応じて Azure Windows Server License または Azure Linux License になります。

LicenseType を空に設定する例:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog"
-CustomProperties '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"><Property
xsi:type="StringProperty" Name="UseManagedDisks" Value="true" /
><Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" /><Property xsi:type="StringProperty"
Name="ResourceGroups" Value="hu-dev-mcs" /><Property
```

```
xsi:type="StringProperty" Name="OsType" Value="Linux" /></
CustomProperties>'
```

ライセンスの種類とその利点については、以下のドキュメントを参照してください。

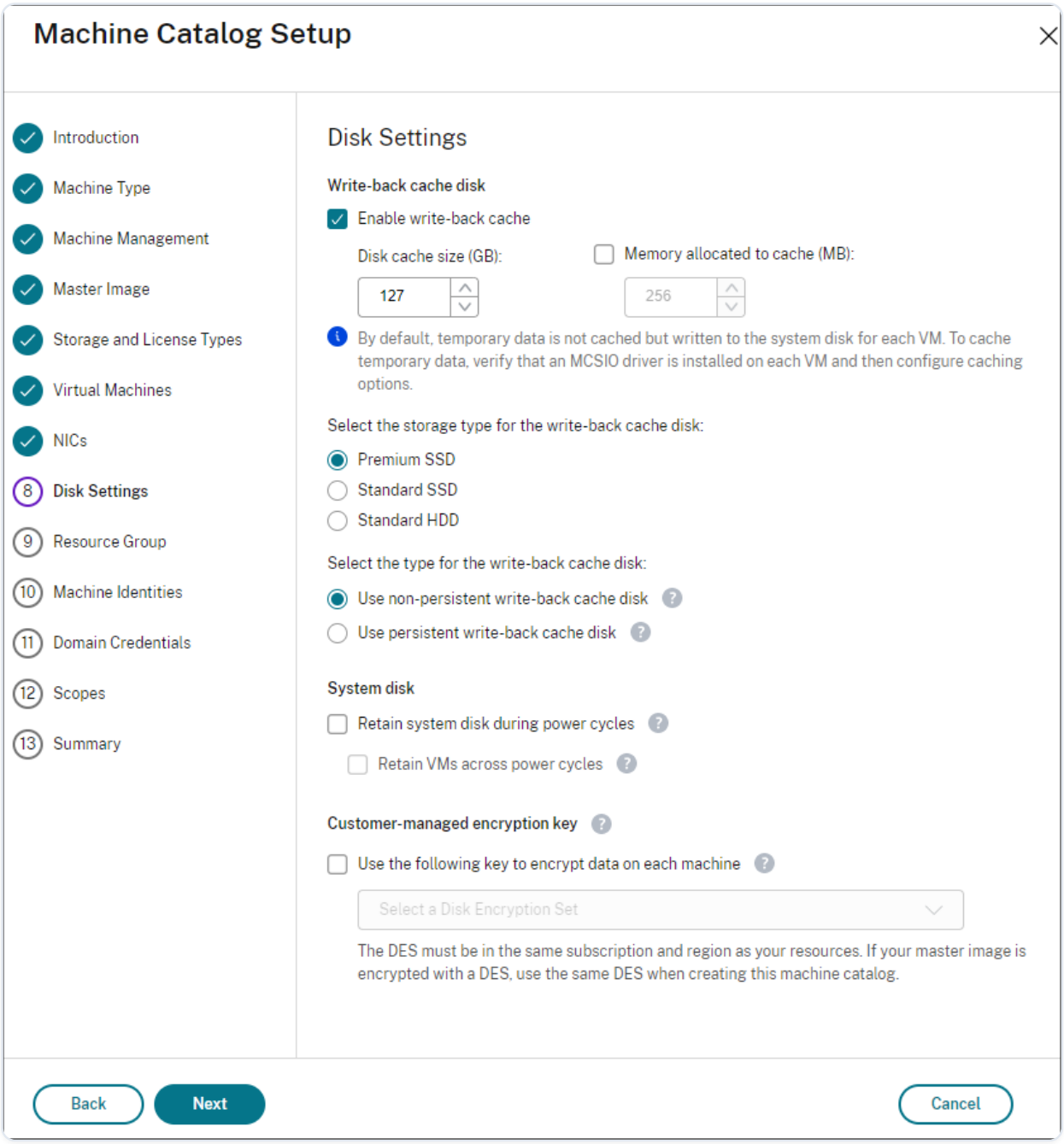
- `<https://docs.microsoft.com/ja-jp/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet>`
- `<https://docs.microsoft.com/ja-jp/azure/virtual-machines/linux/azure-hybrid-benefit-linux>`

Azure Compute Gallery (旧称 Azure Shared Image Gallery) は、イメージを管理および共有するためのリポジトリです。これにより、組織全体でイメージを利用できるようになります。大規模な非永続マシンカタログを作成する際には、VDA OS ディスクのリセットを高速化できるため、イメージを SIG に保存することをお勧めします。 を選択すると、 セクションが表示され、Azure Compute Gallery の詳細設定を指定できます。

- **仮想マシンとイメージレプリカの比率**。Azure が保持する仮想マシンとイメージレプリカの比率を指定できます。デフォルトでは、Azure は非永続マシン40台ごとに1つのイメージレプリカを保持します。永続マシンの場合、この数値はデフォルトで1,000になります。
- **最大レプリカ数**。Azureが保持するイメージレプリカの最大数を指定できます。デフォルトは100です。

> **注:**
>
> イメージを保存するためにACGにギャラリーが作成されます。このギャラリーは、VM作成のためにMCSからのみアクセス可能で、**イメージの選択**ページには表示されません。

- **仮想マシン**ページで、作成するVMの数を指定します。少なくとも1つを指定し、マシンサイズを選択する必要があります。カタログ作成後、カタログを編集してマシンサイズを変更できます。
- **NIC**ページには、Azure固有の情報は含まれていません。(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html#nic)の記事のガイダンスに従ってください。
- **ディスク設定**ページで、ライトバックキャッシュを有効にするかどうかを選択します。MCSストレージ最適化機能が有効になっている場合、カタログ作成時に次の設定を構成できます。これらの設定は、AzureとGCPの両方の環境に適用されます。



ライトバックキャッシュを有効にした後、以下を実行できます。

- 一時データをキャッシュするために使用するディスクとRAMのサイズを構成します。詳細については、「一時データのキャッシュの構成」を参照してください。
- ライトバックキャッシュディスクのストレージタイプを選択します。ライトバックキャッシュディスクには、次のストレージオプションを使用できます。
  - プレミアム SSD
  - スタンダード SSD
  - スタンダード HDD

- プロビジョニングされたVMに対してライトバックキャッシュディスクを永続化するかどうかを選択します。オプションを有効にするには、**ライトバックキャッシュを有効にする**を選択します。デフォルトでは、**非永続ライトバックキャッシュディスクを使用する**が選択されています。
- ライトバックキャッシュディスクの種類を選択します。
  - **非永続的なライトバックキャッシュディスクを使用する**。選択した場合、ライトバックキャッシュディスクは電源サイクル中に削除されます。そこにリダイレクトされたデータはすべて失われます。VMの一時ディスクに十分な空き容量がある場合、コストを削減するためにライトバックキャッシュディスクをホストするために使用されます。カタログ作成後、プロビジョニングされたマシンが一時ディスクを使用しているかどうかを確認できます。これを行うには、カタログをクリックし、**テンプレートプロパティ**タブの情報を確認します。一時ディスクが使用されている場合、**非永続的なライトバックキャッシュディスク**と表示され、その値は**はい（VMの一時ディスクを使用）**になります。そうでない場合、非永続的なライトバックキャッシュディスクと表示され、その値は**いいえ（VMの一時ディスクを使用しない）**になります。
  - **永続的なライトバックキャッシュディスクを使用する**。選択した場合、ライトバックキャッシュディスクはプロビジョニングされたVMに対して永続的になります。このオプションを有効にすると、ストレージコストが増加します。
- 電源サイクル中にVDAのVMとシステムディスクを保持するかどうかを選択します。

  電源サイクル中にVMとシステムディスクを保持する。ライトバックキャッシュを有効にするを選択した場合に利用可能です。デフォルトでは、VMとシステムディスクはシャットダウン時に削除され、起動時に再作成されます。VMの再起動時間を短縮したい場合は、このオプションを選択します。このオプションを有効にすると、ストレージコストも増加することに注意してください。
- **ストレージコストの節約**を有効にするかどうかを選択します。有効にすると、VMがシャットダウンしたときにストレージディスクをStandard HDDにダウングレードすることでストレージコストを節約します。VMは再起動時に元の設定に戻ります。このオプションは、ストレージディスクとライトバックキャッシュディスクの両方に適用されます。または、PowerShellを使用することもできます。詳細については、「VMシャットダウン時にストレージタイプを下位層に変更する」を参照してください。

> **注:**

> Microsoftは、VMシャットダウン中のストレージタイプの変更に制限を課しています。また、Microsoftが将来的にストレージタイプの変更をブロックする可能性もあります。詳細については、このMicrosoft記事を参照してください。

  - カタログでプロビジョニングされたマシン上のデータを暗号化するかどうかを選択します。顧客管理の暗号化キーを使用したサーバー側暗号化により、マネージドディスクレベルで暗号化を管理し、カタログ内のマシン上のデータを保護できます。詳細については、「Azureサーバー側暗号化」を参照してください。

- **リソースグループ** ページで、リソースグループを作成するか、既存のグループを使用するかを選択します。

  - リソースグループを作成することを選択した場合は、**次へ**を選択します。
  - 既存のリソースグループを使用することを選択した場合は、**利用可能なプロビジョニングリソースグループ**リストからグループを選択します。**注意**: カタログで作成するマシンを収容するのに十分なグループを選択してください。選択したグループが少なすぎる場合はメッセージが表示されます。後でカタログにVMを追加する予定がある場合は、最小限必要な数よりも多く選択することをお勧めします。カタログ作成後にリソースグループをカタログに追加することはできません。

  詳細については、Azure リソースグループを参照してください。

- **マシンID**ページで、IDタイプを選択し、このカタログ内のマシンのIDを構成します。VMを**Azure Active Directory参加済み**として選択した場合、それらをAzure ADセキュリティグループに追加できます。詳細な手順は次のとおりです。

  a. **IDタイプ**フィールドから、**Azure Active Directory参加済み**を選択します。**Azure ADセキュリティグループ（オプション）**オプションが表示されます。
  b. **Azure ADセキュリティグループ: 新規作成**をクリックします。
  c. グループ名を入力し、**作成**をクリックします。
  d. 画面の指示に従ってAzureにサインインします。 グループ名がAzureに存在しない場合は、緑色のアイコンが表示されます。それ以外の場合は、新しい名前を入力するよう求めるエラーメッセージが表示されます。
  e. VMのマシンアカウント命名規則を入力します。

  カタログ作成後、Citrix Virtual Apps and Desktops™はユーザーに代わってAzureにアクセスし、セキュリティグループとグループの動的メンバーシップルールを作成します。このルール

に基づいて、このカタログで指定された命名規則を持つVMは自動的にセキュリティグループに追加されます。

このカタログに異なる命名スキームを持つ VM を追加するには、Azure にサインインする必要があります。その後、Citrix Virtual Apps and Desktops は Azure にアクセスし、新しい命名スキームに基づいて動的メンバーシップルールを作成できます。

このカタログを削除する際、Azure からセキュリティグループを削除するには、Azure へのサインインも必要です。

- **ドメイン資格情報**および**概要**ページには、Azure固有の情報は含まれていません。マシンカタログの作成の記事のガイダンスに従ってください。

ウィザードを完了します。

Azure一時ディスクがライトバックキャッシュディスクとして適格であるための条件

Azure一時ディスクをライトバックキャッシュディスクとして使用できるのは、以下のすべての条件が満たされている場合のみです。

- Azure一時ディスクは永続的なデータに適していないため、ライトバックキャッシュディスクは非永続的である必要があります。
- 選択したAzure VMサイズには、一時ディスクが含まれている必要があります。
- エフェメラルOSディスクを有効にする必要はありません。
- ライトバックキャッシュファイルをAzure一時ディスクに配置することを受け入れます。
- Azure一時ディスクのサイズは、（ライトバックキャッシュディスクサイズ + ページングファイル用の予約スペース + 1 GBのバッファースペース）の合計サイズよりも大きい必要があります。

非永続的なライトバックキャッシュディスクのシナリオ

マシンカタログ作成時に一時ディスクをライトバックキャッシュに使用する3つの異なるシナリオを、次の表に示します。

シナリオ	結果
ライトバックキャッシュに一時ディスクを使用するためのすべての条件が満たされています。	WBCファイル `mcsdif.vhdx` は一時ディスクに配置されます。

シナリオ	結果
一時ディスクには、ライトバックキャッシュの使用に十分なスペースがありません。	VHDディスク `MCSWCDisk` が作成され、WBCファイル `mcsdif.vhdx` がこのディスクに配置されます。
一時ディスクにはライトバックキャッシュの使用に十分なスペースがありますが、`UseTempDiskForWBC` が **false** に設定されています。	VHDディスク `MCSWCDisk` が作成され、WBCファイル `mcsdif.vhdx` がこのディスクに配置されます。

Azureテンプレート仕様を作成する

AzureポータルでAzureテンプレート仕様を作成し、Web StudioおよびPowerShellコマンドで使用して、MCSマシンカタログを作成または更新できます。

既存のVMのAzureテンプレート仕様を作成するには：

1. Azureポータルに移動します。リソースグループを選択し、VMとネットワークインターフェイスを選択します。上部にある **...** メニューから、**Export template** をクリックします。
2. カタログプロビジョニング用のテンプレート仕様を作成する場合は、**Include parameters** チェックボックスをオフにします。JSONファイルで `parameters` および `variables` セクションが次のように表示されていることを確認します。

   ```
   "parameters": {},

   "variables": {}
   ```

3. 「**ダウンロード**」をクリックして、テンプレートをJSONファイルとして保存します。
4. Azureポータルで、「**テンプレート仕様**」を選択し、「**テンプレートのインポート**」をクリックします。
5. コンピューターに保存されているマシンプロファイル（JSON形式）を参照してインポートします。
6. 「**名前**」、「**サブスクリプション**」、「**リソースグループ**」、「**場所**」、「**バージョン**」を指定します。「**次へ: テンプレートの編集**」をクリックします。
7. 「**確認と作成**」を作成し、テンプレート仕様を作成します。
8. 「**テンプレート仕様**」ページで、作成したテンプレート仕様を確認します。テンプレート仕様をクリックします。左側のパネルで、「**バージョン**」をクリックします。

9. 「**新しいバージョンの作成**」をクリックして、新しいバージョンを作成できます。新しいバージョン番号を指定し、現在のテンプレート仕様に変更を加え、「**確認と作成**」をクリックして、テンプレート仕様の新しいバージョンを作成します。

以下のPowerShellコマンドを使用して、テンプレートスペックとテンプレートバージョンの情報を取得できます。

- テンプレートスペックの情報を取得するには、以下を実行します。

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec
```

- テンプレートスペックバージョンの情報を取得するには、以下を実行します。

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec\bgg1.0.templatespecversion
```

カタログの作成または更新でのテンプレート仕様の使用

MCSマシンカタログは、マシンプロファイル入力としてテンプレート仕様を使用して作成または更新できます。これを行うには、Web StudioまたはPowerShellコマンドを使用できます。

- Web Studioについては、「Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する」を参照してください。
- PowerShellについては、「PowerShellを使用してカタログを作成または更新する際のテンプレート仕様の使用」を参照してください。

Azureサーバー側暗号化

Citrix Virtual Apps and Desktopsは、Azure Key Vaultを介したAzureマネージドディスクの顧客管理暗号化キーをサポートしています。このサポートにより、独自の暗号化キーを使用してマシンカタログのマネージドディスクを暗号化することで、組織およびコンプライアンス要件を管理できます。詳細については、「Azure Disk Storageのサーバー側暗号化」を参照してください。

マネージドディスクでこの機能を使用する場合：

- ディスクの暗号化に使用するキーを変更するには、`DiskEncryptionSet` で現在のキーを変更します。その `DiskEncryptionSet` に関連付けられているすべてのリソースは、新しいキーで暗号化されるように変更されます。

- キーを無効にするか削除すると、そのキーを使用しているディスクを持つすべてのVMは自動的にシャットダウンします。シャットダウン後、キーが再度有効になるか、新しいキーを割り当てるまで、VMは使用できません。そのキーを使用しているカタログは電源をオンにできず、VMを追加することもできません。

顧客管理暗号化キーを使用する際の重要な考慮事項

この機能を使用する際は、次の点を考慮してください。

- 顧客管理キーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンに存在する必要があります。
- 顧客管理キーで暗号化されたディスク、スナップショット、およびイメージは、別のリソースグループやサブスクリプションに移動できません。
- ディスク暗号化セットのリージョンごとの制限については、Microsoft サイトを参照してください。

> **注:**
>
> Azure サーバー側暗号化の構成については、クイックスタート: Azure portal を使用して Key Vault を作成する を参照してください。

Azureカスタマーマネージド暗号化キー

マシンカタログを作成する際、カタログにプロビジョニングされたマシン上のデータを暗号化するかどうかを選択できます。カスタマーマネージド暗号化キーによるサーバー側暗号化を使用すると、マネージドディスクレベルで暗号化を管理し、カタログ内のマシン上のデータを保護できます。ディスク暗号化セット（DES）は、カスタマーマネージドキーを表します。この機能を使用するには、まずAzureでDESを作成する必要があります。DESは次の形式です。

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryptionSet`

リストからDESを選択します。選択するDESは、リソースと同じサブスクリプションとリージョンにある必要があります。

「顧客管理キーを使用したマシンカタログの作成」を参照してください。

ホストでのAzureディスク暗号化

ホストでの暗号化機能を持つMCSマシンカタログを作成できます。現在、MCSはこの機能に対してマシンプロファイルワークフローのみをサポートしています。マシンプロファイルの入力として、VMまたはテンプレート仕様を使用できます。

この暗号化方法は、Azureストレージを介してデータを暗号化しません。VMをホストするサーバーがデータを暗号化し、その後、暗号化されたデータがAzureストレージサーバーを介して流れます。したがって、この暗号化方法はデータをエンドツーエンドで暗号化します。

制限事項：

ホストでのAzureディスク暗号化は次のとおりです。

- すべてのAzureマシンサイズでサポートされているわけではありません
- Azure ディスク暗号化と互換性がありません

ホストでの暗号化機能を持つマシンカタログを作成するには：

1. サブスクリプションでホストでの暗号化機能が有効になっているかどうかを確認します。これを行うには、`<https://learn.microsoft.com/ja-jp/rest/api/resources/features/get?tabs=HTTP/>`を参照してください。有効になっていない場合は、サブスクリプションでこの機能を有効にする必要があります。サブスクリプションで機能を有効にする方法については、`<https://learn.microsoft.com/ja-jp/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/>`を参照してください。
2. 特定のAzure VMサイズがホストでの暗号化をサポートしているかどうかを確認します。これを行うには、PowerShellウィンドウで次のいずれかを実行します。

   ```
   PS XDHyp:\Connections\<your connection>\east
   us.region\serviceoffering.folder>
   ```

   ```
   PS XDHyp:\HostingUnits\<your hosting unit>\serviceoffering.folder>
   ```

3. ホストでの暗号化を有効にして、Azure portalでマシンプロファイルの入力としてVMまたはテンプレート仕様を作成します。
   - VMを作成する場合は、ホストでの暗号化をサポートするVMサイズを選択します。VMを作成すると、VMプロパティの**ホストでの暗号化**が有効になります。

- テンプレート仕様を使用する場合は、`securityProfile`内でパラメーター`Encryption at Host`を**true**として割り当てます。

4. VMまたはテンプレート仕様のいずれかを選択して、マシンプロファイルワークフローでMCSマシンカタログを作成します。

   - OSディスク/データディスク：顧客管理キーとプラットフォーム管理キーを介して暗号化されます
   - エフェメラルOSディスク：プラットフォーム管理キーのみを介して暗号化されます
   - キャッシュディスク: 顧客管理キーとプラットフォーム管理キーによって暗号化されます

   Web StudioまたはPowerShellコマンドを実行して、マシンカタログを作成できます。

マシンプロファイルからホストでの暗号化情報を取得する

`AdditionalData`パラメーターを指定してPowerShellコマンドを実行すると、マシンプロファイルからホストでの暗号化情報を取得できます。`EncryptionAtHost`パラメーターが**True**の場合、そのマシンプロファイルでホストでの暗号化が有効になっていることを示します。

例: マシンプロファイルの入力が VM の場合、次のコマンドを実行します。

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def.v
m).AdditionalData
```

例: マシンプロファイルの入力がテンプレート仕様の場合、次のコマンドを実行します。

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def_t
emplatespec.templatespec\EncryptionAtHost.templatespecversion).AdditionalD
ata
```

マネージドディスクの二重暗号化

二重暗号化を使用してマシンカタログを作成できます。この機能で作成されたカタログはすべて、プラットフォーム管理キーと顧客管理キーの両方でサーバー側で暗号化されます。Azure Key Vault、暗号化キー、およびディスク暗号化セット (DES) はお客様が所有および管理します。

二重暗号化は、プラットフォーム側暗号化 (デフォルト) と顧客管理暗号化 (CMEK) です。したがって、暗号化アルゴリズム、実装、または侵害されたキーに関連するリスクを懸念するセキュ

リティ意識の高いお客様は、この二重暗号化を選択できます。永続OSディスクとデータディスク、スナップショット、およびイメージはすべて、二重暗号化によって保存時に暗号化されます。

注:

- Web StudioおよびPowerShellコマンドを使用して、二重暗号化でマシンカタログを作成および更新できます。PowerShellコマンドについては、「二重暗号化でマシンカタログを作成する」を参照してください。
- 二重暗号化でマシンカタログを作成または更新するには、マシンプロファイルに基づかないワークフローまたはマシンプロファイルに基づくワークフローを使用できます。
- マシンプロファイルに基づかないワークフローを使用してマシンカタログを作成する場合、保存されている `DiskEncryptionSetId` を再利用できます。
- マシンプロファイルを使用する場合、VMまたはテンプレート仕様をマシンプロファイルの入力として使用できます。

制限事項:

- Ultra DisksまたはPremium SSD v2ディスクでは、二重暗号化はサポートされていません。
- アンマネージドディスクでは、二重暗号化はサポートされていません。
- カタログに関連付けられているDiskEncryptionSetキーを無効にすると、そのカタログのVMも無効になります。
- 顧客管理キーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンに存在する必要があります。
- サブスクリプションごとに、リージョンあたり最大50個のディスク暗号化セットしか作成できません。

Azureリソースグループ

Azureプロビジョニングリソースグループは、ユーザーにアプリケーションとデスクトップを提供するVMをプロビジョニングする方法を提供します。MCSマシンカタログを作成する際に、既存の空のAzureリソースグループを追加することも、新しいリソースグループを自動的に作成させることもできます。Azureリソースグループの詳細については、Microsoftドキュメントを参照してください。

Azureリソースグループの使用法

Azureリソースグループあたりの仮想マシン、マネージドディスク、スナップショット、およびイメージの数に制限はありません。（Azureリソースグループあたり240個のVM、800個のマネージドディスクという制限は削除されました。）

- フルスコープのサービスプリンシパルを使用してマシンカタログを作成する場合、MCSは1つのAzureリソースグループのみを作成し、そのグループをカタログに使用します。
- ナロースコープのサービスプリンシパルを使用してマシンカタログを作成する場合、カタログ用に空の、事前に作成されたAzureリソースグループを提供する必要があります。

Azureエフェメラルディスク

Azureエフェメラルディスクを使用すると、キャッシュディスクまたは一時ディスクを再利用して、Azure対応仮想マシンのOSディスクを保存できます。この機能は、標準のHDDディスクよりも高性能なSSDディスクを必要とするAzure環境で役立ちます。Azureエフェメラルディスクを使用してカタログを作成する方法については、Azureエフェメラルディスクを使用してカタログを作成するを参照してください。

> **注記:**
>
> 永続カタログは、エフェメラルOSディスクをサポートしていません。
>
> エフェメラルOSディスクでは、プロビジョニングスキームでマネージドディスクと共有イメージギャラリーを使用する必要があります。

エフェメラルOS一時ディスクの保存

エフェメラルOSディスクをVMの一時ディスクまたはリソースディスクに保存するオプションがあります。この機能により、キャッシュがないか、キャッシュが不十分なVMでエフェメラルOSディスクを使用できます。そのようなVMには、`Ddv4`などのエフェメラルOSディスクを保存するための一時ディスクまたはリソースディスクがあります。

次の点を考慮してください:

- エフェメラルディスクは、VMキャッシュディスク、またはVMの一時（リソース）ディスクのいずれかに保存されます。キャッシュディスクがOSディスクのコンテンツを保持するのに十分な大きさでない場合を除き、キャッシュディスクは一時ディスクよりも優先されます。
- 更新の場合、キャッシュディスクより大きく、一時ディスクより小さい新しいイメージは、エフェメラルOSディスクをVMの一時ディスクに置き換えることになります。

AzureエフェメラルディスクとMachine Creation Services (MCS) ストレージ最適化 (MCS I/O)

AzureエフェメラルOSディスクとMCS I/Oを同時に有効にすることはできません。

重要な考慮事項は次のとおりです。

- エフェメラルOSディスクとMCS I/Oの両方を同時に有効にしてマシンカタログを作成することはできません。
- PowerShellパラメーター (`UseWriteBackCache` および `UseEphemeralOsDisk`) を `New-ProvScheme` または `Set-ProvScheme` で**true**に設定すると、適切なエラーメッセージとともに失敗します。
- 両方の機能が有効になっている状態で作成された既存のマシンカタログの場合、引き続き次のことができます:
  - マシンカタログを更新する。
  - VM を追加または削除する。
  - マシンカタログを削除する。

アジュール コンピュート ギャラリー

Azure で MCS によってプロビジョニングされたマシンの公開イメージリポジトリとして、Azure Compute Gallery (旧称 Azure Shared Image Gallery) を使用します。ギャラリーに公開イメージを保存することで、OS ディスクの作成とハイドレーションを高速化し、非永続 VM の起動時間とアプリケーション起動時間を改善できます。共有イメージギャラリーには、次の3つの要素が含まれています。

- *ギャラリー*: イメージはここに保存されます。MCS は、マシンカタログごとに1つのギャラリーを作成します。
- *ギャラリーイメージ定義*: この定義には、公開イメージに関する情報 (オペレーティングシステムの種類と状態、Azure リージョン) が含まれています。MCS は、カタログ用に作成されたイメージごとに1つのイメージ定義を作成します。
- *ギャラリーイメージバージョン*: Shared Image Gallery の各イメージは複数のバージョンを持つことができ、各バージョンは異なるリージョンに複数のレプリカを持つことができます。各レプリカは、公開イメージの完全なコピーです。

> **注:**
>
> 共有イメージギャラリー機能は、マネージドディスクとのみ互換性があります。レガシーマシンカタログでは使用できません。

> 詳細については、「Azure Compute Gallery の概要」を参照してください。

PowerShell を使用して Azure Compute Gallery イメージでマシンカタログを作成または更新する方法については、「Azure Compute Gallery イメージを使用してマシンカタログを作成または更新する」を参照してください。

Azure 機密 VM

Azure 機密コンピューティング VM は、仮想デスクトップがメモリ内で暗号化され、使用中に保護されることを保証します。

MCS を使用して、Azure 機密 VM を含むカタログを作成できます。このようなカタログを作成するには、マシンプロファイルのワークフローを使用する必要があります。マシンプロファイルの入力として、VM と ARM テンプレート仕様の両方を使用できます。

機密 VM に関する重要な考慮事項

サポートされているVMサイズと、機密VMでマシンカタログを作成する際の重要な考慮事項は次のとおりです。

- サポートされているVMサイズ：機密VMは次のVMサイズをサポートしています。
  - DCasv5 シリーズ
  - DCadsv5 シリーズ
  - ECasv5 シリーズ
  - ECadsv5 シリーズ
- 機密VMを使用してマシンカタログを作成します。
  - Web StudioおよびPowerShellコマンドを使用して、Azure Confidential VMでマシンカタログを作成できます。
  - Azure Confidential VMでマシンカタログを作成するには、マシンプロファイルベースのワークフローを使用する必要があります。VMまたはテンプレート仕様をマシンプロファイルの入力として使用できます。
  - マスターイメージとマシンプロファイルの入力は、両方とも同じ機密セキュリティタイプで有効にする必要があります。セキュリティタイプは次のとおりです。
    - **VMGuestStateOnly**: VMゲストの状態のみが暗号化された機密VM

    - **DiskWithVMGuestState**: OSディスクとVMゲストの状態の両方がプラットフォーム管理キーまたは顧客管理キーで暗号化された機密VM。通常ディスクとエフェメラルOSディスクの両方を暗号化できます。

- マネージドディスク、スナップショット、Azure Compute Galleryイメージ、VM、ARMテンプレート仕様など、さまざまなリソースタイプの機密VM情報をAdditionalDataパラメーターを使用して取得できます。例：

  ```
  PS C:\Users\username> (get-item XDHyp:
  \HostingUnits\mynetwork\image.folder\username-dev-testing-
  rg.resourcegroup\username-dev-tsvda.vm).AdditionalData
  ```

  追加データフィールドは次のとおりです。

    - DiskSecurityType
    - ConfidentialVMDiskEncryptionSetId
    - DiskSecurityProfiles

  マシンサイズの機密コンピューティングプロパティを取得するには、次のコマンドを実行します: `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

  追加データフィールドは`ConfidentialComputingType`です。
- マスターイメージまたはマシンプロファイルを、機密から非機密セキュリティタイプへ、あるいは非機密から機密セキュリティタイプへ変更することはできません。
- 不適切な構成に対しては、適切なエラーメッセージが表示されます。

マスターイメージとマシンプロファイルの準備

機密VMのセットを作成する前に、それらのマスターイメージとマシンプロファイルを準備するために、次の手順に従います:

1. Azureポータルで、次のような特定の構成で機密VMを作成します。

    - **セキュリティの種類**: 機密仮想マシン
    - **機密OSディスク暗号化**: 有効。
    - **キー管理**: プラットフォーム管理キーによる機密ディスク暗号化 機密VMの作成に関する詳細については、このMicrosoft記事を参照してください。

2. 作成したVMでマスターイメージを準備します。作成したVMに必要なアプリケーションとVDAをインストールします。

   > **注:**
   >
   > VHDを使用した機密VMの作成はサポートされていません。代わりに、Azure Compute Gallery、マネージドディスク、またはスナップショットを使用してください。

3. マシンプロファイルは、次のいずれかの方法で作成します。

   - ステップ1で作成した既存のVMが必要なマシンプロパティを持っている場合は、それを使用します。
   - マシンプロファイルとしてARMテンプレート仕様を選択する場合は、必要に応じてテンプレート仕様を作成します。特に、*SecurityEncryptionType* や *diskEncryptionSet* (顧客管理キーの場合) など、機密VMの要件を満たすパラメーターを構成します。詳細については、「Azureテンプレート仕様の作成」を参照してください。

     > **注:**
     >
     > - マスターイメージとマシンプロファイルが同じセキュリティキータイプであることを確認してください。
     > - 顧客管理キーによる機密OSディスク暗号化を必要とする機密VMを作成するには、マスターイメージとマシンプロファイルの両方でディスク暗号化セットIDが同じであることを確認してください。

Web Studio または PowerShell コマンドを使用して機密VMを作成する

機密VMのセットを作成するには、マスターイメージと、目的の機密VMから派生したマシンプロファイルを使用してマシンカタログを作成します。

Web Studioを使用してカタログを作成するには、「マシンカタログの作成」に記載されている手順に従ってください。以下の考慮事項に留意してください。

- **イメージ**ページで、機密VMの作成用に準備したマスターイメージとマシンプロファイルを選択します。マシンプロファイルの選択は必須であり、選択したマスターイメージと同じセキュリティ暗号化タイプに一致するプロファイルのみが選択可能です。

- 「**仮想マシン**」ページでは、機密VMをサポートするマシンサイズのみが選択肢として表示されます。
- 「**ディスク設定**」ページでは、選択したマシンプロファイルから継承されるため、ディスク暗号化セットを指定することはできません。

Azure Marketplace (アジュール マーケットプレイス)

Citrix Virtual Apps and Desktops は、プラン情報を含むAzure上のマスターイメージを使用してマシンカタログを作成することをサポートしています。詳細については、「Microsoft Azure Marketplace」を参照してください。

> **ヒント:**
>
> 標準のWindows Serverイメージなど、Azure Marketplaceで見つかる一部のイメージには、プラン情報が付加されていません。Citrix Virtual Apps and Desktops機能は、有料イメージ向けです。

Shared Image Gallery で作成されたイメージに Azure プラン情報が含まれていることを確認します

このセクションの手順を使用して、Web Studio で Shared Image Gallery のイメージを表示します。これらのイメージは、オプションでマスターイメージとして使用できます。イメージを Shared Image Gallery に配置するには、ギャラリーでイメージ定義を作成します。

Azure Marketplace 共有イメージギャラリー(/en-us/citrix-virtual-apps-desktops/2407/media/azure-marketplace-sig.png)

公開オプションページで、購入プラン情報を確認します。

購入プラン情報フィールドは最初は空です。これらのフィールドに、イメージに使用された購入プラン情報を入力します。購入プラン情報を入力しないと、マシンカタログプロセスが失敗する可能性があります。

Azure MarketplaceがVDA公開オプションを検証する(/en-us/citrix-virtual-apps-desktops/2407/media/azure-marketplace-sig-publishing-options.png)

購入プラン情報を確認したら、定義内にイメージバージョンを作成します。これはマスターイメージとして使用されます。**Add version**をクリックします。

Azure MarketplaceでVDAバージョンを追加する(/en-us/citrix-virtual-apps-desktops/2407/media/azure-marketplace-add-vda-version.png)

Version detailsセクションで、イメージスナップショットまたはマネージドディスクをソースとして選択します。

Azure MarketplaceでVDAオプションを選択する(/en-us/citrix-virtual-apps-desktops/2407/media/azure-marketplace-add-vda-version-info.png)

ネストされた仮想化

マスターVMを入れ子になった仮想化が有効な状態で構成すると、そのマスターVMを使用して作成されたMCSマシンカタログ内のすべてのVMで、入れ子になった仮想化が有効になります。この機能は、永続VMと非永続VMの両方に適用されます。既存のMCSマシンカタログと既存のVMを、イメージ更新によって入れ子になった仮想化を有効にするように更新できます。

現在、入れ子になった仮想化をサポートしているのは、Dv3およびEv3 VMサイズのみです。

ネストされた仮想化の詳細については、Microsoft のブログ Nested Virtualization in Azure を参照してください。

PowerShell を使用してマシンカタログを作成する

このセクションでは、PowerShell を使用してカタログを作成する方法について詳しく説明します。

- 非永続的なライトバックキャッシュディスクを持つカタログを作成する
- 永続的なライトバックキャッシュディスクを持つカタログを作成する
- MCSIO で起動パフォーマンスを向上させる
- PowerShell を使用してカタログを作成または更新する際にテンプレート仕様を使用する
- 信頼された起動を持つマシンカタログ
- マシンプロファイルのプロパティ値を使用する
- 顧客管理の暗号化キーを使用してマシンカタログを作成する
- 二重暗号化を使用してマシンカタログを作成する
- Azure エフェメラルディスクを使用してカタログを作成する
- Azure 専用ホスト
- Azure Compute Gallery イメージを使用してマシンカタログを作成または更新する
- 共有イメージギャラリーを構成する
- 指定された可用性ゾーンにマシンをプロビジョニングする
- ストレージの種類

- ページファイル設定の更新
- Azure Spot VM を使用したカタログの作成
- バックアップ VM サイズの構成
- すべてのリソースにタグをコピー
- Azure Monitor Agent がインストールされたカタログ VM のプロビジョニング

非永続的なライトバックキャッシュディスクを持つカタログの作成

非永続的なライトバックキャッシュディスクを持つカタログを構成するには、PowerShell パラメーター `New-ProvScheme CustomProperties` を使用します。カスタムプロパティ `UseTempDiskForWBC` は、ライトバックキャッシュファイルを保存するために Azure 一時ストレージを使用することを受け入れるかどうかを示します。一時ディスクをライトバックキャッシュディスクとして使用する場合は、`New-ProvScheme` の実行時にこれを true に構成する必要があります。このプロパティが指定されていない場合、パラメーターはデフォルトで **False** に設定されます。

例えば、`CustomProperties` パラメーターを使用して `UseTempDiskForWBC` を **true** に設定する場合:

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="true"/
> `
```

```
</CustomProperties>'
```

注:

ライトバックキャッシュファイルにAzureローカル一時ストレージを使用するようにマシンカタログをコミットした後、後でVHDを使用するように変更することはできません。

永続的なライトバックキャッシュディスクを持つカタログを作成する

永続的なライトバックキャッシュディスクを持つカタログを構成するには、PowerShell パラメーター `New-ProvScheme CustomProperties` を使用します。このパラメーターは、MCS でプロビジョニングされたマシンに対してライトバックキャッシュディスクがどのように永続化されるかを決定するために使用される追加のプロパティ `PersistWBC` をサポートします。`PersistWBC` プロパティは、`UseWriteBackCache` パラメーターが指定され、`WriteBackCacheDiskSize` パラメーターがディスクが作成されることを示すように設定されている場合にのみ使用されます。

`PersistWBC` をサポートする前の `CustomProperties` パラメーターに見られるプロパティの例は次のとおりです。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

</CustomProperties>
```

これらのプロパティを使用する場合、`CustomProperties` パラメーターからプロパティが省略されていると、それらはデフォルト値を含むことに注意してください。`PersistWBC` プロパティには、**true** または **false** の2つの可能な値があります。

`PersistWBC`プロパティを**true**に設定しても、Citrix Virtual Apps and Desktops管理者がWeb Studioを使用してマシンをシャットダウンするときに、ライトバックキャッシュディスクは削除されません。

`PersistWBC`プロパティを**false**に設定すると、Citrix Virtual Apps and Desktops管理者がWeb Studioを使用してマシンをシャットダウンするときに、ライトバックキャッシュディスクが削除されます。

注：

`PersistWBC`プロパティが省略されている場合、プロパティのデフォルトは**false**になり、Web Studioを使用してマシンがシャットダウンされるとライトバックキャッシュは削除されます。

たとえば、`CustomProperties`パラメーターを使用して`PersistWBC`をtrueに設定するには：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

重要：

`PersistWBC`プロパティは、`New-ProvScheme` PowerShellコマンドレットを使用してのみ設定できます。作成後にプロビジョニングスキームの`CustomProperties`を変更しようと

しても、マシンカタログや、マシンのシャットダウン時のライトバックキャッシュディスクの永続性には影響しません。

たとえば、`New-ProvScheme`をライトバックキャッシュを使用するように設定し、`PersistWBC`プロパティをtrueに設定するには：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127
```

```
-WriteBackCacheMemorySize 256
```

MCSIOで起動パフォーマンスを向上させる

MCSIOが有効になっている場合、AzureおよびGCPのマネージドディスクの起動パフォーマンスを向上させることができます。この機能を構成するには、`New-ProvScheme`コマンドでPowerShell `PersistOSDisk`カスタムプロパティを使用します。`New-ProvScheme`に関連するオプションは次のとおりです。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->

````````Groups" Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```

この機能を有効にするには、`PersistOSDisk`カスタムプロパティを`true`に設定します。例：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"
```
```

```
-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

PowerShellを使用してカタログを作成または更新する際にテンプレート仕様を使用する

マシンプロファイル入力としてテンプレート仕様を使用して、MCSマシンカタログを作成または更新できます。これを行うには、Web StudioまたはPowerShellコマンドを使用できます。

Web Studioについては、「Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する」を参照してください。(#create-a-machine-catalog-using-an-azure-resource-manager-image-in-web-studio)

PowerShellコマンドを使用する場合：

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. カタログを作成または更新します。
    - カタログを作成するには：
        a. テンプレート仕様をマシンプロファイルの入力として使用して、`New-ProvScheme`コマンドを使用します。例：

```
New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
image.folder/fgthj.resourcegroup/nab-ws-
vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>

[-LoggingId <Guid>]

[-BearerToken <String>][-AdminAddress <String>]

[<CommonParameters>]
```

b. カタログの作成を完了します。

- カタログを更新するには、テンプレート仕様をマシンプロファイルの入力として使用して、`Set-ProvScheme`コマンドを使用します。例：

```
Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
Us.region/vm.folder/MasterDisk.vm'

MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/testing.templatespec/V1.templatespecversion'

[-ProvisioningSchemeName] <String>

[-CustomProperties <String>][-ServiceOffering <String>] [-PassThru]

[-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <String>]
[<CommonParameters>]
```

信頼できる起動によるマシンカタログ

信頼できる起動でマシンカタログを正常に作成するには、以下を使用します。

- 信頼できる起動を備えたマシンプロファイル
- 信頼できる起動をサポートするVMサイズ
- 信頼できる起動をサポートするWindows VMバージョン。現在、Windows 10、Windows 11、Windows Server 2016、2019、および2022が信頼できる起動をサポートしています。

> **重要：**
>
> MCSは、信頼できる起動が有効なVMを使用して新しいカタログを作成することをサポートしています。ただし、既存の永続カタログと既存のVMを更新するには、Azure portalを使用する必要があります。非永続カタログの信頼できる起動を更新することはできません。詳しくは、MicrosoftドキュメントのEnable Trusted launch on existing Azure VMsを参照してください。

> Citrix Virtual Apps and Desktopsの提供インベントリ項目を表示し、VMサイズが信頼できる起動をサポートしているかどうかを判断するには、次のコマンドを実行します。

1. PowerShell ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、**asnp citrix***を実行します。
3. 次のコマンドを実行します。

   ```
   $s = (ls XDHyp:\HostingUnits\<name of hosting
   unit>\serviceoffering.folder\"<VM size>.serviceoffering)
   ```

4. `$s | select -ExpandProperty Additionaldata` を実行します。
5. `SupportsTrustedLaunch` 属性の値を確認します。
   - `SupportsTrustedLaunch` が**True**の場合、VMサイズはトラステッド起動をサポートしています。
   - `SupportsTrustedLaunch` が**False**の場合、VMサイズはトラステッド起動をサポートしていません。

AzureのPowerShellに従って、トラステッド起動をサポートするVMサイズを判断するには、次のコマンドを使用できます。

```
(Get-AzComputeResourceSku | where {$_.Locations.Contains($region) -and
($_.Name -eq "<VM size>") })[0].Capabilities
```

Azure PowerShell コマンドを実行した後、VM サイズが信頼された起動をサポートするかどうかを説明する例を次に示します。

- *例 1*: Azure VM が Generation 1 のみをサポートしている場合、その VM は信頼された起動をサポートしていません。したがって、Azure PowerShell コマンドを実行しても、`TrustedLaunchDisabled` 機能は表示されません。
- *例 2*: Azure VM が Generation 2 のみをサポートし、`TrustedLaunchDisabled` 機能が **True** の場合、Generation 2 VM サイズは信頼された起動ではサポートされません。
- *例 3*: Azure VM が Generation 2 のみをサポートし、PowerShell コマンドを実行しても `TrustedLaunchDisabled` 機能が表示されない場合、Generation 2 VM サイズは信頼された起動でサポートされます。

Azure仮想マシンのトラステッド起動の詳細については、Microsoftドキュメント「Azure仮想マシンのトラステッド起動」を参照してください。

トラステッド起動でマシンカタログを作成する

1. トラステッド起動が有効なマスターイメージを作成します。Microsoftドキュメント「トラステッド起動VMイメージ」を参照してください。
2. セキュリティの種類を **trusted launch virtual machines** として VM またはテンプレート仕様を作成します。VM またはテンプレート仕様の作成の詳細については、Microsoft ドキュメント「Deploy a trusted launch VM」を参照してください。
3. Web StudioまたはPowerShellコマンドを使用してマシンカタログを作成します。
   - Web Studioを使用する場合は、「Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する」を参照してください。
   - PowerShellコマンドを使用する場合は、VMまたはテンプレート仕様をマシンプロファイルの入力として`New-ProvScheme`コマンドを使用します。カタログを作成するためのコマンドの完全なリストについては、「カタログの作成」を参照してください。

     VMをマシンプロファイルの入力とする`New-ProvScheme`の例:

     ```
     New-ProvScheme -CleanOnBoot -HostingUnitName "name"
     -IdentityPoolName "name" -InitialBatchSizeHint 1

     -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
     fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

     -MachineProfile "XDHyp:
     \HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<mac
     ```

```
hine profile vm.vm>"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>]

[<CommonParameters>]
```

テンプレート仕様をマシンプロファイルの入力とする`New-ProvScheme`の例:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name"
-IdentityPoolName "name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>]

[<CommonParameters>]
```

信頼された起動でマシンカタログを作成する際のエラー

信頼された起動でマシンカタログを作成する際に、以下のシナリオで適切なエラーが発生します。

シナリオ	エラー
アンマネージドカタログの作成中にマシンプロファイルを選択した場合	`MachineProfileNotSupportedForUnmanagedCatalog`

シナリオ	エラー
マスターイメージとしてアンマネージドディスクを使用するカタログの作成中に、信頼された起動をサポートするマシンプロファイルを選択した場合	`SecurityTypeNotSupportedForUnmanagedDisk`
セキュリティの種類として信頼された起動を持つマスターイメージソースでマネージドカタログを作成する際に、マシンプロファイルを選択しない場合	`MachineProfileNotFoundForTrustedLaunchMasterImage`
マスターイメージのセキュリティの種類とは異なるセキュリティの種類を持つマシンプロファイルを選択した場合	`SecurityTypeConflictBetweenMasterImageAndMachineProfile`
Trusted launchをサポートしないVMサイズを選択したが、カタログ作成時にTrusted launchをサポートするマスターイメージを使用した場合	`MachineSizeNotSupportTrustedLaunch`

マシンプロファイルプロパティ値の使用

マシンカタログは、カスタムプロパティで定義されている次のプロパティを使用します。

- アベイラビリティゾーン
- 専用ホストグループID
- ディスク暗号化セットID
- OSの種類
- ライセンスの種類
- ストレージの種類

これらのカスタムプロパティが明示的に定義されていない場合、プロパティ値は、マシンプロファイルとして使用されるARMテンプレート仕様またはVMから設定されます。さらに、`ServiceOffering`が指定されていない場合、マシンプロファイルから設定されます。

> **注:**

> マシンプロファイルに一部のプロパティが欠落しており、カスタムプロパティで定義されていない場合、該当する場所ではプロパティのデフォルト値が適用されます。

> 次のセクションでは、`CustomProperties` がすべてのプロパティを定義しているか、値がMachineProfileから派生している場合の、`New-ProvScheme` および `Set-ProvScheme` におけるいくつかのシナリオについて説明します。

- New-ProvSchemeのシナリオ
  - MachineProfileにすべてのプロパティがあり、CustomPropertiesが定義されていない場合。
    例:

    `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

    カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpA-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="<mpA-value>"/>

<Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
Value="<mpA-value>"/>

<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
value>"/>
```

```
</CustomProperties>
```

- MachineProfileに一部のプロパティがあり、CustomPropertiesが定義されていない場合。例: MachineProfileにはLicenseTypeとOsTypeのみがあります。

  `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

  カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
value>"/>

</CustomProperties>
```

- MachineProfileとCustomPropertiesの両方がすべてのプロパティを定義している場合。例:

  `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

  カスタムプロパティが優先されます。カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>
```

```
<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones"
Value="<CustomPropertiesA-value>"/>

</CustomProperties>
```

- MachineProfileで一部のプロパティが定義され、CustomPropertiesで一部のプロパティが定義されている場合。例:
  - CustomProperties は LicenseType と StorageAccountType を定義します
  - MachineProfile は LicenseType、OsType、および Zones を定義します

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

カタログのカスタムプロパティとして、次の値が設定されます。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>
```

```
<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
value>"/>

</CustomProperties>
```

- 一部のプロパティは MachineProfile で定義され、一部のプロパティは CustomProperties で定義されています。さらに、ServiceOffering は定義されていません。例:
  - CustomProperties は StorageType を定義します
  - MachineProfile は LicenseType を定義します

```
New-ProvScheme -MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mp
.vm"

-ServiceOffering "XDHyp:
\HostingUnits\azureunit\serviceoffering.folder\<explicit-machine-
size>.serviceoffering"
```

カタログのカスタムプロパティとして、次の値が設定されます。

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<explicit-machine-size>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="explicit-storage-type"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="value-
from-machineprofile"/>
```

```
</CustomProperties>
```

- OsType が CustomProperties にも MachineProfile にも含まれていない場合、次のようになります:
  - 値はマスターイメージから読み取られます。
  - マスターイメージがアンマネージドディスクの場合、OsType は Windows に設定されます。例:

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -MasterImageVM "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-image.manageddisk"`

マスターイメージからの値は、この場合 Linux のカスタムプロパティに書き込まれます。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="OSType" Value="Linux"/>

</CustomProperties>
```

- Set-ProvSchemeのシナリオ
  - 既存のカタログで、次のものを含む:
    - カスタムプロパティ（`StorageAccountType`およびOsType）
    - ゾーンを定義する MachineProfile `mpA.vm`
  - 更新:
    - StorageAccountType を定義する MachineProfile mpB.vm
    - LicenseType と OsType を定義する新しいカスタムプロパティセット $CustomPropertiesB

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm" -CustomProperties $CustomPropertiesB`

カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesB-value>"/>

    </CustomProperties>
```

- 既存のカタログ (以下を含む):
  - S`torageAccountType` および OsType の CustomProperties
  - StorageAccountType と LicenseType を定義する MachineProfile `mpA.vm`
- 更新:
  - StorageAccountType と OsType を定義する新しいカスタムプロパティセット $CustomPropertiesB。

`Set-ProvScheme -CustomProperties $CustomPropertiesB`

カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
```

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mp-A-
value>"/>

</CustomProperties>
```

- 既存のカタログ (以下を含む):
  - カスタムプロパティ（`StorageAccountType`およびOsType）
  - ゾーンを定義するMachineProfile `mpA.vm`
- 更新:
  - StorageAccountType と LicenseType を定義する MachineProfile mpB.vm
  - `ServiceOffering` は指定されていません

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm"`

カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<value-from-machineprofile>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<prior-
```

```
CustomProperties-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpB-
value>"/>

</CustomProperties>
```

Azure Monitor Agent がインストールされたカタログVMをプロビジョニングする

Azure モニタリングは、Azure およびオンプレミス環境からのテレメトリデータを収集、分析、および操作するために使用できるサービスです。

Azure Monitor Agent (AMA) は、仮想マシンなどのコンピューティングリソースから監視データを収集し、そのデータを Azure Monitor に配信します。現在、イベントログ、Syslog、パフォーマンスメトリックの収集をサポートしており、Azure Monitor Metrics および Azure Monitor Logs のデータソースに送信します。

監視データ内のVMを一意に識別して監視を有効にするには、MCS マシンカタログのVMを、AMA を拡張機能としてインストールしてプロビジョニングできます。

要件

- 権限: 必要な Azure 権限 に指定されている最小限の Azure 権限と、Azure Monitor を使用するための以下の権限があることを確認してください:
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- データ収集ルール: Azure portal でデータ収集ルールを設定します。DCR の設定については、「データ収集ルールを作成する」を参照してください。DCR はプラットフォーム固有 (Windows または Linux) です。必要なプラットフォームに応じて DCR を作成してください。AMA は、データ収集ルール (DCR) を使用して、VM などのリソースと、Azure Monitor Metrics や Azure Monitor Logs などのデータソース間のマッピングを管理します。
- デフォルトワークスペース: Azure portal でワークスペースを作成します。ワークスペースの作成については、「Log Analytics ワークスペースを作成する」を参照してください。ログとデータを収集すると、その情報はワークスペースに保存されます。ワークスペースには一意のワークスペース ID とリソース ID があります。ワークスペース名は、特定のリソースグループに対

して一意である必要があります。ワークスペースを作成したら、データソースとソリューションを設定して、そのデータをワークスペースに保存します。

- モニター拡張機能のホワイトリスト登録: 拡張機能 `AzureMonitorWindowsAgent` および `AzureMonitorLinuxAgent` は、Citrix が定義したホワイトリスト登録済み拡張機能です。ホワイトリスト登録済み拡張機能のリストを表示するには、PoSH コマンド `Get-ProvMetadataConfiguration` を使用します。
- マスターイメージ: Microsoft は、既存のマシンから新しいマシンを作成する前に、既存のマシンから拡張機能を削除することを推奨しています。拡張機能が削除されない場合、残存ファイルや予期しない動作につながる可能性があります。詳細については、「既存の VM から VM を再作成する場合」を参照してください。

AMA を有効にしてカタログ VM をプロビジョニングするには:

1. マシンプロファイルテンプレートを設定します。
   - VMをマシンプロファイルテンプレートとして使用する場合：
     a. Azure portal で VM を作成します。
     b. VMの電源を入れます。
     c. **リソース**の下のデータ収集ルールにVMを追加します。これにより、テンプレートVMにエージェントのインストールが呼び出されます。

> **注:**
>
> Linuxカタログを作成する必要がある場合は、Linuxマシンを設定します。

   - テンプレート仕様をマシンプロファイルテンプレートとして使用する場合：
     a. テンプレート仕様を設定します。
     b. 生成されたテンプレート仕様に、次の拡張機能とデータ収集ルール関連付けを追加します:

```
{

"type": "Microsoft.Compute/virtualMachines/extensions",

"apiVersion": "2022-03-01",
```

```
"name": "<vm-name>/AzureMonitorWindowsAgent",

"dependsOn": [

    "Microsoft.Compute/virtualMachines/<vm-name>"

],

"location": "<azure-region>",

"properties": {

    "publisher": "Microsoft.Azure.Monitor",

    "type": "AzureMonitorWindowsAgent",

    "typeHandlerVersion": "1.0",

    "autoUpgradeMinorVersion": true,

    "enableAutomaticUpgrade": true

}

},

 {

    "type": "Microsoft.Insights/dataCollectionRuleAssociations",

    "apiVersion": "2021-11-01",

    "name": "<associatio-name>",

    "scope": "Microsoft.Compute/virtualMachines/<vm-name>",

    "dependsOn": [

     "Microsoft.Compute/virtualMachines/<vm-name>",

    "Microsoft.Compute/virtualMachines/<vm-name>/extensions/
AzureMonitorWindowsAgent"
```

```
    ],

    "properties": {

       "description": "Association of data collection rule.
Deleting this association will break the data collection for this
Arc server.",

     "dataCollectionRuleId": "/subscriptions/<azure-
subscription>/resourcegroups/<azure-resource-group>/providers/
microsoft.insights/datacollectionrules/<azure-data-collection-
rule>"

     }

    }
```

2. 既存のMCSマシンカタログを作成または更新します。

   - 新しいMCSカタログを作成するには:

     a. Web Studioで、そのVMまたはテンプレート仕様をマシンプロファイルとして選択します。

     b. カタログを作成するための次の手順に進みます。

   - 既存のMCSカタログを更新するには、次のPoSHコマンドを使用します:

     - 新しいVMに更新されたマシンプロファイルテンプレートを取得させるには、次のコマンドを実行します:

```
Set-ProvScheme -ProvisioningSchemeName "name"

-MachineProfile "XDHyp:
\HostingUnits\Unit1\machineprofile.folder\abc.resourcegroup\ab-
machine-profile.vm"
```

     - 既存のVMを更新されたマシンプロファイルテンプレートで更新するには:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

3. カタログVMの電源を入れます。
4. Azureポータルに移動し、モニター拡張機能がVMにインストールされていること、およびVMがDCRのリソースの下に表示されていることを確認します。数分後、監視データがAzure Monitorに表示されます。

トラブルシューティング

Azure Monitor Agentのトラブルシューティングガイダンスについては、以下を参照してください:

- https://learn.microsoft.com/ja-jp/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/ja-jp/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

顧客管理の暗号化キーでマシンカタログを作成する

顧客管理の暗号化キーを使用してマシンカタログを作成する詳細な手順は次のとおりです。

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために `asnp citrix*` を実行します。
3. `cd xdhyp:/` を入力します。
4. `cd .\HostingUnits\(your hosting unit)` を入力します。
5. `cd diskencryptionset.folder` を入力します。
6. ディスク暗号化セットのリストを取得するには、`dir` を入力します。
7. ディスク暗号化セットのIDをコピーします。
8. ディスク暗号化セットのIDを含めるカスタムプロパティ文字列を作成します。例：

```
$customProperties = "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"Standard_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"persistWBC`"
Value=`"False`" />

<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"false`" />
```

```
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/resourceGroups/
abc/providers/Microsoft.Compute/diskEncryptionSets/abc-des`"/>

</CustomProperties>
```

9. まだ作成されていない場合は、IDプールを作成します。例：

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain def.local -NamingSchemeType Numeric
```

10. New-ProvSchemeコマンドを実行します。例：

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\azure-
res2\image.folder\def.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-res2\
\virtualprivatecloud.folder\def.resourcegroup\def-
vnet.virtualprivatecloud\subnet1.network"}

-ProvisioningSchemeName "name"

-ServiceOffering "XDHyp:\HostingUnits\azure-
res2\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-MachineProfile "XDHyp:
\HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<machin
e profile vm.vm>"

-CustomProperties $customProperties
```

11. マシンカタログの作成を完了します。

二重暗号化でマシンカタログを作成する

Web Studio および PowerShell コマンドを使用して、二重暗号化されたマシンカタログを作成および更新できます。

二重暗号化でマシンカタログを作成する詳細な手順は次のとおりです。

1. プラットフォーム管理キーと顧客管理キーを使用して、Azure Key VaultとDESを作成します。Azure Key VaultとDESの作成方法については、マネージドディスクの保存時にAzureポータルを使用して二重暗号化を有効にするを参照してください。
2. ホスティング接続で利用可能なDiskEncryptionSetsを参照するには：
   a. **PowerShell**ウィンドウを開きます。
   b. 次のPowerShellコマンドを実行します：
      i. `asnp citrix*`
      ii. `cd xdhyp:`:
      iii. `cd HostingUnits`
      iv. `cd YourHostingUnitName` (例として azure-east など)
      v. `cd diskencryptionset.folder`
      vi. `dir`

   カスタムプロパティを使用してカタログを作成または更新するには、`DiskEncryptionSet`のIDを使用できます。
3. マシンプロファイルワークフローを使用する場合は、VMまたはテンプレート仕様をマシンプロファイル入力として作成します。
   - VMをマシンプロファイル入力として使用する場合：
     a. Azure PortalでVMを作成します。
     b. **ディスク>キー管理**に移動して、任意の`DiskEncryptionSetID`でVMを直接暗号化します。
   - テンプレート仕様をマシンプロファイル入力として使用する場合：
     a. テンプレートの`properties>storageProfile>osDisk>managedDisk`の下に、`diskEncryptionSet`パラメーターを追加し、二重暗号化DESのIDを追加します。
4. マシンカタログを作成します。

- Web Studioを使用している場合は、マシンカタログの作成の手順に加えて、次のいずれかを実行します。
  - マシンプロファイルベースのワークフローを使用しない場合は、**ディスク設定**ページで、**各マシン上のデータを暗号化するために次のキーを使用**を選択します。次に、ドロップダウンメニューから二重暗号化DESを選択します。カタログの作成を続行します。
  - マシンプロファイルワークフローを使用している場合は、**イメージ**ページでマスターイメージとマシンプロファイルを選択します。マシンプロファイルのプロパティにディスク暗号化セットIDがあることを確認してください。

  カタログで作成されたすべてのマシンは、選択した DES に関連付けられたキーによって二重に暗号化されます。
- PowerShellコマンドを使用している場合は、次のいずれかを実行します。
  - マシンプロファイルベースのワークフローを使用しない場合は、`New-ProvScheme`コマンドにカスタムプロパティ`DiskEncryptionSetId`を追加します。例：

```
New-ProvScheme -CleanOnBoot -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />

</CustomProperties>'

-HostingUnitName "Redacted"

-IdentityPoolName "Redacted"

-InitialBatchSizeHint 1
```

```
-MasterImageVM "Redacted"

-NetworkMapping @{"0"="Redacted"}

-ProvisioningSchemeName "Redacted"

-ServiceOffering "Redacted"
```

- マシンプロファイルベースのワークフローを使用する場合は、`New-ProvScheme`コマンドでマシンプロファイル入力を利用します。例:

```
New-ProvScheme -CleanOnBoot

-HostingUnitName azure-east

-IdentityPoolName aio-ip

-InitialBatchSizeHint 1

-MasterImageVM XDHyp:\HostingUnits\azure-
east\image.folder\abc.resourcegroup\fgb-vda-snapshot.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-
east\virtualprivatecloud.folder\apa-
resourceGroup.resourcegroup\apa-resourceGroup-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName aio-test

-MachineProfile XDHyp:\HostingUnits\azure-
east\machineprofile.folder\abc.resourcegroup\abx-
mp.templatespec\1.0.0.templatespecversion
```

5. リモートPowerShell SDKを使用してカタログの作成を完了します。リモートPowerShell SDKを使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。カタログで作成されたすべてのマシンは、選択したDESに関連付けられたキーによって二重に暗号化されます。

暗号化されていないカタログを二重暗号化を使用するように変換する

マシンカタログの暗号化タイプ（カスタムプロパティまたはマシンプロファイルを使用）を更新できます。

- マシンプロファイルベースのワークフローを使用しない場合は、`Set-ProvScheme`コマンドにカスタムプロパティDiskEncryptionSetIdを追加します。例：

```
Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/12345678-xxxx-1234-1234-123456789012/resourceGroups/
Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/
SampleEncryptionSet" />

</CustomProperties>'
```

- マシンプロファイルベースのワークフローを使用している場合は、`Set-ProvScheme`コマンドでマシンプロファイル入力を使用します。例：

```
Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
XDHyp:\HostingUnits\azure-
east\machineprofile.folder\aelx.resourcegroup\elx-
mp.templatespec\1.0.0.templatespecversion
```

成功すると、カタログに追加するすべての新しいVMは、選択したDESに関連付けられたキーによって二重暗号化されます。

カタログが二重暗号化されていることを確認する

- ウェブスタジオで:

a. **マシンカタログ**に移動します。

b. 確認するカタログを選択します。画面下部にある**テンプレートプロパティ**タブをクリックします。

c. **Azureの詳細**の下で、**ディスク暗号化セット**のディスク暗号化セットIDを確認します。カタログのDES IDが空白の場合、カタログは暗号化されていません。

d. Azure Portal で、DES ID に関連付けられている DES の暗号化の種類がプラットフォーム管理キーと顧客管理キーであることを確認します。

- PowerShellコマンドを使用する:

a. **PowerShell** ウィンドウを開きます。

b. `asnp citrix*` を実行して、Citrix 固有の PowerShell モジュールをロードします。

c. `Get-ProvScheme` を使用して、マシンカタログの情報を取得します。例:

```
Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
```

d. マシンカタログの DES ID カスタムプロパティを取得します。例:

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-1234-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />
```

e. Azure Portal で、DES ID に関連付けられている DES の暗号化の種類がプラットフォーム管理キーと顧客管理キーであることを確認します。

Azureエフェメラルディスクを使用してカタログを作成する

エフェメラルディスクを使用するには、`New-ProvScheme` の実行時にカスタムプロパティ `UseEphemeralOsDisk` を **true** に設定する必要があります。

注:

カスタムプロパティ `UseEphemeralOsDisk` が **false** に設定されているか、値が指定されていない場合、すべてのプロビジョニングされたVDAは、プロビジョニングされたOSディスクを使い続けます。

以下は、プロビジョニングスキームで使用するカスタムプロパティのセットの例です。

```
"CustomProperties": [

            {
```

```
            "Name": "UseManagedDisks",
            "Value": "true"
        },
        {
            "Name": "StorageType",
            "Value": "Standard_LRS"
        },
        {
            "Name": "UseSharedImageGallery",
            "Value": "true"
        },
        {
            "Name": "SharedImageGalleryReplicaRatio",
            "Value": "40"
        },
        {
            "Name": "SharedImageGalleryReplicaMaximum",
            "Value": "10"
        },
        {
            "Name": "LicenseType",
            "Value": "Windows_Server"
```

```
            },
            {
                "Name": "UseEphemeralOsDisk",
                "Value": "true"
            }
        ],
```

カタログのエフェメラルディスクを構成する

カタログのAzureエフェメラルOSディスクを構成するには、`Set-ProvScheme`で`UseEphemeralOsDisk`パラメーターを使用します。`UseEphemeralOsDisk`パラメーターの値を**true**に設定します。

注:

この機能を使用するには、`UseManagedDisks`と`UseSharedImageGallery`のパラメーターも有効にする必要があります。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk"
Value="true" />

</CustomProperties>'
```

エフェメラルディスクに関する重要な考慮事項

`New-ProvScheme` を使用してエフェメラルOSディスクをプロビジョニングするには、次の制約を考慮してください。

- カタログに使用されるVMサイズは、エフェメラルOSディスクをサポートしている必要があります。
- VMサイズに関連付けられているキャッシュまたは一時ディスクのサイズは、OSディスクのサイズ以上である必要があります。
- 一時ディスクのサイズは、キャッシュディスクのサイズよりも大きくする必要があります。

また、以下の点も考慮してください。

- プロビジョニングスキームを作成する際。
- プロビジョニングスキームを変更する際。
- イメージを更新する際。

Azure 専用ホスト

MCS を使用して、Azure 専用ホストに VM をプロビジョニングできます。Azure 専用ホストに VM をプロビジョニングする前に、次の手順を実行します。

- ホストグループを作成します。
- そのホストグループ内にホストを作成します。
- カタログと仮想マシンを作成するために、十分なホスト容量が予約されていることを確認します。

次の PowerShell スクリプトを使用して、ホストテナンシーが定義されたマシンのカタログを作成できます。

```
New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <Property xsi:type="StringProperty" Name="HostGroupId"
Value="myResourceGroup/myHostGroup" />

 ...other Custom Properties...

 </CustomProperties>
```

MCS を使用して Azure 専用ホストに仮想マシンをプロビジョニングする場合、次の点を考慮してください。

- *専用ホスト*はカタログプロパティであり、カタログ作成後に変更することはできません。専用テナンシーは現在、Azure ではサポートされていません。
- `HostGroupId` パラメーターを使用する場合、ホスティングユニットのリージョンに、事前に構成された Azure ホストグループが必要です。
- Azure の自動配置が必要です。この機能は、ホストグループに関連付けられたサブスクリプションをオンボードするための要求を行います。詳細については、「VM Scale Set on Azure Dedicated Hosts - Public Preview」を参照してください。自動配置が有効になっていない場合、MCS はカタログ作成中にエラーをスローします。

Azure Compute Gallery イメージを使用してマシンカタログを作成または更新する

マシンカタログを作成するために使用するイメージを選択する際、Azure Compute Gallery で作成したイメージを選択できます。

これらのイメージを表示するには、次の操作を行う必要があります。

1. Citrix Virtual Apps and Desktopsサイトを構成します。
2. Azure Resource Managerに接続します。
3. Azure portalで、リソースグループを作成します。詳細については、「ポータルを使用してAzure Compute Galleryを作成する」を参照してください。
4. リソースグループで、Azure Compute Galleryを作成します。
5. Azure Compute Galleryで、イメージ定義を作成します。
6. イメージ定義で、イメージバージョンを作成します。

Azure Compute Gallery のイメージを使用してマシンカタログを作成または更新するには、次の PowerShell コマンドを使用します。

1. PowerShell ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group")
```

4. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group\sharedImageGallery.sharedimagegallery")
```

5. 1つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group\sharedImageGallery.sharedimagegallery\sigtestimage.imagedefinitio
n")
```

6. 次の要素を使用してMCSカタログを作成および更新します。

   - リソースグループ
   - ギャラリー
   - ギャラリーイメージ定義
   - ギャラリーイメージバージョン

   Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/ を参照してください。

共有イメージギャラリーの構成

`New-ProvScheme` コマンドを使用して、Shared Image Gallery をサポートするプロビジョニングスキームを作成します。`Set-ProvScheme` コマンドを使用して、プロビジョニングスキームのこの機能を有効または無効にし、レプリカ比率とレプリカの最大値を変更します。

Shared Image Gallery 機能をサポートするために、プロビジョニングスキームに3つのカスタムプロパティが追加されました。

`UseSharedImageGallery`

- 公開されたイメージの保存に Shared Image Gallery を使用するかどうかを定義します。**True** に設定すると、イメージは Shared Image Gallery イメージとして保存され、それ以外の場合はスナップショットとして保存されます。
- 有効な値は**True**と**False**です。

- プロパティが定義されていない場合、デフォルト値は**False**です。

`SharedImageGalleryReplicaRatio`

- マシンとギャラリーイメージバージョンレプリカの比率を定義します。
- 有効な値は0より大きい整数です。
- プロパティが定義されていない場合、デフォルト値が使用されます。永続OSディスクのデフォルト値は1000、非永続OSディスクのデフォルト値は40です。

`SharedImageGalleryReplicaMaximum`

- 各ギャラリーイメージバージョンのレプリカの最大数を定義します。
- プロパティが定義されていない場合、デフォルト値は100です。
- プロパティが定義されていない場合、デフォルト値は100です。

> **ヒント:**
>
> MCSプロビジョニングされたカタログの公開イメージを保存するためにShared Image Galleryを使用する場合、MCSはカタログ内のマシンの数、レプリカ比率、およびレプリカの最大値に基づいてギャラリーイメージバージョンのレプリカ数を設定します。レプリカ数は、カタログ内のマシンの数をレプリカ比率で割って（最も近い整数に切り上げて）計算され、その値を最大レプリカ数で制限します。たとえば、レプリカ比率が20で最大値が5の場合、0〜20台のマシンには1つのレプリカが作成され、21〜40台には2つのレプリカ、41〜60台には3つのレプリカ、61〜80台には4つのレプリカ、81台以上には5つのレプリカが作成されます。

ユースケース：Shared Image Gallery のレプリカ比率とレプリカの最大値の更新

既存のマシンカタログは Shared Image Gallery を使用しています。`Set-ProvScheme` コマンドを使用して、カタログ内のすべての既存マシンおよび将来のマシンのカスタムプロパティを更新します。

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
```

```
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

ユースケース：スナップショットカタログを Shared Image Gallery カタログに変換する

このユースケースの場合:

1. `UseSharedImageGallery`フラグを**True**に設定して`Set-ProvScheme`を実行します。オプションで`SharedImageGalleryReplicaRatio`および`SharedImageGalleryReplicaMaximum`プロパティを含めます。
2. カタログを更新します。
3. マシンの電源を入れ直して、強制的に更新します。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

ヒント:

パラメーター`SharedImageGalleryReplicaRatio`と`SharedImageGalleryReplicaMaximum`は必須ではありません。`Set-ProvScheme`コマンドが完了しても、Shared Image Galleryイメージはまだ作成されていません。カタログがギャラリーを使用するように構成されると、次のカタログ更新操作で公開イメージがギャラリーに保存されます。カタログ更新コマンドは、ギャラリー、ギャラリーイメージ、およびイメージバージョンを作成します。マシンの電源を入れ直すと更新され、必要に応じてレプリカ数が更新されます。その時点から、既存のすべての非永続マシンはShared Image Galleryイメージを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはそのイメージを使用して作成されます。古いスナップショットは数時間以内に自動的にクリーンアップされます。

ユースケース: 共有イメージギャラリーカタログをスナップショットカタログに変換する

このユースケースの場合：

1. `UseSharedImageGallery` フラグを **False** に設定するか、未定義のままにして `Set-ProvScheme` を実行します。
2. カタログを更新します。
3. マシンをパワーサイクルして、強制的に更新します。

例：

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
```

ヒント：

スナップショットから共有イメージギャラリーカタログへの更新とは異なり、各マシンのカスタムデータは、新しいカスタムプロパティを反映するようにまだ更新されていません。元の共有イメージギャラリーのカスタムプロパティを表示するには、次のコマンドを実行します: `Get-ProvVm -ProvisioningSchemeName catalog-name`。`Set-ProvScheme` コマンドが完了しても、イメージスナップショットはまだ作成されていません。カタログがギャラリーを使用しないように構成されると、次回のカタログ更新操作で公開されたイメージがスナップショットとして保存されます。その時点から、既存のすべての非永続マシンはスナップショットを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはスナップショットから作成されます。マシンをパワーサイクルすると更新され、その時点でカスタムマシンデータは `UseSharedImageGallery` が **False** に設定されていることを反映するように更新されます。古い共有イメージギャラリーアセット（ギャラリー、イメージ、バージョン）は、数時間以内に自動的にクリーンアップされます。

指定された可用性ゾーンにマシンをプロビジョニングする

Azure環境では、特定の可用性ゾーンにマシンをプロビジョニングできます。これはPowerShellを使用して実現できます。

> **注：**
>
> ゾーンが指定されていない場合、MCSはAzureにそのリージョン内にマシンを配置させます。複数のゾーンが指定されている場合、MCSはそれらのゾーンにマシンをランダムに分散させます。

PowerShell を使用してアベイラビリティゾーンを構成する

PowerShell を使用して、`Get-Item` で提供されているインベントリアイテムを表示できます。たとえば、*米国東部リージョン* の `Standard_B1ls` サービス提供を表示するには：

```
$serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\Standard_B1ls.serviceoffering"
```

ゾーンを表示するには、アイテムの `AdditionalData` パラメーターを使用します。

`$serviceOffering.AdditionalData`

可用性ゾーンが指定されていない場合、マシンのプロビジョニング方法に変更はありません。

PowerShell を介して可用性ゾーンを構成するには、`New-ProvScheme` 操作で利用できる **Zones** カスタムプロパティを使用します。**Zones** プロパティは、マシンをプロビジョニングする可用性ゾーンのリストを定義します。これらのゾーンには、1つ以上の可用性ゾーンを含めることができます。たとえば、ゾーン1と3の場合は `<Property xsi:type="StringProperty" Name="Zones" Value="1, 3"/>`。

プロビジョニングスキームのゾーンを更新するには、`Set-ProvScheme`コマンドを使用します。

無効なゾーンが提供された場合、プロビジョニングスキームは更新されず、無効なコマンドを修正する方法に関する指示を提供するエラーメッセージが表示されます。

> **ヒント:**

> 無効なカスタムプロパティを指定すると、プロビジョニングスキームは更新されず、関連するエラーメッセージが表示されます。

ストレージの種類

MCS を使用する Azure 環境の仮想マシンには、異なるストレージの種類を選択します。ターゲット VM の場合、MCS は以下をサポートします。

- OS ディスク: プレミアム SSD、SSD、または HDD
- ライトバックキャッシュディスク: プレミアム SSD、SSD、または HDD

これらのストレージの種類を使用する場合、以下を考慮してください。

- VM が選択したストレージの種類をサポートしていることを確認してください。
- 構成で Azure エフェメラルディスクを使用している場合、ライトバックキャッシュディスク設定のオプションは表示されません。

> **ヒント:**
>
> `StorageType` はOSタイプとストレージアカウント用に構成されます。`WBCDiskStorageType` はライトバックキャッシュストレージタイプ用に構成されます。通常のカタログの場合、`StorageType` が必要です。`WBCDiskStorageType` が構成されていない場合、`StorageType` が `WBCDiskStorageType` のデフォルトとして使用されます。

> WBCDiskStorageType が構成されていない場合、StorageType が WBCDiskStorageType のデフォルトとして使用されます。

ストレージの種類を構成する

VM のストレージタイプを構成するには、`New-ProvScheme` の `StorageType` パラメータを使用します。`StorageType` パラメータの値を、サポートされているストレージタイプのいずれかに設定します。

プロビジョニングスキームにおける `CustomProperties` パラメータの設定例を次に示します。

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>'
```

ゾーン冗長ストレージを有効にする

カタログ作成時にゾーン冗長ストレージを選択できます。これは、Azure マネージドディスクを複数の可用性ゾーン間で同期的にレプリケートし、あるゾーンでの障害から他のゾーンの冗長性を利用して回復できるようにします。

ストレージタイプのカスタムプロパティで **Premium_ZRS** と **StandardSSD_ZRS** を指定できます。ZRS ストレージは、既存のカスタムプロパティを使用するか、**MachineProfile** テンプレートを介して設定できます。ZRS ストレージは、`-StartsNow` および `-DurationInMinutes -1` パラメータを持つ `Set-ProvVMUpdateTimeWindow` コマンドでもサポートされており、既存のマシンを LRS から ZRS ストレージに変更できます。

制限事項:

- マネージドディスクのみをサポート
- プレミアムおよび標準ソリッドステートドライブ (SSD) のみでサポート
- `StorageTypeAtShutdown` ではサポートされていません
- 特定のリージョンでのみ利用可能。
- 大規模に ZRS ディスクを作成すると、Azure のパフォーマンスが低下します。したがって、最初の電源投入時には、マシンをより小さなバッチ (一度に300台未満のマシン) で起動してください。

ゾーン冗長ストレージをディスクストレージタイプとして設定する

初期カタログ作成時にゾーン冗長ストレージを選択することも、既存のカタログでストレージタイプを更新することもできます。

POWERSHELLコマンドを使用してゾーン冗長ストレージを選択する

Azureで `New-ProvScheme` PowerShellコマンドを使用して新しいカタログを作成する場合、`StorageAccountType` の値として `Standard_ZRS` を使用します。 例:

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_ZRS" />
```

この値を設定すると、動的APIによって適切に使用できるかどうかが検証されます。ZRSの使用がカタログに対して有効でない場合、以下の例外が発生する可能性があります。

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: StorageTypeAtShutdownカスタムプロパティは、ZRSストレージでは使用できません。
- **StorageAccountTypeNotSupportedInRegion**: この例外は、ZRSをサポートしていないAzureリージョンでZRSストレージを使用しようとした場合に発生します。
- **ZrsRequiresManagedDisks**: ゾーン冗長ストレージは、マネージドディスクでのみ使用できます。

以下のカスタムプロパティを使用して、ディスクストレージタイプを設定できます。

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> **注:**
>
> カタログ作成時、カスタムプロパティが設定されていない場合は、マシンプロファイルのOSディスク`StorageType`が使用されます。

マシンプロファイルからVMとNICの診断設定をキャプチャする

マシンカタログの作成時、既存のマシンカタログの更新時、および既存のVMの更新時に、マシンプロファイルからVMとNICの診断設定をキャプチャできます。

VMまたはテンプレート仕様をマシンプロファイルのソースとして作成できます。

主な手順

1. Azureで必要なIDを設定します。これらのIDはテンプレート仕様で指定する必要があります。
    - ストレージアカウント
    - Log Analyticsワークスペース
    - 標準ティアの価格設定のEvent Hub名前空間

2. マシンプロファイルのソースを作成します。
3. 新しいマシンカタログを作成するか、既存のカタログを更新するか、既存のVMを更新します。

Azureで必要なIDを設定する

Azureで次のいずれかを設定します。

- ストレージアカウント
- ログ分析ワークスペース
- Standardティアの価格設定を持つイベントハブ名前空間

ストレージアカウントを設定する

Azureで標準ストレージアカウントを作成します。テンプレート仕様では、ストレージアカウントの完全なresourceIdを`storageAccountId`として指定します。

VMがストレージアカウントにデータをログ記録するように設定されると、データは`insights-metrics-pt1m`コンテナの下で見つけることができます。

ログ分析ワークスペースを設定する

ログ分析ワークスペースを作成します。テンプレート仕様では、ログ分析ワークスペースの完全なresourceIdをworkspaceIdとして指定します。

VMがワークスペースにデータをログするように設定されると、Azureのログの下でデータをクエリできます。Azureのログの下で次のコマンドを実行して、リソースによってログに記録されたすべてのメトリックの数を表示できます。

```
AzureMetrics | summarize Count=count() by ResourceId
```

イベントハブを設定する

Azureポータルでイベントハブを設定するには、次の手順を実行します。

1. 標準ティアの価格設定でイベントハブ名前空間を作成します。
2. 名前空間の下にイベントハブを作成します。
3. イベントハブの下にある**キャプチャ**に移動します。Avro出力タイプでキャプチャするトグルをオンにします。
4. ログをキャプチャするために、既存のストレージアカウントに新しいコンテナを作成します。
5. テンプレートスペックで、次の形式で`eventHubAuthorizationRuleId`を指定します: `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/`

`providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`

6. イベントハブの名前を指定します。

VMがイベントハブにデータをログするように設定されると、データは構成されたストレージコンテナにキャプチャされます。

マシンプロファイルソースを作成する

VMまたはテンプレートスペックをマシンプロファイルソースとして作成できます。

診断設定を含むVMベースのマシンプロファイルの作成

VMをマシンプロファイルとして作成する場合は、まずテンプレートVM自体に診断設定をセットアップします。詳細な手順については、Microsoftドキュメントの「Azure Monitorの診断設定」を参照してください。

VMまたはNICに関連付けられた診断設定が現在存在することを確認するには、次のコマンドを実行できます。

```
az monitor diagnostic-settings list --resource-group matspo --resource matspo-tog-cc2659 --resource-type microsoft.network/networkInterfaces
```

```
az monitor diagnostic-settings list --resource-group matspo --resource matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
```

診断設定を含むテンプレート仕様ベースのマシンプロファイルの作成

診断設定がすでに有効になっているVMを使用し、それをARMテンプレートスペックにエクスポートする場合、これらの設定はテンプレートに自動的に含まれません。ARMテンプレート内で診断設定を手動で追加または変更する必要があります。

ただし、VMをマシンプロファイルとして使用する場合、MCSは、重要な診断設定が正確にキャプチャされ、MCSカタログ内のリソースに適用されることを保証します。

1. VMとNICを定義する標準テンプレート仕様を作成します。
2. 仕様に従って診断設定を展開するための追加リソースを追加します: Microsoft.Insights diagnosticSettings。スコープについては、テンプレート内のVMまたはNICを部分的なIDで名前によって参照します。たとえば、テンプレート仕様でtest-VMという名前のVMにアタッチされた診断設定を作成する場合、スコープは次のように指定します。

```
"scope": "microsoft.compute/virtualMachines/test-VM",
```

3. テンプレートスペックをマシンプロファイルソースとして使用します。

診断設定を含むカタログの作成または更新

マシンプロファイルソースを作成した後、`New-ProvScheme` コマンドを使用してマシンカタログを作成し、`Set-ProvScheme` コマンドを使用して既存のマシンカタログを更新し、`Request-ProvVMUpdate` コマンドを使用して既存のVMを更新できます。

ページファイルの場所の決定

ページファイルの場所は、次のシナリオに従って決定されます。

注:

デフォルトのページファイル保存場所はOSディスクです。

シナリオ	場所
ページファイルの設定がカスタムプロパティで指定されている	カスタムプロパティで指定されているとおり
エフェメラルOSディスクまたは休止状態が有効になっている	OSディスク
VMに一時ディスクがある	一時ディスク
MCS I/O が有効になっています	WBCディスク

ページファイル設定のシナリオ

次の表は、イメージ準備中およびプロビジョニングスキームの更新中に考えられるページファイル設定のシナリオの一部を示しています。

期間	シナリオ	結果
イメージの準備	ソースイメージのページファイルを一時ディスクに設定しますが、プロビジョニングス	ページファイルはOSに配置されます

期間	シナリオ	結果
	キームで指定したVMサイズには一時ディスクがありません	
イメージの準備	ソースイメージのページファイルをOSディスクに設定しますが、プロビジョニングスキームで指定したVMサイズには一時ディスクがあります	ページファイルは一時ディスクに配置されます
イメージの準備	ソースイメージのページファイルを一時ディスクに設定し、プロビジョニングスキームでエフェメラルOSディスクを有効にします	ページファイルはOSディスクに配置されます
プロビジョニングスキームの更新	VDAバージョンが2311より前の場合に、プロビジョニングスキームの更新を試みます	警告付きでページファイル設定を変更します
プロビジョニングスキームの更新	VDAバージョンが2311以降の場合に、プロビジョニングスキームの更新を試みます	ページファイルの位置の決定に従ってページファイルの場所を決定します

ページファイル設定の指定

PowerShellコマンドを使用して、場所やサイズを含むページファイル設定を指定できます。これにより、MCSによって決定されたページファイル設定が、ページファイルの位置の決定に従って上書きされます。これは、マシンカタログ作成中に次の`New-ProvScheme`コマンドを実行することで行えます。

重要な考慮事項

カタログ作成を進める前に、以下を考慮してください。

- すべてのカスタムプロパティ（'PageFileDiskDriveLetterOverride'、'InitialPageFileSizeInMB'、および'MaxPageFileSizeInMB'）を`New-ProvScheme`コマンドで指定するか、または何も指定しないかのいずれかである必要があります。
- この機能はCitrix Studioではサポートされていません。
- 初期ページファイルサイズは16 MBから16777216 MBの間である必要があります。

- 最大ページファイルサイズは、初期ページファイルサイズ以上で、かつ16777216 MB未満である必要があります。
- 初期ページファイルサイズと最大ページファイルサイズの両方を同時にゼロに設定できます。

注:

マスターイメージを更新することなく、既存のカタログに新しく追加されたVMのページファイル設定を変更できます。ページファイル設定を変更するには、VDAバージョン2311以降が必要です。PowerShellコマンドを使用してページファイル設定を変更できます。詳細については、「ページファイル設定の変更」を参照してください。

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "zijinnet" `

-IdentityPoolName "PageFileSettingExample" `

-ProvisioningSchemeName "PageFileSettingExample" `

-InitialBatchSizeHint 1 `

-MasterImageVM "XDHyp:\HostingUnits\zijinnet\image.folder\neal-zijincloud-
resources.resourcegroup\CustomWin10VDA_OsDisk_1_9473d7c8a6174b2c8284c7d3ef
eea88f.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\zijinnet\
\virtualprivatecloud.folder\\East US.region\\virtualprivatecloud.folder\
\neal-zijincloud-resources.resourcegroup\\neal-zijincloud-resources-
vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\zijinnet\\serviceoffering.folder\
\Standard_B2ms.serviceoffering" `

-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
```

```
<Property xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride"
Value="d"/> `

<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
Value="2048"/> `

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB"
Value="8196"/> `

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `

</CustomProperties>'
```

ページファイル設定の変更

マスターイメージを更新することなく、既存のカタログに新しく追加されたVMのページファイル設定を変更できます。現在、この機能はAzure環境のみに適用されます。

ページファイル設定を変更するには、VDAバージョン2311以降が必要です。PowerShellコマンドを使用してページファイル設定を変更できます。

Azure環境で変更できるページファイル設定は次のとおりです。

- `PageFileDiskDriveLetterOverride`
- `InitialPageFileSizeInMB`
- `MaxPageFileSizeInMB`

既存のカタログのページファイル設定を変更する

既存のマシンカタログのページファイル設定を変更するには、`Set-ProvScheme` コマンドを実行します。この場合、更新はカタログに追加された新しいVMにのみ適用されます。例：

```
Set-ProvScheme -ProvisioningSchemeName $schemeName -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
```

```
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="StandardSSD_LRS" />

<Property xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride"
Value="D" />

<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
Value="2048" />

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB"
Value="8196" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property  xsi:type="StringProperty" Name="Zones" Value="1" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="neal-
test-group1" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

注:

ライトバックキャッシュを有効にして、PowerShell コマンドを使用して `PageFileDiskDriveLetterOverride` を `C:` に設定しようとすると、MCS IO ドライバーはページファイルを自動的に正しいディスクドライブにリダイレクトし、`C:` にはリダイレクトしません。

Azure Spot VMを使用してカタログを作成する

Azure Spot VMを使用すると、Azureの未使用のコンピューティング能力を大幅なコスト削減で活用できます。ただし、Azure Spot VMを割り当てる能力は、現在の容量と価格設定に依存します。そのため、Azureは実行中のVMを強制終了したり、VMの作成に失敗したり、強制排除ポリシーに従ってVMの電源をオンにできなかったりする可能性があります。したがって、Azure Spot VM

は、一部の重要でないアプリケーションやデスクトップに適しています。詳細については、Azure Spot Virtual Machinesの使用を参照してください。

制限事項

- すべてのVMサイズがAzure Spot VMでサポートされているわけではありません。詳細については、制限事項を参照してください。

  VMサイズがSpot VMをサポートしているかどうかを確認するには、次のPowerShellコマンドを実行します。VMサイズがSpot VMをサポートしている場合、`SupportsSpotVM`は**True**になります。

  ```
  (Get-Item "XDHyp:\HostingUnits\azure-res-
  conn2\serviceoffering.folder\Standard_D2ds_v4.serviceoffering").
  AdditionalData
  ```

- 現在、Azure Spot VMは休止状態をサポートしていません。

要件

Azure Spot VMカタログのマシンプロファイルソース（VMまたはテンプレート仕様）を作成する際、(VMを使用している場合は) Azure Spot Instanceを選択するか、(テンプレート仕様を使用している場合は) `priority`を`Spot`として設定する必要があります。

Azure Spot VMを使用してカタログを作成する手順

1. マシンプロファイルソース（VMまたは起動テンプレート）を作成します。

   - Azureポータルを使用してVMを作成する方法については、Azureポータルを使用してAzure Spot Virtual Machinesを展開するを参照してください。
   - テンプレート仕様を作成するには、テンプレート仕様の**resources > type: Microsoft.Compute/virtualMachines > properties**の下に次のプロパティを追加します。例：

     ```
     "priority": "Spot",

     "evictionPolicy": "Deallocate",

     "billingProfile": {

     "maxPrice": 0.01
     ```

```
}
```

注:

- 強制排除ポリシーは**Deallocate**または**Delete**に設定できます。
  - 非永続VMの場合、MCSは常に強制排除ポリシーを**Delete**に設定します。VMが強制排除されると、非永続ディスク（例：OSディスク）とともに削除されます。永続ディスク（例：IDディスク）は削除されません。ただし、カタログタイプが永続であるか、`PersistOsDisk`カスタムプロパティがTrueに設定されている場合、OSディスクは永続的です。同様に、`PersistWbc`カスタムプロパティが**True**に設定されている場合、WBCディスクは永続的です。
  - 永続VMの場合、MCSは常に強制排除ポリシーをDeallocateに設定します。VMが強制排除されると、割り当て解除されます。ディスクに変更は加えられません。
- 最大価格は、1時間あたりに支払う意思のある価格です。**Capacity Only**を使用している場合、これは**-1**です。最大価格は、null、-1、またはゼロより大きい小数である必要があります。詳細については、価格を参照してください。

2. マシンプロファイルがAzure Spot VM対応であるかどうかを確認するには、次のPowerShellコマンドを実行します。`SpotEnabled`パラメーターが**True**で、`SpotEvictionPolicy`が**Deallocate**または**Delete**に設定されている場合、マシンプロファイルはAzure Spot VM対応です。例：

   - マシンプロファイルソースがVMの場合、次のコマンドを実行します。

     ```
     (Get-Item "XDHyp:\HostingUnits\azure-res-
     conn2\machineprofile.folder\fifthcolumn.resourcegroup\kb-spot-
     delete.vm"). AdditionalData
     ```

   - マシンプロファイルソースがテンプレート仕様の場合、次のコマンドを実行します。

     ```
     (Get-Item "XDHyp:\HostingUnits\azure-res-
     conn2\machineprofile.folder\fifthcolumn.resourcegroup\fc-aeh-
     ```

```
templatespec.templatespec\14.0.0-spot-
delete.templatespecversion").AdditionalData
```

3. `New-ProvScheme` PowerShellコマンドを使用して、マシンプロファイルでマシンカタログを作成します。

`Set-ProvScheme`コマンドを使用してカタログを更新できます。また、PowerShellコマンド`Set-ProvVmUpdateTimeWindow`を使用して既存のVMを更新することもできます。マシンプロファイルは次回の電源投入時に更新されます。

実行中のAzure Spot VMでの強制排除

コンピューティング容量が利用できない場合、または時間あたりの価格が設定された最大価格よりも高い場合、Azureは実行中のSpot VMを強制排除します。デフォルトでは、強制排除の通知はされません。VMは単にフリーズし、強制排除されます。Microsoftは、強制排除を監視するためにScheduled Eventsを使用することを推奨しています。強制排除を継続的に監視するを参照してください。VM内からスクリプトを実行して、強制排除前に通知を受け取ることもできます。たとえば、MicrosoftはPythonでポーリングスクリプトScheduledEvents.csを提供しています。

トラブルシューティング

- プロビジョニングされたVMのcustomMachineDataで、`Get-ProvVM`コマンドを使用してSpot VMのプロパティを確認できます。優先度フィールドが**Spot**に設定されている場合、Spotが使用されています。
- Azure PortalでVMがSpotを使用しているかどうかを確認できます。

  a. Azure PortalでVMを見つけます。

  b. **概要**ページに移動します。

  c. 下にスクロールして、**Azure Spot**セクションを見つけます。

    - Spotが使用されていない場合、このフィールドは空です。
    - Spotが使用されている場合、**Azure Spot**および**Azure Spot eviction policy**フィールドが設定されます。

1. 構成ページで、VMの課金プロファイルまたは1時間あたりの最大価格を確認できます。

バックアップVMサイズの構成

パブリッククラウドでは、特定のVMサイズで容量が不足する場合があります。また、Azure Spot VMを使用している場合、Azureの容量要件に基づいてVMはいつでも強制終了されます。Azureの容量不足またはSpot VMの電源投入失敗の場合、MCSはバックアップVMサイズにフォールバック

します。MCSマシンカタログの作成または更新時に、カスタムプロパティ `BackupVmConfiguration` を使用してバックアップVMサイズのリストを提供できます。MCSは、リストで指定された順序でバックアップVMサイズにフォールバックしようとします。

MCSがVMに特定のバックアップ構成を使用する場合、次のシャットダウンまでその構成を使い続けます。次回の電源投入時には、MCSはプライマリVM構成を起動しようとします。失敗した場合、MCSはリストに従ってバックアップVMサイズ構成を再度起動しようとします。

この機能は、以下でサポートされています。

- マシンプロファイルを使用するカタログ
- 永続および非永続MCSマシンカタログ
- 現在のAzure環境

重要な考慮事項

- リストには複数のバックアップVMサイズを指定できます。
- リストは一意である必要があります。
- リスト内の各VMにインスタンスタイププロパティを追加できます。タイプは**Spot**または**Regular**のいずれかです。タイプが指定されていない場合、MCSはVMを**Regular**と見なします。
- 既存のカタログのバックアップVMサイズリストは、`Set-ProvScheme` PowerShellコマンドを使用して変更できます。
- カタログに関連付けられたプロビジョニングスキームから作成された既存のVMは、`Set-ProvVMUpdateTimeWindow` コマンドを使用して更新できます。
- 選択した数の既存のMCS VMのバックアップVMサイズリストは、`Set-ProvVM` コマンドを使用して構成できます。ただし、更新を適用するには、`Set-ProvVMUpdateTimeWindow` を使用してVMの更新時間枠を設定し、その時間枠内でVMを起動します。VMで `Set-ProvVm` コマンドが使用された場合、プロビジョニングスキームのリストが後で更新されても、VMはその特定のVMに設定されたバックアップVMサイズリストを引き続き使用します。VMにプロビジョニングスキームのバックアップリストを使用させるには、`-RevertToProvSchemeConfiguration` とともに `Set-ProvVM` を使用できます。

バックアップVMサイズでカタログを作成する

> **注:**

> Studio UIがフリーズする問題に対処するには、PowerShellコマンドの実行中にすべてのシングルクォートを`"` に置き換えてください。

1. **PowerShell**ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。
3. Broker カタログを作成します。このカタログには、これから作成されるマシンが投入されます。
4. ID プールを作成します。これは、作成されるマシン用に作成された AD アカウントのコンテナになります。
5. マシンプロファイルを使用してプロビジョニングスキームを作成します。「バックアップ構成を構成する方法」を参照してください。
6. プロビジョニングスキームの一意のIDでBrokerCatalogを更新します。
7. VMを作成してカタログに追加します。

既存のカタログを更新する

`Set-ProvScheme` コマンドを使用してプロビジョニングスキームを更新できます。「バックアップ構成を構成する方法」を参照してください。

既存のVMを更新する

`Set-ProvVMUpdateTimeWindow` PowerShell コマンドを使用して、カタログ内の既存の VM を更新できます。このコマンドは、指定された時間枠内で次回の電源投入時に、カタログに関連付けられたプロビジョニングスキームから作成された VM を更新します。例:

- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartTimeInUTC "3/12/2022 3am" -DurationInMinutes 60`
- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartsNow -DurationInMinutes 60`

> **注:**
>
> `StartsNow`はスケジュールされた開始時間を示します。`DurationInMinutes`はスケジュールの時間枠です。

`Set-ProvVM`コマンドを使用して、選択した既存のMCS VMのバックアップVMサイズリストを構成できます。ただし、更新を適用するには、`Set-ProvVMUpdateTimeWindow`を使用してVMの更新時間枠を設定し、その時間枠内でVMを起動します。例：

1. 選択した既存のMCS VMのバックアップVMサイズリストを構成するには、`Set-ProvVM`コマンドを実行します。例：

```
Set-ProvVM -ProvisioningSchemeName "name" -VMName "Vm-001"

-CustomProperties

"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Server`"/>

<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
Value=`"true`"/>

<Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration`"
Value=`"[{&quot;ServiceOffering&quot;: &quot;Standard_D2as_v4&quot;,
&quot;Type&quot;: &quot;Spot&quot;}, {&quot;ServiceOffering&quot;:
&quot;Standard_D2s_v3&quot;, &quot;Type&quot;: &quot;Regular&quot;},
{&quot;ServiceOffering&quot;: &quot;Standard_D2s_v3&quot;,
&quot;Type&quot;: &quot;Spot&quot;}]`"/>

</CustomProperties>"
```

2. 更新を適用するには`Set-ProvVMUpdateTimeWindow`コマンドを実行します。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartsNow -DurationInMinutes 60
```

すべてのリソースにタグをコピーする

マシンプロファイルで指定されたタグを、新しいVMまたはマシンカタログ内の既存のVMのすべてのリソース（複数のNICやディスク（OSディスク、IDディスク、ライトバックキャッシュディスクなど））にコピーできます。マシンプロファイルのソースは、VMまたはARMテンプレート仕様にすることができます。

> **注:**
>
> リソースにタグを保持するには、タグにポリシーを追加するか（タグコンプライアンスのポリシー定義を割り当てるを参照）、マシンプロファイルソースにタグを追加する必要があります。

前提条件

VMのVM、ディスク、およびNICにタグを付けるには、マシンプロファイルソース（VMまたはARMテンプレート仕様）を作成します。

- VMをマシンプロファイルの入力として使用したい場合は、AzureポータルでVMとすべてのリソースにタグを適用します。Azureポータルでタグを適用するを参照してください。
- ARMテンプレート仕様をマシンプロファイルの入力として使用したい場合は、各リソースの下に次のタグブロックを追加します。

```
 "tags": {

"TagC": "Value3"

},
```

> **注:**
>
> テンプレート仕様には、最大1つのディスクと少なくとも1つのNICを含めることができます。

新しいマシンカタログ内のVMのリソースにタグをコピーする

1. VMまたはARMテンプレート仕様をマシンプロファイルの入力として使用して、非永続または永続カタログを作成します。

2. カタログにVMを追加して電源をオンにします。マシンプロファイルで指定されたタグが、そのVMの対応するリソースにコピーされていることを確認する必要があります。

> **注:**
>
> マシンプロファイルで指定されたNICの数と、VMで使用するNICの数に不一致がある場合、エラーが発生します。

既存のVMのリソース上のタグを変更する

1. すべてのリソースにタグを付けたマシンプロファイルを作成します。
2. 既存のマシンカタログを、更新されたマシンプロファイルで更新します。例：

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName>
-MachineProfile <PathToYourMachineProfile>
```

3. 更新を適用したいVMの電源をオフにします。
4. VMのスケジュールされたアップデートを要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <YourCatalogName>  -
VMName machine1 -StartsNow -DurationInMinutes -1
```

5. VMの電源をオンにします。
6. マシンプロファイルで指定されたタグが、対応するリソースにコピーされていることを確認する必要があります。

> **注:**
>
> マシンプロファイルで指定されたNICの数と、`Set-ProvScheme`で指定されたNICの数に不一致がある場合、エラーが発生します。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。

- 構成プロセス全体を確認するには、「」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure.html)を参照してください。
- カタログを管理するには、「」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-manage.html)および「」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-manage/manage-machine-catalog-azure.html)を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マイクロソフト Azure リソース マネージャーへの接続
- マシンカタログの作成

Microsoft System Center Virtual Machine Managerカタログを作成する

マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html)では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Microsoft System Center Virtual Machine Manager (VMM) 仮想化環境に固有の詳細を扱います。

> **注:**
>
> VMMカタログを作成する前に、VMMへの接続の作成を完了する必要があります。「Microsoft System Center Virtual Machine Managerへの接続(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections/connection-mscvmm.html)」を参照してください。

マスターVMを作成する

1. マスターVMにVDAをインストールし、パフォーマンスを向上させるためにデスクトップを最適化するオプションを選択します。
2. バックアップとして使用するために、マスターVMのスナップショットを作成します。
3. 仮想デスクトップを作成します。

SMB 3ファイル共有上のMCS

VMストレージ用のSMB 3ファイル共有上にMCSで作成されたマシンカタログの場合、資格情報が以下の要件を満たしていることを確認してください。これらの要件により、Controllerの

Hypervisor Communications Library (HCL) からの呼び出しがSMBストレージに正常に接続されることが保証されます。

- VMMユーザー資格情報には、SMBストレージへの完全な読み取り/書き込みアクセスが含まれている必要があります。
- VMライフサイクルイベント中のストレージ仮想ディスク操作は、VMMユーザー資格情報を使用してHyper-Vサーバー経由で実行されます。

SMBストレージを使用する場合は、Controllerから個々のHyper-Vマシンへの認証資格情報セキュリティサポートプロバイダー（CredSSP）を有効にします。このプロセスは、Windows Server 2012上のHyper-VとVMM 2012 SP1で使用します。詳細については、CTX137465を参照してください。

HCLは`CredSSP`を使用してHyper-Vマシンへの接続を開きます。この機能は、Kerberosで暗号化されたユーザー資格情報をHyper-Vマシンに渡します。リモートHyper-Vマシン上のセッションで**PowerShell**コマンドは、提供された資格情報で実行されます。この場合、VMMユーザーの資格情報が使用されるため、ストレージへの通信コマンドが正しく機能します。

次のタスクでは、HCLで生成され、SMB 3.0ストレージに対して動作するためにHyper-Vマシンに送信されるPowerShellスクリプトを使用します。

- **マスターイメージの統合**: マスターイメージは、MCSプロビジョニングスキーム（マシンカタログ）を作成します。マスターVMをクローンしてフラット化し、新しく作成されたディスクからVMを作成できるようにします（元のマスターVMへの依存関係を削除します）。

  root\\virtualization\\v2名前空間でのConvertVirtualHardDisk

  例:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)

$result
```

- **差分ディスクの作成:** マスターイメージを統合して生成されたマスターイメージから差分ディスクを作成します。その後、差分ディスクは新しいVMに接続されます。

  root\\virtualization\\v2名前空間でのCreateVirtualHardDisk

  例:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.CreateVirtualHardDisk($vhdastext);

$result
```

- **IDディスクのアップロード**：HCLはIDディスクをSMBストレージに直接アップロードできません。そのため、Hyper-VマシンがIDディスクをストレージにアップロードしてコピーする必要があります。Hyper-Vマシンはコントローラーからディスクを読み取ることができないため、HCLはまずHyper-Vマシンを介してIDディスクを次のようにコピーする必要があります。

  a. HCLは、管理者共有を介してIDをHyper-Vマシンにアップロードします。

  b. Hyper-Vマシンは、PowerShellリモートセッションで実行されているPowerShellスクリプトを介して、ディスクをSMBストレージにコピーします。Hyper-Vマシン上にフォルダーが作成され、そのフォルダーのアクセス許可はVMMユーザーのみにロックされます（リモートPowerShell接続を介して）。

  c. HCLは、管理者共有からファイルを削除します。

  d. HCLがIDディスクのHyper-Vマシンへのアップロードを完了すると、リモートPowerShellセッションはIDディスクをSMBストレージにコピーします。その後、Hyper-Vマシンから削除します。

  IDディスクフォルダーは、削除された場合でも再利用できるように再作成されます。

- **IDディスクのダウンロード:** アップロードと同様に、IDディスクはHyper-Vマシンを経由してHCLに渡されます。次のプロセスでは、Hyper-Vサーバー上にVMMユーザー権限のみを持つフォルダーが存在しない場合に作成します。

  a. Hyper-Vマシンは、PowerShellスクリプトを介してディスクをSMBストレージからローカルのHyper-Vストレージにコピーします。このスクリプトはPowerShell V3リモートセッションで実行されます。

  b. HCLは、Hyper-Vマシンの管理者共有からディスクをメモリに読み込みます。

  c. HCL は管理者共有からファイルを削除します。

マシンプロファイルを使用してカタログを作成する

System Center Virtual Machine Manager (SCVMM) 環境では、マシンプロファイルを使用して MCS マシンカタログを作成および更新できます。vTPM を有効にできます。また、マシンプロファイル VM のカスタムタグをプロビジョニングされた VM に追加することもできます。

重要な考慮事項

- マスターイメージはスナップショットのみであり、VM ではありません。
- マシンプロファイルのソースとして使用できるのは VM のみです。
- VTPM は Hyper-V コンソールから構成でき、SCVMM コンソールからは構成できません。
- マスターイメージで vTPM が有効になっている場合、マシンプロファイルソースで vTPM を有効にする必要があります。
- vTPM は第 2 世代のマシンでのみサポートされています。
- 次のパラメーターは、個別に指定された場合、マシンプロファイルでキャプチャされた値を上書きします。
  - VMCpuCount
  - VMMemoryMB
  - ディスクストレージ
- カスタムタグは、マスターイメージからではなく、マシンプロファイルからのみ継承されます。`CitrixProvisioningSchemeId` タグはデフォルトで VM に追加されます。`CitrixProvisioningSchemeId` タグを含めたくない場合は、ホスティングユニットの作成時に `-NoVmTagging` パラメーターを追加します。例:

```
New-Item -HypervisorConnectionName  $ConnectionName `

    -NetworkPath @($NetworkPath) `

    -Path @($HostingUnitPath) `

    -PersonalvDiskStoragePath @() `

    -RootPath $RootPath `

    -StoragePath @($StoragePath) `

    -NoVmTagging

    ```
```

- 既存のカタログは、`Set-ProvScheme`コマンドを使用して更新できます。
```

マシンプロファイルを使用してマシンカタログを作成する

1. マシンプロファイルのソースとなるVMを作成します。詳しくは、「VMMファブリックでの仮想マシンのプロビジョニング」を参照してください。**世代**は一度選択すると変更できません。SCVMMでは、次のことができます。
   - vTPMを有効にするには：
     a. VMを作成したら、Hyper-Vホストにログオンし、**Hyper-Vマネージャー**でVMを見つけます。
     b. VMを右クリックし、**設定**に移動します。
     c. **セキュリティ**で、**トラステッドプラットフォームモジュールを有効にする**チェックボックスをオンにします。
2. **PowerShell**ウィンドウを開きます。
3. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
4. Brokerカタログを作成します。このカタログには、これから作成されるマシンが格納されます。
5. IDプールを作成します。これは、作成されるマシン用に作成されたADアカウントのコンテナになります。
6. マシンプロファイルを使用してプロビジョニングスキームを作成します。例：

```
New-ProvScheme -HostingUnitName "<hostingunit name>"

-IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1\<path
to the checkpoint/snapshot>"

-ProvisioningSchemeName "<catalogname>"  -MachineProfile "XDHyp:\<path
to the machine profile VM>"
```

7. プロビジョニングスキームの一意のIDでBrokerカタログを更新します。
8. VMを作成してカタログに追加します。

既存のカタログを更新する

Set-ProvSchemeコマンドを使用して、既存のカタログを更新できます。例：

```
Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile
"XDHyp:\<path to the machine profile VM>"
```

VMを削除する

カタログからVMを削除することはできますが、SCVMMからVMを削除しないことも選択できます。この場合、`CitrixProvisioningSchemeId`タグはVMからのみ削除されます。カスタムタグはVMから削除されません。Web StudioまたはPowerShellコマンドを使用してVMを削除できます。

WEB STUDIO を使用して VM を削除する

1. VMを選択して右クリックします。
2. **削除**」をクリックします。
3. **仮想マシンをカタログから削除しますが、仮想マシンは削除しません**を選択します。

POWERSHELLコマンドの使用

`Remove-ProvVM`と`ForgetVM`パラメーターを使用します。詳細については、以下を参照してください。

- タグを削除する
- ハイパーバイザーアクセスなしでマシンを削除する

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループを作成するようにガイドします。
- 構成プロセス全体を確認するには、インストールと構成を参照してください。
- カタログを管理するには、マシンカタログを管理するおよびMicrosoft System Center Virtual Machine Managerカタログを管理するを参照してください。

詳細情報

- 接続とリソースを作成および管理する(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections.html)
- マイクロソフト システムセンター バーチャルマシンマネージャーへの接続
- マシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html)

Nutanixカタログを作成する

「(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html)」では、マシンカタログを作成するウィザードについて説明します。以下の情報では、Nutanix仮想化環境に固有の詳細について説明します。

注:

Nutanixカタログを作成する前に、Nutanixへの接続の作成を完了する必要があります。「(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections/connection-nutanix.html)」を参照してください。

Nutanixスナップショットを使用してマシンカタログを作成する

選択したスナップショットは、カタログ内のVMを作成するために使用されるテンプレートです。カタログを作成する前に、Nutanixでイメージとスナップショットを作成してください。詳細については、Nutanixのドキュメントを参照してください。

カタログ作成ウィザードで：

- 「**オペレーティングシステム**」ページと「**マシン管理**」ページには、Nutanix固有の情報は含まれていません。
- **Container**または**Cluster and Container**ページはNutanix固有のものです。

  Nutanix AHV XIをリソースとして使用してマシンを展開する場合、「**コンテナ**」ページが表示されます。VMのIDディスクが配置されるコンテナを選択します。

  Nutanix AHV Prism Central (PC)をリソースとして使用してマシンを展開する場合、「**クラスターとコンテナ**」ページが表示されます。VMの展開に使用するクラスターを選択し、次にコンテナを選択します。
- 「**イメージ**」ページで、イメージスナップショットを選択します。Citrix Virtual Apps and Desktopsで使用するには、Acropolisスナップショット名に「XD_」のプレフィックスを付ける必要があります。必要に応じて、Acropolisコンソールを使用してスナップショットの名前を変更してください。スナップショットの名前を変更した場合は、カタログ作成ウィザードを再起動して、更新されたリストを表示してください。
- **Virtual Machines**ページで、仮想CPUの数とvCPUあたりのコア数を指定します。
- **ネットワークカード**ページで、関連するネットワークをフィルタリングするNICタイプを選択します。NICタイプには、**VLAN**と**OVERLAY**の2種類があります。マスターイメージに含まれるNICを1つ以上選択し、次に各NICに関連付けられた仮想ネットワークを選択します。
- **Machine Identities**、**Domain Credentials**、**Scopes**、および**Summary**ページには、Nutanix固有の情報は含まれていません。

制限事項

Nutanixホスト接続（特にNutanix AHVプラグイン2.7.1）でMCSカタログを作成する場合、プロビジョニングされたVMのハードディスクサイズがWeb Studioで誤って表示されます。表示されるサイズは、実際のストレージサイズ（50 GB）よりもはるかに小さく（1 GB）なります。ハードディスクサイズはNutanixコンソールでは正しく表示されます。

次のステップ

- これが最初に作成するカタログである場合、Web Studioはデリバリーグループの作成を案内します
- 構成プロセス全体を確認するには、インストールと構成を参照してください
- カタログを管理するには、マシンカタログの管理を参照してください

詳細情報

- 接続とリソースの作成および管理
- Nutanixへの接続
- Nutanixクラウドおよびパートナーソリューションへの接続
- マシンカタログの作成

VMwareカタログを作成する

「(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html)」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、VMware仮想化環境に固有の詳細を扱っています。

> **注:**
>
> VMwareカタログを作成する前に、VMwareへの接続の作成を完了する必要があります。「(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections/connection-vmware-virtualization-environments.html)」を参照してください。

マスターVMを作成する

マスターVMを使用して、マシンカタログでユーザーデスクトップとアプリケーションを提供します。ハイパーバイザーで：

1. マスターVMにVDAをインストールし、パフォーマンスを向上させるデスクトップ最適化オプションを選択します。
2. マスターVMのスナップショットを取得し、バックアップとして使用します。

> **注:**
>
> MCSを使用して、vSAN 8.0環境でVMをプロビジョニングできます。

マシンプロファイルを使用してマシンカタログを作成する

マシンプロファイルを使用してMCSマシンカタログを作成できます。マシンプロファイルの入力元はVMwareテンプレートです。マシンプロファイルは、VMwareテンプレートからハードウェアプロパティを取得し、カタログ内の新しくプロビジョニングされたVMに適用します。

> **注:**
>
> - マスターイメージ入力（スナップショット）とマシンプロファイル入力（VMwareテンプレート）は、両方ともvTPMが有効であるか、両方ともvTPMが無効である必要があります。このルールは`New-ProvScheme`と`Set-ProvScheme`の両方に適用されます。
> - マスターイメージでvTPMが有効になっている場合、VMwareテンプレートはマスターイメージと同じVMソースからのみ取得できます。
> - 暗号化ストレージポリシーはフルクローンのみをサポートします。
> - マシンプロファイルベースのカタログは、提供されたVMwareテンプレートを利用して、接続された仮想ディスクに依存するストレージコントローラー情報を収集します。テンプレートには、仮想マシンの仮想ディスクを構成するために使用されるストレージコントローラー情報を取得するために必要な仮想ディスクを含める必要があります。

> マシンプロファイル内のVMwareテンプレートは、カタログへのVMのプロビジョニングを可能にするために、カタログのライフサイクル中に存在する必要があります。VMwareテンプレートがない場合、新しいVMをプロビジョニングすることはできません。VMwareテンプレートが削除された場合、`Set-ProvScheme`コマンドを使用して新しいテンプレートを提供する必要があります。

- MCSはVMwareテンプレートのプロパティをキャプチャします。Get-Provschemeコマンドを使用して、VMwareテンプレートの保存されたプロパティを参照する新しいVMwareテンプレートを作成できます。
- あるいは、マシンカタログとプロビジョニングされたVMが存在する場合、MCSでプロビジョニングされたマシンを使用して新しいVMwareテンプレートを作成することもできます。

異なるOSに基づいて、異なる構成でマシンカタログを作成できます。

- マスターイメージにWindows 11がインストールされている場合、マスターイメージでvTPMを有効にすることが要件となります。したがって、マシンプロファイルのソースであるVMwareテンプレートには、vTPMがアタッチされている必要があります。
- マスターイメージにvTPMがアタッチされていないWindows 10がインストールされている場合、非vTPM VMwareテンプレートをマシンプロファイルのソースとして使用してマシンカタログを作成できます。

暗号化されたストレージポリシーが適用されたマシンプロファイルテンプレートを使用して、フルコピーディスクモードでマシンカタログを作成できる別の構成があります。

マシンプロファイルを入力としてPowerShellコマンドを使用してマシンカタログを作成するには：

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. 次のコマンドを実行します。

    - vTPMがアタッチされたVMwareテンプレートをマシンプロファイル入力のソースとして、Windows 11がインストールされたマスターイメージでマシンカタログを作成するには：

    ```
    $identityPool = New-AcctIdentityPool  -IdentityPoolName "<string>"

    -NamingScheme "<string>-###"

    -NamingSchemeType Numeric

    -Domain "<domain name"

    -ZoneUid "<Uid>"  -Scope @()
    ```

```
$provScheme =New-ProvScheme  -CleanOnBoot

-HostingUnitName "vSanRg"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<network name>.network"}

-ProvisioningSchemeName "<string>"

-Scope @() -VMCpuCount 4

-VMMemoryMB 6144

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template" -TenancyType Shared

-FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False

-MinimumFunctionalLevel 'L7_9'

-Name "<catalog name>"

-ProvisioningType 'MCS'

-Scope @()
```

```
-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- 非vTPM VMwareテンプレートをマシンプロファイルのソースとして、Windows 10がインストールされたマスターイメージでマシンカタログを作成するには：

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###" -NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-CleanOnBoot -HostingUnitName "<string>"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4  -
VMMemoryMB 8192

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template"
```

```
-TenancyType Shared  -FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False

-MinimumFunctionalLevel 'L7_9' -Name "<string>" -ProvisioningType
'MCS' -Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- 暗号化されたストレージポリシーが適用されたマシンプロファイルテンプレートを使用して、フルコピーディスクモードでマシンカタログを作成するには：

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###"

-NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-HostingUnitName "<string>"
```

```
-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"

-Scope @() -VMCpuCount 4  -VMMemoryMB 8192 -MachineProfile "XDHyp:
\HostingUnits\<hosting unit name>\<template name>.template"

-TenancyType Shared

-FunctionalLevel "L7_20" -UseFullDiskCloneProvisioning
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"  -IsRemotePC $False

-MinimumFunctionalLevel 'L7_9'

-Name "<string>" -ProvisioningType 'MCS' -Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

マシンプロファイルを更新するには、Set-ProvSchemeコマンドを使用します。例：

```
Set-ProvScheme -ProvisioningSchemeName 'name' -IdentityPoolName 'name'
-MachineProfile 'XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template'
```

複数のNICの確認

マシンプロファイルを使用し、`New-ProvScheme`および`Set-ProvScheme`コマンドで`NetworkMapping`パラメーターを使用する場合、複数のNICの事前チェック中にさまざまなエラーメッセージが表示されます。

複数のNICの事前チェックリストは次のとおりです。

- マシンプロファイルテンプレートからのNIC数のみが使用され、検証されます。これらのNICが指すネットワークは、ホスティングユニットネットワークに対して使用または検証されません。
- マシンプロファイルテンプレートのNIC数がホスティングユニットのネットワーク数よりも多い場合、エラーメッセージが表示されます。
- マシンプロファイルテンプレートのNIC数がゼロの場合、エラーメッセージが表示されます。マシンプロファイルテンプレートのNIC数が1の場合：
  - `New-ProvScheme`または`Set-ProvScheme`コマンドでネットワークマッピングが指定されておらず、ホスティングユニットネットワークが1つの場合、そのホスティングユニットネットワークが使用されます。
  - ネットワークマッピングが指定されている場合、それが有効であれば、指定されたネットワークマッピングが使用されます。
- マシンプロファイルテンプレートのNIC数が1より大きい場合、またはホスティングユニットネットワーク数が1より大きい場合：
  - コマンドには有効なネットワークマッピングが必要であり、各NICのマッピングを提供する必要があります（つまり、NetworkMappingの数はマシンプロファイルのNIC数と同じである必要があります）。
  - 複数のNICをホスティングユニット内の同じネットワークにマッピングすることはできません。
  - `NetworkMapping`の数とマシンプロファイルのNIC数は、ホスティングユニットのネットワーク数以下である必要があります。
  - `NetworkMapping`は、0からn-1までの各IDに対して指定する必要があります。ここで、nはマシンプロファイルテンプレート内のネットワークアダプターの数です。

トラブルシューティング

カタログの作成に失敗した場合は、CTX294978を参照してください。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、「」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure.html)を参照してください。
- カタログを管理するには、マシンカタログの管理およびVMwareカタログの管理を参照してください。

詳細情報

- 接続とリソースの作成および管理
- VMwareへの接続
- マシンカタログの作成

異なる結合タイプのカタログを作成する

MCS を使用すると、オンプレミス AD 参加、ハイブリッド Azure AD 参加、またはドメイン非参加としてマシンをプロビジョニングできます。

Web Studio でマシン ID を構成する方法については、「マシンカタログの作成」を参照してください。

マシンIDが結合されたカタログを作成する方法に関する具体的な情報については、以下を参照してください。

- Hybrid Azure Active Directory 参加済みカタログを作成する
- ドメイン非参加カタログを作成する

ハイブリッド Azure Active Directory 参加済みカタログを作成する

> **注:**

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

> この記事では、ハイブリッド Azure Active Directory (AD) 参加済みカタログを作成する方法について説明します。

Web Studio または PowerShell を使用して、Azure AD 参加済みカタログを作成できます。

要件、制限、および考慮事項については、「ハイブリッドAzure Active Directory参加済み」を参照してください。

Web Studioを使用する

以下の情報は、マシンカタログの作成 のガイダンスを補足するものです。ハイブリッド Azure AD 参加済みカタログを作成するには、その記事の一般的なガイダンスに従い、ハイブリッド Azure AD 参加済みカタログに固有の詳細に注意してください。

カタログ作成ウィザードで：

- **マシンID**ページで、**ハイブリッドAzure Active Directory参加済み**を選択します。作成されたマシンは組織によって所有され、その組織に属するActive Directory Domain Servicesアカウントでサインインされます。これらはクラウドとオンプレミスの両方に存在します。

> **注:**
>
> IDの種類として**ハイブリッドAzure Active Directory参加済み**を選択した場合、カタログ内の各マシンには対応するADコンピューターアカウントが必要です。

PowerShell を使用する

以下は、Web Studio での操作に相当する PowerShell の手順です。Remote PowerShell SDK を使用してカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>` を参照してください。

オンプレミス AD 参加済みカタログとハイブリッド Azure AD 参加済みカタログの違いは、ID プールとマシンアカウントの作成方法にあります。

ハイブリッド Azure AD 参加済みカタログのアカウントとともに ID プールを作成するには：

```
New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -Domain
"corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -NamingScheme
"HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU
"CN=AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"

New-AcctADAccount -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
-ADUserName "corp\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -All
-ADUserName "corp\admin1" -ADPassword $password
```

注:

`$password` は、書き込み権限を持つADユーザーアカウントの一致するパスワードです。

ハイブリッド Azure AD 参加済みカタログの作成に使用されるその他のすべてのコマンドは、従来のオンプレミス AD 参加済みカタログの場合と同じです。

ハイブリッド Azure AD 参加プロセスのステータスを表示する

Web Studioでは、デリバリーグループ内のハイブリッドAzure AD参加済みマシンが電源オン状態の場合に、ハイブリッドAzure AD参加プロセスのステータスが表示されます。ステータスを表示するには、Search を使用してそれらのマシンを特定し、下部ペインの **「詳細」** タブで各マシンの **「マシンID」** を確認します。**「マシンID」** には次の情報が表示されます。

- ハイブリッド Azure AD参加済み
- Azure AD にまだ参加していません

注:

- マシンの初期電源投入時に、ハイブリッドAzure AD参加が遅延する場合があります。これは、デフォルトのマシンID同期間隔（Azure AD Connectの30分）が原因です。マシンは、マシンIDがAzure AD Connectを介してAzure ADに同期された後にのみ、ハイブリッドAzure AD参加済み状態になります。

- マシンがハイブリッドAzure AD参加済み状態にならない場合、それらはDelivery Controllerに登録されません。登録ステータスは **「初期化」** と表示されます。

また、Web Studioを使用して、マシンが利用できない理由を知ることができます。そのためには、**「検索」** ノードでマシンをクリックし、下部ペインの **「詳細」** タブで **「登録」** を確認し、ツールヒントを読んで追加情報を確認します。

トラブルシューティング

マシンがハイブリッド Azure AD 参加済みにならなかった場合は、次の操作を行います。

- Microsoft Azure ADポータルを通じて、マシンアカウントがAzure ADに同期されているかどうかを確認します。同期されている場合、**「まだAzure ADに参加していません」** と表示され、登録ステータスが保留中であることを示します。

  マシンアカウントをAzure ADに同期するには、以下を確認してください:

  - マシンアカウントが、Azure ADと同期するように構成されているOU内にあること。**userCertificate**属性を持たないマシンアカウントは、同期するように構成されているOU内にあっても、Azure ADには同期されません。
  - マシンアカウントに**userCertificate**属性が入力されていること。この属性を表示するには、Active Directory Explorerを使用します。
  - マシンアカウントが作成された後、Azure AD Connectが少なくとも1回は同期されている必要があります。同期されていない場合は、Azure AD ConnectマシンのPowerShellコンソールで`Start-ADSyncSyncCycle -PolicyType Delta`コマンドを手動で実行し、即時同期をトリガーします。

- ハイブリッドAzure AD参加用のCitrix管理デバイスキーペアがマシンに正しくプッシュされているか、**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix** の下の **DeviceKeyPairRestored** の値をクエリして確認します。

  値が1であることを確認します。そうでない場合、考えられる理由は次のとおりです。

  - プロビジョニングスキームに関連付けられているIDプール`IdentityType`が`HybridAzureAD`に設定されていません。これは`Get-AcctIdentityPool`を実行して確認できます。
  - マシンが、マシンカタログと同じプロビジョニングスキームを使用してプロビジョニングされていない。

  - マシンがローカルドメインに参加していない。ローカルドメインへの参加は、ハイブリッドAzure AD参加の前提条件です。

- MCSでプロビジョニングされたマシンで`dsregcmd /status /debug`コマンドを実行して、診断メッセージを確認します。
  - ハイブリッドAzure AD参加が成功した場合、コマンドラインの出力で **AzureAdJoined** と **DomainJoined** が **YES** になります。
  - そうでない場合、問題をトラブルシューティングするにはMicrosoftのドキュメントを参照してください: `<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current>`。
  - エラーメッセージ「**Server Message: The user certificate is not found on the device with id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**」が表示された場合は、次のPowerShellコマンドを実行してユーザー証明書を修復してください。

    ```
    Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
    UserCertificate
    ```

    ユーザー証明書の問題の詳細については、CTX566696を参照してください。

非ドメイン参加型カタログを作成する

この記事では、Citrix Virtual Apps and Desktops を使用して非ドメイン参加型カタログを作成する方法について説明します。

要件、制限、および考慮事項については、「非ドメイン参加型」を参照してください。

マシンカタログを作成する前に、次のものが必要です。

1. 新しいリソースの場所
   - Citrix Cloud™ 管理 UI > 左上のハンバーガーメニュー > **リソースの場所** に移動します。
   - 「**+ リソースの場所**」をクリックします。
   - 新しいリソースの場所の名前を入力し、「**保存**」をクリックします。
2. ホスティング接続を作成します。詳細については、「接続の作成と管理」セクションを参照してください。

Citrix Virtual Apps and Desktops を使用すると、ワークグループまたは非ドメイン参加型マシンに基づいてカタログを作成できます。非ドメイン参加型マシンの作成は、アカウントIDプールがど

のように作成されるかによって異なります。アカウントIDプールは、カタログプロビジョニング中にMCSがマシン名を作成および追跡するために使用するメカニズムです。

現在、非ドメイン参加型カタログはPowerShellコマンドを使用してのみ作成できます。

PowerShell を使用する

Remote PowerShell SDK を使用して、非ドメイン参加型カタログのIDプールを作成できます。

PowerShellパラメーターの **WorkgroupMachine** と **IdentityType** を使用して、非ドメイン参加型カタログのIDプールを作成します。これらのパラメーターにより、ドメイン管理者資格情報を含むすべてのAD固有のパラメーターを指定する必要がなくなります。

```
New-AcctIdentityPool -AllowUnicode -IdentityType "Workgroup"
-WorkgroupMachine -IdentityPoolName "NonDomainJoinedCatalog" -NamingScheme
"NDJ-VM-##" -NamingSchemeType "Numeric" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"
```

非ドメイン参加型カタログの作成に使用されるその他のすべてのコマンドは、従来のオンプレミスActive Directory参加型カタログの場合と同じです。

マシンカタログを管理する

注:

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

はじめに

マシンカタログへのマシンの追加または削除、名前の変更、説明の変更、またはカタログのActive Directoryコンピューターアカウントの管理を行うことができます。

カタログの保守には、各マシンに最新のOSアップデートが適用されていることを確認することも含まれます。これには、ウイルス対策アップデート、オペレーティングシステムのアップグレード、または構成変更が含まれます。

- Machine Creation Services™ (MCS) を使用して作成されたプールされたランダムマシンを含むカタログは、カタログで使用されるマスターイメージを更新し、その後マシンを更新することでマシンを保守します。この方法により、多数のユーザーマシンを効率的に更新できます。
- 静的で永続的に割り当てられたマシンを含むカタログ、およびリモートPCアクセス マシンカタログの場合、ユーザーマシンの更新はWeb Studioの外部で管理します。このタスクは、個別に、またはサードパーティのソフトウェア配布ツールを使用してまとめて実行します。

ホストハイパーバイザーへの接続の作成と管理については、「接続とリソース」を参照してください。

> **注:**
>
> MCSはWindows 10 IoT CoreおよびWindows 10 IoT Enterpriseをサポートしていません。詳細については、Microsoftサイトを参照してください。

永続インスタンスについて

永続インスタンスまたは専用インスタンスを使用して作成されたMCSカタログを更新する場合、カタログ用に作成された新しいマシンは更新されたイメージを使用します。既存のインスタンスは元のインスタンスを引き続き使用します。イメージの更新プロセスは、他の種類のカタログと同じ方法で行われます。以下を考慮してください。

- 永続ディスクカタログの場合、既存のマシンは新しいイメージに更新されませんが、カタログに追加される新しいマシンは新しいイメージを使用します。
- 非永続ディスクカタログの場合、マシンイメージはマシンがリセットされるたびに更新されます。
- 永続的なマシンカタログの場合、イメージを更新すると、それを使用するカタログインスタンスも更新されます。
- 永続的ではないカタログの場合、異なるマシンに異なるイメージを使用したい場合は、イメージを別々のカタログに配置する必要があります。

マシンカタログを管理する

マシンカタログは、次の2つの方法で管理できます。

- Web Studioの使用
- PowerShellを使用する

Web Studioを使用する

このセクションでは、Web Studioを使用してカタログを管理する方法について詳しく説明します。

- マシンカタログの管理
  - はじめに
  - 永続インスタンスについて
- マシンカタログの管理
- Web Studioの使用
- カタログの詳細の表示
  - カタログへのマシンの追加
  - カタログからマシンを削除する(#delete-machines-from-a-catalog)
- カタログを編集する(#edit-a-catalog)
- カタログの名前を変更する(#rename-a-catalog)
- カタログを別のゾーンに移動する(#move-a-catalog-to-a-different-zone)
- カタログを削除する(#delete-a-catalog)
- カタログ内のActive Directoryコンピューターアカウントを管理する(#manage-active-directory-computer-accounts-in-a-catalog)
- カタログを更新する(#update-a-catalog)
  - マスターイメージを更新または作成する(#update-or-create-a-master-image)
  - マスターイメージを変更する(#change-the-master-image)
  - マスターイメージをロールバックする(#roll-back-the-master-image)
- 機能レベルを変更または変更を元に戻す(#change-the-functional-level-or-undo-the-change)
- カタログをクローンする(#clone-a-catalog)
- フォルダーを使用してカタログを整理する(#organize-catalogs-using-folders)
  - カタログフォルダーを作成する(#create-a-catalog-folder)
  - カタログを移動する(#move-a-catalog)
  - カタログフォルダーの管理(#manage-catalog-folders)
- カタログ作成の再試行(#retry-catalog-creation)

- トークンを使用してMCS以外でプロビジョニングされたVDAを登録する（プレビュー）(#enroll-non-mcs-provisioned-vdas-using-tokens-preview)
- PowerShellの使用(#use-powershell)
- カタログに関連付けられた警告とエラーの取得(#retrieve-warnings-and-errors-associated-with-a-catalog)
- イメージに説明を追加する(#add-descriptions-to-an-image)
- OSディスクのリセット(#reset-os-disk)
- 既存のプロビジョニングスキームのネットワーク設定を変更する(#change-the-network-setting-for-an-existing-provisioning-scheme)
- マシンカタログのバージョンの管理(#manage-versions-of-a-machine-catalog)
- マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換する(#convert-a-non-machine-profile-based-machine-catalog-to-machine-profile-based-machine-catalog)
- アクティブなコンピューターアカウントのID情報の修復(#repair-the-identity-information-of-active-computer-accounts)
  - 条件(#conditions)
  - IDディスクのリセット(#reset-identity-disk)
- 既存のマシンカタログのキャッシュ構成を変更する(#change-cache-configuration-on-an-existing-machine-catalog)
  - 要件(#requirements)
  - キャッシュ構成を変更する
- ローカルファイル共有アクセスによるVDA更新のサポート
  - PowerShellコマンドレット
  - 前提条件
  - ファイル共有権限の設定方法
  - ローカルファイル共有からのVDA更新
- トラブルシューティング
- 次のステップ

カタログの詳細を表示する

1. 検索機能を使用して特定のマシンカタログを見つけます。手順については、インスタンスの検索を参照してください。
2. 検索結果から、必要に応じてカタログを選択します。
3. カタログ列の説明については、次の表を参照してください。
4. このカタログに関する詳細情報については、下部の詳細ペインにあるタブをクリックしてください。

列	説明	
マシンカタログ	カタログの名前と割り当ての種類。割り当ての種類は次のとおりです。 • ランダム: カタログ内のマシンはユーザーにランダムに割り当てられます。 • 永続: カタログ内のマシンはユーザーに永続的に割り当てられます。	
マシンタイプ	カタログ内のマシンでサポートされているセッションの種類。指定できる値は次のとおりです。 • OSの種類: マルチセッションOS (仮想); ユーザーデータ: 破棄。 • OSの種類: マルチセッションOS (仮想); ユーザーデータ: ローカルディスク上	

列	説明
	• OSの種類: シングルセッションOS (リモートPCアクセス)
	OSタイプ: シングルセッションOS (仮想); ユーザーデータ: 破棄
	OSタイプ: シングルセッションOS (仮想); ユーザーデータ: ローカルディスク上
マシン数	カタログ内のマシン数とプロビジョニング方法。可能なプロビジョニング方法には、マシン作成サービス (MCSマシン)、手動、Citrix Provisioning™サービスがあります。
割り当て済み数	デリバリーグループに割り当てられているカタログ内のマシン数。
フォルダー	**マシンカタログ**ツリー内でのカタログの場所。カタログが属するフォルダーの名前 (末尾のバックスラッシュを含む) または、カタログがルートレベルにある場合は `-` が表示されます。
VDAアップグレード	VDAアップグレードの状態。可能な値には、未構成、スケジュール済み、利用可能、最新があります。
イメージステータス	カタログのイメージ更新ステータス。非永続マシンカタログにのみ適用されます。可能な値には、完全に更新済

列	説明
	み、部分的に更新済み、更新保留中、準備中があります。

マシンをカタログに追加する

開始する前に:

- 仮想化ホストに、追加のマシンを収容するのに十分なプロセッサ、メモリ、ストレージがあることを確認してください。
- 未使用のActive Directoryコンピューターアカウントが十分にあることを確認してください。既存のアカウントを使用している場合、追加できるマシンの数は利用可能なアカウントの数によって制限されます。
- Web Studioを使用して追加のマシン用のActive Directoryコンピューターアカウントを作成する場合、適切なドメイン管理者権限が必要です。

マシンをカタログに追加するには：

1. Web Studioにサインインします。
2. 左ペインで**マシンカタログ**を選択します。
3. マシンカタログを選択し、アクションバーで**マシンの追加**を選択します。
4. 追加する仮想マシンの数を選択します。
5. 追加するVMの数に対して既存のActive Directoryアカウントが不足している場合は、アカウントが作成されるドメインと場所を選択します。連続する数字または文字が表示される場所を示すためにハッシュマークを使用して、アカウントの命名スキームを指定します。OU名にスラッシュ（/）を使用しないでください。名前は数字で始めることはできません。たとえば、PC-Sales-##（0-9が選択されている場合）という命名スキームは、PC-Sales-01、PC-Sales-02、PC-Sales-03などのコンピューターアカウントになります。
6. 既存のActive Directoryアカウントを使用する場合は、アカウントを参照するか、**インポート**をクリックしてアカウント名を含む.csvファイルを指定します。追加するすべてのマシンに対して十分なアカウントがあることを確認してください。Web Studioはこれらのアカウントを管理します。Web Studioにすべてのアカウントのパスワードをリセットさせるか、すべてのアカウントで同じである必要があるアカウントパスワードを指定します。

マシンはバックグラウンドプロセスとして作成され、多数のマシンを作成する場合は時間がかかることがあります。Web Studioを閉じても、マシンの作成は続行されます。

カタログからマシンを削除する

マシンカタログからマシンを削除すると、ユーザーはそのマシンにアクセスできなくなるため、マシンを削除する前に、以下を確認してください。

- ユーザーデータがバックアップされているか、不要になっている。
- すべてのユーザーがログオフしている。メンテナンスモードをオンにすると、マシンへの新しい接続が停止します。
- マシンは電源オフの状態です。

カタログからマシンを削除するには：

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. カタログを選択し、アクションバーで を選択します。
4. 1つ以上のマシンを選択し、アクションバーで を選択します。

削除するマシンを削除するかどうかを選択します。マシンを削除することを選択した場合は、それらのマシンのActive Directoryアカウントを保持するか、無効にするか、削除するかを指定します。

カタログを編集する

1. ページで、カタログの説明を変更します。
2. 左側のペインで を選択します。
3. カタログを選択し、アクションバーで を選択します。
4. ページで、スコープを変更します。
5. ページで、次の操作を実行します。

    - NICのサブネットマッピングを変更するには、 フィールドからネットワークを選択します。
    - サブネットマッピングを追加するには、 を選択し、 フィールドからネットワークを選択して、 をクリックします。

    カタログに関連付けられたホストに存在するサブネットのみが、**関連付けられたネットワーク**フィールドに表示されます。

    マシンプロファイルのないAzureマシンカタログにのみNICを追加できます。

> **注:**
>
> - AWSマシンカタログの場合、同じサブネットを複数のNICにマッピングすることはできません。
> - マシンプロファイルを持つマシンカタログの場合、カタログ上のNICの数は、マシンプロファイル上のNICの数と等しくなければなりません。
> - この機能は、IBM Cloudハイパーバイザーではサポートされていません。
> - この機能は、Nutanixハイパーバイザーの場合、Nutanix Prism Elementでのみサポートされています。

6. カタログの種類によっては、他のページが表示される場合があります。

   Azure Resource Managerイメージを使用して作成されたカタログの場合、以下のページが表示されます。行った変更は、後でカタログに追加するマシンにのみ適用されることに注意してください。既存のマシンは変更されません。

   - **Virtual Machines**ページで、マシンを作成するマシンサイズと可用性ゾーンを変更します。

     > **注:**
     >
     > ◦ カタログがサポートするマシンサイズのみが表示されます。
     > ◦ 必要に応じて、マシンサイズリストをフィルタリングするには、**他のマシンカタログで使用されているマシンサイズのみを表示**を選択します。

   - **Machine Profile**ページで、マシンプロファイルを使用するか変更するかを選択します。
   - （カタログが専用グループホストで構成されている場合にのみ表示）**専用ホストグループ**ページで、ホストグループを変更するかどうかを選択します。
   - 「**ストレージとライセンスの種類**」ページで、ストレージの種類、ライセンスの種類、およびAzure Computer Galleryの設定を変更するかどうかを選択します（「**準備済みイメージをAzure Galleryに配置**」が使用されている場合のみ利用可能）。

> 「**注：**」:

> 新しく選択した設定が現在のマシンサイズをサポートしていない場合、設定を変更するとマシンサイズの設定がリセットされることを通知する警告ダイアログボックスが表示されます。続行することを選択すると、**仮想マシン**メニューの横に赤い点が表示され、新しいマシンサイズを選択するように促されます。

- **ライセンスの種類**ページで、WindowsライセンスまたはLinuxライセンスの設定を変更するかどうかを選択します。

Remote PC Accessカタログの場合、以下のページが表示されます。

- **電源管理**ページで、電源管理設定を変更し、電源管理接続を選択します。
- **組織単位**ページで、Active Directory OUを追加または削除します。

7. 行った変更を適用するには**適用**をクリックし、終了するには**保存**をクリックします。

カタログの名前を変更する

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**マシンカタログの名前を変更**を選択します。
4. 新しい名前を入力します。

カタログを別のゾーンに移動する

展開に複数のゾーンがある場合、カタログをあるゾーンから別のゾーンに移動できます。

カタログを、そのカタログ内のVMを含むハイパーバイザー以外のゾーンに移動すると、パフォーマンスに影響します。

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**移動**を選択します。
4. カタログを移動するゾーンを選択します。

カタログを削除する

カタログを削除する前に、以下を確認してください。

- すべてのユーザーがログオフしており、切断されたセッションが実行されていないこと。

- カタログ内のすべてのマシンでメンテナンスモードがオンになっており、新しい接続ができないこと。
- カタログ内のすべてのマシンの電源がオフになっていること。
- カタログがデリバリーグループに関連付けられていないこと。つまり、デリバリーグループにそのカタログのマシンが含まれていないこと。

カタログを削除するには：

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**マシンカタログの削除**を選択します。
4. カタログ内のマシンを削除するかどうかを指定します。マシンを削除することを選択した場合、それらのマシンのActive Directoryコンピューターアカウントを保持するか、無効にするか、削除するかを指定します。

カタログ内のActive Directoryコンピューターアカウントを管理する

マシンカタログ内のActive Directoryアカウントを管理するには、次の操作を実行できます。

- シングルセッションOSおよびマルチセッションOSカタログからActive Directoryコンピューターアカウントを削除することで、未使用のマシンアカウントを解放します。これらのアカウントは、他のマシンで使用できます。
- カタログにマシンが追加されたときに、コンピューターアカウントがすでに存在するようにアカウントを追加します。OU名にスラッシュ (/) を使用しないでください。

Active Directoryアカウントを管理するには：

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**Manage AD accounts**を選択します。
4. コンピューターアカウントを追加するか削除するかを選択します。アカウントを追加する場合は、アカウントのパスワードをどうするかを指定します。すべてリセットするか、すべてのアカウントに適用されるパスワードを入力します。

   現在のアカウントパスワードがわからない場合は、パスワードをリセットできます。パスワードのリセットを実行する権限が必要です。パスワードを入力すると、アカウントがインポートされるときにパスワードが変更されます。アカウントを削除するときは、Active Directory内のアカウントを保持するか、無効にするか、削除するかを選択します。

カタログからマシンを削除したり、カタログを削除したりする際に、Active Directoryアカウントを保持するか、無効にするか、削除するかを指定します。

カタログを更新する

カタログ内のマシンを更新する前に、マスターイメージのコピーまたはスナップショットを保存することをお勧めします。データベースは、各マシンカタログで使用されたマスターイメージの履歴レコードを保持します。カタログ内のマシンをロールバックまたは元に戻して、マスターイメージの以前のバージョンを使用します。ユーザーがデスクトップに展開した更新プログラムで問題が発生した場合に、このタスクを実行します。これにより、ユーザーのダウンタイムが最小限に抑えられます。マスターイメージを削除、移動、または名前変更しないでください。それらを使用してカタログを元に戻すことはできません。

マシンが更新されると、自動的に再起動します。

マスターイメージを更新または作成する

マシンカタログを更新する前に、既存のマスターイメージを更新するか、ホストハイパーバイザー上に新しいマスターイメージを作成します。

1. ハイパーバイザーで、現在のVMのスナップショットを取得し、そのスナップショットに意味のある名前を付けます。このスナップショットは、必要に応じてカタログ内のマシンを元に戻す（ロールバックする）ために使用できます。
2. 必要に応じて、マスターイメージの電源をオンにし、ログオンします。
3. 更新プログラムをインストールするか、マスターイメージに必要な変更を加えます。
4. VMの電源をオフにします。
5. VMのスナップショットを取得します。Web Studioでカタログが更新されたときに認識されるような、意味のある名前を付けます。Web Studioでスナップショットを作成することもできますが、Citrixではハイパーバイザー管理コンソールを使用して作成することをお勧めします。その後、Web Studioでそのスナップショットを選択します。このプロセスにより、自動生成された名前ではなく、意味のある名前と説明を提供できます。GPUマスターイメージの場合、マスターイメージはXenServer®コンソールからのみ変更できます。

マスターイメージを変更する

カタログ内のすべてのマシンに更新プログラムを準備して展開するには：

1. Web Studioにサインインします。
2. 左ペインで**マシンカタログ**を選択します。
3. カタログを選択し、アクションバーで**マスターイメージの変更**を選択します。

4. **イメージ**ページで、展開するホストとイメージを選択します。

> **ヒント：**
>
> MCSで作成されたカタログの場合、イメージにメモを追加してイメージに注釈を付けることができます。メモは最大500文字まで含めることができます。マスターイメージを変更するたびに、メモを追加したかどうかにかかわらず、メモ関連のエントリが作成されます。メモを追加せずにカタログを更新した場合、エントリはnull (-) と表示されます。イメージのメモ履歴を表示するには、カタログを選択し、下部のペインで**テンプレートプロパティ**をクリックし、**メモ履歴の表示**をクリックします。

5. 「**ロールアウト戦略**」ページで、マシンカタログ内のマシンを新しいマスターイメージで更新するタイミング（次回のシャットダウン時または即時）を選択します。

> **注：**
>
> **［ロールアウト戦略］** ページは永続VMでは利用できません。ロールアウトは非永続VMにのみ適用されるためです。

6. 「**概要**」ページで情報を確認し、「**完了**」をクリックします。各マシンは更新後に自動的に再起動します。

更新の進行状況を追跡するには、「**マシンカタログ**」でカタログを見つけ、インラインの進行状況バーと段階的な進行状況グラフを表示します。

Web StudioではなくPowerShell SDKを直接使用してカタログを更新する場合は、ハイパーバイザーテンプレート（**VMTemplates**）を指定します。これは、イメージまたはイメージのスナップショットの代替として使用します。

ロールアウト戦略：

次回のシャットダウン時にイメージを更新すると、現在使用されていないマシン、つまりアクティブなユーザーセッションがないマシンにすぐに影響します。使用中のシステムは、現在のアクティブセッションが終了したときに更新を受け取ります。以下を考慮してください。

- 該当するマシンでの更新が完了するまで、新しいセッションを起動することはできません。
- シングルセッションOSマシンでは、マシンが使用されていないとき、またはユーザーがログインしていないときに、マシンはすぐに更新されます。

- 子マシンを持つマルチセッションOSの場合、再起動は自動的に行われません。更新されたマスターイメージを適用するには、Studio、PowerShell、またはWorkspaceを使用してマシンを再起動します。マシンまたはハイパーバイザーから再起動しても、更新は適用されません。

> **ヒント：**
>
> ホスト接続の詳細設定を使用して、再起動されるマシンの数を制限します。これらの設定を使用して、特定のカタログに対して実行されるアクションを変更します。詳細設定はハイパーバイザーによって異なります。

マスターイメージをロールバックする

更新された、または新しいマスターイメージをロールアウトした後、それをロールバックできます。このプロセスは、新しく更新されたマシンで問題が発生した場合に必要になることがあります。ロールバックすると、カタログ内のマシンは最後に正常に動作したイメージにロールバックされます。新しいイメージを必要とする新機能は利用できなくなります。ロールアウトと同様に、マシンのロールバックには再起動が含まれます。

1. Web Studioにサインインします。
2. 左側のペインで**マシンカタログ**を選択します。
3. カタログを選択し、アクションバーで**マスターイメージのロールバック**を選択します。
4. ロールアウト操作に関する前のセクションで説明されているように、以前のマスターイメージをマシンに適用するタイミングを指定します。

ロールバックは、元に戻す必要があるマシンにのみ適用されます。新しいまたは更新されたマスターイメージで更新されていないマシンは、通知メッセージを受信せず、強制的にログオフされることもありません。

ロールバックの進行状況を追跡するには、 でカタログを見つけて、インラインの進行状況バーと段階的な進行状況グラフを表示します。

機能レベルを変更するか、変更を元に戻す

マシンのVDAを新しいバージョンにアップグレードした後、マシンカタログの機能レベルを変更します。Citrixでは、すべての最新機能にアクセスできるように、すべてのVDAを最新バージョンにアップグレードすることをお勧めします。

マシンカタログの機能レベルを変更する前に、次の点に注意してください。

- アップグレードされたマシンを起動して、Controllerに登録させます。このプロセスにより、Web Studioはカタログ内のマシンがアップグレードを必要としていることを判断できます。

カタログの機能レベルを変更するには：

1. Web Studioにサインインします。
2. 左側のペインで**マシンカタログ**を選択します。
3. カタログを選択します。下部のペインにある**詳細**タブにバージョン情報が表示されます。
4. **機能レベルの変更**を選択します。Web Studioがカタログのアップグレードが必要であると検出した場合、メッセージが表示されます。プロンプトに従います。1つ以上のマシンをアップグレードできない場合は、その理由を説明するメッセージが表示されます。すべてのマシンが正常に機能するように、Citrixは**変更**をクリックして続行する前に、マシンの問題を解決することをお勧めします。

カタログの変更が完了した後、カタログを選択し、アクションバーで**機能レベルの変更を元に戻す**を選択することで、マシンを以前のVDAバージョンに戻すことができます。

カタログを複製する

カタログをクローンする前に、以下の考慮事項に注意してください。

- オペレーティングシステムおよびマシン管理に関連する設定は変更できません。クローンされたカタログは、元のカタログからこれらの設定を継承します。
- カタログのクローン作成には時間がかかる場合があります。必要に応じて、**進行状況を非表示**を選択して、バックグラウンドでクローン作成を実行できます。
- クローンされたカタログは元のカタログの名前を継承し、サフィックス`Copy`が付きます。名前は変更できます。カタログの名前を変更するを参照してください。
- クローン作成が完了したら、クローンされたカタログをデリバリーグループに割り当てるようにしてください。

1. Web Studioにサインインし、左ペインで**マシンカタログ**を選択します。
2. カタログを選択し、アクションバーで**クローン**を選択します。
3. **選択したマシンカタログのクローン**ウィンドウで、クローンされたカタログの設定を表示し、必要に応じて設定を構成します。**次へ**を選択して次のページに進みます。
4. **概要**ページで、設定の概要を確認し、**完了**を選択してクローン作成を開始します。
5. 必要に応じて、**進行状況を非表示**を選択して、バックグラウンドでクローン作成を実行できます。

フォルダーを使用してカタログを整理する

アクセスしやすいように、フォルダーを作成してカタログを整理できます。たとえば、イメージの種類別や組織構造別にカタログを整理できます。

カタログフォルダーを作成する

始める前に、まずカタログの整理方法を計画してください。以下を考慮してください。

- フォルダーは最大5レベルまでネストできます（デフォルトのルートフォルダーを除く）。
- カタログフォルダーには、カタログとサブフォルダーを含めることができます。
- Web Studioのすべてのノード（**マシンカタログ**ノードや**アプリケーション**ノードなど）は、バックエンドでフォルダーツリーを共有しています。フォルダーの名前変更や移動の際に他のノードとの名前の競合を避けるため、異なるノードの第一レベルフォルダーには異なる名前を付けることをお勧めします。

カタログフォルダーを作成するには、次の手順に従います。

1. 左側のペインで**Machine Catalogs**を選択します。
2. フォルダー階層でフォルダーを選択し、**アクション**バーで**フォルダーの作成**を選択します。
3. 新しいフォルダーの名前を入力し、**完了**をクリックします。

> **ヒント:**

> 意図しない場所にフォルダーを作成した場合でも、正しい場所にドラッグして移動できます。

カタログを移動する

カタログはフォルダー間で移動できます。詳細な手順は次のとおりです。

1. 左ペインで**マシンカタログ**を選択します。
2. フォルダーごとにカタログを表示します。フォルダー階層の上にある**すべて表示**をオンにすると、すべてのカタログを一度に表示することもできます。
3. カタログを右クリックし、**マシンカタログの移動**を選択します。
4. カタログを移動するフォルダーを選択し、**完了**をクリックします。

> **ヒント:**

> カタログをフォルダーにドラッグできます。

カタログフォルダーの管理

カタログフォルダーの削除、名前の変更、移動ができます。

フォルダーとそのサブフォルダーにカタログが含まれていない場合にのみ、フォルダーを削除できます。

フォルダーを管理するには、以下の手順に従います。

1. 左側のペインで**Machine Catalogs**を選択します。
2. フォルダー階層でフォルダーを選択し、必要に応じて**アクション**バーでアクションを選択します。
   - フォルダーの名前を変更するには、**フォルダー名の変更**を選択します。
   - フォルダーを削除するには、**フォルダーの削除**を選択します。
   - フォルダーを移動するには、**フォルダーの移動**を選択します。
3. 画面の指示に従って、残りの手順を完了します。

カタログ作成を再試行する

> **注:**
>
> この機能はMCSカタログにのみ適用されます。

> 失敗したカタログにはエラーアイコンが表示されます。詳細を確認するには、各カタログの**トラブルシューティング**タブに移動してください。カタログの作成を再試行する前に、以下の考慮事項に注意してください。

- まずトラブルシューティング情報を確認し、問題を解決してください。この情報には、検出された問題とその解決策に関する推奨事項が記載されています。
- Operating systemおよびmachine managementに関連する設定は変更できません。カタログはこれらの設定を元のものから継承します。
- 作成には時間がかかる場合があります。必要に応じて、**進行状況を非表示**を選択して、バックグラウンドで作成を実行してください。

カタログの作成を再試行するには、次の手順を実行します。

1. Web Studioから、左側のペインで**マシンカタログ**を選択します。
2. カタログを選択し、その**トラブルシューティング**タブに移動します。
3. 再試行ハイパーリンクをクリックして、カタログの作成を再試行します。
4. 表示されるウィザードで、必要に応じて設定を変更します。変更の必要がない場合は、直接**概要**ページに進むことができます。
5. 完了したら、**完了**を選択して作成を開始します。

トークンを使用して非MCSプロビジョニングVDAを登録する（プレビュー）

非MCSプロビジョニングVDAの登録トークンを生成および管理できるようになりました。この実装により、MCSでVDAをプロビジョニングすることなく、WebSocket経由でVDA登録が可能になります。この機能は、Linux Virtual Delivery Agent、macOS用Citrix Virtual Delivery Agent、およびCitrix Virtual Apps and Desktopsを使用するドメイン非参加VDAもサポートしています。

始める前に

1. サイトを構成します。詳細については、サイトの作成を参照してください。
2. Delivery Controller に TLS 証明書をインストールします。詳細については、「コントローラーに TLS サーバー証明書をインストールする」を参照してください。
3. Delivery Controller を信頼するために、VDA にルート CA と中間 CA をインストールします。
4. Delivery Controller で WebSocket 接続を有効にします。サイト上の各 Delivery Controller で次のコマンドを実行します。

```
New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy"
-Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -Force
```

> **注:**
>
> WebSocketを有効にした後、必ずDelivery Controllerを再起動してください。

登録トークンを生成する

Citrix 以外でプロビジョニングされたマシンに対してトークンベースの登録を有効にすることを決定したら、まずマシンカタログごとにトークンを生成し、VDA インストール管理者と共有する必要があります。

登録トークンの機能:

- 登録範囲: 1〜100 台の VDA マシン
- 有効期間: 最大 14 日間

Web Studioを使用してカタログのトークンを生成するには、次の手順に従います。

1. **Web Studio > マシンカタログ**で、**マシン数**列に**プロビジョニング方法: 手動**と表示されている、MCS 以外でプロビジョニングされたカタログを見つけます。
2. カタログを右クリックし、**登録トークンの管理**を選択します。
3. 表示される**登録トークンの生成**ページで、次のトークン情報を入力します。
   - トークンの名前を入力します。
   - 有効期間を入力します。期間は14日以内である必要があります。トークンは指定された期間のみ有効です。
   - （オプション）トークンで登録されたVDAの電源管理のためにホスト接続を選択します。オプションには、このカタログのゾーン下のすべてのホスト接続が含まれます。
   - トークンの使用制限（1〜100の間）を入力します。
4. **生成**をクリックします。
5. 表示される**トークンが正常に生成されました**ウィンドウで、トークンをコピーして安全な場所に保存するか、**ダウンロード**をクリックして**ダウンロード**フォルダーにダウンロードします。

   トークンリストにトークンレコードが表示されます。

   トークンの生成(/en-us/citrix-virtual-apps-desktops/2407/media/token-based-enrollment.png)
6. VDAインストール管理者とトークンを共有します。

   マシンにVDAとトークンをインストールする方法の詳細については、VDAのインストールを参照してください。

トークンの管理

トークンを取り消し、VDA登録に使用できないようにするには、2つのオプションがあります。

- 取り消し：トークンを取り消しますが、ログ記録のためにリストに残します。
- 削除：トークンを取り消し、リストから削除します。

> **注:**
>
> 期限切れのトークンは14日後に自動的に削除されます。

WebSocket VDA登録ツールを使用してマシンをカタログに登録する

WebSocket VDA登録ツールは、VDAマシン向けのトークンベースの登録を容易にします。このツールは、登録トークンを使用してVDAをマシンカタログに追加することで、接続をWebSocket接続に変換するのに役立ちます。

> **注:**
>
> このツールは、どのマシンカタログにも登録されていないVDAマシンを登録するために設計されています。

登録ツールを実行するには、次の手順に従ってください。

1. VDAにログインします。
2. `C:\Program Files\Citrix\Virtual Desktop Agent\Web Socket Vda Enrollment Tool` 内にあるツール `EnrollMachine.exe` を見つけます。
3. 適切な入力パラメーターを指定してツールを実行します。例: `EnrollMachine.exe -websocket_token_string:xxxxxxxxx`

次の表は、登録ツールの入力パラメータについて説明しています。

パラメータ名	必須	説明	例
`-websocket_token_stdin`	はい	登録トークンを読み取ります。	`.\EnrollMachine.exe -websocket_token_stdin`

パラメータ名	必須	説明	例
`-websocket_token_string`		コマンドラインパラメータから登録トークンを直接読み取ります。	`.\EnrollMachine.exe -websocket_token_string:<token>`
`-websocket_token_file:[token-file-path]`		指定されたパスから登録トークンを読み取ります。	`.\EnrollMachine.exe -websocket_token_file:C:\token\test2.txt`
`log:[log-file-path]`	いいえ	登録ツールのログを表示します。	`.\EnrollMachine.exe log:[C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt]`
`-help`	いいえ	短いヘルプテキストを表示します。	`.\EnrollMachine.exe -help`

登録が成功すると、ツールおよびログに成功メッセージが表示されます。Web Studioにサインインして、VDAマシンがカタログに追加され、マシンのステータスが登録済みであることを確認してください。

トラブルシューティング

デフォルトでは、登録ツールのログは次の場所にあります。

`C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt`

ログに別のパスを指定した場合は、`log:[log-file-path]` を使用してログを取得できます。

次の表に、登録ツールが返すコードを示します。

コード	文字列	説明
0	成功	VDAがマシンカタログに正常に追加されました。
-1	無効な引数	登録トークンの入力パラメーターが無効です。
-2	ブローカーエージェントが見つかりません	ブローカーエージェントサービスが見つかりません。
-3	トークンが無効です	入力されたトークンが無効です。
-4	トークンに必要なクレームがありません	トークンに必要なクレーム（CustomerId、登録URIなど）がありません。
-5	内部エラー	一般的なエラーが発生しました。
-6	TimedOut	タスクがタイムアウトしました。
-7	FailedToDetermineMachineADJoinedStatus	マシンのAD参加ステータスを返すサービスが失敗しました。
-8	ADMachineFailedToFindSid	ADマシンのSIDを返すサービスが失敗しました。
-9	EnrollRequestFailed	HTTPエラーによりリクエストが失敗しました。
-10	EnrollResponseMissingRequiredFields	登録ツールの応答にパラメーター `VirtualSiteId` がありません。
-11	InsufficientPermission	タスクを実行するために必要な権限がありません。

コード	文字列	説明
-12	FailedToDetermineMachineAadJoinedStatus	マシンのAD参加ステータスを確認するサービスがエラーをスローしました。
-13	AadMachineFailedToFindDeviceId	システムによって追加された追加パラメーター `AAD device id` が空です。
-14	AadDeviceIdNotValid	システムによって追加された追加パラメーター `AAD device id` が有効なGUIDではありません。
-15	NoValidMacAddress	無効なMACアドレスです。
-16	FailedToGetComputerHostNameForVdaInstanceName	追加パラメーター `VdaInstanceName` を設定するためのコンピューターのホスト名の取得に失敗しました。
-17	VirtualDesktopAgentRegistryKeyFailedToOpen	Delivery Controller のリストを書き込むための VDA レジストリキーを開けませんでした。
-18	失敗したトークンが最大数に達しました	失敗したトークンが最大数に達しました。

PowerShell を使用する

このセクションでは、PowerShellを使用してカタログを管理する方法について詳しく説明します。

- カタログに関連付けられている警告とエラーを取得する
- イメージに説明を追加する
- OS ディスクをリセットする
- 既存のプロビジョニングスキームのネットワーク設定を変更する

- マシンカタログのバージョンを管理する(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-manage.html#manage-versions-of-a-machine-catalog)
- マシンプロファイルに基づかないマシンカタログを、マシンプロファイルに基づくマシンカタログに変換する(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-manage.html#convert-a-non-machine-profile-based-machine-catalog-to-machine-profile-based-machine-catalog)
- アクティブなコンピューターアカウントのID情報を修復する
- 既存のマシンカタログのキャッシュ構成を変更する
- ローカルファイル共有アクセスによるVDA更新のサポート(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-manage.html#vda-update-support-via-local-file-share-access)

カタログに関連付けられた警告とエラーを取得する

履歴エラーと警告を取得して、MCSマシンカタログの問題を理解し、それらの問題を修正できます。

PowerShellコマンドを使用して、次のことができます。

- エラーまたは警告のリストを取得する
- 警告の状態を**新規**から**確認済み**に変更する
- エラーまたは警告を削除する

PowerShellコマンドを実行するには:

1. PowerShell ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。

エラーと警告のリストを取得するには：

`Get-ProvOperationEvent` コマンドを実行します。

- パラメーターなしの場合: すべてのエラーと警告を取得します
- `LinkedObjectType` および `LinkedObjectUid` パラメーターを使用する場合: 特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告を取得します
- `EventId` パラメーターを使用する場合: このイベントIDに一致する特定のエラーまたは警告を取得します

- `Filter` パラメーターを使用する場合: カスタマイズされたフィルターでエラーまたは警告を取得します

エラーまたは警告の状態を **New** から **Acknowledged** に変更するには：

`Confirm-ProvOperationEvent` コマンドを実行します。

- `EventId` パラメーターを使用する場合: このイベントIDに一致する特定のエラーまたは警告の状態を設定します。特定のイベントIDの `EventId` は、`Get-ProvOperationEvent` コマンドの出力として取得できます。
- `LinkedObjectType` および `LinkedObjectUid` パラメーターを使用する場合: 特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告の状態を設定します
- `All` パラメーターを使用する場合: すべてのエラーと警告の状態を**確認済み**に設定します

エラーまたは警告を削除するには：

`Remove-ProvOperationEvent` コマンドを実行します。

- `EventId` パラメーターを使用する場合: このイベントIDに一致する特定のエラーまたは警告を削除します。特定のイベントIDの `EventId` は、`Get-ProvOperationEvent` コマンドの出力として取得できます。
- `LinkedObjectType` および `LinkedObjectUid` パラメーターを使用する場合: 特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告を削除します
- `All` パラメーターを使用する場合: すべてのエラーと警告を削除します

詳しくは、Citrix PowerShell SDKを参照してください。

ハイパーバイザーアクセスなしでマシンを削除する

VMまたはプロビジョニングスキームを削除する場合、MCSはVMから、場合によってはベースディスクからもタグを削除する必要があります。これにより、削除オプションに含まれるリソースがMCSによって追跡または識別されなくなります。しかし、これらのリソースの一部はハイパーバイザーを介してのみアクセス可能です。ハイパーバイザーアクセスがない場合でも、`Remove-ProvVM` PowerShellの `PurgeDBOnly` オプションを使用して、VM、ベースディスク、ACG内のイメージなどのVMリソースオブジェクトをデータベースから削除します。

このオプションは以下で有効になります。

- サポートされているすべてのハイパーバイザー
- 永続的および非永続的VM

制限事項

コマンド-PurgeDBOnlyと-ForgetVMを同時に使用することはできません。

PurgeDBOnly コマンドを使用する

PowerShell コマンド `Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -ForgetVM` を実行すると、以下のシナリオで削除操作が失敗する可能性があります。

- ホスト接続がメンテナンスモードになっている
- 無効な資格情報
- 認証失敗
- 許可されていない操作
- ハイパーバイザーに到達できません

> **注：**
>
> Remove-provVM -ForgetVMは永続VMのみを対象とします。リスト内のいずれかのVMが非永続である場合、操作は失敗します。

> ハイパーバイザーに到達できないために操作が失敗した場合、次のプロンプトが表示されます。

`Try to use -PurgeDBOnly option to clean DDC database.`.

MCSデータベースからVMの参照を削除するには、`Remove-ProvVM` PowerShellコマンドで`-PurgeDBOnly`オプションを使用します。例：

```
Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -PurgeDBOnly
```

イメージに説明を追加

マシンカタログのイメージ更新に関連する変更について、情報提供の記述を追加できます。この機能を使用して、カタログの作成時、またはカタログの既存のマスターイメージを更新する際に説明を追加します。カタログ内の各マスターイメージの情報を表示することもできます。イメージの説明を追加または表示するには、次のコマンドを使用します。

- マスターイメージを使用してマシンカタログを作成する際にメモを追加するには、`NewProvScheme`コマンドでパラメーター`MasterImageNote`を使用します。例：

```
C:\PS>New-ProvScheme -ProvisioningSchemeName <name> -HostingUnitName
<name> -IdentityPoolName <name> -MasterImageVM

XDHyp:\HostingUnits\<hosting unit name>\<vm name>.vm\Base.snapshot
-MasterImageNote "Note"
```

- マシンカタログに関連付けられているマスターイメージを更新するには、`Publish-ProvMasterVMImage`コマンドでパラメーター`MasterImageNote`を使用します。例：

```
C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName <name>
-MasterImageVM XDHyp:\HostingUnits\<hosting unit name>\<vm
name>.vm\base.snapshot -MasterImageNote "Note"
```

- 各イメージの情報を表示するには、Get-ProvSchemeMasterVMImageHistoryコマンドを使用します。例：

```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
MyScheme -Showall
```

ロールバックの進行状況を追跡するには、**マシンカタログ**でカタログを見つけ、インラインの進行状況バーと段階的な進行状況グラフを表示します。

次のような特定のシナリオでは、ロールバックできません。(**マスターイメージのロールバック**オプションは表示されません)。

- ロールバックする権限がありません。
- カタログがMCSを使用して作成されていません。
- カタログはOSディスクのイメージを使用して作成されました。
- カタログの作成に使用されたスナップショットが破損しています。
- カタログ内のマシンに対するユーザーの変更が保持されません。
- カタログ内のマシンが実行中です。

OSディスクをリセットする

MCSで作成されたマシンカタログ内の永続VMのOSディスクをリセットするには、PowerShellコマンド`Reset-ProvVMDisk`を使用します。現在、この機能はAWS、Azure、XenServer、Google Cloud、SCVMM、VMwareの仮想化環境に適用できます。

PowerShellコマンドを正常に実行するには、以下を確認してください。

- ターゲットVMが永続MCSカタログに存在すること。
- MCSマシンカタログが正常に機能していること。
- これは、プロビジョニングスキームとホストが存在し、プロビジョニングスキームに正しいエントリがあることを意味します。
- ハイパーバイザーがメンテナンスモードではないこと。
- ターゲットVMが電源オフでメンテナンスモードであること。

OSディスクをリセットするには、次の手順を実行します。

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、**asnp citrix*** を実行します。
3. PowerShellコマンド `Reset-ProvVMDisk` を次のいずれかの方法で実行します。

   - VMのリストをコンマ区切りリストとして指定し、各VMでリセットを実行します。

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc","def")
     -OS
     ```

   - VMのリストを `Get-ProvVM` コマンドからの出力として指定し、各VMでリセットを実行します。

     ```
     (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk "abc"
     -OS
     ```

   - 名前で単一のVMを指定します。

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
     ```

   - `Get-ProvVM` コマンドによって返される各VMに対して個別のリセットタスクを作成します。各タスクがハイパーバイザーの機能チェック、各VMの接続チェックなど、同じ冗長なチェックを実行するため、これは効率的ではありません。

     ```
     Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk
     -ProvisioningSchemeName "xxx" -OS
     ```

4. リセットされるVMのリストと、回復不能な操作であるという警告メッセージが表示された確認プロンプトが表示されます。回答を入力せずに **Enter** キーを押すと、それ以上のアクションは実行されません。

   > **注:**
   >
   > リセットプロセスが完了するまで、VMをメンテナンスモードから解除したり、電源をオンにしたりしないでください。

   > PowerShellコマンド `-WhatIf` を実行して、実行されるアクションを出力し、アクションを実行せずに終了できます。

   次のいずれかの方法を使用して、確認プロンプトをバイパスすることもできます。

   - `-Force` パラメーターを指定します。

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
     -Force
     ```

   - `-Confirm:$false` パラメーターを指定します。

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
     -Confirm:$false
     ```

   - `Reset-ProvVMDisk` を実行する前に、 `$ConfirmPreference` を**None**に変更します。

     ```
     PS C:\Windows\system32> $ConfirmPreference='None'

     PS C:\Windows\system32> $ConfirmPreference

     None

     PS C:\Windows\system32> Reset-ProvVMDisk -ProvisioningSchemeName
     "xxx" -VMName "abc" -OS
     ```

5. `Reset-ProvVMDisk` コマンドによって返されたタスクのステータスを取得するには、 `Get-ProvTask` を実行します。

既存のプロビジョニングスキームのネットワーク設定を変更する

既存のプロビジョニングスキームのネットワーク設定を変更して、新しいVMが新しいサブネットワーク上に作成されるようにすることができます。ネットワーク設定を変更するには、`Set-ProvScheme`コマンドでパラメータ`-NetworkMapping`を使用します。

> **注記：**
>
> この機能は、Citrix Virtual Apps and Desktops 2203 LTSR CU3以降のバージョンでサポートされています。

> 既存のプロビジョニングスキームのネットワーク設定を変更するには、次の手順を実行します。

1. PowerShellウィンドウで、PowerShellモジュールをロードするために、コマンド`asnp citrix*`を実行します。
2. `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps`を実行して、変更したいネットワークパスに移動します。
3. 新しいネットワーク設定に変数を割り当てます。例:

   ```
   $NewNetworkMap = @{"0"= "XDHYP:\HostingUnits\MyNetworks\Network 0.network"}
   ```

4. `Set-ProvScheme -ProvisioningSchemeName "name" -NetworkMapping $NewNetworkMap`を実行します。
5. `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps`を実行して、既存のプロビジョニングスキームの新しいネットワーク設定を確認します。

マシンカタログのバージョンを管理する

MCSマシンカタログが`Set-ProvScheme`コマンドで更新されると、現在の構成がバージョンとして保存されます。その後、PowerShellコマンドを使用して、マシンカタログのさまざまなバージョンを管理できます。次のことができます。

- マシンカタログのバージョンリストを表示する
- 以前のバージョンを使用してマシンカタログを更新する
- そのマシンカタログのVMによって使用されていない場合、バージョンを手動で削除する

- マシンカタログによって保持される最大バージョン数を変更する（デフォルトは99）

マシンカタログのバージョンには、以下の情報が含まれます。

- VMCpuCount
- VMMemoryMB
- CustomProperties
- ServiceOffering
- MachineProfile
- NetworkMapping
- SecurityGroup

マシンカタログのさまざまなバージョンを管理するには、次のコマンド（例として提供）を実行します。

- マシンカタログのさまざまなバージョンの構成詳細を表示するには：

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
```

- マシンカタログの特定のバージョンの構成詳細を表示するには：

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version 2
```

- マシンカタログに関連付けられているバージョンの総数を表示するには：

```
(Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count
```

- 以前のバージョンを使用してマシンカタログを更新するには：

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
```

- そのマシンカタログのVMで使用されていないバージョンを手動で削除するには：

```
Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version
3
```

- マシンカタログが保持する最大バージョン数を設定するには（デフォルトは99）。この設定はすべてのカタログに適用されます。たとえば、この場合、すべてのMCSプロビジョニング済みカタログに対して最大15バージョンが保持されます。

```
Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -Value
15
```

バージョン数が最大バージョン数に達した場合、マシンカタログ内のいずれかのVMで古いバージョンが使用されていると、新しいバージョンを作成できません。その場合は、次のいずれかを実行してください。

- マシンカタログによって保持される最大バージョン数の制限を増やします。
- 古いバージョンを使用している一部のVMを更新して、それらの古いバージョンがどのVMからも参照されなくなり、削除できるようにします。

マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換する

VM、テンプレート仕様（Azureの場合）、または起動テンプレート（AWSの場合）をマシンプロファイルの入力として使用して、マシンプロファイルに基づかないマシンカタログをマシンプロファイルに基づくマシンカタログに変換できます。カタログに追加された新しいVMは、明示的なカスタムプロパティによって上書きされない限り、マシンプロファイルからプロパティ値を取得します。

> **注:**
>
> 既存のマシンプロファイルベースのマシンカタログを、マシンプロファイルベースではないマシンカタログに変更することはできません。

> これを行うには：

1. 永続的または非永続的なマシンカタログを、VMを使用して、マシンプロファイルなしで作成します。
2. **PowerShell**ウィンドウを開きます。
3. `Set-ProvScheme`コマンドを実行して、マシンプロファイルからのプロパティ値を、マシンカタログに追加された新しいVMに適用します。例：
    - Azureの場合:

```
Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile XDHyp:
\HostingUnits\<HostingUnitName>\machineprofile.folder\<ResourceGroup
Name>\<TemplateSpecName>\<VersionName>
```

- AWSの場合:

```
Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile "XDHyp:
\HostingUnits\<hosting-unit>\<launch-
template>.launchtemplate\<launch-template-
version>.launchtemplateversion"
```

アクティブなコンピューターアカウントのID情報を修復する

ID関連の問題があるアクティブなコンピューターアカウントのID情報をリセットできます。マシンパスワードと信頼キーのみをリセットするか、IDディスクのすべての構成をリセットするかを選択できます。この実装は、永続および非永続の両方のMCSマシンカタログに適用できます。

注記:

現在、この機能はAWS、GCP、Azure、XenServer、およびVMware仮想化環境でサポートされています。

条件

IDディスクを正常にリセットするには、以下を確認してください。

- VMをシャットダウンし、メンテナンスモードに設定します
- PowerShellコマンドにパラメーター -OSを含めないでください

IDディスクのリセット

IDディスクをリセットするには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. ID情報をリセットします。
    - マシンパスワードと信頼キーのみをリセットするには、次のコマンドを実行します。

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1
-PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
-Target IdentityInfo
```

コマンドで使用されるパラメーターの説明は次のとおりです。

- IdentityAccountName: 修復する必要があるIDアカウントの名前。
- PrivilegedUserName: IDプロバイダー（ADまたはAzureAD）に対する書き込み権限を持つユーザーアカウント。
- PrivilegedUserPassword: PrivilegedUserName のパスワード。
- Target: 修復アクションのターゲット。アカウントのパスワード/信頼キーを修復するための IdentityInfo、および Hybrid AzureAD に参加しているマシンIDのユーザー証明書属性を修復するための UserCertificate を指定できます。

- IDディスクのすべての構成をリセットするには、次のコマンドを次の順序で実行します。

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1
-PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
-Target IdentityInfo
```

```
Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>  -
Identity
```

- IDディスクを完全に再作成するには:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name>
-Identity -Recreate
```

4. アクションを確定するには「**y**」と入力します。`-Force` パラメーターを使用して確認プロンプトをスキップすることもできます。例:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name>
-Identity -Force
```

5. 更新されたIDディスク設定を確認するには、`Get-ProvVM -ProvisioningSchemeName <name -VMName <name>` を実行します。IDディスクの属性（例: `IdentityDiskId`）は更新されている必要があります。`StorageId` と `IdentityDiskIndex` は変更されていてはなりません。

既存のマシンカタログのキャッシュ構成を変更する

MCSIOを有効にして非永続カタログを作成した後、Set-ProvSchemeコマンドを使用して以下のパラメータを変更できます。

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

この機能は現在、以下に適用されます。

- GCPおよびMicrosoft Azure環境、および
- MCSIOが有効な非永続カタログ

要件

キャッシュ構成を変更するための要件は次のとおりです。

- VDAを最新バージョン（2308以降）に更新します。
- 既存のマシンカタログに対してパラメーター `UseWriteBackCache` を有効にします。`UseWriteBackCache` が有効なマシンカタログを作成するには、`New-ProvScheme` を使用します。例：

```
New-ProvScheme -ProvisioningSchemeName $CatalogName -HostingUnitUid
$HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

-MasterImageVM $MasterImage `

-ServiceOffering $ServiceOffering `

-NetworkMap $NetworkMap `

-SecurityGroup $SecurityGroup `

-UseWriteBackCache -WriteBackCacheDiskSize 8
```

キャッシュ構成を変更する

Set-ProvSchemeコマンドを実行します。例:

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.ProvisioningSchemeName
-WriteBackCacheDisk32 -WriteBackCacheMemorySize 128
```

注:

- 少なくとも 1 GB のキャッシュディスクストレージが必要なため、`WriteBackCacheDiskSize` の値はゼロより大きくする必要があります。
- `WriteBackCacheMemorySize` の値は、マシンカタログのメモリサイズよりも小さくする必要があります。
- これらの変更は、変更後にカタログに追加された新しい VM にのみ影響します。既存の VM はこれらの変更の影響を受けません。

ローカルファイル共有アクセスによるVDAアップデートのサポート

PowerShellコマンドレットを介してVDAインストーラーの場所を指定することで、各VDAがCitrix Managed Azure CDNから新しいVDAインストーラーを取得できるようにするためのネットワークルールを提供する手間を省くことができます。

PowerShellコマンドレット

ローカルファイル共有からインストーラーを使用できるようにする、**New-VusCatalogSchedule** および **New-VusMachineUpgrade** コマンドレットに2つの新しいオプションパラメーターが追加されました

- **VdaWorkstationPackageUri** - ワークステーションOS VDAインストーラーへのUNCパスを指定します。
- **VdaServerPackageUri** - サーバーOS VDAインストーラーへのUNCパスを指定します。

前提条件

- VDA 2311に付属するVUSエージェントインストーラー
- VDAアップグレードエージェントをバージョン7.40.0.35以降にアップグレード（VDAインストーラーバージョン2311以降を使用）
- Virtual Apps and Desktops Remote PowerShell SDK バージョン 7.40 以降 (Jan 10, 2024 以降にリリース)

ファイル共有権限の設定方法

VDAインストーラーパッケージを含むネットワーク共有は、Local System (NT AUTHORITY\SYSTEM プリンシパル) として実行されるVDAアップグレードエージェントサービスに対して読み取りアクセス権を持っている必要があります。

- **ドメイン参加済みファイル共有権限**

  VDAマシンがドメインに参加している場合、**ローカルシステム**アカウント（VUAはローカルシステムとして実行されます）は、ネットワーク共有にアクセスする際にコンピューターの資格情報を使用します。

  最小特権の権限は、ドメインコンピューターに**読み取り**アクセス権を付与することで設定できます。

  a. ファイルを共有したいネットワーク上のユーザーを選択します。
  b. **詳細な共有設定**をクリックし、**ファイルとプリンターの共有**をオンにします。

- **ドメイン非参加ファイル共有権限**

  VDA マシンがドメインに参加していない場合、**ローカルシステム** アカウント (VUA はローカルシステムとして実行されます) は、ネットワーク共有にアクセスするときに **ANONYMOUS LOGON** を使用します。

  a. 共有フォルダーを選択します。
  b. パスワード保護を無効にします。
     a. フォルダーの**プロパティ**に移動します。
     b. 「**ネットワークと共有センター**」を選択します。
     c. 「**パスワード保護共有**」をオフにします。
  c. 共有アクセス許可を付与するには、「**詳細な共有設定**」をクリックします。
     a. 「**アクセス許可**」を選択します。
     b. **ANONYMOUS LOGON**に**読み取り**共有アクセス許可を付与します。
  d. フォルダーのアクセス許可を付与するには、「**セキュリティ**タブ」を選択します。
     a. 共有フォルダーにアクセス許可を追加するには、「**編集**」をクリックします。
     b. **ANONYMOUS LOGON**にフォルダーのアクセス許可を付与するには、共有フォルダーを選択します。

e. **ファイルとプリンターの共有**を有効にするには、「**詳細設定**」をクリックします。

f. 共有フォルダー名を**ネットワークアクセスセキュリティポリシー**に追加します。

> **注:**
>
> 変更をすぐに有効にするには、マシンを再起動します。

ローカルファイル共有からのVDAアップデート

1. VDAインストーラーをダウンロードし、共有ファイルに配置します。

> **注:**
>
> Virtual Upgrade Service を使用すると、Current Release トラックまたは LTSR トラックのいずれかを選択できます。
>
> **例:** マシンカタログが Current Release (2311) に設定されており、VDA バージョンが 2305 の場合、VDA をバージョン 2311 にアップグレードする必要があります。

a. 弊社のWebサイト の **ダウンロード** ページに移動します。

b. 製品として **Citrix Virtual Apps and Desktops** を選択します。

c. 「**Citrix Virtual Apps and Desktops 7 2311, 全エディション**」を選択します。

d. **製品ISOに含まれるが個別にパッケージ化されているコンポーネント** の展開可能な項目からVDAインストーラーを選択します。

2. カタログの種類に基づいて、関連するVDAインストーラーを選択します。

- カタログの種類が **マルチセッション** の場合は、**マルチセッションOS VDAインストーラー** をダウンロードします。
- カタログの種類が **シングルセッション** の場合は、**シングルセッションOS VDAインストーラー** をダウンロードします。
- カタログの種類が **Remote PC Access** の場合は、**シングルセッションOSコアサービスVDAインストーラー** をダウンロードします。

> **注:**

ファイル共有インストーラーのバージョンは、VUSによってクラウドに公開された最新のインストーラーバージョンと**正確に**一致している必要があります。

トラブルシューティング

- 「電源状態不明」のステータスのマシンについては、ガイダンスとして CTX131267 を参照してください。
- 不明な電源状態を継続的に表示するVMを修正するには、不明な電源状態を継続的に表示するVMを修正する方法 を参照してください。

次のステップ

特定のクラウドサービスカタログの管理については、以下を参照してください。

- AWSカタログの管理
- XenServerカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-manage/manage-machine-catalog-citrix-hypervisor.html)
- Google Cloud Platformカタログの管理
- Microsoft Azureカタログの管理
- Microsoft System Center Virtual Machine Manager カタログを管理する
- VMwareカタログの管理

AWSカタログの管理

(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-manage.html)では、マシンカタログを管理するウィザードについて説明します。以下の情報は、AWSクラウド環境に固有の詳細を扱っています。

注:

AWSカタログを管理する前に、AWSカタログの作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create/create-machine-catalog-aws.html)を参照してください。

タグを削除する

カタログまたはVMを作成すると、MCSによって作成されたタグが以下のリソースに作成されます。

- 仮想マシン
- ルートディスクボリューム
- 識別ディスクボリューム
- NIC
- ルートディスクイメージ (AMI)
- 起動テンプレート
- AMIまたはルートディスクのスナップショット

Citrix®データベースからVMとマシンカタログを削除し、MCSによって作成されたタグを削除できます。以下を使用できます。

- マシンカタログから単一のVMまたはVMのリストからVMとMCSによって作成されたタグを削除するには、`Remove-ProvVM`と`ForgetVM`パラメーターを使用します。
- `Remove-ProvScheme` と `ForgetVM` パラメーターを使用して、Citrix データベースからマシンカタログを削除し、マシンカタログからリソースを削除します。

この機能は、永続VMにのみ適用されます。

これを行うには：

1. **PowerShell** ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。
3. VMを削除する前に、VMのロックを解除します。例：

   ```
   Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
   ```

4. リソースからVM、マシンカタログ、およびMCSによって作成されたタグを削除するには、次のいずれかのコマンドを実行します。

   - Citrix データベースからVMを削除し、VMからタグを削除するには、`ForgetVM` を指定して `Remove-ProvVM` を実行します。例：

```
Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"
-ForgetVM
```

- Citrix データベースからマシンカタログを削除し、マシンカタログからリソースを削除するには、`Remove-ProvScheme` を実行します。例：

```
Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -ForgetVM
```

5. VMがDelivery Controller™から削除されていることを確認しますが、ハイパーバイザーからは削除されていません。

   a. `Get-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"` を実行します。これは何も返さないはずです。

   b. AWS EC2 コンソールに移動します。VMは表示されますが、タグは削除されています。以下のリソースからタグが削除されます：

      - 仮想マシン
      - ルートディスクボリューム
      - 識別ディスクボリューム
      - NIC

6. マシンカタログを削除する場合は、カタログがDelivery Controllerから削除されていることを確認してください。

   a. `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`を実行します。これはエラーを返すはずです。

   b. AWS EC2コンソールで、以下のリソースが削除されていることを確認してください。

      - ルートディスクイメージ (AMI)
      - 起動テンプレート
      - AMIまたはルートディスクのスナップショット

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
IDディスク	"名前": "VMName_IdentityDisk"
	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
イメージ	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
NIC	"説明": "XD NIC"
	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OSディスク	"名前": "VMName_rootDisk"
	"Xd設定": "XdProvisioned=True"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "Citrix リソース": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] 「CitrixOperationalResource」：「」
PrepVM	"Name": "準備 - カタログ名 - xxxxxxxxxx"
	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "Citrix リソース": ""

リソース名	タグ
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
公開済みスナップショット	"XdConfig": "XdProvisioned=true"
	ボリュームワーカーAMIのスナップショットでない場合、"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
テンプレート	[when AwsCaptureInstanceProperties = true] "XdConfig": "XdProvisioned=true"
	[when AwsCaptureInstanceProperties = true] "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "CitrixResource": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
カタログ内のVM	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "CitrixResource": ""
	[when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:id":"lt-xxxx"
	[when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:version": "n"
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""

リソース名	タグ
ボリュームワーカー AMI	"XdConfig": "XdProvisioned=true"
ボリュームワーカー ブートストラッパー	"名前": "XenDesktop® Temp"
	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixVolumeWorkerBootstrapper": ""
ボリュームワーカー インスタンス	"名前": "Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx"
	"Xd設定": "XdProvisioned=true"

詳細情報

- 接続とリソースの作成および管理
- AWSへの接続
- マシンカタログの作成
- AWS カタログを作成する
- マシンカタログの管理

XenServer®カタログを管理する

マシンカタログを管理するウィザードについては、マシンカタログの管理で説明しています。以下の情報は、XenServer仮想化環境に固有の詳細を扱っています。

> **注:**
>
> XenServerカタログを管理する前に、XenServerカタログの作成を完了する必要があります。XenServerカタログの作成を参照してください。

MCSによって作成されたリソースを特定する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
公開されたベースディスクと、各ネットワークまたはローカルストレージ上のそのコピー	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
IDディスク	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OSディスク	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
準備用VM	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
カタログ内のVM	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
WBCディスク	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

詳細情報

- 接続とリソースの作成および管理
- XenServerへの接続
- マシンカタログの作成
- XenServerカタログを作成する
- マシンカタログの管理

Google Cloud Platformカタログを管理する

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Google Cloud環境に固有の詳細を扱います。

> **注:**
>
> Google Cloud Platformカタログを管理する前に、Google Cloud Platformカタログの作成を完了する必要があります。Google Cloud Platformカタログの作成を参照してください。

マシンカタログの管理

カタログにマシンを追加したり、マシンを更新したり、更新をロールバックしたりするには、「マシンカタログの管理」を参照してください。

電源管理

Citrix DaaS™では、Google Cloudマシンの電源管理が可能です。左ペインの**検索**ノードを使用して、電源管理するマシンを見つけます。次の電源操作が利用可能です。

- 削除
- 起動
- 再起動
- 強制再起動
- シャットダウン
- 強制シャットダウン
- デリバリーグループに追加
- タグの管理
- メンテナンスモードをオンにする

Autoscale を使用して Google Cloud マシンを電源管理することもできます。そのためには、Google Cloud マシンをデリバリーグループに追加し、そのデリバリーグループで Autoscale を有効にします。Autoscale の詳細については、Autoscale を参照してください。

PowerShellを使用してプロビジョニングされたマシンを更新する

`Set-ProvScheme` コマンドはプロビジョニングスキームを変更します。ただし、既存のマシンには影響しません。PowerShell コマンド `Set-ProvVMUpdateTimeWindow` を使用すると、現在のプロビジョニングスキームを既存の永続マシンまたは非永続マシン、あるいはマシンセットに適用できるようになりました。現在、GCP では、この機能でサポートされているプロパティの更新はマシンプロファイルです。

更新できるもの:

- 単一のVM
- 特定のVMのリスト、またはプロビジョニングスキームIDに関連付けられている既存のすべてのVM
- プロビジョニングスキーム名に関連付けられた特定のVMのリスト、またはすべての既存のVM

既存のVMを更新するには：

1. 既存のマシンの構成を確認します。例えば、,

```
Get-ProvScheme | select ProvisioningSchemeName,
ProvisioningSchemeVersion
```

2. プロビジョニングスキームを更新します。例えば、,

```
`Set-ProvScheme –ProvisioningSchemeName "my-catalog" –MachineProfile
"XDHyp:\HostingUnits\<hosting-unit>\machineprofileinstance.vm"
```

3. VM の現在のプロパティが現在のプロビジョニングスキームと一致するか、および VM に保留中の更新アクションがあるかを確認します。例:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

   特定のバージョンのマシンを見つけることもできます。例:

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
ProvisioningSchemeVersion
```

4. 既存のマシンを更新します。

   - すべての既存のマシンを更新するには：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

   - 特定のマシンのリストを更新するには：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

   - `Get-ProvVM`の出力に基づいてマシンを更新するには：

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
-DurationInMinutes -1
```

5. 更新がスケジュールされているマシンを見つけます。例:

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

6. マシンを再起動します。次回の電源投入時に、プロパティの変更が既存のマシンに適用されます。次のコマンドを使用して、更新されたステータスを確認できます。

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

既存のカタログのディスク関連のカスタムプロパティを変更する

既存のカタログおよびカタログの既存のVMの、以下のディスク関連のカスタムプロパティを変更できます。

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

注記:

- `StorageType` プロパティはOSディスク用です
- `PersistOsDisk` プロパティは、ライトバックキャッシュが有効な非永続カタログに対してのみ設定できます

この実装により、カタログ作成後でもディスクごとに異なるストレージタイプを選択できるようになり、異なるストレージタイプに関連する価格のバランスを取ることができます。

これを行うには、PowerShellコマンド `Set-ProvScheme` と `Set-ProvVMUpdateTimeWindow` を使用します。

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*` を実行します。
3. カスタムプロパティを取得するには、`Get-ProvVM -VMName <VM name>` を実行します。
4. カスタムプロパティ文字列を変更します。
   a. カスタムプロパティをメモ帳にコピーし、カスタムプロパティを変更します。
   b. **PowerShell** ウィンドウで、メモ帳から変更したカスタムプロパティを貼り付け、変更したカスタムプロパティに変数を割り当てます。例：

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com/2014/xd/
machinecreation xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="CatalogZones" Value="" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" /
>

<Property xsi:type="StringProperty" Name="PersistOSDisk"
Value="true" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="pd-standard" />

<Property xsi:type="StringProperty" Name="StorageType" Value="pd-
standard" />

</CustomProperties>'
```

5. 既存のカタログを更新します。例：

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName>
-CustomProperties $cp
```

6. 既存のVMを更新します。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

7. VM を再起動します。次回の電源投入時に、カスタムプロパティの変更が既存の VM に適用されます。

偶発的なマシン削除からの保護

Citrix DaaSでは、Google Cloud上のMCSリソースを保護して、偶発的な削除を防ぐことができます。`deletionProtection` フラグをTRUEに設定して、プロビジョニングされたVMを構成します。

デフォルトでは、MCSまたはGoogle Cloudプラグインを介してプロビジョニングされたVMは、InstanceProtectionが有効な状態で作成されます。この実装は、永続カタログと非永続カタログの両方に適用されます。非永続カタログは、インスタンスがテンプレートから再作成されるときに更新されます。既存の永続マシンについては、Google Cloudコンソールでフラグを設定できます。フラグの設定の詳細については、Google Documentation site を参照してください。永続カタログに追加された新しいマシンは、`deletionProtection` が有効な状態で作成されます。

`deletionProtection` フラグを設定したVMインスタンスを削除しようとすると、リクエストは失敗します。ただし、`compute.instances.setDeletionProtection` 権限が付与されているか、IAMの**Compute Admin**ロールが割り当てられている場合は、フラグをリセットしてリソースの削除を許可できます。

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
IDディスク	"CitrixResource": "内部"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
イメージ	"CitrixResource": "内部"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OSディスク	"CitrixResource": "内部"

リソース名	タグ
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
PrepVM	"CitrixResource": "内部"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
公開済みスナップショット	"CitrixResource": "内部"
ストレージバケット	"Citrixリソース": "内部"
テンプレート	"CitrixResource": "内部"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
カタログ内のVM	"CitrixResource": "内部"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"。プラグインは、MCSでプロビジョニングされたVMにもこのラベル「"citrix-provisioning-scheme-id": "provSchemeId"」を追加します。このラベルを使用して、GCPコンソールでカタログ別にフィルタリングできます。
WBCディスク	"CitrixResource": "内部"
	Citrix プロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

注:

MCSによって作成されたリソースとして識別するために**CitrixResource**タグが追加されている場合、VMはCitrixインベントリに表示されません。タグを削除または名前変更することで、表示させることができます。

詳細情報

- 接続とリソースの作成および管理
- Google Cloud環境への接続
- マシンカタログの作成
- Google Cloud Platform カタログを作成する
- マシンカタログの管理

HPE Moonshot カタログの管理

マシンカタログの管理(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-manage.html)では、マシンカタログを管理するウィザードについて説明します。以下の情報は、HPE Moonshotカタログに固有の詳細を扱っています。

> **注:**
>
> HPE Moonshotカタログを管理する前に、HPE Moonshotカタログの作成を完了する必要があります。

電源管理

Citrix Virtual Apps and Desktops™では、HPE Moonshotマシンの電源管理を行うことができます。電源管理を行うマシンを見つけるには、ナビゲーションペインの**検索**ノードを使用します。以下の電源操作が利用可能です。

- 起動
- シャットダウン
- 強制シャットダウン
- 再起動
- リセット

> **注:**
>
> **一時停止**および**再開**の電源操作はサポートされていません。

詳細情報

- 接続とリソースの作成および管理(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections.html)
- HPE Moonshotへの接続(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections/connection-hpe-moonshot.html)
- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html)
- HPE Moonshotマシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create/create-machine-catalog-hpe-moonshot.html)
- マシンカタログの管理(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-manage.html)

Microsoft Azureカタログを管理する

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

(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-manage.html)では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Microsoft Azure Resource Managerクラウド環境に固有の詳細を扱います。

> **注：**
>
> Microsoft Azureカタログを管理する前に、Microsoft Azureカタログの作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html)を参照してください。

VMシャットダウン時にストレージタイプを下位層に変更する

VMをシャットダウンするときに、管理ディスクのストレージタイプを下位層に切り替えることで、ストレージコストを節約できます。これを行うには、`StorageTypeAtShutdown`カスタムプロパティを使用します。

VMをシャットダウンすると、ディスクのストレージタイプは下位層（`StorageTypeAtShutdown`カスタムプロパティで指定）に変更されます。VMの電源をオンにすると、ストレージタイプは元の状態（`StorageType`カスタムプロパティまたは`WBCDiskStorageType`カスタムプロパティで指定）に戻ります。

> **重要:**
>
> ディスクは、VMが少なくとも一度電源オンになるまで存在しません。したがって、VMを最初に電源オンにしたときにストレージタイプを変更することはできません。

要件

- 管理ディスクに適用されます。これは、カスタムプロパティ`UseManagedDisks`をtrueに設定することを意味します。
- 永続OSディスクを持つ永続および非永続カタログに適用されます。これは、カスタムプロパティ`persistOsDisk`をtrueに設定することを意味します。
- 永続WBCディスクを持つ非永続カタログに適用されます。これは、カスタムプロパティ`persistWBC`をtrueに設定することを意味します。

制限

- Microsoftによると、ディスクの種類は1日に2回しか変更できません。Microsoft ドキュメントを参照してください。Citrixによると、VMの開始または割り当て解除アクションがあるたびに`StorageType`の更新が行われます。したがって、VMあたりの電源アクションの数を1日2回に制限してください。たとえば、午前中にVMを開始するための電源アクションを1回、夕方にVMを割り当て解除するための電源アクションを1回実行します。

ストレージタイプを下位層に変更する

手順に進む前に、(#requirements)と(#restriction)を参照してください。

1. カスタムプロパティ`StorageTypeAtShutdown`を追加し、値をStandard_LRS (HDD)に設定して、`New-ProvScheme`を使用してカタログを作成します。PowerShellを使用してカタログを

作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

> **注:**
>
> `StorageTypeAtShutdown`が空またはStandard_LRS (HDD)以外の値を持つ場合、操作は失敗します。

永続カタログ作成時のカスタムプロパティ設定例：

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

非永続カタログ作成時のカスタムプロパティ設定例：

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

注:

マシンプロファイルを使用する場合、カスタムプロパティは`MachineProfile`で定義されたプロパティよりも優先されます。

2. VMをシャットダウンし、AzureポータルでVMのストレージタイプを確認します。ディスクのストレージタイプは、`StorageTypeAtShutdown`カスタムプロパティで指定された下位層に変更されます。

3. VMを起動します。ディスクのストレージタイプは、以下に記載されているストレージタイプに戻ります。

   - OSディスクの`StorageType`カスタムプロパティ
   - `CustomProperties`で指定した場合にのみ、WBCディスクの`WBCDiskStorageType`カスタムプロパティ。それ以外の場合は、`StorageType`に記載されているストレージタイプに戻ります。

既存のカタログに`StorageTypeAtShutdown`を適用する

手順に進む前に、要件と制限を参照してください。

既存のカタログにVMを追加するには、`Set-ProvScheme`を使用します。この機能は、`Set-ProvScheme`の実行後に新しく追加されたVMに適用されます。既存のマシンには影響しません。

既存のカタログにVMを追加する際にカスタムプロパティを設定する例:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />
```

```
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'



$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName



Set-ProvScheme -ProvisioningSchemeName $ProvScheme.ProvisioningSchemeName
-CustomProperties $customProperties
```

既存のVMのストレージタイプをシャットダウン時に下位層に変更する

手順に進む前に、要件と制限を参照してください。

VMのシャットダウン時に既存のVMのストレージタイプを下位層に変更することで、ストレージコストを節約できます。これを行うには、`StorageTypeAtShutdown`カスタムプロパティを使用します。

カタログ内の既存のマシンのストレージタイプを、VMシャットダウン時に下位層に変更するには:

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. `Get-Provscheme -ProvisioningSchemeName $CatalogName`を実行します。
4. カスタムプロパティ文字列を変更します。

   ```
   $customProperties = '<CustomProperties xmlns="http://
   schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
   www.w3.org/2001/XMLSchema-instance">

   <Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
   Value="Standard_LRS" />

   </CustomProperties>'
   ```

5. 既存のカタログのプロビジョニングスキームを更新します。この更新は、`Set-ProvScheme`の実行後に新しく追加されたVMに適用されます。

```
Set-ProvScheme -ProvisioningSchemeName $CatalogName -CustomProperties
$customProperties
```

6. 既存のVMを更新して`StorageTypeAtShutdown`を有効にします。

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName $CatalogName
-StartsNow -DurationInMinutes -1
```

7. 次回マシンを起動すると、マシンの`StorageTypeAtShutdown`プロパティが更新されます。ストレージタイプは次回のシャットダウン時に変更されます。
8. カタログ内の各VMの`StorageTypeAtShutdown`値を表示するには、次のコマンドを実行します。

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach { $vmName =
$_.VMName; $storageTypeAtShutdown = ($_.CustomVmData | ConvertFrom-
Json).StorageTypeAtShutdown.DiskStorageAccountType; return New-Object
psobject -Property @{ "VMName" = $vmName; "StorageTypeAtShutdown" =
$storageTypeAtShutdown } }
```

プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する

`Set-ProvScheme`コマンドはプロビジョニングスキームを変更します。ただし、既存のマシンには影響しません。PowerShellコマンド`Set-ProvVMUpdateTimeWindow`を使用すると、既存の永続的または非永続的なマシン、またはマシンセットに現在のプロビジョニングスキームを適用できます。また、既存のMCSプロビジョニング済みマシンの構成更新のタイムスロットをスケジュールすることもできます。スケジュールされたタイムスロット中の電源オンまたは再起動は、スケジュールされたプロビジョニングスキームの更新をマシンに適用します。現在、Azureでは、`ServiceOffering`、`MachineProfile`、および次のカスタムプロパティを更新できます。

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`

- `PersistVm`

注:

- Azure環境でマネージドディスクを使用するカタログの場合、`StorageType`、`WBCDiskStorageType`、および`IdentityDiskStorageType`カスタムプロパティのみを更新できます。
- `Set-ProvVMUpdateTimeWindow`を2回実行した場合、最新のコマンドが有効になります。

更新できるもの:

- 単一のVM
- 特定のVMのリスト、またはプロビジョニングスキームIDに関連付けられている既存のすべてのVM
- 特定のVMのリスト、またはプロビジョニングスキーム名（マシンカタログ名）に関連付けられている既存のすべてのVM

プロビジョニングスキームに以下の変更を加えると、Azureの永続カタログの場合、VMインスタンスが再作成されます:

- `MachineProfile`を変更する
- 削除 `LicenseType`
- 削除 `DedicatedHostGroupId`

注:

既存のマシンのOSディスクとそのすべてのデータはそのまま残り、新しいVMがそのディスクに接続されます。

既存のVMを更新する前に:

1. 既存のマシンの構成を確認します。例えば、,

```
Get-ProvScheme | select ProvisioningSchemeName,
ProvisioningSchemeVersion
```

2. プロビジョニングスキームを更新します。例えば、,

   - マシンプロファイルの入力としてVMを使用する場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-catalog" -MachineProfile
     "XDHyp:\HostingUnits\<hosting-unit>\machineprofile.folder\<resource-
     group>.resourcegroup\<virtual-machine>.vm"
     ```

   - マシンプロファイルの入力としてテンプレート仕様を使用する場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-catalog"

     -MachineProfile "XDHyp:\HostingUnits\<hosting-
     unit>\machineprofile.folder\<resource-
     group>.resourcegroup\<template-spec>.templatespec\<template-spec-
     version>.templatespecversion"

     -ServiceOffering "XDHyp:\HostingUnits\<hosting-
     unit>\serviceoffering.folder\<service-offering>.serviceoffering"
     ```

   - サービスオファリングのみを使用する場合：

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-catalog" -ServiceOffering
     "XDHyp:\HostingUnits\<hosting-unit>\serviceoffering.folder\<service-
     offering>.serviceoffering"
     ```

3. VMの現在のプロパティが現在のプロビジョニングスキームと一致するか、およびVMに保留中の更新アクションがあるかを確認します。例：

   ```
   Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
   ```

   特定のバージョンを持つマシンを見つけることもできます。例：

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
ProvisioningSchemeVersion
```

既存のマシンに次回の再起動時に適用される更新を要求するには：

1. 既存のマシンを更新し、次回の再起動時に更新が適用されるようにするには、次のコマンドを実行します。

   - 既存のすべてのマシンを更新するには。例：

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -StartsNow -DurationInMinutes -1
     ```

   - 特定のリストのマシンを更新するには。例：

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
     ```

   - Get-ProvVMの出力に基づいてマシンを更新するには。例：

     ```
     Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
     ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
     -DurationInMinutes -1
     ```

   注：

   - `StartsNow` は、スケジュールされた開始時刻が現在の時刻であることを示します。
   - 負の数（例：–1）の `DurationInMinutes` は、スケジュールの時間枠に上限がないことを示します。

2. 更新がスケジュールされているマシンを見つけます。例：

   ```
   Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
   ProvisioningSchemeUpdateAfter
   ```

3. マシンを再起動します。次回の電源投入時に、プロパティの変更が既存のマシンに適用されます。更新されたステータスは、次のコマンドを使用して確認できます。例：

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

スケジュールされた時間枠内で次回起動時に最新のプロビジョニング設定に更新するようにVMをスケジュールするには：

1. 次のコマンドを実行します。

   - 開始時刻を現在時刻として更新をスケジュールするには

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
   -VMName vm1 -StartsNow -DurationInMinutes 120
   ```

   - 週末に更新をスケジュールするには

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
   -VMName “vm1” -StartTimeInUTC “10/15/2022 9:00am” -DurationInMinutes
   (New –TimeSpan –Days 2).TotalMinutes
   ```

注：

- `VMName` はオプションです。指定しない場合、更新はカタログ全体に対してスケジュールされます。
- `StartTimeInUTC` の代わりに `StartsNow` を使用して、スケジュール開始時刻が現在時刻であることを示します。
- `DurationInMinutes` はオプションです。デフォルトは120分です。負の数（例：–1）は、スケジュールの時間枠に上限がないことを示します。

2. 更新ステータスを確認します。

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
```

3. VM の電源を入れます。スケジュールされた時間枠の後にマシンの電源を入れた場合、構成の更新は適用されません。スケジュールされた時間枠内にマシンの電源を入れた場合、,
    - マシンがオフになっていて、
        - マシンの電源を入れない場合、構成の更新は適用されません
        - マシンの電源を入れる場合、構成の更新が適用されます
    - マシンの電源がオンの場合、かつ
        - マシンを再起動しない場合、構成の更新は適用されません
        - マシンを再起動すると、構成の更新が適用されます。

構成の更新をキャンセルするには：

単一のVM、複数のVM、またはカタログ全体の構成更新をキャンセルすることもできます。構成更新をキャンセルするには：

1. `Clear-ProvVMUpdateTimeWindow` を実行します。例：
    - 単一のVMに対してスケジュールされた構成更新をキャンセルするには：

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
-VMName “vm1”
```

    - 複数のVMに対してスケジュールされた構成更新をキャンセルするには：

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog"
-VMName "vm1","vm2"
```

> **注：**
>
> VM は同じカタログのものである必要があります。

個々のVMのプロパティを更新する

PowerShellコマンド `Set-ProvVM` を使用して、永続的なMCSマシンカタログ内の個々のVMのプロパティを更新できます。ただし、更新はすぐに適用されません。更新を適用するには、

PowerShellコマンド `Set-ProvVMUpdateTimeWindow` を使用して時間枠を設定する必要があります。

この実装により、マシンカタログ全体を更新することなく、個々のVMを効率的に管理できます。現在、この機能はAzure環境にのみ適用されます。

現在、更新できるプロパティは次のとおりです。

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

この機能を使用すると、次のことができます。

- VMのプロパティを更新する
- マシンカタログの更新後もVMで更新されたプロパティを保持する
- VM に適用された構成の更新を元に戻す

VMのプロパティを更新する前に：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. 既存のマシンカタログの構成を確認します。例：

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

4. 更新を適用するVMの構成を確認します。例：

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

VMのプロパティを更新する

VMのプロパティを更新するには、次の手順を実行します。

1. 更新を適用したいVMの電源をオフにします。
2. VMのプロパティを更新します。例えば、VMのストレージタイプ (`StorageType`) カスタムプロパティを更新したい場合は、以下を実行します。

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

マシンカタログ内の2つのVMのプロパティを同時に更新できます。例:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2
-CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

注:

更新はすぐに適用されません。

3. 更新対象として指定されたプロパティのリストと構成バージョンを取得します。例:

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -VMName
machine1
```

`Version` のプロパティ値と、更新するプロパティ（この場合は `StorageType`）を確認します。

4. 設定バージョンを確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion` のプロパティ値を確認します。更新はまだ適用されていません。VMはまだ古い構成のままです。

5. スケジュールされた更新を要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog
-StartsNow -DurationInMinutes -1
```

スケジュールされた更新の詳細については、プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する を参照してください。

> **注:**
>
> 保留中のプロビジョニングスキームの更新も適用されます。

6. VMを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

7. 設定バージョンを確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion` のプロパティ値を確認します。更新が適用されました。VMは新しい構成になりました。

8. VM にさらに構成更新を適用するには、VM の電源をオフにして、手順を繰り返します。

マシンカタログの更新後にVMで更新されたプロパティを保持する

VM で更新されたプロパティを保持するには、次の操作を行います。

1. 更新を適用する VM の電源をオフにします。
2. マシンカタログを更新します。たとえば、VM サイズ (`ServiceOffering`) とストレージタイプ (`StorageType`) を変更する場合は、次を実行します。

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -ServiceOffering
Standard_E4_v3 -CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

3. マシンカタログの構成詳細を取得します。例:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

`ProvisioningSchemeVersion` は1つ増えました。VMサイズとストレージタイプも更新されます。

4. VMのプロパティを更新します。たとえば、VMにマシンプロファイルを提供します。

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-MachineProfile "XDHyp:\HostingUnits\<hosting-
unit>\machineprofile.folder\<resource-group>.resourcegroup\<template-
spec>.templatespec\<template-spec-version>.templatespecversion"
```

> **注:**
>
> マシンプロファイルの入力には、タグと異なるVMサイズ (`ServiceOffering`) が指定されています。

5. VM上の構成アップデートとマシンカタログのアップデートをマージした後にVMが持つプロパティのリストを取得します。例:

```
Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName
AzureCatalog -VMName machine1
```

> **注:**
>
> VMに対する更新は、マシンカタログで行われた更新を上書きします。

6. VMのスケジュールされたアップデートを要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -VMName
machine1 -StartsNow -DurationInMinutes -1
```

7. VMを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

   VMは、マシンプロファイルから派生した更新済みのVMサイズを保持します。マシンプロファイルで指定されたタグ値もVMに適用されます。ただし、ストレージタイプは最新のプロビジョニングスキームから派生します。

8. VMの構成バージョンを取得します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvisioningSchemeVersion` と `ProvVMConfigurationVersion` に最新バージョンが表示されます。

VMに適用された構成の更新を元に戻す

1. VMに更新を適用した後、VMをシャットダウンします。
2. VMに適用された更新を削除するには、次のコマンドを実行します。例：

```
Set-ProvVM -RevertToProvSchemeConfiguration -ProvisioningSchemeName
AzureCatalog -VMName machine1
```

3. VMのスケジュールされたアップデートを要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -VMName
machine1 -StartsNow -DurationInMinutes -1
```

4. VMを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

5. VMの構成バージョンを確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

の `ProvVMConfigurationVersion` 値が、マシンカタログの構成バージョンになります。

ディスク暗号化の変更

Azure仮想化環境でディスク暗号化を変更し、次の操作を実行できます。

- `New-ProvScheme` コマンドを使用して、マスターイメージのDESとは異なるディスク暗号化セット（DES）を持つMCSマシンカタログを作成します。例えば：

```
$customProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<Property xsi:type="DiskEncryptionSetId" Name="Zones" Value="/
subscriptions/XXXXXXXXXXXXXXXXXXXXXXXXXXXX/resourceGroups/testrsg/
providers/Microsoft.Compute/diskEncryptionSets/test-diskEncryptionSet"/
>

</CustomProperties>

"@

New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName $provisioningSchemeName `

-HostingUnitName $hostingUnitName `

-IdentityPoolName $identityPoolName `

-InitialBatchSizeHint $numberOfVms `

-masterImagePath $masterImagePath `

-NetworkMapping $networkMapping `

-CustomProperties $customProperties
```

- 既存のMCSマシンカタログおよび既存のVMのディスク暗号化タイプを、あるDESキーから別のDESキーに変更するには、`Set-ProvScheme`および`Set-ProvVMUpdateTimeWindow`コマンドを使用します。VMを再起動すると、更新されたDESキーが表示されます。例：

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- 以前CMEKが有効になっていなかったMCSマシンカタログとVMを、`Set-ProvScheme` および `Set-ProvVMUpdateTimeWindow` コマンドを使用して、顧客管理暗号化キー（CMEK）暗号化（DES）、ホストでのディスク暗号化、または二重暗号化を持つように更新します。異なる暗号化タイプについては、Azure サーバー側暗号化、ホストでのAzureディスク暗号化、およびマネージドディスクでの二重暗号化 を参照してください。
- `Set-ProvScheme` および `Set-ProvVMUpdateTimeWindow` コマンドを使用して、以前暗号化されていた既存のMCSマシンカタログとVMを非暗号化に更新します。例えば：

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties

Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- プライベートエンドポイントでディスク暗号化を有効にします（`ProxyHypervisorTrafficThroughConnector` で有効化されたホスト接続を使用したMCSマシンカタログ）。プライベートエンドポイントでディスク暗号化を有効にする方法については、プライベートエンドポイントでディスク暗号化を有効にする を参照してください。

プライベートエンドポイントでディスク暗号化を有効にする

Azureの制限により、現在、プライベートエンドポイントに対して顧客管理キーによるサーバー側暗号化を使用することはできません。ただし、既存のMCSマシンカタログとプライベートエンドポイントを持つVMをDESキーで暗号化するように更新することは可能です。

プライベートエンドポイントを持つ既存のマシンカタログを更新する

プライベートエンドポイントを持つ既存のマシンカタログを更新する詳細な手順は次のとおりです。

1. ディスク暗号化なしでカタログを`ProxyHypervisorTrafficThroughConnector`経由で作成します。
2. `Set-ProvScheme`を実行して、`DiskEncryptionSetId`でカタログを更新します。

> **注:**
>
> `DiskEcryptionSetId`は、`CustomProperties`または`MachineProfile`を介して構成できます。`CustomProperties`と`MachineProfile`の両方で定義されている場合、`CustomProperties`で定義されているプロパティが適用されます。

`CustomProperties`を使用する場合の例:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1"/>

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

MachineProfileを使用する場合の例: ディスク暗号化が有効なVM、またはディスク暗号化設定を持つテンプレート仕様を使用します。

```
Set-ProvScheme -ProvisioningSchemeName azure-catalog -MachineProfile
"XDHyp:
\HostingUnits\azureunit\machineprofile.folder\testrg.resourcegroup\new-
template.vm"
```

または、Web Studioを使用してマシンプロファイルを更新することもできます。

3. 既存のカタログVMを更新するには、`Set-ProvVMUpdateTimeWindow`を実行します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

4. VMを再起動すると、AzureポータルのVMのディスクで更新されたディスク暗号化を確認できます。
5. 新しいカタログVMを追加する前に、`Set-ProvScheme`を実行してディスク暗号化を解除します。

> **注:**
>
> プライベートエンドポイントカタログを更新しているため、この手順が必要です。この手順を実行しないと、新しいVMをカタログに追加しようとしたときにエラーが発生します。

例:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

6. カタログに新しい VM を追加します。

個々のカタログ VM を更新する

個々のカタログVMを更新する詳細な手順は次のとおりです。

1. `ProxyHypervisorTrafficThroughConnector` を使用して、ディスク暗号化なしでカタログを作成します。
2. `Set-ProvVM` を実行して、`DiskEncryptionSetId` でカタログVMを更新します。

> **注:**
>
> `DiskEcryptionSetId` は、`CustomProperties` または `MachineProfile` のいずれかを使用して構成できます。
>
> `CustomProperties` を使用する場合の例:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />

</CustomProperties>'

Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01
-CustomProperties $customProperties
```

MachineProfile を使用する場合の例:

```
Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01
-MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\testrg.resourcegroup\new-
template.vm"
```

3. `Set-ProvVMUpdateTimeWindow` を実行して、既存のカタログVMを更新します。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01 -StartsNow -DurationInMinutes -1
```

4. VMを再起動すると、Azure portal のVMディスクで更新されたディスク暗号化を確認できます。
5. カタログに新しいVMを追加します。

Azure VM、スナップショット、OS ディスク、およびギャラリーイメージ定義の情報を取得する

Azure VM の情報（OSディスクと種類、スナップショット、ギャラリーイメージ定義を含む）を表示できます。この情報は、マシンカタログが割り当てられている場合にマスターイメージ上のリソースに対して表示されます。この機能を使用して、Linux または Windows イメージを表示および選択します。PowerShell プロパティ `TemplateIsWindowsTemplate` が `AdditionDatafield` パラメーターに追加されました。このフィールドには、VMの種類、OSディスク、ギャラリーイメージ情報、OSの種類情報など、Azure固有の情報が含まれています。`TemplateIsWindowsTemplate` を **True** に設定するとOSの種類がWindowsであることを示し、`TemplateIsWindowsTemplate` を **False** に設定するとOSの種類がLinuxであることを示します。

> **ヒント:**
>
> `TemplateIsWindowsTemplate` PowerShell プロパティによって表示される情報は、Azure API から派生しています。このフィールドが空の場合があります。たとえば、データディスクからのスナップショットには `TemplateIsWindowsTemplate` フィールドが含まれていません。これは、OSの種類をスナップショットから取得できないためです。

> たとえば、PowerShell を使用して、Windows OS タイプの場合に Azure VM の `AdditionData` パラメーターを **True** に設定します。

```
PS C:\Users\username> (get-item XDHyp:
\HostingUnits\mynetwork\image.folder\username-dev-testing-
rg.resourcegroup\username-dev-tsvda.vm).AdditionalData

Key Value

ServiceOfferingDescription Standard_B2ms

HardDiskSizeGB 127

ResourceGroupName FENGHUAJ-DEV-TESTING-RG

ServiceOfferingMemory 8192

ServiceOfferingCores 2

TemplateIsWindowsTemplate True
```

```
ServiceOfferingWithTemporaryDiskSizeInMb 16384

SupportedMachineGenerations Gen1,Gen2
```

MCSによって作成されたリソースを識別する

以下は、MCSがリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
IDディスク	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
イメージ	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
NIC	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
OSディスク	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
準備VM	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
公開済みスナップショット	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
リソースグループ	"CitrixResource" : "内部"
	CitrixSchemaVersion: 2.0

リソース名	タグ
	"シトリックスプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
ストレージアカウント	"シトリックスプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
カタログ内のVM	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
WBC ディスク	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"

注記:

MCSによって作成されたリソースとして識別するために**CitrixResource**タグが追加されている場合、VMはCitrixインベントリに表示されません。表示させるには、タグを削除または名前変更できます。

タグを削除する

カタログまたはVMを作成すると、次のリソースにタグが作成されます。

- リソースグループ
- 仮想マシン
- OSディスク
- IDディスク
- ネットワークインターフェイス
- ストレージアカウント

CitrixデータベースからVMとマシンカタログを削除し、タグを削除できます。使用できるのは次のとおりです。

- マシンカタログから単一のVMまたはVMのリストからVMとタグを削除するには、`ForgetVM` パラメーターを指定した`Remove-ProvVM`を使用します。
- Citrixデータベースからマシンカタログを削除し、マシンカタログ全体からタグを削除するには、`ForgetVM`パラメーターを指定した`Remove-ProvScheme`を使用します。

この機能は、永続VMにのみ適用されます。

これを行うには:

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、**asnp citrix***を実行します。
3. CitrixデータベースからVMを削除し、VMからタグを削除するには、`Remove-ProvVM`を実行します。 例:

```
Remove-ProvVM -ProvisioningSchemeName “ProvisioningSchemeName” -VMName “vmname” -ForgetVM
```

4. Citrixデータベースからマシンカタログを削除し、マシンカタログからタグを削除するには、`Remove-ProvScheme`を実行します。例:

```
Remove-ProvScheme -ProvisioningSchemeName “ProvisioningSchemeName” -ForgetVM
```

> **注:**
>
> `Remove-ProvScheme`で`ForgetVM`パラメーターを使用すると、プロビジョニングスキームがBYORG（Bring Your Own Resource Group）またはCitrix管理リソースグループのいずれかに存在する場合、MCSはベースディスクスナップショットを含むすべてのスナップショットを削除します。

詳細情報

- 接続とリソースの作成および管理
- Microsoft Azureへの接続
- マシンカタログの作成
- Microsoft Azureカタログの作成

- マシンカタログの管理

Microsoft System Center Virtual Machine Managerカタログを管理する

マシンカタログを管理するウィザードについては、マシンカタログの管理で説明しています。以下の情報は、Microsoft System Center Virtual Machine Manager（VMM）仮想化環境に固有の詳細を扱っています。

> **注:**
>
> VMMカタログを管理する前に、VMMカタログの作成を完了する必要があります。Microsoft System Center Virtual Machine Managerカタログの作成を参照してください。

MCSによって作成されたリソースを識別する

以下は、MCSがリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
準備VM	タグの文字列: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	カスタムプロパティエントリ: "XdConfig:"XdProvisioned=True"
カタログ内のVM	タグの文字列: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	カスタムプロパティエントリ: "XdConfig:"XdProvisioned=True"

詳細情報

- 接続およびリソースの作成と管理
- マイクロソフト システムセンター バーチャルマシンマネージャーへの接続
- マシンカタログの作成
- マイクロソフト システムセンター バーチャルマシンマネージャーカタログの作成
- マシンカタログの管理

VMwareカタログを管理する

マシンカタログを管理するウィザードについては、マシンカタログの管理で説明しています。以下の情報は、VMware仮想化環境に固有の詳細を扱います。

> **注:**
>
> VMwareカタログを管理する前に、VMwareカタログの作成を完了する必要があります。「VMwareカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create/create-machine-catalog-vmware.html)を参照してください。

マシンカタログのフォルダーIDを更新する

MCSマシンカタログのフォルダーIDは、`Set-ProvScheme`コマンドのカスタムプロパティで`FolderId`を指定することで更新できます。フォルダーIDの更新後に作成されたVMは、この新しいフォルダーIDの下に作成されます。このプロパティが`CustomProperties`で指定されていない場合、VMはマスターイメージが配置されているフォルダーの下に作成されます。

マシンカタログのフォルダーIDを更新するには、次の手順を実行します。

1. Webブラウザーを開き、**vSphere Web Client**のURLを入力します。
2. 資格情報を入力し、**Login**をクリックします。
3. **vSphere Web Client**でVM配置フォルダーを作成します。
4. PowerShellウィンドウを開きます。
5. Citrix固有のPowerShellモジュールをロードするには、**asnp citrix®***を実行します。
6. `Set-ProvScheme`の`CustomProperties`で`FolderID`を指定します。この例では、フォルダーIDの値は`group-v2406`です。

   ```
   Set-ProvScheme -ProvisioningSchemeUid
   "50bb319c-2e83-4a37-9ea1-94f630687372" -CustomProperties
   "<CustomProperties xmlns=""http://schemas.citrix.com/2014/xd/
   machinecreation"" xmlns:xsi=""http://www.w3.org/2001/XMLSchema-
   instance""><Property xsi:type=""StringProperty"" Name=""FolderId""
   Value=""group-v2406"" /></CustomProperties>"
   ```

7. Studioを使用してマシンカタログにVMを追加します。
8. vSphere Web Clientで新しいVMを確認します。新しいVMは新しいフォルダーの下に作成されます。

vSphereでフォルダーIDを検索する

VM のフォルダー ID を見つけるには、任意の ESXi または vCenter サーバーシステムで Managed Object Browser (MOB) にアクセスします。

MOB は、すべての ESX/ESXi および vCenter サーバーシステムに組み込まれている Web ベースのサーバーアプリケーションです。この vSphere ユーティリティを使用すると、VM、データストア、リソースプールなどのオブジェクトに関する詳細情報を表示できます。

1. Web ブラウザーを開き、`http://x.x.x.x/mob` を入力します。ここで、x.x.x.x は vCenter Server または ESX/ESXi ホストの IP アドレスです。例: `<https://10.60.4.70/mob>`。
2. MOB の **Home** ページで、プロパティ **content** の値をクリックします。
3. **rootFolder** の値をクリックします。
4. **childEntity** の値をクリックします。
5. **vmFolder** の値をクリックします。
6. フォルダー ID は **childEntity** の値にあります。

VMのストレージ移行

既存の VM のディスクストレージを古いストレージから新しいストレージに移動できます。移行中、MCS は電源管理、OS ディスクのリセットなどの VM 機能は保持します。新しいディスクストレージを使用して、新しい VM をマシンカタログに追加することもできます。これを行うには、PowerShell コマンド `Move-ProvVMDisk` を使用します。

現在、フルクローン永続 VM のみ移行できます。

新しいストレージは、次の条件を満たしている必要があります。

- 古いストレージと同じクラスター内にある必要があります。
- VMが実行されているホストは、古いデータストアと新しいデータストアの両方にアクセスできる必要があります。

次のタスクを実行できます。

- ディスクストレージの移行
- 古いストレージを非推奨にする

ディスクストレージの移行

ディスクストレージを移行するには：

1. 既存のホスティングユニットに新しいストレージを追加します。古いストレージを**Superseded**に変更します。これはWeb StudioまたはPowerShellコマンドを使用して実行できます。

   - Web Studioを使用している場合は、ストレージの編集を参照してください。
   - PowerShellコマンドを使用している場合：

     - 既存のホスティングユニットに新しいストレージを追加するには、`Add-Hyphostingunitstorage`を実行します。
     - 古いストレージでの新しいVM作成を無効にするには、**Superseded**をtrueとして`Set-Hyphostingunitstorage`を実行します。

2. VMをシャットダウンし、**メンテナンスモード**をオンにします。
3. VMのディスクストレージを新しいストレージに移動し、ストレージ情報を更新します。例:

```
Move-ProvVMDisk -ProvisioningSchemeName "myFullCloneProvScheme" -VMName
("VMware-TestVM01", "VMware-TestVM02") -DiskType OS,Identity
-DestinationStorageId datastore1,datastore1
```

4. 移行のタスクIDを取得します。例:

```
,(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk
-ProvisioningSchemeName xxxxx -DiskType OS,Identity
-DestinationStorageId datastore1,datastore1
```

5. 移行のステータスを確認します。

   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMovedVirtualMachines`：ディスク移行が成功したVMのリストを提供します。これには、すでに新しいストレージに移行されたVMも含まれます。
   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMoveFailedVirtualMachines`: 移行に失敗したVMのリストを提供します。
   - `(Get-ProvTask -TaskID xxxxxxxxx).NotStartedVirtualMachines`: 移行がまだ開始されていないVMのリストを提供します。
   - `Get-ProvVM -ProvisioningSchemeName xxxxx -VMName "VMware-TestVM01`: 移行後の更新されたVMプロパティを提供します。`StorageId`、`AssignedImage`、`BootedImage`、`IdentityDiskId`、`IdentityDiskStorage`、`LastBootTime`などのプロパティを確認してください。

スナップショット付きのMCSで作成されたVMのディスクを移行した後、**Consolidation is required in the VSphere Client** という警告が表示されることがあります。統合してデータ損失を回避するには:

1. VMware VMのバックアップを取ります。たとえば、すべてのVMファイルをデータストア上の別のフォルダーに転送します。
2. 警告が表示されたら、**統合**をクリックし、次に**OK**をクリックして統合を確認します。

古いストレージの廃止

VMディスクの移行後に古いストレージを非推奨にするには：

1. ホスティングユニットの各ディスクストレージにおけるベースディスクとマシン数に関する情報を取得します。例：

   ```
   $result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName xxxxx

   $result

   $result.ProvResourceInStorage | Format-List -Property *
   ```

   移行が成功すると、MCSは古いベースディスクを自動的に削除し、古いストレージにはマシンがなくなります。したがって、コマンドを実行した後、古いストレージにマシンとベースディスクがないことを確認してください。
2. ホスティングユニットから古いストレージを完全に削除するには、`Remove-Hyphostingunitstorage` を実行します。Web Studio を使用して古いストレージを削除することもできます。

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
VMの準備	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"XdConfig:"XdProvisioned=True"
カタログ内のVM	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

リソース名	タグ
	"XdConfig:"XdProvisioned=True"

詳細情報

- 接続とリソースの作成および管理(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections.html)
- VMwareへの接続(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/connections/connection-vmware-virtualization-environments.html)
- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html)
- VMwareカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create/create-machine-catalog-vmware.html)
- マシンカタログの管理(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-manage.html)

電源管理

Citrix Virtual Apps and Desktops™ を使用すると、さまざまなサポート対象ハイパーバイザーおよびクラウドサービス全体で、MCSプロビジョニングされたVMの電源を管理できます。電源管理操作により、以下が提供されます。

- 最適なユーザーエクスペリエンス
- コスト管理と電力節約

利用可能な電源操作は次のとおりです。

- 起動
- シャットダウン
- 再起動
- 一時停止
- 再開
- 強制再起動
- 強制シャットダウン

> **注：**
>
> - 非永続VMの場合、電源サイクル（シャットダウン/起動および再起動）によりOSディスクがリセットされます。
> - 電源操作の機能と動作は、ハイパーバイザーまたはクラウドサービスによって異なります。

> この記事では、特定のサポート対象ハイパーバイザーに関連する主要な電源管理機能について説明します。

- AWS VMの電源管理
- Azure VMの電源管理

AWS VM の電源管理

必要な権限については、「Required AWS permissions」を参照してください。

インスタンスの休止

休止プロセスは、インスタンスのインメモリ状態と、そのプライベートIPアドレスおよびElastic IPアドレスを保存し、中断したところから正確に再開できるようにします。

インスタンスに休止が指示されると、インメモリ状態をルートEBSボリュームのファイルに書き込み、その後シャットダウンします。Amazon EBSボリュームは、インスタンスにアタッチできる耐久性のあるブロックレベルのストレージデバイスです。ボリュームをインスタンスにアタッチすると、物理ハードドライブと同じように使用できます。インスタンスのルートEBSボリュームを暗号化します。暗号化により、メモリからEBSボリュームにコピーされる機密データが適切に保護されます。EBS暗号化の詳細については、「Amazon EBS encryption」を参照してください。

サポートされているインスタンスの休止には、次の制限があります。

- 最大150 GBのインスタンスメモリ（RAM）のみがサポートされます
- UEFIブートモードはサポートされていません
- EBSボリュームタイプとしてサポートされているのは、汎用SSDとプロビジョンドIOPS SSDのみです。

休止をサポートするVMを作成する

休止をサポートするVMを作成するには：

1. ホスト接続を作成します。「Connection to AWS」を参照してください。
2. EBSルートが暗号化され、**Stop-Hibernate**プロパティが有効になっているインスタンスを起動します。インスタンスの起動方法、ルートEBSボリュームの暗号化、および休止の有効化の詳細については、`<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html/>`を参照してください。このインスタンスをマスターイメージとして使用してAMIを作成します。
3. マスターイメージを準備します。
   a. マスターイメージにVDAをインストールします。Citrixでは、最新の機能にアクセスできるように、最新バージョンをインストールすることをお勧めします。マスターイメージにVDAをインストールしないと、カタログの作成が失敗します。VDAのインストール方法の詳細については、「Install VDAs」を参照してください。
   b. マスターイメージを、アプリケーションとデスクトップがメンバーであるドメインに参加させます。マスターイメージが、マシンが作成されるホストで利用可能であることを確認してください。
4. そのインスタンスからAMIを作成します。インスタンスからAMIを作成する方法については、「Amazon EC2インスタンスからAMIを作成する」を参照してください。
5. `New-ProvScheme`コマンドを使用してマシンカタログを作成します。`AwsCaptureInstanceProperties`カスタムプロパティを**True**に設定します。Web StudioでAWSインスタンスプロパティを有効にする方法については、「**Web StudioでのAWSインスタンスプロパティの適用と運用リソースのタグ付け**」を参照してください。

```
New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot

-CustomProperties "AwsCaptureInstanceProperties,true;"

-HostingUnitName "xxx" -IdentityPoolName $catalog_name
-InitialBatchSizeHint 1

-MasterImageVM "xyz.template" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\MyConn\\us-east-2a.availabilityzone\10.0.0.0``/24
(vpc-0f1771e45671aedcd).network"}

-ProvisioningSchemeName $catalog_name

-RunAsynchronously -Scope @() -SecurityGroup @("xxx") -ServiceOffering
"xxx"
```

PowerShell コマンドを使用してマシンカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/>` を参照してください。

ハイバネート可能な VM は、次の場合に作成されます。

- **Stop-Hibernate** プロパティが有効になっているマスターイメージから作成された AMI を選択した場合。
- マスター VM がドメインに参加しており、VDA がインストールされている場合。
- 休止状態を処理できる正しいVMサイズ（サービス提供）を選択します。

New-ProvSchemeコマンドは、次の場合に適切なエラーメッセージとともに失敗します。

- マスターVMが休止状態に対応しているが、サービスオファリングが休止状態を処理できない場合。
- マスターVMがドメインに参加しておらず、VDAがインストールされていない場合。

サービス提供とAMIの休止状態

サービス提供とAMI（テンプレート）の休止状態を取得するには、次のコマンドを実行します。

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b (ami-0e6c5b33a52d2a6b6).template'`
- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

既存のハイバネーション対応プロビジョニングスキームのサービス提供を更新する

1. `Set-ProvScheme`コマンドを実行します。例えば、,

```
Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering
<String>
```

サービス提供が互換性がない場合、システムは例外メッセージを表示します。

ハイバネーション対応のマシンカタログを作成する

マシンカタログを作成する際、ハイバネーションをサポートするマシンプロファイルを使用できます。

1. カタログ作成ウィザードで、マシンプロファイルの選択まで指示に従います。

2. **マシンテンプレート**ページで、**マシンプロファイルの選択**をクリックし、マシンプロファイルを選択します。
3. 「**仮想マシン**」ページで、「**編集**」アイコンをクリックし、VMを選択します。

> **注:**
>
> マシンプロファイルがハイバネーション対応の場合、システムはハイバネート可能なVMのみを表示します。

4. 画面の指示に従ってすべての設定を完了します。**概要**ページには、カタログのハイバネーションステータスが表示されます。

> **注:**
>
> マシンカタログの編集で、マシンプロファイルをハイバネーション対応のものに変更すると、それに応じてVMを再構成するよう求められます。

ハイバネーションをサポートするマシンカタログを更新する

既存のマシンカタログをハイバネーションをサポートしないマシンカタログで更新しようとすると、適切なエラーメッセージが表示されて更新が失敗します。

休止状態のVMの電源管理

休止状態のVMに対して、以下の電源管理操作を実行できます。

1. 実行中の状態からVMをサスペンドします。
2. 一時停止状態からVMを再開します。
3. 一時停止状態からVMを再起動します。

Azure VMの電源管理

必要な権限については、「必要なAzure権限」を参照してください。

Azure オンデマンドプロビジョニング

Azureオンデマンドプロビジョニングでは、プロビジョニングが完了した後、Citrix Virtual Apps and Desktops™ が電源オンアクションを開始したときにのみVMが作成されます。

MCS を使用して Azure Resource Manager でマシンカタログを作成する場合、Azure オンデマンドプロビジョニング機能は次のとおりです。

- ストレージコストを削減します
- カタログ作成を高速化します

MCS カタログを作成すると、Azure portal にリソースグループ内のネットワークセキュリティグループ、ネットワークインターフェイス、ベースイメージ、およびIDディスクが表示されます。

Citrix Virtual Apps and Desktops がVMの電源オンアクションを開始するまで、Azureポータルには VMが表示されません。次の相違点を持つ2種類のマシンがあります。

- プールされたマシンでは、オペレーティングシステムディスクとライトバックキャッシュは、VMが存在する場合にのみ存在します。コンソールでプールされたマシンをシャットダウンすると、VMはAzureポータルに表示されません。マシンを定期的にシャットダウンする場合（たとえば、勤務時間外）、大幅なストレージコストを節約できます。
- 専用マシンでは、オペレーティングシステムディスクは、VMが最初に電源オンされたときに作成されます。AzureポータルのVMは、マシンIDが削除されるまでストレージに残ります。コンソールで専用マシンをシャットダウンすると、VMはAzureポータルに引き続き表示されます。

> **注:**
>
> オンデマンドプロビジョニング機能の前に作成されたAzureカタログ（「レガシー」カタログ）のサポートは非推奨です。したがって、Azureレガシーカタログ VMを再作成してください。カタログはオンデマンドとしてプロビジョニングされ、ストレージコストを節約します。

電源サイクル時にプロビジョニングされた仮想マシンを保持する

電源サイクル時にプロビジョニングされた仮想マシンを保持するかどうかを選択します。PowerShellパラメーター `New-ProvScheme CustomProperties` を使用します。このパラメーターは、電源サイクル時にプロビジョニングされた仮想マシンが永続化するかどうかを決定するために使用される追加のプロパティ `PersistVm` をサポートします。電源オフ時に仮想マシンを永続化するには `PersistVm` プロパティを **true** に設定するか、電源オフ時に仮想マシンが保持されないようにするにはプロパティを **false** に設定します。

> **注:**

`PersistVm` プロパティは、`CleanOnBoot` と `UseWriteBackCache` のプロパティが有効になっているプロビジョニングスキームにのみ適用されます。非永続仮想マシンに対して `PersistVm` プロパティが指定されていない場合、それらは電源オフ時に Azure 環境から削除されます。

次の例では、`New-ProvScheme CustomProperties` パラメーターは `PersistVm` プロパティを **true** に設定します。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
resourcegroup" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>
```

次の例では、`New-ProvScheme CustomProperties` パラメーターは、`PersistVM` を **true** に設定することでライトバックキャッシュを保持します。

```
New-ProvScheme

-AzureAdJoinType "None"

-CleanOnBoot
```

```
 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageType`" Value=`"Standard_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"false`" /
><Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"PersistVm`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"ResourceGroups`" Value=`"demo-resourcegroup`" /><Property
xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Client`" /></CustomProperties>"

 -HostingUnitName "demo"

 -IdentityPoolName "NonPersistent-MCSIO-PersistVM"

 -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-
test.resourcegroup\demo-snapshot.snapshot"

 -NetworkMapping @ {"0"="XDHyp:\HostingUnits\demo\
\virtualprivatecloud.folder\East US.region\virtualprivatecloud.folder\ji-
test.resourcegroup\jitest-vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"

 -ServiceOffering "XDHyp:
\HostingUnits\demo\serviceoffering.folder\Standard_B2ms.serviceoffering"
-UseWriteBackCache

 -WriteBackCacheDiskSize 127

 -WriteBackCacheMemorySize 256
```

ヒント:

`PersistVm` プロパティは、プロビジョニングされた仮想マシンを保持するかどうかを決定します。`PersistOsdisk` プロパティは、OS ディスクを永続化するかどうかを決定します。プロビジョニングされた仮想マシンを保持するには、まず OS ディスクを保持します。

> 仮想マシンを削除せずに OS ディスクを削除しないでください。`PersistVm` パラメーターを指定せずに `PersistOsdisk` プロパティを使用できます。

ストレージタイプ変更失敗時の電源オン動作をカスタマイズする

電源オン時に、Azure の障害により、管理ディスクのストレージタイプが目的のタイプに変更できない場合があります。このようなシナリオでは、VM はオフのままで、障害メッセージが送信されます。ただし、ストレージが構成されたタイプに復元できない場合でも VM の電源をオンにするか、VM の電源をオフのままにするかを選択できます。

- カスタムプロパティ `FailSafeStorageType` を **true** (デフォルト設定) に構成した場合、または `New-ProvScheme` または `Set-ProvScheme` コマンドで指定しない場合:
  - 電源オン時、VM は誤ったストレージタイプで電源がオンになります。
  - シャットダウン時、VM は誤ったストレージタイプでオフのままになります。
- `New-ProvScheme` または `Set-ProvScheme` コマンドでカスタムプロパティ `FailSafeStorageType` を **false** に構成した場合:
  - 電源オン時、VM は誤ったストレージタイプでオフのままになります。
  - シャットダウン時、VM は誤ったストレージタイプでオフのままになります。

マシンカタログを作成するには:

1. PowerShell ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。
3. まだ作成されていない場合は、ID プールを作成します。
4. `New-ProvScheme` にカスタムプロパティを追加します。例:

```
New-ProvScheme -HostingUnitName "Azure-Resources-1" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\Azure-
Resources-1\image.folder\abc.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\Azure-
Resources-1\ght.folder\abc.resourcegroup\abc-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "name"
```

```
-ServiceOffering "XDHyp:\HostingUnits\Azure-
Resources-1\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown`"
Value=`"Standard_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"true`" />

</CustomProperties>"
```

5. マシンカタログを作成します。Remote PowerShell SDKを使用してカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

既存のマシンカタログを更新して、`FailSafeStorageType`カスタムプロパティを含めます。この更新は既存のVMには影響しません。

1. `Set-ProvScheme`コマンドでカスタムプロパティを更新します。例：

```
Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "

<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"false`" />
```

```
</CustomProperties>"
```

Set-ProvScheme で行われた変更を既存の VM に適用するには、`Set-ProvVMUpdateTimeWindow` コマンドを `-StartsNow` および `-DurationInMinutes -1` パラメータとともに実行します。

1. `Set-ProvVMUpdateTimeWindow` コマンドを、`-StartsNow` および `-DurationInMinutes -1` パラメータコマンドとともに実行します。例:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
   <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
   ```

2. VMを再起動します。

休止状態対応VMを作成する

Azure環境では、休止状態をサポートするMCSマシンカタログを作成できます。この機能を使用すると、VMを中断し、ユーザーが再度サインインしたときにVMの以前の状態に再接続できます。

休止状態機能は以下に適用されます。

- シングルセッションOS
- 永続VMと非永続VM
- 静的およびランダム (プールされた) VDI デスクトップ

VDI デスクトップが静的かランダムかに関わらず、VM を休止状態にした後、同じセッションに再開できます。

このセクションでは、以下を参照してください。

- 前提条件
- 制限事項
- 休止状態対応のマシンカタログを作成および管理する
- 既存の休止状態対応 VM 用のマシンカタログを作成する
- 休止状態プロパティを確認する
- VM の電源管理 (手動および自動)

休止状態を使用するための前提条件

休止状態を使用するには、以下のタスクを完了していることを確認してください。

- Windows と Linux の両方のマスターイメージに Azure VM Agent をインストールします。Windows イメージのページファイルは一時ディスクに配置できます。マシンカタログで休止状態が有効になっている場合、MCS はページファイルの場所をベースディスクの C: ドライブに設定します。
- MCS は、生成されたリソースの休止状態プロパティを自動的に設定します。休止状態をサポートするために、マスターリソースのプロパティを設定する必要はありません。
- サブスクリプション内で休止状態をサポートする VM サイズを使用してください。
- VM が休止状態機能を継承できるように、休止状態対応のマシンプロファイル (VM またはテンプレート仕様) を作成します。VM の作成については、休止状態の概要 を参照してください。

> **注:**
>
> Microsoftによると、OSディスクから休止状態が有効なVMを展開できます。この機能は現在一部のリージョンでサポートされており、まもなくすべてのリージョンで利用可能になります。詳細については、「OSディスクから休止状態が有効なVMを展開する」を参照してください。

テンプレート仕様を作成するには、次の手順を実行します。

a. Azure Portalを開きます。テンプレートで使用する構成のVMを選択します。左ペインで**テンプレートのエクスポート**を選択します。

b. **パラメーターを含める**チェックボックスをオフにします。コンテキストをコピーし、例えば`VMExportTemplate.json`のようなJSONファイルとして保存します。

c. パラメーター`hibernationEnabled`がテンプレート上で`true`であることを確認してください。パラメーターが`true`でない場合は、使用したVM構成を確認してください。テンプレートファイルでサポートされているVMサイズを指定できます。ただし、カタログの作成時にマシンサイズを指定することもできます。

d. ネットワークインターフェースリソースのテンプレートをJSONファイル`VMExportTemplate.json`に追加します。その結果、2つのリソースを持つARMテンプレートファイルが作成されます。

e. **Azure Portal > テンプレート仕様 > テンプレートのインポート > ローカルテンプレートファイルの選択**を選択して、このテンプレートファイルをARMテンプレート仕様としてインポートします。

f. ARMテンプレート仕様が作成されたら、それをマシンプロファイルとして使用できます。

> **注:**
>
> Citrix Studioに同期されるまで数分かかる場合があります。

詳細については、Microsoftドキュメント「休止状態を使用するための前提条件」を参照してください。

制限事項

- シングルセッションOSマシンカタログ（永続的および非永続的）のみがサポートされています。
- エフェメラルOSディスクおよびMCS I/O機能は、Azure休止状態をサポートしていません。
- 自動Windowsアップデート中に休止状態が失敗する可能性があります。

詳細については、Microsoft ドキュメントを参照してください。

休止状態対応のマシンカタログを作成および管理する

休止状態対応のVMを作成するには、以下を使用して休止状態対応のマシンカタログを作成および管理できます。

- Web Studio、または
- PowerShell コマンド

WEB STUDIO を使用してカタログを作成する

1. **マシンカタログの作成**を選択します。カタログ作成ウィザードが開きます。
2. **マシンタイプ**ページで、このカタログの**シングルセッションOS**マシンタイプを選択します。
3. **マシン管理**ページで、次のように設定を選択します。
   a. 「**電源管理されているマシン（仮想マシンやブレードPCなど）**」を選択します。
   b. 「**Citrix Machine Creation Services™ (MCS)**」を選択します。
4. **デスクトップエクスペリエンス**ページで、必要に応じてランダムまたは静的デスクトップエクスペリエンスを選択します。
5. **イメージ**ページで、マスターイメージを選択します。**マシンプロファイルを使用する**チェックボックスをオンにし、休止状態をサポートするマシンプロファイルを選択します。ツールヒントをクリックして、マシンプロファイルが休止状態をサポートしているかどうかを確認します。

6. **ストレージとライセンスの種類**ページで、このカタログに使用するストレージとライセンスを選択します。
7. 「**仮想マシン**」ページで、VMの数、VMサイズ、および可用性ゾーンを選択します。

> 「**注：**」：
>
> 休止状態をサポートするマシンサイズのみが、選択肢として表示されます。

8. 「**NIC**」ページで、VMで使用するNICを追加します。
9. 「**ディスク設定**」ページで、ライトバックキャッシュディスクのストレージタイプとサイズを選択します。
10. 「**リソースグループ**」ページで、VMをプロビジョニングするリソースグループを選択します。
11. 「**マシンID**」ページで、「**新しいActive Directoryアカウントを作成**」を選択します。次に、アカウントの命名スキームを指定します。
12. 「**ドメイン資格情報**」ページで、「**資格情報を入力**」をクリックします。ターゲットのActive Directoryドメインでアカウント作成を実行するために、ドメイン資格情報を入力します。
13. 「**概要**」ページで、マシンカタログの名前を入力し、「**完了**」をクリックします。

MCSマシンカタログの作成が完了したら、カタログリストでカタログを見つけ、「**テンプレートプロパティ**」タブをクリックします。パラメーター「**休止状態**」の値は「**サポート済み**」である必要があります。

マシンカタログを編集する場合は、以下の制限事項を考慮してください。

- 現在のマシンカタログが休止状態をサポートしている場合、次のことはできません。
  - VMサイズを休止状態に対応していないものに変更すること。
  - マシンプロファイルを休止状態に対応していないものに変更すること。
- 現在のマシンカタログが休止状態をサポートしていない場合、次のことはできません。
  - 現在、Web Studio を使用してマシンプロファイルを休止状態対応のものに変更します。

既存の休止状態対応VMを管理するためのマシンカタログを作成する

すでに休止状態対応VMがあり、それらを一時停止および再開したい場合は、それらのVMを電源管理のためにインポートするマシンカタログを作成します。

> **注:**
>
> 休止状態対応VMと非対応VMの両方を含むマシンカタログを作成できます。ただし、休止状態関連の機能が必要な場合は、休止状態対応VMのみでマシンカタログを作成する必要があります。

> Web Studio を使用して既存の休止状態対応VMのカタログを作成するには、画面の指示に従って手順を完了し、以下の主要な設定に注意してください。

1. **マシン管理**ページで、**電源管理されているマシン**を選択し、マシンの展開方法として**その他のサービスまたはテクノロジー**を選択します。
2. **仮想マシン**ページで、休止状態対応VMのみを追加またはインポートします。

POWERSHELLコマンドを使用してマシンカタログを作成する

休止状態を使用するためのすべての要件を満たした後、`New-ProvScheme`コマンドを使用して休止状態対応マシンカタログを作成できます。Remote PowerShell SDK を使用してカタログを作成する方法については、New-ProvSchemeを参照してください。

カタログの作成中に、以下のPowerShellコマンドを使用して、VMサイズとマシンプロファイルが休止状態をサポートしているかどうかを確認できます。

- VMサイズの場合、次のコマンドを実行し、プロパティ`supportsHibernation`が**True**であるかどうかを確認します。例：

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath
@("XDHyp:\HostingUnits\ <VirtualNetwork> \serviceoffering.folder") |
select Name, AdditionalData | ConvertTo-Json
```

- マシンプロファイルの場合、次のコマンドを実行し、プロパティ`supportsHibernation`が**True**であるかどうかを確認します。例：

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath
@("XDHyp:\HostingUnits\ <VirtualNetwork>
\machineprofile.folder\abc.resourcegroup")|select Name, AdditionalData|
ConvertTo-Json
```

マシンカタログを編集する場合は、次の制限事項を考慮してください。

- 現在のマシンカタログが休止状態をサポートしている場合、次のことはできません。

  - VMサイズを休止状態非対応のものに変更する
  - マシンプロファイルを休止状態非対応のものに変更する

- 現在のマシンカタログが休止状態をサポートしていない場合、次のことはできません。
  - 現時点では、Web Studioを使用してマシンプロファイルを休止状態にできるものに変更すること。

Remote PowerShell SDKを使用してカタログのVMサイズとマシンプロファイルを変更する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/>`を参照してください。

休止状態のプロパティを確認する

PowerShellコマンドを使用して、マシンカタログ、VM、およびブローカーマシンの休止状態のプロパティを確認できます。

- プロビジョニングスキームの休止状態のプロパティを確認するには、次のPowerShellコマンドを実行します。`HibernationEnabled`パラメーターは`True`である必要があります。

```
(Get-ProvScheme -provisioningSchemeName <YourSchemeName>).VMMetadata
-join "" |  ConvertFrom-Json | Select HibernationEnabled
```

- プロビジョニングVMの休止状態のプロパティを確認するには、次のPowerShellコマンドを実行します。`SupportsHibernation`パラメーターは`True`である必要があります。

```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json |
Select SupportsHibernation
```

- ブローカーマシンの休止状態の機能を確認するには、次のPowerShellコマンドを実行します。**Suspend**および**Resume**電源アクションは、休止状態の機能を示します。

```
(Get-BrokerMachine -MachineName
<YourMachineName>).SupportedPowerActions
```

休止状態に対応したVMの電源管理

休止状態に対応したVMに対して、次の電源管理操作を実行できます。

- 実行状態からVMを**一時停止**する
- 一時停止状態からVMを**再開**する

- 一時停止状態からVMを**強制シャットダウン**する
- サスペンド状態からVMを**強制再起動**する

詳細については、以下を参照してください。

- サスペンド
- 再開

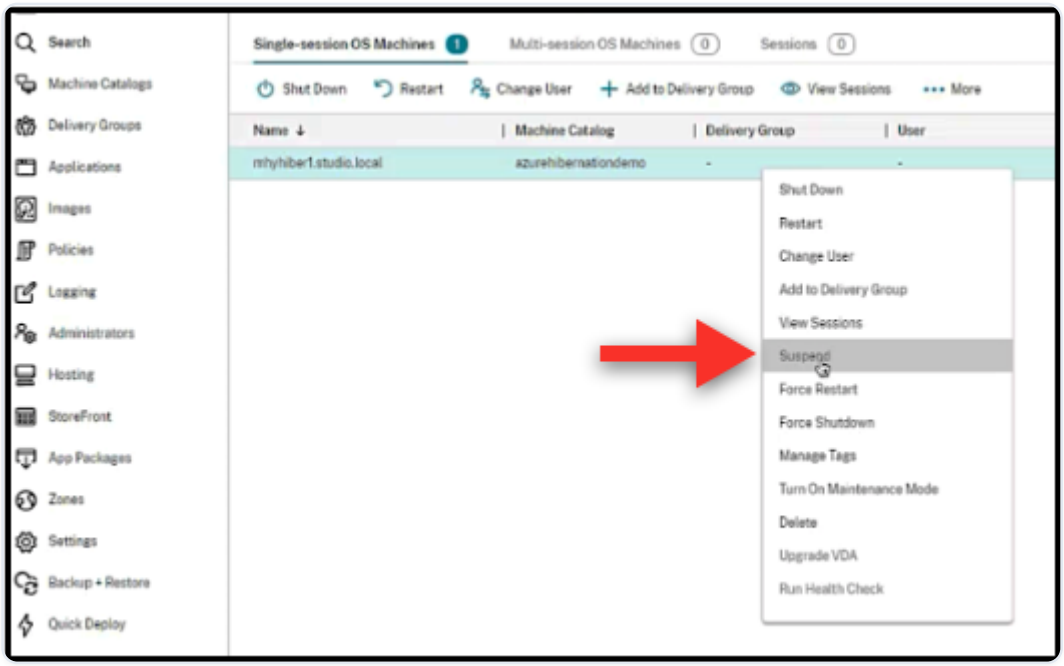
サスペンド

次のいずれかの方法でVMをサスペンドできます。

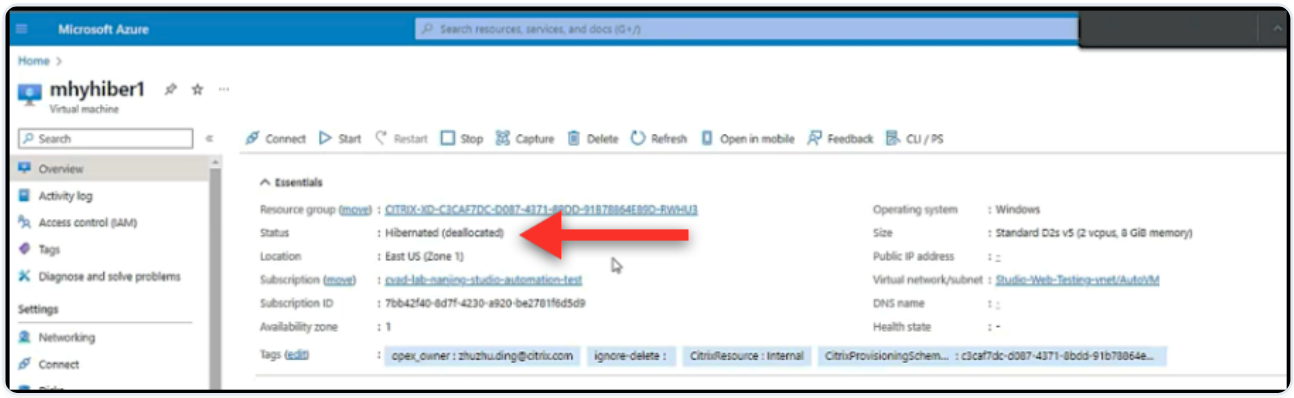
- Web Studioを使用して**手動で**
- タイムアウトポリシーを使用して**自動的に**: 詳細については、その他の設定を参照してください。

VMを手動でサスペンドするには:

1. VMを右クリックし、**サスペンド**を選択します。**はい**をクリックしてアクションを確定します。**電源状態**が**サスペンド中**から**サスペンド済み**に変わります。



AzureポータルでVMのステータスを確認できます。



再開

休止状態のVMを再開するには、次のいずれかの方法を使用します。

- **手動**:
  - 管理者はWeb Studioを使用してVMを再開できます。

    Web Studioを使用してVMを再開する(/en-us/citrix-virtual-apps-desktops/2407/media/resume-hibernation-vms.png)
  - エンドユーザーは、デスクトップアイコンをクリックすると、Citrix Workspace™メニューを使用してVMを起動できます。

    Citrix Workspaceを使用してVMを再開する(/en-us/citrix-virtual-apps-desktops/2407/media/resume-vm-workspace.png)
- **自動**:
  - ピーク時間を正しく構成すると、Autoscale™は休止状態のマシンを自動的に起動できます。タイムスケジュールをクリックして、ピーク時間を30分間隔で設定できます。各青いフレームは、ピーク時間としてマークされたタイムスロットを表します。ピーク時間には、連続したタイムスロットと非連続のタイムスロットを設定できます。
    - 連続したタイムスロット

      連続したピークタイムスロット(/en-us/citrix-virtual-apps-desktops/2407/media/consecutive-peak-time-autoscale.png)
    - 連続しない時間帯

      非連続のピークタイムスロット(/en-us/citrix-virtual-apps-desktops/2407/media/non-consecutive-peak-time-autoscale.png)

> **注:**

> **Autoscaleの管理 > 負荷ベースの設定**で、**アクション**が**中断**として構成されている場合、そのデリバリーグループ内のすべてのVMが休止機能を備えていることを確認してください。そうでない場合、休止できないVMは実行を継続します。

> Autoscaleの負荷ベースの設定を管理する(/en-us/citrix-virtual-apps-desktops/2407/media/azure-hibernation-autoscale.png)

休止失敗の警告メッセージを取得する

MCSプロビジョニング済みおよび既存の休止状態対応VMの休止状態失敗の場合に、PowerShellコマンド`Get-ProvOperationEvent`を使用して警告メッセージを取得できます。PowerShellコマンドの詳細については、SDKドキュメントGet-ProvOperationEventを参照してください。

これを行うには：

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. 休止状態の失敗の場合に警告メッセージを取得するために`Get-ProvOperationEvent`を実行します。

   ```
   Get-ProvOperationEvent -filter { OperationName -eq "Suspend" }
   ```

   出力：

   ```
   EventAdditionalData : Error code = OperationNotAllowed and Error
   message = The Hibernate-Deallocate Operation cannot be performed on a
   VM that has extension 'AzureHibernateExtension' in failed state. For
   more information, see https://aka.ms/hibernate-resume/errors. Error
   details from the extension : Enabling

                    hibernate failed. Response from the powercfg command.
   Exit Code: 1. Error message:

                    Hibernation failed with the following error: The
   request is not supported.



                    The following items are preventing hibernation on
   this system.
   ```

```
                    The current Device Guard configuration has disabled
hibernation.

                    An internal system component has disabled
hibernation.

                            Hypervisor

                Status: 409

                ErrorCode: OperationNotAllowed



                Content:

                {

                  "error": {

                    "code": "OperationNotAllowed",

                    "message": "The Hibernate-Deallocate Operation
cannot be performed on a VM that has extension
'AzureHibernateExtension' in failed state. For more information, see
https://aka.ms/hibernate-resume/errors. Error details from the
extension : Enabling hibernate failed. Response from the

                powercfg command. Exit Code: 1. Error message:
\nHibernation failed with the following error: The request is not
supported.\r\r\n\r\nThe following items are preventing hibernation on
this system.\r\n\tThe current Device Guard configuration has disabled
hibernation.\r\n\tAn internal system

                component has disabled hibernation.
\r\n\t\tHypervisor"

                  }

                }

EventCategory       : Warning
```

```
EventDateTime       : 1/11/2024 4:18:31 AM

EventId             : 0

EventMessage        : Failed to suspend machine my-resource-group/my-
vm.

EventSeverity       : Important

EventSource         : AzureRmPlugin

EventState          : New

LinkedObjectType    : ProvisioningScheme

LinkedObjectUid     : 589cb600-6e65-479f-9d47-9715c4732366

OperationName       : Suspend

OperationTargetName : my-resource-group/my-vm

OperationTargetType : VirtualMachine

OperationType       : PowerManagement

Recommendation      :
```

休止状態の問題のトラブルシューティング

休止状態と信頼できる起動VM機能の両方を有効にしようとすると、ゲストOSの構成が正しくない場合、次のエラーメッセージが表示されます。

エラーコード	エラーメッセージ
OperationNotAllowed	拡張機能「AzureHibernateExtension」が失敗状態のVMでは、休止状態解除操作を実行できません。詳細については、`<https://aka.ms/hibernate-resume/errors/>`を参照してください。拡張機能からのエラー詳細：休止状態の有効化に失敗しました。powercfgコマンドからの応答。終了コード：1。エラーメッセージ：次のエラーにより休止状態に失敗しました：要求はサポートされていませ

エラーコード	エラーメッセージ
	ん。以下の項目がこのシステムでの休止状態を妨げています。**現在のDevice Guard構成により休止状態が無効になっています。内部システムコンポーネントにより休止状態が無効になっています。**

この問題を解決するには、ゲストVM内で仮想化が有効になっていることを確認してください。たとえば、Windows環境でHyper-Vが有効になっていることを確認します。Microsoft Windowsの制限によると、信頼できる起動がVMで有効になっている場合、休止状態はネストされた仮想化でのみサポートされます。

警告メッセージの詳細については、MicrosoftドキュメントVM休止状態のトラブルシューティングを参照してください。

> **注：**
>
> VMの再開の失敗に関連するエラーメッセージは、今後のリリースで提供される予定です。

詳細情報

Citrix Azureの休止状態の詳細については、Citrix Tech Zoneの記事を参照してください。

セキュリティポリシー

この記事では、サポートされているさまざまなクラウドサービスにおけるセキュリティ機能について説明します。セキュリティ機能には、次のものがあります。

- セキュリティグループ(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/security-policies/security-group.html)
- セキュアブート(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/security-policies/secure-boot.html)
- 暗号化機能(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/security-policies/encryption-capabilities.html)

セキュリティグループ

セキュリティグループは、仮想ネットワーク内のリソース間のネットワークトラフィックをフィルタリングするためのセキュリティルールのグループです。セキュリティルールは、いくつかの種類のリソースに対するインバウンドネットワークトラフィック、またはそれらのリソースからのアウトバウンドネットワークトラフィックを許可または拒否します。各ルールは次のプロパティを指定します。

- 名前: ネットワークセキュリティグループ内の一意の名前
- 優先度: ルールは優先度順に処理され、数値が小さいほど優先度が高いため、数値が小さいものから先に処理されます
- 送信元または宛先: 任意、または個別のIPアドレス、クラスレスドメイン間ルーティング (CIDR) ブロック (例: 10.0.0.0/24)、サービスタグ、またはアプリケーションセキュリティグループ
- プロトコル: 各セキュリティグループのルールを追加する際のベースとなるプロトコル
- 方向: ルールがインバウンドトラフィックまたはアウトバウンドトラフィックに適用されるかどうか
- ポート範囲: 個別のポートまたはポート範囲を指定できます
- アクション: 許可または拒否

サポートされているハイパーバイザーの詳細については、以下を参照してください。

- AWSのセキュリティグループ
- Microsoft Azureのセキュリティグループ
- Google Cloud Platformのセキュリティグループ

AWSのセキュリティグループ

セキュリティグループは、VPC内のインスタンスのトラフィックを制御する仮想ファイアウォールとして機能します。パブリックサブネット内のインスタンスがプライベートサブネット内のインスタンスと通信できるようにするルールをセキュリティグループに追加します。これらのセキュリティグループをVPC内の各インスタンスに関連付けることもできます。インバウンドルールはインスタンスへの受信トラフィックを制御し、アウトバウンドルールはインスタンスからの送信トラフィックを制御します。

イメージ準備中のネットワーク設定の詳細については、イメージ準備中のネットワーク設定を参照してください。

インスタンスを起動する際、1つ以上のセキュリティグループを指定できます。セキュリティグループの設定については、セキュリティグループの設定を参照してください。

Microsoft Azure のセキュリティグループ

Citrix Virtual Apps and Desktopsは、Azureのネットワークセキュリティグループをサポートしています。ネットワークセキュリティグループはサブネットに関連付けられることが想定されています。詳細については、ネットワークセキュリティグループを参照してください。

イメージの準備中に作成されるネットワークセキュリティグループの詳細については、「Azure Resource Manager イメージを使用してマシンカタログを作成する」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#create-a-machine-catalog-using-an-azure-resource-manager-image-in-web-studio)を参照してください。

Google Cloud Platform のセキュリティグループ

マシンカタログの準備中に、カタログのマスターイメージシステムディスクとして機能するマシンイメージが準備されます。このプロセスが発生すると、ディスクは一時的に仮想マシンに接続されます。この VM は、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを防止する分離された環境で実行する必要があります。これは、すべてのトラフィックを拒否するファイアウォールルールによって実現されます。詳細については、「ファイアウォールルール」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create/create-machine-catalog-gcp.html#firewall-rules)を参照してください。

暗号化機能

暗号化機能は、共有仮想マシンホスト上の悪意のあるゲストによる攻撃や、ホスト上のすべての仮想マシンを管理するハイパーバイザー制御ソフトウェアによる攻撃から、仮想マシンのコンテンツを保護します。

サポートされているクラウドサービスの詳細については、以下を参照してください。

- AWSの暗号化機能
- Google Cloud Platformの暗号化機能
- Microsoft Azureの暗号化機能

AWSの暗号化機能

このセクションでは、AWS仮想化環境における暗号化機能について説明します。

自動暗号化

アカウントで作成された新しい Amazon EBS ボリュームとスナップショットコピーの自動暗号化を有効にできます。詳細については、「自動暗号化」を参照してください。

Google Cloud Platformの暗号化機能

このセクションでは、Google Cloud Platform (GCP) 仮想化環境における暗号化機能について説明します。

Google管理の暗号化キーが許可するよりもキー操作を詳細に制御する必要がある場合は、顧客管理の暗号化キーを使用できます。顧客管理の暗号化キーを使用する場合、オブジェクトがバケットに保存されるときにCloud Storageによってキーで暗号化され、リクエスターに提供されるときにCloud Storageによって自動的に復号化されます。詳細については、「顧客管理の暗号化キー」を参照してください。

MCSカタログには、顧客管理の暗号化キー (CMEK) を使用できます。詳細については、「顧客管理の暗号化キー (CMEK) の使用」を参照してください。

Microsoft Azureの暗号化機能

このセクションでは、Azure仮想化環境における暗号化機能について説明します。

Azureサーバー側暗号化

ほとんどのAzureマネージドディスクは、Azure Storage暗号化によって暗号化されています。これは、サーバー側暗号化（SSE）を使用してデータを保護し、セキュリティおよびコンプライアンスのコミットメントを満たすのに役立ちます。Citrix Virtual Apps and Desktopsは、Azure Key Vaultを介してAzureマネージドディスクの顧客管理暗号化キーをサポートしています。詳細については、「Azureサーバー側暗号化」を参照してください。

ホストでのAzureディスク暗号化

ホストでの暗号化機能を持つMCSマシンカタログを作成できます。

この暗号化方法は、Azureストレージを介してデータを暗号化しません。VMをホストするサーバーがデータを暗号化し、その後、暗号化されたデータがAzureストレージサーバーを介して流れます。したがって、この暗号化方法はデータをエンドツーエンドで暗号化します。

ホストでの暗号化機能を持つMCSマシンカタログの作成の詳細については、「ホストでのAzureディスク暗号化」を参照してください。

Azure二重暗号化

二重暗号化は、プラットフォーム側暗号化（デフォルト）と顧客管理暗号化（CMEK）です。したがって、暗号化アルゴリズム、実装、または侵害されたキーに関連するリスクを懸念する高セ

キュリティに敏感な顧客である場合は、この二重暗号化を選択できます。永続OSディスクとデータディスク、スナップショット、およびイメージはすべて、二重暗号化によって保存時に暗号化されます。詳細については、「マネージドディスクの二重暗号化」を参照してください。

Azure機密VM

Azure機密コンピューティングVMは、仮想デスクトップがメモリ内で暗号化され、使用中に保護されることを保証します。

MCSを使用して、Azure機密VMを含むカタログを作成できます。このようなカタログを作成するには、マシンプロファイルワークフローを使用する必要があります。VMとARMテンプレート仕様の両方をマシンプロファイル入力として使用できます。

詳細については、「Azure機密VM」を参照してください。

デリバリーグループの作成

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

> デリバリーグループは、1つ以上のマシンカタログから選択されたマシンのコレクションです。デリバリーグループは、どのユーザーがそれらのマシンを使用できるか、およびそれらのユーザーが利用できるアプリケーションとデスクトップを指定します。

デリバリーグループの作成は、サイトの作成とマシンカタログの作成に続く、展開の構成における次のステップです。後で、最初のデリバリーグループの初期設定を変更したり、他のデリバリーグループを作成したりできます。また、デリバリーグループの作成時ではなく、編集時にのみ構成できる機能や設定もあります。

Remote PC Accessの場合、サイトを作成すると、「Remote PC Access Desktops」という名前のデリバリーグループが自動的に作成されます。

デリバリーグループを作成するには：

1. デリバリーグループなしでサイトとマシンカタログを作成した場合、Web Studioはデリバリーグループを作成するための正しい開始場所に案内します。

2. すでにデリバリーグループを作成しており、別のデリバリーグループを作成する場合は、次の手順に従います。

   a. **Delivery Groups** を選択します。アクションペインで **Create Delivery Group** を選択します。

   b. フォルダーを使用してデリバリーグループを整理するには、デフォルトの **Delivery Groups** フォルダーの下にフォルダーを作成します。詳しくは、「フォルダーの作成」を参照してください。

   c. グループを作成するフォルダーを選択し、**Create Delivery Group** をクリックします。グループ作成ウィザードが開きます。

3. ウィザードは **Introduction** ページから起動します。このページは、次回以降のウィザード起動時に表示しないように設定できます。

4. ウィザードは、次のセクションで説明するページを順に案内します。各ページの作業が完了したら、最後のページに到達するまで **Next** をクリックします。

手順 1. マシン

マシンページで、カタログを選択し、そのカタログから使用するマシンの数を選択します。

知っておくと良いこと:

- 選択したカタログには、少なくとも1台のマシンが未使用のまま残っている必要があります。
- 1つのカタログを複数のデリバリーグループで指定できます。1台のマシンは1つのデリバリーグループでのみ使用できます。
- 1つのデリバリーグループは複数のカタログのマシンを使用できます。ただし、それらのカタログには同じマシンタイプ（マルチセッションOS、シングルセッションOS、またはRemote PCアクセス）が含まれている必要があります。つまり、デリバリーグループ内でマシンタイプを混在させることはできません。同様に、展開環境にWindowsマシンのカタログとLinuxマシンのカタログがある場合、デリバリーグループにはどちらかのOSタイプのマシンを含めることはできますが、両方を含めることはできません。
- Citrixでは、すべてのマシンに最新のVDAバージョンをインストールまたはアップグレードすることを推奨しています。必要に応じて、カタログとデリバリーグループをアップグレードしてください。デリバリーグループを作成する際に、異なるVDAバージョンがインストールされているマシンを選択した場合、デリバリーグループは最も古いVDAバージョンと互換性があります。これはグループの*機能レベル*と呼ばれます。たとえば、マシンの1つにVDAバージョン7.1がインストールされており、他のマシンに現在のバージョンがインストールされている場合、グループ内のすべてのマシンはVDA 7.1でサポートされていた機能のみを使用できます。これ

は、より新しいVDAバージョンを必要とする一部の機能が、そのデリバリーグループでは利用できない可能性があることを意味します。

- Remote PCアクセス カタログ内の各マシンは、自動的にデリバリーグループに関連付けられます。Remote PCアクセスサイトを作成すると、「Remote PC Access Machines」という名前のカタログと「Remote PC Access Desktops」という名前のデリバリーグループが自動的に作成されます。
- 以下の互換性チェックが実行されます:
  - MinimumFunctionalLevelは互換性がある必要があります。
  - SessionSupportは互換性がある必要があります。
  - AllocationTypeはSingleSessionと互換性がある必要があります。
  - ProvisioningTypeは互換性がある必要があります。
  - PersistChangesはMCSおよびCitrix Provisioning™と互換性がある必要があります。
  - RemotePCカタログはRemote PCアクセス カタログとのみ互換性があります。
  - AppDisk関連のチェック

ステップ 2. 負荷分散

デリバリーグループの作成中に負荷分散設定を構成するには：

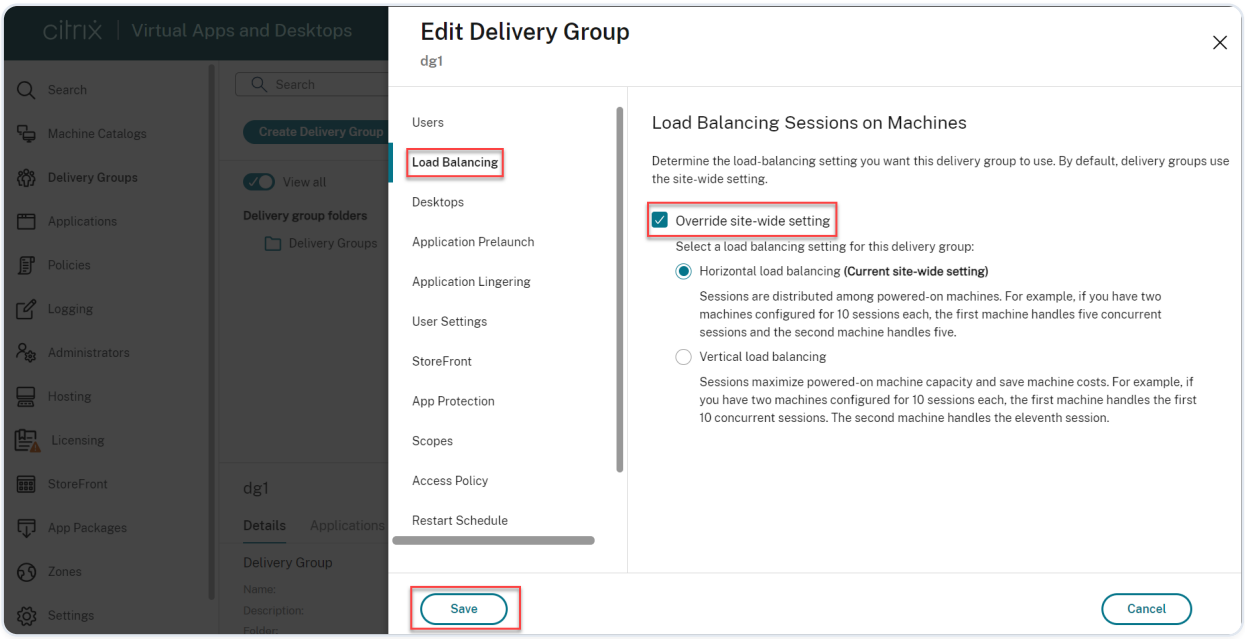
1. Web Studioにサインインします。
2. 左側のナビゲーションで、**Delivery Groups**をクリックします。
3. **Delivery Groups**ページで、**Create Delivery Group**をクリックします。
4. **Create Delivery Group**ウィザードで、**Next**をクリックします。**Machine**ウィザードが開きます。
5. **Machines**ウィザードで、必要なマシンカタログを選択し、**Next**をクリックします。**Load Balancing**ウィザードが開きます。
6. **Load Balancing**ウィザードで、**Override site-wide setting**チェックボックスを選択します。
7. 必要に応じて、**Horizontal load balancing**または**Vertical load balancing**オプションを選択し、**Next**をクリックします。

   デリバリーグループ作成時の負荷分散設定(/en-us/citrix-virtual-apps-desktops/2407/media/load-balance-create-delivery-group.png)

既存のデリバリーグループの編集中に負荷分散設定を構成するには：

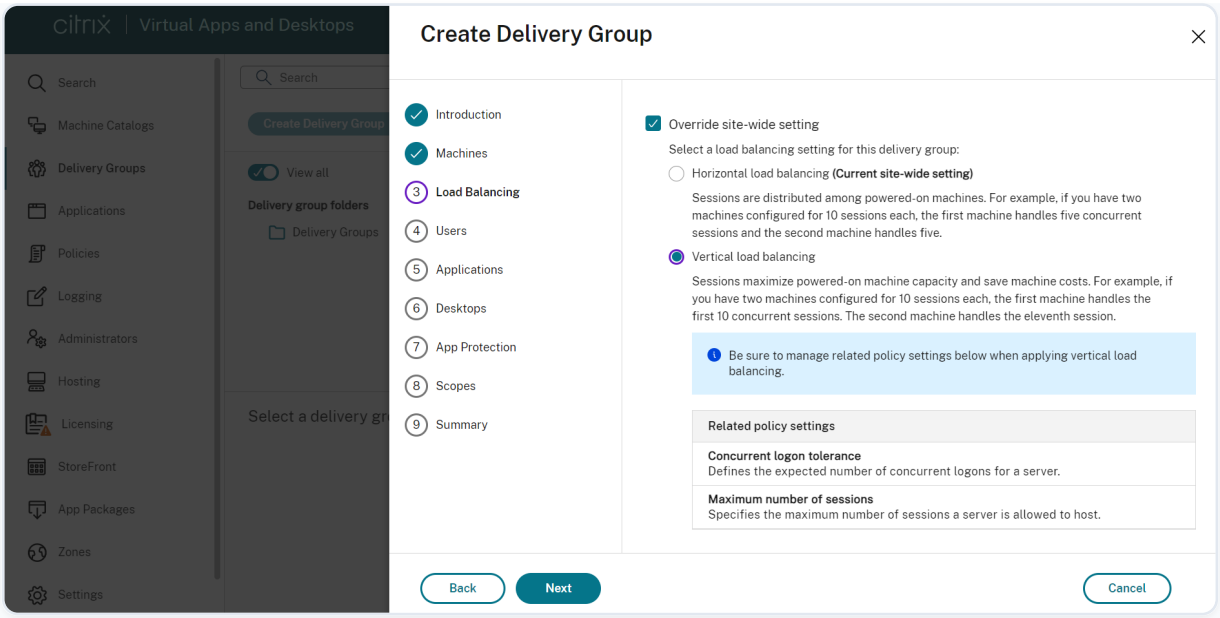
1. Web Studioにサインインします。

2. 左側のペインで、**Delivery Groups**をクリックします。
3. リストから**Delivery Group**を選択し、**Edit**をクリックします。**Edit Delivery Group**ウィザードが開きます。
4. **Edit Delivery Group**ページで、**Load Balancing**をクリックします。
5. **サイト全体の構成を上書き**チェックボックスをオンにします。
6. 必要に応じて、**水平ロードバランシング**または**垂直ロードバランシング**のいずれかのオプションを選択し、**保存**をクリックします。



注:

垂直ロードバランシング設定が適用されている場合、**同時ログオン許容数**および**最大セッション数**ポリシーが適切に構成されていることを確認してください。



サイトおよびデリバリーグループレベルでの負荷分散について詳しくは、「マシンの負荷分散」を参照してください。

手順3. デリバリーの種類

このページは、静的（割り当て済み）シングルセッションOSマシンを含むカタログを選択した場合にのみ表示されます。

デリバリーの種類ページで、**アプリケーション**または**デスクトップ**のいずれかを選択します。両方を有効にすることはできません。

マルチセッションOSまたはシングルセッションOSのランダム（プール）カタログからマシンを選択した場合、デリバリーの種類はアプリケーションとデスクトップであると見なされます。アプリケーション、デスクトップ、またはその両方をデリバリーできます。

手順4. ユーザー

デリバリーグループ内のアプリケーションとデスクトップを使用できるユーザーとユーザーグループを指定します。

ユーザーリストの指定場所

Active Directoryユーザーリストは、以下を作成または編集するときに指定されます。

- サイトのユーザーアクセスリスト（Web Studioでは構成されません）。デフォルトでは、アプリケーションエンタイトルメントポリシーのルールにはすべてのユーザーが含まれます。詳細については、PowerShell SDKの`BrokerAppEntitlementPolicyRule`コマンドレットを参照してください。

- アプリケーショングループ（構成されている場合）。
- デリバリーグループ。
- アプリケーション。

StoreFront™を介してアプリケーションにアクセスできるユーザーのリストは、上記のユーザーリストの共通部分によって形成されます。たとえば、他のグループへのアクセスを不必要に制限することなく、特定の部門にアプリケーションAの使用を構成するには、次のようにします。

- すべてのユーザーを含むデフォルトのアプリケーションエンタイトルメントポリシーのルールを使用します。
- デリバリーグループのユーザーリストを構成して、すべての本社ユーザーがデリバリーグループで指定された任意のアプリケーションを使用できるようにします。
- （アプリケーショングループが構成されている場合）アプリケーショングループのユーザーリストを構成して、管理および財務部門のメンバーがアプリケーションAからLにアクセスできるようにします。
- アプリケーションAのプロパティを構成して、その可視性を管理および財務部門の売掛金担当者のみに制限します。

認証済みユーザーと未認証ユーザー

ユーザーには、認証済みと未認証の2種類があります（未認証は匿名とも呼ばれます）。デリバリーグループでは、いずれか一方または両方のタイプを構成できます。

- **認証済み:** アプリケーションやデスクトップにアクセスするには、指定したユーザーおよびグループメンバーが、スマートカードやユーザー名とパスワードなどの資格情報をStoreFrontまたはCitrix Workspace™アプリに提示する必要があります。シングルセッションOSマシンを含むデリバリーグループの場合、後でデリバリーグループを編集してユーザーデータ（ユーザーのリスト）をインポートできます。
- **未認証（匿名）:** マルチセッションOSマシンを含むデリバリーグループの場合、ユーザーがStoreFrontまたはCitrix Workspaceアプリに資格情報を提示することなく、アプリケーションやデスクトップにアクセスできるようにすることができます。たとえば、キオスクではアプリケーションが資格情報を要求する場合がありますが、Citrixアクセス ポータルやツールは要求しません。最初のDelivery Controllerをインストールすると、匿名ユーザーグループが作成されます。

  未認証ユーザーにアクセスを許可するには、デリバリーグループ内の各マシンにWindows Server OS用VDA（最小バージョン7.6）がインストールされている必要があります。未認証ユーザーが有効になっている場合、未認証のStoreFrontストアが必要です。

未認証ユーザーアカウントは、セッションが起動されるとオンデマンドで作成され、Anon*XYZ*という名前が付けられます。ここで*XYZ*は一意の3桁の値です。

認証されていないユーザーセッションには、デフォルトで10分間のアイドルタイムアウトがあり、クライアントが切断されると自動的にログオフされます。再接続、クライアント間のローミング、およびWorkspace Controlはサポートされていません。

次の表は、**ユーザー**ページでの選択肢を示しています。

アクセスを有効にする対象	ユーザーとユーザーグループを追加/割り当てますか？	「認証されていないユーザーにアクセスを許可する」チェックボックスを有効にしますか？
認証済みユーザーのみ	はい	いいえ
認証されていないユーザーのみ	いいえ	はい
認証済みユーザーと未認証ユーザーの両方	はい	はい

ステップ5. アプリケーション

ご参考：

- 既定では、追加する新しいアプリケーションは「Applications」という名前のフォルダーに配置されます。別のフォルダーを指定することもできます。詳細については、「アプリケーションの管理」の記事を参照してください。
- アプリケーションをデリバリーグループに追加するとき、または後で、そのアプリケーションのプロパティを変更できます。詳細については、「アプリケーションの管理」の記事を参照してください。
- アプリケーションを追加しようとして、そのフォルダーに同じ名前のアプリケーションが存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。拒否した場合、そのアプリケーションフォルダー内で一意になるようにサフィックスが付けられてアプリケーションが追加されます。
- 複数のデリバリーグループにアプリケーションを追加する場合、それらのすべてのデリバリーグループでアプリケーションを表示するための十分な権限がないと、表示の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが追加されたすべてのデリバリーグループを含むようにスコープを拡張してもらってください。

- 同じ名前の2つのアプリケーションを同じユーザーに公開する場合は、Web Studioでアプリケーション名（ユーザー向け）プロパティを変更してください。そうしないと、ユーザーはCitrix Workspaceアプリで重複した名前を目にすることになります。
- パッケージ化されたアプリケーションを、シングルセッションの静的デリバリーグループおよびRemote PC Accessデリバリーグループに追加できます。これらのパッケージは、ユーザーがデスクトップまたはリモートPCにサインインするたびに自動的にマウントされます。

追加をクリックして、アプリケーションソースを表示します。

- **スタートメニューから：** 選択したカタログのマスターイメージから作成されたマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションを選択し、**OK**をクリックします。
- **手動で：** デリバリーグループ内のVDAまたはネットワーク上の別の場所にあるアプリケーション。このソースを選択すると、次の方法で追加するアプリケーションを指定する新しいページが開きます。
  - 実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、および管理者とユーザーの表示名を入力します。
  - デリバリーグループ内のVDAからアプリケーションを選択します。これを行うには、**参照**をクリックし、VDAにアクセスするための資格情報を入力し、VDAに接続されるまで待ってから、VDAからアプリケーションを選択します。選択したアプリケーションのプロパティが、ページ上のフィールドに自動的に入力されます。
- **既存：** 以前にサイトに追加されたアプリケーション（おそらく別のデリバリーグループ内）。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。アプリケーションを追加し、**OK**をクリックします。
- **アプリケーションパッケージ：** App-V、MSIX、またはMSIX app attachアプリケーションパッケージ内のアプリケーション。このソースを選択すると、ソースの種類を選択し、結果の表示から追加するアプリケーションを選択できる新しいページが起動します。

アプリケーションソースまたはアプリケーションが利用できないか無効な場合、表示されないか、選択できません。たとえば、サイトにアプリケーションが追加されていない場合、**既存**ソースは利用できません。または、アプリケーションが選択したカタログ内のマシンでサポートされているセッションタイプと互換性がない場合があります。

ステップ6. デスクトップ

このページのタイトルは、**マシン**ページで選択したカタログによって異なります。

- プールされたマシンを含むカタログを選択した場合、このページのタイトルは**デスクトップ**です。
- シングルセッションの静的マシンを含むカタログを選択し、**配信の種類**ページで「デスクトップ」を指定した場合、このページのタイトルは**デスクトップユーザー割り当て**です。
- シングルセッションの静的マシンを含むカタログを選択し、**配信の種類**ページで「アプリケーション」を指定した場合、このページのタイトルは**アプリケーションマシンユーザー割り当て**です。

追加をクリックします。ダイアログボックスで、次のようにします。

- 表示名と説明のフィールドに、Citrix Workspaceアプリに表示される情報を入力します。
- デスクトップにタグ制限を追加するには、**このタグを持つマシンへの起動を制限する**を選択し、ドロップダウンリストからタグを選択します。詳しくは、「タグ」を参照してください。
- ラジオボタンを使用して、デスクトップを起動するか、デスクトップの起動時にマシンを割り当てます。ユーザーは、このデリバリーグループにアクセスできるすべてのユーザー、または特定のユーザーとユーザーグループのいずれかです。
- グループにシングルセッションの静的マシンが含まれている場合は、ユーザーあたりのデスクトップの最大数を指定します。これは1以上の値である必要があります。
- デスクトップ（プールされたマシンの場合）またはデスクトップ割り当てルール（シングルセッションの静的マシンの場合）を有効または無効にします。デスクトップを無効にすると、デスクトップの配信が停止します。デスクトップ割り当てルールを無効にすると、ユーザーへのデスクトップの自動割り当てが停止します。
- ダイアログボックスでの作業が完了したら、**OK**をクリックします。

サイト内のデスクトップの最大インスタンス数（PowerShellのみ）

サイト内のデスクトップの最大インスタンス数を構成するには（PowerShellのみ）：

- PowerShellで、適切なBrokerEntitlementPolicyRuleコマンドレットをMaxPerEntitlementInstancesパラメーターとともに使用します。たとえば、次のコマンドレットは`tsvda-desktop`ルールを変更して、サイトで許可されるデスクトップの同時実行インスタンスの最大数を2に設定します。2つのデスクトップインスタンスが実行されているときに、3番目のサブスクライバーがデスクトップを起動しようとすると、エラーが発生します。

  ```
  Set-BrokerEntitlementPolicyRule -Name tsvda-desktop
  -MaxPerEntitlementInstances 2
  ```

- ガイダンスについては、Get-Help コマンドレットを使用してください。例: `Get-Help Set-BrokerEntitlementPolicyRule-Parameter MaxPerEntitlementInstances`。

手順7：ローカルホストキャッシュ設定

この設定は、電源管理されたシングルセッションのプールされたマシンを含むデリバリーグループにのみ表示されます。

デフォルトでは、これらのマシンはデータ漏洩のリスクがあるため、ローカルホストキャッシュ (LHC) モードでは利用できません。デフォルトの動作を変更し、LHC モードで新しいユーザー接続に利用できるようにするには、**リソースを常に利用可能にする** を選択します。

または、PowerShell コマンドを使用してデフォルトの動作を変更することもできます。詳細については、「アプリケーションとデスクトップのサポート」を参照してください。

> **重要:**
>
> 電源管理されたシングルセッションのプールされたマシンへのアクセスを有効にすると、以前のユーザーセッションからのデータや変更が、後続のセッションに存在する可能性があります。

手順8：概要

デリバリーグループの名前を入力します。また、(オプションで) 説明を入力することもできます。この説明は、Citrix Workspace アプリおよび Web Studio に表示されます。

概要情報を確認し、**「完了」**をクリックします。

デリバリーグループを管理する

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

はじめに

この記事では、管理コンソールからデリバリーグループを管理する手順について説明します。グループ作成時に指定した設定を変更するだけでなく、デリバリーグループ作成時には利用できないその他の設定も構成できます。

手順のカテゴリには、全般、ユーザー、マシン、セッションがあります。一部のタスクは複数のカテゴリにまたがります。たとえば、「ユーザーがマシンに接続できないようにする」はマシンのカテゴリで説明されていますが、ユーザーにも影響します。あるカテゴリでタスクが見つからない場合は、関連するカテゴリを確認してください。

その他の関連情報を含む記事は次のとおりです。

- アプリケーションには、デリバリーグループ内のアプリケーションの管理に関する情報が含まれています。
- デリバリーグループの管理には、Delivery Group Administratorの組み込みロール権限が必要です。詳細については、「委任管理」を参照してください。

全般

- グループの詳細を表示する
- デリバリーの種類を変更する
- StoreFront™アドレスを変更する
- 機能レベルを変更する
- Remote PC Accessデリバリーグループを管理する
- フォルダを使用してデリバリーグループを整理する(#organize-delivery-groups-using-folders)
- アプリ保護を管理する(#manage-app-protection)

グループの詳細を表示

1. 検索機能を使用して特定のデリバリーグループを検索します。手順については、「インスタンスの検索」を参照してください。
2. 検索結果から、必要に応じてグループを選択します。
3. グループ列の説明については、次の表を参照してください。
4. このグループの詳細については、下部の詳細ペインにあるタブをクリックしてください。

列	説明
デリバリーグループ	グループ名とセッションの種類。セッションの種類には、シングルセッションOSとマルチセッションOSがあります。
配信	このグループから配信されるリソースの種類。指定できる値には、アプリケーション、デスクトップ、およびアプリケーションとデスクトップがあります。デリバリーグループが専用マシンで構成されている場合は、「静的マシン割り当て」と表示されます。
使用中のセッション	セットアップされているマシンの数と、切断状態にあるマシンの数。
割り当て済み数	デリバリーグループに割り当てられたカタログ内のマシンの数。
フォルダー	**デリバリーグループ**ツリー内でのグループの場所。グループが存在するフォルダーの名前（末尾のバックスラッシュを含む）が表示されます。グループがルートレベルにある場合は `-` と表示されます。

デリバリーグループのデリバリータイプを変更する

デリバリータイプは、グループが提供できるもの（アプリケーション、デスクトップ、またはその両方）を示します。

アプリケーションのみまたは**デスクトップとアプリケーション**タイプを**デスクトップのみ**タイプに変更する前に、グループからすべてのアプリケーションを削除してください。

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. **デリバリータイプ**ページで、目的のデリバリータイプを選択します。
4. **適用**をクリックして変更を適用し、ウィンドウを開いたままにします。または、**保存**をクリックして変更を適用し、ウィンドウを閉じます。

StoreFrontアドレスを変更する

1. 左ペインで**デリバリーグループ**を選択します。

2. グループを選択し、アクションバーで**編集**をクリックします。
3. **StoreFront**ページで、StoreFront URLを選択または追加します。これらのURLは、デリバリーグループ内の各マシンにインストールされているCitrix Workspace™アプリによって使用されます。
4. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

左側のペインで**StoreFront**を選択して、StoreFrontサーバーアドレスを指定することもできます。

機能レベルを変更する

デリバリーグループの機能レベルは、そのマシン上のVDAと、デリバリーグループで使用されているマシンを含むマシンカタログをアップグレードした後に変更します。

開始する前に：

- Citrix Provisioning™（旧Provisioning Services）を使用している場合は、Citrix Provisioningコンソールで VDAバージョンをアップグレードします。
- アップグレードされたVDAを含むマシンを起動し、Delivery Controllerに登録できるようにします。このプロセスにより、デリバリーグループで何がアップグレードされる必要があるかがコンソールに通知されます。
- 以前のVDAバージョンを引き続き使用する必要がある場合、新しい製品機能は利用できません。詳しくは、アップグレードのドキュメントを参照してください。

デリバリーグループの機能レベルを変更するには：

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**機能レベルの変更**をクリックします。**機能レベルの変更**アクションは、アップグレードされたVDAが検出された場合にのみ表示されます。
3. **変更**をクリックします。

表示には、機能レベルに変更できないマシンがある場合、そのマシンと理由が示されます。その後、変更アクションをキャンセルし、マシンの問題を解決してから、変更アクションを再度実行できます。

変更が完了したら、マシンを以前の状態に戻すことができます。デリバリーグループを選択し、アクションバーで**機能レベルの変更を元に戻す**を選択します。

リモートPCアクセスデリバリーグループの管理

Remote PC Accessマシンカタログ内のマシンが割り当てられていない場合、そのマシンは一時的にそのカタログに関連付けられたデリバリーグループに割り当てられます。この一時的な割り当てにより、後でマシンをユーザーに割り当てることができます。

デリバリーグループとマシンカタログの関連付けには優先度値があります。優先度は、マシンがシステムに登録されるとき、またはユーザーがマシンの割り当てを必要とするときに、マシンの割り当てられたデリバリーグループを決定します。値が小さいほど、優先度が高くなります。Remote PC Access マシンカタログに複数のデリバリーグループ割り当てがある場合、ソフトウェアは最も優先度の高い一致を選択します。この優先度値を設定するには、PowerShell SDK を使用します。

最初に作成されたとき、Remote PC Access マシンカタログはデリバリーグループに関連付けられます。後でカタログに追加されたマシンアカウントまたは組織単位は、デリバリーグループに追加できます。この関連付けは、オン/オフを切り替えることができます。

Remote PC Accessマシンカタログとデリバリーグループの関連付けを追加または削除するには：

1. 左ペインで を選択します。
2. Remote PC Access グループを選択します。
3. セクションで、 タブをクリックし、Remote PC Access カタログを選択します。
4. 関連付けを追加または復元するには、 をクリックします。関連付けを削除するには、 をクリックします。

フォルダーを使用したデリバリーグループの整理

デリバリーグループに簡単にアクセスできるように、フォルダーを作成できます。

必要な役割

デフォルトでは、デリバリーグループフォルダーを作成および管理するには、Cloud Administrator、Full Administrator、またはDelivery Group Administratorの組み込み役割が必要です。必要に応じて、デリバリーグループフォルダーの作成と管理のための役割をカスタマイズできます。詳しくは、「必要な権限」を参照してください。

デリバリーグループフォルダーを作成する

開始する前に、デリバリーグループの整理方法を計画してください。次の点を考慮してください。

- フォルダーは最大5レベルまでネストできます（デフォルトのルートフォルダーを除く）。
- フォルダーには、デリバリーグループとサブフォルダーを含めることができます。

- すべてのノード（**マシンカタログ**、**アプリケーション**、**デリバリーグループ**などのノード）は、バックエンドでフォルダーツリーを共有しています。フォルダーの名前変更や移動時に他のノードとの名前の競合を避けるため、異なるノードの第一レベルフォルダーには異なる名前を付けることをお勧めします。

デリバリーグループフォルダーを作成するには、次の手順に従います。

1. 左側のペインで**デリバリーグループ**を選択します。
2. フォルダー階層でフォルダーを選択し、**アクション**バーで **Create Folder** を選択します。
3. 新しいフォルダーの名前を入力し、**Done** をクリックします。

> **ヒント:**
>
> 意図しない場所にフォルダーを作成してしまった場合は、正しい場所にドラッグできます。

デリバリーグループを移動する

デリバリーグループはフォルダー間で移動できます。詳細な手順は次のとおりです。

1. 左側のペインで**デリバリーグループ**を選択します。
2. フォルダーごとにグループを表示します。フォルダー階層の上にある **View all** をオンにすると、すべてのグループを一度に表示することもできます。
3. グループを右クリックし、**Move Delivery Group** を選択します。
4. グループを移動するフォルダーを選択し、**Done** をクリックします。

> **ヒント:**
>
> グループをフォルダーにドラッグできます。

デリバリーグループフォルダーの管理

デリバリーグループフォルダーを削除、名前変更、移動できます。

フォルダーとそのサブフォルダーにデリバリーグループが含まれていない場合にのみ、フォルダーを削除できることに注意してください。

フォルダーを管理するには、次の手順に従います。

1. 左ペインで**デリバリーグループ**を選択します。
2. フォルダー階層でフォルダーを選択し、必要に応じて**アクション**バーでアクションを選択します。
   - フォルダーの名前を変更するには、**フォルダー名の変更**を選択します。
   - フォルダーを削除するには、**フォルダーの削除**を選択します。
   - フォルダーを移動するには、**フォルダーの移動**を選択します。
3. 画面の指示に従って、残りの手順を完了してください。

必要な権限

次の表に、デリバリーグループフォルダーに対してアクションを実行するために必要な権限を示します。

アクション	必要な権限
デリバリーグループフォルダーを作成する	デリバリーグループフォルダーを作成
デリバリーグループフォルダーを削除する	デリバリーグループフォルダーを削除
デリバリーグループフォルダーを移動する	デリバリーグループフォルダーを移動
デリバリーグループフォルダーの名前を変更する	デリバリーグループフォルダーを編集
デリバリーグループをフォルダーに移動する	デリバリーグループフォルダーを編集およびデリバリーグループのプロパティを編集

アプリ保護の管理

以下の情報は、アプリ保護 を補足するものです。以下の詳細に注意してください。

- 有効なアプリ保護の資格が必要です。アプリ保護機能を購入するには、Citrix の営業担当者にお問い合わせください。
- アプリ保護には XML 信頼が必要です。XML 信頼を有効にするには、**設定 > XML 信頼を有効にする** に移動します。
- 画面キャプチャ防止について：
  - Windows および macOS では、保護されたコンテンツのウィンドウのみが空白になります。保護されたウィンドウが最小化されていない場合、アプリ保護はアクティブになります。

- Linux では、キャプチャ全体が空白になります。保護されたウィンドウが最小化されているかどうかにかかわらず、アプリ保護はアクティブになります。

デリバリーグループのアプリ保護方法を選択するには、次の手順に従います。

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**を選択します。
3. **App Protection**ページには、次のオプションが表示されます。

オプション	説明
適用しない	設定を適用しない場合は、このオプションを選択します。
このデリバリーグループに適用	**キーロギング対策**および/または**キーキャプチャ対策**オプションを選択します。これらの各設定にカーソルを合わせると、ツールチップに詳細が表示されます。
コンテキストに応じて適用	この設定を適用するには、**アクセスポリシー設定**ページでアクセスポリシーを構成します。
	1. 左ペインで**アクセス ポリシー**をクリックし、**追加**をクリックします。
	1. **ポリシーの追加**ページで、次の操作を行います。
	- i. **ポリシー名**を入力し、必要に応じて設定を構成します。
	- ii. **フィルター**フィールドと**値**フィールドに詳細を入力し、**完了**をクリックします。新しいポリシーが**アプリ保護**ページに表示されます。このポリシーに必要な設定を有効にします。
	- iii. **保存**をクリックします。

4. **デリバリーグループ**ページで、**デリバリーグループ**を選択し、下部にある**詳細**タブをクリックします。適用された新しい**アプリ保護**設定が表示されます。

ユーザー

このセクションでは、次のトピックについて説明します。

- ユーザー設定の変更
- ユーザーの追加または削除
- ユーザー割り当ての管理

デリバリーグループのユーザー設定を変更する

このページの名前は、 または のいずれかで表示されます。

1. 左側のペインで を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. (または) ページで、次の表の設定を変更します。
4. をクリックして変更を適用し、ウィンドウを開いたままにします。または、 をクリックして変更を適用し、ウィンドウを閉じます。

設定	説明
説明	Citrix Workspace (またはStoreFront) が使用し、ユーザーに表示されるテキスト。
デリバリーグループを有効にする	デリバリーグループが有効になっているかどうか。
タイムゾーン	このデリバリーグループのマシンが存在する必要があるタイムゾーン。このオプションには、サイトでサポートされているタイムゾーンが一覧表示されます。**注：**デリバリーグループのタイムゾーンを変更すると、そのデリバリーグループ内のマシンが再起動する可能性があります。これを回避するには、稼働時間外にタイムゾーン設定を変更してください。
Secure ICA® を有効にする	SecureICA を使用してデリバリーグループ内のマシンとの間の通信を保護します。SecureICA は ICA プロトコルを暗号化します。デフォルトのレベルは 128 ビットです。レベルは SDK を使用して変更できます。Citrix は、パブリックネットワークを通過する際に TLS 暗号化などのより多くの暗号化方法を使

設定	説明
	用することを推奨します。また、SecureICA はデータ整合性をチェックしません。

デリバリーグループでのユーザーの追加または削除

ユーザーの詳細については、「 (/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/delivery-groups-create.html#step-3-users)」を参照してください。

1. 左ペインで を選択します。
2. グループを選択し、アクションバーの をクリックします。
3. ページで、次の操作を行います。
   - ユーザーを追加するには、 をクリックし、追加するユーザーを指定します。
   - ユーザーを削除するには、1人以上のユーザーを選択し、 をクリックします。
   - 認証されていないユーザーによるアクセスを許可するには、チェックボックスをオンまたはオフにします。
4. 行った変更を適用してウィンドウを開いたままにするには、 をクリックします。または、変更を適用してウィンドウを閉じるには、 をクリックします。

ユーザーリストのインポートまたはエクスポート

物理的なシングルセッションOSマシンを含むデリバリーグループの場合、デリバリーグループの作成後に.csvファイルからユーザー情報をインポートできます。ユーザー情報を.csvファイルにエクスポートすることもできます。.csvファイルには、以前の製品バージョンのデータを含めることができます。

CSVファイルの最初の行には、コンマで区切られた2つの列ヘッダーが含まれている必要があります。最初のヘッダーが `Machine Account` で、2番目のヘッダーが `User Names` であることを確認してください。（追加のヘッダーを含めることもできますが、サポートされていません。）ファイルの以降の行には、コンマ区切りのデータが含まれます。`Machine Account` エントリは、コンピューターSID、FQDN、またはドメインとコンピューター名のペアにすることができます。

ユーザー情報をインポートまたはエクスポートするには：

1. 左ペインで を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。

3. **マシン割り当て**ページで、**リストのインポート**または**リストのエクスポート**を選択し、ファイルの場所を参照します。
4. **適用**をクリックして変更を適用し、ウィンドウを開いたままにします。または、**保存**をクリックして変更を適用し、ウィンドウを閉じます。

ユーザー割り当ての管理

デリバリーグループ内のマシンのユーザー割り当てを管理します。デリバリーグループにデスクトップ割り当てルールが構成されている場合、マシンは最初のデスクトップ起動時にユーザーにランダムに割り当てられ、ユーザー割り当てが変更されない限り、ユーザーに割り当てられたままになります。割り当てられていないマシンを特定のユーザーに手動で割り当てたい場合、またはマシンの既存のユーザー割り当てを変更したい場合は、このトピックで説明されている手順に従って変更を行います。これらの手順を使用すると、ユーザーに割り当てられたマシンのCitrix Workspaceアプリに表示される名前を変更することもできます。

詳細な手順は次のとおりです。

1. コンソールで、左側のペインから**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**を選択します。
3. 左側のペインで、**マシン割り当て**を選択します。グループ内の各マシンの次の詳細が表示されます。

    - **マシン名:** マシンの名前を表示します。
    - **表示名:** Citrix Workspaceアプリでのマシンの表示名を表示します。
    - **ユーザー:** このマシンに割り当てられているユーザーを表示します。デスクトップ割り当てルールが構成されている場合、マシンは最初のデスクトップ起動時にユーザーにランダムに割り当てられ、ユーザー割り当てが変更されない限り、ユーザーに割り当てられたままになります。

4. マシンを見つけて、ユーザーを割り当てるか、ユーザー割り当てを変更します。

    - **参照**をクリックしてユーザーを参照します。
    - **ユーザー**列に、セミコロンで区切られたユーザー名のリストを入力します。
    - CSVファイルを使用して設定の詳細をインポートするには、「**CSVファイルからインポート**」をクリックします。

5. (オプション) マシンがユーザーに割り当てられている場合は、必要に応じて表示名を変更します。

注:

表示名フィールドは、マシンがユーザーに割り当てられている場合にのみ有効になります。

- マシンがデスクトップ割り当てルールに基づいてユーザーに割り当てられている場合、このフィールドにはそのルールで構成された表示名が表示されます。
- マシンが手動でユーザーに割り当てられ、フィールドが空白のままの場合、デリバリーグループの公開名（指定されている場合）がマシンの表示名として使用されます。公開名が指定されていない場合は、デリバリーグループの名前が使用されます。デリバリーグループの公開名はPowerShell経由でのみ指定できることに注意してください。

6. 変更を適用してウィンドウを開いたままにするには、**適用**を選択します。または、変更を適用してウィンドウを閉じるには、**OK**を選択します。

マシン

- マシンからユーザーへの割り当てを変更する
- 電源管理されたシングルセッションのプールされたVDAでローカルホストキャッシュを有効にする
- ユーザーあたりの最大マシン数を変更する
- マシンを更新する
- デスクトップのタグ制限を追加、変更、または削除する
- マシンを削除する
- マシンへのアクセスを制限する
- ユーザーがマシンに接続するのを防ぐ（メンテナンスモード）
- マシンをシャットダウンして再起動する
- マシンの再起動スケジュールを作成および管理する
- 1回限りの再起動スケジュールを有効にする
- 管理対象マシンをロードする
- 管理対象マシンの電源を管理する

デリバリーグループ内のマシンからユーザーへの割り当てを変更する

MCSでプロビジョニングされたシングルセッションOSマシンの割り当てを変更できます。マルチセッションOSマシンまたはCitrix Provisioningでプロビジョニングされたマシンの割り当ては変更できません。

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. **デスクトップ**または**デスクトップ割り当てルール**ページ（ページタイトルは、デリバリーグループが使用するマシンカタログの種類によって異なります）で、新しいユーザーを指定します。
4. 加えた変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

電源管理されたシングルセッションプールVDAのローカルホストキャッシュを有効にする

デフォルトでは、電源管理されたシングルセッションのプールされたマシンは、ローカルホストキャッシュモードでは使用できません。デリバリーグループごとにデフォルトの動作を上書きできます。詳細な手順は次のとおりです。

1. Studioで、左側のペインで**デリバリーグループ**を選択します。

   グループリストでは、MCSまたはCitrix Provisioningによってプロビジョニングされたシングルセッションのプールされたマシンを含むグループに警告アイコンが表示されます。
2. 必要に応じてグループを選択し、アクションバーで**編集**を選択します。
3. 「**ローカルホストキャッシュ**」ページで、**リソースを常に利用可能にする**を選択します。
4. 加えた変更を適用してウィンドウを開いたままにするには、**適用**を選択します。または、変更を適用してウィンドウを閉じるには、**OK**を選択します。

または、PowerShellコマンドを使用してデフォルトの動作を上書きすることもできます。詳細については、「アプリケーションとデスクトップのサポート」を参照してください。

> **重要:**
>
> 電源管理されたシングルセッションのプールされたマシンへのアクセスを有効にすると、以前のユーザーセッションのデータと変更が後続のセッションに存在する可能性があります。

デリバリーグループ内のユーザーあたりの最大マシン数を変更する

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. 「**デスクトップ割り当てルール**」ページで、ユーザーあたりの最大デスクトップ数を設定します。
4. 加えた変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

デリバリーグループ内のマシンを更新する

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**マシンの表示**をクリックします。
3. マシンを選択し、アクションバーの **「マシンの更新」** をクリックします。

別のイメージを選択するには、**「イメージ」** を選択してからスナップショットを選択します。

変更を適用してマシンユーザーに通知するには、**「エンドユーザーへのロールアウト通知」** を選択します。次に、以下を指定します。

- マスターイメージを更新するタイミング：今すぐ、または次回の再起動時
- 再起動の配布時間（グループ内のすべてのマシンの更新を開始するまでの合計時間）
- ユーザーに再起動が通知されるかどうか
- ユーザーが受信するメッセージ

デスクトップのタグ制限を追加、変更、または削除する

タグ制限の追加、変更、削除は、起動対象となるデスクトップに予期せぬ影響を与える可能性があります。「タグ」の考慮事項と注意点を確認してください。

1. 左ペインで **「デリバリーグループ」** を選択します。
2. グループを選択し、アクションバーの **「編集」** をクリックします。
3. **「デスクトップ」** ページで、デスクトップを選択し、**「編集」** をクリックします。
4. タグ制限を追加するには、**「タグを持つマシンへの起動を制限する」** を選択し、タグを選択します。
5. タグ制限を変更または削除するには、次のいずれかを実行します。
    - 別のタグを選択します。
    - 「**このタグを持つマシンへの起動を制限する**」をクリアして、タグの制限を削除します。

6. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

デリバリーグループからマシンを削除する

マシンを削除すると、デリバリーグループから削除されます。デリバリーグループが使用するマシンカタログからは削除されません。したがって、そのマシンは別のデリバリーグループに割り当てることができます。

マシンは、削除する前にシャットダウンする必要があります。マシンを削除している間、ユーザーがマシンに接続するのを一時的に停止するには、シャットダウンする前にマシンをメンテナンスモードにします。

マシンには個人データが含まれている可能性があるため、別のユーザーにマシンを割り当てる前に注意してください。マシンの再イメージングを検討してください。

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**マシンの表示**をクリックします。
3. マシンがシャットダウンされていることを確認します。
4. マシンを選択し、アクションバーで**デリバリーグループから削除**をクリックします。

マシンが使用する接続を介して、デリバリーグループからマシンを削除することもできます。

デリバリーグループ内のマシンへのアクセスを制限する

デリバリーグループ内のリソースへのアクセスを制限するために行った変更は、使用する方法に関係なく、以前の設定に優先します。次のことができます。

- **委任管理スコープを使用して管理者へのアクセスを制限する:** 管理者がすべてのアプリケーションにアクセスすることを許可するスコープと、特定のアプリケーションにのみアクセスを提供する別のスコープを作成して割り当てることができます。詳細については、「委任管理」を参照してください。
- **スマートアクセスポリシー式を介してユーザーのアクセスを制限する:** 特定のデリバリーグループへのユーザーアクセスを制御するために、アクセスポリシー規則を構成できます。例を次に示します。
    - ユーザーのサブセットへのアクセスを制限し、許可されたユーザーデバイスを指定します。
    - (StoreFront ではなく) Workspace を介して接続しているユーザーへのアクセスを制限します。

- 特定の Workspace URL を介して接続しているユーザーへのアクセスを制限します。

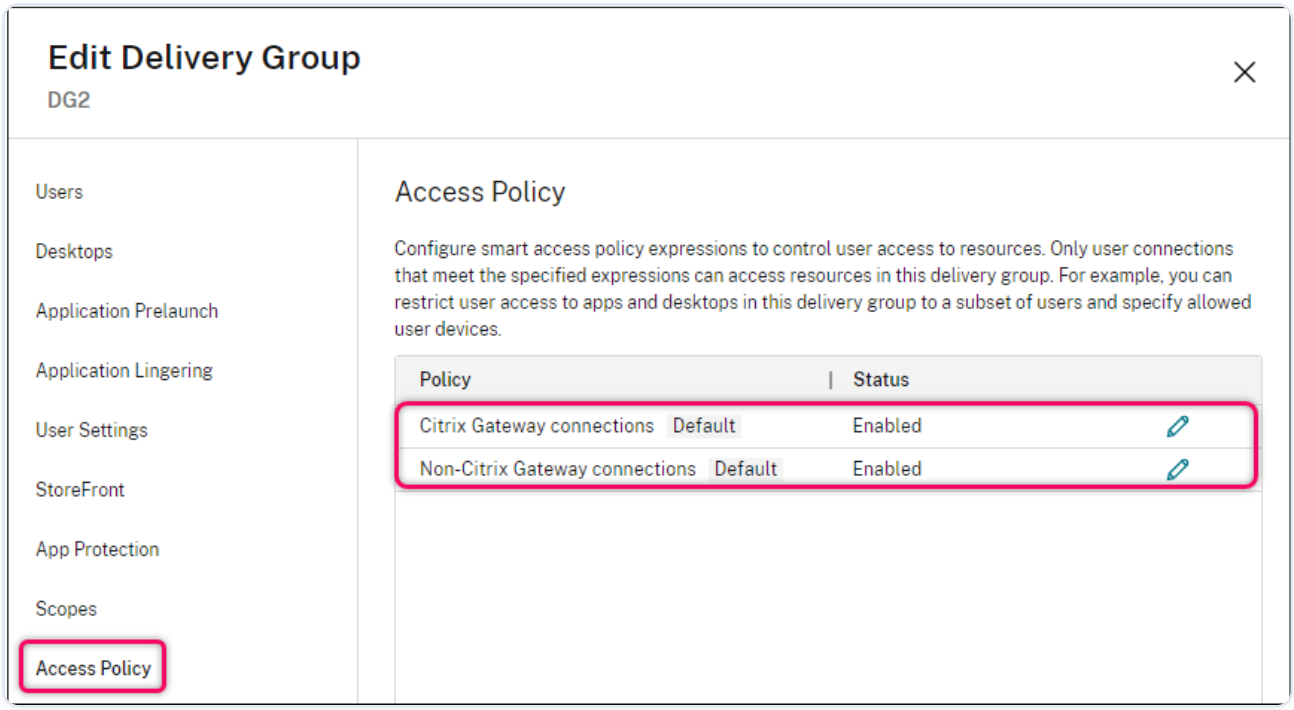
このセクションでは、アクセス ポリシー ルールを使用してデリバリー グループへのユーザー アクセスを制限する方法について説明します。

- アクセス ポリシー ルールについて
- アクセス ポリシー ルールを追加する
- Web Studio を使用してアクセス ポリシー ルールを管理する
- PowerShell を使用してポリシー ルールを追加および調整する

アクセス ポリシー ルールについて

デリバリー グループに対して複数のアクセス ポリシー ルールを構成できます。デリバリー グループ内のアプリとデスクトップは、ユーザーの接続が、定義したアクセス ポリシー ルールのいずれかに一致する場合に、順序に関係なく、ユーザーの StoreFront または Workspace に表示されます。

各ルールは個別に有効または無効にできます。無効なルールは、アクセス ポリシーが評価されるときに無視されます。



Web Studio のアクセス ポリシー リストには、次のデフォルトの SmartAccess ポリシー ルールが含まれています。必要に応じて追加できます。

- **Citrix Gateway 接続。** このポリシーでは、Citrix Gateway を介して行われたユーザー接続のみがデリバリー グループ内のリソースにアクセスできます。デバイス ポスチャまたはネットワー

ク ロケーション機能が有効になっている場合に Workspace を介して行われたユーザー接続も、Citrix Gateway を介した接続と見なされます。

- **Citrix Gateway 以外の接続。** このポリシーでは、Citrix Gateway を介していないユーザー接続のみがデリバリー グループ内のリソースにアクセスできます。

注記:

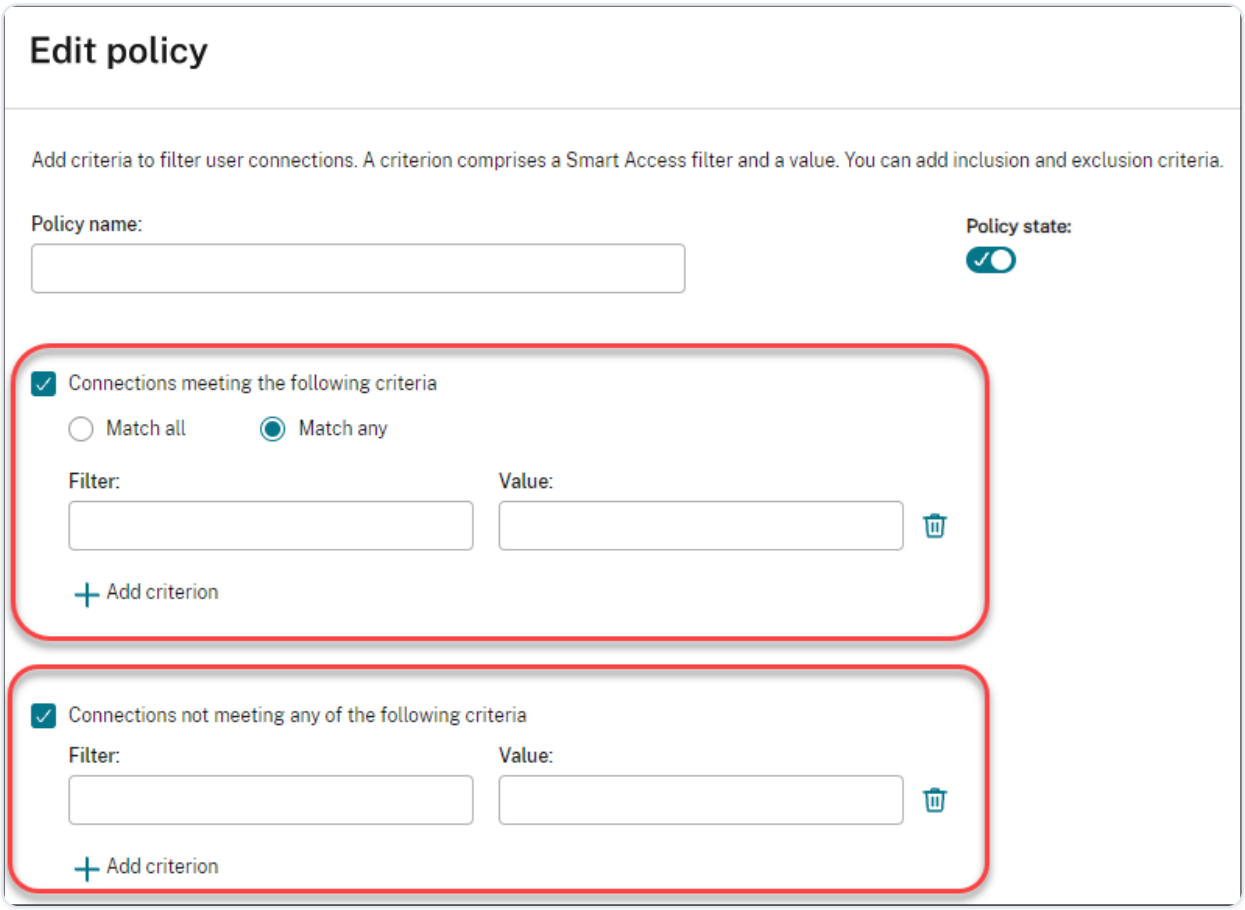
- デフォルトのルールが新しく構成されたルールを上書きしないようにするには、デフォルトのルールを無効にするか、新しいポリシーで使用されているフィルターを除外するように調整する必要があります。
- デフォルトのポリシーは削除できませんが、無効にすることはできます。ポリシーを無効にするには、**編集**アイコンをクリックし、**ポリシーの状態**を**無効**に変更します。
- ポリシーリストには、PowerShell コマンドを使用して追加された規則も表示されます。これらのポリシーは削除できますが、Web Studio で編集することはできません。

Web Studioを使用してアクセスポリシールールを追加する

アクセスポリシールールは、一連のフィルターで構成されます。フィルターについて詳しくは、この記事を参照してください。アクセスポリシールールを追加するときは、必要に応じて複数の条件フィルターをルールに追加します。

Web Studioを使用してデリバリーグループのポリシーを追加するには、次の手順に従います。

1. コンソールで、左ペインの**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーの**編集**をクリックします。
3. **アクセスポリシー**ページで、**追加**をクリックします。**ポリシーの追加**ページが表示されます。



4. **ポリシー名**フィールドに、ポリシーのわかりやすい名前を入力します。この名前は、展開内で一意である必要があります。
5. 許可されるユーザー接続の基準を定義するには、次の手順に従います。
   a. **次の基準を満たす接続**を選択します。
   b. **基準の追加**をクリックします。
   c. 「**Filter**」フィールドに、使用するフィルターの名前を入力します。「**Value**」フィールドに、フィルターの目的の値を入力します。たとえば、StoreFrontではなくWorkspaceを介して接続されたユーザーのみがこのデリバリーグループのリソースにアクセスできるようにするには、「**Filter**」に`Citrix-Via-Workspace`、「**Value**」に`True`と入力します。
   d. さらに条件を追加するには、手順b～cを繰り返します。
   e. 条件間の関係を選択します。
      - **いずれかに一致**。受信ユーザー接続が構成されたフィルター条件のいずれかを満たす場合にのみアクセスを許可します。
      - **すべてに一致**。受信ユーザー接続が構成されたフィルター条件のすべてを満たす場合にのみアクセスを許可します。
6. 禁止されているユーザー接続の条件を定義するには、次の手順に従います:

a. 「**次の条件のいずれも満たさない接続**」を選択します。

b. 「**条件の追加**」をクリックします。

c. 「**Filter**」フィールドに、使用するフィルターの名前を入力します。「**Value**」フィールドに、フィルターの目的の値を入力します。たとえば、`example.cloud.com` Workspace URLを介して接続されたユーザーがこのデリバリーグループのリソースにアクセスすることを禁止するには、「**Filter**」に`Citrix.Workspace.UsingDomain`、「**Value**」に`example.cloud.com`と入力します。

d. さらに条件を追加するには、手順b～cを繰り返します。

> **注:**
>
> 構成された条件のいずれかを満たすユーザー接続は、このデリバリーグループのリソースへのアクセスを禁止されます。

7. **完了**をクリックします。

   新しいポリシーがポリシーリストに表示されます。

8. この新しいポリシーでカバーされる接続との意図しない重複を避けるために、デフォルトのポリシー規則を確認し、調整してください。既存のポリシーを調整するには、以下の方法を使用します。

   - デフォルトのポリシー規則を無効にします。
   - 新しいポリシーの包含条件に追加したSmartAccessフィルターを除外するように、デフォルトのポリシー規則を構成します。詳細については、「Web Studio を使用したポリシー規則の管理」および「PowerShell を使用したアクセスポリシー規則の追加と管理」を参照してください。

> **重要:**
>
> 「アクセスポリシー規則について」で説明されているように、ユーザーの接続がデリバリーグループ内の1つ以上のポリシー規則に一致すると、ユーザーはそのリソースにアクセスできます。したがって、規則を作成した後、新しい規則でカバーされる接続との意図しない重複を避けるために、既存の規則を慎重に確認し、調整する必要があります。

Web Studio を使用したアクセスポリシー規則の管理

包含条件と除外条件を使用して、デフォルトのポリシーを調整できます。たとえば、それらの接続のサブセットへのアクセスを制限するには、次の手順に従います。

1. デフォルトのポリシーを編集します。
2. **「次のいずれかの条件を満たす接続」** を選択します。
3. 許可されたユーザーアクセスシナリオのSmartAccessポリシー式を追加、編集、または削除します。

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

PowerShell を使用したアクセスポリシー規則の追加と管理

デリバリーグループのアクセスポリシー規則を追加および管理するには、次のPowerShellコマンドレットを使用できます。

- New-BrokerAccessPolicyRule
- Get-BrokerAccessPolicyRule
- Set-BrokerAccessPolicyRule
- リネーム-ブローカーアクセスポリシールール
- リムーブ-ブローカーアクセスポリシールール

詳細については、Citrix Developer Documentationの関連記事を参照してください。

デリバリーグループ内のマシンへのユーザー接続を防止する（メンテナンスモード）

マシンへの新しい接続を一時的に停止する必要がある場合は、デリバリーグループ内の1台またはすべてのマシンでメンテナンスモードをオンにできます。これは、パッチを適用する前や管理ツールを使用する前に行うことがあります。

- マルチセッションOSマシンがメンテナンスモードの場合、ユーザーは既存のセッションに接続できますが、新しいセッションを開始することはできません。
- シングルセッションOSマシン（またはリモートPCアクセスを使用するPC）がメンテナンスモードの場合、ユーザーは接続または再接続できません。現在の接続は、切断またはログオフするまで接続されたままになります。

メンテナンスモードをオンまたはオフにするには：

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択します。

3. デリバリーグループ内のすべてのマシンでメンテナンスモードをオンにするには、アクションバーの****をクリックします。

   1台のマシンでメンテナンスモードをオンにするには、アクションバーで**マシンの表示**をクリックします。マシンを選択し、アクションバーで**メンテナンスモードをオンにする**をクリックします。
4. デリバリーグループ内の1台またはすべてのマシンでメンテナンスモードをオフにするには、前述の手順に従いますが、アクションバーで**メンテナンスモードをオフにする**をクリックします。

Windowsリモートデスクトップ接続（RDC）の設定も、マルチセッションOSマシンがメンテナンスモードであるかどうかに影響します。以下のいずれかが発生した場合、メンテナンスモードがオンになります。

- メンテナンスモードが前述のとおりオンに設定されている。
- RDC は **このコンピューターへの接続を許可しない** に設定されています。
- RDC は **このコンピューターへの接続を許可しない** に設定されていません。**リモートホスト構成ユーザーログオンモード** の設定は、**再接続を許可するが、新しいログオンは禁止する** または **サーバーが再起動されるまで再接続を許可するが、新しいログオンは禁止する** のいずれかです。

以下のメンテナンスモードをオンまたはオフにすることもできます。

- 接続。その接続を使用しているマシンに影響します。
- マシンカタログ。そのカタログ内のマシンに影響します。

デリバリーグループ内のマシンをシャットダウンして再起動する

この手順は、リモートPCアクセス マシンではサポートされていません。

1. 左側のペインで **デリバリーグループ** を選択します。
2. グループを選択し、アクションバーで **マシンの表示** をクリックします。
3. マシンを選択し、アクションバーで次のいずれかのエントリをクリックします。

   - **強制シャットダウン:** マシンの電源を強制的にオフにし、マシンリストを更新します。
   - **再起動:** オペレーティングシステムにシャットダウンを要求し、その後マシンを再起動します。オペレーティングシステムがこれに応じられない場合、マシンは現在の状態のままになります。

- **強制再起動:** オペレーティングシステムを強制的にシャットダウンし、その後マシンを再起動します。
- **一時停止:** マシンをシャットダウンせずに一時停止し、マシンリストを更新します。
- **シャットダウン:** オペレーティングシステムにシャットダウンを要求します。

強制ではないアクションの場合、マシンが10分以内にシャットダウンしないと、電源がオフになります。シャットダウン中にWindowsがアップデートをインストールしようとすると、アップデートが完了する前にマシンの電源がオフになるリスクがあります。

Citrixでは、シングルセッションOSマシンのユーザーがセッション内で**シャットダウン**を選択できないようにすることをお勧めします。詳細については、Microsoftのポリシーに関するドキュメントを参照してください。

マシンをシャットダウンして、接続で再起動することもできます。

デリバリーグループ内のマシンに対する再起動スケジュールの作成と管理

> **注:**
>
> - Autoscale™が有効なデリバリーグループに再起動スケジュールが適用されると、そのマシンは単に電源がオフにされ、Autoscaleが電源をオンにするまでそのままになります。
> - ランダムなシングルセッションマシンに再起動スケジュールが適用されると、コストを節約するため、それらのマシンは再起動されるのではなく、電源がオフになります。マシンの電源をオンにするには、Autoscaleを使用することをお勧めします。
> - デリバリーグループのタイムゾーンを変更すると、そのデリバリーグループ内のマシンが再起動される可能性があります。これを避けるには、稼働時間外にタイムゾーン設定を変更するようにしてください。

再起動スケジュールは、デリバリーグループ内のマシンが定期的に再起動されるタイミングを指定します。デリバリーグループに対して1つ以上のスケジュールを作成できます。スケジュールは次のいずれかに影響を与えることができます。

- グループ内のすべてのマシン。
- グループ内の1つ以上の（ただしすべてではない）マシン。マシンは、適用したタグによって識別されます。これはタグ制限と呼ばれます。タグは、そのタグを持つ項目のみにアクションを制限するためです。

たとえば、すべてのマシンが1つのデリバリーグループにあるとします。すべてのマシンを週に1回再起動し、経理チームが使用するマシンを毎日再起動したいとします。これを実現するには、すべてのマシンに対して1つのスケジュールを設定し、経理部門のマシンのみに対して別のスケジュールを設定します。

スケジュールには、再起動が開始される曜日と時刻、および期間が含まれます。

スケジュールを有効または無効にできます。スケジュールを無効にすることは、テスト中、特別な期間中、またはスケジュールが必要になる前に準備する際に役立ちます。

管理コンソールから自動電源オンまたはシャットダウンにスケジュールを使用することはできません。再起動のみに使用できます。

スケジュールの重複

複数のスケジュールが重複する可能性があります。上記の例では、両方のスケジュールが経理用マシンに影響を与えます。これらのマシンは日曜日に2回再起動される可能性があります。スケジューリングコードは、同じマシンが意図したよりも頻繁に再起動されるのを避けるように設計されていますが、保証はできません。

- スケジュールが開始時刻と期間で正確に一致する場合、マシンが再起動されるのは1回だけである可能性が高くなります。
- スケジュールが開始時刻と期間で異なるほど、複数回の再起動が発生する可能性が高くなります。
- スケジュールによって影響を受けるマシンの数も、重複の可能性に影響します。この例では、すべてのマシンに影響する週次スケジュールは、それぞれに指定された期間に応じて、経理用マシンの日次スケジュールよりも早く再起動を開始する可能性があります。

再起動スケジュールについて詳しく知るには、「再起動スケジュールの内部」を参照してください。

再起動スケジュールの表示

1. 左側のペインで を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **Restart Schedule**ページを選択します。

ページには、設定されている各スケジュールについて次の情報が含まれています。

- スケジュール名
- 使用されているタグ制限（ある場合）

- マシンの再起動がどのくらいの頻度で発生するか
- マシンユーザーが通知を受け取るかどうか
- スケジュールが有効になっているかどうか

タグの追加（適用）

タグ制限を使用する再起動スケジュールを構成する場合は、そのスケジュールが影響するマシンにタグが追加されていることを確認してください。上記の例では、経理チームが使用する各マシンにタグが適用されています。詳細については、「タグ」を参照してください。

1台のマシンに複数のタグを適用できますが、再起動スケジュールで指定できるタグは1つだけです。

1. 左側のペインで**デリバリーグループ**を選択します。
2. スケジュールによって制御されるマシンを含むグループを選択します。
3. 「**マシンの表示**」をクリックし、タグを追加するマシンを選択します。
4. アクションバーで「**タグの管理**」をクリックします。
5. タグが存在する場合は、タグ名の横にあるチェックボックスをオンにします。タグが存在しない場合は、 をクリックし、タグの名前を指定します。タグが作成されたら、新しく作成されたタグ名の横にあるチェックボックスをオンにします。
6. 「**タグの管理**」ダイアログで「**保存**」をクリックします。

再起動スケジュールの作成

> **注:**
>
> 再起動スケジュールは、電源管理されているすべてのマルチセッションマシンと、電源管理されていないマルチセッションマシンに適用できます。

1. 左側のペインで「**デリバリーグループ**」を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. 「**再起動スケジュール**」ページで、「**追加**」をクリックします。
4. 「**再起動スケジュールの追加**」ページで、次のようにします。
   - スケジュールを有効にするには「**はい**」を選択します。スケジュールを無効にするには「**いいえ**」を選択します。
   - スケジュール名と説明を入力します。

- 「**タグへの制限**」で、タグの制限を適用します。
- 「**メンテナンスモードのマシンを含める**」で、メンテナンスモードのマシンをこのスケジュールに含めるかどうかを選択します。代わりにPowerShellを使用するには、「メンテナンスモードのマシンのスケジュールされた再起動」を参照してください。
- 「**再起動頻度**」で、再起動の発生頻度（毎日、毎週、毎月、または1回）を選択します。「**毎週**」または「**毎月**」を選択した場合は、1つまたは複数の特定の日を指定できます。
- 「**繰り返し間隔**」で、スケジュールを実行する頻度を指定します。
- 「**開始日**」で、スケジュールの初回実行の開始日を指定します。
- 「**再起動開始時刻**」で、再起動を開始する時刻を24時間形式で指定します。
- 「**再起動期間**」について:
  - 自然な再起動を使用しない場合は、「**すべてのマシンを同時に再起動**」または「**すべてのマシンを一定期間内に再起動**」を選択します。
  - 自然な再起動を使用する場合は、「**すべてのセッションがドレインされた後にすべてのマシンを再起動**」を選択します。

    自然な再起動を使用するように構成された再起動スケジュールを開始すると:

    - デリバリーグループに属するすべてのアイドル状態のマシンが直ちに再起動されます。
    - アクティブなセッションが1つ以上あるデリバリーグループに属する各マシンは、すべてのセッションがログオフされたときに再起動されます。

    > **注:**
    >
    > 自然な再起動スケジュールは、電源管理されたマシンのみを再起動できます。

- で、再起動が開始される前に、該当するマシンに通知メッセージを表示するかどうかを選択します。デフォルトでは、メッセージは表示されません。
- 再起動が開始される15分前にメッセージを表示することを選択した場合、最初のメッセージの後に5分ごとにメッセージを繰り返すように選択できます（ で）。デフォルトでは、メッセージは繰り返されません。
- 通知のタイトルとテキストを入力します。デフォルトのテキストはありません。

メッセージに再起動までのカウントダウンを含める場合は、変数 **%m%** を含めます。すべてのマシンを同時に再起動することを選択しない限り、メッセージは再起動前の適切なタイミングで各マシンに表示されます。

5. をクリックして変更を適用し、 ウィンドウを閉じます。
6. 「**適用**」をクリックして変更を適用し、ウィンドウを開いたままにします。または、「**保存**」をクリックして変更を適用し、ウィンドウを閉じます。

ドレイン後の再起動

PowerShellを使用してマシン再起動スケジュールを作成または更新する場合（`New-BrokerRebootSchedulev2` または `Set-BrokerRebootSchedulev2`）、別の再起動期間値が利用可能です。

`-UseNaturalReboot <Boolean>` パラメーターでドレイン後の再起動機能を有効にすると、すべてのセッションがドレインされた後にすべてのマシンが再起動されます。再起動時刻になると、マシンはドレイン状態になり、すべてのセッションがログオフされたときに再起動されます。

この機能は、シングルセッションまたはマルチセッションマシンを含むデリバリーグループでサポートされています。このオプションは、電源管理されているマシンと、電源管理されていないマシンの両方で使用できます。

オンプレミス環境では、この機能は PowerShell を使用する場合にのみサポートされます。この機能は Web Studio では利用できません。

再起動スケジュールの編集、削除、有効化、または無効化

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. **再起動スケジュール**ページで、スケジュールのチェックボックスをオンにします。

    - スケジュールを編集するには、**編集**をクリックします。(#create-a-restart-schedule)のガイダンスに従って、スケジュール構成を更新します。
    - スケジュールを有効または無効にするには、**編集**をクリックします。**再起動スケジュールを有効にする**チェックボックスをオンまたはオフにします。
    - スケジュールを削除するには、 をクリックします。削除を確認します。スケジュールを削除しても、影響を受けるマシンに適用されているタグには影響しません。

データベースの停止により遅延したスケジュールされた再起動

> **注:**
>
> この機能はPowerShellでのみ利用可能です。

> デリバリーグループ内のマシン（VDA）のスケジュールされた再起動が開始される前にサイトデータベースの停止が発生した場合、停止が終了したときに再起動が開始されます。これにより、意図しない結果が生じる可能性があります。

たとえば、デリバリーグループの再起動を非稼働時間中 (03:00 から) に発生するようにスケジュールしたとします。スケジュールされた再起動が開始される1時間前 (02:00) にサイトデータベースの停止が発生しました。停止は6時間 (08:00 まで) 続きました。Delivery Controller とサイトデータベース間の接続が復元されると、再起動スケジュールが開始されます。VDA の再起動は元のスケジュールから5時間後に開始され、稼働時間中に VDA が再起動されることになります。

この状況を回避するために、`New-BrokerRebootScheduleV2` および `Set-BrokerRebootScheduleV2` コマンドレットで `MaxOvertimeStartMins` パラメーターを使用できます。この値は、再起動スケジュールが開始できる、スケジュールされた開始時刻を超える最大分数を示します。

- その時間内（スケジュールされた時間 + `MaxOvertimeStartMins`）にデータベース接続が復元された場合、VDAの再起動が開始されます。
- その時間内にデータベース接続が復元されない場合、VDAの再起動は開始されません。
- このパラメーターが省略されているか、値がゼロの場合、停止期間に関係なく、データベースへの接続が復元されたときにスケジュールされた再起動が開始されます。

詳細については、コマンドレットのヘルプを参照してください。この機能はPowerShellでのみ利用可能です。Web Studioで再起動スケジュールを構成する際には、この値を設定できません。

メンテナンスモードのマシンのスケジュールされた再起動

> **注:**
>
> この機能はPowerShellでのみ利用可能です。オプション `IgnoreMaintenanceMode` は、Citrix Virtual Apps and Desktops 7 2006以降でサポートされています。

> 再起動スケジュールがメンテナンスモードのマシンに影響するかどうかを示すには、`BrokerRebootScheduleV2` コマンドレットで `IgnoreMaintenanceMode` オプションを使用します。

たとえば、次のコマンドレットは、メンテナンスモードのマシン（メンテナンスモードではないマシンに加えて）を再起動するスケジュールを作成します。

```
New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup> -IgnoreMaintenanceMode $true
```

次のコマンドレットは、既存の再起動スケジュールを変更します。

```
Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode $true
```

詳細については、コマンドレットのヘルプを参照してください。この機能はPowerShellでのみ利用可能です。

1回限りの再起動スケジュールを有効にする

PowerShellを使用して1回限りの再起動スケジュールを有効にする場合は、次の `BrokerCatalogRebootSchedule` PowerShellコマンドを使用して、再起動スケジュールを作成、変更、削除します。

- Get-BrokerCatalogRebootSchedule
- New-BrokerCatalogRebootSchedule
- Set-BrokerCatalogRebootSchedule
- Remove-BrokerCatalogRebootSchedule
- Rename-BrokerCatalogRebootSchedule

制限事項:

- タイムゾーンが構成されていないカタログに関連付けられたカタログ再起動スケジュールは作成されますが、開始されません。
- カタログ再起動スケジュールが作成されると、その再起動スケジュールはデリバリーグループに属するカタログVMでのみ実行されます。

例、,

- **BankTellers** という名前のカタログ内のVMの再起動スケジュールを、Feb 3, 2022 の午前2時から午前4時の間に開始するように作成します。

```
C:\PS> New-BrokerCatalogRebootSchedule -Name BankTellers -CatalogName
BankTellers  -StartDate "2022-02-03" -StartTime "02:00" -Enabled $true
-RebootDuration 120
```

- UID 17を持つカタログ内のVMの再起動スケジュールを、Feb 3, 2022の午前1時から午前5時の間に開始するように作成します。再起動の10分前に、各VMは、すべてのユーザーセッションで、タイトルが**WARNING: Reboot pending**、メッセージが**Save your work**のメッセージボックスを表示するように設定されます。

```
C:\PS> New-BrokerCatalogRebootSchedule -Name 'Update reboot'
-CatalogUid 17 -StartDate "2022-02-03" -StartTime "01:00" -Enabled
$true -RebootDuration 240 -WarningTitle "WARNING: Reboot pending"
-WarningMessage "Save your work" -WarningDuration 10
```

- **Old Name** という名前のカタログ再起動スケジュールを **New Name** に変更します。

```
C:\PS> Rename-BrokerCatalogRebootSchedule -Name "Old Name" -NewName
"New Name"
```

- UID 1を持つすべてのカタログ再起動スケジュールを表示し、その後、UID 1を持つカタログ再起動スケジュールを**New Name**に名前変更します。

```
C:\PS> Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
```

- **Accounting**という名前のカタログ再起動スケジュールを、各VMの再起動の10分前に、タイトルが**WARNING: Reboot pending, and the message**、メッセージが**Save your work**のメッセージを表示するように設定します。このメッセージは、そのVM上のすべてのユーザーセッションに表示されます。

```
C:\PS> Set-BrokerCatalogRebootSchedule -Name Accounting -WarningMessage
"Save your work" -WarningDuration 10 -WarningTitle "WARNING: Reboot
pending"
```

- 無効になっているすべての再起動スケジュールを表示し、その後、無効になっているすべての再起動スケジュールを有効にします。

```
C:\PS> Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
BrokerCatalogRebootSchedule -Enabled $true
```

- UID 17を持つカタログ再起動スケジュールを、各VMの再起動の15分前、10分前、5分前に**Rebooting in %m% minutes**というメッセージを表示するように設定します。

```
C:\PS> Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Rebooting in
%m% minutes." -WarningDuration 15 -WarningRepeatInterval 5
```

- 「**MyCatalog**」という名前のカタログのタイムゾーンを構成します。

```
C:\PS> Set-BrokerCatalog -Name "MyCatalog" -TimeZone &lt;TimeZone>
```

デリバリーグループ内の管理対象マシンをロードする

マルチセッションOSマシンのみ負荷管理できます。

負荷管理は、サーバー負荷を測定し、現在の環境条件に基づいてどのサーバーを選択するかを決定します。この選択は以下に基づいています:

- **サーバーメンテナンスモードの状態:** マルチセッションOSマシンは、メンテナンスモードがオフの場合にのみ負荷分散の対象となります。
- **サーバー負荷インデックス:** マルチセッションOSマシンを提供するサーバーが接続を受け入れる可能性を決定します。このインデックスは、セッション数、およびCPU、ディスク、メモリ使用量などのパフォーマンスメトリックの設定といった負荷評価指標の組み合わせです。負荷評価指標は、負荷管理ポリシー設定で指定されます。

  サーバー負荷インデックスが10000の場合、サーバーが完全に負荷されていることを示します。他に利用可能なサーバーがない場合、ユーザーはセッションを起動したときに、デスクトップまたはアプリケーションが利用できないというメッセージを受け取る可能性があります。

  ロードインデックスは、Director (Monitor)、Web Studio (Manage) 検索、およびSDKで監視できます。

  コンソール表示で、**サーバー負荷インデックス**列（デフォルトでは非表示）を表示するには、マシンを選択し、列ヘッダーを右クリックして、**列の選択**を選択します。**マシンカテゴリ**で、**負荷インデックス**を選択します。

SDKでは、`Get-BrokerMachine` コマンドレットを使用します。詳細については、「CTX202150」を参照してください。

- **同時ログオン許容ポリシー設定**: サーバーへの同時ログオン要求の最大数。（この設定は、XenApp 6.xバージョンでの負荷調整に相当します。）

  すべてのサーバーが同時ログオン許容設定以上の場合、次のログオン要求は、保留中のログオンが最も少ないサーバーに割り当てられます。複数のサーバーがこれらの条件を満たす場合、ロードインデックスが最も低いサーバーが選択されます。

デリバリーグループ内の電源管理されたマシン

仮想シングルセッションOSマシンのみ電源管理できます。物理マシン (Remote PC Accessマシンを含む) は電源管理できません。GPU機能を備えたシングルセッションOSマシンは一時停止できないため、電源オフ操作は失敗します。マルチセッションOSマシンについては、再起動スケジュールを作成できます。

プールされたマシンを含むデリバリーグループでは、仮想シングルセッションOSマシンは次のいずれかの状態になります:

- ランダムに割り当てられ、使用中
- 割り当てられておらず、未接続

静的マシンを含むデリバリーグループでは、仮想シングルセッションOSマシンは次のようになります。

- 永続的に割り当てられ、使用中
- 永続的に割り当てられ、未接続（ただし準備完了）
- 割り当てられておらず、未接続

通常の使用時、静的デリバリーグループには通常、永続的に割り当てられたマシンと未割り当てのマシンの両方が含まれます。最初は、デリバリーグループの作成時に手動で割り当てられたマシンを除き、すべてのマシンが未割り当てです。ユーザーが接続すると、マシンは永続的に割り当てられます。これらのデリバリーグループ内の未割り当てマシンは完全に電源管理できますが、永続的に割り当てられたマシンは部分的にしか管理できません。

- **プールとバッファ：** プールされたデリバリーグループおよび未割り当てマシンを持つ静的デリバリーグループの場合、プール（この場合）とは、電源オン状態に保たれ、ユーザーが接続する準備ができている未割り当てまたは一時的に割り当てられたマシンのセットです。ユーザーはログオン後すぐにマシンを取得します。プールサイズ（電源オン状態に保たれるマシン

の数）は、時間帯によって構成可能です。静的デリバリーグループの場合、SDKを使用してプールを構成します。

バッファとは、プール内のマシンの数がしきい値を下回ったときに電源がオンになる、未割り当てマシンの追加のスタンバイセットです。しきい値はデリバリーグループサイズのパーセンテージです。大規模なデリバリーグループの場合、しきい値を超えるとかなりの数のマシンがオンになる可能性があります。したがって、デリバリーグループのサイズを慎重に計画するか、SDKを使用してデフォルトのバッファサイズを調整してください。

- **電源状態タイマー：** 電源状態タイマーを使用して、ユーザーが指定された時間切断された後にマシンを一時停止できます。たとえば、ユーザーが少なくとも10分間切断された場合、勤務時間外にマシンは自動的に一時停止します。

  タイマーは、平日と週末、およびピーク時と非ピーク時の間隔で構成できます。

- **永続的に割り当てられたマシンの部分的な電源管理：** 永続的に割り当てられたマシンでは、電源状態タイマーを設定できますが、プールやバッファは設定できません。マシンは各ピーク期間の開始時にオンになり、各オフピーク期間の開始時にオフになります。消費されたマシンを補うために利用可能になるマシンの数について、未割り当てマシンで得られるようなきめ細かな制御はできません。

仮想シングルセッションOSマシンの電源管理

1. 左ペインで**Delivery Groups**を選択します。
2. グループを選択し、アクションバーで**Edit Delivery Group**をクリックします。
3. **Power Management**ページで、**Power manage machines**の**Weekdays**を選択します。デフォルトでは、平日は月曜日から金曜日です。
4. ランダムデリバリーグループの場合、**Machines to be powered on**で**Edit**をクリックし、平日のプールサイズを指定します。次に、電源をオンにするマシンの数を選択します。
5. **ピーク時間**で、各日のピーク時間とオフピーク時間を設定します。
6. 平日のピーク時間とオフピーク時間の電源状態タイマーを設定します。**ピーク時間中 > 切断時**で、デリバリーグループ内の切断されたマシンをサスペンドするまでの遅延時間（分単位）を指定し、**サスペンド**を選択します。**オフピーク時間中 > 切断時**で、デリバリーグループ内のログオフされたマシンをシャットダウンするまでの遅延時間を指定し、**シャットダウン**を選択します。このタイマーは、ランダムなマシンを含むデリバリーグループでは使用できません。
7. **マシンの電源管理**で**週末**を選択し、週末のピーク時間と電源状態タイマーを設定します。
8. 加えた変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

SDKを使用して、次の操作を行います。

- 電源状態タイマーに応じてマシンを中断するのではなくシャットダウンするか、タイマーを接続解除ではなくログオフに基づいて設定したい場合。
- デフォルトの平日と週末の定義を変更する。
- 電源管理を無効にする。「CTX217289」を参照してください。

切断されたセッションを持つVDIマシンが異なる時間帯に移行する際の電源管理

> **重要:**
>
> この機能強化は、切断されたセッションを持つVDIマシンにのみ適用されます。ログオフされたセッションを持つVDIマシンには適用されません。

> 以前のリリースでは、アクション（切断アクション = 「**サスペンド**」または「**シャットダウン**」）が必要な時間帯に移行するVDIマシンは、電源が入ったままでした。このシナリオは、アクション（切断アクション = 「**何もしない**」）が不要な時間帯（ピーク時またはオフピーク時）にマシンが切断された場合に発生しました。

Citrix Virtual Apps and Desktops 7 1909以降、指定された切断時間が経過すると、宛先時間帯に構成されている切断アクションに応じて、マシンは中断または電源オフされます。

たとえば、VDIデリバリーグループに対して次の電源ポリシーを構成します。

- `PeakDisconnectAction`を「何もしない」に設定します。
- `OffPeakDisconnectAction`を「シャットダウン」に設定します。
- `OffPeakDisconnectTimeout`を「10」に設定します。

電源ポリシーの切断アクションの詳細については、https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policyおよびhttps://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/を参照してください。

以前のリリースでは、ピーク時にセッションが切断されたVDIマシンは、ピークからオフピークに移行しても電源がオンのままでした。Citrix Virtual Apps and Desktops 7 1909以降、`OffPeakDisconnectAction`および`OffPeakDisconnectTimeout`ポリシーアクションは、期間移行時にVDIマシンに適用されます。その結果、マシンはオフピークに移行してから10分後に電源がオフになります。

以前の動作に戻したい場合（つまり、切断されたセッションでピークからオフピーク、またはオフピークからピークに移行するマシンに対してアクションを実行しない場合）は、次のいずれかを実行します。

- `LegacyPeakTransitionDisconnectedBehaviour` レジストリ値を `1` に設定します。これは、以前の動作を有効にする*true*に相当します。デフォルトでは、値は `0`、つまり*false*であり、期間移行時に切断電源ポリシーアクションをトリガーします。
  - パス: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer`
  - 名前: `LegacyPeakTransitionDisconnectedBehaviour`
  - 種類: `REG_DWORD`
  - データ: `0x00000001 (1)`
- `Set-BrokerServiceConfigurationData` PowerShellコマンドを使用して設定を構成します。例:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

期間移行時に電源ポリシーアクションを適用する前に、マシンは次の基準を満たす必要があります。

- 切断されたセッションがあること。
- 保留中の電源アクションがないこと。
- VDI (シングルセッション) デリバリーグループに属し、異なる時間帯に移行する。
- 特定の時間帯（ピーク時またはオフピーク時）にセッションが切断され、電源アクションが割り当てられている期間に移行する。

カタログの電源オン状態のVDAの割合を変更する

1. デリバリーグループの**電源管理**セクションから、デリバリーグループのピーク時間を調整します。
2. デスクトップグループ名をメモします。
3. 管理者権限でPowerShellを起動し、次のコマンドを実行します。「Desktop Group Name」を、実行中のVDAの割合が変更されたデスクトップグループの名前に置き換えます。

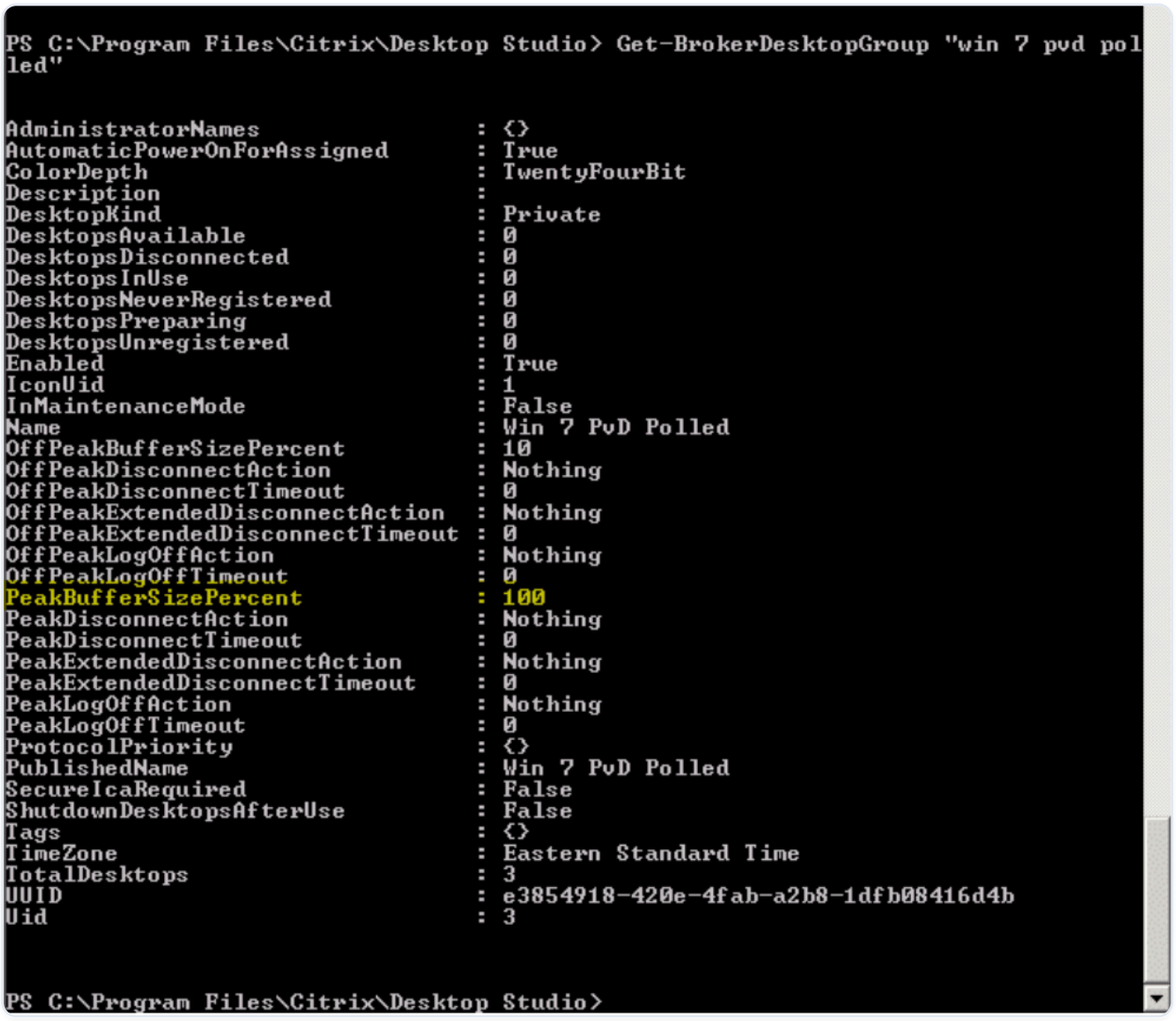
   ```
   asnp Citrix*
   ```

   ```
   # Set-BrokerDesktopGroup "Desktop Group Name" -PeakBufferSizePercent 100
   ```

値が100の場合、VDAの100%が準備完了状態であることを意味します。

4. 次を実行してソリューションを確認します。

```
#Get-BrokerDesktopGroup "Desktop Group Name"
```



変更が有効になるまでに最大1時間かかる場合があります。

ユーザーがログオフした後にVDAをシャットダウンするには、次を入力します。

```
# Set-BrokerDesktopGroup "Desktop Group Name" -ShutDownDesktopsAfterUse $True
```

ピーク時にVDAを再起動して、ユーザーがログオフした後に使用できるようにするには、次のように入力します。

```
# Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssignedDuringPeak $True
```

セッション

- セッションをログオフまたは切断するか、ユーザーにメッセージを送信する
- セッションの事前起動とセッションの維持を構成する
- メンテナンスモードのマシンから切断された場合のセッションの再接続を制御する
- セッションローミングを構成する

セッションをログオフまたは切断する

1. 左ペインで**デリバリーグループ**を選択します。
2. デリバリーグループを選択し、アクションバーで**マシンを表示**を選択します。
3. 中央ペインでマシンを選択し、アクションバーで**セッションを表示**を選択してから、セッションを選択します。
   - または、中央ペインで**セッション**タブを選択し、セッションを選択します。
4. セッションからログオフするには、アクションバーで**ログオフ**を選択します。セッションが閉じられ、ユーザーはログアウトされます。マシンが特定のユーザーに割り当てられていない限り、他のユーザーが使用できるようになります。
5. セッションを切断するには、アクションバーで**切断**を選択します。アプリケーションはセッション内で実行を継続し、マシンはそのユーザーに割り当てられたままになります。ユーザーは同じマシンに再接続できます。

シングルセッションOSマシンでは、未使用のセッションを自動的に処理するように電源状態タイマーを構成できます。詳細については、「電源管理されたマシン」を参照してください。

デリバリーグループにメッセージを送信する

1. 左側のペインで、［**デリバリーグループ**］ を選択します。
2. デリバリーグループを選択し、アクションバーで ［**マシンの表示**］ を選択します。
3. 中央のペインで、メッセージを送信するマシンを選択します。
4. アクションバーで ［**セッションの表示**］ を選択します。
5. 中央のペインで、すべてのセッションを選択し、アクションバーで ［**メッセージの送信**］ を選択します。
6. メッセージを入力し、 ［**OK**］ をクリックします。必要に応じて、重大度レベルを指定できます。オプションには、 ［**重大**］、 ［**質問**］、 ［**警告**］、 ［**情報**］ があります。

または、Citrix Director を使用してメッセージを送信することもできます。詳しくは、「ユーザーへのメッセージの送信」を参照してください。

デリバリーグループでセッションの事前起動とセッションの維持を構成する

これらの機能は、マルチセッションOSマシンでのみサポートされます。

セッションの事前起動とセッションの保持機能は、セッションが要求される前にセッションを開始する（セッションの事前起動）ことと、ユーザーがすべてのアプリケーションを閉じた後もアプリケーションセッションをアクティブに保つ（セッションの保持）ことによって、指定されたユーザーがアプリケーションにすばやくアクセスできるようにします。

デフォルトでは、セッションの事前起動とセッションの保持は使用されません。セッションは、ユーザーがアプリケーションを起動したときに開始（起動）され、セッション内の最後に開いたアプリケーションが閉じられるまでアクティブなままです。

考慮事項:

- デリバリーグループはアプリケーションをサポートしている必要があり、マシンはマルチセッションOS用のVDA（最小バージョン7.6）を実行している必要があります。
- これらの機能は、Citrix Workspaceアプリ for Windowsを使用している場合にのみサポートされ、追加のCitrix Workspaceアプリの構成も必要です。手順については、お使いのCitrix Workspaceアプリ for Windowsのバージョンの製品ドキュメントで「session prelaunch」を検索してください。
- Citrix Workspace app for HTML5 はサポートされていません。
- セッションの事前起動を使用しているときに、ユーザーのマシンがサスペンドモードまたは休止状態になった場合、事前起動は機能しません（セッションの事前起動設定に関係なく）。ユーザーは自分のマシン/セッションをロックできます。ただし、ユーザーがCitrix Workspaceアプリからログオフすると、セッションは終了し、事前起動は適用されなくなります。
- セッションの事前起動を使用している場合、物理クライアントマシンはサスペンドまたは休止状態の電源管理機能を使用できません。クライアントマシンのユーザーはセッションをロックできますが、ログオフしてはいけません。
- 事前起動セッションと残留セッションは同時接続ライセンスを消費しますが、接続されている場合に限ります。ユーザー/デバイスライセンスを使用している場合、ライセンスは90日間有効です。未使用の事前起動セッションと残留セッションは、デフォルトで15分後に切断されます。この値はPowerShell (`New/Set-BrokerSessionPreLaunch` コマンドレット) で構成できます。
- これらの機能が互いに補完し合うように調整するには、ユーザーのアクティビティパターンを慎重に計画し、監視することが不可欠です。最適な構成とは、ユーザーがアプリケーションをより早く利用できるというメリットと、ライセンスの使用とリソースの割り当てにかかるコストとのバランスが取れているものです。

- Citrix Workspaceアプリで、セッションの事前起動を特定の時刻にスケジュール設定することもできます。

未使用の事前起動セッションと残留セッションがアクティブなままになる期間

ユーザーがアプリケーションを起動しない場合に、未使用のセッションがアクティブなままになる期間を指定する方法はいくつかあります。構成されたタイムアウトとサーバー負荷のしきい値です。これらすべてを構成できます。最初に発生したイベントによって、未使用のセッションが終了します。

- **タイムアウト:** 構成されたタイムアウトは、未使用の事前起動セッションまたは残留セッションがアクティブなままになる分数、時間、または日数を指定します。タイムアウトを短くしすぎると、事前起動セッションは、ユーザーがアプリケーションにすばやくアクセスできるというメリットを提供する前に終了してしまいます。タイムアウトを長くしすぎると、サーバーに十分なリソースがないため、受信ユーザー接続が拒否される可能性があります。

  このタイムアウトは、管理コンソールからではなく、SDKからのみ有効にできます (`New/Set-BrokerSessionPreLaunch` コマンドレット)。タイムアウトを無効にすると、そのデリバリーグループのコンソール表示や **デリバリーグループの編集** ページには表示されません。

- **しきい値:** サーバー負荷に基づいて事前起動セッションと残留セッションを自動的に終了すると、サーバーリソースが利用可能である限り、セッションが可能な限り長く開いたままになります。未使用の事前起動セッションと残留セッションは、新しいユーザーセッションにリソースが必要なときに自動的に終了するため、接続拒否の原因にはなりません。

  2つのしきい値を構成できます。デリバリーグループ内のすべてのサーバーの平均負荷率と、グループ内の単一サーバーの最大負荷率です。しきい値を超えると、事前起動状態または残留状態にあった時間が最も長いセッションが終了します。負荷がしきい値を下回るまで、セッションは1分間隔で1つずつ終了します。しきい値を超えている間は、新しい事前起動セッションは開始されません。

Controllerに登録されていないVDAを持つサーバーと、メンテナンスモードのサーバーは、完全にロードされていると見なされます。予期せぬ停止が発生すると、容量を解放するために事前起動セッションと残留セッションが自動的に終了します。

セッションの事前起動を有効にするには

1. グループを選択し、アクションバーで **デリバリーグループの編集** をクリックします。
2. 「**アプリケーションの事前起動**」ページで、セッションを起動するタイミングを選択してセッションの事前起動を有効にします。

- ユーザーがアプリケーションを起動したとき。これがデフォルト設定です。セッションの事前起動は無効になっています。
- デリバリーグループ内のいずれかのユーザーがCitrix Workspaceアプリ for Windowsにログオンしたとき。
- ユーザーおよびユーザーグループのリスト内のいずれかのユーザーがCitrix Workspaceアプリ for Windowsにログオンしたとき。このオプションを選択する場合は、ユーザーまたはユーザーグループも指定してください。

アプリケーションの事前起動セッションページ(/en-us/citrix-virtual-apps-desktops/2407/media/dws-session-2.png)

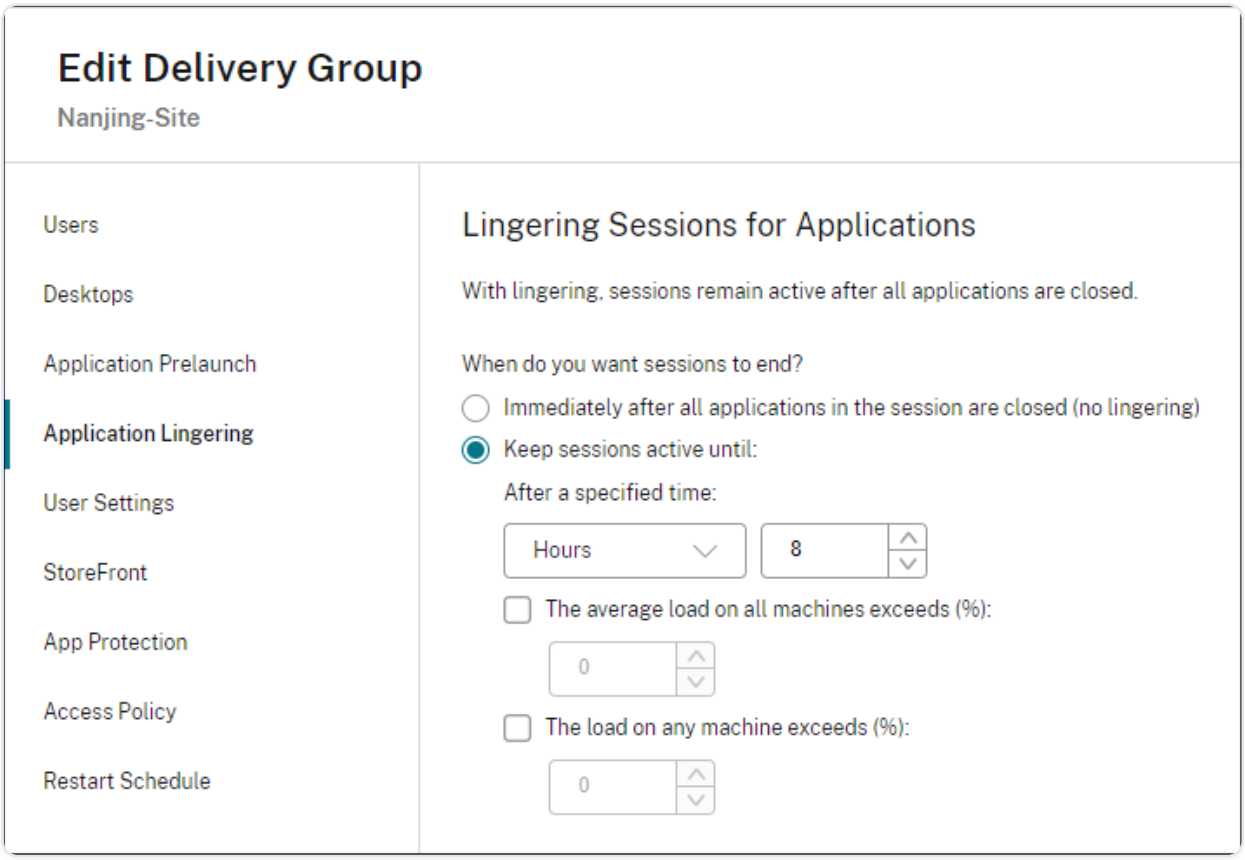
3. ユーザーがアプリケーションを起動すると、事前起動されたセッションは通常のセッションに置き換えられます。ユーザーがアプリケーションを起動しない場合（事前起動されたセッションが未使用の場合）、以下の設定がそのセッションがアクティブなままになる期間に影響します。

   - 指定された時間間隔が経過したとき。時間間隔は変更できます（1〜99日、1〜2376時間、または1〜142,560分）。
   - デリバリーグループ内のすべてのマシンの平均負荷が指定された割合（1〜99%）を超えたとき。
   - デリバリーグループ内のいずれかのマシンの負荷が指定された割合（1〜99%）を超えたとき。

   まとめ: 事前起動されたセッションは、ユーザーがアプリケーションを起動する、指定された時間が経過する、または指定された負荷しきい値を超える、のいずれかのイベントが発生するまでアクティブなままになります。

セッションの維持を有効にするには

1. 左側のペインで「**デリバリーグループ**」を選択します。
2. グループを選択し、アクションバーで「**デリバリーグループの編集**」をクリックします。
3. 「**アプリケーションの維持**」ページで、「**セッションをアクティブなままにする**」を選択してセッションの維持を有効にします。



4. ユーザーが別のアプリケーションを起動しない場合、残存セッションがアクティブなままになる期間に影響するいくつかの設定があります。

   - 指定された時間間隔が経過した場合。時間間隔は変更できます: 1〜99日、1〜2376時間、または1〜142,560分。
   - デリバリーグループ内のすべてのマシンにおける平均負荷が指定されたパーセンテージ（1〜99%）を超えた場合。
   - デリバリーグループ内のいずれかのマシンにおける負荷が指定されたパーセンテージ（1〜99%）を超えた場合。

   まとめ: 残存セッションは、ユーザーがアプリケーションを起動する、指定された時間が経過する、または指定された負荷しきい値を超える、のいずれかのイベントが発生するまでアクティブなままです。

メンテナンスモードのマシンから切断された場合のセッション再接続の制御

> **注：**
>
> この機能はPowerShellでのみ利用可能です。

> メンテナンスモードのマシンで切断されたセッションが、デリバリーグループ内のマシンに再接続できるかどうかを制御できます。

バージョン2106より前は、メンテナンスモードのマシンから切断されたシングルセッションのプールされたデスクトップセッションの再接続は許可されていませんでした。バージョン2106以降では、メンテナンスモードのマシンからの切断後、デリバリーグループで再接続を許可または禁止するように構成できます（セッションの種類に関係なく）。

デリバリーグループを作成または編集する際（`New-BrokerDesktopGroup`、`Set-BrokerDesktopGroup`）、`-AllowReconnectInMaintenanceMode <boolean>`パラメーターを使用して、メンテナンスモードのマシンから切断されたマシンへの再接続を許可または禁止します。

- trueに設定すると、セッションはグループ内のマシンに再接続できます。
- 「false」に設定されている場合、セッションはグループ内のマシンに再接続できません。

デフォルト値:

- シングルセッション: 無効
- マルチセッション: 有効

セッションローミングの構成

デフォルトでは、デリバリーグループでセッションローミングが有効になっています。セッションは、ユーザーとともにクライアントデバイス間をローミングします。ユーザーがセッションを起動し、別のデバイスに移動すると、同じセッションが使用され、アプリケーションは両方のデバイスで同時に利用可能になります。複数のデバイスでアプリケーションを表示できます。アプリケーションは、デバイスや現在のセッションの有無にかかわらず追従します。多くの場合、アプリケーションに割り当てられたプリンターやその他のリソースも追従します。または、PowerShellを使用することもできます。詳細については、「セッションローミング」を参照してください。

アプリケーションのセッションローミングの構成

アプリケーションのセッションローミングを構成するには、次の手順に従います。

1. コンソールで、左ペインの**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**デリバリーグループの編集**を選択します。
3. **ユーザー**ページで、**ユーザーがデバイス間を移動するときにセッションをローミングする**チェックボックスをオンにして、セッションローミングを有効にします。

- 有効にすると、ユーザーがアプリケーションセッションを起動して別のデバイスに移動した場合、同じセッションが使用され、両方のデバイスで利用可能になります。無効にすると、セッションはデバイス間をローミングしなくなります。

4. 変更を適用してウィンドウを閉じるには、**OK**を選択します。

デスクトップのセッションローミングの構成

デスクトップのセッションローミングを構成するには、次の手順に従います。

1. コンソールで、左ペインの**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**を選択します。
3. **デスクトップ**ページで、デスクトップを選択し、**編集**を選択します。
4. 「**セッションローミング**」チェックボックスをオンにして、セッションローミングを有効にします。

- 有効にすると、ユーザーがデスクトップを起動してから別のデバイスに移動した場合、同じセッションが使用され、アプリケーションは両方のデバイスで利用可能になります。無効にすると、セッションはデバイス間をローミングしなくなります。

OK を選択して変更を適用し、ウィンドウを閉じます。

アプリケーション

デリバリーグループのアプリケーションを表示および追加します。

1. コンソールで、左側のペインの を選択します。
2. グループを選択します。このグループにアプリケーションが含まれている場合、アクションバーに が表示されます。
3. を選択します。このグループで利用可能なすべてのアプリケーションが表示される ノードに移動します。
4. このグループにアプリケーションを追加するには、 ノードに移動し、グループを選択して、アクションバーの を選択します。

トラブルシューティング

- Delivery Controller に登録されていない VDA は、仲介セッションの起動時に考慮されません。これにより、利用可能なリソースが十分に活用されないことになります。VDA が登録されない理由はさまざまあり、その多くは管理者がトラブルシューティングできます。詳細表示には、

カタログ作成ウィザードおよびカタログをデリバリーグループに追加した後のトラブルシューティング情報が表示されます。

デリバリーグループを作成すると、デリバリーグループの詳細ペインに、登録可能だが登録されていないマシンの数が表示されます。たとえば、1台以上のマシンが電源オンでメンテナンスモードではないが、現在Controllerに登録されていない場合などです。「登録されていないが、登録されるべき」マシンを表示するときは、詳細ペインの タブで考えられる原因と推奨される是正措置を確認してください。

機能レベルに関するメッセージについては、「VDA のバージョンと機能レベル」を参照してください。

VDA 登録のトラブルシューティングについては、「CTX136668」を参照してください。

- デリバリーグループの表示では、詳細ペインの が、マシンに実際にインストールされているバージョンと異なる場合があります。マシンのWindowsのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- 「**電源状態不明**」のステータスを持つマシンについては、CTX131267でガイダンスを参照してください。

アプリケーショングループの作成

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

はじめに

アプリケーショングループを使用すると、アプリケーションのコレクションを管理できます。複数のデリバリーグループ間で共有されるアプリケーション、またはデリバリーグループ内のユーザーのサブセットによって使用されるアプリケーションに対して、アプリケーショングループを作成します。アプリケーショングループはオプションであり、同じアプリケーションを複数のデリバリーグループに追加する代替手段を提供します。デリバリーグループを複数のアプリケーショングループに関連付けたり、アプリケーショングループを複数のデリバリーグループに関連付けたりできます。

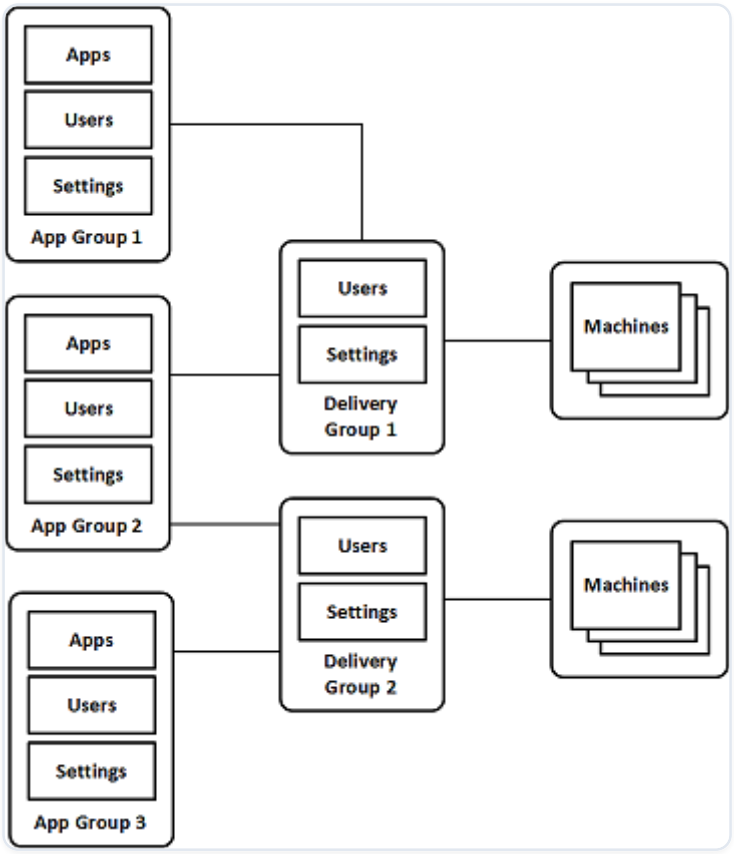
アプリケーショングループを使用すると、より多くのデリバリーグループを使用する場合と比較して、アプリケーション管理とリソース制御の利点が得られます。

- アプリケーションとその設定を論理的にグループ化することで、それらのアプリケーションを単一の単位として管理できます。たとえば、同じアプリケーションを個々のデリバリーグループに一度に1つずつ追加（公開）する必要はありません。
- アプリケーショングループ間のセッション共有により、リソース消費を節約できます。それ以外の場合、アプリケーショングループ間のセッション共有を無効にすることが有益な場合もあります。
- タグ制限機能を使用すると、選択したデリバリーグループ内のマシンの一部のみを考慮して、アプリケーショングループからアプリケーションを公開できます。タグ制限を使用すると、既存のマシンを複数の公開タスクに使用できるため、追加のマシンを展開および管理するコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）することと考えることができます。タグ制限のあるアプリケーショングループまたはデスクトップを使用すると、デリバリーグループ内のマシンの一部を分離してトラブルシューティングする際に役立ちます。

構成例

例 1:

次のグラフィックは、アプリケーショングループを含むCitrix Virtual Apps and Desktops展開を示しています。



この構成では、アプリケーションはデリバリーグループではなく、アプリケーショングループに追加されます。デリバリーグループは、使用されるマシンを指定します。（図には示されていませんが、マシンはマシンカタログにあります。）

アプリケーショングループ1はデリバリーグループ1に関連付けられています。アプリケーショングループ1で指定されたユーザーによって、アプリケーショングループ1内のアプリケーションにアクセスします。これらのグループは、デリバリーグループ1のユーザーリストにも含まれている場合にのみ表示されます。この構成は、アプリケーショングループのユーザーリストが、関連付けられたデリバリーグループのユーザーリストのサブセット（制限）であるというガイダンスに従っています。アプリケーショングループ1の設定（アプリケーショングループ間のアプリケーションセッション共有、関連付けられたデリバリーグループなど）は、そのグループ内のアプリケーションとユーザーに適用されます。デリバリーグループ1の設定は、アプリケーショングループ1および2のユーザーに適用されます。これは、これらのアプリケーショングループがそのデリバリーグループに関連付けられているためです。

アプリケーショングループ2は、2つのデリバリーグループ（1と2）に関連付けられています。これらのデリバリーグループのそれぞれには、アプリケーショングループ2で優先順位が割り当てられ、アプリケーションが起動されるときにデリバリーグループがチェックされる順序を示します。優先順位が同じデリバリーグループは、負荷分散されます。アプリケーショングループ2で指定されたユーザーは、アプリケーショングループ2内のアプリケーションにアクセスします。ただし、

それらのユーザーはデリバリーグループ1およびデリバリーグループ2のユーザーリストにも含まれている必要があります。

例2：

このシンプルなレイアウトでは、タグ制限を使用して、特定のデスクトップおよびアプリケーションの起動にどのマシンが考慮されるかを制限します。このサイトには、1つの共有デリバリーグループ、1つの公開デスクトップ、および2つのアプリケーションで構成された1つのアプリケーショングループがあります。

タグの例(/en-us/citrix-virtual-apps-desktops/2407/media/tags-example.png)

3台のマシン（VDA 101～103）のそれぞれにタグが追加されています。

アプリケーショングループは、「Orange」タグ制限で作成されました。そのアプリケーションはそれぞれ、そのデリバリーグループ内で「Orange」タグを持つマシン（VDA 102および103）でのみ起動されます。

アプリケーショングループ（およびデスクトップ）でのタグ制限の使用に関するより包括的な例とガイダンスについては、「タグ」を参照してください。

ガイダンスと考慮事項

Citrixでは、アプリケーションをアプリケーショングループまたはデリバリーグループのいずれかに追加することをお勧めします。両方に追加することはお勧めしません。そうしないと、2種類のグループにアプリケーションが存在することによる複雑さが増し、管理が困難になる可能性があります。

デフォルトでは、アプリケーショングループは有効になっています。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

デフォルトでは、アプリケーショングループ間のアプリケーションセッション共有は有効になっています。「アプリケーショングループ間のセッション共有」を参照してください。

Citrixでは、デリバリーグループを現在のバージョンにアップグレードすることをお勧めします。このプロセスには、次のものが必要です。

1. デリバリーグループで使用されているマシン上のVDAのアップグレード。
2. それらのマシンを含むマシンカタログのアップグレード。
3. デリバリーグループのアップグレード。

詳細については、「デリバリーグループの管理」を参照してください。

アプリケーショングループを使用するには、コアコンポーネントが最小バージョン7.9である必要があります。

アプリケーショングループを作成するには、デリバリーグループ管理者組み込みロールの委任管理権限が必要です。詳細については、「委任管理」を参照してください。

この記事では、アプリケーションを複数のアプリケーショングループに「関連付ける」ことについて言及しています。これは、利用可能なソースからそのアプリケーションのインスタンスを追加する操作とは異なります。同様に、デリバリーグループはアプリケーショングループに関連付けられ、互いの追加要素やコンポーネントではありません。

アプリケーショングループとのセッション共有

アプリケーションセッション共有が有効になっている場合、すべてのアプリケーションは同じアプリケーションセッションで起動します。これにより、より多くのアプリケーションセッションを起動するコストが削減され、コピー＆ペースト操作など、クリップボードを使用するアプリケーション機能を利用できるようになります。ただし、状況によってはセッション共有をクリアできます。

アプリケーショングループを使用する場合、デリバリーグループのみを使用する場合に利用できる標準のセッション共有動作を拡張する、次の3つの方法でアプリケーションセッション共有を構成できます。

- アプリケーショングループ間でセッション共有が有効。
- 同じアプリケーショングループ内のアプリケーション間でのみセッション共有が有効。
- セッション共有が無効。

アプリケーショングループ間のセッション共有

アプリケーショングループ間でアプリケーションセッション共有を有効にすることも、無効にして同じアプリケーショングループ内のアプリケーションのみにアプリケーションセッション共有を制限することもできます。

- **アプリケーショングループ間のセッション共有を有効にすると役立つ例:**

  アプリケーショングループ1にはWordやExcelなどのMicrosoft Officeアプリケーションが含まれています。アプリケーショングループ2にはメモ帳や電卓などの他のアプリケーションが含まれており、両方のアプリケーショングループは同じデリバリーグループにアタッチされています。両方のアプリケーショングループにアクセスできるユーザーがWordを起動してアプリケーションセッションを開始し、次にメモ帳を起動します。コントローラーが、ユーザーの既存の

Word実行セッションがメモ帳の実行に適していると判断した場合、メモ帳は既存のセッション内で起動されます。既存のセッションからメモ帳を実行できない場合（たとえば、タグ制限によってセッションが実行されているマシンが除外されている場合など）、セッション共有を使用するのではなく、適切なマシン上に新しいセッションが作成されます。

- **アプリケーショングループ間のセッション共有を無効にすると役立つ例:**

  同じマシンにインストールされている他のアプリケーションとうまく相互運用できない一連のアプリケーションの構成。たとえば、同じソフトウェアスイートの2つの異なるバージョンや、同じWebブラウザーの2つの異なるバージョンなどです。ユーザーが同じセッションで両方のバージョンを起動することを許可しないようにしたい場合。

  ソフトウェアスイートの各バージョンに対してアプリケーショングループを作成し、ソフトウェアスイートの各バージョンのアプリケーションを対応するアプリケーショングループに追加します。これらのアプリケーショングループのそれぞれでグループ間のセッション共有が無効になっている場合、それらのグループで指定されたユーザーは、同じセッションで同じバージョンのアプリケーションを実行できます。ユーザーは同時に他のアプリケーションを実行できますが、同じセッションでは実行できません。異なるバージョンのアプリケーションのいずれか、またはアプリケーショングループに含まれていないアプリケーションを起動すると、そのアプリケーションは新しいセッションで起動されます。

このアプリケーショングループ間のセッション共有機能は、セキュリティサンドボックス機能ではありません。これは完璧ではなく、ユーザーが他の手段（たとえば、Windowsエクスプローラー経由など）でアプリケーションをセッションに起動するのを防ぐことはできません。

マシンが容量に達している場合、新しいセッションは開始されません。必要に応じて、セッション共有を使用して、既存のセッションで新しいアプリケーションが起動されます。

アプリケーションセッション共有が許可されているアプリケーショングループに対してのみ、プレランチセッションを利用可能にできます。（セッションリンガー機能を使用するセッションは、すべてのアプリケーショングループで利用可能です。）これらの機能は、アプリケーショングループに関連付けられている各デリバリーグループで有効にして構成する必要があります。アプリケーショングループでは構成できません。

デフォルトでは、アプリケーショングループを作成すると、アプリケーショングループ間のアプリケーションセッション共有が有効になります。グループ作成時にこれを変更することはできません。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。アプリケーショングループの管理を参照してください。

アプリケーショングループ内でのセッション共有を無効にする

同じアプリケーショングループ内のアプリケーション間でのアプリケーションセッション共有を防ぐことができます。

- **アプリケーショングループ内でのセッション共有を無効にすることが役立つ例:**

  ユーザーに、別々のモニターでアプリケーションの複数の同時フルスクリーンセッションにアクセスさせたい場合。

  アプリケーショングループを作成し、そこにアプリケーションを追加します。

デフォルトでは、アプリケーショングループを作成すると、アプリケーションセッション共有が有効になります。グループ作成時にこの設定を変更することはできません。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。アプリケーショングループの管理を参照してください。

アプリケーショングループを作成する

アプリケーショングループを作成するには：

1. Web Studioにサインインします。
2. 左ペインで **Applications** を選択し、次に **Application Groups** タブを選択します。
3. フォルダーを使用してアプリケーショングループを整理するには、**Application Groups** ルートフォルダーの下にフォルダーを作成します。
4. グループを作成するフォルダーを選択し、次に **Create Application Group** をクリックします。グループ作成ウィザードが **Introduction** ページで起動します。このウィザードの今後の起動時にこのページを削除できます。
5. 以下のページで説明されている設定を構成するには、ウィザードに従います。各ページの作業が完了したら、**Summary** ページに到達するまで **Next** を選択します。

ステップ1. デリバリーグループ

Delivery Groups ページには、すべてのデリバリーグループが一覧表示され、各グループに含まれるマシンの数が示されます。

- **Compatible Delivery Groups** リストには、選択できるデリバリーグループが含まれています。互換性のあるデリバリーグループには、ランダム（永続的または静的に割り当てられていない）なマルチセッションまたはシングルセッションOSマシンが含まれています。

- **Incompatible Delivery Groups** リストには、選択できないデリバリーグループが含まれています。各エントリは、静的に割り当てられたマシンが含まれているなど、互換性がない理由を説明しています。

アプリケーショングループは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループと関連付けることができます。

次の両方の条件が満たされている場合、デスクトップのみを配信する共有マシンを含むデリバリーグループも選択できます。

- デリバリーグループに共有マシンが含まれており、XenDesktopバージョン7.9より前に作成されたものであること。
- 編集デリバリーグループ権限があること。

アプリケーショングループ作成ウィザードがコミットされると、デリバリーグループの種類は自動的に「デスクトップとアプリケーション」に変換されます。

関連付けられたデリバリーグループがないアプリケーショングループを作成することはできますが（アプリケーションを整理するため、または現在使用されていないアプリケーションのストレージとして機能させるためなど）、少なくとも1つのデリバリーグループが指定されるまで、そのアプリケーショングループをアプリケーションの配信に使用することはできません。また、デリバリーグループが指定されていない場合、**From Start** メニューソースからアプリケーショングループにアプリケーションを追加することはできません。

選択したデリバリーグループは、アプリケーションの配信に使用されるマシンを指定します。アプリケーショングループに関連付けるデリバリーグループの横にあるチェックボックスをオンにします。

タグ制限を追加するには、「**タグを持つマシンへの起動を制限する**」を選択し、ドロップダウンリストからタグを選択します。

手順2. ユーザー

アプリケーショングループでアプリケーションユーザーを指定します。前のページで選択したデリバリーグループ内のすべてのユーザーとユーザーグループを許可するか、それらのデリバリーグループから特定のユーザーとユーザーグループを選択します。指定されたユーザーに利用を制限する場合、デリバリーグループで指定されたユーザーのみが、アプリケーショングループ内のこのグループのアプリケーションにアクセスできます。基本的に、アプリケーショングループのユーザーリストは、デリバリーグループのユーザーリストに対するフィルターとして機能します。

認証されていないユーザーによるアプリケーションの使用を有効または無効にする機能は、アプリケーショングループではなく、デリバリーグループでのみ利用できます。

展開でユーザーリストが指定される場所については、「ユーザーリストが指定される場所」を参照してください。

ステップ3. アプリケーション

知っておくと良いこと:

- デフォルトでは、追加する新しいアプリケーションは**アプリケーション**という名前のフォルダーに配置されます。別のフォルダーを指定することもできます。アプリケーションを追加しようとして、同じ名前のアプリケーションがそのフォルダーに既に存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。提案された一意の名前に同意すると、その新しい名前でアプリケーションが追加されます。そうでない場合は、追加する前に自分で名前を変更する必要があります。詳細については、「アプリケーションフォルダーの管理」を参照してください。
- アプリケーションのプロパティ（設定）は、追加時または後で変更できます。「アプリケーションプロパティの変更」を参照してください。同じ名前のアプリケーションを2つ同じユーザーに公開する場合、Web Studioで**アプリケーション名（ユーザー向け）**プロパティを変更してください。そうしないと、ユーザーはCitrix Workspaceアプリで重複した名前を目にすることになります。
- アプリケーションを複数のアプリケーショングループに追加する場合、それらのすべてのグループでアプリケーションを表示する十分な権限がないと、表示の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが追加されたすべてのグループを含むようにスコープを拡張してください。

アプリケーションソースを表示するには、ドロップダウンメニューから「**追加**」をクリックします。

- **スタートメニューから**：選択したデリバリーグループ内のマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、「**OK**」をクリックします。

  以下のいずれかを選択した場合、このソースは選択できません。

  - 関連付けられたデリバリーグループがないアプリケーショングループ。
  - 関連付けられたデリバリーグループにマシンが含まれていないアプリケーショングループ。
  - マシンが含まれていないデリバリーグループ。

- **手動で定義:** サイト内またはネットワーク内の他の場所にあるアプリケーション。このソースを選択すると、新しいページが起動し、実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、管理者とユーザーの表示名を入力します。この情報を入力したら、**OK**をクリックします。
- **既存:** 以前にサイトに追加されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスを選択し、**OK**をクリックします。サイトにアプリケーションがない場合、このソースは選択できません。
- **App-V:** App-Vパッケージ内のアプリケーション。このソースを選択すると、新しいページが起動し、**App-Vサーバー**または**アプリケーションライブラリ**を選択します。表示された画面から、追加するアプリケーションのチェックボックスを選択し、**OK**をクリックします。詳しくは、「App-Vアプリケーションの展開と配信」を参照してください。サイトでApp-Vが構成されていない場合、このソースは選択できません（または表示されない場合があります）。

前述のとおり、**追加**ドロップダウンメニューの一部のエントリは、その種類の有効なソースがない場合、選択できません。互換性のないソースはまったく表示されません（たとえば、アプリケーショングループにアプリケーショングループを追加することはできないため、アプリケーショングループを作成するときにそのソースは表示されません）。

ステップ4. スコープ

このページは、以前にカスタムスコープを作成した場合にのみ表示されます。デフォルトでは、**すべて**のスコープが選択されています。詳しくは、「委任管理」を参照してください。

ステップ5. 概要

アプリケーショングループの名前を入力します。説明を（オプションで）入力することもできます。

概要情報を確認し、**「完了」**をクリックします。

アプリケーショングループの管理

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

はじめに

この記事では、作成したアプリケーショングループを管理する方法について説明します。

アプリケーショングループまたはデリバリーグループでアプリケーションを管理する方法については、アプリケーションを参照してください。これには、以下の方法が含まれます。

- アプリケーショングループ内のアプリケーションを追加または削除する。
- アプリケーショングループの関連付けを変更する。

アプリケーショングループの管理には、Delivery Group Administratorの組み込みロールの委任管理権限が必要です。詳細については、委任管理を参照してください。

アプリケーショングループを有効または無効にする

アプリケーショングループが有効になっている場合、そのグループに追加されたアプリケーションを配信できます。アプリケーショングループを無効にすると、そのグループ内の各アプリケーションも無効になります。ただし、それらのアプリケーションが他の有効なアプリケーショングループにも関連付けられている場合、それらの他のグループから配信できます。アプリケーションがアプリケーショングループに関連付けられたデリバリーグループに明示的に追加されている場合、アプリケーショングループを無効にしても、それらのデリバリーグループ内のアプリケーションには影響しません。

アプリケーショングループは作成時に有効になります。グループの作成時にこの設定を変更することはできません。

1. 左側のペインで**アプリケーション**を選択し、次に**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、次にアクションバーで**アプリケーショングループの編集**を選択します。
3. **設定**ページで、**アプリケーショングループを有効にする**チェックボックスをオンまたはオフにします。
4. ウィンドウを開いたままにするには**適用**をクリックし、変更を適用してウィンドウを閉じるには**保存**をクリックします。

アプリケーションセッションのアプリケーショングループ間での共有を有効または無効にする

アプリケーショングループ間のセッション共有は、アプリケーショングループを作成するときに有効になります。グループの作成時にこの構成を変更することはできません。詳しくは、「アプリケーショングループとのセッション共有」を参照してください。

1. 左ペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **設定**ページで、**アプリケーショングループ間のアプリケーションセッション共有を有効にする**チェックボックスをオンまたはオフにします。
4. ウィンドウを開いたままにするには**適用**をクリックし、変更を適用してウィンドウを閉じるには**保存**をクリックします。

アプリケーショングループ内でのアプリケーションセッション共有を無効にする

同じアプリケーショングループ内のアプリケーション間のセッション共有は、アプリケーショングループを作成するときにデフォルトで有効になります。アプリケーショングループ間のアプリケーションセッション共有を無効にしても、同じアプリケーショングループ内のアプリケーション間のセッション共有は有効のままです。

PowerShell SDKを使用して、アプリケーションセッション共有がアプリケーション間で無効になっているアプリケーショングループを構成できます。状況によっては、このオプションが望ましい場合があります。たとえば、ユーザーに非シームレスアプリケーションを別のモニターの全画面表示アプリケーションウィンドウで起動させたい場合があります。

アプリケーショングループ内でアプリケーションセッション共有を無効にすると、そのグループ内の各アプリケーションは新しいアプリケーションセッションで起動します。同じアプリケーションを実行している適切な切断されたセッションが利用可能な場合、それは再接続されます。たとえば、メモ帳を実行している切断されたセッションでメモ帳を起動する場合、新しいセッションを作成する代わりにそのセッションが再接続されます。複数の適切な切断されたセッションが利用可能な場合、ランダムではあるが決定論的な方法で、いずれかのセッションが再接続のために選択されます。同じ状況で再発生した場合、同じセッションが選択されますが、それ以外の場合、セッションは必ずしも予測可能ではありません。

PowerShell SDKを使用して、既存のアプリケーショングループ内のすべてのアプリケーションのアプリケーションセッション共有を無効にするか、アプリケーションセッション共有が無効になっているグループを作成します。

PowerShellコマンドレットの例

セッション共有を無効にするには、Broker PowerShellコマンドレット `New-BrokerApplicationGroup` または `Set-BrokerApplicationGroup` を使用し、パラメーター `SessionSharingEnabled` を `False` に、パラメーター `SingleAppPerSession` を `True` に設定します。

- たとえば、グループ内のすべてのアプリケーションでアプリケーションセッション共有が無効になっているアプリケーショングループを作成するには：

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

- 例えば、既存のアプリケーショングループ内のすべてのアプリケーション間でアプリケーションセッション共有を無効にするには、次のようにします。

  ```
  Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

考慮事項

- `SingleAppPerSession` プロパティを有効にするには、`SessionSharingEnabled` プロパティを False に設定する必要があります。これら2つのプロパティを同時に有効にすることはできません。`SessionSharingEnabled` パラメーターは、アプリケーショングループ間のセッション共有を指します。
- アプリケーションセッション共有は、アプリケーショングループに関連付けられているがデリバリーグループには関連付けられていないアプリケーションでのみ機能します。デリバリーグループに直接関連付けられているすべてのアプリケーションは、デフォルトでセッションを共有します。
- アプリケーションが複数のアプリケーショングループに割り当てられている場合、グループの設定が競合しないようにしてください。たとえば、あるグループのオプションが `True` に設定され、別のグループのオプションが `False` に設定されている場合、予期しない動作が発生します。

アプリケーショングループの名前を変更する

1. 左側のペインで を選択し、 タブを選択します。
2. アプリケーショングループを選択し、アクションバーで を選択します。
3. 新しい一意の名前を指定し、 をクリックします。

アプリケーショングループとのデリバリーグループの関連付けを追加、削除、または優先度を変更する

アプリケーショングループは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。

以下の両方の条件が満たされている場合は、デスクトップのみを配信する共有マシンを含むデリバリーグループを選択することもできます。

- デリバリーグループに共有マシンが含まれており、バージョン7.9より前のバージョンで作成されている。
- デリバリーグループの編集権限があること。

ダイアログがコミットされると、デリバリーグループの種類は自動的に「デスクトップとアプリケーション」に変換されます。

1. 左ペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **デリバリーグループ**ページを選択します。
4. デリバリーグループを追加するには、**追加**をクリックします。利用可能なデリバリーグループのチェックボックスを選択します。（互換性のないデリバリーグループは選択できません。）選択が完了したら、**OK**をクリックします。
5. デリバリーグループを削除するには、削除するグループのチェックボックスを選択し、**削除**をクリックします。プロンプトが表示されたら削除を確定します。
6. デリバリーグループの優先度を変更するには、デリバリーグループのチェックボックスを選択し、**優先度の編集**をクリックします。優先度（0 = 最高）を入力し、**OK**をクリックします。
7. 加えた変更を適用してウィンドウを開いたままにするには**適用**をクリックし、変更を適用してウィンドウを閉じるには**保存**をクリックします。

アプリケーショングループのタグ制限を追加、変更、または削除する

タグ制限の追加、変更、削除は、アプリケーション起動の対象となるマシンに予期せぬ影響を与える可能性があります。タグの考慮事項と注意事項を確認してください。

1. 左側のペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **デリバリーグループ**ページを選択します。

4. タグ制限を追加するには、**タグを持つマシンへの起動を制限する**を選択し、ドロップダウンリストからタグを選択します。
5. タグ制限を変更または削除するには、別のタグを選択するか、**このタグを持つマシンへの起動を制限する**のチェックを外してタグ制限を完全に削除します。
6. 行った変更を適用してウィンドウを開いたままにするには、**適用**をクリックするか、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

アプリケーショングループでのユーザーの追加または削除

ユーザーの詳細については、「アプリケーショングループの作成」を参照してください。

1. 左ペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **ユーザー**ページを選択します。関連付けられたデリバリーグループ内のすべてのユーザーにアプリケーショングループ内のアプリケーションの使用を許可するか、特定のユーザーとグループのみに許可するかを指定します。ユーザーを追加するには、**追加**をクリックし、追加するユーザーを指定します。ユーザーを削除するには、1人以上のユーザーを選択し、**削除**をクリックします。
4. 行った変更を適用してウィンドウを開いたままにするには、**適用**をクリックするか、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

アプリケーショングループでのアプリケーションアイコンの追加、変更、または削除

アプリケーションアイコンを追加、変更、または削除するには、次の手順を実行します。

1. 左ペインで**アプリケーション**を選択します。
2. **アプリケーション**タブで、アプリケーションを選択し、**プロパティ**を選択します。

   アプリケーショングループレベルで変更を行うには、**アプリケーショングループ**タブに移動し、グループ内のアプリケーションを選択して、**プロパティ**を選択します。
3. **デリバリー**ページを選択し、**変更**を選択します。**アイコンの選択**ウィンドウが表示されます。
4. **アイコンの選択**ウィンドウで、次のいずれかを実行します。

   - アイコンを追加するには、**追加**を選択し、アイコンを参照します。
   - アイコンを削除するには、アイコンを選択し、**削除**を選択します。
   - アイコンを変更するには、アプリケーションのアイコンを選択します。

重要:

- サイズが200 KBを超えるアイコンを追加することはできません。
- .iconファイルのみを追加できます。
- 組み込みアイコンを削除することはできません。
- 使用中のアプリケーションのアイコンを削除することはできません。

5. **Save** を選択して変更を適用し、ウィンドウを閉じます。

アプリケーショングループのスコープを変更する

スコープを作成した場合にのみスコープを変更できます（「すべてのスコープ」は編集できません）。詳しくは、委任管理を参照してください。

1. 左側のペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **スコープ**ページを選択します。スコープの横にあるチェックボックスをオンまたはオフにします。
4. **適用**をクリックして変更を適用し、ウィンドウを開いたままにするか、**保存**をクリックして変更を適用し、ウィンドウを閉じます。

アプリケーショングループのスコープを変更する

スコープは、作成した場合にのみ変更できます (すべてのスコープは編集できません)。詳細については、「委任管理」を参照してください。

1. 左ペインで を選択し、 タブを選択します。
2. アプリケーショングループを選択し、アクションバーで を選択します。
3. ページを選択します。変更するスコープの横にあるチェックボックスをオンまたはオフにします。
4. 変更を適用してウィンドウを開いたままにするには を選択し、変更を適用してウィンドウを閉じるには を選択します。

アプリケーショングループを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに関連付けられている必要があります。アプリケーショングループを削除した結果、1つ以上のアプリケーションがどのグループにも属さなくなる場合、そのグループを削除するとそれらのアプリケーションも削除されるという警告が表示されます。その後、削除を確定またはキャンセルできます。

アプリケーションを削除しても、元のソースから削除されるわけではありません。ただし、再度利用可能にする場合は、もう一度追加する必要があります。

1. 左ペインで を選択し、 タブを選択します。
2. アプリケーショングループを選択し、アクションバーで を選択します。
3. プロンプトが表示されたら削除を確定します。

フォルダーを使用してアプリケーション グループを整理する

フォルダーを作成してアプリケーション グループを整理し、簡単にアクセスできるようにすることができます。

必要な役割

デフォルトでは、次の組み込みロールのいずれかを持っている場合、アプリケーション グループのフォルダーを作成および管理できます。

- クラウド管理者
- フル管理者
- アプリケーション グループ管理者

カスタム ロールを作成することで、管理アクションを他のユーザーに委任できます。次の表に、各アクションに必要な権限を示します。

アクション	必要な権限
アプリケーション グループ フォルダーの作成	アプリケーション グループ フォルダーの作成
アプリケーション グループ フォルダーの削除	アプリケーション グループ フォルダーの削除
アプリケーション グループ フォルダーの移動	アプリケーション グループ フォルダーの移動
アプリケーショングループフォルダーの名前を変更	アプリケーショングループフォルダーの編集

アクション	必要な権限
アプリケーショングループをフォルダーに移動	アプリケーショングループフォルダーの編集、アプリケーショングループプロパティの編集

詳しくは、「役割の作成と管理」を参照してください。

フォルダーの作成と管理

アクションバーまたは右クリックメニューを使用して、アプリケーショングループフォルダーを作成および管理できます。さらに、アプリケーショングループまたはフォルダーをフォルダーツリー内の目的の場所にドラッグできます。

知っておくと良いこと:

- フォルダーは最大5レベルまでネストできます (デフォルトのルートフォルダーを除く)。
- フォルダーには、アプリケーショングループとサブフォルダーを含めることができます。フォルダーとそのサブフォルダーにアプリケーショングループが含まれていない場合にのみ、フォルダーを削除できます。
- すべてのノード (マシンカタログ、デリバリーグループ、アプリケーション、アプリケーショングループなど) は、バックエンドでフォルダーツリーを共有します。フォルダーの名前変更または移動時に他のリソースフォルダーとの名前の競合を避けるため、異なるフォルダーツリー内の第1レベルのフォルダーには異なる名前を付けることをお勧めします。

リモートPCアクセス

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

Remote PC Accessは、Citrix Virtual Apps and Desktopsの機能であり、組織が従業員に企業リソースへのリモートアクセスを安全に簡単に許可できるようにします。Citrixプラットフォームは、ユーザーが物理的なオフィスPCにアクセスできるようにすることで、この安全なアクセスを可能にします。ユーザーがオフィスPCにアクセスできれば、仕事に必要なすべ

てのアプリケーション、データ、リソースにアクセスできます。Remote PC Accessは、テレワークに対応するための他のツールの導入と提供の必要性を排除します。例えば、仮想デスクトップやアプリケーション、およびそれらに関連するインフラストラクチャなどです。

Remote PC Accessは、仮想デスクトップとアプリケーションを提供するCitrix Virtual Apps and Desktopsのコンポーネントと同じものを使用します。その結果、Remote PC Accessの展開と構成の要件とプロセスは、仮想リソースを提供するためのCitrix Virtual Apps and Desktopsの展開に必要なものと同じです。この一貫性により、一貫した統一された管理エクスペリエンスが提供されます。ユーザーは、Citrix HDX™を使用してオフィスPCセッションを配信することで、最高のユーザーエクスペリエンスを得られます。

この機能は、**Remote PC Access**タイプのマシンカタログで構成されており、次の機能を提供します。

- OUを指定してマシンを追加する機能。この機能により、PCの一括追加が容易になります。
- オフィスWindows PCにログオンするユーザーに基づいた自動ユーザー割り当て。シングルユーザーおよび複数ユーザーの割り当てをサポートしています。デフォルトでは、複数のユーザーを次の未割り当てマシンに自動的に割り当てます。自動割り当てをシングルユーザーに制限するには、Web Studioにサインインし、**設定**に移動して、**Remote PC Accessの複数ユーザーの自動割り当てを有効にする**設定をオフにします。

Citrix Virtual Apps and Desktopsは、他の種類のマシンカタログを使用することで、物理PCのより多くのユースケースに対応できます。これらのユースケースには、次のものが含まれます。

- 物理Linux PC
- プールされた物理PC（つまり、ランダムに割り当てられ、専用ではないもの）

注:

サポートされているOSバージョンの詳細については、シングルセッションOSおよびLinux VDAのVDAのシステム要件を参照してください。

オンプレミス展開の場合、Remote PC AccessはCitrix Virtual Apps and Desktops AdvancedまたはPremiumライセンスでのみ有効です。セッションは、他のCitrix Virtual Desktops™セッションと同じ方法でライセンスを消費します。Citrix Cloudの場合、Remote PC AccessはCitrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）およびWorkspace Premium Plusで有効です。

考慮事項

Citrix Virtual Apps and Desktops全般に適用される技術要件と考慮事項はすべてRemote PC Accessにも適用されますが、物理PCのユースケースにより関連性が高かったり、排他的であったりするものもあります。

重要:

Windows 11物理システム（および一部のWindows 10を実行しているシステム）には、仮想化ベースのセキュリティ機能が含まれており、その結果、VDAソフトウェアがそれらを仮想マシンとして誤って検出します。この問題を軽減するには、以下のオプションがあります。

- VDAコマンドラインインストールの一部として、「/remotepc」オプションとともに「/physicalmachine」オプションを使用する
- 以前に言及したオプションを使用しなかった場合は、VDAのインストール後に次のレジストリ値を追加します `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
  - 名前: ForceEnableRemotePC
  - 種類: DWORD
  - データ: 1

展開に関する考慮事項

Remote PC Accessの展開を計画する際には、いくつかの一般的な決定を下します。

- 既存のCitrix Virtual Apps and Desktops展開にRemote PC Accessを追加できます。このオプションを選択する前に、次の点を考慮してください。
  - 現在のDelivery ControllerまたはCloud Connectorは、Remote PC Access VDAに関連する追加の負荷をサポートするのに適切なサイズですか？
  - オンプレミスのサイトデータベースおよびデータベースサーバーは、Remote PC Access VDAに関連する追加の負荷をサポートするのに適切なサイズですか？
  - 既存のVDAと新しいRemote PC Access VDAは、サイトあたりの最大サポートVDA数を超えることになりますか？
- VDAは、自動プロセスを通じてオフィスPCに展開する必要があります。利用可能なオプションは次のとおりです。

  - SCCMなどの電子ソフトウェア配信（ESD）ツール: Install VDAs using SCCM.
  - 展開スクリプト: Install VDAs using scripts.

- Remote PC Access security considerationsを確認してください。

> **注:**
>
> Remote PC Access を設計する際、リモート PC の GPU に接続され、現在構成/動作している物理モニターの数を考慮する必要があります。モニターが Citrix セッションで使用されていなくても、GPU によって検出された場合、そのモニターの存在は GPU がサポートする最大モニター数制限にカウントされます。

マシンカタログに関する考慮事項

必要なマシンカタログの種類は、ユースケースによって異なります。

- Remote PC Accessマシンカタログ
  - Windows専用PC
  - Windows専用マルチユーザーPC。このユースケースは、複数のユーザーが異なるシフトでリモートからアクセスできる物理的なオフィスPCに適用されます。
  - プールされたWindows PC。このユースケースは、コンピューターラボのように、複数のランダムなユーザーがアクセスできる物理PCに適用されます。
- シングルセッションOSマシンカタログ
  - 静的 - 専用Linux PC
  - ランダム - プールされたLinux PC

マシンカタログの種類を特定したら、次の点を考慮してください。

- マシンは一度に1つのマシンカタログにのみ割り当てることができます。
- 委任管理を容易にするために、地理的な場所、部署、または各カタログの管理を適切な管理者に委任しやすくするその他のグループに基づいてマシンカタログを作成することを検討してください。
- マシンアカウントが存在するOUを選択する際は、より詳細な粒度を得るために下位レベルのOUを選択してください。そのような粒度が必要ない場合は、上位レベルのOUを選択できま

す。たとえば、Bank/Officers/Tellers の場合、より詳細な粒度を得るには **Tellers** を選択します。それ以外の場合は、要件に基づいて **Officers** または **Bank** を選択できます。

- Remote PC Access マシンカタログに割り当てられた後にOUを移動または削除すると、VDAの関連付けに影響を与え、将来の割り当てで問題が発生します。したがって、マシンカタログのOU割り当て更新がActive Directoryの変更計画に考慮されるように、適切に計画してください。
- OU構造のためにマシンカタログにマシンを追加するOUを選択するのが難しい場合、OUを選択する必要はありません。後でPowerShellを使用してカタログにマシンを追加できます。デスクトップの割り当てがデリバリーグループで正しく構成されていれば、ユーザーの自動割り当ては引き続き機能します。ユーザー割り当てとともにマシンカタログにマシンを追加するサンプルスクリプトは、GitHubで入手できます。
- 統合されたWake on LANは、**Remote PC Access**タイプのマシンカタログでのみ利用可能です。

Linux VDAに関する考慮事項

以下の考慮事項は、Linux VDAに固有のものです。

- 物理マシンでは、Linux VDAを非3Dモードでのみ使用してください。NVIDIAドライバーの制限により、HDX 3Dモードが有効になっている場合、PCのローカル画面をブラックアウトできず、セッションのアクティビティが表示されます。この画面を表示することはセキュリティリスクです。
- 物理Linuxマシンには、シングルセッションOSタイプのマシンカタログを使用します。
- 自動ユーザー割り当てはLinuxマシンでは利用できません。
- ユーザーがすでにローカルでPCにログオンしている場合、StoreFront™からPCを起動しようとすると失敗します。
- 省電力オプションはLinuxマシンでは利用できません。

技術要件と考慮事項

このセクションでは、物理PCの技術要件と考慮事項について説明します。

- 以下はサポートされていません。
  - KVMスイッチ、またはセッションを切断する可能性のあるその他のコンポーネント。
  - オールインワンPCやNVIDIA Optimus搭載のノートPCおよびPCを含むハイブリッドPC。
  - デュアルブートマシン。

- キーボードとマウスはPCに直接接続してください。モニターや、電源を切ったり切断したりできるその他のコンポーネントに接続すると、これらの周辺機器が使用できなくなる可能性があります。入力デバイスをモニターなどのコンポーネントに接続する必要がある場合は、それらのコンポーネントの電源を切らないでください。
- PCはActive Directory Domain Servicesドメインに参加している必要があります。
- セキュアブートはWindows 10およびWindows 11でのみサポートされています。
- PCにはアクティブなネットワーク接続が必要です。信頼性と帯域幅を向上させるため、有線接続を推奨します。
- Wi-Fiを使用する場合は、以下を実行してください。

  a. 電源設定でワイヤレスアダプターをオンのままにするように設定します。

  b. ユーザーがログオンする前にワイヤレスネットワークに自動接続できるように、ワイヤレスアダプターとネットワークプロファイルを構成します。そうしないと、ユーザーがログオンするまでVDAは登録されません。ユーザーがログオンするまで、PCはリモートアクセスに利用できません。

  c. Wi-FiネットワークからDelivery ControllerまたはCloud Connectorに到達できることを確認してください。

- ノートPCでRemote PC Accessを使用できます。ノートPCがバッテリーではなく電源に接続されていることを確認してください。ノートPCの電源オプションをデスクトップPCのオプションと一致するように構成します。例：

  a. 休止状態機能を無効にします。

  b. スリープ機能を無効にします。

  c. 蓋を閉じたときの動作を「**何もしない**」に設定します。

  d. 「電源ボタンを押したときの動作」を「**シャットダウン**」に設定します。

  e. ビデオカードとNICの省電力機能を無効にします。

- Remote PC Accessは、Windows 10を搭載したSurface Proデバイスでサポートされています。前述のラップトップに関するガイドラインに従ってください。
- ドッキングステーションを使用している場合、ラップトップのドッキング解除と再ドッキングが可能です。ラップトップをドッキング解除すると、VDAはWi-Fi経由でDelivery ControllerまたはCloud Connectorに再登録します。ただし、ラップトップを再ドッキングしても、ワイヤレスアダプターを切断しない限り、VDAは有線接続に切り替わりません。一部のデバイスには、有線接続が確立されたときにワイヤレスアダプターを切断する組み込み機能が備わっています。その他のデバイスでは、ワイヤレスアダプターを切断するためにカスタムソリューショ

ンまたはサードパーティユーティリティが必要です。前述のWi-Fiに関する考慮事項を確認してください。

Remote PC Accessデバイスのドッキングとドッキング解除を有効にするには、次の手順を実行します。

a. **スタート**メニューで、**設定 > システム > 電源とスリープ**を選択し、**スリープ**を**なし**に設定します。

b. **デバイスマネージャー > ネットワークアダプター > イーサネットアダプター**で、**電源の管理**に移動し、**電力の節約のために、コンピューターでこのデバイスの電源をオフにできるようにする**のチェックを外します。**このデバイスで、コンピューターのスタンバイ状態を解除できるようにする**がオンになっていることを確認します。

- 同じオフィスPCにアクセスできる複数のユーザーは、Citrix Workspaceで同じアイコンを表示します。ユーザーがCitrix Workspaceにログオンしたときに、そのリソースが別のユーザーによってすでに使用されている場合、そのリソースは利用不可として表示されます。
- オフィスPCにアクセスする各クライアントデバイス（例：自宅のPC）にCitrix Workspaceアプリをインストールします。

構成シーケンス

このセクションでは、**Remote PC Access**タイプのマシンカタログを使用する場合のRemote PC Accessの構成方法の概要を説明します。他の種類のマシンカタログの作成方法については、「マシンカタログの作成」を参照してください。

1. オンプレミスサイトのみ - 統合されたWake on LAN機能を使用するには、「Wake on LAN」に記載されている前提条件を構成します。
2. Remote PC Access用に新しいCitrix Virtual Apps and Desktopsサイトが作成された場合：

   a. **Remote PC Access**サイトの種類を選択します。

   b. 「**電源管理**」ページで、デフォルトのRemote PC Accessマシンカタログの電源管理を有効または無効にするかを選択します。この設定は、後でマシンカタログのプロパティを編集して変更できます。Wake on LANの構成について詳しくは、「Wake on LAN」を参照してください。

   c. 「**ユーザー**」および「**マシンアカウント**」ページで情報を入力します。

   これらの手順を完了すると、**Remote PC Access Machines**という名前のマシンカタログと、**Remote PC Access Desktops**という名前のデリバリーグループが作成されます。
3. 既存のCitrix Virtual Apps and Desktopsサイトに追加する場合：

a. **Remote PC Access**タイプのマシンカタログを作成します（ウィザードの「オペレーティングシステム」ページ）。マシンカタログの作成方法について詳しくは、「マシンカタログの作成」を参照してください。ターゲットPCがRemote PC Accessで使用できるように、正しいOUを割り当ててください。

b. マシンカタログ内のPCへのユーザーアクセスを提供するデリバリーグループを作成します。デリバリーグループの作成方法について詳しくは、「デリバリーグループの作成」を参照してください。デリバリーグループを、PCへのアクセスを必要とするユーザーを含むActive Directoryグループに割り当ててください。

4. オフィスPCにVDAを展開します。

- シングルセッションOSコアVDAインストーラー（VDAWorkstationCoreSetup.exe）を使用することをお勧めします。
- シングルセッションの完全なVDAインストーラー（VDAWorkstationSetup.exe）を`/remotepc/physicalmachine`オプションとともに使用することもできます。これは、コアVDAインストーラーを使用した場合と同じ結果になります。

> **注：**
>
> RemotePCのインストールでは、特定のユーザーシナリオでVDAが期待どおりに動作するように、`/physicalmachine`引数を`/remotepc`とともに使用します。

- ヘルプデスクチームがCitrix Directorを介してリモートサポートを提供できるように、Windowsリモートアシスタンスを有効にすることを検討してください。そのためには、`/enable_remote_assistance`オプションを使用します。詳しくは、「コマンドラインを使用したインストール」を参照してください。
- Directorでログオン期間情報を表示するには、シングルセッションの完全なVDAインストーラーを使用し、**Citrix User Profile Management WMI Plugin**コンポーネントを含める必要があります。このコンポーネントは、`/includeadditional`オプションを使用して含めます。詳しくは、「コマンドラインを使用したインストール」を参照してください。
- SCCMを使用してVDAを展開する方法について詳しくは、「SCCMを使用したVDAのインストール」を参照してください。
- 展開スクリプトを使用してVDAを展開する方法について詳しくは、「スクリプトを使用したVDAのインストール」を参照してください。

ステップ2〜4を正常に完了すると、ユーザーがPCにローカルでログオンしたときに、自分のマシンに自動的に割り当てられます。

5. ユーザーに、オフィスPCにリモートでアクセスするために使用する各クライアントデバイスにCitrix Workspaceアプリをダウンロードしてインストールするよう指示します。Citrix Workspaceアプリは、`https://www.citrix.com/downloads/`またはサポートされているモバイルデバイスのアプリケーションストアから入手できます。

レジストリを介して管理される機能

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

複数ユーザーの自動割り当てを無効にする

各Delivery Controller™で、次のレジストリ設定を追加します。

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- 名前: AllowMultipleRemotePCAssignments
- 種類: DWORD
- データ: 0

スリープモード (最小バージョン 7.16)

Remote PC Accessマシンをスリープ状態にするには、VDAでこのレジストリ設定を追加し、マシンを再起動します。再起動後、オペレーティングシステムの省電力設定が適用されます。事前設定されたアイドルタイマーが経過すると、マシンはスリープモードに入ります。マシンがウェイクアップすると、Delivery Controllerに再登録されます。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: DisableRemotePCSleepPreventer
- 種類: DWORD
- データ: 1

セッション管理

既定では、ローカルユーザーがそのマシンでセッションを開始すると (CTRL+ALT+DELを押すことで)、リモートユーザーのセッションは自動的に切断されます。この自動的な動作を防ぐには、オフィスPCに以下のレジストリエントリを追加し、その後、マシンを再起動します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: SasNotification
- 種類: DWORD
- データ: 1

デフォルトでは、接続メッセージがタイムアウト期間内に確認されない場合、リモートユーザーがローカルユーザーよりも優先されます。この動作を設定するには、以下の設定を使用します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: RpcaMode
- 種類: DWORD
- データ:
  - 1 - 指定されたタイムアウト期間内にメッセージングUIに応答しない場合、リモートユーザーが常に優先されます。この設定が構成されていない場合、この動作がデフォルトです。
  - 2 - ローカルユーザーが優先されます。

Remote PC Accessモードを適用するためのタイムアウトは、デフォルトで30秒です。このタイムアウトは構成できますが、30秒未満に設定しないでください。タイムアウトを構成するには、このレジストリ設定を使用します。

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: RpcaTimeout
- 種類: DWORD
- データ: タイムアウトの秒数（10進値）

ユーザーが強制的にコンソールアクセスを取得したい場合: ローカルユーザーは、10秒の間にCtrl+Alt+Delを2回押すことで、リモートセッションのローカル制御を取得し、切断イベントを強制できます。

レジストリ変更とマシンの再起動後、リモートユーザーが使用中にローカルユーザーがCtrl+Alt+Delを押してそのPCにログオンしようとすると、リモートユーザーにプロンプトが表示されます。このプロンプトは、ローカルユーザーの接続を許可するか拒否するかを尋ねます。接続を許可すると、リモートユーザーのセッションは切断されます。

セッション管理のログ記録

Remote PC Accessには、アクティブなICA®セッションを持つPCに誰かがアクセスしようとしたときにログを記録するログ機能が追加されました。これにより、不要なアクティビティや予期しないアクティビティがないか環境を監視し、インシデントを調査する必要がある場合にそのようなイベントを監査できます。

イベントはWindowsイベントビューアーを使用してログに記録され、**アプリケーションとサービス > Citrix > HostCore > ICA Service > Admin**にあります。

Remote PC Accessを使用すると、3つの異なるイベントがログに記録されます。

Ctrl+Alt+Delイベント

このイベントは、アクティブなリモートセッション中にローカルユーザーがコンソールキーボードでCtrl+Alt+Delを押したときに表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベントID: 43, 44, 45
- ソース: ICA サービス

イベント ID 43

このイベント ID は、SasNotification レジストリ値が存在しない場合、または SasNotification レジストリ値が 0 の場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to automatically disconnect the
remote session.
```

イベント ID 44

このイベント ID は、SasNotification レジストリ値が 1 で、RpcaMode レジストリ値が 1 の場合、または RpcaMode レジストリ値が存在しない場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user. The
user preference is set to remote user.
```

イベント ID 45

このイベント ID は、SasNotification レジストリ値が 1 で、RpcaMode レジストリ値が 2 の場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user.

The user preference is set to local user.
```

リモートセッション切断イベント

このイベントは、さまざまな理由でリモートセッションが切断されたときに表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベント ID: 46, 47, 48
- ソース: ICA Service

イベントID 46

このイベントIDは、リモートセッションが切断され、SasNotification レジストリ値が存在しないか、SasNotification レジストリ値が0である場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected.
```

イベントID 47

このイベントIDは、リモートユーザーがセッションの切断に同意し、SasNotification レジストリ値が1であり、RpcaMode レジストリ値が1であるか、RpcaMode レジストリ値が2であるか、または RpcaMode レジストリ値が存在しない場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected
because the user accepted the request to disconnect the session.
```

イベントID 48

このイベントIDは、リモートユーザーが指定されたタイムアウト期間内に切断要求を拒否せず、SasNotification レジストリ値が1であり、RpcaMode レジストリ値が2である場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected
because the user did not decline the disconnection request within the
configured timeout period (&lt;timeout period>).
```

Ctrl+Alt+Del 2回押しイベント

このイベントは、10秒以内にCtrl+Alt+Delが2回押された場合に表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベントID: 49
- ソース: ICA Service

イベントID 49

このイベントIDは、Ctrl+Alt+Delが10秒以内に2回押されたときに表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been forcibly
disconnected.
```

ウェイク・オン・LAN

Remote PC AccessはWake on LANをサポートしており、ユーザーは物理PCをリモートで起動できます。この機能により、ユーザーは使用していないときにオフィスPCの電源を切ったままにして、エネルギーコストを節約できます。また、誤ってマシンの電源が切れてしまった場合でも、リモートアクセスを可能にします。

Wake on LAN機能を使用すると、デリバリーコントローラーからの指示があった場合、マジックパケットはPC上で実行されているVDAから、PCが存在するサブネットに直接送信されます。これにより、マジックパケットの配信のために追加のインフラストラクチャコンポーネントやサードパーティソリューションに依存することなく、この機能が動作します。

Wake on LAN機能は、レガシーなSCCMベースのWake on LAN機能とは異なります。SCCMベースのWake on LANの詳細については、「Wake on LAN – SCCM統合」を参照してください。

制限事項

Wake on LAN機能を使用するRemote PC Accessは、ピーク時の自動電源オンをサポートしていません。

システム要件

Wake on LAN機能を使用するためのシステム要件は次のとおりです。

- コントロールプレーン:
  - シトリックス DaaS™
  - シトリックス バーチャル アプリケーションズ アンド デスクトップス 2009以降
- 物理PC：
  - VDAバージョン2009以降
  - Windows 10またはWindows 11。サポートの詳細については、VDAシステム要件を参照してください。
  - BIOS/UEFIでWake on LANが有効になっていること
  - Windows構成内のネットワークアダプターのプロパティでWake on LANが有効になっていること

Wake on LANの構成

オンプレミスのCitrix Virtual Apps and Desktopsを使用している場合、統合Wake on LANの構成はPowerShellを使用してのみサポートされます。

Wake on LANを構成するには:

1. まだ作成していない場合は、Remote PC Accessマシンカタログを作成します。
2. まだ作成していない場合は、Wake on LANホスト接続を作成します。

> **注：**
>
> Wake on LAN機能を使用するには、「Microsoft Configuration Manager Wake on LAN」タイプのホスト接続がある場合、新しいホスト接続を作成します。

3. Wake on LAN ホスト接続の一意の識別子を取得します。
4. Wake on LAN ホスト接続をマシンカタログに関連付けます。

Wake on LAN ホスト接続を作成するには：

```
# Load Citrix SnapIns

Add-PSSnapIn -Name "*citrix*"



# Provide the name of the Wake on LAN host connection

[string]$connectionName = "Remote PC Access Wake on LAN"



# Create the hypervisor connection

$hypHc = New-Item -Path xdhyp:\Connections `

                -Name $connectionName `

                -HypervisorAddress "N/A" `

                -UserName "woluser" `

                -Password "wolpwd" `

                -ConnectionType Custom `
```

```
                -PluginId VdaWOLMachineManagerFactory `
                -CustomProperties "<CustomProperties></CustomProperties>"
`
                -Persist


$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid


# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{
    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid
}
```

ホスト接続の準備ができたら、次のコマンドを実行してホスト接続の一意の識別子を取得します。

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
$hypUid = $bhc.Uid
```

接続の一意の識別子を取得したら、次のコマンドを実行して、その接続を Remote PC Access マシンカタログに関連付けます。

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog
-RemotePCHypervisorConnectionUid $hypUid
```

設計上の考慮事項

Remote PC Access で Wake on LAN を使用する予定がある場合は、次の点を考慮してください。

- 複数のマシンカタログで同じWake on LANホスト接続を使用できます。
- あるPCが別のPCを起動するには、両方のPCが同じサブネット内にあり、同じWake on LANホスト接続を使用している必要があります。PCが同じマシンカタログにあるか、異なるマシンカタログにあるかは関係ありません。
- ホスト接続は特定のゾーンに割り当てられます。展開に複数のゾーンが含まれる場合、各ゾーンにWake on LANホスト接続が必要です。これはマシンカタログにも当てはまります。
- マジックパケットは、グローバルブロードキャストアドレス255.255.255.255を使用してブロードキャストされます。このアドレスがブロックされていないことを確認してください。
- そのサブネット内のマシンを起動できるようにするには、Wake on LAN接続ごとに、サブネット内で少なくとも1台のPCがオンになっている必要があります。

運用上の考慮事項

Wake on LAN機能を使用する際の考慮事項は次のとおりです。

- 統合されたWake on LAN機能を使用してPCを起動するには、VDAが少なくとも1回登録されている必要があります。
- Wake on LANはPCを起動するためにのみ使用できます。再起動やシャットダウンなどの他の電源操作はサポートしていません。
- Wake on LAN接続が作成されると、Web Studioに表示されます。ただし、Citrix Virtual Apps and Desktopsオンプレミスを使用している場合、Web Studio内でのプロパティの編集はサポートされていません。
- マジックパケットは次の2つの方法のいずれかで送信されます。
  a. ユーザーがPCへのセッションを起動しようとしたときにVDAが登録解除されている場合
  b. 管理者がWeb StudioまたはPowerShellから手動で電源オンコマンドを送信した場合
- デリバリーコントローラーはPCの電源状態を認識しないため、Web Studioでは電源状態の下に**サポートされていません**と表示されます。デリバリーコントローラーは、VDAの登録状態を使用してPCのオン/オフを判断します。

Wake on LAN – SCCM統合

SCCM統合Wake on LANは、Remote PC Accessの代替Wake on LANオプションであり、オンプレミスのCitrix Virtual Apps and Desktopsでのみ利用可能です。

システム要件

SCCM統合Wake on LAN機能を使用するためのシステム要件は次のとおりです。

- Citrix Virtual Apps and Desktops のバージョン1912以降
- 物理PC:
  - VDA バージョン 1912 以降
  - Windows 10。サポートの詳細については、VDA システム要件を参照してください。
  - BIOS/UEFIでWake on LANが有効になっていること
  - Windows構成内のネットワークアダプターのプロパティでWake on LANが有効になっていること
- System Center Configuration Manager (SCCM) のバージョン2012 R2以降

SCCM 統合型 Wake on LAN の構成

以下の前提条件を完了してください。

1. 組織内でSCCM 2012 R2、2016、または2019を構成します。次に、すべてのRemote PC AccessマシンにSCCMクライアントを展開し、スケジュールされたSCCMインベントリサイクルが実行されるのを待つか、必要に応じて手動で強制実行します。
2. Wake Proxyのサポートについては、SCCMでオプションを有効にします。Remote PC AccessのWake on LAN機能を使用するPCを含む組織内の各サブネットについて、3台以上のマシンがセンチネルマシンとして機能できることを確認します。
3. マジックパケットのサポートについては、サブネット指向ブロードキャストまたはユニキャストのいずれかを使用して、マジックパケットが送信されるようにネットワークルーターとファイアウォールを構成します。
4. 各PCのBIOS/UEFI設定でWake on LANを構成します。
5. まだVDAを展開していない場合は、物理PCにVDAを展開します。

前提条件に対処した後、Delivery Controller が SCCM と通信できるように、次の手順を完了します。

1. SCCMのホスト接続を作成します。詳細については、「接続とリソース」を参照してください。
   - 接続の種類として **Microsoft Configuration Manager Wake on LAN** を選択します。
   - 入力された資格情報には、スコープ内のコレクションへのアクセス権があり、**Remote Tools Operator** ロールが必要です。

2. Web Studioで接続を選択し、**接続の編集** を選択して、**詳細** をクリックします。
3. Wake on LANを処理するための適切なオプションを選択します。
    - Wake-upプロキシを使用している場合は、最初のオプションである **Microsoft System Center Configuration Manager Wake-up proxy** を選択します。
    - マジックパケットを使用している場合は、2番目のオプションである **Delivery Controllerによって送信されるWake on LANパケット** を選択します。
        - 適切な送信方法を選択します: **サブネット指向ブロードキャスト** または **ユニキャスト**。

ホスト接続を作成したら、その接続をRemote PC Accessカタログに関連付けます。

- 新しいRemote PC Accessカタログを作成する場合は、カタログ作成ウィザードの**オペレーティングシステム**ページで、カタログの種類として**Remote PC Access**を選択し、ドロップダウンリストから適切な接続を選択します。
- 既存のRemote PC AccessカタログにWake on LANを追加するには:
    a. Web Studioで**マシンカタログ**ノードに移動し、マシンカタログを選択して、**マシンカタログの編集**を選択します。
    b. **電源管理**タブを選択し、**はい**を選択してマシンカタログの電源管理を有効にします。
    c. ドロップダウンリストから適切な接続を選択し、**OK**をクリックします。

トラブルシューティング

モニターのブランキングが機能しない

アクティブなHDXセッション中にWindows PCのローカルモニターがブランクにならない場合（ローカルモニターにセッションで発生している内容が表示される場合）、GPUベンダーのドライバーに問題がある可能性があります。この問題を解決するには、次のレジストリ値を設定して、Citrix Indirect Displayドライバー（IDD）にグラフィックカードのベンダードライバーよりも高い優先順位を与えます。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- 名前: CitrixIDD
- 種類: DWORD
- データ: 3

ディスプレイアダプターの優先順位とモニターの作成の詳細については、Knowledge Centerの記事CTX237608を参照してください。

セッション管理通知が有効になっているマシンでCtrl+Alt+Delを選択すると、セッションが切断されます

SasNotificationレジストリ値によって制御されるセッション管理通知は、VDAでRemote PC Accessモードが有効になっている場合にのみ機能します。物理PCでHyper-Vの役割または仮想化ベースのセキュリティ機能が有効になっている場合、そのPCは仮想マシンとして報告されます。VDAが仮想マシン上で実行されていることを検出すると、Remote PC Accessモードを自動的に無効にします。Remote PC Accessモードを有効にするには、次のレジストリ値を追加します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: ForceEnableRemotePC
- 種類: DWORD
- データ: 1

設定を有効にするには、PCを再起動します。

診断情報

Remote PC Accessに関する診断情報は、Windowsアプリケーションイベントログに書き込まれます。情報メッセージはスロットリングされません。エラーメッセージは、重複するメッセージを破棄することでスロットリングされます。

- 3300（情報）: マシンがカタログに追加されました
- 3301（情報）: マシンがデリバリーグループに追加されました
- 3302（情報）: マシンがユーザーに割り当てられました
- 3303 (エラー): 例外

電源管理

Remote PC Accessの電源管理が有効になっている場合、サブネット指向ブロードキャストでは、Controllerとは異なるサブネットにあるマシンを起動できないことがあります。サブネット指向ブロードキャストを使用してサブネット間で電源管理が必要で、AMTサポートが利用できない場合は、Wake-upプロキシまたはユニキャスト方式を試してください。これらの設定が電源管理接続の詳細プロパティで有効になっていることを確認してください。

アクティブなリモートセッションはローカルのタッチスクリーン入力を記録します

VDA が Remote PC Access モードを有効にすると、マシンはアクティブなセッション中にローカルのタッチスクリーン入力を無視します。物理 PC で Hyper-V ロールまたは仮想化ベースのセキュリティ機能が有効になっている場合、その PC は仮想マシンとして報告されます。VDA が仮想マシン上で実行されていることを検出すると、Remote PC Access モードを自動的に無効にします。Remote PC Access モードを有効にするには、次のレジストリ設定を追加します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: ForceEnableRemotePC
- 種類: DWORD
- データ: 1

設定を有効にするには、PC を再起動してください。

その他のリソース

以下は Remote PC Access に関するその他のリソースです。

- ソリューション設計ガイダンス: Remote PC Access Design Decisions。
- Remote PC Access アーキテクチャの例: Citrix Remote PC Access ソリューションのリファレンスアーキテクチャ。

コンテンツを公開する

> **注:**

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

> Microsoft WordドキュメントやWebリンクなどのリソースへのURLまたはUNCパスにすぎないアプリケーションを公開できます。この機能は公開コンテンツとして知られています。コンテンツを公開する機能により、ユーザーへのコンテンツ配信方法に柔軟性が加わります。既存のアクセス制御とアプリケーション管理の恩恵を受けることができます。また、コンテ

> ンツを開くためにローカルアプリケーションを使用するか、公開アプリケーションを使用するかを指定することもできます。

公開されたコンテンツは、StoreFront™およびCitrix Workspace™アプリの他のアプリケーションと同様に表示されます。ユーザーはアプリケーションにアクセスするのと同じ方法でアクセスします。クライアントでは、リソースは通常どおり開きます。

- ローカルにインストールされたアプリケーションが適切な場合、それが起動されてリソースが開かれます。
- ファイルの種類関連付けが定義されている場合、公開されたアプリケーションが起動されてリソースが開かれます。

コンテンツはPowerShell SDKを使用して公開します。Web Studioを使用してコンテンツを公開することはできません。ただし、公開後にWeb Studioを使用してアプリケーションのプロパティを編集することはできます。

構成の概要と準備

コンテンツの公開には、次の主要なプロパティを持つ `New-BrokerApplication` コマンドレットを使用します。（すべてのコマンドレットプロパティの説明については、コマンドレットのヘルプを参照してください。）

```
New-BrokerApplication –ApplicationType PublishedContent
-CommandLineExecutable location -Name app-name -DesktopGroup delivery-
group-name
```

`ApplicationType` プロパティは `PublishedContent` である必要があります。

`CommandLineExecutable` プロパティは、公開されたコンテンツの場所を指定します。255文字の制限があり、以下の形式がサポートされています。

- HTML Webサイトアドレス（例: `<http://www.citrix.com>`）
- Webサーバー上のドキュメントファイル（例: `https://www.citrix.com/press/pressrelease.doc`）
- FTPサーバー上のディレクトリ（例: `ftp://ftp.citrix.com/code`）
- FTPサーバー上のドキュメントファイル（例: `ftp://ftp.citrix.com/code/Readme.txt` >）
- UNCディレクトリパス（例: `file://myServer/myShare or \\\\myServer\\myShare`）

- UNCファイルパス（例: `file://myServer/myShare/myFile.asf` または `\\myServer\myShare\myFile.asf`）

正しいSDKがあることを確認してください。

- Citrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）の展開の場合、Citrix Virtual Apps and Desktops Remote PowerShell SDKをダウンロードしてインストールします。
- オンプレミスのCitrix Virtual Apps and Desktops展開の場合、Delivery Controllerとともにインストールされているの PowerShell SDKを使用します。公開コンテンツアプリケーションを追加するには、最低バージョン7.11のDelivery Controllerが必要です。

次の手順では例を使用します。例では次のようになります。

- マシンカタログが作成されています。
- `PublishedContentApps` という名前のデリバリーグループが作成されています。このグループは、カタログからマルチセッションOSマシンを使用します。WordPadアプリケーションがグループに追加されています。
- デリバリーグループ名、`CommandLineExecutable` の場所、およびアプリケーション名が割り当てられます。

はじめに

PowerShell SDKを含むマシンで、PowerShellを開きます。

次のコマンドレットは、適切なPowerShell SDKスナップインを追加し、返されたデリバリーグループレコードを割り当てます。

`Add-PsSnapin Citrix* $dg = Get-BrokerDesktopGroup –Name PublishedContentApps`

Citrix DaaSを使用している場合は、Citrix Cloud™の資格情報を入力して認証します。顧客が複数いる場合は、1つを選択します。

URLを公開する

場所とアプリケーション名を割り当てた後、次のコマンドレットは、Citrixのホームページをアプリケーションとして公開します。

```
$citrixUrl = "https://www.citrix.com/"

$appName = "Citrix Home Page"
```

```
New-BrokerApplication –ApplicationType PublishedContent –
CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.Uid
```

成功を確認します:

- StoreFrontを開き、PublishedContentAppsデリバリーグループ内のアプリケーションにアクセスできるユーザーとしてログオンします。デフォルトのアイコンを持つ新しく作成されたアプリケーションが表示されます。アイコンのカスタマイズについては、`<https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/>`を参照してください。
- **Citrix Home Page**アプリケーションをクリックします。URLは、ローカルで実行されているデフォルトブラウザの新しいタブで起動します。

UNCパスにあるリソースを公開する

この例では、管理者は`PublishedResources`という名前の共有をすでに作成しています。場所とアプリケーション名を割り当てた後、以下のコマンドレットはその共有内のRTFファイルとDOCXファイルをリソースとして公開します。

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\\PublishedResources\\PublishedRTF.rtf"

$rtfAppName = "PublishedRTF"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $rtfUNC -Name $rtfAppName

-DesktopGroup $dg.Uid



$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx"

$docxAppName = "PublishedDOCX"
```

```
New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $docxUNC -Name $docxAppName

-DesktopGroup $dg.Uid
```

成功を確認する:

- StoreFrontウィンドウを更新して、新しく公開されたドキュメントを表示します。
- **PublishedRTF**および**PublishedDOCX**アプリケーションをクリックします。各ドキュメントは、ローカルで実行されているWordPadで開きます。

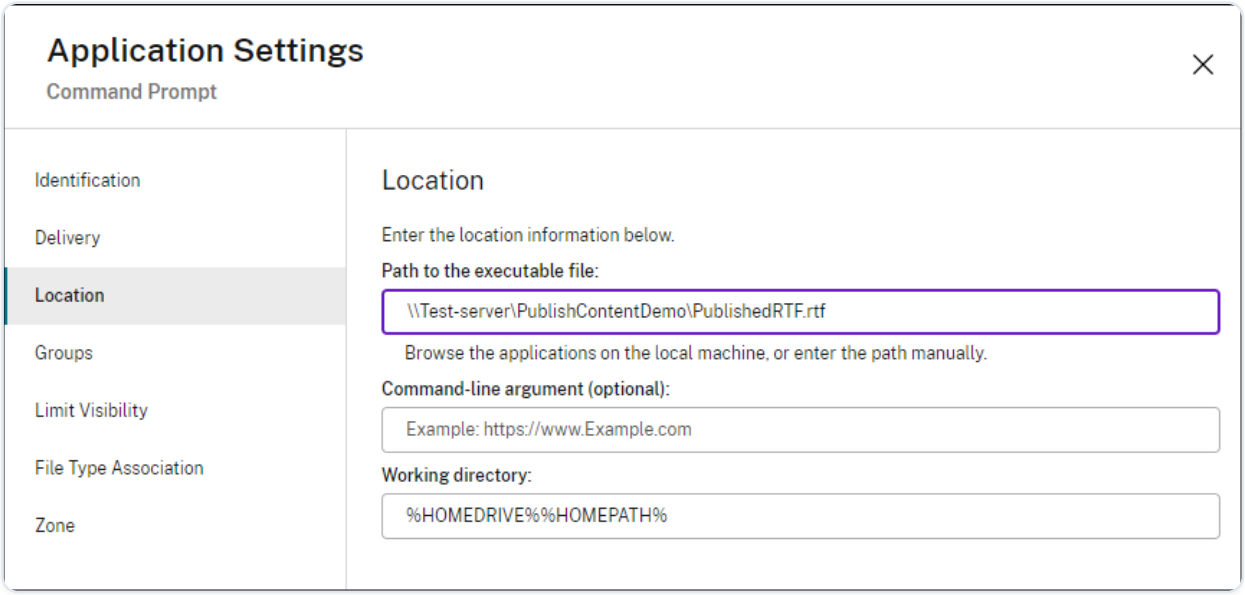
PublishedContentアプリケーションの表示と編集

公開されたコンテンツは、他のアプリケーションタイプで使用する方法と同じ方法で管理します。

`PublishedContent`アプリケーションを表示および編集するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**アプリケーション**を選択します。
2. **アプリケーション**タブで、PublishedContentアプリケーションを選択し、次に**プロパティ**を選択します。

   アプリケーションのプロパティ（ユーザーの可視性、グループの関連付け、ショートカットなど）は、公開されたコンテンツに適用されます。ただし、**場所**ページでは、コマンドライン引数または作業ディレクトリのプロパティを変更することはできません。
3. リソースを変更するには、そのページの**実行可能ファイルへのパス**フィールドを変更します。



4. 公開されたアプリケーションを使用して`PublishedContent`アプリケーション（ローカルアプリケーションではなく）を開くには、次の手順に従います。

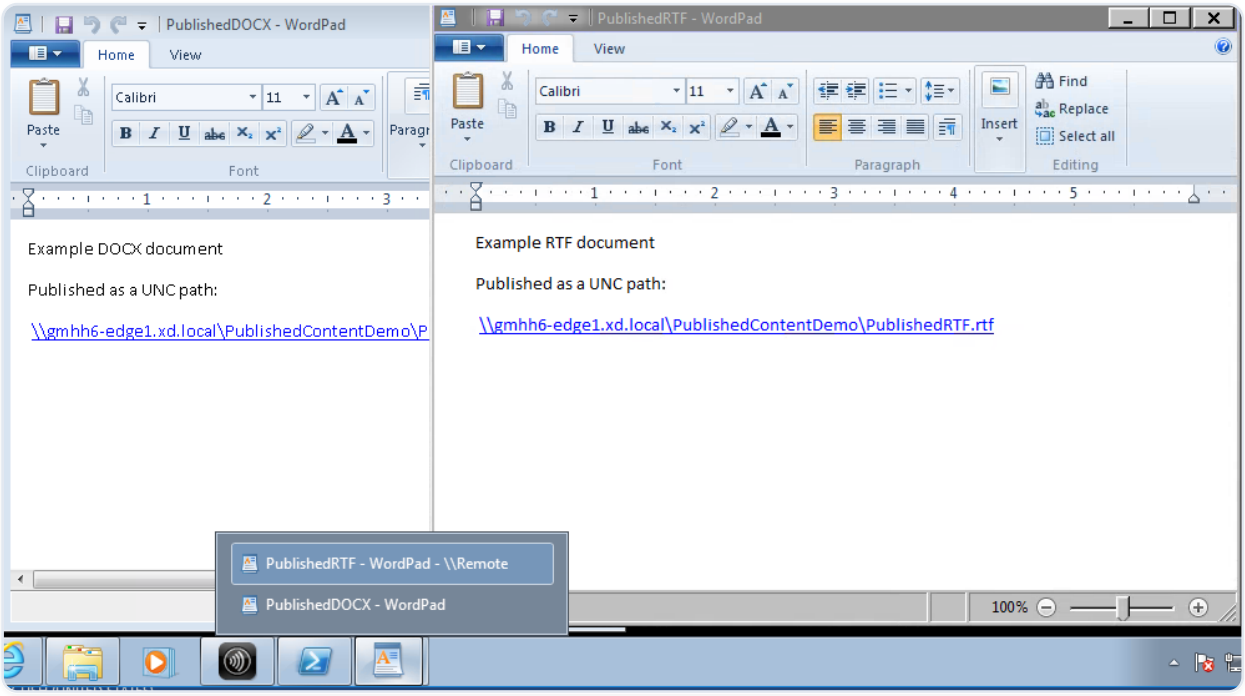
   この例では、公開されたWordPadアプリケーションが編集され、.rtfファイル用のファイルタイプ関連付けが作成されます。

   a. デリバリーグループのメンテナンスモードをオンにします。

   b. **ファイルタイプ関連付け**プロパティを編集します。

   c. 完了したらメンテナンスモードをオフにします。

   d. StoreFrontを更新してファイルタイプ関連付けの変更を読み込み、**PublishedRTF**および**PublishedDOCX**アプリケーションをクリックします。違いに注目してください。**PublishedDOCX**は引き続きローカルのWordPadで開きます。ただし、**PublishedRTF**はファイルタイプ関連付けにより、公開されたWordPadで開くようになりました。



詳細情報

- マシンカタログの作成
- デリバリーグループの作成
- アプリケーションプロパティの変更

サーバー VDI

Server VDI (Virtual Desktop Infrastructure) 機能を使用して、単一ユーザー向けにサーバーオペレーティングシステムからデスクトップを配信します。

- エンタープライズ管理者は、サーバーオペレーティングシステムをVDIデスクトップとして配信できます。これは、エンジニアやデザイナーなどのユーザーにとって価値があります。
- サービスプロバイダーは、クラウドからデスクトップを提供できます。これらのデスクトップは、Microsoft Services Provider License Agreement (SPLA) に準拠しています。

サポート:

- Citrix Virtual Apps and Desktops™ および Citrix DaaS (旧 Citrix Virtual Apps and Desktops service) の展開では、Server VDI は Windows Server 2022 および Windows Server 2019 でサポートされています。
- すべてのServer VDI展開は、ユーザーパーソナライゼーションレイヤーテクノロジーをサポートしています。
- Server VDI がスキャナーなどの TWAIN デバイスで動作するには、Windows Server のデスクトップエクスペリエンス機能がインストールされている必要があります。
- 以下の機能はServer VDIでは使用できません:
  - ホスト型アプリケーション
  - ローカルアプリアクセス
  - 直接 (ブローカーなし) デスクトップ接続
  - リモートPCアクセス

Server VDIのインストールと構成

1. Windowsサーバーをインストール用に準備します。
   - Windows Server Manager を使用して、リモートデスクトップサービス役割サービスがインストールされていないことを確認します。以前にインストールされていた場合は、削除してください。これらの役割サービスがインストールされていると、VDA のインストールは失敗します。
   - **各ユーザーを単一セッションに制限する**プロパティが有効になっていることを確認します。Windows サーバーで、ターミナルサーバー設定のレジストリを編集します。

     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server`

     `DWORD fSingleSessionPerUser = 1`
2. Citrix Virtual Apps and Desktops インストーラーのコマンドラインインターフェイスを使用して、サポートされているサーバーまたはサーバーマスターイメージに VDA をインストールし、`/quiet` および `/servervdi` オプションを指定します。（デフォルトでは、インストー

ラーのグラフィカルインターフェイスは、サーバーオペレーティングシステム上のWindowsシングルセッションOS VDAをブロックします。コマンドラインを使用すると、この動作が上書きされます。）次のいずれかのコマンドを使用します。

- Citrix Virtual Apps and Desktops 展開の場合：
  - `XenDesktopVdaSetup.exe /quiet /servervdi`
  - `VDAWorkstationSetup.exe /quiet /servervdi`
- Citrix DaaS™ 展開の場合：
  - `VDAWorkstationSetup.exe /quiet /servervdi`

その他のオプション：

- Delivery Controller または Cloud Connector を指定するには、`/controllers` を使用します。
- ファイアウォールを手動で構成しない限り、ファイアウォールでポートを開くには `/enable_hdx_ports` を使用します。
- イメージに VDA をインストールし、そのイメージから MCS を使用してサーバー VM を作成する場合は、`/mastermcsimage` (または `/masterimage`) を使用します。
- すべてのオプションの詳細については、「コマンドラインを使用したインストール」を参照してください。

3. Server VDI 用のマシンカタログを作成します。カタログ作成ウィザードで:
   - **オペレーティングシステム**ページで、**シングルセッションOS**を選択します。
   - **概要**ページで、Server VDIであることを明確に識別できるマシンカタログ名と管理者向けの記述を指定します。これは、カタログがServer VDIをサポートしていることをStudioで示す唯一のインジケーターです。

   Studioで検索を使用すると、VDAがマルチセッションマシンにインストールされている場合でも、Server VDIカタログは**シングルセッションOSマシン**タブに表示されます。
4. デリバリーグループを作成し、作成したServer VDIカタログを選択します。

VDAのインストール中にDelivery ControllerまたはCloud Connectorを指定しなかった場合は、後でそれらを指定することを忘れないでください。詳細については、「VDA登録」を参照してください。

ユーザーパーソナライゼーションレイヤー

注:

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

Citrix Virtual Apps and Desktopsのユーザーパーソナライゼーションレイヤー機能は、非永続マシンカタログの機能を拡張し、セッション間でユーザーのデータとローカルにインストールされたアプリケーションを保持します。基盤となるCitrix App Layeringテクノロジーを搭載したユーザーパーソナライゼーションレイヤー機能は、非永続マシンカタログでCitrix ProvisioningおよびMachine Creation Services™ (MCS)をサポートします。

マスターイメージ内でVirtual Delivery Agentとともにユーザーパーソナライゼーションレイヤーコンポーネントをインストールします。VHDファイルは、ユーザーがローカルにインストールしたアプリケーションを保存します。イメージにマウントされたVHDは、ユーザー自身の仮想ハードドライブとして機能します。

重要:

Citrix Virtual Apps and Desktopsでユーザーパーソナライゼーションレイヤーを展開するか、イメージテンプレートで有効になっているApp Layeringユーザーレイヤーを展開することができますが、両方を展開することはできません。App Layering内のレイヤーにユーザーパーソナライゼーションレイヤー機能をインストールしないでください。

この機能はPersonal vDisk (PvD)に代わるものであり、非永続（プールされた）デスクトップ環境でユーザーに永続的なワークスペースエクスペリエンスも提供します。

ユーザーパーソナライゼーションレイヤー機能を展開するには、記事に詳述されている手順を使用してインストールおよび構成します。

アプリケーションのサポート

以下の例外を除き、ユーザーがデスクトップにローカルでインストールするすべてのアプリケーションは、ユーザーパーソナライゼーションレイヤーでサポートされます。

例外

以下のアプリケーションは例外であり、ユーザーパーソナライゼーションレイヤーではサポートされません。

- MS OfficeやVisual Studioなどのエンタープライズアプリケーション。
- ネットワークスタックまたはハードウェアを変更するアプリケーション。例：VPNクライアント。
- ブートレベルのドライバーを持つアプリケーション。例：ウイルススキャナー。
- ドライバー ストアを使用するドライバーを持つアプリケーション。例：プリンタードライバー。

> **注:**
>
> Windowsグループポリシーオブジェクト（GPO）を使用してプリンターを利用可能にすることができます。

サポートされていないアプリケーションをローカルにインストールすることをユーザーに*許可しないでください*。代わりに、これらのアプリケーションはマスターイメージに直接インストールしてください。

ローカルユーザーまたは管理者アカウントを必要とするアプリケーション

ユーザーがアプリケーションをローカルにインストールすると、そのアプリはユーザーレイヤーに格納されます。その後、ユーザーがローカルユーザーまたはグループを追加または編集しても、その変更はセッションを超えて保持されません。

> **重要:**
>
> 必要なローカルユーザーまたはグループは、マスターイメージに追加してください。

要件

ユーザーパーソナライゼーションレイヤー機能には、次のコンポーネントが必要です。

- Citrix バーチャルアプリとデスクトップ 7 1909 以降
- Virtual Delivery Agent (VDA)、バージョン1912以降

- Citrix Provisioning™、バージョン1909以降
- Windowsファイル共有 (SMB)、またはオンプレミスAD認証が有効なAzure Files

OSがシングルセッションとして展開されている場合、以下のWindowsバージョンにユーザーパーソナライゼーションレイヤー機能を展開できます。サポートはシングルセッション上の単一ユーザーに限定されます。

- ウィンドウズ 11 エンタープライズ x64
- Windows 10 Enterprise x64、バージョン1607以降
- Windows Server 2019 (Azure Filesがサポートされています)
- Windows Server 2022 (Azure Filesがサポートされています)

Citrix Virtual Apps and Desktops 7の場合、ユーザーパーソナライゼーションレイヤーでのAzure Filesの使用は、Windows Server 2022、Windows Server 2019、およびWindows 10クライアントでサポートされています。

> **注：**
>
> サーバーOSを使用している場合、Server VDIのみがサポートされます。展開の詳細については、Server VDIの記事を参照してください。
>
> ユーザーパーソナライゼーションレイヤーは、マシンごとに一度に1人のユーザーのみをサポートし、その後、ディスクをリセットするためにマシンを再起動する必要があります。ユーザーパーソナライゼーションレイヤーは、マルチセッションサーバーオペレーティングシステムでは使用できず、シングルセッションサーバーシステムでのみ使用できます。ユーザーパーソナライゼーションレイヤーは、非永続デスクトップでのみサポートされます。
>
> ユーザーパーソナライゼーションレイヤー機能がインストールされている場合は、アンインストールします。最新リリースをインストールする前に、マスターイメージを再起動します。

ファイル共有をセットアップする

ユーザーパーソナライゼーションレイヤー機能には、Windows Server Message Block (SMB) ストレージが必要です。Windowsファイル共有を作成するには、使用しているWindowsオペレーティングシステムの通常の手順に従ってください。

Azureベースのカタログでは Azure Files を使用する方法の詳細については、ユーザーパーソナライゼーションレイヤー用のAzure Filesストレージをセットアップするを参照してください。

推奨事項

ユーザーパーソナライゼーションレイヤーの展開を成功させるには、このセクションの推奨事項に従ってください。

マイクロソフト システムセンター コンフィギュレーションマネージャー (SCCM)

ユーザーパーソナライゼーションレイヤー機能でSCCMを使用している場合は、VDI環境でイメージを準備するためのMicrosoftガイドラインに従ってください。詳細については、このMicrosoft TechNet記事を参照してください。

ユーザーレイヤーのサイズ

ユーザーレイヤーは、ディスク上のスペースが使用されるにつれて拡張するシンプロビジョニングされたディスクです。ユーザーレイヤーに許可されるデフォルトサイズは10 GBで、これは推奨される最小サイズです。

> **注:**
>
> インストール中に値がゼロ (0) に設定されている場合、デフォルトのユーザーレイヤーサイズは10 GBに設定されます。

> ユーザーレイヤーのサイズを変更したい場合は、**User Layer Size**ポリシーに別の値を入力できます。**Optional: Click Select next to User Layer Size in GB.の下にある手順5：デリバリーグループのカスタムポリシーを作成する**を参照してください。

ユーザーレイヤーのサイズを上書きするためのツール (オプション)

Windowsツールを使用してユーザーレイヤーファイル共有にクォータを定義することで、ユーザーレイヤーのサイズを上書きできます。

以下のMicrosoftクォータツールのいずれかを使用して、**Users**という名前のユーザーレイヤーディレクトリにハードクォータを設定します。

- ファイルサーバーリソースマネージャー (FSRM)
- クォータマネージャー

注:

クォータを増やすと、新しいユーザーレイヤーに影響し、既存のユーザーレイヤーが拡張されます。クォータを減らすと、新しいユーザーレイヤーのみに影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

ユーザーパーソナライゼーションレイヤーを展開する

ユーザーパーソナライゼーション機能を展開する際は、Web Studio内でポリシーを定義します。その後、その機能を展開するマシンカタログにバインドされたデリバリーグループにポリシーを割り当てます。

マスターイメージにユーザーパーソナライゼーションレイヤーの設定がない場合、サービスはアイドル状態のままであり、オーサリングアクティビティを妨げません。

マスターイメージでポリシーを設定すると、サービスはマスターイメージ内でユーザーレイヤーを実行およびマウントしようとします。マスターイメージは予期しない動作や不安定性を示します。

ユーザーパーソナライゼーションレイヤー機能を展開するには、次の手順をこの順序で完了します。

- ステップ1：Citrix Virtual Apps and Desktops環境の可用性を確認します。
- ステップ2：マスターイメージを準備します。
- ステップ3：マシンカタログを作成します。
- ステップ4：デリバリーグループを作成します。
- ステップ5：デリバリーグループのカスタムポリシーを作成します。

注:

イメージ上のWindows 10をアップグレードした後、初回ログインには通常よりも時間がかかります。ユーザーのレイヤーが新しいバージョンのWindows 10用に更新される必要があり、その結果、ログオン時間が増加します。

ステップ 1: Citrix Virtual Apps and Desktops 環境が利用可能であることを確認する

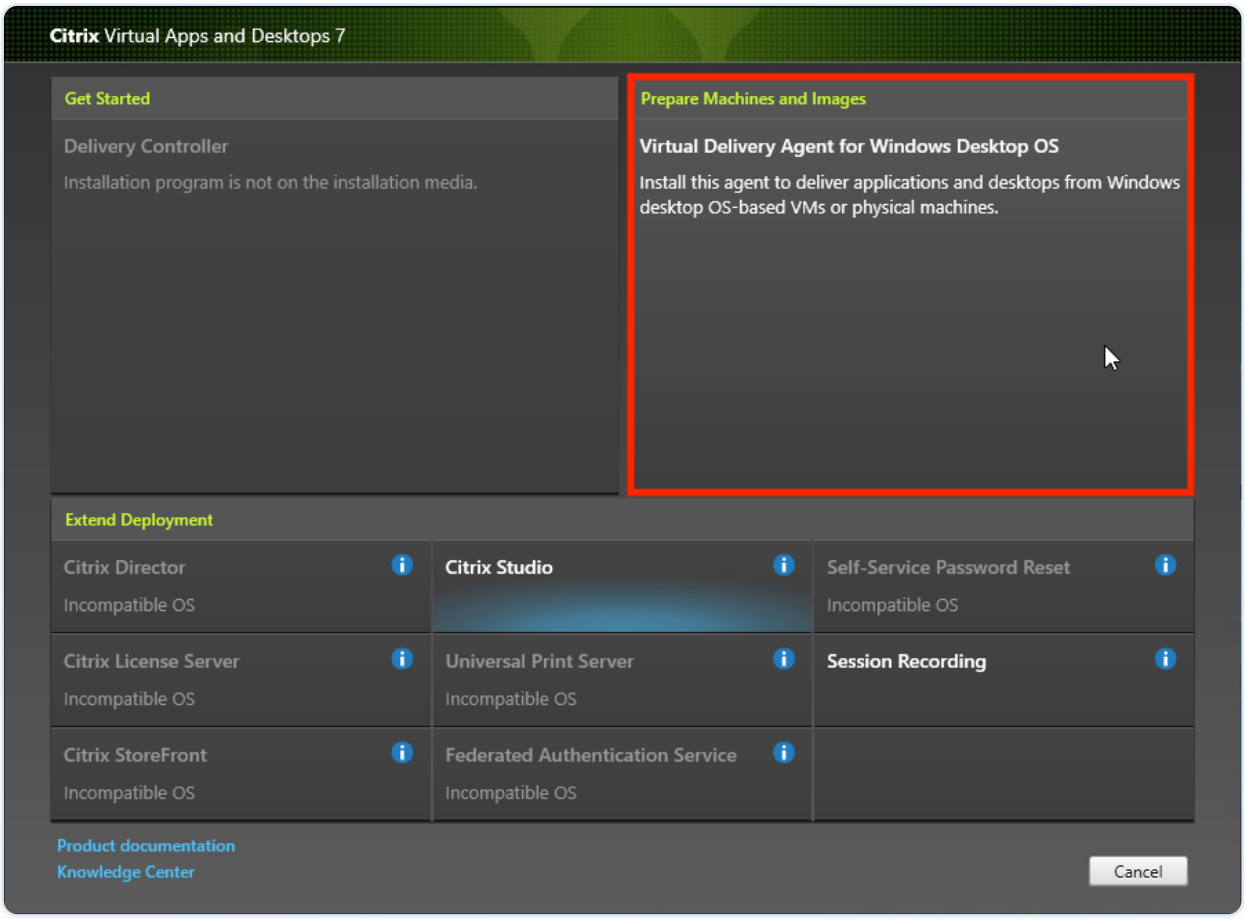
この新機能を使用できるように、Citrix Virtual Apps and Desktops環境が利用可能であることを確認してください。セットアップの詳細については、「Citrix Virtual Apps and Desktopsのインストールと構成」を参照してください。

ステップ 2: マスターイメージを準備する

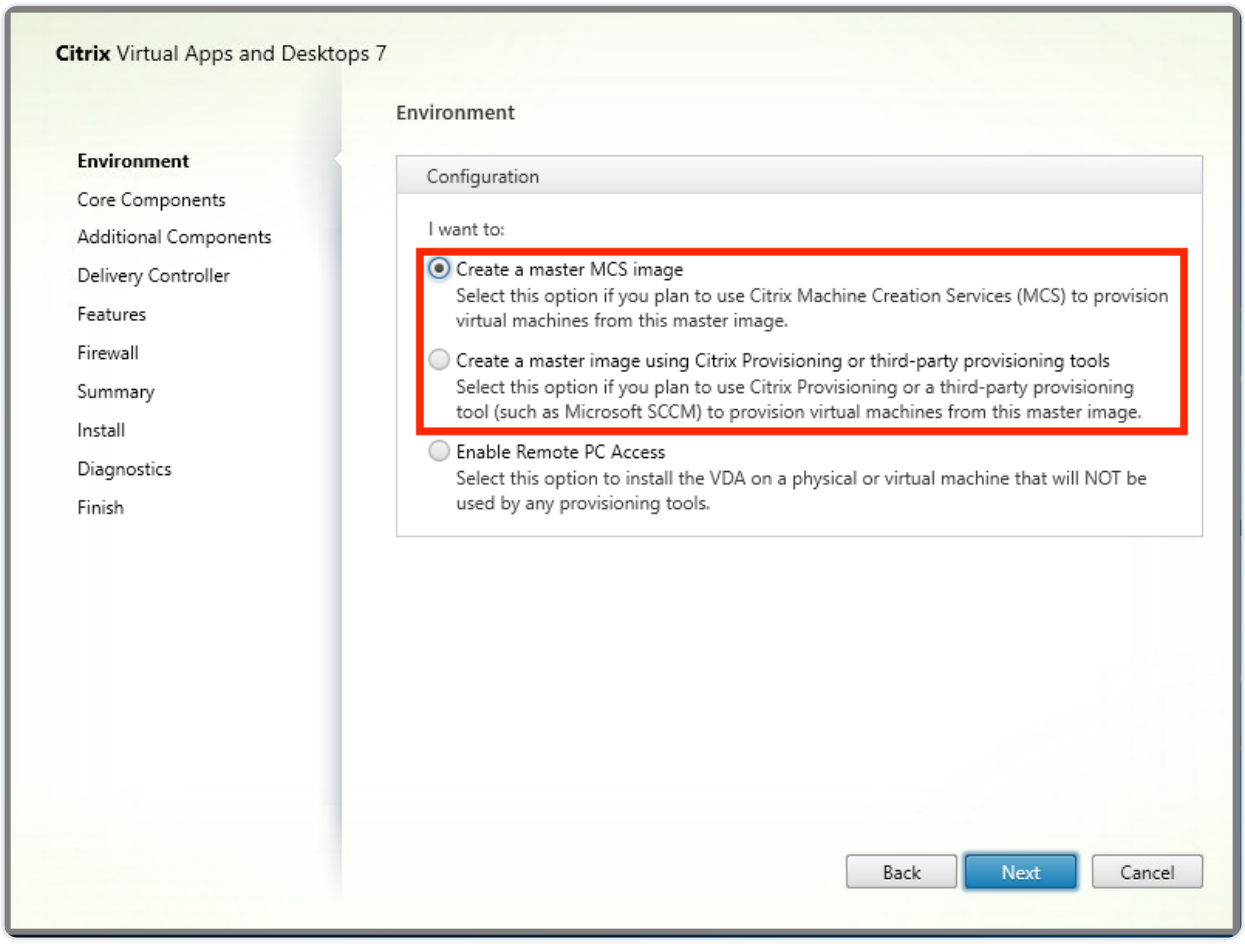
マスターイメージを準備するには:

1. マスターイメージを見つけます。組織のエンタープライズアプリケーションと、ユーザーが一般的に役立つその他のアプリをインストールします。
2. Server VDI を展開する場合は、Server VDI の記事の手順に従ってください。オプションコンポーネントである **User personalization layer** を必ず含めてください。詳細については、VDA のインストール用コマンドラインオプション を参照してください。
3. Windows 10 を使用している場合は、Virtual Delivery Agent (VDA) 1912 以降をインストールします。古いバージョンの VDA がすでにインストールされている場合は、まず古いバージョンをアンインストールします。新しいバージョンをインストールする際は、オプションコンポーネントである **Citrix User Personalization Layer** を次のように選択してインストールしてください。

    a. **Virtual Delivery Agent for Windows Desktop OS**タイルをクリックします:

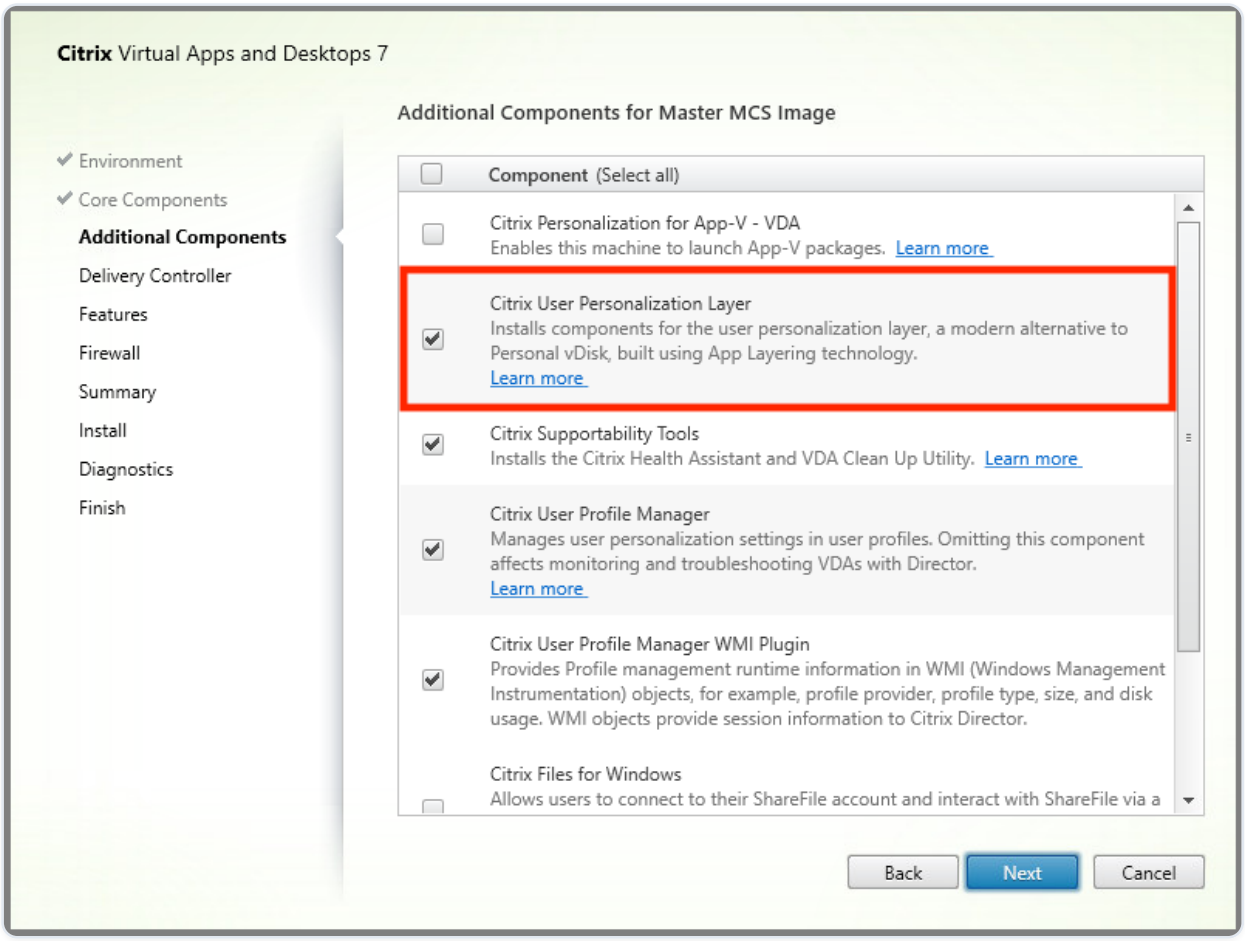


a. **環境: マスター MCS イメージを作成** または **Citrix Provisioning** またはサードパーティの**プロビジョニングツールを使用してマスターイメージを作成** のいずれかを選択します。



a. **コアコンポーネント:** 「次へ」をクリックします。

b. **追加コンポーネント: Citrix User Personalization Layer** をオンにします。



a. 残りのインストール画面を進み、必要に応じて VDA を構成し、**インストール** をクリックします。インストール中にイメージが 1 回以上再起動します。

4. **Windows の更新** は無効のままにします。ユーザーパーソナライゼーションレイヤーのインストーラーは、イメージ上の Windows 更新を無効にします。更新は無効のままにしてください。

イメージをWeb Studioにアップロードする準備ができました。

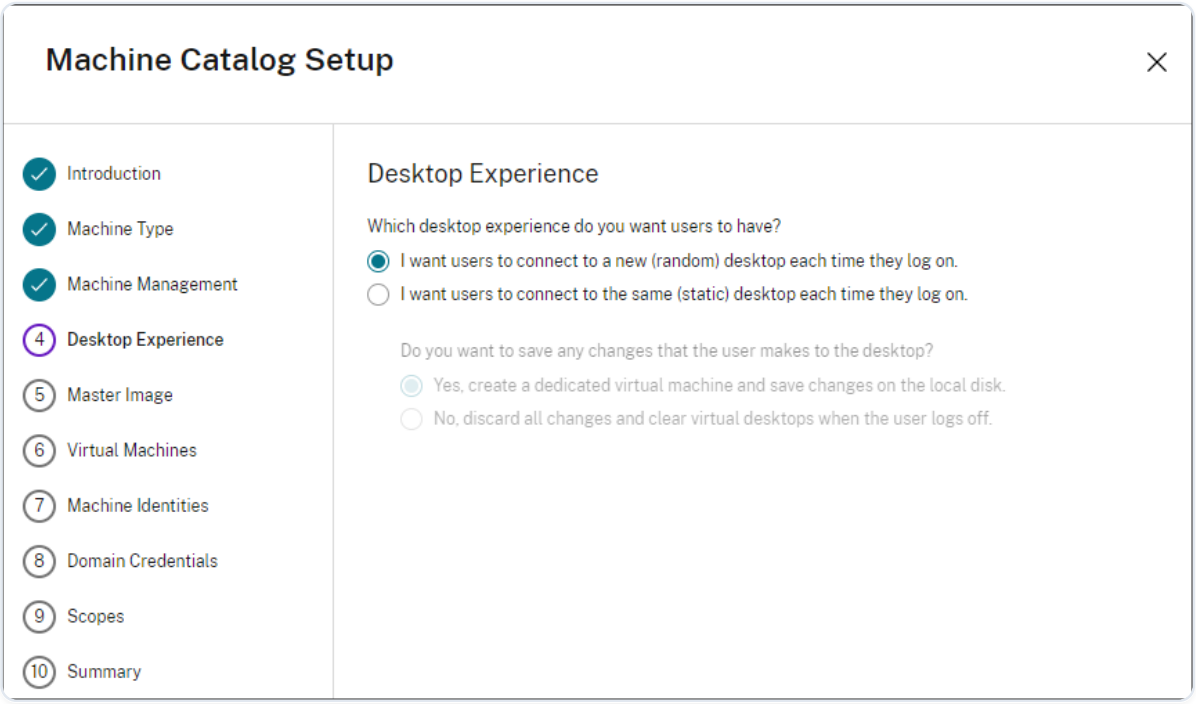
> **注:**
>
> ユーザーパーソナライゼーションレイヤー (UPL) を単にアップグレードしたい場合は、新しいバージョンのUPLとスタンドアロンパッケージを使用してアップグレードできます。VDA をアップグレードする必要はありません。

ステップ 3: マシンカタログを作成する

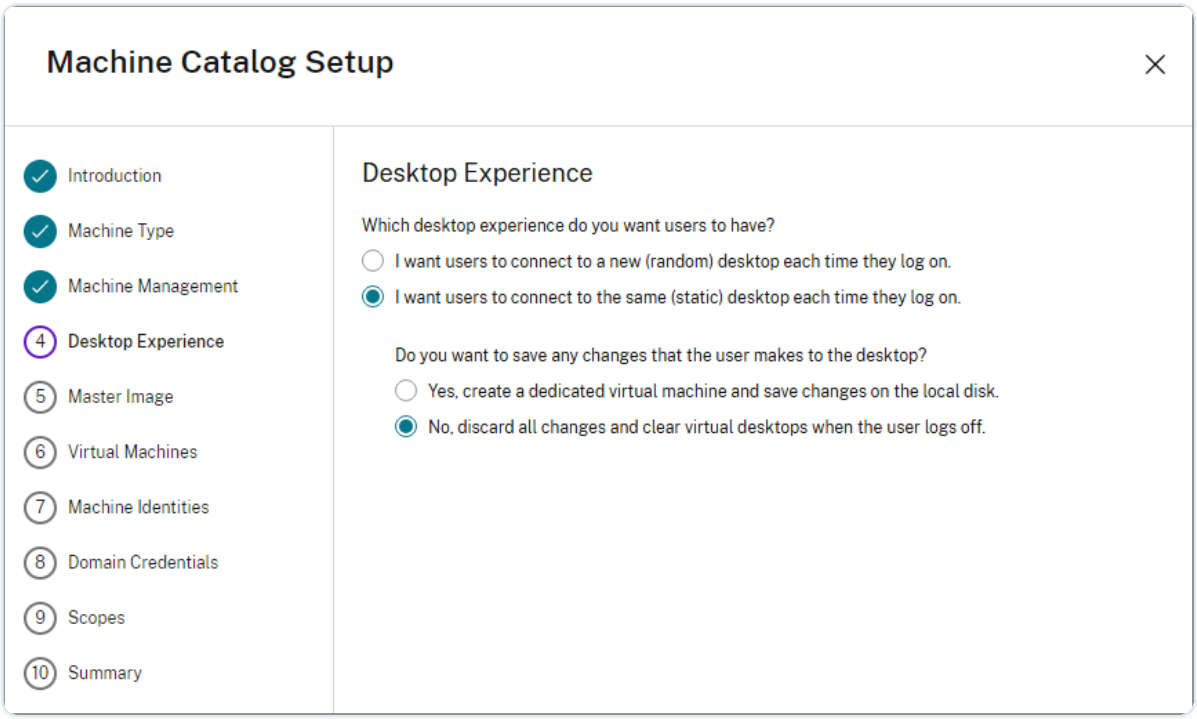
Web Studioで、マシンカタログを作成する手順に従います。カタログ作成時に以下のオプションを使用します:

1. **オペレーティングシステム**を選択し、**シングルセッションOS**に設定します。
2. **マシン管理**を選択し、**電源管理されているマシン**に設定します。たとえば、仮想マシンやブレードPCなどです。
3. **デスクトップエクスペリエンス**を選択し、以下の例のように**プールされたランダム**または**プールされた静的**カタログタイプに設定します:

   - **プールされたランダム:**



   - **プールされた静的:** プールされた静的を選択した場合、次のスクリーンショットに示すように、ユーザーがログオフしたときにすべての変更を破棄し、仮想デスクトップをクリアするようにデスクトップを構成します:



注:

ユーザーパーソナライゼーションレイヤーは、Citrix Personal vDiskを使用するように構成されたプールされた静的カタログ、または専用仮想マシンとして割り当てられたものをサポートしていません。

4. MCSを使用している場合は、**イメージ**と、前のセクションで作成したイメージのスナップショットを選択します。
5. 環境に合わせて、残りのカタログプロパティを必要に応じて構成します。

ステップ 4: デリバリーグループを作成する

作成したマシンカタログのマシンを含め、**デリバリーグループ**を作成および構成します。詳細については、デリバリーグループの作成を参照してください。

ステップ 5: デリバリーグループのカスタムポリシーを作成する

Virtual Delivery Agent内でユーザーレイヤーのマウントを有効にするには、構成パラメータを使用して以下を指定します。

- ネットワーク上のどこでユーザーレイヤーにアクセスするか。
- ユーザーレイヤーディスクの最大許容サイズ。

Web Studioでパラメータをカスタムポリシーとして定義し、デリバリーグループに割り当てます。

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。

   Studioでポリシーを選択(/en-us/citrix-virtual-apps-desktops/2407/media/upl-studio-select-policies.png)

2. アクションバーで**ポリシーの作成**を選択します。ポリシーの作成ウィンドウが表示されます。
3. 検索フィールドに`user layer`と入力します。利用可能なポリシーのリストに次の3つのポリシーが表示されます。

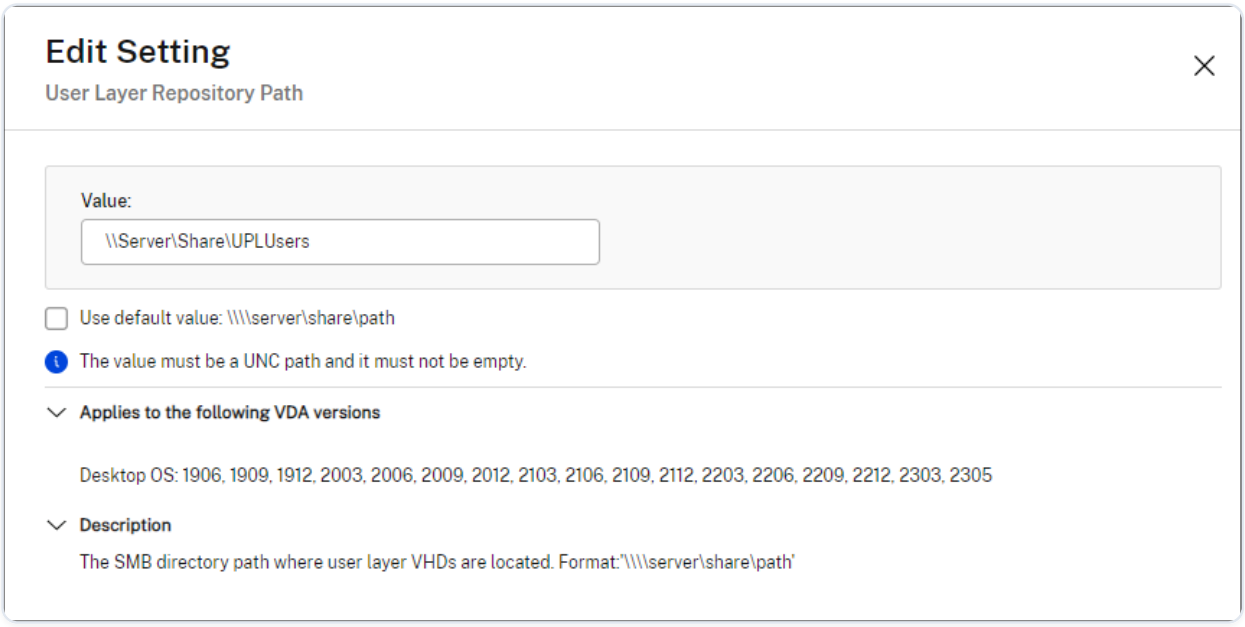
   - ユーザーレイヤーの除外
   - ユーザーレイヤーリポジトリパス
   - ユーザーレイヤーサイズ (GB)

   > **注:**
   >
   > サイズを増やすと、新しいユーザーレイヤーと既存のユーザーレイヤーが拡張されます。サイズを減らすと、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

   ユーザーレイヤーポリシーの選択(/en-us/citrix-virtual-apps-desktops/2407/media/user-layer-policies.png)

4. 「**User Layer Repository Path**」の横にあるチェックボックスをオンにして、「**Edit**」をクリックします。「**Edit Setting**」ウィンドウが表示されます。
5. 「**Value**」フィールドにパスを入力し、「**Save**」をクリックします。

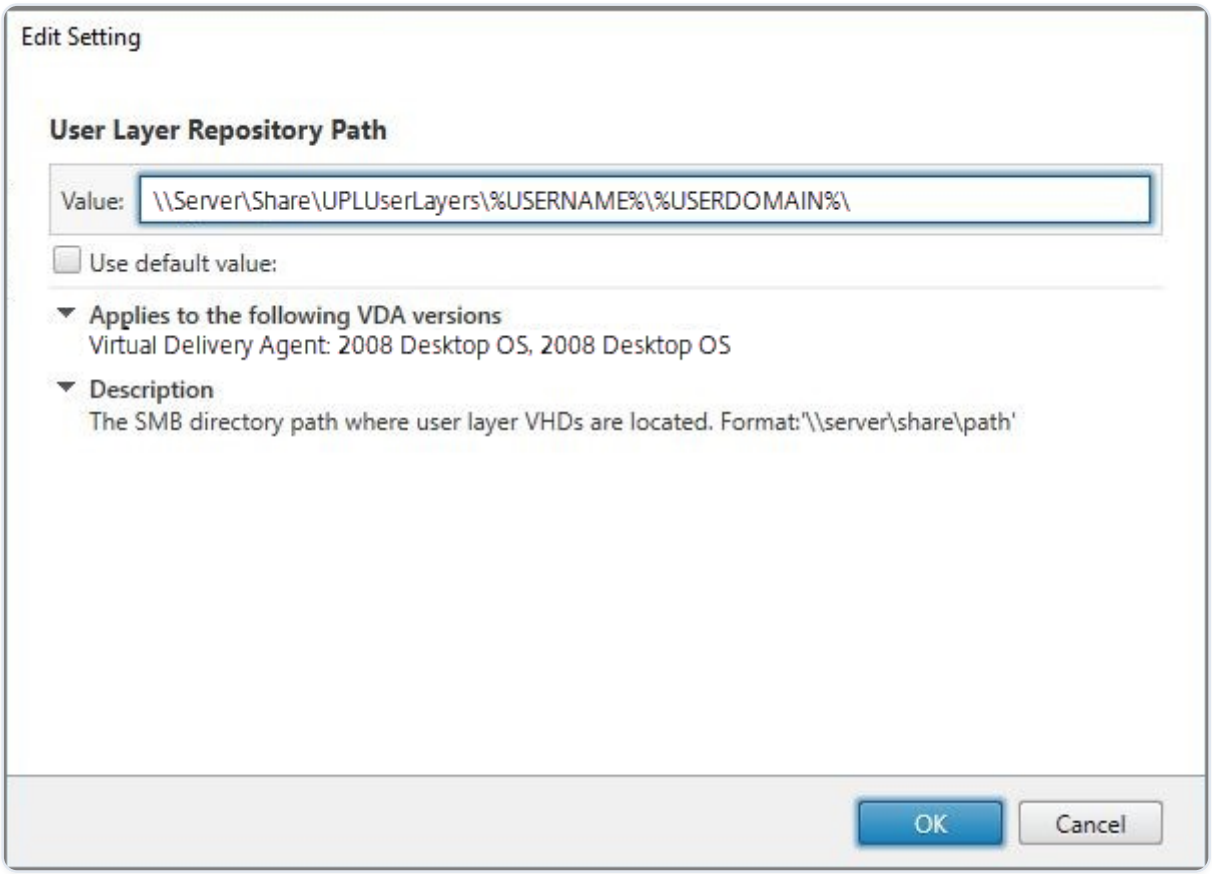
   - **パス形式:** `\\server-name-or-address\share-name\folder`
   - **パスの例:** `\\Server\Share\UPLUsers`
   - **結果のパスの例: CoolCompanyDomainのAlex**という名前のユーザーの場合、パスは次のとおりです。`\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`



`%USERNAME%`と`%USERDOMAIN%`変数、マシン環境変数、およびActive Directory (AD)属性を使用してパスをカスタマイズできます。これらの変数を展開すると、明示的なパスになります。

環境変数の例:

- **パス形式:** `\\Server-name-or-address\share-name\folder-with-environment-variables`
- **パスの例:** `\\Server\Share\UPLUserLayers\%USERNAME%\%USERDOMAIN%`
- **結果のパスの例: CoolCompanyDomainのAlex**という名前のユーザーの場合、パスは次のようになります。`\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`



カスタムAD属性の例:

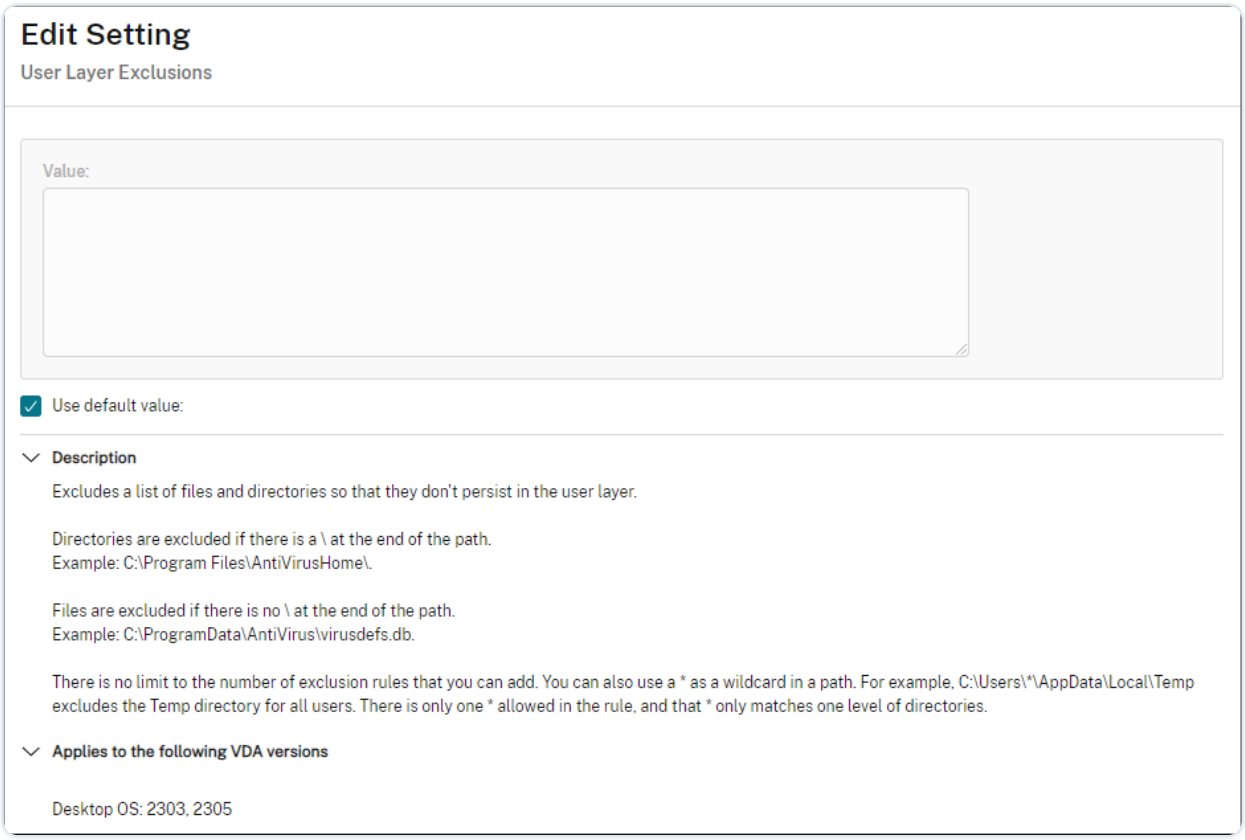
- パス形式: `\\Server-name-or-address\share-name\AD-attribute`
- パスの例: `\\Server\share#sAMAccountName#`
- 結果のパスの例: `\\Server\share\JohnSmith` (現在のユーザーに対して #sAMAccountName# が JohnSmith に解決される場合)

6. オプション: **ユーザーレイヤーサイズ (GB)** の横にあるチェックボックスをオンにし、**編集** をクリックします。

   ユーザーレイヤーリポジトリパス(/en-us/citrix-virtual-apps-desktops/2407/media/upl-select-user-layer-size.png)

   設定の編集ウィンドウが表示されます。

7. オプション: デフォルト値の **10 GB** を、各ユーザーレイヤーが拡張できる最大サイズに変更します。**Save** をクリックします。
8. オプション: **ユーザーレイヤーの除外** の横にあるチェックボックスをオンにし、**編集** をクリックします。



9. オプション: 除外するファイルとフォルダを指定し、**保存** をクリックします。詳細については、Citrix App Layering のドキュメント を参照してください。
10. 割り当てるユーザーとマシンを設定するには、**次へ** をクリックします。この画像で強調表示されている **デリバリーグループの割り当て** リンクをクリックします。

    ユーザーレイヤーリポジトリパス(/en-us/citrix-virtual-apps-desktops/2407/media/upl-delivery-group-assign.png)
11. **Delivery Group** メニューで、前のセクションで作成したデリバリーグループを選択します。**OK** をクリックします。

    デリバリーグループを選択(/en-us/citrix-virtual-apps-desktops/2407/media/upl-delivery-group-select.png)
12. ポリシーの名前を入力します。ポリシーを有効にするには、チェックボックスをオンにして、**Finish** をクリックします。

    ユーザーレイヤーポリシー名(/en-us/citrix-virtual-apps-desktops/2407/media/upl-name-policy.png)

ユーザーレイヤーフォルダのセキュリティ設定を構成する

ドメイン管理者として、ユーザーレイヤーのストレージ場所を複数指定できます。各ストレージ場所 (デフォルトの場所を含む) ごとに `\Users` サブフォルダーを作成します。次の設定を使用して、各場所を保護します。

設定名	値	適用先	
作成者/所有者	変更	サブフォルダーとファイルのみ	
所有者の権限	変更	サブフォルダーとファイルのみ	
ユーザーまたはグループ	フォルダーの作成/データの追加; フォルダーの横断/ファイルの実行; フォルダーの一覧表示/データの読み取り; 属性の読み取り	選択したフォルダーのみ	
システム	フルコントロール	選択されたフォルダー、サブフォルダー、およびファイル	
ドメイン管理者、および選択された管理者グループ	フルコントロール	選択されたフォルダー、サブフォルダー、およびファイル	

ユーザーレイヤーメッセージ

ユーザーがユーザーレイヤーにアクセスできない場合、次のいずれかの通知メッセージが表示されます。

- **ユーザーレイヤーが使用中です**

  `We were unable to attach your user layer because it is in use. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **ユーザーレイヤーが利用できません**

`We were unable to attach your user layer. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **ユーザーサインアウト後にシステムがリセットされませんでした**

  `This system was not shut down properly. Please log off immediately and contact your system administrator.`.

トラブルシューティング時に使用するログファイル

ログファイル ulayersvc.log には、変更がログに記録されるユーザーパーソナライゼーションレイヤーソフトウェアの出力が含まれています。

```
C:\ProgramData\Unidesk\Logs\ulayersvc.log
```

ユーザーレイヤー/UPL領域の再利用

ユーザーがログオフするたびにVHDXファイルを自動的に圧縮するには、**ユーザーレイヤー/UPL領域の再利用**を使用できます。 詳細については、「ユーザーレイヤー/UPL領域の再利用」を参照してください。

制限事項

ユーザーパーソナライゼーションレイヤー機能をインストールして使用する際は、以下の制限事項に注意してください。

- App Layering内のレイヤーにユーザーパーソナライゼーションレイヤーソフトウェアを展開することは*避けてください*。ユーザーパーソナライゼーションレイヤーはCitrix Virtual Apps and Desktopsに展開するか、App Layeringイメージテンプレートでユーザーレイヤーを有効にするかのいずれかであり、両方ではありません。どちらのプロセスでも、必要なユーザーレイヤーが生成されます。
- 永続的なマシンカタログでユーザーパーソナライゼーションレイヤー機能を構成することは*避けてください*。
- セッションホストを使用することは*避けてください*。
- 新しいOSインストール（同じバージョンのWindows 10であっても）を実行しているイメージでマシンカタログを更新することは*避けてください*。ベストプラクティスは、マシンカタログの作成時に使用した同じマスターイメージ内でOSに更新を適用することです。

- 起動時ドライバーやその他の早期起動パーソナライゼーションを使用することは*避けて*ください。
- PvDデータをユーザーパーソナライゼーションレイヤー機能に移行することは*避けて*ください。
- 既存のユーザーレイヤーを完全なApp Layering製品からユーザーパーソナライゼーションレイヤー機能に移行することは*避けて*ください。
- 異なるマスターOSイメージを使用して作成されたユーザーレイヤーにアクセスするために、ユーザーレイヤーSMBパスを変更することは*避けて*ください。
- ユーザーがセッションからログアウトし、再度ログインすると、新しいセッションはプール内の別のマシンで実行されます。VDI環境では、Microsoft Software Centerは最初のマシンではアプリケーションを**インストール済み**と表示しますが、2番目のマシンでは**利用不可**と表示します。

  アプリケーションの実際の状態を確認するには、ユーザーにSoftware Centerでアプリケーションを選択し、**インストール**をクリックするように指示します。すると、SCCMが状態を実際の値に更新します。
- ユーザーパーソナライゼーションレイヤー機能が有効になっているVDA内で、Software Centerが起動直後に停止することがあります。この問題を回避するには、「XenDesktop VDI環境でのSCCMの実装」に関するMicrosoftの推奨事項に従ってください。また、Software Centerを起動する前に、`ccmexec`サービスが実行されていることを確認してください。
- グループポリシー（コンピューター設定）では、ユーザーレイヤー設定がマスターイメージに適用される設定を上書きします。そのため、GPOを使用してコンピューター設定で行った変更が、次のセッションログイン時にユーザーに常に反映されるとは限りません。

  この問題を回避するには、次のコマンドを発行するユーザーログオンスクリプトを作成します。

  ```
  gpupdate /force
  ```

  たとえば、あるお客様はユーザーがログインするたびに次のコマンドを実行するように設定しました。

  ```
  gpudate /Target:Computer /force
  ```

  最良の結果を得るには、ユーザーがログインした後で、コンピューター設定への変更をユーザーレイヤーに直接適用します。

- ドメインユーザーアカウントは、マスターイメージに最後にログインしたユーザーであってはなりません。そうしないと、そのイメージからプロビジョニングされたマシンに問題が発生する可能性があります。
- Azure で実行されている Windows の根本的な問題により、純粋な Azure AD 環境で UPL が有効になっている場合、カスタム証明書は保持されません。Microsoft が将来の機能強化でこの問題を修正した場合、この記事を更新します。

コンポーネントの削除

コンポーネントを削除するには、Citrix® は、Windows のプログラムの削除または変更機能を使用することを推奨します。あるいは、コマンドラインまたはインストールメディア上のスクリプトを使用してコンポーネントを削除することもできます。

コンポーネントを削除しても、前提条件は削除されず、ファイアウォール設定も変更されません。たとえば、デリバリーコントローラー™ を削除しても、SQL Server ソフトウェアとデータベースは削除されません。

Web Interfaceを含む以前の展開からControllerをアップグレードした場合は、Web Interfaceコンポーネントを個別に削除する必要があります。インストーラーを使用してWeb Interfaceを削除することはできません。

以下に記載されていない機能の削除については、その機能のドキュメントを参照してください。

準備

Controllerを削除する前に、サイトから削除してください。詳しくは、「Controllerを削除する」を参照してください。

Studio と Director を削除する前に、それらを閉じてください。

Windowsのプログラムの削除または変更機能を使用してコンポーネントを削除する

Windowsのプログラムの削除または変更機能から：

- Controller、Studio、Director、License Server、またはStoreFrontを削除するには、**Citrix Virtual Apps *version*** または **Citrix Virtual Apps and Desktops™ *version*** を右クリックして、**アンインストール**を選択します。インストーラーが起動します。削除するコンポーネントを選択します。

あるいは、**Citrix StoreFront** を右クリックし、**アンインストール**を選択して、StoreFront™ を削除することもできます。

- VDA を削除するには、**Citrix Virtual Delivery Agent *version*** を右クリックし、**アンインストール**を選択します。インストーラーが起動し、削除するコンポーネントを選択できます。削除後、デフォルトでマシンは自動的に再起動します。
- Universal Print Server を削除するには、**Citrix Universal™ Print Server** を右クリックし、**アンインストール**を選択します。

コマンドラインを使用してコアコンポーネントを削除する

`\x64\XenDesktop Setup` ディレクトリから、`XenDesktopServerSetup.exe` コマンドを実行します。

- 1つ以上のコンポーネントを削除するには、`/remove` および `/components` オプションを指定します。
- すべてのコンポーネントを削除するには、`/removeall` オプションを指定します。

コマンドとパラメーターの詳細については、コマンドラインを使用したインストールを参照してください。

例えば、次のコマンドはWeb Studioを削除します。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components webstudio
```

コマンドラインを使用してVDAを削除する

`\x64\XenDesktop Setup` ディレクトリから、`XenDesktopVdaSetup.exe` コマンドを実行します。

- 1つ以上のコンポーネントを削除するには、`/remove` および `/components` オプションを使用します。たとえば、VDAとCitrix Workspaceアプリを削除するには、`/remove /components vda,plugin` を使用します。
- `/removeall` オプションはVDAのみを削除します。Citrix Workspaceアプリは削除しません。

コマンドとパラメーターの詳細については、コマンドラインを使用したインストールを参照してください。

既定では、削除後にマシンは自動的に再起動します。

Active Directoryでスクリプトを使用してVDAを削除するには、スクリプトを使用したVDAのインストールまたは削除を参照してください。

アップグレードと移行

はじめに

アップグレードすると、新しいマシンやサイトをセットアップすることなく、展開がCitrix Virtual Apps and Desktops™ 7 **Current Release (CR)** に変更されます。これはインプレースアップグレードとして知られています。

アップグレードすると、利用資格のある最新の機能やテクノロジーにアクセスできるようになります。アップグレードには、以前のバージョンからの修正、明確化、機能強化も含まれる場合があります。

アップグレードの概要

1. アップグレードを開始する前に、展開のアップグレード の記事を確認してください。これは、アップグレードの準備と実装方法を学ぶための主要な情報源です。
2. 現在のCustomer Success Servicesの有効期限が切れていないことを確認してください。詳細については、Customer Success Servicesの更新ライセンス の記事を参照してください。
3. 準備ガイドを完了します。
4. インストーラーを実行してコアコンポーネントをアップグレードします。
5. システムデータベースとサイトをアップグレードします。
6. イメージ上のVDA (またはマシンに直接) をアップグレードします。
7. その他のコンポーネントをアップグレードします。

各準備およびアップグレードの手順は、展開のアップグレード で詳しく説明されています。

アップグレード可能なバージョン

Citrix Virtual Apps and Desktops 2407 には、以下からアップグレードできます。

- Virtual Apps and Desktops 2203 LTSR（CUの有無にかかわらず、CU5までを含む）
- Virtual Apps and Desktops 1912 LTSR（CUの有無にかかわらず、CU9までを含む）
- Citrix Virtual Apps and Desktopsの現在サポートされているCRバージョン

アップグレード可能な Citrix Virtual Apps and Desktops (および XenApp および XenDesktop) のバージョンの一覧については、(/ja-jp/upgrade.html) の も参照してください。

注:

- アップグレードプロセスを開始する前に、Citrix®は、お客様が管理された環境でアップグレードをテストし、特定の要件を満たしていることを確認することを推奨します。さらに、スムーズな移行を確実にするために、非推奨リストや既知の問題を含むすべての関連製品ドキュメントを確認することをお勧めします。このアプローチは、本番システムへの潜在的な中断を軽減し、全体的なアップグレードエクスペリエンスを向上させるのに役立ちます。
- Citrix Virtual Apps and Desktops 1912 LTSRは、まもなくサポート終了フェーズに達します。 サポートされているバージョンの一覧については、Product Matrixを参照してください。

よくある質問

このセクションでは、Citrix Virtual Apps and Desktopsのアップグレードに関するよくある質問に回答します。

- **Virtual Apps and Desktops環境をアップグレードする正しい順序は何ですか？**

  推奨されるアップグレードシーケンスの図と説明については、アップグレードシーケンスおよびアップグレード手順を参照してください。

- **私のサイトには複数のDelivery Controller（異なるゾーンに）があります。一部だけをアップグレードした場合、どうなりますか？同じメンテナンスウィンドウ中にサイト内のすべてのControllerをアップグレードする必要がありますか？**

  各 Controller 上のさまざまなサービスが相互に通信するため、すべての Delivery Controller を同じメンテナンス期間中にアップグレードすることがベストプラクティスです。異なるバージョンを維持すると、問題が発生する可能性があります。メンテナンス期間中には、Controller の半分をアップグレードし、サイトをアップグレードしてから、残りの Controller をアップグレードすることをお勧めします。詳細については、アップグレード手順 を参照してください。

- **最新バージョンに直接アップグレードできますか、それとも段階的なアップグレードを行う必要がありますか？**

アップグレード先のバージョンの**新機能**の記事で明示的に記載されていない限り、ほとんどの場合、最新バージョンにアップグレードし、中間リリースをスキップできます。

- **お客様はLong Term Service Release (LTSR) 環境からCurrent Releaseにアップグレードできますか？**

  はい。お客様は長期間にわたってLong Term Service Releaseにとどまる必要はありません。お客様は、ビジネス要件と機能に基づいて、LTSR環境をCurrent Releaseに移行できます。

- **コンポーネントの混在バージョンは許可されていますか？**

  各サイト内で、Citrixはすべてのコンポーネントを同じバージョンにアップグレードすることを推奨しています。一部のコンポーネントで以前のバージョンを使用することはできますが、最新バージョンのすべての機能が利用できない場合があります。詳細については、混在環境に関する考慮事項を参照してください。

- **Current Releaseはどのくらいの頻度でアップグレードする必要がありますか？**

  Current Releaseは、リリース日から6か月後にEnd of Maintenance (EOM) に達します。Citrixは、お客様が最新のCurrent Releaseを採用することを推奨しています。Current Releaseは、リリース日から18か月後にEnd of Life (EOL) に達します。

- **推奨されるのは、LTSRへのアップグレードですか、それともCRへのアップグレードですか？**

  Current Release (CR) は、最新かつ最も革新的なアプリ、デスクトップ、およびサーバー仮想化の機能を提供します。これにより、最先端のテクノロジーを維持し、競合他社の一歩先を行くことができます。

  Long Term Service Release (LTSR) は、長期間同じベースバージョンを維持することを好む大規模なエンタープライズ本番環境に最適です。

```
For details, see [Servicing Options]( https://www.citrix.com/support/
citrix-customer-success-services/citrix-virtual-apps-and-desktops-
servicing-options.md).
```

- **ライセンスをアップグレードする必要がありますか？**

  現在のライセンスの有効期限が切れておらず、アップグレードするリリースに対して有効であることを確認してください。CTX111618を参照してください。更新については、Customer Success Servicesの更新ライセンスを参照してください。

- **アップグレードにはどのくらい時間がかかりますか？**

展開のアップグレードにかかる時間は、インフラストラクチャとネットワークによって異なります。そのため、正確な時間をお伝えすることはできません。

- **ベストプラクティスは何ですか？**

  準備ガイダンスを理解し、それに従ってください。

- **サポートされているオペレーティングシステムは何ですか？**

  アップグレード先のバージョンのシステム要件の記事に、サポートされているOSが記載されています。

  現在の展開でサポートされなくなったオペレーティングシステムを使用している場合は、以前のオペレーティングシステムを参照してください。

- **サポートされているVMware vSphere (vCenter + ESXi) のバージョンは何ですか？**

  CTX131239には、サポートされているホストとバージョン、および既知の問題へのリンクが記載されています。

- **私のバージョンはいつEOLになりますか？**

  製品マトリックスを確認してください。

- **最新リリースにおける既知の問題は何ですか？**

  - シトリックス バーチャル アプリケーションズ アンド デスクトップ
  - StoreFront
  - シトリックス プロビジョニング
  - シトリックス ライセンス サーバー
  - Windows 用 Citrix Workspace アプリ

詳細情報

Long Term Service Release (LTSR) の展開更新では、累積更新プログラム (CU) が使用されます。CU は LTSR のベースラインコンポーネントを更新し、各 CU には独自のメタインストーラーが含まれています。

各 CU には専用のドキュメントがあります。例えば、2203 LTSR の場合、最新の CU については、その LTSR の **新機能** ページにあるリンクを確認してください。各 CU ページには、サポートされているバージョン情報、手順、および CU ダウンロードパッケージへのリンクが含まれています。

移行

クラウドへの移行

Citrix Virtual Apps and Desktopsの自動構成ツールを使用して、オンプレミス展開をクラウドに移行できます。詳しくは、「クラウドへの移行」を参照してください。

レガシー移行

移行とは、以前の展開から新しいバージョンにデータを移動することです。このプロセスには、新しいコンポーネントのインストールと新しいサイトの作成、古いファームからのデータのエクスポート、そして新しいサイトへのデータのインポートが含まれます。

XenApp および XenDesktop のバージョン、または以前の Citrix Virtual Apps and Desktops のバージョンを移行するためのサポートされているツールやスクリプトはありません。この製品ドキュメントに記載されている Citrix Virtual Apps and Desktops のバージョンでは、*アップグレード*がサポートされています。

以前の XenApp 6.x の移行コンテンツについては、以下を参照してください。スクリプトも記事もサポートされておらず、メンテナンスもされていません。

- XenApp 6.x バージョン用のオープンソース移行スクリプトは `<https://github.com/citrix/xa65migrationtool>` で入手できます。Citrix はこれらの移行スクリプトをサポートまたは保守していません
- 7.x の変更点
- XenApp 6.5 ワーカーを新しい VDA にアップグレードする
- XenApp 6.x を移行する

デプロイメントのアップグレード

はじめに

新しいマシンやサイトを最初にセットアップすることなく、特定の展開を新しいバージョンにアップグレードできます。これはインプレースアップグレードと呼ばれます。

アップグレードできるCitrix Virtual Apps and Desktopsのバージョンについては、(/ja-jp/citrix-virtual-apps-desktops/2407/upgrade-migrate.html#versions-you-can-upgrade)を参照してください。

Citrix Virtual Apps and Desktopsのいずれかのリリースにアップグレードする前に、現在のCustomer Success Servicesの有効期限が切れていないことを確認してください。詳細については、(/ja-jp/licensing/current-release/customer-success-services.html#customer-success-services-renewal-licenses)の記事を参照してください。

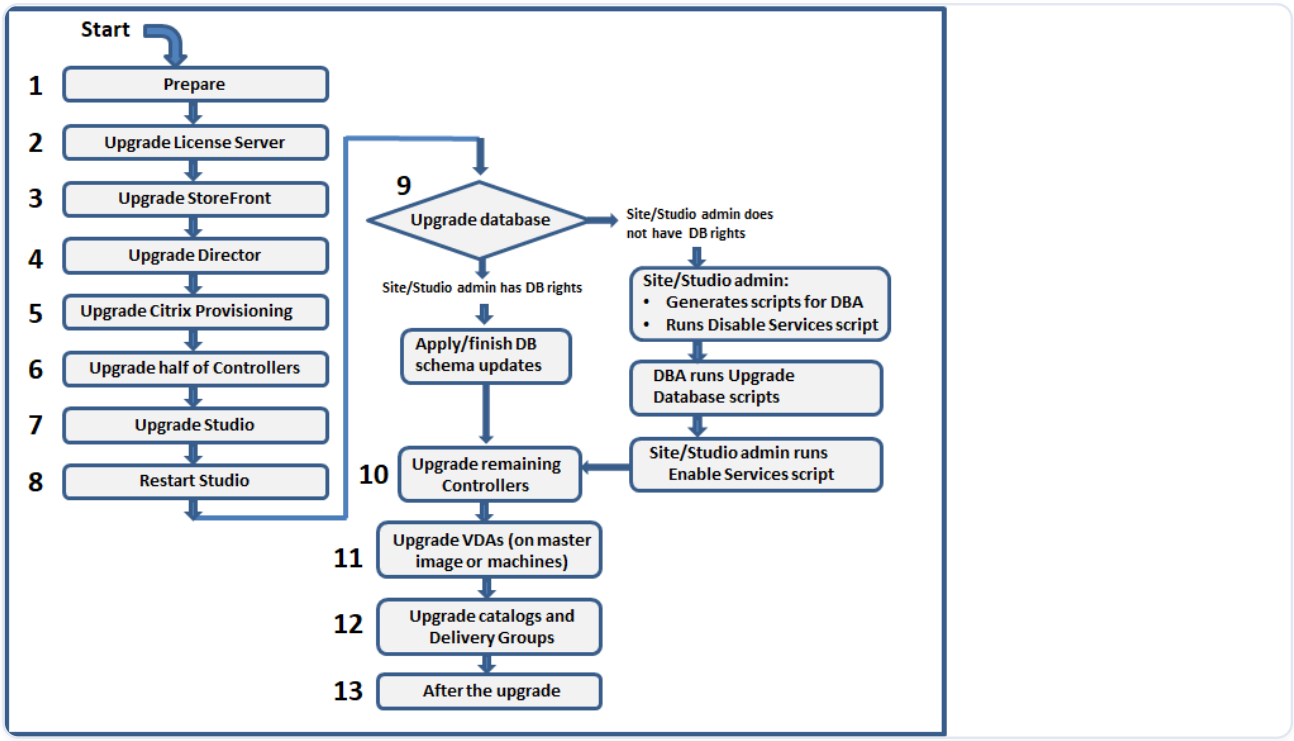
アップグレードを開始するには、新しいバージョンのインストーラーを実行して、以前にインストールされたコアコンポーネント、VDA、およびその他の特定のコンポーネントをアップグレードします。その後、データベースとサイトをアップグレードします。

新しいバージョンが提供されている場合、フルプロダクトインストーラー（およびスタンドアロンVDAインストーラー）でインストールできるすべてのコンポーネントをアップグレードできます。フルプロダクトインストーラーでインストールされないその他のコンポーネント（Citrix Provisioning™やProfile Managementなど）については、そのコンポーネントのドキュメントを参照してください。ホストのアップグレードについては、適切なドキュメントを参照してください。

アップグレードを開始する前に、この記事のすべての情報を確認してください。

アップグレードシーケンス

次の図は、アップグレードシーケンスのステップを示しています。Upgrade procedure には、図の各ステップの詳細が含まれています。



注:

障害を回避するため、新しいマシンカタログの作成、マシンカタログの削除、デリバリーグループ内のマシンの更新など、プロビジョニングおよびデリバリーグループ関連のタスクを実行する前に、すべてのDelivery Controllerとデータベースをアップグレードする必要があります。

ハイブリッド権限ライセンス

ハイブリッド権限ライセンスは、顧客が永続ライセンスからクラウドサービスサブスクリプションに移行またはアップグレードする際に、クラウドサービスサブスクリプションに加えて提供される期間ベースのサブスクリプションライセンスです。DaaSサブスクリプションでハイブリッド権限アドオンを購入することもできます。

SaaS属性を持つハイブリッドライツライセンスをお持ちの場合、Citrix Virtual Apps and Desktops™ LTSR 2203以降にアップグレードすると、Citrix Virtual Apps and Desktops LTSR 1912では利用できなかった機能にアクセスできるようになります。これらの機能には、Microsoft Azure、AWS EC2、Google Cloudなどのパブリッククラウドでのワークロードのプロビジョニングとホスティングが含まれます。新しいライセンスファイルを展開する前に、ライセンスサーバーを最新バージョンに更新してください。

SaaS属性のないハイブリッドライツライセンスにアクセスできる場合は、以下の手順に従ってSaaS属性付きの新しいハイブリッドライツライセンスにアクセスしてください。

注：

- 新しいライセンスコードが記載されたメールが届きます。詳細については、「ライセンスアクセスコードの使用」を参照してください。
- 既存のライセンスは取り消されます。取り消されたライセンスは、ライセンスサーバーから削除し、新しいライセンスをインストールする必要があります。詳細については、「ライセンスファイルの削除」を参照してください。

1. citrix.comのライセンス管理ポータルにアクセスし、クラウドプロビジョニング権限が有効になっている（SaaS属性付きの）新しいハイブリッドライツライセンスファイルをダウンロードします。詳細については、「ライセンスのダウンロード」を参照してください。次の画像は、インクリメントセクションにSaaS属性を持つハイブリッドライツライセンスファイルを示しています。

```
INCREMENT XDT_PLT_CCS CITRIX 2022.1201 01-dec-2022 5 \
    VENDOR_STRING=;LT=RetailS;GP=720;PSL=10;CL=VDS,VDA,VDE,VDP,SaaS:SA=0;ODP=0;NUDURMIN=2880;NUDURMAX=525600;AP=ADMIN/INT/14
    OVERDRAFT=1 DUP_GROUP=V ISSUED=18-dec-2005 NOTICE="Citrix \
    Systems Inc." SN=RetailSSaaS SIGN="..."
```

2. ハイブリッドライツライセンスファイルをライセンスサーバーにインストールします。詳細については、「ライセンスのインストール」を参照してください。
3. ライセンスのエディションまたはモデルに変更がある場合は、brokerコマンドを実行してエディションとモデルを設定し、インプレースアップグレードを開始してください。Brokerコマンドの詳細については、「Broker PowerShell SDK」セクションを参照してください。

Citrix Virtual Apps and Desktops Current ReleasesおよびLong Term Service Releasesでのパブリッククラウドサポートの詳細については、「CTX270373」を参照してください。

アップグレード手順

主要な製品コンポーネントのほとんどは、コンポーネントを含むマシンで製品インストーラーを実行することでアップグレードできます。

1台のマシンに複数のコンポーネント（例：Studioとライセンスサーバー）が含まれている場合、製品メディアに新しいバージョンのソフトウェアが含まれていれば、そのマシン上のすべてのコンポーネントがアップグレードされます。

インストーラーを使用するには：

- 製品インストーラーのグラフィカルインターフェイスを実行するには、マシンにログオンし、メディアを挿入するか、新しいリリースのISOドライブをマウントします。**AutoSelect**をダブルクリックします。
- コマンドラインインターフェイスを使用するには、適切なコマンドを発行します。「コマンドラインを使用したインストール」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/install-command.html)を参照してください。

ステップ1: 準備

アップグレードを開始する前に、準備ができていることを確認してください。必要なタスクを読み、完了してください。

- 「PVD、AppDisks™、およびサポートされていないホストの削除」(#remove-pvd-appdisks-and-unsupported-hosts)
- 「PvDまたはAppDiskコンポーネントを持つVDA」(#vdas-that-have-pvd-or-appdisks-components)
- 「制限事項」(#limitations)

- 「混在環境に関する考慮事項」(#mixed-environment-considerations)
- 「以前のオペレーティングシステム」(#earlier-operating-systems)
- 「準備」(#preparation)
- 「サイトの事前テスト」(#preliminary-site-tests)
- 「SQL Serverのバージョンチェック」(#sql-server-version-check)

ステップ2: ライセンスサーバーのアップグレード

インストールにCitrix License Serverソフトウェアの新しいバージョンがある場合は、他のコンポーネントよりも先にこのコンポーネントをアップグレードしてください。

ライセンスサーバーが新しいバージョンと互換性があるかどうかをまだ「確認していない」(#preparation)場合は、他のコアコンポーネントをアップグレードする前に、ライセンスサーバーでインストーラーを実行することが不可欠です。

ステップ3: StoreFront™のアップグレード

インストールメディアに新しいバージョンのStoreFrontソフトウェアが含まれている場合は、StoreFrontサーバーを含むマシンでインストーラーを実行します。

- グラフィカルインターフェイスで、**［展開の拡張］**セクションから**［Citrix StoreFront］**を選択します。
- コマンドラインから、Citrix Virtual Apps and Desktopsインストールメディアの`x64`フォルダーにある`CitrixStoreFront-x64.exe`を実行します。

ステップ4：Directorのアップグレード

インストールメディアに新しいバージョンのDirectorソフトウェアが含まれている場合は、Directorを含むマシンでインストーラーを実行します。

ステップ5：Citrix Provisioningのアップグレード

Citrix Provisioningインストールメディアは、Citrix Virtual Apps and Desktopsインストールメディアとは別に提供されます。Citrix Provisioningサーバーおよびターゲットデバイスソフトウェアのインストールおよびアップグレード方法については、［Citrix Provisioning製品ドキュメント］(/ja-jp/provisioning)を参照してください。

ステップ6：Delivery Controllerの半分をアップグレードする

たとえば、サイトに4つのControllerがある場合、そのうち2つでインストーラーを実行します。

Controllerの半分をアクティブなままにしておくことで、ユーザーはサイトにアクセスできます。VDAは残りのControllerに登録できます。利用可能なControllerが少ないため、サイトの容量が減少する場合があります。アップグレードによって中断が発生するのは、最終的なデータベースアップグレード手順中に新しいクライアント接続を確立するごく短時間のみです。アップグレードされたControllerは、サイト全体がアップグレードされるまで要求を処理できません。

サイトにControllerが1つしかない場合、アップグレード中は動作しません。

実際のアップグレードが開始される前に、最初のControllerで事前サイトテストが実行されます。詳細については、［事前サイトテスト］(#preliminary-site-tests)を参照してください。

ステップ7：Studioのアップグレード

Web Studio をまだアップグレードしていない場合（別のコンポーネントと同じマシンにあったため）、Studio が含まれているマシンでインストーラーを実行します。

注:

Web Studioをアップグレードした後、バージョン情報がすぐに更新されない場合があります。Web Studioがすでに最新の状態であっても、アップグレードを促されることがあります。この問題に対処するには、Web Studioサーバーに移動し、Internet Information Services (IIS) マネージャーを開き、 > > に移動して、 ペインで を選択します。

ステップ8：Studioの再起動

アップグレードされた Web Studio を再起動します。アップグレードプロセスが自動的に再開されます。

ステップ9：データベースとサイトのアップグレード

注:

障害を避けるため、新しいマシンカタログの作成、マシンカタログの削除、デリバリーグループ内のマシンの更新など、プロビジョニングおよびデリバリーグループ関連のタスクを実行する前に、すべてのDelivery Controllerとデータベースをアップグレードする必要があります。

> SQL Serverデータベースのスキーマを更新するために必要な権限については、準備を確認してください。

- SQL Serverデータベーススキーマを更新する十分な権限がある場合は、データベースの自動アップグレードを開始できます。データベースとサイトを自動的にアップグレードするに進んでください。
- データベースの十分な権限がない場合は、スクリプトを使用する手動アップグレードを開始し、データベース管理者（必要な権限を持つ人）の助けを借りて進めることができます。手動アップグレードの場合、Studioユーザーがスクリプトを生成し、サービスを有効/無効にするスクリプトを実行します。データベース管理者は、SQLCMDユーティリティまたはSQLCMDモードのSQL Server Management Studioを使用して、データベーススキーマを更新する他のスクリプトを実行します。データベースとサイトを手動でアップグレードするに進んでください。
- マルチゾーン展開でデータベースとサイトを自動的にアップグレードする場合、Citrixは、dbschemaのアップグレードを、サイトのSQL Serverデータベースをホストするのと同じゾーンで実行することを推奨します。そうしないと、データベースとサイトの自動アップグレードが失敗する可能性があります。

Citrixは、アップグレード前にデータベースをバックアップすることを強く推奨します。CTX135207を参照してください。データベースのアップグレード中は、製品サービスが無効になります。その間、Controllerはサイトの新しい接続を仲介できないため、慎重に計画してください。

データベースとサイトを自動的にアップグレードする

1. 新しくアップグレードされたStudioを起動します。
2. サイトのアップグレードを自動的に開始することを示し、準備ができたことを確認します。

データベースとサイトのアップグレードが進行します。

データベースとサイトを手動でアップグレードする

1. 新しくアップグレードされたStudioを起動します。
2. サイトを手動でアップグレードすることを示します。ウィザードはライセンスサーバーの互換性を確認し、確認を求めます。
3. データベースをバックアップしたことを確認します。

   ウィザードは、スクリプトとアップグレード手順のチェックリストを生成して表示します。アップグレード対象の製品バージョン以降、データベースのスキーマが変更されていない場

合、そのスクリプトは生成されません。たとえば、ログデータベースのスキーマが変更されない場合、`UpgradeLoggingDatabase.sql` スクリプトは生成されません。

4. 以下のスクリプトを記載されている順序で実行します。

   - `DisableServices.ps1`: Studioユーザーは、製品サービスを無効にするために、ControllerでこのPowerShellスクリプトを実行します。
   - `UpgradeSiteDatabase.sql`: データベース管理者は、サイトデータベースを含むサーバーでこのSQLスクリプトを実行します。
   - `UpgradeMonitorDatabase.sql`: データベース管理者は、監視データベースを含むサーバーでこのSQLスクリプトを実行します。
   - `UpgradeLoggingDatabase.sql`: データベース管理者は、構成ログデータベースを含むサーバーでこのSQLスクリプトを実行します。このスクリプトは、このデータベースが変更された場合（たとえば、ホットフィックスを適用した後など）にのみ実行します。
   - `EnableServices.ps1`: Studioユーザーは、製品サービスを有効にするために、ControllerでこのPowerShellスクリプトを実行します。

   データベースのアップグレードが完了し、製品サービスが有効になると、Studioは環境と構成を自動的にテストし、HTMLレポートを生成します。問題が特定された場合は、データベースのバックアップを復元できます。問題を解決した後、データベースを再度アップグレードできます。

5. チェックリストのタスクを完了したら、**Finish upgrade**をクリックします。

手順10: 残りのDelivery Controllerをアップグレードする

新しくアップグレードされたStudioから、ナビゲーションペインで**Citrix Studio** *site-name*を選択します。**Common Tasks**タブで、**Upgrade remaining Delivery Controllers**を選択します。

> **注:**
>
> **残りのDelivery Controllerのアップグレード**を利用できるようにするには、サイト用に少なくとも1つのマシンカタログと1つのデリバリーグループを作成します。

> アップグレードが完了し、完了を確認したら、Studioを閉じてから再度開きます。Studioは、Controllerのサービスをサイトに登録するため、またはゾーンIDが存在しない場合に作成するために、追加のサイトアップグレードを要求する場合があります。

手順11：VDAのアップグレード

> **重要:**
>
> VDAをバージョン1912以降にアップグレードする場合は、VDAを1912以降にアップグレードするを参照してください。

VDAを含むマシンで製品インストーラーを実行します。

Machine Creation Services™とマスターイメージを使用してマシンを作成した場合、ホストに移動し、マスターイメージ上のVDAをアップグレードします。利用可能なVDAインストーラーのいずれかを使用できます。

- グラフィックインターフェイスのガイダンスについては、VDAのインストールを参照してください。
- コマンドラインのガイダンスについては、コマンドラインを使用したインストールを参照してください。

Citrix Provisioningを使用してマシンを作成した場合は、アップグレードに関するガイダンスについてCitrix Provisioning製品ドキュメントを参照してください。

手順12：マシンカタログとデリバリーグループの更新

- アップグレードされたVDAを使用するマシンを含むカタログを更新する。
- アップグレードされたVDAを使用するマシンを含むカタログをアップグレードする。
- アップグレードされたVDAを使用するマシンを含むデリバリーグループをアップグレードする。

ステップ 13: アップグレード後

展開内の他のコンポーネントをアップグレードします。ガイダンスについては、以下の製品ドキュメントを参照してください。

- StoreFront
- AppDNA
- シトリックス アプリ レイヤリング
- HDX リアルタイム最適化パック
- プロファイル管理

- シトリックス プロビジョニング
- セッション レコーディング
- ワークスペース環境管理

Microsoft SQL Server Express LocalDB ソフトウェアを新しいバージョンに置き換える必要がある場合は、Replace SQL Server Express LocalDBを参照してください。

Dbschema のアップグレード

展開を更新すると、複数のデータベーススキーマをアップグレードできます。次の表に、そのプロセスでアップグレードされるデータベーススキーマを示します。

From\To	1912 CU1	1912 CU2	1912 CU3	1912 CU4	1912 CU5	2203
7.15 RTM or 7.15 CU releases	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 RTM	Config	Site, Config	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU1		Site	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU2			Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU3				Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU4					Site, Config	Site; Monitor; Config; Logging
1912 CU5						Site; Monitor; Config; Logging
2112						Site; Monitor; Config

用語の定義:

- サイト: サイトデータストア。サイトデータストアに対してDbschemaの更新が行われます。
- モニター: モニターデータストア。モニターデータストアに対してDbschemaの更新が行われます。
- 構成: 構成テーブル。構成テーブルで、Desktop Studioのバージョン、ライセンス情報、またはその両方が更新されます。
- ログ: ログデータストア。ログデータストアに対してDbschemaの更新が行われます。

VDAを2203以降にアップグレードする

VDAにPersonal vDisk (PvD) コンポーネントがインストールされていた場合、そのVDAはバージョン2203以降にアップグレードできません。新しいVDAを使用するには、現在のVDAをアンインストールしてから、新しいVDAをインストールする必要があります。

この指示は、PvDを一度も使用したことがない場合でも適用されます。

以前のバージョンでPvDコンポーネントがインストールされた可能性がある方法は次のとおりです。

- VDAインストーラーのグラフィカルインターフェイスでは、PvDは**追加コンポーネント**ページでオプションとして提供されていました。

- コマンドラインでは、`/baseimage`オプションでPvDがインストールされました。このオプションを指定した場合、またはこのオプションを含むスクリプトを使用した場合は、PvDがインストールされました。

VDAにPvDがインストールされているかどうかわからない場合は、マシンまたはイメージで新しいVDA（2203以降）のインストーラーを実行してください。

- PvDがインストールされている場合、互換性のないコンポーネントがあることを示すメッセージが表示されます。
  - グラフィカルインターフェイスから、メッセージが表示されているページで**キャンセル**をクリックし、インストーラーを閉じたいことを確認します。
  - CLIからは、コマンドは表示されたメッセージとともに単に失敗します。
- PvDがインストールされていない場合、アップグレードが続行されます。

対処法

VDAにPvDがインストールされていない場合は、通常のアップグレード手順に従ってください。

VDAにPvDがインストールされている場合：

1. 現在のVDAをアンインストールします。
2. 新しいVDAをインストールします。

Windows 10 (1607以前、更新なし) マシンでPvDを継続して使用する場合は、VDA 7.15 LTSRが最新のサポート対象バージョンです。

> **注:**

> *XenAppおよびXenDesktop 7.15 LTSRでWindows 7デスクトップとPersonal vDiskを使用できますか？*

> Citrixは、2016年1月に発表されたXenAppおよびXenDesktop 7.6 LTSRからPersonal vDisk (PvD) を除外しました。さらに、CitrixはPvDテクノロジーの非推奨を発表し、今後Citrix App Layeringの使用を開始するようお客様に推奨しています。Citrix App Layering (バージョン4.4以降) は、XenAppおよびXenDesktop 7.15 LTSRの互換性のあるコンポーネントです。ただし、Windows 7上の既存のPvD展開を持つお客様がCitrix App Layeringテクノロジーに移行できるよう、CitrixはXenAppおよびXenDesktop 7.15 LTSR累積更新プログラム (CU) を通じてWindows 7デスクトップ向けPvD展開の期間限定サポートをJan 14, 2020まで提供すること

を決定しました。PvDコンポーネントはLTSR CUから削除され、Jan 14, 2020以降はサポートされません。また、Jan 14, 2020以降にWindows 7でPvDを使用すると、LTSRサイトは非準拠となります。さらに、Windows 10向けPvDは7.15 LTSRから引き続き除外されています。したがって、お客様は7.15 LTSRサイトでこれを使用しないでください。

PvD、AppDisks、およびサポートされていないホストを削除する

Citrix Virtual Apps and Desktops 7 Current Release展開では、以下のテクノロジーとホストタイプはサポートされていません。

- カタログ内のユーザーのVMの隣にデータを保存するための**Personal vDisks (PvD)**。ユーザーパーソナライゼーションレイヤー機能がユーザーの永続性を処理するようになりました。
- デリバリーグループで使用されるアプリケーションを管理するための**AppDisks**。
- **ホストタイプ：** Azure Classic、CloudPlatform (元のCitrix製品)。
    - このリリースでサポートされているホストタイプについては、システム要件を参照してください。
    - ARMとAWSを引き続き使用できる代替方法については、CTX270373を参照してください。

現在の展開でPvDまたはAppDiskを使用している場合、あるいはサポートされていないホストタイプ（Microsoft Azure Classicなど）への接続がある場合、それらのテクノロジーを使用する項目を削除した後にのみ、バージョン2006（またはそれ以降のサポートされているバージョン）にアップグレードできます。現在の展開でパブリッククラウドホスト接続（AWSなど）を使用している場合は、アップグレードする前にハイブリッド権限ライセンスがあることを確認してください。インストーラーがサポートされていないテクノロジーまたはハイブリッド権限ライセンスのないホスト接続を1つ以上検出すると、アップグレードは一時停止または停止し、説明メッセージが表示されます。インストーラーログに詳細が含まれています。

アップグレードを確実に成功させるために、サポートされていない項目を削除するための該当するガイダンスを確認し、それに従ってください。

- PvDを削除
- AppDiskを削除
- サポートされていないホスト項目を削除

展開でPvDまたはAppDiskを使用していなかったとしても、関連するMSIが以前のVDAインストールまたはアップグレードに含まれていた可能性があります。VDAをバージョン2006（またはそれ以降のサポートされているバージョン）にアップグレードする前に、たとえ一度も使用していな

かったとしても、そのソフトウェアを削除する必要があります。グラフィカルインターフェイスを使用する場合、その削除は自動的に行われるか、CLIを使用する際に削除オプションを含めることができます。詳細については、PvDまたはAppDiskコンポーネントを持つVDAのアップグレードを参照してください。

PvDを削除

PvDを使用するように構成されているすべてのマシンを削除するまで、展開のアップグレードは成功しません。これはカタログとデリバリーグループに影響します。

グループとカタログからPvDを削除するには：

1. Studioで、デリバリーグループにPvDを使用するカタログのマシンが含まれている場合、「それらのマシンをグループから削除」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/delivery-groups-manage.html#remove-a-machine-from-a-delivery-group)します。
2. Studioで、PvDを使用するマシンを含む「すべてのカタログを削除」(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-manage.html#delete-a-catalog)します。

VDAのアップグレード： 展開のアップグレードでは、VDAにAppDiskまたはPvDコンポーネントがインストールされているかどうかは検出されません。ただし、VDAインストーラーは検出します。詳細については、PvDまたはAppDiskコンポーネントを持つVDAを参照してください。

PvDの代わりにApp Layeringを使用する予定がある場合は、データの移行に関する情報についてPvDからApp Layeringへの移行を参照してください。

AppDiskを削除

デプロイメントのアップグレードは、AppDiskを使用するすべてのデリバリーグループからAppDiskを削除し、その後AppDisk自体を削除するまで続行できません。

1. Studioナビゲーションペインで****を選択します。
2. グループを選択し、アクションペインで****をクリックします。
3. グループからAppDiskを削除するアクションをクリックします。
4. AppDiskを使用する各デリバリーグループに対して、手順2と3を繰り返します。
5. Studioナビゲーションペインで****を選択します。
6. AppDiskを選択し、AppDiskを削除するアクションをクリックします。
7. 各AppDiskについて、手順5と6を繰り返します。

VDAのアップグレード: デプロイメントのアップグレードでは、VDAにAppDiskまたはPvDコンポーネントがインストールされているかどうかは検出されません。ただし、VDAインストーラー

は検出します。詳細については、「PvDまたはAppDiskコンポーネントを持つVDA」を参照してください。

サポートされていないホストアイテムを削除する

サイトがCitrix CloudPlatformやMicrosoft Azure Classicなどのサポートされていないホストタイプへの接続を持っている場合、バージョン2006（またはそれ以降のサポートされているバージョン）へのデプロイメントのアップグレードは続行できません。アップグレードを試みる前に、以下のタスクを完了してください。

Studioから:

- サポートされていないホストへのすべての接続を削除します。
- デリバリーグループに、サポートされていないホストのマスターイメージで作成されたカタログのマシンが含まれている場合、それらのマシンをグループから削除します。
- サポートされていないホストのマスターイメージを使用して作成されたすべてのカタログを削除します。

PvDまたはAppDisksコンポーネントがインストールされているVDA

PvDおよびAppDisksテクノロジーを有効にするコンポーネントがVDAにインストールされている場合、それらのコンポーネントが削除されるまで、そのVDAはアップグレードできません。

> **注：**
>
> バージョン1912にアップグレードする場合、現在のVDAをアンインストールしてから新しいVDAをインストールする必要がありました。このバージョンでは、Citrixがコンポーネントを削除してアップグレードを続行するかどうかを尋ねられます。
>
> AppDiskおよびPvDコンポーネントは、それらのテクノロジーを一度も使用していなくても、以前のVDAバージョンでインストールされている可能性があります。

- グラフィカルインターフェイス：VDAインストーラーの**追加コンポーネント**ページには、**Citrix AppDisk / Personal vDisk**オプションが含まれていました。7.15 LTSRおよびそれ以前の7.xリリースでは、このオプションがデフォルトで有効になっていました。したがって、デフォルトを受け入れた場合（または、このオプションが提供されたリリースで明示的に有効にした場合）、そのコンポーネントがインストールされました。
- CLI：`/baseimage`オプションを指定すると、コンポーネントがインストールされました。

対処法

VDAインストーラーが現在インストールされているVDAでAppDisksまたはPvDコンポーネントを検出しない場合、アップグレードは通常どおり続行されます。

インストーラーが現在インストールされているVDAでAppDisksまたはPvDコンポーネントを検出した場合：

- グラフィカルインターフェイス：アップグレードが一時停止します。サポートされていないコンポーネントを自動的に削除するかどうかを尋ねるメッセージが表示されます。**OK**をクリックすると、コンポーネントは自動的に削除され、アップグレードが続行されます。
- CLI：コマンドの失敗を避けるため、コマンドに次のオプションを含めます。
  - `/remove_appdisk_ack`
  - `/remove_pvd_ack`

制限事項

アップグレードには次の制限が適用されます。

- **コンポーネントの選択的インストール:** 新しいバージョンにコンポーネントをインストールまたはアップグレードしても、アップグレードが必要な他のコンポーネント（別のマシン上）をアップグレードしない場合、Studioから通知されます。たとえば、アップグレードにControllerとStudioの新しいバージョンが含まれているとします。Controllerをアップグレードしても、Studioがインストールされているマシンでインストーラーを実行しない場合、Studioをアップグレードするまで、Studioはサイトの管理を続行できません。

  VDAをアップグレードする必要はありませんが、利用可能なすべての機能を使用できるように、すべてのVDAをアップグレードすることをお勧めします。
- **早期リリースまたはテクノロジプレビューバージョン：** 早期リリース、テクノロジプレビュー、またはプレビューバージョンからアップグレードすることはできません。
- **以前のオペレーティングシステム上のコンポーネント：** MicrosoftまたはCitrixでサポートされなくなったオペレーティングシステムに現在のVDAをインストールすることはできません。詳しくは、「以前のオペレーティングシステム」を参照してください。
- **混在環境/サイト：** 以前のバージョンのサイトと現在のバージョンのサイトを継続して実行する必要がある場合は、「混在環境に関する考慮事項」を参照してください。
- **製品の選択：** 以前のバージョンからアップグレードする場合、インストール時に設定された製品（Citrix Virtual AppsまたはCitrix Virtual Apps and Desktops）を選択または指定することはありません。

混在環境に関する考慮事項

アップグレードする際は、すべてのコンポーネントとVDAをアップグレードすることをお勧めします。これにより、エディションとバージョンに含まれるすべての新機能と強化された機能にアクセスできるようになります。

たとえば、以前のControllerバージョンを含む展開で現在のVDAを使用することはできますが、現在のリリースに含まれる新機能は利用できない場合があります。最新ではないバージョンを使用している場合、VDA登録の問題が発生することもあります。

環境によっては、すべてのVDAを最新バージョンにアップグレードできない場合があります。その場合、マシンカタログを作成するときに、マシンにインストールされているVDAバージョンを指定できます。（これは機能レベルと呼ばれます。）デフォルトでは、この設定は推奨される最小VDAバージョンを指定します。ほとんどの展開では、デフォルト値で十分です。カタログにデフォルトよりも古いVDAが含まれている場合にのみ、設定を以前のバージョンに変更することを検討してください。マシンカタログでVDAバージョンを混在させることはお勧めしません。

カタログがデフォルトの最小VDAバージョン設定で作成され、1つ以上のマシンにデフォルトバージョンよりも古いVDAがある場合、それらのマシンはControllerに登録できず、機能しません。

詳細については、VDAバージョンと機能レベルを参照してください。

異なるバージョンを持つ複数のサイト

環境に異なる製品バージョンを持つサイト（例えば、XenDesktop 7.18サイトとCitrix Virtual Apps and Desktops 1909サイト）が含まれている場合、CitrixはStoreFrontを使用して異なる製品バージョンからのアプリケーションとデスクトップを集約することを推奨します。詳細については、StoreFrontのドキュメントを参照してください。

混在環境では、各リリースに対応するStudioおよびDirectorのバージョンを引き続き使用しますが、異なるバージョンは別々のマシンにインストールされていることを確認してください。

以前のオペレーティングシステム

サポートされているオペレーティングシステム（OS）バージョンを実行しているマシンに、以前のバージョンのコンポーネントをインストールしたとします。現在、より新しいコンポーネントバージョンを使用したいのですが、そのOSは現在のコンポーネントバージョンではサポートされていません。

たとえば、Windows Server 2016マシンにサーバーVDAをインストールしたとします。現在、そのVDAを現在のリリースにアップグレードしたいが、アップグレード先の現在のリリースではWindows Server 2016がサポートされていません。

許可されていないオペレーティングシステムにコンポーネントをインストールまたはアップグレードしようとすると、「このオペレーティングシステムにはインストールできません」などのエラーメッセージが表示されます。

これらの考慮事項は、Current ReleaseおよびLong Term Service Releaseバージョンのアップグレードに適用されます。（LTSRバージョンにCUを適用することには影響しません。）

サポートされているOSについては、以下のリンクを参照してください。

- Citrix Virtual Apps and Desktops (現在のリリース):
  - デリバリーコントローラー、スタジオ、ディレクター、VDA、ユニバーサルプリントサーバー
  - フェデレーション認証サービス
  - StoreFront、Self-Service Password Reset、Session Recordingについては、現在のリリースのシステム要件の記事を参照してください。
- LTSRについては、LTSRバージョンとCUのコンポーネントリストを参照してください。(メインのCitrix Virtual Apps and Desktops製品ドキュメントページからLTSRバージョンを選択してください。)

無効なオペレーティングシステム

次の表は、現在のリリースでコンポーネントのインストール/アップグレードに無効な以前のオペレーティングシステムを示しています。各OSでサポートされている最新の有効なコンポーネントバージョンと、インストールおよびアップグレードが無効になったコンポーネントバージョンが示されています。

表中のオペレーティングシステムにはサービスパックと更新プログラムが含まれます。

オペレーティングシステム	コンポーネント/機能	最新の有効なバージョン	インストール/アップグレードが不可能になったバージョン
Windows 7および Windows 8	VDA	7.15 LTSR	7.16
Windows 7および Windows 8	その他のインストーラーコンポーネント	7.17	7.18

オペレーティングシステム	コンポーネント/機能	最新の有効なバージョン	インストール/アップグレードが不可能になったバージョン
Windows 10バージョン1607より前のバージョン	VDA	7.15 LTSR	7.16
Windows 10 x86 バージョン	VDA	1906.2.0	1909
Windows サーバー 2008 R2	VDA	7.15 LTSR	7.16
Windows サーバー 2008 R2	その他のインストーラーコンポーネント	7.17	7.18
Windows サーバー 2012	VDA	7.15 LTSR	7.16
Windows サーバー 2012	その他のインストーラーコンポーネント	7.17	7.18
ウィンドウズ サーバー 2012 R2	その他のインストーラーコンポーネント *	1912 LTSR	2003
ウィンドウズ サーバー 2012 R2	サーバーVDI	7.15 LTSR	7.16
Windows サーバー 2016	サーバーVDI	7.15 LTSR	7.16

Windows XPおよびWindows Vistaは、7.xのコンポーネントまたはテクノロジでは無効です。

* Delivery Controller、Studio、Director、およびVDAに適用されます。

実行できること

選択肢があります。次のことができます。

- 現在のOSを使い続ける(#continue-with-the-current-os)
- マシンの再イメージ化またはアップグレード(#reimage-or-upgrade-the-machine)

- 新しいマシンを追加してから古いマシンを削除する(#add-new-machines-and-then-remove-old-machines)

現在のOSを使い続ける

これらの方法はVDAで実行可能です。以前のOSを搭載したマシンの使用を継続する場合は、次のいずれかを選択できます。

- インストールされているコンポーネントバージョンを使い続ける。
- 最新の有効なコンポーネントバージョンをダウンロードし、そのバージョンにコンポーネントをアップグレードする。（これは、最新の有効なコンポーネントバージョンがまだインストールされていないことを前提としています。）

たとえば、Windows 7 SP1マシンに7.14 VDAがインストールされているとします。Windows 7 OSマシンで有効な最新のVDAバージョンは、XenApp and XenDesktop 7.15 LTSRです。7.14を使い続けるか、7.15 LTSR VDAをダウンロードしてVDAをそのバージョンにアップグレードすることができます。これらの以前のVDAバージョンは、新しいバージョンのDelivery Controllerを含む展開で動作します。たとえば、7.15 LTSR VDAはCitrix Virtual Apps and Desktops 7 1808 Controllerに接続できます。

マシンの再イメージ化またはアップグレード

これらの方法は、VDAや、コアコンポーネント（Delivery Controllerなど）がインストールされていないその他のマシンに実行可能です。次のいずれかを選択してください。

- マシンをサービスから外した後（メンテナンスモードをオンにし、すべてのセッションを閉じさせた後）、サポートされているWindows OSバージョンに再イメージ化し、その後、コンポーネントの最新バージョンをインストールできます。
- VDAマシンで再イメージ化せずにOSをアップグレードするには、まず、アップグレード先のOSでサポートされているVDAバージョンをインストールするか、OSのアップグレード後にVDAをアップグレードする必要があります。そうしないと、Citrixソフトウェアはサポートされなくなります。VDAをアンインストールせずにインプレースアップグレードを実行する場合、次の最小OSバージョンにアップグレードできます。
  - Windows 11で2023-07 Cumulative Update for Windows 11 (KB5028185)以降がインストールされているもの（ビルド22621.1992以降）。
  - Windows 10で2023-07 Dynamic Update for Windows 10 (KB5028311)がインストールされているもの。

- アップグレードを計画しているWindowsバージョンが上記のガイドラインに合致しない場合、OSをアップグレードする前にVDAをアンインストールし、OSアップグレードの完了後にサポートされているVDAバージョンをインストールする必要があります。

新しいマシンを追加し、古いマシンを削除する

この方法は、Delivery Controller™ またはその他のコアコンポーネントを含むマシンの OS をアップグレードする必要がある場合に実行可能です。

Citrixは、サイト内のすべてのControllerが同じOSを持つことを推奨します。次のアップグレードシーケンスは、異なるControllerが異なるOSを持つ期間を最小限に抑えます。

1. サイト内のすべてのDelivery Controllerのスナップショットを取得し、その後、サイトデータベースをバックアップします。
2. サポートされているオペレーティングシステムを搭載したクリーンなサーバーに、新しいDelivery Controllerをインストールします。
3. 新しいControllerをサイトに追加します。
4. 現在のリリースで有効ではないオペレーティングシステムで実行されているControllerを削除します。Delivery ControllersでControllerを削除するための推奨事項に従ってください。

準備

アップグレードを開始する前に、以下の情報を確認し、必要なタスクを完了してください。

> **注:**
>
> VDA のアップグレードは アップグレードシーケンス の後半で行われますが、アップグレードを開始する前にインストーラーを選択し、手順を確認して、何が予想されるかを知っておくことをお勧めします。

インストーラーとインターフェイスを選択する

コンポーネントをアップグレードするには、製品ISOのフルプロダクトインストーラーを使用します。VDAは、フルプロダクトインストーラーまたはスタンドアロンVDAインストーラーのいずれかを使用してアップグレードできます。すべてのインストーラーは、グラフィカルインターフェイスとコマンドラインインターフェイスを提供します。

詳細については、インストーラー を参照してください。

インストールの詳細: 準備作業を完了し、インストーラーを起動する準備ができたら、インストール記事には、表示される内容 (グラフィカルインターフェイスを使用している場合) または入力する内容 (コマンドラインインターフェイスを使用している場合) が示されています。

- グラフィカルインターフェイスを使用してコアコンポーネントをインストール/アップグレードする
- コマンドラインを使用してコアコンポーネントをインストール/アップグレードする
- グラフィカルインターフェイスを使用してVDAをインストール/アップグレードする
- コマンドラインを使用してVDAをインストール/アップグレードする

シングルセッションVDAを`VDAWorkstationCoreSetup.exe`インストーラーで最初にインストールした場合、そのインストーラーを使用してアップグレードすることをお勧めします。フルプロダクトVDAインストーラーまたは`VDAWorkstationSetup.exe`インストーラーを使用してVDAをアップグレードすると、明示的にアップグレードから除外しない限り、元々除外されていたコンポーネントがインストールされる可能性があります。

VDAを現在のリリースにアップグレードする際、アップグレードプロセス中にマシンの再起動が発生します（この要件は7.17リリースから始まりました）。これは回避できません。再起動後、アップグレードは自動的に再開されます（コマンドラインで`/noresume`を指定しない限り）。

データベース操作

サイト、監視、および構成ログデータベースをバックアップします。CTX135207の手順に従ってください。アップグレード後に問題が発見された場合、バックアップを復元できます。

サポートされなくなったSQL Serverバージョンのアップグレードについては、SQL Serverバージョンチェックを参照してください。(これは、サイト、モニター、および構成ログデータベースに使用されるSQL Serverを指します。)

Microsoft SQL Server Express LocalDBは、ローカルホストキャッシュで使用するために自動的にインストールされます。以前のバージョンを置き換える必要がある場合、新しいバージョンはSQL Server Express LocalDB 2019である必要があります。コンポーネントとサイトをアップグレードした後にSQL Server Express LocalDBを新しいバージョンに置き換える方法の詳細については、SQL Server Express LocalDBの置き換えを参照してください。

Citrixライセンスが最新であることを確認する

Citrixライセンスの管理に関する包括的な情報については、Citrixライセンスのアクティブ化、アップグレード、および管理を参照してください。

フル製品インストーラーを使用してライセンスサーバーをアップグレードできます。または、ライセンスコンポーネントを個別にダウンロードしてアップグレードすることもできます。アップグレードを参照してください。

アップグレードする前に、Customer Success Services / Software Maintenance / Subscription Advantageの日付が新しい製品バージョンに対して有効であることを確認してください。日付は2021.11.15以降である必要があります。

Citrixライセンスサーバーの互換性を確認する

Citrixライセンスサーバーが新しいバージョンと互換性があることを確認してください。これを行うには2つの方法があります。

- 他のCitrixコンポーネントをアップグレードする前に、Delivery Controllerを含むマシンでISOレイアウトから`XenDesktopServerSetup.exe`インストーラーを実行します。互換性の問題がある場合、インストーラーは推奨される解決手順とともにそれを報告します。
- インストールメディアの`XenDesktop Setup`ディレクトリから、コマンド`.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`を実行します。表示でライセンスサーバーが互換性があるかどうかが示されます。ライセンスサーバーに互換性がない場合は、ライセンスサーバーをアップグレードしてください。

StoreFrontの変更をバックアップする

アップグレードを開始する前に、`C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`内のファイル（*default.ica*や*usernamepassword.tfrm*など）を変更している場合は、各ストアについてそれらをバックアップしてください。アップグレード後、それらを復元して変更を元に戻すことができます。

アプリケーションとコンソールを閉じる

アップグレードを開始する前に、管理コンソールやPowerShellセッションなど、ファイルロックを引き起こす可能性のあるすべてのプログラムを閉じてください。

マシンを再起動すると、ファイルロックがすべて解除され、保留中のWindowsアップデートがないことが保証されます。

アップグレードを開始する前に、サードパーティの監視エージェントサービスを停止して無効にします。

適切な権限があることを確認する

ドメインユーザーであることに加えて、製品コンポーネントをアップグレードするマシンのローカル管理者である必要があります。

サイトデータベースとサイトは、自動または手動でアップグレードできます。データベースの自動アップグレードの場合、Studioユーザーの権限には、SQL Serverデータベーススキーマを更新する機能（たとえば、`db_securityadmin`または`db_owner`データベースロール）が含まれている必要があります。詳細については、「データベース」を参照してください。

Studioユーザーがこれらの権限を持っていない場合、手動データベースアップグレードを開始すると、スクリプトが生成されます。Studioユーザーは、Studioから一部のスクリプトを実行します。データベース管理者は、SQL Server Management Studioなどのツールを使用して、他のスクリプトを実行します。

その他の準備タスク

- 必要に応じて、テンプレートをバックアップし、ハイパーバイザーをアップグレードします
- 事業継続計画で定められているその他の準備タスクを完了します。

サイトの事前テスト

Delivery Controllerとサイトをアップグレードすると、実際のアップグレードが始まる前に予備サイトテストが実行されます。これらのテストでは、以下が検証されます。

- サイトデータベースにアクセスでき、バックアップされていること
- 重要なCitrixサービスへの接続が正しく機能していること
- Citrixライセンスサーバーのアドレスが利用可能であること
- 構成ログデータベースにアクセスできること
- パブリッククラウドホスト接続（AWSなど）を追加する場合は、ハイブリッド権限ライセンスがあることを確認してください。そうでない場合、サイトの事前テストは一時停止または停止し、説明メッセージが表示されます。

テストの実行後、結果のレポートを表示できます。その後、検出された問題を修正し、テストを再度実行できます。予備サイトテストを実行せず、問題を解決しないと、サイトの動作に影響を与える可能性があります。

テスト結果を含むレポートは、インストールログと同じディレクトリにあるHTMLファイル（`PreliminarySiteTestResult.html`）です。このファイルが存在しない場合は作成されます。ファイルが存在する場合は、その内容が上書きされます。

テストを実行する

- インストーラーのグラフィカルインターフェイスを使用してアップグレードする場合、ウィザードにはテストを開始してレポートを表示できるページが含まれています。テストが実行さ

れ、レポートを確認し、検出された問題を解決した後、テストを再実行できます。テストが正常に完了したら、 をクリックしてウィザードを続行します。

- コマンドラインインターフェイスを使用してアップグレードする場合、テストは自動的に実行されます。デフォルトでは、テストが失敗した場合、アップグレードは実行されません。レポートを確認し、問題を解決した後、コマンドを再実行してください。

Citrixでは、Controllerとサイトのアップグレードを続行する前に、常に予備サイトテストを実行し、問題を解決することをお勧めします。テストを実行するのにかかるわずかな時間に対して、潜在的なメリットは十分にあります。ただし、この推奨されるアクションを上書きすることもできます。

- グラフィカルインターフェイスでアップグレードする場合、テストをスキップしてアップグレードを続行することを選択できます。
- コマンドラインからアップグレードする場合、テストをスキップすることはできません。デフォルトでは、サイトテストが失敗すると、アップグレードを実行せずにインストーラーが失敗します。通常、`/ignore_site_test_failure` オプションを含めると、テストの失敗は無視され、アップグレードが続行されます。(例外については、SQL Server version check を参照してください。)

複数のControllerをアップグレードする場合

1つのControllerでアップグレードを開始し、同じサイト内の別のControllerでアップグレードを開始する場合（最初のアップグレードが完了する前）：

- 最初のControllerで予備サイトテストが完了している場合、他のControllerのウィザードには予備サイトテストページは表示されません。
- 他のControllerでアップグレードを開始したときに最初のControllerでのテストが進行中の場合、他のControllerのウィザードにサイトテストページが表示されます。ただし、最初のControllerでのテストが完了すると、最初のControllerからのテスト結果のみが保持されます。

サイトの健全性に関連しないテストの失敗

- メモリ不足が原因で予備サイトテストが失敗した場合は、メモリを増やしてからテストを再実行してください。
- アップグレードの権限はあるが、サイトテストを実行する権限がない場合、予備サイトテストは失敗します。これを解決するには、テストを実行する権限を持つユーザーアカウントでインストーラーを再実行してください。

SQL Serverバージョンの確認

Citrix Virtual Apps and Desktopsの展開を成功させるには、サイト、モニター、および構成ログデータベース用にサポートされているバージョンのMicrosoft SQL Serverが必要です。サポートされなくなったSQL ServerバージョンでCitrix展開をアップグレードすると、機能上の問題が発生し、サイトがサポート対象外になる可能性があります。

アップグレードするCitrixリリースでサポートされているSQL Serverのバージョンを確認するには、そのリリースのシステム要件の記事を参照してください。

Controllerをアップグレードする際、Citrixインストーラーは、サイト、モニター、および構成ログデータベースに使用されている現在インストールされているSQL Serverのバージョンを確認します。

- チェックの結果、現在インストールされているSQL Serverのバージョンが、アップグレードするCitrixリリースでサポートされているバージョンではないと判断された場合：
  - グラフィカルインターフェイス：アップグレードはメッセージとともに停止します。**I understand**をクリックし、次に**Cancel**をクリックしてCitrixインストーラーを閉じます。(アップグレードを続行することはできません。)
  - コマンドラインインターフェイス：コマンドは失敗します（コマンドに`/ignore_db_check_failure`オプションを含めた場合でも）。

  SQL Serverのバージョンをアップグレードしてから、Citrixのアップグレードを再度開始してください。
- チェックで現在インストールされているSQL Serverのバージョンを特定できない場合は、アップグレードするバージョンで現在インストールされているバージョンがサポートされているかどうかを確認してください（システム要件）。
  - グラフィカルインターフェイス：アップグレードはメッセージとともに停止します。
    - 現在インストールされているSQL Serverのバージョンがサポートされている場合は、**I understand**をクリックしてメッセージを閉じ、**Next**をクリックしてCitrixのアップグレードを続行します。
    - 現在インストールされているSQL Serverのバージョンがサポートされていない場合は、**I understand**をクリックしてメッセージを閉じ、**Cancel**をクリックしてCitrixのアップグレードを終了します。SQL Serverをサポートされているバージョンにアップグレードしてから、Citrixのアップグレードを再度開始してください。
  - コマンドラインインターフェイス：コマンドはメッセージとともに失敗します。メッセージを閉じた後：

- 現在インストールされているSQL Serverのバージョンがサポートされている場合は、`/ignore_db_check_failure`オプションを指定してコマンドを再度実行します。
- 現在インストールされているSQL Serverのバージョンがサポートされていない場合は、SQL Serverをサポートされているバージョンにアップグレードします。コマンドを再度実行してCitrixのアップグレードを開始します。

SQL Serverのアップグレード

新しいSQL Serverを立ち上げてサイトデータベースを移行する場合は、接続文字列を更新する必要があります。

サイトが現在、サイトデータベースにSQL Server Expressを使用している場合（Citrixがサイト作成時に自動的にインストールしたもの）：

1. 最新のSQL Server Expressバージョンをインストールします。
2. データベースをデタッチします。
3. データベースを新しいSQL Server Expressにアタッチします。
4. 接続文字列を移行します。

詳細については、「接続文字列の構成」およびMicrosoft SQL Server製品ドキュメントを参照してください。

SQL Server Express LocalDBを置き換える

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

CitrixはSQL Server Express LocalDBを自動的に更新しません。SQL Server Express LocalDBのバージョンを更新するには、このセクションのガイダンスに従ってください。

- Delivery ControllerをCitrix Virtual Apps and Desktopsバージョン2203 LTSR以降のバージョンにアップグレードする場合、サポートされるバージョンはSQL Server Express LocalDB 2019またはSQL Server Express LocalDB 2022です。

必要なもの:

- Citrix Virtual Apps and Desktopsインストールメディア。
- Windows SysinternalsツールボックスのPsExecツール。

手順:

1. Citrix Virtual Apps and Desktopsのコンポーネント、データベース、およびサイトのアップグレードを完了します。（これらのデータベースアップグレードは、サイト、監視、および構成ログデータベースに影響します。SQL Server Express LocalDBを使用するローカルホストキャッシュデータベースには影響しません。）
2. SQL Server Express LocalDBを更新するDelivery Controllerにログオンします。
3. MicrosoftからPsExecをダウンロードし、そのDelivery Controller上のアクセスしやすい場所（例: C:\Temp）に配置します。
4. Windowsシステムサービスから、Delivery Controller上のCitrix High Availability Serviceを停止します。
5. Delivery Controllerでコマンドプロンプトを開き、PsExecがある場所（例: `C:\Temp`）に移動してから、次のコマンドを実行してNetwork Serviceアカウントでコマンドプロンプトを昇格させます。

   ```
   psexec -i -u "NT AUTHORITY\NETWORKSERVICE" cmd
   ```

6. `whoami`を実行して、コマンドプロンプトがNetwork Serviceアカウントとして実行されていることを確認します。次の出力が得られるはずです: `nt authority\networkservice`。
7. コマンドプロンプトを使用して、SQL LocalDBインスタンスに移動します。

   - SQL LocalDB 2014からアップグレードする場合:

     ```
     cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
     ```

   - SQL LocalDB 2017からアップグレードする場合:

     ```
     cd "C:\Program Files\Microsoft SQL Server\140\Tools\Binn"
     ```

   - SQL LocalDB 2019からアップグレードする場合:

     ```
     cd "C:\Program Files\Microsoft SQL Server\150\Tools\Binn"
     ```

8. SQL LocalDBインスタンスを停止して削除します: `CitrixHA`。

   ```
   SqlLocalDB stop CitrixHA
   ```

```
SqlLocalDB delete CitrixHA
```

9. Delivery Controllerから以下のファイルを削除します:

```
C:\Windows\ServiceProfiles\NetworkService\HADatabaseName.*

C:\Windows\ServiceProfiles\NetworkService\HADatabaseName_log.*

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName.* (if
exists)

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName_log.*
(if exists)
```

10. プログラムの削除のためのWindowsのネイティブ機能を使用して、Delivery Controllerから既存のSQL LocalDB SQL Server Expressをアンインストールします。
11. アンインストールが完了したら、Delivery Controllerを再起動します。
12. Windowsシステムサービスから、Delivery Controller上のCitrix High Availability Serviceを停止します。
13. Citrix Virtual Apps and DesktopsのインストールメディアをDelivery Controllerにマウントします。
14. Delivery Controllerに管理者としてSQL Server Express LocalDB 2022をインストールします。
    a. Citrix Virtual Apps and Desktopsインストールメディアの`Support > SQLLocalDB`フォルダーにある`sqllocaldb.msi`ファイルを使用します。たとえば、インストールメディアが`E drive`ドライブ文字にマウントされている場合、ファイルは`E:\Support\SQLLocalDB\sqllocaldb.msi`にあります。インストールを完了するには再起動が必要です。
    b. 新しいSQL LocalDBは`C:\Program Files\Microsoft SQL Server\160\Tools\Binn`にある必要があります。
15. WindowsシステムサービスからDelivery Controller上のCitrix High Availability Serviceを開始します。
16. Delivery Controllerのコマンドプロンプトで、`C:\Program Files\Microsoft SQL Server\160\Tools\Binn`に移動し、`SqlLocalDB i`を実行してCitrixHAインスタンスが作成

されたことを確認します。返されたインスタンスのリストには`CitrixHA`が含まれている必要があります。

> **注：**
>
> Citrix High Availability Serviceの開始後、CitrixHAデータベースが作成されるまでに最大15分かかる場合があります。

17. ローカルホストキャッシュデータベースファイルが作成されていることを確認し、必要に応じて高可用性サービス（セカンダリブローカー）が引き継ぐことができることを確認します。
    a. Delivery Controllerで、`C:\Windows\ServiceProfiles\NetworkService`を参照します。
    b. `HaDatabaseName.mdf`と`HaDatabaseName_log.ldf`が作成されていることを確認します。
18. 残りのDelivery Controllerで手順を繰り返します。

VDAアップグレードエージェントのプロキシサポート

VDAアップグレードエージェントのプロキシサポートは、2311 VDAで追加されました。

2311 VDA (バージョン: 7.40) のVDAアップグレードエージェントは、プロキシを介してトラフィックを認識し、送信できます。

VDAアップグレードエージェント (VUA) は、Hostname:Port (IP:Port) およびPACファイルの形式でプロキシをサポートしています。

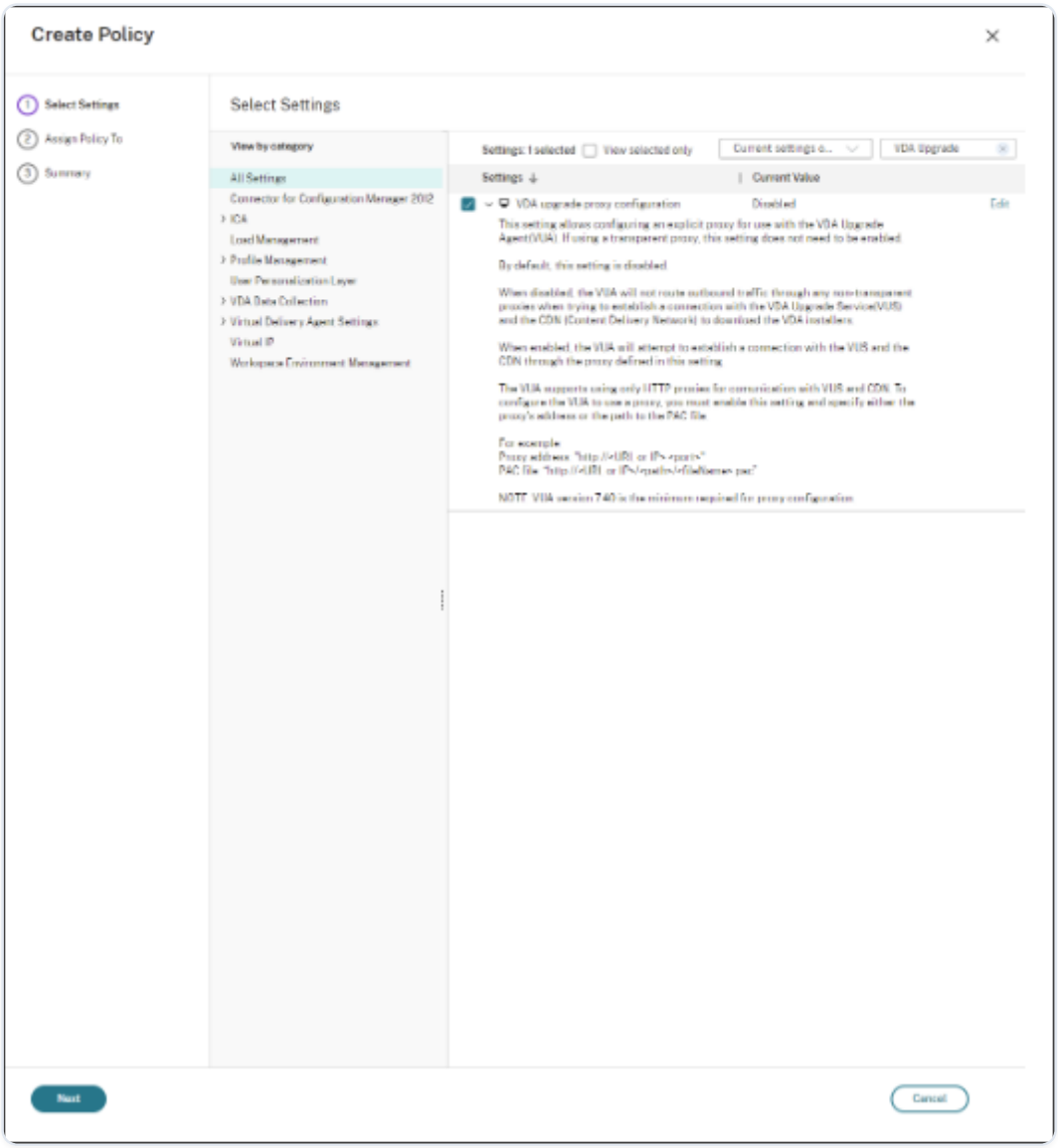
HTTPプロキシのみがサポートされています。 パケットの復号化と検査はサポートされていません。

プロキシ認証はサポートされていません。 SOCKS5はサポートされていません。

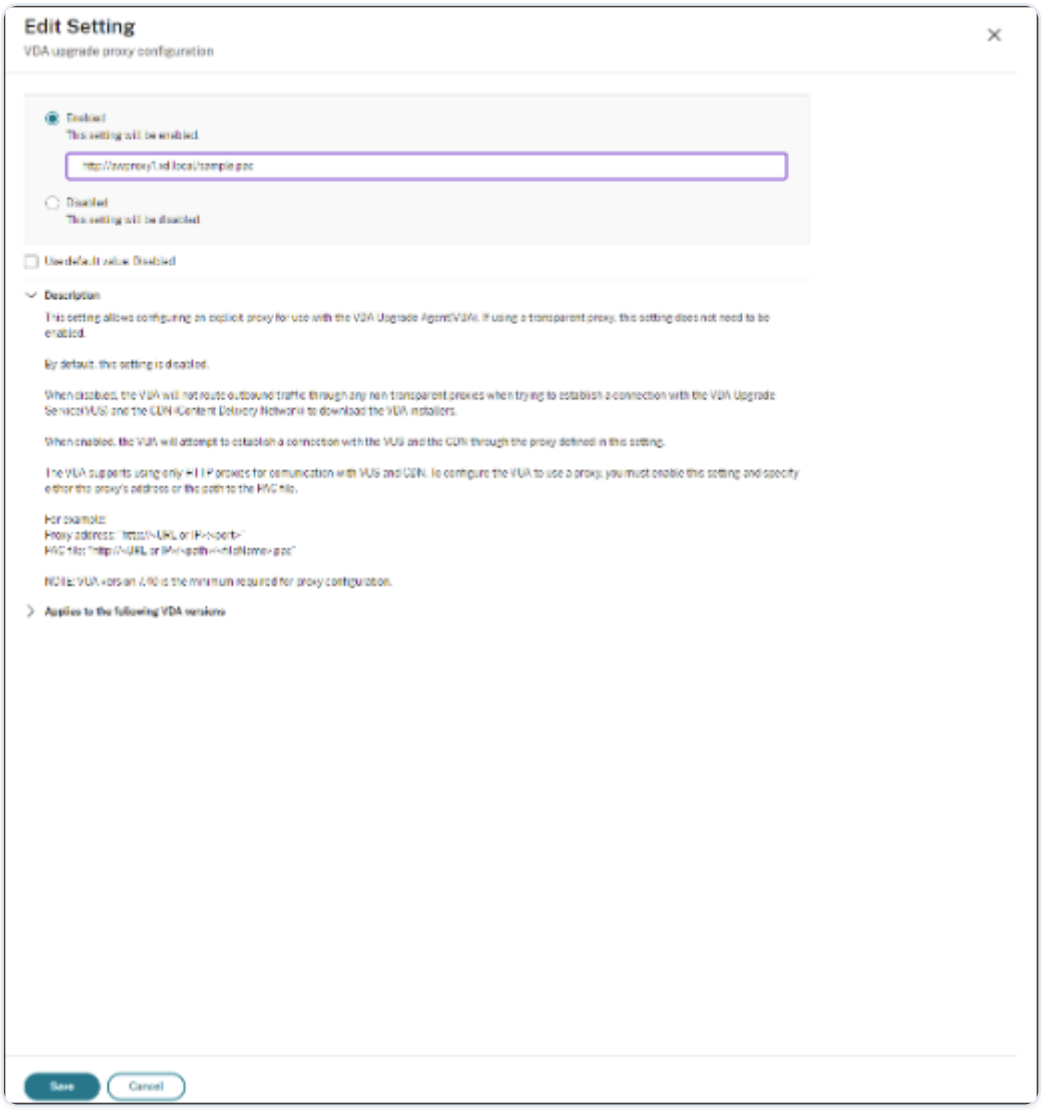
VDAアップグレードエージェントプロキシの構成

VDAアップグレードエージェントプロキシは、次の2つの方法で構成できます。

1. **Webstudioポリシー**を使用して**VDAアップグレードエージェントポリシーを構成**する。
2. **ポリシーの作成**ページで、**設定**から**VDAアップグレードプロキシ構成**を選択します。



3. この設定を有効にします。デフォルトでは、この設定は無効になっています。



4. レジストリキーを使用したVDAアップグレードエージェントの構成。

   レジストリキーは、VDAインストール中にMeta-Installerに設定されます。

   レジストリ:

   キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`

   値の型: 文字列

   値の名前: ProxySettings

   値のデータ: プロキシアドレスまたはPACファイルへのパス。

   例:

   a. プロキシアドレス: `http://<URL or IP>:<port>`

   b. PACファイル: `http://<URL or IP>/<path/<filename>.pac`

セキュリティ

FIDO2認証

FIDO2およびWebAuthnを使用したローカル認証と仮想認証

ユーザーは、FIDO2セキュリティキーと、TPM 2.0およびWindows Helloを搭載した統合生体認証デバイスを使用して、仮想セッションでFIDO2またはWebAuthnを利用するアプリケーションに認証できます。

FIDO2の詳細については、「FIDO2: WebAuthn & CTAP」を参照してください。

この機能の使用方法については、「FIDO2リダイレクト」を参照してください。

> **注**
>
> この機能は、WebAuthnまたはFIDO2を使用した仮想セッションへのログオンをサポートしていません。この機能は、仮想セッション内のアプリケーションでこれらの認証方法を使用することのみを許可します。

> この機能は、ダブルホップシナリオではサポートされていません。

サポートマトリックス

セッションホストオペレーティングシステム	WEBアプリケーション認証	UWPアプリケーション認証
ウィンドウズ サーバー 2016	USBリダイレクト経由でサポート	サポートされていません
Windows サーバー 2019	サポートされています	サポートされていません
Windows サーバー 2022	サポートされています	サポートされています
ウィンドウズ 10	サポートされています	サポートされています

セッションホストオペレーティングシステム	WEBアプリケーション認証	UWPアプリケーション認証
ウィンドウズ 11	サポートされています	サポートされています

詳細については、以下の要件を確認してください。

Webアプリケーション認証

要件

WebアプリケーションでFIDO2およびWebAuthn認証を使用するための要件は次のとおりです。

Citrix® コントロールプレーン

- Citrix Virtual Apps and Desktops™ 2009以降のバージョン

セッションホスト

- オペレーティングシステム
  - Windows 10 1809以降
  - Windows Server 2019以降のバージョン
- VDA
  - Windows: バージョン2009以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809以降
  - Linux: Workspace app for Linuxのシステム要件を参照してください。
- Workspaceアプリ
  - Windows: バージョン2009.1以降
  - Linux: 2303以降

Webブラウザーの要件

- 32ビットおよび64ビットブラウザ

サポートされる認証方法

- FIDO2セキュリティキー
- ウィンドウズ ハロー
  - TPM 2.0
  - 統合生体認証
    - 顔認証
    - 指紋スキャナー
  - WebAuthn

UWPアプリケーション認証

Citrix Virtual Apps and Desktops 2112のリリースにより、CitrixはUWPアプリケーションでのWebAuthnおよびFIDO2認証をサポートします。

Microsoft Teams、Office 365向けMicrosoft Outlook、OneDriveなどのアプリケーションは、Azure Active Directoryへのリンクとして認証にUWPアプリケーションを使用します。Citrixは、これらのアプリケーションの認証にFIDO2を使用することをサポートするようになりました。

要件

UWPアプリケーションでFIDO2およびWebAuthn認証を使用するための要件は次のとおりです。

Citrixコントロールプレーン

- シトリックス バーチャル アプリケーションズ アンド デスクトップス 2112 以降

セッションホスト

- オペレーティングシステム
  - Windows 10 1809以降
  - Windows Server 2022 またはそれ以降
- VDA
  - Windows: バージョン2112以降

クライアントデバイス

- オペレーティングシステム

- Windows 10 1809 以降
- Linux: Workspace app for Linuxのシステム要件を参照してください。

- Workspaceアプリ
  - Windows: バージョン2009.1以降
  - Linux: 2303以降

UWPアプリケーションの要件

- 32 ビットおよび 64 ビットアプリケーション

サポートされる認証方法

- FIDO2セキュリティキー
- ウィンドウズ ハロー
  - TPM 2.0
  - 統合生体認証
    - 顔認識
    - 指紋スキャナー
  - WebAuthn

> **注:**
>
> クライアント、VDA、またはオペレーティングシステムで機能がサポートされていないためFIDO2リダイレクトが利用できないシナリオでは、USBベースのFIDO2キーはUSBリダイレクトを使用してリダイレクトできます。 FIDO2リダイレクトが利用可能なシナリオでも、USBリダイレクトを使用してUSBベースのFIDO2キーをリダイレクトすることが可能です。この場合、FIDO2リダイレクトを無効にし、適切なUSBリダイレクトルールを構成する必要があります。 USBリダイレクトルールを使用してFIDO2キーを構成する方法の詳細については、USBリダイレクトデバイスルールのドキュメントを参照してください。

msedgewebview2.exeベースのアプリケーションの高度な構成

> **注:**

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

> msedgewebview2.exeベースのWebアプリケーションを持つ企業の場合、HDXセッション内でFIDO2リダイレクトを機能させるために、VDAに追加のレジストリ値を追加する必要があります。

msedgewebview2.exeのフルパスをAllowedProcessesレジストリ値に追加します。

- キー: HKLM\SOFTWARE\Citrix\WebAuthnAllowedProcesses
- 値の名前: AllowedProcesses
- 値の型: REG_MULTISZ
- 値のデータ: `<add full path of the msedgewebview2.exe here >`

64ビットアプリケーションの場合、以下の値を設定する必要があります。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\msedgewebview2
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: FilePathName
- 値の型: REG_SZ
- 値のデータ: C:\Program Files\Citrix\HDX\bin\CtxWebAuthnHook.dll
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: Flag
- 値の型: DWORD
- 値のデータ: 00000002

32ビットアプリケーションの場合、以下の値を設定する必要があります。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook

- 値の名前: FilePathName
- 値の型: REG_SZ
- 値のデータ: C:\Program Files\Citrix\HDX\bin\CtxWebAuthnHook.dll
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: Flag
- 値の型: DWORD
- 値のデータ: 00000002

msedgewebview2.exeベースのアプリケーションでFIDO2リダイレクトを有効にするためのレジストリ値を設定した後、VDAを再起動します。

シトリックス バーチャル アプリケーションズ アンド デスクトップス™ を シトリックス ゲートウェイ と統合する

StoreFront™ サーバーは、公開されたリソースとデータへのアクセスを管理するために展開および構成されます。リモートアクセスの場合、StoreFront の前に Citrix Gateway を追加することをお勧めします。

> **注:**
>
> Citrix Virtual Apps and Desktops を Citrix Gateway と統合する方法の詳細な構成手順については、StoreFront ドキュメントを参照してください。

> 以下の図は、Citrix Gateway を含む簡素化された Citrix 展開の例を示しています。Citrix Gateway は StoreFront と通信し、Citrix Virtual Apps and Desktops によって提供されるアプリとデータを保護します。ユーザーデバイスは Citrix Workspace™ アプリを実行して、安全な接続を作成し、アプリ、デスクトップ、ファイルにアクセスします。

Citrix Gateway を含む簡素化された Citrix 展開(/en-us/citrix-virtual-apps-desktops/2407/media/sample-deployment-overview.png)

ユーザーは Citrix Gateway を使用してログオンし、認証します。Citrix Gateway は DMZ に展開され、保護されています。2 要素認証が構成されています。ユーザー資格情報に基づいて、ユーザーには関連するリソースとアプリケーションが提供されます。アプリケーションとデータは適切な

サーバー上にあります（図には示されていません）。セキュリティ上機密性の高いアプリケーションとデータには、個別のサーバーが使用されます。

セキュリティに関する考慮事項とベストプラクティス

> **注:**
>
> 組織によっては、規制要件を満たすために特定のセキュリティ標準に準拠する必要がある場合があります。このようなセキュリティ標準は時間とともに変化するため、このドキュメントではこの主題については扱いません。セキュリティ標準とCitrix製品に関する最新情報については、Citrix Trust Centerを参照してください。

ファイアウォール

環境内のすべてのマシンを、必要に応じてエンクレーブ境界を含め、境界ファイアウォールで保護します。

環境内のすべてのマシンは、パーソナルファイアウォールによって保護されている必要があります。コアコンポーネントとVDAをインストールする際、Windowsファイアウォールサービスが検出された場合（ファイアウォールが有効になっていなくても）、コンポーネントと機能の通信に必要なポートを自動的に開くように選択できます。これらのファイアウォールポートを手動で構成することもできます。別のファイアウォールを使用する場合は、手動で構成する必要があります。必要なポートの詳細については、「技術文書：Citrixテクノロジーで使用される通信ポート」を参照してください。

従来の環境をこのリリースに移行する場合、既存の境界ファイアウォールの再配置や新しい境界ファイアウォールの追加が必要になる場合があります。たとえば、データセンター内の従来のクライアントとデータベースサーバーの間に境界ファイアウォールがあるとします。このリリースを使用する場合、その境界ファイアウォールは、仮想デスクトップとユーザーデバイスが一方にあり、データセンター内のデータベースサーバーとDelivery Controllerがもう一方にあるように配置する必要があります。したがって、データセンター内にデータベースサーバーとControllerを格納するエンクレーブを作成することを検討してください。また、ユーザーデバイスと仮想デスクトップ間の保護も検討してください。

> **注:**

> TCPポート1494と2598はICAとCGPに使用されるため、データセンター外のユーザーがアクセスできるようにファイアウォールで開かれている可能性が高いです。管理インターフェイスが誤って攻撃にさらされる可能性を避けるため、これらのポートを他の目的に使用しないことをCitrixは推奨します。ポート1494と2598は、Internet Assigned Number Authority (http://www.iana.org/) に正式に登録されています。

Delivery Controller™とのセキュアな通信

HTTPSを使用した通信の暗号化

StoreFrontとNetScaler Gatewayは、HTTPまたはHTTPSを介してデリバリーコントローラーで実行されているXMLサービスと通信します。構成によっては、VDAはWebSocketを使用してデリバリーコントローラーと通信する場合があります。HTTPSを有効にし、HTTPを無効にすることをお勧めします。これには、Delivery ControllerでHTTPSを有効にするを有効にする必要があります。

- HTTPSを使用して接続するようにStoreFrontを構成するには、「Citrix Desktops as a Service のリソースフィードを追加する」および「Citrix Gatewayアプライアンスを追加する」を参照してください。
- HTTPSを使用してDelivery Controllerに接続するようにNetScaler Gatewayを構成するには、「NetScaler GatewayでのSecure Ticket Authorityの構成」を参照してください。

あるいは、IPSecを使用してサーバー間の通信を保護するようにWindowsを構成することもできます。

セキュリティキー

承認されたStoreFrontサーバーとNetScalerサーバーのみがクラウドコネクタ経由でDaaSに接続できるように、セキュリティキーを使用できます。これは、XML信頼を有効にしている場合に特に重要です。

XML信頼

デフォルトでは、StoreFrontが列挙や起動などのアクションのためにデリバリーコントローラーに接続する場合、DaaSがユーザーを認証し、ユーザーのグループメンバーシップを確認できるように、StoreFrontはユーザーのActive Directory資格情報を渡す必要があります。ただし、ドメインパススルー、スマートカード、SAMLなどの他の認証方法を使用する場合、StoreFrontはActive Directoryパスワードを持っていません。この場合、「XML信頼」を有効にする必要があります。XML信頼が有効になっている場合、CVADはStoreFrontがユーザーのパスワードを検証することなく、アプリケーションの列挙や起動など、ユーザーに代わってアクションを実行することを許可します。XML信頼を有効にする前に、セキュリティキーまたはファイアウォールやIPsecなどの別の

メカニズムを使用して、信頼できるStoreFrontサーバーのみがデリバリーコントローラーに接続できるようにしてください。

XML信頼設定を確認、有効化、または無効化するには、Citrix Virtual Apps and Desktops PowerShell SDKを使用します。

- XML信頼設定の現在の値を確認するには、`Get-BrokerSite`を実行し、`TrustRequestsSentToTheXMLServicePort`の値を調べます。
- XML信頼を有効または無効にするには、パラメーター`TrustRequestsSentToTheXmlServicePort`を指定して`Set-BrokerSite`を実行します。

VDAとDelivery Controller間の通信

VDAがコントローラーと通信するためのメカニズムは2つあります。

- ウィンドウズ コミュニケーション ファンデーション

  Windows Communication Foundation (WCF) のメッセージレベル保護は、デリバリーコントローラーとVDA間の通信を保護します。これにより、TLSを使用した追加のトランスポートレベル保護の必要がなくなります。VDAとデリバリーコントローラー間の通信に使用されるデフォルトポートは80です。ただし、ポートをカスタマイズできます。詳細については、「VDAのカスタマイズ」を参照してください。

  WCFのメッセージセキュリティの詳細については、Microsoftドキュメントの「WCFのメッセージセキュリティ」を参照してください。

  WCF構成では、コントローラーとVDA間の相互認証にKerberosを使用します。暗号化には256ビットキーのCBCモードAESを使用します。メッセージの整合性にはSHA-1を使用します。

  Microsoftによると、WCFが使用するセキュリティプロトコルは、WS-SecurityPolicy 1.2を含むOASIS（Organization for the Advancement of Structured Information Standards）の標準に準拠しています。さらに、Microsoftは、WCFがSecurity Policy 1.2に記載されているすべてのアルゴリズムスイートをサポートしていると述べています。

  コントローラーとVDA間の通信にはbasic256アルゴリズムスイートが使用され、そのアルゴリズムは上記のとおりです。

  WCF構成では、メッセージレベルのセキュリティ暗号化とともにSOAP over HTTPプロトコルを使用します。

- WebSockets

これはWCFの最新の代替手段です。VDAからDelivery Controllerへの通信にはTLSポート443のみを使用するという利点があります。現在、MCSでプロビジョニングされたマシンでのみ利用可能です。詳細については、VDAとDelivery Controller間のWebSocket通信を参照してください。

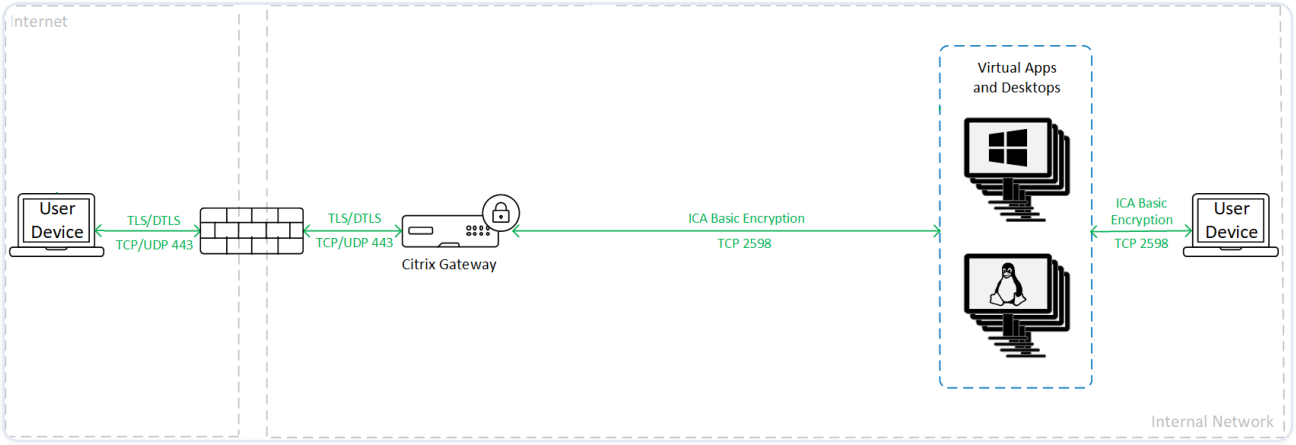
ICA®通信の保護

Citrix CVADは、クライアントとVDA間のICAトラフィックを保護するためのいくつかのオプションを提供します。利用可能なオプションは次のとおりです。

- **基本暗号化:** デフォルト設定です。
- **SecureICA:** RC5 (128ビット) 暗号化を使用してセッションデータを暗号化できます。
- **VDA TLS/DTLS:** TLS/DTLSを使用してネットワークレベルの暗号化を可能にします。

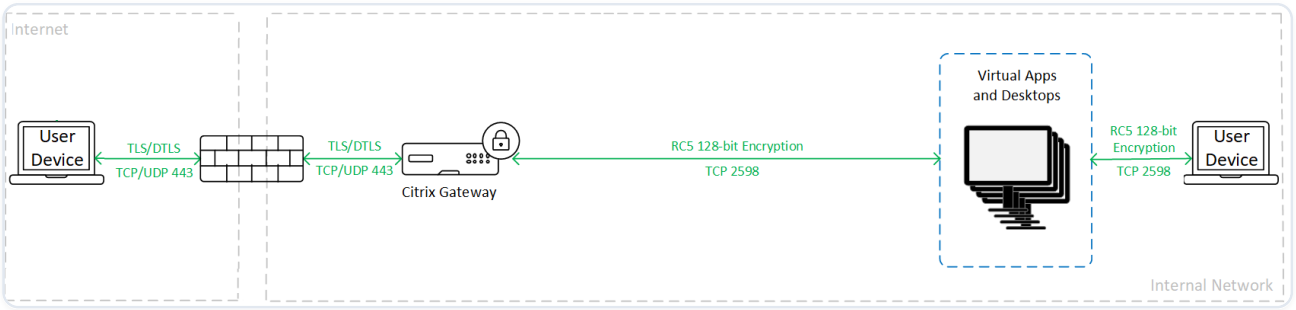
基本暗号化

基本暗号化を使用する場合、トラフィックは次の図に示すように暗号化されます。



SecureICA

SecureICAを使用する場合、トラフィックは次の図に示すように暗号化されます。



詳細については、セキュリティポリシー設定を参照してください。

> **注1:**

> Workspace app for HTML5を使用している場合、SecureICAはサポートされません。

> **注2:**
>
> Citrix SecureICAはICA/HDXプロトコルの一部ですが、Transport Layer Security (TLS) のような標準準拠のネットワークセキュリティプロトコルではありません。

VDA TLS/DTLS

VDA TLS/DTLS暗号化を使用する場合、トラフィックは次の図に示すように暗号化されます。

TLS/DTLS使用時のトラフィック暗号化(/en-us/citrix-virtual-apps-desktops/2407/media/vda-tls.png)

VDA TLS/DTLSを構成するには、VDA上のTLS設定を参照してください。

仮想チャネル

仮想チャネル許可リストを使用して、環境で許可されるCitrix以外の仮想チャネルを制御します。

印刷サーバーとの安全な通信

Virtual Delivery Agent (VDA) とUniversal Print Server間のTCPベースの接続にTLSを有効にできます。詳細については、Universal Print Server上のTransport Layer Security (TLS)を参照してください。

サイトデータベースとの安全な通信

サイトデータベースへのTLSを有効にする方法については、CTX137556を参照してください。

VDAマシンのセキュリティ

一般的な推奨事項

VDAが最新のオペレーティングセキュリティ更新プログラムとウイルス対策ソフトウェアで常に最新の状態に保たれていることを確認してください。

アプリケーションセキュリティ

非管理者ユーザーが悪意のある操作を実行するのを防ぐため、CitrixはVDAホスト上のインストーラー、アプリケーション、実行可能ファイル、およびスクリプトに対してWindows AppLockerルールを構成することを推奨します。

8.3形式のファイル名

VDAで8.3ファイル名を無効にできます。Microsoft fsutil documentationを参照してください。

データストレージに関する考慮事項

デスクトップ環境は、プールされたデスクトップや専用デスクトップなど、さまざまな種類のデスクトップで構成されている場合があります。ユーザーは、プールされたデスクトップなど、ユーザー間で共有されるデスクトップにデータを保存しないでください。ユーザーが専用デスクトップにデータを保存する場合、そのデスクトップが後で他のユーザーに利用可能になった場合は、そのデータを削除する必要があります。

ユーザーアカウント管理

アカウント管理にはWindowsのベストプラクティスを適用してください。Machine Creation ServicesまたはProvisioning Servicesによって複製される前に、テンプレートまたはイメージ上にアカウントを作成しないでください。保存された特権ドメインアカウントを使用してタスクをスケジュールしないでください。共有Active Directoryマシンアカウントを手動で作成しないでください。これらの慣行は、マシン攻撃がローカルの永続的なアカウントパスワードを取得し、それらを使用して他のユーザーに属するMCS/PVS共有イメージにログオンするのを防ぐのに役立ちます。

ユーザーには必要な機能のみを付与してください。Microsoft Windowsの特権は通常の方法でデスクトップに適用され続けます。つまり、ユーザー権利の割り当てを通じて特権を構成し、グループポリシーを通じてグループメンバーシップを構成します。このリリースの利点の1つは、デスクトップが保存されているコンピューターに対する物理的な制御を付与することなく、ユーザーにデスクトップへの管理者権限を付与できることです。

デスクトップの特権を計画する際は、以下に注意してください。

- デフォルトでは、非特権ユーザーがデスクトップに接続すると、自身のユーザーデバイスのタイムゾーンではなく、デスクトップを実行しているシステムのタイムゾーンが表示されます。デスクトップを使用する際にユーザーがローカル時間を確認できるようにする方法については、「デリバリーグループの管理」の記事を参照してください。
- デスクトップの管理者であるユーザーは、そのデスクトップを完全に制御できます。デスクトップが専用デスクトップではなくプールされたデスクトップである場合、そのユーザーは、

将来のユーザーを含む、そのデスクトップの他のすべてのユーザーに関して信頼できる必要があります。デスクトップのすべてのユーザーは、この状況によって引き起こされるデータセキュリティへの潜在的な永続的なリスクを認識する必要があります。この考慮事項は、単一のユーザーしか持たない専用デスクトップには適用されません。そのユーザーは、他のどのデスクトップでも管理者であってはなりません。

- デスクトップの管理者であるユーザーは、一般的に、悪意のあるソフトウェアを含むソフトウェアをそのデスクトップにインストールできます。また、ユーザーはデスクトップに接続されている任意のネットワーク上のトラフィックを監視または制御できる可能性もあります。

ログオン権限の管理

ログオン権限は、ユーザーアカウントとコンピューターアカウントの両方に必要です。Microsoft Windowsの特権と同様に、ログオン権限は通常の方法でデスクトップに適用され続けます。ログオン権限はユーザー権利の割り当てを通じて、グループメンバーシップはグループポリシーを通じて構成します。

Windowsのログオン権限は、ローカルでのログオン、リモートデスクトップサービス経由でのログオン、ネットワーク経由でのログオン（ネットワークからこのコンピューターにアクセス）、バッチジョブとしてのログオン、サービスとしてのログオンです。

コンピューターアカウントの場合、コンピューターには必要なログオン権限のみを付与します。「ネットワークからこのコンピューターにアクセス」のログオン権限は、デリバリーコントローラーのコンピューターアカウントに必要です。

ユーザーアカウントの場合、ユーザーには必要なログオン権限のみを付与します。

Microsoftによると、デフォルトでは、Remote Desktop Usersグループには「リモートデスクトップサービス経由でのログオンを許可」というログオン権限が付与されています（ドメインコントローラーを除く）。

組織のセキュリティポリシーによっては、このグループをそのログオン権限から削除するよう明示的に規定している場合があります。次のアプローチを検討してください。

- Multi-session OS 用のVirtual Delivery Agent (VDA) は、Microsoft Remote Desktop Servicesを使用します。Remote Desktop Usersグループを制限付きグループとして構成し、Active Directoryグループポリシーを介してグループのメンバーシップを制御できます。詳細については、Microsoftのドキュメントを参照してください。
- Single-session OS 用のVDAを含むCitrix Virtual Apps and Desktops™のその他のコンポーネントでは、Remote Desktop Usersグループは不要です。したがって、これらのコンポーネントの

場合、Remote Desktop Usersグループは「リモートデスクトップサービス経由でのログオンを許可」というログオン権限を必要としません。これを削除できます。さらに：

- リモートデスクトップサービスを介してこれらのコンピューターを管理する場合は、そのようなすべての管理者がすでにAdministratorsグループのメンバーであることを確認してください。
- リモートデスクトップサービスを介してこれらのコンピューターを管理しない場合は、これらのコンピューターでリモートデスクトップサービス自体を無効にすることを検討してください。

ユーザーとグループを「リモートデスクトップサービス経由でのログオンを拒否」というログオン権限に追加することは可能ですが、ログオン拒否権限の使用は一般的に推奨されません。詳細については、Microsoftのドキュメントを参照してください。

Delivery Controllerのセキュリティ

Delivery Controller上のWindowsサービス

Delivery Controllerのインストールにより、以下のWindowsサービスが作成されます。

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService): VMのMicrosoft Active Directoryコンピューターアカウントを管理します。
- Citrix Analytics (NT SERVICE\CitrixAnalytics): サイト管理者が承認した場合、Citrixが使用するためのサイト構成の使用状況情報を収集します。その後、この情報をCitrixに送信し、製品の改善に役立てます。
- Citrix App Library (NT SERVICE\CitrixAppLibrary): AppDiskの管理とプロビジョニング、AppDNA統合、およびApp-Vの管理をサポートします。
- Citrix Broker Service (NT SERVICE\CitrixBrokerService): ユーザーが利用できる仮想デスクトップまたはアプリケーションを選択します。
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging): 管理者がサイトに対して行ったすべての構成変更およびその他の状態変更を記録します。
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService): 共有構成のためのサイト全体のリポジトリ。
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin): 管理者に付与された権限を管理します。
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest): 他のDelivery Controllerサービスのセルフテストを管理します。

- Citrix Host Service (NT SERVICE\CitrixHostService): Citrix Virtual AppsまたはCitrix Virtual Desktopsの展開で使用されるハイパーバイザーインフラストラクチャに関する情報を保存し、また、コンソールがハイパーバイザープール内のリソースを列挙するために使用する機能も提供します。
- Citrix Machine Creation Services (NT SERVICE\CitrixMachineCreationService): デスクトップVMの作成をオーケストレーションします。
- Citrix Monitor Service (NT SERVICE\CitrixMonitor): Citrix Virtual AppsまたはCitrix Virtual Desktopsのメトリックを収集し、履歴情報を保存し、トラブルシューティングおよびレポートツール用のクエリインターフェイスを提供します。
- Citrix Storefront Service (NT SERVICE\ CitrixStorefront): StoreFrontの管理をサポートします。（StoreFrontコンポーネント自体の一部ではありません。）
- Citrix Storefront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService): StoreFrontの特権管理操作をサポートします。（StoreFrontコンポーネント自体の一部ではありません。）
- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService): メインサイトデータベースからローカルホストキャッシュに構成データを伝播します。
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService): メインサイトデータベースが利用できない場合に、ユーザーが利用できる仮想デスクトップまたはアプリケーションを選択します。

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これらは、他のCitrixコンポーネントと一緒にインストールされた場合にも作成されます。

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc): Citrixサポートが使用するための診断情報の収集をサポートします。
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService): Citrixによる分析のために診断情報を収集し、管理者が分析結果と推奨事項を表示してサイトの問題の診断に役立てられるようにします。

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これは現在使用されていません。有効になっている場合は、無効にしてください。

- Citrix リモート ブローカー プロバイダー (NT SERVICE\XaXdCloudProxy)

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これらは現在使用されていませんが、有効にする必要があります。無効にしないでください。

- Citrix オーケストレーション サービス (NT SERVICE\CitrixOrchestration)

- Citrix トラスト サービス (NT SERVICE\CitrixTrust)

Citrix Storefront™ Privileged Administration Serviceを除き、これらのサービスには「サービスとしてログオン」のログオン権限と、「プロセスのメモリクォータの調整」、「セキュリティ監査の生成」、「プロセスレベルトークンの置き換え」の特権が付与されています。これらのユーザー権限を変更する必要はありません。これらの特権はデリバリーコントローラーでは使用されず、自動的に無効になります。

Citrix Storefront Privileged AdministrationサービスとCitrix Telemetry Serviceを除き、上記のデリバリーコントローラーWindowsサービスはNETWORK SERVICE IDとしてログオンするように構成されています。これらのサービス設定を変更しないでください。

Citrix Config Synchronizer Service は、Delivery Controller 上のローカル管理者グループに NETWORK SERVICE アカウントが属している必要があります。これにより、ローカルホストキャッシュが正しく機能します。

Citrix Storefront Privileged Administrationサービスは、ローカルシステム (NT AUTHORITY\SYSTEM) としてログオンするように構成されています。これは、通常サービスでは利用できないDelivery Controller StoreFront操作 (Microsoft IISサイトの作成を含む) に必要です。そのサービス設定を変更しないでください。

Citrix Telemetry Service は、サービス固有の ID としてログオンするように構成されています。

Citrix Telemetryサービスは無効にできます。このサービスと、すでに無効になっているサービスを除き、これらのDelivery Controller Windowsサービスのいずれも無効にしないでください。

ログオン権限の管理

VDAsのコンピューターアカウントには、「ネットワークからこのコンピューターにアクセス」というログオン権限が必要です。(/ja-jp/advanced-concepts/implementation-guides/ad-ou-controller-discovery.html)を参照してください。

クライアントアクセス

クライアントアクセスは通常、(/ja-jp/storefront)を展開することで提供されます。StoreFrontのセキュリティ保護の詳細については、(/ja-jp/storefront/current-release/install-standard/secure)を参照してください。

リモートユーザーが StoreFront および VDA に安全に接続できるようにするには、NetScaler® Gateway を展開します。

Citrixでは、クライアントがCitrix Workspaceアプリを使用してStoreFrontに接続することを推奨しています。詳細については、各オペレーティングシステム用のCitrix Workspaceアプリの(/ja-jp/citrix-workspace-app.html)のセキュリティセクションを参照してください。または、ユーザーはWebブラウザーを使用してStoreFrontにアクセスすることもできます。

ユーザーがCitrix Workspace™アプリ以外のアプリケーションを実行する能力が制限されているシンクライアントをユーザーに提供することを検討してください。デバイスが組織によって管理されている場合は、オペレーティングシステムのセキュリティ更新プログラムとウイルス対策ソフトウェアの展開を確実にするためのポリシーを設定する必要があります。ただし、多くの場合、ユーザーは組織の管理外にある管理されていないデバイスから接続できる必要があります。次の機能の使用を検討してください。

- Endpoint Analysisは、エンドポイントをスキャンして、オペレーティングシステムやウイルス対策などのセキュリティ情報を確認し、セキュリティ要件を満たさないクライアントへのアクセスを拒否します。
- (/ja-jp/citrix-workspace-app/app-protection.html)は、キーロガーと画面キャプチャをブロックします。

混在バージョン環境

VDAのバージョンがDelivery Controllerと異なる場合など、混在バージョン環境は一部のアップグレード中に避けられません。ベストプラクティスに従い、異なるバージョンのCitrixコンポーネントが共存する時間を最小限に抑えてください。混在バージョン環境では、セキュリティポリシーなどが一貫して適用されない場合があります。

> **注:**
>
> これは他のソフトウェア製品にも共通しています。以前のバージョンのActive Directoryを使用すると、新しいバージョンのWindowsではグループポリシーが部分的にしか適用されません。

> 次のシナリオでは、特定の混在バージョンCitrix環境で発生する可能性のあるセキュリティ問題について説明します。Citrix Receiver 1.7を使用してXenAppおよびXenDesktop 7.6 Feature Pack 2のVDAを実行している仮想デスクトップに接続すると、サイトでポリシー設定**デスクトップとクライアント間のファイル転送を許可する**が有効になりますが、XenAppおよびXenDesktop 7.1を実行しているDelivery Controllerでは無効にできません。これは、製品の後のバージョンでリリースされたポリシー設定を認識しないためです。このポリシー設定により、ユーザーはファイルを仮想デスクトップにアップロードおよびダウンロードでき

るため、これがセキュリティ問題となります。これを回避するには、Delivery Controller（またはStudioのスタンドアロンインスタンス）をバージョン7.6 Feature Pack 2にアップグレードし、グループポリシーを使用してポリシー設定を無効にします。または、影響を受けるすべての仮想デスクトップでローカルポリシーを使用します。

Remote PC Accessのセキュリティに関する考慮事項

(/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/remote-pc-access.html)は、次のセキュリティ機能を実装しています。

- スマートカードの使用がサポートされています。
- リモートセッションが接続されると、オフィスPCのモニターは空白で表示されます。
- Remote PC Accessは、CTRL+ALT+DEL、USB対応スマートカード、生体認証デバイスを除くすべてのキーボードおよびマウス入力をリモートセッションにリダイレクトします。
- SmoothRoamingは単一ユーザーのみサポートされています。
- ユーザーがオフィスPCにリモートセッションを接続している場合、そのユーザーのみがオフィスPCへのローカルアクセスを再開できます。ローカルアクセスを再開するには、ユーザーはローカルPCでCtrl-Alt-Delを押し、リモートセッションで使用したのと同じ資格情報でログオンします。システムに適切なサードパーティのCredential Provider統合がある場合、ユーザーはスマートカードを挿入するか、生体認証を利用してローカルアクセスを再開することもできます。このデフォルトの動作は、グループポリシーオブジェクト（GPO）を介して高速ユーザー切り替えを有効にするか、レジストリを編集することで上書きできます。

注:

Citrixでは、VDA管理者権限を一般セッションユーザーに割り当てないことをお勧めします。

自動割り当て

デフォルトでは、Remote PC Accessは複数のユーザーのVDAへの自動割り当てをサポートしています。XenDesktop 5.6 Feature Pack 1では、管理者はRemotePCAccess.ps1 PowerShellスクリプトを使用してこの動作を上書きできました。このリリースでは、複数の自動リモートPC割り当てを許可または禁止するためにレジストリエントリを使用します。この設定はサイト全体に適用されます。

注意:

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

> 自動割り当てを単一ユーザーに制限するには：

サイト内の各コントローラーで、次のレジストリエントリを設定します。

```
HKEY_LOCAL_MACHINE\Software\Citrix|DesktopServer

Name: AllowMultipleRemotePCAssignments

Type: REG_DWORD

Data: 0 = Disable multiple user assignment, 1 = (Default) Enable multiple
user assignment.
```

既存のユーザー割り当てがある場合は、SDKコマンドを使用してそれらを削除し、VDAがその後単一の自動割り当ての対象となるようにします。

- VDAから割り当てられているすべてのユーザーを削除します: `$machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine`
- デリバリーグループからVDAを削除します: `$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`

物理的なオフィスPCを再起動します。

スマートカード

スマートカードおよび同等のテクノロジーは、この記事で説明されているガイドライン内でサポートされています。Citrix Virtual AppsまたはCitrix Virtual Desktops™でスマートカードを使用するには：

- スマートカードの使用に関する組織のセキュリティポリシーを理解してください。これらのポリシーには、たとえば、スマートカードの発行方法やユーザーがスマートカードを保護する方法が記載されている場合があります。これらのポリシーの一部は、Citrix Virtual Apps™またはCitrix Virtual Desktops環境で再評価する必要があるかもしれません。

- スマートカードで使用するユーザーデバイスの種類、オペレーティングシステム、および公開アプリケーションを決定します。
- スマートカードテクノロジーと、選択したスマートカードベンダーのハードウェアおよびソフトウェアについて理解を深めてください。
- 分散環境でデジタル証明書を展開する方法を理解してください。

注：

スマートカードの登録は、高速スマートカードではサポートされていません。高速スマートカードが無効になっている場合、スマートカードの登録は機能する可能性がありますが、スマートカードとミドルウェアの種類によって異なります。Citrix Virtual Apps and Desktopsとの統合および仮想セッションを介したスマートカード登録のサポートについては、スマートカードおよびミドルウェアベンダーにお問い合わせください。

スマートカードの種類

エンタープライズ用スマートカードとコンシューマー用スマートカードは、同じ寸法、電気コネクタを持ち、同じスマートカードリーダーに適合します。

エンタープライズ用スマートカードにはデジタル証明書が含まれています。これらのスマートカードはWindowsログオンをサポートし、ドキュメントやメールのデジタル署名および暗号化のためのアプリケーションでも使用できます。Citrix Virtual Apps and Desktops™はこれらの用途をサポートしています。

コンシューマー用スマートカードにはデジタル証明書は含まれていません。共有シークレットが含まれています。これらのスマートカードは、支払い（チップと署名、またはチップとPINのクレジットカードなど）をサポートできます。Windowsログオンや一般的なWindowsアプリケーションはサポートしていません。これらのスマートカードを使用するには、特殊なWindowsアプリケーションと適切なソフトウェアインフラストラクチャ（たとえば、決済カードネットワークへの接続を含む）が必要です。Citrix Virtual AppsまたはCitrix Virtual Desktopsでこれらの特殊なアプリケーションをサポートする方法については、Citrix担当者にお問い合わせください。

エンタープライズ用スマートカードには、同様の方法で使用できる互換性のある同等品があります。

- スマートカードと同等のUSBトークンは、USBポートに直接接続します。これらのUSBトークンは通常、USBフラッシュドライブと同じくらいのサイズですが、携帯電話で使用されるSIM

カードと同じくらい小さい場合もあります。これらは、スマートカードとUSBスマートカードリーダーの組み合わせとして表示されます。

- Windows Trusted Platform Module (TPM) を使用する仮想スマートカードは、スマートカードとして表示されます。これらの仮想スマートカードは、Citrix Workspace app (最小バージョンCitrix Receiver 4.3) を使用して、Windows 8およびWindows 10でサポートされています。
  - XenAppおよびXenDesktop 7.6 FP3より前のバージョンのCitrix Virtual Apps and Desktops（旧XenAppおよびXenDesktop）は、仮想スマートカードをサポートしていません。
  - 仮想スマートカードの詳細については、「仮想スマートカードの概要」を参照してください。

  注：「仮想スマートカード」という用語は、ユーザーコンピューターに保存されているデジタル証明書を指す場合もあります。これらのデジタル証明書は、厳密にはスマートカードと同等ではありません。

Citrix Virtual Apps and Desktopsのスマートカードサポートは、Microsoft Personal Computer/Smart Card (PC/SC) 標準仕様に基づいています。最低要件として、スマートカードおよびスマートカードデバイスは、基盤となるWindowsオペレーティングシステムによってサポートされ、Microsoft Windows Hardware Quality Labs (WHQL) によって承認されている必要があります。これにより、対象となるWindowsオペレーティングシステムを実行しているコンピューターで使用できます。ハードウェアのPC/SC準拠に関する追加情報については、Microsoftのドキュメントを参照してください。他の種類のユーザーデバイスもPS/SC標準に準拠している場合があります。詳細については、「Citrix Readyプログラム」を参照してください。

通常、各ベンダーのスマートカードまたは同等のものには、個別のデバイスドライバーが必要です。ただし、スマートカードがNIST Personal Identity Verification (PIV) 標準などの標準に準拠している場合、さまざまなスマートカードに単一のデバイスドライバーを使用できる可能性があります。デバイスドライバーは、ユーザーデバイスとVirtual Delivery Agent (VDA) の両方にインストールする必要があります。デバイスドライバーは、Citrixパートナーから入手できるスマートカードミドルウェアパッケージの一部として提供されることが多く、このスマートカードミドルウェアパッケージは高度な機能を提供します。デバイスドライバーは、Cryptographic Service Provider (CSP)、Key Storage Provider (KSP)、またはミニドライバーとも呼ばれることがあります。

Windowsシステム用の以下のスマートカードとミドルウェアの組み合わせは、Citrixによってそのタイプの代表的な例としてテストされています。ただし、他のスマートカードとミドルウェアも使用できます。Citrix互換のスマートカードとミドルウェアの詳細については、`<http://www.citrix.com/ready>`を参照してください。

ミドルウェア	対応カード
Gemalto .NETカード用ミニドライバー	ジェムアルト .NET v2+

その他の種類のデバイスでのスマートカードの使用に関する情報については、そのデバイス用のCitrix Workspace™アプリのドキュメントを参照してください。

リモートPCアクセス

スマートカードは、Windows 10、Windows 8、またはWindows 7を実行している物理的なオフィスPCへのリモートアクセスでのみサポートされます。

以下のスマートカードは、Remote PC Accessでテストされました。

ミドルウェア	対応カード
Gemalto .NETミニドライバー	ジェムアルト ドットネット v2以降

高速スマートカード

高速スマートカードは、既存のHDX PC/SCベースのスマートカードリダイレクトに対する改善点です。スマートカードが高遅延のWAN環境で使用される場合のパフォーマンスを向上させます。遅延が大きい場合、パフォーマンスの向上は顕著になります（例: Windows高速スマートカードログオンでは15秒、PC/SCベースのスマートカードリダイレクトでは1分以上かかるところが改善されます）。

高速スマートカードは、現在サポートされているWindows VDAを搭載したホストマシンでデフォルトで有効になっています。ホスト側で高速スマートカードを無効にするには（診断目的など）、'Disable Cryptographic Redirection' レジストリ設定をゼロ以外の値に設定します。

```
HKLM\SOFTWARE\Citrix\SmartCard

CryptographicRedirectionDisable (DWORD)
```

クライアント側で高速スマートカードを有効にするには、関連するStoreFrontサイトの *default.ica* ファイルにSmartCardCryptographicRedirection ICAパラメーターを含めます。

```
[WFClient]

SmartCardCryptographicRedirection=On
```

さらに、クライアント側では、高速スマートカードを強制的に有効または無効にすることができます（診断目的など）。以下のレジストリ設定を使用します。

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceEnableCryptographicRedirection (ゼロ以外のDWORDとして)

または

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceDisableCryptographicRedirection (ゼロ以外のDWORDとして)

クライアントマシンが64ビットの場合、32ビットレジストリハイブを指定する必要があります（`WOW6432Node`を使用）。

制限事項:

- Citrix Workspaceアプリ for Windowsのみが高速スマートカードをサポートします。default.icaファイルで高速スマートカードを設定した場合でも、Windows用ではないCitrix Workspaceアプリは、既存のPC/SCリダイレクトを使用します。
- 高速スマートカードがサポートする唯一のダブルホップシナリオは、両方のホップで高速スマートカードが有効になっているICA® > ICAです。高速スマートカードはICA > RDPダブルホップシナリオをサポートしないため、これらのシナリオは機能しません。
- 高速スマートカードはCryptography Next Generationをサポートしていません。したがって、高速スマートカードは楕円曲線暗号（ECC）スマートカードをサポートしていません。
- 高速スマートカードは読み取り専用のキーコンテナ操作のみをサポートしています。
- 高速スマートカードはスマートカードPINの変更をサポートしていません。

VDAバージョン2203およびWindows用Citrix Workspaceアプリバージョン2202（またはそれ以降）以降、高速スマートカードはCryptography Next Generation (CNG)と互換性があります。さらに、楕円曲線暗号（ECC）スマートカードは、ECDSAとECDHの両方で、P-256、P-384、P-521ビットの以下の曲線に対応しています。

VDAバージョン2203以降、高速スマートカードは、同じユーザーのログオンセッションからのアプリケーション間でスマートカードPINをキャッシュする機能を追加しました。たとえば、**セッションPINキャッシュ**が有効になっていて、エンドユーザーが以前にOutlookにスマートカードPINを提供していた場合、Wordでドキュメントに署名する際に、Wordはすでにキャッシュされているスマートカードpin（Outlookに送信されたもの）を使用します。**セッションPINキャッシュ**は、ユーザーがスマートカードPINを入力する回数を減らすことで、ユーザーエクスペリエンスを向上させます。さらに、スマートカードがVDAへのログオンに使用される場合、Windowsスマート

カードログオンPINをオプションで**セッションPINキャッシュ**に保存できます。これにより、ユーザーエクスペリエンスがさらに向上します。

セッションPINキャッシュはデフォルトで無効になっています。VDAで以下のレジストリ設定を使用して有効化および制御できます。

HKLM\SOFTWARE\Citrix\SmartCard内：

- `EnablePinSessionCache` をDWORDとして（有効にするにはゼロ以外）
- `EnableLogonPinSessionCache` をDWORDとして（有効にするにはゼロ以外）
- `PinSessionCacheEntryStaleTimeout` をDWORDとして（エントリが古くなるまでの秒数、デフォルトは1時間）

スマートカードリーダーの種類

スマートカードリーダーは、ユーザーデバイスに内蔵されている場合もあれば、ユーザーデバイスに別途接続されている場合もあります（通常はUSBまたはBluetooth経由）。USBチップ/スマートカードインターフェースデバイス（CCID）仕様に準拠する接触型カードリーダーがサポートされています。これらには、ユーザーがスマートカードを挿入するスロットまたはスワイプが含まれています。ドイツ信用経済（DK）標準は、接触型カードリーダーの4つのクラスを定義しています。

- クラス1スマートカードリーダーは最も一般的で、通常はスロットを備えています。クラス1スマートカードリーダーは、通常、オペレーティングシステムに付属の標準CCIDデバイスドライバーでサポートされています。
- クラス2スマートカードリーダーには、ユーザーデバイスからアクセスできないセキュアなキーパッドも含まれています。クラス2スマートカードリーダーは、統合されたセキュアなキーパッドを備えたキーボードに組み込まれている場合があります。クラス2スマートカードリーダーについては、Citrix担当者にお問い合わせください。セキュアなキーパッド機能を有効にするには、リーダー固有のデバイスドライバーが必要になる場合があります。
- クラス3スマートカードリーダーには、セキュアなディスプレイも含まれています。クラス3スマートカードリーダーはサポートされていません。
- クラス4スマートカードリーダーには、セキュアトランザクションモジュールも含まれています。クラス4スマートカードリーダーはサポートされていません。

> **注:**
>
> スマートカードリーダーのクラスは、USBデバイスクラスとは関係ありません。

> スマートカードリーダーは、対応するデバイスドライバーをインストールしてユーザーデバイスにインストールする必要があります。

サポートされているスマートカードリーダーについては、使用しているCitrix Workspaceアプリのドキュメントを参照してください。Citrix Workspaceアプリのドキュメントでは、サポートされているバージョンは、スマートカードに関する記事またはシステム要件に関する記事に記載されています。

ユーザーエクスペリエンス

スマートカードのサポートは、Citrix Virtual Apps and Desktopsに統合されており、特定のICA/HDXスマートカード仮想チャネルを使用します。これはデフォルトで有効になっています。

重要: スマートカードリーダーに汎用USBリダイレクトを使用しないでください。これはスマートカードリーダーではデフォルトで無効になっており、有効にしてもサポートされません。

同じユーザーデバイス上で複数のスマートカードと複数のリーダーを使用できますが、パススルー認証が使用されている場合は、ユーザーが仮想デスクトップまたはアプリケーションを起動するときに、スマートカードを1枚だけ挿入する必要があります。アプリケーション内でスマートカードを使用する場合（たとえば、デジタル署名や暗号化機能の場合）、スマートカードの挿入やPINの入力に関する追加のプロンプトが表示されることがあります。これは、複数のスマートカードが同時に挿入されている場合に発生する可能性があります。

- スマートカードがすでにリーダーに挿入されているにもかかわらず、スマートカードの挿入を促すプロンプトが表示された場合は、ユーザーはキャンセルを選択する必要があります。
- PINの入力を求められた場合は、ユーザーはPINを再度入力する必要があります。

カード管理システムまたはベンダーユーティリティを使用してPINをリセットできます。

> **重要:**

> Citrix Virtual AppsまたはCitrix Virtual Desktopsセッション内で、Microsoft Remote Desktop Connectionアプリケーションとスマートカードを使用することはサポートされていません。これは「ダブルホップ」の使用として説明されることがあります。

スマートカードを展開する前に

- スマートカードリーダー用のデバイスドライバーを入手し、ユーザーデバイスにインストールします。多くのスマートカードリーダーは、Microsoftが提供するCCIDデバイスドライバーを使用できます。
- スマートカードベンダーからデバイスドライバーと暗号サービスプロバイダー (CSP) ソフトウェアを入手し、ユーザーデバイスと仮想デスクトップの両方にインストールします。ドライバーとCSPソフトウェアは、Citrix Virtual Apps and Desktopsと互換性がある必要があります。互換性については、ベンダーのドキュメントを確認してください。ミニドライバーモデルをサポートおよび使用するスマートカードを使用する仮想デスクトップの場合、スマートカードミニドライバーは自動的にダウンロードされますが、http://catalog.update.microsoft.comまたはベンダーから入手することもできます。また、PKCS#11ミドルウェアが必要な場合は、カードベンダーから入手してください。
- 重要: Citrixでは、Citrixソフトウェアをインストールする前に、物理コンピューターにドライバーとCSPソフトウェアをインストールしてテストすることをお勧めします。
- Windows 10でInternet Explorerを使用してスマートカードを使用するユーザーのために、Citrix Receiver™ for WebのURLを信頼済みサイトリストに追加します。Windows 10では、信頼済みサイトの場合、Internet Explorerはデフォルトで保護モードで実行されません。
- 公開キーインフラストラクチャ (PKI) が適切に構成されていることを確認します。これには、Active Directory環境で証明書からアカウントへのマッピングが正しく構成されており、ユーザー証明書の検証が正常に実行できることを確認することが含まれます。
- 展開が、Citrix WorkspaceアプリやStoreFrontなど、スマートカードで使用される他のCitrixコンポーネントのシステム要件を満たしていることを確認します。
- サイト内の以下のサーバーへのアクセスを確保します。
    - スマートカード上のログオン証明書に関連付けられているユーザーアカウントのActive Directoryドメインコントローラー
    - デリバリーコントローラー™
    - シトリックス ストアフロント
    - シトリックス ゲートウェイ/シトリックス アクセス ゲートウェイ 10.x
    - VDA
    - (Remote PC Accessの場合オプション): Microsoft Exchange Server

スマートカードの使用を有効にする

手順1. カード発行ポリシーに従って、ユーザーにスマートカードを発行します。

ステップ 2. (オプション) ユーザーがRemote PC Access を利用できるようにスマートカードを設定します。

ステップ 3. スマートカードのリモート処理のために、Delivery Controller と StoreFront (まだインストールされていない場合) をインストールして構成します。

ステップ4. スマートカードの使用のために StoreFront を有効にします。詳細については、StoreFront ドキュメントの「スマートカード認証の構成」を参照してください。

ステップ5. スマートカードの使用のために Citrix Gateway/Access Gateway を有効にします。詳細については、NetScaler ドキュメントの「認証と承認の構成」および「Web Interface を使用したスマートカードアクセスの構成」を参照してください。

ステップ6. スマートカードの使用のために VDA を有効にします。

- VDA に必要なアプリケーションと更新プログラムがあることを確認します。
- ミドルウェアをインストールします。
- スマートカードのリモート処理を設定し、ユーザーデバイス上のCitrix Workspace アプリと仮想デスクトップセッション間のスマートカードデータの通信を有効にします。

ステップ7. スマートカードの使用のためにユーザーデバイス (ドメイン参加済みまたは非ドメイン参加済みのマシンを含む) を有効にします。詳細については、StoreFront ドキュメントの「スマートカード認証の構成」を参照してください。

- 証明機関のルート証明書と発行証明機関の証明書をデバイスのキーストアにインポートします。
- ベンダーのスマートカードミドルウェアをインストールします。
- Windows 用 Citrix Workspace アプリをインストールして構成します。その際、グループポリシー管理コンソールを使用して icaclient.adm をインポートし、スマートカード認証を有効にしてください。

ステップ 8. 展開をテストします。テストユーザーのスマートカードを使用して仮想デスクトップを起動し、展開が正しく構成されていることを確認します。可能なすべてのアクセスメカニズム（たとえば、Internet Explorer および Citrix Workspace アプリを介したデスクトップへのアクセス）をテストします。

スマートカードリーダーの挿入回数を追跡する

スマートカードのリモート処理を使用すると、SCardGetStatusChange 関数を使用して、スマートカードがリーダーに挿入または取り外された回数を追跡できます。この関数は、監視するリーダーごとに 1 つの SCARD_READERSTATE データ構造の配列を更新します。各

SCARD_READERSTATE の dwEventState フィールドのハイワード（16 ビット）には、リーダーのカウントが含まれています。詳細については、Microsoft の記事 SCardGetStatusChangeA function および SCARD_READERSTATEA structure を参照してください。

リーダー挿入回数レポート設定は、デフォルトで無効になっています。追跡を有効にするには、次のレジストリキーを追加します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

名前: EnableReaderInsertCountReporting

種類: DWORD

値: ゼロ以外の任意の値

セッションが切断されると、カウントはゼロにリセットされます。

リーダー挿入回数レポートは、サードパーティのスマートカードミドルウェアと互換性があります。

スマートカードの展開

この製品バージョンおよびこのバージョンを含む混在環境では、以下の種類のスマートカード展開がサポートされています。その他の構成は動作する可能性がありますが、サポートされていません。

種類	STOREFRONT™接続
ローカルのドメイン参加済みコンピューター	直接接続
ドメイン参加済みコンピューターからのリモートアクセス	Citrix Gateway経由で接続
ドメイン非参加コンピューター	直接接続
ドメイン非参加コンピューターからのリモートアクセス	Citrix Gateway経由で接続
Desktop Applianceサイトにアクセスするドメイン非参加コンピューターおよびシンクライアント	Desktop Applianceサイト経由で接続

種類	STOREFRONT™接続
XenApp® Services URL経由でStoreFrontにアクセスするドメイン参加済みコンピューターおよびシンクライアント	XenApp Services URL を介して接続

展開タイプは、スマートカードリーダーが接続されているユーザーデバイスの特性によって定義されます。

- デバイスがドメイン参加済みか、非ドメイン参加済みか。
- デバイスがStoreFrontにどのように接続されているか。
- 仮想デスクトップとアプリケーションを表示するためにどのソフトウェアが使用されているか。

さらに、Microsoft WordやMicrosoft Excelなどのスマートカード対応アプリケーションをこれらの展開で使用できます。これらのアプリケーションを使用すると、ユーザーはドキュメントにデジタル署名したり、暗号化したりできます。

バイモーダル認証

これらの展開のそれぞれで可能な場合、Receiverは、スマートカードの使用とユーザー名およびパスワードの入力のいずれかを選択できるようにすることで、バイモーダル認証をサポートします。これは、スマートカードが使用できない場合（たとえば、ユーザーが自宅に忘れた場合やログオン証明書の有効期限が切れた場合）に役立ちます。

非ドメイン参加デバイスのユーザーはReceiver for Windowsに直接ログオンするため、ユーザーが明示的な認証にフォールバックできるようにすることができます。バイモーダル認証を構成すると、ユーザーは最初にスマートカードとPINを使用してログオンするように求められますが、スマートカードに問題が発生した場合は明示的な認証を選択するオプションがあります。

Citrix Gatewayを展開する場合、ユーザーは自分のデバイスにログオンし、Receiver for WindowsによってCitrix Gatewayへの認証を求められます。これは、ドメイン参加済みデバイスと非ドメイン参加済みデバイスの両方に適用されます。ユーザーは、スマートカードとPIN、または明示的な資格情報のいずれかを使用してCitrix Gatewayにログオンできます。これにより、Citrix Gatewayログオンに対してバイモーダル認証をユーザーに提供できます。Citrix GatewayからStoreFrontへのパススルー認証を構成し、スマートカードユーザーの資格情報検証をCitrix Gatewayに委任することで、ユーザーはStoreFrontにサイレント認証されます。

複数のActive Directoryフォレストに関する考慮事項

Citrix環境では、スマートカードは単一のフォレスト内でサポートされます。フォレストをまたがるスマートカードログオンには、すべてのユーザーアカウントへの直接的な双方向フォレスト信頼が必要です。スマートカードを含むより複雑なマルチフォレスト展開（つまり、信頼が一方通行であるか、異なるタイプである場合）はサポートされていません。

リモートデスクトップを含むCitrix環境でスマートカードを使用できます。この機能は、ローカル（スマートカードが接続されているユーザーデバイス上）またはリモート（ユーザーデバイスが接続するリモートデスクトップ上）にインストールできます。

スマートカード取り外しポリシー

製品に設定されているスマートカード取り外しポリシーは、セッション中にリーダーからスマートカードを取り外した場合に何が起こるかを決定します。スマートカード取り外しポリシーは、Windowsオペレーティングシステムを介して構成および処理されます。

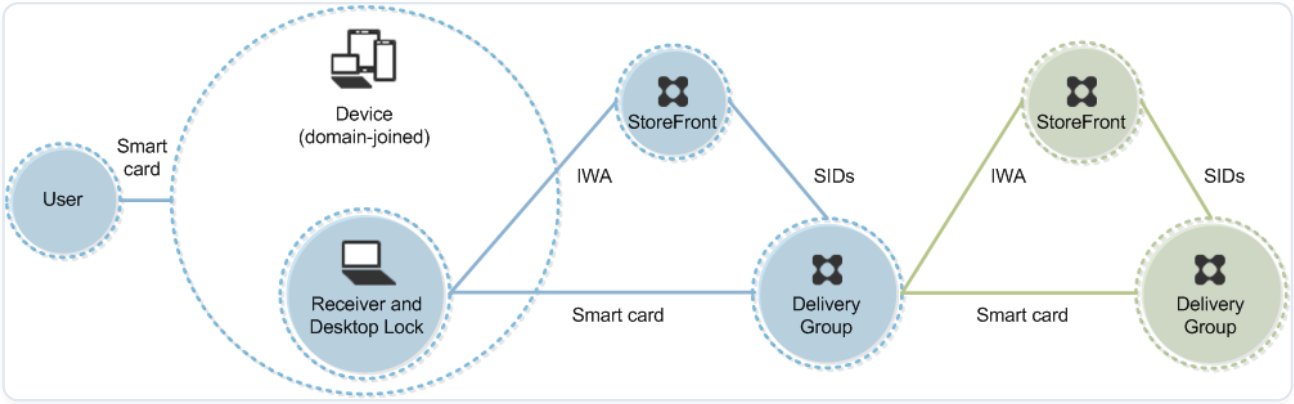
ポリシー設定	デスクトップの動作
何もしない	何もしません。
ワークステーションをロックする	デスクトップセッションは切断され、仮想デスクトップはロックされます。
強制ログオフ	ユーザーは強制的にログオフされます。ネットワーク接続が失われ、この設定が有効になっている場合、セッションがログオフされ、ユーザーはデータを失う可能性があります。
リモートターミナルサービスセッションの場合に切断する	セッションは切断され、仮想デスクトップはロックされます。

証明書失効チェック

証明書失効チェックが有効になっており、ユーザーが無効な証明書を含むスマートカードをカードリーダーに挿入した場合、ユーザーは認証できず、証明書に関連するデスクトップまたはアプリケーションにアクセスできません。たとえば、無効な証明書がメールの復号化に使用された場合、メールは暗号化されたままになります。認証に使用されるものなど、カード上の他の証明書がまだ有効な場合、それらの機能はアクティブなままです。

展開例：ドメイン参加済みコンピューター

この展開では、Desktop Viewer を実行し、StoreFront に直接接続するドメイン参加済みユーザーデバイスが使用されます。



ユーザーはスマートカードとPINを使用してデバイスにログオンします。Receiver は、統合Windows認証 (IWA) を使用してユーザーをStoreFrontサーバーに認証します。StoreFront は、ユーザーセキュリティ識別子 (SID) を Citrix Virtual Apps または Citrix Virtual Desktops に渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、Receiver でシングルサインオン機能が構成されているため、PIN の再入力を求められることはありません。

この展開は、2つ目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2つ目のStoreFrontサーバーに認証します。この2つ目の接続には、任意の認証方法を使用できます。最初のホップに示されている構成は、2つ目のホップで再利用することも、2つ目のホップでのみ使用することもできます。

展開例: ドメイン参加済みコンピューターからのリモートアクセス

この展開では、Desktop Viewer を実行し、Citrix Gateway/Access Gateway を介して StoreFront に接続するドメイン参加済みユーザーデバイスが関与します。

展開例: ドメイン参加済みコンピューターからのリモートアクセス(/en-us/citrix-virtual-apps-desktops/2407/media/smartcard2_1.png)

ユーザーはスマートカードとPINを使用してデバイスにログオンし、その後Citrix Gateway/Access Gatewayに再度ログオンします。この展開ではReceiverがバイモーダル認証を許可しているため、この2回目のログオンはスマートカードとPIN、またはユーザー名とパスワードのいずれかを使用できます。

ユーザーはStoreFrontに自動的にログオンし、StoreFrontはユーザーセキュリティ識別子 (SID) をCitrix Virtual Apps™またはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたは

アプリケーションを起動すると、Receiverでシングルサインオン機能が構成されているため、PINの再入力を求められることはありません。

この展開は、2つ目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2つ目のStoreFrontサーバーに認証します。この2つ目の接続には、任意の認証方法を使用できます。最初のホップに示されている構成は、2つ目のホップで再利用することも、2つ目のホップでのみ使用することもできます。

展開例：ドメイン非参加コンピューター

この展開では、Desktop Viewerを実行し、StoreFrontに直接接続するドメイン非参加ユーザーデバイスが使用されます。

展開例：ドメイン非参加コンピューター(/en-us/citrix-virtual-apps-desktops/2407/media/smartcard3_1.png)

ユーザーはデバイスにログオンします。通常、ユーザーはユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンの資格情報はオプションです。この展開ではバイモーダル認証が可能であるため、Receiverはユーザーにスマートカードと PIN、またはユーザー名とパスワードのいずれかを要求します。その後、ReceiverはStoreFrontに認証します。

StoreFrontは、ユーザーセキュリティ識別子 (SID) をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、この展開ではシングルサインオン機能が利用できないため、PINの再入力を求められます。

この展開は、2つ目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2つ目のStoreFrontサーバーに認証します。この2つ目の接続には、任意の認証方法を使用できます。最初のホップに示されている構成は、2つ目のホップで再利用することも、2つ目のホップでのみ使用することもできます。

展開例：ドメイン非参加コンピューターからのリモートアクセス

この展開では、Desktop Viewerを実行し、StoreFrontに直接接続するドメインに参加していないユーザーデバイスが使用されます。

展開例：ドメインに参加していないコンピューターからのリモートアクセス(/en-us/citrix-virtual-apps-desktops/2407/media/smartcard4_1.png)

ユーザーはデバイスにログオンします。通常、ユーザーはユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンの資格情報はオプションです。この展開ではバイモーダル認証が可能なため、Receiverはスマートカードと PIN、またはユーザー名とパスワードのいずれかをユーザーに要求します。その後、ReceiverはStoreFrontに対して認証を行います。

StoreFrontは、ユーザーセキュリティ識別子（SID）をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。この展開ではシングルサインオン機能が利用できないため、ユーザーが仮想デスクトップまたはアプリケーションを起動すると、PINの入力を再度求められます。

この展開は、2台目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2台目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示された構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: ドメイン非参加コンピューター

この展開では、Desktop Viewer を実行し、StoreFront に直接接続するドメイン非参加ユーザーデバイスが関与します。

展開例: ドメイン非参加コンピューター(/en-us/citrix-virtual-apps-desktops/2407/media/smartcard3_1.png)

ユーザーはデバイスにログオンします。通常、ユーザーはユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンの資格情報はオプションです。この展開ではバイモーダル認証が可能であるため、Receiverはユーザーにスマートカードと PIN、またはユーザー名とパスワードのいずれかを要求します。その後、ReceiverはStorefrontに対して認証を行います。

StoreFrontはユーザーセキュリティ識別子（SID）をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、この展開ではシングルサインオン機能が利用できないため、PINの再入力を求められます。

この展開は、2台目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2台目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示された構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: ドメイン非参加コンピューターからのリモートアクセス

この展開では、Desktop Viewer を実行し、StoreFront に直接接続するドメイン非参加ユーザーデバイスが関与します。

展開例: ドメイン非参加コンピューターからのリモートアクセス(/en-us/citrix-virtual-apps-desktops/2407/media/smartcard4_1.png)

ユーザーがデバイスにログオンします。通常、ユーザーはユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンの資格情報はオプションです。この展開ではバイモーダル認証が可能なため、ReceiverはスマートカードとPIN、またはユーザー名とパスワードのいずれかをユーザーに要求します。その後、ReceiverはStorefrontに対して認証を行います。

StoreFrontはユーザーセキュリティ識別子（SID）をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、この展開ではシングルサインオン機能が利用できないため、ユーザーは再度PINを要求されます。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップに示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例：ドメインに参加していないコンピューターとシンクライアントがDesktop Applianceサイトにアクセスする場合

この展開では、Desktop Lockを実行し、Desktop Applianceサイトを介してStoreFrontに接続する可能性のある、ドメインに参加していないユーザーデバイスが使用されます。

Desktop Lockは、Citrix Virtual Apps、Citrix Virtual Desktops、およびVDI-in-a-Boxとともにリリースされる個別のコンポーネントです。これはDesktop Viewerの代替であり、主に再利用されたWindowsコンピューターとWindowsシンクライアント向けに設計されています。Desktop Lockは、これらのユーザーデバイスのWindowsシェルとタスクマネージャーを置き換え、ユーザーが基になるデバイスにアクセスするのを防ぎます。Desktop Lockを使用すると、ユーザーはWindows Server MachineデスクトップとWindows Desktop Machineデスクトップにアクセスできます。Desktop Lockのインストールはオプションです。

展開例：ドメインに参加していないコンピューターとシンクライアントがDesktop Applianceサイトにアクセスする場合(/en-us/citrix-virtual-apps-desktops/2407/media/smartcard5_1.png)

ユーザーはスマートカードを使用してデバイスにログオンします。デバイスでDesktop Lockが実行されている場合、デバイスはキオスクモードで実行されているInternet Explorerを介してDesktop Applianceサイトを起動するように構成されます。サイト上のActiveXコントロールは、ユーザーにPINを要求し、それをStoreFrontに送信します。StoreFrontは、ユーザーセキュリティ識別子（SID）をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。割り当てられたデスクトップグループのアルファベット順リストで最初に利用可能なデスクトップが起動します。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップに示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例：ドメインに参加しているコンピューターとシンクライアントがXenApp Services URLを介してStoreFrontにアクセスする場合

この展開では、Desktop Lockを実行し、XenApp Services URLを介してStoreFrontに接続するドメインに参加しているユーザーデバイスが使用されます。

Desktop Lockは、Citrix Virtual Apps、Citrix Virtual Desktops、およびVDI-in-a-Boxとともにリリースされる個別のコンポーネントです。これはDesktop Viewerの代替であり、主に再利用されたWindowsコンピューターとWindowsシンクライアント向けに設計されています。Desktop Lockは、これらのユーザーデバイスのWindowsシェルとタスクマネージャーを置き換え、ユーザーが基になるデバイスにアクセスするのを防ぎます。Desktop Lockを使用すると、ユーザーはWindows Server MachineデスクトップとWindows Desktop Machineデスクトップにアクセスできます。Desktop Lockのインストールはオプションです。

展開例：ドメインに参加しているコンピューターとシンクライアントがXenApp Services URLを介してStoreFrontにアクセスする場合(/en-us/citrix-virtual-apps-desktops/2407/media/smartcard6.png)

ユーザーはスマートカードとPINを使用してデバイスにログオンします。デバイスでDesktop Lockが実行されている場合、統合Windows認証 (IWA) を使用してユーザーをStoreFrontサーバーに認証します。StoreFrontは、ユーザーセキュリティ識別子 (SID) をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップを起動すると、シングルサインオン機能がReceiverで構成されているため、PINの再入力を求められることはありません。

この展開は、2つ目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2つ目のStoreFrontサーバーに対して認証を行います。この2つ目の接続には、任意の認証方法を使用できます。最初

のホップで示された構成は、2つ目のホップで再利用することも、2つ目のホップでのみ使用することもできます。

スマートカードによるパススルー認証とシングルサインオン

パススルー認証

スマートカードによる仮想デスクトップへのパススルー認証は、Windows 10、Windows 8、Windows 7 SP1 EnterpriseおよびProfessional Editionを実行しているユーザーデバイスでサポートされています。

スマートカードによるホスト型アプリケーションへのパススルー認証は、Windows Server 2012およびWindows Server 2008 R2 SP1を実行しているサーバーでサポートされています。

スマートカードホスト型アプリケーションでパススルー認証を使用するには、サイトの認証方法として「スマートカードによるパススルー」を構成する際に、Kerberosの使用を有効にしてください。

注：スマートカードによるパススルー認証の利用可能性は、以下を含む（ただしこれらに限定されない）多くの要因に依存します。

- パススルー認証に関する組織のセキュリティポリシー。
- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアのPINキャッシュポリシー。

スマートカードによるパススルー認証は、Citrix StoreFrontで構成されます。詳細については、StoreFrontのドキュメントを参照してください。

シングルサインオン

シングルサインオンは、仮想デスクトップおよびアプリケーションの起動時にパススルー認証を実装するCitrixの機能です。この機能は、ドメイン参加済み、StoreFrontへの直接接続、およびドメイン参加済み、NetScalerからStoreFrontへのスマートカード展開で使用でき、ユーザーがPINを入力する回数を減らすことができます。これらの展開タイプでシングルサインオンを使用するには、StoreFrontサーバーにあるdefault.icaファイルで以下のパラメーターを編集します。

- ドメイン参加済み、StoreFrontへの直接接続スマートカード展開 — DisableCtrlAltDelをOffに設定
- ドメイン参加済み、NetScalerからStoreFrontへのスマートカード展開 — UseLocalUserAndPasswordをOnに設定

これらのパラメーターの設定に関する詳細な手順については、StoreFrontまたはCitrix Gatewayのドキュメントを参照してください。

シングルサインオン機能の利用可否は、以下を含む多くの要因に依存します（ただし、これらに限定されません）。

- シングルサインオンに関する組織のセキュリティポリシー。
- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアのPINキャッシュポリシー。

> **注:**
>
> ユーザーがスマートカードリーダーが接続されたマシン上のVirtual Delivery Agent (VDA) にログオンすると、スマートカードやパスワードなど、以前に成功した認証モードを表すWindowsタイルが表示されることがあります。その結果、シングルサインオンが有効になっている場合、シングルサインオンタイルが表示されることがあります。ログオンするには、シングルサインオンタイルは機能しないため、ユーザーは別のタイルを選択するために**ユーザーの切り替え**を選択する必要があります。

Delivery Controllers で TLS を有効にする

delivery controller™ で TLS を有効にするには、次の手順を実行する必要があります。

- すべての Delivery Controller にサーバー証明書を取得、インストール、および登録します。詳細については、「証明書の要求とインストール」を参照してください。
- TLS 証明書を使用してポートを構成します。詳細については、「証明書の要求とインストール」を参照してください。
- HTTPを無効にしてHTTPSトラフィックを強制します。詳細については、「HTTPSトラフィックのみを強制する」を参照してください。
- オプションで、Controller が HTTP および HTTPS トラフィックをリッスンするために使用するポートを変更できます。詳細については、「HTTP または HTTPS ポートの変更」を参照してください。

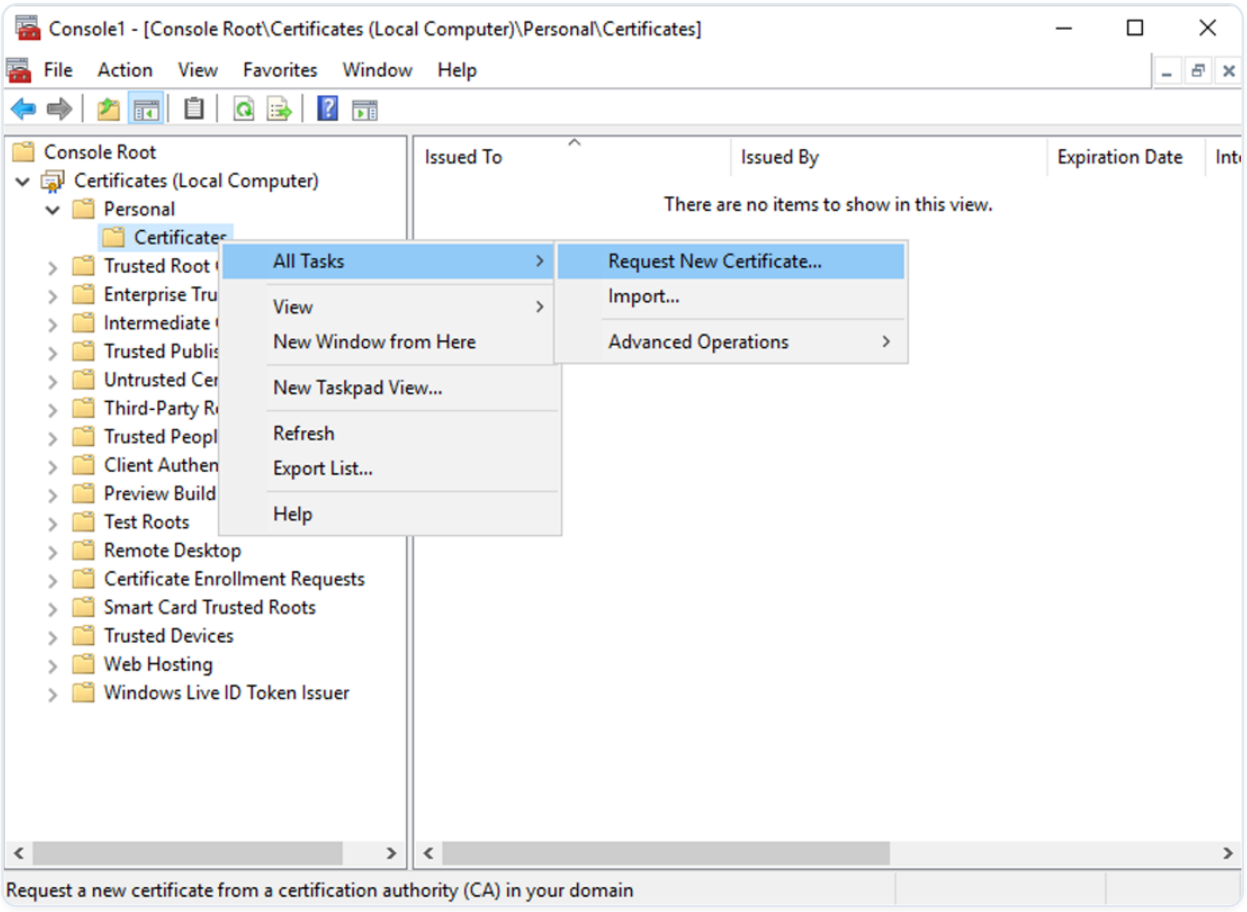
証明書の要求とインストール

TLSを使用するには、代替名にDDCのFQDNが含まれる証明書をインストールする必要があります。適切な証明書を作成する必要があります。これは、Microsoft証明機関またはその他の内部または外部の証明機関を使用して行うことができます。

Microsoft 証明機関を使用して証明書を作成する

Microsoft 証明機関が Active Directory ドメインまたは Delivery Controller が参加している信頼されたフォレストに統合されている場合、証明書 MMC スナップインの証明書登録ウィザードから証明書を取得できます。Microsoft 証明機関は、Web サーバーでの使用に適した証明書テンプレートを公開している必要があります。別のドメインで Citrix Gateway または StoreFront™ サーバーを使用している場合は、ルート証明機関証明書をエクスポートし、Citrix Gateway および StoreFront にインポートする必要があります。

1. Delivery Controller で、MMC コンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、 を選択します。
2. **個人 > 証明書** を展開し、**すべてのタスク > 新しい証明書の要求** コンテキストメニューコマンドを使用します。



3. 開始するには **次へ** をクリックし、Active Directory 登録から証明書を取得することを確認するには **次へ** をクリックします。

4. **Web Server Exportable** などの適切なテンプレートを選択します。テンプレートが Subject の値を自動的に提供するように設定されている場合は、詳細を提供せずに **登録** をクリックできます。

   「証明書を要求」ダイアログ(/en-us/citrix-virtual-apps-desktops/2407/media/tls-request-certificates.png)

5. 証明書テンプレートの詳細を指定するには、**詳細**の矢印ボタンをクリックして、以下を構成します。

   サブジェクト名: 共通名を選択し、Delivery Controller の FQDN を追加します。

   代替名: DNS を選択し、Delivery Controller の FQDN を追加します。

   証明書のプロパティ(/en-us/citrix-virtual-apps-desktops/2407/media/tls-certificate-properties.png)

6. **OK** を押します。
7. **登録** を押して証明書を作成およびインストールします。

既存の証明書ファイルをインストールする

ファイルとして既存の証明書がある場合は、それをインストールできます。

1. Delivery Controllerで、MMCコンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、コンピューターアカウントを選択します。
2. **個人 > 証明書** を展開し、**すべてのタスク > インポート** のコンテキストメニューコマンドを使用します。
3. 証明書ファイルを参照します。

SSL/TLS リスナーポートの構成

Web Studio および Director の一部としてインストールされている IIS Windows コンポーネントが同じサーバーにインストールされている場合は、IIS を使用して TLS を構成できます。詳細については、「Web Studio および Director で TLS を有効にする」を参照してください。それ以外の場合は、PowerShell を使用して証明書を構成します。

1. 既存の証明書がバインドされているかを確認するには、コマンドプロンプトを開き、`netsh http show sslcert` を実行します。

   ```
   netsh http show sslcert
   ```

2. 既存のバインドがある場合は、それを削除します。

```
netsh http delete sslcert ipport=0.0.0.0:443
```

既存のバインドで特定の IP アドレスとポートが指定されていた場合は、`0.0.0.0:443` をその IP アドレスとポートに置き換えます。

3. 以前にインストールした証明書のサムプリントを見つけます。サムプリントを表示するには、**コンピューター証明書の管理**を開き、証明書を参照して開き、**詳細**タブに移動します。

サムプリントを示す証明書のプロパティのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2411/media/certificate-thumbprint.png)

または、PowerShellを使用することもできます。たとえば、次のスクリプトは、共通名がサーバーのホスト名と一致する証明書を検索し、サムプリントを出力します。

```
$HostName =
([System.Net.Dns]::GetHostByName(($env:computerName))).Hostname

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.Subject -match ("CN=" + $HostName)}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $
($Thumbprint)" -Foreground Yellow
```

証明書の共通名がホスト名と一致しない場合、これは失敗します。ホスト名に対して複数の証明書がある場合、これは連結された複数のサムプリントを返し、適切なサムプリントを選択する必要があります。

次の例では、フレンドリ名で証明書を検索します。

```
$friendlyName = "My certificate name"

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.FriendlyName -eq $friendlyNam}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $friendlyName: $
($Thumbprint)" -Foreground Yellow
```

指定されたフレンドリ名を持つ証明書が複数ある場合、これは連結された複数のサムプリントを返し、適切なサムプリントを選択する必要があります。

4. 証明書をポートにバインドするには、`netsh http add sslcert`コマンドを使用します。

```
netsh http add sslcert ipport=[IP address]:443 certhash=[certificate
hash] appid=[application GUID] disablelegacytls=enable
```

- `ipport`: IPアドレスとポート。0.0.0.0:443を使用すると、すべてのIPアドレスに適用されます。代わりに、特定のIPアドレスを指定することもできます。
- `certhash`: 前の手順で特定した証明書のサムプリント。
- `appid`: シトリックス ブローカー サービス の GUID。

> **注:**
>
> 証明書を更新または再バインドする際は、任意のGUIDではなく、Broker Serviceに関連付けられた特定の`appid`を使用してください。
>
> Citrix Broker Serviceの正しい`appid`を見つけるには：

a. 管理者としてPowerShellコマンドウィンドウを開き、次のコマンドを実行します。

```
Get-WmiObject -Class Win32_Product | Select-String -Pattern
"broker"
```

b. 出力でCitrix Broker ServiceのIdentifyingNumber (GUID) を見つけます（例：`{D333C884-187F-447C-8C67-463F33989C8F}`）。このGUIDを`appid`パラメーターに使用します。

- `disablelegacytls=enable`: レガシーバージョンのTLSを無効にします。このパラメーターはWindows 2022以降で利用可能です。Windows 2022ではTLS 1.0と1.1を無効にします。Windows 2025では、TLS 1.0と1.1がデフォルトで無効になっているため、これは不要です。

例えば、すべてのIPアドレスで、サムプリント`bc96f958848639fd101a793b87915d5f2829b0b6`の証明書をポート`443`にバインドするには、次のコマンドを実行します。

```
netsh http add sslcert ipport=0.0.0.0:443
certhash=bc96f958848639fd101a793b87915d5f2829b0b6 appid={91fe7386-
e0c2-471b-a252-1e0a805febac} disablelegacytls=enable
```

HTTPSが有効になったら、デリバリーコントローラーへの接続にHTTPではなくHTTPSを使用するように、StoreFront展開 とNetscaler Gatewayを構成する必要があります。

暗号スイートを構成する

暗号スイートの順序リストには、`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` または `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` の暗号スイート（またはその両方）を含める必要があります。また、これらの暗号スイートは、`TLS_DHE_` の暗号スイートよりも前に配置する必要があります。

1. Microsoftグループポリシーエディターを使用して、**コンピューターの構成 > 管理用テンプレート > ネットワーク > SSL構成設定**に移動します。
2. 「SSL暗号スイートの順序」ポリシーを編集します。デフォルトでは、このポリシーは「未構成」に設定されています。このポリシーを「有効」に設定します。
3. スイートを正しい順序に並べ替えます。使用したくない暗号スイートは削除します。

`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` または `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` のいずれかが、`TLS_DHE_` の暗号スイートよりも前に配置されていることを確認してください。

Microsoft Learn で、TLS 暗号スイートの順序の構成 も参照してください。

HTTPS トラフィックのみを強制する

XML Service が HTTP トラフィックを無視するように構成することをお勧めします。

1. `regedit` を実行します。
2. HKLM\Software\Citrix\DesktopServer\ を開きます。
3. 名前が `XmlServicesEnableNonSsl` の新しいDWORD値を作成し、0に設定します。
4. Broker Serviceを再起動します。

HTTPSトラフィックを無視するために作成できる、対応するレジストリDWORD値 `XmlServicesEnableSsl` があります。それが0に設定されていないことを確認してください。

HTTPまたはHTTPSポートの変更

デフォルトでは、Controller上のXMLサービスは、HTTPトラフィックにはポート80を、HTTPSトラフィックにはポート443をリッスンします。デフォルト以外のポートを使用することもできますが、Controllerを信頼されていないネットワークに公開することによるセキュリティリスクに注意してください。デフォルトを変更するよりも、スタンドアロンのStoreFrontサーバーを展開する方が望ましいです。

Controllerで使用されるデフォルトのHTTPまたはHTTPSポートを変更するには、Studioから次のコマンドを実行します。

```
BrokerService.exe -StoreFrontPort <http-port> -StoreFrontTlsPort <https-port>
```

ここで、`<http-port>` はHTTPトラフィックのポート番号であり、`<https-port>` はHTTPSトラフィックのポート番号です。

> **注:**
>
> ポートを変更した後、Studioはライセンスの互換性とアップグレードに関するメッセージを表示する場合があります。この問題を解決するには、次のPowerShellコマンドレットシーケンスを使用してサービスインスタンスを再登録します。

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS
|

Unregister-ConfigRegisteredServiceInstance

Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |

Register-ConfigServiceInstance
```

VDAsでTLSを有効にする

Citrix Workspace™ appとVirtual Delivery Agents (VDAs)間のTLS接続を有効にするには、以下のタスクを完了します。

- VDAsに証明書をインストールします。詳細については、証明書のリクエストとインストールを参照してください。

- VDAsがインストールされているマシンでTLSを構成します。(便宜上、VDAsがインストールされているマシンは、以降「VDA」と表記します。) TLS/DTLSの構成には、Citrixが提供するPowerShellスクリプトを使用することを強くお勧めします。詳細については、PowerShellスクリプトを使用してVDAでTLSを構成するを参照してください。ただし、TLS/DTLSを手動で構成する場合は、VDAでTLSを手動で構成するを参照してください。
- Studioで一連のPowerShellコマンドレットを実行して、VDAsを含むデリバリーグループでTLSを構成します。詳細については、デリバリーグループでTLSを構成するを参照してください。

要件と考慮事項:

- コンポーネントのインストール、サイトの作成、マシンカタログの作成、デリバリーグループの作成を行った後、デリバリーグループとVDAsでTLSを構成します。
- デリバリーグループでTLSを構成するには、コントローラーアクセスルールを変更する権限が必要です。フル管理者にはこの権限があります。
- VDAsでTLSを構成するには、VDAがインストールされているマシンでWindows管理者である必要があります。
- Machine Creation Services™またはProvisioning ServicesによってプロビジョニングされたプールされたVDAでは、再起動時にVDAマシンイメージがリセットされ、以前のTLS設定が失われます。VDAが再起動されるたびにPowerShellスクリプトを実行して、TLS設定を再構成してください。

デリバリーグループには、TLSが構成されているVDAとTLSが構成されていないVDAが混在することはできません。デリバリーグループのTLSを構成する前に、そのデリバリーグループ内のすべてのVDAに対してTLSがすでに構成されていることを確認してください。

VDAsでTLSを構成すると、インストールされているTLS証明書の権限が変更され、ICA® Serviceに証明書の秘密キーへの読み取りアクセス権が付与され、ICA Serviceに以下の情報が通知されます。

- TLSに使用する証明書ストア内の証明書。
- TLS接続に使用するTCPポート番号。

  Windowsファイアウォール (有効な場合) は、このTCPポートでの受信接続を許可するように構成する必要があります。この構成は、PowerShellスクリプトを使用すると自動的に行われます。
- 許可するTLSプロトコルのバージョン。

> **重要:**

> CitrixではTLS 1.2以降の使用を推奨しています。SSLおよびそれ以前のバージョンのTLSは非推奨です。

> サポートされているTLSプロトコルバージョンは、階層（最低から最高）に従います: SSL 3.0、TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3。許可される最小バージョンを指定します。そのバージョンまたはそれより高いバージョンを使用するすべてのプロトコル接続が許可されます。

たとえば、TLS 1.1を最小バージョンとして指定した場合、TLS 1.1、TLS 1.2、TLS 1.3プロトコル接続が許可されます。SSL 3.0を最小バージョンとして指定した場合、サポートされているすべてのバージョンの接続が許可されます。TLS 1.3を最小バージョンとして指定した場合、TLS 1.3接続のみが許可されます。

- 許可するTLS暗号スイート。

  暗号スイートは、接続に使用される暗号化を選択します。クライアントとVDAは、異なる暗号スイートのセットをサポートできます。クライアント（Citrix Workspaceアプリ）が接続してサポートされているTLS暗号スイートのリストを送信すると、VDAはクライアントの暗号スイートの1つを、構成されている暗号スイートの独自のリスト内の暗号スイートの1つと照合し、接続を受け入れます。一致する暗号スイートがない場合、VDAは接続を拒否します。

  VDAは、3つの暗号スイートセット（コンプライアンスモードとも呼ばれます）をサポートしています：GOV（政府）、COM（商用）、およびALL。許容される暗号スイートは、Windows FIPSモードにも依存します。Windows FIPSモードの詳細については、`<http://support.microsoft.com/kb/811833>`を参照してください。次の表に、各セットの暗号スイートを示します。

暗号スイート	すべて	COM	GOV	すべて	COM	GOV
FIPSモード	オフ	オフ	オフ	オン	オン	オン
TLS_AES_256_GCM_SHA384	X		X	X		X
TLS_AES_128_G	X			X		X

暗号スイート	すべて	COM	GOV	すべて	COM	GOV
CM_SHA256						
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	X	X		X	X	

注:

VDAはDHE暗号スイート（例: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384、TLS_DHE_RSA_WITH_AES_256_CBC_SHA、TLS_DHE_RSA_WITH_AES_128_GCM_SHA256、TLS_DHE_RSA_WITH_AES_128_CBC_SHA）をサポートしていません。Windowsによって選択された場合、接続は失敗します。

NetScaler Gatewayを使用している場合は、バックエンド通信の暗号スイートサポートに関する情報について、NetScalerのドキュメントを参照してください。TLS暗号スイートのサポートについては、「Citrix ADCアプライアンスで利用可能な暗号」を参照してください。DTLS暗号スイートのサポートについては、「DTLS暗号のサポート」を参照してください。

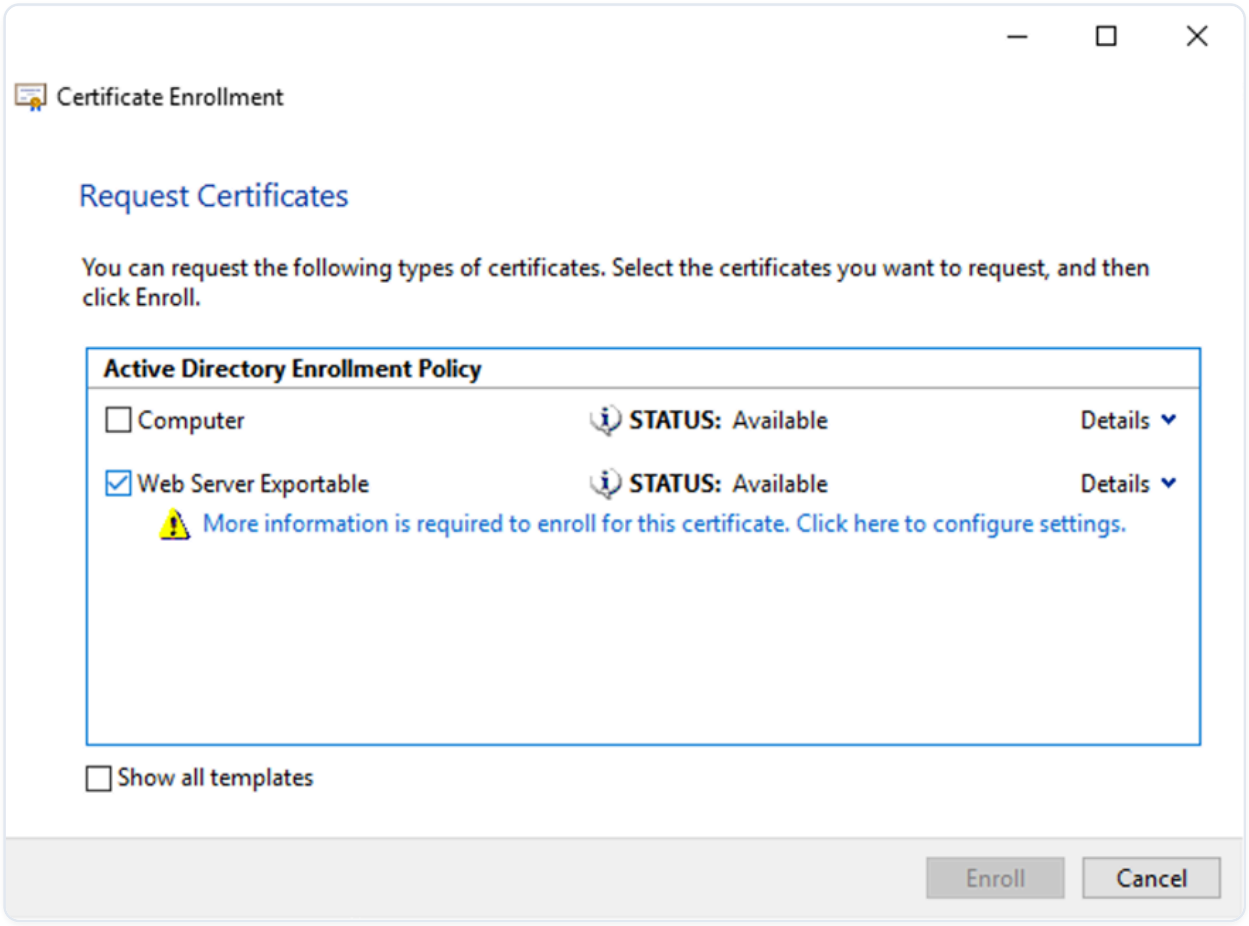
証明書を要求してインストールする

TLSを使用するには、代替名にVDAのFQDNが含まれる証明書をインストールする必要があります。この証明書は、VDAに直接接続する（Citrix Gatewayを介さない）すべてのクライアントによって信頼されている必要があります。証明書を簡単に展開できない管理対象外のデバイスがVDAに接続できるようにするには、NetScaler® Gatewayの展開を検討してください。

Microsoft 証明機関を使用して証明書を作成する

クライアントとVDAが信頼されたフォレストにあり、Microsoft証明機関がある場合、証明書MMCスナップインの証明書登録ウィザードから証明書を取得できます。

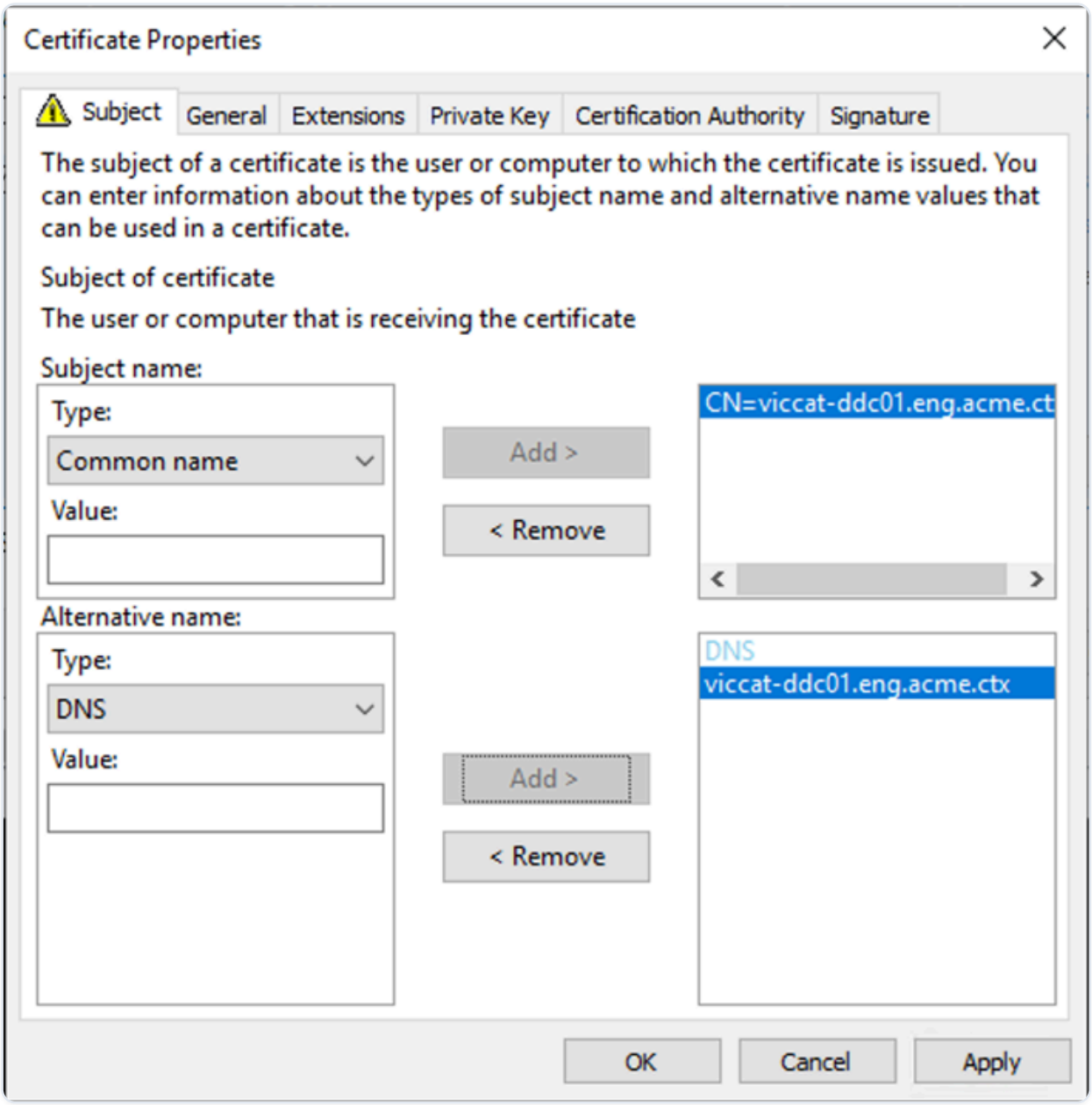
1. VDAで、MMCコンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、コンピューターアカウントを選択します。
2. **個人 > 証明書**を展開し、コンテキストメニューコマンド**すべてのタスク > 新しい証明書の要求**を使用します。
3. **次へ**をクリックして開始し、**次へ**をクリックして、Active Directory登録から証明書を取得することを確認します。
4. サーバー認証証明書のテンプレートを選択します。デフォルトのWindows **コンピューター**または**Webサーバーのエクスポート可能**のいずれも使用できます。テンプレートがSubjectの値を自動的に提供するように設定されている場合は、詳細を指定せずに**登録**をクリックできます。



5. 証明書テンプレートの詳細を指定するには、**詳細**をクリックして以下を構成します。

   サブジェクト名 — 種類として**共通名**を選択し、VDAのFQDNを追加します

   代替名 — タイプ **DNS** を選択し、VDA の FQDN を追加します。



注:

Active Directory証明書サービス証明書の自動登録を使用して、VDAへの証明書の発行と展開を自動化します。これについては、「証明書の自動登録を有効にする」で説明されています）。

ワイルドカード証明書を使用して、単一の証明書で複数の VDA を保護できます。

サブジェクト名 — タイプ **共通名** を選択し、VDA の *.primary.domain を入力します。

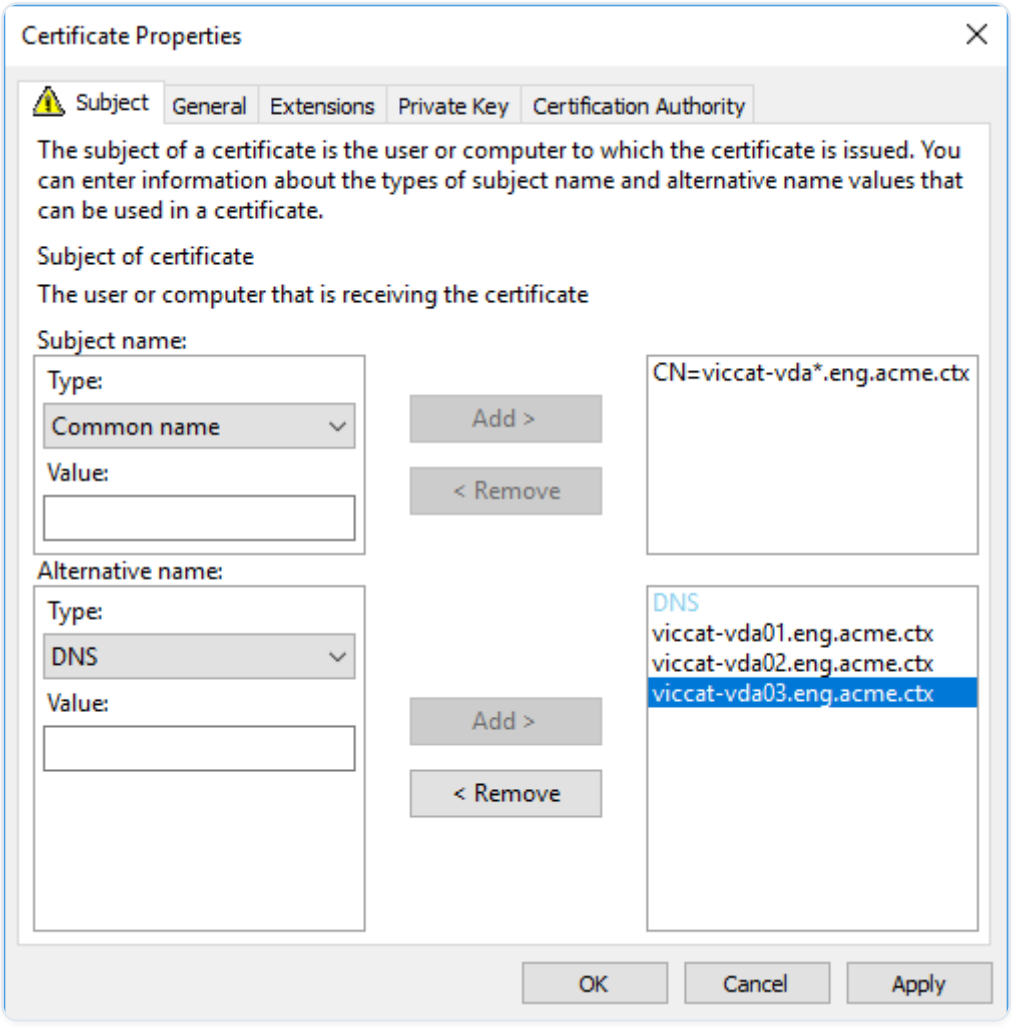
代替名 — タイプ **DNS** を選択し、VDA の *.primary.domain を追加します。

ワイルドカード証明書要求ダイアログ(/en-us/citrix-virtual-apps-desktops/2407/media/tls-request-certificates-wildcard.png)

SAN 証明書を使用して、単一の証明書で複数の特定の VDA を保護できます。

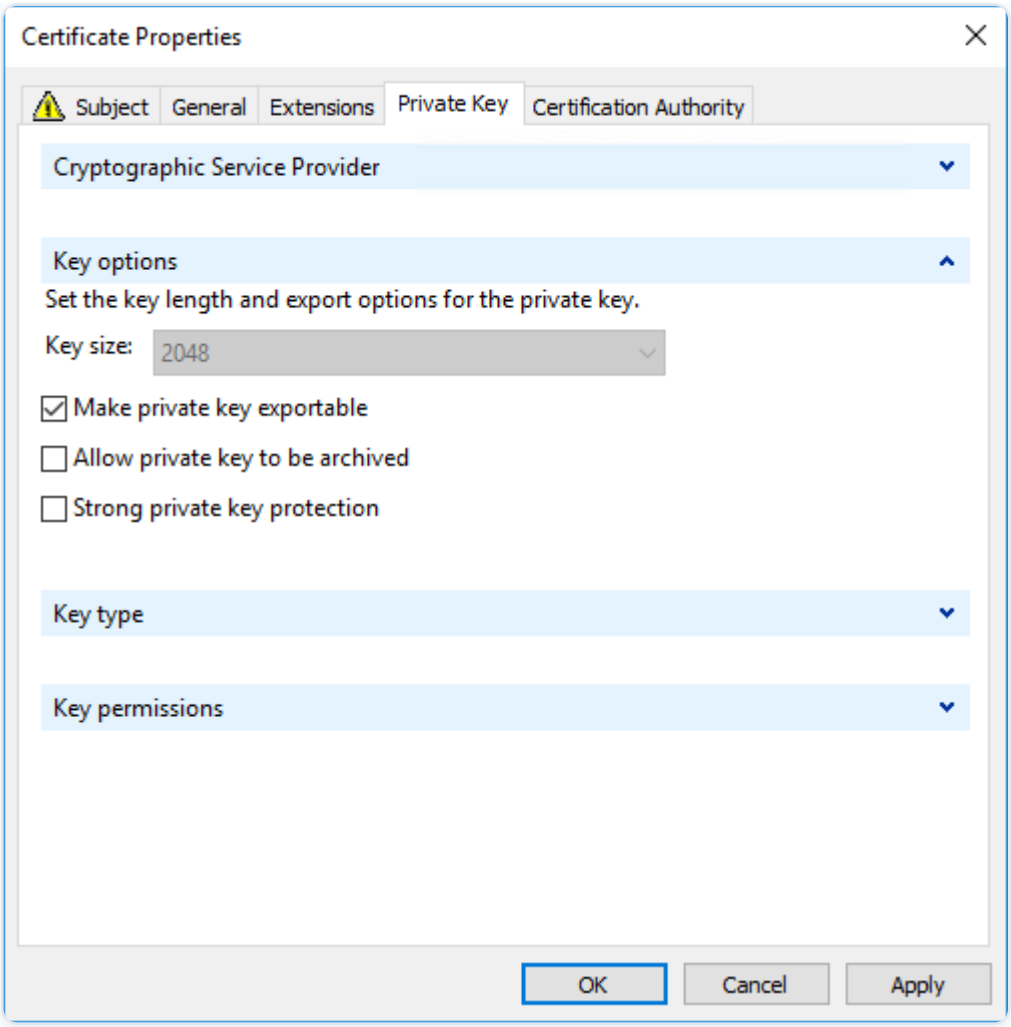
サブジェクト名 — タイプ **共通名** を選択し、証明書の使用状況を識別するのに役立つ文字列を入力します。

代替名 — タイプ **DNS** を選択し、各 VDA の FQDN のエントリを追加します。最適な TLS ネゴシエーションを確保するために、代替名の数を最小限に抑えてください。



注:

ワイルドカード証明書とSAN証明書の両方で、タブで**秘密キーをエクスポート可能にする**が選択されている必要があります。



PowerShellスクリプトを使用してVDAでTLSを構成する

TLS証明書を証明書ストアの「ローカルコンピューター > 個人 > 証明書」領域にインストールします。その場所に複数の証明書がある場合は、PowerShellスクリプトに証明書のサムプリントを指定します。

注:

XenAppおよびXenDesktop 7.15 LTSR以降、PowerShellスクリプトはVDAのFQDNに基づいて正しい証明書を検索します。VDAのFQDNに対して単一の証明書のみが存在する場合、サムプリントを指定する必要はありません。

Enable-VdaSSL.ps1スクリプトは、VDAでTLSリスナーを有効または無効にします。このスクリプトは、インストールメディアの*Support* > *Tools* > *SslSupport*フォルダーにあります。

TLSを有効にすると、DHE暗号スイートは無効になります。ECDHE暗号スイートは影響を受けません。

TLSを有効にすると、スクリプトは指定されたTCPポートの既存のWindowsファイアウォール規則をすべて無効にします。次に、ICAサービスがTLS TCPポートとUDPポートでのみ受信接続を受け入れることを許可する新しい規則を追加します。また、次のWindowsファイアウォール規則も無効にします。

- Citrix ICA（デフォルト：1494）
- Citrix CGP（デフォルト：2598）
- Citrix WebSocket（デフォルト：8008）

その結果、ユーザーはTLSまたはDTLSを使用してのみ接続できます。TLSまたはDTLSなしでは、ICA/HDX、セッションの信頼性を備えたICA/HDX、またはWebSocket経由のHDXを使用できません。

> **注:**

> DTLSは、UDPリアルタイムトランスポート経由のICA/HDXオーディオ、またはICA/HDX Framehawkではサポートされていません。

> 「ネットワークポート」を参照してください。(/ja-jp/tech-zone/build/tech-papers/citrix-communication-ports.html#citrix-virtual-apps-and-desktops).

スクリプトには、以下の構文の説明と追加の例が含まれています。この情報はNotepad++などのツールを使用して確認できます。

> **重要:**

> EnableまたはDisableパラメーターと、CertificateThumbPrintパラメーターを指定します。その他のパラメーターはオプションです。

構文

```
Enable-VdaSSL {-Enable | -Disable} -CertificateThumbPrint "<thumbprint>" [-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"\<suite>"]
```

パラメーター	説明
有効にする	VDAにTLSリスナーをインストールして有効にします。このパラメーターまたはDisableパラメーターのいずれかが必要です。
無効にする	VDA上のTLSリスナーを無効にします。このパラメーターまたはEnableパラメーターのいずれかが必要です。このパラメーターを指定した場合、他のパラメーターは無効です。
証明書のサムプリント "<thumbprint>"	証明書ストア内のTLS証明書のサムプリントを引用符で囲みます。スクリプトは、指定されたサムプリントを使用して、使用する証明書を選択します。このパラメーターが省略された場合、誤った証明書が選択されます。
SSLポート <port>	TLSポート。デフォルト: 443
SSL最小バージョン "<version>"	引用符で囲まれた最小TLSプロトコルバージョン。有効な値: `SSL_3.0`、`TLS_1.0` (デフォルト)、`TLS_1.1`、`TLS_1.2`、および `TLS_1.3`。`TLS_1.3` にはWindows 11またはWindows Server 2022以降が必要です。
SSLCipherSuite "<スイート>"	引用符で囲まれたTLS暗号スイート。有効な値: 「GOV」、「COM」、および「ALL」(デフォルト)。

例

次のスクリプトは、TLSプロトコルバージョンの値をインストールして有効にします。サムプリント（この例では「12345678987654321」として表されます）は、使用する証明書を選択するために使用されます。

```
Enable-VdaSSL -Enable -CertificateThumbPrint "12345678987654321"
```

次のスクリプトは、TLSリスナーをインストールして有効にし、TLSポート400、GOV暗号スイート、および最小TLS 1.2プロトコル値を指定します。サムプリント（この例では「12345678987654321」として表されます）は、使用する証明書を選択するために使用されます。

```
Enable-VdaSSL -Enable

-CertificateThumbPrint "12345678987654321"

-SSLPort 400 -SSLMinVersion "TLS_1.2"

-SSLCipherSuite "All"
```

次のスクリプトは、VDA上のTLSリスナーを無効にします。

```
Enable-VdaSSL -Disable
```

VDAでTLSを手動で構成する

VDAでTLSを手動で構成する場合、各VDAの適切なサービス（WindowsシングルセッションOS用VDAの場合はNT SERVICE\PorticaService、WindowsマルチセッションOS用VDAの場合はNT SERVICE\TermService）に対して、TLS証明書の秘密キーへの汎用読み取りアクセスを許可します。VDAがインストールされているマシンで：

手順 1. Microsoft管理コンソール (MMC) を起動します。 > > mmc.exe。

手順 2. MMCに証明書スナップインを追加します。

1. > を選択します。
2. を選択し、 をクリックします。
3. 「このスナップインは常に次の証明書を管理します:」と表示されたら、「コンピューターアカウント」を選択し、 をクリックします。
4. 「このスナップインで管理するコンピューターを選択してください」と表示されたら、「ローカルコンピューター」を選択し、 をクリックします。

ステップ3。 「証明書 (ローカル コンピューター) > 個人 > 証明書」で、証明書を右クリックし、「すべてのタスク > プライベート キーの管理」を選択します。

ステップ4。「アクセス制御リストエディター」に「(FriendlyName) プライベートキーのアクセス許可」が表示されます。(FriendlyName) はTLS証明書の名前です。次のいずれかのサービスを追加し、読み取りアクセス権を付与します。

- WindowsシングルセッションOS用VDAの場合、「PORTICASERVICE」
- Windows Multi-session OS 用 VDA の場合、「TERMSERVICE」

ステップ5。インストールされているTLS証明書をダブルクリックします。証明書のダイアログで、「詳細」タブを選択し、一番下までスクロールします。「拇印」をクリックします。

ステップ6。regeditを実行し、HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawdに移動します。

1. SSL Thumbprint キーを編集し、TLS 証明書の拇印の値をこのバイナリ値にコピーします。 ダイアログボックスの不明な項目（「0000」や特殊文字など）は無視しても問題ありません。
2. SSLEnabled キーを編集し、DWORD 値を 1 に変更します。（後で SSL を無効にするには、DWORD 値を 0 に変更します。）
3. デフォルト設定を変更する場合（オプション）は、同じレジストリパスで以下を使用します。

   SSLPort DWORD – SSLポート番号。デフォルト: 443。

   SSLMinVersion DWORD – 1 = SSL 3.0、2 = TLS 1.0、3 = TLS 1.1、4 = TLS 1.2、5 = TLS 1.3。デフォルト: 2 (TLS 1.0)。

   SSLCipherSuite DWORD – 1 = GOV、2 = COM、3 = ALL。デフォルト: 3 (ALL)。

ステップ7。TLS TCPおよびUDPポートがデフォルトの443でない場合、Windowsファイアウォールで開いていることを確認します。（Windowsファイアウォールで受信規則を作成する際は、そのプロパティで「接続を許可する」と「有効」のエントリが選択されていることを確認してください。）

ステップ8。他のアプリケーションやサービス（IISなど）がTLS TCPポートを使用していないことを確認します。

ステップ9。マルチセッションVDAの場合、変更を有効にするためにマシンを再起動します。（シングルセッションVDAマシンを再起動する必要はありません。）

ステップ10. 接続の問題を回避するために、VDAでサポートされている暗号スイートが最も高い優先順位を持つように、Windowsの暗号スイート設定を変更します。

> **重要:**
>
> 以下に概説するグループポリシーの変更は、システムを再起動した後にのみ有効になります。
>
> MCSまたはPVSでプロビジョニングされた非永続的なセッションホストを使用している場合、これらの設定をマスターイメージに適用する必要があります。

オプション1:

グループポリシーエディターを使用して、 > > > > > に移動します。以下の暗号スイートがリストの最上位にあることを確認してください。

```
TLS_AES_256_GCM_SHA384_P384

TLS_AES_256_GCM_SHA384_P256

TLS_AES_128_GCM_SHA256_P384

TLS_AES_128_GCM_SHA256_P256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

注:

TLS_AES_256_GCM_SHA384およびTLS_AES_128_GCM_SHA256は、Windows 11およびWindows Server 2022以降にのみ適用されます。古いオペレーティングシステムを使用している場合は、これらの暗号スイートをリストに含めないでください。

リストされている暗号スイートは、楕円曲線P384またはP256も指定しており、「curve25519」が選択されないようにしていることに注意してください。FIPSモードは「curve25519」の使用を妨げません。

リストから暗号スイートを削除する必要はありません。これらの設定はシステム全体に適用されるため、暗号スイートを削除する場合は、セッションホストで実行されているアプリ

ケーションやサービスによってそれらが必要とされていないことを確認する必要があります。

オプション2:

グループポリシーエディターを使用して、 > > > > > に移動します。以下の暗号スイートがリストの最上位にあることを確認してください。

```
TLS_AES_256_GCM_SHA384

TLS_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
```

注: TLS_AES_256_GCM_SHA384およびTLS_AES_128_GCM_SHA256は、Windows 11およびWindows Server 2022以降にのみ適用されます。古いオペレーティングシステムを使用している場合は、これらの暗号スイートをリストに含めないでください。

リストから暗号スイートを削除する必要はありません。これらの設定はシステム全体に適用されるため、暗号スイートを削除する場合は、セッションホストで実行されているアプリケーションやサービスによってそれらが必要とされていないことを確認する必要があります。

グループポリシーエディターを使用して、コンピューターの構成 > ポリシー > 管理用テンプレート > ネットワーク > SSL構成設定 > ECC曲線の順序 に移動します。設定を有効にし、以下の曲線をリストに含めます。

```
NistP384

NistP256
```

注:

> これにより、「curve25519」が選択されないようにします。FIPSモードは「curve25519」の使用を妨げません。

> VDAは、グループポリシーリストと、選択されたコンプライアンスモード（COM、GOV、またはALL）のリストの両方に表示される場合にのみ、暗号スイートを選択します。暗号スイートは、クライアント（Citrix Workspaceアプリ）から送信されたリストにも表示されている必要があります。

デリバリーグループでTLSを構成する

TLS接続用に構成したVDAを含む各デリバリーグループに対して、この手順を完了してください。

1. StudioからPowerShellコンソールを開きます。
2. Citrix製品のコマンドレットをロードするには、**asnp Citrix.*** を実行します。
3. **Get-BrokerAccessPolicyRule -DesktopGroupName '\<*delivery-group-name*>' \| Set-BrokerAccessPolicyRule -HdxSslEnabled $true** を実行します。
4. **Set-BrokerSite -DnsResolutionEnabled $true** を実行します。

自動登録を使用したプールされたVDAのSSL有効化

プールされたVDAを使用する場合、マスターイメージに証明書を追加すると、すべてのVDAが同じイメージを共有します。ワイルドカード証明書を使用することもできますが、欠点は、いずれかのVDAが侵害された場合、この強力な証明書により、すべてのVDAに属するHDX™接続が危険にさらされる可能性があることです。

代わりに、より安全な代替策として、Microsoft Active Directory証明書サービスを活用して、グループポリシーを使用して証明書を自動的にプロビジョニングする方法があります。VDA上でスタートアップスクリプトを使用して、新しい証明書を動的にプロビジョニングし、VDAでSSLを有効にすることができます。

このアプローチは、シングルセッションデスクトップVDAでのみ機能することに注意してください。マルチセッションVDAの場合、証明書が自動的にプロビジョニングされる前に、起動プロセス中にICAリスナーが早すぎる段階で起動されます。

Active Directory証明書サービスは内部のエンタープライズ証明機関を使用するため、すべてのWindowsインストールで自動的に信頼されるわけではありません。クライアントが企業によって管理され、ドメインフォレストの一部である場合、信頼されたCA証明書はグループポリシーを使用して自動的に配布できます。BYODやその他のドメインに参加していないデバイスの場合、信頼

されたCA証明書を別のメカニズム（ダウンロードリンクの提供など）でユーザーに配布するか、NetScaler Gatewayを使用する必要があります。

証明書の自動登録を有効にする

まず、VDAドメインフォレスト内のサーバーにActive Directory証明書サービスロールがインストールされており、エンタープライズCAが提供されていることを確認してください。そうしないと、自動登録はできません。

VDAは起動ごとに証明書要求を送信するため、これによりエンタープライズCAに通常よりもかなり高い負荷がかかる可能性があることに注意してください。負荷に対応できるよう、CAサーバーに十分なCPUとメモリを割り当て、本番環境に移行する前に、常にラボ環境で展開のスケーラビリティをテストしてください。

グループポリシー管理エディターで、SSLが有効になっているプールされたVDAを含む組織単位に適用される新しいポリシーを次のように作成します。

1. コンピューターの構成 -> ポリシー -> Windowsの設定 -> セキュリティの設定 -> 公開キーのポリシー を展開します
2. 「証明書サービス クライアント – 自動登録ポリシー」オブジェクトのプロパティを編集します
3. 以下のスクリーンショットに示すように構成します。
4. 自動証明書要求コンテナを右クリックし、「新規 -> 自動証明書要求...」を選択します。
5. 自動証明書要求セットアップウィザードで、「次へ」をクリックします。
6. コンピューター証明書テンプレートが選択されていることを確認し、「次へ」をクリックします。
7. 「完了」をクリックします。

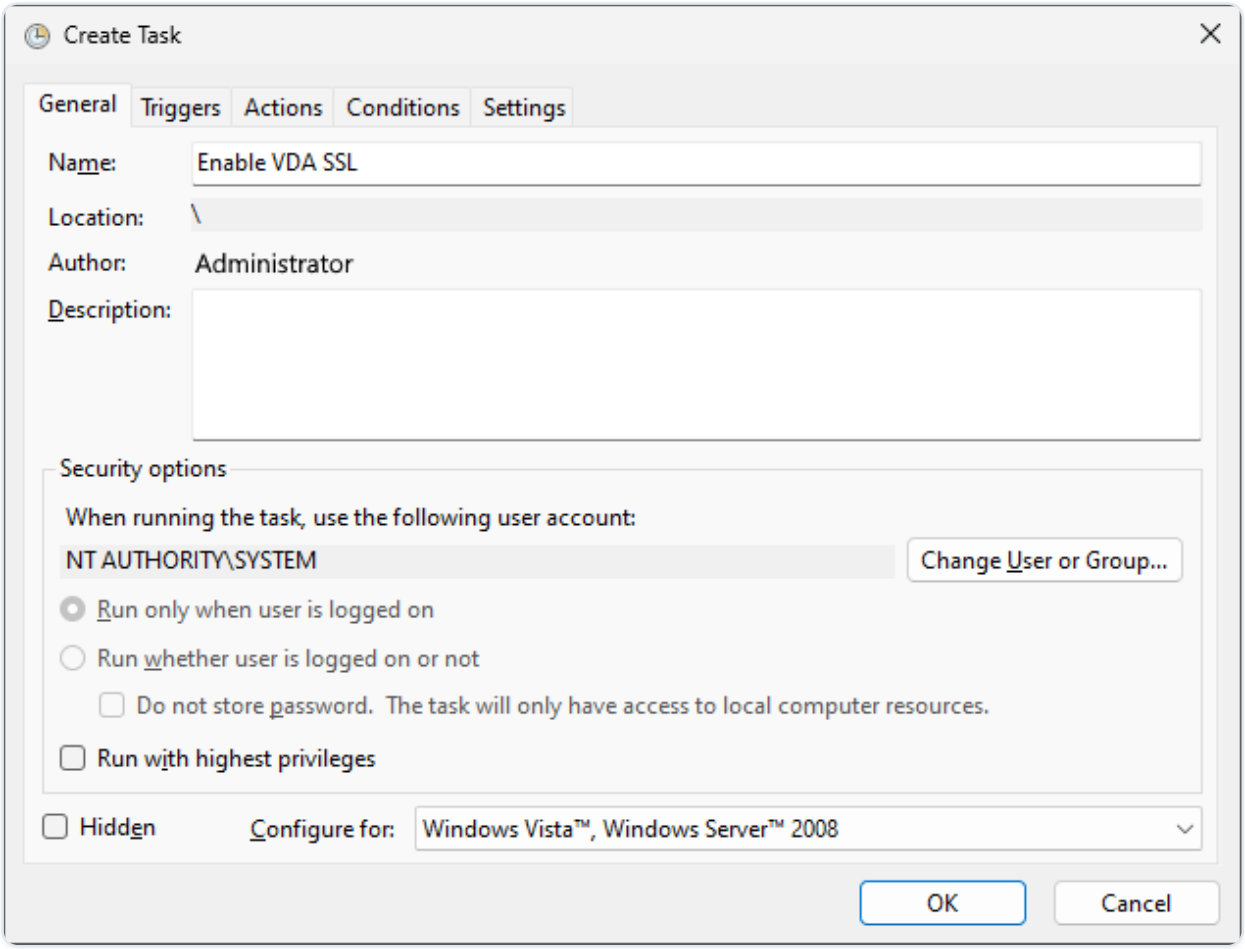
登録ポリシーのスクリーンショット (/en-us/citrix-virtual-apps-desktops/2407/media/ssltask-autoenrollment-policy.png)

Windowsマスターイメージの準備

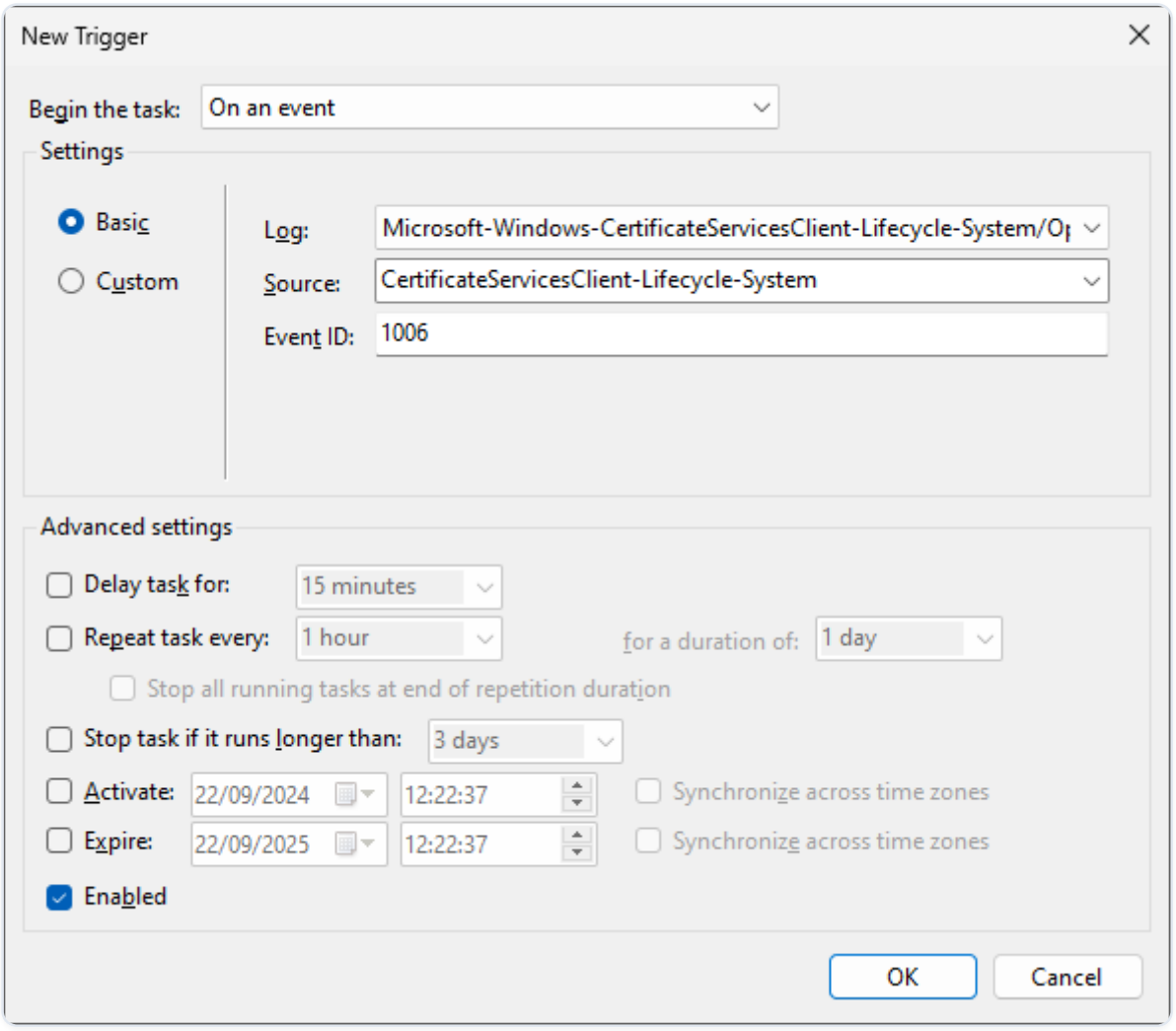
Enable-VdaSsl.ps1スクリプトを、製品インストールメディアの `Support\Tools\SslSupport` フォルダーからVDAマスターイメージにコピーします。マスターイメージには、HDX SSL接続に使用する証明書を含めないでください。証明書は、MCSまたはPVSマシンカタログが作成されるときにプロビジョニングされます。次に、次のように新しいスケジュールされたタスクを作成します（スケジュールされたタスクは今すぐ実行しないでください）。

1. タスクスケジューラを開きます。

2. **操作**ペインで、「**タスクの作成...**」を押します。
3. 「全般」タブで:
   - 「**名前**」に`Enable VDA SSL`などの名前を入力します
   - 「**ユーザーまたはグループの変更...**」をクリックし、「ユーザーまたはグループの選択」ダイアログボックスに`SYSTEM`を入力して「**OK**」をクリックします



4. 「トリガー」タブを選択します
5. 「**新規...**」をクリックします。「**新しいトリガー**」ダイアログで:
   a. 「**タスクの開始**」を「**イベント時**」に設定します
   b. 「**ログ**」を「**Microsoft-Windows-CertificateServicesClient-Lifecycle-System/Operational**」に設定します
   c. 「**ソース**」を「**Microsoft-Windows-CertificateServicesClient-Lifecycle-System**」に設定します
   d. 「**イベントID**」を`1006`に設定します
   e. 「**OK**」をクリックしてトリガーを保存します



6. 「**操作**」タブを選択します
7. 「**新規...**」をクリックします
8. 「**新しい操作**」ダイアログで:

    a. **アクション**を**プログラムの開始**に設定します

    b. プログラム/スクリプトフィールドに、`powershell.exe`を入力します

    c. 「引数の追加」フィールドに、PowerShellスクリプトへのパスを含めて`-ExecutionPolicy RemoteSigned Enable-VdaSsl.ps1 -Enable -Confirm:$False`を入力します。

    d. 「**OK**」を押してアクションを保存します。

    新しいアクションウィンドウのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2407/media/ssltask-action.png)

9. 「**OK**」を押してタスクを保存します。

トラブルシューティング

接続エラーが発生した場合は、VDAのシステムイベントログを確認してください。

Windows向けCitrix Workspaceアプリを使用しているときに、TLSエラーを示す接続エラーが発生した場合は、Desktop Viewerを無効にしてから、再度接続を試してください。接続が引き続き失敗する場合でも、根本的なTLS問題の説明が提供されることがあります（たとえば、証明機関から証明書を要求する際に誤ったテンプレートを指定したなど）。

HDX Adaptive Transportを使用するほとんどの構成は、DTLSで正常に動作します。これには、Citrix Workspaceアプリ、Citrix Gateway、およびVDAの最新バージョンを使用しているものも含まれます。Citrix WorkspaceアプリとCitrix Gatewayの間、およびCitrix GatewayとVDAの間でDTLSを使用する一部の構成では、追加のアクションが必要です。

次の場合、追加の操作が必要です。

- Citrix ReceiverのバージョンがHDX Adaptive TransportとDTLSをサポートしている場合: Receiver for Windows (4.7, 4.8, 4.9)、Receiver for Mac (12.5, 12.6, 12.7)、Receiver for iOS (7.2, 7.3.x)、またはReceiver for Linux (13.7)

以下のいずれかに該当する場合も同様です。

- Citrix GatewayのバージョンがVDAへのDTLSをサポートしているが、VDAのバージョンがDTLSをサポートしていない場合（バージョン7.15以前）、,
- VDAのバージョンがDTLSをサポートしているが（バージョン7.16以降）、Citrix Gatewayのバージョンが VDAへのDTLSをサポートしていない場合。

Citrix Receiver™ からの接続が失敗するのを避けるには、次のいずれかを実行します。

- Citrix Receiver を、Receiver for Windows バージョン 4.10 以降、Receiver for Mac 12.8 以降、または Receiver for iOS バージョン 7.5 以降にアップデートする、または,
- Citrix Gateway を、VDA への DTLS をサポートするバージョンにアップデートする、または,
- VDA をバージョン 7.16 以降にアップデートする、または,
- VDA で DTLS を無効にする、または,
- HDX Adaptive Transport を無効にする。

> **注:**

> Receiver for Linux の適切なアップデートはまだ利用できません。Receiver for Android (バージョン 3.12.3) は、Citrix Gateway 経由の HDX Adaptive Transport および DTLS をサポートしていないため、影響を受けません。

> VDAでDTLSを無効にするには、VDAファイアウォール構成を変更してUDPポート443を無効にします。(/ja-jp/tech-zone/build/tech-papers/citrix-communication-ports.html#citrix-virtual-apps-and-desktops)を参照してください。

TLS と HTML5 ビデオリダイレクト、およびブラウザコンテンツリダイレクト

HTML5 ビデオリダイレクトとブラウザコンテンツリダイレクトを使用して、HTTPS Web サイトをリダイレクトできます。これらの Web サイトに挿入される JavaScript は、VDA で実行されている Citrix HDX HTML5 Video Redirection Service への TLS 接続を確立する必要があります。これを実現するために、HTML5 Video Redirection Service は、VDA の証明書ストアに 2 つのカスタム証明書を生成します。サービスを停止すると、証明書は削除されます。

HTML5 ビデオリダイレクトポリシーは、デフォルトで無効になっています。

ブラウザコンテンツリダイレクトはデフォルトで有効になっています。

HTML5 ビデオリダイレクトの詳細については、「マルチメディアポリシー設定」を参照してください。

Universal Print Server で TLS を有効にする

トランスポート層セキュリティ (TLS) プロトコルは、Virtual Delivery Agent (VDA) と Universal Print Server 間の TCP ベースの接続でサポートされています。

> **警告:**

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

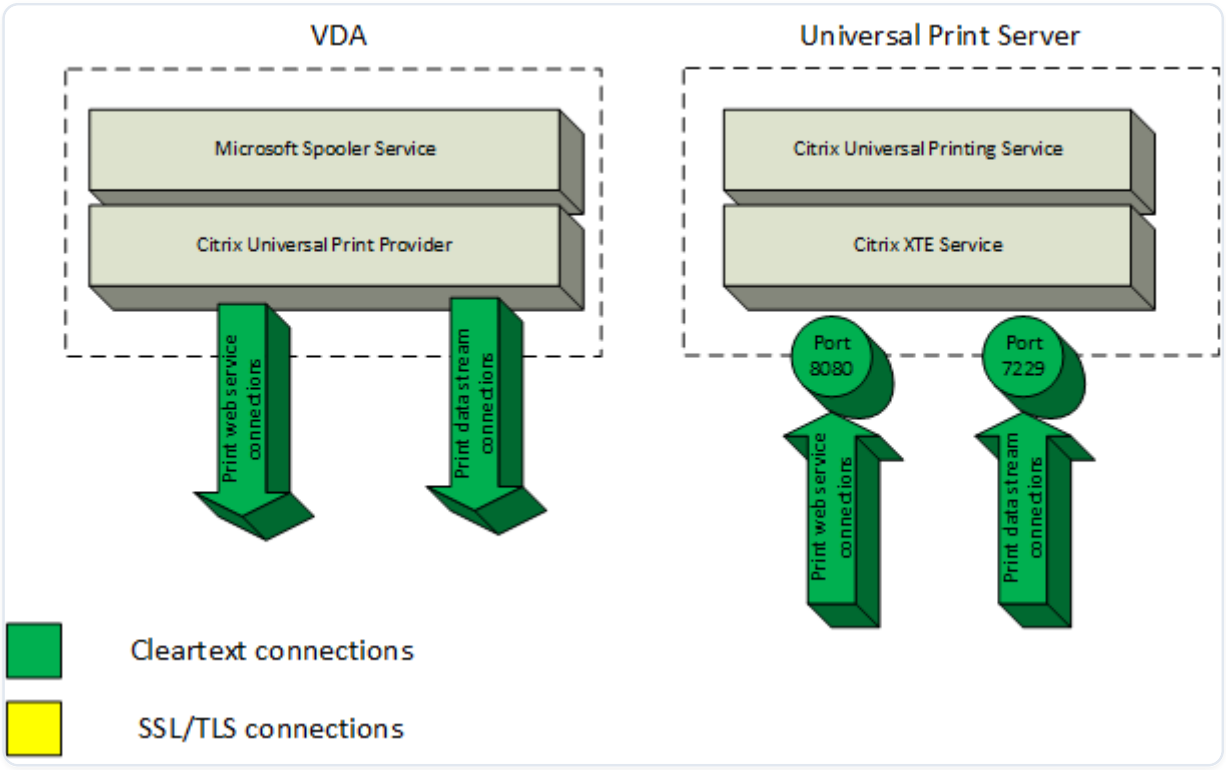
VDA と Universal Print Server 間の印刷接続の種類

クリアテキスト接続

印刷に関連する以下の接続は、VDA から発信され、Universal Print Server のポートに接続します。これらの接続は、**SSL enabled** ポリシー設定が **Disabled** (デフォルト) に設定されている場合にのみ行われます。

- クリアテキスト印刷 Web サービス接続 (TCP ポート 8080)
- クリアテキスト印刷データストリーム (CGP) 接続 (TCP ポート 7229)

Microsoft のサポート記事 Service overview and network port requirements for Windows には、Microsoft Windows Print Spooler サービスが使用するポートが記載されています。このドキュメントの SSL/TLS 設定は、Windows Print Spooler サービスによって行われる NetBIOS および RPC 接続には適用されません。**Universal Print Server enable** ポリシー設定が **Enabled with fallback to Windows' native remote printing** に設定されている場合、VDA は Windows Network Print Provider (win32spl.dll) をフォールバックとして使用します。

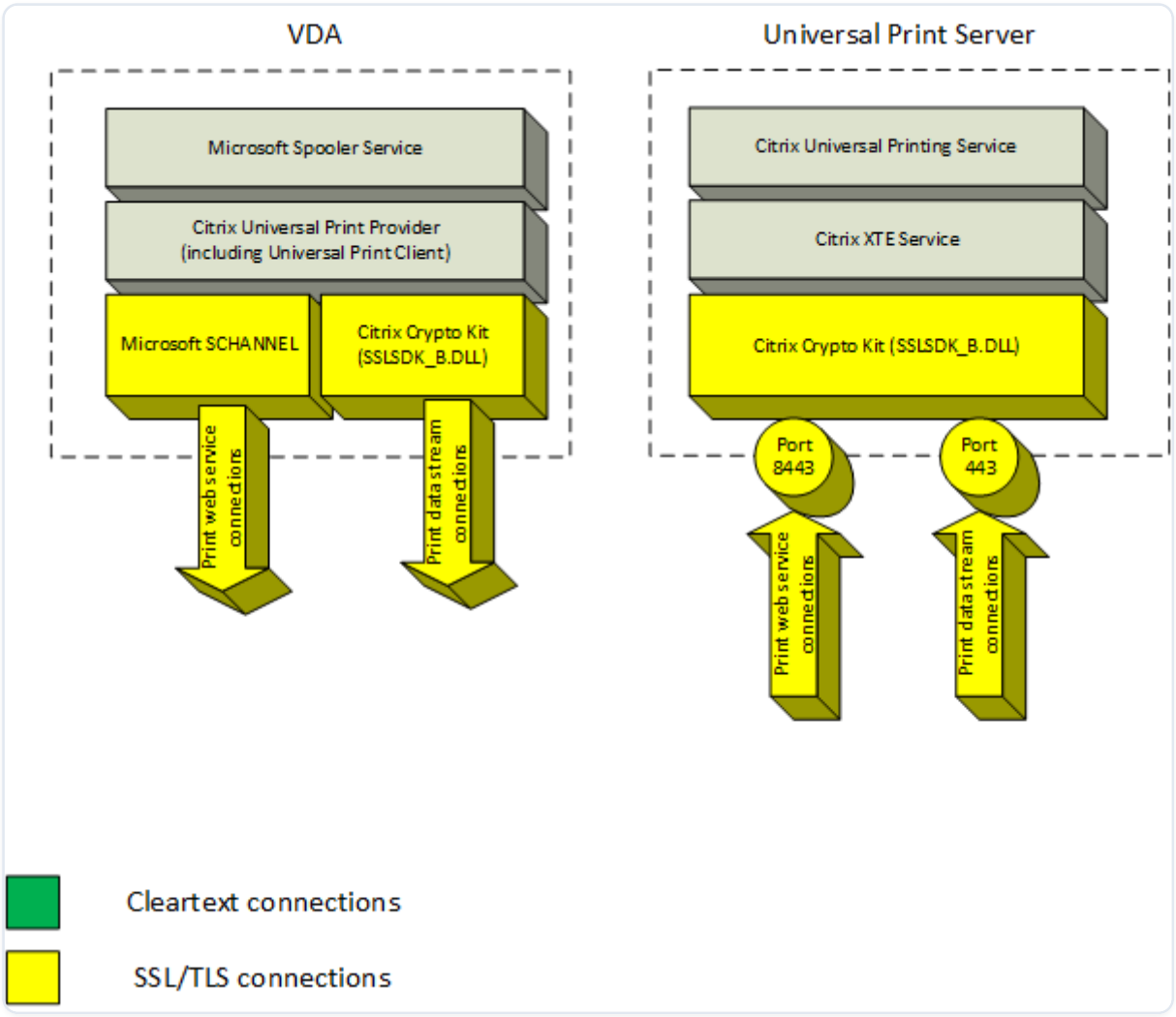


暗号化された接続

印刷に関連するこれらの SSL/TLS 接続は、VDA から発信され、Universal Print Server のポートに接続します。これらの接続は、**SSL enabled** ポリシー設定が **Enabled** に設定されている場合にのみ行われます。

- 暗号化された印刷 Web サービス接続 (TCP ポート 8443)

- 暗号化された印刷データストリーム (CGP) 接続 (TCP ポート 443)



SSL/TLS クライアント構成

VDA は SSL/TLS クライアントとして機能します。

Microsoft Group Policyとレジストリを使用して、暗号化された印刷Webサービス接続（TCPポート8443）用にMicrosoft SCHANNEL SSPを構成します。Microsoftサポート記事「TLS Registry Settings」には、Microsoft SCHANNEL SSPのレジストリ設定が記載されています。

VDAでグループポリシーエディターを使用して、 **> > > >** に移動します。TLS 1.3が設定されている場合は、次の順序を選択します。

TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256

TLS 1.2 が設定されている場合は、次の順序を選択します。

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

> **注:**

> このグループポリシー設定が構成されている場合、VDA は、暗号化された印刷 Web サービス接続 (デフォルトポート: 8443) の暗号スイートを、接続が両方の SSL 暗号スイートリストに表示されている場合にのみ選択します。

> - グループポリシー SSL 暗号スイート順序リスト
> - 選択した SSL 暗号スイートポリシー設定 (COM、GOV、または ALL) に対応するリスト

> このグループポリシー構成は、VDA上の他のTLSアプリケーションおよびサービスにも影響します。アプリケーションが特定の暗号スイートを必要とする場合、このグループポリシー暗号スイート順序リストに追加する必要がある場合があります。

> **重要:**

> TLS構成のグループポリシー変更は、オペレーティングシステムの再起動後にのみ有効になります。

> Citrix ポリシーを使用して、暗号化された印刷データストリーム (CGP) 接続 (TCP ポート 443) の SSL/TLS 設定を構成します。

SSL/TLS サーバー構成

Universal Print Server は SSL/TLS サーバーとして機能します。

SSL/TLS設定を構成するには、`Enable-UpsSsl.ps1` PowerShellスクリプトを使用します。

Universal Print ServerにTLSサーバー証明書をインストールする

HTTPSの場合、Universal Print Serverはサーバー証明書を使用してTLS機能をサポートします。クライアント証明書は使用されません。Universal Print Serverの証明書を要求するには、Microsoft Active Directory証明書サービスまたは別の認証局を使用します。

Microsoft Active Directory Certificate Services を使用して証明書を登録/要求する際は、以下の考慮事項に留意してください。

1. 証明書をローカルコンピューターの**個人**証明書ストアに配置します。
2. 証明書のサブジェクト識別名 (Subject DN) の**共通名**属性を、Universal Print Serverの完全修飾ドメイン名 (FQDN) に設定します。これは証明書テンプレートで指定します。
3. 証明書要求と秘密キーの生成に使用される暗号化サービスプロバイダー (CSP) を、**Microsoft Enhanced RSA and AES Cryptographic Provider (Encryption)** に設定します。これは証明書テンプレートで指定します。
4. キーサイズを2048ビット以上に設定します。これは証明書テンプレートで指定します。

Universal Print ServerでのSSLの構成

Universal Print Server上のXTEサービスは、着信接続をリッスンします。SSLが有効な場合、SSLサーバーとして機能します。着信接続には、印刷コマンドを含む印刷Webサービス接続と、印刷ジョブを含む印刷データストリーム接続の2種類があります。これらの接続でSSLを有効にできます。SSLは、これらの接続の機密性と整合性を保護します。デフォルトでは、SSLは無効になっています。

SSLの構成に使用されるPowerShellスクリプトは、インストールメディアにあり、ファイル名は次のとおりです: `\Support\Tools\SslSupport\Enable-UpsSsl.ps1.`.

Universal Print Serverでのリスニングポート番号の構成

XTEサービスのデフォルトポートは次のとおりです。

- クリアテキスト印刷Webサービス（HTTP）TCPポート: 8080
- クリアテキスト印刷データストリーム (CGP) TCPポート: 7229
- 暗号化された印刷Webサービス (HTTPS) TCPポート: 8443
- 暗号化された印刷データストリーム (CGP) TCPポート: 443

Universal Print Server の XTE サービスで使用されるポートを変更するには、管理者として PowerShell で次のコマンドを実行します (Enable-UpsSsl.ps1 PowerShell スクリプトの使用に関する注意点については、後のセクションを参照してください):

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` または `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`
3. `Start-Service CitrixXTEServer`

ユニバーサルプリントサーバーでのTLS設定

負荷分散構成で複数の Universal Print Server を使用している場合は、すべての Universal Print Server で **TLS** 設定が一貫して構成されていることを確認してください。

Universal Print Server で TLS を構成すると、インストールされている TLS 証明書のアクセス許可が変更され、Universal Printing Service に証明書の秘密キーへの読み取りアクセス権が付与されます。また、Universal Printing Service に次の情報が通知されます。

- TLS に使用する証明書ストア内の証明書。
- TLS 接続に使用する TCP ポート番号。

Windows ファイアウォール (有効な場合) は、これらの TCP ポートでの受信接続を許可するように構成する必要があります。この構成は、Enable-UpsSsl.ps1 PowerShell スクリプトを使用すると自動的に行われます。

- 許可する TLS プロトコルのバージョン。

Universal Print Server は TLS プロトコルバージョン 1.3 および 1.2 をサポートしています。許可される最小バージョンを指定します。

デフォルトの TLS プロトコルバージョンは 1.2 です。

> **注:**
>
> TLS 1.1 および 1.0 は、Citrix Virtual Apps and Desktops バージョン 2311 以降ではサポートされなくなりました。

- 許可する TLS 暗号スイート。

暗号スイートは、接続に使用される暗号アルゴリズムを選択します。VDAとUniversal Print Serverは、異なる暗号スイートのセットをサポートできます。VDAが接続し、サポートされているTLS暗号スイートのリストを送信すると、Universal Print Serverはクライアントの暗号スイートの1つを、自身の構成済み暗号スイートのリストにある暗号スイートの1つと照合し、接続を受け入れます。一致する暗号スイートがない場合、Universal Print Serverは接続を拒否します。

Universal Print Serverは、OPEN、FIPS、およびSP800-52ネイティブCrypto Kitモードに対して、GOV（政府）、COM（商用）、およびALLという名前の以下の暗号スイートセットをサポートしています。許容される暗号スイートは、**SSL FIPSモード**ポリシー設定とWindows FIPSモードに

も依存します。Windows FIPSモードの詳細については、このMicrosoftサポート記事を参照してください。

暗号スイート（優先順位の降順）	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_AES256_GCM_SHA384	X		X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA384	X		X	X		X	X		X
TLS_ECDHE_RSA_AES256_C	X	X		X	X		X	X	

暗号スイート（優先順位の降順）	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
BC_SHA									

PowerShellスクリプトを使用してUniversal Print ServerでTLSを構成する

TLS証明書を証明書ストアの**ローカルコンピューター > 個人 > 証明書**領域にインストールします。その場所に複数の証明書がある場合は、`Enable-UpsSsl.ps1` PowerShellスクリプトに証明書のサムプリントを指定します。

> **注:**
>
> PowerShellスクリプトは、Universal Print ServerのFQDNに基づいて正しい証明書を検索します。Universal Print ServerのFQDNに対して証明書が1つしかない場合は、証明書のサムプリントを指定する必要はありません。

> `Enable-UpsSsl.ps1`スクリプトは、VDAからUniversal Print ServerへのTLS接続を有効または無効にします。このスクリプトは、インストールメディアの**Support > Tools > SslSupport**フォルダーにあります。

TLSを有効にすると、スクリプトはUniversal Print ServerのTCPポートに対する既存のWindowsファイアウォール規則をすべて無効にします。その後、XTEサービスがTLS TCPおよびUDPポートでのみ受信接続を受け入れることを許可する新しい規則を追加します。また、以下のWindowsファイアウォール規則も無効にします。

- クリアテキスト印刷Webサービス接続（デフォルト：8080）
- クリアテキスト印刷データストリーム（CGP）接続（デフォルト：7229）

その結果、VDAはTLSを使用している場合にのみこれらの接続を行うことができます。

> **注:**

TLSを有効にしても、VDAからUniversal Print ServerへのWindows Print Spooler RPC/SMB接続には影響しません。

重要:

最初のパラメーターとして**Enable**または**Disable**のいずれかを指定します。ローカルコンピューターの個人証明書ストアにUniversal Print ServerのFQDNを持つ証明書が1つしかない場合、CertificateThumbprintパラメーターはオプションです。その他のパラメーターもオプションです。

構文

```
Enable-UpsSSL.ps1 -Enable [-HTTPPort &lt;port&gt;] [-CGPPort &lt;port&gt;] [-HTTPSPort &lt;port&gt;] [-CGPSSLPort &lt;port&gt;] [-SSLMinVersion &lt;version&gt;] [-SSLCipherSuite &lt;name&gt;] [-CertificateThumbprint &lt;thumbprint&gt;] [-FIPSMode &lt;Boolean&gt;] [-ComplianceMode &lt;mode&gt;]

Enable-UpsSSL.ps1 -Disable [-HTTPPort &lt;portnum&gt;] [-CGPPort &lt;portnum&gt;]
```

パラメーター	説明
有効化	XTEサーバーでSSL/TLSを有効にします。このパラメーターまたはDisableパラメーターのいずれかが必要です。
無効化	XTEサーバーでSSL/TLSを無効にします。このパラメーターまたはEnableパラメーターのいずれかが必要です。
証明書のサムプリント `"<thumbprint>"`	ローカルコンピューターの個人証明書ストアにあるTLS証明書のサムプリント。引用符で囲みます。スクリプトは、指定されたサムプリントを使用して、使用する証明書を選択します。
HTTPPort `<port>`	クリアテキスト印刷Webサービス (HTTP/SOAP) ポート。デフォルト: 8080

パラメーター	説明
CGPポート `<port>`	クリアテキスト印刷データストリーム (CGP) ポート。デフォルト: 7229
HTTPSポート `<port>`	暗号化された印刷Webサービス (HTTPS/SOAP) ポート。デフォルト: 8443
CGPSSLポート `<port>`	暗号化された印刷データストリーム (CGP) ポート。デフォルト: 443
SSLMinVersion `"<version>"`	引用符で囲まれた最小TLSプロトコルバージョン。有効な値: 「TLS_1.2」および「TLS_1.3」。デフォルト: TLS_1.2。
SSLCipherSuite `"<name>"`	引用符で囲まれたTLS暗号スイートパッケージの名前。有効な値: 「GOV」、「COM」、および「ALL」(デフォルト)。
FIPSモード `<Boolean>`	XTEサーバーでFIPS 140モードを有効または無効にします。有効な値: FIPS 140モードを有効にする場合は$true、FIPS 140モードを無効にする場合は$false。

例

次のスクリプトはTLSを有効にします。サムプリント（この例では「12345678987654321」として表されています）は、使用する証明書を選択するために使用されます。

```
Enable-UpsSsl.ps1 –Enable -CertificateThumbprint "12345678987654321"
```

次のスクリプトはTLSを無効にします。

```
Enable-UpsSsl.ps1 –Disable
```

FIPSモードの構成

米国連邦情報処理標準 (FIPS) モードを有効にすると、Universal Print Server の暗号化された接続に FIPS 140 準拠の暗号化のみが使用されるようになります。

クライアントでFIPSモードを構成する前に、サーバーでFIPSモードを構成してください。

Windows FIPSモードの有効化または無効化については、Microsoftのドキュメントサイトでご確認ください。

クライアントでのFIPSモードの有効化

Delivery Controller™で、Web Studioを実行し、Citrixポリシー設定の**SSL FIPS Mode**を**Enabled**に設定します。Citrixポリシーを有効にします。

各VDAで次の操作を行います。

1. Windows FIPSモードを有効にします。
2. VDAを再起動します。

サーバーでのFIPSモードの有効化

各Universal Print Serverで、次の操作を行います。

1. Windows FIPSモードを有効にします。
2. 管理者として次のPowerShellコマンドを実行します: `stop-service CitrixXTEServer, UpSvc`
3. `-Enable -FIPSMode $true` パラメーターを指定して `Enable-UpsSsl.ps1` スクリプトを実行します。
4. Universal Print Serverを再起動します。

クライアントでのFIPSモードの無効化

Web Studioで、**SSL FIPSモード**のCitrixポリシー設定を**無効**に設定します。Citrixポリシーを有効にします。**SSL FIPSモード**のCitrixポリシー設定を削除することもできます。

各VDAで、次の操作を行います。

1. Windows FIPSモードを無効にします。
2. VDAを再起動します。

サーバーでのFIPSモードの無効化

各Universal Print Serverで、次の操作を行います。

1. Windows FIPSモードを無効にします。
2. 管理者として次のPowerShellコマンドを実行します: `stop-service CitrixXTEServer, UpSvc`
3. `-Enable -FIPSMode $false` パラメーターを指定して `Enable-UpsSsl.ps1` スクリプトを実行します。
4. Universal Print Server を再起動します。

> **注:**
>
> SSLプロトコルバージョンがTLS 1.3に設定されている場合、FIPSモードはサポートされません。

SSL/TLSプロトコルバージョンの構成

デフォルトの SSL/TLS プロトコルバージョンは TLS 1.2 です。TLS 1.2 および TLS 1.3 は、本番環境での使用が推奨される SSL/TLS プロトコルバージョンです。トラブルシューティングのために、非本番環境で SSL/TLS プロトコルバージョンを一時的に変更する必要がある場合があります。

SSL 2.0 および SSL 3.0 は Universal Print Server ではサポートされていません。

サーバーでのSSL/TLSプロトコルバージョンの設定

各 Universal Print Server でこれを行います。

1. 管理者としてこのPowerShellコマンドを実行します: `stop-service CitrixXTEServer, UpSvc`
2. `-Enable -SSLMinVersion` バージョンパラメーターを指定して、`Enable-UpsSsl.ps1` スクリプトを実行します。テストが完了したら、これをTLS 1.2またはTLS 1.3に戻すことを忘れないでください。
3. Universal Print Serverを再起動します。

クライアントでのSSL/TLSプロトコルバージョンの設定

各 VDA でこれを行います。

1. Delivery Controller で、**SSL プロトコルバージョン** ポリシー設定を目的のプロトコルバージョンに設定し、ポリシーを有効にします。
2. Microsoft サポート記事 TLS レジストリ設定 は、Microsoft SCHANNEL SSP のレジストリ設定について説明しています。レジストリ設定を使用して、クライアント側の **TLS 1.2 または TLS 1.3** を有効にします。

> **重要:**
>
> テストが完了したら、レジストリ設定を元の値に戻すことを忘れないでください。

3. VDA を再起動します。

トラブルシューティング

接続エラーが発生した場合は、Universal Print Server の C:\Program Files (x86)\Citrix\XTE\logs\error.log ファイルを確認してください。

SSL/TLS ハンドシェイクが失敗した場合、このログファイルにエラーメッセージ「**SSL handshake from client failed**」が表示されます。このような失敗は、VDA と Universal Print Server の SSL/TLS プロトコルバージョンが一致しない場合に発生する可能性があります。

Universal Print Server ホスト名を含む以下のポリシー設定で、Universal Print Server の FQDN を使用してください。

- セッションプリンター
- プリンターの割り当て
- 負荷分散用のUniversal Print Server

Universal Print Server と VDA で、システムクロック（日付、時刻、タイムゾーン）が正しいことを確認してください。

仮想チャネル許可リスト

仮想チャネル許可リストは、Citrix以外の仮想チャネルのうち、どのチャネルを環境で許可するかを制御できる機能です。デフォルトでは、仮想チャネル許可リスト機能は有効になっています。その結果、Citrix Virtual Apps and Desktops™セッションでは、Citrix仮想チャネルのみが開くことが許可されます。自社製またはサードパーティ製のカスタム仮想チャネルを使用する必要がある場合は、それらを明示的に許可リストに追加する必要があります。

構成

仮想チャネル許可リストはデフォルトで有効になっています。この機能は、Citrixポリシーの以下の設定を使用して構成できます。

- **仮想チャネル許可リスト**: この機能を有効または無効にし、仮想チャネルをリストに追加します。
- **仮想チャネル許可リストログのスロットリング**: 仮想チャネル許可リストのイベントログのスロットリング期間を設定します。
- **仮想チャネル許可リストのログ記録**: 仮想チャネル許可リストのログレベルを設定します。

仮想チャネルを許可リストに追加する

仮想チャネルを許可リストに追加するには、以下の情報が必要です。

1. コードで定義されている仮想チャネル名。最大7文字です。例: `CTXCVC1`。
2. VDAマシン上で仮想チャネルを開くプロセスのパス。例: `C:\Program Files\Application\run.exe`。

必要な情報が揃ったら、仮想チャネル許可リストポリシー設定を使用して、仮想チャネルを許可リストに追加する必要があります。仮想チャネルをリストに追加するには、仮想チャネル名の後にコンマを入力し、次に仮想チャネルにアクセスするプロセスのパスを入力します。複数のプロセスがある場合は、各プロセスをコンマで区切って追加できます。

単一プロセスの場合

前の例を使用して、以下のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe
```

複数のプロセスの場合

複数のプロセスがある場合は、次のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

ワイルドカードの使用

ワイルドカード (*) の使用がサポートされています。アプリケーションのバージョンによってディレクトリ名や実行可能ファイル名が変わる場合、またはサードパーティコンポーネントがユーザープロファイルにインストールされている場合に、ワイルドカードを使用できます。

次のシナリオでワイルドカードを使用できます。

- ディレクトリ名全体を置き換える場合。 例: `C:\Program Files\Application*\run1.exe`
- ディレクトリ名の一部を置き換える場合。 例: `C:\Program Files\Application\v*\run1.exe`
- 実行可能ファイル名を置き換える場合。 例: `C:\Program Files\Application\v1.2*.exe`
- 実行可能ファイル名の一部を置き換える場合。 例: `C:\Program Files\Application\v1.2\run*.exe`

次の制限が適用されます。

- ワイルドカードは、単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルが `C:\Program Files\Application\v1.2\run1.exe` にある場合
  - 許可される例: `C:\Program Files\Application*\run1.exe`
  - 許可されない例: `C:\Program Files*\run1.exe`
- エントリにはファイル名拡張子を含める必要があります。
  - 許可: `C:\Program Files\Application\v1.2*.exe`
  - 不許可: `C:\Program Files\Application\v1.2*`
- すべてのパスはローカルである必要があります。

注:

- ネットワークパスは許可されていません。
- ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2206 から利用可能です。
- ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2203 LTSR (CU2以降) で利用可能です。

システム環境変数の使用

システム環境変数を使用して、許可リスト内の信頼されたプロセスの定義を簡素化できます。`%programfiles%`、`%programfiles(x86)%`、`%systemdrive%`、`%systemroot%` などの既成の変数を使用できます。

カスタム環境変数も、システムレベルで定義されている限り使用できます。

次の例は、既成の環境変数を示しています。

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

次の例は、カスタムシステム環境変数を示しています。

- カスタム変数名: `app`
- カスタム変数値: `%programfiles%\Application\`
- 許可リストエントリ: `CTXCVC1,%app%\run.exe`

> **注:**
>
> ユーザー環境変数はサポートされていません。

> 環境変数のサポートは、Citrix Virtual Apps and Desktops バージョン 2209 以降で利用できます。

仮想チャネル名とプロセスを取得する

VDA マシン上で仮想チャネル名とそれを開くプロセスを取得する最も簡単な方法は、仮想チャネルを提供した開発者またはサードパーティベンダーから情報を入手することです。

または、機能のログを適用し、次の手順に従って情報を取得することもできます。

1. カスタム仮想チャネルのクライアントコンポーネントとサーバーコンポーネントが配置されたら、仮想アプリケーションまたは仮想デスクトップを起動します。
2. VDA マシンのシステムイベントログで、カスタム仮想チャネルの名前と、それを開こうとしたプロセスを探します。利用可能なイベントの詳細については、「イベントログ」を参照してください。
3. セッションからログアウトします。
4. 特定された仮想チャネルとプロセスについて、仮想チャネル許可リストポリシー設定にエントリを追加します。
5. マシンを再起動します。
6. VDA が登録されたら、仮想アプリケーションまたは仮想デスクトップを実行して、カスタム仮想チャネルが正常に開くことを検証します。

Citrix仮想チャネルに関する考慮事項

すべての組み込みCitrix仮想チャネルは信頼されており、追加設定なしで開くことが許可されています。ただし、以下の2つの機能は、外部依存関係のため、許可リストに明示的なエントリを必要とします。

- マルチメディアリダイレクト

- Skype for Business 用 HDX リアルタイム最適化パック

マルチメディアリダイレクト

システムのメディアプレーヤーとしてWindows Media Player以外のメディアプレーヤーを使用する場合、信頼されたプロセスとして許可リストに追加する必要があります。許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXMM`
- プロセス: VDAマシンで使用されるメディアプレーヤーへのパス。例: `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`。
- 許可リストエントリ: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

Skype for Business 用 HDX リアルタイム最適化パック

許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXRMEP`
- プロセス: VDAマシン内のSkype for Business実行可能ファイルへのパス。これはSkype for Businessのバージョンやカスタムインストールパスの使用によって異なる場合があります。例: `C:\Program Files\Microsoft Office\root\Office16\lync.exe.`.
- 許可リストエントリ: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

VDA と Delivery Controller™ 間の WebSocket 通信

この記事では、WCF通信の代替として、VDAとDelivery Controller間の通信にWebSocket接続を設定する方法について説明します。これにより、VDAからDelivery Controllerへの通信にTLSポート443のみを使用できるという利点があります。

現在、これはMCSプロビジョニングされたマシンでのみ利用可能です。手動でプロビジョニングされたマシンはテクニカルプレビュー段階です。詳細については、/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-manage#enroll-non-mcs-provisioned-vdas-using-tokens-preview)を参照してください。

動作の仕組み

次のセクションでは、Delivery ControllerとVDA間のWebSocket接続のワークフローについて説明します。

1. Citrix Virtual Apps and Desktops™管理者は、Machine Creation Service (MCS)を使用してVDAをプロビジョニングすることでプロセスを開始します。
2. MCSプロビジョニングプロセス中に、MCSは各VDAの公開鍵と秘密鍵のペアを生成し、公開鍵をDelivery Controller上のFMAトラストサービスに登録します。MCSは、公開鍵と秘密鍵のペアをVDAのIDディスク下のファイルとして保存します。
3. VDAマシンが起動すると、VDAマシンにインストールされているMCSエージェントは、IDディスクからキーペアを読み取り、この情報をVDAレジストリの場所に書き込みます。
4. VDAにインストールされているブローカーエージェントは、レジストリからキーペアを読み取り、秘密鍵で署名されたサービスキーを含むSSL対応のWebSocketリクエストをDelivery Controllerに生成します。
5. Delivery Controllerは、FMAトラストサービスからの公開鍵を使用して、署名されたサービスキー認証ヘッダーを検証します。
6. 検証が完了すると、システムはVDAとDelivery Controller間のWebSocket接続を確立します。

WebSocket のサポート

始める前に

1. サイトを構成します。詳細については、「サイトの作成」を参照してください。
2. Delivery ControllerにTLS証明書をインストールします。詳細については、「ControllerにTLSサーバー証明書をインストールする」を参照してください。
3. VDAにルートCAと中間CAをインストールして、Delivery Controllerを信頼します。

手順

WebSocket 接続を設定するには、次の手順に従います。

1. Delivery ControllerでWebSocket接続を有効にします。サイト上の各Delivery Controllerで次のコマンドを実行します。

   ```
   New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy" -Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -Force
   ```

   > **注:**
   >
   > WebSocketを有効にした後、必ずDelivery Controllerを再起動してください。

2. MCSプロビジョニングを使用して、AD参加済みVDA用のマシンカタログを作成します。詳細については、「マシンカタログの作成」を参照してください。
3. デリバリーグループを作成し、VDAを追加します。詳細については、「デリバリーグループの作成」を参照してください。
4. VDAでWebSocket接続を有効にします。VDAで次のPowerShellコマンドを実行します。

```
New-ItemProperty
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAgent
\WebSocket" -Name "Enabled" -PropertyType "DWord" -Value 1 -Force
```

   - WebSocketが有効になっているか確認するには、次のレジストリキーの値を確認します。`Enabled`の値は1である必要があります。

     キー:

     ```
     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAge
     nt\WebSocket
     ```

     名前: Enabled

     種類: REG_DWORD

     値: 1

HDX™ 接続性

Citrix HDX は、あらゆるデバイスおよびあらゆるネットワーク経由で、集中型アプリケーションおよびデスクトップのユーザーに高精細なエクスペリエンスを提供する幅広いテクノロジーのセットです。

HDXは、次の3つの技術原則に基づいて設計されています。

- インテリジェントなリダイレクト
- 適応型圧縮
- データ重複排除

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

HDXの機能では、独自のプロプライエタリなトランスポートプロトコル経由で接続し、セッション確立時に最大伝送ユニットを利用し、Citrix SD-WANで接続性を最適化できます。

アダプティブトランスポート

アダプティブトランスポートは、Citrix Virtual Apps and Desktops™ のメカニズムであり、優先トランスポートプロトコルを使用してHDXセッションの接続を確立し、優先プロトコルでの接続が利用できない場合はTCPにフォールバックします。

次のトランスポートプロトコルがサポートされています。

- エンライトンド データ トランスポート (EDT)
- 伝送制御プロトコル (TCP)

構成

アダプティブトランスポートはデフォルトで有効になっています。アダプティブトランスポートは以下のモードで動作するように構成できます。

- **優先**: (デフォルト) クライアントは優先プロトコルでの接続を試行し、優先プロトコルでの接続が利用できない場合はTCPにフォールバックします。

- **診断モード**: クライアントは優先プロトコルのみを使用して接続を試行します。TCPへのフォールバックは無効になります。
- **オフ**: クライアントはTCPのみを使用して接続を試行します。

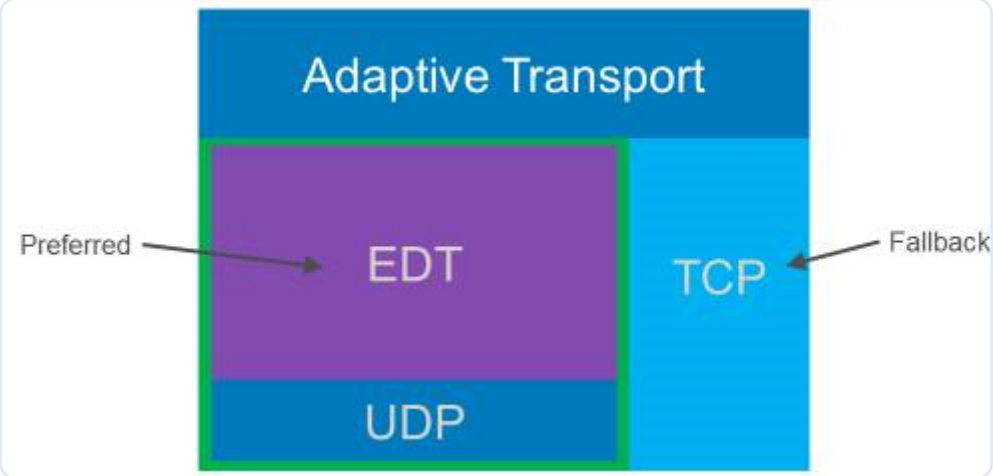
動作の仕組み

アダプティブトランスポートが`Preferred`に設定されている場合、クライアントは優先プロトコルとTCPの両方でセッションへの接続を並行して試行します。これにより、優先プロトコルで接続できない場合にクライアントがTCPにフォールバックする必要がある場合でも、接続時間を最適化できます。TCPを使用して接続が確立された場合、クライアントは5分ごとにバックグラウンドで優先プロトコルでの接続を試行します。

アダプティブトランスポートが`Diagnostic mode`に設定されている場合、クライアントは優先プロトコルのみを使用してセッションに接続します。クライアントが優先プロトコルを使用して接続を確立できない場合、TCPにフォールバックせず、接続は失敗します。

アダプティブトランスポートが`Off`に設定されている場合、**アダプティブトランスポート**は無効になり、クライアントはTCPのみを使用してセッションに接続します。

ネットワークスタック(/en-us/citrix-virtual-apps-desktops/2407/media/hdx-1.png)



システム要件

アダプティブトランスポートとEDTを使用するための要件は次のとおりです。

- コントロールプレーン
  - シトリックス DaaS (旧シトリックス バーチャル アプリケーションズ アンド デスクトップス サービス)
  - Citrix Virtual Apps and Desktops: 現在サポートされているバージョン

- 仮想デリバリーエージェント
  - Windows: 現在サポートされているバージョン（2402以降を推奨）
  - Linux: 現在サポートされているバージョン（2402以降を推奨）
- Citrix Workspace™アプリ
  - Windows: 現在サポートされているバージョン（2402以降を推奨）
  - Linux: 現在サポートされているバージョン（2402以降を推奨）
  - Mac: 現在サポートされているバージョン（2402以降を推奨）
  - iOS: Apple App Storeで入手可能な最新バージョン
  - Android: Google Playで入手可能な最新バージョン
- Citrix NetScaler® ゲートウェイ
  - 14.1.12.30以降 (推奨)
  - 13.1.17.42以降 (13.1-52.19以降を推奨)

> **注:**
>
> Linux VDA の詳細については、Linux Virtual Delivery Agent ドキュメントを参照してください。

ネットワーク要件

以下は、アダプティブトランスポートでEDTを使用するためのネットワーク要件です。

セッションホスト

セッションホストに Windows Defender ファイアウォールなどのファイアウォールがある場合、内部接続のために以下の受信トラフィックを許可する必要があります。

説明	送信元	プロトコル	ポート
内部接続 - セッションの信頼性が有効	クライアント	UDP	2598
内部接続 - セッションの信頼性が無効			1494

説明	送信元	プロトコル	ポート
内部接続 - HDX™ DirectまたはVDA SSL			443

注:

VDAインストーラーは、Windows Defender ファイアウォールに適切な受信規則を追加します。別のファイアウォールを使用する場合は、上記の規則を追加する必要があります。

内部ネットワーク

次の表は、ネットワークでEDTを使用するために必要なファイアウォール規則を示しています。

説明	プロトコル	送信元	宛先	宛先ポート
直接内部接続 - セッションの信頼性が有効	UDP	クライアントネットワーク	VDAネットワーク	2598
直接内部接続 - セッションの信頼性が無効				1494
直接内部接続 - HDX DirectまたはVDA SSL				443
ネットスケーラー ゲートウェイ		NetScaler SNIP		2598
ネットスケーラー ゲートウェイ - VDA SSL				443

注:

Citrix Gateway Serviceを使用している場合、トランスポートプロトコルとしてEDTを使用するには、**Rendezvous**を有効にする必要があります。システムおよびネットワーク要件については、Rendezvousのドキュメントを参照してください。

クライアントネットワーク

以下の表は、クライアントデバイスの接続要件を示しています。

説明	プロトコル	送信元	宛先	宛先ポート
内部接続 - セッションの信頼性が有効	UDP	クライアントIP	VDAネットワーク	2598
内部接続 - セッションの信頼性が無効				1494
内部接続 - HDX Direct または SSL VDA				443
外部接続 - NetScaler Gateway			NetScaler Gateway のパブリック IP アドレス	443
外部接続 - Citrix Gateway Service			Citrix Gateway サービス	443

注記：

Citrix Gateway Serviceを使用している場合、クライアントは`<https://*.*.nssvc.net>`に到達できる必要があります。`<https://*.*.nssvc.net>`を使用してすべてのサブドメインを許可できない場合は、代わりに`<https://*.c.nssvc.net>`と`<https://*.g.nssvc.net>`を使用できます。詳細については、Knowledge Centerの記事CTX270584を参照してください。

適応型データ転送

Enlightened Data Transport (EDT) は、User Datagram Protocol (UDP) 上に構築された Citrix 独自のトランスポートプロトコルです。これは、サーバーのスケーラビリティを維持しながら、困難な長距離接続で優れたユーザーエクスペリエンスを提供します。EDT は、信頼性の低いネットワーク上のすべての ICA® 仮想チャネルのデータスループットを向上させ、より優れた一貫性のあるユーザーエクスペリエンスを提供します。

アダプティブトランスポートが有効な場合、EDT が優先プロトコルです。

知っておくべきこと

- NetScaler® Gateway および Citrix Gateway Service で **MTU Discovery** と EDT を使用するには、**セッションの信頼性**を有効にする必要があります。
- パケットの断片化は、パフォーマンスの低下、場合によってはセッションを開くことの失敗を引き起こす可能性があります。これを防ぐには、EDT MTU をネットワークに適した値に調整する必要があります。EDT MTU Discovery を使用するか、非標準 MTU のネットワークで EDT を使用する場合の MSS の構成方法 で説明されている手動の回避策を使用できます。
- NetScaler Gateway で EDT の使用を有効にする方法の詳細については、「Enlightened Data Transport をサポートするように NetScaler Gateway を構成する」を参照してください。

EDT MTU検出

MTU Discovery を使用すると、EDT はセッション確立時に最大伝送単位 (MTU) を自動的に決定できます。これにより、パフォーマンスの低下やセッション確立の失敗につながる可能性のある EDT パケットの断片化を防ぎます。

MTU Discovery はデフォルトで有効になっています。無効にする必要がある場合は、詳細について「レジストリで管理される HDX 機能」を参照してください。

> **注:**
>
> - MTU Discovery が機能するには、**セッションの信頼性**を有効にする必要があります。
> - Multi-Stream ICA を使用した MTU Discovery は、VDA バージョン 2209 以降で利用できます。

トラブルシューティング

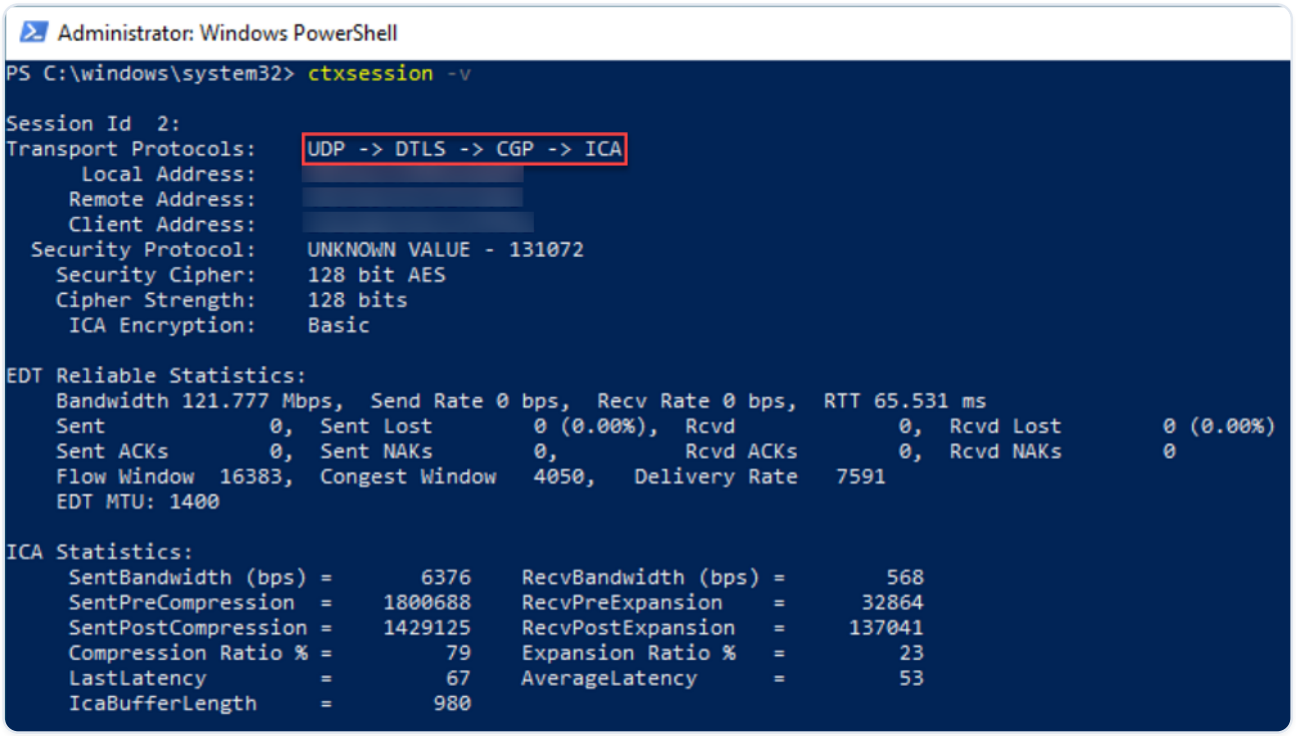
セッションのトランスポートプロトコルとしてEDTが使用されていることを確認するには、DirectorまたはVDA上の`CtxSession.exe`コマンドラインユーティリティを使用できます。

Directorでセッションを検索し、**詳細**を選択します。**接続の種類**が`HDX`で、**プロトコル**が`UDP`の場合、EDTがセッションのトランスポートプロトコルとして使用されています。

EDT ディレクター(/en-us/citrix-virtual-apps-desktops/2407/media/edt-director.png)

CtxSession.exeユーティリティを使用するには、セッション内でコマンドプロンプトまたはPowerShellを起動し、`ctxsession.exe`を実行します。詳細な統計を表示するには、`ctxsession.exe -v`を実行します。EDTが使用されている場合、トランスポートプロトコルは次のいずれかを表示します。

- **UDP > ICA®** (セッションの信頼性が無効)
- **UDP > CGP > ICA** (セッションの信頼性が有効)
- **UDP > DTLS > CGP > ICA** (ICAはDTLSでエンドツーエンド暗号化されています)



EDTでセッションが接続に失敗する場合

Adaptive Transportと**EDT**のトラブルシューティングには、以下をお勧めします。

1. システム要件、ネットワーク要件、既知の問題、および注意事項を確認し、すべての項目が対処されていることを確認してください。

2. StudioまたはGPOで、目的の**HDXアダプティブトランスポート**設定を上書きするCitrix®ポリシーがないか確認してください。
3. クライアント側で、目的のHDXアダプティブトランスポート設定を上書きする設定がないか確認してください。これは、GPO設定、オプションのWorkspaceアプリ管理テンプレートを使用して構成された設定、またはレジストリやクライアントの構成ファイルでの**HDXoverUDP**設定の手動構成である可能性があります。
4. マルチセッションVDAマシンでは、UDPリスナーがアクティブであることを確認してください。VDAマシンでコマンドプロンプトを開き、`netstat -a -p udp`を実行します。詳細については、「HDX Enlightened Data Transportプロトコルを確認する方法」を参照してください。
5. ネットワークファイアウォールとVDAマシン上で実行されているファイアウォールの両方で、適切なファイアウォールルールが構成されているか確認します。
6. NetScaler® GatewayまたはCitrix Gateway Serviceをバイパスして、内部で直接セッションを起動し、使用中のプロトコルを確認します。セッションがEDTを使用している場合、VDAはNetScaler GatewayまたはCitrix Gateway Serviceを介した外部接続にEDTを使用する準備ができています。
7. EDTが内部の直接接続では機能するが、NetScaler GatewayまたはCitrix Gateway Serviceを介するセッションでは機能しない場合：

   - **セッションの信頼性**が有効になっていることを確認します。
   - NetScaler Gatewayを使用している場合は、(/ja-jp/netscaler-gateway/current-release/hdx-enlightened-data-transport-support/configuring-citrix-gateway.html)に記載されている必要な構成に準拠していることを確認してください。

8. Citrix Gateway Serviceを使用している場合は、Rendezvousが有効になっており、機能していることを確認します。
9. ユーザーの接続に非標準のMTUが必要かどうかを確認します。実効MTUが1500バイト未満の接続では、EDTパケットの断片化が発生し、パフォーマンスに影響を与えたり、セッション起動の失敗を引き起こしたりする可能性があります。この問題は、VPN、一部のWi-Fiアクセスポイント、および4Gや5Gなどのモバイルネットワークを使用している場合に一般的です。MTU検出が有効になっているか、(https://support.citrix.com/article/CTX231821/how-to-configure-mss-when-using-edt-on-networks-with-nonstandard-mtu)に記載されているようにカスタムMTUを設定していることを確認してください。

既知の問題

- 非対称ネットワークパスは、NetScaler GatewayまたはCitrix Gateway Serviceを介さない接続でMTU検出が失敗する原因となる可能性があります。この問題に対処するには、VDAバージョン2103以降にアップグレードしてください。
- NetScaler Gatewayを使用している場合、非対称ネットワークパスはMTU検出の失敗を引き起こす可能性があります。これは、Gatewayの問題により、EDTパケットヘッダーのDon't Fragment (DF) ビットが伝播されないためです。この問題の修正は、ファームウェアリリース13.1ビルド17.42以降で利用可能です。修正を有効にする方法の詳細については、(/ja-jp/netscaler-gateway/current-release/hdx-enlightened-data-transport-support/pmtud-support-on-citrix-gateway.html)を参照してください。
- DS-Liteネットワークを介して接続するユーザーの場合、MTU検出が失敗することがあります。一部のモデムでは、パケット処理が有効になっている場合にDFビットが尊重されず、MTU検出が断片化を検出できないことがあります。この状況では、以下のオプションが利用可能です。
  - ユーザーのモデムでパケット処理を無効にします。
  - **MTU検出**を無効にし、非標準MTUのネットワークでEDTを使用する場合のMSSの構成方法に記載されているようにハードコードされたMTUを使用します。
  - **アダプティブトランスポート**を無効にして、セッションがTCPを使用するように強制します。一部のユーザーのみが影響を受ける場合は、他のユーザーがEDTを引き続き使用できるように、クライアント側で無効にすることを検討してください。

HDX™ Direct (プレビュー)

Citrixが提供するリソースにアクセスする場合、HDX Directにより、直接通信が可能な場合に内部および外部のクライアントデバイスの両方がセッションホストとの安全な直接接続を確立できます。

> **重要:**
>
> HDX Direct は現在プレビュー版です。この機能はサポート対象外であり、本番環境での使用はまだ推奨されていません。フィードバックを送信したり、問題を報告したりするには、このフォームを使用してください。

システム要件

HDX Directを使用するためのシステム要件は以下のとおりです。

- コントロールプレーン
  - シトリックス DaaS™
  - Citrix Virtual Apps and Desktops™ 2402以降のバージョン
- バーチャル デリバリー エージェント (VDA)
  - Windows: バージョン2402以降
- Workspaceアプリ
  - Windows: バージョン2402以降
- アクセスティア
  - シトリックス ゲートウェイ サービスを備えたシトリックス ワークスペース™
  - シトリックス ワークスペース と NetScaler® Gateway
- その他
  - 外部からの直接接続には、Adaptive Transportを有効にする必要があります

ネットワーク要件

HDX Directを使用するためのネットワーク要件は次のとおりです。

セッションホスト

セッションホストにWindows Defender Firewallなどのファイアウォールがある場合、内部接続のために次の受信トラフィックを許可する必要があります。

説明	送信元	プロトコル	ポート
直接内部接続	クライアント	TCP	443
直接内部接続	クライアント	UDP	443

> 注:

> VDA インストーラーは、Windows Defender ファイアウォールに適切な受信規則を追加します。別のファイアウォールを使用する場合は、上記の規則を追加する必要があります。

クライアントネットワーク

以下の表は、内部および外部ユーザー向けのクライアントネットワークについて説明しています。

内部ユーザー

説明	プロトコル	ソース	ソースポート	宛先	宛先ポート
直接内部接続	TCP	クライアントネットワーク	1024–65535	VDAネットワーク	443
直接内部接続	UDP	クライアントネットワーク	1024–65535	VDAネットワーク	443

外部ユーザー

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
STUN (外部ユーザーのみ)	UDP	クライアントネットワーク	1024–65535	インターネット (下記の注記を参照)	3478, 19302
外部ユーザー接続	UDP	クライアントネットワーク	1024–65535	データセンターのパブリックIPアドレス	1024–65535

データセンターネットワーク

以下の表は、内部ユーザーと外部ユーザー向けのデータセンターネットワークについて説明しています。

内部ユーザー

説明	プロトコル	ソース	送信元ポート	宛先	宛先ポート
直接内部接続	TCP	クライアントネットワーク	1024–65535	VDAネットワーク	443
直接内部接続	UDP	クライアントネットワーク	1024–65535	VDAネットワーク	443

外部ユーザー

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
STUN (外部ユーザーのみ)	UDP	VDAネットワーク	1024–65535	インターネット (下記の注記を参照)	3478, 19302
外部ユーザー接続	UDP	DMZ / 内部ネットワーク	1024–65535	VDAネットワーク	55000–55250
外部ユーザー接続	UDP	VDAネットワーク	55000–55250	クライアントのパブリックIP	1024–65535

注:

VDAとWorkspaceアプリの両方が、以下のサーバーに同じ順序でSTUNリクエストを送信しようとします。

- stunserver.stunprotocol.org:3478
- employees.org:3478
- stun.l.google.com:19302

> **HDX Directポート範囲**ポリシー設定を使用して外部ユーザー接続のデフォルトポート範囲を変更した場合、対応するファイアウォールルールはカスタムポート範囲と一致している必要があります。

構成

HDX Directはデフォルトで無効になっています。この機能は、Citrixポリシーの**HDX Direct**設定を使用して構成できます。

- **HDX Direct**：機能を有効または無効にします。
- **HDX Directモード**：**HDX Direct**が内部クライアントのみに利用可能か、内部クライアントと外部クライアントの両方に利用可能かを決定します。
- **HDX Directポート範囲**：VDAが外部クライアントからの接続に使用するポート範囲を定義します。

考慮事項

HDX Directを使用する際の考慮事項は次のとおりです。

- 外部ユーザー向けのHDX Directは、トランスポートプロトコルとしてEDT (UDP) を使用する場合にのみ利用可能です。したがって、**アダプティブトランスポート**を有効にする必要があります。
- **HDX Insight**を使用している場合、**HDX Direct**を使用すると、セッションがNetScaler Gatewayを介してプロキシされなくなるため、HDX Insightのデータ収集が妨げられることに注意してください。
- 仮想アプリおよびデスクトップに非永続マシンを使用する場合、Citrix では、マスター/テンプレートイメージではなくセッションホストで **HDX Direct** を有効にすることをお勧めします。これにより、各マシンが独自の証明書を生成します。
- HDX Direct で独自の証明書を使用することは、現在サポートされていません。

動作の仕組み

HDX Directを使用すると、直接通信が可能な場合、クライアントはセッションホストへの直接接続を確立できます。HDX Directを使用して直接接続が行われる場合、ネットワークレベルの暗号化 (TLS/DTLS) を使用して直接接続を保護するために、自己署名証明書が使用されます。

内部ユーザー

次の図は、内部ユーザーのHDX Direct接続プロセスの概要を示しています。

HDX Directの概要(/en-us/citrix-virtual-apps-desktops/2407/media/hdx-direct-overview.png)

1. クライアントはGateway Serviceを介してHDXセッションを確立します。
2. 接続が成功すると、VDAは、HDX接続を介して、VDAマシンのFQDN、そのIPアドレスのリスト、およびVDAマシンの証明書をクライアントに送信します。
3. クライアントはIPアドレスをプローブして、VDAに直接到達できるかどうかを確認します。
4. クライアントが共有されたいずれかのIPアドレスでVDAに直接到達できる場合、クライアントは、手順 (2) で交換された証明書と一致する証明書を使用して、(D)TLSで保護されたVDAとの直接接続を確立します。
5. 直接接続が正常に確立されると、セッションは新しい接続に転送され、Gateway Serviceへの接続は終了します。

> **注:**
>
> 上記のステップ2で接続を確立した後、セッションはアクティブになります。その後の手順は、ユーザーが仮想アプリケーションまたはデスクトップを使用する能力を遅らせたり、妨げたりすることはありません。その後の手順のいずれかが失敗した場合でも、ユーザーのセッションを中断することなく、Gateway経由の接続は維持されます。

外部ユーザー

次の図は、外部ユーザー向けのHDX Direct接続プロセスの概要を示しています。

HDX Direct接続プロセス(/en-us/citrix-virtual-apps-desktops/2407/media/hdx-direct-connection-process.png)

1. クライアントはGateway Serviceを介してHDXセッションを確立します。
2. 接続が成功すると、クライアントとVDAの両方がSTUNリクエストを送信して、それぞれのパブリックIPアドレスとポートを検出します。
3. STUNサーバーは、クライアントとVDAにそれぞれのパブリックIPアドレスとポートで応答します。
4. HDX接続を介して、クライアントとVDAはそれぞれのパブリックIPアドレスとUDPポートを交換し、VDAはクライアントに証明書を送信します。
5. VDAはクライアントのパブリックIPアドレスとUDPポートにUDPパケットを送信します。クライアントはVDAのパブリックIPアドレスとUDPポートにUDPパケットを送信します。

6. VDAからのメッセージを受信すると、クライアントはセキュアな接続リクエストで応答します。
7. DTLSハンドシェイク中に、クライアントは証明書がステップ(4)で交換された証明書と一致することを確認します。検証後、クライアントは認証トークンを送信します。これでセキュアな直接接続が確立されます。
8. 直接接続が正常に確立されると、セッションは新しい接続に転送され、Gateway Serviceへの接続は終了します。

> **注:**
>
> 上記のステップ2で接続を確立した後、セッションはアクティブになります。その後の手順は、ユーザーが仮想アプリケーションまたはデスクトップを使用する能力を遅らせたり、妨げたりすることはありません。その後の手順のいずれかが失敗した場合でも、ユーザーのセッションを中断することなく、Gateway経由の接続は維持されます。

証明書管理

セッションホスト

VDA マシン上の次の2つのサービスは、証明書の作成と管理を処理します。どちらもマシンの起動時に自動的に実行されるように設定されています。

- Citrix ClxMtp Service: CA証明書キーの生成とローテーションを担当します。
- Citrix Certificate Manager Service: 自己署名ルートCA証明書とマシン証明書の生成と管理を担当します。

次の手順は、証明書管理プロセスを示しています。

1. サービスはマシンの起動時に開始されます。
2. `Citrix ClxMtp Service` は、まだ作成されていない場合にキーを作成します。
3. Citrix Certificate Manager Serviceは、**HDX Direct**が有効になっているかを確認します。有効でない場合、サービスは自身を停止します。
4. **HDX Direct**が有効になっている場合、Citrix Certificate Manager Serviceは自己署名ルートCA証明書が存在するかを確認します。存在しない場合、自己署名ルート証明書が作成されます。
5. ルートCA証明書が利用可能になると、Citrix Certificate Manager Serviceは自己署名マシン証明書が存在するかを確認します。存在しない場合、サービスはキーを生成し、マシンのFQDNを使用して新しい証明書を作成します。

6. Citrix Certificate Manager Serviceによって作成された既存のマシン証明書があり、サブジェクト名がマシンのFQDNと一致しない場合、新しい証明書が生成されます。

> **注:**
>
> Citrix Certificate Manager Serviceは、2048ビットキーを利用するRSA証明書を生成します。

クライアントデバイス

安全な**HDX Direct**接続を正常に確立するには、クライアントはセッションを保護するために使用される証明書を信頼する必要があります。これを容易にするために、クライアントはICA®ファイル（Workspaceによって提供される）を介してセッションのCA証明書を受け取るため、CA証明書をクライアントデバイスの証明書ストアに配布する必要はありません。

NAT互換性

外部ユーザーデバイスとセッションホスト間の直接接続を確立するために、HDX™ Directは、NATトラバーサルのためのホールパンチングと、クライアントデバイスおよびセッションホストのパブリックIPアドレスとポートマッピングの交換を容易にするSTUNを活用します。これは、VoIP、ユニファイドコミュニケーション、P2Pソリューションの仕組みに似ています。

ファイアウォールやその他のネットワークコンポーネントがSTUNリクエストおよびHDXセッションのUDPトラフィックを許可するように構成されている限り、外部ユーザー向けのHDX Directは機能すると予想されます。ただし、ユーザーとセッションホストのネットワークのNATタイプが互換性のない組み合わせとなり、HDX Directが失敗する特定のシナリオがあります。

検証

STUNTMANのSTUNクライアントユーティリティを使用して、クライアントとセッションホストのNATタイプを検証できます。

1. stunprotocol.orgからターゲットプラットフォームに適したパッケージをダウンロードし、内容を抽出します。
2. ターミナルプロンプトを開き、内容が抽出されたディレクトリに移動します。
3. 次のコマンドを実行します: `.\stunclient.exe stunserver2024.stunprotocol.org --mode behavior`
4. 出力を記録します。

バインディングテストと動作テストが成功した場合、**バインディングテスト**と**動作テスト**の両方が成功を報告し、NAT動作が指定されます。



テストが失敗した場合、**バインディングテスト**と**動作テスト**の両方が失敗を報告します。



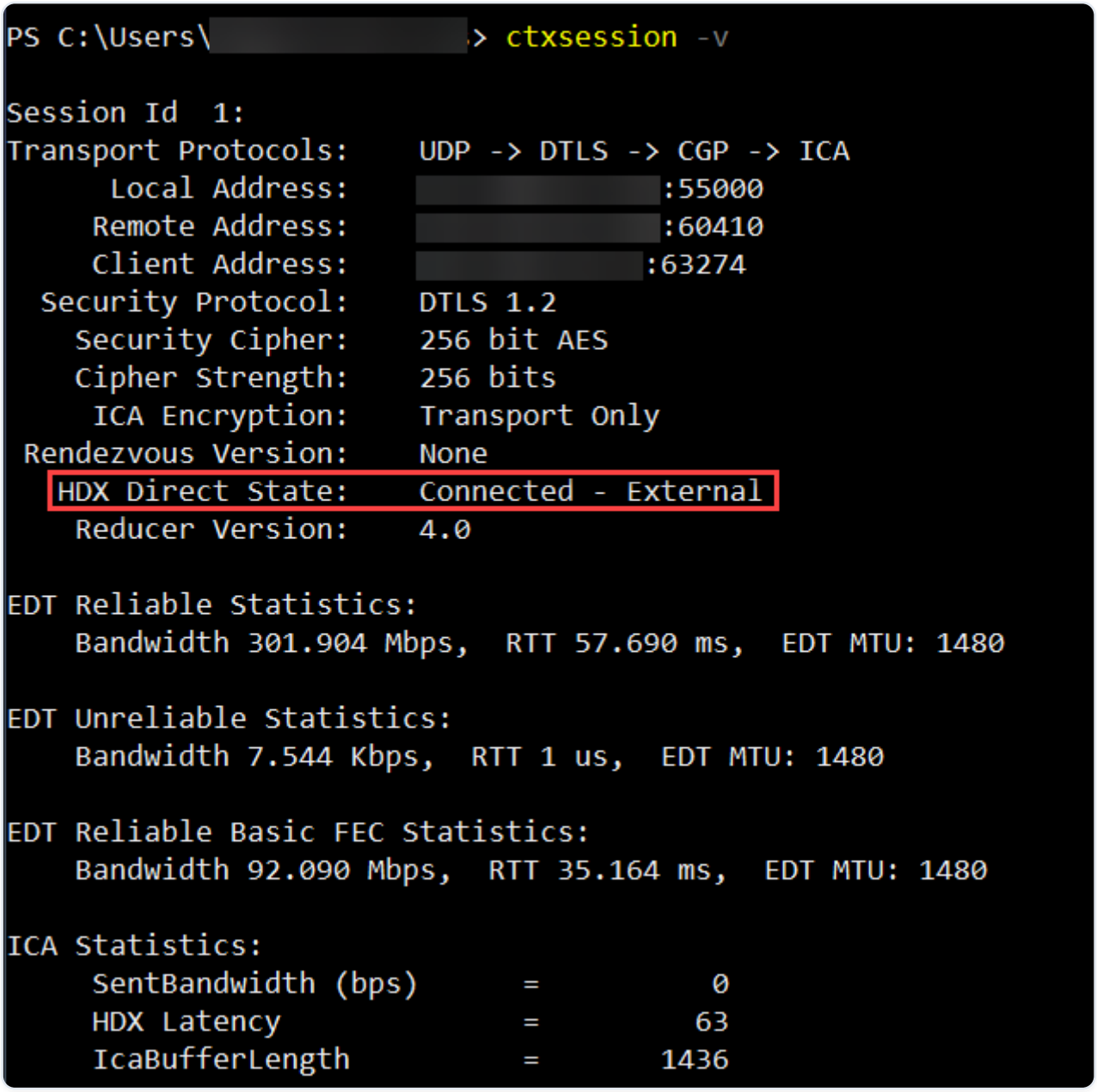
クライアントとセッションホストの両方のテスト結果に基づいて、外部ユーザー向けのHDX Directが機能するかどうかを判断するには、次の表を参照してください。

クライアントデバイス	セッションホスト	動作が期待されますか？
エンドポイント独立マッピング	エンドポイント独立マッピング	はい
エンドポイント独立マッピング	エンドポイント依存マッピング	はい
エンドポイント依存マッピング	エンドポイント独立マッピング	はい
エンドポイント依存マッピング	エンドポイント依存マッピング	いいえ
アドレスとポート依存マッピング	任意のNATタイプ	いいえ
任意のNATタイプ	アドレスとポート依存マッピング	いいえ
失敗	任意のNATタイプ	いいえ
任意のNATタイプ	失敗	いいえ
失敗	失敗	いいえ

トラブルシューティング

HDX Direct が直接接続を正常に確立したことを確認するには、VDA マシンで `CtxSession.exe` ユーティリティを使用できます。

`CtxSession.exe` ユーティリティを使用するには、セッション内でコマンドプロンプトまたは PowerShell を起動し、`ctxsession.exe -v` を実行します。**HDX Direct** 接続が正常に確立されると、**HDX Direct Status** は `Connected` になります。



セッションホストのイベントログで、HDX™ Direct 接続が正常に確立されたか、失敗したかに関する情報を確認することもできます。詳細については、「**イベントログ**」セクションを参照してください。

> 注:

> 環境およびセッションホストで利用可能な IP アドレスの数によっては、HDX Direct 接続が確立されるまでに最大 5 分かかる場合があります。

HDX Direct が直接接続を確立できない場合

HDX Direct が直接接続を確立できない場合は、次の手順を確認してください。

1. 使用している VDA バージョンと Workspace アプリバージョンが、システム要件に従ってこの機能をサポートしていることを確認します。
2. HDX Direct を有効にするポリシーが VDA に適用されており、この機能を無効にする優先度の高い他のポリシーがないことを確認します。
3. 目的の HDX Direct モードを設定するポリシーが VDA に適用されており、構成を上書きする優先度の高い他のポリシーがないことを確認します。
4. Citrix ClxMtp Service がセッションホストで実行されていることを確認します。
5. Citrix Certificate Manager Service がセッションホストで実行されていることを確認します。実行されていない場合は、手動で起動してみてください。HDX Direct が無効になっている場合、このサービスは自動的に停止します。
6. セッションホストに自己署名ルート CA 証明書があるかどうかを確認します。
    a. 発行先: `CA-<hostname>` (例: CA-FTLW11-001)
    b. 発行元: `CA-<hostname>` (例: CA-FTLW11-001)
    c. 発行者の詳細: 組織はCitrix Systems, Inc.です。
7. セッションホストに自己署名サーバー証明書があるか確認してください:
    a. 発行先: `<host FQDN>` (例: FTLW11-001.ctxlab.net)
    b. 発行元: `CA-<hostname>` (例: CA-FTLW11-001)
    c. 発行者情報: 組織はCitrix Systems, Inc.です。
8. 証明書が見つからない場合は、Citrixテクニカルサポートにお問い合わせください。
9. 証明書が存在する場合:
    a. セッションホスト上でCitrix Certificate Managerサービスを停止します。
    b. 自己署名ルートCA証明書と自己署名サーバー証明書の両方を削除します。
    c. セッションホスト上でCitrix Certificate Managerサービスを開始します。サービスが開始されると、新しい証明書が作成されます。

10. 内部ユーザーの場合:

    a. セッションホストのファイアウォールが、HDX over EDTおよびHDX over TCPのインバウンドトラフィックをそれぞれUDP 443またはTCP 443でブロックしていないことを確認してください。

    b. クライアントネットワークとセッションホストネットワークの間で、ネットワークファイアウォールがUDP 443およびTCP 443上のトラフィックをブロックしていないことを確認してください。

11. 外部ユーザーの場合：

    a. クライアントとセッションホストのNATタイプを確認し、その組み合わせが機能することが期待されることを確認します。詳細については、「NAT互換性」セクションを参照してください。

    b. クライアントまたはセッションホストのいずれかでNATテストが失敗した場合：

        i. システムでファイアウォールが実行されている場合は、UDP 3478での送信トラフィックをブロックしていないことを確認してください。

        ii. ネットワークファイアウォールがUDP 3478での送信トラフィックをブロックしていないことを確認してください。

        iii. ファイアウォールがSTUNサーバーの応答をブロックしていないことを確認してください。

    c. ネットワークファイアウォールに、必要なすべてのトラフィックを許可するための適切なルールが構成されていることを確認してください。詳細については、「ネットワーク要件」セクションを参照してください。

    d. HDX Directポート範囲ポリシー設定を使用してデフォルトのポート範囲を変更する場合は、ファイアウォールルールがカスタムポート範囲に設定されていることを確認してください。

イベントログ

次のイベントがVDAマシンのイベントログに記録されます。

ログ	ID	送信元	レベル	説明
アプリケーションとサービスログ > Citrix-HostCore-HDX	1	HDX ダイレクト	情報	内部ユーザー `<username>` のHDX Direct接

ログ	ID	送信元	レベル	説明
Direct/Operational				続が確立されました。
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/Operational	2	HDX ダイレクト	情報	外部ユーザー `<username>` のHDX Direct接続が確立されました。
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/Operational	3	HDX ダイレクト	情報	ユーザー `<username>` のHDX Direct接続が失敗しました。

既知の問題

HDX Direct が、**HDX Direct** がすでに有効になっているマシンで VDA のインプレースアップグレードを実行した後、動作しなくなることがあります。 この問題を解決するには、次の手順を実行します。

1. セッションホストで Citrix Certificate Manager Service を停止します。
2. 自己署名ルートCA証明書と自己署名サーバー証明書を削除します。
3. レジストリを開きます。
4. `HKLM\Software\Citrix\HDX-Direct` キーを削除します。
5. `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd` にアクセスします。
6. **SSLEnabled** の値を `0` に設定します。
7. **SSLThumbprint** の値の内容を削除します。
8. **Citrix Certificate Managerサービス**を開始します。

Secure HDX™ (プレビュー)

Secure HDX は、トラフィックパス内のネットワーク要素が HDX トラフィックを検査できないようにする、アプリケーションレベル暗号化 (ALE) ソリューションです。Citrix Workspace™ アプリ

(クライアント) と VDA (セッションホスト) の間で、AES-256-GCM 暗号化を使用して、アプリケーションレベルで真のエンドツーエンド暗号化 (E2EE) を提供することでこれを実現します。

> **重要:**
>
> Secure HDX は現在プレビュー段階です。この機能はサポートなしで提供されており、本番環境での使用はまだ推奨されません。フィードバックを送信したり、問題を報告したりするには、こちらのフォームをご利用ください。

システム要件

以下のリストは、Secure HDX を使用するためのシステム要件を示しています。

- コントロールプレーン
  - シトリックス DaaS™
  - シトリックス バーチャルアプリおよびデスクトップ™ 2402 以降
- セッションホスト
  - オペレーティングシステム
    - ウィンドウズ 10 22H2
    - Windows 11 22H2 以降
    - ウィンドウズ サーバー 2019 以降
  - バーチャル デリバリー エージェント (VDA)
    - Windows: バージョン 2402 以降
    - Linux: バージョン 2407 以降
- Workspace アプリ
  - Windows: バージョン 2402 以降
  - Linux: バージョン 2408 以降
  - Mac: バージョン 2409 以降
  - Chrome OS: バージョン 2409 以降
  - HTML5: バージョン 2408 以降

- アクセス層
  - シトリックス ワークスペース
  - Citrix StoreFront™ 2402 以降

> **注：**
>
> Linux VDA で Secure HDX を構成する方法の詳細については、Linux VDA のドキュメントを参照してください。

構成

Secure HDX はデフォルトで無効になっています。この機能は、Citrix ポリシーの Secure HDX 設定を使用して構成できます。

Secure HDX：この機能は、すべてのセッションで有効にするか、直接接続でのみ有効にするか、または無効にするかを定義します。

考慮事項

Secure HDXを使用する際の考慮事項は次のとおりです。

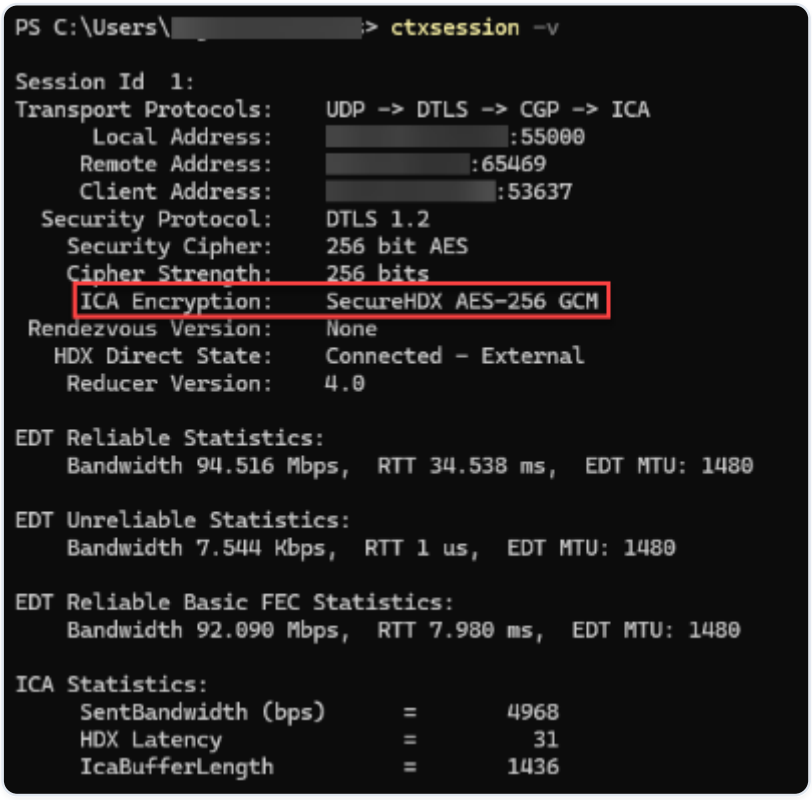
- ユーザーがSecure HDXが有効になっているセッションホストに、この機能をサポートしないクライアントを使用して接続しようとすると、接続は拒否されます。
- Secure HDXでは、Service Continuityは現在サポートされていません。Citrix Cloud™環境でService Continuityが有効になっている場合、クラウドサービスの停止時に、Secure HDXが有効になっているセッションホストに接続できなくなります。
- HDX Insightを使用している場合、Secure HDXを使用すると、NetScaler®が暗号化されたHDXトラフィックを検査できないため、HDX Insightのデータ収集が妨げられることに注意してください。HDX Insightを使用する必要がある場合は、Secure HDXを直接接続でのみ有効にするように設定できます。
- SmartControlを使用している場合、Secure HDXを使用すると、NetScalerが暗号化されたHDXトラフィックを検査できないため、SmartControlが機能しなくなることに注意してください。SmartControlを使用する必要がある場合は、Secure HDXを直接接続でのみ有効にするように設定できます。
- Secure HDXが有効になっている場合、Multi-Stream ICA®はサポートされません。

- HDXトラフィックの検査に依存するサードパーティソリューションを使用している場合、HDXトラフィックが暗号化されるため、Secure HDXを有効にするとそれらは機能しなくなります。
- Secure HDXを有効にしたいデリバリーグループでSecure ICAが有効になっている場合は、まずSecure ICAを無効にする必要があります（デリバリーグループの編集 > ユーザー設定）。

トラブルシューティング

Secure HDXがアクティブであることを確認するには、VDAマシンで`ctxsession.exe`ユーティリティを使用できます。

`CtxSession.exe`ユーティリティを使用するには、セッション内でコマンドプロンプトまたはPowerShellを開き、`ctxsession.exe -v`を実行します。Secure HDXが使用されている場合、ICA Encryptionは`SecureHDX AES-256 GCM`と表示されます。



セッションでSecure HDXが有効にならない場合

- 使用中のVDAバージョンが、システム要件に従ってこの機能をサポートしていることを確認してください。
- Secure HDXを有効にするポリシーがVDAに適用されており、この機能を無効にする優先度の高い他のポリシーがないことを確認してください。

- クライアントデバイスがNetScaler GatewayまたはGateway Serviceを介して接続している場合、Secure HDXが「直接接続のみ」に設定されていないことを確認してください。
- Secure HDXを設定したときにセッションホストがすでに実行中だった場合は、変更を有効にするためにマシンを再起動してください。

仮想チャネル許可リスト

仮想チャネル許可リストは、環境内でどの非Citrix仮想チャネルを許可するかを制御できる機能です。デフォルトでは、仮想チャネル許可リスト機能は有効になっています。その結果、Citrix Virtual Apps and Desktops™セッションでは、Citrix仮想チャネルのみが開くことが許可されます。自社製またはサードパーティ製のカスタム仮想チャネルを使用する必要がある場合は、それらを明示的に許可リストに追加する必要があります。

構成

仮想チャネル許可リストはデフォルトで有効になっています。この機能は、Citrixポリシーの以下の設定を使用して構成できます。

- **仮想チャネル許可リスト**: この機能を有効または無効にし、仮想チャネルをリストに追加します。
- **仮想チャネル許可リストログスロットリング**: 仮想チャネル許可リストイベントログのスロットリング期間を設定します。
- **仮想チャネル許可リストログ記録**: 仮想チャネル許可リストのログレベルを設定します。

仮想チャネルを許可リストに追加する

仮想チャネルを許可リストに追加するには、以下の情報が必要です。

1. コードで定義されている仮想チャネル名。最大7文字です。例: `CTXCVC1`。
2. VDAマシン上で仮想チャネルを開くプロセスのパス。例: `C:\Program Files\Application\run.exe`。

必要な情報が揃ったら、仮想チャネル許可リストポリシー設定を使用して仮想チャネルを許可リストに追加する必要があります。仮想チャネルをリストに追加するには、仮想チャネル名の後にコンマを入力し、次に仮想チャネルにアクセスするプロセスのパスを入力します。複数のプロセスがある場合は、各プロセスをコンマで区切って追加できます。

単一プロセスの場合

前の例を使用して、以下のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe
```

複数のプロセスの場合

複数のプロセスがある場合は、次のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

ワイルドカードの使用

ワイルドカード (*) の使用がサポートされています。ワイルドカードは、ディレクトリ名や実行可能ファイル名がアプリケーションのバージョンによって変更される場合や、サードパーティコンポーネントがユーザープロファイルにインストールされている場合に使用できます。

次のシナリオでワイルドカードを使用できます。

- ディレクトリ名全体を置き換える場合。 例: `C:\Program Files\Application*\run1.exe`
- ディレクトリ名の一部を置き換える場合。 例: `C:\Program Files\Application\v*\run1.exe`
- 実行可能ファイル名を置き換える場合。 例: `C:\Program Files\Application\v1.2*.exe`
- 実行可能ファイル名の一部を置き換える場合。 例: `C:\Program Files\Application\v1.2\run*.exe`

次の制限が適用されます。

- ワイルドカードは、単一のディレクトリを置き換える場合にのみ使用できます。たとえば、実行可能ファイルが `C:\Program Files\Application\v1.2\run1.exe` にある場合
  - 許可: `C:\Program Files\Application*\run1.exe`
  - 不許可: `C:\Program Files*\run1.exe`
- エントリにはファイル名拡張子を含める必要があります。
  - 許可: `C:\Program Files\Application\v1.2*.exe`
  - 不許可: `C:\Program Files\Application\v1.2*`
- すべてのパスはローカルである必要があります。

> **注:**
>
> - ネットワークパスは許可されていません。
> - ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2206から利用可能です。
> - ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2203 LTSRのCU2から利用可能です。

システム環境変数の使用

システム環境変数を使用して、許可リスト内の信頼されたプロセスの定義を簡素化できます。`%programfiles%`、`%programfiles(x86)%`、`%systemdrive%`、`%systemroot%` などの標準変数を使用できます。

システムレベルで定義されている限り、カスタム環境変数も使用できます。

以下の例は、標準の環境変数を示しています。

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

以下の例は、カスタムシステム環境変数を示しています。

- カスタム変数名: `app`
- カスタム変数値: `%programfiles%\Application\`
- 許可リストエントリ: `CTXCVC1,%app%\run.exe`

> **注:**
>
> ユーザー環境変数はサポートされていません。

> 環境変数のサポートは、Citrix Virtual Apps and Desktopsバージョン2209以降で利用可能です。

仮想チャネル名とプロセスを取得する

VDAマシン上で仮想チャネル名とそれを開くプロセスを取得する最も簡単な方法は、仮想チャネルを提供した開発者またはサードパーティベンダーから情報を入手することです。

または、機能のログを適用し、以下の手順に従って情報を取得することもできます。

1. カスタム仮想チャネルのクライアントコンポーネントとサーバーコンポーネントが配置されたら、仮想アプリケーションまたは仮想デスクトップを起動します。
2. VDAマシンのシステムイベントログで、カスタム仮想チャネル名とそれを開こうとしたプロセスを探します。利用可能なイベントの詳細については、「イベントログ」を参照してください。
3. セッションからログアウトします。
4. 識別された仮想チャネルとプロセスについて、仮想チャネル許可リストポリシー設定にエントリを追加します。
5. マシンを再起動します。
6. VDAが登録されたら、仮想アプリケーションまたは仮想デスクトップを実行して、カスタム仮想チャネルが正常に開くことを検証します。

Citrix仮想チャネルに関する考慮事項

すべての組み込みCitrix仮想チャネルは信頼されており、追加設定なしで開くことができます。ただし、以下の2つの機能は、外部依存関係のため、許可リストに明示的なエントリが必要です。

- マルチメディアリダイレクト
- スカイプ フォー ビジネス 用 HDX RealTime Optimization Pack

マルチメディアリダイレクト

Windows Media Player以外のメディアプレーヤーをシステムメディアプレーヤーとして使用する場合、それを信頼されたプロセスとして許可リストに追加する必要があります。許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXMM`
- プロセス: VDAマシンで使用されるメディアプレーヤーへのパス。例: `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`。
- 許可リストエントリ: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

スカイプ フォー ビジネス 用 HDX RealTime Optimization Pack

許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXRMEP`
- プロセス: VDAマシン内のSkype for Business実行可能ファイルへのパス。これはSkype for Businessのバージョンやカスタムインストールパスの使用によって異なる場合があります。例: `C:\Program Files\Microsoft Office\root\Office16\lync.exe.`.
- 許可リストエントリ: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

トラブルシューティング

カスタム仮想チャネルが開かない場合は、次の手順を確認してください。

1. 正しいVDAバージョンを使用していることを確認してください。
2. 仮想チャネル許可リストにカスタム仮想チャネルを含むポリシーがVDAに適用されており、この構成を上書きする優先度の高い他のポリシーがないことを確認してください。
3. VDAのイベントログを確認し、報告されている仮想チャネル名が許可リストで定義されているものと一致することを確認してください。

    a. 複数のプロセスがある場合は、仮想チャネルを許可リストに追加するで説明されているように、これらが適切に定義されていることを確認してください。

    b. 定義されたプロセスパスでワイルドカードを使用している場合は、ワイルドカードの使用のガイドラインに従っていることを確認してください。

    c. 定義されたプロセスパスで環境変数を使用している場合は、システム環境変数の使用のガイドラインに従っていることを確認してください。

イベントログ

次のイベントがVDAマシンのイベントログに記録されます。

シングルセッションVDA

次のイベントがシングルセッションVDAマシンのイベントログに記録されます。

ログ名	ID	送信元	レベル	説明
システム	2001	`Picadd`	情報	カスタム仮想チャネル `<vcName>` はプロセス

ログ名	ID	送信元	レベル	説明
				`<processName>` によって開かれました
システム	2002	`Picadd`	警告	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開くことができません
システム	2003	`Picadd`	情報	`<username>` がカスタム仮想チャネル `<vcName>` を開きました
システム	2004	`Picadd`	警告	`<username>` がカスタム仮想チャネル `<vcName>` を開こうとしました
システム	2005	`Picadd`	エラー	ポリシー `<pathInPolicy>` で指定されたパスはプロセスパスに解決できません
システム	2007	`Picadd`	情報	ロードされたプロセスパスは `<processPath>` です
システム	2008	`Picadd`	エラー	VCポリシーパス内の環境変数

ログ名	ID	送信元	レベル	説明
				`<varName>` が見つかりません

マルチセッションVDA

マルチセッションVDAマシンのイベントログに、次のイベントが記録されます。

ログ名	ID	送信元	レベル	説明
システム	13	`Rpm`	情報	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開かれました
システム	14	`Rpm`	警告	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開けません
システム	15	`Rpm`	情報	`<username>` がカスタム仮想チャネル `<vcName>` を開きました
システム	16	`Rpm`	警告	`<username>` がカスタム仮想チャネル `<vcName>` を開こうとしました
システム	17	`Rpm`	エラー	ポリシー `<pathInPolicy>` で指定され

ログ名	ID	送信元	レベル	説明
				たパスをプロセスパスに解決できません
システム	18	`Rpm`	情報	ロードされたプロセスパスは `<processPath>` です
システム	19	`Rpm`	エラー	VCポリシーパス内の環境変数 `<varName>` が見つかりません

既知のサードパーティ仮想チャネル

以下は、カスタムCitrix®仮想チャネルを使用する既知のサードパーティソリューションです。このリストには、カスタムCitrix仮想チャネルを使用するすべてのソリューションが含まれているわけではありません。

- サーナー
- ControlUp
- シスコ WebEx Teams
- シスコ ウェブエックス ミーティングス バーチャル デスクトップ ソフトウェア
- deviceTrust
- エピック ワープドライブ
- エピック スリングショット
- インプリバタ ワンサイン
- ミッドマーク IQパス クライアント拡張機能
- ニュアンス パワーマイク クライアント拡張機能
- ニュアンス ドラゴン メディカル ネットワーク エディション 360 vSync
- ズーム ミーティングス for VDI
- アルティマ IA-Connect

関連する仮想チャネルを許可リストに追加するための詳細については、ソリューションのベンダーにお問い合わせください。または、仮想チャネル名とプロセスの取得セクションに記載されている手順に従ってください。

DVC 用仮想チャネル許可リスト

DVC用仮想チャネル許可リストを使用して、環境で許可されるカスタム動的仮想チャネルを制御できます。デフォルトでは、動的仮想チャネルは許可されていません。動的仮想チャネルが必要な場合は、明示的に許可リストに追加する必要があります。

構成

DVC用仮想チャネル許可リストは、デフォルトで有効になっています。この機能は、Citrix®ポリシーの以下の設定を使用して構成できます。

- DVC用仮想チャネル許可リスト: この機能を有効または無効にし、動的仮想チャネルをリストに追加します。
- 仮想チャネル許可リストログスロットリング: 仮想チャネル許可リストイベントログのスロットリング期間を設定します。
- 仮想チャネル許可リストログ: 仮想チャネル許可リストのログレベルを設定します。

動的仮想チャネルを許可リストに追加する

動的仮想チャネルを許可リストに追加するには、以下の情報が必要です。

1. クライアント上のDVCプラグインの名前。例: `DvcPlugin1.dll`。
2. DVCリスナーの名前。例: `ListenerName1`。
3. VDAマシン上で動的仮想チャネルにアクセスするプロセスのパス。例: `C:\Program Files\Application\run.exe`。

必要な情報が揃ったら、DVC用仮想チャネル許可リストポリシー設定を使用して、動的仮想チャネルを許可リストに追加する必要があります。動的仮想チャネルをリストに追加するには、セッションホストでDVCにアクセスするプロセスのパスを入力し、その後にコンマ、クライアント側プラグイン名、コンマ、およびプラグインが使用するリスナー名を入力します。複数のリスナー名はコンマで区切って追加できます。

単一リスナーの場合

前の例を使用して、次のエントリをリストに追加します。 `C:\Program Files\App\run1.exe,DvcPlugin1,ListenerName1`

複数リスナーの場合

複数のリスナーがある場合は、リストに次のエントリを追加します。 `C:\Program Files\App\run1.exe,DvcPlugin1,ListenerName1,ListenerName2`

ワイルドカードの使用

ワイルドカード (*) の使用がサポートされています。アプリケーションのバージョンに基づいてディレクトリ名または実行可能ファイル名が変更される場合、またはサードパーティコンポーネントがユーザープロファイルにインストールされている場合に、ワイルドカードを使用できます。

次のシナリオでワイルドカードを使用できます。

- 完全なディレクトリ名を置き換える場合。例: `C:\Program Files\App*\run1.exe`
- ディレクトリ名の一部を置き換える場合。例: `C:\Program Files\App\v*\run1.exe`
- 実行可能ファイル名を置き換える場合。例: `C:\Program Files\App\v1.2*.exe`
- 実行可能ファイル名の一部を置き換える場合。例: `C:\Program Files\App\v1.2\run*.exe`

次の制限が適用されます。

- ワイルドカードは、単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルが `C:\Program Files\App\v1.2\run1.exe` にある場合
  - 許可: `C:\Program Files\App*\run1.exe`
  - 不許可: `C:\Program Files*\run1.exe`
- エントリにはファイル名拡張子を含める必要があります。
  - 許可: `C:\Program Files\App\v1.2*.exe`
  - 不許可: `C:\Program Files\App\v1.2*`
- すべてのパスはローカルである必要があります。

デバイス

スキャン

TWAINリダイレクト

はじめに

TWAIN は、画像ソフトウェアをスキャナーまたはデジタルカメラに接続するために使用されるスキャンプロトコルです。

TWAINの仕組み

- Citrix®セッション内の32ビットアプリケーションを使用してドキュメントをスキャンします。

> **注:**
>
> ローカルに接続されたTWAIN準拠のスキャナーを使用してドキュメントをスキャンします。

- Citrix スキャンモジュールは、TWAIN リクエストをクライアントのスキャナーにリダイレクトします。
- スキャンが完了すると、セッションホストに通知されます。

要件

Citrixコントロールプレーン

- シトリックス バーチャルアプリおよびデスクトップ™ 1912 以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ 11

- ウィンドウズ サーバー 2022 以降

- VDA
  - バージョン1912以降
- アプリケーション
  - 32ビットアプリケーション

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ 11
- Workspaceアプリ
  - Windows: バージョン 1912 以降
- スキャナー
  - TWAIN準拠スキャナー

構成

- クライアントエンドポイントにTWAINドライバーをインストールします。
- TWAINとWIAの両方をサポートしている場合は、必要なスキャンプロトコルを選択するようにデバイスまたはアプリケーションを設定します。
- スキャナーをクライアントエンドポイントにローカルで（USB経由で）接続します。
- 必要に応じて、USBリダイレクトを介してTWAINデバイスをセッションにリダイレクトします。

> **注:**
>
> TWAINデバイスはUSBリダイレクトと相性が悪く、スキャン品質が低下する可能性があります。

ポリシー設定

TWAINリダイレクトを設定し、スキャンを改善するためのポリシー設定。

- **クライアントTWAINデバイスリダイレクト：** TWAINリダイレクトを有効または無効にします。

> **注:**
>
> デフォルトでは、TWAINリダイレクトは有効になっています。

- **TWAIN圧縮レベル：** クライアントからホストへの画像の圧縮レベルを設定します。

詳細については、TWAINデバイスポリシー設定を参照してください。

トラブルシューティング

TWAINを公開テストアプリのTwackerで試してください。これはこのURLからダウンロードできます。

公開されたデスクトップセッション内でTWAINを検証するには、以下の手順に従ってください。

1. VDAに**Twacker**をインストールします。
2. **Twacker** (32ビット版) を起動します。
3. **ファイル > ソースの選択**をクリックし、リストからスキャナーを選択します。
4. **ファイル > 取得**をクリックします。
5. スキャナーをテストするには、**スキャンボタン**をクリックします。

Twackerが正常にスキャンできる場合、**Citrix Virtual Apps and Desktops**のセットアップが以下の状態であることを確認できます。

- USBリダイレクト用に構成されている
- TWAINデバイスを使用している
- すべてのローカルクライアントデバイス要件を満たしている

特定のアプリケーション内でスキャンに関する問題がまだ発生する場合は、ソフトウェアの問題である可能性が高いです。

WIA デバイス

要件

- スキャナーはWIA準拠である必要があります。

- WIAドライバーをローカルデバイスにインストールします。サーバーには必要ありません。
- スキャナーをローカルに接続します（例：USB経由）。
- スキャナーがTWAINドライバーではなく、ローカルのWindowsイメージ取得サービスを使用していることを確認してください。
- テストに使用されるユーザーアカウントに、ICA®セッション内の帯域幅を制限するポリシーが適用されていないことを確認してください。たとえば、クライアントUSBリダイレクトの帯域幅制限などです。

Windows イメージ取得アプリケーション許可リスト

許可リストを使用すると、VDA上のどのアプリケーションがWindows Image Acquisitionスキャナーリダイレクトにアクセスできるかを制御できます。レジストリエディターは、Windows Image Acquisitionを含む各VDAの許可リスト設定からの入力を使用します。デフォルトでは、どのアプリケーションもWindows Image Acquisitionにアクセスできません。

VDA上のアプリケーションに対してWindowsイメージ取得を調整するには、レジストリを通じて管理される機能のリストにあるWindowsイメージ取得アプリケーションの許可リスト設定を参照してください。

ポリシー設定の詳細については、WIAデバイスのポリシー設定を参照してください。

汎用USBデバイス

はじめに

汎用USBリダイレクト機能により、USBデバイスをクライアントマシンからHDX™セッションにリダイレクトでき、エンドユーザーはHDXセッションで幅広い汎用USBデバイスを操作できます。これは、最適化されたサポートがない、または不適切な特殊デバイスを使用する必要があるシナリオで役立ちます。

> **注:** 仮想チャネルサポート用に最適化されていないUSBデバイスは、生のUSBリダイレクトを使用して汎用USB仮想チャネルにフォールバックします。

仕組み?

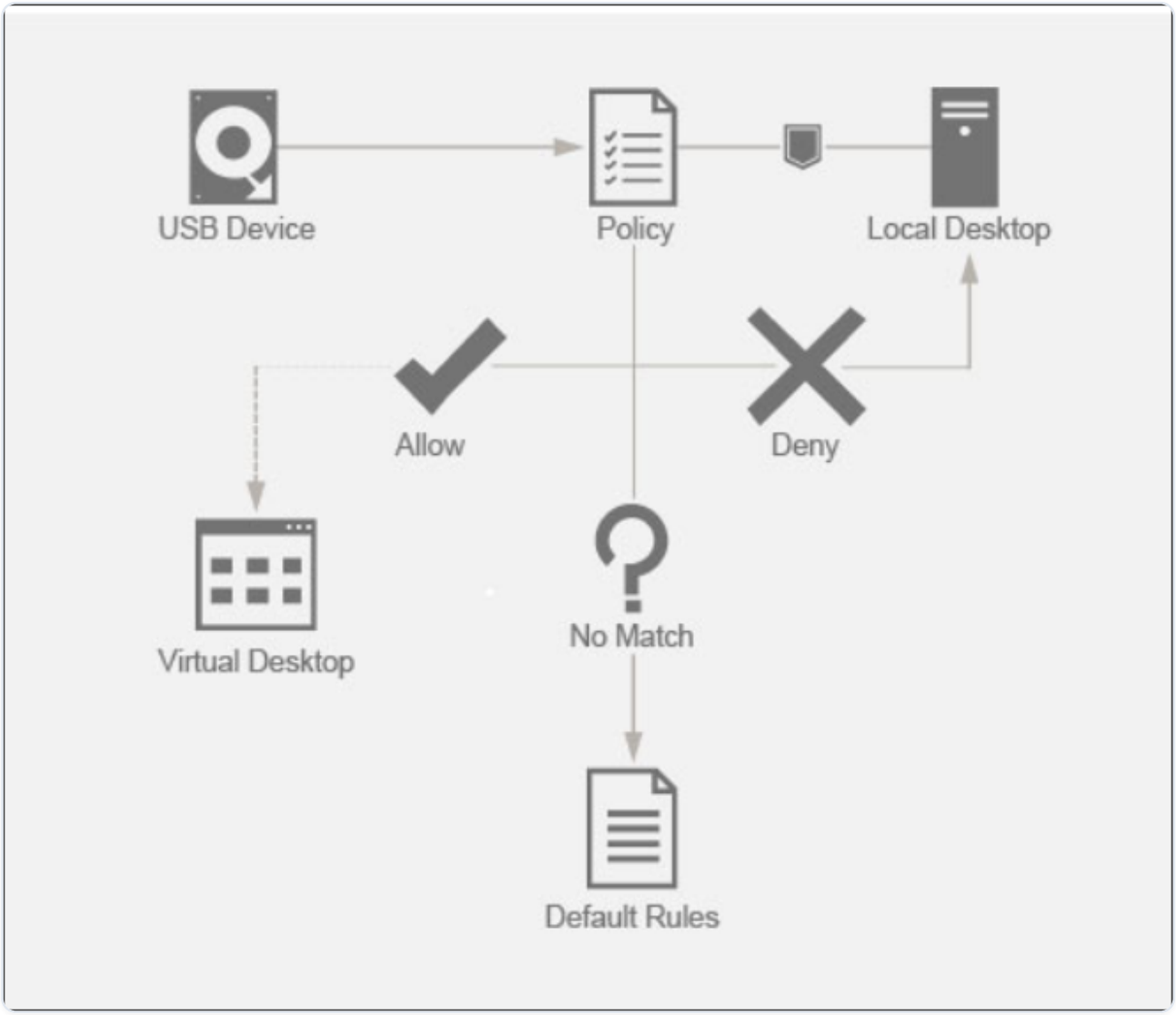
汎用USBリダイレクトは低レベルで機能し、クライアントマシンとXenDesktop®仮想デスクトップ間でUSB要求および応答メッセージをリダイレクトします。

クライアントマシンに互換性のあるデバイスドライバーが必要となることを回避し、ドライバーは仮想デスクトップでのみサポートされることが想定されています。USBリダイレクトポリシー規則は特定の優先順位に従い、DDCポリシー規則が評価および適用された後で、クライアント側のポリシーとデフォルト規則が尊重されるようにします。これにより、Citrix管理者は、不正なデバイスや偽装されたデバイスがセッション内でリダイレクトされるのを防ぐことができます。

さらに、リモートセッションへのアクセスを試みる不正なデバイスのイベントログは監査およびフラグ付けすることができ、管理者はデータ漏洩を防ぐための追加措置を講じることができます。

ユーザーがUSBデバイスを接続すると、セッションホストは一致が見つかるまで各ポリシー規則と連続して照合します。任意のデバイスに対する最初の一致が最終的なものと見なされます。

- 最初の一致が許可規則である場合、デバイスは仮想デスクトップにリダイレクトされます。
- 最初の一致が拒否規則である場合、デバイスはセッションにリダイレクトされず、ローカルユーザーデバイスでのみ使用できます。一致が見つからない場合、デフォルト規則が使用されます。



構成

USBリダイレクトはデフォルトで無効になっています。Citrix®ポリシーで以下の設定を使用して、汎用USBリダイレクトを構成できます。

- **クライアントUSBデバイスリダイレクト**: USBリダイレクトを有効または無効にする
- **クライアントUSBデバイスリダイレクトルール**: 特定のデバイスアクション、つまり特定のデバイスへのアクセスを許可または拒否するように指定する
- **クライアントUSBデバイスリダイレクトルール (バージョン2)**: USBデバイスのフィルタリング、分割、自動接続のルールを指定する
- **クライアントUSBデバイス最適化ルール**: 最適化を無効にするか、最適化モードを変更する
- **既存のUSBデバイスの自動接続を許可する**: HDX™セッション開始時にクライアントエンドポイントに接続されている既存のUSBデバイスの自動接続を許可または禁止する
- **新しく接続されたUSBデバイスの自動検出を許可する**: HDXセッション中にクライアントエンドポイントに接続されたUSBデバイスの自動接続を許可または禁止する

詳細については、USBポリシー設定を参照してください。

USBリダイレクトの構成方法

デフォルトでは、USBリダイレクトの構成は無効になっています。これを使用するには、USBリダイレクトポリシーと特定のリダイレクトルールをDDCで有効にして構成する必要があります。

> **注:**
>
> バージョン2212より前のコンポーネントを使用している場合、またはLinux/Mac版Workspaceアプリを使用している場合は、USBリダイレクトの構成方法の詳細についてレガシーUSBリダイレクト構成を参照してください。

汎用USBリダイレクトの有効化

1. **Citrix Web Studio™ポリシー**を開き、**［ポリシー］**タブをクリックします。
2. **［ポリシーの作成］をクリックし、［ICA®］>［USBデバイスポリシー］**を展開します。
3. **クライアントUSBデバイスリダイレクトポリシー**を編集します。
4. 「**許可**」を選択し、「**保存**」をクリックします。

USBリダイレクトポリシー規則の作成

ユーザーがUSBデバイスをVirtual Desktopにリダイレクトしようとすると、一致が見つかるまで各USBポリシー規則に対して順にチェックされます。いずれかのデバイスに対する最初の一致が最終と見なされます。最初の一致が**許可**規則である場合、一致したデバイスは仮想デスクトップにリダイレクトが許可されます。最初の一致が**拒否**規則である場合、一致したデバイスはローカルデスクトップでのみ利用可能です。一致が見つからない場合は、デフォルトの規則が使用されます。

デバイス規則

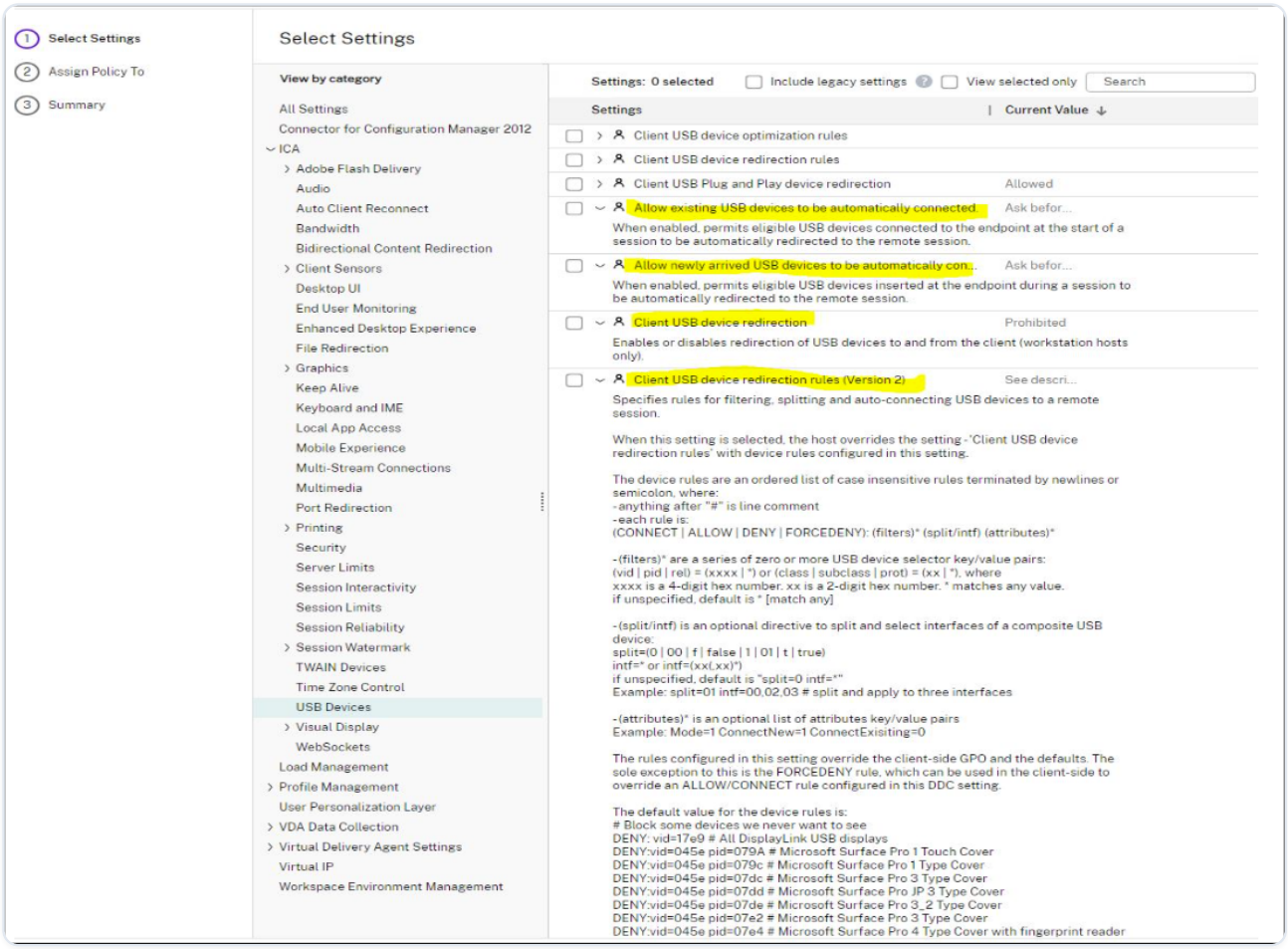
通常のUSBデバイスと同様に、エンドポイントのポリシーまたはクライアントCitrix Workspace™アプリ構成で設定されたデバイス規則は、転送するデバイスを選択します。Citrix Workspaceアプリはこれらの規則を使用して、どのUSBデバイスをリモートセッションへの転送を許可または防止するかを決定します。

各規則は、アクションキーワード（**Allow、Connect、またはDeny**）、コロン（:）、およびエンドポイントのUSBサブシステムにある実際のデバイスと一致する0個以上のフィルターパラメーターで構成されます。これらのフィルターパラメーターは、すべてのUSBデバイスが自身を識別するために使用するUSBデバイス記述子メタデータに対応しています。

デバイス規則はクリアテキストであり、各規則は1行に記述され、#文字の後にオプションのコメントが続きます。規則は上から下へ（優先順位の降順で）照合されます。デバイスまたは子インターフェイスに一致する最初の規則が適用されます。同じデバイスまたはインターフェイスを選択する後続の規則は無視されます。

例: ALLOW VID=1050 PID=0421 #Device1 **例:** CONNECT VID=xxxx PID=yyyy Class=03 #Device2

キーワード	説明
CONNECT	このキーワードを使用して、USB仮想チャネル経由でのデバイスのリダイレクトを許可し、セッション起動時および挿入時の自動リダイレクトを有効にします。
ALLOW	このキーワードを使用して、USB仮想チャネル経由でのデバイスのリダイレクトを許可します。
DENY	このキーワードを使用して、USB仮想チャネル経由でのデバイスのリダイレクトを拒否します。



DDC でポリシーを設定する:

1. **Citrix Web Studio ポリシー**」を開き、「**ポリシー**」タブをクリックします。
2. **ポリシーの作成**」をクリックし、「**ICA > USB デバイス ポリシー**」を展開します。
3. **クライアント USB デバイス リダイレクト規則**」を編集します (「**バージョン 2**」)。
4. リダイレクトする必要がある各 USB デバイスの説明に記載されている例に基づいて値を設定し、「保存」をクリックします。

   例: 許可: VID=056A PID=00A4 #STU-430 拒否: Class=08 subclass=05 # マスストレージ

> **注:**
>
> Citrix 管理者が「**既定値を使用**」をオンにして「**保存**」をクリックすると、既定の規則は VDA の次のレジストリにあります。

> **注意!**

> レジストリエディターを使用する前に、この記事の最後にある免責事項を参照してください。

> `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

注記:

> ポリシーは、グループポリシーデバイスルールを使用してクライアントデバイスに設定できますが、CVADおよびCWAの新しいバージョンでは不要になりました。

> USBデバイスのレガシー構成については、レガシーUSBリダイレクト構成を参照してください。

USBデバイスの自動リダイレクトを構成する（オプション）

USBサポートが有効になっている場合、USBデバイスは自動的にリダイレクトされます。また、USBユーザー設定はUSBデバイスを自動的に接続するように設定されています。すべてのUSBデバイスをリダイレクトすることが常に最適とは限りません。ユーザーは、自動的にリダイレクトされないデバイスをUSBデバイスリストから明示的にリダイレクトできます。USBデバイスが一覧表示されたりリダイレクトされたりするのを防ぐには、クライアントエンドポイントまたはDDCポリシーでDeviceRulesを使用します。 このポリシーは、DDC、GPOを使用したクライアント、Citrix Workspace Preferences、またはCDViewerのタブのいずれかで設定できます。これらの方法はすべて以下に説明されています。

DDC でポリシーを設定する:

DDCには、USBデバイスの自動リダイレクトを許可するように設定できる2つのポリシーがあります。

- 既存のUSBデバイスの自動接続を許可する
- 新しく接続されたUSBデバイスの自動接続を許可する

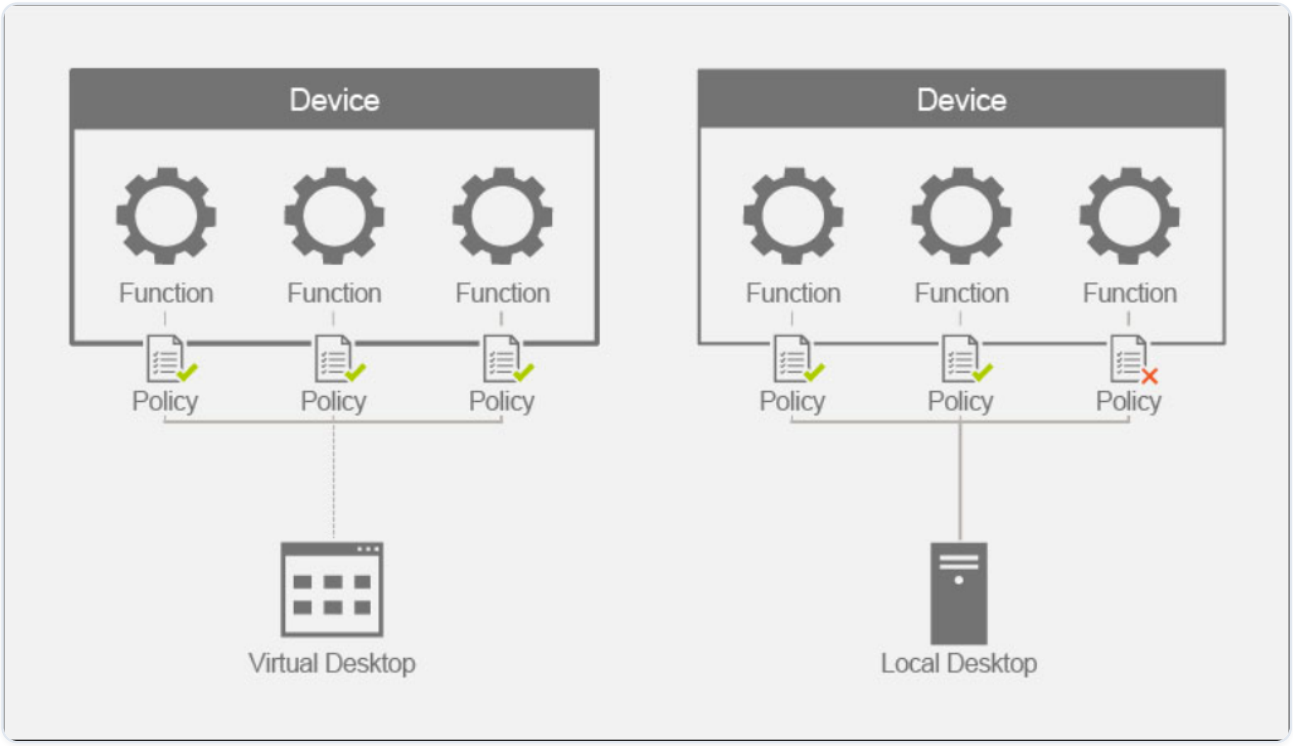
a. **Citrix Web Studioポリシー**を開き、**ポリシー**タブをクリックします。
b. **ポリシーの作成**をクリックし、**ICA > USBデバイスポリシー**を展開します。
c. 設定「**既存のUSBデバイスの自動接続を許可する**」を編集します。
d. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクトする**」を選択して、**保存**をクリックします。

e. 設定「**新しく接続されたUSBデバイスの自動接続を許可する**」を編集します。

f. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクトする**」を選択して、**保存**をクリックします。

複合デバイスとデバイス分割

複合USBデバイスは、コンピューターに接続された複数の独立したUSBデバイスのように機能する単一のデバイスです。単一のUSBコネクタを持ちますが、それぞれ独自の機能セットを持つ複数のインターフェイスをコンピューターに公開できます。ユーザーが複合USBデバイスを接続すると、ホストデバイスはすべての機能（インターフェイス）を各ポリシー規則と照合して確認します。いずれかの機能（インターフェイス）に対する最初の照合が拒否規則である場合、その規則は複合デバイスに対して最終的なものと見なされ、デバイスは拒否されます。機能（インターフェイス）に対する最初の照合が許可規則である場合、ホストデバイスは次の機能（インターフェイス）に対して規則の照合を続行します。複合デバイスは、ポリシー規則によって機能（インターフェイス）が拒否されない場合に許可されます。複合デバイスに対する最終的な照合が拒否規則である場合、デバイスはローカルデスクトップでのみ利用可能であり、それ以外の場合は仮想デスクトップにリモート化されます。照合が見つからない場合は、デフォルトの規則が使用されます。



複合デバイスの特定の機能のみを許可するために、デバイスリダイレクト規則（バージョン2）ポリシーで適切な規則を使用して複合デバイスを分割できます。たとえば、FIDO2キーのHID機能のみを使用し、スマートカード機能は使用したくない場合があります。その場合、規則は次のように設定します。

1. Connect: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikeyシリーズ5のFIDO2 HID機能が許可されています。
2. Deny: VID=1050 PID=0407 split=01 intf=02 #Yubikeyシリーズ5のスマートカード機能がブロックされました。

> **ヒント:**
>
> 新しいポリシー規則を作成する際は、USB Webサイトで入手できるUSBクラスコードを参照してください。

署名パッドの構成

1. VDAホストに適切なデバイスドライバーをインストールします。
2. **Citrix Web Studio™**で**クライアントUSBデバイスリダイレクト**ポリシー設定を有効にします。
3. **クライアントUSBデバイスリダイレクト規則（バージョン2）**ポリシー設定を編集します。
    a. リダイレクトする必要がある署名パッドの**VID**および**PID**情報を設定し、**保存**をクリックします。例：**Connect**: VID=06A8 PID=0057 class=03 #Topaz HSB
4. ポリシー設定**クライアントUSBデバイス最適化規則**を編集します。
    a. モードとその他のデバイス情報を設定します。例：Mode=00000004 VID=06A8 PID=0057 class=03 #キャプチャモードで動作する入力デバイス
5. 「**既存のUSBデバイスの自動接続を許可する**」ポリシー設定を編集します。
6. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクトする**」を選択して、「**保存**」をクリックします。
7. 「**新しく接続されたUSBデバイスの自動接続を許可する**」ポリシー設定を編集します。
8. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクトする**」を選択して、「**保存**」をクリックします。

これらの設定が構成されると、以降のセッション起動ではデバイスが自動的にリダイレクトされ、エンドユーザーによる追加のアクションは不要になります。

> **注:**

> VIDとPIDを、リダイレクトするデバイスの実際のVIDとPIDに置き換えます。

USBリダイレクトを使用したBloombergキーボードの構成

1. **Citrix Web Studio**で**クライアントUSBデバイスリダイレクト**ポリシー設定を有効にします。
2. Bloomberg 5キーボードは、**クライアントUSBデバイスリダイレクト規則（バージョン2）**ポリシー設定でデフォルトで設定されており、追加の管理者アクションは不要です。
3. 「**既存のUSBデバイスの自動接続を許可する**」ポリシー設定を編集します。
4. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクトする**」を選択して、「**保存**」をクリックします。
5. 「**新しく接続されたUSBデバイスの自動接続を許可する**」ポリシー設定を編集します。
6. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクトする**」を選択して、「**保存**」をクリックします。

これらの設定が構成されると、以降のHDX™セッションでBloombergキーが自動的に表示され、エンドユーザーによる追加のアクションは不要になります。

USBリダイレクトを使用したFIDO2キーの構成

Citrixでは、HDXセッションでFIDO2キーを使用するためにFIDO2リダイレクトを使用することをお勧めします。ただし、代わりにUSBリダイレクトを使用してFIDO2キーをリダイレクトする必要がある状況もあります。これには、クライアント、VDA、またはオペレーティングシステム（例：Windows Server 2016）でこの機能がサポートされていないため、FIDO2リダイレクトが利用できないシナリオが含まれます。

キーに複数のモードが有効になっているが、HDXセッションではその一部のみを許可したいという状況も考えられます。たとえば、FIDO2とOTPは許可するが、スマートカードはブロックしたい場合などです。

以下の手順は、USBリダイレクトを使用してFIDO2キー（Yubikey vid=1050, pid=0407）を構成する方法を示しています。

1. **Citrix Web Studio**で**クライアントUSBデバイスリダイレクト**ポリシー設定を有効にします。
2. **クライアントUSBデバイスリダイレクトルール（バージョン2）**ポリシー設定を編集します。
    a. セッションでリダイレクトされるFIDO2キーの**VID**と**PID**情報、および分割デバイス構成を設定し、**保存**をクリックします。

   b. **接続**: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikeyシリーズ5で許可されるFIDO2 HID機能。
   c. **拒否**: VID=1050 PID=0407 split=01 intf=02 # Yubikeyシリーズ5のスマートカード機能はブロックされます。

3. ポリシー設定**既存のUSBデバイスの自動接続を許可する**を編集します。
4. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクト**を選択して、**保存**をクリックします。
5. ポリシー設定**新しく接続されたUSBデバイスの自動接続を許可する**を編集します。
6. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクト**を選択して、**保存**をクリックします。

これらの設定が構成されると、FIDO2キーボードは以降のHDXセッションで自動的に表示され、エンドユーザーによる追加の操作は不要になります。

USBリダイレクトを使用した3Dマウスの構成

現在、3dConnexion SpaceMouseドライバーはワークステーションOS（Windows 10およびWindows 11）でのみサポートされています。サーバーOSでは動作しません。ワークステーションOS（vid=046D、pid=C016）でSpaceMouse Enterpriseを構成する手順は次のとおりです。

1. 最新のWindowsドライバーをVDAホストにインストールします。
2. 「**Citrix Web Studio**」で「**クライアントUSBデバイスリダイレクト**」ポリシー設定を有効にします。
3. 「**クライアントUSBデバイスリダイレクト規則**」（**バージョン2**）ポリシー設定を編集します。

   a. リダイレクトする必要がある署名パッドの**VID**および**PID**情報を追加し、**保存**をクリックします。例: **Connect**: VID=046D PID=C016 #SpaceMouse Enterprise

4. 「**クライアントUSBデバイス最適化規則**」ポリシー設定を編集します。

   a. モードとその他のデバイス情報を設定します。例: Mode=00000004 VID=046D PID=C016 class=03 #Input device operating in capture mode

5. 「**既存のUSBデバイスの自動接続を許可する**」ポリシー設定を編集します。
6. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクトする**」を選択して、**保存**をクリックします。
7. 「**新しく接続されたUSBデバイスの自動接続を許可する**」ポリシー設定を編集します。

8. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクトする**」を選択して、**保存**をクリックします。

USBリダイレクトを使用して、異なるデバイス規則で2つ以上のデバイスを構成する

HDXセッション内で、異なるデバイス規則を使用して複数のデバイスをリダイレクトできます。管理者は、一方のデバイスを自動的にリダイレクトし、もう一方のデバイスをエンドユーザーがリダイレクトするオプションを提供したい場合があります。異なる規則で2つのデバイスを構成する手順は次のとおりです。

1. 「**Citrix Web Studio**」で「**クライアントUSBデバイスリダイレクト**」ポリシー設定を有効にします。
2. 「**クライアントUSBデバイスリダイレクト規則**」（**バージョン2**）ポリシー設定を編集します。

    a. セッション内で適切なデバイス規則を使用してリダイレクトする2つのデバイスの**VID**と**PID**情報を追加し、**保存**をクリックします。

    b. **許可**: VID=0911 PID=0c1c #フィリップス製スピーチマイク.

    c. **接続**: VID=06A8 PID=0043 class=03 # Topaz HSB署名パッド

3. ポリシー設定 **既存のUSBデバイスの自動接続を許可する** を編集します。
4. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクトする**」を選択して、**保存**をクリックします。
5. ポリシー設定 **新しく接続されたUSBデバイスの自動接続を許可する** を編集します。
6. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクトする**」を選択して、**保存**をクリックします。

これらの設定が構成されると、Topaz HSB署名パッドは、その後のHDXセッションで自動的に表示され、追加のエンドユーザー操作は不要になります。一方、Phillipsスピーチマイクは、エンドユーザーがConnection CenterまたはCDViewerのタブでリダイレクトを有効にする必要があります。

トラブルシューティング

USBリダイレクト関連の問題をトリアージするには、以下の手順に従う必要があります。

1. USBリダイレクトのシステム要件が満たされていることを確認します。これには、正しいCVADおよびCWAバージョン、検討中のOSプラットフォームでサポートされているデバイスとデバイスドライバーが含まれます。

2. 環境で使用されているコンポーネントのバージョンとプラットフォームに基づいて、構成が適切であることを確認してください。(/ja-jp/citrix-virtual-apps-desktops/2407/devices/usb-devices/legacy-usb-redirection-configuration.html)を必要とするコンポーネントの詳細については、「Legacy USB Redirection Configuration」の注記を参照してください。
3. デバイスがクライアントによって列挙されたデバイスの下にリストされていることを確認します。

    a. Workspace Preferencesツールバー: WorkspaceアプリのPreferencesツールバーのタブに列挙されているデバイスを確認します（**CWAアイコンを右クリック > Connection Center > Preferences**… **Devices**タブをクリック）。

    b. `CtxUsbDiagnostics.exe`（推奨）：コマンドプロンプトウィンドウでこのツールを実行します。出力には、特定のセッションのデバイス固有の情報が表示されます。デバイスがリダイレクトされているかどうか、また、デバイスルールセットがデバイスのリダイレクトを妨げているかどうかがわかります。詳細については、(/ja-jp/citrix-virtual-apps-desktops/2407/devices/usb-devices/usb-diagnostics-tool.html)を参照してください。

    c. USBViewまたはその他のサードパーティツール: エンドポイント/クライアントマシンでUSBViewのようなサードパーティツールを実行し、デバイスがエンドポイントで検出されていることを確認します。

4. デバイスが列挙されている場合：

    a. 特定のデバイスについてCtxUsbDiagnosticsツールの出力にDenyルールが表示される場合は、Studioで構成されているポリシーを確認し、バージョン2ポリシーでルールが正しく設定されていることを確認してください。拒否ルールがStudioポリシーに表示されない場合は、クライアント側ポリシー、そして最後にクライアント側デフォルトの順に確認して、一致する拒否ルールを見つけてください。

    b. CtxUsbDiagnostics出力に拒否ルールがない場合、CWAは、環境設定ウィンドウのデバイスタブ（デバイス > デバイスの管理）で適切なボタンをチェック/クリックすることで、デバイスのリダイレクトを許可します。一度リダイレクトされたデバイスは、セッションで利用可能になります。これは、HDXセッションでデバイスマネージャー/USBViewまたは同様のアプリケーションを確認することで検証できます。

5. セッション内にデバイスが表示されない場合：

    a. VDAホストに正しいデバイスドライバーが正しくインストールされていない可能性があります。VDAホストに最新バージョンのデバイスドライバーが正しくインストールされていることを確認してください。一部のデバイスドライバーはターミナルサーバーマシンでサポートされていないため、リダイレクトしようとしているデバイスがそうでないことを確認してください。

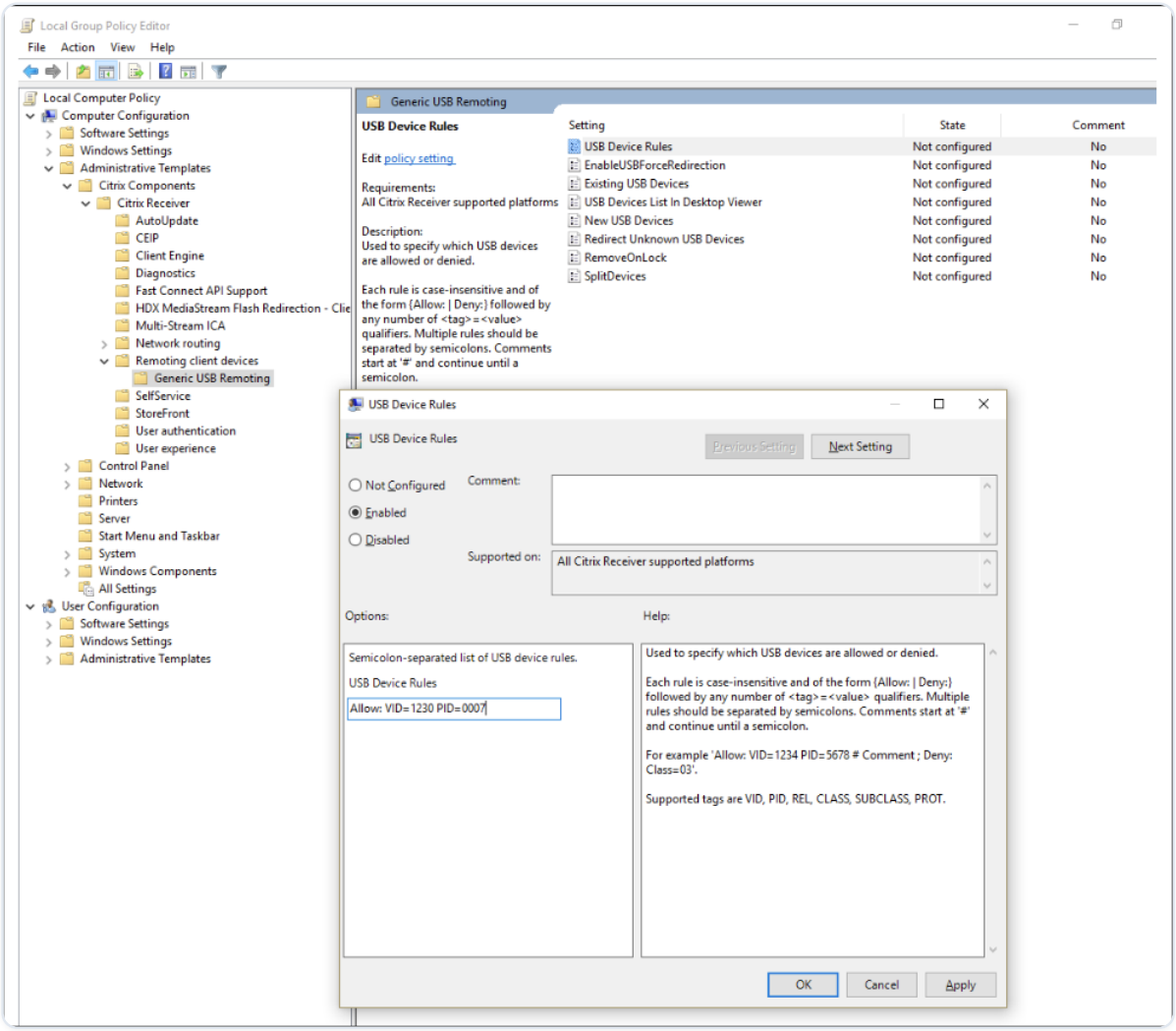
b. デバイスがクライアントエンドポイントで使用されていないことを確認してください。一部のデバイスはクライアントエンドポイントにもドライバーのインストールが必要であり、これがセッションでのリダイレクトを妨げる可能性があります。

6. クライアントエンドポイントでUSB関連のルールが正しく設定されていることを確認します。

   a. **Windows 向け CWA**:

      i. クライアントのグループポリシー (これについては詳細とSSを追加してください) が適切に設定されており、Studioで設定されたルールと競合しないことを確認します。

      ii. クライアントのレジストリにあるデフォルトルールを検証します。



`(HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules) are appropriately set and not in conflict with the rules set in Studio and client group policy.`.

   b. CWA for Linux - CWA for Linux の問題のトリアージについては、CWA for Linux の USB ドキュメントを参照してください。

c. CWA for Mac - CWA for Macの問題をトリアージするには、CWA for Macを参照してください。

注:

- TSVDAでは、オーディオデバイスはデフォルトでUSBリダイレクトの使用がブロックされています。これらのデバイスを使用する推奨される方法は、最適化されたオーディオVCを使用することです。
- デバイスを分割するための正しいデバイスリダイレクトルールが設定されていても、USB複合デバイスが自動的に分割されない場合があります。この問題は、デバイスが低電力モードになっているために発生します。このような場合、低電力モードになった子デバイスがデバイスリストに表示されないことがあります。この問題を解決するには、以下の回避策を使用できます。
  - セッションを切断し、USB デバイスを挿入して、セッションに再接続します。
  - USBデバイスを抜き差しします。この操作により、デバイスは低電力モードから復帰します。
- バッテリー寿命を最適化するために、USBバッテリーセーバー設定が有効になっている場合があります。クライアントエンドポイントがスリープ状態になると、USBデバイスが切断されることがあります。そのようなシナリオでは、セッションでデバイスを再度表示するために、デバイスを抜き差しする必要がある場合があります。

イベントログ

管理者は、ユーザーがリダイレクトしようとする不正なデバイスを監視し、適切な措置を講じることができるようになりました。以下に、リダイレクトが許可されているデバイスと許可されていないデバイスについて、VDA ホストのイベントビューアーに記録されるイベントメッセージの一部を示します。

Id	1000
Name	UsbEventAcceptDevice
Severity	Informational
Facility	System
Text	The Citrix USB Service allows the USB Device with Product ID: %2, Vendor ID: %3, and Device ID: %4 to be remoted.
Comment	This message logs the device info of a device redirected in an HDX session

Id	1001
Name	UsbEventPolicyRejectsDeviceV1
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the legacy “Client USB device redirection rules” policy rule.
Arguments	

Id	1002
Name	UsbEventPolicyRejectsDeviceV2
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules (Version 2)" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the "Client USB device redirection rules (Version 2)" policy rule. For instance, if the studio policy rule allows an approved set of devices and denies all other devices and an end user tries to create a new rule on the client endpoint via group policy, this event will get logged. This message would be indicative of an unauthorized device redirection attempt.
Arguments	

USB診断ツール

`CtxUsbDiagnostics.exe` は、Citrix管理者がクライアントで発生するUSBデバイスのリダイレクトに関する問題を迅速に診断し解決するのに役立つ、VDA上のコマンドラインツールです。このユーティリティツールは、HDXセッション内でリダイレクトに失敗しているクライアントに接続されたUSBデバイスに関連する構成の問題をトリアージするために必要な重要な情報を収集します。

```
> **Note :**

>

> Running Command Prompt or Powershell as an administrator is required to
```

```
ensure the tool has the necessary permissions to perform system-level
operations.
```

要件

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
  - ウィンドウズ サーバー 2016 以降
- VDA
  - Windows版: Citrix Virtual Apps and Desktops™ バージョン 2311 以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809以降
- ワークスペースアプリ
  - Windows: バージョン2311以降

このツールでできること?

このツールは現在、以下を提供します。

- SessionID
- VDAデバイスポリシー（Studioで設定されたデバイスルール）
- クライアントデバイスとクライアントデバイスポリシー（デバイスルール）
- デバイスのリスト、そのリダイレクト状態、および許可または拒否された理由



> **注記：**
>
> 管理者は、すべてのアクティブなセッションのデバイス情報を確認できます。

表示される情報

- **Citrix Studio ルール - バージョン 1/2**
  - DDCルールは、Studioでレガシーの「**Client USB device redirection rules**」または「**Client USB device redirection rules (Version 2)**」ポリシーが使用されていることを示します。このセクションに記載されている情報は、Citrix®管理者が構成したすべてのルールをリストします。



- **クライアントのデフォルトデバイスルール**
  - このセクションには、クライアントのレジストリに設定されているルールが一覧表示されます。



- **デバイス最適化ルール**
  - このセクションには、「クライアントUSBデバイス最適化ルール」で設定されているデバイス最適化ルールが一覧表示されます。



デバイスリスト

このセクションには、クライアントエンドポイントに接続されている各デバイスに関する貴重な情報（ハードウェア情報、リダイレクトされているかどうか、正しいデバイスリダイレクトルールが設定されているかどうかなど）が一覧表示されます。

タグ名	説明
displayName	デバイスの共通名を一覧表示します。
ベンダーID	ベンダーID
製品ID	製品ID
インターフェイス	複合デバイスが複数の子デバイスに分割されている場合、このサブセクションにはすべてのインターフェースが一覧表示されます。
InterfaceNum	インターフェース記述子のインデックスを示します

タグ名	説明
クラス	クラスコード
サブクラス	サブクラスコード
プロトコル	プロトコル
redirectionState	**Local** は、デバイスがICA®セッションでリダイレクトされていないことを示します。**ThisSession** は、デバイスがICAセッションでリダイレクトされていることを示します。**OtherSession** は、デバイスが別のICAセッションでリダイレクトされていることを示します。
optiEnabled	**true** は、デバイスが最適化されていることを示します。**false** は、デバイスが最適化されておらず、データ転送がUSB仮想チャネル経由で行われることを示します。
deviceType	**generic** は、デバイスに最適化された仮想チャネルがなく、トラフィックがUSB仮想チャネル経由で流れていることを示します。**optimized** は、デバイスに関連付けられたデータ転送が専用の仮想チャネル経由で行われていることを意味します。
isDenied	**true** は、管理者が設定したポリシー規則によりデバイスがリダイレクトされないことを示します。`false` は、適用されたポリシーによりデバイスがリダイレクトされることを示します。
denyRule	このフィールドは、**isDenied** が `true` に設定されている場合に役立ちます。これにより、管理者は、デバイスがリダイレクトされない原因となっているポリシー内の特定の規則セットを知ることができます。

レガシーUSBリダイレクトの構成

バージョン2212より古いコンポーネントを使用している場合、またはLinux版CWAを使用している場合は、このガイドに従って環境でUSBリダイレクトを構成してください。

汎用USBリダイレクトの有効化

1. **Citrix Web Studio™ポリシー**を開き、**ポリシー**タブをクリックします。
2. **ポリシーの作成**をクリックし、**ICA® > USBデバイスポリシー**を展開します。
3. **クライアントUSBデバイスリダイレクトポリシー**を編集します。
4. **許可**を選択し、**保存**をクリックします。

USBリダイレクトポリシー規則の作成

ユーザーがUSBデバイスを仮想デスクトップにリダイレクトしようとすると、一致が見つかるまで各USBポリシー規則に対して順番にチェックされます。いずれかのデバイスに対する最初の一致が最終と見なされます。最初の一致が許可規則である場合、一致したデバイスは仮想デスクトップへのリダイレクトが許可されます。最初の一致が拒否規則である場合、一致したデバイスはローカルデスクトップでのみ利用可能です。一致が見つからない場合は、デフォルトの規則が使用されます。

DDC でポリシーを設定する:

1. **Citrix Web Studioポリシー**を開き、**ポリシー**タブをクリックします。
2. **ポリシーの作成**をクリックし、**ICA > USBデバイスポリシー**を展開します。
3. **クライアントUSBデバイスリダイレクト規則**を編集します。
4. リダイレクトする必要がある各USBデバイスの説明に記載されている例に基づいて値を設定し、をクリックします。 例: Allow: VID=056A PID=00A4 #STU-430 Deny: Class=08 subclass=05 # Mass Storage

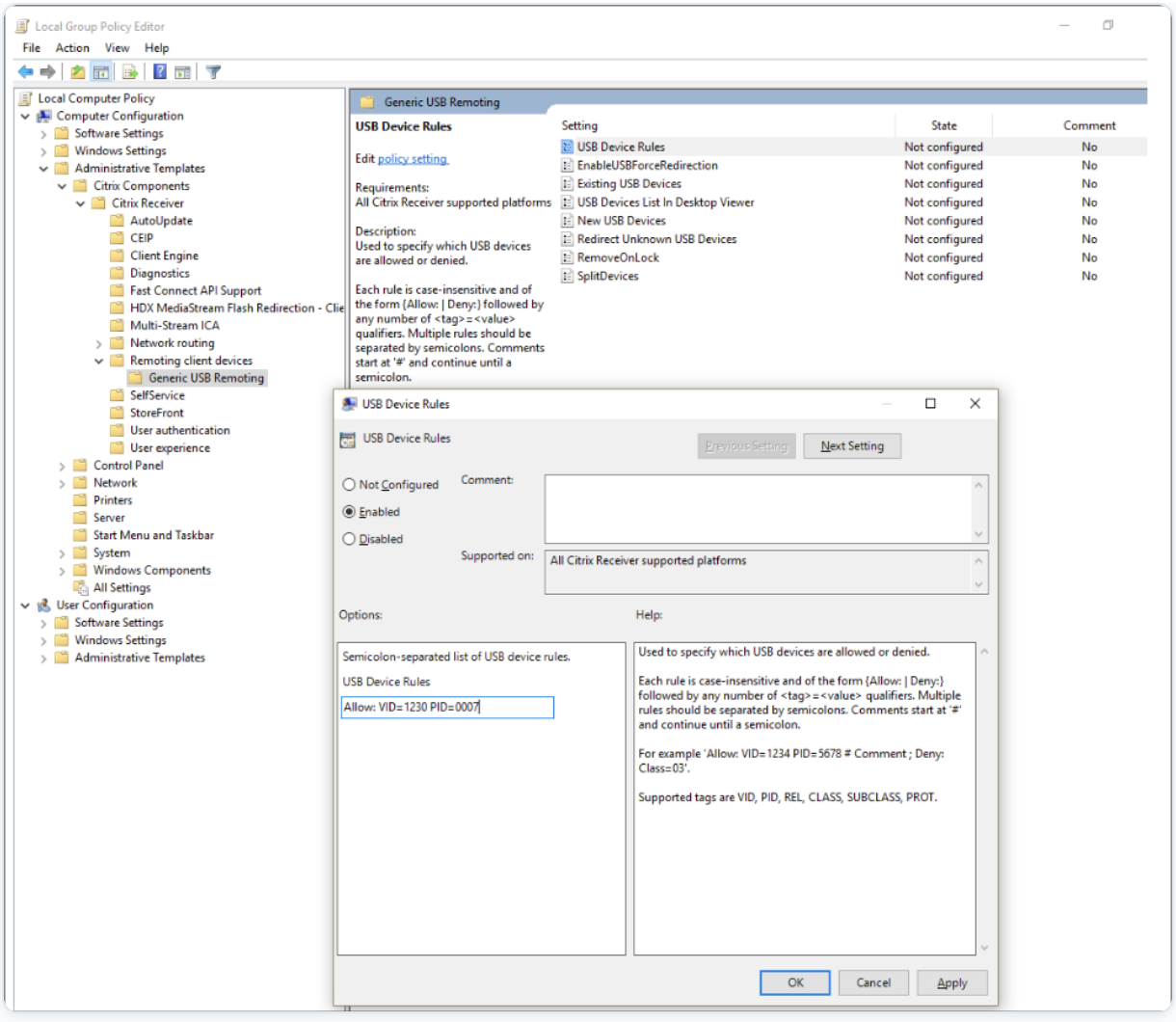
> **注:**
>
> Citrix®管理者が「既定値を使用」をチェックして「保存」をクリックすると、既定のルールはVDAの以下のレジストリにあります。
>
> **注意！:**

> レジストリエディターを使用する前に、この記事の最後にある免責事項を参照してください。 `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

クライアントでGPOを使用する:

1. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrix Components > Citrix Receiver™ > リモートクライアントデバイス > Generic USB Remoting**に移動します。
2. **USBデバイスルール設定**を開き、この設定を有効にします。この例のようにUSBデバイスルールを追加します。 Allow: VID=1230 PID=0007ルールは、ベンダーID 1230および製品ID 0007のデバイスを許可します。

> **注:**
>
> 特定のデバイスがデバイスルールリストの最上位にある必要がある場合は、Allow: VID=xxxx PID=xxxxルールを使用します。



> **注:**
>
> USBViewのようなツール、または接続ツールバーを使用して、VIDやPIDなどのデバイスの詳細を特定できます。

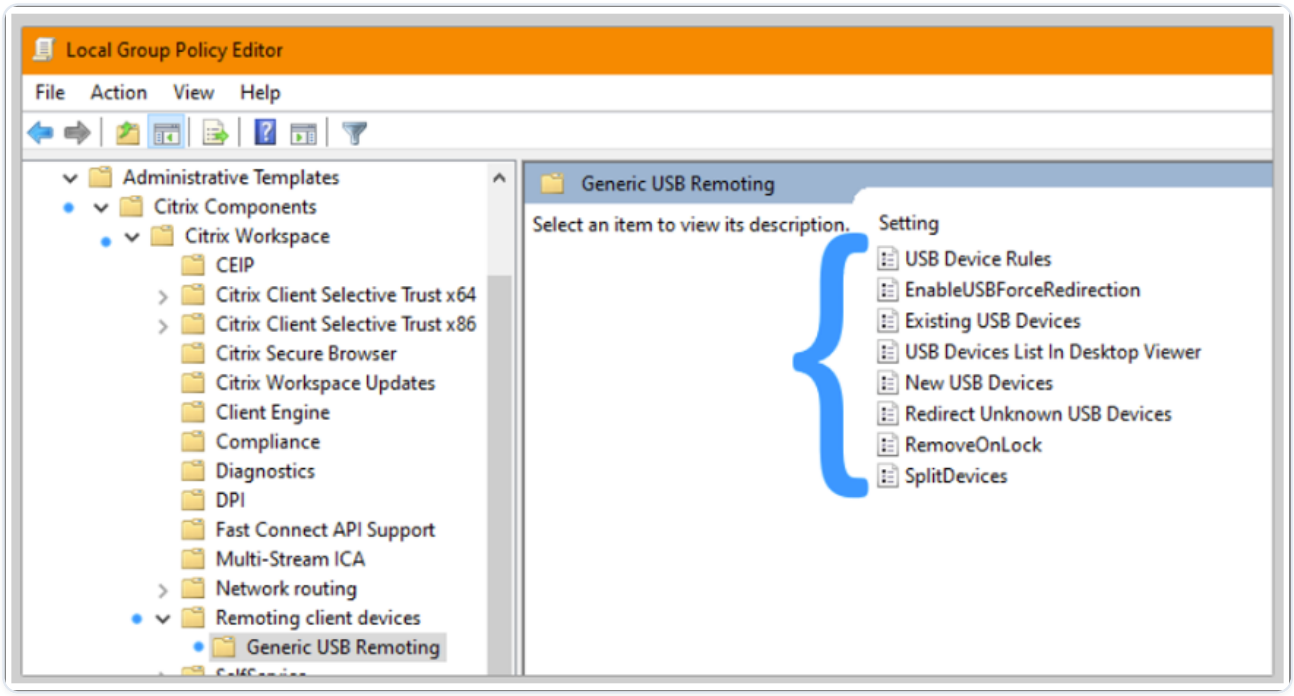
USBデバイスの自動リダイレクトを構成する

USBサポートが有効になっている場合、USBデバイスは自動的にリダイレクトされます。また、USBユーザー設定はUSBデバイスを自動的に接続するように設定されています。すべてのUSBデバイスをリダイレクトすることが常に最適とは限りません。ユーザーは、自動的にリダイレクトされないUSBデバイスリストからデバイスを明示的にリダイレクトできます。USBデバイスが一覧表示されたりリダイレクトされたりするのを防ぐには、クライアントエンドポイントでDeviceRulesポリシー設定を使用します。

このポリシーは、GPO、クライアント側レジストリ、Citrix Workspace™設定、またはCDViewerの接続タブを使用してクライアントで設定できます。これらの方法はすべて以下に説明されています。

クライアントでGPOを使用する:

1. 「**ローカル グループ ポリシー エディター**」を開き、「**管理用テンプレート > Citrix コンポーネント > Citrix Receiver > クライアントデバイスのリモート処理 > 汎用USBリモート処理**」に移動します。
2. 「**新しいUSBデバイス**」を開き、「**有効**」を選択して「**OK**」をクリックします。
3. 「**既存のUSBデバイス**」を開き、「**有効**」を選択して「**OK**」をクリックします。

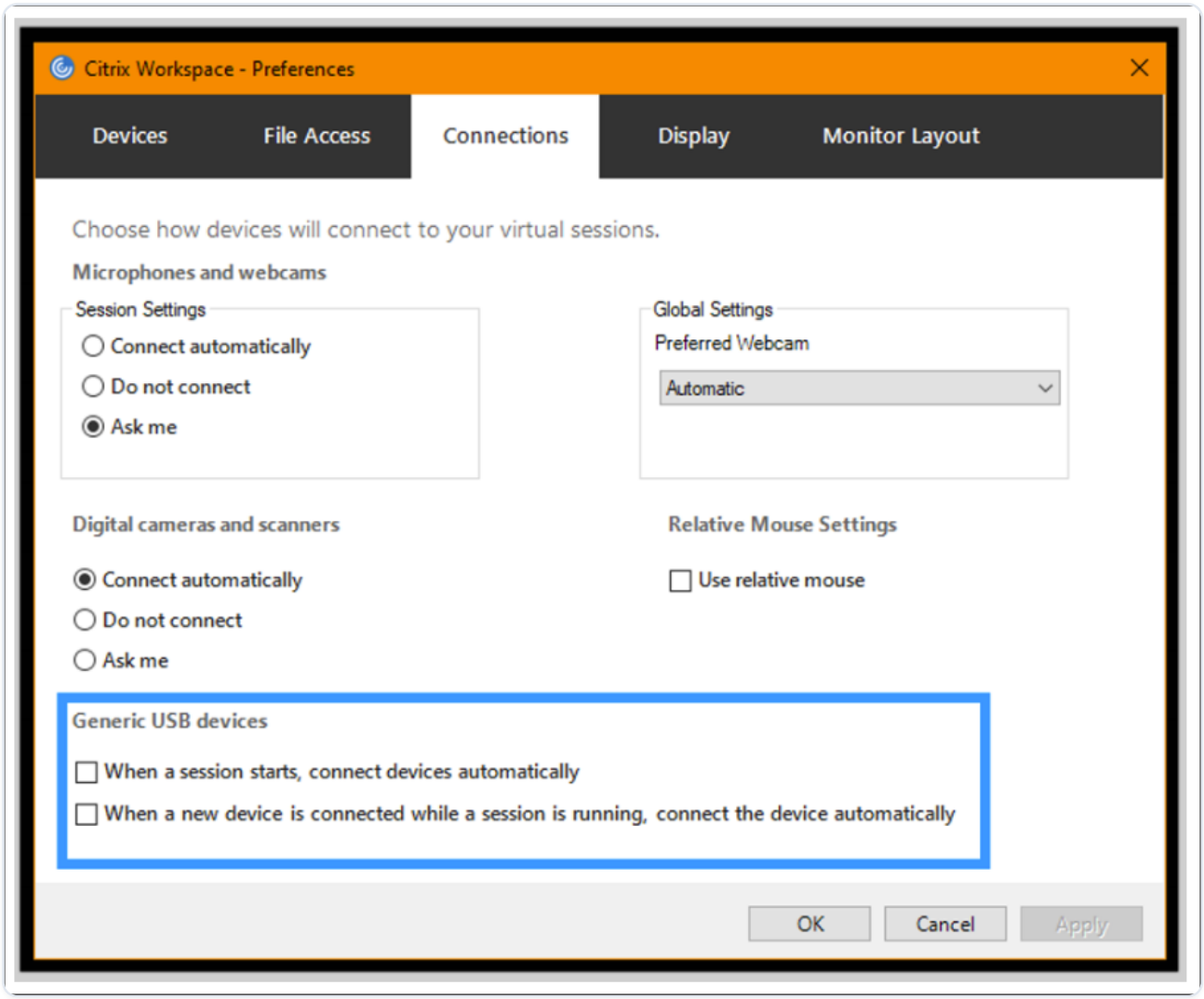


Citrix Connection Centerを使用する場合：

1. 「**Citrix Workspaceの基本設定 > 接続**」に移動します。
2. 次のオプションが選択されていることを確認します。
   a. セッション開始時にデバイスを自動的に接続する
   b. セッション実行中に新しいデバイスが接続された場合、デバイスを自動的に接続する。
3. 「**OK**」をクリックします。

CDViewer接続ツールバーを使用する場合：

1. セッション開始後、「**CDViewer**」ドロップダウンをクリックし、「**Citrix Workspaceの基本設定 > 接続**」タブを選択します。
2. 次のオプションが選択されていることを確認します。
   a. セッション開始時にデバイスを自動的に接続する
   b. セッション実行中に新しいデバイスが接続された場合、デバイスを自動的に接続する。
3. 「**適用**」と「**OK**」をクリックしてポリシーを保存します。



クライアントベースの構成の場合、レジストリキーは次の場所にクライアントデバイスに設定されます。

> **注意！:**
>
> レジストリエディターを使用する前に、この記事の最後にある免責事項を参照してください。 `HKLM\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB`

異なるデバイスルールを使用してUSBリダイレクトで2つ以上のデバイスを構成する

複数のデバイスを異なるデバイスルールでHDX™セッション内にリダイレクトできます。管理者は、あるデバイスを自動的にリダイレクトし、別のデバイスをエンドユーザーがリダイレクトするオプションを提供したい場合があります。以下に、異なるルールで2つのデバイスを構成する手順を示します。

1. **Citrix Web Studio**で**クライアントUSBデバイスリダイレクト**ポリシー設定を有効にします。

2. クライアント側のGPOで**USBデバイスルール**設定を編集します。

    a. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrix Components > Citrix Receiver > リモートクライアントデバイス > Generic USB Remoting**に移動します。

    b. **USBデバイスルール設定**を開き、この設定を有効にします。この例のようにUSBデバイスルールを追加します。**Allow: VID=0911 PID=0c1c**ルールは、**ベンダーID 0911**および**製品ID 0c1c**のデバイスを許可しますが、自動的にはリダイレクトされません。**Connect: VID=06A8 PID=0043**ルールは、ステップ3で言及されている自動リダイレクトポリシーが設定されている場合、**ベンダーID 06A8**および**製品ID 0043**のデバイスを自動的にリダイレクトします。

    c. **Allow**: VID=0911 PID=0c1c #Phillips スピーチマイク。

    d. **Connect**: VID=06A8 PID=0043 class=03 # Topaz HSB シグネチャパッド

3. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrix Components > Citrix Receiver > リモートクライアントデバイス > Generic USB Remoting**に移動します。
4. **新しいUSBデバイス**を開き、**有効**を選択して**OK**をクリックします。
5. **既存のUSBデバイス**を開き、**有効**を選択して**OK**をクリックします。

これらの設定が構成されると、Topaz署名パッドはHDXセッション内に自動的にリダイレクトされ、セッション内でPhillipsスピーチマイクをリダイレクトするには、追加のエンドユーザー操作（接続センターまたはCDビューアーのデバイスタブでリダイレクトオプションを選択）が必要になります。

> **注：**

> 上記の手順2と3の設定は、GenericUSBキー (HKLM\SOFTWARE\Wow6432Citrix\ICA Client\GenericUSB) の下のクライアント側レジストリ値「**DeviceRules**」に直接適用できますが、これは推奨される方法ではありません。

クライアントドライブマッピング

クライアントドライブマッピングを使用すると、クライアントエンドポイント上のストレージドライブがCitrix HDX™セッション内で利用可能になり、ファイルやフォルダーをクライアントからセッションホストへ、またはその逆に転送できるようになります。この機能は、読み取りおよび書き込みの両方の権限でデフォルトで有効になっています。マップされたクライアントデバイス上

のファイルやフォルダーをユーザーが追加または変更できないようにするには、**読み取り専用クライアントドライブアクセス**ポリシー設定を有効にします。この設定をポリシーに追加する際は、**クライアントドライブリダイレクト**設定が**許可**に設定されており、ポリシーにも追加されていることを確認してください。

セキュリティ上の予防措置として、エンドポイントドライブはデフォルトで実行権限なしでマップされます。ユーザーがマップされたクライアントドライブから直接実行可能ファイルを実行できるようにするには、セッションホストで**ExecuteFromMappedDrive**レジストリ値を編集します。詳細については、**レジストリで管理されるHDX機能**セクションのマップされたクライアントドライブを参照してください。

要件

CDMを使用するための要件は次のとおりです。

Citrixコントロールプレーン

- Citrix Virtual Apps and Desktops™ 1912以降のバージョン
- Citrix DaaS™ サービス

セッションホスト

- オペレーティングシステム
  - Windows 10 1809以降
  - Windows Server 2016 以降のバージョン
  - Linux: Linux VDAのシステム要件を参照してください。
- VDA
  - Windows: Citrix Virtual Apps and Desktops 1912 以降のバージョン
  - Linux: Linux VDA のドキュメントを参照してください。

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809以降
  - Linux: Workspace app for Linux のシステム要件を参照してください。

関連ポリシー

CDM設定については、ポリシー設定リファレンスセクションを参照してください。

ダブルホップシナリオ

CDMはダブルホップシナリオでサポートされています。デフォルトでは、クライアントエンドポイントのドライブはセカンドホップセッションにマップされ、ファーストホップのドライブは利用できません。ただし、クライアントエンドポイントのドライブの代わりに、ファーストホップのドライブがセカンドホップセッションにマップされるように設定することもできます。

この機能を構成するには、以下のレジストリ値を編集します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientDrive\
- 値の名前: NativeDriveMapping
- 値の型: REG_SZ
- 値のデータ:
  - True - ファーストホップセッションのドライブをセカンドホップセッションにマップします
  - False - セカンドホップセッションでクライアントエンドポイントのドライブをマップします

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

モバイルデバイスとタッチスクリーンデバイス

Citrix Virtual Apps and Desktops™ を使用すると、ユーザーは公開されたアプリケーションやデスクトップにモバイルおよびタッチスクリーンクライアントデバイスからアクセスできます。

要件

Citrix® コントロールプレーン

- Citrix Virtual Apps and Desktops 1912 以降
- Citrix DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1903 以降
  - Windows 11 21H2 以降
- VDA
  - ウィンドウズ: Citrix Virtual Apps and Desktops バージョン 7.15 以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
- Windows 版 Citrix Workspace™ アプリ バージョン 1808 以降

Windows Continuum を使用するタッチスクリーンデバイスのタブレットモード

Continuum は、クライアントデバイスの使用方法に適応する Windows 10 の機能です。VDA は、タッチ対応クライアントでキーボードまたはマウスの存在を検出すると、クライアントをデスクトップモードにします。キーボードまたはマウスが存在しない場合、VDA はクライアントをタブレット/モバイルモードにします。この検出は、セッション接続時および再接続時、ならびにセッション中にキーボードまたはマウスが接続または切断されたときに発生します。

この機能はデフォルトで有効になっています。この機能を無効にするには、ポリシー設定 タブレットモード切り替えポリシー設定 を構成します。

上記のタッチスクリーンデバイスの要件に加えて、Windows Continuumには以下が必要です。

XenServer (ゼノサーバー) (旧称: Citrix Hypervisor™)

- Citrix Hypervisor 8.2 以降

- ラップトップ/タブレットの切り替えを許可するには、XenServer CLI コマンドを実行します。
  xe vm-param-set uuid=\<VM_UUID\> platform:acpi_laptop_slate=1

重要:

メタデータ設定を変更した後に既存のマシンカタログのベースイメージを更新しても、以前にプロビジョニングされたVMには影響しません。XenServer VMのベースイメージを変更した後、カタログを作成し、ベースイメージを選択して、新しいMachine Creation Services™ (MCS) マシンをプロビジョニングします。

セッションホスト

- オペレーティングシステム
  - Windows 10 1903 以降
  - Windows 11 21H2 以降
- VDA
  - Windows: バージョン 7.16 以降
  - **オペレーティングシステム構成の現在の制限により、ユーザーは最初のICA®セッションを開始してVDAを再起動した後、ドロップダウンメニューから次のオプションを設定する必要があります。**
    - **設定 > システム > タブレットモード**
      - ハードウェアに適したモードを使用する
      - 確認せずに常に切り替える

タブレットモードは、タッチスクリーンにより適したユーザーインターフェイスを提供します。

- わずかに大きいボタン。
- スタート画面と起動するすべてのアプリが全画面で開きます。
- タスクバーに「戻る」ボタンが含まれています。
- タスクバーからアイコンが削除されます。

ファイルエクスプローラーにアクセスできます。

Windows 10 は、この更新された BIOS に基づいて、ターゲット仮想マシンに GPIO ドライバーをロードします。これは、仮想マシン内でタブレットモードとデスクトップモードを切り替えるために使用されます。

HTML5 用 Citrix Workspace アプリは、Windows Continuum 機能をサポートしていません。

デスクトップモードは、PCとキーボード、マウスを使用するのと同じ方法で操作できる、従来のユーザーインターフェイスを提供します。

Microsoft Surface Pro および Surface Book のペン

Windows Inkベースのアプリケーションで標準のペン機能に対応しています。サポートには、ポインティング、消去、筆圧、Bluetooth信号、およびオペレーティングシステムのファームウェアとペンモデルに応じたその他の機能が含まれます。たとえば、筆圧は最大4096レベルまで可能です。この機能はデフォルトで有効になっています。

ペン機能のサポート要件は次のとおりです。

Citrixコントロールプレーン

- Citrix Virtual Apps and Desktops のバージョン 1903 以降
- シトリックス DaaS

セッションホスト

- オペレーティングシステム
  - Windows 10 1809以降
  - Windows 11 21H2 以降
- VDA
  - Windows: シトリックス バーチャルアプリおよびデスクトップ 1903 以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809以降
  - Windows 11 21H2以降
- Windows版Citrix Workspaceアプリ バージョン1902以降

Windows Inkとペン機能のデモンストレーションについては、このグラフィックをクリックしてください:



この機能を無効または有効にするには、レジストリで管理される機能の一覧にあるMicrosoft Surface ProおよびSurface Bookペンを参照してください。

既知の問題

ペンサポートに関する既知の問題は次のとおりです。

- Windows Server 2k22のOSの制限により、ユーザーは2k22サーバーアプリケーションまたはデスクトップに接続している際に、コントロールパネルでペンのショートカットを設定したり、ペン/インクの設定を調整したりすることはできません。
- OSの制限により、ペン対応のWindows 11クライアントからのペンのショートカットは機能しません。

シリアルポート

ほとんどの新しいPCには、内蔵のシリアル（COM）ポートがありません。USBコンバーターを使用すると、ポートを簡単に追加できます。シリアルポートに適したアプリケーションには、センサー、コントローラー、古いチェックリーダー、パッドなどがよく含まれます。一部のUSB仮想COMポートデバイスは、Windowsが提供するドライバー（usbser.sys）の代わりに、ベンダー固有のドライバーを使用します。これらのドライバーを使用すると、USBデバイスの仮想COMポートを強制的に設定できるため、異なるUSBソケットに接続しても変更されません。これは、**デバイスマネージャー > ポート (COM と LPT) > プロパティ**から、またはデバイスを制御するアプリケーションから行うことができます。

クライアントCOMポートマッピングを使用すると、ユーザーのエンドポイントのCOMポートに接続されたデバイスを仮想セッション中に使用できます。これらのマッピングは、他のネットワークマッピングと同様に使用できます。

各COMポートには、オペレーティングシステムのドライバーがCOM1やCOM2などのシンボリックリンク名を割り当てます。アプリケーションは、そのリンクを使用してポートにアクセスします。

> **重要:**

デバイスがUSBを直接使用してエンドポイントに接続できるからといって、汎用USBリダイレクトを使用してリダイレクトできるとは限りません。一部のUSBデバイスは仮想COMポートとして機能し、アプリケーションは物理シリアルポートと同じ方法でアクセスできます。オペレーティングシステムはCOMポートを抽象化し、ファイル共有のように扱うことができます。仮想COMの2つの一般的なプロトコルは、CDC ACMまたはMCTです。RS-485ポートを介して接続すると、アプリケーションがまったく機能しない場合があります。RS-485をCOMポートとして使用するには、RS-485-to-RS232コンバーターを入手してください。 **重要:**

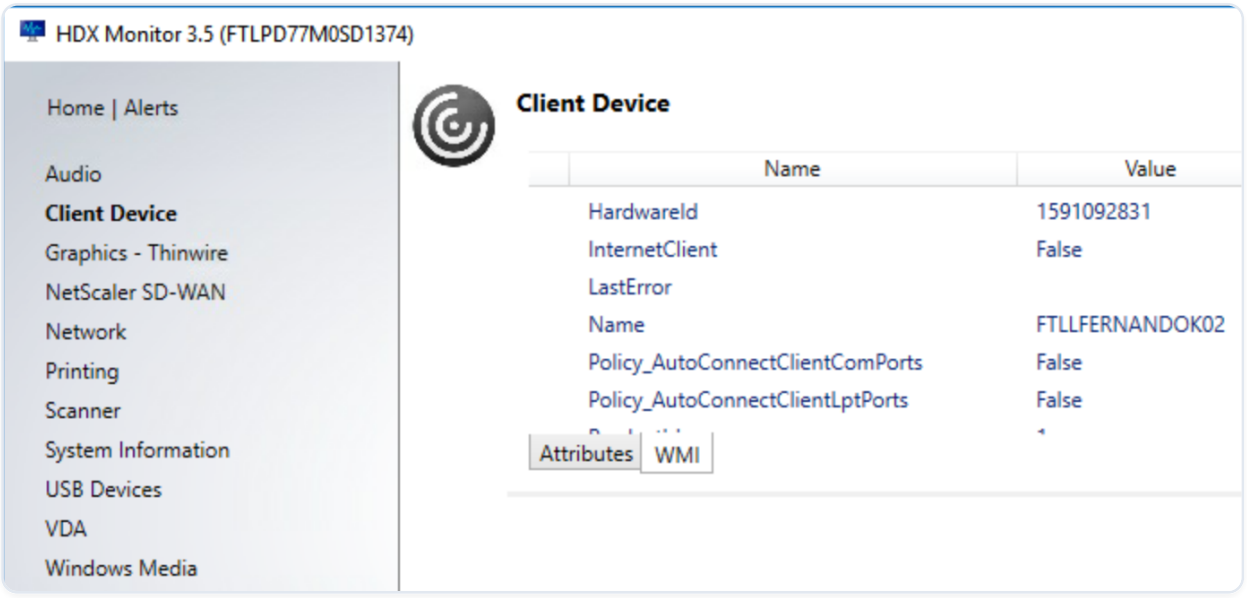
一部のアプリケーションは、デバイス（署名パッドなど）がクライアントワークステーションのCOM1またはCOM2に接続されている場合にのみ、一貫して認識します。

クライアントCOMポートをサーバーCOMポートにマッピングする

クライアントCOMポートをCitrix®セッションにマッピングするには、3つの方法があります。

- Studioポリシー。ポリシーの詳細については、「ポートリダイレクトポリシー設定」を参照してください。
- VDAコマンドプロンプト。
- リモートデスクトップ（ターミナルサービス）構成ツール。

1. **クライアントCOMポートリダイレクト**ポリシーと**クライアントCOMポートの自動接続Studio**ポリシーを有効にします。適用後、一部の情報はHDX™ Monitorで利用できます。



2. **クライアントCOMポートの自動接続**がポートのマッピングに失敗した場合は、手動でポートをマッピングするか、ログオンスクリプトを使用できます。VDAにログオンし、コマンドプロンプトウィンドウで次のように入力します。

   NET USE COMX: `\CLIENT\COMZ`:

   または

   NET USE COMX: `\CLIENT\CLIENTPORT:COMZ`:

   X は VDA 上の COM ポートの番号です (ポート 1 から 9 までがマッピングに利用可能です)。**Z** はマッピングしたいクライアント COM ポートの番号です。

   操作が成功したことを確認するには、VDA のコマンドプロンプトで **NET USE** と入力します。表示されるリストには、マップされたドライブ、LPT ポート、およびマップされた COM ポートが含まれます。



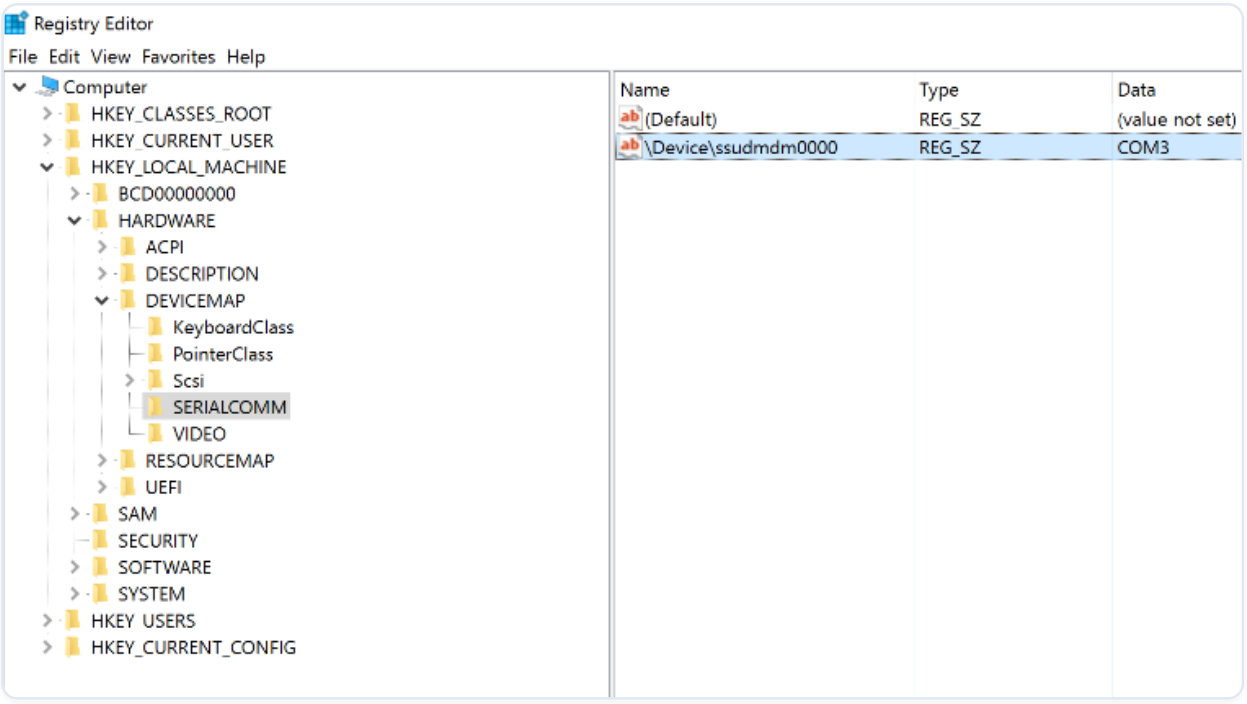
3. このCOMポートを仮想デスクトップまたはアプリケーションで使用するには、ユーザーデバイスアプリケーションをインストールし、マップされたCOMポート名を指定します。たとえば、クライアント上のCOM1をサーバー上のCOM3にマップする場合、VDAにCOMポートデバイスアプリケーションをインストールし、セッション中にCOM3を指定します。このマップされたCOMポートは、ユーザーデバイス上のCOMポートと同様に使用します。

重要:

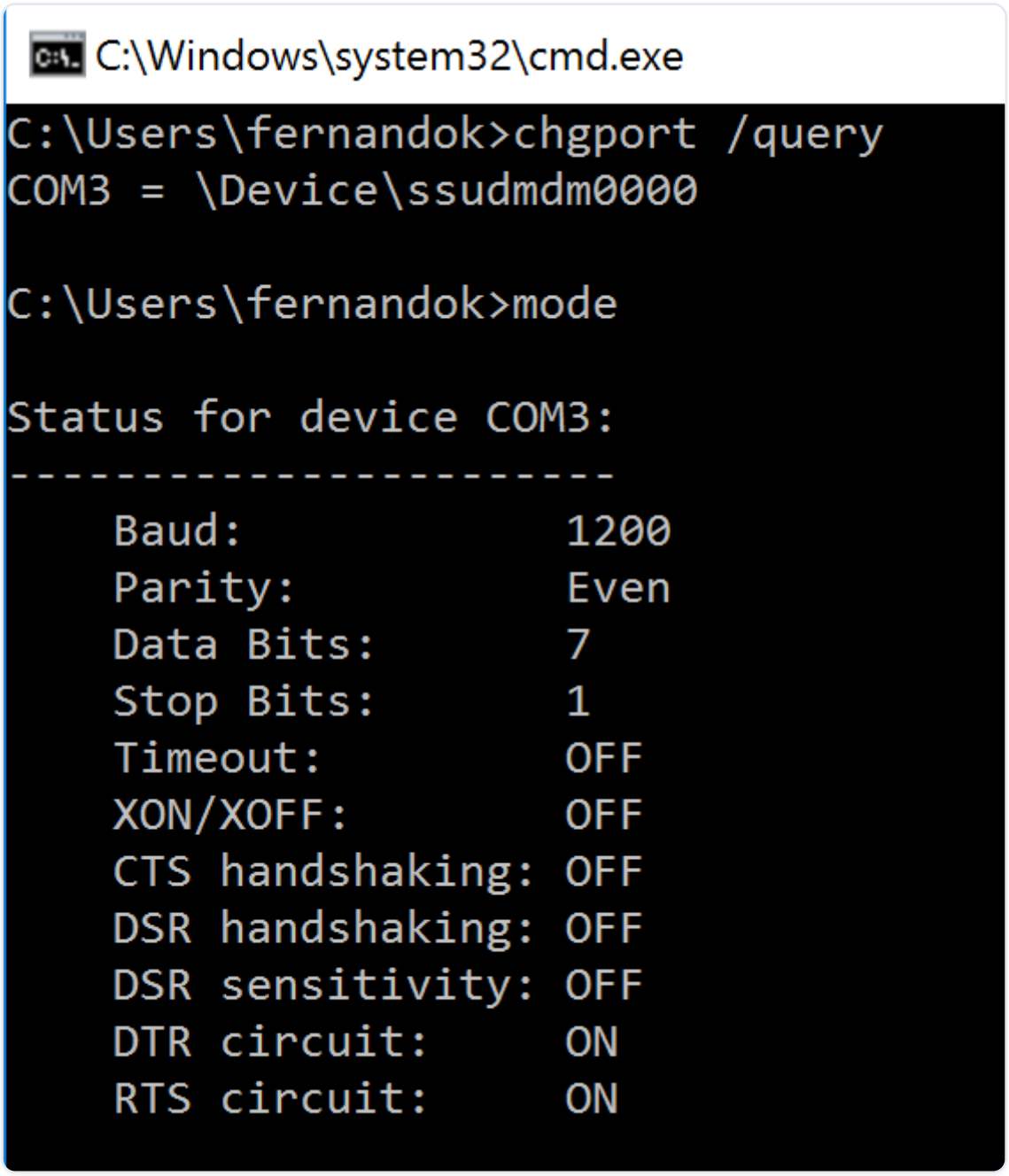
COM ポートマッピングは TAPI と互換性がありません。Windows Telephony Application Programming Interface (TAPI) デバイスをクライアント COM ポートにマップすることはできません。TAPI は、アプリケーションがデータ、FAX、音声通話の電話機能を制御するための標準的な方法を定義します。TAPI は、ダイヤル、応答、通話終了などのシグナリングを管理します。また、保留、転送、会議通話などの付加サービスも管理します。

トラブルシューティング

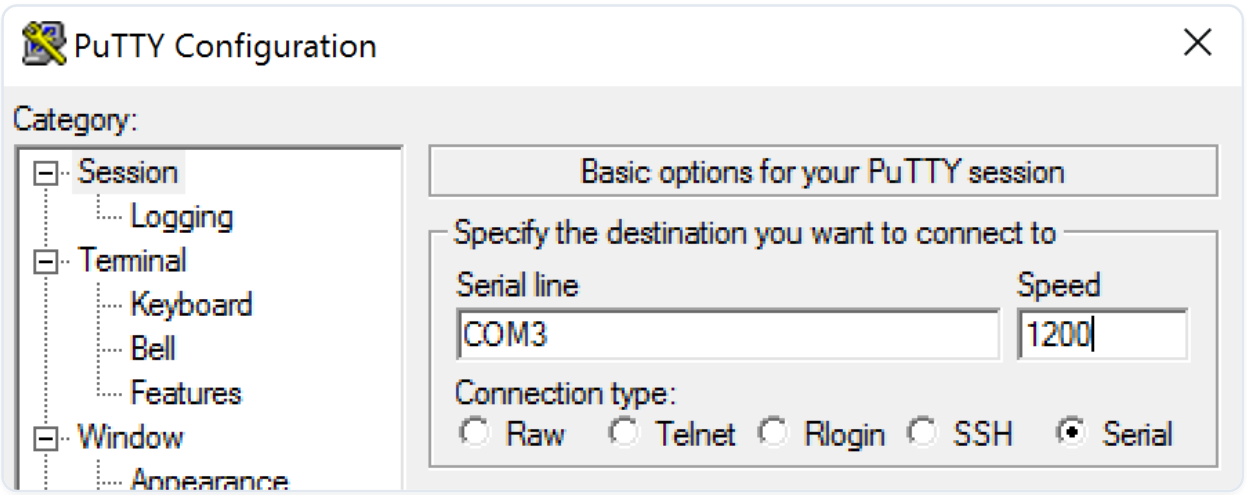
1. Citrix をバイパスして、エンドポイントからデバイスに直接アクセスできることを確認してください。ポートが VDA にマップされていない間は、Citrix セッションに接続されていません。デバイスに付属のトラブルシューティング手順に従い、まずローカルで動作することを確認してください。 デバイスがシリアル COM ポートに接続されている場合、ここに示されているハイブにレジストリキーが作成されます。



この情報は、コマンドプロンプトで **chgport /query** を実行することでも確認できます。



デバイスのトラブルシューティング手順が利用できない場合は、PuTTYセッションを開いてみてください。**Session** を選択し、**Serial line** でCOMポートを指定します。



ローカルコマンドウィンドウで**MODE**を実行できます。出力には、使用中のCOMポートと、PuTTYセッションで必要となるボーレート/パリティ/データビット/ストップビットが表示される場合があります。PuTTY接続が成功した場合、**Enter**キーを押してデバイスからのフィードバックを確認します。入力した文字が画面に繰り返されたり、応答されたりする場合があります。この手順が失敗した場合、仮想セッションからデバイスにアクセスすることはできません。

2. ローカルのCOMポートをVDAにマップし (ポリシーまたは**NET USE COMX: `\CLIENT\COMZ`:**を使用して)、前の手順と同じPuTTYの手順を繰り返しますが、今回はVDAのPuTTYから実行します。PuTTYがエラー「**Unable to open connection to COM1. Unable to open serial port**」を表示する場合、別のデバイスがCOM1を使用している可能性があります。

3. **chgport /query**を実行します。VDA上の組み込みWindowsシリアルドライバーが \Device\Serial0をVDAのCOM1ポートに自動割り当てしている場合、次の手順を実行します。
   A. VDAでCMDを開き、**NET USE**と入力します。

   B. VDA上の既存のマッピング（例：COM1）を削除します。

   NET USE COM1 /DELETE

   C. デバイスをVDAにマッピングします。

   NET USE COM1: `\CLIENT\COM3`:

   D. VDA上のアプリケーションをCOM3にポイントします。

   最後に、ローカルのCOMポート (例: COM3) をVDA上の別のCOMポート (COM1以外、例: COM3) にマップしてみてください。アプリケーションがそれを指していることを確認してください: **NET USE COM3: `\CLIENT\COM3`**

4. ポートがマッピングされていることが確認でき、PuTTYは動作しているもののデータが通過しない場合、それは競合状態である可能性があります。アプリケーションがマッピングされる前にポートに接続して開いてしまい、マッピングをロックしている可能性があります。次のいずれかを試してください。

   - 同じサーバーで公開されている2番目のアプリケーションを開きます。ポートがマッピングされるまで数秒待ち、その後、ポートを使用しようとする実際のアプリケーションを開きます。
   - Studioではなく、Active Directoryのグループポリシーエディターから COMポートリダイレクトポリシーを有効にします。これらのポリシーは「**Client COM port redirection**」と「**Auto connect client COM ports**」です。このように適用されたポリシーは、Studioポリ

シーよりも前に処理され、COMポートが確実にマッピングされるようにする可能性があります。CitrixポリシーはVDAにプッシュされ、次の場所に保存されます。
`HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`

- ユーザーにこのログオンスクリプトを使用するか、アプリケーションを公開する代わりに、まずVDA上のマッピングを削除し、仮想COMポートを再マッピングしてからアプリケーションを起動する.batスクリプトを公開します。

@echo off NET USE COM1 /delete NET USE COM2 /delete NET USE COM1: `\CLIENT\COM1` : NET USE COM2: `\CLIENT\COM2` : MODE COM1: BAUD=1200 (または必要な値) MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (または必要な値) START `C:\Program Files\<Your Software Path>\<your_software.exe>`

5. SysinternalsのProcess Monitorは、最後の手段となるツールです。VDAでこのツールを実行する際、COM3、picaser.sys、CdmRedirectorなどのオブジェクト、特に\<your_app\>.exeを見つけてフィルターします。エラーは「アクセス拒否」またはそれに類するものとして表示される場合があります。

特殊キーボード

Bloombergキーボード

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

Citrix Virtual Apps and Desktops™ は、Bloomberg モデル 5、モデル 4 Starboard キーボード（およびそれ以前のモデル 3）をサポートしています。このキーボードにより、金融業界のお客様は、キーボードの特殊機能を使用して金融市場データにアクセスし、迅速に取引を実行できます。

> **重要:**

> Bloombergキーボードは1つのセッションでのみ使用することをお勧めします。複数の同時セッション（1つのクライアントから複数のセッションへ）でキーボードを使用することはお勧めしません。

> Bloomberg キーボードは、1つの物理シェルに複数の USB デバイスを搭載した USB コンポジットデバイスです。

- キーボード。
- 指紋リーダー。
- 音量を上げたり下げたり、スピーカーとマイクをミュートしたりするキーを備えたオーディオデバイス。このデバイスには、オンボードスピーカー、マイク、およびマイクとヘッドセット用のジャックが含まれています。
- これらのデバイスすべてをシステムに接続するための USB ハブ。

要件:

- Citrix Workspace™ app for Windows が接続するセッションは、USB デバイスをサポートしている必要があります。
- Bloomberg キーボードモデル 5 をサポートするには、Citrix Workspace app 2207 for Linux 以降が必要です。
- Bloomberg keyboard モデル 5 をサポートするには、Windows 用 Citrix Workspace アプリ 2109 以降が必要です。
- Bloomberg keyboard モデル 3 および 4 をサポートするには、Windows 用 Citrix Workspace アプリ 1808 以降、または Windows 用 Citrix Receiver 4.8 以降が必要です。
- モデル 4 で KVM モード (KVM を介してルーティングされる 1 本を含む 2 本の USB ケーブル) を使用するには、Windows 用 Citrix Workspace アプリ 1808 以降、または Windows 用 Citrix Receiver 4.12 以降が必要です。

Windows 用 Citrix Workspace アプリでの Bloomberg keyboard の構成については、「Bloomberg keyboard の構成」を参照してください。

Bloomberg keyboard のサポートを有効にするには、レジストリで管理される機能のリストにある「Bloomberg keyboard」を参照してください。

サポートを確認する:

Citrix Workspace アプリで Bloomberg keyboard のサポートが有効になっているかどうかを確認するには、Desktop Viewer が Bloomberg keyboard のデバイスを正しく報告しているかどうかを確認します。

デスクトップシナリオ:

Desktop Viewer を開きます。Bloomberg keyboard のサポートが有効になっている場合、Desktop Viewer には USB アイコンの下に 3 つのデバイスが表示されます。

Bloomberg 5 keyboard の場合:

- ブルームバーグLP ブルームバーグ生体認証モジュール
- Bloomberg LP Keyboard (2 つのインターフェイスを持つ複合デバイス)
- Bloomberg LP Keyboard Audio (3 つのインターフェイスを持つ複合デバイス)

Bloomberg 3 および 4 keyboard の場合:

- ブルームバーグ 指紋スキャナー
- Bloomberg キーボードの機能
- Bloomberg LP キーボード 2013

シームレスアプリケーションのみのシナリオ:

Citrix Workspaceアプリの通知領域アイコンから**接続センター**メニューを開きます。Bloomberg キーボードのサポートが有効になっている場合、3つのデバイスが**デバイス**メニューに表示されます。

これらの各デバイスのチェックマークは、それらがセッションにリモート接続されていることを示します。

Windows - キーボードおよびIMEサポートツール

これは、キーボードと入力方式エディターに関連する問題を診断できるセルフサービスのコマンドラインツールです。

さまざまなユーザー要件を満たし、プラットフォームの汎用性を提供し、ユーザーにパーソナライズされたニーズを提供するために、キーボードと入力方式エディター (IME) の機能は、VDA と Citrix Workspace™ アプリのさまざまな構成と機能に依存しています。

VDAまたはクライアント側の設定が正しくないと、予期しない入力動作を引き起こす可能性があります。

ただし、Citrix® はいくつかの一般的な使用シナリオに対して推奨設定を提供しており、これらの推奨事項は診断結果にも含まれています。

このツールを使用すると、以下のカテゴリの問題を特定できます。

- **キーボードタイプの不一致:** VDAキーボードタイプとクライアントキーボードタイプをチェックし、不一致がないか確認します。たとえば、VDAが101英語キーボードを使用しているのに、クライアントが日本語106キーボードを使用している場合などです。この診断は、JP 106/109キーボードおよびKO 103/106キーボードの使用事例を対象としています。
- **キーボードレイアウト同期モードの不一致:** キーボードレイアウト同期設定、レジストリ設定、グループポリシーをチェックし、特定の環境における同期モード構成の問題を解決します。
- **クライアントキーボードレイアウトとVDAキーボードレイアウトの不一致:** クライアントキーボードレイアウトがVDAキーボードレイアウトと同じであるかを確認します
- **アプリケーションセッションでリモート言語バーが表示されない:** エンドユーザーがアプリケーションセッションを起動し、複数のキーボードレイアウトを使用している場合に、リモート言語バーが表示されているかを確認します。

このコマンドラインツールはWindows VDA - `CtxKbImeDiagnostics.exe` にホストされています。 コマンドラインインターフェースは以下のとおりです。

インターフェース	説明	注
`CtxKbimeDiagnostics`	現在のICA®セッションのみの診断結果を表示	ユーザーが管理者権限を持っている場合、すべてのアクティブなICAセッションの診断を表示します。ユーザーが管理者権限を持っていない場合、現在のユーザーのICAセッションの診断を表示します。
`CtxKbimeDiagnostics [-v]`	現在のセッションの設定情報と診断結果を表示	ユーザーが管理者権限を持っている場合、すべてのアクティブなICAセッションの診断を表示します。
`CtxKbimeDiagnostics [-v] [-s Session_Id]`	このセッションの設定情報と診断結果を表示する	

インターフェース	説明	注
`CtxKbimeDiagnostics [-s Session_Id]`	セッションを指定し、そのセッションの診断結果を表示する	管理者権限を持つユーザーは他のICAセッションを照会できます/一般ユーザーは自分のICAセッションのみを照会できます
`CtxKbimeDiagnostics [-s Session_Id] [-v]`	セッションを指定し、そのセッションのすべての設定情報と診断結果を表示する	管理者権限を持つユーザーは他のICAセッションを照会できます。一般ユーザーは自分のICAセッションのみを照会できます。
`CtxKbimeDiagnostics [-h]`	サポートされている引数/パラメーターと例を表示する	「ヘルプ」インターフェース
`CtxKbimeDiagnostics [-V]`	現在のツールバージョンを表示する	

注記:

このバージョンでは、クライアントとしてのCWA Windowsのみがサポートされています。

Webカメラ

高解像度Webカメラストリーミング

Webカメラは、仮想セッション内で実行されているビデオ会議アプリケーションで使用できます。サーバー上のアプリケーションは、サポートされているフォーマットタイプに基づいてWebカメラのフォーマットと解像度を選択します。セッションが開始されると、クライアントはWebカメラ情報をサーバーに送信します。ビデオ会議アプリケーションからWebカメラを選択します。Webカメラとアプリケーションの両方が高解像度レンダリングをサポートしている場合、アプリケーションは高解像度を使用します。Webカメラの解像度は最大1920x1080までサポートしています。

この機能には、Citrix Receiver for Windowsバージョン4.10以降が必要です。HDX Webカメラリダイレクトをサポートするクライアントプラットフォームのリストについては、「Citrix Workspace app feature matrix」を参照してください。

高解像度Webカメラストリーミングの詳細については、「HDX video conferencing and webcam video compression」を参照してください。

レジストリキーを使用してこの機能を無効または有効にし、特定の解像度を構成できます。詳細については、レジストリで管理される機能のリストにある「High-definition webcam streaming and High-definition webcam resolution」を参照してください。

グラフィックス

Citrix HDXグラフィックスには、Citrix Virtual Apps and Desktopsからのリッチグラフィックスアプリケーションの配信を最適化する、広範なグラフィックスアクセラレーションおよびエンコーディングテクノロジーが含まれています。これらのグラフィックテクノロジーは、グラフィックスを多用する仮想アプリケーションをリモートで操作する際に、物理デスクトップを使用するのと同じエクスペリエンスを提供します。

グラフィックレンダリングには、ソフトウェアまたはハードウェアを使用できます。ソフトウェアレンダリングには、ソフトウェアラスタライザーと呼ばれるサードパーティ製ライブラリが必要です。たとえば、WindowsにはDirectXベースのグラフィック用のWARPラスタライザーが含まれています。場合によっては、代替のソフトウェアレンダラーを使用したいと思うかもしれません。ハードウェアレンダリング（ハードウェアアクセラレーション）には、グラフィックプロセッサ（GPU）が必要です。

HDX™ Graphicsは、最も一般的なユースケース向けに最適化されたデフォルトのエンコーディング構成を提供します。Citrixポリシーを使用することで、IT管理者はさまざまな要件を満たし、望ましいユーザーエクスペリエンスを提供するために、さまざまなグラフィック関連設定を構成することもできます。

シンワイヤー

Thinwireは、Citrix Virtual Apps and Desktopsで使用されるCitrixのデフォルトのディスプレイリモートテクノロジーです。

ディスプレイリモートテクノロジーにより、あるマシンで生成されたグラフィックスを、通常はネットワーク経由で別のマシンに送信して表示できます。グラフィックスは、キーボード入力やマウス操作などのユーザー入力の結果として生成されます。

HDX スリーディープロ

Citrix Virtual Apps and DesktopsのHDX 3D Pro機能を使用すると、ハードウェアアクセラレーションにグラフィックス処理ユニット（GPU）を使用して最高のパフォーマンスを発揮するデスクトップとアプリケーションを配信できます。これらのアプリケーションには、OpenGLおよびDirectXベースの3Dプロフェッショナルグラフィックスアプリケーションが含まれます。標準VDAはDirectXのGPUアクセラレーションのみをサポートします。

WindowsシングルセッションOSのGPUアクセラレーション

HDX 3D Proを使用すると、ホスト型デスクトップまたはシングルセッションOSマシン上のアプリケーションの一部として、グラフィックを多用するアプリケーションを配信できます。HDX 3D Proは、物理ホストコンピューター（デスクトップ、ブレード、ラックワークステーションを含む）と、XenServer®、vSphere、Hyper-V（パススルーのみ）ハイパーバイザーが提供するGPUパススルーおよびGPU仮想化テクノロジーをサポートします。

GPUパススルーを使用すると、専用のグラフィックス処理ハードウェアに排他的にアクセスできるVMを作成できます。ハイパーバイザーに複数のGPUをインストールし、これらのGPUのそれぞれにVMを1対1で割り当てることができます。

GPU仮想化を使用すると、複数の仮想マシンが単一の物理GPUのグラフィックス処理能力に直接アクセスできます。

WindowsマルチセッションOSのGPUアクセラレーション

HDX 3D Proを使用すると、WindowsマルチセッションOSセッションで実行されているグラフィックス負荷の高いアプリケーションを、サーバーのグラフィックス処理ユニット（GPU）でレンダリングできます。OpenGL、DirectX、Direct3D、およびWindows Presentation Foundation（WPF）のレンダリングをサーバーGPUに移行することで、グラフィックスレンダリングがサーバーCPUの速度を低下させることはありません。また、ワークロードがCPUとGPUに分割されるため、サーバーはより多くのグラフィックスを処理できます。

フレームホーク

> **重要:**

> Citrix Virtual Apps and Desktops 7 1903以降、Framehawk はサポートされなくなりました。代わりに、Thinwire を アダプティブトランスポート を有効にして使用してください。

> Framehawk は、ブロードバンドワイヤレス接続（Wi-Fi および 4G/LTE 携帯電話ネットワーク）を使用するモバイルワーカー向けのディスプレイリモートテクノロジーです。Framehawk は、スペクトル干渉とマルチパス伝播の課題を克服し、仮想アプリおよびデスクトップのユーザーに、スムーズでインタラクティブなユーザーエクスペリエンスを提供します。

テキストベースのセッションウォーターマーク

テキストベースのセッションウォーターマークは、データ盗難を抑止し、追跡を可能にするのに役立ちます。この追跡可能な情報は、写真やスクリーンキャプチャを使用してデータを盗む者への抑止力として、セッションデスクトップに表示されます。テキストのレイヤーであるウォーターマークを指定できます。ウォーターマークは、元のドキュメントのコンテンツを変更することなく、セッション画面全体に表示できます。テキストベースのセッションウォーターマークには VDA のサポートが必要です。

アダプティブリフレッシュレート

新しいスケーラビリティの改善により、HDX は、仮想モニターのリフレッシュレートをターゲット FPS ポリシー設定に一致させます。アダプティブリフレッシュレート（ARR）は、シングルセッション VDA とマルチセッション VDA の両方で利用でき、GPU アクセラレーションシナリオと非 GPU シナリオの両方で機能します。

ロス許容モード

ロス耐性モードは徹底的に再設計され、パケットロスが検出された場合でもセッションがインタラクティブな状態を維持するようにします。

関連情報

- エイチディーエックス スリーディー プロ
- Windows シングルセッション OS 用 GPU アクセラレーション
- Windows マルチセッション OS 用 GPU アクセラレーション
- フレームホーク
- シンワイヤ
- テキストベースのセッションウォーターマーク

10ビット ハイダイナミックレンジ (HDR)

10ビットハイダイナミックレンジ (HDR) 仮想デスクトップセッションでは、拡張されたエンコードおよびデコード機能を使用して、より広い色域、より高いコントラストと明るさで高品質の画像やビデオをレンダリングできます。また、ホワイト輝度レベル、Extended Display Identification Data (EDID)、および視覚品質をカスタマイズして、ユーザーエクスペリエンスを向上させることができます。

システム要件

エンドポイント:

- NVIDIA GPU 用の Citrix Workspace™ Windows 用アプリ 2209 以降
- エンドポイントで10ビットHEVC (H.265) 444デコードをサポートするNVIDIA GPU
- 10ビットHDR対応モニター。すべてのモニターでディスプレイ設定を使用して10ビットHDRを有効にする必要があります。

サーバー:

- NVIDIA GPU 用 Windows シングルセッションOS VDA 2209 以降、およびIntel GPU 用 VDA 2308 以降
- VDA上で10ビットHEVC 444エンコードをサポートするNVIDIA GPU

必要なポリシー

エンドポイント:

- グラフィックのH.265デコードを有効にする

サーバー:

- 3Dグラフィックワークロード向けに最適化する
- グラフィックスステータスインジケーター (オプション)

サーバー構成

10ビットHDR対応のエンドポイントモニターでCitrix®セッションを起動すると、HDRセッションがデフォルトで有効になります。マルチモニターHDRセッションでは、すべてのエンドポイントモニターで10ビットHDRが有効になっている必要があります。HDRセッションは、ウィンドウモードと全画面モードの両方でサポートされています。

参照白色レベル

この設定は、ニット値によって白色輝度レベルを定義します。セッション内の相対的なHDR画面の明るさを制御します。デフォルト値は80ニットです。異なるニット値を定義するには、次のレジストリキーを設定します。

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- 種類: REG_DWORD
- 名前: RefWhiteLevel

設定を有効にするには、セッションのサイズを変更するか、セッションを切断して再起動する必要があります。

EDIDのオーバーライド

VDAをHDRセッションでエンドポイントモニターのEDIDを使用するように構成できます。これにより、色域と輝度範囲を一致させることで、モニターの表示機能を最大限に活用できます。デフォルトでは、HDRセッションはHDR1000対応のディスプレイを想定しています。 エンドポイントモニターのEDIDは、NVIDIAまたはその他のツールを使用してエクスポートできます。次のレジストリキーを使用してVDAに適用します。

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- 種類: REG_BINARY
- 設定名: EDIDOverride

EDIDをレジストリに保存する際、コンマ、スペース、または特殊文字を含めてはなりません。
オーバーライドEDIDを有効にするには、サインアウトして新しいセッションを起動します。

視覚的にロスレスなエクスペリエンス

視覚的にロスレスなエクスペリエンスを実現するには、次のポリシーを有効にします。

- 視覚的にロスレス圧縮を許可する
- 視覚品質: 常にロスレスまたはロスレスに構築

ポリシーを設定した後、グラフィックステータスインジケーターを使用して、画質スライダーを使用するか、ピクセルパーフェクトモードに切り替えることで、HDRセッションの品質を制御できます。

Windowsの画面ロックを許可する

このポリシーを使用すると、画面ロックを含むすべてのWindowsディスプレイタイムアウトを、ワークステーションOS上のCitrix Virtual Desktopセッションに適用できます。この設定は、Citrix StudioのCitrixグループポリシーオブジェクトを使用して設定できます。

デフォルトでは、この設定が有効になっていない場合、アクティブなセッション中にCitrix Virtual Desktopはセッションロック、スクリーンセーバー、またはディスプレイオフのタイムアウトに応答しません。

ワークステーションVDAでパスワード保護されたスクリーンセーバーが構成されている場合、スクリーンセーバーのタイムアウトに達したときにCitrix Virtual Desktopセッションが自動的にロックされるようにするには、この設定を有効にする必要があります。

VDAでディスプレイオフタイムアウトが構成されているときにこの設定を有効にすると、そのタイムアウトの期限切れにより、ユーザーがセッションとの対話を再開するまで更新されないセッションになります。たとえば、表示されている時間は更新されず、新しい通知も表示されません。

その他の考慮事項

- 仮想GPU上で最大4台のモニターで10ビットHDRセッションを起動できます。
- 次の場合、Citrixセッションは8ビットの非HDRモードに戻ります。
  - いずれかのエンドポイントモニターで10ビットHDRが有効になっていない場合
  - 画面共有を有効にする。
  - VDAで仮想ディスプレイレイアウトを設定する。
  - **視覚的にロスレスな圧縮を許可**ポリシーを設定せずにピクセルパーフェクトモードに切り替える。

HDX™ 3D プロ

Citrix Virtual Apps and Desktops™のHDX 3D Pro機能を使用すると、ハードウェアアクセラレーションのためにグラフィック処理ユニット (GPU) を使用して最高のパフォーマンスを発揮するデスクトップとアプリケーションを提供できます。これらのアプリケーションには、OpenGLおよびDirectXベースの3Dプロフェッショナルグラフィックアプリケーションが含まれます。標準VDAはDirectXのGPUアクセラレーションのみをサポートします。

HDX 3D Proポリシー設定については、「3Dグラフィックワークロードの最適化」(/ja-jp/citrix-virtual-apps-desktops/2407/policies/reference/ica-policy-settings/graphics-policy-settings.html#optimize-for-3d-graphics-workload)を参照してください。

サポートされているすべてのCitrix Workspaceアプリは、3Dグラフィックで使用できます。複雑な3Dワークロード、高解像度モニター、マルチモニター構成、高フレームレートアプリケーションで最高のパフォーマンスを得るには、Citrix Workspace app for WindowsおよびCitrix Workspace app for Linuxの最新バージョンをお勧めします。Citrix Workspaceアプリのサポートされているバージョンに関する詳細については、Citrix Workspaceアプリのライフサイクルマイルストーンを参照してください。

3Dプロフェッショナルアプリケーションの例は次のとおりです。

- コンピューター支援設計、製造、エンジニアリング (CAD/CAM/CAE) アプリケーション
- 地理情報システム (GIS) ソフトウェア
- 医用画像処理通信システム (PACS)

- 最新のOpenGL、DirectX、NVIDIA CUDA、OpenCL、およびWebGLバージョンを使用するアプリケーション
- 並列コンピューティングにNVIDIA Compute Unified Device Architecture (CUDA) GPUを使用する、計算負荷の高い非グラフィックアプリケーション

HDX 3D Proは、あらゆる帯域幅で最高のユーザーエクスペリエンスを提供します。

- WAN接続の場合: 1.5 Mbpsという低い帯域幅のWAN接続でも、インタラクティブなユーザーエクスペリエンスを提供します。
- LAN接続の場合: LAN接続では、ローカルデスクトップと同等のユーザーエクスペリエンスを提供します。

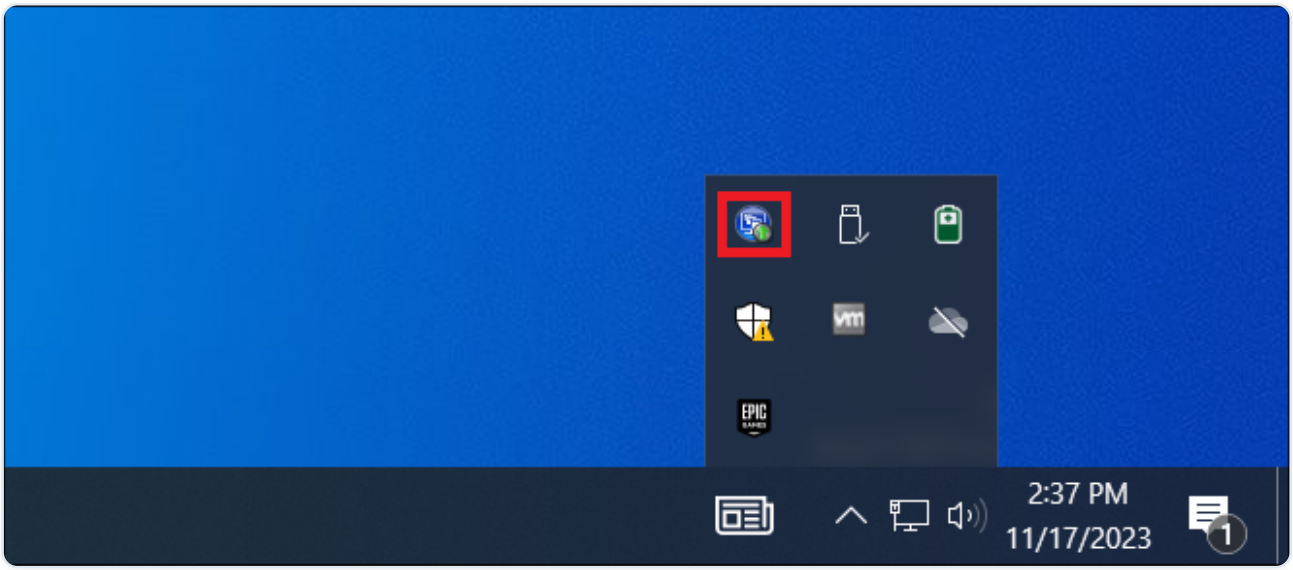
  グラフィック処理をデータセンターに移動して一元管理することで、複雑で高価なワークステーションをよりシンプルなユーザーデバイスに置き換えることができます。

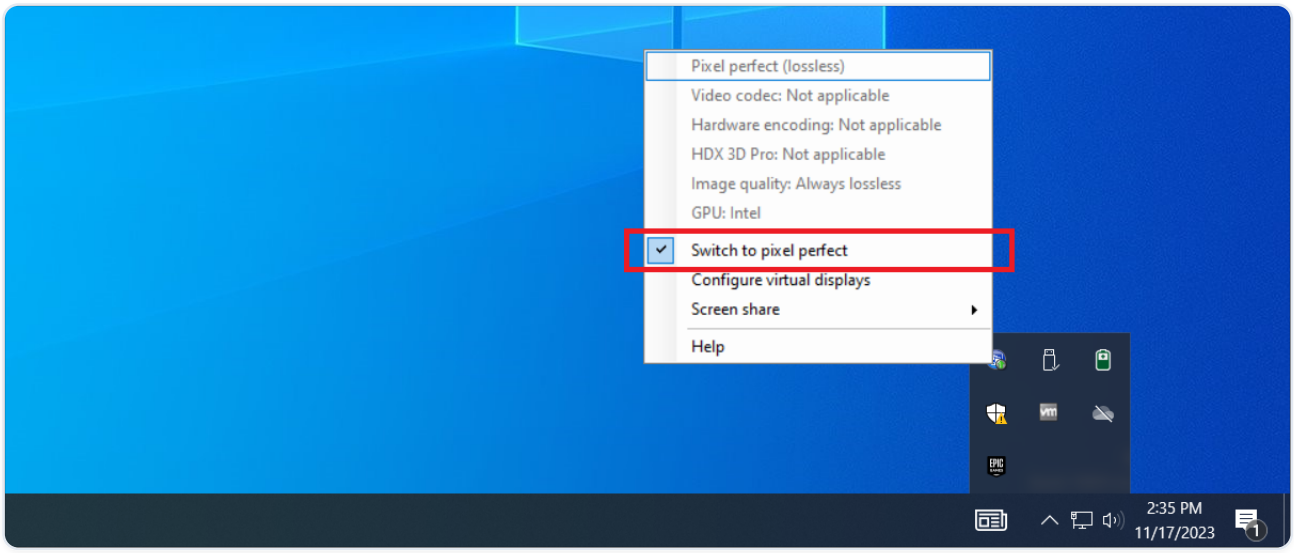
特殊なユースケース向けのロスレス圧縮オプション

HDX 3D Proは、医用画像処理など、ピクセルパーフェクトなグラフィックが必要なアプリケーションをサポートするために、CPUベースのロスレスコーデックも提供します。真のロスレス圧縮は、より多くのネットワークリソースと処理リソースを消費するため、特殊なユースケースでのみ推奨されます。

ロスレス圧縮を使用する場合:

- 通知領域アイコンであるグラフィックステータスインジケーターのロスレスインジケーターは、表示されている画面がロッシーフレームかロスレスフレームかをユーザーに通知します。このアイコンは、**視覚品質**ポリシー設定で**ロスレスにビルド**が指定されている場合に役立ちます。送信されるフレームがロスレスの場合、ロスレスインジケーターは緑色に変わります。





- ロスレススイッチを使用すると、セッション中にいつでも**常にロスレス**モードに変更できます。セッション内で**ロスレス**を選択または解除するには、アイコンを右クリックして**ピクセルパーフェクトに切り替え**をクリックするか、ショートカットALT+SHIFT+1を使用します。
  - ロスレス圧縮の場合: HDX 3D Proは、ポリシーで選択されたコーデックに関係なく、圧縮にロスレスコーデックを使用します。
  - ロッシー圧縮の場合: HDX 3D Proは、デフォルトまたはポリシーで選択された元のコーデックを使用します。 ロスレススイッチの設定は、以降のセッションでは保持されません。すべての接続でロスレスコーデックを使用するには、**視覚品質ポリシー**設定で**常にロスレス**を選択します。

セッション内でロスレスを選択または選択解除するためのデフォルトのショートカットALT+SHIFT+1を上書きできます。
`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator`で新しいレジストリ設定を構成します。

- 名前: HKEY_LOCAL_MACHINE_HotKey、種類: String
- ショートカットの組み合わせを構成する形式は、C=0|1, A=0|1, S=0|1, W=0|1, K=valです。キーはコンマ「,」で区切る必要があります。キーの順序は関係ありません。
- A、C、S、W、Kはキーであり、C=Control、A=ALT、S=SHIFT、W=Win、K=有効なキーです。Kに許可される値は、0〜9、a〜z、および任意の仮想キーコードです。
- 例: F10の場合、K=0x79を設定 Ctrl + F10の場合、C=1, K=0x79を設定 Alt + Aの場合、A=1, K=a または A=1, K=A または K=A, A=1を設定 Ctrl + Alt + 5の場合、C=1, A=1, K=5 または A=1, K=5, C=1を設定 Ctrl + Shift + F5の場合、A=1, S=1, K=0x74を設定

HDX 3D Proのユーザーエクスペリエンスを最適化する

複数のユーザーが帯域幅の制限された接続（たとえば、支店など）を共有している場合、各ユーザーが利用できる帯域幅を制限するために、全体的なセッション帯域幅制限ポリシー設定を使用することをお勧めします。この設定を使用すると、ユーザーがログオンおよびログオフしても、利用可能な帯域幅が大きく変動しないようにできます。HDX 3D Proは利用可能なすべての帯域幅を使用するように自動的に調整されるため、ユーザーセッション全体で利用可能な帯域幅が大きく変動すると、パフォーマンスに悪影響を及ぼす可能性があります。 たとえば、20人のユーザーが60 Mbpsの接続を共有している場合、各ユーザーが利用できる帯域幅は、同時ユーザー数に応じて3 Mbpsから60 Mbpsの間で変動する可能性があります。このシナリオでユーザーエクスペリエンスを最適化するには、ピーク時にユーザーごとに必要な帯域幅を決定し、常にこの量にユーザーを制限します。 3Dマウスのユーザーの場合、汎用USBリダイレクト仮想チャネルの優先度を0に上げることをお勧めします。仮想チャネルの優先度を変更する方法については、Knowledge Centerの記事CTX128190を参照してください。 HDX Monitorツールを使用して、HDX視覚化テクノロジーの操作と構成を検証し、HDXの問題を診断およびトラブルシューティングします。このツールは、Citrix Virtual Apps and Desktopsのインストールメディアの**Support**フォルダーにあります。

WindowsマルチセッションOS向けGPUアクセラレーション

Citrix Virtual Apps and Desktops™ は、WindowsマルチセッションOSセッションで実行されるグラフィック負荷の高いアプリケーションが、サーバーのグラフィック処理ユニット (GPU) でレンダリングされることをサポートします。OpenGL、DirectX、Direct3D、およびWindows Presentation Foundation (WPF) のレンダリングをサーバーのGPUに移行することで、サーバーのCPUをより効率的に使用できます。

Windows Serverはマルチユーザーオペレーティングシステムであるため、複数のユーザーがGPU仮想化 (vGPU) を必要とせずに、Citrix Virtual Apps™ によってアクセスされるGPUを共有できます。

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

GPU 共有

GPU共有により、リモートデスクトップセッションでOpenGLおよびDirectXアプリケーションのGPUハードウェアレンダリングが可能になります。これには次の特徴があります。

- アプリケーションのスケーラビリティとパフォーマンスを向上させるために、ベアメタルまたは仮想マシンで使用できます。
- 複数の同時セッションで GPU リソースを共有できます (ほとんどのユーザーは専用 GPU のレンダリングパフォーマンスを必要としません)。
- 特別な設定は必要ありません。

GPUは、ハイパーバイザーおよびGPUベンダーの要件に従って、フルパススルーモードまたは仮想GPU (vGPU) モードのいずれかでWindows Server仮想マシンに割り当てることができます。物理Windows Serverマシンへのベアメタル展開もサポートされています。

GPU 共有は、特定のグラフィックカードに依存しません。

- 仮想マシンの場合は、使用しているハイパーバイザーと互換性のあるグラフィックカードを選択してください。XenServerのハードウェア互換性リストについては、「ハイパーバイザーハードウェア互換性リスト」を参照してください。
- ベアメタルで実行する場合は、オペレーティングシステムによって有効化された単一のディスプレイアダプターを使用することをお勧めします。ハードウェアに複数のGPUがインストールされている場合は、デバイスマネージャーを使用して、1つを除くすべてを無効にしてください。

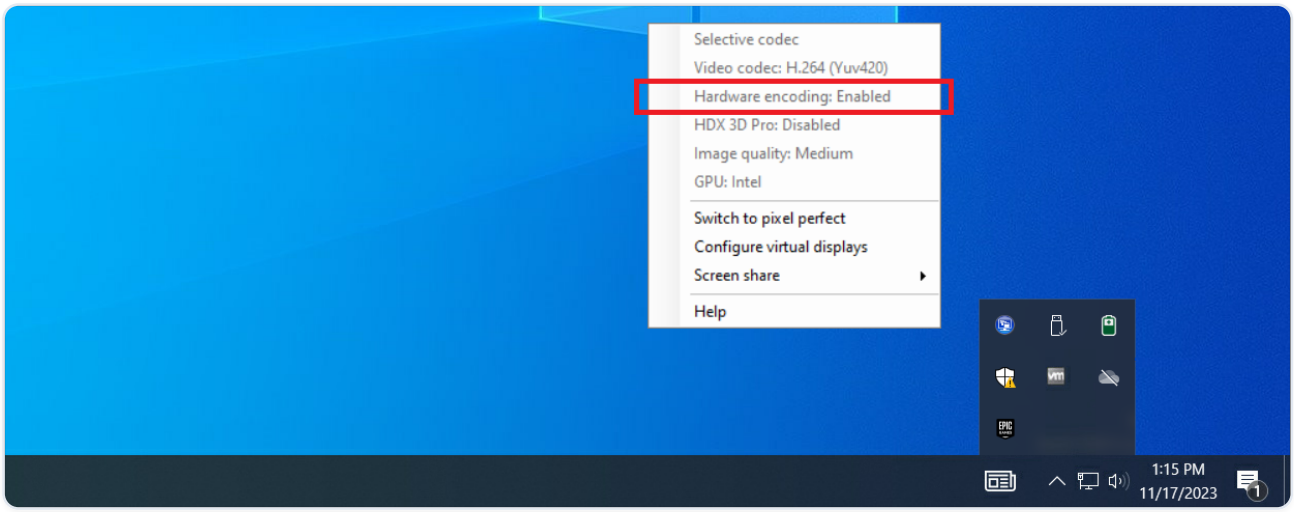
GPU Sharing を使用したスケーラビリティは、いくつかの要因によって異なります。

- 実行されているアプリケーション
- 消費するビデオRAMの量
- グラフィックカードの処理能力

一部のアプリケーションは、他のアプリケーションよりもビデオ RAM の不足をうまく処理します。ハードウェアが過負荷になると、グラフィックカードドライバーの不安定化やクラッシュが発生する可能性があります。このような問題を回避するには、同時ユーザー数を制限してください。

- NVIDIA GPUおよびIntel Iris Proグラフィックプロセッサ用の高性能ビデオエンコーダーへのアクセス。ポリシー設定（デフォルトで有効）がこの機能を制御し、H.264エンコーディング（利用可能な場合）にハードウェアエンコーディングの使用を許可します。このようなハードウェアが利用できない場合、VDAはソフトウェアビデオコーデックを使用したCPUベースのエンコーディングにフォールバックします。詳しくは、「グラフィックポリシー設定」を参照してください。

GPU アクセラレーションが機能していることを確認するには、グラフィックステータスインジケーターを使用できます。



DirectX、Direct3D、および WPF レンダリング

DirectX、Direct3D、および WPF レンダリングは、ディスプレイドライバーインターフェイス（DDI）バージョン 9ex、10、または 11 をサポートする GPU を搭載したサーバーでのみ利用できます。

- Windows Server 2016以降では、RDセッションホストサーバー上のRemote Desktop Services（RDS）セッションは、Microsoft基本表示ドライバーをデフォルトのアダプターとして使用します。Windows Server 2016以降のRDSセッションでGPUを使用するには、グループポリシーの**ローカルコンピューターポリシー** \> **コンピューターの構成** \> **管理用テンプレート** \> **Windowsコンポーネント** \> **Remote Desktop Services** \> **リモートデスクトップセッションホスト** \> **リモートセッション環境**で、**すべてのRemote Desktop Servicesセッションにハードウェアの既定のグラフィックアダプターを使用する**設定を有効にします。
- WPFアプリケーションがサーバーのGPUを使用してレンダリングできるようにするには、WindowsマルチセッションOSセッションを実行しているサーバーのレジストリに設定を作成します。レジストリ設定の詳細については、レジストリで管理される機能のリストにある「Windows Presentation Foundation (WPF) レンダリング」を参照してください。

CUDAまたはOpenCLアプリケーションのGPUアクセラレーション

ユーザーセッションで実行されているCUDAおよびOpenCLアプリケーションのGPUアクセラレーションは、デフォルトで無効になっています。

CUDA アクセラレーション機能を使用するには、レジストリ設定を有効にします。詳細については、レジストリで管理される機能のリストにある「CUDA または OpenCL アプリケーションの GPU アクセラレーション」を参照してください。

WindowsシングルセッションOS向けGPUアクセラレーション

HDX 3D Proを使用すると、グラフィックを多用するアプリケーションを、ホストされたデスクトップまたはシングルセッションOSマシン上のアプリケーションの一部として配信できます。HDX 3D Proは、物理ホストコンピューター（デスクトップ、ブレード、ラックワークステーションを含む）と、XenServer®、vSphere、Nutanix、Hyper-V（パススルーのみ）ハイパーバイザーが提供するGPUパススルーおよびGPU仮想化テクノロジーをサポートしています。

HDX™ 3D Proは以下の機能を提供します。

- WANおよびワイヤレスパフォーマンスを最適化するための、適応型H.264ベースまたはH.265ベースのディープ圧縮。HDX 3D Proは、エンコードのデフォルト圧縮技術としてCPUベースのフルスクリーンH.264圧縮を使用します。H.264によるハードウェアエンコードは、NVENCをサポートするNVIDIA、Intel、およびAMDカードで使用されます。H.265によるハードウェアエンコードは、NVENCをサポートするNVIDIAカードで使用されます。
- 特殊なユースケース向けのロスレス圧縮オプション。HDX 3D Proは、医療画像処理など、ピクセルパーフェクトなグラフィックが必要なアプリケーションをサポートするために、CPUベースのロスレスコーデックも提供します。真のロスレス圧縮は、より多くのネットワークリソースと処理リソースを消費するため、特殊なユースケースでのみ推奨されます。

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

- マルチモニターおよび高解像度モニターのサポート。シングルセッションOSマシンでは、最大8台の4Kモニターがサポートされます。ユーザーはモニターを任意の構成で配置でき、異なる解像度と向きのモニターを混在させることができます。モニターの数は、ホストコンピューターのGPU、ユーザーデバイス、および利用可能な帯域幅の機能によって制限されます。HDX 3D Proはすべてのモニター解像度をサポートしており、ホストコンピューターのGPUの機能によってのみ制限されます。
- 動的解像度。仮想デスクトップまたはアプリケーションウィンドウを任意の解像度にリサイズできます。**注：** 解像度を変更する唯一のサポートされている方法は、VDAセッションウィンドウのサイズを変更することです。VDAセッション内から（**コントロールパネル > デザイン**と

パーソナライズ > ディスプレイ > 画面の解像度を使用して）解像度を変更することはサポートされていません。

- NVIDIA vGPUアーキテクチャのサポート。HDX 3D ProはNVIDIA vGPUカードをサポートしています。詳細については、GPUパススルーとGPU共有に関するNVIDIA vGPUを参照してください。NVIDIA vGPUを使用すると、複数のVMが、非仮想化オペレーティングシステムに展開されているものと同じNVIDIAグラフィックドライバーを使用して、単一の物理GPUに同時に直接アクセスできます。
- Virtual Direct Graphics Acceleration (vDGA) を使用したVMware vSphereおよびVMware ESXのサポート - HDX 3D ProをvDGAと組み合わせて、RDSおよびVDIワークロードの両方で使用できます。
- VMware vSphere/ESX のサポート。
- Windows Server 2016のDiscrete Device Assignmentを使用したMicrosoft HyperVのサポート。
- Intel Xeon Processor E3ファミリーおよびIntel Data Center GPU Flexシリーズによるデータセンターグラフィックスのサポート。詳細については、`<https://www.intel.com/content/www/us/en/products/details/discrete-gpus/data-center-gpu/flex-series.html>`を参照してください。
- AMD GPUのサポート。

> 注:
>
> AMD MxGPU (GPU仮想化) のサポートは、VMware vSphere vGPUでのみ機能します。Citrix HypervisorおよびHyper-Vは、GPUパススルーでサポートされています。詳細については、`<https://www.amd.com/en/graphics/workstation-virtual-graphics>`を参照してください。

- NVIDIA GPU、AMD GPU、Intel GPU向けの高性能ビデオエンコーダーへのアクセス。ポリシー設定（デフォルトで有効）がこの機能を制御します。この機能により、H.264、H.265、またはAV1エンコーディング（利用可能な場合）にハードウェアエンコーディングを使用できます。そのようなハードウェアが利用できない場合、VDAはソフトウェアビデオコーデックを使用したCPUベースのエンコーディングにフォールバックします。詳細については、「グラフィックポリシー設定」を参照してください。

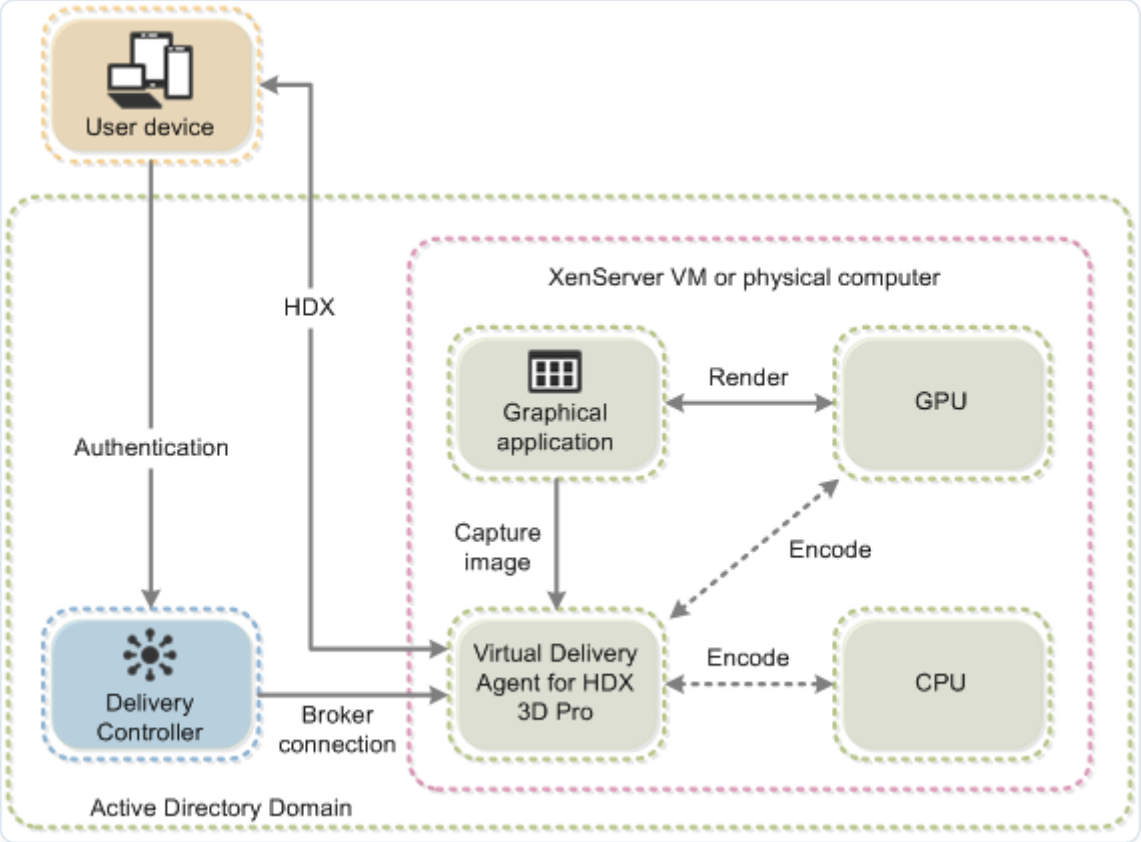
次の図に示すように：

- ユーザーがCitrix Workspace™アプリにログインし、仮想アプリケーションまたはデスクトップにアクセスすると、Controllerがユーザーを認証します。その後、ControllerはHDX 3D Pro用

のVDAに接続し、グラフィカルアプリケーションをホストするコンピューターへの接続を仲介します。

HDX 3D Pro用VDAは、ホスト上の適切なハードウェアを使用して、デスクトップ全体またはグラフィックアプリケーションのみのビューを圧縮します。

- デスクトップまたはアプリケーションのビューと、それらに対するユーザーの操作は、ホストコンピューターとユーザーデバイス間で送信されます。この送信は、Citrix WorkspaceアプリとHDX 3D Pro用VDA間の直接HDX接続を介して行われます。



HDX 3D Proのユーザーエクスペリエンスを最適化する

複数のユーザーが限られた帯域幅の接続を共有している場合（たとえば、支店など）、各ユーザーが利用できる帯域幅を制限するために、**セッション全体の帯域幅制限**ポリシー設定を使用することをお勧めします。この設定を使用すると、ユーザーがログオンおよびログオフする際に、利用可能な帯域幅が大きく変動しないようにすることができます。HDX 3D Proは利用可能なすべての帯域幅を使用するように自動的に調整するため、ユーザーセッション中に利用可能な帯域幅が大きく変動すると、パフォーマンスに悪影響を及ぼす可能性があります。

たとえば、20人のユーザーが60 Mbpsの接続を共有している場合、各ユーザーが利用できる帯域幅は、同時ユーザー数に応じて3 Mbpsから60 Mbpsの間で変動する可能性があります。このシナ

リオでユーザーエクスペリエンスを最適化するには、ピーク時のユーザーあたりの必要な帯域幅を決定し、常にこの量にユーザーを制限します。

3Dマウスのユーザーの場合、汎用USBリダイレクト仮想チャネルの優先度を0に上げることをお勧めします。仮想チャネルの優先度を変更する方法については、Knowledge Centerの記事「CTX128190」を参照してください。

ロスレス圧縮

ロスレス圧縮を使用する場合：

- ロスレスインジケーター（通知領域アイコン）は、表示されている画面がロッシーフレームかロスレスフレームかをユーザーに通知します。このアイコンは、**視覚品質**ポリシー設定で**ロスレスにビルド**が指定されている場合に役立ちます。送信されるフレームがロスレスの場合、ロスレスインジケーターは緑色に変わります。
- ロスレススイッチを使用すると、ユーザーはセッション中にいつでも**Always Lossless**モードに変更できます。セッション中にいつでもロスレスを選択または選択解除するには、アイコンを右クリックして**Switch to pixel perfect**をクリックするか、ショートカット**ALT+SHIFT+1**を使用します。
- ロスレス圧縮の場合: HDX 3D Proは、ポリシーで選択されたコーデックに関係なく、ロスレスコーデックを圧縮に使用します。
- 非可逆圧縮の場合: HDX 3D Proは、デフォルトまたはポリシーで選択された元のコーデックを使用します。
- ロスレススイッチの設定は、以降のセッションでは保持されません。すべての接続でロスレスコーデックを使用するには、**Visual quality**ポリシー設定で**Always lossless**を選択します。

ロスレスホットキー

デフォルトのショートカット**ALT+SHIFT+1**を使用して、セッション内でいつでもホットキーで**ロスレス**を選択または解除できます。

Windowsレジストリで、デフォルトのショートカット**ALT+SHIFT+1**を上書きできます。 新しいレジストリ設定を構成するには、以下のレジストリ値を設定します。

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\Graphics`
- **名前**: `HKLM_HotKey`
- **種類**: `String`

ショートカットの組み合わせを構成する形式は`C=0|1, A=0|1, S=0|1, W=0|1, K=val`です。キーはスペースなしでコンマ「,」で区切る必要があります。キーの順序は関係ありません。

A、C、S、W、Kはキーであり、C=Control、A=ALT、S=SHIFT、W=Win、K=有効なキー（Kに許可される値は0～9、a～z、および任意の仮想キーコード）です。

例:

- **F10**の場合、K=0x79を設定します。
- **Ctrl + F10**の場合、C=1、K=0x79を設定します。
- 「**Alt + A**」の場合、A=1,K=a または A=1,K=A または K=A,A=1 を設定します
- 「**Ctrl + Alt + 5**」の場合、C=1, A=1,K=5 または A=1,K=5,C=1 を設定します
- 「**Ctrl + Shift + F5**」の場合、A=1,S=1,K=0x74 を設定します

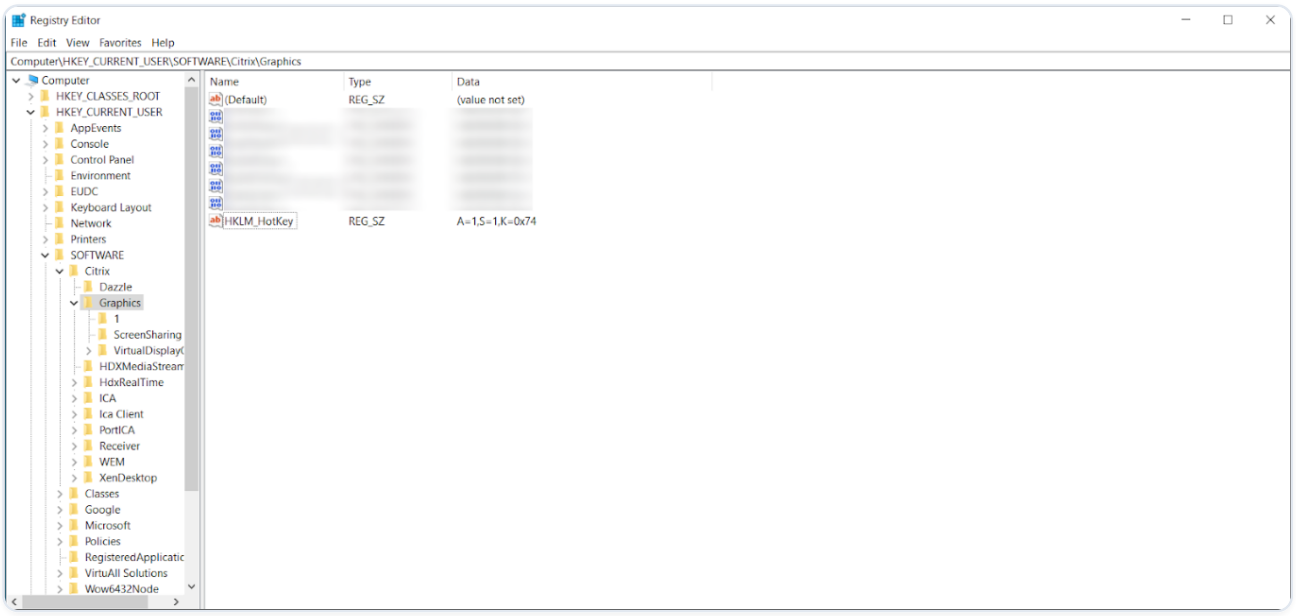
次の表は、仮想キーコードの例を示しています。

キー	値
F1	0x70
F2	0x71
F3	0x72
F4	0x73
F5	0x74
F6	0x75
F7	0x76
F8	0x77
F9	0x78
F10	0x79
F11	0x7A
F12	0x7B
PAGE UP キー	0x21
PAGE DOWN キー	0x22

キー	値
END キー	0x23
HOME キー	0x24
左矢印キー	0x25
上矢印キー	0x26
右矢印キー	0x27
下矢印キー	0x28

ショートカットの組み合わせの間にスペースがないことを確認してください。例:

正しい: C=1,K=0x74 誤り: C=1, K=0x74



注意:

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

シンワイヤー

はじめに

Thinwireは、Citrix HDXテクノロジーの一部であり、Citrix Virtual Apps and Desktopsで使用されるCitrixのデフォルトのディスプレイリモートテクノロジーです。

ディスプレイリモートテクノロジーにより、あるマシンで生成されたグラフィックを、通常はネットワーク経由で別のマシンに送信して表示できます。

成功したディスプレイリモートソリューションは、ローカルPCと同様の高度にインタラクティブなユーザーエクスペリエンスを提供します。Thinwireは、複雑で効率的なさまざまな画像分析および圧縮技術を使用することで、このエクスペリエンスを実現します。Thinwireは、サーバーのスケーラビリティを最大化し、他のディスプレイリモートテクノロジーよりも少ない帯域幅を消費します。

このバランスにより、Thinwire はほとんどの一般的なビジネスユースケースに対応し、Citrix Virtual Apps and Desktops のデフォルトのディスプレイリモートテクノロジーとして使用されています。

HDX™ 3D プロ

デフォルト構成では、Thinwireは3Dまたは高度にインタラクティブなグラフィックを配信し、グラフィック処理ユニット（GPU）が存在する場合はそれを使用できます。ただし、GPUが存在するシナリオでは、**Optimize for 3D graphics workload**または**Visual quality > Build to lossless**ポリシーを使用してHDX 3D Proモードを有効にすることをお勧めします。これらのポリシーは、GPUが存在する場合に、ビデオコーデック（H.264、H.265、またはAV1）を使用して画面全体をハードウェアアクセラレーションでエンコードするようにThinwireを構成します。これにより、3Dプロフェッショナルグラフィックのよりスムーズなエクスペリエンスが提供されます。詳細については、H.264 Build to lossless、HDX 3D Pro、およびGPU acceleration for Windows Single-session OSを参照してください。

要件

Thinwireは、Windows Server 2022、Windows Server 2019、Windows 10、およびWindows 7などの最新のオペレーティングシステム向けに最適化されています。Windows Server 2008 R2では、レガシーグラフィックモードが推奨されます。これらのユースケースに対するCitrix推奨のポリシー設定の組み合わせを提供するには、組み込みのCitrixポリシーテンプレート、High Server Scalability-Legacy OS、およびOptimized for WAN-Legacy OSを使用してください。

- Thinwireの動作を制御するポリシー設定である**Use video codec for compression**は、Citrix Virtual Apps and Desktops 7 1808以降およびXenApp and XenDesktop 7.6 FP3以降のVDAバージョンで利用できます。**Use video codec when preferred**オプションは、Citrix Virtual Apps and Desktops 7 1808以降およびXenApp and XenDesktop 7.9以降のVDAバージョンでのデフォルト設定です。
- All Citrix Workspace™ apps support Thinwire. Some Citrix Workspace apps might support features of Thinwire that others do not, for example, 8-bit or 16-bit graphics for reduced bandwidth usage. Support for such features is automatically negotiated by the Citrix Workspace app.
- Thinwire uses more server resources (CPU, memory) in multi-monitor and high-resolution scenarios. It is possible to tune the amount of resources Thinwire uses, however, bandwidth usage might increase as a result.
- 低帯域幅または高遅延のシナリオでは、インタラクティブ性を向上させるために8ビットまたは16ビットグラフィックを有効にすることを検討してください。特に8ビットの色深度では、視覚品質が影響を受ける可能性があります。

エンコード方法

Thinwireは、ポリシーとクライアントの機能に応じて、2つの異なるエンコードモードで動作できます。

- Adaptive JPEGを使用したThinwire **圧縮にビデオコーデックを使用する**ポリシー設定: **ビデオコーデックを使用しない**
- Selective H.264、H.265、またはAV1を使用したThinwire **圧縮にビデオコーデックを使用する**ポリシー設定: **優先される場合はビデオコーデックを使用する** または **アクティブに変化する領域の場合**
- フルスクリーンH.264、H.265、またはAV1を使用したThinwire **圧縮にビデオコーデックを使用する**ポリシー設定: **画面全体の場合**

H.265

High Efficiency Video Coding (HEVC)、別名H.265は、H.264の後継です。 H.265ビデオコーデックによるハードウェアエンコードは、以下のGPUでサポートされています。

- NVIDIA MaxwellベースのGPU以降
- Intel第6世代GPU以降
- AMD RavenベースのGPU以降

AV1

CitrixはAV1ビデオコーデックのサポートを追加しました。AV1の利点は、H.264およびH.265と比較して、優れた画像圧縮、より良い画質、および低い帯域幅使用量を持つことです。

AV1の以下の要件を満たす必要があります。

- NVIDIA GPUの場合はVDA 2305以降、または
- Intel GPUの場合はVDA 2308以降

以下のGPUがエンコードに対応しています。

- NVIDIA Ada LovelaceベースのGPU
- Intel ARCまたはIntel Data Center GPU Flexシリーズ GPU

NVIDIAのAda Lovelace GPUの詳細については、ADAアーキテクチャを参照してください。

IntelのARCワークステーションおよびデータセンターFlexシリーズGPUの詳細については、Flex seriesおよびOverviewを参照してください。

自動ビデオコーデック選択

圧縮ポリシーの**ビデオコーデックを使用**が有効になっている場合、またはVDAで3Dグラフィックワークロードの最適化が有効になっている場合に、最適なビデオコーデックを自動的に検出できます。Citrix Workspaceアプリfor Windowsのインストール中に、エンドポイントのデコード機能が評価されます。この情報に基づいて、Citrix Workspaceアプリfor Windowsは、接続時にVDAと使用する最適なコーデックをネゴシエートします。ビデオコーデックが評価される順序は次のとおりです。

- AV1
- H.265
- H.264

自動選択は、これらのコーデックの4:2:0バリアントにのみ適用されます。**視覚品質**設定が「Build-to-Lossless」または「Always Lossless」に設定されており、視覚的にロスレスを許可が「有効」に設定されている場合、ビデオコーデックの自動選択は無効になります。

リソースに接続する際、Citrix Workspaceアプリはエンドポイントの H.265およびAV1のデコード機能をテストし、その機能をレジストリに保存します。その後、Citrix Workspaceアプリは使用する最適なビデオコーデックを自動的に選択し、VDAとネゴシエートします。VDAとクライアントの両方がH.265とAV1を使用できる場合、AV1がビデオコーデックとして選択されます。VDAまた

はクライアントのいずれかでAV1が利用できない場合、H.265がネゴシエートされます。H.265もどちらかで利用できない場合、セッションはH.264をビデオコーデックとして使用します。

> **注:**
>
> この機能はデフォルトで有効になっています。この動作は、新しいクライアント側レジストリ設定`DisableDecoderCaps`を設定することで変更できます。
>
> ビデオコーデックの自動選択を無効にするには、「DisableDecoderCaps」を次のように設定します。`HKLM\Software\WOW6432Node\Policies\Citrix\ICA Client\Graphics Engine DWORD DisableDecoderCaps = 1`または`HKCU\Software\Policies\Citrix\ICA Client\Graphics Engine DWORD DisableDecoderCaps = 1`に設定します。

これらの値のいずれかが1に設定されている場合、ビデオコーデックの自動選択は使用されません。 グラフィックステータスインジケーターとHDXモニターでビデオコーデックを監視できます。

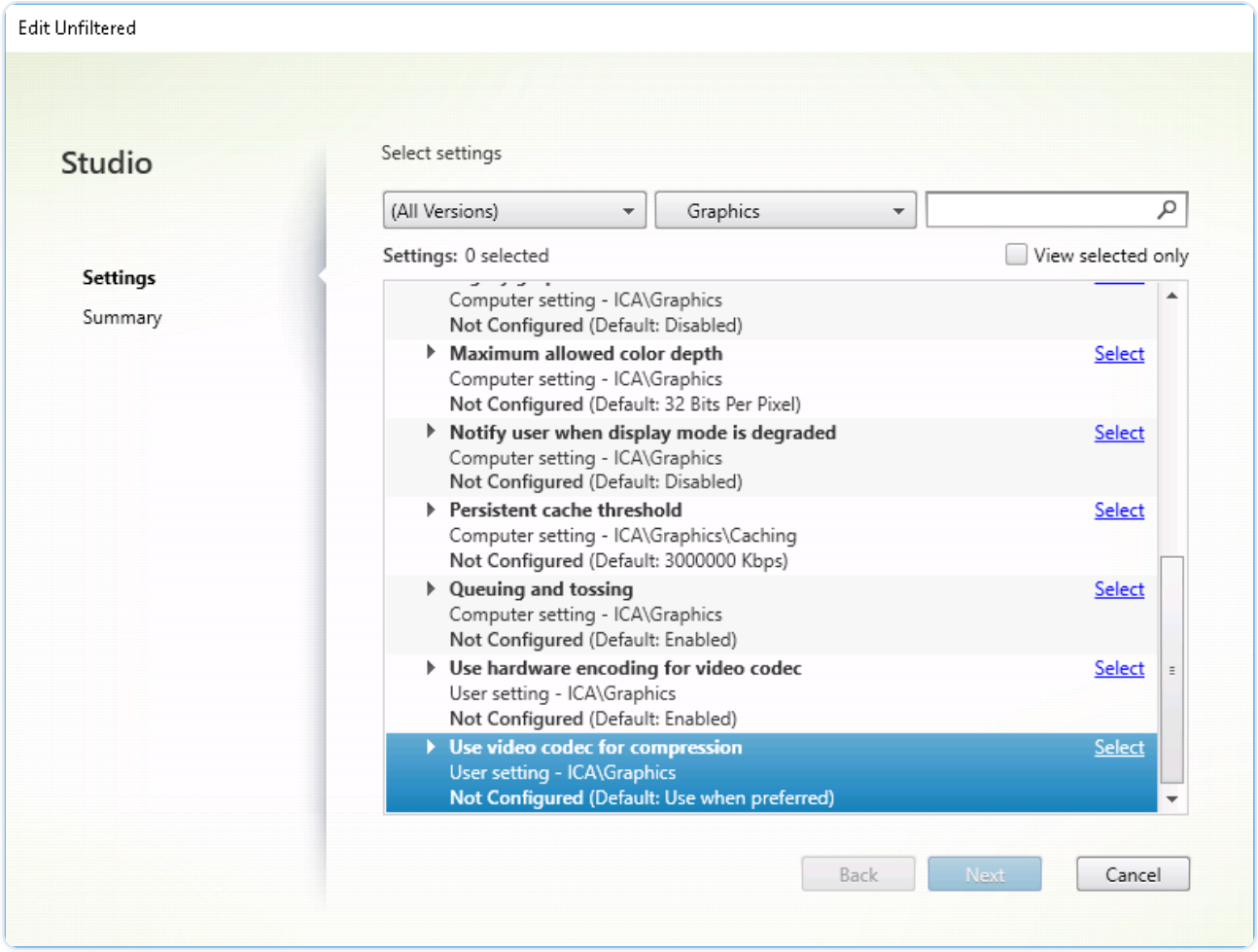
構成

Thinwire は、デフォルトのディスプレイリモートテクノロジーです。

次のグラフィックポリシー設定は、デフォルトを設定し、さまざまなユースケースの代替手段を提供します。

- 圧縮にビデオコーデックを使用
  - **優先する場合にビデオコーデックを使用**。これがデフォルト設定です。追加の構成は不要です。この設定をデフォルトのままにすることで、すべてのCitrix接続でThinwireが選択され、一般的なデスクトップワークロードのスケーラビリティ、帯域幅、および優れた画質のために最適化されます。これは、**アクティブに変更される領域の場合**と機能的に同等です。
- このポリシー設定の他のオプションは、さまざまなユースケースで他のテクノロジーとともにThinwireを引き続き使用します。例：
  - **アクティブに変更される領域の場合**。Thinwire のアダプティブディスプレイテクノロジーは、動く画像（ビデオ、モーション中の3D）を識別し、画像が動いている画面の一部でのみ H.264、H.265、または AV1 を使用します。

- **画面全体の場合**。3Dグラフィックを多用するケースで、ユーザーエクスペリエンスと帯域幅の向上を最適化するために、H.264、H.265、またはAV1によるフルスクリーンでThinwireを提供します。H.264 4:2:0 の場合（**視覚的にロスレス**ポリシーが無効になっている場合）、最終画像はピクセルパーフェクト（ロスレス）ではなく、特定のシナリオには適さない可能性があります。そのような場合は、代わりにH.264 Build to lossless または H.265 Build to lossless の使用を検討してください。



次の視覚表示ポリシー設定を含む、さまざまな他のポリシー設定を使用して、ディスプレイリモートテクノロジーのパフォーマンスを微調整できます。Thinwire はこれらすべてをサポートしています。

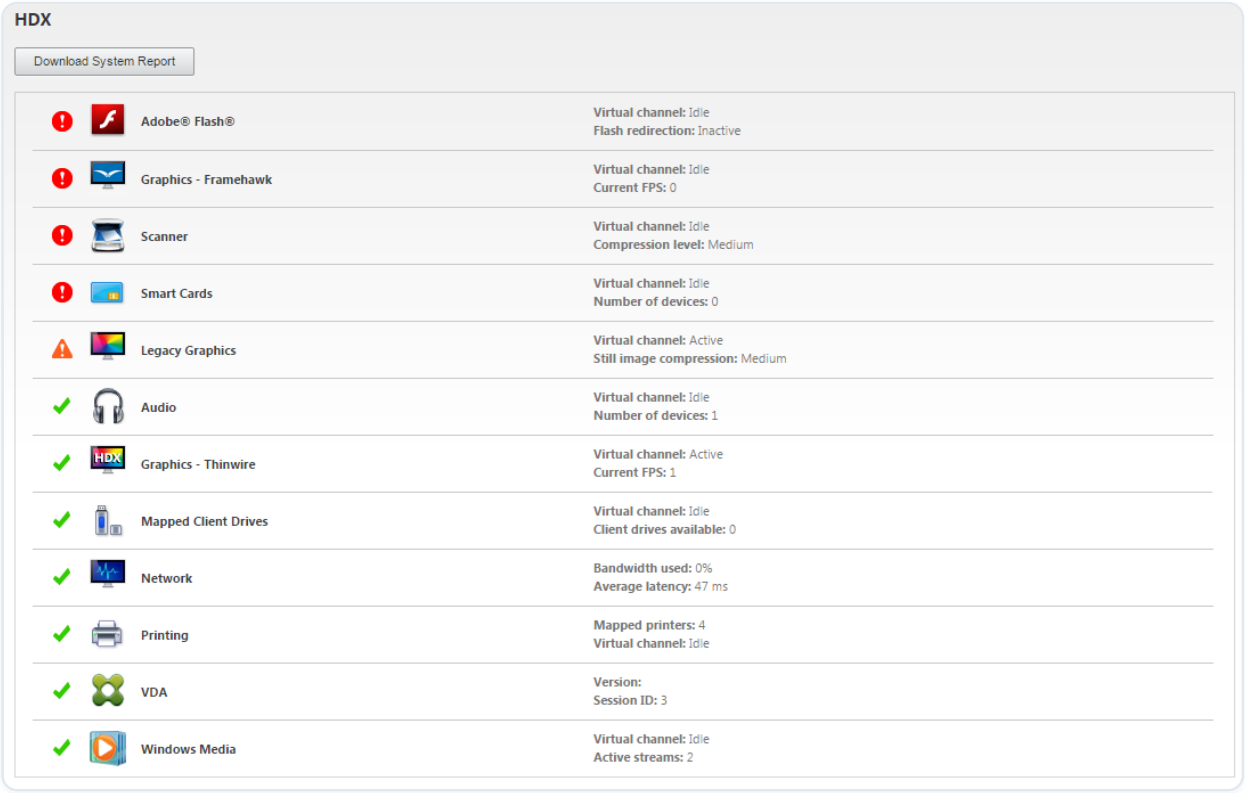
- シンプルグラフィックの優先色深度
- ターゲットフレームレート
- 視覚的品質

さまざまなビジネスユースケースにCitrixが推奨するポリシー設定の組み合わせを取得するには、組み込みのCitrixポリシーテンプレートを使用します。**高サーバー拡張性**および**超高精細ユーザーエクスペリエンス**テンプレートは、組織の優先順位とユーザーの期待に最適なポリシー設定の組み合わせでThinwireを使用します。

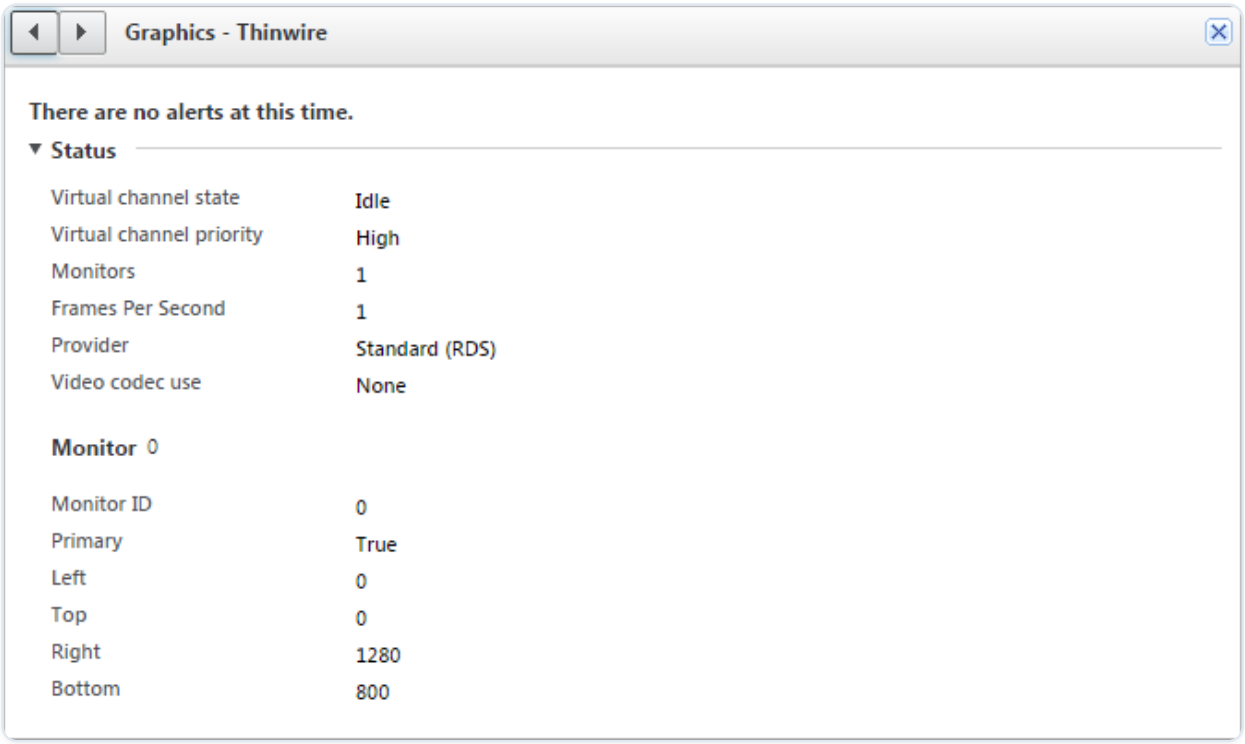
Thinwire の監視

Citrix DirectorからThinwireの使用状況とパフォーマンスを監視できます。HDX仮想チャネルの詳細ビューには、任意のセッションでThinwireのトラブルシューティングと監視を行うための役立つ情報が含まれています。Thinwire関連のメトリックを表示するには：

1. Directorで、ユーザー、マシン、またはエンドポイントを検索し、アクティブなセッションを開いて**詳細**をクリックします。または、**フィルター** > **セッション** > **すべてのセッション**を選択し、アクティブなセッションを開いて**詳細**をクリックすることもできます。
2. **HDX**パネルまでスクロールダウンします。



3. **グラフィック - Thinwire**を選択します。



ロスレス圧縮コーデック（MDRLE）

一般的なデスクトップセッションでは、ほとんどの画像は単純なグラフィックまたはテキスト領域です。Thinwireはこれらの領域を特定し、2DRLEコーデックを使用してロスレスエンコードのためにこれらの領域を選択します。Citrix Workspaceアプリクライアント側では、これらの要素はCitrix Workspaceアプリ側の2DRLEデコーダーを使用してセッション表示のためにデコードされます。

XenApp and XenDesktop 7.17では、2DRLEコーデックよりも一般的なデスクトップセッションで消費帯域幅が少ない、より高い圧縮率のMDRLEコーデックを追加しました。この新しいコーデックは、サーバーのスケーラビリティに影響を与えません。

通常、帯域幅が低いほど、セッションの対話性が向上し（特に共有リンクや制約のあるリンクの場合）、コストが削減されます。

MDRLEコーデックの構成は不要です。Citrix WorkspaceアプリがMDRLEデコードをサポートしている場合、VDAはVDA MDRLEエンコードとCitrix WorkspaceアプリMDRLEデコードを使用します。Citrix WorkspaceアプリがMDRLEデコードをサポートしていない場合、VDAは自動的に2DRLEエンコードにフォールバックします。

MDRLEの要件：

- Citrix Virtual Apps and Desktopsの最小バージョン7 1808 VDA
- XenAppおよびXenDesktopの最小バージョン7.17 VDA

- Windows向けCitrix Workspaceアプリの最小バージョン1808
- Citrix Receiver for Windows 最小バージョン 4.11

プログレッシブモード

Citrix Virtual Apps and Desktops 1808では、プログレッシブモードが導入され、デフォルトで有効になりました。ネットワーク条件が制限されている場合（デフォルト：帯域幅 < 2 Mbps、または遅延 > 200 ms）、Thinwireは、画面アクティビティ中のインタラクティブ性を向上させるために、テキストと静止画像の圧縮を強化しました。画面アクティビティが停止すると、高度に圧縮されたテキストと画像は、ランダムなブロック形式で段階的にシャープ化されます。このように圧縮とシャープ化を行うことで、全体的なインタラクティブ性は向上しますが、キャッシュ効率が低下し、帯域幅の使用量が増加します。

Citrix Virtual Apps and Desktops 1906以降、プログレッシブモードはデフォルトで無効になっています。現在、当社は異なるアプローチを採用しています。静止画の品質は、ネットワーク条件に基づいており、各**視覚品質**設定の事前定義された最小値と最大値の間で変動します。明示的なシャープ化ステップがないため、Thinwireは画像配信を最適化し、キャッシュ効率を維持しながら、プログレッシブモードのほぼすべての利点を提供します。

プログレッシブモードの動作の変更

レジストリキーを使用して、プログレッシブモードの状態を変更できます。詳細については、レジストリで管理される機能のリストにあるプログレッシブモードを参照してください。

ロスレスビルド

ロスレスビルドは、対話性と最終的な画質のためにグラフィック配信を最適化する特別なThinwire構成です。この設定は、**視覚品質**ポリシーを**ロスレスビルド**に設定することで有効にできます。

ビルドトゥロスレスは、画面アクティビティ中にH.264、H.265、またはAV1を使用して画面を圧縮し、アクティビティが停止するとピクセルパーフェクト（ロスレス）にシャープ化します。損失のある画質は、利用可能なリソースに適応し、可能な限り最高のフレームレートを維持します。シャープ化のステップは段階的に実行されます。たとえば、モデルを選択して回転させる場合などです。

ビルドトゥロスレスは、ハードウェアアクセラレーションを含む、画面全体にビデオコーデックを使用するすべての利点を提供しますが、最終的に保証されたロスレス画面という追加の利点があります。これは、最終的なピクセルパーフェクトな画像を必要とする3Dタイプのワークロードにとって重要です。たとえば、医療画像を操作する場合などです。また、H.264 **ビルドトゥロスレス**は、フルスクリーンH.264 4:4:4よりも少ないリソースを使用します。その結果、**ビルドトゥロ**

スレスを使用すると、通常、視覚的にロスレスなH.264 4:4:4よりも高いフレームレートが得られます。

> **注:**
>
> ビルドトゥロスレスを使用している場合でも、ビデオコーデックの使用を無効にできます。**ビデオコーデックの使用**ポリシーを`Do not use video codec`に設定するだけです。これにより、動画は代わりにアダプティブJPEGでエンコードされます。

視覚的にロスレスなエンコード

視覚的にロスレスなエンコードは、ビデオコーデック圧縮にクロマサブサンプリングされたYUV 4:2:0カラースペースではなく、YUV 4:4:4カラースペースを使用します。これにより、カラースペース変換中に色情報が失われることがなく、デコード後には元のRGB画像と視覚的に区別できないようになります。

次の例を考えてみましょう。画面全体を圧縮するためにビデオコーデックを使用する場合、4:2:0の色圧縮は、テキストのような高コントラストの詳細を劣化させ、ぼやけて読みにくくする可能性があります。対照的に、4:4:4はほぼすべての色情報を保持し、視覚的に認識できる劣化を示しません。



ピクセルパーフェクトな品質や正確な色表示を必要とするワークロードは、視覚的にロスレスなエンコードの恩恵を受けることができます。

視覚的にロスレスなエンコードは、H.264とH.265の両方で利用できます。H.264 4:4:4エンコードは純粋なソフトウェアベースのソリューションであるため、VDAとクライアントの両方でCPU使用率に大きな影響を与える可能性があります。これにより、フレームレートにも影響が出る場合があります。

H.265 4:4:4のサポートは、Citrix Workspaceアプリ2305のリリースで追加され、ThinwireがH.265 4:4:4エンコードのためにVDAとクライアントの両方でGPUを使用できるようになり、パフォーマンスが大幅に向上しました。

視覚的にロスレスな4:4:4エンコードを許可するには、2つのポリシーを有効にする必要があります。

- **視覚品質**: `Build to Lossless`または`Always Lossless`に設定
- **視覚的にロスレスを許可**: `Enabled`に設定

> **注:**
>
> **視覚的にロスレスを許可**が有効になっていない場合、Thinwireエンコーダーは`Build to lossless`または`Always Lossless`のいずれかに切り替わります。

> H.265 4:4:4の視覚的にロスレスには、追加の要件があります。

- NVIDIA GPUにはVDAバージョン2209以降が必要です。
- Intel GPUにはVDAバージョン2308以降が必要です。

H.265 4:4:4でサポートされているGPUは次のとおりです。

- NVIDIA Pascal世代以降のGPU
- Intel 第10世代以降のGPU

クライアントには、Citrix Workspace app for Windows バージョン 2305 が必要です（バージョン 2309.1 を推奨）。

H.265 4:4:4 のハードウェアデコードは、以下のクライアントデバイスの GPU で可能です。

- NVIDIA Turing世代以降のGPU
- Intel第10世代以降のGPU

テキストベースのセッションウォーターマーク

テキストベースのセッションウォーターマークは、データ盗難を抑止し、追跡できるようにするのに役立ちます。この追跡可能な情報は、写真やスクリーンキャプチャを使用してデータを盗む者への抑止力として、セッションデスクトップに表示されます。元のドキュメントの内容を変更することなく、セッション画面全体に表示されるテキストのレイヤーであるウォーターマークを指定できます。テキストベースのセッションウォーターマークにはVDAサポートが必要です。

> **重要:**

> テキストベースのセッションウォーターマークはセキュリティ機能ではありません。このソリューションはデータ盗難を完全に防ぐものではありませんが、ある程度の抑止力と追跡可能性を提供します。この機能を使用しても完全な情報追跡可能性を保証するものではありませんが、必要に応じて他のセキュリティソリューションと組み合わせて使用することをお勧めします。

> セッションウォーターマークはテキストであり、ユーザーに配信されるセッションに適用されます。セッションウォーターマークには、データ盗難を追跡するための情報が含まれています。最も重要なデータは、スクリーンイメージが取得された現在のセッションのログオンユーザーのIDです。データ漏洩をより効果的に追跡するには、サーバーまたはクライアントのインターネットプロトコルアドレスや接続時間などの他の情報を含めます。

ユーザーエクスペリエンスを調整するには、セッションウォーターマークポリシー設定 を使用して、画面上の配置とウォーターマークの外観を構成します。

要件:

仮想配信エージェント:

マルチセッションOS 7.17 シングルセッションOS 7.17

制限事項:

- ローカルアプリアクセス、Windowsメディアリダイレクト、MediaStream、ブラウザコンテンツリダイレクト、HTML5ビデオリダイレクトが使用されているセッションでは、セッションウォーターマークはサポートされていません。セッションウォーターマークを使用するには、これらの機能が無効になっていることを確認してください。
- セッションが全画面ハードウェアアクセラレーションモード（全画面H.264またはH.265エンコーディング）で実行されている場合、セッションウォーターマークはサポートされず、表示されません。
- これらのHDX™ポリシーを設定すると、ウォーターマーク設定は有効にならず、セッション表示にウォーターマークは表示されません。

ビデオコーデックにハードウェアエンコーディングを使用 を **有効** **圧縮にビデオコーデックを使用** を **画面全体**

- これらのHDXポリシーを設定すると、動作は未定義となり、ウォーターマークが表示されない場合があります。

ビデオコーデックにハードウェアエンコーディングを使用 を **有効** **圧縮にビデオコーデックを使用** を **優先する場合にビデオコーデックを使用**

ウォーターマークが表示されるようにするには、**ビデオコーデックにハードウェアエンコードを使用**を**無効**に設定するか、**圧縮にビデオコーデックを使用**を**頻繁に変化する領域の場合**または**ビデオコーデックを使用しない**に設定します。

- セッションウォーターマークは、Thinwireグラフィックモードのみをサポートします。
- セッション録画を使用している場合、録画されたセッションにはウォーターマークは含まれません。
- Windowsリモートアシスタンスを使用している場合、ウォーターマークは表示されません。
- ユーザーが画面をキャプチャするために**Print Screen**キーを押した場合、VDA側でキャプチャされた画面にはウォーターマークは含まれません。キャプチャされた画像がコピーされないように対策を講じることをお勧めします。

画面共有

画面共有を使用すると、ユーザーはCitrix Virtual Desktopセッションを、画面コンテンツ、キーボード、マウスコントロールを含めて他のユーザーと共有できます。

システム要件

- Windows: シングルセッションまたはマルチセッションOS VDA
- Linux: Linuxセッションの共有に関する詳細については、Linux VDAドキュメントを参照してください。
- デスクトップセッションのみ共有できます。
- セッションをホストするVDAと、共有セッションに接続するマシンとの間にネットワーク接続が必要です。ネットワークポート要件は、使用中のICAポート（TCP/UDP 1494または2598）と、画面共有ポリシーの構成（デフォルトではTCP 52525〜52625）に基づいています。

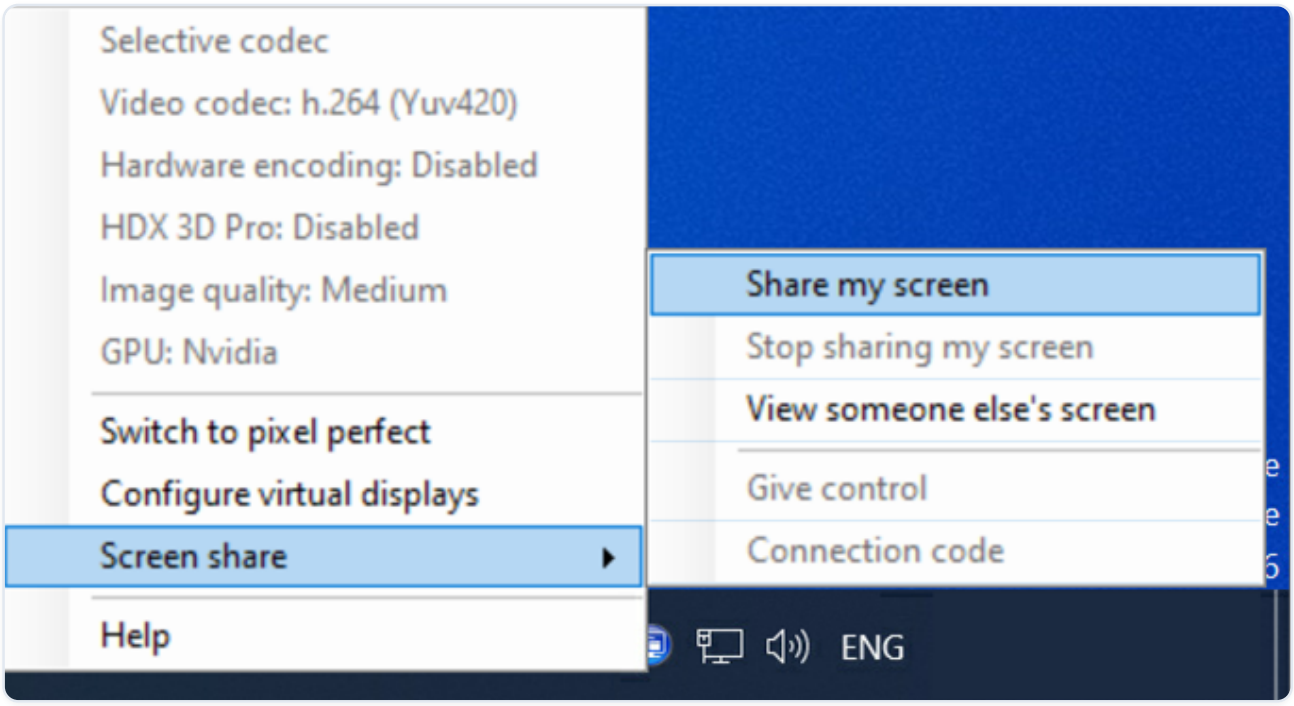
構成

画面共有はCitrixポリシーを使用して有効にする必要があります。画面共有はデフォルトで無効になっています。画面共有ポリシーを構成して、この機能を有効または無効にし、使用可能なネットワークポート範囲を割り当てます。

セッションの共有と接続のコントロールを含むユーザーインターフェイスを表示するには、グラフィックステータスインジケーターポリシーを有効にします。

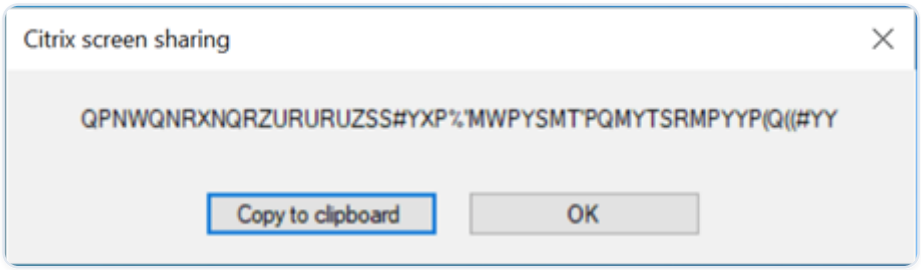
セッションの共有

セッションを共有するには、Windowsの通知領域にあるHDX™グラフィックステータスインジケーターアイコンを探します。それを右クリックしてメニューを表示し、**画面共有 > 自分の画面を共有**を選択します。



クリップボードにコピーをクリックするか、ダイアログボックスに表示されている文字列全体を手動で選択してコピーします。この文字列は、電子メールやIMクライアントなど、選択したアプリケーションに貼り付けて、他のユーザーに配布できます。

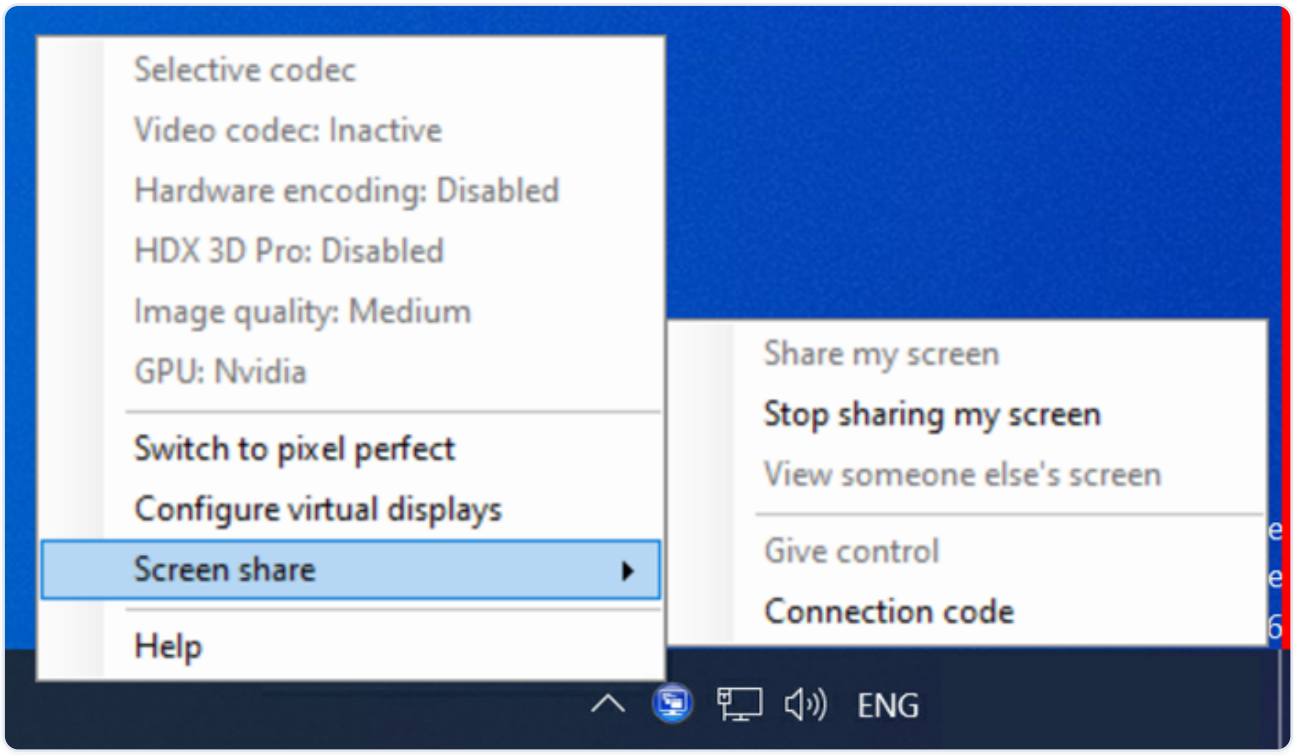
OKまたは**x**をクリックしてダイアログボックスを閉じます。セッションが共有されている間はいつでも、**Screen share > Connection code**メニューオプションから接続コードを取得できます。



セッションが共有され、他のユーザーに表示されていることを示す赤い枠線が画面の周囲に表示されます。

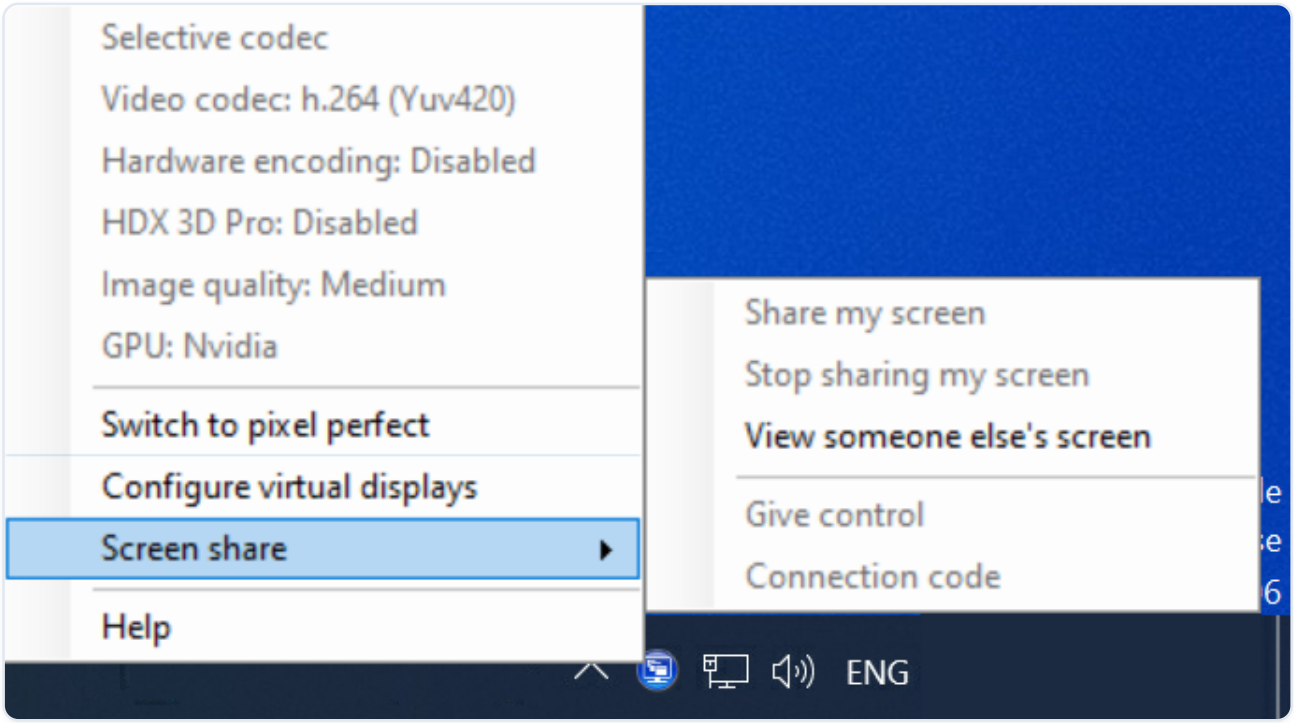
キーボードとマウスのコントロールも、**Screen share > Give control**メニューオプションを使用して他のユーザーと共有できます。

セッションの共有を停止し、すべてのユーザーを切断するには、**画面共有 > 自分の画面の共有を停止** メニューオプションを使用します。

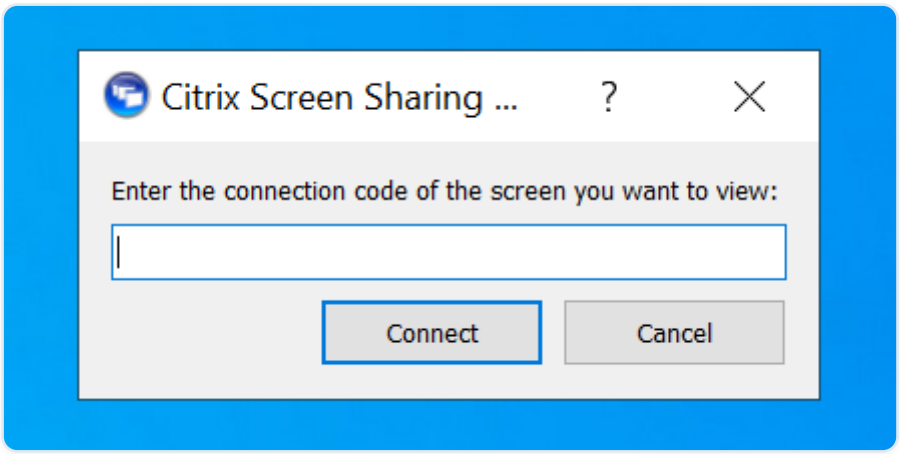


共有セッションへの接続

他のユーザーのセッションに接続するには、Windowsの通知領域にあるHDXグラフィックステータスインジケーターアイコンを探します。それを右クリックしてメニューを表示し、**画面共有 > 他のユーザーの画面を表示** を選択します。

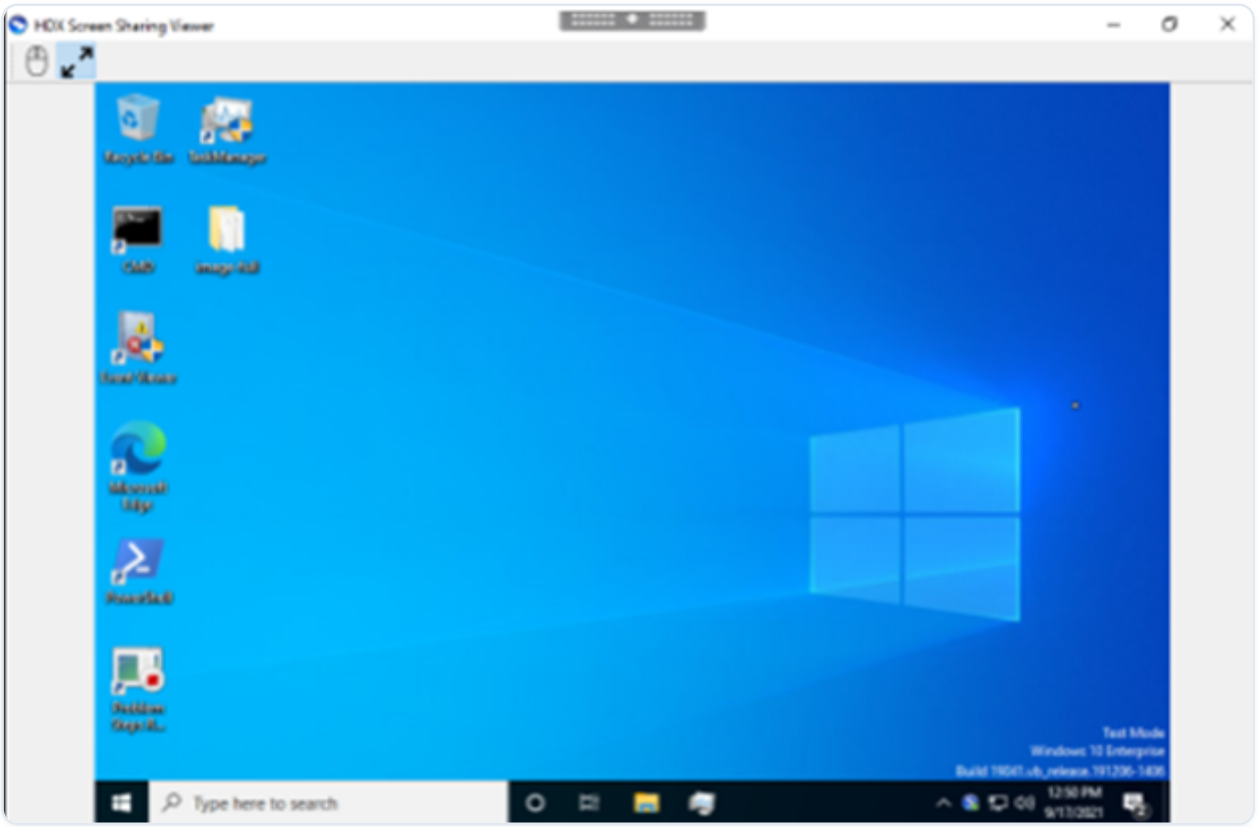


セッションを共有しているユーザーから提供された接続文字列をテキストボックスに入力または貼り付けます。接続を確立するには、**接続**をクリックします。



HDX画面共有ビューア ウィンドウの左上隅にあるマウスアイコンをクリックすると、キーボードとマウスのコントロールを要求できます。

共有セッションからいつでも切断するには、**HDX画面共有ビューア** ウィンドウを閉じます。



その他の考慮事項

- 画面共有ビューアアプリケーションは、VDAに *C:\Program Files\Citrix\HDX\bin\TwPlayer.exe* として含まれており、Virtual Apps Serverを使用して公開アプリケーションとして展開される場合があります。この代替展開モデルにより、仮想デスクトップにアクセスできないユーザーとのコラボレーションが可能になります。

- 共有セッションに接続できるユーザー数は、画面共有ポリシーのネットワークポート範囲を使用して制限できます。ユーザーごとに1つのポートが必要です。デフォルトの範囲では、最大100人のユーザーが許可されます。
- セッションに接続されているすべてのモニターが共有されます。個々のモニターを選択することはできません。
- H.265ビデオコーデックはサポートされていません。

マルチメディア

HDX™テクノロジースタックは、2つの補完的なアプローチを通じてマルチメディアアプリケーションの配信をサポートします。

- サーバー側レンダリングによるマルチメディア配信
- クライアント側レンダリングによるマルチメディアリダイレクト

この戦略により、優れたユーザーエクスペリエンスで幅広いマルチメディア形式を配信できると同時に、サーバーのスケーラビリティを最大化してユーザーあたりのコストを削減できます。

サーバー側でレンダリングされるマルチメディア配信では、オーディオおよびビデオコンテンツはアプリケーションによってCitrix Virtual Apps and Desktopsサーバー上でデコードおよびレンダリングされます。その後、コンテンツは圧縮され、ICAプロトコルを使用してユーザーデバイス上のCitrix Workspaceアプリに配信されます。この方法は、さまざまなアプリケーションおよびメディア形式との互換性を最大限に高めます。ビデオ処理は計算負荷が高いため、サーバー側でレンダリングされるマルチメディア配信は、オンボードのハードウェアアクセラレーションから大きな恩恵を受けます。たとえば、DirectX Video Acceleration (DXVA) のサポートにより、H.264デコードを個別のハードウェアで実行することでCPUの負荷を軽減します。Intel Quick Sync、AMD RapidFire、NVIDIA NVENCテクノロジーは、ハードウェアアクセラレーションによるH.264エンコーディングを提供します。

ほとんどのサーバーはビデオ圧縮のためのハードウェアアクセラレーションを提供しないため、すべてのビデオ処理がサーバーCPUで行われる場合、サーバーのスケーラビリティは悪影響を受けます。多くのマルチメディア形式をローカルレンダリングのためにユーザーデバイスにリダイレクトすることで、高いサーバーのスケーラビリティを維持できます。

- Windows Mediaリダイレクトは、通常Windows Media Playerに関連付けられているさまざまなメディア形式について、サーバーの負荷を軽減します。
- HTML5ビデオは普及しており、Citrix®はこの種のコンテンツ向けにリダイレクトテクノロジーを導入しました。HTML5、HLS、DASH、またはWebRTCを使用するWebサイトには、ブラウザコンテンツリダイレクトをお勧めします。
- 一般的なコンテンツリダイレクトテクノロジーであるホストからクライアントへのリダイレクトとローカルアプリアクセスをマルチメディアコンテンツに適用できます。

これらのテクノロジーをまとめると、リダイレクトを設定しない場合、HDXはサーバー側レンダリングを実行します。 リダイレクトを設定すると、HDXはサーバーフェッチとクライアントレンダリング、またはクライアントフェッチとクライアントレンダリングのいずれかを使用します。これらの方法が失敗した場合、HDXは必要に応じてサーバー側レンダリングにフォールバックし、フォールバック防止ポリシーの対象となります。

シナリオ例

シナリオ例(/en-us/citrix-virtual-apps-desktops/2407/media/multimedia.png)

シナリオ1。（サーバーフェッチとサーバーレンダリング）：

1. サーバーはソースからメディアファイルを取得し、デコードしてから、オーディオデバイスまたはディスプレイデバイスにコンテンツを提示します。
2. サーバーは、表示デバイスまたはオーディオデバイスから、それぞれ提示された画像またはサウンドを抽出します。
3. サーバーは必要に応じてそれを圧縮し、クライアントに送信します。

このアプローチでは、高いCPUコスト、高い帯域幅コスト（抽出された画像/音声が効率的に圧縮されていない場合）、および低いサーバー拡張性が発生します。

Thinwireおよびオーディオ仮想チャネルがこのアプローチを処理します。このアプローチの利点は、クライアントのハードウェアおよびソフトウェア要件を削減できることです。このアプローチを使用すると、デコードはサーバーで行われ、より幅広い種類のデバイスとフォーマットで動作します。

シナリオ2。（サーバーフェッチとクライアントレンダリング）：

このアプローチは、メディアコンテンツがデコードされてオーディオまたはディスプレイデバイスに提示される前に、それを傍受できることに依存します。圧縮されたオーディオ/ビデオコンテンツは、代わりにクライアントに送信され、そこでローカルでデコードおよび提示されます。このアプローチの利点は、それらがクライアントデバイスにオフロードされ、サーバーのCPUサイクルを節約できることです。

しかし、これはクライアントに追加のハードウェアおよびソフトウェア要件ももたらします。クライアントは、受信する可能性のある各フォーマットをデコードできる必要があります。

シナリオ3。（クライアントフェッチとクライアントレンダリング）：

このアプローチは、メディアコンテンツのURLがソースからフェッチされる前に、それを傍受できることに依存します。URLはクライアントに送信され、そこでメディアコンテンツがフェッチ、デコード、およびローカルで提示されます。このアプローチは概念的にシンプルです。その利点は、サーバーのCPUサイクルと帯域幅の両方を節約できることです。なぜなら、サーバーは制御コマンドのみを送信するからです。ただし、メディアコンテンツが常にクライアントからアクセスできるとは限りません。

フレームワークとプラットフォーム：

シングルセッションオペレーティングシステム（Windows、Mac OS X、Linux）は、マルチメディアアプリケーションのより迅速な開発を可能にするマルチメディアフレームワークを提供します。この表は、より一般的なマルチメディアフレームワークの一部を示しています。各フレームワークは、メディア処理をいくつかの段階に分割し、パイプラインベースのアーキテクチャを使用します。

フレームワーク	プラットフォーム
DirectShow	Windows (98以降)
メディアファンデーション	ウィンドウズ (ビスタ 以降)
Gストリーマー	リナックス
QuickTime	Mac OS テン

メディアリダイレクト技術によるダブルホップサポート

オーディオリダイレクト	いいえ
ブラウザコンテンツリダイレクト	いいえ
HDX Webカメラリダイレクト	はい
HTML5ビデオのリダイレクト	はい
Windows Mediaリダイレクト	はい

オーディオ機能

HDXオーディオ機能を最適化するポリシーに、以下のCitrixポリシー設定を構成および追加できます。使用方法の詳細、および他のポリシー設定との関係と依存関係については、オーディオポリ

シー設定、帯域幅ポリシー設定、およびマルチストリーム接続ポリシー設定を参照してください。

適応型オーディオ

適応型オーディオを使用すると、VDAでオーディオ品質ポリシーを手動で構成する必要がありません。適応型オーディオは、お使いの環境に合わせて設定を最適化し、古いオーディオ圧縮形式を置き換えることで、優れたユーザーエクスペリエンスを提供します。

適応型オーディオはデフォルトで有効になっています。適応型オーディオを無効にするには、オーディオポリシー設定を参照してください。

重要:

リアルタイムオーディオアプリケーションが必要な場合は、Citrix®はTCPではなくUser Datagram Protocol (UDP)を使用してオーディオを配信することを推奨します。UDPでは、以下のオーディオ転送オプションが利用可能です。

- UDP経由のオーディオ
- HDX™アダプティブトランスポート (Enlightened Data Transport)

DTLSを使用したUDPオーディオ暗号化は、Citrix GatewayとCitrix Workspace™アプリの間でのみ利用可能です。したがって、場合によってはTCP転送を使用する方が望ましいことがあります。TCPは、VDAからCitrix Workspaceアプリへのエンドツーエンドの TLS暗号化をサポートします。

適応型オーディオおよびUDPオーディオの詳細については、UDPリアルタイムトランスポート経由のオーディオおよびオーディオUDPポート範囲を参照してください。

オーディオの損失許容モード

損失許容モードはオーディオをサポートします。この機能は、高遅延およびパケット損失のあるネットワークを介してユーザーが接続している場合に、リアルタイムストリーミングのユーザーエクスペリエンスを向上させ、EDT経由のオーディオ品質を改善します。この機能はデフォルトで無効になっています。

> **注:**
>
> この機能が動作するには、**HDXアダプティブトランスポート (EDT)** および**オーディオの損失許容モード**の両方のポリシーを有効にする必要があります。

システム要件

以下の製品が、損失許容モードをサポートする最小バージョンであることを確認してください。

- シトリックス Virtual Delivery Agent (VDA) 2308
- Windows向けCitrix Workspaceアプリ 2309

さらに、以下の機能を有効にする必要があります。

- HDX Adaptive Transportポリシー。
- (オプション) リモート接続の場合、Citrix Gateway Service が必要です。

> **注：**
>
> 上記の条件が満たされない場合、オーディオはEDT Reliableトランスポート経由で送信されます。

追加情報

損失許容モードは、マルチメディアコンテンツを再送信することなく、送信中のパケット損失を許容する損失許容トランスポートプロトコルであり、ユーザーによりリアルタイムなエクスペリエンスをもたらします。

Enlightened Data Transport (EDT) は、Citrix独自のトランスポートプロトコルであり、サーバーのスケーラビリティを維持しながら、困難な長距離接続で優れたユーザーエクスペリエンスを提供します。損失許容モードは、ネットワークの輻輳に直面しても安定した接続を維持するために、損失許容モードをトランスポートプロトコルとして使用するCitrix Gatewayサービスの機能です。これにより、リモートワーカーに一貫した安定したエクスペリエンスが保証されます。通常の状況では、EDTと損失許容モードの両方が同様の結果を提供します。ただし、パケット損失のあるネットワーク状況では、損失許容モードはEDTと比較してより良いオーディオエクスペリエンスを提供します。このため、リアルタイムマルチメディアに依存するリモートワーカーにとって不可欠な機能となります。

オーディオ品質

一般的に、音質が高いほど、より多くのオーディオデータをユーザーデバイスに送信するため、より多くの帯域幅とサーバーCPU使用率を消費します。サウンド圧縮を使用すると、音質とセッション全体のパフォーマンスのバランスを取ることができます。Citrixポリシー設定を使用して、サウンドファイルに適用する圧縮レベルを構成します。

デフォルトでは、TCPトランスポートが使用されている場合、**オーディオ品質ポリシー**設定は「高 - 高精細オーディオ」に設定されています。UDPトランスポート（推奨）が使用されている場合、ポリシーは「中 - 音声用に最適化」に設定されます。**高精細オーディオ**設定は、高忠実度のステレオオーディオを提供しますが、他の品質設定よりも多くの帯域幅を消費します。最適化されていない音声チャットまたはビデオチャットアプリケーション（ソフトフォンなど）には、このオーディオ品質を使用しないでください。その理由は、リアルタイム通信に適さない遅延をオーディオパスに導入する可能性があるためです。選択したトランスポートプロトコルに関係なく、リアルタイムオーディオには「音声用に最適化」ポリシー設定を推奨します。

帯域幅が制限されている場合（衛星接続やダイヤルアップ接続など）、オーディオ品質を**低**に設定すると、消費される帯域幅が最小限になります。この状況では、高帯域幅接続のユーザーが悪影響を受けないように、低帯域幅接続のユーザー向けに個別のポリシーを作成してください。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

オーディオ再生と録音の帯域幅ガイドライン:

- アダプティブオーディオ (デフォルト)
  - ビットレート: 可変適応型
  - チャンネル数: 再生用2 (ステレオ)、マイク入力用1 (モノラル)
  - 周波数: 48000 Hz
  - ビット深度: 16ビット
- 高品質
  - ビットレート: 再生用約100 kbps (最小75、最大175 kbps) / マイク入力用約70 kbps
  - チャンネル数: 再生用2 (ステレオ)、マイク入力用1 (モノラル)
  - 周波数: 44100 Hz
  - ビット深度: 16ビット
- 中品質 (VoIPに推奨)

- ビットレート: 再生用約16 kbps (最小20、最大40 kbps)、マイク入力用約16 kbps
- チャンネル数: 再生とキャプチャの両方で1 (モノラル)
- 周波数: 16000 Hz (広帯域)
- ビット深度: 16ビット

- 低品質
  - ビットレート: 再生で約11 kbps (最小10; 最大25 kbps)、マイクキャプチャで約11 kbps
  - チャンネル数: 再生とキャプチャの両方で1 (モノラル)
  - 周波数: 8000 Hz (狭帯域)
  - ビット深度: 16ビット

クライアントオーディオリダイレクト

ユーザーがサーバー上のアプリケーションからのオーディオを、ユーザーデバイスのスピーカーまたはその他のサウンドデバイスを介して受信できるようにするには、**クライアントオーディオリダイレクト**設定を**許可**のままにします。これがデフォルトです。

クライアントオーディオマッピングは、サーバーとネットワークに追加の負荷をかけます。ただし、クライアントオーディオリダイレクトを禁止すると、すべてのHDXオーディオ機能が無効になります。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

クライアントマイクのリダイレクト

ユーザーがユーザーデバイス上のマイクなどの入力デバイスを使用してオーディオを録音できるようにするには、**クライアントマイクのリダイレクト**設定をデフォルト（許可）のままにします。

セキュリティのため、ユーザーデバイスは、信頼できないサーバーがマイクへのアクセスを試みた場合に、ユーザーに警告します。ユーザーはマイクを使用する前に、アクセスを許可するか拒否するかを選択できます。ユーザーはCitrix Workspaceアプリでこの警告を無効にできます。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでClient audio settingsを有効にすることを忘れないでください。

オーディオプラグアンドプレイ

オーディオプラグアンドプレイポリシー設定は、複数のオーディオデバイスを使用してサウンドを録音および再生することを許可または禁止します。この設定は、デフォルトで**有効**になっています。オーディオプラグアンドプレイにより、オーディオデバイスが認識されるようになります。ユーザーセッションが開始されるまで接続されていなくても、デバイスは認識されます。

この設定は、WindowsマルチセッションOSマシンにのみ適用されます。

設定の詳細については、「オーディオポリシー設定」を参照してください。

オーディオリダイレクト帯域幅制限とオーディオリダイレクト帯域幅制限（パーセント）

オーディオリダイレクト帯域幅制限ポリシー設定は、セッションでのオーディオの再生と録音の最大帯域幅（キロビット/秒）を指定します。

オーディオリダイレクト帯域幅制限（パーセント）設定は、オーディオリダイレクトの最大帯域幅を、利用可能な総帯域幅のパーセンテージとして指定します。

デフォルトでは、両方の設定でゼロ（最大なし）が指定されています。両方の設定が構成されている場合、帯域幅制限が最も低い方が使用されます。

設定の詳細については、「帯域幅ポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

UDPリアルタイムトランスポート経由のオーディオとオーディオUDPポート範囲

デフォルトでは、ユーザーデータグラムプロトコル（UDP）リアルタイムトランスポート経由のオーディオは許可されています（インストール時に選択した場合）。これは、UDPリアルタイムトランスポート経由のオーディオを使用する接続のために、サーバー上にUDPポートを開きます。ネットワークの輻輳やパケット損失がある場合、可能な限り最高のユーザーエクスペリエンスを確保するために、オーディオにUDP/RTPを構成することをお勧めします。ソフトフォンアプリケーションなどのリアルタイムオーディオの場合、EDTよりもUDPオーディオが推奨されます。UDPは再送信なしでパケット損失を許容するため、パケット損失が多い接続で遅延が追加されないようにします。

> **重要:**

Citrix Gatewayが経路にない場合、UDPで送信されるオーディオデータは暗号化されません。Citrix GatewayがCitrix Virtual Apps and Desktops™リソースにアクセスするように構成されている場合、エンドポイントデバイスとCitrix Gateway間のオーディオトラフィックはDTLSプロトコルを使用して保護されます。

オーディオUDPポート範囲は、Windows VDAがユーザーデバイスとオーディオパケットデータを交換するために使用するポート番号の範囲を指定します。

デフォルトでは、範囲は16500から16509です。

注:

アダプティブオーディオにUDPリアルタイムトランスポート経由のオーディオが不要な場合、Citrixはポリシー設定を「無効」に構成することを推奨します。これにより、Citrix WorkspaceアプリクライアントがUDP接続のオープンを要求したり、不要なCitrix Workspaceアプリクライアントのファイアウォール構成ダイアログウィンドウが表示されたりするのを防ぐことができます。

UDPリアルタイムトランスポート経由のオーディオの設定の詳細については、「オーディオポリシー設定」を参照してください。オーディオUDPポート範囲の詳細については、「マルチストリーム接続ポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

UDP経由のオーディオにはWindows VDAが必要です。Linux VDAでサポートされているポリシーについては、「ポリシーサポートリスト」を参照してください。

ユーザーデバイスのオーディオ設定ポリシー

1. 「グループポリシーオブジェクト管理用テンプレートの構成」に従って、グループポリシーテンプレートをロードします。
2. グループポリシーエディターで、**［管理用テンプレート］>［Citrix Components］>［Citrix Workspace］>［ユーザーエクスペリエンス］** の順に展開します。
3. **［クライアントオーディオ設定］** で、**［未構成］**、**［有効］**、または **［無効］** を選択します。

    - **［未構成］**。既定では、オーディオリダイレクトは高品質オーディオまたは以前に構成されたカスタムオーディオ設定を使用して有効になります。

- **［有効］**。選択したオプションを使用してオーディオリダイレクトを有効にします。
- **［無効］**。オーディオリダイレクトを無効にします。

4. **［有効］** を選択した場合は、音質を選択します。UDPオーディオの場合は、**［中］**（既定）を使用します。
5. UDPオーディオの場合のみ、**［リアルタイムトランスポートを有効にする］** を選択し、ローカルのWindowsファイアウォールで開く受信ポートの範囲を設定します。
6. Citrix GatewayでUDPオーディオを使用するには、**［ゲートウェイ経由のリアルタイムトランスポートを許可する］** を選択します。DTLSでCitrix Gatewayを構成します。詳しくは、こちらの記事を参照してください。

管理者として、これらの変更を行うためのエンドポイントデバイスを制御できない場合は、StoreFrontのdefault.ica属性を使用してUDPオーディオを有効にします。たとえば、BYODデバイスや家庭用コンピューターの場合などです。

1. StoreFrontマシンで、C:\inetpub\wwwroot\Citrix\\\<Store Name>\App_Data\default.icaをメモ帳などのエディターで開きます。
2. セクションに以下のエントリを作成します。

```
; このテキストはリアルタイムトランスポートを有効にします

EnableRtpAudio=有効

; このテキストはゲートウェイ経由のリアルタイムトランスポートを許可します

EnableUDPThroughGateway=有効

; このテキストはオーディオ品質を「中」に設定します

AudioBandwidthLimit=1

; UDP ポート範囲

RtpAudioLowestPort=16500

RtpAudioHighestPort=16509
```

default.ica を編集してユーザーデータグラムプロトコル (UDP) オーディオを有効にすると、そのストアを使用しているすべてのユーザーに対して UDP オーディオが有効になります。

マルチメディア会議中のエコーを回避する

オーディオまたはビデオ会議のユーザーはエコーを聞くことがあります。エコーは通常、スピーカーとマイクが互いに近すぎるときに発生します。そのため、オーディオおよびビデオ会議にはヘッドセットの使用をお勧めします。

HDXは、エコーを最小限に抑えるエコーキャンセルオプション（デフォルトで有効）を提供します。エコーキャンセルの有効性は、スピーカーとマイクの間の距離に影響されます。デバイスが互いに近すぎたり遠すぎたりしないようにしてください。

レジストリ設定を変更して、エコーキャンセルを無効にできます。詳細については、レジストリを介して管理される機能のリストにあるマルチメディア会議中のエコーを回避するを参照してください。

ソフトフォン

ソフトフォンとは、電話インターフェースとして機能するソフトウェアです。コンピューターやその他のスマートデバイスからインターネット経由で電話をかけるためにソフトフォンを使用します。ソフトフォンを使用すると、画面を使って電話番号をダイヤルしたり、その他の電話関連機能を実行したりできます。

Citrix Virtual Apps and Desktopsは、ソフトフォンを配信するためのいくつかの代替手段をサポートしています。

- **制御モード**。ホストされているソフトフォンが物理的な電話機を制御します。このモードでは、Citrix Virtual Apps and Desktopsサーバーを介してオーディオトラフィックが流れることはありません。
- **HDX RealTime最適化ソフトフォンサポート（推奨）**。メディアエンジンはユーザーデバイス上で実行され、Voice over Internet Protocolトラフィックはピアツーピアで流れます。例については、以下を参照してください。
    - Microsoft Teams向けHDX最適化
    - HDX RealTime Optimization Pack（Microsoft Skype for Businessの配信を最適化します）
    - Cisco Jabber VDI用ソフトフォン (旧称 VXME)
    - Cisco Webex VDI用ミーティング
    - アバイア VDI エクイノックス (旧称 VDI コミュニケーター)
    - Zoom VDIプラグイン
    - ジェネシス ピュアエンゲージ クラウド
    - Nuance Dragon PowerMicディクテーションデバイス

- **Local App Access**。ソフトフォンなどのアプリケーションをWindowsユーザーデバイスでローカルに実行しながら、仮想/公開デスクトップとシームレスに統合されているように見せるCitrix Virtual Apps and Desktopsの機能です。この機能は、すべてのオーディオ処理をユーザーデバイスにオフロードします。詳しくは、「Local App AccessとURLリダイレクト」を参照してください。
- **HDX RealTime汎用ソフトフォンサポート。** ICA経由のVoice over Internet Protocol。

汎用ソフトフォンサポート

汎用ソフトフォンサポートを使用すると、変更されていないソフトフォンをデータセンターのXenAppまたはXenDesktopでホストできます。オーディオトラフィックは、Citrix ICAプロトコル（UDP/RTPの使用が望ましい）を介して、Citrix Workspaceアプリを実行しているユーザーデバイスに送信されます。

汎用ソフトフォンサポートは、HDX RealTimeの機能です。このソフトフォン配信のアプローチは、特に次の場合に役立ちます。

- ソフトフォンを配信するための最適化されたソリューションが利用できず、ユーザーがLocal App Accessを使用できるWindowsデバイスを使用していない場合。
- ソフトフォンの最適化された配信に必要なメディアエンジンがユーザーデバイスにインストールされていないか、ユーザーデバイスで実行されているオペレーティングシステムのバージョンで利用できない場合。このシナリオでは、汎用HDX RealTimeが貴重なフォールバックソリューションを提供します。

Citrix Virtual Apps and Desktopsを使用する際のソフトフォン配信には、次の2つの考慮事項があります。

- ソフトフォンアプリケーションが仮想/公開デスクトップにどのように配信されるか。
- オーディオがユーザーのヘッドセット、マイク、スピーカー、またはUSB電話機にどのように送受信されるか。

Citrix Virtual Apps and Desktopsには、汎用ソフトフォン配信をサポートするための多数のテクノロジーが含まれています。

- リアルタイムオーディオの高速エンコードと帯域幅の効率化のための音声に最適化されたコーデック。
- 低遅延オーディオスタック。
- ネットワーク遅延が変動するときにオーディオをスムーズにするためのサーバー側ジッターバッファ。

- サービス品質（QoS）のためのパケットタグ付け（DSCPおよびWMM）。
  - RTPパケットのDSCPタグ付け (レイヤー3)
  - Wi-Fi用WMMタグ付け

Windows、Linux、Chrome、Mac版のCitrix WorkspaceアプリもVoice over Internet Protocolに対応しています。Windows版Citrix Workspaceアプリは、以下の機能を提供します。

- クライアント側ジッターバッファ - ネットワーク遅延が変動する場合でも、スムーズなオーディオを保証します。
- エコーキャンセル - ヘッドセットを使用しない作業者向けに、マイクとスピーカー間の距離の許容範囲を広げます。
- オーディオプラグアンドプレイ - オーディオデバイスはセッションを開始する前に接続する必要はありません。いつでも接続できます。
- オーディオデバイスルーティング - ユーザーは着信音をスピーカーに、音声パスをヘッドセットに振り向けることができます。
- マルチストリームICA - ネットワーク経由で柔軟なQuality of Serviceベースのルーティングを可能にします。
- ICAは4つのTCPストリームと2つのUDPストリームをサポートします。UDPストリームの1つは、RTP経由のリアルタイムオーディオをサポートします。

Citrix Workspaceアプリの機能の概要については、Citrix Receiverの機能マトリックスを参照してください。

システム構成の推奨事項

クライアントハードウェアとソフトウェア: 最適なオーディオ品質を得るには、Citrix Workspaceアプリの最新バージョンと、音響エコーキャンセル（AEC）機能を備えた高品質のヘッドセットをお勧めします。Windows、Linux、Mac版のCitrix WorkspaceアプリはVoice over Internet Protocolをサポートしています。また、Dell WyseはThinOS（WTOS）向けにVoice over Internet Protocolサポートを提供しています。

CPUに関する考慮事項: VDAのCPU使用率を監視して、各仮想マシンに2つの仮想CPUを割り当てる必要があるかどうかを判断します。リアルタイムの音声とビデオはデータ集約型です。2つの仮想CPUを構成すると、スレッド切り替えの遅延が減少します。したがって、Citrix Virtual Desktops™ VDI環境では2つのvCPUを構成することをお勧めします。

2つの仮想CPUを持つことは、物理CPUの数を2倍にすることを必ずしも意味しません。物理CPUはセッション間で共有できるためです。

セッションの信頼性機能に使用されるCitrix Gateway Protocol（CGP）も、CPU消費量を増加させます。高品質のネットワーク接続では、VDAでのCPU消費量を削減するためにこの機能を無効にできます。強力なサーバーでは、上記のいずれのステップも必要ない場合があります。

UDP Audio: UDP経由のオーディオは、ネットワークの輻輳とパケット損失に対して優れた耐性を提供します。利用可能な場合は、TCPの代わりにこれをお勧めします。

LAN/WAN configuration: 良好なリアルタイムオーディオ品質のためには、ネットワークの適切な構成が不可欠です。通常、過剰なブロードキャストパケットがジッターを引き起こす可能性があるため、仮想LAN（VLAN）を構成する必要があります。IPv6対応デバイスは、多くのブロードキャストパケットを生成する可能性があります。IPv6サポートが不要な場合は、それらのデバイスでIPv6を無効にすることができます。Quality of Serviceをサポートするように構成してください。

Settings for use WAN connections: LANおよびWAN接続を介してボイスチャットを使用できます。WAN接続では、オーディオ品質は接続の遅延、パケット損失、およびジッターに依存します。WAN接続のユーザーにソフトフォンを配信する場合、データセンターとリモートオフィス間でNetScaler® SD-WANを使用することをお勧めします。これにより、高いQuality of Serviceが維持されます。NetScaler SD-WANは、UDPを含むMulti-Stream ICAをサポートしています。また、単一のTCPストリームの場合でも、さまざまなICA仮想チャネルの優先順位を区別して、高優先度のリアルタイムオーディオデータが優先的に処理されるようにすることが可能です。

DirectorまたはHDX Monitorを使用して、HDX構成を検証します。

リモートユーザー接続: Citrix Gatewayは、DTLSをサポートしており、UDP/RTPトラフィックをネイティブに（TCPでのカプセル化なしで）配信します。 ポート443経由のUDPトラフィックに対して、ファイアウォールを双方向に開いてください。

Codec selection and bandwidth consumption: ユーザーデバイスとデータセンター内のVDA間では、Medium Qualityオーディオとも呼ばれる**Optimized-for-Speech**コーデック設定を使用することをお勧めします。VDAプラットフォームとIP-PBX間では、ソフトフォンは構成またはネゴシエートされたコーデックを使用します。例：

- G711は良好な音声品質を提供しますが、1コールあたり80キロビット/秒から100キロビット/秒の帯域幅を必要とします（ネットワークレイヤー2のオーバーヘッドによって異なります）。
- G729は良好な音声品質を提供し、1コールあたり30キロビット/秒から40キロビット/秒という低い帯域幅要件です（ネットワークレイヤー2のオーバーヘッドによって異なります）。

仮想デスクトップへのソフトフォンアプリケーションの配信

XenDesktop®仮想デスクトップにソフトフォンを配信するには、2つの方法があります。

- アプリケーションを仮想デスクトップイメージにインストールできます。
- アプリケーションはMicrosoft App-Vを使用して仮想デスクトップにストリーミングできます。このアプローチは、仮想デスクトップイメージが整理された状態に保たれるため、管理上の利点があります。仮想デスクトップにストリーミングされた後、アプリケーションは通常の方法でインストールされたかのようにその環境で実行されます。すべてのアプリケーションがApp-Vと互換性があるわけではありません。

ユーザーデバイスとの間でオーディオを配信する

Generic HDX RealTimeは、ユーザーデバイスとの間でオーディオを配信する2つの方法をサポートしています。

- **Citrix Audio Virtual Channel**。Citrix Audio Virtual Channelはオーディオ転送のために特別に設計されているため、一般的にこれをお勧めします。
- **汎用USBリダイレクト**。ユーザーデバイスがCitrix Virtual Apps and Desktopsサーバーへの LANまたはLANに類似した接続上にある場合、ボタンまたはディスプレイ（あるいはその両方）を備えたオーディオデバイス、ヒューマンインターフェースデバイス（HID）をサポートします。

Citrix オーディオ仮想チャネル

双方向のCitrixオーディオ仮想チャネル（CTXCAM）により、オーディオをネットワーク経由で効率的に配信できます。汎用HDX RealTimeは、ユーザーのヘッドセットまたはマイクからのオーディオを取得し、圧縮します。その後、ICA経由で仮想デスクトップ上のソフトフォンアプリケーションに送信します。同様に、ソフトフォンのオーディオ出力は圧縮され、ユーザーのヘッドセットまたはスピーカーに逆方向に送信されます。この圧縮は、ソフトフォン自体が使用する圧縮（G.729やG.711など）とは独立しています。これは、Optimized-for-Speechコーデック（中品質）を使用して行われます。その特性は、Voice over Internet Protocolに最適です。エンコード時間が短く、ネットワーク帯域幅はピーク時で約56キロビット/秒（各方向28 Kbps）しか消費しません。このコーデックはデフォルトのオーディオコーデックではないため、Studioコンソールで明示的に選択する必要があります。デフォルトはHDオーディオコーデック（高品質）です。このコーデックは高忠実度のステレオサウンドトラックに優れていますが、Optimized-for-Speechコーデックと比較してエンコードが遅くなります。

汎用 USB リダイレクト

Citrix汎用USBリダイレクトテクノロジー（CTXGUSB仮想チャネル）は、複合デバイス（オーディオとHID）およびアイソクロナスUSBデバイスを含むUSBデバイスをリモートで利用するため

の汎用的な手段を提供します。このアプローチは、LAN接続されたユーザーに限定されます。その理由は、USBプロトコルがネットワーク遅延に敏感であり、かなりのネットワーク帯域幅を必要とする傾向があるためです。アイソクロナスUSBリダイレクトは、一部のソフトフォンを使用する場合にうまく機能します。このリダイレクトは、優れた音声品質と低遅延を提供します。ただし、Citrixオーディオ仮想チャネルはオーディオトラフィックに最適化されているため、こちらが推奨されます。主な例外は、ボタン付きのオーディオデバイスを使用している場合です。例えば、データセンターにLAN接続されたユーザーデバイスに接続されたUSB電話などです。この場合、汎用USBリダイレクトは、ソフトフォンに信号を送り返すことで機能を制御する電話機またはヘッドセットのボタンをサポートします。デバイス上でローカルに機能するボタンには問題ありません。

オーディオ診断コマンドラインツール

VDA上のオーディオ診断コマンドラインツールは、オーディオポリシー、構成、およびデータ転送に関連するセッションデータを照会するために使用できます。

使用方法

コマンドプロンプトを開き、`C:\Program Files\Citrix\HDX\bin`フォルダーから`CtxAudio.exe`を実行します。

- 管理者としてツールを実行すると、すべてのアクティブなICAセッションのオーディオ情報が表示されます。
- 非管理者としてツールを実行すると、現在ユーザーのICAセッションオーディオ情報が表示されます。

出力

このツールは、セッション内のオーディオ関連の問題の診断に役立つさまざまな構成設定を出力します。

セクション	説明
ポリシー情報	現在のセッションに適用されているオーディオポリシー。
設定情報	レジストリに保存されているオーディオ関連の構成設定。
状態情報	現在のセッションに適用されているオーディオの状態、バージョン、コーデック、およびトランスポート。

セクション	説明
デバイス情報	セッションで使用されているデバイス名、その役割、およびステータス。

注:

出力は、マルチセッション (TS) VDA またはシングルセッション VDA (WSVDA) のどちらでツールを実行するかによって異なります。

制限事項

クライアントにオーディオデバイスをインストールし、オーディオリダイレクトを有効にして、RDSセッションを開始します。オーディオファイルが再生に失敗し、エラーメッセージが表示されることがあります。

回避策として、RDSマシンにレジストリキーを追加し、マシンを再起動します。詳細については、レジストリで管理される機能のリストにあるオーディオの制限を参照してください。

ブラウザコンテンツリダイレクト

ブラウザコンテンツリダイレクトは、VDA側での許可リスト内のWebページのレンダリングを防ぎます。この機能は、Windows版Citrix Workspace™アプリまたはLinux版Citrix Workspaceアプリを使用して、クライアント側で対応するレンダリングエンジンをインスタンス化し、URLからHTTPおよびHTTPSコンテンツを取得します。

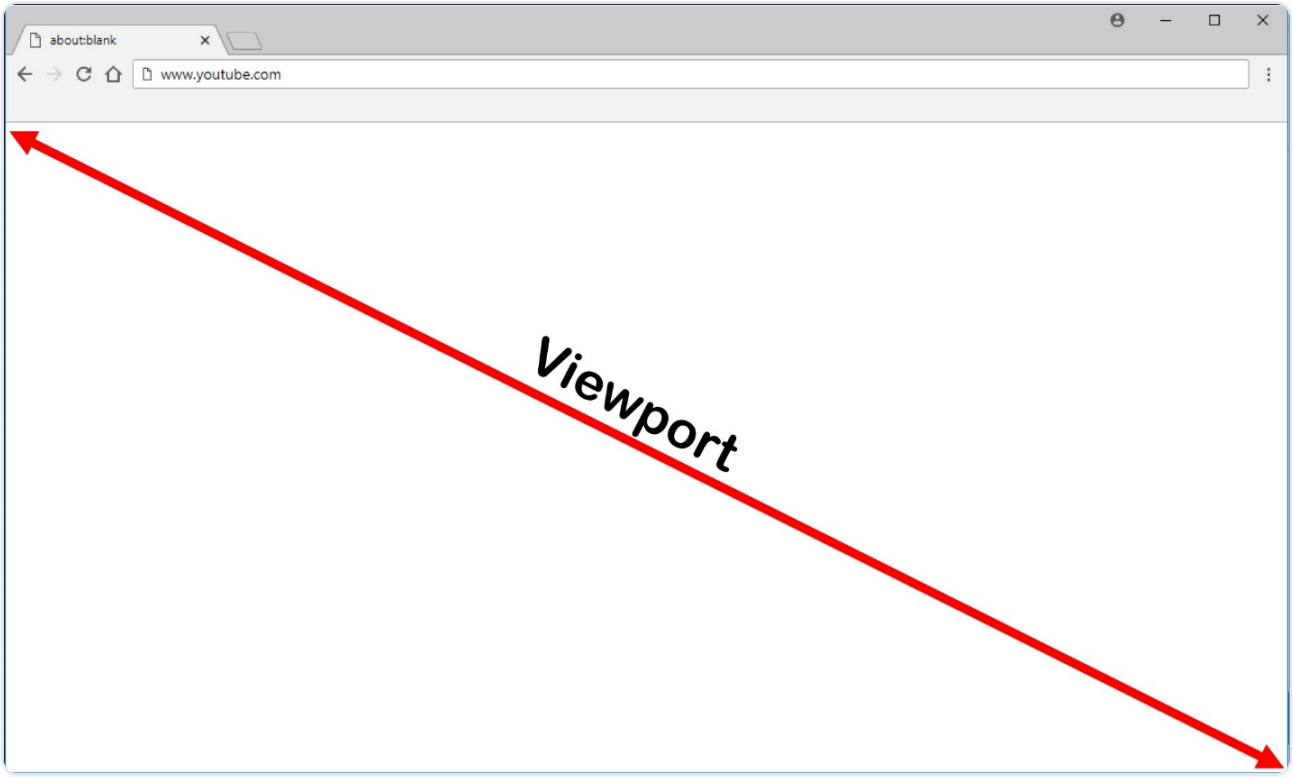
注:

ブロックリストを使用することで、WebページをVDA側にリダイレクトする（クライアント側にはリダイレクトしない）ように指定できます。

このオーバーレイWebレイアウトエンジンは、VDA上ではなくエンドポイントデバイス上で実行され、エンドポイントのCPU、GPU、RAM、およびネットワークを使用します。

ブラウザのビューポートのみがリダイレクトされます。ビューポートとは、ブラウザ内でコンテンツが表示される長方形の領域です。ビューポートには、アドレスバー、**お気に入り**ツール

バー、**ステータス**バーなどの項目は含まれません。これらの項目は、VDA内のブラウザで引き続き実行されているユーザーインターフェイスにあります。



1. リダイレクト用の許可リストに含まれるURL、または特定のURLパスのリダイレクトを無効にするブロックリストを含むアクセス制御リストを指定するStudioポリシーを構成します。VDA上のブラウザが、ユーザーが移動しているURLが許可リストと一致するか、またはブロックリストと一致しないかを検出するために、ブラウザ拡張機能が比較を実行します。Chromeの場合、ブラウザ拡張機能はChromeウェブストアで入手でき、グループポリシーとADMXファイルを使用して展開できます。Chrome拡張機能はユーザーごとにインストールされます。拡張機能を追加または削除するためにゴールデンイメージを更新する必要はありません。Microsoft Edgeの場合、拡張機能は直接利用できません。Chromeストアからの拡張機能を許可して、それを見つけてインストールする必要があります。
2. 許可リストに一致するものが見つかり（例：`https://www.mycompany.com/`）、ブロックリスト内のURLに一致するものがない場合（例：`https://www.mycompany.com/engineering`）、仮想チャネル（CTXCSB）がCitrix Workspaceアプリにリダイレクトが必要であることを指示し、URLを中継します。その後、Citrix Workspaceアプリはローカルレンダリングエンジンをインスタンス化し、ウェブサイトを表示します。
3. その後、Citrix Workspaceアプリはウェブサイトを仮想デスクトップのブラウザコンテンツ領域にシームレスにブレンドし直します。

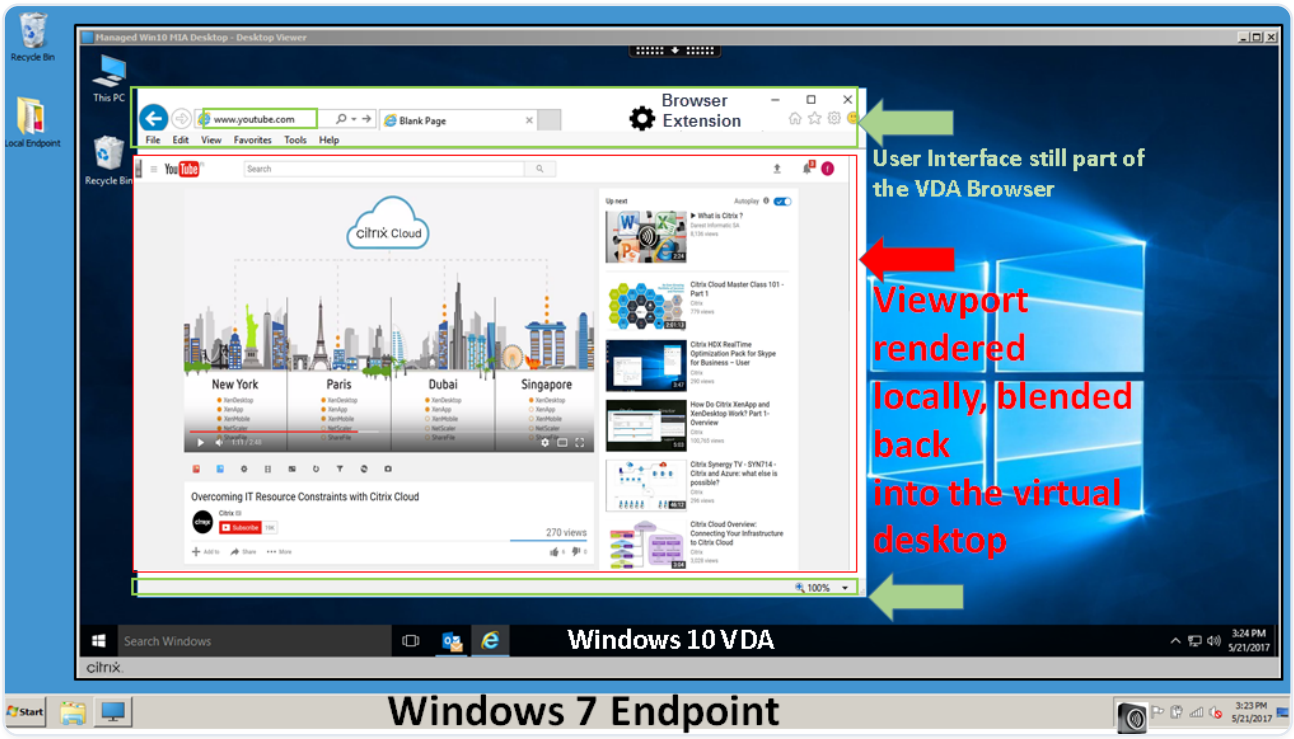
> **注:**

> ブラウザコンテンツリダイレクト拡張機能の新機能と修正に関する詳細については、Chromeウェブストアにアクセスし、`citrix bcr`を検索して拡張機能を見つけてください。

> ロゴの色は、Chrome拡張機能のステータスを示します。以下の3色のいずれかです。

- 緑：アクティブで接続済み。
- 灰色：現在のタブで非アクティブ/アイドル状態。
- 赤: 破損/動作していません。

拡張機能メニューの**オプション**を使用して、ログのデバッグができます。



Citrix Workspaceアプリがコンテンツをフェッチするシナリオを以下に示します。

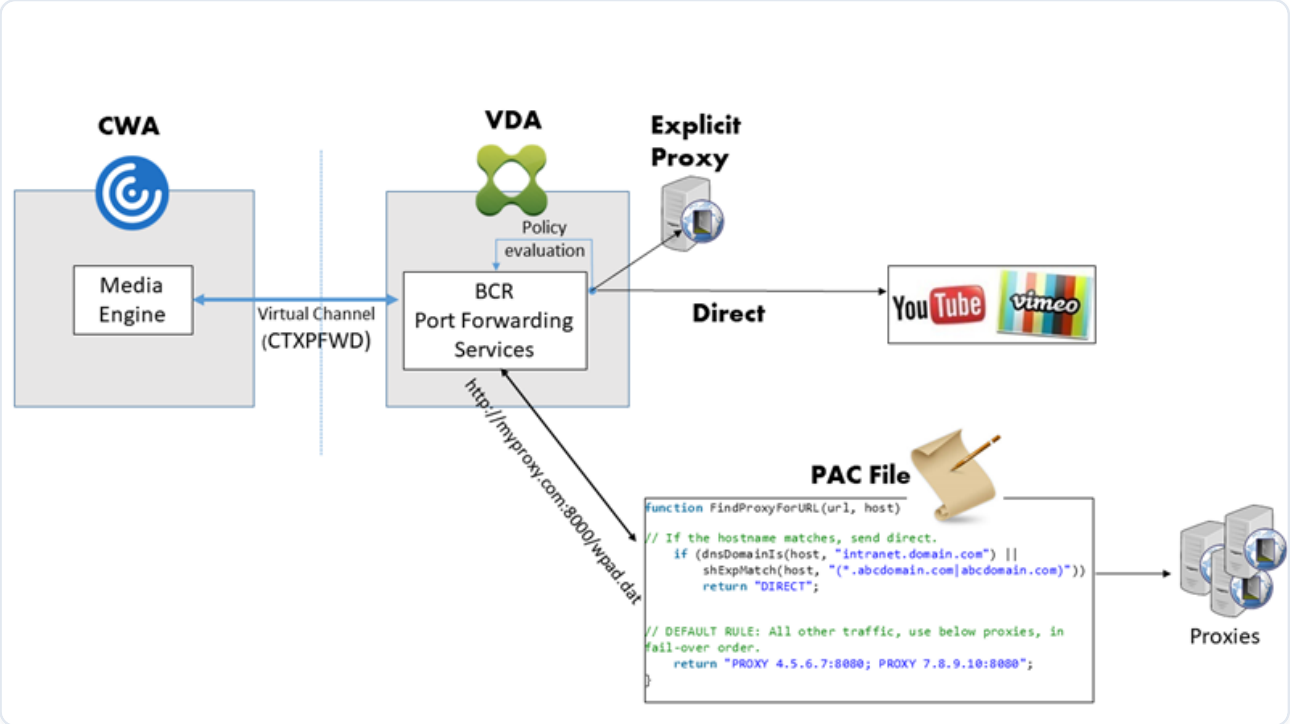
- **サーバーフェッチとサーバーレンダリング**: サイトを許可リストに追加しなかったか、リダイレクトが失敗したため、リダイレクトは行われません。VDAでWebページをレンダリングし、Thinwireを使用してグラフィックを削除するフォールバックを行います。フォールバック動作を制御するにはポリシーを使用します。VDAでのCPU、RAM、帯域幅の消費量が高くなります。
- **サーバーフェッチとクライアントレンダリング**: Citrix Workspaceアプリは、仮想チャネル（CTXPFWD）を使用してVDA経由でWebサーバーに接続し、コンテンツをフェッチします。このオプションは、クライアントがインターネットにアクセスできない場合（シンクライアン

トなど）に役立ちます。VDAでのCPUとRAMの消費量は低いですが、ICA®仮想チャネルで帯域幅が消費されます。

このシナリオには3つの動作モードがあります。「プロキシ」という用語は、VDAがインターネットアクセスを取得するためにアクセスするプロキシデバイスを指します。

選択するポリシーオプション:

- **明示的プロキシ**: データセンターに単一の明示的プロキシがある場合。
- **直接または透過的**: プロキシがない場合、または透過的プロキシを使用している場合。
- **PACファイル**: PACファイルに依存している場合、VDA内のブラウザは指定されたURLをフェッチするための適切なプロキシサーバーを自動的に選択できます。



- **クライアントフェッチとクライアントレンダリング**: Citrix WorkspaceアプリはWebサーバーに直接接続するため、インターネットアクセスが必要です。このシナリオでは、XenAppおよびXenDesktop®サイトからのネットワーク、CPU、RAMの使用量をすべてオフロードします。

  利点:

  - より良いエンドユーザーエクスペリエンス (アダプティブビットレート (ABR))
  - VDAリソース使用量の削減 (CPU/RAM/IO)
  - 帯域幅消費量の削減

ブラウザビューポートリダイレクトシナリオの画像(/en-us/citrix-virtual-apps-desktops/2407/media/browser-viewport-redirection-scenarios.png)

フォールバックメカニズム:

クライアントリダイレクトが失敗する場合があります。たとえば、クライアントマシンがインターネットに直接アクセスできない場合、エラー応答がVDAに戻されることがあります。このような場合、VDA上のブラウザはページをサーバー上で再読み込みしてレンダリングできます。

既存の**Windows Mediaフォールバック防止**ポリシーを使用して、ビデオ要素のサーバーレンダリングを抑制できます。このポリシーを**すべてのコンテンツをクライアントでのみ再生**または**クライアントでアクセス可能なコンテンツのみをクライアントで再生**に設定します。これらの設定は、クライアントリダイレクトに失敗した場合に、ビデオ要素がサーバーで再生されるのをブロックします。このポリシーは、ブラウザコンテンツリダイレクトを有効にし、**アクセス制御リスト**ポリシーにフォールバックするURLが含まれている場合にのみ有効になります。URLはブロックリストポリシーに含まれていてはなりません。

システム要件

シトリックス バーチャル アプリケーションズ アンド デスクトップ™

- シトリックス バーチャル アプリケーションズ アンド デスクトップ 7 1808 以降
- XenApp and XenDesktop 7.15 CU5以降
- VDA OS: ウィンドウズ 10 および 11、ウィンドウズ サーバー 2016/2019/2022
- VDA上のブラウザ:
  - Google Chromeの最新バージョン
  - Microsoft Edgeの最新バージョン
- VDAのブラウザにChromeウェブストアからインストールされたBCR拡張機能

Windowsエンドポイント

- Windows 10および11
- Citrix Workspaceアプリ 1809 for Windows以降

> **注:**
>
> ブラウザコンテンツリダイレクトは、Citrix WorkspaceアプリLTSRリリース1912および2203.1ではサポートされていません。

Linuxエンドポイント

- Citrix Workspaceアプリ 1808 for Linux以降
- シンクライアント端末にはWebKitGTK+が含まれている必要があります

Macエンドポイント（プレビュー）

- macOS 11 ビッグサー
- macOS 12 モントレー
- macOS 13 ベンチュラ
- Citrix Workspaceアプリの最小バージョンが2311のmacOS 14 Sonoma（14.2.1まで）

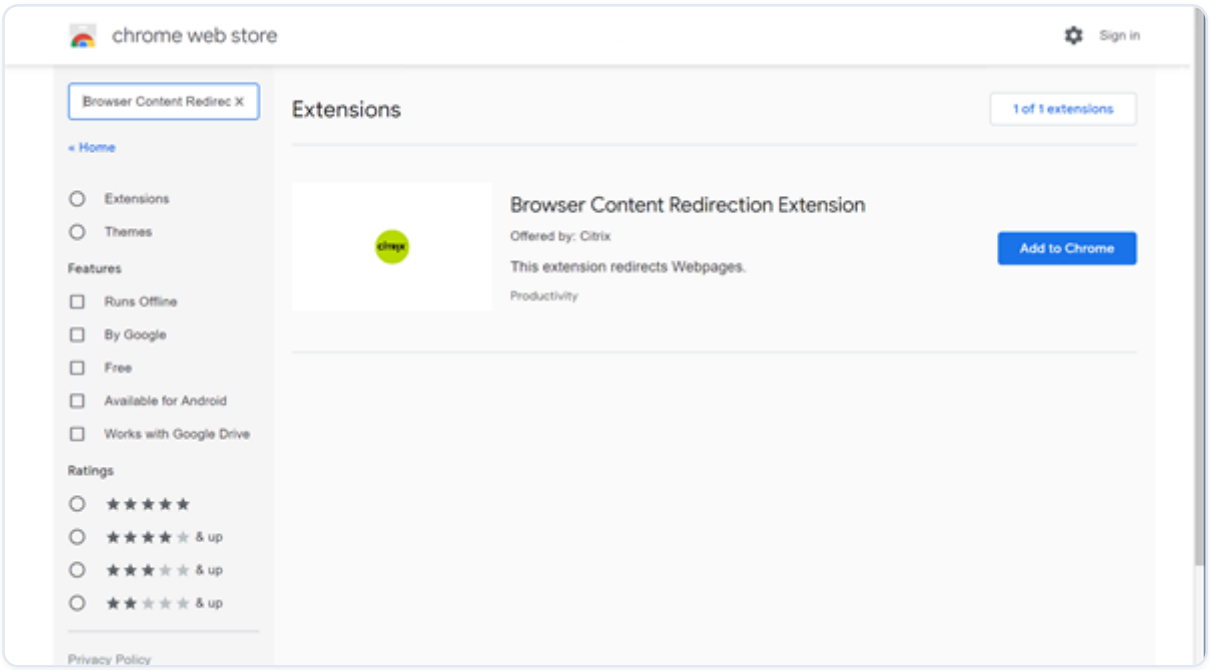
トラブルシューティング

トラブルシューティング情報については、「ブラウザコンテンツリダイレクトのトラブルシューティング方法ナレッジセンター」の記事を参照してください。

ブラウザコンテンツリダイレクトChrome拡張機能

Chromeでブラウザコンテンツリダイレクトを使用するには、Chromeウェブストアからブラウザコンテンツリダイレクト拡張機能を追加します。Citrix Virtual Apps and Desktops環境で をクリックします。

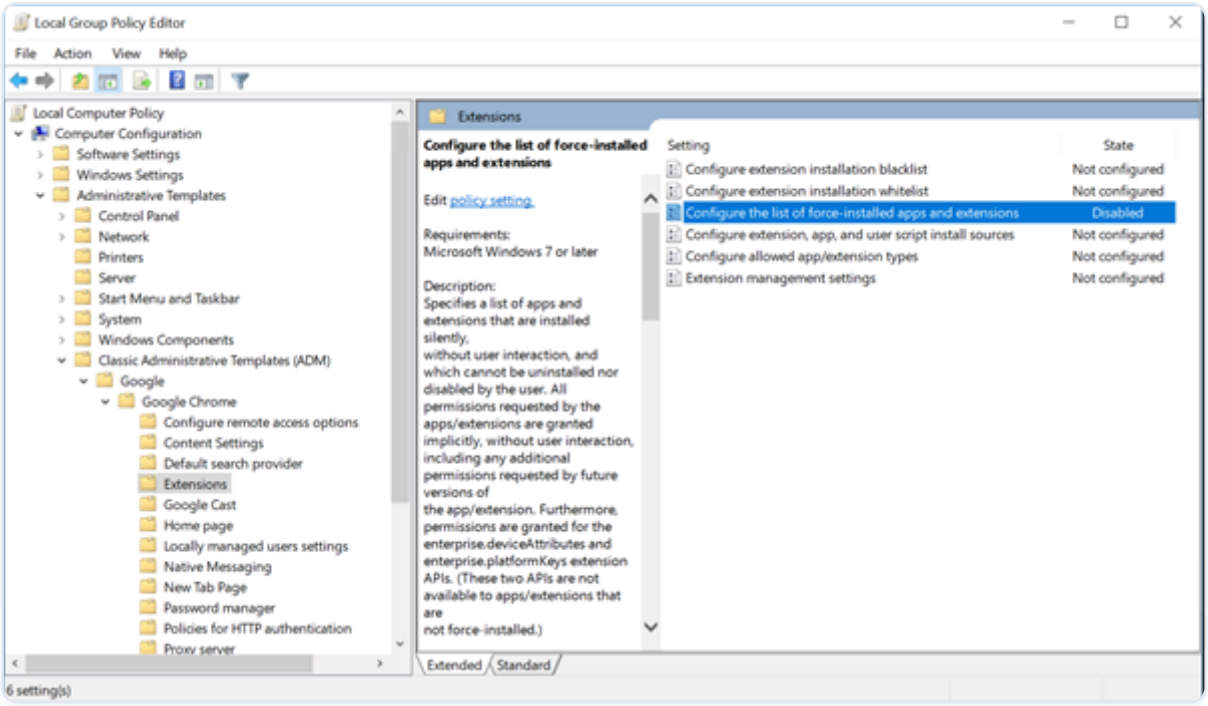
この拡張機能は、ユーザーのクライアントマシンには**不要**です。VDA にのみ必要です。



この方法は個々のユーザーに有効です。組織内の大規模なユーザーグループに拡張機能を展開するには、グループポリシーを使用して拡張機能を展開します。

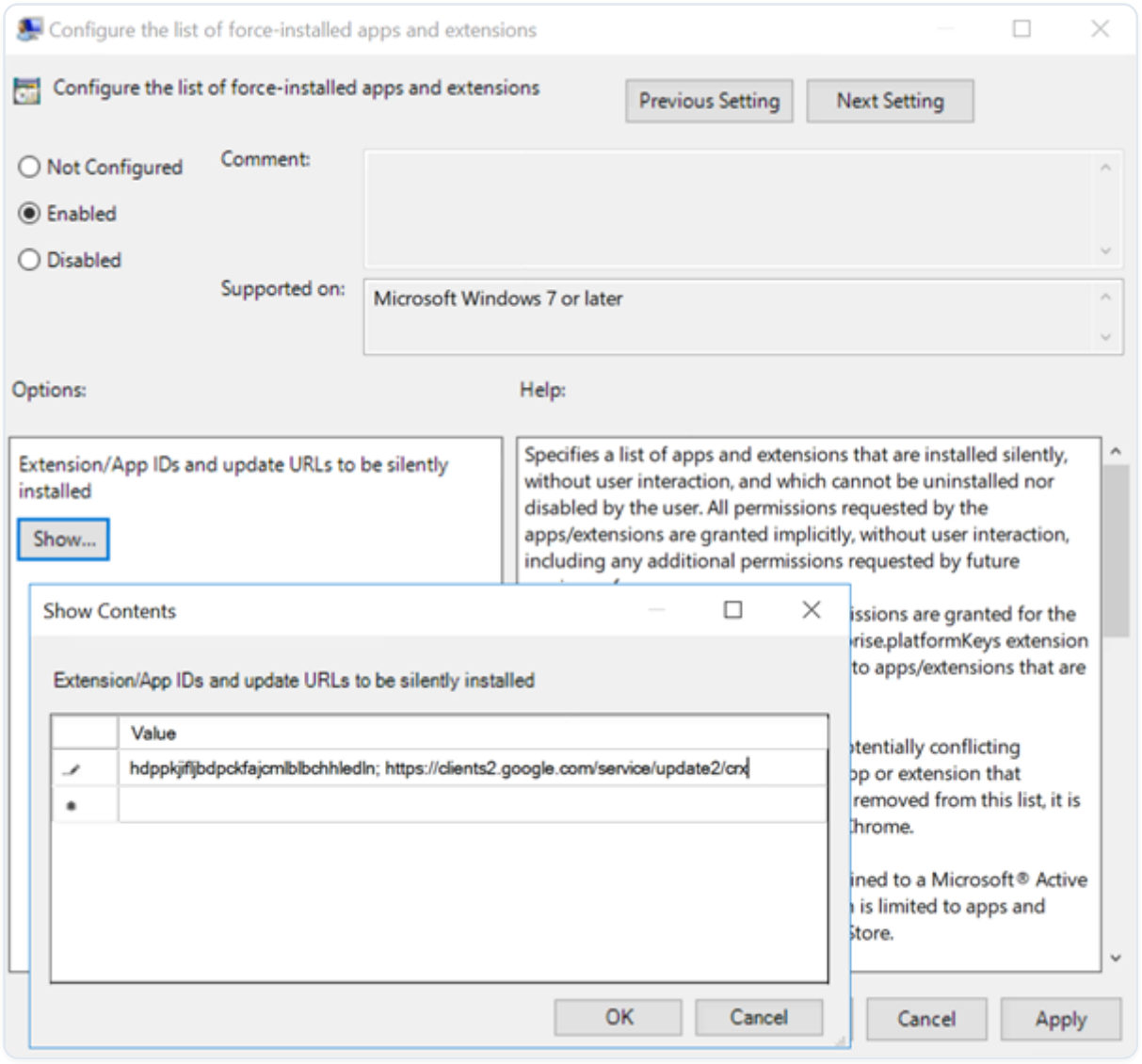
グループポリシーを使用した拡張機能の展開

1. Google Chrome ADMX ファイルを環境にインポートします。ポリシーテンプレートのダウンロード、およびグループポリシーエディターへのテンプレートのインストールと構成については、「管理対象 PC で Chrome ブラウザポリシーを設定する」を参照してください。
2. グループポリシー管理コンソールを開き、**ユーザーの構成 \ 管理用テンプレート\従来の管理用テンプレート (ADM) \ Google\ Google Chrome \ 拡張機能**に移動します。「**強制的にインストールするアプリと拡張機能のリストを構成する**」設定を有効にします。



3. をクリックし、拡張機能IDに対応する次の文字列を入力します。ブラウザコンテンツリダイレクト拡張機能のURLを更新します。

   `hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx`



4. 設定を適用し、**gpupdate**で更新すると、ユーザーは自動的に拡張機能を受け取ります。ユーザーのセッションでChromeブラウザを起動すると、拡張機能はすでに適用されており、削除することはできません。

   拡張機能への更新は、設定で指定した更新 URL を介してユーザーのマシンに自動的にインストールされます。

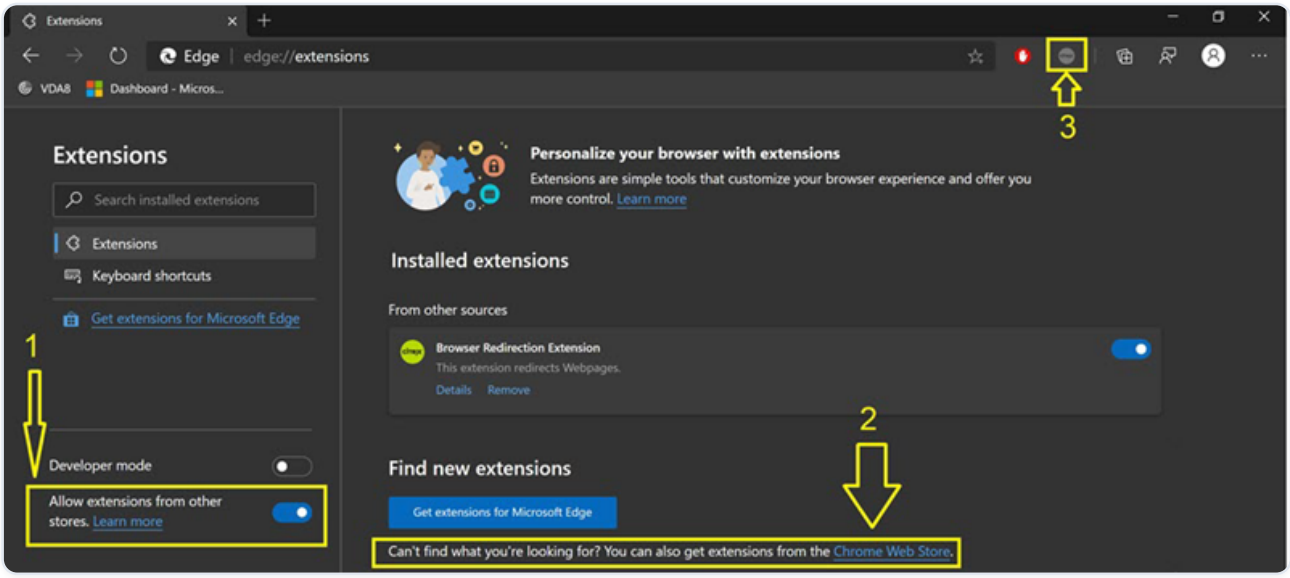
   「**強制的にインストールするアプリと拡張機能のリストを構成する**」設定が「**無効**」に設定されている場合、拡張機能はすべてのユーザーの Chrome から自動的に削除されます。

ブラウザコンテンツリダイレクト Edge Chromium 拡張機能

Edge にブラウザコンテンツリダイレクト拡張機能をインストールするには、Edge ブラウザのバージョン **83.0.478.37** 以降がインストールされていることを確認してください。

1. **拡張機能**オプションをクリックします。**拡張機能の管理**を選択します。**他のストアからの拡張機能を許可する**をオンにします。

2. **Chrome Web Store**リンクをクリックすると、拡張機能が右上のバーに表示されます。Microsoft Edge 拡張機能の詳細については、拡張機能を参照してください。



ブラウザーコンテンツリダイレクトとDPI

ユーザーのマシンでDPI（スケーリング）が100%を超えて設定されている状態でブラウザコンテンツリダイレクトを使用すると、リダイレクトされたブラウザコンテンツ画面が正しく表示されません。この問題を回避するには、ブラウザコンテンツリダイレクトを使用する際にDPIを設定しないでください。この問題を回避するもう1つの方法は、ユーザーのマシンにレジストリキーを作成して、Chrome のブラウザコンテンツリダイレクトGPUアクセラレーションを無効にすることです。詳細については、レジストリで管理される機能のリストにあるブラウザコンテンツリダイレクトとDPIを参照してください。

統合Windows認証によるシングルサインオン

ブラウザコンテンツリダイレクトは、VDA と同じドメイン内で統合Windows認証 (IWA) が構成されたWebサーバーへの認証に**Negotiate**スキームを使用するようにオーバーレイを強化します。

デフォルトでは、ブラウザコンテンツリダイレクトは、ユーザーがWebサーバーにアクセスするたびにVDA資格情報で認証することを要求する基本認証スキームを使用します。シングルサインオンの場合、**ブラウザコンテンツリダイレクト統合Windows認証サポート**ポリシー設定を有効にするか、VDA にレジストリキーを作成することができます。

シングルサインオンを有効にする前に、以下を完了してください。

- ホスト名から構築されたサービスプリンシパル名 (SPN) のチケットを発行するようにKerberosインフラストラクチャを構成します。例: `HTTP/serverhostname.com`。

- サーバーフェッチの場合: サーバーフェッチモードでブラウザコンテンツリダイレクトを使用する場合、VDA でDNSが適切に構成されていることを確認してください。
- クライアントフェッチの場合: クライアントフェッチモードでブラウザコンテンツリダイレクトを使用する場合、クライアントデバイスでDNSが適切に構成されており、オーバーレイからWebサーバーのIPアドレスへのTCP接続を許可していることを確認してください。

Browser content redirectionポリシーを使用してシングルサインオンを構成するには、Browser content redirection Integrated Windows Authentication support設定を参照してください。

または、VDAにレジストリキーを追加することで、Webサーバーへのシングルサインオンを有効にできます。詳しくは、レジストリで管理される機能のリストにあるブラウザコンテンツリダイレクトの統合Windows認証によるシングルサインオンを参照してください。

ユーザーエージェントリクエストヘッダー

ユーザーエージェントヘッダーは、ブラウザコンテンツリダイレクトから送信されるHTTPリクエストを識別するのに役立ちます。この設定は、プロキシおよびファイアウォールルールを構成する際に役立ちます。たとえば、サーバーがブラウザコンテンツリダイレクトから送信されるリクエストをブロックする場合、ユーザーエージェントヘッダーを含むルールを作成して、特定の要件をバイパスできます。

Windowsデバイスのみがユーザーエージェントリクエストヘッダーをサポートします。

デフォルトでは、ユーザーエージェントリクエストヘッダー文字列は無効になっています。クライアントでレンダリングされるコンテンツのユーザーエージェントヘッダーを有効にするには、レジストリエディターを使用します。詳しくは、レジストリで管理される機能のリストにあるユーザーエージェントリクエストヘッダーを参照してください。

ブラウザコンテンツリダイレクトクライアントの互換性

WMIを使用して、クライアントがブラウザコンテンツリダイレクトと互換性があるかどうかを確認できます。WMIにアクセスするための任意の方法を使用できます。以下はPowerShellを使用した例です。

1. PowerShellを開きます。
2. `Get-WmiObject -Class CTXBCRStatus`を実行します。
3. `BCR_Capable`パラメーターを確認します。
    - `True`の場合、クライアントはブラウザコンテンツリダイレクトと互換性があります。
    - `False`の場合、クライアントはブラウザコンテンツリダイレクトと互換性がありません。

追加情報

- `CtxBrowserSvc`が利用できない場合、コマンド実行時に結果は表示されません。
- `CtxBrowserSvc`が一度も実行されていない場合、結果は無効なクラスエラーを返します。

ブラウザコンテンツリダイレクトの制限事項

ブラウザコンテンツリダイレクトは、次のユースケースをサポートできません。

- ポップアップウィンドウを必要とするWebアプリケーションはサポートされていません。
- セッションクッキーの永続性を必要とするWebアプリケーションもサポートされていません。Google認証サービスに依存するアプリケーション（例：Google Meet）は、ブロックされる可能性があります。
- 拡張機能プラグインは、Microsoft Edgeストアでは公式に公開されていません。ただし、Chromeストアを使用して拡張機能をインストールできます。
- ブラウザコンテンツリダイレクトが使用されている場合、HTML5ビデオリダイレクトポリシーは無効にする必要があります。
- ブラウザコンテンツリダイレクトは、ARMhf (ARM hard float) frameworkではサポートされていません。
- 信頼性の低いネットワーク、非常に変動の大きいネットワーク遅延、またはワイヤレスデバイスの範囲制限が原因で、ユーザーがセッションから切断されることがあります。現在、BCRにはこのようなシナリオに対する十分なフォールバックまたはレポートメカニズムがありません。
- BCRオーバーレイブラウザでは、ファイルをダウンロードしたり印刷したりすることはできません。
- シークレットモードまたはプライベートブラウジングモードは、ブラウザコンテンツリダイレクトではサポートされていません。

HDX™ ビデオ会議とWebカメラビデオ圧縮

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

> ウェブカメラは、HDXウェブカメラビデオ圧縮またはHDXプラグアンドプレイ汎用USBリダイレクトを使用して、仮想セッション内で実行されているアプリケーションによって使用できます。モードを切り替えるには、**Citrix Workspace™アプリ > 環境設定 > デバイス**を使用します。Citrixは、可能な限り常にHDXウェブカメラビデオ圧縮を使用することを推奨します。HDX汎用USBリダイレクトは、HDXビデオ圧縮とのアプリケーション互換性の問題がある場合、またはウェブカメラの高度なネイティブ機能が必要な場合にのみ推奨されます。パフォーマンスを向上させるために、CitrixはVirtual Delivery Agentに少なくとも2つの仮想CPUを搭載することを推奨します。

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

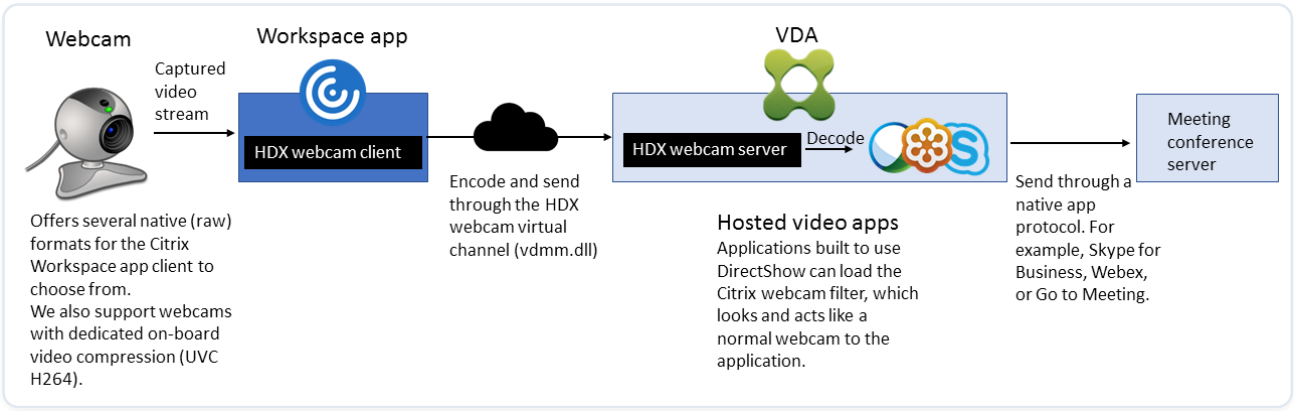
HDXウェブカメラビデオ圧縮

HDXウェブカメラビデオ圧縮は、**最適化された**ウェブカメラモードとも呼ばれます。この種類のウェブカメラビデオ圧縮は、H.264ビデオを仮想セッションで実行されているビデオ会議アプリケーションに直接送信します。VDAリソースを最適化するため、HDXウェブカメラ圧縮はウェブカメラビデオのエンコード、トランスコード、デコードを行いません。この機能はデフォルトで有効になっています。

サーバーからビデオ会議アプリへの直接ビデオストリーミングを無効にするには、VDAでレジストリキーを0に設定します。詳細については、レジストリで管理される機能のリストにあるウェブカメラビデオ圧縮を参照してください。

ビデオリソースをストリーミングするためのデフォルト機能を無効にすると、HDXウェブカメラビデオ圧縮は、クライアントオペレーティングシステムの一部であるマルチメディアフレームワークテクノロジーを使用して、キャプチャデバイスからのビデオをインターセプトし、トランスコードして圧縮します。キャプチャデバイスの製造元は、OSカーネルストリーミングアーキテクチャに接続するドライバーを提供します。

クライアントはウェブカメラとの通信を処理します。その後、クライアントはビデオを適切に表示できるサーバーにのみ送信します。サーバーはウェブカメラを直接処理しませんが、その統合によりデスクトップで同じエクスペリエンスが得られます。Workspaceアプリは、帯域幅を節約し、WANシナリオでの回復性を向上させるためにビデオを圧縮します。



HDXウェブカメラビデオ圧縮には、**マルチメディア会議**ポリシーを有効にする必要があります。このポリシーはデフォルトで有効になっています。

ウェブカメラがハードウェアエンコーディングをサポートしている場合、HDXビデオ圧縮はデフォルトでハードウェアエンコーディングを使用します。ハードウェアエンコーディングは、ソフトウェアエンコーディングよりも多くの帯域幅を消費する可能性があります。ソフトウェア圧縮を強制するには、クライアントのレジストリキーを編集します。詳細については、レジストリで管理される機能のリストにあるウェブカメラソフトウェア圧縮を参照してください。

HDXウェブカメラビデオ圧縮の要件

HDXウェブカメラビデオ圧縮は、Citrix Workspaceアプリの次のバージョンをサポートしています。

プラットフォーム	プロセッサー
Windows向けCitrix Workspaceアプリ	Windows向けCitrix Workspaceアプリは、XenAppおよびXenDesktop 7.17以降で32ビットおよび64ビットアプリのWebカメラビデオ圧縮をサポートしています。以前のバージョンでは、Windows向けCitrix Workspaceアプリは32ビットアプリのみをサポートしています。
Mac向けCitrix Workspaceアプリ	Mac向けCitrix Workspaceアプリ2006以降は、XenAppおよびXenDesktop 7.17以降で64ビットアプリのWebカメラビデオ圧縮をサポートしています。以前のバージョンでは、Mac向けCitrix Workspaceアプリは32ビットアプリのみをサポートしています。
Linux向けCitrix Workspaceアプリ	Linux向けCitrix Workspaceアプリは、仮想デスクトップ上で32ビットおよび64ビットの両方のアプリをサポートしています。

プラットフォーム	プロセッサー
Chrome向けCitrix Workspaceアプリ	一部のARM ChromebookはH.264エンコーディングをサポートしていないため、最適化されたHDX Webカメラビデオ圧縮を使用できるのは32ビットアプリのみです。

Media Foundationベースのビデオアプリケーションは、Windows 10以降およびWindows Server 2019以降でHDX Webカメラビデオ圧縮をサポートしています。詳細については、Knowledge Centerの記事CTX132764を参照してください。

その他のユーザーデバイス要件:

- サウンドを生成するための適切なハードウェア。
- DirectShow互換のWebカメラ（Webカメラのデフォルト設定を使用）。ハードウェアエンコーディング対応のWebカメラは、クライアント側のCPU使用率を削減します。
- HDX Webカメラビデオ圧縮の場合、可能であれば、カメラメーカーから入手したWebカメラドライバーをクライアントにインストールします。デバイスドライバーのインストールはサーバー上では不要です。

さまざまなWebカメラが異なるフレームレートを提供し、明るさやコントラストのレベルも異なります。Webカメラのコントラストを調整すると、アップストリームトラフィックを大幅に削減できます。Citrixは、初期機能検証のために以下のWebカメラを使用しています。

- Microsoft LifeCam VX モデル (2000、3000、5000、7000)
- クリエイティブ ライブ！カム オプティア プロ
- ロジクール クイックカム メッセンジャー
- ロジクール C600、C920
- HP デラックス ウェブカメラ

優先するビデオフレームレートを調整するには、クライアントでレジストリキーを編集します。詳しくは、レジストリで管理される機能の一覧にあるWebカメラビデオ圧縮フレームレートを参照してください。

高解像度Webカメラストリーミング

サーバー上のビデオ会議アプリケーションは、サポートされているフォーマットタイプに基づいてWebカメラのフォーマットと解像度を選択します。セッションが開始されると、クライアントはWebカメラ情報をサーバーに送信します。アプリケーションからWebカメラを選択します。

Webカメラとビデオ会議アプリケーションが高解像度レンダリングをサポートしている場合、アプリケーションは高解像度を使用します。すべてのWebカメラの解像度をサポートしています。

この機能には、Citrix Workspaceアプリ for Windows バージョン1808以降、またはCitrix Receiver for Windows バージョン4.10以降が必要です。

レジストリキーを使用して、この機能を無効または有効にできます。詳しくは、レジストリで管理される機能の一覧にある高解像度Webカメラストリーミングを参照してください。

メディアタイプのネゴシエーションが失敗した場合、HDXはデフォルトのVGA解像度（640 x 480 ピクセル）にフォールバックします。クライアントのレジストリキーを使用して、デフォルトの解像度を構成できます。カメラが指定された解像度をサポートしていることを確認してください。詳しくは、レジストリで管理される機能の一覧にある高解像度Webカメラ解像度を参照してください。

HDX Webカメラビデオ圧縮は、プラグアンドプレイの汎用USBリダイレクトと比較して帯域幅を大幅に少なく使用し、WAN接続でも良好に動作します。帯域幅を調整するには、クライアントでレジストリキーを設定します。詳しくは、レジストリで管理される機能の一覧にある高解像度Webカメラ帯域幅を参照してください。

ビット/秒単位で値を入力します。帯域幅を指定しない場合、ビデオ会議アプリケーションはデフォルトで350000 bpsを使用します。

HDXプラグアンドプレイ汎用USBリダイレクト

HDX plug-n-play 汎用 USB リダイレクト（アイソクロナス）は、**汎用**ウェブカメラモードとも呼ばれます。HDX plug-n-play 汎用 USB リダイレクトの利点は、シンクライアント/エンドポイントにドライバーをインストールする必要がないことです。USB スタックは仮想化されているため、ローカルクライアントに接続したものはすべてリモート VM に送信されます。リモートデスクトップは、ネイティブに接続したかのように動作します。Windows デスクトップは、ハードウェアとのすべてのやり取りを処理し、プラグアンドプレイロジックを実行して適切なドライバーを見つけます。ほとんどのウェブカメラは、ドライバーがサーバー上に存在し、ICA 経由で動作できる場合に機能します。汎用ウェブカメラモードは、非圧縮ビデオを USB プロトコルでネットワーク経由で送信するため、はるかに多くの帯域幅（毎秒数メガビット）を使用します。

Microsoft Teams の最適化 (新規)

Citrix® は、VDI 環境で Microsoft Teams のオーディオとビデオを最適化する 2 つの方法をサポートしています。Citrix HDX™ Optimization と、Microsoft が提供する Teams 用の新しい VDI ソ

リューションです。Classic Teams はサポート終了に達したため、このページで説明されている最適化アプローチは現在の Microsoft Teams クライアントに適用されます。

注:

Microsoft は、Windows エンドポイントにおける WebRTC ベースの Citrix HDX Optimization for Microsoft Teams の非推奨化を発表しました。以下の 2 つのマイルストーンが適用されます。

- October 1, 2026 - サポート終了: Microsoft または Citrix による公式サポートは終了します。
- April 1, 2027 - 提供終了: WebRTC ベースの最適化は機能しなくなります。レガシー最適化のための Citrix Studio ポリシーは適用されなくなります。

お客様は、Teams 向け新規 VDI ソリューションへの移行をお勧めします。この変更は Windows エンドポイントのみに影響します。macOS、Linux、ChromeOS、および HTML5 エンドポイントは影響を受けません。詳細については、Microsoft Blog を参照してください。

最適化アプローチ

- **Citrix HDX Optimization (MTOP)**: Citrix と Microsoft の組み合わせソリューションで、Citrix が所有する仮想チャネル (CTXMTOP) を使用します。メディアオフロードは、Citrix Workspace™ アプリの `HdxRtcEngine` によって処理されます。このソリューションは従来 MTOP と呼ばれています。
- **Teams 用の新しい VDI ソリューション**: Microsoft が所有および管理する新しい最適化で、Microsoft が所有する仮想チャネル (MSTEAMS、MSTEAM1、MSTEAM2) を使用します。Windows および Mac エンドポイントで利用できます。詳細については、Microsoft ドキュメントの Teams 用の新しい VDI ソリューション を参照してください。

主な違い

CITRIX HDX 最適化	TEAMS 用の新しい VDI ソリューション
最適化は Citrix と Microsoft の組み合わせソリューションであり、Citrix が所有する仮想チャネル (CTXMTOP) を使用します。	最適化ソリューションは Microsoft が所有および管理しており、Microsoft が所有する仮想チャネル (MSTEAMS、MSTEAM1、MSTEAM2) を使用します。
メディアオフロードは、Citrix Workspaceアプリに存在する`HdxRtcEngine`によって処理されます。	メディアオフロードは、WindowsおよびMacのエンドポイントでSlimCoreメディアエンジンによって処理されます。
Citrix Workspaceアプリのインストールを除いて、エンドポイントに追加のコンポーネントは不要です。	追加コンポーネント - **Teams VDI Plugin**は、さまざまな方法でエンドポイントに展開する必要があります。このプラグインは、SlimCoreメディアエンジンのダウンロードと更新を管理します。
エンドポイントプラットフォーム（Windows、macOS、Linux、ChromeOS）で利用可能です。	エンドポイントプラットフォーム（WindowsおよびMac）で利用可能です。
新機能は、CitrixとMicrosoftの間で連携して管理されます。	新機能はMicrosoftによって管理されます。ユーザーは、Citrix HDX最適化では利用できない一部の新機能にアクセスできます。
関連するコンポーネントに応じて、CitrixとMicrosoftの両方でサポートされます。お客様はCitrixまたはMicrosoftのいずれかにケースをオープンでき、必要に応じて適切なチームにリダイレクトされます。	Microsoftが所有およびサポートします。Citrixは、Citrix Workspaceアプリ、仮想チャネル許可リスト、プラグイン展開メカニズムなど、関連するCitrixコンポーネントをサポートします。

相互運用性およびローミング

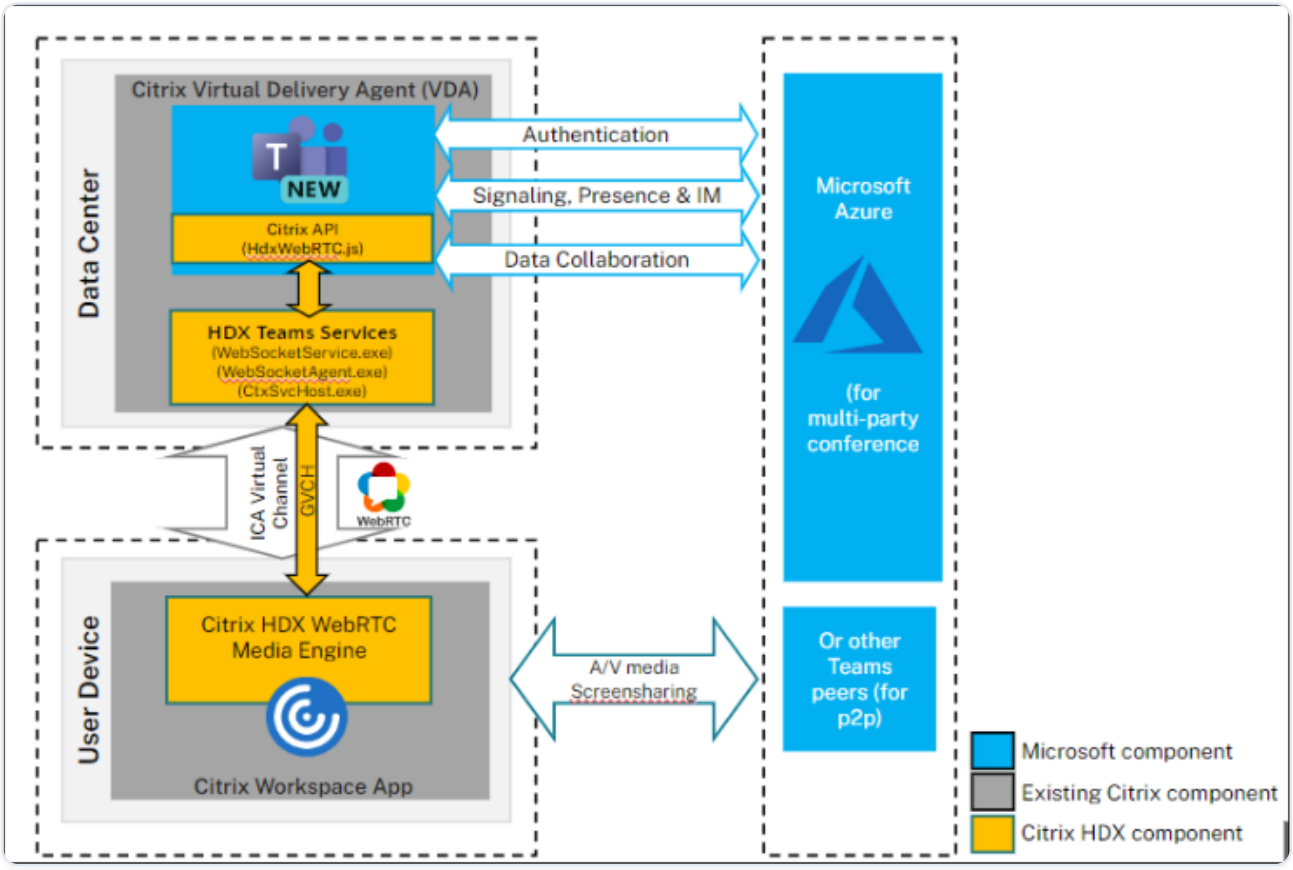
Citrix HDX最適化とTeams向け新しいVDIソリューションは並行して存在できますが、Teamsクライアントは一度にいずれか一方のみを使用します。

- Teamsアプリの起動時に、次の順序で最適化が選択されます。Teams向け新しいVDIソリューション、次にCitrix HDX最適化（WebRTC）、その後、標準のオーディオ/ビデオリダイレクト。

- Teams向けの新VDIソリューションが失敗した場合、TeamsはWebRTCではなく、標準のオーディオ/ビデオリダイレクトに直接フォールバックします。選択を再実行し、適切な最適化を選択するには、Teamsアプリの再起動が必要です。
- エンドポイント間のローミングはシームレスであり、Teamsアプリの再起動は不要です。これには、ユーザーがTeams向け新しいVDIソリューションをサポートするエンドポイントとサポートしないエンドポイントの間をローミングする場合も含まれます。

Citrix HDX™ の最適化

Citrix HDX (WebRTC Optimization) では、オフロードされたメディアの処理を担当するエンドポイント上のメディアエンジン (HdxRtcEngine) が Citrix Workspace™ app に組み込まれており、Citrix Workspace app をインストールすると、エンジンも自動的にインストールされます。



システム要件

このセクションでは、新しいTeamsクライアントをサポートするために必要な最小バージョンと推奨バージョンについて説明します。最小バージョンでは、重要なバグ修正や最新機能が利用できない場合があることに注意してください。最新の修正と機能で最高の体験を得るには、推奨バージョンを展開してください。

VDI オペレーティングシステム

詳細については、Microsoft ドキュメントに記載されている推奨事項を参照してください。

注:

- Windows Server 2016 はサポートされていません。Citrix は、それに応じてアップグレードを計画することをお勧めします。
- バージョンは頻繁に更新されるため、ここに記載されているバージョンはサポート終了となる可能性があります。したがって、異なるコンポーネントのサポートされているバージョンを使用していることを確認するために、Citrix Workspace app および Citrix Virtual Apps and Desktops の製品ライフサイクルページを参照してください。
- Citrix Virtual Apps and Desktops™ 1912 LTSR をご利用の場合、2024年12月にサポート終了となるため、アップグレードを計画することをお勧めします。

仮想配信エージェント (VDA)

最小バージョン	推奨バージョン
1912 LTSR CU8+; 2203 LTSR (任意のCU); 2212 CR	2203 LTSR CU5+ (または) 2402 LTSR およびそれ以降のCRバージョン

シトリックス ワークスペース アプリ

最小バージョン	推奨バージョン
ウィンドウズ 2203 エルティーエスアール (最新のCU); ウィンドウズ 2302 シーアール; リナックス 2207; マック 2302; クローム/HTML5 2301	ウィンドウズ 2402 エルティーエスアール; ウィンドウズ 2405 シーアール; リナックス 2405; マック 2405; クロームオーエス/HTML5 2405

展開

1. VDIに新しいTeamsクライアントをインストールします。詳細については、VDI向け新しいTeamsの展開を参照してください。
2. 新しいTeamsを最適化するために、VDAで以下のレジストリキーを設定します。
   - **場所**: `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`
   - **キー (REG_Multi_SZ)**: `ProcessWhitelist`
   - **値**: `msedgewebview2.exe`

> **注:**
>
> Citrix Virtual Apps and Desktops 2402 LTSR (または) Citrix Virtual Apps and Desktops 2203 LTSR CU5+ 以降では、`msedgewebview2.exe` レジストリエントリはデフォルトで許可リストに含まれているため、手動で構成する必要はありません。

3. Microsoft Teamsリダイレクトポリシーが有効になっていることを確認してください。このポリシーはデフォルトで有効になっています。
4. クライアント側で追加の設定は不要です。ウィザードの指示に従ってCitrix Workspaceアプリをインストールしてください。

App レイヤリング

新しいMicrosoft Teamsはインストール方法が変更され、C:\Program Files\WindowsApps にインストールされるようになりました。この変更をサポートするには、App Layeringバージョン2403.2以降を実行する必要があります。この修正を含むアップグレードディスクは、App Layeringダウンロード ページからダウンロードできます。

詳細については、App Layeringドキュメントを参照してください。

Citrix プロファイル管理

新しいMicrosoft Teamsのローミングを有効にする方法については、Citrix Profile Managementドキュメントを参照してください。Citrix Profile Managementの現在の最小バージョンガイダンスは、2402 LTSR (または) 2203 LTSR CU5+です。

ネットワークに関する考慮事項

新しいTeamsのネットワーク要件は、従来のTeamsと変わりません。したがって、従来のTeamsドキュメントのNetwork Requirementセクションを参照してください。

機能マトリックスとバージョンサポート

バージョンは頻繁に更新されるため、ここで言及されている一部の古いバージョンはサポート終了となる可能性があります。したがって、さまざまなコンポーネントのサポートされているバージョンを使用していることを確認するために、Citrix Workspace App および Citrix Virtual Apps and Desktops の製品ライフサイクルページを参照してください。

> **注:**

- ここで言及されているバージョンは、特定の機能がサポートされる最小バージョン、または新しいTeamsがサポートされる最小バージョンのいずれか高い方です。
- 最小バージョンセクションに記載されているCitrix Virtual Apps and Desktops 1912 LTSR CU8+は、2024年12月にサポート終了となるため、以下の表には記載されていません。ただし、それまでは引き続きサポート対象バージョンです。
- 最小Citrix Virtual Apps and Desktopsバージョンが `N/A` である機能は、VDA側からの変更を伴わないことを意味します。

機能	VDA (最小バージョン)	WINDOWS向けCITRIX WORKSPACEアプリ (最小バージョン)	MAC向けCITRIX WORKSPACEアプリ (最小バージョン)	LINUX向けCITRIX WORKSPACEアプリ (最小バージョン)	CHROMEOS向けCITRIX WORKSPACEアプリ (最小バージョン)
オーディオ/ビデオ (P2Pおよび会議)	2203 LTSR (任意のCU)、2212 CR	2203 LTSR 最新CU、2302 CR	2302	2207	2301
画面共有	2203 LTSR (任意のCU)、2212 CR	2203 LTSR 最新CU、2302 CR	2302	2207	2301
i. 画面インジケーターの赤い枠線	2203 LTSR (任意のCU), 2212 CR	2203 LTSR 最新CU, 2302 CR	2302	2207	なし
ii. キャプチャをDesktop Viewerに限定	2203 LTSR (任意のCU), 2212 CR	2203 LTSR 最新CU, 2302 CR	2302	2207	なし
iii. マルチモニター	2203 LTSR (任意の	2203 LTSR 最新 CU, 2302 CR	2302	2207	いいえ

機能	VDA (最小バージョン)	WINDOWS向けCITRIX WORKSPACEアプリ (最小バージョン)	MAC向けCITRIX WORKSPACEアプリ (最小バージョン)	LINUX向けCITRIX WORKSPACEアプリ (最小バージョン)	CHROMEOS向けCITRIX WORKSPACEアプリ (最小バージョン)
	CU), 2212 CR				
DTMF	N/A	2203 LTSR 最新 CU, 2302 CR	2302	2207	2301
プロキシサーバーのサポート	N/A	2203 LTSR 最新 CU, 2302 CR	2302	2207	2305
アプリ共有	2203 LTSR (任意の CU), 2212 CR	2203 LTSR 最新CU, 2302 CR	2302	2209	いいえ
ライブキャプション	N/A	2203 LTSR 最新CU, 2302 CR	2302	2207	2303
動的e911	N/A	2203 LTSR 最新のCU, 2302 CR	2302	2207	2301
コントロールを付与	N/A	2203 LTSR 最新のCU, 2302 CR	2302	2207	いいえ
コントロールを要求	N/A	2203 LTSR 最新のCU, 2302 CR	2302	2207	2303
マルチウィンドウ	2203 LTSR (任意の	2203 LTSR 最新CU、2302 CR	2302	2207	2303

機能	VDA (最小バージョン)	WINDOWS向けCITRIX WORKSPACEアプリ (最小バージョン)	MAC向けCITRIX WORKSPACEアプリ (最小バージョン)	LINUX向けCITRIX WORKSPACEアプリ (最小バージョン)	CHROMEOS向けCITRIX WORKSPACEアプリ (最小バージョン)
	CU)、2212 CR				
会議の文字起こし	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新CU、2302 CR	2302	2207	2303
背景のぼかし	2203 LTSR (任意の CU), 2212 CR	2203 LTSR 最新CU, 2302 CR	2302	2212	2303
スクリーン共有 (アプリ保護あり)	2203 LTSR (任意の CU), 2212 CR	2402 LTSR, 2309.1 CR	2308	2311	いいえ
シマルキャスト	2203 LTSR (任意の CU), 2212 CR	2402 LTSR, 2305 CR	2305	2305	2312
セカンダリリンガー	2203 LTSR (任意の CU)、2212 CR	2402 LTSR、2307.1 CR	2308	2308	2312
システムオーディオを共有	2203 LTSR (任意の CU)、2212 CR	2402 LTSR、2403 CR	2405	2402	なし

トラブルシューティングとその他の考慮事項

New Teams については、CTX253754、Microsoft Teams のトラブルシューティング を参照してください。New Teams に関連する最新情報については、CTX585013 を参照してください。

既知の制限事項

Citrix Workspaceアプリの制限事項

- HID サポート - 通話の応答と終了はサポートされていません。音量の上げ下げはサポートされています。
- ユーザーは、VDA でスニッピングツールを使用している間は、Microsoft Teams のコンテンツのスクリーンショットを撮ることができません。ただし、クライアント側でスニッピングツールを使用すると、コンテンツをキャプチャできます。
- システムオーディオ共有の制限事項
  - RAVE および BCR リダイレクトされたアプリまたはタブで画面を共有している場合、この機能を使用してオーディオを共有することはできません。
  - この機能は公開デスクトップでのみサポートされています

VDA の制限事項

- 公開 (シームレス) アプリケーションとしての New Teams はサポートされていません
  - CVAD 2402 LTSR、2203 LTSR CU5 以降で修正済み
- Citrix Workspaceアプリの「高DPI」設定を「はい」に構成すると、リダイレクトされたビデオウィンドウがずれて表示されます。この制限は、モニターのDPIスケーリング係数が100%を超えて設定されている場合に発生します。
- Microsoft Teams 2.1 は、一度に 1 つの Web カメラのリダイレクトのみをサポートします。ただし、シングルセッション VDA での複数 Web カメラのリダイレクトやプラグアンドプレイ (PnP) Web カメラのリダイレクトはサポートしていません。

Citrix WorkspaceアプリとVDAに関する制限事項

- 最適化された通話の音量は、クライアントマシンの音量バーを使用してのみ制御できます。VDA では制御できません。

Microsoftからの制限事項の詳細については、VDIでサポートされていない機能を参照してください。

Teams 向け新しい VDI ソリューション

注：

Teams 向け新しい VDI ソリューションは現在、Citrix® 上の Windows および Mac エンドポイントで一般提供されています。このソリューションには、最小バージョンの Microsoft Teams が必要です。「システム要件」を参照してください。

Teams 向け新しい VDI ソリューションでは、Microsoft は Citrix Virtual Channel SDK を使用してカスタム仮想チャネルを構築します。エンドポイントでは、メディアは `HdxRtcEngine` ではなく Microsoft メディアエンジン (SlimCore) にオフロードされます。カスタム仮想チャネルは、VDA 上の Teams とエンドポイント上のメディアエンジン間の通信を伝送します。

注：

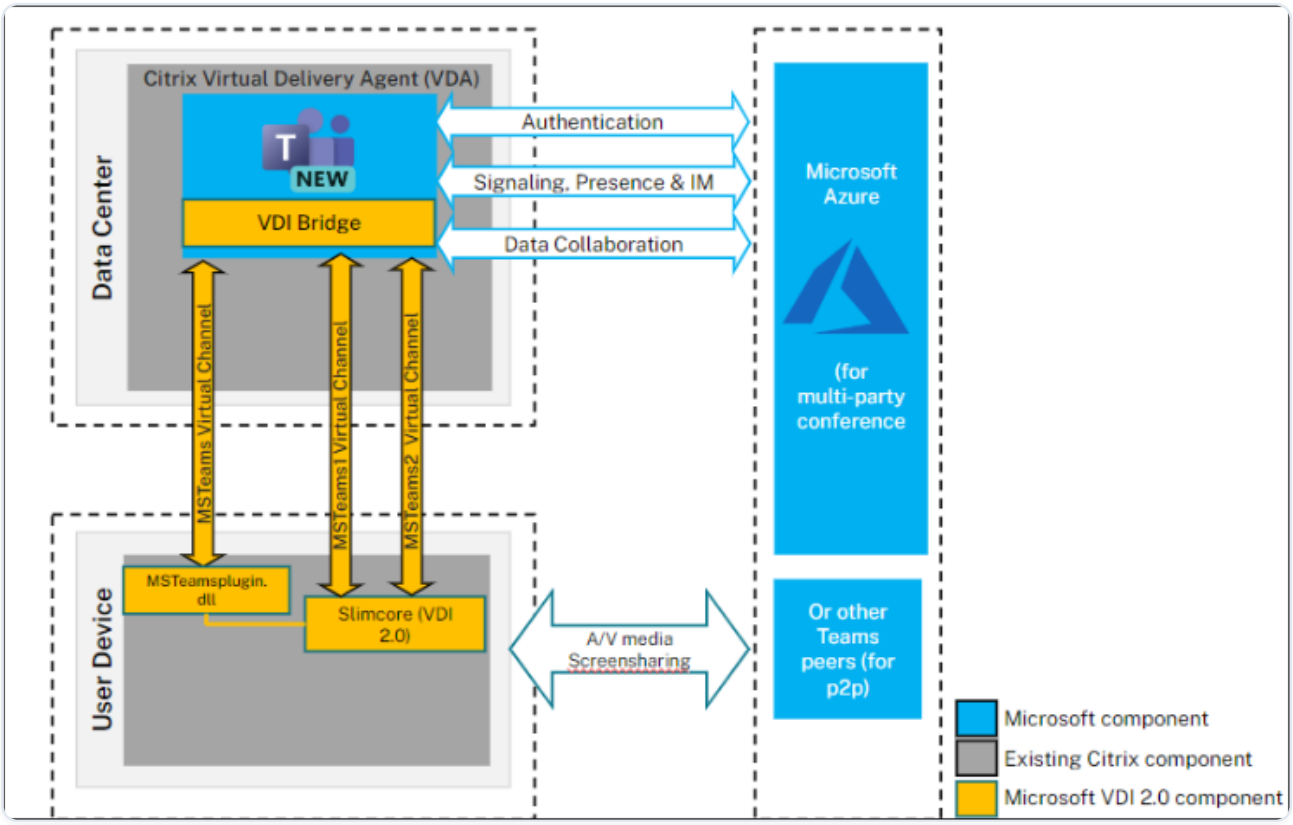
Microsoft は、Windows エンドポイントにおける Microsoft Teams 向け WebRTC ベースの Citrix HDX™ 最適化の非推奨を発表しました。2つのマイルストーンが適用されます。

- October 1, 2026 - サポート終了: MicrosoftまたはCitrixによって公式にサポートされなくなります。
- April 1, 2027 - 提供終了: WebRTCベースの最適化は機能しなくなります。レガシー最適化のためのCitrix Studioポリシーは適用されなくなります。

お客様は、Teams 向け新しい VDI ソリューションへの移行をお勧めします。この変更は Windows エンドポイントのみに影響します。macOS、Linux、ChromeOS、および HTML5 エンドポイントは影響を受けません。詳細については、「Microsoft Blog」を参照してください。

このソリューションは Microsoft が所有および管理しています。Citrix は、関連する Citrix コンポーネント（Citrix Workspace™ アプリ、仮想チャネルの許可リスト、およびこのページで説明されているプラグイン展開メカニズム）をサポートします。Microsoft が所有するアー

キテクチャと詳細については、Microsoft ドキュメントの「Teams 向け新しい VDI ソリューション」を参照してください。



システム要件

このセクションでは、Teams 向け新しい VDI ソリューションをサポートするために必要な最小バージョンと推奨バージョンをリストします。最小バージョンでは、一部の重要なバグ修正や最新機能が利用できない場合があります。最高の体験を得るには、推奨バージョンを展開してください。

仮想配信エージェント (VDA)

注：

2203 LTSR CU2以前、または2303 CR以前をご利用の場合は、これらのバージョンの制限を理解し、アップグレードを計画するためにCTX682593を参照してください。

最小バージョン	推奨バージョン
2203 LTSR CU3; 2305 CR	2203 LTSR CU5+; 2402 LTSR およびそれ以降のCR

Windows版 Citrix Workspaceアプリ

最小バージョン	推奨バージョン
2203 LTSR (最新 CU); 2302 CR	2402 LTSR; 2405 CR またはそれ以降

Mac向けCitrix Workspaceアプリ

最小バージョン	推奨バージョン
2508.10	2607 またはそれ以降

MacエンドポイントにはmacOS 14、15、または26が必要です。macOS 26にはCitrix Workspaceアプリ2511以降が必要です。Citrix Workspaceアプリ for Mac 2508.10では、プラグインを手動でインストールする必要があります。Citrix Workspaceアプリ、クライアントアプリ管理、または仮想チャネルプラグインマネージャーを介してプラグインをインストールするオプションは、Citrix Workspaceアプリ for Mac 2603から利用できます。

最小Microsoft Teamsバージョン、エンドポイントOS要件、およびハードウェア要件については、Microsoftドキュメントを参照してください。

コンポーネント

- 新しいTeams `vdiBridge`：Teamsにバンドルされているサーバー側の仮想チャネルモジュール。
- カスタム仮想チャネル（VC）：Microsoft Teamsが所有するカスタムVC。
- プラグイン：クライアント側のVC DLL。メディアエンジンのダウンロードとクリーンアップを担当します。
- メディアエンジン（SlimCore）：MicrosoftによってMSIXパッケージとして提供される、オペレーティングシステム固有のメディアエンジン。

展開

1. 前提条件に記載されているMicrosoft Teamsバージョンがあることを確認してください。

2. **仮想チャネル許可リスト**ポリシーを構成して、Microsoft Teams仮想チャネルを許可します。これらのチャネルにより、Teamsクライアントはクライアント側のプラグインに接続できます。詳細については、仮想チャネルセキュリティを参照してください。

   このソリューションには、3つのカスタム仮想チャネルが必要です。ワイルドカードを使用して、`ms-teams.exe`実行可能ファイルとカスタム仮想チャネルを許可します。

   ```
   MSTEAMS,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

   MSTEAM1,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

   MSTEAM2,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe
   ```

   注：

   - VDA 2603以降では、これら3つの仮想チャネルがデフォルトで許可されます。これらのバージョンでは、Studioポリシーの構成は不要です。
   - 仮想チャネル許可リストポリシーのワイルドカードは、CVAD 2203 LTSR CU2以降、またはCitrix Virtual Apps and Desktops™ 2206 CR以降で利用できます。
   - ポリシーを有効にするには、VDAマシンを再起動する必要があります。
   - MSTeamsのインストールパスはMSIXアプリケーションであるため変更されるため、ワイルドカードが必要です。上記に示されている正確な行を許可します。

3. このソリューションは、Citrixポリシーではなく、Microsoft Teams側のポリシーによって制御されます。デフォルトで有効になっています。特定のユーザーグループに対して有効または無効にするには、Microsoftのドキュメントを参照してください。
4. エンドポイントにTeamsプラグインを展開します。Teamsプラグインをインストールするオプションを参照してください。
5. メディアエンジンのステージングと登録、およびMSIXのインストールをブロックできるグループポリシーについては、Microsoftのドキュメントを参照してください。

Teamsプラグインをインストールするオプション

インストール方法に関わらず、プラグインはエンドポイントのCitrix Workspaceアプリの場所に配置されます。

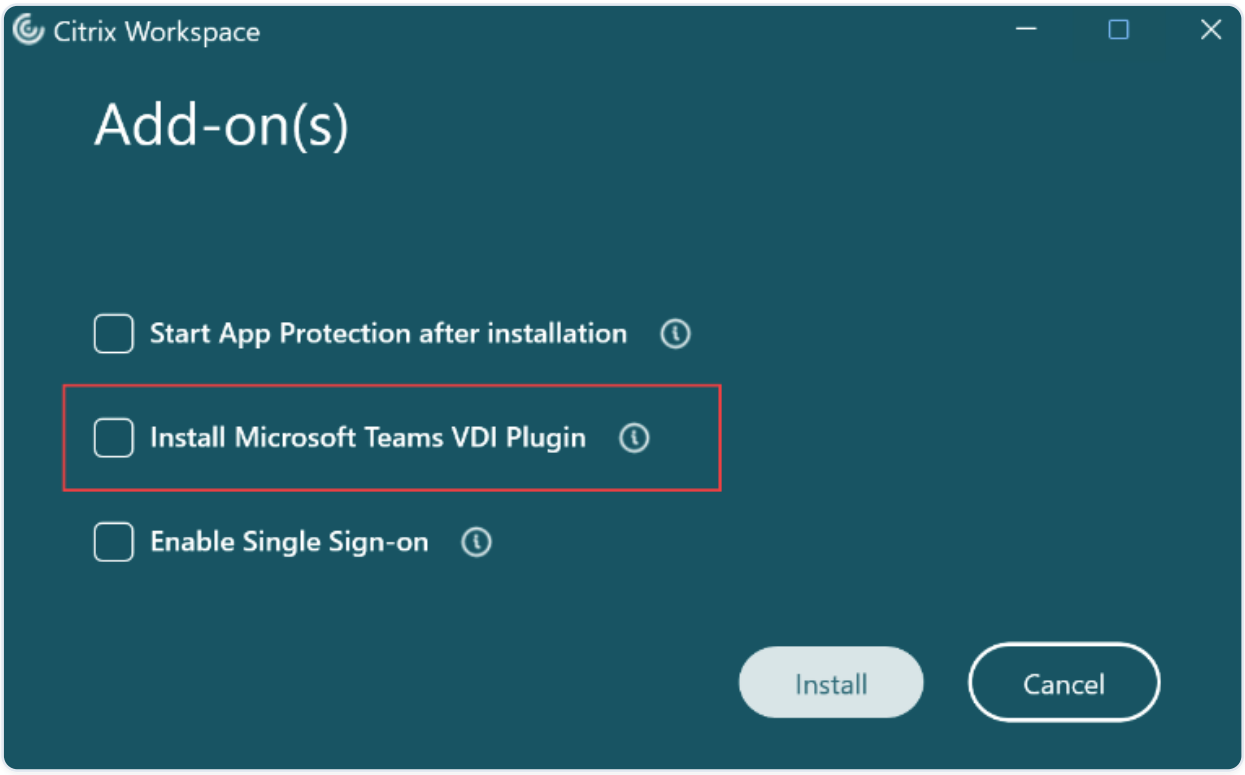
- Windows (`MsTeamsPluginCitrix.dll`): 64ビット `C:\Program Files (x86)\Citrix\ICA Client`; 32ビット `C:\Program Files\Citrix\ICA Client`
- Mac: `/Applications/Utilities/MsTeamsVdi.Plugin.app`

注:

- Windowsでは、仮想チャネルが正しく開くように、Citrix Workspaceアプリを管理者モードでインストールしてください。Citrix Workspaceアプリのユーザーごとのインストールはサポートされていません。
- Microsoft StoreからCitrix Workspaceアプリがインストールされている場合、Microsoft Teams VDIプラグインはサポートされません。
- エンドポイントにCitrix Workspaceアプリが見つからない場合、プラグインのインストールは停止します。
- Windowsでは、プラグインとCitrix Workspaceアプリは同じアーキテクチャである必要があります。32ビットのCitrix Workspaceアプリは64ビットのプラグインをロードできません。
- プラグインはアップグレードまたは修復できますが、ダウングレードはできません。また、アクティブなセッションがない場合にのみ可能です。

オプション1：Citrix Workspaceアプリのインストールによる方法

- **Windows:** 新規インストールまたは手動アップグレード中に、**アドオン**ページで**Microsoft Teams VDI プラグインのインストール**を選択します。Citrix Workspaceアプリ for Windows 2508以降では、このオプションはデフォルトで選択されています。インストールをスキップするには、このチェックを外します。アップグレードでは、以前の選択が記憶されます。



`/InstallMSTeamsPlugin` スイッチを使用してコマンドラインからインストールすることもできます。たとえば、`CitrixWorkspaceApp.exe /InstallMSTeamsPlugin=Y` はプラグインをインストールし、`/InstallMSTeamsPlugin=N` はインストールを阻止します。

新規インストールの場合、最小要件はCitrix Workspaceアプリ for Windows 2402 LTSRです。インプレースアップグレードの場合、最小要件はCitrix Workspaceアプリ for Windows 2405 CRです。最新の詳細については、サードパーティ製プラグインのインストールを参照してください。

- **Mac:** Citrix Workspaceアプリのインストール中にプラグインをインストールするオプションは、Citrix Workspaceアプリ for Mac 2603以降で利用可能であり、ユーザーによる操作が必要です。Citrix Workspaceアプリ for Mac 2607では、プラグインがデフォルトで自動的にインストールされます。Citrix Workspaceアプリ for Mac 2508.10では、プラグインを手動でインストールしてください。オプション2: プラグインを直接ダウンロードするを参照してください。

オプション2: プラグインを直接ダウンロードする

- **Windows:** MSIをダウンロードし、SCCMやIntuneなどのツールを使用して、サポートされている任意のCitrix Workspaceアプリのバージョンに展開します。
  - 32ビット版Citrix Workspaceアプリ: aka.ms/plugin
  - 64ビット版Citrix Workspaceアプリ: aka.ms/plugin_x64
  - ArmベースのCitrix Workspaceアプリ: aka.ms/plugin_arm64

- **Mac:** aka.ms/macpluginからプラグインをダウンロードし、JAMFなどのツールを使用して展開します。

オプション3: クライアントアプリ管理 (旧Global App Configurationサービス)

クライアントアプリ管理 (旧Global App Configurationサービス、またはGACS) は、管理対象および非管理対象のエンドポイントのアプリ設定を管理し、Teamsプラグインをエンドポイント全体に展開できます。Macでは、Citrix Workspaceアプリ for Mac 2603以降が必要です。Microsoft Teams VDI プラグイン管理を参照してください。

オプション4: 仮想チャネルプラグインマネージャー

仮想チャネルプラグインマネージャーは、Teams向けの新VDIソリューションを含む、エンドポイントコンポーネントを必要とするアプリケーションのために、クライアントエンドポイント全体にプラグインを展開します。VDAで実行されているアプリケーションを検出し、ユーザーにエンドポイントへのプラグインのインストールを促します。管理者はBYODシナリオでこれを使用できます。Macでは、Citrix Workspaceアプリ for Mac 2603以降が必要です。仮想チャネルプラグインマネージャーを参照してください。

プラグインの更新シナリオ

オプション1、3、または4を介してプラグインがインストールされている場合、CitrixはTeamsプラグインの更新をシームレスに処理します。プラグインが手動でインストールされている場合（オプション2）、Citrixは更新を処理しません。

- プラグインの自動更新のために、Citrix Workspaceアプリの自動更新がオンになっていることを確認してください。
- Citrix Workspaceアプリ for Windows 2405以降であることを確認してください。Citrix Workspaceアプリ for Windows 2508以降では、Citrix Workspaceアプリが自動更新されるとプラグインが自動的にインストールされます。
- Citrixはプラグインのアンインストールを処理しません。必要に応じて、プラグインを個別にアンインストールしてください。

注:

CitrixはTeamsプラグインの更新を処理しますが、メディアエンジンは処理しません。Microsoftがメディアエンジンを提供し、更新します。

Citrix公開アプリとしてのTeams

Citrix Virtual Appsアプリケーションとして公開されたTeamsは、必要なすべてのコンポーネントが最小バージョンを満たしている場合、このソリューションで最適化できます。必要なバージョンと既知の制限については、Microsoft ドキュメントを参照してください。

相互運用性とローミング

Teams向けの新VDIソリューションとCitrix HDX最適化がどのように相互運用され、ローミングがどのように動作するかについては、Microsoft Teamsの最適化 を参照してください。

ネットワークに関する考慮事項

Microsoftドキュメントのネットワークに関する考慮事項 を参照してください。

機能サポート

機能セットと実装はMicrosoftが所有しています。Microsoftドキュメントの機能リスト を参照してください。

トラブルシューティング

Microsoft Teams クライアントは最適化ステータスを報告し、最適化に失敗した場合はエラーコードを報告します。これらのステータスインジケーターとエラーコードは Microsoft によって定義されています。完全なリストとエンドツーエンドのトラブルシューティングについては、Microsoft ドキュメントの Teams の新しい VDI ソリューションのトラブルシューティング を参照してください。

Citrix Monitor は、このソリューションの最適化の状態を可視化します。セッションの詳細では、セッション トポロジ ビューにアプリケーションが最適化されているかどうかが表示され、プラグイン マネージャー、プラグインとそのバージョン、仮想チャネルの状態、仮想チャネル許可リストのステータスなど、不足しているコンポーネントにフラグが付けられます。詳細については、リアルタイム通信の最適化の可視性 を参照してください。

一部の Microsoft エラーコードは、Citrix 側の構成を指しています。一般的な Citrix の確認事項:

- Teams クライアントがカスタム仮想チャネルがブロックされていると報告した場合 (Microsoft エラー 2003)、仮想チャネル許可リストに MSTEAMS、MSTEAM1、および MSTEAM2 が含まれていることを確認してください。
- Teams クライアントがプラグインが検出されないと報告した場合 (Microsoft エラー 2000)、プラグインがインストールされ、ロードされていることを確認してください。Process Explorer で `wfica32.exe` を選択し、下部ペインを表示して、DLL タブで `MsTeamsPluginCitrix.dll` を確認します。

- Teams クライアントがサポートされていない Citrix Workspace アプリのバージョンを報告した場合 (Microsoft エラー 2004)、サポートされているバージョンにアップグレードしてください。システム要件 を参照してください。

既知の制限事項

機能と実装は Microsoft が所有しています。Microsoft ドキュメントの 既知の問題 を参照してください。

Microsoft Teams (Classic) の最適化

> **注：**

> 新しいMicrosoft Teams 2.1はVDAで一般提供されるようになりました。このMicrosoft Teamsバージョンは、WebRTC (VDI 1.0) を使用したCitrix Microsoft Teams最適化と互換性があります。

> Citrix Virtual Apps and Desktops 2402以降、`msedgewebview2.exe`レジストリエントリはデフォルトで許可リストに含まれるため、手動で構成する必要はありません。

> 公開アプリケーションは、新しいMicrosoft Teamsでサポートされるようになりました。

> Citrixは、Citrix Virtual Apps and Desktops™およびCitrix Workspace™アプリを使用して、デスクトップベースのMicrosoft Teams向けに最適化を提供します。デフォルトでは、必要なすべてのコンポーネントをCitrix WorkspaceアプリとVirtual Delivery Agent (VDA) にバンドルしています。

Microsoft Teamsの最適化には、VDA側のHDX™サービスと、コマンドを受信するためにMicrosoft Teamsホスト型アプリとインターフェイスするためのAPIが含まれています。これらのコンポーネントは、Citrix Workspaceアプリ側のメディアエンジンへの制御仮想チャネル (CTXMTOP) を開きます。エンドポイントはマルチメディアをローカルでデコードして提供し、Citrix Workspaceアプリウィンドウをホストされ たMicrosoft Teamsアプリに戻します。

認証とシグナリングは、他のMicrosoft Teamsサービス (チャットやコラボレーションなど) と同様に、Microsoft Teamsホスト型アプリでネイティブに行われます。オーディオ/ビデオのリダイレクトはこれらに影響しません。

`CTXMTOP`はコマンドおよび制御仮想チャネルです。これは、Citrix WorkspaceアプリとVDAの間でメディアが交換されないことを意味します。

クライアントフェッチ/クライアントレンダリングのみが利用可能です。

このビデオデモンストレーションでは、Citrix仮想環境でMicrosoft Teamsがどのように機能するかを説明します。



Microsoft Teamsのインストール

CitrixとMicrosoftは、Microsoft Teamsの最新バージョンを使用し、常に最新の状態に保つことを推奨しています。 現在のバージョンのリリース日から90日以上古いリリース日のMicrosoft Teamsデスクトップアプリのバージョンはサポートされていません。 サポートされていないMicrosoft Teamsデスクトップアプリのバージョンでは、ユーザーにブロックページが表示され、アプリの更新が要求されます。

最新の利用可能なバージョンについては、Microsoft Teamsアプリ（デスクトップおよびMac）の更新履歴を参照してください。

Microsoft Teams のマシン全体へのインストール ガイドライン に従うことをお勧めします。`AppData` に Microsoft Teams をインストールする .exe インストーラーの使用は避けてください。代わりに、コマンドラインから `ALLUSER=1` フラグを使用して `C:\Program Files (x86)\Microsoft\Teams` にインストールしてください。

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1 ALLUSERS=1
```

この例では、`ALLUSERS=1` パラメーターも使用します。このパラメーターを設定すると、Microsoft Teams マシン全体インストーラーが **コントロール パネル** の **プログラムと機能** に表示されます。また、コンピューターのすべてのユーザーに対して、Windows の設定の **アプリと機能** にも表示されます。すべてのユーザーは、管理者資格情報があれば Microsoft Teams をアンインストールできます。

`ALLUSERS=1` と `ALLUSER=1` の違いを理解することが重要です。`ALLUSERS=1` パラメーターは、非 VDI 環境と VDI 環境の両方で使用できます。`ALLUSER=1` パラメーターは、VDI 環境でのみ使用して、マシンごとのインストールを指定します。

`ALLUSER=1` モードでは、新しいバージョンがリリースされても Microsoft Teams アプリケーションは自動更新されません。このモードは、Windows Server または Windows 10 のランダム/プールされたカタログからのホストされた共有アプリやデスクトップなど、非永続的な環境に推奨され

ます。詳細については、「MSI を使用した Microsoft Teams のインストール (VDI インストール セクション)」を参照してください。

Windows 10 の専用永続 VDI 環境があるとします。Microsoft Teams アプリケーションを自動更新し、`Appdata/Local` の下にユーザーごとに Microsoft Teams をインストールすることを希望する場合、`.exe` インストーラーまたは `ALLUSER=1` なしの MSI を使用します。

> 「**注:**」:
>
> Citrix では、ゴールデン イメージに Microsoft Teams をインストールする前に VDA をインストールすることをお勧めします。`ALLUSER=1` フラグを有効にするには、このインストール順序が必要です。VDA をインストールする前に仮想マシンに Microsoft Teams をインストールした場合は、Microsoft Teams をアンインストールして再インストールしてください。

リモート PC アクセスの場合

Citrix では、VDA のインストール後に Microsoft Teams バージョン 1.4.00.22472 以降をインストールすることをお勧めします。そうしないと、Microsoft Teams が VDA を期待どおりに検出するために、サインアウトして再度サインインする必要があります。バージョン 1.4.00.22472 以降には、VDA 検出のために Microsoft Teams の起動時およびサインイン時に実行される拡張ロジックが含まれています。これらのバージョンには、アクティブなセッション タイプ識別 (HDX、RDP、またはクライアント マシンにローカル接続) も含まれています。ローカル接続している場合、以前のバージョンの Microsoft Teams では、特定の機能や UI 要素を検出して無効にできない場合があります。たとえば、ブレイクアウトルーム、会議やチャットのポップアウトウィンドウ、会議のリアクションなどです。

> 「**重要:**」:
>
> ローカル セッションから HDX セッションにローミングし、Microsoft Teams がバックグラウンドで開いたまま実行されている場合、HDX で正しく最適化するには、Microsoft Teams を終了して再起動する必要があります。 逆に、最適化された HDX セッションを介して Microsoft Teams をリモートで使用する場合は、HDX セッションを切断し、デバイスで同じ Windows セッションにローカルで再接続します。オフィスで作業する場合は、Microsoft Teams がリモート PC アクセスの状態 (HDX またはローカル) を正しく検出できるように、Microsoft Teams を再起動する必要があります。Microsoft Teams は、アプリの起動時にのみ VDI モードを評価でき、バックグラウンドで既に実行されている間は評価できないためで

> す。再起動しないと、Microsoft Teams はポップアウト ウィンドウ、ブレイクアウトルーム、会議のリアクションなどの機能を読み込めない場合があります。

App Layeringの場合

Citrix App Layering を使用して VDA と Microsoft Teams のインストールを異なるレイヤーで管理する場合、コマンドラインから `ALLUSER=1` フラグを使用して Microsoft Teams をインストールする前に、Windows VDA 上にレジストリ キーを作成する必要があります。詳細については、「マルチメディア」の「*Citrix App Layering を使用した Microsoft Teams の最適化*」セクションを参照してください。

プロファイル管理の推奨事項

Windows Server およびプールされた VDI Windows 10 環境には、マシン全体のインストーラーを使用することをお勧めします。

コマンドラインから MSI に **ALLUSER=1** フラグが渡されると (マシン全体のインストーラー)、Microsoft Teams アプリは `C:\Program Files (x86)` (~300 MB) にインストールされます。このアプリは、ログに `AppData\Local\Microsoft\TeamsMeetingAddin` を、ユーザー固有の設定、ユーザーインターフェイスの要素のキャッシュなどに `AppData\Roaming\Microsoft\Teams` (~600〜700 MB) を使用します。

> **重要:**

> **ALLUSER=1**フラグを渡さない場合、MSIはTeams.exeインストーラーと`setup.json`を`C:\Program Files (x86)\Teams Installer`に配置します。レジストリキー（TeamsMachineInstaller）は`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`の下に追加されます。

> その後のユーザーログオンで、代わりに **AppData** に最終インストールがトリガーされます。

マシン全体のインストーラー

以下は、任意の Windows Server 64 ビット VM に Microsoft Teams マシン全体のインストーラーをインストールすることによって作成されるフォルダー、デスクトップショートカット、およびレジストリの例です。

フォルダー:

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

デスクトップショートカット:

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

レジストリ:

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- 名前: `Teams`
- 種類: `REG_SZ`
- 値: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> **注:**
>
> レジストリの場所は、基盤となるオペレーティングシステムとビット数によって異なります。

推奨事項

- Microsoft Teamsのレジストリキーを削除して自動起動を無効にすることをお勧めします。これにより、同時に発生する多数のログオン（たとえば、勤務開始時など）によるVMのCPUスパイクを防ぐことができます。
- 仮想デスクトップにGPU/vGPUがない場合は、パフォーマンスを向上させるために、Microsoft Teamsの**設定**で**GPUハードウェアアクセラレーションを無効にする**を設定することをお勧めします。この設定 (`"disableGpu":true`) は、 `desktop-config.json` の `%Appdata%\Microsoft\Teams` に保存されています。ログオンスクリプトを使用してそのファイルを編集し、値を `true` に設定できます。
- Citrix Workspace Environment Management™ (WEM) を使用している場合は、Microsoft Teams のプロセッサ消費を管理するために、**CPUスパイク保護**を有効にしてください。

ユーザーごとのインストーラー

`.exe` インストーラーを使用する場合、インストールプロセスは異なります。すべてのファイルはAppDataに配置されます。

フォルダー:

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

デスクトップショートカット:

`C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe"`

レジストリ:

`HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

ベストプラクティス

ベストプラクティスの推奨事項は、ユースケースシナリオに基づいています。 非永続的なセットアップでMicrosoft Teamsを使用する場合、効率的なMicrosoft Teamsランタイムデータの同期にはプロファイルキャッシュマネージャーが必要です。プロファイルキャッシュマネージャーを使用すると、ユーザーセッション中に適切なユーザー固有の情報がキャッシュされます。たとえば、ユーザー固有の情報には、ユーザーデータ、プロファイル、設定が含まれます。これら2つのフォルダーのデータを同期します。

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

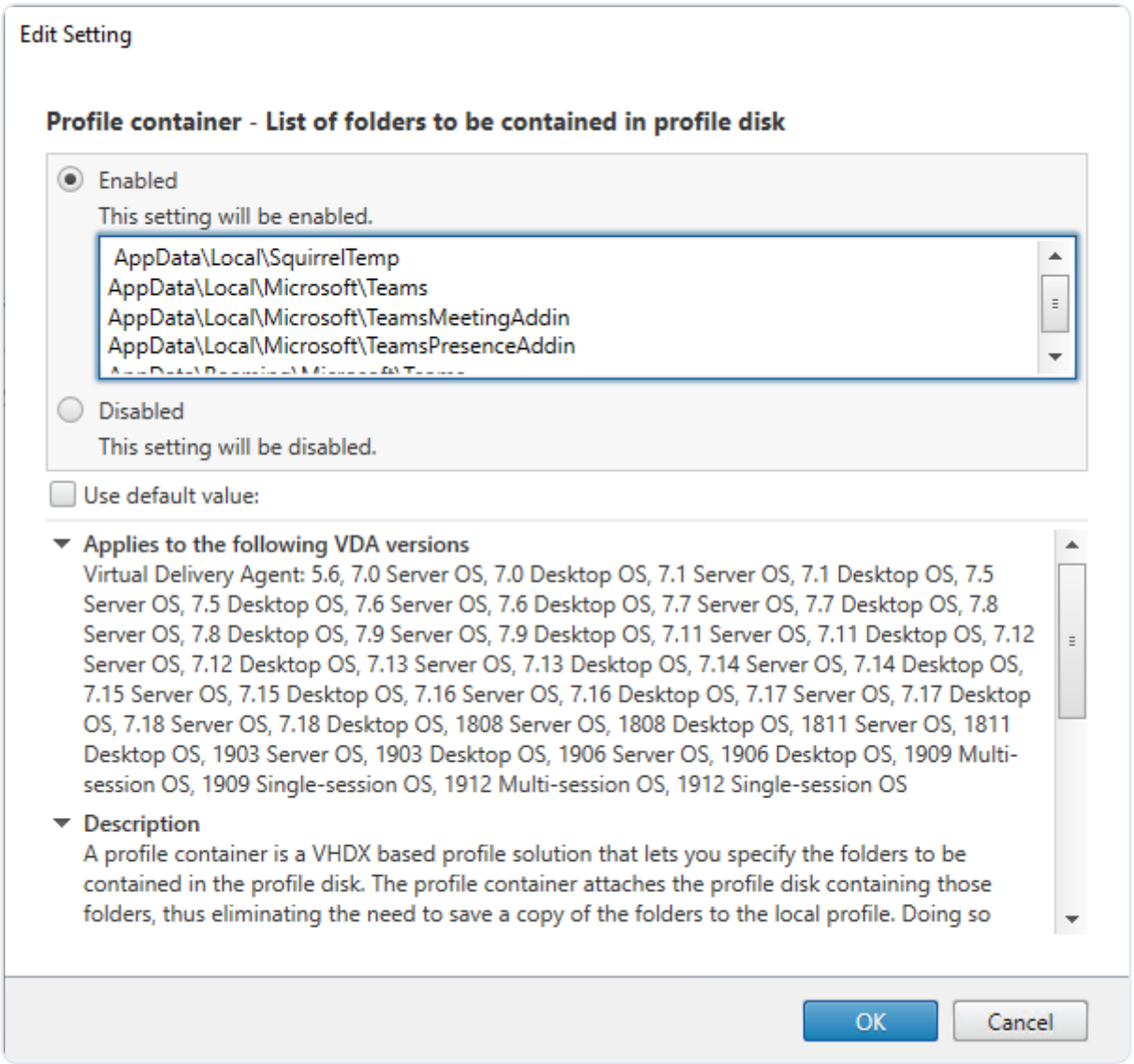
非永続的なセットアップにおけるMicrosoft Teamsのキャッシュコンテンツ除外リスト

Microsoft ドキュメントに記載されているように、Microsoft Teams のキャッシュフォルダーからファイルとディレクトリを除外します。この操作により、ユーザーのキャッシュサイズを削減し、非永続的セットアップをさらに最適化できます。

ユースケース：シングルセッションシナリオ

このシナリオでは、エンドユーザーは一度に1つの場所でMicrosoft Teamsを使用します。同時に2つのWindowsセッションでMicrosoft Teamsを実行する必要はありません。一般的な仮想デスクトップ展開では、各ユーザーに1つのデスクトップが割り当てられ、Microsoft Teamsは仮想デスクトップに1つのアプリケーションとして展開されます。 Citrix Profileコンテナを有効にし、ユーザーごとのインストーラーにリストされているユーザーごとのディレクトリをコンテナにリダイレクトすることをお勧めします。

1. ゴールデンイメージにMicrosoft Teamsのコンピューター全体インストーラー (**ALLUSER=1**) を展開します。
2. Citrix Profile Managementを有効にし、適切な権限でユーザープロファイルストアを設定します。
3. 次のProfile Managementポリシー設定を有効にします: **ファイルシステム > 同期 > プロファイルコンテナ – プロファイルディスクに含めるフォルダーのリスト。**



この構成内のすべてのユーザーごとのディレクトリを一覧表示します。これらの設定は、Citrix Workspace Environment Management (WEM) サービスを使用して構成することもできます。

4. 設定を適切なデリバリーグループに適用します。
5. 展開を検証するためにログインします。

システム要件

推奨される最小バージョン - Delivery Controller (DDC) 1906.2

以前のバージョンを使用している場合は、Microsoft Teamsの最適化を有効にするを参照してください:

サポートされているオペレーティングシステム:

- Windows Server 2022、2019、2016、2012R2 StandardおよびDatacenterエディション、ならびにServer Coreオプション

最小バージョン - Virtual Delivery Agents (VDA) 1906.2

サポートされているオペレーティングシステム:

- ウィンドウズ 11
- Windows 10 64-bit、バージョン1607以降。VMホスト型アプリは、Windows 2109.1以降のCitrix Workspaceアプリでサポートされています。
- Windows Server 2022、2019、2016、および2012 R2 (Standard および Datacenter エディション)

要件:

- BCR_x64.msi - Microsoft Teamsの最適化コードを含み、GUIから自動的に起動するMSI。VDAインストールのコマンドラインインターフェイスを使用している場合でも、これを除外しないでください。

推奨バージョン – Windows向けCitrix Workspaceアプリ最新CR、最小バージョン – Windows向けCitrix Workspaceアプリ1907

- ウィンドウズ 11。
- Windows 10 (32ビット版および64ビット版、Embedded版を含む) (Windows 7のサポートはバージョン2006で終了) (Windows 8.1のサポートはバージョン2204.1で終了)。
- Windows 10 IoT Enterprise 2016 LTSB (v1607) および 2019 LTSC (v1809)。

- サポートされるプロセッサ (CPU) アーキテクチャ: x86およびx64 (ARMはサポートされていません)。
- エンドポイント要件: ピアツーピアのビデオ会議中に720p HD解像度をサポートできる、約2.2～2.4 GHzのデュアルコアCPU。
- Intel Turbo BoostまたはAMD Turbo Coreを搭載し、少なくとも2.4 GHzまでブーストできる、ベース速度が低い (~1.5 GHz) デュアルコアまたはクアッドコアCPU。
- 検証済みHPシンクライアント: t630/t640、t730/t740、mt44/mt45。
- 検証済みDellシンクライアント: 5070、5470 Mobile TCおよびAIO。
- 検証済み10ZiGシンクライアント: 4510および5810q。
- 検証済みエンドポイントの完全なリストについては、シンクライアントを参照してください。
- Citrix Workspace app には、最低 600 MB の空きディスク容量と 1 GB の RAM が必要です。
- Microsoft .NET Framework の最小要件はバージョン 4.8 です。Citrix Workspace app は、システムに .NET Framework が存在しない場合、自動的にダウンロードしてインストールします。

管理者は、Microsoft Teams Optimization policy を変更することで、最適化モードで Microsoft Teams を起動できるように/できないように設定できます。Citrix Workspace app で最適化モードで起動するユーザーは、Microsoft Teams を無効にできません。

最小バージョン - Linux 用 Citrix Workspace app 2006

詳しくは、Linux 用 Citrix Workspace app ドキュメントの「Optimization for Microsoft Teams」を参照してください。

ソフトウェア:

- `GStreamer` 1.0以降またはCairo 2
- `libc++-9.0` 以降
- `libgdk` 3.22 以降
- OpenSSL 1.1.1d
- `libnsl`
- Ubuntu 20.04 以降

認証の強化:

- Libsecret ライブラリ
- libunwind-12 ライブラリ。詳しくは、「Adding the libunwind-12 library dependency for llvm-12」を参照してください。

ハードウェア:

- ピアツーピアのビデオ会議通話中に720p HD解像度をサポートできる、最低1.8 GHzのデュアルコアCPU
- ベース速度1.8 GHz、Intel Turbo Boostの高速が2.9 GHz以上のデュアルコアまたはクアッドコアCPU

検証済みのエンドポイントの完全なリストについては、「Thin Clients」を参照してください。

詳しくは、「Prerequisites to install Citrix Workspace app」を参照してください。

`/opt/Citrix/ICAClient/config/module.ini`ファイルで**VDWEBRTC**フィールドの値をOffに更新することで、Microsoft Teamsの最適化を無効にできます。デフォルトはVDWEBRTC=Onです。更新が完了したら、セッションを再起動してください。(ルート権限が必要です)。

最小バージョン - Mac用Citrix Workspaceアプリ2012

サポートされているオペレーティングシステム:

- macOS Catalina (10.15)。
- macOS Big Sur 11.0.1以降。
- macOS モントレー。

サポートされている機能:

- オーディオ
- ビデオ
- 画面共有の最適化（送受信）

> **注記:**

> Citrix Viewerアプリが画面共有を機能させるには、macOSのセキュリティとプライバシー設定へのアクセスが必要です。ユーザーは、**Appleメニュー > システム設定 > セキュリティとプライバシー > プライバシータブ > 画面収録**でこの設定を構成し、**Citrix Viewer**を選択します。

> Microsoft Teamsの最適化は、Citrix Workspaceアプリ2012以降およびmacOS 10.15でデフォルトで機能します。

Microsoft Teamsの最適化を無効にするには、ターミナルでこのコマンドを実行し、Citrix Workspaceアプリを再起動します。

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

最小バージョン - 最新バージョンのChromeOSで実行されているChromeOS用Citrix Workspaceアプリの最新バージョン

ハードウェア:

- Intel i3、クアッドコア2.4 GHzと同等またはそれ以上の性能を持つプロセッサ。

サポートされている機能:

- オーディオ
- ビデオ
- 画面共有の最適化 (送受信) - デフォルトで無効。有効にする方法については、これらの設定を参照してください。

シングルサーバーのスケーラビリティ

このセクションでは、単一の物理ホストでサポートできるユーザー数または仮想マシン (VM) 数を推定するための推奨事項とガイダンスを提供します。これは一般に、Citrix Virtual Apps and Desktopsのシングルサーバーのスケーラビリティ (SSS) と呼ばれます。Citrix Virtual Apps (CVA) またはセッション仮想化のコンテキストでは、ユーザー密度とも呼ばれます。その目的は、主要なハイパーバイザーを実行している単一のハードウェアで、いくつのユーザーまたはVMを実行できるかを明らかにすることです。

> **注記:**
>
> このセクションでは、SSS を推定するためのガイダンスを説明します。このガイダンスは一般的なものであり、お客様固有の状況や環境に必ずしも特化したものではない場合があります。Citrix Virtual Apps and Desktops の SSS を真に理解する唯一の方法は、Login VSI のようなスケーラビリティまたはロードテストツールを使用することです。Citrix は、SSS を迅速に推定するために、このガイダンスとこれらの簡単なルールのみを使用することを推奨します。ただし、ハードウェアを購入したり、財務上の決定を下したりする前に、結果を検証するために Login VSI または選択したロードテストツールを使用することを Citrix は推奨します。

ハードウェア（テスト対象システム）

- デル パワーエッジ R740
- Intel Xeon (Gold) 6126 @ 2.60 GHz (最大ターボ 3.70 GHz)、ソケットあたり 12 コア、ハイパースレッディング有効のデュアルソケット
- 382 GB RAM
- ローカル SSD RAID 0 ストレージ (11 ディスク) 6 TB

ソフトウェア

Citrix Virtual Apps and Desktops 2106 を実行する Windows 2019 (TSVDA) を搭載した単一の仮想マシン (40 論理プロセッサ) VMware ESXi 6.7

用語

- ナレッジワーカーのワークロード: Acrobat Reader、Freemind/Java、フォトビューアー、Edge、および Excel、Outlook、PowerPoint、Word などの MS Office アプリが含まれます。
- ベースライン: ナレッジワーカーのワークロード (Microsoft Teams なし) で実行されるサーバーのスケーラビリティテスト。
- Microsoft Teams ワークロード: ナレッジワーカーの一般的なワークロード + Microsoft Teams。

Microsoft Teams のストレステスト方法

- Microsoft Teams は HDX で最適化されています。そのため、すべてのマルチメディア処理はエンドポイントまたはクライアントにオフロードされ、測定には含まれません。
- ワークロードが開始される前に、すべての Microsoft Teams プロセスが停止または終了されます。
- Microsoft Teams を開く (コールドスタート)。
- Microsoft Teams の起動にかかる時間と、Microsoft Teams のプライマリウィンドウがフォーカスを取得するまでの時間を測定します。
- キーボードショートカットを使用してチャットウィンドウに切り替えます。
- キーボードショートカットを使用してカレンダーウィンドウに切り替えます。
- キーボードショートカットを使用して、特定のユーザーにチャットメッセージを送信します。
- キーボードショートカットを使用して Microsoft Teams ウィンドウに切り替えます。

結果

- Microsoft Teams ワークロード (81 ユーザー) では、ベースライン (137 ユーザー) と比較して、スケーラビリティに 40% の影響があります。
- サーバー容量を約 40% (CPU) 増やすと、ベースラインワークロードの場合と同じユーザー数に戻ります。
- Microsoft Teams ワークロードでは、ベースラインと比較して 20% の追加メモリが必要です。
- ユーザーあたりのストレージサイズを 512〜1024 MB 増やします。
- IOPS 書き込みが約 50% 増加し、IOPS 読み取りが約 100% 増加します。Microsoft Teams は、ストレージが遅い環境では大きな影響を与える可能性があります。

機能マトリックスとバージョンサポート

機能	MICROSOFT TEAMS (最小バージョン)	VDA (最小バージョン)	WINDOWS CR 向け CITRIX WORKSPACE アプリ (最小バージョン)	MAC 向け CITRIX WORKSPACE アプリ (最小バージョン)	LINUX 向け CITRIX WORKSPACE アプリ (最小バージョン)	CHROME OS 向け CITRIX WORKSPACE アプリ (最小バージョン)
オーディオ/ビデオ (P2P および会議)	現在のバージョンから90日前	1906	1907	2009	2004	2105.5
画面共有	現在のバージョンから90日前	1906	1907	2012	2006	2105.5
i. 画面インジケーターの赤い枠線	現在のバージョンから90日前	1906	2002	2012	2006	いいえ
ii. キャプチャを Desktop Viewerに制限	現在のバージョンから90日前	1906	2009.5	2012	2006	いいえ

機能	MICROSOFT TEAMS (最小バージョン)	VDA (最小バージョン)	WINDOWS CR 向け CITRIX WORKSPACE アプリ (最小バージョン)	MAC 向け CITRIX WORKSPACE アプリ (最小バージョン)	LINUX 向け CITRIX WORKSPACE アプリ (最小バージョン)	CHROME OS 向け CITRIX WORKSPACE アプリ (最小バージョン)
iii. マルチモニター	現在のバージョンから90日前	1912 CU6+	2106 (1)	2106	2106	いいえ
DTMF	現在のバージョンから90日前	該当なし	2102	2101	2101	2111.1
プロキシサーバーのサポート	現在のバージョンから90日前	N/A	2012 (2)	2104 (3)	2101 (3)	2305
アプリ共有	現在のバージョンから90日前	2109	2109.1	2203.1	2209	いいえ
ライブキャプション	現在のバージョンから90日前	該当なし (4)	2109.1	2109	2109	2303
ダイナミック e911	現在のバージョンから90日前	該当なし	2112.1	2112	2112	2112
制御を付与	現在のバージョンから90日前	N/A	2112.1	2203.1	いいえ	いいえ

機能	MICROSOFT TEAMS (最小バージョン)	VDA (最小バージョン)	WINDOWS CR 向け CITRIX WORKSPACE アプリ (最小バージョン)	MAC 向け CITRIX WORKSPACE アプリ (最小バージョン)	LINUX 向け CITRIX WORKSPACE アプリ (最小バージョン)	CHROME OS 向け CITRIX WORKSPACE アプリ (最小バージョン)
制御を要求	現在のバージョンから90日前	N/A	2112.1	2203.1	2203	2303
マルチウィンドウ	1.5.00.11865	2112, 1912 CU6 (5)	2112.1	2203.1	2203	2303
会議の文字起こし	現在のバージョンから90日遡ったもの	2112.1, 1912 CU6+	2112	2203.1	2203	2303
背景ぼかし	現在のバージョンから90日遡ったもの	2112, 1912 CU6+	2207	2301	2212	2303

1. CD Viewerは全画面モードのみ。SHIFT+F2はサポートされていません。
2. Negotiate/Kerberos、NTLM、Basic、およびDigest。`Pac`ファイルもサポートされています。
3. 匿名のみ。
4. VDAが2112以降の場合、ライブキャプションは、Citrix Workspaceアプリのバージョンが MAC用2203.1、Linux用2203、またはWindows用2112の場合にのみ機能します。これは、Microsoft Teamsがシングルウィンドウ UIモードまたはマルチウィンドウモードの場合、ライブキャプションの動作が異なるためです。
5. MultiWindowは2112 VDAで導入されましたが、VDA 1912 LTSR CU6リリースにバックポートされました。

注:

- **Citrix Workspace app for Windows 1912 CU6 (またはそれ以降)** に記載されているすべての機能は、Citrix Workspace app for Windows 2203.1 LTSR CU1に適用されます。
- Microsoftは、Microsoft Teamsにおけるシングルウィンドウモードのサポートを非推奨としました。これに対応するため、VDAを1912 CU6+ LTSRに、Citrix Workspaceアプリを2203 CU2+以降にアップグレードする必要があります。これらはMultiWindowモードをサポートしています。

Microsoft Teamsの最適化を有効にする

Microsoft Teamsの最適化を有効にするには、Microsoft Teams redirectionポリシーに記載されている管理ポリシーを使用します。このポリシーはデフォルトで**ON**になっています。このポリシーが有効になっていることに加えて、HDXはCitrix Workspaceアプリのバージョンが少なくとも必要な最小バージョンであることを確認します。ポリシーを有効にし、Citrix Workspaceアプリのバージョンがサポートされている場合、VDA上で**HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport**が自動的に**1**に設定されます。Microsoft Teamsは、VDIモードでロードするためにこのキーを読み取ります。

「注：」:

バージョン1906.2以降のVDA、またはManageコンソール（Studio）でポリシーが利用できない古いコントローラーバージョン（バージョン7.15など）を使用している場合でも、VDAを最適化できます。Microsoft TeamsのHDX最適化は、VDAでデフォルトで有効になっています。

> をクリックすると、**Citrix HDX Optimized** の凡例が表示されます。

Citrix向けに最適化された凡例(/en-us/citrix-virtual-apps-desktops/2407/media/teams-opt.png)

Citrix HDX Not Connected と表示される場合、Citrix APIはMicrosoft Teamsにロードされています。APIのロードはリダイレクトへの最初のステップです。しかし、スタックの後続の部分でエラーが発生しています。このエラーは、VDAサービスまたはCitrix Workspaceアプリにある可能性が最も高いです。

Citrix向けに最適化されていない凡例(/en-us/citrix-virtual-apps-desktops/2407/media/teams-not-conn.png)

凡例が表示されない場合、Microsoft TeamsはCitrix APIのロードに失敗しました。通知領域のアイコンを右クリックしてMicrosoft Teamsを終了し、再起動してください。管理ポリシーが に設定されていないこと、およびCitrix Workspaceアプリのバージョンがサポートされていることを確認してください。

Citrix凡例なし(/en-us/citrix-virtual-apps-desktops/2407/media/teams-no-api.png)

> **「重要: セッションの再接続」**

- 接続が変更された場合、HDX最適化セッションを取得するためにMicrosoft Teamsを再起動する必要がある場合があります。たとえば、サポートされていないエンドポイント（iOS、Android、またはWindows/Linux/Macの古いバージョンのWorkspaceアプリ）からサポートされているエンドポイント（Windows/Linux/Mac/ChromeOS/HTML5のWorkspaceアプリ）にローミングする場合、またはその逆の場合です。
- VDAにMicrosoft Teamsの.exeインストーラーを使用してアプリをインストールした場合も、Microsoft Teamsの再起動が必要です。.exeインストーラーは、永続VDI展開に推奨されます。このような場合、HDXセッションが切断状態にある間にMicrosoft Teamsが自動更新されることがあります。そのため、HDXセッションに再接続するユーザーは、Microsoft Teamsが最適化されて実行されていないことに気づきます。
- ローカルセッションからHDXセッションにローミングする場合、HDXで最適化するためにMicrosoft Teamsを再起動する必要があります。この操作は、リモートPCアクセスシナリオで必要です。

ネットワーク要件

Microsoft Teamsは、会議や多人数通話のためにMicrosoft 365のメディアプロセッサーサーバーに依存しています。また、Microsoft Teamsは、次のシナリオでMicrosoft 365トランスポートリレーに依存しています。

- ポイントツーポイント通話の2つのピアが直接接続されていない
- 参加者がメディアプロセッサに直接接続されていない。

そのため、ピアとMicrosoft 365クラウド間のネットワークの状態が通話のパフォーマンスを決定します。ネットワーク計画に関する詳細なガイドラインについては、Microsoft 365 network connectivity principlesを参照してください。

全体的なクラウド音声およびビデオの展開に影響を与える可能性のあるリスクと要件を特定するために、環境を評価することをお勧めします。 ネットワークがMicrosoft Teamsに対応しているかテストするには、Skype for Business Network Assessment Toolを使用してください。サポート情報については、Supportを参照してください。

Real Time Protocol (RTP) トラフィックに関する主要なネットワーク推奨事項の概要

- 支社からMicrosoft 365ネットワークにできるだけ直接接続します。
- 支社で十分な帯域幅を計画し、提供します。
- 各支社のネットワーク接続と品質を確認します。
- 支店で以下のいずれかを使用する必要がある場合は、RTP/UDPトラフィック（Citrix WorkspaceアプリのHdxRtcEngine.exeによって処理される）が妨げられないことを確認してください。
  - プロキシサーバーをバイパスする
  - ネットワークSSLインターセプト
  - ディープパケットインスペクションデバイス
  - VPNヘアピン（可能であればスプリットトンネリングを使用）

> **重要: VPNスプリットトンネル構成**

> HdxRtcEngine.exeトラフィックはVPNトンネルから迂回させ、ユーザーのローカルインターネット接続を使用してサービスに直接接続できるようにする必要があります。これを実現する方法は、使用されるVPN製品とマシンプラットフォームによって異なりますが、ほとんどのVPNソリューションでは、このロジックを適用するためのポリシーの簡単な構成が可能です。VPNプラットフォーム固有のスプリットトンネルガイダンスの詳細については、この Microsoft記事を参照してください。

> Workspaceアプリ（HdxRtcEngine.exe）のWebRTCメディアエンジンは、クライアントにオフロードされるマルチメディアストリームにSecure Real-time Transport Protocol (SRTP) を使用します。SRTPはRTPに機密性と認証を提供します。この機能では、対称鍵（DTLSとネゴシエート）を使用して、AES暗号化方式でメディアと制御メッセージを暗号化します。

良好なユーザーエクスペリエンスのために、以下のメトリックが推奨されます。

メトリック	エンドポイントからMICROSOFT 365まで
遅延 (片道)	< 50 ミリ秒
遅延 (RTT)	< 100 ミリ秒
パケット損失	15秒間隔で1%未満
パケット到着間隔ジッター	15秒間隔で30ミリ秒未満

詳細については、「Microsoft Teams 用に組織のネットワークを準備する」を参照してください。

帯域幅要件については、Microsoft Teams の最適化では、オーディオ (OPUS/G.722/PCM G711) およびビデオ (H264) 用にさまざまなコーデックを使用できます。

ピアは、セッション記述プロトコル (SDP) の Offer/Answer を使用して、通話確立プロセス中にこれらのコーデックをネゴシエートします。 Citrix のユーザーごとの最小推奨事項は次のとおりです。

タイプ	帯域幅	コーデック
音声 (双方向)	約 90 kbps	G.722
音声 (双方向)	約 60 kbps	オーパス*
ビデオ (双方向)	約 700 kbps	H264 360p 30フレーム/秒 16:9
画面共有	約 300 kbps	H264 1080p 15フレーム/秒

* Opus は、6 kbps から 510 kbps までの定ビットレートおよび可変ビットレートエンコーディングをサポートします。

OpusとH264は、ピアツーピアおよび電話会議に推奨されるコーデックです。

> **重要:**

> パフォーマンスに関して、クライアントマシンでのCPU使用率では、デコードよりもエンコードの方がコストがかかります。LinuxおよびWindows版Citrix Workspaceアプリで、最大

> エンコード解像度をハードコードできます。「エンコーダーのパフォーマンス見積もり」および「Microsoft Teamsの最適化」を参照してください。

プロキシサーバー

プロキシの場所に応じて、以下を考慮してください。

- VDAでのプロキシ構成:

  VDAで明示的なプロキシサーバーを構成し、localhostへの接続をプロキシ経由でルーティングすると、リダイレクトは失敗します。プロキシを正しく構成するには、**Internet Options > Connections > LAN Settings > Proxy Servers**で**ローカルアドレスにはプロキシサーバーを使用しない**設定を選択し、`127.0.0.1:9002`をバイパスする必要があります。

  PACファイルを使用する場合、PACファイルからのVDAプロキシ構成スクリプトは、`wss://127.0.0.1:9002`に対して **DIRECT** を返す必要があります。そうでない場合、最適化は失敗します。スクリプトが **DIRECT** を返すことを確認するには、`shExpMatch(url, "wss://127.0.0.1:9002/*")`を使用します。

- Citrix Workspaceアプリでのプロキシ構成:

  支社がプロキシ経由でインターネットにアクセスするように構成されている場合、以下のバージョンがプロキシサーバーをサポートします。

  - Citrix Workspaceアプリ for Windowsバージョン2012 (Negotiate/Kerberos、NTLM、Basic、Digest。`Pac`ファイルもサポートされています)
  - Citrix Workspaceアプリ for Windowsバージョン1912 CU5 (Negotiate/Kerberos、NTLM、Basic、Digest。`Pac`ファイルもサポートされています)
  - Citrix Workspaceアプリ for Linuxバージョン2101 (匿名認証)
  - Citrix Workspaceアプリ for Macバージョン2104 (匿名認証)

以前のバージョンのCitrix Workspaceアプリを使用しているクライアントデバイスは、プロキシ構成を読み取ることができません。これらのデバイスは、トラフィックをMicrosoft 365 TURNサーバーに直接送信します。

> **重要:**

- クライアントデバイスがDNS解決を行うためにDNSサーバーに接続できることを確認してください。クライアントデバイスは、以下のMicrosoft Teamsリレーサーバーの FQDN を解決できる必要があります。
  - `worldaz.relay.teams.microsoft.com`
  - `inaz.relay.teams.microsoft.com`
  - `uaeaz.relay.teams.microsoft.com`
  - `euaz.relay.teams.microsoft.com`
  - `usaz.relay.teams.microsoft.com`
  - `turn.dod.teams.microsoft.us`
  - `turn.gov.teams.microsoft.us`

DNS要求が失敗した場合、外部ユーザーとのP2P通話およびメディア確立を伴う会議通話は失敗します。

- 会議サーバーの場所は、最初の参加者の仮想デスクトップの場所に基づいて選択されます (クライアントではありません)。

通話の確立とメディアフローパス

可能な場合、Citrix WorkspaceアプリのHDX WebRTCメディアエンジン (HdxRtcEngine.exe) は、ピアツーピア通話でユーザーデータグラムプロトコル (UDP) を介した直接ネットワークセキュアリアルタイムトランスポートプロトコル (SRTP) 接続を確立しようとします。UDPハイポートがブロックされている場合、メディアエンジンはTCP/TLS 443にフォールバックします。

HDXメディアエンジンは、候補の検出と接続の確立のために、ICE、NAT用セッショントラバーサルユーティリティ (STUN)、およびNAT周辺のリレーを使用したトラバーサル (TURN) をサポートしています。このサポートは、エンドポイントがDNS解決を実行できる必要があることを意味します。

2つのピア間、またはピアと会議サーバー間に直接パスがなく、多人数通話または会議に参加しているシナリオを検討してください。HdxRtcEngine.exeは、Microsoft 365のMicrosoft Teamsトランスポートリレーサーバーを使用して、他のピアまたは会議がホストされているメディアプロセッサに到達します。クライアントマシンは、3つのMicrosoft 365サブネットIPアドレス範囲と4つのUDPポート (UDPがブロックされている場合はフォールバックとしてTCP/TLS 443) にアクセスで

きる必要があります。詳細については、通話設定 および Office 365のURLとIPアドレス範囲ID 11 のアーキテクチャ図を参照してください。

ID	カテゴリ	アドレス	宛先ポート
11	最適化が必要	13.107.64.0/18, 52.112.0.0/14, 52.122.0.0/15	**UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (フォールバック)

これらの範囲には、Azure Load Balancer によってフロントエンド化されたトランスポートリレーとメディアプロセッサの両方が含まれます。 Microsoft Teams トランスポートリレーはSTUNおよびTURN機能を提供しますが、ICEエンドポイントではありません。また、Microsoft Teams トランスポートリレーは、メディア、TLSを終端したり、トランスコーディングを行ったりしません。他のピアまたはメディアプロセッサにトラフィックを転送する際、TCP (HdxRtcEngine.exeがTCPを使用する場合) をUDPにブリッジできます。

WorkspaceアプリのWebRTCメディアエンジンは、Microsoft 365クラウド内の最も近いMicrosoft Teamsトランスポートリレーに接続します。メディアエンジンは、エニーキャストIPとポート3478〜3481 UDP（ワークロードごとに異なるUDPポートですが、多重化が発生する可能性があります）、またはフォールバック用に443 TCP/TLSを使用します。通話品質は、基盤となるネットワークプロトコルに依存します。UDPは常にTCPよりも推奨されるため、ブランチオフィスでUDPトラフィックに対応できるようにネットワークを設計することをお勧めします。

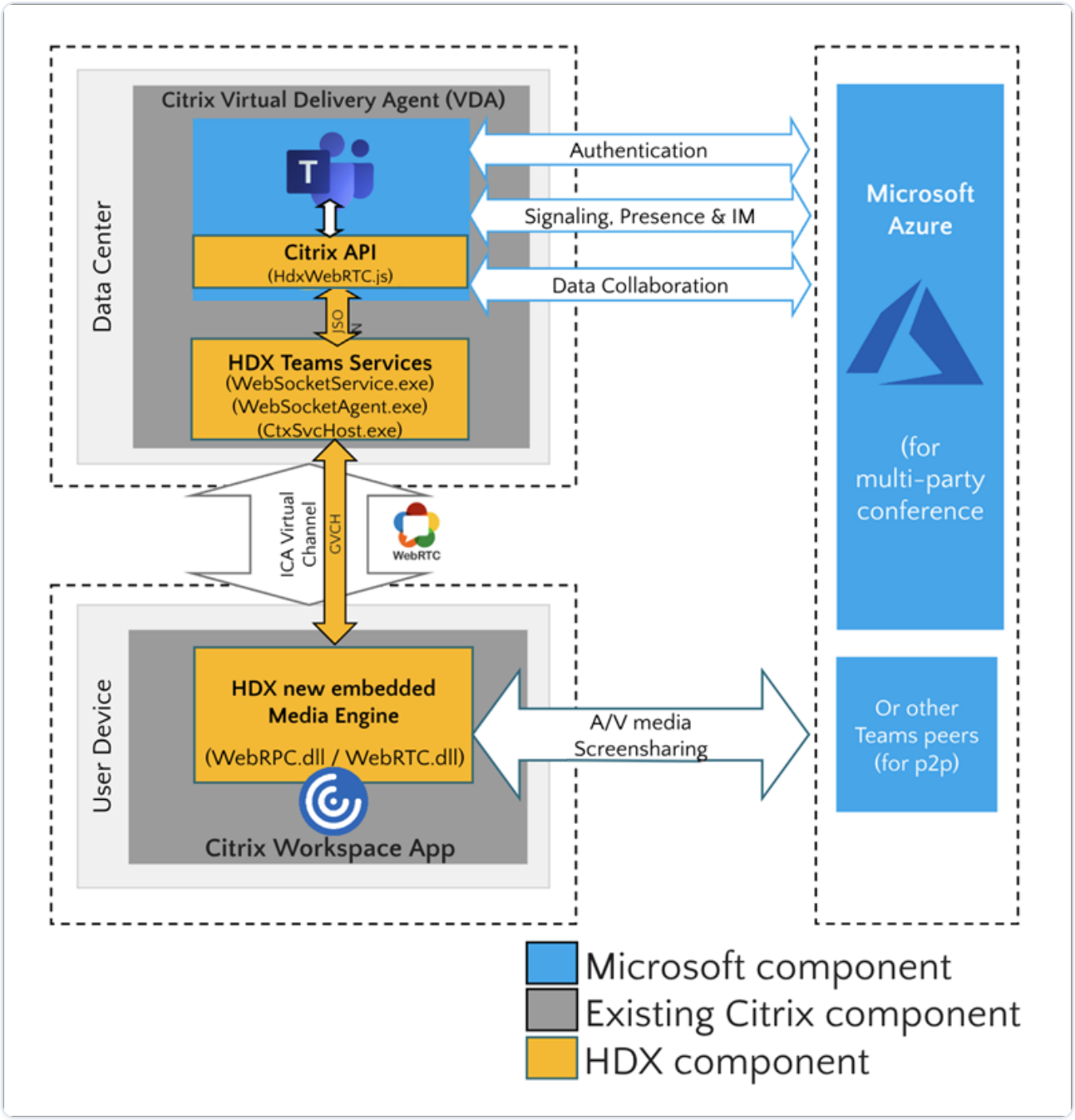
Microsoft Teamsが最適化モードでロードされ、HdxRtcEngine.exeがエンドポイントで実行されている場合、ICEの障害により通話設定の失敗や、片方向のみのオーディオ/ビデオが発生する可能性があります。通話が完了できない場合やメディアストリームが全二重でない場合は、まずエンドポイントの**Wiresharkトレース**を確認してください。ICE候補収集プロセスに関する詳細については、サポートセクションの「ログの収集」を参照してください。

> **注：**
>
> エンドポイントがインターネットにアクセスできない場合でも、両方のユーザーが同じLAN上にいれば、ピアツーピア通話を行うことができる場合があります。会議は失敗します。この場合、通話設定が開始されるまでに30秒のタイムアウトがあります。

通話設定

このアーキテクチャ図を、通話フローシーケンスの視覚的な参照として使用してください。対応する手順は図に示されています。

アーキテクチャ



1. Microsoft Teams を起動します。
2. Microsoft Teams は O365 に対して認証を行います。テナントポリシーは Microsoft Teams クライアントにプッシュダウンされ、関連するTURNおよびシグナリングチャネル情報がアプリに中継されます。

3. Microsoft Teams は VDA で実行されていることを検出し、Citrix JavaScript API に API 呼び出しを行います。
4. Microsoft Teams 内の Citrix JavaScript は、VDA で実行されている WebSocketService.exe へのセキュアな WebSocket 接続を開き、これによりユーザーセッション内に WebSocketAgent.exe が生成されます。
5. WebSocketAgent.exe は、Citrix HDX Microsoft Teams Redirection Service (CtxSvcHost.exe) を呼び出すことにより、汎用仮想チャネルをインスタンス化します。
6. Citrix Workspace アプリの wfica32.exe (HDX エンジン) は、HdxRtcEngine.exe と呼ばれる新しいプロセスを生成します。これは、Microsoft Teams の最適化に使用される新しい WebRTC エンジンです。
7. Citrix メディアエンジンと Teams.exe は双方向の仮想チャネルパスを持ち、マルチメディア要求の処理を開始できます。

   -----ユーザー通話------

8. **Peer A** が**通話**ボタンをクリックします。Teams.exe は Microsoft 365 の Microsoft Teams サービスと通信し、**Peer B** とのエンドツーエンドのシグナリングパスを確立します。Microsoft Teams は HdxRtcEngine に、サポートされている一連の通話パラメーター（コーデック、解像度など。これらはセッション記述プロトコル (SDP) オファーとして知られています）を要求します。これらの通話パラメーターは、シグナリングパスを使用して Microsoft 365 の Microsoft Teams サービスに中継され、そこからもう一方のピアに中継されます。
9. SDP のオファー/アンサー（シングルパスネゴシエーション）はシグナリングチャネルを介して行われ、ICE 接続チェック（STUN バインド要求を使用した NAT およびファイアウォールトラバーサル）が完了します。その後、Secure Real-time Transport Protocol (SRTP) メディアは HdxRtcEngine.exe ともう一方のピア（会議の場合は Microsoft 365 会議サーバー）の間で直接流れます。

マイクロソフト 電話システム

Phone System は、Microsoft Teams を使用して Microsoft 365 クラウドで通話制御と PBX を可能にする Microsoft のテクノロジーです。Microsoft Teams の最適化は、Microsoft 365 Calling Plans または Direct Routing を使用して Phone System をサポートします。Direct Routing を使用すると、追加のオンプレミスソフトウェアなしで、サポートされている独自のセッションボーダーコントローラーを Microsoft Phone System に直接接続できます。 通話キュー、転送、フォワード、保留、ミュート、通話再開がサポートされています。

DTMF

デュアルトーン多周波（DTMF）機能は、以下のバージョンのCitrix Workspaceアプリ（およびそれ以降）でサポートされています。

- Citrix Workspaceアプリ for Windowsバージョン2102
- Citrix Workspace アプリケーション Windows用 LTSR 1912 CU5 (Windows 10 OSのみ)
- Citrix Workspaceアプリ for Linuxバージョン2101
- Citrix Workspaceアプリ for Macバージョン2101
- Citrix Workspaceアプリ for ChromeOSバージョン2111.1

動的e911のサポート

バージョン2112以降、Citrix Workspaceアプリは動的緊急通報をサポートしています。Microsoft Calling Plans、Operator Connect、およびDirect Routingで使用する場合、以下のことが可能になります。

- 緊急通報の設定とルーティング。
- セキュリティ担当者への通知。

通知は、VDAで実行されているMicrosoft Teamsクライアントではなく、エンドポイントで実行されているCitrix Workspaceアプリの現在の場所に基づいて提供されます。

Ray Baum法では、911通報者の派遣可能な位置情報を適切な公共安全応答拠点 (PSAP) に送信することが義務付けられています。HDXによるMicrosoft Teamsの最適化は、以下のバージョンのCitrix Workspaceアプリで使用する場合、Ray Baum法に準拠しています。

- Citrix Workspaceアプリ for Windowsバージョン2112.1以降
- Citrix Workspaceアプリ for Linuxバージョン2112以降
- Citrix Workspaceアプリ for Macバージョン2112以降
- ChromeOS版Citrix Workspaceアプリバージョン2112以降

動的な緊急通報を有効にするには、管理者はMicrosoft Teams管理センターを使用して、ネットワークまたは緊急ロケーションマップを作成するために以下を構成する必要があります。

- ネットワーク設定
- ロケーション情報サービス (LIS)

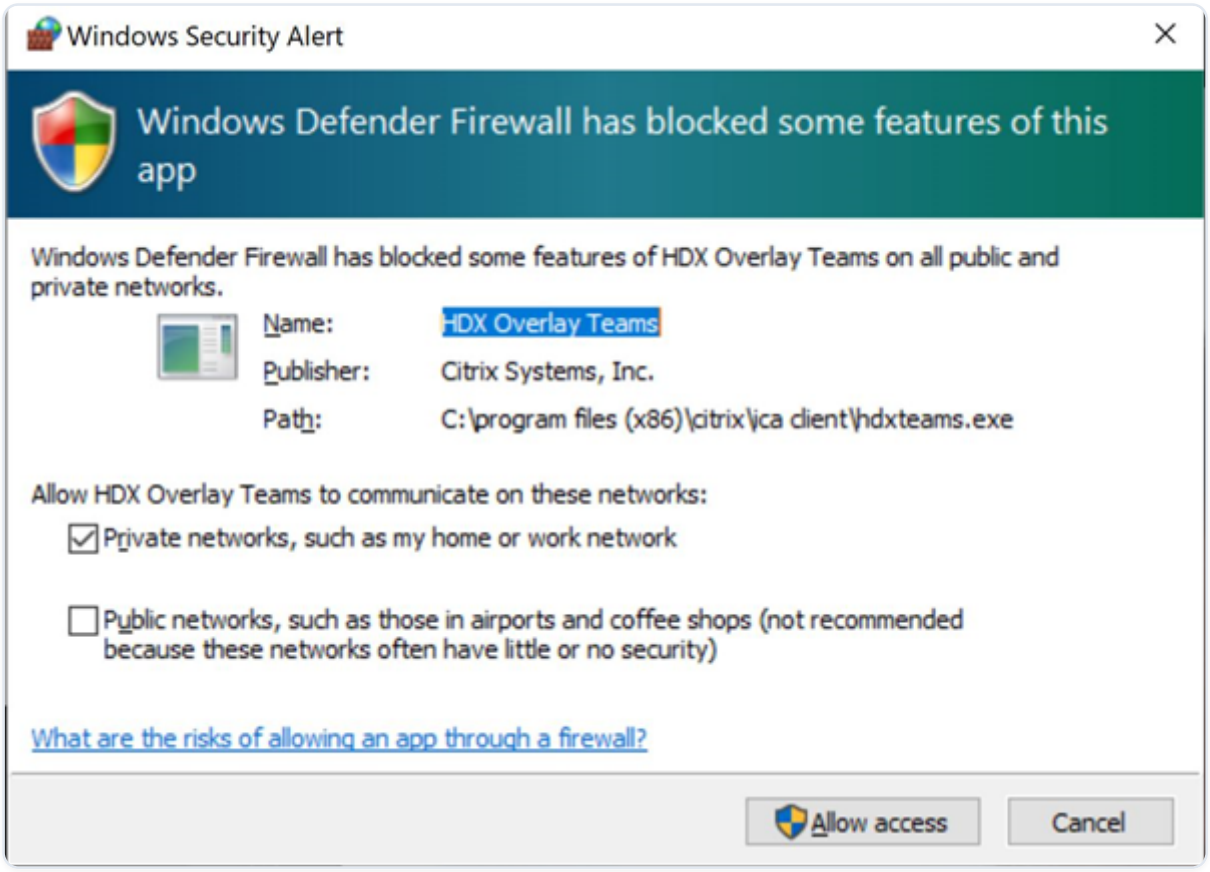
動的緊急通報の詳細については、Microsoft のドキュメントを参照してください。

Citrix WorkspaceアプリがMicrosoft Teamsに中継するディスパッチ可能な位置情報は次のとおりです。

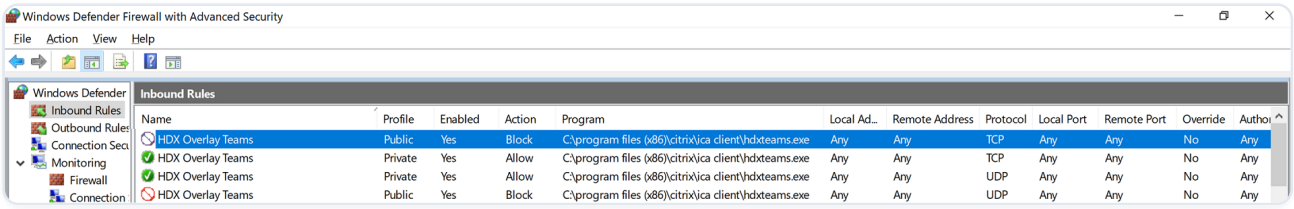
- イーサネット/スイッチ接続用のリンク層検出プロトコル (LLDP) を使用したシャーシ ID / ポート ID。イーサネット/スイッチ (LLDP) は以下でサポートされています。
  - Windows バージョン 8.1 および 10
  - LLDP 有効化ソフトウェアを必要とする macOS。LLDP 有効化ソフトウェアをダウンロードするには、`www.microsoft.com`にアクセスして「LLDP enablement software」を検索してください。
  - Linux。シンクライアントのオペレーティングシステム (OS) ディストリビューションに LLDP ライブラリを含める必要があります。
- Citrix Workspace アプリがインストールされているエンドポイントの WLAN BBSID および {IPv4-IPv6; サブネット; MAC アドレス}。
  - サブネットおよび WiFi ベースのロケーションは、Windows、Linux、Mac 用 Workspace アプリでサポートされています。
- Citrix WorkspaceアプリがインストールされているOSレベルでユーザーの許可が与えられている場合（権限がHDX RTC Engineに設定されている場合）の緯度と経度
  - すべてのWorkspaceアプリプラットフォームでサポートされています。ただし、Citrix Workspace for Linuxの場合、シンクライアントのOSディストリビューションに`libgps`ライブラリを含める必要があります（>sudo apt-get install libgps23 gpsd lldpd）。

ファイアウォールの考慮事項

ユーザーがMicrosoft Teamsクライアントを使用して最適化された通話を初めて開始すると、**Windows ファイアウォール**の設定に関する警告が表示されることがあります。この警告は、HdxTeams.exeまたはHdxRtcEngine.exe (HDX Overlay Microsoft Teams) の通信を許可するようユーザーに求めます。



Windows Defender ファイアウォール > セキュリティが強化されたWindows Defender ファイアウォールコンソールの**受信の規則**の下に、次の4つのエントリが追加されます。必要に応じて、より制限の厳しい規則を適用することもできます。

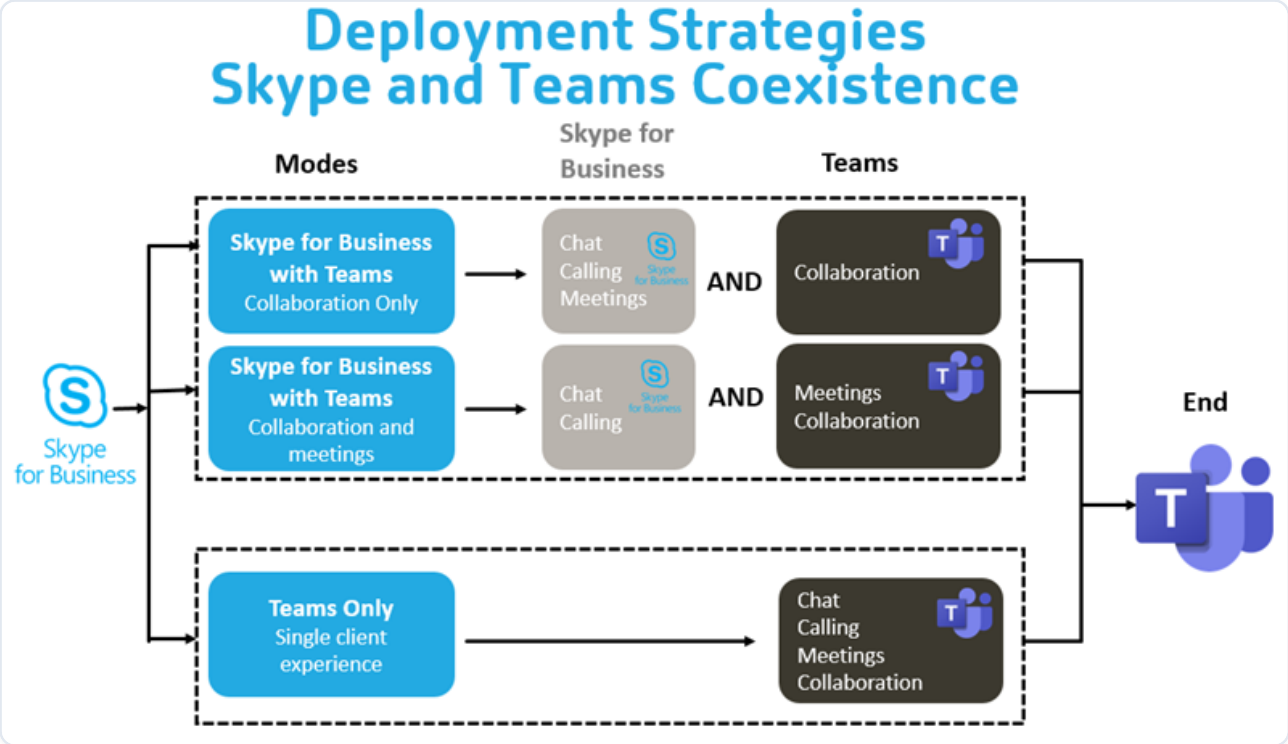


Microsoft Teams および Skype for Business の共存

Microsoft Teams と Skype for Business は、機能が重複する2つの個別のソリューションとして並行して展開できます。 詳細については、Understand Microsoft Teams and Skype for Business coexistence and interoperability を参照してください。

Citrix RealTime Optimization PackとMicrosoft Teamsマルチメディアエンジン用のHDX最適化は、環境で設定された構成を尊重します。例としては、アイランドモードや、Microsoft TeamsとのSkype for Businessコラボレーションが挙げられます。また、Microsoft TeamsとのSkype for Businessコラボレーションと会議も含まれます。

周辺機器へのアクセスは、一度に1つのアプリケーションにのみ許可されます。たとえば、通話中にRealTime Media EngineによるWebカメラアクセスは、通話中にイメージングデバイスをロックします。デバイスが解放されると、Microsoft Teamsで利用可能になります。



Citrix SD-WAN™: Microsoft Teams向けに最適化されたネットワーク接続

最適なオーディオおよびビデオ品質には、低遅延、低ジッター、低パケット損失のMicrosoft 365クラウドへのネットワーク接続が必要です。支店拠点のCitrix Workspaceアプリユーザーからの Microsoft Teamsオーディオビデオ RTPトラフィックを、インターネットに接続する前にデータセンターにバックホールすると、過剰な遅延が発生する可能性があります。また、WANリンクで輻輳を引き起こす可能性もあります。Citrix SD-WANは、Microsoft 365ネットワーク接続の原則に従ってMicrosoft Teamsの接続を最適化します。Citrix SD-WANは、Microsoft RESTベースの Microsoft 365 IPアドレスとWebサービス、および近接DNSを使用して、Microsoft Teamsトラフィックを識別、分類、および誘導します。

多くの地域で、ビジネスブロードバンドインターネット接続は、断続的なパケット損失、過剰なジッター期間、および停止に悩まされています。

Citrix SD-WANは、ネットワークの状態が不安定または劣化している場合に、Microsoft Teamsのオーディオ/ビデオ品質を維持するための2つのソリューションを提供します。

- Microsoft Azureを使用している場合、Azure VNETに展開されたCitrix SD-WAN仮想アプライアンス (VPX) は、高度な接続最適化を提供します。これらの最適化には、シームレスなリンクフェイルオーバーとオーディオパケットレーシングが含まれます。
- Citrix SD-WANのお客様は、Citrix Cloud™ Directサービスを介してMicrosoft 365に接続できます。このサービスは、すべてのインターネット向けトラフィックに対して信頼性の高い安全な配信を提供します。

支社インターネット接続の品質が問題にならない場合は、遅延を最小限に抑えるだけで十分な場合があります。遅延を最小限に抑えるには、Microsoft TeamsのトラフィックをCitrix SD-WANブランチアプライアンスから最寄りのMicrosoft 365フロントドアに直接誘導します。詳細については、「Citrix SD-WAN Office 365 optimization」を参照してください。

シトリックス SD-WAN](/en-us/citrix-virtual-apps-desktops/2407/media/sd-wan.png)

マルチウィンドウ会議とチャット

Windows版Microsoft Teamsでは、複数の会議またはチャットウィンドウを使用できます。ポップアウト機能の詳細については、Microsoft 365サイトのMicrosoft Teams Pop-Out Windows for Chats and Meetingsを参照してください。

> **注:**
>
> この機能は、Citrix Workspaceアプリ for Windows 2112.1、Mac 2203、Linux 2203、ChromeOS 2303でサポートされています。VDA 2112以降が必要で、1912 CU6+ LTSRにバックポートされました。

背景のぼかしと背景効果

Windows、Mac、Linux、ChromeOS/HTML5 用 Citrix Workspace アプリは、HDX を使用した Microsoft Teams の最適化において、背景のぼかしと背景効果をサポートしています。

背景をぼかしたり、デフォルトの画像に置き換えたりすることで、シルエット（体と顔）に会話を集中させ、予期せぬ邪魔を避けることができます。この機能はP2Pまたは電話会議で使用できます。

> **注:**
>
> この機能はMicrosoft TeamsのUI/ボタンと統合されています。マルチウィンドウのサポートは前提条件であり、VDAを2112以降にアップデートする必要があります。詳細については、「Multi-window meetings and chat」を参照してください。

> 背景のぼかしと効果に関するMicrosoft TeamsのUIコントロールには、以下の最小バージョンが必要です。

- Citrix Workspace アプリ Windows向け 2207

- Citrix Workspace アプリ Mac向け 2301
- Citrix Workspace アプリ Linux向け 2307
- ChromeOS 2303 用 Citrix Workspace アプリ

制限事項:

- クライアントは、背景画像をMicrosoft Teamsのデフォルト画像に置き換える間、インターネットに接続されている必要があります。
- 管理者およびユーザー定義の背景画像の置き換えは、Microsoft Teams UIではサポートされていません。カスタム背景画像は、画像がクライアントにも保存されている場合、クライアント上の構成設定を使用して構成できます。

カスタム背景画像の設定

以下のレジストリキーは、Microsoft Teams UI を使用して機能を制御する予定がない場合、または管理者がデフォルトの動作を上書きしたい場合にのみ必要です。たとえば、エンドポイントの性能が十分でないため、背景のぼかしを無効にする場合などです。

Windows の場合

カスタム背景画像を設定するには、管理者またはエンドユーザーがクライアントまたはエンドポイントで以下のレジストリキーを構成する必要があります。

場所: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- 名前: VideoBackgroundEffect
- 種類: DWORD
- 値: 0 (無効)、1 (有効)、2 (背景画像の置き換え)

値が 1 に設定されている場合、背景がぼかされます。この値は、エンドユーザーまたは管理者が設定できます。

値が 2 に設定されている場合は、**VideoBackgroundImage** キーも存在する必要があります。この値は管理者のみが設定できます。以下のキーは、背景画像を置き換えたい場合のみ必要であり、ぼかしには必要ありません。

- 名前: VideoBackgroundImage
- 種類: REG_SZ
- 値: my_image_name.jpeg

ビデオの背景画像は`C:\Program Files (x86)\Citrix\ICA Client`ディレクトリに存在する必要があります。

このレジストリ設定は、Microsoft Teams UIセレクターなしでCitrix Workspaceアプリ2206で背景のぼかしまたは画像の置き換えを有効にするためにも使用できます。つまり、環境またはVDAがマルチウィンドウをサポートしていない場合でも、Citrix Workspaceアプリ2206以降でHKCUレジストリの回避策を適用して同様の結果を得ることができますが、ユーザーはHDXセッション中またはMicrosoft Teams通話中に機能を制御することはできません。

レジストリキーの変更は、HDXセッションが接続したときにのみ有効になります。

Macの場合

ユーザーがダウンロードした画像の場所: */Users/username/Downloads/any_image.png*

カスタム画像をデフォルト画像として設定するには、次のコマンドを実行します。

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2
```

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "/Users/username/Downloads/any_image.png"
```

Linuxの場合

ユーザーがダウンロードした画像の場所: */home/username/Downloads/any_image.jpg*

ファイル */var/.config/citrix/hdx_rtc_engine/config.json* を作成し、以下の構成キーをJSON形式で追加します。例：

```
{


"VideoBackgroundEffect":2,


"VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"


}
```

HTML5の場合

1. **HTML5Client**フォルダー内の**configuration.js**ファイルに移動します。
2. **backgroundEffects**属性を追加し、属性を**true**に設定します。例:

```
'features' : {

    'msTeamsOptimization' :

    {

        'backgroundEffects' : true

    }

}
```

3. 変更を保存します。

クライアントCPU消費に関する考慮事項

ぼかし機能はCPUへの負荷が低いですが、消費量の増加が予想されます。たとえば、4コア、1.5 GHz Intel® Pentium® Silverチップ（TurboBoostで最大2.8 GHz）を搭載したシンクライアントでは、背景のぼかしによりCPU使用率が約2%増加します。平均CPU使用率は20%未満です。

Microsoft Teamsのギャラリービューとアクティブスピーカー

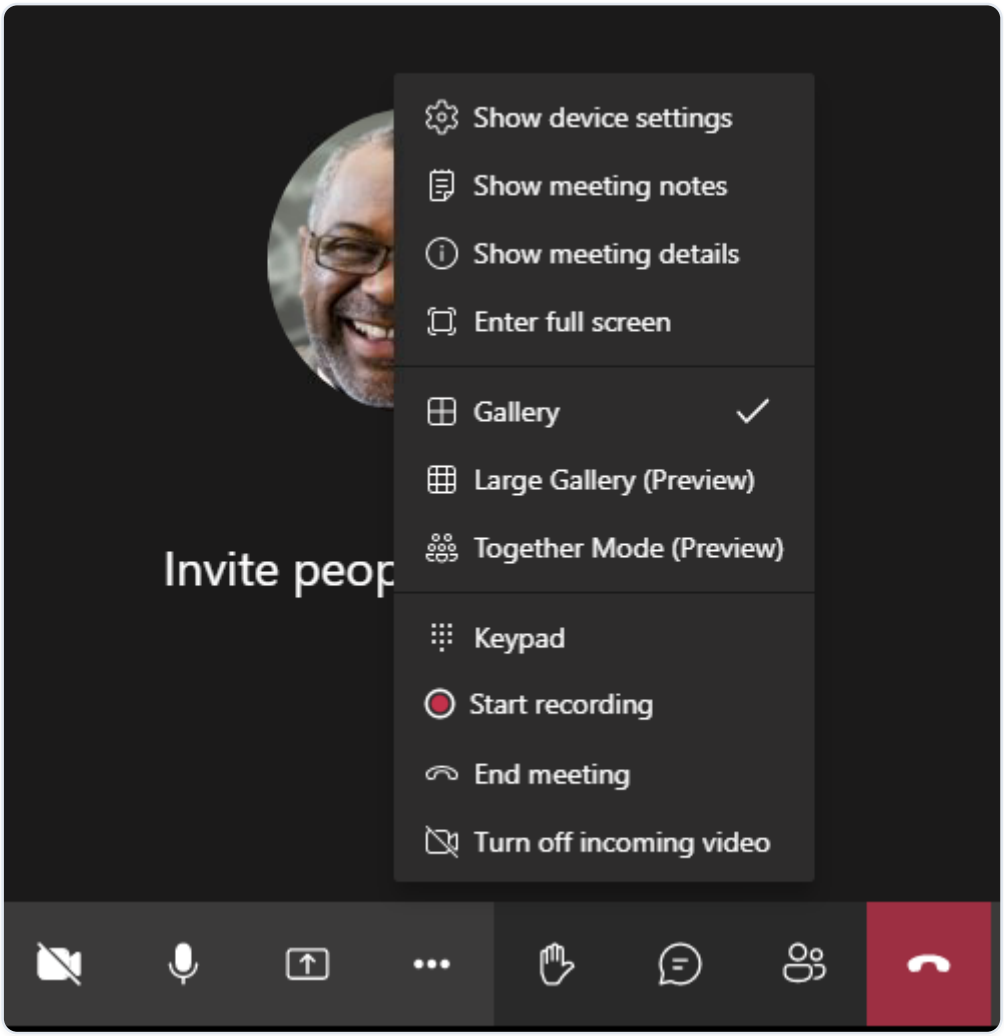
Microsoft Teamsは、**ギャラリー**、**大規模ギャラリー**、および**Together**モードのレイアウトをサポートしています。

Microsoft Teamsは、4人の参加者のビデオストリームを2x2のグリッドで表示します（**ギャラリー**として知られています）。この場合、Microsoft Teamsは4つのビデオストリームをクライアントデバイスに送信してデコードします。4人を超える参加者がビデオを共有している場合、画面には直近の最もアクティブな4人のスピーカーのみが表示されます。

Microsoft Teamsは、最大7x7のグリッドを持つ大規模ギャラリービューも提供します。その結果、Microsoft Teams会議サーバーは単一のビデオフィードを合成し、それをクライアントデバイスに送信してデコードするため、CPU消費量が低減されます。この単一のマトリックス形式のフィードには、ユーザーのセルフプレビュービデオも含まれる場合があります。

最後に、Microsoft Teamsは新しい会議エクスペリエンスの一部である**Together**モードをサポートしています。AIセグメンテーション技術を使用して参加者を共有背景にデジタル配置することで、Microsoft Teamsはすべての参加者を同じ講堂に配置します。

ユーザーは、会議中に省略記号メニューで**ギャラリー**、**大規模ギャラリー**、または**Together**モードのレイアウトを選択することで、これらのモードを制御できます。



ビデオアスペクト比の制約のサポート（Citrix Workspaceアプリ for Windows 2102、Citrix Workspaceアプリ for Linux 2106、Citrix Workspaceアプリ for MAC 2106以降）：

- **フレームに合わせる**オプションは、ギャラリー/大規模ギャラリービューで利用できます。このオプションは、ビデオサイズをサブウィンドウに収まるようにトリミングします。一方、**フレームにフィット**は、ビデオの側面に黒いバー（レターボックス）を表示するため、トリミングは行われません。

次の表は、ギャラリーレイアウトと大規模ギャラリーレイアウトの比較を示しています。

	ギャラリービュー 2X2 (デフォルト)	大規模ギャラリービュー
レイアウト / グリッド	4人の参加者のビデオストリームを含む2x2グリッドを表示します。画面には直近で最もアクティブな4人の発言者のみが表示され、他の参加者はグリッドに表示されません。	49人の参加者のビデオストリームを含む7x7グリッドを表示します。
ミキシング技術	メディアルーターは、各参加者からの個別のストリームをすべてのユーザーに転送します。	中央の会議サーバーは、すべてのオーディオまたはビデオをミキシングおよびトランスコードして、各参加者向けにカスタマイズされた複合レイアウトを作成します。この処理により、追加の遅延が発生する場合があります。
アクティブな発言者	新しいアクティブな発言者が、グリッド内で最もアクティブでない発言者と入れ替わります。	アクティブか非アクティブかに関わらず、すべての参加者を表示します。
エンドポイントでのエンコード	Simulcastが有効になっている場合、1つ以上のビデオストリームがエンドポイントでエンコードされることがあります。Simulcastのサポートに関する詳細については、Simulcastを参照してください。	Simulcastが有効になっている場合、1つ以上のビデオストリームがエンドポイントでエンコードされることがあります。Simulcastのサポートに関する詳細については、Simulcastを参照してください。
エンドポイントでのデコード	各参加者は最大4つの個別のメディアストリームを受信します。これにより、HdxRtcEngine.exeによるエンドポイントでのCPU消費量が増加します（デコード/レンダリングのため）。	各参加者は、オーディオとビデオの単一ストリームのみを受け取ります。この設定により、エンドポイントでのCPU消費が削減されます。

	ギャラリービュー 2X2 (デフォルト)	大規模ギャラリービュー
最大解像度	720p。4人の参加者がビデオを共有している場合、最大解像度はビデオフィードあたり360pです。4人未満の参加者がビデオを共有している場合、ビデオフィードあたりの解像度は高くなる可能性があります。	複合レイアウトまたはミキシングの場合は720p。複合レイアウトでは、参加者ごとに高品質のビデオストリームは必要ありません。この条件により、各送信者は解像度またはアップロードビットレートを削減します。
「低速ユーザー」の問題	送信者は、各モダリティ（オーディオ/ビデオ/画面共有）の品質を、参加者間の最低共通ネットワーク品質に調整します。このマルチメディアストリームは、他のすべての参加者に転送されます。結果として、ネットワーク状態の悪い参加者は、通話中の他の全員の品質に影響を与えます。	最低共通ネットワーク品質のシナリオの影響を受けにくい。会議サーバーは、個々の参加者のネットワーク状態に基づいて異なる品質を提供します。
セルフプレビュー	自分自身を小さなサムネイルでリアルタイムに表示します。	自分自身をサムネイルで表示し、他のビデオフィードと混合します。結果として、メインのビデオレイアウトに自分自身が追加の遅延とともに含まれて表示されることがあります。

Microsoft Teamsでの画面共有

Microsoft Teamsは、ビデオベースの画面共有（VBSS）に依存しており、共有されているデスクトップをH264などのビデオコーデックで効率的にエンコードし、高精細ストリームを作成します。HDX最適化を使用すると、受信する画面共有はビデオストリームとして扱われます。

Windows、Linux、Mac向けのCitrix Workspaceアプリ2109以降、およびChromeOS向けのCitrix Workspaceアプリ2303以降では、ユーザーは画面とビデオカメラを同時に共有できます。

以前のバージョンでは、ビデオ通話中に相手がデスクトップの共有を開始すると、元のカメラビデオフィードは一時停止されます。代わりに、画面共有ビデオフィードが表示されます。その後、相手は手動でカメラ共有を再開する必要があります。

PowerPoint Liveに関する注意

PowerPoint Liveからコンテンツを共有している場合、この制限は存在しません。その場合、他のピアは引き続きあなたのウェブカメラとコンテンツを見ることができ、他のスライドを確認するために前後に移動できます。このシナリオでは、スライドはVDAでレンダリングされます。PowerPoint Liveのスライドデッキにアクセスするには、「Share tray」ボタンをクリックして提案されたPowerPointスライドのいずれかを選択するか、「Browse」をクリックしてコンピューターまたはOneDriveでPowerPointファイルを見つけます。

送信画面共有も最適化され、Citrix Workspaceアプリにオフロードされます。この場合、メディアエンジンはCitrix Desktop Viewer (CDViewer.exe) ウィンドウのみをキャプチャして送信し、その周囲に赤い枠線が描画されます。Desktop Viewerと重なっているローカルアプリケーションはキャプチャされません。

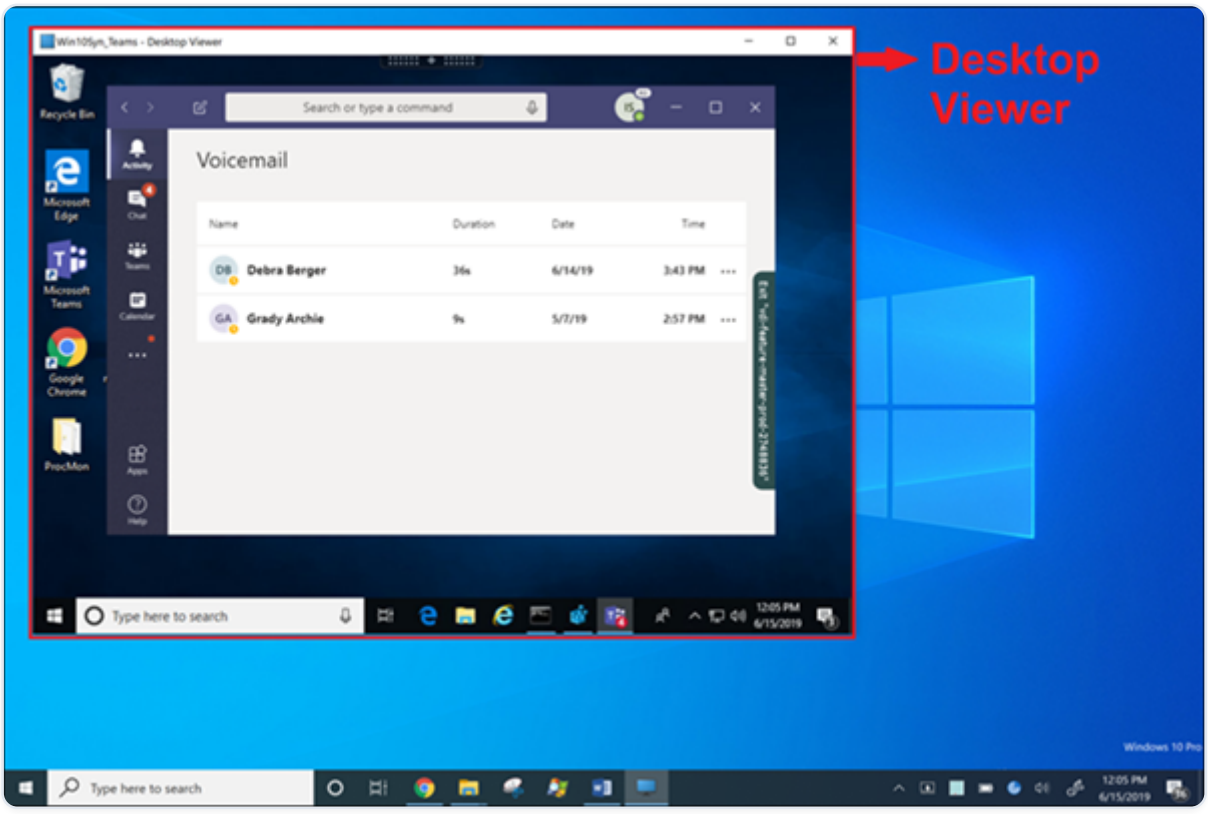
注

Mac版Citrix Workspaceアプリで画面共有を有効にするには、特定の権限を設定します。詳細については、システム要件を参照してください。

既知の制限:

- Desktop Viewerが無効になっている場合、またはDesktop Lockが使用されている場合、Microsoft Teamsの画面ピッカーでマルチモニター選択は利用できません。Desktop Viewerは、`.ICA`ファイルテンプレートを編集するか、`StoreFront web.config`によって無効にされる可能性があります。SHIFT+F2ホットキーはマルチモニター画面共有と互換性がありません。
- Workspaceアプリのバージョン2106より古い場合、プライマリモニターのみが共有されます。通話中の他のピアに見せるには、仮想デスクトップ内のアプリケーションをプライマリモニターにドラッグしてください。

- 仮想モニターレイアウト機能（単一の物理モニターの論理パーティション）でCitrix Workspaceアプリを設定した場合、マルチモニター画面共有が機能しない可能性があります。この場合、すべての仮想モニターは複合画像として共有されます。
- Windows版Citrix Workspaceアプリの古いバージョン（1907から2008まで）では、クライアントマシンで実行されているローカルアプリケーションも共有されます。この共有は、ローカルアプリがDesktop Viewerの上に重ねて表示されている場合にのみ可能です。この動作は2009.6以降および1912 CU5以降で削除されました。
- 画面共有中に、ウィンドウモードから全画面表示に切り替えると、画面共有が停止します。画面共有を機能させるには、一度停止してから再度共有する必要があります。
- 最適化されたMicrosoft Teamsでは、共有コントロールを特定の場所にピン留めすることはできません。
- 最小化されたアプリを共有すると、アプリのタイトルバーも共有される場合があります。



シームレスアプリケーションからの画面共有:

Microsoft Teamsをスタンドアロンのシームレスアプリケーションとして公開している場合、画面共有は物理エンドポイントのローカルデスクトップをキャプチャします。Citrix Workspaceアプリの最小バージョン1909が必要です。

アプリ共有

Citrix Workspaceアプリ for Windows 2112.1およびVDA 2112以降、Microsoft Teamsはアプリ共有をサポートしています。

Citrix Workspaceアプリ for Windows 2109、Mac 2203、Linux 2209およびVDA 2109以降、Microsoft Teamsは仮想セッションで実行されている特定のアプリの画面共有をサポートします。最適化されたMicrosoft Teamsを使用して、Javaなどのカスタム社内アプリケーションを共有することもできます。特定のアプリを共有するには：

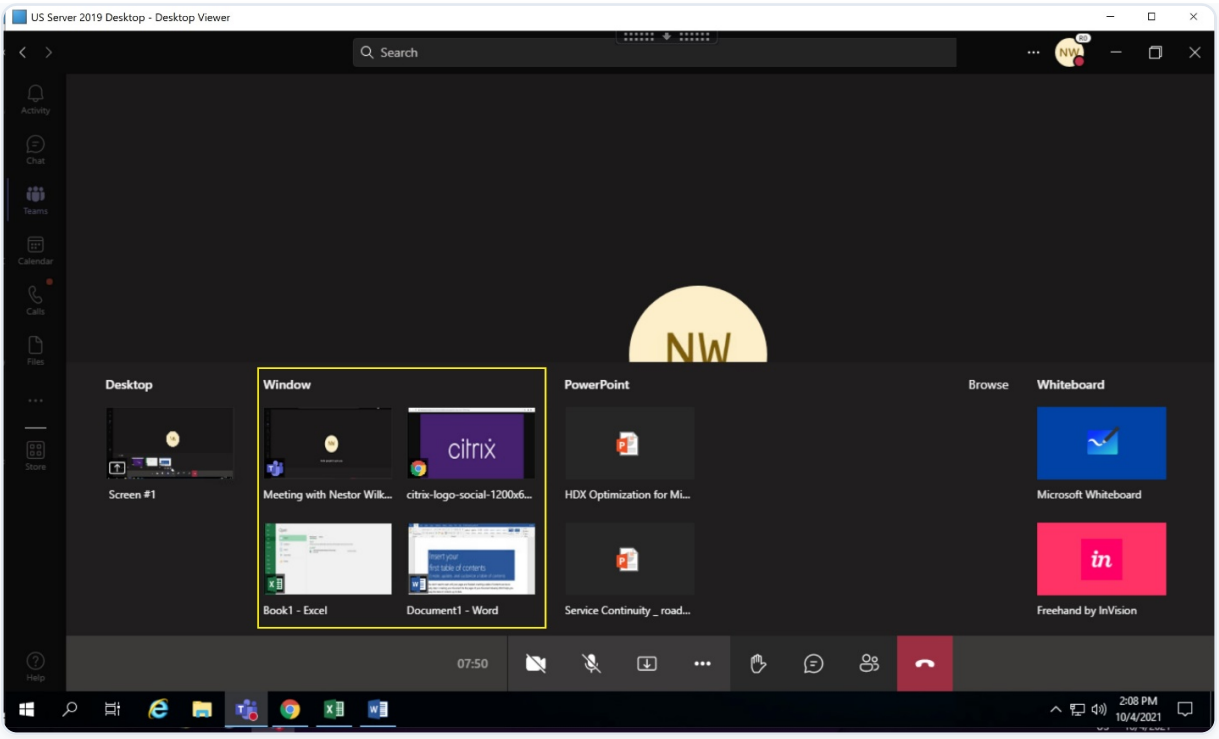
1. リモートセッション内でMicrosoft Teamsアプリに移動します。
2. Microsoft Teams UIで**コンテンツを共有**をクリックします。
3. 会議で共有するアプリを選択します。選択したアプリの周囲に赤い枠が表示され、通話中のピアは共有されたアプリを見ることができます。

別のアプリを共有するには、もう一度**コンテンツを共有**をクリックして、新しいアプリを選択します。

アプリ共有を無効にする場合は、VDAの`HKLM\SOFTWARE\Citrix\Graphics`に次のレジストリキーを作成します。 名前: `UseWsProvider` 種類: `DWORD` 値: 0

注:

- アプリを最小化すると、Microsoft Teamsは共有されたアプリの最後の画像を表示します。ウィンドウを最大化すると、画面共有を再開できます。
- 画面共有は、VDA側でのウィンドウのキャプチャに依存します。コンテンツは最大速度でCitrix Workspaceアプリに中継されます。最大速度は1秒あたり30フレームです。Citrix Workspaceアプリは、コンテンツをピアまたは会議サーバーに転送します。



特定のアプリの画面共有に関する既知の制限事項：

- アプリを画面共有している間、マウスカーソルは表示されません。
- アプリを共有中に最小化すると、画面ピッカーにはアプリのアイコンのみが表示されます。アプリのサムネイルは画面ピッカーにプレビューされません。アプリを最大化するまで、コンテンツを共有できず、赤い枠も表示されません。
- LAAアプリは、VDAの最適化されたMicrosoft Teamsでデスクトップアプリと共有できるアプリのリストを表示します。ただし、リストからアプリを選択しても、期待どおりの結果にならない場合があります。

アプリ保護との互換性 特定のアプリの画面共有は、HDX最適化されたMicrosoft Teamsのアプリ保護機能と互換性があります。アプリ保護が有効になっているデリバリーグループからアプリまたはデスクトップを起動した場合、特定のアプリの画面を共有できます。

Microsoft Teams UIで**コンテンツを共有**をクリックすると、スクリーンピッカーから**デスクトップ**オプションが削除されます。開いているアプリを共有するには、**ウィンドウ**オプションのみを選択できます。

> **注:**
>
> アプリ保護が有効になっているデリバリーグループからアプリまたはデスクトップを起動する場合、Citrix Workspaceアプリ for Windows 2202以前を使用していると、受信ビデオまたは画面共有を表示できません。

Microsoft Teamsで制御を付与および要求する

この機能は、Citrix Workspaceアプリの以下のバージョンでサポートされています（VDAバージョンやオペレーティングシステム、シングルセッションまたはマルチセッションには依存しません）。

- Citrix Workspaceアプリ for Windows バージョン2112.1以降
- Citrix Workspaceアプリ for Mac バージョン2203.1以降
- Citrix Workspaceアプリ for Linux バージョン2203以降
- ChromeOS 版 Citrix Workspace アプリ バージョン 2303 以降

Microsoft Teams通話中に参加者が画面を共有している場合、制御を要求できます。制御を取得すると、共有画面に対して選択、編集、その他のキーボードおよびマウス操作を行うことができます。

画面が共有されているときに制御を取得するには、Microsoft Teams UIの**制御を要求**ボタンをクリックします。画面を共有している会議参加者は、要求を許可または拒否できます。

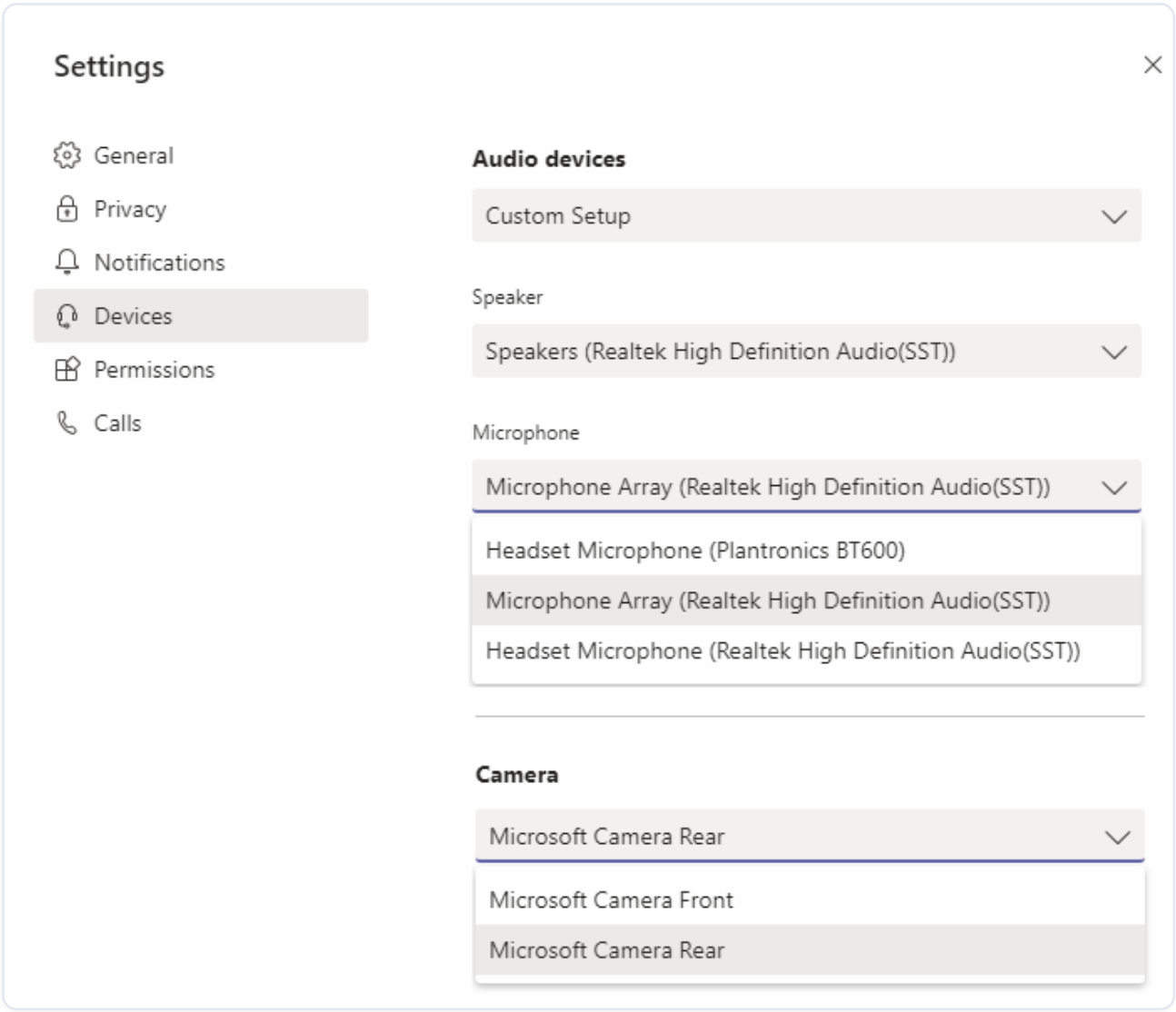
制御している間は、共有画面に対して選択、編集、その他の変更を行うことができます。これらの操作には、キーボードとマウスの両方を使用できます。完了したら、**制御を要求**をクリックします。

制限事項:

- ユーザーが単一のアプリを共有している場合（アプリ共有とも呼ばれます）、「制御を要求」および「制御を渡す」は利用できません。デスクトップ全体またはモニターを共有する必要があります。
- コントロールバーを特定の場所に固定する機能は利用できません。

Microsoft Teams の周辺機器

Microsoft Teams の最適化が有効な場合、Citrix Workspace アプリは周辺機器（ヘッドセット、マイク、カメラ、スピーカーなど）にアクセスします。その後、周辺機器は Microsoft Teams UI（**設定 > デバイス**）に適切に表示されます。



Microsoft Teams はデバイスに直接アクセスしません。代わりに、メディアの取得、キャプチャ、処理のために Workspace アプリの WebRTC メディアエンジンに依存します。Microsoft Teams は、ユーザーが選択できるようにデバイスを一覧表示します。

Microsoft Teams のアクティブ中に挿入された周辺機器は、デフォルトでは選択されません。Microsoft Teams UI の **設定** > **デバイス** 画面から周辺機器を手動で選択する必要があります。周辺機器が選択されると、Microsoft Teams はその周辺機器の情報をキャッシュします。その結果、同じエンドポイントからセッションに再接続すると、周辺機器が自動的に選択されます。

推奨事項:

- エコーキャンセリング機能が内蔵された Microsoft Teams 認定ヘッドセット。マイクとスピーカーが別々のデバイスにある追加の周辺機器を使用するセットアップでは、エコーが発生する可能性があります。たとえば、内蔵マイク付きのウェブカメラとスピーカー付きのモニターなどです。外部スピーカーを使用する場合は、マイクからできるだけ離して配置してください。また、音をマイクに屈折させる可能性のある表面からも離して配置してください。詳細につい

ては、`www.microsoft.com` にアクセスし、Microsoft Teams 認定ヘッドセットを検索してください。

- Microsoft Teams 認定カメラ。ただし、Skype for Business 認定周辺機器も Microsoft Teams と互換性があります。詳細については、<www.microsoft.com> にアクセスし、Microsoft Teams 認定カメラと Skype for Business 認定周辺機器を検索してください。
- Citrix Workspace アプリのメディアエンジンは、オンボード H.264 エンコーディング（UVC 1.1 および 1.5）を実行するウェブカメラで CPU オフロードを利用できません。

注:

Windows 用 Workspace アプリ 2009.6 は、24 ビットまたは 96 kHz を超える周波数のオーディオ形式を持つ周辺機器を取得できるようになりました。

HdxTeams.exe（Windows 用 Citrix Workspace アプリ 2009 以前）は、以下の特定のオーディオデバイス形式（チャンネル、ビット深度、サンプルレート）のみをサポートします。

- 再生デバイス: 最大 2 チャンネル、16 ビット、最大 96,000 Hz の周波数
- 録音デバイス：最大4チャンネル、16ビット、最大96,000 Hzの周波数

スピーカーまたはマイクのいずれかが予期される設定と一致しない場合でも、Microsoft Teamsでのデバイス列挙は失敗し、**設定 > デバイス**の下に**なし**と表示されます。

HdxTeams.exeの**Webrpc**ログには、この種類の情報が表示されます。

`Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing...`.

`Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't create audio module!` !

回避策として、特定のデバイスを無効にするか、次のいずれかを実行します。

1. **サウンドコントロールパネル** (mmsys.cpl) を開きます。

2. 再生または録音デバイスを選択します。
3. **プロパティ > 詳細**に移動し、設定をサポートされているモードに変更します。

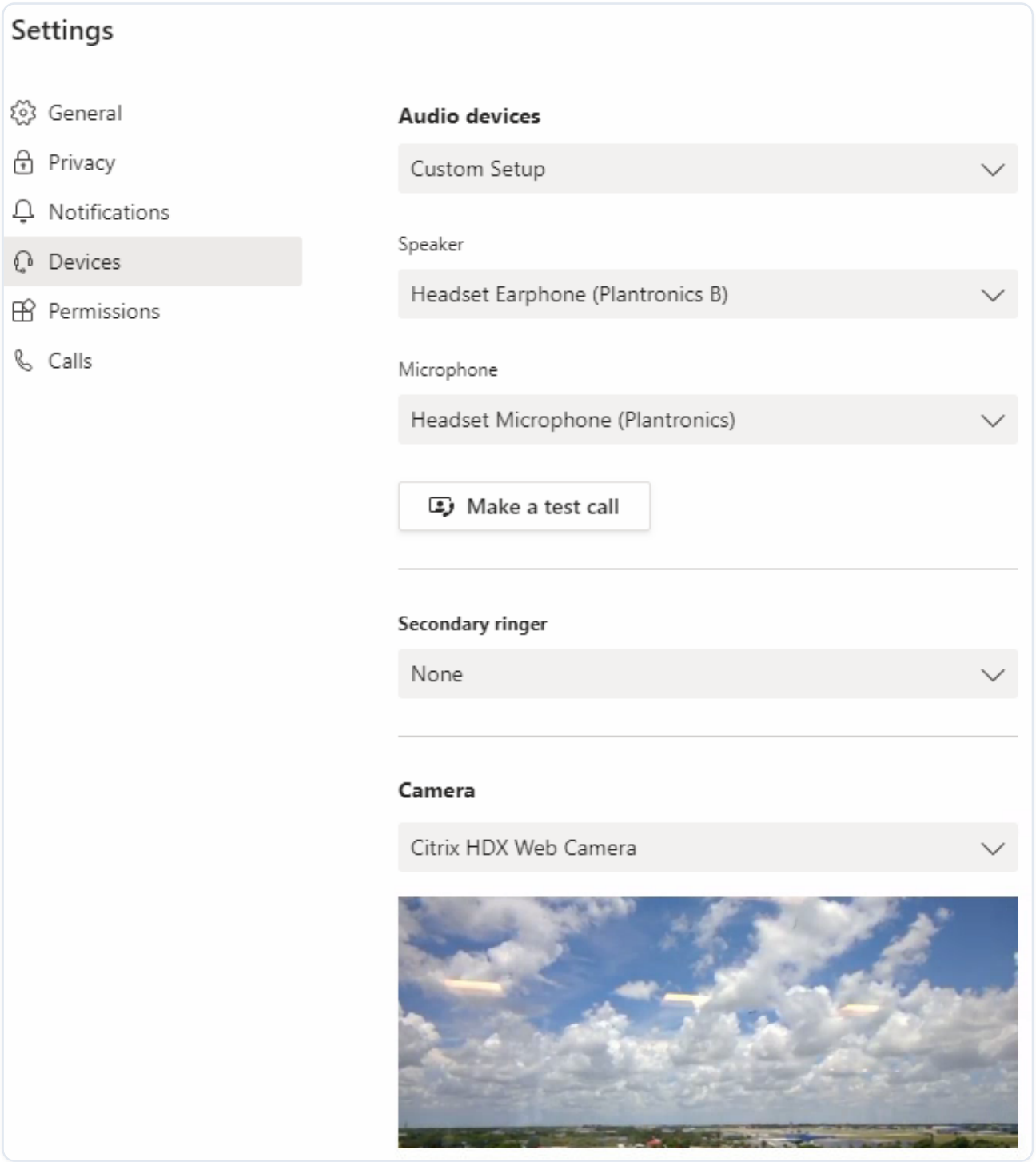
フォールバックモード

Microsoft Teamsが最適化されたVDIモード（Microsoft Teams/バージョン情報/バージョンで「Citrix HDX Not Connected」と表示される場合）でロードに失敗すると、VDAはレガシーHDXテクノロジーにフォールバックします。レガシーHDXテクノロジーには、Webカメラのリダイレクト、クライアントオーディオ、マイクのリダイレクトなどがあります。Microsoft Teamsの最適化をサポートしないWorkspaceアプリのバージョン/プラットフォームOSを使用している場合、フォールバックレジストリキーは適用されません。 フォールバックモードでは、周辺機器はVDAにマッピングされます。周辺機器は、仮想デスクトップにローカルで接続されているかのようにMicrosoft Teamsアプリに表示されます。

VDAでレジストリキーを設定することにより、フォールバックメカニズムをきめ細かく制御できるようになりました。詳細については、レジストリを介して管理される機能のリストにあるMicrosoft Teamsフォールバックモードを参照してください。

この機能には、Microsoft Teamsバージョン1.3.0.13565以降が必要です。

Microsoft Teamsアプリの**設定 > デバイス**タブで、最適化モードか非最適化モードかを判断するには、カメラ名が主な違いとなります。Microsoft Teamsが非最適化モードでロードされると、レガシーHDXテクノロジーが起動します。Webカメラ名には、次の図に示すように**Citrix HDX**のサフィックスが付いています。スピーカーとマイクのデバイス名は、最適化モードと比較してわずかに異なる（または切り詰められる）場合があります。



レガシー HDX テクノロジーが使用されている場合、Microsoft Teams はオーディオ、ビデオ、画面共有の処理をエンドポイントの Citrix Workspace アプリ WebRTC メディアエンジンにオフロードしません。代わりに、HDX テクノロジーはサーバー側レンダリングを使用します。ビデオをオンにすると、VDA で高い CPU 消費が予想されます。リアルタイムオーディオのパフォーマンスは最適ではない可能性があります。

既知の制限事項

Citrixの制限事項

Citrix Workspaceアプリの制限事項：

- HIDボタン - 通話の応答と終了はサポートされていません。音量の上げ下げはサポートされています。
- Microsoft Teamsの管理センターにおけるQoS設定は、VDIユーザーには適用されません。
- VDAでSnipping Toolを使用している間は、Microsoft Teamsコンテンツのスクリーンショットを撮ることはできません。ただし、クライアント側でSnipping Toolを使用した場合、コンテンツをキャプチャできます。

VDAの制限事項：

- **Citrix Workspace アプリの高 DPI** 設定を `Yes` に構成すると、リダイレクトされたビデオウィンドウがずれて表示されます。この制限は、モニターの DPI スケーリング係数が 100% を超える値に設定されている場合に発生します。

Citrix Workspace アプリと VDA の制限事項:

- 最適化された通話の音量は、クライアントマシンの音量バーを使用してのみ制御できます。VDAでは制御できません。

サイマルキャスト

最適化されたMicrosoft Teamsビデオ会議通話のサイマルキャストサポートは、WindowsおよびMacで有効になっています。Linuxについては、シンクライアントベンダーにご確認ください。 サイマルキャストを使用すると、すべての通話者にとって最適な通話体験のために適切な解像度に調整することで、異なるエンドポイント間でのビデオ会議通話の品質とエクスペリエンスが向上します。

この改善されたエクスペリエンスにより、各ユーザーは、エンドポイントの機能、ネットワークの状態など、いくつかの要因に応じて、異なる解像度（たとえば、720p、360pなど）で複数のビデオストリームを配信できます。受信側のエンドポイントは、処理できる最大品質の解像度を要求し、それによってすべてのユーザーに最適なビデオエクスペリエンスを提供します。

> **注:**
>
> この機能は、Microsoft Teamsからのアップデートが展開された後にのみ利用可能です。ETAについては、`<https://www.microsoft.com/>` にアクセスし、Microsoft 365ロードマップ

を検索してください。Microsoftによってアップデートが展開されたら、ドキュメントの更新と発表についてはCTX253754 を確認してください。

Microsoftの制限事項

- 3x3ギャラリービューはサポートされていません。Microsoft Teamsの依存関係 – 3x3グリッドの提供時期についてはMicrosoftにお問い合わせください。
- Skype for Businessとの相互運用性は音声通話に限定されており、ビデオモダリティは利用できません。
- 送受信ビデオストリームの最大解像度は720pです。
- PSTN通話の呼び出し音はサポートされていません。
- ダイレクトルーティングのメディアバイパスはサポートされていません。
- ブロードキャストおよびライブイベントのプロデューサーとプレゼンターの役割はサポートされていません。参加者の役割はサポートされていますが、最適化されていません（代わりにVDAでレンダリングされます）。
- Microsoft Teamsのズームインおよびズームアウト機能はサポートされていません。
- ロケーションベースルーティングとメディアバイパスはサポートされていません。
- 通話のマージはサポートされていません（ユーザーインターフェイスにオプションが表示されません）。

CitrixとMicrosoftの制限事項

- 画面共有を行う際、**システムオーディオを含める**オプションは利用できません。
- サイマルキャストはChromeOSではサポートされていません。

今後のMicrosoft Teamsシングルウィンドウ EOL

January 31, 2024に、Microsoftは、VDI Microsoft Teams最適化を使用する際のシングルウィンドウUIに対するMicrosoft Teamsのサポートを終了し、マルチウィンドウエクスペリエンスのみをサポートします。Microsoftは、9/8/2023にM365管理者センター（投稿ID: MC674419）でこの非推奨化について通知しました。 マルチウィンドウ機能に関する公開されている詳細は、Tech Communityの記事: New Meeting and Calling Experience in Microsoft Teamsで確認できます。

注:

Citrixは、ビデオおよび画面共有のために最適化されたモードでMicrosoft Teamsを引き続き使用するために、VDAとCitrix Workspaceアプリをサポートされているバージョンにアップグレードすることを推奨します。インフラストラクチャとエンドポイントをマルチウィンドウをサポートするようにアップグレードしない場合、通話、ビデオ通話、および画面共有は最適化されなくなります。これにより、通話品質の問題、レイテンシーの増加、およびサーバーへの負荷の増加が発生する可能性があります。

以下の表は、Citrix VDIでMicrosoft Teamsの最適化された通話を継続して使用するために必要なVDAおよびCitrix Workspaceアプリの最小バージョン、LTSRバージョン、および推奨バージョンを示しています。

コンポーネント	最小バージョン (1)	LTSRサポートバージョン (2)	推奨バージョン (3)
マイクロソフト チームズ	1.5.00.11865	該当なし	最新
VDA	1912 CU6 LTSR、2109 CR、2203 LTSR	1912 CU8+、2203 LTSR CU2+ (4)	2308 CR+
Windows向けCitrix Workspaceアプリ	2112.1 CR	2203 CU2+ (4)	2309 CR+
Mac向けCitrix Workspaceアプリ	2203 CR	該当なし	2308 CR+
Linux向けCitrix Workspaceアプリ	2202 CR	該当なし	2308 CR+
ChromeOSまたはHTML5向けCitrix Workspaceアプリ	2303 CR	該当なし	2309 CR+

注:

1. 最小バージョン: これはマルチウィンドウが最初に導入されたバージョンです。ここに記載されている最小バージョンの一部は、サポート終了となっている場合があります。

2. LTSRサポート対象バージョン: これは、Citrixがマルチウィンドウ向けにサポートしているLTSRバージョンです。これらのLTSRリリースの古いバージョンは動作する可能性がありますが、新しいLTSR CUバージョンがリリースされると、それらのバージョンに対するサポートは利用できなくなります。LTSRサポートポリシーの詳細については、`<https://support.citrix.com/article/CTX205549/faq-citrix-virtual-apps-and-desktops-and-citrix-hypervisor-long-term-service-release-ltsr>`を参照してください。
3. 推奨バージョン: これは、ユーザー/顧客がソフトウェアのアップグレードを選択した場合にCitrixが推奨するソフトウェアのバージョンです。これらはすべてCRバージョンです。
4. VDAおよびCWAベースバージョンのバージョン2203 LTSRには、マルチウィンドウ機能が含まれています。これらのバージョンは、公式にサポートされている最新のCUに置き換えられています。お客様は、これらのサポート対象外のバージョンを自己責任で引き続き使用できます。Citrixは、LTSRリリースをご利用のお客様に最新のCUへのアップグレードを推奨しています。

WebRTCからのSDP形式（プランB）の非推奨のお知らせ

Citrixは、今後のリリースでWebRTCからの現在のSDP形式（プランB）のサポートを廃止する予定です。最適化されたMicrosoft Teams機能に対応するには、WebRTCでUnified Planを使用する必要があります。

影響を受ける製品

Citrix Workspaceアプリケーションの今後のリリースでは、Citrix Workspaceアプリの次期リリースを搭載したエンドポイントと、Citrix Workspaceアプリ2108以前のバージョンを搭載したエンドポイント間の通話はサポートされません。この通話の非互換性には、1912 LTSR Citrix Workspaceアプリクライアント（CWA）が含まれます。影響を受けるCWAクライアントは次のとおりです。

- Windows向けCitrix Workspaceアプリ
- Linux向け Citrix Workspace アプリ
- Mac向けCitrix Workspaceアプリ
- Chrome向けCitrix Workspaceアプリ

プランBの代替

Citrix Workspaceアプリのバージョンが2109より古い場合は、サポートされているバージョン（できれば最新のCRリリース）にアップグレードする必要があります。そうしないと、将来のリリースまたは新しいエンドポイントとの通話は接続に失敗します。フェデレーションパートナーがCitrix Workspaceをアップグレードしていない場合、将来のリリースとフェデレーション通信パートナー間の通話も完了しない可能性があります。

Citrix Workspaceアプリバージョン2108は2023年3月にサポート期限が終了しており、新しいバージョンにアップグレードする必要があります。詳細については、Citrix Workspaceアプリのバージョンサポートに関するWorkspaceアプリを参照してください。

プランBの廃止に関する詳細については、WebRTCのドキュメントを参照してください。

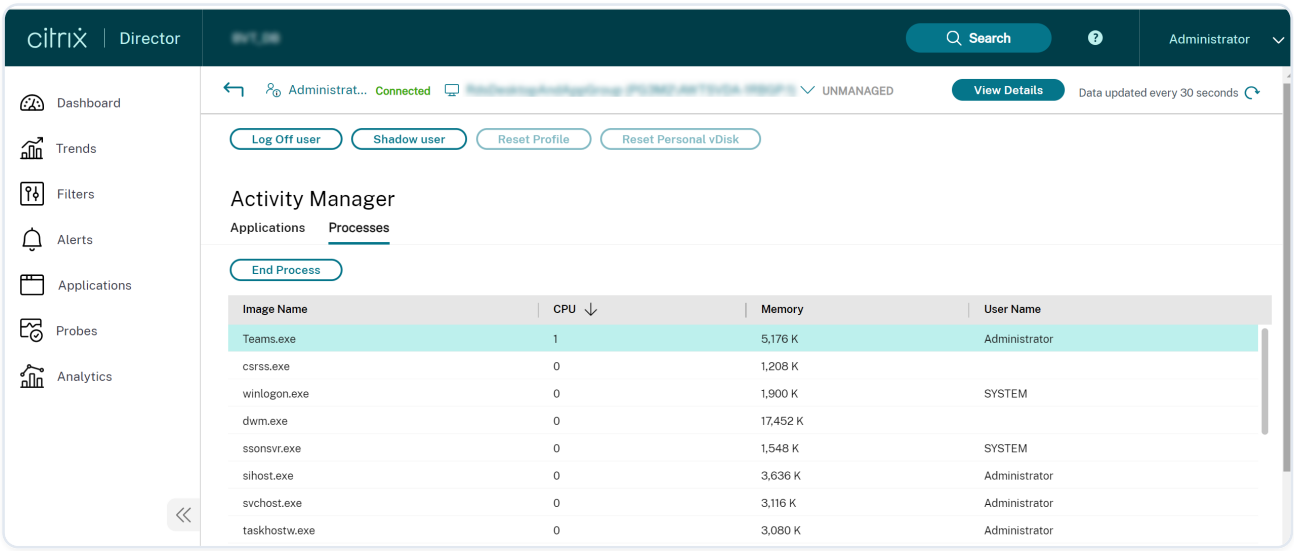
追加情報

- Microsoft Teams の監視、トラブルシューティング、サポート
- VM への Microsoft Teams デスクトップアプリの展開
- MSI を使用した Microsoft Teams のインストール (VDI インストールセクション)
- シンクライアント
- Skype for Business ネットワーク評価ツール
- Microsoft Teams と Skype for Business の共存と相互運用性を理解する

Microsoft Teams の監視、トラブルシューティング、サポート

Teams の監視

このセクションでは、HDX を使用した Microsoft Teams の最適化を監視するためのガイドラインを説明します。 最適化モードで実行しており、`HdxRtcEngine.exe` がクライアントマシンで実行されている場合、VDA 上の `WebSocketAgent.exe` というプロセスがセッションで実行されています。アプリケーションを表示するには、Director の **Activity Manager** を使用します。



Microsoft Teams の最適化ステータスは、Director > **User Details** ページ > **Session Details** パネル > **MS Teams Optimization** フィールドで確認できます。Microsoft Teams が最適化されていることは、クリアなオーディオとビデオなど、より良いユーザーエクスペリエンスのために不可欠です。この機能は、VDA バージョン 2311 以降で利用可能です。サポートされている Citrix Workspace™ app のバージョンは、「Optimization for Microsoft Teams」に記載されています。Director は、Microsoft Teams が公開アプリケーションとして、または公開デスクトップ内で実行されている場合にのみ、Microsoft Teams の最適化ステータスを表示します。 詳細については、「Microsoft Teams の最適化ステータス」を参照してください。

VDA の最小バージョン 1912 を使用すると、Citrix HDX Monitor (最小バージョン 3.11) を使用してアクティブな Teams 通話を監視できます。Citrix Virtual Apps and Desktops 製品 ISO には、フォルダー `layout\image-full\Support\HDX Monitor` に最新の `hdxmonitor.msi` が含まれています。 VDA の最小バージョン 1912 を使用すると、Citrix HDX Monitor (最小バージョン 3.11) を使用してアクティブな Microsoft Teams 通話を監視できます。Citrix Virtual Apps and Desktops 製品 ISO には、フォルダー `layout\image-full\Support\HDX Monitor` に最新の `hdxmonitor.msi` が含まれています。

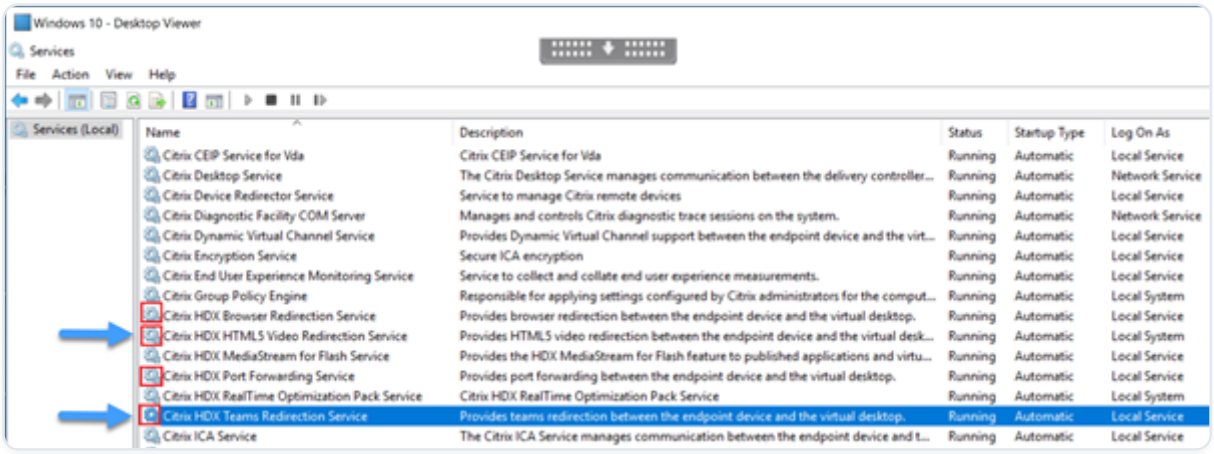
詳細については、Knowledge Center の記事 CTX253754 の「*監視*」を参照してください。

トラブルシューティング

このセクションでは、Microsoft Teams の最適化を使用する際に発生する可能性のある問題のトラブルシューティングのヒントを提供します。詳細については、CTX253754 を参照してください。

仮想配信エージェント上で

BCR_x64.msi によって 4 つのサービスがインストールされます。VDA での Microsoft Teams リダイレクトを担当するのはそのうちの 2 つだけです。



- **Citrix HDX Teams Redirection Service** は、Microsoft Teams で使用される仮想チャネルを確立します。このサービスは CtxSvcHost.exe に依存しています。
- **Citrix HDX HTML5 Video Redirection Service** は、127.0.0.1:9002 TCP でリッスンする WebSocketService.exe として実行されます。WebSocketService.exe は、主に次の 2 つの機能を実行します。

  i. **セキュアな WebSocket のための TLS 終端** は、Microsoft Teams アプリ内のコンポーネントである vdiCitrixPeerConnection.js からセキュアな WebSocket 接続を受信します。これは Process Monitor で追跡できます。証明書の詳細については、セクション (TLS と HTML5 ビデオリダイレクト、およびブラウザコンテンツリダイレクト) を参照してください。

  一部のアンチウイルスおよびデスクトップセキュリティソフトウェアは、`WebSocketService.exe` とその証明書の適切な機能に干渉します。Citrix HDX HTML5ビデオリダイレクトサービスが `services.msc` コンソールで実行されている場合でも、netstatで確認すると、localhost `127.0.0.1:9002` TCPソケットがリスニングモードになっていないことがあります。サービスを再起動しようとすると、ハングアップします（「停止中...」）。`WebSocketService.exe` プロセスに適切な除外設定を適用してください。

  「プロセスモニター」(/en-us/citrix-virtual-apps-desktops/2407/media/team-process-monitor.png)

  ii. **ユーザーセッションマッピング。**Microsoft Teamsアプリケーションが起動すると、WebSocketService.exeはVDAのユーザーセッションでWebSocketAgent.exeプロセスを開始します。WebSocketService.exeは、LocalSystemアカウントとしてセッション0で実行されます。

  「WebSocketAgent.exeサービス」(/en-us/citrix-virtual-apps-desktops/2407/media/websocketservice-websocketagent.png)

  VDAでWebSocketService.exeサービスがアクティブなリッスン状態にあるかどうかを確認するには、`netstat` を使用できます。

昇格されたコマンドプロンプトウィンドウから`netstat -anob -p tcp`を実行します。

```
 TCP    127.0.0.1:9001         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
 TCP    127.0.0.1:9002         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
```

接続が成功すると、状態はESTABLISHEDに変わります。

「netstatの成功例」(/en-us/citrix-virtual-apps-desktops/2407/media/teams-netstat-success.png)

重要:

WebSocketService.exeは、127.0.0.1:9001と127.0.0.1:9002の2つのTCPソケットでリッスンします。ポート9001は、ブラウザコンテンツリダイレクトとHTML5ビデオリダイレクトに使用されます。ポート9002は、Microsoft Teamsリダイレクトに使用されます。Teams.exeとWebSocketService.exe間の直接通信を妨げる可能性のあるプロキシ設定がVDAのWindows OSにないことを確認してください。Internet Explorer 11で明示的なプロキシ（**インターネットオプション > 接続 > LAN の設定 > プロキシサーバー**）を設定すると、接続が割り当てられたプロキシサーバーを経由する場合があります。手動および明示的なプロキシ設定を使用する場合は、**ローカルアドレスにはプロキシサーバーを使用しない**がチェックされていることを確認してください。

サービスの位置と説明

サービス	WINDOWS SERVER OSでの実行可能ファイルのパス	ログオンアカウント	説明
Citrix HTML5 ビデオリダイレクトサービス	"C:\Program Files (x86)\Citrix\System32\WebSocketService.exe" /service	ローカルシステムアカウント	仮想デスクトップとエンドポイントデバイス間でメディアリダイレクトを実行するために必要な初期フレームワークを、複数のHDXマルチメディアサービスに提供します。

サービス	WINDOWS SERVER OSでの実行可能ファイルのパス	ログオンアカウント	説明
Citrix HDX ブラウザコンテンツリダイレクトサービス	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g BrowserRedirSvcs	このアカウント (ローカルサービス)	エンドポイントデバイスと仮想デスクトップ間でブラウザコンテンツリダイレクトを提供します。
Citrix ポートフォワーディングサービス	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g PortFwdSvcs	このアカウント (ローカルサービス)	ブラウザコンテンツリダイレクトのために、エンドポイントデバイスと仮想デスクトップ間でポートフォワーディングを提供します。
Citrix HDX Teams リダイレクトサービス	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g TeamsSvcs	ローカルシステムアカウント	エンドポイントデバイスと仮想デスクトップ間でMicrosoft Teamsのリダイレクトを提供します。

シトリックス ワークスペース アプリ

ユーザーのエンドポイントでは、Windows版Citrix WorkspaceアプリがHdxTeams.exeまたはHdxRtcEngine.exeという新しいサービスをインスタンス化します。これは、VDAでMicrosoft Teamsが起動され、ユーザーがセルフプレビューで通話しようとしたり、周辺機器にアクセスしようとしたりするときに行われます。このサービスが表示されない場合は、以下を確認してください。

1. Windows版Workspaceアプリバージョン1905以降がインストールされていることを確認してください。WorkspaceアプリのインストールパスにHdxTeams.exeまたはHdxRtcEngine.exeとwebrpc.dllバイナリが表示されますか？
2. ステップ1を検証した場合は、HdxTeams.exeまたはHdxRtcEngine.exeが起動されているかどうかを確認するために、以下を実行してください。
    a. VDA上のMicrosoft Teamsを終了します。
    b. VDAでservices.mscを起動します。
    c. Citrix HDX Teamsリダイレクトサービスを停止します。

d. ICA®セッションを切断します。
e. ICAセッションに接続します。
f. Citrix HDX Teamsリダイレクトサービスを開始します。
g. Citrix HDX HTML5ビデオリダイレクトサービスを再起動します。
h. VDAでMicrosoft Teamsを起動します。

3. クライアントエンドポイントでHdxTeams.exeまたはHdxRtcEngine.exeがまだ起動されていない場合は、以下を実行してください。

a. VDAを再起動します。
b. クライアントエンドポイントを再起動します。

サポート

CitrixとMicrosoftは、Microsoft Teamsの最適化を使用して、Citrix Virtual Apps and Desktops™からMicrosoft Teamsを配信することを共同でサポートしています。この共同サポートは、両社間の緊密な連携の結果です。有効なサポート契約があり、このソリューションで問題が発生した場合は、問題の原因となっていると思われるコードのベンダーにサポートチケットをオープンしてください。つまり、TeamsについてはMicrosoft、最適化コンポーネントについてはCitrixです。 CitrixまたはMicrosoftがチケットを受け取り、問題をトリアージし、必要に応じてエスカレートします。各社のサポートチームに連絡する必要はありません。

問題が発生した場合は、Teams UIで** > **をクリックすることをお勧めします。VDA側のログは、技術的な問題をより迅速に解決するために、CitrixとMicrosoft間で自動的に共有されます。

ログの収集

HDXメディアエンジンログはユーザーのマシン上（VDA上ではない）にあります。問題が発生した場合は、サポートケースにログを添付してください。

Windowsログ：

Windowsログは、**HDXTeams**フォルダー（AppData/Local/Temp/HDXTeamsまたはAppData/Local/Temp/HdxRtcEngine）内の%TEMP%にあります。webrpc_Day_Month_timestamp_Year.txtという名前の.txtファイルを探してください。Citrix Workspaceアプリの新しいバージョン（Citrix Workspaceアプリ2009.5以降など）を使用している場合は、ログをAppData\Local\Temp\HdxRtcEngineに保存します。

各セッションは、ログ用に個別のフォルダーを作成します。

Macログ：

1. VDWEBRTCログ - 仮想チャネルの実行を記録します。

   場所：`/Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt`

2. HdxRtcEngineログ - HdxRtcEngine上のプロセスの実行を記録します。

   場所: `$TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log`

   HdxRtcEngineログはデフォルトで有効になっています。

3. Webrpcログ - webrtcライブラリのラップアップの実行を記録する最も重要なログです。

   場所: `/Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log`

Linuxログ：

Linuxログは`/tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/`フォルダーにあります。 Webrtcログ：`/tmp/webrpc/<current date>/webrtc.log` カーネルログ：`/var/log/syslog`

ICE/STUN/TURN/ログ：

通話を確立する際には、次の4つのICEフェーズが必要です。

- 候補収集
- 候補交換
- 接続チェック (STUNバインド要求)
- 候補昇格

HdxRtcEngine.exeログでは、以下のエントリが関連するInteractive Connectivity Establishment (ICE) エントリです。これらのエントリは、通話設定が成功するために必要です。収集段階のサンプルスニペットを以下に示します。

```
RPCStubs Info: -> device id = \\?
\display#int3470#4&1835d135&0&uid13424#{65e8773d-8f56-11d0-
a3b9-00a0c9223196}\{bf89b5a5-61f7-4127-a279-e187013d7caf} label =
Microsoft Camera Front groupId =



webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1

webrtcapi.RTCPeerConnection Info: setLocalDescription.
```

```
>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveLocalOffer



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Gathering



[…]

>>> begin:sdp

candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
generation 0 ufrag oVk6 network-id 1

<<< end:sdp

[…]

>>> begin:sdp

candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay raddr
73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1 network-cost
10

<<< end:sdp

[…]

>>> begin:sdp

candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx raddr
10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id 1

<<< end:sdp
```

```
[…]



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Complete
webrtcapi.RTCPeerConnection Info: setRemoteDescription.

>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveRemotelOffer
```

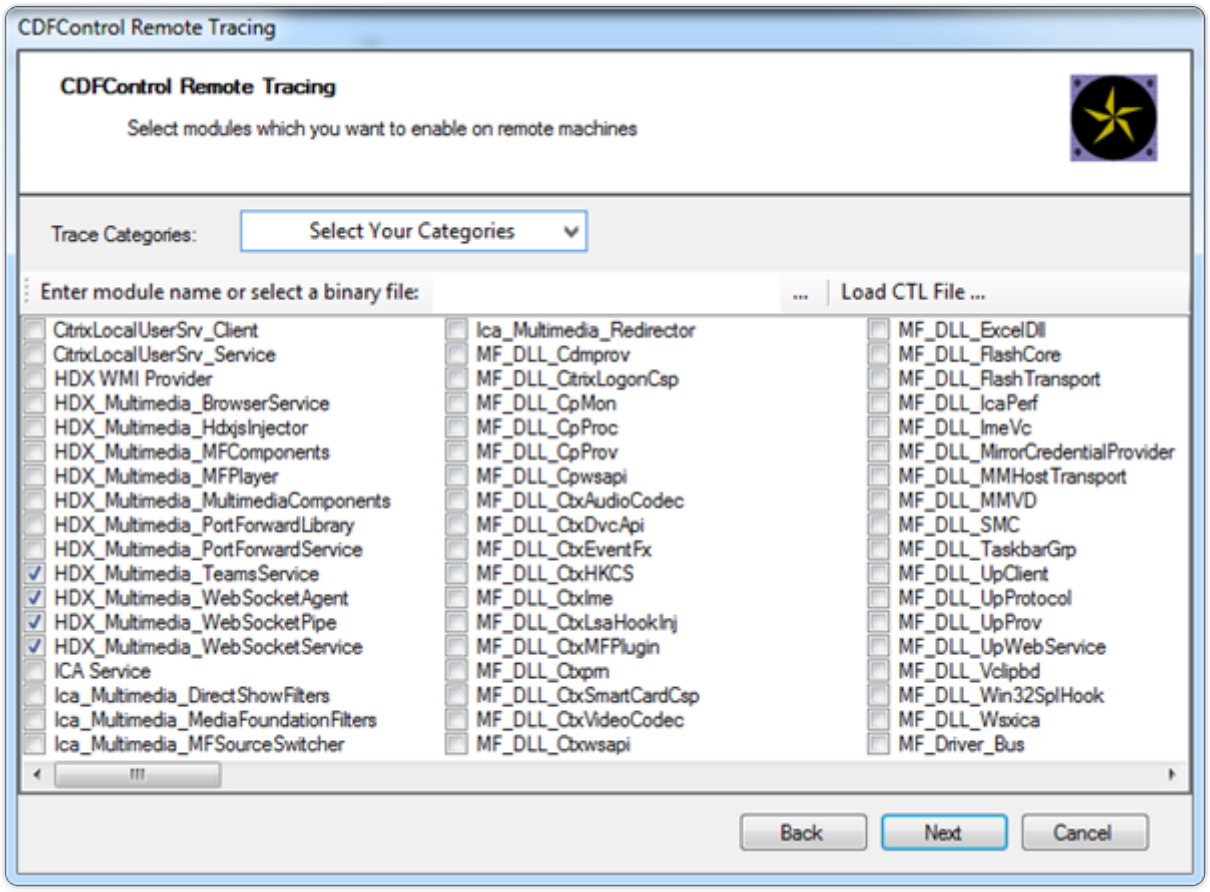
複数のICE候補がある場合、優先順位は次のとおりです。

1. ホスト
2. ピア反射型
3. サーバー反射型
4. トランスポートリレー

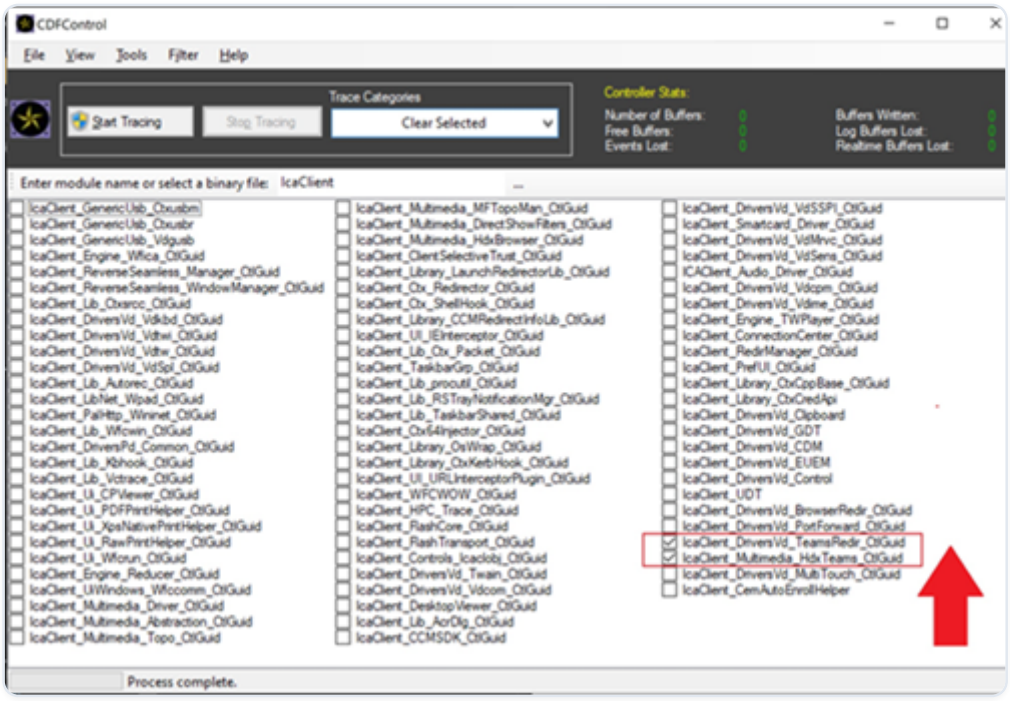
問題が発生し、それを一貫して再現できる場合は、Microsoft Teams で **ヘルプ > 問題の報告** をクリックすることをお勧めします。Microsoft にケースをオープンした場合、技術的な問題を解決するために、ログは Citrix と Microsoft の間で共有されます。 Citrix サポートに問い合わせる前に CDF トレースをキャプチャすることも有益です。詳細については、Knowledge Center の記事 CDFcontrol を参照してください。

CDF トレース収集の推奨事項については、Knowledge Center の記事 Recommendations for Collecting the CDF Traces を参照してください。

VDA 側の CDF トレース - 次の CDF トレースプロバイダーを有効にします。



Workspace アプリ側の CDF トレース - 次の CDF トレースプロバイダーを有効にします。



- IcaClient_DriversVd_TeamsRedir (オプション)
- IcaClient_Multimedia_HdxTeams (Citrix Workspace アプリ 2012 以降が必要)

Windows Media リダイレクト

Windows Media リダイレクトは、サーバーがストリーミングオーディオとビデオをユーザーに配信する方法を制御し、最適化します。メディアのランタイムファイルをサーバーではなくクライアントデバイスで再生することで、Windows Media リダイレクトは、マルチメディアファイルの再生に必要な帯域幅を削減します。Windows Media リダイレクトは、仮想Windowsデスクトップで実行されているWindows Media Playerおよび互換性のあるプレーヤーのパフォーマンスを向上させます。

Windows Media クライアント側コンテンツフェッチの要件が満たされない場合、メディア配信は自動的にサーバー側フェッチを使用します。この方法はユーザーには透過的です。使用されている方法を特定するには、Citrix Scoutを使用してHostMMTransport.dllからCitrix Diagnosis Facility (CDF) トレースを実行できます。詳しくは、「Citrix Scout」(/ja-jp/citrix-virtual-apps-desktops/2407/manage-deployment/cis/scout.html)を参照してください。

Windows Media リダイレクトは、ホストサーバーでメディアパイプラインをインターセプトし、メディアデータをネイティブの圧縮形式でキャプチャし、コンテンツをクライアントデバイスにリダイレクトします。その後、クライアントデバイスはメディアパイプラインを再構築して、ホストサーバーから受信したメディアデータを解凍およびレンダリングします。Windows Media リダイレクトは、Windowsオペレーティングシステムを実行しているクライアントデバイスでうまく機能します。これらのデバイスには、ホストサーバーに存在していたメディアパイプラインを再構築するために必要なマルチメディアフレームワークがあります。Linuxクライアントは、同様のオープンソースメディアフレームワークを使用してメディアパイプラインを再構築します。

ポリシー設定の**Windows Media リダイレクト**は、この機能を制御し、デフォルトで**許可**されています。通常、この設定により、サーバーからレンダリングされるオーディオおよびビデオの品質が、クライアントデバイスでローカルに再生されるコンテンツに匹敵するレベルに向上します。まれに、Windows Media リダイレクトを使用して再生されるメディアが、基本的なICA®圧縮と通常のオーディオを使用してレンダリングされるメディアよりも悪く見えることがあります。この機能を無効にするには、**Windows Media リダイレクト**設定をポリシーに追加し、その値を**禁止**に設定します。

ポリシー設定の詳細については、Multimedia policy settingsを参照してください。

制限事項:

セッション内でWindows Media PlayerとRemote Audio & Video Extensions (RAVE) を有効にしている場合、黒い画面が表示されることがあります。この黒い画面は、ビデオコンテンツを右クリックして**常に再生中を最前面に表示**を選択した場合に表示されることがあります。

仮想チャネルプラグインマネージャー

はじめに

仮想チャネルプラグインマネージャーは、指定されたアプリケーションのクライアントエンドポイント全体にプラグインを展開するように設計されています。プラグインマネージャーは、VDAで実行されている特定のアプリケーションを検出し、アプリケーションの実行時に最高の体験を得るために、エンドポイントにプラグインをインストールするようユーザーに促します。

ユーザーは、プラグインのインストール、スキップ、または拒否を選択できます。プラグインマネージャーは、管理対象か非管理対象かを問わず、すべてのエンドポイントでプラグインを管理する柔軟性を提供します。

例: Microsoft Teams は新しいアーキテクチャ (SlimCore Optimization) を採用しており、最適化を機能させるにはエンドポイントにプラグインをインストールする必要があります。仮想チャネルプラグインマネージャーは、エンドポイント全体にプラグインを展開できます。詳細については、Teams 向けの新しい VDI ソリューション を参照してください。

システム要件

仮想チャネルプラグインマネージャーの最小要件は次のとおりです。

- 仮想デスクトップエージェント (VDA)
  - 2411 CR
- DDC
  - クラウド 121 リリース
  - 2407 CR
- Citrix Workspace™ アプリ (Citrix Workspace アプリ)
  - Citrix Workspace アプリ Windows 用 2409

> **注:**
>
> この機能は現在、Windowsエンドポイントに適用可能です。

サポートされるアプリケーション

- 現在サポートされているアプリケーションは以下のとおりです。

- Microsoft Teams - Teams向け新しいVDIソリューションを参照してください

仮想チャネルプラグインマネージャーの概要

機能の理解

Citrix®は、お客様の環境が複雑になる可能性があり、管理対象および非管理対象のエンドポイント全体にプラグインを展開するにはかなりの労力が必要であることを理解しています。この機能は、そのプロセスを簡素化するように設計されています。

この機能には2つのコンポーネントが含まれています。1つはVDA側（検出プロセス）、もう1つはCitrix Workspace™ App側（インストーラープロセス）です。管理者が、ポリシーの有効化、レジストリエントリの作成、監視するアプリケーションの指定など、上記の前提条件を満たすと、次のようになります。

- VDA側の検出プロセスは、エンドユーザーが仮想デスクトップにログオンすると、アプリケーションの起動を監視します。
- 検出プロセスは、Citrix Workspace App側に、指定されたアプリケーションを最適化するために必要なプラグインをインストールするようユーザーに促すことを通知します。
- ユーザーは、プラグインに関する簡単な詳細情報が記載されたポップアップを画面で受け取ります。ユーザーは、プラグインをインストールするか、スキップするか、またはインストールしないことを選択できます。
  - ユーザーがインストールプロセスをスキップした場合、そのセッションではポップアップが再度表示されることはありません。インストールプロンプトは、セッションの再接続時に表示されます。
  - ユーザーがプラグインをインストールしないことを選択した場合、その選択は管理者による可視性のためにユーザープロファイルに記録されます。
- ユーザーがプラグインのインストールを選択した場合、Citrix Workspace App側はエンドポイントにプラグインをダウンロードしてインストールします。
  - インストールが成功すると、プラグインを有効にするためにセッションを再接続するようユーザーにメッセージが表示されます。ユーザーはすぐに再接続するか、成功メッセージを閉じて後で再接続するかを選択できます。
  - インストールが失敗した場合、ユーザーにはエラーメッセージが表示され、その失敗は管理者による可視性のために記録されます。

仮想チャネルプラグインマネージャーの構成

展開

1. Microsoft Teamsリダイレクトポリシーが有効になっているか確認します。詳細については、Microsoft Teamsリダイレクトポリシーを参照してください。

   このポリシーは、監視対象のアプリケーションに関係なく有効にする必要があります。将来、より多くのアプリケーションがサポートされ、Microsoft Teamsの代わりにそれらのアプリケーションを監視したい場合でも、このポリシーは有効にする必要があります。このポリシーはデフォルトで有効になっています。

2. 仮想チャネルプラグインマネージャーポリシーを有効にする必要があります。ポリシーを有効にする方法の詳細については、仮想チャネルプラグインマネージャーポリシー設定を参照してください。

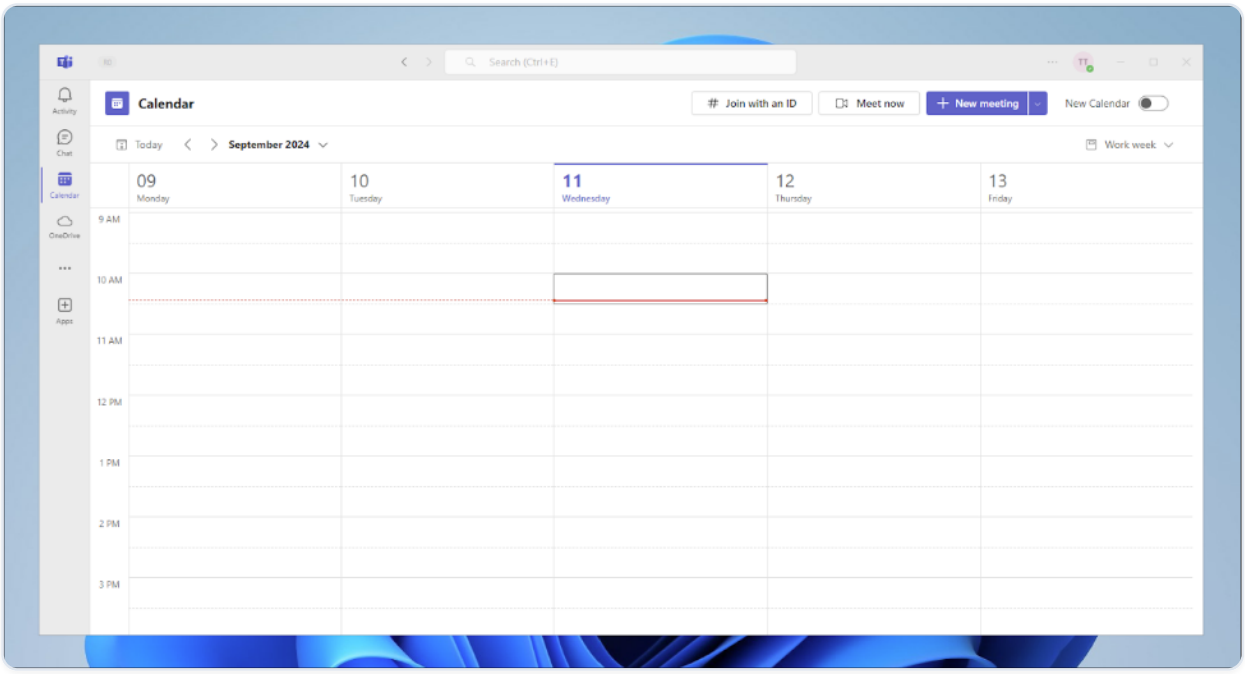
   このポリシーは、Citrix Studioのマルチメディアポリシー設定で利用できます。このポリシーを有効にすると、監視するアプリケーション名（例: 「Microsoft Teams」）を指定できます。このポリシーはデフォルトで無効になっています。

3. Citrix Workspace™アプリはシステム全体モードでインストールする必要があります。

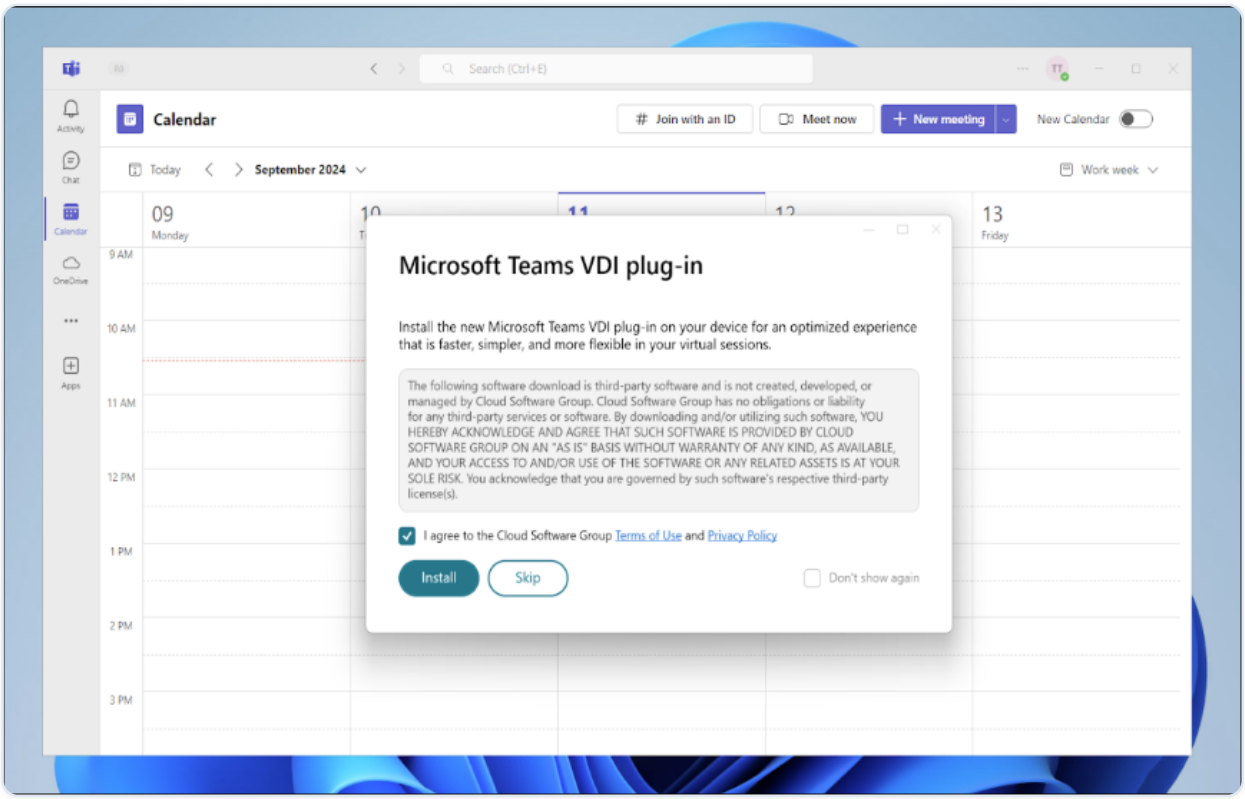
> **注:**
>
> プラグインは、サードパーティのCDNからエンドポイントにダウンロードされます。たとえば、Microsoft Teamsを選択した場合、プラグインはMicrosoft CDNからダウンロードされます。したがって、エンドポイントはサードパーティのCDNにアクセスできる必要があります。そうでない場合、プラグインのインストールは失敗します。

手順

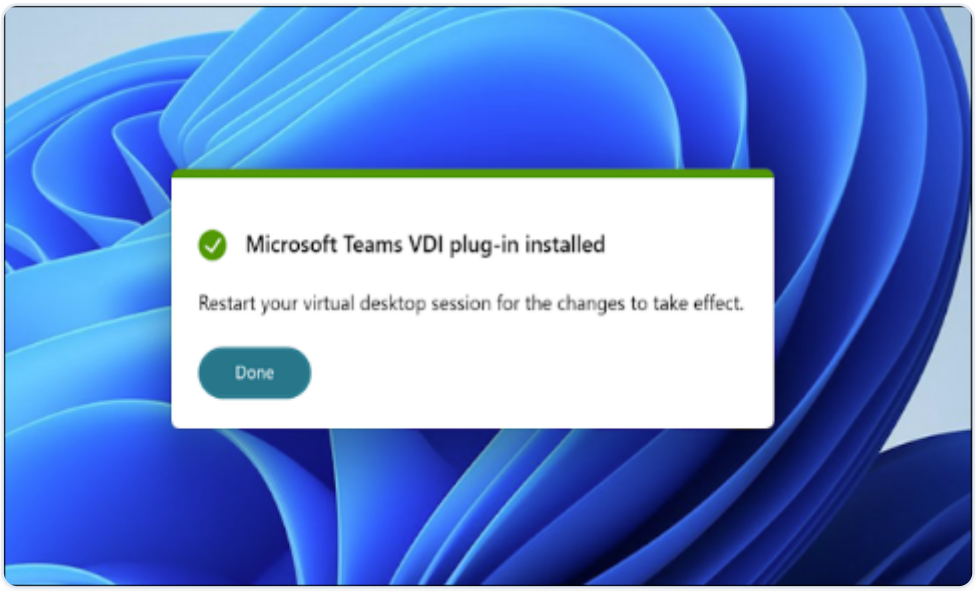
1. ユーザーはCitrixセッションでアプリケーションを起動します。例: Microsoft Teams。



2. ユーザーは、より良いエクスペリエンスのためにエンドポイントにTeams VDIプラグインをインストールするためのポップアップを受け取ります。プラグインはエンドポイントにインストールされるため、ポップアップはセッション内ではなくセッションの上に表示されます。



3. ユーザーがインストールボタンをクリックすると、プラグインがインストールされます。変更を有効にするには、仮想デスクトップセッションを再起動する必要があります。



既知の問題と制限事項

- 2407 VDAでは、機能を有効にするためにポリシーに加えて、VDA上で以下のレジストリ設定を1に設定する必要があります。このレジストリ設定は、2411 VDA以降では自動的に許可され、構成する必要はありません。

  `HKLM\SOFTWARE\Citrix\HDXMediaStream

  Name: EnableAppDetector Type: DWORD`

- 今後、さらに制限事項が追加されます。

一般的なコンテンツリダイレクト

クライアントフォルダーリダイレクト

クライアントフォルダーリダイレクトは、ホスト側のセッションでクライアント側のファイルにアクセスする方法を変更します。サーバーでクライアントドライブマッピングのみを有効にすると、クライアント側の完全なボリュームは、Universal Naming Convention (UNC) リンクとしてセッションに自動的にマッピングされます。サーバーでクライアントフォルダーリダイレクトを有効にし、ユーザーがユーザーデバイスでそれを構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

ユーザーが指定したフォルダーのみが、セッション内でUNCリンクとして表示されます。つまり、ユーザーデバイス上の完全なファイルシステムではなく。レジストリを介してUNCリンクを無効にすると、クライアントフォルダーはセッション内でマップされたドライブとして表示されます。

クライアントフォルダーリダイレクトは、WindowsシングルセッションOSマシンでのみサポートされています。

外部USBドライブのクライアントフォルダーリダイレクトは、デバイスの取り外しと再接続時に保存されません。

サーバーでクライアントフォルダーリダイレクトを有効にします。次に、クライアントデバイスで、リダイレクトするフォルダーを指定します。クライアントフォルダーオプションを指定するために使用するアプリケーションは、このリリースに付属のCitrix Workspace™アプリに含まれています。

要件:

サーバーの場合:

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

クライアントの場合:

- Windows 10、32ビットおよび64ビットエディション（最小バージョン1607）

- Windows 8.1、32ビットおよび64ビットエディション（Embeddedエディションを含む）
- Windows 7、32ビットおよび64ビットエディション（Embeddedエディションを含む）

サーバーでクライアントフォルダーリダイレクトを有効にするには、レジストリを介して管理される機能のリストにあるクライアントフォルダーリダイレクトを参照してください。

ユーザーデバイスで、リダイレクトするフォルダーを指定します:

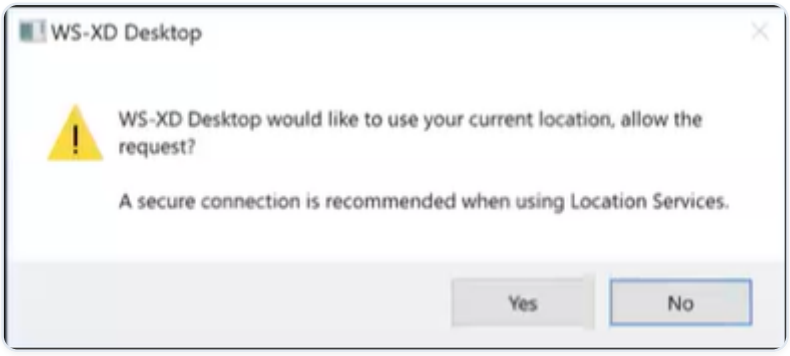
1. Citrix Workspaceアプリの最新バージョンがインストールされていることを確認してください。
2. Citrix Workspaceアプリのインストールディレクトリから、CtxCFRUI.exeを起動します。
3. **Custom**ラジオボタンを選択し、フォルダーを追加、編集、または削除します。
4. 設定を有効にするには、セッションを切断して再接続してください。

クライアント位置情報リダイレクト

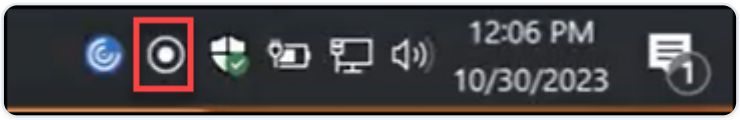
クライアント位置情報リダイレクトを有効にすると、VDAでホストされているアプリとデスクトップセッションが、クライアントの現在の位置情報にシームレスにアクセスできるようになります。マルチセッションオペレーティングシステム（TS VDAまたはマルチセッションWS VDA）では、各セッションは接続されたクライアントによって提供される独自の場所を持ちます。この機能を使用すると、位置情報に依存するVDA上のアプリケーションは、クライアントの正確な位置情報を取得できます。

詳細については、Microsoft ドキュメントを参照してください。

クライアント位置情報リダイレクトが有効になり、サーバー側とクライアント側の両方で位置情報へのアクセスが許可されると、位置情報にアクセスするアプリケーションまたはデスクトップを起動したときに、クライアントは次のダイアログボックスで現在の位置情報を共有するように求めます。



クライアント位置情報リダイレクトを有効にすると、VDAでホストされているアプリまたはデスクトップが現在の位置情報を照会した場合に、クライアントのタスクバーに次のアイコンが表示されます。



システム要件

サーバーの場合：

- シングルセッション（Win10/11）またはマルチセッション（Win 11 22H2およびServer 2022 23H2以降）OS VDA
- Windows、iOS、またはAndroid用Citrix Workspace™アプリ

構成

この機能が動作するには、Citrix®ポリシーを使用してクライアント位置情報リダイレクトを有効にする必要があります。クライアント位置情報リダイレクトはデフォルトで無効になっています。

クライアント位置情報リダイレクトを有効にするには、次の手順を実行します。

Windows VDAおよびクライアント側で：

1. **設定 > プライバシー > 位置情報**で、次のオプションを有効にします。
    - **このデバイスの位置情報へのアクセスを許可する**
    - **アプリがあなたの位置情報にアクセスすることを許可する**
    - **デスクトップアプリがあなたの位置情報にアクセスすることを許可する**
2. マルチセッションOSの場合、「**位置情報の上書き**」設定を有効にします。

Controller/DDC側で：

「**Studio > ポリシー > 位置情報 > 設定 > クライアントデバイスの物理的な位置情報の使用をアプリケーションに許可する**」ポリシーを有効にします。 詳細については、「クライアントセンサーポリシー設定」を参照してください。

双方向コンテンツリダイレクト

双方向コンテンツリダイレクトにより、Webブラウザ内、またはアプリケーションに埋め込まれたHTTPまたはHTTPS URLを、Citrix VDAセッションとクライアントエンドポイント間で双方向に転送できます。Citrixセッションで実行されているブラウザに入力されたURLは、クライアントのデフォルトブラウザを使用して開くことができます。逆に、クライアントで実行されているブラウザに入力されたURLは、公開アプリケーションまたはデスクトップのいずれかを使用して、Citrixセッションで開くことができます。双方向コンテンツリダイレクトの一般的なユースケースには、次のものがあります。

- 起動元のブラウザがソースへのネットワークアクセスを持たない場合のWeb URLのリダイレクト。
- ブラウザの互換性およびセキュリティ上の理由によるWeb URLのリダイレクト。
- CitrixセッションまたはクライアントでWebブラウザを実行したくない場合に、アプリケーションに埋め込まれたWeb URLをリダイレクトする。

システム要件

- シングルセッションまたはマルチセッションOS VDA
- シトリックス ワークスペース™ アプリ Windows 用 2311 以降
- シトリックス ワークスペース™ アプリ Linux 用 2503 以降
- シトリックス ワークスペース™ アプリ Mac 用 2607 以降

ブラウザー：

- シトリックス ブラウザ リダイレクト 拡張機能を搭載した Google Chrome
  - Google Chrome拡張機能
- シトリックス ブラウザ リダイレクト 拡張機能を搭載した Microsoft Edge
  - Microsoft Edge拡張機能

構成

Citrix Virtual Apps and Desktops™ バージョン 2311 以降、双方向コンテンツリダイレクトはCitrix Studioのみで構成されます。以前のリリースでは、クライアントエンドポイントとStudioの両方でポリシー設定が構成されていました。双方向コンテンツリダイレクトはデフォルトで無効になっています。

VDAの構成については、**ICAポリシー**設定の「双方向コンテンツリダイレクト」(/ja-jp/citrix-virtual-apps-desktops/2407/policies/reference/ica-policy-settings/bidirectional-content-redirection.html)を参照してください。

ブラウザリダイレクトを機能させるには、示されているコマンドを使用して、元のブラウザ（URLがリダイレクトされる場所）にブラウザ拡張機能を登録する必要があります。使用しているブラウザに基づいて、必要に応じてVDAとクライアントでコマンドを実行します。

ブラウザ	VDA	クライアント
グーグル クローム	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regChrome	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regChrome
マイクロソフト エッジ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regEdge	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regEdge
すべての利用可能なブラウザ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regall コマンド	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regall コマンド

ブラウザ拡張機能を登録解除するには：

ブラウザ	VDA	クライアント
グーグル クローム	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregChrome	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregChrome
マイクロソフト エッジ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregEdge	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregEdge
利用可能なすべてのブラウザ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregall	"%ProgramFiles(x86)%\Citrix\ICA

ブラウザ	VDA	クライアント
		Client\redirector.exe" /unregall

注：

- これらのコマンドを管理者権限でコマンドプロンプト (CMD) ウィンドウで実行します。
- 登録コマンドを実行すると、Chrome および Edge ブラウザは、初回起動時にCitrix Browser Redirection Extension を有効にするようユーザーに促します。
- 登録コマンドは、Browser Redirection Extension をネイティブメッセージングホストにリンクさせ、これにより拡張機能がネイティブコードと通信できるようになります。これがないと、ブラウザは通信をブロックします。
- ブラウザ拡張機能は、Google Chrome Web Store から手動でインストールすることもできます。Microsoft Edge アドオンストアからBrowser Redirection Extension を使用するには、Virtual Delivery Agent (VDA) バージョン2503以降が必要です。古いVDAバージョンの場合は、Microsoft Edgeブラウザ内でGoogle Chrome Web Storeから拡張機能をインストールしてください（Chrome Web StoreからMicrosoft Edgeに拡張機能を追加するを参照）。
- システム要件に記載されているCitrix Workspaceアプリのバージョンは、双方向コンテンツリダイレクトとOAuthリダイレクトの両方をサポートするために必要な最小バージョンです。
- Macの場合：公証済みアプリケーションのmacOSセキュリティ要件により、カスタムOAuthコールバックURLスキームはCitrixに事前登録する必要があり、インストール後に動的に変更することはできません。デフォルトでは`citrix-oauth-redir`のみがサポートされています。URLスキームを登録するには、Citrix製品チームにお問い合わせください。

Citrix VDAからクライアントへのワイルドカードリダイレクト

双方向コンテンツリダイレクトは、リダイレクトするURLを定義する際にワイルドカードの使用をサポートしています。双方向コンテンツリダイレクトを設定するには、構成の手順を参照してください。

VDAからクライアントへのカスタムプロトコルリダイレクト

双方向コンテンツリダイレクトは、Citrix VDAからクライアントへのカスタムプロトコルのリダイレクトをサポートしています。HTTPまたはHTTPS以外のプロトコルがサポートされています。双方向コンテンツリダイレクトを設定するには、構成の手順を参照してください。

Web Studioで、**双方向コンテンツリダイレクト**でカスタムプロトコルを設定します。

注：

- これらのコマンドを実行するには、管理者権限が必要です。
- クライアントには、プロトコルを処理するために登録されたアプリケーションが必要です。そうでない場合、URLはクライアントにリダイレクトされますが、起動に失敗します。
- ChromeおよびEdgeブラウザで入力または起動するカスタムプロトコルURLはサポートされておらず、リダイレクトされません。
- 以下のプロトコルはサポートされていません: `rtsp://, rtspu://, pnm://, mms://`.

その他の考慮事項

- ブラウザの要件と構成は、リダイレクトを開始するブラウザにのみ適用されます。リダイレクトが成功した後にURLが開かれる宛先ブラウザは、サポートの対象外です。VDAからクライアントにURLをリダイレクトする場合、サポートされるブラウザ構成はVDA上でのみ必要です。逆に、クライアントからVDAにURLをリダイレクトする場合、サポートされるブラウザ構成はクライアント上でのみ必要です。リダイレクトされたURLは、方向に応じて、クライアントまたはVDAのいずれかの宛先マシンで構成されているデフォルトのブラウザに渡されます。VDAとクライアントで同じブラウザタイプを使用する必要はありません。
- リダイレクトルールがループ構成にならないことを確認してください。たとえば、VDAポリシーが `https://www.citrix.com` をリダイレクトするように設定され、クライアントポリシーが同じURLをリダイレクトするように設定されている場合、無限ループが発生します。
- URL短縮サービスはサポートされていません。
- クライアントからVDAへのリダイレクトには、Windowsクライアントを管理者権限でインストールする必要があります。
- 宛先ブラウザがすでに開いている場合、リダイレクトされたURLは新しいタブで開きます。そうでない場合、URLは新しいブラウザウィンドウで開きます。

- 双方向コンテンツリダイレクトは、ローカルアプリアクセス (LAA) が有効になっている場合は機能しません。

ホストからクライアントへのリダイレクト

ホストからクライアントへのリダイレクトにより、Citrix®セッションで実行されているアプリケーションにハイパーリンクとして埋め込まれたURLを、ユーザーのエンドポイントデバイス上の対応するアプリケーションを使用して開くことができます。ホストからクライアントへのリダイレクトの一般的なユースケースには、次のものがあります。

- Citrixサーバーがインターネットまたはソースへのネットワークアクセスを持たない場合のWebサイトのリダイレクト。
- セキュリティ、パフォーマンス、互換性、またはスケーラビリティの理由から、Citrixセッション内でWebブラウザを実行することが望ましくない場合のWebサイトのリダイレクト。
- URLを開くために必要なアプリケーションがCitrixサーバーにインストールされていない場合の、特定のURLタイプのリダイレクト。

ホストからクライアントへのリダイレクトは、Webページでアクセスしたり、Citrixセッションで実行されているWebブラウザのアドレスバーに入力したりするURLを対象としていません。Webブラウザでのリダイレクトについては、「双方向URLリダイレクト」または「ブラウザコンテンツリダイレクト」を参照してください。

システム要件

- マルチセッションOS VDA
- サポートされているクライアント:
  - Windows向けCitrix Workspace™アプリ
  - Mac向けCitrix Workspaceアプリ
  - Linux向け Citrix Workspace アプリ
  - HTML5向けCitrix Workspaceアプリ
  - Chrome向けCitrix Workspaceアプリ

クライアントデバイスには、URLタイプのリダイレクトを処理するために、アプリケーションがインストールされ、構成されている必要があります。

設定

この機能を有効にするには、ホストからクライアントへのリダイレクト Citrixポリシーを使用します。**ホストからクライアントへのリダイレクト**は、デフォルトで無効になっています。ホストからクライアントへのリダイレクトポリシーを有効にすると、Citrix Launcherアプリケーションは Windowsサーバーに登録され、URLをインターセプトしてクライアントデバイスに送信できるようになります。

次に、必要なURLタイプのデフォルトアプリケーションとしてCitrix Launcherを使用するように Windowsグループポリシーを設定する必要があります。CitrixサーバーVDAで、 ServerFTAdefaultPolicy.xmlファイルを作成し、次のXMLコードを挿入します。

```
<?xml version="1.0" encoding="UTF-8"?>



<DefaultAssociations>



<Association Identifier="http" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



<Association Identifier="https" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



</DefaultAssociations>
```

グループポリシー管理コンソールから、**コンピューターの構成 > 管理用テンプレート > Windows コンポーネント > エクスプローラー > 既定の関連付け構成ファイルの設定** に移動し、 ServerFTAdefaultPolicy.xmlファイルを保存します。

注:

Citrixサーバーにグループポリシー設定がない場合、WindowsはURLを開くためのアプリケーションを選択するようユーザーに促します。

デフォルトでは、以下のURLタイプのリダイレクトをサポートしています。

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

リダイレクトのリストに、追加の標準またはカスタムURLタイプを含めるには、前述のServerFTAdefaultPolicy.xmlファイルに新しい**関連付け識別子**行を作成します。例:

```
<Association Identifier="ftp" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="mailto" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="customtype1" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="customtype2" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

URLタイプをリストに追加するには、クライアント構成も必要です。Windowsクライアントで以下のレジストリキーと値を作成してください。

注:

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

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- 値の名前: ExtraURLProtocols

- 値の型: REG_SZ
- 値のデータ: 必要なURLタイプをセミコロンで区切って指定します。URLのオーソリティ部分より前のすべてを含めます。例: `ftp://;mailto:;customtype1://;custometype2://`

URLの種類はWindowsクライアントにのみ追加できます。上記のレジストリ設定がないクライアントは、Citrixセッションへのリダイレクトを拒否します。クライアントには、指定されたURLの種類を処理するようにインストールおよび構成されたアプリケーションが必要です。

デフォルトのリダイレクトリストからURLタイプを削除するには、サーバーVDAで以下のレジストリキーと値を作成してください。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前: DisableServerFTA
- 値の型: DWORD
- 値のデータ: 1
- 値の名前: NoRedirectClasses
- 値の型: REG_MULTI_SZ
- 値のデータ: `http`、`https`、`rtsp`、`rtspu`、`pnm`、または`mms`のいずれかの値を組み合わせて指定します。複数の値を指定する場合は、それぞれを別の行に入力します。例:

`http`

`https`

`rtsp`

特定のWebサイトのセットに対してホストからクライアントへのリダイレクトを有効にするには、サーバーVDAにレジストリキーと値を作成します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前: ValidSites
- 値の型: REG_MULTI_SZ
- 値のデータ: 完全修飾ドメイン名 (FQDN) の任意の組み合わせを指定します。複数のFQDNは別々の行に入力します。プロトコル (`http://` または `https://`) を含めず、FQDNのみを含めます。FQDNには、ワイルドカード文字としてアスタリスク (`*`) を左端の位置にのみ含めることができます。このワイルドカードは、RFC 6125の規則と一致する単一レベルのドメインに一致します。例:

`www.exmaple.com`

`*.example.com`

> **注:**
>
> **ValidSites**キーを**DisableServerFTA**キーおよび**NoRedirectClasses**キーと組み合わせて使用することはできません。

サーバーVDAのデフォルトブラウザー構成

このセクションで参照されているホストからクライアントへのリダイレクトを有効にすると、サーバーVDA上の以前のデフォルトブラウザー構成がすべて上書きされます。Web URLがリダイレクトされない場合、Citrix Launcherは、`command_backup`レジストリキーで構成されているブラウザーにURLを渡します。このキーはデフォルトでInternet Explorerを指しますが、別のブラウザーへのパスを含むように変更できます。詳しくは、レジストリで管理される機能の一覧にあるサーバーVDAのデフォルトブラウザー構成を参照してください。

ローカルアプリアクセスとURLリダイレクト

はじめに

Local App Accessは、ローカルにインストールされたWindowsアプリケーションを、デスクトップを切り替えることなくホストされたデスクトップ環境にシームレスに統合します。Local App Accessを使用すると、次のことが可能になります。

- 物理的なラップトップ、PC、またはその他のデバイスにローカルにインストールされたアプリケーションに、仮想デスクトップから直接アクセスできます。
- 柔軟なアプリケーション配信ソリューションを提供します。ユーザーが仮想化できない、またはIT部門が保守していないローカルアプリケーションを持っていても、それらのアプリケーションは仮想デスクトップにインストールされているかのように動作します。
- アプリケーションが仮想デスクトップとは別にホストされている場合のダブルホップの遅延を排除します。これを行うには、公開されたアプリケーションへのショートカットをユーザーのWindowsデバイスに配置します。
- 次のようなアプリケーションを使用できます。
  - GoToMeetingなどのビデオ会議ソフトウェア。
  - まだ仮想化されていない特殊なアプリケーションやニッチなアプリケーション。

    - ユーザーデバイスからサーバーへ、そしてユーザーデバイスへ大量のデータを転送する可能性のあるアプリケーションと周辺機器。たとえば、DVDバーナーやTVチューナーなど。

Citrix Virtual Apps and Desktops™では、ホストされたデスクトップセッションはURLリダイレクトを使用してローカルアプリアクセスアプリケーションを起動します。URLリダイレクトにより、アプリケーションは複数のURLアドレスで利用可能になります。デスクトップセッション内のブラウザーで埋め込みリンクを選択することにより、ローカルブラウザー（ブラウザーのURLブロックリストに基づいて）が起動されます。ブロックリストにないURLに移動すると、そのURLはデスクトップセッションで再度開かれます。

URLリダイレクトはデスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。アプリケーションセッションで使用できる唯一のリダイレクト機能は、ホストからクライアントへのコンテンツリダイレクトです。これは、サーバーFTA（ファイルタイプ関連付け）リダイレクトの一種です。このFTAは、HTTP、HTTPS、RTSP、MMSなどの特定のプロトコルをクライアントにリダイレクトします。たとえば、HTTPで埋め込みリンクのみを開く場合、リンクはクライアントアプリケーションで直接開かれます。URLブロックリストまたは許可リストのサポートはありません。

ローカルアプリアクセスが有効になっている場合、ローカルで実行されているアプリケーションから、ユーザーがホストするアプリケーションから、またはデスクトップ上のショートカットとしてユーザーにリンクとして表示されるURLは、次のいずれかの方法でリダイレクトされます。

- ユーザーのコンピューターからホストされたデスクトップへ
- Citrix Virtual Apps and Desktopsサーバーからユーザーのコンピューターへ
- 起動された環境でレンダリングされる（リダイレクトされない）

特定のWebサイトからのコンテンツのリダイレクトパスを指定するには、Virtual Delivery AgentでURL許可リストとURLブロックリストを構成します。これらのリストには、URLリダイレクトポリシー設定を指定する複数文字列のレジストリキーが含まれています。詳細については、「ローカルアプリアクセス ポリシー設定」を参照してください。

URLは、以下の例外を除き、VDAでレンダリングできます。

- 地域/ロケール情報 — msn.comやnews.google.comなど、ロケール情報を必要とするWebサイト（地域に基づいて国固有のページを開く）。たとえば、VDAが英国のデータセンターからプロビジョニングされ、クライアントがインドから接続している場合、ユーザーはin.msn.comが表示されることを期待します。しかし、ユーザーにはuk.msn.comが表示されます。
- マルチメディアコンテンツ — リッチメディアコンテンツを含むWebサイトは、クライアントデバイスでレンダリングされると、エンドユーザーにネイティブなエクスペリエンスを提供し、高遅延ネットワークでも帯域幅を節約します。この機能は、Silverlightなどの他のメディア

タイプを含むサイトをリダイレクトします。このプロセスは安全な環境で行われます。つまり、管理者が承認したURLはクライアントで実行され、残りのURLはVDAにリダイレクトされます。

URLリダイレクトに加えて、FTAリダイレクトを使用できます。FTAは、セッションでファイルが検出されたときにローカルアプリケーションを起動します。ローカルアプリが起動された場合、そのローカルアプリはファイルを開くためにファイルへのアクセス権を持っている必要があります。したがって、ネットワーク共有またはクライアントドライブ（クライアントドライブマッピングを使用）にあるファイルのみをローカルアプリケーションを使用して開くことができます。たとえば、PDFファイルを開く際に、PDFリーダーがローカルアプリである場合、そのPDFリーダーを使用してファイルが開かれます。ローカルアプリはファイルに直接アクセスできるため、ファイルを開くためのICA®を介したネットワーク転送は発生しません。

要件、考慮事項、および制限事項

WindowsマルチセッションOS用VDAおよびWindowsシングルセッションOS用VDAの有効なオペレーティングシステムで、ローカルアプリアクセスをサポートしています。ローカルアプリアクセスには、Citrix Workspaceアプリ for Windowsバージョン4.1（最小）が必要です。以下のブラウザがサポートされています。

- Edge、最新バージョン
- Firefox、最新バージョンおよび延長サポートリリース
- Chrome、最新バージョン

ローカルアプリアクセスとURLリダイレクトを使用する際の以下の考慮事項と制限事項を確認してください。

- ローカルアプリアクセスは、すべてのモニターにまたがる全画面表示の仮想デスクトップ向けに設計されています。
    - ウィンドウモードで実行される仮想デスクトップ、またはすべてのモニターをカバーしない仮想デスクトップでローカルアプリアクセスを使用すると、ユーザーエクスペリエンスが混乱する可能性があります。
    - 複数モニター — 1つのモニターが最大化されると、そのセッションで起動されたすべてのアプリケーションのデフォルトデスクトップになります。このデフォルトは、後続のアプリケーションが通常別のモニターで起動される場合でも発生します。
    - この機能は1つのVDAをサポートします。複数の同時VDAとの統合はありません。
- 一部のアプリケーションは予期しない動作をする可能性があり、ユーザーに影響を与えます。

- ドライブ文字は、仮想デスクトップのC:ドライブではなくローカルのC:ドライブなど、ユーザーを混乱させる可能性があります。
- 仮想デスクトップで利用可能なプリンターは、ローカルアプリケーションでは利用できません。
- 昇格された権限を必要とするアプリケーションは、クライアントホスト型アプリケーションとして起動できません。
- シングルインスタンスアプリケーション（Windows Media Playerなど）には特別な処理はありません。
- ローカルアプリケーションは、ローカルマシンのWindowsテーマで表示されます。
- 全画面表示アプリケーションはサポートされていません。これらのアプリケーションには、PowerPointのスライドショーやデスクトップ全体を覆うフォトビューアなど、全画面で開くアプリケーションが含まれます。
- ローカルアプリアクセスは、ローカルアプリケーションのプロパティ（クライアントのデスクトップやスタートメニューのショートカットなど）をVDAにコピーします。ただし、ショートカットキーや読み取り専用属性などの他のプロパティはコピーしません。
- 重複するウィンドウの順序の処理方法をカスタマイズするアプリケーションは、予測できない結果になる可能性があります。たとえば、一部のウィンドウが非表示になる場合があります。
- ショートカットは、マイコンピュータ、ごみ箱、コントロールパネル、ネットワークドライブのショートカット、フォルダーのショートカットなど、サポートされていません。
- 次のファイルの種類とファイルはサポートされていません。カスタムファイルの種類、関連付けられたプログラムのないファイル、zipファイル、隠しファイル。
- 32ビットと64ビットが混在するクライアントホスト型またはVDAアプリケーションでは、タスクバーのグループ化はサポートされていません。つまり、32ビットのローカルアプリケーションと64ビットのVDAアプリケーションをグループ化することです。
- COMを使用してアプリケーションを起動することはできません。たとえば、Officeアプリケーション内から埋め込みOfficeドキュメントをクリックしても、プロセスの開始を検出できず、ローカルアプリケーションの統合は失敗します。

- ユーザーが別の仮想デスクトップセッション内から仮想デスクトップを起動するダブルホップシナリオはサポートされていません。
- URLリダイレクトは、明示的なURL（つまり、ブラウザーのアドレスバーに表示されるURL、またはブラウザーに応じてブラウザー内ナビゲーションを使用して見つかるURL）のみをサポートします。

- URLリダイレクトは、デスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。
- VDAセッションのローカルデスクトップフォルダーでは、ユーザーがファイルを作成することはできません。
- ローカルで実行されているアプリケーションの複数のインスタンスは、仮想デスクトップ用に確立されたタスクバー設定に従って動作します。ただし、ローカルで実行されているアプリケーションへのショートカットは、それらのアプリケーションの実行中のインスタンスとはグループ化されません。また、ホストされているアプリケーションの実行中のインスタンスや、ホストされているアプリケーションへのピン留めされたショートカットともグループ化されません。ユーザーは、タスクバーからローカルで実行されているアプリケーションのウィンドウのみを閉じることができます。ユーザーはローカルアプリケーションウィンドウをデスクトップのタスクバーやスタートメニューにピン留めできますが、これらのショートカットを使用するとアプリケーションが常に起動するとは限りません。
- 「**Allow Local App Access**」ポリシー設定を「**Enabled**」に設定すると、ブラウザーコンテンツリダイレクトはサポートされません。デフォルトでは、Local App Accessは禁止されています。

Windowsとの対話

Local App AccessとWindowsとの対話には、次の動作が含まれます。

- Windows 8およびWindows Server 2012のショートカットの動作
  - クライアントにインストールされているWindowsストアアプリケーションは、ローカルアプリアクセスのショートカットの一部として列挙されません。
  - 画像ファイルとビデオファイルは、デフォルトでWindowsストアアプリケーションを使用して開かれます。ただし、ローカルアプリアクセスはWindowsストアアプリケーションを列挙し、デスクトップアプリケーションでショートカットを開きます。
- ローカルプログラム
  - Windows 7の場合、フォルダーはスタートメニューで利用できます。
  - Windows 8の場合、ローカルプログラムは、ユーザーがスタート画面からカテゴリとして**すべてのアプリ**を選択した場合にのみ利用できます。すべてのサブフォルダーがローカルプログラムに表示されるわけではありません。
- アプリケーション向けのWindows 8グラフィック機能

- デスクトップアプリケーションはデスクトップ領域に制限され、スタート画面とWindows 8スタイルのアプリケーションによって覆われます。
- ローカルアプリアクセスアプリケーションは、マルチモニターモードではデスクトップアプリケーションのように動作しません。マルチモニターモードでは、スタート画面とデスクトップが異なるモニターに表示されます。

- Windows 8とローカルアプリアクセスURLリダイレクト
  - Windows 8のInternet Explorerではアドオンが有効になっていないため、URLリダイレクトを有効にするにはデスクトップ版Internet Explorerを使用してください。
  - Windows Server 2012では、Internet Explorerはデフォルトでアドオンを無効にします。URLリダイレクトを実装するには、Internet Explorerの拡張構成を無効にします。その後、Internet Explorerのオプションをリセットして再起動し、標準ユーザー向けにアドオンが有効になっていることを確認します。

ローカルアプリアクセスとURLリダイレクトの構成

Citrix Workspace™アプリでローカルアプリアクセスとURLリダイレクトを使用するには：

- ローカルクライアントマシンにCitrix Workspaceアプリをインストールします。Citrix Workspaceアプリのインストール中に両方の機能を有効にするか、グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にすることができます。
- **ローカルアプリアクセスを許可**ポリシー設定を**有効**に設定します。URLリダイレクトのURL許可リストおよびブロックリストポリシー設定も構成できます。詳しくは、「ローカルアプリアクセス ポリシー設定」を参照してください。

ローカルアプリアクセスとURLリダイレクトを有効にする

すべてのローカルアプリケーションでローカルアプリアクセスを有効にするには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**［ポリシー］**をクリックします。
2. アクションバーで、**［ポリシーの作成］**をクリックします。
3. ［ポリシーの作成］ウィンドウで、検索ボックスに「Allow Local App Access」と入力し、**［選択］**をクリックします。
4. ［設定の編集］ウィンドウで、**［許可］**を選択します。デフォルトでは、**ローカルアプリアクセスを許可**ポリシーは禁止されています。この設定が許可されている場合、VDAは、公開アプリケーションとローカルアプリアクセスのショートカットをセッションで有効にするかどうかをエンドユーザーが決定できるようにします。（この設定が禁止されている場合、公開ア

プリケーションとローカルアプリアクセスのショートカットの両方がVDAで機能しません。）このポリシー設定は、マシン全体とURLリダイレクトポリシーに適用されます。

5. ［ポリシーの作成］ウィンドウで、検索ボックスに「URL redirection allow list」と入力し、**［選択］**をクリックします。URLリダイレクト許可リストは、リモートセッションのデフォルトブラウザーで開くURLを指定します。
6. 「設定の編集」ウィンドウで、「**追加**」をクリックしてURLを追加し、「**OK**」をクリックします。
7. 「ポリシーの作成」ウィンドウで、検索ボックスに「URL redirection block list」と入力し、「**選択**」をクリックします。URLリダイレクトブロックリストは、エンドポイントで実行されているデフォルトのブラウザーにリダイレクトされるURLを指定します。
8. 「設定の編集」ウィンドウで、「**追加**」をクリックしてURLを追加し、「**OK**」をクリックします。
9. 「設定」ページで、「**次へ**」をクリックします。
10. 「ユーザーとマシン」ページで、該当するデリバリーグループにポリシーを割り当て、「**次へ**」をクリックします。
11. 「概要」ページで、設定を確認し、「**完了**」をクリックします。

Citrix Workspaceアプリのインストール中にすべてのローカルアプリケーションでURLリダイレクトを有効にするには、次の手順に従います。

1. マシン上のすべてのユーザー向けにCitrix Workspaceアプリをインストールするときに、URLリダイレクトを有効にします。これにより、URLリダイレクトに必要なブラウザーアドオンも登録されます。
2. コマンドプロンプトから、次のいずれかのオプションを使用してCitrix Workspaceアプリをインストールするための適切なコマンドを実行します。
   - CitrixReceiver.exeの場合は、`/ALLOW_CLIENTHOSTEDAPPSURL=1`を使用します。
   - CitrixReceiverWeb.exeの場合は、`/ALLOW_CLIENTHOSTEDAPPSURL=1`を使用します。

グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にする

> **注：**

- グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にする前に、receiver.admx/admlテンプレートファイルをローカルGPOに追加します。
- Citrix Workspaceアプリfor Windowsのテンプレートファイルは、CitrixBase.admx/CitrixBase.admlを%systemroot%\policyDefinitionsフォルダーに追加した場合にのみ、ローカルGPOの「**管理用テンプレート > Citrix Components > Citrix Workspace**」フォルダーで使用できます。

グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にするには、次の手順に従います。

1. **gpedit.msc**を実行します。
2. **コンピューターの構成 > 管理用テンプレート > 従来の管理用テンプレート (ADM) > Citrix Components > Citrix Workspace > ユーザーエクスペリエンス**に移動します。
3. **ローカルアプリアクセス設定**をクリックします。
4. **有効**を選択し、次に**URLリダイレクトを許可**を選択します。URLリダイレクトの場合、この記事の後半にある「*ブラウザアドオンの登録*」セクションで説明されているコマンドラインを使用してブラウザアドオンを登録します。

公開アプリケーションにのみアクセスを提供する

レジストリエディターまたはPowerShell SDKを使用して、公開アプリケーションへのアクセスを提供できます。

レジストリエディターについては、レジストリを介して管理される機能のリストにある「公開アプリケーションのローカルアプリアクセス」を参照してください。

PowerShell SDKを使用するには：

1. Delivery Controller™が実行されているマシンでPowerShellを開きます。
2. 次のコマンドを入力します: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`。

クラウドサービス展開で**ローカルアプリアクセスアプリケーションの追加**にアクセスするには、Citrix DaaS Remote PowerShell SDKを使用します。詳しくは、「Citrix DaaS Remote PowerShell SDK」を参照してください。

1. インストーラーをダウンロードします。

   `<https://download.apps.cloud.com/CitrixPoshSdk.exe>`

2. 次のコマンドを実行します。

    a. `asnp citrix.*`.

    b. `Get-XdAuthentication`

3. 次のコマンドを入力します: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`。

該当する前の手順を完了したら、以下の手順に従って続行します。

1. Web Studio にサインインし、左側のペインで **Applications** を選択します。
2. 上部中央のペインで、空白の領域を右クリックし、コンテキストメニューから **Add Local App Access Application** を選択します。アクションバーで **Add Local App Access Application** をクリックすることもできます。アクションバーに Add Local App Access Application オプションを表示するには、**Refresh** をクリックします。
3. ローカルアプリアクセスアプリケーションを公開します。

    - ローカルアプリケーションアクセスウィザードが紹介ページとともに起動します。この紹介ページは、今後のウィザード起動時に表示しないように設定できます。
    - ウィザードは、以下に説明するグループ、場所、識別、配信、概要の各ページを案内します。各ページの作業が完了したら、概要ページに到達するまで **Next** をクリックします。
    - グループページで、新しいアプリケーションを追加するデリバリーグループを1つ以上選択し、**Next** をクリックします。
    - 場所ページで、ユーザーのローカルマシン上のアプリケーションの完全な実行可能パスを入力し、アプリケーションが配置されているフォルダーへのパスを入力します。Citrix は、システム環境変数パスを使用することをお勧めします。例: %ProgramFiles(x86)%\Internet Explorer\iexplore.exe。
    - 識別ページで、デフォルト値を受け入れるか、必要な情報を入力し、**Next** をクリックします。
    - 配信ページで、このアプリケーションをユーザーに配信する方法を設定し、**Next** をクリックします。選択したアプリケーションのアイコンを指定できます。また、仮想デスクトップ上のローカルアプリケーションへのショートカットを、スタートメニュー、デスクトップ、またはその両方に表示するかどうかを指定できます。
    - 概要ページで設定を確認し、**Finish** をクリックしてローカルアプリケーションアクセスウィザードを終了します。

ブラウザアドオンを登録する

> **注記:**
>
> コマンドラインからCitrix Workspaceアプリを/ALLOW_CLIENTHOSTEDAPPSURL=1オプションを使用してインストールすると、URLリダイレクトに必要なブラウザアドオンが自動的に登録されます。

1つまたはすべてのアドオンを登録および登録解除するには、次のコマンドを使用します。

- クライアントデバイスでアドオンを登録するには: \<*client-installation-folder*>\redirector.exe /reg\<*browser*>
- クライアントデバイスでアドオンを登録解除するには: \<*client-installation-folder*>\redirector.exe /unreg\<*browser*>
- VDAでアドオンを登録するには: \<*VDAinstallation-folder*>\VDARedirector.exe /reg\<*browser*>
- VDAでアドオンを登録解除するには: \<*VDAinstallation-folder*>\VDARedirector.exe /unreg\<*browser*>

ここで、\<*browser*> はInternet Explorer、Firefox、Chrome、またはAllです。

例として、次のコマンドはCitrix Workspaceアプリを実行しているデバイスでInternet Explorerアドオンを登録します。

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

次のコマンドは、WindowsマルチセッションOS VDAですべてのアドオンを登録します。

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

ブラウザ間のURLインターセプト

- デフォルトでは、Internet Explorerは指定されたURLをリダイレクトします。URLがブロックリストにないが、ブラウザまたはWebサイトが別のURLにリダイレクトする場合、最終的なURLはリダイレクトされません。ブロックリストにある場合でもリダイレクトされません。

URLリダイレクトが正しく機能するように、ブラウザからプロンプトが表示されたらアドオンを有効にしてください。インターネットオプションを使用しているアドオン、またはプロンプト内のアドオンが無効になっている場合、URLリダイレクトは正しく機能しません。

- Firefoxのアドオンは常にURLをリダイレクトします。

アドオンがインストールされると、Firefoxは新しいタブページにアドオンのインストールを許可するか、または防止するかを促します。機能が動作するようにアドオンを許可してください。

- Chromeのアドオンは、入力されたURLではなく、常にナビゲートされた最終URLをリダイレクトします。

拡張機能は外部からインストールされています。拡張機能を無効にすると、ChromeでURLリダイレクト機能が動作しません。シークレットモードでURLリダイレクトが必要な場合は、ブラウザの設定でそのモードでの拡張機能の実行を許可してください。

ログオフ時および切断時のローカルアプリケーションの動作を構成する

> **注:**
>
> これらの手順に従って設定を構成しない場合、デフォルトでは、ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは実行を継続します。再接続後、ローカルアプリケーションが仮想デスクトップで利用可能な場合、それらは再統合されます。

ログオフ時および切断時のローカルアプリケーションの動作を構成するには、レジストリを介して管理される機能のリストにあるログオフ時および切断時のローカルアプリケーションの動作を参照してください。

汎用USBリダイレクトとクライアントドライブに関する考慮事項

HDX™テクノロジーは、ほとんどの一般的なUSBデバイスに対して**最適化されたサポート**を提供します。最適化されたサポートは、WAN経由でパフォーマンスと帯域幅の効率を向上させ、ユーザーエクスペリエンスを改善します。最適化されたサポートは、特に高遅延またはセキュリティに敏感な環境において、通常は最良の選択肢です。

HDXテクノロジーは、最適化されたサポートがない、または不適切な特殊デバイスに対して**汎用USBリダイレクト**を提供します。例を挙げます。

- USBデバイスに、最適化されたサポートに含まれない高度な機能がある場合（例：マウスやWebカメラにボタンが多い場合）。
- ユーザーが最適化されたサポートに含まれない機能を必要とする場合。

- USBデバイスが、テストおよび測定機器や産業用コントローラーなどの特殊なデバイスである場合。
- アプリケーションが、デバイスにUSBデバイスとして直接アクセスする必要がある場合。
- USBデバイスにWindowsドライバーしか利用できない場合。たとえば、スマートカードリーダーには、Android版Citrix Workspace™アプリ用のドライバーが利用できない場合があります。
- Citrix Workspaceアプリのバージョンが、この種類のUSBデバイスに対して最適化されたサポートを提供していない場合。

汎用USBリダイレクトでは、次のようになります。

- ユーザーはユーザーデバイスにデバイスドライバーをインストールする必要がありません。
- USBクライアントドライバーはVDAマシンにインストールされます。

重要:

- 汎用USBリダイレクトは、最適化されたサポートと併用できます。汎用USBリダイレクトを有効にする場合は、汎用USBリダイレクトと最適化されたサポートの両方について、CitrixのUSBデバイスポリシー設定を構成してください。
- クライアントUSBデバイス最適化ルールのCitrixポリシー設定は、特定のUSBデバイスに対する汎用USBリダイレクトの特定のポリシー設定です。ここで説明されている最適化されたサポートには適用されません。

USBデバイスのパフォーマンスに関する考慮事項

ネットワークの遅延と帯域幅は、一部の種類のUSBデバイスで汎用USBリダイレクトを使用する場合、ユーザーエクスペリエンスとUSBデバイスの動作に影響を与える可能性があります。たとえば、タイミングに敏感なデバイスは、高遅延で低帯域幅のリンクでは正しく動作しない場合があります。可能な場合は、代わりに最適化されたサポートを使用してください。

一部のUSBデバイスは、使用可能にするために高い帯域幅を必要とします。たとえば、3Dマウス（通常、高い帯域幅を必要とする3Dアプリで使用）などです。帯域幅を増やすことができない場合は、帯域幅ポリシー設定を使用して他のコンポーネントの帯域幅使用量を調整することで、問題を軽減できる場合があります。詳細については、クライアントUSBデバイスリダイレクトの帯域幅ポリシー設定と、マルチストリーム接続ポリシー設定を参照してください。

USBデバイスのセキュリティに関する考慮事項

一部のUSBデバイスは、スマートカードリーダー、指紋リーダー、署名パッドなど、本質的にセキュリティに敏感です。USBストレージデバイスなどの他のUSBデバイスは、機密データである可能性のあるデータを送信するために使用できます。

USBデバイスはマルウェアの配布によく使用されます。Citrix WorkspaceアプリおよびCitrix Virtual Apps and Desktops™の設定により、これらのUSBデバイスからのリスクを軽減できますが、排除することはできません。この状況は、汎用USBリダイレクトを使用する場合でも、最適化されたサポートを使用する場合でも当てはまります。

重要:

セキュリティに敏感なデバイスとデータについては、常にHDX接続を保護してください。クライアントとVDA間の通信を参照してください。

必要なUSBデバイスのサポートのみを有効にしてください。このニーズを満たすように、汎用USBリダイレクトと最適化されたサポートの両方を構成してください。

USBデバイスを安全に使用するためのガイダンスをユーザーに提供してください。

- 信頼できる情報源から入手したUSBデバイスのみを使用してください。
- インターネットカフェなどで、USBデバイスを無人で放置しないでください。
- 複数のコンピューターでUSBデバイスを使用するリスクを説明してください。

汎用USBリダイレクトとの互換性

汎用USBリダイレクトは、USB 2.0以前のデバイスでサポートされています。汎用USBリダイレクトは、USB 2.0またはUSB 3.0ポートに接続されたUSB 3.0デバイスでもサポートされています。汎用USBリダイレクトは、スーパースピードなど、USB 3.0で導入されたUSB機能をサポートしていません。

以下のCitrix Workspaceアプリは、汎用USBリダイレクトをサポートしています。

- Windows向けCitrix Workspaceアプリ。「アプリケーション配信の構成」を参照してください。

- Citrix Workspaceアプリ for Mac。詳しくは、Citrix Workspaceアプリ for Macを参照してください。
- Linux向けCitrix Workspaceアプリ。「最適化」を参照してください。
- Chrome OS 向け Citrix Workspace アプリについては、Citrix Workspace app for Chromeを参照してください。

Citrix Workspace アプリのバージョンについては、Citrix Workspace app feature matrixを参照してください。

以前のバージョンのCitrix Workspaceアプリを使用している場合は、Citrix Workspaceアプリのドキュメントを参照して、汎用USBリダイレクトがサポートされていることを確認してください。サポートされているUSBデバイスの種類に関する制限については、Citrix Workspaceアプリのドキュメントを参照してください。

汎用USBリダイレクトは、VDA for Single-session OSバージョン7.6から現在までのデスクトップセッションでサポートされています。

汎用USBリダイレクトは、VDA for Multi-session OSバージョン7.6以降のデスクトップセッションで、以下の制限付きでサポートされています。

- VDAは、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019、またはWindows Server 2022を実行している必要があります。
- USBデバイスドライバーは、完全な仮想化サポートを含め、VDA OS (Windows 2012 R2) の Remote Desktop Session Host (RDSH) と完全に互換性がある必要があります。

一部の種類のUSBデバイスは、リダイレクトしても有用ではないため、汎用USBリダイレクトではサポートされていません。

- USBモデム。
- USBネットワークアダプター。
- USBハブ。USBハブに接続されたUSBデバイスは個別に処理されます。
- USB仮想COMポート。汎用USBリダイレクトではなく、COMポートリダイレクトを使用してください。

汎用USBリダイレクトでテスト済みのUSBデバイスについては、Citrix Ready Marketplaceを参照してください。一部のUSBデバイスは、汎用USBリダイレクトでは正しく動作しません。

汎用USBリダイレクトを構成する

汎用USBリダイレクトを使用するUSBデバイスの種類を、個別に制御および構成できます。

- VDAでは、Citrixポリシー設定を使用します。詳しくは、「ポリシー設定リファレンス」のクライアントドライブとユーザーデバイスのリダイレクトおよびUSBデバイスポリシー設定を参照してください。
- Citrix Workspaceアプリでは、Citrix Workspaceアプリに依存するメカニズムを使用します。たとえば、管理用テンプレートは、Windows向けCitrix Workspaceアプリを構成するレジストリ設定を制御します。デフォルトでは、USBリダイレクトは特定のクラスのUSBデバイスに対して許可され、他のデバイスに対しては拒否されます。詳しくは、Windows向けCitrix Workspaceアプリのドキュメントの構成を参照してください。

この個別の構成により、柔軟性が向上します。例：

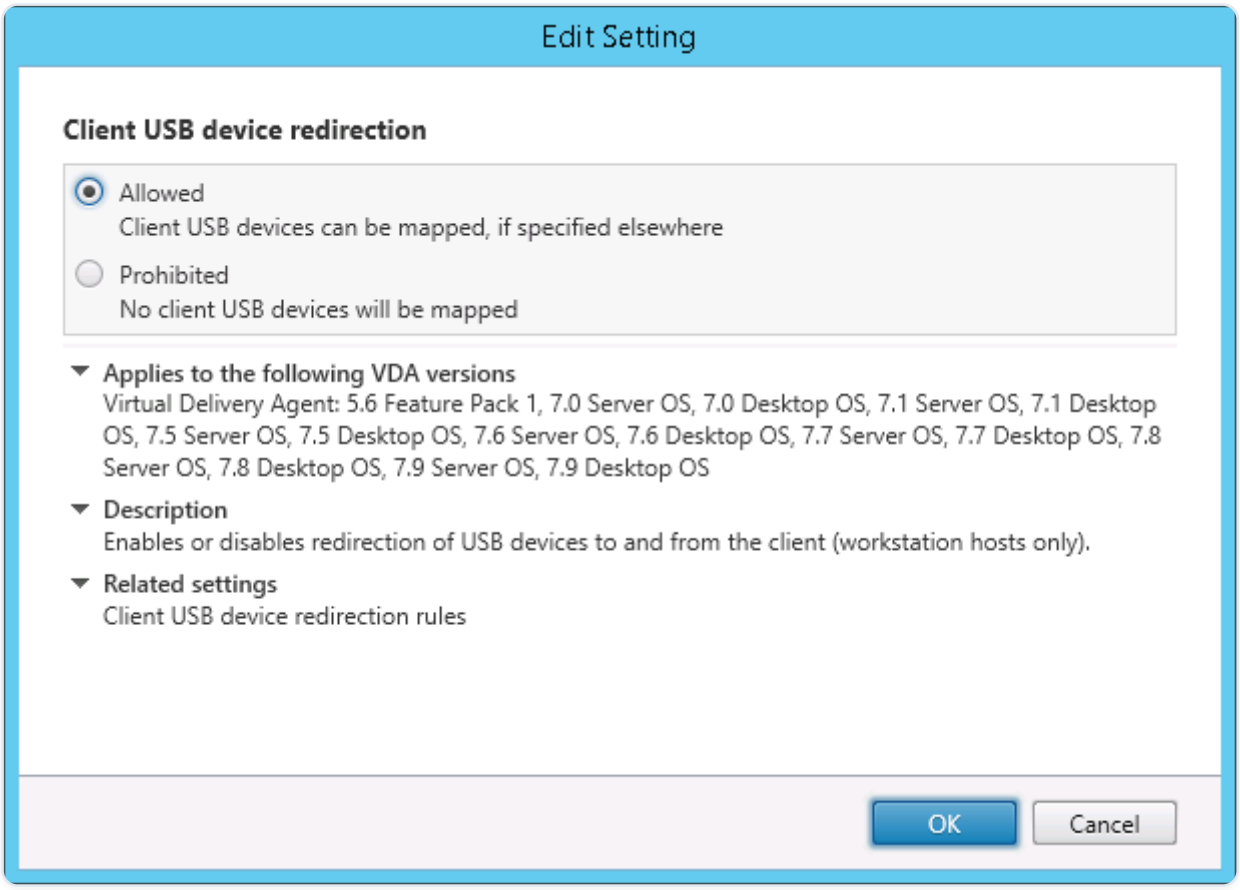
- 2つの異なる組織または部門がCitrix WorkspaceアプリとVDAを担当している場合、それぞれ個別に制御を適用できます。この構成は、ある組織のユーザーが別の組織のアプリケーションにアクセスする場合に適用されます。
- Citrixポリシー設定は、特定のユーザーのみに許可されるUSBデバイス、またはLAN経由でのみ接続するユーザー（Citrix Gatewayを使用しない場合）に許可されるUSBデバイスを制御できます。

汎用USBリダイレクトを有効にする

汎用USBリダイレクトを有効にし、ユーザーによる手動リダイレクトを不要にするには、Citrixポリシー設定とCitrix Workspaceアプリの接続設定の両方を構成します。

Citrixポリシー設定で：

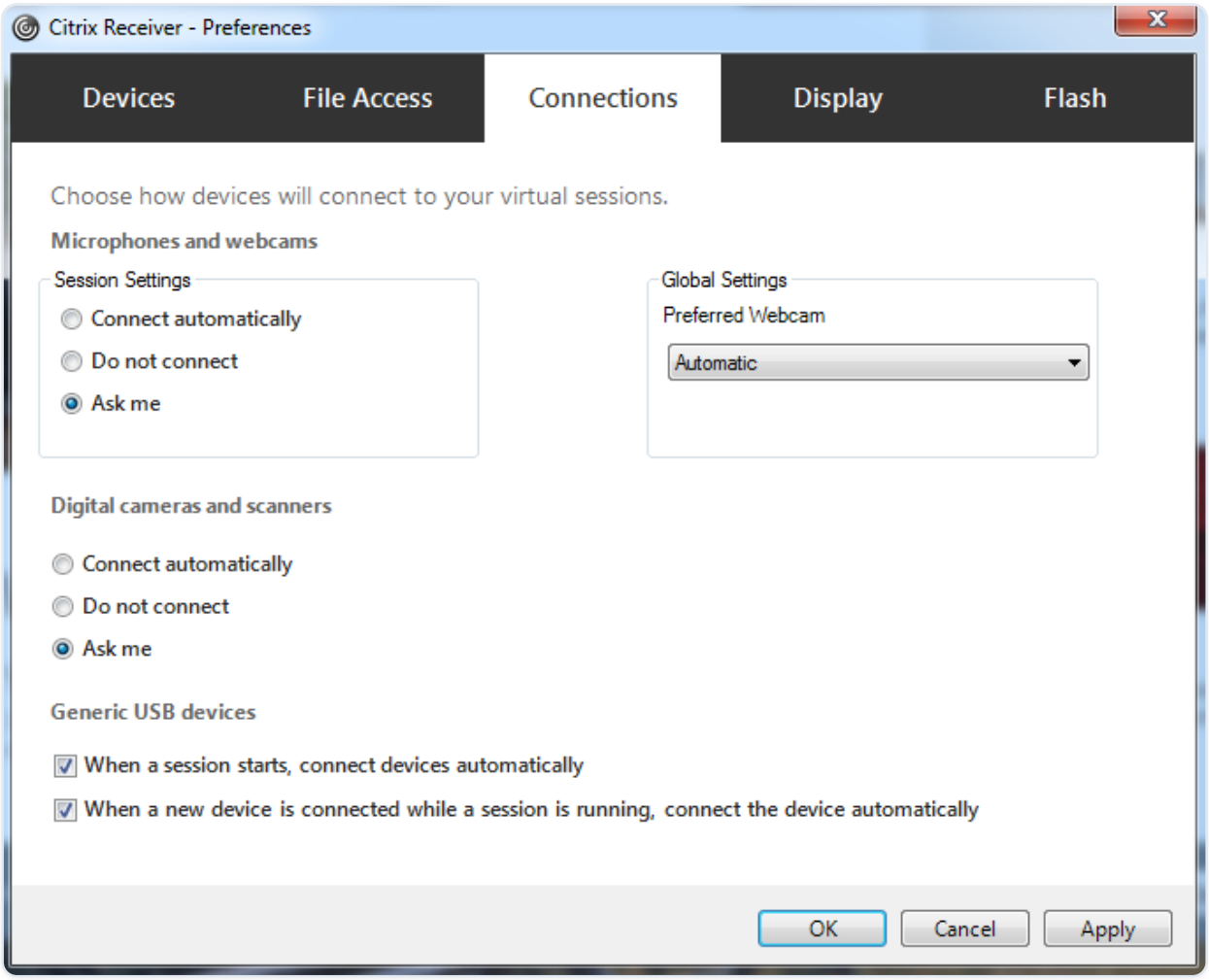
1. クライアントUSBデバイスリダイレクトをポリシーに追加し、その値を**許可**に設定します。



2. （オプション）リダイレクトに利用できるUSBデバイスのリストを更新するには、クライアントUSBデバイスリダイレクトルール設定をポリシーに追加し、USBポリシー規則を指定します。

ポリシー設定が完了したら、Citrix Workspaceアプリで：

3. デバイスが手動リダイレクトなしで自動的に接続されるように指定します。これは、管理用テンプレートを使用するか、Windows向けCitrix Workspaceアプリの**基本設定 > 接続**で実行できます。



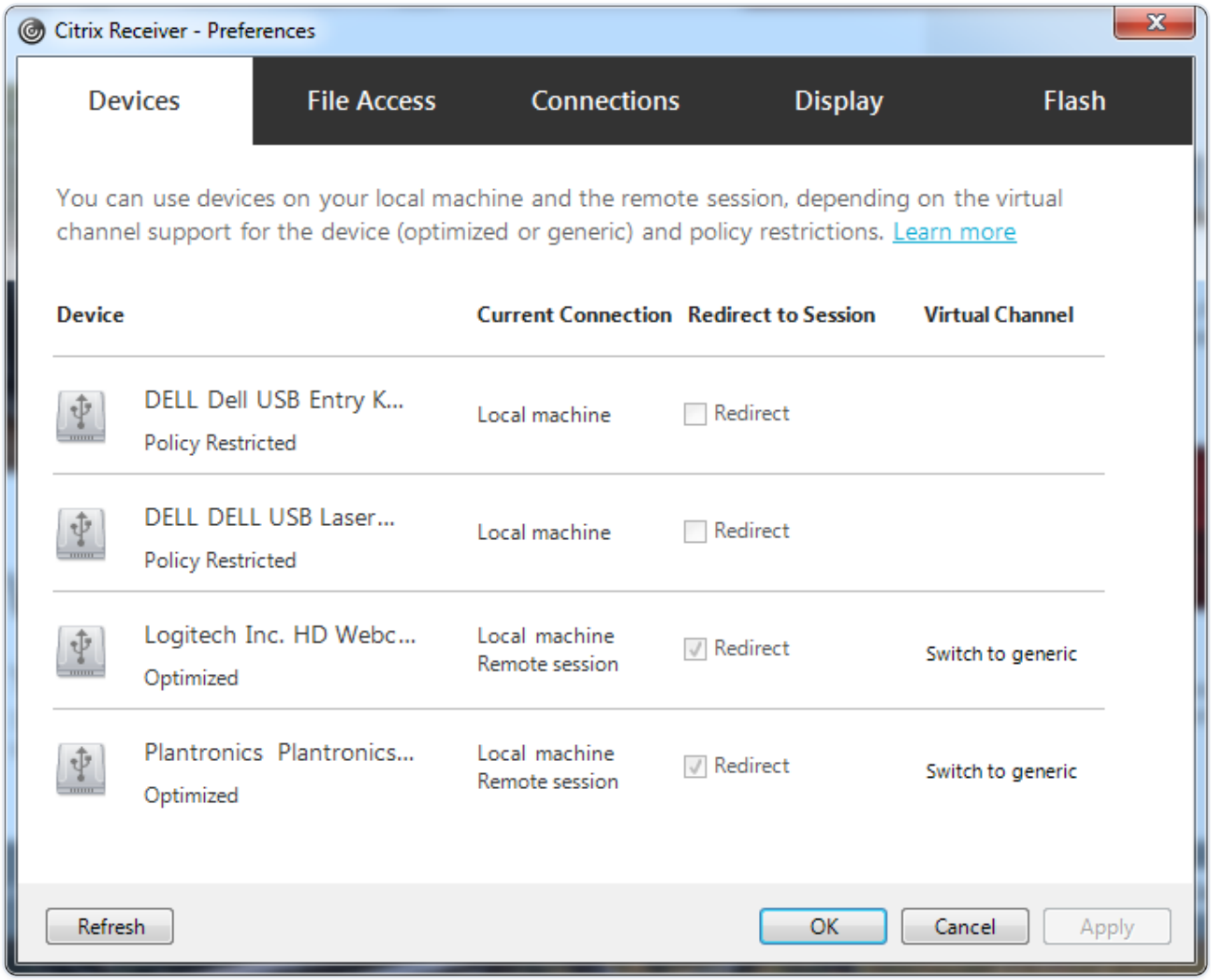
前のステップでVDAのUSBポリシー規則を指定した場合は、Citrix Workspaceアプリにも同じポリシー規則を指定します。

シンクライアントについては、USBサポートの詳細と必要な構成について製造元にお問い合わせください。

汎用USBリダイレクトで利用可能なUSBデバイスの種類を構成する

USBサポートが有効になっており、USBユーザー設定でUSBデバイスを自動的に接続するように設定されている場合、USBデバイスは自動的にリダイレクトされます。接続バーがない場合も、USBデバイスは自動的にリダイレクトされます。

ユーザーは、USBデバイスリストからデバイスを選択することで、自動的にリダイレクトされないデバイスを明示的にリダイレクトできます。詳しくは、Citrix Workspaceアプリ for Windowsのユーザーヘルプ記事「Display your devices in the Desktop Viewer」を参照してください。



最適化されたサポートではなく、汎用USBリダイレクトを使用するには、次のいずれかの方法があります。

- Citrix Workspaceアプリで、汎用USBリダイレクトを使用するUSBデバイスを手動で選択し、環境設定ダイアログボックスの［デバイス］タブから**［汎用に切り替える］** を選択します。
- USBデバイスの種類（例: AutoRedirectStorage=1）の自動リダイレクトを構成し、USBユーザー設定でUSBデバイスを自動的に接続するように設定することで、汎用USBリダイレクトを使用するUSBデバイスを自動的に選択します。詳しくは、「Configure automatic redirection of USB devices」を参照してください。

注:

Webカメラ**が**HDXマルチメディアリダイレクトと互換性がないことが判明した場合にのみ、Webカメラで使用する汎用USBリダイレクトを構成してください。

> USBデバイスが一覧表示されたりリダイレクトされたりするのを完全に防ぐには、Citrix WorkspaceアプリとVDAのデバイス規則を指定できます。

汎用USBリダイレクトの場合、少なくともUSBデバイスクラスとサブクラスを知っている必要があります。すべてのUSBデバイスが、その明白なUSBデバイスクラスとサブクラスを使用するわけではありません。例：

- ペンはマウスデバイスクラスを使用します。
- スマートカードリーダーは、ベンダー定義またはHIDデバイスクラスを使用できます。

より正確な制御のためには、ベンダーID、製品ID、およびリリースIDを知る必要があります。この情報はデバイスベンダーから入手できます。

> **重要：**
>
> 悪意のあるUSBデバイスは、意図された用途と一致しないUSBデバイス特性を示す可能性があります。デバイスルールは、この動作を防ぐことを目的としていません。

> デフォルトのUSBポリシー規則を上書きするために、USBデバイスリダイレクト規則を指定することで、汎用USBリダイレクトで利用可能なUSBデバイスを制御します。

Citrix DaaS（旧シトリックス Virtual Apps and Desktops サービス）：

- ほとんどの場合、Citrix Group Policy Management Console MSI（`CitrixGroupPolicyManagement_x64.msi`）を ダウンロード してActive Directoryシステムにインストールし、ADグループポリシーを管理します。（MSIをVDAにインストールしないでください。）
- Windows向けCitrix Workspaceアプリの場合、ユーザーデバイスのレジストリを編集します。インストールメディアには管理用テンプレート（ADMファイル）が含まれているため、Active Directoryグループポリシーを通じてユーザーデバイスを変更できます：dvd root `\os\lang\Support\Configuration\icaclient_usb.adm`

オンプレミスCitrix Virtual Apps and Desktops：

- VDAの場合、グループポリシー規則を通じて、マルチセッションOSマシンの管理者上書き規則を編集します。Group Policy Management Consoleはインストールメディアに含まれています：

  - x64: DVDルート `\os\lang\x64\Citrix Policy\CitrixGroupPolicyManagement_x64.msi`
  - x86: DVDルート `\os\lang\x86\Citrix Policy\CitrixGroupPolicyManagement_x86.msi`

- Windows向けCitrix Workspaceアプリの場合、ユーザーデバイスのレジストリを編集します。インストールメディアには管理用テンプレート（ADMファイル）が含まれているため、Active Directoryグループポリシーを通じてユーザーデバイスを変更できます：dvd root `\os\lang\Support\Configuration\icaclient_usb.adm`

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

> 製品のデフォルトルールは、HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\GenericUSBに保存されています。これらの製品デフォルトルールを編集しないでください。代わりに、この記事の後半で説明する管理者オーバーライドルールを作成するためのガイドとして使用してください。GPOオーバーライドは、製品デフォルトルールよりも前に評価されます。

管理者オーバーライドルールは、HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRulesに保存されています。GPOポリシーのルールは、**{Allow: `|` Deny:}** の形式で、その後に空白で区切られた*tag=value*式のセットが続きます。

次のタグがサポートされています。

タグ	説明
VID	デバイス記述子からのベンダーID
PID	デバイス記述子からの製品ID
REL	デバイス記述子からのリリースID

タグ	説明
クラス	デバイス記述子またはインターフェース記述子のいずれかからのクラス。利用可能なUSBクラスコードについては、`<http://www.usb.org/>`のUSBウェブサイトを参照してください。
サブクラス	デバイス記述子またはインターフェース記述子のいずれかからのサブクラス
保護	デバイス記述子またはインターフェイス記述子のいずれかからのプロトコル

ポリシールールを作成する際は、以下に注意してください。

- 規則では大文字と小文字は区別されません。
- 規則の末尾には、`#`で始まるオプションのコメントを付けることができます。区切り文字は不要で、コメントは照合目的では無視されます。
- 空白行と純粋なコメント行は無視されます。
- 空白は区切り文字として使用されますが、数値または識別子の途中に含めることはできません。たとえば、Deny: Class = 08 SubClass=05 は有効な規則ですが、Deny: Class=0 Sub Class=05 は無効です。
- タグは一致演算子 = を使用する必要があります。例：VID=1230。
- 各規則は新しい行で開始するか、セミコロン区切りのリストの一部である必要があります。

注:

- Citrix Virtual Apps and Desktopsバージョン2212以降、一部のUSBデバイスは汎用USBリダイレクト機能の使用が無効になっています。これらのデバイスは、それぞれのベンダーID（VID）と製品ID（PID）を使用して明示的に追加する必要があります。
- ADMテンプレートファイルを使用している場合は、規則をセミコロン区切りのリストとして1行で作成する必要があります。

例:

- 次の例は、ベンダーおよび製品識別子に対する管理者定義のUSBポリシールールを示しています。

  ```
  Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse Deny: VID=046D # Deny all Logitech products
  ```

- 次の例は、定義されたクラス、サブクラス、およびプロトコルに対する管理者定義のUSBポリシールールを示しています。

  ```
  Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF # Allow all USB-Miscellaneous devices
  ```

USBデバイスの使用と取り外し

ユーザーは、仮想セッションを開始する前または開始後にUSBデバイスを接続できます。

Citrix Workspaceアプリfor Windowsを使用する場合、以下が適用されます。

- セッション開始後に接続されたデバイスは、Desktop ViewerのUSBメニューにすぐに表示されます。
- USBデバイスが適切にリダイレクトされない場合は、仮想セッションが開始されるまでデバイスの接続を待つことで問題を解決できる場合があります。
- データ損失を避けるため、USBデバイスを取り外す前にWindowsの「ハードウェアを安全に取り外す」アイコンを使用してください。

USB大容量記憶装置のセキュリティ制御

USB大容量記憶装置には最適化されたサポートが提供されます。このサポートは、Citrix Virtual Apps and Desktopsのクライアントドライブマッピングの一部です。ユーザーデバイス上のドライブは、ユーザーがログオンすると仮想デスクトップ上のドライブ文字に自動的にマッピングされます。ドライブは、マッピングされたドライブ文字を持つ共有フォルダーとして表示されます。クライアントドライブマッピングを構成するには、**クライアントリムーバブルドライブ**設定を使用します。この設定は、ICAポリシー設定のファイルリダイレクトポリシー設定セクションにあります。

USB大容量記憶装置では、クライアントドライブマッピング、汎用USBリダイレクト、またはその両方を使用できます。これらはCitrixポリシーを使用して制御します。主な違いは次のとおりです。

機能	クライアントドライブマッピング	汎用USBリダイレクト
デフォルトで有効	はい	いいえ
読み取り専用アクセス設定可能	はい	いいえ
暗号化されたデバイスへのアクセス	はい、デバイスにアクセスする前に暗号化が解除されている場合	はい
BitLocker To Goデバイス	いいえ	いいえ
セッション中にデバイスを安全に削除できる	いいえ	はい、ユーザーが安全な取り外しに関するオペレーティングシステムの推奨事項に従う場合

汎用USBリダイレクトとクライアントドライブマッピングポリシーの両方が有効になっており、セッション開始前または開始後に大容量記憶装置が挿入された場合、クライアントドライブマッピングを使用してリダイレクトされます。汎用USBリダイレクトとクライアントドライブマッピングポリシーの両方が有効になっており、デバイスが自動リダイレクト用に構成されており、セッション開始前または開始後に大容量記憶装置が挿入された場合、汎用USBリダイレクトを使用してリダイレクトされます。詳細については、Knowledge Centerの記事CTX123015を参照してください。

注：

USBリダイレクトは、例えば50 Kbpsのような低帯域幅接続でもサポートされています。ただし、大きなファイルのコピーは機能しません。

印刷

環境でプリンターを管理するには、多段階のプロセスが必要です:

1. まだ慣れていない場合は、印刷の概念に慣れてください。
2. 印刷アーキテクチャを計画します。これには、ビジネスニーズ、既存の印刷インフラストラクチャ、ユーザーとアプリケーションが現在どのように印刷とやり取りしているか、およびどの印刷管理モデルが環境に最適であるかの分析が含まれます。
3. プリンタープロビジョニング方法を選択し、印刷設計を展開するためのポリシーを作成して、印刷環境を構成します。新しい従業員やサーバーが追加されたら、ポリシーを更新します。
4. ユーザーに展開する前に、パイロット印刷構成をテストします。
5. プリンタードライバーを管理し、印刷パフォーマンスを最適化することで、Citrix® 印刷環境を維持します。
6. 発生する可能性のある問題のトラブルシューティングを行います。

印刷の概念

展開の計画を開始する前に、印刷に関する以下の主要な概念を理解していることを確認してください:

- 利用可能なプリンタープロビジョニングの種類
- 印刷ジョブのルーティング方法
- プリンタードライバー管理の基本

印刷の概念は、Windowsの印刷の概念に基づいています。環境で印刷を構成し、正常に管理するには、Windowsのネットワーク印刷とクライアント印刷がどのように機能するか、そしてそれがこの環境での印刷動作にどのように変換されるかを理解する必要があります。

印刷プロセス

この環境では、すべての印刷は、アプリケーションをホストするマシン上で（ユーザーによって）開始されます。印刷ジョブは、ネットワークプリントサーバーまたはユーザーデバイスを介して印刷デバイスにリダイレクトされます。

仮想デスクトップおよびアプリケーションのユーザーには、永続的なワークスペースはありません。セッションが終了するとユーザーのワークスペースは削除されるため、すべての設定は各セッションの開始時に再構築する必要があります。その結果、ユーザーが新しいセッションを開始するたびに、システムはユーザーのワークスペースを再構築する必要があります。

ユーザーが印刷する場合：

- ユーザーに提供するプリンターを決定します。これはプリンタープロビジョニングとして知られています。
- ユーザーの印刷設定を復元します。
- セッションのデフォルトプリンターを決定します。

プリンタープロビジョニング、印刷ジョブのルーティング、プリンタープロパティの保持、およびドライバー管理のオプションを構成することで、これらのタスクの実行方法をカスタマイズできます。さまざまなオプション設定が、環境での印刷パフォーマンスとユーザーエクスペリエンスにどのように影響するかを評価してください。

プリンタープロビジョニング

セッションでプリンターを利用可能にするプロセスは、プロビジョニングとして知られています。プリンタープロビジョニングは通常、動的に処理されます。つまり、セッションに表示されるプリンターは事前に決定されて保存されるわけではありません。代わりに、ログオン時および再接続時にセッションが構築される際に、ポリシーに基づいてプリンターが組み立てられます。その結果、ポリシーに反映されていれば、ポリシー、ユーザーの場所、およびネットワークの変更に応じてプリンターが変更される可能性があります。したがって、異なる場所に移動するユーザーは、ワークスペースの変更を確認する場合があります。

システムはまた、クライアント側のプリンターを監視し、クライアント側のプリンターへの追加、削除、変更に基づいて、セッション内で自動作成されたプリンターを動的に調整します。この動的なプリンター検出は、モバイルユーザーがさまざまなデバイスから接続する際に役立ちます。

プリンタープロビジョニングの最も一般的な方法は次のとおりです。

- **Universal Print Server** - Citrix Universal Print Server は、ネットワークプリンターのユニバーサル印刷サポートを提供します。Universal Print Server は、ユニバーサルプリントドライバーを使用します。このソリューションにより、Multi-session OS マシンで単一のドライバーを使用して、任意のデバイスからネットワーク印刷を行うことができます。

Citrix は、リモート印刷サーバーのシナリオで Citrix Universal™ Print Server を推奨しています。Universal Print Server は、最適化され圧縮された形式で印刷ジョブをネットワーク経由で転送するため、ネットワーク使用量を最小限に抑え、ユーザーエクスペリエンスを向上させます。

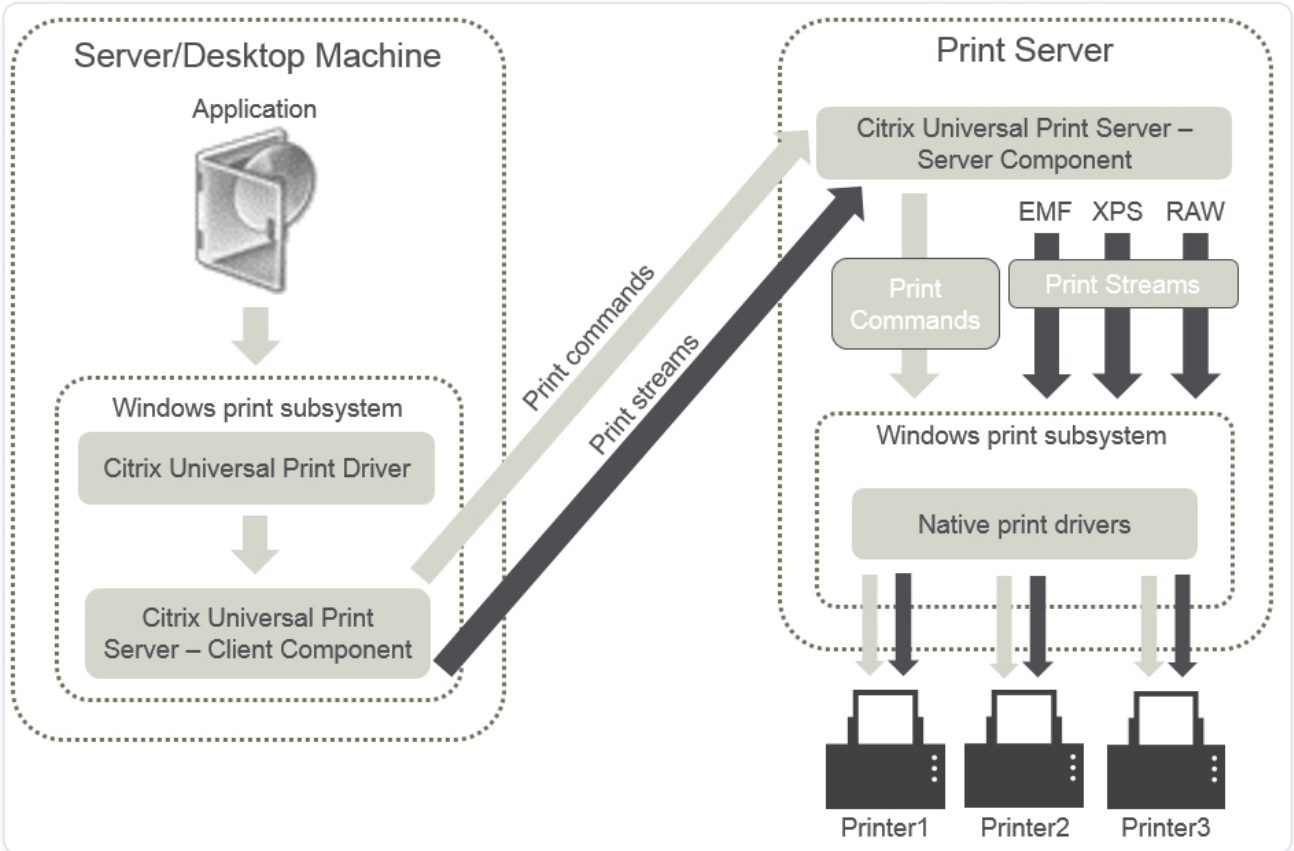
Universal Print Server の機能は次のとおりです。

クライアントコンポーネント、**UPClient** - セッションネットワークプリンターをプロビジョニングし、ユニバーサルプリントドライバーを使用する各 Multi-session OS マシンで UPClient を有効にします。

サーバーコンポーネント、**UPServer** - セッションネットワークプリンターをプロビジョニングし、セッションプリンター（セッションプリンターが集中管理されているかどうかにかかわらず）にユニバーサル印刷ドライバーを使用する各印刷サーバーにUPServerをインストールします。

Universal Print Server の要件とセットアップの詳細については、システム要件 および インストール の記事を参照してください。

次の図は、Universal Print Server を使用する環境におけるネットワークベースのプリンターの一般的なワークフローを示しています。



Citrix Universal Print Server を有効にすると、接続されているすべてのネットワークプリンターが自動検出によって自動的にそれを活用します。

- **自動作成** - *自動作成*とは、各セッションの開始時に自動的に作成されるプリンターを指します。リモートネットワークプリンターとローカル接続クライアントプリンターの両方を自動作成できます。ユーザーあたりのプリンター数が多い環境では、デフォルトのクライアントプリンターのみを自動作成することを検討してください。プリンターの自動作成数を減らすと、マルチセッションOSマシンでのオーバーヘッド（メモリとCPU）が少なくなります。自動作成されるプリンターを最小限に抑えることで、ユーザーのログオン時間も短縮できます。

  自動作成されるプリンターは、以下に基づいています。

  - ユーザーデバイスにインストールされているプリンター。
  - セッションに適用されるポリシー。

    自動作成ポリシー設定を使用すると、自動作成されるプリンターの数または種類を制限できます。デフォルトでは、ローカルに接続されたプリンターとネットワークプリンターを含む、ユーザーデバイス上のすべてのプリンターを自動的に構成すると、プリンターはセッションで利用可能になります。

  ユーザーがセッションを終了すると、そのセッションのプリンターは削除されます。

  クライアントおよびネットワークプリンターの自動作成には、関連するメンテナンスが必要です。たとえば、プリンターを追加するには、次の操作が必要です。

  - セッションプリンターポリシー設定を更新します。
  - プリンタードライバーマッピングおよび互換性ポリシー設定を使用して、すべてのマルチセッションOSマシンにドライバーを追加します。

印刷ジョブのルーティング

「印刷経路」という用語は、印刷ジョブがルーティングされるパスと、印刷ジョブがスプールされる場所の両方を指します。この概念の両方の側面が重要です。ルーティングはネットワークトラフィックに影響を与えます。スプーリングは、ジョブを処理するデバイス上のローカルリソースの利用に影響を与えます。

この環境では、印刷ジョブは印刷デバイスに到達するために2つのパスを取ることができます。クライアント経由か、ネットワークプリントサーバー経由かです。これらのパスは、クライアント印刷経路とネットワーク印刷経路と呼ばれます。どちらのパスがデフォルトで選択されるかは、使用されるプリンターの種類によって異なります。

ローカル接続プリンター

システムは、Multi-session OSマシンからクライアントを介して、ローカル接続プリンターにジョブをルーティングし、その後印刷デバイスにルーティングします。ICA®プロトコルは、印刷ジョブのトラフィックを最適化および圧縮します。印刷デバイスがユーザーデバイスにローカルに接続されている場合、印刷ジョブはICA仮想チャネル経由でルーティングされます。

ローカル接続プリンターへの印刷ジョブのルーティング図(/en-us/citrix-virtual-apps-desktops/2407/media/cds-print-local-attached.png)

ネットワークベースのプリンター

デフォルトでは、ネットワークプリンター宛てのすべての印刷ジョブは、マルチセッションOSマシンからネットワーク経由で直接プリントサーバーにルーティングされます。ただし、次の状況では、印刷ジョブはICA接続経由で自動的にルーティングされます。

- 仮想デスクトップまたはアプリケーションがプリントサーバーに接続できない場合。
- ネイティブプリンタードライバーがマルチセッションOSマシンで利用できない場合。

Universal Print Serverが有効になっていない場合、ネットワーク印刷用にクライアント印刷経路を構成することは、ICA接続経由でジョブを送信することによって得られる最適化とトラフィック圧縮の恩恵を受けることができる、広域ネットワークなどの低帯域幅接続に役立ちます。

クライアント印刷経路では、トラフィックを制限したり、印刷ジョブに割り当てられる帯域幅を制限したりすることもできます。印刷機能のないシンクライアントのように、ユーザーデバイスを介したジョブのルーティングが不可能な場合は、ICA/HDXトラフィックを優先し、良好なセッション内ユーザーエクスペリエンスを確保するために、Quality of Serviceを構成する必要があります。

ネットワーク接続プリンターへの印刷ジョブのルーティング図(/en-us/citrix-virtual-apps-desktops/2407/media/cds-print-network-attached.png)

印刷ドライバー管理

Citrix Universal Printer Driver (UPD) は、ほとんどのプリンターと互換性のある、デバイスに依存しない印刷ドライバーです。Citrix UPDは2つのコンポーネントで構成されています。

サーバーコンポーネント。Citrix UPDは、Citrix Virtual Apps and Desktops™ VDAのインストールの一部としてインストールされます。VDAは、Citrix UPDとともに次のドライバーをインストールします。「Citrix Universal Printer」（EMFドライバー）と「Citrix XPS Universal Printer」（XPSドライバー）。

Name	Processor	Type
Citrix Universal Printer	x64	Type 3 - User Mode
Citrix XPS Universal Printer	x64	Type 3 - User Mode

VDAインストーラーは、Universal Print Server PDFプリンタードライバーのインストールを制御するオプションを提供しなくなりました。PDFプリンタードライバーは、常に自動的にインストールされるようになりました。7.17 VDA（またはそれ以降のサポートされるバージョン）にアップグレードすると、以前にインストールされていたCitrix PDFプリンタードライバーは自動的に削除され、最新バージョンに置き換えられます。

印刷ジョブが開始されると、ドライバーはアプリケーションの出力を記録し、変更せずにエンドポイントデバイスに送信します。

クライアントコンポーネント。Citrix UPDは、Citrix Workspace™アプリのインストールの一部としてインストールされます。Citrix Virtual Apps and Desktopsセッションの受信印刷ストリームを取得します。その後、印刷ストリームをローカル印刷サブシステムに転送し、そこでデバイス固有のプリンタードライバーを使用して印刷ジョブがレンダリングされます。

Citrix UPDは、以下の印刷形式をサポートしています。

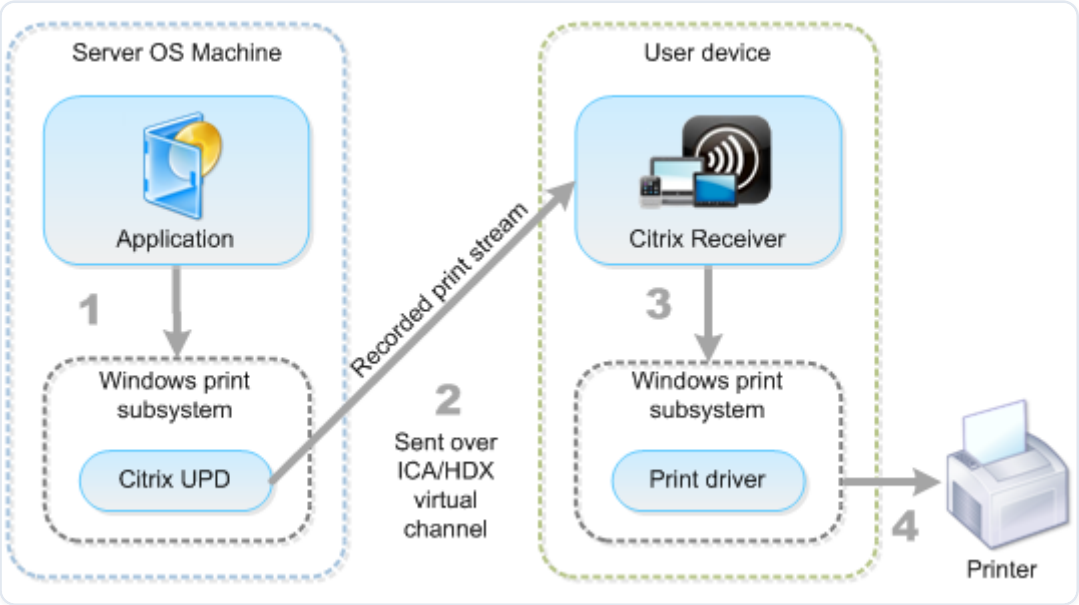
- 拡張メタファイル形式（**EMF**）。デフォルト。EMFは、Windowsメタファイル（WMF）形式の32ビットバージョンです。EMFドライバーは、Windowsベースのクライアントでのみ使用できます。
- XML Paper Specification（**XPS**）。XPSドライバーはXMLを使用して、Adobe PDF形式に似たプラットフォームに依存しない「電子ペーパー」を作成します。
- Printer Command Language（**PCL5c**および**PCL4**）。PCLは、元々ヒューレット・パッカードがインクジェットプリンター向けに開発した印刷プロトコルです。基本的なテキストとグラフィックの印刷に使用され、HP LaserJetおよび多機能周辺機器で広くサポートされています。
- PostScript（**PS**）。PostScriptは、テキストやベクターグラフィックの印刷に使用できるコンピューター言語です。このドライバーは、低コストのプリンターや多機能周辺機器で広く使用されています。

PCLおよびPSドライバーは、MacやUNIXクライアントなどのWindows以外のデバイスを使用する場合に最適です。Citrix UPDがドライバーを使用しようとする順序は、Universal driver preferenceポリシー設定を使用して変更できます。

Citrix UPD（EMFおよびXPSドライバー）は、ステープルや給紙元選択などの高度な印刷機能をサポートしています。これらの機能は、ネイティブドライバーがMicrosoft Print Capabilityテクノロジーを使用して利用可能にしている場合に利用できます。ネイティブドライバーは、Print Capabilities XMLで標準化されたPrint Schema Keywordsを使用する必要があります。非標準の

キーワードが使用されている場合、Citrix Universal Print Driverでは高度な印刷機能は利用できません。

次の図は、Universal Print Driverのコンポーネントと、デバイスにローカルに接続されたプリンターの一般的なワークフローを示しています。



ドライバー管理戦略を計画する際には、Universal Print Driver、デバイス固有のドライバー、またはその両方をサポートするかどうかを決定します。標準ドライバーをサポートする場合、以下を決定する必要があります。

プリンターの自動作成中に、システムがユーザーデバイスに接続された新しいローカルプリンターを検出した場合、必要なプリンタードライバーをMulti-session OSマシンで確認します。デフォルトでは、Windowsネイティブドライバーが利用できない場合、システムはUniversal Print Driverを使用します。

印刷を成功させるには、Multi-session OSマシン上のプリンタードライバーとユーザーデバイス上のドライバーが一致している必要があります。次の図は、クライアント印刷でプリンタードライバーが2か所でどのように使用されるかを示しています。

クライアントがローカルプリンターに印刷する図(/en-us/citrix-virtual-apps-desktops/2407/media/cds-print-client-routing.png)

- サポートするドライバーの種類。
- Multi-session OSマシンにプリンタードライバーがない場合に、自動的にインストールするかどうか。
- ドライバー互換性リストを作成するかどうか。

関連コンテンツ

- 印刷構成の例(/ja-jp/citrix-virtual-apps-desktops/2407/printing/printing-configuration-example.html)
- ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作(/ja-jp/citrix-virtual-apps-desktops/2407/printing/printing-best-practices.html)
- 印刷ポリシーと設定(/ja-jp/citrix-virtual-apps-desktops/2407/printing/printing-policies-preferences.html)
- プリンターのプロビジョニング(/ja-jp/citrix-virtual-apps-desktops/2407/printing/printing-provision-printers.html)
- 印刷環境の維持(/ja-jp/citrix-virtual-apps-desktops/2407/printing/printing-maintain-environment.html)

印刷構成の例

ニーズと環境に最も適した印刷構成オプションを選択することで、管理を簡素化できます。デフォルトの印刷構成では、ほとんどの環境でユーザーが印刷できますが、デフォルトでは、期待されるユーザーエクスペリエンスや、環境に最適なネットワーク使用量と管理オーバーヘッドが提供されない場合があります。

印刷構成は以下に依存します。

- ビジネスニーズと既存の印刷インフラストラクチャ。

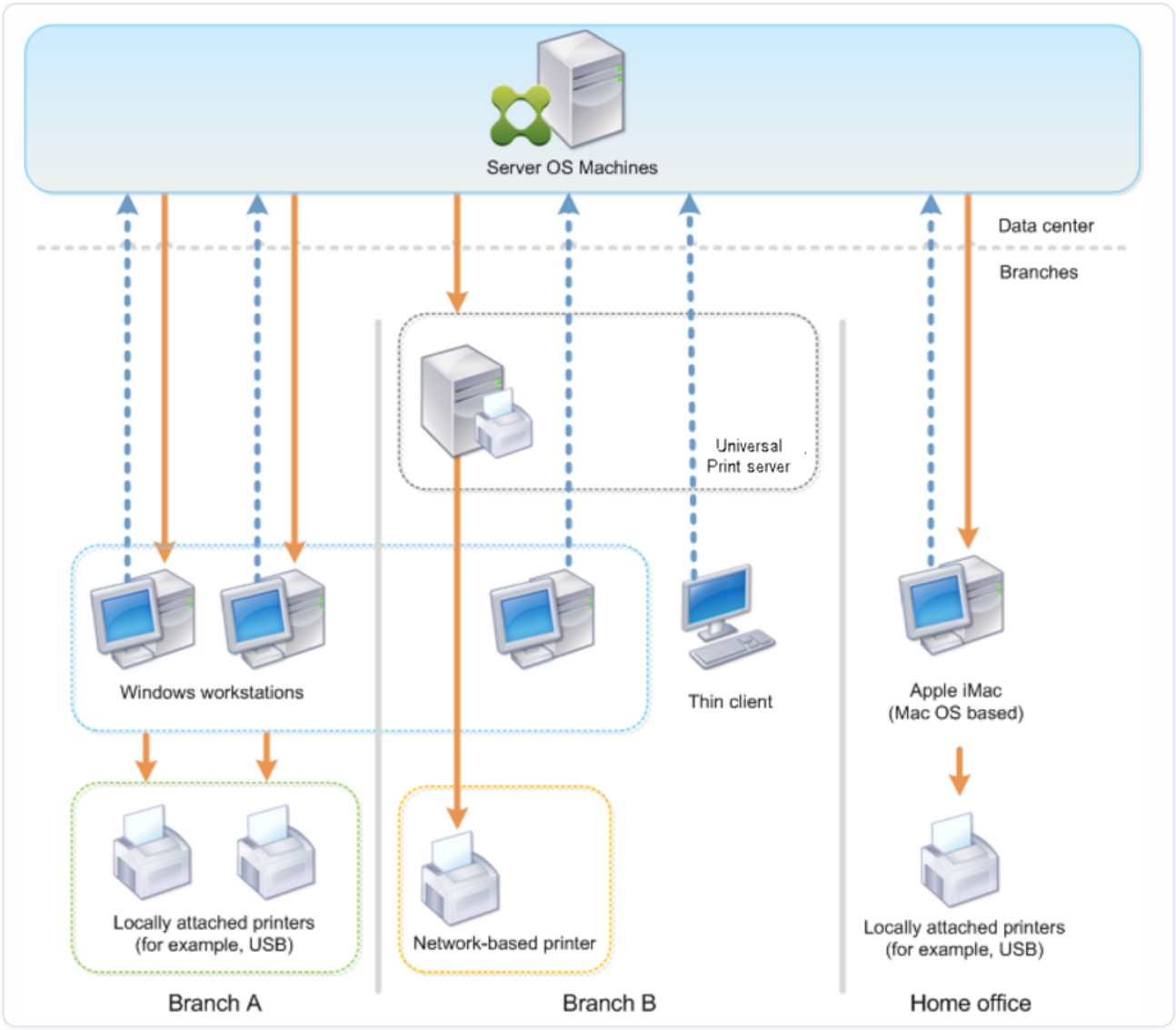
  組織のニーズに合わせて印刷構成を設計します。既存の印刷実装（ユーザーがプリンターを追加できるかどうか、どのユーザーがどのプリンターにアクセスできるかなど）は、印刷構成を定義する際の有用なガイドとなる場合があります。
- 組織に特定のユーザー（たとえば、人事部や給与計算用のプリンター）のためにプリンターを予約するセキュリティポリシーがあるかどうか。
- ユーザーが主な作業場所から離れている間、たとえばワークステーション間を移動する従業員や出張中の従業員などが印刷する必要があるかどうか。

印刷構成を設計する際には、ローカルユーザーデバイスから印刷する場合と同様に、セッション内でユーザーに同じエクスペリエンスを提供するように努めてください。

印刷展開の例

次の図は、これらのユースケースの印刷展開を示しています。

- **支店A** - 数台のWindowsワークステーションがある小規模な海外支店。各ユーザーワークステーションには、ローカルに接続されたプライベートプリンターがあります。
- **支店B** - シンクライアントとWindowsベースのワークステーションがある大規模な支店。効率を高めるため、この支店のユーザーはネットワークベースのプリンター（フロアごとに1台）を共有します。支店内に設置されたWindowsベースのプリントサーバーが印刷キューを管理します。
- **ホームオフィス** - 会社のCitrix®インフラストラクチャにアクセスするMac OSベースのユーザーデバイスがあるホームオフィス。ユーザーデバイスにはローカルに接続されたプリンターがあります。



次のセクションでは、環境の複雑さを最小限に抑え、管理を簡素化する構成について説明します。

自動作成されたクライアントプリンターとCitrix Universal™プリンタードライバー

支店Aでは、すべてのユーザーがWindowsベースのワークステーションで作業するため、自動作成されたクライアントプリンターとユニバーサルプリンタードライバーが使用されます。これらのテクノロジーは、以下の利点を提供します。

- パフォーマンス - 印刷ジョブはICA®印刷チャネルを介して配信されるため、印刷データを圧縮して帯域幅を節約できます。

  大容量のドキュメントを印刷する単一のユーザーが、他のユーザーのセッションパフォーマンスを低下させないようにするため、Citrixポリシーが構成され、最大印刷帯域幅が指定されます。

  代替ソリューションとして、マルチストリームICA接続を活用する方法があります。この接続では、印刷トラフィックが別の低優先度TCP接続内で転送されます。マルチストリームICAは、WAN接続でQuality of Service (QoS) が実装されていない場合の選択肢です。
- 柔軟性 - Citrix Universalプリンタードライバーを使用することで、クライアントに接続されているすべてのプリンターを、データセンターに新しいプリンタードライバーを統合することなく、仮想デスクトップまたはアプリケーションセッションから使用できます。

Citrix ユニバーサル プリントサーバー

支店Bでは、すべてのプリンターがネットワークベースであり、そのキューはWindowsプリントサーバーで管理されているため、Citrix Universal Print Serverが最も効率的な構成となります。

必要なすべてのプリンタードライバーは、ローカル管理者によってプリントサーバーにインストールおよび管理されます。仮想デスクトップまたはアプリケーションセッションへのプリンターのマッピングは、次のとおりです。

- Windowsベースのワークステーションの場合 - ローカルITチームは、ユーザーが適切なネットワークベースのプリンターをWindowsワークステーションに接続するのを支援します。これにより、ユーザーはローカルにインストールされたアプリケーションから印刷できるようになります。

  仮想デスクトップまたはアプリケーションセッション中に、ローカルで構成されたプリンターは自動作成によって列挙されます。その後、仮想デスクトップまたはアプリケーションは、可能であれば直接ネットワーク接続としてプリントサーバーに接続します。

Citrix Universal Print Serverコンポーネントがインストールされ有効になっているため、ネイティブプリンタードライバーは不要です。ドライバーが更新されたり、プリンターキューが変更されたりしても、データセンターでの追加構成は必要ありません。

- シンクライアントの場合 - シンクライアントユーザーの場合、プリンターは仮想デスクトップまたはアプリケーションセッション内で接続する必要があります。ユーザーに最もシンプルな印刷エクスペリエンスを提供するために、管理者はフロアごとに単一のCitrixセッションプリンターポリシーを構成し、そのフロアのプリンターをデフォルトプリンターとして接続します。

  ユーザーがフロア間を移動しても正しいプリンターが接続されるように、ポリシーはサブネットまたはシンクライアントの名前に基づいてフィルタリングされます。この構成は近接印刷と呼ばれ、ローカルプリンタードライバーのメンテナンスを可能にします（委任された管理モデルに従って）。

  プリンターキューを変更または追加する必要がある場合、Citrix管理者は環境内の該当するセッションプリンターポリシーを変更する必要があります。

ネットワーク印刷トラフィックはICA仮想チャネル外に送信されるため、QoSが実装されています。ICA/HDXトラフィックで使用されるポートでのインバウンドおよびアウトバウンドネットワークトラフィックは、他のすべてのネットワークトラフィックよりも優先されます。この構成により、ユーザーセッションが大規模な印刷ジョブによって影響を受けることはありません。

自動作成されたクライアントプリンターとCitrixユニバーサルプリンタードライバー

ユーザーが非標準のワークステーションで作業し、管理されていない印刷デバイスを使用するホームオフィスの場合、最も簡単なアプローチは、自動作成されたクライアントプリンターとユニバーサルプリンタードライバーを使用することです。

展開の概要

要約すると、サンプル展開は次のように構成されています。

- マルチセッションOSマシンにはプリンタードライバーはインストールされていません。Citrixユニバーサルプリンタードライバーのみが使用されます。ネイティブ印刷へのフォールバックとプリンタードライバーの自動インストールは無効になっています。
- すべてのユーザーに対してすべてのクライアントプリンターを自動作成するようにポリシーが構成されています。マルチセッションOSマシンは、デフォルトで印刷サーバーに直接接続します。必要な構成は、ユニバーサルプリントサーバーコンポーネントを有効にすることだけです。

- ブランチBの各フロアに対してセッションプリンターポリシーが構成され、それぞれのフロアのすべてのシンクライアントに適用されます。
- 優れたユーザーエクスペリエンスを確保するために、ブランチBにQoSが実装されています。

ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作

ベストプラクティス

特定の環境に最適な印刷ソリューションを決定する要因は多数あります。これらのベストプラクティスの一部は、お客様のサイトには適用されない場合があります。

- Citrix Universal™ Print Serverを使用します。
- ユニバーサルプリンタードライバーまたはWindowsネイティブドライバーを使用します。
- マルチセッションOSマシンにインストールされているプリンタードライバーの数を最小限に抑えます。
- ネイティブドライバーへのドライバーマッピングを使用します。
- 未テストのプリンタードライバーを本番環境にインストールしないでください。
- ドライバーの更新は避けてください。常にドライバーをアンインストールし、プリントサーバーを再起動してから、交換用ドライバーをインストールするようにしてください。
- 未使用のドライバーをアンインストールするか、プリンタードライバーマッピングと互換性ポリシーを使用して、そのドライバーでプリンターが作成されないようにします。
- バージョン2のカーネルモードドライバーの使用は避けてください。
- プリンターモデルがサポートされているかどうかを確認するには、製造元に問い合わせるか、www.citrix.com/readyにあるCitrix Ready製品ガイドを参照してください。

  一般的に、Microsoftが提供するすべてのプリンタードライバーはTerminal Servicesでテストされており、Citrixで動作することが保証されています。ただし、サードパーティ製のプリンタードライバーを使用する前に、Windows Hardware Quality Labs (WHQL) プログラムによってTerminal Services向けにドライバーが認定されていることをプリンタードライバーベンダーに確認してください。Citrixはプリンタードライバーを認定していません。

セキュリティに関する考慮事項

Citrixの印刷ソリューションは、設計上安全です。

- Citrix Print Manager Serviceは、ログオンとログオフ、切断、再接続、セッション終了などのセッションイベントを常に監視し、対応します。実際のセッションユーザーを偽装してサービス要求を処理します。
- Citrix印刷は、各プリンターにセッション内で一意の名前空間を割り当てます。
- Citrix印刷は、自動作成されたプリンターのデフォルトのセキュリティ記述子を設定し、あるセッションで自動作成されたクライアントプリンターが、他のセッションで実行中のユーザーからアクセスできないようにします。デフォルトでは、管理ユーザーは、他のセッションのクライアントプリンターの権限を表示したり手動で調整したりできる場合でも、誤ってそのプリンターに印刷することはできません。

デフォルトの印刷操作

デフォルトでは、ポリシー規則を設定しない場合、印刷動作は次のとおりです。

- ユニバーサルプリントサーバーは無効になっています。
- ユーザーデバイスで構成されているすべてのプリンターは、各セッションの開始時に自動的に作成されます。

  この動作は、Citrixポリシー設定「Auto-create client printers」を「Auto-create all client printers」オプションで構成することに相当します。
- システムは、ユーザーデバイスにローカルに接続されたプリンターにキューイングされたすべての印刷ジョブをクライアント印刷ジョブとしてルーティングします（つまり、ICA®チャネルを介してユーザーデバイス経由で）。
- システムは、ネットワークプリンターにキューイングされたすべての印刷ジョブをMulti-session OSマシンから直接ルーティングします。システムがネットワーク経由でジョブをルーティングできない場合、ユーザーデバイスを介してリダイレクトされたクライアント印刷ジョブとしてルーティングします。

  この動作は、Citrixポリシー設定「Direct connection to print servers」を無効にすることに相当します。
- システムは、ユーザーの印刷設定と印刷デバイス固有の設定の組み合わせである印刷プロパティを、ユーザーデバイスに保存しようとします。クライアントがこの操作をサポートしていない場合、システムはMulti-session OSマシンのユーザープロファイルに印刷プロパティを保存します。

  この動作は、Citrixポリシー設定「Printer properties retention」を「Held in profile only if not saved on client」オプションで構成することに相当します。

- VDAバージョン7.16以降では、Citrixポリシー設定「Automatic installation of inbox printer drivers」は、Windows 8以降のWindowsオペレーティングシステムバージョンには影響しません。これは、V3インボックスプリンタードライバーがオペレーティングシステムに含まれていないためです。
- 7.16より前のVDAでは、Multi-session OSマシンで利用可能な場合、システムはプリンタードライバーのWindowsバージョンを使用します。プリンタードライバーが利用できない場合、システムはWindowsオペレーティングシステムからドライバーをインストールしようとします。Windowsでドライバーが利用できない場合、Citrixユニバーサルプリントドライバーを使用します。

  この動作は、Citrixポリシー設定「Automatic installation of in-box printer drivers」を有効にし、ユニバーサル印刷設定を「Use universal printing only if requested driver is unavailable」で構成することに相当します。

  「Automatic installation of in-box printer drivers」を有効にすると、多数のネイティブプリンタードライバーがインストールされる可能性があります。

> **注意:**
>
> 印刷の出荷時デフォルト設定が不明な場合は、新しいポリシーを作成し、すべての印刷ポリシー規則を「Enabled」に設定して表示します。表示されるオプションがデフォルトです。

常時オンロギング

常時オンロギング機能は、VDA上のプリントサーバーと印刷サブシステムで利用可能です。

ログをZIP形式でまとめてメール送信するため、またはCitrix Insight Servicesにログを自動的にアップロードするためには、**Start-TelemetryUpload** PowerShellコマンドレットを使用します。

印刷ポリシーと設定

ユーザーが公開アプリケーションからプリンターにアクセスする際、Citrix®ポリシーを設定して以下を指定できます。

- プリンターがプロビジョニングされる方法（またはセッションに追加される方法）
- 印刷ジョブがルーティングされる方法
- プリンタードライバーが管理される方法

ユーザーデバイス、ユーザー、またはポリシーがフィルターされるその他のオブジェクトごとに異なる印刷構成を設定できます。

ほとんどの印刷機能は、Citrixの印刷ポリシー設定を通じて構成されます。印刷設定は、標準のCitrixポリシーの動作に従います。

ユーザーのネットワークアカウントに十分な権限がある場合、システムはセッションの終了時にプリンター設定をプリンターオブジェクトに書き込むか、クライアント印刷デバイスに書き込むことができます。デフォルトでは、Citrix Workspace™アプリは、設定や環境設定を他の場所で探す前に、セッション内のプリンターオブジェクトに保存されている設定を使用します。

デフォルトでは、システムはプリンターのプロパティをユーザーデバイス上（デバイスがサポートしている場合）またはMulti-session OSマシンのユーザープロファイルに保存または保持します。ユーザーがセッション中にプリンターのプロパティを変更すると、それらの変更はマシンのユーザープロファイルに更新されます。次回ユーザーがログオンまたは再接続すると、ユーザーデバイスはそれらの保持された設定を継承します。つまり、ユーザーデバイスでのプリンタープロパティの変更は、ユーザーがログオフして再度ログオンするまで、現在のセッションには影響しません。

印刷設定の場所

Windowsの印刷環境では、印刷設定への変更はローカルコンピューターまたはドキュメントに保存できます。この環境では、ユーザーが印刷設定を変更すると、設定は次の場所に保存されます。

- **ユーザーデバイス自体** - Windowsユーザーは、コントロールパネルでプリンターを右クリックし、［印刷設定］を選択することで、ユーザーデバイスのデバイス設定を変更できます。たとえば、ページ方向として［横］が選択されている場合、そのプリンターのデフォルトのページ方向設定として［横］が保存されます。
- **ドキュメント内** - ワープロプログラムやデスクトップパブリッシングプログラムでは、ページ方向などのドキュメント設定がドキュメント内に保存されることがよくあります。たとえば、ドキュメントを印刷キューに入れると、Microsoft Wordは通常、指定した印刷設定（ページ方向やプリンター名など）をドキュメント内に保存します。これらの設定は、次回そのドキュメントを印刷するときにデフォルトで表示されます。
- **ユーザーがセッション中に行った変更から** - システムは、自動作成されたプリンターの印刷設定への変更がセッション内のコントロールパネル（つまり、Multi-session OSマシン上）で行われた場合にのみ、その変更を保持します。
- **Multi-session OSマシン上** - これらは、マシン上の特定のプリンタードライバーに関連付けられたデフォルト設定です。

任意のWindowsベースの環境で保持される設定は、ユーザーが変更を行った場所によって異なります。これは、スプレッドシートプログラムなど、ある場所に表示される印刷設定が、ドキュメントなど、他の場所の設定と異なる場合があることも意味します。その結果、特定のプリンターに適用される印刷設定は、セッション中に変化する可能性があります。

ユーザー印刷設定の階層

印刷設定は複数の場所に保存できるため、システムは特定の優先順位に従ってそれらを処理します。また、デバイス設定はドキュメント設定とは別に扱われ、通常はドキュメント設定よりも優先されることに注意することが重要です。

デフォルトでは、システムは、他の設定を考慮する前に、ユーザーがセッション中に変更した印刷設定（つまり、保持された設定）を常に適用します。ユーザーが印刷すると、システムはMulti-session OSマシンに保存されているデフォルトのプリンター設定と、保持されているクライアントプリンター設定を結合して適用します。

ユーザー印刷設定の保存

Citrixでは、プリンタープロパティの保存場所を変更しないことをお勧めします。ユーザーデバイスにプリンタープロパティを保存するデフォルト設定は、一貫した印刷プロパティを確保する最も簡単な方法です。システムがユーザーデバイスにプロパティを保存できない場合、Multi-session OSマシンのユーザープロファイルに自動的にフォールバックします。

次のシナリオに該当する場合は、プリンタープロパティ保持ポリシー設定を確認してください。

- ユーザーがユーザーデバイスにプリンタープロパティを保存できないレガシープラグインを使用している場合。
- Windowsネットワークで強制プロファイルを使用しており、ユーザーのプリンタープロパティを保持したい場合。

プリンターのプロビジョニング

Citrix Universal™ プリントサーバー

環境に最適な印刷ソリューションを決定する際には、次の点を考慮してください。

- Universal Print Serverは、Windows Print Providerでは利用できない機能（イメージとフォントのキャッシュ、高度な圧縮、最適化、QoSサポートなど）を提供します。
- Universal Print Driverは、Microsoftによって定義されたパブリックなデバイス非依存設定をサポートします。ユーザーがプリンタードライバーメーカー固有のデバイス設定にアクセスする

必要がある場合、Windowsネイティブドライバーと組み合わせたUniversal Print Serverが最適なソリューションとなる可能性があります。この構成により、Universal Print Serverの利点を維持しつつ、ユーザーに特殊なプリンター機能へのアクセスを提供できます。考慮すべきトレードオフとして、Windowsネイティブドライバーにはメンテナンスが必要です。

- Citrix Universal Print Serverは、ネットワークプリンターのユニバーサル印刷をサポートします。Universal Print Serverは、Multi-session OSマシン上の単一ドライバーであるUniversal Print Driverを使用し、シンクライアントやタブレットを含むあらゆるデバイスからのローカルまたはネットワーク印刷を可能にします。

WindowsネイティブドライバーでUniversal Print Serverを使用するには、Universal Print Serverを有効にします。デフォルトでは、Windowsネイティブドライバーが利用可能な場合はそれが使用されます。そうでない場合は、Universal Print Driverが使用されます。その動作の変更（Windowsネイティブドライバーのみを使用するか、Universal Print Driverのみを使用するなど）を指定するには、Universal Print Driverの使用ポリシー設定を更新します。

Universal Print Serverをインストールする

Universal Print Serverを使用するには、インストールドキュメントに記載されているとおり、プリントサーバーにUpsServerコンポーネントをインストールして構成します。詳細については、「コアコンポーネントのインストール」および「コマンドラインを使用したインストール」を参照してください。

UPClientコンポーネントを個別に展開したい環境（例: **XenApp 6.5**を使用する場合）:

1. Windows Single-session OSまたはWindows Multi-session OS用のCitrix Virtual Apps and Desktops™ Virtual Delivery Agent (VDA) スタンドアロンパッケージをダウンロードします。
2. コマンドラインを使用したインストールに記載されているコマンドライン手順を使用してVDAを抽出します。
3. \\Image-Full\\Support\\VcRedist_2013_RTMから前提条件をインストールします。
    - Vcredist_x64 / vcredist_x86
        - 32ビット展開の場合はx86を、64ビット展開の場合は両方を実行します。
4. \\Image-Full\\x64\\Virtual Desktop Components または \\Image-Full\\x86\\Virtual Desktop Components から cdf の前提条件をインストールします。
    - Cdf_x64 / Cdf_x86
        - 32ビット版はx86、64ビット版はx64

5. \\Image-Full\\x64\\Virtual Desktop Components または \\Image-Full\\x86\\Virtual Desktop Components でUPClientコンポーネントを見つけます。
6. UPClientコンポーネントを、コンポーネントのMSIを抽出してから起動してインストールします。
7. UPClientコンポーネントのインストール後、再起動が必要です。

Universal Print ServerのCEIPを無効にする

Universal Print Serverをインストールすると、Citrix Customer Experience Improvement Program (CEIP) に自動的に登録されます。データの初回アップロードは、インストール日時から7日後に実行されます。

CEIPを無効にするには、レジストリキー **HKLM\\Software\\Citrix\\Universal Print Server\\CEIPEnabled** を編集し、**DWORD**値を**0**に設定します。

再度有効にするには、DWORD値を1に設定します。

注意: レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。レジストリエディターの誤用により発生した問題が解決されることをCitrixは保証できません。レジストリエディターはご自身の責任においてご使用ください。編集する前に必ずレジストリをバックアップしてください。

詳しくは、Citrix Insight Servicesを参照してください。

Universal Print Serverを構成する

Universal Print Serverを構成するには、以下のCitrixポリシー設定を使用します。詳しくは、画面上のポリシー設定ヘルプを参照してください。

- **Universal Print Serverを有効にする**。Universal Print Serverはデフォルトで無効になっています。Universal Print Serverを有効にすると、Universal Print Serverが利用できない場合にWindows Print Providerを使用するかどうかを選択できます。Universal Print Serverを有効にすると、ユーザーはWindows Print ProviderおよびCitrix Providerインターフェイスを介してネットワークプリンターを追加および列挙できます。
- **Universal Print Server印刷データストリーム (CGP) ポート**。Universal Print Server印刷データストリームCGP (Common Gateway Protocol) リスナーが使用するTCPポート番号を指定します。デフォルトは**7229**です。
- **ユニバーサルプリントサーバーウェブサービス (HTTP/SOAP) ポート**。ユニバーサルプリントサーバーリスナーが受信HTTP/SOAP要求に使用するTCPポート番号を指定します。既定値は**8080**です。

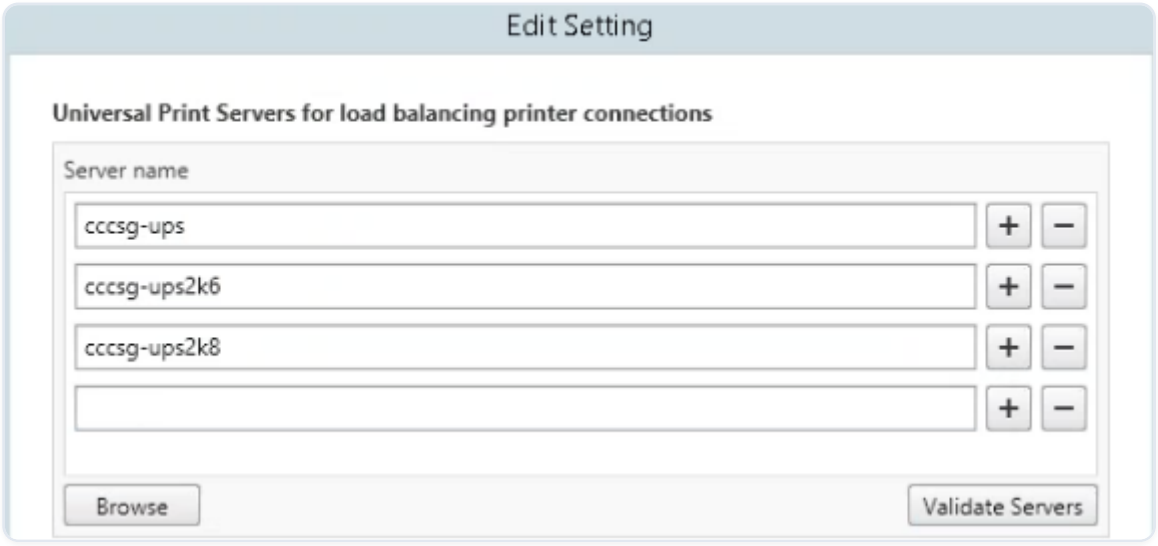
Citrix Virtual Apps and Desktops VDAへのUniversal Print Server通信のデフォルトポートであるHTTP 8080を変更するには、Universal Print Serverコンピューターで以下のレジストリを作成し、ポート番号の値を変更する必要があります。

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies`

"UpsHttpPort"=DWORD:\<portnumber\>

このポート番号は、StudioのHDXポリシー、Universal Print Server Webサービス (HTTP/SOAP) ポートと一致している必要があります。

- **Universal Print Server印刷ストリーム入力帯域幅制限 (kbps)**。各印刷ジョブからCGPを使用してUniversal Print Serverに配信される印刷データの転送速度の上限 (キロビット/秒) を指定します。デフォルトは0 (無制限) です。
- **負荷分散用のUniversal Print Server**。この設定は、他のCitrix印刷ポリシー設定を評価した後、セッション起動時に確立されたプリンター接続の負荷分散に使用されるUniversal Print Serverを一覧表示します。プリンター作成時間を最適化するために、Citrixはすべての印刷サーバーが同じ共有プリンターのセットを持つことを推奨します。



- **Universal Print Serverサービス停止しきい値**。ロードバランサーが、利用できない印刷サーバーが回復するまで待機する時間を指定します。この時間を過ぎると、サーバーは永続的にオフラインであると判断され、その負荷は他の利用可能な印刷サーバーに再分散されます。デフォルトは180 (秒) です。

Delivery Controller™で印刷ポリシーが変更されると、ポリシーの変更がVDAに適用されるまでに数分かかる場合があります。

他のポリシー設定との相互作用 - Universal Print Serverは、他のCitrix印刷ポリシー設定を尊重し、以下の表に示すようにそれらと相互作用します。提供される情報は、Universal Print Serverポ

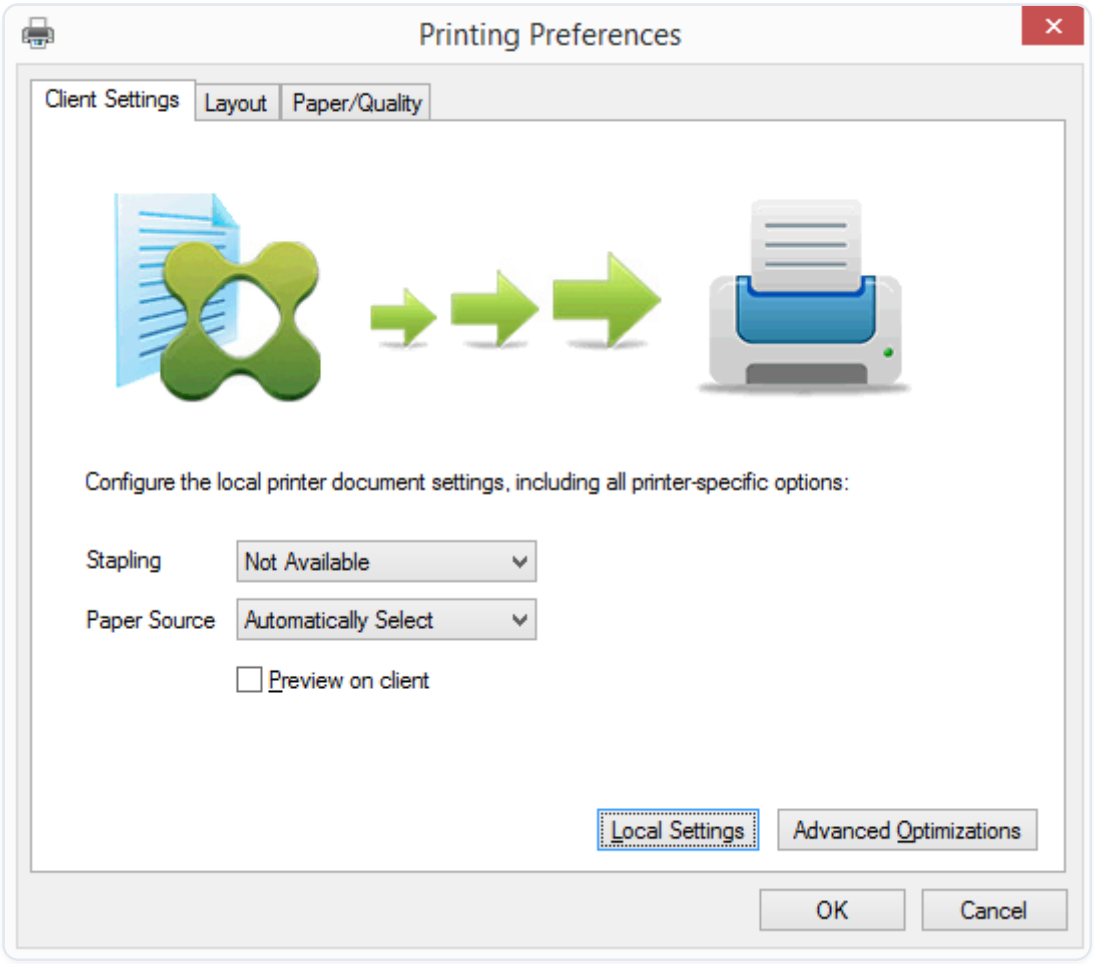
リシー設定が有効になっており、Universal Print Serverコンポーネントがインストールされ、ポリシー設定が適用されていることを前提としています。

ポリシー設定	相互作用
クライアントプリンターリダイレクト、クライアントプリンターの自動作成	Universal Print Serverが有効になると、クライアントネットワークプリンターは、ネイティブドライバーではなくUniversal Print Driverを使用して作成されます。ユーザーには以前と同じプリンター名が表示されます。
セッションプリンター	Citrix Universal Print Serverソリューションを使用する場合、ユニバーサルプリントドライバーのポリシー設定が適用されます。
プリントサーバーへの直接接続	Universal Print Serverが有効で、ユニバーサルプリントドライバーの使用ポリシー設定がユニバーサル印刷のみを使用するように構成されている場合、ユニバーサルプリントドライバーを使用して、プリントサーバーへの直接ネットワークプリンター接続を作成できます。
UPDの優先設定	EMFおよびXPSドライバーをサポートします。

ユーザーインターフェイスへの影響 - Universal Print Serverで使用されるCitrix Universal Print Driverは、以下のユーザーインターフェイスコントロールを無効にします。

- プリンターのプロパティダイアログボックスの「ローカルプリンター設定」ボタン
- ドキュメントのプロパティダイアログボックスの「ローカルプリンター設定」および「クライアントでプレビュー」ボタン

Citrix Universal Print Driver（EMFおよびXPSドライバー）は、ステープルや給紙元などの高度な印刷機能をサポートしています。セッション内でUPDにマッピングされているクライアントプリンターまたはネットワークプリンターがこれらの機能をサポートしている場合、ユーザーはカスタムUPD印刷ダイアログから「ステープル」または「給紙元」オプションを選択できます。



ステープルやセキュアPINなどの非標準のプリンター設定を行うには、Citrix UPD EMFまたはXPSドライバーを使用するクライアントマッププリンターのカスタムUPD印刷ダイアログで、**ローカル設定**を選択します。マップされたプリンターの**印刷設定**ダイアログがセッション外のクライアントに表示され、ユーザーは任意のプリンターオプションを変更できます。変更されたプリンター設定は、そのドキュメントを印刷する際にアクティブなセッションで使用されます。

これらの機能は、ネイティブドライバーがMicrosoft Print Capabilityテクノロジーを使用して利用可能にしている場合に利用できます。ネイティブドライバーは、Print Capabilities XMLで標準化されたPrint Schemaキーワードを使用する必要があります。非標準のキーワードが使用されている場合、Citrix Universal Print Driverでは高度な印刷機能は利用できません。

Universal Print Serverを使用する場合、Citrix Print Providerのプリンターの追加ウィザードは、Windows Print Providerのプリンターの追加ウィザードと同じですが、以下の例外があります。

- 名前またはアドレスでプリンターを追加する場合、プリントサーバーのHTTP/SOAPポート番号を指定できます。そのポート番号はプリンター名の一部となり、表示されます。
- 「Citrix Universal print driver usage」ポリシー設定でユニバーサル印刷を使用する必要があると指定されている場合、プリンターを選択するとユニバーサルプリントドライバー名が表示されます。Windows Print Providerはユニバーサルプリントドライバーを使用できません。

Citrix Print Providerはクライアント側レンダリングをサポートしていません。

Universal Print Serverの詳細については、CTX200328を参照してください。

自動作成されたクライアントプリンター

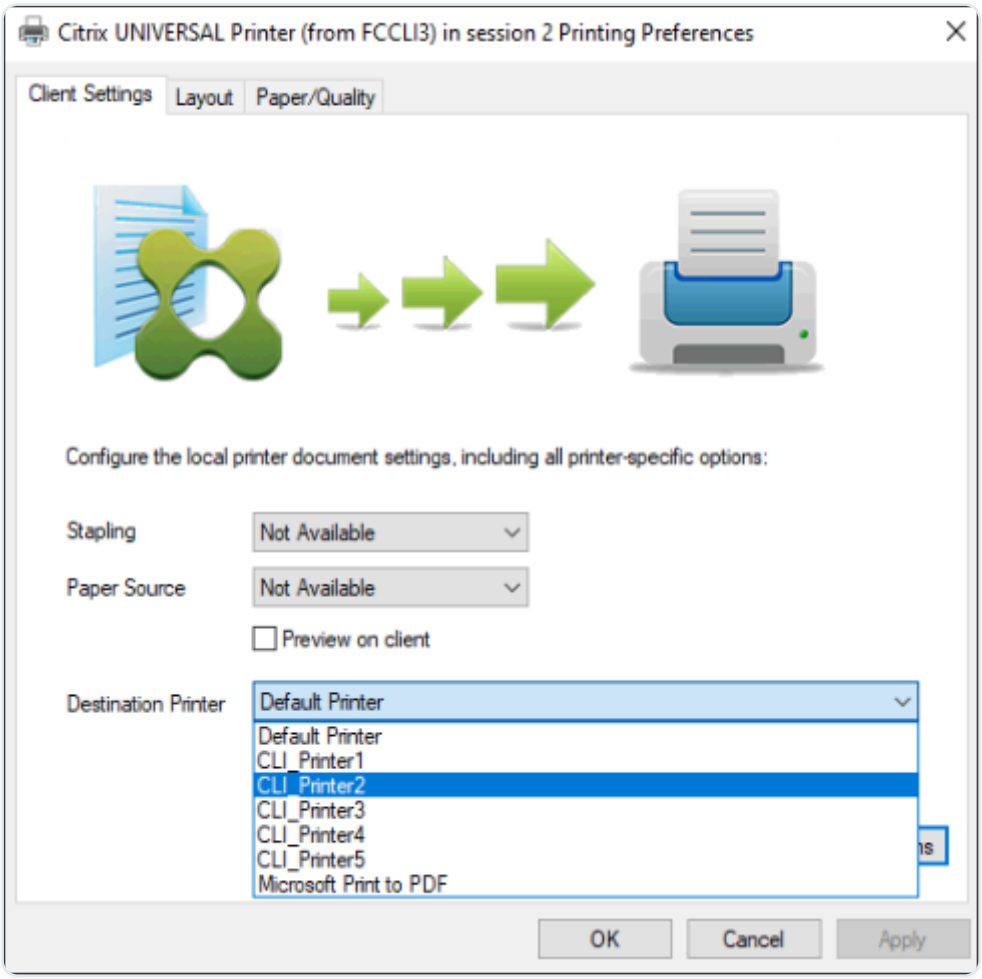
クライアントプリンターには、次のユニバーサル印刷ソリューションが提供されます。

- **Citrix Universal Printer** - セッションの開始時に作成される汎用プリンターで、印刷デバイスに縛られません。Citrix Universal Printerのみを自動作成して使用すると、リソース使用量が削減され、ユーザーのサインイン時間が短縮される可能性があります。Universal Printerは、任意のクライアント側印刷デバイスに印刷できます。

  Citrix Universal Printerは、環境内のすべてのユーザーデバイスまたはCitrix Workspace™アプリで動作しない場合があります。Citrix Universal PrinterはWindows環境を必要とし、Citrix Offline Plug-inやクライアントにストリーミングされるアプリケーションをサポートしていません。このような環境では、自動作成されたクライアントプリンターとUniversal print driverの使用を検討してください。

  Windows以外のCitrix Workspaceアプリでユニバーサル印刷ソリューションを使用するには、PostscriptまたはPCLベースの他のUniversal print driverのいずれかを使用します。

  Citrix Universal Printerを使用すると、クライアントのデフォルトプリンターまたは特定のクライアントプリンターを印刷先として選択できます。印刷ジョブに特定のプリンターを選択するには、**Printing Preferences**ダイアログボックスを開きます。**Destination Printer**ドロップダウンを選択します。**Default Printer**オプションは、印刷ジョブをクライアントのデフォルトプリンターに送信します。セッションを実行しているエンドポイントに接続されているクライアントリダイレクトプリンターも一覧表示されます。選択したプリンターは、今後の印刷ジョブの宛先プリンターとして保存されます。



- **Citrix Universal print drivers** - デバイスに依存しないプリンタードライバーです。Citrix Universal print driverを構成すると、システムはデフォルトでEMFベースのUniversal print driverを使用します。

  Citrix Universal print driverは、古いまたは高度でないプリンタードライバーよりも小さい印刷ジョブを作成する可能性があります。ただし、特殊なプリンターの印刷ジョブを最適化するには、デバイス固有のドライバーが必要になる場合があります。

ユニバーサル印刷の構成 - ユニバーサル印刷を構成するには、以下のCitrixポリシー設定を使用します。詳細については、画面上のポリシー設定ヘルプを参照してください。

- Universal print driver usage。ユニバーサル印刷を使用するタイミングを指定します。
- Auto-create generic universal printer。ユニバーサル印刷と互換性のあるユーザーデバイスが使用されているセッションで、汎用Citrix Universal Printerオブジェクトの自動作成を有効または無効にします。デフォルトでは、汎用Universal Printerオブジェクトは自動作成されません。
- ユニバーサルドライバーの優先順位。システムがユニバーサルプリントドライバーを使用しようとする順序を、リストの最初のエントリから指定します。ドライバーの追加、編集、削除、およびリスト内のドライバーの順序変更が可能です。

- ユニバーサル印刷プレビューの優先順位。自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して印刷プレビュー機能を使用するかどうかを指定します。
- ユニバーサル印刷EMF処理モード。Windowsユーザーデバイス上のEMFスプールファイルの処理方法を制御します。デフォルトでは、EMFレコードはプリンターに直接スプールされます。プリンターに直接スプールすることで、スプーラーはレコードをより速く処理し、CPUリソースの使用量を削減できます。

その他のポリシーについては、「印刷パフォーマンスの最適化」を参照してください。用紙サイズ、印刷品質、色、両面印刷、部数などの設定のデフォルトを変更するには、「CTX113148」を参照してください。

ユーザーデバイスからのプリンターの自動作成 - セッションの開始時に、システムはデフォルトでユーザーデバイス上のすべてのプリンターを自動作成します。ユーザーにプロビジョニングされるプリンターの種類を制御したり、自動作成を防止したりできます。

Citrixポリシー設定「 クライアントプリンターの自動作成」を使用して、自動作成を制御します。以下を指定できます。

- ネットワークプリンターやローカル接続プリンターを含む、ユーザーデバイスに表示されるすべてのプリンターが、各セッションの開始時に自動的に作成されます（デフォルト）。
- ユーザーデバイスに物理的に接続されているすべてのローカルプリンターが自動的に作成されます。
- ユーザーデバイスのデフォルトプリンターのみが自動的に作成されます。
- すべてのクライアントプリンターで自動作成が無効になります。

「クライアントプリンターの自動作成」設定では、「クライアントプリンターのリダイレクト」設定が「許可」（デフォルト）である必要があります。

ユーザーへのネットワークプリンターの割り当て

デフォルトでは、ユーザーデバイス上のネットワークプリンターはセッションの開始時に自動的に作成されます。システムは、各セッション内で作成されるネットワークプリンターを指定することで、列挙およびマップされるネットワークプリンターの数を減らすことができます。このようなプリンターはセッションプリンターと呼ばれます。

IPアドレスでセッションプリンターポリシーをフィルタリングして、近接印刷を提供できます。近接印刷により、指定されたIPアドレス範囲内のユーザーは、同じ範囲内に存在するネットワーク印刷デバイスに自動的にアクセスできます。近接印刷はCitrix Universal Print Serverによって提供され、このセクションで説明されている構成は必要ありません。

近接印刷には、次のシナリオが含まれる場合があります。

- 会社の内部ネットワークは、ユーザーにIPアドレスを自動的に割り当てるDHCPサーバーで動作します。
- 社内のすべての部署には、一意に割り当てられたIPアドレス範囲があります。
- 各部署のIPアドレス範囲内にネットワークプリンターが存在します。

近接印刷が構成されており、従業員がある部署から別の部署に移動した場合、追加の印刷デバイス構成は不要です。ユーザーデバイスが新しい部署のIPアドレス範囲内で認識されると、その範囲内のすべてのネットワークプリンターにアクセスできるようになります。

セッションでリダイレクトする特定のプリンターを構成する - 管理者によって割り当てられたプリンターを作成するには、Citrixポリシー設定の「セッションプリンター」を構成します。次のいずれかの方法を使用して、そのポリシーにネットワークプリンターを追加します。

- `\\servername\printername`の形式を使用して、プリンターのUNCパスを入力します。
- ネットワーク上のプリンターの場所を参照します。
- 特定のサーバー上のプリンターを参照します。`\\servername`の形式を使用してサーバー名を入力し、「参照」をクリックします。

重要：サーバーは、適用されているすべてのポリシーの有効なセッションプリンター設定を、優先度の高いものから低いものへとマージします。プリンターが複数のポリシーオブジェクトで構成されている場合、カスタムのデフォルト設定は、そのプリンターが構成されている最も優先度の高いポリシーオブジェクトからのみ取得されます。

「セッションプリンター」設定で作成されたネットワークプリンターは、サブネットなどのオブジェクトでフィルタリングすることにより、セッションが開始された場所に応じて異なる場合があります。

セッションのデフォルトネットワークプリンターを指定する - デフォルトでは、ユーザーのメインプリンターがセッションのデフォルトプリンターとして使用されます。Citrixポリシー設定の「デフォルトプリンター」を使用して、セッションでユーザーデバイスのデフォルトプリンターがどのように確立されるかを変更します。

1. 「デフォルトプリンター設定」ページで、「クライアントのデフォルトプリンターを選択」の設定を選択します。
    - ネットワークプリンター名。「セッションプリンター」ポリシー設定で追加されたプリンターがこのメニューに表示されます。このポリシーのデフォルトとして使用するネットワークプリンターを選択します。

- ユーザーのデフォルトプリンターを調整しない。デフォルトプリンターには、現在のターミナルサービスまたはWindowsユーザープロファイル設定を使用します。詳細については、画面上のポリシー設定ヘルプを参照してください。

2. 影響を与えたいユーザーグループ（またはその他のフィルターされたオブジェクト）にポリシーを適用します。

近接印刷を構成する - 近接印刷はCitrix Universal Print Serverによっても提供され、ここに記載されている構成は不要です。

1. 各サブネット（またはプリンターの場所に対応する）ごとに個別のポリシーを作成します。
2. 各ポリシーで、そのサブネットの地理的な場所にあるプリンターをSession printers設定に追加します。
3. Default printer設定を「ユーザーのデフォルトプリンターを調整しない」に設定します。
4. クライアントIPアドレスでポリシーをフィルターします。DHCP IPアドレス範囲の変更を反映するように、これらのポリシーを必ず更新してください。

印刷環境の維持

印刷環境の維持には、以下が含まれます。

- プリンタードライバーの管理
- 印刷パフォーマンスの最適化
- プリンターの表示と印刷キューの管理

プリンタードライバーの管理

管理オーバーヘッドとプリンタードライバーの問題発生の可能性を最小限に抑えるため、Citrixは Citrix Universal™プリントドライバーの使用を推奨しています。

自動作成が失敗した場合、デフォルトでは、システムはWindowsに付属のWindowsネイティブプリンタードライバーをインストールします。ドライバーが利用できない場合、システムは Universalプリントドライバーにフォールバックします。プリンタードライバーのデフォルト設定の詳細については、「ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作」を参照してください。

すべてのシナリオでCitrix Universalプリントドライバーが選択肢とならない場合、Multi-session OSマシンにインストールされるドライバーの数を最小限に抑えるために、プリンタードライバー

をマッピングします。さらに、プリンタードライバーをマッピングすることで、次のことが可能になります。

- 指定されたプリンターがCitrix Universalプリントドライバーのみを使用できるようにする
- 指定されたドライバーでプリンターが作成されることを許可または防止する
- 古いドライバーや破損したドライバーを適切なプリンタードライバーに置き換える
- クライアントドライバー名に対して、Windowsサーバーで利用可能なドライバーを置き換える

プリンタードライバーの自動インストールを防止する - Multi-session OSマシン全体で一貫性を確保するために、プリントドライバーの自動インストールは無効にする必要があります。これは、Citrix®ポリシー、Microsoftポリシー、またはその両方を通じて実現できます。Windowsネイティブプリンタードライバーの自動インストールを防止するには、Citrixポリシー設定「Automatic installation of in-box printer drivers」を無効にします。

クライアントプリンタードライバーをマッピングする - 各クライアントは、ログオン時にプリンタードライバー名を含むクライアント側のプリンターに関する情報を提供します。クライアントプリンターの自動作成中に、クライアントから提供されたプリンターモデル名に対応するWindowsサーバープリンタードライバー名が選択されます。その後、自動作成プロセスは、識別された利用可能なプリンタードライバーを使用して、リダイレクトされたクライアント印刷キューを構築します。

マップされたクライアントプリンタードライバーのドライバー置換ルールを定義し、印刷設定を編集するための一般的なプロセスは次のとおりです。

1. 自動作成されたクライアントプリンターのドライバー置換ルールを指定するには、Citrixポリシー設定の「Printer driver mapping and compatibility」を構成します。これには、クライアントプリンタードライバー名を追加し、「Find printer driver」メニューからクライアントプリンタードライバーの代わりに置換するサーバードライバーを選択します。この設定ではワイルドカードを使用できます。たとえば、すべてのHPプリンターに特定のドライバーを使用させるには、ポリシー設定で「HP*」と指定します。
2. プリンタードライバーを禁止するには、ドライバー名を選択し、「Do not create」設定を選択します。
3. 必要に応じて、既存のマッピングを編集したり、マッピングを削除したり、リスト内のドライバーエントリの順序を変更したりします。
4. マップされたクライアントプリンタードライバーの印刷設定を編集するには、プリンタードライバーを選択し、「設定」をクリックして、印刷品質、向き、色などの設定を指定します。プリンタードライバーがサポートしていない印刷オプションを指定した場合、そのオプションは

無効になります。この設定は、ユーザーが以前のセッションで設定した保持されているプリンター設定を上書きします。

5. 特定のドライバーでのみ利用可能なプリンター機能があるため、ドライバーをマッピングした後は、プリンターの動作を詳細にテストすることをCitrixは推奨します。

ユーザーがログオンすると、システムはクライアントプリンターを設定する前に、クライアントプリンタードライバーの互換性リストをチェックします。

印刷パフォーマンスの最適化

印刷パフォーマンスを最適化するには、Universal Print ServerとUniversal Print Driverを使用します。以下のポリシーは、印刷の最適化と圧縮を制御します。

- ユニバーサル印刷の最適化のデフォルト。セッション用にユニバーサルプリンターが作成される際のデフォルト設定を指定します。
    - 希望する画質は、ユニバーサル印刷に適用されるデフォルトの画像圧縮制限を指定します。デフォルトでは、「標準品質」が有効になっており、ユーザーは標準または低品質の圧縮を使用してのみ画像を印刷できます。
    - ヘビーウェイト圧縮を有効にするは、画質を損なうことなく、「希望する画質」で設定された圧縮レベルを超えて帯域幅を削減することを有効または無効にします。デフォルトでは、ヘビーウェイト圧縮は無効になっています。
    - 画像とフォントのキャッシュ設定は、印刷ストリームに複数回出現する画像とフォントをキャッシュするかどうかを指定し、各固有の画像またはフォントがプリンターに一度だけ送信されるようにします。デフォルトでは、埋め込み画像とフォントはキャッシュされます。
    - 管理者以外のユーザーがこれらの設定を変更することを許可するは、ユーザーがセッション内でデフォルトの印刷最適化設定を変更できるかどうかを指定します。デフォルトでは、ユーザーはデフォルトの印刷最適化設定を変更できません。
- ユニバーサル印刷の画像圧縮制限。Universal Print Driverで印刷される画像の最大品質と最小圧縮レベルを定義します。デフォルトでは、画像圧縮制限は「最高品質（ロスレス圧縮）」に設定されています。
- ユニバーサル印刷の印刷品質制限。セッションで印刷出力を生成するために利用できる最大ドット/インチ (dpi) を指定します。デフォルトでは、制限は指定されていません。

デフォルトでは、ネットワークプリンター宛てのすべての印刷ジョブは、マルチセッションOSマシンからネットワーク経由で直接印刷サーバーにルーティングされます。ネットワークにかなりの遅延や帯域幅の制限がある場合は、ICA®接続経由で印刷ジョブをルーティングすることを検討し

てください。そのためには、Citrixポリシー設定「Direct connections to print servers」を無効にします。ICA接続経由で送信されるデータは圧縮されるため、WANを介してデータが転送される際の帯域幅の消費が少なくなります。

印刷帯域幅を制限してセッションパフォーマンスを向上させる - マルチセッションOSマシンからユーザープリンターにファイルを印刷している間、特にユーザーが低速ネットワーク経由でサーバーにアクセスしている場合、帯域幅の競合により、他の仮想チャネル（ビデオなど）のパフォーマンスが低下する可能性があります。このような劣化を防ぐために、ユーザー印刷で使用される帯域幅を制限できます。印刷のデータ転送速度を制限することで、HDX™データストリームでビデオ、キーストローク、マウスデータの転送により多くの帯域幅を利用できるようになります。

> **重要:**
>
> プリンターの帯域幅制限は、他のチャネルが使用されていない場合でも常に適用されます。
>
> 印刷帯域幅のセッション制限を構成するには、以下のCitrixポリシーの帯域幅プリンター設定を使用します。サイトの制限を設定するには、Studioを使用してこのタスクを実行します。個々のサーバーの制限を設定するには、各マルチセッションOSマシンでWindowsのグループポリシー管理コンソールを使用してこのタスクを実行します。

- 「Printer redirection bandwidth limit」設定は、印刷に利用できる帯域幅をキロビット/秒 (kbps) で指定します。
- 「Printer redirection bandwidth limit percent」設定は、印刷に利用できる帯域幅を、利用可能な全体帯域幅の割合に制限します。

  注: 「Printer redirection bandwidth limit percent」設定を使用して帯域幅をパーセンテージで指定するには、「Overall session bandwidth limit」も有効にする必要があります。

  両方の設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

印刷帯域幅に関するリアルタイム情報を取得するには、Citrix Directorを使用します。

ユニバーサル印刷サーバーの負荷分散

ユニバーサル印刷サーバーソリューションは、負荷分散ソリューションに印刷サーバーを追加することで拡張できます。各VDAには独自のロードバランサーがあり、印刷負荷をすべての印刷サーバーに分散するため、単一障害点はありません。

ポリシー設定のUniversal Print Servers for load balancingとUniversal Print Servers out-of-service thresholdを使用して、負荷分散ソリューション内のすべての印刷サーバーに印刷負荷を分散します。

印刷サーバーで予期せぬ障害が発生した場合、各VDAのロードバランサーのフェイルオーバーメカニズムは、障害が発生した印刷サーバーに割り当てられていたプリンター接続を他の利用可能な印刷サーバーに自動的に再分散します。これにより、既存および新規のすべてのセッションがユーザーエクスペリエンスに影響を与えることなく、また管理者の即時介入を必要とせずに正常に機能します。

管理者は、パフォーマンスカウンターのセットを使用して、VDA上のロードバランスされた印刷サーバーのアクティビティを以下の項目で追跡できます。

- VDA上のロードバランスされた印刷サーバーのリストとその状態（利用可能、利用不可）
- 各印刷サーバーが受け入れたプリンター接続の数
- 各印刷サーバーで失敗したプリンター接続の数
- 各印刷サーバー上のアクティブなプリンター接続の数
- 各印刷サーバー上の保留中のプリンター接続の数

印刷キューの表示と管理

次の表は、環境内でプリンターを表示し、印刷キューを管理できる場所をまとめたものです。

	印刷経路	場所
クライアントプリンター（ユーザーデバイスに接続されたプリンター）	クライアント印刷経路	UAC有効時: Microsoft Management Consoleにある印刷の管理スナップイン; UAC無効時: Windows 8以前: コントロールパネル、Windows 8: 印刷の管理スナップイン
ネットワークプリンター（ネットワーク印刷サーバー上のプリンター）	ネットワーク印刷経路	UAC有効時: 印刷サーバー \> Microsoft Management Consoleにある印刷の管理スナップイン; UAC無効時: 印刷サーバー \> コントロールパネル

	印刷経路	場所
ネットワークプリンター (ネットワーク印刷サーバー上のプリンター)	クライアント印刷パス	UAC有効時: 印刷サーバー \> Microsoft Management Consoleにある印刷の管理スナップイン; UAC無効時: Windows 8以前: コントロールパネル, Windows 8: 印刷の管理スナップイン
ローカルネットワークサーバープリンター (ネットワーク印刷サーバーからマルチセッションOSマシンに追加されたプリンター)	ネットワーク印刷パス	UAC有効時: 印刷サーバー \> コントロールパネル; UAC無効時: 印刷サーバー \> コントロールパネル

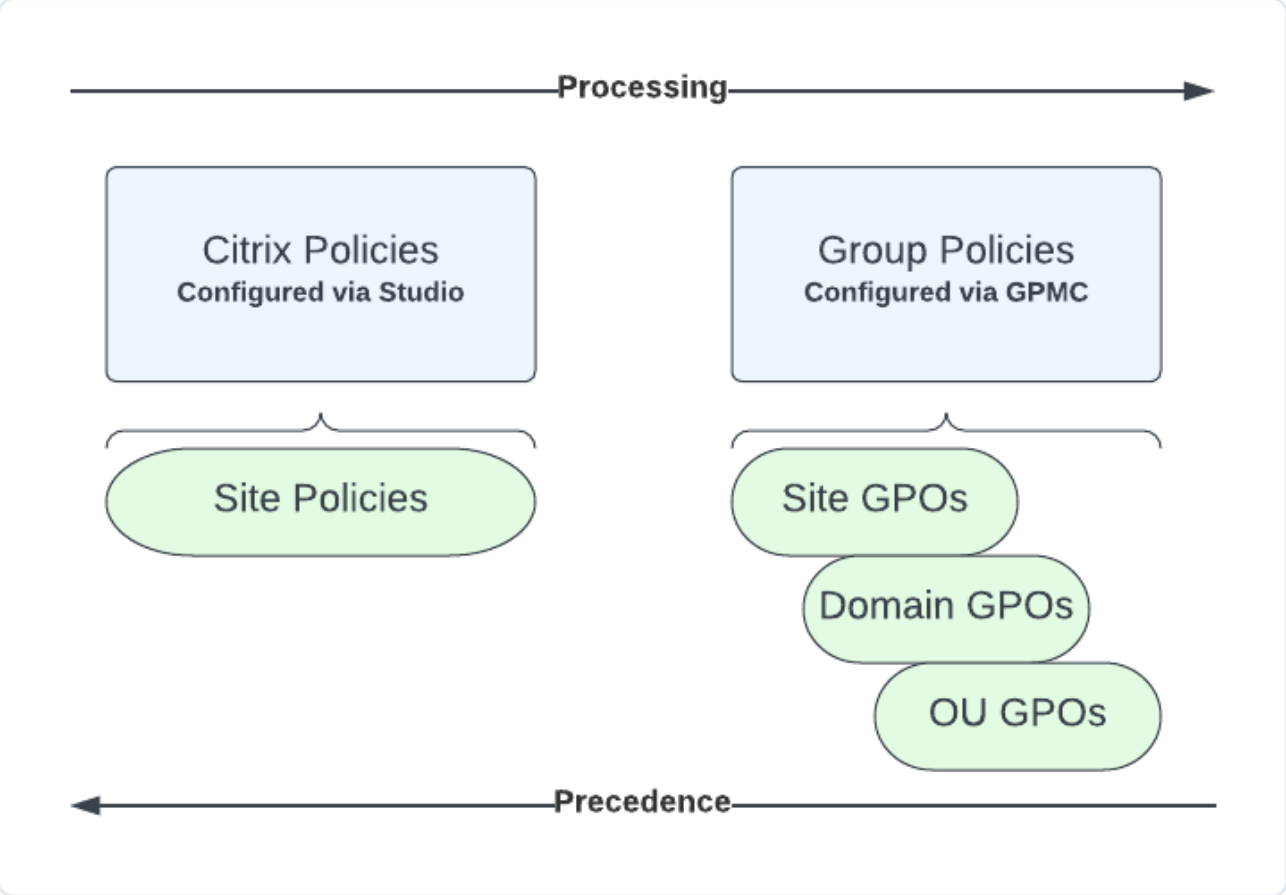
注:

ネットワーク印刷経路を使用するネットワークプリンターの印刷キューはプライベートであり、システムを通じて管理することはできません。

ポリシー

ポリシーとは、ユーザー、デバイス、または接続の種類ごとに、セッション、帯域幅、およびセキュリティがどのように管理されるかを定義する設定の集合です。

ポリシー設定は、物理マシン、仮想マシン、またはユーザーに適用できます。設定は、ローカルレベルの個々のユーザー、またはActive Directoryのセキュリティグループに適用できます。構成は特定の基準とルールを定義します。ポリシーを具体的に割り当てない場合、設定はすべての接続に適用されます。



ポリシーは、ネットワークのさまざまなレベルに適用できます。組織単位GPOレベルに配置されたポリシー設定は、ネットワーク上で最も高い優先順位を持ちます。ドメインGPOレベルのポリシーは、サイトグループポリシーオブジェクトレベルのポリシーを上書きします。サイトグループポリシーオブジェクトレベルは、MicrosoftおよびCitrixローカルポリシーレベルの両方における競合するポリシーを上書きします。

すべてのCitrixローカルポリシーは、Web Studioコンソールで作成および管理され、サイトデータベースに保存されます。グループポリシーは、Microsoftグループポリシー管理コンソール（GPMC）を使用して作成および管理され、Active Directoryに保存されます。Microsoftローカルポリシーは、Windowsオペレーティングシステムで作成され、レジストリに保存されます。

Studioは、モデリングウィザードを使用して、管理者がテンプレートとポリシー内の構成設定を比較し、競合する設定や冗長な設定を排除するのに役立ちます。管理者はGPMCを使用してGPOを設定し、設定を構成できます。また、それらをネットワークのさまざまなレベルのターゲットユーザーセットに適用することもできます。

これらのGPOはActive Directoryに保存されます。これらの設定の管理へのアクセスは、セキュリティ上の理由からほとんどのIT担当者に対して制限されています。

設定は、優先度とその条件に従ってマージされます。無効な設定は、下位の有効な設定を上書きします。未構成のポリシー設定は無視され、下位の設定を上書きしません。

ローカルポリシーは、Active Directory内のグループポリシーと競合することもあり、状況によっては互いに上書きし合う可能性があります。

すべてのポリシーは次の順序で処理されます。

1. エンドユーザーはドメイン資格情報を使用してマシンにログオンします。
2. 資格情報はドメインコントローラーに送信されます。
3. Active Directoryは、すべてのポリシー（エンドユーザー、エンドポイント、組織単位、ドメイン）を適用します。
4. エンドユーザーはCitrix Workspace™アプリにログオンし、アプリケーションまたはデスクトップにアクセスします。
5. Citrix と Microsoft のポリシーは、エンドユーザーとリソースをホストするマシンに対して処理されます。
6. Active Directory はポリシー設定の優先順位を決定します。その後、それらをエンドポイントデバイスのレジストリと、リソースをホストするマシンに適用します。
7. エンドユーザーがリソースからログオフします。エンドユーザーとエンドポイントデバイスに対する Citrix ポリシーは無効になります。
8. エンドユーザーがユーザーデバイスからログオフすると、GPO ユーザーポリシーが解放されます。
9. エンドユーザーがデバイスの電源を切ると、GPO マシンポリシーが解放されます。

ユーザー、デバイス、マシンのグループに対してポリシーを作成する場合、一部のメンバーは異なる要件を持つ可能性があり、一部のポリシー設定に例外が必要になることがあります。例外は、ポリシーが誰または何に影響するかを決定する Studio および GPMC のフィルターによって作成されます。

> **注:**
>
> 同じ GPO 内で Windows ポリシーと Citrix ポリシーを混在させることはサポートしていません。

ポリシーの操作

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

ユーザーアクセスとセッション環境を制御するためにCitrixポリシーを構成します。Citrixポリシーは、接続、セキュリティ、帯域幅の設定を制御する最も効率的な方法です。特定のユーザーグループ、デバイス、または接続タイプに対してポリシーを作成できます。各ポリシーには複数の設定を含めることができます。

Citrixポリシーを操作するためのツール

Citrixポリシーでは、次のツールを使用できます。

- **Web Studio。** グループポリシーを管理する権限のないCitrix管理者の場合は、Web Studioを使用してサイトのポリシーを作成します。Web Studioを使用して作成されたポリシーはサイトデータベースに保存され、更新はVDAがブローカーに登録されたとき、またはユーザーがそのVDAに接続したときにVDAにプッシュされます。
- **ローカルグループポリシーエディター** (Microsoft Management Consoleスナップイン)。ネットワーク環境でActive Directoryを使用しており、グループポリシーを管理する権限がある場合は、ローカルグループポリシーエディターを使用してサイトのポリシーを作成できます。構成

した設定は、グループポリシー管理コンソールで指定したグループポリシーオブジェクト (GPO) に影響します。

重要:

一部のポリシー設定を構成するには、ローカルグループポリシーエディターを使用することをお勧めします。例としては、VDAをコントローラーに登録するための設定や、Microsoft App-Vサーバーに関連する設定などがあります。 追加のポリシー検証が追加されます。その結果、無効なポリシー設定が存在する場合、インプレースアップグレードを行うとポリシーデータが失われる可能性があります。Web Studio以外の方法でポリシーを作成または編集する場合は、最新バージョンのSDKとスナップインを使用することをお勧めします。

ポリシーの処理順序と優先順位

グループポリシー設定は、次の順序で処理されます。

1. ローカルGPO
2. Virtual Apps and DesktopsサイトGPO (サイトデータベースに保存)
3. サイトレベルのGPO
4. ドメインレベルのGPO
5. 組織単位

ただし、競合が発生した場合、最後に処理されたポリシー設定が、以前に処理された設定を上書きします。ポリシー設定の優先順位は次のとおりです。

1. 組織単位
2. ドメインレベルのGPO
3. サイトレベルのGPO
4. Virtual Apps and DesktopsサイトGPO（サイトデータベースに保存）
5. ローカルGPO

たとえば、Citrix管理者がWeb Studioを使用して、会社の営業担当者向けにクライアントファイルリダイレクトを有効にするポリシー（ポリシーA）を作成します。一方、別の管理者がグループポリシーエディターを使用して、営業担当者向けにクライアントファイルリダイレクトを無効にするポリシー（ポリシーB）を作成します。営業担当者が仮想デスクトップにログオンすると、ポリ

シーBが適用され、ポリシーAは無視されます。その理由は、ポリシーBがドメインレベルで処理され、ポリシーAがVirtual Apps and DesktopsサイトGPOレベルで処理されたためです。

ただし、ユーザーがICA®またはリモートデスクトッププロトコル（RDP）セッションを起動すると、Citrixセッション設定が、Active Directoryポリシーまたはリモートデスクトップセッションホスト構成で構成された同じ設定を上書きします。この設定には、一般的なRDPクライアント接続設定に関連する設定が含まれます。RDPクライアント接続設定の例としては、デスクトップの壁紙、メニューアニメーション、ドラッグ中のウィンドウコンテンツの表示などがあります。

複数のポリシーを使用する場合、競合する設定を含むポリシーに優先順位を付けることができます。詳しくは、「ポリシーの比較、優先順位付け、モデル化、トラブルシューティング」を参照してください。

Citrixポリシーのワークフロー

ポリシーを構成するプロセスは次のとおりです。

1. ポリシーを作成します。
2. ポリシー設定を構成します。
3. ポリシーをマシンオブジェクトとユーザーオブジェクトに割り当てます。
4. ポリシーの優先順位を設定します。
5. Citrix Group Policy Modelingウィザードを実行して、有効なポリシーを確認します。

> **注:**
>
> Citrix Group Policy Modelingウィザードを開くには、**Policies > Modeling**タブに移動し、アクションバーで**Launch Modeling Wizard**をクリックします。**Modeling**タブは、お客様の要望に応じてWeb Studioで利用できます。

Citrixポリシーと設定をナビゲートする

ローカルグループポリシーエディターでは、ポリシーと設定は「コンピューターの構成」と「ユーザーの構成」の2つのカテゴリに表示されます。各カテゴリにはCitrixポリシーノードがあります。このスナップインのナビゲーションと使用方法の詳細については、Microsoftのドキュメントを参照してください。

Web Studioでは、ポリシー設定は、影響を与える機能または特徴に基づいてカテゴリに分類されます。たとえば、**Profile Management**セクションには、Profile Managementのポリシー設定が含まれています。

- コンピューター設定（マシンに適用されるポリシー設定）は、仮想デスクトップの動作を定義し、仮想デスクトップの起動時に適用されます。これらの設定は、仮想デスクトップ上でアクティブなユーザーセッションがない場合でも適用されます。
- ユーザー設定は、ICAを使用して接続する際のユーザーエクスペリエンスを定義します。ユーザーポリシーは、ユーザーがICAを使用して接続または再接続するときに適用されます。ユーザーがRDPを使用して接続したり、コンソールに直接ログオンしたりする場合は、ユーザーポリシーは適用されません。

  ポリシー、設定、またはテンプレートにアクセスするには、Web Studioの左ペインで**Policies**を選択します。

  - **Policies**タブにはすべてのポリシーが一覧表示されます。ポリシーを選択すると、下部に次のタブが表示されます。
    - 概要 - 名前、優先度、有効/無効の状態、および説明を一覧表示します
    - 設定 - 構成されているすべての設定を一覧表示します
    - 割り当て先 - ポリシーが割り当てられているユーザーオブジェクトとマシンオブジェクトを一覧表示します。 詳細については、「ポリシーの作成」を参照してください。
  - 「**テンプレート**」タブには、Citrix が提供するテンプレートと、作成したカスタムテンプレートが一覧表示されます。テンプレートを選択すると、下部に次のタブが表示されます。
    - 説明（テンプレートを使用する理由）
    - 設定（構成された設定のリスト）。詳細については、「ポリシーテンプレート」を参照してください。
  - **比較**タブでは、ポリシーまたはテンプレートの設定を、他のポリシーまたはテンプレートの設定と比較できます。たとえば、ベストプラクティスへの準拠を確実にするために、設定値を確認したい場合があります。詳細については、「ポリシーの比較、優先順位付け、モデル化、トラブルシューティング」を参照してください。

  ポリシーまたはテンプレートで設定を検索するには：

  a. ポリシーまたはテンプレートを選択します。
  b. アクションバーで**ポリシーの編集**または**テンプレートの編集**を選択します。

c. **設定**ページで、**検索**フィールドに設定の名前を入力します。

次の項目を選択して、検索を絞り込むことができます。

- 特定の製品バージョン
- カテゴリ（例: 帯域幅）
- 設定名に含まれるキーワード
- 「**選択済みのみ表示**」チェックボックス
- 選択したポリシーに追加された設定のみを検索する場合。

フィルタリングされていない検索の場合は、**すべての設定**を選択します。

- ポリシー内の設定を検索するには:

a. ポリシーを選択します。

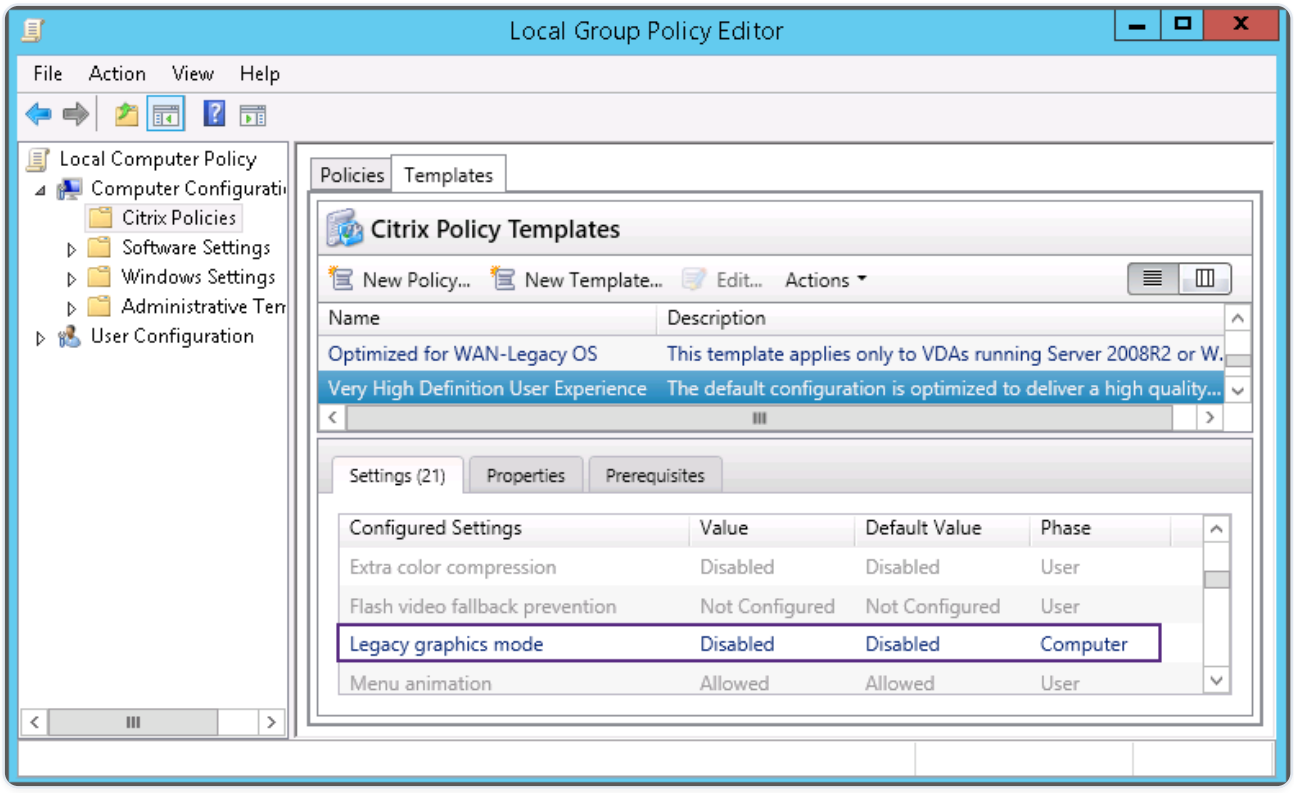
b. **設定**タブを選択し、設定の名前を入力します。

特定の製品バージョンを選択するか、カテゴリを選択して検索を絞り込むことができます。フィルタリングされていない検索の場合は、**すべての設定**を選択します。

ポリシーは、一度作成されると、使用されたテンプレートとは独立します。新しいポリシーの**説明**フィールドを使用して、使用されたソーステンプレートを追跡できます。

グループポリシーエディターでは、コンピューター設定とユーザー設定は、両方の種類の設定を含むテンプレートから作成された場合でも、個別に適用する必要があります。この例では、コンピューターの構成で「非常に高精細なユーザーエクスペリエンス」を使用することを選択しています。

- レガシーグラフィックモードは、このテンプレートから作成されたポリシーで使用されるコンピューター設定です。
- グレー表示されているユーザー設定は、このテンプレートから作成されたポリシーでは使用されません。



ポリシーテンプレート

注:

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

テンプレートは、特定の成果を達成するためのポリシー作成に使用することが推奨される設定の集合体です。たとえば、エンドユーザーに高精細なユーザーエクスペリエンスを提供するためのポリシーを作成する場合、「Very High Definition User Experience」テンプレートで定義されている設定を、そのようなポリシーを作成するための参照点および開始点として使用できます。

テンプレートはポリシーではありません。テンプレートは、Citrixポリシー設定の補足ドキュメントです。これらは、特定のユーザー関連設定の集合的な機能を示します。

テンプレートの使用は任意です。管理者はテンプレートを使用せずにポリシーを作成できます。テンプレートは、サイトをどのように構成すべきかについて大まかなアイデアを持っているものの、目的の構成を実現するためにどの設定を使用すべきか確信が持てない管理者にとって役立ちます。

管理者は、既存のテンプレート、既存のポリシー、またはゼロからテンプレートを作成できます。

ADMX/ADML

ここで説明するCitrixグループポリシーテンプレートは、Windowsポリシーテンプレートとは関係ありません。ここで説明するテンプレートとWindowsポリシーテンプレートは、2つの異なる概念です。CitrixグループポリシーテンプレートはADMXファイルではありません。

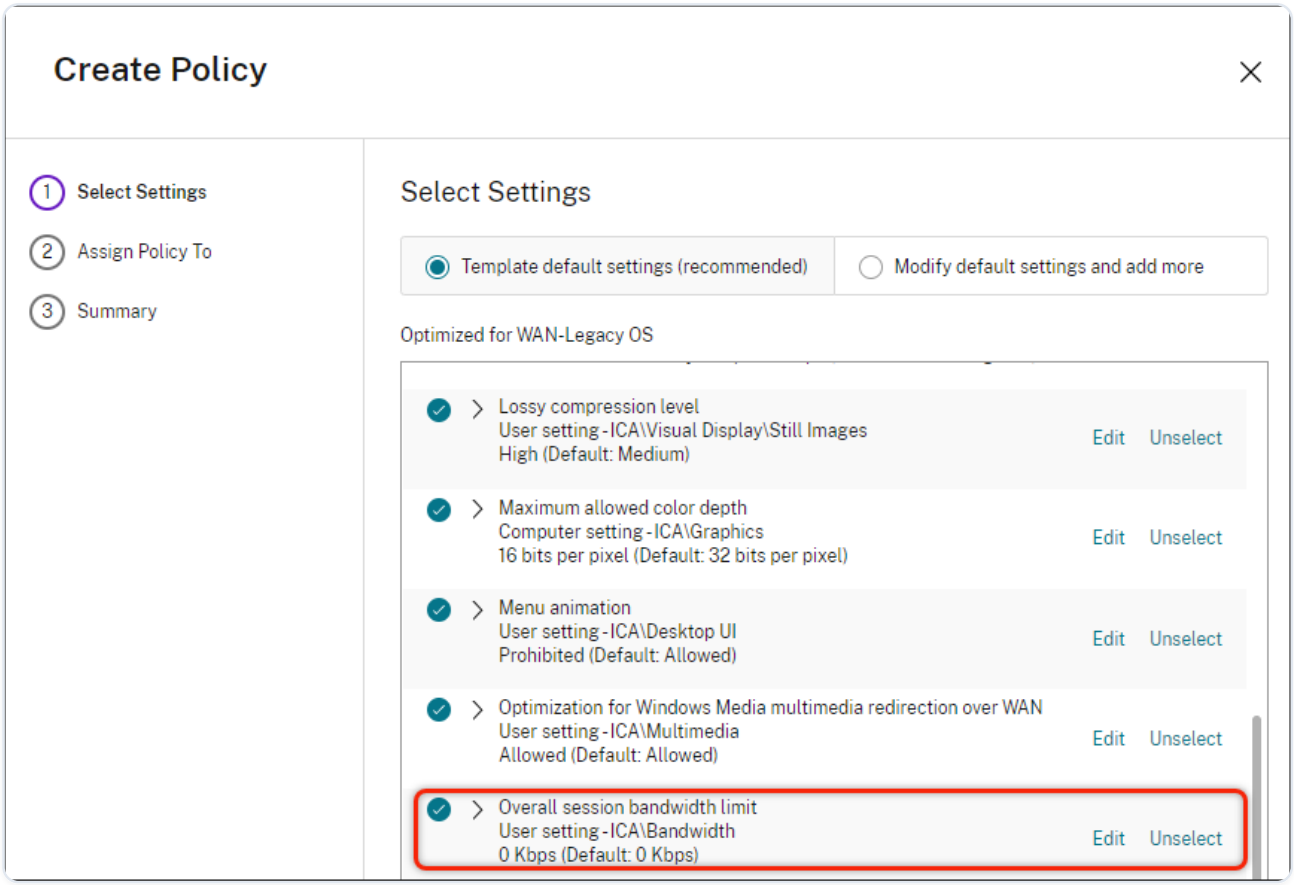
組み込みのCitrixテンプレート

以下のポリシーテンプレートが利用可能です。

- **Very High Definition User Experience**。このテンプレートは、ユーザーエクスペリエンスを最大化するデフォルト設定を適用します。複数のポリシーが優先順位に従って処理されるシナリオでこのテンプレートを使用します。
- **High Server Scalability**。このテンプレートを適用して、サーバーリソースを節約します。このテンプレートは、ユーザーエクスペリエンスとサーバーのスケーラビリティのバランスを取ります。単一サーバーでホストできるユーザー数を増やしながら、良好なユーザーエクスペリエンスを提供します。このテンプレートは、グラフィックの圧縮にビデオコーデックを使用せず、サーバー側のマルチメディアレンダリングを防止します。
- **High Server Scalability-Legacy OS**。このHigh Server Scalabilityテンプレートは、Windows Server 2008 R2またはWindows 7以前を実行しているVDAにのみ適用されます。このテンプレートは、これらのオペレーティングシステムにより効率的なレガシーグラフィックモードに依存しています。
- **NetScaler SD-WAN向けに最適化**。Citrix Virtual Desktopsの配信を最適化するために、NetScaler SD-WANを使用している支社のユーザーにこのテンプレートを適用します。(NetScaler SD-WANはCloudBridgeの新しい名称です)。
- **WAN向け最適化**。このテンプレートは、共有WAN接続を使用するブランチオフィスのタスクワーカー、またはグラフィックがシンプルなユーザーインターフェイスとマルチメディアコンテンツが少ないアプリケーションにアクセスする低帯域幅接続のリモートロケーション向けです。このテンプレートは、ビデオ再生エクスペリエンスと一部のサーバー拡張性を犠牲にして、帯域幅効率を最適化します。
- **WAN向け最適化 - レガシーOS**。この*WAN向け最適化*テンプレートは、Windows Server 2008 R2またはWindows 7以前を実行しているVDAにのみ適用されます。このテンプレートは、これらのオペレーティングシステムにとってより効率的なレガシーグラフィックモードに依存しています。
- **セキュリティと制御**。このテンプレートは、リスク許容度が低い環境で、Citrix Virtual Apps and Desktopsでデフォルトで有効になっている機能を最小限に抑えるために使用します。この

テンプレートには、ユーザーデバイスでの印刷、クリップボード、周辺機器、ドライブマッピング、ポートリダイレクト、Flashアクセラレーションへのアクセスを無効にする設定が含まれています。このテンプレートを適用すると、より多くの帯域幅を使用し、サーバーあたりのユーザー密度が低下する可能性があります。

Citrixの組み込みテンプレートをデフォルト設定で使用することをお勧めしますが、特定の推奨値を持たない設定もあります。たとえば、WAN向け最適化テンプレートに含まれる**セッション全体の帯域幅制限**などです。この場合、管理者がこの設定がシナリオに適用される可能性が高いことを理解できるように、テンプレートがその設定を公開しています。



XenAppおよびXenDesktop 7.6 FP3より前の展開（ポリシー管理およびVDA）を使用しており、高サーバー拡張性およびWAN向け最適化テンプレートが必要な場合は、該当する場合、これらのテンプレートのレガシーOSバージョンを使用してください。

注：

Citrixは組み込みテンプレートを作成および更新します。これらのテンプレートは変更または削除できません。

Web Studioを使用したテンプレートの作成と管理

テンプレートに基づいてテンプレートを作成するには：

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。
2. **テンプレート**タブを選択し、テンプレートを作成する元となるテンプレートを選択します。
3. **テンプレートの作成**タブを選択します。**設定の選択**画面が表示されます。
4. テンプレートに含めるポリシー設定を選択して構成します。
5. 「**次へ**」をクリックします。「**概要**」画面が表示されます。
6. テンプレートの名前を入力します。
7. **完了**をクリックします。新しいテンプレートが**テンプレート**タブに表示されます。

ポリシーに基づいてテンプレートを作成するには：

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。
2. **ポリシー**タブを選択し、テンプレートを作成する元となるポリシーを選択します。
3. **その他**タブをクリックします。
4. 「**テンプレートとして保存**」を選択します。「**設定の選択**」画面が表示されます。
5. テンプレートに含める新しいポリシー設定を選択して構成します。
6. 「**次へ**」をクリックします。「**概要**」画面が表示されます。
7. テンプレートの名前と説明を入力し、「**完了**」をクリックします。

テンプレートと委任管理

Web Studioのテンプレートはサイトデータベースに保存されますが、Citrix Studioのテンプレートは、現在の管理者のユーザープロファイルフォルダーに`.gpt`拡張子を持つファイルとして保存されます。ある管理者が作成したCitrix Studioのテンプレートは、他の管理者や、別のマシン上の同じ管理者には表示されません。Web Studioのテンプレートは、権限と委任管理の対象となるすべての管理者に表示されます。

ポリシーの作成

> **注:**
>
> Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb

> Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> ポリシーを作成する前に、それが影響を与える可能性のあるユーザーまたはデバイスのグループを決定してください。ユーザーの職務、接続タイプ、ユーザーデバイス、または地理的な場所に基づいてポリシーを作成することができます。Windows Active Directoryグループポリシーで使用するのと同じ基準を使用することもできます。

すでにグループに適用されるポリシーを作成している場合は、別のポリシーを作成するのではなく、そのポリシーを編集することを検討してください。ポリシーを編集した後、適切な設定を構成します。特定の機能を有効にするためだけにポリシーを作成したり、特定のユーザーにポリシーが適用されないようにするためだけにポリシーを作成したりすることは避けてください。

ポリシーを作成する際、ポリシーテンプレートの設定に基づいて作成し、必要に応じて設定をカスタマイズできます。テンプレートを使用せずに、必要なすべての設定を追加して作成することもできます。

Web Studioでは、**ポリシーを有効にする**チェックボックスが明示的にチェックされていない限り、新しく作成されたポリシーは無効に設定されます。

ポリシー作成時および設定構成時に、システムは設定タイプを表示するオプションを提供します。次の設定タイプを表示できます。

- すべての設定 - すべてのVDAバージョンに適用されるすべての設定を表示
- 現在の設定のみ - 現在のVDAバージョンに固有の設定を表示
- レガシー設定のみ - 非推奨のVDAバージョンにのみ適用される設定を表示

設定を構成しながら設定を表示するには：

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。
2. **ポリシー**タブで、**ポリシーの作成**をクリックします。
3. **設定の選択**テーブルで、**設定**の横にあるドロップダウンをクリックします。
4. ドロップダウンから以下のいずれかのオプションを選択します。

- すべての設定 - すべてのVDAバージョンのすべての設定を表示します。
- 現在の設定のみ - 現在のVDAバージョンのみの設定を表示します。
- レガシー設定のみ - 非推奨のVDAバージョンのみの設定を表示します。

1. 「**設定**」テーブルには、前の手順に基づいて利用可能な設定が一覧表示されます。

ポリシー設定

ポリシー設定は、有効、無効、または未構成にできます。デフォルトでは、ポリシー設定は構成されていません。つまり、ポリシーに追加されていません。設定は、ポリシーに追加された場合にのみ適用されます。

ポリシー設定は、依存ポリシー間の明確さを提供するために強化されています。この機能により、子ポリシー設定が構成されたときに有効になるように、親ポリシーが最初に構成されることが保証されます。

ポリシー設定を構成するには：

1. **ポリシーの作成**ページで、**設定の選択**の下にある「overall」を検索します。 **セッション全体の帯域幅制限**に関連するすべてのポリシー（親と子）が一覧表示されます。
2. 子ポリシーにカーソルを合わせると、**セッション全体の帯域幅制限**親ポリシーが構成されるまで、子ポリシーは構成できないことを示すツールヒントが表示されます。
3. 親ポリシー設定を構成し、次に子ポリシー設定を構成して、**保存**をクリックします。
4. **設定**列と**現在の値**列には、**ポリシーの作成/編集**テーブルで構成された値が表示されます。このテーブルには、構成された設定を変更するための**編集**オプションが表示されます。

依存ポリシー設定(/en-us/citrix-daas/media/dependent-policy-settings.png)

> **注**:
>
> - 親ポリシーが構成されるまで、子ポリシーは選択できません。
> - 親ポリシーのチェックが外れると、関連付けられている子ポリシーもチェックが外れるか、選択解除されることを示すポップアップメッセージが表示されます。

次の表に、親ポリシーと、それに対応する依存ポリシーまたは子ポリシーのリストを示します。

親ポリシー	依存子ポリシー
セッション全体の帯域幅制限	オーディオリダイレクト帯域幅制限の割合
	クリップボードリダイレクト帯域幅制限の割合

親ポリシー	依存子ポリシー
	COMポートリダイレクト帯域幅制限の割合
	ファイルリダイレクト帯域幅制限の割合
	HDX™ MediaStreamマルチメディアアクセラレーション帯域幅制限の割合
	LPTポートリダイレクト帯域幅制限の割合
	プリンターリダイレクト帯域幅制限の割合
	クライアントUSBデバイスリダイレクト帯域幅制限の割合
	TWAINデバイスリダイレクト帯域幅制限の割合
双方向コンテンツリダイレクトを許可	クライアントにリダイレクトされる許可されたURL
	VDAにリダイレクトされる許可されたURL
CPU使用率	CPU使用率から除外されるプロセスの優先度
レガシーグラフィックモード	プログレッシブ圧縮レベル
セッションウォーターマークを有効にする	ウォーターマークのカスタムテキスト
	セッションウォーターマークのスタイル
	透かしの透明度
HDXアダプティブトランスポート	オーディオのロストレラントモード

一部のポリシー設定は、次のいずれかの状態になります。

- 許可または禁止は、設定によって制御されるアクションを許可または禁止します。セッション内で設定のアクションを管理することをユーザーに許可または禁止する場合があります。たとえば、メニューアニメーション設定が「許可」に設定されている場合、ユーザーはクライアント環境でメニューアニメーションを制御できます。

- 有効または無効は、設定をオンまたはオフにします。設定を無効にすると、下位のポリシーでは有効になりません。

さらに、一部の設定は、依存する設定の有効性を制御します。たとえば、クライアントドライブリダイレクトは、ユーザーがデバイス上のドライブにアクセスできるかどうかを制御します。ユーザーがネットワークドライブにアクセスできるようにするには、この設定と「**クライアントネットワークドライブ**」設定の両方をポリシーに追加する必要があります。「**クライアントドライブリダイレクト**」設定が無効になっている場合、「**クライアントネットワークドライブ**」設定が有効になっていても、ユーザーはネットワークドライブにアクセスできません。

一般に、マシンに影響を与えるポリシー設定の変更は、仮想デスクトップが再起動したとき、またはユーザーがログオンしたときに有効になります。ユーザーに影響を与えるポリシー設定の変更は、ユーザーが次回ログオンしたときに有効になります。Active Directoryを使用している場合、ポリシー設定はActive Directoryが90分間隔でポリシーを再評価するときに更新されます。そして、ポリシー設定は、仮想デスクトップが再起動したとき、またはユーザーがログオンしたときに適用されます。

一部のポリシー設定では、設定をポリシーに追加するときに値を入力または選択できます。「デフォルト値を使用」を選択することで、設定の構成を制限できます。この選択により、設定の構成が無効になり、ポリシーが適用されるときに設定のデフォルト値のみが使用されるようになります。この選択は、「デフォルト値を使用」を選択する前に入力された値に関係なく適用されます。

セキュアデフォルト設定が有効になっている場合、VDAインストール中に、ポリシー設定の優先順位は次のように影響を受けます。

- カスタマイズされた設定が最も高い優先順位を持ちます
- セキュアなデフォルト設定が2番目の優先順位を持ちます
- デフォルト設定が最も低い優先順位を持ちます

ポリシーのセキュアデフォルト設定を表示するには：

1. Web Studioにログインします。
2. 左側のナビゲーションで、**ポリシー**をクリックします。
3. **ポリシー**タブで、**ポリシーの作成**をクリックします。
4. **設定の選択**テーブルで、現在の値が**許可？**となっている設定にカーソルを合わせると、**セキュアなデフォルト値: 禁止**が表示されます。

   セキュアなデフォルト設定 (en-us/citrix-virtual-apps-desktops/2402-ltsr/media/secure-default-setting.png)

ベストプラクティスとして：

- ポリシーは個々のユーザーではなく、グループに割り当てます。グループにポリシーを割り当てると、グループへのユーザーの追加または削除時に割り当てが自動的に更新されます。
- リモートデスクトップセッションホスト構成で、競合する設定や重複する設定を有効にしないでください。リモートデスクトップセッションホスト構成は、Citrixポリシー設定と同様の機能を提供することがあります。トラブルシューティングを容易にするため、可能な限りすべての設定を一貫性のある状態（有効または無効）に保ってください。
- 使用されていないポリシーは無効にします。設定が追加されていないポリシーは、不要な処理を発生させます。

ポリシーの割り当て

ポリシーを作成する際、特定のユーザーおよびマシンオブジェクトに割り当てます。そのポリシーは、特定の基準またはルールに従って接続に適用されます。一般的に、基準の組み合わせに基づいて、ポリシーに好きなだけ割り当てを追加できます。

割り当てを指定しない場合、または割り当てを指定しても無効にする場合、ポリシーは**すべて**の接続に適用されます。

> **注:**
>
> ポリシーの割り当ては、ポリシーフィルターとも呼ばれます。詳細については、以下のトピックを参照してください。
>
> - ポリシーのフィルターを作成、変更、または削除する
> - フィルターはどのように適用されますか？
>
> 次の表に、利用可能な割り当てを示します。

割り当て名	ポリシーの適用基準
アクセス制御	クライアントが接続する際のアクセス制御条件。*接続の種類* - NetScaler® Gatewayを使用する接続と使用しない接続のどちらにポリシーを適用するか。*NetScaler Gatewayファーム名* - NetScaler Gateway仮想サーバーの名

割り当て名	ポリシーの適用基準
	前。*アクセス条件* - 使用するエンドポイント分析ポリシーまたはセッションポリシーの名前。
NetScaler SD-WAN	ユーザーセッションがNetScaler SD-WANを介して起動されるかどうか。**注：**ポリシーには、NetScaler SD-WANの割り当てを1つだけ追加できます。
クライアントIPアドレス	セッションへの接続に使用されるユーザーデバイスのIPアドレス：IPv4の例：12.0.0.0、12.0.0.*、12.0.0.1-12.0.0.70、12.0.0.1/24。IPv6の例：2001:0db8:3c4d:0015:0:0:abcd:ef12、2001:0db8:3c4d:0015::/54
クライアント名	ユーザーデバイスの名前。完全一致: ClientABCName。ワイルドカードの使用: Client*Name。
デリバリーグループ	デリバリーグループのメンバーシップ。
デリバリーグループの種類	デスクトップまたはアプリケーションの種類: プライベートデスクトップ、共有デスクトップ、プライベートアプリケーション、または共有アプリケーション。**注:** プライベートデスクトップと共有デスクトップのフィルターオプションは、Citrix Virtual Apps and Desktops 7.xでのみ利用可能です。詳細については、CTX219153を参照してください。
組織単位 (OU)	組織単位。
タグ	タグ。**注:** このポリシーをすべてのタグ付きマシンに適用します。アプリケーションタグは含まれません。
ユーザーまたはグループ	ユーザーまたはグループ名。

ユーザーがログオンすると、接続の割り当てに一致するすべてのポリシーが識別されます。これらのポリシーは優先順位順に並べ替えられ、設定の複数のインスタンスが比較されます。各設定

は、ポリシーの優先順位に従って適用されます。無効になっているポリシー設定は、有効になっている下位ランクの設定よりも優先されます。構成されていないポリシー設定は無視されます。

> **重要:**

> Group Policy Management Console を使用して Active Directory ポリシーと Citrix ポリシーの両方を構成する場合、割り当てと設定が期待どおりに適用されないことがあります。詳細については、CTX127461を参照してください。

> 「Unfiltered」という名前のポリシーがデフォルトで提供されます。

- Web Studioを使用してCitrixポリシーを管理する場合、「Unfiltered」ポリシーに追加した設定は、サイト内のすべてのサーバー、デスクトップ、および接続に適用されます。
- ローカルグループポリシーエディターを使用してCitrixポリシーを管理する場合、「Unfiltered」ポリシーに追加した設定は、すべてのサイトと接続に適用されます。サイトと接続は、ポリシーを含むグループポリシーオブジェクト (GPO) のスコープ内にある必要があります。たとえば、営業OUには、米国の営業チームのすべてのメンバーを含むSales-USというGPOが含まれています。Sales-US GPOは、複数のユーザーポリシー設定を含むUnfilteredポリシーで構成されています。米国の営業マネージャーがサイトにログオンすると、Unfilteredポリシーの設定がセッションに自動的に適用されます。この構成は、ユーザーがSales-US GPOのメンバーであるためです。

割り当てのモードは、ポリシーがすべての割り当て基準に一致する接続にのみ適用されるかどうかを決定します。モードが (デフォルト) に設定されている場合、ポリシーは割り当て基準に一致する接続にのみ適用されます。モードが に設定されている場合、接続が割り当て基準に一致しない場合にポリシーが適用されます。以下の例は、複数の割り当てが存在する場合に割り当てモードが Citrix ポリシーにどのように影響するかを示しています。

- **例: モードが異なる同種の割り当て** - 同じ種類の2つの割り当てがあり、一方が に設定され、もう一方が に設定されているポリシーでは、接続が両方の割り当てを満たす場合、 に設定された割り当てが優先されます。例:

  ポリシー 1 には次の割り当てが含まれます。

  - 割り当て A は Sales グループを指定します。モードは に設定されています。
  - 割り当て B は営業マネージャーのアカウントを指定します。モードは に設定されています。

割り当て B のモードが に設定されているため、ユーザーが Sales グループのメンバーであっても、営業マネージャーがサイトにログオンしたときにポリシーは適用されません。

- **例: モードが同じでタイプが異なる割り当て** - タイプが異なる2つ以上の割り当てがあり、 に設定されているポリシーでは、ポリシーが適用されるためには、接続が各タイプの少なくとも1つの割り当てを満たす必要があります。例:

  ポリシー 2 には次の割り当てが含まれます。

  - 割り当て C は、Sales グループを指定するユーザー割り当てです。モードは に設定されています。
  - 割り当て D は、10.8.169.* (企業ネットワーク) を指定するクライアント IP アドレス割り当てです。モードは に設定されています。

  営業マネージャーがオフィスからサイトにログオンすると、接続が両方の割り当てを満たすため、ポリシーが適用されます。

  ポリシー3には、次の割り当てが含まれます。

  - 割り当て E は、Sales グループを指定するユーザー割り当てです。モードは「許可」に設定されています。
  - 割り当て F は、NetScaler Gateway 接続条件を指定するアクセス制御割り当てです。モードは「許可」に設定されています。

  営業マネージャーがオフィスからサイトにログオンしても、接続が割り当て F を満たさないため、ポリシーは適用されません。

Web Studio を使用して、テンプレートに基づいてポリシーを作成する

1. Web Studio にサインインし、左ペインで を選択します。
2. タブを選択し、テンプレートを選択します。
3. アクションバーで を選択します。
4. デフォルトでは、新しいポリシーはテンプレート内のすべてのデフォルト設定を使用します。この場合、 が選択されています。設定を変更する場合は、 を選択し、設定を追加または削除します。
5. 次のいずれかを選択して、ポリシーの適用方法を指定します。

   - 。ポリシーを選択したユーザーおよびマシンオブジェクトに適用するには、 をクリックして、ポリシーを適用する必要があるユーザーおよびマシンオブジェクトを選択します。
   - 。ポリシーをサイト内のすべてのユーザーおよびマシンオブジェクトに適用します。

6. ポリシーの名前を入力します。ポリシーが影響する対象 (例: 経理部、リモートユーザー) に応じて名前を付けることを検討してください。必要に応じて、説明を追加します。

   ポリシーはデフォルトで無効になっていますが、有効にすることができます。ポリシーを有効にすると、ログオンするユーザーにすぐに適用されます。無効にすると、ポリシーは適用されません。ポリシーの優先順位を付けたり、後で設定を追加したりする必要がある場合は、適用する準備が整うまでポリシーを無効にしておくことを検討してください。

Web Studio を使用してポリシーを作成する

1. Web Studio にサインインし、左ペインで を選択します。
2. **ポリシー**タブを選択します。
3. アクションバーで**ポリシーの作成**を選択します。
4. ポリシー設定を追加および構成します。
5. 次のいずれかを選択して、ポリシーを適用する方法を指定します。

   - 選択したユーザーオブジェクトとマシンオブジェクトに割り当ててから、ポリシーを適用する必要があるユーザーオブジェクトとマシンオブジェクトを選択します。
   - サイト内のすべてのオブジェクトに割り当てて、サイト内のすべてのユーザーオブジェクトとマシンオブジェクトにポリシーを適用します。

6. ポリシーの名前を入力するか、デフォルトを受け入れます。ポリシーが影響する対象（例: 経理部、リモートユーザーなど）に基づいてポリシーに名前を付けることを検討してください。必要に応じて、説明を追加します。

   ポリシーはデフォルトで有効になっていますが、無効にすることもできます。ポリシーを有効にすると、ログオンするユーザーにすぐに適用されます。無効にすると、ポリシーの適用が防止されます。ポリシーの優先順位を付けたり、後で設定を追加したりする必要がある場合は、適用する準備ができるまでポリシーを無効にしておくことを検討してください。

グループポリシーエディターを使用してポリシーを作成および管理する

グループポリシーエディターで、**コンピューターの構成またはユーザーの構成**を展開します。**ポリシー**ノードを展開し、**Citrixポリシー**を選択します。適切なアクションを選択します。

タスク	手順
ポリシーを作成する	**ポリシー**タブで、**新規**をクリックします。

タスク	手順
既存のポリシーを編集する	「**ポリシー**」タブでポリシーを選択し、「**編集**」をクリックします。
既存のポリシーの優先度を変更する	「**ポリシー**」タブでポリシーを選択し、「**上位**」または「**下位**」をクリックします。
ポリシーに関する概要情報を表示する	「**ポリシー**」タブでポリシーを選択し、「**概要**」タブをクリックします。
ポリシー設定を表示および修正する	「**ポリシー**」タブでポリシーを選択し、「**設定**」タブをクリックします。
ポリシーフィルターを表示および修正する	「**ポリシー**」タブでポリシーを選択し、「**フィルター**」タブをクリックします。ポリシーに複数のフィルターを追加する場合、ポリシーが適用されるには、すべてのフィルター条件が満たされている必要があります。
ポリシーを有効または無効にする	「**ポリシー**」タブでポリシーを選択し、「**アクション > 有効**」または「**アクション > 無効**」のいずれかを選択します。
既存のテンプレートからポリシーを作成する	「**テンプレート**」タブでテンプレートを選択し、「**新規ポリシー**」をクリックします。

ポリシーセット

ポリシーセットは、Citrix Virtual Apps and Desktops™ のオブジェクトであり、ポリシーを集約して、簡素化されたロールベースのアクセスと容易な管理を可能にします。管理者チームや会社の論理的な区分を反映するようにポリシーセットを作成できます。例えば、地理的な地域、事業単位、または特定のユースケースごとにポリシーセットを作成できます。作成後、スコープとデリバリーグループがポリシーセットに割り当てられ、承認された管理者のみが、関連するユーザーとマシンに適用されるポリシーを管理できるようになります。

> **注:**
>
> ポリシーセットを有効にする前に、Citrix® は以下の点に注意することを推奨します。

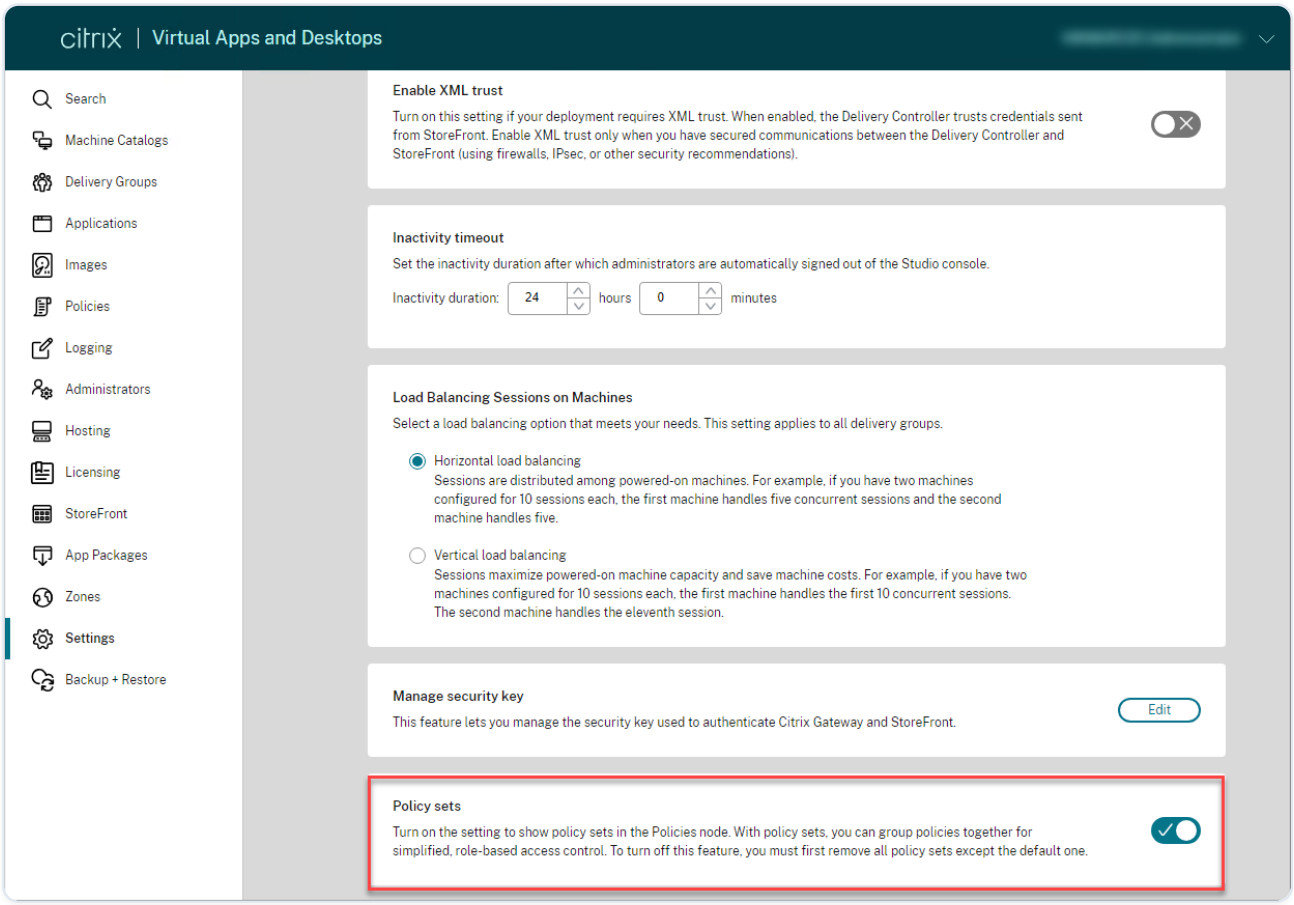
- 追加のポリシー検証が追加されます。その結果、無効なポリシー設定が存在する場合、インプレースアップグレードを行うとポリシーデータが失われる可能性があります。
- 無効なデータを検出するには、GPOスキャナーツール を使用し、アップグレード前に必要な編集を行ってください。詳細については、CTX676686 を参照してください。
- 今後のすべてのアップグレードでは、最新のSDKを使用することをCitrixは推奨します。古いSDKを使用してポリシーを更新すると、無効なデータがポリシー設定に追加される可能性があり、ポリシーデータが失われるリスクにつながる可能性があります。

利点

- 分散型管理者チーム向けのロールベースのアクセス制御
- 合併、買収、統合の簡素化
- 限定された障害ドメイン
- ポリシーのマルチテナントサポート

ポリシーセットを有効にする

Virtual Apps and Desktops の **管理** タブから、**設定** に移動し、**ポリシーセット** の設定をオンにします。



注:

ポリシーセットを作成する前に、ポリシーセットを有効にする必要があります。

機能比較

ポリシーセット適用前	ポリシーセット適用後
サイト全体のポリシー、設定、フィルター、およびポリシーの優先順位は、Citrix Studio内で一箇所で構成されます。	ポリシー、設定、フィルター、およびポリシーの優先順位は、各ポリシーセットに対して個別に構成されます。
1つのポリシーを管理する場合、すべてのポリシーを管理する必要があります。	フル管理者は、特定のポリシーセットを個別に管理する機能を下位レベルの管理者に委任できます。
大規模で分散された環境のポリシーは、複雑になり管理が困難になります。	大規模で分散された環境のポリシーは、簡単に分割して管理できます。

ポリシーセットの仕組み?

概要

- ポリシーセットはデリバリーグループに割り当てられます
- ポリシーセットには、1つまたは複数のスコープがあります。
- ポリシーセットが割り当てられていないデリバリーグループは、デフォルトのポリシーセットを受け取ります。
- デリバリーグループには、1つのポリシーセットのみを割り当てることができます。
- 複数のデリバリーグループで同じポリシーセットを使用できます。
- ポリシーセットがデリバリーグループに割り当てられていても、ポリシーはフィルターを維持します。

詳細については、「フィルターはどのように適用されますか？」を参照してください。ポリシーセットのポリシー割り当てまたはポリシーフィルターの動作方法に変更はありません。つまり、ポリシーの場合と同じように機能します。

デフォルトのポリシーセット

- ポリシーセット設定がオンの場合、既存のすべてのポリシーはデフォルトのポリシーセット内にグループ化されます。
- 管理者チームがポリシーセットを作成してデリバリーグループに割り当てない限り、すべてのデリバリーグループはデフォルトのポリシーセットを受け取ります。
- デリバリーグループに別のポリシーセットが割り当てられると、デフォルトのポリシーセットからポリシーを取得しなくなります。

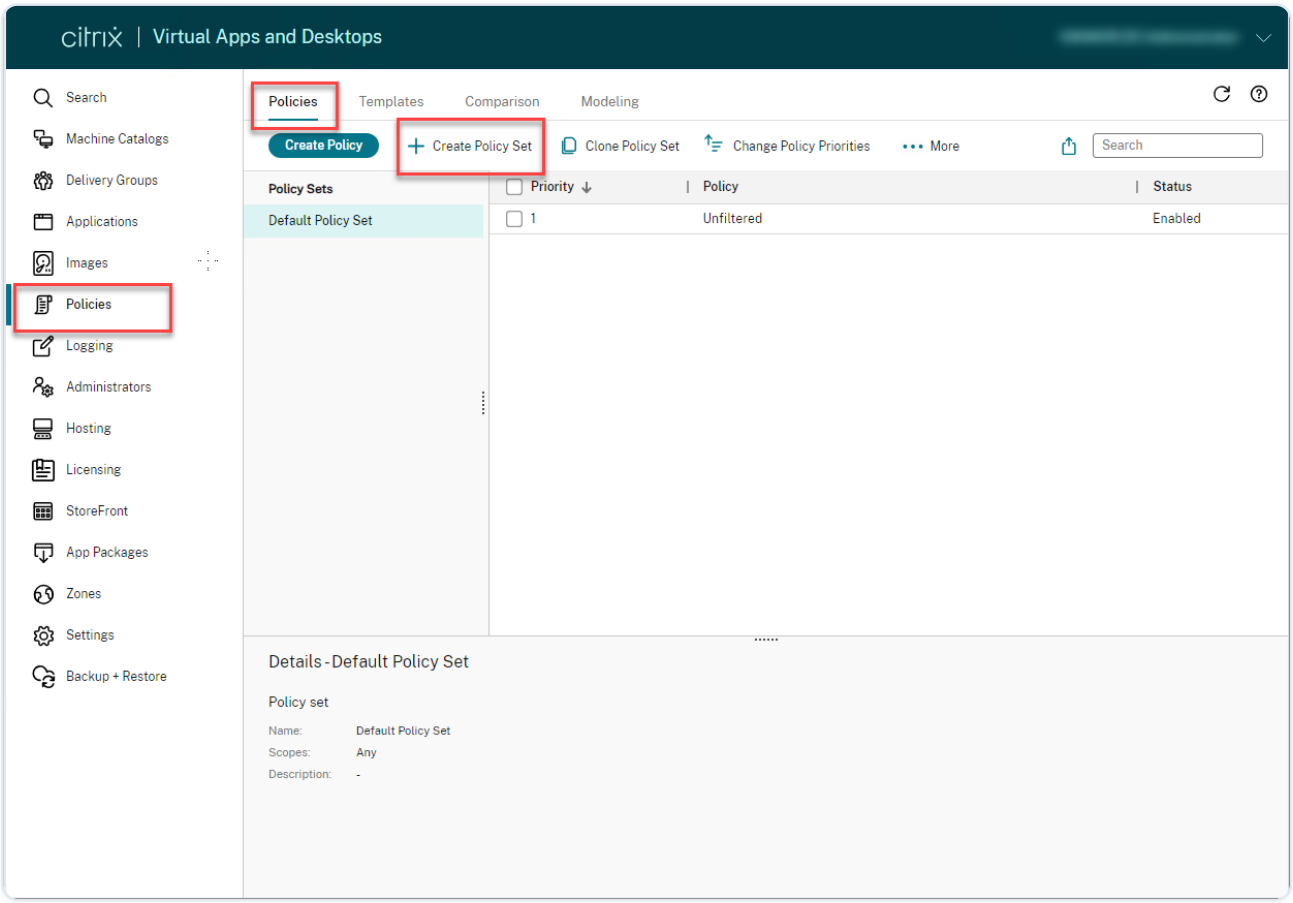
ポリシーセットの作成

ポリシーセットは次の2つの方法で作成できます。

- ポリシーセットの作成 - このアクションにより、空のポリシーセットが作成されます
- ポリシーセットのクローン作成 - このアクションにより、既存のポリシーセットに基づいてポリシーセットが作成されます

ポリシーセットの作成

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。



1. 「**ポリシーセットの作成**」を選択します。「**はじめに**」タブが表示されます。
2. 「**次へ**」をクリックするか、「**名前と説明**」タブをクリックします。
3. ポリシーセットの名前と説明を入力します。
4. 「**次へ**」をクリックするか、「**割り当て**」タブをクリックします。
5. ポリシーセットを割り当てるデリバリーグループを1つ以上選択します。
6. 「**次へ**」をクリックするか、「**スコープ**」タブをクリックします。
7. ポリシーセットのスコープを選択します。
8. 「**作成**」をクリックします。定義された割り当てとスコープでポリシーセットが作成されます。

ポリシーセットの複製

1. Web Studioにサインインし、左側のペインで「**ポリシー**」を選択します。
2. 「**ポリシーセットのクローンを作成**」を選択します。
3. ポリシーセットの名前を変更します。
4. ポリシーセットの割り当てを変更または作成し、「**次へ**」をクリックします。
5. クローン作成されたポリシーセットに含めるポリシーを選択または選択解除します。

6. ポリシーのスコープを変更します。
7. 「**作成**」をクリックします。ポリシーセットが作成されます。

ポリシーセットの編集

1. Web Studioにサインインし、左側のペインで**ポリシー**を選択します。
2. **ポリシーセットの編集**を選択します。
3. ポリシーセットの名前を変更し、**次へ**をクリックします。
4. ポリシーセットの割り当てを変更または作成し、**次へ**をクリックします。
5. ポリシーのスコープを変更します。
6. **Create** をクリックします。

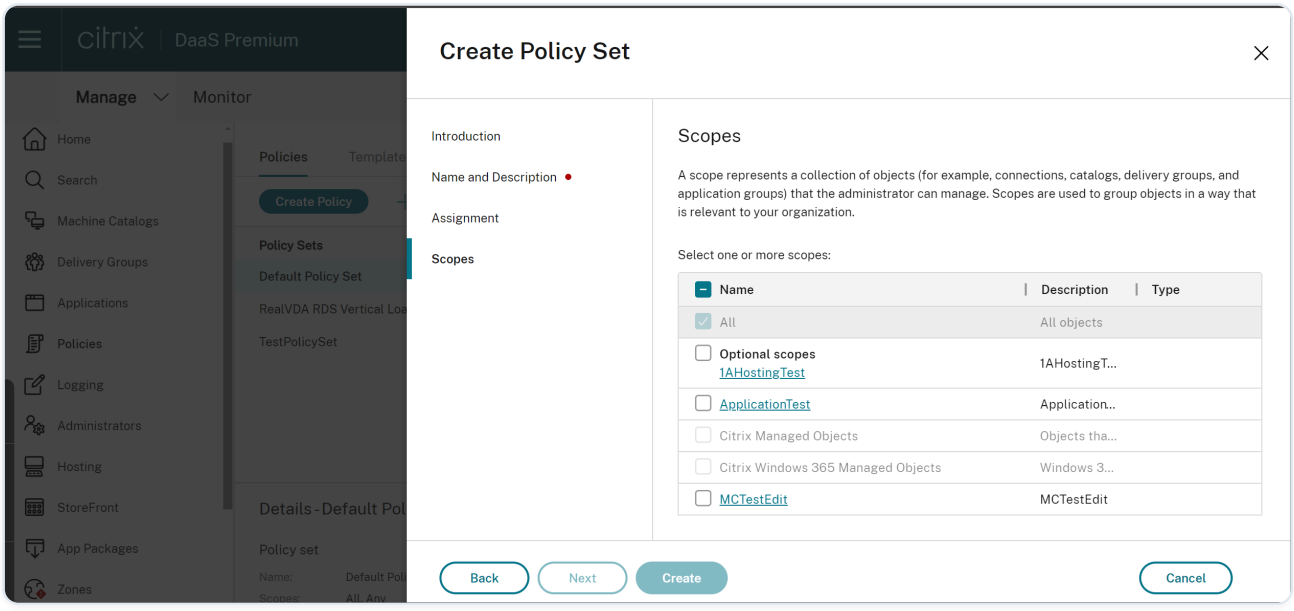
ポリシーセットの割り当て

ポリシーセットはデリバリーグループに割り当てられます。ポリシーセットの作成時または編集時に割り当てを構成できます。また、デリバリーグループの作成時または編集時にも割り当てを構成できます。

ポリシーセットのスコープ

管理者は、承認された管理者のみがポリシーセットを表示または編集できるように、ポリシーセットのスコープを定義できます。ポリシーセットの作成時または編集時にスコープを構成できます。

ポリシーセットの導入により、API を使用して Citrix Policy を作成および管理することもできます。詳細については、Citrix DaaS でポリシーセットを作成する方法を参照してください。



ポリシーの比較、優先順位付け、トラブルシューティング

注：

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

複数のポリシーを使用して、ユーザーの職務、地理的な場所、または接続の種類に基づいて、ユーザーのニーズに合わせて環境をカスタマイズできます。たとえば、セキュリティを強化するために、機密データを定期的に操作するユーザーグループに制限を設けることができます。

ユーザーが機密ファイルをローカルクライアントドライブに保存できないようにするポリシーを作成することもできます。ただし、ユーザーグループ内の一部のユーザーがローカルドライブへのアクセスを必要とする場合は、それらのユーザー専用の別のポリシーを作成できます。その後、どちらが優先されるかを制御するために、2つのポリシーをランク付けまたは優先順位付けします。複数のポリシーを使用する場合、次のことを決定する必要があります。

- ポリシーの優先順位付け方法
- 例外の作成方法
- ポリシーが競合する場合に有効なポリシーを表示する方法。

一般に、ポリシーは、サイト全体、特定のDelivery Controller、またはユーザーデバイス用に構成された同様の設定を上書きします。この原則の例外はセキュリティです。環境内で最も高い暗号化設定は、常に他の設定やポリシーを上書きします。最も高い暗号化設定には、オペレーティングシステムと最も制限の厳しいシャドウイング設定が含まれます。

Citrixポリシーは、オペレーティングシステムで設定したポリシーと相互作用します。Citrix環境では、Citrix設定は、Active Directoryポリシーで構成された設定、またはリモートデスクトップセッションホスト構成を使用して構成された設定と同じ設定を上書きします。この設定には、一般的なリモートデスクトッププロトコル（RDP）クライアント接続設定に関連する設定が含まれます。一般的なRDP設定には、デスクトップの壁紙、メニューアニメーション、ドラッグ中のウィンドウコンテンツの表示などの設定が含まれます。

Secure ICA®などの一部のポリシー設定は、オペレーティングシステムの設定と一致している必要があります。より高い優先度の暗号化レベルが別の場所で設定されている場合、ポリシーで指定した、またはアプリケーションとデスクトップを配信するときに指定した**Secure ICAポリシー**設定は上書きされる可能性があります。

たとえば、デリバリーグループを作成するときに指定する暗号化設定は、環境全体で指定した暗号化設定と同じレベルである必要があります。

> **注：**
>
> ダブルホップシナリオの2番目のホップでは、シングルセッションOS VDAがマルチセッションOS VDAに接続することを考慮してください。この場合、Citrixポリシーは、シングルセッションOS VDAをユーザーデバイスであるかのように扱います。たとえば、ポリシーがユーザーデバイスに画像をキャッシュするように設定されているとします。この例では、ダブルホップシナリオの2番目のホップ用にキャッシュされた画像は、シングルセッションOS VDAマシンにキャッシュされます。

ポリシーモデリングウィザードを使用する

ポリシーモデリングは、計画およびテスト目的で、フィルター付きの有効なポリシーをシミュレートするのに役立ちます。フィルター付きの有効なポリシーのみがモデル化されます。無効なポリシーは適用されず、フィルターなしの有効なポリシーは常に適用されます。

ポリシーモデリングウィザードを開くには、次の手順を実行します。

1. 左側のナビゲーションから**ポリシー**を選択します。
2. **モデリング**タブを選択します。
3. アクションバーで**ポリシーモデリング**を選択します。
4. **はじめに**ページを読み、**次へ**をクリックします。
5. ユーザーまたはコンピューターを選択します。コンテナーまたは特定のユーザーやコンピューターを参照できます。**次へ**をクリックします。
6. フィルターの証拠を選択します。オプションで、**デリバリーグループ**、**タグ**、**クライアントIPアドレス**などの追加の詳細を入力して、シミュレーションをより詳細にすることができます。**次へ**をクリックします。
7. 選択内容の概要を確認し、**実行**をクリックします。

実行をクリックすると、ウィザードはモデリング結果のレポートを生成します。このレポートを表示している間、次のことができます。

- ドロップダウンメニューで、**すべての設定**、**コンピューター設定**、または**ユーザー設定**を表示するかどうかを選択します。
- 検索バーを使用して、特定の設定を検索します。
- 特定の設定をクリックして、その設定の詳細を表示します。たとえば、特定のポリシーに対してすべてのユーザー設定が適用されなかった場合、**詳細**ペインに設定が適用されなかった理由が表示されます。
- **エクスポート**をクリックして、モデリング結果をJSON形式、HTML形式、またはその両方でエクスポートします。

ポリシーモデリングを実行すると、さらに多くのオプションが利用可能になります。次のことができます。

- **モデリングレポートの表示**: 上記と同じモデリングレポートが開き、再度表示したりエクスポートしたりできます。
- **ポリシーモデリングの再実行**: これにより、以前に選択したのと同じ基準セットでポリシーモデリングを再実行し、新しいモデリング結果を生成できます。これは、一部のポリシーが変更され、それらの変更が現在のモデルにどのように影響するかを確認したい場合に役立ちます。
- **モデリングレポートの削除**: 現在のモデリングレポートを削除します。

ポリシーとテンプレートの比較

ポリシーまたはテンプレートの設定を、他のポリシーまたはテンプレートの設定と比較できます。たとえば、ベストプラクティスへの準拠を維持するために、設定値を検証する必要がある場合があります。また、ポリシーまたはテンプレートの設定を、Citrixが提供するデフォルト設定と比較することもできます。

1. Web Studioにサインインし、左ペインで**［ポリシー］**を選択します。
2. **［比較］タブをクリックし、［選択］**をクリックします。
3. 比較するポリシーまたはテンプレートを選択します。比較にデフォルト値を含めるには、**［デフォルト設定と比較］**チェックボックスをオンにします。
4. **［比較］**をクリックすると、構成された設定が列に表示されます。
5. すべての設定を表示するには、**［すべての設定を表示］を選択します。デフォルトビューに戻るには、［共通設定を表示］**を選択します。

ポリシーの優先順位付け

ポリシーに優先順位を付けることで、競合する設定が含まれる場合にポリシーの優先順位を定義できます。ユーザーがログオンすると、接続の割り当てに一致するすべてのポリシーが特定されます。これらのポリシーは優先順位順に並べ替えられ、設定の複数のインスタンスが比較されます。各設定は、ポリシーの優先順位に従って適用されます。

ポリシーには異なる優先順位番号を付けて優先順位を付けます。デフォルトでは、新しいポリシーには最も低い優先順位が与えられます。ポリシー設定が競合する場合、優先順位が高いポリシー（優先順位番号1が最高）は、優先順位が低いポリシーを上書きします。設定は、優先順位と設定の条件（たとえば、設定が無効か有効かなど）に従ってマージされます。無効な設定は、有効な下位ランクの設定を上書きします。構成されていないポリシー設定は無視され、下位ランクの設定を上書きすることはありません。

1. 左ペインで**［ポリシー］**を選択します。［ポリシー］**タブが選択されていることを確認してください。
2. **［ポリシー］**タブで、アクションバーの**［ポリシーの優先順位の変更］**を選択します。［ポリシーの優先順位の変更］**ページが表示されます。
3. 優先順位リストで、ポリシーの優先順位を変更するには、次のいずれかの方法を使用します。
   - ポリシーを目的の位置にドラッグします。
   - 1つ上または下に移動するには、それぞれ上矢印アイコンまたは下矢印アイコンをクリックします。
   - リストの先頭または末尾に移動するには、それぞれ一番上または一番下の矢印アイコンをクリックします。
   - 優先順位番号を変更するには、**編集**アイコンをクリックし、必要に応じて番号を入力してから、**保存**をクリックします。
4. 「**保存**」をクリックします。

例外

ユーザー、ユーザーデバイス、またはマシンのグループに対してポリシーを作成する場合、グループの一部のメンバーが特定のポリシー設定に対する例外を必要とすることがあります。例外は次の方法で作成できます。

- 例外を必要とするグループメンバーのみにポリシーを作成し、そのポリシーをグループ全体のポリシーよりも上位にランク付けする
- ポリシーに追加された割り当てに拒否モードを使用する

モードが「拒否」に設定された割り当ては、割り当て条件に一致しない接続にのみポリシーを適用します。たとえば、ポリシーには次の割り当てが含まれます。

- 割り当てAは、208.77.88.*の範囲を指定するクライアントIPアドレス割り当てです。モードは許可に設定されています。
- 割り当てBは、特定のユーザーアカウントを指定するユーザー割り当てです。モードは拒否に設定されています。

このポリシーは、割り当てAで指定された範囲のIPアドレスを使用してサイトにログオンするすべてのユーザーに適用されます。ただし、割り当てBで指定されたユーザーアカウントを使用してサイトにログオンするユーザーには適用されません。

接続に適用されるポリシーを決定する

複数のポリシーが適用されるため、接続が期待どおりに応答しない場合があります。優先度の高いポリシーが接続に適用される場合、元のポリシーで構成した設定を上書きする可能性があります。ポリシーの結果セットを計算し、接続に対して最終的なポリシー設定がどのようにマージされるかを判断できます。

ポリシーの結果セットは、次の方法で計算できます。

- **Citrix Group Policy Modeling**ウィザードを使用して、接続シナリオをシミュレートし、Citrixポリシーがどのように適用されるかを判断します。接続シナリオの条件を次のように指定できます。
  - ドメインコントローラー
  - ユーザー
  - Citrix ポリシー割り当ての証拠値
  - 低速ネットワーク接続などのシミュレートされた環境設定 ウィザードが生成するレポートには、シナリオで有効になるCitrixポリシーが一覧表示されます。ドメインユーザーとしてControllerにログオンするため、ウィザードはサイトポリシー設定とActive Directoryグループポリシーオブジェクト（GPO）の両方を使用して結果を計算します。
- **グループポリシーの結果**を使用して、特定のユーザーとコントローラーに有効なCitrixポリシーを記述したレポートを作成します。グループポリシーの結果ツールは、環境内のGPOの現在の状態を評価するのに役立ち、レポートを生成します。生成されたレポートには、Citrixポリシーを含むこれらのオブジェクトが、特定のユーザーとコントローラーに現在どのように適用されているかが記述されています。

Web StudioでCitrix Group Policy Modelingウィザードを起動できます。または、Windowsのグループポリシー管理コンソールからグループポリシーの結果ツールを起動することもできます。

Web Studio を使用して作成されたサイトポリシー設定は、次の場合、ポリシーの結果セットに含まれません。

- グループポリシー管理コンソールからCitrix Group Policy Modelingウィザードを実行する場合
- グループポリシー管理コンソールからグループポリシーの結果ツールを実行する場合

最も包括的なポリシーの結果セットが得られることを確認するには、グループポリシー管理コンソールのみを使用してポリシーを作成する場合を除き、CitrixはWeb StudioからCitrix Group Policy Modelingウィザードを起動することをお勧めします。

ポリシーのトラブルシューティング

ユーザー、IPアドレス、およびその他の割り当てられたオブジェクトには、同時に適用される複数のポリシーが存在する場合があります。このシナリオでは、ポリシーが期待どおりに動作しない競合が発生する可能性があります。Citrix Group Policy Modelingウィザードまたはグループポリシーの結果ツールを実行すると、ユーザー接続にポリシーが適用されていないことが判明する場合があります。このようなシナリオでは、ポリシー評価基準に一致する条件下でアプリケーションやデスクトップに接続するユーザーには、ポリシー設定が適用されません。この状況は、次の場合に発生します。

- ポリシー評価基準に一致する割り当てを持つポリシーがありません。
- 割り当てに一致するポリシーに設定が構成されていません。
- 割り当てに一致するポリシーが無効になっています。

指定された基準を満たす接続にポリシー設定を適用したい場合は、次のことを確認してください。

- それらの接続に適用したいポリシーが有効になっていること。
- 適用したいポリシーに適切な設定が構成されていること。

デフォルトのポリシー設定

以下の表に、ポリシー設定、そのデフォルト値、および適用されるVirtual Delivery Agent (VDA) のバージョンを示します。

ICA®

名前	デフォルト設定	VDA
アダプティブトランスポート	オフ。優先される場合に使用します	VDA 7.13～7.15、VDA 7.16以降
クライアントクリップボードリダイレクト	許可	すべてのVDAバージョン
クライアントクリップボード書き込み許可形式	形式は指定されていません	VDA 7.6以降
デスクトップの起動	禁止	マルチセッションOS用VDA 7から現在まで
ICAリスナーポート番号	1494	すべてのVDAバージョン
クライアント接続中の非公開プログラムの起動	禁止	マルチセッションOS用VDA 7から現在まで
クリップボードのクライアントからセッションへの転送サイズを制限	無効	VDA 2009
クリップボードのセッションからクライアントへの転送サイズを制限	無効	VDA 2009
損失許容モード	許可	VDA 2003。注: 損失許容モードはまだ利用できません。このバージョンのVDAは、利用可能になった時点でこれをサポートします。
損失許容しきい値	損失許容モードが利用可能な場合: パケット損失: 5%、遅延: 300 ms (RTT)	VDA 2003以降
ランデブープロトコル	無効	Citrix Cloudを介して確立されたHDXセッションにのみ適用されます。

名前	デフォルト設定	VDA
クライアントクリップボードへの書き込みを制限	禁止	VDA 7.6以降
セッションクリップボードへの書き込みを制限	禁止	VDA 7.6以降
セッションクリップボード書き込み許可形式	形式は指定されていません	VDA 7.6から現在まで
タブレットモードの切り替え	有効	VDA 7.16から現在まで。VDA 7.14および7.15 LTSRの場合、この設定はレジストリを使用して構成します。
仮想チャネル許可リスト	有効	VDA 2109から現在まで
セッションメトリック収集	許可	7.42から現在まで

ICA®/Adobe Flash 配信/Flash リダイレクト

名前	デフォルト設定	VDA
Flashビデオのフォールバック防止	未構成	VDA 7.6 FP3 から現在まで
Flashビデオのフォールバック防止エラー *.swf	VDA 7.6 FP3 から現在まで	

ICA/オーディオ

名前	デフォルト設定	VDA
アダプティブオーディオ	有効	Citrix Virtual Apps and Desktops™ 2109以降を使用するVDAの、シングルセッションOSおよびマルチセッションOSの両方のセッションに適用されます。

名前	デフォルト設定	VDA
UDPリアルタイムトランスポート経由のオーディオ	許可	すべてのVDAバージョン
オーディオプラグアンドプレイ	許可	マルチセッションOS 7以降のVDA
オーディオ品質	高 - 高精細オーディオ	すべてのVDAバージョン
クライアントオーディオリダイレクト	許可	すべてのVDAバージョン
クライアントマイクのリダイレクト	許可	すべてのVDAバージョン
オーディオのロス許容モード	禁止	VDAバージョン2402以降

ICA/自動クライアント再接続

名前	デフォルト設定	VDA
自動クライアント再接続	許可	すべてのVDAバージョン
自動クライアント再接続認証	認証を要求しない	すべてのVDAバージョン
自動クライアント再接続ログ	自動再接続イベントをログに記録しない	すべてのVDAバージョン
自動クライアント再接続タイムアウト	120秒	VDA 7.13から現在まで
再接続UIの透明度レベル	80%	VDA 7.13から現在まで

ICA/帯域幅

名前	デフォルト設定	VDA
オーディオリダイレクト帯域幅制限	ゼロ Kbps	すべてのVDAバージョン
オーディオリダイレクト帯域幅制限の割合	0	すべてのVDAバージョン

名前	デフォルト設定	VDA
クライアントUSBデバイスリダイレクト帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
クライアントUSBデバイスリダイレクト帯域幅制限の割合	0	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
クリップボードリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
クリップボードリダイレクト帯域幅制限の割合	0	すべてのVDAバージョン
COMポートリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン。VDA 7.0から7.8の場合、この設定はレジストリを使用して構成します。
COMポートリダイレクト帯域幅制限の割合	0	すべてのVDAバージョン。VDA 7.0から7.8の場合、この設定はレジストリを使用して構成します
ファイルリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
ファイルリダイレクト帯域幅制限の割合	0	すべてのVDAバージョン
HDX MediaStreamマルチメディアアクセラレーション帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、Multi-session OS用VDA 7およびSingle-session OS用VDA 7から現在のMulti-session OS用VDAおよびSingle-session OS用VDAまで

名前	デフォルト設定	VDA
HDX MediaStreamマルチメディアアクセラレーション帯域幅制限の割合	0	VDA 5.5、5.6 FP1、Multi-session OS用VDA 7から現在まで、Single-session OS用VDA 7から現在まで
LPTポートリダイレクトの帯域幅制限	0 キロビット/秒	すべてのVDAバージョン。VDA 7.0から7.8の場合、この設定はレジストリを使用して構成します
LPTポートリダイレクトの帯域幅制限の割合	0	すべてのVDAバージョン。VDA 7.0から7.8の場合、この設定はレジストリを使用して構成します
セッション全体の帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
プリンターリダイレクトの帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
プリンターリダイレクトの帯域幅制限の割合	0	すべてのVDAバージョン
TWAINデバイスリダイレクト帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
TWAINデバイスリダイレクト帯域幅制限率	0	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/双方向コンテンツリダイレクト

名前	デフォルト設定	VDA
双方向コンテンツリダイレクトを許可する	禁止	VDA 7.13 から現在まで

名前	デフォルト設定	VDA
クライアントにリダイレクトを許可するURL	空	VDA 7.13 から現在まで
VDAにリダイレクトされる許可されたURL	空	VDA 7.13 から現在まで
双方向コンテンツリダイレクトの構成	無効	VDA 2311 から現在まで

ICA/ブラウザコンテンツリダイレクト

名前	デフォルト設定	VDA
ブラウザコンテンツリダイレクト	許可	VDA 7.16 から現在まで
ブラウザコンテンツリダイレクトACL構成	`https://www.youtube.com/*`	VDA 7.16 以降
ブラウザコンテンツリダイレクトの統合Windows認証サポート	禁止	VDA 2106 以降
ブラウザコンテンツリダイレクトのプロキシ構成	空	VDA 7.16 以降
ブラウザコンテンツリダイレクトのサーバーフェッチWebプロキシ認証	禁止	VDA 2012 以降

ICA/クライアントセンサー

名前	デフォルト設定	VDA
アプリケーションがクライアントデバイスの物理的な場所を使用することを許可する	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7～現在、シングルセッションOS用VDA 7～現在

ICA/デスクトップUI

名前	デフォルト設定	VDA
デスクトップコンポジションリダイレクト	無効 (7.6 FP3～現在); 有効 (5.6～7.6 FP2)	VDA 5.6、シングルセッションOS用VDA 7～7.15
デスクトップコンポジションリダイレクトのグラフィック品質	中	VDA 5.6、シングルセッションOS用VDA 7～7.15
デスクトップの壁紙	許可	すべてのVDAバージョン
メニューアニメーション	許可	すべてのVDAバージョン
ドラッグ中にウィンドウの内容を表示	許可	すべてのVDAバージョン

ICA/エンドユーザー監視

名前	デフォルト設定	VDA
ICAラウンドトリップ計算	有効	すべてのVDAバージョン
ICAラウンドトリップ計算間隔	15秒	すべてのVDAバージョン
アイドル接続のICAラウンドトリップ計算	無効	すべてのVDAバージョン

ICA/強化されたデスクトップエクスペリエンス

名前	デフォルト設定	VDA
強化されたデスクトップエクスペリエンス	許可	マルチセッションOS 7以降のVDA

ICA/ファイルリダイレクト

名前	デフォルト設定	VDA
クライアントドライブの自動接続	許可	すべてのVDAバージョン
クライアントドライブのリダイレクト	許可	すべてのVDAバージョン
クライアントの固定ドライブ	許可	すべてのVDAバージョン
クライアントのフロッピーディスクドライブ	許可	すべてのVDAバージョン
クライアントのネットワークドライブ	許可	すべてのVDAバージョン
クライアント光学ドライブ	許可	すべてのVDAバージョン
クライアントリムーバブルドライブ	許可	すべてのVDAバージョン
ホストからクライアントへのリダイレクト	無効	マルチセッションOS用VDA 7から現在まで
クライアントドライブ文字を保持	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7から現在まで
読み取り専用クライアントドライブアクセス	無効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
特殊フォルダーリダイレクト	許可	Web Interface展開のみ。マルチセッションOS用VDA 7以降
非同期書き込みを使用	無効	すべてのVDAバージョン

ICA/グラフィック

名前	デフォルト設定	VDA
視覚的にロスレスな圧縮を許可	無効	VDA 7.6以降
表示メモリ制限	65,536 Kb	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
表示モードの劣化優先順位	色深度を優先的に劣化させる	すべてのVDAバージョン
動的ウィンドウプレビュー	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7 以降、シングルセッションOS用VDA 7 以降
グラフィックステータスインジケーター	無効	VDA 7.16 以降
イメージキャッシュ	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7 以降、シングルセッションOS用VDA 7 以降
レガシーグラフィックモード	無効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
許可される最大色深度	32ビット/ピクセル	すべてのVDAバージョン
ディスプレイモードが劣化した場合にユーザーに通知する	無効	マルチセッションOS用VDA 7以降
3Dグラフィックワークロード向けに最適化	無効	VDA 7.17から現在まで
キューイングとトッシング	有効	すべてのVDAバージョン
画面共有	無効	VDA 2112
圧縮にビデオコーデックを使用	優先される場合にビデオコーデックを使用	VDA 7.6 FP3から現在まで

名前	デフォルト設定	VDA
ビデオコーデックにハードウェアエンコードを使用	有効	VDA 7.11から現在まで

ICA/グラフィック/キャッシュ

名前	デフォルト設定	VDA
永続キャッシュしきい値	300万 bps	マルチセッションOS用VDA 7から現在まで

ICA/グラフィック/Framehawk

名前	デフォルト設定	VDA
Framehawk 表示チャネル	無効	VDA 7.6 FP2 以降
Framehawk 表示チャネルポート範囲	3224,3324	VDA 7.6 FP2 以降

ICA/キープアライブ

名前	デフォルト設定	VDA
ICA キープアライブ タイムアウト	60秒	すべてのVDAバージョン
ICAキープアライブ	ICAキープアライブメッセージを送信しない	すべてのVDAバージョン

ICA/キーボードおよびIME

名前	デフォルト設定	VDA
クライアントキーボードレイアウト同期およびIMEの改善	無効	1912 LTSR CU2以降にのみ適用されます。
Unicode キーボードレイアウトマッピングを有効にする	許可 (2407 から現在まで); 禁止 (以前のバージョン)	1912 LTSR CU2以降にのみ適用されます。

名前	デフォルト設定	VDA
キーボードレイアウト切り替えポップアップメッセージボックスを非表示にする	禁止	1912 LTSR CU2以降にのみ適用されます。

ICA/ローカルアプリアクセス

名前	デフォルト設定	VDA
ローカルアプリアクセスを許可	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
URLリダイレクトブロックリスト	サイトは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
URLリダイレクト許可リスト	サイトは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/モバイルエクスペリエンス

名前	デフォルト設定	VDA
自動キーボード表示	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7 以降、シングルセッションOS用VDA 7 以降
タッチ最適化デスクトップの起動	許可	VDA 5.6 FP1、VDA for Multi-session OS 7 以降、VDA for Single-session OS 7 以降。この設定は無効になっており、Windows 10 および Windows Server 2016 マシンでは利用できません。
コンボボックスのリモート化	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7 以降、シ

名前	デフォルト設定	VDA
		ングルセッションOS用VDA 7 以降

ICA/マルチメディア

名前	デフォルト設定	VDA
HTML5ビデオリダイレクト	禁止	VDA 7.12以降
ビデオ品質の制限	未構成	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
Microsoft Teamsリダイレクト	許可	マルチセッションOS用VDA 1906以降、シングルセッションOS用VDA 1906以降。
マルチメディア会議	許可	すべてのVDAバージョン
WAN経由でのWindows Mediaマルチメディアリダイレクトの最適化	許可	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
WAN経由でのWindows Mediaマルチメディアリダイレクトの最適化にGPUを使用する	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
Windows Mediaフォールバック防止	未構成	VDA 7.6 FP3以降
Windows Mediaクライアント側コンテンツフェッチ	許可	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
Windows Mediaリダイレクト	許可	すべてのVDAバージョン
Windows Mediaリダイレクトバッファサイズ	5秒	VDA 5、5.5、5.6 FP1から現在まで

名前	デフォルト設定	VDA
Windows Mediaリダイレクトバッファサイズの使用	無効	VDA 5、5.5、5.6 FP1から現在まで

ICA/マルチストリーム接続

名前	デフォルト設定	VDA
UDP経由のオーディオ	許可	VDA for Multi-session OS 7から現在まで
オーディオUDPポート範囲	16500、16509	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
マルチポートポリシー	プライマリポート (2598) は高優先度	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
マルチストリーム コンピューター設定	無効	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
マルチストリーム ユーザー設定	無効	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
マルチストリーム仮想チャネルストリーム割り当て設定	デフォルトのストリーム割り当てについては、マルチストリーム仮想チャネル割り当て設定を参照してください。	VDA 2003

ICA/ポートリダイレクト

名前	既定の設定	VDA
クライアントCOMポートの自動接続	無効	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します
クライアントLPTポートの自動接続	無効	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します
クライアントCOMポートのリダイレクト	禁止	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します
クライアントLPTポートのリダイレクト	禁止	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します

ICA/印刷

名前	デフォルト設定	VDA
クライアントプリンターリダイレクト	許可	すべてのVDAバージョン
デフォルトプリンター	デフォルトプリンターをクライアントのメインプリンターに設定する	すべてのVDAバージョン
プリンターの割り当て	ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用される	すべてのVDAバージョン
プリンターの自動作成イベントログ設定	エラーと警告をログに記録する	すべてのVDAバージョン

名前	デフォルト設定	VDA
セッションプリンター	プリンターは指定されていません	すべてのVDAバージョン
プリンターが作成されるまで待機する（デスクトップ）	無効	すべてのVDAバージョン

ICA/印刷/クライアントプリンター

名前	デフォルト設定	VDA
クライアントプリンターの自動作成	すべてのクライアントプリンターを自動作成	すべてのVDAバージョン
汎用ユニバーサルプリンターの自動作成	無効	すべてのVDAバージョン
クライアントプリンター名	標準プリンター名	VDA 5.6
印刷サーバーへの直接接続	有効	すべてのVDAバージョン
プリンタードライバーのマッピングと互換性	ルールは指定されていません	すべてのVDAバージョン
プリンタープロパティの保持	クライアントに保存されていない場合にのみプロファイルに保持	すべてのVDAバージョン
保持および復元されたクライアントプリンター	許可	VDA 5、5,5、5.6 FP1

ICA/Printing/Drivers

名前	デフォルト設定	VDA
インボックスプリンタードライバーの自動インストール	有効	すべてのVDAバージョン
ユニバーサルドライバーの優先順位	イーエムエフ; エックスピーエス; ピーシーエルファイブ	すべてのVDAバージョン

名前	デフォルト設定	VDA
	シー; ピーシーエルフォー; ピーエス	
ユニバーサルプリントドライバーの使用	要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用する	すべてのVDAバージョン

ICA/印刷/ユニバーサルプリントサーバー

名前	デフォルト設定	VDA
Universal Print Serverの有効化	無効	すべてのVDAバージョン
Universal Print Server印刷データストリーム (CGP) ポート	7229	すべてのVDAバージョン
Universal Print Server印刷ストリーム入力帯域幅制限 (kbps)	0	すべてのVDAバージョン
Universal Print Server Web サービス (HTTP/SOAP) ポート	8080	すべてのVDAバージョン
ロードバランシング用のユニバーサルプリントサーバー	VDAバージョン7.9から現在まで	
ユニバーサルプリントサーバーのサービス停止しきい値	180 (秒)	VDAバージョン7.9から現在まで

ICA/印刷/ユニバーサル印刷

名前	デフォルト設定	VDA
ユニバーサル印刷EMF処理モード	プリンターに直接スプールする	すべてのVDAバージョン
ユニバーサル印刷画像圧縮制限	最高品質 (ロスレス圧縮)	すべてのVDAバージョン

名前	デフォルト設定	VDA
ユニバーサル印刷の最適化のデフォルト	画像圧縮: 希望する画質 = 標準品質、ヘビーウェイト圧縮を有効にする = False; 画像とフォントのキャッシュ: 埋め込み画像のキャッシュを許可する = True; 管理者以外のユーザーによるこれらの設定の変更を許可する = False;	すべてのVDAバージョン
ユニバーサル印刷プレビューの優先設定	自動作成または汎用ユニバーサルプリンターには印刷プレビューを使用しない	すべてのVDAバージョン
ユニバーサル印刷の印刷品質制限	制限なし	すべてのVDAバージョン

ICA/セキュリティ

名前	デフォルト設定	VDA
SecureICAの最小暗号化レベル	基本	マルチセッションOS用VDA 7以降

ICA/サーバー制限

名前	デフォルト設定	VDA
サーバーアイドルタイマー間隔	0ミリ秒	マルチセッションOS用VDA 7以降

ICA/セッション制限

名前	デフォルト設定	VDA
切断されたセッションタイマー	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
リモートPCアクセス切断セッションタイマー	無効	シングルセッションOS用VDA 7以降
切断セッションタイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッション接続タイマー	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッション接続タイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッションアイドルタイマー	有効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッションアイドルタイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降

ICA/セッションの信頼性

名前	デフォルト設定	VDA
セッションの信頼性接続	許可	すべてのVDAバージョン
セッションの信頼性ポート番号	2598	すべてのVDAバージョン
セッションの信頼性タイムアウト	180秒	すべてのVDAバージョン

ICA/タイムゾーン制御

名前	デフォルト設定	VDA
レガシークライアントのローカル時刻を推定する	有効	マルチセッションOS 7以降のVDA
セッション切断またはログオフ時にシングルセッションOSのタイムゾーンを復元する	有効	現在のVDAバージョン
クライアントのローカル時刻を使用する	サーバーのタイムゾーンを使用する	すべてのVDAバージョン

ICA/TWAINデバイス

名前	デフォルト設定	VDA
クライアントTWAINデバイスリダイレクト	許可	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
TWAIN圧縮レベル	中	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/USBデバイス

名前	デフォルト設定	VDA
クライアントUSBデバイス最適化ルール	有効（VDA 7.6 FP3以降）。無効（VDA 7.11以降）。デフォルトでは、ルールは指定されていません	VDA 7.6 FP3 から現在まで
クライアントUSBデバイスリダイレクト	禁止	すべてのVDAバージョン

名前	デフォルト設定	VDA
クライアントUSBデバイスリダイレクト規則	規則は指定されていません	すべてのVDAバージョン
クライアントUSBプラグアンドプレイデバイスリダイレクト	許可	マルチセッションOS用VDA 7から現在まで、シングルセッションOS用VDA 7から現在まで

ICA/ビジュアルディスプレイ

名前	デフォルト設定	VDA
シンプルなグラフィックの優先色深度	24 ビット/ピクセル	VDA 7.6 FP3 から現在まで
ターゲットフレームレート	30 フレーム/秒	すべてのVDAバージョン
画質	中	マルチセッションOS 用 VDA 7 以降、シングルセッション OS 用 VDA 7 以降

ICA/ビジュアルディスプレイ/動画

名前	デフォルト設定	VDA
最小画像品質	標準	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7から現在まで、シングルセッションOS用VDA 7から現在まで
動画圧縮	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
プログレッシブ圧縮レベル	なし	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
プログレッシブ圧縮しきい値	2,147,483,647 キロビット/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
ターゲット最小フレームレート	10 フレーム/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

注：

「**目標最小フレームレート**」ポリシーは廃止されました。

ICA/視覚表示/静止画像

名前	デフォルト設定	VDA
追加の色圧縮	無効	すべてのVDAバージョン
追加の色圧縮しきい値	8,192 キロビーピーエス	すべてのVDAバージョン
高負荷圧縮	無効	すべてのVDAバージョン
非可逆圧縮レベル	中	すべてのVDAバージョン
損失圧縮しきい値	2,147,483,647 キロビット毎秒	すべてのVDAバージョン

ICA/WebSockets

名前	デフォルト設定	VDA
WebSockets接続	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
WebSocketsポート番号	8008	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
WebSockets信頼済みオリジンサーバーリスト	ワイルドカード「*」は、すべてのReceiver for Web URLを信頼するために使用されます	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

負荷管理

名前	デフォルト設定	VDA
同時ログオン許容数	2	マルチセッションOS用VDA 7以降
CPU使用率	無効	マルチセッションOS用VDA 7以降
CPU使用率から除外されるプロセスの優先度	標準以下または低	マルチセッションOS用VDA 7以降
ディスク使用量	無効	マルチセッションOS用VDA 7以降
最大セッション数	250	マルチセッションOS用VDA 7以降
メモリ使用量	無効	マルチセッションOS用VDA 7以降
メモリ使用量のベースロード	ゼロロード: 768 MB	マルチセッションOS用VDA 7以降

プロファイル管理/詳細設定

名前	デフォルト設定	VDA
自動構成を無効にする	無効	すべてのVDAバージョン

名前	デフォルト設定	VDA
問題が発生した場合にユーザーをログオフする	無効	すべてのVDAバージョン
ロックされたファイルへのアクセス時の再試行回数	5	すべてのVDAバージョン
ログオフ時にインターネットCookieファイルを処理する	無効	すべてのVDAバージョン

プロファイル管理/基本設定

名前	デフォルト設定	VDA
アクティブライトバック	無効	すべてのVDAバージョン
プロファイル管理を有効にする	無効	すべてのVDAバージョン
除外グループ	無効。すべてのユーザーグループのメンバーが処理されます。	すべてのVDAバージョン
オフラインプロファイルのサポート	無効	すべてのVDAバージョン
ユーザーストアへのパス	ウィンドウズ	すべてのVDAバージョン
ローカル管理者によるログオンの処理	無効	すべてのVDAバージョン
処理されるグループ	無効。すべてのユーザーグループのメンバーが処理されます。	すべてのVDAバージョン

プロファイル管理/クロスプラットフォーム設定

名前	デフォルト設定	VDA
クロスプラットフォーム設定ユーザーグループ	無効。処理済みグループで指定されたすべてのユーザーグループが処理されます	すべてのVDAバージョン
クロスプラットフォーム設定を有効にする	無効	すべてのVDAバージョン
クロスプラットフォーム定義へのパス	無効。パスは指定されていません。	すべてのVDAバージョン
クロスプラットフォーム設定ストアへのパス	無効。Windows\PM_CMが使用されます。	すべてのVDAバージョン
クロスプラットフォーム設定の作成元	無効	すべてのVDAバージョン

プロファイル管理/ファイルシステム/除外

名前	デフォルト設定	VDA
除外リスト - ディレクトリ	無効。ユーザープロファイル内のすべてのフォルダーが同期されます。	すべてのVDAバージョン
除外リスト - ファイル	無効。ユーザープロファイル内のすべてのファイルが同期されます。	すべてのVDAバージョン

プロファイル管理/ファイルシステム/同期

名前	デフォルト設定	VDA
同期するディレクトリ	無効。除外されていないフォルダーのみが同期されます。	すべてのVDAバージョン
同期するファイル	無効。除外されていないファイルのみが同期されます。	すべてのVDAバージョン

名前	デフォルト設定	VDA
ミラーリングするフォルダー	無効。フォルダーはミラーリングされません。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト

名前	デフォルト設定	VDA
管理者アクセスを許可する	無効	すべてのVDAバージョン
ドメイン名を含める	無効	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/AppData(Roaming)

名前	デフォルト設定	VDA
AppData(Roaming)パス	無効。場所は指定されていません。	すべてのVDAバージョン
AppData(Roaming)のリダイレクト設定	コンテンツは、AppData(Roaming)パスのポリシー設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/連絡先

名前	デフォルト設定	VDA
連絡先パス	無効。場所は指定されていません。	すべてのVDAバージョン
連絡先のフォルダーリダイレクト設定	コンテンツは、**連絡先パスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/デスクトップ

名前	デフォルト設定	VDA
デスクトップパス	無効。場所は指定されていません。	すべてのVDAバージョン
デスクトップのフォルダーリダイレクト設定	コンテンツは、**デスクトップパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ドキュメント

名前	デフォルト設定	VDA
ドキュメントパス	無効。場所は指定されていません。	すべてのVDAバージョン
ドキュメントのリダイレクト設定	コンテンツは、**ドキュメントパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ダウンロード

名前	デフォルト設定	VDA
ダウンロードパス	無効。場所は指定されていません。	すべてのVDAバージョン
ダウンロードのリダイレクト設定	コンテンツは、**ダウンロードパスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/お気に入り

名前	デフォルト設定	VDA
お気に入りパス	無効。場所は指定されていません。	すべてのVDAバージョン

名前	デフォルト設定	VDA
お気に入りのリダイレクト設定	コンテンツは、**お気に入りパスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/リンク

名前	デフォルト設定	VDA
リンクパス	無効。場所は指定されていません。	すべてのVDAバージョン
リンクのリダイレクト設定	コンテンツは、**リンクパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ミュージック

名前	デフォルト設定	VDA
ミュージックパス	無効。場所は指定されていません。	すべてのVDAバージョン
ミュージックのリダイレクト設定	コンテンツは、「**ミュージックパスポリシー**」設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ピクチャ

名前	デフォルト設定	VDA
ピクチャパス	無効。場所は指定されていません。	すべてのVDAバージョン
ピクチャのリダイレクト設定	コンテンツは、「**ピクチャパスポリシー**」設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/保存されたゲーム

名前	デフォルト設定	VDA
保存されたゲームパス	無効。場所は指定されていません。	すべてのVDAバージョン
保存されたゲームのリダイレクト設定	コンテンツは、「**保存されたゲームパスポリシー**」設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/検索

名前	デフォルト設定	VDA
検索パス	無効。場所は指定されていません。	すべてのVDAバージョン
検索のリダイレクト設定	コンテンツは、**検索パスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/スタートメニュー

名前	デフォルト設定	VDA
スタートメニューパス	無効。場所は指定されていません。	すべてのVDAバージョン
スタートメニューのリダイレクト設定	コンテンツは、スタートメニューパスポリシー設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ビデオ

名前	デフォルト設定	VDA
ビデオパス	無効。場所は指定されていません。	すべてのVDAバージョン

名前	デフォルト設定	VDA
ビデオのリダイレクト設定	コンテンツは、**ビデオパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/ログ設定

名前	デフォルト設定	VDA
Active Directory のアクション	無効	すべてのVDAバージョン
一般情報	無効	すべてのVDAバージョン
一般的な警告	無効	すべてのVDAバージョン
ログの有効化	無効	すべてのVDAバージョン
ファイルシステムのアクション	無効	すべてのVDAバージョン
ファイルシステム通知	無効	すべてのVDAバージョン
ログオフ	無効	すべてのVDAバージョン
ログオン	無効	すべてのVDAバージョン
ログファイルの最大サイズ	1048576	すべてのVDAバージョン
ログファイルへのパス	無効。ログファイルはデフォルトの場所である %SystemRoot%\System32\Logfiles\UserProfileManager に保存されます。	すべてのVDAバージョン
パーソナライズされたユーザー情報	無効	すべてのVDAバージョン
ログオン時とログオフ時のポリシー値	無効	すべてのVDAバージョン
レジストリアクション	無効	すべてのVDAバージョン

名前	デフォルト設定	VDA
ログオフ時のレジストリの差異	無効	すべてのVDAバージョン

プロファイル管理/プロファイルの処理

名前	デフォルト設定	VDA
キャッシュされたプロファイルを削除するまでの遅延	0	すべてのVDAバージョン
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効	すべてのVDAバージョン
ローカルプロファイルの競合処理	ローカルプロファイルを使用する	すべてのVDAバージョン
既存プロファイルの移行	ローカルとローミング	すべてのVDAバージョン
テンプレートプロファイルへのパス	無効。新しいユーザープロファイルは、ユーザーが最初にログオンしたデバイスのデフォルトユーザープロファイルから作成されます。	すべてのVDAバージョン
テンプレートプロファイルがローカルプロファイルを上書きする	無効	すべてのVDAバージョン
テンプレートプロファイルが移動プロファイルを上書きする	無効	すべてのVDAバージョン
すべてのログオンでCitrix®必須プロファイルとして使用されるテンプレートプロファイル	無効	すべてのVDAバージョン

プロファイル管理/レジストリ

名前	デフォルト設定	VDA
除外リスト	無効。ユーザーがログオフすると、HKCUハイブ内のすべてのレジストリキーが処理されます。	すべてのVDAバージョン
インクルージョンリスト	無効。ユーザーがログオフすると、HKCUハイブ内のすべてのレジストリキーが処理されます。	すべてのVDAバージョン

プロファイル管理/ストリーム配信ユーザープロファイル

名前	デフォルト設定	VDA
常にキャッシュ	無効	すべてのVDAバージョン
常にキャッシュするサイズ	0 MB	すべてのVDAバージョン
プロファイルストリーミング	無効	すべてのVDAバージョン
ストリーミングされたユーザープロファイルグループ	無効。OU内のすべてのユーザープロファイルは正常に処理されます。	すべてのVDAバージョン
保留中のエリアロックファイルのタイムアウト（日数）	1日	すべてのVDAバージョン

レシーバー

名前	デフォルト設定	VDA
StoreFront™アカウントリスト	ストアは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ユーザーパーソナライゼーションレイヤー

名前	デフォルト設定	VDA
ユーザーレイヤーリポジトリパス	無効。パスは指定されていません。	VDA 19.12以降のバージョン
ユーザーレイヤーサイズ (GB)	10 GB。ユーザーレイヤーは、設定されたサイズまで拡張するシンプロビジョニングディスクです。ユーザーレイヤーのサイズが小さくなることはありません。	VDA 19.12以降のバージョン

仮想デリバリーエージェント

名前	デフォルト設定	VDA
コントローラー登録IPv6ネットマスク	ネットマスクは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
コントローラー登録ポート	80	すべてのVDAバージョン
コントローラーSID	SIDは指定されていません	すべてのVDAバージョン
コントローラー	コントローラーは指定されていません	すべてのVDAバージョン
コントローラーの自動更新を有効にする	有効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
IPv6コントローラー登録のみを使用する	無効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
サイト GUID	GUID は指定されていません	すべての VDA バージョン

バーチャル デリバリー エージェント/HDX 3D Pro

名前	デフォルト設定	VDA
ロスレスを有効にする	有効	VDA 5.5、5.6 FP1
HDX 3D Pro品質設定	VDA 5.5、5.6 FP1	

バーチャル デリバリー エージェント/監視

名前	デフォルト設定	VDA
プロセス監視を有効にする	無効	VDA 7.11以降
リソース監視を有効にする	有効	VDA 7.11以降

仮想IP

名前	デフォルト設定	VDA
仮想IPループバックサポート	無効	VDA 7.6 以降
仮想IP仮想ループバックプログラムリスト	なし	VDA 7.6 以降

ポリシー設定リファレンス

ポリシーには、ポリシーが適用されるときに適用される設定が含まれます。このセクションの説明では、機能を有効にするためにより多くの設定が必要かどうか、または設定に類似しているかどうかも示されています。

クイックリファレンス

次の表に、ポリシー内で構成できる設定を示します。左の列で完了したいタスクを見つけ、右の列で対応する設定を見つけてください。

すべてのポリシー設定の完全なリストは、.CHM (コンパイル済み HTML) 形式および .CSV 形式で利用できます。これらのファイルは、ブローカー (デリバリーコントローラー) がインストールされているサーバーの `\program files\citrix\grouppolicy` フォルダーにあります。ポリシー設定の最新バージョンは、こちらをクリックしてダウンロードすることもできます。

オーディオ

このタスクの場合	このポリシー設定を使用する
複数のオーディオデバイスの使用を許可するかどうかを制御する	オーディオプラグアンドプレイ
ユーザーデバイスのマイクからのオーディオ入力を許可するかどうかを制御する	クライアントマイクのリダイレクト
ユーザーデバイスのオーディオ品質を制御する	オーディオ品質
ユーザーデバイスのスピーカーへのオーディオマッピングを制御する	クライアントオーディオリダイレクト

ユーザーデバイスの帯域幅

使用される帯域幅を制限するには	このポリシー設定を使用
クライアントオーディオマッピング	オーディオリダイレクト帯域幅制限またはオーディオリダイレクト帯域幅制限パーセント
ローカルクリップボードを使用した切り取りと貼り付け	クリップボードリダイレクト帯域幅制限またはクリップボードリダイレクト帯域幅制限パーセント
セッションでのローカルクライアントドライブへのアクセス	ファイルリダイレクト帯域幅制限またはファイルリダイレクト帯域幅制限パーセント
HDX™ MediaStream マルチメディアアクセラレーション	HDX MediaStream マルチメディアアクセラレーション帯域幅制限またはHDX MediaStream マルチメディアアクセラレーション帯域幅制限パーセント
クライアントセッション	セッション全体の帯域幅制限
印刷	プリンターリダイレクト帯域幅制限またはプリンターリダイレクト帯域幅制限率
TWAINデバイス（カメラやスキャナーなど）	TWAINデバイスリダイレクト帯域幅制限またはTWAINデバイスリダイレクト帯域幅制限率

使用される帯域幅を制限するには	このポリシー設定を使用
USBデバイス	クライアントUSBデバイスリダイレクト帯域幅制限またはクライアントUSBデバイスリダイレクト帯域幅制限率

クライアントドライブおよびユーザーデバイスのリダイレクト

このタスクの場合	このポリシー設定を使用する
ユーザーがサーバーにログオンしたときに、ユーザーデバイス上のドライブが接続されるかどうかを制御します	クライアントドライブの自動接続
サーバーとローカルクリップボード間の切り取りと貼り付けのデータ転送を制御します	クライアントクリップボードリダイレクト
ユーザーデバイスからドライブがどのようにマップされるかを制御します	クライアントドライブリダイレクト
セッション内でユーザーのローカルハードドライブが利用可能かどうかを制御します	クライアント固定ドライブとクライアントドライブのリダイレクト
ユーザーのローカルフロッピーディスクドライブをセッションで利用可能にするかどうかを制御します	クライアントフロッピーディスクドライブとクライアントドライブのリダイレクト
ユーザーのネットワークドライブをセッションで利用可能にするかどうかを制御します	クライアントネットワークドライブとクライアントドライブのリダイレクト
ユーザーのローカルCD、DVD、またはBlu-rayドライブをセッションで利用可能にするかどうかを制御します	クライアント光学ドライブとクライアントドライブのリダイレクト
ユーザーのローカルリムーバブルドライブをセッションで利用可能にするかどうかを制御します	クライアントリムーバブルドライブとクライアントドライブのリダイレクト
スキャナーやカメラなどのユーザーのTWAINデバイスをセッションで利用可能にするかどうかを制御し、画像データ転送の圧縮を制御します	クライアントTWAINデバイスのリダイレクト。TWAIN圧縮のリダイレクト

このタスクの場合	このポリシー設定を使用する
USBデバイスをセッションで利用可能にするかどうかを制御します	クライアントUSBデバイスのリダイレクトとクライアントUSBデバイスのリダイレクト規則
WAN経由でクライアントディスクへのファイルの書き込みとコピーの速度を向上させます	非同期書き込みを使用する

コンテンツリダイレクト

このタスクの場合	このポリシー設定を使用する
サーバーからユーザーデバイスへのコンテンツリダイレクトを使用するかどうかを制御します	ホストからクライアントへのリダイレクト

デスクトップUI

このタスクの場合	このポリシー設定を使用する
ユーザーセッションでデスクトップの壁紙を使用するかどうかを制御します	デスクトップの壁紙
ウィンドウのドラッグ中にウィンドウの内容を表示	ドラッグ中のウィンドウの内容を表示

グラフィックとマルチメディア

重要:

Flashポリシーは、古いVDAを使用している顧客が新しいコントローラー（たとえば、バージョン1912コントローラー）を使用し、引き続きFlashを使用できるようにするためにのみ残されています。このVDAバージョンはFlashをサポートしていません。

このタスクの場合	このポリシー設定を使用します
仮想デスクトップからユーザーデバイスに送信される1秒あたりの最大フレーム数を制御します。	ターゲットフレームレート
ユーザーデバイスに表示される画像の視覚的な品質を制御します。	視覚的な品質
セッションでアクセスされたときに、Webサイトが Flashコンテンツを表示できるかどうかを制御します。	Flashサーバー側コンテンツ取得URLリスト; Flash URL互換性リスト; Flashビデオフォールバック防止ポリシー設定; Flashビデオフォールバック防止エラー *.swf
サーバーでレンダリングされたビデオの圧縮を制御します。	圧縮にビデオコーデックを使用。ビデオコーデックにハードウェアエンコードを使用。
ユーザーへのHTML5マルチメディアWebコンテンツの配信を制御します。	HTML5ビデオリダイレクト

マルチストリームネットワークトラフィックの優先順位付け

このタスクの場合	このポリシー設定を使用
複数の接続を介したICA®トラフィックのポートを指定し、ネットワークの優先順位を確立します	マルチポートポリシー
サーバーとユーザーデバイス間のマルチストリーム接続のサポートを有効にします	マルチストリーム（コンピューターとユーザーの設定）

印刷

このタスクの場合	このポリシー設定を使用します
ユーザーデバイスでのクライアントプリンターの作成を制御します	クライアントプリンターの自動作成とクライアントプリンターのリダイレクト
プリンタープロパティの保存場所を制御します	プリンタープロパティの保持

このタスクの場合	このポリシー設定を使用します
クライアントまたはサーバーのどちらが印刷要求を処理するかを制御します	印刷サーバーへの直接接続
ユーザーが自分のユーザーデバイスに接続されているプリンターにアクセスできるかどうかを制御します	クライアントプリンターのリダイレクト
クライアントおよびネットワークプリンターを自動的に作成する際のネイティブWindowsドライバーのインストールを制御する	インボックスプリンタードライバーの自動インストール
ユニバーサルプリンタードライバーを使用するタイミングを制御する	ユニバーサルプリンタードライバーの使用
ローミングユーザーセッション情報に基づいてプリンターを選択する	デフォルトプリンター
ユニバーサルプリントサーバーの負荷分散とフェールオーバーしきい値の設定	負荷分散のためのユニバーサルプリントサーバー。ユニバーサルプリントサーバーのサービス停止しきい値

注：

ポリシーを使用して、デスクトップまたはアプリケーションセッションでスクリーンセーバーを有効にすることはできません。スクリーンセーバーを必要とするユーザーの場合、スクリーンセーバーはユーザーデバイスに実装できます。

ICA® ポリシー設定

注:

このページでは、ICAポリシー設定の説明とサポートされている構成値を提供します。ポリシーの操作の詳細については、「ポリシーの操作」セクションを参照してください。

アダプティブトランスポート

この設定は、EDTをプライマリとして、TCPをフォールバックとしてデータ転送を許可または防止します。

デフォルトでは、アダプティブトランスポートは有効になっており（**優先**）、可能な場合はEDTが使用され、TCPにフォールバックします。必要に応じて設定を変更できます。

- **優先**。可能な場合はEDT経由のアダプティブトランスポートが使用され、TCPにフォールバックします。
- **診断モード**。EDTが強制的にオンになり、TCPへのフォールバックは無効になります。この設定はトラブルシューティングの場合にのみ推奨されます。
- **オフ**。TCPが強制的にオンになり、EDTは無効になります。

詳細については、「アダプティブトランスポート」を参照してください。

ドラッグアンドドロップ設定

この設定は、クライアントと仮想アプリケーションまたはデスクトップの間でのファイルのドラッグを許可または防止します。デフォルトでは、ドラッグアンドドロップポリシーは無効になっています。必要に応じて、このポリシーを有効にできます。

アプリケーション起動待機タイムアウト

この設定は、セッションが最初のアプリケーションの起動を待機するミリ秒単位の待機タイムアウト値を指定します。アプリケーションの起動がこの期間を超えると、セッションは終了します。

デフォルトの時間（10,000ミリ秒）を選択するか、ミリ秒単位で数値を指定できます。

クライアントクリップボードリダイレクト

この設定は、ユーザーデバイスのクリップボードがサーバー上のクリップボードにマップされることを許可または禁止します。

デフォルトでは、クリップボードのリダイレクトは許可されています。

セッションとローカルクリップボード間でのコピー＆ペーストによるデータ転送を防ぐには、**禁止**を選択します。ユーザーは、セッション内で実行されているアプリケーション間では、引き続きデータをコピー＆ペーストできます。

この設定を許可した後、クライアント接続でクリップボードが消費できる最大許容帯域幅を構成します。**クリップボードリダイレクト帯域幅制限**または**クリップボードリダイレクト帯域幅制限率**の設定を使用します。

クライアントクリップボード書き込み許可形式

クライアントクリップボード書き込みの制限設定が**有効**の場合、ホストクリップボードデータはクライアントエンドポイントと共有できません。この設定を使用して、特定のデータ形式をクライアントエンドポイントクリップボードと共有することを許可できます。この設定を使用するには、これを有効にし、許可する特定の形式を追加します。

次のクリップボード形式はシステム定義です。

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

XenAppおよびXenDesktopとCitrix Virtual Apps and Desktops™には、以下のカスタム形式が事前定義されています。

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- CFX_FILE

HTML形式はデフォルトで無効になっています。この機能を有効にするには:

- **クライアントクリップボードリダイレクト**が**許可**に設定されていることを確認します。
- **クライアントクリップボード書き込みの制限**が**有効**に設定されていることを確認します。
- **クライアントクリップボード書き込み許可形式**に**CF_HTML**（およびサポートしたいその他の形式）のエントリを追加します。

カスタム形式をさらに追加できます。カスタム形式名は、システムに登録される形式と一致している必要があります。形式名は大文字と小文字を区別します。

この設定は、**クライアントクリップボードリダイレクト**ポリシーが**禁止**に設定されている場合、または**クライアントクリップボード書き込みの制限**ポリシーが**無効**に設定されている場合には適用されません。

> **注:**
>
> HTML 形式のクリップボードコピーサポート (CF_HTML) を有効にすると、コピーされたコンテンツのソースから宛先にスクリプトがコピーされます。コピーを進める前に、ソースを信頼できることを確認してください。スクリプトを含むコンテンツをコピーした場合、それらは宛先ファイルをHTMLファイルとして保存して実行した場合にのみ有効になります。

クリップボードのクライアントからセッションへの転送サイズを制限する

この設定は、ユーザーが単一のコピー＆ペースト操作中にクライアントエンドポイントから仮想セッションに転送できるクリップボードデータの最大サイズを指定します。

クリップボード転送サイズを制限するには、**「クリップボードのクライアントからセッションへの転送サイズを制限する」**設定を有効にします。次に、「サイズ制限」**フィールドにキロバイト単位の値を入力して、ローカルクリップボードとセッション間のデータ転送サイズを定義します。

既定では、この設定は無効になっており、クライアントからセッションへの転送に制限はありません。

HDX™ ダイレクト

HDX Directを使用すると、直接通信が可能な場合にクライアントがセッションホストとの直接接続を自動的に確立できます。接続は、ネットワークレベルの暗号化を使用して安全に確立されます。

HDX Direct モード

HDX Directは、内部クライアントと外部クライアントの両方でセッションホストとの直接接続を確立するために使用できます。この設定は、HDX Directが内部クライアントのみに利用可能か、内部クライアントと外部クライアントの両方に利用可能かを決定します。

「内部」のみに設定されている場合、HDX Directは内部ネットワーク内のクライアントに対してのみ直接接続を確立しようとします。

「内部」と「外部」に設定されている場合、HDX Directは内部クライアントと外部クライアントの両方に対して直接接続を確立しようとします。

既定では、HDX Direct は内部クライアントのみに設定されています。

HDX Direct ポート範囲

外部ユーザーからの接続にHDX Directが使用するポートの範囲。 デフォルトでは、HDX Directはポート範囲55000～55250を使用します。

クリップボードのセッションからクライアントへの転送サイズを制限する

この設定は、ユーザーが単一のコピー＆ペースト操作中に仮想セッションからクライアントエンドポイントに転送できるクリップボードデータの最大サイズを指定します。

クリップボード転送サイズを制限するには、**「クリップボードのセッションからクライアントへの転送サイズを制限する」設定を有効にします。次に、「サイズ制限」**フィールドにキロバイト単位の値を入力して、セッションとローカルクリップボード間のデータ転送サイズを定義します。

既定では、この設定は無効になっており、セッションからクライアントへの転送に制限はありません。

クライアントクリップボードへの書き込みを制限する

この設定が**有効**になっている場合、ホストのクリップボードデータはクライアントエンドポイントと共有できません。**クライアントクリップボードへの書き込みを許可する形式**設定を有効にすることで、特定の形式を許可できます。

デフォルトでは、この設定は**無効**です。

セッションクリップボードへの書き込みを制限する

この設定が**有効**になっている場合、クライアントのクリップボードデータはセッションアプリケーションと共有できません。**セッションクリップボードへの書き込みを許可する形式**設定を有効にすることで、特定の形式を許可できます。

デフォルトでは、この設定は**無効**です。

セッションクリップボードへの書き込みを許可する形式

セッションクリップボードへの書き込みを制限する設定が**有効**になっている場合、クライアントのクリップボードデータはセッションアプリケーションと共有できません。この設定を使用して、特定のデータ形式をセッションクリップボードと共有することを許可できます。

以下のクリップボード形式はシステム定義です。

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY

- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

XenApp and XenDesktopおよびCitrix Virtual Apps and Desktopsでは、以下のカスタム形式が事前定義されています。

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

HTML形式はデフォルトで無効になっています。この機能を有効にするには：

- **クライアントクリップボードリダイレクト**が**許可**に設定されていることを確認します。
- **セッションクリップボード書き込みの制限**が**有効**に設定されていることを確認します。
- **セッションクリップボード書き込み許可形式**に**CF_HTML**（およびサポートしたいその他の形式）のエントリを追加します。

さらにカスタム形式を追加できます。カスタム形式名は、システムに登録される形式と一致している必要があります。形式名は大文字と小文字を区別します。

クライアントクリップボードリダイレクトポリシーが**禁止**に設定されている場合、または**セッションクリップボード書き込みの制限**ポリシーが**無効**に設定されている場合、この設定は適用されません。

> **注:**
>
> HTML形式のクリップボードコピーサポート（CF_HTML）を有効にすると、コピーされたコンテンツのソースから宛先にスクリプトがコピーされます。コピーを続行する前に、ソースを信頼できることを確認してください。スクリプトを含むコンテンツをコピーした場合、それらは宛先ファイルをHTMLファイルとして保存して実行した場合にのみ有効になります。

デスクトップの起動

この設定は、VDA Direct Access Usersグループの非管理者ユーザーがICA接続を使用してそのVDA上のセッションに接続することを許可または禁止します。

デフォルトでは、非管理者ユーザーはこれらのセッションに接続できません。

この設定は、RDP接続を使用しているVDAダイレクトアクセスユーザーグループ内の非管理者ユーザーには影響しません。これらのユーザーは、この設定が有効または無効になっている場合でもVDAに接続できます。この設定は、VDAダイレクトアクセスユーザーグループに属していない非管理者ユーザーには影響しません。これらのユーザーは、この設定が有効または無効になっている場合、VDAに接続できません。

FIDO2リダイレクト

この設定は、FIDO2リダイレクトを有効または無効にします。FIDO2リダイレクトにより、ユーザーは仮想マシン内のローカルエンドポイントFIDO2コンポーネントを活用できます。ユーザーは、TPM 2.0とWindows Helloを搭載したデバイスで、FIDO2セキュリティキーまたは統合生体認証を介して仮想セッションを認証できます。

この設定が**許可**されている場合、ユーザーはローカルエンドポイント機能を使用してFIDO2認証を行うことができます。デフォルトでは、この設定は**許可**されています。

ICAリスナー接続タイムアウト

この設定は、ICAプロトコルを使用した接続が完了するまでの最大待機時間を指定します。

デフォルトでは、最大待機時間は120,000ミリ秒、つまり2分です。

ICAリスナーポート番号

この設定は、サーバー上のICAプロトコルで使用されるTCP/IPポート番号を指定します。

デフォルトでは、ポート番号は1494に設定されています。

有効なポート番号は0～65535の範囲でなければならず、他の既知のポート番号と競合してはなりません。ポート番号を変更した場合は、新しい値を有効にするためにサーバーを再起動してください。サーバーのポート番号を変更した場合は、そのサーバーに接続するすべてのCitrix Workspace™アプリまたはプラグインでも変更する必要があります。

キーボードと入力方式エディター (IME)

この設定は、次の項目を有効または無効にします。

- 動的キーボードレイアウト同期
- 入力方式エディター (IME)
- Unicode キーボードレイアウトマッピング
- キーボードレイアウト切り替え通知ダイアログメッセージの表示/非表示

1. Web Studioで、**［キーボードとIME］**を選択します。
2. VDAでの動的キーボードレイアウト同期と汎用クライアント入力方式エディター (IME) 機能を制御するには、**［クライアントキーボードレイアウト同期とIMEの改善］**を選択します。以下を構成できます。

   ［無効］ - 動的キーボードレイアウト同期と汎用クライアント入力方式エディター (IME)。

   動的なクライアントキーボードレイアウト同期をサポート - 動的なキーボードレイアウト同期を有効にします。

   ［動的クライアントキーボードレイアウト同期とIMEの改善をサポート］ - 動的キーボードレイアウト同期と汎用クライアント入力方式エディター (IME) の両方を有効にします。
3. Unicode キーボードマッピングを有効または無効にするには、**［Unicode キーボードレイアウトマッピングを有効にする］**を選択します。
4. ユーザーがクライアントキーボードレイアウトを変更したときに、キーボードレイアウトが同期中であることを示すメッセージを表示するかどうかを制御するには、**［キーボードレイアウト切り替えポップアップメッセージボックスを非表示にする］**を選択します。メッセージが表示されないようにすると、ユーザーは誤った文字入力にならないように、入力する前に数秒待つ必要があります。

デフォルト設定：

- **クライアントキーボードレイアウト同期とIMEの改善**
  - Windows Server 2016およびWindows Server 2019では無効。
  - Windows Server 2012およびWindows 2010での動的クライアントキーボードレイアウト同期とIMEの改善をサポートします。
- **Unicodeキーボードレイアウトマッピングを無効にする**
- **キーボードレイアウト切り替えポップアップメッセージボックスを表示する**

このポリシーは、ポリシー設定の**説明**セクションに記載されているレジストリ設定を置き換えます。

ログオフチェッカーの起動遅延

この設定は、ログオフチェッカーの起動を遅延させる期間を指定します。このポリシーを使用して、クライアントセッションがセッションを切断するまでに待機する時間（秒単位）を設定します。

この設定は、ユーザーがサーバーからログオフするのにかかる時間も増加させます。

ロス許容モード

> **重要:**
>
> - この機能には、Windows版Citrix Workspaceアプリ2002以降が必要です。VDAのこのバージョンは、利用可能になり次第サポートされます。
> - グラフィックの損失許容モードは、Citrix GatewayおよびCitrix Gateway Serviceでサポートされています。このモードは、直接接続の場合にのみ利用可能です。

この設定は、グラフィックのロス許容モードを有効または無効にします。

デフォルトでは、グラフィックのロス許容モードは**許可**されています。

許可されている場合、パケット損失と遅延がしきい値を超えると、このモードに入ります。しきい値は、ロス許容しきい値ポリシーを使用して設定できます。

ロス許容しきい値

損失許容モードが利用可能な場合、この設定は、グラフィックの損失許容モードにセッションが切り替わるネットワークメトリックのしきい値を指定します。

デフォルトのしきい値は次のとおりです。

- パケット損失: 5%
- 遅延: 300ミリ秒 (RTT)

詳細については、損失許容モードを参照してください。

オーディオの損失許容モード

この設定は、オーディオの損失許容モードを有効または無効にします。

有効にすると、オーディオは損失許容モードで送信されます。

デフォルトでは、オーディオの損失許容モードは**禁止**されています。

ポリシーを有効にするには、オーディオポリシーの損失許容モードのレジストリを**許可**に編集します。

オーディオの損失許容モードを有効にするには、EDTトランスポートが必要です。

Rendezvous プロトコル

この設定は、Citrix Gateway Serviceを使用する際のHDXセッションのプロキシ方法を変更します。有効にすると、HDXトラフィックはCitrix Cloud Connectorを経由しなくなります。代わりに、VDAはCitrix Gateway Serviceに直接アウトバウンド接続を確立します（Cloud Connectorのスケーラビリティを向上させます）。

> **重要:**
>
> Citrix Cloud™の機能トグルとHDXポリシー設定がこの機能を制御します。Citrix Cloudの機能トグルはデフォルトで有効になっていますが、HDX設定はデフォルトで無効になっています。HDX設定は、Citrix Gateway Serviceを介して確立されたHDXセッションにのみ影響します。この設定は、クライアントとVDA間で直接確立されたセッションや、オンプレミスのCitrix Gatewayを介して確立されたセッションには影響しません。

> 詳細については、Rendezvousプロトコルを参照してください。

Rendezvousプロキシ構成

この設定により、Rendezvousプロトコルで使用する明示的なプロキシを構成できます。透過型プロキシを使用している場合、この設定を有効にする必要はありません。

デフォルトでは、この設定は無効になっています。

無効にすると、VDAはGateway ServiceとのRendezvous接続を確立しようとするときに、非透過型プロキシを介してアウトバウンドトラフィックをルーティングしません。

有効にすると、VDAはこの設定で定義されたプロキシを介してGateway ServiceとのRendezvous接続を確立しようとします。

VDAは、Rendezvous接続にHTTPおよびSOCKS5プロキシの使用をサポートしています。Rendezvous接続にプロキシを使用するようにVDAを構成するには、この設定を有効にする必要があります。また、プロキシのアドレスまたはPACファイルへのパスを指定します。例：

- プロキシアドレス: `http://<URL or IP>:<port>` または `socks5://<URL or IP>:<port>`
- PACファイル: `http://<URL or IP>/<path>/<filename>.pac`

  VDAバージョン2103は、PACファイルを使用したプロキシ構成でサポートされる最小バージョンです。SOCKS5プロキシのPACファイルスキーマの詳細については、「プロキシ構成」を参照してください。

注:

SOCKS5 プロキシのみが EDT を介したデータ転送をサポートしています。HTTP プロキシの場合は、ICA のトランスポートプロトコルとして TCP を使用してください。

詳細については、「Rendezvousプロトコル」を参照してください。

クライアント接続中の非公開プログラムの起動

この設定は、サーバー上でRDPを介して初期アプリケーションの起動を許可するかどうかを指定します。

デフォルトでは、サーバー上でRDPを介して初期アプリケーションの起動は許可されていません。

セッションメトリックの収集

この設定により、Citrix は VDA と Workspace 間のユーザーおよびマシンセッションメトリックを収集し、ユーザーエクスペリエンスを向上させることができます。

オペレーティングシステム、稼働時間、コンピューターシステム情報、ビデオコントローラーの詳細、VDAバージョン、展開タイプ、ドメイン参加ステータスなどのデータがCitrixによって収集されます。さらに、製品改善の取り組みを支援するために、いくつかのセッション構成、パフォーマンスおよび信頼性データも収集できます。カスタマーエクスペリエンス向上プログラムの詳細については、以下を参照してください。

- `<https://more.citrix.com/XD-CEIP>`
- `<https://docs.citrix.com/ja-jp/linux-virtual-delivery-agent/current-release/configure/administration/linux-vda-data-collection-program>`
- `<https://docs.citrix.com/ja-jp/mac-vda/configure/session/supportability-service>`

デフォルトでは、この設定は有効になっています。

タブレットモード切り替えポリシー設定

タブレットモードの切り替えは、VDA上のストアアプリ、Win32アプリ、およびWindowsシェルを最適化します。これは、電話やタブレットなどの小型デバイス、またはタッチ対応デバイスから接続する際に、仮想デスクトップを自動的にタブレットモードに切り替えることで実現されます。

このポリシーが無効になっている場合、VDAはユーザーが設定したモードになり、クライアントの種類に関係なく、そのモードを維持します。

クライアント自動再接続ポリシー設定

クライアント自動再接続セクションには、セッションの自動再接続を制御するためのポリシー設定が含まれています。

クライアント自動再接続

この設定は、接続が中断された後に同じクライアントによる自動再接続を許可または禁止します。

Citrix Receiver for Windows 4.7以降およびCitrix Workspaceアプリ1808以降では、クライアント自動再接続はCitrix Studioのポリシー設定のみを使用します。Studioでこれらのポリシーを更新すると、クライアント自動再接続がサーバーからクライアントに同期されます。Citrix Receiver for Windowsの以前のバージョンでクライアント自動再接続を構成するには、Studioポリシーを使用し、レジストリまたはdefault.icaファイルを変更します。

クライアント自動再接続を許可すると、接続が切断されたときに中断された場所からユーザーが作業を再開できます。自動再接続は切断された接続を検出し、ユーザーをセッションに再接続します。

セッションIDと資格情報へのキーを含むCitrix Workspace™アプリのCookieが使用されない場合、自動再接続によって新しいセッションが開始される可能性があります。つまり、既存のセッションに再接続するのではなく、新しいセッションが開始される可能性があります。Cookieの有効期限が切れている場合、Cookieは使用されません。たとえば、再接続の遅延や資格情報の再入力が必要な場合、Cookieの有効期限が切れることがあります。ユーザーが意図的に切断した場合、クライアント自動再接続はトリガーされません。

再接続が進行中の場合、セッションウィンドウはグレー表示されます。カウントダウンタイマーは、セッションが再接続されるまでの残り時間を表示します。セッションがタイムアウトすると、切断されます。

アプリケーションセッションの場合、自動再接続が許可されていると、通知領域にカウントダウンタイマーが表示されます。このタイマーは、セッションが再接続されるまでの残り時間を指定します。Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルするまで、セッションへの再接続を試行します。

ユーザーセッションの場合、自動再接続が許可されていると、Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルしない限り、指定された期間、セッションへの再接続を試行します。デフォルトでは、この期間は2分です。この期間を変更するには、ポリシーを編集します。

デフォルトでは、クライアント自動再接続は許可されています。ポリシーを**禁止**に設定することで無効にできます。

クライアント自動再接続認証

この設定は、クライアント自動再接続に認証が必要かどうかを指定します。

ユーザーが最初にログオンすると、資格情報は暗号化され、メモリに保存され、暗号化キーを含むCookieが作成されます。CookieはCitrix Workspaceアプリに送信されます。この設定が構成されている場合、Cookieは使用されません。代わりに、Citrix Workspaceアプリが自動的に再接続しようとすると、資格情報を要求するダイアログボックスがユーザーに表示されます。

デフォルトでは、認証は必要ありません。

自動クライアント再接続ログ

この設定は、イベントログへの自動クライアント再接続の記録を有効または無効にします。

ログ記録が有効な場合、サーバーのシステムログは、成功および失敗した自動再接続イベントに関する情報をキャプチャします。サイトは、すべてのサーバーの再接続イベントの結合ログを提供しません。

デフォルトでは、ログ記録は無効です。

自動クライアント再接続のタイムアウト

デフォルトでは、自動クライアント再接続のタイムアウトは120秒に設定されており、自動クライアント再接続のタイムアウトの最大構成可能値は300秒です。このポリシーを使用してタイムアウト値を設定します。

再接続UIの透明度レベル

この設定により、セッションの信頼性再接続中にXenAppまたはXenDesktop®セッションウィンドウに適用される不透明度レベルを指定できます。

デフォルトでは、再接続UIの透明度は80%に設定されています。

オーディオポリシー設定

オーディオセクションには、パフォーマンスを低下させることなく、ユーザーデバイスがセッションでオーディオを送受信できるようにするポリシー設定が含まれています。

アダプティブオーディオ

この設定は、アダプティブオーディオを有効または無効にします。このポリシーを有効にすると、最高のユーザーエクスペリエンスを提供するためにオーディオ品質設定が動的に調整されます。こ

の設定は、Citrix Virtual Apps and Desktops™ 2109以降を使用するVDAのシングルセッションOSおよびマルチセッションOSセッションの両方に適用されます。

この設定が禁止されている場合、オーディオ品質ポリシーが適用されます。詳細については、「オーディオ品質」を参照してください。

デフォルトでは、アダプティブオーディオポリシーは有効になっています。

UDPリアルタイムトランスポート経由のオーディオ

この設定は、User Datagram Protocol (UDP) を使用してRTP経由でVDAとユーザーデバイス間でオーディオを送受信することを許可または禁止します。この設定が無効になっている場合、オーディオはTCP経由で送受信されます。

デフォルトでは、UDP経由のオーディオは許可されています。

オーディオプラグアンドプレイ

この設定は、複数のオーディオデバイスを使用してサウンドを録音および再生することを許可または禁止します。

デフォルトでは、複数のオーディオデバイスの使用は許可されています。

この設定は、WindowsマルチセッションOSマシンにのみ適用されます。

オーディオ品質

この設定は、ユーザーセッションで受信されるサウンドの品質レベルを指定します。

デフォルトでは、サウンド品質は「高 - 高精細オーディオ」に設定されています。

サウンド品質を制御するには、次のいずれかのオプションを選択します。

- 低帯域幅接続の場合は、「低 - 低速接続用」を選択します。ユーザーデバイスに送信されるサウンドは最大16 Kbpsに圧縮されます。この圧縮により、サウンドの品質は大幅に低下しますが、低帯域幅接続でも適切なパフォーマンスが得られます。
- 中 - 音声に最適化されており、Voice over Internet Protocolアプリケーションを提供します。この設定は、512 Kbps未満の回線、または著しい輻輳やパケット損失があるような困難なネットワーク接続でメディアアプリケーションを提供します。このコーデックはエンコード時間が速く、サーバー側のメディア処理が必要な場合にソフトフォンやユニファイドコミュニケーションアプリケーションでの使用に最適です。

  ユーザーデバイスに送信されるオーディオは、最大64 Kbpsに圧縮されます。この圧縮により、ユーザーデバイスで再生されるオーディオの品質は中程度に低下しますが、低遅延で低帯域幅の消費を実現します。Voice over Internet Protocolの品質が不十分な場合は、「Audio over

UDP Real-time Transport」ポリシー設定が「許可」に設定されていることを確認してください。

現在、UDP経由のリアルタイムトランスポート（RTP）は、このオーディオ品質が選択されている場合にのみサポートされます。低速（512 Kbps未満）回線のような困難なネットワーク接続でメディアアプリケーションを配信する場合でも、このオーディオ品質を使用してください。また、ネットワークに輻輳やパケット損失がある場合も同様です。

- 「高」を選択 - 帯域幅が豊富で音質が重要な接続には、高精細オーディオを使用します。クライアントはネイティブレートでサウンドを再生できます。サウンドはCD品質まで維持される高音質レベルで圧縮され、最大112 Kbpsの帯域幅を使用します。この量のデータを送信すると、CPU使用率が増加し、ネットワークが輻輳する可能性があります。

帯域幅は、オーディオの録音または再生中にのみ消費されます。両方が同時に発生する場合、帯域幅の消費量は2倍になります。

最大帯域幅を指定するには、**オーディオリダイレクト帯域幅制限**または**オーディオリダイレクト帯域幅制限率**の設定を構成します。

クライアントオーディオリダイレクト

この設定は、サーバーでホストされているアプリケーションが、ユーザーデバイスにインストールされているサウンドデバイスを介してサウンドを再生できるかどうかを指定します。この設定は、ユーザーがオーディオ入力を録音できるかどうかも指定します。

デフォルトでは、オーディオリダイレクトは許可されています。

この設定を許可した後、オーディオの再生または録音によって消費される帯域幅を制限できます。オーディオによって消費される帯域幅の量を制限すると、アプリケーションのパフォーマンスが向上する可能性がありますが、オーディオ品質が低下する可能性もあります。帯域幅は、オーディオの録音または再生中にのみ消費されます。両方が同時に発生する場合、帯域幅の消費量は2倍になります。最大帯域幅を指定するには、**オーディオリダイレクト帯域幅制限**または**オーディオリダイレクト帯域幅制限パーセント**設定を構成します。

WindowsマルチセッションOSマシンでは、複数のオーディオデバイスをサポートするために、**オーディオプラグアンドプレイ**設定が有効になっていることを確認してください。

重要：クライアントオーディオリダイレクトを禁止すると、すべてのHDX™オーディオ機能が無効になります。

クライアントマイクのリダイレクト

この設定は、クライアントマイクのリダイレクトを有効または無効にします。有効にすると、ユーザーはセッションでマイクを使用してオーディオ入力を録音できます。

デフォルトでは、マイクのリダイレクトは許可されています。

セキュリティのため、信頼されていないサーバーがデバイスを介してマイクにアクセスしようとすると、ユーザーに警告が表示されます。ユーザーはアクセスを許可するかどうかを選択できます。Citrix Workspace™アプリで警告を無効にすることもできます。

WindowsマルチセッションOSマシンでは、複数のオーディオデバイスをサポートするために、オーディオプラグアンドプレイ設定が有効になっていることを確認してください。

ユーザーデバイスで**クライアントオーディオリダイレクト**設定が無効になっている場合、このルールは無効になります。

帯域幅ポリシー設定

「**帯域幅**」セクションには、クライアントセッションの帯域幅使用に関連するパフォーマンスの問題を回避するためのポリシー設定が含まれています。

重要: これらのポリシー設定を**マルチストリームポリシー**設定と併用すると、予期しない結果が生じる可能性があります。ポリシーでマルチストリーム設定を使用する場合は、これらの帯域幅制限ポリシー設定が含まれていないことを確認してください。

オーディオリダイレクト帯域幅制限

この設定は、ユーザーセッションでオーディオを再生または録音するために許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**オーディオリダイレクト帯域幅制限の割合**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

オーディオリダイレクト帯域幅制限の割合

この設定は、オーディオの再生または録音に許可される最大帯域幅制限を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**オーディオリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合は、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

クライアントUSBデバイスリダイレクト帯域幅制限

この設定は、USBデバイスのクライアントとの間のリダイレクトに許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**クライアントUSBデバイスリダイレクト帯域幅制限率**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

クライアントUSBデバイスリダイレクト帯域幅制限率

この設定は、USBデバイスのクライアントとの間のリダイレクトに許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**クライアントUSBデバイスリダイレクト帯域幅制限**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

クリップボードリダイレクト帯域幅制限

この設定は、セッションとローカルクリップボード間のデータ転送に許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**クリップボードリダイレクト帯域幅制限率**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

クリップボードリダイレクト帯域幅制限率

この設定は、セッションとローカルクリップボード間のデータ転送に許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**クリップボードリダイレクト帯域幅制限**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

COMポートリダイレクトの帯域幅制限

注: Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。「COMポートおよびLPTポートリダイレクト設定をレジストリで構成する」(/ja-jp/xenapp-and-xendesktop/current-release/policies/reference/configure-com-ports-and-lpt-redirection-using-registry.html)を参照してください。

この設定は、クライアント接続でCOMポートにアクセスするために許可される最大帯域幅をキロビット/秒で指定します。この設定に値を入力し、**COMポートリダイレクト帯域幅制限率**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

COMポートリダイレクト帯域幅制限率

注: Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。「COMポートおよびLPTポートリダイレクト設定をレジストリで構成する」(/ja-jp/xenapp-and-xendesktop/current-release/policies/reference/configure-com-ports-and-lpt-redirection-using-registry.html)を参照してください。

この設定は、クライアント接続でCOMポートにアクセスするために許可される最大帯域幅を、総セッション帯域幅の割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**COMポートリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

ファイルリダイレクト帯域幅制限

この設定は、ユーザーセッションでクライアントドライブにアクセスするために許可される最大帯域幅を指定します。許可される最大帯域幅はキロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**ファイルリダイレクト帯域幅制限率**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

ファイルリダイレクト帯域幅制限率

この設定は、クライアントドライブにアクセスするために許可される最大帯域幅制限を、総セッション帯域幅の割合として指定します。

既定では、最大値（ゼロ）は指定されていません。

この設定と**ファイルリダイレクト帯域幅制限**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合は、クライアントセッションで利用可能な帯域幅の合計量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

HDX™ MediaStreamマルチメディアアクセラレーション帯域幅制限

この設定は、HDX MediaStreamマルチメディアアクセラレーションを使用してストリーミングオーディオおよびビデオを配信するための最大許容帯域幅制限を指定します。最大許容帯域幅はキロビット/秒で指定されます。

既定では、最大値（ゼロ）は指定されていません。

この設定と**HDX MediaStreamマルチメディアアクセラレーション帯域幅制限（パーセント）**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

HDX MediaStreamマルチメディアアクセラレーション帯域幅制限（パーセント）

この設定は、HDX MediaStreamマルチメディアアクセラレーションを使用してストリーミングオーディオおよびビデオを配信するための最大許容帯域幅を、セッション全体の帯域幅に対する割合として指定します。

既定では、最大値（ゼロ）は指定されていません。

この設定と**HDX MediaStreamマルチメディアアクセラレーション帯域幅制限**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合は、クライアントセッションで利用可能な帯域幅の合計量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

LPTポートリダイレクト帯域幅制限

注：Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、単一ユーザーセッションでLPTポートを使用する印刷ジョブに許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**LPTポートリダイレクト帯域幅制限の割合**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

LPTポートリダイレクトの帯域幅制限（パーセント）

注：Virtual Delivery Agent 7.0から7.8では、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、単一クライアントセッションでLPTポートを使用する印刷ジョブの帯域幅制限を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**LPTポートリダイレクト帯域幅制限**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の合計量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

セッション全体の帯域幅制限

この設定は、ユーザーセッションで利用可能な総帯域幅を、1秒あたりのキロビット単位で指定します。

適用可能な帯域幅の最大値は20 Mbps（20,000 Kbps）です。デフォルトでは、最大値（ゼロ）は指定されていません。

クライアント接続によって消費される帯域幅の量を制限すると、クライアント接続外の他のアプリケーションが限られた帯域幅を競合している場合に、パフォーマンスを向上させることができます。

プリンターリダイレクト帯域幅制限

この設定は、ユーザーセッションでクライアントプリンターにアクセスするために許可される最大帯域幅を指定します。許可される最大帯域幅はキロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**プリンターリダイレクト帯域幅制限の割合**設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

プリンターリダイレクト帯域幅制限の割合

この設定は、クライアントプリンターへのアクセスに許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**プリンターリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

TWAINデバイスリダイレクト帯域幅制限

この設定は、公開アプリケーションからTWAINイメージングデバイスを制御するために許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**TWAINデバイスリダイレクト帯域幅制限の割合**設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

TWAINデバイスリダイレクト帯域幅制限の割合

この設定は、公開アプリケーションからTWAINイメージングデバイスを制御するために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**TWAINデバイスリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

双方向コンテンツリダイレクトポリシー設定

双方向コンテンツリダイレクトセクションには、クライアントからVDAへ、およびVDAからクライアントへのURLリダイレクトを有効または無効にするためのポリシー設定があります。

サーバーポリシーはWeb Studioで設定されます。Citrix Workspace™アプリバージョン2311以降、この設定は、Web Studioで非推奨となった以下の3つのレガシー設定に代わるものです。

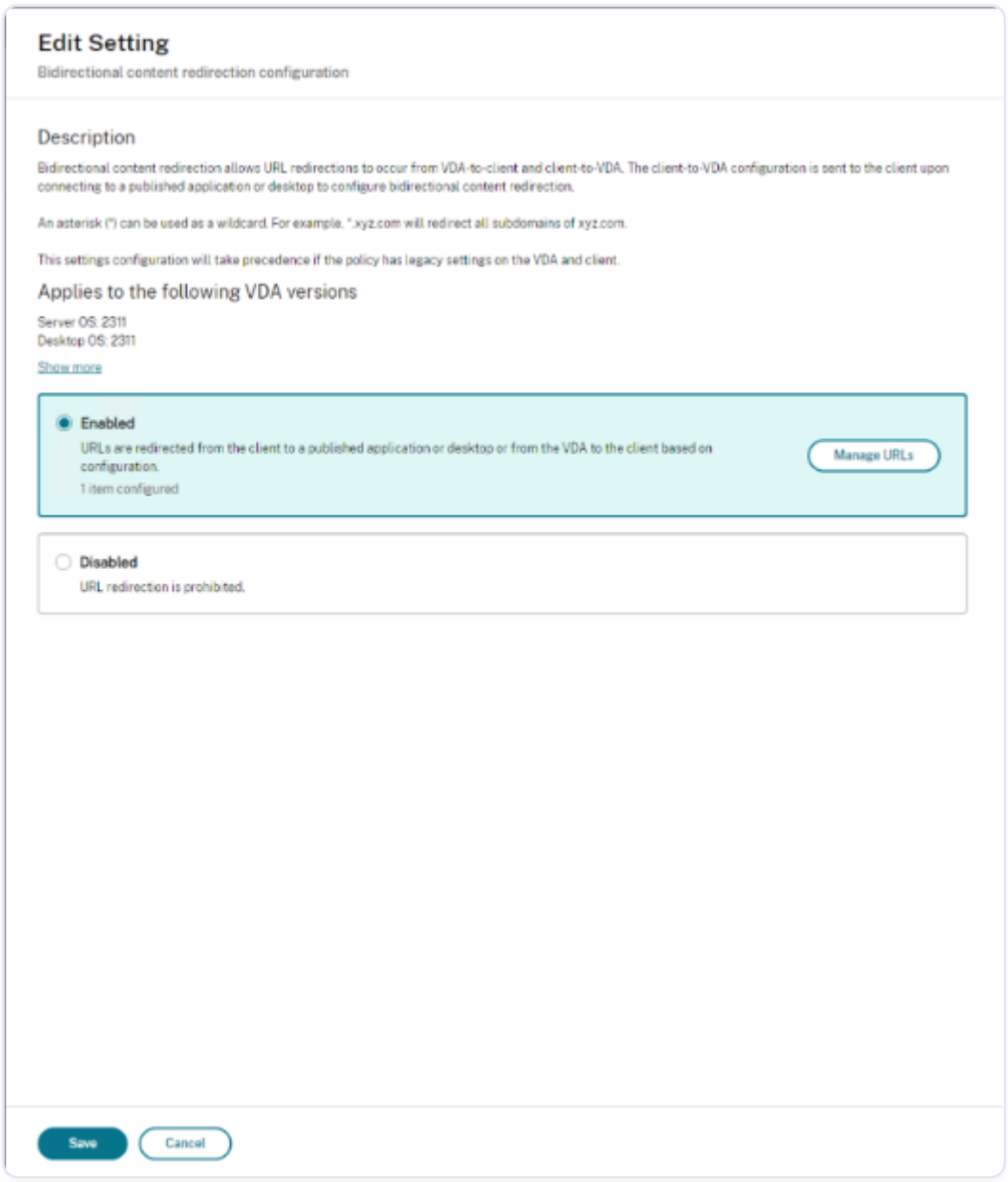
- 双方向コンテンツリダイレクトを許可する
- VDAにリダイレクトされる許可されたURL
- クライアントにリダイレクトされる許可されたURL

また、Windowsクライアント上の以下の3つのローカルグループポリシーオブジェクト (GPO) 設定も置き換わります。

- 双方向コンテンツリダイレクト

- 双方向コンテンツリダイレクトのオーバーライド
- OAuthリダイレクト

この設定が有効になっている場合、公開されたアプリまたはデスクトップに接続すると、双方向コンテンツリダイレクトを構成するためのクライアントからVDAへの設定がクライアントに送信されます。



この設定が構成されている場合、Web Studioおよびクライアント上のレガシー設定よりも優先されます。Citrix®は、予期しない動作を避けるために、新しいポリシー設定のみを使用し、レガシー設定を削除することを推奨します。

VDAとDDCがバージョン2311以降を実行している場合、クライアントポリシーを設定してはいけません。そうでない場合、クライアントポリシーはCitrix Workspaceアプリのグループポリシーオブジェクト管理テンプレートから設定されます。

Citrixは、ホストからクライアントへのリダイレクトと、クライアントからURLへのリダイレクトのためのローカルアプリアクセスを提供しています。ただし、Citrixはドメイン参加済みWindowsクライアントには双方向コンテンツリダイレクトを使用することを推奨します。

Citrix は、Desktop Studio の代わりに Web Studio の新しい UI を使用して機能を構成することをお勧めします。

ワイルドカードリダイレクト

双方向コンテンツリダイレクトは、リダイレクトする URL を定義する際にワイルドカードの使用をサポートします。詳細および双方向コンテンツリダイレクトの構成については、構成 の手順を参照してください。 Web Studio で、`hostToClientUrls` 配列または `clientToHostUrls` 配列の `url` キーの値として JSON 文字列を編集して、ワイルドカード URL を設定します。

> **注:**
>
> - 無限ループを避けるため、`hostToClientUrls` と `clientToHostUrls` に同じ URL を設定しないでください。
> - トップレベルドメインはサポートされていません。たとえば、`<https://www.citrix.*>` や `<http://www.citrix.co*>` はリダイレクトされません。

双方向コンテンツリダイレクトの構成

このポリシーを `Enabled` に設定して機能の構成を開始し、**URL の管理**をクリックします。次の構成を設定します。

- **VDA からクライアントへのリダイレクト**
- **クライアントから VDA へのリダイレクト**

VDA からクライアントへのリダイレクト

VDA からクライアントに URL をリダイレクトするには、1 行に 1 つの URL を入力します。ワイルドカードが許可されます。 OAuth リダイレクトを使用すると、クライアントエンドポイントのブラウザを使用して認証を実行し、トークンを VDA に送り返すことができます。

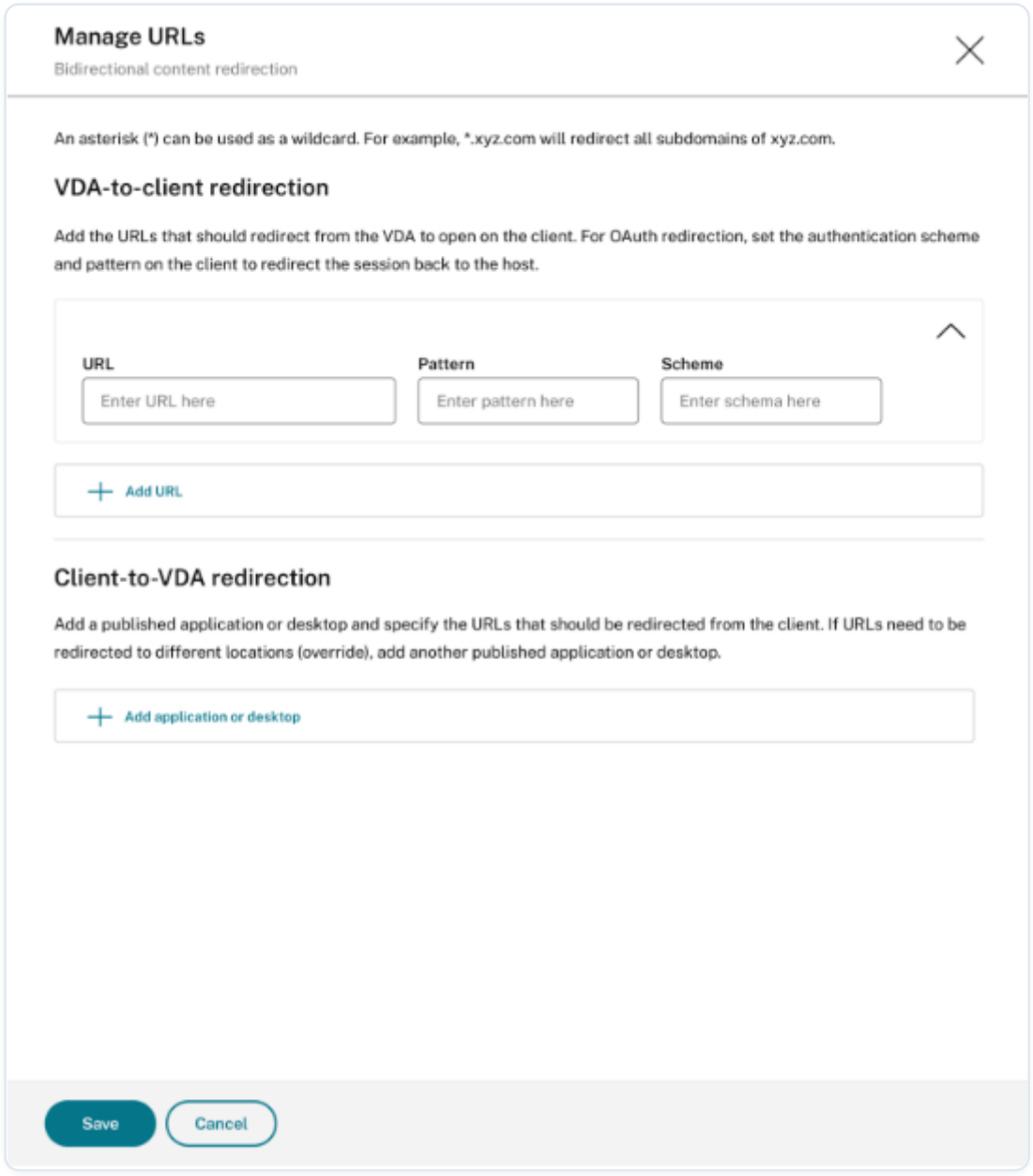
利点:

- ホストされた環境にこれらの資格情報を保存することを回避できます。
- エンドポイントで利用可能で、VDA では利用できない生体認証機能を使用できます。

構成：

URLのVDAからクライアントへのリダイレクトを構成するには、以下を指定します。

- **URL** (必須) VDAからクライアントで開くようにリダイレクトする必要があるURLを追加します。**OAuthリダイレクト**の場合、セッションをホストにリダイレクトするために、クライアントで認証スキームとパターンを設定します。
- **パターン**: (オプション) VDAからクライアントへのURLリダイレクトを介してクライアントにリダイレクトされたときに、OAuth認証フローが開始されたかのように追跡され、フローが完了したとき（結果のスキームまたはリダイレクトURLパターンが開かれたことによって検出される）、その結果のURLが、そのフローを開始したホストVDAにリダイレクトされるURL正規表現。
- **スキーム**: (オプション) **スキーム**が指定されている場合、終了URLは`<scheme>`:// `<something>`の形式であると想定されます。スキームが指定されていない（空である）とします。その場合、元の結果のURLパターンは、正規表現キャプチャグループ（パターンで指定する必要がある）を介してパターンから抽出され、元のURLは`citrix-oauth-redir://`リダイレクトURLを使用するように書き換えられます。フローが完了すると、元のリダイレクトURLはホスト（VDA）にリダイレクトされます。この場合、OAuth認証サーバーは`citrix-oauth-redir://byIndex/1 (2, 3, ... N)`リダイレクトURLを許可するように構成する必要があります。



注:

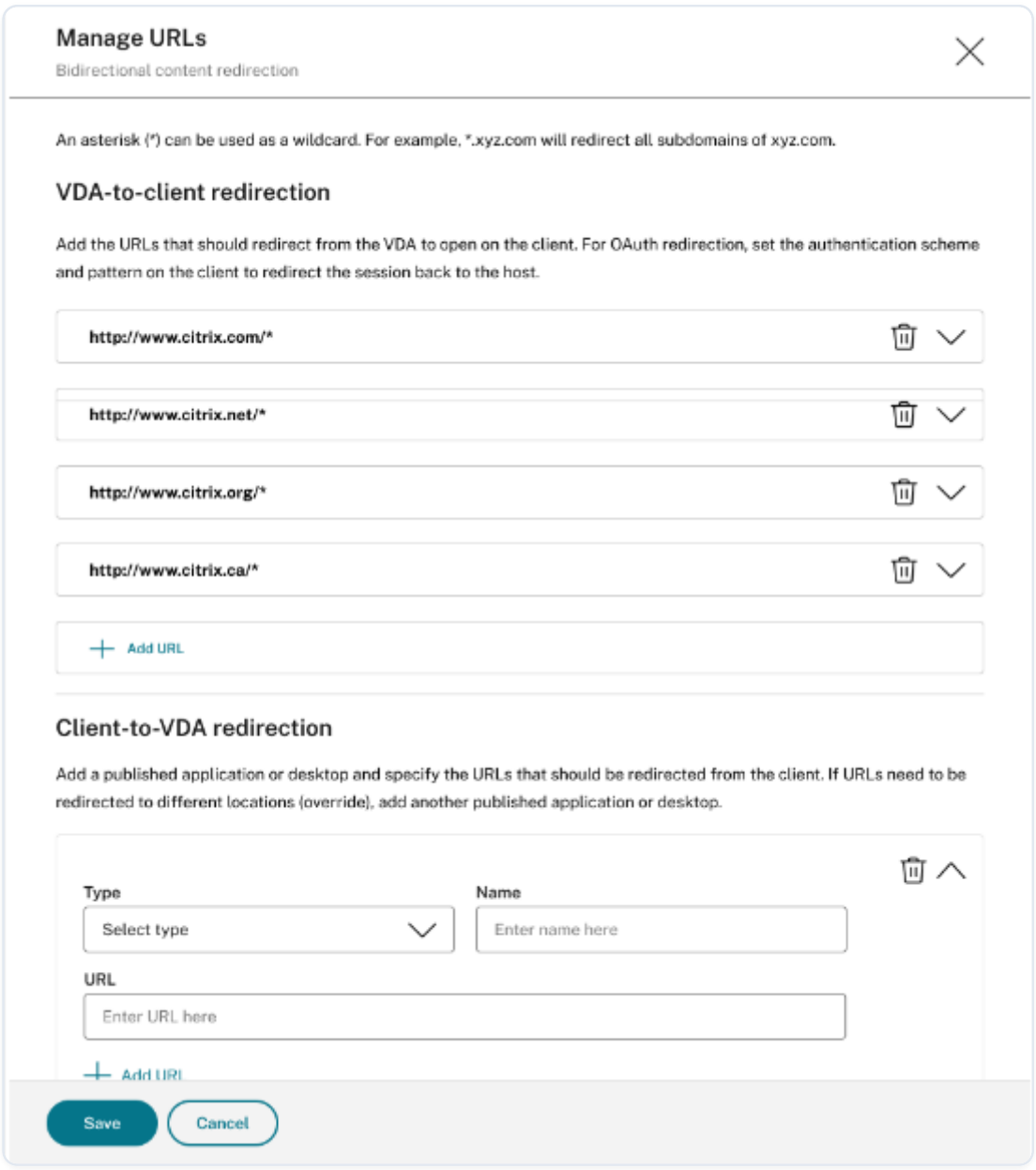
パターンと**スキーム**はどちらもオプションですが、**パターン**が指定されている場合は、**スキーム**も指定する必要があります。

クライアントからVDAへのリダイレクト

クライアントからVDAにURLをリダイレクトするには、次の手順を実行します。

1. クライアントURLの宛先を構成します。
2. 公開アプリケーションまたは公開デスクトップのいずれかを選択します。
3. そのリソースの名前を指定します。

4. そのリソースにリダイレクトする必要があるすべてのURLを追加します。 新しいアプリケーションまたはデスクトップを追加し、そのリソースにリダイレクトするURLを指定することで、このデフォルトのリソースを上書きできます。



デスクトップスタジオ

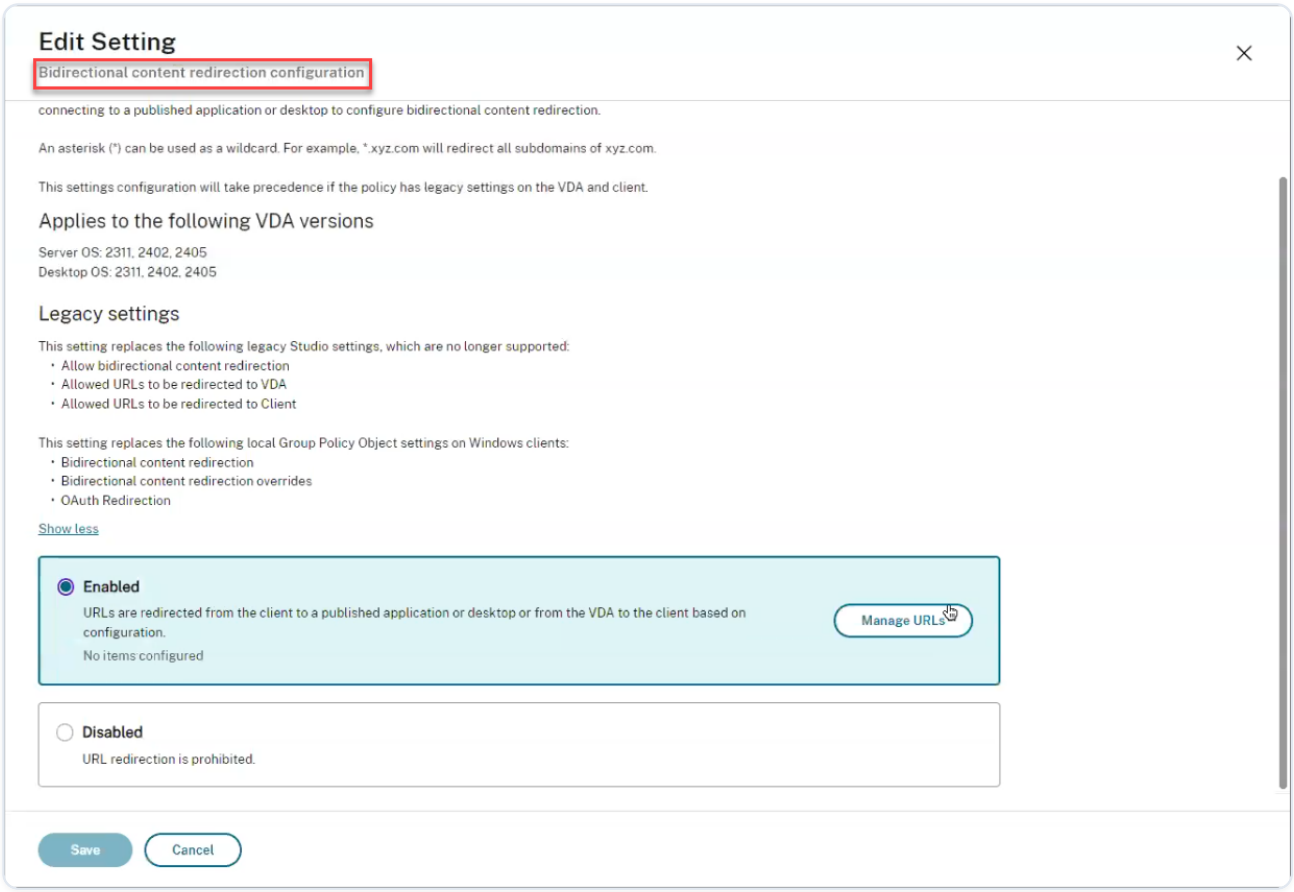
注:

Citrix Virtual Apps and Desktops™ バージョン 2402 以降では、Web Studio を使用してこの機能を構成することをお勧めします。

2311 の双方向コンテンツリダイレクトを構成するには、次の形式で JSON 文字列を作成します。

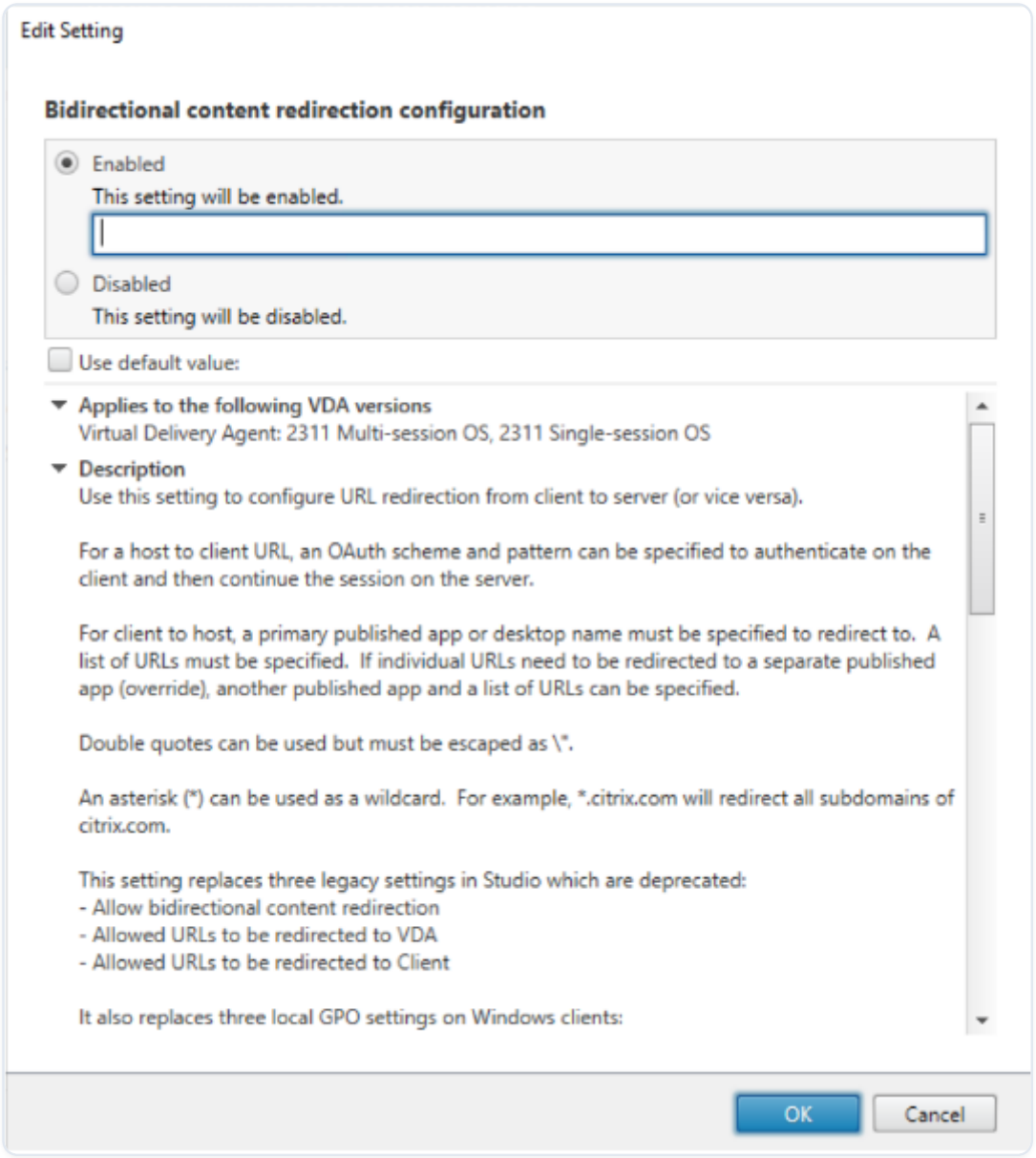
```
{
  "version": 1,
  "hostToClientConfig": [
    {
      "hostToClientUrls": [
        {
          "url": "http://www.citrix.com/*"
        },
        {
          "url": "www.example.com"
        },
        {
          "url": "https://login.example.org/*",
          "oAuthRedirectionPattern": "https://login.example.org/
oauth2?.*",
          "oAuthScheme": "idm.desktop-authentication"
        }
      ]
    }
  ],
  "clientToHostConfig": [
```

```
    {
      "publishedAppOrDesktopNameType": "Desktop",
      "publishedAppOrDesktopName": "Win11Desktop",
      "clientToHostUrls": [
        "https://www.example.net",
        "https://*.citrix.example"
      ]
    },
    {
      "publishedAppOrDesktopNameType": "Application",
      "publishedAppOrDesktopName": "Chrome",
      "clientToHostUrls": [
        "https://tibco.example"
      ]
    }
  ]
}
```



次のパラメーターを設定する必要があります。

- **version**: (必須) 1 に設定します。
- VDA からクライアントへの URL リダイレクトの場合、単一の `hostToClientConfig` を作成します。
- **hostToClientUrls**: (必須) ホスト (VDA) からクライアントにリダイレクトされる URL のリスト。ワイルドカードが許可されます。「*」が指定されている場合、`clientToHostConfig` は `publishedAppOrDesktopNameType`、空の `publishedAppOrDesktopName`、および空の `clientToHostUrls` とともに指定する必要があります。



OAuth リダイレクト

OAuth リダイレクトを使用すると、クライアントエンドポイントブラウザーを使用して認証し、トークンを VDA に送り返すことができます。

利点：

- これらの資格情報をホスト環境に保存することを回避できます。
- エンドポイントで利用可能で、VDA では利用できない生体認証機能を使用できます。

URLのOAuthリダイレクトを構成するには、次のパラメータを指定します。

- **oAuthRedirectionPattern**: (オプション) VDAからクライアントへのURLリダイレクトを介してクライアントにリダイレクトされると、OAuth認証フローが開始されたかのように追跡されるURL正規表現。フローが完了したとき（結果のスキームまたはリダイレクトURLパターンが

開かれることによって検出される）、その結果のURLは、そのフローを開始したホストVDAにリダイレクトされます。

- **oAuthScheme**: (オプション) スキームが指定されている場合、終了URLは`<scheme>`://`<something>`の形式であると想定されます。スキームが指定されていない（空である）とします。その場合、元の結果URLパターンは、正規表現キャプチャグループ（パターンで指定する必要がある）を介してパターンから抽出され、元のURLは`citrix-oauth-redir://`リダイレクトURLを使用するように書き換えられます。フローが完了すると、元のリダイレクトURLはホスト（VDA）にリダイレクトされます。この場合、任意のOAuth認証サーバーは、`citrix-oauth-redir://byIndex/1 (2, 3, ... N)`リダイレクトURLを許可するように構成する必要があります。

クライアントからVDAへのリダイレクトの場合、リダイレクトする各リソースに対して**clientToHostConfig**を作成します。 各リソースには、次のパラメータを含めます。

- **publishedAppOrDesktopNameType**: (必須) Web Studioで構成された公開デスクトップ（「Desktop」）または公開アプリケーション（「Application」のいずれか。リソースが無効な場合、リダイレクトは正しく機能しません。
- **publishedAppOrDesktopName**: (必須) Web Studioで構成されたリソース名。
- **clientToHostUrls**: (必須) クライアントからホスト（VDA）にリダイレクトされるURLのリスト。ワイルドカードが許可されます。

既知の制限

PowerShellを使用してカスタムURLスキーム（HTTPまたはHTTPSではない）でブラウザを起動すると、カスタムURLはクライアントにリダイレクトされません。

ブラウザコンテンツリダイレクトポリシー設定

「ブラウザコンテンツリダイレクト」セクションには、この機能を構成するためのポリシー設定が含まれています。

ブラウザコンテンツリダイレクトは、Citrix Virtual Apps and Desktops™ があらゆるWebブラウザコンテンツ（HTML5など）をユーザーに配信する方法を制御し、最適化します。コンテンツが表示されるブラウザの表示領域のみがリダイレクトされます。

HTML5ビデオリダイレクトとブラウザコンテンツリダイレクトは独立した機能です。この機能が動作するためにHTML5ビデオリダイレクトポリシーは必要ありません。ただし、Citrix HDX HTML5 Video Redirection Serviceはブラウザコンテンツリダイレクトに使用されます。詳細については、「ブラウザコンテンツリダイレクト」を参照してください。

> **注:**
>
> Web Studioで利用可能なポリシー設定は、VDA上のレジストリキーで上書きできますが、レジストリキーはオプションです。

TLSとブラウザコンテンツリダイレクト

ブラウザコンテンツリダイレクトを使用してHTTPS Webサイトをリダイレクトできます。これらのWebサイトに挿入されるJavaScriptは、VDAで実行されているCitrix HDX HTML5ビデオのリダイレクトサービス（WebSocketService.exe）へのTLS接続を確立する必要があります。このリダイレクトを実現し、WebページのTLS整合性を維持するために、Citrix HDX HTML5ビデオのリダイレクトサービスはVDAの証明書ストアに2つのカスタム証明書を生成します。

HdxVideo.jsは、セキュアWebソケットを使用して、VDA上で実行されているWebSocketService.exeと通信します。このプロセスはローカルシステム上で実行され、SSL終端とユーザーセッションマッピングを実行します。

WebSocketService.exeは、127.0.0.1ポート9001でリッスンしています。

ブラウザコンテンツリダイレクト

デフォルトでは、Citrix Workspace™アプリはクライアントフェッチとクライアントレンダリングを試行します。クライアントフェッチとクライアントレンダリングが失敗した場合、サーバー側レンダリングが試行されます。ブラウザコンテンツリダイレクトプロキシ構成ポリシーも有効にすると、Citrix Workspaceアプリはサーバーフェッチとクライアントレンダリングのみを試行します。

デフォルトでは、この設定は「許可」です。

ブラウザコンテンツリダイレクトの統合Windows認証サポート設定

ブラウザコンテンツリダイレクトは、認証にNegotiateスキームを使用するオーバーレイを有効にします。この機能強化により、VDAと同じドメイン内の統合Windows認証（IWA）で構成されたWebサーバーへのシングルサインオンが提供されます。

「**許可**」に設定すると、ブラウザーコンテンツリダイレクトオーバーレイは、ユーザーのVDA資格情報を使用してNegotiateチケットを取得します。その後、ユーザーはシングルサインオンでWebサーバーに認証します。

「**禁止**」に設定すると、ブラウザーコンテンツリダイレクトオーバーレイはVDAからNegotiateチケットを要求しません。ユーザーは基本認証方法を使用してWebサーバーに認証します。この認

証方法では、ユーザーがWebサーバーにアクセスするたびにVDA資格情報を入力する必要があります。

デフォルトでは、この設定は「禁止」です。

ブラウザーコンテンツリダイレクトサーバーフェッチWebプロキシ認証設定

この設定は、オーバーレイで発生するHTTPトラフィックをダウンストリームWebプロキシ経由でルーティングします。ダウンストリームWebプロキシは、Negotiate認証スキームを使用してVDAユーザーのドメイン資格情報によりHTTPトラフィックを承認および認証します。

ブラウザーコンテンツリダイレクトプロキシ構成ポリシーを使用して、PACファイルでサーバーフェッチモードのブラウザーコンテンツリダイレクトを構成する必要があります。PACスクリプトで、オーバーレイトラフィックをダウンストリームWebプロキシ経由でルーティングする手順を指定します。次に、ダウンストリームWebプロキシを構成して、Negotiate認証スキームを介してVDAユーザーを認証します。

「**許可**」に設定すると、Webプロキシは**Proxy-Authenticate: Negotiate**ヘッダーを含む407 Negotiateチャレンジで応答します。その後、ブラウザーコンテンツリダイレクトは、VDAユーザーのドメイン資格情報を使用してKerberosサービスチケットを取得します。また、その後のWebプロキシへの要求にはサービスチケットを含めます。

「**禁止**」に設定すると、ブラウザーコンテンツリダイレクトは、オーバーレイとWebプロキシ間のすべてのTCPトラフィックを干渉することなくプロキシします。オーバーレイは、基本認証資格情報またはその他の利用可能な資格情報を使用してWebプロキシに認証します。

デフォルトでは、この設定はProhibitedです。

ブラウザコンテンツリダイレクトACL（アクセス制御リスト）構成ポリシー設定

この設定を使用して、ブラウザーコンテンツリダイレクトを使用できる、またはブラウザーコンテンツリダイレクトへのアクセスが拒否されるURLのアクセス制御リスト（ACL）を構成します。

承認済みURLとは、コンテンツがクライアントにリダイレクトされる許可リスト内のURLです。

ワイルドカード `*` は許可されていますが、URLのプロトコルまたはドメインアドレス部分内では許可されていません。ただし、Citrix Virtual Apps and Desktops 7 2206以降では、ワイルドカード `*` はURLのサブドメインアドレス部分内で許可されています。

許可: `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`, `http://*.xyz.com/`

許可されていません: `http://*.*.com/`

URLでパスを指定することで、よりきめ細かな設定が可能です。たとえば、`https://www.xyz.com/sports/index.html`を指定した場合、index.htmlページのみがリダイレクトされます。

デフォルトでは、この設定は`https://www.youtube.com/*`に設定されています。

詳しくは、Knowledge Centerの記事CTX238236を参照してください。

> **注:**
>
> ACLを構成して、BCRがWebサイトをエンドポイントにリダイレクトすることを許可できます。また、認証サイトを構成して、構成されたURLで使用される認証のために、OktaやDuoなどのIDプロバイダー（IdP）を許可できます。

ブラウザーコンテンツリダイレクト認証サイト

この設定を使用して、URLのリストを構成します。ブラウザーコンテンツリダイレクトを使用してリダイレクトされたサイトは、このリストを使用してユーザーを認証します。この設定は、許可リスト内のURLから移動した場合に、ブラウザーコンテンツリダイレクトがアクティブ（リダイレクトされた状態）のままになるURLを指定します。

典型的なシナリオは、認証にIDプロバイダー（IdP）を使用するWebサイトです。たとえば、Webサイト`www.xyz.com`はエンドポイントにリダイレクトする必要がありますが、Okta（`www.xyz.okta.com`）のようなサードパーティのIdPが認証部分を処理します。管理者は、ブラウザーコンテンツリダイレクトACL構成ポリシーを使用して`www.xyz.com`を許可リストに追加します。次に、ブラウザーコンテンツリダイレクト認証サイトを使用して`www.xyz.okta.com`を許可リストに追加します。

詳しくは、Knowledge Centerの記事CTX238236を参照してください。

ブラウザーコンテンツリダイレクトブロックリスト設定

この設定は、ブラウザーコンテンツリダイレクトACL構成設定と連携して機能します。ブラウザーコンテンツリダイレクトACL構成設定とブロックリスト構成設定の両方にURLが存在する場合、ブロックリスト構成が優先され、URLのブラウザーコンテンツはリダイレクトされません。

未承認URL： ブロックリスト内のURLのうち、ブラウザーコンテンツがクライアントにリダイレクトされず、サーバーでレンダリングされるURLを指定します。

ワイルドカード「*」は許可されますが、プロトコルまたはURLのドメインアドレス部分内では許可されません。

許可されるもの：`http://www.xyz.com/index.html`、`https://www.xyz.com/*`、`http://www.xyz.com/*videos*`

許可されないもの：`http://*.xyz.com/`

URL にパスを指定することで、より詳細な粒度を実現できます。たとえば、`https://www.xyz.com/sports/index.html` を指定した場合、index.html のみがブロックリストに含まれます。

ブラウザコンテンツリダイレクトプロキシ設定

この設定は、ブラウザコンテンツリダイレクト用の VDA 上のプロキシ設定の構成オプションを提供します。有効なプロキシアドレスとポート番号、PAC / WPAD URL、または直接/透過設定で有効にすると、Citrix Workspace アプリはサーバーフェッチとクライアントレンダリングのみを試行します。

無効になっているか、構成されておらず、デフォルト値を使用している場合、Citrix Workspace アプリはクライアントフェッチとクライアントレンダリングを試行します。

デフォルトでは、この設定は禁止されています。

明示的なプロキシの許可パターン:

`http://<hostname/ip address\>:\<port\>`

例:

`http://proxy.example.citrix.com:80` `http://10.10.10.10:8080`

PAC/WPAD ファイルの許可パターン:

`http://<hostname/ip address>:<port>/<path>/<Proxy.pac>`

例： `http://wpad.myproxy.com:30/configuration/pac/Proxy.pac`

`https://<hostname/ip address>:<port>/<path>/<wpad.dat>`

例: `http://10.10.10.10/configuration/pac/wpad.dat`

直接または透過プロキシの許可パターン:

ポリシーテキストボックスに「**DIRECT**」と入力します。

ブラウザコンテンツリダイレクトのレジストリキーのオーバーライド

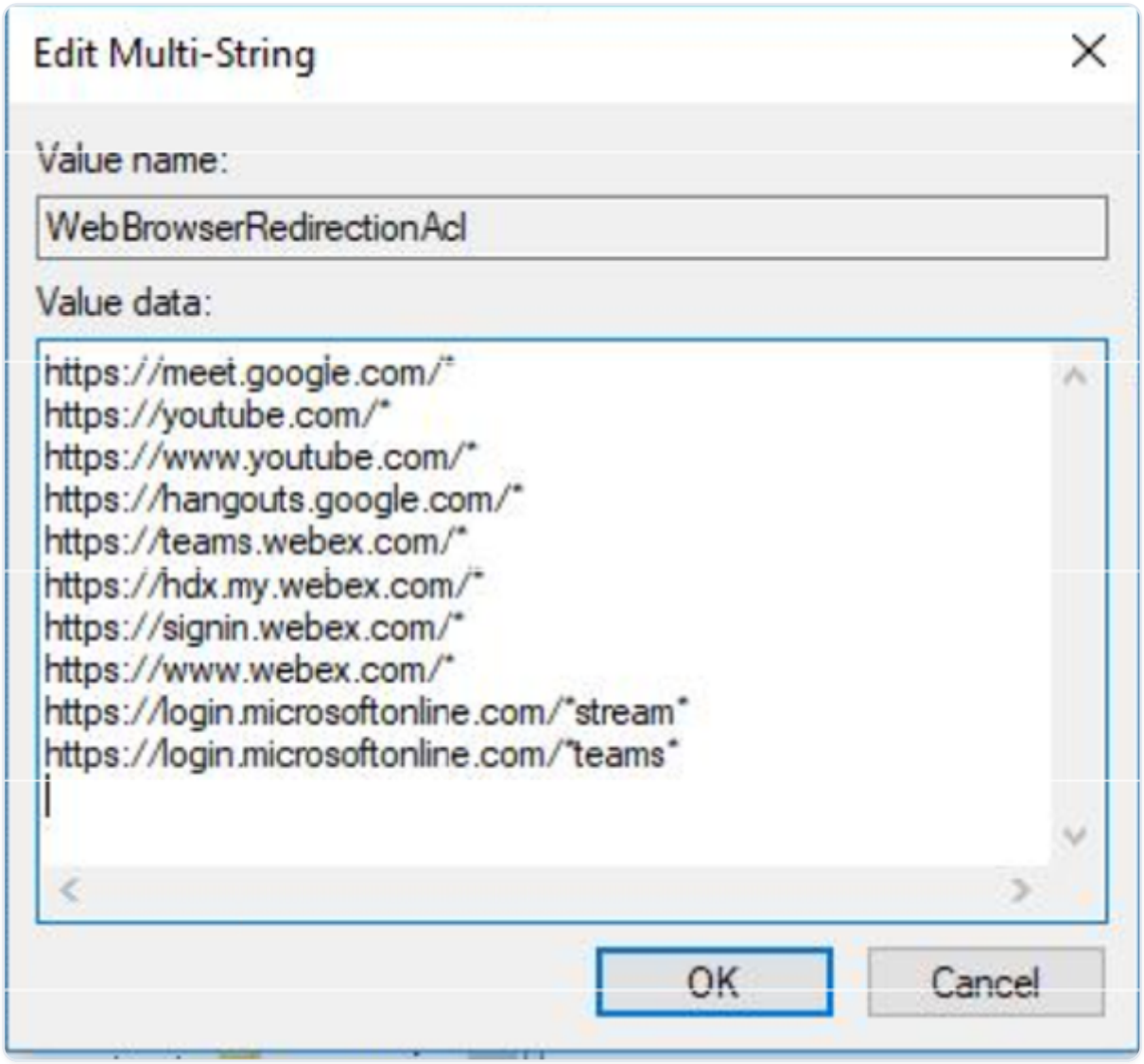
警告:

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

ポリシー設定のレジストリオーバーライドオプション:

`\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream`

名前	タイプ	値
WebBrowserRedirection	DWORD	1=許可, 0=禁止
WebBrowserRedirectionAcl	REG_MULTI_SZ	
WebBrowserRedirectionAuthenticationSites	REG_MULTI_SZ	
WebBrowserRedirectionProxyAddress	REG_SZ	`http://myproxy.citrix.com:8080` または `http://10.10.10.10:8888`
WebBrowserRedirectionBlacklist	REG_MULTI_SZ	



ブラウザコンテンツリダイレクトのためのHDXVideo.jsの挿入

ブラウザコンテンツリダイレクトの画像(/en-us/citrix-virtual-apps-desktops/2407/media/browsercontentredirectionflowchart-blacklist.png)

HdxVideo.jsは、ブラウザコンテンツリダイレクトChrome拡張機能またはInternet Explorer Browser Helper Object (BHO) を使用して、Webページに挿入されます。BHOはInternet Explorer用のプラグインモデルです。これはブラウザAPIのフックを提供し、プラグインがページのDocument Object Model (DOM) にアクセスしてナビゲーションを制御できるようにします。

BHOは、特定のページにHdxVideo.jsを挿入するかどうかを決定します。その決定は、前のフローチャートに示されている管理ポリシーに基づいています。

JavaScriptを挿入し、ブラウザコンテンツをクライアントにリダイレクトすることを決定した後、VDA上のInternet Explorerブラウザではページが空白になります。**document.body.innerHTML**を空に設定すると、VDA上のWebページの本文全体が削除されます。

ページは、クライアント上のオーバーレイブラウザ (Hdxbrowser.exe) に表示するために、クライアントに送信される準備ができています。

クライアントセンサーポリシー設定

クライアントセンサーセクションには、ユーザーセッションでモバイルデバイスのセンサー情報がどのように処理されるかを制御するためのポリシー設定が含まれています。

アプリケーションによるクライアントデバイスの物理的な位置情報の使用を許可する

この設定は、モバイルデバイス上のセッションで実行されているアプリケーションが、ユーザーデバイスの物理的な位置情報を使用できるかどうかを決定します。

デフォルトでは、位置情報の使用は禁止されています。

この設定が禁止されている場合、アプリケーションが位置情報を取得しようとすると、「アクセス拒否」の値が返されます。

この設定が許可されている場合、ユーザーはCitrix Workspace™アプリの位置情報へのアクセス要求を拒否することで、位置情報の使用を禁止できます。AndroidおよびiOSデバイスでは、各セッションで位置情報が最初に要求されたときにプロンプトが表示されます。

「アプリケーションによるクライアントデバイスの物理的な位置情報の使用を許可する」設定を使用するホスト型アプリケーションを開発する際は、以下を考慮してください。

- 位置情報が有効なアプリケーションが、位置情報が利用可能であることに依存しないようにしてください。その理由は次のとおりです。
  - ユーザーが位置情報へのアクセスを許可しない場合があります。
  - アプリケーションの実行中に、位置情報が利用できないか、変更される可能性があります。
  - ユーザーが、位置情報をサポートしていない別のデバイスからアプリケーションセッションに接続する場合があります。
- 位置情報が有効なアプリケーションは、次の要件を満たす必要があります。
  - 位置情報機能をデフォルトでオフにする。
  - アプリケーションの実行中に、ユーザーがその機能を許可または禁止するオプションを提供する。
  - アプリケーションがキャッシュする位置情報を消去するオプションをユーザーに提供します。(Citrix Workspaceアプリは位置情報をキャッシュしません。)

- 位置情報対応アプリケーションは、位置情報の粒度を管理する必要があります。この管理により、取得されたデータがアプリケーションの目的に適切であることが保証されます。また、すべての関連法域の規制に準拠します。
- 位置情報サービスを使用する際は、安全な接続 (TLSやVPNの使用など) を強制します。Citrix Workspaceアプリを信頼できるサーバーに接続します。
- 位置情報サービスの使用に関して、法的助言を得ることを検討してください。

デスクトップUIポリシー設定

デスクトップUIセクションには、デスクトップの壁紙、メニューアニメーション、ドラッグイメージなどの視覚効果を制御するポリシー設定が含まれています。これらのポリシー設定は、クライアント接続で使用される帯域幅の管理に役立ちます。帯域幅の使用を制限することで、WANでのアプリケーションパフォーマンスを向上させることができます。

> **重要:**
>
> このリリースでは、レガシーグラフィックモードとデスクトップコンポジションリダイレクト (DCR) はサポートされていません。このポリシーは、以下を使用する場合の後方互換性のためのみに含まれています。
>
> - XenApp 7.15 LTSR
> - XenDesktop 7.15 LTSR
> - Windows 7およびWindows 2008 R2を使用している以前のVDAリリース。

デスクトップコンポジションリダイレクト

この設定は、ユーザーによりスムーズなWindowsデスクトップエクスペリエンスを提供するために、ローカルのDirectXグラフィックレンダリングに以下の処理機能を使用するかどうかを指定します。

- ユーザーデバイス上のグラフィック処理ユニット（GPU）
- または、,
- ユーザーデバイス上の統合グラフィックプロセッサ（IGP）

有効にすると、**デスクトップコンポジションリダイレクト**は、サーバーの高いスケーラビリティを維持しながら、応答性の高いWindowsエクスペリエンスを提供します。

デフォルトでは、**デスクトップコンポジションリダイレクト**は無効になっています。

デスクトップコンポジションリダイレクトの選択を解除し、ユーザーセッションで必要な帯域幅を削減するには、この設定をポリシーに追加する際に**無効**を選択します。

デスクトップコンポジションリダイレクトのグラフィック品質

この設定は、デスクトップコンポジションリダイレクトに使用されるグラフィックの品質を指定します。

デフォルトは「高」です。

「高」、「中」、「低」、または「ロスレス」の品質から選択します。

デスクトップの壁紙

この設定は、ユーザーセッションでの壁紙の表示を許可または禁止します。

デフォルトでは、ユーザーセッションで壁紙を表示できます。

デスクトップの壁紙を選択解除し、ユーザーセッションで必要な帯域幅を削減するには、この設定をポリシーに追加するときに**「禁止」**を選択します。

メニューアニメーション

この設定は、ユーザーセッションでのメニューアニメーションを許可または禁止します。

デフォルトでは、メニューアニメーションは許可されています。

メニューアニメーションは、アクセシビリティのためのMicrosoftの個人設定です。有効にすると、短い遅延の後、スクロールまたはフェードインによってメニューが表示されます。メニューの下部には矢印アイコンが表示されます。その矢印をポイントするとメニューが表示されます。

このポリシー設定が**「許可」**に設定され、メニューアニメーションのMicrosoft個人設定が有効になっている場合、デスクトップでメニューアニメーションが有効になります。

> **注:**
>
> メニューアニメーションのMicrosoft個人設定への変更は、デスクトップに影響します。セッション終了時にデスクトップが変更を破棄するように設定されているとします。この場合、メニューアニメーションを有効にしているユーザーは、その後のセッションでメニューアニメーションを利用できない可能性があります。メニューアニメーションを必要とするユーザーの場合は、デスクトップのメインイメージでMicrosoft設定を有効にするか、デスクトップがユーザーの変更を保持するようにしてください。

ドラッグ中のウィンドウの内容の表示

この設定は、画面上でウィンドウをドラッグしているときに、ウィンドウの内容の表示を許可または禁止します。

デフォルトでは、ウィンドウの内容の表示は許可されています。

許可に設定すると、ウィンドウをドラッグしたときにウィンドウ全体が移動するように見えます。**禁止**に設定すると、ドロップするまでウィンドウの輪郭のみが移動するように見えます。

ファイルリダイレクトポリシー設定

「**ファイルリダイレクト**」セクションには、クライアントドライブマッピングとクライアントドライブ最適化に関連するポリシー設定が含まれています。

クライアントドライブの自動接続

この設定は、ユーザーがログオンしたときのクライアントドライブの自動接続を許可または禁止します。

デフォルトでは、自動接続は許可されています。

この設定をポリシーに追加する際は、自動接続したいドライブタイプの関連設定を有効にしてください。たとえば、ユーザーのCD-ROMドライブの自動接続を許可するには、この設定と「**クライアント光学ドライブ**」設定を構成します。

関連するポリシー設定は次のとおりです。

- **クライアントドライブリダイレクト**
- **クライアントフロッピーディスクドライブ**
- **クライアント光学ドライブ**
- **クライアント固定ドライブ**
- **クライアントネットワークドライブ**
- **クライアントリムーバブルドライブ**

クライアントドライブリダイレクト

この設定は、ユーザーデバイス上のドライブとの間でファイルリダイレクトを有効または無効にします。

既定では、ファイルリダイレクトは有効になっています。

> **注:**
>
> クライアントドライブリダイレクトポリシー設定は、汎用USBリダイレクトを使用してセッションにマップされたドライブには適用されません。

> 有効にすると、ユーザーはすべてのクライアントドライブにファイルを保存できます。無効にすると、すべてのファイルリダイレクトが防止されます。この構成は、個々のファイルリダイレクト設定の状態に関係なく適用されます。個々のファイルリダイレクト設定には、クライアントフロッピードライブとクライアントネットワークドライブが含まれます。

関連するポリシー設定は次のとおりです。

- **クライアントフロッピードライブ**
- **クライアント光学ドライブ**
- **クライアント固定ドライブ**
- **クライアントネットワークドライブ**
- **クライアントリムーバブルドライブ**

クライアント固定ドライブ

この設定は、ユーザーがユーザーデバイス上の固定ドライブにアクセスしたりファイルを保存したりすることを許可または禁止します。

既定では、クライアント固定ドライブへのアクセスは許可されています。

この設定をポリシーに追加するときは、**クライアントドライブリダイレクト**設定が存在し、許可に設定されていることを確認してください。これらの設定が無効になっている場合、クライアント固定ドライブはマップされず、**クライアント固定ドライブ**設定の状態に関係なく、ユーザーはこれらのドライブに手動でアクセスできません。

ユーザーがログオンしたときに固定ドライブが自動的に接続されるように、**クライアントドライブの自動接続**設定を構成します。

クライアント フロッピー ドライブ

この設定は、ユーザーがユーザーデバイス上のフロッピー ドライブにファイルにアクセスしたり保存したりすることを許可または禁止します。

デフォルトでは、クライアントフロッピー ドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合、**クライアント ドライブ リダイレクト**設定が存在し、「許可」に設定されていることを確認してください。これらの設定が無効になっている場合、**クライアント フロッピー ドライブ**設定の状態にかかわらず、クライアントフロッピー ドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。

ユーザーがログオンするときにフロッピー ドライブが自動的に接続されるようにするには、**クライアント ドライブの自動接続**設定を構成します。

クライアント ネットワーク ドライブ

この設定は、ユーザーがユーザーデバイスを介してネットワーク (リモート) ドライブにファイルにアクセスしたり保存したりすることを許可または禁止します。

デフォルトでは、クライアント ネットワーク ドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合、**クライアント ドライブ リダイレクト**設定が存在し、「許可」に設定されていることを確認してください。これらの設定が無効になっている場合、クライアント ネットワーク ドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、**クライアント ネットワーク ドライブ**設定の状態にかかわらず適用されます。

ユーザーがログオンするときにネットワーク ドライブが自動的に接続されるようにするには、**クライアント ドライブの自動接続**設定を構成します。

クライアント 光学ドライブ

この設定は、ユーザーが次の場所にファイルにアクセスしたり保存したりすることを許可または禁止します。

- ユーザーデバイス上のCD-ROM
- ユーザーデバイス上のDVD-ROM
- ユーザーデバイス上のBD-ROM ドライブ。

デフォルトでは、クライアント光学ドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合は、**Client drive redirection** 設定が存在し、**Allowed** に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントの光学ドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、**Client optical drives** 設定の状態に関係なく適用されます。

ユーザーがログオンしたときに光学ドライブが自動的に接続されるようにするには、**Auto connect client drives** 設定を構成します。

クライアントリムーバブルドライブ

この設定により、ユーザーはユーザーデバイス上のUSBドライブへのファイルアクセスまたは保存を許可または禁止されます。

デフォルトでは、クライアントリムーバブルドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合は、**Client drive redirection** 設定が存在し、Allowed に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントのリムーバブルドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、**Client removable drives** 設定の状態に関係なく適用されます。

ユーザーがログオンしたときにリムーバブルドライブが自動的に接続されるようにするには、**Auto connect client drives** 設定を構成します。

ホストからクライアントへのリダイレクト

この設定は、URLおよび一部のメディアコンテンツのファイルタイプ関連付けを有効または無効にし、ユーザーデバイスで開かれるようにします。無効にすると、コンテンツはサーバーで開かれます。

デフォルトでは、ファイルタイプ関連付けは無効になっています。

この設定を有効にすると、以下のURLタイプがローカルで開かれます。

- HTTP
- HTTPS
- リアルプレーヤーおよびQuickTime (RTSP)
- リアルプレーヤーおよびQuickTime (RTSPU)
- レガシーReal Player (PNM)
- マイクロソフト メディア サーバー (MMS)

クライアントドライブ文字の保持

この設定は、セッション内でクライアントドライブを同じドライブ文字にマップすることを有効または無効にします。

デフォルトでは、クライアントドライブ文字は保持されません。

この設定をポリシーに追加する場合は、**クライアントドライブのリダイレクト**設定が存在し、許可に設定されていることを確認してください。

読み取り専用クライアントドライブアクセス

この設定は、ユーザーとアプリケーションが以下の操作を行うことを許可または禁止します。

- マップされたクライアントドライブ上にファイルを作成する
- マップされたクライアントドライブ上のファイルを変更する
- マップされたクライアントドライブ上のフォルダーを変更する

デフォルトでは、マップされたクライアントドライブ上のファイルとフォルダーは変更できます。

有効に設定すると、ファイルとフォルダーは読み取り専用のアクセス許可でアクセスできます。

この設定をポリシーに追加する場合は、**クライアントドライブのリダイレクト**設定が存在し、許可に設定されていることを確認してください。

特殊フォルダーのリダイレクト

この設定は、Citrix Workspace™アプリおよびWeb Interfaceのユーザーが、セッションからローカルのドキュメントおよびデスクトップの特殊フォルダーを表示することを許可または禁止します。

デフォルトでは、特殊フォルダーのリダイレクトは許可されています。

この設定は、ポリシーによってフィルタリングされたオブジェクトが特殊フォルダーのリダイレクトを持つことを防ぎます。これは、他の場所に存在する設定に関係なく適用されます。この設定が禁止されている場合、StoreFront™、Web Interface、またはCitrix Workspaceアプリに指定されている関連設定はすべて無視されます。

特殊フォルダーのリダイレクトを許可するユーザーを定義するには、**許可**を選択し、この設定を、この機能を適用したいユーザーにフィルタリングされたポリシーに含めます。この設定は、他のすべての特殊フォルダーのリダイレクト設定を上書きします。

ユーザーがローカルハードドライブへのファイルアクセスや保存を禁止するポリシー設定は、特殊フォルダーのリダイレクトが機能することも防ぎます。この状況は、特殊フォルダーのリダイレクトがユーザーデバイスと対話する必要があるために発生します。

この設定をポリシーに追加する際は、**クライアント固定ドライブ**設定が存在し、「許可」に設定されていることを確認してください。

ファイル転送ポリシー

デフォルトでは、ファイル転送は有効になっています。これらのポリシーを変更するには、Web Studioの**ユーザー設定 - ICA\ファイルリダイレクト**にある設定を使用します。ファイル転送ポリシーを使用する際は、以下を考慮してください。

- **Chrome OS/HTML5向けCitrix Workspaceアプリのファイル転送** - ユーザーがCitrix Virtual Apps and Desktopsセッションとデバイス間でファイルを転送することを許可または禁止します。
- **Chrome OS/HTML5向けCitrix Workspaceアプリのファイルアップロード** - ユーザーがデバイスからCitrix Virtual Apps and Desktopsセッションにファイルをアップロードすることを許可または禁止します。
- **Chrome OS/HTML5向けCitrix Workspaceアプリのファイルダウンロード** - ユーザーがCitrix Virtual Apps and Desktopsセッションからデバイスにファイルをダウンロードすることを許可または禁止します。

> **注:**
>
> ファイル転送ポリシーは、HTML5向けCitrix WorkspaceアプリおよびChrome OS向けCitrix Workspaceアプリにのみ適用されます。

非同期書き込みを使用する

この設定は、非同期ディスク書き込みを有効または無効にします。

デフォルトでは、非同期書き込みは無効になっています。

非同期ディスク書き込みは、比較的高い帯域幅と高い遅延が特徴であるWAN経由でのファイル転送速度とクライアントディスクへの書き込み速度を向上させることができます。ただし、接続またはディスクに障害が発生した場合、書き込み中のクライアントファイルが未定義の状態になる可能性があります。この未定義の状態が発生した場合、ポップアップウィンドウで影響を受けるファイルがユーザーに通知されます。ユーザーは、再接続時またはディスク障害が修正されたときに中断されたファイル転送を再開するなどの是正措置を講じることができます。

Citrix®は、リモート接続を必要とし、良好なファイルアクセス速度を持ち、接続またはディスク障害が発生した場合に失われたファイルやデータを容易に回復できるユーザーに対してのみ、非同期ディスク書き込みを有効にすることを推奨します。

この設定をポリシーに追加する際は、**クライアントドライブリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。この設定が無効になっている場合、非同期書き込みは行われません。

グラフィックポリシー設定

グラフィックセクションには、ユーザーセッションで画像がどのように処理されるかを制御するためのポリシー設定が含まれています。

視覚的にロスレスな圧縮を許可する

この設定により、グラフィックで真のロスレス圧縮の代わりに視覚的にロスレスな圧縮を使用できます。視覚的にロスレスな圧縮は、真のロスレス圧縮よりもパフォーマンスが向上しますが、目には認識できないわずかな損失があります。この設定は、視覚品質設定の値の使用方法を変更します。

デフォルトでは、この設定は無効になっています。

グラフィックステータスインジケーター

この設定は、グラフィックステータスインジケーターがユーザーセッションで実行されるように構成します。このツールを使用すると、ユーザーはアクティブなグラフィックモードに関する情報を確認できます。この情報には、ビデオコーデック、ハードウェアエンコード、画質、およびセッションで使用中のモニターに関する詳細が含まれます。グラフィックステータスインジケーターを使用すると、ユーザーはピクセルパーフェクトモードを有効または無効にすることもできます。

Citrix Virtual Apps and Desktops™ 2103以降のリリースには、画質とインタラクティブ性の適切なバランスをユーザーが見つけるのに役立つ画質スライダーが含まれています。

Citrix Virtual Apps and Desktops 2109以降のリリースには、グラフィックステータスインジケーターを使用して起動されるユーザーインターフェイスを介して仮想ディスプレイレイアウトを構成する機能が含まれています。

グラフィックステータスインジケーターは、以前のバージョンのロスレスインジケーターツールを置き換えます。このポリシーは、Citrix Virtual Apps and Desktopsバージョン7.16から1809までのでロスレスインジケーターを有効にします。

画面共有

この設定により、ユーザーは画面コンテンツ、キーボード、マウスを含むセッションを他のユーザーと共有できます。

デフォルトでは、この設定は無効になっています。

VDAは、TCPポート範囲のポートを使用してデータを交換しようとします。これは、最も低いポートから始まり、その後の接続ごとに増分されます。このポートは、インバウンドトラフィックとアウトバウンドトラフィックの両方を処理します。

デフォルトでは、TCPポート範囲は52525-52625に設定されています。

画面共有に使用されるポートは、ファイアウォールの例外リストに追加する必要があります。このオプションは、VDA のインストール時にチェックボックスとして表示されます。デフォルトでは、このオプションはチェックされていません。

ディスプレイメモリ制限

この設定は、セッションの最大ビデオバッファサイズをキロバイト単位で指定します。

デフォルトでは、ディスプレイメモリ制限は 65,536 キロバイトです。

セッションの最大ビデオバッファサイズをキロバイト単位で指定します。128 から 4,194,303 までのキロバイト単位の量を指定します。最大値 4,194,303 はディスプレイメモリを制限しません。デフォルトでは、ディスプレイメモリは 65,536 キロバイトです。接続により多くの色深度と高い解像度を使用するには、より多くのメモリが必要です。レガシーグラフィックモードでは、メモリ制限に達すると、「ディスプレイモードの劣化設定」に従ってディスプレイが劣化します。

より多くの色深度と高い解像度を必要とする接続の場合、制限を増やします。次の式を使用して、必要な最大メモリを計算します。

メモリ深度（バイト）= (1ピクセルあたりのビット単位の色深度 / 8) x (ピクセル単位の垂直解像度) x (ピクセル単位の水平解像度)。

たとえば、色深度 32、垂直解像度 600、水平解像度 800 のシナリオを考えます。この場合、必要な最大メモリは (32 / 8) x (600) x (800) = 1920000 バイトとなり、ディスプレイメモリ制限は 1920 KB になります。

32 ビット以外の色深度は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ利用できます。

HDX™ は、各セッションに必要なディスプレイメモリの量のみを割り当てます。したがって、一部のユーザーのみがデフォルトよりも多くを必要とする場合でも、ディスプレイメモリ制限を増やしてもスケーラビリティに悪影響はありません。

ディスプレイモードの劣化設定

> **注：**

> Virtual Delivery Agent 7.x の場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> セッションのディスプレイメモリ制限に達した場合、この設定は色深度と解像度のどちらが先に劣化するかを指定します。

デフォルトでは、色深度が先に劣化します。

セッションのメモリ制限に達すると、表示される画像の品質を下げることができます。この品質は、最初に色深度と解像度のどちらを低下させるかを選択することで下げられます。色深度が最初に低下すると、表示される画像はより少ない色を使用します。解像度が最初に低下すると、表示される画像は1インチあたりのピクセル数が少なくなります。

色深度または解像度が低下したときにユーザーに通知するには、「表示モードが低下したときにユーザーに通知」設定を構成します。

動的ウィンドウプレビュー

この設定は、シームレスウィンドウの表示を有効または無効にします。

- フリップ-
- フリップ 3D
- タスクバープレビュー
- Windows ピーク

WINDOWS AEROプレビューオプション	説明
タスクバープレビュー	ユーザーがウィンドウのタスクバーアイコンにカーソルを合わせると、そのウィンドウの画像がタスクバーの上に表示されます。
Windows ピーク	ユーザーがタスクバープレビュー画像にカーソルを合わせると、ウィンドウのフルサイズの画像が画面に表示されます。
フリップ	ユーザーがALT+TABを押すと、開いている各ウィンドウの小さなプレビューアイコンが表示されます。

WINDOWS AEROプレビューオプション	説明
フリップ 3D	ユーザーがTAB+Windowsロゴキーを押すと、開いているウィンドウの大きな画像が画面全体にカスケード表示されます。

デフォルトでは、この設定は有効になっています。

イメージキャッシュ

> **注:**
>
> Virtual Delivery Agent 7.x の場合、このポリシー設定は、レガシーグラフィックモードのポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、セッション内の画像のセクションのキャッシュと取得を有効または無効にします。画像をセクションにキャッシュし、必要に応じてこれらのセクションを取得すると、次のことが可能になります。

- ユーザーデバイスでのスクロールがよりスムーズになる
- ユーザーデバイスでネットワーク経由で送信されるデータ量を削減する
- ユーザーデバイスで必要な処理を削減する

デフォルトでは、画像キャッシュ設定は有効になっています。

> **注:**
>
> 画像キャッシュ設定は、画像がどのようにキャッシュされ、取得されるかを制御します。この設定は、画像がキャッシュされるかどうかを制御するものではありません。画像は、レガシーグラフィックモード設定が有効になっている場合にキャッシュされます。

レガシーグラフィックモード - サポートされていません。下位互換性のためのみ

> **重要:**

> このリリースでは、レガシーグラフィックモードおよびデスクトップコンポジションリダイレクト (DCR) はサポートされていません。このポリシーは、XenApp 7.15 LTSR、XenDesktop 7.15 LTSR、およびWindows 7とWindows 2008 R2を使用する以前のVDAリリースとの下位互換性のためにのみ含まれています。

> この設定は、リッチグラフィックエクスペリエンスを無効にします。この設定を使用してレガシーグラフィックエクスペリエンスに戻し、WANまたはモバイル接続での帯域幅の消費を削減します。XenAppおよびXenDesktop 7.13で導入された帯域幅の削減により、このモードは廃止されました。

デフォルトでは、この設定は無効になっており、ユーザーにはリッチグラフィックエクスペリエンスが提供されます。

レガシーグラフィックモードは以下でサポートされています:

- ウィンドウズ 7
- ウィンドウズ サーバー 2008 R2 VDA。

レガシーグラフィックモードは以下ではサポートされていません:

- Windows 8.xおよび10
- Windows Server 2012、2012 R2、および2016。

XenAppおよびXenDesktop 7.6 FP3以降でのグラフィックモードとポリシーの最適化については、CTX202687を参照してください。

最大許容色深度

> **注:**

> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、セッションで許可される最大色深度を指定します。

デフォルトでは、許可される最大色深度は1ピクセルあたり32ビットです。

この設定は、Thinwireドライバーと接続にのみ適用されます。プライマリディスプレイドライバーとしてThinWire以外のドライバーを使用するVDAには適用されません。これらのVDAは、

Windows Display Driver Model (WDDM) ドライバーをプライマリディスプレイドライバーとして使用するVDAです。Windows 8などのWDDMドライバーをプライマリディスプレイドライバーとして使用するシングルセッションOS VDAの場合、この設定は効果がありません。Windows Server 2019などのWDDMドライバーを使用するWindowsマルチセッションOS VDAの場合、この設定によりユーザーがVDAに接続できなくなる可能性があります。

高い色深度を設定すると、より多くのメモリが必要になります。メモリ制限に達したときに色深度を低下させるには、**表示モードの低下設定**を構成します。色深度が低下すると、表示される画像はより少ない色を使用します。

表示モードが低下したときにユーザーに通知する

> **注:**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、色深度または解像度が低下したときに、ユーザーに簡単な説明を表示します。

デフォルトでは、ユーザーへの通知は無効になっています。

3Dグラフィックワークロード向けに最適化

この設定は、グラフィックを多用するワークロードに最適なデフォルト設定を構成します。グラフィックを多用するアプリケーションにワークロードが集中しているユーザーに対して、この設定を有効にします。このポリシーは、セッションでGPUが利用可能な場合にのみ適用してください。このポリシーによって設定されたデフォルト設定を明示的に上書きする他の設定は、優先されます。

デフォルトでは、3Dグラフィックワークロード向けに最適化する設定は無効になっています。

キューイングとトッシング

> **注:**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、別の画像に置き換えられたキュー内の画像を破棄します。

デフォルトでは、キューイングとトッシングは有効になっています。

この設定は、グラフィックがユーザーデバイスに送信される際の応答を改善します。この設定を構成すると、フレームがドロップされるため、アニメーションが途切れることがあります。

圧縮にビデオコーデックを使用する

エンドポイントでビデオデコードが利用可能な場合、グラフィックの圧縮にビデオコーデックの使用を許可します。**画面全体に適用**が選択されている場合、ビデオコーデックはすべてのデフォルトコーデックとして適用されます。**アクティブに変更される領域に適用**が選択されている場合、ビデオコーデックは画面上で常に変化する領域に使用され、その他のデータは静止画圧縮とビットマップキャッシュを使用します。エンドポイントでビデオデコードが利用できない場合、または**ビデオコーデックを使用しない**を指定した場合、静止画圧縮とビットマップキャッシュの組み合わせが使用されます。**推奨時に使用**が選択されている場合、システムはさまざまな要因に基づいて選択します。選択方法が強化されるにつれて、結果はバージョン間で異なる場合があります。

推奨時に使用を選択すると、システムが現在のシナリオに最適な設定を選択するために最善を尽くすことができます。

画面全体に適用を選択すると、特にサーバーレンダリングされたビデオや3Dグラフィックを多用する場合に、ユーザーエクスペリエンスと帯域幅の向上に最適化されます。

アクティブに変更される領域に適用を選択すると、特に低帯域幅でビデオパフォーマンスが向上するように最適化され、静的およびゆっくりと変化するコンテンツのスケーラビリティを維持できます。この設定はマルチモニター展開でサポートされています。

ビデオコーデックを使用しないを選択すると、サーバーのCPU負荷、および多数のサーバーレンダリングされたビデオやその他のグラフィックを多用するアプリケーションがない場合に最適化されます。

デフォルトは**推奨時に使用**です。

ビデオにハードウェアエンコーディングを使用する

この設定により、利用可能な場合、グラフィックハードウェアを使用して画面要素をビデオコーデックで圧縮できます。そのようなハードウェアが利用できない場合、VDAはソフトウェアビデオコーデックを使用したCPUベースのエンコーディングにフォールバックします。

このポリシー設定のデフォルトオプションは**有効**です。

複数のモニターがサポートされています。

ビデオデコードをサポートするCitrix Workspace™アプリは、ハードウェアエンコーディングで使用できます。

NVIDIA

NVIDIA GRID GPUの場合、ハードウェアエンコードはマルチセッションOSおよびシングルセッションOS用VDAでサポートされています。

NVIDIA GPUはNVENCハードウェアエンコードをサポートしている必要があります。サポートされているGPUのリストについては、NVIDIAビデオコーデックSDKを参照してください。

NVIDIA GRIDにはドライバーバージョン3.1以降が必要です。NVIDIA Quadroにはドライバーバージョン362.56以降が必要です。CitrixはNVIDIA Release R361ブランチのドライバーを推奨します。

ロスレステキストはNVENCハードウェアエンコードと互換性がありません。ロスレステキストを有効にした場合、ロスレステキストがNVENCハードウェアエンコードよりも優先されます。

アクティブに変化する領域に対するH.264ハードウェアコーデックの選択的な使用がサポートされています。

視覚的にロスレス（YUV 4:4:4）圧縮がサポートされています。視覚的にロスレス（グラフィックポリシー設定、視覚的にロスレスな圧縮を許可）には、Citrix Workspaceアプリ1808以降またはCitrix Receiver for Windows 4.5以降が必要です。

インテル

Intel Iris Proグラフィックプロセッサの場合、ハードウェアエンコードはシングルセッションOSおよびマルチセッションOS用VDAでサポートされています。

Intel Broadwellプロセッサファミリー以降のIntel Iris Proグラフィックプロセッサがサポートされています。Intel Remote Displays SDKバージョン1.0が必要であり、IntelのWebサイトからダウンロードできます: Remote Displays SDK。

ロスレステキストは、ビデオコーデックポリシーが画面全体に設定されており、**3Dグラフィックワークロードの最適化**ポリシーが無効になっている場合にのみサポートされます。

視覚的にロスレス（YUV 4:4:4）はサポートされていません。

Intelエンコーダーは、最大8つのエンコードセッション（たとえば、1人のユーザーが8台のモニターを使用する場合、または8人のユーザーがそれぞれ1台のモニターを使用する場合）で良好なユーザーエクスペリエンスを提供します。8つを超えるエンコードセッションが必要な場合は、仮想マシンが接続するモニターの数を確認してください。管理者は、良好なユーザーエクスペリエンスを維持するために、このポリシー設定をユーザーごとまたはマシンごとに構成するかどうかを決定します。

AMD

AMDの場合、ハードウェアエンコードはシングルセッションOS用VDAでサポートされています。

AMD GPUはRapidFire SDKをサポートする必要があります。例えば、AMD Radeon ProまたはFirePro GPUなどです。

エンコードを機能させるには、最新のAMDドライバーをインストールしてください。これらのドライバーは`<https://www.amd.com/en/support>`からダウンロードできます。

ロスレステキストはAMDハードウェアエンコードと互換性がありません。ロスレステキストを有効にした場合、ロスレステキストがAMDハードウェアエンコードよりも優先されます。

活発に変化する領域向けのH.264ハードウェアコーデックの選択的な使用がサポートされています。

キャッシュポリシー設定

このセクションには、クライアント接続の帯域幅が制限されている場合に、ユーザーデバイスで画像データをキャッシュできるようにするポリシー設定が含まれています。

永続キャッシュしきい値

注: Virtual Delivery Agent 7.xの場合、このポリシー設定は、**レガシーグラフィックモード**ポリシー設定が有効になっている場合にのみ適用されます。

この設定は、ユーザーデバイスのハードドライブにビットマップをキャッシュし、以前のセッションからの大きく頻繁に使用される画像を再利用できるようにします。

デフォルトでは、しきい値は1秒あたり3000000ビットです。

しきい値は、永続キャッシュ機能が有効になる下限を表します。たとえば、デフォルト値を使用すると、帯域幅が3000000 bpsを下回ったときに、ビットマップがユーザーデバイスのハードドライブにキャッシュされます。

Framehawkポリシー設定

> **重要:**
>
> Citrix Virtual Apps and Desktops 7 1903以降、Framehawk はサポートされなくなりました。代わりに、Thinwireをアダプティブトランスポートを有効にして使用してください。

> **Framehawk**セクションには、サーバー上でFramehawkディスプレイチャネルを有効にして構成するポリシー設定が含まれています。

FRAMEHAWKディスプレイチャネル

有効にすると、サーバーはユーザーのグラフィックと入力のリモート処理にFramehawkディスプレイチャネルを使用しようとします。このディスプレイチャネルは、UDPを使用して、損失と遅延の特性が高いネットワークでより良いユーザーエクスペリエンスを提供します。ただし、他のグラフィックモードよりも多くのサーバーリソースと帯域幅を使用する可能性があります。

デフォルトでは、Framehawkディスプレイチャネルは無効になっています。

FRAMEHAWKディスプレイチャネルのポート範囲

このポリシー設定は、VDAがユーザーデバイスとFramehawkディスプレイチャネルデータを交換するために使用するUDPポート番号の範囲を指定します。ポート番号は、*最小ポート番号または最大ポート番号*の形式です。VDAは、最小ポート番号から開始し、その後の各試行でインクリメントしながら、各ポートを使用しようとします。このポートは、インバウンドおよびアウトバウンドトラフィックを処理します。

デフォルトでは、ポート範囲は3224,3324です。

キープアライブ ポリシー設定

キープアライブセクションには、ICA®キープアライブメッセージを管理するためのポリシー設定が含まれています。

ICA キープアライブ タイムアウト

この設定は、連続するICAキープアライブメッセージ間の秒数を指定します。

デフォルトでは、キープアライブメッセージの間隔は60秒です。

ICAキープアライブメッセージを送信する1～3600秒の間隔を指定します。ネットワーク監視ソフトウェアが非アクティブな接続を閉じる役割を担っている場合は、この設定を構成しないでください。

ICA キープアライブメッセージ

この設定は、ICAキープアライブメッセージの定期的な送信を有効または無効にします。

デフォルトでは、キープアライブメッセージは送信されません。

この設定を有効にすると、切断された接続が切断されるのを防ぎます。サーバーがアクティビティを検出しない場合、この設定はリモートデスクトップサービス (RDS) がセッションを切断するのを防ぎます。サーバーは数秒ごとにキープアライブメッセージを送信して、セッションがアクティ

ブであるかどうかを検出します。セッションがアクティブでなくなった場合、サーバーはセッションを切断済みとしてマークします。

セッションの信頼性を使用している場合、ICAキープアライブは機能しません。ICAキープアライブは、セッションの信頼性を使用していない接続に対してのみ構成してください。

関連するポリシー設定: セッションの信頼性接続。

ローカルアプリアクセス ポリシー設定

ローカルアプリアクセスセクションには、ユーザーのローカルにインストールされたアプリケーションをホストされたアプリケーションで管理するポリシー設定が含まれています。これらのポリシー設定は、ホストされたデスクトップ環境での統合を管理します。

ローカルアプリアクセスを許可

この設定は、ユーザーのローカルにインストールされたアプリケーションとホストされたアプリケーションの統合を許可または禁止します。これらのポリシー設定は、ホストされたデスクトップ環境での統合を管理します。

ユーザーがローカルにインストールされたアプリケーションを起動すると、そのアプリケーションは仮想デスクトップ内で実行されているように見えますが、実際にはローカルで実行されています。

ローカルアプリアクセスを許可ポリシー設定を**有効**にすると、ブラウザコンテンツリダイレクトはサポートされず、デスクトップセッションにクライアント側の通知領域のバッテリーステータスは表示されません。

デフォルトでは、**ローカルアプリアクセスを許可**は禁止されています。

URLリダイレクトブロックリスト

この設定は、ローカルWebブラウザにリダイレクトされて起動されるWebサイトを指定します。これらのWebサイトには、次のものが含まれる場合があります。

- msn.comやnewsgoogle.comなど、ロケール情報を必要とするWebサイト
- ユーザーデバイスでより適切にレンダリングされるリッチメディアコンテンツを含むWebサイト。

デフォルトでは、サイトは指定されていません。

URLリダイレクト許可リスト

この設定は、起動された環境でレンダリングされるWebサイトを指定します。

デフォルトでは、サイトは指定されていません。

モバイルエクスペリエンスポリシー設定

「**モバイルエクスペリエンス**」セクションには、Citrix Mobility Packを処理するためのポリシー設定が含まれています。

キーボードの自動表示

この設定は、モバイルデバイスの画面でのキーボードの自動表示を有効または無効にします。

デフォルトでは、キーボードの自動表示は無効になっています。

タッチ最適化デスクトップの起動

この設定は無効になっており、Windows 10またはWindows Server 2016マシンでは使用できません。

この設定は、Citrix Workspace™アプリの全体的なインターフェイス動作を決定します。この設定により、タブレットデバイス向けに最適化されたタッチフレンドリーなインターフェイスの使用を許可または禁止します。

デフォルトでは、タッチフレンドリーなインターフェイスが使用されます。

Windowsインターフェイスのみを使用するには、このポリシー設定を「禁止」に設定します。

コンボボックスのリモート化

この設定は、モバイルデバイスのセッションで表示できるコンボボックスの種類を決定します。このポリシー設定を「許可」に設定すると、デバイスネイティブのコンボボックスコントロールが表示されます。この設定が許可されている場合、ユーザーはCitrix Workspace app for iOSセッション設定を変更して、Windowsコンボボックスを使用できます。

デフォルトでは、**コンボボックスのリモート化**機能は禁止されています。

マルチメディアポリシー設定

マルチメディアセクションには、ユーザーセッションにおけるストリーミングHTML5およびWindowsのオーディオとビデオを管理するためのポリシー設定が含まれています。

> **警告**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤った

> 使用によって生じる問題が解決できることを保証できません。レジストリエディターの使用は自己責任で行ってください。編集する前に必ずレジストリをバックアップしてください。

マルチメディアポリシー

デフォルトでは、Delivery Controller™で設定されたすべてのマルチメディアポリシーは、以下のレジストリに保存されます。

マシンポリシー:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies

ユーザーポリシー:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix{ユーザーセッションID}\User\MultimediaPolicies

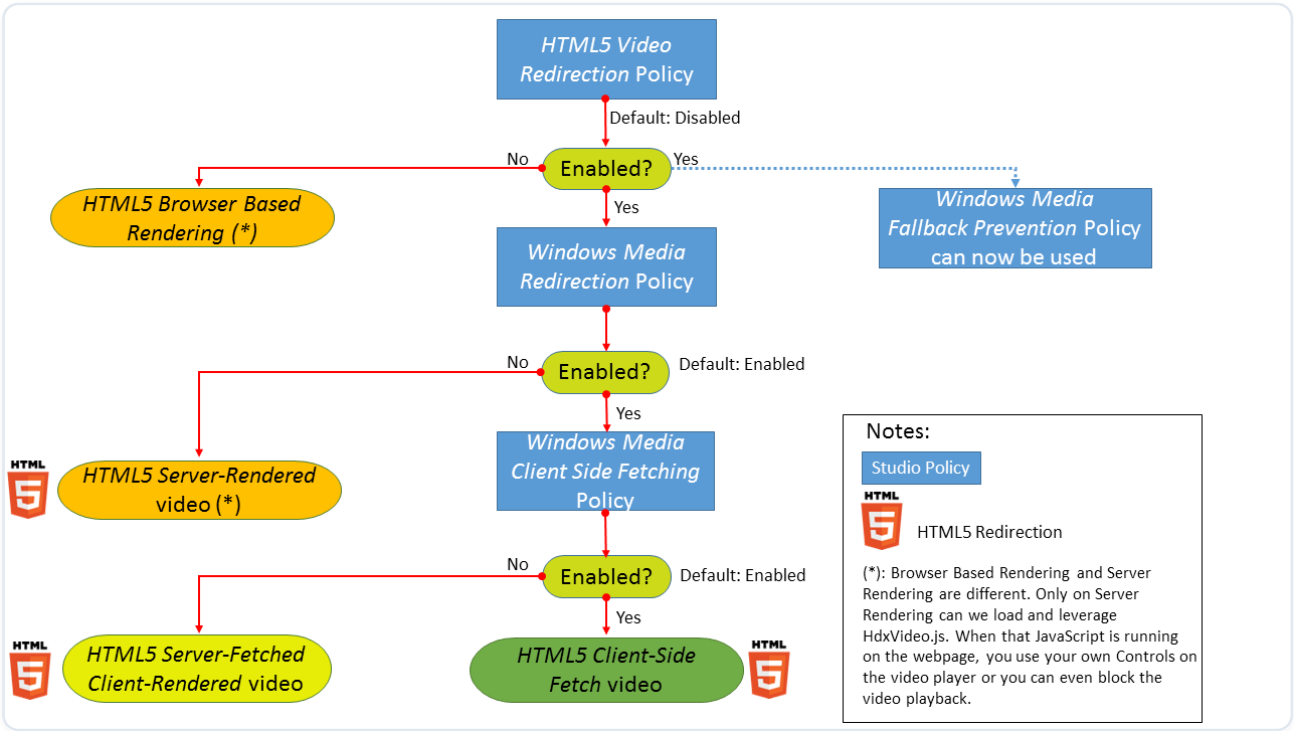
現在のユーザーセッションIDを見つけるには、Windowsコマンドラインで**qwinsta**コマンドを発行します。

HTML5ビデオのリダイレクト

Citrix Virtual Apps and Desktops™サーバーがHTML5マルチメディアWebコンテンツをユーザーに配信する方法を制御し、最適化します。

デフォルトでは、この設定は無効になっています。

HTML5リダイレクトのグラフィックイメージ



このリリースでは、この機能は制御されたWebページでのみ利用可能です。HTML5マルチメディアコンテンツが利用可能なWebページ（例: 社内トレーニングサイトのビデオ）にJavaScriptを追加する必要があります。

HTML5ビデオリダイレクトを構成するには:

1. VDAインストール上の%Program Files%/Citrix/ICA Service/HTML5 Video Redirectionからファイル**HdxVideo.js**を社内Webページの場所にコピーします。
2. この行をWebページに挿入します（Webページに他のスクリプトがある場合は、それらのスクリプトの前に**HdxVideo.js**を含めます）。 `<script src="HdxVideo.js" type="text/javascript"\></script>`

注: HdxVideo.jsがWebページと同じ場所にない場合は、**src**属性を使用してその完全なパスを指定します。

JavaScriptが管理対象のWebページに追加されておらず、ユーザーがHTML5ビデオを再生する場合を考えてみましょう。この場合、Citrix Virtual Apps and Desktopsはサーバー側レンダリングにデフォルト設定されます。

HTML5ビデオのリダイレクトを機能させるには、***Windows Media Redirection***を許可します。このポリシーは、Server Fetch Client Renderには必須であり、Client Side Fetchingには必要です。Client Side Fetchingは、さらに*Windows Media client-side content fetching*も許可されている必要があります。

Microsoft Edgeはこの機能をサポートしていません。

HdxVideo.jsは、ブラウザのHTML5プレーヤーコントロールを独自のコントロールに置き換えます。特定のWebサイトでHTML5ビデオリダイレクトポリシーが有効になっていることを確認するには、プレーヤーコントロールを**HTML5ビデオリダイレクト**ポリシーが禁止されているシナリオと比較します。

（ポリシーが許可されている場合のCitrixカスタムコントロール）



（ポリシーが禁止されているか、構成されていない場合のネイティブWebページコントロール）



次のビデオコントロールがサポートされています。

- 再生

- 一時停止
- シーク
- 繰り返し
- オーディオ
- 全画面表示

HTML5ビデオリダイレクトテストページを表示できます。

TLS、HTML5ビデオリダイレクト、およびブラウザーコンテンツリダイレクト

HTML5ビデオリダイレクトは、次の目的で使用できます。

- HTTPS Webサイトからのビデオをリダイレクトする
- または
- Webサイト全体をリダイレクトするためのブラウザーコンテンツリダイレクト

これらのWebサイトに挿入されたJavaScriptは、VDAで実行されているCitrix HDX HTML5ビデオリダイレクトサービス (WebSocketService.exe) へのTLS接続を確立する必要があります。VDA上の証明書ストアにあるCitrix HDX HTML5ビデオリダイレクトサービスは、次の2つのカスタム証明書を生成します。

- ビデオのリダイレクトを実現する
- WebページのTLS整合性を維持する

HdxVideo.jsは、Secure WebSocketsを使用して、VDAで実行されているWebSocketService.exeと通信します。このプロセスはローカルシステムアカウントとして実行され、SSL終端とユーザーセッションマッピングを行います。

WebSocketService.exeは、127.0.0.1ポート9001でリッスンしています。

ビデオ品質を制限する

この設定は、Windows Mediaにのみ適用され、HTML5には適用されません。**WAN経由のWindows Mediaマルチメディアリダイレクトの最適化**を有効にする必要があります。

この設定は、HDX™ 接続で許可される最大ビデオ品質レベルを指定します。設定すると、最大ビデオ品質は指定された値に制限され、環境内でマルチメディアのサービス品質 (QoS) が維持されます。

デフォルトでは、この設定は構成されていません。

許可される最大ビデオ品質レベルを制限するには、次のいずれかのオプションを選択します。

- 1080p/8.5Mbps
- 720p/4.0Mbps
- 480p/720Kbps
- 380p/400Kbps
- 240p/200Kbps

同じサーバーで複数のビデオを同時に再生すると、大量のリソースが消費され、サーバーのスケーラビリティに影響を与える可能性があります。

Microsoft Teamsのリダイレクト

この設定は、HDX テクノロジーに基づいた Microsoft Teams の最適化を有効にします。

このポリシーが有効で、サポートされているバージョンのCitrix Workspace™アプリを使用している場合、このレジストリキーはVDA上で**1**に設定されます。Microsoft Teamsアプリケーションは、VDIモードでロードするためにこのキーを読み取ります。 レジストリキーを手動で設定する必要はありません。

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

名前: MSTeamsRedirSupport

Value: DWORD (1 - オン、0 - オフ)

> **注:**
>
> Web Studioでポリシーが利用できない古いバージョンのControllerと、バージョン1906.2以降のVDAを使用しているとします。Controllerの古いバージョンの例としては、バージョン7.15があります。この場合、HDX最適化はVDAでデフォルトで有効になっています。Workspaceアプリのバージョンが1907以降の場合、Microsoft Teamsは最適化モードで起動します。7.15 LTSR ControllerとCR VDAの混在に関する注意点については、Knowledge Centerの記事CTX205549を参照してください。
>
> この場合、特定のユーザーに対して機能を無効にするには、レジストリ設定を上書きできます。ユーザーの組織単位にログオンスクリプトを適用するグループポリシーを使用して、レジストリ設定を上書きします。
>
> デフォルトでは、Microsoft Teamsリダイレクトは有効になっています。

マルチメディア会議

この設定により、ビデオ会議アプリケーションによる最適化されたWebカメラリダイレクトテクノロジーの使用を許可または禁止します。

デフォルトでは、ビデオ会議のサポートは許可されています。

この設定をポリシーに追加する際は、**Windows Mediaリダイレクト**設定が存在し、**許可**（デフォルト）に設定されていることを確認してください。

マルチメディア会議を使用する場合は、次の条件が満たされていることを確認してください。

- マルチメディア会議に使用されるWebカメラの製造元提供ドライバーがクライアントにインストールされていること。
- ビデオ会議セッションを開始する前に、Webカメラをユーザーデバイスに接続してください。サーバーは、一度に1つのインストール済みWebカメラのみを使用します。ユーザーデバイスに複数のWebカメラがインストールされている場合、サーバーは各Webカメラを順次使用しようとします。この試行は、ビデオ会議セッションが正常に作成されるまで続行されます。

汎用USBリダイレクトを使用してWebカメラをリダイレクトする場合、このポリシーは必要ありません。その場合は、VDAにWebカメラドライバーをインストールしてください。

WAN経由のWindows Mediaマルチメディアリダイレクトの最適化

この設定はWindows Mediaにのみ適用され、HTML5には適用されません。この設定により、以下が可能になります。

- リアルタイムマルチメディアトランスコーディング
- 劣化ネットワーク経由でのモバイルデバイスへのオーディオおよびビデオメディアストリーミングを許可します
- WAN経由でのWindows Mediaコンテンツの配信方法を改善することで、ユーザーエクスペリエンスを向上させます。

デフォルトでは、WAN経由でのWindows Mediaコンテンツの配信は最適化されています。

この設定をポリシーに追加する場合は、**Windows Media Redirection**設定が存在し、**Allowed**に設定されていることを確認してください。

この設定が有効になっている場合、メディアストリーミングを可能にするために、必要に応じてリアルタイムのマルチメディアトランスコーディングが自動的に展開されます。また、極端なネットワーク条件下でもシームレスなユーザーエクスペリエンスを提供します。

WAN経由でのWindows Mediaマルチメディアリダイレクトの最適化にGPUを使用する

この設定はWindows Mediaにのみ適用され、Virtual Delivery Agent (VDA) 上のグラフィックス処理ユニット (GPU) でリアルタイムマルチメディアトランスコーディングを実行できるようにします。これにより、サーバーのスケーラビリティが向上します。GPUトランスコーディングは、VDAがハードウェアアクセラレーションに対応したGPUを搭載している場合にのみ利用可能です。それ以外の場合は、トランスコーディングはCPUにフォールバックします。

注： GPUトランスコーディングはNVIDIA GPUでのみサポートされています。

デフォルトでは、WAN経由でのWindows Mediaコンテンツの配信を最適化するためにVDA上のGPUを使用することは禁止されています。

この設定をポリシーに追加する場合は、以下の設定が存在し、Allowedに設定されていることを確認してください。

- **Windows Mediaリダイレクト**
- **WAN経由のWindows Mediaマルチメディアリダイレクトの最適化設定**

Windows Mediaフォールバック防止

この設定は、ブラウザコンテンツリダイレクト、HTML5、およびWindows Mediaに適用されます。HTML5をサポートするには、**HTML5 video redirection**ポリシーを**Allowed**に設定します。

管理者は、**Windows Media フォールバック防止**ポリシー設定を使用して、ストリーミングコンテンツをユーザーに配信するために試行される方法を指定できます。

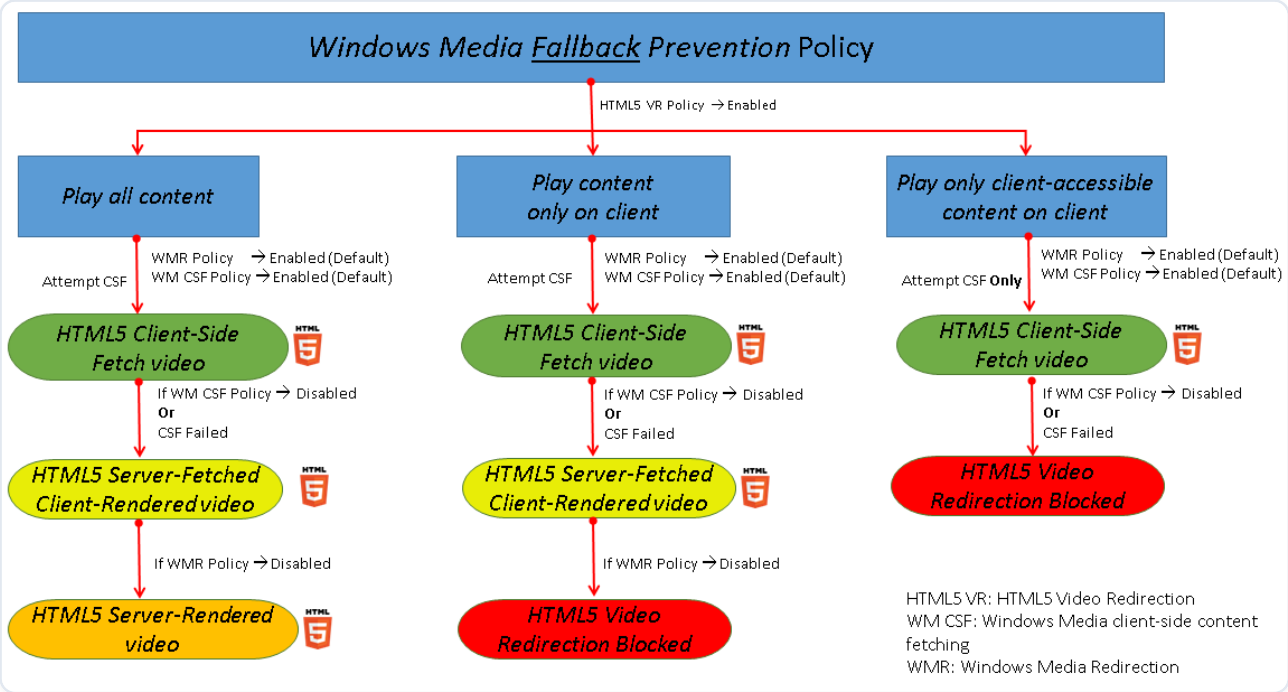
デフォルトでは、この設定は構成されていません。この設定が「未構成」に設定されている場合、動作は**すべてのコンテンツを再生**と同じになります。

この設定を構成するには、次のいずれかのオプションを選択します。

- **すべてのコンテンツを再生**。クライアント側のコンテンツ取得を試行し、次にWindows Mediaリダイレクトを試行します。失敗した場合は、サーバーでコンテンツを再生します。
- **すべてのコンテンツをクライアントでのみ再生**。クライアント側の取得を試行し、次にWindows Mediaリダイレクトを試行します。失敗した場合は、コンテンツは再生されません。
- **クライアントでクライアントがアクセス可能なコンテンツのみを再生**。クライアント側の取得のみを試行します。失敗した場合は、コンテンツは再生されません。

コンテンツが再生されない場合、プレーヤーウィンドウに次のエラーメッセージが表示されます（デフォルトの表示時間は5秒）。

「リソース不足のため、会社がビデオをブロックしました」



このエラーメッセージの表示時間は、VDA上の次のレジストリキーでカスタマイズできます。レジストリエントリが存在しない場合、表示時間はデフォルトで5秒になります。

レジストリパスは、VDAのアーキテクチャによって異なります。

```
\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream
```

または

\HKLM\SOFTWARE\Citrix\HdxMediastream

レジストリキー：

名前: VideoLoadManagementErrDuration

種類: DWORD

範囲: 1 - DWORD制限まで（デフォルト = 5）

単位: 秒

Windows Media クライアント側コンテンツフェッチ

この設定はHTML5とWindows Mediaの両方に適用されます。この設定により、ユーザーデバイスは、XenAppまたはXenDesktop®ホストサーバーを介さずに、インターネットまたはイントラネット上のソースプロバイダーからマルチメディアファイルを直接ストリーミングできるようになります。

デフォルトでは、この設定は**許可**されています。この設定を許可すると、ネットワーク使用量とサーバーのスケーラビリティが向上します。この改善は、メディアに関する処理をホストサーバーからユーザーデバイスに移行することで実現されます。また、Microsoft DirectShowやMedia Foundationなどの高度なマルチメディアフレームワークをユーザーデバイスにインストールする必要がなくなります。ユーザーデバイスには、URLからファイルを再生する機能のみが必要です。

この設定をポリシーに追加するときは、**Windows Mediaリダイレクト**設定が存在し、**許可**に設定されていることを確認してください。**Windows Mediaリダイレクト**が無効になっている場合、ソースプロバイダーからユーザーデバイスへのマルチメディアファイルの直接ストリーミングも無効になります。

Windows Mediaリダイレクト

この設定はHTML5とWindows Mediaの両方に適用され、サーバーがストリーミングオーディオとビデオをユーザーに配信する方法を制御および最適化します。

デフォルトでは、この設定は**許可**されています。HTML5の場合、ポリシー**HTML5ビデオリダイレクト**が**禁止**されていると、この設定は有効になりません。

この設定が有効になっている場合、サーバーからレンダリングされるオーディオとビデオの品質は、ユーザーデバイスでローカルに再生されるオーディオとビデオに匹敵するレベルに向上します。サーバーはマルチメディアを元の圧縮形式でクライアントにストリーミングし、ユーザーデバイスがメディアを解凍してレンダリングできるようにします。

Windows Mediaリダイレクトは、Microsoft DirectShow、DirectX Media Objects (DMO)、およびMedia Foundationの標準に準拠するコーデックでエンコードされたマルチメディアファイルを最適化します。特定のマルチメディアファイルを再生するには、そのマルチメディアファイルのエンコード形式と互換性のあるコーデックがユーザーデバイスに存在する必要があります。

デフォルトでは、Citrix Workspaceアプリでオーディオは無効になっています。ユーザーがICA®セッションでマルチメディアアプリケーションを実行できるようにするには、オーディオをオンにするか、Citrix Workspaceアプリインターフェイスでオーディオをオンにする権限をユーザーに付与します。

Windows Mediaリダイレクトを使用してメディアを再生したときに、基本的なICA圧縮と通常のオーディオを使用してレンダリングした場合よりも品質が悪い場合にのみ、**禁止**を選択してください。この状況はまれですが、低帯域幅の条件下、たとえばキーフレームの頻度が低いメディアの場合に発生する可能性があります。

Windows Mediaリダイレクトのバッファサイズ

この設定はレガシーであり、HTML5には適用されません。

この設定は、マルチメディアアクセラレーションのバッファサイズを1〜10秒で指定します。

デフォルトでは、バッファサイズは5秒です。

Windows Mediaリダイレクトのバッファサイズの使用

この設定はレガシーであり、HTML5には適用されません。

この設定は、**Windows Media Redirection buffer size** 設定で指定されたバッファサイズの使用を有効または無効にします。

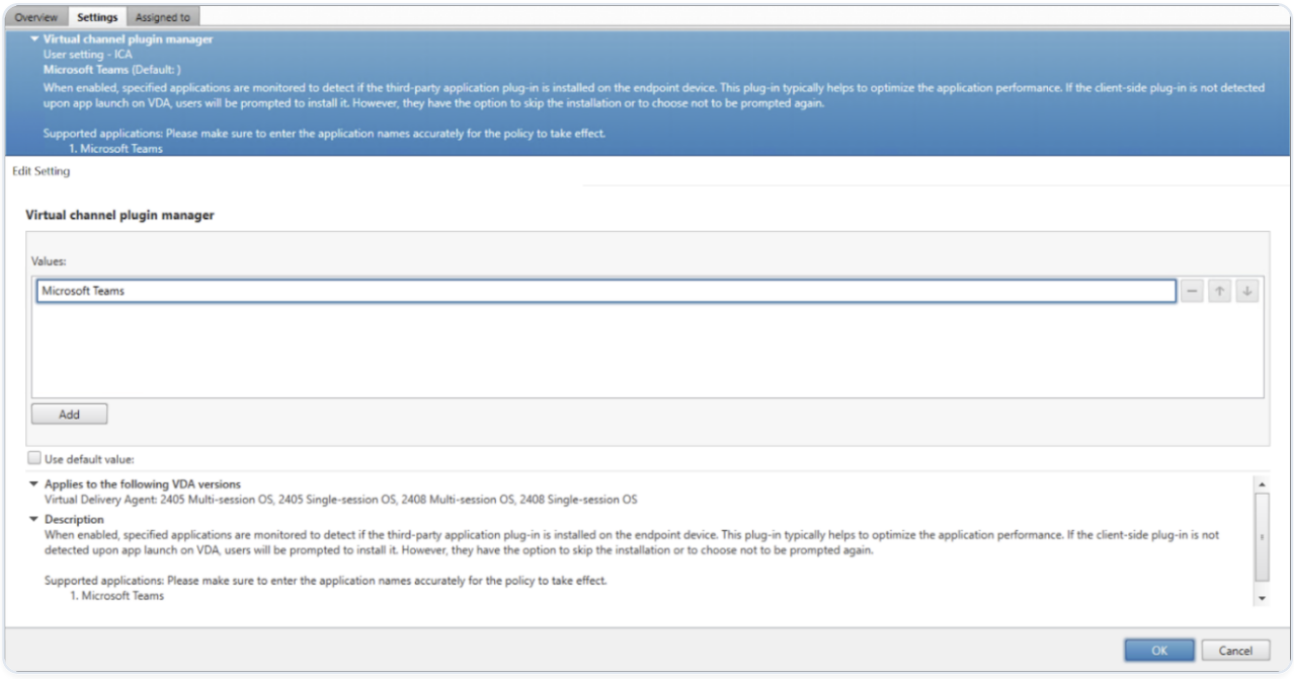
デフォルトでは、指定されたバッファサイズは使用されません。

この設定が無効になっている場合、または**Windows Media Redirection buffer size** 設定が構成されていない場合、サーバーはデフォルトのバッファサイズ値（5秒）を使用します。

仮想チャネルプラグインマネージャーポリシー

仮想チャネルプラグインマネージャーセクションには、この機能を構成するためのポリシー設定が含まれています。

仮想チャネルプラグインマネージャーは、特定の指定されたアプリケーションのクライアントエンドポイント全体にプラグインを展開するように設計されています。プラグインマネージャーは、VDAで実行されている特定のアプリケーションを検出し、アプリケーションの実行時に最高の体験を得るために、エンドポイントにプラグインをインストールするようユーザーに促します。



- 管理者はポリシーを使用して、エンドポイント全体にプラグインをインストールする必要があるアプリケーションを指定できます。

- アプリケーション名は、ポリシーの説明にある「サポートされているアプリケーション」に記載されている名前と同じである必要があります。
- デフォルトでは、ポリシーは無効になっています。
- 現在サポートされているアプリケーション
  - 「Microsoft チームズ」
- 今後、さらに多くのアプリケーションがサポートされる予定です。

マルチストリーム接続ポリシー設定

「**マルチストリーム接続**」セクションには、セッション内の複数のICA®接続のサービス品質の優先順位付けを管理するためのポリシー設定が含まれています。

> **注:**
>
> マルチストリーム接続ポリシーが有効になっている場合、MTU検出はサポートされません。

UDP経由のオーディオ

この設定は、サーバー上でのUDP経由のオーディオを許可または禁止します。

デフォルトでは、サーバー上でのUDP経由のオーディオは許可されています。

有効にすると、この設定は、UDP経由のオーディオリアルタイムトランスポートを使用するように構成されたすべての接続をサポートするために、サーバー上にUDPポートを開きます。

オーディオUDPポート範囲

この設定は、Virtual Delivery Agent (VDA) が使用するポート番号の範囲 (最小ポート番号、最大ポート番号) を指定します。この指定は、ユーザーデバイスとの間でオーディオパケットデータを交換するのに役立ちます。VDAは、ユーザーデバイスとのデータ交換のために、各UDPポートペアを最小値から開始し、その後の試行ごとに2ずつ増やして使用しようとします。各ポートは、インバウンドトラフィックとアウトバウンドトラフィックの両方を処理します。

デフォルトでは、この範囲は16500,16509に設定されています。

マルチポートポリシー

この設定は、ICAトラフィックに使用するTCPポートを指定し、各ポートのネットワーク優先順位を確立します。

デフォルトでは、プライマリポート (2598) は高優先度です。

ポートを構成するとき、次の優先順位を割り当てることができます。

- **非常に高い:** ウェブカメラ会議などのリアルタイムアクティビティ用
- **高い:** 画面、キーボード、マウスなどのインタラクティブな要素用
- **中:** クライアントドライブマッピングなどのバルク処理用
- **低い:** 印刷などのバックグラウンドアクティビティ用

各ポートには一意の優先順位が必要です。たとえば、CGPポート1とCGPポート3の両方に「非常に高」の優先順位を割り当てることはできません。

ポートを優先順位付けから削除するには、ポート番号を0に設定します。プライマリポートを削除したり、その優先順位レベルを変更したりすることはできません。

この設定を構成するときは、サーバーを再起動してください。この設定は、**Multi-Stream computer** 設定ポリシー設定が有効になっている場合にのみ有効になります。

マルチストリーム コンピューター設定

この設定は、サーバー上でMulti-Streamを有効または無効にします。

デフォルトでは、Multi-Streamは無効になっています。Citrix SD-WAN™またはサードパーティ製ルーターを使用して目的のQuality of Serviceを実現する場合は、Multi-Stream computerポリシー設定を構成してください。

Multi-Streamが有効になっている場合、Adaptive Transportの機能であるMTU Discoveryはサポートされません。

この設定を構成するときは、変更を有効にするためにサーバーを再起動してください。

> **重要:**
>
> このポリシー設定を、全体的なセッション帯域幅制限などの帯域幅制限ポリシー設定と併用すると、予期しない結果が生じる可能性があります。この設定をポリシーに含める場合は、帯域幅制限設定を含めないようにしてください。

マルチストリーム ユーザー設定

この設定は、ユーザーデバイスでマルチストリームを有効または無効にします。

デフォルトでは、マルチストリームはすべてのユーザーに対して無効になっています。Citrix SD-WANまたはサードパーティ製ルーターを使用して目的のサービス品質を実現する場合は、マルチストリームのユーザー設定を構成します。

この設定は、**マルチストリームコンピューター**設定ポリシー設定が有効になっているホストでのみ有効になります。

> **重要:**
>
> このポリシー設定を、全体的なセッション帯域幅制限などの帯域幅制限ポリシー設定と併用すると、予期しない結果が生じる可能性があります。この設定をポリシーに含める場合は、帯域幅制限設定が含まれていないことを確認してください。

マルチストリーム仮想チャネル割り当て設定

この設定は、マルチストリームが使用されている場合に仮想チャネルが割り当てられるICAストリームを指定します。

これらの設定を構成しない場合、仮想チャネルはデフォルトのストリームに保持されます。仮想チャネルをICAストリームに割り当てるには、仮想チャネル名の横にある**ストリーム番号**リストから、目的のストリーム番号（0、1、2、3）を選択します。

環境でカスタム仮想チャネルが使用されている場合は、**追加**をクリックし、**仮想チャネル**の下のテキストボックスに仮想チャネル名を指定し、その横にある**ストリーム番号**リストから目的のストリーム番号を選択します。指定する名前は、フレンドリ名ではなく、実際の仮想チャネル名である必要があります。たとえば、Citrix Browser AccelerationではなくCTXSBRです。

これらの設定は、マルチストリームコンピューター設定を有効にした場合にのみ有効になります。

デフォルトでは、仮想チャネルとそのストリーム割り当ては次のとおりです。

- AppFlow®: 2
- オーディオ: 0
- ブラウザコンテンツリダイレクト: 2
- クライアントCOMポートマッピング: 3
- クライアントドライブマッピング: 2
- クライアントプリンターマッピング: 3

- クリップボード: 2
- CTXDND: 1 (**注:** これは、Citrixセッションとローカルエンドポイント間でファイルをドラッグアンドドロップする機能をサポートします。)
- DVCプラグイン (DVCプラグインのフレンドリ名から自動生成された静的VC名、または管理者によって割り当てられたもの): 2
- エンドユーザーエクスペリエンス監視: 1
- ファイル転送 (HTML5 Receiver): 2
- 汎用データ転送: 2
- ICA制御: 1
- 入力メソッドエディター: 1
- レガシー クライアント プリンター マッピング (COM1): 1, 3
- レガシー クライアント プリンター マッピング (COM2): 2, 3
- レガシー クライアント プリンター マッピング (LPT1): 1, 3
- レガシー クライアント プリンター マッピング (LPT2): 2, 3
- ライセンス管理: 1
- Microsoft Teams/WebRTC リダイレクト: 1
- モバイルレシーバー: 1
- マルチタッチ: 1
- ポートフォワーディング: 2
- リモートオーディオおよびビデオ拡張機能 (RAVE): 2
- シームレス (透過ウィンドウ統合): 1
- センサーと位置情報: 1
- スマートカード: 1
- Thinwire グラフィック: 1
- 透過UI統合/ログオンステータス: 2
- TWAIN リダイレクト: 2
- USB: 2
- ゼロレイテンシーフォントとキーボード: 2
- ゼロレイテンシーデータチャネル: 2

仮想チャネルの割り当てと優先度について詳しくは、Knowledge Center の記事 CTX131001 を参照してください。

ポートリダイレクトポリシー設定

ポートリダイレクトセクションには、クライアントLPTおよびCOMポートマッピングのポリシー設定が含まれています。

Virtual Delivery Agentのバージョン**7.0より前**の場合、ポートリダイレクトを構成するには以下のポリシー設定を使用します。VDAのバージョン**7.0から7.8**の場合、これらの設定はレジストリを使用して構成します。詳しくは、レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成を参照してください。VDAのバージョン**7.9**の場合、以下のポリシー設定を使用します。

クライアントCOMポートの自動接続

この設定は、ユーザーがサイトにログオンしたときに、ユーザーデバイス上のCOMポートの自動接続を有効または無効にします。

デフォルトでは、クライアントCOMポートは自動的に接続されません。

クライアントLPTポートの自動接続

この設定は、ユーザーがサイトにログオンしたときに、ユーザーデバイス上のLPTポートの自動接続を有効または無効にします。

デフォルトでは、クライアントLPTポートは自動的に接続されません。

クライアントCOMポートリダイレクト

この設定は、ユーザーデバイス上のCOMポートへのアクセスを許可または禁止します。

デフォルトでは、COMポートリダイレクトは禁止されています。

関連するポリシー設定は次のとおりです。

- COMポートリダイレクト帯域幅制限
- COMポートリダイレクト帯域幅制限（パーセント）

クライアントLPTポートリダイレクト

この設定は、ユーザーデバイス上のLPTポートへのアクセスを許可または禁止します。

デフォルトでは、LPTポートリダイレクトは禁止されています。

LPTポートは、LPTポートに印刷ジョブを送信するレガシーアプリケーションでのみ使用されます。これらのポートは、ユーザーデバイス上の印刷オブジェクトに印刷ジョブを送信するレガシーアプリケーションでは使用されません。現在のほとんどのアプリケーションは、プリンターオブジェクトに印刷ジョブを送信できます。このポリシー設定は、LPTポートに印刷するレガシーアプリケーションをホストするサーバーにのみ必要です。

クライアントCOMポートリダイレクトは双方向ですが、LPTポートリダイレクトは出力のみであり、ICAセッション内では`\client\LPT1`および`\client\LPT2`に制限されます。

以下のポリシー設定は関連しています。

- LPTポートリダイレクト帯域幅制限
- LPTポートリダイレクトの帯域幅制限（パーセント）

印刷ポリシー設定

印刷セクションには、クライアント印刷を管理するためのポリシー設定が含まれています。

クライアントプリンターリダイレクト

この設定は、ユーザーがセッションにログオンしたときに、クライアントプリンターがサーバーにマップされるかどうかを制御します。

デフォルトでは、クライアントプリンターのマッピングは許可されています。この設定が無効になっている場合、セッション用のPDFプリンターは自動作成されません。

関連するポリシー設定: クライアントプリンターの自動作成

デフォルトプリンター

この設定は、ユーザーデバイス上のデフォルトプリンターがセッションでどのように確立されるかを指定します。

デフォルトでは、ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます。

デフォルトプリンターに現在のRemote Desktop ServicesまたはWindowsユーザープロファイル設定を使用するには、「ユーザーのデフォルトプリンターを調整しない」を選択します。このオプションを選択すると、デフォルトプリンターはプロファイルに保存されず、他のセッションまたはクライアントプロパティに従って変更されることもありません。セッション内のデフォルトプリンターは、セッションで自動作成された最初のプリンターであり、次のいずれかです。

- **コントロールパネル > デバイスとプリンター**でWindowsサーバーにローカルに追加された最初のプリンター。

- サーバーにローカルに追加されたプリンターがない場合、最初に自動作成されたプリンター。

このオプションを使用すると、プロファイル設定を通じてユーザーに最も近いプリンターを提示できます（近接印刷として知られています）。

プリンターの割り当て

この設定は、デフォルトプリンターとセッションプリンターの設定の代替手段を提供します。個別のデフォルトプリンターとセッションプリンターの設定を使用して、サイト、大規模グループ、または組織単位の動作を構成します。**プリンター割り当て**設定を使用して、多数のプリンターを複数のユーザーに割り当てます。

この設定は、一覧表示されたユーザーデバイスのデフォルトプリンターがセッションでどのように確立されるかを指定します。

デフォルトでは、ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます。

また、各ユーザーデバイスのセッションで自動作成されるネットワークプリンターも指定します。デフォルトでは、プリンターは指定されていません。

- デフォルトプリンターの値を設定する場合：

  ユーザーデバイスの現在のデフォルトプリンターを使用するには、「調整しない」を選択します。

  デフォルトプリンターに現在のRemote Desktop ServicesまたはWindowsユーザープロファイル設定を使用するには、「調整しない」を選択します。このオプションを選択した場合、デフォルトプリンターはプロファイルに保存されず、他のセッションまたはクライアントのプロパティに応じて変更されません。セッションのデフォルトプリンターは、セッションで自動作成された最初のプリンターであり、それは次のいずれかです。

  - **コントロールパネル > デバイスとプリンター**でWindowsサーバーにローカルに追加された最初のプリンター。
  - サーバーにローカルに追加されたプリンターがない場合、自動作成された最初のプリンター。

- セッションプリンターの値を設定する場合：プリンターを追加するには、自動作成したいプリンターのUNCパスを入力します。プリンターを追加した後、ログオンごとに現在のセッションにカスタマイズされた設定を適用できます。

プリンターの自動作成イベントログ設定

この設定は、プリンターの自動作成プロセス中にログに記録されるイベントを指定します。エラーや警告をログに記録しない、エラーのみをログに記録する、またはエラーと警告をログに記録するを選択できます。

デフォルトでは、エラーと警告がログに記録されます。

警告の例としては、プリンターのネイティブドライバーをインストールできず、代わりにユニバーサルプリントドライバーがインストールされるイベントがあります。このシナリオでユニバーサルプリントドライバーを使用するには、ユニバーサルプリントドライバーの使用設定を「ユニバーサル印刷のみを使用する」または「要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用する」に構成します。

セッションプリンター

この設定は、セッションで自動作成されるネットワークプリンターを指定します。ICA/HDXセッション内では、Citrix Print Managerサービス（CpSvc.exe）が、**セッションプリンター**ポリシー設定で指定された各ネットワークプリンターに対して、セッションログオン中にネットワークプリンター接続を作成します。セッションログオフ中にプリンターを削除します。デフォルトでは、プリンターは指定されていません。

「**セッションプリンター**」ポリシー設定では、ネットワークプリンターはWindowsプリントサーバーまたはCitrix Universal™プリントサーバーに配置できます。

- **Windowsプリントサーバー:** 1つ以上のネットワークプリンターを共有します。また、ネットワークプリンターを使用するために必要なネイティブプリンタードライバーも備えています。
- **Universal Print Server:** Citrix Universal Print ServerソフトウェアがインストールされているWindowsプリントサーバーです。

Windows Print Server を使用する場合、Citrix Print Manager サービスはネイティブプリンタードライバーを使用してネットワークプリンター接続を作成します。Citrix Virtual Apps™ サーバーには、ネイティブプリンタードライバーがインストールされている必要があります。

Citrix Universal Print Server を使用する場合、Citrix Print Manager サービスは、ネイティブプリンタードライバー、Citrix Universal Printer Driver、または Citrix Universal XPS Printer Driver のいずれかを使用してネットワークプリンター接続を作成します。使用するドライバーは、Universal Print Driver の使用ポリシー設定によって制御されます。

すべての Windows プリンタードライバーは現在、v3 または v4 ドライバーバージョンのいずれかに分類されます。詳細については、「Support for the Microsoft V3 and V4 Printer Driver Architectures」を参照してください。

セッションプリンターを追加し、セッションに表示されるかどうかを確認するには、次の手順を実行します。

1. Web Studioにサインインし、左ペインで**［ポリシー］を選択し、［ポリシー］**タブをクリックします。
2. **［セッションプリンター］**ポリシーを有効にします。
3. ポリシーで、セッションプリンターを追加します。プリンターを追加するには、自動作成するプリンターのUNCパスを入力します。プリンターを追加した後、ログオンごとに現在のセッションのカスタマイズされた設定を適用できます。セッションプリンターがリストに表示される必要があります。
4. ポリシーが設定された後、公開アプリケーションにセッションプリンターが表示されない場合があります。この問題は、Citrix Virtual Appsサーバーにプリンタードライバーがないか、ポリシーが作成されたものの有効になっていないために発生する可能性があります。

> **注：**
>
> セッションプリンターにネイティブプリンタードライバーが必要で、そのネイティブプリンタードライバーがVDAにインストールされていない場合、セッションプリンターはセッションに作成されない可能性があります。

5. 公開デスクトップを起動し、**［デバイスとプリンター］>［コントロールパネル］**でセッションプリンターを手動で追加します。
6. これが失敗した場合は、Citrix Virtual Appsサーバーとプリントサーバー間の通信を調査します。RDPでテストを実行することを検討してください。

プリンターが作成されるのを待つ

Delivery Controller のポリシーを使用して、Citrix Virtual Desktops でこの機能を有効にします。

プリンターの作成を待機する (サーバーデスクトップ):

この設定により、セッションへの接続を遅延させ、クライアントリダイレクトされたプリンターを自動作成できます。

デフォルトでは、接続遅延は発生しません。

プリンターの作成を待機する (Citrix Virtual Apps):

次の PowerShell コマンドレットを実行すると、マルチセッションホストで実行されている仮想アプリへの接続を遅延させ、アプリケーションが開かれる前にクライアントリダイレクトされたプリンターを自動作成できます。

```
Set-BrokerApplication -Name <VirtualAppName> -WaitForPrinterCreation $true
```

デフォルトでは、接続遅延は発生しません。

クライアントプリンターのポリシー設定

クライアントプリンターセクションには、クライアントプリンターのポリシー設定が含まれています。これには、クライアントプリンターの自動作成、プリンタープロパティの保持、印刷サーバーへの接続に関する設定が含まれます。

クライアントプリンターの自動作成

この設定は、自動作成されるクライアントプリンターを指定します。この設定は、デフォルトのクライアントプリンター自動作成設定を上書きします。

デフォルトでは、すべてのクライアントプリンターが自動作成されます。

この設定は、**クライアントプリンターリダイレクト**設定が存在し、**許可**に設定されている場合にのみ有効になります。

この設定をポリシーに追加するときは、オプションを選択します。

- **すべてのクライアントプリンターを自動作成**すると、ユーザーデバイス上のすべてのプリンターが自動的に作成されます。
- **クライアントのデフォルトプリンターのみを自動作成**すると、ユーザーデバイスでデフォルトプリンターとして選択されているプリンターのみが自動的に作成されます。
- **ローカル（非ネットワーク）クライアントプリンターのみを自動作成**すると、LPT、COM、USB、TCP/IP、またはその他のローカルポートを介してユーザーデバイスに直接接続されているプリンターのみが自動的に作成されます。
- **クライアントプリンターを自動作成しない**を選択すると、ユーザーがログオンするときに、すべてのクライアントプリンターの自動作成がオフになります。このオプションを選択すると、クライアントプリンターを自動作成するためのRemote Desktop Services (RDS) 設定が、優先度の低いポリシーでこの設定を上書きします。

汎用ユニバーサルプリンターの自動作成

この設定は、セッションの汎用Citrix Universal™ Printerオブジェクトの自動作成を有効または無効にします。これらのセッションには、Universal Printingと互換性のあるユーザーデバイスが使用されているセッションのみが含まれます。

デフォルトでは、汎用ユニバーサルプリンターオブジェクトは自動作成されません。

関連するポリシー設定は次のとおりです。

- ユニバーサルプリントドライバーの使用
- ユニバーサルドライバーの優先順位

PDFユニバーサルプリンターの自動作成

この設定は、以下のセッションでCitrix PDFプリンターの自動作成を有効または無効にします。

- Windows向けCitrix Workspaceアプリ（VDA 7.19以降）
- HTML5向けCitrix Workspace™アプリ
- Chrome向けCitrix Workspaceアプリ

デフォルトでは、Citrix PDFプリンターは自動作成されません。

クライアントプリンター名

この設定は、自動作成されたクライアントプリンターの命名規則を選択します。

デフォルトでは、標準のプリンター名が使用されます。

標準プリンター名を選択すると、「セッション3のクライアント名からのHPLaserJet 4」のようなプリンター名が使用されます。

レガシープリンター名を選択すると、旧式のクライアントプリンター名が使用され、製品のXenDesktopバージョンに存在するレガシープリンター名との下位互換性が維持されます。このオプションは、現在のCitrix Virtual Apps and Desktopsバージョンの製品でも使用できます。レガシープリンター名の例は「Client/clientname#/HPLaserJet 4」です。このオプションはセキュリティが低下します。

Citrix Workspaceアプリ for HTML5から起動されたセッションでCitrix PDFプリンターを使用する場合、**クライアントプリンター名**の設定をデフォルトにするか、**標準プリンター名**を選択してください。**レガシープリンター名**を選択した場合、Citrix Workspaceアプリ for HTML5はCitrix PDFプリンターオプションをサポートしません。

プリントサーバーへの直接接続

この設定は、仮想デスクトップまたはサーバーホスティングアプリケーションからクライアントプリンター用のプリントサーバーへの直接接続を有効または無効にします。ここで、クライアントプリンターはアクセス可能なネットワーク共有でホストされます。

デフォルトでは、直接接続が有効になっています。

ネットワークプリントサーバーが仮想デスクトップまたはサーバーホスティングアプリケーションからWANを介していない場合は、直接接続を有効にします。ネットワークプリントサーバーと仮想デスクトップまたはサーバーホスティングアプリケーションが同じLAN上にある場合、直接通信により印刷が高速化されます。

ネットワークがWANを介している場合、または大幅な遅延や帯域幅の制限がある場合は、直接接続を無効にします。印刷ジョブはユーザーデバイスを経由してルーティングされ、そこでネットワークプリントサーバーにリダイレクトされます。ユーザーデバイスに送信されるデータは圧縮されるため、WANを介してデータが転送される際の帯域幅の消費が少なくなります。

2つのネットワークプリンターが同じ名前を持つ場合、ユーザーデバイスと同じネットワーク上のプリンターが使用されます。

プリンタードライバーのマッピングと互換性

この設定は、自動作成されたクライアントプリンターのドライバー置換ルールを指定します。

この設定は、Microsoft OneNoteおよびXPS Document Writerを自動作成されたクライアントプリンターリストから除外するように構成されています。

ドライバー置換ルールを定義すると、指定されたドライバーでプリンターが作成されることを許可または防止できます。また、作成されたプリンターがユニバーサルプリントドライバーのみを使用することを許可できます。ドライバー置換は、ユーザーデバイスが提供するプリンタードライバー名を上書きまたはマッピングし、サーバー上の同等のドライバーに置き換えます。これらのルールにより、サーバーアプリケーションは、サーバーと同じドライバーを持つがドライバー名が異なるクライアントプリンターにアクセスできるようになります。

次のことができます。

- ドライバーマッピングを追加する
- 既存のマッピングを編集する
- マッピングのカスタム設定を上書きする
- マッピングを削除する
- リスト内のドライバーエントリの順序を変更する

マッピングを追加する際は、クライアントプリンタードライバー名を入力し、置き換えたいサーバードライバーを選択します。

プリンタープロパティの保持

この設定では、プリンタープロパティを保存するかどうか、および保存場所を指定します。

デフォルトでは、プリンタープロパティをユーザーデバイスに保存するか（利用可能な場合）、またはユーザープロファイルに保存するかをシステムが決定します。

この設定をポリシーに追加するときは、オプションを選択してください。

- 「クライアントデバイスのみに保存」は、保存されない強制プロファイルまたは移動プロファイルを持つユーザーデバイス用です。
- 「ユーザープロファイルのみに保持」は、帯域幅（このオプションはネットワークトラフィックを削減します）とログオン速度によって制約されるユーザーデバイス、またはレガシープラグインを使用するユーザー向けです。このオプションは、プリンタープロパティをサーバー上のユーザープロファイルに保存し、ユーザーデバイスとのプロパティ交換を防ぎます。このオプションは、リモートデスクトップサービス（RDS）の移動プロファイルが使用されている場合にのみ適用されます。
- 「クライアントに保存されていない場合のみプロファイルに保持」では、プリンタープロパティの保存場所をシステムが決定できます。プリンタープロパティは、利用可能な場合はユーザーデバイスに、またはユーザープロファイルに保存されます。このオプションは最も柔軟ですが、ログオン時間を遅くしたり、システムチェックのために余分な帯域幅を使用したりする可能性があります。
- 「プリンタープロパティを保持しない」は、プリンタープロパティの保存を防ぎます。

保持および復元されたクライアントプリンター

この設定は、ユーザーデバイス上のプリンターの保持と再作成を有効または無効にします。デフォルトでは、クライアントプリンターは自動保持および自動復元されます。

Retained printers are user-created printers that are created again, or remembered, at the start of the next session. When Citrix Virtual Apps™ recreates a retained printer, it considers all policy settings except the **Auto-create client printers** setting.

復元されたプリンターとは、管理者が完全にカスタマイズし、クライアントポートに永続的にアタッチされた保存状態を持つプリンターです。

CITRIX PDFユニバーサルプリンタードライバー

The Citrix PDF Universal Printer driver enables users to print documents opened with hosted applications or applications that are running on virtual desktops delivered by Citrix Virtual Apps and Desktops. When a user selects the **Citrix PDF Printer** option, the driver converts the file to PDF and transfers the PDF to the local device. The PDF is then opened for viewing and printing from a locally attached printer. PDF is one of the formats supported with Citrix Universal Printing (in addition to EMF and XPS). The PDF printer can be enabled, configured, and set as default using a

Citrix Policy. The **Citrix PDF Printer** option is available to users of the Citrix Workspace app for Windows, Chrome, and HTML5.

> **注:**
>
> WindowsエンドポイントにはPDFビューアーが必要です。クライアントには、PDFファイルを開くためにWindowsにファイルタイプ関連付けが登録されているアプリケーションが必要です。

ドライバーポリシー設定

「**ドライバー**」セクションには、プリンタードライバーに関連するポリシー設定が含まれています。

インボックスプリンタードライバーの自動インストール

> **注**
>
> このリリースでは、このポリシーはVDAをサポートしていません。

> この設定は、以下のプリンタードライバーの自動インストールを有効または無効にします。

- Windowsインボックスドライバーセット
- `pnputil.exe /a`を使用してホストにステージングされたドライバーパッケージ

デフォルトでは、これらのドライバーは必要に応じてインストールされます。

ユニバーサルドライバーの優先順位

この設定は、リストの最初のエントリから始まる、ユニバーサルプリンタードライバーが使用される順序を指定します。

デフォルトでは、優先順位は次のとおりです。

- EMF
- XPS
- PCL5c (ピーシーエルファイブシー)
- PCL4
- PS

ドライバーの追加、編集、削除、およびリスト内のドライバーの順序変更が可能です。

ユニバーサルプリントドライバーの使用

この設定は、ユニバーサル印刷を使用するタイミングを指定します。

デフォルトでは、ユニバーサル印刷は、要求されたドライバーが利用できない場合にのみ使用されます。

ユニバーサル印刷では、標準のモデル固有ドライバーの代わりに汎用プリンタードライバーが使用されるため、ホストコンピューターでのドライバー管理の負担が軽減される可能性があります。ユニバーサルプリントドライバーの可用性は、ユーザーデバイス、ホスト、およびプリントサーバーソフトウェアの機能によって異なります。特定の構成では、ユニバーサル印刷が利用できない場合があります。

この設定をポリシーに追加するときは、次の表からオプションを選択します。

オプション	説明
プリンターモデル固有のドライバーのみを使用する	クライアントプリンターが、サインイン時に自動作成される標準のモデル固有ドライバーのみを使用することを指定します。要求されたドライバーが利用できない場合、クライアントプリンターは自動作成できません。
ユニバーサル印刷のみを使用する	標準のモデル固有ドライバーは使用しないことを指定します。プリンターの作成にはユニバーサルプリントドライバーのみが使用されます。
要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用する	利用可能な場合は、標準のモデル固有ドライバーを使用してプリンターを作成します。ドライバーがサーバーで利用できない場合、クライアントプリンターは適切なユニバーサルドライバーで自動的に作成されます。
ユニバーサル印刷が利用できない場合にのみ、プリンターモデル固有のドライバーを使用する	利用可能な場合は、ユニバーサルプリントドライバーを使用します。ドライバーがサーバーで利用できない場合、クライアントプリンターは適切なモデル固有のプリンタードライバーで自動的に作成されます。

ユニバーサルプリントサーバーのポリシー設定

ユニバーサルプリントサーバーセクションには、ユニバーサルプリントサーバーを処理するためのポリシー設定が含まれています。

SSL暗号スイート

この設定は、暗号化された印刷データストリーム (CGP) 接続のためにUniversal Print Clientで使用されるSSL/TLS暗号スイートのセットを指定します。

暗号化された印刷Webサービス (HTTPS/SOAP) 接続のためにUniversal Print Clientで使用される暗号スイートパッケージを制御するには、を参照してください。

デフォルト値: ALL

この設定には、ALL、COM、またはGOVの以下の値があります。

各値に対応する暗号スイートは以下のとおりです。

ALL:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

COM:

TLS_ECDHE_RSA_AES128_CBC_SHA

GOV:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

SSL準拠モード

この設定は、Universal Print Clientが暗号化された印刷データストリーム（CGP）接続に使用するNIST Special Publication 800-52への準拠レベルを指定します。

デフォルト値：なし。

この設定には、次の値があります。

なし。

暗号化された印刷データストリーム（CGP）接続は、デフォルトの準拠モードを使用します。

SP800-52。

暗号化された印刷データストリーム（CGP）接続は、NIST Special Publication 800-52準拠モードを使用します。

SSL有効

この設定は、Universal Print Clientが以下の目的でSSL/TLSを使用するかどうかを指定します。

- 印刷データストリーム（CGP）接続
- Webサービス（HTTP/SOAP）接続

Universal Print Serverを有効にするを**Windowsのネイティブリモート印刷へのフォールバックを有効にする**に設定すると、Microsoft Windowsネットワーク印刷プロバイダーによってフォールバック接続が行われます。この設定は、これらのフォールバック接続には影響しません。

既定値: 無効

この設定は次の値をとります。

有効。

Universal Print ClientはSSL/TLSを使用してUniversal Print Serverに接続します。

無効。

Universal Print ClientはSSL/TLSを使用してUniversal Print Serverに接続します。

SSL FIPSモード

この設定は、Universal Print Clientが印刷データストリーム (CGP) 接続のために使用するSSL/TLS暗号モジュールがFIPSモードで実行されるかどうかを指定します。

既定値: 無効

この設定は次の値をとります。

有効。

FIPSモードがオンになります。

無効。

FIPSモードがオフになります。

SSLプロトコルバージョン

この設定は、Universal Print Client が使用するSSL/TLSプロトコルバージョンを指定します。

デフォルト値: ALL

この設定には、次の値があります。

ALL。

TLSバージョン1.0、1.1、または1.2を使用します。

TLSバージョン1.

TLSバージョン1.0を使用します。

TLSv1.1。

TLSバージョン1.1を使用します。

TLSv1.2。

TLSバージョン1.2を使用します。

SSL UNIVERSAL PRINT SERVER 暗号化印刷データストリーム (CGP) ポート

この設定は、Universal Print Server 暗号化印刷データストリーム (CGP) ポートのTCPポート番号を指定します。このポートは、印刷ジョブのデータを受信します。

デフォルト値: 443

SSL UNIVERSAL PRINT SERVER 暗号化WEBサービス (HTTPS/SOAP) ポート

この設定は、Universal Print Serverの暗号化されたWebサービス（HTTPS/SOAP）ポートのTCPポート番号を指定します。このポートは、印刷コマンドのデータを受信します。

デフォルト値: 8443

UNIVERSAL PRINT SERVERの有効化

このポリシーは、Citrix Universal Print Server (UPS) の使用を有効または無効にします。このポリシー設定は、仮想デスクトップまたはサーバーホスティングアプリケーションを含む組織単位 (OU) に適用します。このポリシー設定には、Citrix UPSコンポーネントが要求されたプリントサーバーにインストールされていないか、利用できない場合に、ネイティブのWindowsリモート印刷サービスを使用してプリントサーバーへの接続を許可するフォールバックオプションが含まれています。このポリシーへの変更は、VDAが再起動された後にのみ適用されます。

デフォルトでは、Universal Print Serverは無効になっています。

この設定をポリシーに追加する際は、次のいずれかのオプションを選択します。

- **Windowsネイティブリモート印刷へのフォールバックを有効にする**: 可能な場合、Universal Print Serverがネットワークプリンター接続を処理します。Universal Print Serverが利用できない場合、Windows Print Providerが使用されます。Windows Print Providerは、以前にWindows Print Providerで作成されたすべてのプリンターの処理を継続します。
- **Windowsネイティブリモート印刷へのフォールバックなしで有効にする**: Universal Print Serverがネットワークプリンター接続を排他的に処理します。Universal Print Serverが利用できない場合、ネットワークプリンター接続は失敗します。この設定は、Windows Print Providerを介したネットワーク印刷を実質的に無効にします。この設定を含むポリシーがアクティブな間は、以前にWindows Print Providerで作成されたプリンターは作成されません。
- **無効**: Universal Print Server機能は無効です。UNC名を持つネットワークプリンターに接続する際、Universal Print Serverへの接続は試行されません。リモートプリンターへの接続は、引き続きWindowsネイティブのリモート印刷機能を使用します。

UNIVERSAL PRINT SERVER印刷データストリーム (CGP) ポート

この設定は、Universal Print Server印刷データストリームのCommon Gateway Protocol (CGP) リスナーが使用するTCPポート番号を指定します。このポリシー設定は、プリントサーバーを含むOUにのみ適用します。

デフォルトでは、ポート番号は7229に設定されています。

有効なポート番号は1～65535の範囲である必要があります。

UNIVERSAL PRINT SERVER印刷ストリーム入力帯域幅制限 (KBPS)

この設定は、印刷データの転送速度の上限（キロビット/秒）を指定します。転送速度は、CGPを使用して各印刷ジョブからUniversal Print Serverに配信される印刷データに対して計算されます。このポリシー設定は、仮想デスクトップまたはサーバーホスティングアプリケーションを含むOUに適用します。

デフォルトでは、値は0で、上限がないことを示します。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) ポート

この設定は、Universal Print ServerのWebサービス (HTTP/SOAP) リスナーが使用するTCPポート番号を指定します。Universal Print Serverは、ネットワーク印刷シナリオでCitrixユニバーサル印刷ドライバーの使用を可能にするオプションコンポーネントです。

Universal Print Serverが使用される場合、印刷コマンドはCitrix Virtual Apps and Desktopsホストから SOAP over HTTPを介してUniversal Print Serverに送信されます。この設定は、Universal

Print Serverが受信HTTP/SOAPリクエストをリッスンするデフォルトのTCPポートを変更します。

ホストとプリントサーバーの両方のHTTPポートを同じように構成する必要があります。ポートを同じように構成しない場合、ホストソフトウェアはUniversal Print Serverに接続しません。この設定は、Citrix Virtual Apps and Desktops上のVDAを変更します。さらに、Universal Print Serverのデフォルトポートも変更する必要があります。

デフォルトでは、ポート番号は8080に設定されています。

有効なポート番号は0～65535の範囲である必要があります。

負荷分散用のUNIVERSAL PRINT SERVER

この設定は、他のCitrix®印刷ポリシー設定を評価した後、セッション起動時に確立されたプリンター接続の負荷分散に使用されるUniversal Print Serverを一覧表示します。プリンター作成時間を最適化するために、Citrixはすべてのプリントサーバーが同じ共有プリンターセットを持つことを推奨します。負荷分散のために追加できるプリントサーバーの数に上限はありません。

この設定は、プリントサーバーのフェイルオーバー検出とプリンター接続の回復も実装します。プリントサーバーは定期的に可用性がチェックされます。サーバー障害が検出された場合、そのサーバーは負荷分散スキームから削除されます。また、そのサーバー上のプリンター接続は、他の利用可能なプリントサーバーに再配布されます。障害が発生したプリントサーバーが回復すると、負荷分散スキームに戻されます。

「**サーバーの検証**」をクリックして、各サーバーがプリントサーバーであること、サーバーリストに重複するサーバー名が含まれていないこと、およびすべてのサーバーに同一の共有プリンターセットがインストールされていることを確認します。この操作には時間がかかる場合があります。

UNIVERSAL PRINT SERVERサービス停止しきい値

この設定は、ロードバランサーが利用できないプリントサーバーが回復するのをどれだけ長く待つかを指定します。この時間を過ぎると、サーバーは永続的にオフラインであると判断され、その負荷は他の利用可能なプリントサーバーに再配布されます。

デフォルトでは、しきい値は180（秒）に設定されています。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) 接続タイムアウト

この設定は、Universal Print ClientがUniversal Print Server Webサービスのconnect()操作がタイムアウトするまで待機する秒数を指定します。この設定には以下の値があります。これらの値はすべて数値であり、単位（時間）は秒です。

- 最小値は0です。

- 最大値は60です。
- デフォルト値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Clientは、操作が完了するまで指定された時間待機します。この操作は、TCPソケット接続操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Client はオペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この設定は、この変更前のUniversal Print Client の以前のバージョンで利用可能だった設定です。

Universal Print Client は、Universal Print Server と通信するVirtual Delivery Agent (VDA) のコンポーネントです。

> **注:**
>
> このポリシー設定は、VDAバージョン7.35以降で適用されます。

UNIVERSAL PRINT SERVER WEB サービス (HTTP/SOAP) 受信タイムアウト

この設定は、Universal Print Client が Universal Print Server Web サービスの recv() 操作がタイムアウトするまで待機する秒数を指定します。この設定には以下の値があり、これらの値はすべて数値であり、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- デフォルト値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Client は操作が完了するまで指定された時間待機します。この操作は、TCPソケットの受信操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Clientはオペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前のUniversal Print Clientの以前のバージョンで利用可能だった構成です。

Universal Print Clientは、Universal Print Serverと通信するVirtual Delivery Agent (VDA) のコンポーネントです。

> **注：**
>
> このポリシー設定は、VDAバージョン7.35以降に適用されます。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) 受信タイムアウト

この設定は、Universal Print ClientがUniversal Print Server Webサービスのrecv()操作がタイムアウトするまで待機する秒数を指定します。この設定には次の値があり、これらの値はすべて数値で、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- デフォルト値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Clientは、操作が完了するまで指定された時間待機します。この操作は、TCPソケット受信操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Clientは、オペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前のUniversal Print Clientの以前のバージョンで利用可能だった構成です。

Universal Print Clientは、Universal Print Serverと通信するVirtual Delivery Agent (VDA) のコンポーネントです。

> **注：**
>
> このポリシー設定は、VDAバージョン7.35以降で適用されます。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) 送信タイムアウト

この設定は、Universal Print Client が Universal Print Server Webサービスの send() 操作がタイムアウトするまで待機する秒数を指定します。この設定には次の値があります。これらの値はすべて数値であり、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- デフォルト値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Client は操作が完了するまで指定された時間待機します。この操作はTCPソケット送信操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Client はオペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前のUniversal Print Clientの以前のバージョンで利用可能だった構成です。

Universal Print Client は、Universal Print Server と通信するVDAのコンポーネントです。

> **注:**
>
> このポリシー設定は、VDAバージョン7.35以降で適用されます。

ユニバーサル印刷ポリシー設定

ユニバーサル印刷セクションには、ユニバーサル印刷を管理するためのポリシー設定が含まれています。

ユニバーサル印刷EMF処理モード

この設定は、Windowsユーザーデバイス上のEMFスプールファイルの処理方法を制御します。

デフォルトでは、EMFレコードはプリンターに直接スプールされます。

この設定をポリシーに追加するときは、オプションを選択します。

- プリンター用のEMFを再処理すると、EMFスプールファイルが再処理され、ユーザーデバイス上のGDIサブシステムを介して送信されます。この設定は、EMFの再処理を必要とするが、セッションで自動的に選択されない可能性のあるドライバーに使用できます。
- Citrix Universal™プリンタードライバーで使用する場合、プリンターに直接スプールすると、EMFレコードがスプールされ、処理のためにユーザーデバイスに配信されます。通常、これらのEMFスプールファイルはクライアントのスプールキューに直接挿入されます。EMF形式と互換性のあるプリンターおよびドライバーの場合、これが最速の印刷方法です。

ユニバーサル印刷画像圧縮制限

この設定は以下を指定します:

- Citrix Universal Print Driverで印刷される画像に利用可能な最大品質
- Citrix Universal Print Driverで印刷される画像に利用可能な最小圧縮レベル

デフォルトでは、画像圧縮制限は「最高品質（ロスレス圧縮）」に設定されています。

「圧縮なし」が選択されている場合、EMF印刷のみ圧縮が無効になります。

この設定をポリシーに追加するときは、オプションを選択します。

- 圧縮なし
- 最高品質 (ロスレス圧縮)
- 高品質
- 標準品質
- 低品質 (最大圧縮)

Universal printing optimization defaults 設定を含むポリシーにこの設定を追加する場合は、次の点に注意してください。

- **Universal printing image compression limit** 設定の圧縮レベルが、**Universal printing optimization defaults** 設定で定義されているレベルよりも低いとします。この場合、画像は Universal printing image compression limits 設定で定義されているレベルで圧縮されます。
- 圧縮が無効になっている場合、Universal printing optimization defaults 設定の「Desired image quality」および「Enable heavyweight compression」オプションはポリシーに影響しません。

ユニバーサル印刷の最適化の既定値

この設定は、セッション用にユニバーサル印刷ドライバーが作成される際の印刷最適化のデフォルト値を指定します。

- Desired image quality は、ユニバーサル印刷に適用されるデフォルトの画像圧縮制限を指定します。デフォルトでは、標準品質が有効になっており、ユーザーは標準品質または低品質の圧縮を使用してのみ画像を印刷できます。
- Enable heavyweight compression は、Desired image quality で設定された圧縮レベルを超えて帯域幅を削減するかどうかを有効または無効にします。画質は低下しません。デフォルトでは、ヘビーウェイト圧縮は無効になっています。
- Image and Font Caching 設定は、印刷ストリームに複数回出現する画像とフォントをキャッシュするかどうかを指定します。この設定により、一意の画像またはフォントがプリンターに一度だけ送信されるようになります。デフォルトでは、埋め込み画像とフォントはキャッシュされます。これらの設定は、ユーザーデバイスがこの動作をサポートしている場合にのみ適用されます。
- Allow non-administrators to modify these settings は、ユーザーがセッション内でデフォルトの印刷最適化設定を変更できるかどうかを指定します。デフォルトでは、ユーザーはデフォルトの印刷最適化設定を変更できません。

注: これらのオプションはすべて EMF 印刷でサポートされています。XPS 印刷では、Desired image quality オプションのみがサポートされています。

この設定を、**ユニバーサル印刷イメージ圧縮制限**設定を含むポリシーに追加する場合は、次の点に注意してください。

- **ユニバーサル印刷イメージ圧縮制限**設定の圧縮レベルが、**ユニバーサル印刷最適化のデフォルト**設定で定義されているレベルよりも低いとします。この場合、イメージはユニバーサル印刷イメージ圧縮制限設定で定義されているレベルで圧縮されます。
- 圧縮が無効になっている場合、ユニバーサル印刷最適化のデフォルト設定の「希望する画質」と「高負荷圧縮を有効にする」オプションは、ポリシーに影響を与えません。

ユニバーサル印刷プレビューの優先順位

この設定は、自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して印刷プレビュー機能を使用するかどうかを指定します。

デフォルトでは、自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して印刷プレビューは使用されません。

この設定をポリシーに追加するときは、オプションを選択します。

- 自動作成されたプリンターまたは汎用ユニバーサルプリンターに印刷プレビューを使用しない
- 自動作成されたプリンターにのみ印刷プレビューを使用する
- 汎用ユニバーサルプリンターにのみ印刷プレビューを使用する
- 自動作成されたプリンターと汎用ユニバーサルプリンターの両方に印刷プレビューを使用する

ユニバーサル印刷の印刷品質制限

この設定は、セッションで印刷出力を生成するために利用できる最大ドット/インチ (dpi) を指定します。

デフォルトでは、「制限なし」が有効になっており、ユーザーは接続先のプリンターで許可されている最高の印刷品質を選択できます。

この設定が構成されている場合、出力解像度の観点から、ユーザーが利用できる最大印刷品質が制限されます。印刷品質自体と、ユーザーが接続するプリンターの印刷品質機能の両方が、構成された設定に制限されます。

例えば、中解像度 (600 DPI) に設定されている場合、ユーザーは最大 600 DPI の品質でしか出力を印刷できません。また、**Universal Printer** ダイアログボックスの **詳細設定** タブにある **印刷品質** 設定には、中品質 (600 DPI) までの解像度設定のみが表示されます。

この設定をポリシーに追加するときは、オプションを選択します。

- 下書き (150 DPI)
- 低解像度 (300 DPI)
- 中解像度 (600 DPI)
- 高解像度 (1200 DPI)
- 制限なし

セキュリティポリシー設定

セキュリティセクションには、セッション暗号化とログオンデータの暗号化を構成するためのポリシー設定が含まれています。

SecureICAの最小暗号化レベル

この設定は、サーバーとユーザーデバイス間で送信されるセッションデータを暗号化する最小レベルを指定します。

重要: Virtual Delivery Agent 7.xの場合、このポリシー設定は、RC5 128ビット暗号化によるログオンデータの暗号化を有効にするためにのみ使用できます。その他の設定は、Citrix Virtual Apps and Desktopsのレガシーバージョンとの下位互換性のためにのみ提供されています。

VDA 7.xの場合、セッションデータの暗号化はVDAのDelivery Groupの基本設定を使用して行われます。Delivery GroupでEnable Secure ICAが選択されている場合、セッションデータはRC5 (128ビット) 暗号化を使用して暗号化されます。Delivery GroupでEnable Secure ICAが選択されていない場合、セッションデータは基本暗号化で暗号化されます。

この設定をポリシーに追加するときは、オプションを選択してください。

- Basicは、非RC5アルゴリズムを使用してクライアント接続を暗号化します。データストリームが直接読み取られるのを防ぎますが、復号化される可能性があります。デフォルトでは、サーバーはクライアントとサーバー間のトラフィックにBasic暗号化を使用します。
- RC5（128ビット）ログオンのみは、RC5 128ビット暗号化を使用してログオンデータを暗号化し、Basic暗号化を使用してクライアント接続を暗号化します。
- RC5（40ビット）は、RC5 40ビット暗号化を使用してクライアント接続を暗号化します。
- RC5（56ビット）は、RC5 56ビット暗号化を使用してクライアント接続を暗号化します。
- RC5（128ビット）は、RC5 128ビット暗号化を使用してクライアント接続を暗号化します。

クライアントとサーバー間の暗号化に指定する設定は、環境内の他の暗号化設定やWindowsオペレーティングシステムと相互作用する可能性があります。サーバーまたはユーザーデバイスのいず

れかで、より高い優先度の暗号化レベルが設定されているとします。この場合、公開リソースに指定した設定が上書きされる可能性があります。

特定のユーザーの通信とメッセージの整合性をさらに保護するために、暗号化レベルを上げることができます。ポリシーでより高い暗号化レベルが必要な場合、より低い暗号化レベルを使用しているCitrix Receiversは接続を拒否されます。

SecureICAは認証を実行したり、データの整合性をチェックしたりしません。サイトにエンドツーエンドの暗号化を提供するには、SecureICAをTLS暗号化と組み合わせて使用します。

SecureICAはFIPS準拠アルゴリズムを使用しません。この設定が問題となる場合は、サーバーとCitrix ReceiverをSecureICAを使用しないように構成してください。

SecureICAは、機密性のためにRFC 2040で説明されているRC5ブロック暗号を使用します。ブロックサイズは64ビット（32ビットワード単位の倍数）です。キー長は128ビットです。ラウンド数は12です。

RC5ブロック暗号のキーは、セッションが作成されるときにネゴシエートされます。ネゴシエーションはDiffie-Hellmanアルゴリズムを使用して実行されます。このネゴシエーションでは、Diffie-Hellman公開パラメーターが使用されます。これらのパラメーターは、Virtual Delivery Agentがインストールされるときにレジストリに保存されます。公開パラメーターは秘密ではありません。Diffie-Hellmanネゴシエーションの結果は秘密キーであり、そこからRC5ブロック暗号のセッションキーが導出されます。ユーザーログオンとデータ転送には、個別のセッションキーが使用されます。また、Virtual Delivery Agentとの間のトラフィックにも個別のセッションキーが使用されます。したがって、各セッションには4つのセッションキーがあります。秘密キーとセッションキーは保存されません。RC5ブロック暗号の初期化ベクトルも秘密キーから導出されます。

セッション制限ポリシー設定

セッション制限セクションには、セッションが強制的にログオフされるまでに接続を維持する期間を制御するポリシー設定が含まれています。

切断されたセッションタイマー

この設定は、切断されロックされたデスクトップが、セッションがログオフされるまでにロックされたままになる期間を指定するタイマーを有効または無効にします。

このタイマーが有効になっている場合、タイマーの期限が切れると、切断されたセッションはログオフされます。

デフォルトでは、切断されたセッションはログオフされません。

Remote PC Accessの切断されたセッションタイマー

この設定は、タイマーの期限が切れた後に切断されたユーザーセッションをログオフするタイマーを有効または無効にします。この設定を有効にする場合は、**切断されたセッションタイマー間隔**設定を使用して、ユーザーセッションがログオフされるまでに切断されたデスクトップがロックされたままになる時間を分数で指定します。

デフォルトでは、この設定は無効になっています。

切断されたセッションタイマー間隔

この設定は、切断されロックされたデスクトップが、セッションがログオフされるまでにロックされたままになる時間を分数で指定します。

デフォルトでは、期間は1,440分（24時間）です。

切断されたセッションタイマー – マルチセッション

この設定は、切断されたRDSセッションがログオフされるまでにどのくらいの期間持続できるかを決定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっており、切断されたセッションはログオフされません。

切断されたセッションタイマー間隔 – マルチセッション

この設定は、切断されたRDSセッションがログオフされるまでにどのくらいの期間（分単位）持続できるかを決定します。デフォルトでは、期間は1440分（24時間）です。

セッション接続タイマー

この設定は、ユーザーデバイスとデスクトップ間の途切れない接続の最大継続時間を指定するタイマーを有効または無効にします。このタイマーが有効になっている場合、タイマーの期限が切れるとセッションは切断またはログオフされます。Microsoftの**時間制限に達したらセッションを終了する**設定が、セッションの次の状態を決定します。

デフォルトでは、このタイマーは無効になっています。

セッション接続タイマー間隔

この設定は、ユーザーデバイスとデスクトップ間の途切れない接続の最大時間（分）を指定します。

デフォルトでは、最大継続時間は1,440分（24時間）です。

セッション接続タイマー – マルチセッション

この設定は、ユーザーデバイスとターミナルサーバー間の途切れない接続の最大継続時間を指定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっています。

セッション接続タイマー間隔 – マルチセッション

この設定は、ユーザーデバイスとRDSセッション間の途切れない接続の最大時間（分）を指定します。デフォルトでは、最大継続時間は1440分（24時間）です。

セッションアイドルタイマー

ユーザーが何も入力しない場合、この設定は以下を有効または無効にするために使用されます。

- デスクトップへの途切れないユーザーデバイス接続がどのくらいの期間維持されるかを指定するタイマー。

このタイマーの期限が切れると、セッションは切断状態になり、**切断されたセッションタイマー**が適用されます。**切断されたセッションタイマー**が無効になっている場合、セッションはログオフされません。

デフォルトでは、このタイマーは有効になっています。

セッションアイドルタイマー間隔

ユーザーからの入力がない場合、この設定は以下を指定するために使用されます。

- デスクトップへのユーザーデバイスの途切れない接続が維持される分数。

デフォルトでは、アイドル状態の接続は1,440分（24時間）維持されます。

セッションアイドルタイマー – マルチセッション

この設定は、ユーザーデバイスとターミナルサーバー間のアイドル接続の最大期間を決定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっています。

セッションアイドルタイマー間隔 – マルチセッション

この設定は、ユーザーデバイスとRDSセッション間のアイドル接続が何分間続くかを指定します。デフォルトでは、最大期間は1440分（24時間）です。

> **注:**
>
> Citrix®ポリシーを使用して構成されたマルチセッションマシンのタイマー設定は、Microsoftグループポリシーを通じて構成されたタイマー設定を上書きすることが想定されています。予期せぬ動作を避けるため、いずれかの方法を使用してタイマー設定を構成することをお勧めします。

セッションの信頼性ポリシー設定

セッションの信頼性セクションには、セッションの信頼性接続を管理するためのポリシー設定が含まれています。

セッションの信頼性接続

この設定により、ネットワーク接続が失われたときにセッションを開いたままにするかどうかが決まります。セッションの信頼性は、自動クライアント再接続と連携して、ネットワーク障害から回復した後、ユーザーがCitrix Workspace™アプリセッションに自動的に再接続できるようにします。デフォルトでは、セッションの信頼性は「許可」されています。

Web Studioの設定は、クライアントで以下に対して適用されます。

- Citrix Workspaceアプリ1808以降
- Citrix Receiver for Windows 4.7以降のバージョン。

Web Studioポリシーは、クライアント上のCitrix Receiver™グループポリシーオブジェクトを上書きします。Web Studioでこれらのポリシーを更新すると、セッションの信頼性がサーバーからクライアントに同期されます。

> **注:**
>
> - Citrix Receiver for Windows 4.7以降およびWindows向けCitrix Workspaceアプリ - Web Studioでポリシーを設定します。
> - Citrix Receiver for Windows 4.7より前のバージョン - Web Studioでポリシーを設定します。また、一貫した動作のために、クライアントでCitrix Receiverグループポリシーオブジェクトテンプレートを設定します。

> セッションの信頼性により、ネットワーク接続が中断された場合でも、セッションがアクティブな状態に保たれ、ユーザーの画面に表示されます。ユーザーは、ネットワーク接続が再開されるまで、使用中のアプリケーションを引き続き見ることができます。

セッションの信頼性を使用して、サーバー上でセッションをアクティブな状態に保ちます。接続が失われたことを示すために、ユーザーのディスプレイは不透明になります。中断中にユーザーはフリーズしたセッションを見る可能性があります。ネットワーク接続が復元されると、ユーザーはアプリケーションとの対話を再開できます。セッションの信頼性により、再認証のプロンプトなしでユーザーが再接続されます。

セッションの信頼性と自動クライアント再接続の両方を使用する場合、これら2つの機能は順番に動作します。セッションの信頼性は、セッションの信頼性タイムアウト設定で指定された時間の経過後にユーザーセッションを閉じ（または切断し）ます。その後、自動クライアント再接続設定が有効になり、切断されたセッションにユーザーを再接続しようとします。

デフォルトでは、セッションの信頼性は「許可」されています。

> **注:**
>
> Citrix ADCを使用している場合、ICA接続をプロキシするには、Citrix StoreFront > **Manage Citrix Gateways** / **Secure Ticket Authority** で **Enable session reliability** を選択する必要があります。

セッションの信頼性ポート番号

この設定は、受信セッションの信頼性接続用のTCPポート番号を指定します。

デフォルトでは、ポート番号は2598に設定されています。

セッションの信頼性タイムアウト

この設定は、時間（秒単位）を指定します。この時間は、セッションの信頼性プロキシがユーザーの再接続を待機し、セッションが切断されるのを許可するまでの時間です。

セッションが開いている時間を延長することはできますが、この機能は利便性のためであり、ユーザーに再認証を促すものではありません。セッションが開いている時間が長くなるほど、ユーザーがデバイスを放置し、不正なユーザーがアクセスする可能性が高まります。

デフォルトでは、タイムアウトは180秒、つまり3分に設定されています。

セッションウォーターマークポリシー設定

セッションウォーターマークセクションには、この機能を構成するためのポリシー設定が含まれています。 この機能を有効にすると、VDAマシンのネットワーク帯域幅とCPU使用率が大幅に増加します。利用可能なハードウェアリソースに基づいて、選択したVDAマシンにセッションウォーターマークを構成することをお勧めします。

> **重要**

> 他のウォーターマークポリシー設定を有効にするには、セッションウォーターマークを有効にします。より良いユーザーエクスペリエンスを実現するために、ウォーターマークテキスト項目を2つ以上有効にしないでください。

セッションウォーターマークを有効にする

この設定を有効にすると、セッションディスプレイにセッション固有の情報を表示する不透明なテキストウォーターマークが表示されます。他のウォーターマーク設定は、この設定が有効になっているかどうかに依存します。

デフォルトでは、セッションウォーターマークは無効になっています。

クライアントIPアドレスを含める

この設定を有効にすると、セッションは現在のクライアントIPアドレスをウォーターマークとして表示します。

デフォルトでは、クライアントIPアドレスを含めるは無効になっています。

接続時間を含める

この設定を有効にすると、セッションウォーターマークに接続時間が表示されます。形式はyyyy/mm/dd hh:mmです。表示される時刻は、システムクロックとタイムゾーンに基づいています。

デフォルトでは、接続時間を含めるは無効になっています。

ログオンユーザー名を含める

この設定を有効にすると、セッションは現在のログオンユーザー名をウォーターマークとして表示します。表示形式はUSERNAME@DOMAINNAMEです。ユーザー名は最大20文字にすることをお勧めします。ユーザー名が20文字を超えると、文字フォントが過度に小さくなったり、切り捨てられたりして、ウォーターマークの効果が低下する可能性があります。

デフォルトでは、「ログオンユーザー名を含める」は有効になっています。

VDAホスト名を含める

この設定を有効にすると、セッションは現在のICA®セッションのVDAホスト名をウォーターマークとして表示します。

デフォルトでは、「VDAホスト名を含める」は有効になっています。

VDA IPアドレスを含める

この設定を有効にすると、セッションは現在のICAセッションのVDA IPアドレスをウォーターマークとして表示します。

デフォルトでは、VDA IPアドレスは無効になっています。

セッションウォーターマークのスタイル

この設定は、単一のウォーターマークテキストラベルを表示するか、複数のラベルを表示するかを制御します。「**値**」ドロップダウンメニューから「**複数**」または「**単一**」を選択します。

「**複数**」は、セッションに5つのウォーターマークラベルを表示します。中央に1つ、四隅に4つです。

「**単一**」は、セッションの中央に単一のウォーターマークラベルを表示します。

デフォルトでは、セッションウォーターマークのスタイルは「複数」です。

ウォーターマークのカスタムテキスト

この設定を使用すると、セッションウォーターマークに表示するカスタムテキスト（例：会社名）を適用できます。空でない文字列を設定すると、ウォーターマークで有効になっている他の情報に加えて、そのテキストが新しい行に表示されます。ウォーターマークのカスタムテキストは25 Unicode文字に制限されています。より長い文字列を設定した場合、25文字に切り詰められます。

デフォルトのテキストはありません。

Citrix Virtual Apps and Desktops™ 7 2206 以降、テキスト内のカスタムタグを使用して、より多くのカスタマイズを追加できます。その結果、カスタムテキストの最大文字数は1024に増加しました。

ウォーターマーク設定で利用可能なタグは、次の表に記載されています。

タグ	説明	例
`<font=value>`	ウォーターマークテキストのフォントを変更できます。値はVDAで利用可能なフォントの名前です。	`<font=Courier New>`
`<fontzoom=value>`	フォントのズーム率を設定できます。ウォーターマークテキストの200%ズームの場合、値は200です。	`<fontzoom=200>`
`<position=value>`	ウォーターマークテキストの位置を変更できます。値は `center`、`topleft`、	`<position=topright>`

タグ	説明	例
	`topright`、`bottomleft`、および`bottomright`です。このタグはシングルスタイルでのみ適用可能です。	
`<rotation=value>`	ウォーターマークテキストを回転できます。値は度で指定され、範囲は-360から360です。	`<rotation=45>`
`<style=value>`	表示スタイルを変更できます。このタグは、セッションウォーターマークスタイルポリシーを上書きします。	`<style=single>`

以下のウォーターマークスタイルが利用可能です。

- シングルスタイル - セッションの中央に単一のウォーターマークテキストラベルが表示されます。位置タグを使用して場所を変更できます。
- xスタイルまたは複数 - セッションに5つのウォーターマークラベルが表示されます。中央に1つ、各コーナーに1つずつです。
- タイル - セッションに複数のラベルが表示されます。ウォーターマークテキストは画面全体に均等に配置されます。

ウォーターマークテキストを変更するために利用できるタグは、以下の表に記載されています。

タグ	説明
`<clientip>`	エンドポイントのIPアドレス。
`<date>`	セッションが確立された日付。
`<domain>`	ログインしているユーザーアカウントのドメイン名。
`<hostname>`	VDAのマシン名。
`<newline>`	追加の行を作成します。
`<serverip>`	VDAのIPアドレス。

タグ	説明
`<time>`	セッションが確立された時刻。
`<username>`	ユーザーの名前。

注:

- **ウォーターマークカスタムテキスト**ポリシーは、**セッションウォーターマークを有効にする**ポリシーが有効になっている場合にのみ適用されます。デフォルト値は*無効*です。
- ウォーターマークテキストを変更するためのタグを使用する場合、「**セッションウォーターマークを有効にする**」を除く他のすべてのセッションウォーターマークポリシーは無視されます。ウォーターマークテキスト設定にタグを使用する場合、他のすべてのウォーターマークポリシーを使用できます。

透かしの透明度

ウォーターマークの不透明度を0から100まで指定できます。指定する値が大きいほど、ウォーターマークは不透明になります。

デフォルトでは、値は17です。

タイムゾーン制御ポリシー設定

「**タイムゾーン制御**」セクションには、セッションでローカル時間を使用することに関連するポリシー設定が含まれています。

レガシークライアントのローカル時間を推定する

この設定は、ユーザーデバイスのローカルタイムゾーンの推定を有効または無効にします。これらのデバイスには、サーバーに不正確なタイムゾーン情報を送信するユーザーデバイスが含まれます。

デフォルトでは、サーバーは必要に応じてローカルタイムゾーンを推定します。

この設定は、詳細なタイムゾーン情報をサーバーに送信しないレガシーCitrix ReceiverまたはICAクライアントで使用することを目的としています。この設定が、詳細なタイムゾーン情報をサーバーに送信するCitrix Receiver（たとえば、サポートされているバージョンのCitrix Receiver™ for Windows）で使用される場合を考慮してください。この場合、この設定は効果がありません。

セッション切断またはログオフ時にデスクトップOSのタイムゾーンを復元する

ユーザーがセッションを切断またはログオフした場合を考慮してください。この場合、この設定は、シングルセッションOS VDAのタイムゾーン設定がマシンの元のタイムゾーンに復元されるかどうかを決定します。この設定を有効にすると、ユーザーが切断またはログオフしたときに、VDAはマシンのタイムゾーンを元の設定に復元します。この設定を有効にするには、**クライアントのローカル時間を使用**を**クライアントのタイムゾーンを使用**に設定します。

デフォルトでは、この設定は有効になっています。

クライアントのローカル時間を使用

この設定は、ユーザーセッションのタイムゾーン設定を決定します。選択肢は、ユーザーセッションのタイムゾーン（サーバータイムゾーン）またはユーザーデバイスのタイムゾーン（クライアントタイムゾーン）です。

デフォルトでは、ユーザーセッションのタイムゾーンが使用されます。

この設定を有効にするには、グループポリシーエディターで「**Allow time zone redirection**」設定を有効にします。この設定は、「**ローカルコンピューターポリシー**」>「**コンピューターの構成**」>「**管理用テンプレート**」>「**Windows コンポーネント**」>「**リモートデスクトップサービス**」>「**リモートデスクトップセッションホスト**」>「**デバイスとリソースのリダイレクト**」にあります。

サーバーOSを実行しているマシンでシングルセッションVDA（以前のWorkstation VDA）を使用している場合は、ローカルユーザー権限の**タイムゾーンの変更**を**Everyone**に構成します。このユーザー権限は、**ローカルコンピューターポリシー** > **コンピューターの構成** > **Windowsの設定** > **セキュリティの設定** > **ローカルポリシー** > **ユーザー権利の割り当て**にあります。

> **注:**
>
> シングルセッションOSでは、**ユーザー**は、ユーザー権利の割り当てである**タイムゾーンの変更**に含まれますが、マルチセッションOSでは含まれません。マルチセッションOSでは、タイムゾーンは次のグループポリシーを使用して同期されます: Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Allow timezone redirection。このポリシーは、サーバーがマルチセッションOS VDAのリモートデスクトップセッションホストである場合（`/ServerVDI`コマンドでインストールされている場合）に適用されます。マルチセッションOSでは、デフォルトで、また設計上、ユーザーはタイムゾーンを変更するローカルの権利を持ちません。

TWAINデバイスのポリシー設定

TWAINデバイスセクションには、以下のポリシー設定が含まれています。

- デジタルカメラやスキャナーなどのクライアントTWAINデバイスのマッピング
- サーバーからクライアントへの画像転送の最適化

> **注:**
>
> Citrix Receiver for Windows 4.5では、TWAIN 2.0がサポートされています。

クライアントTWAINデバイスのリダイレクト

TWAINデバイスは、TWAINプロトコルを使用して、サーバーでホストされている画像処理アプリケーションと通信します。

この設定により、ユーザーはユーザーデバイス上のTWAINデバイスにアクセスできるようになります。またはアクセスが禁止されます。デフォルトでは、TWAINデバイスのリダイレクトは許可されています。

以下のポリシー設定が関連しています。

- TWAIN圧縮レベル
- TWAINデバイスのリダイレクト帯域幅制限
- TWAINデバイスリダイレクト帯域幅制限の割合

TWAIN圧縮レベル

この設定は、クライアントからサーバーへの画像転送の圧縮レベルを指定します。最良の画質には「低」、良好な画質には「中」、低い画質には「高」を使用します。デフォルトでは、中程度の圧縮が適用されます。

USBデバイスポリシー設定

USBデバイスセクションには、USBデバイスのファイルリダイレクトを管理するためのポリシー設定が含まれています。

クライアントUSBデバイス最適化ルール

クライアントUSBデバイス最適化ルールは、最適化を無効にするか、最適化モードを変更するためにデバイスに適用できます。

ユーザーがUSB入力デバイスを接続すると、ホストは**USBポリシー**設定がそのデバイスを許可するかどうかを確認します。デバイスが許可されている場合、ホストはデバイスの**クライアントUSBデバイス最適化ルール**を確認します。ルールが指定されていない場合、デバイスは最適化されません。キャプチャモード（04）は、署名デバイスに推奨されるモードです。高遅延によってパフォーマンスが低下する他のデバイスの場合、管理者はインタラクティブモード（02）を有効にできます。この記事の表で利用可能なモードの説明を参照してください。

知っておくとよいこと

- Wacom署名パッドおよびタブレットを使用する場合は、スクリーンセーバーを無効にすることをお勧めします。スクリーンセーバーを無効にする手順は、このセクションの最後にあります。
- Wacom STU署名パッドおよびタブレット製品シリーズの最適化のサポートは、Citrix Virtual Apps and Desktops™ポリシーのインストール時に事前設定されています。
- 署名デバイスはCitrix Virtual Apps and Desktops全体で機能し、署名デバイスとして使用するためにドライバーを必要としません。Wacomには、デバイスをさらにカスタマイズするためにインストールできる追加のソフトウェアがあります。`<http://www.wacom.com/>`を参照してください。
- 描画タブレット。特定の描画入力デバイスは、PCI/ACPIバス上でHIDデバイスとして表示される場合があり、サポートされていません。これらのデバイスは、Citrix Virtual Desktopsセッション内でリダイレクトするために、クライアント上のUSBホストコントローラーに接続してください。

ポリシー規則は、空白で区切られたtag=value式の形式を取ります。次のタグがサポートされています。

タグ名	説明
モード	最適化モードは、class=**03**の入力デバイスでサポートされています。サポートされているモードは次のとおりです。最適化なし - 値**01**。インタラクティブモード - 値**02**。ペンタブレットや3D Proマウスなどのデバイスに推奨されます。キャプチャモード - 値**04**。署名パッドなどのデバイスに推奨されます。
VID	デバイス記述子からのベンダーID。4桁の16進数として。

タグ名	説明
PID	デバイス記述子からの製品ID。4桁の16進数として。
REV	デバイス記述子からのリビジョンID。4桁の16進数として。
クラス	デバイス記述子またはインターフェイス記述子のいずれかからのクラス。
サブクラス	デバイス記述子またはインターフェイス記述子のいずれかからのサブクラス。
プロトコル	デバイス記述子またはインターフェイス記述子のいずれかからのプロトコル。

例

Mode=00000004 VID=067B PID=1230 class=03 #キャプチャモードで動作する入力デバイス

Mode=00000002 VID=067B PID=1230 class=03 #対話モードで動作する入力デバイス（デフォルト）

Mode=00000001 VID=067B PID=1230 class=03 #最適化なしで動作する入力デバイス

Mode=00000100 VID=067B PID=1230 #デバイスセットアップの最適化が無効（デフォルト）

Mode=00000200 VID=067B PID=1230 #デバイスセットアップの最適化が有効

Wacom署名パッドデバイスのスクリーンセーバーを無効にする

Wacom署名パッドおよびタブレットを使用するには、Citrix®はスクリーンセーバーを次のように無効にすることをお勧めします。

1. デバイスをリダイレクトした後、**Wacom-STU-Driver**をインストールします。
2. 署名パッドのコントロールパネルにアクセスするには、**Wacom-STU-Display MSI**をインストールします。
3. **コントロールパネル > Wacom STU Display > STU430** または **STU530** に移動し、お使いのモデルのタブを選択します。
4. 「**変更**」を選択し、UACセキュリティウィンドウが表示されたら「**はい**」を選択します。
5. 「**スライドショーを無効にする**」を選択し、「**適用**」を選択します。

1つの署名パッドモデルに設定が適用されると、すべてのモデルに適用されます。

クライアントUSBデバイスのリダイレクト

この設定は、USBデバイスのユーザーデバイスとの間のリダイレクトを許可または禁止します。

デフォルトでは、USBデバイスはリダイレクトされません。

クライアントUSBデバイスリダイレクト規則

この設定は、USBデバイスのリダイレクトルールを指定します。

デフォルトでは、ルールは指定されていません。

ユーザーがUSBデバイスを接続すると、ホストデバイスは一致が見つかるまで各ポリシー規則と照合して確認します。いずれかのデバイスに対する最初の一致が最終的なものと見なされます。最初の一致が許可ルールである場合、デバイスは仮想デスクトップにリモート接続されます。最初の一致が拒否ルールである場合、デバイスはローカルデスクトップでのみ利用可能です。一致が見つからない場合、デフォルトのルールが使用されます。

ポリシー規則は、{Allow:|Deny:} の形式で、その後に空白で区切られたタグ=値の式が続きます。サポートされているタグは次のとおりです。

タグ名	説明
VID	デバイス記述子からのベンダーID
PID	デバイス記述子からの製品ID
REL	デバイス記述子からのリリースID
クラス	デバイス記述子またはインターフェース記述子のいずれかからのクラス
サブクラス	デバイス記述子またはインターフェース記述子のいずれかからのサブクラス
プロトコル	デバイス記述子またはインターフェイス記述子のいずれかからのプロトコル

ポリシー規則を作成する際は、次の点に注意してください。

- ルールでは大文字と小文字は区別されません。
- ルールには、# で始まるオプションのコメントを末尾に含めることができます。

- 空行および純粋なコメント行は無視されます。
- タグは一致演算子 = を使用する必要があります（例：VID=067B_）。
- 各ルールは新しい行から開始するか、セミコロンで区切られたリストの一部である必要があります。
- USB Implementers Forum, Inc. のWebサイトで利用可能なUSBクラスコードを参照してください。

管理者定義の USB ポリシールールの例:

- 許可: VID=067B PID=0007 # 別の産業、別のフラッシュドライブ
- 拒否: Class=08 subclass=05 # マスストレージ
- すべての USB デバイスを拒否するルールを作成するには、他のタグなしで「DENY:」を使用します。

クライアント USB プラグアンドプレイデバイスのリダイレクト

この設定は、カメラやPOS (Point-of-Sale) デバイスなどのプラグアンドプレイデバイスがクライアントセッションで使用されることを許可または禁止します。

デフォルトでは、プラグアンドプレイデバイスのリダイレクトは許可されています。「許可」に設定すると、特定のユーザーまたはグループのすべてのプラグアンドプレイデバイスがリダイレクトされます。「禁止」に設定すると、デバイスはリダイレクトされません。

USB デバイスの自動リダイレクトを構成する

USB サポートが有効になっている場合、USB デバイスは自動的にリダイレクトされます。また、USB ユーザー設定は USB デバイスを自動的に接続するように設定されています。

> **注:**

> Receiver for Windows 4.2 では、デスクトップアプライアンスモードで動作している場合も USB デバイスは自動的にリダイレクトされます。また、接続バーは表示されません。以前のバージョンの Citrix Receiver for Windows では、USB デバイスは以下のモードで動作している場合も自動的にリダイレクトされます。

> - デスクトップアプライアンスモード
> - 仮想マシン (VM) ホスト型アプリケーション

すべてのUSBデバイスをリダイレクトすることが常に最適とは限りません。ユーザーは、自動的にリダイレクトされないUSBデバイスリストからデバイスを明示的にリダイレクトできます。USBデバイスが一覧表示されたりリダイレクトされたりするのを防ぐには、クライアントエンドポイントまたはDDCポリシーのいずれかでDeviceRulesを使用します。詳細については、管理者ガイドを参照してください。

注意:

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

USBデバイスの自動リダイレクトに関するユーザー設定

ポリシー:

1. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrix Components > Citrix Receiver™ > リモートクライアントデバイス > Generic USB Remoting**に移動します。
2. **新しいUSBデバイス**を開き、**有効**を選択して、**OK**をクリックします。
3. 「**既存のUSBデバイス**」を開き、「**有効**」を選択して、「**OK**」をクリックします。

シトリックス レシーバー:

1. **Citrix Receiverの環境設定 > 接続**に移動します。
2. 次のオプションが選択されていることを確認します。
   - セッション開始時にデバイスを自動的に接続する
   - セッション実行中に新しいデバイスが接続された場合、デバイスを自動的に接続します。
3. 「**OK**」をクリックします。

すべてのレジストリキーとポリシーの変更は、Windowsクライアントデバイスに適用されます。

通常のUSBプリンターのリダイレクト

通常のUSBプリンターに最適なソリューションは、専用のユニバーサルプリンタードライバーと仮想チャネルを使用して印刷を実行することです。デフォルトでは、通常のUSBプリンターは自動的にリダイレクトされません。

通常のプリンターはヒューリスティックを使用して検出されます。また、例えばスキャン機能を備えた高度なプリンターは、完全に機能させるためにUSBサポートを使用してリダイレクトする必要がある場合があります。

通常のプリンターが自動的にリダイレクトされるかどうかを構成するには、このレジストリを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectPrinters

種類: DWORD

データ: 00000000

デフォルト値は0です（自動的にリダイレクトしません）。値を0より大きい任意の数値に変更すると、USBサポートが有効になり、通常のUSBプリンターをリダイレクトできるようになります。

このレジストリキーにActive Directoryポリシーを展開することもでき、両方が存在する場合は非ポリシー値を上書きします。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectPrinters

種類: DWORD

データ: 00000000

通常のオーディオデバイスのリダイレクト

通常のプリンターと同様に、通常のオーディオデバイスからオーディオデータを送信するには、ICA®の専用オーディオ仮想チャネルを使用することで最高のユーザーエクスペリエンスが得られます。ただし、USBサポートを使用して一部の特殊なデバイスをリダイレクトする必要がある場合があります。どのデバイスが通常のオーディオデバイスであるかを判断するためにヒューリスティックが使用されます。

クライアントエンドポイントでこのレジストリを使用し、通常のオーディオデバイスが自動的にリダイレクトされるかどうかを構成します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectAudio

種類: DWORD

データ: 00000000

デフォルトは0に設定されています（自動的にリダイレクトしません）。値を0以外に変更すると、USBサポートにより通常のUSBオーディオデバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値をレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectAudio

種類: DWORD

データ: 00000000

プレーンストレージデバイス（マスストレージデバイス）のリダイレクト

プレーンストレージデバイスの場合、最適化も実行するクライアントドライブマッピングなどの専用仮想チャネルを使用することで、最高のユーザーエクスペリエンスを実現できます。単純なファイルの読み書きに加えて、CD/DVDの書き込みや暗号化されたファイルシステムデバイスへのアクセスなどの特定の特殊なタスクを実行するには、汎用USBサポートを使用してデバイスをリダイレクトする必要がある場合があります。

どのデバイスがプレーンストレージデバイスであるかを判断するためにヒューリスティックが使用されます。プレーンストレージデバイスを自動的にリダイレクトするかどうかを構成するには、このレジストリキーを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectStorage

種類: DWORD

データ: 00000000

デフォルトは0に設定されています（自動的にリダイレクトされません）。値を0以外に変更すると、汎用USBサポートを使用してプレーンUSBストレージデバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値を以下のレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きすることもできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectStorage

種類: DWORD

データ: 00000000

> **注:**
>
> 汎用USBサポートを使用している場合、通常のストレージデバイスへの読み取り専用アクセスは構成できませんが、CDMを使用している場合は構成できます。

ハードウェア暗号化機能付きUSBフラッシュドライブのリダイレクト

ハードウェア暗号化されたUSBフラッシュドライブは通常、暗号化されたストレージパーティションと、暗号化されたパーティションをロック解除するためのユーティリティを含む2番目のユーティリティパーティションで構成されています。USBフラッシュドライブデバイスの場合、最適化も実行する専用のクライアントドライブマッピング/ダイナミックサムドライブマッピングHDX仮想チャネルを使用することで、最高のユーザーエクスペリエンスを実現できます。

汎用USBリダイレクトは、次の場合に必要です。

- Windows以外のクライアント (例: Linuxクライアント)
- 顧客がクライアント上のローカル機能へのユーザーアクセスを制限している（ロックダウンしている）クライアント

汎用USBリダイレクトは、ハードウェア暗号化なしで任意のUSBストレージデバイスをシングルセッションOSおよびマルチセッションOS VDAセッションの両方にリダイレクトできます。

Citrix Virtual Apps and Desktops 7 1808より前は、ハードウェア暗号化されたUSBフラッシュドライブをシングルセッションOSまたはマルチセッションOS VDAセッションに有用な方法でリダイレクトできませんでした。Citrix Virtual Apps and Desktops 7 1808で導入された新機能強化により、ハードウェア暗号化されたUSBフラッシュドライブの汎用USBリダイレクトがシングルセッションOSおよびマルチセッションOS VDAセッションでサポートされるようになりました。 デバイスがリダイレクトされた後、そのドライブはローカルクライアントに表示されません。そのため、ドライブのロック解除が必要な場合は、セッション内で実行してください。この機能にはWindows Update KB4074590が必要です。

通常の静止画像デバイス (スキャナーおよびデジタルカメラ)

通常の静止画像デバイスの場合、最適化も実行する専用の仮想チャネル（TWAIN仮想チャネルなど）を使用することで、最高のユーザーエクスペリエンスを実現できます。これらのデバイスは業

界標準に準拠している必要があります。デバイスが非準拠であるか、元の意図に従って使用されていないと見なされる場合、汎用USBリダイレクトがデバイスを使用する唯一の方法となる可能性があります。どのデバイスが通常の静止画像デバイスであるかを判断するためにヒューリスティックが使用されます。

通常の静止画像デバイスが自動的にリダイレクトされるかどうかを構成するには、このレジストリキーを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectImage

種類: DWORD

データ: 00000000

デフォルトは0に設定されています（自動的にリダイレクトされません）。値をゼロ以外に変更すると、汎用USBでプレーンなUSB静止画デバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値をこのレジストリキーに展開することもでき、両方が存在する場合は非ポリシー値を上書きします。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectImage

種類: DWORD

データ: 00000000

デバイス固有の設定

Citrix最適化可能デバイスを選択するために使用されるヒューリスティックは、必ずしもお客様の希望と一致するとは限りません。Citrix最適化可能デバイスの例としては、プリンター、オーディオ、ビデオ、ストレージ、静止画デバイスなどがあります。上記にリストされていないデバイスの自動リダイレクトを制御したい場合があります。自動リダイレクトはデバイス固有に制御できます。

例として、DemoTech 2,000バーコードリーダーはUSBサポートを使用してリダイレクトする必要はありません。ベンダー識別子12ABと製品識別子5678を持っています。これらの16進数はデバイスマネージャーで確認できます。

これが自動的にリダイレクトされるのを防ぐには、このデバイス固有のレジストリキーを作成します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名前: AutoRedirect

種類: DWORD

データ: 00000000

値が0の場合、デバイスは自動的にリダイレクトされません。0以外の値は、デバイスが自動リダイレクトの対象となる必要があることを示します（ユーザー設定による）。ベンダー識別子と製品識別子の間には、単一のスペース文字があります。

この値は、Active Directoryポリシーを使用してこのレジストリキーに展開することもできます。両方が存在する場合、非ポリシー値を上書きします。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名前: AutoRedirect

種類: DWORD

データ: 00000000

デバイス固有のAutoRedirect設定は、上記で説明したより一般的なAutoRedirectXXX値よりも優先されます。Citrix最適化デバイスのデフォルトのヒューリスティックは、デバイスを汎用として誤って解釈する可能性があります。したがって、デバイスを自動的にリダイレクトするには、デバイス固有のAutoRedirect値を1に設定します。

既存のUSBデバイスの自動接続を許可する

この設定は、セッション開始時にエンドポイントに接続されている既存のUSBデバイスのリモートセッションへの自動接続を許可または禁止します。

この設定をポリシーに追加するときは、次のいずれかのオプションを選択します。

- 利用可能なUSBデバイスをリダイレクトする前に確認する。
- 利用可能なUSBデバイスを自動的にリダイレクトしない。
- 利用可能なUSBデバイスを自動的にリダイレクトする。

デフォルトでは、**利用可能なUSBデバイスのリダイレクト前に確認する**オプションが選択されています。選択されたポリシーに基づいて、クライアントの**基本設定** > **デバイス**セクションで選択されたオプションが上書きされる場合があります。

> **注:**
>
> 現在、**既存のUSBデバイスの自動接続を許可する**ポリシーは、Windows向けCitrix Workspace™アプリにのみ適用されます。

新しく接続されたUSBデバイスの自動接続を許可する

この設定は、セッション中にエンドポイントに挿入されたUSBデバイスのリモートセッションへの自動接続を許可または禁止します。

この設定をポリシーに追加するときは、次のいずれかのオプションを選択します。

- 利用可能なUSBデバイスをリダイレクトする前に確認する。
- 利用可能なUSBデバイスを自動的にリダイレクトしない。
- 利用可能なUSBデバイスを自動的にリダイレクトします。

デフォルトでは、**利用可能なUSBデバイスのリダイレクト前に確認する**オプションが選択されています。選択されたポリシーに基づいて、クライアントの**基本設定** > **デバイス**セクションで選択されたオプションが上書きされる場合があります。

> **注:**
>
> 現在、**新しく接続されたUSBデバイスの自動接続を許可する**ポリシーは、Windows向けCitrix Workspaceアプリにのみ適用されます。

クライアントUSBデバイスリダイレクト規則 (バージョン2)

この設定は、USBデバイスをリモートセッションにフィルタリング、分割、および自動接続するためのルールを指定します。

この設定が選択されている場合、ホストは「*クライアントUSBデバイスリダイレクト規則*」設定を、この設定で構成されたデバイス規則で上書きします。

詳細については、「複合USBデバイスリダイレクトの構成」(/ja-jp/citrix-workspace-app-for-windows/configure.html#composite-usb-device-redirection)を参照してください。

仮想チャネル許可リストポリシー設定

仮想チャネル許可リストポリシー設定は、ICA®セッションで開くことが許可されている仮想チャネルを指定する許可リストの使用を有効にします。

無効にすると、すべての仮想チャネルが許可されます。

有効にすると、Citrix®仮想チャネルのみが許可されます。

カスタムまたはサードパーティの仮想チャネルを使用するには、仮想チャネルをリストに追加します。仮想チャネルをリストに追加するには：

1. 仮想チャネル名の後にコンマを入力します。
2. 仮想チャネルにアクセスするプロセスのパスを入力します。

複数の実行可能パスをリストでき、パスはコンマで区切られます。

例:

```
CTXCVC1,C:\VC1\vchost.exe
```

```
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```

Citrix Virtual Apps and Desktops 7 2109以降、仮想チャネル許可リストはデフォルトで有効になっています。許可リストに仮想チャネルを追加する方法の詳細については、「許可リストへの仮想チャネルの追加」を参照してください。

Skype for Business 用の HDX RealTime Optimization Pack を使用している場合は、仮想チャネルを許可リストに追加します。詳細については、「HDX RealTime Optimization Pack のドキュメント」を参照してください。

> **重要:**
>
> 設定を有効にするには、VDAマシンを再起動する必要があります。

> 仮想チャネルの詳細については、「ICA仮想チャネル」を参照してください。

仮想チャネル許可リストのログ記録

このポリシー設定を使用して、仮想チャネル許可リストのログ記録レベルを構成できます。

次のオプションが利用可能です。

オプション	説明
無効	すべてのログイベントを無効にします。

警告のみをログに記録	許可リストに含まれていない、開こうとするカスタム仮想チャネルに対してのみイベントがログに記録されます。
すべてのイベントをログに記録	すべてのイベントがログに記録されます

仮想チャネル許可リストのログスロットリング

このポリシー設定を使用して、アクティブなセッションのイベントログ記録の頻度を構成できます。

各仮想チャネルのすべてのイベントは、最初に発生したときにログに記録されます。セッションがアクティブな間、スロットリング期間中は繰り返し発生するイベントは抑制されます。セッションが切断された場合、スロットリング期間はリセットされます。

DVCの仮想チャネル許可リスト

ICAセッションで開くことを許可されている動的仮想チャネルを指定する許可リストの使用を有効にします。

無効にすると、すべての動的仮想チャネルが許可されます。

有効にすると、動的仮想チャネルは許可されません。この機能で動的仮想チャネル (DVC) を使用するには、DVCをリストに追加する必要があります。リストにDVCを追加するには、セッションホストでDVCにアクセスするプロセスのパスを入力し、その後にコンマ、次にクライアント側プラグイン名、その後にコンマ、そしてプラグインが使用するリスナー名を入力します。複数のリスナー名はコンマで区切って追加できます。

ワイルドカードを使用して、プラグインがサポートするすべてのリスナーを許可できます。

ワイルドカードを使用して、プロセスパス内の単一のディレクトリ名を置き換えたり、プロセスパス内のディレクトリ名の一部を置き換えたり、実行可能ファイル名を置き換えたり、実行可能ファイル名の一部を置き換えたりすることもできます。

この設定への変更は、セッションホストの再起動後にのみ適用されます。

例: クライアント側プラグイン: `DvcPlugin1.dll`, `DvcPlugin2.dll`, `DvcPlugin3.dll`

許可リストエントリ: `C:\Program Files\App\run1.2.exe,DvcPlugin1,` ListenerName1 `C:\Program Files*\run*.exe,DvcPlugin2,ListenerName1,ListenerName2` `C:\Program Files\App\run1.2.exe,DvcPlugin3,*`

視覚表示ポリシー設定

視覚表示セクションには、仮想デスクトップからユーザーデバイスに送信される画像の品質を制御するためのポリシー設定が含まれています。

シンプルなグラフィックの優先色深度

このポリシー設定は、VDAバージョン7.6 FP3以降で利用できます。8ビットオプションは、VDAバージョン7.12以降で利用できます。

この設定により、シンプルなグラフィックがネットワーク経由で送信される際の色深度を下げることができます。ピクセルあたり8ビットまたは16ビットに下げることで、低帯域幅接続での応答性が向上する可能性があります。ただし、この操作は画質のわずかな劣化を招く可能性があります。(/ja-jp/citrix-virtual-apps-desktops/2407/policies/reference/ica-policy-settings/graphics-policy-settings.html)ポリシー設定が**画面全体**に設定されている場合、8ビットの色深度はサポートされません。

デフォルトの優先色深度はピクセルあたり24ビットです。

8ビット設定がVDAバージョン7.11以前に適用された場合、VDAは24ビット（デフォルト）の色深度にフォールバックします。

ターゲットフレームレート

この設定は、仮想デスクトップからユーザーデバイスに送信される1秒あたりの最大フレーム数を指定します。

デフォルトでは、最大は1秒あたり30フレームです。

1秒あたりのフレーム数を高く設定する（例：30）と、ユーザーエクスペリエンスは向上しますが、より多くの帯域幅が必要になります。1秒あたりのフレーム数を減らす（例：10）と、ユーザーエクスペリエンスを犠牲にしてサーバーのスケーラビリティが最大化されます。CPUが遅いユーザーデバイスの場合は、ユーザーエクスペリエンスを向上させるために低い値を指定してください。

1秒あたりの最大サポートフレームレートは60です。

視覚品質

この設定は、ユーザーデバイスに表示される画像の希望する視覚品質を指定します。

デフォルトでは、この設定はMediumです。

画像の品質を指定するには、次のいずれかのオプションを選択します。

- **低** - 帯域幅が制限されたネットワークで、対話性のために視覚的な品質を犠牲にできる場合に推奨されます。
- **中** - ほとんどのユースケースで最高のパフォーマンスと帯域幅効率を提供します。
- **高** - 視覚的にロスレスな画質が必要な場合に推奨されます。
- **ロスレスにビルド** - ネットワークアクティビティが高い期間はロッシー画像をユーザーデバイスに送信し、ネットワークアクティビティが低下した後はロスレス画像を送信します。この設定により、帯域幅が制限されたネットワーク接続でのパフォーマンスが向上します。
- **常にロスレス** - 画像データの保持が不可欠な場合は、「**常にロスレス**」を選択して、ロッシーデータがユーザーデバイスに送信されないようにします。たとえば、画質の低下が許されないX線画像を表示する場合などです。

動的画像ポリシー設定

動的画像セクションには、動的画像の圧縮を削除または変更できる設定が含まれています。

最小画像品質

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、アダプティブディスプレイの許容される最小画像品質を指定します。使用される圧縮が少ないほど、表示される画像の品質は高くなります。超高、非常に高、高、標準、低の圧縮から選択します。

デフォルトでは、これは標準に設定されています。

動的画像圧縮

この設定は、アダプティブディスプレイが有効になっているかどうかを指定します。アダプティブディスプレイは、利用可能な帯域幅に基づいて、スライドショー内のビデオやトランジションスライドの画質を自動的に調整します。アダプティブディスプレイが有効になっている場合、ユーザーは品質の低下なしにスムーズに実行されるプレゼンテーションを見ることができます。

デフォルトでは、アダプティブディスプレイは有効になっています。

VDA バージョン 7.0 から 7.6 の場合、この設定はレガシーグラフィックモードが有効になっている場合にのみ適用されます。VDA バージョン 7.6 FP1 以降の場合、この設定はレガシーグラフィックモードが有効になっている場合、またはレガシーグラフィックモードが無効でビデオコーデックがグラフィックの圧縮に使用されていない場合に適用されます。

レガシーグラフィックモードが有効になっている場合、ポリシー変更を有効にするにはセッションを再起動する必要があります。アダプティブディスプレイはプログレッシブディスプレイと相互排他的です。アダプティブディスプレイを有効にするとプログレッシブディスプレイが無効にな

り、その逆も同様です。ただし、プログレッシブディスプレイとアダプティブディスプレイの両方を同時に無効にすることができます。プログレッシブディスプレイはレガシー機能であるため、XenApp または XenDesktop では推奨されません。プログレッシブしきい値レベルを設定すると、アダプティブディスプレイが無効になります。

プログレッシブ圧縮レベル

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定により、詳細度は低いものの、画像の初期表示が高速になります。

デフォルトでは、プログレッシブ圧縮は適用されません。

通常の非可逆圧縮設定で定義された、より詳細な画像は、利用可能になったときに表示されます。写真などの帯域幅を多く消費するグラフィックの表示を改善するには、非常に高いまたは超高圧縮を使用してください。

プログレッシブ圧縮を有効にするには、その圧縮レベルが「ロッシー圧縮レベル」設定よりも高くする必要があります。

注：プログレッシブ圧縮に関連する圧縮レベルの増加は、クライアント接続を介した動的画像のインタラクティブ性も向上させます。回転する3Dモデルのような動的画像の品質は、画像が動きを停止するまで一時的に低下し、その時点で通常の非可逆圧縮設定が適用されます。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮しきい値
- プログレッシブヘビーウェイト圧縮

プログレッシブ圧縮しきい値

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、プログレッシブ圧縮が適用される接続の最大帯域幅を1秒あたりのキロビットで表します。これは、この帯域幅以下のクライアント接続にのみ適用されます。

デフォルトでは、しきい値は1秒あたり2147483647キロビットです。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮しきい値
- プログレッシブヘビーウェイト圧縮

目標最小フレームレート

この設定は、低帯域幅の条件下で、動的画像に対してシステムが維持しようとする1秒あたりの最小フレームレートを指定します。

デフォルトでは、これは10fpsに設定されています。

VDAバージョン7.0から7.6では、この設定はレガシーグラフィックモードが有効な場合にのみ適用されます。VDAバージョン7.6 FP1以降では、この設定はレガシーグラフィックモードが無効または有効のいずれの場合でも適用されます。

> **注:**
>
> 目標最小フレームレートポリシーは非推奨となり、10 fpsに設定されています。これは、グラフィックステータスインジケーターの品質スライダーを使用してエンドユーザーが変更できます。

WebSocketsポリシー設定

「**WebSockets**」セクションには、Citrix Workspace™ app for HTML5 を使用して仮想デスクトップおよびホスト型アプリケーションにアクセスするためのポリシー設定が含まれています。WebSockets 機能は、ブラウザベースのアプリケーションとサーバー間の双方向通信を行うことで、セキュリティを向上させ、オーバーヘッドを削減します。この機能は、複数の HTTP 接続を開くことなくこれを実現します。

WebSockets接続

この設定では、WebSockets接続を許可または禁止します。

デフォルトでは、WebSocket接続は禁止されています。

WebSocketsポート番号

この設定では、受信 WebSocket 接続のポートを識別します。

デフォルトでは、値は8008です。

WebSockets信頼済みオリジンサーバーリスト

この設定では、通常は Citrix Workspace app for Web である、URL として表現された信頼済みオリジンサーバーのコンマ区切りリストを提供します。サーバーは、これらのアドレスのいずれかから発信された WebSockets 接続のみを受け入れます。

デフォルトでは、ワイルドカード * を使用して、すべての Citrix Workspace app for Web URL を信頼します。

リストにアドレスを入力する場合は、次の構文を使用します。

\<protocol>://\<ホストの完全修飾ドメイン名>:

プロトコルは HTTP または HTTPS である必要があります。ポートが指定されていない場合、HTTP にはポート 80 が使用され、HTTPS にはポート 443 が使用されます。

ワイルドカード `*` は URL 内で使用できますが、IP アドレスの一部としては使用できません (`10.105.*.*`)。

WIA デバイスのポリシー設定

WIA デバイスセクションには、Windows Image Acquisition (WIA) を使用したスキャナーリダイレクトを管理するためのポリシー設定が含まれています。

WIA リダイレクト

デジタルカメラやスキャナーなどのWIAデバイスは、WIAフレームワークを使用してサーバーでホストされている画像処理アプリケーションと通信します。この設定により、ユーザーデバイス上のWIAデバイスへのユーザーのアクセスを許可または禁止します。デフォルトでは、WIAリダイレクトは禁止されています。

WIA準拠デバイスについては、WIAデバイスを参照してください。

レジストリを介して管理されるHDX™機能

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

> レジストリエディターを開くには、サーバーで `regedit.exe` を実行します。次に、設定を追加または編集するレジストリキーに移動します。

デバイス

Bloombergキーボード

Citrix Virtual Apps and Desktops™は、Bloombergモデル4およびモデル3のスターボードキーボードをサポートしています。デフォルトでは、拡張Bloombergキーボードのサポートは無効になっています。

Bloombergキーボードのサポートを有効にするには、接続を開始する前にクライアントマシンで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB`
- **値の名前**: `EnableBloombergHID`
- **値の型**: `DWORD`
- **値のデータ**:
  - `0` - 無効
  - `1` - 有効

詳細については、「Bloombergキーボード」を参照してください。

マップされたクライアントドライブ

セキュリティ上の予防措置として、ユーザーがCitrix Virtual Apps and Desktopsにログオンすると、デフォルトでサーバーはユーザーの実行権限なしでクライアントドライブをマップします。ユーザーがマップされたクライアントドライブにある実行可能ファイルを実行できるようにするには、サーバーのレジストリを編集してこのデフォルトを上書きします。

アクセスを許可するには、次のレジストリ値を編集します（**CDMSettings**が存在しない場合は作成します）。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\CDMSettings`
- **値の名前**: `ExecuteFromMappedDrive`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 権限を許可
  - `0` - マップされたドライブでの権限を拒否

この変更は、レジストリを編集した後に接続されたセッションに適用されます。

Citrix Virtual Apps and Desktops 7 2006は、このレジストリの場所を含む最初のバージョンです。以前のバージョンのCitrix Virtual Apps and Desktopsでは、異なるレジストリの場所が使用されていました。

詳しくは、「」(/ja-jp/citrix-virtual-apps-desktops/2407/devices/client-drive-mapping.html)を参照してください。

マイクロソフト Surface Pro および Surface Book ペン

Citrix Virtual Apps and Desktopsは、Windows Inkベースのアプリケーションで標準のペン機能をサポートしています。デフォルトでは、この機能は有効になっています。

この機能を無効または有効にするには、次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent\PenApi`
- **値の名前**: `DisablePen`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 無効
  - `0` - 有効

詳細については、「Microsoft Surface Pro および Surface Book のペン」を参照してください。

Windows Image Acquisition アプリケーション許可リスト

この設定により、VDA 上のどのアプリケーションが Windows Image Acquisition スキャナーリダイレクトにアクセスできるかを制御できます。

デフォルトでは、どのアプリケーションも Windows Image Acquisition にアクセスできません。

VDA 上のアプリケーションに対して Windows Image Acquisition を調整するには、次のレジストリ設定を作成します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`
- **値の名前**: `WIAAllowedProcesses`

  WIAAllowedProcesses を選択して右クリックします。**新規 > 複数行文字列値** を選択し、新しい値の名前を **AllowProcesses** に変更します。
- 値のデータ: Windows Image Acquisition にアクセスできる各アプリケーションの完全なパスとプロセス名を入力します。各アプリケーションを新しい行に入力してください。

この設定への変更は、次回 VDA でセッションを起動したときに有効になります。

全般

HDX リデューサー

セッションホストで使用するHDX圧縮アルゴリズム（Reducer）のバージョンを設定できます。

シングルセッションVDAでReducer V4を有効にするには、次のレジストリ値を設定します。

キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\WDSettings` **値の名前**: `ReducerOverrideMask` **値の型**: `DWORD` **値のデータ**: `23` (10進数)

マルチセッションVDAでReducer V4を有効にするには、次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **値の名前**: `ReducerOverrideMask`
- **値の型**: `DWORD`
- **値のデータ**: `23` (10進数)

EDTタイムアウトの構成

VDAでEDTタイムアウトを5秒から25秒の任意の値に構成できます。デフォルトのEDTタイムアウト値は25秒です。

- **キー**: `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\Tds\udp\UDPStackParameters`
- **値の型**: `DWORD`
- **値の名前**: `edtConnectionTimeout`
- **値のデータ**: 5〜25秒の時間 (10進数)

Windows向けCitrix Workspace™アプリのタイムアウトも構成できます。

- **キー**: `HKLM\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\EDT`
- **値の型**: `String / REG_SZ`
- **値の名前**: `edtConnectionTimeout`
- **値のデータ**: 5〜25秒の時間 (10進数)

Rendezvousのバージョンを構成する

使用するRendezvousのバージョンを構成するには、次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`
- **値の型**: `DWORD`
- **値の名前**: `GctRegistration`
- **値のデータ**:
  - `1` - V2を有効にするには
  - `0` - V1を有効にするには

VDAへの自動ログオンを構成する

この設定により、Windows 10シングルセッションOSおよびマルチセッションOS VDAで、**常にパスワードを要求する** Microsoftポリシー設定を有効または無効にできます。

もし**常にパスワードを要求する**が有効になっている場合、ユーザーはリモートセッションを開始するときにVDAで資格情報を入力する必要があります。この設定が無効になっている場合、ユーザーはVDAで資格情報を提供することなく、自動的にリモートセッションに接続します。

デフォルトでは、Microsoftポリシー設定は無効になっています。**常にパスワードを要求する**設定を有効または無効にするには、VDAで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Portica`
- **値の名前**: `AutoLogon`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - Microsoftポリシー設定を無効にし、ユーザーがリモートセッションに自動的にサインインできるようにします。
  - `0` – Microsoftポリシー設定を有効にし、ユーザーがリモートセッションを起動するときに資格情報の入力を求めます。

タイムアウト警告を無効にする

デフォルトでは、非アクティブまたはアイドル状態のセッションを持つユーザーは、セッションが自動的に切断される2分前に警告メッセージを受け取ります。

この設定は、以下の環境でアイドルセッションのタイムアウト制限に達したユーザーに対する警告メッセージを無効にし、削除します。

- ウィンドウズ サーバー 2004
- Windows 10マルチセッション2004以降のマルチセッションOS

警告を削除するには、VDAで以下のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\ICA-CGP`
- **値の名前**: `fEnableTimeoutWarning`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 警告メッセージを無効にする
  - `0` - 警告メッセージを有効にする

警告メッセージを表示するには、レジストリ値を削除するか、`0`に設定します。

EDT MTU検出

MTU検出により、EDTはセッション確立時に最大転送単位（MTU）を自動的に決定できます。これにより、パフォーマンスの低下やセッション確立の失敗につながる可能性のあるEDTパケットの断片化を防ぎます。

この設定はデフォルトで有効になっています。EDT MTU検出を無効にするには、以下のレジストリ値を構成し、VDAを再起動します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **値の名前**: `MtuDiscovery`
- **値の型**: `DWORD`
- **値のデータ**: `0`

この設定はマシン全体に適用され、サポートされているクライアントから接続するすべてのセッションに影響します。

一般的なコンテンツリダイレクト

ホストからクライアントへのリダイレクト用のURLタイプを追加する

デフォルトでは、HTTP、HTTPS、RTSP、RTSPU、PNM、MMSのURLタイプのリダイレクトをサポートしています。Windowsクライアントで以下のレジストリキーと値を作成することで、URLタイプをリストに追加できます。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA`
- **値の名前**: `ExtraURLProtocols`
- **値の型**: `REG_SZ`
- **値のデータ**: 必要なURLタイプをセミコロンで区切って指定します。URLの権限部分より前のすべてを含めます。例: `ftp://;mailto:;customtype1://;custometype2://`

URLタイプはWindowsクライアントにのみ追加できます。このレジストリ設定がないクライアントは、Citrixセッションへのリダイレクトを拒否します。クライアントには、指定されたURLタイプを処理するようにインストールおよび構成されたアプリケーションが必要です。

詳細については、「ホストからクライアントへのリダイレクト」を参照してください。

クライアントフォルダーリダイレクト

クライアントフォルダーリダイレクトは、クライアント側のファイルがホスト側のセッションでアクセスされる方法を変更します。サーバーでクライアントフォルダーリダイレクトを有効にし、ユーザーがユーザーデバイスでそれを構成した場合を考えてみましょう。この場合、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

サーバーでクライアントフォルダーリダイレクトを有効にするには、以下のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection`
- **値の名前**: `CFROnlyModeAvailable`
- **値の型**: `DWORD`
- **値のデータ**: `1`

詳細については、「クライアントフォルダーリダイレクト」を参照してください。

特定のWebサイトセットに対するホストからクライアントへのリダイレクト

特定のWebサイトセットに対してホストからクライアントへのリダイレクトを有効にするには、サーバーVDAで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- **値の名前**: `ValidSites`
- **値の型**: `REG_MULTI_SZ`
- **値のデータ**: 完全修飾ドメイン名 (FQDN) の任意の組み合わせを指定します。複数のFQDNを別々の行に入力します。プロトコル (`http://` または `https://`) なしで、FQDNのみを含

めます。FQDNには、最も左の位置にのみアスタリスク (`*`) をワイルドカード文字として含めることができます。このワイルドカードは、RFC 6125のルールと一致する単一レベルのドメインに一致します。例:

`www.example.com`

`*.example.com`

詳細については、「ホストからクライアントへのリダイレクト」を参照してください。

ログオフ時および切断時のローカルアプリケーションの動作

デフォルトでは、ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは実行を継続します。再接続後、ローカルアプリケーションが仮想デスクトップで利用可能な場合、それらは再統合されます。ログオフ時および切断時のローカルアプリケーションの動作を構成するには、ホストされているデスクトップで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies`
- **値の名前**: `Session State`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは引き続き実行されます。再接続すると、ローカルアプリケーションが仮想デスクトップで利用可能な場合、再統合されます。
  - `3` - ユーザーが仮想デスクトップからログオフまたは切断すると、ローカルアプリケーションは閉じます。

詳しくは、「Local App Access and URL redirection」を参照してください。

ホストからクライアントへのリダイレクトのデフォルトリストからURLタイプを削除する

デフォルトのリダイレクトリストからURLタイプを削除するには、サーバーVDAで以下のレジストリキーと値を作成します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- **値の名前**: `DisableServerFTA`
- **値の型**: `DWORD`
- **値のデータ**: `1`

- **値の名前**: `NoRedirectClasses`
- **値の型**: `REG_MULTI_SZ`
- **値のデータ**: 以下の値の任意の組み合わせを指定します: `http`、`https`、`rtsp`、`rtspu`、`pnm`、または`mms`。複数の値を入力する場合は、別々の行に入力します。例:

`http`

`https`

`rtsp`

詳細については、「ホストからクライアントへのリダイレクト」を参照してください。

サーバーVDAのデフォルトブラウザ構成

ホストからクライアントへのリダイレクトを有効にすると、サーバーVDA上のデフォルトのブラウザ構成を上書きできます。Web URLがリダイレクトされない場合、Citrixランチャーは、`command_backup`レジストリキーで構成されたブラウザにURLを渡します。このキーはデフォルトでInternet Explorerを指しますが、別のブラウザへのパスを含むように変更できます。

- Internet Explorer (デフォルト)
  - **キー**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"c:\program files\internet explorer\iexplore.exe" "%1"`
  - **キー**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"c:\program files\internet explorer\iexplore.exe" "%1"`
- グーグル クローム
  - **キー**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "%1"`

  - **キー**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "%1"`

- マイクロソフト エッジ
  - **キー**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "%1"`
  - **キー**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "%1"`

公開アプリケーションのローカルアプリアクセス

ローカルアプリアクセスは、ローカルにインストールされたWindowsアプリケーションを、デスクトップを切り替えることなくホストされたデスクトップ環境にシームレスに統合します。公開アプリケーションへのアクセスを提供するには、サーバーで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio`
- **値の名前**: `ClientHostedAppsEnabled`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 有効
  - `0` - 無効

詳細については、ローカルアプリアクセスとURLリダイレクトを参照してください。

グラフィック

CUDAまたはOpenCLアプリケーションのGPUアクセラレーション

ユーザーセッションで実行されているCUDAおよびOpenCLアプリケーションのGPUアクセラレーションは、デフォルトで無効になっています。

CUDAアクセラレーションPOC機能を使用するには、次のレジストリ設定を有効にします。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- **値の名前**: `CUDA`
- **値の型**: `DWORD`
- **値のデータ**: `00000001`

OpenCLアクセラレーションPOC機能を使用するには、次のレジストリ設定を有効にします。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- **値の名前**: `OpenCL`
- **値の型**: `DWORD`
- **値のデータ**: `00000001`

詳しくは、「WindowsマルチセッションOSのGPUアクセラレーション」を参照してください。

プログレッシブモード

プログレッシブモードはデフォルトで無効になっています。以下のレジストリ値でプログレッシブモードの状態を変更できます:

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics`
- **値の型**: `REG_DWORD`
- **値の名前**: `ProgressiveDisplay`
- **値のデータ**:
  - `0` - 常にオフ (プログレッシブモードを無効にします。この値がデフォルトです。)
  - `1` - 自動 (ネットワークの状態に基づいて切り替えます。)
  - 2 = 常にオン

詳細については、プログレッシブモードを参照してください。

> **注:**
>
> プログレッシブモードは非推奨になりました。Thinwireは、画像の配信を最適化し、キャッシュ効率を維持しながら、プログレッシブモードのほぼすべての利点を提供する代替オプションです。

Windows Presentation Foundation (WPF) レンダリング

HDX 3D Proを使用すると、Windows Multi-session OSセッションで実行されているグラフィックを多用するアプリケーションを、サーバーのグラフィック処理ユニット (GPU) でレンダリングできます。Windows Presentation Foundation (WPF) レンダリングをサーバーのGPUに移行することで、グラフィックレンダリングがサーバーのCPUを遅くすることはありません。

サーバーのGPUを使用してWPFアプリケーションのレンダリングを有効にするには、Windows multi-session OSを実行しているサーバーのレジストリに次の設定を作成します。

1. VDAでレジストリエディターを開き、次のキーに移動します。

   ```
   HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper
   ```

2. 次のレジストリ値を作成または編集します。

   - AdapterHandle = 0x00000001
   - DevicePath = 0x00000001
   - フラグ = 0x00000412
   - WPF = 0x00000001

3. WPFアプリの実行可能ファイル名でサブキーを作成します。たとえば、アプリが「mywpfapp.exe」という名前の場合、次のキーを作成します。

   ```
   HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper\mywpfapp.exe
   ```

4. 設定を有効にするには、サーバーを再起動します。

詳細については、WindowsマルチセッションOSでのGPUアクセラレーション および Windowsマルチセッション OSでWPFアプリを最大限に活用する のブログを参照してください。

マルチメディア

マルチメディア会議中のエコーを回避する

Citrix Virtual Apps and Desktopsは、エコーを最小限に抑えるエコーキャンセルオプションを提供します。この機能はデフォルトで有効になっています。エコーキャンセルを無効にするには、次のいずれかのレジストリ設定を変更できます。

- **キー**:
  - 32ビット: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
  - 64ビット: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
- **値の名前**: `EchoCancellation`
- **値の型**: `String/REG_SZ`
- **値のデータ**: `False`

詳細については、オーディオ機能を参照してください。

オーディオの制限

クライアントにオーディオデバイスをインストールし、オーディオリダイレクトを有効にしてRDSセッションを開始した後、オーディオファイルが再生されない場合があります。回避策として、RDSマシンに次のレジストリキーを追加し、マシンを再起動してください。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig`
- **値の名前**: `EnableSvchostMitigationPolicy`
- **値の型**: `DWORD`
- **値のデータ**: `0`

詳細については、オーディオ機能を参照してください。

ブラウザーコンテンツリダイレクトとDPI

ユーザーのマシンでDPI（スケーリング）が100%を超えて設定されている状態でブラウザーコンテンツリダイレクトを使用すると、リダイレクトされたブラウザーコンテンツ画面が正しく表示されません。この問題を回避するには、ユーザーのマシンに次のレジストリ値を作成して、ChromeのブラウザーコンテンツリダイレクトGPUアクセラレーションを無効にします。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream`

- **値の名前**: `GPU`
- **値の型**: `DWORD`
- **値のデータ**: `0`

詳しくは、「ブラウザコンテンツリダイレクトとDPI」(/ja-jp/citrix-virtual-apps-desktops/2407/multimedia/browser-content-redirection.html#browser-content-redirection-and-dpi)を参照してください。

高解像度ウェブカメラの解像度

メディアタイプのネゴシエーションが失敗した場合、HDXはデフォルトのVGA解像度（640 x 480ピクセル）にフォールバックします。クライアントのレジストリキーを使用して、デフォルトの解像度を構成できます。以下のレジストリキーを設定する前に、カメラが指定された解像度をサポートしていることを確認してください。

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- 幅
  - **値の名前**: `DefaultWidth`
  - **値の型**: `DWORD`
  - **値のデータ**: 10進数での希望の幅（例: 1280）
- 高さ
  - **値の名前**: `DefaultHeight`
  - **値の型**: `DWORD`
  - **値のデータ**: 10進数での希望の高さ（例: 720）

Microsoft Teamsのフォールバックモード

Microsoft Teamsが最適化されたVDIモードでロードに失敗した場合（Teams/バージョン情報/バージョンで「Citrix HDX Not Connected」と表示される場合）、VDAはウェブカメラリダイレクトやクライアントオーディオおよびマイクのリダイレクトなどのレガシーHDXテクノロジーにフォールバックします。Microsoft Teamsの最適化をサポートしないWorkspaceアプリのバージョン/プラットフォームOSを使用している場合、フォールバックレジストリキーは適用されません。

フォールバックメカニズムを制御するには、VDAで以下のいずれかのレジストリ値を設定します:

- **キー** (いずれか1つのみ必要):
  - **コンピューター設定:** `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams`

  - **ユーザー設定:** `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Teams`

- **値の名前**: `DisableFallback`
- **値の型**: `DWORD`
- 値のデータ:

  - `1` - フォールバックモードを無効にする
  - `2` - オーディオのみを有効にする

値が存在しないか0に設定されている場合、フォールバックモードが有効になります。この機能には、Microsoft Teamsバージョン1.3.0.13565以降が必要です。詳細については、「Microsoft Teamsの最適化」を参照してください。

Citrix App Layering™を使用したMicrosoft Teamsの最適化

異なるレイヤーでVDAとMicrosoft Teamsのインストールを管理するためにCitrix App Layeringを使用している場合、コマンドラインから`ALLUSER=1`フラグを使用してMicrosoft Teamsをインストールする前に、Windows上に**PortICA**という名前の空のレジストリキーを作成します。デフォルトの値の名前、型、データはそのままにしておきます。

- レジストリエディターの32ビット版のキー:
  `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA`
- レジストリエディターの64ビット版のキー:
  `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

詳細については、「Microsoft Teamsの最適化」を参照してください。

ブラウザコンテンツリダイレクトでの統合Windows認証によるシングルサインオン

この設定により、VDA と同じドメイン内で統合 Windows 認証 (IWA) が構成された Web サーバーへのシングルサインオンが提供されます。シングルサインオンを有効にするには、次のレジストリ値を 1 に設定します。

- **キー**:

  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream`

  または

  - `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\HdxMediastream`

- **値の名前**: `WebBrowserRedirectionIwaSupport`
- **値の型**: `DWORD`

- **値のデータ**: `1`

詳細については、「統合 Windows 認証によるシングルサインオン」を参照してください。

ユーザーエージェント要求ヘッダー

ユーザーエージェントヘッダーは、ブラウザーコンテンツリダイレクトから送信される HTTP 要求を識別するのに役立ちます。この設定は、プロキシとファイアウォールルールを構成する際に役立ちます。たとえば、サーバーがブラウザーコンテンツリダイレクトから送信される要求をブロックする場合、ユーザーエージェントヘッダーを含むルールを作成して、特定の要件をバイパスできます。ユーザーエージェント要求ヘッダーは、Windows デバイスのみがサポートしています。

デフォルトでは、ユーザーエージェント要求ヘッダーストリングは無効になっています。クライアントでレンダリングされるコンテンツのユーザーエージェントヘッダーを有効にするには、レジストリエディターを使用します。

各 Citrix Workspace アプリ for Windows クライアントで、次のいずれかのレジストリ設定を行います。

- **キー**:
  - 32ビット: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStream`
  - 64ビット: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream`
- **値の名前**: `EnableCefUserAgentString`
- **値の型**: `DWORD`
- **値のデータ**: `1`

レジストリ値を追加すると、ユーザーエージェントヘッダーにはCitrixBCR/2102.1というテキストが含まれます。ここで、2102.1はWindows版Citrix Workspaceアプリのバージョンです。

Webカメラのソフトウェア圧縮

Webカメラがハードウェアエンコードをサポートしている場合、HDXビデオ圧縮はデフォルトでハードウェアエンコードを使用します。ハードウェアエンコードは、ソフトウェアエンコードよりも多くの帯域幅を消費する可能性があります。ソフトウェア圧縮を強制するには、クライアントに次の値を追加します。

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HdxRealTime`
- **値の名前**: `DeepCompress_ForceSWEncode`
- **値の型**: `DWORD`

- **値のデータ**: `1`

詳細については、「」を参照してください(/ja-jp/citrix-virtual-apps-desktops/2407/multimedia/webcam-compression.html)。

Webカメラのビデオ圧縮

HDX Webカメラビデオ圧縮は、H.264ビデオを仮想セッションで実行されているビデオ会議アプリケーションに直接送信します。VDAリソースを最適化するために、HDX Webカメラ圧縮はWebカメラビデオのエンコード、トランスコード、デコードを行いません。この機能はデフォルトで有効になっています。

サーバーからビデオ会議アプリへの直接ビデオストリーミングを無効にするには、VDAで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime`
- **値の名前**: `OfferH264ToApp`
- **値の型**: `DWORD`
- **値のデータ**: `0`

詳細については、HDX webcam video compressionを参照してください。

Webカメラビデオ圧縮フレームレート

優先するビデオフレームレートを調整するには、クライアントで以下のレジストリ値を編集します。

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- **値の名前**: `FramesPerSecond`
- **値の型**: `DWORD`
- **値のデータ**: `15`

ウェブカメラが指定されたフレームレートをサポートしていない場合、アプリケーションはデフォルトで15 FPSを使用します。

詳細については、HDXウェブカメラビデオ圧縮を参照してください。

ロード管理ポリシー設定

「**負荷管理**」セクションには、WindowsマルチセッションOSマシンを提供するサーバー間の負荷管理を有効にして構成するためのポリシー設定が含まれています。

ロード評価インデックスの計算については、CTX202150を参照してください。

同時ログオン許容数

この設定は、サーバーが受け入れ可能な同時ログオンの最大数を指定します。

デフォルトでは、この値は2に設定されています。

この設定が有効になっている場合、負荷分散は、指定された数を超えるログオンがサーバーVDAで同時にアクティブにならないように試みます。ただし、この制限は厳密には適用されません。制限を適用し（指定された数を超える同時ログオンを失敗させる）、次のレジストリキーを作成します。

> HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit 種類: DWORD 値: 1

CPU使用率

この設定は、サーバーがフルロードを報告するCPU使用率のレベルをパーセンテージで指定します。有効にすると、サーバーがフルロードを報告するデフォルト値は90%です。

デフォルトでは、この設定は無効になっており、CPU使用率は負荷計算から除外されます。

CPU使用率から除外されるプロセスの優先度

> **注:**

> Workspace Environment Managementがマシンを管理するシナリオでは、この設定をCPU Priority設定と併用すると、意図しない結果が生じる可能性があります。CPU Priority設定を使用する場合は、この設定を無効にすることをお勧めします。

> この設定は、プロセスのCPU使用率がCPU使用率負荷インデックスから除外される優先度レベルを指定します。

デフォルトでは、この値は**標準以下**または**低**に設定されています。

ディスク使用量

この設定は、サーバーが75%のフルロードを報告するディスクキューの長さを指定します。有効にすると、ディスクキューの既定値は8です。

デフォルトでは、この設定は無効になっており、ディスク使用率は負荷計算から除外されます。

セッションの最大数

この設定は、サーバーがホストできるセッションの最大数を指定します。有効にすると、サーバーがホストできるセッションの最大数のデフォルト設定は250になります。

デフォルトでは、この設定は有効になっています。

メモリ使用量

この設定は、サーバーがフルロードを報告するメモリ使用量のレベルをパーセンテージで指定します。有効にすると、サーバーがフルロードを報告するデフォルト値は90%になります。

デフォルトでは、この設定は無効になっており、メモリ使用量は負荷計算から除外されます。

メモリ使用量のベースロード

この設定は、ベースオペレーティングシステムのメモリ使用量の近似値を指定します。また、サーバーがゼロロードと見なされるメモリ使用量をMB単位で定義します。

デフォルトでは、この値は768 MBに設定されています。

プロファイル管理ポリシー設定

高度なポリシー設定

ロックされたファイルへのアクセス時の再試行回数

ロックされたファイルへのアクセス時の再試行回数を設定します。

このポリシーが無効になっている場合、デフォルト値の5回の再試行が使用されます。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここで、または.iniファイルで構成されていない場合、デフォルト値が使用されます。

ログオフ時にインターネットCookieファイルを処理する

一部の展開では、`Index.dat`が参照しない余分なインターネットCookieが残されます。継続的なブラウジングの後、ファイルシステムに残された余分なCookieは、プロファイルの肥大化につながる可能性があります。このポリシーを使用すると、Profile Managementを有効にしてIndex.datの処理を強制し、余分なCookieを削除できます。このポリシーはログオフ時間を増加させるため、この問題が発生した場合にのみ有効にしてください。

このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここで、または.iniファイルで構成されていない場合、Index.datの処理は行われません。

自動構成を無効にする

Profile Managementは、Citrix Virtual Desktops™環境（パーソナルvDiskの有無など）を検査し、それに応じてグループポリシーを構成します。「未構成」状態のProfile Managementポリシーのみが調整されるため、行ったカスタマイズはすべて保持されます。

このポリシーにより、展開を高速化し、最適化を簡素化できます。このポリシーを構成する必要はありません。ただし、次のいずれかの操作を行う場合は、自動構成を無効にできます。

- 以前のバージョンからの設定を保持するためにアップグレードする場合
- トラブルシューティング時

自動構成は、実行時に環境に応じてデフォルトのポリシー設定を自動的に構成する動的な構成チェッカーと見なすことができます。これにより、設定を手動で構成する必要がなくなります。実行時環境には以下が含まれます。

- Windows オペレーティングシステム
- Windows OSのバージョン
- Citrix Virtual Desktops が存在すること
- パーソナルvDiskの存在

環境が変更された場合、自動構成によって以下のポリシーが変更される可能性があります。

- アクティブライトバック
- 常にキャッシュ
- ログオフ時にローカルにキャッシュされたプロファイルを削除
- キャッシュされたプロファイルを削除するまでの遅延
- プロファイルストリーミング

さまざまなOSでのポリシーのデフォルトステータスについては、以下の表を参照してください。

	マルチセッションOS	シングルセッションOS
アクティブライトバック	有効	Personal vDiskが使用されている場合は*無効*。それ以外の場合は有効。
常にキャッシュ	無効	Personal vDisk が使用されている場合は*無効*。それ以外の場合は有効。

	マルチセッションOS	シングルセッションOS
ログオフ時にローカルにキャッシュされたプロファイルを削除	有効	次のいずれかの状況が発生した場合は*無効*：Personal vDisk が使用されている、Citrix Virtual Desktops が割り当てられている、または Citrix Virtual Desktops がインストールされていない。それ以外の場合は有効。
キャッシュされたプロファイルを削除するまでの遅延	0 秒	ユーザーの変更が永続的でない場合は 60 秒。それ以外の場合は 0 秒。
プロファイルストリーミング	有効	Personal vDisk が使用されている場合は*無効*。それ以外の場合は有効。

ただし、自動構成が無効になっている場合、上記のすべてのポリシーは既定で**無効**になります。

重要:

Personal vDisk は非推奨です。詳細については、PVD、AppDisk、およびサポートされていないホストの削除を参照してください。

Profile Management 1909 以降、Windows 10 (バージョン 1607 以降) のスタートメニューで改善されたエクスペリエンスを得ることができます。この改善は、以下のポリシーの自動構成によって実現されます:

- 「`Appdata\Local\Microsoft\Windows\Caches` と `Appdata\Local\Packages`」を「**ミラーリングするフォルダー**」に追加します。
- 「`Appdata\Local\Microsoft\Windows\UsrClass.Dat*`」を「**同期するファイル**」に追加します。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がここで構成されておらず、.ini ファイルでも構成されていない場合、自動構成がオンになります。この場合、環境が変更されると、Profile Management の設定が変更される可能性があります。

問題が発生した場合にユーザーをログオフする

問題が発生した場合に Profile Management がユーザーをログオフするかどうかを指定できます。

このポリシーが無効になっているか、構成されていない場合、問題が発生すると Profile Management は一時プロファイルをユーザーに提供します。たとえば、ユーザー ストアが利用できない場合などです。

有効になっている場合、エラーメッセージが表示され、ユーザーはログオフされます。この設定により、問題のトラブルシューティングが簡素化されます。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がここで構成されておらず、.ini ファイルでも構成されていない場合、一時プロファイルが提供されます。

カスタマー エクスペリエンス向上プログラム

デフォルトでは、匿名統計と使用状況データを収集することにより、Citrix® 製品の品質とパフォーマンスを向上させるために、カスタマーエクスペリエンス向上プログラムが有効になっています。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

Outlook の検索インデックスローミングを有効にする

ユーザープロファイルとともに Outlook 検索データを自動的にローミングすることで、ユーザーベースの Outlook 検索エクスペリエンスを可能にします。この機能には、Outlook の検索インデックスを保存するために、ユーザー ストアに追加の領域が必要です。

このポリシーを有効にするには、ログオフしてから再度ログオンしてください。

Outlook 検索インデックス データベース – バックアップと復元

Outlookの検索インデックスローミングを有効にするポリシーが有効になっている場合に、ログオン中にProfile Managementが何を行うかを指定できます。

このポリシーが有効になっている場合、Profile Managementは、ログオン時にデータベースが正常にマウントされるたびに、検索インデックスデータベースをバックアップします。Profile Managementは、そのバックアップを検索インデックスデータベースの正常なコピーとして扱いま

す。データベースの破損により検索インデックスデータベースのマウントが失敗した場合、Profile Managementは検索インデックスデータベースを最後に確認された正常なコピーに戻します。

> 注：
>
> 新しいバックアップが正常に保存されると、Profile Managementは以前に保存されたバックアップを削除します。バックアップは利用可能なVHDXストレージを消費します。

OUTLOOK検索データローミングの同時セッションサポートを有効にする

Profile Managementが、同じユーザーの同時セッションでネイティブのOutlook検索エクスペリエンスを提供できるようにします。このポリシーは、Outlookの検索インデックスローミングポリシーと組み合わせて使用します。

このポリシーを有効にすると、同時セッションごとに個別のOutlook OSTファイルが使用されます。

デフォルトでは、Outlook OSTファイルを保存するために使用できるVHDXディスクは2つだけです（ディスクごとに1ファイル）。ユーザーがさらにセッションを開始した場合、そのOutlook OSTファイルはローカルユーザープロファイルに保存されます。Outlook OSTファイルを保存するためのVHDXディスクの最大数を指定できます。

ONEDRIVEコンテナを有効にする

OneDriveフォルダーをユーザーとともにローミングできるようにします。

OneDriveコンテナは、VHDXベースのフォルダーローミングソリューションです。Profile Managementは、ファイル共有上にユーザーごとにVHDXファイルを作成し、ユーザーのOneDriveフォルダーをVHDXファイルに保存します。VHDXファイルは、ユーザーがログオンするときにアタッチされ、ログオフするときにデタッチされます。

UWPアプリのローミング

UWP（Universal Windows Platform）アプリをユーザーとともにローミングできるようにします。これにより、ユーザーは異なるデバイスから同じUWPアプリにアクセスできます。

このポリシーを有効にすると、Profile ManagementはUWPアプリを個別のVHDXディスクに保存することで、ユーザーと共にローミングできるようにします。これらのディスクはユーザーログオン時にアタッチされ、ユーザーログオフ時にデタッチされます。

構成の優先順位:

この設定がここで構成されていない場合、.iniファイルの値が使用されます。 この設定がここで、または.iniファイルで構成されていない場合、この機能は無効になります。

ログオン時のユーザーグループポリシーの非同期処理を有効にする

Windowsは、ユーザーグループポリシーに同期モードと非同期モードの2つの処理モードを提供します。Windowsは、次のユーザーログオンの処理モードを決定するためにレジストリ値を使用します。レジストリ値が存在しない場合、同期モードが適用されます。レジストリ値はマシンレベルの設定であり、ユーザーと共にローミングしません。したがって、ユーザーが次の場合、非同期モードは期待どおりに適用されません。

- 異なるマシンにログオンする。
- ログオフ時にローカルにキャッシュされたプロファイルを削除するポリシーが有効になっている同じマシンにログオンする。

このポリシーを有効にすると、レジストリ値はユーザーと共にローミングします。その結果、ユーザーがログオンするたびに処理モードが適用されます。

VHDディスクの圧縮をトリガーする空き領域の比率

VHDディスクの圧縮を有効にする が有効な場合に適用されます。VHDディスクの圧縮をトリガーする空き領域の比率を指定できます。ユーザーログオフ時に空き領域の比率が指定された値を超えると、ディスクの圧縮がトリガーされます。

空き領域の比率 = (現在のVHDファイルサイズ – 必要な最小VHDファイルサイズ*) ÷ 現在のVHDファイルサイズ

* Microsoft Windowsオペレーティングシステムの `MSFT_Partition` クラスのGetSupportedSizeメソッドを使用して取得されます。

VHDディスクの圧縮をトリガーするログオフ回数

VHDディスクの圧縮を有効にする が有効な場合に適用されます。VHDディスクの圧縮をトリガーするユーザーログオフ回数を指定できます。

最後の圧縮以降のログオフ回数が指定された値に達すると、ディスク圧縮が再度トリガーされます。

VHDディスク圧縮のデフラグを無効にする

VHDディスク圧縮を有効にする が有効な場合に適用されます。VHDディスク圧縮のファイルデフラグを無効にするかどうかを指定できます。

VHDディスク圧縮が有効な場合、VHDディスクファイルはまずWindowsに組み込まれている `defrag` ツールを使用して自動的にデフラグされ、その後圧縮されます。VHDディスクのデフラグはより良い圧縮結果をもたらしますが、無効にするとシステムリソースを節約できます。

プロファイルコンテナのマルチセッションライトバックを有効にする

マルチセッションシナリオでプロファイルコンテナのライトバックを有効にします。有効にすると、すべてのセッションでの変更がプロファイルコンテナに書き戻されます。無効にすると、プロファイルコンテナでは最初のセッションのみが読み取り/書き込みモードであるため、最初のセッションでの変更のみが保存されます。Citrix Profile Managementプロファイルコンテナは Citrix Profile Management 2103以降でサポートされています。FSLogix Profile ContainerはCitrix Profile Management 2003以降でサポートされています。

FSLogix Profile Containerでこのポリシーを使用するには、以下の前提条件が満たされていることを確認してください。

- FSLogix Profile Container機能がインストールされ、有効になっていること。
- FSLogixでプロファイルタイプが **読み取り/書き込みプロファイルを試行し、読み取り専用にフォールバックする** に設定されていること。

ユーザーストアをレプリケートする

リモートユーザープロファイルストアを、ログオンおよびログオフごとに複数のパスにレプリケートできます。これにより、Profile Managementはユーザーログオンのプロファイル冗長性を提供できます。

このポリシーを有効にすると、システムI/Oが増加し、ログオフ時間が長くなる可能性があります。

> **注:**
>
> この機能は、ファイルベースとコンテナベースの両方のプロファイルソリューションで利用できます。

ユーザーストアへの資格情報ベースのアクセスを有効にする

デフォルトでは、Citrix Profile Managementは現在のユーザーを偽装してユーザーストアにアクセスします。ユーザーストアへのアクセス時にProfile Managementが現在のユーザーを偽装しないようにする場合は、この機能を有効にしてください。現在のユーザーがアクセス権を持たないストレージリポジトリ（Azure Filesなど）にユーザーストアを配置できます。

Profile Managementがユーザー ストアにアクセスできるようにするには、プロファイルストレージサーバーの資格情報をWorkspace Environment Management™ (WEM) またはWindows資格情報マネージャーに保存します。Profile Managementが実行される各マシンで同じ資格情報を構成する必要をなくすために、Workspace Environment Managementを使用することをお勧めします。Windows資格情報マネージャーを使用する場合は、ローカルシステムアカウントを使用して資格情報を安全に保存してください。

> **注:**
>
> このポリシーは、ファイルベースとVHDXベースの両方のユーザー ストアで利用できます。Profile Managementバージョン2212より前では、このポリシーはVHDXベースのユーザー ストアでのみ利用できます。

> この設定がここで構成されていない場合、.iniファイルの値が使用されます。この設定がここでも.iniファイルでも構成されていない場合、デフォルトで無効になります。

VHDXファイルのストレージパスをカスタマイズ

Profile Managementは、次のVHDXベースのポリシーを提供します：プロファイルコンテナ、Outlookの検索インデックスローミング、フォルダーミラーリングの高速化。デフォルトでは、VHDXファイルはユーザー ストアに保存されます。このポリシーを使用すると、それらを保存するための別個のパスを指定できます。

VHDコンテナのデフォルト容量

VHDコンテナのデフォルトのストレージ容量 (GB単位) を指定できます。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、デフォルトは50 (GB) です。

セッションでVHDXディスクを自動的に再アタッチ

このポリシーを有効にすると、Profile ManagementはVHDXベースのポリシーの高い安定性を確保します。デフォルトでは、このポリシーは有効になっています。

このポリシーが有効になっている場合、Profile ManagementはVHDXベースのポリシーで使用されているVHDXディスクを監視します。いずれかのディスクがデタッチされた場合、Profile Managementはディスクを自動的に再アタッチします。

プロファイルコンテナの自動拡張しきい値

プロファイルコンテナが自動拡張をトリガーするストレージ容量の使用率を指定できます。

構成の優先順位:

- このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここで、または.iniファイルで構成されていない場合、デフォルトはストレージ容量の90%です。

プロファイルコンテナの自動拡張増分

自動拡張がトリガーされたときにプロファイルコンテナが自動的に拡張するストレージ容量（GB単位）を指定できます。

構成の優先順位:

- このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここで、または.iniファイルで構成されていない場合、デフォルトは10 GBです。

プロファイルコンテナの自動拡張制限

自動拡張がトリガーされたときにプロファイルコンテナが自動的に拡張できる最大ストレージ容量（GB単位）を指定できます。

構成の優先順位:

- このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここで、または.iniファイルで構成されていない場合、デフォルトは80 GBです。

ユーザーレベルのポリシー設定を有効にする

このポリシーを有効にすると、マシンレベルのポリシー設定がユーザーレベルで機能し、ユーザーレベルの設定がマシンレベルの設定を上書きします。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここで構成されておらず、.iniファイルでも構成されていない場合、無効になります。

ユーザーグループの優先順位を設定する

ユーザーグループの優先順位を指定できます。この順序は、ユーザーが異なるポリシー設定を持つ複数のグループに属している場合に、どのグループが優先されるかを決定します。

ユーザーが競合するポリシー設定を持つ複数のグループに属している場合、以下を考慮してください:

- ユーザーがこのポリシーで定義されている1つ以上のグループに属している場合、最も優先順位の高いグループが優先されます。
- ユーザーがこのポリシーで定義されているどのグループにも属していない場合、アルファベット順で最も早くリストされているSIDを持つグループが優先されます。

ユーザーストアの選択方法

複数のユーザーストアが利用可能な場合に、ユーザーストアの選択方法を指定できます。オプションは次のとおりです:

- **構成順序。** Profile Managementは、最も早く構成されたストアを選択します。
- **アクセスパフォーマンス。** Profile Managementは、最高のアクセスパフォーマンスを持つストアを選択します。

構成の優先順位:

1. この設定がここで構成されていない場合、.iniファイルの値が使用されます。
2. ここまたは.iniファイルでこの設定が構成されていない場合、**構成順序**が使用されます。

ユーザー ストア間のセッション内プロファイル コンテナー フェールオーバーを有効にする

デフォルトでは、複数のユーザー ストアが展開されている場合、プロファイル コンテナーのフェールオーバーはユーザー ログオン時にのみ発生します。その結果、プロファイルの冗長性はユーザー ログオン時にのみ利用可能です。このポリシーを使用すると、フェールオーバーの範囲をセッション全体に拡大し、セッション全体でプロファイルの冗長性を確保できます。このポリシーを有効にすると、セッション中に Profile Management がアクティブなプロファイル コンテナーへの接続を失った場合、自動的に別の利用可能なコンテナーに切り替わります。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。
2. このポリシーがここで、または.iniファイルで構成されていない場合、この設定は無効になります。

基本的なポリシー設定

このセクションには、Profile Management の基本的な構成に関連するポリシー設定が含まれています。

Profile Management を有効にする

デフォルトでは、展開を容易にするため、Profile Management はログオンまたはログオフを処理しません。Profile Management は、他のすべてのセットアップタスクを実行し、Citrix® ユーザープロファイルが環境でどのように動作するかをテストした後にのみ有効にしてください。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、Profile Management は Windows ユーザープロファイルを一切処理しません。

処理されるグループ

コンピューターローカルグループとドメイングループ（ローカル、グローバル、ユニバーサル）の両方を使用できます。ドメイングループは、DOMAIN NAME\GROUP NAME の形式で指定する必要があります。

このポリシーがここで構成されている場合、Profile Management はこれらのユーザーグループのメンバーのみを処理します。このポリシーが無効になっている場合、Profile Management はすべてのユーザーを処理します。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、すべてのユーザーグループのメンバーが処理されます。

除外されるグループ

コンピューターローカルグループとドメイングループ（ローカル、グローバル、ユニバーサル）を使用して、特定のユーザープロファイルが処理されないようにすることができます。ドメイングループは、DOMAIN NAME\ GROUP NAME の形式で指定します。

この設定がここで構成されている場合、Profile Management はこれらのユーザーグループのメンバーを除外します。この設定が無効になっている場合、Profile Management はどのユーザーも除外しません。この設定がここで構成されていない場合、.ini ファイルの値が使用されます。この設定がここでも .ini ファイルでも構成されていない場合、どのグループのメンバーも除外されません。

ローカル管理者によるログオンの処理

BUILTIN\Administrators グループのメンバーによるログオンを処理するかどうかを指定します。Citrix Virtual Apps 環境などのマルチセッションオペレーティングシステムでは、このポリシーを無効にするか、構成しないことを検討してください。この場合、Profile Management は、ドメイ

ンユーザーによるログオンは処理する必要があるが、ローカル管理者によるログオンは処理する必要がないと想定します。シングルセッションオペレーティングシステム（Citrix Virtual Desktops 環境など）では、ローカル管理者によるログオンが処理されます。このポリシーにより、ローカル管理者権限を持つドメインユーザー（通常は割り当てられた仮想デスクトップを持つ Citrix Virtual Desktops ユーザー）は、次のことが可能になります。

- 処理をバイパスする
- ログオンする
- Profile Management を使用したデスクトップ関連の問題のトラブルシューティング

注: ドメインユーザーのログオンは、通常、製品ライセンスへの準拠を確実にするために、グループメンバーシップによって課される制限の対象となる場合があります。 このポリシーが無効になっている場合、Profile Management はローカル管理者によるログオンを処理しません。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、管理者は処理されません。

ユーザー ストアへのパス

ユーザー設定（レジストリの変更と同期ファイル）が保存されるディレクトリ（ユーザー ストア）へのパスを設定します。

パスは次のいずれかです。

- 相対パス。ホームディレクトリ（通常、Active Directory のユーザーの #homeDirectory# 属性として構成されます）に対する相対パスである必要があります。
- UNC パス。通常、サーバー共有または DFS 名前空間を指定します。
- 無効または未構成。この場合、#homeDirectory#\Windows の値が想定されます。

このポリシーでは、次の種類の変数を使用できます。

- パーセント記号で囲まれたシステム環境変数（例: %ProfVer%）。システム環境変数は通常、追加の設定が必要です。
- ハッシュで囲まれた Active Directory ユーザーオブジェクトの属性（例: #sAMAccountName#）。
- Profile Management 変数。詳細については、Profile Management 変数製品ドキュメントを参照してください。

ユーザー環境変数は、`%username%` および `%userdomain%` を除いて使用できません。場所やユーザーなどを完全に定義するために、カスタム属性を作成することもできます。属性は大文字と小文字を区別します。

例:

- \\server\share#sAMAccountName# は、ユーザー設定を UNC パス \\server\share\JohnSmith に保存します（現在のユーザーに対して #sAMAccountName# が JohnSmith に解決される場合）。
- \\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS! は \\server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64 に展開される場合があります

重要: どの属性または変数を使用する場合でも、このポリシーが NTUSER.DAT を含むフォルダーの 1 レベル上のフォルダーに展開されることを確認してください。たとえば、このファイルが \\server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile に含まれている場合、ユーザー ストアへのパスは \\server\profiles$\JohnSmith.Finance\Win8x64 (\UPM_Profile サブフォルダーではない) として設定します。

ユーザー ストアへのパスを指定する際に変数を使用する方法について詳しくは、次のトピックを参照してください。

- 複数のファイルサーバーでCitrixユーザープロファイルを共有する
- OU内およびOU間でプロファイルを管理する
- Profile Managementによる高可用性と災害復旧

ユーザー ストアへのパスが無効になっている場合、ユーザー設定はホーム ディレクトリのWindowsサブディレクトリに保存されます。

このポリシーが無効になっている場合、ユーザー設定はホーム ディレクトリのWindowsサブディレクトリに保存されます。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここで、または.iniファイルで構成されていない場合、ホーム ドライブのWindowsディレクトリが使用されます。

ユーザーストアの移行

ユーザー設定（レジストリの変更と同期されたファイル）が以前に保存されていたフォルダーへのパス（以前使用していたユーザー ストアのパス）を指定します。

この設定が構成されている場合、以前のユーザー ストアに保存されているユーザー設定は、「ユーザー ストアへのパス」ポリシーで指定された現在のユーザー ストアに移行されます。

パスは、絶対UNCパスまたはホーム ディレクトリに対する相対パスのいずれかです。

どちらの場合も、次の種類の変数を使用できます。

- パーセント記号で囲まれたシステム環境変数

- ハッシュ記号で囲まれたActive Directoryユーザー オブジェクトの属性

例:

- フォルダ `Windows\%ProfileVer%` は、ユーザー設定をユーザー ストアの `Windows\W2K3` というサブフォルダに保存します (%ProfileVer% が W2K3 に解決されるシステム環境変数である場合)。
- `\\server\share#SAMAccountName#` は、ユーザー設定を UNC パス `\\server\share\<JohnSmith>` に保存します (`#SAMAccountName#` が現在のユーザーに対して JohnSmith に解決される場合)。

パスでは、`%username%` および `%userdomain%` を除くユーザー環境変数を使用できます。

この設定が無効になっている場合、ユーザー設定は現在のユーザーストアに保存されます。

この設定がここで構成されていない場合、.ini ファイルの対応する設定が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、ユーザー設定は現在のユーザー ストアに保存されます。

アクティブライトバック

変更されたファイルとフォルダ (レジストリエントリは除く) は、ログオフ前にセッションの途中でユーザー ストアに同期できます。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、有効になります。

オフラインプロファイルのサポート

このポリシーにより、プロファイルを可能な限り早い機会にユーザー ストアと同期できます。これは、ローミングするラップトップまたはモバイルデバイスのユーザーを対象としています。ネットワーク接続が切断されても、再起動または休止状態の後でも、プロファイルはラップトップまたはデバイス上でそのまま維持されます。モバイルユーザーが作業するにつれて、プロファイルはローカルで更新されます。また、ネットワーク接続が再確立されると、最終的にユーザー ストアと同期されます。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、オフラインプロファイルは無効になります。

アクティブライトバックレジストリ

このポリシーは「アクティブライトバック」と併用してください。変更されたレジストリエントリは、セッションの途中でユーザー ストアに同期できます。

ここでこの設定を構成しない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定を構成しない場合、アクティブライトバックレジストリは無効になります。

セッションロックおよび切断時のアクティブライトバック

このポリシーと**アクティブライトバック**ポリシーの両方が有効になっている場合、プロファイルファイルとフォルダーは、セッションがロックまたは切断されたときにのみ書き戻されます。

このポリシーと**アクティブライトバック**および**アクティブライトバックレジストリ**ポリシーの両方が有効になっている場合、レジストリエントリは、セッションがロックまたは切断されたときにのみ書き戻されます。

オフラインプロファイルのサポート

オフラインプロファイル機能を有効にします。この機能は、ネットワークから頻繁に切断されるコンピューター向けです。たとえば、サーバーやデスクトップではなく、ラップトップやモバイルデバイスなどです。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定が構成されていない場合、オフラインプロファイルのサポートは無効になります。

クロスプラットフォームポリシー設定

このセクションには、**Profile Management cross-platform** 設定機能の構成に関連するポリシー設定が含まれています。

クロスプラットフォーム設定を有効にする

デフォルトでは、展開を容易にするために、クロスプラットフォーム設定は無効になっています。このポリシーを有効にすることで処理をオンにできますが、この機能の十分な計画とテストを行った後に限ります。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、クロスプラットフォーム設定は適用されません。

クロスプラットフォーム設定ユーザーグループ

1つ以上のWindowsユーザーグループを入力します。たとえば、このポリシーを使用して、テストユーザーグループのプロファイルのみを処理することができます。このポリシーが構成されている場合、Profile Managementのクロスプラットフォーム設定機能は、これらのユーザーグループの

メンバーのみを処理します。このポリシーが無効になっている場合、この機能は「処理済みグループ」ポリシーで指定されたすべてのユーザーを処理します。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、すべてのユーザーグループが処理されます。

クロスプラットフォーム定義へのパス

ダウンロードパッケージからコピーした定義ファイルのネットワーク上の場所を識別します。このパスはUNCパスである必要があります。ユーザーはこの場所への読み取りアクセス権を持ち、管理者は書き込みアクセス権を持っている必要があります。この場所は、Server Message Block (SMB) またはCommon Internet File System (CIFS) ファイル共有である必要があります。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、クロスプラットフォーム設定は適用されません。

クロスプラットフォーム設定ストアへのパス

クロスプラットフォーム設定ストアへのパスを設定します。これは、ユーザーのクロスプラットフォーム設定が保存されるフォルダーです。ユーザーはこの領域への書き込みアクセス権を持っている必要があります。パスは絶対UNCパスまたはホームディレクトリに対する相対パスにすることができます。

この領域は、複数のプラットフォームで共有されるプロファイルデータが配置されるユーザーストアの共通領域です。ユーザーはこの領域への書き込みアクセス権を持っている必要があります。パスは絶対UNCパスまたはホームディレクトリに対する相対パスにすることができます。**ユーザーストアへのパス**と同じ変数を使用できます。

このポリシーが無効になっている場合、パスWindows\PM_CPが使用されます。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、デフォルト値が使用されます。

クロスプラットフォーム設定を作成するためのソース

このポリシーがそのプラットフォームのOUで有効になっている場合、プラットフォームをベースプラットフォームとして指定します。このポリシーは、ベースプラットフォームのプロファイルからクロスプラットフォーム設定ストアにデータを移行します。

各プラットフォーム独自のプロファイルセットは、個別のOUに保存されます。クロスプラットフォーム設定ストアをシードするために、どのプラットフォームのプロファイルデータを使用するかを決定する必要があります。これはベースプラットフォームと呼ばれます。クロスプラット

フォーム設定ストアにデータのない定義ファイルが含まれている場合、または単一プラットフォームプロファイルのキャッシュデータがストア内の定義データよりも新しい場合を考慮してください。この場合、このポリシーを無効にしない限り、プロファイル管理は単一プラットフォームプロファイルからストアにデータを移行します。

> **重要:**
>
> このポリシーが複数のOU、または複数のユーザーオブジェクトやマシンオブジェクトで有効になっている場合、最初にユーザーがログオンしたプラットフォームがベースプロファイルになります。 デフォルトでは、このポリシーは有効になっています。

ファイルシステムポリシー設定

除外ポリシー設定

このセクションでは、ユーザープロファイル内のどのファイルとディレクトリを同期プロセスから除外するかを設定するためのポリシー設定について説明します。

除外リスト - ファイル

同期中に無視されるファイルのリスト。ファイル名はユーザープロファイル (%USERPROFILE%) に対する相対パスである必要があります。ワイルドカードはファイル名とフォルダー名でサポートされていますが、ファイル名のワイルドカードのみが再帰的に適用されます。

例:

- `Desktop\Desktop.ini` は、`Desktop` フォルダー内のファイル `Desktop.ini` を無視します。
- `%USERPROFILE%*.tmp` は、プロファイル全体で拡張子 `.tmp` を持つすべてのファイルを無視します。
- `AppData\Roaming\MyApp*.tmp` は、プロファイルの一部で拡張子 `.tmp` を持つすべてのファイルを無視します。
- `Downloads*\a.txt` は、`Downloads` フォルダーの直下のサブフォルダーにある `a.txt` を無視します。

このポリシーが無効になっている場合、ファイルは除外されません。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ファイルは除外されません。

デフォルトの除外リストを有効にする - ディレクトリ

同期中に無視されるディレクトリのデフォルトリスト。このポリシーを使用して、GPO 除外ディレクトリを手動で入力することなく指定します。

このポリシーを無効にすると、Profile Management はデフォルトでどのディレクトリも除外しません。

このポリシーをここで構成しない場合、Profile Management は .ini ファイルの値を使用します。このポリシーをここでも .ini ファイルでも構成しない場合、Profile Management はデフォルトでどのディレクトリも除外しません。

除外リスト - ディレクトリ

同期中に無視されるフォルダーのリスト。フォルダー名は、ユーザープロファイル (%USERPROFILE%) に対する相対パスとして指定する必要があります。フォルダー名でのワイルドカードはサポートされていますが、再帰的には適用されません。

例:

- `Desktop\Desktop.ini` は `Desktop` フォルダー内のファイル `Desktop.ini` を無視します。
- `%USERPROFILE%*.tmp` はプロファイル全体で拡張子 `.tmp` を持つすべてのファイルを無視します。
- `AppData\Roaming\MyApp*.tmp` はプロファイルの一部で拡張子 `.tmp` を持つすべてのファイルを無視します。
- `Downloads*\a.txt` は `Downloads` フォルダーの直下のサブフォルダーにある `a.txt` を無視します。

このポリシーが無効になっている場合、ファイルは除外されません。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ファイルは除外されません。

デフォルトの除外リストを有効にする - ディレクトリ

同期中に無視されるディレクトリのデフォルトリスト。このポリシーを使用して、GPO 除外ディレクトリを手動で入力することなく指定できます。

このポリシーを無効にすると、Profile Management はデフォルトでどのディレクトリも除外しません。

このポリシーをここで構成しない場合、Profile Management は .ini ファイルの値を使用します。このポリシーをここでも .ini ファイルでも構成しない場合、Profile Management はデフォルトでどのディレクトリも除外しません。

除外リスト - ディレクトリ

同期中に無視されるフォルダーのリスト。フォルダー名はユーザープロファイル (%USERPROFILE%) に対する相対パスとして指定する必要があります。フォルダー名でのワイルドカードはサポートされていますが、再帰的には適用されません。

例:

- `Desktop` はユーザープロファイル内の `Desktop` フォルダーを無視します

このポリシーが無効になっている場合、フォルダーは除外されません。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、フォルダーは除外されません。

ログオン除外チェック

この設定は、ユーザーストア内のプロファイルに除外されたファイルまたはフォルダーが含まれている場合に、Profile Management が実行する動作を構成します。可能なポリシー設定とそれに対応するアクションを次の表に示します。

ポリシー設定	アクション
設定が無効になっているか、「ログオン時に除外されたファイルまたはフォルダーを同期する」の値がデフォルトに設定されている	ユーザーがログオンすると、Profile Management はユーザーストアからローカルプロファイルに除外されたファイルまたはフォルダーを同期します。
設定が「ログオン時に除外されたファイルまたはフォルダーを無視する」に設定されている	ユーザーがログオンすると、Profile Management はユーザーストア内の除外されたファイルまたはフォルダーを無視します。
設定が「ログオン時に除外されたファイルまたはフォルダーを削除する」に設定されている	ユーザーがログオンすると、Profile Management はユーザーストア内の除外されたファイルまたはフォルダーを削除します。
設定がWeb Studioで構成されていない	.ini ファイルの値が使用されます
Web Studio または .ini ファイルで設定が構成されていません	除外されたファイルまたはフォルダーは、ユーザーがログオンするときに、ユーザー ス

ポリシー設定	アクション
	トアからローカル プロファイルに同期されます。

ラージファイルの処理 - シンボリックリンクとして作成されるファイル

ログオンパフォーマンスを向上させ、サイズの大きいファイルを処理するために、Profile Management はこのリスト内のファイルをコピーする代わりにシンボリックリンクを作成します。

ファイルを参照するポリシーではワイルドカードを使用できます。例: `!ctx_localappdata!\Microsoft\Outlook*.OST`。

Microsoft Outlook のオフラインフォルダーファイル (`*.ost`) を処理するには、**Outlook** フォルダーが Profile Management で除外されていないことを確認してください。

これらのファイルは、複数のセッションで同時にアクセスすることはできません。

同期ポリシー設定

「**同期**」セクションでは、プロファイルがインストールされているシステムとユーザー ストアの間で、ユーザー プロファイル内のどのファイルとフォルダーを同期するかを指定するためのポリシー設定について説明します。

同期するディレクトリ

デフォルトでは、Profile Management は、ユーザー プロファイルがインストールされているシステムとユーザー ストアの間でユーザー プロファイルを同期します。同期からフォルダーを除外した場合、このポリシーを使用すると、除外されたフォルダーのサブフォルダーを同期に含めることができます。

このリストのパスは、ユーザー プロファイルに対する相対パスである必要があります。フォルダー名でのワイルドカードはサポートされていますが、再帰的には適用されません。

ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。ここで、または .ini ファイルでこのポリシーが構成されていない場合、ユーザー プロファイル内の除外されていないフォルダーのみが同期されます。

同期するファイル

デフォルトでは、Profile Management は、ユーザー プロファイルがインストールされているシステムとユーザー ストアの間でユーザー プロファイルを同期します。同期からフォルダーを除外し

た場合、このポリシーを使用すると、除外されたフォルダー内のファイルを同期に含めることができます。

このリストのパスは、ユーザー プロファイルに対する相対パスである必要があります。ファイル名とフォルダー名でワイルドカードがサポートされていますが、ファイル名のワイルドカードのみが再帰的に適用されます。ワイルドカードをネストすることはできません。

例:

- `AppData\Local\Microsoft\Office\Access.qat` は、デフォルト構成で除外されているフォルダーの下にあるファイルを指定します。
- `AppData\Local\MyApp*.cfg` は、プロファイルフォルダー `AppData\Local\MyApp` とそのサブフォルダー内の拡張子 `.cfg` を持つすべてのファイルを指定します。

このポリシーを無効にすると、有効にして空のリストを構成した場合と同じ効果があります。

ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。ここで、または .ini ファイルでこのポリシーが構成されていない場合、ユーザー プロファイル内の除外されていないファイルのみが同期されます。

ミラーリングするフォルダー

このポリシーを使用すると、トランザクションフォルダー（参照フォルダーとも呼ばれます）に関する問題を解決できます。そのフォルダーには相互依存ファイルが含まれており、あるファイルが別のファイルを参照しています。

フォルダーのミラーリングにより、プロファイル管理はトランザクションフォルダーとその内容を単一のエンティティとして処理し、プロファイルの肥大化を防ぐことができます。たとえば、**Internet Explorer の Cookie** フォルダーをミラーリングして、Index.dat がインデックス化する Cookie と同期されるようにすることができます。このような状況では、「最後の書き込みが優先されます」。そのため、複数のセッションで変更されたミラーリングされたフォルダー内のファイルは、最後の更新によって上書きされ、プロファイル変更が失われます。

たとえば、次の表は、ユーザーがインターネットを閲覧しているときにIndex.datがCookieを参照する方法を示しています。

シナリオ	INDEX.DATがCOOKIEを参照する方法	
ユーザーは2つのInternet Explorerセッションを持ち、それぞれ異なるサーバー上に	各サイトのCookieは、適切なサーバーに追加されます。	各サイトのCookieは、適切なサーバーに追加されます。

シナリオ	INDEX.DATがCOOKIEを参照する方法	
あり、各セッションで異なるサイトにアクセスします。		
ユーザーが最初のセッションからログオフするか、セッションの途中でログオフします（アクティブなライトバック機能が構成されている場合）。	2番目のセッションのCookieは、最初のセッションのCookieを置き換える必要があります。	
最初のセッションと2番目のセッションがマージされ、Index.dat内のCookieへの参照が古くなります。	新しいセッションでのさらなるブラウジングは、繰り返しのマージと肥大化したCookieフォルダーにつながります。	

Cookieフォルダーをミラーリングすることで、この問題は解決されます。この場合、ユーザーがログオフするたびに、Cookieは最後のセッションのCookieで上書きされます。そのため、Index.datは常に最新の状態に保たれます。

このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、フォルダーはミラーリングされません。

フォルダーのミラーリングを高速化する

このポリシーと**ミラーリングするフォルダー**ポリシーの両方を有効にすると、**Profile Management はミラーリングされた**フォルダーを VHDX ベースの仮想ディスクに保存します。仮想ディスクはログオン時にアタッチされ、ログオフ時にデタッチされます。このポリシーを有効にすると、ユーザー ストアとローカル プロファイル間でフォルダーをコピーする必要がなくなり、フォルダーのミラーリングが高速化されます。

フォルダリダイレクトポリシー設定

このセクションには、プロファイルによく表示されるフォルダーを共有ネットワークの場所にリダイレクトするかどうかを指定するポリシー設定が含まれています。

管理者アクセス権の付与

この設定により、管理者はユーザーのリダイレクトされたフォルダーの内容にアクセスできるようになります。

> **注:**
>
> この設定は、ドメインへの完全かつ無制限のアクセス権を持つ管理者に対して権限を付与します。

> デフォルトでは、この設定は無効になっており、ユーザーにはリダイレクトされたフォルダーの内容への排他的なアクセス権が付与されます。

ドメイン名を含める

この設定により、UNC パスの一部として `%userdomain%` 環境変数を含めることができます。この UNC パスは、リダイレクトされたフォルダーに指定されます。

デフォルトでは、この設定は無効になっています。また、リダイレクトされたフォルダーに指定されている UNC パスの一部として、`%userdomain%` 環境変数は含まれません。

ドキュメントポリシー設定

このセクションには、**ドキュメント**フォルダーの内容を共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ドキュメントパス

この設定は、**ドキュメント**フォルダー内のファイルがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ドキュメントパス設定は、**ドキュメント**フォルダーへのファイルのリダイレクトだけでなく、**ミュージック**、**ピクチャ**、**ビデオ**フォルダーへのファイルのリダイレクトのためにも有効にする必要があります。

ドキュメントのリダイレクト設定

この設定は、**ドキュメント**フォルダーの内容をリダイレクトする方法を指定します。

デフォルトでは、内容は UNC パスにリダイレクトされます。

ドキュメントフォルダーの内容をリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次の UNC パスにリダイレクトします。ドキュメントパスポリシー設定で指定された UNC パスにコンテンツをリダイレクトします。
- ユーザーのホームディレクトリにリダイレクトします。コンテンツをユーザーのホームディレクトリにリダイレクトします。これは通常、Active Directory のユーザーの #homeDirectory# 属性として構成されます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

お気に入りポリシー設定

このセクションには、「**お気に入り**」フォルダーの内容を共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

お気に入りパス

この設定は、「**お気に入り**」フォルダーの内容がリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

この設定がここで構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

お気に入りのリダイレクト設定

この設定は、「**お気に入り**」フォルダーの内容をリダイレクトする方法を指定します。

デフォルトでは、内容は UNC パスにリダイレクトされます。

この設定がここで構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

リンクポリシー設定

このセクションでは、**リンク**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定について説明します。

リンクパス

この設定は、**リンク**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

この設定がここで構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

リンクのリダイレクト設定

この設定は、**リンク**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

この設定がここで構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

「ピクチャ」ポリシー設定

このセクションには、「**ピクチャ**」フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

画像パス

この設定は、「**ピクチャ**」フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

この設定がここで構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

「ピクチャ」のリダイレクト設定

この設定は、「**ピクチャ**」フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

「**ピクチャ**」フォルダーのコンテンツをリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次のUNCパスにリダイレクトする。コンテンツを「ピクチャパス」ポリシー設定で指定されたUNCパスにリダイレクトします。
- ドキュメントフォルダーを基準にリダイレクトする。コンテンツをドキュメントフォルダーを基準としたフォルダーにリダイレクトします。

コンテンツを「**ドキュメント**」フォルダーを基準としたフォルダーにリダイレクトするには、「**ドキュメントパス**」設定を有効にする必要があります。

この設定がここで構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

スタートメニューのポリシー設定

このセクションには、**スタートメニュー**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

スタートメニューのリダイレクト設定

この設定は、**スタートメニュー**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

スタートメニューのパス

この設定は、**スタートメニュー**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

Searchesポリシー設定

このセクションには、**検索**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

SEARCHESのリダイレクト設定

この設定は、**検索**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

SEARCHESパス

この設定は、**検索**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ログポリシー設定

このセクションには、Profile Management のログ記録を構成するポリシー設定が含まれています。

Active Directory のアクション

この設定は、Active Directory で実行されるアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログの有効化**設定も有効になっていることを確認してください。

この設定が Web Studio で構成されていない場合、.ini ファイルの値が使用されます。

この設定が Web Studio または .ini ファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

一般情報

この設定は、一般情報の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログの有効化**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

一般的な警告

この設定は、一般的な警告の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログの有効化**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログの有効化

この設定は、デバッグ（詳細ログ）モードでのProfile Managementログを有効または無効にします。デバッグモードでは、"%SystemRoot%\System32\Logfiles\UserProfileManager" にあるログファイルに詳細なステータス情報が記録されます。

デフォルトでは、この設定は無効になっており、エラーのみがログに記録されます。

Citrix®は、Profile Managementのトラブルシューティングを行う場合にのみ、この設定を有効にすることをお勧めします。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、エラーのみがログに記録されます。

ファイルシステムのアクション

この設定は、ファイルシステムで実行されたアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログの有効化**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ファイルシステム通知

この設定は、ファイルシステム通知の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオフ

この設定は、ユーザーのログオフの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオン

この設定は、ユーザーのログオンの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログファイルの最大サイズ

この設定は、Profile Managementログファイルの最大許容サイズをバイト単位で指定します。

デフォルトでは、この値は1048576バイト（1 MB）に設定されています。

十分なディスク容量がある場合、Citrixはこのファイルのサイズを5 MB以上に増やすことを推奨します。ログファイルが最大サイズを超えて増加した場合：

- 既存のファイルのバックアップ（.bak）が削除されます
- ログファイルは.bakに名前が変更されます

- 新しいログファイルが作成されます

ログファイルは`%SystemRoot%\System32\Logfiles\UserProfileManager`に作成されます。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここで、または.iniファイルで構成されていない場合、デフォルト値が使用されます。

ログファイルへのパス

この設定は、Profile Management のログファイルを保存するための代替パスを指定します。

デフォルトでは、この設定は無効になっており、ログファイルはデフォルトの場所である%SystemRoot%\System32\Logfiles\UserProfileManagerに保存されます。

パスはローカルドライブまたはリモートのネットワークベースドライブ (UNC パス) を指すことができます。リモートパスは大規模な分散環境で役立つ場合がありますが、ログファイルには不適切な大量のネットワークトラフィックを生成する可能性があります。永続的なハードドライブを持つプロビジョニングされた仮想マシンの場合は、そのドライブへのローカルパスを設定します。この設定により、マシンの再起動時にログファイルが保持されます。永続的なハードドライブを持たない仮想マシンの場合は、UNC パスを設定することでログファイルを保持できます。ただし、マシンのシステムアカウントは UNC 共有への書き込みアクセス権を持っている必要があります。オフラインプロファイル機能によって管理されるラップトップには、ローカルパスを使用してください。

ログファイルに UNC パスを使用する場合、Citrix はログファイルフォルダーに適切なアクセス制御リストを適用することを推奨します。この設定により、承認されたユーザーまたはコンピューターアカウントのみが保存されたファイルにアクセスできるようになります。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

ここまたは .ini ファイルでこの設定が構成されていない場合、デフォルトの場所 %SystemRoot%\System32\Logfiles\UserProfileManager が使用されます。

パーソナライズされたユーザー情報

この設定は、パーソナライズされたユーザー情報の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合、**ログの有効化**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

Web Studio または .ini ファイルでこの設定が構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオン時とログオフ時のポリシー値

この設定は、ユーザーがログオンおよびログオフするときのポリシー値の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合、**ログの有効化**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

レジストリアクション

この設定は、レジストリで実行されたアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオフ時のレジストリの相違点

この設定は、ユーザーがログオフしたときのレジストリの相違点の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

プロファイル処理ポリシー設定

このセクションには、Profile Management がユーザープロファイルを処理する方法を指定するポリシー設定が含まれています。

キャッシュされたプロファイルを削除するまでの遅延

この設定は、ログオフ時に Profile Management がローカルにキャッシュされたプロファイルを削除するまでの遅延を、分単位で任意に延長する時間を指定します。

値が 0 の場合、ログオフプロセスの終了時にプロファイルがすぐに削除されます。Profile Management は 1 分ごとにログオフをチェックします。その結果、値が 60 の場合、ユーザーがログオフしてから 1 ～ 2 分の間にプロファイルが削除されることが保証されます。このアクションは、最後のチェックがいつ行われたかによって異なります。ログオフ中にプロセスがファイルまたはユーザーレジストリハイブを開いたままにしていることがわかっている場合、遅延を延長すると便利です。大規模なプロファイルの場合、このプロセスはログオフを高速化することもできます。

デフォルトでは、この値は 0 に設定されており、Profile Management はローカルにキャッシュされたプロファイルをすぐに削除します。

この設定を有効にする場合は、「ログオフ時にローカルにキャッシュされたプロファイルを削除する」も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、プロファイルはすぐに削除されます。

ログオフ時にローカルにキャッシュされたプロファイルを削除する

この設定は、ユーザーがログオフした後にローカルにキャッシュされたプロファイルが削除されるかどうかを指定します。

この設定が有効になっている場合、ユーザーのローカルプロファイルキャッシュはログオフ後に削除されます。Citrix® は、ターミナルサーバーでこの設定を有効にすることをお勧めします。

デフォルトでは、この設定は無効になっており、ユーザーのローカルプロファイルキャッシュはログオフ後も保持されます。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、キャッシュされたプロファイルは削除されません。

ローカルプロファイルの競合処理

この設定は、ユーザープロファイルが以下の両方に存在する場合のProfile Managementの動作を構成します。

- ユーザーストア
- ローカルWindowsユーザープロファイル（Citrixユーザープロファイルではない）

デフォルトでは、Profile ManagementはローカルWindowsプロファイルを使用しますが、それを一切変更しません。

Profile Management の動作を制御するには、次のいずれかのオプションを選択します。

- ローカルプロファイルを使用する。Profile Managementはローカルプロファイルを使用しますが、それを一切変更しません。
- ローカルプロファイルを削除する。Profile ManagementはローカルWindowsユーザープロファイルを削除し、ユーザーストアからCitrixユーザープロファイルをインポートします。
- ローカルプロファイルの名前を変更する。Profile ManagementはローカルWindowsユーザープロファイルの名前を変更し（バックアップ目的で）、ユーザーストアからCitrixユーザープロファイルをインポートします。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がここで、または .ini ファイルで構成されていない場合、既存のローカルプロファイルが使用されます。

既存プロファイルの移行

この設定は、ユーザーがユーザーストアに現在のプロファイルを持っていない場合に、ログオン中にユーザーストアに移行されるプロファイルの種類を指定します。

ユーザーがユーザーストアにプロファイルを持っていない場合、Profile Managementはログオン中に既存のプロファイルを「オンザフライ」で移行できます。その後、ユーザーストアプロファイルは以下の両方でProfile Managementによって使用されます。

- 現在のセッション
- 同じユーザー ストアへのパスで構成されたその他のセッション

デフォルトでは、ローカルプロファイルと移動プロファイルの両方がログオン中にユーザー ストアに移行されます。

ログオン中にユーザー ストアに移行されるプロファイルの種類を指定するには、次のいずれかのオプションを選択します。

- ローカルプロファイルと移動プロファイル
- ローカル
- ローミング
- なし (無効)

なしを選択すると、Profile Managementがインストールされていない環境であるかのように、システムは既存のWindowsメカニズムを使用してプロファイルを作成します。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、既存のローカルプロファイルとローミングプロファイルが移行されます。

既存のアプリケーションプロファイルの自動移行

この設定は、異なるオペレーティングシステム間で既存のアプリケーションプロファイルを自動的に移行するかどうかを有効または無効にします。アプリケーションプロファイルには、`AppData`フォルダー内のアプリケーションデータと、`HKEY_CURRENT_USER\SOFTWARE`の下のレジストリエントリの両方が含まれます。この設定は、異なるオペレーティングシステム間でアプリケーションプロファイルを移行したい場合に役立ちます。

たとえば、オペレーティングシステム（OS）をWindows 10バージョン1803からWindows 10バージョン1809にアップグレードするとします。この設定が有効になっている場合、各ユーザーが最初にログオンするときに、Profile Managementは既存のアプリケーション設定をWindows 10バージョン1809に自動的に移行します。その結果、`AppData`フォルダー内のアプリケーションデータとHKEY_CURRENT_USER\SOFTWAREの下のレジストリエントリが移行されます。

複数の既存のアプリケーションプロファイルがある場合、Profile Managementは次の優先順位で移行を実行します。

1. 同じOSタイプのプロファイル (シングルセッションOSからシングルセッションOS、マルチセッションOSからマルチセッションOS)。
2. 同じWindows OSファミリーのプロファイル（例：Windows 10からWindows 10、またはWindows Server 2016からWindows Server 2016）。
3. 以前のバージョンのOSのプロファイル（例：Windows 7からWindows 10、またはWindows Server 2012からWindows 2016）。
4. 最も近いOSのプロファイル。

注： ユーザーストアパスに変数「!CTX_OSNAME!」を含めることで、OSの短い名前を指定する必要があります。これにより、Profile Managementは既存のアプリケーションプロファイルを特定できます。

ここでこの設定が構成されていない場合、.iniファイルの設定が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、デフォルトで無効になります。

テンプレートプロファイルへのパス

この設定は、Profile Managementがユーザープロファイルを作成するためのテンプレートとして使用するプロファイルへのパスを指定します。

指定されたパスは、NTUSER.DATレジストリファイルと、テンプレートプロファイルに必要なその他のフォルダーおよびファイルを含むフォルダーへの完全なパスである必要があります。

注：パスにNTUSER.DATを含めないでください。たとえば、ファイル \\\myservername\myprofiles\template\ntuser.dat の場合、場所を \\\myservername\myprofiles\template に設定します。

絶対パスを使用してください。絶対パスはUNCパスまたはローカルマシン上のパスのいずれかです。後者は、たとえばCitrix Provisioning™ Servicesイメージ上にテンプレートプロファイルを永続的に指定する場合に使用します。相対パスはサポートされていません。

注: この設定は、Active Directory属性、システム環境変数、または`%USERNAME%`および`%USERDOMAIN%`変数の展開をサポートしていません。

デフォルトでは、この設定は無効になっており、新しいユーザープロファイルは、ユーザーが最初にログオンするデバイス上のデフォルトのユーザープロファイルから作成されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、テンプレートは使用されません。

テンプレートプロファイルがローカルプロファイルを上書きする

この設定により、ユーザープロファイルの作成時にテンプレートプロファイルがローカルプロファイルを上書きできるようになります。

ユーザーがCitrixユーザープロファイルを持たず、ローカルのWindowsユーザープロファイルを持っているとします。この場合、この値が有効になっていると、デフォルトでローカルプロファイルが使用され、ユーザーストアに移行されます。このポリシー設定を有効にすると、ユーザープロファイルの作成時に使用されるローカルプロファイルをテンプレートプロファイルが上書きできるようになります。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定が構成されていない場合、テンプレートは使用されません。

テンプレートプロファイルが移動プロファイルを上書きする

この設定により、ユーザープロファイルの作成時にテンプレートプロファイルが移動プロファイルを上書きできるようになります。

ユーザーがCitrixユーザープロファイルを持たず、移動Windowsユーザープロファイルを持っているとします。この場合、この値が有効になっていると、デフォルトで移動プロファイルが使用され、ユーザーストアに移行されます。このポリシー設定を有効にすると、ユーザープロファイルの作成時に使用される移動プロファイルをテンプレートプロファイルが上書きできるようになります。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定が構成されていない場合、テンプレートは使用されません。

すべてのログオンでCitrix強制プロファイルとして使用されるテンプレートプロファイル

この設定により、Profile Managementはテンプレートプロファイルをすべてのユーザープロファイル作成のデフォルトプロファイルとして使用できるようになります。

デフォルトでは、この設定は無効になっており、新しいユーザープロファイルは、ユーザーが最初にログオンしたデバイスのデフォルトユーザープロファイルから作成されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定が構成されていない場合、テンプレートは使用されません。

レジストリポリシー設定

このセクションには、Profile Management の処理に含める、または除外するレジストリキーを指定するポリシー設定が含まれています。

除外リスト

ログオフ時に無視されるHKCUハイブ内のレジストリキーのリスト。

例: Software\Policies

このポリシーが無効になっている場合、レジストリキーは除外されません。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、レジストリキーは除外されません。

包含リスト

ログオフ時に処理されるHKCUハイブ内のレジストリキーのリスト。

例: Software\Adobe。

このポリシーが有効になっている場合、このリストにあるキーのみが処理されます。このポリシーが無効になっている場合、HKCUハイブ全体が処理されます。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、HKCUのすべてが処理されます。

デフォルトの除外リストを有効にする - Profile Management 5.5

ユーザープロファイルに同期されないHKCUハイブ内のレジストリキーのデフォルトリスト。このポリシーを使用して、GPO除外ファイルを手動で入力することなく指定します。

このポリシーを無効にすると、Profile Management はデフォルトでレジストリキーを除外しません。ここでこのポリシーを構成しない場合、Profile Management は .ini ファイルの値を使用します。ここで、または .ini ファイルでこのポリシーを構成しない場合、Profile Management はデフォルトでレジストリキーを除外しません。

NTUSER.DATのバックアップ

NTUSER.DATの最後に正常だったコピーのバックアップを有効にし、破損がある場合にロールバックします。

ここでこのポリシーを構成しない場合、Profile Management は .ini ファイルの値を使用します。ここで、または .ini ファイルでこのポリシーを構成しない場合、Profile Management は NTUSER.DAT をバックアップしません。

ストリーム配信ユーザープロファイルポリシー設定

このセクションには、Profile Management がストリーム配信ユーザープロファイルを処理する方法を指定するポリシー設定が含まれています。

常にキャッシュ

この設定は、ユーザーのログオン後、Profile Management がストリーム配信ファイルをできるだけ早くキャッシュするかどうかを指定します。ユーザーのログオン後にファイルをキャッシュすると、ネットワーク帯域幅が節約され、ユーザーエクスペリエンスが向上します。

この設定は、**プロファイルストリーミング**設定と組み合わせて使用します。

デフォルトでは、この設定は無効になっており、ユーザーのログオン後、ストリーム配信ファイルはできるだけ早くキャッシュされません。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

ここでも .ini ファイルでもこの設定が構成されていない場合、この設定は無効になります。

常にキャッシュするサイズ

この設定は、ストリーミングされるファイルのサイズの下限をMB単位で指定します。Profile Management は、ユーザーがログオンした直後に、このサイズ以上のファイルをキャッシュします。

デフォルトでは、値は 0 (ゼロ) に設定されており、プロファイル全体をキャッシュする機能が使用されます。プロファイル全体をキャッシュする機能が有効になっている場合、Profile Management は、ユーザーのログオン後、ユーザーストア内のすべてのプロファイルコンテンツをバックグラウンドタスクとしてフェッチします。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

ここでも .ini ファイルでもこの設定が構成されていない場合、この設定は無効になります。

プロファイルストリーミング

この設定は、Citrix® ストリーミングユーザープロファイル機能を有効または無効にします。有効にすると、プロファイルファイルとフォルダーは、ユーザーがログオン後にアクセスした場合にのみ、ユーザーストアからローカルコンピューターにフェッチされます。レジストリエントリと保留領域のファイルはすぐにフェッチされます。

既定では、プロファイルストリーミングは無効になっています。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、無効になります。

ストリーミングされたユーザープロファイルグループ

この設定は、Windows ユーザーグループに基づいて、OU 内のどのユーザープロファイルをストリーム配信するかを指定します。

有効にすると、指定されたユーザーグループ内のユーザープロファイルのみがストリーミングされます。その他のすべてのユーザープロファイルは通常どおり処理されます。

既定では、この設定は無効になっており、OU内のすべてのユーザープロファイルは通常どおり処理されます。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、すべてのユーザープロファイルが処理されます。

プロファイルストリーミング除外を有効にする

プロファイルストリーミング除外が有効な場合：

- Profile Managementは、除外リスト内のフォルダーをストリーミングしません
- ユーザーがログオンすると、すべてのフォルダーがユーザーストアからローカルコンピューターにすぐにフェッチされます

詳しくは、「ユーザープロファイルのストリーミング」を参照してください。

ペンディングエリアロックファイルのタイムアウト

この設定は、ストレージサーバーが応答しなくなったときにユーザーストアがロックされたままの場合、ペンディングエリアからユーザーストアにユーザーファイルが書き戻されるまでの日数を指定します。この動作により、ペンディングエリアの肥大化が防止され、ユーザーストアに常に最新のファイルが含まれることが保証されます。

デフォルトでは、この設定は1日（1）に設定されています。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、デフォルト値が使用されます。

ペンディングエリアのプロファイルストリーミングを有効にする

ペンディングエリア内のファイルとフォルダーに対してプロファイルストリーミング機能を有効にできます。

保留領域は、プロファイルストリーミングが有効になっている間、プロファイルの一貫性を確保するために使用されます。これは、同時セッションで変更されたプロファイルファイルとフォルダーを一時的に保存します。

既定では、このポリシーは無効になっており、ログオン時に保留領域内のすべてのファイルとフォルダーがローカルプロファイルにフェッチされます。このポリシーを有効にすると、保留領域内のファイルは要求されたときにのみローカルプロファイルにフェッチされます。このポリシーをプロファイルストリーミングポリシーと組み合わせて使用すると、同時セッションシナリオで最適なログオンエクスペリエンスを確保できます。

このポリシーは、フォルダーのプロファイルストリーミングを有効にするポリシーが有効になっている場合に、保留領域内のフォルダーに適用されます。

ユーザーパーソナライゼーションポリシー設定

Virtual Delivery Agent内でユーザーレイヤーのマウントを有効にするには、構成パラメータを使用して以下を指定します。

- ネットワーク上のどこでユーザーレイヤーにアクセスするか。
- 新しいユーザーレイヤーディスクがどのくらい大きくなるか。

そのため、利用可能なポリシーのリストには、次の2つのポリシーが表示されます。

- ユーザーレイヤーリポジトリパス - 値フィールドに「\\サーバー名またはアドレス\フォルダー名」の形式でパスを入力します。
- ユーザーレイヤーサイズGB - デフォルトのユーザーレイヤーサイズ10 GBは、Citrix®が推奨する最小値です。ユーザーレイヤーは、スペースが使用されるにつれて設定されたサイズまで拡張するシンプロビジョニングディスクです。ユーザーレイヤーのサイズが小さくなることはありません。

> **注:**
>
> ユーザーレイヤーサイズを増やすと、新しいユーザーレイヤーに影響し、既存のレイヤーを拡張します。レイヤーサイズを減らすと、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

詳細については、「ユーザーパーソナライゼーションレイヤー」を参照してください。

Virtual Delivery Agent ポリシー設定

Virtual Delivery Agent (VDA) セクションには、VDA とサイトのコントローラー間の通信を制御するポリシー設定が含まれています。

重要: 自動更新機能を使用しない場合、VDA が Delivery Controller™ に登録するには、これらの設定によって提供される情報が必要です。この情報は登録に必要であるため、VDA のインストール中にこの情報を提供しない限り、グループポリシーエディターを使用して以下の設定を構成する必要があります。

- コントローラー登録 IPv6 ネットマスク
- コントローラー登録ポート
- コントローラー SID
- コントローラー
- IPv6 コントローラー登録のみを使用
- サイト GUID

コントローラー登録 IPv6 ネットマスク

このポリシー設定により、管理者は VDA を優先サブネットのみに制限できます（グローバル IP が登録されている場合でも）。この設定は、VDA が登録する IPv6 アドレスとネットワークを指定します。VDA は、指定されたネットマスクに一致する最初のアドレスにのみ登録します。「IPv6 コントローラー登録のみを使用」ポリシー設定が有効になっている場合にのみ、この設定は有効です。

デフォルトでは、この設定は空白です。

コントローラー登録ポート

この設定は、**コントローラーの自動更新を有効にする** 設定が無効になっている場合にのみ使用してください。

この設定は、レジストリベースの登録を使用する際に、VDA がコントローラーに登録するために使用する TCP/IP ポート番号を指定します。

既定では、ポート番号は80に設定されています。

コントローラーSID

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用してください。

この設定は、レジストリベースの登録を使用する場合にVDAがコントローラーに登録するために使用する、スペース区切りのコントローラーセキュリティ識別子（SID）のリストを指定します。この設定はオプションであり、登録に使用されるコントローラーのリストを制限するために**コントローラー**設定と組み合わせて使用される場合があります。

既定では、この設定は空白です。

コントローラー

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用してください。

この設定は、レジストリベースの登録を使用する場合にVDAがコントローラーに登録するために使用する、スペース区切りのコントローラー完全修飾ドメイン名（FQDN）のリストを指定します。この設定はオプションであり、**コントローラーSID**設定と組み合わせて使用される場合があります。

既定では、この設定は空白です。

コントローラーの自動更新を有効にする

この設定により、VDAはインストール後にコントローラーに自動的に登録できるようになります。

VDAが登録されると、登録先のコントローラーは現在のコントローラーFQDNとSIDのリストをVDAに送信します。VDAはこのリストを永続ストレージに書き込みます。各コントローラーは、90分ごとにサイトデータベースでコントローラー情報を確認します。次のいずれかが発生した場合、コントローラーは登録済みのVDAに更新されたリストを送信します。

- 前回の確認以降にコントローラーが追加または削除された
- ポリシーの変更が発生した

VDAは、受信した最新のリストにあるすべてのコントローラーからの接続を受け入れます。

デフォルトでは、この設定は有効になっています。

IPv6コントローラー登録のみを使用

この設定は、VDAがControllerに登録するために使用するアドレス形式を制御します。

- 有効にすると、VDAはマシンのIPv6アドレスを使用してControllerに登録します。VDAがControllerと通信する場合、次のアドレス順序を使用します: グローバルIPアドレス、ユニークローカルアドレス (ULA)、リンクローカルアドレス (他のIPv6アドレスが利用できない場合)。

- 無効にすると、VDAはマシンのIPv4アドレスを使用してControllerに登録し、通信します。

デフォルトでは、この設定は無効になっています。

サイトGUID

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用してください。

この設定は、Active Directoryベースの登録を使用する際に、VDAがControllerに登録するために使用するサイトのグローバル一意識別子 (GUID) を指定します。

デフォルトでは、この設定は空白です。

HDX™ 3D Pro ポリシー設定

HDX 3D Proセクションには、ユーザー向けの画質構成ツールを有効化および構成するためのポリシー設定が含まれています。このツールを使用すると、ユーザーは利用可能な帯域幅の使用を最適化できます。この最適化のために、画質と応答性のバランスがリアルタイムで調整されます。

ロスレスを有効にする

この設定は、ユーザーが画質構成ツールを使用してロスレス圧縮を有効または無効にできるかどうかを指定します。デフォルトでは、ユーザーにロスレス圧縮を有効にするオプションは提供されません。

ユーザーがロスレス圧縮を有効にしたとします。この場合、画質は画質構成ツールで利用可能な最大値に自動的に設定されます。デフォルトでは、ユーザーデバイスとホストコンピューターの機能に応じて、GPUベースまたはCPUベースの圧縮のいずれかを使用できます。

HDX 3D Pro 品質設定

この設定は、画質構成ツールでユーザーが利用できる最小値と最大値を指定します。これらの値を使用して、ユーザーは画質構成ツールで画質調整の範囲を定義できます。

画質の値は0から100の範囲（両端を含む）で指定します。最大値は最小値以上である必要があります。

監視ポリシー設定

「**監視**」セクションには、プロセス、リソース監視、およびアプリケーション障害監視のポリシー設定が含まれています。

これらのポリシーのスコープは、以下に基づいて定義できます。

- サイト

- デリバリーグループ
- デリバリーグループの種類
- 組織単位
- タグ

プロセスおよびリソース監視のポリシー

CPU、メモリ、プロセスの各データポイントはVDAから収集され、監視データベースに保存されます。VDAからデータポイントを送信するとネットワーク帯域幅を消費し、それらを保存すると監視データベースの相当なスペースを消費します。特定のスコープ（たとえば、特定のデリバリーグループまたは組織単位）に対して、リソースデータ、プロセスデータ、またはその両方を監視したくない場合を考慮してください。この場合、ポリシーを無効にすることをお勧めします。

プロセス監視を有効にする

この設定を有効にすると、VDAがインストールされているマシンで実行されているプロセスの監視が可能になります。CPU使用率やメモリ使用量などの統計情報は監視サービスに送信されます。これらの統計情報は、Directorでのリアルタイム通知および履歴レポートに使用されます。

この設定のデフォルトは無効です。

リソース監視を有効にする

この設定を有効にすると、VDAがインストールされているマシンで重要なパフォーマンスカウンターの監視が可能になります。統計情報（CPU使用率、メモリ使用量、IOPS、ディスク遅延データなど）は監視サービスに送信されます。これらの統計情報は、Directorでのリアルタイム通知および履歴レポートに使用されます。

この設定のデフォルトは有効です。

スケーラビリティ

CPUおよびメモリデータは、各VDAから5分間隔でデータベースにプッシュされます。プロセスデータ（有効な場合）は10分間隔でデータベースにプッシュされます。IOPSおよびディスク待機時間データは1時間間隔でデータベースにプッシュされます。

CPUとメモリデータ

CPUとメモリのデータは、デフォルトで**有効**になっています。データ保持期間の値は以下のとおりです（Platinumライセンス）：

データ粒度	日数
5分間データ	1日

データ粒度	日数
10分間データ	7日
1時間データ	30日
日次データ	90日

IOPSとディスク待機時間データ

IOPSとディスク待機時間データは、デフォルトで**有効**です。データ保持期間の値は次のとおりです (Platinumライセンス):

データ粒度	日数
時間データ	3日間
日次データ	90日間

データ保持設定により、1つのVDAに対して1年間で次の情報を保存するために、約276 KBのディスク領域が必要になります:

- CPU
- メモリ
- IOPS
- ディスク遅延データ

マシン数	必要なストレージ容量の目安
1	276 KB
1K	270 MB
40K	10.6 GB

プロセスデータ

プロセスデータはデフォルトで**無効**です。必要に応じて、一部のマシンでプロセスデータを有効にすることをお勧めします。プロセスデータのデフォルトのデータ保持設定は次のとおりです。

データ粒度	日数
10分間データ	1日
時間データ	7日間

プロセスデータがデフォルトの保持設定で有効になっている場合、プロセスデータは1年間でVDAあたり約1.5 MB、ターミナルサービスVDA (TS VDA) あたり3 MBを消費します。

マシンの数	必要なストレージの目安 VDA	必要なストレージの目安 TS VDA
1	1.5 MB	3 MB
1K	1.5 GB	3 GB

注:

以前に提示された数値には、インデックス領域は含まれていません。また、すべての計算は概算であり、展開によって異なります。

オプション構成

必要に応じて、デフォルトの保持設定を変更できます。ただし、この構成は追加のストレージを消費します。以下の設定を有効にすることで、プロセス使用率データの精度を高めることができます。有効にできる構成は次のとおりです。

ENABLEMINUTELEVELGRANULARITYPROCESSUTILIZATION

ENABLEDAYLEVELGRANULARITYPROCESSUTILIZATION

これらの構成は、監視PowerShellコマンドレットから有効にできます: Set-MonitorConfiguration

アプリケーション障害監視のポリシー

デフォルトでは、**アプリケーション障害**タブには、マルチセッションOS VDAからのアプリケーション障害のみが表示されます。アプリケーション障害監視の設定は、以下の監視ポリシーで変更できます:

アプリケーション障害の監視を有効にする

この設定を使用して、アプリケーション障害監視を構成し、アプリケーションエラーまたは障害（クラッシュおよび未処理の例外）、あるいはその両方を監視します。 **値**を**なし**に設定すると、

アプリケーション障害監視が無効になります。 この設定のデフォルトは「アプリケーション障害のみ」です。

シングルセッションOS VDAでのアプリケーション障害の監視を有効にする

デフォルトでは、マルチセッションOS VDAでホストされているアプリケーションからの障害のみが監視されます。シングルセッションOS VDAを監視するには、ポリシーを**Allowed**に設定します。 この設定のデフォルトは**Prohibited**です。

障害監視から除外されるアプリケーションのリスト

障害監視の対象としないアプリケーションのリストを指定します。 デフォルトでは、このリストは空です。

Analytics用のデータ収集ポリシー

ANALYTICS用のVDAデータ収集

このポリシーを使用して、パフォーマンスおよびセキュリティ分析のために、Monitorサービスが VDAのパフォーマンスおよびセキュリティ関連のメトリックを収集することを有効または無効にします。デフォルトでは、ポリシーは**許可**されています。VDAからのデータ収集を停止するには、ポリシーを**禁止**に設定します。

セキュリティ監視のためのクリップボード場所メタデータ収集

このポリシーを使用して、セキュリティ監視、監査、コンプライアンスのために、Brokerサービスによるクリップボード場所メタデータ収集を有効または無効にします。デフォルトでは、ポリシーは**有効**です。VDAからのデータ収集を停止するには、ポリシーを**無効**に設定します。

パフォーマンス監視のための診断データ収集

このポリシーを使用して、セッション情報、UPM/EUEMサービスの状態、Microsoft Teamsの最適化、接続プロトコルなどの診断データを収集するために監視サービスを有効にします。デフォルトでは、ポリシーは**有効**です。VDAからのデータ収集を停止するには、ポリシーを**無効**に設定します。

ストレージ計画のヒント

グループポリシー。リソースデータまたはプロセスデータの監視に関心がない場合は、グループポリシーを使用してその両方または一方をオフにできます。詳細については、ポリシーの作成の**グループポリシー**セクションを参照してください。

データグルーミング。デフォルトのデータ保持設定を変更して、データを早期にグルーミングし、ストレージスペースを解放できます。グルーミング設定について詳しくは、「API を使用したデータアクセス」の「データの粒度と保持」を参照してください。

レジストリを使用してCOMポートおよびLPTポートリダイレクト設定を構成する

VDAバージョン7.0から7.8では、**COMポートおよびLPTポート**設定は、レジストリを使用してのみ構成できます。VDAバージョン7.0より前、およびVDAバージョン7.9以降では、これらの設定はWeb Studioで構成できます。詳しくは、「ポートリダイレクトポリシー設定」および「帯域幅ポリシー設定」を参照してください。

COMポートおよびLPTポートリダイレクトのポリシー設定は、VDAイメージまたはマシン上のHKLM\Software\Citrix\GroupPolicy\Defaults\Deprecatedにあります。

COMポートおよびLPTポートリダイレクトを有効にするには、次のようにREG_DWORD型の新しいレジストリキーを追加します。

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

レジストリキー	説明	許可される値
AllowComPortRedirection	COMポートリダイレクトを許可または禁止する	1（許可）または0（禁止）
LimitComBw	COMポートリダイレクトチャネルの帯域幅制限	数値
LimitComBWPercent	COMポートリダイレクトチャネルの帯域幅制限（セッションの総帯域幅に対する割合）	0～100の数値
AutoConnectClientComPorts	ユーザーデバイスからCOMポートを自動的に接続する	1（許可）または0（禁止）
AllowLptPortRedirection	LPTポートリダイレクトを許可または禁止する	1（許可）または0（禁止）
LimitLptBw	LPTポートリダイレクトチャネルの帯域幅制限	数値

レジストリキー	説明	許可される値
LimitLptBwPercent	LPTポートリダイレクトチャネルの帯域幅制限（セッションの総帯域幅に対する割合）	0〜100の数値
AutoConnectClientLptPorts	ユーザーデバイスからLPTポートを自動的に接続する	1 (許可) または 0 (禁止)

これらの設定を構成した後、マシンカタログを変更して、新しいマスターイメージまたは更新された物理マシンを使用するようにします。デスクトップは、ユーザーが次回ログオフしたときに新しい設定で更新されます。

コンフィギュレーション マネージャー 2012 用コネクタ ポリシー設定

Configuration Manager 2012用コネクタのセクションには、Citrix Connector 7.5エージェントを構成するためのポリシー設定が含まれています。

> **重要:**
>
> 警告、ログオフ、および再起動メッセージのポリシーは、手動で管理されているか、Provisioning Services によって管理されているマルチセッションOSマシンカタログへの展開にのみ適用されます。これらのマシンカタログの場合、コネクタサービスは、保留中のアプリケーションのインストールまたはソフトウェアアップデートがある場合にユーザーに警告します。

> MCSで管理されているカタログの場合、Web Studioを使用してユーザーに通知します。手動で管理されているシングルセッションOSカタログの場合、Configuration Managerを使用してユーザーに通知します。Provisioning Servicesで管理されているシングルセッションOSカタログの場合、Provisioning Servicesを使用してユーザーに通知します。

警告頻度間隔

この設定は、ユーザーへの警告メッセージの表示間隔を定義します。

間隔はddd.hh:mm:ssの形式で設定されます。ここで、:

- dddは日数で、オプションのパラメーターであり、0〜999の範囲です。
- hhは時間で、0〜23の範囲です。

- mmは分で、0〜59の範囲です。
- ssは秒で、0〜59の範囲です。

デフォルトでは、間隔設定は1時間（01:00:00）です。

警告メッセージボックスの本文テキスト

この設定には、今後のソフトウェアアップデートまたはログオフを必要とするメンテナンスについてユーザーに通知するメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージは次のとおりです: {TIMESTAMP} 作業を保存してください。サーバーは{TIMELEFT}後にメンテナンスのためオフラインになります。

警告メッセージボックスのタイトル

この設定には、ユーザーへの警告メッセージのタイトルバーの編集可能なテキストが含まれています。

デフォルトでは、タイトルは「Upcoming Maintenance」です。

警告期間

この設定は、メンテナンスのどれくらい前に警告メッセージが最初に表示されるかを定義します。

時間はddd.hh:mm:ssの形式で設定されます。ここで、:

- dddは日数で、オプションのパラメーターであり、範囲は0〜999です。
- hhは時間で、範囲は0〜23です。
- mmは分で、範囲は0〜59です。
- ssは秒で、範囲は0〜59です。

既定では、設定は16時間 (16:00:00) であり、最初の警告メッセージがメンテナンスの約16時間前に表示されることを示します。

最終強制ログオフメッセージボックスの本文テキスト

この設定には、強制ログオフが開始されたことをユーザーに警告するメッセージの編集可能なテキストが含まれています。

既定では、メッセージは次のとおりです: サーバーは現在、メンテナンスのためオフラインになります

最終強制ログオフメッセージボックスのタイトル

この設定には、最終強制ログオフメッセージのタイトルバーの編集可能なテキストが含まれています。

デフォルトでは、タイトルは「ITスタッフからの通知」です。

強制ログオフ猶予期間

この設定は、ユーザーにログオフを通知してから、保留中のメンテナンスを処理するための強制ログオフが実行されるまでの期間を定義します。

時刻はddd.hh:mm:ssの形式で設定されます。ここで、:

- dddは日数で、オプションのパラメーターであり、範囲は0〜999です。
- hhは時間で、範囲は0〜23です。
- mmは分で、範囲は0〜59です。
- ssは秒で、範囲は0〜59です。

デフォルトでは、設定は16時間（16:00:00）であり、最初の警告メッセージがメンテナンスの約16時間前に表示されることを示します。

最終強制ログオフメッセージボックスの本文

この設定には、強制ログオフが開始されたことをユーザーに警告するメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージは「The server is currently going offline for maintenance」です。

最終強制ログオフメッセージボックスのタイトル

この設定には、最終的な強制ログオフメッセージのタイトルバーの編集可能なテキストが含まれています。

デフォルトでは、タイトルは「ITスタッフからの通知」です。

強制ログオフ猶予期間

この設定は、ユーザーにログオフを通知してから、保留中のメンテナンスを処理するための強制ログオフが実行されるまでの期間を定義します。

時間はddd.hh:mm:ssの形式で設定され、ここで:

- dddは日数で、オプションのパラメーターであり、範囲は0〜999です。

- hhは時間で、範囲は0〜23です。
- mmは分で、範囲は0〜59です。
- ssは秒で、範囲は0〜59です。

デフォルトでは、強制ログオフ猶予期間の設定は5分（00:05:00）です。

強制ログオフメッセージボックスの本文

この設定には、強制ログオフを開始する前に作業を保存してログオフするようユーザーに伝えるメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージには次の内容が含まれます: {TIMESTAMP} 作業を保存してログオフしてください。サーバーは{TIMELEFT}後にメンテナンスのためオフラインになります。

強制ログオフメッセージボックスのタイトル

この設定には、強制ログオフメッセージのタイトルバーの編集可能なテキストが含まれています。

デフォルトでは、タイトルは「ITスタッフからの通知」です。

イメージ管理モード

Connectorエージェントは、Provisioning ServicesまたはMCSによって管理されているマシンのクローン上で実行されているかどうかを自動的に検出します。エージェントは、イメージ管理されたクローンでのConfiguration Managerの更新をブロックし、カタログのマスターイメージに更新を自動的にインストールします。

マスターイメージが更新された後、Web Studioを使用してMCSカタログクローンの再起動をオーケストレーションします。Connector Agentは、Configuration Managerのメンテナンスウィンドウ中にPVSカタログクローンの再起動を自動的にオーケストレーションします。この動作を上書きして、Configuration Managerによってカタログクローンにソフトウェアがインストールされるようにするには、「イメージ管理モード」を「無効」に変更します。

再起動メッセージボックスの本文

この設定には、サーバーが再起動されるときにユーザーに通知するメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージは「サーバーは現在、メンテナンスのためにオフラインになります。」です。

エージェントタスクを実行する通常の時間間隔

この設定は、Citrix Connector™エージェントタスクが実行される頻度を決定します。

時刻はddd.hh:mm:ss形式で設定されます。ここで、:

- dddは日数で、オプションのパラメーターであり、範囲は0～999です。
- hhは時間で、範囲は0～23です。
- mmは分で、範囲は0～59です。
- ssは秒で、範囲は0～59です。

既定では、定期的な時間間隔の設定は5分 (00:05:00) です。

ポリシーの変更

以下の表は、Citrix Virtual Apps and Desktops™ 7 2407におけるポリシーの更新（追加、削除、名前の変更、デフォルト状態の変更を含む）を示しています。

ポリシー設定	変更点
全般 - 依存ポリシーに関する明確化	詳細はこちら。
全般 - 複数のポリシーを選択する機能	詳細はこちら。
プロファイル管理 > 詳細設定 > ユーザー ストア間でのセッション内ポリシー コンテナ フェールオーバーを有効にする	ユーザー ストア間でのセッション内プロファイル コンテナ フェールオーバーに関する新しいポリシー。詳細はこちら。
プロファイル管理 > レジストリ > インクルージョン リスト	レジストリの除外と包含のサポートが、コンテナベースのプロファイル ソリューションに拡張されました。詳細はこちら。
プロファイル管理 > レジストリ > エクスクルージョン リスト	
プロファイル管理 > フォルダー リダイレクト	フォルダリダイレクトポリシーの機能強化。詳細はこちら(/ja-jp/profile-management/current-release/whats-new#enhancements-to-folder-redirection-policies)。
セッションメトリックの収集(/ja-jp/citrix-virtual-apps-desktops/2407/policies/policies-default-settings#ica)	詳細については、ICAポリシー設定(/ja-jp/citrix-virtual-apps-desktops/2407/policies/reference/ica-policy-settings#session-metric-collection)を参照してください。
クライアントプリンターポリシー設定 > 保持および復元されたクライアントプリンター(/ja-	2402以降非推奨

ポリシー設定	変更点
jp/citrix-virtual-apps-desktops/2402-ltsr/policies/reference/ica-policy-settings/printing-policy-settings/client-printers-policy-settings#retained-and-restored-client-printers)	

注：

アップグレードする前に、すべての非推奨設定を削除してください。非推奨設定が使用されたままになっている場合、アップグレードはエラーで失敗する可能性があります。

管理

Citrix Virtual Apps and Desktops™ サイトの管理には、さまざまな項目とタスクが含まれます。

ライセンス

サイトを作成する際には、Citrix License Serverへの有効な接続が必要です。後で、Studioからライセンスの追加、ライセンスの種類やモデルの変更、ライセンス管理者の管理など、いくつかのライセンス関連タスクを完了できます。Studioからライセンス管理コンソールにアクセスすることもできます。

アプリケーション

デリバリーグループ、およびオプションでアプリケーショングループ内のアプリケーションを管理します。

ゾーン

地理的に分散した展開では、ゾーンを使用してアプリケーションとデスクトップをエンドユーザーに近づけることで、パフォーマンスを向上させることができます。サイトをインストールして構成すると、すべてのコントローラー、マシンカタログ、およびホスト接続は1つのプライマリゾーンに配置されます。後で、Studioを使用して、これらの項目を含むサテライトゾーンを作成できます。サイトに複数のゾーンがある場合、新しく作成されたマシンカタログ、ホスト接続、または追加されたコントローラーがどのゾーンに配置されるかを示すことができます。ゾーン間で項目を移動することもできます。

接続とリソース

ハイパーバイザーまたはその他のサービスを使用して、ユーザーにアプリケーションとデスクトップを提供するマシンをホストしている場合、サイトを作成する際に、そのハイパーバイザーまたはその他のサービスへの最初の接続を作成します。その接続のストレージとネットワークの詳細が、そのリソースを構成します。後で、その接続とそのリソースを変更したり、さらに多くの接続を作成したりできます。構成された接続を使用するマシンを管理することもできます。

ローカルホストキャッシュ

ローカルホストキャッシュを使用すると、Delivery Controller™とサイトデータベース間の接続が失敗した場合でも、サイト内の接続仲介操作を続行できます。

仮想IPと仮想ループバック

Microsoft の仮想IPアドレス機能は、公開アプリケーションにセッションごとに一意の動的に割り当てられたIPアドレスを提供します。Citrix の仮想ループバック機能を使用すると、localhost との通信に依存するアプリケーションを、localhost 範囲内の一意の仮想ループバックアドレスを使用するように構成できます。

デリバリーコントローラー

この記事では、サイトへのControllerの追加と削除に関する考慮事項と手順について説明します。また、Controllerを別のゾーンまたはサイトに移動する方法、およびVDAを別のサイトに移動する方法についても説明します。

ControllerへのVDA登録

VDAがアプリケーションとデスクトップの配信を支援する前に、Controllerに登録（通信を確立）する必要があります。Controllerのアドレスはいくつかの方法で指定でき、それらについてはこの記事で説明します。サイトでControllerが追加、移動、削除される際に、VDAが最新の情報を持っていることが重要です。

セッション

セッションアクティビティを維持することは、最高のユーザーエクスペリエンスを提供するために不可欠です。いくつかの機能により、セッションの信頼性を最適化し、不便さ、ダウンタイム、生産性の損失を軽減できます。

- セッションの信頼性
- クライアントの自動再接続
- ICA®キープアライブ
- ワークスペースコントロール
- セッションローミング

Studioでの検索の使用

Studioでマシン、セッション、マシンカタログ、アプリケーション、またはデリバリーグループに関する情報を表示したい場合は、柔軟な検索機能を使用します。

タグ

タグを使用して、マシン、アプリケーション、グループ、ポリシーなどのアイテムを識別します。その後、特定のタグを持つアイテムに適用されるように特定の操作を調整できます。

IPv4/IPv6

Citrix Virtual Apps and Desktops は、純粋な IPv4、純粋な IPv6、および IPv4 と IPv6 の重複するネットワークを使用するデュアルスタック展開をサポートしています。この記事では、これらの展開について説明し、図解します。また、IPv4 または IPv6 の使用を制御する Citrix ポリシー設定についても説明します。

ユーザープロファイル

デフォルトでは、VDA をインストールすると Citrix Profile Management が自動的にインストールされます。このプロファイルソリューションを使用する場合は、一般的な情報についてこの記事を確認してください。詳細については、Profile Management のドキュメントを参照してください。

Citrix Diagnostic Facility (CDF) トレースの収集

CDFControl ユーティリティは、さまざまな Citrix トレースプロバイダーから表示される Citrix Diagnostic Facility (CDF) トレースメッセージをキャプチャするためのイベントトレースコントローラーまたはコンシューマーです。これは、複雑な Citrix 関連の問題のトラブルシューティング、フィルターサポートの解析、およびパフォーマンスデータの収集のために作成されています。

シトリックス インサイト サービス

Citrix Insight Services (CIS) は、計測、テレメトリ、およびビジネスインサイト生成のための Citrix プラットフォームです。

シトリックス スカウト

Citrix Scout は診断情報を収集し、ヘルスチェックを実行します。結果は、Citrix Virtual Apps and Desktops 展開におけるプロアクティブなメンテナンスに利用できます。Citrix は、Citrix Insight Services を通じて、診断コレクションの包括的な自動分析を提供します。また、Scout を使用して、単独で、または Citrix サポートのガイダンスを受けて問題をトラブルシューティングすることもできます。

アプリケーション

> **注:**
>
> Citrix Virtual Apps and Desktops™の展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb

> Studioのみを扱います。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

展開でデリバリーグループのみを使用している場合（アプリケーショングループは使用しない場合）、アプリケーションはデリバリーグループに追加します。アプリケーショングループも使用している場合は、通常、代わりにアプリケーショングループにアプリケーションを追加します。このガイダンスにより、管理が容易になります。アプリケーションは常に少なくとも1つのデリバリーグループまたはアプリケーショングループに属している必要があります。

アプリケーションの追加ウィザードでは、1つ以上のデリバリーグループ、または1つ以上のアプリケーショングループを選択できますが、両方を同時に選択することはできません。後でアプリケーションのグループ関連付けを変更することはできますが（たとえば、アプリケーションをアプリケーショングループからデリバリーグループに移動するなど）、ベストプラクティスとしては、そのような複雑さを追加することは推奨されません。アプリケーションは1種類のグループに保持してください。

アプリケーションを複数のグループに関連付けると、それらのすべてのグループでアプリケーションを表示する十分な権限がない場合に、表示の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが関連付けられているすべてのグループを含むようにスコープを拡張してください。

同じ名前の2つのアプリケーション（異なるグループからのものなど）を同じユーザーに公開する場合、Web Studioで`Application name (for user)`プロパティを変更します。そうしないと、ユーザーはCitrix Workspace™アプリで重複する名前を目にすることになります。

アプリケーションのプロパティ（設定）は、追加時または後で変更できます。アプリケーションが配置されているアプリケーションフォルダーも、アプリケーションの追加時または後で変更できます。

詳細については、以下を参照してください。

- デリバリーグループの作成
- アプリケーショングループの作成
- タグ

アプリケーションの追加

アプリケーションは、デリバリーグループまたはアプリケーショングループの作成時に追加できます。これらの手順は、デリバリーグループの作成およびアプリケーショングループの作成に詳しく説明されています。以下の手順では、グループ作成後にアプリケーションを追加する方法について説明します。

知っておくべきこと:

- Remote PC Accessデリバリーグループにはアプリケーションを追加できません。
- アプリケーションの追加ウィザードを使用して、デリバリーグループまたはアプリケーショングループからアプリケーションを削除することはできません。これは別の操作です。

1つ以上のアプリケーションを追加するには：

1. 左ペインで**［Applications］**を選択し、アクションバーで**［Add Applications］**を選択します。
2. アプリケーションの追加ウィザードが**［Introduction］**ページとともに起動します。このページは、次回以降のウィザード起動時に表示しないように設定できます。
3. ウィザードは、**［Groups］**、**［Applications］**、**［Summary］**の各ページを案内します。各ページの作業が完了したら、**［Next］**をクリックして**［Summary］**ページに進みます。

単一のデリバリーグループまたはアプリケーショングループにアプリケーションを追加する場合の、手順1の代替案:

- **1つのデリバリーグループにのみアプリケーションを追加する場合：** 手順1で、Web Studioの左ペインで**［Delivery Groups］**を選択し、中央ペインでデリバリーグループを選択してから、アクションバーで**［Add Applications］**を選択します。ウィザードには**［Groups］**ページが表示されません。
- **1つのアプリケーショングループにのみアプリケーションを追加する場合：** 手順1で、Web Studioの左ペインで**［Applications］**を選択し、中央ペインでアプリケーショングループを選択してから、アクションバーのアプリケーショングループ名の配下にある**［Add Applications］**エントリを選択します。ウィザードには**［Groups］**ページが表示されません。

グループページ

このページには、サイト内のすべてのデリバリーグループが一覧表示されます。アプリケーショングループも作成している場合は、アプリケーショングループとデリバリーグループが一覧表示されます。どちらかのグループを選択できますが、両方のグループを選択することはできません。つまり、アプリケーショングループとデリバリーグループに同時にアプリケーションを追加することは

できません。通常、アプリケーショングループを使用している場合は、デリバリーグループではなくアプリケーショングループにアプリケーションを追加します。

アプリケーションを追加するときは、少なくとも1つのデリバリーグループ（または利用可能な場合はアプリケーショングループ）の横にあるチェックボックスをオンにします。すべてのアプリケーションは、常に少なくとも1つのグループに関連付けられている必要があります。

アプリケーションページ

［Add］をクリックしてアプリケーションソースを表示します。

- **メニューから:** 選択したデリバリーグループ内のマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、 をクリックします。

  このソースは、(1)関連付けられたデリバリーグループのないアプリケーショングループを選択した場合、(2)関連付けられたデリバリーグループにマシンが含まれていないアプリケーショングループを選択した場合、または(3)マシンが含まれていないデリバリーグループを選択した場合は選択できません。

- **手動で:** デリバリーグループ内のVDAまたはネットワーク上の別の場所にあるアプリケーション。このソースを選択すると、新しいページが開き、次の方法で追加するアプリケーションを指定できます。

  - 実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、および管理者とユーザーの表示名を入力します。
  - デリバリーグループ内のVDAからアプリケーションを選択します。これを行うには、 をクリックし、VDAにアクセスするための資格情報を入力し、VDAへの接続を待ってから、VDAからアプリケーションを選択します。選択したアプリケーションのプロパティが、ページ上のフィールドに自動的に入力されます。

- **既存:** 以前にサイトに追加されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、 をクリックします。

  サイトにアプリケーションがない場合、このソースは選択できません。

- **アプリケーションパッケージ:** App-V、MSIX、MSIX app attach、またはFlexAppアプリケーションパッケージ内のアプリケーション。このソースを選択すると、 ページが起動します。アプリケーションパッケージソースを選択し、表示された結果から追加するアプリケーションを選択して、 を選択します。詳しくは、「アプリパッケージの展開と配信」を参照してください。

- **アプリケーショングループ:** アプリケーショングループ。このソースを選択すると、アプリケーショングループのリストを含む新しいページが起動します。（表示には各グループ内のアプリケーションもリストされますが、個々のアプリケーションではなくグループのみを選択できます。）選択したグループ内の現在および将来のすべてのアプリケーションが追加されます。追加するアプリケーショングループのチェックボックスをオンにして、 をクリックします。

  このソースは、(1)アプリケーショングループがない場合、または(2)選択したデリバリーグループがアプリケーショングループをサポートしていない場合（たとえば、静的に割り当てられたマシンを持つデリバリーグループ）は選択できません。

表に示されているように、 リストの一部のソースは、その種類の有効なソースがない場合は選択できません。互換性のないソース（たとえば、アプリケーショングループにアプリケーショングループを追加できないなど）はリストに含まれません。選択したグループに既に追加されているアプリケーションは選択できません。

このページまたは後で、アプリケーションのプロパティ（設定）を変更できます。

デフォルトでは、追加されたアプリケーションは`Applications`という名前のアプリケーションフォルダーに配置されます。アプリケーションは、このページまたは後で変更できます。アプリケーションを追加しようとして、同じ名前のアプリケーションが同じフォルダーに存在する場合、追加するアプリケーションの名前を変更するように求められます。提示された新しい名前を受け入れるか、拒否してアプリケーションの名前を変更するか、別のフォルダーを選択できます。たとえば、 フォルダーに`app`が既に存在し、そのフォルダーに`app`という名前の別のアプリケーションを追加しようとすると、新しい名前`app_1`が提示されます。

概要ページ

10個以下のアプリケーションを追加する場合、それらの名前は**** にリストされます。10個を超えるアプリケーションを追加する場合、合計数が指定されます。

概要情報を確認し、**「完了」**をクリックします。

アプリケーションのグループ関連付けを変更する

アプリケーションを追加した後、そのアプリケーションが関連付けられているデリバリーグループとアプリケーショングループを変更できます。

アプリケーションを別のグループにドラッグできます。これは、アクションバーのコマンドを使用する代替手段です。

アプリケーションが複数のデリバリーグループまたはアプリケーショングループに関連付けられている場合、グループの優先度を使用して、アプリケーションを検索するために複数のグループがチェックされる順序を指定できます。デフォルトでは、すべてのグループの優先度は0（最高）です。同じ優先度のグループは負荷分散されます。

アプリケーションは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。また、共有マシンを含むデリバリーグループがデスクトップのみを配信する場合でも、(1) デリバリーグループに共有マシンが含まれており、XenDesktop 7.x のバージョン 7.9 より前のバージョンで作成されていること、および (2) `Edit delivery group` 権限がある場合に限り、そのデリバリーグループを選択できます。プロパティダイアログがコミットされると、デリバリーグループの種類は自動的に `desktops and applications` に変換されます。

1. Web Studioにサインインし、左側のペインで**アプリケーション**を選択し、アプリケーションを選択します。
2. アクションバーで**プロパティ**を選択します。
3. **グループ**ページを選択します。
    - グループを追加するには、**追加**をクリックし、**アプリケーショングループ**または**デリバリーグループ**を選択します。（アプリケーショングループを作成していない場合、唯一の項目は**デリバリーグループ**です。）次に、利用可能なグループを1つ以上選択します。アプリケーションと互換性のないグループ、またはすでにアプリケーションに関連付けられているグループは選択できません。
    - グループを削除するには、1つ以上のグループを選択し、**削除**をクリックします。グループの関連付けを削除した結果、アプリケーションがどのグループにも関連付けられなくなる場合、アプリケーションが削除されることを警告されます。
    - グループの優先度を変更するには、グループを選択し、**優先度の編集**をクリックします。優先度値を選択し、**OK**をクリックします。
4. 完了したら、**適用**をクリックして変更を適用し、ウィンドウを開いたままにするか、**OK**をクリックして変更を適用し、ウィンドウを閉じます。

アプリケーションの複製、有効化または無効化、名前の変更、または削除

次のアクションが利用可能です。

- **複製:** アプリケーションを複製して、異なるパラメーターやプロパティを持つ別のバージョンを作成したい場合があります。アプリケーションを複製すると、一意のサフィックスで自動的

に名前が変更され、元のアプリケーションの隣に配置されます。アプリケーションを複製してから、別のグループに追加したい場合もあります。(複製後、アプリケーションを移動する最も簡単な方法はドラッグすることです。)

- **有効化または無効化:** アプリケーションの有効化と無効化は、デリバリーグループまたはアプリケーショングループの有効化と無効化とは異なるアクションです。
- **名前の変更:** 一度に1つのアプリケーションのみ名前を変更できます。アプリケーションの名前を変更しようとして、同じ名前のアプリケーションが同じフォルダーまたはグループに存在する場合、別の名前を指定するように求められます。
- **削除:** アプリケーションを削除すると、関連付けられていたデリバリーグループおよびアプリケーショングループから削除されますが、元々アプリケーションを追加するために使用されたソースからは削除されません。アプリケーションの削除は、デリバリーグループまたはアプリケーショングループから削除するのとは異なるアクションです。

アプリケーションを複製、有効化、無効化、名前変更、または削除するには：

1. 左ペインで を選択します。
2. 中央ペインで1つ以上のアプリケーションを選択し、アクションバーで適切なタスクを選択します。
3. プロンプトが表示されたら、アクションを確認します。

デリバリーグループからアプリケーションを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに関連付けられている（属している）必要があります。アプリケーションをデリバリーグループから削除しようとして、そのアプリケーションがどのデリバリーグループまたはアプリケーショングループとの関連付けも失うことになる場合、続行するとアプリケーションが削除されることが通知されます。そのような場合、そのアプリケーションを配信したい場合は、有効なソースから再度追加する必要があります。

1. 左ペインで を選択します。
2. デリバリーグループを選択します。中央下部のペインで、 タブから削除するアプリケーションを選択します。
3. アクションバーから を選択します。
4. 削除を確認します。

アプリケーショングループからアプリケーションを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに属している必要があります。アプリケーションをアプリケーショングループから削除しようとして、その結果、そのアプリケーションがどのグループにも属さなくなる場合、続行するとアプリケーションが削除されるという通知が表示されます。その場合、そのアプリケーションを配信したい場合は、有効なソースから再度追加する必要があります。

1. 左側のペインで、 を選択します。
2. 中央のペインでアプリケーショングループを選択し、1つまたは複数のアプリケーションを選択します。
3. アクションバーで を選択します。
4. 削除を確認します。

アプリケーションのプロパティを変更する

アプリケーションのプロパティは、一度に1つしか変更できません。

アプリケーションのプロパティを変更するには：

1. 左側のペインで を選択します。
2. アプリケーションを選択し、アクションバーで を選択します。
3. 変更するプロパティが含まれるページを選択します。
4. 完了したら、 をクリックして変更を適用し、ウィンドウを開いたままにするか、 をクリックして変更を適用してウィンドウを閉じます。

次のリストでは、ページが括弧内に示されています。

プロパティ	ページ
Citrix Workspace アプリケーション内でアプリケーションが提示される分類または格納場所	デリバリー
コマンドライン引数。公開アプリケーションにパラメーターを渡すを参照	場所
アプリケーションが利用可能なデリバリーグループとアプリケーショングループ	グループ
説明	識別

プロパティ	ページ
ファイル名拡張子とファイルの種類関連付け: アプリケーションが自動的に開く拡張子	ファイルの種類関連付け
アイコン	デリバリー
StoreFront™用キーワード	識別
制限。アプリケーション制限の構成を参照	配信
名前：ユーザーおよび管理者から見える名前	識別
実行可能ファイルへのパス。「公開アプリケーションにパラメーターを渡す」を参照してください。	場所
ユーザーのデスクトップ上のショートカット：有効または無効	配信
可視性：Citrix Workspaceアプリでアプリケーションを表示できるユーザーを制限します。非表示のアプリケーションでも起動できます。利用不可かつ非表示にするには、別のグループに追加します。	可視性の制限
作業ディレクトリ	場所

アプリケーションの変更は、現在のアプリケーションユーザーがセッションからログオフするまで有効にならない場合があります。

アプリケーション制限を構成する

アプリケーション制限を構成して、アプリケーションの使用を管理します。たとえば、アプリケーション制限を使用して、アプリケーションに同時にアクセスするユーザーの数を管理できます。同様に、アプリケーション制限を使用して、リソースを大量に消費するアプリケーションの同時インスタンス数を管理できます。この制限は、サーバーのパフォーマンスを維持し、サービスの劣化を防ぐのに役立ちます。

この機能は、Controllerによって仲介されるアプリケーション起動の数（Citrix WorkspaceアプリやStoreFrontなどからの起動）を制限するものであり、他の方法で起動できる実行中のアプリケーションの数を制限するものではありません。これは、アプリケーション制限が同時使用の管理に

おいて管理者を支援するものの、すべてのシナリオで強制力を持つわけではないことを意味します。たとえば、Controllerが停止モードの場合、アプリケーション制限は適用できません。

デフォルトでは、同時に実行できるアプリケーションインスタンスの数に制限はありません。アプリケーション制限の設定はいくつかあります。それらのいずれか、またはすべてを構成できます。

- デリバリーグループ内のすべてのユーザーによる、アプリケーションの同時実行インスタンスの最大数。
- デリバリーグループ内のユーザーごとのアプリケーションインスタンス数（1つ）。
- マシンごとのアプリケーションの同時実行インスタンスの最大数（PowerShellのみ）。

制限が構成されている場合、ユーザーが構成された制限を超えるアプリケーションインスタンスを起動しようとすると、エラーメッセージが生成されます。複数の制限が構成されている場合、最初に到達した制限でエラーが報告されます。

アプリケーション制限の使用例：

- **同時インスタンス数の上限:** デリバリーグループで、アプリケーション `Alpha` の同時インスタンスの最大数を15に構成します。その後、そのデリバリーグループのユーザーは、そのアプリケーションのインスタンスを15個同時に実行しています。そのデリバリーグループのいずれかのユーザーが `Alpha` を起動しようとすると、エラーメッセージが生成されます。構成された同時アプリケーションインスタンスの制限（15）を超えるため、`Alpha` は起動されません。
- **ユーザーごとのインスタンス数制限:** 別のデリバリーグループで、アプリケーション `Beta` のユーザーごとのインスタンス数オプションを有効にします。ユーザーのTonyはアプリケーション `Beta` を正常に起動します。その日の後半、そのアプリケーションがTonyのセッションでまだ実行されている間に、彼は `Beta` の別のインスタンスを起動しようとします。ユーザーごとのインスタンス数制限を超えるため、エラーメッセージが生成され、`Beta` は起動されません。
- **同時インスタンス数の上限とユーザーごとのインスタンス数制限:** 別のデリバリーグループで、同時インスタンスの最大数を10に構成し、アプリケーション `Delta` のユーザーごとのインスタンス数オプションを有効にします。その後、そのデリバリーグループの10人のユーザーがそれぞれ `Delta` のインスタンスを実行している場合、そのデリバリーグループの他のユーザーが `Delta` を起動しようとすると、エラーメッセージが表示されます。`Delta` は起動されません。現在の10人の `Delta` ユーザーのいずれかがそのアプリケーションの2番目のインスタンスを起動しようとすると、エラーメッセージが表示され、2番目のインスタンスは起動されません。

- **マシンごとの同時インスタンス数の上限とタグ制限の使用:** アプリケーション `Charlie` には、特定のサーバーで同時に実行できるインスタンスの数を規定するライセンスおよびパフォーマンス要件があります。これらの要件は、サイト内のすべてのサーバーで同時に実行できるインスタンスの数も規定します。

  アプリケーションのインスタンス数/マシン制限は、サイト内の任意のサーバー（特定のデリバリーグループ内のマシンだけでなく）に影響します。サイトに3台のサーバーがあるとします。アプリケーション `Charlie` の場合、マシンごとのアプリインスタンス制限を2に構成します。したがって、サイト全体でアプリケーション `Charlie` のインスタンスは6つまでしか起動できません。（これは、3台のサーバーそれぞれでCharlieのインスタンスが2つという制限です。）

  アプリケーションの使用をデリバリーグループ内の特定のコンピューターのみに制限するには（サイト全体のすべてのコンピューターでのインスタンス制限に加えて）：

  - それらのマシンにタグ付け機能を使用します。
  - そのアプリケーションのマシンごとのインスタンス数の最大制限を構成します。

アプリケーションがControllerブローカー以外の方法（たとえば、Controllerが停止モードの場合など）で起動され、構成された制限を超過した場合、ユーザーは制限を超過しないように十分なインスタンスを閉じるまで、それ以上のインスタンスを起動できません。制限を超過したインスタンスは強制的にシャットダウンされません。ユーザーがそれらを閉じるまで、実行が許可されます。

セッションローミングを無効にする場合は、ユーザーごとのアプリケーションインスタンス数制限を無効にします。ユーザーごとのアプリケーションインスタンス数制限を有効にする場合は、新しいデバイスでの新しいセッションを許可する2つの値のいずれも構成しないでください。ローミングについて詳しくは、「セッション」(/ja-jp/citrix-virtual-apps-desktops/2407/manage-deployment/sessions.html)を参照してください。

デリバリーグループごとの最大インスタンス数制限と、ユーザーごとのインスタンス数制限を構成するには：

1. 左側のペインで **［アプリケーション］** を選択し、アプリケーションを選択します。
2. アクションバーで **［アプリケーションプロパティの編集］** を選択します。
3. **［配信］** ページで、次のいずれかのオプションを選択します。

   - **アプリケーションの無制限の使用を許可する**。同時に実行できるインスタンスの数に制限はありません。これがデフォルトです。
   - **アプリケーションの制限を設定する**。制限の種類は2つあります。いずれか一方または両方を指定します。

    - マシンごとに同時に実行できるインスタンスの最大数を指定します
    - ユーザーごとにアプリケーションのインスタンスを1つに制限する

4. **［OK］** をクリックして変更を適用し、ダイアログボックスを閉じます。または、 **［適用］** をクリックして変更を適用し、ダイアログボックスを開いたままにします。

マシンごとの最大インスタンス数制限を構成するには（PowerShellのみ）：

- PowerShellで（Citrix Cloud™展開の場合はRemote PowerShell SDKを、オンプレミス展開の場合はPowerShell SDKを使用して）、適切な`BrokerApplication`コマンドレットを`MaxPerMachineInstances`パラメーターとともに指定します。
- ガイダンスについては、`Get-Help`コマンドレットを使用してください。例：

  ```
  Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
  ```

公開アプリケーションにパラメーターを渡す

アプリケーションのプロパティの**場所**ページを使用して、コマンドラインを入力し、公開アプリケーションにパラメータを渡します。

公開アプリケーションをファイルの種類に関連付けると、`"%*"` (二重引用符で囲まれたパーセント記号とアスタリスク記号) がアプリケーションのコマンドラインの末尾に追加されます。これらの記号は、ユーザーデバイスに渡されるパラメータのプレースホルダーとして機能します。

公開アプリケーションが期待どおりに起動しない場合は、そのコマンドラインに正しい記号が含まれていることを確認してください。デフォルトでは、`"%*"` 記号が追加されると、ユーザーデバイスから提供されるパラメータが検証されます。ユーザーデバイスから提供されるカスタマイズされたパラメータを使用する公開アプリケーションの場合、コマンドライン検証をバイパスするために、`"%**"` 記号がコマンドラインに追加されます。アプリケーションのコマンドラインにこれらの記号が表示されない場合は、手動で追加してください。

実行可能ファイルへのパスにスペースを含むディレクトリ名が含まれている場合 (`"C:\Program Files"` など)、そのスペースがコマンドラインの一部であることを示すために、アプリケーションのコマンドラインを二重引用符で囲みます。これを行うには、パスを二重引用符で囲み、`%*` 記号を別の二重引用符で囲みます。パスの閉じ引用符と `%*` 記号の開き引用符の間にスペースを含めるようにしてください。

たとえば、公開アプリケーションであるWindows Media Playerのコマンドラインは次のとおりです。

```
"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"
```

> **注：**
>
> 公開アプリケーションを起動するためのコマンドラインの最大文字数 (引数を含む) は203文字です。

公開アプリケーションでのセッションサインアウトの問題のトラブルシューティング

アプリケーションを公開する場合、公開アプリケーションのメイン実行可能ファイルのみが指定されます。しかし、一部のアプリケーションは、バックグラウンドで実行され、メインの公開アプリケーションが閉じられたときに、対応するメイン実行可能ファイルによって閉じられない追加の（子）プロセスを生成する場合があります。追加のプロセスは、実行されるスクリプトや、`Run` や `RunOnceKey` のような特定のレジストリキーから作成されることもあります。これらのアプリケーションは、正常なサインアウトを妨げ、セッションが残存したりハングしたりする原因となり、セッションが閉じられず、ユーザーがサインアウトされない可能性があります。

この場合、Citrix Director を使用してこれらのセッションをリセットまたは終了する必要があります。

適切にサインアウトされないセッションを特定し、トラブルシューティングするために、Citrixは3つのレジストリエントリを提供しています。これらの問題により適切にログオフされないセッションの特定とトラブルシューティングは、次の3つのステップからなるプロセスです。

1. どのセッションが公開アプリケーションによって正常なサインアウトを妨げているかを特定する
2. それらの公開アプリケーションが追加の（子）プロセスを生成するかどうかを特定する
3. これらのプロセスを指定されたレジストリエントリに追加して、サインアウトを妨げないようにする

ステップ2：公開アプリケーションが追加の（子）プロセスを生成するかどうかを特定する

公開アプリケーションが正常なサインアウトを妨げていると特定されたら、次のステップは、このアプリケーションが実行時に追加のプロセスを生成するかどうかを判断することです。

公開アプリケーションが閉じられたときに、プロセスが正常なサインアウトをブロックしているかどうかを判断するには、`HKCU\Software\CitrixVolatile\Seamless\Sessions\[ID]\LogoffCheckerBlockingProcess` を参照してください。

以下の例では、キー `LogoffCheckerBlockingProcess` に次のエントリが含まれています。

```
PhoneExperienceHost.exe

SkypeApp.exe

SkypeBackgroundHost.exe
```

これらのプロセスが正常なサインアウトを妨げていました。

注:

確認したいセッションの正しいセッションIDで を置き換えてください。

ステップ3：これらのプロセスを指定されたレジストリエントリに追加して、サインアウトを妨げないようにする

これらのプロセスを以下のレジストリキーに追加することで、今後のセッションでサインアウトを妨げないようにすることができます。

```
Add the process file name to the following registry key:

Caution! Refer to the Disclaimer at the end of this article before using
the Registry Editor.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

Value Name:LogoffCheckSysModules

Type:REG_SZ

String:MyAppName.exe
```

`LogoffCheckSysModules` の詳細については、「公開アプリケーションからの正常なログオフによりセッションがアクティブ状態になる」を参照してください。

ステップバイステップのトラブルシューティングガイド

1. テスト対象のVDAでリモートレジストリサービスを開始します。

a. コントロールパネルで、**管理ツール > サービス** を選択します。
b. **リモートレジストリサービス** を右クリックし、**プロパティ** を選択します。
c. **スタートアップの種類** で、ドロップダウンメニューから **自動** を選択します。

公開アプリケーションレジストリ(/en-us/citrix-virtual-apps-desktops/2407/media/published-app-registry.png)

2. テスト対象のVDAでWindowsファイアウォールをオフにするか、ポート455を有効にする受信ファイアウォール規則を作成します。

a. コントロールパネルで、**Windows Defender ファイアウォール > 詳細設定**を選択します。
b. **受信の規則**を右クリックし、**新しい規則**を選択します。
c. **新しい受信の規則ウィザード**で、**ポート**を選択します。
d. **プロトコルおよびポート**ページで、**TCPおよび特定のローカルポート**を選択します。ローカルポートとして `445` を入力します。
e. **操作**ページで**接続を許可する**を選択します。
f. 新しい受信規則を適用するファイアウォールプロファイルを選択します。
g. ファイアウォール規則に名前を付け、**完了**を選択して**新しい受信の規則ウィザード**を終了します。

公開アプリケーションファイアウォールポート(/en-us/citrix-virtual-apps-desktops/2407/media/published-app-firewall-port.png)

3. 同じドメイン内の別のVM（DC、DDC、または別のVDAでも可）から、`Regedit` を実行し、リモートレジストリに接続します。

公開アプリケーションレジストリエディター(/en-us/citrix-virtual-apps-desktops/2407/media/published-app-registry-editor.png)

4. テスト対象のVDAのIPアドレスを入力し、**OK**をクリックします。`regedit` ツリーには、テスト対象のVDAのブランチが表示されるはずです。

公開アプリケーションregedit(/en-us/citrix-virtual-apps-desktops/2407/media/published-app-regedit.png)

5. **コマンドプロンプト**公開アプリケーションを開きます。

公開アプリの管理(/en-us/citrix-virtual-apps-desktops/2407/media/published-app-manage.png)

コマンドプロンプトアプリがCitrix Workspaceに表示されます。

公開アプリのコマンドプロンプト(/en-us/citrix-virtual-apps-desktops/2407/media/published-app-cmd-prompt.png)

6. クライアントで**接続センター**を開きます。これは、開いているシームレスアプリを閉じた後、セッションがサインアウトされたときに監視するために使用されます。以下の画像で、コマンドプロンプトプロセス`c:\Windows\system32\cmd.exe`がリモートVDIでアクティブになっていることがわかります。

   公開アプリの接続(/en-us/citrix-virtual-apps-desktops/2407/media/published-app-citrix-workspace-connection-center.png)

7. **regedit** が実行されている VDA から、次のリモート IP の場所に移動します。
   `HKEY_USERS\S-1-X-XX-XXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXX\SOFTWARE\CitrixVolatile\Seamless\Sessions\X\`

   > **注:**
   >
   > 新しいセッションを開くたびにこのパスは変更されます。

8. ここに読み取るべき2つのキーがあります（ここでは変更しないでください）：**LogoffCheckBlockingProcess**と**LogoffCheckerBlockingVisibleProcess**。これらのキーは、サインアウトをブロックしているプログラムを表示します。最初のキーは、開いていてまだ閉じられていないため、`C:\Windows\System32\cmd.exe`を表示する必要があります。

   > **注:**
   >
   > **LogoffCheckBlockingProcess** と **LogoffCheckerBlockingVisibleProcess** は手動で編集しないでください。これらのレジストリ値を手動で編集すると、セッションが不安定になる可能性があります。

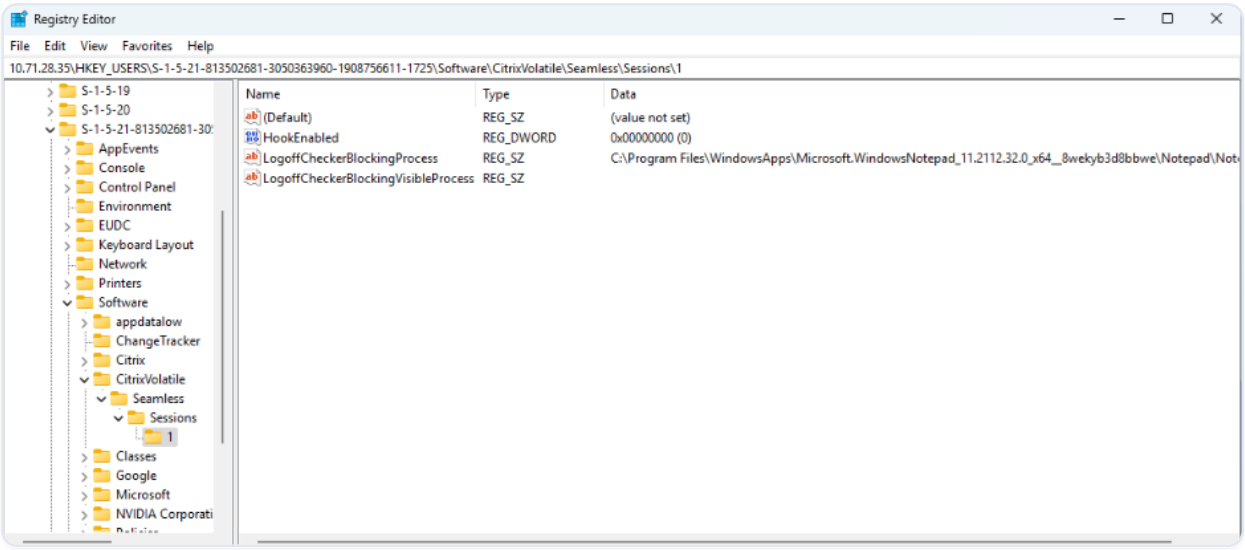
   公開アプリ2(/en-us/citrix-virtual-apps-desktops/2407/media/published-app-regedit-2.png)

9. 右上隅の **X** をクリックして **Seamless CMD** を終了します。
10. 接続センターでセッションが閉じるかどうかを確認します。閉じるまでに最大30秒かかる場合があります。セッションが閉じた場合、正常なサインアウトを妨げたアプリケーションやプロセスはありませんでした。

    正常なサインアウト(/en-us/citrix-virtual-apps-desktops/2407/media/published-app-bwd.png)

11. セッションが閉じなかった場合は、F5 キーで **regedit** の出力を更新します。
12. **LogoffCheckBlockingProcess** と **LogoffCheckerBlockingVisibleProcess** の内容を再度確認します。CMD は表示されなくなっているはずですが、別のプロセスが一覧表示されているはずです。現在セッションのサインアウトをブロックしているプロセスがここに表示されているはずです。

    この場合、コマンドプロンプトが閉じられる前に、公開されたコマンドプロンプトから **Notepad.exe** が開かれており、このリモートのメモ帳プロセスが正常なサインアウトを妨げています。



13. この実行可能ファイルへのパスと、それが表示されたキーをメモし、リモートツリーの下にある以下のレジストリキーに入力します。

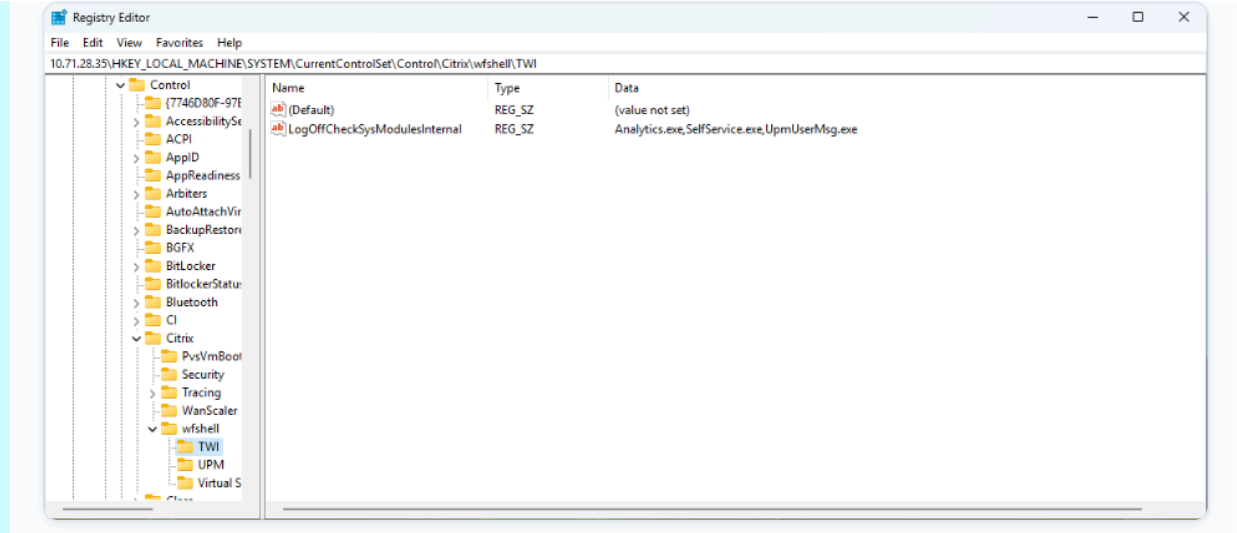
    - **LogoffCheckBlockingProcess** に表示される場合:

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckSysModulesInterna`

    - **LogoffCheckerBlockingVisibleProcess** に表示される場合:

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckVisibleSysModules`

> **注：**
>
> キーにすでに1つ以上のエントリがある場合は、末尾にコンマを追加し、その後に新しいエントリを配置します。



14. クライアントの接続センターからセッションをサインアウトし、リモートアプリケーションを再度開きます。
15. リモートアプリケーションを閉じてから30秒以内にセッションが自動的にサインアウトされるまで、手順9～16を繰り返します。

> **注：**
>
> トラブルシューティング後、必要に応じて、リモートレジストリへのアクセスを許可するための一時的なファイアウォールの変更を元に戻します。

公開されたアプリケーションを開くときに、Windowsの免責事項メッセージをフルサイズで表示するようにLogonUIを変更する方法

認証パススルーが発生しないシナリオでは、**LogonUI** ウィンドウのスケーリングが改善されました。**LogonUI** ウィンドウは、使用されているモニターの解像度とDPI設定に基づいてスケーリングされ、**LogonUI** ウィンドウ全体がクリッピングなしで表示されるようにします。

ウィンドウのサイズは、レジストリで手動でピクセル単位で設定することもできます。

1. **ファイル名を指定して実行**コマンドで `regedit` を使用して、**レジストリエディター**を開きます。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\` にアクセスします。
3. 2つの新しいDWORDキー、**LogonUIWidth**と**LogonUIHeight**を作成します。
4. キーの値を、**LogonUI**ウィンドウに必要な幅と高さ（ピクセル単位）に設定します。

LogonUIウィンドウのサイズを手動で設定すると、自動スケーリングは無効になります。

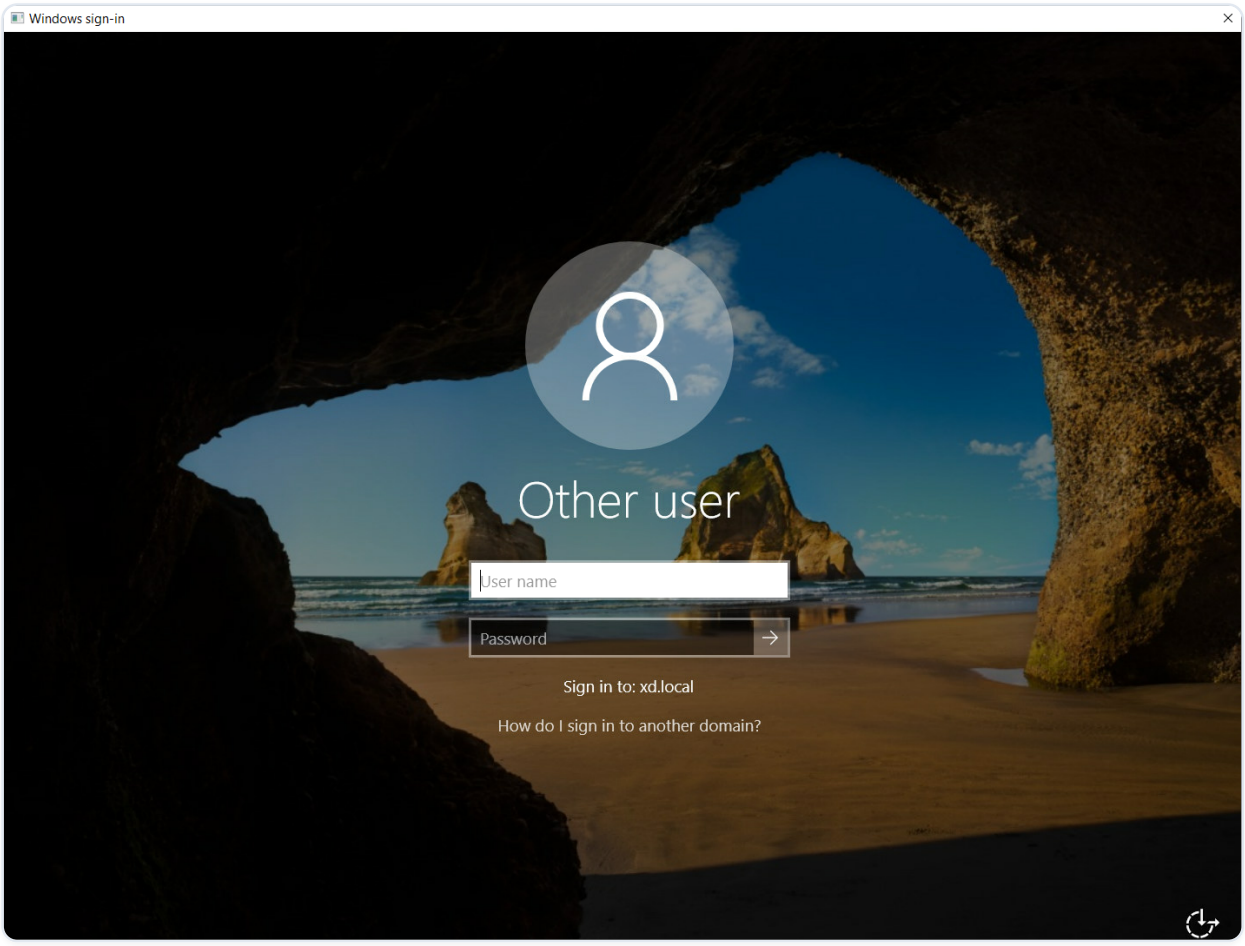
> **注：**
>
> これらのレジストリパスは2407以降変更されました。古いレジストリ値は無視され、非推奨です。

デフォルトでは、**LogonUI**ウィンドウには閉じるボタン付きのタイトルバーが含まれており、必要に応じてエンドユーザーがセッションから切断できるようになっています。

タイルバーを無効にする

以下のレジストリキーを使用して、**LogonUI**ウィンドウのタイトルバーを無効にできます。

1. **ファイル名を指定して実行**コマンドで`regedit`を使用して、レジストリエディターを開きます。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`にアクセスします。
3. 新しいDWORDキー**LogonUICaption**を作成し、キーの値を`0`に設定します。



アプリケーションフォルダーの管理

デフォルトでは、デリバリーグループに追加する新しいアプリケーションは、**Applications**という名前のフォルダーに配置されます。デリバリーグループの作成時、アプリケーションの追加時、または後で、別のフォルダーを指定できます。

知っておくと良いこと:

- Applicationsフォルダーの名前を変更したり削除したりすることはできませんが、その中に含まれるすべてのアプリケーションを、作成した他のフォルダーに移動することはできます。
- フォルダー名には1～64文字を含めることができます。スペースも使用できます。
- フォルダーは最大5レベルまでネストできます。
- フォルダーにアプリケーションを含める必要はありません。空のフォルダーも許可されます。
- Web Studioでは、フォルダーはアルファベット順に表示されますが、フォルダーを移動したり、作成時に別の場所を指定したりした場合は除きます。
- 各フォルダーの親フォルダーが異なる限り、同じ名前のフォルダーを複数持つことができます。同様に、各アプリケーションが異なるフォルダーにある限り、同じ名前のアプリケーションを複数持つことができます。

- フォルダー内のアプリケーションを表示するには`View Applications`権限が必要です。また、アプリケーションを含むフォルダーを削除、名前変更、または削除するには、そのフォルダー内のすべてのアプリケーションに対して`Edit Application Properties`権限が必要です。
- 以下のほとんどの手順では、Web Studioのアクションバーを使用してアクションを要求します。または、右クリックメニューを使用するか、項目をドラッグすることもできます。たとえば、意図しない場所にフォルダーを作成または移動した場合、ドラッグアンドドロップで正しい場所に移動できます。

アプリケーションフォルダーを管理するには、左側のペインで**Applications**を選択します。以下のリストを参考にしてください。

- **すべてのフォルダーを表示するには（ネストされたフォルダーを除く）:** フォルダーリストの上にある**すべて表示**をクリックします。
- **最上位レベルにフォルダーを作成するには（ネストしない）: Applications**フォルダーを選択します。新しいフォルダーを**Applications**以外の既存のフォルダーの下に配置するには、そのフォルダーを選択します。次に、アクションバーで**フォルダーの作成**を選択します。名前を入力します。
- **フォルダーを移動するには:** フォルダーを選択し、アクションバーで **フォルダーの移動** を選択します。ネストされたフォルダーが含まれていない限り、一度に1つのフォルダーしか移動できません。(フォルダーを移動する最も簡単な方法は、ドラッグすることです。)
- **フォルダーの名前を変更するには:** フォルダーを選択し、アクションバーで **フォルダー名の変更** を選択します。名前を入力します。
- **フォルダーを削除するには:** フォルダーを選択し、アクションバーで **フォルダーの削除** を選択します。アプリケーションや他のフォルダーを含むフォルダーを削除すると、それらのオブジェクトも削除されます。アプリケーションを削除すると、デリバリーグループからのアプリケーション割り当てが削除されます。マシンからは削除されません。
- **アプリケーションをフォルダーに移動するには:** 1つまたは複数のアプリケーションを選択します。次に、アクションバーで **アプリケーションの移動** を選択します。フォルダーを選択します。

デリバリーグループまたはアプリケーショングループを作成する際に、**アプリケーション** ページで追加するアプリケーションをフォルダーに配置することもできます。デフォルトでは、追加されたアプリケーションは **アプリケーション** フォルダーに入ります。**変更** をクリックしてフォルダーを選択または作成します。

公開デスクトップでのアプリケーションのローカル起動を制御する

ユーザーが公開デスクトップ内から公開アプリケーションを起動するときに、そのデスクトップセッションでアプリケーションを起動するか、公開アプリケーションとして起動するかを制御できます。Citrix Workspaceアプリは、VDA上のWindowsレジストリでアプリケーションのインストールパスを検索し、存在する場合はアプリケーションのローカルインスタンスを起動します。それ以外の場合は、ホストされたアプリケーションのインスタンスが起動されます。VDAにインストールされていないアプリケーションを起動すると、ホストされたアプリケーションが起動されます。詳細については、「vPrefer起動」を参照してください。

PowerShell（Citrix Cloud展開環境ではRemote PowerShell SDK、オンプレミス展開環境ではPowerShell SDKを使用）で、このアクションを変更できます。

`New-Broker` Applicationまたは`Set-BrokerApplication` コマンドレットで、`LocalLaunchDisabled` オプションを使用します。例：

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

デフォルトでは、このオプションの値はfalse (`-LocalLaunchDisabled $false`) です。公開デスクトップ内から公開アプリケーションを起動すると、アプリケーションはそのデスクトップセッションで起動されます。

オプションの値をtrue (`-LocalLaunchDisabled $true`) に設定すると、公開アプリケーションが起動されます。これにより、公開デスクトップから（Windows用Citrix Workspaceアプリを使用して）公開アプリケーションへの個別の追加セッションが作成されます。

要件と制限：

- アプリケーションの `ApplicationType` の値は `HostedOnDesktop` である必要があります。
- このオプションは、適切なPowerShell SDKを介してのみ利用可能です。現在、Web Studioのグラフィカルインターフェイスでは利用できません。
- このオプションには、最低限、StoreFront 3.14、Citrix Receiver for Windows 4.11、およびDelivery Controller 7.17が必要です。

アプリパッケージ

> **注：**

- Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb Studioのみを扱います。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。
- アプリパッケージの展開と配信にWeb StudioとCitrix Studioを相互に利用することはお勧めしません。それぞれ異なるメカニズムを使用しているため、App-Vサーバーの情報が一方では正しく表示されるが、もう一方では表示されないといった不一致が生じる可能性があります。

Microsoftは、アプリケーションをユーザーに配信するための3つのパッケージングテクノロジーを提供しています: App-V、MSIX、およびMSIX app attach。この記事では、**Web Studio > アプリパッケージ**を使用してこれらのパッケージ化されたアプリケーションを展開および配信する方法について説明します。

- App-Vアプリケーションの展開と配信
- MSIXおよびMSIX app attachアプリケーションの展開と配信

App-Vアプリケーションの展開と配信

このセクションでは、次の情報について説明します。

- 概要。App-Vパッケージを配信および管理するための管理方法について説明します。
- 手順。これらのパッケージを展開および配信するための手順を提供します。

概要

このセクションでは、App-Vパッケージを配信および管理するための管理方法について説明します。App-Vパッケージ化されたアプリケーションを配信する際に操作するコンポーネントと概念の詳細については、Microsoftのドキュメントを参照してください: `<https://docs.microsoft.com/ja-jp/windows/application-management/app-v/appv-for-windows>`。

App-Vパッケージを配信および管理するには、以下の方法を使用できます。

- **デュアル管理**。アプリケーションパッケージはApp-Vサーバーで構成および管理されます。Citrix Virtual Apps and DesktopsとApp-Vサーバーが連携してパッケージを配信および管理します。

この方法では、Citrix Virtual Apps and DesktopsがApp-Vサーバーの状態のスナップショットビューを定期的に更新する必要があります。これには、ハードウェア、インフラストラクチャ、および管理のオーバーヘッドが発生します。Citrix Virtual Apps and DesktopsとApp-Vサーバーは、特にユーザー権限に関して、同期を維持する必要があります。

デュアル管理は、App-Vと環境が密接に連携している展開で最適に機能します。

- **App-V管理サーバー**。App-Vパッケージと動的構成ファイルのライフサイクルを公開および管理します。
- VDAマシンにインストールされている**Citrix Personalizationコンポーネント**。アプリケーションの起動に必要な適切なApp-V公開サーバーの登録を管理します。

この方法により、App-V公開サーバーが適切なタイミングでユーザーと同期されるようになります。公開サーバーは、ログオン時の更新や接続グループなど、パッケージライフサイクルの他の側面を維持します。

- **シングル管理者**。アプリケーションパッケージはネットワーク共有に保存されます。Citrix Virtual Apps and Desktopsは、パッケージを独立して配信および管理します。

  この方法では、展開でApp-Vサーバーとデータベースインフラストラクチャが不要になるため、オーバーヘッドが削減されます。

  この方法では、App-Vパッケージをネットワーク共有に保存し、その場所からメタデータを環境にアップロードします。VDAマシンにインストールされているCitrix Personalizationコンポーネントは、次のようにアプリケーションを管理および配信します。

  - アプリケーションが起動されたときに、展開構成ファイルとユーザー構成ファイルを処理します。
  - ホストマシン上のパッケージのライフサイクルのすべての側面を管理します。

両方の管理方法を同時に使用できます。つまり、デリバリーグループにアプリケーションを追加するときに、アプリケーションはApp-Vサーバーまたはネットワーク共有に存在するApp-Vパッケージから取得できます。

> **注:**
>
> 両方の管理方法を同時に使用していて、App-Vパッケージが両方の場所に動的構成ファイルを持っている場合、App-Vサーバー上のファイル（デュアル管理者）が使用されます。

手順

App-Vアプリケーションの配信をサポートするには、VDAマシンにCitrix Personalizationコンポーネントをインストールする必要があります。詳細については、「VDAマシンにCitrix Personalizationコンポーネントをインストールする」を参照してください。

App-Vパッケージ化されたアプリケーションをユーザーに配信するには、次の手順に従います。

1. アプリケーションパッケージをネットワーク共有に保存する。
2. アプリケーションパッケージを環境にアップロードする。
3. デリバリーグループにアプリケーションを追加する。
4. 相互依存するApp-Vパッケージの自動配信を有効にするには、分離グループを作成する。

Citrix Virtual Apps and Desktopsでシングル管理者方式のApp-V動的構成ファイルを認識して適用させるには、このCitrixブログを参照してください。

MSIX および MSIX app attach アプリケーションの展開と配信

このセクションでは、以下の情報について説明します。

- 概要。MSIX および MSIX app attach パッケージがどのように配信および管理されるかについて説明します。
- 手順。これらのパッケージを展開および配信するための手順を提供します。

概要

Citrix Virtual Apps and Desktops は、VDA マシンにインストールされている Citrix Personalization コンポーネントを介して、MSIX および MSIX app attach アプリケーションをユーザーに配信します。このコンポーネントは、ホストマシン上のパッケージのライフサイクルのすべての側面を管理します。

MSIX および MSIX app attach の詳細については、Microsoft ドキュメントの `<https://docs.microsoft.com/ja-jp/windows/msix/>` と `<https://docs.microsoft.com/ja-jp/azure/virtual-desktop/what-is-app-attach>` をそれぞれ参照してください。

手順

MSIXおよびMSIX app attachパッケージの配信をサポートするには、VDAマシンにCitrix Personalizationコンポーネントをインストールする必要があります。詳細については、「VDAマシンへのCitrix Personalizationコンポーネントのインストール」を参照してください。

MSIXおよびMSIX app attachパッケージ化されたアプリケーションをユーザーに配信するには、次の手順に従います。

1. アプリケーションパッケージをネットワーク共有に保存する。
2. アプリケーションパッケージを環境にアップロードする。
3. デリバリーグループにアプリケーションを追加する。

VDAマシンにCitrix Personalizationコンポーネントをインストールする

Citrix Personalizationコンポーネントは、App-V、MSIX、およびMSIX app attach形式のアプリケーションパッケージの公開プロセスを管理します。このコンポーネントは、VDAをインストールする際にデフォルトではインストールされません。コンポーネントはVDAのインストール中またはインストール後にインストールできます。

VDAのインストール中にコンポーネントをインストールするには、次のいずれかの方法を使用します。

- インストールウィザードで、**［追加コンポーネント］**ページに移動し、**［Citrix Personalization for App-V - VDA］**チェックボックスをオンにします。
- コマンドラインインターフェイスでは、**/includeadditional "Citrix Personalization for App-V – VDA"** オプションを使用します。

VDAのインストール後にコンポーネントをインストールするには、次の手順に従います。

1. VDAマシンで、**コントロールパネル > プログラム > プログラムと機能**に移動し、**Citrix Virtual Delivery Agent**を右クリックして、**変更**を選択します。
2. 表示されるウィザードで、**［追加コンポーネント］**ページに進み、**［Citrix Personalization for App-V - VDA］**チェックボックスを有効にします。

> **注:**
>
> Microsoft App-V Desktop Client は、ユーザーデバイス上でApp-Vパッケージから仮想アプリケーションを実行するコンポーネントです。Windows 10 (1607以降) および Windows Server 2019 には、このApp-Vクライアントソフトウェアがすでに含まれています。VDAマシンで有効にするだけで済みます。詳細については、このMicrosoftドキュメント記事を参照してください: `<https://docs.microsoft.com/ja-jp/windows/application-management/app-v/appv-enable-the-app-v-desktop-client>`。

アプリケーションパッケージをネットワーク共有に保存する

インフラストラクチャをセットアップした後、アプリケーションパッケージを生成し、UNCまたはSMBネットワーク共有、あるいはAzureファイル共有などのネットワークロケーションに保存します。

詳細な手順は次のとおりです。

1. アプリケーションパッケージを生成します。詳細については、Microsoftのドキュメントを参照してください。
2. アプリケーションパッケージをネットワークロケーションに保存します。
   - **App-V Single Admin**の場合: パッケージと対応する動的構成ファイル (App-V) をUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
   - **App-V Dual Admin**の場合: UNCパスからApp-V管理サーバーにパッケージを公開します。(HTTP URLからの公開はサポートされていません。)
   - **MSIXまたはMSIX app attach**の場合: パッケージをUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
3. VDAがパッケージストレージパスに対する読み取り権限を持っていることを確認してください。
   - ADドメイン内のUNCまたはSMBネットワーク共有にパッケージを保存する場合は、VDAマシンにストレージパスへの読み取り権限を付与します。これを行うには、マシンのADアカウントに共有への読み取り権限を明示的に付与するか、その権限を持つADグループにアカウントを含めます。
   - Azureファイル共有にパッケージを保存する場合は、まずAzureのストレージパスに対するユーザーアカウントの読み取り権限を付与します。次に、VDAマシンで実行されている`ctxAppVService`がそのユーザーアカウントを使用してパッケージストレージパスにアクセスするように構成します。詳細な手順については、次のセクションを参照してください。

ユーザーログオンアカウントの変更

VDAはパッケージストレージパスにアクセスするために`ctxAppVService`を呼び出します。デフォルトでは、`ctxAppVService`はマシンの**ローカルシステムアカウント**を使用してパッケージストレージパスにアクセスします。このタイプのマシン認証はADドメインでは機能しますが、ユーザーアカウントベースの認証を必要とするADとAzure ADの統合シナリオでは機能しません。

Azureファイル共有にパッケージを保存する場合は、`ctxAppVService`のログオンアカウントを、パッケージストレージパスに対する読み取り権限を持つユーザーアカウントに変更します。詳細な手順は次のとおりです。

1. **サービス**を開始し、**ctxAppVService**を右クリックし、**プロパティ**を選択します。
2. **［ログオン］タブで、［このアカウント］**を選択し、パッケージストレージパスへの読み取り権限を持つユーザーアカウントを入力し、ユーザーのパスワードを2回入力します。
3. **OK**をクリックします。

アプリケーションパッケージを環境にアップロードする

必要に応じてアプリケーションパッケージをネットワークの場所に保存した後、配信のために環境にアップロードします。必要に応じて、以下のいずれかの方法を使用します。

- 一括アップロード
- 1つずつアップロード

準備

Citrix Virtual Apps and Desktops は、パッケージ検出のためのネットワークロケーションへの接続をセットアップするために VDA マシンを使用します。そのため、事前に (/ja-jp/citrix-virtual-apps-desktops/2407/install-configure/delivery-groups-create.html) を作成し、グループ内の少なくとも1つの VDA が以下の要件を満たしていることを確認してください。

- VDAバージョン:
  - App-Vパッケージを検出する場合: 2203以降
  - MSIXおよびMSIXアプリ添付パッケージを検出する場合: 2209以降
- Citrix Personalization for App-Vコンポーネント: インストール済み
- パッケージの場所に対する権限: 読み取り (詳細はステップ2: アプリケーションパッケージをネットワーク共有に保存するを参照してください。)
- 電源: オン
- 状態: 登録済み

アプリケーションパッケージを一括アップロードする

ネットワークの場所にあるパッケージを環境にアップロードします。アップロードする前に、次の項目が準備されていることを確認してください。

- (#preparations) の要件を満たすデリバリーグループ

- ネットワークの場所のパス

パッケージを一括でアップロードするには、次の手順に従います。

1. 左側のペインで、 を選択します。
2. タブで、 ボタンをクリックします。 ページが表示されます。
3. フィールドに、パッケージソースのわかりやすい名前を入力します。
4. フィールドで、 をクリックします。次に、準備に記載されている要件を満たすデリバリーグループを選択し、 をクリックします。
5. フィールドで、パッケージの保存場所に応じて または を選択し、対応する設定を完了します。

   - を選択した場合は、次の情報を入力します。
     - 管理サーバーのURL。例: `http://appv-server.example.com`
     - 管理サーバー管理者のログイン資格情報。
     - 公開サーバーのURLとポート番号。例: `http://appv-server.example.com:3330`
   - を選択した場合は、次の情報を指定します。
     - ネットワーク共有のUNCパスを入力します。例: `\\Package-Server\apps\`
     - アップロードするパッケージの種類を選択します。オプションには、App-V、MSIX、MSIX app attach があります。
     - パッケージのサブフォルダーを検索するかどうかを指定します。
6. **ソースの追加**をクリックします。

   ソースの追加ページが閉じ、新しく追加されたソースがソースリストに表示されます。Citrix Virtual Apps and Desktops は、デリバリーグループ内の VDA を使用してパッケージを環境にアップロードします。アップロードが完了すると、ステータスフィールドに*インポート成功*と表示されます。対応するパッケージは**パッケージ**タブに表示されます。

> **注：**
>
> ソースの場所でパッケージの更新を確認し、環境にインポートするには、ソースリストで場所を選択し、**パッケージの更新を確認**をクリックします。

アプリケーションパッケージを1つずつアップロードする

ネットワーク共有から環境にアプリケーションパッケージをアップロードします。アップロードする前に、次の項目が準備されていることを確認してください。

- (#preparations) で述べられている要件を満たすデリバリーグループ
- ネットワークの場所のパス。

パッケージを環境にアップロードするには、次の手順に従います。

1. 左側のペインで、**アプリパッケージ**を選択します。
2. **パッケージ**タブで、**パッケージの追加**ボタンをクリックします。**パッケージの追加**ページが表示されます。
3. **デリバリーグループ**フィールドで、**デリバリーグループの選択**をクリックします。次に、準備に記載されている要件を満たすデリバリーグループを選択し、**OK**をクリックします。
4. **パッケージのフルパス**フィールドに、必要に応じてパスを入力します。
   - 複数のパッケージを一度にアップロードするには、セミコロンで区切ってそれらのフルパスを入力します (`;`)。例: `\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - ネットワーク共有に存在するすべてのパッケージをアップロードするには、ストレージパスを入力します。例: \\package-Server\apps\
5. **パッケージの追加**をクリックします。

   アプリケーションパッケージが「**パッケージ**」タブに表示されます。

デリバリーグループにアプリケーションを追加する

アプリケーションパッケージが完全にアップロードされた後、必要に応じてそのアプリケーションを1つ以上のデリバリーグループに追加します。その結果、それらのデリバリーグループに関連付けられたユーザーはアプリケーションにアクセスできるようになります。

パッケージ内の1つ以上のアプリケーションを複数のデリバリーグループに追加するには、次の手順に従います。

1. 左ペインで、**アプリパッケージ**を選択します。
2. **パッケージ**タブで、必要に応じてパッケージを選択します。
3. アクションバーで、**デリバリーグループの追加**をクリックします。デリバリーグループの追加ページが表示されます。
4. 必要に応じてパッケージ内の1つ以上のアプリケーションを選択し、**次へ**をクリックします。

5. デリバリーグループのリストで、アプリケーションを割り当てるグループを選択し、**次へ**をクリックします。 **注:** MSIXまたはMSIXアプリ添付パッケージを選択した場合、機能レベルが2106以降のデリバリーグループのみがリストに表示されます。
6. **完了**をクリックします。

次の場合に、パッケージ化されたアプリケーションをデリバリーグループに追加することもできます。

- デリバリーグループを作成する場合。詳細については、「デリバリーグループの作成」を参照してください。
- 既存のデリバリーグループまたはアプリケーショングループを編集する場合。詳細については、「アプリケーションの追加」を参照してください。

（オプション）App-Vパッケージの分離グループを作成する

相互依存するApp-Vパッケージの自動配信を有効にするために、分離グループを作成できます。

> **注:**
>
> 分離グループは、App-Vシングル管理者方式でサポートされています。App-Vデュアル管理者方式を使用している場合は、Microsoft App-Vインフラストラクチャで*接続グループ*を作成することで、同じ目標を達成できます。詳しくは、次のMicrosoftドキュメント記事を参照してください：`<https://docs.microsoft.com/ja-jp/windows/application-management/app-v/appv-connection-group-file>`。

分離グループについて

分離グループとは、仮想環境を作成するために同じWindows Sandboxで実行する必要がある、相互依存するアプリケーションパッケージの集合です。Citrix App-V分離グループは、App-V接続グループに似ていますが、同一ではありません。分離グループには、次の2種類のパッケージが含まれます。

- **明示的**アプリケーションパッケージ。特定のライセンス要件を持つアプリケーション。これらのアプリケーションをデリバリーグループに追加することで、特定の範囲のユーザーに制限できます。
- **自動**アプリケーションパッケージ。デリバリーグループに追加されているかどうかに関係なく、常にすべてのユーザーが利用できるアプリケーション。

たとえば、アプリケーション`app-a`を実行するにはJRE 1.7が必要です。app-a（*明示的*としてマーク）とJRE 1.7（*自動*としてマーク）を含む分離グループを作成できます。次に、`app-a`のApp-Vパッケージを1つ以上のデリバリーグループに追加します。ユーザーがapp-aを起動すると、JRE 1.7が自動的に展開されます。

ユーザーが分離グループ内で*明示的*としてマークされたApp-Vアプリケーションを起動すると、Citrix Virtual Apps and Desktopsはデリバリーグループ内のアプリケーションに対するユーザーのアクセス許可を確認します。ユーザーがアプリケーションにアクセスする許可を持っている場合、同じ分離グループ内の*自動*アプリケーションパッケージはユーザーに利用可能になります。

*自動*パッケージをどのデリバリーグループにも追加する必要はありません。分離グループ内に別の*明示的*アプリケーションパッケージがある場合、そのパッケージは同じデリバリーグループ内にある場合にのみユーザーに利用可能になります。

分離グループについて詳しくは、このCitrixブログを参照してください。

APP-V分離グループを作成する

分離グループを作成し、相互依存するアプリケーションパッケージを追加します。詳細な手順は次のとおりです。

1. 「**分離グループ**」タブで、「**分離グループの追加**」をクリックします。
2. 分離グループの名前と説明を入力します。環境内のすべてのアプリケーションパッケージが「**利用可能なパッケージ**」リストに表示されます。
3. 「**利用可能なパッケージ**」リストから必要に応じてアプリケーションを選択し、右矢印をクリックします。選択したアプリケーションが「**分離グループ内のパッケージ**」リストに表示されます。
4. 「**展開**」フィールドで、アプリケーションに対して「**明示的**」または「**自動**」を選択します。
5. さらにパッケージを追加するには、手順2〜3を繰り返します。
6. リスト内のパッケージの順序を調整するには、上矢印または下矢印をクリックします。
7. 「**保存**」をクリックします。

> **注:**
>
> 隔離グループ構成により、VDA上にApp-V接続グループが作成されます。展開シナリオは複雑になる可能性があり、App-Vクライアントは一度に1つのアクティブな接続グループにのみ存在するパッケージをサポートします。同じパッケージを、同じデリバリーグループに追加された2つの異なる隔離グループに追加することは避けることをお勧めします。

パッケージ化されたアプリケーションをシングルセッションまたは共有デスクトップVDAに公開する

App-V、MSIX、およびMSIX app attachパッケージを、デリバリーグループを介してシングルセッションまたは共有デスクトップVDAセッションに直接配信できるようになりました。アプリケーションに設定されているアクセス許可に基づいて、サインイン時にデスクトップVDAでパッケージ化されたアプリケーションにアクセスできます。

利点

- サインイン時にVDAで利用可能であり、WorkspaceまたはStoreFrontを介してオンデマンドでステージングされないアプリケーション。
- パッケージ化されたアプリケーションへのアクセス時の起動時間の改善。
- VDAのベースイメージとは別に、パッケージ化されたアプリケーションの独立したメンテナンスを容易にします。

考慮事項

- このオプションは、適切なPowerShell SDKを介して、シングルセッションVDAでのみ利用可能です。現在、Web Studioワークフローでは利用できません。共有デスクトップへの公開は、PowerShell SDKを使用するか、Web Studioワークフローを介した既存の方法で行うことができます。既存の手順の詳細については、「デリバリーグループへのアプリケーションの追加」を参照してください。
- アプリケーションはデリバリーグループの一部である必要があります。

始める前に

- パッケージ化されたアプリケーションが署名されており、ファイル共有またはUNCの場所に存在することを確認してください。詳細については、「ネットワーク共有にアプリケーションパッケージを保存する」を参照してください。
- VDAマシンにCitrix Personalizationコンポーネントをインストールします。

手順

パッケージ化されたアプリケーションをデスクトップVDAに配信するには、次の手順に従います。

1. Web Studioにアプリケーションパッケージをインポートします。
2. パッケージ化されたBrokerApplicationを公開します。
3. Web Studioでのアプリケーションの可視性を制限します。

Web Studioにアプリケーションパッケージをインポートする

1. Webブラウザを開きます。`https://<address of the server hosting Web Studio>/Citrix/Studio`と入力します。
2. デリバリーグループを作成します。詳細については、「デリバリーグループの作成」を参照してください。
3. アプリケーションパッケージをWeb Studioにインポートします。詳細については、「アプリケーションパッケージの一括アップロード」を参照してください。

BrokerApplicationでパッケージ化されたアプリケーションを公開する

マルチセッション（共有）VDAまたはシングルセッションアプリケーションVDAに公開する場合、公開手順は変更されません。詳細については、「デリバリーグループへのアプリケーションの追加」を参照してください。 シングルセッションデスクトップVDAに公開する場合は、次の手順を実行します。

Delivery Controller™上で、以下のPowerShellコマンドを実行します:

1. パッケージ内に存在するコマンドを取得するには：

   ```
   Import-Module "D:\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
   ```

   > **注:**
   >
   > この機能をサポートする`App-V package discovery module`のバージョンは、上記のパスにあるCitrix Virtual Apps and Desktops ISO（2311以降のバージョン）で確認できます。

2. 関連するデリバリーグループIDとパッケージ化されたアプリケーションIDを取得するには:

   `Get-BrokerDesktopGroup | Format-Table Uid, Name` `Get-AppLibAppVApplication | Format-Table Uid, Name`

3. パッケージを公開し、適切なBrokerMachineConfigurationを作成するには:

   ```
   Publish-PackagedApplication -AppLibararyApplicationUid <AppLibararyApplication.Uid > -DesktopGroupUid <DesktopGroup.Uid>
   ```

4. 後でVDA上のBrokerエージェントに送信されるBroker構成を同期するには：

   ```
   Update-DesktopGroupMachineConfigurations -DesktopGroupUid <DesktopGroup.Uid>
   ```

> **注:**
>
> VDAからパッケージ化されたアプリケーションを公開または削除した後で、PowerShellコマンド`Update-DesktopGroupMachineConfigurations`を実行してください。

Web Studio でのアプリケーションの可視性を制限する

デフォルトでは、ユーザーはVDAを提供するデリバリーグループに割り当てられたすべてのパッケージ化されたアプリケーションをデスクトップセッションで利用できます。Web Studioで特定のユーザーまたはグループにアプリケーションの可視性を設定することで、デスクトップVDA上のパッケージ化されたアプリケーションの可視性を制御できます。パッケージ化されたアプリケーションの可視性を管理するには、アプリケーションプロパティの変更を参照してください。

ユニバーサル Windows プラットフォームアプリ

ユニバーサル Windows プラットフォーム (UWP) アプリについては、以下の Microsoft ドキュメントを参照してください。

- ユニバーサル Windows プラットフォーム (UWP) アプリとは
- Windows パッケージマネージャー

要件と制限

Citrix Virtual Apps and Desktops™ は、以下の Windows マシン上の VDA で UWP アプリを使用することをサポートしています。

- Windows 10 以降のバージョン
- Windows Server 2016 以降のバージョン

VDA はバージョン 7.11 以降である必要があります。

UWP アプリを使用する場合、以下の Citrix Virtual Apps and Desktops の機能はサポートされていないか、制限されています。

- ファイルタイプの関連付けはサポートされていません。
- ローカルアプリアクセスはサポートされていません。
- 動的プレビュー：セッションで実行中のアプリが重なっている場合、プレビューにはデフォルトのアイコンが表示されます。動的プレビューに使用される Win32 API は、UWP アプリではサポートされていません。

- アクションセンターのリモート処理：UWP アプリは、セッション内のメッセージを表示するためにアクションセンターを使用できます。これらのメッセージは現在、ユーザーに表示するためにエンドポイントにリダイレクトされません。

同じサーバーから UWP アプリと非 UWP アプリを起動することはサポートされていません。代わりに、UWP アプリと非 UWP アプリを別々のデリバリーグループまたはアプリケーショングループに配置してください。

マシンにインストールされているすべてのUWPアプリが列挙されるため、Citrix®はWindowsストアへのユーザーアクセスを無効にすることを推奨します。これにより、あるユーザーがインストールしたUWPアプリが別のユーザーによってアクセスされるのを防ぎます。

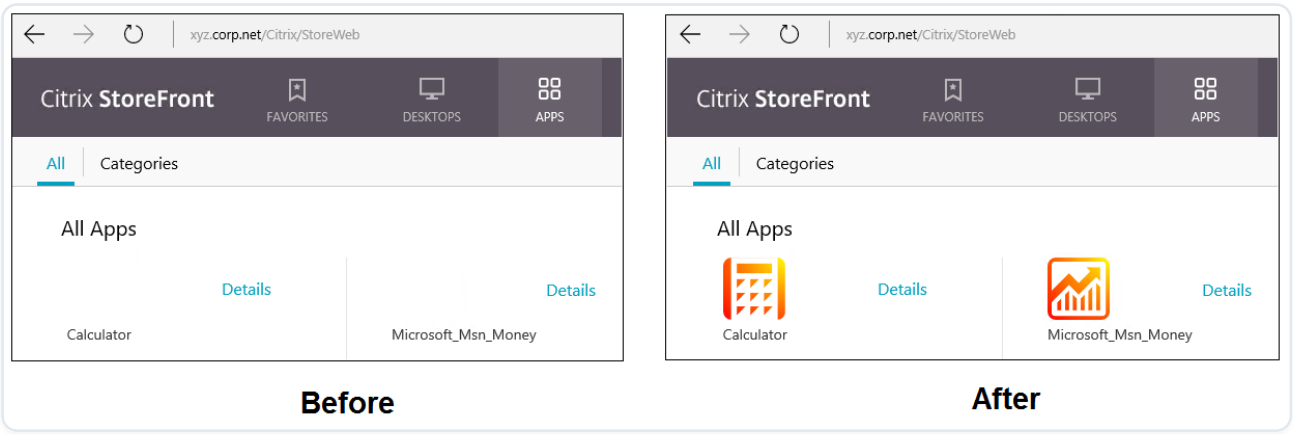
サイドローディング中、UWPアプリはマシンにインストールされ、他のユーザーが使用できるようになります。別のユーザーがアプリを起動すると、アプリがインストールされ、OSはそのAppXデータベースを更新して、そのユーザーによって「インストール済み」であることを示します。

固定ウィンドウまたはシームレスウィンドウで起動された公開UWPアプリから開始された正常なログオフは、VDAセッションが閉じないようにし、ユーザーを強制的にログオフさせる可能性があります。この場合、VDAセッションに残っているいくつかのプロセスが、セッションが適切に閉じないようにします。これを解決するには、VDAセッションが閉じないようにしているプロセスを特定し、CTX891671のガイダンスに従って、「LogoffCheckSysModules」レジストリキー値に追加します。

UWPアプリのアプリケーション表示名と説明が正しくない場合があります。アプリケーションをデリバリーグループに追加する際に、これらのプロパティを編集して修正してください。

その他の問題については、既知の問題を確認してください。

現在、いくつかのUWPアプリは透明度が有効な白いアイコンを持っており、StoreFrontの白い背景に対してアイコンが見えなくなることがあります。この問題を回避するには、背景を変更できます。たとえば、StoreFrontマシンでファイル `C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css` を編集します。ファイルの最後に `.storeapp-icon {background-image: radial-gradient( circle at top right, yellow, red ); }` を追加します。次の図は、この例の変更前と変更後を示しています。



Windows Server 2016以降のバージョンでは、UWPアプリの起動時にサーバーマネージャーも起動する場合があります。これを防ぐには、`HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon`レジストリキーを使用して、ログオン時のサーバーマネージャーの自動起動を無効にすることができます。詳細については、`<https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/>`を参照してください。

UWPアプリのインストールと公開

UWPアプリのサポートはデフォルトで有効になっています。

VDA（またはマスターイメージ）に1つ以上のUWPアプリをインストールするには、次のいずれかの方法を使用します。

- Windows Store for Businessからオフラインインストールを完了し、Deployment Image Servicing and Management (DISM) などのツールを使用して、アプリをデスクトップイメージに展開します。詳細については、Windows Package Managerを参照してください。
- アプリをサイドロードします。詳細については、Windowsクライアントデバイスでの基幹業務（LOB）アプリのサイドロードを参照してください。
- 各対象ユーザー向けに、Windows Store for Businessから直接UWPアプリをインストールします。

Citrix Virtual AppsまたはCitrix Virtual Desktops™で1つ以上のUWPアプリを追加（公開）するには：

1. UWPアプリがマシンにインストールされたら、UWPアプリをデリバリーグループまたはアプリケーショングループに追加します。これは、グループの作成時または後で行うことができます。「**アプリケーション**」ページで、「**追加**」メニューから「**スタートメニューから**」を選択します。
2. アプリケーションリストが表示されたら、公開するUWPアプリを選択します。
3. ウィザードを続行するか、編集ダイアログを閉じます。

VDAでユニバーサルアプリの使用を無効にするには、`HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle`にレジストリ設定**EnableUWASeamlessSupport**を追加し、**0**に設定します。

UWPアプリのアンインストール

`Remove-AppXPackage`のようなコマンドでUWPアプリをアンインストールしても、その項目は管理者に対してのみアンインストールされます。アプリを起動して使用した可能性のあるユーザーのマシンからアプリを削除するには、各マシンで削除コマンドを実行します。1つのコマンドですべてのユーザーのマシンからAppXパッケージをアンインストールすることはできません。

オートスケール™

> **注:**
>
> Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この機能はWeb Studioでのみ利用可能です。

> Autoscaleは、マシンをプロアクティブに電力管理するための、一貫性のある高性能なソリューションを提供する機能です。コストとユーザーエクスペリエンスのバランスを取ることを目的としています。

Autoscaleは、デリバリーグループ内の登録されているすべてのシングルセッションおよびマルチセッションOSマシンのプロアクティブな電源管理を可能にします。

Autoscaleの機能は次のとおりです。

- スケジュールベースおよび負荷ベースの設定
- 動的セッションタイムアウト
- Autoscaleタグ付きマシン（クラウドバースト）
- ユーザーログオフ通知

サポートされているVDAホスティングプラットフォーム

Autoscaleは、Citrix Virtual Apps and Desktopsがサポートするすべてのプラットフォームをサポートしています。これには、XenServer、Amazon Web Services、Google Cloud Platform、Microsoft Azure Resource Manager、VMware vSphereなど、さまざまなインフラストラクチャプ

ラットフォームが含まれます。サポートされているプラットフォームの完全なリストについては、Citrix Virtual Apps and Desktopsのシステム要件を参照してください。

> **注:**
>
> 展開にパブリッククラウドホスト接続を追加する場合、ハイブリッド権限ライセンスが必要です。ハイブリッド権限ライセンスの詳細については、ハイブリッド権限による移行とトレードアップ（TTU）を参照してください。ライセンスの追加については、サイトの作成を参照してください。

サポートされているワークロード

Autoscaleは、マルチセッションOSとシングルセッションOSの両方のデリバリーグループをサポートしています。注意すべきユーザーインターフェイスは3つあります。

- マルチセッションOSデリバリーグループ（旧RDSデリバリーグループ）用のAutoscaleユーザーインターフェイス
- シングルセッションOSランダム（プール型）デリバリーグループ（旧プール型VDIデリバリーグループ）用のAutoscaleユーザーインターフェイス
- シングルセッションOS静的デリバリーグループ（旧静的VDIデリバリーグループ）用のAutoscaleユーザーインターフェイス

さまざまなデリバリーグループのユーザーインターフェイスの詳細については、「Autoscale user interfaces」を参照してください。

利点

Autoscale機能には、次の利点があります。

- デリバリーグループ内のマシンを電源管理するための、単一で一貫したメカニズムを提供します。
- 負荷ベースまたはスケジュールベースの電源管理、あるいはその両方の組み合わせでマシンに電力を供給することにより、可用性を確保し、コストを管理します。
- コスト削減やキャパシティ使用率などのメトリックを監視し、通知を有効にするには、Directorを使用します。

2分間のビデオを見る

次のビデオでは、Autoscaleの簡単なツアーを提供します。

<iframe src="https://www.youtube.com/embed/5yxERrFZQ68" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

Autoscale™ の概要

Autoscale はデリバリーグループレベルで動作します。設定したスケジュールに基づいて、デリバリーグループ内のマシンの電源をプロアクティブに管理します。

Autoscale は、すべての種類のデリバリーグループに適用されます。

- シングルセッション静的 OS
- シングルセッションランダム OS
- マルチセッションランダム OS

この記事では、Autoscale 関連の基本的な概念について説明し、デリバリーグループで Autoscale を有効にして構成する方法に関するガイダンスを提供します。

基本的な概念

開始する前に、Autoscale の次の基本的な概念について学習してください。

- スケジュール
- 容量バッファ
- 負荷インデックス

スケジュール

Autoscaleは、設定したスケジュールに基づいて、デリバリーグループ内のマシンの電源をオン/オフします。

スケジュールには、各タイムスロットのアクティブなマシンの数と、ピーク時およびオフピーク時が定義されています。

スケジュールの設定は、デリバリーグループの種類によって異なります。詳細については、以下を参照してください。

- マルチセッションOSデリバリーグループ
- シングルセッションOSランダムデリバリーグループ
- シングルセッションOS静的デリバリーグループ

容量バッファ

容量バッファは、動的な負荷増加に対応するために、現在の需要に予備容量を追加するために使用されます。注意すべき2つのシナリオがあります。

- マルチセッションOSデリバリーグループの場合、容量バッファは、ロードインデックスの観点から、デリバリーグループの総容量のパーセンテージとして定義されます。
- シングルセッションOSデリバリーグループの場合、容量バッファは、デリバリーグループ内のマシンの総数のパーセンテージとして定義されます。

ロードインデックス

> **重要：**
>
> 負荷インデックスは、マルチセッションデリバリーグループにのみ適用されます。
>
> ロードインデックスメトリックは、マシンがユーザーログオン要求を受信する可能性を決定します。これは、同時ログオン、セッション、CPU、ディスク、メモリの使用量に対して構成された**Citrix Load Management policy**設定を使用して計算されます。

ロードインデックスは0から10,000の範囲です。デフォルトでは、マシンが250セッションをホストしている場合、完全にロードされていると見なされます。

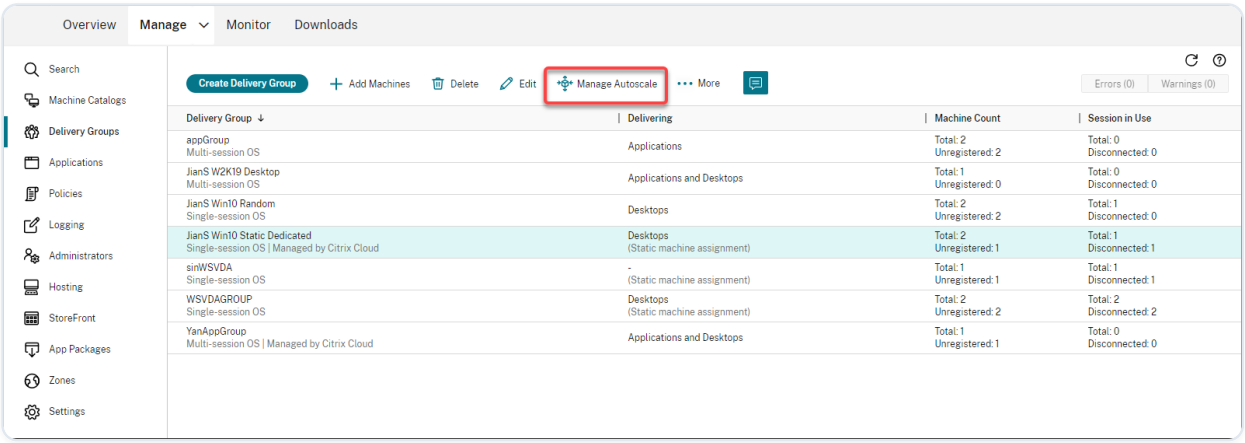
- 数字の「0」はアンロードされたマシンを示します。ロードインデックス値が0のマシンは、ベースライン負荷にあります。
- 「10,000」は、これ以上セッションを実行できない完全にロードされたマシンを示します。

デリバリーグループのAutoscaleを有効にする

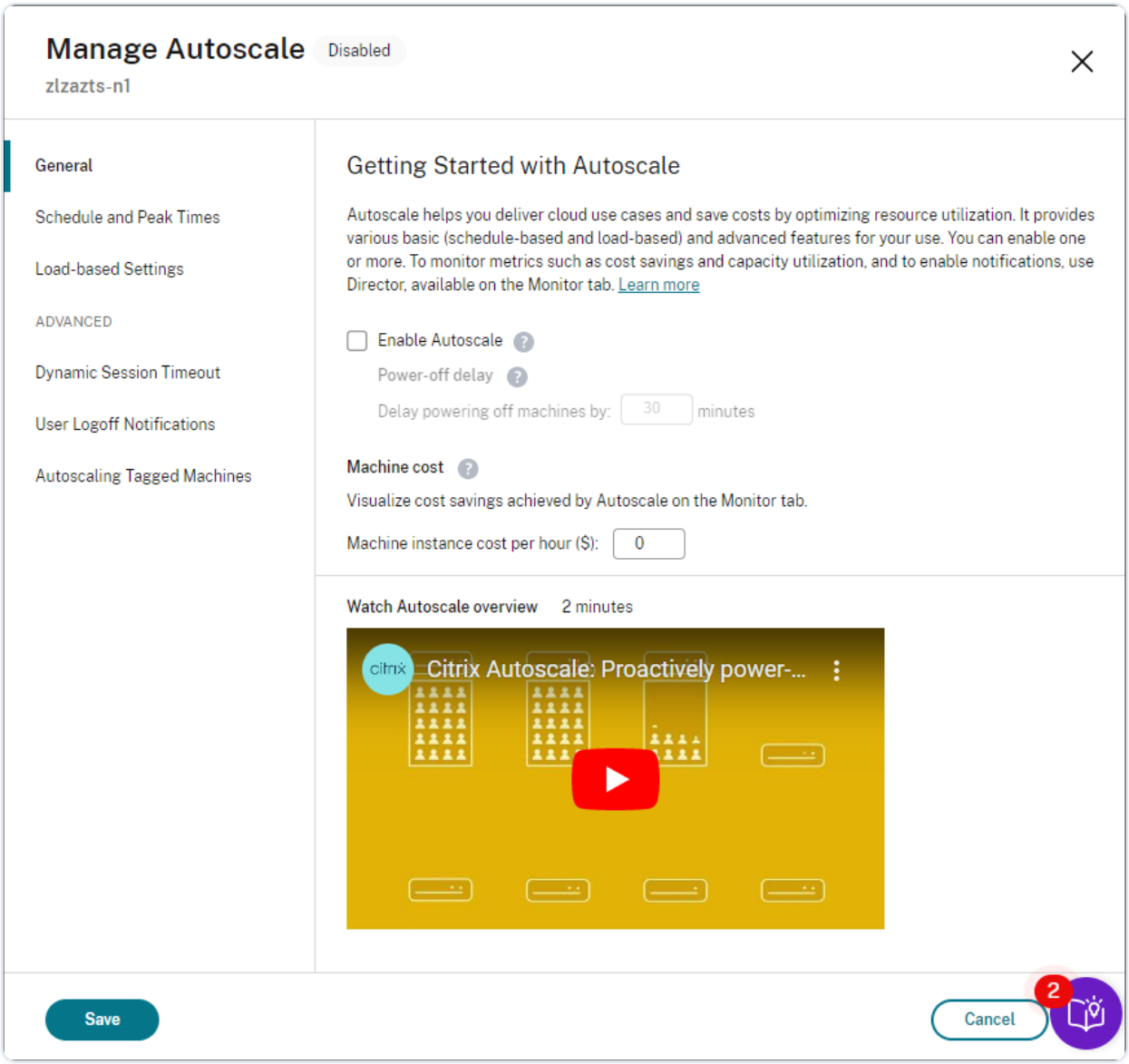
デリバリーグループを作成すると、Autoscaleはデフォルトで無効になります。Web Studioを使用してデリバリーグループのAutoscaleを有効にして構成するには、次の手順に従います。

PowerShellコマンドを使用して、デリバリーグループのAutoscaleを有効にして構成することもできます。詳細については、「Broker PowerShell SDK コマンド」を参照してください。

1. 左側のペインで を選択します。
2. 管理するデリバリーグループを選択し、**Autoscaleの管理**をクリックします。



3. ページで、 チェックボックスをオンにしてAutoscaleを有効にします。Autoscaleを有効にすると、ページ上のオプションが有効になります。



4. 組織のニーズに基づいてデフォルト設定を変更するには、次の設定を完了します。

   - スケジュールを設定する

- 非アクティブなマシンをより効率的に電源オフするには、動的セッションタイムアウト と ユーザーログオフ通知 を使用します。
- デリバリーグループ内のマシンの一部を電源管理するには、タグ付けされたマシンの Autoscale を使用します。

Autoscaleを無効にするには、 チェックボックスをオフにします。ページ上のオプションがグレー表示され、選択したデリバリーグループでAutoscaleが無効になっていることを示します。

重要:

- Autoscaleを無効にすると、Autoscaleによって管理されていたすべてのマシンは、無効にした時点の状態のままになります。
- Autoscale を無効にすると、ドレイン状態のマシンはドレイン状態から解除されます。ドレイン状態の詳細については、「ドレイン状態」を参照してください。

メトリックの監視

デリバリーグループで Autoscale を有効にすると、Director から Autoscale で管理されているマシンの次のメトリックを監視できます。

- マシンの使用状況
- 推定節約額
- マシンとセッションのアラート通知
- マシンのステータス
- 負荷評価の傾向

注:

デリバリーグループで Autoscale を最初に有効にした場合、そのデリバリーグループの監視データが表示されるまでに数分かかることがあります。 Autoscale が有効になり、その後デリバリーグループで無効になった場合でも、監視データは引き続き利用できます。Autoscale は 5 分間隔で監視データを収集します。

メトリックの詳細については、「Autoscale で管理されているマシンの監視」を参照してください。

知っておくとよいこと

Autoscale はデリバリーグループレベルで機能します。デリバリーグループごとに構成されます。選択したデリバリーグループ内のマシンのみを電源管理します。

容量とマシンの登録

Autoscale は、容量を決定する際に、サイトに登録されているマシンのみを含めます。登録されていない電源オンのマシンはセッション要求を受け入れることができません。そのため、デリバリーグループの全体的な容量には含まれません。

複数のマシンカタログ全体でのスケーリング

一部のサイトでは、複数のマシンカタログが単一のデリバリーグループに関連付けられている場合があります。Autoscaleは、スケジュールまたはセッションの需要要件を満たすために、各カタログからマシンをランダムに電源オンにします。

たとえば、あるデリバリーグループに 2 つのマシンカタログがあるとします。カタログ A には 3 台のマシンが起動しており、カタログ B には 1 台のマシンが起動しています。Autoscale が追加のマシンを起動する必要がある場合、カタログ A またはカタログ B のいずれかのマシンを起動する可能性があります。

マシンのプロビジョニングとセッションの需要

デリバリーグループに関連付けられているマシンカタログには、需要の増減に応じて起動および停止するのに十分なマシンが必要です。セッションの需要がデリバリーグループ内の登録済みマシンの総数を超えた場合、Autoscale はすべての登録済みマシンが起動していることを保証します。ただし、**Autoscale は追加のマシンをプロビジョニングしません**。

インスタンスサイズの考慮事項

パブリッククラウドでインスタンスのサイズを適切に設定すると、コストを最適化できます。ワークロードのパフォーマンスと容量要件に合致する限り、より小さなインスタンスをプロビジョニングすることをお勧めします。

小さいインスタンスは、大きいインスタンスよりも少ないユーザーセッションをホストします。そのため、最後のユーザーセッションがログオフされるまでの時間が短いため、Autoscale はマシンをより速くドレイン状態にします。結果として、Autoscale は小さいインスタンスをより早くシャットダウンし、コストを削減します。

ドレイン状態

Autoscale は、デリバリーグループ内の電源オン状態のマシンの数を、構成されたプールサイズと容量バッファにまでスケールダウンしようとします。

この目標を達成するために、Autoscale はセッション数が最も少ない余分なマシンを「ドレイン状態」にし、すべてのセッションがログオフされたときにそれらをシャットダウンします。この動作は、セッションの需要が減少し、スケジュールが起動しているマシンよりも少ないマシンを必要とする場合に発生します。

Autoscale は余分なマシンを「ドレイン状態」に 1 台ずつ移行します。

- 2 台以上のマシンが同じ数のアクティブセッションを持っている場合、Autoscale は指定されたシャットダウン遅延時間起動していたマシンをドレインします。

  これにより、最近起動されたマシンがドレイン状態になるのを避けることができます。なぜなら、それらのマシンはセッション数が最も少ない可能性が高いからです。
- 2 台以上のマシンが指定されたシャットダウン遅延時間起動していた場合、Autoscale はそれらのマシンをランダムに 1 台ずつドレインします。

ドレイン状態のマシンは新しいセッションの起動をホストしなくなり、既存のセッションがログオフされるのを待機しています。マシンは、すべてのセッションがログオフされた場合にのみシャットダウンの候補となります。ただし、セッション起動にすぐに利用できるマシンがない場合、Autoscaleは、マシンの電源をオンにするよりも、ドレイン状態のマシンにセッション起動を誘導することを優先します。

次のいずれかの条件が満たされた場合、マシンはドレイン状態から解除されます。

- マシンの電源がオフになる。
- マシンが属するデリバリーグループで Autoscale が無効になっている。
- Autoscale は、スケジュールまたは負荷需要の要件を満たすためにマシンを使用します。このケースは、スケジュール（スケジュールベースのスケーリング）または現在の需要（負荷ベースのスケーリング）が、現在電源がオンになっているマシンの数よりも多くのマシンを必要とする場合に発生します。

> **重要:**

> セッション起動に利用できるマシンがすぐにない場合、Autoscale はマシンの電源をオンにするよりも、ドレイン状態のマシンにセッション起動を誘導することを優先します。セッション起動をホストするドレイン状態のマシンは、ドレイン状態のままになります。

> どのマシンがドレイン状態にあるかを確認するには、`Get-BrokerMachine` PowerShellコマンドを使用します。例えば、`Get-BrokerMachine -DrainingUntilShutdown $true`。

> または、管理コンソールを使用できます。「ドレイン状態のマシンを表示」を参照してください。

ドレイン状態のマシンを表示する

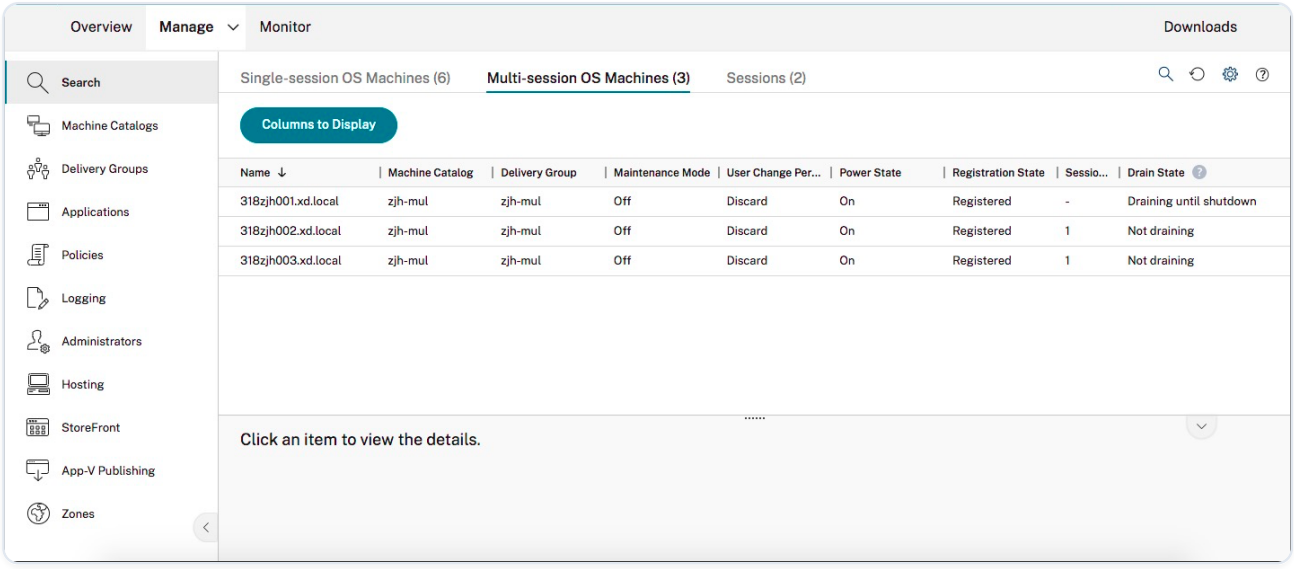
> **注:**
>
> この機能はマルチセッションマシンにのみ適用されます。

> Web Studio では、ドレイン状態のマシンを表示して、どのマシンがシャットダウンしようとしているかを知ることができます。次の手順を完了します。

1. **検索**ノードに移動し、次に**表示する列**をクリックします。
2. **表示する列**ウィンドウで、**ドレイン状態**の横にあるチェックボックスを選択します。
3. **保存**をクリックして、**表示する列**ウィンドウを終了します。

ドレイン状態列には、次の情報が表示されます。

- **シャットダウンまでドレイン中。** マシンがシャットダウンされるまでドレイン状態にある場合に表示されます。
- **ドレインしていません。** マシンがまだドレイン状態にない場合に表示されます。



詳細情報

Autoscaleの詳細については、Tech ZoneのCitrix Autoscaleを参照してください。

スケジュールベースおよび負荷ベースの設定

Autoscale™ によるマシンの電源管理

Autoscale は、選択されたスケジュールに基づいてマシンの電源をオン/オフします。Autoscale を使用すると、特定の曜日を含む複数のスケジュールを設定し、その時間帯に利用可能なマシンの数を調整できます。特定の曜日の特定の時間に一連のユーザーがマシンリソースを消費すると予想される場合、Autoscale は最適化されたエクスペリエンスを提供するのに役立ちます。これらのマシンは、セッションが実行されているかどうかにかかわらず、スケジュール中に電源がオンになることに注意してください。

> **注：**
>
> Autoscaleは、電源管理されているすべてのマシンをサポートします。

> スケジュールは、デリバリーグループの**タイムゾーン**に基づいています。タイムゾーンを変更するには、デリバリーグループのユーザー設定を変更します。詳しくは、「デリバリーグループの管理」を参照してください。

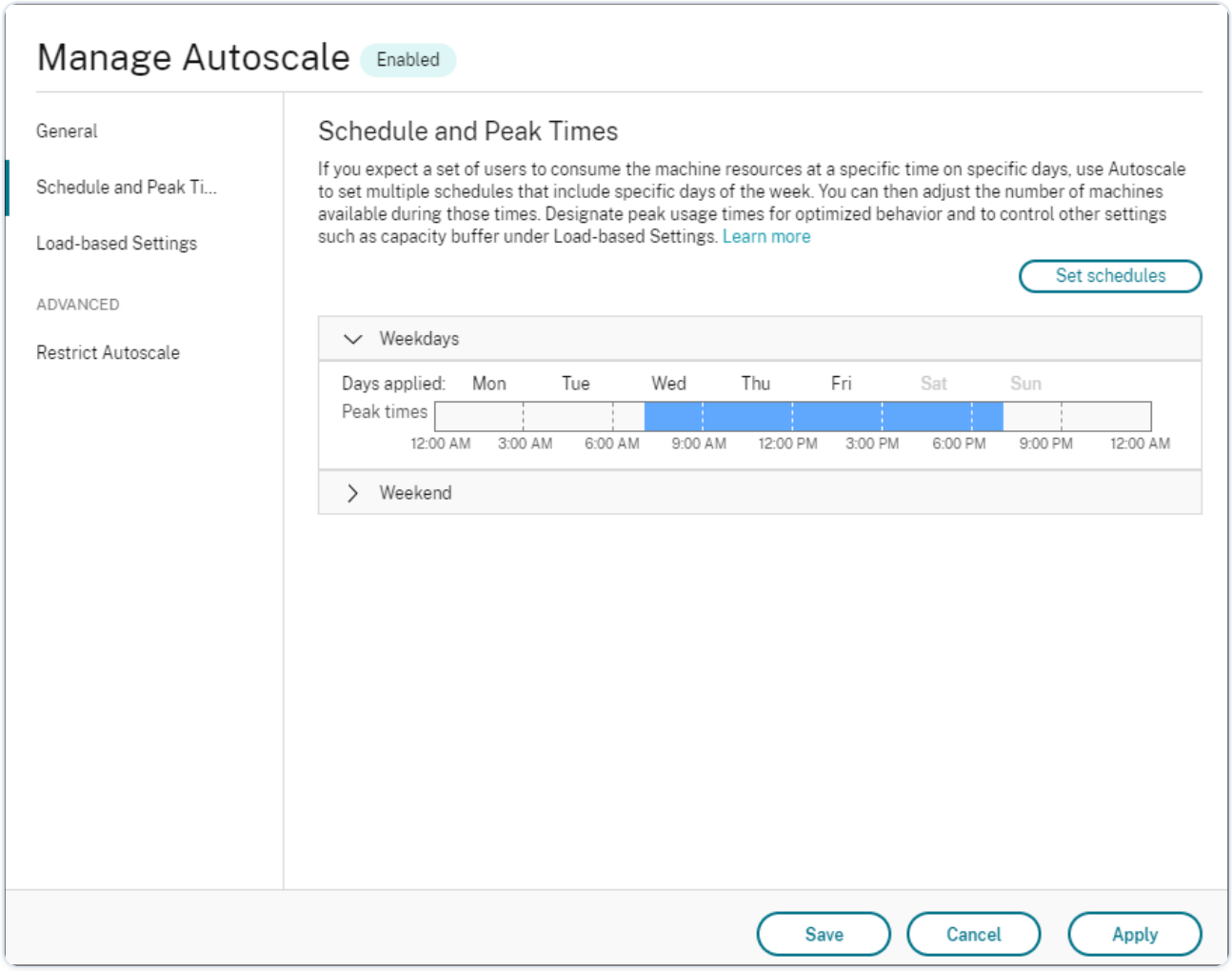
Autoscale には、*平日*（月曜日から金曜日）と*週末*（土曜日と日曜日）の2つのデフォルトスケジュールがあります。デフォルトでは、**平日**スケジュールでは、ピーク時に午前7時から午後6時30分まで1台のマシンの電源がオンになり、オフピーク時には電源がオフになります。デフォルトの容量バッファは、ピーク時とオフピーク時で10%に設定されています。デフォルトでは、**週末**スケジュールでは、マシンの電源はオンになりません。

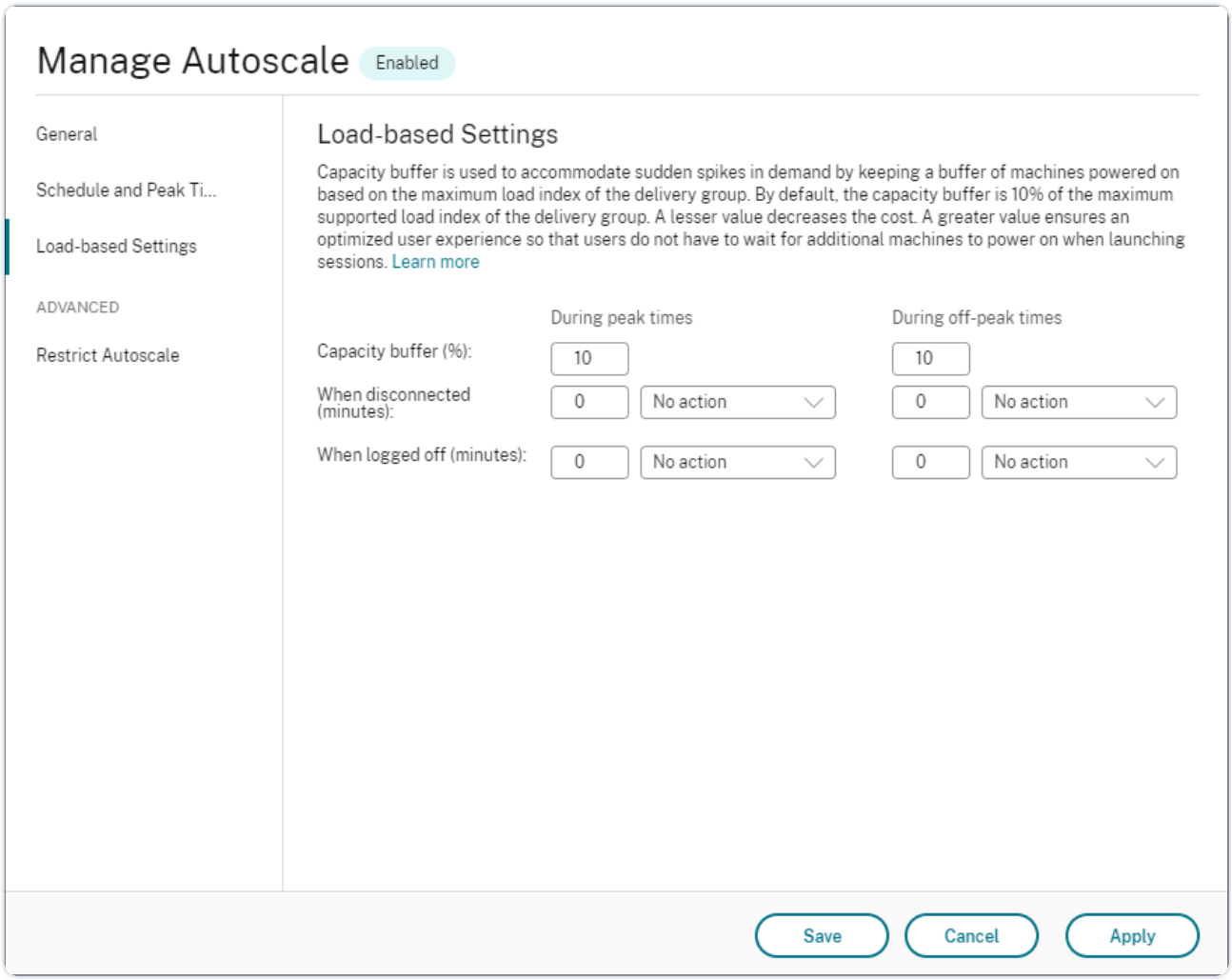
> **注：**
>
> Autoscaleは、サイトに登録されているマシンのみを、計算における利用可能な容量の一部として扱います。「登録済み」とは、マシンが使用可能であるか、すでに使用中であることを意味します。これにより、ユーザーセッションを受け入れられるマシンのみがデリバリーグループの容量に含まれるようになります。

ユーザーインターフェイス

認識しておくべきユーザーインターフェイスは3種類あります。

*シングルセッションOS静的デリバリーグループ*のユーザーインターフェイス：


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
Weekdays
Days applied: Mon Tue Wed Thu Fri Sat Sun
Peak times
12:00 AM 3:00 AM 6:00 AM 9:00 AM 12:00 PM 3:00 PM 6:00 PM 9:00 PM 12:00 AM
Weekend
Save
Cancel
Apply

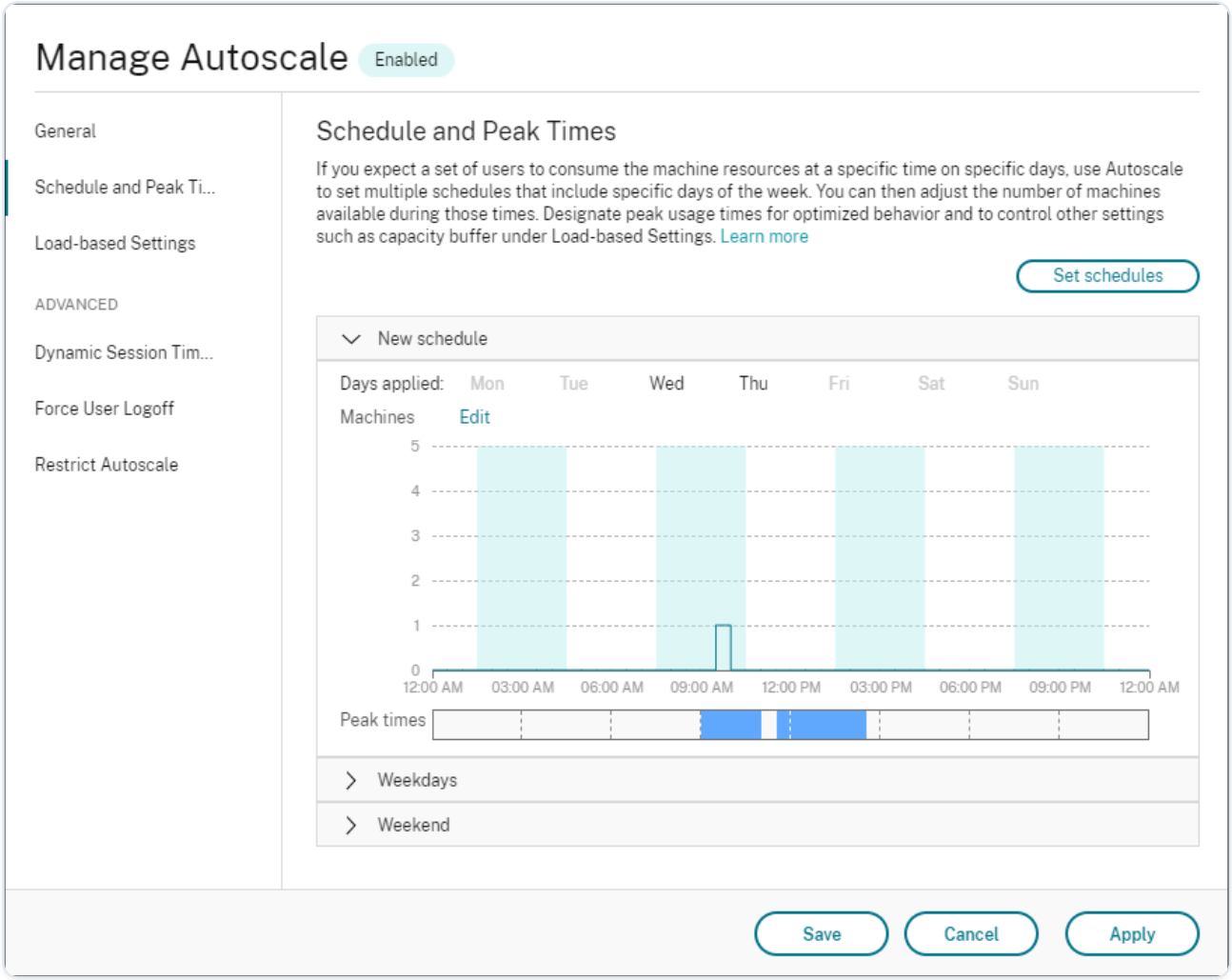


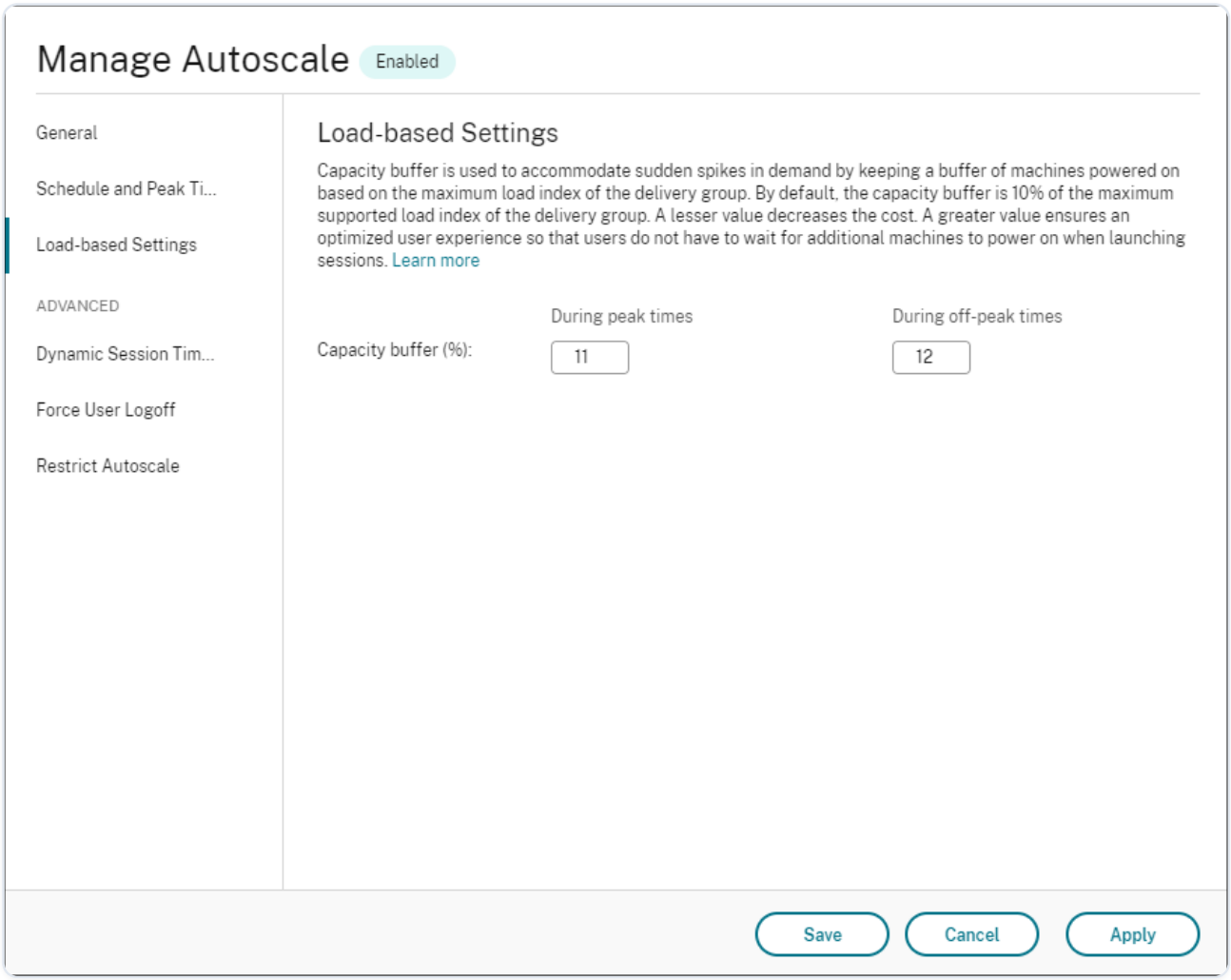
*シングルセッションOSランダムデリバリーグループの*Autoscaleユーザーインターフェイス：

Autoscale シングルセッションOS (ランダム) - スケジュール(/en-us/citrix-virtual-apps-desktops/2407/media/autoscale-schedule-ss-random.png)

Autoscale シングルセッションOS (ランダム) - 負荷ベース(/en-us/citrix-virtual-apps-desktops/2407/media/autoscale-load-based-ss-random.png)

*マルチセッションOSデリバリーグループの*Autoscaleユーザーインターフェイス：


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Dynamic Session Tim...
Force User Logoff
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
New schedule
Days applied: Mon Tue Wed Thu Fri Sat Sun
Machines Edit
5
4
3
2
1
0
12:00 AM 03:00 AM 06:00 AM 09:00 AM 12:00 PM 03:00 PM 06:00 PM 09:00 PM 12:00 AM
Peak times
Weekdays
Weekend
Save
Cancel
Apply



スケジュールベースの設定

Autoscale スケジュール。スケジュールの追加、編集、選択、削除ができます。

適用日。選択したスケジュールに適用した日を強調表示します。残りの日はグレー表示されます。

編集。マシンを1時間ごとまたは30分ごとに割り当てることができます。マシンは数値またはパーセンテージで割り当てることができます。

> **注:**
>
> - このオプションは、マルチセッションOSおよびシングルセッションOS (ランダム) デリバリーグループのAutoscaleユーザーインターフェイスでのみ使用できます。
> - **編集**の横にあるヒストグラムは、異なる時間帯で実行されているマシンの数または割合を示します。

- **ピーク時間**の上にある**編集**をクリックして、各時間帯に**マシンを割り当てる**ことができます。**起動するマシン**ウィンドウのメニューから選択したオプションに応じて、マシンを数値またはパーセンテージで割り当てることができます。
- マルチセッションOSデリバリーグループの場合、各日において30分単位で実行中のマシンの最小数を個別に設定できます。シングルセッションOS (ランダム) デリバリーグループの場合、各日において60分単位で実行中のマシンの最小数を個別に設定できます。

独自のスケジュールを定義するには、次の手順に従います。

1. 「**Autoscaleの管理**」ウィンドウの「**スケジュールとピーク時間**」ページで、「**スケジュールの設定**」をクリックします。
2. **Autoscaleスケジュールの編集**ウィンドウで、各スケジュールに適用する日を選択します。必要に応じてスケジュールを削除することもできます。
3. **完了**をクリックしてスケジュールを保存し、**スケジュールとピーク時間**ページに戻ります。
4. 該当するスケジュールを選択し、必要に応じて構成します。
5. **適用**をクリックして、**Autoscaleの管理**ウィンドウを終了するか、他のページで設定を構成します。

重要:

- Autoscaleでは、異なるスケジュールで同じ曜日が重複することはできません。たとえば、schedule1で月曜日を選択した後、schedule2で月曜日を選択すると、schedule1の月曜日は自動的にクリアされます。
- スケジュール名は大文字と小文字を区別しません。
- スケジュール名は空白にしたり、スペースのみを含めたりすることはできません。
- Autoscaleでは、文字間に空白スペースを入れることができます。
- スケジュール名には、次の文字を含めることはできません: \ / ; : # . * ? = < > \| ( ) { } " ' `。
- Autoscaleは重複するスケジュール名をサポートしていません。各スケジュールに異なる名前を入力してください。
- Autoscaleは空のスケジュールをサポートしていません。つまり、曜日が選択されていないスケジュールは保存されません。

注:

選択したスケジュールに含まれる曜日は強調表示され、含まれない曜日はグレー表示されます。

負荷ベースの設定

ピーク時間。選択したスケジュールに適用した日のピーク時間を定義できます。これを行うには、横棒グラフを右クリックします。ピーク時間を定義すると、残りの未定義の時間はデフォルトでオフピーク時間になります。**デフォルト**では、選択したスケジュールに含まれる日のピーク時間として、午前7時から午後7時までの時間帯が定義されています。

重要:

- マルチセッションOSデリバリーグループの場合、ピーク時間の棒グラフは容量バッファーに使用されます。
- シングルセッションOSデリバリーグループの場合、ピーク時間の棒グラフは容量バッファーに使用され、ログオフ後および/または切断後にトリガーされるアクションを制御します。
- マルチセッションOSおよびシングルセッションOSデリバリーグループの両方で、スケジュールに含まれる日のピーク時間を30分単位で細かく定義できます。または、代わりに`New-BrokerPowerTimeScheme PowerShell`コマンドを使用することもできます。詳しくは、「Broker PowerShell SDKコマンド」を参照してください。

容量バッファー。電源がオンになっているマシンのバッファーを維持できます。値が小さいほどコストが削減されます。値が大きいほど、セッション起動時にユーザーが追加のマシンの電源がオンになるのを待つ必要がないため、最適化されたユーザーエクスペリエンスが保証されます。デフォルトでは、容量バッファーはピーク時間とオフピーク時間で10%です。容量バッファーを0に設定すると、セッション起動時にユーザーが追加のマシンの電源がオンになるのを待つ必要がある場合があります。Autoscaleでは、ピーク時間とオフピーク時間で容量バッファーを個別に決定できます。

その他の設定

ヒント:

- Broker PowerShell SDKを使用してその他の設定を構成することもできます。詳しくは、「Broker PowerShell SDKコマンド」を参照してください。
- 切断時およびログオフ時の設定に関連するSDKコマンドを理解するには、`<https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy>`を参照してください。

切断時。セッション切断後、切断されロックされたマシンが、中断またはシャットダウンされるまで電源がオンのままになる時間を指定できます。時間値を指定すると、構成したアクションに応じて、指定された切断時間が経過したときにマシンが中断またはシャットダウンされます。デフォルトでは、切断されたマシンにはアクションが割り当てられません。ピーク時間とオフピーク時間でアクションを個別に定義できます。これを行うには、下矢印をクリックし、メニューから次のいずれかのオプションを選択します。

- **アクションなし**。選択すると、セッション切断後もマシンの電源はオンのままになります。Autoscaleはそれに対してアクションを実行しません。
- **中断**。選択すると、指定された切断時間が経過したときに、Autoscaleはマシンをシャットダウンせずに一時停止します。**中断**を選択すると、次のオプションが利用可能になります。
  - **再接続なしの場合（分）**。中断されたマシンは、切断されたユーザーが再接続したときに利用可能ですが、新しいユーザーには利用できません。すべてのワークロードを処理するためにマシンを再び利用可能にするには、シャットダウンします。Autoscaleがそれらをシャットダウンするまでのタイムアウトを分単位で指定します。
- **シャットダウン**。選択すると、指定された切断時間が経過したときに、Autoscaleはマシンをシャットダウンします。

注:

このオプションは、シングルセッションOSのランダムおよび静的デリバリーグループ用のAutoscaleユーザーインターフェイスでのみ使用できます。

ログオフ時。セッションログオフ後、マシンがサスペンドまたはシャットダウンされるまでに電源がオンのままになる時間を指定できます。時間値を指定した場合、設定したアクションに応じて、指定されたログオフ時間が経過するとマシンはサスペンドまたはシャットダウンされます。デフォルトでは、ログオフされたマシンにはアクションが割り当てられていま

せん。ピーク時とオフピーク時でアクションを個別に定義できます。これを行うには、下矢印をクリックし、メニューから次のいずれかのオプションを選択します。

- **アクションなし**。選択した場合、セッションログオフ後もマシンは電源がオンのままになります。Autoscale はそのマシンに対して何も実行しません。
- **サスペンド**。選択した場合、指定されたログオフ時間が経過すると、Autoscale はマシンをシャットダウンせずに一時停止します。
- **シャットダウン**。選択した場合、指定されたログオフ時間が経過すると、Autoscale はマシンをシャットダウンします。

注:

このオプションは、シングルセッションOSの静的デリバリーグループ用のAutoscaleユーザーインターフェイスでのみ使用できます。

切断されたセッションを持つ、異なる時間帯に移行するシングルセッションOSマシンの電源管理

重要:

- この機能強化は、切断されたセッションを持つシングルセッションOSマシンにのみ適用されます。ログオフされたセッションを持つシングルセッションOSマシンには適用されません。
- この機能強化を有効にするには、該当するデリバリーグループでAutoscaleを有効にする必要があります。そうしないと、期間移行時に切断電源ポリシーアクションはトリガーされません。

以前のリリースでは、アクション（切断アクション = 「**一時停止**」または「**シャットダウン**」）が必要な時間帯に移行するシングルセッションOSマシンは、電源が入ったままでした。このシナリオは、マシンがアクション（切断アクション = 「**何もしない**」）が不要な時間帯（ピーク時またはオフピーク時）に切断された場合に発生しました。

このリリースから、Autoscale は、指定された切断時間が経過すると、移行先の時間帯に設定された切断アクションに応じて、マシンをサスペンドまたは電源オフにします。

例えば、シングルセッションOSデリバリーグループに対して、以下の電源ポリシーを設定します。

- `PeakDisconnectAction` を「何もしない」に設定する
- `OffPeakDisconnectAction` を「シャットダウン」に設定する
- 'OffPeakDisconnectTimeout' を「10」に設定する

> **注:**
>
> 切断アクション電源ポリシーの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy>` および `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>` を参照してください。

> 以前のリリースでは、ピーク時にセッションが切断されたシングルセッションOSマシンは、ピークからオフピークに移行しても電源が入ったままでした。このリリース以降、期間移行時に `OffPeakDisconnectAction` および `OffPeakDisconnectTimeout` ポリシーアクションがシングルセッションOSマシンに適用されます。その結果、マシンはオフピークに移行してから10分後に電源がオフになります。

以前の動作に戻したい場合（つまり、切断されたセッションを持つマシンがピークからオフピークへ、またはオフピークからピークへ移行する際に何もアクションを実行しない場合）は、以下のいずれかを実行します。

- 「LegacyPeakTransitionDisconnectedBehaviour」レジストリ値を1（true; 以前の動作を有効にする）に設定します。デフォルトでは、値は0（false; 期間移行時に切断電源ポリシーアクションをトリガーする）です。
  - パス: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - 名前: LegacyPeakTransitionDisconnectedBehaviour
  - 種類: REG_DWORD
  - データ: 0x00000001 (1)
- `Set-BrokerServiceConfigurationData` PowerShellコマンドを使用して設定を構成します。例:

- `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

マシンに期間移行時に電源ポリシーアクションを適用する前に、以下の条件を満たす必要があります。

- 切断されたセッションがある。
- 保留中の電源アクションがない。
- 異なる期間に移行するシングルセッションOSデリバリーグループに属している。
- 特定の期間（ピーク時またはオフピーク時）にセッションが切断され、電源アクションが割り当てられている期間に移行する。

キャパシティバッファの仕組み

キャパシティバッファは、動的な負荷増加に対応するために、現在の需要に予備容量を追加するために使用されます。注意すべき2つのシナリオがあります。

- マルチセッションOSデリバリーグループの場合、キャパシティバッファは、ロードインデックスの観点からデリバリーグループの総容量の割合として定義されます。ロードインデックスの詳細については、ロードインデックスを参照してください。
- シングルセッションOSデリバリーグループの場合、キャパシティバッファは、マシンの数の観点からデリバリーグループの総容量の割合として定義されます。

> **注:**
>
> Autoscaleをタグ付きマシンに制限するシナリオでは、キャパシティバッファは、ロードインデックスの観点からデリバリーグループ内のタグ付きマシンの総容量の割合として定義されます。

> Autoscaleでは、ピーク時とオフピーク時でキャパシティバッファを個別に設定できます。キャパシティバッファフィールドの値が小さいほど、Autoscaleが起動する予備容量が少なくなるため、コストが削減されます。値が大きいほど、ユーザーがセッションを起動する際に追加のマシンの起動を待つ必要がないため、最適化されたユーザーエクスペリエンスが保証されます。デフォルトでは、キャパシティバッファは10%です。

> **重要:**

キャパシティバッファにより、総予備容量がデリバリーグループの総容量の「X」パーセントを下回るレベルに低下した場合にマシンが起動されます。これにより、必要な割合の予備容量が確保されます。

マルチセッションOSデリバリーグループ

マシンはいつ起動されますか?

重要:

スケジュールが選択されている場合、Autoscale はスケジュールで電源オンになるように構成されているすべてのマシンの電源をオンにします。Autoscale は、負荷に関係なく、スケジュール中に指定された数のマシンの電源をオンに保ちます。

デリバリーグループ内の電源オン状態のマシン数が、負荷インデックスの観点からバッファ容量を維持するために必要なバッファを満たせなくなった場合、Autoscale は追加のマシンの電源をオンにします。たとえば、デリバリーグループに 20 台のマシンがあり、スケジュールベースのスケーリングの一部として、容量バッファ 20% で 3 台のマシンの電源がオンになるようにスケジュールされているとします。最終的に、負荷がない場合でも 4 台のマシンの電源がオンになります。これは、バッファとして 4 x 10k の負荷インデックスが必要であるため、少なくとも 4 台のマシンの電源をオンにする必要があるためです。このケースは、ピーク時、マシンの負荷増加、新しいセッションの起動、およびデリバリーグループに新しいマシンを追加するときに発生する可能性があります。Autoscale は、次の条件を満たすマシンのみの電源をオンにすることに注意してください。

- マシンがメンテナンスモードではない。
- マシンが実行されているハイパーバイザーがメンテナンスモードではない。
- マシンが現在電源オフ状態であること。
- マシンに保留中の電源操作がないこと。

マシンはいつ電源オフになりますか?

重要:

- スケジュールが選択されている場合、Autoscale はスケジュールに基づいてマシンの電源をオフにします。
- Autoscale は、スケジュール中に電源オンになるようにスケジュールで構成されているマシンの電源をオフにしません。

デリバリーグループのターゲットとなる電源オン状態のマシン数（バッファを含む）をサポートするのに十分なマシン数を超えている場合、Autoscale は余分なマシンの電源をオフにします。このケースは、オフピーク時、マシンの負荷減少、セッションログオフ、およびデリバリーグループからマシンを削除するときに発生する可能性があります。Autoscale は、次の条件を満たすマシンのみの電源をオフにします。

- マシンおよびマシンが実行されているハイパーバイザーがメンテナンスモードではないこと。
- マシンが現在電源オン状態であること。
- マシンは、起動後に利用可能として登録されるか、登録待ちの状態になります。
- マシンにアクティブなセッションはありません。
- マシンに保留中の電源操作はありません。
- マシンは指定された電源オフ遅延を満たしています。これは、マシンが少なくとも「X」分間電源オンの状態であったことを意味します。「X」はデリバリーグループに指定された電源オフ遅延です。

例のシナリオ

次のシナリオを想定します。

- **デリバリーグループの構成**。Autoscale で電源管理するデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscale の構成**
  - キャパシティバッファは10%に設定されています。
  - 選択されたスケジュールにはマシンが含まれていません。

シナリオは次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. より多くのユーザーセッションが開始されます。
4. セッション終了により、ユーザーセッションの負荷が減少します。

5. セッション負荷がオンプレミスリソースのみで処理されるまで、ユーザーセッションの負荷はさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期状態）
  - 1台のマシン（例: M1）が電源オンになります。このマシンは、構成されたキャパシティバッファのために電源オンになります。この場合、10（マシン数）x 10,000（負荷インデックス）x 10%（構成されたキャパシティバッファ）は10,000に等しくなります。したがって、1台のマシンが電源オンになります。
  - 電源オンになったマシン（M1）の負荷インデックス値は、ベースライン負荷（負荷インデックスは0）です。
- 最初のユーザーがログオンします
  - セッションはマシンM1でホストされるように指示されます。
  - 電源オンになったマシンM1の負荷インデックスが増加し、マシンM1はベースライン負荷ではなくなります。
  - 構成されたキャパシティバッファにより、Autoscale は需要を満たすために追加のマシン (M2) の電源をオンにし始めます。
  - マシン M2 の負荷インデックス値はベースライン負荷にあります。
- ユーザーが負荷を増加させます
  - セッションはマシン M1 と M2 の間で負荷分散されます。その結果、起動中のマシン (M1 と M2) の負荷インデックスが増加します。
  - 総予備容量は、負荷インデックスの観点から依然として 10,000 を超えるレベルにあります。
  - マシン M2 の負荷インデックス値はもはやベースライン負荷ではありません。
- より多くのユーザーセッションが開始されます
  - セッションはマシン (M1 と M2) の間で負荷分散されます。その結果、起動中のマシン (M1 と M2) の負荷インデックスがさらに増加します。
  - 負荷インデックスの観点から総予備容量が 10,000 を下回るレベルに低下すると、Autoscale は構成されたキャパシティバッファにより、需要を満たすために追加のマシン (M3) の電源をオンにし始めます。
  - マシン M3 の負荷インデックス値はベースライン負荷にあります。

- さらに多くのユーザーセッションが開始されます
  - セッションはマシン (M1 から M3) の間で負荷分散されます。その結果、起動中のマシン (M1 から M3) の負荷インデックスが増加します。
  - 総予備容量は、負荷インデックスの観点から 10,000 を超えるレベルにあります。
  - マシン M3 の負荷インデックス値はもはやベースライン負荷ではありません。
- セッション終了によりユーザーセッションの負荷が減少します
  - ユーザーがセッションからログオフするか、アイドルセッションがタイムアウトすると、M1からM3までのマシンで解放された容量が、他のユーザーが開始したセッションをホストするために再利用されます。
  - ロードインデックスの観点から総予備容量が10,000を超えるレベルに増加すると、Autoscaleはマシンの1つ（たとえばM3）をドレイン状態にします。その結果、新しい変更が発生しない限り、他のユーザーが開始したセッションはそのマシンに転送されなくなります。たとえば、エンドユーザーの負荷が再び増加したり、他のマシンの負荷が最も低くなったりした場合です。
- ユーザーセッションの負荷は減少し続けます
  - マシンM3上のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、AutoscaleはマシンM3の電源をオフにします。
  - さらに多くのユーザーがセッションを終了すると、電源がオンになっているマシン（M1とM2）で解放された容量が、他のユーザーが開始したセッションをホストするために再利用されます。
  - ロードインデックスの観点から総予備容量が10,000を超えるレベルに増加すると、Autoscaleはマシンの1つ（たとえばM2）をドレイン状態にします。その結果、他のユーザーが開始したセッションはそのマシンに転送されなくなります。
- セッションがなくなるまでユーザーセッションの負荷は減少し続けます
  - マシンM2上のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、AutoscaleはマシンM2の電源をオフにします。
  - 電源がオンになっているマシン（M1）のロードインデックス値はベースライン負荷です。構成された容量バッファーのため、AutoscaleはマシンM1をドレイン状態にしません。

> **注:**

> マルチセッションOSデリバリーグループの場合、ユーザーがセッションからログオフすると、デスクトップへのすべての変更は失われます。ただし、構成されている場合、ユーザー固有の設定はユーザープロファイルとともにローミングされます。

シングルセッションOSランダムデリバリーグループ

容量バッファーは、デリバリーグループ内のマシンの総数に基づいて、電源がオンになっているマシンのバッファーを維持することで、需要の急増に対応するために使用されます。デフォルトでは、容量バッファーはデリバリーグループ内のマシンの総数の10%です。

マシンの数（容量バッファーを含む）が現在電源がオンになっているマシンの総数を超える場合、需要を満たすために追加のマシンの電源がオンになります。マシンの数（容量バッファーを含む）が現在電源がオンになっているマシンの総数よりも少ない場合、余分なマシンは、構成したアクションに応じてシャットダウンまたは中断されます。

電源ポリシー

さまざまなシナリオでマシンの電源を管理するポリシーを構成します。各シナリオについて、待機時間（分単位）と、指定された時間が終了した後に実行するアクションを指定できます。電源ポリシーは、シングルセッションOSランダムデリバリーグループおよびシングルセッションOS静的デリバリーグループに適用されます。

電源ポリシーのアクション(/en-us/citrix-virtual-apps-desktops/2407/media/power-policies-actions.png)

切断後、ピーク時とオフピーク時の両方で、以下の設定が適用されます。

- ドロップダウンから、待機時間を分単位で設定し、「アクションなし」、「一時停止」、「シャットダウン」などのアクションを選択できます。
- 一時停止アクションを選択した場合、マシンをシャットダウンするための追加の待機時間を構成します。

> **注:**
>
> - ピーク時およびオフピーク時において、シャットダウンアクションの待機時間は、一時停止の待機時間よりも長くする必要があります。
> - 一時停止されたマシンは、切断されたユーザーが再接続した場合にのみアクセス可能です。一時停止されたマシンを新規ユーザーが利用できるようにするには、シャットダウンしてください。

- 一時停止フィールドとシャットダウンフィールドの時刻設定が正しく構成されていない場合、**保存**オプションが無効になり、設定エラーを示す赤い点もナビゲーション項目の横に表示されます。

シングルセッションOSランダムDG電源ポリシー設定(/en-us/citrix-virtual-apps-desktops/2407/media/single-session-os-random-dg-power-policies-settings.png)

例

- 待機時間を12分に設定し、最初のアクションを「アクションなし」に選択した場合、12分経過後もマシンは電源オン状態を維持します。
- 待機時間を15分に設定し、最初のアクションを「一時停止」、2番目の待機時間を20分に選択した場合、15分経過後にマシンは一時停止されます。2番目の待機時間経過後にマシンはシャットダウンされます。
- 待機時間を18分に設定し、最初のアクションを「シャットダウン」に選択した場合、18分経過後にマシンはシャットダウンされます。

例のシナリオ

次のシナリオを想定します。

- **デリバリーグループの構成**。Autoscaleで電源管理するデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscaleの構成**
  - 容量バッファは10%に設定されています。
  - 選択したスケジュールにマシンは含まれていません。

シナリオは次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. さらに多くのユーザーセッションが開始されます。
4. セッション終了により、ユーザーセッションの負荷が減少します。
5. ユーザーセッションの負荷は、オンプレミスリソースのみで処理されるまでさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかの詳細については、以下を参照してください。

- ユーザー負荷なし（初期状態）
  - 1台のマシン（例：M1）が電源オンになります。このマシンは、構成されたキャパシティバッファのために電源オンになります。この場合、10（マシン数）x 10,000（負荷インデックス）x 10%（構成されたキャパシティバッファ）は10,000に等しくなります。したがって、1台のマシンが電源オンになります。
  - 電源オンのマシン（M1）の負荷インデックス値は、ベースライン負荷（負荷インデックスは0に等しい）です。
- 最初のユーザーがログオンします
  - セッションはマシンM1でホストされるように指示されます。
  - 電源オンのマシンM1の負荷インデックスが増加し、マシンM1はベースライン負荷ではなくなります。
  - Autoscaleは、構成されたキャパシティバッファのために需要を満たすために、追加のマシン（M2）の電源をオンにし始めます。
  - マシンM2の負荷インデックス値はベースライン負荷です。
- 2番目のユーザーがログオンします
  - ユーザーにはM2マシンからデスクトップが割り当てられます。
  - 設定されたキャパシティバッファにより需要を満たすため、Autoscaleは追加のマシン（M3）の電源をオンにし始めます。
- より多くのユーザーセッションが開始されます
  - セッションはマシン (M1 および M2) 間で負荷分散されます。その結果、電源がオンになっているマシン (M1 および M2) の負荷インデックスがさらに増加します。
  - 合計予備容量が負荷インデックスで10,000を下回ると、構成された容量バッファにより、Autoscale は需要を満たすため追加のマシン (M3) の電源をオンにし始めます。
  - マシン M3 の負荷インデックス値はベースライン負荷です。
- さらに多くのユーザーセッションが開始されます
  - セッションはマシン (M1 から M3) 間で負荷分散されます。その結果、電源がオンになっているマシン (M1 から M3) の負荷インデックスが増加します。
  - 合計予備容量は負荷インデックスで10,000を上回っています。
  - マシン M3 の負荷インデックス値はベースライン負荷ではなくなります。
- セッション終了によりユーザーセッションの負荷が減少します

    - ユーザーがセッションからログオフするか、アイドルセッションがタイムアウトすると、マシン M1 から M3 で解放された容量は、他のユーザーが開始したセッションをホストするために再利用されます。
    - 合計予備容量が負荷インデックスで10,000を上回ると、Autoscale はマシンの1つ (たとえば M3) をドレイン状態にします。その結果、新しい変更が発生しない限り、他のユーザーが開始したセッションはそのマシンに転送されなくなります。たとえば、エンドユーザーの負荷が再び増加したり、他のマシンの負荷が最も低くなったりした場合です。

- ユーザーセッションの負荷は減少し続けます
    - マシン M3 のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、Autoscale はマシン M3 の電源をオフにします。
    - さらに多くのユーザーがセッションを終了すると、電源がオンになっているマシン (M1 および M2) で解放された容量は、他のユーザーが開始したセッションをホストするために再利用されます。
    - 合計予備容量が負荷インデックスで10,000を上回ると、Autoscale はマシンの1つ (たとえば M2) をドレイン状態にします。その結果、他のユーザーが開始したセッションはそのマシンに転送されなくなります。

- セッションがなくなるまでユーザーセッションの負荷は減少し続けます
    - マシンM2上のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、Autoscaleはマシン M2の電源をオフにします。
    - 電源がオンになっているマシン（M1）の負荷インデックス値は、ベースライン負荷です。構成されたキャパシティバッファのため、AutoscaleはマシンM1をドレイン状態にしません。

> **注:**
>
> マルチセッションOSデリバリーグループの場合、ユーザーがセッションからログオフすると、デスクトップへのすべての変更は失われます。ただし、構成されている場合、ユーザー固有の設定はユーザープロファイルとともにローミングされます。

シングルセッションOSランダムデリバリーグループ

キャパシティバッファは、デリバリーグループ内のマシンの総数に基づいて、電源がオンになっているマシンのバッファを維持することで、需要の急増に対応するために使用されます。デフォルトでは、キャパシティバッファはデリバリーグループ内のマシンの総数の10%です。

マシンの数（キャパシティバッファを含む）が現在電源がオンになっているマシンの総数を超える場合、需要を満たすために追加のマシンが電源オンになります。マシンの数（キャパシティバッファを含む）が現在電源がオンになっているマシンの総数よりも少ない場合、余分なマシンは構成したアクションに応じてシャットダウンまたは中断されます。

電源ポリシー

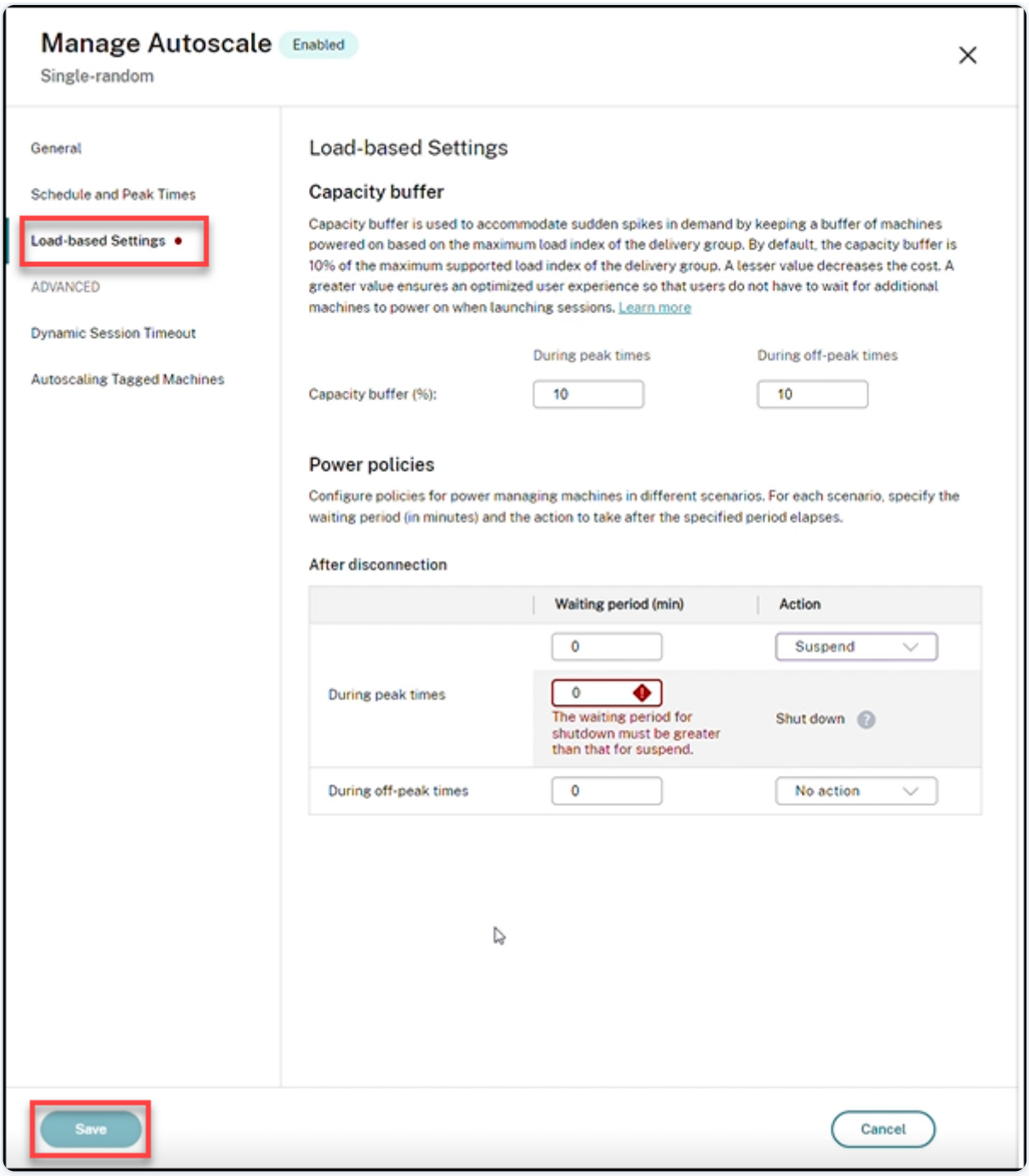
さまざまなシナリオでマシンの電源を管理するポリシーを構成します。各シナリオで、待機時間（分単位）と、指定された時間が終了した後に実行するアクションを指定できます。電源ポリシーは、シングルセッションOSランダムデリバリーグループおよびシングルセッションOS静的デリバリーグループに適用されます。

電源ポリシーのアクション(/en-us/citrix-virtual-apps-desktops/2407/media/power-policies-actions.png)

切断後、ピーク時とオフピーク時の両方で以下の設定が適用されます。

- ドロップダウンから、待機時間（分単位）と、アクション（アクションなし、中断、シャットダウンなど）を設定できます。
- 中断アクションを選択した場合、マシンをシャットダウンするための追加の待機時間を構成します。

> **注:**
>
> - ピーク時とオフピーク時では、シャットダウンアクションの待機時間は中断の待機時間よりも長くする必要があります。
> - 中断されたマシンは、再接続時に切断されたユーザーのみがアクセスできます。新規ユーザーが中断されたマシンを利用できるようにするには、シャットダウンします。
> - 中断およびシャットダウンのフィールドの時刻設定が正しく構成されていない場合、**保存**オプションは無効になり、設定エラーを示す赤い点もナビゲーション項目の横に表示されます。



たとえば

- 待機時間を12分に設定し、最初のアクションを「アクションなし」に選択した場合、12分経過後も、マシンは電源オンの状態を維持します。
- 待機時間を15分に設定し、最初のアクションを「中断」に選択し、2番目の待機時間を20分に設定した場合、15分経過後、マシンは中断されます。2番目の待機時間経過後、マシンはシャットダウンされます。
- 待機時間を18分に設定し、最初のアクションを「シャットダウン」に選択した場合、18分経過後、マシンはシャットダウンされます。

シナリオ例

次のシナリオを想定します。

- **デリバリーグループの構成**。Autoscaleで電源管理するデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscaleの構成**
  - キャパシティバッファは10%に設定されています。
  - 選択したスケジュールにはマシンが含まれていません。

シナリオは次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. より多くのユーザーセッションが開始されます。
4. セッション終了により、ユーザーセッションの負荷が減少します。
5. セッション負荷がオンプレミスリソースのみで処理されるまで、ユーザーセッションの負荷はさらに減少します。

上記のシナリオにおけるAutoscaleの動作の詳細については、以下を参照してください。

- ユーザー負荷なし（初期状態）
  - 1台のマシン（M1）が電源オンになります。このマシンは、構成されたキャパシティバッファのために電源オンになります。この場合、10（マシン数）x 10%（構成されたキャパシティバッファ）は1に等しくなります。したがって、1台のマシンが電源オンになります。
- 最初のユーザーがログオンします
  - ユーザーがデスクトップを使用するために初めてログオンすると、電源オンになっているマシンでホストされているデスクトップのプールからデスクトップが割り当てられます。この場合、ユーザーにはマシンM1からデスクトップが割り当てられます。
  - Autoscaleは、構成されたキャパシティバッファにより、需要を満たすためにもう1台のマシン（M2）の電源をオンにし始めます。
- 2番目のユーザーがログオンします
  - ユーザーにはマシンM2からデスクトップが割り当てられます。

    - Autoscaleは、構成されたキャパシティバッファにより、需要を満たすためにもう1台のマシン（M3）の電源をオンにし始めます。

- 3番目のユーザーがログオンします
    - ユーザーにはマシンM3からデスクトップが割り当てられます。
    - Autoscale は、設定された容量バッファのために、需要を満たすため追加のマシン (M4) の電源を入れ始めます。
- ユーザーがログオフする
    - ユーザーがログオフするか、ユーザーのデスクトップがタイムアウトすると、解放された容量 (例: M3) がバッファとして利用可能になります。その結果、容量バッファが10%に設定されているため、Autoscale はマシン M4 の電源を切り始めます。
- ユーザーがいなくなるまで、さらに多くのユーザーがログオフする
    - さらに多くのユーザーがログオフした後、Autoscale はマシン (例: M2 または M3) の電源を切ります。
    - ユーザーが残っていなくても、Autoscale は残りの1台のマシン (例: M1) の電源を切りません。なぜなら、そのマシンは予備容量として予約されているからです。

> **注:**
>
> シングルセッションOSのランダムデリバリーグループの場合、ユーザーがセッションをログオフすると、デスクトップへのすべての変更は失われます。ただし、設定されている場合、ユーザー固有の設定はユーザープロファイルとともにローミングされます。

シングルセッションOSの静的デリバリーグループ

容量バッファは、デリバリーグループ内の未割り当てマシンの総数に基づいて、電源がオンになっている未割り当てマシンのバッファを維持することで、急な需要の急増に対応するために使用されます。デフォルトでは、容量バッファはデリバリーグループ内の未割り当てマシンの総数の10%です。

> **重要:**
>
> デリバリーグループ内のすべてのマシンが割り当てられた後、容量バッファはマシンの電源のオン/オフには関与しません。

> マシンの数 (容量バッファを含む) が現在電源がオンになっているマシンの総数を超える場合、需要を満たすために追加の未割り当てマシンが電源オンになります。マシンの数 (容量バッファを含む) が現在電源がオンになっているマシンの総数よりも少ない場合、設定したアクションに応じて、余分なマシンは電源オフまたは一時停止されます。

シングルセッションOS静的デリバリーグループの場合、Autoscaleは次のようになります。

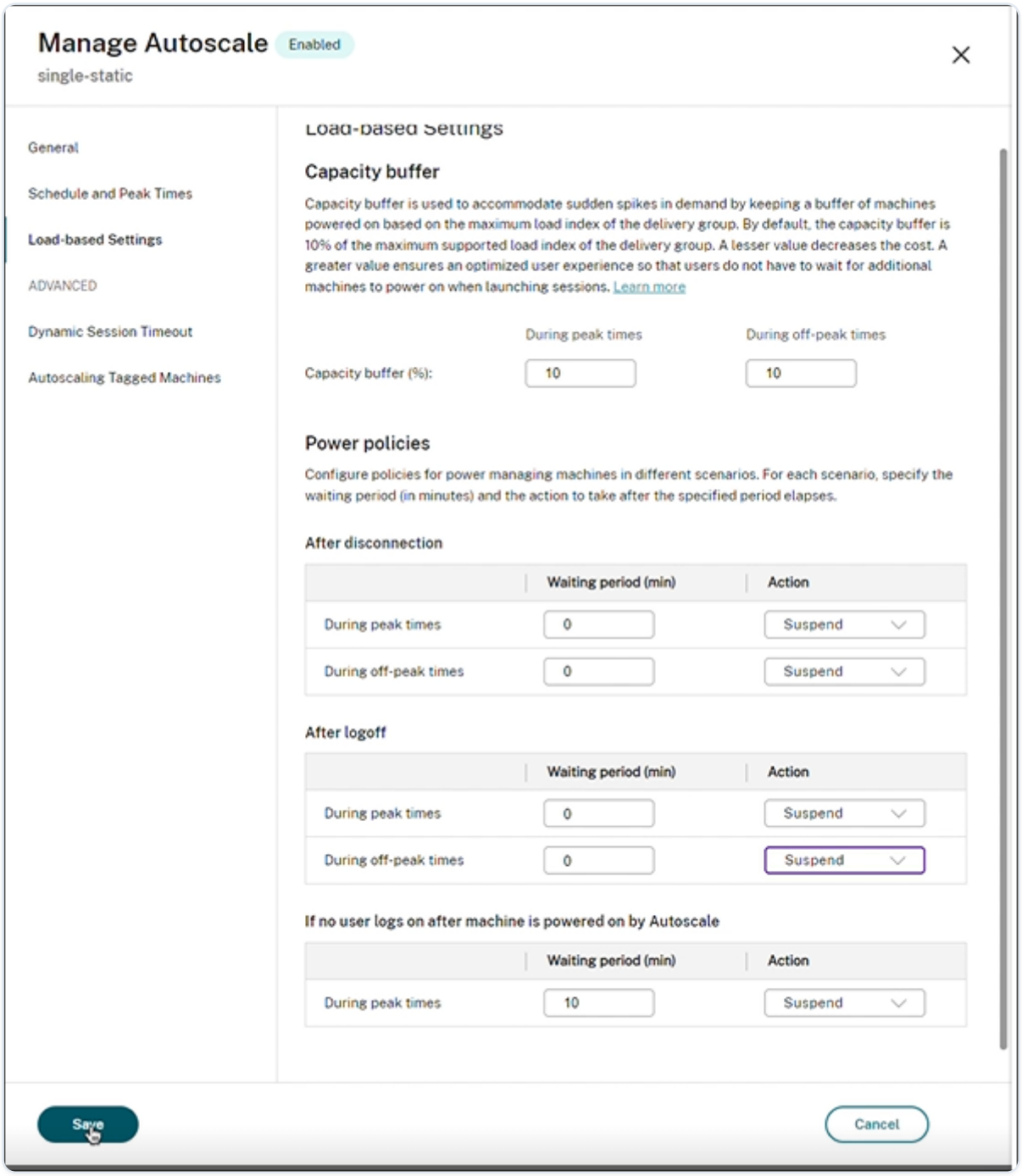
- 該当するシングルセッションOSデリバリーグループの `AutomaticPowerOnForAssigned` プロパティが true に設定されている場合にのみ、ピーク時に割り当てられたマシンの電源をオンにし、オフピーク時に電源をオフにします。
- ピーク時にマシンがオフになっていて、そのマシンが属するデリバリーグループの `AutomaticPowerOnForAssignedDuringPeak` プロパティがtrueに設定されている場合、自動的にマシンをオンにします。

割り当てられたマシンで容量バッファがどのように機能するかを理解するには、以下を考慮してください。

- 容量バッファは、デリバリーグループに1台以上の未割り当てのマシンがある場合にのみ機能します。
- デリバリーグループに未割り当てのマシンがない場合（デリバリーグループ内のすべてのマシンが割り当てられている場合）、容量バッファはマシンの電源オン/オフに影響しません。
- `AutomaticPowerOnForAssignedDuringPeak` プロパティは、ピーク時に割り当てられたマシンの電源がオンになるかどうかを決定します。trueに設定されている場合、Autoscaleはピーク時にマシンの電源をオンのままにします。また、電源がオフになっている場合でも、Autoscaleはそれらの電源をオンにします。

電源ポリシー

さまざまなシナリオでマシンの電源を管理するためのポリシーを構成します。各シナリオについて、待機時間（分単位）と、指定された時間が終了した後に実行するアクションを指定できます。電源ポリシーは、シングルセッションOSランダムデリバリーグループとシングルセッションOS静的デリバリーグループに適用されます。



切断後および**ログオフ後**については、ピーク時とオフピーク時の両方で以下の設定が適用されます。ドロップダウンから、待機時間（分単位）と、アクションなし、一時停止、シャットダウンなどのアクションを設定できます。

Autoscaleによってマシンの電源がオンになった後にユーザーがログオンしない場合、以下の設定はピーク時にのみ適用されます。ピーク時にドロップダウンから、待機時間（分単位）と、アクションなし、一時停止、シャットダウンなどのアクションを設定できます。

例のシナリオ

次のシナリオを想定します。

- **デリバリーグループの構成**。Autoscaleで電源管理するデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscaleの構成**
  - マシンM1～M3は割り当て済みで、マシンM4～M10は未割り当てです。
  - ピーク時とオフピーク時のキャパシティバッファは10%に設定されています。
  - 選択されたスケジュールに従って、Autoscaleは午前9時から午後6時までマシンを電源管理します。

上記のシナリオでAutoscaleがどのように機能するかについては、以下を参照してください。

- スケジュールの開始 – 午前9時
  - AutoscaleはマシンM1からM3の電源をオンにします。
  - 設定されたキャパシティバッファのため、Autoscaleは追加のマシン（例：M4）の電源をオンにします。マシンM4は未割り当てです。
- 最初のユーザーがログオンします
  - ユーザーがデスクトップを使用するために初めてログオンすると、未割り当ての電源オン状態のマシンでホストされているデスクトップのプールからデスクトップが割り当てられます。この場合、ユーザーにはマシンM4からデスクトップが割り当てられます。そのユーザーによるその後のログオンは、初回使用時に割り当てられた同じデスクトップに接続します。
  - 設定されたキャパシティバッファのため、Autoscaleは需要を満たすために追加のマシン（例：M5）の電源をオンにし始めます。
- 2番目のユーザーがログオンします
  - ユーザーには、未割り当ての電源オン状態のマシンからデスクトップが割り当てられます。この場合、ユーザーにはマシンM5からデスクトップが割り当てられます。そのユーザーによるその後のログオンは、初回使用時に割り当てられた同じデスクトップに接続します。
  - 設定されたキャパシティバッファのため、Autoscaleは需要を満たすために追加のマシン（例：M6）の電源をオンにし始めます。
- ユーザーがログオフします
  - ユーザーがデスクトップからログオフするか、デスクトップがタイムアウトすると、Autoscaleは午前9時から午後6時までマシンM1からM5の電源をオンのままにします。それ

らのユーザーが次回ログオンするときは、初回使用時に割り当てられた同じデスクトップに接続します。

- 未割り当てのマシンM6は、受信する未割り当てのユーザーにデスクトップを提供するのを待機しています。

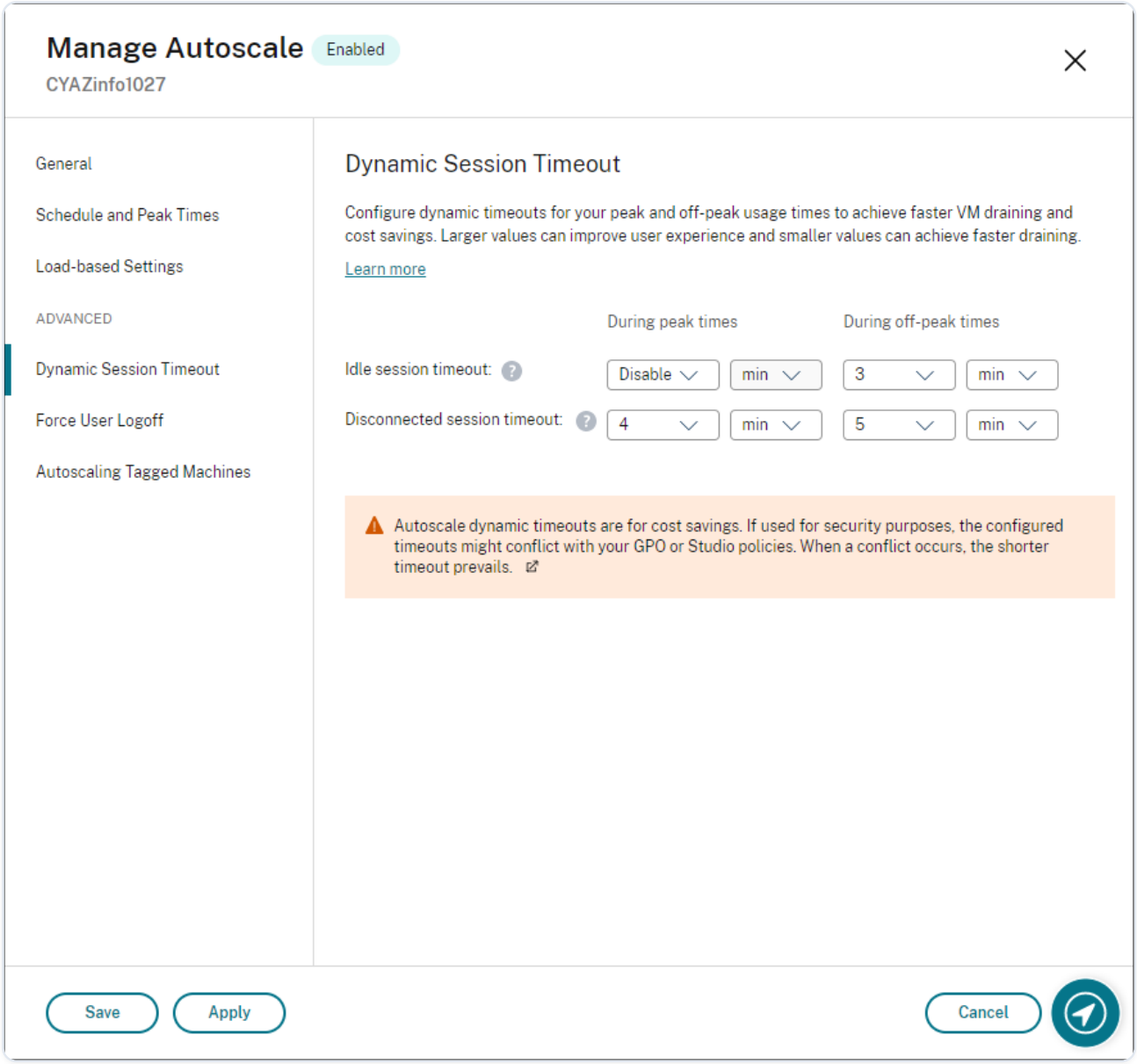
- スケジュールの終了 – 午後6時
  - 午後6時に、AutoscaleはマシンM1からM5の電源をオフにします。
  - Autoscaleは、構成された容量バッファのため、割り当てられていないマシンM6の電源をオンのままにします。そのマシンは、新しく割り当てられるユーザーにデスクトップを提供するのを待機しています。
  - デリバリーグループでは、マシンM6からM10は割り当てられていないマシンです。

動的セッションタイムアウト

この機能を使用すると、ピーク時とオフピーク時の使用時間に合わせて切断およびアイドルセッションタイムアウトを構成し、マシンのより迅速なドレインとコスト削減を実現できます。この機能は以下に適用されます。

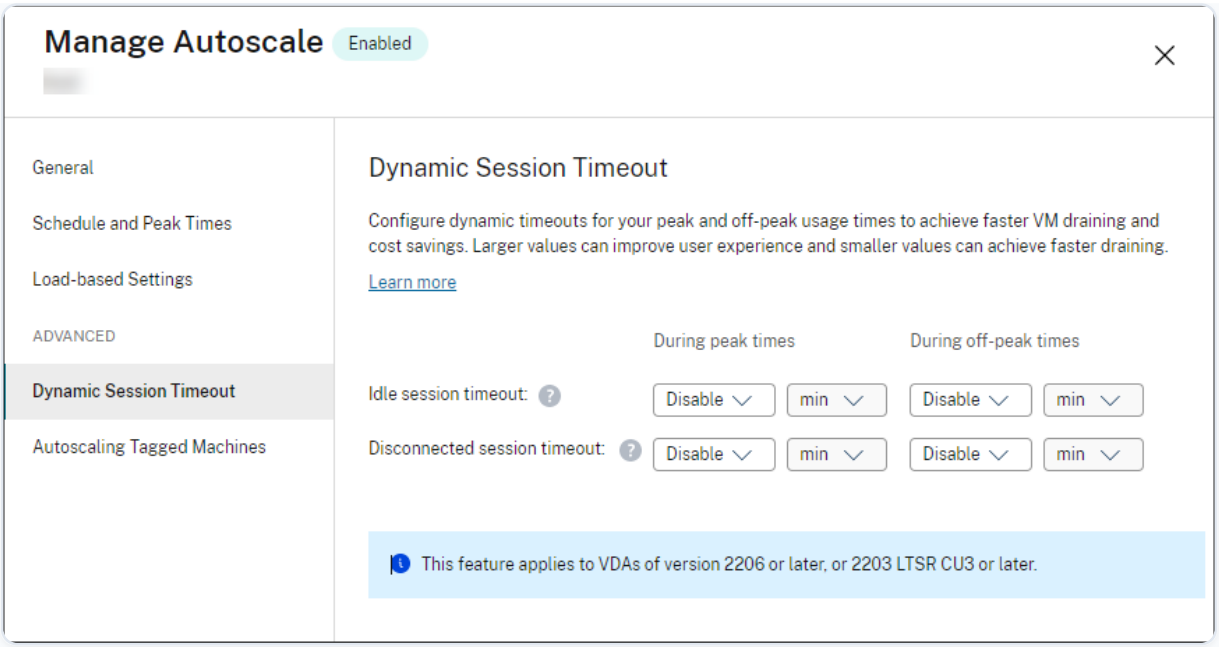
- シングルセッションおよびマルチセッションOSマシン。
- オートスケール用にタグ付けされているかどうかにかかわらず、デリバリーグループ内のすべてのマシン。

VDAは、10分以上アイドル状態であったセッションのアイドル時間を報告するため、動的セッションタイムアウトは、アイドル状態になってから10分以内にアイドルセッションを切断することはできません。より短い値を設定すると、残存セッションがより早く削除され、コストが削減されます。



注:

- この機能は、マルチセッションOSデリバリーグループで常に利用可能です。
- シングルセッションOSデリバリーグループの場合、この機能はバージョン2206 CR以降、または2203 LTSR CU3以降のVDAに適用されます。これらのVDAがCitrix Cloud™に少なくとも1回登録されていることを確認してください。利用できない場合、次のユーザーインターフェイスが表示されます。



- Autoscale™の動的タイムアウトはコスト削減を目的としています。セキュリティ目的で使用する場合、構成されたタイムアウトがGPOまたは管理コンソールポリシーと競合する可能性があります。競合が発生した場合、短い方のタイムアウトが優先されます。

アイドルセッションタイムアウト。ユーザー入力がない場合に、中断されていないユーザー接続が維持される時間を指定するタイマーを有効または無効にします。タイマーが期限切れになると、セッションは切断状態になり、**切断セッションタイムアウト**が適用されます。**切断セッションタイムアウト**が無効になっている場合、セッションはログオフされません。

重要:

- 10分（600秒）以下の値を指定した場合、Autoscaleは、関連するセッションが10分間アイドル状態になった後に切断します。これは、AutoscaleがVDAが報告するセッションのアイドル時間に依存しているためです。VDAは、10分以上アイドル状態であったセッションのアイドル時間のみを報告します。
- アイドルセッションタイムアウトに達するまでの最後の5分以内にユーザーが操作した場合でも、アイドルセッションは切断状態になることがあります。

> **切断されたセッションのタイムアウト**。切断されたデスクトップがセッションからログオフされるまでにロックされたままになる時間を指定するタイマーを有効または無効にします。有効にすると、タイマーの期限が切れたときに切断されたセッションがログオフされます。

よくある質問

動的セッションタイムアウト機能は、オートスケール用にタグ付けされたマシンにのみ適用されます?

動的セッションタイムアウト機能は、オートスケール用にタグ付けされているかどうかにかかわらず、デリバリーグループ内のすべてのマシンに適用されます。

動的セッションタイムアウトによりセッションがログオフされた場合、タグ付けされていないマシンも、タグ付けされたマシンのオートスケールターゲットに含まれます?

動的セッションタイムアウト機能は、オートスケールのタグ付け機能とは関係ありません。動的セッションタイムアウトによってセッションが終了した場合、マシンがシャットダウンされるまでドレインされていることを条件に、タグ付けされていないマシンもそのプロセス中にシャットダウンされる可能性があります。

タグ付けされたマシンのオートスケール (クラウドバースト)

> **注:**
>
> この機能は以前、Restrict Autoscale と呼ばれていました。

はじめに

Autoscaleは、デリバリーグループ内のマシンの一部のみを電源管理する柔軟性を提供します。これを実現するには、1つ以上のマシンにタグを適用し、その後、Autoscaleを構成してタグ付きマシンのみを電源管理します。

この機能は、クラウドベースのリソースが追加の需要（つまり、バーストワークロード）に対応する前に、オンプレミスリソース（または予約済みのパブリッククラウドインスタンス）を使用してワークロードを処理したいクラウドバーストのユースケースで役立ちます。オンプレミス環境のマシン（または予約済みインスタンス）に最初にワークロードを処理させるには、タグ制限とゾーン優先度を組み合わせて使用する必要があります。

タグ制限は、Autoscaleによって電源管理されるマシンを指定します。ゾーン優先度は、ユーザー起動要求を処理する優先ゾーン内のマシンを指定します。詳細については、「タグ」および「ゾーン優先度」を参照してください。

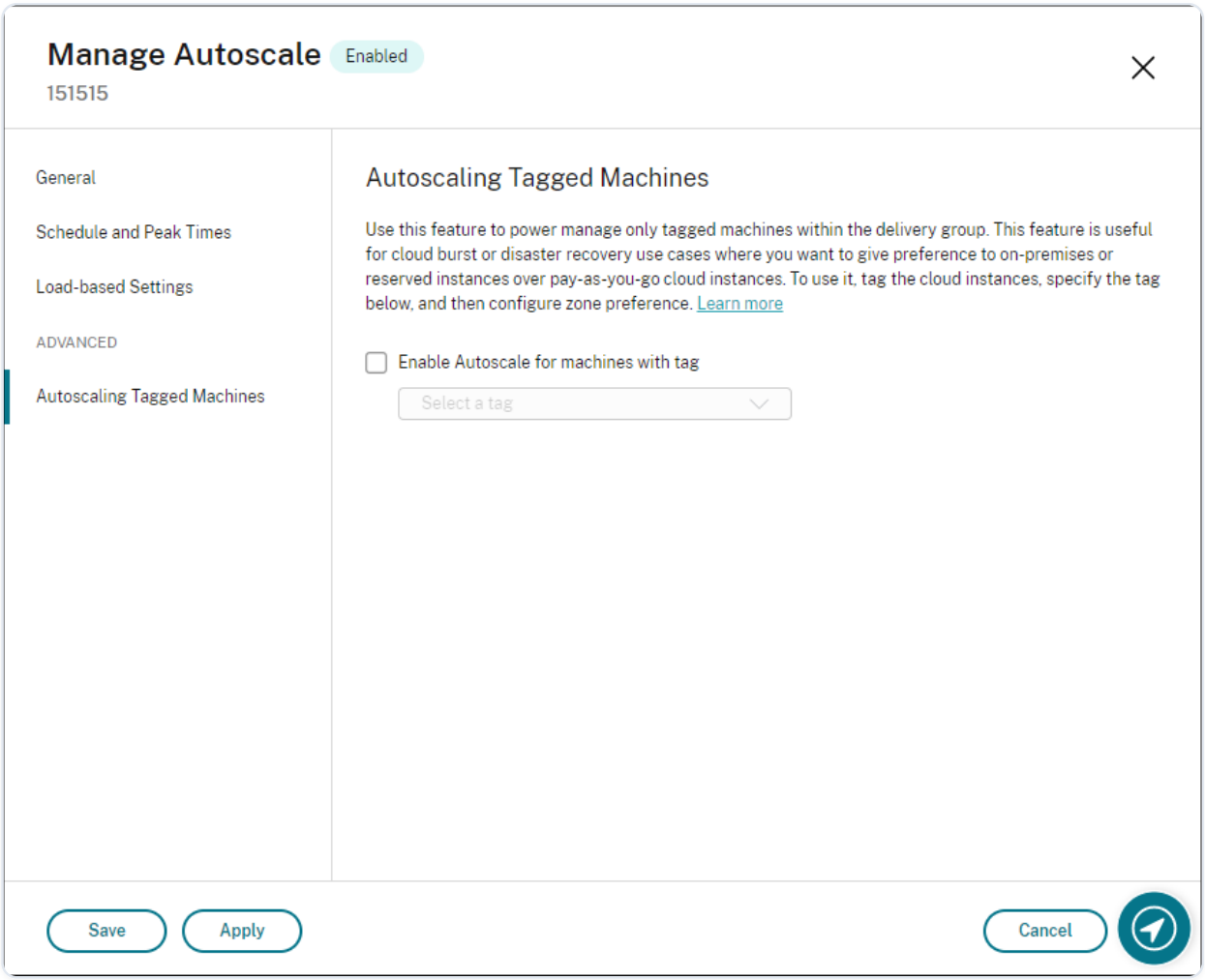
特定のタグ付きマシンをオートスケールするには、Manage コンソールまたは PowerShell を使用できます。

Manage コンソールを使用して特定のタグ付きマシンをオートスケールする

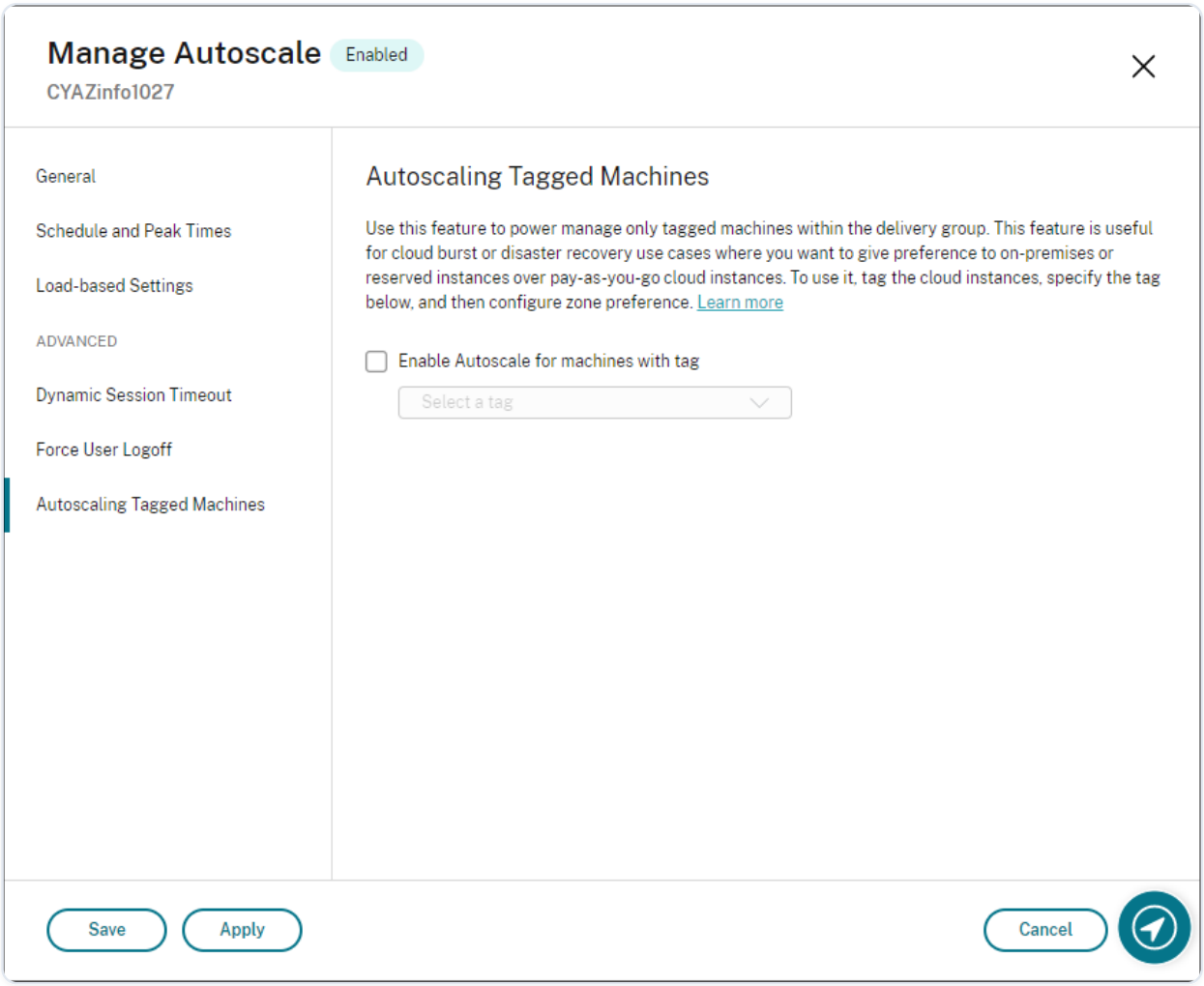
特定のタグ付きマシンをオートスケールするには、次の手順を実行します。

1. タグを作成し、そのタグをデリバリーグループ内の該当するマシンに適用します。詳細については、「タグとタグ制限の管理」を参照してください。
2. デリバリーグループを選択し、**Manage Autoscale** ウィザードを開きます。
3. **タグ付きマシンの自動スケーリング**ページで、**タグ付きマシンのAutoscaleを有効にする**を選択し、リストからタグを選択して、**適用**をクリックして変更を保存します。

   シングルセッションOSの*静的*および*ランダム*なデリバリーグループのユーザーインターフェイス:



マルチセッションOSデリバリーグループのユーザーインターフェイス:



警告:

- 特定のタグを持つマシンのAutoscaleにより、タグごとのマシンの数を反映するようにヒストグラムが自動的に更新される場合があります。**スケジュールとピーク時間**ページで、必要に応じて各時間帯にマシンを手動で割り当てることができます。
- タグ付きマシンで使用されているタグは削除できません。そのタグを削除するには、まずタグの制限を解除する必要があります。

タグの制限を適用した後、後でデリバリーグループからそれを削除したい場合があります。そのためには、**Autoscaleの管理 > タグ付きマシンのAutoscale**ページに移動し、**タグ付きマシンのAutoscaleを有効にする**のチェックを外します。

警告:

- **タグ付きマシンのAutoscaleを有効にする**のチェックを外さずに、該当するマシンからタグを削除すると、**Autoscaleの管理**ウィザードを開いたときに警告が表示される場合があります。マシンからタグを削除すると、Autoscaleで指定したタグが無効になるため、Autoscaleが管理するマシンがなくなる可能性があります。警告を解決するには、**タグ付きマシンのAutoscale**ページに移動し、無効なタグを削除して、**適用**をクリックして変更を保存します。

Autoscaleがリソースの電源をオンにするタイミングを制御する

タグ付けされていないマシンの使用状況に基づいて、Autoscaleがタグ付けされたマシンの電源をオンにし始めるタイミングを制御することもできます。これにより、タグ付けされたワークロードまたはパブリッククラウドワークロードの消費をさらに最適化できます。

これを行うには、次の手順を完了します。

1. **タグ付きマシンのAutoscale**ページで、**Autoscaleがタグ付きマシンの電源をオンにし始めるタイミングを制御する**を選択します。
2. ピーク時間とオフピーク時間の両方で到達したいタグなしマシンの使用率を入力し、**適用**をクリックします。サポートされる値: 0〜100。

Autoscaleがタグ付けされたマシンの電源をオンにし始めるタイミングを制御する(/en-us/citrix-virtual-apps-desktops/2407/media/autoscale-powers-on-tagged-machines.png)

ヒント:

このパーセンテージは、Autoscale がタグ付きマシンの電源をオンにし始めるタイミングを制御します。パーセンテージがしきい値 (デフォルトは 10%) を下回ると、Autoscale はタグ付きマシンの電源をオンにし始めます。パーセンテージがしきい値を超えると、Autoscale は電源オフモードになります。パーセンテージを入力する際は、次の 2 つのシナリオを考慮してください。

- シングルセッションOSデリバリーグループの場合: この値は、アイドル状態のタグなしマシンの総数に対する割合として定義されます。例: タグなしのシングルセッションOS

マシンが10台あるとします。セッションがないマシンが1台だけになった場合、Autoscale はタグ付きマシンの電源をオンにし始めます。

- マルチセッションOSデリバリーグループの場合: この値は、利用可能なタグなしマシンの総容量 (負荷インデックスの観点から) に対する割合として定義されます。例: タグなしのマルチセッションOSマシンが10台あるとします。それらが90%ロードされた場合、Autoscale はタグ付きマシンの電源をオンにし始めます。

PowerShell を使用して特定のタグ付きマシンを自動スケールする

PowerShell SDK を直接使用するには、次の手順を実行します。

1. **タグを作成します。** New-Brokertag PowerShell コマンドを使用してタグを作成します。
   - 例: `$managed = New-BrokerTag Managed`。この場合、タグは「Managed」という名前です。New-Brokertag PowerShell コマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/>` を参照してください。
2. **マシンにタグを適用します。** Get-Brokermachine PowerShell コマンドを使用して、Autoscale で電源管理するカタログ内のマシンにタグを適用します。
   - 例: `Get-BrokerMachine -CatalogName "cloud" | Add-BrokerTag $managed.Name`。この場合、カタログは「cloud」という名前です。
   - Get-Brokermachine PowerShell コマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/>` を参照してください。

注:

タグを適用した後で、新しいマシンをカタログに追加する場合があります。その場合、タグは新しいマシンに自動的に適用 *されません*。

3. **Autoscale で電源管理するデリバリーグループにタグ付きマシンを追加します。** Get-BrokerDesktopGroup PowerShell コマンドを使用して、マシンを含むデリバリーグループにタグ制限を追加します (つまり、「タグ X のマシンへの起動を制限する」)。

- 例: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`。この場合、デリバリーグループの UID は 1 です。
- Get-BrokerDesktopGroup PowerShell コマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>` を参照してください。

タグ制限を適用した後、後でデリバリーグループから削除したい場合があります。これを行うには、Get-BrokerDesktopGroup PowerShellコマンドを使用します。

例: `Get-BrokerDesktopGroup –Uid 1 | Set-BrokerDesktopGroup –RestrictAutoscaleTagUid $null`。この場合、デリバリーグループのUIDは1です。

> **注：**
>
> タグ付けされていないマシンは、ユーザーが電源をオフにすると自動的に再起動します。この動作により、ワークロードをより早く処理できるようになります。これは、`Set-BrokerDesktopGroup` の `AutomaticRestartForUntaggedMachines` プロパティを使用して、デスクトップグループごとに有効または無効にできます。詳しくは、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>` を参照してください。

例のシナリオ

次のシナリオを想定します。

- **マシンカタログ構成**。2つのマシンカタログ（C1とC2）があります。
  - カタログC1には、オンプレミス展開のローカルにある5台のマシン（M1～M5）が含まれています。
  - カタログC2には、クラウド展開のリモートにある5台のマシン（M6～M10）が含まれています。
- **タグ制限**。「Cloud」という名前のタグが作成され、カタログC2のM6～M10マシンに適用されます。
- **ゾーン構成**。2つのゾーン（Z1とZ2）が作成されます。
  - カタログC1を含むゾーンZ1は、オンプレミス展開に対応します。

  - カタログC2を含むゾーンZ2は、クラウド展開に対応します。

- **デリバリーグループ構成**
  - デリバリーグループには、10台のマシン（M1～M10）が含まれており、カタログC1から5台（M1～M5）、カタログC2から5台（M6～M10）です。
  - マシンM1からM5は手動で電源がオンにされ、スケジュール期間中ずっと電源がオンのままになります。
- **Autoscaleの構成**
  - 容量バッファは10%に設定されています。
  - Autoscaleは「Cloud」タグを持つマシンのみを電源管理します。この場合、Autoscaleはクラウドマシン M6からM10を電源管理します。
- **公開アプリケーションまたはデスクトップ構成**。公開デスクトップ（例）にはゾーン設定が構成されており、ユーザー起動要求ではゾーンZ2よりもゾーンZ1が優先されます。
  - ゾーンZ1は、公開デスクトップの優先ゾーン（ホームゾーン）として構成されています。

シナリオは次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. 利用可能なすべてのオンプレミス マシンが消費されるまで、ユーザーセッションはさらに増加します。
4. さらにユーザーセッションが開始されます。
5. セッション終了によりユーザーセッションが減少します。
6. セッション負荷がオンプレミス マシンのみで処理されるまで、ユーザーセッションはさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期状態）
  - オンプレミス マシン M1からM5はすべて電源がオンになっています。
  - クラウド内の1台のマシン（例: M6）の電源がオンになっています。このマシンは、構成されたキャパシティバッファのために電源がオンになっています。この場合、10（マシン数）x 10,000（負荷インデックス）x 10%（構成されたキャパシティバッファ）は10,000になります。したがって、1台のマシンの電源がオンになっています。

  - 電源がオンになっているすべてのマシン（M1からM6）の負荷インデックス値は、ベースライン負荷（負荷インデックスは0に等しい）にあります。

- ユーザーがログオンします
  - セッションは、構成されたゾーン設定を通じてM1からM5のマシンでホストされるように誘導され、これらのオンプレミス マシン間で負荷分散されます。
  - 電源がオンになっているマシン（M1からM5）の負荷インデックス値が増加します。
  - 電源がオンになっているマシンM6の負荷インデックス値はベースライン負荷にあります。
- ユーザーが負荷を増やし、すべてのオンプレミス リソースを消費します
  - セッションは、構成されたゾーン設定を通じてM1からM5のマシンでホストされるように誘導され、これらのオンプレミス マシン間で負荷分散されます。
  - 電源がオンになっているすべてのマシン（M1からM5）の負荷インデックス値は10,000に達しました。
  - 電源がオンになっているマシンM6の負荷インデックス値はベースライン負荷のままです。
- もう1人のユーザーがログオンします
  - セッションはゾーン設定を超過し、クラウド マシンM6でホストされるように誘導されます。
  - 電源がオンになっているすべてのマシン（M1からM5）の負荷インデックス値は10,000に達しました。
  - 電源がオンになっているマシンM6の負荷インデックス値が増加し、ベースライン負荷ではなくなります。負荷インデックスの観点から総予備容量が10,000を下回ると、Autoscaleは構成されたキャパシティバッファのために、需要を満たすために追加のマシン（M7）の電源をオンにし始めます。マシンM7の電源をオンにするには時間がかかる場合があることに注意してください。そのため、マシンM7が準備できるまでに遅延が発生する可能性があります。
- ユーザーがさらにログオンします。
  - セッションはマシンM6でホストされるように指示されます。
  - 起動中のすべてのマシン（M1～M5）のロードインデックス値が10,000に達しました。
  - 起動中のマシンM6のロードインデックス値はさらに増加しますが、総予備容量はロードインデックスの観点から10,000を超えるレベルにあります。
  - 起動中のマシンM7のロードインデックス値はベースライン負荷のままです。

- さらに多くのユーザーがログオンします。
  - マシンM7の準備ができた後、セッションはマシンM6とM7でホストされるように指示され、これらのマシン間で負荷分散されます。
  - 起動中のすべてのマシン（M1～M5）のロードインデックス値が10,000に達しました。
  - マシンM7のロードインデックス値はもはやベースライン負荷ではありません。
  - 起動中のマシン（M6とM7）のロードインデックス値が増加します。
  - 総予備容量は、ロードインデックスの観点から依然として10,000を超えるレベルにあります。
- セッション終了によりユーザーセッション負荷が減少します。
  - ユーザーがセッションからログオフするか、アイドルセッションがタイムアウトした後、マシンM1からM7で解放された容量は、他のユーザーが開始したセッションをホストするために再利用されます。
  - ロードインデックスの観点から総予備容量が10,000を超えるレベルに増加すると、Autoscaleはクラウドマシン（M6からM7）のいずれかをドレイン状態にします。その結果、新しい変更が発生しない限り、他のユーザーが開始したセッションはそのマシン（たとえばM7）に転送されなくなります。たとえば、ユーザー負荷が再び増加したり、他のクラウドマシンの負荷が最も低くなったりする場合です。
- 1つ以上のクラウドマシンが不要になるまで、ユーザーセッション負荷はさらに減少します。
  - マシンM7上のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、AutoscaleはマシンM7の電源をオフにします。
  - 電源がオンになっているすべてのマシン（M1～M5）のロードインデックス値は、10,000を下回るレベルまで低下する可能性があります。
  - 電源がオンになっているマシン（M6）のロードインデックス値は減少します。
- ユーザーセッションは、クラウドマシンが不要になるまでさらに減少します。
  - マシンM6にユーザーセッションがないにもかかわらず、予備容量として予約されているため、Autoscaleは電源をオフにしません。
  - 設定された容量バッファのため、Autoscaleは残りのクラウドマシンM6の電源をオンのままにします。そのマシンは、着信するユーザーにデスクトップを提供するのを待機しています。
  - オンプレミス環境のマシンに利用可能な容量がある限り、セッションはマシンM6でホストされるようには指示されません。

ユーザーログオフ通知（旧：ユーザーの強制ログオフ）

重要:

この機能は、マルチセッションアプリベースのデリバリーグループ向けのAutoscale™ユーザーインターフェイスでのみ利用可能です。

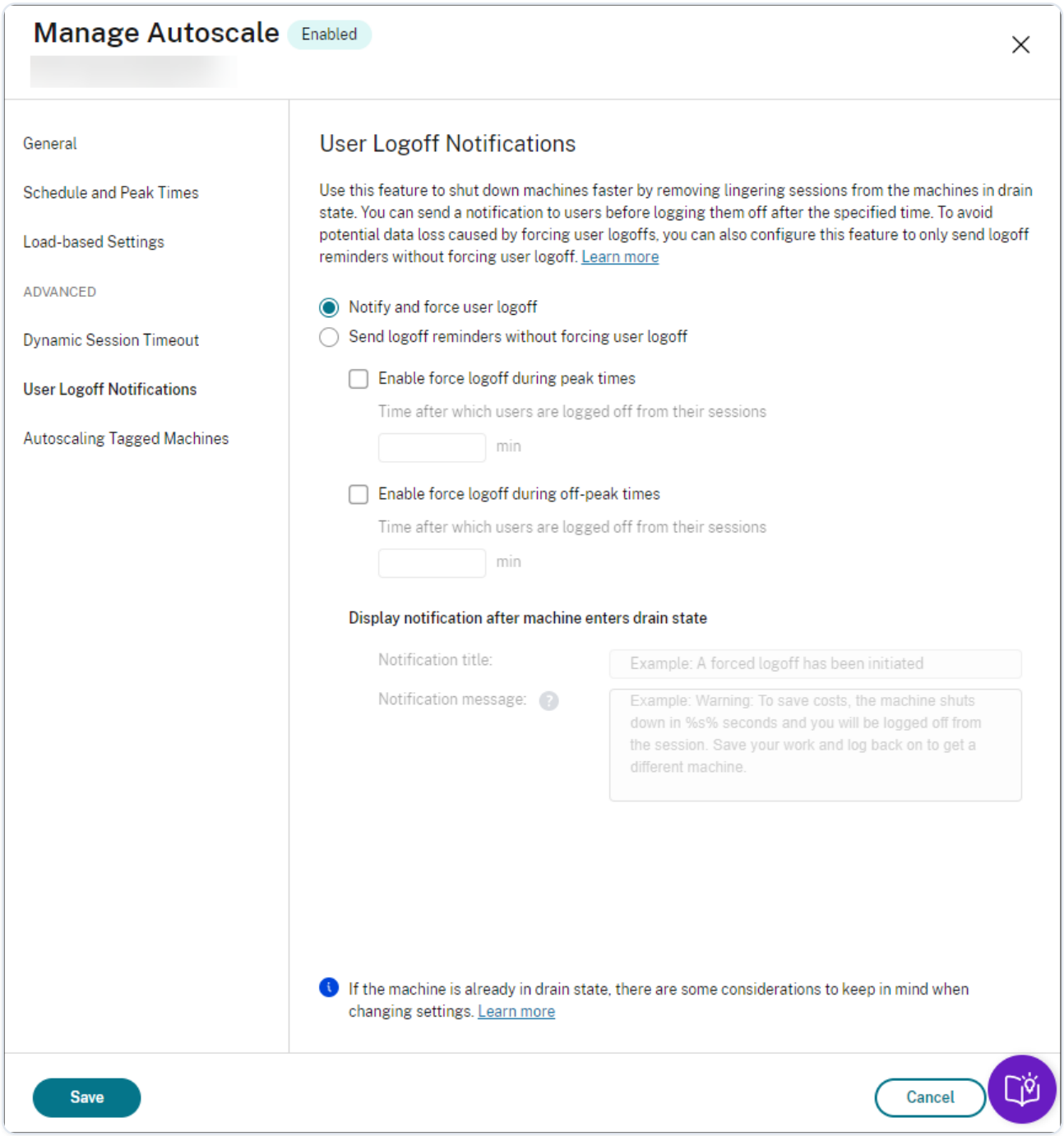
コスト削減をより効果的に実現するため、Autoscaleでは、残存セッションを強制的にログオフできます。これは、ユーザーにカスタム通知を送信し、セッションが強制的にログオフされるまでの猶予期間を指定することで行われます。これは、ドレイン状態のマシンに対してのみ行われ、すべての電源オンのマシンに対して行われるわけではありません。ユーザーの強制ログオフによって発生する可能性のあるデータ損失を回避するために、この機能をユーザーのログオフを強制することなくログオフリマインダーのみを送信するように構成することもできます。

以下の2つのオプションがあります。

- **通知してユーザーを強制ログオフ**
- **ユーザーのログオフを強制せずにログオフリマインダーを送信**

ユーザーに通知してログオフを強制する

選択した場合、Autoscaleは、以下で指定された時間が経過した後、ユーザーをセッションからログオフします。



ピーク時の強制ログオフを有効にする。選択した場合、Autoscaleは、指定された時間が経過したピーク時に、それらのユーザーをセッションからログオフします。

オフピーク時の強制ログオフを有効にする。選択した場合、Autoscaleは、指定された時間が経過したオフピーク時に、それらのユーザーをセッションからログオフします。

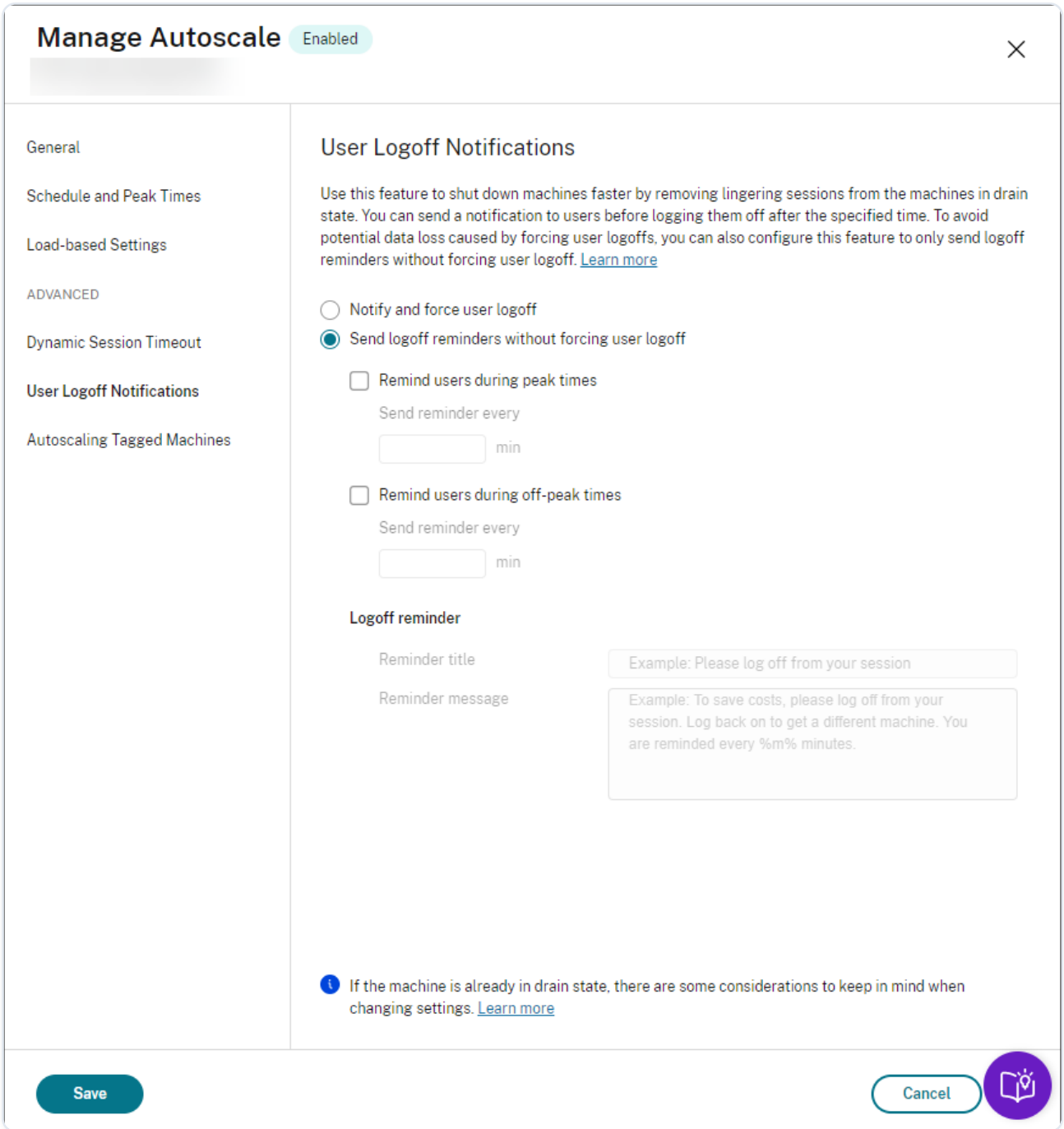
マシンがドレイン状態になった後に通知を表示する。マシンがドレイン状態になった後、ユーザーに通知を送信できます。

- **通知のタイトル。**ユーザーに送信する通知のタイトルを指定できます。例: `A forced logoff has been initiated.`.

- **通知メッセージ**。ユーザーに送信する通知の内容を指定できます。メッセージ内で指定された時間を示す変数として%s%または%m%を使用できます。時間を秒で表すには%s%を使用し、分で表すには%m%を使用します。例: `Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine.`.

ユーザーのログオフを強制せずにログオフリマインダーを送信する

選択した場合、マシンがドレイン状態に入った後、ユーザーはマシンからログオフするようリマインダーを受け取ります。このリマインダーは、以下で指定された間隔で送信されるように構成できます。



ピーク時にユーザーにリマインダーを送信する。選択した場合、ユーザーはピーク時にX分ごと（Xは指定された時間を示す）にセッションからログオフするようリマインダーを受け取ります。

オフピーク時にユーザーにリマインダーを送信する。選択した場合、ユーザーはオフピーク時にX分ごと（Xは指定された時間を示す）にセッションからログオフするようリマインダーを受け取ります。

ログオフリマインダー。マシンがドレイン状態に入った後にユーザーに送信されるリマインダーを構成できます。

- **リマインダーのタイトル。**ユーザーに送信されるリマインダーのタイトルを指定できます。例: `Please log off from your session`。
- **リマインダーメッセージ。**ユーザーに送信されるメッセージを指定できます。例: `Please log off from your session and log back on to save costs`。

考慮事項

マシンがすでにドレイン状態にある場合、設定を変更する際に、以下の点を考慮してください。

- 設定を**ユーザーのログオフを強制せずにログオフリマインダーを送信する**から**通知してユーザーのログオフを強制する**に変更した場合、新しい設定はすぐに有効になります。
- 設定を**通知してユーザーのログオフを強制する**から**ユーザーのログオフを強制せずにログオフリマインダーを送信する**に変更した場合、新しい設定は、マシンが次にドレイン状態に入るまで有効になりません。ユーザーは引き続きログオフを強制されます。

Broker PowerShell SDKコマンド

Broker PowerShell SDKを使用して、デリバリーグループのAutoscaleを構成できます。PowerShellコマンドを使用してAutoscaleを構成するには、PowerShell SDKバージョン7.21.0.12以降を使用する必要があります。PowerShell SDKの詳細については、「SDKとAPI」(/ja-jp/citrix-virtual-apps-desktops/2407/sdk-api.html)を参照してください。

Set-BrokerDesktopGroup

既存のBrokerDesktopGroupを無効または有効にするか、その設定を変更します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`を参照してください。

例

PowerShellコマンドレットの使用方法の詳細については、以下の例を参照してください。

Autoscale™を有効にする

- 名前が「MyDesktop」であるデリバリーグループの Autoscale を有効にするとします。`Set-BrokerDesktopGroup` PowerShell コマンドを使用します。例：
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -AutoscalingEnabled $true`

ピーク時とオフピーク時で容量バッファを個別に構成する

- 名前が「MyDesktop」であるデリバリーグループの容量バッファを、ピーク時は 20%、オフピーク時は 10% に設定するとします。`Set-BrokerDesktopGroup` PowerShell コマンドを使用します。例：
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakBufferSizePercent 20 -OffPeakBufferSizePercent 10`

when disconnected timeout 設定を構成する

- 名前が「MyDesktop」であるデリバリーグループの **when disconnected timeout** 値を、ピーク時は 60 分、オフピーク時は 30 分に設定するとします。`Set-BrokerDesktopGroup` PowerShell コマンドを使用します。例：
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakDisconnectTimeout 60 -OffPeakDisconnectTimeout 30`

「**ログオフタイムアウト**」設定を構成する

- 「MyDesktop」という名前のデリバリーグループについて、ピーク時の「**ログオフタイムアウト**」値を60分に、オフピーク時の値を30分に設定するとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例：
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakLogOffTimeout 60 -OffPeakLogOffTimeout 30`

電源オフ遅延設定を構成する

- 「MyDesktop」という名前のデリバリーグループについて、電源オフ遅延を15分に設定するとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例：
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PowerOffDelay 15`

電源オフ遅延が適用されない期間を構成する

- 「MyDesktop」という名前のデリバリーグループについて、電源オフ遅延が30分経過するまで適用されるようにするとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例：

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -SettlementPeriodBeforeAutoShutdown 30`。

マシンインスタンスコスト設定を構成する

- 「MyDesktop」という名前のデリバリーグループについて、1時間あたりのマシンインスタンスコストを0.2ドルに設定するとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例：
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -MachineCost 0.2`

New-BrokerPowerTimeScheme

デリバリーグループのBrokerPowerTimeSchemeを作成します。詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/>`を参照してください。

例

UID値が3のデリバリーグループに対して電源時間スキームを作成するとします。新しいスキームは週末、月曜日、火曜日を対象とします。午前8時から午後6時30分までの時間帯は、スキームに含まれる日のピーク時間として定義されます。ピーク時間の場合、プールサイズ（電源オン状態を維持するマシンの数）は20です。オフピーク時間の場合、プールサイズは5です。`Set-BrokerDesktopGroup` PowerShellコマンドを使用できます。例：

- `PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { 5 } else { 20 } } )`
- `PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { $false } else { $true } } )`
- `PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week' -DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48`

動的セッションタイムアウトのパラメーター

以下のBroker PowerShell SDKコマンドレットは、複数の新しいパラメーターをサポートすることで、動的セッションタイムアウト用に拡張されました。

- Get-BrokerDesktopGroup
- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

これらのパラメーターには以下が含まれます。

- **DisconnectPeakIdleSessionAfterSeconds** – ピーク時にアイドル状態のセッションが切断されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、ピーク時の関連動作が無効になっていることを示します。0より大きい値は、ピーク時のみデリバリーグループの動作を有効にします。
- **DisconnectOffPeakIdleSessionAfterSeconds** - オフピーク時間中にアイドル状態のセッションが切断されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、オフピーク中の関連動作が無効になっていることを示します。0より大きい値は、オフピーク時間中のみデリバリーグループの関連動作を有効にします。
- **LogoffPeakDisconnectedSessionAfterSeconds** - ピーク時間中に切断されたセッションが終了されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、ピーク時間中の関連動作が無効になっていることを示します。0より大きい値は、ピーク時間中のみデリバリーグループの関連動作を有効にします。
- **LogoffOffPeakDisconnectedSessionAfterSeconds** - オフピーク時間中に切断されたセッションが終了されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、オフピーク中の関連動作が無効になっていることを示します。0より大きい値は、オフピーク時間中のみデリバリーグループの関連動作を有効にします。

例

たとえば、「MyDesktop」という名前のデリバリーグループに対して、ピーク時のアイドルセッションタイムアウトを3,600秒に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -DisconnectOffPeakIdleSessionAfterSeconds 3600`

これにより、「MyDesktop」という名前のデスクトップグループの場合、オフピーク時に1時間以上アイドル状態だったセッションが切断されます。

シトリックス インサイト サービス

Citrix Insight Services (CIS)は、計測、テレメトリ、ビジネスインサイト生成のためのCitrixプラットフォームです。その計測およびテレメトリ機能により、技術ユーザー（顧客、パートナー、エンジニア）は問題を自己診断して修正し、環境を最適化できます。CISとその仕組みに関する詳細および最新情報については、`<https://cis.citrix.com>`を参照してください（Citrixアカウントの資格情報が必要です）。

Citrixにアップロードされるすべての情報は、トラブルシューティングと診断の目的、および製品の品質、信頼性、パフォーマンスの向上のために使用されます。ただし、以下に従います。

- `<https://cis.citrix.com/legal>`にあるCitrix Insight Servicesポリシー
- `<https://www.cloud.com/privacy-policy>`にあるCitrixプライバシーポリシー

このCitrix Virtual Apps and Desktops™リリースは、以下のテクノロジーをサポートしています。

- Citrix Virtual Apps and Desktopsのインストールとアップグレードの分析
- Citrix顧客エクスペリエンス向上プログラム (CEIP)
- シトリックス コールホーム
- シトリックス スカウト

CISおよびCitrix Analyticsとは別に、さらにGoogle Analyticsは、Studioをインストール（またはアップグレード）すると自動的に収集され（その後アップロードされます）。Studioのインストール後、レジストリキーHKLM\\Software\\Citrix\\DesktopStudio\\GAEnabledを使用してこの設定を変更できます。値が1の場合、収集とアップロードが有効になり、0の場合、収集とアップロードが無効になります。

インストールとアップグレードの分析

フルプロダクトインストーラーを使用してCitrix Virtual Apps and Desktopsコンポーネントを展開またはアップグレードすると、インストールプロセスに関する匿名情報が、コンポーネントをインストール/アップグレードしているマシンに収集され、保存されます。このデータは、Citrixが顧客のインストールエクスペリエンスを向上させるのに役立てられます。

この情報は、`%ProgramData%\Citrix\CTQs`にローカルに保存されます。

このデータの自動アップロードは、フルプロダクトインストーラーのグラフィカルインターフェイスとコマンドラインインターフェイスの両方で、デフォルトで有効になっています。

- レジストリ設定のデフォルト値を変更できます。インストール/アップグレード前にレジストリ設定を変更すると、フルプロダクトインストーラーを使用する際にその値が使用されます。
- コマンドラインインターフェイスでインストール/アップグレードする場合、コマンドでオプションを指定することで、デフォルト設定を上書きできます。

自動アップロードの制御:

- インストール/アップグレード分析の自動アップロードを制御するレジストリ設定 (デフォルト = 1):
  - 場所: `HKLM:\Software\Citrix\MetaInstall`
  - 名前: SendExperienceMetrics

  - 値: 0 = 無効、1 = 有効

- PowerShell を使用すると、次のコマンドレットでインストール/アップグレード分析の自動アップロードが無効になります:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
SendExperienceMetrics -PropertyType DWORD -Value 0
```

- XenDesktopServerSetup.exe または XenDesktopVDASetup.exe コマンドで自動アップロードを無効にするには、`/disableexperiencemetrics` オプションを含めます。

  XenDesktopServerSetup.exe または XenDesktopVDASetup.exe コマンドで自動アップロードを有効にするには、`/sendexperiencemetrics` オプションを含めます。

Citrix カスタマーエクスペリエンス向上プログラム

Citrixカスタマーエクスペリエンス向上プログラム (CEIP) に参加すると、匿名の統計情報と使用状況情報が Citrix に送信され、Citrix 製品の品質とパフォーマンスの向上に役立てられます。詳細については、https://more.citrix.com/XD-CEIP を参照してください。

サイト作成時またはアップグレード時の登録

サイトを作成すると (最初の Delivery Controller™ をインストールした後)、CEIP に自動的に登録されます。データの最初のアップロードは、サイト作成後約7日で行われます。

サイト作成後、いつでも参加を停止できます。Web Studio の左ペインで ノードを選択し、 設定 をオフにします。

Citrix Virtual Apps and Desktops 展開をアップグレードする場合:

- CEIP をサポートしていないバージョンからアップグレードする場合、参加するかどうかを尋ねられます。
- CEIPをサポートしていたバージョンからアップグレードし、参加が有効になっていた場合、アップグレードされたサイトでCEIPが有効になります。
- CEIPをサポートしていたバージョンからアップグレードし、参加が無効になっていた場合、アップグレードされたサイトでCEIPが無効になります。
- CEIPをサポートしていたバージョンからアップグレードし、参加状況が不明な場合、参加を希望するかどうか尋ねられます。

収集された情報は匿名であるため、Citrix Insight Servicesにアップロードされた後は閲覧できません。

VDAインストール時の登録

デフォルトでは、Windows VDAをインストールすると、CEIPに自動的に登録されます。このデフォルト設定はレジストリ設定で変更できます。VDAをインストールする前にレジストリ設定を変更した場合、その値が使用されます。

CEIPへの自動登録を制御するレジストリ設定（デフォルト = 1）：

場所: HKLM: \\Software\\Citrix\\Telemetry\\CEIP 名前: 有効 値: 0 = 無効, 1 = 有効

デフォルトでは、`Enabled`プロパティはレジストリに隠されています。指定されていない場合、自動アップロード機能は有効になります。

PowerShellを使用すると、次のコマンドレットでCEIPへの登録を無効にできます。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled
-PropertyType DWORD -Value 0
```

収集されたランタイムデータポイントは、定期的にファイルとして出力フォルダー（デフォルト%programdata%/Citrix/VdaCeip）に書き込まれます。

データの最初のアップロードは、VDAのインストール後約7日で行われます。

その他の製品およびコンポーネントのインストール時の登録

関連するCitrix製品、コンポーネント、テクノロジー（Citrix Provisioning™、AppDNA、Citrix License Server、Citrix Workspace™ app for Windows、Universal Print Server、Session Recordingなど）をインストールする際にも、CEIPに参加できます。インストールと参加のデフォルト値の詳細については、それぞれのドキュメントを参照してください。

シトリックス Call Home

Citrix Virtual Apps and Desktopsで特定のコンポーネントと機能をインストールすると、Citrix Call Homeへの参加を求められます。Call Homeは診断データを収集し、そのデータを含むテレメトリパッケージを分析とトラブルシューティングのためにCitrix Insight Servicesに直接（デフォルトポート443のHTTPS経由で）定期的にアップロードします。

Citrix Virtual Apps and Desktops では、Call Home は Citrix Telemetry Service という名前のバックグラウンドサービスとして実行されます。詳しくは、https://more.citrix.com/XD-CALLHOME を参照してください。

Call Homeのスケジュール機能はCitrix Scoutでも利用できます。詳細については、Citrix Scoutを参照してください。

収集される情報

Citrix Diagnostic Facility (CDF) トレースは、トラブルシューティングに役立つ情報をログに記録します。Call Homeは、VDA登録やアプリケーション/デスクトップの起動など、一般的な障害のトラブルシューティングに役立つCDFトレースのサブセットを収集します。このテクノロジーは、常時オンのトレース (AOT) として知られています。AOTログは、C:\Users\CitrixTelemetryService\Appdata\Local\CitrixAOTにディスクに保存されます。

Call Home は、その他の Event Tracing for Windows (ETW) 情報を収集せず、またそのように構成することもできません。

Call Home は、次のようなその他の情報も収集します。

- Citrix Virtual Apps and Desktopsによって`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`の下に作成されたレジストリ。
- Citrix名前空間下のWindows Management Instrumentation (WMI) 情報。
- 実行中のプロセスの一覧。
- %PROGRAM DATA%\\Citrix\\CDFに保存されているCitrixプロセスのクラッシュダンプ。
- インストールおよびアップグレード情報。これには、製品の完全なメタインストーラーログ、失敗したMSIログ、MSIログアナライザーからの出力、StoreFront™ログ、ライセンス互換性チェックログ、および予備的なサイトアップグレードテストの結果が含まれる場合があります。

トレース情報は収集時に圧縮されます。Citrix Telemetry Serviceは、最大10 MBの圧縮された最新のトレース情報を、最大8日間の期間で保持します。

- データを圧縮することで、Call Home は VDA 上で小さなフットプリントを維持できます。
- プロビジョニングされたマシンでの IOP を回避するため、トレースはメモリに保持されます。
- トレースバッファは、メモリ内のトレースを保持するために循環メカニズムを使用します。

Call Home は、Call Home の主要データポイント に記載されている主要なデータポイントを収集します。

構成と管理の概要

Call Home には、製品全体のインストールウィザードを使用するか、後で PowerShell コマンドレットを使用して登録できます。登録すると、デフォルトで診断情報が収集され、毎週日曜日の午前 3 時頃 (現地時間) に Citrix にアップロードされます。アップロードは、指定された時刻から 2 時間の間隔でランダム化されます。これは、デフォルトのスケジュールを使用するアップロードが午前 3 時から午前 5 時の間に発生することを意味します。

診断情報を定期的にアップロードしたくない場合 (またはスケジュールを変更したい場合) は、PowerShell コマンドレットを使用して診断情報を手動で収集してアップロードするか、ローカルに保存することができます。

スケジュールされた Call Home アップロードに登録する場合、および診断情報を手動で Citrix にアップロードする場合、Citrix アカウントまたは Citrix Cloud™ の資格情報を提供します。Citrix は、資格情報をアップロードトークンと交換し、このトークンは顧客を識別し、データをアップロードするために使用されます。資格情報は保存されません。

アップロードが発生すると、Citrix アカウントに関連付けられたアドレスに通知メールが送信されます。

コンポーネントのインストール時に Call Home を有効にした場合、後で無効にできます。

前提条件

- マシンで PowerShell 3.0 以降が実行されている必要があります。
- Citrix Telemetry Service がマシンで実行されている必要があります。
- システム変数 `PSModulePath` は、Telemetry のインストールパス (例: C:\\Program Files\\Citrix\\Telemetry Service\\.) に設定されている必要があります。

コンポーネントのインストール中に Call Home を有効にする

VDAのインストールまたはアップグレード中: フルプロダクトインストーラーのグラフィカルインターフェイスを使用してVirtual Delivery Agentをインストールまたはアップグレードする際、Call Homeへの参加を求められます。2つのオプションがあります。

- Call Home に参加する。
- Call Home に参加しない。

VDAをアップグレードしていて、以前にCall Homeに登録していた場合、そのウィザードページは表示されません。

Controllerのインストールまたはアップグレード中: グラフィカルインターフェイスを使用してDelivery Controllerをインストールまたはアップグレードする際、Call Homeへの参加を求められます。3つのオプションがあります。

Controllerをインストールしている場合、そのサーバーに「サービスとしてログオン」ポリシー設定が適用されたActive Directory GPOがある場合、インストールウィザードのCall Homeページで情報を構成することはできません。詳細については、CTX218094を参照してください。

Controllerをアップグレードしていて、以前にCall Homeに登録していた場合、参加について尋ねられることはありません。

PowerShellコマンドレット

PowerShellヘルプには、これらの一般的なユースケースでは使用されないコマンドレットとパラメーターの説明を含む、包括的な構文が記載されています。

アップロードにプロキシサーバーを使用するには、「プロキシサーバーを構成する」を参照してください。

- **スケジュールされたアップロードを有効にする:** 診断コレクションはCitrixに自動的にアップロードされます。カスタムスケジュール用の追加のコマンドレットを入力しない場合、デフォルトのスケジュールが使用されます。

  ```
  $cred = Get-Credential

  Enable-CitrixCallHome -Credential $cred
  ```

  スケジュールされたアップロードが有効になっていることを確認するには、`Get-CitrixCallHomeGet-CitrixCallHome`と入力します。有効になっている場合、戻り値は`IsEnabled=True`および`IsMasterImage=False`です。

- **マスターイメージから作成されたマシンに対するスケジュールされたアップロードを有効にする:** マスターイメージでスケジュールされたアップロードを有効にすると、マシンカタログで作成される各マシンを構成する必要がなくなります。

  `Enable-CitrixCallHome -Credential $cred -MasterImage`

  スケジュールされたアップロードが有効になっていることを確認するには、**Get-CitrixCallHome**と入力します。有効になっている場合、戻り値は`IsEnabled=True`および`IsMasterImage=True`です。

- **カスタムスケジュールを作成する:** 診断コレクションとアップロードの毎日または毎週のスケジュールを作成します。

  ```
  $timespan = New-TimeSpan –Hours hours -Minutes minutes

  Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek day
  -UploadFrequency {Daily|Weekly}
  ```

例:

次のコマンドレットは、毎晩22:20にデータをバンドルしてアップロードするスケジュールを作成します。Hoursパラメーターは24時間形式を使用します。`UploadFrequency`パラメーターの値がDailyの場合、`DayOfWeek`パラメーターは指定されていても無視されます。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

スケジュールを確認するには、`Get-CitrixCallHomeSchedule`と入力します。上記の例では、`StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily`が返されます。

次のコマンドレットは、毎週水曜日の夜10時20分にデータをバンドルしてアップロードするスケジュールを作成します。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed
-UploadFrequency Weekly
```

スケジュールを確認するには、`Get-CitrixCallHomeSchedule`と入力します。上記の例では、`StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly`が返されます。

Call Homeを無効にする

PowerShellコマンドレットを使用するか、Citrix Scoutを介してCall Homeを無効にできます。

Call Homeのスケジュールされたアップロードが無効になっている場合でも、AOTログは収集され、ディスクに保存されます。(スケジュールされたアップロードが無効になっている場合、AOTログはCitrixに自動的にアップロードされません。)AOTログの収集とローカルストレージを無効にできます。

PowerShellでCall Homeを無効にする

次のコマンドレットを実行すると、診断データはCitrixに自動的にアップロードされなくなります。(Citrix ScoutまたはテレメトリPowerShellコマンドレットを使用して、診断データをアップロードすることは引き続き可能です。)

`Disable-CitrixCallHome`

Call Homeが無効になっていることを確認するには、`Get-CitrixCallHome`と入力します。無効になっている場合、戻り値は`IsEnabled=False`と`IsMasterImage=False`です。

Citrix Scoutを使用して収集スケジュールを無効にする

Citrix Scoutを使用して診断収集スケジュールを無効にするには、コレクションのスケジュールのガイダンスに従ってください。ステップ3で、**オフ**をクリックして、選択したマシンのスケジュールをキャンセルします。

AOT ログの収集を無効にする

次の cmdlet を実行し、`Enabled` フィールドを `false` に設定すると、AOT ログは収集されなくなります。

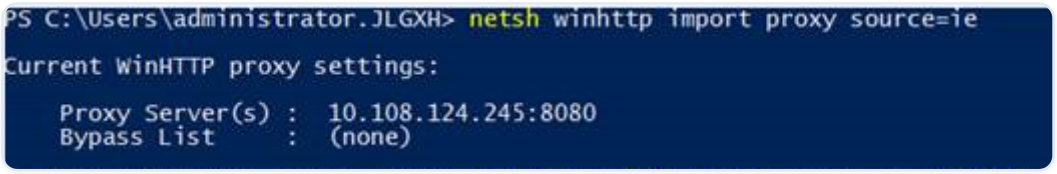
```
Enable-CitrixTrace -Listen'{"trace":{"enabled":false,"persistDirectory":"C:\Users\Public","maxSizeBytes":1000000, "sliceDurationSeconds":300}}'
```

`Listen` パラメーターには、JSON 形式の引数が含まれます。

Call Home のアップロード用プロキシサーバーを構成する

Call Home が有効になっているマシンで、次の作業を実行します。以下の手順の図では、例としてサーバーアドレスとポート 10.158.139.37:3128 を使用しています。実際の環境の情報は異なります。

1. ブラウザーにプロキシサーバーの情報を追加します。Internet Explorer で **インターネットオプション \> 接続 \> LAN の設定** を選択します。**LAN にプロキシサーバーを使用する** を選択し、プロキシサーバーのアドレスとポート番号を入力します。
2. PowerShell で `netsh winhttp import proxy source=ie` を実行します。



3. テキストエディターを使用して、C:\\Program Files\\Citrix\\Telemetry Service にある TelemetryService.exe の構成ファイルを編集します。赤い枠で示されている情報を追加します。



4. Telemetry Service を再起動します。

PowerShell で Call Home の cmdlet を実行します。

診断情報を手動で収集してアップロードする

CIS の Web サイトを使用して、診断情報のバンドルを CIS にアップロードできます。また、PowerShell cmdlet を使用して診断情報を収集し、CIS にアップロードすることもできます。

CIS Webサイトを使用してバンドルをアップロードするには：

1. Citrixアカウントの資格情報を使用してCitrix Insight Servicesにログオンします。
2. **My Workspace**を選択します。
3. **Healthcheck**を選択し、データの場所に移動します。

CISは、データアップロードを管理するいくつかのPowerShellコマンドレットをサポートしています。このドキュメントでは、2つの一般的なケースのコマンドレットについて説明します。

- `Start-CitrixCallHomeUpload`コマンドレットを使用して、診断情報バンドルを手動で収集し、CISにアップロードします。（バンドルはローカルに保存されません。）
- `Start-CitrixCallHomeUpload`コマンドレットを使用してデータを手動で収集し、診断情報バンドルをローカルに保存します。これにより、データをプレビューできます。後で、`Send-CitrixCallHomeBundle`コマンドレットを使用して、そのバンドルのコピーを手動でCISにアップロードします。（最初に保存したデータはローカルに残ります。）

PowerShellヘルプには、これらの一般的なユースケースでは使用されないコマンドレットとパラメーターの説明を含む、包括的な構文が記載されています。

CISにデータをアップロードするコマンドレットを入力すると、アップロードの確認を求められます。アップロードが完了する前にコマンドレットがタイムアウトした場合は、システムイベントログでアップロードのステータスを確認してください。サービスがすでにアップロードを実行している場合、アップロード要求は拒否される可能性があります。

データの収集とバンドルのCISへのアップロード:

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath string]
[-Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploadHeader string] [-AppendHeaders string] [-Collect string]
[<CommonParameters>]
```

データの収集とローカルへの保存:

```
Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
strings] [<CommonParameters>]
```

次のパラメーターが有効です。

- **Credential:** CISへのアップロードを指示します。
- **InputPath:** バンドルに含めるzipファイルの場所。これは、Citrixサポートが要求する追加ファイルである可能性があります。.zip拡張子を含めるようにしてください。
- **OutputPath:** 診断情報が保存される場所。このパラメーターは、Call Homeデータをローカルに保存する場合に必須です。
- **説明とインシデント時刻:** アップロードに関する自由形式の情報。
- **SR番号:** Citrixテクニカルサポートのインシデント番号。
- **名前:** バンドルを識別する名前。
- **UploadHeader:** CISにアップロードされるアップロードヘッダーを指定するJSON形式の文字列。
- **AppendHeaders:** CISにアップロードされる追加ヘッダーを指定するJSON形式の文字列。
- **Collect:** 収集または除外するデータを指定するJSON形式の文字列。形式は{'collector':{'enabled':Boolean}}で、Booleanはtrueまたはfalseです。 有効なコレクター値は次のとおりです。
    - 'WMI'

- 'プロセス'
- 'レジストリ
- 'クラッシュレポート'
- 'トレース'
- 'ファイル'
- 'MSI'
- 'ローカルデータ'
- 'サイトデータ'
- 「sfb」

既定では、「sfb」を除くすべてのコレクターが有効になっています。

'sfb' コレクターは、Skype for Business の問題を診断するためにオンデマンドで使用するように設計されています。「enabled」パラメーターに加えて、「sfb」コレクターはターゲットユーザーを指定するための「account」および「accounts」パラメーターをサポートしています。次のいずれかの形式を使用してください。

- "-収集 "{'sfb':{'account':'domain\\\user1'}}"
- "-収集 "{'sfb':{'accounts':}}"

- **共通パラメーター:** PowerShell のヘルプを参照してください。

以前にローカルに保存されたデータをアップロードする:

```
Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string
[<CommonParameters>]
```

`Path` パラメーターは、以前に保存されたバンドルの場所を指定します。

例:

次のコマンドレットは、Call Home データ（WMI コレクターからのデータを除く）を CIS にアップロードするよう要求します。このデータは、Citrix Provisioning VDA の登録失敗に関連するもので、Citrix Support ケース 123456 のために午後 2 時 30 分に記録されました。Call Home データに加えて、ファイル「c:\\Diagnostics\\ExtraData.zip」がアップロードされるバンドルに組み込まれます。

```
C:\PS\>Start-CitrixCallHomeUpload -InputPath "c:
\Diagnostics\ExtraData.zip" -Description "Registration failures with
Citrix Provisioning VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name
"RegistrationFailure-021812016" -Collect "{'wmi':{'enabled':false}}"
-UploadHeader "{'key1':'value1'}" -AppendHeaders "{'key2':'value2'}"
```

次のコマンドレットは、午前 8 時 15 分に記録された Citrix Support ケース 223344 に関連する Call Home データを保存します。データはネットワーク共有上のファイル mydata.zip に保存されます。Call Home データに加えて、ファイル「c:\\Diagnostics\\ExtraData.zip」が保存されるバンドルに組み込まれます。

```
C:\PS\>Start-CitrixCallHomeUpload -OutputPath \
\mynetwork\myshare\mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip"
-Description "Diagnostics for incident number 223344" -IncidentTime "8:15"
-SRNumber 223344
```

以下のコマンドレットは、以前に保存したデータバンドルをアップロードします。

```
$cred=Get-Credential

C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \
\mynetwork\myshare\mydata.zip
```

Citrix Scout (シトリックス スカウト)

はじめに

Citrix Scoutは、診断情報を収集し、ヘルスチェックを実行します。その結果を使用して、Citrix Virtual Apps and Desktops™展開を維持できます。Citrixは、Citrix Insight Servicesを通じて、診断情報収集の包括的かつ自動化された分析を提供します。また、Scoutを使用して、単独で、またはCitrixサポートのガイダンスを受けて問題をトラブルシューティングすることもできます。

収集ファイルをCitrixにアップロードして、Citrixサポートからの分析とガイダンスを受けることができます。または、収集したファイルをローカルに保存して自分で確認し、後でその収集ファイルをCitrixにアップロードして分析することもできます。

Scoutは次の手順を提供します。

- **収集:** サイトで選択したマシンに対して、1回限りの診断情報収集を実行します。その後、ファイルをCitrixにアップロードするか、ローカルに保存できます。

- **トレースと再現:** 選択したマシンで手動トレースを開始します。その後、それらのマシンで問題を再現します。問題を再現した後、トレースは停止されます。その後、Scoutは他の診断情報を収集し、ファイルをCitrixにアップロードするか、ローカルに保存します。
- **スケジュール:** 選択したマシンで、毎日または毎週指定した時刻に診断情報収集が実行されるようにスケジュールします。ファイルは自動的にCitrixにアップロードされます。
- **ヘルスチェック:** サイトとそのコンポーネントの正常性と可用性を測定するチェックを実行します。Delivery Controller、Virtual Delivery Agent (VDA)、StoreFront™サーバー、およびCitrix License Serverに対してヘルスチェックを実行できます。チェック中に問題が見つかった場合、Scoutは詳細なレポートを提供します。Scoutが起動するたびに、更新されたヘルスチェックスクリプトがないか確認します。新しいバージョンが利用可能な場合、Scoutはそれらを自動的にダウンロードし、次回のヘルスチェック実行時に使用します。

> **注:**
>
> **トレースと再現**、**スケジュール**、および**ヘルスチェック**の手順は、現在Linux VDAでは利用できません。

> この記事で説明されているグラフィカルインターフェイスは、Scoutを使用する主要な方法です。あるいは、PowerShellを使用して、1回限りの診断情報収集またはスケジュールされた診断情報収集とアップロードを構成することもできます。「Call Home」を参照してください。

Scoutの実行場所:

- オンプレミス展開では、Delivery Controller™からScoutを実行して、1つ以上のVirtual Delivery Agent (VDA)、Delivery Controller、StoreFrontサーバー、およびLicense Serverで診断情報を取得したり、チェックを実行したりできます。また、VDAからScoutを実行して、ローカル診断情報を収集することもできます。
- Citrix DaaS (旧称Citrix Virtual Apps and Desktopsサービス) を使用するCitrix Cloud環境では、VDAからScoutを実行してローカル診断情報を収集します。

Scout アプリケーションのログは `C:\ProgramData\Citrix\TelemetryService\ScoutUI.log` に保存されます。このファイルはトラブルシューティングに使用できます。

収集される情報

Scoutによって収集される診断情報には、Citrix Diagnostic Facility（CDF）トレースログファイルが含まれます。Always-on Tracing（AOT）と呼ばれるCDFトレースのサブセットも含まれます。AOT情報は、VDA登録やアプリケーション/デスクトップの起動などの一般的な問題のトラブルシューティングに役立ちます。その他のEvent Tracing for Windows（ETW）情報は収集されません。

収集される情報には以下が含まれます。

- `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`の下にあるCitrix Virtual Apps and Desktopsによって作成されたレジストリエントリ。
- **Citrix名前空間**の下にあるWindows Management Instrumentation (WMI) 情報。
- 実行中のプロセス。
- `%PROGRAMDATA%\Citrix\CDF`に保存されているCitrixプロセスのクラッシュダンプ。
- Citrixポリシー情報（CSV形式）。
- インストールおよびアップグレード情報。収集される情報には、製品の完全なメタインストーラーログ、失敗したMSIログ、MSIログアナライザーからの出力、StoreFrontログ、ライセンス互換性チェックログ、および予備的なサイトアップグレードテストの結果が含まれる場合があります。

トレース情報について：

- トレース情報は収集時に圧縮され、マシン上のフットプリントを小さく保ちます。
- 各マシンでは、Citrix Telemetry Serviceが圧縮された最新のトレース情報を最大8日間保持します。
- Citrix Virtual Apps and Desktops 7 1808以降、AOTトレースはデフォルトでローカルディスクに保存されます。（以前のバージョンでは、トレースはメモリに保持されていました。）デフォルトパス = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`。
- Citrix Virtual Apps and Desktops 7 1811以降、ネットワーク共有に保存されたAOTトレースは、他の診断情報とともに収集されます。
- `Enable-CitrixTrace` cmdletまたは`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen`レジストリ文字列を使用して、最大サイズ（デフォルト = 10 MB）とスライス期間を変更できます。
- トレースは、ファイルが`MaxSize`の10%に達するまでファイルに追加されます。

Scout が収集するデータポイントのリストについては、「Call Home の主要データポイント」を参照してください。

Scoutの構成

ScoutはLinux VDAで動作するように構成できます。Linux VDAとテレメトリの詳細については、「Citrix Telemetry Serviceとの統合」を参照してください。

Linux VDAは、`ctxtelemetry`ソケットポートまたはテレメトリサービス用のポートを自動的に変更する場合があります。その場合は、ポートを手動で構成する必要があります。

1. C:\Program Files\Citrix\Telemetry Serviceに移動します。
2. ScoutUI.exe.configファイルを開きます。
3. LinuxVDATelemetryServicePortまたはLinuxVDATelemetryWakeupPortの値を、Linux VDAで構成された値に変更します。

- `<add key="LinuxVDATelemetryServicePort" value="7502"/>`
- `<add key="LinuxVDATelemetryWakeupPort" value="7503"/>`

1. 変更を保存してファイルを閉じます。
2. 最新の構成が読み込まれていることを確認するために、Scout を再度開きます。

ヘルスチェックについて

ヘルスチェックデータは、`C:\ProgramData\Citrix\TelemetryService\`の下のフォルダーに保存されます。

サイト健全性チェック

サイト健全性チェックは、FlexCast Management Architecture (FMA) サービスの包括的な評価を提供する環境テストサービスに含まれています。サービス可用性の確認に加えて、これらのチェックは、データベース接続などの他の健全性指標も確認します。

サイト健全性チェックは、Delivery Controller で実行されます。サイトの規模によっては、これらのチェックの完了には最大1時間かかる場合があります。

DELIVERY CONTROLLER の構成チェック

サイト健全性チェックの一部として、Delivery Controller の構成チェックは、Virtual Apps and Desktops サイトに関するCitrixの推奨事項に基づき、以下の問題が存在するかどうかを確認します。

- 1 つ以上の Delivery Controller が失敗状態にある。
- サイトに Delivery Controller が 1 つしかない。
- Delivery Controller のバージョンが異なる。

健全性チェックの権限と要件を満たすことに加えて、Delivery Controller の構成チェックには以下が必要です。

- 少なくとも1つのControllerが電源オンになっていること。
- ControllerでBroker Serviceが実行されていること。
- Controllerからサイトデータベースへの動作可能な接続。

VDA健全性チェック

VDA健全性チェックは、一般的なVDA登録、セッション起動、およびタイムゾーンリダイレクトの問題の考えられる原因を特定します。

VDAでの登録について、Scoutは以下をチェックします。

- VDA ソフトウェアのインストール
- VDA マシンのドメインメンバーシップ
- VDA 通信ポートの可用性
- VDA サービスステータス
- Windows ファイアウォール構成
- Controller との通信
- Controller との時刻同期
- VDA 登録ステータス

VDA でのセッション起動について、Scout は以下をチェックします。

- セッション起動通信ポートの可用性
- セッション起動サービスのステータス
- セッション起動 Windows ファイアウォール構成
- VDA リモートデスクトップサービス クライアントアクセスライセンス
- VDA アプリケーション起動パス
- セッション起動レジストリ設定

VDAでのタイムゾーンリダイレクトについて、Scoutは以下をチェックします。

- Windows ホットフィックスのインストール
- Citrix ホットフィックスのインストール
- Microsoft グループポリシー設定

- Citrix グループポリシー設定

VDAでのProfile Managementについて、Scoutは以下をチェックします。

- ハイパーバイザーの検出
- プロビジョニングの検出
- シトリックス バーチャルアプリおよびデスクトップ
- Personal vDiskの構成
- ユーザーストア
- Profile Managementサービスのステータス検出
- Winlogon.exeフッキングテスト

Profile Managementでチェックを実行するには、VDAにProfile Managementをインストールして有効にする必要があります。Profile Managementの構成チェックの詳細については、Knowledge Centerの記事CTX132805を参照してください。

StoreFront のヘルスチェック

StoreFrontのチェックでは以下を確認します。

- Citrix Default Domainサービスが実行中であること
- Citrix Credential Walletサービスが実行中であること
- StoreFrontサーバーからActive Directoryポート88への接続
- StoreFrontサーバーからActive Directoryポート389への接続
- ベースURLが有効なFQDNを持っていること
- ベースURLから正しいIPアドレスが取得できること
- IISアプリケーションプールが.NET 4.0を使用していること
- 証明書がホストURLのSSLポートにバインドされているか
- 証明書チェーンが完全であるか
- 証明書の有効期限が切れているか
- 証明書の有効期限が間もなく切れるか（30日以内）

ライセンスサーバーのチェック

ライセンスサーバーのチェックでは、以下を確認します。

- Delivery Controllerからのライセンスサーバー接続
- ライセンスサーバーのファイアウォールリモートアクセスステータス

- Citrixライセンスサービスのステータス
- ライセンスサーバーのライセンスキャッシュモードの状態
- ライセンスサーバーのポート接続
- Citrixベンダーデーモン (CITRIX) が実行中かどうか
- システムクロックが同期されているかどうか
- Citrixライセンスサービスがローカルサービスアカウントで実行されているかどうか
- `CITRIX.opt` ファイルの存在
- Customer Success Servicesの資格取得日
- Citrixライセンスサーバーの更新
- ライセンスサーバーの証明書がDelivery Controllerの信頼されたルートストアにあるかどうか

ヘルスチェックの権限と要件を満たすことに加えて、ライセンスサーバーはドメインに参加している必要があります。そうでない場合、ライセンスサーバーは検出されません。

ヘルスチェックの実行

ヘルスチェックの手順は、マシンの選択、チェックの開始、および結果レポートの確認で構成されます。

1. Scoutを起動します。マシンの**スタート**メニューから、**Citrix > Citrix Scout**を選択します。開いたページで、**Health Check**をクリックします。
2. マシンを選択します。 をクリックしてマシンを検出します。 ページには、サイトで検出されたすべてのVDA、Delivery Controller、およびライセンスサーバーが一覧表示されます。マシン名で表示をフィルターできます。診断情報を収集する各マシンの横にあるチェックボックスをオンにして、 をクリックします。

   その他のコンポーネントタイプ（StoreFrontサーバーやVDAマシンなど）を追加するには、「Add machines manually」および「Import VDA machines」を参照してください。Citrix Provisioning™サーバーまたはライセンスサーバーを手動で追加することはできません。

   Scoutは、選択した各マシンで検証テストを自動的に起動し、「Verification tests」に記載されている基準を満たしていることを確認します。検証に失敗すると、 列にメッセージが表示され、そのマシンのチェックボックスがオフになります。次のいずれかを実行できます。

   - 問題を解決してから、そのマシンのチェックボックスをもう一度オンにします。これにより、検証テストが再試行されます。
   - そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンではヘルスチェックは実行されません。

検証テストが完了したら、 をクリックします。

3. 選択したマシンでヘルスチェックを実行します。概要には、テストが実行されるマシン（検証テストに合格した選択済みのマシン）が一覧表示されます。 をクリックします。

   チェック中およびチェック後：

   - 列には、マシンの現在のチェック状態が表示されます。
   - 進行中のすべてのチェックを停止するには、ページの右下隅にある をクリックします。（個々のマシンのヘルスチェックをキャンセルすることはできず、選択したすべてのマシンのみをキャンセルできます。チェックが完了したマシンからの情報は保持されます。）.
   - 選択したすべてのマシンのチェックが完了すると、右下隅にある ボタンが に変わります。
   - チェックが失敗した場合は、 列の をクリックできます。
   - チェックが問題なく完了した場合、 列は空になります。
   - チェックで問題が見つかった場合は、 をクリックして結果を表示します。
   - 選択したすべてのマシンのチェックが完了したら、 をクリックしないでください。（クリックすると、チェック結果が失われます。）

4. チェックが完了したら、**完了**をクリックしてScoutの開始ページに戻ります。

ヘルスチェックの結果

レポートを生成するCitrixチェックの場合、レポートには以下が含まれます。

- 結果レポートが生成された日時
- チェックされたマシン
- チェックが対象マシンで探した条件

権限と要件

権限:

- 診断情報を収集するには:
  - 診断情報を収集する各マシンで、ローカル管理者およびドメインユーザーである必要があります。
  - 各マシン上のLocalAppDataディレクトリに書き込む権限が必要です。
- ヘルスチェックを実行するには:
  - ドメインユーザーグループのメンバーである必要があります。

    - フル管理者であるか、サイトに対する読み取り専用および**環境テストの実行**権限を持つカスタムロールを持っている必要があります。
    - スクリプトの実行を許可するには、スクリプト実行ポリシーを少なくとも`RemoteSigned`に設定します。例: `Set-ExecutionPolicy RemoteSigned`。**注:** 他のスクリプト実行権限でも機能する場合があります。

- Scout を起動する際は、**管理者として実行**を使用してください。

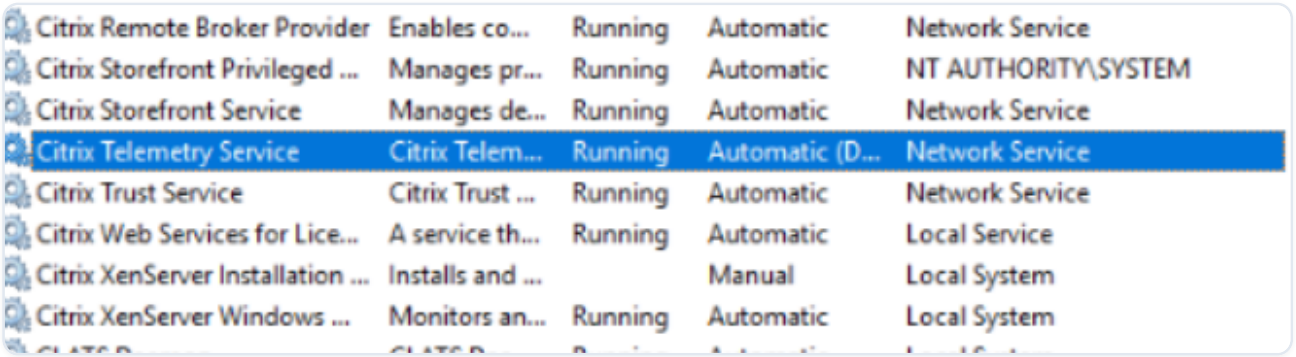
診断情報を収集したり、ヘルスチェックを実行したりする各マシンについて：

- Scout がそのマシンと通信できる必要があります。
- ファイルとプリンターの共有が有効になっている必要があります。
- PSRemoting と WinRM が有効になっている必要があります。また、そのマシンでは PowerShell 3.0 以降が実行されている必要があります。
- Citrix テレメトリサービスがそのマシンで実行されている必要があります。
- Windows Management Infrastructure (WMI) アクセスがそのマシンで有効になっている必要があります。
- 診断情報収集のスケジュールを設定するには、そのマシンで互換性のある Scout バージョンが実行されている必要があります。

パス名で指定されたユーザー名にドル記号 ($) を使用しないでください。これにより、診断情報の収集が妨げられます。

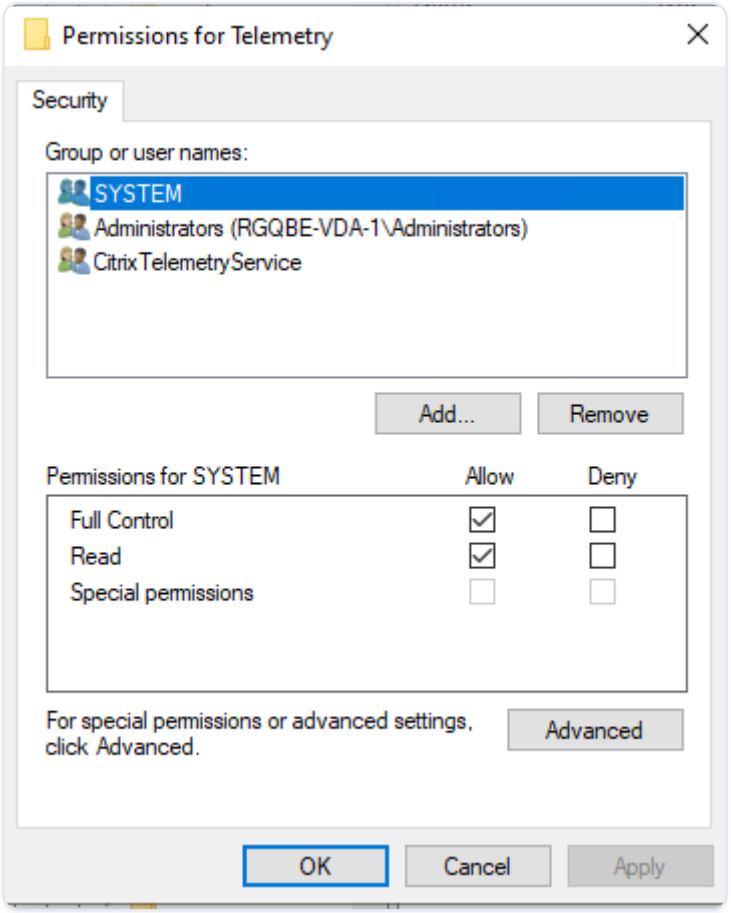
Scout は、選択したマシンで検証テストを実行し、これらの要件が満たされていることを確認します。

Windows 用テレメトリサービスはネットワークサービスで実行されます。

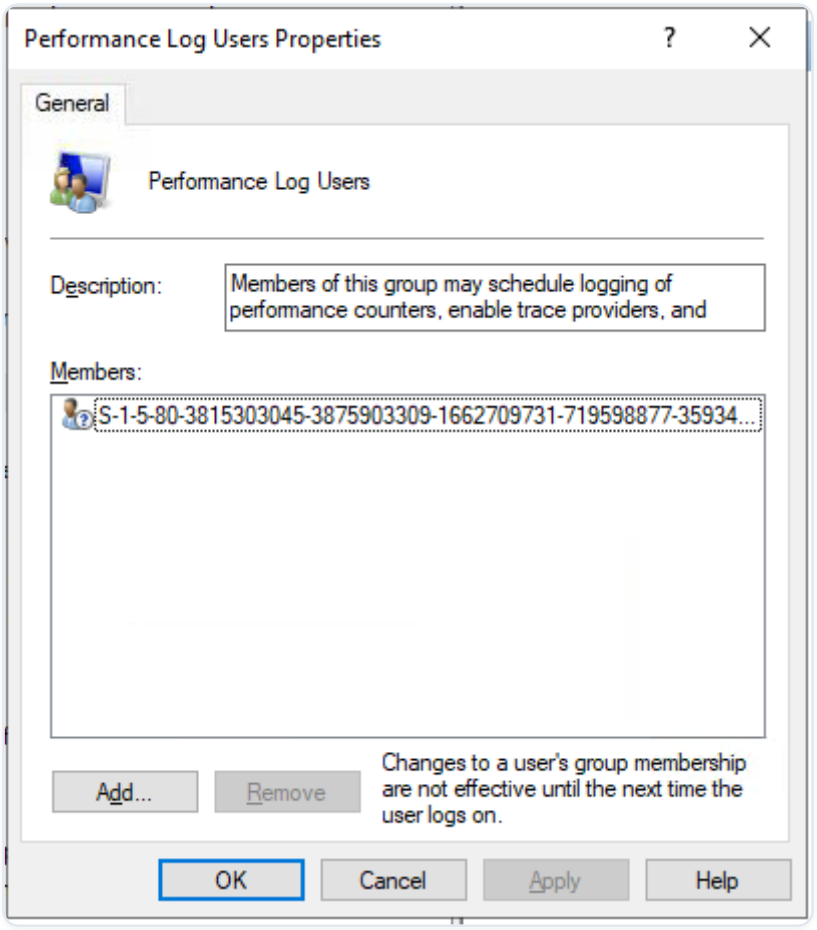


AOT トレースフォルダーは`C:\ProgramData\Citrix\TelemetryService\CitrixAOT`に保存されます。

管理者グループ、System、およびテレメトリサービス SID のユーザーのみが `HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry` レジストリにアクセスする権限を持っています。



Telemetry Serviceをアンインストールした後も、Telemetry Service SIDはPerformance Log Users グループに残りますが、手動で削除できます。



検証テスト

診断情報の収集またはヘルスチェックが開始される前に、選択された各マシンに対して検証テストが自動的に実行されます。これらのテストは、要件が満たされていることを確認します。マシンのテストが失敗した場合、Scout は推奨される是正措置を含むメッセージを表示します。

- **Scout がこのマシンに到達できません** - 以下を確認してください。
  - マシンの電源がオンになっていること。
  - ネットワーク接続が正常に機能していること。（これには、ファイアウォールが適切に構成されていることの確認も含まれます。）
  - ファイルとプリンターの共有がオンになっていること。手順については、Microsoft のドキュメントを参照してください。
- **PSRemoting と WinRM を有効にする** - PowerShell リモート処理と WinRM を同時に有効にできます。**管理者として実行**を使用して、`Enable-PSRemoting` コマンドレットを実行します。詳細については、コマンドレットに関する Microsoft のヘルプを参照してください。
- **Scout には PowerShell 3.0 (最小) が必要です** - マシンに PowerShell 3.0 (またはそれ以降) をインストールし、PowerShell リモート処理を有効にしてください。

- **このマシン上の LocalAppData ディレクトリにアクセスできません** - アカウントがマシンの LocalAppData ディレクトリへの書き込み権限を持っていることを確認してください。
- **Citrix Telemetry Service を見つけられません** - Citrix Telemetry Service がマシンにインストールされ、開始されていることを確認してください。
- **スケジュールを取得できません** - マシンを (最小で) XenApp および XenDesktop 7.14 にアップグレードしてください。
- **WMI がマシンで実行されていません** - Windows Management Instrumentation (WMI) アクセスが有効になっていることを確認してください。
- **WMI 接続がブロックされています** - Windows ファイアウォールサービスで WMI を有効にしてください。
- **Citrix Telemetry Serviceの新しいバージョンが必要です** - (バージョンは、CollectおよびTrace & Reproduceに対してのみチェックされます。) マシン上のTelemetry Serviceのバージョンをアップグレードしてください (インストールとアップグレードを参照)。サービスをアップグレードしない場合、そのマシンは**Collect**または**Trace & Reproduce**アクションに含まれません。
- **Scoutがこのマシン上のsystemdソケットに接続できません** - 以下を確認してください。
  - ポート7503が開いていること。`systemd ctxtelemetry.socket`がマシン上のポート7503でリッスンしていることを確認してください。`ctxtelemetry.socket`ポートが変更されている場合、ポートが異なる可能性があります。ポートを調整するには、Scoutの構成を参照してください。
  - ネットワーク接続が正常に機能していること。(これには、ファイアウォールが適切に構成されていることの確認が含まれる場合があります。)
- **このマシンでLinux VDA Telemetry Serviceが開始されていません** - 以下を確認してください。
  - ポート7502が開いていること。Linux VDA Telemetry Serviceがマシンにインストールされ、開始されていることを確認してください。テレメトリサービスポートが変更されている場合、ポートが異なる可能性があります。ポートを調整するには、Scoutの構成を参照してください。
  - ネットワーク接続が正常に機能していること。(これには、ファイアウォールが適切に構成されていることの確認が含まれる場合があります。)

バージョン互換性

このバージョンのScout (3.x) は、Citrix Virtual Apps and Desktops (または最低でもXenApp and XenDesktop 7.14) のコントローラーおよびVDAで実行することを目的としています。

Scoutの以前のバージョンは、XenApp and XenDesktop 7.14より前のバージョンで提供されています。その以前のバージョンについては、CTX130147を参照してください。

7.14 より前の Controller または VDA をバージョン 7.14 (またはそれ以降のサポートされているバージョン) にアップグレードすると、以前のバージョンの Scout は現在のバージョンに置き換えられます。

| 機能 | スカウト 2.23 | スカウト 3.0 | --- | --- | ---| -- | Citrix Virtual Apps and Desktops (および XenApp and XenDesktop 7.14〜7.18) をサポート | はい | はい XenDesktop 5.x、7.1〜7.13をサポート | はい | いいえ XenApp 6.x、7.5〜7.13をサポート | はい | いいえ 製品に同梱 | 7.1〜7.13 | 7.14以降 CTX記事からダウンロード可能 | はい | いいえ CDFトレースをキャプチャ | はい | はい Always-on-Traces (AOT) をキャプチャ | いいえ | はい 診断データの収集を許可 | 一度に最大10台のマシン（デフォルト） | 無制限（リソースの可用性による） 診断データをCitrixに送信することを許可 | はい | はい 診断データをローカルに保存することを許可 | はい | はい Citrix Cloud™資格情報をサポート | いいえ | はい Citrix資格情報をサポート | はい | はい アップロード用のプロキシサーバーをサポート | はい | はい スケジュールを調整 | 該当なし | はい スクリプトのサポート | コマンドライン（ローカルControllerのみ） | Call Homeコマンドレットを使用するPowerShell（Telemetry Serviceがインストールされている任意のコンピューター） ヘルスチェック | いいえ | はい データマスキング | いいえ | 3.17以降

インストールとアップグレード

デフォルトでは、VDAまたはControllerをインストールまたはアップグレードする際に、Citrix Telemetry Serviceの一部としてScoutが自動的にインストールまたはアップグレードされます。

VDAのインストール時にCitrix Telemetry Serviceを省略した場合、または後でサービスを削除した場合は、Citrix Virtual Apps and Desktopsインストールメディアの`x64\Virtual Desktop Components`または`x86\Virtual Desktop Components`フォルダーから`TelemetryServiceInstaller_xx.msi`を実行します。

Collectまたは**Trace & Reproduce**アクションを選択すると、マシンで古いバージョンのCitrix Telemetry Serviceが実行されている場合に通知されます。Citrixでは、サポートされている最新バージョンを使用することをお勧めします。そのマシンでTelemetry Serviceをアップグレードしない場合、そのマシンは**Collect**または**Trace & Reproduce**アクションに含まれません。Telemetry Serviceをアップグレードするには、インストールと同じ手順を使用します。

アップロードの承認

診断コレクションをCitrixにアップロードする予定がある場合は、CitrixアカウントまたはCitrix Cloudアカウントが必要です。（これらは、Citrixダウンロードにアクセスしたり、Citrix Cloud

Control Centerにアクセスしたりするために使用する資格情報です。）アカウント資格情報が検証されると、トークンが発行されます。

CitrixアカウントまたはCitrix Cloudアカウントで認証する場合は、リンクをクリックして、デフォルトのブラウザーでHTTPSを使用してCitrix Cloudにアクセスします。Citrix Cloudの資格情報を入力すると、トークンが表示されます。トークンをコピーしてScoutに貼り付けます。その後、Scoutウィザードを続行できます。

トークンは、Scoutを実行しているマシンにローカルに保存されます。次回**Collect**または**Trace & Reproduce**を実行するときにそのトークンを使用できるようにするには、**Store token and skip this step in the future**チェックボックスをオンにします。

Scoutの開始ページで**Schedule**を選択するたびに、再承認する必要があります。スケジュールを作成または変更する際に、保存されたトークンを使用することはできません。

アップロードにプロキシを使用する

プロキシサーバーを使用してCitrixにコレクションをアップロードしたい場合は、Scoutにブラウザのインターネットプロパティで設定されたプロキシ設定を使用するように指示できます。あるいは、プロキシサーバーのIPアドレスとポート番号を指定することもできます。

マシンの検索

収集、**トレースと再現**、**スケジュール**の手順では、Scoutは自動的に検出したコントローラーとVDAを一覧表示します。

Delivery ControllerからScout Health Checkを実行するときは、**マシンの検索**をクリックして、デリバリーコントローラー、VDA、ライセンスサーバー、StoreFrontサーバーなどのマシンを検出します。

ドメインに参加しているがDelivery ControllerではないマシンからScout Health Checkを実行すると、Scoutはマシンを自動的に検出できません。手動でマシンを追加するか、VDAマシンをインポートする必要があります。

マシンを手動で追加する

Scout が検出したコントローラーと VDA を一覧表示した後、StoreFront サーバー、ライセンスサーバー、Citrix Provisioning サーバーなど、展開内の他のマシンを手動で追加できます。

ヘルスチェック の実行時：

- ドメイン内のCitrixライセンスサーバーは自動的に検出されます。ライセンスサーバーを手動で追加することはできません。

- ヘルスチェックは現在、Citrix Provisioningサーバーをサポートしていません。

検出されたマシンを一覧表示するScoutの任意のページで、**+ マシンの追加**をクリックします。追加するマシンのFQDNを入力し、**続行**をクリックします。必要に応じて、他のマシンを追加するために繰り返します。（FQDNの代わりにDNSエイリアスを入力しても有効に見えることがありますが、ヘルスチェックが失敗する可能性があります。）

手動で追加されたマシンは、常に検出されたマシンよりも上の、マシンリストの先頭に表示されます。

手動で追加されたマシンを識別する簡単な方法は、行の右端にある赤い削除ボタンです。そのボタンがあるのは手動で追加されたマシンのみです。検出されたマシンにはありません。

手動で追加されたマシンを削除するには、行の右端にある赤いボタンをクリックします。削除を確認します。他の手動で追加されたマシンを削除するために繰り返します。

Scout は、手動で追加されたマシンを削除するまで記憶しています。Scout を閉じてから再度開くと、手動で追加されたマシンは引き続きリストの先頭に表示されます。

StoreFront サーバーで **Trace & Reproduce** を使用する場合、CDF トレースは収集されません。ただし、その他のすべてのトレース情報は収集されます。

VDA マシンをインポートする

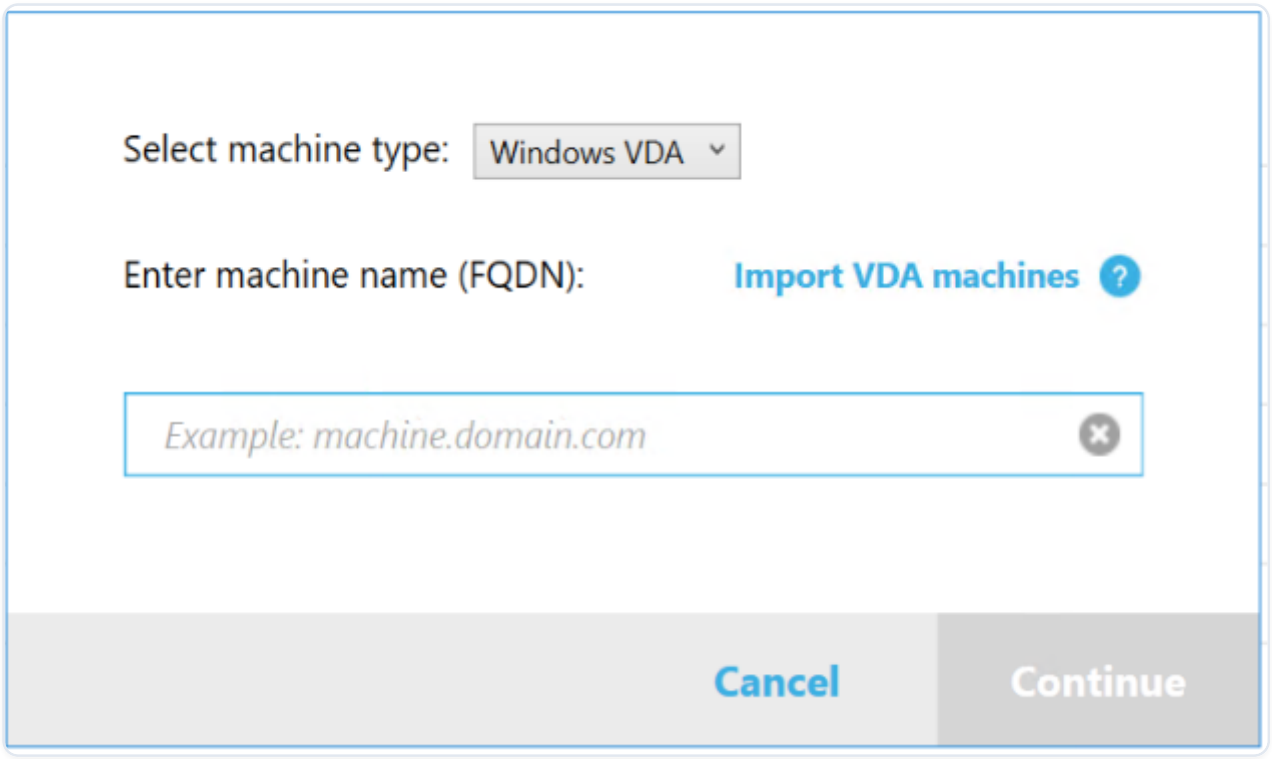
ヘルスチェックを実行する際に、展開にVDAマシンをインポートできます。

1. Delivery ControllerまたはConnectorで、PowerShellコマンドを使用してマシンリストファイルを生成します。Connectorでは、Citrixの資格情報を入力し、ポップアップダイアログで顧客を選択する必要があります。

   ```
   Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList.txt
   ```

2. machineList.txtファイルを、Scout Health Checkを起動するドメイン参加済みマシンにコピーします。
3. Scout Health Check ページで、 をクリックします。
4. マシンタイプを選択します。
5. をクリックします。
6. machineList.txt ファイルを選択します。
7. をクリックします。

インポートされたVDAマシンは、Scout Health Checkページに表示されます。



診断情報の収集

収集手順は、マシンの選択、診断情報の収集の開始、その後、収集情報を含むファイルをCitrixにアップロードするか、ローカルに保存することから構成されます。

1. Scout を起動します。マシンの**スタート**メニューから、**Citrix > Citrix Scout** を選択します。開いたページで、**収集**をクリックします。
2. マシンを選択します。

   - コントローラーでは、**マシンの選択**ページにサイト内のすべての VDA とコントローラーが一覧表示されます。マシン名で表示をフィルターできます。他のマシン (StoreFront や Citrix Provisioning サーバーなど) を手動で追加するには、「マシンの手動追加」を参照してください。
   - その他のコンポーネント (VDA サーバーなど) では、**マシンの選択**ページにローカルマシンのみが表示されます。マシンの手動追加はサポートされていません。

   診断情報を収集する各マシンの横にあるチェックボックスをオンにしてから、**続行**をクリックします。

   Scout は、選択された各マシンで検証テストを自動的に起動し、「検証テスト」に記載されている基準を満たしていることを確認します。検証に失敗した場合、**ステータス**列にメッセージが表示され、そのマシンのチェックボックスはオフになります。次のいずれかを実行できます。

- 問題を解決してから、そのマシンのチェックボックスを再度オンにします。これにより、検証テストが再試行されます。
- そのマシンをスキップします (チェックボックスをオフのままにします)。そのマシンからは診断情報は収集されません。

検証テストが完了したら、**続行**をクリックします。

3. 診断情報を収集します。概要には、診断情報が収集されるすべてのマシン (検証テストに合格した選択済みのマシン) が一覧表示されます。**収集開始**をクリックします。

   収集中:

   - **ステータス**列には、マシンの現在の収集状態が表示されます。
   - 単一マシンでの進行中の収集を停止するには、そのマシンの**アクション**列にある**キャンセル**をクリックします。
   - すべての進行中の収集を停止するには、ページ右下隅にある**収集停止**をクリックします。収集が完了したマシンからの診断情報は保持されます。収集を再開するには、各マシンの**アクション**列にある**再試行**をクリックします。
   - 選択されたすべてのマシンの収集が完了すると、右下隅にある**収集停止**ボタンが**続行**に変わります。
   - 診断を再度収集するには、そのマシンの 列にある をクリックします。新しい収集が以前の収集を上書きします。
   - 収集が失敗した場合は、 列にある をクリックできます。正常に収集されたもののみがアップロードまたは保存されます。
   - 選択したすべてのマシンで収集が完了したら、 をクリックしないでください。（クリックすると、収集は失われます。）

   収集が完了したら、 をクリックします。

4. 収集を保存またはアップロードします。ファイルをCitrixにアップロードするか、ローカルマシンに保存するかを選択します。

   今すぐファイルをアップロードする場合は、手順5に進みます。

   ファイルをローカルに保存する場合：

   - Windowsの ダイアログボックスが表示されます。目的の場所に移動します。
   - ローカル保存が完了すると、ファイルのパス名が表示され、リンクされます。ファイルを表示できます。後でファイルをCitrixにアップロードできます。CTX136396を参照してください。

をクリックしてScoutの開始ページに戻ります。この手順でこれ以上ステップを完了する必要はありません。

5. アップロードの認証を行い、必要に応じてプロキシを指定します。詳細については、(#upload-authorization)を参照してください。

   - Scoutを通じて認証していない場合は、この手順に進みます。
   - Scoutを通じて認証済みの場合、保存されている認証トークンがデフォルトで使用されます。この操作を行う場合は、このオプションを選択して をクリックします。この収集では資格情報の入力を求められません。手順6に進みます。
   - 以前に認証済みで、再認証して新しいトークンを取得したい場合は、 をクリックしてこの手順に進みます。

   アップロードを認証するためにCitrix資格情報を使用するか、Citrix Cloud資格情報を使用するかを選択します。 をクリックします。資格情報ページは、保存されたトークンを使用していない場合にのみ表示されます。

   資格情報ページで:

   - ファイルアップロードにプロキシサーバーを使用する場合は、**プロキシの構成**をクリックします。Scoutに、ブラウザのインターネットプロパティ用に構成されたプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
   - Citrix Cloudアカウントの場合は、**トークンを生成**をクリックします。デフォルトのブラウザがCitrix Cloudページに起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
   - Citrixアカウントの場合は、資格情報を入力します。

   完了したら、**続行**をクリックします。

6. アップロードに関する情報を入力します。

   - 名前フィールドには、収集された診断ファイルのデフォルト名が含まれています。ほとんどのコレクションではこれで十分ですが、名前を変更することもできます。(デフォルト名を削除して名前フィールドを空のままにした場合、デフォルト名が使用されます。)
   - オプションで、8桁のCitrixサポートケース番号を指定します。
   - オプションの**説明**フィールドに、問題について説明し、該当する場合は問題が発生した時期を示します。

   完了したら、**アップロードを開始**をクリックします。

アップロード中、ページの左下部分にアップロードの完了パーセンテージの概算が表示されます。進行中のアップロードをキャンセルするには、**アップロードを停止**をクリックします。

アップロードが完了すると、その場所のURLが表示され、リンクされます。リンクをたどってCitrixの場所に移動し、アップロードの分析を表示したり、リンクをコピーしたりできます。

完了をクリックしてScoutの開始ページに戻ります。

トレースと再現

トレースと再現の手順は、マシンの選択、トレースの開始、問題の再現、診断コレクションの完了、そしてファイルをCitrixにアップロードするかローカルに保存することから構成されます。

この手順は標準の**収集**手順に似ています。ただし、マシン上でトレースを開始し、それらのマシンで問題を再現することができます。すべての診断コレクションにはAOTトレース情報が含まれています。この手順では、トラブルシューティングに役立つCDFトレースを追加します。

1. Scoutを起動します。マシンの**スタート**メニューから、**Citrix > Citrix Scout**を選択します。開いたページで、**Trace & Reproduce**をクリックします。
2. マシンを選択します。**Select machines**ページには、サイト内のすべてのVDAとコントローラーが一覧表示されます。マシン名で表示をフィルタリングできます。トレースと診断を収集する各マシンの横にあるチェックボックスを選択します。次に、**Continue**をクリックします。

   他のマシンを手動で追加するには（StoreFrontやCitrix Provisioningサーバーなど）、Add machines manuallyを参照してください。

   Scoutは、選択された各マシンで検証テストを自動的に起動し、Verification testsに記載されている基準を満たしていることを確認します。マシンの検証が失敗した場合、**Status**列にメッセージが表示され、そのマシンのチェックボックスは選択解除されます。次のいずれかを実行できます。

   - 問題を解決し、マシンのチェックボックスを再度選択します。これにより、検証テストが再試行されます。
   - そのマシンをスキップします（チェックボックスは選択解除のままにします）。そのマシンからは診断とトレースは収集されません。

   検証テストが完了したら、**Continue**をクリックします。
3. トレースを開始します。概要には、トレースが収集されるすべてのマシンが一覧表示されます。**Start Tracing**をクリックします。

選択した1台以上のマシンで、発生した問題を再現します。その間もトレースの収集は続行されます。問題の再現が完了したら、Scoutで**Continue**をクリックします。これによりトレースが停止します。

トレースを停止した後、トレース中に問題を再現したかどうかを示します。

4. マシンから診断を収集します。**Start Collecting**をクリックします。収集中：

   - **Status**列は、マシンの現在の収集状態を示します。
   - 単一マシンでの進行中の収集を停止するには、そのマシンの**Action**列にある**Cancel**をクリックします。
   - すべての進行中の収集を停止するには、ページの右下隅にある**Stop Collection**をクリックします。収集が完了したマシンからの診断は保持されます。収集を再開するには、各マシンの**Action**列にある**Retry**をクリックします。
   - すべての選択されたマシンで収集が完了すると、右下隅の**収集を停止**ボタンが**続行**に変わります。
   - マシンから診断を再度収集するには、そのマシンの**アクション**列にある**再収集**をクリックします。新しい収集が以前のものを上書きします。
   - 収集が失敗した場合、**アクション**列の**再試行**をクリックできます。成功した収集のみがアップロードまたは保存されます。
   - すべての選択されたマシンで収集が完了した後、**戻る**をクリックしないでください。(クリックすると、収集は失われます。)

   収集が完了したら、**続行**をクリックします。

5. コレクションを保存またはアップロードします。ファイルをCitrixにアップロードするか、ローカルマシンに保存するかを選択します。

   今すぐファイルをアップロードすることを選択した場合、ステップ6に進みます。

   ファイルをローカルに保存することを選択した場合:

   - Windowsの**保存**ダイアログボックスが表示されます。目的の場所に移動します。
   - ローカル保存が完了すると、ファイルのパス名が表示され、リンクされます。ファイルを表示できます。後でファイルをCitrixにアップロードできます。CTX136396を参照してください。

   完了をクリックしてScoutの開始ページに戻ります。この手順でこれ以上ステップを完了する必要はありません。

6. アップロードの認証を行い、必要に応じてプロキシを指定します。詳細については、(#upload-authorization)を参照してください。

   - Scoutを通じて認証していない場合は、この手順に進みます。
   - Scoutを通じて認証済みの場合、保存されている認証トークンがデフォルトで使用されます。これを行う場合は、このオプションを選択して**続行**をクリックします。このコレクションの資格情報は要求されません。手順6に進みます。
   - 以前に認証済みだが、再認証して新しいトークンを取得したい場合は、**変更/再認証**をクリックしてこの手順に進みます。

   アップロードを認証するためにCitrix資格情報を使用するか、Citrix Cloud資格情報を使用するかを選択します。**続行**をクリックします。資格情報ページは、保存されたトークンを使用していない場合にのみ表示されます。

   資格情報ページで:

   - ファイルアップロードにプロキシサーバーを使用したい場合は、**プロキシの構成**をクリックします。Scoutにブラウザのインターネットプロパティに設定されているプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
   - Citrix Cloudアカウントの場合、**トークンの生成**をクリックします。デフォルトのブラウザがCitrix Cloudページに起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
   - Citrixアカウントの場合、資格情報を入力します。

   完了したら、「**続行**」をクリックします。

7. アップロードに関する情報を入力します。

   - 名前フィールドには、収集された診断ファイルのデフォルト名が含まれています。ほとんどのコレクションではこれで十分ですが、名前を変更することもできます。(デフォルト名を削除して名前フィールドを空のままにすると、デフォルト名が使用されます。)
   - 必要に応じて、8桁のCitrixサポートケース番号を指定します。
   - オプションの「**説明**」フィールドに、問題について説明し、該当する場合は問題が発生した時期を示します。

   完了したら、「**アップロードの開始**」をクリックします。

   アップロード中、ページの左下部分にアップロードの完了率が概算で表示されます。進行中のアップロードをキャンセルするには、「**アップロードの停止**」をクリックします。

アップロードが完了すると、その場所のURLが表示され、リンクされます。リンクをたどってCitrixの場所にアクセスし、アップロードの分析を表示したり、リンクをコピーしたりできます。

「**完了**」をクリックして、Scoutの開始ページに戻ります。

トレースと再現

「**トレースと再現**」手順は、マシンの選択、トレースの開始、問題の再現、診断コレクションの完了、そしてファイルをCitrixにアップロードするかローカルに保存することから構成されます。

この手順は標準の「**収集**」手順に似ています。ただし、マシンでトレースを開始し、それらのマシンで問題を再作成することができます。すべての診断コレクションにはAOTトレース情報が含まれています。この手順では、トラブルシューティングに役立つCDFトレースが追加されます。

1. Scoutを起動します。マシンの「**スタート**」メニューから「**Citrix > Citrix Scout**」を選択します。開始ページで、「**トレースと再現**」をクリックします。
2. マシンを選択します。**マシンを選択**ページには、サイト内のすべてのVDAとコントローラーが一覧表示されます。マシン名で表示をフィルターできます。トレースと診断を収集する各マシンの横にあるチェックボックスをオンにします。次に、**続行**をクリックします。

   その他のマシンを手動で追加するには (StoreFrontまたはCitrix Provisioningサーバーなど)、マシンを手動で追加するを参照してください。

   Scoutは、選択した各マシンで検証テストを自動的に起動し、検証テストに記載されている基準を満たしていることを確認します。マシンの検証が失敗した場合、**ステータス**列にメッセージが表示され、そのマシンのチェックボックスはオフになります。次のいずれかを実行できます。

   - 問題を解決してから、そのマシンのチェックボックスを再度オンにします。これにより、検証テストが再試行されます。
   - そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンからは診断情報とトレースは収集されません。

   検証テストが完了したら、**Continue** をクリックします。
3. トレースを開始します。概要には、トレースが収集されるすべてのマシンが一覧表示されます。**Start Tracing** をクリックします。

   選択したマシンのいずれかまたは複数で、発生した問題を再現します。その間、トレースの収集は続行されます。問題の再現が完了したら、Scout で **Continue** をクリックします。これによりトレースが停止します。

トレースを停止した後、トレース中に問題を再現したかどうかを示します。

4. マシンから診断情報を収集します。**Start Collecting** をクリックします。収集中に：

   - **Status** 列には、マシンの現在の収集状態が表示されます。
   - 単一マシンで進行中の収集を停止するには、そのマシンの **Action** 列にある **Cancel** をクリックします。
   - 進行中のすべての収集を停止するには、ページの右下隅にある **Stop Collection** をクリックします。収集が完了したマシンからの診断情報は保持されます。収集を再開するには、各マシンの **Action** 列にある **Retry** をクリックします。
   - 選択したすべてのマシンで収集が完了すると、右下隅の **Stop Collection** ボタンが **Continue** に変わります。
   - マシンから診断情報を再度収集するには、そのマシンの **Action** 列にある **Collect Again** をクリックします。新しい収集は以前のものを上書きします。
   - 収集が失敗した場合、**Action** 列にある **Retry** をクリックできます。正常に収集されたもののみがアップロードまたは保存されます。
   - 選択したすべてのマシンで収集が完了したら、**Back** をクリックしないでください。（クリックすると、収集は失われます。）

   収集が完了したら、**続行**をクリックします。

5. コレクションを保存またはアップロードします。ファイルをCitrixにアップロードするか、ローカルに保存するかを選択します。

   今すぐファイルをアップロードする場合は、手順6に進みます。

   ファイルをローカルに保存する場合:

   - Windowsの保存ダイアログボックスが表示されます。目的の場所を選択します。
   - ローカル保存が完了すると、ファイルのパス名が表示され、リンクされます。ファイルを表示できます。注意: 後でCitrixからファイルをアップロードできます。Citrix Insight Servicesについては、CTX136396を参照してください。

   完了をクリックしてScoutの開始ページに戻ります。この手順でこれ以上完了する必要のある手順はありません。

6. アップロードの認証を行い、必要に応じてプロキシを指定します。このプロセスの詳細については、アップロード認証を確認してください。

   - Scoutを通じて認証していない場合、このステップに進みます。

- Scoutを通じて認証した場合、保存されている認証トークンがデフォルトで使用されます。これを実行したい場合は、このオプションを選択して**続行**をクリックします。この収集の資格情報は求められません。ステップ7に進みます。
- 以前に認証済みで、再認証して新しいトークンを取得したい場合は、**変更/再認証**をクリックしてこのステップに進みます。

アップロードの認証にCitrix資格情報を使用するか、Citrix Cloud資格情報を使用するかを選択します。**続行**をクリックします。資格情報ページは、保存されたトークンを使用していない場合にのみ表示されます。

資格情報ページで:

- ファイルのアップロードにプロキシサーバーを使用する場合は、**プロキシの構成**をクリックします。Scoutに、ブラウザのインターネットプロパティ用に構成されたプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
- Citrix Cloudアカウントの場合は、**トークンを生成**をクリックします。デフォルトのブラウザがCitrix Cloudページを起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
- Citrixアカウントの場合は、資格情報を入力します。

完了したら、**続行**をクリックします。

7. アップロードに関する情報を提供します。

アップロードの詳細を入力します。

- 名前フィールドには、収集された診断ファイルのデフォルト名が含まれています。ほとんどのコレクションではこれで十分ですが、名前を変更することもできます。（デフォルト名を削除して名前フィールドを空のままにした場合、デフォルト名が使用されます。）
- オプションで、8桁のCitrixサポートケース番号を指定します。
- オプションの「説明」フィールドに、問題について説明し、該当する場合は問題が発生した時期を示します。

完了したら、**アップロードの開始**をクリックします。

アップロード中、ページの左下部分にアップロードの完了率が概算で表示されます。進行中のアップロードをキャンセルするには、**アップロードを停止**をクリックします。

アップロードが完了すると、その場所のURLが表示され、リンクされます。リンクをたどってCitrixの場所に移動し、アップロードの分析を表示したり、リンクをコピーしたりできます。

完了をクリックして、Scoutの開始ページに戻ります。

追加のログ収集を有効にする

追加ログ収集を有効にする機能を使用すると、perfmon、Netsh、DebugView、Wiresharkなどのより多くのツールと連携して、トレースおよび再現機能を使用できます。

2407 リリース以降、追加のログ収集を有効にすると、Scout はマシンにインストールされている CDC 関連ツールを自動的に検出し、CDC ツール関連のトレースログを zip パッケージに自動収集します。これらの zip ファイルをカスタマイズして Scout に添付できます。この自動化により、Citrix Scout をより効果的に使用でき、問題を迅速に診断するのに役立ちます。

> **注:**
>
> これはローカルマシンにのみ適用されます。

> 追加のログ収集を設定するには：

1. Citrix Scoutを起動します。
2. **設定**ギアアイコンをクリックします。
3. **より多くのツールで追加ログ収集を有効にする**をクリックします。
4. **保存**をクリックします。

   追加ログ収集を有効にする(/en-us/citrix-virtual-apps-desktops/2407/media/enable-additional-log.png)

追加ログ収集を有効にするには、次の必要なツールがインストールされており、指定された場所にそれらのディレクトリが手動で作成されていることを確認してください。

ツールのインストール場所：

- Procdump ログ: Procdump をダウンロードし、%ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\Procdump\procdump.exe に配置します。
- StoreFront ログ: DbgView をダウンロードし、%ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\DebugView\Dbgview.exe に配置します。
- Procmon ログ: Process Monitor をダウンロードし、%ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\ProcessMonitor\Procmon.exe に配置します。

- Wireshark ログ: Wireshark をシステムに手動でインストールします。

追加のログを収集するには：

1. Scout のホームページで、**Trace & Reproduce** をクリックします。
2. **Select or add machines** ページで、ローカルマシンのチェックボックスをオンにしてデータを収集します。ステータスは *Verified* と表示されている必要があります。
3. **Continue** をクリックし、Trace and Reproduce の指示に従います。
4. 完了後、zip ファイル内のログを確認します。ログは *CDCLogs* フォルダーに圧縮されています。

> **注:**

> Procmon ツールがトレース用に選択されている場合、Process Monitor ログはすぐに大きくなる可能性があります。必要なツールのみを選択するようにしてください。ログのサイズは *%temp%\Scout-CDC-Log* で監視することもできます。

コレクションのスケジュール設定

> **注:**

> 現在、コレクションはスケジュールできますが、ヘルスチェックはできません。

> スケジュール手順は、マシンを選択し、スケジュールを設定またはキャンセルすることで構成されます。スケジュールされたコレクションは自動的に Citrix にアップロードされます。(PowerShell インターフェイスを使用して、スケジュールされたコレクションをローカルに保存できます。Citrix Call Home を参照してください。)

1. Scout を起動します。マシンのスタートメニューから **Citrix > Citrix Scout** を選択します。開いたページで、**Schedule** をクリックします。
2. マシンを選択します。サイト内のすべての VDA と Controller が一覧表示されます。マシン名で表示をフィルターできます。

   グラフィカルインターフェイスを使用してVDAとコントローラーをインストールしたときに、Call Homeスケジュールを設定した場合（Citrix Call Homeを参照）、Scoutはデフォルトでそ

れらの設定を表示します。このバージョンのScoutを使用して、初めてスケジュールされた収集を開始したり、以前に構成されたスケジュールを変更したりできます。

コンポーネントのインストール中にマシンごとにCall Homeを有効/無効にしましたが、Scoutで構成されたスケジュールは、選択したすべてのマシンに影響します。

診断を収集する各マシンの横にあるチェックボックスを選択し、**Continue**をクリックします。

他のマシン（StoreFrontサーバーやCitrix Provisioningサーバーなど）を手動で追加するには、手動でマシンを追加するを参照してください。

Scoutは、選択した各マシンで検証テストを自動的に起動し、検証テストの基準を満たしていることを確認します。マシンの検証が失敗した場合、**Status**列にメッセージが表示され、そのマシンのチェックボックスは選択解除されます。次のいずれかを実行できます。

- 問題を解決してから、マシンのチェックボックスをもう一度選択します。これにより、検証テストが再試行されます。
- そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンからは診断（またはトレース）は収集されません。

検証テストが完了したら、**Continue**をクリックします。

概要ページには、スケジュールが適用されるマシンが一覧表示されます。**Continue**をクリックします。

3. スケジュールを設定します。診断を収集するタイミングを指定します。注意：スケジュールは、選択したすべてのマシンに影響します。

    - 選択したマシンの週次スケジュールを構成するには、**Weekly**をクリックします。曜日を選択します。収集を開始する時刻（24時間表記）を入力します。
    - 選択したマシンの日次スケジュールを構成するには、**Daily**をクリックします。収集を開始する時刻（24時間表記）を入力します。
    - 選択した既存のスケジュールをキャンセルし（別のスケジュールに置き換えない）、**Off**をクリックします。これにより、それらのマシンに対して以前に構成されたスケジュールがすべてキャンセルされます。

    Continueをクリックします。

4. アップロードの認証を行い、必要に応じてプロキシを指定します。このプロセスの詳細については、アップロードの承認を参照してください。注意：Scoutスケジュールを使用している場合、保存されたトークンを使用して認証することはできません。

アップロードの認証にCitrix資格情報を使用するか、Citrix Cloud資格情報を使用するかを選択します。**続行**をクリックします。

資格情報ページで：

- ファイルのアップロードにプロキシサーバーを使用する場合は、**プロキシの構成**をクリックします。Scoutに、ブラウザのインターネットプロパティで構成されているプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力できます。プロキシダイアログボックスを閉じます。
- Citrix Cloudアカウントの場合は、**トークンを生成**をクリックします。デフォルトのブラウザがCitrix Cloudページに起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
- Citrixアカウントの場合は、資格情報を入力します。

完了したら、 をクリックします。

構成されたスケジュールを確認します。 をクリックして Scout の開始ページに戻ります。

収集中、選択された各マシンのWindowsアプリケーションログには、収集とアップロードに関するエントリが含まれます。

データマスキング

Citrix Scoutを使用して収集された診断情報には、セキュリティ上機密性の高い情報が含まれる場合があります。Citrix Scoutのデータマスキング機能を使用すると、診断ファイルをCitrixにアップロードする前に、機密データをマスクできます。

Scout のデータマスキングは、IP アドレス、マシン名、ドメイン名、ユーザー名、ハイパーバイザー名、デリバリーグループ名、カタログ名、アプリケーション名、および SID をマスクするように構成されています。

> **注：**
>
> CDF トレースは暗号化されており、マスクできません。
>
> Linux VDA ログは `.tar.gz2` 形式に圧縮されており、マスクできません。

新しい診断情報を収集し、データマスキングを実行する

Citrix Scoutのデータマスキング機能を使用するには、コマンドラインからScoutを起動します。

1. Windowsで、コマンドプロンプトを管理者として開きます。
2. Scoutがインストールされているディレクトリに移動します: `cd C:\Program Files\Citrix\Telemetry Service`。
3. Scoutを起動します: `ScoutUI.exe datamasking`。
4. 診断情報を収集するには、**Collect** または **Trace & Reproduce** をクリックします。
5. 収集が完了したら、**Enable data masking** を選択します。このオプションはデフォルトで有効になっています。
6. データマスクを設定します。デフォルトのルールを使用することも、ルールをカスタマイズすることもできます。
7. 診断情報の収集をアップロードするか保存するかを選択します。

    - **Upload the diagnostics collection to Citrix** を選択すると、マスクされた診断ファイルがCitrixにアップロードされます。
    - **Save the diagnostics collection on your local machine** を選択すると、元の診断情報とマスクされた診断情報の両方が指定された場所に保存されます。

既存の診断情報に対してデータマスキングを実行する

1. Windowsで、コマンドプロンプトを管理者として開きます。
2. Scoutがインストールされているディレクトリに移動します: `cd C:\Program Files\Citrix\Telemetry Service`。
3. データマスキングモードでScoutを直接起動します: `ScoutUI.exe datamasking filePath`。
4. 「データマスキングを有効にする」を選択して続行します。このオプションはデフォルトで有効になっています。
5. データマスクを構成します。デフォルトのルールでデータマスキングを実行することも、ルールをカスタマイズすることもできます。
6. 診断コレクションをアップロードするか保存するかを選択します。

    - **診断コレクションをCitrixにアップロード**を選択した場合、マスクされた診断ファイルがCitrixにアップロードされます。
    - **診断コレクションをローカルマシンに保存**を選択した場合、元の診断とマスクされた診断の両方が指定された場所に保存されます。

マスクされたデータファイルとマッピングファイルの場所

診断コレクションをアップロードまたは保存した後、リンクをクリックして元の診断とマスクされた診断を開き、マッピング情報ファイルを開きます。

使用状況データ収集

Scoutを使用すると、CitrixはGoogle Analyticsを使用して、将来の製品機能と改善に利用される匿名使用状況データを収集します。データ収集はデフォルトで有効になっています。

使用状況データの収集とアップロードを変更するには、Scout UIの**設定**アイコンをクリックします。その後、**はい**または**いいえ**を選択し、**保存**をクリックして情報を送信するかどうかを選択できます。

Scoutの使用状況データ収集(/en-us/citrix-virtual-apps-desktops/2407/media/scout-usage.png)

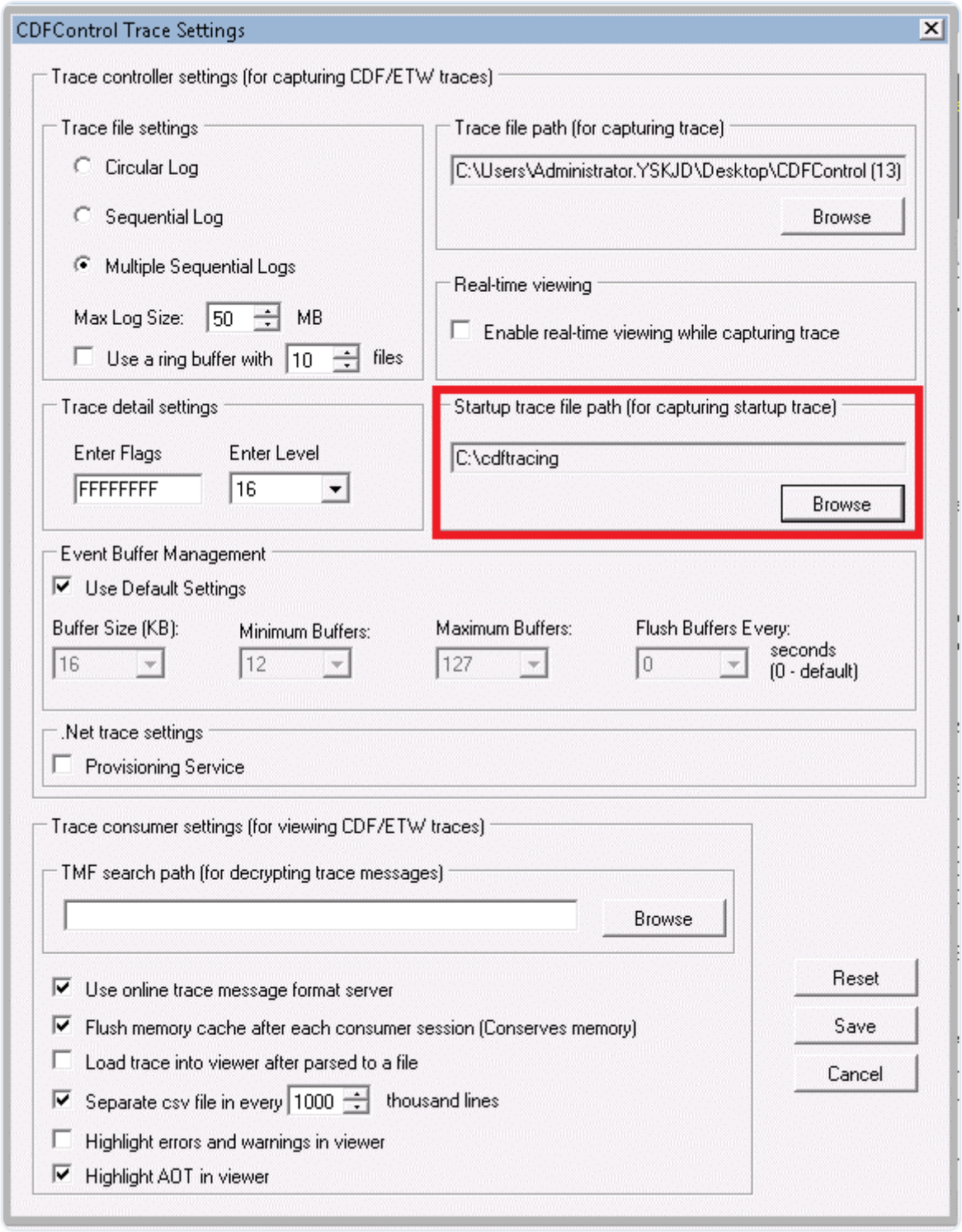
システム起動時にCitrix Diagnostic Facility (CDF) トレースを収集する

CDFControlユーティリティは、さまざまなCitrixトレースプロバイダーから表示されるCitrix Diagnostic Facility (CDF) トレースメッセージをキャプチャするためのイベントトレースコントローラーまたはコンシューマーです。これは、複雑なCitrix関連の問題のトラブルシューティング、フィルターサポートの解析、およびパフォーマンスデータの収集を目的としています。CDFControlユーティリティをダウンロードするには、CTX111961を参照してください。

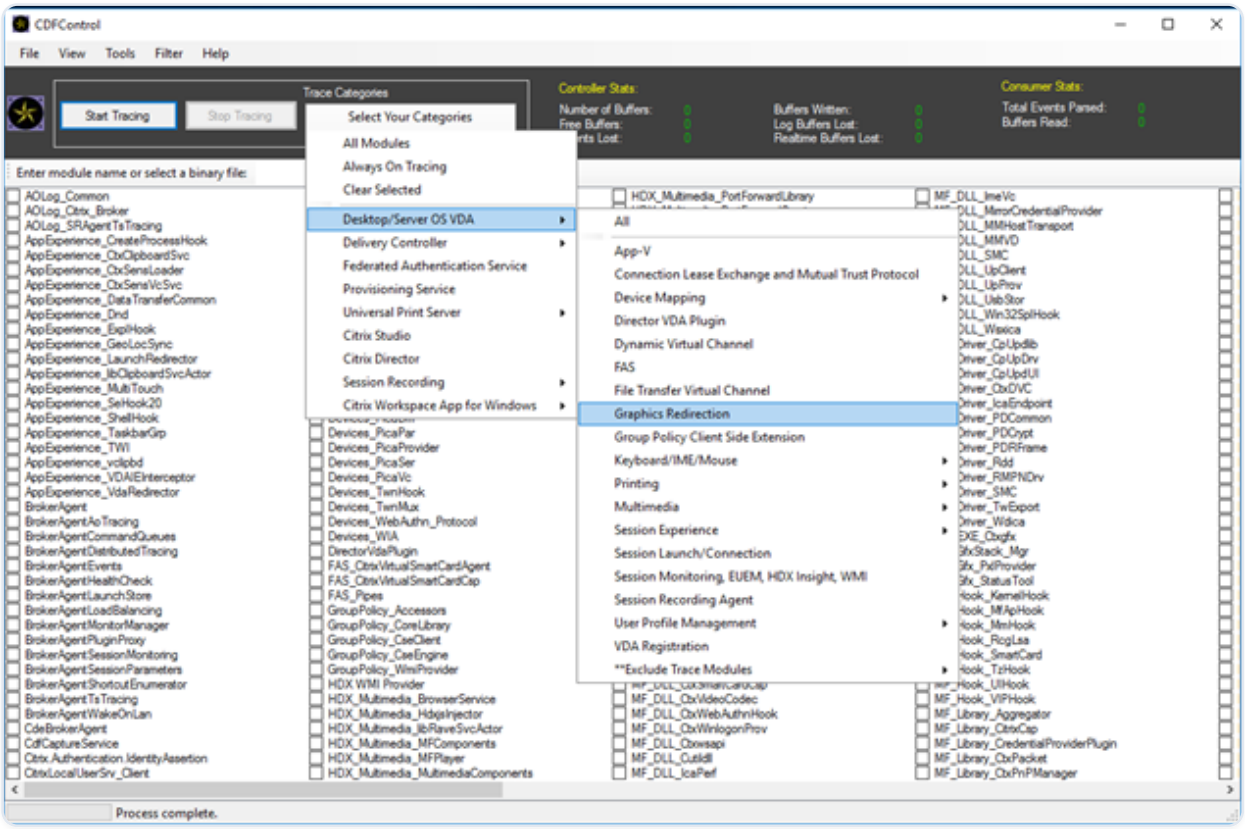
システム起動時にトレースを収集する

システム起動時にCDFトレースを収集するには、次の手順を使用します。管理者権限が必要です。

1. **CDFControl**を起動し、**ツール**メニューから**オプション**を選択します。
2. **起動トレースをキャプチャするための起動トレースファイルパス**セクションでトレースファイルパスを指定します。次に、**保存**をクリックします。



3. Citrixサポートが推奨する**トレースカテゴリ**を選択します。（以下の例では、**グラフィックリダイレクト**が選択されています。この選択は単なる例です。トラブルシューティングしている特定の問題に対してプロバイダーを有効にすることをお勧めします。）



4. **ツール**メニューから**起動トレース**を選択し、**有効にする**を選択します。

   有効にするを選択すると、アニメーションバーがスクロールを開始します。このアクティビティは手順に影響しません。次のステップに進んでください。

5. **起動トレース**が有効になったら、**CDFControlユーティリティ**を閉じてシステムを再起動します。

6. **CDFControl**ユーティリティを起動します。システムが再起動し、エラーが表示されたら、**ツール**メニューから**起動トレース**を選択し、**無効にする**をクリックして起動トレースを無効にします。

7. 手順2で指定したトレースファイルパスに移動し、分析のためにトレースログファイル（.etl）を収集します。

委任管理

> **注:**

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

委任管理モデルは、ロールベースおよびオブジェクトベースの制御を使用して、組織が管理アクティビティを委任する方法に合わせる柔軟性を提供します。委任管理は、あらゆる規模の展開に対応し、展開の複雑さが増すにつれて、より詳細な権限の粒度を構成できるようにします。委任管理では、管理者、ロール、スコープという3つの概念を使用します。

- **管理者:** 管理者は、Active Directoryアカウントによって識別される個人またはグループを表します。各管理者は、1つ以上のロールとスコープのペアに関連付けられています。
- **ロール:** ロールは職務を表し、それに関連付けられた定義済みの権限を持ちます。たとえば、Delivery Group Administratorロールには、「Delivery Groupの作成」や「Delivery Groupからのデスクトップの削除」などの権限があります。管理者はサイトに対して複数のロールを持つことができるため、ある人物がDelivery Group AdministratorとMachine Catalog Administratorの両方になることができます。ロールは組み込みまたはカスタムにすることができます。

  組み込みロールは次のとおりです。

ロール	権限
フル管理者	すべてのタスクと操作を実行できます。フル管理者は常に「すべて」スコープと組み合わされます。
読み取り専用管理者	グローバル情報に加えて、指定されたスコープ内のすべてのオブジェクトを表示できますが、何も変更できません。たとえば、Scope=Londonの読み取り専用管理者は、すべてのグローバルオブジェクト（構成ログなど）と、Londonスコープのオブジェクト（Londonデリバリーグループなど）を表示できます。ただし、その管理者はNew Yorkスコープ内のオブジェクトを表示できません（LondonとNew Yorkのスコープが重複しないと仮定した場合）。
ヘルプデスク管理者	デリバリーグループを表示し、それらのグループに関連付けられたセッションとマシンを管理できます。監視対象のデリバリーグループのマシンカタログとホスト情報を表示できます。また、それらのデリバリーグループ内のマシンに対して、セッション管理およびマシン電源管理操作を実行できます。

ロール	権限
マシンカタログ管理者	マシンカタログを作成および管理し、それらにマシンをプロビジョニングできます。仮想化インフラストラクチャ、Provisioning Services、および物理マシンからマシンカタログを構築できます。この役割は、ベースイメージの管理とソフトウェアのインストールはできますが、アプリケーションやデスクトップをユーザーに割り当てることはできません。
デリバリーグループ管理者	アプリケーション、デスクトップ、およびマシンを配信できます。関連するセッションも管理できます。ポリシーや電源管理設定など、アプリケーションとデスクトップの構成も管理できます。
ホスト管理者	ホスト接続とそれに関連するリソース設定を管理できます。マシン、アプリケーション、またはデスクトップをユーザーに配信することはできません。

特定の製品エディションでは、組織の要件に合わせてカスタム役割を作成し、より詳細な権限を委任できます。カスタム役割を使用して、コンソール内のアクションまたはタスクの粒度で権限を割り当てることができます。

- **スコープ:** スコープはオブジェクトのコレクションを表します。スコープは、組織に関連する方法でオブジェクトをグループ化するために使用されます（たとえば、営業チームが使用するデリバリーグループのセット）。オブジェクトは複数のスコープに属することができます。オブジェクトに1つ以上のスコープがラベル付けされていると考えることができます。「すべて」という組み込みスコープが1つあり、すべてのオブジェクトが含まれます。フル管理者役割は常に**すべて**スコープとペアになります。

例

XYZ社は、部門（経理、営業、倉庫）とデスクトップオペレーティングシステム（Windows 7またはWindows 8）に基づいてアプリケーションとデスクトップを管理することにしました。管理者は5つのスコープを作成し、各デリバリーグループに2つのスコープをラベル付けしました。1つは使用される部門用、もう1つは使用されるオペレーティングシステム用です。

次の管理者が作成されました。

管理者	ロール	スコープ
domain/fred	完全管理者	すべて（完全管理者ロールは常にすべてのスコープを持ちます）
domain/rob	読み取り専用管理者	すべて
domain/heidi	読み取り専用管理者、ヘルプデスク管理者	すべての営業
domain/warehouseadmin	ヘルプデスク管理者	倉庫
domain/peter	デリバリーグループ管理者、マシンカタログ管理者	Win7

- フレッドは完全管理者であり、システム内のすべてのオブジェクトを表示、編集、削除できます。
- Robはサイト内のすべてのオブジェクトを表示できますが、編集または削除はできません。
- ハイジはすべてのオブジェクトを表示でき、Salesスコープ内のデリバリーグループに対してヘルプデスクタスクを実行できます。これにより、彼女はそれらのグループに関連付けられているセッションとマシンを管理できますが、マシンの追加や削除など、デリバリーグループに変更を加えることはできません。
- warehouseadmin Active Directoryセキュリティグループのメンバーであれば誰でも、Warehouseスコープ内のマシンを表示し、ヘルプデスクタスクを実行できます。
- ピーターはWindows 7のスペシャリストであり、どの部門スコープに属していても、すべてのWindows 7マシンカタログを管理し、Windows 7アプリケーション、デスクトップ、およびマシンを配信できます。管理者はピーターをWin7スコープのフル管理者にする検討をしましたが、フル管理者は「サイト」や「管理者」など、スコープが設定されていないすべてのオブジェクトに対しても完全な権限を持つため、この案は却下しました。

委任管理の使用方法

一般に、管理者の数と権限の粒度は、展開の規模と複雑さによって異なります。

- 小規模な展開や概念実証の展開では、1人または数人の管理者がすべての作業を行います。委任はありません。この場合、各管理者を、Allスコープを持つ組み込みのフル管理者ロールで作成します。

- マシン、アプリケーション、デスクトップが多い大規模な展開では、より多くの委任が必要です。複数の管理者が、より具体的な機能的責任（ロール）を持つ場合があります。たとえば、2人がフル管理者で、他の管理者がヘルプデスク管理者である場合があります。また、管理者がマシンカタログなど、特定のオブジェクトグループ（スコープ）のみを管理する場合もあります。この場合、新しいスコープを作成し、組み込みロールのいずれかと適切なスコープを持つ管理者を作成します。
- さらに大規模な展開では、より多くの（またはより具体的な）スコープ、および型にはまらないロールを持つ異なる管理者が必要になる場合があります。この場合、スコープを編集または追加作成し、カスタムロールを作成し、組み込みロールまたはカスタムロール、および既存のスコープと新しいスコープを持つ各管理者を作成します。

柔軟性と構成の容易さのために、管理者を作成するときにスコープを作成できます。マシンカタログまたは接続を作成または編集するときに、スコープを指定することもできます。

管理者の作成と管理

ローカル管理者としてサイトを作成すると、ユーザーアカウントは自動的にすべてのオブジェクトに対する完全な権限を持つフル管理者になります。サイトが作成された後、ローカル管理者には特別な権限はありません。

フル管理者ロールは常にAllスコープを持ちます。これは変更できません。

デフォルトでは、管理者は有効になっています。管理者を今作成するが、その人が後で管理業務を開始する場合、管理者を無効にする必要があるかもしれません。既存の有効な管理者については、オブジェクト/スコープを再編成している間にいくつか無効にし、更新された構成で稼働準備ができたときに再度有効にすることができます。有効なフル管理者がいなくなる場合、フル管理者を無効にすることはできません。有効/無効チェックボックスは、管理者を作成、コピー、または編集するときに利用できます。

管理者をコピー、編集、または削除する際にロール/スコープのペアを削除すると、その管理者に対するロールとスコープ間の関連付けのみが削除されます。ロールまたはスコープのいずれも削除されません。また、そのロール/スコープのペアで構成されている他の管理者には影響しません。

管理者を作成および管理するには、次の手順に従います。

1. Web Studioにサインインし、左側のペインで**管理者**をクリックし、次に**管理者**タブをクリックします。
2. 実行するタスクの手順に従います。

- **管理者を作成する:** アクションバーで **Create Administrator** をクリックします。ユーザーアカウント名を入力または参照し、スコープを選択または作成してから、役割を選択します。新しい管理者はデフォルトで有効になっています。これは変更できます。
- **管理者をコピーする:** 管理者を選択し、アクションバーで **Copy Administrator** をクリックします。ユーザーアカウント名を入力または参照します。役割/スコープのペアを選択して編集または削除したり、新しいペアを追加したりできます。新しい管理者はデフォルトで有効になっています。これは変更できます。
- **管理者を編集する:** 管理者を選択し、アクションバーで **Edit Administrator** をクリックします。役割/スコープのペアを編集または削除したり、新しいペアを追加したりできます。
- **管理者を削除する:** 管理者を選択し、アクションバーで **Delete Administrator** をクリックします。有効なフル管理者がいなくなる場合、フル管理者を削除することはできません。

上部のペインには、作成した管理者が表示されます。管理者を選択すると、下部のペインにその詳細が表示されます。**警告**列は、管理者に関連付けられているロールとスコープのペアに、使用できないロールまたはスコープが含まれているかどうかを示します。関連付けられているロールとスコープのペアに、使用できないロールまたはスコープが含まれている場合、次の警告メッセージが表示されます。

- 関連付けられているロールまたはスコープが使用できません

> **重要:**
>
> 警告メッセージは、関連付けられているロールとスコープのペアに、使用できないロール、スコープ、またはその両方が含まれている場合にのみ表示されます。

> 管理者からロールとスコープのペアを削除するには、次のいずれかの手順を実行します。

- ロールとスコープのペアを削除します。
  a. アクションバーで、**管理者編集**をクリックします。
  b. **管理者名と詳細**ウィンドウで、役割とスコープのペアを選択し、**削除**をクリックします。
  c. 終了するには**保存**をクリックします。
- 管理者を削除します。
  a. アクションバーで、**管理者削除**をクリックします。
  b. 確認ウィンドウで、**削除**をクリックします。

役割の作成と管理

管理者がロールを作成または編集する場合、自分自身が持っている権限のみを有効にできます。これにより、管理者が現在持っている権限よりも多くの権限を持つロールを作成して自分に割り当てたり（またはすでに割り当てられているロールを編集したり）することを防ぎます。

ロール名には最大64個のUnicode文字を含めることができます。ただし、バックスラッシュ、スラッシュ、セミコロン、コロン、ポンド記号、コンマ、アスタリスク、疑問符、等号、左右の矢印、パイプ、左右の角括弧、左右の丸括弧、引用符、アポストロフィは含めることができません。説明には最大256個のUnicode文字を含めることができます。

組み込みの役割を編集または削除することはできません。カスタム役割が管理者によって使用されている場合、その役割を削除することはできません。

> **注:**
>
> 特定の製品エディションのみがカスタム役割をサポートしています。カスタム役割をサポートするエディションのみが、アクションバーに関連エントリを持っています。

役割を作成および管理するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**管理者**をクリックし、**役割**タブをクリックします。
2. 実行したいタスクの手順に従います。

    - **ロールの詳細を表示：** ロールを選択します。下部のペインに、ロールのオブジェクトタイプと関連する権限が一覧表示されます。下部のペインにある「**管理者**」タブをクリックすると、現在このロールを持つ管理者の一覧が表示されます。
    - **カスタムロールを作成：** アクションペインで「**ロールの作成**」をクリックします。名前と説明を入力します。オブジェクトタイプと権限を選択します。
    - **役割をコピーする:** 役割を選択し、アクションバーで**役割をコピー**をクリックします。必要に応じて、名前、説明、オブジェクトの種類、および権限を変更します。
    - **カスタム役割を編集する:** 役割を選択し、アクションバーで**役割を編集**をクリックします。必要に応じて、名前、説明、オブジェクトの種類、および権限を変更します。
    - **カスタム役割を削除する:** 役割を選択し、アクションバーで**役割を削除**をクリックします。プロンプトが表示されたら、削除を確認します。

スコープの作成と管理

サイトを作成するときに利用できるスコープは「すべて」スコープのみであり、これは削除できません。

次の手順でスコープを作成できます。管理者を作成するときにもスコープを作成できます。各管理者は、少なくとも1つのロールとスコープのペアに関連付けられている必要があります。デスクトップ、マシンカタログ、アプリケーション、またはホストを作成または編集するときに、それらを既存のスコープに追加できます。スコープに追加しない場合、それらは「すべて」スコープの一部として残ります。

サイトの作成はスコープ化できず、委任された管理オブジェクト（スコープと役割）もスコープ化できません。ただし、スコープ化できないオブジェクトは「すべて」スコープに含まれます。（フル管理者は常に「すべて」スコープを持ちます。）マシン、電源アクション、デスクトップ、およびセッションは直接スコープ化されません。管理者は、関連するマシンカタログまたはデリバリーグループを通じて、これらのオブジェクトに対する権限を割り当てることができます。

スコープの作成と管理に関するルール:

- スコープ名には最大64文字のUnicode文字を含めることができます。スコープ名には、バックスラッシュ、スラッシュ、セミコロン、コロン、ポンド記号、コンマ、アスタリスク、疑問符、等号、左矢印、右矢印、パイプ、左右の角かっこ、左右の丸かっこ、引用符、またはアポストロフィを含めることはできません。
- スコープの説明には最大256文字のUnicode文字を含めることができます。
- スコープをコピーまたは編集する際は、スコープからオブジェクトを削除すると、それらのオブジェクトに管理者がアクセスできなくなる可能性があることに留意してください。編集されたスコープが1つ以上のロールとペアになっている場合、スコープの更新によってどのロール/スコープのペアも使用できなくならないようにしてください。

スコープを作成および管理するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**管理者**をクリックしてから、**スコープ**タブをクリックします。
2. 実行するタスクの手順に従います。

    - **スコープを作成する:** アクションバーで**新しいスコープを作成**をクリックします。名前と説明を入力します。特定の種類のすべてのオブジェクト（例: デリバリーグループ）を含めるには、オブジェクトの種類を選択します。特定のオブジェクトを含めるには、種類を展開してから個々のオブジェクト（例: 営業チームが使用するデリバリーグループ）を選択します。

- **スコープのコピー:** スコープを選択し、アクションバーで**スコープのコピー**をクリックします。名前と説明を入力します。必要に応じて、オブジェクトの種類とオブジェクトを変更します。
- **スコープの編集:** スコープを選択し、アクションバーで**スコープの編集**をクリックします。必要に応じて、名前、説明、オブジェクトの種類、およびオブジェクトを変更します。
- **スコープの削除:** スコープを選択し、アクションバーで**スコープの削除**をクリックします。プロンプトが表示されたら、削除を確定します。

テナント管理のセットアップ

単一のCitrix Virtual Apps and Desktopsサイト内に管理パーティションを作成するために、テナント管理をセットアップします。各テナントには、マシンカタログやデリバリーグループなどの分離されたリソースと構成があります。特定のテナントにアクセスできる管理者は、そのテナントに関連付けられたリソースと構成のみを管理できます。使用例としては、単一サイト内に異なるビジネスサイロ（独立した部門または個別のIT管理チーム）を持つ企業が挙げられます。

大まかに言うと、テナント管理をセットアップするためのワークフローには以下が含まれます。

1. テナントの作成
2. テナントの管理者を追加

テナントの作成

テナントスコープを作成してテナントを作成します。詳細な手順は次のとおりです。

1. Web Studioにサインインし、左ペインで**管理者**をクリックし、**スコープ**タブをクリックします。
2. *スコープの作成**をクリックして、テナントの作成を開始します。
3. テナントスコープの以下の詳細を入力します。

    a. スコープのわかりやすい名前を入力します。この名前はテナントの識別子としても機能します。

    b. （オプション）簡単な説明を入力します。

    c. **テナントスコープ**を選択します。

    d. 必要に応じて、テナントに関連付けられているオブジェクトを選択します。オブジェクトの作成時または管理時に、テナントスコープにオブジェクトを追加することもできます。

    e. 「**OK**」をクリックして作成を完了します。

完了後、以下を確認できます。

- 新しいテナントスコープレコードがスコープリストに表示され、**種類**列で**テナント**として識別されます。
- スコープ名は、Web Studioの右上隅にある**すべてのテナント**ドロップダウンリストに表示されます。

テナントスコープを操作する際は、次の考慮事項に留意してください。

- テナントプロパティは、ホスティング > マシンカタログ > デリバリーグループ > アプリケーションという階層的な割り当て順序に従います。下位レベルのオブジェクトは、上位レベルのオブジェクトからテナントプロパティを継承します。たとえば、テナントスコープのデリバリーグループを選択する場合は、関連するホスティングとマシンカタログも選択していることを確認してください。そうしないと、デリバリーグループはテナントのプロパティを継承できません。
- テナントスコープを作成した後、オブジェクトを変更してテナントの割り当てを編集できます。テナントの割り当てが変更された場合でも、同じテナントまたはそれらのテナントのサブセットに割り当てる必要があるという制約が適用されます。ただし、テナントの割り当てが変更されても、下位レベルのオブジェクトは再評価されません。テナントの割り当てを変更する際は、オブジェクトが適切に制限されていることを確認してください。たとえば、マシンカタログが `TenantA` と `TenantB` で利用可能な場合、`TenantA` 用と `TenantB` 用のデリバリーグループを作成できます。(`TenantA` と `TenantB` は両方ともそのマシンカタログに関連付けられています。)その後、マシンカタログを `TenantA` のみに関連付けるように変更できます。その結果、`TenantB` に関連付けられているデリバリーグループは無効になります。

テナントの管理者を追加する

管理者ロールとテナントを持つユーザーアカウントを割り当てることで、テナントの管理者を追加します。

テナントの管理者を追加するには、次の手順に従います。

1. Web Studio にサインインし、左ペインで「**管理者**」をクリックし、次に「**管理者**」タブをクリックします。
2. 「**管理者を追加**」をクリックし、次の手順に従って完了します。
   a. ユーザーアカウント名を入力または参照し、「**次へ**」をクリックします。
   b. 「**カスタムアクセス**」を選択し、必要に応じて1つ以上の役割（例：マシンカタログ管理者）を選択します。
   c. 各役割の横にある「**スコープの編集**」をクリックし、スコープを「**すべて**」から目的のテナントスコープに変更して、「**保存**」をクリックします。

3. **Next**をクリックします。
4. 「**確認と確定**」ページで、「**招待状を送信**」をクリックします。

レポートの作成

委任管理レポートには、次の2種類を作成できます。

- 管理者に関連付けられている役割/スコープのペアと、各種類のオブジェクト（例：デリバリーグループとマシンカタログ）の個々の権限を一覧表示するHTMLレポート。このレポートはWeb Studioから生成します。

  このレポートを作成するには、次の手順に従います。

  a. Web Studioにサインインし、左ペインで「**管理者**」をクリックします。
  b. 管理者を選択し、アクションバーで「**レポートの作成**」をクリックします。

  管理者の作成、コピー、または編集時に、このレポートを要求することもできます。
- すべての組み込み役割とカスタム役割を権限にマッピングするHTMLまたはCSVレポート。このレポートは、OutputPermissionMapping.ps1という名前のPowerShellスクリプトを実行して生成します。

  このスクリプトを実行するには、フル管理者、読み取り専用管理者、または役割を読み取る権限を持つカスタム管理者である必要があります。スクリプトは、Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scriptsにあります。

  構文：

  `OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path string] [-AdminAddress string] [-Show] [CommonParameters]`

パラメーター	説明
`-Help`	スクリプトのヘルプを表示します。
`-Csv`	CSV 出力を指定します。デフォルト = HTML
`-Path string`	出力の書き込み先。デフォルト = stdout
`-AdminAddress string`	接続先の Delivery Controller™ の IP アドレスまたはホスト名。デフォルト = localhost

パラメーター	説明
`-Show`	(`-Path` パラメーターも指定されている場合にのみ有効) 出力をファイルに書き込むと、`-Show` によって、Web ブラウザーなどの適切なプログラムで出力が開かれます。
共通パラメーター	`Verbose`、`Debug`、`ErrorAction`、`ErrorVariable`、`WarningAction`、`WarningVariable`、`OutBuffer`、および `OutVariable`。詳細については、Microsoft のドキュメントを参照してください。

次の例では、HTML テーブルを Roles.html という名前のファイルに書き込み、Web ブラウザーでテーブルを開きます。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

-Path Roles.html –Show
```

次の例では、CSVテーブルをRoles.csvという名前のファイルに書き込みます。テーブルは表示されません。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

–CSV -Path Roles.csv
```

Windowsのコマンドプロンプトから、上記の例のコマンドは次のとおりです。

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'

-CSV -Path Roles.csv"
```

デリバリーコントローラー

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

デリバリーコントローラーは、ユーザーアクセスを管理し、接続の仲介と最適化を行うサーバー側コンポーネントです。コントローラーは、デスクトップおよびサーバーイメージを作成する Machine Creation Services™ も提供します。

サイトには少なくとも1つのコントローラーが必要です。最初のコントローラーをインストールした後、サイトの作成時または後でコントローラーを追加できます。サイトに複数のコントローラーを配置することには、主に2つの利点があります。

- **冗長性:** ベストプラクティスとして、本番サイトでは常に異なる物理サーバー上に少なくとも2つのコントローラーを配置してください。1つのコントローラーが故障した場合でも、他のコントローラーが接続を管理し、サイトを管理できます。
- **スケーラビリティ:** サイトのアクティビティが増加すると、コントローラーのCPU使用率とデータベースアクティビティも増加します。追加のコントローラーにより、より多くのユーザー、アプリケーション、およびデスクトップ要求を処理できるようになり、全体的な応答性が向上します。

各コントローラーはサイトデータベースと直接通信します。複数のゾーンがあるサイトでは、各ゾーンのコントローラーは、プライマリゾーンのサイトデータベースと通信します。

> **重要:**
>
> サイトの構成後、コントローラーのコンピューター名またはドメインメンバーシップを変更しないでください。

VDAがコントローラーに登録する方法

VDAを使用する前に、サイト内のDelivery Controllerに登録（通信を確立）する必要があります。VDA登録の詳細については、「VDA registration with Controllers」を参照してください。

コントローラーの追加、削除、または移動

コントローラーを追加、削除、または移動するには、「Databases」の記事に記載されているサーバーロールとデータベースロールの権限が必要です。

SQLクラスタリングまたはSQLミラーリングインストール内のノードにコントローラーをインストールすることはサポートされていません。

サイトにDelivery Controller™を追加する際は、高可用性のために使用するレプリカSQL Serverにそのマシンのログオン資格情報を追加してください。

展開でデータベースミラーリングを使用している場合:

- Controllerを追加、削除、または移動する前に、プライマリデータベースとミラーデータベースの両方が実行されていることを確認してください。さらに、SQL Server Management Studioでスクリプトを使用する場合は、スクリプトを実行する前にSQLCMDモードを有効にしてください。
- Controllerを追加、削除、または移動した後にミラーリングを確認するには、PowerShell `Get-configdbconnection` コマンドレットを実行します。このコマンドレットは、接続文字列でミラーへのフェールオーバーパートナーが設定されていることを確認します。

Controller を追加、削除、または移動した後:

- 自動更新が有効になっている場合、VDAは90分以内にControllerの更新されたリストを受け取ります。
- 自動更新が有効になっていない場合は、すべてのVDAに対してControllerポリシー設定またはListOfDDCsレジストリキーが更新されていることを確認してください。Controllerを別のサイトに移動した後、両方のサイトでポリシー設定またはレジストリキーを更新してください。

Controllerを追加する

Controllerは、サイトの作成時および後から追加できます。このソフトウェアの以前のバージョンでインストールされたControllerを、このバージョンで作成されたサイトに追加することはできません。

1. サポートされているオペレーティングシステムを含むサーバーでインストーラーを実行します。Delivery Controllerコンポーネントと、必要なその他のコアコンポーネントをインストールします。インストールウィザードを完了します。
2. まだサイトを作成していない場合は、このControllerでCitrix Site Manager を実行してサイトを作成します。このControllerのIPアドレスは、新しいサイトに自動的に追加されます。

データベースを初期化するスクリプトを生成する予定がある場合は、スクリプトを生成する前にControllerを追加してください。

3. 既にサイトを作成している場合は、次の手順に従ってください。

   a. このControllerでCitrix Site Manager を実行し、**Join an existing site** をクリックして、参加したいサイトのControllerのアドレスを入力します。

   b. Studio configuration tool を実行して、ControllerをWeb Studioに追加します。

Controller を削除する

サイトからコントローラーを削除しても、Citrixソフトウェアやその他のコンポーネントがアンインストールされるわけではありません。この操作は、コントローラーをデータベースから削除し、接続の仲介やその他のタスクに使用できなくするものです。コントローラーを削除しても、後で同じサイトまたは別のサイトに再度追加できます。サイトには少なくとも1つのコントローラーが必要なため、Web Studioに表示されている最後のコントローラーを削除することはできません。

サイトからコントローラーを削除しても、データベースサーバーへのコントローラーのログオンは削除されません。これは、同じマシン上の他の製品のサービスで使用されているログオンが誤って削除されるのを防ぐためです。ログオンが不要になった場合は、手動で削除する必要があります。ログオンを削除するには、`securityadmin`サーバーロールのアクセス許可が必要です。

Controller を削除した後:

- 自動更新を使用するVDAは、他の利用可能なコントローラーに再登録します。この再登録は、自動更新メカニズムが有効になっており、VDAが他のコントローラー（削除されたコントローラーと同じセカンダリゾーン、またはオンプレミス展開のプライマリゾーン）に到達できる場合にのみ発生します。
- Citrix StoreFrontでコントローラー情報を更新します。詳しくは、「」(/ja-jp/storefront/2507-ltsr/stores/sites)を参照してください。
- Citrix StoreFrontで、Citrix Gatewayを介したリモートアクセス用のSecure Ticket Authority (STA) URLを更新します。詳しくは、「」(/ja-jp/storefront/2507-ltsr/integrate-with-citrix-gateway-and-citrix-adc/configure-citrix-gateway.html#add-citrix-gateway-appliance)を参照してください。
- Citrix Gatewayで、仮想サーバーのSTA URLを更新します。詳しくは、「」(/ja-jp/citrix-gateway/current-release.html)を参照してください。

> **重要:**

> サイトからコントローラーを削除するまでは、Active Directoryからコントローラーを削除しないでください。

1. Web Studioが読み込まれ、削除するコントローラーが表示されるように、コントローラーの電源がオンになっていることを確認してください。
2. Web Studioがコントローラーを完全に読み込んだ後、コントローラー上のすべてのサービスが実行されており、コントローラーの電源がオンのままであることを確認します。
3. Web Studioにサインインし、左側のペインで**［設定］**を選択します。
4. **［Delivery Controller］タイルを見つけて、［編集］**をクリックします。
5. **［Delivery Controllerの管理］**ページで、削除するコントローラーを選択します。
6. 「**Controllerの削除**」を選択します。適切なデータベースロールと権限がない場合は、データベース管理者がControllerを削除できるようにするスクリプトを生成するオプションが提示されます。

   Web Studioは、Controllerを削除する前に事前チェックを実行します。Controllerは、電源がオフになっており、以下のサービスステータスではない場合に安全に削除できます。

   - 不明
   - 障害保留中
   - 古いバージョン
   - 新しいバージョン
   - バージョン変更中
   - 必須機能が不足

   Controllerの電源がオフになっておらず、上記のいずれかのサービスステータスである場合、Web StudioはControllerの電源をオフにするよう求めます。
7. データベースサーバーから Controller のマシンアカウントを削除する必要があります。削除する前に、別サービスがそのアカウントを使用していないことを確認してください。

Web Studioを使用してControllerを削除した後、現在のタスクが適切に完了するように、そのControllerへのトラフィックが短時間残る場合があります。短時間でControllerの削除を強制したい場合は、Citrixは、Controllerがインストールされていたサーバーをシャットダウンするか、そのサーバーをActive Directoryから削除することをお勧めします。その後、サイト上の他のControllerを再起動して、削除されたControllerとの通信がこれ以上行われないようにします。

Controller を別のゾーンに移動する

サイトに複数のゾーンが含まれている場合は、Controllerを別のゾーンに移動できます。この移動がVDA登録やその他の操作にどのように影響するかについては、「ゾーン」を参照してください。

1. 左側のペインで「**ゾーン**」を選択します。
2. 中央のペインでゾーンを選択し、Controllerを選択します。
3. アクションバーで**アイテムの移動**を選択します。
4. 表示される**アイテムの移動**ページで、Controllerを移動するゾーンを選択します。
5. **保存**をクリックします。

VDA を別のサイトに移動する

Citrix Provisioning™を使用してプロビジョニングされたVDA、または既存のイメージであるVDAは、アップグレード時、またはテストサイトで作成されたVDAイメージを本番サイトに移動する際に、別のサイト（サイト1からサイト2へ）に移動できます。Machine Creation Services (MCS) を使用してプロビジョニングされたVDAは、あるサイトから別のサイトへ移動できません。MCSは、VDAがControllerに登録するためにチェックするListOfDDCsの変更をサポートしていません。MCSを使用してプロビジョニングされたVDAは、常に作成されたサイトに関連付けられているListOfDDCsをチェックします。

VDA を別のサイトに移動する方法は、インストーラーを使用する方法と Citrix ポリシーを使用する方法の 2 つがあります。

インストーラー

インストーラーを実行してControllerを追加し、サイト2のControllerのFQDN（DNSエントリ）を指定します。

インストーラーでControllerを指定するのは、Controllerポリシー設定が使用されていない場合のみです。

グループポリシーエディター

次の例では、複数のVDAをサイト間で移動します。

1. サイト1で以下の設定を含むポリシーを作成し、そのポリシーをデリバリーグループレベルにフィルターして、サイト間の段階的なVDA移行を開始します。
   - Controller：サイト2の1つ以上のControllerのFQDN（DNSエントリ）を含みます。
   - Controllerの自動更新を有効にする：無効に設定します。

2. デリバリーグループ内の各VDAは、新しいポリシーが適用されてから90分以内に通知を受け取ります。VDAは受信したControllerのリストを無視し（自動更新が無効になっているため）、ポリシーで指定されたControllerのいずれかを選択します。これはサイト2のControllerをリストしています。
3. VDAがサイト2のControllerに正常に登録されると、サイト2のListOfDDCsとポリシー情報を受け取ります。これらはデフォルトで自動更新が有効になっています。サイト1でVDAが登録されていたControllerは、サイト2のControllerから送信されたリストには含まれていません。そのため、VDAはサイト2のリストにあるControllerの中から選択して再登録します。それ以降、VDAはサイト2からの情報で自動的に更新されます。

グループポリシーエディターの使用方法については、Citrixポリシーのドキュメントを参照してください。

IPv4/IPv6 のサポート

このリリースでは、純粋な IPv4、純粋な IPv6、および重複する IPv4 と IPv6 ネットワークを使用するデュアルスタック展開をサポートしています。

次のコンポーネントは IPv4 のみをサポートします。その他すべてのコンポーネントは IPv4 と IPv6 をサポートします。

- XenServer®
- **IPv6 Controller登録のみを使用**ポリシー設定によって制御されないVirtual Delivery Agent（VDA）

IPv6 通信は、VDA 接続に関連する2つの Citrix® ポリシー設定によって制御されます。

- **IPv6の使用を強制する主要な設定:** IPv6 Controller登録のみを使用。

  このポリシー設定は、VDA が Delivery Controller に登録するために使用するアドレス形式を制御します。

  有効にすると、VDAは次の優先順位で選択された単一のIPv6アドレスを使用してControllerに登録し、通信します。グローバルIPアドレス、ユニークローカルアドレス（ULA）、リンクローカルアドレス（他のIPv6アドレスが利用できない場合のみ）。

  無効にすると、VDAはマシンのIPv4アドレスを使用してControllerに登録し、通信します。これがデフォルト値です。

チームが頻繁にIPv6ネットワークを使用する場合、**IPv6 Controller登録のみを使用**ポリシー設定が有効になっているイメージまたは組織単位（OU）に基づいて、それらのユーザー向けにデスクトップとアプリケーションを公開します。

チームが頻繁にIPv4ネットワークを使用する場合、**IPv6 Controller登録のみを使用**ポリシー設定が無効になっているイメージまたはOUに基づいて、それらのユーザー向けにデスクトップとアプリケーションを公開します。

- **IPv6ネットマスクを定義する依存設定:** Controller登録IPv6ネットマスク。

  マシンは複数のIPv6アドレスを持つことができます。このポリシー設定により、管理者は、VDAが登録されている場合に、グローバルIPではなく、優先するサブネットのみにVDAを制限できます。この設定は、VDAが登録するネットワークを指定します。VDAは、指定されたネットマスクに一致する最初のアドレスでのみ登録します。

  この設定は、**IPv6 Controller登録のみを使用**ポリシー設定が有効な場合にのみ有効です。デフォルト = 空の文字列

展開に関する考慮事項

環境にIPv4ネットワークとIPv6ネットワークの両方が含まれている場合は、IPv4専用クライアントとIPv6ネットワークにアクセスできるクライアント用に、別々のデリバリーグループ構成を作成します。ユーザーを区別するために、命名規則、手動のActive Directoryグループ割り当て、またはSmartAccessフィルターの使用を検討してください。 接続がIPv6ネットワークで開始され、その後IPv4アクセスのみを持つクライアントから再接続しようとすると、セッションの再接続が失敗する可能性があります。

注 - DNS解決が有効になっている場合は、これらの考慮事項は適用されません。

Web Studio を使用した Citrix Virtual Apps and Desktops™ のライセンス

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

> Web Studio から、ライセンスサーバーが Web Studio と同じドメイン内にあるか、または信頼されたドメイン内にある場合、ライセンスを管理および追跡できます。ライセンス関連のタスクについては、ライセンスドキュメント および 複数タイプのライセンス を参照してください。

次の表に、サポートされているエディションとライセンスモデルを示します。

製品	エディション	ライセンスモデル
シトリックス バーチャル アプリ	プレミアム、アドバンスト、スタンダード	同時
シトリックス バーチャル デスクトップ	プレミアム、アドバンスト、スタンダード	ユーザー/デバイスおよび同時

詳細については、同時ライセンス および ユーザー/デバイスライセンス を参照してください。

サポートされている現在のリリース (CR) および長期サービスリリース (LTSR) バージョン

Citrix は、含まれる可能性のある機能的またはセキュリティ上の改善から利益を得るために、常に Citrix License Server の最新バージョンを使用することを強く推奨します。

> **注意:**
>
> License Server VPX は非推奨となり、今後のメンテナンスやセキュリティ修正は提供されません。License Server VPX のバージョン 11.16.6 以前を使用しているお客様は、できるだけ早く Windows 用 License Server の最新バージョンに移行することをお勧めします。

> Citrix 製品のライフサイクル日付の詳細については、製品マトリックスを参照してください。

レガシー製品および製品バージョンに関する情報については、レガシー製品マトリックスを参照してください。

次のタスクを完了するには、完全なライセンス管理者である必要があります。Web Studio でライセンス情報を表示するには、管理者は少なくとも「ライセンスの読み取り」委任管理権限を持っている必要があります。組み込みの「完全管理者」および「読み取り専用管理者」ロールには、その権限があります。

Web Studio を使用して Citrix からライセンスをダウンロードしてインストールする

1. Web Studio にサインインし、左ペインで**ライセンス**を選択します。
2. アクションバーで**ライセンスの割り当て**を選択します。
3. ライセンスアクセスコードを入力します。これは、ライセンスの購入または更新後に Citrix からメールで受け取ったものです。
4. 製品を選択し、**ライセンスの割り当て**を選択します。その製品で利用可能なライセンスが割り当てられ、ダウンロードされます。特定のライセンスアクセスコードのすべてのライセンスを割り当ててダウンロードした後、そのライセンスアクセスコードを再利用することはできません。同じコードで他の取引を行うには、マイアカウントにログオンしてください。

ローカルコンピューターまたはネットワークに保存されているライセンスを追加する

1. Web Studio にサインインし、左ペインで**ライセンス**を選択します。
2. アクションバーで**ライセンスの追加**を選択します。
3. ライセンスファイルを参照し、ライセンスサーバーに追加します。

ライセンスサーバーを変更する

1. Web Studioにサインインし、左ペインで を選択します。
2. アクションバーで を選択します。
3. ライセンスサーバーのアドレスを *name:port* の形式で入力します。ここで、nameはDNS、NetBIOS、またはIPアドレスです。ポート番号を指定しない場合、デフォルトのポート（27000）が使用されます。

使用するライセンスの種類を選択する

- サイトを構成する際、ライセンスサーバーを指定すると、使用するライセンスの種類を選択するよう求められます。サーバーにライセンスがない場合、ライセンスなしで製品を30日間試用するオプションが自動的に選択されます。
- サーバーにライセンスがある場合、その詳細が表示され、いずれかを選択できます。または、ライセンスファイルをサーバーに追加してから、そのライセンスを選択することもできます。

製品エディションとライセンスモデルを変更する

1. Web Studioにサインインし、左ペインで を選択します。
2. アクションバーで を選択します。

3. 適切なオプションを更新します。

License Administration Consoleにアクセスするには、アクションバーで を選択します。コンソールがすぐに表示されるか、ダッシュボードがパスワードで保護されている場合は、License Administration Consoleの資格情報の入力を求められます。コンソールの使用方法の詳細については、ライセンスドキュメントを参照してください。

> **注:**
>
> Web Studioでライセンスを切り替えると、Citrix Directorに反映されるまでに最大5分かかります。たとえば、AdvancedとPremiumを切り替える場合などです。

ライセンス管理者を追加する

1. Web Studio にサインインし、左ペインで **Licensing** を選択します。
2. **Licensing Administrators** タブを選択します。
3. アクションバーで **Add licensing administrator** を選択します。
4. 管理者として追加するユーザーを参照し、権限を選択します。

ライセンス管理者のアクセス許可を変更またはライセンス管理者を削除する

1. Web Studio にサインインし、左ペインで **Licensing** を選択します。
2. **Licensing Administrators** タブを選択し、管理者を選択します。
3. アクションバーで **Edit licensing administrator** または **Delete licensing administrator** のいずれかを選択します。

ライセンス管理者グループを追加する

1. Web Studio にサインインし、左ペインで **Licensing** を選択します。
2. **Licensing Administrators** タブを選択します。
3. アクションバーで **Add licensing administrator group** を選択します。
4. ライセンス管理者として機能させたいグループを参照し、権限を選択します。Active Directoryグループを追加すると、そのグループ内のユーザーにライセンス管理者権限が付与されます。

ライセンス管理者グループの権限を変更または削除する

1. Web Studio にサインインし、左側のペインで **Licensing** を選択します。
2. **Licensing Administrators** タブを選択し、管理者グループを選択します。
3. アクションバーで、**Edit licensing administrator group** または **Delete licensing administrator group** のいずれかを選択します。

ライセンス情報を表示する

Web Studio にサインインし、左側のペインで **Licensing** を選択します。サイトのライセンス使用状況と設定の概要が、指定されたライセンスサーバーに現在インストールされているすべてのライセンスのリストとともに表示されます。

製品タイプ、ライセンスエディション、ライセンスモデルを含むサイトのライセンス設定が、構成済みのライセンスサーバーが使用するライセンスと一致していることを確認してください。一致しない場合は、サイトのライセンス設定に合わせるために、既存のライセンスをダウンロードまたは割り当てる必要がある場合があります。

次のライセンス情報を取得するには、コマンド `Get-Brokersite` を実行します。

- TotalUniqueLicenseUsers
- PeakConcurrentLicenseUsers
- PeakConcurrentLicensedDevice

> **注:**
>
> Citrix DaaS の情報を取得するには、クラウドライセンスAPIを使用します。クラウドライセンスAPIの詳細については、「APIs to manage Citrix Cloud licensing」を参照してください。

ライセンス有効期限アラートを表示する

Web Studio は、Citrix License Server からライセンスファイルの有効期限を照会します。ライセンスファイルの有効期限が近づいているか、すでに期限切れになっている場合、Web Studio は概要タブで管理者にアラートを表示します。

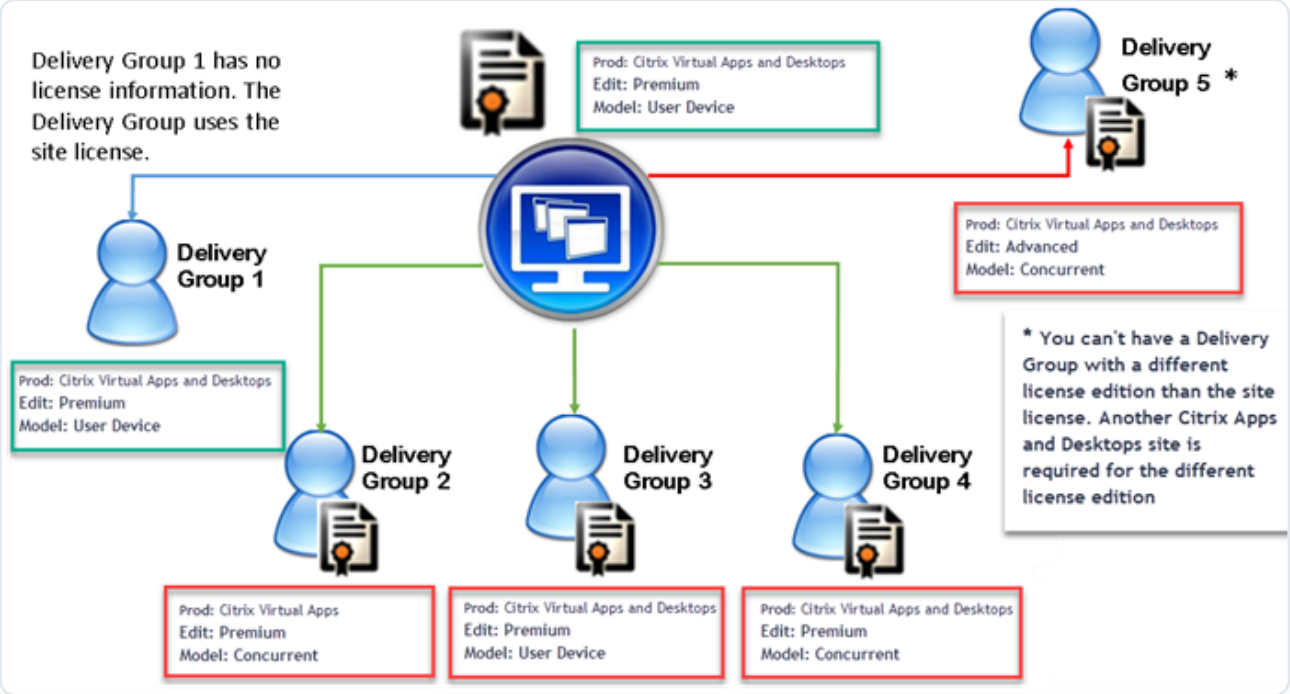
関連リンク

- 「Citrix オンプレミス年間および期間ベースのリテールライセンスのサブスクリプション」(/ja-jp/licensing/current-release/license-types.html#citrix-on-premises-subscription-for-annual-and-term-based-retail-licenses)を参照してください。
- 「ハイブリッド権限による移行とアップグレード (TTU)」(/ja-jp/licensing/current-release/hybrid-rights-ttu.html)を参照してください。

マルチタイプライセンス

マルチタイプライセンスは、単一のCitrix Virtual Apps and Desktopsサイト上のデリバリーグループに対して、異なるライセンスタイプの消費をサポートします。**タイプ**とは、製品ID（XDTまたはMPS）とモデル（UserDeviceまたはConcurrent）の単一の組み合わせです。デリバリーグループは、サイトレベルで構成されているものと同じ製品エディション（PLT/PremiumまたはENT/Advanced）を使用する必要があります。Citrix Virtual Apps and Desktops展開環境でマルチタイプライセンスを構成する際には、この記事の最後にある特別な考慮事項に注意してください。

マルチタイプライセンスが構成されていない場合、異なるライセンスタイプは、個別のサイト用に構成されている場合にのみ使用できます。デリバリーグループはサイトライセンスを使用します。マルチタイプライセンスが構成されている場合の重要な通知の制限については、特別な考慮事項 を参照してください。



異なる種類のライセンスを消費するデリバリーグループを特定するには、以下の Broker PowerShell コマンドレットを使用します。

- New-BrokerDesktopGroup

- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

ライセンスをインストールするには、次を使用します。

- シトリックス スタジオ
- シトリックス ライセンシング マネージャー
- citrix.com

Customer Success Servicesの有効期限は、各ライセンスファイル、各製品、および各モデルに固有です。異なる設定のデリバリーグループは、互いに異なるCustomer Success Servicesの有効期限を持つ場合があります。

特別な考慮事項

マルチタイプライセンスは、通常のCitrix Virtual Apps and Desktops™ライセンスとは異なる機能があります。

DirectorまたはStudioからは、サイト構成とは異なるタイプを使用するように構成されたデリバリーグループに対するアラートや通知はありません。

- ライセンス制限に近づいている場合、またはライセンスバーストモードのトリガーや有効期限切れに関する情報はありません。
- 特定のグループに問題がある場合の通知はありません。

マルチタイプライセンス用に構成されたデリバリーグループは、そのライセンスタイプのみを消費し、完全に消費されてもサイト構成にフォールバックしません。

Citrix Virtual Apps StandardとCitrix Virtual Desktops™ Standardのライセンスエディション名はどちらもStandardであることを示していますが、これらは同じエディションではありません。マルチタイプライセンスは、Citrix Virtual Apps StandardおよびCitrix Virtual Desktop Standardライセンスでは利用できません。

ライセンス互換性マトリックス

この表は、古い製品名、新しい製品名、および関連する機能名を詳述しています。4つの互換性列は、マルチタイプライセンスで互換性のある製品とライセンスモデルの組み合わせを指定します。CCUとCCSは同時使用ライセンスを表し、UDはユーザー/デバイスライセンスを表します。

ライセンス互換性マトリックスと新旧の名称(/en-us/citrix-virtual-apps-desktops/2407/media/multi-type-compatibility-names.png)

ブローカー PowerShell SDK

DesktopGroupオブジェクトには、関連するNew-BrokerDesktopGroupおよびSet-BrokerDesktopGroupコマンドレットを使用して操作できるこれら2つのプロパティがあります。

名前	値	制限
LicenseModel	グループのライセンスモデルを指定するパラメーター（ConcurrentまたはUserDevice）。何も指定されていない場合、サイト全体のライセンスモデルが使用されます。	機能トグルが無効になっている場合、プロパティを設定しようとすると失敗します。
ProductCode	グループのライセンス製品IDを指定するXDT（Citrix Virtual Desktopsの場合）またはMPS（Citrix Virtual Apps™の場合）のテキスト文字列。何も指定されていない場合、サイト全体の製品コードが使用されます。	機能トグルが無効になっている場合、プロパティを設定しようとすると失敗します。

LicenseModelとProductCodeの詳細については、about_Broker_Licensingを参照してください。

New-BrokerDesktopGroup

デスクトップグループのブローカーを管理するためのデスクトップグループを作成します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/>`を参照してください。

Set-BrokerDesktopGroup

既存のブローカーデスクトップグループを無効または有効にするか、その設定を変更します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`を参照してください。

Get-BrokerDesktopGroup

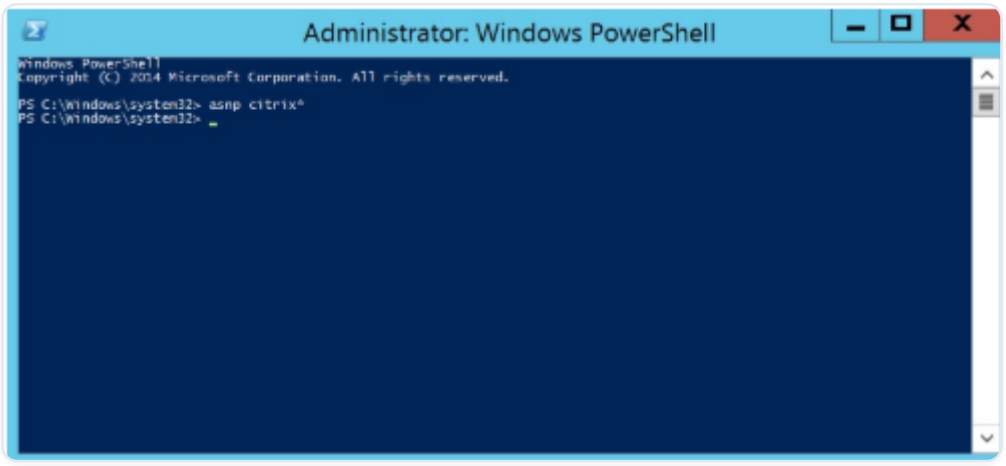
指定された条件に一致するデスクトップグループを取得します。Get-BrokerDesktopGroupコマンドレットの出力には、グループの**ProductCode**および**LicenseModel**プロパティが含まれます。New-BrokerDesktopGroupまたはSet-BrokerDesktopGroupを使用してプロパティが設定されていない場合、null値が返されます。nullの場合、サイト全体のライセンスモデルと製品コードが使用さ

れます。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/>`を参照してください。

デリバリーグループごとに異なるライセンス製品とモデルを構成する

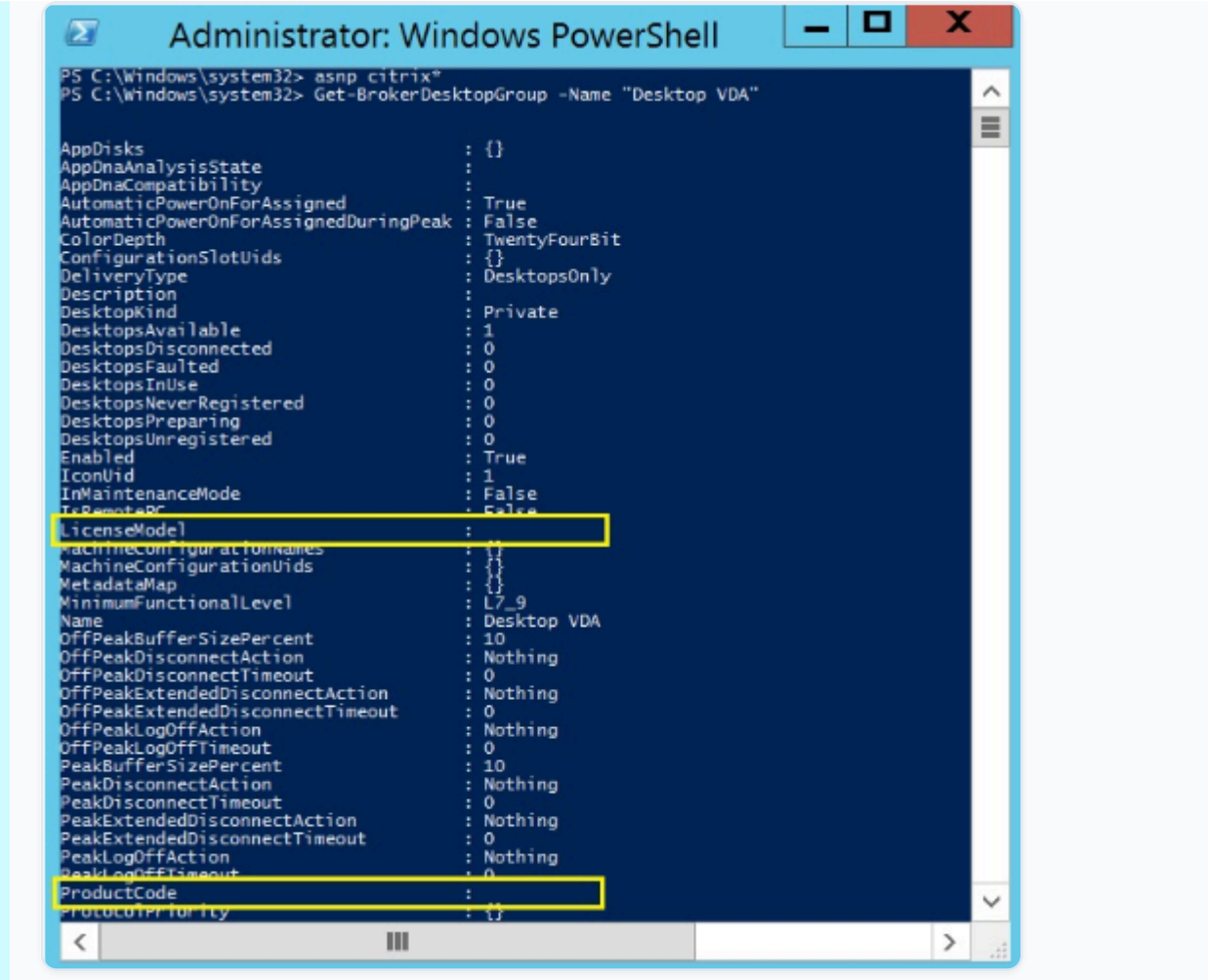
> **注:**
>
> 単一のデリバリーグループで、2つ以上の異なる種類の製品、エディション、またはライセンスモデルを構成することはできません。異なる種類の製品、エディション、またはライセンスモデルがある場合は、それらを別々のデリバリーグループで構成してください。

1. 管理者権限でPowerShellを開き、Citrixスナップインを追加します。

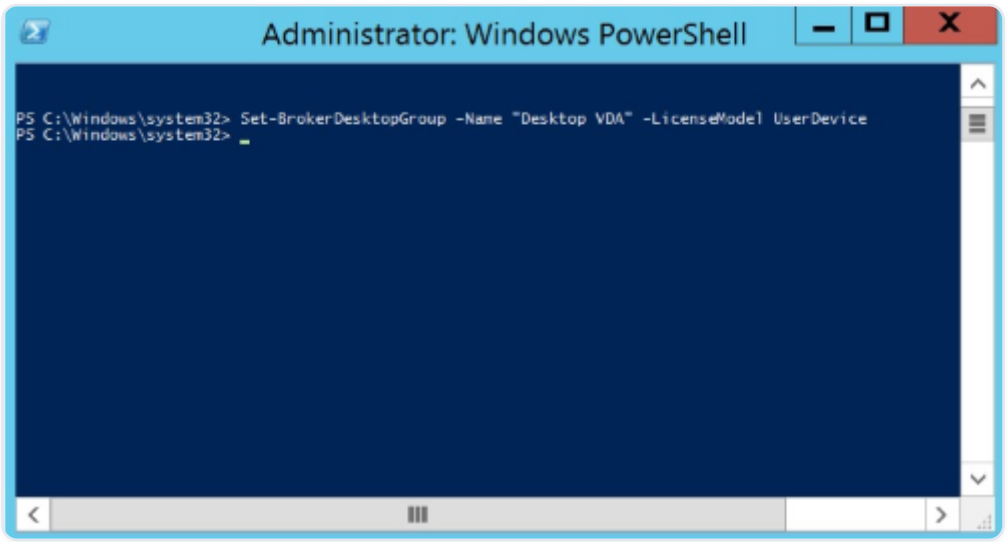


2. 「**Get-BrokerDesktopGroup –Name “DeliveryGroupName”**」コマンドを実行して、現在のライセンス構成を表示します。**LicenseModel** と **ProductCode** パラメーターを見つけてください。これらのパラメーターを以前に構成していない場合、空白になっている可能性があります。

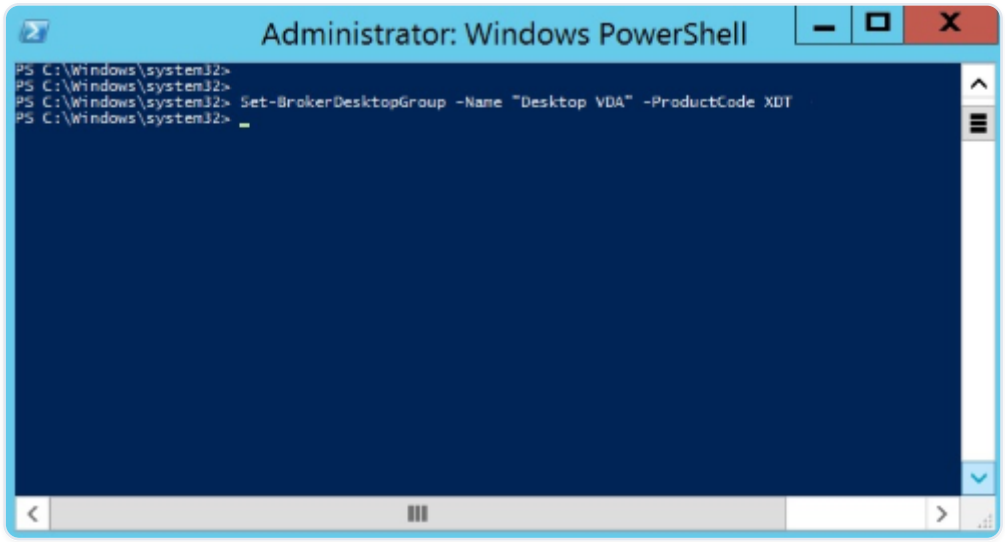
> **注:**
>
> デリバリーグループにライセンス情報が設定されていない場合、デフォルトで**サイトレベルのサイトライセンス**になります。



3. 次のコマンドを実行して、ライセンスモデルを変更します: **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –LicenseModel LicenseModel**。

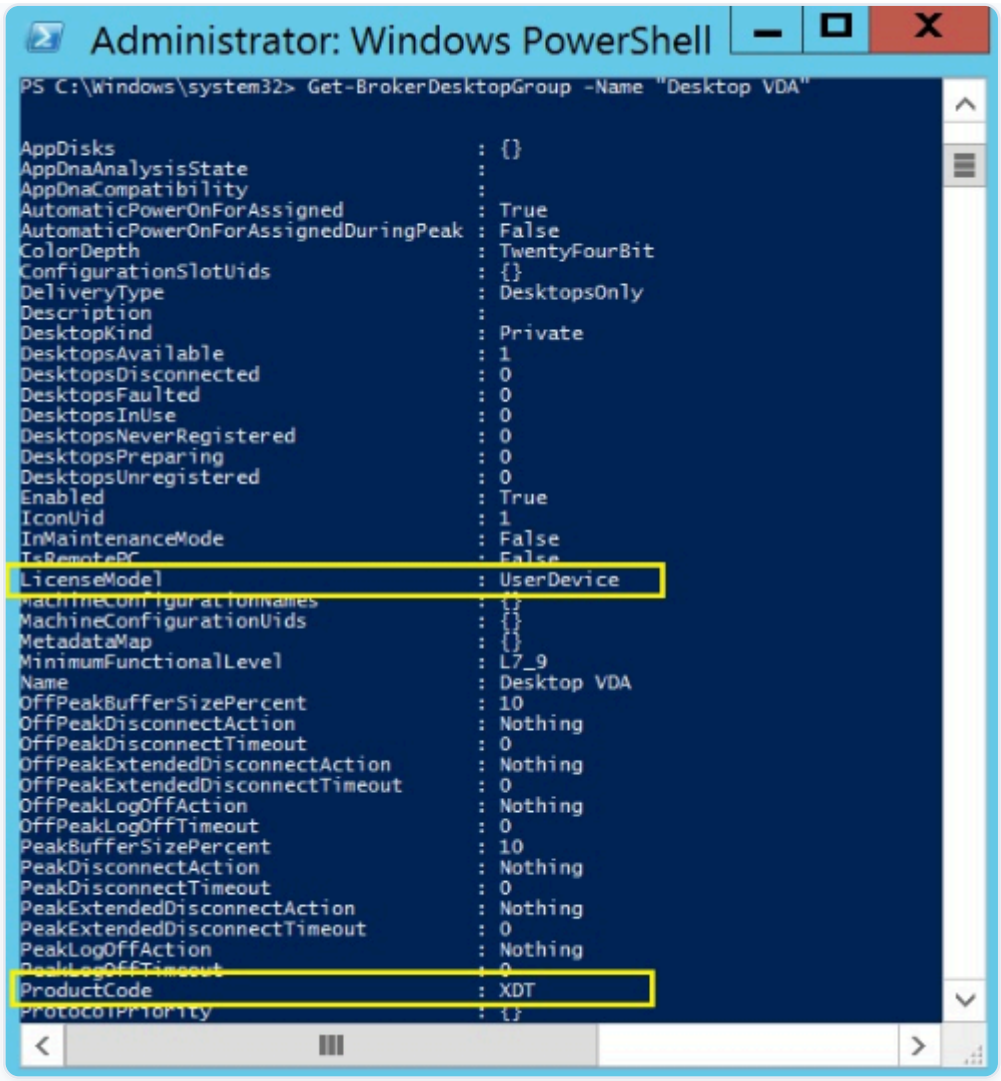


4. 次のコマンドを実行して、ライセンス製品を変更します: **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –ProductCode ProductCode**。



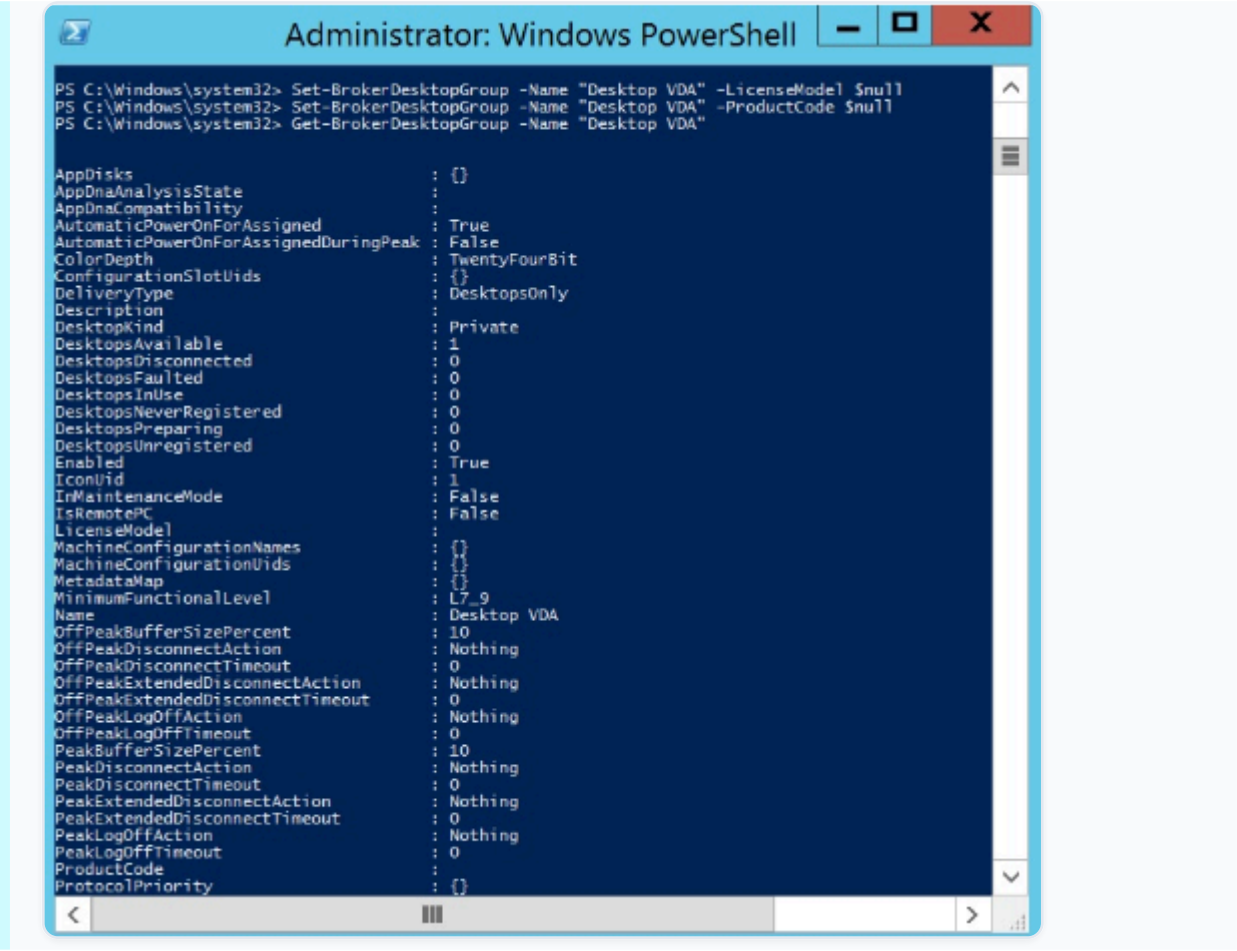
5. 変更を検証するには、**Get-BrokerDesktopGroup –Name “DeliveryGroupName”** コマンドを入力します。

> **注:**
>
> 同じサイト内でエディションを混在させることはできません。たとえば、Premiumライセンスと Advancedライセンスなどです。異なるエディションのライセンスがある場合は、複数のサイトが必要です。



6. 前述の手順で説明したのと同じ **Set-BrokerDesktopGroup** コマンドを実行し、値を **$null** に設定して、ライセンス構成を削除します。

> **注:**
>
> Studioでは、各デリバリーグループのライセンス構成は表示されません。現在の構成を表示するには、PowerShellを使用します。



例

このPowerShellコマンドレットの例は、既存の2つのデリバリーグループに対するマルチタイプライセンスの設定方法を示し、3つ目のデリバリーグループを作成して設定します。

デリバリーグループに関連付けられているライセンス製品とライセンスモデルを確認するには、**Get-BrokerDesktopGroup** PowerShellコマンドレットを使用します。

1. 最初のデリバリーグループをXenApp®とConcurrentに設定します。

   Set-BrokerDesktopGroup -Name "シトリックス バーチャル アプリ プレミアム コンカレント用デリバリーグループ" -ProductCode MPS -LicenseModel Concurrent

2. 2番目のデリバリーグループをXenDesktop®とConcurrentに設定します。

   Set-BrokerDesktopGroup -Name "シトリックス バーチャル デスクトップ プレミアム コンカレント 用デリバリーグループ" -ProductCode XDT -LicenseModel Concurrent

3. 3番目のデリバリーグループをXenDesktopとUserDeviceに対して作成し設定します。

New-BrokerDesktopGroup -Name "Citrix Virtual Desktops Premium UserDevice 用デリバリーグループ" -PublishedName "マイデスクトップ" -DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

Citrix Virtual Apps and Desktops™ テレメトリーデータ要素

ブローカー

使用方法

ヘッダー

キー	説明	例
バージョン	テレメトリーイベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	SendBrokerTelemetryData
st	Brokerでイベントが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
製品	使用状況イベントの元の製品と展開を識別します。	XenDesktop.Broker (クラウド) OnPrem.Broker (OnPrem)
prodVer	Citrix DaaS/Citrix Virtual Apps and Desktops の製品バージョンを示します。	7.25.0.0

ペイロード

フィールド	説明	例
TotalPublishedApps	公開されているアプリケーションの総数を示します。	10
TotalPublishedDesktops	公開されているデスクトップの総数を示します。	10
VDAs.Total	VDA の総数を示します。	10
VDAs.OSTypes	Windows、Linux、Mac などの OS タイプ別の VDA の総数を示します。	10
VDAs.OSVersions	Windows 10、11、2022、2019などのOSバージョンごとの合計数を示します。	10
VDAs.HostingLocations.Azure	Azure、AWS、GCP、Nutanix、VMWare、XenServer、HyperVなど、サポートされている各ホスティングロケーションのVDAの数を示します。	10
VDAs.HostingLocations.AWS		
VDAs.HostingLocations.Nutanix		
VDAs.HostingLocations.VMWare		
VDAs.HostingLocations.XenServer		
VDAs.HostingLocations.HyperV		
VDAs.ProvisionedMethod.MCS	Machine Creation Service (MCS) によってプロビジョニングされたマシンの数を示します。	10

フィールド	説明	例
VDAs.ProvisionedMethod.ManualOr3P	手動または3Pでプロビジョニングされたマシンの数を示します。	10
VDAs.SessionSupport.StaticSingle	静的に割り当てられたシングルセッションのマシンの数を示します。	10
VDAs.SessionSupport.DynamicSingle	動的に割り当てられたシングルセッションのマシンの数を示します。	10
VDAs.SessionSupport.Multi	マルチセッションマシンの総数を示します。	10
VDAs.RemotePCAccess.Windows	OSタイプ (Win、Mac、Linux) 別のRemote PC Accessマシンの数を示します。	10
VDAs.RemotePCAccess.Linux		
VDAs.RemotePCAccess.MacOS		
VDAs.ActiveSessionRecordingAgents	アクティブなセッション記録エージェントを持つVDAの数を示します。	5
VDAs.Subscriptions	VDAのパブリッククラウドサブスクリプションの数を示します。	2
VDAs.LocationTypes	VDAのロケーションタイプの数を示します。	2
AutoScale.DGWithAutoscaleEnabled	**Autoscale** が有効なデリバリーグループの数を示します。	2
AutoScale.TotalMachinesCtrlByAutoscale	Autoscaleによって制御されるマシンの数を示します。	5

フィールド	説明	例
AutoScale.VerticalAutoscaleEnabledByDGandSite	DGおよびサイトによって**垂直オートスケール**が有効になっているマシンの数を示します。	2
AutoScale.TaggedBasedAutoscaledDG	タグベースのオートスケールされたデリバリーグループの数を示します。	2
DeliveryGroup.TotalRebootSchedulesEnabled	**再起動スケジュール**が有効になっているデリバリーグループの数を示します。	2
DeliveryGroup.Total	デリバリーグループの総数を示します。	10
Policy.TotalPolicySets	ポリシーセットの数を示します。	3
Policy.TotalPolicies	グループポリシーの数を示します。	2
Policy.TotalPolicySettings	グループ設定の数を示します。	2
PublishedPackageApps.AppVSingleAdmin	AppVシングル管理者モードで公開されているパッケージアプリの総数を示します。	2
PublishedPackageApps.AppVDualAdmin	AppVデュアル管理者モードで公開されているパッケージアプリの総数を示します。	2
PublishedPackageApps.Msix	MSIXモードで公開されているパッケージアプリの総数を示します。	2
PublishedPackageApps.AppAttach	AppAttachモードで公開されたパッケージ化されたアプリの総数を示します。	2

フィールド	説明	例
PublishedPackageApps.FlexApp	FlexAppモードで公開されたパッケージ化されたアプリの総数を示します。	2

セッション

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	Cloud.Licensing
st	Broker でイベントが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
製品	使用状況イベントの発生元製品と展開を識別します。	XenDesktop.Broker (クラウド) OnPrem.Broker (OnPrem)
prodVer	Citrix DaaS または Citrix Virtual Apps and Desktops の製品バージョンを示します。	7.25.0.0

フィールド	説明	例
ユーザー	セッション起動を開始するユーザーを一意に識別するためのユーザーIDを特定します。**値はスクランブル化されています。**	fullName: C648FE671A44B3F7 **(常にスクランブル化されています)** samName:C758LH671A44B3F7 **(常にスクランブル化されています)** upn: C7948FE671A44B3F7 **(常にスクランブル化されています)** userLicenseId:C265FE671A44B3F7 **(常にスクランブル化されています)**
		userSid: C097FE671A44B3F7 **(常にスクランブル化されています)**
テナントのID	Citrix Cloud™アカウントの顧客IDを示します。オンプレミス展開の場合、このフィールドは適用されず、値はありません。	ジョジイチエムエイチゼロゴキュウハチティージェイ
デバイスのデバイスID	セッション起動が開始されたデバイスを一意に識別するためのデバイスIDを示します。	AE18C4D5

フィールド	説明	例
デバイスのデバイス名	デバイスのフレンドリ名を示します。**値はスクランブル化されています。**	C758LH671A44B3F7 **(常にスクランブル化されています)**

ペイロード

フィールド	説明	例
appProtectionKeyLoggingRequired	セッションがキーロギング保護を有効にして起動されたかどうかを示します。	偽
appProtectionScreenCaptureRequired	セッションが画面キャプチャ保護を有効にして起動されたかどうかを示します。	偽
cspTenantCustomerId	CSPテナントのCitrix Cloudアカウントの顧客IDを示します。オンプレミス展開の場合、このフィールドは適用されず、値はありません。	ロクシーツーブイティーエックスジーエックスワイエフティーティー
isAnonymousUser	認証されていないセッションが起動されたかどうかを示します。	偽
licenseActivityTimeStamp	ペイロードが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
licenseActivityType	ライセンスイベントの種類を示します。このフィールドは、ライセンスイベント	接続

フィールド	説明	例
	の種類が割り当てアクション用か、解放アクション用かを示します。	
licenseModel	展開のライセンスモデルを示します。	UserDevice
productEdition	展開の製品エディションを示します。	プレミアム
productId	展開内の製品の製品IDを示します。	CAVDS
プロトコル	セッションの起動に使用されたプロトコルを示します。	HDX™
sessionKey	セッションの一意の識別子を示します。	uq390c5fc3-86eb-4df3-bd9a-f4a8fed2c9e2
sessionSupport	セッションサポートの種類を示します。	SingleSession
sessionType	セッションの種類を示します。	アプリケーション
バージョン	ペイロードのバージョンを示します。	1.3
workerSid	セッションに使用されるVDAの一意の識別子を示します。**値はスクランブル化されています。**	1E5LH671A44B3F7 **(常にスクランブル化されています)**
isWindows365	セッションがWindows 365向けに起動されたかどうかを示します。	はい

フィールド	説明	例
entitlementType	顧客のライセンスエンタイトルメントの種類を示します。	本番
siteId	サイトの一意の識別子を示します。	a35647d0-901c-4477-87e0-dcd781d455f4
desktopGroupId	デスクトップまたはデリバリーグループの一意の識別子を示します。	e9d859dc-1bfc-4b3e-bad3-41806bb4e694
clientType	Citrix Workspace™ アプリのタイプを示します。	ウィンドウズ
clientVersion	Citrix Workspaceアプリのバージョンを示します。	23.5.1.83
workerCloudType	VDAプロビジョニングに使用されるパブリッククラウドの種類を示します。	アジュール
enabledFeatures	セッションで有効になっている機能を示します。たとえば、`AppProtectionScreenCaptureRequired` と `SessionRecording` が有効になっているセッションでは、このフィールドの値は66です。	66
launchRequestSource	起動を要求するために使用された製品を記録します。オンプ	0 (StoreFront or 3P)

フィールド	説明	例
	レミスの StoreFront™またはCloud StoreFrontのいずれかです。	1 (ワークスペース)
isEvents	{{page.lic}}における重大な障害を示します。	STデータベースを作成できません。
heartBeatTime	CISまたはCitrix Analytic Serviceへのライセンスサーバーのハートビート時間を示します。	1689058813
vdaTelemetry	App Layering、User Personalization Layer、User Profile management、Workspace Environment Management™、およびHDX機能のためにキャプチャされるペイロードを示します。	vdaTelemetry SessionTelemetry CPM_feature: 32 HDX1: 66 HDX2: 0 MachineTelemetry AL_productVersion: 23.12.0.1001 UPL_isEnabled: 1 CPMのバージョン: 22.3.4000 wem_enableMethod: 1 wem_agentVersion: 2402.1

スタジオ

使用方法

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	8c2e20a5-ca3f-4401-ad69-d037933c40a0
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別するために使用するイベントの種類を示します。	Studio.Usage
st	Studio でイベントが生成されたときのタイムスタンプを示します。	2024-03-22T01:32:23.4056195Z
プロダクション	使用状況イベントの元の製品と展開を識別します。	XenDesktop.Studio
prodVer	Citrix DaaS/Citrix Virtual Apps and Desktops の製品バージョンを示します	7.42.0.0

ペイロード

フィールド	説明	例
AdminLoginList	一意の管理者 SamAccountName のリストを示します。**値はスクランブルされています。**	{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw= =]}**(常にスクランブルされます)**
TotalApiRequests	オーケストレーションサービスのAPIリクエストを示します。	{TotalApiRequests: 1000}

フィールド	説明	例
BackupCount	Studio管理者によって操作されたバックアップの数を示します。	{BackupCount: 200}
RestoreCount	Studio管理者によって実行された復元回数を示します。	{RestoreCount: 20}

ディレクター

使用状況レポート

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	8c2e20a5-ca3f-4401-ad69-d037933c40a0
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	テレメトリ
st	Studio でイベントが生成されたときのタイムスタンプを示します。	2024-03-22T01:32:23.4056195Z
製品	使用状況イベントの発生元となる製品と展開を識別します。	XenApp.Monitor
prodVer	Director の製品バージョンを示します。	7.42.0.0

ペイロード

フィールド	説明	例
AdminLoginCount	これは、管理者のログイン数を提供するペイロードのセクションです。	タイプ: AdminLogin 統計 0: 1 1: 7
FeatureUsageCount	このペイロードのセクションには、Director で使用される主要な機能の数が含まれています。	タイプ: FeatureUsage 統計情報 0: 15 1: 20 5: 10
OdataUsageCount	このペイロードのセクションには、Odata API の使用回数が含まれています	タイプ: OData_v3 統計 0: 1 2: 7 5: 9 タイプ: OData_v4 統計 0: 1 2: 8 6: 7
AppUsage	公開されたアプリケーションの週次使用状況メトリックを示します。	種類: AppUsage ヘッダー: applicationName,pr

フィールド	説明	例
		ocessName,totalDurationInMinutes 期間: 01/05/24-07/05/24 値: [Calc_AWTSVDA-1907R,calc.exe,0.13, Notepad_AWTSVDA-1907R,notepad.exe,4]
UniqueAppUsers	公開されたアプリケーションについて、1か月間のユニークユーザー数とアプリケーションの合計起動数を示します。	種類: UniqueAppUsers ヘッダー: applicationName,totalLaunches,totalUniqueUsers 期間: 04/24 値: [Calc_AWTSVDA-1907R,100,10, Notepad_AWTSVDA-1907R,200,20]
DesktopUsage	公開されたデスクトップの週ごとの使用状況メトリックを示します。	タイプ: DesktopUsage ヘッダー: desktopGroupName,sessionSupport,totalDurationInMinutes

フィールド	説明	例
		期間: 01/05/24-07/05/24 値: [RdsDesktopAndAppGroup,1,10]
UniqueDesktopUsers	公開デスクトップの月間合計起動数とともに、ユニークユーザーの数を表します。	タイプ: UniqueDesktopUsers ヘッダー: desktopGroupName,totalLaunches,totalUniqueUsers 期間: 04/24 値: [RdsDesktopAndAppGroup,10,5]
AvgLogonDuration	平均ログオン期間を示します。	タイプ: 平均ログオン時間 ヘッダー: 総ユーザーログオン数, 平均ログオン時間（秒） 期間: 01/05/24-07/05/24 値: [200,4]
CostSaved	顧客が1か月に節約したコストを示します。	タイプ: CostSaved

フィールド	説明	例	
		ヘッダー: ハイパーバイザー,削減コスト,通貨 期間: 04/24 値: [	
		1,221.02,1	
		2,301.02,2]	

委任管理

使用方法

ヘッダー

キー	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用イベントの一意の識別子を示します。	8c2e20a5-ca3f-4401-ad69-d037933c40a0
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別するために使用するイベントの種類を示します。	DelegatedAdmin.Usage
st	Delegated Admin でイベントが生成されたときのタイムスタンプを示します。	2024-03-22T01:32:23.4056195Z
製品	使用イベントの発生元の製品と展開を識別します。	XenDesktop.DelegatedAdmin (クラウド)
		OnPrem.DelegatedAdmin (OnPrem)

キー	説明	例
prodVer	Citrix DaaS または Citrix Virtual Apps and Desktops の製品バージョンを示します。	7.42.0.0

ペイロード

キー	説明	例
TotalCustomScopes	カスタムスコープの総数を示します。	2
TotalCustomRoles	カスタムロールの総数を示します。	4

ライセンス テレメトリー データのスクランブル

ライセンス テレメトリで送信される情報の機密性を考慮し、Citrix はデータを難読化するオプションを提供します。

次の表に、難読化できるデータを示します。

フィールド	説明	例
ユーザー	セッション起動を開始するユーザーを一意に識別するためのユーザー ID を識別します。	• fullName: `C648FE671A44B3F7` • samName: `C758LH671A44B3F7` • ユーザープリンシパル名: `C7948FE671A44B3F7` • userLicenseId: `C265FE671A44B3F7`

フィールド	説明	例
		• userSid: `C097FE671A44B3F7`
デバイス -> デバイス名	デバイスのフレンドリ名を示します。	`C758LH671A44B3F7`
workerSid	セッションに使用されるVDAの一意の識別子を示します。	`1E5LH671A44B3F7`
AdminLoginList	一意の管理者SamAccountNameのリストを示します	`{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw= =]}`

スクランブルを有効または無効にするには、Delivery Controllerで次のPowerShellコマンドを実行します。

> **注:**
>
> Citrix Service Provider™ (CSP) のお客様の場合、スクランブルは常に無効になっています。CSP のお客様は、PowerShell コマンドを使用してスクランブルを有効にすることはできません。

1. Delivery Controller ホストから PowerShell ウィンドウを開きます。
2. コマンド `asnp citrix` を実行して、Citrix 固有の PowerShell モジュールをロードします。
3. 次のコマンドを実行して、スクランブルを有効または無効にします。

   デフォルトでは、値は `1` または `true` であり、これによりライセンス テレメトリ データのスクランブルが有効になります。

   無効にするには：

   ```
   Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
   -SettingValue $false
   ```

スクランブルを無効にした後、次のコマンドを使用して有効にできます。

```
Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
-SettingValue $true
```

ライセンスに関するFAQ

注:

- COVID-19パンデミックに関連する事業継続リソースについては、CTX27055を参照してください。
- 事業継続の維持に関する一般情報については、Business continuity — on demandを参照してください。
- 現在のCitrix License Serverに関する詳細については、Licensingを参照してください。

Citrix®ライセンス

ライセンスファイルはどのように入手できますか?

ライセンスアクセスコードは電子メールで送信されます。ライセンスアクセスコードを使用してライセンスファイルを生成する方法は3つあります。

- `citrix.com`のMyAccountページにある**Manage Licenses**。詳細については、Manage licenses on citrix.comを参照してください。
- Web Studioでご購入を割り当てると、ライセンスファイルがCitrix License Serverに自動的にインストールされます。
- Citrix License Server内のCitrix Licensing Managerでご購入を割り当て、ライセンスファイルをインストールします。詳細については、Install icensesを参照してください。

MyAccountでライセンスを割り当てる方法?

ライセンスの割り当てを参照してください。

割り当てられたライセンスをライセンスサーバーに追加する方法?

ライセンスの変更を参照してください。

Citrixライセンスはどのポートを使用しますか?

- ライセンスサーバーのポート番号は27000です。
- ベンダーデーモンのポート番号は7279です。
- ライセンス用Webサービスのポートは8083です。

Citrixライセンスサーバーとは何ですか?

Citrixライセンスサーバーは、ネットワーク全体でライセンスを共有できるシステムです。詳細については、「ライセンス操作の概要」を参照してください。

Citrixライセンスサーバーを仮想化またはクラスター化できますか?

はい。Citrixライセンスサーバーを仮想化またはクラスター化できます。詳しくは、「クラスター化されたライセンスサーバー」を参照してください。

Citrixライセンスサーバーを仮想化すると、どのようなメリットがありますか?

Citrixライセンスサーバーを仮想化することで、冗長なソリューションが提供されます。このソリューションにより、ダウンタイムなしで複数の物理サーバー間を移動できます。

Citrixライセンスサーバーを仮想化する場合、考慮すべき制限はありますか?

いいえ。

Citrixライセンスサーバーは、Citrix Virtual Apps and Desktops™展開のすべてのライセンスを管理しますか?

Citrixライセンスサーバーは、Citrix Gatewayで使用されるPremium Editionのライセンスを除く、Citrix Virtual Apps™ and Desktopで受け取るすべてのライセンスを管理します。これらのセキュリティ指向のネットワークデバイスに必要な、ネットワークアプライアンスに組み込まれたライセンスサーバーが、それらのライセンスを管理します。

Citrix Licensing Managerとは何ですか?

Citrix Licensing Managerを使用すると、Citrix Licensing Managerをインストールしたライセンスサーバーからライセンスファイルをダウンロードして割り当てることができます。Citrix Licensing Managerは、推奨されるライセンスサーバー管理方法であり、次の機能を提供します。

- ライセンスサーバーのCitrix Cloud™へのショートコード登録と、登録の簡単な削除。
- ユーザーアカウントとグループアカウントを構成します。
- ダッシュボードを使用して、インストール済み、使用中、期限切れ、利用可能なライセンス、およびCustomer Success Servicesの期日を表示します。
- レポート作成に使用するため、ライセンス使用状況データをエクスポートします。

- 履歴使用状況データの保持期間を構成します。デフォルトのデータ保持期間は180日です。
- ライセンスアクセスコードまたはダウンロードしたファイルを使用して、ライセンスサーバーへのライセンスファイルのインストールを簡素化します。
- ライセンスバーストモードを有効化および無効化します。
- カスタマーエクスペリエンス向上プログラム (CEIP) と コールホーム を構成します。
- Customer Success Servicesの更新ライセンスを自動的または手動で確認し、見つかった場合は通知するか、ライセンスをインストールします。
- ライセンスサーバーの状態（起動ライセンスの不足、時間の問題、アップローダーの障害）を通知します。
- これらのポートを変更します。
  - ライセンスサーバー (デフォルト 27000)
  - ベンダーデーモン (デフォルト 7279)
  - ライセンス用Webサービス (デフォルト 8083)

詳細については、「Citrix Licensing Manager」を参照してください。

Citrix License Administration Consoleはどこにありますか?

License Administration Consoleはサポートされなくなり、License Serverバージョン11.16.6から削除されました。Citrix Licensing Managerを使用することをお勧めします。

License ServerがStudioと同じドメイン内にあるか、信頼されたドメイン内にある場合、Studioを使用してライセンスを管理および追跡できます。

詳細については、「Citrix Licensing Manager」を参照してください。

ライセンス割り当て期間とは何ですか?

ライセンス割り当て期間とは、Citrix Virtual Apps and Desktopsライセンスがユーザーまたはデバイスに割り当てられる期間のことです。デフォルトのライセンス割り当て期間は90日です。

組織が購入したライセンス数を確認する方法?

購入したすべてのライセンスは、`<https://www.citrix.com>`の**My Account**ページの安全な**Manage Licenses**ツールボックスからいつでも（24時間365日）確認およびアクセスできます。

いつでも使用中のライセンス数を確認する方法?

Citrix Licensing ManagerとStudioは、リアルタイムのライセンス使用状況に関する詳細を提供します。

License Serverのディザスターリカバリとメンテナンス

License Serverのディザスターリカバリとメンテナンスについては、Citrix Licensingドキュメントの Disaster recovery and maintenance を参照してください。

Citrix Virtual Apps and Desktopsのライセンス

Citrix Virtual Apps and Desktopsのライセンス方法?

Citrix Virtual Apps and Desktops のライセンスは、ユーザー/デバイスおよび同時使用ライセンスモデルを提供します。

ユーザー/デバイス:

柔軟なユーザー/デバイスモデルは、以下と連携します。

- 全社的なデスクトップ利用。
- 基盤となるMicrosoftデスクトップ仮想化ライセンス。
- 仮想デスクトップやアプリへのアクセスが時々しか必要ないユーザーを持つ顧客向けの同時使用ライセンス。

ユーザー/デバイスライセンスは、ユーザーが無制限の数のデバイスから仮想デスクトップとアプリにアクセスできるようにします。デバイスライセンスは、無制限の数のユーザーが単一のデバイスから仮想デスクトップとアプリにアクセスできるようにします。このアプローチにより、最大限の柔軟性が提供され、Microsoftデスクトップ仮想化ライセンスとの整合性が向上します。

> **重要:**

> ライセンスをユーザーまたはデバイスに手動で割り当てることはできません。ライセンスサーバーまたはクラウドサービスがライセンスを割り当てます。ユーザー/デバイスライセンスでは、一度割り当てられたライセンスは、90日間非アクティブになるまで別のユーザーに割り当てることはできません。

> **同時使用:**

同時使用ライセンスは、任意のユーザーおよび任意のデバイスに対して、無制限の数の仮想アプリおよびデスクトップへの1つの接続を許可します。ライセンスはアクティブなセッション中にのみ消費されます。セッションが切断または終了した場合、ライセンスはプールに戻されます。

ユーザー/デバイスライセンスの詳細については、ユーザー/デバイスライセンス を参照してください。同時使用ライセンスについては、同時使用ライセンス を参照してください。

ライセンス購入前のCitrix Virtual Apps and Desktops試用について?

はい。Citrix Virtual Apps and Desktopsソフトウェアをダウンロードし、試用モードで実行できます。試用モードでは、ライセンスなしで、オンプレミスでCitrix Virtual Apps and Desktopsを30日間、10接続まで使用できます。詳細については、評価ライセンス を参照してください。

Citrix Cloud向けのCitrix DaaS™ (旧Citrix Virtual Apps and Desktopsサービス) は、承認に基づいて試用サービスとして利用できます。詳細については、Citrix担当者にお問い合わせください。

CitrixはCitrix Virtual Apps and Desktopsの同時使用をどのように定義していますか?

Citrix Virtual Apps and Desktops の同時接続モデルでは、任意のユーザーと任意のデバイスに対して、無制限の数の仮想アプリとデスクトップへの単一の接続を許可します。ライセンスはアクティブなセッション中にのみ消費されます。セッションが切断または終了すると、ライセンスは再発行のためにプールに戻されます。詳細については、「同時接続ライセンス」を参照してください。

共通のライセンスサーバーにCitrix Virtual Apps and Desktopsライセンスの複数のエディションを展開できますか?

はい。ライセンスサーバーは、Citrix Virtual Apps と Citrix Virtual Desktops の両方のライセンスを同時に管理します。最新のライセンスサーバーバージョンをインストールすることをお勧めします。お使いのライセンスサーバーのバージョンが最新であるか不明な場合は、Citrix ダウンロードサイトの番号とバージョンを比較して確認してください。

単一のサイトでCitrix Virtual AppsとCitrix Virtual Apps and Desktopsの両方のライセンスを使用できます?

バージョンによっては、単一の Citrix Virtual Apps または Citrix Virtual Apps and Desktops サイトで、ユーザー/デバイスまたは同時接続の両方のライセンスモデルをサポートできます。単一の Citrix Virtual Apps または Citrix Virtual Apps and Desktops サイトでサポートできるエディションは1つだけです。詳細については、「複数タイプライセンス」を参照してください。

マルチタイプライセンスをサポートする最小バージョンは、XenAppおよびXenDesktop 7.15 Long Term Service Release (LTSR) とCitrix Virtual Apps and Desktops 7 1808です。

ライセンスサーバーに Citrix Virtual Apps and Desktops のユーザー/デバイスライセンスまたは Citrix Virtual Apps and Desktops の同時接続ライセンスがインストールされている場合、製品モデルとして Citrix Virtual Apps の同時接続を選択できますか?

Citrix Virtual Apps and Desktops Advanced または Premium Edition の機能として Citrix Virtual Apps を使用する場合、そのライセンスモデルは、当該 Advanced または Premium Edition と同じになります。Citrix Virtual Apps and Desktops を購入した場合、Citrix Virtual Apps の機能のみを使用する予定であっても、ライセンスを本製品として構成してください。製品モデルとして Citrix

Virtual Apps を選択するのは、ライセンスサーバーにその同時使用スタンドアロンライセンスがインストールされている場合に限られます。

各 Citrix Virtual Apps および Citrix Virtual Apps and Desktops エディションには、どのような製品コンポーネントが含まれていますか?

エディションごとの全機能マトリックスについては、「Citrix Virtual Apps and Desktopsの機能」を参照してください。

Citrix Virtual Apps and Desktops EULA に準拠して Citrix Virtual Desktops™ 環境のライセンスを付与するにはどうすればよいですか?

Citrix Virtual Apps and Desktops EULAに準拠して、ユーザー/デバイスまたは同時接続ライセンスモデルでCitrix Virtual Apps and Desktopsを展開するには、ライセンスファイルをライセンスサーバーに適用します。ライセンスサーバーは、ライセンスコンプライアンスを制御および監視します。購入した製品に基づいて製品を構成することをお勧めします。たとえば、Citrix Virtual Apps and Desktops Premiumを購入したが、Citrix Virtual Apps機能のみを使用したい場合は、コンプライアンスを満たすために製品をCitrix Virtual Apps and Desktopsに構成してください。詳細については、「製品ライセンスコンプライアンスセンター」を参照してください。

Citrix Virtual Apps EULA に準拠して Citrix Virtual Apps 環境のライセンスを付与する方法?

Citrix Virtual Apps EULAに準拠して、同時接続ライセンスモデルでCitrix Virtual Appsを展開するには、ライセンスファイルをライセンスサーバーに適用します。ライセンスサーバーは、ライセンスコンプライアンスを制御および監視します。

Citrix Virtual Apps and Desktops Servicing Options: 長期サービスリリース (LTSR) または現在のリリース (CR) にライセンス要件はありますか?

長期サービスリリースなどのCitrix Virtual Apps and Desktops Servicing Optionsは、Customer Success Servicesプログラムの特典です。LTSRの特典を利用する資格を得るには、アクティブなCustomer Success Servicesが必要です。詳細については、[Citrix Virtual Apps、Citrix Virtual Apps and Desktops、およびXenServer Servicing Optionsを参照してください。

Remote Browser Isolation (RBI) サービスのプールされた時間はどのように機能します?

サービスを25ユーザー以上購入すると、すべてのユーザーで共有される5000時間のサービス使用権が付与されます。その後のユーザー権利の購入によって、プールされた時間の権利が増えることはありません。サービス時間の権利を増やすには、アドオンパックを購入してください。

CCUライセンスでRemote PC Accessを使用できます?

はい。

Remote PC Accessに関する情報については、Remote PC Accessを参照してください。

Citrix環境のソフトウェアメンテナンスが期限切れになった場合、どうなりますか?

ソフトウェアメンテナンス (SWM) またはサブスクリプションが期限切れになると、ソフトウェアアップグレードとテクニカルサポートへのアクセスが一時停止されます。また、ライセンスの種類と製品バージョンに応じて、エンドユーザーと管理者は、環境がサポートされていないことを示す特定の警告通知を受け取ります。

これらの通知は、サーバー上のすべてのライセンスが期限切れになった場合にのみトリガーされます。

エンドユーザーエクスペリエンス

ユーザーはセッション起動後に警告メッセージを受け取ります。メッセージには次のように表示されます。

```
Citrix Virtual Apps and Desktops warning: Your corporate Citrix
environment is currently unsupported. Please contact your IT department to
resolve.
```

管理者エクスペリエンス

管理者は、Citrix Studioコンソール内で、今後の期限切れまたはアクティブな期限切れを警告するアラートを目にします。

ライセンスの種類別の期限切れの動作

これらのメッセージの表示タイミングは、ライセンスの種類とインストールされているCitrix Virtual Apps and Desktopsのバージョンによって異なります。

オンプレミスサブスクリプションライセンス

- エンドユーザー警告：サブスクリプションの有効期限が切れた後、猶予期間中に表示されます。
- 管理者警告：サブスクリプションの有効期限が切れる30日前にStudioに表示されます。
- サポートされるバージョン：
  - 現在のリリース：Citrix Virtual Apps and Desktops 2411以降。
  - LTSR：2203 CU6、2402 CU1、およびそれ以降のLTSRリリース

ユーザーまたはデバイスライセンス

Citrixは、ユーザー/デバイスライセンスモデルでユーザーにライセンスをどのように割り当てますか?

ユーザー/デバイスライセンスモデルでは、ライセンスサーバーは一意のユーザーIDにライセンスを割り当てます。これにより、その単一ユーザーは無制限のデバイスから無制限の接続を行うことができます。ユーザーがデスクトップまたはデバイスに接続する場合、仮想デスクトップまたはアプリケーションにアクセスするには、そのユーザーに割り当てられた1つのライセンスが必要です。ライセンスサーバーまたはクラウドサービスがライセンスを割り当てます。これらのライセンスを手動で割り当てることはできません。ライセンスは共有デバイスではなく、ユーザーに割り当てられます。一度ライセンスが割り当てられると、90日間非アクティブになるまで、別のユーザーに割り当てることはできません。詳しくは、「ユーザー/デバイスライセンス」を参照してください。

Citrixは、ユーザー/デバイスライセンスモデルでライセンスデバイスをどのように定義しますか?

ライセンスデバイスには、一意のエンドポイントデバイスIDが必要です。ユーザー/デバイスモデルでは、デバイスとは、Citrix Virtual Apps and Desktopsのインスタンスにアクセスするために個人が使用することを承認したあらゆる機器を指します。共有デバイスの場合、1つのCitrix Virtual Apps and Desktopsユーザー/デバイスライセンスで、デバイスを共有する複数のユーザーをサポートできます。たとえば、共有デバイスは、教室のワークステーションや病院の臨床ワークステーションなどです。

シトリックス バーチャル デスクトップ スタンダード エディションの同時使用ライセンスをユーザー/デバイスモデルに変換できますか?

Citrix Virtual Desktops Standard Editionの同時使用ライセンスをCitrix Virtual Desktops Standard Editionのユーザー/デバイスライセンスに変換することはできません。同様に、Citrix Virtual Desktops Standard Editionのユーザー/デバイスライセンスをCitrix Virtual Desktops Standard Editionの同時使用ライセンスに変換することもできません。

Citrix Virtual Desktops Standard Editionの同時使用ライセンスをお持ちで、ユーザー/デバイスライセンスモデルをご希望の場合は、Citrix Virtual Apps and Desktops AdvancedまたはPremium Editionにアップグレードしてください。

元	スタンダード同時接続へ	スタンダードユーザー/デバイスへ	アドバンストユーザー/デバイスへ	プレミアムユーザー/デバイスへ
Citrix Virtual Desktops スタンダードエディ	N/A	Concurrent から user/device	ライセンスモデルを変換することはできません	ライセンスモデルを変換することはできません

元	スタンダード同時接続へ	スタンダードユーザー/デバイスへ	アドバンストユーザー/デバイスへ	プレミアムユーザー/デバイスへ
ション同時接続ライセンス		への変換は許可されていません	が、Citrix Virtual Apps and Desktops Advanced または Premium Edition にアップグレードすることはできます。	が、Citrix Virtual Apps and Desktops Advanced または Premium Edition にアップグレードすることはできます。
シトリックス バーチャル デスクトップ スタンダード エディション ユーザー/デバイス ライセンス	User/device から concurrent への変換は許可されていません	N/A	N/A	N/A

同時使用ライセンスとユーザー/デバイスライセンスの違い?

同時接続ライセンスは、デバイスの同時接続数に基づいています。同時接続ライセンスは、デバイスがアクティブな接続を確立している場合にのみ使用されます。接続が終了すると、同時接続ライセンスはすぐに使用可能なライセンスプールに戻されます。このライセンスモデルは、一時的な使用におすすめです。ユーザー/デバイスライセンスは一定期間リースされ、リース期間が終了するまで他のユーザーは利用できません。

ユーザー/デバイスモデルにおける、同じ企業内でのユーザーとデバイスへのライセンス割り当て?

はい。両方のタイプを同じ企業内で使用できます。ライセンスサーバーは、使用状況に基づいてユーザーまたはデバイスにライセンスを最適に割り当てます。これらのライセンスを手動で割り当てることはできません。

ライセンスを付与するユーザーまたはデバイスの数をどのように決定すればよいですか?

適切なライセンス数を決定するために、ユースケースの要件を評価してください。ユーザー/デバイスライセンスは、無制限のデバイスから無制限の仮想デスクトップと仮想アプリへの無制限のアクセスを可能にします。同時接続ライセンスは、無制限のユーザーが使用できる単一のデバイスから無制限の仮想デスクトップと仮想アプリへの無制限のアクセスを可能にします。次の式を考慮してください。

```
(Number of total users) – (number of users that only access exclusively

 with shared devices) + (number shared devices) = total number

 of licenses to buy.



For example, there are 1000 total users at the hospital. If 700 of them
access only

Citrix Virtual Desktops from 300 shared devices in the hospital, the
number of

licenses to purchase is 1000 – 700 + 300 = 600 licenses.
```

ユーザー/デバイスモデルでは、ライセンスユーザーが自分の環境に接続するために使用できるデバイスの最大数はいくつですか?

各ライセンスユーザーは、接続されているデバイスまたはオフラインのデバイスを無制限に使用する権利があります。

ユーザー/デバイスモデルでは、ライセンスデバイスにアクセスできるユーザーの最大数はいくつですか?

各ライセンスデバイスは、組織内で無制限のユーザーにサービスを提供できます。

ユーザー/デバイスモデルでは、ライセンスユーザーが一度に消費できる仮想デスクトップまたはRBI Webアプリケーションの最大数はいくつですか?

各ライセンスユーザーは、無制限の仮想デスクトップまたはWebアプリケーションに接続できます。

既存のCitrix Virtual Apps and Desktops環境で、ライセンスユーザー/デバイスの数を増やすためにCitrix Virtual Apps and Desktopsライセンスを購入できますか?

はい。既存のCitrix Virtual Apps and Desktops環境で、ライセンスユーザー/デバイスの数を増やすためにCitrix Virtual Apps and Desktopsライセンスを購入できます。

承認されたユーザー/デバイスライセンスを解放するにはどうすればよいですか?

承認されたユーザー/デバイスの割り当てを解除するには、EULAの条項に従って`udadmin`ユーティリティを使用します。その後、ライセンスサーバーは次の適切なユーザー/デバイスにライセ

ンスを割り当てます。詳細については、ユーザーまたはデバイスのライセンスを表示または解放するを参照してください。

購入したユーザー/デバイスライセンス数を超過した場合、どうなりますか?

ユーザー/デバイスライセンスには10%の超過分が含まれており、これはライセンスが生成される際に含まれます。この超過分は、インストールされているライセンス数にも含まれます。使用量が超過分を含むインストール済みライセンス数を超過した場合、追加ユーザーのアクセスは拒否されます。追加ユーザーのアクセスを有効にするには、新しいライセンスを購入して展開してください。

ライセンスの超過分を含め、すべてのライセンスが使用中の場合、ライセンスバーストモードにより製品への無制限の接続が可能になります。ライセンスバーストモードは、最大ライセンス数を超過した理由を特定し、ユーザーを中断することなく追加のライセンスを購入するための時間を提供します。この期間は、15日が経過するか、追加の小売ライセンスをインストールするかのいずれか早い方まで続きます。詳細については、ライセンスバーストモードを参照してください。

Directorはライセンスキャッシュモードの状態を表示します。詳細については、Directorダッシュボードのパネルを参照してください。

ライセンスユーザーが一度に利用できる仮想アプリケーションの最大数はいくつですか?

各ライセンスユーザーは、無制限の仮想アプリケーションに接続できます。

ライセンスユーザーが組織を離れた場合、どうなりますか?

既存のライセンスユーザーが組織を離れる場合、Citrixに通知することなく、そのユーザーのライセンスを解放できます。ライセンスを解放するには、`udadmin`ユーティリティを使用します。ライセンスを解放しない場合、ライセンスサーバーは90日間の非アクティブ状態の後、自動的にライセンスを解放します。この情報はEULAに指定された条項に従います。

ライセンスユーザーが長期間不在の場合、どうなりますか?

既存のライセンスユーザーが長期間不在の場合、Citrix に通知することなくライセンスを解放し、再割り当てできるようにすることができます。ライセンスを解放するには、`udadmin` ユーティリティを使用します。

組織内のライセンスデバイスを交換した場合、どうなりますか?

既存のライセンスデバイスを交換する場合、Citrix に通知することなくライセンスを解放し、再割り当てできるようにすることができます。ライセンスを解放するには、`udadmin` ユーティリティを使用します。

ライセンスデバイスが長期間サービス停止になった場合はどうなりますか?

既存のライセンスデバイスが長期間サービス停止になった場合、Citrixに通知することなくライセンスを解放し、再割り当て可能にすることができます。ライセンスを解放するには、`udadmin` ユーティリティを使用します。ライセンスを解放しない場合、ライセンスサーバーは90日間の非アクティブ状態の後、自動的にライセンスを解放します。この情報はEULAに指定された条項に従います。

ライセンスをデバイスまたはユーザーに割り当てた後で、ユーザーライセンスをデバイスライセンスに、またはその逆に切り替えることはできますか?

はい。この変更は自動的に行われます。ライセンスサーバーは、使用パターンに基づいて、ユーザーまたはデバイスのいずれかにライセンスを割り当てます。使用パターンが変更された場合、ライセンスサーバーは新しい使用状況に基づいて割り当てを切り替えることがあります。ライセンスサーバーは常に、お客様にとって最も経済的な方法でライセンスを割り当てます。また、ライセンスサーバーは、90日間の割り当て期間が経過した後に**未使用**のライセンスを特定するためにライセンスを監視します。90日間の割り当て期間が経過した後に未使用と識別されたライセンスは、他のユーザーまたはデバイスに再割り当てできます。

同時使用ライセンス

同時使用モデルでは、Citrix Virtual Apps and Desktopsのライセンスユーザーが一度に消費できる仮想デスクトップの最大数はいくつですか?

エンドポイントは多数のユーザーにサービスを提供でき、無制限の接続を許可します。

以前のバージョンのCitrix Virtual Apps and Desktopsの同時使用ライセンスと、新しいユーザー/デバイスライセンスまたは同時使用ライセンスを単一のライセンスサーバーに展開できます?

はい。同じライセンスサーバーを使用して、ユーザー/デバイスライセンスまたは同時使用ライセンスの展開をサポートし続けることができます。

同時使用ライセンスとユーザー/デバイスライセンスまたは同時使用ライセンスを単一のライセンスサーバーに展開できます?

はい。同じライセンスサーバーを使用して、同時使用ライセンスとユーザー/デバイスライセンスまたは同時使用ライセンスの展開をサポートし続けることができます。

Citrix Virtual Apps and Desktops AdvancedおよびPremiumエディションには、Citrix Virtual Appsの同時使用ライセンスが含まれていますか?

Citrix Virtual Apps and Desktops AdvancedおよびPremiumのユーザー/デバイスライセンスには、互換性のためのみにCitrix Virtual Appsの同時使用ライセンスが含まれています。これらの同時使用ライセンスは、ユーザー/デバイスライセンスと互換性のない以前の製品バージョンでのみ使用で

きます。ユーザー/デバイスライセンスに含まれる同時使用互換ライセンスの使用は、XenAppバージョン6.5より前、およびXenDesktopバージョン5.0 Service Pack 1より前のバージョンでのみ許可されます。

購入した同時使用ライセンス数を超過した場合はどうなりますか?

すべてのライセンスが使用中の場合、ライセンスバーストモードにより、製品への無制限の接続が可能になります。ライセンスバーストモードは、最大ライセンス数を超過した理由を特定し、ユーザーを中断することなく追加のライセンスを購入するための時間を提供します。この期間は、15日が経過するか、または追加の小売ライセンスをインストールするかのいずれか早い方まで続きます。詳細については、「ライセンスバーストモード」を参照してください。

Directorは猶予期間の状態を表示します。詳細については、「Directorダッシュボードのパネル」を参照してください。

超過ライセンス

超過ライセンスはどのように入手できますか?

ユーザー/デバイス、ユーザー、またはデバイスライセンスモデルをサポートする製品（Citrix Cloudを除く）には、アクセス拒否を防ぐために限られた数の追加ライセンスを使用できるライセンス超過機能が含まれています。当社は、超過機能をライセンスエンタイトルメントとしてではなく、便宜のために提供しています。同時使用ライセンスおよびサーバーライセンスには超過機能は含まれていません。使用された超過ライセンスは、初回使用から30日以内に購入する必要がありますが、使用期間は30日に限定されません。Citrixは、新しい製品リリースで超過機能を削除する権利を留保します。詳細については、ライセンス超過を参照してください。

ライセンス超過の識別方法?

Citrix Licensing Managerで、超過しているライセンス数を含む使用状況情報を表示できます。Studioにも超過使用状況情報が含まれています。

超過ライセンスが消費されるとどうなりますか?

Citrix Virtual Apps and Desktops環境へのアクセスを有効にするために、インストールされているライセンスからライセンスが割り当てられます。この超過ライセンスは、他のライセンスと同等のアクセスと機能を提供します。

超過ライセンスが消費されたときにアラートを受け取ることはできますか?

現在、オーバードラフトライセンスが消費されたときに提供される特定の警告はありません。

オーバードラフトライセンスはどのくらいの期間消費できます?

最初に使用してから30日以内に使用されたオーバードラフトライセンスを購入してください。

その他の製品固有のライセンス情報

- シトリックス ADC
- シトリックス クラウド
- シトリックス エンドポイント マネジメント
- シトリックス ゲートウェイ
- XenServer
- Citrixライセンス

マシンの負荷分散

> **注:**
>
> Citrix Virtual Apps and Desktops™展開は、Web Studio (Webベース) と Citrix Studio (Windowsベース) の2つの管理コンソールを使用して管理できます。この機能はWeb Studioでのみ利用可能です。

> この機能は、シングルセッションOSまたはマルチセッションOSのすべてのカタログに適用されます。垂直負荷分散は、マルチセッションOSマシンにのみ適用されます。

> ロードバランシングは、サイトレベルとデリバリーグループレベルで構成できます。垂直と水平の2つのオプションがあります。デフォルトでは、水平ロードバランシングが有効になっています。

サイトレベルでのロードバランシング設定

- **垂直ロードバランシング**。最大負荷に達していない最も負荷の高いマシンに、受信ユーザーセッションを割り当てます。これにより、新しいマシンに移行する前に既存のマシンが飽和状態になります。既存のマシンから切断されたユーザーは、それらのマシンの容量を解放します。その後、受信負荷はそれらのマシンに割り当てられます。垂直ロードバランシングはユーザーエクスペリエンスを低下させますが、コストを削減します（セッションが電源オンのマシン容量を最大化するため）。

  例：それぞれ10セッション用に構成された2台のマシンがあるとします。最初のマシンは最初の10の同時セッションを処理します。2番目のマシンは11番目のセッションを処理します。

> **ヒント:**
>
> マシンがホストできる最大セッション数を指定するには、Maximum number of sessions ポリシー設定を使用します。
>
> あるいは、PowerShellを使用して、サイト全体で垂直負荷分散を有効または無効にできます。`Set-BrokerSite` コマンドレットで `UseVerticalScalingForRdsLaunches` 設定を使用します。`UseVerticalScalingForRdsLaunches` 設定の値を表示するには、`Get-BrokerSite` を使用します。詳細については、コマンドレットのヘルプを参照してください。

- **水平ロードバランシング**。利用可能な最も負荷の低い、電源オンのマシンに受信ユーザーセッションを割り当てます。水平ロードバランシングはユーザーエクスペリエンスを向上させますが、コストが増加します（より多くのマシンが電源オンのままになるため）。デフォルトでは、水平ロードバランシングが有効になっています。

  例：それぞれ10セッション用に構成された2台のマシンがあるとします。最初のマシンは5つの同時セッションを処理します。2番目のマシンも5つを処理します。

この機能を構成するには、Web Studioから左ペインで**設定**を選択します。**マルチセッションカタログのロードバランス**の下のオプションを選択します。

デリバリーグループレベルでのロードバランシング設定

デリバリーグループレベルでロードバランシングを構成すると、サイトレベルから継承されたロードバランシング設定を上書きできます。デリバリーグループレベルで垂直ロードバランシングを選択すると、各マシンの最大利用率を達成できます。これにより、パブリッククラウドでのコスト削減に役立ちます。この構成は、新しいデリバリーグループの作成時または既存のデリバリーグループの編集時に行うことができます。

水平ロードバランシング。セッションは、電源がオンになっているマシン間で分散されます。たとえば、それぞれ10セッション用に構成された2台のマシンがある場合、最初のマシンが5つの同時セッションを処理し、2番目のマシンも5つを処理します。

垂直ロードバランシング。セッションは、電源がオンになっているマシンの容量を最大化し、マシンコストを節約します。たとえば、それぞれ10セッション用に構成された2台のマシンがある場合、最初のマシンが最初の10個の同時セッションを処理します。2番目のマシンは11番目のセッションを処理します。

ローカルホストキャッシュ

Citrix Virtual Apps and Desktopsサイトデータベースが常に利用可能であることを保証するため、Citrixは、Microsoftの可用性の高いベストプラクティスに従って、フォールトトレラントなSQL Server展開から始めることを推奨します。(サポートされているSQL Serverの高可用性機能については、「データベース」(/ja-jp/citrix-virtual-apps-desktops/2407/system-requirements.html#databases)を参照してください。) しかし、ネットワークの問題や中断により、ユーザーがアプリケーションやデスクトップに接続できなくなる可能性があります。

ローカルホストキャッシュ機能により、障害発生時でもサイト内の接続仲介操作を続行できます。障害は、オンプレミスのCitrix®環境でDelivery Controller™とサイトデータベース間の接続が失敗した場合に発生します。サイトデータベースに90秒間アクセスできない場合、ローカルホストキャッシュが有効になります。

XenAppおよびXenDesktop 7.16以降、接続リース機能（以前のリリースにおける先行の高可用性機能）は製品から削除され、利用できなくなりました。

データコンテンツ

ローカルホストキャッシュには、メインデータベース内の情報の一部である次の情報が含まれています。

- サイトから公開されたリソースへの権限が割り当てられているユーザーおよびグループのID。
- サイトから公開されたリソースを現在使用している、または最近使用したユーザーのID。
- サイトで構成されているVDAマシン（リモートPCアクセスを含む）のID。
- 公開されたリソースへの接続に積極的に使用されているクライアントCitrix Receiver™マシンのID（名前とIPアドレス）。

また、メインデータベースが利用できなかった間に確立された、現在アクティブな接続に関する情報も含まれます。

- Citrix Receiverによって実行されたクライアントマシンのエンドポイント分析の結果。
- サイトに関与するインフラストラクチャマシン（NetScaler GatewayやStoreFront™サーバーなど）のID。
- ユーザーによる最近のアクティビティの日付、時刻、および種類。

動作の仕組み

次の図は、通常の操作中のローカルホストキャッシュのコンポーネントと通信パスを示しています。

ローカルホストキャッシュの通常の操作中の通信パスの図(/en-us/citrix-virtual-apps-desktops/2407/media/lhc-normal1.png)

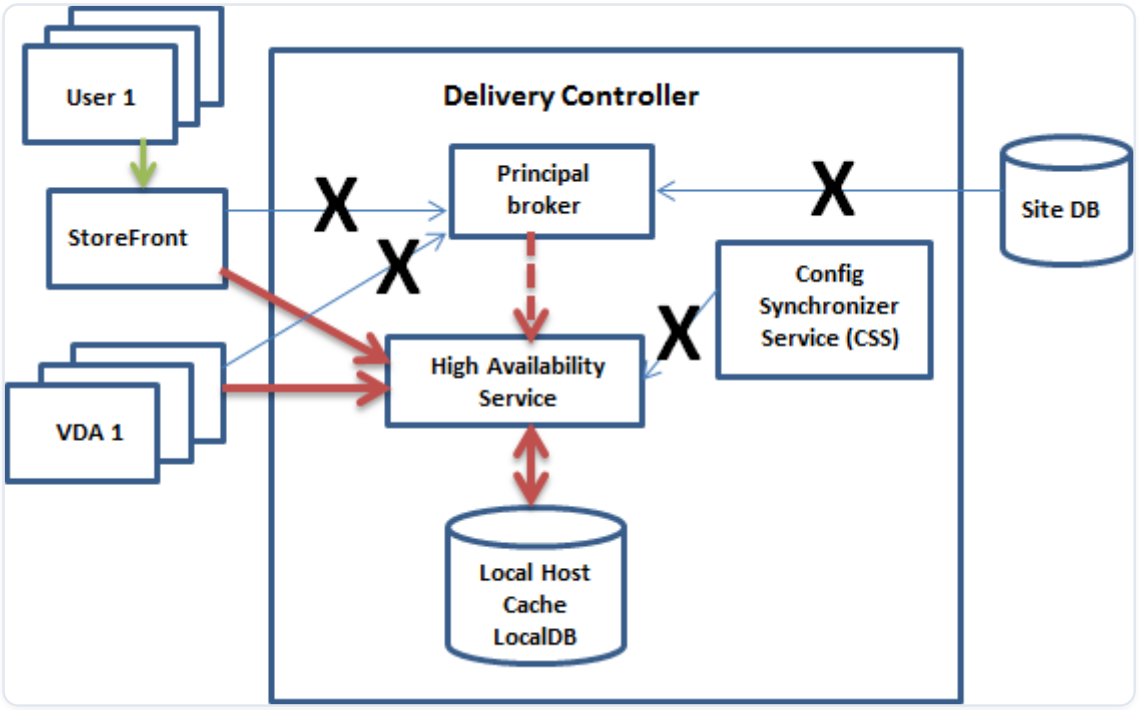
通常の操作中

- Controller上の *プライマリブローカー*（Citrix Broker Service）は、StoreFrontからの接続要求を受け入れます。ブローカーはサイトデータベースと通信し、Controllerに登録されているVDAとユーザーを接続します。
- Citrix Config Synchronizer Service（CSS）は、約5分ごとにブローカーに確認し、変更があったかどうかを調べます。これらの変更は、管理者によって開始されたもの（デリバリーグループのプロパティの変更など）である場合もあれば、システムアクション（マシンの割り当てなど）である場合もあります。
- 前回のチェック以降に構成変更があった場合、CSSは情報をController上のセカンダリブローカーに同期（コピー）します。（セカンダリブローカーは高可用性サービスとも呼ばれます。）

  前回のチェック以降に変更された項目だけでなく、すべての構成データがコピーされます。CSSは構成データをController上のMicrosoft SQL Server Express LocalDBデータベースにインポートします。このデータベースはローカルホストキャッシュデータベースと呼ばれます。CSSは、ローカルホストキャッシュデータベースの情報がサイトデータベースの情報と一致していることを確認します。ローカルホストキャッシュデータベースは、同期が行われるたびに再作成されます。

  Microsoft SQL Server Express LocalDB（ローカルホストキャッシュデータベースで使用）は、Controllerをインストールすると自動的にインストールされます。（コマンドラインからControllerをインストールする際に、このインストールを禁止できます。）ローカルホストキャッシュデータベースは、複数のController間で共有することはできません。ローカルホストキャッシュデータベースをバックアップする必要はありません。構成変更が検出されるたびに再作成されます。
- 前回のチェック以降に変更がない場合、データはコピーされません。

次の図は、プリンシパルブローカーがサイトデータベースとの接続を失った場合 (停止が開始された場合) の通信パスの変化を示しています。



停止中

停止が開始されると:

- セカンダリブローカーは、接続要求のリッスンと処理を開始します。
- 停止が開始された時点では、セカンダリブローカーは最新のVDA登録データを持っていませんが、VDAがセカンダリブローカーと通信すると、登録プロセスがトリガーされます。そのプロセス中に、セカンダリブローカーは当該VDAに関する最新のセッション情報も取得します。
- セカンダリブローカーが接続を処理している間、ブローカリングプリンシパルは引き続き接続を監視します。接続が復元されると、ブローカリングプリンシパルはセカンダリブローカーに接続情報のリスニングを停止するよう指示し、ブローカリングプリンシパルはブローカリング操作を再開します。VDAが次にブローカリングプリンシパルと通信するときに、登録プロセスがトリガーされます。セカンダリブローカーは、以前の停止から残っているVDA登録をすべて削除します。CSSは、展開で構成変更が発生したことを認識すると、情報の同期を再開します。

同期中に停止が発生するという万が一の事態では、現在のインポートは破棄され、最後に認識された構成が使用されます。

イベントログには、同期と停止に関する情報が記載されています。

停止モードでの運用に時間制限はありません。

通常モードと停止モード間の移行は、既存のセッションには影響しません。新しいセッションの起動のみに影響します。

意図的に停止をトリガーすることもできます。その理由と方法の詳細については、「停止の強制」を参照してください。

複数のControllerがあるサイト

CSSは、他のタスクの中でも、ゾーン内のすべてのControllerに関する情報をセカンダリブローカーに定期的に提供します。（展開に複数のゾーンが含まれていない場合、このアクションはサイト内のすべてのControllerに影響します。）その情報を持つことで、各セカンダリブローカーは、ゾーン内の他のControllerで実行されているすべてのピアセカンダリブローカーについて認識します。

セカンダリブローカーは、別のチャネルで相互に通信します。これらのブローカーは、停止が発生した場合にゾーン内でブローカー操作を行うセカンダリブローカーを決定（選出）するために、実行されているマシンのFQDN名のアルファベット順リストを使用します。停止中、すべてのVDAは選出されたセカンダリブローカーに登録します。ゾーン内の選出されていないセカンダリブローカーは、受信接続およびVDA登録要求を積極的に拒否します。

停止中に選出されたセカンダリブローカーが失敗した場合、別のセカンダリブローカーが選出されて引き継ぎ、VDAは新しく選出されたセカンダリブローカーに登録します。

停止中にControllerが再起動された場合：

- そのControllerが選出されたブローカーでない場合、再起動による影響はありません。
- そのControllerが選出されたブローカーである場合、別のControllerが選出され、VDAが登録されます。再起動されたControllerが起動すると、自動的にブローカー処理を引き継ぎ、VDAが再度登録されます。このシナリオでは、登録中にパフォーマンスが影響を受ける可能性があります。

通常の操作中にControllerの電源をオフにし、停止中に電源をオンにした場合、そのControllerがブローカーとして選出されると、そのControllerでローカルホストキャッシュを使用できません。

イベントログには、選出に関する情報が記載されています。

停止中に利用できないもの、およびその他の違い

停止モードでの運用に時間制限はありません。ただし、Citrixは可能な限り迅速に接続を復元することを推奨しています。

停止中：

- Studioを使用できません。
- PowerShell SDKへのアクセスは制限されます。

    - まず、次の操作を行う必要があります。
        - 値が1のレジストリキー `EnableCssTestMode` を追加します: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
        - ポート89を使用します: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ControllerDNSName, DesktopGroupName, RegistrationState`
    - これらのコマンドを実行すると、以下にアクセスできます。
        - すべての `Get-Broker*` コマンドレット。

- ハイパーバイザーの資格情報はホストサービスから取得できません。すべてのマシンは不明な電源状態になり、電源操作を発行することはできません。ただし、電源がオンになっているホスト上の VM は、接続要求に使用できます。
- 割り当てられたマシンは、通常の操作中に割り当てが行われた場合にのみ使用できます。停止中に新しい割り当てを行うことはできません。
- Remote PC Access マシンの自動登録と構成はできません。ただし、通常の操作中に登録および構成されたマシンは使用可能です。
- サーバーでホストされているアプリケーションおよびデスクトップのユーザーは、リソースが異なるゾーンにある場合、構成されたセッション制限よりも多くのセッションを使用する可能性があります。
- ユーザーは、現在アクティブ/選出されているセカンダリブローカーを含むゾーン内の登録済み VDA からのみアプリケーションとデスクトップを起動できます。ゾーンをまたいだ起動（あるゾーンのセカンダリブローカーから別のゾーンの VDA への起動）は、停止中はサポートされません。
- 配信グループ内のVDAのスケジュールされた再起動が開始される前にサイトデータベースの停止が発生した場合、停止が終了すると再起動が開始されます。これは意図しない結果を招く可能性があります。詳細については、「データベース停止により遅延したスケジュールされた再起動」を参照してください。
- ゾーンの優先順位は構成できません。構成されている場合、セッション起動時に優先順位は考慮されません。
- タグがゾーンの指定に使用されるタグ制限は、セッション起動ではサポートされていません。このようなタグ制限が構成されており、StoreFrontストアの高度なヘルスチェックオプションが有効になっている場合、セッションが断続的に起動に失敗する可能性があります。

アプリケーションとデスクトップのサポート

LHCは、次の種類のVDAと配信モデルをサポートしています。

VDAの種類	配信モデル	LHCイベント中のVDAの可用性
マルチセッションOS	アプリケーションとデスクトップ	常に利用可能。
シングルセッションOS静的（割り当て済み）	デスクトップ	常に利用可能。
電源管理されたシングルセッションOSランダム（プール済み）	デスクトップ	デフォルトでは利用できません。プールされたデリバリーグループ内の電源管理されたVDAへのすべてのセッション起動試行は、デフォルトで失敗します。LHCイベント中に新しい接続でそれらを利用可能にできます。詳細については、Web Studioを使用した有効化およびPowerShellを使用した有効化を参照してください。 **重要:** 電源管理されたシングルセッションのプールされたマシンへのアクセスを有効にすると、以前のユーザーセッションからのデータや変更が後続のセッショ

VDAの種類	配信モデル	LHCイベント中のVDAの可用性	
		ンに存在する可能性があります。	

注:

プールされたデリバリーグループ内の電源管理されたデスクトップVDAへのアクセスを有効にしても、通常の操作中に構成された`ShutdownDesktopsAfterUse`プロパティがどのように機能するかには影響しません。LHC中にこれらのデスクトップへのアクセスが有効になっている場合、LHCイベントが完了してもVDAは自動的に再起動しません。プールされたデリバリーグループ内の電源管理されたデスクトップVDAは、VDAが再起動するまで以前のセッションからのデータを保持できます。VDAの再起動は、非LHC操作中にユーザーがVDAからログオフした場合、または管理者がVDAを再起動した場合に発生する可能性があります。

Web Studioを使用して、電源管理されたシングルセッションOSのプールされたVDAでLHCを有効にする

Web Studioを使用すると、LHCイベント中にデリバリーグループごとに、それらのマシンを新しい接続で利用可能にできます。

- デリバリーグループ作成時にこの機能を有効にするには、デリバリーグループの作成を参照してください。
- 既存のデリバリーグループでこの機能を有効にするには、デリバリーグループの管理を参照してください。

注:

この設定は、電源管理されたVDAを提供するプールされたデスクトップデリバリーグループに対してのみ、Web Studioで利用できます。

PowerShellを使用して、電源管理されたシングルセッションOSのプールされたVDAに対してLHCを有効にする

特定のデリバリーグループ内のVDAに対してLHCを有効にするには、次の手順に従います。

1. 次のコマンドを実行して、サイトレベルでこの機能を有効にします。

   ```
   Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
   ```

2. デリバリーグループ名を指定して次のコマンドを実行し、デリバリーグループに対してLHCを有効にします。

   ```
   Set-BrokerDesktopGroup -Name "name" -ReuseMachinesWithoutShutdownInOutage $true
   ```

電源管理されたVDAを持つ新規作成されたプールされたデリバリーグループのデフォルトのLHC可用性を変更するには、次のコマンドを実行します。

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

RAMサイズの考慮事項

LocalDBサービスは、約1.2 GBのRAM（データベースキャッシュに最大1 GB、SQL Server Express LocalDBの実行に200 MB）を使用できます。セカンダリブローカーは、停止が長期間続き、多くのログオンが発生する場合（たとえば、10Kユーザーで12時間）、最大1 GBのRAMを使用できます。これらのメモリ要件は、コントローラーの通常のRAM要件に追加されるため、RAM容量の合計を増やす必要がある場合があります。

サイトデータベースにSQL Server Expressのインストールを使用する場合、サーバーには2つのsqlserver.exeプロセスがあります。

CPUコアとソケット構成の考慮事項

コントローラーのCPU構成、特にSQL Server Express LocalDBで利用可能なコアの数は、メモリ割り当てよりも直接的にローカルホストキャッシュのパフォーマンスに影響します。このCPUオーバーヘッドは、データベースにアクセスできず、セカンダリブローカーがアクティブな停止期間中にのみ観察されます。

LocalDBは複数のコア（最大4つ）を使用できますが、シングルソケットに制限されています。ソケットを追加してもパフォーマンスは向上しません（たとえば、1コアのソケットを4つ持つ場合）。代わりに、Citrixは複数のソケットと複数のコアを使用することを推奨しています。Citrixのテストでは、2x3（2ソケット、3コア）構成が4x1および6x1構成よりも優れたパフォーマンスを提供しました。

ストレージに関する考慮事項

停止中にユーザーがリソースにアクセスすると、LocalDBは増大します。たとえば、1秒あたり10回のログオンで実行されるログオン/ログオフテスト中に、データベースは2〜3分ごとに1MB増加しました。通常の操作が再開されると、ローカルデータベースが再作成され、スペースが返されま

す。ただし、停止中のデータベースの増大に対応するため、LocalDBがインストールされているドライブには十分な空き容量が必要です。ローカルホストキャッシュは、停止中により多くのI/Oも発生させます。具体的には、1秒あたり約3MBの書き込みと数十万回の読み取りです。

パフォーマンスに関する考慮事項

停止中、1つのセカンダリブローカーがすべての接続を処理するため、通常の操作中に複数のコントローラー間で負荷分散を行うサイト（またはゾーン）では、停止中に選出されたセカンダリブローカーは、通常よりもはるかに多くの要求を処理する必要がある場合があります。そのため、CPUの要求は高くなります。サイト（ゾーン）内のすべてのセカンダリブローカーは、ローカルホストキャッシュデータベースと影響を受けるすべてのVDAによって課される追加の負荷を処理できる必要があります。これは、停止中に選出されるセカンダリブローカーは変更される可能性があるためです。

VDIの制限:

- シングルゾーンVDI展開では、停止中に最大10,000台のVDAを効果的に処理できます。
- マルチゾーンVDI展開では、停止中に各ゾーンで最大10,000台のVDAを効果的に処理でき、サイト全体で最大40,000台のVDAまで対応できます。たとえば、以下の各サイトは停止中に効果的に処理できます。
    - 4つのゾーンを持つサイトで、各ゾーンに10,000台のVDAが含まれる場合。
    - 7つのゾーンを持つサイトで、1つのゾーンに10,000台のVDAが含まれ、残りの6つのゾーンにそれぞれ5,000台のVDAが含まれる場合。

停止中、サイト内の負荷管理が影響を受ける可能性があります。負荷評価機能（特にセッション数ルール）が超過する可能性があります。

すべてのVDAがセカンダリブローカーに登録するのにかかる時間中、そのサービスは現在のセッションに関する完全な情報を持っていない可能性があります。そのため、その期間中のユーザー接続要求により、既存のセッションへの再接続が可能であったとしても、新しいセッションが起動される可能性があります。この期間（「新しい」セカンダリブローカーが再登録中にすべてのVDAからセッション情報を取得する間）は避けられません。停止開始時に接続されているセッションは、移行期間中に影響を受けませんが、新しいセッションやセッションの再接続は影響を受ける可能性があります。

この期間は、VDAが登録する必要がある場合に発生します。

- 停止が開始されるとき: プリンシパルブローカーからセカンダリブローカーに移行するとき。
- 停止中のセカンダリブローカーの障害: 障害が発生したセカンダリブローカーから新しく選出されたセカンダリブローカーに移行するとき。

- 停止からの回復: 通常の操作が再開され、プリンシパルブローカーが制御を再開するとき。

Citrix Broker Protocolの`HeartbeatPeriodMs`レジストリ値を下げることで、間隔を短縮できます(デフォルト = 600000 ms、つまり10分)。このハートビート値は、VDAがpingに使用する間隔の2倍であるため、デフォルト値では5分ごとにpingが実行されます。

たとえば、次のコマンドはハートビートを5分 (300000ミリ秒) に変更します。これにより、2.5分ごとにpingが実行されます。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name HeartbeatPeriodMs -PropertyType DWORD –Value 300000
```

ハートビート値を変更する際は注意してください。頻度を増やすと、通常モードと停止モードの両方でControllerへの負荷が増大します。

VDAがどれだけ迅速に登録されても、この間隔を完全に排除することはできません。

セカンダリブローカー間の同期にかかる時間は、オブジェクト (VDA、アプリケーション、グループなど) の数が増えるにつれて長くなります。たとえば、5000台のVDAを同期するには、完了までに10分以上かかる場合があります。

XenApp 6.xリリースとの違い

このローカルホストキャッシュの実装は、XenApp 6.xおよびそれ以前のXenAppリリースにおけるローカルホストキャッシュ機能と同じ名前を共有していますが、重要な改善点があります。この実装は、より堅牢で破損しにくいです。定期的な`dsmaint`コマンドの必要性を排除するなど、メンテナンス要件が最小限に抑えられています。このローカルホストキャッシュは、技術的にはまったく異なる実装です。

ローカルホストキャッシュの管理

ローカルホストキャッシュが正しく機能するには、各ControllerのPowerShell実行ポリシーをRemoteSigned、Unrestricted、またはBypassに設定する必要があります。

SQL Server エクスプレス ローカルDB

ローカルホストキャッシュが使用するMicrosoft SQL Server Express LocalDBソフトウェアは、Controllerをインストールするか、バージョン7.9より前のControllerをアップグレードすると自動的にインストールされます。セカンダリブローカーのみがこのデータベースと通信します。このデータベースに関する変更は、PowerShellコマンドレットを使用して行うことはできません。LocalDBはController間で共有できません。

ローカルホストキャッシュが有効になっているかどうかに関わらず、SQL Server Express LocalDBデータベースソフトウェアはインストールされます。

そのインストールを防ぐには、`XenDesktopServerSetup.exe`コマンドを使用してControllerをインストールまたはアップグレードし、`/exclude "Local Host Cache Storage (LocalDB)"`オプションを含めます。ただし、ローカルホストキャッシュ機能はデータベースなしでは機能せず、セカンダリブローカーで別のデータベースを使用することはできないことに注意してください。

このLocalDBデータベースのインストールは、サイトデータベースとして使用するためにSQL Server Expressをインストールするかどうかには影響しません。

以前のSQL Server Express LocalDBバージョンを新しいバージョンに置き換える方法については、「SQL Server Express LocalDBの置き換え」(/ja-jp/citrix-virtual-apps-desktops/2407/upgrade-migrate/upgrade.html#replace-sql-server-express-localdb)を参照してください。

製品のインストールとアップグレード後のデフォルト設定

Citrix Virtual Apps and Desktopsの新規インストール時（最小バージョン7.16）には、ローカルホストキャッシュが有効になります。

アップグレード後（バージョン7.16以降）は、展開全体で10,000未満のVDAがある場合、ローカルホストキャッシュが有効になります。

ローカルホストキャッシュの有効化と無効化

- ローカルホストキャッシュを有効にするには、次のように入力します。

  ```
  Set-BrokerSite -LocalHostCacheEnabled $true
  ```

  ローカルホストキャッシュが有効になっているかどうかを確認するには、`Get-BrokerSite`と入力します。`LocalHostCacheEnabled`プロパティが`True`であることを確認します。
- ローカルホストキャッシュを無効にするには、次のように入力します。

  ```
  Set-BrokerSite -LocalHostCacheEnabled $false
  ```

注意: XenAppおよびXenDesktop 7.16以降、接続リース（バージョン7.6からローカルホストキャッシュに先行していた機能）は製品から削除され、利用できなくなりました。

ローカルホストキャッシュが機能していることを確認する

ローカルホストキャッシュが正しく設定され、機能していることを確認するには：

- 同期インポートが正常に完了していることを確認します。イベントログを確認してください。

- 各Delivery ControllerにSQL Server Express LocalDBデータベースが作成されていることを確認します。これにより、必要に応じてセカンダリブローカーが引き継ぐことができることが確認されます。
  - Delivery Controllerサーバーで、`C:\Windows\ServiceProfiles\NetworkService`を参照します。
  - `HaDatabaseName.mdf`と`HaDatabaseName_log.ldf`が作成されていることを確認します。
- Delivery ControllerでForce an outageを実行します。ローカルホストキャッシュが機能することを確認したら、すべてのControllerを通常モードに戻すことを忘れないでください。これには約15分かかる場合があります。

イベントログ

イベントログは、同期と停止が発生した時期を示します。イベントビューアーログでは、停止モードは*HA モード.** と呼ばれます。

コンフィグシンクロナイザーサービス:

通常の操作中、CSSがローカルホストキャッシュブローカーを使用して構成データをローカルホストキャッシュデータベースにインポートする際に、次のイベントが発生する可能性があります。

- 503: Citrix Config Sync Serviceが更新された構成を受信しました。このイベントは、同期プロセスの開始を示します。
- 504: Citrix Config Sync Serviceが更新された構成をインポートしました。構成のインポートは正常に完了しました。
- 505: Citrix Config Sync Serviceがインポートに失敗しました。構成のインポートは正常に完了しませんでした。以前に成功した構成が利用可能な場合、停止が発生したときにそれが使用されます。ただし、それは現在の構成から古くなります。以前の構成が利用できない場合、サービスは停止中にセッションブローカーに参加できません。この場合、トラブルシューティングセクションを参照し、Citrixサポートに連絡してください。
- 507: システムが停止モードであり、ローカルホストキャッシュブローカーがブローカー処理に使用されているため、Citrix Config Sync Serviceはインポートを中止しました。サービスは新しい構成を受信しましたが、停止が発生したためインポートは中止されました。これは予期される動作です。
- 510: プライマリConfiguration ServiceからConfiguration Service構成データが受信されませんでした。
- 517: プライマリBrokerとの通信に問題がありました。

- 518: セカンダリBroker（High Availability Service）が実行されていないため、Config Syncスクリプトが中止されました。

ハイアベイラビリティサービス:

このサービスは、ローカルホストキャッシュブローカーとも呼ばれます。

- 3502: 停止が発生し、ローカルホストキャッシュブローカーがブローカー操作を実行しています。
- 3503: 停止が解決され、通常の操作が再開されました。
- 3504: どのローカルホストキャッシュブローカーが選出されたか、および選出に関与した他のローカルホストキャッシュブローカーを示します。
- 3507: 2分ごとにローカルホストキャッシュのステータス更新を提供し、選出されたブローカーでローカルホストキャッシュモードがアクティブであることを示します。停止期間、VDA登録、セッション情報を含む停止の概要が含まれます。
- 3508: 選出されたブローカーでローカルホストキャッシュがアクティブでなくなり、通常の操作が復元されたことを通知します。停止期間、ローカルホストキャッシュイベント中に登録されたマシンの数、LHCイベント中の成功した起動の数を含む停止の概要が含まれます。
- 3509: 選出されていないブローカーでローカルホストキャッシュがアクティブであることを通知します。2分ごとの停止期間が含まれ、選出されたブローカーを示します。
- 3510: 選出されていないブローカーでローカルホストキャッシュがアクティブでなくなったことを通知します。停止期間が含まれ、選出されたブローカーを示します。

停止を強制する

意図的に停止を強制したい場合があります。

- ネットワークが繰り返しダウンする場合。ネットワークの問題が解決されるまで停止を強制することで、通常モードと停止モード間の継続的な移行（およびそれに伴う頻繁なVDA登録ストーム）を防ぎます。
- 災害復旧計画をテストするため。
- ローカルホストキャッシュが正しく機能していることを確認するため。
- サイトデータベースサーバーの交換または保守中。

停止を強制するには、Delivery Controllerを含む各サーバーのレジストリを編集します。`HKLM\Software\Citrix\DesktopServer\LHC`で、`OutageModeForced`を`REG_DWORD`として`1`に作成して設定します。この設定により、データベースの状態に関係なく、ローカルホスト

キャッシュブローカーは停止モードに入るように指示されます。値を`0`に設定すると、ローカルホストキャッシュブローカーは停止モードを終了します。

イベントを確認するには、`C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityService`にある`Current_HighAvailabilityService`ログファイルを監視します。

トラブルシューティング

ローカルホストキャッシュデータベースへの同期インポートが失敗し、505イベントが投稿された場合、いくつかのトラブルシューティングツールが利用可能です。

CDFトレース: `ConfigSyncServer`および`BrokerLHC`モジュールのオプションが含まれています。これらのオプションは、他のブローカーモジュールとともに、問題を特定するのに役立つでしょう。

レポート: 同期インポートが失敗した場合、レポートを生成できます。このレポートは、エラーの原因となっているオブジェクトで停止します。このレポート機能は同期速度に影響するため、Citrixは使用しないときは無効にすることを推奨しています。

CSSトレースレポートを有効にして生成するには、次のコマンドを入力します。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1
```

HTMLレポートは`C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.htm`に投稿されます。

レポートが生成されたら、レポート機能を無効にするには次のコマンドを入力します。

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```

ブローカー構成のエクスポート: デバッグ目的で正確な構成を提供します。

```
Export-BrokerConfiguration | Out-File <file-pathname>
```

例: `Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`。

ローカルホストキャッシュのPowerShellコマンド

PowerShellコマンドを使用して、Delivery Controllerでローカルホストキャッシュ (LHC) を管理できます。

PowerShellモジュールは、Delivery Controllerの次の場所にあります。

```
C:\Program Files\Citrix\Broker\Service\ControlScripts
```

> **重要:**
>
> このモジュールはDelivery Controllerでのみ実行してください。

PowerShell モジュールのインポート

モジュールをインポートするには、Delivery Controllerで次を実行します。

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-Module .
\HighAvailabilityServiceControl.psm1
```

LHC を管理するための PowerShell コマンド

以下のコマンドは、Delivery ControllerでLHCモードをアクティブ化および管理するのに役立ちます。

コマンドレット	機能
`Enable-LhcForcedOutageMode`	ブローカーをLHCモードにします。`Enable-LhcForcedOutageMode`が正常に機能するには、ConfigSyncサービスによってLHCデータベースファイルが正常に作成されている必要があります。このコマンドレットは、実行されたDelivery ControllerでのみLHCを強制します。LHCをアクティブにするには、このコマンドをゾーン内のすべてのDelivery Controllerで実行する必要があります。
`Disable-LhcForcedOutageMode`	ブローカーをLHCモードから外します。このコマンドレットは、実行されたDelivery ControllerでのみLHCモードを無効にします。`Disable-LhcForcedOutageMode`は、ゾーン内のすべてのDelivery Controllerで実行する必要があります。

コマンドレット	機能
`Set-LhcConfigSyncIntervalOverride`	Citrix Config Synchronizer Service (CSS) がサイト内の構成変更をチェックする間隔を設定します。時間間隔は60秒（1分）から3600秒（1時間）まで設定できます。この設定は、実行されたDelivery Controllerにのみ適用されます。Delivery Controller間で一貫性を持たせるには、このコマンドレットを各Delivery Controllerで実行することを検討してください。例: `Set-LhcConfigSyncIntervalOverride -Seconds 1200`
`Clear-LhcConfigSyncIntervalOverride`	Citrix Config Synchronizer Service (CSS) がサイト内の構成変更をチェックする間隔を、デフォルト値の300秒（5分）に設定します。この設定は、実行されたDelivery Controllerにのみ適用されます。Delivery Controller間で一貫性を持たせるには、このコマンドレットを各Delivery Controllerで実行することを検討してください。
`Enable-LhcHighAvailabilitySDK`	実行されたDelivery Controller内のすべての `Get-Broker*` コマンドレットへのアクセスを有効にします。
`Disable-LhcHighAvailabilitySDK`	実行されたDelivery Controller内のBrokerコマンドレットへのアクセスを無効にします。

注:

- Delivery Controllerで `Get-Broker*` コマンドレットを実行する際は、ポート89を使用します。例:
  - `Get-BrokerMachine -AdminAddress localhost:89`
- LHCモードでない場合、Delivery Controller上のLHC Brokerは構成情報のみを保持します。

- LHCモード中、選出されたDelivery Controller上のLHC Brokerは以下の情報を保持します。
  - リソースの状態
  - セッションの詳細
  - VDA登録
  - 構成情報

「検索」を使用してマシンとセッションを監視および管理する

注:

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

この記事では、Web Studioの**検索**ノードを使用してマシンとセッションを監視および管理する方法について説明します。

ノードについて

検索ノードは、マシンとユーザーセッションを監視および管理するための一元的な場所を提供します。

検索ノードのコンポーネント(/en-us/citrix-virtual-apps-desktops/2407/media/search-components.png)

コールアウト	領域	説明
A	検索バー	複雑な検索条件を定義できるクイック検索とフィルターベースの検索を提供します。詳細については、「インスタンス

コールアウト	領域	説明
		の検索」を参照してください。
B	タイプタブ	マシンを種類別に一覧表示するタブ、またはすべてのセッションを一覧表示するタブが表示されます。インスタンス数はタブ名に表示されます。
C	インスタンスレベルのアクション	*選択したインスタンス* (マシンまたはセッション) に対して実行できるアクションが表示されます。詳細については、マシンアクション および セッションアクション を参照してください。
D	リストレベルのアクション	現在の*リスト*に対して実行できるアクションが表示されます。 • **エクスポート**アイコン: メインビューに表示されているインスタンスのリストをCSVファイルにエクスポートします。 • **表示する列**アイコン: リストのメインビューを

コールアウト	領域	説明	
		カスタマイズします。 • 「**エラー**」ラベル: このラベルを有効にすると、メインビューにエラーのある未登録マシンのみが表示されます。問題の詳細を表示するには、「**詳細**」ペインの「**トラブルシューティング**」タブに移動します。 • 「**警告**」ラベル: このラベルを有効にすると、メインビューに警告のある未登録マシンのみが表示されます。問題の詳細を表示するには、「**詳細**」ペインの「**トラブルシューティング**」タブに移動します。	
E	メインビュー	インスタンスとそのプロパティが表示されます。「**表示する列**」アイコンを選択して、メインビューをカスタマイズでき	

コールアウト	領域	説明
		ます。利用可能な列の詳細については、「マシン列」および「セッション列」を参照してください。
F	詳細ペイン	次の詳細が表示されます: • 選択したインスタンス（マシンまたはセッション）の詳細 • 選択したマシンに適用されたタグ • 選択したマシンに関するエラーまたは警告の詳細。問題、考えられる原因、推奨される解決策を含む

インスタンスの検索

検索機能を使用して、特定のマシンとセッションを検索します。

- フィルターを使用した検索
- クイック検索のために現在のフィルターセットを保存する
- 検索バーにフィルターフィールドをピン留めする
- クイック検索ボックスを使用した検索
- 検索を強化するためのヒント

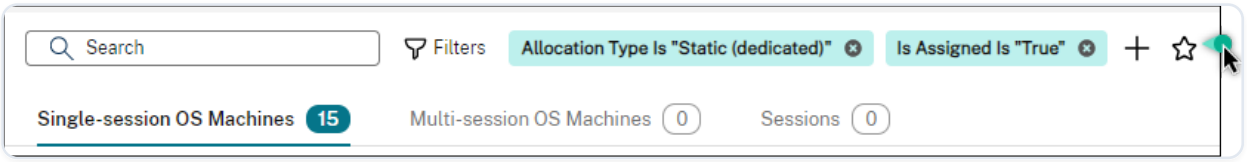
フィルターを使用した検索

たとえば、*静的でユーザーに割り当てられている*すべてのシングルセッションOSマシンを検索するには、次の手順に従います。

1. **シングルセッションOSマシン**タブで、**フィルター**アイコンをクリックします。フィルターパネルが表示されます。
2. 必要なフィルター条件を追加します。

   フィルター付き検索(/en-us/citrix-virtual-apps-desktops/2407/media/search-filter-1.png)
3. すべてのフィルター条件に一致する結果を検索で返すようにしたい場合は、**すべて一致** (AND演算子) を選択します。いずれかのフィルター条件に一致する結果を検索で返すようにしたい場合は、**いずれか一致** (OR演算子) を選択します。
4. **適用** をクリックします。

   フィルターされたリストには、静的でユーザーに割り当てられているすべてのシングルセッションOSマシンが表示されます。



クイック検索のために現在のフィルターセットを保存する

例えば、静的でユーザーに割り当てられているシングルセッションOSマシン用のフィルターセットを将来の使用のために保存するには、次の手順に従います。

1. フィルターベースの検索を実行した後、前の図に示すように、検索バーの **星** アイコンをクリックします。
2. 表示されるページで、このフィルターセットの名前 (例: *静的および割り当て済みマシン*) を入力します。
3. **保存** をクリックします。

   検索ボックスをクリックすると、保存されたフィルターセットが検索履歴リストに表示されます。

   検索フィルターセット(/en-us/citrix-virtual-apps-desktops/2407/media/search-filter-set.png)

> **注:**

フィルターセットはユーザーアカウントごとに保存されます。保存されたフィルターセットを管理するには、**管理** を選択します。

検索機能を使用して、特定のコンピューター、セッション、マシンカタログ、アプリケーション、またはデリバリーグループに関する情報を表示します。Web Studioで**検索**を選択すると、いくつかのオプションが表示されます。

頻繁に使用するフィルター *フィールド* を検索バーにピン留めして、簡単にアクセスできるようにします。例えば、フィルターベースの検索を実行した後、検索バーに **割り当てタイプ** をピン留めしたいとします。次の手順に従います。

- デフォルトでは、次のフィルターがビューにピン留めされています。**名前**、**セッション状態**、および**障害状態**。フィルターを選択して式を作成します。フィルターをカスタマイズするには、省略記号をクリックします。表示されるウィンドウで、次のことができます。

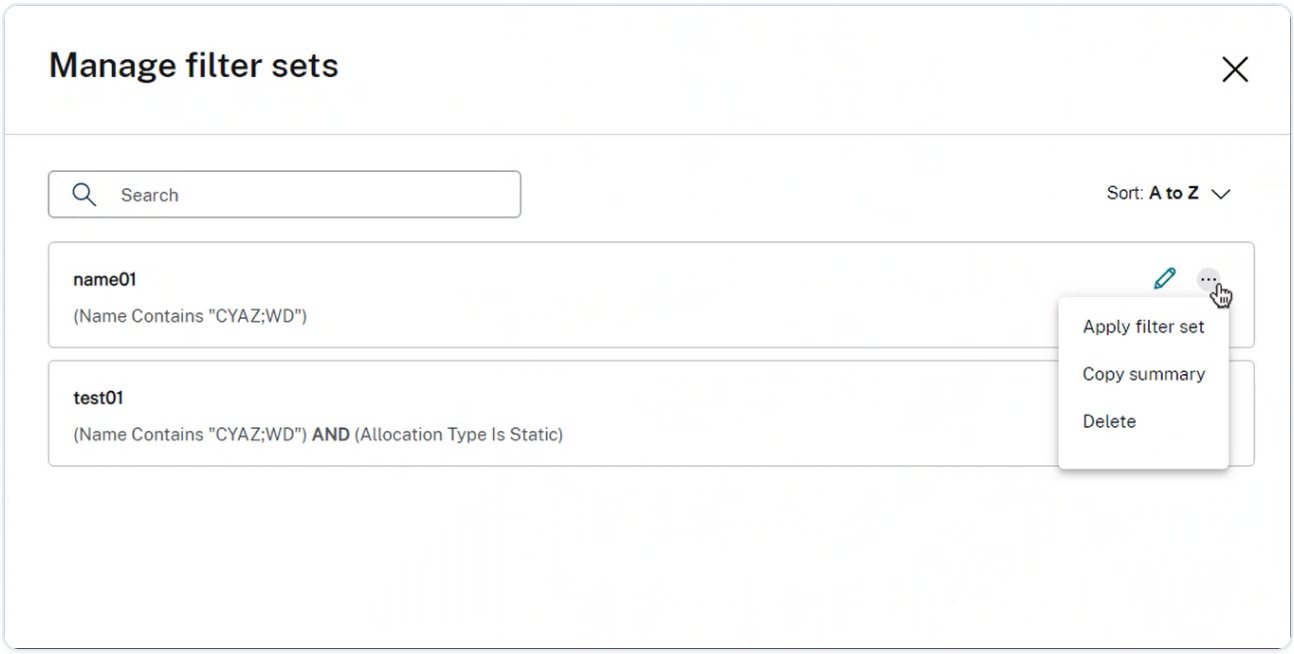
  - フィルターをピン留めまたはピン留め解除します。ピン留め解除されたフィルターは一度限りの使用であり、保存されません。

  - フィルターをクリックしてビューに追加します。

  - フィルターをクリアして、現在のフィルター済み検索をクリアし、ピン留め解除されたフィルターを削除します。

- オペレーターをクリックして、**すべて一致** (**AND** オペレーター) または **いずれか一致** (**OR** オペレーター) を切り替えます。**すべて一致**に設定すると、すべてのフィルター条件に一致する結果が検索で返されます。いずれか一致に設定すると、いずれかのフィルター条件に一致する結果が検索で返されます。

- 星の記号をクリックして、使用中のフィルターを保存します。保存された項目はフィルターセットとして知られています。保存された項目は、保存されたフィルターセットリストに表示されます。(リストにアクセスするには、検索ボックスを選択します。)保存されたフィルターセットをクリックして、検索にフィルターを適用できます。保存されたフィルターセットを管理するには、検索ボックスを選択し、**管理**を選択します。



フィルターなしで検索

検索ボックスに入力すると、プロンプト付きのメニューが表示され、検索をすばやく絞り込むのに役立つさまざまな検索オプションが提供されます。入力したコンテンツが*VM01*であるとします。次のプロンプトのいずれかを選択します。

- VM01 名。名前で検索します。
- VM01 マシンカタログ。名前で検索します。
- VM01 デリバリーグループ。デリバリーグループ名で検索します。

一般的な検索を実行すると、Citrix Virtual Apps and Desktops は以下の条件で一致するものを検索し、関連する結果を提供します。

- **名前**。マシン名またはDNS名で検索します。
- **マシンカタログ**。マシンカタログ名で検索します。
- **デリバリーグループ**。デリバリーグループ名で検索します。
- **ユーザー**。セッションユーザー名で検索します。
- **クライアント**。セッションクライアント名で検索します。
- **VM**。ホストされているマシン名で検索します。これは、ハイパーバイザーが使用するホストされているマシンのフレンドリ名です。
- **ホスティングサーバー名**。ホスティングサーバー名で検索します。
- 「**検索**」ノードで、任意の列を選択して項目を並べ替えます。

マシンカタログまたはデリバリーグループを検索する

マシンカタログノードとデリバリーグループノード内でリソースを検索および特定できます。これらのノードの検索機能は、検索ノードと同じインターフェイスを提供し、Citrix Virtual Apps and Desktops 全体でシームレスな検索エクスペリエンスを提供します。

- マシンに接続されているユーザーデバイスを見つけるには、「**クライアント (IP)**」と「**は**」を使用し、デバイスのIPアドレスを入力します。
- アクティブなセッションを見つけるには、「**セッション状態**」、「**は**」、および「**接続済み**」を使用します。
- 配信グループ内のすべてのマシンを一覧表示するには、左ペインで「**デリバリーグループ**」を選択します。グループを選択し、アクションバーまたはコンテキストメニューから「**マシンの表示**」を選択します。

並べ替え操作を実行する際は、以下の考慮事項に留意してください。

- 項目の数が5,000を超えない限り、任意の列をクリックして項目を並べ替えることができます。数が5,000を超えると、名前または現在のユーザー（表示しているタブによって異なります）でのみ並べ替えることができます。並べ替えを有効にするには、フィルターを使用して項目の数を5,000以下に減らします。
- 項目の数が500より大きく5,000以下の場合：
  - 並べ替えパフォーマンスを向上させるため、すべてのデータをローカルにキャッシュします。「**シングルセッションOSマシン**」タブと「**マルチセッションOSマシン**」タブでは、列（「**名前**」列を除く任意の列）をクリックして並べ替える最初のときにデータをキャッシュします。「**セッション**」タブでは、列（「**現在のユーザー**」列を除く任意の列）をクリックして並べ替える最初のときにデータをキャッシュします。その結果、並べ替えの完了に時間がかかります。パフォーマンスを高速化するには、名前または現在のユーザーで並べ替えるか、フィルターを使用して項目の数を減らします。
  - テーブルの下に表示される「最終更新日時: `<the time when you refreshed the table>`」というメッセージは、データがキャッシュされていることを示します。この場合、並べ替え操作は以前に読み込まれた項目に基づいています。これらの項目は最新ではない可能性があります。最新の状態にするには、更新アイコンをクリックします。

表示する列をカスタマイズする

列をカスタマイズすると、**パフォーマンスが低下します**というラベルが付いた列が表示されます。これらの列を選択すると、コンソールのパフォーマンスが低下する可能性があります。カスタマ

イズが完了すると、選択した列を表示するようにテーブルが更新されます。これらの列が存在すると、テーブルを更新する際に遅延が発生する可能性があります。

1. 「**検索**」ノードで、必要に応じて「**マルチセッションOSマシン**」、「**シングルセッションOSマシン**」、または「**セッション**」タブを選択します。
2. アクションバーの**表示する列**アイコンをクリックし、列を選択します。

   利用可能な列とその説明の詳細については、「マシン列」および「セッション列」を参照してください。

列を選択する際、「**パフォーマンスが低下します**」というラベルが付いた列が表示されることがあります。これらの列を選択すると、コンソールのパフォーマンスが低下する可能性があります。以下の点を考慮してください。

- カスタマイズが完了すると、選択した列を表示するようにテーブルが更新されます。これらの列が存在すると、テーブルの更新時に遅延が発生する可能性があります。
- ブラウザを更新するか、コンソールからサインアウトして再度サインインすると、それらの列を保持するかどうかを尋ねるメッセージが表示されます。保持することを選択した場合、最適なコンソールパフォーマンスを得るために、テーブルの更新は1分間に1回までに制限されます。より頻繁に更新するには、パフォーマンスを低下させる列を削除してください。

検索ノードの各タブで、エクスポートが進行中の間は、別のエクスポートを実行できません。

Searchノードのアクションを使用して、マシンとセッションの問題のトラブルシューティングを行ったり、ユーザー要求を処理したりします。

知っておくと良いこと

- **検索**ノードで、任意の列を選択して項目を並べ替えます。
- 個々のマシンレベル。**Search**ノードを使用して、ターゲットマシンを特定し、アクションを実行します。
- マシンカタログレベル。カタログのマスターイメージの変更、カタログからのマシンの削除、カタログへのマシンの追加などです。詳細については、「マシンカタログの管理」を参照してください。
- デリバリーグループレベル。グループ内のマシンのメンテナンスモードのオン/オフなどです。詳細については、「デリバリーグループの管理」を参照してください。

個々のセッションレベルに加えて、デリバリーグループレベルでもセッションを管理できます。たとえば、デリバリーグループのセッションの事前起動と残存を構成するなどです。詳細については、「デリバリーグループの管理」を参照してください。

- デリバリーグループ内のすべてのマシンを一覧表示するには、左ペインで**デリバリーグループ**を選択します。グループを選択し、アクションバーまたはコンテキストメニューから**マシンの表示**を選択します。

並べ替え操作を実行する際は、以下の考慮事項を念頭に置いてください。

1. 「**検索**」ノードで、「**マルチセッションOSマシン**」、「**シングルセッションOSマシン**」、または「**セッション**」タブを選択します。
2. 必要に応じて、1つまたは複数のインスタンスを選択します。
3. アクションバーまたは右クリックメニューから、それらのインスタンスで発生する問題やユーザー要求に基づいてアクションを選択します。

   利用可能なアクションとその説明の詳細については、「マシンアクション」および「セッションアクション」を参照してください。

> 「**注:**」:
>
> 2つ以上のインスタンスを選択した場合、それらすべてに適用されるアクションのみが利用可能です。

マシンまたはセッションデータをCSVファイルにエクスポートする

タブに表示されているインスタンス（マシンまたはセッション）のリスト（最大30,000項目）をCSVファイルにエクスポートします。詳細な手順は次のとおりです。

1. 「**検索**」ノードで、必要に応じて「**マルチセッションOSマシン**」、「**シングルセッションOSマシン**」、または「**セッション**」タブを選択します。
2. 右上隅にある「**エクスポート**」アイコンをクリックします。
3. 表示されるダイアログボックスで、「**続行**」をクリックします。

   エクスポートには数分かかる場合があります。ファイルはブラウザのデフォルトのダウンロードフォルダーにあります。

> 「**注:**」:
>
> 「**検索**」ノードの各タブで、エクスポートが進行中の間は、別のエクスポートを実行できません。

マシンのアクションと列

この記事では、マシンのアクションと列について、参考として説明を記載しています。

アクション

マシンで実行できるアクションとその説明を表示します。

アクション	説明	適用対象
デリバリーグループから削除	マシンをデリバリーグループから削除します。	シングルセッションおよびマルチセッション
デリバリーグループに追加	マシンをデリバリーグループに追加します。	シングルセッションおよびマルチセッション
セッションの表示	マシンで実行中のセッションを表示します。	シングルセッションおよびマルチセッション
タグの管理	マシンにタグを追加して管理します。タグの一般的な使用例の詳細については、「タグ」を参照してください。	シングルセッションおよびマルチセッション
メンテナンスモードをオンにする	パッチを適用する前、またはトラブルシューティングのために、マシンをメンテナンスモードにします。 このモードでは、そのマシンへの新しい接続が防止されます。ユーザーはそのマシン上の既存のセッションに接続できますが、そのマシンで新しいセッションを開始することはできません。	シングルセッションおよびマルチセッション
メンテナンスモードをオフにする	マシンのメンテナンスモードをオフにします。	シングルセッションおよびマルチセッション
VDAのアップグレード	マシンのVDAをアップグレードします。	特定の要件を満たすシングルセッションまたはマルチセッションOSマシン: 詳細はこちら。

アクション	説明	適用対象
ログオフ	マシンを強制的にログオフする	シングルセッションおよびマルチセッション
削除	ハイパーバイザーまたはクラウドサービス上にVMをそのまま残したまま、マシンカタログからVMを削除する。	シングルセッションおよびマルチセッション
ユーザーの変更	マシンを特定のユーザーに割り当てる。	シングルセッションの*静的*マシン。
開始	マシンを開始する。	シングルセッションおよびマルチセッション
シャットダウン	マシンをシャットダウンする。	シングルセッションおよびマルチセッション
再起動	マシンを再起動する	シングルセッションおよびマルチセッション
サスペンド	マシンを休止状態またはサスペンド状態にします。マシンをサスペンドすると、Delivery Controllerはマシンのメモリ内容をファイルに保存し、その後マシンをシャットダウンします。	シングルセッションOSマシン
再開	サスペンドされたマシンを再開します。サスペンドされたマシンを再開すると、Delivery Controllerはマシンを起動し、以前の状態に復元します。	シングルセッションOSマシン
強制再起動	マシンを強制再起動する。	シングルセッションOSマシン
強制シャットダウン	マシンを強制シャットダウンする。	シングルセッションOSマシン

列

タイプ別にすべてのマシン列とその説明を表示します。

- マシン
- マシンの詳細
- アプリケーション
- ホスティング
- 接続
- 登録
- セッションの詳細
- セッション

マシン

マシンカテゴリの列。

列	説明	適用対象
名前	マシンのDNSホスト名。	シングルセッションおよびマルチセッション
マシンカタログ	マシンが属するカタログの名前。	シングルセッションおよびマルチセッション
デリバリーグループ	マシンが属するデリバリーグループの名前。	シングルセッションおよびマルチセッション
ユーザー表示名	マシンに関連付けられているユーザーのフルネーム (通常、`Firstname Lastname`の形式)。関連付けられているユーザーとは、共有マシンの現在のユーザーと、専用マシンに割り当てられてい	シングルセッションおよびマルチセッション

列	説明	適用対象
	るユーザーを指します。	
ユーザー	マシンに関連付けられているユーザーのユーザー名(「domain\user」の形式)。関連付けられているユーザーとは、共有マシンの現在のユーザーと、専用マシンに割り当てられているユーザーを指します。	シングルセッションとマルチセッション
ユーザープリンシパル名	マシンに関連付けられているユーザーのユーザープリンシパル名（「user@domain」の形式）。関連付けられているユーザーは、共有マシンの現在のユーザーと、専用マシンに割り当てられているユーザーです。	シングルセッションとマルチセッション
デスクトップ表示名	セッションの起動に元々使用されたマシンの公開名。Citrix Workspace™アプリまたはStoreFrontに表示される名前です。	シングルセッションのみ
	注: デスクトップの表示を変更するには、**Perform Machine Update** 権限が必要です。表示	

列	説明	適用対象
	名の変更にはマシンプロパティの更新が含まれるためです。	
デスクトップの状態	マシンの未解決のデスクトップ状態のリスト。可能な値: Unknown、CPU、ICALatency、UPMLogonTime。	シングルセッションとマルチセッション
割り当てタイプ	マシンの割り当てタイプ: ユーザーに永続的に割り当てられる場合は **Permanent**。ランダムに割り当てられる場合は **Random**。	シングルセッションおよびマルチセッション
メンテナンスモード	マシンがメンテナンスモードであるかどうかを示します。	シングルセッションおよびマルチセッション
Windows接続設定	Windowsによって報告されるログオンモード。	マルチセッションのみ
	指定可能な値: LogonEnabled、Draining、DrainingUntilRestart、および LogonDisabled。	
割り当て済み	専用デスクトップがユーザーまたはクライアント（名前/アドレス）に割り当てられているかどうかを示します。ユーザーは明示的に割り当てることも、マシンの	シングルセッションおよびマルチセッション

列	説明	適用対象
	初回使用時に割り当てることもできます。	
物理	マシンが物理であるかどうかを示します。`True` はマシンが物理であることを示し、これはDelivery Controllerによって電源管理されていないことを意味します。`False` はそうでないことを示します。	シングルセッションおよびマルチセッション
プロビジョニングの種類	マシンがどのようにプロビジョニングされたか。考えられる値 • 手動: PVSまたはMCSを使用してプロビジョニングされていません。 • PVS: PVSを使用してプロビジョニング済み(物理マシン、ブレードマシン、仮想マシン) • MCS: MCSを使用してプロビジョニング済み(VMのみ)	シングルセッションおよびマルチセッション

列	説明	適用対象	
スケジュールされた再起動	マシンのスケジュールされた再起動操作の状態。考えられる値 • なし: 再起動はスケジュールされていません。 • 保留中: 再起動を待機中ですが、使用可能です。 • ドレイン中: 再起動を待機中で、新しいセッションには使用できません。ただし、既存の接続への再接続は引き続き許可されます。 • 進行中: スケジュールされた再起動がアクティブに実行されています。 • 自然: 自然な再起動が進行中です。マシンは再起動を待機しています。	シングルセッションおよびマルチセッション	

列	説明	適用対象
ゾーン	マシンが配置されているゾーンの名前。	シングルセッションおよびマルチセッション
状態	マシンに関連付けられているデスクトップの全体的な状態。これは、セッション状態、登録状態、電源状態など、さまざまな特定の状態から派生しています。	シングルセッションおよびマルチセッション
	可能な状態: オフ、未登録、利用可能、切断済み、使用中、準備中。	
タグ	マシンに関連付けられているタグのリスト。	シングルセッションおよびマルチセッション
VDAアップグレード	VDAパッケージのアップグレードアクションのマシン状態。	シングルセッションとマルチセッション
	指定可能な値: MissingUpgradeType, UpgradeScheduled, UpgradeAvailable, UpToDate, Unknown。	
サスペンド可能	マシンが電源アクション（サスペンドと再開）をサポートしているかどうかを示します。	シングルセッションとマルチセッション

列	説明	適用対象
ロードインデックス	現在のロードインデックス。詳細については、詳細はこちらを参照してください。	マルチセッションのみ
ドレイン状態	マシンがドレイン中で、マシン上のすべてのセッションが終了した後にシャットダウンするかどうかを示します。Trueは、電源管理されたマルチセッションマシンにのみ表示されます。	マルチセッションのみ
	注: マシンがメンテナンスモードの場合、シャットダウンしません。メンテナンスモードが解除された後にのみシャットダウンします。	

マシンの詳細

「**マシンの詳細**」カテゴリの列。

列	説明	適用対象
エージェントバージョン	マシンにインストールされているCitrix Virtual Delivery Agent (VDA) のバージョン。	シングルセッションおよびマルチセッション
IPアドレス	マシンのIPアドレス。	シングルセッションおよびマルチセッション
割り当て済み	専用デスクトップがユーザーまたはクライアント（名前/アドレス）に割り当てられてい	シングルセッションおよびマルチセッション

列	説明	適用対象
	るかどうかを示します。ユーザーは明示的に割り当てることも、マシンの初回使用時に割り当てることもできます。	
OSタイプ	マシンで実行されているオペレーティングシステムのタイプ。	シングルセッションのみ

アプリケーション

アプリケーションカテゴリの列。

列	説明	適用対象
使用中のアプリケーション	マシンで使用中のアプリケーションのリスト（ブラウザ名として表示）。	シングルセッションおよびマルチセッション
公開済みアプリケーション	マシンによって公開されているアプリケーションのリスト（ブラウザ名として表示）。	シングルセッションおよびマルチセッション

接続

接続カテゴリの列。

列	説明	適用対象
クライアント (IP)	マシンに接続されているクライアントのIPアドレス。	シングルセッションのみ
クライアント	マシンに接続されているクライアントのホスト名。	シングルセッションのみ
プラグインバージョン	接続されているクライアント上のCitrix Workspaceアプリのバージョン。	シングルセッションのみ
接続元	受信接続のホスト名。通常、ゲートウェイ、ルーター、またはクライアントです。	シングルセッションのみ

列	説明	適用対象
接続元 (IP)	受信接続のIPアドレス。通常、ゲートウェイ、ルーター、またはクライアントです。	シングルセッションのみ
接続タイプ	セッションに使用されるプロトコル。可能な値: HDX、RDP、およびコンソール。注: XenDesktop® 5 VDA上のコンソールセッションの場合、このフィールドは空白になります。	シングルセッションのみ
最終接続時刻 (UTC)	失敗または成功した、最後に検出された接続試行の時刻。	シングルセッションおよびマルチセッション
最終接続ユーザー	最後にマシンへの接続を試行したユーザーのSAM名（「DOMAIN\user」の形式）。SAM名が利用できない場合は、SIDが使用されます。	シングルセッションおよびマルチセッション
Secure ICA® アクティブ	現在のセッションでSecureICAがアクティブであるかどうかを示します。マルチセッションマシンでは常にnullです。	シングルセッションおよびマルチセッション

ホスティング

ホスティングカテゴリの列。

列	説明	適用対象
VM	セッションを実行しているホストされたマシンの、ハイパーバイザーによって使用されるフレンドリ名。これは、マシン	シングルセッションおよびマルチセッション

列	説明	適用対象
	のDNS名またはAD名のいずれとも必ずしも一致しません。	
ホスティングサーバー名	管理対象の場合、マシンをホストしているハイパーバイザーのDNS名。	シングルセッションおよびマルチセッション
接続	セッションをホストしているマシンに割り当てられているホスト接続の名前。	シングルセッションおよびマルチセッション
保留中の更新	ホストされたマシンのVMイメージが古くなっており、マシンの次回の再起動時に新しいイメージに更新される予定であるかどうかを示します。	シングルセッションおよびマルチセッション
ユーザー変更の永続性	ユーザーの変更がどのように処理されるか、つまり変更が永続的であるかどうかを示します。 • OnLocal: Persistent. ユーザーの変更はローカルに保存されます。 • Discard: Non-persistent. ユーザーの変更は破棄されます。	シングルセッションおよびマルチセッション

列	説明	適用対象
保留中の電源アクション	そのマシンに対して保留中の電源アクションがあるかどうかを示します。	シングルセッションおよびマルチセッション
電源状態	マシンの電源状態。可能な値: Unmanaged、Unknown、Unavailable、Off、On、Suspended、TurningOn、TurningOff、Suspending、Resuming。	シングルセッションおよびマルチセッション
使用後にシャットダウン	電源管理されたシングルセッションマシンにのみ適用されます。マシンが汚染されており、すべてのセッションが終了した後にシャットダウンするかどうかを示します。	シングルセッションのみ
	注: マシンがメンテナンスモードの場合、シャットダウンしません。メンテナンスモードを解除した後にのみシャットダウンします。	

登録

登録カテゴリの列。

列	説明	適用対象
最終登録失敗	マシンがブローカーから最後に登録解除された理由。	シングルセッションおよびマルチセッション
	指定可能な値は、AgentShutdown、AgentSuspended、AgentRequested、IncompatibleVersion、AgentAddressResolutionFailed、AgentNotContactable、AgentWrongActiveDirectoryOU、EmptyRegistrationRequest、MissingRegistrationCapabilities、MissingAgentVersion、InconsistentRegistrationCapabilities、NotLicensedForFeature、UnsupportedCredentialSecurityVersion、InvalidRegistrationRequest、SingleMultiSessionMismatch、FunctionalLevelTooLowForCatalog、FunctionalLevelTooLowForDesktopGroup、PowerOff、DesktopRestart、DesktopRemoved、AgentRejectedSettingsUpdate、	

列	説明	適用対象
	SendSettingsFailure、SessionAuditFailure、SessionPrepareFailure、ContactLost、SettingsCreationFailure、UnknownError、およびBrokerRegistrationLimitReachedです。	
最終登録失敗時刻 (UTC)	マシンが最後に登録解除された時刻。	シングルセッションおよびマルチセッション
登録状態	マシンの登録状態。指定可能な値：Unregistered、Initializing、Registered、およびAgentError。	シングルセッションおよびマルチセッション
障害状態	マシンの現在の障害状態の概要。指定可能な値： • なし: 障害なし。マシンは正常です。 • 起動失敗: マシンの前回の電源投入操作が失敗しました。 • 起動停止: 電源投入後、マシン	シングルセッションおよびマルチセッション

列	説明	適用対象	
	が起動に失敗しました。 • 未登録: マシンが予期された期間内に登録に失敗したか、登録が拒否されました。 • 最大容量: マシンが最大容量に達していると報告しています。		

セッションの詳細

「**セッションの詳細**」カテゴリの列。

列	説明	適用対象
起動元	現在の仲介セッションの起動に使用されたStoreFrontサーバーのホスト名。マルチセッションマシンでは常にnullです。	シングルセッションおよびマルチセッション
起動元 (IP)	現在の仲介セッションの起動に使用されたStoreFrontサーバーのIPアドレス。マルチセッションマシンでは常にnullです。	シングルセッションおよびマルチセッション
セッション変更時刻 (UTC)	現在のセッションの最終状態変更時刻。	シングルセッションのみ
SmartAccessフィルター	現在のセッションのSmart Accessタグ。マルチセッションマシンでは常にnullです。	シングルセッションおよびマルチセッション

セッション

セッションカテゴリの列。

列	説明	適用対象
セッションの状態	現在のセッションの状態。可能な値: Other、PreparingSession、Connected、Active、Disconnected、Reconnecting、NonBrokeredSession、Unknown。	シングルセッションのみ
現在のユーザー	現在のセッションのユーザー名（「DOMAIN\user」の形式）。	シングルセッションのみ
開始時刻 (UTC)	現在のセッションの開始時刻。	シングルセッションのみ
セッション数	マシン上のセッション数。	マルチセッションのみ

セッションのアクションと列

この記事では、参照用にマシンアクションと列を説明とともに一覧表示します。

アクション

セッションに対して実行できるアクションとその説明を表示します。

アクション	説明	適用対象セッション
ログオフ	セッションからユーザーをログオフします。	シングルセッションOSマシンまたはマルチセッションOSマシン
メッセージを送信	セッションのユーザーにメッセージを送信します。	シングルセッションOSマシンまたはマルチセッションOSマシン

アクション	説明	適用対象セッション
マシンの表示	セッションのホストマシンを表示します。	シングルセッションOSマシンまたはマルチセッションOSマシン
切断	セッションを切断します。セッションが切断されても、セッションはアクティブなままでアプリケーションは実行され続けますが、ユーザーデバイスはDelivery Controllerと通信しなくなります。	シングルセッションOSマシンまたはマルチセッションOSマシン
マシンのシャットダウン	セッションに関連付けられているマシンをシャットダウンします。	シングルセッションOSマシン
マシンの再起動	セッションに関連付けられているマシンを再起動します。	シングルセッションOSマシン

列

セッションの列とその説明を表示します。

列	説明
現在のユーザー	ユーザーの名前。ユーザーのユーザープリンシパル名(UPN)。
名前	セッションをホストしているマシンのDNSホスト名。
デリバリーグループ	セッションをホストしているマシンを含むデリバリーグループの名前。
マシンカタログ	セッションをホストしているマシンを含むマシンカタログの名前。

列	説明
エージェントバージョン	セッションをホストしているマシンにインストールされているCitrix Virtual Delivery Agent (VDA) のバージョン。
使用中のアプリケーション	セッションで使用されているアプリケーションのリスト。管理名で識別されます。
自律的に仲介済み	これは、仲介されずに直接接続によって確立されたHDX™セッションであるかどうか。
仲介時間 (UTC)	セッションが仲介された時刻。
仲介ユーザー名	ブローカーユーザーの名前。
クライアント (IP)	セッションに接続されているクライアントのIPアドレス。
クライアント	セッションに接続されているクライアントのホスト名。
プラグインバージョン	セッションに接続されているクライアントで実行されているCitrix Workspace™アプリのバージョン。
接続元	受信接続のホスト名。通常はゲートウェイ、ルーター、またはクライアントです。
接続元 (IP)	受信接続のIPアドレス。通常はゲートウェイ、ルーター、またはクライアントです。
割り当ての種類	セッションが共有か専用か。
非表示	セッションがユーザーから非表示になっているか、再接続

列	説明
	されないように設定されているか。
VM	セッションをホストしているVMの、ハイパーバイザーで使用されているフレンドリ名。これは、マシンのDNS名またはAD名のいずれとも必ずしも一致しません。
ホスティングサーバー名	セッションのホスティングマシンをホストしているハイパーバイザーのDNS名。
接続	セッションをホストしているマシンに割り当てられているホスト接続の名前。
更新保留中	ホストされているマシンのVMイメージが古く、次回のマシン再起動時に新しいイメージに更新される予定であるかどうか。
メンテナンスモード	セッションをホストしているマシンがメンテナンスモードであるかどうか。
IPアドレス	セッションをホストしているマシンのIPアドレス。
物理的であるか	セッションをホストしているマシンが物理的であるかどうか。`True` はマシンが物理的であることを示し、これはDelivery Controllersによって電源管理されていないことを意味します。`False` はそうでないことを示します。

列	説明
起動元	セッションの起動に使用されたStoreFront™サーバーのホスト名。セッションがWorkspace経由で起動された場合は空白です。
起動元 (IP)	セッションの起動に使用されたStoreFrontサーバーのIPアドレス。セッションがWorkspace経由で起動された場合は空白です。
OSタイプ	セッションをホストしているオペレーティングシステムの識別文字列。
ユーザー変更の永続性	ユーザーの変更がどのように処理されるか、変更が永続的であるかを示します。 • OnLocal: 永続的。ユーザーの変更はローカルに保存されます。 • Discard: 非永続的。ユーザーの変更は破棄されます。
接続タイプ	HDX、RDP、Consoleなど、セッションに使用されるプロトコル。 **注記:** XenDesktop® 5 VDA上のコンソールセッションの場合、このフィールドは空白です。

列	説明
プロビジョニングの種類	セッションをホストしているマシンがどのようにプロビジョニングされたか • 手動: PVSまたはMCSを使用してプロビジョニングされていません。 • PVS: PVSによってプロビジョニングされました（物理マシン、ブレードマシン、仮想マシン）。 • MCS: MCSによってプロビジョニングされました（VMのみ）。
Secure ICA® アクティブ	セッションでSecureICAがアクティブであるかどうか。
セッションの状態	セッションの状態。可能な値: 接続済み、アクティブ、または切断済み。L7より前の機能レベルのマシン上のセッションでは、PreparingSession、Reconnecting、NonBrokeredSession、Other、Unknownなどの他の状態が発生する場合があります。
セッション変更時刻	セッションの最新の状態変更時刻。
アプリケーションの状態	セッション内のアプリケーションの状態。可能な値: PreLogon、PreLaunched、Active、Desktop、Lingering、NoApps。

列	説明
セッションサポート	セッションをホストしているマシンが複数セッションをサポートするか、単一セッションをサポートするか。
ゾーン	セッションをホストしているマシンが配置されているゾーンの名前。
SmartAccessフィルター	セッションのSmart Accessタグ。
開始時刻 (UTC)	セッションが開始された日時。
状態	マシンの概要状態。可能な値 : Unregistered、Disconnected、またはInUse。
状態時間 (UTC)	セッションが現在の状態になってからの時間。
デリバリーコントローラー™	セッションのホストマシンが登録されているコントローラーのDNSホスト名。
ユーザー表示名	ユーザーのフルネーム。
デスクトップ表示名	セッションの起動に元々使用されたマシンの公開名。Citrix Workspaceアプリまたはストアフロントに表示される名前です。アプリケーションセッションの場合、そのアプリケーションが終了していても、セッションに起動された最初のアプリケーションの名前です。リソースが後で名前変更または削除されても、名前は変更されません。

セキュリティキー

重要:

- この機能は、StoreFront™ 1912 LTSR CU2以降と組み合わせて使用する必要があります。
- Secure XML機能は、Citrix ADCおよびCitrix Gatewayリリース12.1以降でのみサポートされています。

注:

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

この機能を使用すると、承認された StoreFront および Citrix Gateway マシンのみが Delivery Controller と通信できるようになります。この機能を有効にすると、キーを含まないすべての要求がブロックされます。この機能を使用して、内部ネットワークから発生する攻撃から保護するための追加のセキュリティ層を追加します。

この機能を使用するための一般的なワークフローは次のとおりです。

1. Web Studioを有効にして、機能設定を表示します。
2. サイトの設定を構成します。
3. StoreFrontの設定を構成します。
4. Citrix ADCの設定を構成します。

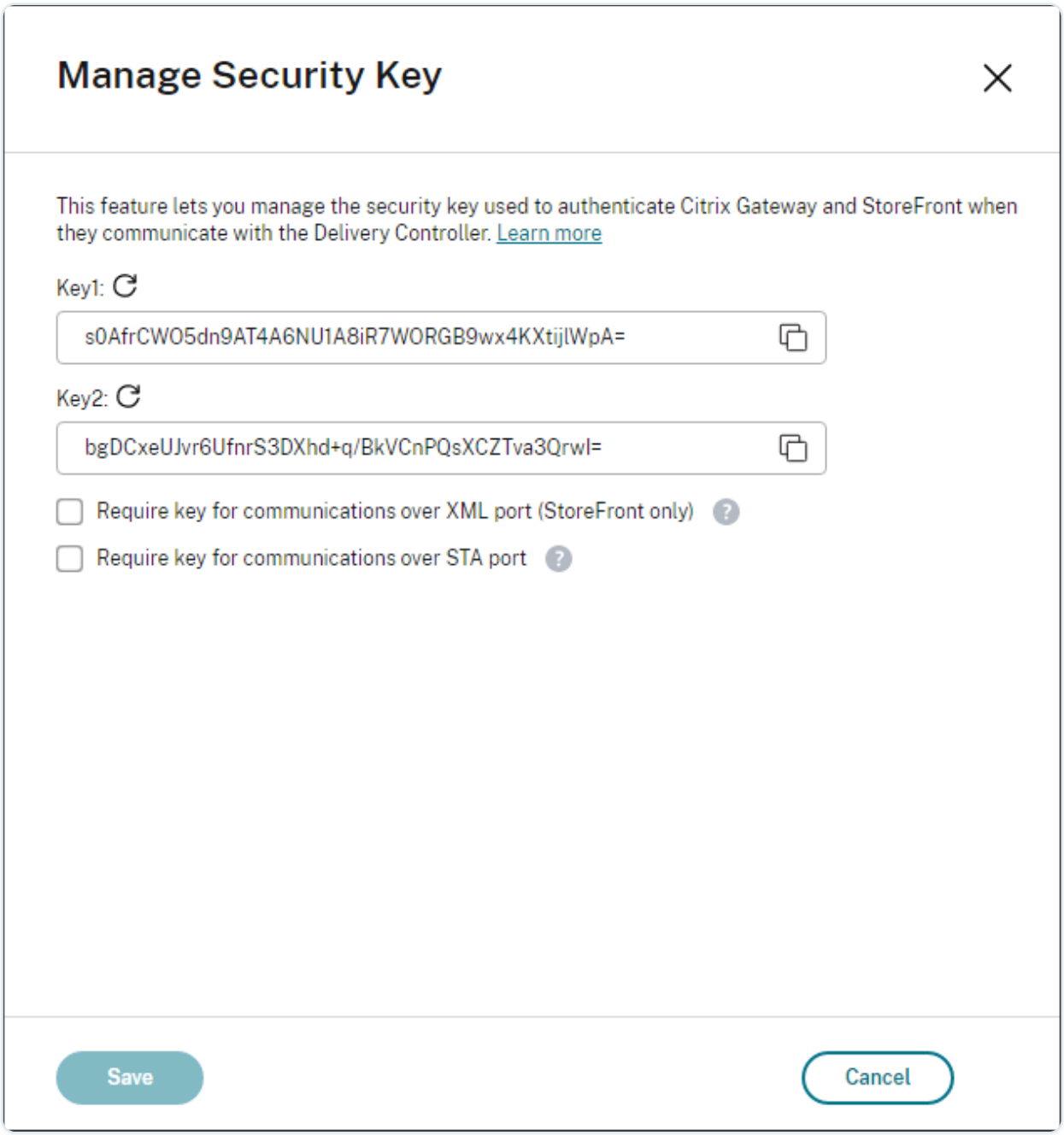
サイトの設定を構成する

Web StudioまたはPowerShellを使用して、サイトのセキュリティキー設定を構成できます。

Web Studioを使用する

1. Web Studioにサインインし、左ペインで**設定**を選択します。

2. **セキュリティキーの管理**タイルを見つけて**編集**をクリックします。**セキュリティキーの管理**ページが表示されます。



3. キーを生成するには、更新アイコンをクリックします。

重要:

- 使用できるキーは2つあります。XMLポートおよびSTAポートを介した通信には、同じキーまたは異なるキーを使用できます。一度に1つのキーのみを使用することをお勧めします。未使用のキーは、キーのローテーションにのみ使用されます。

> - 使用中のキーを更新するために更新アイコンをクリックしないでください。クリックすると、サービスが中断されます。

4. 通信にキーが必要な場所を選択します。
   - **XMLポートを介した通信にキーを要求する（StoreFrontのみ）**。選択した場合、XMLポートを介した通信を認証するためにキーが必要になります。StoreFrontはこのポートを介してCitrix Cloudと通信します。XMLポートの変更については、Knowledge Centerの記事CTX127945を参照してください。
   - **STAポートを介した通信にキーを要求する**。選択した場合、STAポートを介した通信を認証するためにキーが必要になります。Citrix GatewayとStoreFrontはこのポートを介してCitrix Cloudと通信します。STAポートの変更については、Knowledge Centerの記事CTX101988を参照してください。
5. 変更を適用してウィンドウを閉じるには、**保存**をクリックします。

PowerShell を使用する

以下は、Web Studioの操作に相当するPowerShellの手順です。

1. シトリックス バーチャル アプリケーションズ アンド デスクトップ リモート PowerShell SDK を実行します。
2. コマンドウィンドウで、次のコマンドを実行します。
   - `Add-PSSnapIn Citrix*`
3. キーを生成し、Key1 を設定するには、次のコマンドを実行します。
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. キーを生成し、Key2 を設定するには、次のコマンドを実行します。
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. 通信の認証でキーの使用を有効にするには、次のコマンドのいずれかまたは両方を実行します。
   - XML ポート経由で通信を認証するには:

    - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`

- STA ポート経由で通信を認証するには:

    - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

ガイダンスと構文については、PowerShell コマンドのヘルプを参照してください。

StoreFrontの設定を構成する

サイトの構成が完了したら、PowerShellを使用してStoreFrontの関連設定を構成する必要があります。

StoreFront サーバーで、以下の PowerShell コマンドを実行します。

XMLポートを介した通信用のキーを構成するには、コマンドを使用します。例:

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [secret]
```

次のパラメータに適切な値を入力します。

- `Path to store`
- `Resource feed name`
- `secret`

STAポート経由の通信用にキーを構成するには、`New-STFSecureTicketAuthority`および`Set-STFRoamingGateway`コマンドを使用します。例:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]
```

```
Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

次のパラメータに適切な値を入力します。

- `Gateway name`
- `STA URL`
- `Secret`

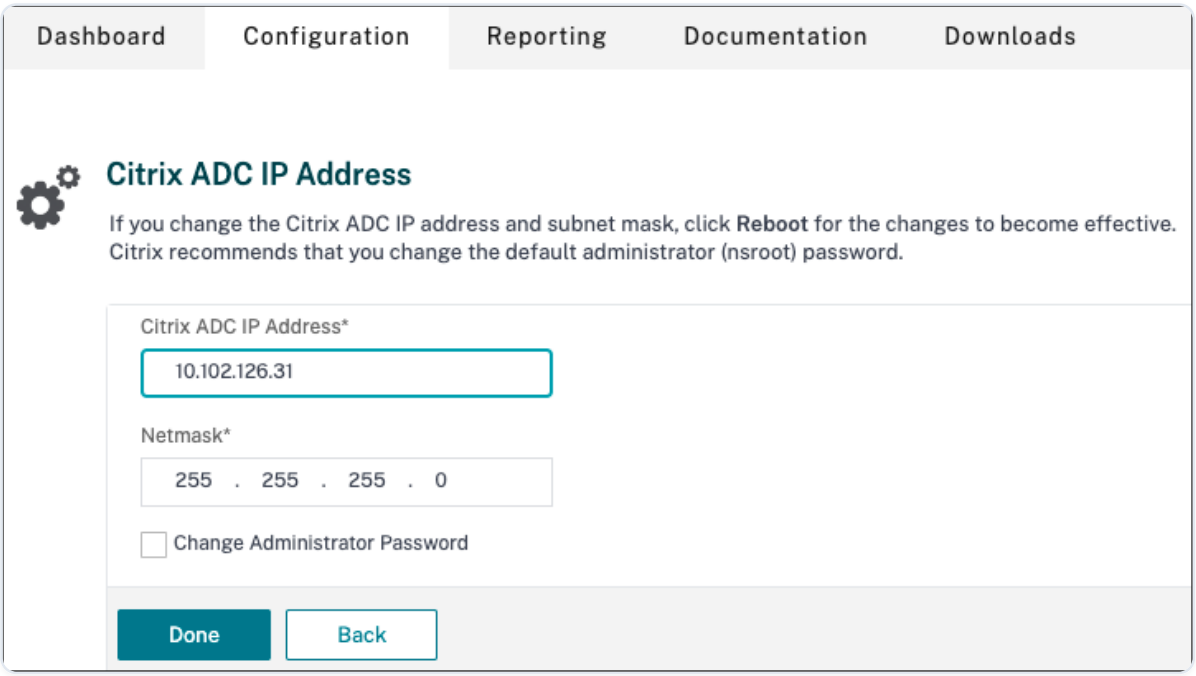
ガイダンスと構文については、PowerShellコマンドのヘルプを参照してください。

Citrix ADCの設定を構成する

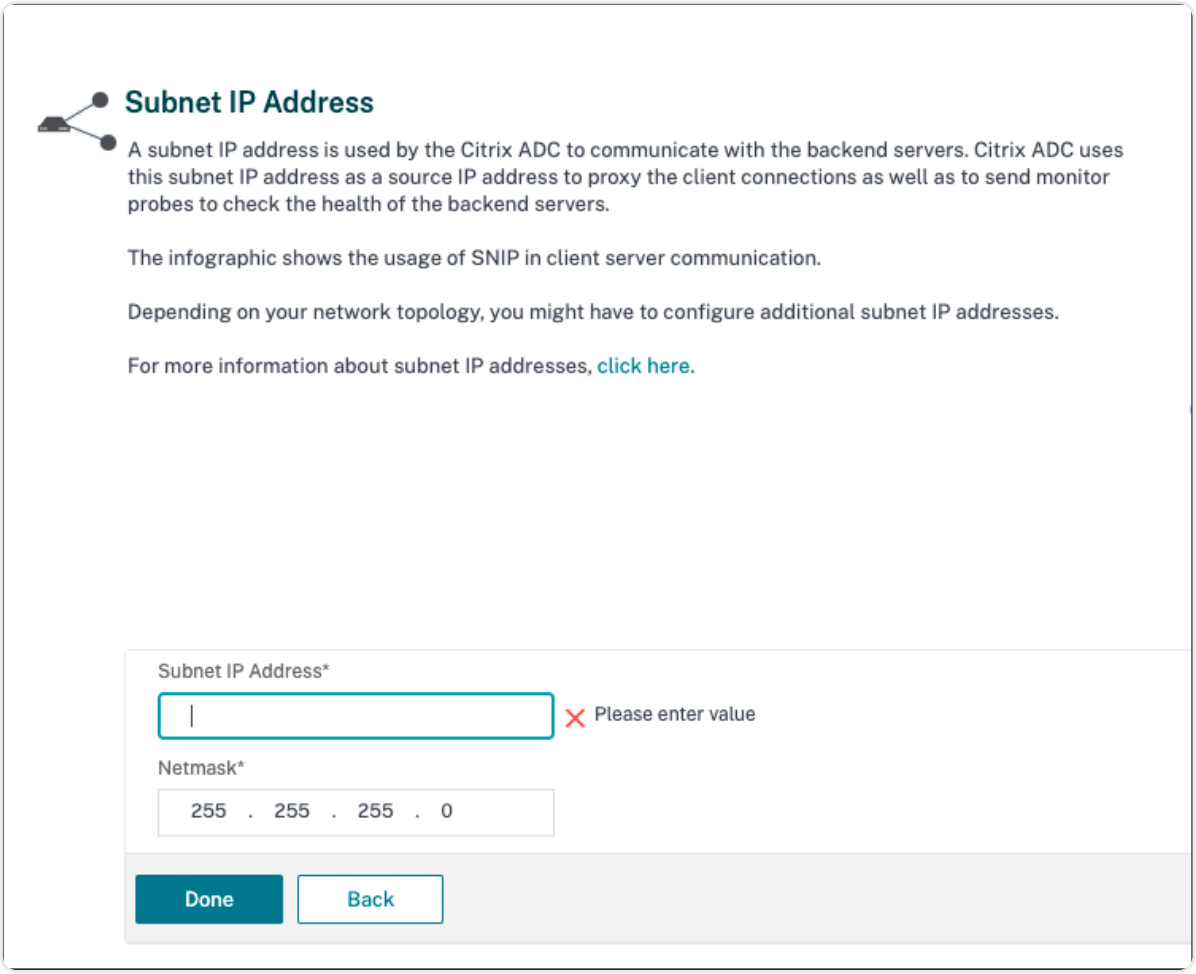
注:

Citrix ADCをゲートウェイとして使用しない限り、Citrix ADCのこの機能の構成は不要です。Citrix ADCを使用する場合は、次の手順に従います。

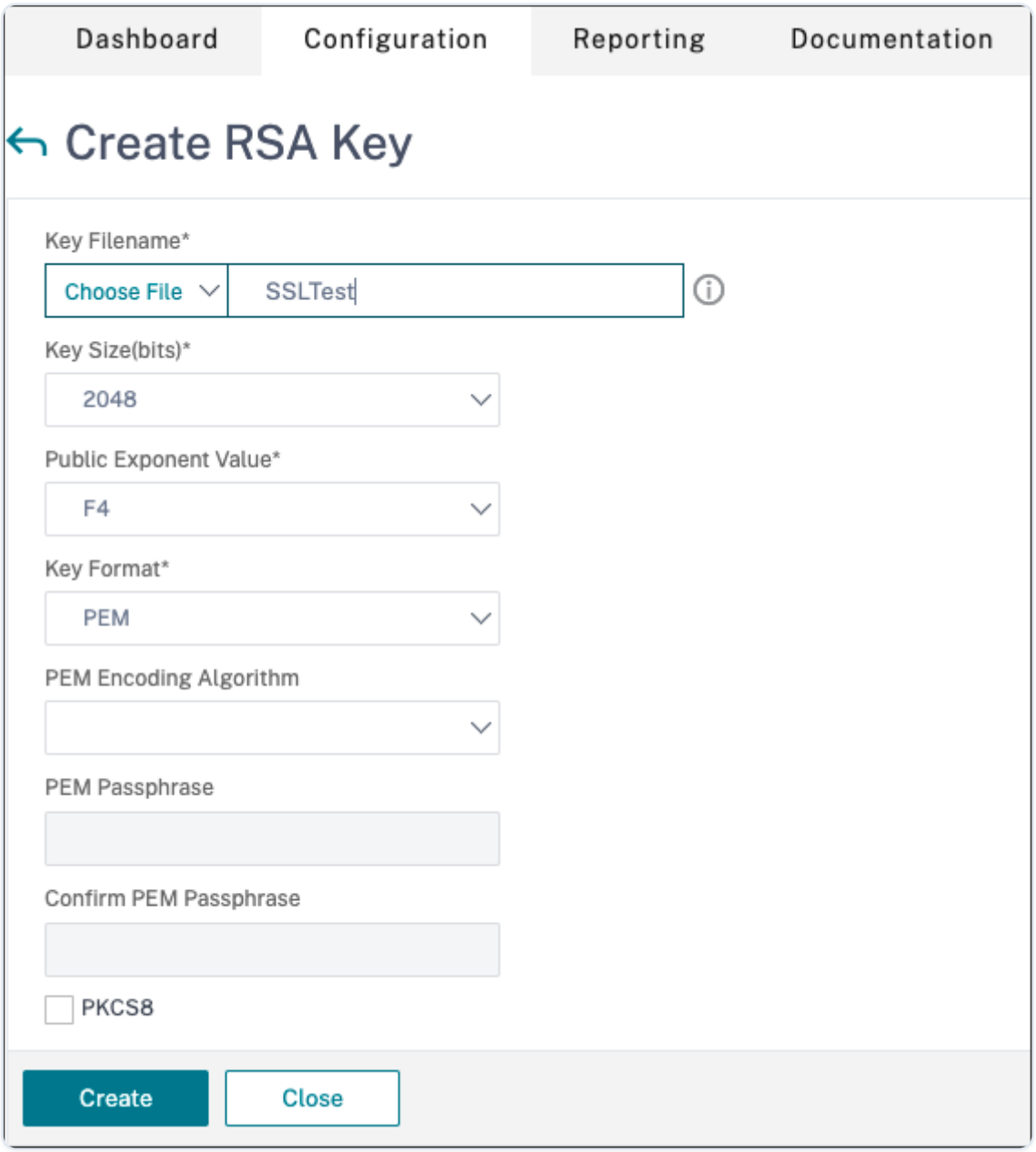
1. 以下の前提条件となる構成がすでに設定されていることを確認してください:
    - 以下のCitrix ADC関連のIPアドレスが構成されています。
        - Citrix ADCコンソールにアクセスするための Citrix ADC管理IP（NSIP）アドレス。詳細については、「NSIPアドレスの構成」を参照してください。



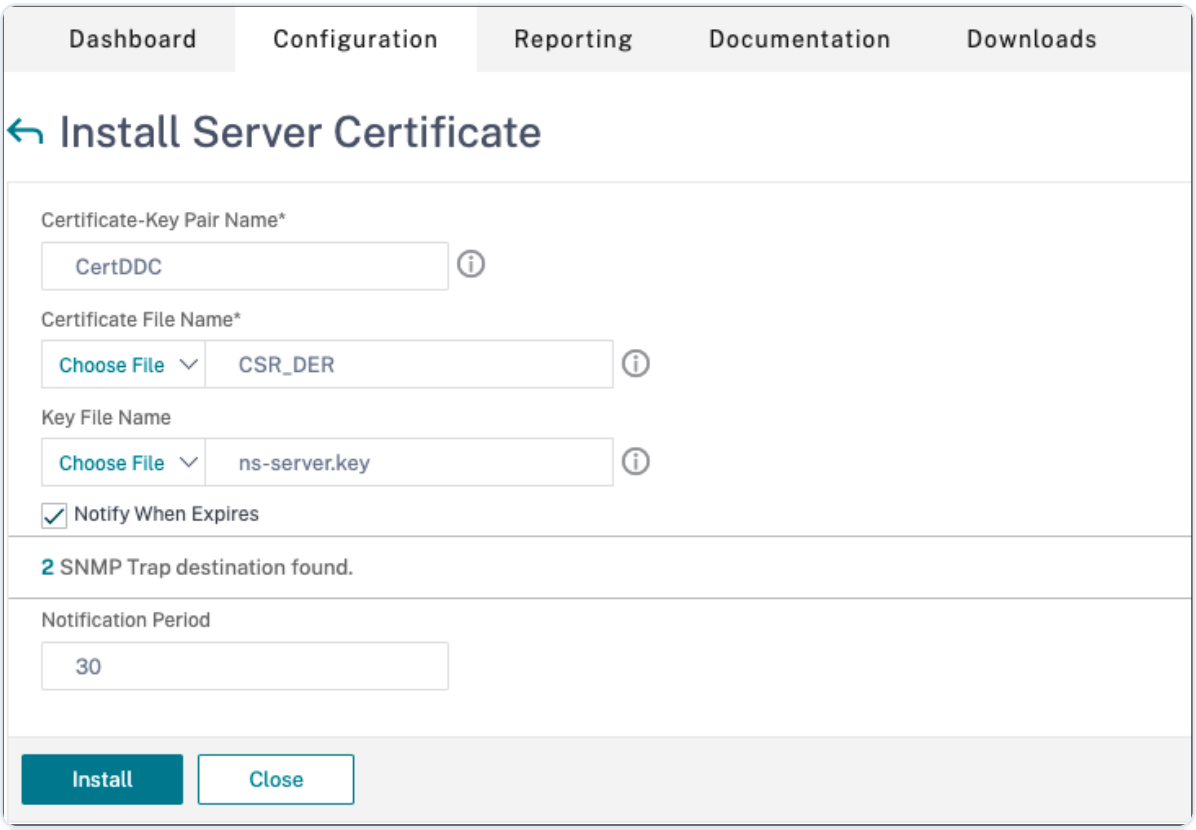
- Citrix ADCアプライアンスとバックエンドサーバー間の通信を有効にするためのサブネットIP（SNIP）アドレス。詳細については、「サブネットIPアドレスの構成」を参照してください。
- セッション起動のためにADCアプライアンスにログインするためのCitrix Gateway仮想IPアドレスとロードバランサー仮想IPアドレス。詳細については、「仮想サーバーの作成」を参照してください。

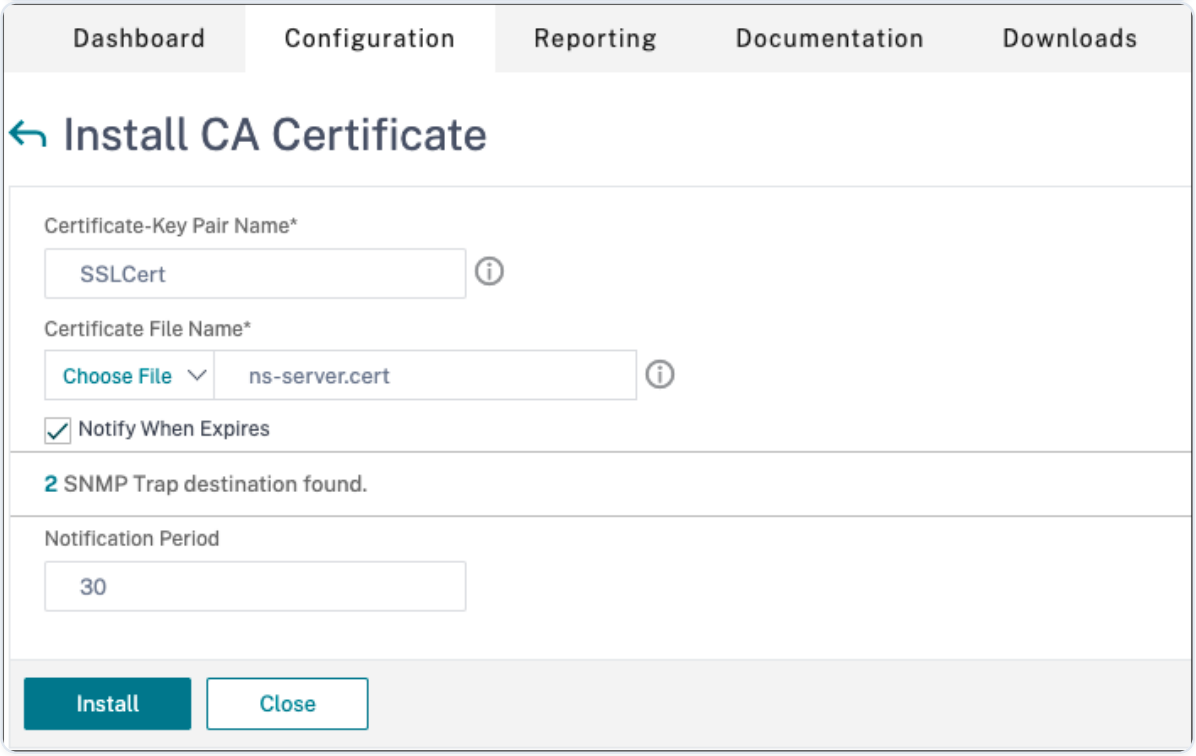


- Citrix ADCアプライアンスで必要なモードと機能が有効になっています。
  - モードを有効にするには、Citrix ADC GUIで **System > Settings > Configure Mode** に移動します。
  - 機能を有効にするには、Citrix ADC GUIで **System > Settings > Configure Basic Features** に移動します。
- 証明書関連の構成が完了しています。
  - 証明書署名要求（CSR）が作成されます。詳細については、「証明書の作成」を参照してください。

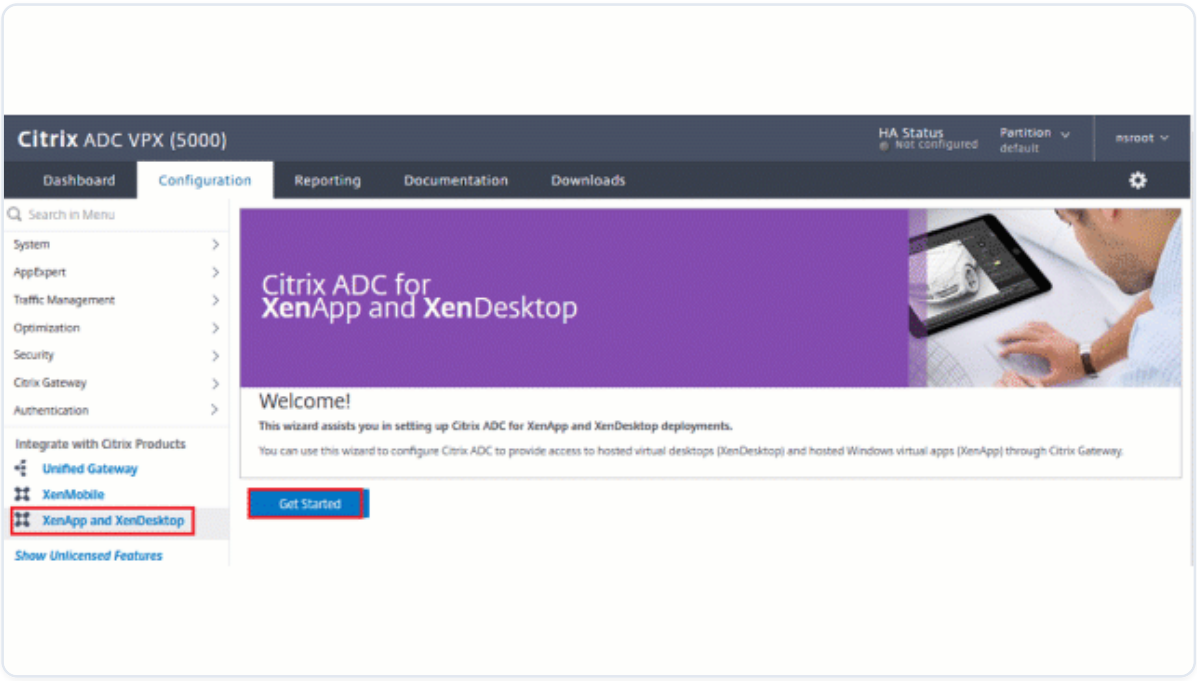


- サーバー証明書、CA証明書、およびルート証明書がインストールされます。詳細については、「インストール、リンク、および更新」を参照してください。





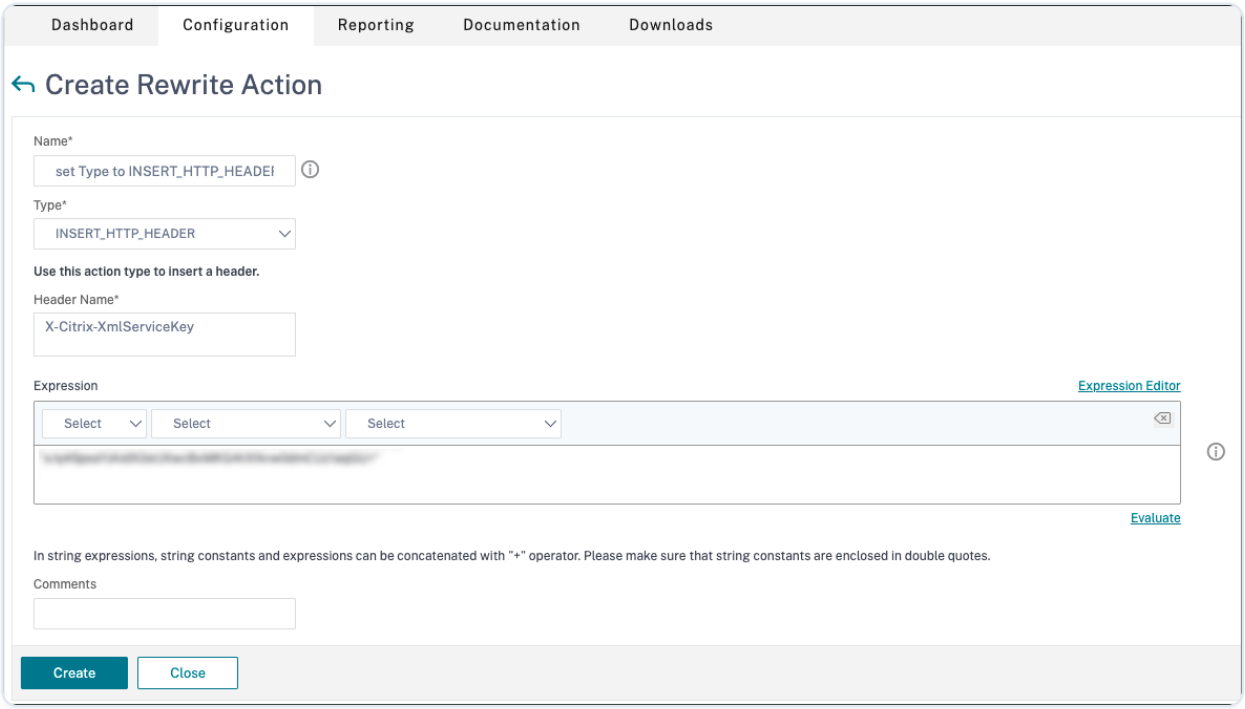
- Citrix Virtual Desktops用にCitrix Gatewayが作成されました。**Test STA Connectivity**ボタンをクリックして接続をテストし、仮想サーバーがオンラインであることを確認します。詳細については、「Citrix Virtual Apps and Desktops向けCitrix ADCのセットアップ」(/ja-jp/citrix-adc/current-release/solutions/deploy-xa-xd.html)を参照してください。



2. リライトアクションを追加します。詳細については、「リライトアクションの構成」を参照してください。

   a. **AppExpert > Rewrite > Actions**に移動します。

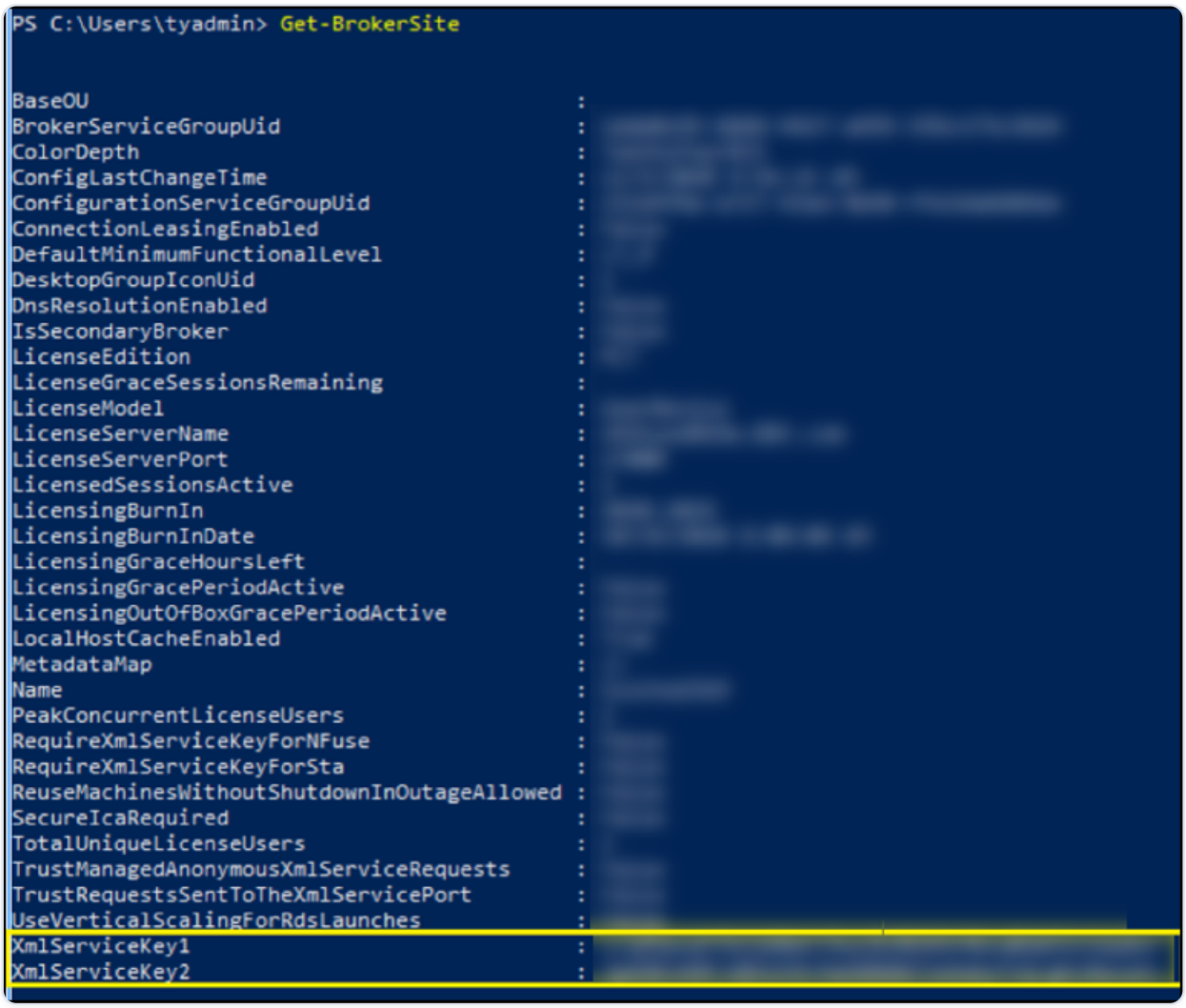
   b. **Add**をクリックして、新しいリライトアクションを追加します。アクションの名前は「set Type to INSERT_HTTP_HEADER」にすることができます。



   a. **タイプ**で、**INSERT_HTTP_HEADER**を選択します。

   b. **ヘッダー名**に「X-Citrix-XmlServiceKey」と入力します。

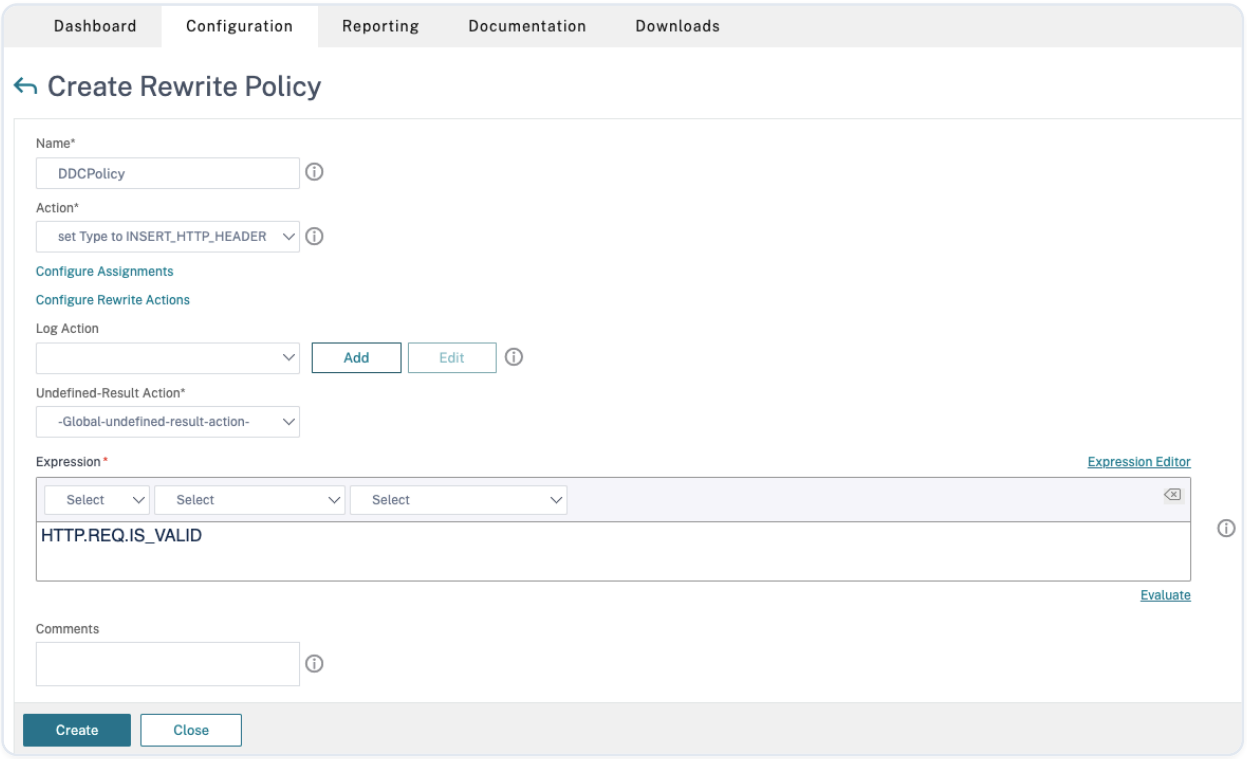
c. **式**に、引用符付きで `<XmlServiceKey1 value>` を追加します。XmlServiceKey1 の値は、Desktop Delivery Controller™ の構成からコピーできます。



3. 書き換えポリシーを追加します。詳細については、「書き換えポリシーの構成」を参照してください。

   a. 「**AppExpert > Rewrite > Policies**」に移動します。

   b. 新しいポリシーを追加するには、**追加**をクリックします。



a. 「**アクション**」で、以前の手順で作成したアクションを選択します。

b. 「**式**」で、HTTP.REQ.IS_VALIDを追加します。

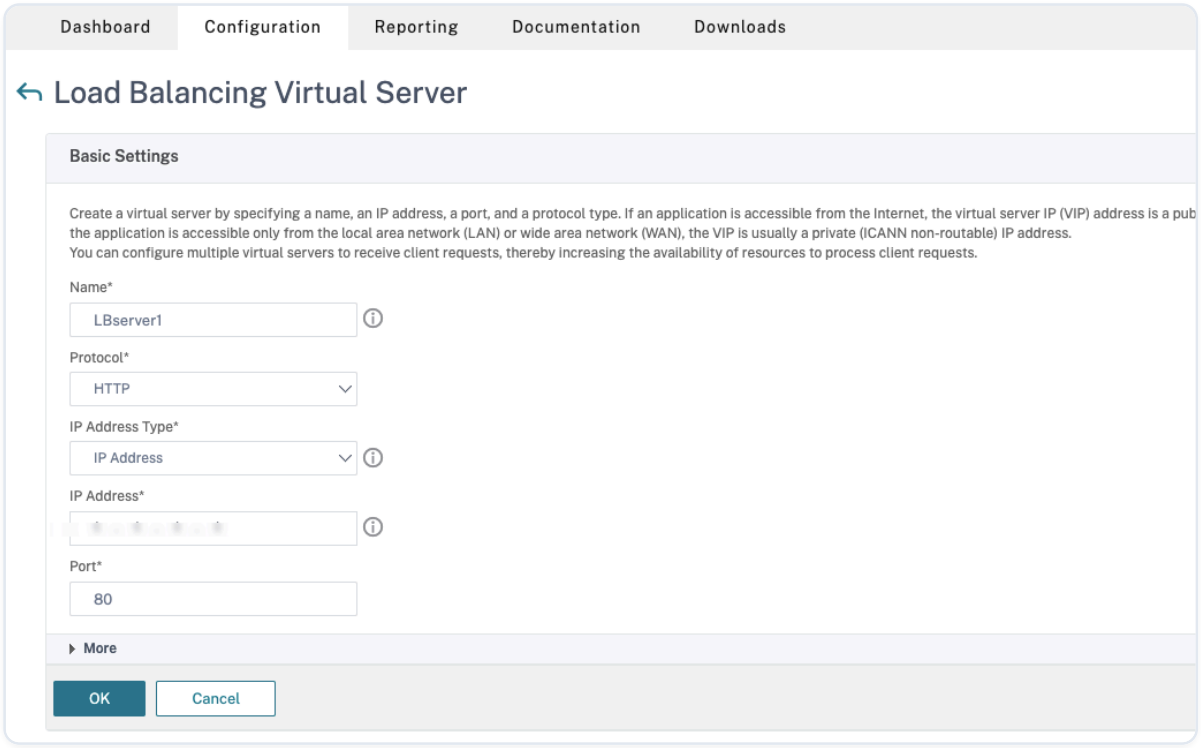
c. 「**OK**」をクリックします。

4. 負荷分散を設定します。STAサーバーごとに1つの負荷分散仮想サーバーを構成する必要があります。構成しない場合、セッションの起動に失敗します。

   詳細については、基本的な負荷分散の設定を参照してください。

   a. 負荷分散仮想サーバーを作成します。

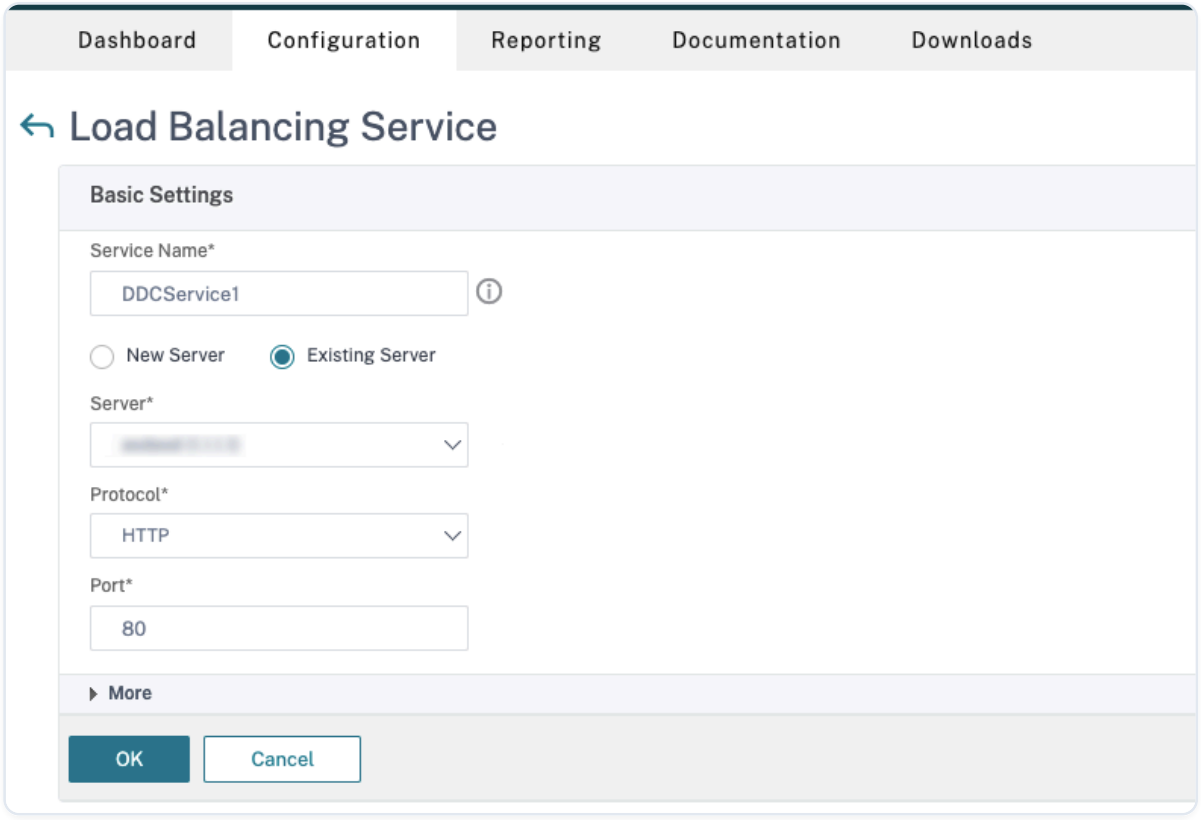
      - **トラフィック管理 > ロードバランシング > サーバー**に移動します。
      - 「**仮想サーバー**」ページで、「**追加**」をクリックします。



- **Protocol**で、**HTTP**を選択します。
- 負荷分散仮想IPアドレスを追加し、**Port**で**80**を選択します。
- **OK**をクリックします。

b. 負荷分散サービスを作成します。

- **トラフィック管理 > ロードバランシング > サービス**に移動します。



- **Existing Server**で、前のステップで作成した仮想サーバーを選択します。
- **Protocol**で**HTTP**を選択し、**Port**で**80**を選択します。
- **OK**をクリックし、その後**Done**をクリックします。

c. サービスを仮想サーバーにバインドします。

- 以前に作成した仮想サーバーを選択し、「**Edit**」をクリックします。
- **サービスとサービスグループ**で、**ロードバランシング仮想サーバーサービスバインディングなし**をクリックします。

仮想サーバーにサービスをバインドします(/en-us/citrix-virtual-apps-desktops/2407/media/adc-bind-service-to-lbvserver.png)

- 「**Service Binding**」で、以前に作成したサービスを選択します。
- 「**Bind**」をクリックします。

d. 以前に作成したリライトポリシーを仮想サーバーにバインドします。

- 以前に作成した仮想サーバーを選択し、「**Edit**」をクリックします。
- 「**Advanced Settings**」で「**Policies**」をクリックし、次に「**Policies**」セクションで「**+**」をクリックします。

リライトポリシーをバインドします(/en-us/citrix-virtual-apps-desktops/2407/media/adc-bind-rewrite-policy.png)

- 「**Choose Policy**」で「**Rewrite**」を選択し、「**Choose Type**」で「**Request**」を選択します。
- 「**Continue**」をクリックします。
- 「**ポリシーの選択**」で、以前作成した書き換えポリシーを選択します。
- 「**バインド**」をクリックします。
- 「**完了**」をクリックします。

e. 必要に応じて、仮想サーバーの永続性を設定します。

- 以前作成した仮想サーバーを選択し、「**編集**」をクリックします。
- 「**詳細設定**」で、「**永続性**」をクリックします。

永続性の設定(/en-us/citrix-virtual-apps-desktops/2407/media/adc-lb-vserver-persistence.png)

- 永続性の種類として**その他**を選択します。
- 仮想サーバーによって選択されたサービスのIPアドレス（宛先IPアドレス）に基づいて永続性セッションを作成するには、**DESTIP**を選択します。
- **IPv4ネットマスク**で、DDCと同じネットワークマスクを追加します。
- **OK**をクリックします。

f. 他の仮想サーバーについても、これらの手順を繰り返します。

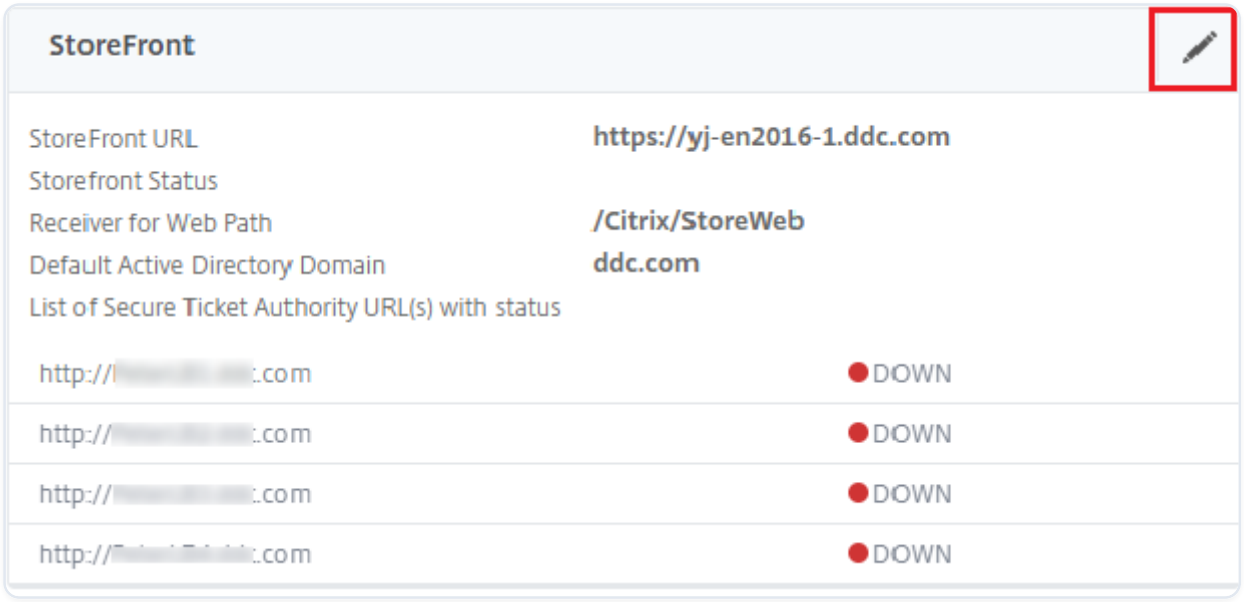
Citrix ADCアプライアンスがCitrix Virtual Desktops™で既に構成されている場合の構成の変更点

Citrix ADCアプライアンスをCitrix Virtual Desktopsで既に構成している場合、Secure XML機能を使用するには、以下の構成変更を行う必要があります。

- セッション起動前に、ゲートウェイの「**セキュリティチケット機関のURL**」を変更して、負荷分散仮想サーバーのFQDNを使用するようにします。
- `TrustRequestsSentToTheXmlServicePort`パラメーターがFalseに設定されていることを確認します。デフォルトでは、`TrustRequestsSentToTheXmlServicePort`パラメーターはFalseに設定されています。ただし、お客様がCitrix Virtual Desktops用にCitrix ADCをすでに構成している場合、`TrustRequestsSentToTheXmlServicePort`はTrueに設定されます。

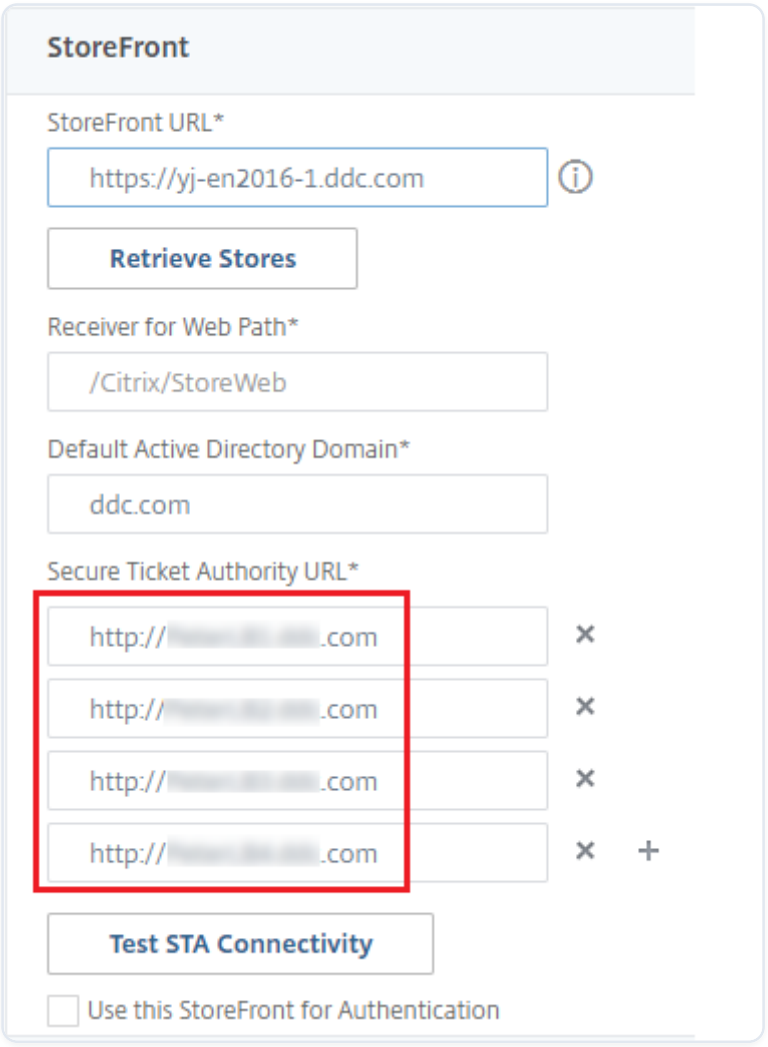
1. Citrix ADC GUIで、**「Configuration」>「Integrate with Citrix Products」**の順に移動し、「XenApp and XenDesktop®」**をクリックします。
2. ゲートウェイインスタンスを選択し、編集アイコンをクリックします。

   既存のゲートウェイ構成を編集(/en-us/citrix-virtual-apps-desktops/2407/media/edit-gateway-instance.png)
3. StoreFrontペインで、編集アイコンをクリックします。



4. **Secure Ticket Authority URL**を追加します。

   - Secure XML機能が有効になっている場合、STA URLはロードバランシングサービスのURLである必要があります。
   - Secure XML機能が無効になっている場合、STA URLはSTAのURL（DDCのアドレス）である必要があり、DDC上の`TrustRequestsSentToTheXmlServicePort`パラメーターはTrueに設定されている必要があります。



セッションの回復性設定

セッションアクティビティを維持することは、最高のユーザーエクスペリエンスを提供するために不可欠です。信頼性の低いネットワーク、変動の大きいネットワーク遅延、ワイヤレスデバイスの範囲制限による接続の喪失は、ユーザーの不満につながる可能性があります。デバイス間を素早く移動し、ログオンするたびに同じアプリケーションにアクセスすることは、医療従事者などの多くのモバイルワーカーにとって優先事項です。

この記事で説明する機能は、セッションの信頼性を最適化し、不便、ダウンタイム、生産性の損失を軽減します。これらの機能を使用することで、モバイルユーザーはデバイス間を迅速かつ簡単に移動できます。

セッションの信頼性

セッションの信頼性により、ネットワーク接続が中断された場合でも、セッションはアクティブな状態を維持し、ユーザーの画面に表示されます。ユーザーは、ネットワーク接続が再開されるまで、使用しているアプリケーションを引き続き見ることができます。

この機能は、ワイヤレス接続を使用するモバイルユーザーにとって特に便利です。たとえば、ワイヤレス接続を使用しているユーザーが鉄道トンネルに入り、一時的に接続が失われたとします。通常、セッションは切断され、ユーザーの画面から消え、ユーザーは切断されたセッションに再接続する必要があります。セッションの信頼性を使用すると、セッションはマシン上でアクティブなままになります。接続が失われたことを示すために、ユーザーのディスプレイはフリーズし、カーソルは砂時計のアイコンに変わり、トンネルの反対側で接続が再開されるまでその状態が続きます。ユーザーは中断中もディスプレイにアクセスし続け、ネットワーク接続が復元されるとアプリケーションとの対話を再開できます。セッションの信頼性により、再認証のプロンプトなしでユーザーが再接続されます。

Citrix Workspace™アプリのユーザーは、Controllerの設定を上書きできません。

セッションの信頼性は、トランスポート層セキュリティ（TLS）と併用できます。TLSは、ユーザーデバイスとCitrix Gatewayの間で送信されるデータのみを暗号化します。

セッションの信頼性を有効にして構成するには、次のポリシー設定を使用します。

- 「セッションの信頼性接続」ポリシー設定は、セッションの信頼性を許可または禁止します。
- 「セッションの信頼性タイムアウト」ポリシー設定のデフォルトは180秒、つまり3分です。セッションの信頼性がセッションを開いたままにする時間を延長することはできますが、この機能はユーザーの利便性のために設計されています。そのため、ユーザーに再認証を促すことはありません。セッションを開いたままにする時間を延長すると、ユーザーが注意をそらされてユーザーデバイスから離れる可能性が高まります。これらの行動は、セッションを不正なユーザーがアクセスできる状態にする可能性があります。
- 受信セッションの信頼性接続は、ポート2598を使用します。ただし、「セッションの信頼性ポート番号」ポリシー設定でポート番号を変更した場合は除きます。
- ユーザーが再認証なしで中断されたセッションに再接続できないようにするには、自動クライアント再接続機能を使用します。中断されたセッションに再接続する際にユーザーに再認証を促すように、「自動クライアント再接続認証」ポリシー設定を構成できます。

セッションの信頼性と自動クライアント再接続の両方を使用する場合、これら2つの機能は順次動作します。セッションの信頼性は、「セッションの信頼性タイムアウト」ポリシー設定で指定した時間の経過後にユーザーセッションを閉じ、または切断します。その後、自動クライアント再接続ポリシー設定が有効になり、ユーザーを切断されたセッションに再接続しようとします。

クライアントの自動再接続

自動クライアント再接続機能を使用すると、Citrix Workspaceアプリは意図しないICA®セッションの切断を検出し、影響を受けるセッションにユーザーを自動的に再接続できます。この機能が

サーバーで有効になっている場合、ユーザーは作業を続行するために手動で再接続する必要はありません。

アプリケーションセッションの場合、Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルするまで、セッションへの再接続を試みます。

デスクトップセッションの場合、Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルしない限り、指定された期間、セッションへの再接続を試行します。デフォルトでは、この期間は5分です。この期間を変更するには、ユーザーデバイスで次のレジストリ設定を編集します（`seconds`は、セッションの再接続がそれ以上試行されなくなるまでの秒数です）。

`HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>`

次のポリシー設定で自動クライアント再接続を有効にして構成します。

- **自動クライアント再接続:** 接続が中断された後にCitrix Workspaceアプリによる自動再接続を有効または無効にします。
- **自動クライアント再接続認証:** 自動再接続後のユーザー認証の要件を有効または無効にします。
- **自動クライアント再接続ログ記録:** イベントログへの再接続イベントのログ記録を有効または無効にします。ログ記録はデフォルトで無効になっています。有効にすると、サーバーのシステムログに、成功した自動再接続イベントと失敗した自動再接続イベントに関する情報が記録されます。各サーバーは、再接続イベントに関する情報を独自のシステムログに保存します。サイトは、すべてのサーバーの再接続イベントの統合ログを提供しません。

> **注：**
>
> 再認証なしの自動クライアント再接続は、パスワード認証でのみサポートされています。フェデレーション認証サービスまたはスマートカード認証を使用する場合、再認証なしの自動クライアント再接続はサポートされません。そのような場合、ユーザーはログイン画面にリダイレクトされます。

> 自動クライアント再接続には、暗号化されたユーザー資格情報に基づく認証メカニズムが組み込まれています。ユーザーが最初にログオンすると、サーバーはユーザー資格情報を暗号化してメモリに保存します。サーバーはまた、暗号化キーを含むCookieを作成し、Citrix Workspaceアプリに送信します。Citrix Workspaceアプリは、再接続のためにキーをサー

> バーに送信します。サーバーは資格情報を復号化し、認証のためにWindowsログオンに送信します。Cookieの有効期限が切れると、ユーザーはセッションに再接続するために再認証する必要があります。

Auto Client Reconnect認証設定を有効にすると、Cookieは使用されません。代わりに、Citrix Workspaceアプリが自動的に再接続を試みるときに、資格情報を要求するダイアログボックスがユーザーに表示されます。

ユーザー資格情報とセッションを最大限に保護するために、クライアントとサイト間のすべての通信に暗号化を使用してください。

icaclient.admファイルを使用して、Windows版Citrix Workspaceアプリで自動クライアント再接続を無効にします。詳細については、お使いのWindows版Citrix Workspaceアプリのバージョンに関するドキュメントを参照してください。

接続の設定もAuto Client Reconnectに影響します。

- 既述のとおり、デフォルトでは、自動クライアント再接続はサイトレベルのポリシー設定によって有効になっています。ユーザーの再認証は不要です。ただし、サーバーのICA TCP接続が、切断された通信リンクでセッションをリセットするように構成されている場合、自動再接続は行われません。自動クライアント再接続は、切断された接続またはタイムアウトした接続がある場合に、サーバーがセッションを切断する場合にのみ機能します。このコンテキストでは、ICA TCP接続とは、TCP/IPネットワーク上のセッションに使用されるサーバーの仮想ポート（実際のネットワーク接続ではなく）を指します。
- デフォルトでは、サーバー上のICA TCP接続は、切断された接続またはタイムアウトした接続を持つセッションを切断するように設定されています。切断されたセッションはシステムメモリにそのまま残り、Citrix Workspaceアプリによる再接続が可能です。
- 接続は、切断された接続またはタイムアウトした接続を持つセッションをリセットまたはログオフするように構成できます。セッションがリセットされると、再接続を試みると新しいセッションが開始されます。ユーザーが使用中のアプリケーションの同じ場所に戻るのではなく、アプリケーションが再起動されます。
- サーバーがセッションをリセットするように構成されている場合、自動クライアント再接続は新しいセッションを作成します。このプロセスでは、ユーザーはサーバーにログオンするために資格情報を入力する必要があります。
- Citrix Workspaceアプリまたはプラグインが誤った認証情報を送信した場合（攻撃中に発生する可能性あり）、またはサーバーが切断された接続を検出してから時間が経ちすぎたと判断した場合、自動再接続は失敗することがあります。

ICA キープアライブ

ICA Keep-Alive機能を有効にすると、切断された接続が切断されるのを防ぎます。有効にすると、サーバーがアクティビティを検出しない場合、この機能はリモートデスクトップサービスがそのセッションを切断するのを防ぎます。アクティビティがない例としては、クロックの変更がない、マウスの動きがない、画面の更新がないなどが挙げられます。サーバーは数秒ごとにキープアライブパケットを送信して、セッションがアクティブであるかどうかを検出します。セッションがアクティブでなくなった場合、サーバーはそのセッションを切断済みとしてマークします。

> **重要:**
>
> ICA Keep-Aliveは、セッションの信頼性を使用していない場合にのみ機能します。セッションの信頼性には、切断された接続が切断されるのを防ぐための独自のメカニズムがあります。ICA Keep-Aliveは、セッションの信頼性を使用しない接続に対してのみ構成してください。

> ICA Keep-Alive設定は、Windowsグループポリシーで構成されているキープアライブ設定を上書きします。

次のポリシー設定でICA Keep-Aliveを有効にして構成します。

- **ICAキープアライブタイムアウト:** ICAキープアライブメッセージの送信に使用される間隔（1～3600秒）を指定します。途切れた接続が非常にまれで、ユーザーがセッションに再接続できることが問題にならない環境で、ネットワーク監視ソフトウェアに非アクティブな接続を閉じさせたい場合は、このオプションを構成しないでください。

  デフォルトの間隔は60秒です。ICA Keep-Aliveパケットは60秒ごとにユーザーデバイスに送信されます。ユーザーデバイスが60秒以内に応答しない場合、ICAセッションのステータスは切断済みに変わります。

- **ICAキープアライブ：** ICAキープアライブメッセージを送信または送信しないようにします。

ワークスペースコントロール

ワークスペースコントロールにより、デスクトップとアプリケーションはユーザーがデバイス間を移動しても追従します。このローミング機能により、ユーザーはログオンするだけで、どこからでもすべてのデスクトップや開いているアプリケーションにアクセスでき、各デバイスでデスクトップやアプリケーションを再起動する必要がありません。たとえば、ワークスペースコントロールは、病院で異なるワークステーション間を迅速に移動し、ログオンするたびに同じアプリケーションセットにアクセスする必要がある医療従事者を支援できます。ワークスペースコントロール

オプションを許可するように構成した場合、これらの医療従事者は、1つのクライアントデバイスで複数のアプリケーションから切断し、別のクライアントデバイスで同じアプリケーションに再接続できます。

ワークスペースコントロールは、次のアクティビティに影響します。

- **ログオン：** デフォルトでは、ワークスペースコントロールにより、ユーザーはログオン時に実行中のすべてのデスクトップとアプリケーションに自動的に再接続でき、手動で再開する必要がありません。ワークスペースコントロールを通じて、ユーザーは切断されたデスクトップやアプリケーション、および別のクライアントデバイスでアクティブなアプリケーションを開くことができます。デスクトップまたはアプリケーションから切断すると、それはサーバー上で実行されたままになります。一部のデスクトップまたはアプリケーションを1つのクライアントデバイスで実行したままにし、別のクライアントデバイスでデスクトップまたはアプリケーションの一部に再接続する必要があるローミングユーザーがいる場合、ログオン再接続動作を、以前にユーザーが切断したデスクトップまたはアプリケーションのみを開くように構成できます。
- **再接続：** サーバーにログオンした後、ユーザーはいつでも をクリックして、すべてのデスクトップまたはアプリケーションに再接続できます。デフォルトでは、 は切断されたデスクトップまたはアプリケーション、および現在別のクライアントデバイスで実行されているアプリケーションを開きます。 を、以前にユーザーが切断したデスクトップまたはアプリケーションのみを開くように構成できます。
- **ログオフ：** StoreFront™ を介してデスクトップまたはアプリケーションを開くユーザーの場合、**ログオフ** コマンドを構成して、StoreFront とすべてのアクティブなセッションからユーザーをログオフするか、StoreFront のみからログオフさせることができます。
- **切断：** ユーザーは、実行中のすべてのデスクトップとアプリケーションから一度に切断でき、個別に切断する必要はありません。

ワークスペースコントロールは、Citrix StoreFront接続を介してデスクトップおよびアプリケーションにアクセスするCitrix Workspaceアプリユーザーのみが利用できます。デフォルトでは、仮想デスクトップセッションではワークスペースコントロールは無効になっていますが、ホスト型アプリケーションでは有効になっています。公開されたデスクトップと、それらのデスクトップ内で実行されている公開されたアプリケーションの間では、デフォルトではセッション共有は行われません。

ユーザーが新しいクライアントデバイスに移動すると、ユーザーポリシー、クライアントドライブマッピング、およびプリンター構成が適切に変更されます。ポリシーとマッピングは、ユーザーがセッションにログオンしているクライアントデバイスに応じて適用されます。たとえば、医療従事者が救急治療室のデバイスからログオフし、X線検査室のワークステーションにログオンする場

合、X線検査室でのセッションに適したポリシー、プリンターマッピング、およびクライアントドライブマッピングがセッション開始時に有効になります。

ユーザーが場所を変更したときに表示されるプリンターをカスタマイズできます。また、ユーザーがローカルプリンターに印刷できるかどうか、ユーザーがリモートで接続したときに消費される帯域幅の量、およびその他の印刷エクスペリエンスの側面を制御することもできます。

ユーザー向けにワークスペースコントロールを有効化および構成する方法については、StoreFrontのドキュメントを参照してください。

セッションローミング

> **注:**
>
> 以下の情報は、PowerShellを使用してセッションローミングを構成する方法を説明しています。代わりにWeb Studioを使用することもできます。詳細については、「デリバリーグループの管理」を参照してください。

> デフォルトでは、セッションはユーザーとともにクライアントデバイス間をローミングします。ユーザーがセッションを起動し、別のデバイスに移動すると、同じセッションが使用され、両方のデバイスでアプリケーションが利用可能になります。アプリケーションは、デバイスや現在のセッションの有無にかかわらず追従します。多くの場合、アプリケーションに割り当てられたプリンターやその他のリソースも追従します。

このデフォルトの動作には多くの利点がありますが、すべての場合に理想的とは限りません。PowerShell SDKを使用してセッションローミングを防止できます。

例1：医療従事者が2台のデバイスを使用しており、デスクトップPCで保険フォームを完成させ、タブレットで患者情報を閲覧しています。

- セッションローミングが有効になっている場合、両方のアプリケーションが両方のデバイスに表示されます（1つのデバイスで起動されたアプリケーションは、使用中のすべてのデバイスで表示されます）。これはセキュリティ要件を満たさない可能性があります。
- セッションローミングが無効になっている場合、患者記録はデスクトップPCに表示されず、保険フォームはタブレットに表示されません。

例2：生産マネージャーがオフィスにあるPCでアプリケーションを起動します。デバイス名と場所によって、そのセッションで利用できるプリンターやその他のリソースが決まります。その日の後半、彼はプリンターの使用が必要となる会議のため、隣の建物のオフィスへ行きます。

- セッションローミングが有効になっている場合、生産管理者は会議室近くのプリンターにアクセスできない可能性があります。なぜなら、彼がオフィスで以前に起動したアプリケーションによって、その場所近くのプリンターやその他のリソースが割り当てられたためです。
- セッションローミングが無効になっている場合、彼が別のマシンに（同じ資格情報を使用して）ログオンすると、新しいセッションが開始され、近くのプリンターやリソースが利用可能になります。

セッションローミングの構成

セッションローミングを構成するには、「SessionReconnection」プロパティを持つ以下のエンタイトルメントポリシー規則コマンドレットを使用します。オプションで、「LeasingBehavior」プロパティも指定できます。

デスクトップセッションの場合：

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

アプリケーションセッションの場合：

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

`value` には、次のいずれかを指定できます。

- **Always:** クライアントデバイスやセッションが接続されているか切断されているかに関係なく、セッションは常にローミングします。これがデフォルト値です。
- **DisconnectedOnly:** 既に切断されているセッションにのみ再接続します。それ以外の場合は、新しいセッションを起動します。（セッションは、まず切断するか、Workspace Control を使用して明示的にローミングすることで、クライアントデバイス間をローミングできます。）別のクライアントデバイスからのアクティブな接続済みセッションは決して使用されません。代わりに、新しいセッションが起動されます。
- **SameEndpointOnly:** ユーザーは使用するクライアントデバイスごとに一意のセッションを取得します。これにより、ローミングが完全に無効になります。ユーザーは、以前セッションで使用したのと同じデバイスにのみ再接続できます。

「LeasingBehavior」プロパティについては、以下で説明します。

他の設定からの影響:

セッションローミングを無効にすると、デリバリーグループのアプリケーションのプロパティにあるアプリケーション制限 **ユーザーごとにアプリケーションのインスタンスを1つのみ許可する** の影響を受けます。

- セッションローミングを無効にする場合は、「インスタンスを1つのみ許可...」アプリケーション制限も無効にしてください。
- 「インスタンスを1つのみ許可...」アプリケーション制限を有効にする場合は、新しいデバイスでの新しいセッションを許可する2つの値のいずれも構成しないでください。

ログオン間隔

デスクトップVDAを含む仮想マシンがログオンプロセス完了前に閉じられた場合、そのプロセスにより多くの時間を割り当てることができます。7.6以降のバージョンのデフォルトは180秒です（7.0〜7.5のデフォルトは90秒です）。

マシン上（またはマシンカタログで使用されるマスターイメージ上）で、次のレジストリキーを設定します。

キー: `HKLM\SOFTWARE\Citrix\PortICA`

- 値: `AutoLogonTimeout`
- 種類: `DWORD`
- 10進数で時間を秒単位で指定します。範囲は0〜3600です。

マスターイメージを変更した場合は、カタログを更新してください。

この設定は、デスクトップVDAを搭載したVMにのみ適用されます。サーバーVDAを搭載したマシンでのログオンタイムアウトは、Microsoftが制御します。

設定

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

> Web Studioを使用して、以下の設定を管理できます。

- 認証の管理
- Citrixカスタマーエクスペリエンス向上プログラム
- デリバリーコントローラーの削除
- ログデータベースの変更
- 日付と時刻の設定
- サイト管理の一元化
- リモートPCアクセスでの複数ユーザーの自動割り当てを有効にする
- DNS解決を有効にする
- XML信頼を有効にする
- セキュリティキーの管理
- Studioコンソールの非アクティブタイムアウトを設定する

認証の管理

デフォルトでは、ユーザーはドメインのユーザー名とパスワードを使用してWeb Studioにログオンします。スマートカード認証や統合Windows認証など、ユーザーに対して別の認証方法を選択することもできます。

ユーザーの認証方法を選択するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで設定を選択します。
2. 「認証」タイルを見つけて「編集」をクリックし、オプションを選択します。

    - ドメイン資格情報
    - ドメイン資格情報または統合 Windows 認証

      統合 Windows 認証が有効になっている場合、ユーザーは Windows 資格情報 (Kerberos/NTLM) またはクライアント証明書を使用して Web Studio にアクセスできます。

      Web Studio と Delivery Controller™ が異なるマシンにインストールされている場合、統合 Windows 認証を機能させるには、クロスオリジンアクセスを許可し、Web Studio サーバーの URL を許可リストに追加します。

      > **重要**

> Web Studio が Delivery Controller のプロキシとして構成されている場合、統合 Windows 認証は機能しません。

- スマートカード認証。
- ドメイン資格情報またはスマートカード認証

  スマートカード認証を有効にするには、追加の構成が必要です。詳細については、「Web Studioのスマートカード認証を設定する」を参照してください。

統合 Windows 認証オプションを有効にすると、次回ユーザーがログオンするときに、自動的にサインインされます。ユーザーとして自動的にサインインできない場合は、統合 Windows 認証を許可するようにWebブラウザーを構成するには、次の手順に従ってください。

Google Chromeの場合：

1. コントロールパネルから、「インターネットオプション」を選択します。
2. 「**詳細設定**」タブを選択します。
3. 「**統合 Windows 認証を有効にする**」を選択します。
4. 「**セキュリティ**」タブを選択します。
5. 「**ローカルイントラネット > サイト > 詳細設定**」を選択します。
6. 「**このWebサイトをゾーンに追加する**」ボックスで：
   - Web StudioとDelivery Controllerが同じサーバー上にある場合は、Web Studioを実行しているホストのURLを入力します。
   - そうでない場合は、ワイルドカードドメインを入力します。例：Delivery Controllerが `ddc.domain.com` にある場合、`*.domain.com` と入力します。
7. 「**追加 > 閉じる**」をクリックします。

Mozilla Firefoxの場合：

1. ブラウザから、URLボックスに `about:config` と入力します。
2. 「**検索**」ボックスに `network negotiate` と入力します。
3. **network.negotiate-auth.trusted-uris**を右クリックし、「**変更**」を選択します。
4. 「**文字列値を入力**」ボックスで：

- Web Studio と Delivery Controller が同じサーバー上にある場合は、Web Studio をホストしているサーバー名を参照する URL および/またはエイリアスのコンマ区切りリストを追加します。
- そうでない場合は、次のように URL を追加します。例: Delivery Controller が `ddc.domain.com` にある場合、「`*.domain.com`」と入力します。

ブラウザを設定した後、サインインページで**Windows統合サインイン**をクリックして再試行できます。

Web Studio と Delivery Controller が異なるマシンにインストールされている場合、統合 Windows 認証を機能させるには、「**クロスオリジンアクセスを許可**」を有効にする必要があります。

「**クロスオリジンアクセスを許可**」を有効にするには、次の手順に従います。

1. **クロスオリジンアクセスを許可**チェックボックスをオンにします。
2. Web StudioサーバーのURLを許可リストに追加します。
3. **URLを入力**フィールドにURLを入力します。必要に応じて、**追加**をクリックしてさらに追加します。

> **注**
>
> - URL は正しい形式 `<scheme>://<hostname>` に従う必要があります。パスや末尾のスラッシュを含まないようにしてください。
> - IP アドレスと FQDN がサポートされています。URL を追加するときは、Web Studio へのアクセス方法と一致していることを確認してください。たとえば、IP アドレスを使用して Web Studio にアクセスする場合は、IP アドレスベースの URL をリストに追加します。
> - デフォルト以外のポートを使用する場合は、ポート番号を含めるようにしてください。

4. 必要に応じて、「**追加**」をクリックしてさらに追加します。
5. 完了したら、「**完了**」をクリックして保存し、終了します。

タイムゾーンを設定する

日付と時刻の形式を好みに合わせてカスタマイズするには、次の手順に従います。

1. Web Studio にサインインし、左ペインで「**設定**」を選択します。
2. 「**日付と時刻**」タイルを見つけて「**編集**」をクリックし、次のオプションを設定します。
   - **時刻形式:**
     - 12時間形式（例: 午後09:00）または24時間形式（例: 21:00）で時刻を表示するように選択します。
   - **日付形式:**
     - yyyy/MM/dd のように、好みに合わせて日付形式を設定します。
   - **タイムゾーン:**
     - **UTC:** ユーザーインターフェイス全体で日付と時刻をUTCで表示します。日付と時刻にマウスを合わせると、その情報がローカルタイムゾーンで表示されます。
     - **ローカルタイムゾーン:** ユーザーインターフェイス全体で日付と時刻をローカルタイムゾーンで表示します。日付と時刻にマウスを合わせると、その情報がUTCで表示されます。

> **注:**
>
> これらの設定は、各ユーザーアカウントに固有のものです。

DNS解決を有効にする

ICA®ファイルでIPアドレスの代わりにDNS名を表示するには、次の手順に従います。

1. Web Studioにサインインし、左側のペインで**設定**を選択します。
2. **DNS解決を有効にする**設定をオンにします。

Studioコンソールの非アクティビティタイムアウトを設定する

管理者がStudioコンソールから自動的にサインアウトされるまでの非アクティビティ期間を設定できます。

1. Web Studioにサインインし、左側のペインで「**設定**」を選択します。
2. 10分から24時間の範囲で期間を入力します。
3. この設定を適用するには、ページを更新するか、サインアウトしてから再度サインインします。

サイト管理を一元化する

この機能を使用すると、1つのWeb Studioコンソールで複数のCitrix Virtual Apps and Desktopsサイトを管理できます。詳細については、「複数のサイト管理を有効にする」を参照してください。

タグ

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

はじめに

タグは、マシン、アプリケーション、デスクトップ、デリバリーグループ、アプリケーショングループ、ポリシーなどの項目を識別する文字列です。タグを作成して項目に追加すると、特定のタグを持つ項目にのみ適用されるように特定の操作を調整できます。

- Web Studioでの検索表示を調整します。

  たとえば、テスター向けに最適化されたアプリケーションのみを表示するには、「test」という名前のタグを作成し、それらのアプリケーションに追加（適用）します。これで、Web Studioの検索を「test」タグでフィルタリングできます。
- アプリケーショングループからアプリケーションを公開したり、デリバリーグループから特定のデスクトップを公開したりする際に、選択したデリバリーグループ内のマシンの一部のみを考慮します。これは*タグ制限*と呼ばれます。

  タグ制限を使用すると、既存のマシンを複数の公開タスクに使用できるため、より多くのマシンを展開および管理するコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）するものと考えることができます。その機能は、XenApp 7.xより前のリリースにおけるワーカーグループと似ていますが、同一ではありません。

  タグ制限付きのアプリケーショングループまたはデスクトップを使用すると、デリバリーグループ内のマシンの一部を分離してトラブルシューティングする際に役立ちます。
- デリバリーグループ内のマシンの一部に対して定期的な再起動をスケジュールします。

マシンにタグ制限を使用すると、新しいPowerShellコマンドレットを使用して、デリバリーグループ内のマシンの一部に対して複数の再起動スケジュールを構成できます。例と詳細については、「デリバリーグループの管理」を参照してください。

- 指定されたタグを持つ（または持たない）デリバリーグループ、デリバリーグループの種類、またはOU内のマシンの一部にCitrixポリシーの適用（割り当て）を調整します。

  たとえば、より強力なワークステーションにのみCitrixポリシーを適用したい場合は、それらのマシンに「high power」という名前のタグを追加します。次に、ポリシー作成ウィザードの**ポリシーの割り当て**ページで、そのタグと**有効にする**チェックボックスを選択します。デリバリーグループにタグを追加し、そのグループにCitrixポリシーを適用することもできます。詳細については、「ポリシーの作成」を参照してください。

タグを適用できる項目:

- マシン
- アプリケーション
- マシンカタログ (PowerShell のみ。(#tags-on-machine-catalogs)を参照)
- デリバリーグループ
- アプリケーショングループ

Web Studio で以下を作成または編集する際に、タグ制限を構成できます。

- 共有デリバリーグループ内のデスクトップ
- アプリケーショングループ

> **重要:**
>
> タグは、マシンに明示的に適用することも、マシンカタログまたはデリバリーグループレベルで明示的に適用することもできます。タグがマシンカタログまたはデリバリーグループレベルで適用されると、そのカタログまたはデリバリーグループ内のすべてのマシンが暗黙的にタグを継承します。これらの継承されたタグは、マシンレベルで削除できません。タグの効果を削除するには、マシンカタログまたはデリバリーグループレベルからタグを削除する必要があります。

デスクトップまたはアプリケーショングループのタグ制限

タグ制限にはいくつかの手順があります。

- タグを作成し、マシンに追加（適用）します。
- タグ制限付きのグループを作成または編集します（つまり、「タグ x のあるマシンへの起動を制限する」）。

タグ制限は、ブローカーのマシン選択プロセスを拡張します。ブローカーは、アクセスポリシー、構成されたユーザーリスト、ゾーン設定、起動準備状況、およびタグ制限（存在する場合）に従って、関連付けられたデリバリーグループからマシンを選択します。アプリケーションの場合、ブローカーは優先順位に従って他のデリバリーグループにフォールバックし、検討対象の各デリバリーグループに同じマシン選択ルールを適用します。

例 1: シンプルなレイアウト

この例では、タグ制限を使用して、特定のデスクトップおよびアプリケーションの起動に考慮されるマシンを制限するシンプルなレイアウトを紹介します。サイトには、共有デリバリーグループが1つ、公開デスクトップが1つ、2つのアプリケーションで構成されたアプリケーショングループが1つあります。

シンプルなレイアウトでタグ制限を使用する例。(/en-us/citrix-virtual-apps-desktops/2407/media/tags-example.png)

- 3台のマシン（VDA 101～103）のそれぞれにタグが追加されています。
- 共有デリバリーグループ内のデスクトップは、「Red」という名前のタグ制限で作成されました。デスクトップは、そのデリバリーグループ内で「Red」タグを持つマシン（VDA 101および102）でのみ起動できます。
- アプリケーショングループは「Orange」タグ制限で作成されたため、その各アプリケーション（CalculatorとNotepad）は、そのデリバリーグループ内で「Orange」タグを持つマシン（VDA 102および103）でのみ起動できます。

マシンVDA 102は両方のタグ（RedとOrange）を持っているため、アプリケーションとデスクトップの起動に考慮されます。

例 2: より複雑なレイアウト

この例には、タグ制限付きで作成された複数のアプリケーショングループが含まれています。これにより、デリバリーグループのみを使用した場合に必要となるよりも少ないマシンで、より多くのアプリケーションを配信できるようになります。

例 2 の構成方法 は、この例でタグを作成および適用し、タグ制限を構成するために使用される手順を示しています。

複雑なレイアウトでタグ制限を使用する例。(/en-us/citrix-virtual-apps-desktops/2407/media/tags-example2.png)

この例では、10台のマシン（VDA 101～110）、1つのデリバリーグループ（D01）、および3つのアプリケーショングループ（A100、A200、A300）を使用します。各マシンにタグを適用し、各アプリケーショングループの作成時にタグ制限を指定することで、次のことが可能になります。

- グループ内の経理ユーザーは、5台のマシン（VDA 101～105）で必要なアプリにアクセスできます。
- グループ内のCADデザイナーは、5台のマシン（VDA 106～110）で必要なアプリにアクセスできます。
- グループ内でOfficeアプリケーションを必要とするユーザーは、10台のマシン（VDA 101～110）でOfficeアプリにアクセスできます。

使用されるマシンは10台のみで、デリバリーグループは1つだけです。デリバリーグループのみを使用する場合（アプリケーショングループなし）は、マシンが1つのデリバリーグループにしか属せないため、2倍の数のマシンが必要になります。

タグとタグ制限の管理

タグは、Web Studioの**［タグの管理］**アクションを通じて、選択したアイテムに対して作成、追加（適用）、編集、削除されます。

（例外：ポリシー割り当てに使用されるタグは、Web Studioの**タグの管理**アクションを通じて作成、編集、削除されます。ただし、タグはポリシー作成時に適用（割り当て）されます。詳細については、「ポリシーの作成」を参照してください。）

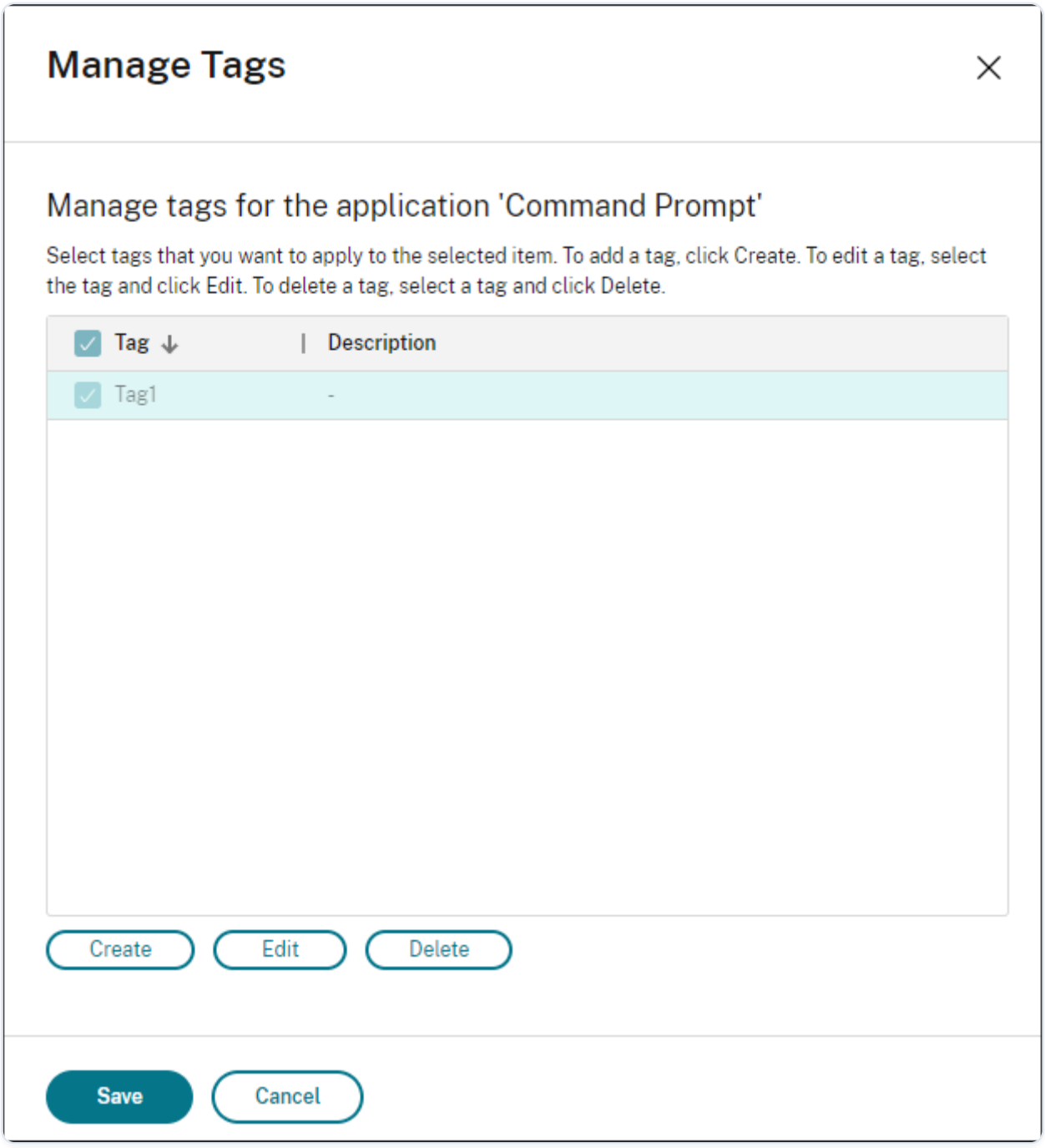
タグ制限は、デリバリーグループでデスクトップを作成または編集するとき、およびアプリケーショングループを作成および編集するときに構成されます。

Web Studioで「タグの管理」ダイアログを使用する

Web Studioで、タグを適用するアイテム（1つまたは複数のマシン、アプリケーション、デスクトップ、デリバリーグループ、またはアプリケーショングループ）を選択し、アクションバーで**［タグの管理］**を選択します。ダイアログボックスには、選択したアイテムだけでなく、サイトで作成されたすべてのタグが一覧表示されます。

- チェックマークが付いたチェックボックスは、そのタグが選択した項目にすでに追加されていることを示します。（以下のスクリーンショットでは、選択したマシンに「Tag1」という名前のタグが適用されています。）

- 複数の項目を選択した場合、ハイフンを含むチェックボックスは、選択した項目の一部にのみそのタグが追加されていることを示します。



タグの管理ダイアログボックスから、次のアクションを実行できます。「タグを使用する際の注意点」を必ず確認してください。

- **タグを作成するには:**

  作成をクリックします。名前と説明を入力します。タグ名は一意である必要があり、大文字と小文字は区別されません。次に、**OK**をクリックします。（タグを作成しても、選択した項目に自動的に適用されるわけではありません。チェックボックスを使用してタグを適用します。）

- **1つ以上のタグを追加（適用）するには:**

  タグ名の横にあるチェックボックスを有効にします。複数の項目を選択し、タグの横にあるチェックボックスにハイフンが含まれている場合（選択した項目の一部にのみタグがすでに適用されていることを示す）、それをチェックマークに変更すると、選択したすべてのマシンに影響します。

  1つ以上のマシンにタグを追加しようとして、そのタグがアプリケーショングループで制限として使用されている場合、その操作によってそれらのマシンが起動可能になる可能性があるという警告が表示されます。それが意図したものであれば、続行してください。

- **1つ以上のタグを削除するには:**

  タグ名の横にあるチェックボックスをオフにします。複数の項目を選択していて、タグの横にあるチェックボックスにハイフンが含まれている場合（選択した項目の一部にのみタグが適用されていることを示す）、チェックボックスをオフにすると、選択したすべてのマシンからタグが削除されます。

  タグを制限として使用しているマシンからタグを削除しようとすると、その操作が起動対象となるマシンに影響を与える可能性があるという警告が表示されます。それが意図したものであれば、続行してください。

- **タグを編集するには:**

  タグを選択し、**編集**をクリックします。新しい名前、説明、またはその両方を入力します。一度に編集できるタグは1つだけです。

- **1つ以上のタグを削除するには:**

  タグを選択し、**削除**をクリックします。「タグの削除」ダイアログボックスには、現在選択されているタグを使用している項目の数（例：「2台のマシン」）が表示されます。項目をクリックすると、詳細情報が表示されます。たとえば、「2台のマシン」項目をクリックすると、そのタグが適用されている2台のマシンの名前が表示されます。タグを削除するかどうかを確認します。

  Web Studioを使用して、制限として使用されているタグを削除することはできません。まず、アプリケーショングループを編集してタグ制限を削除するか、別のタグを選択してください。

タグの管理ダイアログボックスでの作業が完了したら、**保存**をクリックします。

マシンにタグが適用されているかどうかを確認するには：左ペインで**デリバリーグループ**を選択します。中央ペインでデリバリーグループを選択し、アクションバーで**マシンの表示**を選択します。中央ペインでマシンを選択し、**詳細**ペインで**タグ**タブを選択します。

タグ制限を管理する

タグ制限の構成は複数の手順からなるプロセスです。まずタグを作成し、それをマシンに追加/適用します。次に、アプリケーショングループまたはデスクトップに制限を追加します。

- **タグを作成して適用する：**

  タグを作成し、前述の**タグの管理**アクションを使用して、タグ制限の影響を受けるマシンにそのタグを追加（適用）します。

- **アプリケーション グループにタグ制限を追加するには:**

  アプリケーション グループを作成または編集します。**Delivery Groups** ページで、**タグを持つマシンへの起動を制限**を選択し、リストからタグを選択します。

- **アプリケーション グループのタグ制限を変更または削除するには:**

  グループを編集します。**Delivery Groups** ページで、リストから別のタグを選択するか、**タグを持つマシンへの起動を制限**のチェックを外してタグ制限を完全に削除します。

- **デスクトップにタグ制限を追加するには:**

  デリバリー グループを作成または編集します。**Desktops** ページで、**追加**または**編集**をクリックします。「デスクトップの追加」ダイアログ ボックスで、**タグを持つマシンへの起動を制限**を選択し、メニューからタグを選択します。

- **デリバリー グループのタグ制限を変更または削除するには:**

  グループを編集します。Desktops ページで、**編集**をクリックします。ダイアログ ボックスで、リストから別のタグを選択するか、**タグを持つマシンへの起動を制限**のチェックを外してタグ制限を完全に削除します。

タグを使用する際の注意点

アイテムに適用されたタグはさまざまな目的に使用できるため、タグの追加、削除、および削除が意図しない影響を与える可能性があることに留意してください。Web Studio の検索フィールドでマシンの表示を並べ替えるためにタグを使用できます。アプリケーション グループまたはデスクトップを構成する際に、同じタグを制限として使用できます。タグは、指定されたデリバリー グループ内でそのタグを持つマシンのみに起動の考慮事項を制限します。

デスクトップまたはアプリケーション グループのタグ制限としてタグが構成された後で、マシンにそのタグを追加しようとすると、警告が表示されます。そのタグを追加すると、マシンが追加のアプリケーションまたはデスクトップの起動に利用可能になる可能性があります。それが意図したものであれば、続行してください。そうでない場合は、操作をキャンセルできます。

たとえば、「Red」タグ制限を持つアプリケーション グループを作成したとします。その後、そのアプリケーション グループで使用されているのと同じデリバリー グループに他のマシンをいくつか追加します。そのマシンに「Red」タグを追加しようとすると、Web Studio に次のようなメッセージが表示されます。「タグ「Red」は、以下のアプリケーション グループの制限として使用されています。このタグを追加すると、選択したマシンがこのアプリケーション グループ内のアプリケーションを起動できるようになる可能性があります。」その後、それらの追加のマシンにそのタグを追加することを確認またはキャンセルできます。

同様に、アプリケーション グループが起動を制限するためにタグを使用している場合、Web Studio は、グループを編集して制限として削除するまでタグを削除できないことを警告します。（アプリケーション グループで制限として使用されているタグを削除することが許可された場合、そのアプリケーション グループに関連付けられているデリバリー グループ内のすべてのマシンでアプリケーションの起動が許可される可能性があります。）デスクトップの起動の制限としてタグが使用されている場合も、タグの削除に対する同じ禁止が適用されます。そのタグ制限を削除するためにアプリケーション グループまたはデリバリー グループ内のデスクトップを編集した後、タグを削除できます。

すべてのマシンが同じアプリケーション セットを持っているとは限りません。ユーザーは複数のアプリケーション グループに属することができ、それぞれが異なるタグ制限と、デリバリー グループからの異なるまたは重複するマシン セットを持っています。次の表は、マシンの考慮事項がどのように決定されるかを示しています。

アプリケーションが追加された場合	選択されたデリバリーグループ内のこれらのマシンが起動対象と見なされます
タグ制限のない1つのアプリケーショングループ	任意のマシン。
タグ制限Aのある1つのアプリケーショングループ	タグAが適用されているマシン。
2つのアプリケーショングループ（1つはタグ制限A、もう1つはタグ制限B）	タグAとタグBを持つマシン。利用可能なマシンがない場合は、タグAまたはタグBを持つマシン。
2つのアプリケーショングループ（1つはタグ制限A、もう1つはタグ制限なし）	タグAを持つマシン。利用可能なマシンがない場合は、任意のマシン。

マシン再起動スケジュールでタグ制限を使用した場合、タグの適用または制限に影響を与える変更は、次のマシン再起動サイクルに影響します。変更が行われている間に進行中の再起動サイクルには影響しません。

例2の構成方法

以下の手順では、タグを作成して適用し、2番目の例で示されているアプリケーショングループのタグ制限を構成する手順を示します。

VDAとアプリケーションはすでにマシンにインストールされており、デリバリーグループも作成されています。

マシンにタグを作成して適用します。

1. Web Studioで、デリバリーグループD01を選択し、アクションバーで**マシンを表示**を選択します。
2. マシンVDA 101～105を選択し、アクションバーで**タグの管理**を選択します。
3. タグの管理ダイアログボックスで、**作成**をクリックし、`CADApps`という名前のタグを作成します。**OK**をクリックします。
4. もう一度**作成**をクリックし、OfficeAppsという名前のタグを作成します。**OK**をクリックします。
5. **タグの管理**ダイアログボックスにいる間に、新しく作成したタグを、各タグの名前（`CADApps`と`OfficeApps`）の横にあるチェックボックスを有効にすることで、選択したマシンに追加（適用）します。完了したら、ダイアログボックスを閉じます。
6. デリバリーグループD01を選択し、アクションバーで**マシンを表示**を選択します。
7. マシンVDA 106～110を選択し、アクションバーで**タグの管理**を選択します。
8. **タグの管理**ダイアログボックスで、**作成**をクリックします。`AcctgApps`という名前のタグを作成します。**OK**をクリックします。
9. 新しく作成した`AcctgApps`タグと`OfficeApps`タグを、各タグ名の横にあるチェックボックスをクリックして、選択したマシンに適用し、ダイアログボックスを閉じます。

タグ制限付きのアプリケーショングループを作成します。

1. Web Studioで、左側のペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択し、アクションバーで**アプリケーショングループの作成**を選択します。アプリケーショングループの作成ウィザードが起動します。
2. ウィザードの**デリバリーグループ**ページで、デリバリーグループD01を選択します。**タグを持つマシンへの起動を制限する**を選択し、リストから`AcctgApps`タグを選択します。
3. 会計ユーザーと会計アプリケーションを指定して、ウィザードを完了します。（アプリケーションを追加するときは、`AcctgApps`タグを持つマシンでアプリケーションを検索する**ス**

タートメニューからソースを選択します。）**概要**ページで、グループに`A100`という名前を付けます。

4. 前述の手順を繰り返して、アプリケーショングループ`A200`を作成し、`CADApps`タグを持つマシン、および適切なユーザーとアプリケーションを指定します。
5. 手順を繰り返して、アプリケーショングループ`A300`を作成し、`OfficeApps`タグを持つマシン、および適切なユーザーとアプリケーションを指定します。

マシンカタログのタグ

マシンカタログでタグを使用できます。タグを作成してカタログに適用する全体的な手順は、前述のとおりです。ただし、カタログへのタグの適用はPowerShellインターフェイスを介してのみサポートされています。Web Studioを使用してカタログにタグを適用したり、カタログからタグを削除したりすることはできません。Web Studioのカタログ表示では、タグが適用されているかどうかは示されません。

概要：Web StudioまたはPowerShellを使用して、カタログで使用するタグを作成または削除できます。PowerShellを使用して、タグをカタログに適用します。

カタログでタグを使用する例をいくつか示します。

- デリバリーグループには複数のカタログのマシンが含まれていますが、特定のカタログのマシンのみに操作（再起動スケジュールなど）を適用したい場合。そのカタログにタグを適用することで、これが実現します。
- アプリケーショングループで、アプリケーションセッションを特定のカタログのマシンに制限したい場合。そのカタログにタグを適用することで、これが実現します。

影響を受けるPowerShellコマンドレット:

- `Add-BrokerTag`や`Remove-BrokerTag`などのコマンドレットにカタログオブジェクトを渡すことができます。
- `Get-BrokerTagUsage`は、タグを含むカタログの数を示します。
- `Get-BrokerCatalog`には、`Tags`という名前のプロパティがあります。

たとえば、次のコマンドレットは、`acctg`という名前のカタログに`fy2018`という名前のタグを追加します。`Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`。（タグは以前にWeb StudioまたはPowerShellのいずれかを使用して作成されています。）

詳細なガイダンスと構文については、PowerShellコマンドレットのヘルプを参照してください。

自動タグ（プレビュー）

自動タグ付けにより、管理者はカスタムルールに基づいて、さまざまなCitrix Virtual Apps and Desktopsオブジェクトにタグを自動的に設定および削除できます。この機能強化により、環境最適化のために定期的に実行されるさまざまなスクリプトを維持する必要がなくなります。

ユースケース

自動タグ付けを使用すると、コスト削減、インフラストラクチャの最適化、消費の促進など、ビジネスドライバーに関連するルールを実装できます。以下にいくつかのユースケースを示します。

- **未使用のVDIを再利用** - 事前設定された日数以上使用されていない専用ワークロードを、利用可能なプールに解放するため。
- **アプリケーションの乱雑さを解消** - 事前設定された日数以上使用されていないアプリケーションを特定することで、アプリケーションの乱雑さを軽減するため。
- **X未満の機能レベルを持つDG** - 特定の機能レベル未満のデリバリーグループを見つけるため。
- **非アクティブユーザー** - 事前設定された日数以上ログオンしていないユーザーのリソースを再利用するため。

PowerShellコマンド

PowerShellコマンドを使用してオートタグを作成できます。オートタグルールが作成されると、600秒の頻度で評価されます。詳細については、New-BrokerAutoTagRuleを参照してください。

例

`New-BrokerAutoTagRule`は、`Get-BrokerMachine`コマンドレットと同じオブジェクトタイプとフィルターパラメーターを使用します。詳細については、GetBrokerMachineを参照してください。

1. 30日以上使用されていない専用VDIにID 123でタグ付けします。
    a. 未使用のVDIにタグ付けするためのタグを定義します。例えば、**unused-VDI**です。
        - タグ名 : unused-VDI
        - タグID : 123
    b. 未使用のマシンにタグ付けするための自動タグ付けルールを作成します。ルールパラメーターを定義します。
        - 名前 : ルールの一般的な名前。
        - オブジェクトタイプ : マシン。

- Rule text : 最終接続時間が30日を超えるか、値がない静的で割り当てられたマシン。
- Tag Uid : 関連付けたいタグID、123。

```
New-BrokerAutoTagRule -Name ‘UnusedVdi’ -ObjectType ‘Machine’ -RuleText “-AllocationType Static -IsAssigned $true -Filter { SummaryState -ne `”InUse`” -and ( LastConnectionTime -lt ‘-30’ -or LastConnectionTime -eq `$null ) }” -TagUid 123
```

c. **unused-VDI**タグが付けられたマシンを確認し、解放します。

2. 機能レベルがX未満のデリバリーグループにタグを付けるには (**L7_20**を閾値機能レベルとして使用):

```
New-BrokerAutoTagRule -Name 'LowFL' -ObjectType 'DesktopGroup' -RuleText "-Filter { MinimumFunctionalLevel -lt 'L7_20' } " -TagUid 123
```

1. フォルダーなしで公開されたユーザーに表示されるアプリにタグを付けるには:

```
New-BrokerAutoTagRule -Name 'NoFolder' -ObjectType 'Application' -RuleText "-Enabled $true -Filter { ClientFolder -eq $null )} " -TagUid 123
```

詳細情報

ブログ投稿: デスクトップを特定のサーバーに割り当てる方法。

ユーザープロファイル

デフォルトでは、Virtual Delivery Agent のインストール時に Citrix Profile Management がマスターイメージにサイレントインストールされますが、プロファイルソリューションとして Profile Management を使用する必要はありません。

ユーザーのさまざまなニーズに合わせて、Citrix Virtual Apps and Desktops™ ポリシーを使用して、各 Delivery Group のマシンに異なるプロファイル動作を適用できます。たとえば、ある Delivery Group では、テンプレートが1つのネットワークロケーションに保存されている Citrix 強制プロファイルが必要な場合があり、別の Delivery Group では、複数のリダイレクトされたフォルダーとともに別のロケーションに保存されている Citrix ローミングプロファイルが必要な場合があります。

- 組織内の他の管理者が Citrix Virtual Apps and Desktops ポリシーを担当している場合は、彼らと協力して、Delivery Group 全体でプロファイル関連のポリシーが設定されていることを確認してください。

- Profile Management ポリシーは、グループポリシー、Profile Management .ini ファイル、および個々の仮想マシン上でローカルに設定することもできます。プロファイル動作を定義するこれらの複数の方法は、次の順序で読み取られます。

  a. グループポリシー (.adm または .admx ファイル)

  b. ポリシーノード内の Citrix Virtual Apps and Desktops ポリシー

  c. ユーザーが接続する仮想マシン上のローカルポリシー

  d. Profile Management .ini ファイル

  たとえば、グループポリシーとポリシーノードの両方で同じポリシーを構成した場合、システムはグループポリシーのポリシー設定を読み取り、Citrix Virtual Apps and Desktops ポリシー設定を無視します。

どのプロファイルソリューションを選択しても、Director 管理者は診断情報にアクセスし、ユーザープロファイルのトラブルシューティングを行うことができます。詳細については、Director ドキュメントを参照してください。

自動構成

デスクトップの種類は、Virtual Delivery Agent のインストールに基づいて自動的に検出され、Studio で行う構成の選択に加えて、それに応じて Profile Management のデフォルトが設定されます。

Profile Management が調整するポリシーを次の表に示します。デフォルト以外のポリシー設定は保持され、この機能によって上書きされることはありません。各ポリシーの詳細については、Profile Management のドキュメントを参照してください。プロファイルを作成するマシンの種類は、調整されるポリシーに影響します。主な要因は、マシンが永続的かプロビジョニング済みか、および複数のユーザーで共有されるか、1人のユーザー専用であるかです。

永続システムには何らかのローカルストレージがあり、その内容はシステムがシャットダウンしても保持されることが期待されます。永続システムは、SAN などのストレージテクノロジーを使用してローカルディスクを模倣する場合があります。対照的に、プロビジョニング済みシステムは、ベースディスクと何らかのIDディスクから「オンザフライ」で作成されます。ローカルストレージは通常、RAM ディスクまたはネットワークディスクによって模倣され、後者は高速リンクを備えた SAN によって提供されることがよくあります。プロビジョニングテクノロジーは通常、Citrix Provisioning または Machine Creation Services™ (またはサードパーティの同等品) です。プロビジョニング済みシステムが永続的なローカルストレージを持つ場合もあります。これらは永続的として分類されます。

これら2つの要素を合わせると、以下のマシンタイプが定義されます。

- **永続的かつ専用**。例としては、Machine Creation Servicesで作成された静的割り当てと永続的なローカルストレージを持つシングルセッションOSマシン、物理ワークステーション、ラップトップなどがあります。
- **永続的かつ共有**。例としては、Machine Creation Servicesで作成されたマルチセッションOSマシン、およびCitrix Virtual Appsサーバーなどがあります。
- **プロビジョニング済みかつ専用**。例としては、Citrix Provisioning Service (Citrix Virtual Desktops™内) で作成された、静的割り当てを持つが永続ストレージを持たないシングルセッションOSマシンなどがあります。
- **プロビジョニング済みかつ共有**。例としては、Citrix Provisioning™ Service (Citrix Virtual Desktops内) で作成されたランダム割り当てを持つシングルセッションOSマシン、およびCitrix Virtual Appsサーバーなどがあります。

以下のプロファイル管理ポリシー設定は、異なるマシンタイプに対する推奨ガイドラインです。これらはほとんどの場合でうまく機能しますが、展開の要件に応じてこれらから逸脱することもできます。

> **重要:**
>
> **ログオフ時にローカルにキャッシュされたプロファイルを削除**、**プロファイルストリーミング**、および**常にキャッシュ**は、自動構成機能によって適用されます。その他のポリシーは手動で調整してください。

永続マシン

ポリシー	永続的かつ専用	永続的かつ共有
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効	有効
プロファイルストリーミング	無効	有効
常にキャッシュ	有効 (注1)	無効 (注2)
アクティブライトバック	無効	無効 (注3)
ローカル管理者によるログオンの処理	有効	無効 (注4)

プロビジョニング済みマシン

ポリシー	プロビジョニング済みと専用の両方	プロビジョニング済みと共有の両方
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効 (注5)	有効
プロファイルストリーミング	有効	有効
常にキャッシュ	無効 (注6)	無効
アクティブライトバック	有効	有効
ローカル管理者のログオンを処理する	有効	有効 (注 7)

1. このマシンタイプでは**プロファイルストリーミング**が無効になっているため、**常にキャッシュ**設定は常に無視されます。
2. **常にキャッシュ**を無効にします。ただし、このポリシーを有効にし、ファイルサイズ制限 (MB単位) を定義することで、ログオン後できるだけ早く大きなファイルがプロファイルにロードされるようにすることができます。このサイズ以上のファイルは、できるだけ早くローカルにキャッシュされます。
3. Citrix Virtual Appsサーバー間を移動するユーザーのプロファイルの変更を保存する場合を除き、**アクティブライトバック**を無効にします。この場合は、このポリシーを有効にします。
4. ホスト型共有デスクトップの場合を除き、**ローカル管理者のログオンを処理**を無効にします。この場合は、このポリシーを有効にします。
5. **ログオフ時にローカルにキャッシュされたプロファイルを削除**を無効にします。この設定は、ローカルにキャッシュされたプロファイルを保持します。マシンはログオフ時にリセットされますが、個々のユーザーに割り当てられているため、プロファイルがキャッシュされている場合はログオンが高速になります。
6. **常にキャッシュ**を無効にします。ただし、このポリシーを有効にし、ファイルサイズ制限 (MB単位) を定義することで、ログオン後できるだけ早く大きなファイルがプロファイルにロードされるようにすることができます。このサイズ以上のファイルは、できるだけ早くローカルにキャッシュされます。

7. Citrix Virtual Apps and Desktopsサーバー間を移動するユーザーのプロファイルの場合を除き、**ローカル管理者のログオンを処理**を有効にします。この場合は、このポリシーを無効にします。

フォルダーリダイレクト

フォルダーリダイレクトを使用すると、プロファイルが保存されている場所とは異なるネットワーク共有にユーザーデータを保存できます。フォルダーリダイレクトはプロファイルサイズとロード時間を削減しますが、ネットワーク帯域幅に影響を与える可能性があります。フォルダーリダイレクトは、Citrixユーザープロファイルが使用されていることを必要としません。ユーザープロファイルを独自に管理し、フォルダーをリダイレクトすることもできます。

StudioのCitrixポリシーを使用してフォルダーリダイレクトを構成します。

- リダイレクトされたフォルダーのコンテンツを保存するために使用されるネットワークの場所が利用可能であり、適切な権限を持っていることを確認してください。場所のプロパティは検証されます。
- リダイレクトされたフォルダーはネットワーク上に設定され、その内容はログオン時にユーザーの仮想デスクトップから取り込まれます。

フォルダーリダイレクトは、CitrixポリシーまたはActive Directoryグループポリシーオブジェクトのいずれか一方のみを使用して構成し、両方は使用しないでください。両方のポリシーエンジンを使用してフォルダーリダイレクトを構成すると、予期しない動作が発生する可能性があります。

高度なフォルダーリダイレクト

複数のオペレーティングシステム (OS) を使用する展開では、ユーザープロファイルの一部を各OSで共有したい場合があります。プロファイルの残りの部分は共有されず、1つのOSでのみ使用されます。OS間で一貫したユーザーエクスペリエンスを確保するには、各OSで異なる構成、つまり高度なフォルダーリダイレクトが必要です。たとえば、2つのOSで実行されているアプリケーションの異なるバージョンが共有ファイルを読み書きする必要がある場合、両方のバージョンがアクセスできる単一のネットワーク場所にリダイレクトすることに決定します。あるいは、**スタートメニュー**フォルダーの内容が2つのOSで異なる構造になっているため、両方ではなく1つのフォルダーのみをリダイレクトすることに決定します。このアプローチにより、各OSで**スタートメニュー**フォルダーとその内容が分離され、ユーザーに一貫したエクスペリエンスが保証されます。

展開で高度なフォルダーリダイレクトが必要な場合は、ユーザーのプロファイルデータの構造を理解し、そのどの部分をOS間で共有できるかを判断する必要があります。フォルダーリダイレクトが正しく使用されないと、予期しない動作が発生する可能性があります。

高度な展開でフォルダーをリダイレクトするには：

- 各OSに個別のデリバリーグループを使用します。
- 仮想デスクトップ上の仮想アプリケーションを含む、仮想アプリケーションがユーザーデータと設定をどこに保存するかを理解し、データの構造を理解します。
- 安全にローミングできる共有プロファイルデータ（各OSで同じ構造になっているため）については、各デリバリーグループ内のコンテナーフォルダーをリダイレクトします。
- ローミングできない非共有プロファイルデータについては、デスクトップグループのいずれか1つ（通常は最も使用されているOSまたはデータが最も関連性の高いOS）のコンテナーフォルダーをリダイレクトします。あるいは、OS間でローミングできない非共有データについては、両方のシステム上のコンテナーフォルダーを別々のネットワーク場所にリダイレクトします。

高度な展開の例

この展開には、Windows 10デスクトップで実行されるMicrosoft OutlookおよびInternet Explorerのバージョンを含むアプリケーションと、Windows Server 2019によって提供されるOutlookおよびInternet Explorerの他のバージョンを含むアプリケーションがあります。2つのOS用に2つのデリバリーグループをすでに設定しています。ユーザーは、両方のアプリケーションのバージョンで同じ**連絡先**と**お気に入り**のセットにアクセスしたいと考えています。

重要: 以下の決定とアドバイスは、説明されているOSと展開に有効です。組織では、リダイレクトするフォルダーとそれらを共有するかどうかの決定は、特定の展開に固有のさまざまな要因によって異なります。

- デリバリーグループに適用されるポリシーを使用して、次のフォルダーをリダイレクトするように選択します。

フォルダ	WINDOWS 10でリダイレクトされますか？	WINDOWS SERVER 2019でリダイレクトされますか？
マイドキュメント	はい	はい
アプリケーションデータ	いいえ	いいえ
連絡先	はい	はい
デスクトップ	はい	いいえ
ダウンロード	いいえ	いいえ
お気に入り	はい	はい

フォルダ	WINDOWS 10でリダイレクトされますか？	WINDOWS SERVER 2019でリダイレクトされますか？
リンク	はい	いいえ
マイミュージック	はい	はい
マイピクチャ	はい	はい
マイビデオ	はい	はい
検索	はい	いいえ
保存されたゲーム	いいえ	いいえ
スタートメニュー	はい	いいえ

- 共有され、リダイレクトされたフォルダーの場合：
  - OutlookとInternet Explorerの異なるバージョンによって保存されたデータの構造を分析した結果、**連絡先**と**お気に入り**フォルダーを共有しても安全であると判断しました。
  - **ドキュメント**、**ミュージック**、**ピクチャ**、**ビデオ**フォルダーの構造はOS間で標準的であることがわかっています。そのため、これらのフォルダーを各デリバリーグループで同じネットワーク場所に保存しても安全です。
- 共有されない、リダイレクトされたフォルダーの場合：
  - Windows Serverデリバリーグループでは、デスクトップ、リンク、検索、または**スタートメニュー**フォルダーをリダイレクトしません。これらのフォルダー内のデータは2つのOSで異なる方法で整理されているためです。したがって、共有することはできません。
  - この共有されないデータの予測可能な動作を保証するため、Windows 10デリバリーグループでのみリダイレクトします。Windows 10は、ユーザーが日常業務でより頻繁に使用します。ユーザーはWindows Serverによって提供されるアプリケーションにたまにしかアクセスしません。また、この場合、共有されないデータはアプリケーション環境よりもデスクトップ環境により関連性が高くなります。たとえば、デスクトップショートカットは**デスクトップ**フォルダーに保存され、Windows 10マシンから作成されたものであれば役立つ可能性がありますが、Windows Serverマシンから作成されたものでは役立たない場合があります。
- リダイレクトされないフォルダーの場合：

- ユーザーのダウンロードファイルでサーバーを散らかしたくないため、ダウンロードフォルダーをリダイレクトしないことを選択します
- 個々のアプリケーションからのデータは互換性やパフォーマンスの問題を引き起こす可能性があるため、アプリケーションデータフォルダーをリダイレクトしないことを決定します

フォルダーリダイレクトの詳細については、フォルダーリダイレクト、オフラインファイル、および移動ユーザープロファイルの概要を参照してください。

フォルダーリダイレクトと除外

Citrix Profile Management (ただしStudioではない) では、パフォーマンス強化により、除外を使用してフォルダーが処理されるのを防ぐことができます。この機能を使用する場合、リダイレクトされたフォルダーを除外しないでください。フォルダーリダイレクトと除外機能は連携して動作します。リダイレクトされたフォルダーが除外されないようにすることで、Profile Managementはそれらをプロファイルフォルダー構造に戻し、後でリダイレクトしないと決定した場合でもデータ整合性を維持できます。除外の詳細については、「アイテムの含める/除外」(/ja-jp/profile-management/current-release/configure/include-and-exclude-items.html)を参照してください。

VDA登録

はじめに

> **注:**
>
> オンプレミス環境では、VDAはDelivery Controllerに登録します。Citrix Cloudサービス環境では、VDAはCloud Connectorに登録します。ハイブリッド環境では、一部のVDAはDelivery Controllerに登録し、他のVDAはCloud Connectorに登録します。

> VDAを使用する前に、サイト上の1つ以上のControllerまたはCloud Connectorに登録（通信を確立）する必要があります。VDAは、`ListofDDCs`と呼ばれるリストをチェックして、ControllerまたはConnectorを見つけます。VDA上の`ListOfDDCs`には、そのVDAをサイト上のControllerまたはCloud Connectorにポイントするエントリが含まれています。負荷分散のため、VDAはリスト内のすべてのControllerまたはCloud Connectorに接続を自動的に分散します。

VDA登録がそれほど重要であるのはなぜですか？

- セキュリティの観点から見ると、登録は機密性の高い操作です。ControllerまたはCloud ConnectorとVDA間の接続を確立しています。このような機密性の高い操作では、すべてが完璧な状態でない場合、接続を拒否するのが期待される動作です。事実上、VDAからControllerまたはCloud Connectorへ、およびControllerまたはCloud ConnectorからVDAへの2つの別々の通信チャネルを確立しています。接続にはKerberosが使用されるため、時刻同期やドメインメンバーシップの問題は許容されません。Kerberosはサービスプリンシパル名（SPN）を使用するため、負荷分散されたIP\\ホスト名を使用することはできません。
- Controller（またはCloud Connector）を追加および削除する際に、VDAに正確で最新のControllerまたはCloud Connector情報がない場合、VDAは、リストにないControllerまたはCloud Connectorによって仲介されるセッション起動を拒否する可能性があります。無効なエントリは、仮想デスクトップシステムソフトウェアの起動を遅らせる可能性があります。VDAは、不明で信頼されていないControllerまたはCloud Connectorからの接続を受け入れません。

`ListofDDCs`に加えて、`ListOfSIDs`（セキュリティID）は、`ListofDDCs`内のどのマシンが信頼されているかを示します。`ListofSIDs`は、Active Directoryの負荷を軽減したり、侵害されたDNSサーバーからの潜在的なセキュリティ脅威を回避したりするために使用できます。詳細については、ListOfSIDsを参照してください。

`ListofDDCs`が複数のControllerまたはCloud Connectorを指定している場合、VDAはランダムな順序でそれらに接続しようとします。オンプレミス展開では、`ListofDDCs`にはControllerグループも含まれる場合があります。VDAは、`ListofDDCs`内の他のエントリに移動する前に、グループ内の各Controllerに接続しようとします。

Citrix Virtual Apps and Desktops™は、VDAインストール中に構成されたControllerまたはCloud Connectorへの接続を自動的にテストします。ControllerまたはCloud Connectorに到達できない場合、エラーが表示されます。ControllerまたはCloud Connectorに連絡できないという警告を無視した場合（またはVDAインストール中にControllerまたはCloud Connectorアドレスを指定しなかった場合）、メッセージが表示されて通知されます。

ControllerまたはCloud Connectorアドレスを構成する方法

管理者は、VDAが初めて登録するとき（初回登録時）に使用する構成方法を選択します。初回登録時に、VDA上に永続キャッシュが作成されます。その後の登録では、構成の変更が検出されない限り、VDAはこのローカルキャッシュからControllerまたはCloud Connectorのリストを取得します。

その後の登録でそのリストを取得する最も簡単な方法は、自動更新機能を使用することです。自動更新はデフォルトで有効になっています。詳細については、「自動更新」を参照してください。

VDA上でControllerまたはCloud Connectorアドレスを構成する方法はいくつかあります。

- ポリシーベース (LGPOまたはGPO)
- レジストリベース (手動、グループポリシー設定 (GPP)、VDAインストール時に指定)
- Active Directory OUベース (レガシーOU検出)
- MCSベース (personality.ini)

VDAをインストールする際に、初期登録方法を指定します。(自動更新を無効にした場合、VDAインストール時に選択した方法がその後の登録に使用されます。)

次の図は、VDAインストールウィザードの**Delivery Controller**ページを示しています。

VDAインストールウィザードのDelivery Controllerページ(/en-us/citrix-virtual-apps-desktops/2407/media/vda-install-controllers-all.png)

ポリシーベース (LGPO\\GPO)

Citrix®は、初期VDA登録にGPOを使用することを推奨します。これは最も高い優先順位を持ちます。(自動更新が最も高い優先順位としてリストされていますが、自動更新は初期登録後にのみ使用されます。) ポリシーベースの登録は、構成にグループポリシーを使用することによる一元化の利点を提供します。

この方法を指定するには、以下の両方の手順を完了します。

- VDAインストールウィザードの**Delivery Controller**ページで、**後で実行 (詳細設定)** を選択します。ウィザードは、VDAインストール中にコントローラーアドレスを指定しない場合でも、コントローラーアドレスを指定するよう何度も通知します。(VDA登録はそれほど重要です。)
- Citrixポリシーで`Virtual Delivery Agent Settings > Controllers`設定を使用して、ポリシーベースのVDA登録を有効または無効にします。(セキュリティが最優先事項である場合は、`Virtual Delivery Agent Settings > Controller SIDs`設定を使用します。)

この設定は`HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)`に保存されます。

レジストリベース

この方法を指定するには、以下のいずれかの手順を完了します。

- VDAインストールウィザードの**Delivery Controller**ページで、**手動で実行** を選択します。次に、インストールされているControllerのFQDNを入力し、**追加** をクリックします。複数のControllerをインストールしている場合は、それらのアドレスを追加します。
- コマンドラインVDAインストールの場合、/controllersオプションを使用し、インストールされているControllerまたはCloud ConnectorのFQDNを指定します。

この情報は、レジストリキー`HKLM\Software\Citrix\VirtualDesktopAgent`または`HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent`の下のレジストリ値`ListOfDDCs`に保存されます。

このレジストリキーは手動で構成することも、Group Policy Preferences（GPP）を使用することもできます。この方法は、ポリシーベースの方法よりも推奨される場合があります（たとえば、異なるControllerまたはCloud Connectorの条件付き処理が必要な場合。例：XDW-001-で始まるコンピューター名にはXDC-001を使用する）。

`ListOfDDCs`レジストリキーを更新します。このキーには、サイト内のすべてのControllerまたはCloud ConnectorのFQDNが一覧表示されます。(このキーはActive Directoryサイト OUに相当します。)

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)`

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`レジストリの場所に`ListOfDDCs`キーと`FarmGUID`キーの両方が含まれている場合、ControllerまたはCloud Connectorの検出には`ListOfDDCs`が使用されます。VDAインストール中にサイトOUが指定された場合、`FarmGUID`が存在します。（これはレガシー展開で使用される場合があります。）

オプションで、`ListOfSIDs`レジストリキーを更新します（詳細については、ListOfSIDsを参照してください）。

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)`

注意：Citrixポリシーを介してポリシーベースのVDA登録も有効にすると、VDAインストール中に指定した設定が上書きされます。これは優先度の高い方法であるためです。

Active Directory OUベース (レガシー)

この方法は主に下位互換性のためにサポートされており、推奨されません。まだこの方法を使用している場合は、別の方法に変更することをお勧めします。

この方法を指定するには、以下の両方の手順を完了します。

- VDAインストールウィザードの**Delivery Controller**ページで、**Active Directoryから場所を選択**を選択します。
- `Set-ADControllerDiscovery.ps1`スクリプト（すべてのControllerで利用可能）を使用します。また、各VDAで`FarmGuid`レジストリエントリを構成して、正しいOUを指すようにします。この設定は、グループポリシーを使用して構成できます。

MCSベース

MCSを使用してVMをプロビジョニングする場合、MCSはControllerまたはCloud Connectorのリストを設定します。この機能は自動更新と連携します。カタログ作成時、MCSは初期プロビジョニング中にControllerまたはCloud Connectorのリストを`Personality.ini`ファイルに挿入します。自動更新により、リストは最新の状態に保たれます。

この方法を指定するには、VDAインストールウィザードの **Delivery Controller** ページで、**Machine Creation Services™に任せる** を選択します。

レビューと推奨事項

ベストプラクティスとして:

- 初期登録にはグループポリシー登録方法を使用します。
- 自動更新（デフォルトで有効）を使用して、Controller のリストを最新の状態に保ちます。
- マルチゾーン展開では、初期構成にはグループポリシーを使用します（Controller または Cloud Connector が少なくとも2つある場合）。VDA を、そのゾーン内のローカルな Controller または Cloud Connector に向けます。自動更新を使用して、それらを最新の状態に保ちます。自動更新は、サテライトゾーンの VDA の `ListofDDCs` を自動的に最適化します。
- Controller が利用できない場合の登録問題を回避するために、`ListOfDDCs` レジストリキーに複数の Controller をスペースで区切ってリストします。例:

  ```
  DDC7x.xd.local DDC7xHA.xd.local



  32-bit: HKEY_LOCAL_MACHINE
  \Software\Citrix\VirtualDesktopAgent\ListOfDDCs



  HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\ListOfDDCs
  (REG_SZ)
  ```

- 起動時の登録遅延を防ぐため、`ListofDDCs`の下にリストされているすべての値が有効な完全修飾ドメイン名にマッピングされていることを確認します。

自動更新

自動更新（XenAppおよびXenDesktop 7.6で導入）はデフォルトで有効になっています。これは、VDA登録を最新の状態に保つための最も効率的な方法です。初期登録には使用されませんが、初期登録時に自動更新ソフトウェアが`ListofDDCs`をダウンロードし、VDA上の永続キャッシュに保存します。このプロセスは各VDAに対して実行されます。キャッシュにはマシンポリシー情報も保持され、ポリシー設定が再起動後も維持されるようにします。

自動更新は、MCS または Citrix Provisioning™ を使用してマシンをプロビジョニングする場合にサポートされます。ただし、Citrix Provisioning のサーバー側キャッシュは除きます。サーバー側キャッシュは、自動更新キャッシュ用の永続ストレージがないため、一般的なシナリオではありません。

この方法を指定するには:

- 設定`Virtual Delivery Agent Settings > Enable auto update of Controllers`を含む Citrix ポリシーを通じて、自動更新を有効または無効にします。この設定はデフォルトで有効になっています。

仕組み:

- VDAが再登録されるたびに (たとえば、マシンの再起動後など)、キャッシュが更新されます。各ControllerまたはCloud Connectorも90分ごとにサイトデータベースをチェックします。前回のチェック以降にControllerまたはCloud Connectorが追加または削除された場合、またはVDA登録に影響するポリシー変更が発生した場合、ControllerまたはCloud Connectorは登録済みVDAに更新されたリストを送信し、キャッシュが更新されます。VDAは、最新のキャッシュされたリストにあるすべてのControllerまたはCloud Connectorからの接続を受け入れます。
- VDAが、登録されているControllerまたはCloud Connectorが含まれていないリストを受信した場合 (つまり、そのControllerまたはCloud Connectorがサイトから削除された場合)、VDAは`ListofDDCs`内のControllerまたはCloud Connectorの中から選択して再登録します。

例:

- 展開には3つのController (A、B、C) があります。VDAはController Bに登録します (これはVDAのインストール時に指定されました)。
- その後、2つのController (DとE) がサイトに追加されます。90分以内に、VDAは更新されたリストを受信し、Controller A、B、C、D、Eからの接続を受け入れます。(VDAが再起動されるまで、負荷はすべてのControllerに均等に分散されません。)
- さらにその後、Controller Bは別のサイトに移動されます。90分以内に、元のサイトのVDAは、前回のチェック以降にControllerの変更があったため、更新されたリストを受信します。

元々Controller Bに登録されていたVDA (リストにはもうありません) は、現在のリスト (A、C、D、E) のControllerの中から選択して再登録します。

マルチゾーン展開では、サテライトゾーンの自動更新機能が、まずすべてのローカルControllerを自動的にキャッシュします。プライマリゾーンのすべてのControllerは、バックアップグループにキャッシュされます。サテライトゾーンにローカルControllerが利用できない場合、プライマリゾーンのControllerへの登録が試行されます。

次の例に示すように、キャッシュファイルにはホスト名とセキュリティID (`ListofSIDs`) のリストが含まれています。VDAはSIDを照会しないため、Active Directoryの負荷が軽減されます。

VDAの登録キャッシュファイルの例(/en-us/citrix-virtual-apps-desktops/2407/media/vda-registration-cache-file.png)

キャッシュファイルはWMI呼び出しで取得できます。ただし、SYSTEMアカウントのみが読み取り可能な場所に保存されています。

> **重要:**
>
> この情報は情報提供のみを目的としています。このファイルを変更しないでください。このファイルまたはフォルダーへの変更は、サポートされていない構成になります。

```
Get-WmiObject -Namespace "Root\Citrix\DesktopInformation" -Class "Citrix_VirtualDesktopInfo" -Property "PersistentDataLocation"
```

セキュリティ上の理由から (Active Directoryの負荷軽減とは別に) `ListofSIDs` を手動で構成する必要がある場合、自動更新機能を使用することはできません。詳細については、「ListOfSIDs」を参照してください。

自動更新の優先順位の例外

自動更新は通常、すべてのVDA登録方法の中で最も高い優先順位を持ち、他の方法の設定を上書きしますが、例外があります。キャッシュ内の `NonAutoListOfDDCs` 要素は、初期VDA構成方法を指定します。自動更新はこの情報を監視します。初期登録方法が変更された場合、登録プロセスは自動更新をスキップし、次に高い優先順位で構成された方法を使用します。このプロセスは、VDAを別のサイトに移動する場合 (たとえば、ディザスターリカバリー中) に役立ちます。

構成に関する考慮事項

一般的なVDA登録構成を表示します。

<iframe src="https://www.youtube.com/embed/MgGMZp4SnZgEq9ieibQc9j" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
VDA登録手順を表示します。

<iframe src="https://www.youtube.com/embed/iwsbajSVY5QvoUTh6m7AjG" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
VDA登録に影響を与える可能性のある項目を構成する際は、次の点を考慮してください。

ControllerまたはCloud Connectorのアドレス

ControllerまたはCloud Connectorを指定するためにどの方法を使用するかにかかわらず、CitrixはFQDNアドレスを使用することを推奨します。IPアドレスはDNSレコードよりも侵害されやすいため、信頼できる構成とは見なされません。`ListofSIDs` を手動で入力する場合、`ListofDDCs` でIPを使用できます。ただし、FQDNが引き続き推奨されます。

負荷分散

前述のとおり、VDAは`ListofDDCs`内のすべてのControllerまたはCloud Connectorに接続を自動的に分散します。フェールオーバーと負荷分散機能は、Citrix Brokering Protocol (CBP) に組み込まれています。構成で複数のControllerまたはCloud Connectorを指定した場合、必要に応じて登録はそれらの間で自動的にフェールオーバーします。自動更新では、すべてのVDAで自動フェールオーバーが自動的に発生します。

セキュリティ上の理由から、Citrix ADCなどのネットワークロードバランサーを使用することはできません。VDA登録ではKerberos相互認証を使用します。これは、クライアント（VDA）がサービス（Controller）に対して自身のIDを証明する必要があることを意味します。しかし、ControllerまたはCloud ConnectorもVDAに対して自身のIDを証明する必要があります。これは、VDAとControllerまたはCloud Connectorが同時にサーバーとクライアントとして機能することを意味します。この記事の冒頭で述べたように、VDAからController/Cloud Connectorへ、およびController/Cloud ConnectorからVDAへの2つの通信チャネルがあります。

このプロセスにおけるコンポーネントの1つは、サービスプリンシパル名（SPN）と呼ばれ、Active Directoryコンピューターオブジェクトのプロパティとして保存されます。VDAがControllerまたはCloud Connectorに接続するとき、通信したい相手を指定する必要があります。このアドレスがSPNです。負荷分散されたIPを使用すると、Kerberos相互認証は、そのIPが予期されるControllerまたはCloud Connectorに属していないことを正しく認識します。

詳細については、以下を参照してください。

- Kerberosの概要(https://blogs.technet.microsoft.com/askds/2008/03/06/kerberos-for-the-busy-admin/)

- Kerberosを使用した相互認証(https://docs.microsoft.com/ja-jp/windows-server/security/kerberos/kerberos-authentication-overview)

自動更新によるCNAMEの置き換え

自動更新機能は、XenAppおよびXenDesktop 7.xより前のバージョンにおけるCNAME（DNSエイリアス）機能を置き換えます。CNAME機能は、XenAppおよびXenDesktop 7以降では無効になっています。CNAMEの代わりに自動更新を使用してください。（CNAMEを使用する必要がある場合は、CTX137960を参照してください。DNSエイリアスを常に機能させるには、自動更新とCNAMEの両方を同時に使用しないでください。）

Controller/Cloud Connectorグループ

特定のシナリオでは、ControllerまたはCloud Connectorをグループで処理し、一方のグループを優先し、すべてのController/Cloud Connectorが失敗した場合に他方のグループをフェイルオーバーに使用したい場合があります。ControllerまたはCloud Connectorはリストからランダムに選択されるため、グループ化によって優先的な使用を強制できることに注意してください。

これらのグループは、単一のサイト内での使用を目的としています（複数のサイトではありません）。

Controller/Cloud Connectorのグループを指定するには、かっこを使用します。たとえば、4つのController（プライマリ2つ、バックアップ2つ）がある場合、グループ化は次のようになります。

```
(XDC-001.cdz.lan XDC-002.cdz.lan) (XDC-003.cdz.lan XDC-004.cdz.lan)
```

この例では、最初のグループのController（001と002）が最初に処理されます。両方が失敗した場合、2番目のグループのController（003と004）が処理されます。

XenDesktop 7.0以降では、**登録グループ**機能を使用するために追加の手順を実行する必要があります。Studioから**Controllerの自動更新を有効にする**ポリシーを**禁止**する必要があります。

ListOfSIDs

VDAが登録のために連絡できるControllerのリストは`ListofDDCs`です。VDAは、`ListofDDCs`内のControllerを自動的に信頼しないため、どのControllerを信頼すべきかも知っている必要があります。`ListofSIDs`（セキュリティID）は、信頼されたControllerを識別します。VDAは、信頼されたControllerにのみ登録を試みます。

ほとんどの環境では、`ListofSIDs`は`ListofDDCs`から自動的に生成されます。CDFトレースを使用して`ListofSIDs`を読み取ることができます。

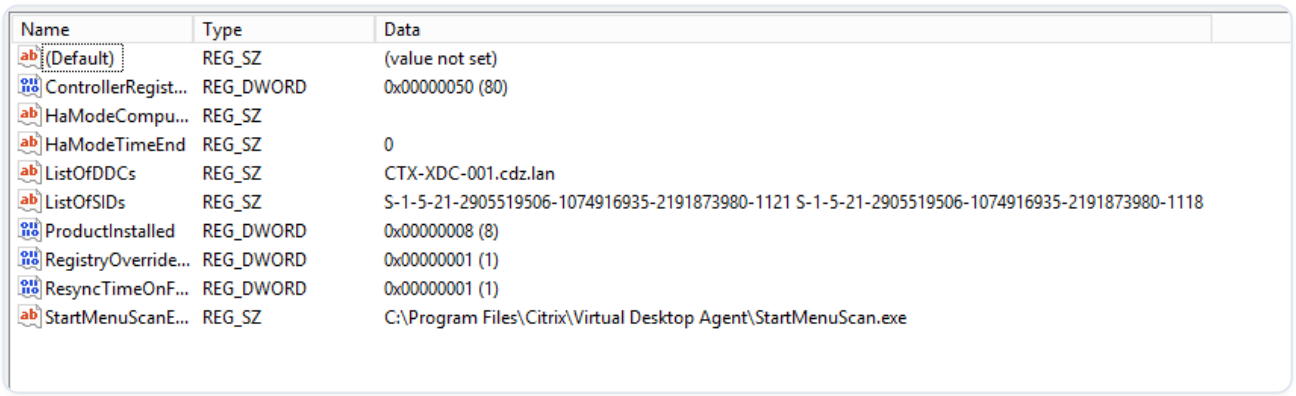
一般的に、`ListofSIDs`を手動で変更する必要はありません。いくつかの例外があります。最初の2つの例外は、新しいテクノロジーが利用可能になったため、もはや有効ではありません。

- **Controllerの役割の分離:** XenAppおよびXenDesktop 7.7でゾーンが導入される前は、Controllerのサブセットのみが登録に使用されていた場合、`ListofSIDs`は手動で構成されていました。たとえば、XDC-001とXDC-002をXMLブローカーとして使用し、XDC-003とXDC-004をVDA登録に使用していた場合、すべてのControllerを`ListofSIDs`に、XDC-003とXDC-004を`ListofDDCs`に指定していました。これは一般的または推奨される構成ではありません。新しい環境では使用しないでください。代わりにゾーンを使用してください。
- **Active Directoryの負荷軽減:** XenAppおよびXenDesktop 7.6で自動更新機能が導入される前は、`ListofSIDs`を使用してドメインコントローラーの負荷を軽減していました。`ListofSIDs`を事前に入力することで、DNS名からSIDへの解決をスキップできます。ただし、この永続キャッシュにはSIDが含まれているため、自動更新機能によりこの作業は不要になります。Citrixでは、自動更新機能を有効にしておくことを推奨しています。
- **セキュリティ:** 一部の高度に保護された環境では、侵害されたDNSサーバーからの潜在的なセキュリティ脅威を回避するために、信頼できるControllerのSIDが手動で構成されていました。ただし、これを行う場合は、自動更新機能も無効にする必要があります。そうしないと、永続キャッシュからの構成が使用されます。

したがって、特別な理由がない限り、`ListofSIDs`を変更しないでください。

`ListofSIDs`を変更する必要がある場合は、`HKLM\Software\Citrix\VirtualDesktopAgent`の下に`ListOfSIDs (REG_SZ)`という名前のレジストリキーを作成します。値は信頼されたSIDのリストで、複数ある場合はスペースで区切ります。

次の例では、VDA登録には1つのController (`ListofDDCs`) が使用されていますが、ブローカー処理には2つのController (List OfSIDs) が使用されています。



VDA 登録中の Controller 検索

VDA が登録を試行すると、Broker Agent はまずローカルドメインで DNS ルックアップを実行し、指定された Controller に到達できることを確認します。

最初のルックアップでControllerが見つからない場合、Broker AgentはADでフォールバックのトップダウンクエリを開始できます。このクエリはすべてのドメインを検索し、頻繁に繰り返されます。Controllerアドレスが無効な場合（たとえば、管理者がVDAのインストール時に誤ったFQDNを入力した場合）、そのクエリのアクティビティがドメインコントローラーで分散型サービス拒否（DDoS）状態を引き起こす可能性があります。

次のレジストリキーは、Broker Agent が最初の検索中に Controller を見つけられない場合に、フォールバックのトップダウンクエリを使用するかどうかを制御します。

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`

- 名前: `DisableDdcWildcardNameLookup`
- 種類: `DWORD`
- 値: `0` (デフォルト) または任意のゼロ以外の値

`0`に設定すると、フォールバック検索が有効になります。Controller の初期検索が失敗した場合、フォールバックのトップダウン検索が開始されます。これはデフォルトの動作です。ただし、ゼロ以外の値に設定すると、フォールバック検索は無効になります。Controller の初期検索が失敗した場合、Broker Agent は検索を停止します。

読み取り専用ドメインコントローラーを使用した VDA 登録中の LDAP バインディングシーケンス

VDA が読み取り専用ドメインコントローラー (RODC) に登録する場合、Broker Agent は無視する Light Directory Access Protocol (LDAP) バインディングを選択する必要があります。この選択を行うには、Broker Agent に適切なレジストリキーが必要です。

レジストリキーが提供されていない場合、またはレジストリキーフィールドが空の場合、元の LDAP バインディングシーケンスを通過する必要があるため、RODC を使用した VDA 登録には時間がかかります。

LDAP バインディングシーケンスを変更するために、レジストリキー `ListofIgnoredBindings` が `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent` に追加されました。`ListofIgnoredBindings` を使用すると、必要に応じて LDAP バインディングシーケンスを変更でき、それによって RODC を使用した VDA 登録を高速化できます。

- 名前: `ListofIgnoredBindings`
- 種類: `REG_SZ`
- 値: `DefaultPath`、`DomainPath`、`PDCPath`

値は、コンマで区切られたバインディングパスオプションのリストです。レジストリキーは、有効として認識しない値を無視します。

VDA 登録の問題のトラブルシューティング

前述のとおり、仲介セッションを起動する際に考慮されるためには、VDA が Delivery Controller または Cloud Connector に登録されている必要があります。未登録の VDA は、利用可能なリソースの利用率低下につながる可能性があります。VDA が登録されない理由はさまざまあり、その多くは管理者がトラブルシューティングできます。Studio は、カタログ作成ウィザードおよびデリバリーグループ作成後にトラブルシューティング情報を提供します。

- **マシンカタログ作成中の問題の特定:** カタログ作成ウィザードで、既存のマシンを追加した後、コンピューターアカウント名のリストは、各マシンがカタログに追加するのに適しているかどうかを示します。各マシンの横にあるアイコンにカーソルを合わせると、そのマシンに関する情報メッセージが表示されます。

  メッセージが問題のあるマシンを特定した場合、そのマシンを削除するか（**削除**ボタンを使用）、またはマシンを追加することができます。たとえば、メッセージがマシンに関する情報が取得されなかったことを示している場合（おそらく登録されたことがないため）、とにかくマシンを追加することを選択できます。

  カタログの機能レベルは、カタログ内のマシンで利用できる製品機能を制御します。新しい製品バージョンで導入された機能を使用するには、新しい VDA が必要になる場合があります。機能レベルを設定すると、そのバージョンで導入されたすべての機能（および機能レベルが変更されない場合はそれ以降のバージョン）がカタログ内のマシンで利用可能になります。ただし、そのカタログ内の以前の VDA バージョンのマシンは登録できません。
- **デリバリーグループ作成後の問題の特定:** デリバリーグループを作成した後、Studio はそのグループに関連付けられたマシンの詳細を表示します。

  デリバリーグループの詳細ペインには、登録が必要だが登録されていないマシンの数が表示されます。つまり、電源が入っていてメンテナンスモードではないが、現在コントローラーに登録されていないマシンが1台以上存在する可能性があります。「登録されていないが、登録が必要な」マシンを表示する際は、詳細ペインの**トラブルシューティング**タブで考えられる原因と推奨される是正措置を確認してください。

VDA登録のトラブルシューティングに関する詳細情報

- 機能レベルの詳細については、「VDAのバージョンと機能レベル」を参照してください。
- VDA登録のトラブルシューティングについて詳しくは、「CTX136668」を参照してください。
- VDA登録とセッション起動のトラブルシューティングには、Citrix Scoutのヘルスチェックも使用できます。詳細については、「ヘルスチェックについて」を参照してください。

仮想IPおよび仮想ループバック

重要:

- Windows 10 Enterprise multi-sessionはRemote Desktop IP Virtualization (Virtual IP) をサポートしておらず、Windows 10 Enterprise multi-sessionではRemote Desktop IP Virtualizationまたは仮想ループバックをサポートしていません。
- Remote Desktop IP Virtualization (Virtual IP) は、クラウドホスト型マシンではサポートされていません。 詳細については、Microsoft ドキュメントを参照してください。

Remote Desktop IP Virtualizationおよび仮想ループバック機能は、Windows Server 2016、Windows Server 2019、およびWindows Server 2022マシンでサポートされています。これらの機能は、WindowsデスクトップOSマシンには適用されません。

Microsoft Remote Desktop IP仮想化アドレス機能は、公開されたアプリケーションにセッションごとに一意の動的に割り当てられたIPアドレスを提供します。Citrix仮想ループバック機能を使用すると、localhost (デフォルトでは127.0.0.1) との通信に依存するアプリケーションを、localhost範囲 (127.*) の一意の仮想ループバックアドレスを使用するように構成できます。

CRMやCTI (Computer Telephony Integration) など、一部のアプリケーションは、アドレス指定、ライセンス、識別、または一意のIPアドレスやループバックアドレスを必要とするその他の目的でIPアドレスを使用します。他のアプリケーションは静的ポートにバインドされる場合があるため、マルチユーザー環境でアプリケーションの追加インスタンスを起動しようとすると、ポートが使用中であるために失敗します。このようなアプリケーションがCitrix Virtual Apps™環境で正しく機能するには、デバイスごとに一意のIPアドレスが必要です。

Remote Desktop IP Virtualizationと仮想ループバックは、互いに独立した機能です。どちらか一方、または両方を使用できます。

管理者アクションの概要:

- Microsoft Remote Desktop IP Virtualizationを使用するには、Windowsサーバーで有効にして構成します。(Citrix®ポリシー設定は不要です。)
- Citrix仮想ループバックを使用するには、Citrixポリシーで2つの設定を構成します。

リモートデスクトップIP仮想化 (仮想IP)

Remote Desktop IP VirtualizationがWindowsサーバーで有効化および構成されている場合、セッションで実行されている構成済みの各アプリケーションは、一意のアドレスを持っているように見えます。ユーザーは、他の公開アプリケーションにアクセスするのと同じ方法で、Citrix Virtual Appsサーバー上のこれらのアプリケーションにアクセスします。プロセスがRemote Desktop IP Virtualizationを必要とするのは、次のいずれかのケースです。

- プロセスがハードコードされたTCPポート番号を使用している
- プロセスがWindowsソケットを使用しており、一意のIPアドレスまたは指定されたTCPポート番号を必要としている

アプリケーションが Remote Desktop IP Virtualization アドレスを使用する必要があるかどうかを判断するには：

1. Microsoftから**TCPView**ツールを入手します。このツールは、特定のIPアドレスとポートをバインドするすべてのアプリケーションを一覧表示します。TCPViewの詳細については、Microsoftドキュメントを参照してください。
2. **IPアドレスの解決**機能を無効にして、ホスト名ではなくアドレスが表示されるようにします。
3. アプリケーションを起動し、**TCPView**を使用して、アプリケーションが開くIPアドレスとポート、およびこれらのポートを開いているプロセス名を確認します。
4. サーバーのIPアドレス、0.0.0.0、または127.0.0.1を開くプロセスを構成します。
5. アプリケーションが異なるポートで同じ IP アドレスを開かないようにするには、アプリケーションの別のインスタンスを起動します。

Microsoft Remote Desktop (RD) IP仮想化の仕組み

- Microsoftサーバーで仮想IPアドレス指定を有効にする必要があります。

  たとえば、Windows Server 2016 環境では、サーバーマネージャーから **Remote Desktop Services > RD Session Host Connections** を展開して、RD IP Virtualization 機能を有効にし、セッションごとまたはプログラムごとに動的ホスト構成プロトコル (DHCP) サーバーを使用して IP アドレスを動的に割り当てる設定を構成します。Remote Desktop IP Virtualization の構成の詳細については、Microsoft ドキュメント を参照してください。

- 機能を有効にすると、セッションの開始時に、サーバーはDHCPサーバーから動的に割り当てられたIPアドレスを要求します。
- The **RD IP Virtualization**機能は、リモートデスクトップ接続にセッションごとまたはプログラムごとにIPアドレスを割り当てます。複数のプログラムにIPアドレスを割り当てる場合、それらはセッションごとのIPアドレスを共有します。
- アドレスがセッションに割り当てられると、次の呼び出しが行われるたびに、システムはプライマリIPアドレスではなく仮想アドレスを使用します: `bind`、`closesocket`、`connect`、`WSAConnect`、`WSAAccept`、`getpeername`、`getsockname`、`sendto`、`WSASendTo`、`WSASocketW`、`gethostbyaddr`、`getnameinfo`、`getaddrinfo`。

リモートデスクトップセッションホスティング構成内でMicrosoft IP仮想化機能を使用する場合、アプリケーションとWinsock関数呼び出しの間に「フィルター」コンポーネントを挿入することで、アプリケーションは特定のIPアドレスにバインドされます。これにより、アプリケーションは使用すべき正しいIPアドレスのみを認識します。アプリケーションがTCPまたはUDP通信をリッスンしようとすると、自動的に割り当てられた仮想IPアドレス（またはループバックアドレス）にバインドされます。アプリケーションによって開かれた発信接続はすべて、アプリケーションにバインドされたIPアドレスから発信されます。

アドレスを返す関数（Windowsポリシーが制御する`GetAddrInfo()`など）で、ローカルホストIPアドレスが要求された場合、リモートデスクトップIP仮想化は返されたIPアドレスを調べ、それをセッションのリモートデスクトップIP仮想化アドレスに変更します。このような名前関数を介してローカルサーバーのIPアドレスを取得しようとするアプリケーションは、そのセッションに割り当てられた一意のリモートデスクトップIP仮想化アドレスのみを認識します。このIPアドレスは、バインドや接続などの後続のソケット呼び出しでよく使用されます。Windowsポリシーの詳細については、Windows ServerでのRDS IP仮想化を参照してください。

多くの場合、アプリケーションはアドレス0.0.0.0でリッスンするためにポートへのバインドを要求します。アプリケーションがこれを行い、静的ポートを使用する場合、アプリケーションの複数のインスタンスを起動することはできません。リモートデスクトップIP仮想化アドレス機能は、これらの呼び出しタイプで0.0.0.0も検索します。これにより、呼び出しが特定のリモートデスクトップIP仮想化アドレスでリッスンするように変更され、複数のアプリケーションが同じコンピューター上の同じポートでリッスンできるようになります。これは、それらすべてが異なるアドレスでリッスンしているためです。呼び出しは、ICAセッション内であり、リモートデスクトップIP仮想化アドレス機能が有効になっている場合にのみ変更されます。たとえば、異なるセッションで実行されているアプリケーションの2つのインスタンスが、両方ともすべてのインターフェイス（0.0.0.0）と特定のポート（9000など）にバインドしようとすると、VIPAddress1:9000とVIPAddress2:9000にバインドされ、競合は発生しません。

仮想ループバック

「**Citrix Remote Desktop IP Virtualization loopback policy**」設定を有効にすると、各セッションが通信用に独自のループバックアドレスを持つことができます。アプリケーションがWinsock呼び出しでlocalhostアドレス（デフォルト = 127.0.0.1）を使用すると、仮想ループバック機能は127.0.0.1を127.X.X.Xに置き換えます。ここで、X.X.Xはセッション ID + 1を表します。たとえば、セッションIDが7の場合、127.0.0.8となります。セッションIDが第4オクテット（255を超える）を超過する可能性は低いですが、その場合、アドレスは次のオクテット（127.0.1.0）に繰り上がり、最大127.255.255.255までとなります。

プロセスが仮想ループバックを必要とするのは、次のいずれかのケースです。

- プロセスがWindowsソケットループバック（localhost）アドレス（127.0.0.1）を使用している場合
- プロセスがハードコードされたTCPポート番号を使用している場合

プロセス間通信にループバックアドレスを使用するアプリケーションには、仮想ループバックポリシー設定を使用します。追加の構成は不要です。仮想ループバックは仮想IPに依存しないため、Microsoftサーバーを構成する必要はありません。

- 仮想IPループバックサポート。有効にすると、このポリシー設定により、各セッションが独自の仮想ループバックアドレスを持つことができます。この設定はデフォルトで無効になっています。この機能は、仮想IP仮想ループバックプログラムリストポリシー設定で指定されたアプリケーションにのみ適用されます。
- 仮想IP仮想ループバックプログラムリスト。このポリシー設定は、仮想IPループバック機能を使用するアプリケーションを指定します。この設定は、仮想IPループバックサポートポリシー設定が有効になっている場合にのみ適用されます。
- 仮想IPループバックポート除外。アプリケーションがこの設定で指定されたポートでループバックアドレスを呼び出す場合、仮想ループバックはセッション固有のループバックアドレスへの呼び出しを変更しません。

関連機能

仮想ループバックが仮想IPよりも優先されるように、以下のレジストリ設定を使用できます。この機能は「優先ループバック」と呼ばれます。ただし、注意して進めてください。

- 優先ループバックは、仮想IPと仮想ループバックの両方が有効になっている場合にのみ使用してください。そうしないと、予期しない結果が生じる可能性があります。
- レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用に

よって生じる問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

アプリケーションが常駐するサーバーでregeditを実行します。

- HKEY_LOCAL_MACHINE\\SOFTWARE\\Wow6432Node\\Citrix\\VIP
- 名前: PreferLoopback, 種類: REG_DWORD, データ: 1
- 名前: PreferLoopbackProcesses, 種類: REG_MULTI_SZ, データ: \<プロセスのリスト\>

ゾーン

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

> WANで接続された広範囲に分散した場所にまたがる展開では、ネットワークの遅延と信頼性により課題が生じる可能性があります。これらの課題を軽減する2つのオプションがあります。

- 複数のサイトを展開し、それぞれに独自のSQL Serverサイトデータベースを持たせる。

  このオプションは、大規模なエンタープライズ展開に推奨されます。複数のサイトは個別に管理され、それぞれに独自のSQL Serverサイトデータベースが必要です。各サイトは独立したCitrix Virtual Apps™展開です。

- 単一サイト内に複数のゾーンを構成する。

  ゾーンを構成することで、リモート地域のユーザーがWANの大部分を通過することなくリソースに接続できるようになります。ゾーンを使用すると、単一のWeb Studioコンソール、Citrix Director、およびサイトデータベースから効果的なサイト管理が可能になります。これにより、リモートロケーションに個別のデータベースを含むより多くのサイトを展開、人員配置、ライセンス供与、および運用するコストを節約できます。

  ゾーンは、あらゆる規模の展開で役立ちます。ゾーンを使用して、アプリケーションとデスクトップをエンドユーザーの近くに配置することで、パフォーマンスを向上させることができま

す。ゾーンには、冗長性と回復性のために1つ以上のControllerをローカルにインストールできますが、必須ではありません。

サイトに構成されているControllerの数は、サイト自体に新しいControllerを追加するなどの一部の操作のパフォーマンスに影響を与える可能性があります。これを避けるため、Citrix Virtual AppsまたはCitrix Virtual Desktops™サイトのゾーン数を50以下に制限することをお勧めします。

ゾーンのネットワーク遅延が250ミリ秒RTTを超える場合は、ゾーンではなく複数のサイトを展開することをお勧めします。

この記事全体を通して、「ローカル」という用語は、議論されているゾーンを指します。たとえば、「VDAがローカルControllerに登録する」とは、VDAがVDAが配置されているゾーン内のControllerに登録することを意味します。

このリリースでのゾーンは、XenAppバージョン6.5以前のゾーンと似ていますが、同じではありません。たとえば、このゾーンの実装では、データコレクターはありません。サイト内のすべてのControllerは、プライマリゾーン内の1つのサイトデータベースと通信します。また、このリリースではフェールオーバーゾーンと優先ゾーンの動作が異なります。

ゾーンの種類

サイトには常に1つのプライマリゾーンがあります。オプションで1つ以上のサテライトゾーンを持つこともできます。サテライトゾーンは、災害復旧、地理的に離れたデータセンター、支店、クラウド、またはクラウド内のアベイラビリティゾーンに使用できます。

プライマリゾーン:

プライマリゾーンのデフォルト名は「Primary」です。このゾーンには、SQL Serverサイトデータベース（および、使用されている場合は高可用性SQLサーバー）、Web Studio、Director、Citrix StoreFront™、Citrix License Server、Citrix Gatewayが含まれます。サイトデータベースは常にプライマリゾーンに保持してください。

プライマリゾーンには、冗長性のために少なくとも2つのControllerが必要です。プライマリゾーンには、データベースおよびインフラストラクチャと密接に連携するアプリケーションを持つVDAを配置できます。

サテライトゾーン:

サテライトゾーンには、1つ以上のVDA、Controller、StoreFrontサーバー、Citrix Gatewayサーバーが含まれます。通常の運用では、サテライトゾーンのControllerはプライマリゾーンのデータベースと直接通信します。

サテライトゾーン、特に大規模なものは、そのゾーンのマシンをプロビジョニングおよび保存するために使用されるハイパーバイザーを含む場合もあります。サテライトゾーンを構成するときは、ハイパーバイザーまたはその他のサービス接続を関連付けることができます。（その接続を使用するカタログがすべて同じゾーンにあることを確認してください。）

サイトには、独自のニーズと環境に基づいて、異なる構成のサテライトゾーンを含めることができます。次の図は、プライマリゾーンとサテライトゾーンの例を示しています。

プライマリゾーンとサテライトゾーンの図(/en-us/citrix-virtual-apps-desktops/2407/media/zones1.png)

図では、次のようになります。

- **プライマリゾーン:** 2つのController、Web Studio、Director、StoreFront、License Server、およびサイトデータベース（高可用性SQL Server展開を含む）が含まれます。プライマリゾーンには、複数のVDAとCitrix Gatewayも含まれます。
- **サテライトゾーン1: Controllerを持つVDA:** サテライトゾーン1には、Controller、VDA、およびStoreFrontサーバーが含まれます。このサテライトゾーンのVDAは、ローカルのControllerに登録されます。ローカルのControllerは、プライマリゾーンのサイトデータベースおよびライセンスサーバーと通信します。

  WANに障害が発生した場合、ローカルホストキャッシュ機能により、サテライトゾーンのControllerは、そのゾーンのVDAへの接続の仲介を継続できます。このような展開は、従業員がローカルのStoreFrontサイトとローカルのControllerを使用してローカルリソースにアクセスするオフィスで効果的です。
- **サテライトゾーン2: 冗長Controllerを持つVDA:** サテライトゾーン2には、2つのController、VDA、およびStoreFrontサーバーが含まれます。これは最も回復力のあるゾーンタイプであり、WANとローカルControllerの1つが同時に障害を起こした場合でも保護を提供します。

VDAの登録場所とControllerのフェールオーバー場所

プライマリゾーンとサテライトゾーンを含むサイトで、VDAの最小バージョンが7.7の場合:

- Primary zone の VDA は、Primary zone の Controller に登録します。Primary zone の VDA は、Satellite zone の Controller に登録しようとすることはありません。
- Satellite zone の VDA は、可能であればローカルの Controller に登録します。(これは優先 Controller と見なされます。) ローカルの Controller が利用できない場合 (たとえば、VDA 登録をこれ以上受け入れられない、または障害が発生した場合など)、VDA は Primary zone の Controller に登録しようとします。この場合、Satellite zone の Controller が再び利用可能に

なっても、VDA は Primary zone に登録されたままになります。Satellite zone の VDA は、別の Satellite zone の Controller に登録しようとすることはありません。

- Controller の VDA 検出で自動更新が有効になっており、VDA のインストール中に Controller アドレスのリストを指定した場合、最初の登録のためにそのリストから Controller がランダムに選択されます (Controller がどのゾーンにあるかに関係なく)。その VDA を持つマシンが再起動されると、VDA はローカルゾーンの Controller への登録を優先するようになります。
- Satellite zone の Controller が失敗した場合、可能であれば別のローカル Controller にフェールオーバーします。ローカル Controller が利用できない場合、Primary zone の Controller にフェールオーバーします。
- Controller をゾーンに出入りさせ、自動更新が有効になっている場合、両方のゾーンの VDA は、どの Controller がローカルで、どの Controller が Primary zone にあるかを示す更新されたリストを受け取ります。これにより、VDA はどの Controller に登録し、どの Controller から接続を受け入れることができるかを知ることができます。
- カタログを別のゾーンに移動すると、そのカタログ内の VDA は、カタログを移動したゾーンの Controller に再登録します。(カタログを別のゾーンに移動する場合、このゾーンと関連するホスト接続があるゾーンが適切に接続されていることを確認してください。帯域幅が制限されている場合や、高遅延の場合は、ホスト接続を関連するマシンカタログを含む同じゾーンに移動してください。)

Primary zone のすべての Controller が失敗した場合:

- Web Studio はサイトに接続できません。
- Primary zone の VDA への接続はできません。
- Primary zone の Controller が利用可能になるまで、サイトのパフォーマンスが低下します。

VDA バージョン 7.7 より前のサイトの場合:

- Satellite zone の VDA は、ローカルゾーンおよび Primary zone の Controller からの要求を受け入れます。(最小バージョン 7.7 の VDA は、他の Satellite zone の Controller 要求を受け入れることができます。)
- Satellite zone の VDA は、Primary zone またはローカルゾーンの Controller にランダムに登録します。(最小バージョン 7.7 の VDA はローカルゾーンを優先します。)

ゾーンの優先順位

ゾーンの優先順位機能を使用するには、StoreFront 3.7 および Citrix Gateway 11.0-65.x 以降を使用している必要があります。

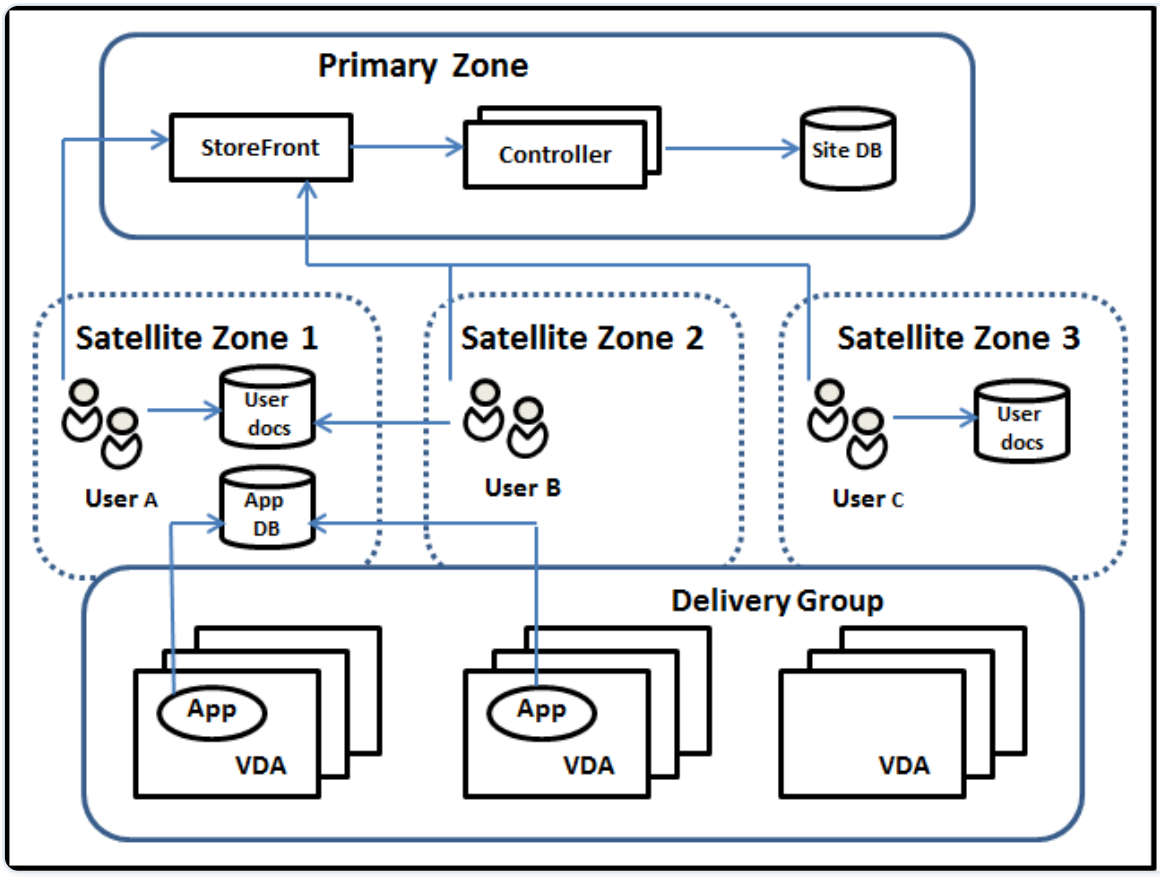
マルチゾーンサイトでは、ゾーン優先機能により、管理者はアプリケーションまたはデスクトップの起動に使用するVDAをより柔軟に制御できます。

ゾーンの優先順位の仕組み

ゾーン優先機能には3つの形式があります。特定のゾーンのVDAを使用することを推奨する場合があります。その判断基準は次のとおりです。

- アプリケーションのデータが保存されている場所。これは「アプリケーションホーム」と呼ばれます。
- プロファイルやホーム共有などのユーザーのホームデータの場所。これは「ユーザーホーム」と呼ばれます。
- ユーザーの現在の場所（Citrix Workspace™アプリが実行されている場所）。これは「ユーザーロケーション」と呼ばれます。

次の図は、マルチゾーン構成の例を示しています。



この例では、VDAは3つのサテライトゾーンに分散していますが、すべて同じデリバリーグループに属しています。そのため、ブローカーはユーザーの起動要求に対してどのVDAを使用するかを選択できます。この例は、ユーザーがCitrix Workspaceアプリのエンドポイントを実行できる場所がいくつかあることを示しています。

- ユーザーAは、サテライトゾーン1でCitrix Workspaceアプリがインストールされたデバイスを使用しています。
- ユーザーBは、サテライトゾーン2でデバイスを使用しています。
- ユーザーのドキュメントはさまざまな場所に保存できます。
  - ユーザーAとBは、サテライトゾーン1にある共有を使用します。
  - ユーザーCは、サテライトゾーンCの共有を使用します。
  - 公開されているアプリケーションの1つは、サテライトゾーン1にあるデータベースを使用します。

ユーザーまたはアプリケーションにホームゾーンを構成することで、ユーザーまたはアプリケーションをゾーンに関連付けます。その後、Delivery Controller™のブローカーは、これらの関連付けを使用して、リソースが利用可能な場合にセッションが起動されるゾーンを選択するのに役立ちます。次のことができます。

- ユーザーをゾーンに追加して、ユーザーのホームゾーンを構成する。
- アプリケーションのプロパティを編集して、アプリケーションのホームゾーンを構成する。

ユーザーまたはアプリケーションは、一度に1つのホームゾーンしか持つことができません。（ユーザーグループのメンバーシップにより複数のゾーンメンバーシップが発生する場合、ユーザーには例外が発生する可能性があります。「その他の考慮事項」セクションを参照してください。ただし、この場合でも、ブローカーは1つのホームゾーンのみを使用します。）

ユーザーとアプリケーションのゾーン設定は構成できますが、ブローカーは起動のために1つの優先ゾーンのみを選択します。優先ゾーンを選択するためのデフォルトの優先順位は、アプリケーションホーム \> ユーザーホーム \> ユーザーロケーションです。この順序を制限できます。「ゾーン設定の調整」(#tailoring-zone-preference)を参照してください。ユーザーがアプリケーションを起動すると、次のようになります。

- そのアプリケーションに構成済みのゾーン関連付け（アプリケーションホーム）がある場合、優先ゾーンはそのアプリケーションのホームゾーンになります。
- アプリケーションに構成済みのゾーン関連付けがないが、ユーザーに構成済みのゾーン関連付け（ユーザーホーム）がある場合、優先ゾーンはそのユーザーのホームゾーンになります。
- アプリケーションにもユーザーにも構成済みのゾーン関連付けがない場合、優先ゾーンはユーザーがCitrix Workspaceアプリインスタンスを実行しているゾーン（ユーザーロケーション）になります。そのゾーンが定義されていない場合、ランダムなVDAとゾーンの選択が使用されます。負荷分散は、優先ゾーン内のすべてのVDAに適用されます。優先ゾーンがない場合、負荷分散はデリバリーグループ内のすべてのVDAに適用されます。

ゾーンの優先順位の調整

ユーザーまたはアプリケーションのホームゾーンを構成（または削除）する際、ゾーン設定の使用方法をさらに制限できます。

- **必須のユーザーホームゾーンの使用：** デリバリーグループでは、セッションがユーザーのホームゾーン（構成されている場合）で起動されるように指定できます。ホームゾーンに利用可能なリソースがない場合でも、他のゾーンへのフェールオーバーは行われません。この制限は、ゾーン間で大きなプロファイルやデータファイルをコピーするリスクを回避する必要がある場合に役立ちます。つまり、別のゾーンでセッションを起動するよりも、セッションの起動を拒否する方が望ましいということです。
- **必須のアプリケーションホームゾーンの使用：** 同様に、アプリケーションのホームゾーンを構成する際、アプリケーションがそのゾーンでのみ起動され、アプリケーションのホームゾーンにリソースがない場合に別のゾーンへのフェールオーバーが行われないように指定できます。
- **アプリケーションホームゾーンなし、および構成済みのユーザーホームゾーンを無視：** アプリケーションのホームゾーンを指定しない場合、そのアプリケーションを起動する際に、構成済みのユーザーゾーンを考慮しないように指定することもできます。たとえば、一部のユーザーが異なるホームゾーンを持っている場合でも、ユーザーロケーションゾーン設定を使用して、ユーザーが自分のデバイスに近いVDAでアプリケーションを実行することを優先する場合があります。

優先ゾーンがセッションの使用に与える影響

ユーザーがアプリケーションまたはデスクトップを起動すると、ブローカーは既存のセッションを使用するよりも優先ゾーンを使用することを優先します。

アプリケーションまたはデスクトップを起動するユーザーが、起動されるリソースに適したセッションをすでに持っている場合（たとえば、アプリケーションのセッション共有を使用できるセッション、または起動されるリソースをすでに実行しているセッション）、そのセッションがユーザー/アプリケーションの優先ゾーン以外のゾーンにあるVDAで実行されていると、システムは新しいセッションを作成する可能性があります。これにより、そのユーザーのセッション要件にとって優先度の低いゾーンのセッションに再接続するよりも先に、正しいゾーンでの起動（利用可能な容量がある場合）が満たされます。

到達不能になった孤立セッションを防ぐため、既存の切断されたセッションへの再接続は、優先ゾーン以外にある場合でも許可されます。

起動を満たすためのセッションの望ましさの順序は次のとおりです。

1. 優先ゾーン内の既存のセッションに再接続する。

2. 優先ゾーン以外のゾーンにある既存の切断されたセッションに再接続する。
3. 優先ゾーンで新しいセッションを開始する。
4. 優先ゾーン以外のゾーンにある接続済みの既存セッションに再接続する。
5. 優先ゾーン以外のゾーンで新しいセッションを開始する。

その他のゾーン優先度に関する考慮事項

- ユーザーグループ（セキュリティグループなど）にホームゾーンを構成すると、そのグループのユーザー（直接的または間接的なメンバーシップを通じて）は指定されたゾーンに関連付けられます。ただし、ユーザーは複数のセキュリティグループのメンバーになることができ、そのため、他のグループメンバーシップを通じて異なるホームゾーンが構成されている場合があります。このような場合、そのユーザーのホームゾーンの決定は曖昧になる可能性があります。

ユーザーがグループメンバーシップを通じて取得したものではない構成済みのホームゾーンを持っている場合、そのゾーンがゾーン優先度に使用されます。グループメンバーシップを通じて取得されたゾーン関連付けはすべて無視されます。

ユーザーがグループメンバーシップのみを通じて取得した複数の異なるゾーン関連付けを持っている場合、ブローカーはゾーンの中からランダムに選択します。ブローカーがこの選択を行うと、そのゾーンは、ユーザーのグループメンバーシップが変更されるまで、その後のセッション起動に使用されます。

- ユーザーロケーションゾーンの優先設定では、エンドポイントデバイスが接続するCitrix GatewayによるエンドポイントデバイスのCitrix Workspaceアプリの検出が必要です。Citrix Gatewayは、IPアドレスの範囲を特定のゾーンに関連付けるように構成する必要があり、検出されたゾーンIDはStoreFrontを介してControllerに渡される必要があります。

ゾーンの優先設定の詳細については、「ゾーンの優先設定の内部」を参照してください。

考慮事項、要件、およびベストプラクティス

- ゾーンには、コントローラー、マシンカタログ、ホスト接続、ユーザー、アプリケーションを配置できます。カタログがホスト接続を使用する場合、カタログと接続が同じゾーンにあることを確認してください。(ただし、低遅延で高帯域幅の接続が利用可能な場合は、異なるゾーンに配置できます。)
- アイテムをサテライトゾーンに配置すると、サイトがそれらやそれらに関連する他のオブジェクトとどのようにやり取りするかに影響します。

  - コントローラーがサテライトゾーンに配置されると、それらのマシンは同じゾーン内のハイパーバイザーおよびVDAに対して良好な（ローカル）接続性を持つと想定されます。そのサテライトゾーンのコントローラーは、それらのハイパーバイザーおよびVDAマシンの処理において、プライマリゾーンのコントローラーよりも優先的に使用されます。
  - ハイパーバイザー接続がサテライトゾーンに配置されると、そのハイパーバイザー接続を介して管理されるすべてのハイパーバイザーもそのサテライトゾーンに存在すると想定されます。そのサテライトゾーンのコントローラーは、そのハイパーバイザー接続と通信する際に、プライマリゾーンのコントローラーよりも優先的に使用されます。
  - マシンカタログがサテライトゾーンに配置されると、そのカタログ内のすべてのVDAマシンがサテライトゾーンにあると想定されます。各VDAの初回登録後にコントローラーリストの自動更新メカニズムがアクティブになった後、サイトへの登録を試みる際には、プライマリゾーンのコントローラーよりもローカルコントローラーが優先的に使用されます。
  - Citrix Gatewayインスタンスもゾーンに関連付けることができます。これは、ここで説明されている他の要素のようにサイト構成の一部としてではなく、StoreFrontのOptimal HDX™ルーティング構成の一部として行われます。Citrix Gatewayがゾーンに関連付けられている場合、そのゾーン内のVDAマシンへのHDX接続が使用されるときに、そのCitrix Gatewayが優先的に使用されます。

- 本番サイトを作成し、最初のカタログとデリバリーグループを作成すると、すべてのアイテムはプライマリゾーンに配置されます。この初期設定が完了するまで、サテライトゾーンを作成することはできません。(空のサイトを作成した場合、プライマリゾーンには最初はコントローラーのみが含まれます。カタログとデリバリーグループを作成する前または後にサテライトゾーンを作成できます。)
- 1つ以上の項目を含む最初のサテライトゾーンを作成すると、サイト内の他のすべての項目はプライマリゾーンに残ります。
- プライマリゾーンはデフォルトで「Primary」という名前ですが、この名前は変更できます。Web Studioはどのゾーンがプライマリゾーンであるかを示しますが、プライマリゾーンには識別しやすい名前を使用することがベストプラクティスです。プライマリゾーンを再割り当てする（つまり、別のゾーンをプライマリゾーンにする）ことはできますが、常にサイトデータベースとすべての高可用性サーバーが含まれている必要があります。
- サイトデータベースは常にプライマリゾーンに保持してください。
- ゾーンを作成した後、後でアイテムをあるゾーンから別のゾーンに移動できます。この柔軟性により、近接して動作するのが最適なアイテムを分離できる可能性があります。たとえば、カタログを、そのカタログ内のマシンを作成する接続（ホスト）とは異なるゾーンに移動すると、パフォーマンスに影響を与える可能性があります。ゾーン間でアイテムを移動する前に、潜在的な意図しない影響を考慮してください。カタログとそれが使用するホスト接続は同じ

ゾーンに、または適切に接続されたゾーン（たとえば、低遅延で高帯域幅のネットワーク経由）に保持してください。

- 最適なパフォーマンスを得るには、Web StudioとDirectorはプライマリゾーンにのみインストールしてください。Web StudioとDirectorはWebアプリケーションであるため、サテライトゾーン（たとえば、プライマリゾーンがアクセス不能になった場合のフェイルオーバーとして使用するコントローラーを含むサテライトゾーン）からアクセスできます。
- 理想的には、サテライトゾーンのCitrix Gatewayは、他のゾーンまたは外部の場所からそのゾーンに入ってくるユーザー接続に使用されますが、ゾーン内の接続にも使用できます。
- 注意：ゾーン優先機能を使用するには、StoreFront 3.7以降およびCitrix Gateway 11.0-65.x以降を使用している必要があります。

接続品質の制限

サテライトゾーンのControllerは、サイトデータベースと直接SQL対話を行います。これにより、サテライトゾーンとサイトデータベースを含むプライマリゾーン間のリンク品質にいくつかの制限が課されます。具体的な制限は、サテライトゾーンに展開されているVDAの数と、それらのVDA上のユーザーセッションの数に関連しています。したがって、VDAとセッションが少ないサテライトゾーンは、VDAとセッションが多いサテライトゾーンよりも、データベースへの接続品質が低い場合でも機能できます。

詳細については、「Latency and SQL Blocking Query Improvements」を参照してください。

遅延がブローカリングパフォーマンスに与える影響

ゾーンによってユーザーは高遅延リンク上に存在できるようになりますが、ローカルブローカーがある場合でも、追加の遅延は必然的にエンドユーザーエクスペリエンスに影響を与えます。ユーザーが行うほとんどの作業において、サテライトゾーンのControllerとサイトデータベース間のラウンドトリップによって引き起こされる遅延を経験します。

アプリケーションを起動する場合、セッションブローカリングプロセスがセッション起動要求を送信するのに適したVDAを特定する際に、追加の遅延が発生します。

ゾーンの作成と管理

フル管理者であれば、すべてのゾーン作成および管理タスクを実行できます。ただし、ゾーンの作成、編集、削除を許可するカスタムロールを作成することもできます。ゾーン間でアイテムを移動する場合、ゾーン関連の権限（ゾーン読み取り権限を除く）は必要ありませんが、移動するアイテムに対する編集権限が必要です。たとえば、カタログをあるゾーンから別のゾーンに移動するには、そのカタログに対する編集権限が必要です。詳細については、「委任管理」を参照してください。

Citrix Provisioning™を使用する場合： Citrix Provisioningコンソールはゾーンを認識しないため、Web Studioを使用してサテライトゾーンのカタログを作成することをお勧めします。Web Studioでカタログを作成し、正しいサテライトゾーンを指定します。その後、Citrix Provisioningコンソールを使用して、そのカタログ内のマシンをプロビジョニングします。（Citrix Provisioningウィザードを使用してカタログを作成した場合、カタログはプライマリゾーンに配置されます。後でWeb Studioを使用してサテライトゾーンに移動する必要があります。）

ゾーンを作成する

1. Web Studioにサインインします。
2. 左ペインで**ゾーン**を選択します。
3. アクションバーで**ゾーンの作成**を選択します。
4. ゾーンの名前と説明（オプション）を入力します。名前はサイト内で一意である必要があります。
5. 新しいゾーンに配置するアイテムを選択します。選択可能なアイテムのリストをフィルター処理または検索できます。空のゾーンを作成することもできます。その場合は、何もアイテムを選択しないでください。
6. **保存**をクリックします。

この方法の代替として、Web Studioで1つ以上の項目を選択し、アクションバーで**ゾーンの作成**を選択できます。

ゾーン名または説明の変更

1. Web Studioにサインインします。
2. 左ペインで**ゾーン**を選択します。
3. 中央ペインでゾーンを選択し、アクションバーで**ゾーンの編集**を選択します。
4. ゾーン名、説明、またはその両方を変更します。プライマリゾーンの名前を変更する場合は、そのゾーンがプライマリゾーンとして容易に識別できることを確認してください。
5. または をクリックします。

ゾーン間でアイテムを移動する

1. Web Studioにサインインします。
2. 左ペインで**ゾーン**を選択します。
3. 中央ペインでゾーンを選択し、1つ以上の項目を選択します。

4. 項目を移動先のゾーンにドラッグするか、アクションバーで**項目の移動**を選択し、移動先のゾーンを指定します。

確認メッセージには、選択したアイテムが一覧表示され、それらすべてを移動してもよろしいかどうかが尋ねられます。

注意: カタログがハイパーバイザーまたはその他のサービスへのホスト接続を使用する場合、カタログと接続の両方を同じゾーンに配置してください。そうしないと、パフォーマンスに影響が出る可能性があります。一方を移動する場合は、もう一方も移動してください。

ゾーンを削除する

ゾーンは削除する前に空である必要があります。プライマリゾーンは削除できません。

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. 中央のペインでゾーンを選択します。
4. アクションバーから を選択します。ゾーンが空でない場合（アイテムが含まれている場合）、それらのアイテムを移動するゾーンを選択するよう求められます。
5. 削除を確認します。

ユーザーのホームゾーンを追加する

ユーザーのホームゾーンを構成することは、*ユーザーをゾーンに追加する*とも呼ばれます。

1. Web Studioにサインインします。
2. 左ペインで**ゾーン**を選択し、中央ペインでゾーンを選択します。
3. アクションバーで**ゾーンへのユーザーの追加**を選択します。
4. **ゾーンへのユーザーの追加**ダイアログボックスで、**追加**をクリックし、ゾーンに追加するユーザーとユーザーグループを選択します。すでにホームゾーンを持つユーザーを指定した場合、メッセージに2つの選択肢が表示されます。**はい** = ホームゾーンを持たない指定したユーザーのみを追加します。**いいえ** = ユーザー選択ダイアログに戻ります。
5. **OK**をクリックします。

ホームゾーンが構成されているユーザーの場合、セッションをそのホームゾーンからのみ起動するように要求できます。

1. デリバリーグループを作成または編集します。
2. 「**ユーザー**」ページで、「**セッションは、構成されている場合、ユーザーのホームゾーンで起動する必要があります**」チェックボックスを選択します。

そのデリバリーグループ内のユーザーが起動するすべてのセッションは、そのユーザーのホームゾーン内のマシンから起動する必要があります。デリバリーグループ内のユーザーに構成済みのホームゾーンがない場合、この設定は無効です。

ユーザーのホームゾーンを削除する

この手順は、ゾーンからユーザーを削除することとも呼ばれます。

1. Web Studioにサインインします。
2. 左ペインで「**ゾーン**」を選択し、中央ペインでゾーンを選択します。
3. アクションバーで「**ゾーンからユーザーを削除**」を選択します。
4. 「**ゾーンにユーザーを追加**」ダイアログボックスで、「**削除**」をクリックし、ゾーンから削除するユーザーとグループを選択します。この操作は、ユーザーをゾーンからのみ削除します。これらのユーザーは、所属するデリバリーグループおよびアプリケーショングループに残ります。
5. プロンプトが表示されたら削除を確定します。

アプリケーションのホームゾーンを管理する

アプリケーションのホームゾーンを構成することは、アプリケーションをゾーンに追加することとも呼ばれます。デフォルトでは、マルチゾーン環境では、アプリケーションにホームゾーンはありません。

アプリケーションのホームゾーンは、アプリケーションのプロパティで指定されます。アプリケーションをグループに追加するとき、または後でアプリケーションのプロパティを構成できます。

- デリバリーグループを作成するとき、アプリケーショングループを作成するとき、または既存のグループにアプリケーションを追加するときに、ウィザードの**Applications**ページで**Properties**を選択します。
- アプリケーションの追加後にアプリケーションのプロパティを変更するには、左ペインで**Applications**を選択します。アプリケーションを選択し、アクションバーで**Edit Application Properties**を選択します。

アプリケーションのプロパティ/設定の ページで、次の操作を行います。

- アプリケーションにホームゾーンを設定する場合：
  - **Use the selected zone to decide**ラジオボタンを選択し、ゾーンを選択します。
  - アプリケーションを、選択したゾーンからのみ（他のゾーンからは起動しないように）起動する場合は、ゾーン選択の下にあるチェックボックスをオンにします。

- アプリケーションにホームゾーンを設定しない場合：
  - ラジオボタンを選択します。
  - このアプリケーションを起動する際に、ブローカーが構成済みのユーザーゾーンを考慮しないようにする場合は、ラジオボタンの下にあるチェックボックスを選択します。この場合、アプリケーションまたはユーザーのホームゾーンのいずれも、このアプリケーションを起動する場所を決定するために使用されません。

ゾーンの指定を含むその他のアクション

少なくとも1つのサテライトゾーンを作成した後、ホスト接続を追加するか、カタログを作成する際にゾーンを指定できます。

通常、プライマリゾーンがデフォルトです。Machine Creation Services™を使用してカタログを作成する場合、ホスト接続用に構成されたゾーンが自動的に選択されます。

サイトにサテライトゾーンが含まれていない場合、プライマリゾーンが想定され、ゾーン選択ボックスは表示されません。

モニター

管理者およびヘルプデスク担当者は、さまざまな機能とツールを使用してCitrix Virtual Apps and Desktops™サイトを監視できます。これらのツールを使用して、以下を監視できます。

- ユーザーセッションとセッションの使用状況
- ログオンパフォーマンス
- 接続とマシン（障害を含む）
- 負荷評価
- 履歴トレンド
- インフラストラクチャ

Citrix Director (シトリックス ディレクター)

Directorは、監視、トラブルシューティング、およびエンドユーザーのサポートタスクの実行に使用できるリアルタイムのWebツールです。

詳細については、Director の記事を参照してください。

構成ログ

構成ログを使用すると、管理者はサイトへの管理変更を追跡できます。構成ログは、構成変更が行われた後の問題の診断とトラブルシューティング、変更管理と構成の追跡を支援し、管理アクティビティを報告するのに役立ちます。

Studioからログに記録された情報のレポートを表示および生成できます。また、Directorでトレンドビューを使用してログに記録された項目を表示し、構成変更の通知を提供することもできます。この機能は、Studioにアクセスできない管理者にとって役立ちます。

トレンドビューは、一定期間にわたる構成変更の履歴データを提供するため、管理者はサイトに対してどのような変更がいつ誰によって行われたかを評価し、問題の原因を特定できます。このビューは、構成情報を次の3つのカテゴリに分類します。

- 接続障害
- 失敗したシングルセッションマシン

- 失敗したマルチセッションマシン

構成ログの有効化と構成方法の詳細については、構成ログを参照してください。Directorの記事では、そのツールからログに記録された情報を表示する方法について説明しています。

イベントログ

Citrix Virtual Apps and Desktops内のサービスは、発生したイベントをログに記録します。イベントログは、操作の監視とトラブルシューティングに使用されます。

詳細については、イベントログを参照してください。個々の機能に関する記事にも、イベント情報が含まれている場合があります。

構成ログ

構成ログは、サイト構成の変更と管理アクティビティをデータベースにキャプチャする機能です。この機能はデフォルトで有効になっています。ログに記録されたコンテンツは、次の目的で使用できます。

- 構成変更後、問題の診断とトラブルシューティングを行います。ログは追跡記録を提供します。
- 変更管理を支援し、構成を追跡します。
- 管理アクティビティを報告します。

Citrix Studioから、構成ログ設定の指定、構成ログの表示、HTMLおよびCSVレポートの生成を行うことができます。構成ログの表示は、日付範囲や全文検索結果でフィルタリングできます。強制ログが有効になっている場合、ログに記録できない構成変更は行えません。適切な権限があれば、構成ログからエントリを削除できます。構成ログ機能を使用してログコンテンツを編集することはできません。

構成ログは、PowerShell SDKと構成ログサービスを使用します。構成ログサービスは、サイト内のすべてのControllerで実行されます。いずれかのControllerが失敗した場合、別のControllerのサービスが自動的にログ要求を処理します。

デフォルトでは、構成ログ機能は有効になっており、サイト作成時に作成されるデータベース（サイト構成データベース）を使用します。データベースの別の場所を指定できます。構成ログデータベースは、サイト構成データベースと同じ高可用性機能をサポートしています。

構成ログへのアクセスは、委任管理を通じて、ログ設定の編集権限と構成ログの表示権限によって制御されます。

構成ログは作成時にローカライズされます。たとえば、英語で作成されたログは、リーダーのロケールに関係なく、英語で読み取られます。

ログに記録される内容

Studio、Director、およびPowerShellスクリプトから開始された構成変更と管理アクティビティがログに記録されます。ログに記録される構成変更の例には、以下に関する作業（作成、編集、削除、割り当て）が含まれます。

- マシンカタログ
- デリバリーグループ（電源管理設定の変更を含む）
- 管理者ロールとスコープ
- ホストリソースと接続
- Studioを介したCitrixポリシー

ログに記録される管理変更の例は次のとおりです。

- 仮想マシンまたはユーザーデスクトップの電源管理
- StudioまたはDirectorがユーザーにメッセージを送信する

次の操作はログに記録されません。

- 仮想マシンのプール管理電源投入などの自律的な操作。
- グループポリシー管理コンソール (GPMC) を介して実装されたポリシーアクション。これらのアクションのログを表示するには、Microsoft ツールを使用してください。
- レジストリ、データベースへの直接アクセス、または Studio、Director、PowerShell 以外のソースを介して行われた変更。
- 展開が初期化されると、最初の構成ログサービスインスタンスが構成サービスに登録されたときに、構成ログが利用可能になります。したがって、構成の初期段階はログに記録されません（たとえば、データベーススキーマが取得および適用されたとき、ハイパーバイザーが初期化されたときなど）。

構成ログの管理

デフォルトでは、構成ログはサイトの作成時に作成されるデータベース（サイト構成データベースとも呼ばれます）を使用します。Citrix は、以下の理由から、構成ログデータベース（および監視データベース）に別の場所を使用することを推奨します。

- 構成ログデータベースのバックアップ戦略は、サイト構成データベースのバックアップ戦略とは異なる可能性があります。
- 構成ログ（および監視サービス）のために収集されるデータ量によって、サイト構成データベースで利用可能な領域に悪影響が及ぶ可能性があります。
- これにより、3つのデータベースの単一障害点が分割されます。

構成ログをサポートしない製品エディションには、Studioにログノードがありません。

構成ログと強制ログの有効化と無効化

デフォルトでは、構成ログは有効になっており、強制ログは無効になっています。

1. Web Studioにサインインし、左ペインで**ログ**を選択します。
2. アクションバーで**設定**を選択します。構成ログダイアログボックスには、データベース情報が含まれており、構成ログと強制ログが有効か無効かを示します。
3. 目的のアクションを選択します。

   構成ログを有効にするには、**有効にする**を選択します。これはデフォルト設定です。データベースに書き込みできない場合、ログ情報は破棄されますが、操作は続行されます。

   構成ログを無効にするには、**無効にする**を選択します。以前にログが有効になっていた場合、既存のログはPowerShell SDKで読み取り可能です。

   強制ログを有効にするには、**データベースが利用できない場合にサイト構成の変更を防止する**を選択します。通常ログに記録される構成変更または管理アクティビティは、構成ログデータベースに書き込みできない限り許可されません。強制ログは、構成ログが有効になっている場合（**有効にする**が選択されている場合）にのみ有効にできます。構成ログサービスが失敗し、高可用性が使用されていない場合、強制ログが適用されます。このような場合、通常ログに記録される操作は実行されません。

   強制ログを無効にするには、**データベースが利用できない場合にサイト構成の変更を許可する**を選択します。構成ログデータベースにアクセスできない場合でも、構成変更と管理アクティビティは許可されます。これはデフォルト設定です。

構成ログデータベースの場所を変更する

強制ログが有効になっている場合、データベースの場所を変更することはできません。場所の変更には、ログに記録できない短い切断間隔が含まれるためです。

1. サポートされているSQL Serverバージョンを使用して、データベースサーバーを作成します。
2. Web Studioにサインインし、左ペインで**ログ**を選択します。

3. アクションバーで**設定**を選択します。
4. 「ログ設定」ダイアログボックスで、「**ログデータベースの変更**」を選択します。
5. 「ログデータベースの変更」ダイアログボックスで、新しいデータベースサーバーを含むサーバーの場所を指定します。有効な形式については、「データベースアドレス形式」を参照してください。
6. Studioでデータベースを作成するには、「**OK**」をクリックします。プロンプトが表示されたら「**OK**」をクリックすると、データベースが自動的に作成されます。Studioは、現在のStudioユーザーの資格情報を使用してデータベースへのアクセスを試行します。失敗した場合は、データベースユーザーの資格情報の入力を求められます。その後、Studioはデータベーススキーマをデータベースにアップロードします。（資格情報はデータベース作成中のみ保持されます。）
7. データベースを手動で作成するには、「**データベーススクリプトの生成**」をクリックします。生成されたスクリプトには、データベースを手動で作成するための手順が含まれています。スキーマをアップロードする前に、データベースが空であり、少なくとも1人のユーザーがデータベースにアクセスして変更する権限を持っていることを確認してください。

以前のデータベースの構成ログデータは、新しいデータベースにはインポートされません。ログを取得する際に、両方のデータベースからログを集約することはできません。新しい構成ログデータベースの最初のログエントリは、データベースの変更が発生したことを示しますが、以前のデータベースを特定するものではありません。

構成ログコンテンツの表示

構成変更や管理アクティビティを開始すると、StudioとDirectorによって作成された上位レベルの操作が、Studioの上部中央ペインに表示されます。上位レベルの操作は、1つ以上のサービスおよびSDK呼び出し（下位レベルの操作）をもたらします。上部ペインで上位レベルの操作を選択すると、下部ペインに下位レベルの操作が表示されます。

操作が完了する前に失敗した場合、ログ操作がデータベースで完了しない可能性があります。たとえば、開始レコードに対応する停止レコードがない場合があります。このような場合、ログには情報が欠落していることが示されます。時間範囲に基づいてログを表示すると、ログ内のデータが基準に一致する場合、不完全なログが表示されます。たとえば、過去5日間のすべてのログが要求され、過去5日間に開始時刻があるが終了時刻がないログが存在する場合、それは含まれます。

PowerShellコマンドレットを呼び出すスクリプトを使用する場合、親の上位レベルの操作を指定せずに下位レベルの操作を作成すると、構成ログは代替の上位レベルの操作を作成します。

構成ログコンテンツを表示するには、Studioナビゲーションペインで「**ログ**」を選択します。デフォルトでは、中央ペインにログコンテンツが日付ごとに区切られ、時系列順（最新のエントリが最初）に表示されます。次のことができます。

- 列ヘッダーで表示を並べ替えます。
- 日付間隔を指定するか、「**検索**」ボックスにテキストを入力して表示をフィルターします。検索を使用した後に標準表示に戻るには、「**検索**」ボックスのテキストをクリアします。
- テーブルの右上隅にある「**表示する列**」アイコンを選択して、表示する列を選択します。たとえば、管理者がWeb Studioにアクセスするために使用するIPアドレスを表示するには、アイコンをクリックして「**クライアントIP**」列を追加します。

レポートを生成する

構成ログデータを含むCSVおよびHTMLレポートを生成できます。

- CSVレポートには、指定された時間間隔のすべてのログデータが含まれます。データベース内の階層データは、単一のCSVテーブルにフラット化されます。データのどの側面もファイル内で優先されません。書式設定は使用されず、人間が読み取れることは想定されていません。ファイル（MyReportという名前）には、普遍的に利用可能な形式でデータが含まれています。CSVファイルは、データのアーカイブや、Microsoft Excelなどのレポート作成ツールまたはデータ操作ツールのデータソースとしてよく使用されます。
- HTMLレポートは、指定された時間間隔のログデータを人間が読み取れる形式で提供します。変更を確認するための構造化されたナビゲート可能なビューを提供します。HTMLレポートは、SummaryとDetailsという2つのファイルで構成されます。Summaryには、各操作がいつ、誰によって、どのような結果になったかなど、高レベルの操作が一覧表示されます。各操作の横にある**Details**リンクをクリックすると、Detailsファイル内の低レベルの操作に移動し、追加情報が表示されます。

構成ログレポートを生成するには、Studioナビゲーションペインで**Logging**を選択し、アクションバーで**Create custom report**を選択します。

- レポートの日付範囲を選択します。
- レポート形式（CSV、HTML、またはその両方）を選択します。
- レポートを保存する場所を参照します。

構成ログコンテンツを削除する

構成ログを削除するには、特定の委任管理権限とSQL Serverデータベース権限が必要です。

- **委任管理:** 展開構成の読み取りを許可する委任管理ロールが必要です。完全管理者ロールにはこの権限があります。カスタムロールには、 カテゴリで または が選択されている必要があります。

  構成ログデータを削除する前にバックアップを作成するには、カスタムロールで カテゴリの または も選択されている必要があります。

- **SQL Serverデータベース:** データベースからレコードを削除する権限を持つSQL Serverログインが必要です。これには2つの方法があります。

  - データベースサーバーで任意のアクティビティを実行できるsysadminサーバーロールを持つSQL Serverデータベースログインを使用します。または、`serveradmin`または`setupadmin`サーバーロールを使用すると、削除操作を実行できます。
  - 展開でより高いセキュリティが必要な場合は、データベースからレコードを削除する権限を持つデータベースユーザーにマッピングされた非sysadminデータベースログインを使用します。

    a. SQL Server Management Studioで、「sysadmin」以外のサーバーロールを持つSQL Serverログインを作成します。

    b. ログインをデータベース内のユーザーにマッピングします。SQL Serverは、ログインと同じ名前のユーザーをデータベースに自動的に作成します。

    c. データベースロールメンバーシップで、データベースユーザーのロールメンバーを少なくとも1つ指定します: `ConfigurationLoggingSchema_ROLE` または `dbowner`。

    詳細については、SQL Server Management Studioのドキュメントを参照してください。

構成ログを削除するには:

1. Web Studioにサインインし、左ペインで**ログ**を選択します。
2. アクションバーで**ログの削除**を選択します。
3. ログを削除する前にバックアップを作成するかどうかを尋ねられます。バックアップを作成することを選択した場合、バックアップアーカイブが保存される場所を参照します。バックアップはCSVファイルとして作成されます。

構成ログがクリアされた後、ログの削除は空のログに投稿される最初の活動となります。そのエントリには、誰がいつログを削除したかに関する詳細が記載されています。

APIおよびPowerShellログの表示

現在のセッション中に作成されたAPIリクエストを監視するには、**API**タブをクリックします。APIログは、Web Studioからサインアウトするとクリアされます。

その日に行ったUIアクションに対応するPowerShellコマンドを表示するには、**PowerShell**タブをクリックします。

構成ログにメタデータを関連付ける

`MetadataMap` と呼ばれる `name-value` ペアをログレコードに関連付けることで、構成ログにメタデータを添付できます。

> **注:**
>
> - メタデータは、高レベルの操作オブジェクトにのみ添付できます。
> - メタデータは、実行時に既存のレコードに関連付けられます。

メタデータを設定する

ログレコードを`MetadataMap`に関連付けるには、PowerShellコマンド`Set-LogHighLevelOperationMetadata`を実行します。 `Set-LogHighLevelOperationMetadata`は次のパラメータを受け取ります。

- **Id**: 上位レベルの操作のID。
- **InputObject**: メタデータを追加する上位レベルの操作。これは、上位レベルの操作オブジェクトまたはオブジェクトのリストがPowerShellコマンドに渡される`Id`パラメータの代替です。
- **Name**: 追加するメタデータのプロパティ名。このプロパティは、指定された上位レベルの操作に対して一意である必要があります。このプロパティには、次の文字を含めることはできません: ()\/;:#.*?=<>|'"。
- **Value**: プロパティの値。
- **Map**: プロパティの(名前、値)ペアの辞書。これは、`-Name`および`-Value`パラメータを使用してメタデータを設定する代替手段です。

例えば、ID 40のすべての高レベルログレコードにメタデータを添付するには、次のPowerShellコマンドを実行します。

```
Get-LogHighLevelOperation – Id 40 | Set-LogHighLevelOperationMetadata -Name A -Value B
```

ユーザー`abc@example.com`を持つ上位レベルのレコードにメタデータを添付するには、次のPowerShellコマンドを実行します。

```
Get-LogHighLevelOperation – User `abc@example.com` | Set-
LogHighLevelOperationMetadata -Name C -Value D
```

メタデータを使用して取得する

関連付けられたメタデータを使用してログレコードを取得するには、次のPowerShellコマンドを実行します。

- キーと値で検索:

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- 値で任意のキーを検索:

  ```
  Get-LogHighLevelOperation -Metadata "*:Value"
  ```

- キーと任意の値で検索:

  ```
  Get-LogHighLevelOperation -Metadata "Key:*"
  ```

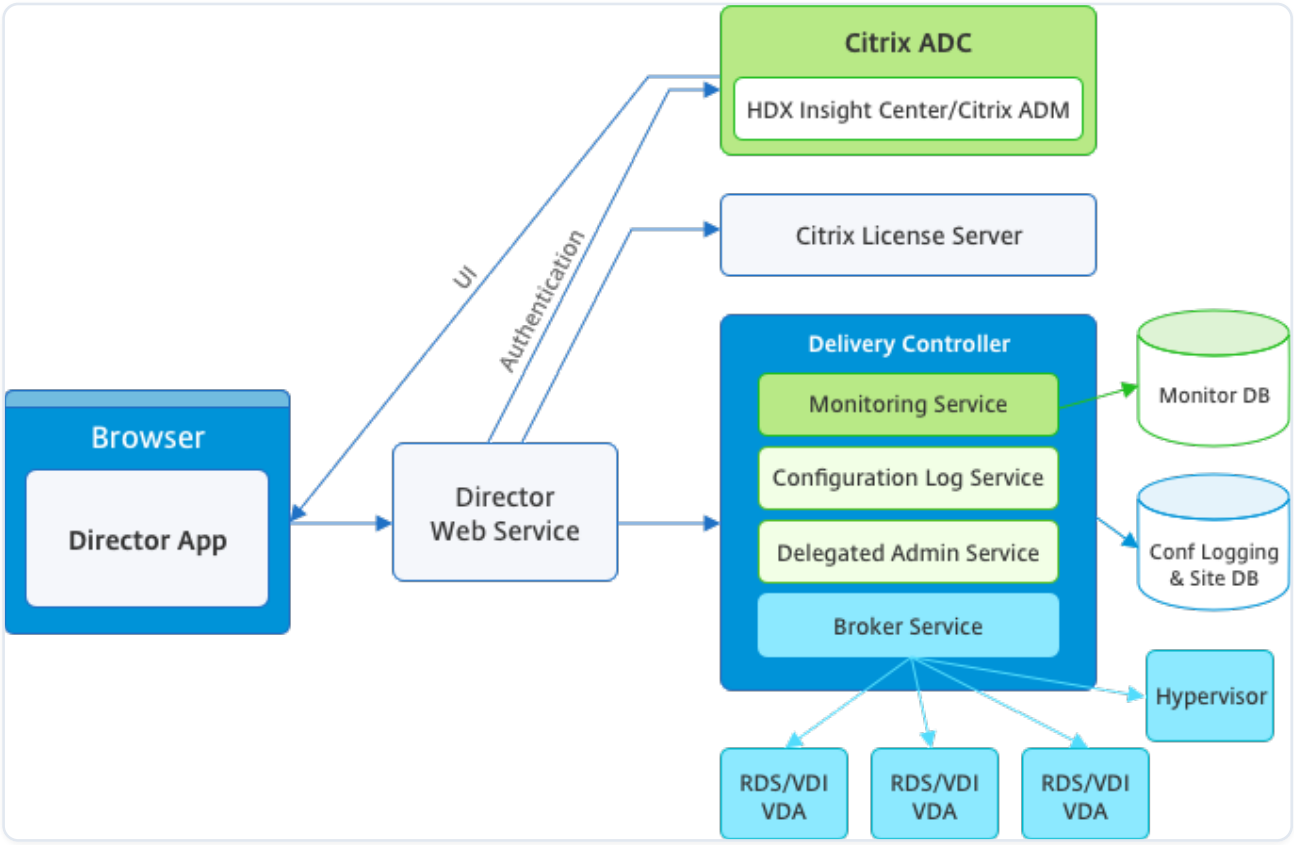
メタデータを削除する

関連付けられたメタデータを削除するには、PowerShell コマンド `Remove-LogHighLevelOperationMetadata` を実行します。 `Remove-LogHighLevelOperationMetadata` は次のパラメーターを受け取ります:

- **Id**: 上位レベルの操作のID。
- **InputObject**: メタデータを追加する上位レベルの操作。これは、上位レベルの操作オブジェクトまたはオブジェクトのリストがPowerShellコマンドに渡される`Id``パラメーターの代替です。
- **Name**: 削除するメタデータのプロパティ名。指定されたオブジェクトのすべてのメタデータを削除するには、$nullに設定します。
- **Map**: プロパティの(名前、値)ペアの辞書。これは、ハッシュテーブル (@{"name1" = "val1"; "name2" = "val2"} で作成) または文字列辞書 (new-object "System.Collections.Generic.Dictionary" で作成) のいずれかです。マップ内のキーと名前が一致するプロパティは削除されます。

ディレクター

Directorは、Citrix Virtual Apps and Desktopsの監視およびトラブルシューティングコンソールです。



Directorは以下にアクセスできます:

- Analytics、Performance Manager、およびNetwork Inspectorと統合された統合コンソールを使用して、Broker Agentからのリアルタイムデータ。Citrix Virtual Apps™またはDesktops環境におけるネットワークに起因するボトルネックを特定するために、以下の分析がCitrix ADMによって提供されます:
  - 健全性と容量保証のためのパフォーマンス管理
  - 履歴傾向とネットワーク分析
- Configuration Loggingデータベースにアクセスするための、Monitorデータベースに保存されている履歴データ。
- Citrix ADMを使用したCitrix GatewayからのICA®データ。

- Citrix Virtual AppsまたはDesktopsの仮想アプリケーション、デスクトップ、およびユーザーのエンドユーザーエクスペリエンスの可視性を得る。
- 効果的なトラブルシューティングのために、ネットワークデータをアプリケーションデータおよびリアルタイムメトリックと関連付ける。
- Citrix Virtual Desktop 7 Director監視ツールと統合する。

Directorは、Citrix Virtual AppsまたはDesktopsサイトのリアルタイムおよび履歴の健全性監視を提供するトラブルシューティングダッシュボードを使用します。この機能により、リアルタイムで障害を確認でき、エンドユーザーが何を経験しているかをよりよく把握できます。

Director機能とDelivery Controller (DC)、VDA、およびその他の依存コンポーネントとの互換性に関する詳細については、機能互換性マトリックスを参照してください。

> **注:**
>
> MeltdownおよびSpectreの投機的実行サイドチャネル脆弱性の開示に伴い、Citrixは関連する緩和パッチをインストールすることを推奨します。これらのパッチはSQL Serverのパフォーマンスに影響を与える可能性があります。詳細については、Microsoftサポート記事「Protect SQL Server from attacks on Spectre and Meltdown side-channel vulnerabilities」を参照してください。Citrixは、実稼働環境にパッチを展開する前に、規模をテストし、ワークロードを計画することを推奨します。

> Directorは、デフォルトでDelivery Controller上のWebサイトとしてインストールされます。前提条件およびその他の詳細については、本リリースのシステム要件ドキュメントを参照してください。Directorのインストールと構成に関する具体的な情報については、Directorのインストールと構成を参照してください。

Directorへのログオン

Director の Web サイトは、https または `http://<Server FQDN>/Director` にあります。

マルチサイト展開でいずれかのサイトがダウンしている場合、ダウンしているサイトへの接続を試みるため、ログオンに少し時間がかかります。

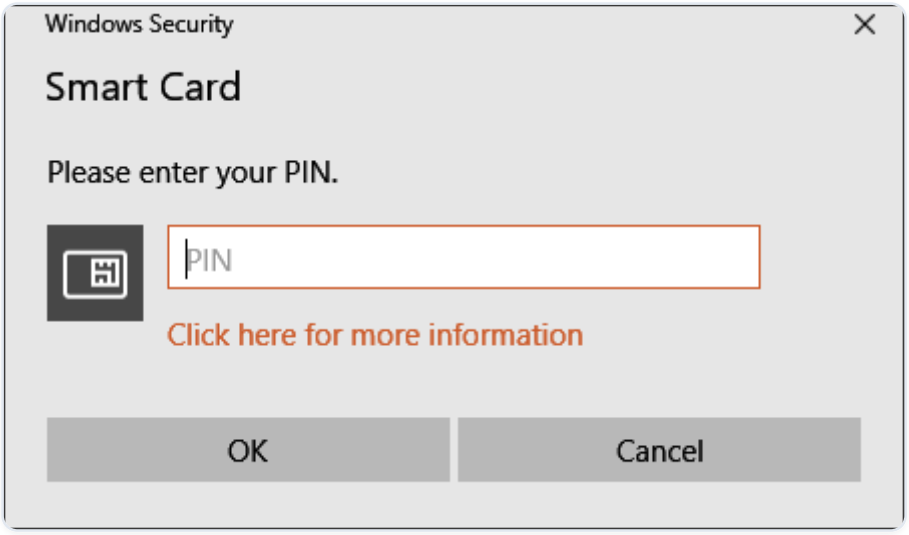
PIV スマートカード認証での Director の使用

Directorは、Personal Identity Verification (PIV) ベースのスマートカード認証によるログオンをサポートするようになりました。この機能は、アクセス制御にスマートカードベースの認証を使用する組織や政府機関にとって役立ちます。 スマートカード認証には、Directorサーバーおよび Active Directoryでの特定の構成が必要です。構成手順の詳細は、PIVスマートカード認証の構成に記載されています。

> **注:**
>
> スマートカード認証は、同じ Active Directory ドメインのユーザーのみがサポートされます。

必要な構成を実行した後、スマートカードを使用して Director にログオンできます。

1. スマートカードをスマートカードリーダーに挿入します。
2. ブラウザを開き、DirectorのURL `https://<directorfqdn>/Director` にアクセスします。
3. 表示されたリストから有効なユーザー証明書を選択します。
4. スマートカードトークンを入力します。



5. 認証後、Directorログオンページで追加の資格情報を入力することなく、Directorにアクセスできます。

統合 Windows 認証での Director の使用

統合Windows認証 (IWA) を使用すると、ドメイン参加ユーザーは、Directorログオンページで資格情報を再入力することなく、Directorに直接アクセスできます。統合Windows認証とDirectorを使用するための前提条件は次のとおりです。

- DirectorをホストするIIS Webサイトで統合Windows認証を有効にします。Directorをインストールすると、匿名認証とフォーム認証が有効になります。統合Windows認証とDirectorをサポートするには、匿名認証を無効にし、Windows認証を有効にします。ドメイン外のユーザーの認証のために、フォーム認証は有効のままにしておく必要があります。

  a. IISマネージャーを起動します。
  b. **サイト** \> **既定のWebサイト** \> **Director**に移動します。
  c. **認証**を選択します。
  d. **匿名認証**を右クリックし、**無効**を選択します。
  e. **Windows認証**を右クリックし、**有効**を選択します。

Windows認証 (/en-us/citrix-virtual-apps-desktops/2407/media/windowsauth.png)

- Directorマシンに対するActive Directory委任権限を構成します。この構成は、DirectorとDelivery Controller™が別々のマシンにインストールされている場合にのみ必要です。

  a. Active Directoryマシンで、Active Directory管理コンソールを開きます。
  b. Active Directory管理コンソールで、**ドメイン名** \> **コンピューター** に移動します。Directorマシンを選択します。
  c. 右クリックして **プロパティ** を選択します。
  d. プロパティで、**委任** タブを選択します。
  e. オプション「**このコンピューターを任意のサービスへの委任に信頼する (Kerberos のみ)**」を選択します。

- Directorへのアクセスに使用するブラウザーは、統合Windows認証をサポートしている必要があります。FirefoxおよびChromeでは、追加の構成手順が必要になる場合があります。詳しくは、ブラウザーのドキュメントを参照してください。
- 監視サービスは、Microsoft .NET Framework 4.5.1以降の、Directorのシステム要件に記載されているサポート対象バージョンを実行している必要があります。詳しくは、「システム要件」を参照してください。

ユーザーがDirectorからログオフするか、セッションがタイムアウトすると、ログオンページが表示されます。ログオンページから、ユーザーは認証の種類を「**自動ログオン**」または「**ユーザー資格情報**」に設定できます。

インターフェイスビュー

Directorは、特定の管理者に合わせて調整されたさまざまなインターフェイスビューを提供します。製品の権限によって、表示される内容と利用可能なコマンドが決まります。

たとえば、ヘルプデスク管理者は、ヘルプデスクタスクに合わせて調整されたインターフェイスを表示します。Directorを使用すると、ヘルプデスク管理者は、問題を報告しているユーザーを検索し、そのユーザーに関連するアクティビティを表示できます。たとえば、ユーザーのアプリケーションとプロセスのステータスなどです。応答しないアプリケーションやプロセスを終了する、ユーザーのマシンでの操作をシャドウする、マシンを再起動する、ユーザープロファイルをリセットするなどの操作を実行することで、問題を迅速に解決できます。

対照的に、完全な管理者はサイト全体を表示および管理し、複数のユーザーとマシンに対してコマンドを実行できます。ダッシュボードは、セッションのステータス、ユーザーログオン、サイトインフラストラクチャなど、展開の主要な側面を概観できます。情報は毎分更新されます。問題が発生した場合、発生した障害の数と種類に関する詳細が自動的に表示されます。

Directorにおけるさまざまな役割とその権限について詳しくは、「委任管理とDirector」を参照してください。

Pendoによる使用状況データの収集

Directorのインストール後、DirectorサービスはPendoを使用して使用状況データの収集を開始します。トレンドページの使用状況に関する統計情報とOData API呼び出し分析が収集されます。分析データの収集は、Citrixプライバシーポリシーに準拠しています。Directorをインストールすると、データ収集はデフォルトで有効になります。

Pendoのデータ収集をオプトアウトするには、Directorがインストールされているマシンのレジストリキーを編集します。レジストリキーが存在しない場合は、作成して目的の値に設定します。レジストリキーの値を変更した後、Directorインスタンスを更新してください。

注意： レジストリエディターを誤って使用すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターの使用

は、お客様ご自身の責任において行ってください。Citrixは、変更を行う前にWindowsレジストリをバックアップすることをお勧めします。

場所：HKEY_LOCAL_MACHINE\Software\Citrix\Director

名前：DisableGoogleAnalytics

> **注:**
>
> 以前、Director Service は Google Analytics を使用してデータを収集していました。現在、同じレジストリキーが Pendo に使用されています。
>
> 値：0 = 有効（デフォルト）、1 = 無効

Pendoによるデータ収集を無効にするには、次のPowerShellコマンドレットを使用できます。

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

新機能ガイド

Director には、Director の現在のバージョンでリリースされた新機能に関する洞察を提供する Pendo を使用した製品内ガイドがあります。適切な製品内メッセージと組み合わせた簡単な概要は、製品の新機能を理解するのに役立ちます。

この機能をオプトアウトするには、Director がインストールされているマシンで、以下に説明するようにレジストリキーを編集します。レジストリキーが存在しない場合は、作成して目的の値に設定します。レジストリキーの値を変更した後、Director インスタンスを更新します。

> **注意:**
>
> レジストリエディターを誤って使用すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix は、レジストリエディターの誤った使用によって発生した問題が解決できることを保証できません。レジストリエ

> ディターの使用は自己責任で行ってください。Citrix は、Windows レジストリを変更する前にバックアップすることをお勧めします。

> 場所: HKEY_LOCAL_MACHINE\Software\Citrix\Director

名前: DisableGuidedHelp

値: 0 = 有効（デフォルト）、1 = 無効

製品内ガイドを無効にするには、次のPowerShellコマンドレットを使用できます。

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
-PropertyType DWORD -Value 1
```

参照記事

- Citrix DirectorからのMTTRの削減
- Citrix Director - PowerShellによるアラートと通知の管理と構成
- Citrix Virtual Apps and Desktops開発者向けドキュメント

関連製品の新機能

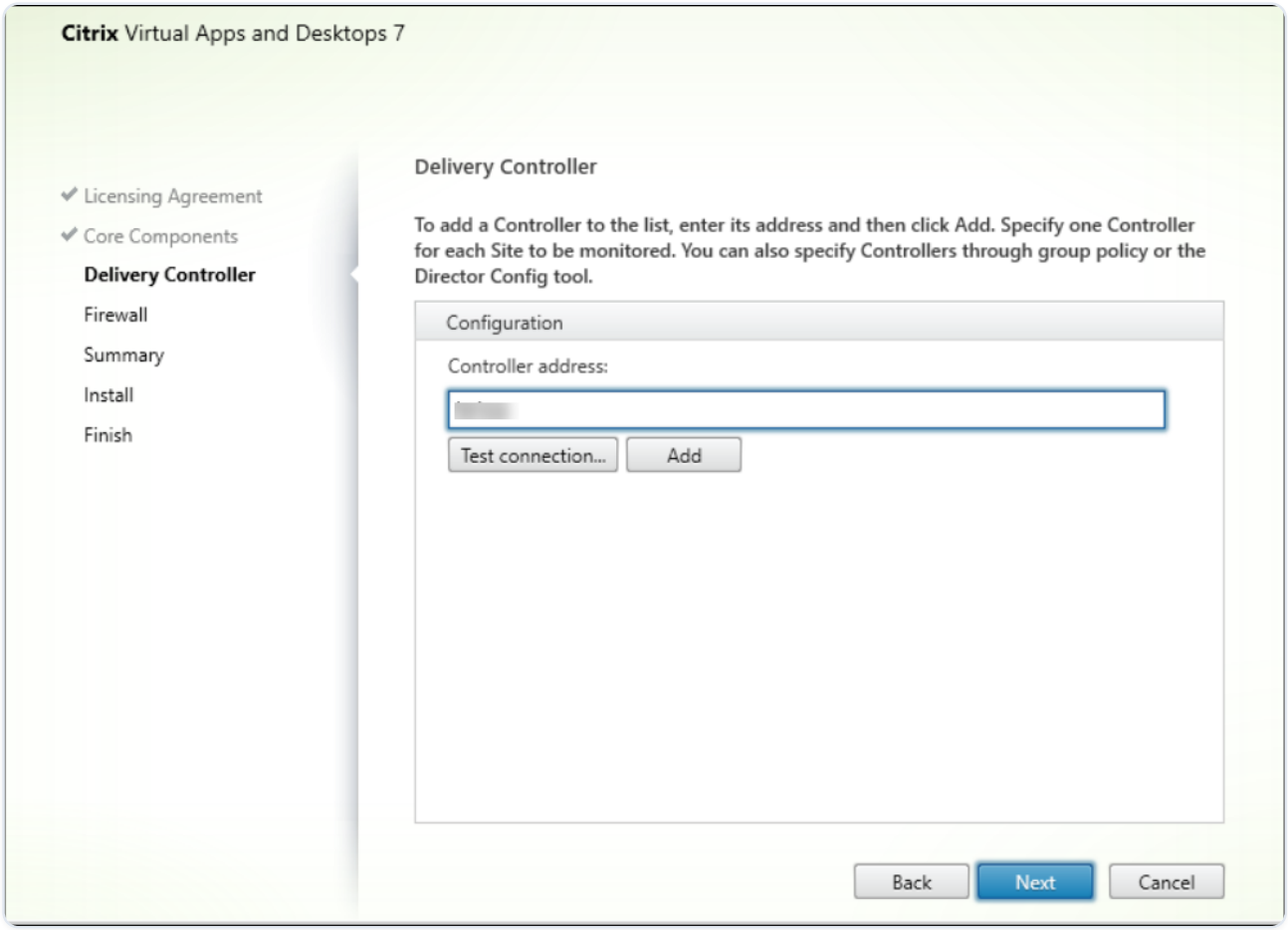
- 「シトリックス DaaS」(/ja-jp/citrix-daas/whats-new)
- StoreFront
- 「セキュアプライベートアクセス」(/ja-jp/citrix-secure-private-access/service/citrix-secure-private-access-whats-new)
- 「シトリックス エンタープライズ ブラウザ」(/ja-jp/citrix-enterprise-browser/whats-new)
- 「シトリックス ワークスペース」(/ja-jp/citrix-workspace/whats-new)
- 「プロビジョニング」(/ja-jp/provisioning/2402-ltsr/whats-new)

インストールと構成

Directorのインストール

Citrix Virtual Apps and Desktopsのフル製品ISOインストーラーを使用してDirectorをインストールします。これにより、前提条件の確認、不足しているコンポーネントのインストール、Director Webサイトのセットアップ、および基本的な構成が実行されます。前提条件およびその他の詳細については、このリリースのシステム要件ドキュメントを参照してください。このリリースのDirectorは、6.5より前のVirtual Apps展開または7より前のVirtual Desktops展開とは互換性がありません。 ISOインストーラーによって提供されるデフォルト構成は、一般的な展開に対応します。インストール時にDirectorが含まれていなかった場合は、ISOインストーラーを使用してDirectorを追加します。追加のコンポーネントを追加するには、ISOインストーラーを再実行し、インストールするコンポーネントを選択します。ISOインストーラーの使用方法については、インストールドキュメントのコアコンポーネントのインストールを参照してください。Citrixでは、.MSIファイルではなく、フル製品ISOインストーラーのみを使用してインストールすることをお勧めします。

DirectorがControllerにインストールされている場合、サーバーアドレスとしてlocalhostが自動的に構成され、Directorはデフォルトでローカルcontrollerと通信します。Controllerから離れた専用サーバーにDirectorをインストールする場合は、ControllerのFQDNまたはIPアドレスを入力するよう求められます。



注:

監視するControllerを追加するには、**［追加］**をクリックします。

Directorは、デフォルトで指定されたControllerと通信します。監視するサイトごとにControllerアドレスを1つだけ指定してください。Directorは、同じサイト内の他のすべてのControllerを自動的に検出し、指定したControllerが失敗した場合は、それらの他のControllerにフォールバックします。

注:

DirectorはController間で負荷分散を行いません。

ブラウザーとWebサーバー間の通信を保護するために、Citrix®はDirectorをホストするIIS WebサイトでTLSを実装することをお勧めします。手順については、Microsoft IISのドキュメントを参照してください。TLSを有効にするためにDirectorの構成は必要ありません。

Directorの展開と構成

複数のサイトを含む環境でDirectorを使用する場合は、Controller、Director、およびその他のコアコンポーネントがインストールされているすべてのサーバーでシステムクロックを同期してください。そうしないと、Directorでサイトが正しく表示されない可能性があります。

重要:

ネットワーク経由でプレーンテキストで送信されるユーザー名とパスワードのセキュリティを保護するため、Director接続にはHTTPではなくHTTPSのみを使用してください。特定のツールは、HTTP（暗号化されていない）ネットワークパケット内のプレーンテキストのユーザー名とパスワードを読み取ることができ、ユーザーにとって潜在的なセキュリティリスクを生じさせる可能性があります。

権限の構成

Directorにログオンするには、Directorの権限を持つ管理者はActive Directoryドメインユーザーである必要があり、以下の権限が必要です。

- 検索対象となるすべてのActive Directoryフォレストでの読み取り権限 (「(/ja-jp/citrix-virtual-apps-desktops/2407/director/install-and-configure/advanced-configuration.html)」を参照)。
- 構成済みの委任管理者ロール (「(/ja-jp/citrix-virtual-apps-desktops/2407/director/install-and-configure/permissions.html)」を参照)。
- ユーザーをシャドウするには、管理者はWindowsリモートアシスタンス用のMicrosoftグループポリシーを使用して構成する必要があります。さらに、:
  - VDAをインストールする際、すべてのユーザーデバイスでWindowsリモートアシスタンス機能が有効になっていることを確認してください (デフォルトで選択されています)。
  - サーバーにDirectorをインストールする場合、Windowsリモートアシスタンスがインストールされていることを確認してください (デフォルトで選択されています)。ただし、サーバーではデフォルトで無効になっています。Directorがエンドユーザーにアシスタンスを提供するために、この機能を有効にする必要はありません。Citrixは、サーバーのセキュリティを向上させるために、この機能を無効のままにしておくことを推奨します。
  - 管理者がWindowsリモートアシスタンスを開始できるようにするには、リモートアシスタンス用の適切なMicrosoftグループポリシー設定を使用して、必要な権限を付与します。詳細については、CTX127388: Desktop Directorでリモートアシスタンスを有効にする方法を参照してください。

高度な構成

Director は、ユーザー、Delivery Controller (DC)、VDA、および Director が異なるフォレストに配置されているフォレスト構成にまたがるマルチフォレスト環境をサポートできます。これには、フォレスト間の信頼関係と構成設定の適切なセットアップが必要です。

マルチフォレスト環境での推奨構成

推奨される構成では、ドメイン全体の認証を使用して、フォレスト間で送信および受信フォレスト信頼関係を作成する必要があります。

マルチフォレストサイト構成の図(/en-us/citrix-virtual-apps-desktops/2407/media/multiforest-config.png)

Director からの信頼関係により、異なるフォレストにあるユーザーセッション、VDA、および Delivery Controller の問題をトラブルシューティングできます。

Director が複数のフォレストをサポートするために必要な高度な構成は、Internet Information Services (IIS) マネージャーで定義された設定によって制御されます。

> **重要:**
>
> IIS で設定を変更すると、Director サービスは自動的に再起動し、ユーザーをログオフします。

IIS を使用して高度な設定を構成するには:

1. Internet Information Services (IIS) マネージャーコンソールを開きます。
2. デフォルトの Web サイトの下にある Director Web サイトに移動します。
3. **アプリケーション設定**をダブルクリックします。
4. 設定をダブルクリックして編集します。
5. 新しい設定を追加するには、**追加**をクリックします。

Director は Active Directory を使用してユーザーを検索し、ユーザーとマシンの詳細情報を参照します。デフォルトでは、Director は次のドメインまたはフォレストを検索します。

- 管理者アカウントがメンバーです。
- Director Webサーバーがメンバーです（異なる場合）。

Directorは、Active Directoryグローバルカタログを使用してフォレストレベルで検索を実行しようとします。フォレストレベルで検索する権限がない場合、ドメインのみが検索されます。

別のActive Directoryドメインまたはフォレストからデータを検索または参照するには、検索するドメインまたはフォレストを明示的に設定する必要があります。IISマネージャーで、Director Webサイトに次のアプリケーション設定を構成します。

```
Connector.ActiveDirectory.Domains = (user),(server)
```

値属性のuserとserverは、それぞれDirectorユーザー（管理者）とDirectorサーバーのドメインを表します。

追加のドメインまたはフォレストからの検索を有効にするには、この例に示すように、ドメイン名をリストに追加します。

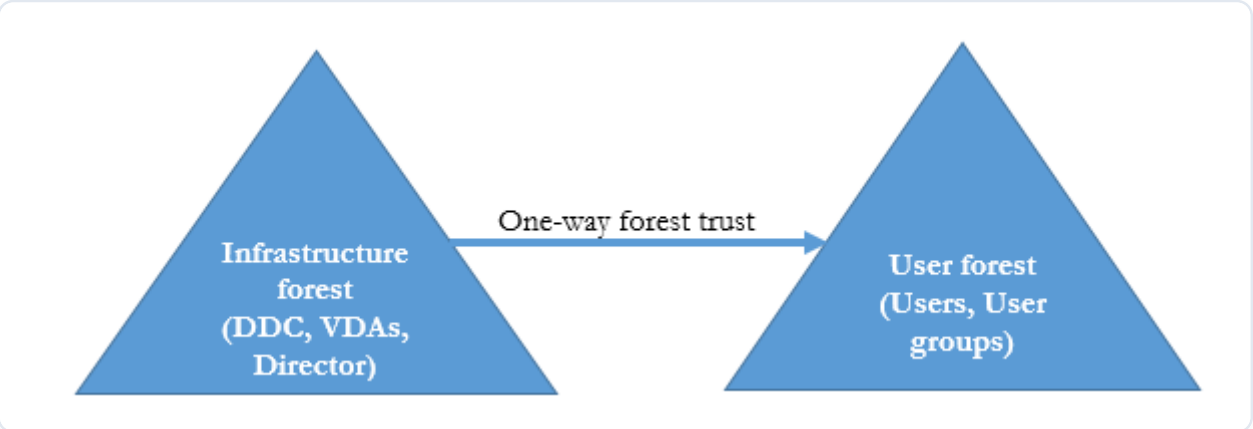
```
Connector.ActiveDirectory.Domains = (user),(server),\&lt;domain1\>,
\&lt;domain2\>
```

リスト内の各ドメインについて、Directorはフォレストレベルで検索を実行しようとします。フォレストレベルで検索する権限がない場合、ドメインのみが検索されます。

ドメインローカルグループの構成

ほとんどの Citrix Service Provider (CSP) は、インフラストラクチャフォレストに VDA、DC、および Director を含む同様の環境設定を持っています。ユーザーまたはユーザーグループのレコードは顧客フォレストに属します。インフラストラクチャフォレストから顧客フォレストへの一方向の送信信頼が存在します。

CSP 管理者は通常、インフラストラクチャフォレストにドメインローカルグループを作成し、顧客フォレストのユーザーまたはユーザーグループをこのドメインローカルグループに追加します。



Director はこのようなマルチフォレスト設定をサポートし、ドメインローカルグループを使用して構成されたユーザーのセッションを監視できます。

1. IISマネージャーで、Director Webサイトに次のアプリケーション設定を追加します。

   ```
   Connector.ActiveDirectory.DomainLocalGroupSearch= true



   DomainLocalGroupSearchDomains= \&lt;domain1\>,\&lt;domain2\>
   ```

   \<domain1\>\<domain2\> は、ドメインローカルグループが存在するフォレストの名前です。

2. ドメインローカルグループをWeb Studioのデリバリーグループに割り当てます。
3. IISを再起動し、変更を有効にするためにDirectorに再度ログオンします。これで、Directorはこれらのユーザーのセッションを監視し、表示できるようになります。

Directorにサイトを追加する

Directorがすでにインストールされている場合は、複数のサイトで動作するように構成します。構成するには、各DirectorサーバーでIISマネージャーコンソールを使用して、アプリケーション設定のサーバーアドレスリストを更新します。

各サイトのコントローラーのアドレスを次の設定に追加します。

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
```

SiteAControllerとSiteBControllerは、2つの異なるサイトのDelivery Controllerのアドレスです。

アクティビティマネージャーで実行中のアプリケーションの可視性を無効にする

デフォルトでは、Directorのアクティビティマネージャーは、ユーザーセッションのすべての実行中のアプリケーションのリストを表示します。この情報は、Directorのアクティビティマネージャー機能にアクセスできるすべての管理者が表示できます。委任された管理者ロールの場合、これにはフル管理者、デリバリーグループ管理者、およびヘルプデスク管理者が含まれます。

ユーザーのプライバシーと実行中のアプリケーションを保護するために、**アプリケーション**タブを無効にして、実行中のアプリケーションを一覧表示しないようにすることができます。

警告:

レジストリを誤って編集すると、オペレーティングシステムを再インストールする必要があるような深刻な問題が発生する可能性があります。Citrix® は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証しません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

1. VDAで、HKEY_LOCAL_MACHINE\\Software\\Citrix\\Director\\TaskManagerDataDisplayedにあるレジストリキーを変更します。デフォルトでは、このキーは1に設定されています。値を0に変更すると、VDAから情報が収集されなくなり、アクティビティマネージャーに表示されなくなります。
2. Directorがインストールされているサーバーで、実行中のアプリケーションの表示を制御する設定を変更します。デフォルトでは、値は「true」であり、アプリケーションタブで実行中のアプリケーションの表示が許可されます。値を「false」に変更すると、表示が無効になります。このオプションは、VDAではなく、Directorのアクティビティマネージャーのみに影響します。 次の設定の値を変更します。 UI.TaskManager.EnableApplications = false

重要:

実行中のアプリケーションの表示を無効にするには、Activity Managerにデータが表示されないように両方の変更を行います。

PIVスマートカード認証を構成する

この記事では、スマートカード認証機能を有効にするためにDirectorサーバーとActive Directoryで必要な構成について説明します。

注:

スマートカード認証は、同じActive Directoryドメインのユーザーのみがサポートされます。

Directorサーバーの構成

Directorサーバーで次の構成手順を実行します。

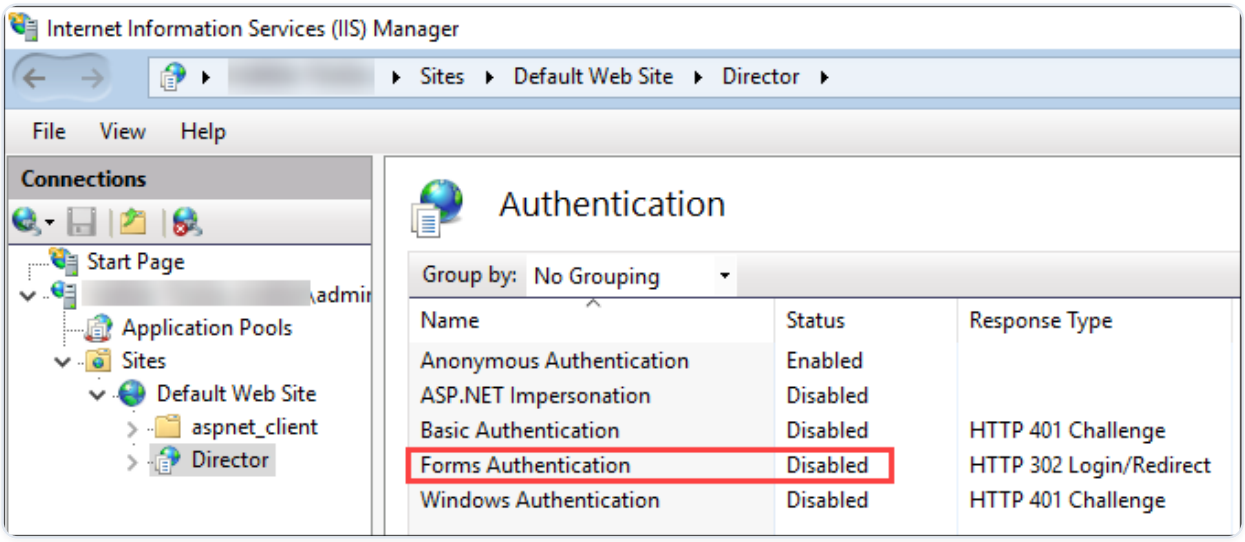
1. クライアント証明書マッピング認証をインストールして有効にします。Microsoftドキュメント「クライアント証明書マッピング認証」の**Active Directory を使用したクライアント証明書マッピング認証**の手順に従ってください。
2. Directorサイトでフォーム認証を無効にします。

   IISマネージャーを起動します。

   サイト \> **既定の Web サイト** \> **Director**に移動します。

   認証 を選択します。

   フォーム認証を右クリックし、**無効にする**を選択します。



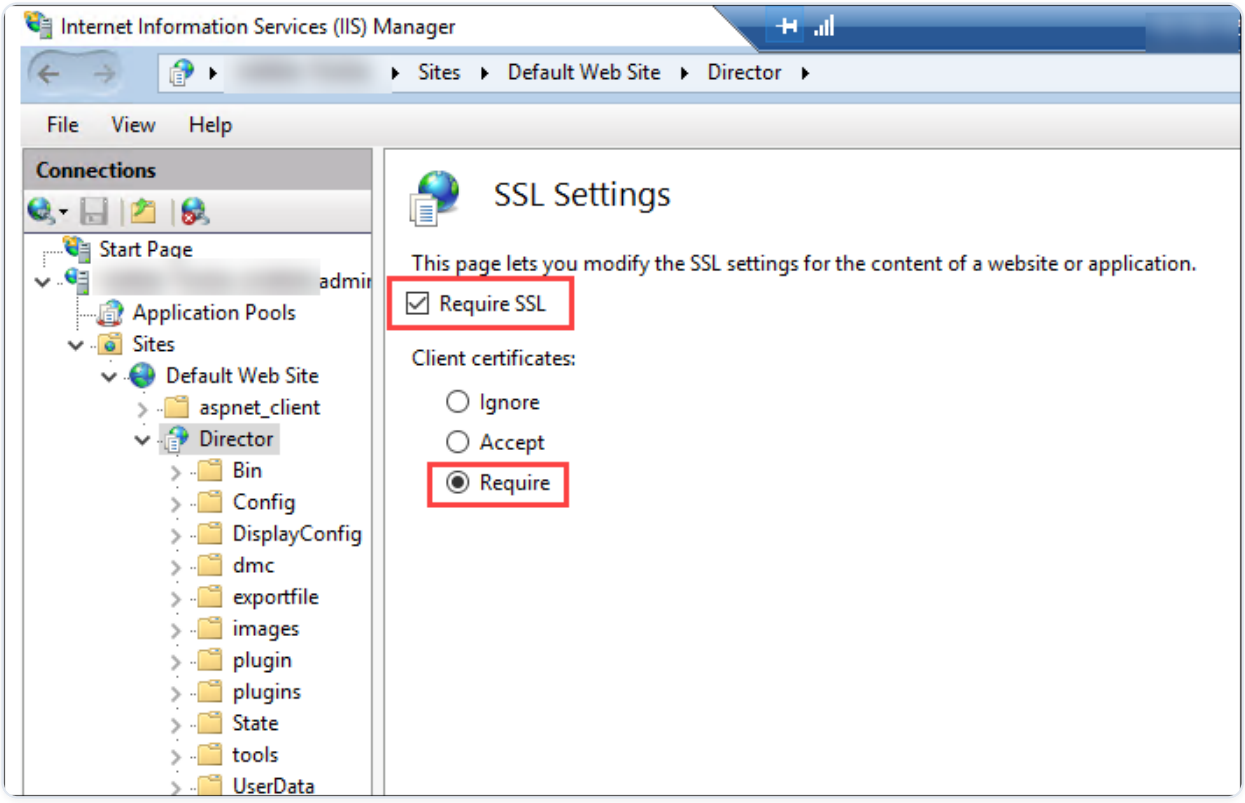
3. クライアント証明書認証のために、Director URLをより安全なHTTPSプロトコル（HTTPの代わりに）に構成します。

   a. IISマネージャーを起動します。

   b. **サイト** > **既定のWebサイト** > **Director** に移動します。

   c. **SSL設定** を選択します。

   d. **SSLを要求** と **クライアント証明書** \> **要求** を選択します。



4. web.configを更新します。テキストエディターを使用してweb.configファイル（c:\\inetpub\\wwwroot\\Directorにあります）を開きます。

`<system.webServer>` 親要素の下に、次のスニペットを最初の子要素として追加します。

```
&lt;defaultDocument>

   &lt;files>

       &lt;add value="LogOn.aspx"/>

   &lt;/files>

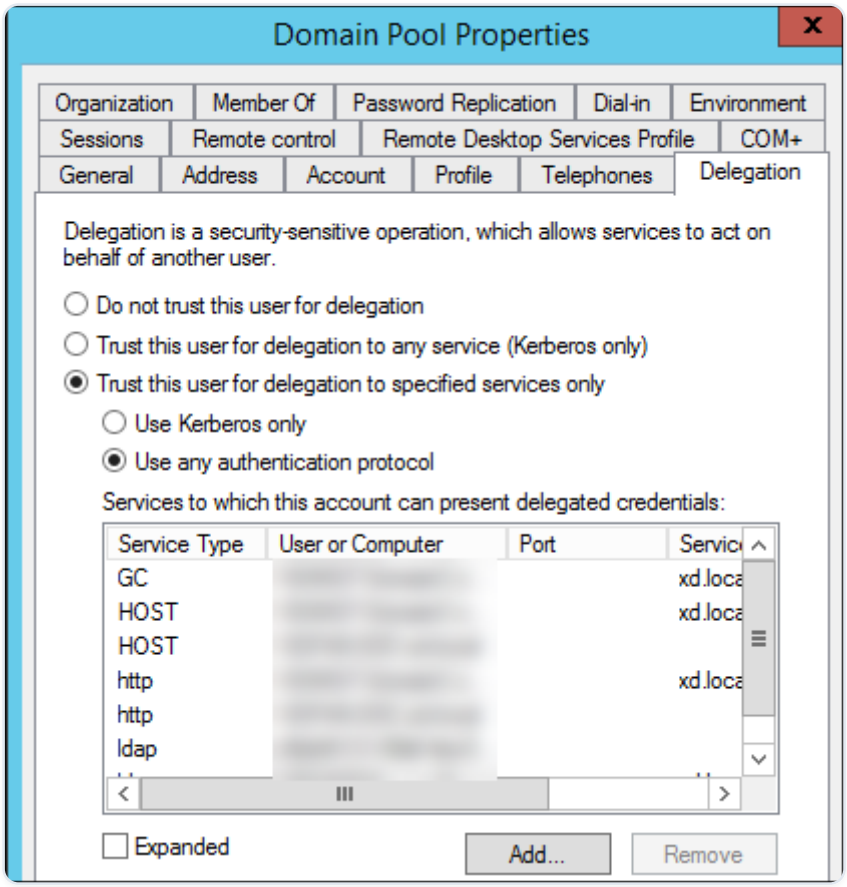
&lt;/defaultDocument>
```

Active Directoryの構成

デフォルトでは、Directorアプリケーションは **アプリケーションプール** のIDプロパティで実行されます。スマートカード認証には委任が必要であり、DirectorアプリケーションIDはサービスホスト上でTrusted Computing Base（TCB）権限を持っている必要があります。

Citrixでは、アプリケーションプールID用に個別のサービスアカウントを作成することをお勧めします。Microsoft MSDNの記事「Protocol Transition with Constrained Delegation Technical Supplement」の手順に従って、サービスアカウントを作成し、TCB権限を割り当ててください。

新しく作成したサービスアカウントを Director アプリケーションプールに割り当てます。次の図は、サンプルサービスアカウント「Domain Pool」のプロパティダイアログを示しています。



このアカウントに対して、次のサービスを構成します:

- デリバリーコントローラー™: HOST, HTTP
- ディレクター: HOST, HTTP
- アクティブディレクトリ：GC、LDAP

構成するには、,

1. ユーザーアカウントのプロパティダイアログで、**追加**をクリックします。
2. **サービスの追加**ダイアログで、ユーザーまたはコンピューターをクリックします。
3. Delivery Controllerのホスト名を選択します。
4. **利用可能なサービス**リストから、HOSTとHTTPの**サービスの種類**を選択します。

サービスを構成する(/en-us/citrix-virtual-apps-desktops/2407/media/dir-smartcard-config4.png)

同様に、**Director**および**Active Directory**ホストのサービスの種類を追加します。

サービスプリンシパル名レコードを作成する

各Directorサーバーと、Directorサーバーのプールへのアクセスに使用されるロードバランシングされた仮想IP（VIP）ごとにサービスアカウントを作成する必要があります。新しく作成された

サービスアカウントへの委任を構成するには、サービスプリンシパル名（SPN）レコードを作成する必要があります。

- DirectorサーバーのSPNレコードを作成するには、次のコマンドを使用します。

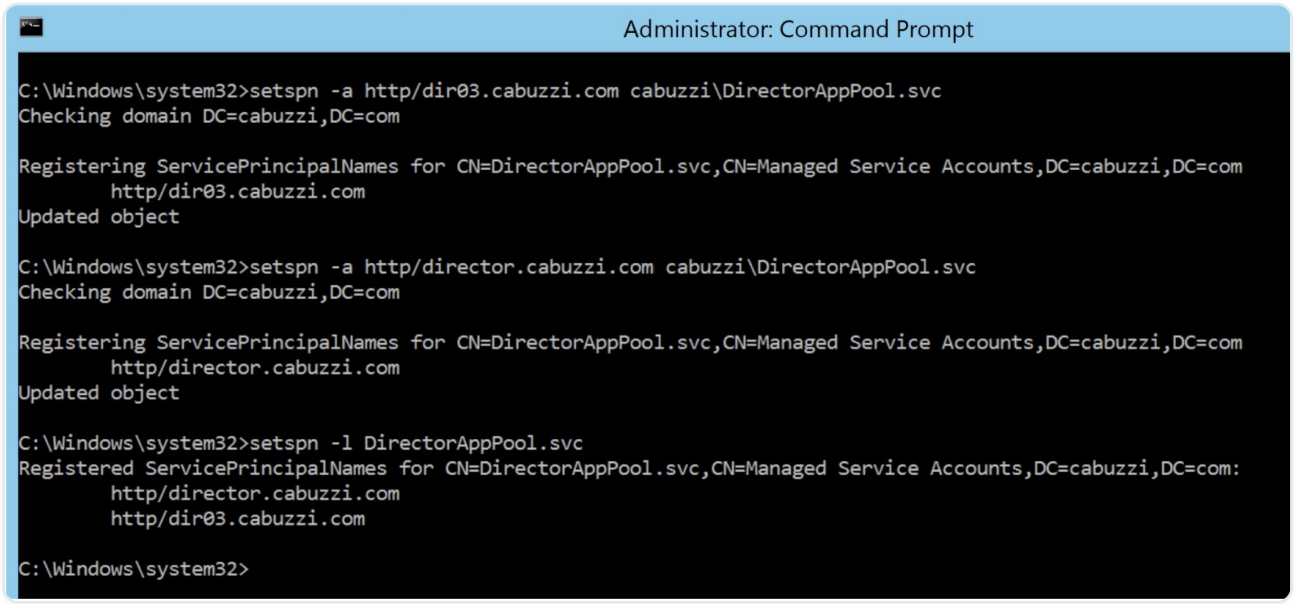
```
  setspn -a http/<directorServer>.<domain_fqdn>
<domain>\<DirectorAppPoolServiceAcct>
```

- ロードバランシングされたVIPのSPNレコードを作成するには、次のコマンドを使用します。

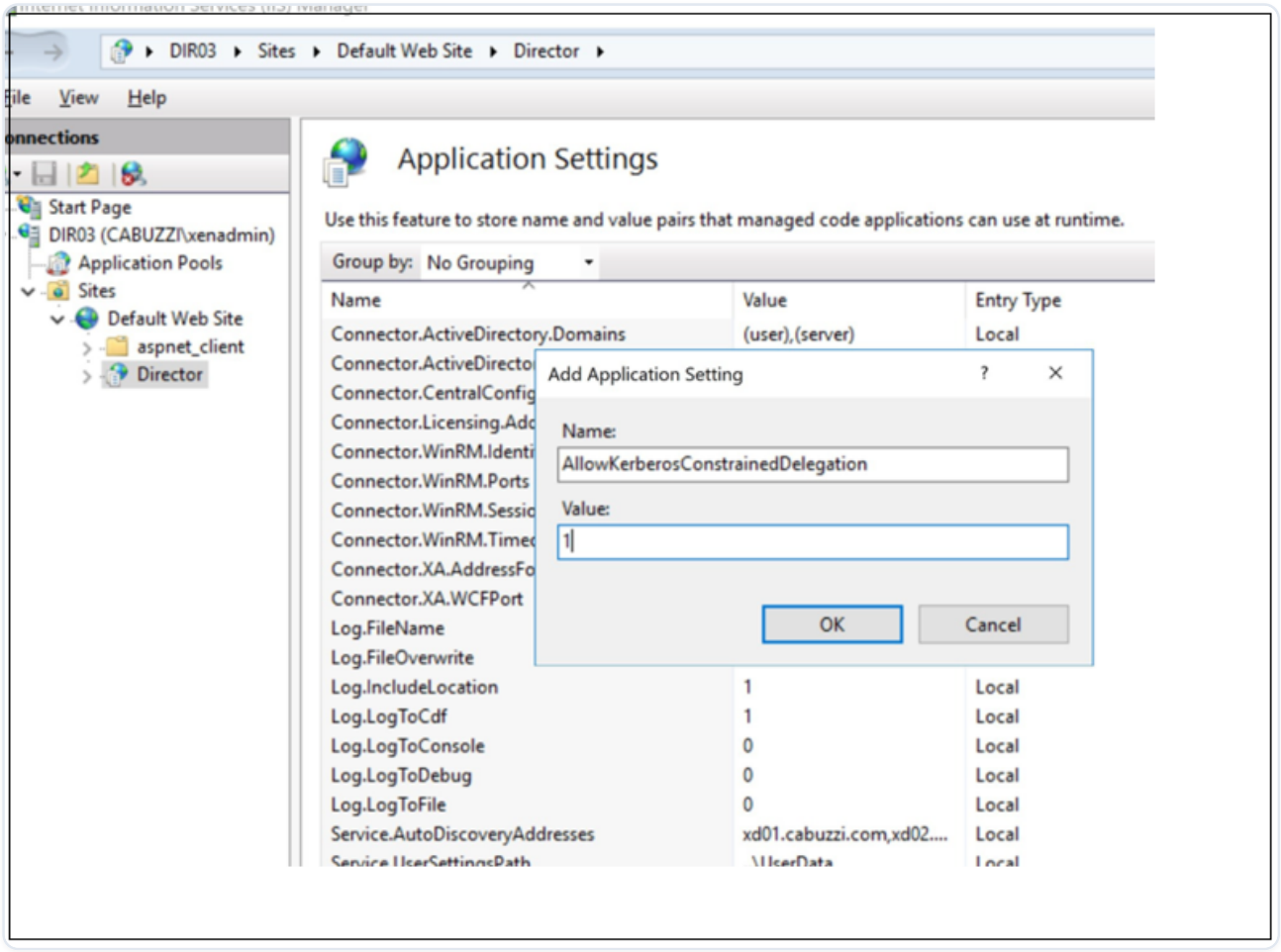
```
  setspn -S http/<DirectorFQDN> <domain>\<DirectorAppPoolServiceAcct>
```

- 作成されたSPNを表示またはテストするには、次のコマンドを使用します。

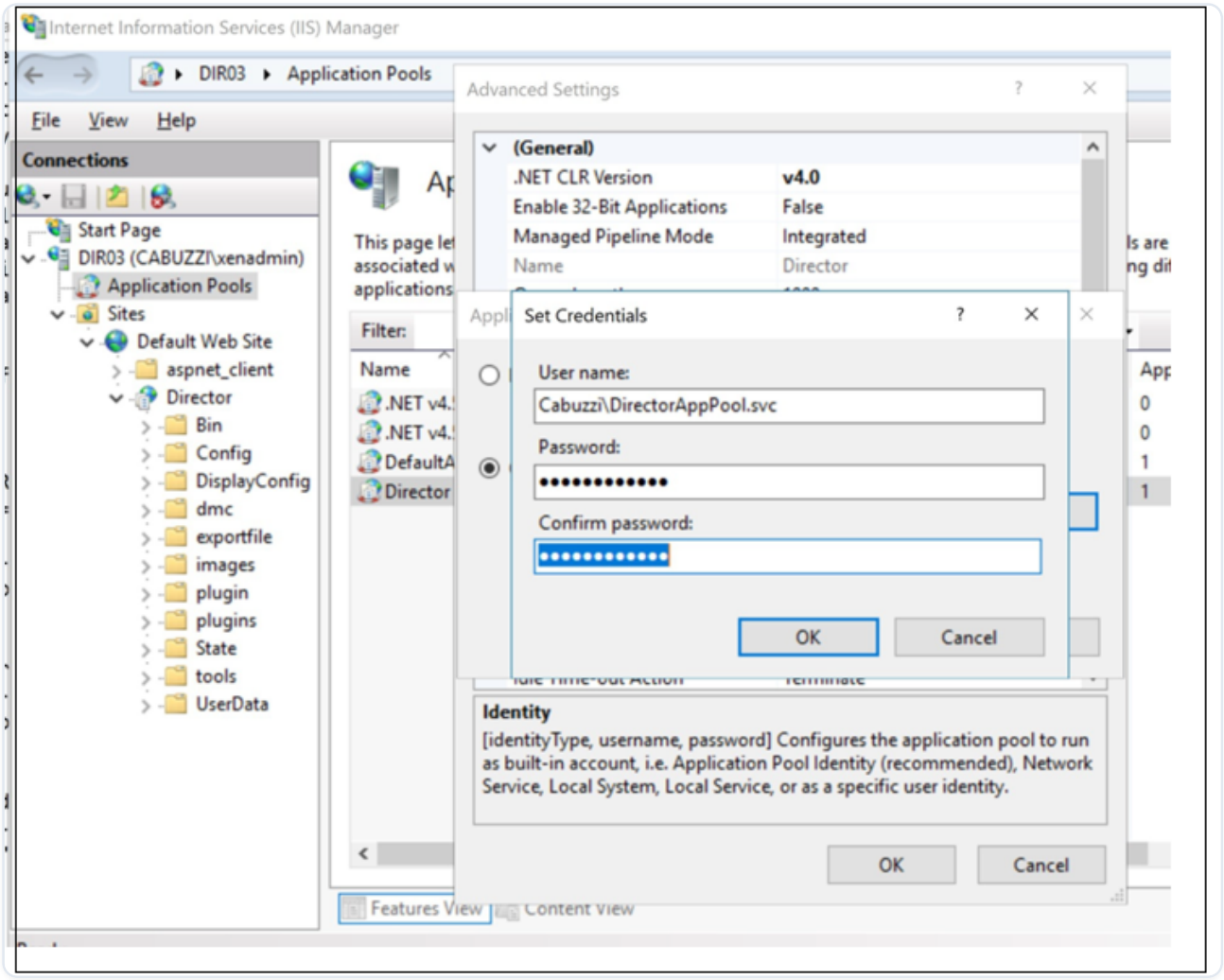
```
  setspn –l <DirectorAppPoolServiceAcct>
```



- 左ペインでDirector仮想ディレクトリを選択し、**アプリケーション設定**をダブルクリックします。アプリケーション設定ウィンドウ内で、**追加**をクリックし、**AllowKerberosConstrainedDelegation**が1に設定されていることを確認します。



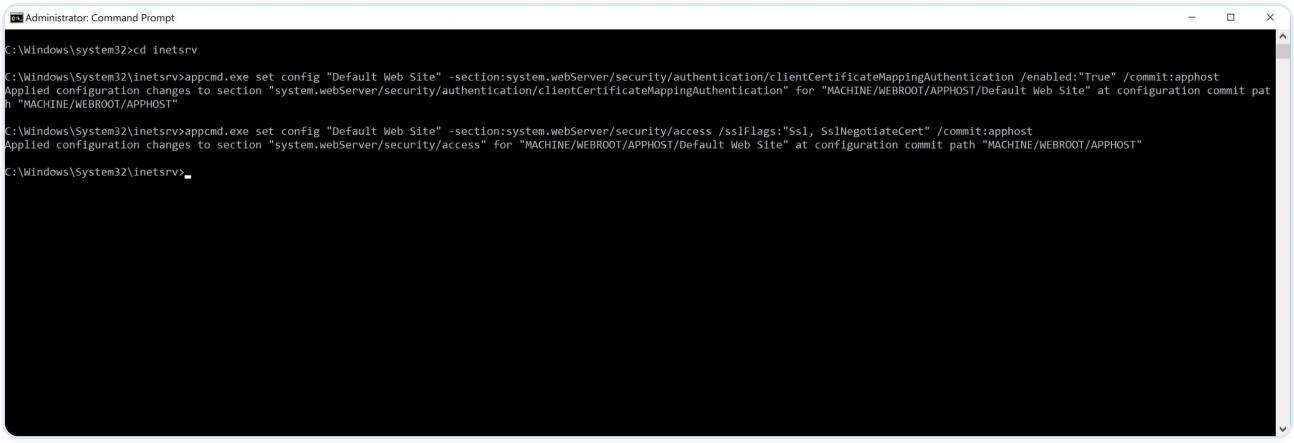
- 左側のペインで「**アプリケーションプール**」を選択し、Directorアプリケーションプールを右クリックして「**詳細設定**」を選択します。
- 「**ID**」を選択し、省略記号（「…」）をクリックしてサービスアカウントのドメイン\ログオンとパスワードの資格情報を入力します。IISコンソールを閉じます。



- 管理者として実行したコマンドプロンプトから、ディレクトリを C:\Windows\System32\inetsrv に変更し、次のコマンドを入力します。

```
   appcmd.exe set config “Default Web Site” -section:system.webServer/
security/authentication/clientCertificateMappingAuthentication /
enabled:”True” /commit:apphost
```

```
    appcmd.exe set config “Default Web Site” -section:system.webServer/
security/access /sslFlags:”Ssl, SslNegotiateCert” /commit:apphost
```



Firefoxブラウザーの構成

Firefoxブラウザーを使用するには、OpenSC 0.17.0で入手可能なPIVドライバーをインストールします。インストールと構成の手順については、FirefoxでのOpenSC PKCS#11モジュールのインストール、ステップバイステップを参照してください。 Directorでのスマートカード認証機能の使用方法については、Directorの記事の「PIVベースのスマートカード認証でDirectorを使用する」セクションを参照してください。

ネットワーク分析の構成

> **注：** この機能の利用可否は、組織のライセンスと管理者権限によって異なります。

> DirectorはCitrix ADMと統合され、ネットワーク分析とパフォーマンス管理を提供します。

- ネットワーク分析は、Citrix ADMからのHDX™ Insightレポートを使用して、ネットワークのアプリケーションおよびデスクトップのコンテキストビューを提供します。この機能により、Directorは展開におけるICAトラフィックの高度な分析を提供します。
- パフォーマンス管理は、履歴保持とトレンドレポートを提供します。リアルタイム評価と比較したデータの履歴保持により、容量や健全性のトレンドを含むトレンドレポートを作成できます。

Directorでこの機能を有効にすると、HDX InsightレポートはDirectorに追加情報を提供します。

- トレンドページの「ネットワーク」タブには、展開全体におけるアプリケーション、デスクトップ、ユーザーの遅延と帯域幅の影響が表示されます。
- 「ユーザーの詳細」ページには、特定のユーザーセッションに固有の遅延と帯域幅の情報が表示されます。

制限事項:

- ビューでは、バージョン7より前のVDAのHDX接続ログオンデータは収集されません。それ以前のVDAの場合、グラフデータは0として表示されます。

ネットワーク分析を有効にするには、DirectorにCitrix ADMをインストールして構成する必要があります。Directorには、Citrix ADMバージョン11.1ビルド49.16以降が必要です。MASはXenServer上で動作する仮想アプライアンスです。ネットワーク分析を使用すると、Directorは展開に関連する情報を通信し、収集します。

詳しくは、Citrix ADMドキュメントを参照してください。

注:

Citrix NetScaler Insight Centerは、15 May 2018をもってメンテナンス終了日を迎えました。Citrix Product Matrixを参照してください。ネットワーク分析のためにDirectorをCitrix ADMと統合します。NetScaler Insight CenterからCitrix ADMへの移行については、「NetScaler Insight CenterからCitrix ADMへの移行」を参照してください。

1. Directorがインストールされているサーバーで、C:\\inetpub\\wwwroot\\Director\\toolsにあるDirectorConfigコマンドラインツールを見つけ、コマンドプロンプトからパラメーター/confignetscalerを指定して実行します。
2. プロンプトが表示されたら、Citrix ADMマシン名（FQDNまたはIPアドレス）、ユーザー名、パスワード、HTTPS接続タイプ（HTTPよりも推奨）を入力し、Citrix ADM統合を選択します。
3. 変更を確認するには、ログオフして再度ログオンします。

注:

セキュリティ上の理由から、HDX Insightのみにアクセスするための十分な権限を持つ、DirectorとのADM統合用のカスタムロールを作成することをお勧めします。

詳細については、アクセスポリシーの構成を参照してください。

委任管理とDirector

委任管理では、管理者、ロール、スコープという3つの概念を使用します。権限は、管理者のロールと、そのロールのスコープに基づいています。たとえば、管理者にヘルプデスク管理者ロールが割り当てられ、そのスコープが1つのサイトのエンドユーザーのみの責任を含む場合があります。

委任管理者の作成については、メインの委任管理の記事を参照してください。

管理権限によって、管理者に表示されるDirectorインターフェイスと、実行できるタスクが決まります。権限によって以下が決定されます。

- 管理者がアクセスできるビュー（総称してビューと呼ばれます）。
- 管理者が表示および操作できるデスクトップ、マシン、およびセッション。
- 管理者が実行できるコマンド（ユーザーセッションのシャドウやメンテナンスモードの有効化など）。

組み込みのロールと権限によっても、管理者がDirectorをどのように使用するかが決定されます。

管理者ロール	DIRECTORでの権限
フル管理者	すべてのビューにフルアクセスでき、ユーザーセッションのシャドウ、メンテナンスモードの有効化、トレンドデータのエクスポートを含むすべてのコマンドを実行できます。
デリバリーグループ管理者	すべてのビューにフルアクセスでき、ユーザーセッションのシャドウ、電源管理とセッション管理、メンテナンスモードの有効化、トレンドデータのエクスポートを含むすべてのコマンドを実行できます。
読み取り専用管理者	指定されたスコープ内のすべてのビューにアクセスし、すべてのオブジェクトとグローバル情報を表示できます。HDX™チャネルからレポートをダウンロードしたり、トレンドビューの「エクスポート」オプションを使用してトレンドデータをエクスポートしたりできます。その他のコマンドを実行したり、ビュー内の何かを変更したりすることはできません。
ヘルプデスク管理者	ヘルプデスクビューとユーザー詳細ビューにのみアクセスでき、管理者が管理を委任されて

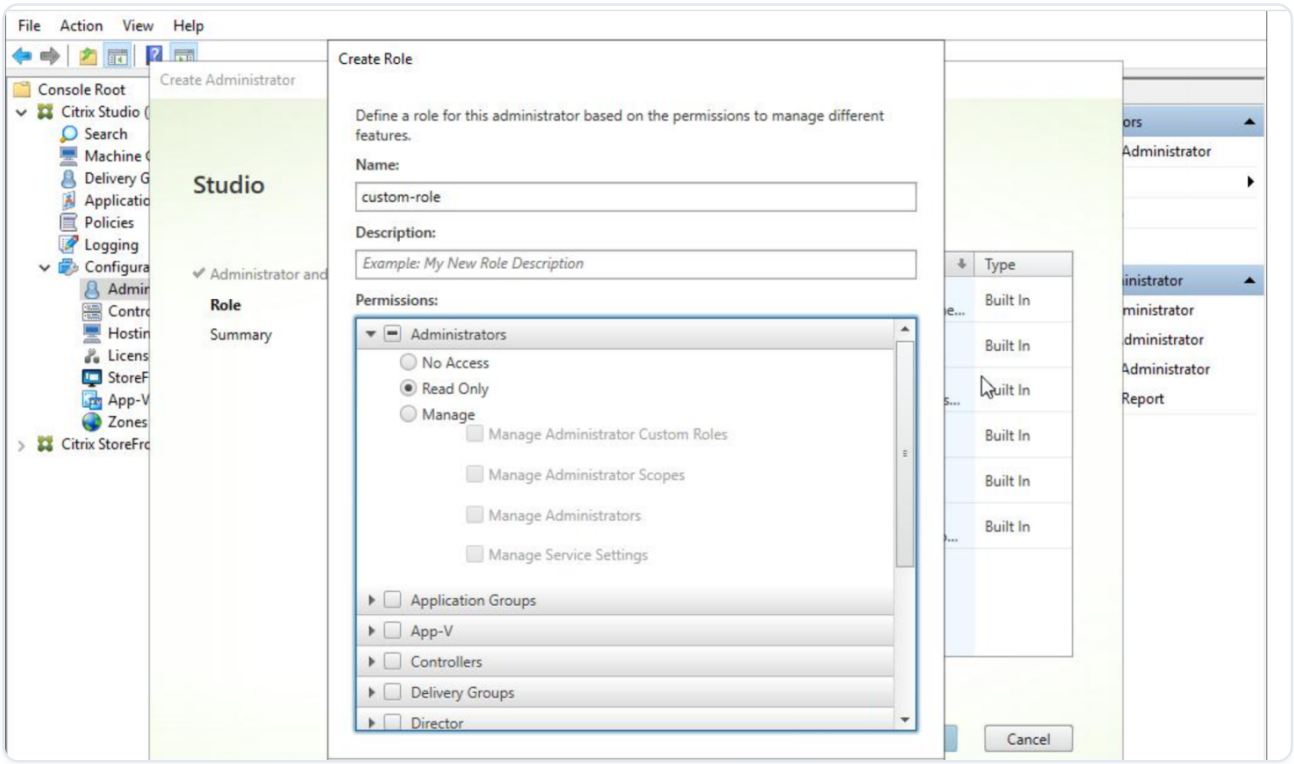
管理者ロール	DIRECTORでの権限
	いるオブジェクトのみを表示できます。ユーザーのセッションをシャドウし、そのユーザーに対してコマンドを実行できます。メンテナンスモード操作を実行できます。シングルセッションOSマシンに対して電源制御オプションを使用できます。ダッシュボード、トレンド、アラート、またはフィルタービューにはアクセスできません。マルチセッションOSマシンに対して電源制御オプションを使用することはできません。
マシンカタログ管理者	マシン詳細ページ（マシンベース検索）にのみアクセスできます。
ホスト管理者	アクセス不可。この管理者はDirectorではサポートされておらず、データを表示できません。

Director管理者用のカスタム役割を構成する

Studioでは、組織の要件により厳密に一致させ、より柔軟に権限を委任するために、Director固有のカスタムロールを構成することもできます。たとえば、組み込みのヘルプデスク管理者ロールを制限して、この管理者がセッションをログオフできないようにすることができます。

Director権限を持つカスタム役割を作成する場合、その役割に他の一般的な権限も付与する必要があります。

- Delivery Controller™ の Director にログオンするための権限 - 少なくとも管理者ノードでの読み取り専用アクセス
- Directorで配信グループに関連するデータを表示するための配信グループへの権限 - 少なくとも読み取り専用アクセス

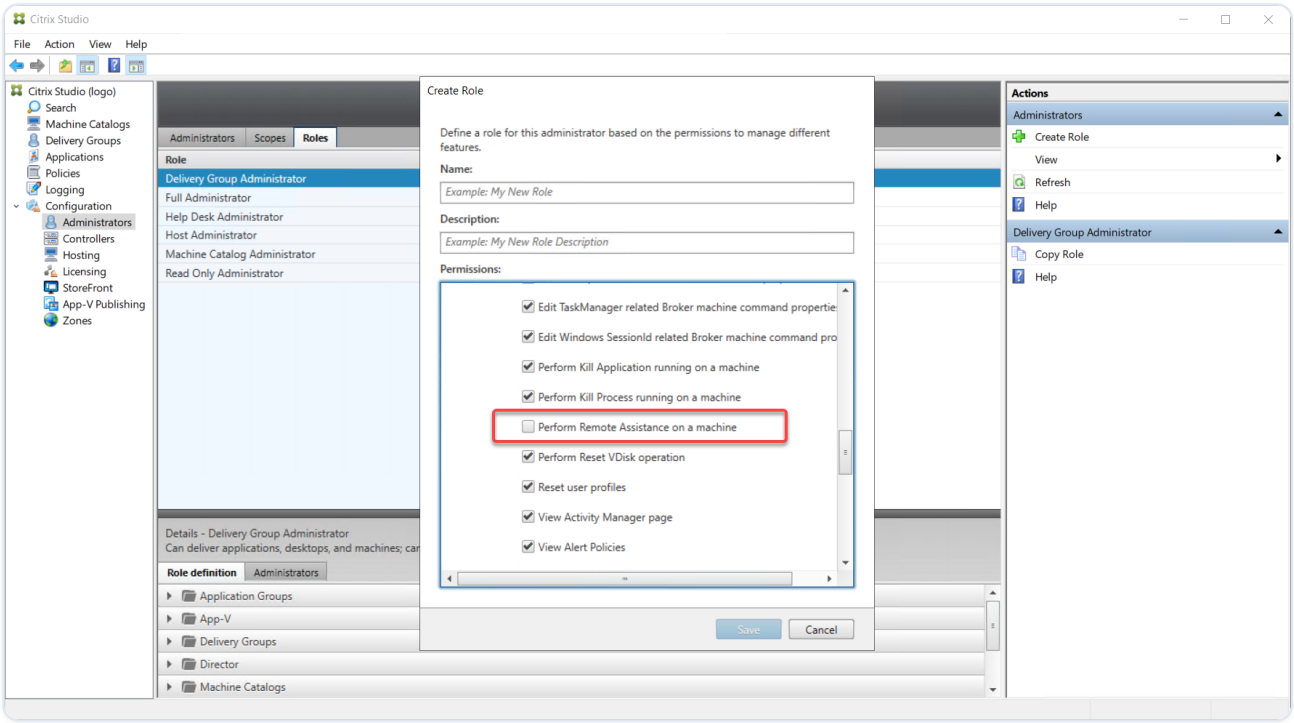


または、既存のロールをコピーして、異なるビューに対する追加の権限を含めることで、カスタムロールを作成できます。たとえば、ヘルプデスクロールをコピーし、ダッシュボードまたはフィルターページを表示する権限を含めることができます。

カスタムロールのDirector権限を選択します。これには以下が含まれます。

- マシン上で実行中のアプリケーションの強制終了を実行する
- マシン上で実行中のプロセスの強制終了を実行する
- マシン上でリモートアシスタンスを実行する
- ユーザープロファイルをリセットする
- クライアント詳細ページを表示
- ダッシュボードページの表示
- フィルターページを表示する
- マシン詳細ページを表示
- トレンドページの表示
- ユーザー詳細ページを表示

この例では、シャドウイング（マシン上でリモートアシスタンスを実行する）が無効になっています。



権限は、UIで適用可能になるために他の権限に依存する場合があります。たとえば、**マシンで実行中のアプリケーションを強制終了する**権限を選択すると、役割に権限があるパネルでのみ**アプリケーションの終了**機能が有効になります。次のパネル権限を選択できます。

- フィルターページを表示する
- ユーザー詳細ページを表示する
- 「マシン詳細」ページを表示
- 「クライアント詳細」ページを表示

さらに、他のコンポーネントの権限リストから、デリバリーグループの以下の権限を検討してください。

- デリバリーグループのメンバーシップを使用して、マシンのメンテナンスモードを有効/無効にする。
- デリバリーグループのメンバーシップを使用して、Windowsデスクトップマシンで電源操作を実行する。
- デリバリーグループのメンバーシップを使用して、マシンでセッション管理を実行する。

Directorのセキュアな展開

この記事では、Directorを展開および構成する際にシステムセキュリティに影響を与える可能性のある領域に焦点を当てています。

Microsoft インターネット インフォメーション サービス (IIS) の構成

制限されたIIS構成でDirectorを構成できます。

アプリケーションプールのリサイクル制限

以下のアプリケーションプールリサイクル制限を設定できます。

- 仮想メモリ制限: 4,294,967,295
- プライベートメモリ制限: StoreFront™サーバーの物理メモリのサイズ
- リクエスト制限: 4,000,000,000

ファイル名拡張子

リストにないファイル名拡張子を許可しないことができます。

Directorは、リクエストフィルタリングで次のファイル名拡張子を必要とします。

- .aspx 拡張子
- 「.css」
- .html 拡張子
- .js
- .pngファイル
- .svcファイル
- .gifファイル
- .jsonファイル
- .woffファイル
- .woff2ファイル
- .ttfファイル

Director では、要求フィルターで次の HTTP 動詞が必要です。リストにない動詞は許可しないことができます。

- GET
- POST
- HEAD

Director は以下を必要としません。

- ISAPIフィルター

- ISAPI拡張機能
- CGIプログラム
- FastCGIプログラム

> **重要:**
>
> - Director には完全な信頼が必要です。グローバルな .NET 信頼レベルを High 以下に設定しないでください。
> - Director は個別のアプリケーションプールを維持します。Director の設定を変更するには、Director サイトを選択して変更します。

ユーザー権限の構成

Directorがインストールされると、そのアプリケーションプールには以下が付与されます。

- **サービスとしてログオン**のログオン権限
- **プロセスに対するメモリクォータの調整**、**セキュリティ監査の生成**、および**プロセスレベルトークンの置き換え**の特権

言及されている権限と特権は、アプリケーションプールが作成される際の通常のインストール動作です。

これらのユーザー権限を変更する必要はありません。これらの特権は Director では使用されず、自動的に無効になります。

Directorの通信

実稼働環境では、Directorとサーバー間でやり取りされるデータを保護するために、インターネットプロトコルセキュリティ（IPsec）またはHTTPSプロトコルを使用してください。

IPsec は、インターネットプロトコルに対する標準拡張機能のセットであり、データの整合性とリプレイ保護を備えた認証済みで暗号化された通信を提供します。IPsec はネットワーク層プロトコルセットであるため、上位レベルのプロトコルは変更なしでこれを使用できます。HTTPS は、トランスポート層セキュリティ (TLS) プロトコルを使用して強力なデータ暗号化を提供します。

> **注:**

- Citrix®は、Directorコンソールへのアクセスをイントラネット内に制限することを強く推奨します。
- Citrixは、実稼働環境でDirectorへのセキュリティで保護されていない接続を有効にしないことを強く推奨します。
- Directorからの安全な通信には、接続ごとに個別の構成が必要です。
- SSLプロトコルは推奨されません。代わりに、より安全なTLSプロトコルを使用してください。
- IPsecではなくTLSを使用して、Citrix ADCとの通信を保護してください。

DirectorとCitrix Virtual Apps and Desktopsサーバー間の通信を保護するには（監視およびレポート用）、データアクセスセキュリティを参照してください。

DirectorとCitrix ADC間の通信を保護するには（Citrix Insight用）、ネットワーク分析の構成を参照してください。

Directorとライセンスサーバー間の通信を保護するには、ライセンス管理コンソールの保護を参照してください。

Directorのセキュリティ分離

Directorと同じWebドメイン（ドメイン名とポート）に任意のWebアプリケーションをデプロイできます。ただし、それらのWebアプリケーションにセキュリティリスクがあると、Director展開のセキュリティが低下する可能性があります。より高度なセキュリティ分離が必要な場合は、CitrixはDirectorを別のWebドメインに展開することを推奨します。

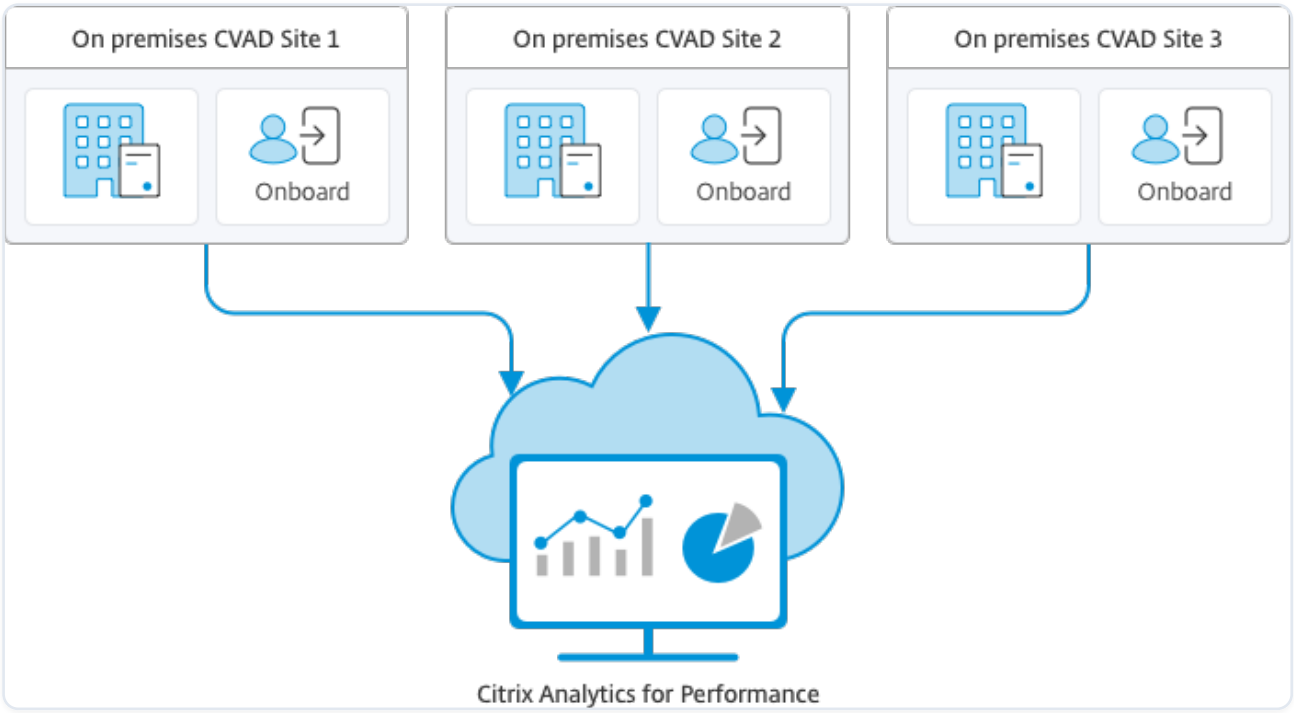
Citrix Analytics for Performance™ を使用したオンプレミスサイトの構成

Citrix Analytics for Performance (Performance Analytics) は、Citrix Analytics Cloud Service の包括的なパフォーマンス監視ソリューションです。Performance Analytics は、パフォーマンスメトリックに基づいて構築された高度なインサイトと分析を提供します。Performance Analytics を使用すると、組織内の1つ以上のCitrix Virtual Apps and Desktops™サイトの使用状況とパフォーマンスメトリックを監視および表示できます。

Performance Analyticsの詳細については、Performance Analyticsの記事を参照してください。

サイトから Citrix Cloud™ 上の Citrix Analytics for Performance にパフォーマンスデータを送信して、その高度なパフォーマンス分析機能を活用できます。Performance Analytics を表示および使

用するには、まず **Director** の **Analytics** タブからオンプレミスサイトを Citrix Analytics for Performance で構成する必要があります。



Performance Analyticsは安全な方法でデータにアクセスし、Citrix Cloudからオンプレミス環境にデータが転送されることはありません。

前提条件

DirectorからCitrix Analytics for Performanceを構成するために、新しいコンポーネントをインストールする必要はありません。次の要件が満たされていることを確認してください。

- Delivery ControllerとDirectorがバージョン1912 CU2以降であること。詳細については、機能互換性マトリックスを参照してください。

注:

- Delivery Controller で Microsoft .NET Framework のバージョン 4.8 より前のバージョンが実行されている場合、Director からオンプレミスサイトを Citrix Analytics for Performance で構成すると失敗する可能性があります。回避策として、Delivery Controller の .NET Framework をバージョン 4.8 にアップグレードしてください。LCM-9255。
- Citrix Virtual Apps and Desktops バージョン 2012 を実行しているオンプレミスサイトを Director から Citrix Analytics for Performance で構成すると、数時間後または Delivery Controller の Citrix Monitor Service の再起動後に構成が失敗する可能性があります。この

> 場合、Analytics タブには「未接続」ステータスが表示されます。回避策として、Delivery Controller のレジストリに Encryption フォルダーを作成します。場所: HKEY_LOCAL_MACHINE\Software\Citrix\XDservices\Monitor、フォルダー名: Encryption。CitrixMonitor アカウントが Encryption フォルダーに対してフルコントロールアクセス権を持っていることを確認してください。Citrix Monitor Service を再起動します。DIR-14324。

- この構成を実行するための**Analytics**タブへのアクセスは、フル管理者のみが利用できます。
- Performance Analyticsがパフォーマンスメトリックにアクセスできるようにするには、すべてのDelivery ControllerとDirectorがインストールされているマシンで、アウトバウンドインターネットアクセスが利用可能である必要があります。具体的には、次のURLへのアクセス可能性を確認してください。
  - Citrixキー登録: `https://*.citrixnetworkapi.net/`
  - シトリックス クラウド: `https://*.citrixworkspacesapi.net/`
  - シトリックス アナリティクス: `https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/` Delivery Controller および Director マシンがイントラネット内にあり、アウトバウンドインターネットアクセスがプロキシサーバー経由である場合は、以下を確認してください。
- プロキシサーバーは、上記の URL のリストを許可する必要があります。
- Director の web.config および citrix.monitor.exe.config ファイルに以下の構成を追加します。この構成は、必ず **configuration** タグ内に追加してください。

```
&lt;system.net>

    &lt;defaultProxy>

        &lt;proxy  usesystemdefault = "false"  proxyaddress = "http://
&lt;your_proxyserver_address>:80" bypassonlocal = "true"  />

    &lt;/defaultProxy>

&lt;/system.net>
```

  - Director の web.config は、Director がインストールされているマシン上の `C:\inetpub\wwwroot\Director\web.config` にあります。

- citrix.monitor.exe.config は、Delivery Controller がインストールされているマシン上の `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` にあります。

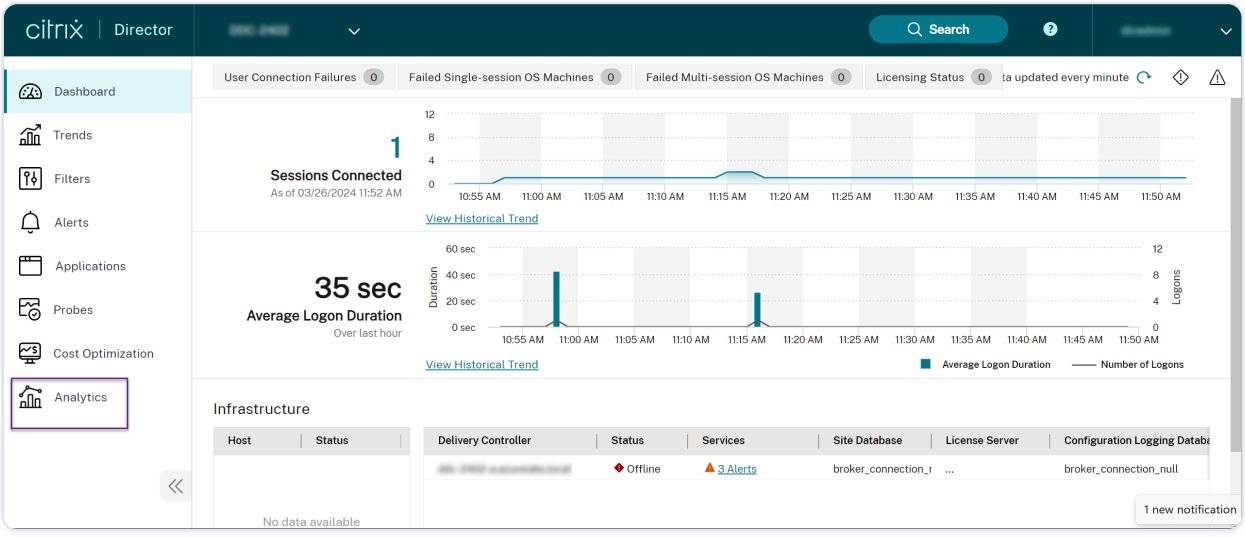
この設定は、IIS 上で Microsoft によって提供されます。詳細については、`https://docs.microsoft.com/ja-jp/dotnet/framework/network-programming/proxy-configuration` を参照してください。 構成ファイル内の **defaultproxy** フィールドは、Director および Monitor Service のアウトバウンドアクセスを制御します。Performance Analytics との構成および通信には、**defaultproxy** フィールドを **true** に設定する必要があります。有効なポリシーによってこのフィールドが false に設定されている可能性があります。この場合、手動でフィールドを true に設定する必要があります。変更を行う前に構成ファイルのバックアップを取ってください。変更を反映させるために、Delivery Controller™ 上の監視サービスを再起動してください。

- Citrix Analytics for Performance のアクティブな Citrix Cloud エンタイトルメントを所有している必要があります。
- Citrix Cloud アカウントは、Product Registration Experience への権限を持つ管理者アカウントである必要があります。管理者権限の詳細については、管理者権限の変更 を参照してください。

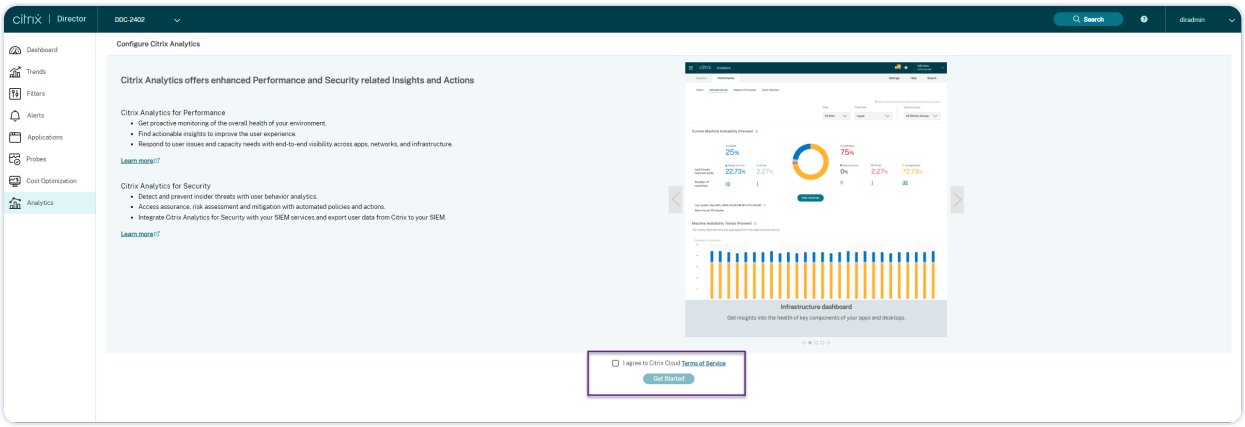
構成手順

前提条件を確認したら、以下を実行します。

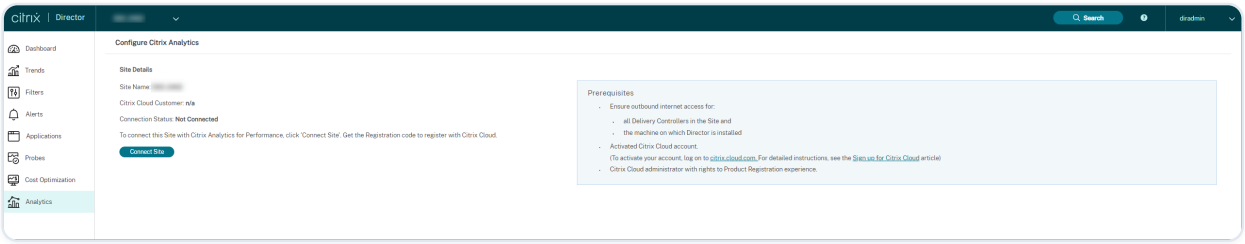
1. Director にフル管理者としてサインインし、Performance Analytics で構成するサイトを選択します。Director ダッシュボードページが表示されます。



2. **Analytics** タブをクリックします。**Citrix Analytics の構成**ページが表示されます。

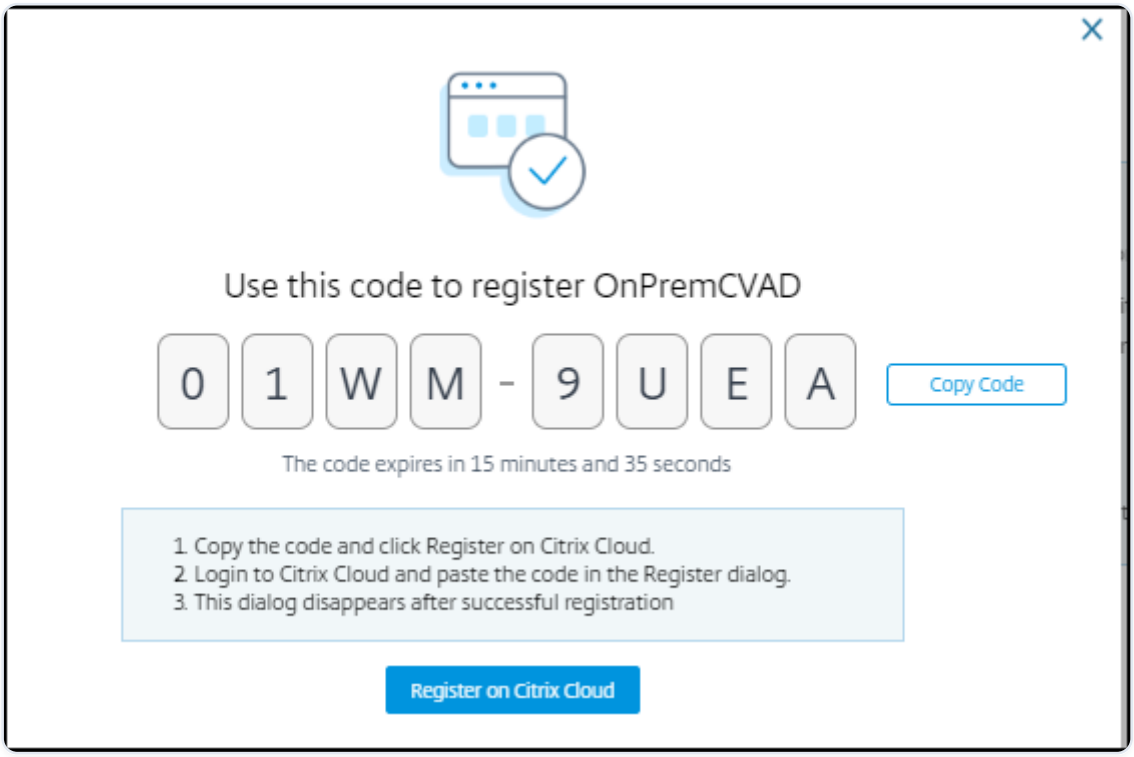


3. 手順を確認し、サービス規約を選択してから、**開始する**をクリックします。**サイトの詳細**ページが表示されます。



4. 前提条件を確認し、満たされていることを確認します。サイトの詳細を確認します。
5. 構成プロセスを開始するには、**サイトの接続**をクリックします。

   このサイトを Citrix Cloud に登録するために使用する、一意の8桁の登録コードが生成されます。



6. コードをコピーするには、**コードをコピー**をクリックし、**Citrix Cloudに登録**をクリックします。Citrix Cloudの登録URLにリダイレクトされます。
7. Citrix Cloudの資格情報でサインインし、顧客を選択します。
8. Citrix Cloudの「製品登録」ページに、コピーした登録コードを貼り付けます。登録するには、**［続行］**をクリックします。登録の詳細を確認し、［登録］**をクリックします。

   Citrix Cloudでの登録(/en-us/citrix-virtual-apps-desktops/2407/media/dir-onboarding6.png)

   オンプレミスサイトがCitrix Cloudに登録されます。
9. **Director**から、**［Analytics］**タブの**［Analyticsに移動］**をクリックします。

   Analyticsに移動(/en-us/citrix-virtual-apps-desktops/2407/media/dir-onboarding7.png)

   Performance Analyticsがブラウザーの新しいタブで開きます。 Performance Analyticsダッシュボード(/en-us/citrix-virtual-apps-desktops/2407/media/dir-onboarding-pa-dashboard.png)

   Citrix Cloudセッションの有効期限が切れている場合、Citrix.comまたはMy Citrixアカウントのログオンページにリダイレクトされることがあります。
10. 複数のサイトをPerformance Analyticsに登録するには、Directorから各サイトについて前述の構成手順を繰り返します。構成されたすべてのサイトのメトリックは、Performance Analyticsダッシュボードに表示されます。

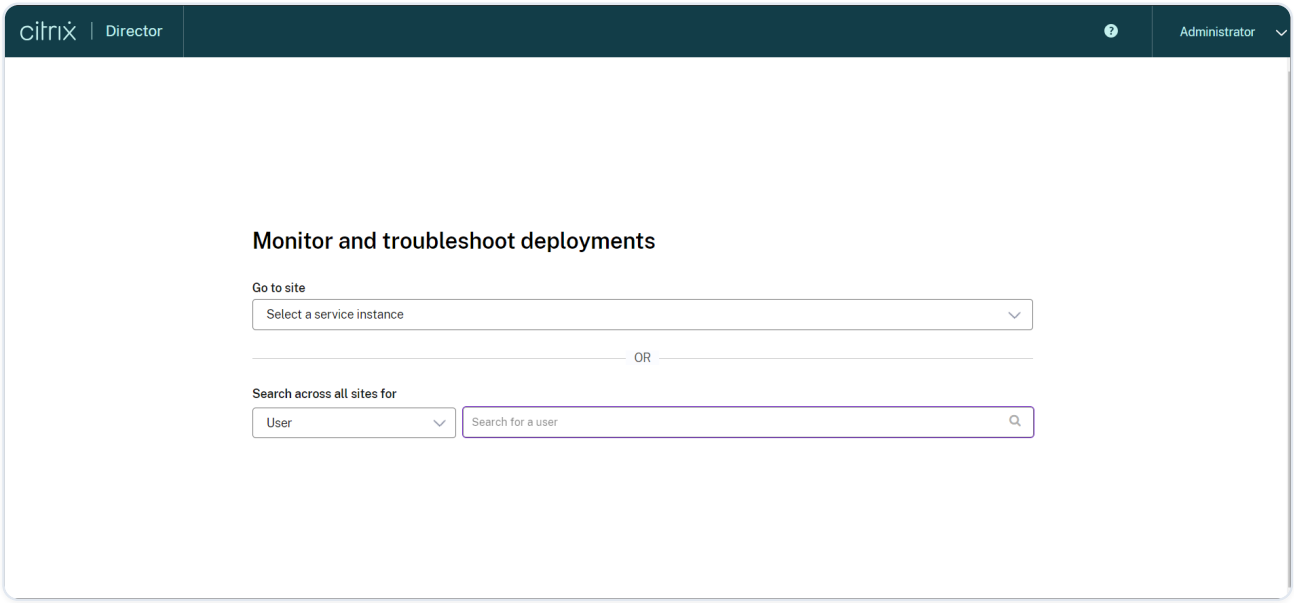
    サイトごとに複数のDirectorインスタンスが実行されている場合は、いずれか1つのDirectorインスタンスから構成します。サイトに接続されている他のすべてのDirectorインスタンスは、構成プロセス後の次回の更新時に更新されます。
11. サイトをCitrix Cloudから切断するには、 をクリックします。このオプションは、既存の構成を削除します。

> **注:**
>
> サイトを初めて構成する場合、サイトからのイベントの処理には時間がかかる場合があり（約1時間）、Performance Analyticsダッシュボードでのメトリックの表示が遅れることがあります。その後、イベントは定期的に更新されます。
>
> 切断後、新しいアカウントからのイベントが送信されるまで、古いアカウントからのデータ送信はしばらく継続されます。データ送信が停止してから約1時間、古いアカウントに関連する分析はPerformance Analyticsダッシュボードに表示されたままになります。

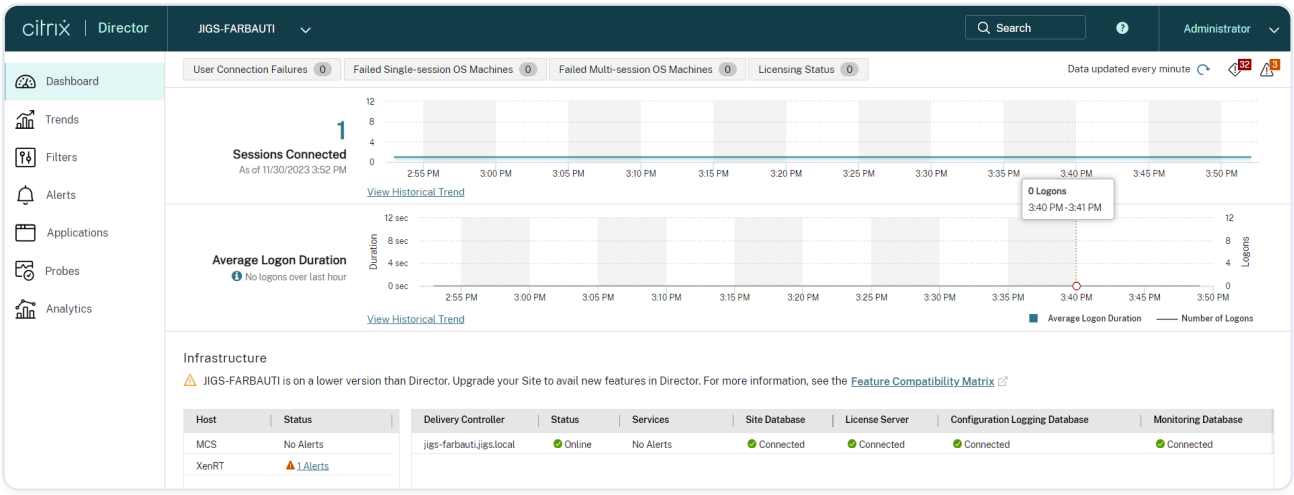
> Citrix Analyticsサービスのエンタイトルメントの有効期限が切れると、サイトメトリックのPerformance Analyticsへの送信が停止するまでに最大1日かかります。

サイト分析

Director を使用すると、展開の健全性を監視できます。オンボードされたすべてのサイトでユーザー、エンドポイント、またはマシンを検索することで、パフォーマンスの問題をトラブルシューティングできます。



完全な管理者権限がある場合、Director を開くと、ダッシュボードはサイトの健全性と使用状況を監視するための一元的な場所を提供します。



現在障害がなく、過去60分間に障害が発生していない場合、パネルは折りたたまれたままになります。障害が発生すると、特定の障害パネルが自動的に表示されます。

> **注：**
>
> 組織のライセンスと管理者権限によっては、一部のオプションまたは機能が利用できない場合があります。

Director ダッシュボードのパネル

ユーザー接続障害

過去 60 分間の接続障害。合計数の横にあるカテゴリをクリックすると、その種類の障害のメトリックが表示されます。隣接するテーブルでは、その数がデリバリーグループ別に分類されています。接続障害には、アプリケーション制限に達したことによって引き起こされる障害が含まれます。アプリケーション制限の詳細については、「アプリケーション」を参照してください。

失敗したシングルセッションOSマシンまたは失敗したマルチセッションOSマシン

過去 60 分間の合計障害数をデリバリーグループ別に分類。障害は、起動失敗、ブート中に停止、未登録などの種類別に分類されます。マルチセッションOSマシンの場合、障害には最大負荷に達したマシンも含まれます。

ライセンスステータス

ライセンスサーバーアラートは、ライセンスサーバーによって送信されたアラートと、アラートを解決するために必要なアクションを表示します。License Serverバージョン11.12.1以降が必要です。Delivery Controllerアラートは、Controllerによって認識されたライセンス状態の詳細を表示し、Controllerによって送信されます。XenApp 7.6またはXenDesktop 7.6以降のControllerが必要です。Studioでアラートのしきい値を設定できます。**Delivery Controllers** > **Details** > **Product Editions** > **PLT** に表示されるライセンスステータスは、**Premium** を示し、**Platinum** ではありません。

猶予状態

Director は以下のいずれかのグレース状態を表示します。この情報は Delivery Controller から取得されます。

1. **アクティブではありません:** いかなる種類のライセンスキャッシュモードでもありません。通常のライセンス制限が適用されます。
2. **緊急グレース:** ライセンスサーバーに到達できない場合、または接続の仲介中にライセンス情報を取得できない場合に有効になります。ユーザーには影響ありません。Director に表示されるエラーは、ライセンスサーバーに到達可能になるまで解除できません。

3. **猶予期間の期限切れ:** 緊急ライセンスキャッシュモードの有効期限が切れました。

詳細については、ライセンスの超過 および ライセンスバーストモード を参照してください。

接続されたセッション

過去 60 分間のすべてのデリバリーグループにわたる接続済みセッション。

平均ログオン時間

過去 60 分間のログオンデータ。左側の大きな数字は、1 時間あたりの平均ログオン時間です。XenDesktop 7.0 より前の VDA のログオンデータは、この平均には含まれません。詳細については、ユーザーログオンの問題の診断 を参照してください。

インフラストラクチャ

サイトのインフラストラクチャ（ホストとコントローラー）を一覧表示します。XenServer または VMware のインフラストラクチャの場合、パフォーマンスアラートを表示できます。たとえば、XenCenter を構成して、管理対象サーバーまたは仮想マシンで CPU、ネットワーク I/O、またはディスク I/O の使用率が指定されたしきい値を超えたときにパフォーマンスアラートを生成できます。デフォルトでは、アラートの繰り返し間隔は 60 分ですが、これも構成できます。詳細については、XenServer 製品ドキュメント の「XenCenter パフォーマンスアラート」セクションを参照してください。

> **注:**
>
> 特定のメトリックにアイコンが表示されない場合、そのメトリックは使用しているホストの種類でサポートされていないことを示します。たとえば、System Center Virtual Machine Manager (SCVMM) ホスト、AWS、および CloudStack では、正常性情報は利用できません。

これらのオプション（以下のセクションで説明されています）を使用して、問題のトラブルシューティングを続行します。

- ユーザーマシンの電源を制御する
- マシンへの接続を防止する

セッションの監視

セッションが切断されても、セッションはアクティブなままでアプリケーションは実行され続けますが、ユーザーデバイスはサーバーと通信しなくなります。

アクション	説明
ユーザーの現在接続されているマシンまたはセッションを表示する	アクティビティマネージャーとユーザー詳細ビューから、ユーザーが現在接続しているマシンまたはセッション、およびこのユーザーがアクセスできるすべてのマシンとセッションのリストを表示します。このリストにアクセスするには、ユーザータイトルバーのセッションスイッチャーアイコンをクリックします。詳細については、セッションの復元 を参照してください。
すべてのデリバリーグループにおける接続済みセッションの総数を表示する	ダッシュボードの**接続済みセッション**ペインで、過去60分間のすべてのデリバリーグループにおける接続済みセッションの合計数を表示します。次に、大きな合計数をクリックすると、フィルタービューが開き、選択したデリバリーグループと範囲、およびデリバリーグループ全体の使用状況に基づいてグラフィカルなセッションデータを表示できます。
アイドルセッションを終了する	セッションフィルタービューには、すべてのアクティブなセッションに関連するデータが表示されます。関連ユーザー、デリバリーグループ、セッション状態、およびしきい値期間を超えるアイドル時間に基づいてセッションをフィルター処理します。フィルター処理されたリストから、ログオフまたは切断するセッションを選択します。詳細については、アプリケーションのトラブルシューティング を参照してください。
より長い期間のデータを表示する	トレンドビューで、**セッション**タブを選択すると、より長い期間（つまり、過去60分より前のセッション合計）の接続済みセッションと切断済みセッションに関するより具体的な使用状況データをドリルダウンして表示できます。この情報を表示するには、**履歴トレンドの表示**をクリックします。

注:

ユーザーデバイスがレガシーVirtual Delivery Agent（VDA）（バージョン7より前のVDAやLinux VDAなど）を実行している場合、Directorはセッションに関する完全な情報を表示できません。代わりに、情報が利用できないことを示すメッセージが表示されます。

デスクトップ割り当てルールの制限: Web Studioでは、異なるユーザーまたはユーザーグループに対して複数のデスクトップ割り当てルール (DAR) をデリバリーグループ内の単一のVDAに割り当てることができます。StoreFront™は、ログインしているユーザーのDARに従って、対応する**表示名**で割り当てられたデスクトップを表示します。しかし、DirectorはDARをサポートしておらず、ログインしているユーザーに関係なく、デリバリーグループ名を使用して割り当てられたデスクトップを表示します。その結果、Directorで特定のデスクトップをマシンにマッピングすることはできません。 StoreFrontに表示される割り当てられたデスクトップを、Directorに表示されるデリバリーグループ名にマッピングするには、次のPowerShellコマンドを使用します。

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq
"\&lt;Name on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property
Name, Uid
```

セッション転送プロトコル

セッションの詳細パネルで、現在のセッションのHDX接続タイプに使用されている転送プロトコルを表示します。この情報は、バージョン7.13以降のVDAで起動されたセッションで利用できます。

転送プロトコル (/en-us/citrix-virtual-apps-desktops/2407/media/sessions-transport-protocol.png)

- **HDX™** 接続タイプの場合、,
  - HDX接続にEDTが使用されている場合、プロトコルは **UDP** と表示されます。
  - HDX接続にTCPが使用されている場合、プロトコルは **TCP** と表示されます。
- **RDP**接続タイプの場合、プロトコルは**n/a**と表示されます。

アダプティブトランスポートが構成されている場合、セッション転送プロトコルは、ネットワークの状態に基づいてEDT（UDP経由）とTCPの間で動的に切り替わります。EDTを使用してHDXセッションを確立できない場合、TCPプロトコルにフォールバックします。

アダプティブトランスポートの構成の詳細については、「アダプティブトランスポート」を参照してください。

レポートのエクスポート

定期的な使用状況および容量管理レポートを生成するために、トレンドデータをエクスポートできます。エクスポートはPDF、Excel、CSVレポート形式をサポートしています。PDFおよびExcel形式のレポートには、グラフと表で表されたトレンドが含まれます。CSV形式のレポートには、ビューを生成するために処理できる、またはアーカイブできる表形式のデータが含まれます。

レポートをエクスポートするには：

1. **トレンド**タブに移動します。
2. フィルター条件と期間を設定し、**適用**をクリックします。トレンドグラフとテーブルにデータが入力されます。
3. **エクスポート**をクリックし、レポートの名前と形式を入力します。

Directorは、選択したフィルター条件に基づいてレポートを生成します。フィルター条件を変更した場合は、**エクスポート**をクリックする前に**適用**をクリックしてください。

> **注:**
>
> 大量のデータをエクスポートすると、Directorサーバー、Delivery Controller、およびSQLサーバーのメモリとCPUの使用量が大幅に増加します。最適なエクスポートパフォーマンスを達成するために、サポートされる同時エクスポート操作の数とエクスポートできるデータ量はデフォルトの制限に設定されています。

サポートされるエクスポート制限

エクスポートされたPDFおよびExcelレポートには、選択されたフィルター条件の完全なグラフィカルチャートが含まれています。ただし、すべてのレポート形式の表形式データは、テーブル内の行数またはレコード数のデフォルト制限を超えて切り捨てられます。サポートされるレコードのデフォルト数は、レポート形式に基づいて定義されます。

Internet Information Services (IIS) のDirectorアプリケーション設定を構成することで、デフォルトの制限を変更できます。

レポート形式	サポートされるレコードのデフォルト数	DIRECTORアプリケーション設定のフィールド	サポートされるレコードの最大数
PDF	500	UI.ExportPdfDrilldownLimit	5000

レポート形式	サポートされるレコードのデフォルト数	DIRECTORアプリケーション設定のフィールド	サポートされるレコードの最大数
エクセル	100,000	UI.ExportExcelDrilldownLimit	100,000
CSV	100,000 (「**セッション**」タブでは10,000,000)	UI.ExportCsvDrilldownLimit	100,000

エクスポートできるレコード数の制限を変更するには:

1. IISマネージャーコンソールを開きます。
2. デフォルトのWebサイトの下にあるDirector Webサイトに移動します。
3. **アプリケーション設定**をダブルクリックします。
4. 必要に応じて、UI.ExportPdfDrilldownLimit、UI.ExportExcelDrilldownLimit、またはUI.ExportCsvDrilldownLimitフィールドの設定を編集または追加します。

アプリケーション設定でこれらのフィールド値を追加すると、デフォルト値が上書きされます。

> **警告:**
>
> サポートされている最大レコード数を超えるフィールド値を設定すると、エクスポートのパフォーマンスに影響を与える可能性があり、サポートされていません。

エラー処理

このセクションでは、エクスポート操作中に発生する可能性のあるエラーの対処方法に関する情報を提供します。

- **Directorがタイムアウトしました**

このエラーは、DirectorサーバーまたはMonitor Serviceでのネットワークの問題や高いリソース使用率が原因で発生する可能性があります。

デフォルトのタイムアウト期間は100秒です。Director Serviceのタイムアウト期間を延長するには、Internet Information Services (IIS)のDirectorアプリケーション設定で**Connector.DataServiceContext.Timeout**フィールドの値を設定します。

1. IISマネージャーコンソールを開きます。
2. デフォルトのWebサイトの下にあるDirector Webサイトに移動します。
3. **アプリケーション設定**をダブルクリックします。
4. **Connector.DataServiceContext.Timeout**の値を編集します。

- **Monitorがタイムアウトしました**

このエラーは、Monitor ServiceまたはSQLサーバーでのネットワークの問題や高いリソース使用率が原因で発生する可能性があります。

Monitor Serviceのタイムアウト期間を長くするには、Delivery Controllerで次のPowerShellコマンドを実行します。

```
asnp Citrix.*

Get-MonitorConfiguration

Set-MonitorConfiguration -MonitorQueryTimeoutSeconds &lt;timeout value>
```

- **同時実行中のエクスポートまたはプレビュー操作の最大数**

Director は、エクスポートまたはプレビューのインスタンスを 1 つサポートします。「**Max concurrent Export or Preview operations ongoing**」エラーが発生した場合は、次のエクスポート操作を後でもう一度試してください。

同時実行のエクスポートまたはプレビュー操作の数を増やすことは可能ですが、Director のパフォーマンスに影響を与える可能性があり、サポートされていません。

1. IISマネージャーコンソールを開きます。
2. デフォルトのWebサイトの下にあるDirector Webサイトに移動します。
3. をダブルクリックします。
4. 値**UI.ConcurrentExportLimit**を編集します。

- **Directorのディスク容量不足**

各エクスポート操作には、Windows Temp フォルダーに最大 2 GB のハードディスク容量が必要です。Director サーバーの空き容量を確保するか、ハードディスク容量を追加してから、エクスポートを再試行してください。

Monitorのホットフィックス

特定のマシン VDA (物理または仮想マシン) にインストールされているホットフィックスを表示するには、 ビューを選択します。

ユーザーマシンの電源状態を制御する

Director で選択したマシンの状態を制御するには、電源制御オプションを使用します。これらのオプションは、シングルセッション OS マシンで利用できますが、マルチセッション OS マシンでは利用できない場合があります。

注：

この機能は、物理マシンまたはリモートPCアクセスを使用するマシンでは利用できません。

コマンド	機能
再起動	VMを正常に（ソフトに）シャットダウンし、VMを再起動する前に実行中のすべてのプロセスを個別に停止します。たとえば、Directorで「起動に失敗しました」と表示されるマシンを選択し、このコマンドを使用して再起動します。
強制再起動	シャットダウン手順を最初に実行せずにVMを再起動します。このコマンドは、物理サーバーのプラグを抜き、再度差し込んで電源を入れ直すのと同じように機能します。
シャットダウン	VMを正常に（ソフトに）シャットダウンします。実行中のすべてのプロセスが個別に停止されます。
強制シャットダウン	シャットダウン手順を最初に実行せずにVMをシャットダウンします。このコマンドは、物理サーバーのプラグを抜くのと同じように機能します。実行中のすべてのプロセスが常にシャットダウンされるとは限ら

コマンド	機能
	ず、この方法でVMをシャットダウンするとデータが失われるリスクがあります。
一時停止	実行中のVMを現在の状態で一時停止し、その状態をデフォルトのストレージリポジトリ上のファイルに保存します。このオプションを使用すると、VMのホストサーバーをシャットダウンし、後で再起動した後にVMを再開して、元の実行状態に戻すことができます。
再開	一時停止されたVMを再開し、元の実行状態に復元します。
起動	電源がオフになっているVMを起動します（コールドスタートとも呼ばれます）。

電源制御アクションが失敗した場合、アラートにマウスを重ねると、失敗の詳細を示すポップアップメッセージが表示されます。

マシンへの接続を防止する

適切な管理者がイメージのメンテナンス作業を実行している間、メンテナンスモードを使用して一時的に新しい接続を防止します。

マシンでメンテナンスモードを有効にすると、無効にするまで新しい接続は許可されません。ユーザーが現在ログオンしている場合、すべてのユーザーがログオフするとすぐにメンテナンスモードが有効になります。ログオフしないユーザーには、マシンが特定の時間にシャットダウンされることを通知するメッセージを送信し、電源制御を使用してマシンを強制的にシャットダウンしてください。

1. ユーザー詳細ビューからマシンを選択するか、フィルタービューでマシンのグループを選択します。
2. **メンテナンスモード**を選択し、オプションをオンにします。

ユーザーが割り当てられたデスクトップにメンテナンスモード中に接続しようとすると、デスクトップが利用できないことを示すメッセージが表示されます。メンテナンスモードを無効にするまで、新しい接続はできません。

アプリケーション分析

アプリケーションタブには、アプリケーションベースの分析が単一の統合ビューで表示され、アプリケーションのパフォーマンスを効率的に分析および管理するのに役立ちます。サイトで公開されているすべてのアプリケーションの健全性と使用状況に関する貴重な洞察を得ることができます。プローブ結果、アプリケーションごとのインスタンス数、公開されたアプリケーションに関連する障害やエラーなどのメトリックが表示されます。詳細については、**アプリケーションのトラブルシューティング**のアプリケーション分析セクションを参照してください。

アラートと通知

アラートは、Directorのダッシュボードやその他の高レベルビューに、警告および重大なアラートシンボルとともに表示されます。アラートは**Premium**ライセンスサイトで利用できます。アラートは1分ごとに自動的に更新されます。また、オンデマンドでアラートを更新することもできます。

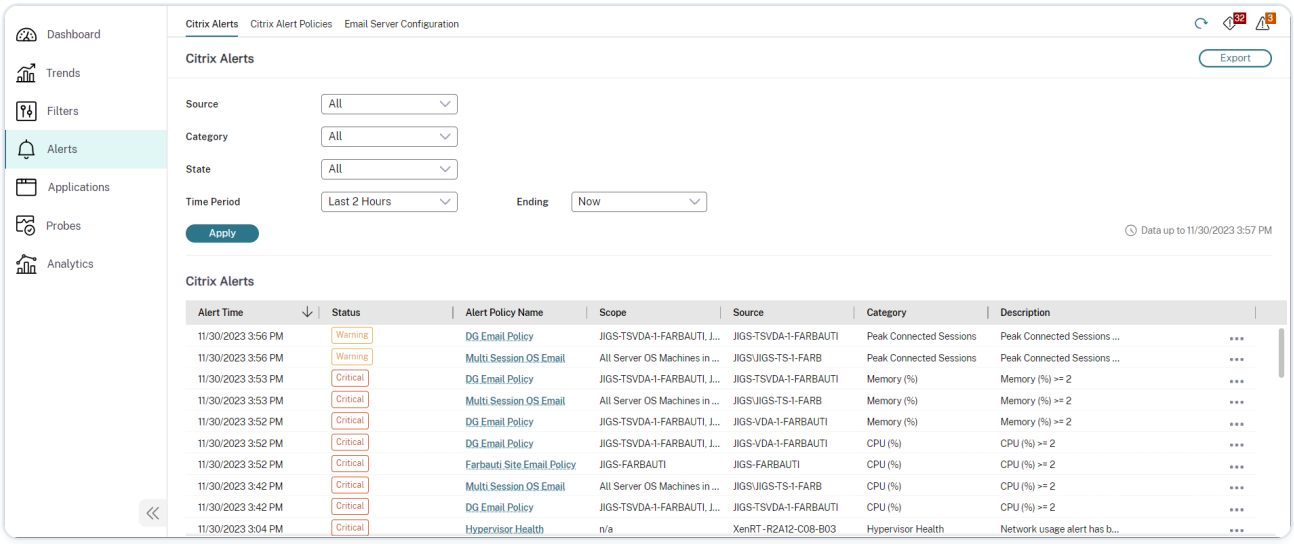
Directorのアラート(/en-us/citrix-virtual-apps-desktops/2407/media/dir-alerts.png)

警告アラート（琥珀色の三角形）は、条件の警告しきい値に達したか、それを超えたことを示します。

重大アラート（赤い丸）は、条件の重大なしきい値に達したか、それを超えたことを示します。

アラートに関する詳細情報は、サイドバーからアラートを選択するか、サイドバーの下部にある**Go to Alerts**リンクをクリックするか、Directorページの上部から**Alerts**を選択することで表示できます。

アラートビューでは、アラートをフィルター処理してエクスポートできます。たとえば、特定のデリバリーグループの過去1か月間の失敗したマルチセッションOSマシン、または特定のユーザーのすべてのアラートなどです。詳細については、「レポートのエクスポート」を参照してください。



Citrix®アラート

Citrixアラートは、Citrixコンポーネントから発生し、Directorで監視されるアラートです。Citrixアラートは、Directorの**Alerts** \> **Citrix Alerts Policy**で構成できます。構成の一部として、アラートが設定したしきい値を超えた場合に、個人やグループに電子メールで通知を送信するように設定できます。Citrixアラートの設定の詳細については、「アラートポリシーの作成」を参照してください。

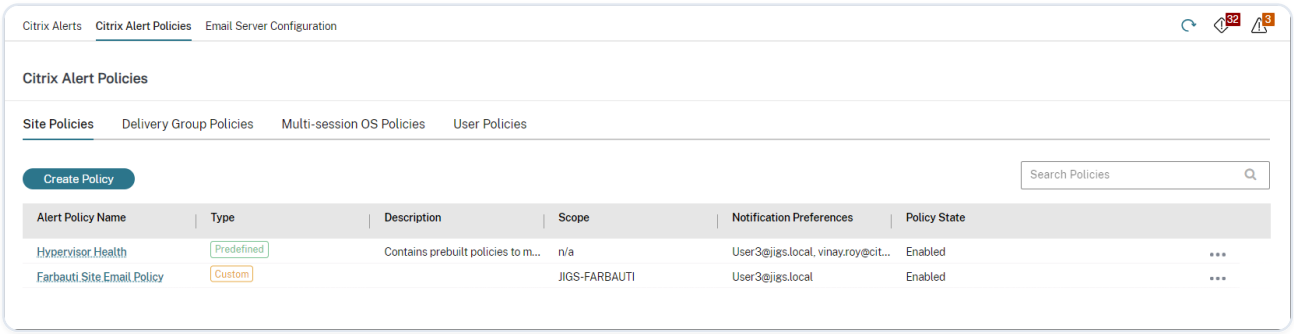
> **注:**
>
> ファイアウォール、プロキシ、またはMicrosoft Exchange Serverがメールアラートをブロックしないようにしてください。

スマートアラートポリシー

事前定義されたしきい値を持つ一連の組み込みアラートポリシーは、デリバリーグループおよびマルチセッションOS VDAスコープで利用できます。この機能には、Delivery Controllerバージョン7.18以降が必要です。組み込みアラートポリシーのしきい値パラメーターは、**Alerts** \> **Citrix Alerts Policy**で変更できます。 これらのポリシーは、サイトで少なくとも1つのアラートターゲット（デリバリーグループまたはマルチセッションOS VDA）が定義されている場合に作成されます。さらに、これらの組み込みアラートは、新しいデリバリーグループまたはマルチセッションOS VDAに自動的に追加されます。

Directorとサイトをアップグレードする場合、以前のDirectorインスタンスのアラートポリシーが引き継がれます。組み込みアラートポリシーは、Monitorデータベースに対応するアラートルールが存在しない場合にのみ作成されます。

組み込みのアラートポリシーのしきい値については、アラートポリシーの条件セクションを参照してください。



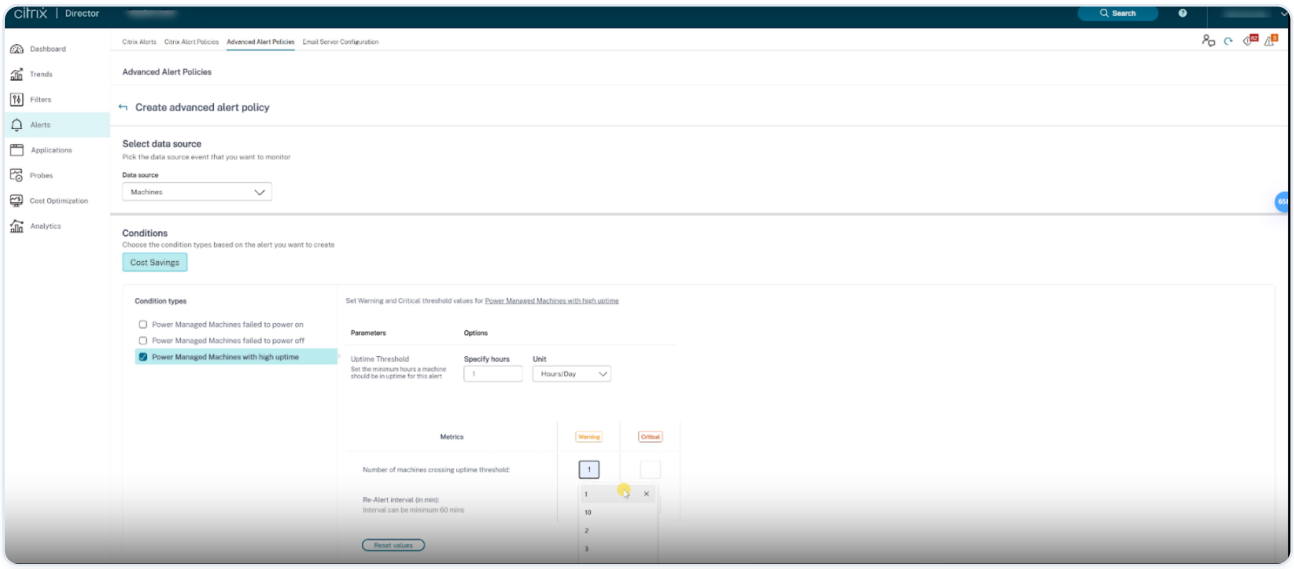
高度なアラートポリシー

Directorのプロアクティブな通知およびアラート機能が強化され、**高度なアラートポリシー**という新しいアラートフレームワークが追加されました。この機能を使用すると、各要素または条件に詳細な情報を含めてアラートを作成できるため、アラートの範囲に対する制御が強化されます。現在、これらのポリシーには、コスト削減とインフラストラクチャに関するアラートが含まれています。

データソース駆動型アラートである高度なアラートポリシーの導入により、複数条件のスコープフィルタリングを使用できるようになりました。

この機能は、過剰なアラートを減らすのに役立ちます。過剰なアラートは、重要な問題への対応の遅延や効果の低下につながる可能性があります。このポリシーは、アラートポリシーの有効性と管理者からのエンゲージメントを測定するのに役立ちます。

アラート > **高度なアラートポリシー** > **ポリシーの作成**セクションから、高度なアラートポリシーを作成できます。



カテゴリとして、**電源管理対象マシンが起動に失敗しました**、**電源管理対象マシンがシャットダウンに失敗しました**、**稼働時間の長い電源管理対象マシン**を選択し、ポリシーに必要な条件を選択できます。ポリシーの作成方法の詳細については、アラートポリシーの作成を参照してください。ポリシーが作成された後、Citrix Alertsページでポリシーを編集、削除、または無効にすることができます。

上記の各条件について、特定のパラメーターと対応するオプションを選択できます。

稼働時間の長い電源管理マシンカテゴリは、次のメトリックをチェックします。

- 稼働時間のしきい値を超過したマシンの数
- 再アラート間隔（分単位）。間隔は最低60分です。

電源管理マシンが起動に失敗しましたおよび**電源管理マシンがシャットダウンに失敗しました**カテゴリは、次のメトリックをチェックします。

- 稼働時間のしきい値を超過したマシンの数
- サンプリング間隔（分単位）は30分の倍数にできます
- 再アラート間隔（分単位）は60分の倍数にできます

必要に応じて、上記のカテゴリの重大度を設定できます。これらのアラートの再アラート間隔をスケジュールすることもできます。

ポリシーのスコープを定義する

アラートのスコープを定義し、例外を追加できます。アラートは選択されたスコープに対してのみ生成され、例外の追加によって除外されたサブスコープはアラート生成に含まれません。この機能は、詳細なレベルでアラートを作成するのに役立ちます。

電子メールまたはWebhook URLを介して通知を作成できます。アラートを受信する希望の言語を選択することもできます。また、電子メールの場合は.CSVファイル添付として、Webhook URLを介した場合はJSONペイロードとしてアラートパラメータを受信するオプションを選択することもできます。添付ファイルには、必要なパラメータの詳細が含まれています。詳細については、「アラートコンテンツの機能強化」を参照してください。

以下のデータは、電子メールまたは**Citrix Alerts**ページでアラートとして受信されます。

フィールド	説明
顧客ID	サイトの顧客ID。

フィールド	説明
アラートレベル	この値は、各アラート条件に対して設定された事前定義値です。可能な値は、Critical（重大）とWarning（警告）です。
条件	この値は、ポリシー作成時に設定された条件です。たとえば、未登録マシンの数が20以上である場合などです。
ターゲット	アラートがトリガーされるデリバリーグループまたはサイトの名前。
サイト	サイトの名前。
スコープ	ポリシーのスコープ。この値にはサブスコープも含まれます。
ポリシー	ポリシーの名前。
説明	アラートがトリガーされる問題の説明。

PowerShellスクリプトを使用して高度なアラートポリシーを作成する方法?

アラートポリシーを作成するためのPowerShellスクリプト:

```
asnp Citrix.Monitor.*

# Add Parameters

$timeSpan = New-TimeSpan -Seconds 30

$alertThreshold = 1

$alarmThreshold = 2

# Add Target UID's

$targetIds = @()

$targetIds += "e9a211b4-a1f3-4f74-b6c7-85225902e997"

# Add email addresses
```

```
$emailaddress = @()

$emailaddress += "loki@abc.com"

# Create new policy

$policy = New-MonitorNotificationPolicy -Name
"FailedMachinePercentageAlertCreationViaPowershell" -Description "Policy
created to test urm" -Enabled $true
```

次の行をFAILEDMACHINEPERCENTAGEの正しい条件に置き換えます

```
Add-MonitorNotificationPolicyCondition -Uid $policy.Uid -ConditionType
FailedMachinePercentage -AlertThreshold $alertThreshold -AlarmThreshold
$alarmThreshold -AlertRenotification $timeSpan -AlarmRenotification
$timeSpan

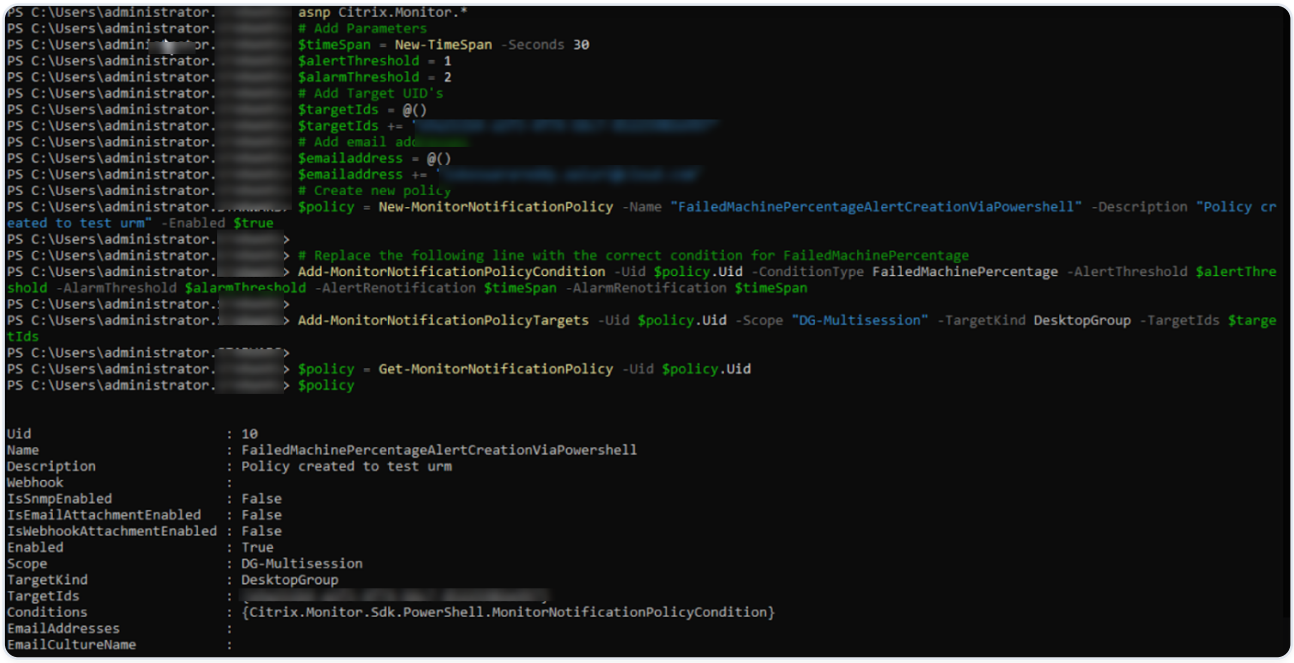


Add-MonitorNotificationPolicyTargets -Uid $policy.Uid -Scope "DG-
Multisession" -TargetKind DesktopGroup -TargetIds $targetIds



$policy = Get-MonitorNotificationPolicy -Uid $policy.Uid

$policy
```



上記の画像から、ポリシーが作成され、Uidが10であることがわかります。

構成にメールを追加するには

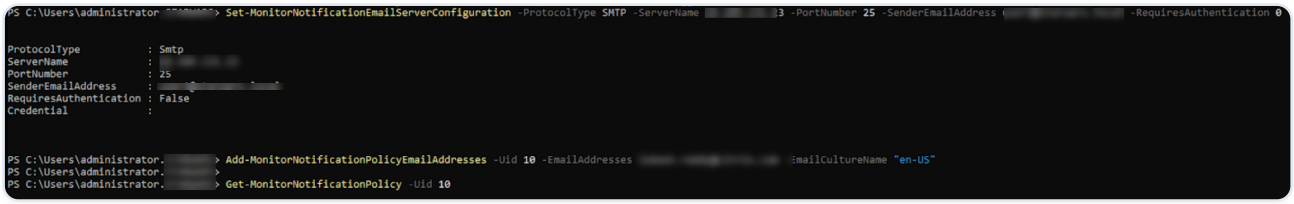
```
Set-MonitorNotificationEmailServerConfiguration -ProtocolType SMTP
-ServerName NameOfTheSMTPServerOrIPAddress -PortNumber 80
-SenderEmailAddress loki@abc.com -RequiresAuthentication 0
```

ポリシーにメールを追加するには

```
Add-MonitorNotificationPolicyEmailAddresses -Uid $policy.Uid
-EmailAddresses $emailaddress -EmailCultureName "en-US"
```

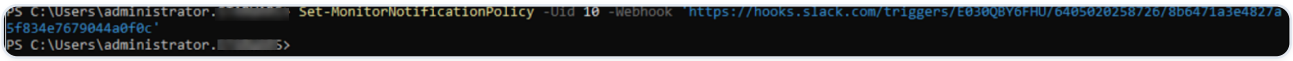
メールを追加するためのサンプルスクリプト:

```
Add-MonitorNotificationPolicyEmailAddresses -Uid 10 -EmailAddresses
$emailaddress -EmailCultureName "en-US"
```



ポリシーにWEBHOOK URLを追加するには

```
Set-MonitorNotificationPolicy –Uid $polcy.Uid –Webhook 'URL'
```

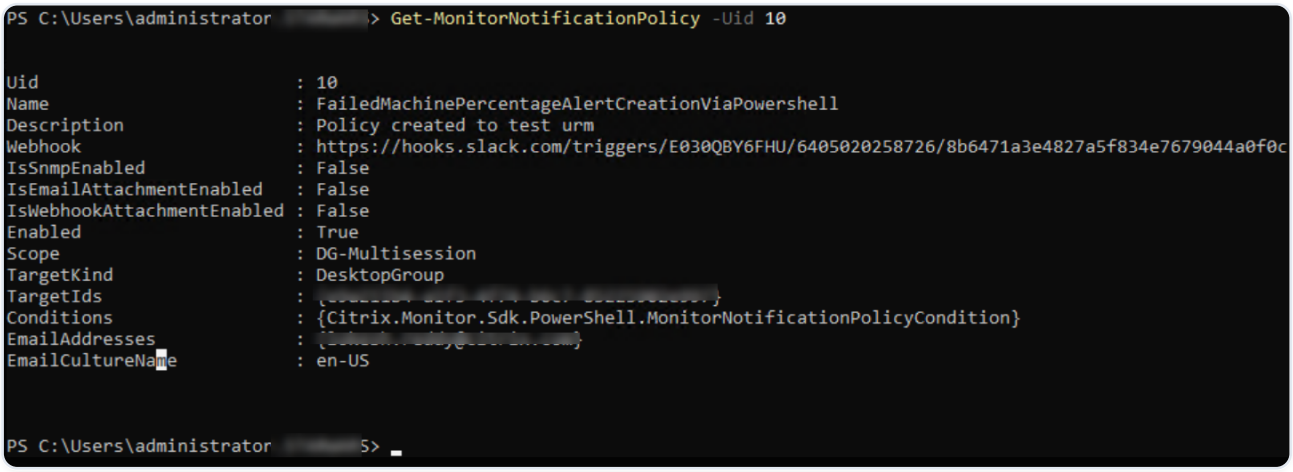


Webhook URLを追加するためのサンプルスクリプト:

```
Set-MonitorNotificationPolicy –Uid 10  –Webhook  'https://hooks.slack.com/
triggers/E030QBY6FHU/6405020258726/8b6471a3e4827a5f834e7679022a1f1c'
```

作成されたポリシーの詳細を取得する

```
Get-MonitorNotificationPolicy -Uid 10
```



インフラストラクチャポリシー（プレビュー）

これらのポリシーは、サポートされているCitrix Virtual Apps and Desktops™コンポーネントの健全性に関連するアラートを作成するために導入されました。

インフラストラクチャ監視 のセットアップが完了すると、Directorで利用可能な健全性データを使用して、必要なコンポーネントのアラートを設定できます。管理者は、条件、スコープ、および通知媒体を設定して、電子メールまたはWebhookを介したJSONペイロードで重要なアラートを受信できます。発生したアラートは、分析と管理のために**Citrix Alerts**セクションでも利用できます。

新しく導入されたインフラストラクチャポリシーの一部として、アラート条件は次の4つのセクションに分類されます。

- 到達可能性
- 依存サービス
- 影響
- リソース使用率

各カテゴリ内の条件は、組織の優先順位に基づいて、**重大**および**警告**の重大度で設定できます。これらのアラートの再アラート間隔をスケジュールすることもできます。

インフラストラクチャポリシーは、**アラート** > **Citrixアラートポリシー**セクションから作成できます。必要なカテゴリを選択し、ポリシーに必要な条件を選択できます。ポリシーの作成方法の詳細については、「アラートポリシーの作成」を参照してください。ポリシーが作成された後、Citrixアラートページでポリシーを編集、削除、または無効にできます。

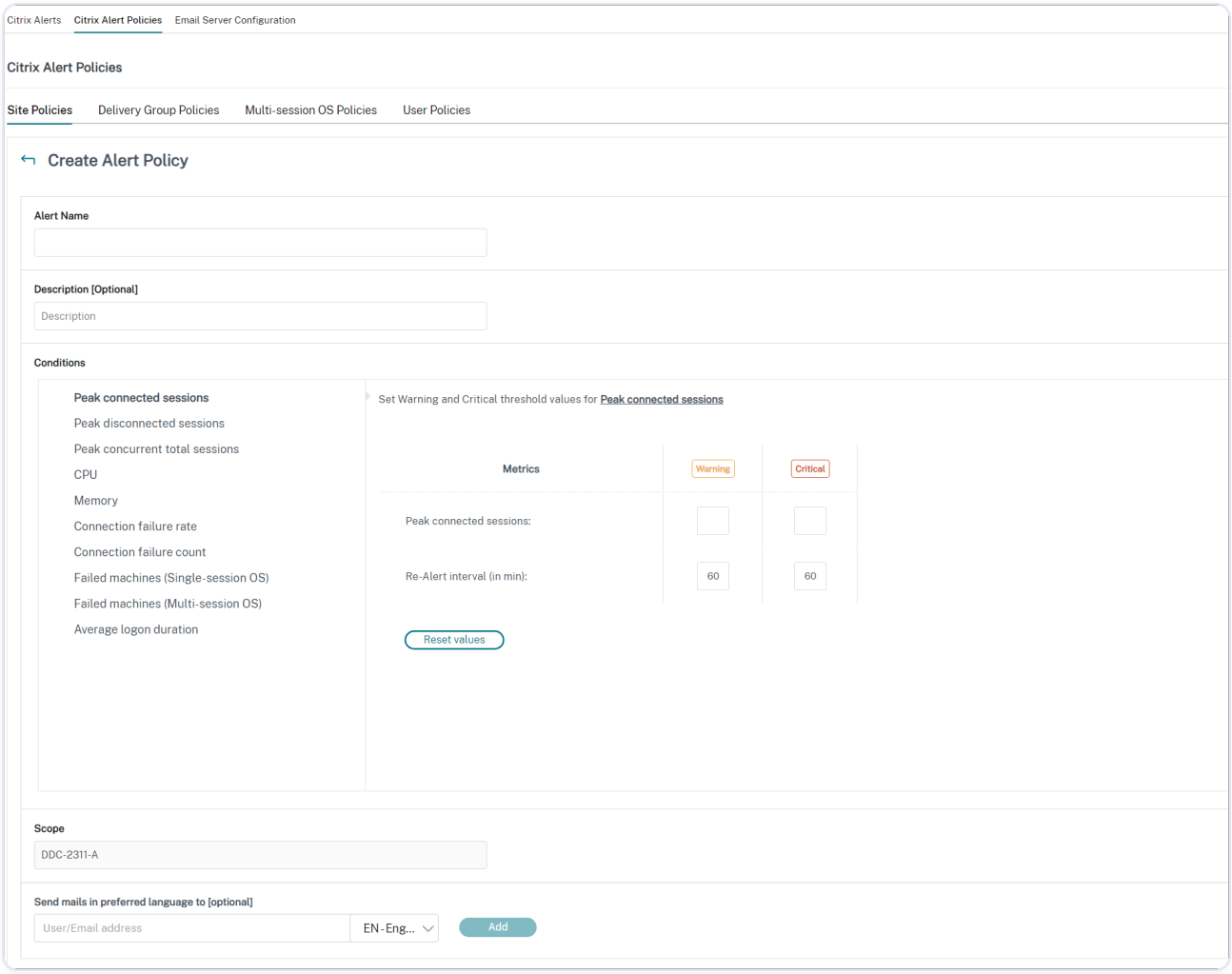
各カテゴリとコンポーネントでサポートされている条件の詳細については、以下を参照してください。

- PVSヘルス指標
- StoreFrontヘルス指標

次のデータは、電子メールまたは Citrix Alert ページでアラートとして受信されます。

フィールド	説明
顧客ID	サイトの顧客ID。
アラートレベル	指定できる値は、CriticalとWarningです。
ターゲット	アラートがトリガーされたマシンの名前。
時間	アラートがトリガーされた時刻。
スコープ	ポリシーのスコープ。
ポリシー	ポリシーの名前。
説明	アラートがトリガーされる問題の説明。

アラートポリシーを作成する



アラートポリシーを作成するには、たとえば、特定のセッション数条件が満たされたときにアラートを生成するには、次の手順を実行します。

1. **アラート** > **Citrixアラートポリシー** に移動し、たとえば、Multi-session OS Policy を選択します。
2. **作成** をクリックします。
3. ポリシーに名前を付けて説明し、アラートがトリガーされる条件を設定します。たとえば、ピーク接続セッション、ピーク切断セッション、およびピーク同時合計セッションの警告数と危険数を指定します。警告値は危険値より大きくしてはいけません。詳細については、「アラートポリシーの条件」を参照してください。
4. 再アラート間隔を設定します。アラートの条件が引き続き満たされている場合、この時間間隔でアラートが再度トリガーされ、アラートポリシーで設定されている場合は、電子メール通知が生成されます。却下されたアラートは、再アラート間隔で電子メール通知を生成しません。
5. スコープを設定します。たとえば、特定のデリバリーグループに設定します。

6. 通知設定で、アラートがトリガーされたときに、誰に電子メールで通知する必要があるかを指定します。アラートポリシーで電子メール通知設定を行うには、**電子メールサーバー構成**タブで電子メールサーバーを指定する必要があります。

   a. .CSV添付ファイルまたはJSONペイロードを介してアラートコンテンツを受信することもできます。これには、次のチェックボックスをオンにします。

      - **JSONペイロードをWebhookの添付ファイルとして含める**
      - **CSVファイルを電子メールの添付ファイルとして含める**

> **注:**
>
> 現在、.CSV添付ファイルおよびJSONペイロードオプションを介してアラートコンテンツを受信できるのは、一部のアラートのみです。詳細については、「アラートコンテンツの機能強化」を参照してください。

7. 「**保存**」をクリックします。

スコープで20以上のデリバリーグループが定義されたポリシーを作成すると、構成の完了に約30秒かかる場合があります。この間、スピナーが表示されます。

最大20の固有のデリバリーグループ（合計1000のデリバリーグループターゲット）に対して50を超えるポリシーを作成すると、応答時間が増加する可能性があります（5秒以上）。

アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、マシンパラメーターを使用して定義された誤ったデリバリーグループアラートがトリガーされる可能性があります。

> **注:**
>
> アラートポリシーを削除した後、そのポリシーによって生成されたアラート通知が停止するまでに最大30分かかる場合があります。

アラートコンテンツの機能強化

Directorのアラート機能が強化され、CSV添付ファイルとJSONペイロードが含まれるようになりました。この強化により、電子メールでCSV添付ファイルとして、またはWebhookがある場合はJSONペイロードとしてアラートの詳細を取得できます。このCSV添付ファイルまたはJSONペイ

ロードを使用すると、詳細レベルで豊富なコンテンツを受信でき、問題の迅速な特定と解決に役立ちます。

現在、この機能強化は以下の種類のアラートでのみ利用可能です。

- マシンの稼働時間
- 電源オン失敗アクション
- 電源オフ失敗アクション
- 未登録のマシン (%)

この機能を使用するには、アラートに移動し、次のチェックボックスを選択します。

- **Webhookにjsonペイロードを添付として含める**
- **メールにcsvファイルを添付として含める**

以下は、**Citrix Alert Policies**セクションのスクリーンショットです。

強化されたアラート(/en-us/citrix-virtual-apps-desktops/2407/media/csv-and-webhook.png)

以下は、**Advanced Alert Policies**セクションのスクリーンショットです。

強化されたアラート（詳細）(/en-us/citrix-virtual-apps-desktops/2407/media/csv-and-webhook-advanced.png)

CSV添付ファイル

次の表は、サポートされているすべてのアラートの.CSV添付ファイルの列を示しています。

列	適用可能なアラート
マシン名、IPアドレス、およびデリバリーグループ名	マシンの稼働時間、電源オフ失敗アクションと電源オン失敗アクション、および未登録マシン（%）
現在の登録状態、失敗日、障害状態、およびライフサイクル状態	未登録マシン（%）
最終電源アクション失敗理由、最終電源アクショントリガー元、最終電源アクションタイプ、および最終電源アクション完了日	電源オフ失敗アクションと電源オン失敗アクション
電源状態、電源オン日、および合計稼働時間(分)	マシンの稼働時間

WEBHOOKペイロード

未登録マシンの割合アラート

```
Webhook Payload

{

    "Address": "<Webhook URL>",

    "NotificationId": "<NotificationGUID>",

    "NotificationState": "NotificationActive",

    "Priority": "<Critical/Warning>",

    "Target": "<DeliveryGroupName>",

    "Condition": "Unregistered machines (in %)",

    "Value": "<Value Set as Threshold>",

    "Timestamp": "<Timestamp string Eg: April 25, 2024 9:33 PM (UTC +5)>",

    "PolicyName": "<Alert Policy Name>",

    "Description": "<Alert Policy Description>",

    "Scope": "DeliveryGroup",

    "Site": "<Name of the Site>",

    "AttachmentData": [{

                                        "Machine Name": "<Name of the
Machine>",

                                        "IP Address": “<IP Address>”,

                                        "Delivery Group Name": "<Name of the
DeliveryGroup>",

                                        "Current Registration State":
"Unregistered",
```

```
                                    "Failure Date": “<Date of Failure>”,

                                    "Fault State": "<Fault State of the
Machine>",

                                    "Lifecycle State": "<Lifecycle state
of the Machine>"

                                 },

                                {

                                    "Machine Name": "<Name of the
Machine>",

                                    "IP Address": “<IP Address>”,

                                    "Delivery Group Name": "<Name of the
DeliveryGroup>",

                                    "Current Registration State":
"Unregistered",

                                    "Failure Date": “<Date of Failure>”,

                                    "Fault State": "<Fault State of the
Machine>",

                                    "Lifecycle State": "<Lifecycle state
of the Machine>"

                                 }]

}
```

電源オン失敗アクションアラート

```
Webhook Payload Body

{

    "Address": "<Webhook URL>",
```

```
    "NotificationId": "<NotificationGUID>",

    "NotificationState": "NotificationActive",

    "Priority": "<Critical/Warning>",

    "Target": "<DeliveryGroupName>",

    "Condition": "Failure To PowerOn Action",

    "Value": "<Value Set as Threshold>",

    "Timestamp": "<Timestamp string Eg: April 25, 2024 9:33 PM (UTC +5)>",

    "PolicyName": "<Alert Policy Name>",

    "Description": "<Alert Policy Description>",

    "Scope": "DeliveryGroup",

    "Site": "<Name of the Site>",

    "AttachmentData": [{

                                        "Machine Name": "<Name of the
Machine>",

                                        "IP Address": “<IP Address>”,

                                        "Delivery Group Name": "<Name of the
DeliveryGroup>",

                                       "Last Power Action Failure Reason":
"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Power
Action Type>",

                                        "Last Power Action Triggered By":
"<End-User,Administrator,Auto-Scale,Schedule>",

                                        "Last Power Action Type": “<PowerOn/
PowerOff>”,

                                        "Last Power Action Completed Date":
```

```
"<Time string Eg: 2024-05-15T15:04:27.723>",

                                    {

                                        "Machine Name": "<Name of the
Machine>",

                                        "IP Address": “<IP Address>”,

                                        "Delivery Group Name": "<Name of the
DeliveryGroup>",

                                        "Last Power Action Failure Reason":
"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Power
Action Type>",

                                        "Last Power Action Triggered By":
"<End-User,Administrator,Auto-Scale,Schedule>",

                                        "Last Power Action Type": “<PowerOn/
PowerOff>”,

                                        "Last Power Action Completed Date":
"<Time string Eg: 2024-05-15T15:04:27.723>"

                                     }]

}
```

電源オフ失敗アクションアラート

```
{

    "Address": "<Webhook URL>",

    "NotificationId": "<NotificationGUID>",

    "NotificationState": "NotificationActive",

    "Priority": "<Critical/Warning>",

    "Target": "<DeliveryGroupName>",

    "Condition": "Failure To PowerOff Action",
```

```
    "Value": "<Value Set as Threshold>",

    "Timestamp": "<Timestamp string Eg: April 25, 2024 9:33 PM (UTC +5)>",

    "PolicyName": "<Alert Policy Name>",

    "Description": "<Alert Policy Description>",

    "Scope": "DeliveryGroup",

    "Site": "<Name of the Site>",

    "AttachmentData": [{

                                        "Machine Name": "<Name of the
Machine>",

                                        "IP Address": “<IP Address>”,

                                        "Delivery Group Name": "<Name of the
DeliveryGroup>",

                                        "IP Address": "<IPV4 Address of the
Machine>",

                                        "Last Power Action Failure Reason":
"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Power
Action Type>",

                                        "Last Power Action Triggered By":
"<End-User,Administrator,Auto-Scale,Schedule>",

                                        "Last Power Action Type": “<PowerOn/
PowerOff>”,

                                        "Last Power Action Completed Date":
"<Time string Eg: 2024-05-15T15:04:27.723>"

                                    },

                                   {

                                        "Machine Name": "<Name of the
```

```
Machine>",

                                        "IP Address": “<IP Address>”,

                                        "Delivery Group Name": "<Name of the
DeliveryGroup>",

                                        "IP Address": "<IPV4 Address of the
Machine>",

                                       "Last Power Action Failure Reason":
"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Power
Action Type>",

                                        "Last Power Action Triggered By":
"<End-User,Administrator,Auto-Scale,Schedule>",

                                        "Last Power Action Type": “<PowerOn/
PowerOff>”,

                                        "Last Power Action Completed Date":
"<Time string Eg: 2024-05-15T15:04:27.723>"

                                    }]

}
```

マシンの稼働時間アラート

```
{

    "Address": "<Webhook URL>",

    "NotificationId": "<NotificationGUID>",

    "NotificationState": "NotificationActive",

    "Priority": "<Critical/Warning>",

    "Target": "<DeliveryGroupName>",

    "Condition": "Machine Uptime Alert",

    "Value": "<Value Set as Threshold>",
```

```
    "Timestamp": "<Timestamp string Eg: April 25, 2024 9:33 PM (UTC +5)>",

    "PolicyName": "<Alert Policy Name>",

    "Description": "<Alert Policy Description>",

    "Scope": "DeliveryGroup",

    "Site": "<Name of the Site>",

    "AttachmentData": [{

                                        "Machine Name": "<Name of the
Machine>",

                                        "IP Address": “<IP Address>”,

                                        "Delivery Group Name": "<Name of the
DeliveryGroup>",

                                        "IP Address": "<IPV4 Address of the
Machine>",

                                        "Power State": "<On/Off>",

                                        "Powered On Date": "Time sting Eg:
2024-05-15T15:04:27.723",

                                        "Total Uptime In Minutes": 180

                                    },

                                   {

                                        "Machine Name": "<Name of the
Machine>",

                                        "IP Address": “<IP Address>”,

                                        "Delivery Group Name": "<Name of the
DeliveryGroup>",

                                        "IP Address": "<IPV4 Address of the
```

```
Machine>",
                                        "Power State": "<ON/OFF>",
                                        "Powered On Date": "<Time string Eg:
2024-05-15T15:04:27.723>",
                                        "Total Uptime In Minutes": <Uptime
Duration>
                                    }]
}
```

アラートポリシーの条件

以下に、アラートカテゴリ、アラートを軽減するための推奨されるアクション、および定義されている場合は組み込みのポリシー条件を示します。組み込みのアラートポリシーは、60分のアラート間隔と再アラート間隔で定義されています。

接続セッションのピーク

- 接続セッションのピークについては、Directorのセッショントレンドビューを確認してください。
- セッション負荷に対応する十分な容量があることを確認してください。
- 必要に応じて新しいマシンを追加する

切断セッションのピーク

- 切断セッションのピークについては、Directorのセッショントレンドビューを確認してください。
- セッション負荷に対応する十分な容量があることを確認してください。
- 必要に応じて新しいマシンを追加する。
- 必要に応じて切断されたセッションをログオフする

同時セッション合計のピーク

- 同時セッションのピークについては、Directorのセッショントレンドビューを確認してください。
- セッション負荷に対応する十分な容量があることを確認してください。
- 必要に応じて新しいマシンを追加する。

- 必要に応じて、切断されたセッションをログオフします。

CPU

CPU使用率の割合は、プロセスを含むVDA全体のCPU消費量を示します。対応するVDAの**マシン詳細**ページから、個々のプロセスによるCPU使用率についてさらに詳しく知ることができます。

- **> >** に移動し、CPU を消費しているプロセスを特定します。プロセスレベルのリソース使用状況統計の収集を開始するには、プロセス監視ポリシーが有効になっていることを確認してください。
- 必要に応じてプロセスを終了します。
- プロセスを終了すると、保存されていないデータが失われます。
- すべてが期待どおりに機能している場合は、将来的に追加のCPUリソースを追加します。

> **注:**
>
> ポリシー設定**リソース監視を有効にする**は、VDAがインストールされたマシンでのCPUおよびメモリのパフォーマンスカウンターの監視に対して、デフォルトで許可されています。このポリシー設定が無効になっている場合、CPUおよびメモリの状態に関するアラートはトリガーされません。詳細については、監視ポリシー設定を参照してください。
>
> **スマートポリシー条件:**

- **スコープ：** デリバリーグループ、マルチセッションOSスコープ
- **しきい値：** 警告 - 80%、クリティカル - 90%

メモリ

メモリ使用率の割合は、プロセスを含むVDA全体のメモリ消費量を示します。対応するVDAの**マシン詳細**ページから、個々のプロセスによるメモリ使用量についてさらに詳しく知ることができます。

- **［マシン詳細］>［履歴使用率の表示］>［上位10プロセス］** に移動し、メモリを消費しているプロセスを特定します。プロセスレベルのリソース使用状況統計の収集を開始するには、プロセス監視ポリシーが有効になっていることを確認してください。
- 必要に応じてプロセスを終了します。
- プロセスを終了すると、保存されていないデータが失われます。

- すべてが期待どおりに機能している場合は、将来的に追加のメモリを追加します。

> **注:**
>
> ポリシー設定 ［**リソース監視を有効にする**］ は、VDAがインストールされたマシンでのCPUおよびメモリのパフォーマンスカウンターの監視に対して、デフォルトで許可されています。このポリシー設定が無効になっている場合、CPUおよびメモリの状態に関するアラートはトリガーされません。詳しくは、「監視ポリシー設定」を参照してください。

> **スマートポリシー条件:**
>
> - **スコープ：** デリバリーグループ、マルチセッションOSスコープ
> - **閾値:** 警告 - 80%、危機的 - 90%

接続失敗率

過去1時間の接続失敗の割合。

- 試行された接続の総数に対する総失敗数に基づいて計算されます。
- 構成ログから記録されたイベントについては、Directorの接続失敗傾向ビューを確認してください。
- アプリケーションまたはデスクトップに到達可能かどうかを判断します。

接続失敗数

過去1時間の接続失敗数。

- Director接続失敗トレンドビューで、構成ログから記録されたイベントを確認します。
- アプリケーションまたはデスクトップに到達可能かどうかを判断します。

ICA® RTT (平均)

平均ICAラウンドトリップ時間。

- ICA RTTの内訳についてCitrix ADMを確認し、根本原因を特定します。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、Directorのユーザー詳細ビューでICA RTTと遅延を確認し、それがネットワークの問題なのか、アプリケーションまたはデスクトップの問題なのかを判断します。

ICA RTT (セッション数)

しきい値のICAラウンドトリップ時間を超えるセッション数。

- ICA RTTが高いセッション数についてCitrix ADMを確認します。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、ネットワークチームと協力して根本原因を特定します。

  スマートポリシーの条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 5セッション以上で300ミリ秒、重大 - 10セッション以上で400ミリ秒

ICA RTT (セッションの割合)

平均ICAラウンドトリップ時間を超えるセッションの割合。

- ICA RTTが高いセッション数についてCitrix ADMを確認します。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、ネットワークチームと協力して根本原因を特定します。

ICA RTT (ユーザー)

指定されたユーザーによって起動されたセッションに適用されるICAラウンドトリップ時間。少なくとも1つのセッションでICA RTTがしきい値を超えると、アラートがトリガーされます。

障害が発生したマシン (シングルセッションOS)

障害が発生したシングルセッションOSマシンの数。障害は、Directorのダッシュボードとフィルタービューに示されているように、さまざまな理由で発生する可能性があります。

- Citrix Scout診断を実行して根本原因を特定します。

  スマートポリシー条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 1、重大 - 2

障害が発生したマシン (マルチセッションOS)

障害が発生したマルチセッションOSマシンの数。障害は、Directorのダッシュボードとフィルタービューに示されているように、さまざまな理由で発生する可能性があります。

- Citrix Scout診断を実行して根本原因を特定します。

  スマートポリシー条件:

- **スコープ:** デリバリーグループ、マルチセッションOSスコープ
- **しきい値:** 警告 - 1、重大 - 2

失敗したマシン (割合)

配信グループ内の失敗したシングルセッションおよびマルチセッションOSマシンの割合で、失敗したマシンの数に基づいて計算されます。このアラート条件では、配信グループ内の失敗したマシンの割合としてアラートしきい値を構成でき、30秒ごとに計算されます。 障害は、Directorダッシュボードおよびフィルタービューに示されているように、さまざまな理由で発生する可能性があります。根本原因を特定するには、Citrix Scout診断を実行してください。詳細については、「ユーザーの問題のトラブルシューティング」を参照してください。

失敗した電源オンアクションと失敗した電源オフアクション

配信グループ内の失敗した電源オンアクションの数と失敗した電源オフアクションの数で、電源オンまたはオフに失敗した**電源管理マシン**の数に基づいて計算されます。このアラート条件では、配信グループ内で電源オンまたはオフに失敗した**電源管理マシン**の数としてアラートしきい値を構成でき、30分ごとに計算されます。

管理者は、高度なアラートポリシーでこれらのアラートに対して次のパラメーターを構成できます。

- トリガー元: 電源アクションをトリガーしたもの
- 失敗の理由: アクションが失敗した理由
- しきい値: ポリシーをトリガーするために電源アクションに失敗したマシンのしきい値の数
- サンプリング間隔: 失敗した電源アクションをチェックする必要がある間隔
- 再アラート間隔: アラートを再送信するまでの時間

障害は、Directorダッシュボードおよびフィルタービューに示されているように、さまざまな理由で発生する可能性があります。根本原因を特定するには、Citrix Scout診断を実行してください。詳細については、「ユーザーの問題のトラブルシューティング」を参照してください。

未登録マシン（%）

マシンが再起動によって不安定になった場合、またはデリバリーコントローラーと仮想マシン間の通信に問題がある場合、マシンは未登録と見なされます。**未登録のマシン（%）**は、配信グループ内の未登録のシングルセッションおよびマルチセッションOSマシンの割合で、未登録のマシンの数に基づいて計算されます。このアラート条件では、配信グループ内の未登録のマシンの割合として警告および重大なしきい値を構成できます。再アラートの間隔を設定できます。また、**未登録のマシン（%）の条件が満たされたときに通知を受け取るためにメールを追加することもできます。重大または警告のしきい値を超えると、アラートとメールが生成されます。アラートは**

Citrix Alertsの下で表示できます。**未登録のマシン（%）**カテゴリで、必要な状態と時間でフィルターできます。

メールがある場合はCSV添付ファイルで、Webhookがある場合はJSONペイロードを介してアラートの詳細を受け取ることもできます。

> **注:**
>
> クリティカル値は警告値よりも大きくする必要があります。

> **ポリシー条件:**

- **スコープ**：シングルセッションOS、およびマルチセッションOSデリバリーグループ
- **しきい値**：警告およびクリティカル

マシンの稼働時間アラート

デリバリーグループ内のマシンの稼働時間は、デリバリーグループ内でマシンがオンになっている1日あたりの時間数、1週間あたりの時間数、または1か月あたりの時間数に基づいて計算されます。このアラート条件を使用すると、デリバリーグループ内でマシンがオンになっている時間をアラートしきい値として構成できます。マシンの稼働時間アラートは、次の場合に機能します。

- 1日あたりの時間数 - マシンが1日オンになっている時間数を指定でき、30分ごとに計算されます。設定できる1日あたりの最大時間数は24時間です。
- 1週間あたりの時間数 - マシンが1週間オンになっている時間数を指定でき、6時間ごとに計算されます。設定できる1週間あたりの最大時間数は168時間です。
- 1か月あたりの時間数 - マシンが1か月オンになっている時間数を指定でき、毎日1回計算されます。1か月あたりの最大時間数は720時間です。 設定できる再アラート間隔の最小値は60分です。警告およびクリティカルアラートセクションで、マシンの稼働時間しきい値を超えたマシンの数を入力できます。任意のマシンに例外を追加することもできます。

たとえば、このアラートに5つのデリバリーグループが追加されており、最初のデリバリーグループと4番目のデリバリーグループでマシンの数が警告またはクリティカルしきい値を超えた場合、アラートは最初のデリバリーグループと4番目のデリバリーグループに対して個別にトリガーされます。

このアラートは、管理者がマシンの稼働時間を分析するのに役立ち、この分析に基づいて管理者はコストの最適化に貢献できます。メールがある場合はCSV添付ファイルで、Webhookがある場合はJSONペイロードでアラートの詳細を受け取ることもできます。

平均ログオン時間

過去1時間に発生したログオンの平均ログオン時間。

- Directorダッシュボードをチェックして、ログオン時間に関する最新のメトリックを取得します。短期間に多くのユーザーがログインすると、ログオン時間が増加する可能性があります。
- ログオンのベースラインと内訳を確認して、原因を絞り込みます。詳細については、「ユーザーログオンの問題の診断」を参照してください。

  スマートポリシー条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 45秒、重大 - 60秒

ログオン時間（ユーザー）

過去1時間に発生した、指定されたユーザーのログオンのログオン時間。

負荷評価インデックス

過去5分間の負荷評価インデックスの値。

- Directorで、ピーク負荷（最大負荷）が発生している可能性のあるマルチセッションOSマシンを確認します。ダッシュボード（障害）とトレンドのロード評価インデックスレポートの両方を表示します。

  スマートポリシーの条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 80%、重大 - 90%

Webhook を使用してアラートポリシーを構成する

電子メール通知とは別に、Webhook を使用してアラートポリシーを構成できます。

注: この機能には、Delivery Controller バージョン 7.11 以降が必要です。

PowerShell コマンドレットを使用して、HTTP コールバックまたは HTTP POST でアラートポリシーを構成できます。これらは Webhook をサポートするように拡張されています。

新しい Octoblu ワークフローの作成と、対応する Webhook URL の取得については、Octoblu Developer Hub を参照してください。

新しいアラートポリシーまたは既存のポリシーの Webhook URL を構成するには、次の PowerShell コマンドレットを使用します。

Webhook URLを使用して新しいアラートポリシーを作成します:

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -Description
<Policy description> -Enabled $true -Webhook <Webhook URL>
```

既存のアラートポリシーに Webhook URL を追加する:

```
Set-MonitorNotificationPolicy - Uid <Policy id> -Webhook <Webhook URL>
```

PowerShellコマンドのヘルプについては、PowerShellヘルプを使用してください。例:

```
Get-Help  <Set-MonitorNotificationPolicy>
```

アラートポリシーから生成された通知は、Webhook URL への POST 呼び出しで Webhook をトリガーします。POST メッセージには、JSON 形式の通知情報が含まれています。

```
{"NotificationId" : \<Notification Id\>,


"Target" : \<Notification Target Id\>,


"Condition" : \<Condition that was violated\>,


"Value" : \<Threshold value for the Condition\>,


"Timestamp": \<Time in UTC when notification was generated\>,


"PolicyName": \<Name of the Alert policy\>,


"Description": \<Description of the Alert policy\>,
```

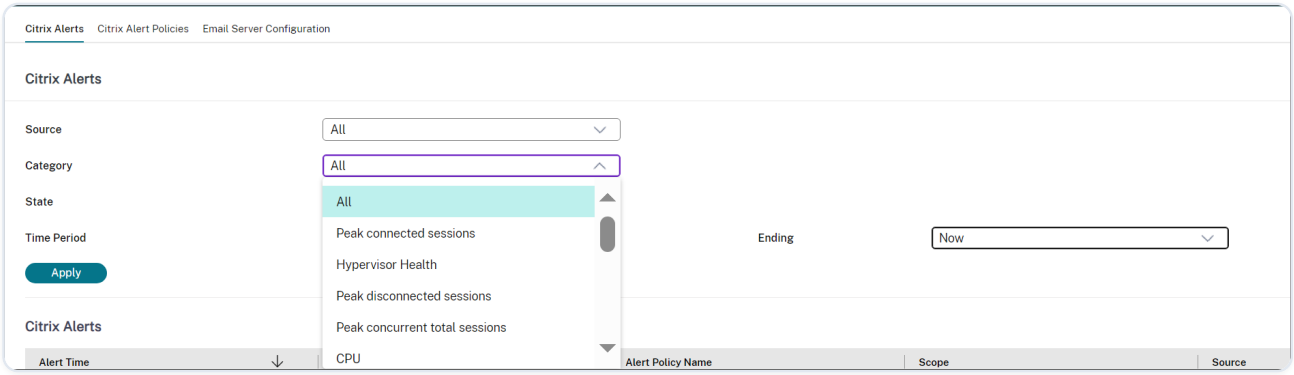
```
"Scope" : \<Scope of the Alert policy\>,

"NotificationState": \<Notification state critical, warning, healthy or
dismissed\>,

"Site" : \<Site name\>}
```

ハイパーバイザーアラートの監視

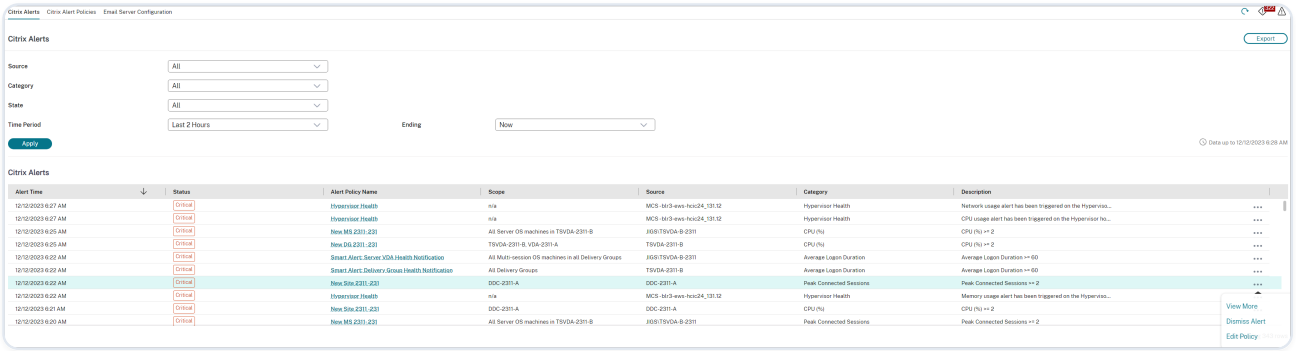
Directorは、ハイパーバイザーの健全性を監視するためのアラートを表示します。XenServer®およびVMware vSphereからのアラートは、ハイパーバイザーのパラメーターと状態の監視に役立ちます。ハイパーバイザーへの接続ステータスも監視され、ホストのクラスターまたはプールが再起動されたり利用できなくなったりした場合にアラートが提供されます。



ハイパーバイザーアラートを受信するには、Web Studioでホスティング接続が作成されていることを確認してください。詳細については、「接続とリソース」を参照してください。ハイパーバイザーアラートの監視対象となるのは、これらの接続のみです。

これらのアラートは、しきい値に達するか、またはしきい値を超過すると表示されます。ハイパーバイザーアラートは次のとおりです。

- 致命的 — ハイパーバイザーアラームポリシーの致命的なしきい値に達したか、または超過した
- 警告 — ハイパーバイザーアラームポリシーの警告しきい値に達したか、または超過した
- 却下済み — アラートがアクティブなアラートとして表示されなくなった



この機能には、Delivery Controllerバージョン7 1811以降が必要です。サイト7 1811以降でDirectorの古いバージョンを使用している場合、ハイパーバイザーアラートの数のみが表示されます。アラートを表示するには、Directorをアップグレードする必要があります。

次の表では、ハイパーバイザーアラートのさまざまなパラメーターと状態について説明します。

アラート	サポートされているハイパーバイザー	トリガー元	条件	構成
CPU使用率	ゼノサーバー、ブイエムウェアブイスフィア	ハイパーバイザー	CPU使用率アラートのしきい値に達したか、超えた場合	アラートのしきい値はハイパーバイザーで構成する必要があります。
メモリ使用率	ゼノサーバー、ブイエムウェアブイスフィア	ハイパーバイザー	メモリ使用量アラートのしきい値に達したか、超えました	アラートのしきい値はハイパーバイザーで構成する必要があります。
ネットワーク使用量	ゼノサーバー、ブイエムウェアブイスフィア	ハイパーバイザー	ネットワーク使用量アラートのしきい値に達したか、超えました	アラートのしきい値はハイパーバイザーで構成する必要があります。
ディスク使用量	ブイエムウェアブイスフィア	ハイパーバイザー	ディスク使用量アラートのしきい値に達したか、超えました	アラートのしきい値はハイパーバイザーで構成する必要があります。

アラート	サポートされているハイパーバイザー	トリガー元	条件	構成
ホスト接続または電源状態	ブイエムウェアブイスフィア	ハイパーバイザー	ハイパーバイザーホストが再起動されたか、利用できません	アラートはVMware vSphereに組み込まれています。追加の設定は不要です。
ハイパーバイザー接続が利用できません	ゼノサーバー、VMware vSphere	デリバリーコントローラー	ハイパーバイザー（プールまたはクラスター）への接続が失われたか、電源がオフになったか、再起動されました。このアラートは、接続が利用できない間は1時間ごとに生成されます。	アラートはDelivery Controllerに組み込まれています。追加の設定は不要です。

注：

アラートの設定の詳細については、Citrix XenCenter Alerts を参照するか、VMware vCenter Alertsのドキュメントを確認してください。

メール通知の設定は、**Citrix Alerts Policy > Site Policy > Hypervisor Health** で構成できます。ハイパーバイザーアラートポリシーのしきい値条件は、Directorからではなく、ハイパーバイザーからのみ構成、編集、無効化、または削除できます。ただし、メール設定の変更やアラートの解除はDirectorで行うことができます。インフラストラクチャの監視に関与しない役割の場合は、アラートを無効にできます。

重要：

- ハイパーバイザーによってトリガーされたアラートはDirectorで取得および表示されます。ただし、ハイパーバイザーアラートのライフサイクル/状態の変更はDirectorには反映されません。
- ハイパーバイザーコンソールで正常または解除済みまたは無効になっているアラートは、Directorに引き続き表示され、明示的に解除する必要があります。
- Directorで解除されたアラートは、ハイパーバイザーコンソールでは自動的に解除されません。

障害のトラブルシューティングを行うためのデータフィルタリング

ダッシュボードの数値をクリックするか、フィルターメニューから事前定義されたフィルターを選択すると、フィルタービューが開き、選択したマシンまたは障害タイプに基づいてデータが表示されます。

事前定義されたフィルターは編集できませんが、事前定義されたフィルターをカスタムフィルターとして保存し、その後変更できます。また、すべてのデリバリーグループにわたるマシン、接続、セッション、およびアプリケーションインスタンスのカスタムフィルタービューを作成できます。

1. ビューを選択します:

   - **マシン**。シングルセッションOSマシンまたはマルチセッションOSマシンを選択します。これらのビューには、構成されたマシンの数が表示されます。マルチセッションOSマシンのタブには、パフォーマンスカウンターの分布を示すロードエバリュエーターインデックスと、リンクにカーソルを合わせると表示されるセッション数のツールヒントも含まれています。
   - **セッション**。過去60分、過去24時間、過去7日間、またはカスタム期間など、異なる期間でセッションをフィルターします。セッションビューからセッション数を確認することもできます。アイドル時間の測定値を使用して、しきい値期間を超えてアイドル状態になっているセッションを特定します。**関連ユーザー**をクリックすると、そのユーザーのアクティビティマネージャーが開きます。**エンドポイント**名をクリックすると、そのエンドポイントのアクティビティマネージャーが開きます。**詳細の表示**をクリックすると、それぞれ**ユーザーの詳細**ページまたは**エンドポイントの詳細**ページが開きます。詳細については、「ユーザーの詳細」を参照してください。
   - **接続**。過去60分、過去24時間、過去7日間、またはカスタム期間など、異なる期間で接続をフィルターします。
   - **アプリケーションインスタンス**。過去60分、過去24時間、過去7日間、またはカスタム期間など、異なる期間でアプリケーションインスタンスをフィルターします。このビューに

は、サーバーおよびシングルセッションOSのVDA上のすべてのアプリケーションインスタンスのプロパティが表示されます。マルチセッションOSのVDA上のアプリケーションインスタンスでは、セッションアイドル時間の測定値が利用可能です。

> **注:**
>
> Windows 10 1809コンピューターにインストールされたVDAでデスクトップセッションを起動した場合、Directorのアクティビティマネージャーは、Microsoft EdgeとOfficeがアクティブに実行されているアプリケーションとして表示されることがありますが、実際にはバックグラウンドでのみ実行されています。

2. **Filter by**で、条件を選択します。
3. 必要に応じて、各ビューの追加タブを使用してフィルターを完了します。
4. 必要に応じて、追加の列を選択して、さらにトラブルシューティングを行います。
5. フィルターを保存して名前を付けます。
6. 複数のDirectorサーバーからフィルターにアクセスするには、それらのサーバーからアクセス可能な共有フォルダーにフィルターを保存します。
   - 共有フォルダーは、Directorサーバー上のアカウントに対して変更権限を持っている必要があります。
   - Directorサーバーは、共有フォルダーにアクセスするように構成する必要があります。構成するには、**IIS Manager**を実行します。**Sites \> Default Web Site \> Director\ > Application Settings**で、**Service.UserSettingsPath**設定を共有フォルダーのUNCパスを反映するように変更します。
7. 後でフィルターを開くには、**Filters**メニューからフィルターの種類（Machines、Sessions、Connections、またはApplication Instances）を選択し、保存されたフィルターを選択します。
8. **Export**をクリックして、データをCSV形式ファイルにエクスポートします。最大100,000レコードのデータをエクスポートできます。この機能は、Delivery Controller™バージョン1808以降で利用できます。
9. 必要に応じて、**Machines**または**Connections**ビューでは、フィルターされたリストで選択したすべてのマシンに対して電源制御を使用します。Sessionsビューでは、セッション制御またはメッセージ送信オプションを使用します。
10. **Machines**ビューと**Connections**ビューで、失敗したマシンまたは接続の**Failure Reason**をクリックすると、障害の詳細な説明と、障害のトラブルシューティングに推奨されるアクション

が表示されます。マシンおよび接続の障害理由と推奨されるアクションについては、Citrix Directorの障害理由とトラブルシューティングを参照してください。

11. **Machines**ビューで、マシン名リンクをクリックすると、対応する**Machine Details**ページに移動します。このページには、マシンの詳細が表示され、電源制御が提供され、CPU、メモリ、ディスク監視、およびGPU監視グラフが表示されます。また、**View Historical Utilization**をクリックすると、マシンのリソース使用率の傾向を確認できます。詳細については、マシンのトラブルシューティングを参照してください。
12. **Application Instances**ビューで、しきい値期間より長い**Idle Time**に基づいて並べ替えまたはフィルター処理を行います。終了するアイドル状態のアプリケーションインスタンスを選択します。アプリケーションインスタンスのログオフまたは切断は、同じセッション内のすべてのアクティブなアプリケーションインスタンスを終了します。詳細については、アプリケーションのトラブルシューティングを参照してください。Director、Delivery Controllers、およびVDAがバージョン7.13以降の場合、Application InstancesフィルターページとSessionsフィルターページでのアイドル時間測定が利用可能です。

> **注:** Web Studioでは、デリバリーグループ内の単一のVDAに対して、異なるユーザーまたはユーザーグループに複数のデスクトップ割り当てルール（DAR）を割り当てることができます。StoreFront™は、ログインユーザーのDARに従って、対応する表示名で割り当てられたデスクトップを表示します。ただし、DirectorはDARをサポートしておらず、ログインユーザーに関係なく、デリバリーグループ名を使用して割り当てられたデスクトップを表示します。その結果、Directorで特定のデスクトップをマシンにマッピングすることはできません。StoreFrontに表示される割り当てられたデスクトップをDirectorに表示されるデリバリーグループ名にマッピングするには、次のPowerShellコマンドを使用します。

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq "\<Name
on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property Name, Uid
```

サイト全体の履歴トレンドを監視する

トレンドビューは、以下のパラメータについて、各サイトの履歴トレンド情報にアクセスします。

- セッション
- 接続障害
- マシンの障害
- ログオンパフォーマンス

- 負荷評価
- キャパシティ管理
- マシン使用状況
- リソース使用率
- 各サイトのネットワーク分析。

この情報を見つけるには、**トレンド**メニューをクリックします。

ズームインしてドリルダウンする機能を使用すると、期間を拡大（グラフ内のデータポイントをクリック）してトレンドチャートをナビゲートし、トレンドに関連する詳細を確認できます。この機能により、誰が、または何が影響を受けているかの詳細をよりよく理解できます。

各グラフのデフォルトのスコープを変更するには、データに別のフィルターを適用します。

履歴トレンド情報が必要な期間を選択してください。期間の利用可能性は、Directorの展開によって次のように異なります。

- Premiumライセンスサイトでは、最大1年間 (365日間) のトレンドレポートを利用できます。
- Advancedライセンスサイトでは、最大1か月間 (31日間) のトレンドレポートを利用できます。
- PremiumおよびAdvanced以外のライセンスサイトでは、最大7日間のトレンドレポートを利用できます。

注:

- すべてのDirector展開において、期間が「先月」（**現在まで**）またはそれより短い期間に設定されている場合、セッション、障害、およびログオンパフォーマンスのトレンド情報はグラフとテーブルとして利用できます。期間がカスタム終了日を指定した「先月」または「昨年」として選択されている場合、トレンド情報はグラフとして利用でき、テーブルとしては利用できません。
- Monitor Serviceのグルーミング保持値は、トレンドデータの可用性を制御します。デフォルト値は、データ粒度と保持で確認できます。Premiumライセンスサイトのお客様は、グルーミング保持を希望する保持日数に変更できます。
- IIS Managerの以下のパラメーターは、選択可能なカスタム終了日の範囲を制御します。ただし、選択された日付のデータ可用性は、測定されている特定のメトリックのグルーミング保持設定に依存します。

パラメーター	デフォルト値
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

利用可能なトレンド

セッションの傾向を表示する： セッションタブから、デリバリーグループと期間を選択して、同時セッション数に関する詳細情報を表示します。

「**セッション自動再接続**」列には、セッション内の自動再接続の数が表示されます。セッションの信頼性またはクライアント自動再接続ポリシーが有効な場合、自動再接続が有効になります。エンドポイントでネットワークの中断が発生した場合、次のポリシーが適用されます。

- セッションの信頼性が適用され（デフォルトで3分間）、Citrix Receiver™またはCitrix Workspace™アプリがVDAへの接続を試行します。
- クライアント自動再接続が3分から5分の間に適用され、クライアントがVDAへの接続を試行します。

両方の再接続がキャプチャされ、ユーザーに表示されます。この情報は、再接続が発生してからDirector UIに表示されるまでに最大5分かかる場合があります。

自動再接続情報は、中断のあるネットワーク接続の表示とトラブルシューティングに役立ちます。また、シームレスなエクスペリエンスを持つネットワークも分析します。フィルターで選択した特定のデリバリーグループまたは期間の再接続数を表示できます。ドリルダウンでは、セッションの信頼性やクライアント自動再接続、タイムスタンプ、エンドポイントIP、Workspaceアプリがインストールされているマシンのエンドポイント名などの追加情報が提供されます。

デフォルトでは、ログはイベントタイムスタンプの降順でソートされます。この機能は、Windows版Citrix Workspaceアプリ、Mac版Citrix Workspaceアプリ、Windows版Citrix Receiver、およびMac版Citrix Receiverで利用できます。この機能には、Delivery Controller™バージョン7 1906以降、およびVDAs 1906以降が必要です。

セッションの再接続の詳細については、「セッション」を参照してください。

ポリシーの詳細については、「クライアント自動再接続ポリシー設定」および「セッションの信頼性ポリシー設定」を参照してください。

自動再接続データがDirectorに表示されない場合があります。その理由は次のとおりです。

- Workspaceアプリが自動再接続データをVDAに送信していません。
- VDAがモニターサービスにデータを送信していません。
- Delivery Controllers は、対応するセッションがない可能性があるため、VDA ペイロードを破棄します。

> **注:**
>
> 特定のCitrix Gatewayポリシーが設定されている場合、クライアントIPアドレスが正しく取得されないことがあります。

> **接続障害の傾向を表示:** 「障害」タブから、接続、マシンタイプ、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のユーザー接続障害に関する詳細情報を含むグラフを表示します。

マシン障害の傾向を表示: Single-session OS Machine FailuresタブまたはMulti-session OS Machinesタブから、障害タイプ、デリバリーグループ、および期間を選択すると、サイト全体のマシン障害に関する詳細情報を含むグラフが表示されます。

ログオンパフォーマンスの傾向を表示: ログオンパフォーマンスタブから、デリバリーグループと期間を選択すると、サイト全体のユーザーログオン時間の詳細情報と、ログオン数がパフォーマンスに影響するかどうかを示すグラフが表示されます。このビューには、ブローカー処理時間やVM起動時間など、ログオンフェーズの平均期間も表示されます。 このデータはユーザーログオン専用であり、切断されたセッションから再接続しようとしているユーザーは含まれません。 グラフの下の表には、ユーザーセッションごとのログオン期間が表示されます。表示する列を選択し、任意の列でレポートを並べ替えることができます。これらのレポートを.CSVファイルにエクスポートすることもできます。 詳細については、「ユーザーログオンの問題の診断」を参照してください。

負荷評価の傾向を表示: Load Evaluator Indexタブから、Multi-session OSマシン間で分散される負荷に関する詳細情報を含むグラフを表示します。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のMulti-session OSマシン、Multi-session OSマシ

ン（デリバリーグループ内のMulti-session OSマシンが選択されている場合にのみ利用可能）、および範囲が含まれます。

ホストされたアプリケーションの使用状況を表示する: この機能の利用可能性は、組織のライセンスによって異なります。 **キャパシティ管理**タブから、**ホストされたアプリケーションの使用状況**タブを選択します。デリバリーグループと期間を選択して、ピーク時の同時使用状況を示すグラフと、アプリケーションベースの使用状況を示す表を表示します。アプリケーションベースの使用状況の表から、特定のアプリケーションを選択して、詳細と、そのアプリケーションを使用している、または使用したユーザーのリストを表示できます。

Single-sessionおよびMulti-session OSの使用状況を表示: トレンドビューには、サイト別およびデリバリーグループ別のSingle-session OSの使用状況が表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、ユーザーごとの使用状況が表示されます。 トレンドビューには、サイト別、デリバリーグループ別、およびマシン別のMulti-session OSの使用状況も表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、マシンごとおよびユーザーごとの使用状況が表示されます。マシンが選択されている場合は、ユーザーごとの使用状況が表示されます。

仮想マシンの使用状況を表示: マシン使用状況タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択すると、VMの使用状況をリアルタイムで確認でき、サイトのキャパシティニーズを迅速に評価できます。 シングルセッションOSの可用性 - サイト全体または特定のデリバリーグループにおけるシングルセッションOSマシン（VDI）の可用性による現在の状態を表示します。 マルチセッションOSの可用性 - サイト全体または特定のデリバリーグループにおけるマルチセッションOSマシンの可用性による現在の状態を表示します。

> **注:** 利用可能なカウンターに表示されるマシンの数には、メンテナンスモードのマシンが含まれます。

> **リソース使用率を表示する: リソース使用率**タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択して、CPUとメモリの使用状況、および各VDIマシンのIOPSとディスク遅延に関する履歴傾向データを把握し、より適切なキャパシティプランニングに役立てます。 この機能には、Delivery ControllersとVDAの**バージョン7.11**以降が必要です。 グラフには、平均CPU、平均メモリ、平均IOPS、ディスク遅延、およびピーク時の同時セッションのデータが表示されます。マシンにドリルダウンして、CPUを消費している上位10個のプロセスのデータとグラフを表示できます。

デリバリーグループと期間でフィルターします。CPU、メモリ使用量、およびピーク時の同時セッションのグラフは、過去2時間、24時間、7日間、月、および年で利用できます。平均IOPSとディスク遅延のグラフは、過去24時間、月、および年で利用できます。

注:

- 履歴マシン使用率ページの「上位10プロセス」テーブルでデータを収集して表示するには、監視ポリシー設定の**プロセス監視を有効にする**を**許可**に設定する必要があります。このポリシーはデフォルトで**禁止**に設定されています。すべてのリソース使用率データはデフォルトで収集されます。これは、**リソース監視を有効にする**ポリシー設定を使用して無効にできます。グラフの下の表には、マシンごとのリソース使用率データが表示されます。詳細については、「監視ポリシー設定」を参照してください。
- 平均IOPSは日次平均を示します。ピークIOPSは、選択した時間範囲におけるIOPS平均の最高値として計算されます。(IOPS平均とは、VDAでその時間に収集されたIOPSの時間ごとの平均です)。
- マシンのドリルダウンには、平均CPU使用率または平均メモリ使用率が1%を超えるプロセスがリストされます。これは、リストされるプロセスが10未満になる場合があることを意味します。

ネットワーク分析データの表示: この機能の利用は、組織のライセンスと管理者権限によって異なります。この機能には、Delivery Controllers **バージョン7.11**以降が必要です。

ネットワークタブから、ネットワーク分析を監視します。これにより、ユーザー、アプリケーション、およびデスクトップのコンテキストでネットワークが表示されます。この機能により、DirectorはCitrix ADMからのHDX Insightレポートを通じて、展開環境におけるICAトラフィックの詳細な分析を提供します。詳しくは、「ネットワーク分析の構成」を参照してください。

アプリケーション障害の表示: アプリケーション障害タブには、VDA上の公開アプリケーションに関連する障害が表示されます。

この機能には、Delivery ControllersおよびVDAの**バージョン7.15**以降が必要です。Windows Vista以降を実行するシングルセッションOS VDA、およびWindows Server 2008以降を実行するマルチセッションOS VDAがサポートされています。 詳しくは、「履歴アプリケーション障害監視」を参照してください。

デフォルトでは、マルチセッションOS VDAからのアプリケーション障害のみが表示されます。監視ポリシーを使用して、アプリケーション障害の監視を設定できます。詳細については、「監視ポリシー設定」を参照してください。

プローブ結果の表示: プローブ結果タブには、構成ページでプローブ用に構成されたアプリケーションおよびデスクトップのプローブ結果が表示されます。ここでは、障害が発生した起動の段階が記録されます。

詳しくは、「アプリケーションおよびデスクトップのプローブ」を参照してください。

カスタマイズされたレポートの作成: カスタムレポートタブは、監視データベースからのリアルタイムデータと履歴データを含むカスタムレポートを表形式で生成するためのユーザーインターフェイスを提供します。

この機能には、Delivery Controllers **バージョン7.12**以降が必要です。

以前に保存したカスタムレポートクエリのリストから、**実行してダウンロード**をクリックしてレポートをCSV形式でエクスポートしたり、**ODataをコピー**をクリックして対応するODataクエリをコピーして共有したり、**編集**をクリックしてクエリを編集したりできます。 マシン、接続、セッション、またはアプリケーションインスタンスに基づいてカスタムレポートクエリを作成できます。マシン、デリバリーグループ、期間などのフィールドに基づいてフィルター条件を指定します。カスタムレポートに必要な追加の列を指定します。プレビューにはレポートデータのサンプルが表示されます。カスタムレポートクエリを保存すると、保存されたクエリのリストに追加されます。

コピーしたODataクエリに基づいてカスタムレポートクエリを作成できます。これを行うには、ODataクエリオプションを選択し、コピーしたODataクエリを貼り付けます。結果のクエリを保存して後で実行できます。

> **注:** ODataクエリを使用して生成されたプレビューおよびエクスポートレポートの列名はローカライズされておらず、英語で表示されます。

> グラフ上のフラグアイコンは、特定の時間範囲における重要なイベントまたはアクションを示します。フラグの上にマウスを移動してクリックすると、イベントまたはアクションがリストされます。

> **注:**

- HDX™接続ログオンデータは、7より前のVDAでは収集されません。以前のVDAの場合、チャートデータは0として表示されます。
- Citrix Studioで削除されたデリバリーグループは、関連データが整理されるまでDirectorのトレンドフィルターで選択可能です。削除されたデリバリーグループを選択すると、保持期間までの利用可能なデータのグラフが表示されます。ただし、テーブルにはデータが表示されません。
- アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、新しいデリバリーグループの**リソース使用率と負荷評価インデックス**テーブルに、古いデリバリーグループと新しいデリバリーグループから統合されたメトリックが表示されます。

Autoscaleで管理されているマシンの監視

Autoscaleは、デリバリーグループ内の登録済みすべてのマルチセッションおよびシングルセッションOSマシンのプロアクティブな電源管理を可能にする電源管理機能です。Web Studioで、選択したデリバリーグループに対してAutoscaleを構成できます。詳しくは、「Autoscale」(/ja-jp/citrix-virtual-apps-desktops/2407/manage-deployment/autoscale.html)を参照してください。Directorを使用して、Autoscaleが有効なマシンの主要なメトリックを監視できます。

マシン使用状況

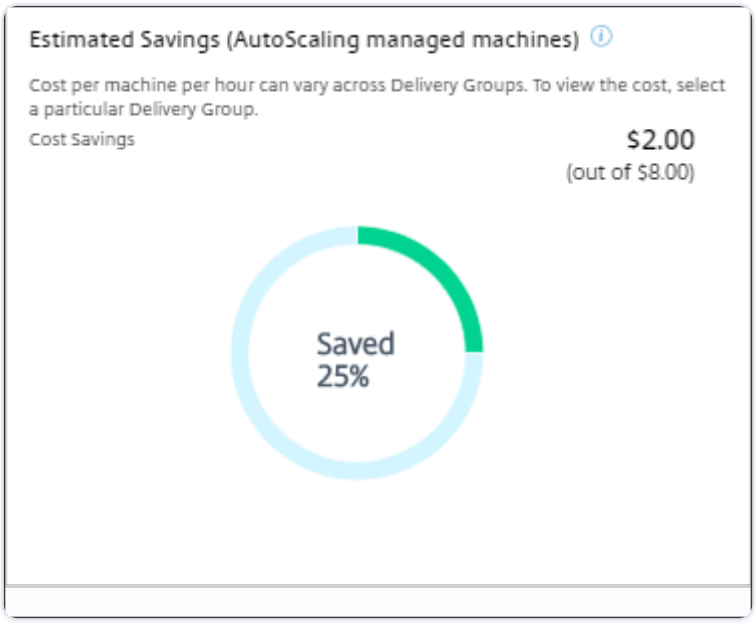
マシン使用状況ページには、選択したデリバリーグループと期間で電源がオンになっている、Autoscaleが有効なマルチセッションおよびシングルセッションOSマシンの合計数が表示されます。このメトリックは、デリバリーグループ内のマシンの実際の使用状況を示します。 **シングルセッションOSマシン**タブまたは**マルチセッションOSマシン**タブから、デリバリーグループと期間を選択します。

グラフには次のメトリックが表示されます。

- **電源オンのマシン** - 電源がオンになっているAutoscaleが有効なマシンの数
- **登録済みマシン** - 登録済みのマルチセッションまたはシングルセッションOSマシンの数
- **メンテナンス中のマシン** - メンテナンスモードがオンになっているマルチセッションまたはシングルセッションOSマシンの数

推定節約額

マシン使用状況ページには、選択したデリバリーグループでAutoscaleを有効にすることによって達成された推定コスト削減額も表示されます。



推定節約額は、**デリバリーグループの編集** > **Autoscale**で構成されているように、1時間あたりのマシンごとの節約額の割合（米ドル）として計算されます。マシンごとの節約額の構成について詳しくは、「Autoscale」(/ja-jp/citrix-virtual-apps-desktops/2407/manage-deployment/autoscale.html)を参照してください。

すべてのデリバリーグループを選択すると、すべてのデリバリーグループにおける推定節約額の平均値が表示されます。

推定節約額は、管理者が既存のインフラストラクチャを統合し、最大限の節約と利用率を達成するためのキャパシティを計画するのに役立ちます。

マシンとセッションのアラート通知

Director ダッシュボードには、さらにドリルダウンできるアラート通知が表示されます。アラートの詳細は、**アラート**ページに表示されます。

- デリバリーグループでアラートポリシーを作成するには、**アラート** > **Citrix アラートポリシー** > **デリバリーグループポリシー**に移動します。
- ここでは、次の警告および重大なしきい値を設定できます。
  - 失敗したマシン（シングルセッションOS）および失敗したマシン（マルチセッションOS）、,
  - デリバリーグループ内のピーク接続セッション、ピーク切断セッション、およびピーク同時合計セッション。
- デリバリーグループ内の対応するメトリックがしきい値に達すると、アラートが生成されます。

アラートポリシーの条件と新しいアラートポリシーの作成に関する詳細については、「アラートと通知」を参照してください。

マシンのステータス

- **フィルター** > **マシン**には、すべてのマシンの電源状態が表形式で表示されます。特定のデリバリーグループでフィルターできます。
- **フィルター** > **セッション**には、マシン名でフィルターして、関連するセッションとそのリアルタイムステータスが表示されます。
- **トレンド** > **セッション**で、デリバリーグループと期間を選択すると、セッションとその関連メトリックのトレンドが表示されます。

詳細については、「障害のトラブルシューティングのためのデータのフィルター」を参照してください。

負荷評価のトレンド

トレンド > **負荷評価インデックス**ページには、マルチセッションOSマシン間で分散される負荷に関する詳細情報を示すグラフが表示されます。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のマルチセッションOSマシン、マルチセッションOSマシン（デリバリーグループ内のマルチセッションOSマシンが選択されている場合にのみ利用可能）、および範囲が含まれます。負荷評価インデックスは、合計CPU、メモリ、ディスク、またはセッションの割合として表示され、最後の間隔での接続ユーザー数と比較して示されます。

展開のトラブルシューティング

アプリケーションのトラブルシューティング

アプリケーション分析

アプリケーションビューには、アプリケーションベースの分析が単一の統合ビューで表示され、アプリケーションのパフォーマンスを効率的に分析および管理するのに役立ちます。サイトで公開されているすべてのアプリケーションの正常性と使用状況に関する貴重な洞察を得ることができます。デフォルトビューは、上位の実行中のアプリケーションを特定するのに役立ちます。 この機能には、Delivery Controllersバージョン7.16以降およびVDAバージョン7.15以降が必要です。

アプリケーションページ(/en-us/citrix-virtual-apps-desktops/2407/media/dir-app-analytics.png)

プローブ結果列には、過去24時間で実行されたアプリケーションプローブの結果が表示されます。プローブ結果リンクをクリックすると、**トレンド** \> **アプリケーションプローブ結果**ページで

詳細を確認できます。アプリケーションプローブの構成方法の詳細については、「アプリケーションおよびデスクトップのプローブ」を参照してください。

インスタンス列には、アプリケーションの使用状況が表示されます。これは、現在実行中のアプリケーションインスタンスの数（接続済みおよび切断済みの両方のインスタンス）を示します。さらにトラブルシューティングを行うには、**インスタンス**フィールドをクリックして、対応する**アプリケーションインスタンス**フィルターページを表示します。ここで、ログオフまたは切断するアプリケーションインスタンスを選択できます。

> **注:**
>
> カスタムスコープ管理者には、Directorはアプリケーショングループの下に作成されたアプリケーションインスタンスを表示しません。すべてのアプリケーションインスタンスを表示するには、フル管理者である必要があります。詳細については、Knowledge Centerの記事「CTX256001」を参照してください。

> **アプリケーション障害**列と**アプリケーションエラー**列を使用して、サイトで公開されているアプリケーションの正常性を監視します。これらの列には、過去1時間に該当するアプリケーションの起動中に発生した障害とエラーの集計数が表示されます。選択したアプリケーションに対応する**トレンド** \> **アプリケーション障害**ページで障害の詳細を表示するには、**アプリケーション障害**または**アプリケーションエラー**フィールドをクリックします。

アプリケーション障害ポリシー設定は、障害とエラーの可用性と表示を管理します。ポリシーとその変更方法の詳細については、**監視ポリシー**設定の「アプリケーション障害監視のポリシー」を参照してください。

リアルタイムアプリケーション監視

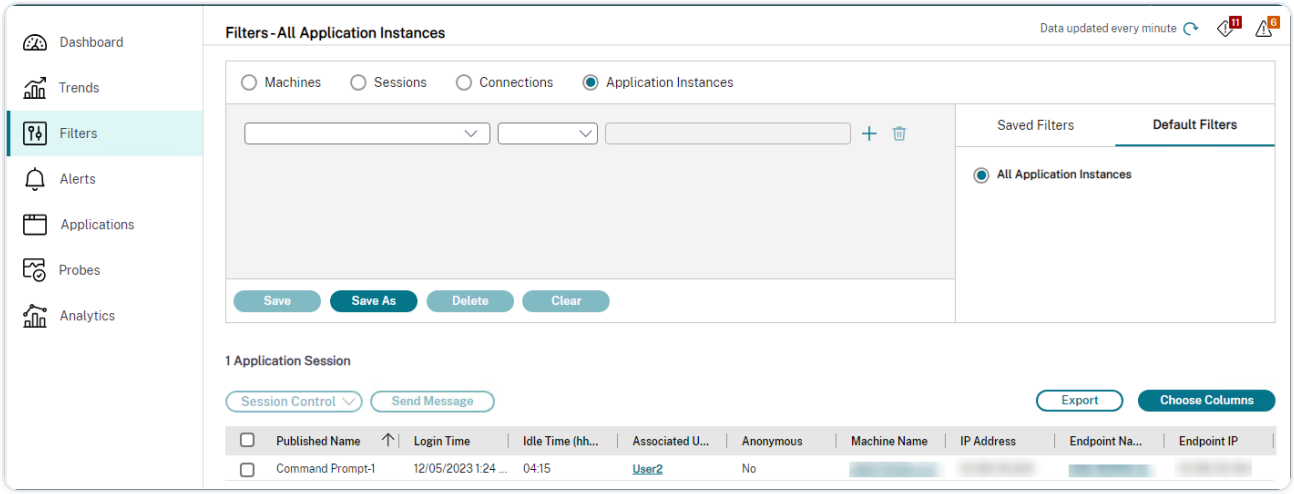
アイドル時間メトリックを使用して、特定の時間制限を超えてアイドル状態になっているインスタンスを特定することで、アプリケーションとセッションのトラブルシューティングを行うことができます。

アプリケーションベースのトラブルシューティングの典型的なユースケースは、従業員がアプリケーションライセンスを共有する医療分野にあります。そこでは、Citrix Virtual Apps and Desktops™環境をパージしたり、パフォーマンスの低いサーバーを再構成したり、アプリケーションを保守およびアップグレードしたりするために、アイドル状態のセッションとアプリケーションインスタンスを終了する必要があります。

アプリケーションインスタンスフィルターページには、サーバーおよびシングルセッションOSのVDA上のすべてのアプリケーションインスタンスが一覧表示されます。関連するアイドル時間測定値は、少なくとも10分間アイドル状態であったマルチセッションOSのVDA上のアプリケーションインスタンスに対して表示されます。

> **注：** アプリケーションインスタンスのメトリックは、すべてのライセンスエディションのサイトで利用できます。

この情報を使用して、特定の期間を超えてアイドル状態になっているアプリケーションインスタンスを特定し、必要に応じてログオフまたは切断します。これを行うには、**フィルター\> アプリケーションインスタンス**を選択し、事前に保存されたフィルターを選択するか、**すべてのアプリケーションインスタンス**を選択して独自のフィルターを作成します。

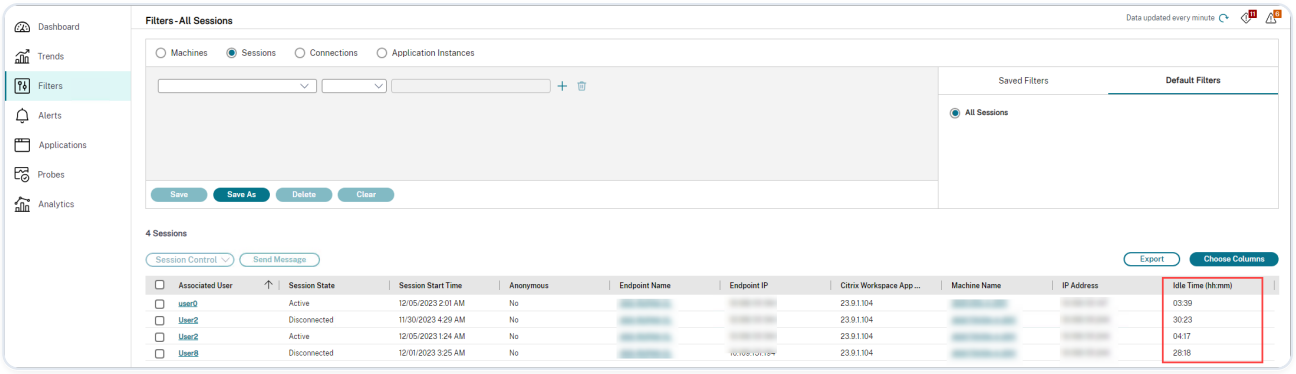


フィルターの例は次のとおりです。**フィルター条件**として、**公開名**（アプリケーションの）と**アイドル時間**を選択します。次に、**アイドル時間**を特定の時間制限の**以上**に設定し、再利用のためにフィルターを保存します。フィルターされたリストから、アプリケーションインスタンスを選択します。メッセージを送信するオプションを選択するか、**セッション制御**ドロップダウンから**ログオフ**または**切断**を選択してインスタンスを終了します。

> **注:** アプリケーションインスタンスをログオフまたは切断すると、現在のセッションがログオフまたは切断され、それによって、同じセッションに属するすべてのアプリケーションインスタンスが終了します。

セッションの状態とセッションアイドル時間のメトリックを使用して、**セッション**フィルターページからアイドルセッションを特定できます。**アイドル時間**列で並べ替えるか、特定の時間制限を超えてアイドル状態になっているセッションを特定するためのフィルターを定

義します。アイドル時間は、少なくとも10分間アイドル状態であったマルチセッションOSのVDA上のセッションに対して表示されます。



セッションまたはアプリケーションインスタンスが次の条件の場合、**アイドル時間**は**N/A**と表示されます。

- 10分以上アイドル状態になっていない場合、,
- シングルセッションOSのVDAで起動されている場合、または
- Version 7.12以前のVDAで起動されます。

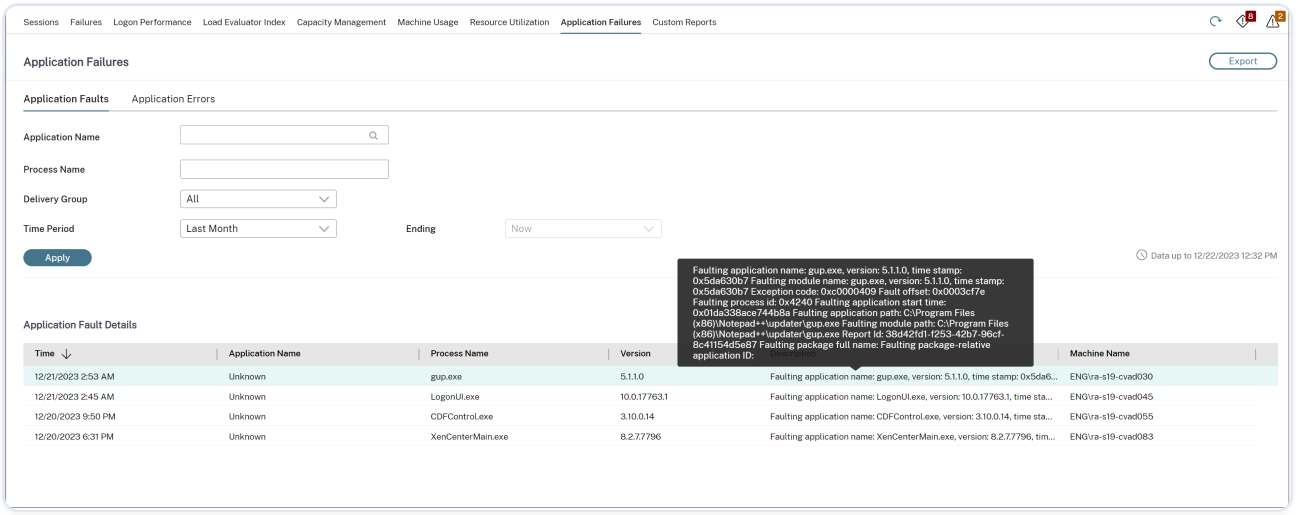
アプリケーション障害の履歴監視

トレンド -\> **アプリケーション障害**タブには、VDA上の公開アプリケーションに関連する障害が表示されます。

アプリケーション障害の傾向は、PremiumおよびAdvancedライセンスサイトでは過去2時間、24時間、7日間、および1か月間利用できます。その他のライセンスタイプでは、過去2時間、24時間、および7日間利用できます。イベントビューアにソース「Application Errors」としてログに記録されたアプリケーション障害が監視されます。**エクスポート**をクリックすると、CSV、Excel、またはPDF形式でレポートが生成されます。

アプリケーション障害監視のグルーミング保持設定であるGroomApplicationErrorsRetentionDaysとGroomApplicationFaultsRetentionDaysは、Premiumおよび非Premiumライセンスサイトの両方で、デフォルトで1日に設定されています。この設定は、PowerShellコマンドを使用して変更できます。

```
Set-MonitorConfiguration -\<setting name\> \<value\>
```



障害は、その重大度に基づいて**アプリケーション障害**または**アプリケーションエラー**として表示されます。アプリケーション障害タブには、機能またはデータの損失に関連する障害が表示されます。アプリケーションエラーは、すぐには関連しない問題を示します。これらは将来問題を引き起こす可能性のある状態を示します。

公開アプリケーション名、**プロセス名**、**デリバリーグループ**、および**期間**に基づいて障害をフィルタリングできます。テーブルには、障害またはエラーコードと、障害の簡単な説明が表示されます。詳細な障害の説明はツールチップとして表示されます。

> **注：** 対応するアプリケーション名を導出できない場合、公開アプリケーション名は「不明」と表示されます。これは通常、起動されたアプリケーションがデスクトップセッションで失敗した場合、または依存する実行可能ファイルによって引き起こされた未処理の例外が原因で失敗した場合に発生します。

> デフォルトでは、マルチセッションOS VDAでホストされているアプリケーションの障害のみが監視されます。監視グループポリシー（アプリケーション障害の監視を有効にする、シングルセッションOS VDAでのアプリケーション障害の監視を有効にする、障害監視から除外されるアプリケーションのリスト）を通じて監視設定を変更できます。詳細については、監視ポリシー設定のアプリケーション障害監視のポリシーを参照してください。

トレンド \> アプリケーションプローブ結果ページには、過去24時間および7日間にサイトで実行されたアプリケーションプローブの結果が表示されます。アプリケーションプローブの構成方法の詳細については、アプリケーションプローブを参照してください。

マシンのトラブルシューティング

> **注:**

> **Citrix Health Assistant** は、未登録のVDAにおける構成の問題をトラブルシューティングするためのツールです。このツールは、VDA登録の失敗やセッション起動、タイムゾーンリダイレクト構成の問題の根本原因を特定するために、いくつかのヘルスチェックを自動化します。Knowledge Centerの記事「Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch」には、**Citrix Health Assistant** ツールのダウンロードと使用方法が記載されています。

> Directorコンソールの **フィルター > マシン** ビューには、サイトで構成されているマシンが表示されます。「マルチセッションOSマシン」タブには、パフォーマンスカウンターの分布を示すロード評価インデックスと、リンクにカーソルを合わせるとセッション数のツールヒントが表示されます。

失敗したマシンの **Failure Reason** 列をクリックすると、失敗の詳細な説明と、その失敗をトラブルシューティングするために推奨されるアクションが表示されます。マシンおよび接続の失敗に関する失敗理由と推奨されるアクションは、「Citrix Director failure reasons and troubleshooting」で確認できます。

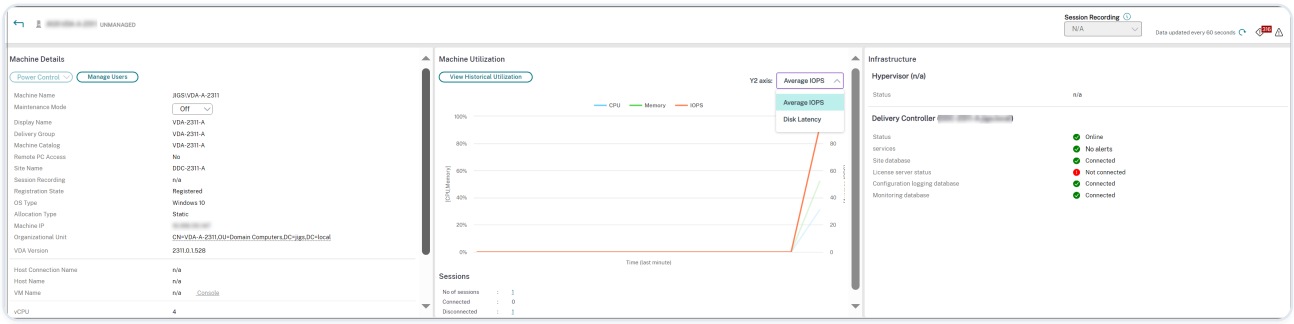
マシン名のリンクをクリックすると、**マシン詳細** ページに移動します。

マシン詳細ページには、マシンの詳細、インフラストラクチャの詳細、およびマシンに適用されたホットフィックスの詳細が一覧表示されます。

マシンベースのリアルタイムリソース使用率

Machine Utilization パネルには、CPUとメモリのリアルタイム使用率を示すグラフが表示されます。さらに、Delivery ControllerとVDAのバージョンが**7.14**以降のサイトでは、ディスクとGPUの監視グラフも利用できます。

ディスク監視グラフ、平均IOPS、ディスク遅延は、VDAディスクに関連する問題を監視およびトラブルシューティングするのに役立つ重要なパフォーマンス測定値です。平均IOPSグラフは、ディスクへの読み取りと書き込みの平均回数を表示します。**Disk Latency** を選択すると、データ要求からディスクからの応答までの遅延（ミリ秒単位）を示すグラフが表示されます。



GPU使用率

マルチセッションおよびシングルセッションOS VDAでGPU関連の問題をトラブルシューティングするには、**GPU Utilization** を選択して、GPU、GPUメモリ、およびエンコーダーとデコーダーの使用率（パーセンテージ）を確認します。

サポートされているGPUバージョン：

- Display Driverバージョン369.17以降を実行しているNVIDIA Tesla M60 GPU。詳細については、「NVIDIA vGPU Software」を参照してください。
- AMD Radeon Instinct MI25 GPU および AMD EPYC 7V12(Rome) CPU。詳細については、AMD Drivers and Support を参照してください。

ドライバー:

適切なドライバーまたは拡張機能をVDAにインストールする必要があります。

- NVIDIA GPU の場合、GRID ドライバーを手動で、または拡張機能経由でインストールします。詳細については、NVIDIA vGPU Software を参照してください。
  - NVIDIA の場合、GRID ドライバーのみがサポートされています。CUDA ドライバーは NVadsA10 v5 シリーズでは動作せず、サポートされていません。
  - Azure ベースのマシンに拡張機能経由で NVIDIA Grid GPU ドライバーをインストールするプロセス例については、NVIDIA GRID drivers. NVIDIA GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines を参照してください。
  - NVIDIA Grid GPU ドライバーを手動でインストールするプロセス例については、Azure N-series NVIDIA GPU driver setup for Windows - Azure Virtual Machines を参照してください。
- AMD GPU の場合、AMD グラフィックドライバーを手動で、または拡張機能経由でインストールします。詳細については、AMD Drivers and Support を参照してください。
  - Azure ベースのマシンに拡張機能経由で AMD GPU ドライバーをインストールするプロセス例については、AMD GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines を参照してください。
  - Azure マシンに AMD GPU ドライバーを手動でインストールするプロセス例については、Install AMD GPU drivers on N-series VMs running Windows を参照してください。

使用上の注意:

- GPU 使用率グラフは、64 ビット Windows を実行している VDA でのみ利用可能です。

- GPU アクセラレーションを提供するには、VDA で HDX 3D Pro を有効にする必要があります。詳細については、GPU acceleration for Windows Single-session OS および GPU acceleration for Windows Multi-session OS を参照してください。
- VDA が複数の GPU にアクセスする場合、使用率グラフには個々の GPU から収集された GPU メトリックの平均が表示されます。GPU メトリックは VDA 全体に対して収集され、個々のプロセスに対しては収集されません。
- AMD の場合、エンコーダーとデコーダーの使用状況は個別にサポートされていません。GPU を使用するエンコード/デコードのワークロードは、GPU 使用率における一般的な 3D 負荷として報告されます。
- NVIDIA WMI をインストール時に必ずインストールしてください。このウィンドウは手動インストール時のみ利用可能です。
- ドライバーがインストールされているのに Director が GPU を検出しない場合
  - タスクマネージャーを確認してください。ドライバーが適切にインストールされていれば、GPU はタスクマネージャーに表示されるはずです。
  - マシンが登録されているか確認してください。マシンがオンラインとして検出されるまでに時間がかかる場合があります。
- Director で GPU 使用率にアクティビティが表示されない場合は、実行しているワークロードが GPU を使用していることを確認してください。グラフィックワークロードの場合、これは「設定」>「システム」>「ディスプレイ」>「グラフィック設定」>「設定するアプリを選択」から有効にできます。「高パフォーマンス」をオンにしてください。場合によっては、他の設定に基づいて、これがシステムデフォルトまたは省電力に設定されていると、Windows はグラフィックワークロードに CPU を使用するようデフォルトで設定されます。
- データは毎分更新され、**GPU 使用率**を選択してから1分以内にデータ視覚化が開始されます。

マシンベースの履歴リソース使用率

マシン使用率パネルで、**履歴使用率の表示**をクリックすると、選択したマシン上のリソースの履歴使用状況が表示されます。 使用率グラフには、CPU、メモリ、ピーク同時セッション、平均 IOPS、ディスク遅延の重要なパフォーマンスカウンターが含まれます。

> **注:**
>
> 監視ポリシー設定の**プロセス監視を有効にする**は、履歴マシン使用率ページの「上位10プロセス」テーブルでデータを収集および表示するために「許可」に設定する必要があります。収集はデフォルトで禁止されています。

CPU とメモリ使用率、平均 IOPS、ディスク遅延データはデフォルトで収集されます。**リソース監視を有効にする**ポリシー設定を使用して、収集を無効にできます。



1. **マシン詳細**ビューの**マシン使用率**パネルから、**履歴使用率の表示**を選択します。
2. **履歴マシン使用率**ページで、**期間**を「過去2時間」、「24時間」、「7日間」、「月」、または「年」に設定して使用状況を表示します。

   注:

   平均IOPSとディスク待機時間の使用状況データは、現在までの過去24時間、月、年についてのみ利用可能です。カスタム終了時刻はサポートされていません。

3. **適用**をクリックし、必要なグラフを選択します。
4. グラフのさまざまなセクションにカーソルを合わせると、選択した期間の詳細情報が表示されます。

IOPSとディスク待機時間を含む過去のマシン利用率(/en-us/citrix-virtual-apps-desktops/2407/media/dir-machine-util-iops-latency.png)

たとえば、**過去2時間**を選択した場合、ベースライン期間は選択した時間範囲の前の2時間です。過去2時間とベースライン時間のCPU、メモリ、セッションの傾向を表示します。**先月**を選択した場合、ベースライン期間は前月です。先月とベースライン時間の平均IOPSとディスク待機時間を表示するように選択します。

1. **エクスポート**をクリックして、選択した期間のリソース使用率データをエクスポートします。詳細については、「展開の監視」のレポートのエクスポートセクションを参照してください。
2. グラフの下の表には、CPUまたはメモリ使用率に基づいて上位10個のプロセスが一覧表示されます。選択した時間範囲におけるアプリケーション名、ユーザー名、セッションID、平均CPU、ピークCPU、平均メモリ、ピークメモリを示す任意の列で並べ替えることができます。IOPSとディスク待機時間の列は並べ替えることができません。

   > **注：**
   >
   > システムプロセスのセッションIDは「0000」と表示されます。

3. 特定のプロセスのリソース消費の履歴傾向を表示するには、上位10個のプロセスのいずれかをドリルダウンします。

マシンコンソールアクセス

XenServerバージョン7.3以降でホストされているシングルセッションおよびマルチセッションOSマシンのコンソールには、Directorから直接アクセスできます。これにより、XenServerでホストされているVDAの問題をトラブルシューティングするためにXenCenterは必要ありません。この機能を利用するには：

- バージョン7.16以降のDelivery Controllerが必要です。
- マシンをホストしているXenServerはバージョン7.3以降である必要があり、Director UIからアクセスできる必要があります。

マシンコンソールアクセス(/en-us/citrix-virtual-apps-desktops/2407/media/director_machine_console_716.png)

マシンをトラブルシューティングするには、対応するマシン詳細パネルの**コンソール**リンクをクリックします。提供されたホスト資格情報が認証されると、ウェブベースのVNCクライアントであるnoVNCを使用して、マシンのコンソールが別のタブで開きます。これで、コンソールにキーボードとマウスでアクセスできるようになります。

> **注:**
>
> - この機能はInternet Explorer 11ではサポートされていません。

- マシンコンソールのマウスポインターの位置がずれている場合は、問題を解決する手順については、CTX230727を参照してください。
- Directorは新しいタブでコンソールアクセスを起動します。ブラウザの設定でポップアップが許可されていることを確認してください。
- セキュリティ上の理由から、Citrix®はブラウザにSSL証明書をインストールすることを推奨しています。

最近の電源操作があるマシンを検査する

成功および失敗した電源操作のステータスを持つマシンを検査できるようになりました。この機能は、以下の分析に役立ちます。

- ユーザーの問題を引き起こす電源オンの失敗
- コストを増加させる電源オフの失敗

注:

データは電源管理されたマシンでのみ利用可能です。この機能がサポートされる前に行われた電源操作のデータは利用できません。

次の方法でマシンの電源操作ステータスを表示できます。

フィルター -> **マシン** タブから。この場合、デフォルトで**電源操作時刻**と**電源操作結果**の列が表示されます。表示したい列を選択することもできます。

コスト最適化タブから。この場合、デフォルトのフィルターは**電源操作のトリガー元**が*Autoscale™*に設定され、**電源操作結果**が*失敗*に設定されています。

この機能を使用すると、電源操作コントロールの詳細を表示できます。たとえば、誰がアクションをトリガーしたか、どのアクションが電源状態を変更したか、失敗の理由、アクションが完了した時刻などを表示できます。これらの詳細をエクスポートすることもできます。

電源操作のステータスを表示するために、次のフィルターが追加されています。

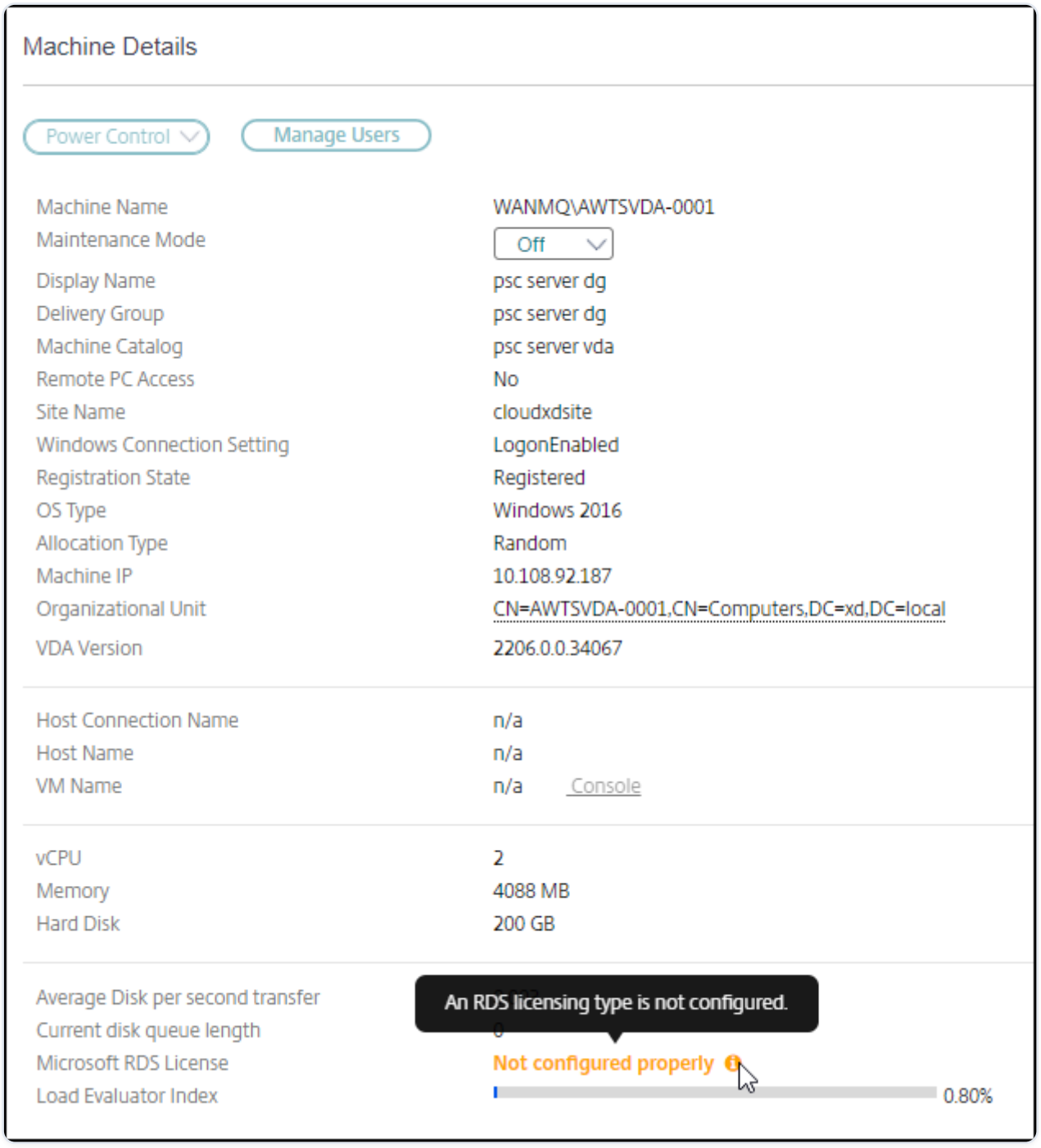
フィルター	説明
電源操作の結果	電源操作の結果を表示します。可能なフィルター値は「成功」と「失敗」です。

フィルター	説明
電源操作のトリガー元	電源操作をトリガーしたユーザーまたは内容を表示します。可能なフィルター値は次のとおりです。
	• オートスケール - この値は、電源操作が次によってトリガーされた場合に表示されます。
	• 管理者がVMのOSディスクを初期状態に戻すためにVMをシャットダウンした場合
	• 設定されたポリシーに基づいてVMがシャットダウンまたは中断された場合
	• プールサイズまたはバッファサイズの構成に基づいてVMが利用可能になった場合
	• 管理者 - この値は、管理者によって電源アクションがトリガーされたときに表示されます。考えられる例としては、管理者がVMのシャットダウン、起動、一時停止、再開、再起動、またはリブートを要求した場合などがあります。
	• ユーザー - この値は、ユーザーによって電源アクションがトリガーされたときに表示されます。例としては、ユーザーがVMをリセット、起動、または作業を再開した場合などがあります。

フィルター	説明
	• その他 - この値は、電源アクションがスケジュールされた理由または不明な理由によってトリガーされたときに表示されます。
最終電源アクション	マシンで発生した正確な電源アクション（電源オン、電源オフ、シャットダウン、再起動、リセット、再開など）を表示します。
電源アクション時刻	電源アクションが完了した時刻。可能なフィルター値は、過去1分、過去5分、過去30分、過去1時間、今日、過去24時間、昨日です。
電源アクション失敗理由	失敗の理由を表示します。可能なフィルター値は、ハイパーバイザー報告の失敗、ハイパーバイザーのレート制限超過、不明なエラー、なしです。アクションが成功した場合は、「なし」と表示されます。

Microsoft RDSライセンスの健全性

マルチセッションOSマシンでは、**マシン詳細**パネルの**マシン詳細**ページと**ユーザー詳細**ページでMicrosoft RDSライセンスのステータスを表示できます。



次のいずれかのメッセージが表示されます。

- ライセンス利用可能
- 適切に構成されていません（警告）
- ライセンスエラー（エラー）
- 互換性のないVDAバージョン（エラー）

> **注:**

有効なライセンスを持つ猶予期間中のマシンのMicrosoft RDSライセンス健全性ステータスは、緑色で**ライセンス利用可能**メッセージを表示します。ライセンスの有効期限が切れる前に更新してください。

警告メッセージとエラーメッセージについては、情報アイコンにカーソルを合わせると、次の表に示す追加情報が表示されます。

メッセージの種類	DIRECTOR内のメッセージ
エラー	VDAバージョン7.16以降で利用可能です。
エラー	新しいRDS接続は許可されていません。
エラー	Microsoft RDSライセンスの猶予期間が過ぎました。
エラー	必要なOSレベルに対して、デバイスごとのクライアントアクセスライセンスの種類でライセンスサーバーが構成されていません。
エラー	構成されているライセンスサーバーが、デバイスごとのクライアントアクセスライセンスの種類でRDSホストOSレベルと互換性がありません。
警告	パーソナルターミナルサーバーは、Citrix Virtual Apps and Desktops™展開において有効なRDSライセンスの種類ではありません。
警告	管理用リモートデスクトップは、Citrix Virtual Apps and Desktops展開において有効なライセンスの種類ではありません。
警告	RDSライセンスの種類が構成されていません。
警告	ユーザーごとのクライアントアクセスRDSライセンスの種類では、ドメインコントローラーまたはライセンスサーバーに到達できません。

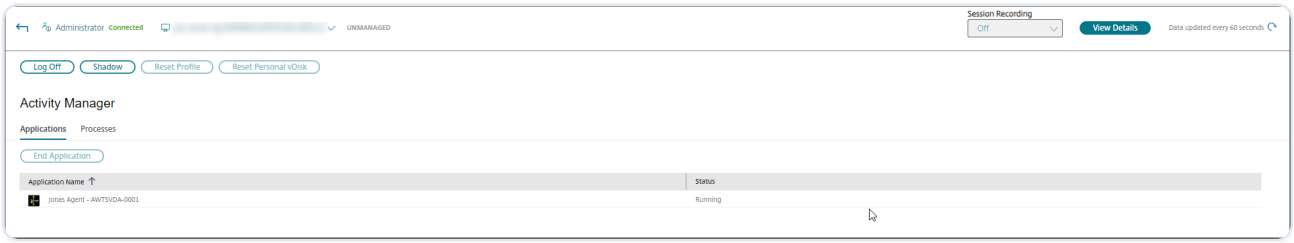
メッセージの種類	DIRECTOR内のメッセージ
警告	デバイスごとのクライアントアクセスライセンスの種類では、必要なOSレベルのライセンスサーバーに到達できないため、クライアントデバイスライセンスを判別できません。

注:

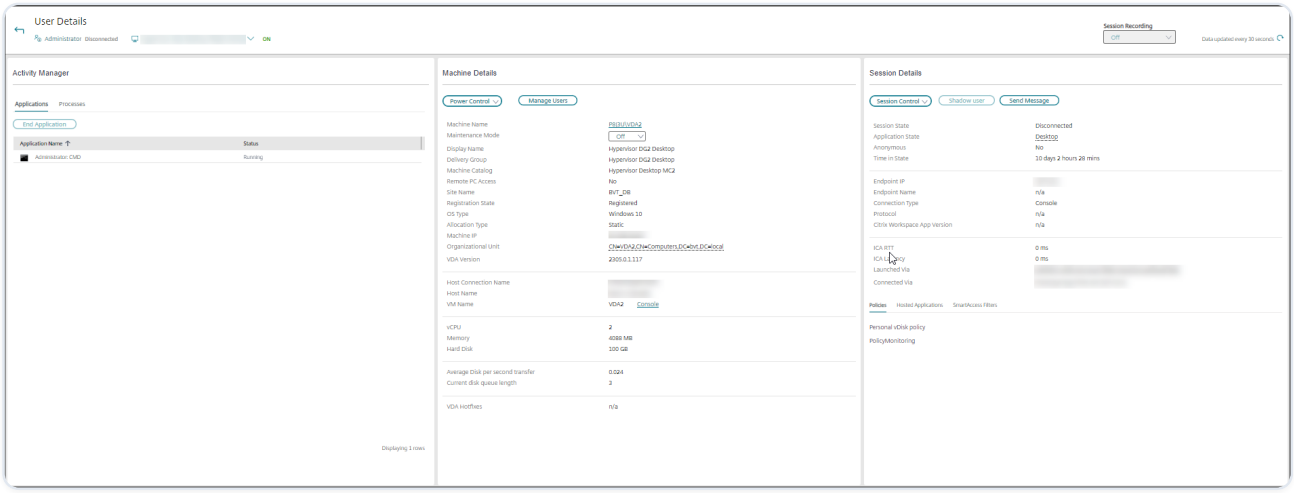
この機能は、Microsoft RDS CAL (クライアントアクセスライセンス) のみに適用されます。

ユーザーの問題のトラブルシューティング

Directorの**ヘルプデスク**ビュー（**アクティビティマネージャー**ページ）を使用して、ユーザーまたはセッションに関する情報を表示します。



ユーザーのアクティビティマネージャーから**詳細の表示**をクリックすると、**ユーザーの詳細**ページが開きます。 エンドポイントのアクティビティマネージャーから**詳細の表示**をクリックすると、**エンドポイントの詳細**ページが開きます。



セッションセレクター

ユーザーが複数のセッションを開始している場合、セッションセレクターはセッションの選択に役立ちます。



詳細を表示するセッションを選択します。

- セッション、ユーザーのサインインエクスペリエンス、セッションの起動、接続、およびアプリケーションに関する詳細を確認します。
- ユーザーのマシンをシャドウできます。
- ICA®セッションを記録します。

Microsoft Teamsの最適化ステータス

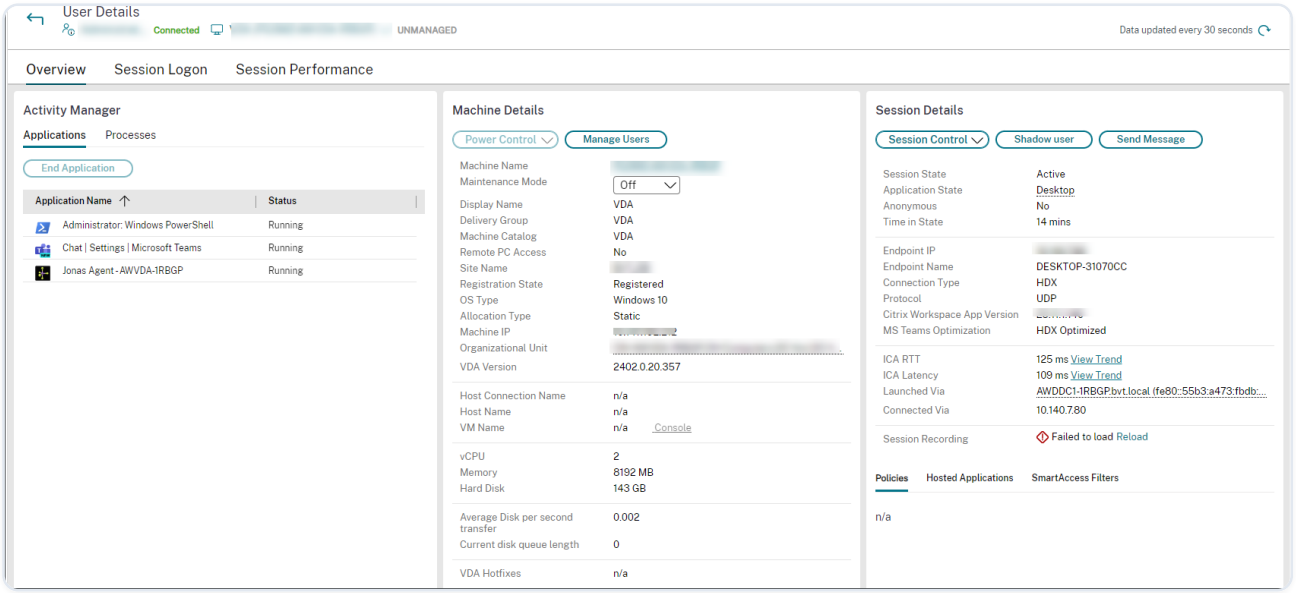
Directorは、HDX™セッションのMicrosoft Teams最適化ステータスを、**ユーザーの詳細**ページ > **セッションの詳細**パネル > **MS Teamsの最適化**フィールドに表示します。Microsoft Teamsが最適化されていることは、クリアなオーディオやビデオなど、より良いユーザーエクスペリエンスにとって重要です。Microsoft Teamsの最適化ステータスの可視性は、チケット解決にかかる時間の短縮に役立ち、管理者がトラブルシューティング中に重要なメトリックを特定するのに役立ちます。

> **注：**
>
> Citrix Directorは、Microsoft Teamsバージョン2.1以前をサポートしています。

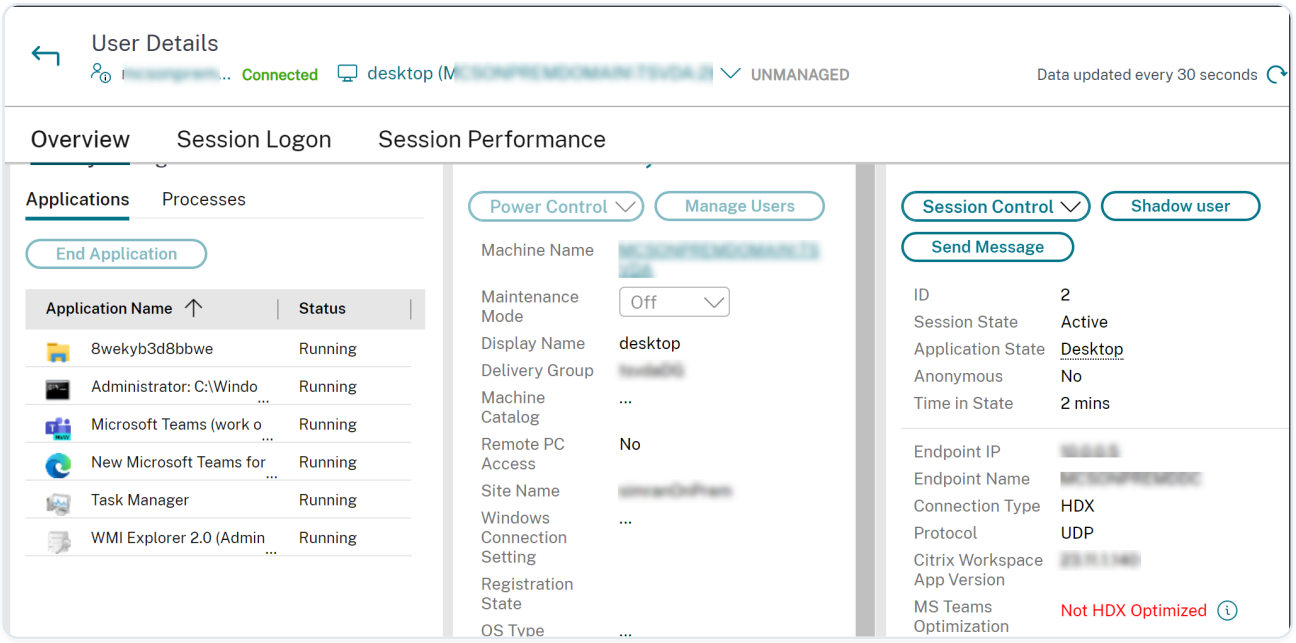
> 前提条件:

- VDA はバージョン 2311 以降で実行されています。

- サポートされている Citrix Workspace アプリのバージョンは、Microsoft Teams の最適化 に記載されています。
- Microsoft Teams は、公開アプリケーションとして、または公開デスクトップ内で実行されます。
- Citrix HDX HTML5 Video Redirection Service などの重要なサービスが実行されています。



Microsoft Teams が最適化されていない場合、ツールヒントには、Microsoft Teams を最適化するためのヒントを含む、HDX からの外部トラブルシューティングライブ記事へのリンクが表示されます。HDX 最適化のトラブルシューティング。



トラブルシューティングのヒント

次の表に記載されている推奨されるアクションで問題をトラブルシューティングし、必要に応じて、適切な管理者に問題をエスカレートしてください。

ユーザーの問題	提案
ログオンに時間がかかる、または断続的または繰り返し失敗する	ユーザーログオンの問題を診断する
セッションの起動に時間がかかる、または断続的または繰り返し失敗する	セッション起動の問題を診断する
セッションの応答が遅い、または応答しない	セッションパフォーマンスの問題を診断する
アプリケーションの動作が遅い、または応答しない	アプリケーションの障害を解決する
接続に失敗しました	デスクトップ接続を復元する
セッションの動作が遅い、または応答しない	セッションを復元する
セッションを記録する	セッションを記録する
ビデオの動作が遅い、または品質が悪い	HDXチャネルシステムレポートを実行する

注: マシンがメンテナンスモードになっていないことを確認するには、ユーザー詳細ビューからマシン詳細パネルを確認してください。

セッションログオン

「**ユーザー詳細**」ビュー > 「**セッションログオン**」タブには、セッションログオンプロセスの包括的なビューが表示されます。このタブには、さまざまなログオンフェーズがプロットされたログオン期間フェーズチャートが含まれています。このデータを使用して、ユーザーログオンの問題をトラブルシューティングします。詳細については、「ユーザーログオンの問題の診断」を参照してください。

セッションパフォーマンス

「**セッションパフォーマンス**」タブには、ユーザーセッション内の問題を特定するためにリアルタイムメトリックを関連付ける機能から始まる、強化されたトラブルシューティングワークフローがあります。「**セッショントポロジ**」パネルは、接続されたHDXセッションのセッション内パスを視覚的に表現します。「**パフォーマンスメトリック**」パネルは、ICARTT、ICA待機時間、1秒あたりのフレーム数、利用可能な出力帯域幅、消費された出力帯域幅などのセッションメトリックの傾向を提供し、これらのメトリックが時間の経過とともにどのようにパフォーマンスを

発揮したかを示します。詳細については、「セッションパフォーマンスの問題の診断」を参照してください。

検索のヒント

検索フィールドにユーザー名を入力すると、DirectorはDirectorをサポートするように構成されているすべてのサイトのActive Directoryでユーザーを検索します。

検索フィールドにマルチユーザーマシンの名前を入力すると、Director は指定されたマシンのマシン詳細を表示します。

検索フィールドにエンドポイント名を入力すると、Directorは特定のEndpointに接続されている認証されていない（匿名）セッションと認証されたセッションを使用します。この検索により、認証されていないセッションのトラブルシューティングが可能になります。認証されていないセッションのトラブルシューティングを可能にするために、エンドポイント名が一意であることを確認してください。

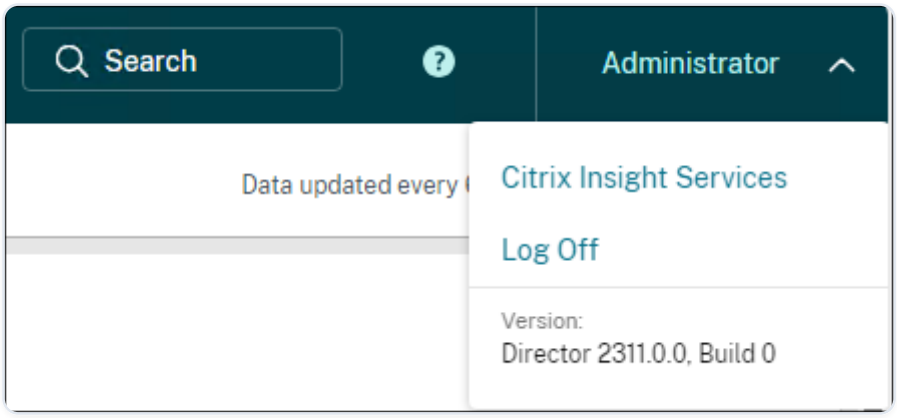
検索結果には、現在マシンを使用していない、またはマシンに割り当てられていないユーザーも含まれます。

- 検索では大文字と小文字は区別されません。
- 部分的な入力により、一致する可能性のあるリストが生成されます。
- スペースで区切られた2つの部分からなる名前の数文字を入力すると、両方の文字列に一致する結果が表示されます。2つの部分からなる名前の例としては、ユーザー名、姓と名、または表示名があります。たとえば、「jo rob」と入力すると、「John Robertson」や「Robert Jones」などの文字列が結果に含まれる場合があります。

ランディングページに戻るには、「**Directorロゴ**」をクリックします。

Citrix Insight Servicesへのアクセス

Directorの「**ユーザー**」ドロップダウンリストからCitrix Insight Services (CIS) にアクセスして、追加の診断情報を取得できます。CISで利用できるデータは、Call HomeやCitrix Scoutなどのソースから取得されます。



トラブルシューティング情報をCitrixテクニカルサポートにアップロードする

単一のDelivery Controller™またはVDAからCitrix Scoutを実行し、主要なデータポイントとCitrix Diagnostics Facility (CDF) トレースをキャプチャして、選択したコンピューターのトラブルシューティングを行います。Scoutは、データをCISプラットフォームに安全にアップロードする機能を提供し、Citrixテクニカルサポートのトラブルシューティングを支援します。Citrixテクニカルサポートは、CISプラットフォームを使用して、顧客から報告された問題の解決にかかる時間を短縮します。

Scoutは、Citrix Virtual Apps and Desktops™コンポーネントとともにインストールされます。Windowsのバージョンに応じて、Citrix Virtual Apps and Desktopsをインストールまたはアップグレードすると、Scoutは**Windowsのスタート**メニューまたはスタート画面に表示されます。

Scoutを起動するには、スタートメニューまたはスタート画面から **\>** を選択します。

Scoutの使用方法と構成、およびFAQについては、CTX130147を参照してください。

セッション起動の問題を診断する

ユーザーログオンの問題の診断セクションで述べられているログオンプロセスフェーズに加えて、Directorはセッション起動時間を表示します。これは、**ユーザー詳細**ページと**マシン詳細**ページで、Workspace Appセッション起動時間とVDAセッション起動時間に分けられます。これらの2つの期間は、さらに個々のフェーズを含み、その起動時間も表示されます。このデータは、セッション起動時間の長さの原因を理解し、トラブルシューティングするのに役立ちます。さらに、セッション起動に関わる各フェーズの所要時間は、個々のフェーズに関連する問題のトラブルシューティングに役立ちます。たとえば、ドライブマッピング時間が長い場合、GPOまたはスクリプトですべての有効なドライブが正しくマッピングされているかを確認できます。この機能は、Delivery Controllerバージョン7 1906以降およびVDA 1903以降で利用可能です。

前提条件

セッション起動時間データが表示されるには、以下の前提条件が満たされていることを確認してください。

- Delivery Controller™ 7 1906 以降のバージョン。
- VDA 1903以降。
- Citrix End User Experience Monitoring (EUEM) サービスがVDA上で実行されている必要があります。

制限事項

Directorがセッション起動時間データを表示する場合、以下の制限事項が適用されます。

- セッション起動時間はHDX™セッションでのみ利用可能です。
- iOSおよびAndroid OSからのセッション起動の場合、VDA起動時間のみが利用可能です。
- ICA®ファイルダウンロード時間 (IFDCD) は、ブラウザから起動する際にWorkspace Appが検出された場合にのみ利用可能です。
- Mac OSからのセッション起動の場合、IFDCDはWorkspace App 1902以降でのみ利用可能です。
- Windows OSからのセッション起動の場合、IFDCDはWorkspace app 1902以降で利用可能です。それ以前のバージョンでは、IFDCDは、ブラウザから起動され、Workspace appが検出されたアプリ起動の場合にのみ表示されます。

注記:

- 前提条件が満たされた後もセッション起動時間の表示に問題がある場合は、CTX130320に記載されているDirectorサーバーおよびVDAログを確認してください。 共有セッション（同じセッションで複数のアプリケーションが起動された場合）の場合、Workspace Appの起動メトリックは、最新の接続または最新のアプリケーション起動に対して表示されます。
- VDAセッション起動の一部のメトリックは、再接続時には適用されません。そのような場合、メッセージが表示されます。

セッション起動(/en-us/citrix-virtual-apps-desktops/2407/media/session_startup.png)

Workspace App セッション起動フェーズ

セッション起動クライアント期間 (SSCD)

このメトリックが高い場合、起動時間が長くなるクライアント側の問題を示しています。問題の根本原因を特定するために、後続のメトリックを確認してください。SSCD は、要求 (マウスクリッ

ク) の時刻にできるだけ近い時点から開始されます。クライアントデバイスと VDA 間の ICA 接続が確立されたときに終了します。共有セッションの場合、サーバーへの新しい接続の作成に関連するセットアップコストの多くが発生しないため、この期間ははるかに短くなります。次のレベルでは、いくつかの詳細なメトリックが利用可能です。

ICA ファイルダウンロード期間

これは、クライアントがサーバーから ICA ファイルをダウンロードするのにかかる時間です。全体的なプロセスは次のとおりです。

1. ユーザーはWorkspaceアプリケーションでリソース（アプリケーションまたはデスクトップ）をクリックします。
2. ユーザーからの要求は、Citrix Gateway（構成されている場合）を介してStoreFront™に送信され、StoreFront™は要求をDelivery Controllerに送信します。
3. Delivery Controllerは要求に対して利用可能なマシンを見つけ、マシン情報とその他の詳細をStoreFrontに送信します。また、StoreFrontはSecure Ticket Authorityからワンタイムチケットを要求し、受け取ります。
4. StoreFrontはICAファイルを生成し、Citrix Gateway（構成されている場合）を介してユーザーに送信します。

IFDCDは、完全なプロセス（ステップ1〜4）にかかる時間を表します。IFDCDの期間は、クライアントがICAファイルを受信したときにカウントを停止します。

LPWD は、プロセスの StoreFront コンポーネントです。

IFDCD が高い (ただし LPWD が正常である) 場合、起動のサーバー側処理は成功しましたが、クライアントデバイスと StoreFront の間に通信の問題がありました。これは、2つのマシン間のネットワークの問題に起因します。したがって、まず潜在的なネットワークの問題をトラブルシューティングできます。

起動ページ WEB サーバー期間 (LPWD)

これは、StoreFront で起動ページ (launch.aspx) を処理するのにかかる時間です。LPWD が高い場合、StoreFront にボトルネックがある可能性があります。

考えられる原因は次のとおりです。

- StoreFrontの負荷が高い。Internet Information Services (IIS) のログと監視ツール、タスクマネージャー、パフォーマンスモニターなどを確認して、速度低下の原因を特定してください。
- StoreFrontがDelivery Controllerなどの他のコンポーネントとの通信に問題がある。StoreFrontとDelivery Controller間のネットワーク接続が遅いか、一部のDelivery Controllerがダウンしているか、過負荷になっていないかを確認してください。

名前解決WEBサーバー期間 (NRWD)

これは、Delivery Controllerが公開アプリケーション/デスクトップの名前をVDAマシンのIPアドレスに解決するのにかかる時間です。

このメトリックが高い場合、Delivery Controllerが公開アプリケーションの名前をIPアドレスに解決するのに時間がかかっていることを示します。

可能性のある原因としては、クライアント側の問題、Delivery Controllerの過負荷などのDelivery Controllerの問題、またはそれらの間のネットワークリンクの問題が挙げられます。

チケット応答WEBサーバー期間 (TRWD)

この期間は、Secure Ticket Authority (STA) サーバーまたはDelivery Controllerからチケットを取得するのにかかる時間 (必要な場合) を示します。この期間が長い場合、STAサーバーまたはDelivery Controllerが過負荷になっていることを示します。

セッション検索クライアント期間 (SLCD)

この期間は、要求された公開アプリケーションをホストするためにすべてのセッションを照会するのにかかる時間を表します。既存のセッションがアプリケーション起動要求を処理できるかどうかを判断するために、クライアントでチェックが実行されます。使用される方法は、セッションが新規か共有かによって異なります。

セッション作成クライアント期間 (SCCD)

この期間は、wfica32.exe (または同等のファイル) が起動されてから接続が確立されるまでの、セッション作成にかかる時間を表します。

VDAセッション起動フェーズ

セッション起動VDA期間 (SSVD)

この期間は、VDAが起動操作全体を実行するのにかかる時間を含む、高レベルのサーバー側接続起動メトリックです。このメトリックが高い場合、セッション起動時間を増加させるVDAの問題があることを示します。これには、VDAで起動操作全体を実行するのに費やされた時間が含まれます。

資格情報取得VDA期間 (COVD)

VDAがユーザー資格情報を取得するのにかかる時間。

ユーザーが時間内に資格情報を提供できない場合、この期間は人為的に増加する可能性があります。そのため、VDA起動期間には含まれません。この時間は、手動ログインが使用され、サーバー側の資格情報ダイアログが表示される場合（またはログイン開始前に法的通知が表示される場合）にのみ重要となる可能性があります。

資格情報認証VDA期間 (CAVD)

これは、VDAが認証プロバイダーに対してユーザーの資格情報を認証するのにかかる時間です。認証プロバイダーは、Kerberos、Active Directory、またはセキュリティサポートプロバイダーインターフェイス (SSPI) のいずれかです。

グループポリシーVDA期間 (GPVD)

この期間は、ログオン中にグループポリシーオブジェクトを適用するのにかかる時間です。

ログオンスクリプト実行VDA期間 (LSVD)

これは、VDAがユーザーのログオンスクリプトを実行するのにかかる時間です。

ユーザーまたはグループのログオンスクリプトを非同期にすることを検討してください。アプリケーション互換性スクリプトを最適化するか、代わりに環境変数を使用することを検討してください。

プロファイル読み込みVDA期間 (PLVD)

これは、VDAがユーザーのプロファイルを読み込むのにかかる時間です。

この期間が長い場合は、ユーザープロファイルの設定を検討してください。ローミングプロファイルのサイズと場所は、セッションの起動が遅くなる原因となります。ユーザーがターミナルサービスローミングプロファイルとホームフォルダーが有効になっているセッションにログオンすると、ログオン中にローミングプロファイルの内容とそのフォルダーへのアクセスがマッピングされます。これには追加のリソースが必要です。場合によっては、CPU使用率を大幅に消費することがあります。この問題を軽減するには、リダイレクトされた個人フォルダーとともに**ターミナルサービスホーム**フォルダーを使用することを検討してください。一般的に、Citrix環境でユーザープロファイルを管理するには、Citrix Profile Managementの使用を検討してください。Citrix Profile Managementを使用しており、ログオン時間が遅い場合は、アンチウイルスソフトウェアがCitrix Profile Managementツールをブロックしていないか確認してください。

プリンター作成VDA期間 (PCVD)

これは、VDAがユーザーのクライアントプリンターを同期的にマッピングするのにかかる時間です。プリンター作成が非同期的に実行されるように設定されている場合、セッション起動の完了に影響しないため、PCVDの値は記録されません。

プリンターのマッピングに過剰な時間が費やされるのは、多くの場合、プリンターの自動作成ポリシー設定が原因です。ユーザーのクライアントデバイスにローカルで追加されたプリンターの数と、印刷構成は、セッションの起動時間に直接影響を与える可能性があります。セッションが開始されると、Citrix Virtual Apps and Desktops™は、クライアントデバイス上のローカルにマッピングされたすべてのプリンターを作成する必要があります。特にユーザーが多数のローカルプリンターを持っている場合は、作成されるプリンターの数を減らすために、印刷ポリシーを再構成す

ることを検討してください。これを行うには、Delivery ControllerおよびCitrix Virtual Apps and Desktopsでプリンター自動作成ポリシーを編集します。

ドライブマッピングVDA期間 (DMVD)

これは、VDAがユーザーのクライアントドライブ、デバイス、ポートをマッピングするのにかかる時間です。

ICAプロトコルを最適化し、セッション全体のパフォーマンスを向上させるために、ベースポリシーに未使用の仮想チャネル（オーディオやCOMポートのマッピングなど）を無効にする設定が含まれていることを確認してください。

アプリケーション/デスクトップ起動VDA期間 (ALVD/DLVD)

このフェーズは、UserinitとShellの期間の組み合わせです。ユーザーがWindowsマシンにログオンすると、winlogonがuserinit.exeを実行します。Userinit.exeはログオンスクリプトを実行し、ネットワーク接続を再確立してからExplorer.exeを起動します。Userinitは、userinit.exeの開始から仮想デスクトップまたはアプリケーションのユーザーインターフェイスの開始までの期間を表します。Shell期間は、ユーザーインターフェイスの初期化からユーザーがキーボードとマウスの制御を受け取るまでの時間です。

セッション作成VDA期間 (SCVD)

この時間には、VDAでのセッション作成時間におけるその他の遅延が含まれます。

ユーザーログオンの問題を診断する

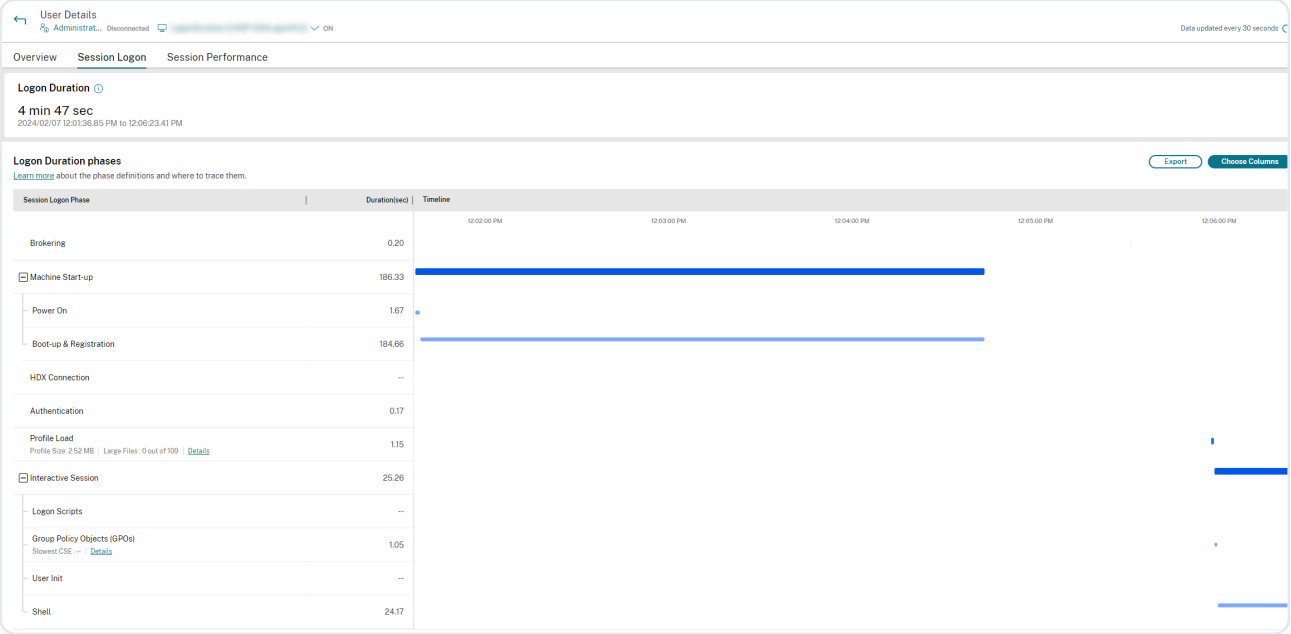
ビューの タブには、セッションログオンプロセスの包括的なビューが表示されます。このデータを使用して、ユーザーログオンの問題をトラブルシューティングします。

ログオン期間は、HDX を使用したデスクトップまたはアプリへの初回接続の場合にのみ測定されます。このデータには、リモートデスクトッププロトコルで接続しようとしているユーザーや、切断されたセッションから再接続しているユーザーは含まれません。具体的には、ユーザーが最初に非 HDX プロトコルを使用して接続し、HDX を使用して再接続する場合、ログオン期間は測定されません。

ユーザーがCitrix Virtual Apps and Desktops™にログオンすると、Monitor Serviceはログオンプロセスのフェーズを追跡します。フェーズは、ユーザーがCitrix Workspace™アプリから接続した時点から、アプリまたはデスクトップが使用可能になるまでの時間で始まります。

「**セッションログオン**」タブには、さまざまなログオンフェーズがプロットされたログオン時間フェーズチャートが含まれています。ログオン時間は、接続を確立し、Delivery Controller™からアプリまたはデスクトップを取得するのに費やされた時間と、仮想アプリまたはデスクトップに

認証してログオンするのに費やされた時間を表します。時間の情報は秒（または秒の端数）で表示されます。



ログオン期間フェーズチャートは、さまざまなログオンフェーズとその開始時刻および終了時刻を明確に表示します。このチャートは、個々のログオンフェーズの重複を示します。合計ログオン時間は、個々のログオンフェーズの期間の合計ではない場合があります。これは、個々のフェーズが重複する可能性があり、すべてのログオンフェーズがこの表現の一部ではないためです。また、特定のフェーズは、ユーザーが仮想アプリまたはデスクトップとの対話を開始した後も延長される可能性があり、この期間は全体のログオン期間の一部として測定されません。

このビューを使用して、セッション起動の遅延を引き起こしている特定のログオンフェーズを特定します。各ログオンフェーズの定義と、情報を追跡できるイベントソースは、さらなるトラブルシューティングに役立ちます。チャートにカーソルを合わせると、現在のセッションのフェーズ期間、ユーザーの7日間平均、およびデリバリーグループの7日間平均を含むツールチップが表示されます。この情報は、現在のセッションのログオン期間を7日間平均値と比較するのに役立ちます。GPO およびプロファイルの詳細の場合、サブフェーズ測定にさらにドリルダウンできます。この視覚化は、ログオン期間に関連する問題を簡単に理解し、トラブルシューティングするのに役立ちます。

前提条件

ログオン期間データとドリルダウンが表示されるように、次の前提条件が満たされていることを確認してください。

1. VDA に **Citrix User Profile Manager** と **Citrix User Profile Manager WMI Plugin** をインストールします。
2. Citrix Profile Management Service が実行されていることを確認します。

3. XenApp および XenDesktop 7.15 以前のサイトでは、GPO 設定 を無効にします。
4. 対話型セッションのドリルダウンには、監査プロセス追跡を有効にする必要があります。
5. GPO ドリルダウンの場合、グループポリシーの運用ログのサイズを増やします。

> **注:**
>
> - ログオン時間は、デフォルトのWindowsシェル (explorer.exe) でのみサポートされ、カスタムシェルではサポートされません。
> - Remote PC Accessのログオン時間は、Remote PC Accessのインストール中に**Citrix User Profile Manager**および**Citrix User Profile Manager WMI Plugin**が追加コンポーネントとしてインストールされている場合にのみ利用可能です。詳細については、Remote PC Accessの構成とシーケンスに関する考慮事項のステップ4を参照してください。

ユーザーログオンの問題をトラブルシューティングする手順

1. **ユーザー詳細**ビュー > **セッションログオン**タブから、ログオン時間グラフを使用してログオン状態をトラブルシューティングします。
   - ユーザーがログオンしている場合、ビューにはログオンのプロセスが反映されます。
   - ユーザーがログオンしている場合、ログオン時間パネルには、ユーザーが現在のセッションにログオンするのにかかった時間が表示されます。
2. ログオンプロセスのフェーズを調べます。

ログオンプロセスのフェーズ

ブローカリング

ユーザーに割り当てるデスクトップを決定するのにかかった時間。

マシンの起動

セッションでマシンの起動が必要だった場合、これは仮想マシンの起動にかかった時間です。以下のサブセクションでは、異なるフェーズで仮想マシンを起動するまでにかかった時間の内訳を示します。

- **電源オン** - 仮想マシンの電源をオンにするのにかかった時間を表示します
- **起動と登録** - 仮想マシンを起動して登録するのにかかった時間を表示します

折りたたみボタンを使用して、**マシンの起動**の下にあるオプションを折りたたんだり展開したりできます。

HDX接続

クライアントから仮想マシンへのHDX接続の設定に必要な手順を完了するのにかかった時間。

認証

リモートセッションへの認証を完了するのにかかった時間。

GPO

仮想マシンでグループポリシー設定が有効になっている場合、これはログオン中にグループポリシーオブジェクトを適用するのにかかった時間です。GPOバーにカーソルを合わせると、CSEs (Clients-Side Extension) に従って各ポリシーを適用するのにかかった時間の詳細がツールチップとして表示されます。



詳細をクリックすると、ポリシーのステータスと対応するGPO名を含むテーブルが表示されます。ドリルダウンの期間はCSE処理時間のみを表し、GPOの合計時間には加算されません。このドリルダウンテーブルは、さらなるトラブルシューティングやレポートでの使用のためにコピーできます。ポリシーのGPO時間はEvent Viewerログから取得されます。ログは、操作ログに割り当てられたメモリ（デフォルトサイズは4 MB）によっては上書きされる可能性があります。操作ログのログサイズを増やす方法の詳細については、Microsoft TechNetの記事「Configuring the Event Logs」を参照してください。

ログオンスクリプト

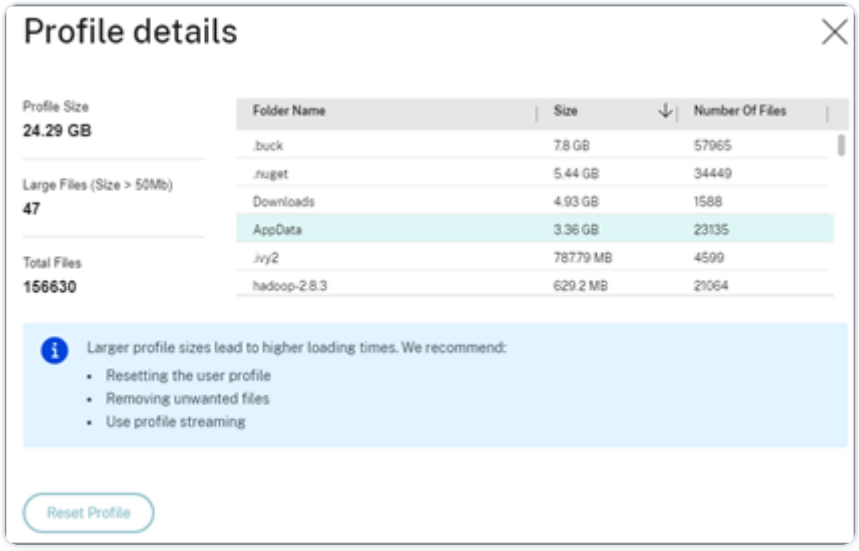
セッションにログオンスクリプトが構成されている場合、これはログオンスクリプトの実行にかかった時間です。

プロファイル読み込み

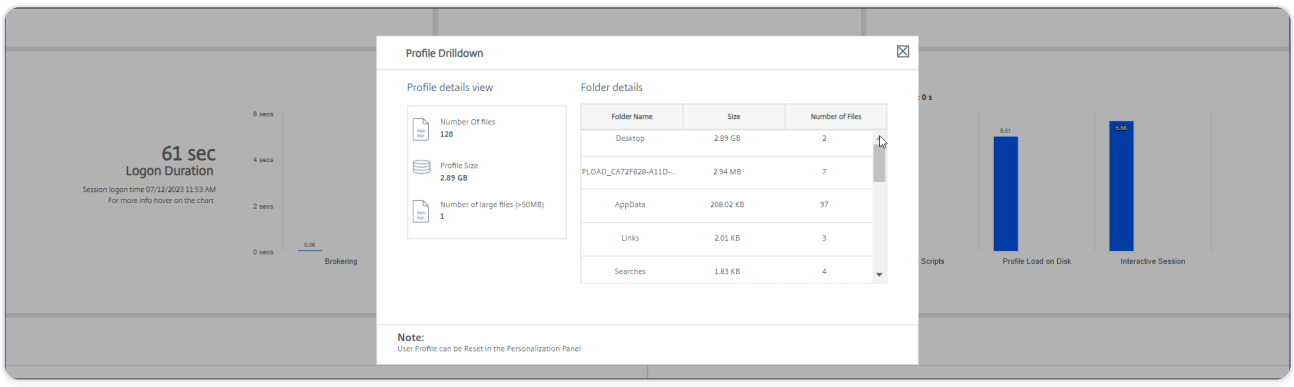
ユーザーまたは仮想マシンにプロファイル設定が構成されている場合、これはプロファイルのロードにかかった時間です。

Citrix Profile ManagementとFSLogixが構成されている場合、Profile LoadバーにはCitrix Profile ManagementとFSLogixがユーザープロファイルを処理するのにかかった時間が含まれます。この情報は、管理者がプロファイル処理時間の延長に関する問題をトラブルシューティングするのに役立ちます。Profile ManagementとFSLogixが構成されている場合、Profile Loadバーは延長された期間を表示します。この延長はこの機能強化によって引き起こされるものであり、パフォーマンスの低下を反映するものではありません。この機能強化はVDAバージョン2407以降で利用可能です。

Profile Loadバーにカーソルを合わせると、現在のセッションのユーザープロファイルの詳細を示すツールチップが表示されます。



「**詳細**」をクリックして、プロファイルルートフォルダー (例: C:/Users/username) 内の各個別のフォルダーをさらにドリルダウンし、そのサイズとファイル数 (ネストされたフォルダー内のファイルを含む) を確認します。



プロファイルのドリルダウンは、Delivery Controllerバージョン7 1811以降およびVDA 1811以降で利用できます。プロファイルのドリルダウン情報を使用すると、プロファイルの読み込み時間が長いことに関する問題を解決できます。次のことができます。

- ユーザープロファイルをリセットする
- 不要な大きなファイルを削除してプロファイルを最適化する
- ネットワーク負荷を軽減するためにファイル数を減らす
- プロファイルストリーミングを使用する

デフォルトでは、プロファイルルート内のすべてのフォルダーがドリルダウンに表示されます。フォルダーの表示を非表示にするには、VDAマシンで次のレジストリ値を編集します。

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

1. VDAで、HKEY_LOCAL_MACHINE\Software\Citrix\Director\に新しいレジストリ値 **ProfileFoldersNameHidden** を追加します。
2. 値を1に設定します。この値はDWORD (32ビット) 値である必要があります。これでフォルダー名の表示が無効になります。
3. フォルダー名を再度表示するには、値を0に設定します。

> **注:**
>
> GPOまたはPowerShellコマンドを使用して、複数のマシンにレジストリ値の変更を適用できます。GPOを使用してレジストリの変更を展開する方法の詳細については、ブログを参照してください。

追加情報

- プロファイルのドリルダウンでは、リダイレクトされたフォルダーは考慮されません。

- ルートフォルダー内のNTUser.datファイルは、エンドユーザーには表示されない場合があります。ただし、これらはプロファイルのドリルダウンに含まれ、**ルートフォルダー**のファイルリストに表示されます。
- AppDataフォルダー内の一部の隠しファイルは、プロファイルのドリルダウンには含まれません。
- ファイル数とプロファイルサイズデータは、特定のWindowsの制限により、パーソナライズパネルのデータと一致しない場合があります。

対話型セッション

対話型セッションとは、ユーザープロファイルがロードされた後、キーボードとマウスの制御をユーザーに「引き渡す」のにかかる時間です。これは通常、ログオンプロセスのすべてのフェーズの中で最も長い期間であり、**対話型セッション期間 = デスクトップ準備完了イベントのタイムスタンプ (VDA上のEventId 1000) - ユーザープロファイルロード済みイベントのタイムスタンプ (VDA上のEventId 2)** として計算されます。対話型セッションには、Pre-userinit、Userinit、Shellの3つのサブフェーズがあります。対話型セッションにカーソルを合わせると、次の情報を示すツールチップが表示されます。

- サブフェーズ
- 各サブフェーズにかかる時間
- これらのサブフェーズ間の累積合計時間遅延

折りたたみボタンを使用して、**対話型セッション**の下のオプションを折りたたんだり展開したりできます。

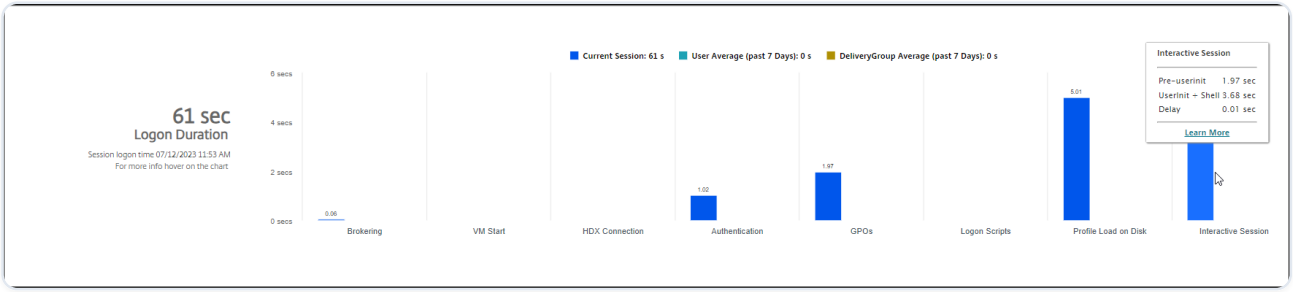
> **注:**
>
> この機能は、VDA 1811以降で利用できます。7.18より前のサイトでセッションを起動し、その後7.18以降にアップグレードした場合、「サーバーエラーのためドリルダウンを利用できません」というメッセージが表示されます。ただし、アップグレード後にセッションを起動した場合は、エラーメッセージは表示されません。

> 各サブフェーズの期間を表示するには、VM (VDA) で監査プロセス追跡を有効にします。監査プロセス追跡が無効になっている場合 (デフォルト)、Pre-userinitの期間と、UserinitおよびShellの合計期間が表示されます。グループポリシーオブジェクト (GPO) を使用して監査プロセス追跡を有効にするには、次の手順を実行します。

1. GPOを作成し、GPOエディターを使用して編集します。

2. **コンピューターの構成 > Windows の設定 > セキュリティの設定 > ローカル ポリシー > 監査ポリシー**に移動します。
3. 右側のペインで、**監査プロセス追跡**をダブルクリックします。
4. **成功**を選択し、OKをクリックします。
5. このGPOを必要なVDAまたはグループに適用します。

監査プロセス追跡とその有効化または無効化の詳細については、Microsoftドキュメントの監査プロセス追跡を参照してください。



ユーザー詳細ビューのログオン期間パネル。

- **対話型セッション – Pre-userinit:** グループポリシーオブジェクトとスクリプトと重複する対話型セッションのセグメント。このサブフェーズは、GPOとスクリプトを最適化することで短縮できます。
- **対話型セッション – Userinit:** ユーザーがWindowsマシンにログオンすると、Winlogonはuserinit.exeを実行します。Userinit.exeはログオンスクリプトを実行し、ネットワーク接続を再確立してから、WindowsユーザーインターフェイスであるExplorer.exeを起動します。対話型セッションのこのサブフェーズは、Userinit.exeの開始から仮想デスクトップまたはアプリケーションのユーザーインターフェイスの開始までの期間を表します。
- **対話型セッション – Shell:** 前のフェーズで、UserinitはWindowsユーザーインターフェイスの初期化を開始します。Shellサブフェーズは、ユーザーインターフェイスの初期化からユーザーがキーボードとマウスの制御を受け取るまでの期間を捕捉します。
- **遅延:** これは、**Pre-userinitとUserinit**サブフェーズ間、および**UserinitとShell**サブフェーズ間の累積時間遅延です。

合計ログオン時間は、これらのフェーズの正確な合計ではありません。たとえば、一部のフェーズは並行して発生し、一部のフェーズでは、合計よりも長いログオン期間につながるより多くの処理が発生します。 合計ログオン時間には、ICAファイルのダウンロードとアプリケーションのICAファイル起動の間の時間であるICA®アイドル時間は含まれません。 アプリケーション起動時にICAファイルを自動的に開くには、ICAファイルのダウンロード時にブラウザがICAファイルを自動的に起動するように設定します。詳細については、CTX804493を参照してください。

> **注:**
>
> ログオン期間グラフは、ログオンフェーズを秒単位で表示します。1秒未満の期間値はサブ秒値として表示されます。1秒を超える値は、最も近い0.5秒に丸められます。グラフは、Y軸の最大値が200秒になるように設計されています。200秒を超える値は、バーの上に実際の値が表示されます。

データのエクスポート

デフォルトのログオン期間フェーズテーブルオプション（セッションログオンフェーズと期間）に加えて、セッションログオンページで以下の列を選択することもできます。

- 開始時刻
- 終了時刻
- デリバリーグループ - 7日間平均 (秒)
- ユーザー - 7日間平均 (秒)

以前のデータを.CSVファイルにエクスポートすることもできます。

トラブルシューティングのヒント

グラフ内の異常な値や予期しない値を特定するには、現在のセッションの各フェーズにかかった時間と、このユーザーの過去7日間の平均所要時間、およびこのデリバリーグループのすべてのユーザーの過去7日間の平均所要時間を比較します。

必要に応じてエスカレートします。たとえば、**マシンの起動**が遅い場合、問題はハイパーバイザーにある可能性があるため、ハイパーバイザー管理者にエスカレートできます。

異常な相違点を確認します。

- ログオンバー（現在）の欠落
- 現在の所要時間とこのユーザーの平均所要時間の間に大きな相違がある場合。原因は次のとおりです。
    - 新しいアプリケーションがインストールされた。
    - オペレーティングシステムのアップデートが行われた。
    - 構成変更が行われた。
    - ユーザーのプロファイルサイズが大きい。この場合、プロファイルロードが高くなります。

- ユーザーのログオン数（現在および平均期間）とデリバリーグループの平均期間との間に大きな不一致がある。

必要に応じて、**再起動**をクリックしてユーザーのログオンプロセスを監視し、**マシンの起動**や**ブローカリング**などの問題をトラブルシューティングします。

セッションパフォーマンスの問題を診断する

「ユーザー詳細」ページの「**セッションパフォーマンス**」タブには、HDX™ユーザーセッション内の問題を特定するのに役立つ強化されたトラブルシューティングワークフローが用意されています。「**セッションのトポロジーとパフォーマンスメトリクス**」パネルは、セッションのコンポーネントビューと複数のパフォーマンスメトリクスを単一のビューで関連付け、セッションエクスペリエンスの問題解決にかかる平均時間を短縮します。

セッションパフォーマンスビュー(/en-us/citrix-virtual-apps-desktops/2407/media/dir-session-performance.png)

エンドツーエンドのネットワークホップビュー

エンドツーエンドのネットワークホップビューは、セッションパス全体の視覚的な表現を提供することで、トラブルシューティングを強化します。エンドツーエンドのネットワークホップビューを見つけるには、**ユーザー詳細** > **セッションパフォーマンス** > **セッションのトポロジー**をクリックします。このビューには、接続されているHDXセッションのコンポーネント、メタデータ、リンク、および公開アプリケーションが表示されます。

このビューは、管理者が次のことを行うのに役立ちます。

- セッションのデータフローを理解する。
- 特定のホップにおけるパフォーマンスのボトルネックを特定する。

> **注:**
>
> パフォーマンスメトリクスは、接続されているHDXセッションでのみ利用可能です。

セッションパフォーマンスメトリクス

管理者が特定のセッションのパフォーマンスを理解するのに役立つ、以下のメトリクスがコンテキストに応じて利用可能です。ホップビューで利用可能なデータは、UIに示された間隔で定期的に更新されます。

エンドポイントメトリクス：

機能名	UIパラメーター	CITRIX WORKSPACE™アプリ FOR WINDOWS バージョン	VIRTUAL DELIVERY AGENTバージョン
エンドポイントのネットワーク詳細	ネットワークインターフェイスの種類	Citrix Workspaceアプリ for Windows バージョン 2405.10 以降	シトリックス バーチャル アプリケーションズ アンド デスクトップス 2407 以降
	Wi-Fi信号強度		
	スループット（受信または送信）		
	リンク速度		

HDXメトリック:

機能名	UIパラメーター	WINDOWS向けCITRIX WORKSPACEアプリのバージョン	VIRTUAL DELIVERY AGENTのバージョン
ICAメトリック	ICA RTT	Windows向けCitrix Workspaceアプリ バージョン2405.10 以降	シトリックス バーチャルアプリおよびデスクトップ 2407 以降
	ICA®遅延		

データ定義:

UIパラメーター	説明
ICA RTT	ユーザーアクションから画面応答までの時間（ICA遅延、エンドポイント遅延、ホスト遅延を含む）を測定します。
ICA遅延	ネットワーク遅延と潜在的な速度低下を示します。
Wi-Fi信号強度	ワイヤレス信号の品質と強度を表示します。
スループット（送受信）	ネットワークインターフェースへのデータ転送速度とネットワークインターフェースからのデータ転送速度を示します。

UIパラメーター	説明
ネットワークインターフェースの種類	イーサネット、Wi-Fi、セルラーなどのネットワーク接続の種類を指定します。
リンク速度	ネットワーク接続の最大データ転送速度を表します。

セッショントポロジのシナリオ

サイトの展開シナリオに応じて、セッションに関与するコンポーネントは次のすべてまたは一部です。

- エンドポイント上のCitrix Workspaceアプリ
- Gatewayサービス/オンプレミスGateway
- Cloud Connector – ハイブリッド接続の場合、GatewayはCloud Connectorを介してDaaSに接続されます。
- VDA

したがって、可能なネットワークトポロジは次のとおりです。

- エンドポイント上のCitrix Workspaceアプリは、Citrix WorkspaceおよびGateway Serviceを介してオンプレミスのVDAに接続します。VDAへの接続にCloud Connectorは使用されません。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/2407/media/dir-session-topology1.png)

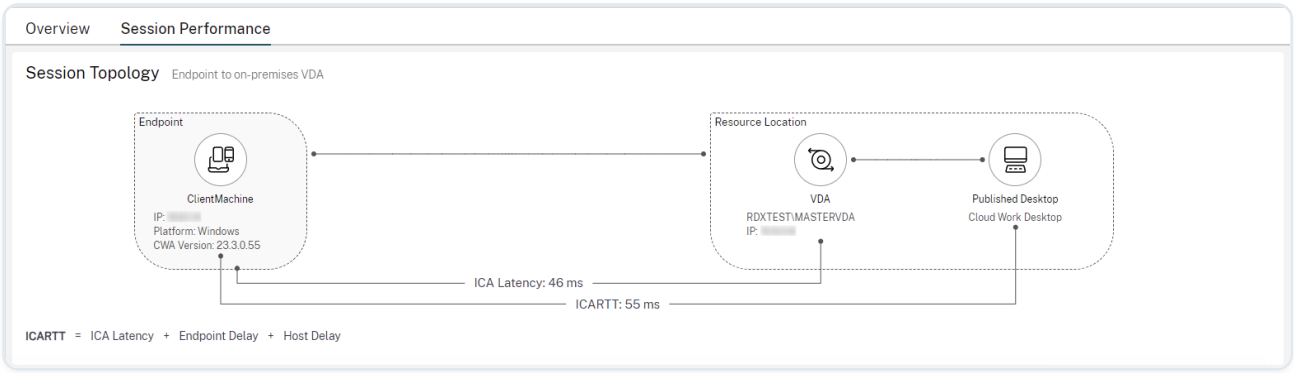
- エンドポイント上のCitrix Workspaceアプリは、Citrix WorkspaceおよびGateway Serviceを介して、Cloud Connector経由でオンプレミスのVDAに接続します。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/2407/media/dir-session-topology2.png)

- エンドポイント上のCitrix Workspaceアプリは、StoreFront™およびオンプレミスGatewayを介してオンプレミスVDAに接続します。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/2407/media/dir-session-topology3.png)

- エンドポイント上のCitrix Workspaceアプリは、StoreFrontを介してオンプレミスVDAに接続します。



パフォーマンスメトリック

パフォーマンスメトリックパネルでは、ユーザーセッション内の問題を特定するためにリアルタイムメトリックを関連付けることができます。セッションメトリックの傾向は、これらのメトリックが時間の経過とともにどのようにパフォーマンスを発揮したかを示すのに役立ちます。**セッションパフォーマンス**タブをクリックすると、リアルタイムデータに加えて、過去15分間および24時間のデータを表示できます。プロットは、複数のコンポーネントパフォーマンスメトリックを単一のビューで関連付けるのに役立ちます。



注：

- 過去15分間のメトリックサポートにより、グラフはセッションが接続および切断された期間についてプロットされます。切断されたセッションのメトリックは、値ゼロで表示されます。
- 過去24時間のメトリックサポートにより、ICARTTおよびICA遅延のプロットは履歴データメトリックで更新されます。

ICARTTおよびICA Latencyの他に、リアルタイムおよび過去15分間のメトリックとして、以下のメトリックが利用可能です。

- 1秒あたりのフレーム数 - 1秒あたりのフレーム数は、セッションの応答性を示す重要なメトリックです。 利用可能な出力帯域幅 - 利用可能な出力帯域幅は、VDAからエンドポイントにデータを送信するために利用可能な総帯域幅の測定値です。
- 消費された出力帯域幅 - 消費された出力帯域幅は、ユーザーにセッションを表示するためにVDAからエンドポイントに送信された実際のデータ量を示します。

利用可能な出力帯域幅と消費された出力帯域幅を分析することで、セッションを提供するために十分な帯域幅が利用可能であるか、およびセッションが帯域幅不足の影響を受けているかどうかを検出するのに役立ちます。

ICA RTTまたはセッションログオン期間データが入力されない場合のトラブルシューティング

以前は、EUEMサービスまたはプロファイル管理サービスが実行に失敗した場合、ICA RTTまたはセッションログオン期間に関連するデータの取得失敗の理由が表示されませんでした。この新機能により、失敗の理由と、その失敗に対する対応する解決策を取得できます。**詳細**リンクには、次の表に示すように、ICA RTTおよびセッションログオン期間のエラー、失敗の理由、および解決策が記載されています。

エラーの種類	エラー	エラーメッセージ	解決策
ICA RTTエラー	ICA RTT値が表示されません。	**Citrix End User Experience Monitoringが実行されていません。**	1. サービスコンソールを開きます。このコンソールを開くには、**スタート**をクリックし、**サービス**と入力します。
			2. Citrix End User Experience Monitoring Serviceが実行されていることを確認してください。
			3. デスクトップセッションを再度開き、試してください。ICA RTT値が表示されるはずです。

エラーの種類	エラー	エラーメッセージ	解決策
			4. 問題が解決しない場合は、Citrix 管理者に連絡してください。
ICA RTT エラー	ICA RTT 値が表示されない.	**Citrix End User Experience Monitoring がインストールされていません。**	1. VDA を再インストールします。
			2. サービスコンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サービス」と入力します。
			3. Citrix End User Experience Monitoring Serviceが実行されていることを確認します。
			4. デスクトップセッションを再度開き、試してください。ICA RTT値が表示されるはずです。
			5. 問題が解決しない場合は、Citrix管理者に連絡してください。
ICA RTTエラー	ICA RTT値が表示されません。	**データの取得中にエラーが発生しました。**	1. サービスコンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サービス」と入力します。

エラーの種類	エラー	エラーメッセージ	解決策
			`2.` **Windows Management Instrumentation Service**が実行されていることを確認します。
			`3.` また、WfShell.exe/PicaShell.exeプロセスが**アクティビティマネージャー** > **プロセス**タブで実行されていることを確認します。実行されていない場合は、デスクトップセッションを再度開きます。
			`4.` 前述の手順が機能しない場合は、Citrix_Euem_RoundTripインスタンスが存在することを確認するために、次のコマンドを実行します: `Get-CimInstance -Namespace 'ROOT\Citrix\Euem' -Query "select * from Citrix_Euem_RoundTrip"`
			`5.` Citrix_Euem_RoundTripインスタンスが存在する場合は、デスクトップセッションを再度開きます。

エラーの種類	エラー	エラーメッセージ	解決策
			6. 問題が解決しない場合は、Citrix 管理者に連絡してください。
セッションログオン期間エラー	グラフが読み込まれていません。	**Citrix Profile Managementが実行されていません**	1. サービスコンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サービス」と入力します。
			2. **Citrix Profile Management Service**が実行されていることを確認してください。
			3. デスクトップセッションを再度開き、試してください。グラフが表示されるはずです。
			4. 問題が解決しない場合は、Citrix 管理者に連絡してください。
セッションログオン期間エラー	グラフが読み込まれていません。	**Citrix Profile Management がインストールされていません。**	1. Citrix Profile Management Service をインストールします。
			2. サービスコンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サー

エラーの種類	エラー	エラーメッセージ	解決策
			ビス」と入力します。
			3. **Citrix Profile Management Service** が実行されていることを確認します。
			4. デスクトップセッションを再度開き、試してください。グラフが表示されるはずです。
			5. 問題が解決しない場合は、Citrix管理者に連絡してください。
セッションログオン期間エラー	グラフが読み込まれません。	**データ取得エラー。**	1. **サービス**コンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サービス」と入力します。
			2. **Windows Management Instrumentation Service**が実行されていることを確認します。
			3. 前述のサービスがすでに実行されている場合、`LogonTimings instance is present`であること

エラーの種類	エラー	エラーメッセージ	解決策
			を確認するために、次のコマンドを実行します: `Get-CimInstance -Namespace 'ROOT\Citrix\Profile\Metrics' -Query "select * from LogonTimings"`
			`4.` 問題が解決しない場合は、Citrix管理者に連絡してください。

シャドウユーザー

Directorから、シャドウユーザー機能を使用して、ユーザーの仮想マシンまたはセッションを直接表示したり操作したりできます。Windows VDAとLinux VDAの両方をシャドウできます。シャドウするマシンにユーザーが接続している必要があります。これは、ユーザーのタイトルバーに表示されているマシン名を確認することで検証できます。

Directorは新しいタブでシャドウを開始します。DirectorのURLからのポップアップを許可するようにブラウザ設定を更新してください。

シャドウ機能には、**ユーザーの詳細**ビューからアクセスします。ユーザーセッションを選択し、アクティビティマネージャービューまたはセッション詳細パネルで**シャドウ**をクリックします。

Linux VDAのシャドウ

シャドウは、バージョン7.16以降のLinux VDAで、RHEL7.3またはUbuntuバージョン16.04のLinuxディストリビューションを実行しているもので利用できます。

> **注：**
>
> - シャドウを機能させるには、VDAがDirector UIからアクセス可能である必要があります。したがって、シャドウはDirectorクライアントと同じイントラネット内のLinux VDAでのみ可能です。

- DirectorはFQDNを使用してターゲットLinux VDAに接続します。Directorクライアントが Linux VDAのFQDNを解決できることを確認してください。
- VDAには、python websockifyおよびx11vncパッケージがインストールされている必要があります。
- VDAへのnoVNC接続はWebSocketプロトコルを使用します。デフォルトでは、**ws://** WebSocketプロトコルが使用されます。セキュリティ上の理由から、Citrixは安全な **wss://** プロトコルを使用することを推奨します。各DirectorクライアントとLinux VDAにSSL証明書をインストールしてください。

セッションシャドウの指示に従って、シャドウ用にVDAを構成してください。

1. **シャドウ**をクリックすると、シャドウ接続が初期化され、ユーザーデバイスに確認プロンプトが表示されます。
2. マシンまたはセッションの共有を開始するには、ユーザーに**はい**をクリックするよう指示してください。
3. 管理者はシャドウされたセッションを表示することしかできません。

Windows VDA のシャドウイング

Windows VDA セッションは、Windows リモートアシスタンスを使用してシャドウイングされます。VDA のインストール中に、**ユーザー Windows リモートアシスタンス**機能を有効にします。詳細については、「機能の有効化または無効化」を参照してください。

1. **シャドウ**をクリックすると、シャドウイング接続が初期化され、.msrc インシデントファイルを開くか保存するかを求めるダイアログボックスが表示されます。
2. デフォルトで選択されていない場合は、リモートアシスタンスビューアーでインシデントファイルを開きます。ユーザーデバイスに確認プロンプトが表示されます。
3. ユーザーに**はい**をクリックするよう指示して、マシンまたはセッションの共有を開始します。
4. より詳細な制御を行うには、ユーザーにキーボードとマウスの制御を共有するよう依頼します。

シャドウイング用にMICROSOFT INTERNET EXPLORERブラウザーを効率化する

Microsoft Internet Explorerブラウザーを構成して、ダウンロードしたMicrosoftリモートアシスタンス（.msra）ファイルをリモートアシスタンスクライアントで自動的に開くようにします。

これを行うには、グループポリシーエディターで「ファイルのダウンロード時に自動的にダイアログを表示する」設定を有効にする必要があります。

コンピューターの構成 \> 管理用テンプレート \> Windows コンポーネント \> Internet Explorer \> インターネット コントロール パネル \> セキュリティのページ \> インターネット ゾーン \> ファイルのダウンロード時に自動的にダイアログを表示する.

既定では、このオプションはローカルイントラネットゾーンのサイトに対して有効になっています。Directorサイトがローカルイントラネットゾーンにない場合は、そのサイトをこのゾーンに手動で追加することを検討してください。

アプリケーション障害の解決

アクティビティマネージャービューで、タブをクリックします。このユーザーがアクセスできるすべてのマシン上のすべてのアプリケーション（現在接続されているマシンのローカルアプリケーションとホストされているアプリケーションを含む）と、それぞれのステータスを表示できます。

> **注:**
>
> アプリケーションタブがグレー表示されている場合は、タブを有効にする権限を持つ管理者に連絡してください。

> リストには、セッション内で起動されたアプリケーションのみが含まれます。

マルチセッションOSマシンおよびシングルセッションOSマシンでは、切断されたセッションごとにアプリケーションが一覧表示されます。ユーザーが接続されていない場合、アプリケーションは表示されません。

アクション	説明
応答しないアプリケーションを終了する	応答しないアプリケーションを選択し、[アプリケーションの終了]をクリックします。アプリケーションが終了したら、ユーザーに再度起動するように依頼します。
応答しないプロセスを終了する	必要な権限がある場合は、[プロセス]タブをクリックします。アプリケーションに関連する、または大量のCPUリソースやメモリを使用しているプロセスを選択し、[プロセスの終了]をクリックします。ただし、プロセスを終了するのに必要な権限がない場合、プロセスを終了しようとすると失敗します。

アクション	説明
ユーザーのマシンを再起動する	シングルセッションOSマシンのみの場合、選択したセッションで[再起動]をクリックします。または、[マシン詳細]ビューから電源コントロールを使用してマシンを再起動またはシャットダウンします。ユーザーに再度ログオンするように指示し、アプリケーションを再確認できるようにします。マルチセッションOSマシンでは、再起動オプションは利用できません。代わりに、ユーザーからログオフし、ユーザーに再度ログオンさせます。
マシンをメンテナンスモードにする	マシンのイメージにパッチやその他の更新などのメンテナンスが必要な場合は、マシンをメンテナンスモードにしてください。マシン詳細ビューから、[詳細] をクリックし、メンテナンスモードオプションをオンにします。適切な管理者にエスカレートしてください。

ユーザープロファイルをリセットする

注意：

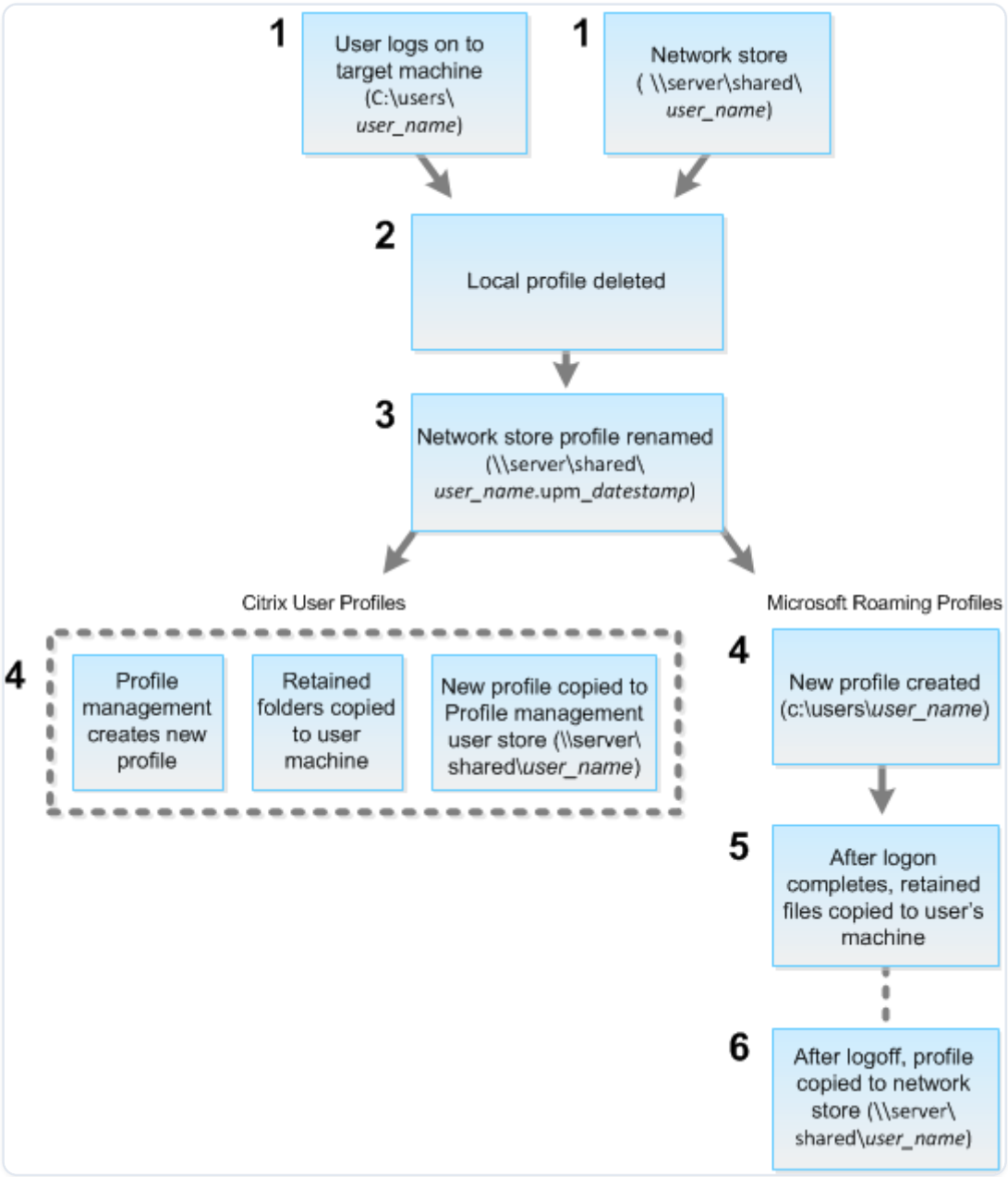
プロファイルがリセットされると、ユーザーのフォルダーとファイルは保存され、新しいプロファイルにコピーされます。ただし、ほとんどのユーザープロファイルデータは失われます（たとえば、レジストリがリセットされ、アプリケーション設定が削除される可能性があります）。

リセット機能は、ファイルベースとコンテナベースの両方のプロファイルソリューションに適用されます。

リセットされたプロファイルの処理方法

Citrix®ユーザープロファイルまたはMicrosoftローミングプロファイルのいずれもリセットできます。ユーザーがログオフし、リセットコマンドを選択すると（DirectorまたはPowerShell SDKを使用して）、Directorはまず使用中のユーザープロファイルを識別し、適切なリセットコマンドを発行します。Directorは、プロファイルサイズ、種類、ログオン時間などの情報をProfile Managementを通じて受け取ります。

この図は、ユーザープロファイルがリセットされた後のユーザーログオンに続くプロセスを示しています。



Directorによって発行されたリセットコマンドは、プロファイルの種類を指定します。その後、Profile Managementサービスはその種類のプロファイルをリセットしようとし、適切なネットワーク共有（ユーザーストア）を探します。ユーザーがProfile Managementによって処理されているにもかかわらず、ローミングプロファイルコマンドを受け取った場合、それは拒否されます（またはその逆も同様です）。

1. ローカルプロファイルが存在する場合、それは削除されます。
2. ネットワークプロファイルの名前が変更されます。
3. 次のアクションは、リセットされるプロファイルがCitrixユーザープロファイルかMicrosoftローミングプロファイルかによって異なります。

Citrixユーザープロファイルの場合、新しいプロファイルはProfile Managementのインポートルールを使用して作成されます。フォルダーはネットワークプロファイルにコピーされ、ユーザーは通常どおりログオンできます。リセットにローミングプロファイルが使用される場合、ローミングプロファイル内のレジストリ設定はリセットされたプロファイルに保持されます。必要に応じて、テンプレートプロファイルがローミングプロファイルを上書きするようにProfile Managementを構成できます。

Microsoftローミングプロファイルの場合、Windowsがプロファイルを作成し、ユーザーがログオンすると、フォルダーはユーザーデバイスにコピーされます。ユーザーが再度ログオフすると、新しいプロファイルはネットワークストアにコピーされます。

Directorでユーザープロファイルをリセットするには

Citrix Virtual Desktops™ (Desktop VDA) を使用している場合は、次の操作を行います。

1. **Director** で、リセットするプロファイルのユーザーを検索し、そのユーザーのセッションを選択します。
2. をクリックします。
3. ユーザーにすべてのセッションからログオフするよう指示します。
4. ユーザーに再度ログオンするよう指示します。 ユーザーのプロファイルから保存されたフォルダーとファイルは、新しいプロファイルにコピーされます。

Citrix Virtual Desktops (Server VDA) を使用している場合、プロファイルのリセットを実行するにはログオンしている必要があります。その後、ユーザーはログオフし、再度ログオンしてプロファイルのリセットを完了する必要があります。

> **重要:**

> ユーザーが複数のプラットフォーム（Windows 8やWindows 7など）にプロファイルを持っている場合は、ユーザーが問題として報告したのと同じデスクトップまたはアプリに最初にログオンし直すように指示します。このログオン操作により、正しいプロファイルがリセットされます。プロファイルがCitrixユーザープロファイルの場合、ユーザーのデスクトップが表示されるまでにプロファイルはすでにリセットされています。プロファイルがMicrosoftローミングプロファイルの場合、フォルダーの復元が短時間進行中の可能性があります。ユーザーは復元が完了するまでログオンしたままにする必要があります。

> プロファイルが正常にリセットされない場合（たとえば、ユーザーがマシンに正常にログオンし直せない、または一部のファイルが欠落している場合）は、元のプロファイルを手動で復元する必要があります。

次の点に注意してください。

- ユーザープロファイルソリューションとしてユーザーストアが有効になっている場合、新しいプロファイルには元のユーザープロファイルから次の個人フォルダーが含まれます。
  - デスクトップ
  - クッキー
  - お気に入り
  - ドキュメント
  - ピクチャ
  - ミュージック
  - ビデオ
- Citrix Profile Managementバージョン2407以降では、プロファイルコンテナがユーザープロファイルソリューション全体として有効になっている場合、新しいプロファイルは上記の個人用フォルダーを保持します。
- Windows 8以降では、プロファイルがリセットされると、Cookieは新しいプロファイルにコピーされません。

リセットに失敗したプロファイルを手動で復元するには

1. ユーザーにすべてのセッションからログオフするよう指示します。
2. ローカルプロファイルが存在する場合は削除します。
3. フォルダー名に日付と時刻が追加されたアーカイブフォルダー（.upm_datestamp拡張子を持つフォルダー）をネットワーク共有上で見つけます。
4. 現在のプロファイル名を削除します。つまり、upm_datestamp拡張子のないものです。
5. アーカイブフォルダーを元のプロファイル名に名前変更します。つまり、日付と時刻の拡張子を削除します。これにより、プロファイルはリセット前の元の状態に戻ります。

PowerShell SDKを使用してプロファイルをリセットするには

Broker PowerShell SDKを使用してプロファイルをリセットできます。

NEW-BROKERMACHINECOMMAND

特定のユーザー、セッション、またはマシンに配信するためにキューに入れられたコマンドを作成します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerMachineCommand/>`を参照してください。

例

PowerShell コマンドレットを使用してプロファイルをリセットする方法の詳細については、以下の例を参照してください。

Profile Management プロファイルをリセットする

- user1 のプロファイルをリセットしたいとします。New-BrokerMachineCommand PowerShell コマンドを使用します。例:
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetUpmProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

> **重要:**
>
> `CommandData $byteArray`は次の形式である必要があります:`<SID>[,<backup path>]`。バックアップパスを指定しない場合、Profile Management は現在の日付と時刻で名前が付けられたバックアップフォルダーを生成します。

Windows ローミングプロファイルをリセットする

- user1 のローミングプロファイルをリセットしたいとします。New-BrokerMachineCommand PowerShell コマンドを使用します。例:
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetRoamingProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

セッションを記録する

Directorの**ユーザー詳細**画面および**マシン詳細**画面にあるセッション記録コントロールを使用して、ICA®セッションを記録できます。この機能は、**Premium**サイトのお客様にご利用いただけます。

動的セッション記録

ユーザー詳細画面のセッション記録コントロールを使用して、現在アクティブなセッションを記録できます。動的セッション記録について詳しくは、「セッション記録サービス」の記事を参照してください。

ポリシーベースのセッション記録

DirectorConfigツールを使用してDirectorでポリシーベースのセッション記録を構成するには、「セッション記録ポリシーの構成」の「**Directorでセッション記録サーバーを使用するように構成する**」セクションを参照してください。 セッション記録コントロールは、ログインしているユーザーがセッション記録ポリシーを変更する権限を持っている場合にのみDirectorで利用できます。この権限は、「ユーザーの承認」で説明されているように、セッション記録承認コンソールで設定できます。

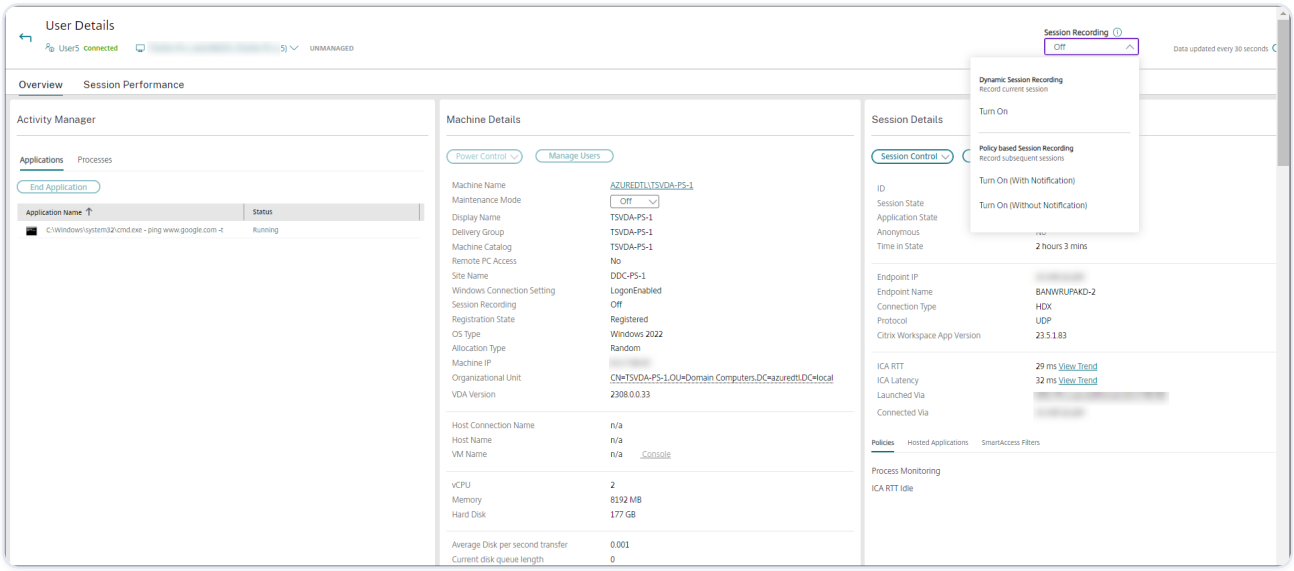
> **注：** Directorまたはセッション録画ポリシーコンソールを介してセッション録画設定に加えられた変更は、次回のICAセッションから有効になります。

Directorのセッション記録コントロール

ユーザー詳細 > **セッション記録**アクションを使用して、現在または以降のセッションを記録できます。

- 動的セッション記録をオンにする - 現在のセッションが記録されます。
- オンにする（通知あり） - 以降のセッションが記録され、ユーザーはICAセッションにログオンする際にセッションが記録されていることを通知されます。
- オンにする（通知なし） - 以降のセッションが記録され、ユーザーに通知することなくセッションがサイレントに記録されます。
- オフにする - ユーザーのセッション記録を無効にします。

ポリシーパネルには、アクティブなセッション記録ポリシーの名前が表示されます。



マシン詳細パネルには、マシンのセッション記録ポリシーのステータスが表示されます。

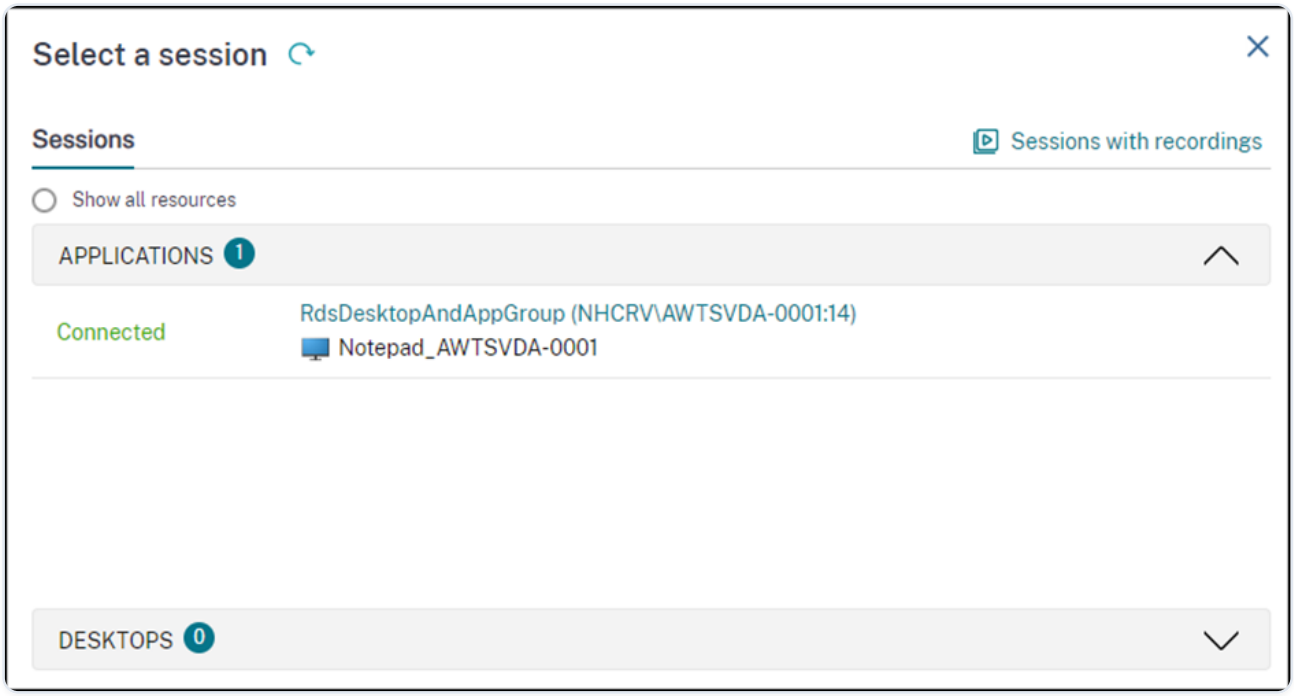
ライブセッションと録画セッションを再生する

ユーザーが遭遇した問題を理解するために、録画されたユーザーセッションとライブユーザーセッションを再生できます。Directorコンソール内で録画とセッション関連のメトリックにすぐにアクセスできるため、複数のセッション録画サーバーで録画を検索したり、録画を表示するためのサードパーティ製アプリを探したりする必要がなくなります。これにより、録画で発見された問題とパフォーマンスメトリックを関連付けるのに役立ちます。

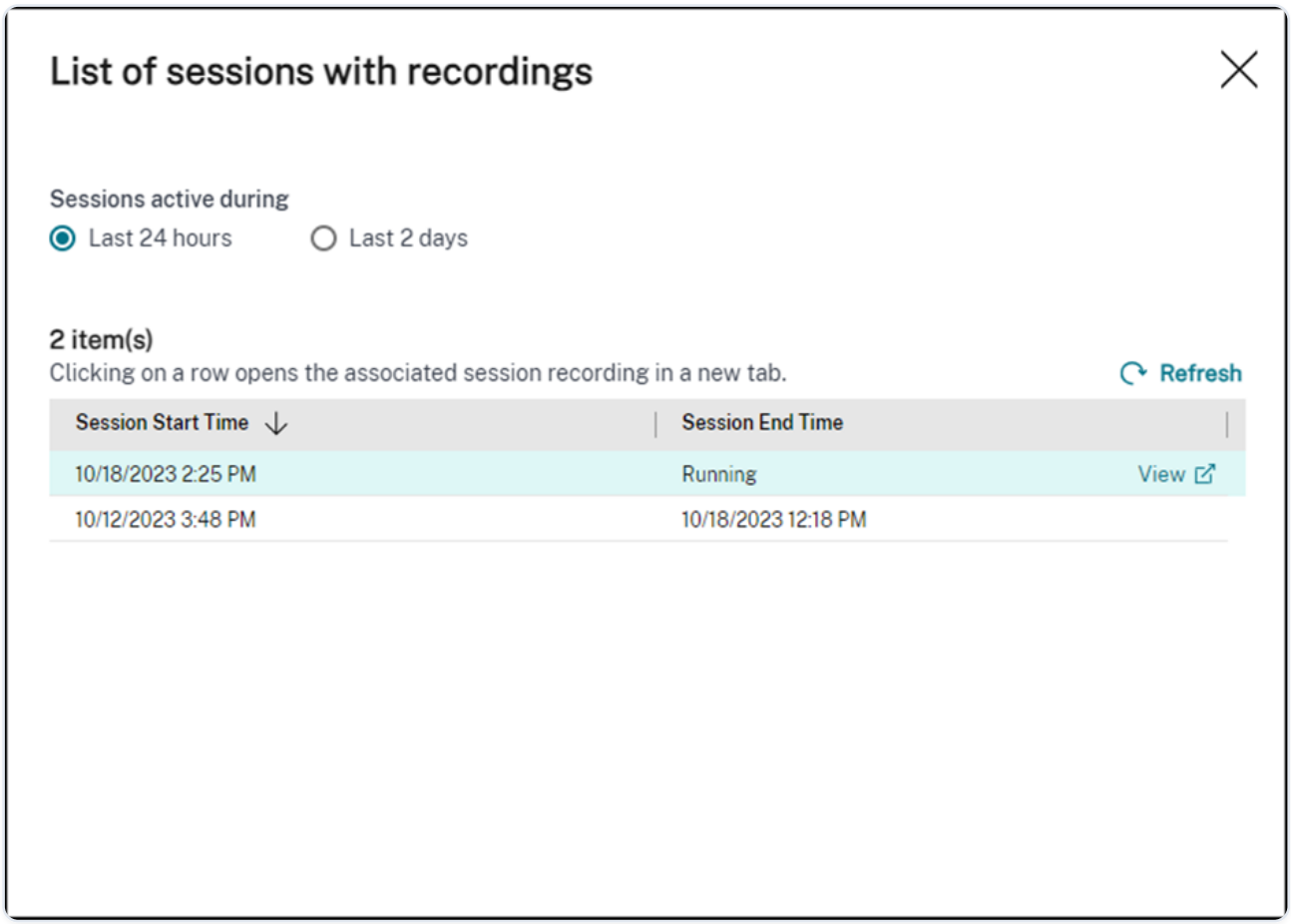
この機能には、以下が必要です。

- VDAとセッション録画サーバーはバージョン2308以降であること。
- Delivery Controller™とDirectorはバージョン2311以降であること。

Directorはセッション録画を一元的なリポジトリに保存します。「**セッションセレクター**」モーダル > 「**録画のあるセッション**」リンクをクリックすると、ユーザーに属する録画のリストが表示されます。



過去24時間または過去2日間にアクティブだったセッションの録画を表示することを選択できます。現在アクティブなセッションのライブ録画は、「**セッション終了時刻**」が「**実行中**」と表示されます。



「**表示**」リンクをクリックして、Citrix Session Recording再生サーバーを使用して新しいタブで録画を再生します。

機能の互換性マトリックス

Citrix Director 7 2407 は以下と互換性があります:

- Citrix Virtual AppsおよびDesktops™ 7 2112 以降
- Citrix Virtual AppsおよびDesktops 7 1912 長期サービスリリース

各サイトでは、Director を以前のバージョンのDelivery Controller™ とともに使用できますが、Director の最新バージョンのすべての機能が利用できない場合があります。Citrix は、Director、Delivery Controller、および VDA を同じバージョンにすることを推奨します。

注:

Delivery Controllerをアップグレードした後、Studio を開くとサイトのアップグレードを促されます。詳細については、展開のアップグレードの「**アップグレードシーケンス**」セクションを参照してください。

Director のアップグレード後に初めてログインすると、構成済みのサイトでバージョンチェックが実行されます。いずれかのサイトが Director のバージョンよりも古いバージョンの Controller を実行している場合、Director コンソールにサイトのアップグレードを推奨するメッセージが表示されます。さらに、サイトのバージョンが Director のバージョンよりも古い間は、この不一致を示すメモが Director ダッシュボードに表示され続けます。

注:

以前のバージョンの Citrix Director では、最近の VDA バージョンで実行されているユーザーセッションに適用されたポリシーは表示されません。Citrix Director 1912 およびそれ以前のバージョンでは、VDA バージョン 2003 以降で実行されているユーザーセッションに適用されたポリシーは表示されません。これらのポリシーを表示するには、Citrix Director バージョン 2003 以降を使用してください。

Delivery Controller (DC)、VDA、およびその他の必要な依存コンポーネントの最小バージョンとライセンスエディションを含む、特定の Director 機能は以下のとおりです。

DIRECTOR のバージョン	機能	依存関係 - 必要な最小バージョン	エディション
2407	コスト最適化	なし	すべて
2407	統合とデータのエクスポート	VDA 2407	すべて
2407	過去のユーザーセッションの診断 (プレビュー)	VDA 2407	すべて
2407	Secure Private Accessセッション用アクティビティマネージャー (プレビュー)	VDA 2407	すべて
2407	Director を使用した TCP および UDP アプリケーションの Secure Private Access 統合 (プレビュー)	VDA 2407	すべて
2407	インフラストラクチャ監視 (プレビュー)	VDA 2407	すべて
2407	未登録マシンアラート	VDA 2407 および DDC 2407	すべて
2407	マシンの稼働時間アラート	VDA 2407 および DDC 2407	すべて
2407	電源オン失敗アクションおよび電源オフ失敗アクションアラート	VDA 2407 および DDC 2407	すべて
2407	アラートメールにCSV添付ファイル、アラートWebhookに	VDA 2407 および DDC 2407	すべて

DIRECTOR のバージョン	機能	依存関係 - 必要な最小バージョン	エディション
	JSONペイロードを含める機能		
2407	最近の電源操作があるマシンを検査	VDA 2407	すべて
2407	高度なアラートポリシー(/ja-jp/citrix-virtual-apps-desktops/2407/director/site-analytics/alerts-notifications#advanced-alert-policies)	VDA 2407 および DDC 2407	すべて
2407	クラウドおよびオンプレミスユーザー向けの統合検索(/ja-jp/citrix-virtual-apps-desktops/2407/director/unified-search)	VDA 2407	すべて
2407	ダッシュボード上の公開アプリケーション使用状況監視チャート(/ja-jp/citrix-virtual-apps-desktops/2407/director/site-analytics/application-usage-monitoring)	VDA 2407 および DDC 2407	Platinumライセンスサイト
2402 LTSR	DirectorによるWebおよびSaaSアプリのSecure Private Access統合（プレビュー）(/ja-jp/citrix-virtual-apps-desktops/2407/2402-ltsr/director/spa-)	VDA 2402 LTSR	すべて

DIRECTOR のバージョン	機能	依存関係 - 必要な最小バージョン	エディション
	integration-with-director)		
2402 LTSR	Microsoft Teams バージョン 2.1 以前のサポート](/ja-jp/citrix-virtual-apps-desktops/2407/2402-ltsr/director/troubleshoot-deployments/user-issues#microsoft-teams-optimization-status)	VDA 2402 LTSR	すべて
2311	ライブセッションと録画セッションの再生](/ja-jp/citrix-virtual-apps-desktops/2407/director/troubleshoot-deployments/user-issues/record-sessions#play-back-live-and-recorded-sessions)	VDA 2308 および DDC 2311	すべて
2311	セッショントポロジ](/ja-jp/citrix-virtual-apps-desktops/2407/director/troubleshoot-deployments/user-issues/session-performance#session-topology)	なし	すべて
2311	最適な画面解像度](/ja-jp/citrix-virtual-apps-desktops/2407/system-	なし	すべて

DIRECTOR のバージョン	機能	依存関係 - 必要な最小バージョン	エディション
	requirements#citrix-director)		
2311	MS Teams の最適化	VDA 2311 および DDC 最新版	すべて
2311	プローブ概要の機能強化	なし	すべて
2311	刷新されたセッションログオン期間ビュー	なし	すべて
2308	プローブの概要とドリルダウン	なし	すべて
2308	Citrix Probe Agent の Citrix Gateway 多要素認証のサポート	シトリックス ゲートウェイ	すべて
2308	ハイパーバイザーアラートの無効化	なし	すべて
2308	セッションエクスペリエンスメトリックの傾向	なし	すべて
2305	Citrix Gateway を介した認証のサポート(/ja-jp/citrix-virtual-apps-desktops/2407/director/probes)	なし	すべて
2305	Director での Autoscale 管理(/ja-jp/citrix-virtual-apps-desktops/2407/director/site-analytics/autoscale-managed-machines)	なし	すべて

DIRECTOR のバージョン	機能	依存関係 - 必要な最小バージョン	エディション
2303	失敗したマシンのアラート(/ja-jp/citrix-virtual-apps-desktops/2407/director/site-analytics/alerts-notifications.html#failed-machines-in-)	DC 7 2303	プレミアム
2203	TLS 1.3 のサポート(/ja-jp/citrix-virtual-apps-desktops/2407/2203-ltsr/whats-new/2203-ltsr-initial-release.html#tls-13-support)	-	すべて
2212	AMD GPUで利用可能なリアルタイムGPU使用率	64ビットWindowsおよびHDX 3D Proが有効なDC 7.14およびVDA 7.14	すべて
2212	高度なプローブスケジューリング	DC 7 1906 および Citrix Probe エージェント 2209	プレミアム
1909	Citrix Analytics for Performanceでオンプレミスサイトを構成	DC 7 1906およびVDA 1906	すべて
1906	セッションの自動再接続	DC 7 1906およびVDA 1906	すべて
1906	「セッション起動時間」(/ja-jp/citrix-virtual-apps-desktops/2407/director/troubleshoot-	DC 7 1906およびVDA 1903	すべて

DIRECTOR のバージョン	機能	依存関係 - 必要な最小バージョン	エディション
	deployments/user-issues/session-startup.html)		
1906	「デスクトッププロービング」(/ja-jp/citrix-virtual-apps-desktops/2407/director/probes.html)	DC 7 1906 および Citrix Probe エージェント 1903	プレミアム
7.9以降	「プロファイルロードにおけるCitrix Profile Managementの期間」(/ja-jp/citrix-virtual-apps-desktops/2407/director/troubleshoot-deployments/user-issues/user-logon.html#profile-load)	VDA 1903	すべて
1811	「プロファイルドリルダウン」(/ja-jp/citrix-virtual-apps-desktops/2407/director/troubleshoot-deployments/user-issues/user-logon.html#profile-load)	DC 7 1811 および VDA 1811	すべて
1811	ハイパーバイザーアラート監視	DC 7 1811	プレミアム
1811	アプリケーションプロービング	DC 7 1811 および Citrix アプリケーションプローブエージェント 1811	プレミアム

DIRECTOR のバージョン	機能	依存関係 - 必要な最小バージョン	エディション
1811	Microsoft RDS ライセンスの正常性	DC 7 1811 および VDA 7.16	すべて
1811	「主要なRTOPデータ表示」(/ja-jp/citrix-virtual-apps-desktops/2407/)	DC 7 1811 および VDA 1808	プレミアム
1808	「フィルターデータのエクスポート」(/ja-jp/citrix-virtual-apps-desktops/2407/director/site-analytics/filters-data.html)	DC 7 1808	すべて
1808	「対話型セッションのドリルダウン」(/ja-jp/citrix-virtual-apps-desktops/2407/director/troubleshoot-deployments/user-issues/user-logon.html)	DC 7 1808 および VDA 1808	すべて
1808	「GPOドリルダウン」(/ja-jp/citrix-virtual-apps-desktops/2407/director/troubleshoot-deployments/user-issues/user-logon.html)	DC 7 1808 および VDA 1808	すべて
1808	OData API を使用して利用可能なマシンの履歴データ(https://developer-docs.citrix.com/projects/monitor-	DC 7 1808	すべて

DIRECTOR のバージョン	機能	依存関係 - 必要な最小バージョン	エディション
	service-odata-api/en/)		
7.18	アプリケーションのプロービング(/ja-jp/citrix-virtual-apps-desktops/2407/director/probes.html)	DC 7.18	プレミアム (旧 プラチナ)
7.18	スマートアラートポリシー(/ja-jp/citrix-virtual-apps-desktops/2407/director/site-analytics/alerts-notifications.html#smart-alert-policies)	DC 7.18	プレミアム (旧 プラチナ)
7.18	Health Assistant リンク(/ja-jp/citrix-virtual-apps-desktops/2407/director/troubleshoot-deployments/machines.html)	なし	すべて
7.18	インタラクティブセッションのドリルダウン	なし	すべて
7.17	PIV スマートカード認証	なし	すべて
7.16	アプリケーション分析	DC 7.16およびVDA 7.15	すべて
7.16	OData エーピーアイ V.4	DC 7.16	すべて
7.16	Linux VDAユーザーのシャドウイング(/ja-jp/citrix-virtual-	VDA 7.16	すべて

DIRECTOR のバージョン	機能	依存関係 - 必要な最小バージョン	エディション
	apps-desktops/2407/director/troubleshoot-deployments/user-issues/shadow-users.html)		
7.16	ドメインローカルグループのサポート(/ja-jp/citrix-virtual-apps-desktops/2407/director/install-and-configure/advanced-configuration.html#domain-local-group-configuration)	なし	すべて
7.16	マシンのコンソールアクセス(/ja-jp/citrix-virtual-apps-desktops/2407/director/troubleshoot-deployments/machines.html#machine-console-access)	DC 7.16	すべて
7.15	アプリケーション障害監視(/ja-jp/citrix-virtual-apps-desktops/2407/director/troubleshoot-deployments/applications.html#real-time-application-monitoring)	DC 7.15 および VDA 7.15	すべて
7.14	アプリケーション中心のトラブルシューティング(/ja-jp/citrix-virtual-apps-desktops/2407/director/troubleshoot-	DC 7.13 および VDA 7.13	すべて

DIRECTOR のバージョン	機能	依存関係 - 必要な最小バージョン	エディション
	deployments/applications.html)		
7.14	ディスク監視(/ja-jp/citrix-virtual-apps-desktops/2407/director/troubleshoot-deployments/applications.html#real-time-application-monitoring)	DC 7.14 および VDA 7.14	すべて
7.14	GPU監視(/ja-jp/citrix-virtual-apps-desktops/2407/director/troubleshoot-deployments/applications.html#real-time-application-monitoring)	DC 7.14 および VDA 7.14	すべて
7.13	セッション詳細パネルのトランスポートプロトコル	DC 7.xおよびVDA 7.13	すべて
7.12	ユーザーフレンドリーな接続およびマシンの障害の説明	DC 7.12およびVDA 7.x	すべて
7.12	Enterpriseエディションでの履歴データの可用性の増加	DC 7.12およびVDA 7.x	エンタープライズ
7.12	カスタムレポート	DC 7.12およびVDA 7.x	プレミアム (旧 Platinum)
7.11	リソース使用率レポート	DC 7.11 および VDA 7.11	すべて

DIRECTOR のバージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.11	CPU、メモリ、ICA RTT条件に対するアラートの拡張	DC 7.11 および VDA 7.11	プレミアム (旧 Platinum)
7.11	レポートのエクスポート機能の改善	DC 7.11 および VDA 7.x	すべて
7.11	Citrix ADMとの統合	DC 7.11、VDA 7.x、およびMASバージョン11.1ビルド49.16	Premium (以前は Platinum)
7.9	ログオン期間の内訳	DC 7.9およびVDA 7.x	すべて
7.7	プロアクティブな監視とアラート	DC 7.7およびVDA 7.x	Premium (以前は Platinum)
7.7	Windows認証統合	DC 7.xおよびVDA 7.x	すべて
7.7	シングルセッションおよびマルチセッションOSの使用状況(/ja-jp/citrix-virtual-apps-desktops/2407/director//site-analytics/trends.html)	DC 7.7 および VDA 7.x	プレミアム (旧 プラチナ)
7.6.300	Framehawk仮想チャネルのサポート(/ja-jp/citrix-virtual-apps-desktops/2407/director/troubleshoot-deployments/user-issues/hdx-channel-reports.html)	DC 7.6 および VDA 7.6	すべて
7.6.200	セッション記録の統合(/ja-jp/citrix-virtual-apps-desktops/2407/director/troubleshoot-	DC 7.6 および VDA 7.x	プレミアム (旧 プラチナ)

DIRECTOR のバージョン	機能	依存関係 - 必要な最小バージョン	エディション
	deployments/user-issues/record-sessions.html)		
7	HDX Insightの統合(/ja-jp/citrix-virtual-apps-desktops/2407/director/install-and-configure/hdx-insight.html)	DC 7.6、VDA 7.x、および Citrix ADM	プレミアム (旧 プラチナ)

データ粒度と保持

データ値の集計

Monitor Serviceは、ユーザーセッションの使用状況、ユーザーログオンパフォーマンスの詳細、セッション負荷分散の詳細、接続およびマシン障害情報など、さまざまなデータを収集します。データは、そのカテゴリに応じて異なる方法で集計されます。OData Method APIを使用して提示されるデータ値の集計を理解することは、データを解釈するために不可欠です。例：

- 接続されたセッションとマシン障害は一定期間に発生します。したがって、それらは期間中の最大値として公開されます。
- ログオン期間は時間の長さを測定するものであるため、期間中の平均値として公開されます。
- ログオン数と接続障害は期間中の発生回数であるため、期間中の合計値として公開されます。

同時データ評価

セッションは、同時と見なされるためには重複している必要があります。ただし、時間間隔が1分の場合、その1分間のすべてのセッション（重複しているかどうかに関わらず）は同時と見なされます。間隔のサイズが非常に小さいため、精度を計算するのに伴うパフォーマンスオーバーヘッドは、追加される価値に見合いません。セッションが同じ時間内に発生しても、同じ分内に発生しない場合、それらは重複しているとは見なされません。

サマリーテーブルと生データの相関

データモデルは、メトリックを2つの異なる方法で表します。

- サマリーテーブルは、メトリックの集計ビューを分単位、時間単位、日単位の粒度で表します。
- 生データは、セッション、接続、アプリケーション、およびその他のオブジェクトで追跡される個々のイベントまたは現在の状態を表します。

API呼び出し間またはデータモデル自体内でデータを関連付けようとするときは、次の概念と制限を理解することが重要です。

- **部分的な間隔のサマリーデータはありません。** メトリックのサマリーは、長期間にわたる履歴トレンドのニーズを満たすように設計されています。これらのメトリックは、完全な間隔についてサマリーテーブルに集計されます。データ収集の開始時（利用可能な最も古いデータ）または終了時の部分的な間隔については、サマリーデータはありません。1日の集計（Interval=1440）を表示する場合、これは最初と最新の不完全な日にはデータがないことを意味します。これらの部分的な間隔には生データが存在する可能性がありますが、決して要約されません。特定のデータ粒度について、最も早い集計間隔と最も遅い集計間隔は、特定のサマリーテーブルからSummaryDateの最小値と最大値を抽出することで判断できます。SummaryDate列は間隔の開始を表します。Granularity列は集計データの期間の長さを表します。
- **時間による相関。** メトリックは、前述のセクションで説明されているように、完全な間隔についてサマリーテーブルに集計されます。これらは履歴トレンドに使用できますが、生イベントはトレンド分析のために要約されたものよりも現在の状態をより正確に反映している可能性があります。サマリーデータと生データの時間ベースの比較を行う場合、発生する可能性のある部分的な間隔や期間の開始と終了についてはサマリーデータがないことを考慮する必要があります。
- **見逃されたイベントと潜在的なイベント。** イベントが見逃されたり、集計期間に対して潜在的であったりする場合、サマリーテーブルに集計されるメトリックはわずかに不正確になる可能性があります。Monitor Serviceは正確な現在の状態を維持しようとしますが、見逃されたイベントや潜在的なイベントのために、サマリーテーブルの集計を過去に遡って再計算することはありません。
- **接続の高可用性。** 接続の高可用性中、現在の接続のサマリーデータカウントにギャップが生じますが、セッションインスタンスは引き続き生データで実行されます。
- **データ保持期間。** サマリーテーブルのデータは、生イベントデータのスケジュールとは異なるグルーミングスケジュールで保持されます。サマリーテーブルまたは生テーブルからグルーミングによってデータが削除されたため、データが欠落している可能性があります。保持期間は、サマリーデータの粒度によっても異なる場合があります。粒度の低いデータ（分単位）は、粒度の高いデータ（日単位）よりも早くグルーミングされます。グルーミングによってある粒度からデータが欠落している場合でも、より高い粒度で見つかる可能性があります。API

呼び出しは要求された特定の粒度のみを返すため、ある粒度でデータが受信されないからといって、同じ期間のより高い粒度でデータが存在しないという意味ではありません。

- **タイムゾーン。** メトリックはUTCタイムスタンプで保存されます。サマリーテーブルは時間単位のタイムゾーン境界で集計されます。時間単位の境界に該当しないタイムゾーンの場合、データが集計される場所に関して多少の不一致が生じる可能性があります。

粒度と保持

Directorによって取得される集計データの粒度は、要求された時間 (T) スパンの関数です。ルールは次のとおりです。

- 0 \< T \<= 1時間 - 分単位の粒度を使用
- 0 \< T \<= 30日 - 時間単位の粒度を使用
- T \> 31日 - 日単位の粒度を使用

集計データから取得されない要求データは、生のセッションおよび接続情報から取得されます。このデータは急速に増加する傾向があるため、独自のグルーミング設定があります。グルーミングにより、関連データのみが長期的に保持されます。グルーミングは、レポートに必要な粒度を維持しながら、より良いパフォーマンスを保証します。Premiumライセンスサイトのお客様は、グルーミング保持期間を希望する保持日数に変更できます。変更しない場合はデフォルトが使用されます。サイトデータベースとの接続が失われた場合、Monitor Serviceは以下の表に指定されているPremiumエンタイトルメントのデフォルトの保持日数を使用します。

設定にアクセスするには、Delivery Controller™ で次のPowerShellコマンドを実行します。

```
asnp Citrix.*

 Get-MonitorConfiguration

 Set-MonitorConfiguration -<setting name> <value>
```

	設定名	影響を受けるグルーミング	PREMIUMの保持日数	ADVANCEDの保持日数
1	GroomSessionsRetentionDays	セッション終了後のセッションおよび接続レコードの保持	90	31

	設定名	影響を受けるグルーミング	PREMIUMの保持日数	ADVANCEDの保持日数
2	GroomFailuresRetentionDays	MachineFailureLog および ConnectionFailureLog レコード	90	31
3	GroomLoadIndexesRetentionDays	LoadIndex レコード	90	31
4	GroomDeletedRetentionDays	LifecycleStateが「Deleted」であるマシン、カタログ、デスクトップグループ、およびハイパーバイザーエンティティ。この設定は、関連するセッション、セッション詳細、概要、障害、またはロードインデックスのレコードも削除します。	90	31
5	GroomSummariesRetentionDays	DesktopGroupSummary、FailureLogSummary、および LoadIndexSummaryのレコード。集計データ - 日次粒度。	365	31
6	GroomMachineHotfixLogRetentionDays	VDAおよびコントローラーマシンに適用された	90	31

	設定名	影響を受けるグルーミング	PREMIUMの保持日数	ADVANCEDの保持日数
		ホットフィックス		
7	GroomMinuteRetentionDays	集計データ - 分単位の粒度	3	3
8	GroomHourlyRetentionDays	集計データ - 時間単位の粒度	32	31
9	GroomApplicationInstanceRetentionDays	アプリケーションインスタンスの履歴	90	該当なし
10	GroomNotificationLogRetentionDays	通知ログレコード	90	該当なし
11	GroomResourceUsageRawDataRetentionDays	リソース使用率データ - 生データ	3	3
12	GroomResourceUsageMinuteDataRetentionDays	リソース使用率サマリーデータ - 分単位の粒度	7	7
13	GroomResourceUsageHourDataRetentionDays	リソース使用率サマリーデータ - 時間単位の粒度	30	30
14	GroomResourceUsageDayDataRetentionDays	リソース使用率サマリーデータ - 日単位の粒度	365	31
15	GroomProcessUsageRawDataRetentionDays	プロセス使用率データ - 生データ	1	1

	設定名	影響を受けるグルーミング	PREMIUMの保持日数	ADVANCEDの保持日数
16	GroomProcessUsageMinuteDataRetentionDays	プロセス使用率データ - 分単位の粒度	3	3
17	GroomProcessUsageHourDataRetentionDays	プロセス使用率データ - 時間単位の粒度	7	7
18	GroomProcessUsageDayDataRetentionDays	プロセス使用率データ - 日単位の粒度	30	30
19	GroomSessionMetricsDataRetentionDays	セッションメトリックデータ	1	1
20	GroomMachineMetricDataRetentionDays	マシンメトリックデータ	3	3
21	GroomMachineMetricDaySummaryDataRetentionDays	マシンメトリックサマリーデータ	365	31
22	GroomApplicationErrorsRetentionDays	アプリケーションエラーデータ	1	1
23	GroomApplicationFaultsRetentionDays	アプリケーション障害データ	1	1

注意：

> Monitor Serviceデータベースの値を変更した場合、新しい値を有効にするにはサービスを再起動する必要があります。Monitor Serviceデータベースへの変更は、Citrixサポートの指示の下でのみ行うことをお勧めします。

> GroomProcessUsageRawDataRetentionDays、GroomResourceUsageRawDataRetentionDays、およびGroomSessionMetricsDataRetentionDaysの設定は、デフォルト値の1に制限されています。一方、GroomProcessUsageMinuteDataRetentionDaysはデフォルト値の3に制限されています。プロセス使用状況データは急速に増加する傾向があるため、これらの値を設定するPowerShellコマンドは無効になっています。 また、ライセンスに基づく保持設定は次のとおりです。

- **Premiumライセンスサイト -** すべての設定のグルーミング保持期間は1000日（Citrixは365日を推奨）に制限されています。
- **Advancedライセンスサイト -** すべての設定のグルーミング保持期間は31日に制限されています。
- **その他のすべてのサイト -** すべての設定のグルーミング保持期間は7日間に制限されます。

例外:

- GroomApplicationInstanceRetentionDaysは、Premiumライセンスサイトでのみ設定できます。
- GroomApplicationErrorsRetentionDaysおよびGroomApplicationFaultsRetentionDaysは、Premiumライセンスサイトでは31日間に制限されます。

長期間データを保持すると、テーブルサイズに以下の影響があります:

- **時間単位のデータ。** 時間単位のデータを最大2年間データベースに残すことを許可すると、1000のデリバリーグループを持つサイトでは、データベースが次のように増大する可能性があります。

  1000のデリバリーグループ x 24時間/日 x 365日/年 x 2年 = 17,520,000行のデータ。集計テーブルにこれほど大量のデータがあると、パフォーマンスへの影響は甚大です。ダッシュボードデータはこのテーブルから取得されるため、データベースサーバーへの要件が大きくなる可能性があります。過度に大量のデータは、パフォーマンスに劇的な影響を与える可能性があります。

- **セッションおよびイベントデータ。** セッションが開始され、接続/再接続が行われるたびに収集されるデータです。大規模なサイト（10万ユーザー）の場合、このデータは急速に増加しま

す。たとえば、これらのテーブルの2年分のデータは1TBを超える量になり、ハイエンドのエンタープライズレベルのデータベースが必要になります。

Citrix Director の障害理由とトラブルシューティング

以下の表は、さまざまな障害カテゴリ、その理由、および問題を解決するために必要なアクションについて説明しています。詳細については、「列挙型、エラーコード、および説明」を参照してください。

接続障害エラー

カテゴリ	理由	問題	アクション
該当なし	[0] 不明。このエラーコードはマッピングされていません。	監視サービスは、ブローカリングサービスから共有された情報から、報告された起動または接続障害の理由を特定できません。	コントローラーでCDFログを収集し、Citrixサポートに連絡してください。
[0] なし	[1] なし	なし	該当なし
[2] MachineFailure	[2] SessionPreparation	デリバリーコントローラーからVDAへのセッション準備要求が失敗しました。考えられる原因: コントローラーとVDA間の通信の問題、準備要求の作成中にブローカーサービスで発生した問題、またはVDAが要求を受け入れない原因となるネットワークの問題。	コントローラーとVDA間の通信の問題を引き起こす一般的な問題については、ナレッジセンターの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops」に記載されているトラブルシューティング手順を参照してください。

カテゴリ	理由	問題	アクション
[2] MachineFailure	[3] RegistrationTimeout	VDAは電源がオンになっていましたが、デリバリーコントローラーへの登録中にタイムアウトが発生しました。	デリバリーコントローラーでCitrix Broker Serviceが実行されていること、およびVDAでDesktopサービスが実行されていることを確認してください。停止している場合は、それぞれを開始してください。
[1] ClientConnectionFailure	[4] ConnectionTimeout	VDAがセッション起動のために準備された後、クライアントがVDAに接続しませんでした。セッションは正常に仲介されましたが、クライアントがVDAに接続するのを待っている間にタイムアウトが発生しました。考えられる原因: ファイアウォール設定、ネットワークの中断、またはリモート接続を妨げる設定。	Directorコンソールで、クライアントが現在アクティブな接続を持っているかどうかを確認してください。これは、ユーザーに影響がないことを意味します。セッションが存在しない場合は、クライアントとVDAのイベントログでエラーがないか確認してください。クライアントとVDA間のネットワーク接続に関する問題を解決してください。
[4] NoLicensesAvailable	[5] ライセンス	ライセンス要求が失敗しました。考えられる原因: ライセンス数が不足している、またはライセンスサーバーが30日以上ダウンしている。	ライセンスサーバーがオンラインで到達可能であることを確認します。ライセンスサーバーへのネットワーク接続の問題を解決するか、ライセンスサーバーが誤動作しているように見える場合は再起動

カテゴリ	理由	問題	アクション
			します。環境内に十分なライセンスがあることを確認し、必要に応じて追加で割り当てます。
[1] ClientConnectionFailure	[6] チケッティング	チケッティング中にエラーが発生しました。これは、VDAへのクライアント接続がブローカーされた要求と一致しないことを示しています。起動要求チケットはブローカーによって準備され、ICA®ファイルで配信されます。ユーザーがセッションを起動しようとすると、VDAはICAファイル内の起動チケットをブローカーで検証します。考えられる原因：ICAファイルが破損しているか、ユーザーが不正な接続を試みている。	デリバリーグループで定義されているユーザーグループに基づいて、ユーザーがアプリケーションまたはデスクトップにアクセスできることを確認します。ユーザーにアプリケーションまたはデスクトップを再起動するよう指示し、これが一時的な問題であるかどうかを判断します。問題が再度発生する場合は、クライアントデバイスのイベントログでエラーを確認します。ユーザーが接続しようとしているVDAが登録されていることを確認します。登録されていない場合は、VDAのイベントログを確認し、登録に関する問題を解決します。
[1] ClientConnectionFailure	[7] その他	クライアントが最初にVDAに接続した後、接続シーケンスが完了する前に、セッションがVDAか	起動前にユーザーによってセッションが終了されていないことを確認します。セッションの再起動を試み、問題が解決

カテゴリ	理由	問題	アクション
		ら終了したと報告されました。	しない場合は、CDFログを収集してCitrixサポートに連絡してください。
[1] ClientConnectionFailure	[8] 一般的な失敗	セッションの起動に失敗しました。考えられる原因：ブローカーがまだ起動中または初期化中にブローカーによる起動が要求された、または起動のブローカーフェーズ中に内部エラーが発生した。	Citrix Broker Serviceが実行中であることを確認し、セッションの起動を再試行します。
[5] 構成	[9] メンテナンスモード	VDA、またはVDAが属するデリバリーグループがメンテナンスモードに設定されています。	メンテナンスモードが必要かどうかを判断します。不要な場合は、該当するデリバリーグループまたはマシンでメンテナンスモードを無効にし、ユーザーに再接続を試みるよう指示します。
[5] 構成	[10] アプリケーション無効	アプリケーションは管理者によって無効にされているため、エンドユーザーはアクセスできません。	アプリケーションが本番環境で使用されることを意図している場合は、アプリケーションを有効にし、ユーザーに再接続するよう指示します。
[4] 利用可能なライセンスなし	[11] ライセンス機能拒否	使用されている機能は、既存のライセンスではカバーされていません。	既存のCitrix Virtual Apps and Desktops™ライセンスのエディションとタイプでカバーされ

カテゴリ	理由	問題	アクション
			ている機能を確認するには、Citrixの営業担当者にお問い合わせください。
[3] 利用可能な容量なし	[13] セッション制限に到達	すべてのVDAが使用中であり、これ以上セッションをホストする容量がありません。考えられる原因：すべてのVDAが使用中である（シングルセッションOS VDAの場合）、またはすべてのVDAが設定された最大同時セッション数に達している（マルチセッションOS VDAの場合）。	メンテナンスモードになっているVDAがないか確認します。容量を増やすために不要な場合は、メンテナンスモードを無効にします。サーバーVDAあたりのセッション数を増やすには、Citrixポリシー設定の**最大セッション数**の値を増やすことを検討してください。マルチセッションOS VDAを追加することを検討してください。シングルセッションOS VDAを追加することを検討してください。
[5] 構成	[14] 許可されていないプロトコル	ICAおよびRDPプロトコルは許可されていません。	デリバリーコントローラーで **Get-BrokerAccessPolicyRule** PowerShellコマンドを実行し、**AllowedProtocols** の値に目的のプロトコルがすべてリストされていることを確認します。この問題は、構成が誤っている場合にのみ発生します。

カテゴリ	理由	問題	アクション
[5] 構成	[15] リソースが利用できません	ユーザーが接続しようとしているアプリケーションまたはデスクトップが利用できません。このアプリケーションまたはデスクトップが存在しないか、実行できるVDAがありません。考えられる原因：アプリケーションまたはデスクトップが非公開になっている、アプリケーションまたはデスクトップをホストしているVDAが最大負荷に達している、またはアプリケーションまたはデスクトップがメンテナンスモードに設定されている。	アプリケーションまたはデスクトップがまだ公開されており、VDAがメンテナンスモードではないことを確認します。マルチセッションOS VDAが最大負荷に達しているかどうかを判断します。その場合は、マルチセッションOS VDAをさらにプロビジョニングします。接続に利用できるシングルセッションOS VDAがあることを確認します。必要に応じて、シングルセッションOS VDAをさらにプロビジョニングします。
[5] 構成	[16] アクティブセッションの再接続が無効	ICAセッションはアクティブで、別のエンドポイントに接続されています。ただし、**Active Session Reconnection** が無効になっているため、クライアントはアクティブなセッションに接続できません。	デリバリーコントローラーで、**Active Session Reconnection** が有効になっていることを確認します。レジストリの **HKEY_LOCAL_MACHINE\Software\Citrix\Desktop\Server** の下にある **DisableActiveSessionReconnect** の値が0に設定されていることを確認します。

カテゴリ	理由	問題	アクション
[2] マシン障害	[17] 再接続するセッションがありません	クライアントは特定のセッションに再接続しようとしましたが、セッションは終了しました。	ワークスペースコントロールの再接続を再試行してください。
[2] MachineFailure	[18] SpinUpFailed	VDAをセッション起動のために電源オンにできません。これはハイパーバイザーが報告した問題です。	マシンがまだ電源オフの状態である場合は、Citrix Studioからマシンの起動を試みてください。これが失敗した場合は、ハイパーバイザーの接続と権限を確認してください。VDAがPVSプロビジョニングされたマシンである場合は、PVSコンソールでマシンが実行中であることを確認してください。そうでない場合は、マシンにPersonal vDiskが割り当てられていることを確認し、ハイパーバイザーにログインしてVMをリセットしてください。
[2] MachineFailure	[19] 拒否	デリバリーコントローラーは、エンドユーザーからの接続に備えるようVDAに要求を送信しますが、VDAはこの要求を積極的に拒否します。	pingを使用して、デリバリーコントローラーとVDAが正常に通信できることを確認してください。通信できない場合は、ファイアウォールまたはネットワークルーティングの問題

カテゴリ	理由	問題	アクション
			を解決してください。
[2] MachineFailure	[20] 構成セット失敗	デリバリーコントローラーは、セッション起動中にポリシー設定やセッション情報などの必要な構成データをVDAに送信しませんでした。考えられる原因：コントローラーとVDA間の通信の問題、構成セット要求の作成中にBroker Serviceで発生した問題、またはVDAが要求を受け入れない結果となったネットワークの問題。	-
[3] NoCapacityAvailable	[21] MaxTotalInstancesExceeded	アプリケーションのインスタンスの最大数に達しました。VDA上でアプリケーションの追加インスタンスを開くことはできません。この問題は、アプリケーション制限機能に関連しています。	ライセンスが許可する場合、アプリケーション設定の「**同時に実行するインスタンスの数を制限する**」をより高い値に増やすことを検討してください。
[3] NoCapacityAvailable	[22] MaxPerUserInstancesExceeded	ユーザーはアプリケーションの複数のインスタンスを開こうとしていますが、アプリケーションはユーザーごとに1つのインスタンスのみを許可するように構成されています。こ	デフォルトでは、ユーザーごとに1つのアプリケーションインスタンスのみが許可されます。ユーザーごとに複数のインスタンスが必要な場合は、アプリケーション設定で「**ユー**

カテゴリ	理由	問題	アクション
		の問題は、アプリケーション制限機能に関連しています。	**ザーごとに1つのインスタンスに制限する**」設定をクリアすることを検討してください。
[1] ClientConnectionFailure	[23] 通信エラー	デリバリーコントローラーは、接続の準備要求などの情報をVDAに送信しようとしましたが、通信中にエラーが発生しました。これはネットワーク障害が原因である可能性があります。	既に開始されている場合は、VDA上のデスクトップサービスを再起動して登録プロセスを再開し、VDAが正常に登録されていることを確認してください。アプリケーションイベントログの詳細を通じて、VDA用に構成されているデリバリーコントローラーが正確であることを確認してください。
[3] NoCapacityAvailable	[100] NoMachineAvailable 監視サービスは、[12] NoDesktopAvailable をこのエラーコードに変換します。	セッションを起動するために割り当てられたVDAが無効な状態であるか、利用できません。考えられる原因：VDAの電源状態が不明または利用できない、前回のユーザーセッション以降VDAが再起動されていない、現在のセッションで有効にする必要があるにもかかわらずセッション共有が無効になっている、またはVDAがデリバリーグループまたはサイトから削除された。	VDAがデリバリーグループにあることを確認してください。そうでない場合は、適切なデリバリーグループに追加してください。ユーザーが要求した公開共有デスクトップまたはアプリケーションを起動できるように、十分なVDAが登録され、準備状態にあることを確認してください。VDAをホストしているハイパーバイザーがメンテナンスモードではないこ

カテゴリ	理由	問題	アクション
			とを確認してください。
[2] MachineFailure	[101] MachineNotFunctional. 監視サービスは、[12] NoDesktopAvailable をこのエラーコードに変換します。	VDAが動作していません。考えられる原因：VDAがデリバリーグループから削除された、VDAが未登録である、VDAの電源状態が利用できない、またはVDAで内部的な問題が発生している。	VDAがデリバリーグループに属していることを確認します。属していない場合は、適切なデリバリーグループに追加します。Citrix StudioでVDAが電源オンとして表示されていることを確認します。複数のマシンの電源状態が不明な場合は、ハイパーバイザーへの接続の問題やホストの障害を解決します。VDAをホストしているハイパーバイザーがメンテナンスモードではないことを確認します。これらの問題が解決されたら、VDAを再起動します。

マシン障害の種類

エラーコード	エラーコードID	問題	アクション
不明	-	-	-
未登録	3	-	-
MaxCapacity (Director では最大負荷として表示)	4	マシンが最大容量、つまり最大負荷インデックスに達していると報告しています	すべてのハイパーバイザーの電源がオンになっていることを確認します。ハイパーバイザーの容量を増やすか、ハイ

エラーコード	エラーコードID	問題	アクション
			パーバイザーを追加して、影響を受けるデリバリーグループにマシンを追加します。
StuckOnBoot	2	VM が起動シーケンスを完了せず、ハイパーバイザーと通信していません。	VM がハイパーバイザー上で正常に起動したことを確認します。OS の問題など、VM 上の他のメッセージを確認します。ハイパーバイザーツールが VM にインストールされていることを確認します。VDA が VM にインストールされていることを確認します。
FailedToStart	1	VM がハイパーバイザー上で起動しようとしたときに問題が発生しました。	ハイパーバイザーのログを確認します。
なし	0	-	-

マシンの登録解除理由 (障害の種類が「未登録」または「不明」の場合に適用)

エラーコード	エラーコードID	問題	アクション
AgentShutdown	0	VDAが正常にシャットダウンされました。	既存の電源管理ポリシーに基づいてVDAがオフになることが想定されない場合は、VDAの電源をオンにしてください。イベントログでエ

エラーコード	エラーコードID	問題	アクション
			ラーを確認してください。
AgentSuspended	1	VDAは休止状態またはスリープモードです。	VDAを休止モードから解除してください。電源設定を通じてCitrix Virtual Apps and Desktops VDAの休止機能を無効にすることを検討してください。
IncompatibleVersion	100	Citrixプロトコルバージョンの不一致により、VDAがデリバリーコントローラーと通信できません。	VDAとデリバリーコントローラーのバージョンを合わせます。
AgentAddressResolutionFailed	101	デリバリーコントローラーがVDAのIPアドレスを解決できませんでした。	VDAマシンアカウントがADに存在することを確認します。存在しない場合は作成します。DNS内のVDAの名前とIPアドレスが正確であることを確認します。正確でない場合は修正します。広範囲にわたる場合は、デリバリーコントローラーのDNS設定を検証します。コントローラーから`nslookup`コマンドを実行してDNS解決を確認します。
[Cloud]:AgentAddressResolutionFailed	101	デリバリーコントローラーがVDAのIPアドレスを解決できませんでした。	VDAマシンアカウントがADに存在することを確認します。存在しない場合は作成

エラーコード	エラーコードID	問題	アクション
			します。DNS内のVDAの名前とIPアドレスが正確であることを確認します。正確でない場合は修正します。
AgentNotContactable	102	デリバリーコントローラーとVDA間で通信の問題が発生しました。	pingを使用して、デリバリーコントローラーとVDAが正常に通信できることを確認します。通信できない場合は、ファイアウォールまたはネットワークの問題を解決します。コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。
[Cloud]: AgentNotContactable	102	デリバリーコントローラーとVDAの間で通信の問題が発生しました。	コントローラーとVDA間の通信問題を引き起こす一般的な問題については、ナレッジセンターの記事「Troubleshooting

エラーコード	エラーコードID	問題	アクション
			Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。Citrixサポートにお問い合わせください。
AgentWrongActiveDirectoryOU	103	Active Directoryの検出設定が誤っています。VDAレジストリで構成されているサイト固有のOU（サイトコントローラー情報がADに保存されている場所）が、別のサイト用です。	Active Directoryの設定が正しいことを確認するか、レジストリ設定を確認してください。
EmptyRegistrationRequest	104	VDAからデリバリーコントローラーに送信された登録要求が空でした。これは、VDAソフトウェアのインストールが破損していることが原因である可能性があります。	VDA上のDesktopサービスを再起動して登録プロセスを再開し、アプリケーションイベントログを介してVDAが正しく登録されていることを確認してください。
MissingRegistrationCapabilities	105	VDAのバージョンがデリバリーコントローラーと互換性がありません。	VDAをアップグレードするか、VDAを削除してから再インストールします。
MissingAgentVersion	106	VDAのバージョンがデリバリーコント	問題がすべてのマシンに影響している場

エラーコード	エラーコードID	問題	アクション
		ローラーと互換性がありません。	合は、VDAソフトウェアを再インストールします。
InconsistentRegistrationCapabilities	107	VDAはBrokerにその機能を通信できません。これは、VDAとデリバリーコントローラーのバージョン間の非互換性が原因である可能性があります。バージョンごとに変更される登録機能は、登録要求と一致しない形式で表現されています。	VDAとデリバリーコントローラーのバージョンを合わせます。
NotLicensedForFeature	108	使用しようとしている機能はライセンスされていません。	Citrixライセンスエディションを確認するか、VDAを削除してから再インストールします。
[Cloud]: NotLicensedForFeature	108	使用しようとしている機能はライセンスされていません。	Citrixサポートにお問い合わせください。
サポートされていないCredentialSecurityバージョン	109	VDAとデリバリーコントローラーは、同じ暗号化メカニズムを使用していません。	VDAとデリバリーコントローラーのバージョンを合わせてください。
無効な登録要求	110	VDAはBrokerに登録要求を行いましたが、要求の内容が破損しているか無効です。	コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration

エラーコード	エラーコードID	問題	アクション
			with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。
SingleMultiSessionの不一致	111	VDAのオペレーティングシステムタイプは、マシンカタログまたはデリバリーグループと互換性がありません。	VDAを、同じオペレーティングシステムを持つマシンを含む正しいマシンカタログタイプまたはデリバリーグループに追加してください。
カタログに対して機能レベルが低すぎます	112	マシンカタログが、インストールされているVDAバージョンよりも高いVDA機能レベルに設定されています。	VDAのマシンカタログ機能レベルがVDAの機能レベルと一致していることを確認します。VDAの機能レベルと一致するようにマシンカタログをアップグレードまたはダウングレードします。
FunctionalLevelTooLowForDesktopGroup	113	デリバリーグループが、インストールされているVDAバージョンよりも高いVDA機能レベルに設定されています。	VDAのデリバリーグループ機能レベルがVDAの機能レベルと一致していることを確認します。VDAの機能レベルと一致するようにマシンカタログをアップグレードまたはダウングレードします。

エラーコード	エラーコードID	問題	アクション
PowerOff	200	VDAが正常にシャットダウンされませんでした。	VDAが電源オン状態であるべき場合は、Citrix StudioからVDAを起動し、正しく起動して登録されることを確認してください。起動または登録に関する問題をトラブルシューティングします。VDAが再び稼働したら、イベントログを確認してシャットダウンの根本原因を特定するのに役立ててください。
AgentRejectedSettingsUpdate	203	Citrixポリシーなどの設定が変更または更新されましたが、VDAへの更新の送信中にエラーが発生しました。これは、更新がインストールされているVDAバージョンと互換性がない場合に発生する可能性があります。	必要に応じてVDAをアップグレードします。適用された更新がVDAバージョンでサポートされているかどうかを確認します。
SessionPrepareFailure	206	ブローカーは、VDAで実行されているセッションの監査を完了しませんでした。	広範囲にわたる場合は、デリバリーコントローラーでCitrix Broker Serviceを再起動してください。
[Cloud]: SessionPrepareFailure	206	ブローカーは、VDAで実行されているセッションの監査を完了しませんでした。	Citrixサポートにお問い合わせください。

エラーコード	エラーコードID	問題	アクション
ContactLost	207	デリバリーコントローラーはVDAとの接続を失いました。これはネットワーク障害が原因である可能性があります。	デリバリーコントローラーでCitrix Broker Serviceが実行されており、VDAでDesktopサービスが実行されていることを確認してください。停止している場合はそれぞれを起動します。すでに起動している場合は、VDA上のDesktopサービスを再起動して登録プロセスを再開し、VDAが正常に登録されることを確認してください。アプリケーションイベントログの詳細を通じて、VDA用に構成されたデリバリーコントローラーが正確であることを確認してください。pingを使用して、デリバリーコントローラーとVDAが正常に通信できることを確認してください。通信できない場合は、ファイアウォールまたはネットワークの問題を解決してください。
[Cloud]: ContactLost	207	デリバリーコントローラーはVDAとの接続を失いました。これはネットワーク	VDA上でDesktopサービスが実行されていることを確認します。停止している場合は開始します。

エラーコード	エラーコードID	問題	アクション
		障害が原因である可能性があります。	
BrokerRegistrationLimitReached	301	デリバリーコントローラーは、同時に登録できるVDAの構成済み最大数に達しました。デフォルトでは、デリバリーコントローラーは10,000の同時VDA登録を許可します。	サイトにデリバリーコントローラーを追加するか、サイトを作成することを検討してください。また、**HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\MaxWorkers** レジストリキーを介して、デリバリーコントローラーに同時に登録できるVDAの数を増やすこともできます。詳細については、ナレッジセンターの記事「Citrix Virtual Apps and Desktops で使用されるレジストリキーエントリ (CTX117446)」を参照してください。この数を増やすと、コントローラーにより多くのCPUおよびメモリリソースが必要になる場合があります。
SettingsCreationFailure	208	ブローカーは、VDAに送信する設定と構成のセットを構築しませんでした。ブローカーがデータを収集できない場合、登録は失敗し、VDA	デリバリーコントローラーのイベントログでエラーがないか確認してください。ログに特定の問題が明らかでない場合は、Broker Serviceを再起動して

エラーコード	エラーコードID	問題	アクション
		は登録解除されます。	ください。Broker Serviceが再起動されたら、影響を受けるVDAでDesktopサービスを再起動し、正常に登録されることを確認してください。
[Cloud]: SettingsCreationFailure	208	ブローカーは、VDAに送信する設定と構成のセットを構築しませんでした。ブローカーがデータを収集できない場合、登録は失敗し、VDAは登録解除されます。	影響を受けるVDAでDesktopサービスを再起動し、正常に登録されることを確認してください。Citrixサポートに連絡してください。
SendSettingsFailure	204	ブローカーは設定および構成データをVDAに送信しませんでした。ブローカーがデータを収集できても送信できない場合、登録は失敗します。	単一のVDAに限定されている場合は、VDA上のDesktopサービスを再起動して再登録を強制し、アプリケーションイベントログを介してVDAが正常に登録されていることを確認します。発生したエラーをトラブルシューティングします。コントローラーとVDA間の通信問題を引き起こす一般的な問題については、ナレッジセンターの記事「Troubleshooting Virtual Delivery Agent Registration with delivery

エラーコード	エラーコードID	問題	アクション
			controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。
AgentRequested	2	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
DesktopRestart	201	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
DesktopRemoved	202	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
SessionAuditFailure	205	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
UnknownError	300	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
RegistrationStateMismatch	302	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
不明	-	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。

サードパーティ通知

Citrix Virtual Apps and Desktops™ のこのリリースには、以下のドキュメントで定義されている条件に基づいてライセンスされたサードパーティソフトウェアが含まれている場合があります。

- Citrix Virtual Apps and Desktops サードパーティ通知(/ja-jp/citrix-virtual-apps-desktops/2407/downloads/third-party-notices-apps-and-desktops.pdf) (PDFダウンロード)
- FlexNet Publisher 2017 (11.15.0.0) の非商用ソフトウェア開示(/ja-jp/citrix-virtual-apps-desktops/2407/downloads/fnp-licensing-11-15-0-ncsd-summary.pdf) (PDFダウンロード)
- FlexNet Publisher 11.15.0 で使用されている FlexNet Publisher ドキュメント補足 サードパーティおよびオープンソースソフトウェア(/ja-jp/citrix-virtual-apps-desktops/2407/downloads/fnp-licensing-11-15-0-opensource.pdf) (PDFダウンロード)

SDKおよびAPI

このリリースでは、いくつかのSDKとAPIが利用可能です。SDKとAPIにアクセスするには、Build anything with Citrixにアクセスしてください。そこから、**Citrix Workspace**を選択して、Citrix Virtual Apps and Desktopsおよび関連コンポーネントのプログラミング情報にアクセスします。

> **注:**
>
> Citrix Virtual Apps and Desktops™ SDKとCitrix Group Policy SDKは、モジュールまたはスナップインとしてインストールできます。いくつかのコンポーネントSDK（Citrix Licensing、Citrix Provisioning、StoreFrontなど）は、スナップインのみを使用してインストールされます。

> この製品は、PowerShellバージョン3から5をサポートしています。

シトリックス仮想アプリおよびデスクトップSDK

Delivery Controller™またはStudioをインストールすると、このSDKはPowerShellモジュールとして自動的にインストールされます。これにより、スナップインを追加することなく、このSDKのコマンドレットを使用できます。（このSDKをスナップインとしてインストールすることを選択した場合の指示は以下に記載されています。）

権限

Citrix管理権限を持つIDを使用してシェルまたはスクリプトを実行する必要があります。Controller上のローカル管理者グループのメンバーは、Citrix Virtual AppsまたはCitrix Virtual Desktops™をインストールするための完全な管理権限を自動的に持っていますが、Citrixは、通常の操作では、ローカル管理者アカウントを使用するのではなく、適切な権限を持つCitrix管理者を作成することを推奨しています。

コマンドレットにアクセスして実行する

1. PowerShellでシェルを起動します。Studioを開き、**PowerShell**タブを選択し、**Launch PowerShell**をクリックします。

2. スクリプト内でSDKコマンドレットを使用するには、PowerShellで実行ポリシーを設定します。PowerShellの実行ポリシーについては、Microsoftのドキュメントを参照してください。
3. モジュールではなくスナップインを使用する場合は、`Add-PSSnapin`（または`asnp`）コマンドレットを使用してスナップインを追加します。

   V1とV2はスナップインのバージョンを示します。XenDesktop 5のスナップインはバージョン1です。Citrix Virtual Apps and Desktops、および以前のXenDesktop 7バージョンのスナップインはバージョン2です。たとえば、Citrix Virtual Apps and Desktopsスナップインをインストールするには、`Add-PSSnapin Citrix.ADIdentity.Admin.V2`と入力します。すべてのコマンドレットをインポートするには、`Add-PSSnapin Citrix.*.Admin.V*`と入力します。

これで、コマンドレットとヘルプファイルを使用できます。

- このSDKのヘルプファイルにアクセスするには、Categoriesリストで製品またはコンポーネントを選択し、次に**Citrix Virtual Apps and Desktops SDK**を選択します。
- PowerShellのガイダンスについては、Windows PowerShell Integrated Scripting Environment (ISE)を参照してください。

グループポリシーSDK

Citrix Group Policy SDKを使用すると、グループポリシーの設定とフィルターを表示および構成できます。このSDKは、PowerShellプロバイダーを使用して、マシンおよびユーザーの設定とフィルターに対応する仮想ドライブを作成します。このプロバイダーは、`New-PSDrive`の拡張機能として表示されます。

Group Policy SDKを使用するには、StudioまたはCitrix Virtual Apps and Desktops SDKのいずれかがインストールされている必要があります。

Citrix Group Policy PowerShell プロバイダーは、モジュールまたはスナップインとして利用できます。

- モジュールを使用する場合、追加の作業は不要です。
- スナップインを追加するには、`Add-PSSnapin citrix.common.grouppolicy` と入力します。

ヘルプにアクセスするには、`help New-PSDrive -path localgpo:/` と入力します。

仮想ドライブを作成し、設定をロードするには、`New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>`と入力します。ここで、Controller文字列は、接続して設定をロードしたいサイト内のControllerの完全修飾ドメイン名です。

シトリックス バーチャルアプリおよびデスクトップ REST API

Citrix Virtual Apps and Desktops REST APIを使用すると、Citrix Virtual Apps and Desktops展開内のリソース管理を自動化できます。

Citrix Virtual Apps and Desktops REST API は `<https://developer.cloud.com/citrixworkspace/citrix-daas-rest-apis/docs/citrix-virtual-apps-and-desktops-apis>` で利用できます。Citrix Virtual Apps and Desktops に適用されない API は、そのようにマークされています。そこにあるガイダンスに従って、API サービスへのアクセスを設定し、API を使用してリソースを管理および最適化してください。

モニターサービス OData

Monitor APIを使用すると、OData APIのバージョン3または4を使用してMonitor Serviceデータにアクセスできます。Monitor Serviceデータからクエリされたデータに基づいて、カスタマイズされた監視およびレポートダッシュボードを作成できます。OData V.4はASP.NET Web APIに基づいており、集計クエリをサポートしています。

詳細については、Monitor Service OData API を参照してください。

__index__

コスト最適化

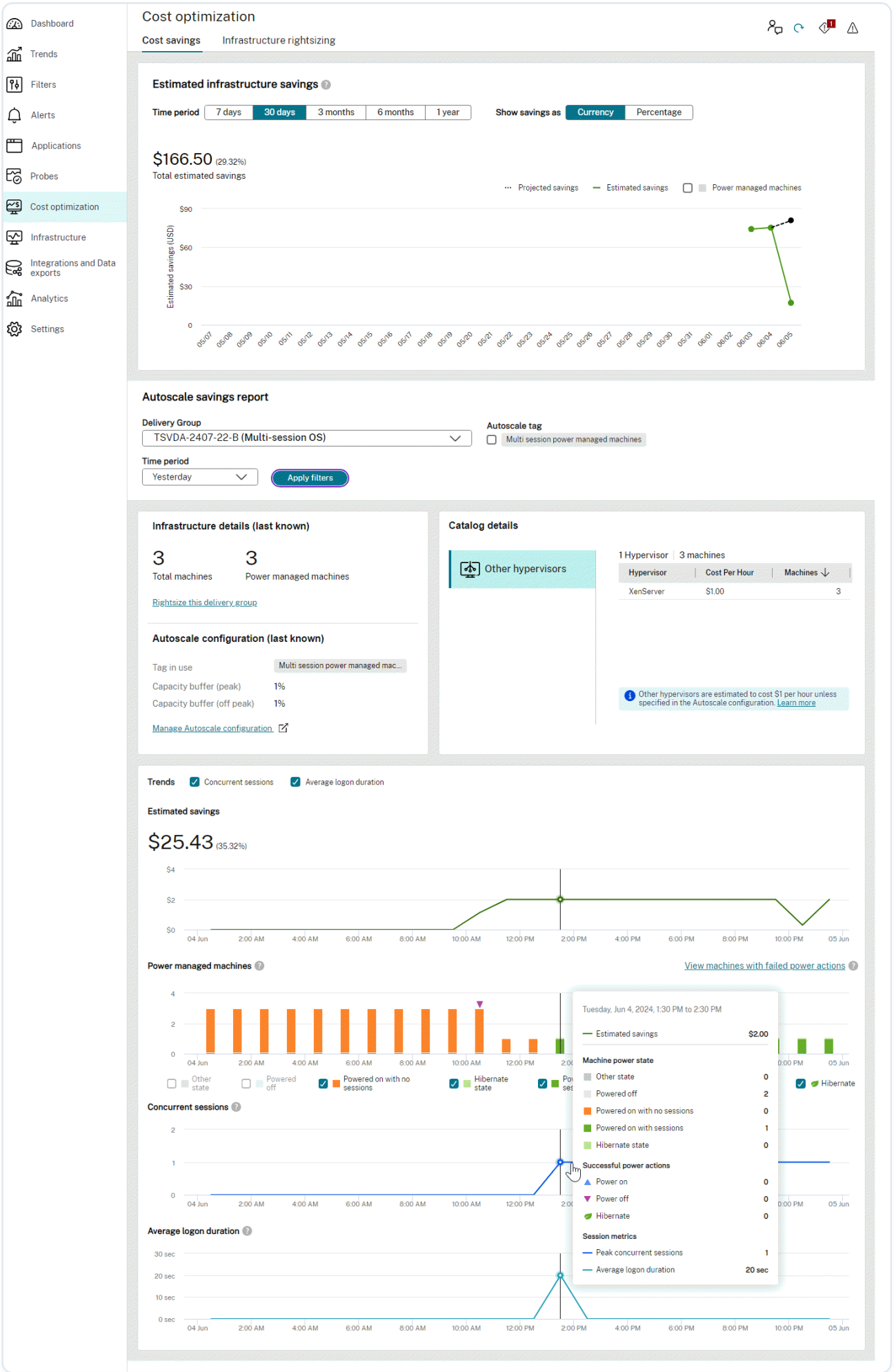
Citrix Director に、仮想マシンとセッションの利用状況を効果的に分析するのに役立つ「コスト最適化」という新機能が導入されました。この機能は、コストを最適化する方法について洞察に満ちた視覚的表現を提供します。また、不要なマシンを排除し、それによってコストを削減するのにも役立ちます。

コスト最適化をサポートするために、以下の警告も導入されています。

- 電源オン失敗アクションと電源オフ失敗アクション
- マシン稼働時間アラート

最近の電源アクションを持つマシンを検査して、ユーザーの問題を引き起こす電源オンの失敗や、コストを増加させる電源オフの失敗を分析することもできます。詳細については、「最近の電源アクションを持つマシンを検査する」セクションを参照してください。

ホームページの左メニューから**コスト最適化**タブをクリックして、**コスト最適化**ページにアクセスします。


Dashboard
Trends
Filters
Alerts
Applications
Probes
Cost optimization
Infrastructure
Integrations and Data exports
Analytics
Settings
Cost optimization
Cost savings
Infrastructure rightsizing
Estimated infrastructure savings
Time period
7 days
30 days
3 months
6 months
1 year
Show savings as
Currency
Percentage
$166.50 (29.32%)
Total estimated savings
Projected savings
Estimated savings
Power managed machines
Estimated savings (USD)
$90
$60
$30
0
05/07
05/08
05/09
05/10
05/11
05/12
05/13
05/14
05/15
05/16
05/17
05/18
05/19
05/20
05/21
05/22
05/23
05/24
05/25
05/26
05/27
05/28
05/29
05/30
05/31
06/01
06/02
06/03
06/04
06/05
Autoscale savings report
Delivery Group
TSVDA-2407-22-B (Multi-session OS)
Autoscale tag
Multi session power managed machines
Time period
Yesterday
Apply filters
Infrastructure details (last known)
3
Total machines
3
Power managed machines
Rightsize this delivery group
Autoscale configuration (last known)
Tag in use
Multi session power managed mac...
Capacity buffer (peak)
1%
Capacity buffer (off peak)
1%
Manage Autoscale configuration
Catalog details
Other hypervisors
1 Hypervisor | 3 machines
Hypervisor
Cost Per Hour
Machines
XenServer
$1.00
3
Other hypervisors are estimated to cost $1 per hour unless specified in the Autoscale configuration. Learn more
Trends
Concurrent sessions
Average logon duration
Estimated savings
$25.43 (35.32%)
$4
$2
$0
04 Jun
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
05 Jun
Power managed machines
View machines with failed power actions
Other state
Powered off
Powered on with no sessions
Hibernate state
Hibernate
Tuesday, Jun 4, 2024, 1:30 PM to 2:30 PM
Estimated savings
$2.00
Machine power state
Other state
0
Powered off
2
Powered on with no sessions
0
Powered on with sessions
1
Hibernate state
0
Successful power actions
Power on
0
Power off
0
Hibernate
0
Session metrics
Peak concurrent sessions
1
Average logon duration
20 sec
Concurrent sessions
Average logon duration
30 sec
20 sec
10 sec
0 sec

コスト最適化ホームページでは、次のことができます。

- 開始リンク - このリンクにアクセスして、コスト最適化機能の詳細を確認してください。
- コスト最適化ページを確認する - **コスト最適化**ページに関するフィードバックを提供できます
- データを更新します。
- アラートを表示する - 重大なアラートと警告アラートの両方を表示できます。

コスト最適化ページには、次の機能が含まれています。

- コスト削減
- インフラストラクチャの適正化

コスト最適化のためのコストはどのように計算されますか?

マシンあたりの時間あたりのコストは、ハイパーバイザーがサポートする通貨で表示されます。このセクションでは、Azure マシンおよびその他のマシンのコストがどのように計算されるかについて説明します。

Azureマシンのコスト

コスト計算の優先順位は次のとおりです:

1. 'Microsoft.Consumption/pricesheets/read 権限が利用可能な場合、実効価格は Azure サブスクリプションで構成されている通貨で表示されます。
2. 権限が利用できない場合、Azure の小売価格が表示されます。詳細については、Azure Retail Prices overview を参照してください。
3. 実効価格または小売価格が利用できない場合、Web Studio で管理者が入力したコストに基づいてコストが表示されます。
4. Web Studio でコストが指定されていない場合、デフォルトのコストとして 1 ドルが考慮されます。

Azureのアカウント詳細を確認し、実効価格を見つけるために必要な権限を追加するには、次の手順を実行します:

1. Citrix DaaS に移動します。
2. **ホスティング**タブをクリックして、ホスティング接続アカウントを見つけます。
3. **ホスティング**タブに記載されている**アプリケーション ID** を探します。

   ホスティングタブ(/en-us/citrix-virtual-apps-desktops/2407/media/daas-azure-hosting.png)
4. Azure AD に移動し、ステップ 3 でメモした**アプリケーション ID** を探します。

5. **サブスクリプション** > **アクセス制御 (IAM)** に移動し、ホスティング接続SPN用に構成されたカスタマイズされた役割を選択します。

   Azure ポータル(/en-us/citrix-virtual-apps-desktops/2407/media/azure-portal.png)

   Azure ポータルのサブスクリプション(/en-us/citrix-virtual-apps-desktops/2407/media/azure-portal-subscriptions.png)

6. 役割に *Microsoft.Consumption/pricesheets/read* 権限を追加します。

Azureの小売価格を確認する方法?

`Microsoft.Consumption/pricesheets/read` が利用できない場合、Azure の小売価格が表示されます。現在、Retail Rates Prices API を使用して、すべての Azure サービスの小売価格を取得できます。以前は、Azure サービスの価格を取得する唯一の方法は、Azure 料金計算ツールを使用するか、Azure portal を使用することでした。詳細については、Azure Retail Prices の概要 を参照してください。

Azure 以外のマシンのコスト計算

その他のマシンについては、Web Studio で管理者が入力したコストに基づいてコストが表示されます。Web Studio でコストが指定されていない場合、デフォルトのコスト $1 が考慮されます。

コスト削減

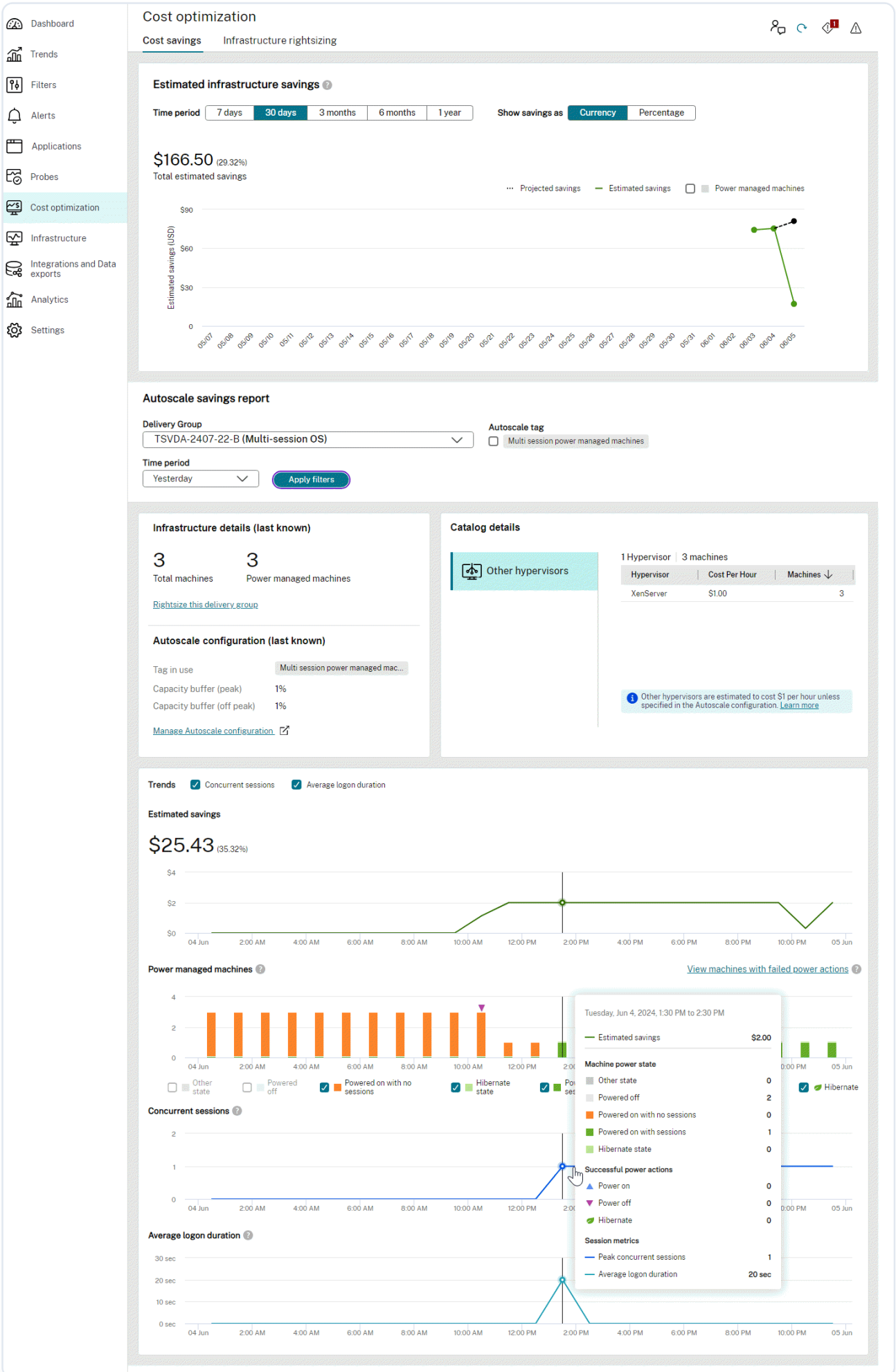
「コスト削減」ページでは、選択した期間にわたって蓄積されたインフラストラクチャの節約額を視覚的に表示し、残りの日数で予想される節約額を予測します。このページは、マシンの使用状況とセッションを分析することで、達成された節約とコスト削減の機会を特定するのに役立ちます。このページでは、以下を提供します。

- インフラストラクチャコストの最適化に関する洞察
- 節約された金額
- 予測コストを超える可能性のあるさまざまなシナリオに関する情報
- インフラストラクチャコストの節約を実現するための特定と戦略的計画の潜在的な機会

マシンの使用状況は通常、ピーク時に増加し、リソースの増加を要求します。Autoscale™機能は、需要の低い期間中に未使用のマシンを自動的に電源オフにすることで、コスト削減に役立ちます。予測される節約額は、この使用パターンに依存します。ただし、未使用のマシンが存在する場合や、Autoscaleの電源アクションに障害がある場合など、特定の状況下ではコストが予想を超える可能性があります。これらの発生の背後にある理由を特定することは、以前は困難でした。

「**コスト最適化**」ページでは、予想コストを超える可能性のあるさまざまなシナリオに関する詳細情報を提供します。同様に、例えば、セッションのないマシンがある場合、さらなるコスト削減の機会を示します。

ホームページの左側のメニューから**コスト最適化**タブをクリックして、**コスト最適化**ページにアクセスします。


Dashboard
Trends
Filters
Alerts
Applications
Probes
Cost optimization
Infrastructure
Integrations and Data exports
Analytics
Settings
Cost optimization
Cost savings
Infrastructure rightsizing
Estimated infrastructure savings
Time period
7 days
30 days
3 months
6 months
1 year
Show savings as
Currency
Percentage
$166.50 (29.32%)
Total estimated savings
Projected savings
Estimated savings
Power managed machines
Estimated savings (USD)
$90
$60
$30
0
05/07
05/08
05/09
05/10
05/11
05/12
05/13
05/14
05/15
05/16
05/17
05/18
05/19
05/20
05/21
05/22
05/23
05/24
05/25
05/26
05/27
05/28
05/29
05/30
05/31
06/01
06/02
06/03
06/04
06/05
Autoscale savings report
Delivery Group
TSVDA-2407-22-B (Multi-session OS)
Autoscale tag
Multi session power managed machines
Time period
Yesterday
Apply filters
Infrastructure details (last known)
3
Total machines
3
Power managed machines
Rightsize this delivery group
Autoscale configuration (last known)
Tag in use
Multi session power managed mac...
Capacity buffer (peak)
1%
Capacity buffer (off peak)
1%
Manage Autoscale configuration
Catalog details
Other hypervisors
1 Hypervisor | 3 machines
Hypervisor
Cost Per Hour
Machines
XenServer
$1.00
3
Other hypervisors are estimated to cost $1 per hour unless specified in the Autoscale configuration. Learn more
Trends
Concurrent sessions
Average logon duration
Estimated savings
$25.43 (35.32%)
$4
$2
$0
04 Jun
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
05 Jun
Power managed machines
View machines with failed power actions
Tuesday, Jun 4, 2024, 1:30 PM to 2:30 PM
Estimated savings
$2.00
Machine power state
Other state
0
Powered off
2
Powered on with no sessions
0
Powered on with sessions
1
Hibernate state
0
Successful power actions
Power on
0
Power off
0
Hibernate
0
Session metrics
Peak concurrent sessions
1
Average logon duration
20 sec
Other state
Powered off
Powered on with no sessions
Hibernate state
Hibernate
Concurrent sessions
Average logon duration
30 sec
20 sec
10 sec
0 sec

コスト最適化ページには、**推定節約額**と**Autoscale節約レポート**が含まれています。

推定節約額: このグラフィカルな表示は、インフラストラクチャリソースの効率的な利用を評価するのに役立ちます。コスト削減額は、ハイパーバイザーの通貨で、または発生したコストのパーセンテージとして表示されます。以下の期間の結果を表示できます。

- 7日間
- 30日間
- 3か月間
- 6ヶ月
- 12ヶ月

推定節約額グラフには、次の情報が表示されます。

- 推定節約額 - 選択した期間にインフラストラクチャで達成された節約額を表示します
- 電源管理されたマシン - 電源管理されたマシンの総数を表示します
- 予測節約額 - 残りの期間でどれだけのインフラストラクチャ節約が可能かを表示します
- 平均ログオン時間 - 選択した期間におけるユーザーの平均ログオン時間を表示します。

Autoscale節約レポート: このグラフィカル表示は、Autoscale機能が構成および有効化されているデリバリーグループの節約レポートを提供します。このレポートは、電源管理されたマシンにのみ適用されます。デリバリーグループを選択し、今日、昨日、先週、来週、今月、または来月のデータを選択できます。グラフにカーソルを合わせると、特定のグラフ値を取得できます。

> **注:**
>
> デリバリーグループが削除された場合、Autoscale節約レポートでデータを取得することはできません。

> デリバリーグループのドロップダウンリストから、以下のオプションにドリルダウンできます。

- **すべて**: インフラストラクチャの詳細には、すべてのデリバリーグループ情報が表示されます。
- **シングルセッション**: シングルセッションマシンであるすべてのデリバリーグループのインフラストラクチャの詳細と、グラフにカーソルを合わせたときに表示されるマシンの電源状態、成功したAutoscale電源アクション、およびセッションのグラフィカル表示。

- **マルチセッション**: マルチセッションマシンであるすべてのデリバリーグループのインフラストラクチャの詳細と、グラフィカル表示。

データは選択した期間で表示されます。**推定節約額**のグラフィカル表示は、ドロップダウンメニューから選択された実際の節約額です。ピークポイントにカーソルを合わせると、マシンの電源状態、成功したAutoscale電源アクション、およびセッションに関する情報が表示されます。

選択したデリバリーグループに基づいて、次の詳細を表示できます。

- **インフラストラクチャの詳細**
  - 総マシン数と電源管理対象マシン数 - 総マシン数と、そのうち電源管理されているマシン数を表示します。このデータは、残りの電源管理されていないマシンを電源管理対象マシンに変換することを検討し、Autoscale機能を有効にしてより包括的なカバレッジを実現するさらなる機会を提供します。インフラストラクチャの詳細セクションのデータは、1時間ごとに更新される最新の既知の情報を表示します。
- **カタログの詳細**

  ハイパーバイザー（サービスプロバイダー）の名前を表示します。詳細については、「サポートされているVDAホスティングプラットフォーム」を参照してください。カタログの詳細のデータは、現在の時点で利用可能な最新のデータ（ライブデータ）を表示します。

  次の詳細を取得できます。

  - **ハイパーバイザー名** - サイトが接続されているハイパーバイザーの名前を表示します。複数のハイパーバイザーが存在する場合は、利用可能なすべてのハイパーバイザーを表示します。
  - **インスタンス** - インスタンスの名前を表示します。
  - **1時間あたりのコスト** - ハイパーバイザーがサポートする通貨で、マシン1台あたりの1時間あたりのコストを表示します。Azureマシンでは、Microsoft.Consumption/pricesheets/read権限が利用可能な場合、Azureサブスクリプションで構成されている通貨で実効価格が表示されます。権限が利用できない場合は、Azureの小売価格が表示されます。詳細については、「Azure Retail Prices overview」を参照してください。その他のマシンについては、Web Studioで管理者が入力したコストに基づいてコストが表示されます。Web Studioでコストが指定されていない場合、デフォルトのコストは1ドルです。詳細については、「コスト最適化のコストはどのように計算されますか？」を参照してください。
  - **マシン** - 選択したインスタンスのマシン数を表示します。
- **Autoscale構成（最新の既知）**

使用中のタグ - Web StudioのAutoscale設定で構成されているマシンのタグを表示します。タグ付けされたマシンに基づいてデータをフィルタリングすることもできます。この場合、タグ付けされたマシンの概要のみが表示されます。

容量バッファ（ピーク時） および **容量バッファ（オフピーク時）**

ピーク時およびオフピーク時のデリバリーグループの最大要件に基づいて、電源がオンになっているマシンのバッファの割合を表示します。

- **推定節約額**

  選択した期間におけるインフラストラクチャで達成された節約額を表示します。

- **電源管理対象マシン**

  Autoscaleが有効になっている場合、コストを最適化するために、使用されていない電源管理されたマシンはオフになります。以下の詳細情報を取得できます。

  - 電源がオフになったマシンの数 - このデータは、電源がオフになり、コスト削減に貢献したマシンの数を分析するのに役立ちます。
  - 休止状態 - このデータは、休止状態にあるマシンの数を分析するのに役立ちます。
  - セッションなしで稼働中のマシン - このデータは、なぜマシンがセッションなしでアクティブであったかを分析する機会を提供します。このデータは、より効果的なインフラストラクチャ節約戦略を計画する機会を提供します。
  - セッションありで稼働中のマシン - このデータは、電源がオンになり、アクティブなセッションがあったマシンの数を分析するのに役立ちます。
  - 電源オフ - このデータは、電源がオフまたは一時停止されたマシンの数と、そのアクションがいつ実行されたかを分析するのに役立ちます。このデータを確認し、さらに変更を加えることで、コスト削減に貢献できます。
  - 電源オン - このデータは、電源がオンになったマシンの数と、そのアクションがいつ実行されたかを分析するのに役立ちます。このデータを確認し、さらに変更を加えることで、コスト削減に役立ちます。

- **同時セッション**

  選択した時点でのセッションの総数を表示します。このデータは、コスト最適化のためにマシンをいつ電源オフにするかを判断するのに役立ちます。

- **平均ログオン時間**

  選択した期間におけるユーザーの平均ログオン時間を表示します。

インフラストラクチャの適正化

「**インフラストラクチャの適正化**」ページでは、リソース使用率に基づいてデリバリーグループのプロビジョニングとサイジングの側面を分析できます。この分析に基づいて、次のことができます。

- 未使用のリソースへの支出を削減する
- 特定のデリバリーグループの消費に対して、マシンが過剰、不足、または適正なサイズであるかを識別する
- 使用率が主にパワーユーザーによって推進されているかどうかを識別する（グループの他のマシンと比較して、上位5パーセンタイルのマシンによる使用率が高いことによって示されます）

インフラストラクチャの適正化は、以下を使用してフィルタリングできます。

- デリバリーグループ - シングルセッションOSまたはマルチセッションOSのデリバリーグループをフィルタリングできます。
- タグ - タグはマシンに適用されるタグ名です。したがって、同じタグを持つマシンをフィルタリングできます。最大5つのタグを複数選択できます。複数のタグを選択すると、選択されたマシンタグのいずれかが少なくとも1つ適用されているすべてのマシンをフィルタリングできます。
- 期間 - 過去24時間、7日間、30日間のデータをフィルタリングできます。

インフラストラクチャの適正化ページでは、次の機能が提供されます。

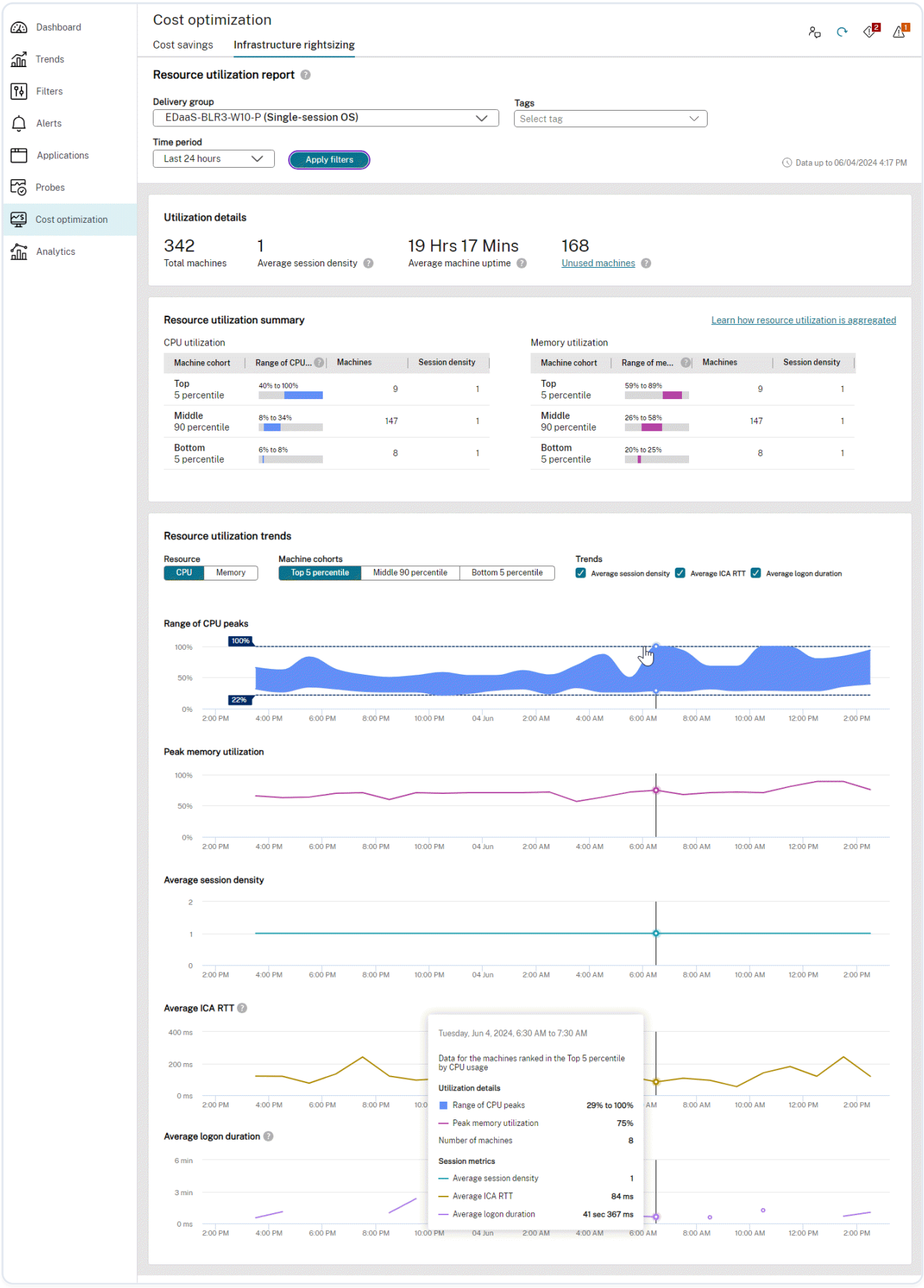
- 使用率の詳細に関するインサイト
- リソース使用率の概要
- リソース使用率の傾向

このページに表示される集計データは、次のように更新されます。

- 過去24時間および過去7日間のフィルターでは1時間ごと
- 「過去30日間」フィルターの場合の1日

ホームページの左メニューから「**コスト最適化**」タブをクリックします。次に、「**インフラストラクチャの適正化**」タブをクリックして、「**インフラストラクチャの適正化**」ページにアクセスします。

「**コスト最適化**」タブ > 「**コスト削減**」にある「**インフラストラクチャの詳細**」セクションから「**このデリバリーグループを適正化**」リンクをクリックして、「**インフラストラクチャの適正化**」ページにアクセスすることもできます。



「インフラストラクチャの適正化」ページには、次のものが含まれます。

- 使用率の詳細

- リソース使用率の概要
- リソース使用率の傾向

「**利用状況の詳細**」: このセクションでは、選択したデリバリーグループと選択したタグの利用状況に関する詳細情報を提供します。過去24時間、7日間、30日間の詳細を表示できます。「利用状況の詳細」セクションでは、選択した時間フィルターの全期間の詳細情報を提供します。たとえば、7日間が選択されている場合、合計マシン数は、その7日間のいずれかの時点で稼働していたマシンの総数です。「利用状況の詳細」セクションでは、次の情報を提供します。

- 「**合計マシン数**」- マシンの総数を表示します。これには、選択した期間中に電源がオンになっていたすべてのマシンが含まれます。たとえば、7日間が選択されている場合、合計マシン数は、その7日間のいずれかの時点で稼働していたマシンの総数です。
- 「**平均セッション密度**」- これは、マシンの数と選択した期間にわたる平均です。マシン上のセッション負荷の量を指し、セッションで利用可能なリソースに影響を与えます。
- 「**平均マシン稼働時間**」- これは、電源管理されているマシンの総稼働時間と選択した期間の比率です。1日あたりのマシンごとの稼働時間です。たとえば、1つのデリバリーグループまたは選択したタグに2台のマシンがあり、1台のマシンが24時間使用され、もう1台のマシンが1時間使用された場合、平均マシン稼働時間は12時間30分です。この例では、選択されたフィルター値は「過去24時間」です。
- 「**未使用のマシン**」- 選択した期間中にセッションがなかったが、電源がオンのままだったマシンの数を表示します。「**未使用のマシン**」リンクをクリックして「**フィルター**」タブを開くと、現在電源がオンになっていてセッションがない、同じデリバリーグループ内のすべてのマシンを表示できます。

「**リソース利用状況の概要**」: このセクションでは、選択したデリバリーグループと選択したタグのリソースがどのように利用されたかについての概要を提供します。最大5つのタグを選択できます。過去24時間、7日間、30日間の詳細を表示できます。マシンは利用状況に基づいてランク付けされます。「リソース利用状況の概要」セクションでは、アクティブなセッションを持つマシンのCPU使用率とメモリ使用率に関する詳細情報を提供します。

- 「**CPU使用率**」:
  - Machine cohort - CPU使用率に基づいて、上位、中間、下位に分類されたマシン群に関する情報を提供します。最も使用頻度の高いマシンの5%は**上位5パーセンタイル**に、最も使用頻度の低いマシンの5%は**下位5パーセンタイル**に、残りの90%は**中間90パーセンタイル**に分類されます。
  - Range of CPU Peaks - マシンコホートに対応するCPU使用率に基づいて、CPUピークの範囲を表示します。

  - Machines - マシンコホートに対応するマシンの数を表示します。
  - Session density - マシンコホートに対応するセッション密度を表示します。

- **メモリ使用率**:
  - Machine cohort - メモリ使用率に基づいて、上位、中間、下位に分類されたマシン群に関する情報を提供します。最も使用頻度の高いマシンの5%は**上位5パーセンタイル**に、最も使用頻度の低いマシンの5%は**下位5パーセンタイル**に、残りの90%は**中間90パーセンタイル**に分類されます。
  - Range of memory Peaks - マシンコホートに対応するメモリ使用率に基づいて、メモリピークの範囲を表示します。
  - Machines - マシンコホートに対応するマシンの数を表示します。
  - Session density - マシンコホートに対応するセッション密度を表示します。

次の表は、セクションに表示される値に基づいて実行できる可能性のあるアクション項目に関する情報を提供します。

シナリオ	アクション項目
CPU使用率が高い	デリバリーグループのCPU仕様を増やします。または、使用率の高いユーザーを特定し、より優れた仕様の別のデリバリーグループに移動します。
CPU使用率が低い	デリバリーグループのCPU仕様を減らします。
メモリ使用率が高い	デリバリーグループのメモリ仕様を増やします。
メモリ使用率が低い	デリバリーグループのメモリ仕様を減らします。

「リソース使用率の概要」セクションのデータはどのように入力されるか?

リソース使用率の概要セクションのデータは、**リソース使用率の傾向**のデータに基づいて入力されます。概要には、アクティブなセッションを持つマシンのみの詳細が表示されます。5台を超えるマシンがある場合、概要はより良い結果を提供します。

選択したデリバリーグループ内のマシンの数に基づいて、最大および最小使用率が計算されます。

たとえば、期間として「過去7日間」を選択し、選択したデリバリーグループに20台のマシンがあるとします。これらの20台のマシンは、さらに**上位5パーセンタイル**、**中間90パーセンタイル**、**下位5パーセンタイル**に分類されます。CPUとメモリの使用率は、アクティブなセッションがある場合に計算されます。たとえば、このケースでは、最初と最後のマシンが上位5パーセンタイルと下位5パーセンタイルに入ります。残りの18台のマシンは中間90パーセンタイルに分類されます。このケースでは、**上位5パーセンタイル**にマシンが1台しかないため、最大値と最小値は同じです。コホートに複数のマシンがある場合、コホートの最高値と最低値は、そのグループで最もランクの高いマシンの最大値と、最もランクの低いマシンの最大値にそれぞれ基づいています。

リソースタイプとして**CPU**を選択すると、選択したマシンの**CPUピークの範囲**と**ピークメモリ使用率**が表示されます。

リソースタイプとしてメモリを選択すると、選択したマシンのメモリピークの範囲とピークCPU使用率が表示されます。

リソース使用率の傾向: このセクションでは、CPUピークの範囲、ピークメモリ使用率、平均セッション密度、平均ICA® RTT、および平均ログオン期間のグラフ表示を提供します。

以下の詳細をフィルターできます。

- リソース - CPUとメモリ
- マシンコホート - 上位5パーセンタイル、中間90パーセンタイル、下位5パーセンタイル
- 傾向 - 平均セッション、平均ICA RTT、平均ログオン期間。

次のグラフを表示できます。

- **CPUピークの範囲** - 帯域内のCPUピークの範囲を表示します。帯域内の任意のポイントにカーソルを合わせると、帯域の上下の値が表示されます。
- **メモリ使用率のピーク** - 選択したマシンと選択した期間のメモリ使用率の最高値をグラフで表示します。
- **平均セッション密度** - 選択したマシンと選択した期間の平均セッション密度をグラフで表示します。
- **平均ICA RTT** - セッションの平均ラウンドトリップ時間を表示します。このグラフは、アクティブなセッションがない場合やセッションが切断された場合に中断を示します。
- **平均ログオン時間** - 選択したマシンと選択した期間の平均ログオン時間をグラフで表示します。このグラフは、選択した期間中に新しいログオンが開始された場合にデータを表示します。

インフラストラクチャ監視

Directorは、Citrix Virtual Apps and Desktops™コンポーネントの運用健全性に関する可視性を提供するようになりました。この機能により、インフラストラクチャに関連する問題を簡単に特定、トラブルシューティング、解決できます。現在、Citrix Provisioning (PVS) およびStoreFrontコンポーネントの健全性が監視されています。

この機能をサポートするために、Citrix コンポーネント向けに Citrix Infrastructure Monitor という新しい Windows 実行可能ファイルが導入されました。これにより、PVS または StoreFront™ サーバーから Director への関連する健全性メトリックの収集と送信が容易になります。

この機能により、Director の単一コンソールで、PVS および StoreFront サーバーのシステムメトリックに関する重要な監視データセットとプロアクティブなアラートを取得できます。最新の情報を確保するため、監視コンポーネントから5分ごとにデータが収集されます。

この機能は、プロアクティブな監視、詳細なメトリック、および自動化されたアラートを提供することで運用効率を向上させ、Citrixインフラストラクチャがスムーズかつ効率的に稼働することを保証します。

主な機能

リアルタイム監視:

- Citrix Provisioning™ (PVS) サーバーや StoreFront などの Citrix インフラストラクチャコンポーネントの継続的な監視。
- システムの健全性、リソース使用率、および関連するパフォーマンスメトリックを表示するダッシュボードビュー。

詳細な分析:

- 各コンポーネントの接続ステータス、サービスまたはプロセスステータスなどのシステム健全性メトリックに関する詳細な分析を提供します。
- CPU、メモリ、ディスク使用率などのリソース使用率メトリックの詳細。

自動アラートと通知:

- 粒度の高いスコープを持つさまざまなメトリックと状態に対するカスタマイズ可能なアラートしきい値。
- メールとWebhookによるリアルタイム通知。

ユースケース

運用効率:

Citrix管理チームがCitrixサーバーとサービスの高い可用性とパフォーマンスを維持できるようにします。この機能は、重要なユーザーグループに影響を与える前に問題を事前に特定して管理者に警告することで、ダウンタイムを最小限に抑えるのにも役立ちます。

チケット解決の迅速化:

サーバーの健全性とパフォーマンスに関する主要なメトリックを監視し、仮想アプリケーションとデスクトップのユーザーへの最適な配信を評価します。これらのメトリックを使用して、関連コンポーネントを分析することで、パフォーマンスに関連するユーザーの苦情を診断し、解決します。

前提条件

- Citrix Virtual Apps and Desktops バージョン2407以降
- DDCでCitrix Infrastructure MonitorのHTTPSを構成します。この前提条件はオプションですが、推奨されます。詳細については、「Citrix Infrastructure MonitorのHTTPSを構成する」を参照してください。
- Citrix Infrastructure Monitorを実行するために必要なユーザーアカウントまたは権限:
    - エンドポイントマシンにCitrix Infrastructure Monitorをインストールするための Windows管理者権限を持つユーザーアカウント。
    - 次のDirector権限を持つフル管理者ユーザーアカウントまたはカスタムロール:
        - アラートポリシーの作成\編集\有効化\削除
        - アラートメールサーバー構成の作成\編集\削除
        - アラートの却下
        - アラートポリシーの表示
        - アラートの表示
        - ダッシュボードページの表示
        - インフラストラクチャモニターページの表示

> **注：**

> **アラート**ページにアクセスする権限がない場合、**インフラストラクチャ監視**ページで**アラートの管理**オプションが無効になります。

インフラストラクチャ監視の概要

ステップ1：Citrix Infrastructure Monitorのインストール

安全なデータ収集のための接続を確立するには、ターゲットコンポーネントにインストールを完了するために、以下の手順を実行します。

ステップ1.1：ターゲットコンポーネントの特定

監視が必要なPVSまたはStoreFrontサーバーなどのターゲットコンポーネントを特定します。

ステップ1.2：Citrix Infrastructure Monitorのダウンロード

ステップ1.1で特定されたターゲットサーバー上のCitrix downloadsページから`CitrixInfraMonitor.msi`をダウンロードできます。

ステップ 1.3: Citrix Infrastructure Monitor を実行する

インストールウィザードの指示に従って、ターゲットコンポーネントで`CitrixInfraMonitor.msi`インストーラーを実行します。

> **注：**
>
> 管理者権限を持つユーザーは、ターゲットコンポーネントにCitrix Infrastructure Monitorをインストールおよび構成できます。

> シトリックス インフラストラクチャ モニター(/en-us/citrix-virtual-apps-desktops/2407/media/citrixinframonitoring-resize.gif)

インストールが成功すると、「**サービス**」セクションでCitrix Infrastructure Monitorサービスを表示できます。

シトリックス インフラストラクチャ モニター(/en-us/citrix-virtual-apps-desktops/2407/media/infra-services.png)

ステップ 1.4: 登録トークンを取得する

Citrix Infrastructure Monitorがインストールされているシステムで、`C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt`にある

`RegistrationToken.txt`ファイルに記載されているトークンを取得し、ステップ3：Citrix Infrastructure Monitorを登録するで使用できるように準備しておきます。

> **注:**
>
> `CitrixInfraMonitor.msi` を正常にインストールすると、インストーラーはポート 9595 の例外を作成します。サードパーティのファイアウォールを使用している場合は、Citrix Infrastructure Monitoring サービスを使用するために、このポートの TCP 通信を手動で許可する必要がある場合があります。

ステップ 2: Citrix Infrastructure Monitor の HTTPS を構成する

> **注:**
>
> Citrix Infrastructure MonitorサービスはHTTPモードでも動作するため、この場合、以下の構成は不要です。ただし、HTTPSモードでの使用を推奨します。Citrix Infrastructure MonitorのHTTPSを構成する必要がある場合にのみ、以下の手順を実行してください。

ステップ 2.1: 証明書をマシンにアップロードする

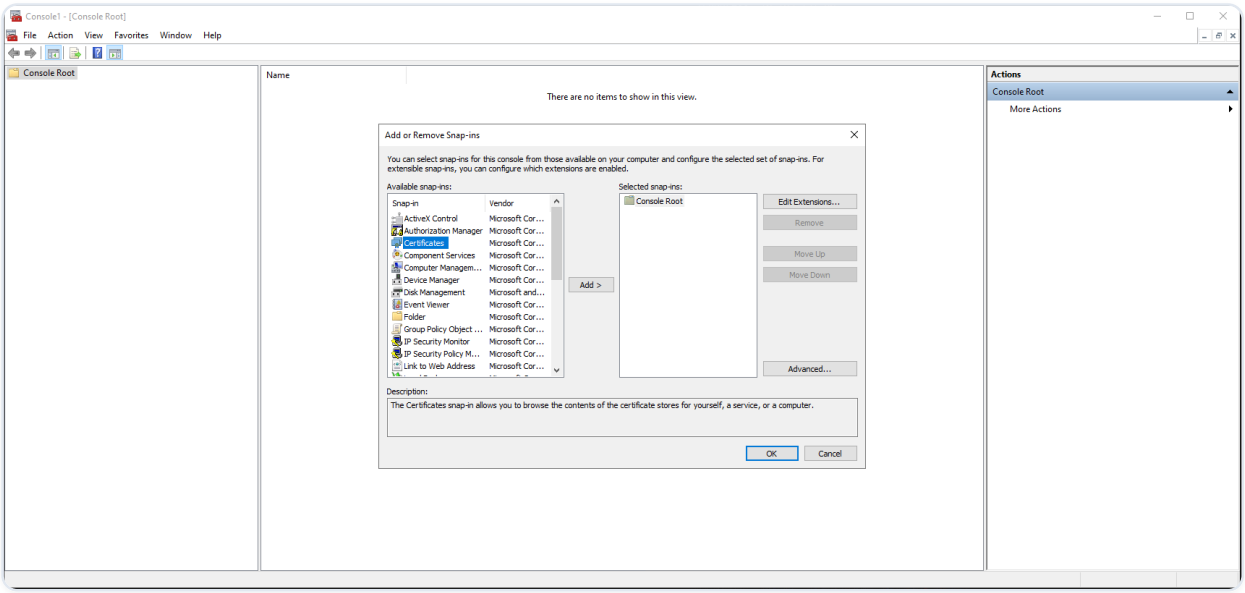
1. Citrix Infrastructure Monitorがインストールされているマシン用のPFX証明書を取得します。PFXファイルの生成の詳細については、「PFXファイルの作成方法」を参照してください。

   > **注:**
   >
   > パスワードで保護されたPFXファイルも使用できます。

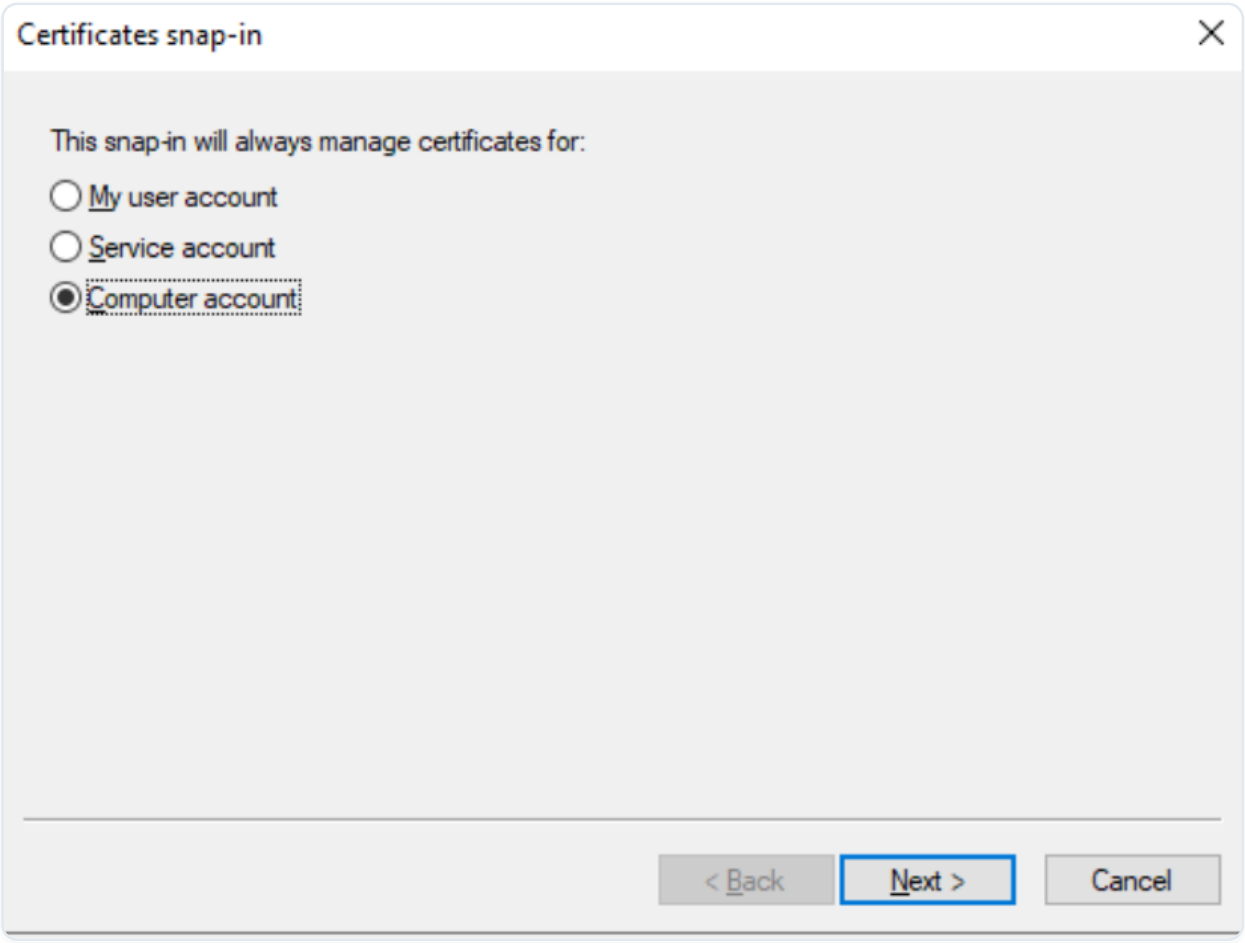
2. 証明書をマシンの任意の場所にアップロードします。

ステップ 2.2: 証明書をコンピューター証明書にインポートする

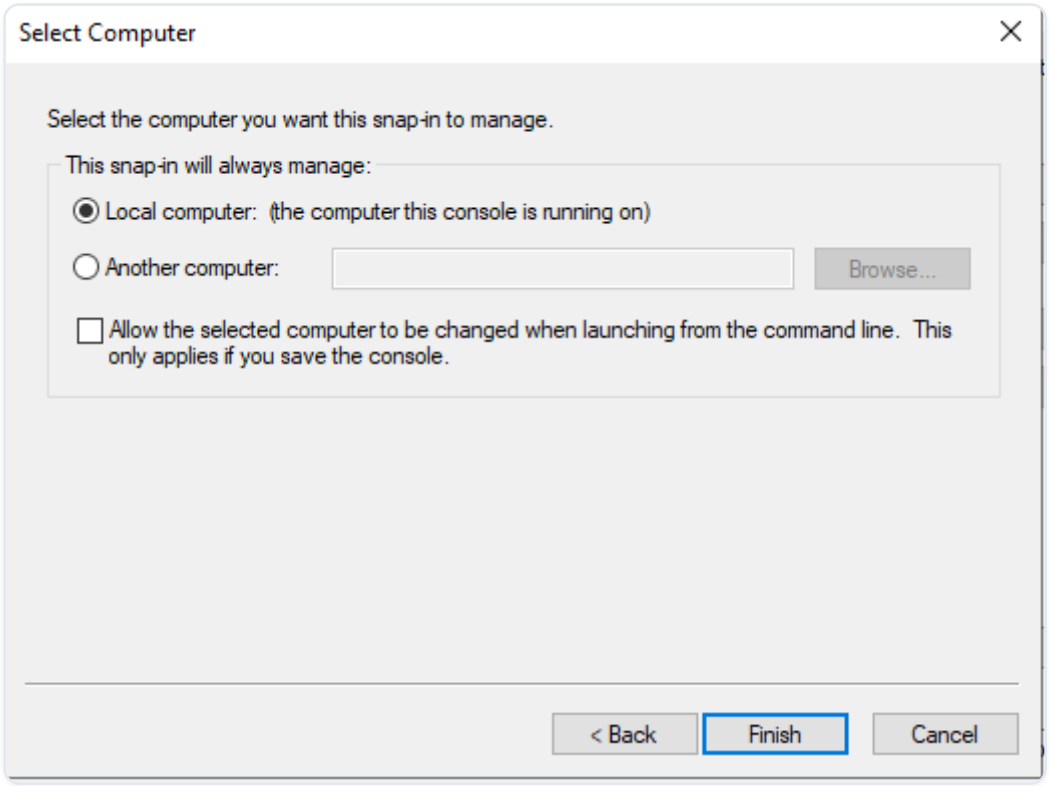
1. > をクリックし、`mmc` と入力して をクリックします。**[コンソール 1 -]** ウィンドウが表示されます。
2. メニューで をクリックします。 ウィンドウが表示されます。



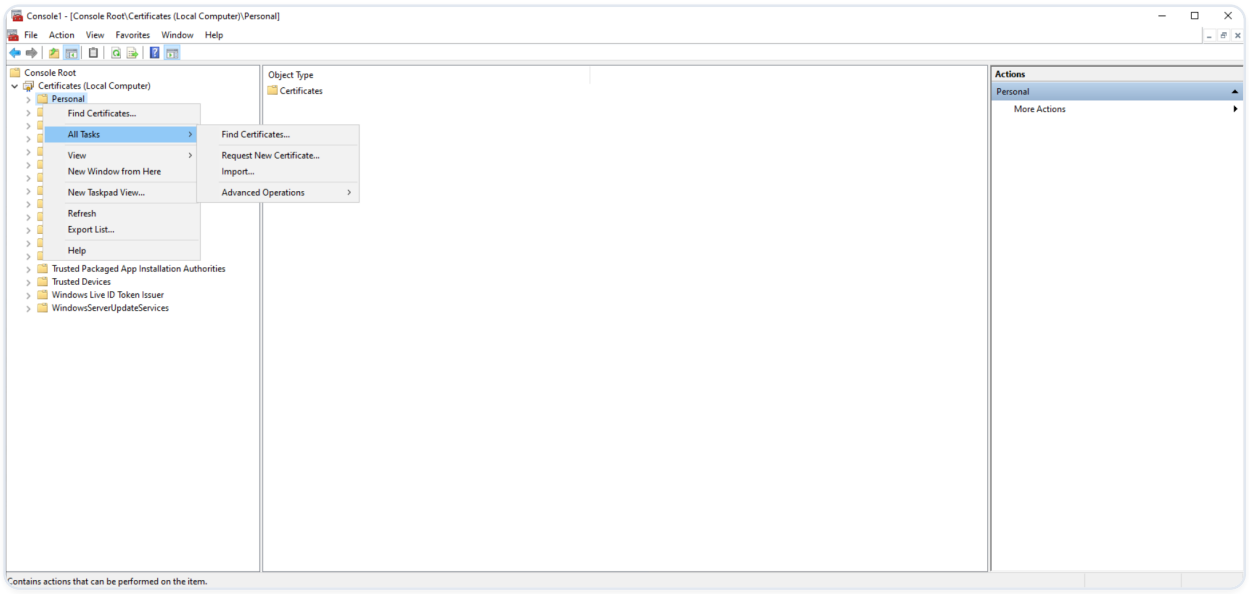
3. で をダブルクリックします。 ウィンドウが表示されます。



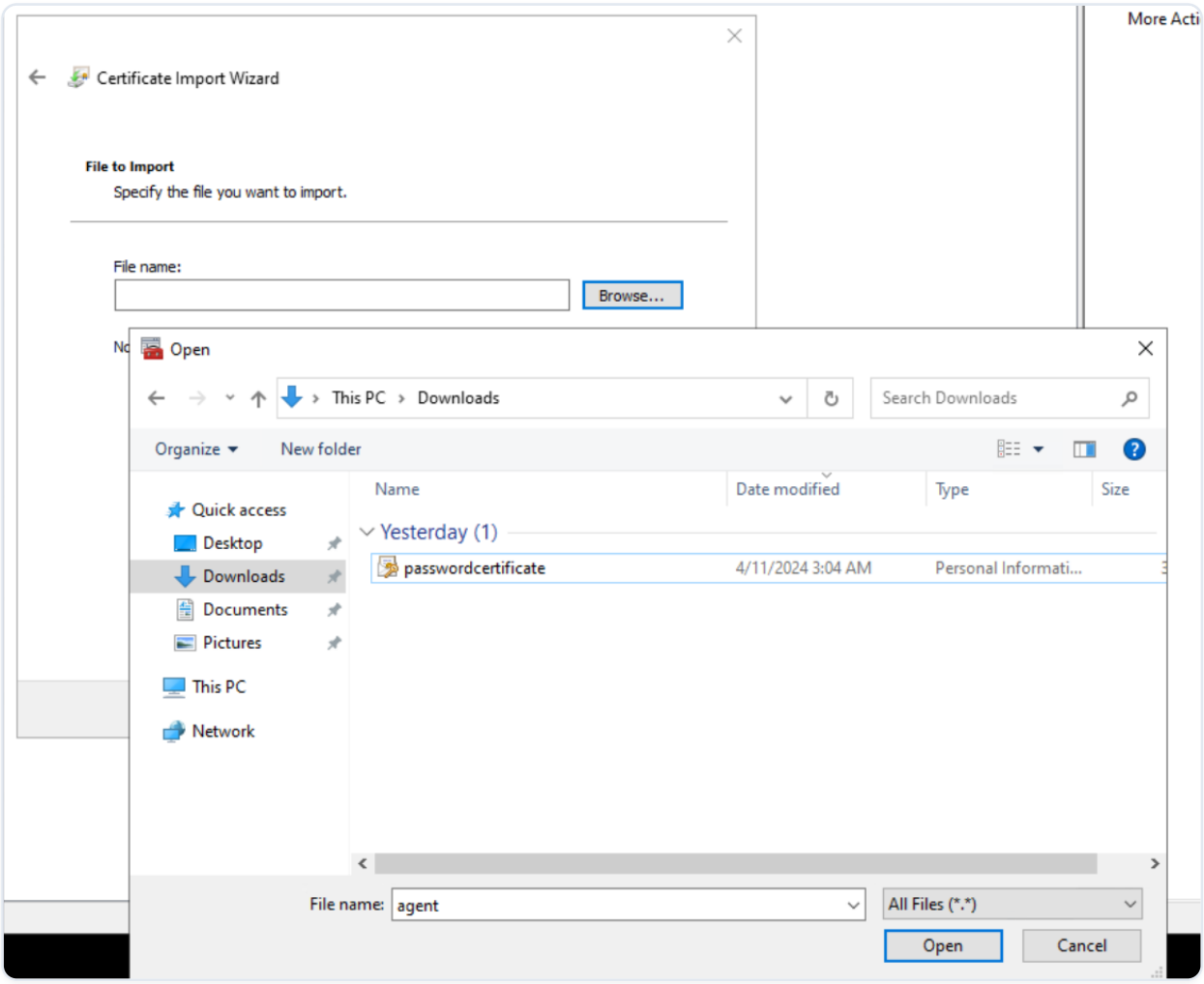
4. 「**コンピューターアカウント**」を選択し、「**次へ**」をクリックします。「**コンピューターの選択**」ウィンドウが表示されます。



5. を選択します。
6. をクリックします。新しいコンソールで選択されたスナップインのリストに セクションが表示されます。
7. をクリックします。
8. を展開し、 > > を右クリックします。 が表示されます。



9. > を選択します。PFXファイルをアップロードした場所に移動し、ファイルの種類を に変更してから、該当のPFX証明書を選択します。



10. PFXパスワードを入力します。パスワードがない場合は空白のままでかまいません。
11. **次へ**をクリックします。
12. 証明書ストアについては、「**すべての証明書を次のストアに配置する**」オプションが選択され、「**証明書ストア**」が「**個人**」として選択されていることを確認してください。

    証明書ストア(/en-us/citrix-virtual-apps-desktops/2407/media/sm-certificate-store.png)
13. **Next**をクリックします。
14. 詳細を確認し、**完了**をクリックします。
15. 確認を待ちます。「*インポートは正常に完了しました*」というメッセージが表示されます。
16. **証明書** > **個人**に移動し、証明書が存在することを確認します。
17. マシンからPFX証明書ファイルを削除します。

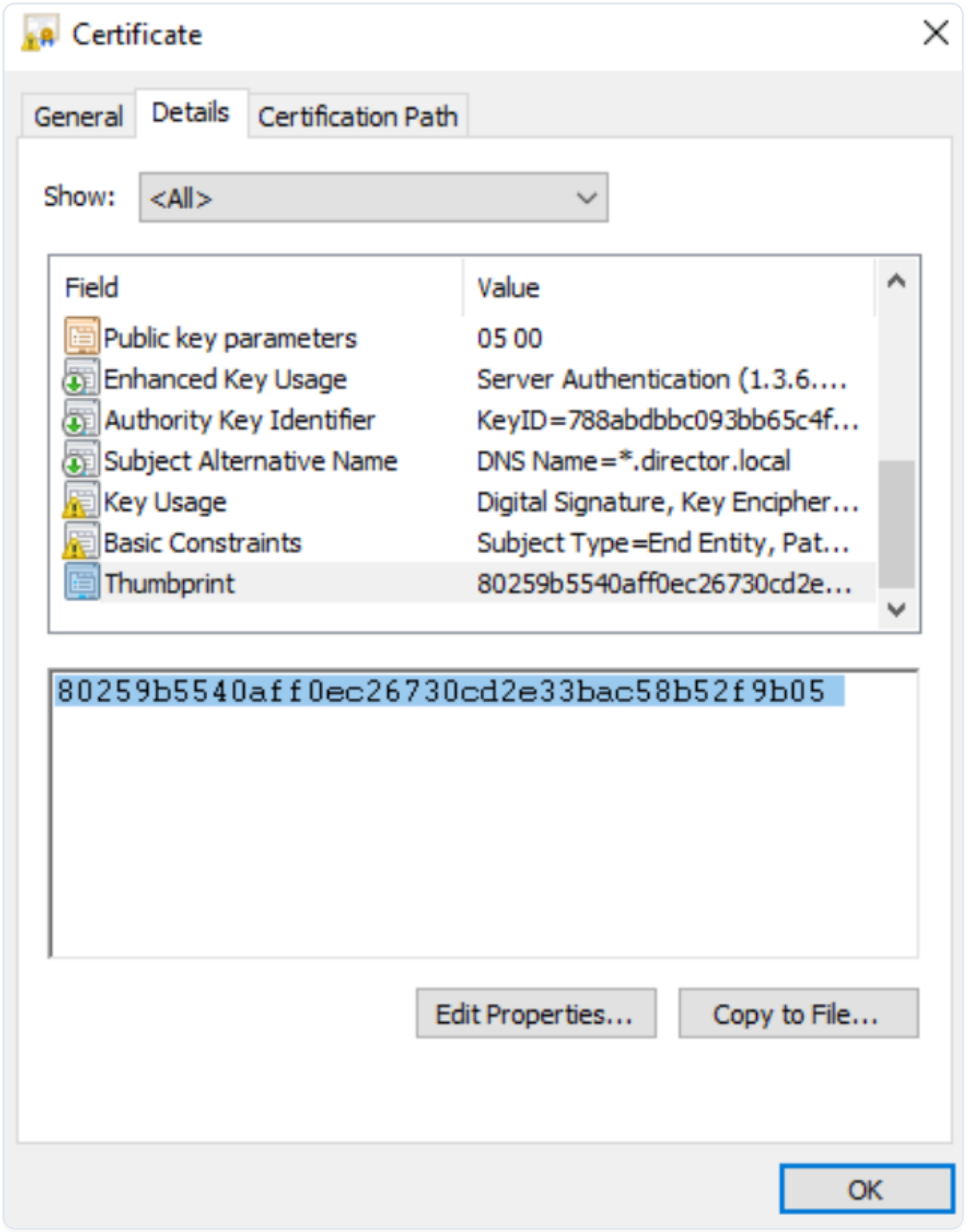
ステップ2.3：証明書への読み取りアクセスを提供する

1. インポートした証明書を右クリックし、**すべてのタスク** > **秘密キーの管理**を選択します。
2. 開いたダイアログで、**追加**を選択し、**Network Service**を検索します。 **OK**をクリックします。

3. **グループ**または**ユーザー名**の下にある**NETWORK SERVICE**を選択します。
4. **NETWORK SERVICEのアクセス許可**の下で*読み取り*アクセスを許可します。
5. **OK**をクリックします。

ステップ2.4: サムプリントの取得

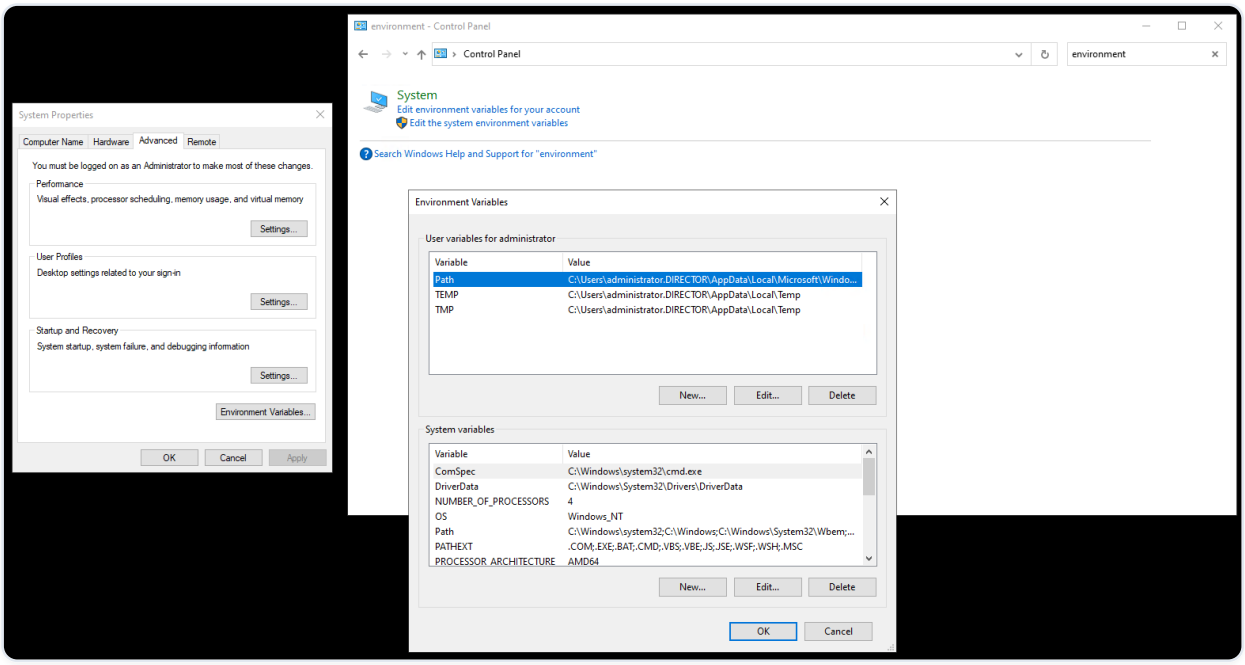
1. インポートされた証明書をダブルクリックします。
2. 開いたダイアログで、「**詳細**」タブに移動し、下までスクロールします。
3. 「**Thumbprint**」をクリックします。



4. 値をコピーし、次のステップのために準備しておきます。

ステップ2.5: 環境変数の設定

1. コントロールパネルを開きます。
2. 「環境」を検索し、「**システム環境変数の編集**」を選択します。
3. 「**システム変数 (すべてのユーザー)**」の下で、「**新規**」をクリックします。



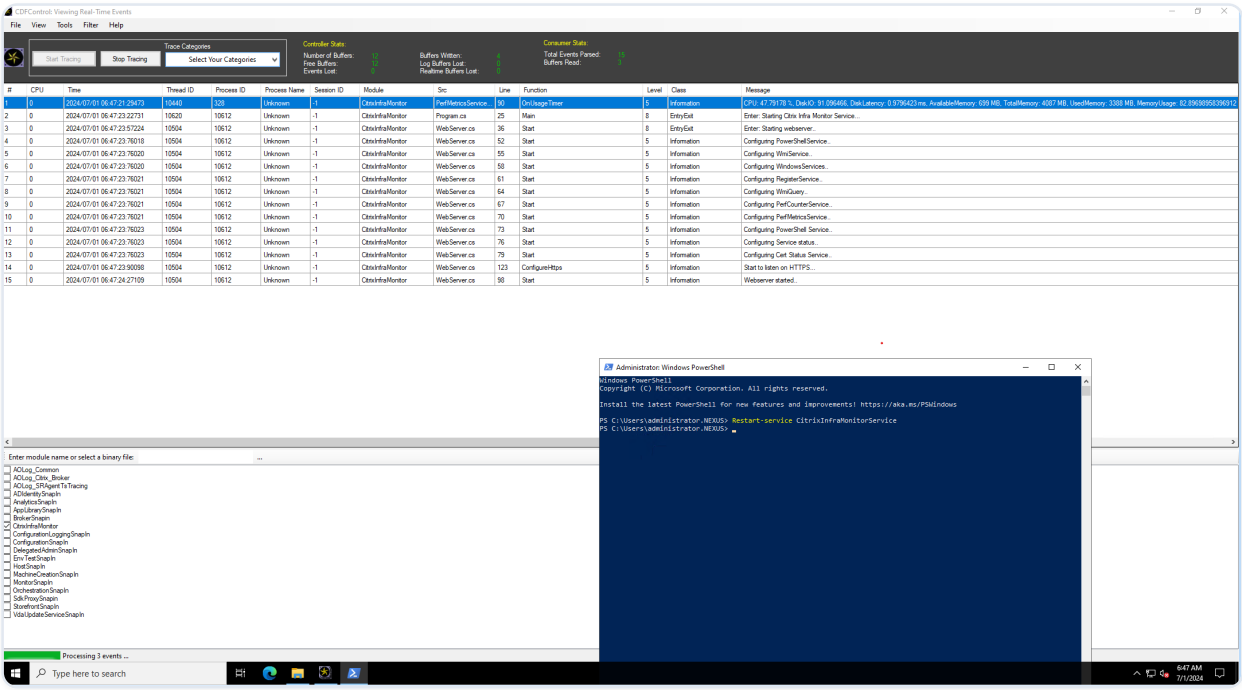
4. **変数**名を *DIRECTOR_AGENT_HTTPS_CERTIFICATE_THUMBPRINT* と指定します。
5. 前のステップで取得したサムプリントを**変数**値の下に指定します。
6. 「**OK**」をクリックします。

ステップ 2.6: CitrixInfraMonitorService を再起動する

1. PowerShell を開き、次のコマンドを実行します。

```
Restart-Service CitrixInfraMonitorService
```

2. **CitrixInfraMonitorService** モジュールをキャプチャし、ログ行 **Start to listen on HTTPS...** を探して、HTTPS が有効になっていることを確認します。



ステップ 2.7: モニター構成で HTTPS を有効にする

DDC マシンで次のコマンドを実行します。

```
Set-MonitorConfiguration -DirectorAgentEnableHttps $true
```

ステップ 3: Citrix Infrastructure Monitor を登録する

前提条件：

- Citrix Infrastructure Monitor が StoreFront または PVS マシンにインストールされていることを確認します。

PVS または StoreFront マシンと通信するために、DDC で Citrix Infrastructure Monitor を登録します。この登録は、PVS または StoreFront マシンで収集されたインフラストラクチャの健全性メトリックを DDC に送信するためのものです。

Citrix Infrastructure Monitor を登録するには、Delivery Controller™ で次の PowerShell コマンドを実行します。

```
Add-MonitorDirectorAgent -Fqdn <FQDN of component> -Component <component>
-Domain <domain> -Username <username> -Password <password> -Token <token>
```

注:

ユーザー名とパスワードはオプションのパラメーターです。ただし、これらのパラメーターを指定しない場合、一部のメトリックは利用できません。

前述のコマンドのパラメーターは次のとおりです。

パラメーター	説明
`Fqdn`	PVS または StoreFront サーバーの FQDN。
`Component`	オンボーディングするコンポーネント。例: PVS または SF。PVS は Citrix Provisioning を表し、SF は StoreFront を表します。
`Domain`	すべてのコンポーネントが属するドメイン。
`Username`	管理者ユーザーのユーザー名。
`Password`	管理者ユーザーのパスワード。
`Token`	Citrix Infrastructure Monitorがインストールされているシステムの `C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt` にある `RegistrationToken.txt` ファイルから、Citrix Infrastructure Monitorトークンを取得します。

注:

- Citrix Infrastructure Monitorサービスを再起動すると、`RegistrationToken.txt` ファイルに存在するトークンテキストが再生成されます。登録が成功すると、トークンファイルはマシンから削除されます。再登録する必要がある場合は、Citrix Infrastructure Monitorサービスを再起動してください。
- セキュリティ上の理由から、無効なトークンによる登録試行が3回失敗すると、トークンファイルは削除されます。

PVS または StoreFront マシンの登録が正常に完了すると、マシン名の詳細が **Director** > **インフラストラクチャ**タブに表示されます。

Citrix Infrastructure Monitorに登録するためのコマンド例は次のとおりです。

インフラモニターを再起動(/en-us/citrix-virtual-apps-desktops/2407/media/sm-sample-comand-im-register-on-prem.png)

コンポーネントの登録を解除する

特定のコンポーネントの登録を解除する必要がある場合は、Delivery Controller で次の PowerShell コマンドを実行します。

```
Remove-MonitorDirectorAgent -Fqdn <FQDN of component> -Component
<component>
```

Citrix Infrastructure Monitorの登録を解除するコマンドの例は次のとおりです。

インフラモニターを再起動(/en-us/citrix-virtual-apps-desktops/2407/media/sm-sample-comand-im-remove-on-prem.png)

注:

コンポーネントの登録を解除すると、特定のコンポーネントから Director へのデータフローが停止するだけです。Citrix Infrastructure Monitor をアンインストールする必要がある場合は、コントロールパネルからアンインストールしてください。

インフラストラクチャダッシュボード

「**インフラストラクチャ監視**」ページで、コンポーネントの健全性値を確認できます。これらの結果は、インフラストラクチャに関する問題を事前に分析し、トラブルシューティングするのに役立ちます。

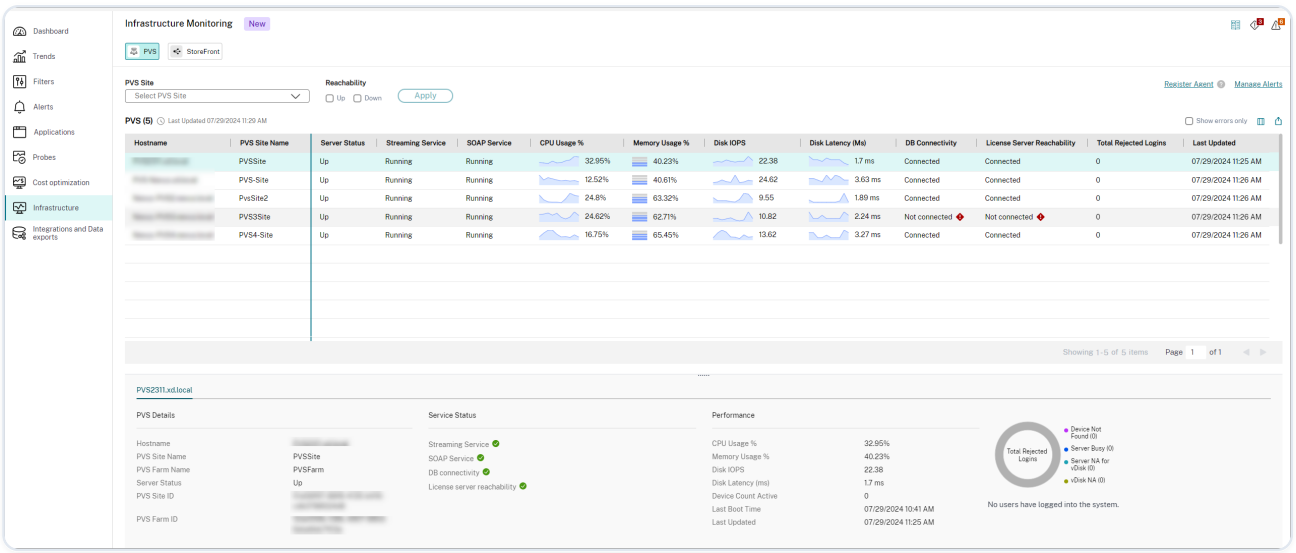
Infrastructure Monitoringページは、次の条件でフィルターできます。

- ホスト名 - ホスト名を選択します
- 到達可能性 - **Up**（サーバーに到達可能）または**Down**（サーバーに到達不能）チェックボックスを選択します
- エラー - エラーのある行のみ表示チェックボックスを選択します。

列の管理オプションを使用して、ダッシュボードに表示するデータを選択します。

PVS健全性メトリック

インフラストラクチャタブをクリックし、**PVS**を選択します。PVSのインフラストラクチャダッシュボードが表示されます。



PVSサーバーでは、以下の詳細が監視されます。

カテゴリ	メトリック	説明
到達可能性	ホスト名	Citrix Infrastructure Monitorがインストールされ ているPVSマシンの名前。このメトリックは文字列値です。
	PVSサイト名	PVSサイトの名前。このメトリックは文字列値です。
	PVSファーム名	PVSファームの名前。このメトリックは文字列値です。
	PVSサイトID	PVSサーバーのサイトIDを表示します。このメトリックは文字列値です。
	PVSファームID	PVSサーバーのファームIDを表示します。このメトリックは文字列値です。
	サーバーの状態	指定されたサーバーの到達可能性の状態を示します。可能

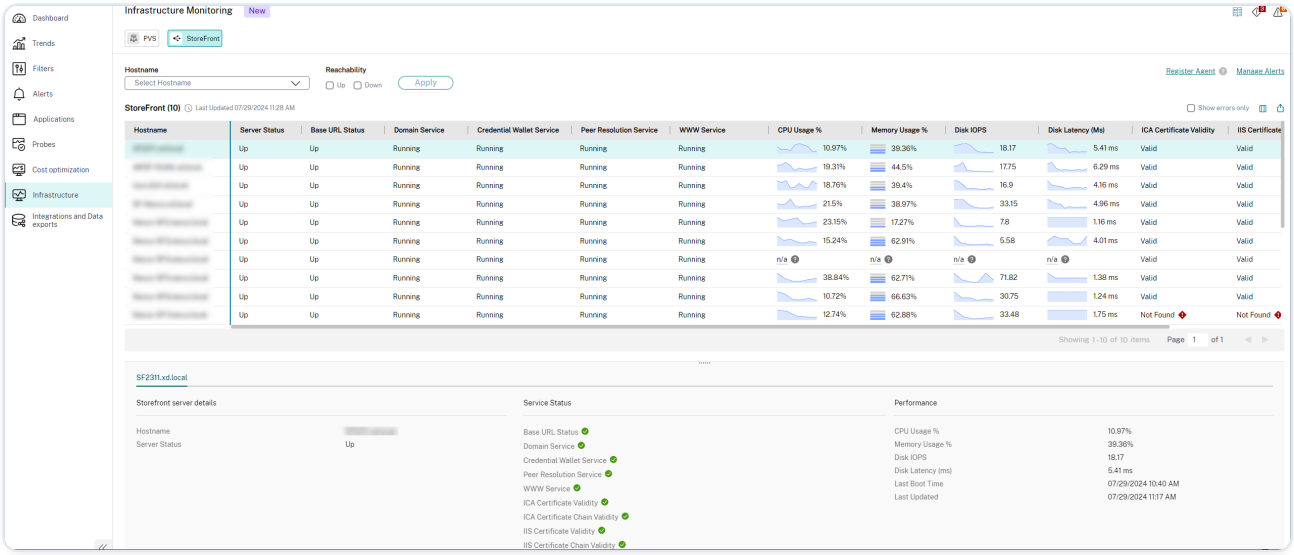
カテゴリ	メトリック	説明
		な値は、*Up*、*Down*、および*Unknown*です。
	最終起動時刻	PVSサーバーが最後に起動された時刻を表示します。
	最終更新	PVSサーバーからデータが収集された時刻を表示します。
依存サービス	ストリーミングサービス	ストリーミングサービスのステータスを表示します。このメトリックは、Windowsサービスのステータスを示します。可能な値は、*実行していません*、*実行中*、*インストールされていません*、および*n/a*（ヘルプアイコン付き）です。
	SOAPサービス	Simple Object Access Protocol (SOAP) サービスのステータスを表示します。このメトリックは、Windows サービスのステータスを示します。可能な値は、*実行していません*、*実行中*、*インストールされていません*、および*n/a* (ヘルプアイコン付き) です。
	DB接続	データベース接続のステータスを表示します。Citrix Provisioningサーバーバージョン2402以前を使用している場合、不明なエラーが発生する可能性があります。可能な値は、*未接続*、*接続済み*、*不明*、および*n/a*（ヘルプアイコン付き）です。

カテゴリ	メトリック	説明
	ライセンスサーバーの到達可能性	ライセンスサーバーに到達可能かどうかを表示します。Citrix Provisioningサーバーバージョン2402以前を使用している場合、不明なエラーが発生する可能性があります。可能な値は、*未接続*、*接続済み*、*不明*、および*n/a*（ヘルプアイコン付き）です。
リソース使用率	CPU使用率 %	CPUの使用率を折れ線グラフでパーセンテージ表示します。表示される値は、過去5分間の終わり時点での最新の値です。
	平均CPU %	過去10分間に集計されたPVSサーバーの平均CPU使用率をパーセンテージで表示します。
	ピークCPU %	過去5分間のPVSサーバーのピークCPU使用率をパーセンテージで表示します。
	メモリ使用率 %	メモリの使用率を積み上げグラフでパーセンテージ表示します。表示される値は、過去5分間の終わり時点での最新の値です。
	平均メモリ %	過去10分間に集計されたPVSサーバーの平均メモリ使用率をパーセンテージで表示します。
	ピークメモリ使用率	過去5分間のPVSサーバーのピークメモリ使用率を表示します。

カテゴリ	メトリック	説明
	ディスクIOPS	折れ線グラフを使用してディスクの入出力値を表示します。
	平均ディスクIOPS使用率	過去10分間に集計されたPVSサーバーの平均ディスクIOPSを表示します。
	ピークディスクIOPS使用率	過去10分間のPVSサーバーのピークディスクIOPS使用率を表示します。
	ディスク遅延 (ミリ秒)	折れ線グラフを使用してディスクの遅延値を表示します。
	平均ディスク待機時間 %	過去10分間に集計されたPVSサーバーの平均ディスク待機時間を表示します。
	ピークディスク待機時間 %	過去5分間のPVSサーバーのピークディスク待機時間の割合を表示します。
影響	拒否されたログインの合計	ログイン試行の合計数で割った、失敗したログインの合計数。
	アクティブなデバイス数	PVSサーバー内のアクティブなデバイスの総数を表示します。このメトリックは整数値です。

StoreFront 健全性メトリック

「**インフラストラクチャ**」タブをクリックし、「**StoreFront**」を選択します。StoreFrontのインフラストラクチャダッシュボードが表示されます。



StoreFrontサーバーについて、以下の詳細が監視されます。

カテゴリ	メトリック	説明
到達可能性	ホスト名	StoreFrontサーバーの名前を表示します。このメトリックは文字列値です。
	サーバーの状態	StoreFrontサーバーの状態を表示します。このメトリックはWindowsサービスのステータスを示します。可能な値は、*実行中ではない*、*実行中*、*インストールされていない*、および*n/a* (ヘルプアイコン付き) です。
	ベースURLの状態	ベースURLの健全性を表示します。HTTPステータスコードが200の場合、ステータスはUPです。それ以外の場合、値はDownです。
	最終起動時刻	StoreFrontサーバーが最後に起動された時刻を表示します。
	最終更新日時	StoreFrontサーバーからデータが収集された時刻を表示します。

カテゴリ	メトリック	説明
依存サービス	ドメインサービス	ドメインサービスという名前のWindowsサービスの正常性。このメトリックはWindowsサービスのステータスを示します。可能な値は、*実行されていません*、*実行中*、*インストールされていません*、および*該当なし*（ヘルプアイコン付き）です。
	資格情報ウォレットサービス	このサービスは、暗号化されたパスワードを保存するために使用されるWindowsサービスです。可能な値は、*実行されていません*、*実行中*、*インストールされていません*、および*該当なし*（ヘルプアイコン付き）です。
	ピア解決サービス	このサービスは、StoreFrontサーバーのピアメッシュを形成するサーバー間グループネットワーク通信を担当するWindowsサービスです。可能な値は、*実行されていません*、*実行中*、*インストールされていません*、および*該当なし*（ヘルプアイコン付き）です。
	WWWサービス	このメトリックはStoreFrontサーバーのWebサービスです。このメトリックはWindowsサービスのステータスを示します。指定できる値は、*実行していません*、*実行中*、*インストールされていません*、および *n/a* (ヘルプアイコン付き) です。

カテゴリ	メトリック	説明
リソース使用率	CPU使用率 %	CPUの使用率を折れ線グラフで表示します。表示される値は、過去5分間の終わりにおける最新のものです。
	平均CPU使用率 %	StoreFrontサーバーの平均CPU使用率を、過去10分間にわたって集計して表示します。
	ピークCPU使用率 %	過去5分間のStoreFrontサーバーのピークCPU使用率を表示します。この値は、CPUに必要な最大容量を決定するのに役立ちます。
	メモリ使用率 %	メモリの使用率を積み上げグラフで表示します。表示される値は、過去5分間の終わりにおける最新のものです。
	平均メモリ使用率 %	過去10分間に集計されたStoreFrontサーバーの平均メモリ使用率を表示します。
	ピークメモリ使用率	過去5分間のStoreFrontサーバーのピークメモリ使用率を表示します。
	ディスクIOPS	折れ線グラフを使用してディスクの入出力値を表示します。
	平均ディスクIOPS %	浮動小数点数を使用してStoreFrontサーバーの平均ディスクIOPSを表示します。
	ピークディスクIOPS %	過去10分間に集計されたStoreFrontサーバーのピークディスクIOPS使用率を表示します。

カテゴリ	メトリック	説明
	ディスク待機時間 (ミリ秒)	ディスクの遅延値を折れ線グラフで表示します。
	平均ディスク遅延 %	過去10分間のStoreFrontサーバーの平均ディスク遅延を集計して表示します。
	ピークディスク遅延 %	過去5分間のStoreFrontサーバーのピークディスク遅延率を表示します。
影響	ICA®証明書の有効性	ICA証明書の有効性を表示します。可能な値は、*期限切れ*、*期限切れ間近*、*有効*、*見つかりません*です。
	ICA証明書チェーンの有効性	StoreFront ICA証明書チェーンが有効かどうかを表示します。可能な値は、*はい*または*いいえ*です。
	IIS証明書の有効性	IIS証明書の有効性を表示します。可能な値は、*期限切れ*、*期限切れ間近*、*有効*、*見つかりません*です。
	IIS証明書チェーンの有効性	StoreFront IIS証明書チェーンが有効かどうかを表示します。可能な値は、*はい*または*いいえ*です。

アラートの作成と管理

関心のある条件や範囲をプロアクティブに監視し、アラート疲れを軽減するためにアラートを設定できます。アラートは、重要度、再アラート間隔、通知媒体で構成でき、製品でサポートされているアラートライフサイクルに従います。

詳細については、アラートページを参照してください。

統合とデータのエクスポート

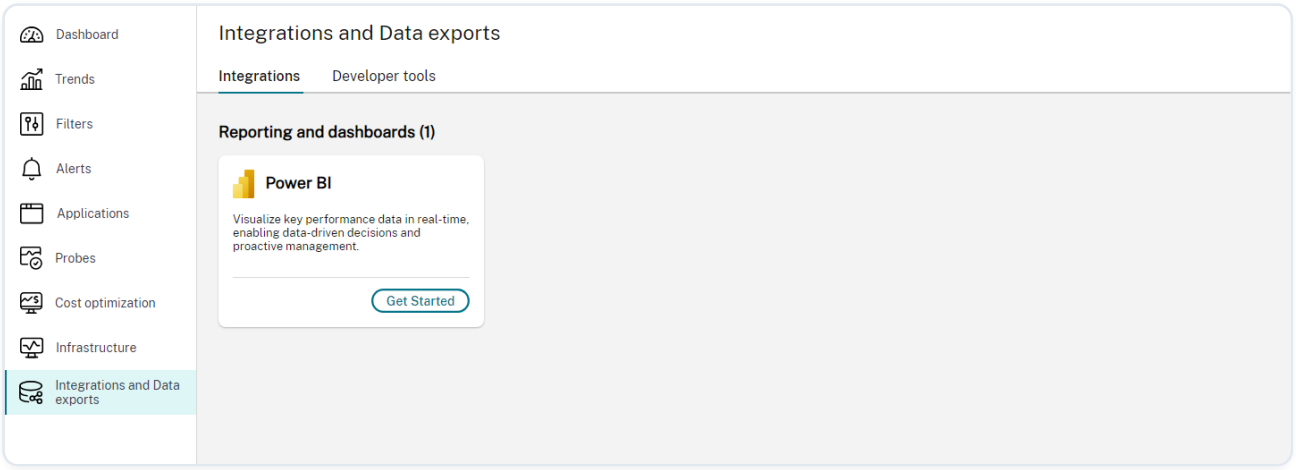
Citrix Director に、統合とデータのエクスポート用の新しい UI が追加されました。この機能は、Citrix Director で利用可能なさまざまなインターフェイスとサードパーティ統合の認識を高めるのに役立ちます。新しく導入された ページには、次のものが表示されます。

- 利用可能な統合
- サポートされている開発者ツール

このページでは、データのエクスポート用に設定された REST API についても説明しています。また、統合と開発者ツールの使用を開始するためのガイドとドキュメントへの参照リンクも提供しています。

現在、Citrix Director は Power BI の可観測性と統合されています。この機能を使用して、REST API を介して Citrix Director から Power BI にパフォーマンスデータとイベントをエクスポートできます。

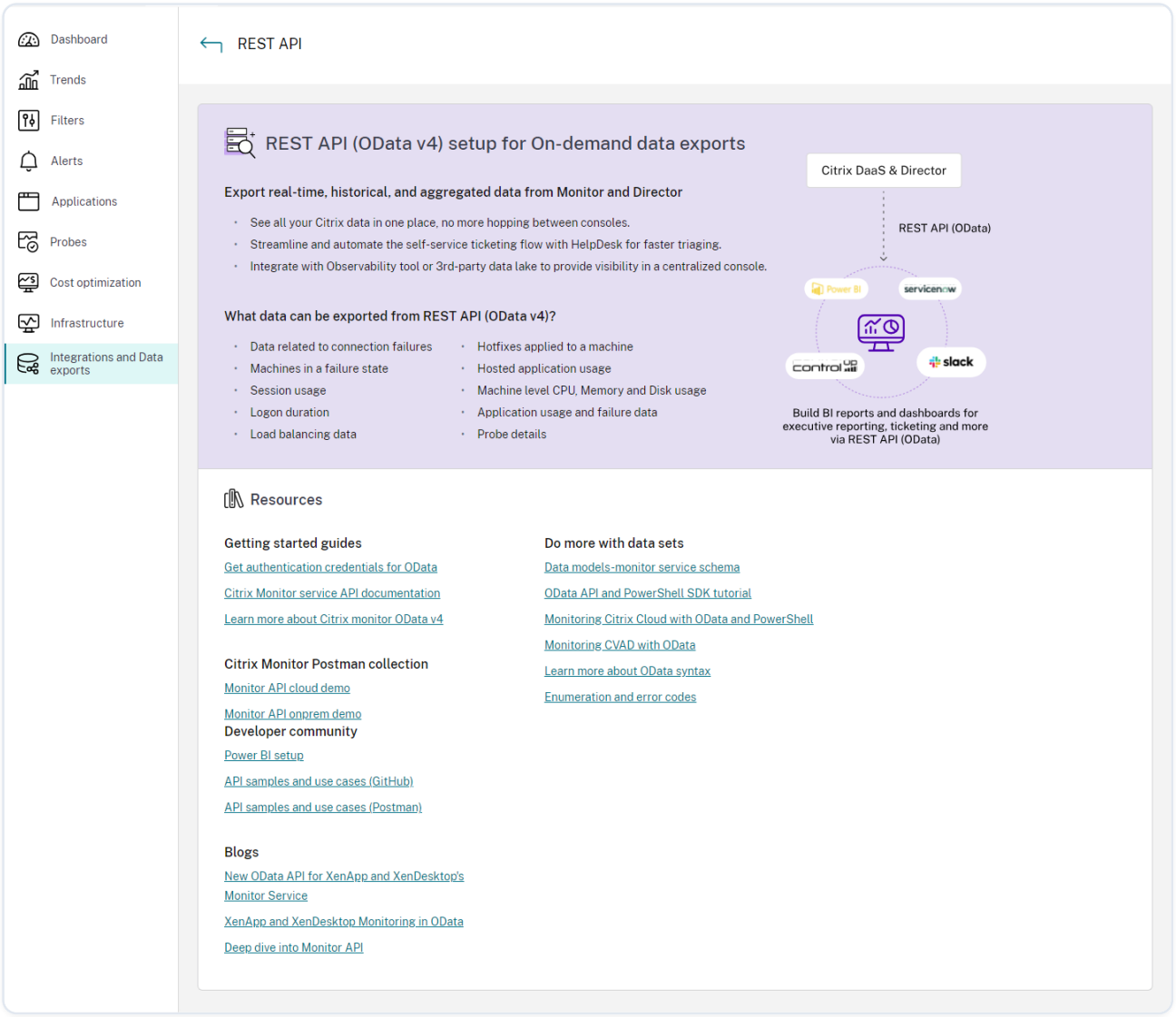
左側のナビゲーションメニューから をクリックします。 ページが表示されます。



利用可能な統合を表示

タブには、Citrix Director で利用可能な統合が表示されます。現在、Citrix Director は Power BI の可観測性と統合されています。

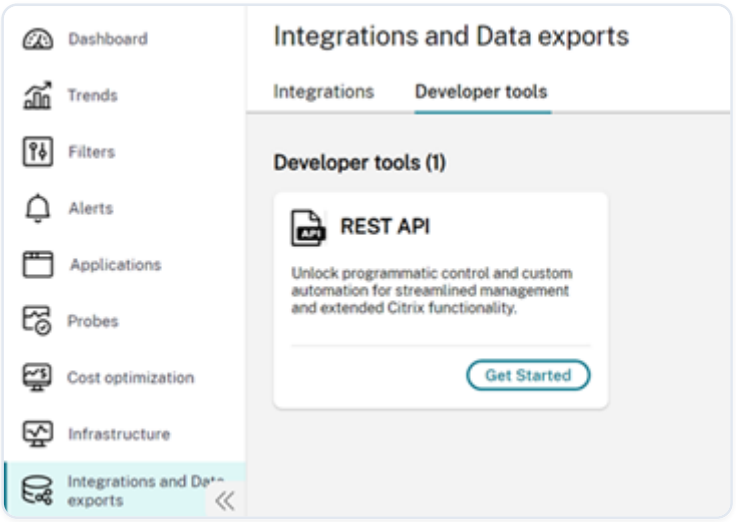
をクリックします。 開発者ツールの詳細ページが表示されます。



このページには、リソースやブログへの参照リンクが記載されています。

サポートされている開発者ツールを表示する

1. 利用可能な開発者ツールを表示するには、 をクリックします。



2. 「**開始**」をクリックします。**REST API**開発者ツールの詳細ページが開きます。リソースやブログへの参照リンクにアクセスできます。

アプリケーションおよびデスクトップのプロービング

アプリケーションおよびデスクトップのプロービングは、StoreFront を使用してサイトに公開されているアプリとデスクトップを連続してテスト起動することで、それらの正常性を確認するプロセスを自動化します。プロービングの結果は Director で確認できます。

要件

- アプリケーションプロービングの場合は Delivery Controller バージョン 7.18 以降、デスクトッププロービングの場合はバージョン 1906 以降が実行されていること。
- プローブエージェントを実行するエンドポイントマシンは、アプリケーションプロービングの場合は Windows 版 Citrix Workspace™ アプリバージョン 1808 以降、デスクトッププロービングの場合はバージョン 1906 以降がインストールされた Windows マシンであること。Unified Windows Platform (UWP) 用 Workspace アプリはサポートされていません。
- Citrix Probe Agent は、Active Directory 資格情報を使用した StoreFront および Citrix Workspace 経由の認証をサポートしています。エンドポイントデバイスが Citrix Gateway 経由で StoreFront / Workspace に接続されている場合、Citrix Gateway ドメイン資格情報または多要素認証 (MFA) を使用して認証できます。Citrix Probe Agent は、シングルサインオン (SSO) などの他の認証方法をサポートしていません。

  > **注:**
  >
  > - ユーザーがCitrix Cloud™でサインインポリシーまたは条件付き認証を有効にしている場合、プローブエージェントはStoreFrontまたはCitrix Workspaceアプリにサインインできません。
  > - Probe Agent は、Citrix Workspace アプリへの認証に Active Directory 認証のみをサポートしています。

- Probe Agent をインストールするエンドポイントマシンに、Microsoft .NET Framework バージョン 4.7.2 以降がインストールされていることを確認してください。

プロービングの実行に必要なユーザーアカウント/権限：

- 各エンドポイントマシンでプローブを実行するための固有の StoreFront ユーザー。StoreFront ユーザーは管理者である必要はなく、プローブは非管理者コンテキストで実行できます。
- エンドポイントマシンに Citrix Probe Agent をインストールおよび構成するための Windows 管理者権限を持つユーザーアカウント
- プロービングのために既存のユーザーアカウントを再利用すると、ユーザーのアクティブなセッションからログオフされる可能性があります。以下の権限を持つ完全な管理者ユーザーアカウントまたはカスタムロール：
    - デリバリーグループの権限：
        - 読み取り専用
    - Directorの権限:
        - アラートメールサーバー構成の作成\\編集\\削除 - メールサーバーがまだ構成されていない場合
        - プローブ構成の作成\\編集\\削除
        - 構成の表示ページ
        - トレンドの表示ページ

構成

複数の地域で、ピーク時間外にプローブを実行するようにスケジュールできます。包括的なプローブ結果は、ユーザーが問題に遭遇する前に、アプリケーション、ホストマシン、または接続に関連する問題をトラブルシューティングするのに役立ちます。

Citrix Probe Agentバージョン2103以降は、サイト集約をサポートしています。Citrix Probe Agentを構成する際、集約されたサイトからのアプリケーションとデスクトップの列挙を有効にするには、Workspace (StoreFront) Site Aggregation Enabledオプションを選択します。以下のサイトの組み合わせがサポートされています:

- 1つのStoreFront URLを持つ複数のオンプレミスサイト。
- StoreFrontまたはWorkspaceのいずれかのURLを持つオンプレミスサイトとクラウドサイト。
- 1つのWorkspace URLを持つ複数のクラウドサイト。
- Citrix Gateway経由でStoreFrontまたはWorkspaceに接続されているオンプレミスサイト。

> **注:**

> 1つのサイトにのみアクセスできるプローブを構成するには、個別の管理者またはユーザーを作成する必要があります。

ステップ1：Citrix Probe Agentをインストールして構成する

Citrix Probe Agent は、ユーザーが StoreFront を介して実際のアプリケーションまたはデスクトップを起動するのをシミュレートする Windows 実行可能ファイルです。Director で構成された起動をテストし、その結果を Director に報告します。

1. プロービングを実行するエンドポイントマシンを特定します。
2. 管理者権限を持つユーザーは、エンドポイントマシンに Citrix Probe Agent をインストールして構成できます。`<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html>` で入手可能な Citrix Probe Agent 実行可能ファイルをダウンロードしてください。ダウンロードリンクは、Director の **Probes** タブでも入手できます。

   プローブ構成(/en-us/citrix-virtual-apps-desktops/2407/media/dir-probe-configuration.png)。
3. 集約されたサイトがある場合は、集約されたサイトからのアプリケーションとデスクトップの列挙を有効にするために、Workspace (StoreFront) Site Aggregation Enabled オプションを選択します。
4. 認証方法を選択し、関連する資格情報を入力します。資格情報は暗号化され、安全に保存されます。
5. StoreFront Active Directory 資格情報で構成します。各エンドポイントマシンで一意の Workspace (StoreFront) ユーザーを構成します。 プローブエージェント(/en-us/citrix-virtual-apps-desktops/2407/media/dir-config-storefront-cred.png)
6. エンドポイントが Citrix Gateway 経由で StoreFront に接続されている場合は、Citrix Gateway オプションを選択し、Citrix Gateway ドメイン資格情報で構成します。

   プローブエージェント(/en-us/citrix-virtual-apps-desktops/2407/media/dir-config-workspace-cred.png)
7. ゲートウェイがサポートしている場合は、多要素認証オプションを選択し、16桁の認証キーを入力します。これは、Single Login Schema を使用して LDAP および Native OTP で構成された Citrix Gateway でのみ利用可能です。
8. タブで、Director の資格情報を入力し、 をクリックします。

   プローブエージェント(/en-us/citrix-virtual-apps-desktops/2407/media/dir-probe-agent.png)
9. サイトを選択し、**次へ**をクリックします。

10. 「**概要の表示**」タブで、構成された詳細が正確であることを確認します。変更が必要な場合は、該当するタブに移動して更新します。

> **注:**
>
> Automating Citrix Probe Agent Installation and Configuration に含まれる PowerShell スクリプトを使用して、Citrix Probe Agent のインストールと構成を自動化できます。

ステップ 2: Director でプローブを構成する

> **制限事項:**
>
> 対話型ログオンメッセージバナーが有効になっている Windows VDA からアプリケーションまたはデスクトップがテスト起動されると、プローブは失敗します。これは、対話型ログオンメッセージの承認を待機している間にタイムアウトが発生するためです。 サーバー VDA でログオンメッセージを無効にするには、 > > > > に移動します。
>
> 以下のフィールドのテキストを削除し、Microsoft ポリシーを更新します。
>
> - 対話型ログオン: ログオンしようとするユーザーのメッセージテキスト
> - 対話型ログオン: ログオンしようとするユーザーのメッセージタイトル
>
> プローブがアプリケーションまたはデスクトップの起動状態を通過できるように、対話型ログオンメッセージバナーが無効になっているこの特定のサーバー VDA にプローブユーザーを割り当てます。
>
> 詳細については、`<https://learn.microsoft.com/ja-jp/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>` を参照してください。

1. **プローブ** \> **アプリケーションプローブ** または **デスクトッププローブ** に移動し、**プローブの作成** をクリックします。
2. **プローブの作成** ページで、プローブの名前を入力します。

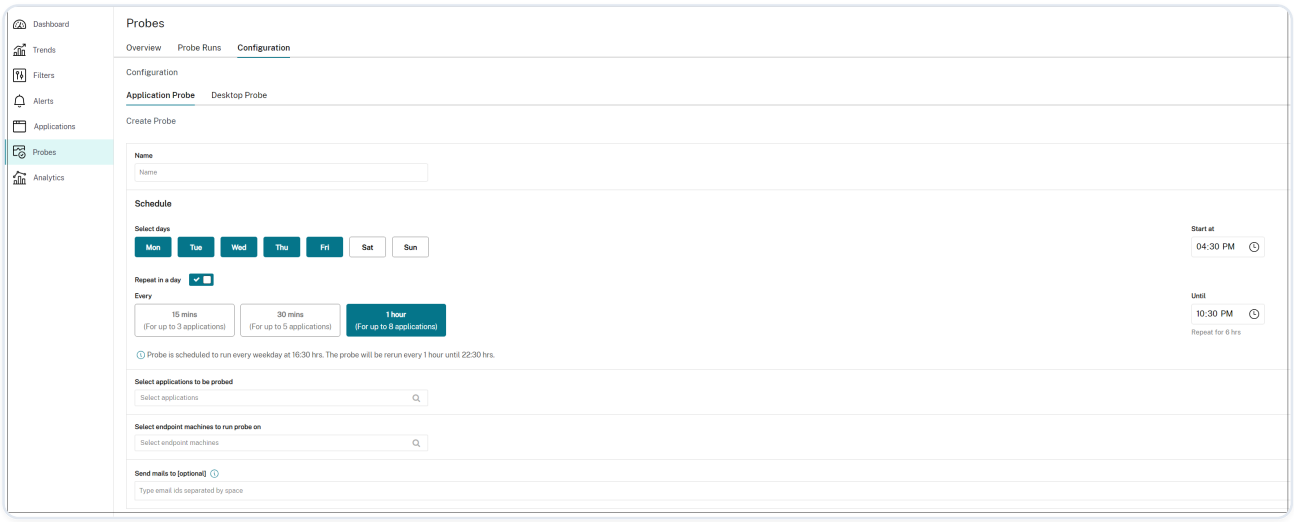
3. スケジュールを選択します:

    a. プローブを実行する曜日を選択します。

    b. プローブを実行する開始時刻を入力します。

    c. さらに、「**Repeat in a day**」オプションを選択できます。プローブを1日の中で繰り返す終了時刻と間隔を入力します。たとえば、以下の構成では、毎週月曜日、水曜日、木曜日、日曜日に、12時08分から16時34分まで30分ごとにアプリケーションプローブを実行します。

4. 間隔に応じて、プローブするアプリケーションまたはデスクトップの推奨数を選択します。
5. プローブを実行する必要があるエンドポイントマシンを選択します。
6. 失敗したプローブの結果を送信する管理者のメールアドレスを入力します。メールサーバーは、**アラート** > **メールサーバーの構成**で構成します。



この構成では、アプリケーションセッションは毎週月曜日、水曜日、木曜日、日曜日に、12時08分、12時38分、13時08分といった具合に、16時08分まで起動します。

注:

- 構成後、エージェントは次の時間から構成されたプローブを実行します。
- **Repeat in a day**オプションが導入される前に設定されたプローブは、引き続きスケジュールされた時間に実行されます。これらのプローブでは、**Repeat in a day**オプションはデフォルトで無効になっています。
- 重複を防ぐため、各実行に5分の期間があるようにプローブを構成することをお勧めします。

ステップ3：プローブの実行

エージェントは、Directorから定期的に取得するプローブ構成に従ってプロービングを実行します。

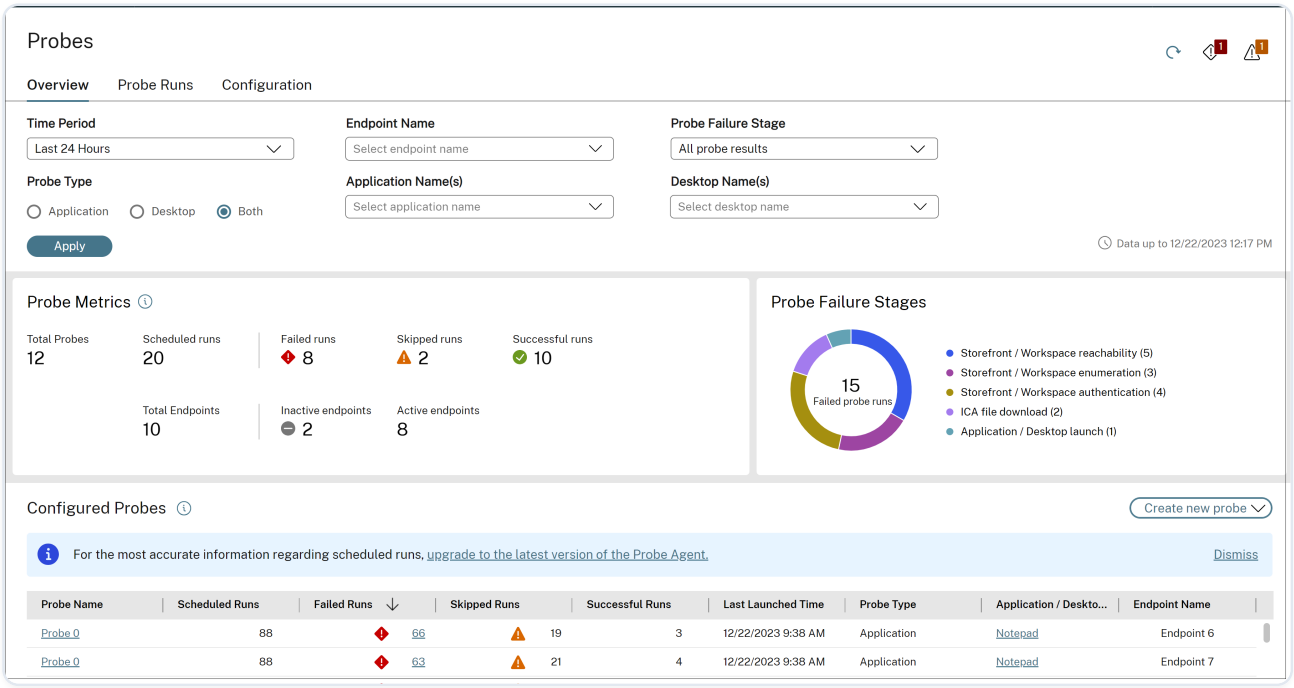
StoreFrontを使用して、選択されたアプリケーションを順次起動します。エージェントは、Monitorデータベースを介してDirectorに結果を報告します。障害は、次の5つの特定の段階で報告されます。

- **StoreFront Reachability** - 構成されたStoreFront URLに到達できません。
- **StoreFront Authentication** - 構成されたStoreFront資格情報が無効です。
- **StoreFront Enumeration** - StoreFront列挙アプリケーションリストに、プローブ対象のアプリケーションまたはデスクトップが含まれていません。
- **ICA® download** - ICAファイルが利用できません。
- **Application / Desktop launch** – アプリケーションまたはデスクトップを起動できませんでした。

ステップ4：プローブ結果の表示

プローブでプローブ結果を確認できます。プローブビューでは、プローブ結果の包括的な概要がわかります。これらの結果は、問題を事前に分析してトラブルシューティングするのに役立ち、ユーザーのセッション起動エクスペリエンスをよりスムーズにします。

概要タブには、構成されているすべてのプローブの概要が1つのビューに表示されます。



時間期間、プローブの種類、エンドポイント名、アプリケーション名、デスクトップ名、およびプローブ結果の種類に基づいてプローブをフィルタリングできます。フィルタ条件に一致するプローブは、プローブ、アプリケーション/デスクトップ、およびエンドポイントごとに次の詳細とともに表示されます。

プローブメトリックには、スケジュール済み、計画済み、スキップ済み、成功、および失敗した実行の数が表示されます。

- 完了した実行 – 完了まで実行されたプローブ実行の数。
- 失敗した実行 – 失敗したプローブ実行の数。
- スキップされた実行 – エンドポイントが非アクティブであるか、サービスが利用できないために完了しなかった実行の数。
- 成功した実行 – アプリ/デスクトップの起動中に、どの段階でも失敗することなく正常に完了したプローブの数。

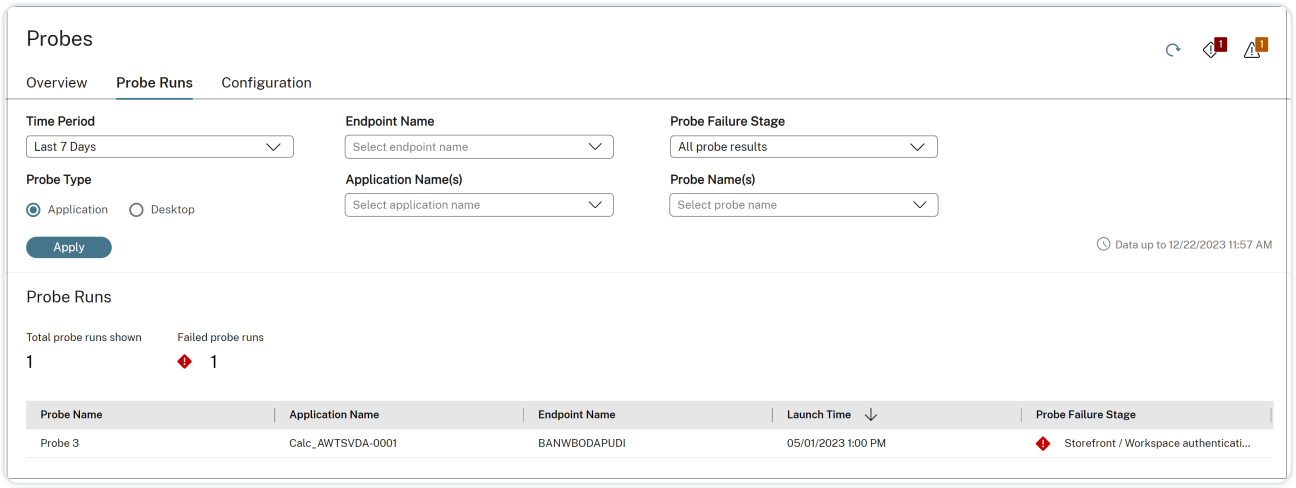
エンドポイントマシンの総数も、アクティブなマシンと非アクティブなマシンの数とともに表示されます。

プローブ失敗ステージには、各失敗グループの失敗分布が視覚的に分類されて表示されます。ほとんどの失敗が発生したステージを分析することで、プローブ結果を解釈し、問題をトラブルシューティングすることが容易になります。グラフィカル表示では、アプリケーション/デスクトップの起動、ICAファイルのダウンロード、StoreFront/Workspaceの列挙、StoreFront/Workspaceの到達可能性、およびStoreFront/Workspaceの認証における失敗したプローブ実行の数が示されます。

ほとんどの失敗が発生したステージを分析するのに役立ちます。この情報は、プローブ結果を迅速に理解し、トラブルシューティングを行うのに役立ちます。

エンドポイントが非アクティブであるか、サービスが利用できないために、一部のプローブ実行が完了しない場合があります。

プローブ実行タブには、完了したプローブ実行の結果が詳細に表示されます。選択したプローブの個々の実行の詳細を表示するためにドリルダウンできます。重要なピボットポイントに基づいて、さらにフィルタリングおよび分析できます。



時間期間、プローブタイプ、エンドポイント名、アプリケーション名、デスクトップ名、およびプローブ障害ステージに基づいてプローブ実行をフィルタリングできます。プローブ障害ステージは、プローブが失敗した段階を表示します。プローブ名、スケジュールされた実行、失敗した実行、アプリケーション/デスクトップ名のリンクをクリックすると、フィルター条件に一致するプローブ実行のリストが表示されたプローブ実行ページに移動します。

アプリケーション使用状況の監視

Citrix Directorは、公開されているアプリケーションの使用状況を監視するのに役立ちます。この機能はダッシュボードにあり、厳選されたグラフが含まれています。これらのグラフは、IT管理者またはアプリケーション管理者が、どのアプリケーションが頻繁に使用されているか、およびその使用範囲を把握するのに役立ちます。

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

> この機能を使用すると、管理者はどの公開アプリケーションが最も使用されているかを確認できます。このデータを使用して、管理者は使用状況の範囲をさらに深く掘り下げることができます。管理者は、過去24時間の人気アプリの詳細を次のデータポイントで分析できます。

- アプリケーションの総数 - 企業のサイト内のすべてのユーザーが使用しているアプリケーションの総数を識別します。
- 個別のユーザー総数による最も使用されているアプリケーション - ユニークユーザーの総数による上位10のアプリを識別します。

- アプリケーション起動総数による最も使用されているアプリケーション - アプリケーション起動総数に基づいた上位10のアプリを識別します。
- 同時実行アプリインスタンスのピーク数上位 - 各アプリケーションの使用状況の同時インスタンスの最大数に基づいた上位10のアプリを識別します。この情報は、リストされているアプリケーションの最大需要を示します。

このグラフはダッシュボードページの下部に表示されます。ただし、画面上部の**Check it out**をクリックすると、グラフに直接アクセスできます。

アプリケーション監視(/en-us/citrix-virtual-apps-desktops/2407/media/application-monitoring.png)

View all app usageをクリックして、単一のアプリの詳細を表示することもできます。このリンクをクリックすると、**Trends** > **Capacity Management** > **Hosted Application Usage**ページが開きます。

このグラフは、アプリの使用状況を視覚的に表現します。また、グラフにカーソルを合わせると、選択したデータポイントの絶対数が表示されます。グラフ上の任意のデータポイントをクリックすると、特定のアプリ名が選択された状態で**Trends** > **Capacity Management** > **Hosted Application Usage**ページが開きます。このデータは、企業のシステムに存在するすべてのアプリに対する比較値を示すものです。データポイントの絶対値も、同じホバーで個別に表示されます。

セキュアプライベートアクセスとDirectorの統合 (プレビュー)

セキュアプライベートアクセスとDirectorの統合により、ヘルプデスク管理者またはフル管理者は、Director内のすべてのセキュアプライベートアクセスセッションを監視およびトラブルシューティングできます。この機能をサポートするには、Director、セキュアプライベートアクセス、Citrix Workspace™ app、およびVDAのバージョン2402以降を使用する必要があります。

利用可能なアクションには、以下の詳細の表示が含まれます。

- **Select a Session**ポップアップ > **Sessions**タブ > **Web SaaS and Client/Server Apps**の下にある、ユーザーのセキュアプライベートアクセスアクティブセッション
- **Select a Session**ポップアップ > **Denied Access**タブの下にある、セキュアプライベートアクセスの失敗またはブロックされた列挙、および失敗したアプリ起動
- アクティブおよび失敗したアプリ起動のセッションおよびアプリケーションの詳細表示
- 失敗およびブロックされた列挙のセッションおよびアプリケーションの詳細表示

> **注:**

> セキュアプライベートアクセスとDirectorの統合は、Directorのフォームベース認証のみをサポートしており、統合Windows認証またはスマートカードベース認証はサポートしていません。

前提条件

1. この機能をサポートするには、以下を使用する必要があります。
   - Director 2402以降のバージョン
   - セキュアプライベートアクセス 2402以降のバージョン
   - Citrix Workspace app 2402以降のバージョン
2. DirectorでCitrix Virtual Apps and Desktops™サイトが少なくとも1つ構成されていることを確認してください。
3. 「Secure Private Access を設定する」(/ja-jp/citrix-secure-private-access/current-release/spa-onprem-setup-spa.html)。
4. DirectorサーバーがSecure Private Accessサーバーへのネットワーク接続を持っていることを確認してください。

   > **注:**
   >
   > Citrix Director への接続を正常に確立するには、Secure Private Access サーバーに信頼された証明書がインストールされている必要があります。

5. Director管理者ユーザーが次の権限を持っていることを確認してください。
   a. Secure Private Access管理コンソールにおけるSecure Private Accessのフル管理者または読み取り専用管理者。
   b. Citrix StudioコンソールにおけるCitrix Virtual Apps™またはDesktopsのヘルプデスク、フル管理者、または読み取り専用管理者。

DirectorをSecure Private Accessと連携して構成する

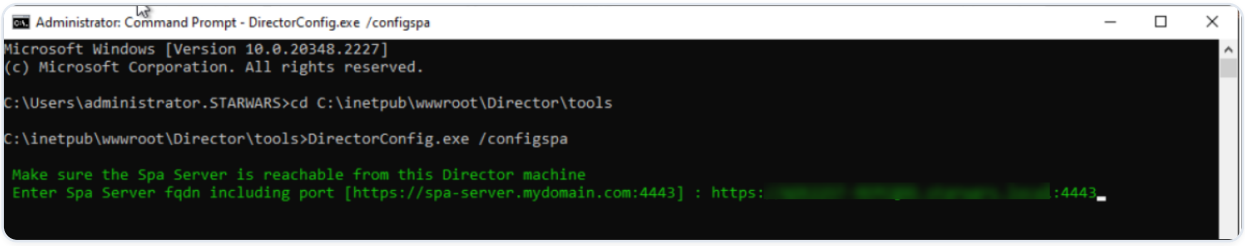
1. Directorがインストールされているマシンで、管理者としてコマンドプロンプトを開きます。
2. 次のコマンドを実行して、`DirectorConfig` ツールのパスに移動します。

```
cd c:\inetpub\wwwroot\Director\tools
```

3. Secure Private Accessを構成するために、次のコマンドを実行します。

```
DirectorConfig.exe /configspa
```

4. Secure Private Access がインストールされているマシンの FQDN とポート番号を入力します。
5. Secure Private Access（サーバーまたはロードバランサー）への接続が安全であり、信頼された証明書が適用されていることを確認してください。



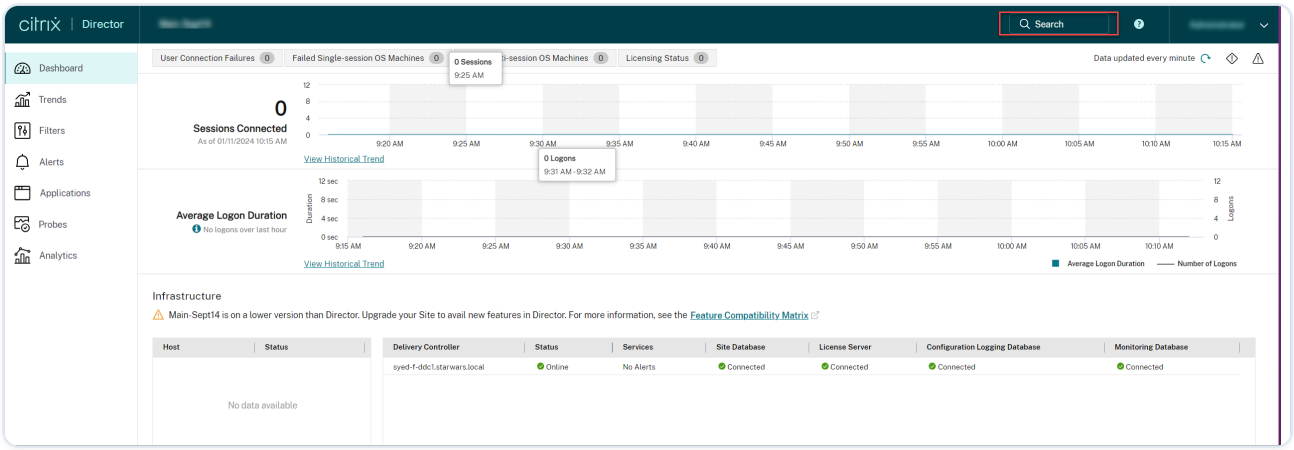
注:

Director で Secure Private Access セッションの詳細を表示するには、管理者を Secure Private Access コンソールに追加する必要があります。詳細については、「管理者の管理」を参照してください。

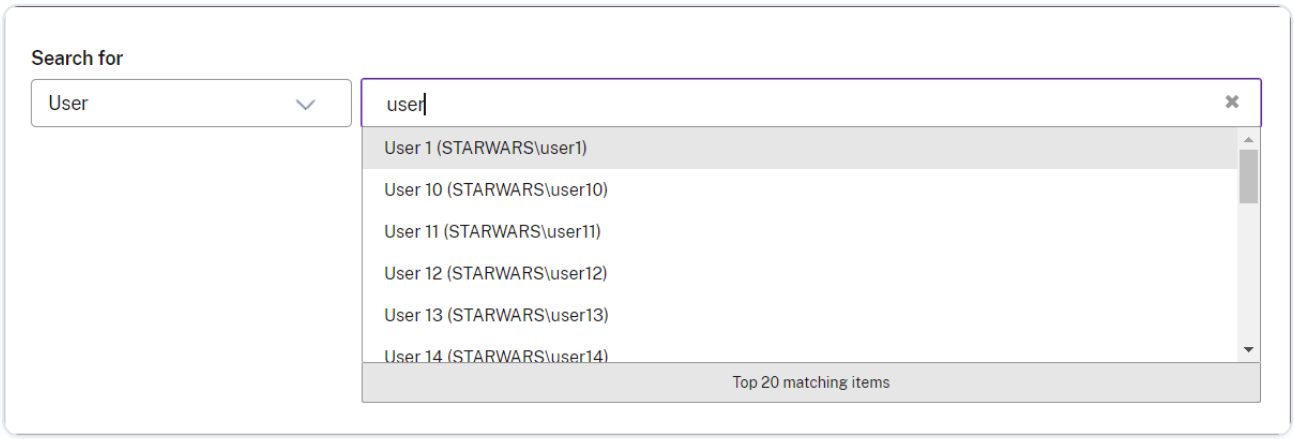
ユーザー別にSecure Private Accessセッションを表示する

Director ダッシュボードで、**「検索」をクリックし、ユーザー名を入力します。**「セッションの選択」**画面が表示されます。

フル管理者:



ヘルプデスク管理者:



Secure Private Accessセッションのアクティビティマネージャーを表示する

Citrix Directorは、Secure Private Accessセッションのアクティビティマネージャービューを提供し、セッションアクティビティの全体像を把握できます。アクティビティマネージャーは、正常に開かれた、開くのに失敗したすべてのアプリとデスクトップ、およびSecure Private Accessアプリで設定されたポリシーの結果を包括的に表示します。この機能は、Citrix Virtual Apps and Desktopsバージョン2407以降で利用できます。

前提条件:

- Director 2407以降のバージョン
- Secure Private Access 2407以降のバージョン

アクティビティマネージャーには、**利用可能なアプリ**と**起動されたアプリ**の詳細が表示されます。次のセッションの詳細を確認できます。

- 起動時間
- リソース名

- リソースの種類
- アクセスされたリソース
- ステータス
- トランザクションID

Activity Managerを表示するには、次の手順を実行します。

1. Director ダッシュボードで、**「検索」をクリックし、ユーザー名を入力します。**「セッションの選択」**画面が表示されます。
2. Secure Private Accessセッションを使用して開かれたセッションを選択します。選択したセッションのアクティビティマネージャーが表示されます。

   アクティビティマネージャー(/en-us/citrix-virtual-apps-desktops/2407/media/spa-activity-manager.png)
3. **利用可能なアプリ**をクリックして、Citrix Workspaceアプリで利用可能なアプリを表示します。

または、,

起動されたアプリ（セッション）をクリックして、Citrix Workspaceアプリで開かれているアプリを表示します。

Secure Private Accessアプリで設定されたリソースのステータスでリソースをフィルタリングできます。

- 許可 - ユーザーがアクセスを許可されているリソース。このステータスは、Secure Private Accessアプリのポリシーを使用して設定されます。このリソースは、Citrix Workspaceアプリでユーザーに表示されます。
- 拒否 - ユーザーがアクセスを拒否されたリソース。このステータスは、Secure Private Accessアプリのポリシーを使用して設定されます。このリソースは、Citrix Workspaceアプリでユーザーに表示されます。
- エラー - Secure Private Accessアプリでユーザーがアクセスを許可されているリソース。ただし、何らかのエラーにより、Citrix Workspaceアプリでリソースが利用できません。列挙エラーとセッションエラーの2種類のエラーがあります。

利用可能なアプリを表示

Citrix Workspaceアプリで利用可能なWebアプリとSaaSアプリは、**利用可能なアプリ**セクションに表示されます。このセクションには、アプリの最後の列挙試行と、その列挙試行のステータスが表示されます。

次の詳細を表示できます:

- リソース名
- ステータス
- トランザクションID

また、**許可**、**拒否**、**エラー**などのアプリケーションステータスで上記の詳細をフィルタリングすることもできます。上下の矢印を使用して詳細を並べ替えることもできます。

> **注:**
>
> TCP/UDPアプリは、**利用可能なアプリ**セクションには表示されません。

起動されたアプリを表示

Citrix Workspaceアプリで開かれたアプリは、**起動されたアプリ（セッション）**セクションに表示されます。以下の詳細を表示できます。

- 起動時間
- リソース名
- リソースタイプ
- アクセスされたリソース
- ステータス
- トランザクションID

前の詳細を、**許可**、**拒否**、**エラー**などのアプリケーションステータスでフィルタリングすることもできます。また、上下の矢印を使用して詳細を並べ替えることもできます。

Secure Private Accessアプリのセッショントポロジビュー

Secure Private Accessを使用して開かれたアプリのセッショントポロジを表示できます。**アクティビティマネージャー**から目的のアプリをクリックして、選択したアプリのセッショントポロジを表示します。

Web/SaaSアプリ:

WebまたはSaaSのセッショントポロジの図](/en-us/citrix-virtual-apps-desktops/2407/media/spa-session-topology-web.png)

TCP/UDPアプリ:

アクティビティマネージャーの図](/en-us/citrix-virtual-apps-desktops/2407/media/spa-session-topology.png)

セッショントポロジ

セッショントポロジビューには、アプリの起動プロセスのフローが表示されます。エンドポイントはCitrix Gatewayに接続し、Citrix GatewayはSecure Private Accessプラグインに接続します。Secure Private Accessプラグインからの情報を使用して、アプリが起動されます。この機能は、Citrix Virtual Apps and Desktopsバージョン2407以降で利用できます。

前提条件:

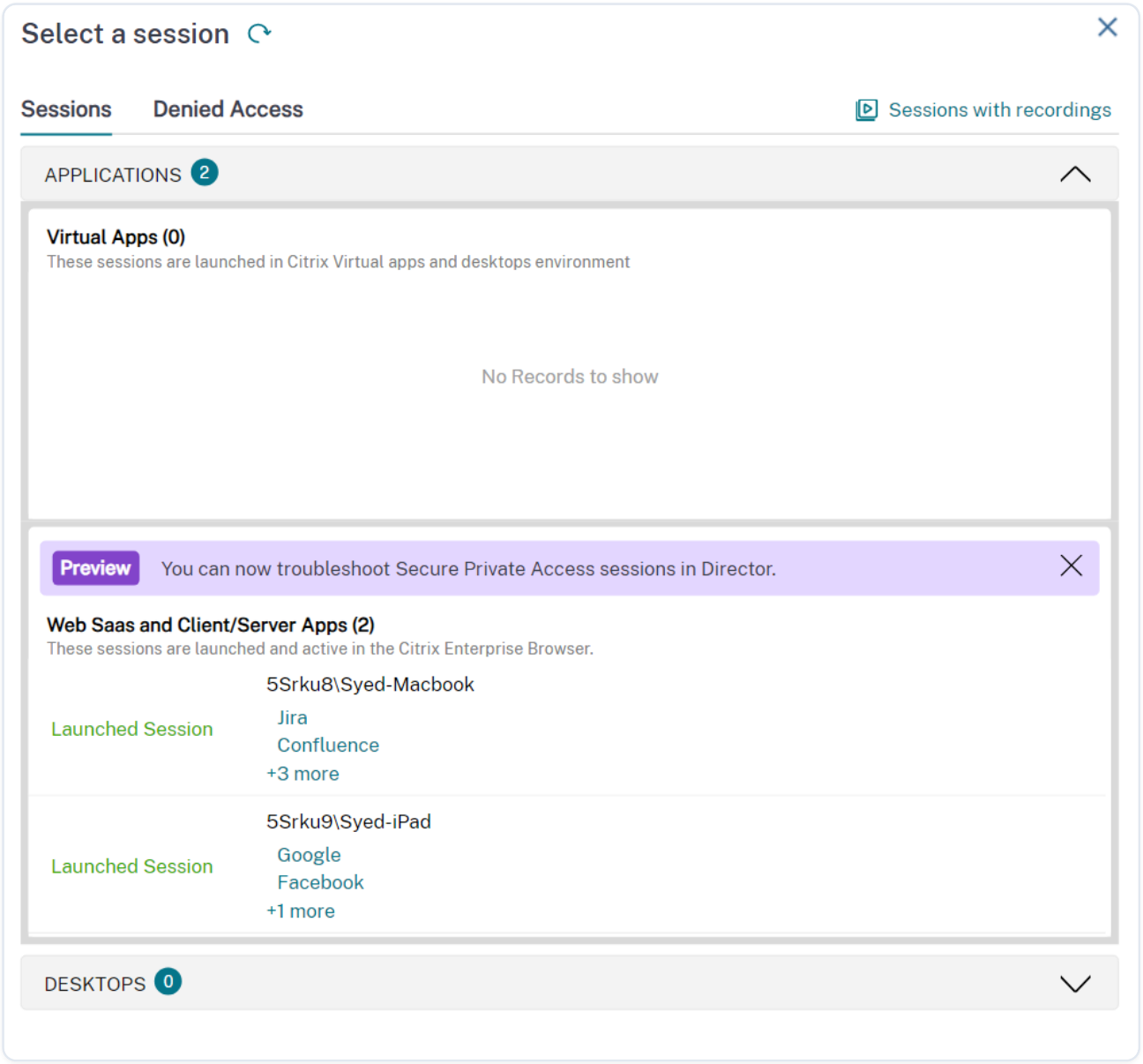
- Director 2407以降のバージョン
- Secure Private Access 2407以降のバージョン
- Citrix Secure Access 24.8.1.x以降のバージョン

以下の項目を表示できます。

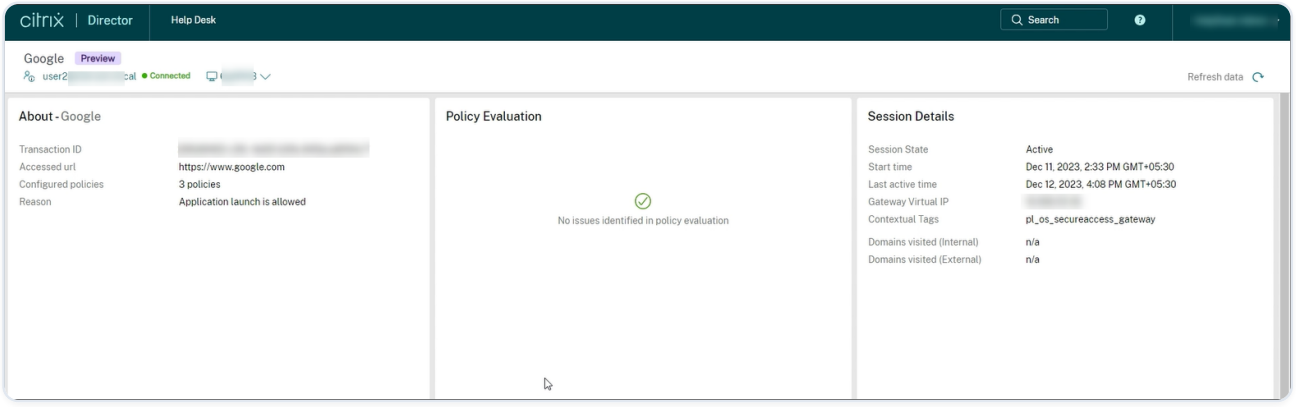
- エンドポイント - アプリが開かれたエンドポイントを表示します。選択可能なオプションは、Citrix WorkspaceアプリとCitrix Secure Agentです。デバイスIDが表示されます。
- 内部ネットワーク - 列挙されたアプリの数と構成されたポリシーの数を表示します。
- ポリシー評価 - Secure Private Accessアプリに設定されているポリシーの結果を表示します。異なる値は、**許可**、**拒否**、**制限付きアクセス許可**、および**エラー**です。これはWebまたはSaaSアプリにのみ適用されます。
- 起動されたアプリ - アプリの種類とアプリ起動のステータスを表示します。アプリの種類として可能な値は、Web/SaaSアプリまたはTCP/UDPアプリです。同様に、アプリ起動ステータスとして可能な値は、**許可**、**拒否**、**制限付きアクセス許可**、および**エラー**です。

正常に起動されたWebアプリとSaaSアプリを表示する

正常に起動されたアプリは、**Web SaaSおよびクライアント/サーバーアプリ**セクションに表示されます。



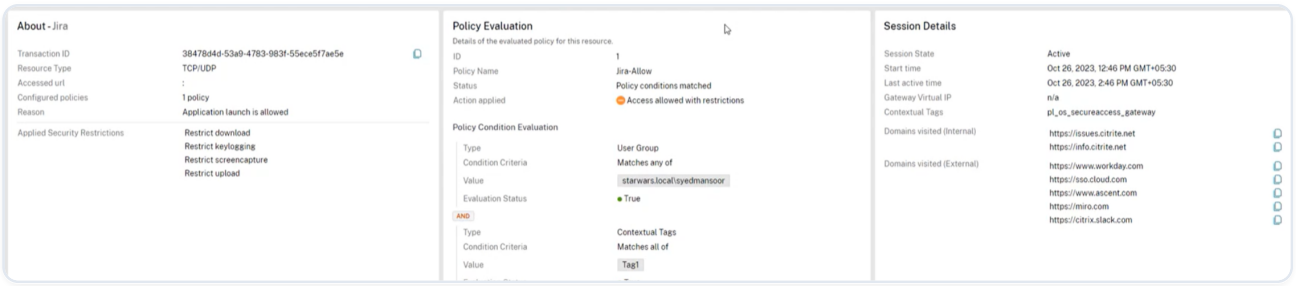
Web SaaSおよびクライアント/サーバーアプリセクションからアプリをクリックして、詳細を表示します。



成功コードの詳細については、「Citrix Director関連コード」を参照してください。

アクセス拒否されたアプリの詳細を表示する

セッションの選択画面で、**アクセス詳細の確認**をクリックします。



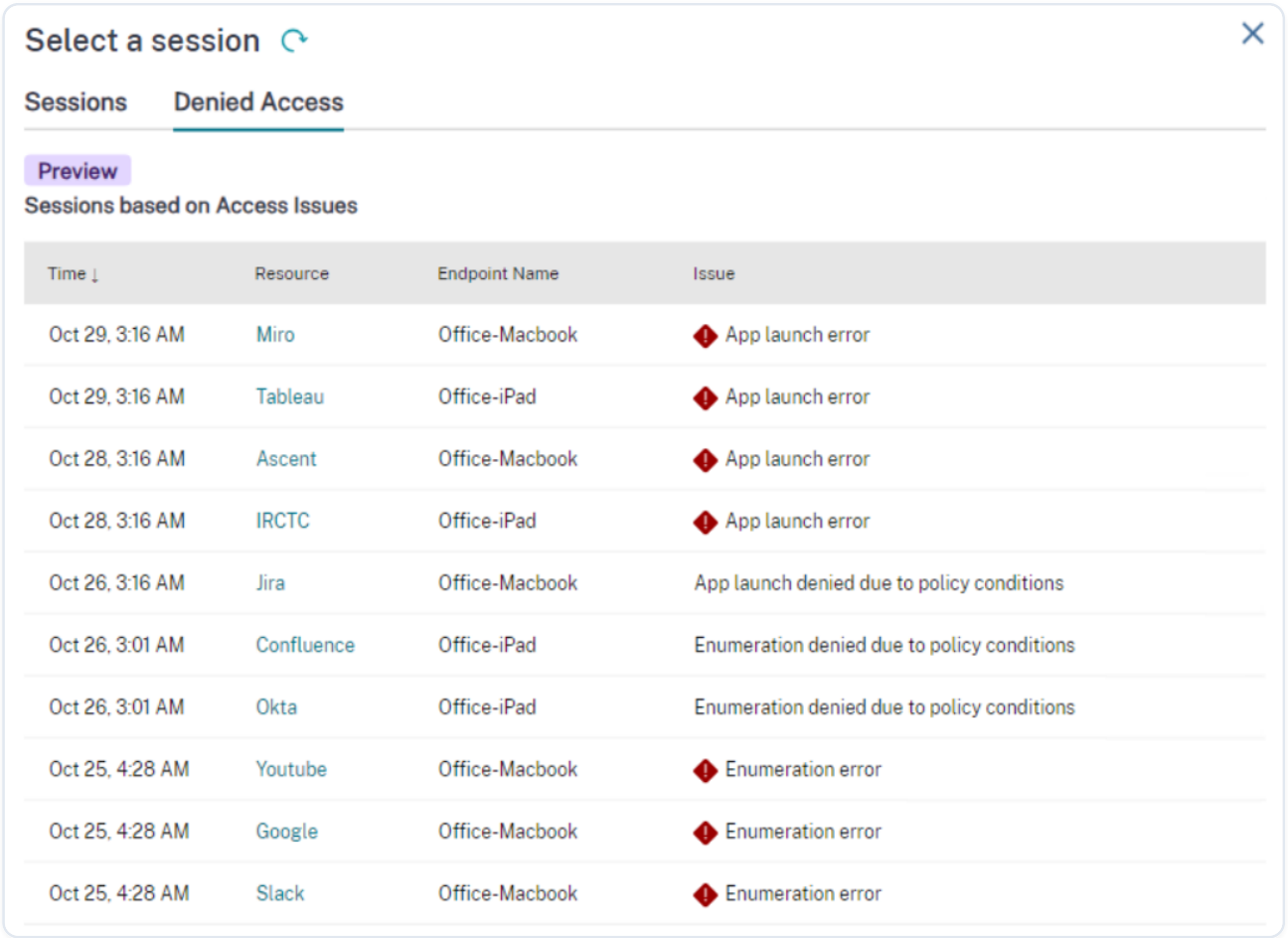
注:

アクセス詳細の確認ボタンは、アクティブなセッションがない場合に表示されます。

または、,

アクセスが拒否されたアプリを表示するには、**アクセス拒否**タブをクリックします。

アクセス拒否タブが開きます。

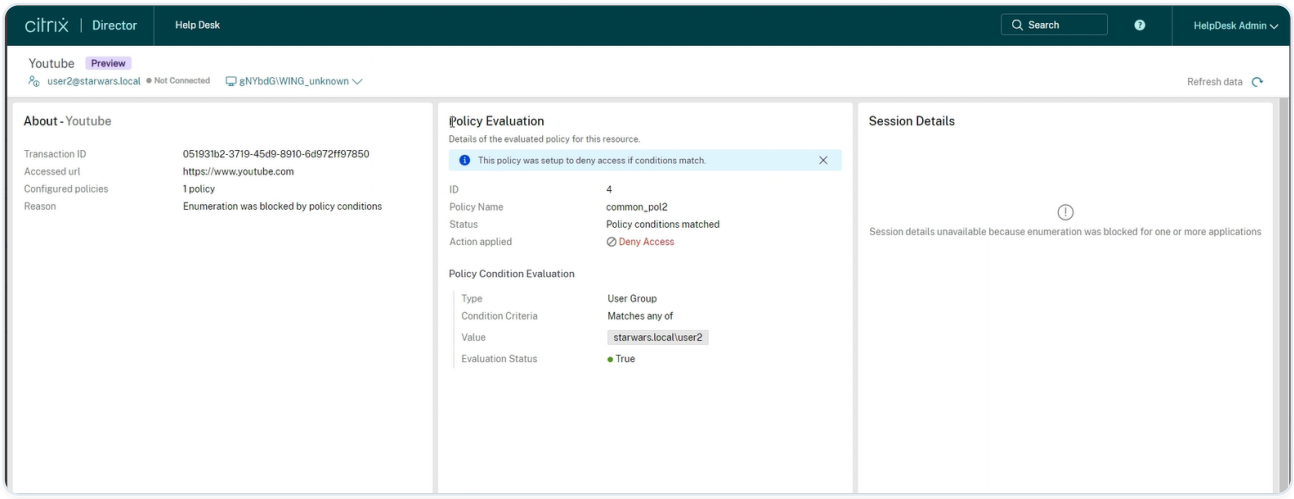


時間、リソース、エンドポイント名、失敗の理由などのセッション詳細が表示されます。エラーコードの詳細については、「Citrix Director関連コード」を参照してください。

現在、以下の問題が確認されています。

- ポリシー条件により列挙が拒否されました
- アプリの起動エラー
- 列挙エラー
- ポリシー条件によりアプリの起動が拒否されました

アクセス拒否タブ > **リソース**列からアプリを選択して、詳細を表示します。



成功または失敗したセッションについて、以下の詳細が表示されます。

- アプリについて
- ポリシー評価
- セッションの詳細

アプリについて

成功、失敗、または拒否されたアプリの名前が表示されます。それに加えて、成功または失敗したアプリの以下の詳細が表示されます。

フィールド	説明
トランザクションID	セッションまたは列挙中のCitrixトランザクションID。
リソースの種類	リソースの種類を表示します。指定できる値は、Web、SaaS、TCP/UDP (サーバーからク

フィールド	説明
	ライアント)、およびTCP/UDP (クライアントからサーバー) です。
アクセスされたリソース	セッションまたは列挙中にアクセスされたリソースのURL。TCPまたはUDPアプリの場合、アクセスされたリソースの種類がTCPかUDPかを示します。
構成済みポリシー	セッションまたは列挙内で使用されるポリシーの数。
理由	セッションまたは列挙アクティビティの分析。
適用されたセキュリティ制限	Secure Private Access アプリで適用されているセキュリティ制限を表示します。

ポリシー評価

成功したセッションの評価中に問題が検出されなかったことを表示します。失敗したセッションまたは列挙の場合、評価されたポリシーの次の詳細が表示されます。

フィールド	説明
ID	Citrix トランザクション ID。
ポリシー名	ポリシーの名前。複数のポリシーがある場合、設定された条件に一致する最初のポリシーが表示されます。
ステータス	ポリシーのステータス。
適用されたアクション	ポリシーに適用されたアクション。例: アクセス拒否。
ポリシー条件の評価	
種類	ポリシー条件の種類です。
条件基準	失敗したセッションまたは列挙に適用されたポリシーの条件基準です。
値	ポリシーの値です。

フィールド	説明
評価ステータス	ポリシーの評価ステータスです。異なる値は、**許可**、**拒否**、**制限付きアクセス許可**、および**エラー**です。

セッションの詳細

失敗したセッションの場合、セッション失敗の理由が表示されます。成功したセッションの場合、次の詳細が表示されます。

フィールド	説明
セッションの状態	セッションがアクティブか非アクティブか、その状態を表示します。
開始時刻	セッションの開始時刻を表示します。
最終アクティブ時刻	成功したセッションの最終アクティブ時刻を表示します。
ゲートウェイ仮想IP	成功したセッションが接続されているゲートウェイの仮想IPアドレスを表示します。
コンテキストタグ	コンテキストタグを表示します。Secure Private Accessプラグインのコンテキストタグは、認証済みユーザーのセッションに適用されるNetScaler® Gatewayポリシー（セッション、事前認証、EPA）の名前です。
アクセスしたドメイン（内部）	成功したセッションを使用してアクセスされた内部ドメインを表示します。
アクセスしたドメイン（外部）	成功したセッションを使用してアクセスされた外部ドメインを表示します。

既知の問題

- TCP または UDP アプリの場合、列挙の詳細は **アクティビティマネージャー** ページには表示されません。
- 終了したセッションが **セッションセレクター** ポップアップでアクティブとして表示される場合があります。

過去のユーザーセッションを診断する

Citrix Directorは、アクティブ、切断、または終了状態のセッションの詳細を表示するようになりました。以前は、アクティブなセッションの詳細のみを表示できました。この機能により、ヘルプデスク管理者は、終了したセッションまたは終了状態のセッションに関する問題をトラブルシューティングできます。終了したセッションの詳細は、過去24時間および過去2日間利用可能です。終了したセッションまたは終了状態のセッションについて、以下の詳細を表示できます。

- マシン詳細パネル - 選択したセッションが起動されたマシンの利用可能な詳細を表示します
- セッション詳細パネル - 選択したセッションの利用可能な詳細を表示します。
- セッションログオン期間 - 選択したセッションにかかったログオン期間に関する情報を表示します。以下の項目にかかった時間のグラフを表示できます。
    - ブローカリング
    - マシンの起動
    - HDX™接続
    - 認証
    - GPO
    - ログオンスクリプト
    - ディスク上のプロファイルロード
    - 対話型セッション

> **注:**
>
> この機能は、Citrix Analytics and Performanceの資格を持つCitrix Directorのお客様のみが利用できます。

過去のユーザーセッションを表示するには、次の手順を実行します。

1. **フィルター** > **セッション**ビューをクリックします。
2. 「**関連ユーザー**」をクリックして、ユーザーのActivity Managerを開きます。

   過去のユーザーセッションのアクティビティマネージャー(/en-us/citrix-virtual-apps-desktops/2407/media/dir-his-user-sessions-am.png)
3. 「**終了したセッション**」セクションから必要なセッションを選択します。

4. 「**マシン詳細**」パネルと「**セッション詳細**」パネルを表示します。

   過去のユーザーセッションの詳細(/en-us/citrix-virtual-apps-desktops/2407/media/dir-his-user-sessions-details.png)

5. 下にスクロールして、終了したセッションの「**セッションログオン期間**」を表示します。

   過去のユーザーセッションの期間(/en-us/citrix-virtual-apps-desktops/2407/media/dir-his-user-sessions-duration.png)

ハイブリッドマルチクラウド展開における統合検索

以前は、トリアージ中にDirectorでユーザーを検索すると、オンプレミスサイトのユーザーである場合にのみ、ユーザーの詳細が表示されました。ユーザーがクラウドサイトのユーザーである場合は、Monitorに移動して再度検索する必要がありました。

この強化された検索機能により、Directorの**検索**オプションを使用して、クラウドサイトまたはオンプレミスサイトのユーザーを検索できます。この機能は、ハイブリッド展開（クラウドサイトとオンプレミスサイトの両方）を使用している場合や、トリアージ目的でDirectorを使用している場合に利用できます。オンプレミスサイトかクラウドサイトかに関わらず、ユーザーの詳細を取得できます。サイトがDirectorに存在する場合は、選択したセッションのActivity ManagerにDirector内で直接移動できます。サイトがDirectorに存在しない場合は、選択したセッションのActivity ManagerにMonitor内で直接移動できます。その後、トリアージを続行できます。

> **注:**
>
> Citrix Directorを介して統合検索コンソールを使用できます。

> この機能により、問題解決までの平均時間が短縮され、クラウドユーザーとオンプレミスユーザーの両方に単一のコンソールでシームレスなエクスペリエンスを提供します。追加の利点として、Directorにはクラウドサイトの詳細のみが追加されるため、データベースのサイズが急激に増加することはありません。ユーザーの詳細はクラウド自体に保存されます。

> **注:**
>
> 最大6つ以下のクラウドサイトの場合、3秒以内に検索結果を取得できます。

この機能を有効にするには、クラウドサイトをDirectorに接続する必要があります。

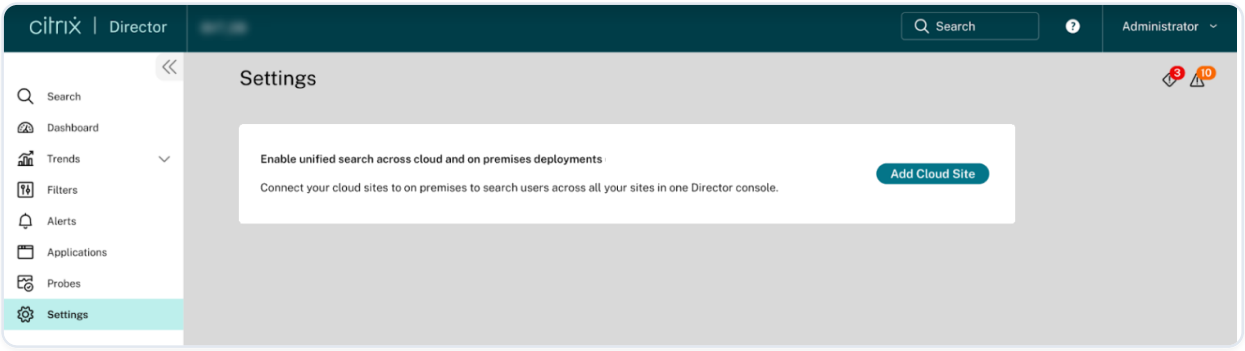
クラウドサイトをDirectorに接続する

前提条件

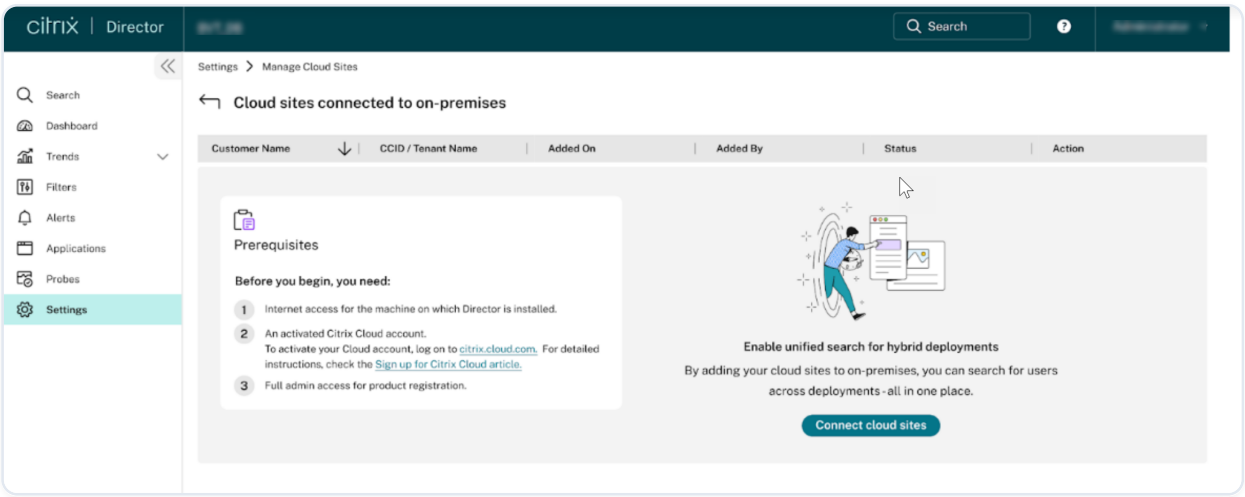
- Citrix Directorがインストールされているマシンにインターネットアクセスがあることを確認してください。
- Citrix Cloudサービスを使用するには、HTTPSポート443を介して必要なCitrixアドレスに接続できる必要があります。詳細については、インターネット接続要件を参照してください。
- 製品登録を実行するための完全な管理者アクセス権があることを確認してください。

構成手順

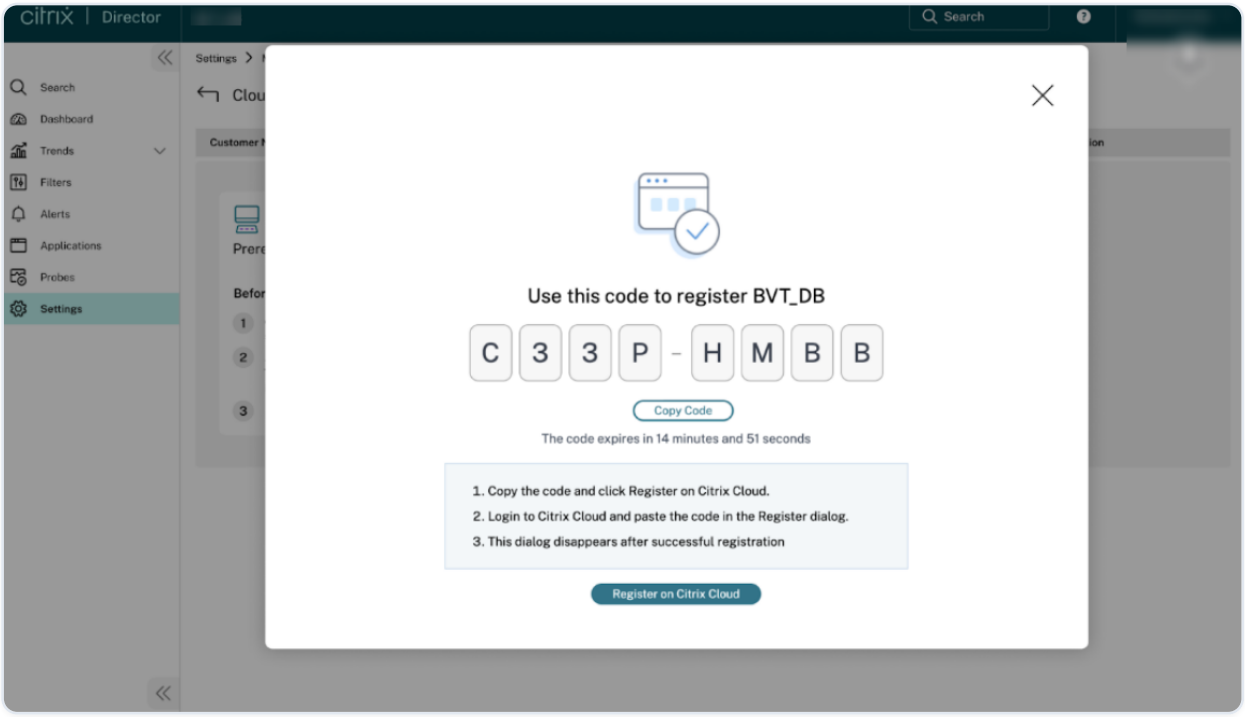
1. フル管理者としてDirectorにサインインします。Directorダッシュボードページが表示されます。
2. 「**Settings**」タブをクリックします。「**Settings**」ページが表示されます。



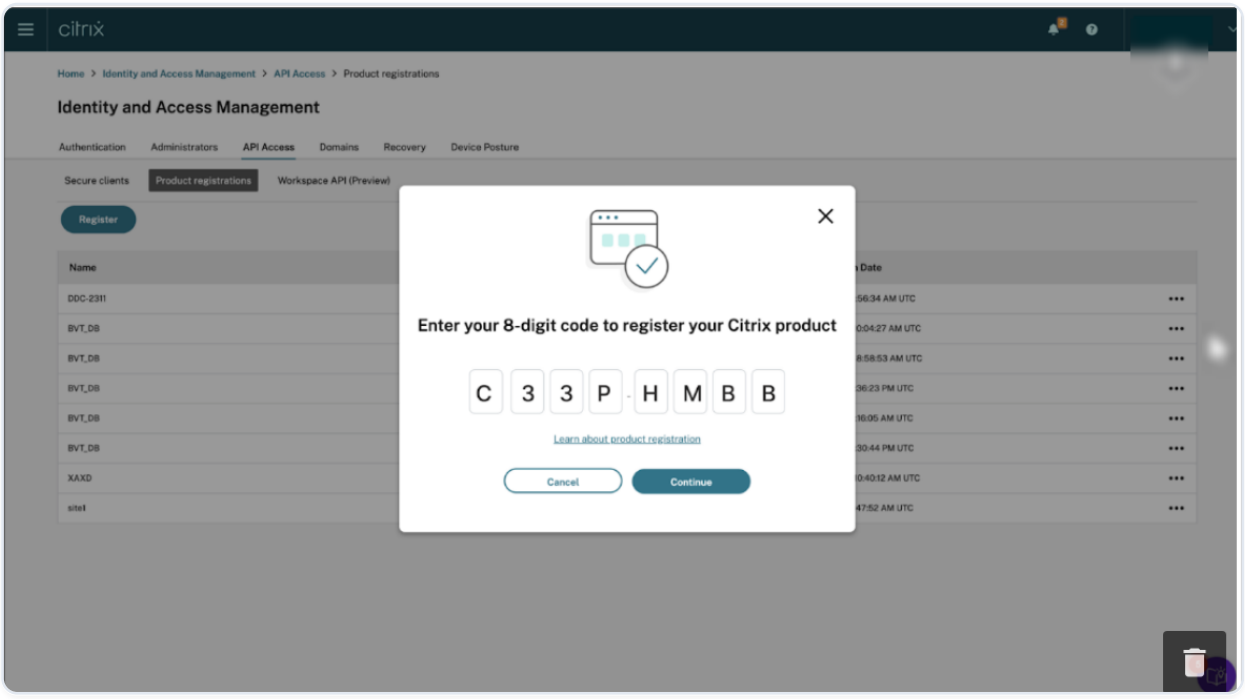
3. 「**Add Cloud Site**」をクリックします。次のページが表示されます。



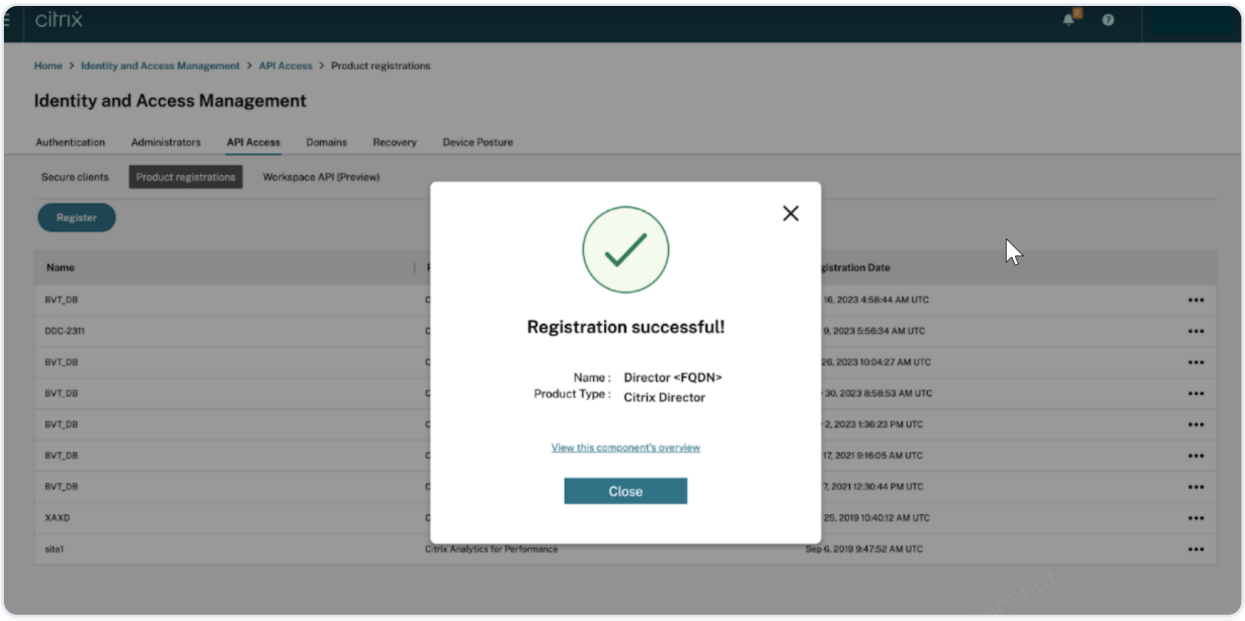
4. 前提条件を確認し、その後「**Connect cloud sites**」をクリックして構成プロセスを開始します。Citrix Cloudにこのサイトを登録するために使用する、一意の8桁の登録コードが生成されます。



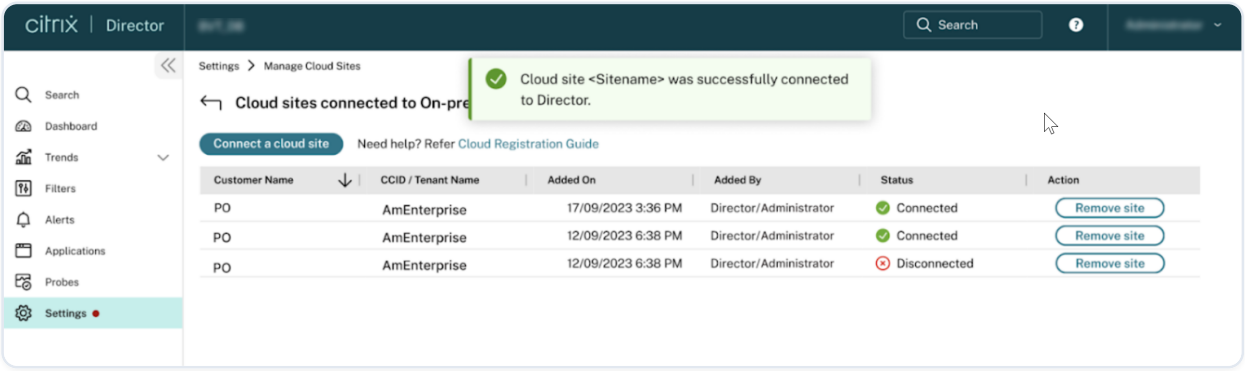
5. 「**Copy Code**」をクリックしてコードをコピーし、その後「**Register on Citrix Cloud**」をクリックします。Citrix Cloudの登録URLにリダイレクトされます。
6. Citrix Cloudの資格情報でサインインし、顧客を選択します。
7. コピーした登録コードをCitrix Cloudの「**Product Registrations**」ページに貼り付けます。「**Continue**」をクリックしてサイトを登録します。



8. 「**Continue**」をクリックします。クラウドサイトがCitrix Directorに登録され、次のメッセージが表示されます。



9. 「**Close**」をクリックします。次の画面が表示されます。



10. Directorで複数のクラウドサイトを構成するには、Directorから各サイトについて前述の構成手順を繰り返します。

    サイトごとに複数のDirectorインスタンスが実行されている場合は、いずれかのDirectorインスタンスから構成します。サイトに接続されている他のすべてのDirectorインスタンスは、構成プロセスの後、次回の更新時に更新されます。

> **注：**
>
> Citrix Directorからサイトを切断するには、**サイトの削除**をクリックします。このオプションは、既存の構成を削除します。

ハイブリッド展開からのユーザー検索

ユーザーを検索するには、次の手順を実行します。

1. 上部のナビゲーションバーで「**検索**」をクリックします。「**展開の監視とトラブルシューティング**」ページが表示されます。

   統合検索サイト(/en-us/citrix-virtual-apps-desktops/2407/media/unified-search-site.png)

2. ドロップダウンリストから**ユーザー**を選択し、ユーザー名を入力します。オンプレミスおよびクラウド展開からのアクティブおよび失敗したセッションのリストが表示されます。

   統合検索 - 完了(/en-us/citrix-virtual-apps-desktops/2407/media/unified-search-done.png)

3. 検査するセッションを選択します。

- クラウド展開を使用するセッションの場合、ユーザーコンテキストを含む関連するDaaS Monitor URLが**アクティビティマネージャー**ページで開かれ、迅速にトラブルシューティングを開始できます。
- オンプレミス展開を使用するセッションの場合、アクティビティマネージャーページが迅速に開かれ、トラブルシューティングを開始できます。

フレームホーク

> **重要:**
>
> Citrix Virtual Apps and Desktops 7 1903 以降、Framehawk はサポートされなくなりました。代わりに、アダプティブトランスポートが有効なThinwireを使用してください。

> Framehawk は、高いパケット損失が発生しやすいブロードバンドワイヤレス接続（Wi-Fi および 4G/LTE セルラーネットワーク）を使用するモバイルワーカー向けの、専門的なディスプレイリモートテクノロジーです。Framehawk は、スペクトル干渉とマルチパス伝播の課題を克服します。Framehawk は、Windows および iOS モバイルデバイス（ラップトップやタブレットなど）で仮想アプリとデスクトップを使用するユーザーに、流動的でインタラクティブなユーザーエクスペリエンスを提供します。サーバーのスケーラビリティを最大化し、ネットワーク帯域幅の消費を最小限に抑えるため、Framehawk は上記の特定のユースケースでのみ使用することをお勧めします。その他のすべてのユースケースでは、データスループットを最大化するために多くの Framehawk の概念を取り入れたアダプティブトランスポートをお勧めします。

Citrix® ポリシーテンプレートを使用して、組織に適した方法で、特定のユーザーセットとアクセスシナリオに対して Framehawk を実装できます。Framehawk は、ラップトップやタブレットなどのシングルスクリーンモバイルユースケースを対象としています。リアルタイムのインタラクティブなパフォーマンスのビジネス価値が、サーバーリソースの追加コストとブロードバンド接続の要件を正当化する場合に、Framehawk を使用してください。

Framehawk がスムーズなユーザーエクスペリエンスを維持する方法

Framehawk は、フレームバッファの内容を見て、画面上のさまざまな種類のコンテンツを識別する、人間の目のソフトウェア実装と考えてください。ユーザーにとって何が重要でしょうか？ビデオや動くグラフィックのように画面の領域が急速に変化する場合、一部のピクセルが失われても人間の目には問題ありません。それらの領域は新しいデータで迅速に上書きされます。

しかし、画面の静的な領域に関しては、人間の目は非常に敏感です。たとえば、通知領域やツールバーのアイコン、またはユーザーが読み始めたい場所にスクロールした後のテキストなどです。ユーザーは、これらの領域がピクセルパーフェクトであることを期待します。**1と0**の観点から技術的に正確であることを目指すプロトコルとは異なり、Framehawk はテクノロジーを使用している人間にとって関連性があることを目指しています。

Framehawk には、次世代のサービス品質信号増幅器と、ワークロードをよりきめ細かく効率的に識別するための時間ベースのヒートマップが含まれています。データ圧縮に加えて、自律的で自己修復型の変換を使用し、データの再送信を回避して、クリック応答、線形性、一貫したケイデンスを維持します。損失の多いネットワーク接続では、Framehawk は補間によって損失を隠すことができ、ユーザーはより流動的なエクスペリエンスを楽しみながら、良好な画質を認識できます。さらに、Framehawk アルゴリズムは、異なる種類のパケット損失をインテリジェントに区別します。たとえば、ランダムな損失（補償のためにさらにデータを送信する）と輻輳による損失（チャネルがすでに詰まっているため、これ以上データを送信しない）などです。

Citrix Workspace™ アプリの Framehawk インテントエンジンは、上下スクロール、ズーム、左右移動、読み取り、入力、その他の一般的なアクションを区別します。このエンジンは、共有辞書を使用して Virtual Delivery Agent (VDA) への通信も管理します。ユーザーが読もうとしている場合、テキストの視覚的品質は優れている必要があります。ユーザーがスクロールしている場合、それは迅速かつスムーズでなければなりません。そして、ユーザーがアプリケーションまたはデスクトップとのインタラクションを常に制御できるように、中断可能である必要があります。

ネットワーク接続上のケイデンス（自転車のチェーンの張力に類似した**ギアリング**）を測定することで、Framehawk ロジックはより迅速に反応し、高遅延接続で優れたエクスペリエンスを提供します。この独自の特許取得済みギアリングシステムは、ネットワーク状態に関する常に最新のフィードバックを提供し、Framehawk が帯域幅、遅延、損失の変化に即座に反応できるようにします。

Thinwire と Framehawk を使用する際の設計上の考慮事項

Framehawk は、(User Datagram Protocol (UDP) の上に構築されたデータ転送層を使用します。Framehawk のパフォーマンスを他の UDP ベースのプロトコルと比較するとわかるように、UDP は Framehawk が損失を克服する方法の小さな部分です。UDP は、Framehawk を際立たせる人間中心の技術に重要な基盤を提供します。

Framehawk にはどのくらいの帯域幅が必要ですか？

ブロードバンドワイヤレスの意味は、接続を共有しているユーザー数、接続の品質、使用されているアプリなど、いくつかの要因に依存します。最適なパフォーマンスを得るために、Citrix は、ベースとして 4 Mbps または 5 Mbps に加え、同時ユーザーあたり約 150 Kbps を推奨しています。

Thinwireの帯域幅の推奨事項は、通常、ベースとして1.5 Mbpsにユーザーあたり150 Kbpsを加えたものです。詳細については、Citrix Virtual Apps and Desktops帯域幅ブログを参照してください。パケット損失が3%の場合、TCP経由のThinwireは、良好なユーザーエクスペリエンスを維持するためにFramehawkよりもはるかに多くの帯域幅を必要とすることがわかります。

Thinwireは、ICA®プロトコルにおける主要なディスプレイリモートチャネルであり続けています。Framehawkはデフォルトで無効になっています。Citrixは、組織内のブロードバンドワイヤレスアクセスシナリオに対処するために、選択的に有効にすることをお勧めします。Framehawkは、Thinwireよりもかなり多くのサーバーリソース（CPUとメモリ）を必要とすることに注意してください。

要件と考慮事項

Framehawkには、VDA 7.6.300以降およびGroup Policy Management 7.6.300以降が必要です。

エンドポイントには、Workspace app for Windows 1808以降、またはCitrix Receiver for Windows 4.3.100以降、Workspace app for iOS 1808以降、またはCitrix Receiver for iOS 6.0.1以降が最低限必要です。

デフォルトでは、Framehawkは双方向のUser Datagram Protocol (UDP) ポート範囲（3224から3324）を使用して、Framehawkディスプレイチャネルデータを Citrix Workspace appと交換します。この範囲は、**Framehawk display channel port range**というポリシー設定でカスタマイズできます。クライアントと仮想デスクトップ間の同時接続ごとに一意のポートが必要です。Citrix Virtual Apps™サーバーなどのマルチユーザーOS環境では、同時ユーザーセッションの最大数をサポートするのに十分なポートを定義してください。VDIデスクトップなどのシングルユーザーOSの場合、単一のUDPポートを定義するだけで十分です。Framehawkは、最初に定義されたポート

から、範囲内で指定された最後のポートまで使用を試みます。これは、Citrix Gatewayを介して接続する場合と、StoreFrontサーバーに直接内部接続する場合の両方に適用されます。

リモートアクセスの場合、Citrix Gatewayを展開する必要があります。デフォルトでは、Citrix GatewayはUDPポート443を使用して、クライアントのCitrix Workspace appとGateway間の暗号化された通信を行います。このポートは、両方向の安全な通信を許可するために、外部ファイアウォールで開いている必要があります。この機能はDatagram Transport Security (DTLS)として知られています。

> **注:**
>
> Framehawk/DTLS接続はFIPSアプライアンスではサポートされていません。
>
> 暗号化されたFramehawk接続は、NetScaler Gatewayバージョン11.0.62以降およびNetScaler Unified Gatewayバージョン11.0.64.34以降でサポートされています。

NetScaler High Availabilityは、XenAppおよびXenDesktop 7.12以降でサポートされています。

Framehawkを実装する前に、以下の推奨事項を考慮してください。

- Framehawk用に定義されたUDPポートがファイアウォールで開いていることを確認するために、セキュリティ管理者に連絡してください。インストールプロセスでは、ファイアウォールは自動的に構成されません。
- 多くの場合、Citrix GatewayはDMZにインストールされ、外部と内部の両側からファイアウォールに挟まれていることがあります。外部ファイアウォールでUDPポート443が開いていることを確認してください。環境がデフォルトのポート範囲を使用している場合は、内部ファイアウォールでUDPポート3224から3324が開いていることを確認してください。

構成

> **注意:**
>
> Citrixは、高いパケット損失が発生する可能性のあるユーザーに対してのみFramehawkを有効にすることを推奨しています。また、サイト内のすべてのオブジェクトに対してFramehawkをユニバーサルポリシーとして有効にしないことを推奨します。

> Framehawkはデフォルトで無効になっています。有効にすると、サーバーはユーザーグラフィックと入力にFramehawkを使用しようとします。何らかの理由で前提条件が満たされない場合、接続はデフォルトモード（Thinwire）を使用して確立されます。

以下のポリシー設定がFramehawkに影響します。

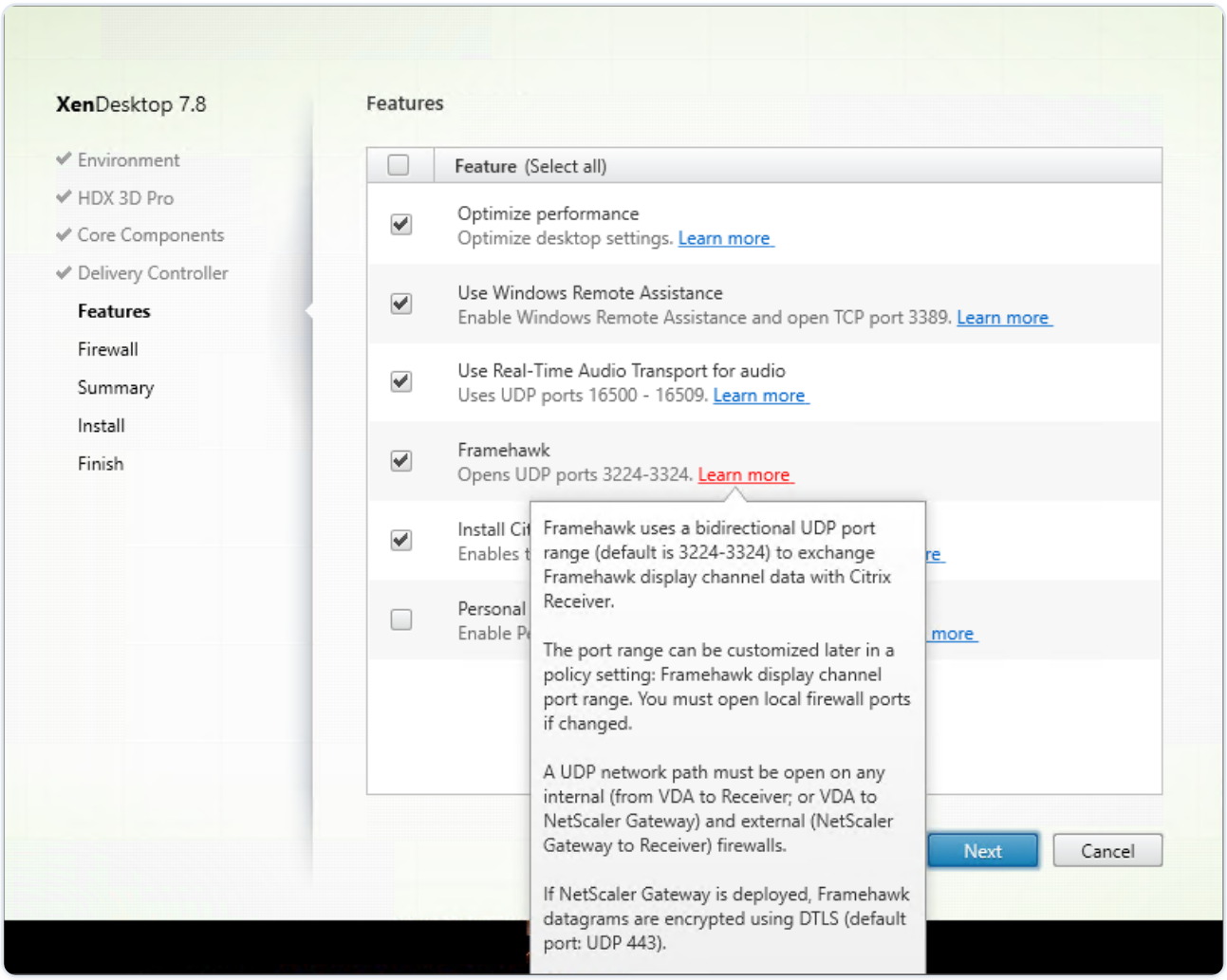
- Framehawkディスプレイチャネル: この機能を有効または無効にします。
- Framehawkディスプレイチャネルポート範囲: VDAがユーザーデバイスとFramehawkディスプレイチャネルデータを交換するために使用するUDPポート番号の範囲（最小ポート番号から最大ポート番号まで）を指定します。VDAは、最小ポート番号から開始し、その後の試行ごとにインクリメントして、各ポートを使用しようとします。このポートは、インバウンドおよびアウトバウンドトラフィックを処理します。

Framehawk ディスプレイチャネルのポートを開く

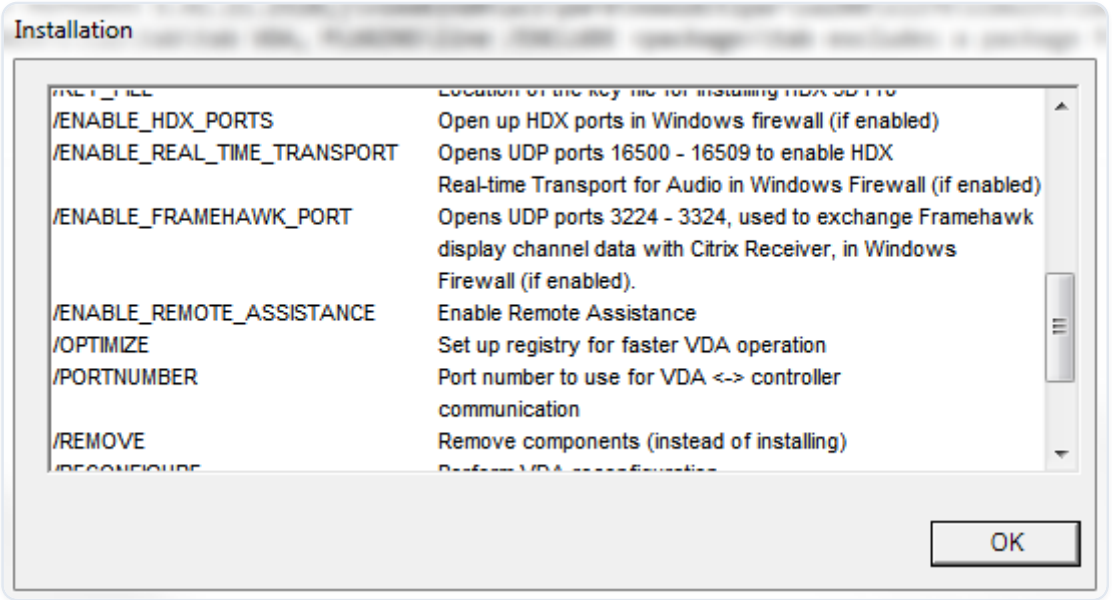
XenAppおよびXenDesktop 7.8以降では、VDAインストーラーの**機能**ステップでファイアウォールを再構成するオプションが利用できます。このチェックボックスを選択すると、Windowsファイアウォールで UDPポート3224から3324が開かれます。次のような状況では、手動でのファイアウォール構成が必要です。

- 任意のネットワークファイアウォールの場合。 または
- デフォルトのポート範囲がカスタマイズされている場合。

これらの UDP ポートを開くには、 チェックボックスをオンにします。



コマンドラインを使用して、**/ENABLE_FRAMEHAWK_PORT** で Framehawk 用の UDP ポートを開くこともできます。

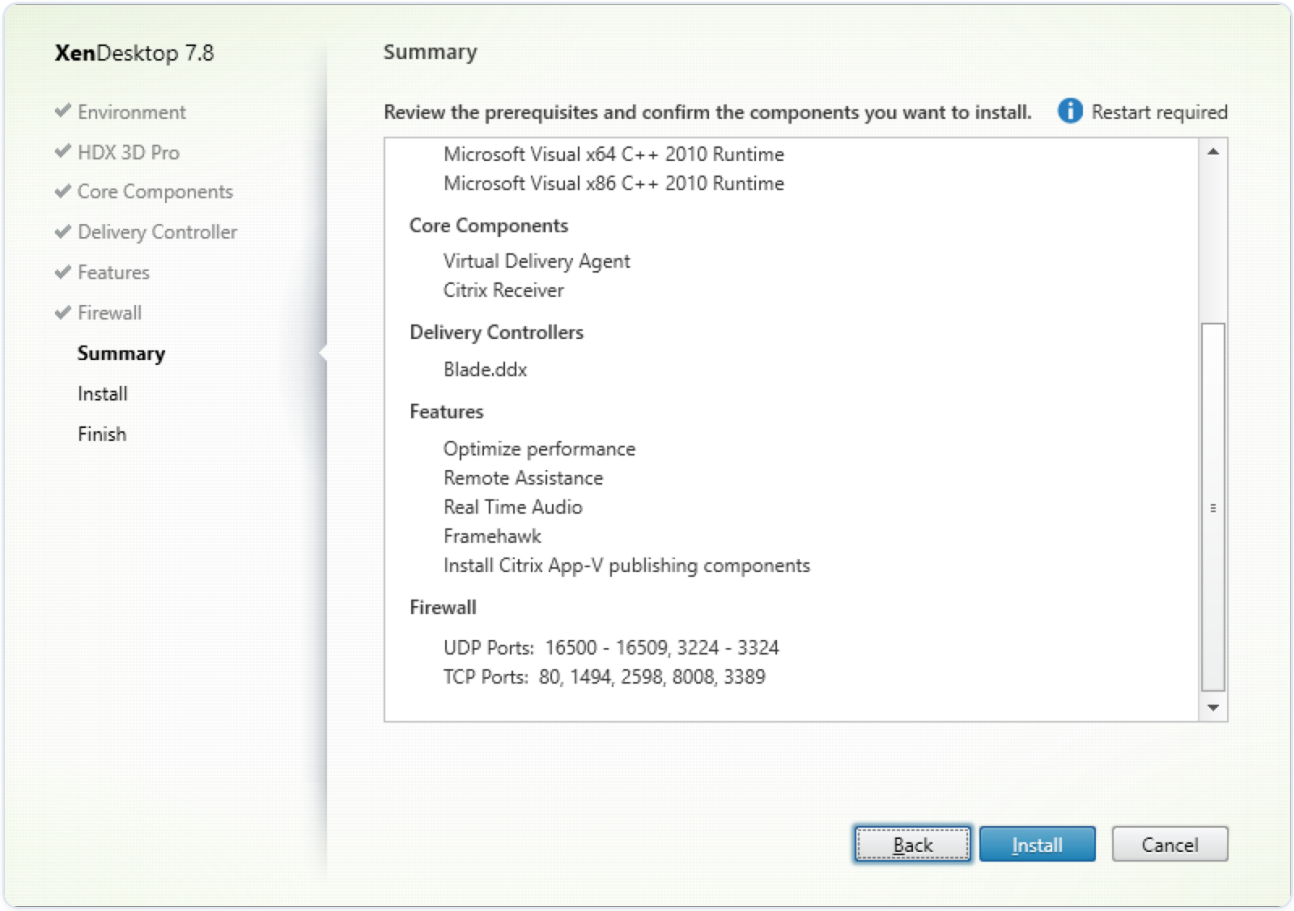


Framehawk UDP ポートの割り当ての確認

インストール中に、**ファイアウォール**画面でFramehawkに割り当てられているUDPポートを確認できます。

デフォルトのUDPポート(/en-us/citrix-virtual-apps-desktops/2407/media/firewall-default-udp-ports-fh.png)

概要画面でFramehawk機能が有効になっているかどうかが示されます。



FramehawkのCitrix Gatewayサポート

暗号化されたFramehawkトラフィックは、Citrix Gateway 1808以降およびNetScaler Gateway 11.0.62.10以降、ならびにCitrix Unified Gateway 1808およびNetScaler Unified Gateway 11.0.64.34以降でサポートされています。

- Citrix Gatewayは、Gateway VPN仮想サーバーがエンドユーザーデバイスから直接アクセスできる展開アーキテクチャを指します。つまり、VPN仮想サーバーにはパブリックIPアドレスが割り当てられており、ユーザーはこのIPアドレスに直接接続します。
- Unified Gatewayを使用するCitrix Gatewayは、Gateway VPN仮想サーバーがコンテンツスイッチング仮想サーバー（CS）のターゲットとしてバインドされている展開を指します。この展

開では、CS仮想サーバーがパブリックインターネットプロトコルアドレスを持ち、Gateway VPN仮想サーバーがダミーのインターネットプロトコルアドレスを持ちます。

Citrix GatewayでFramehawkサポートを有効にするには、Gateway VPN仮想サーバーレベルのDTLSパラメーターを有効にする必要があります。パラメーターが有効になり、Citrix Virtual AppsまたはCitrix Virtual Desktops™のコンポーネントが正しく更新されると、Framehawkのオーディオ、ビデオ、およびインタラクティブトラフィックはGateway VPN仮想サーバーとユーザーデバイス間で暗号化されます。

Citrix Gateway、Unified Gateway、およびCitrix Gateway + グローバルサーバー負荷分散はFramehawkでサポートされています。

以下のシナリオはFramehawkではサポートされていません。

- HDX™ インサイト
- IPv6モードのCitrix Gateway
- Citrix Gatewayダブルホップ
- クラスター設定のCitrix Gateway

シナリオ	FRAMEHAWK のサポート
シトリックス ゲートウェイ	はい
Citrix Gateway + グローバルサーバー負荷分散	はい
Unified Gateway を使用したCitrix Gateway	はい。**注：** Unified Gateway バージョン11.0.64.34以降がサポートされています。
HDX インサイト	いいえ
IPv6モードのCitrix Gateway	いいえ
Citrix Gatewayダブルホップ	いいえ
シトリックス ゲートウェイ上の複数のセキュアチケットオーソリティ	はい
Citrix Gatewayと高可用性	はい
Citrix Gatewayとクラスター設定	いいえ

Framehawk サポートのための Citrix Gateway の構成

Citrix GatewayでFramehawkサポートを有効にするには、Gateway VPN *仮想サーバー* レベルでDTLSパラメーターを有効にします。パラメーターが有効になり、Citrix Virtual Apps and Desktops™のコンポーネントが正しく更新されると、Framehawkのオーディオ、ビデオ、およびインタラクティブトラフィックは、Gateway VPN仮想サーバーとユーザーデバイスの間で暗号化されます。

リモートアクセス用にCitrix GatewayでUDP暗号化を有効にする場合、この構成が必要です。

Framehawk サポートのために Citrix Gateway を構成する場合：

- 外部ファイアウォールでUDPポート443が開いていることを確認します
- 外部ファイアウォールでCGPポート（デフォルト2598）が開いていることを確認します
- VPN仮想サーバーの設定でDTLSを有効にします
- SSL証明書とキーのペアをアンバインドして再バインドします。Citrix Gateway 1808以降、またはNetScalerバージョン11.0.64.34以降を使用している場合は、この手順は不要です。

Framehawk サポートのために Citrix Gateway を構成するには：

1. Citrix Gatewayを展開および構成して、StoreFront™と通信し、Citrix Virtual Apps and Desktopsのユーザーを認証します。
2. Citrix Gateway Configuration タブで、Citrix Gateway を展開し、**Virtual Servers** を選択します。
3. **Edit** を選択して VPN 仮想サーバーの基本設定を表示し、DTLS 設定の状態を確認します。
4. **More** を選択して、その他の構成オプションを表示します。
5. Framehawk などのデータグラムプロトコルに通信セキュリティを提供するには、**DTLS** を選択します。**OK** をクリックします。VPN 仮想サーバーの基本設定領域に、DTLS フラグが **True** に設定されていることが表示されます。
6. サーバー証明書バインド画面を再度開き、**+** をクリックして証明書キーペアをバインドします。
7. 以前の証明書キーペアを選択し、**Select** をクリックします。
8. サーバー証明書バインドへの変更を保存します。
9. 保存後、証明書キーペアが表示されます。**Bind** をクリックします。
10. **No usable ciphers configured on the SSL vserver/service** という警告メッセージが表示された場合は、無視してください。

以前の NetScaler® Gateway バージョンの手順

NetScaler Gateway のバージョンが 11.0.64.34 より古い場合：

1. サーバー証明書バインド画面を再度開き、+ をクリックして証明書キーペアをバインドします。
2. 以前の証明書キーペアを選択し、**Select** をクリックします。
3. サーバー証明書バインドへの変更を保存します。
4. 保存後、証明書キーペアが表示されます。**Bind** をクリックします。
5. 「**SSL vserver/service で使用可能な暗号が構成されていません**」という警告メッセージが表示されても無視してください。

Framehawk をサポートするように Unified Gateway を構成するには、次の手順を実行します。

1. Unified Gateway がインストールされ、適切に構成されていることを確認します。詳細については、Citrix 製品ドキュメントサイトのUnified Gateway情報を参照してください。
2. CS *仮想サーバー*にターゲット *仮想サーバー*としてバインドされている VPN *仮想サーバー*で DTLS パラメーターを有効にします。

制限事項

クライアントデバイスにCitrix Gateway仮想サーバーの古いDNSエントリがある場合、アダプティブトランスポートとFramehawkはUDPトランスポートではなくTCPトランスポートにフォールバックする可能性があります。TCPトランスポートへのフォールバックが発生した場合は、クライアントのDNSキャッシュをフラッシュし、再接続してUDPトランスポートを使用してセッションを確立してください。

Framehawkは、PTC Creoなどのアプリケーションに見られる32ビットのマウスポインターをサポートしていません。

Framehawkは、シングルモニターを使用するラップトップやタブレットなどのモバイルデバイス向けに設計されており、デュアル/マルチモニター構成ではThinwireに戻ります。

その他のVPN製品のサポート

Citrix Gateway は、Framehawk で必要とされる UDP 暗号化をサポートする唯一の SSL VPN 製品です。別の SSL VPN または誤ったバージョンの Citrix Gateway が使用されている場合、Framehawk ポリシーが適用されないことがあります。従来の IPsec VPN 製品は、変更なしで Framehawk をサポートします。

Framehawkの監視

Citrix DirectorからFramehawkの使用状況とパフォーマンスを監視できます。HDX仮想チャネルの詳細ビューには、任意のセッションでFramehawkのトラブルシューティングと監視に役立つ情報が含まれています。Framehawk関連のメトリックを表示するには、［**Graphics-Framehawk**］を選択します。

Framehawk接続が確立されている場合、詳細ページに **Provider = VD3D** および **Connected = True** と表示されます。仮想チャネルの状態がアイドルであるのは正常です。これは、初期ハンドシェイク中にのみ使用されるシグナリングチャネルを監視するためです。このページには、接続に関するその他の有用な統計も表示されます。

問題が発生した場合は、Framehawk のトラブルシューティングブログを参照してください。

負荷分散されたWeb Studio展開をセットアップする

高可用性Web Studio展開をセットアップするには、NetScaler® ADCやWindowsネットワーク負荷分散などのツールを選択できます。この記事では、NetScaler ADCアプライアンスを使用して負荷分散されたWeb Studio展開をセットアップする方法について、ステップバイステップのガイドを提供します。

HA Web Studio の図(/en-us/citrix-virtual-apps-desktops/2407/media/load-balanced-studio.png)

証明書の要件

商用証明機関から証明書を購入する前、またはエンタープライズ証明機関から証明書を発行する前に、ニーズに基づいて以下のオプションを検討してください。

オプション	長所	短所
オプション1: NetScaler ADCアプライアンスのロードバランサーサーバーとWeb Studioサーバーの両方で、**.example.com*ワイルドカード証明書を使用します。	• 構成を簡素化する • 管理が容易 (単一の証明書) • 証明書を更新せずに新しいサブドメインを追加できる	• ワイルドカード証明書が侵害された場合、すべてのサブドメインが危険にさらされます • すべてのアプリケーションがワイルドカード証明書をサポート

オプション	長所	短所	
		しているわけではありません • 個別の証明書よりも費用がかかる場合がある	
オプション2: NetScaler ADCアプライアンスロードバランサーサーバーとWeb Studioサーバーの両方で、サブジェクト代替名 (SAN) を持つ証明書を使用する。	• 柔軟性があり、複数の特定のドメインとサブドメインを含めることができる • 複数のドメインの管理を一元化できる • 複数の異なる名前をサポートし、ワイルドカードよりも柔軟性がある	• ドメイン数が増えるにつれて、SANエントリの管理が複雑になる可能性がある • 新しいドメインを追加するには、証明書の再発行が必要 • CAがサポートするSANエントリの数によって制限される	
オプション3: 各Web StudioサーバーとNetScaler ADCアプライアンスロードバランサーサーバーに個別の証明書を使用する	• 各サーバーは個別に保護される • 1つの証明書が侵害されても、他の証明書には影響しない • 各サーバーのニーズに合わせて特定の証明書を使用できる	• 各証明書を個別に管理する必要があるため、管理上のオーバーヘッドが増加する • 更新する証明書が増え、コストが高くなる可能性 • すべての証明書が一貫して構成されていること	

オプション	長所	短所
		を確認する必要がある

ロードバランサーでサーバー証明書を構成する

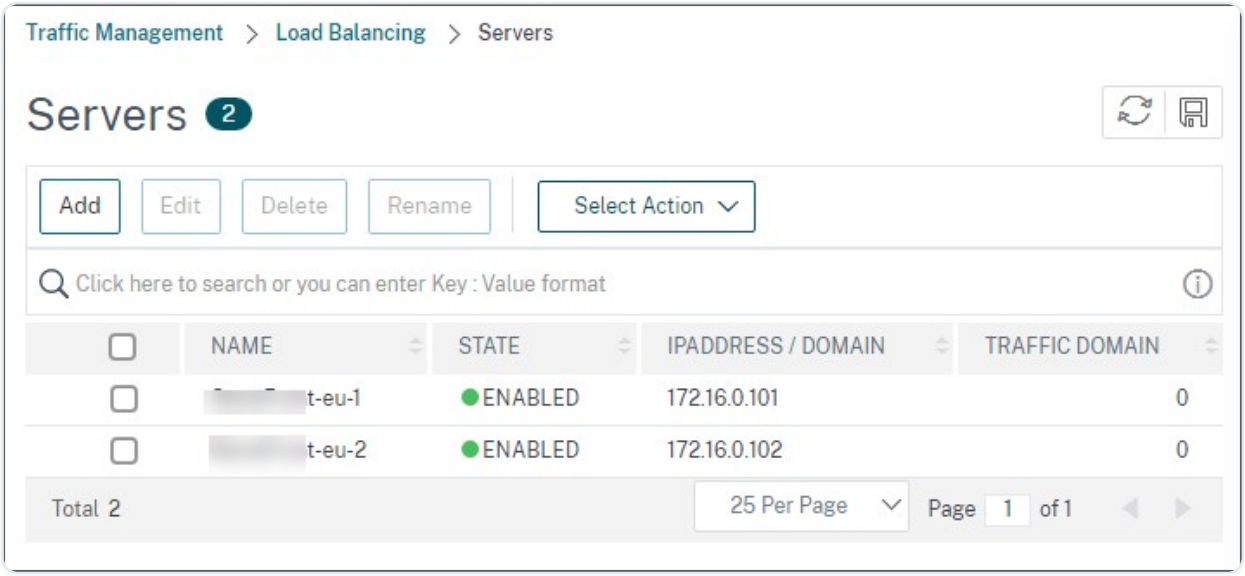
1. NetScaler ADCアプライアンス管理GUIにログオンします。
2. **トラフィック管理 > SSL > 証明書 > サーバー証明書** を選択します。
3. **Install** をクリックします。
4. **Install Server Certificate** ページで、証明書とキーのペア名を入力し、**Choose File** をクリックして、証明書ファイルを参照します。証明書ファイルに秘密キーが含まれていない場合は、**Key File** を選択します。

   証明書インストール画面のスクリーンショット (/en-us/citrix-virtual-apps-desktops/2407/media/cert-install.png)

ステップ1：Web Studioサーバーノードを追加する

すべてのWeb Studioサーバーノード（例: `Studio-eu-1` および `Studio-eu-2`）をロードバランサーに追加します。

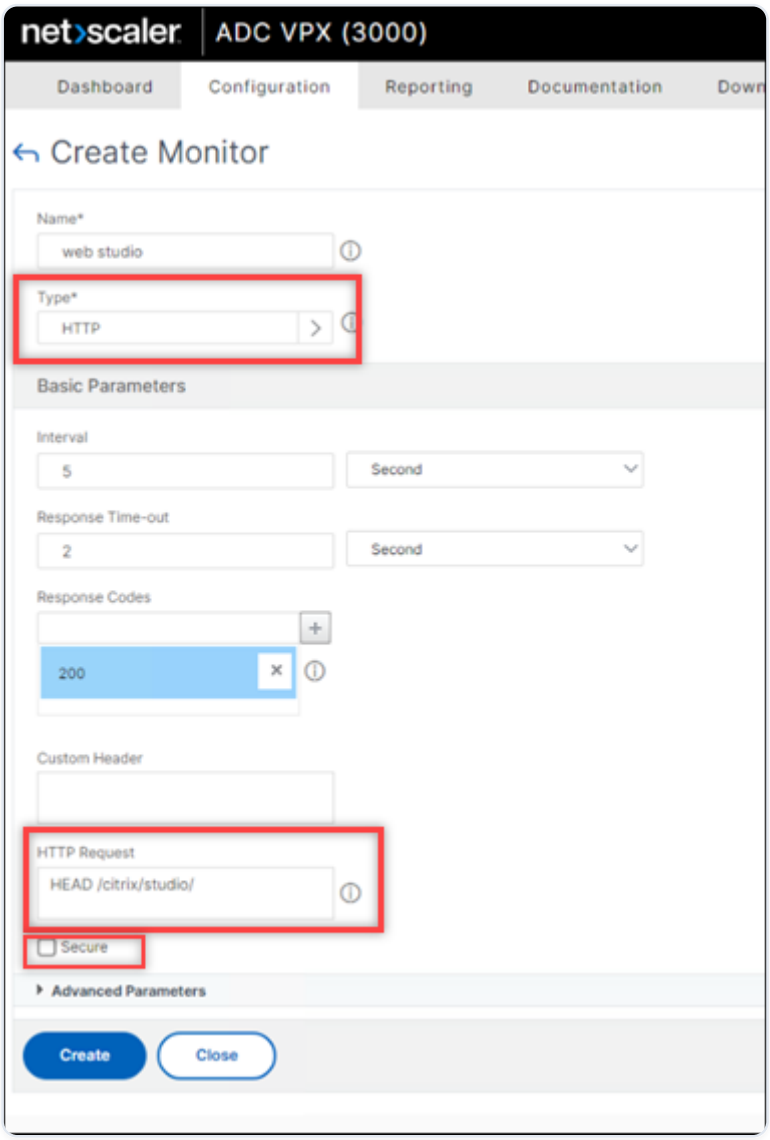
1. NetScaler ADC管理GUIにログオンします。
2. **Traffic Management > Load Balancing > Servers** に移動します。**Add** をクリックします。
3. Web Studioサーバーノードのサーバーipアドレスを入力します。
4. 手順2〜3を繰り返して、他のWeb Studioサーバーを追加します。



ステップ2: Web Studioサーバーノード用のモニターを追加する

すべてのWeb Studioサーバーノードのステータスを確認するために、ロードバランサーでモニターを設定します。

1. 「**トラフィック管理 > ロードバランシング > モニター > 追加**」を選択します。
2. **Configuration** タブで、以下の設定を完了し、その他の設定はデフォルトのままにします。
   - **Name** に「**Web Studio**」と入力します。
   - **Type** に「**HTTP**」または「**SSL**」を選択します。
   - **Secure** オプションを選択します。
   - 「**HTTP Request**」に「**HEAD/citrix/studio/**」と入力します。



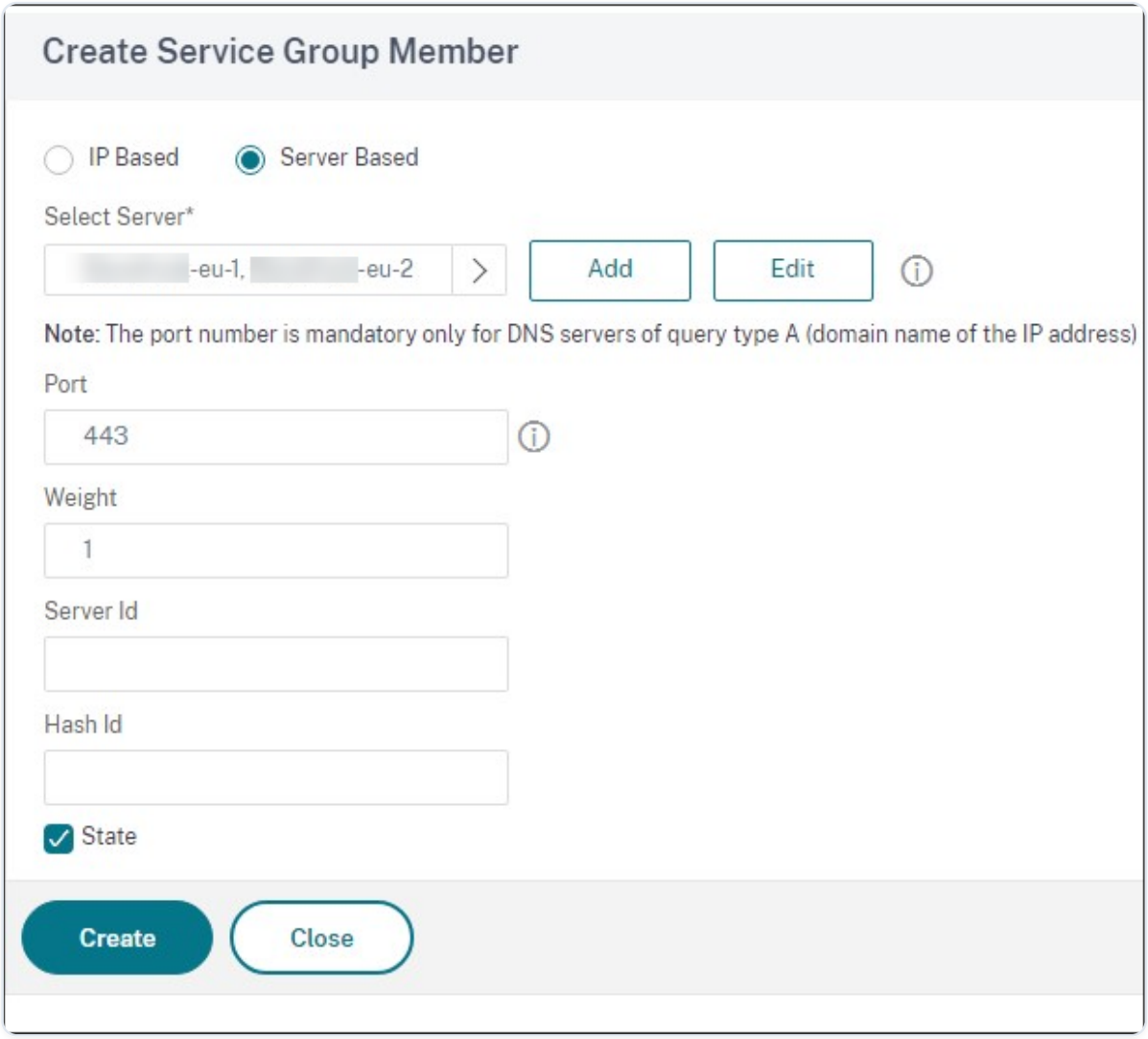
ステップ3: Web Studioサーバーノード用のサービスグループを作成する

1. **Traffic Management > Load Balancing > Service Groups > Add** を選択します。HTTPS経由でWeb Studioサーバーに接続するには、プロトコルとしてSSLを選択し、他の設定はデフォルトのままにして、**OK** をクリックします。
2. サービスグループ内で、**Service Group Members** の下にある **No Service Group Member** をクリックし、以下の手順でメンバーを追加します。

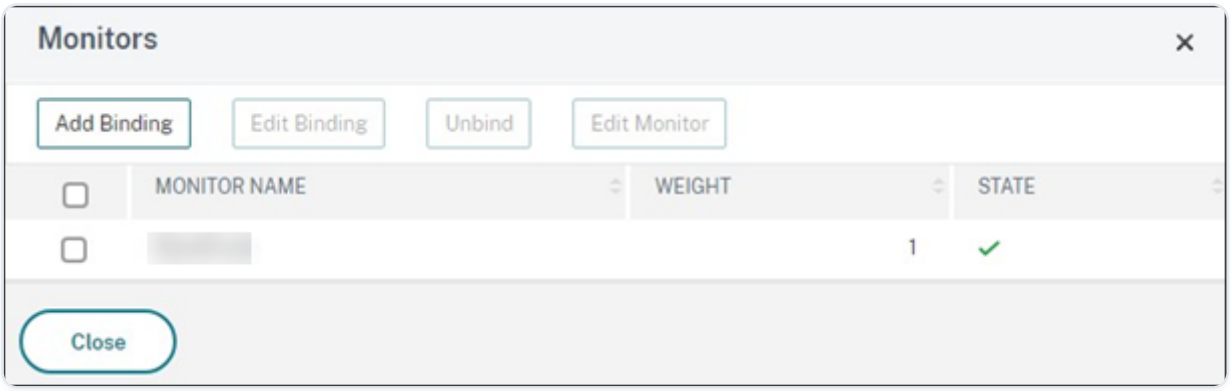
   a. **Service Based** をクリックします。

   b. 以前に追加したすべてのサーバーを選択します。

   c. ポートに**443**を入力します。



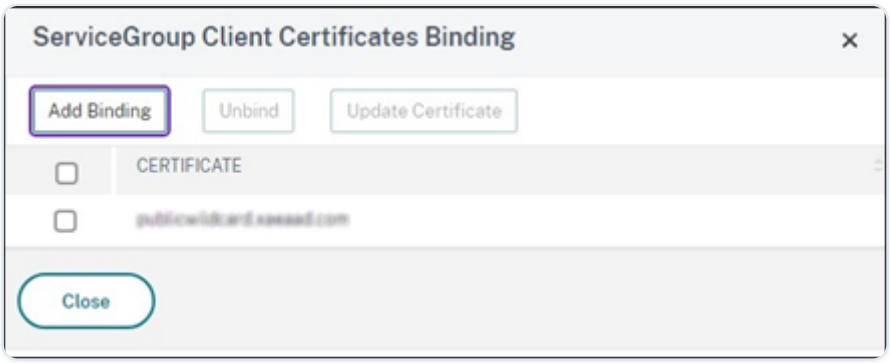
3. **モニター**セクションを追加し、以前に作成したWeb Studioモニターを選択します。



4. **証明書**セクションを追加し、次の設定を完了します。

   a. クライアント証明書をバインドします。

   b. 以前にインポートしたサーバー証明書の署名に使用されたCA証明書、およびPKI信頼チェーンの一部である可能性のあるその他のCAをバインドします。



5. **設定**セクションを追加し、**クライアントIPヘッダーの挿入**を選択し、ヘッダー名として**X-Forwarded-For**を入力します。この設定により、クライアントIPアドレスをポリシーで使用できるようになります。

ステップ4：仮想サーバーを作成する

ユーザーがWeb Studioサーバーグループにアクセスするためのロードバランサー仮想サーバーを作成します。

1. **Traffic Management > Load Balancing > Virtual Servers**に移動し、**Add**をクリックします。
2. 名前を入力し、**プロトコル**に**SSL**を選択し、**ポート**に**443**を入力して、**OK**をクリックします。



3. 以前に作成した**サービスグループ**をロードバランシング仮想サーバーにバインドします。
4. 「手順3: Web Studioサーバーノードのサービスグループを作成する」でサービスグループにバインドしたCA証明書をバインドします。
5. **Method**セクションを追加し、ロードバランシング方法を選択します。Web Studioのロードバランシングで一般的な選択肢は、**ROUNDROBIN**または**LEASTCONNECTION**です。

   負荷分散メソッドセクションのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2407/media/leastconnection.png)
6. 「**Persistence**」セクションを追加し、以下の設定を完了します。

   a. 永続化メソッドを「**COOKIEINSERT**」に設定します。

   b. タイムアウトをWeb Studio内のセッションタイムアウトと同じに設定します (デフォルトでは20分)。

   c. 将来のデバッグを容易にするためにCookieに名前を付けます。例: **NSC_SFPersistence**。

   d. バックアップ永続性を **NONE** に設定します。

   永続性セクションのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2407/media/persistence.png)

> **注:**

> クライアントがHTTP Cookieの保存を許可されていない場合、以降のリクエストにはHTTP Cookieが含まれず、永続化は使用されません。

手順5: 仮想サーバーのDNSレコードを作成する

ドメインコントローラーで、仮想サーバーのIPアドレスをFQDNにマッピングするDNSおよびPTRレコードを作成します。ネットワーク内のWeb Studioユーザーは、このFQDNを使用してWeb Studioサーバーグループにアクセスします。たとえば、webstudio.example.comは負荷分散仮想サーバーのIPアドレス（VIP）に解決されます。

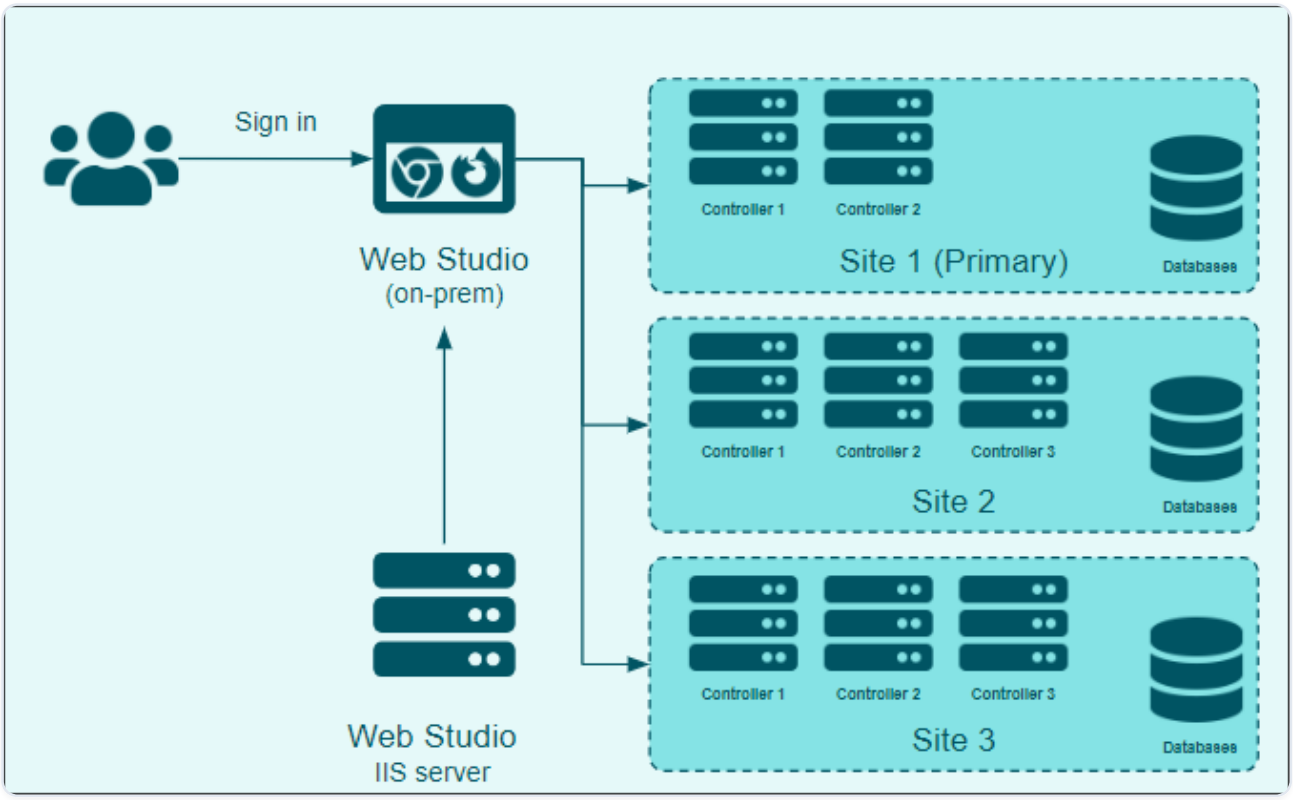
永続性セクションのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2407/media/new-dns.png)

ユーザーがWeb Studioサーバーにアクセスするための URLを提供します: `https://<FQDN of the virtual server>/<text you entered in the HTTP Request field when creating a monitor>`。例: `https://webstudio.example.com/citrix/studio`

複数サイト管理を有効にする

デフォルトでは、1つのWeb Studioコンソールは単一のCitrix Virtual Apps and Desktops™サイトにマッピングされますが、必要に応じて、Web Studioコンソールを複数のサイトを管理するように構成できます。これにより、1つのWeb Studioをインストールするだけで、すべてのサイトを構成および管理できます。

次の図は、単一のWeb Studio展開が複数の独立したCitrix Virtual Apps and Desktopsサイトを管理する、複数サイトアーキテクチャを示しています。



利点

- 統合されたシングルサインオンエクスペリエンスで複数のサイトを管理する際の効率が向上します。
- すべての構成が1つのコンソールからアクセスできるため、トラブルシューティングが容易になります。

考慮事項

サイトを構成および展開する際は、次の点に留意してください。

- 必須バージョン:
  - シトリックス バーチャルアプリおよびデスクトップ 2311 以降。
  - Delivery Controller™のバージョンは、Web Studioのバージョンと一致するか、それ以前のバージョンである必要があります。最小要件は2311以降です。
  - この機能はWeb Studio（Webベース）専用であり、Citrix Studio（Windowsベース）では利用できません。
- シングルサインオンをサポートするには、すべてのサイトを信頼されたドメインに展開します。
- 統合されたWeb Studioコンソールを使用して、最大10個のCitrix Virtual Apps and Desktopsサイトを管理できます。

ワークフロー

始める前に

- プライマリサイトを決定し、プライマリサイト管理のためにWeb Studioコンソールにアクセスできることを確認します。

> **注:**
>
> - プライマリサイトを設計する際は、追加されたサイトのアクセシビリティがプライマリサイトの可用性に依存することに注意してください。プライマリサイトのパフォーマンスの問題は、追加されたサイトへのアクセスに影響を与える可能性があります。
> - Web Studioがインストールされていない場合は、「Web Studioのインストール」を参照してください。

- Web Studioで管理する予定のサイトがすでに設定されていることを確認します。
  - 新しいサイトを作成するには、「サイトの作成」を参照してください。
- (推奨) コンソールでサイトを切り替える際にシングルサインオンを有効にするには、すべてのサイトで統合Windows認証 (IWA) を有効にします。IWAが有効になっていないサイトでは、ログイン資格情報を使用してサインインすることもできます。

手順1：Web Studioコンソールにサインインする

1. Webブラウザーを開きます。`https://<address of the server hosting Web Studio>/Citrix/Studio`と入力します。
2. Web Studioにサインインして、プライマリサイトを管理します。

> **注:**
>
> インストール時に使用するDelivery Controllerのアドレスによってサイトが識別されます。Delivery Controllerがプライマリサイトのものである場合、そのサイトにサインインします。

手順2：Web Studioを使用してサイトを追加する

1. 「**設定**」>「**サイト管理の一元化**」に移動し、「**追加**」をクリックします。

サイト管理の一元化(/en-us/citrix-virtual-apps-desktops/2407/media/centralize-site-mgmt-add.png)

2. **Virtual Apps and Desktopsサイトの追加**ページで、**サイトの追加**をクリックします。

   サイトの追加(/en-us/citrix-virtual-apps-desktops/2407/media/add-cvad-sites.png)

3. Delivery Controllerを追加するには、次のいずれかの操作を実行します。

   - 「**コントローラーの追加**」をクリックし、FQDNを入力します。「**テスト**」をクリックして接続をテストします。
   - 「**検出**」をクリックします。

     a. 「**サイト検出**」ページで、サイト内にあるコントローラーのアドレスを選択または入力します。

     b. コントローラーへの完全なアクセス許可を持つ管理者の資格情報を、「**ユーザー名**」と「**パスワード**」フィールドに入力します。

     c. 「**完了**」をクリックします。

   サイトの検出(/en-us/citrix-virtual-apps-desktops/2407/media/site-discovery.png)

   > **注:**
   >
   > 検出機能は、入力したデリバリーコントローラーのアドレスに基づいて、サイト内で到達可能なデリバリーコントローラーを自動的に追加します。

4. 「**保存**」をクリックします。

   サイト構成を管理または編集するには、「**設定**」>「**サイト管理の一元化**」に移動し、「**管理**」をクリックします。 「**管理**」オプションは、プライマリサイトでのみ有効になります。

   「一元化されたサイトを管理」(/en-us/citrix-virtual-apps-desktops/2407/media/centralize-site-mgmt-manage.png)

ステップ3：サイト設定の管理

サイト構成の変更を反映するには、ブラウザを更新してください。サイト選択ボックスは、コンソールの右上隅に表示されます。

「**設定**」ページで、「**更新**」アイコンの横にある右隅のドロップダウンメニューからサイトを選択します。 コンソールには、選択したサイトの構成が表示されます。

> **注:**
>
> - プライマリサイトに到達できない場合、それに関連付けられている他のサイトにアクセスすることはできません。
> - 別のサイトに切り替える際は、サインインに必要なアクセス許可またはアクセス資格情報があることを確認してください。

サイト構成後のサインインエクスペリエンス

1. Webブラウザーを開きます。`https://<address of the server hosting Web Studio>/Citrix/Studio`を入力します。
2. **サイト**フィールドからサイトを選択します。
3. **Windows統合サインイン**を選択するか、**ユーザー名**と**パスワード**を入力してサインインします。

   > **注:**
   >
   > Windows統合サインインは、選択したサイトで有効になっている場合にのみ利用できます。統合Windows認証の詳細については、認証の管理を参照してください。

「複数サイトのサインイン」(/en-us/citrix-virtual-apps-desktops/2407/media/multi-site-sign-in.png)

Web Studioの展開を保護する（オプション）

Web StudioをDelivery Controller™と一緒にインストールすると、インストーラーは現在のサーバーの`443`ポートにバインドされた自己署名証明書を作成します。Web StudioとDelivery Controllerは、その証明書をTLS証明書として使用します。別のマシンからアクセスする場合、Web Studioにアクセスできないか、Web Studioのログオン画面にエラーが表示されることがあります。

別のマシンからWeb Studioにアクセスしたい場合は、次の手順を実行できます。

1. Delivery Controller から自己署名証明書をエクスポートします。

   自己署名証明書のエクスポート](/en-us/citrix-virtual-apps-desktops/2407/media/export-self-signed-certificate.png)

- **秘密キーのエクスポート**では、**いいえ、秘密キーをエクスポートしません**を選択します。
- **エクスポートファイル形式**では、**DER encoded binary X.509 (.CER)**を選択します。

2. Web Studio にアクセスしたいマシンに移動し、証明書をインストールします。

   証明書のインストール](/en-us/citrix-virtual-apps-desktops/2407/media/install-certificate.png)

   - 「**ストアの場所**」で、「**ローカルコンピューター**」を選択します。

Delivery Controller から離れた専用サーバーに Web Studio をインストールすることを選択した場合、2つのタスクを実行する必要があります。

- **タスク1**: Web StudioサーバーとDelivery Controllerからそれぞれ証明書をエクスポートします。
- **タスク2**: Web Studioにアクセスしたいマシンに2つの証明書をインストールします。

> **注:**
>
> ベストプラクティスとして、外部の公開信頼証明書またはエンタープライズCAからの証明書を使用して、Web Studioの展開を保護することをお勧めします。

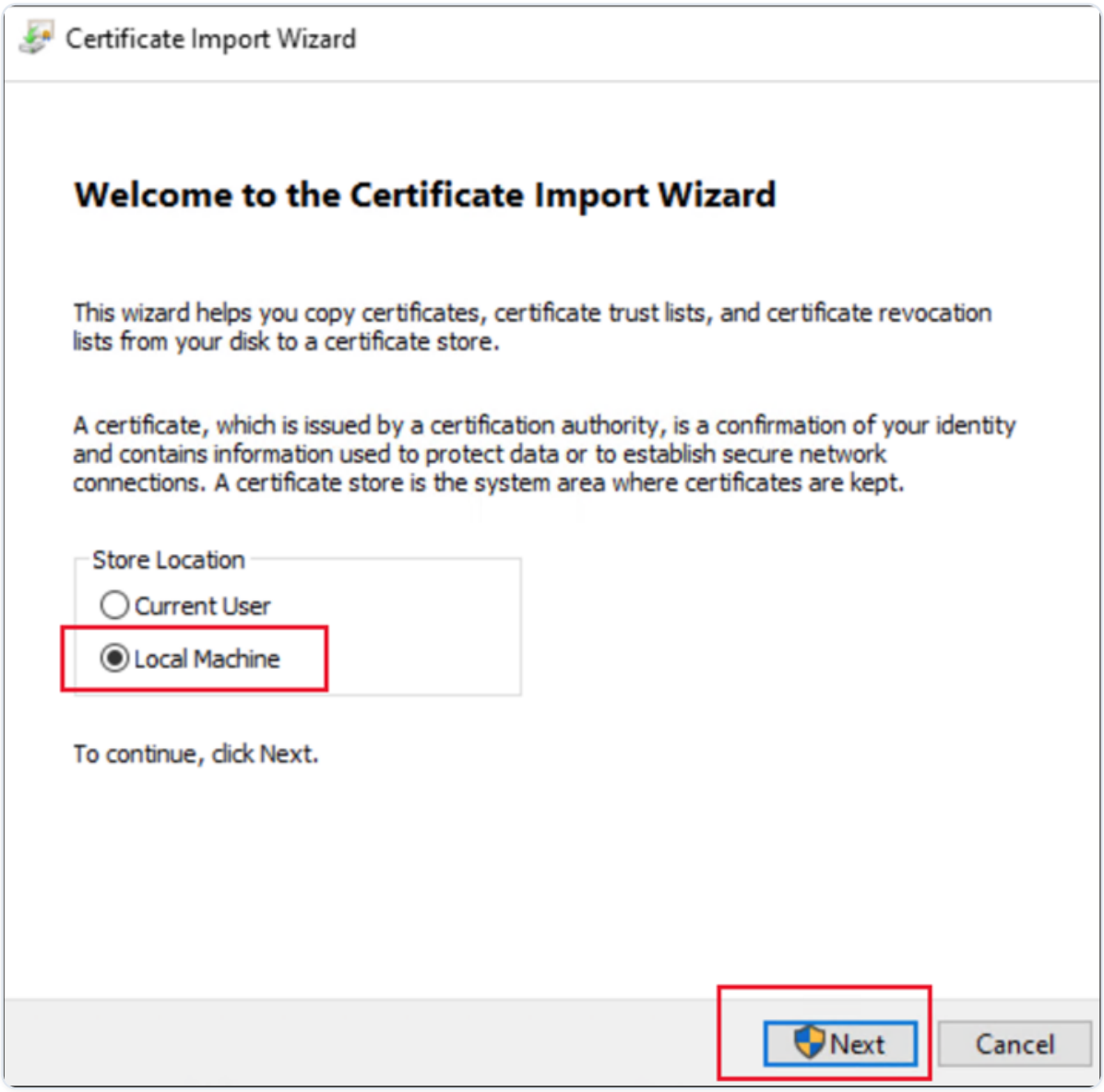
外部の公開信頼証明書を使用する

以下の3つの方法のいずれかを使用して、外部の公開信頼証明書を Web Studio サーバーにインポートできます。

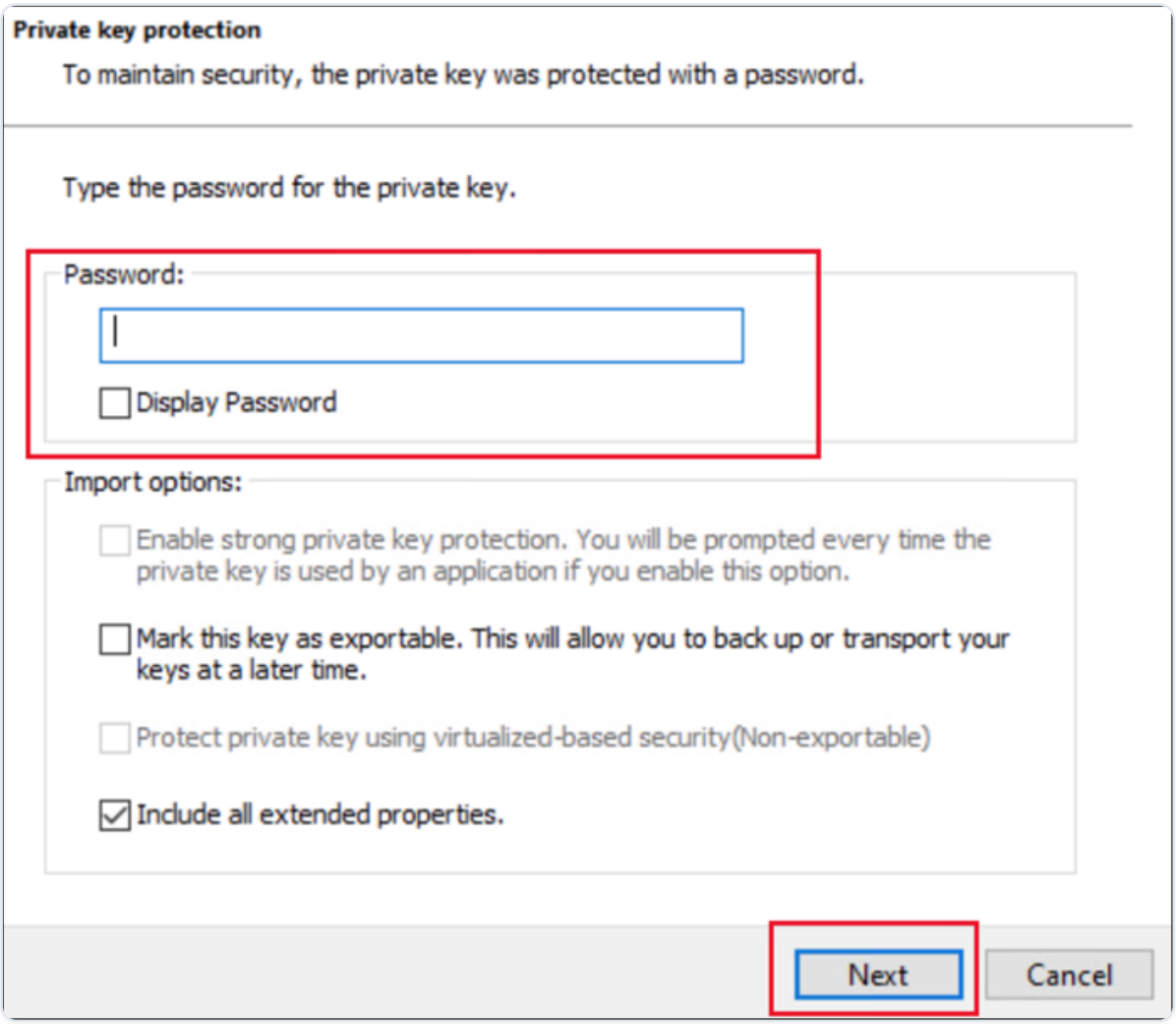
- **PFXファイルをインストールします。**

  a. PFXファイルをダブルクリックします。

  b. 「**ストアの場所**」で、「**ローカルコンピューター**」を選択します。



c. 必要に応じてパスワードを入力します。



d. **証明書ストア**には、**個人**を選択します。

証明書ストア(/en-us/citrix-virtual-apps-desktops/2407/media/certificate-store.png)

- **コンピューター証明書の管理コンソールを使用します。**

a. コンピューター証明書の管理コンソールを開き、**個人 > 証明書 > すべてのタスク > インポート**に移動します。

コンピューター証明書の管理コンソール(/en-us/citrix-virtual-apps-desktops/2407/media/manage-computer-certificates-console.png)

b. PFXファイルを選択し、必要に応じてパスワードを入力します。

- **PowerShellを使用します。**

```
Import-PfxCertificate -Password $(ConvertTo-SecureString -String
"123456" -AsPlainText -Force) -CertStoreLocation Cert:\LocalMachine\My\
-FilePath .\Desktop\certificate.pfx
```

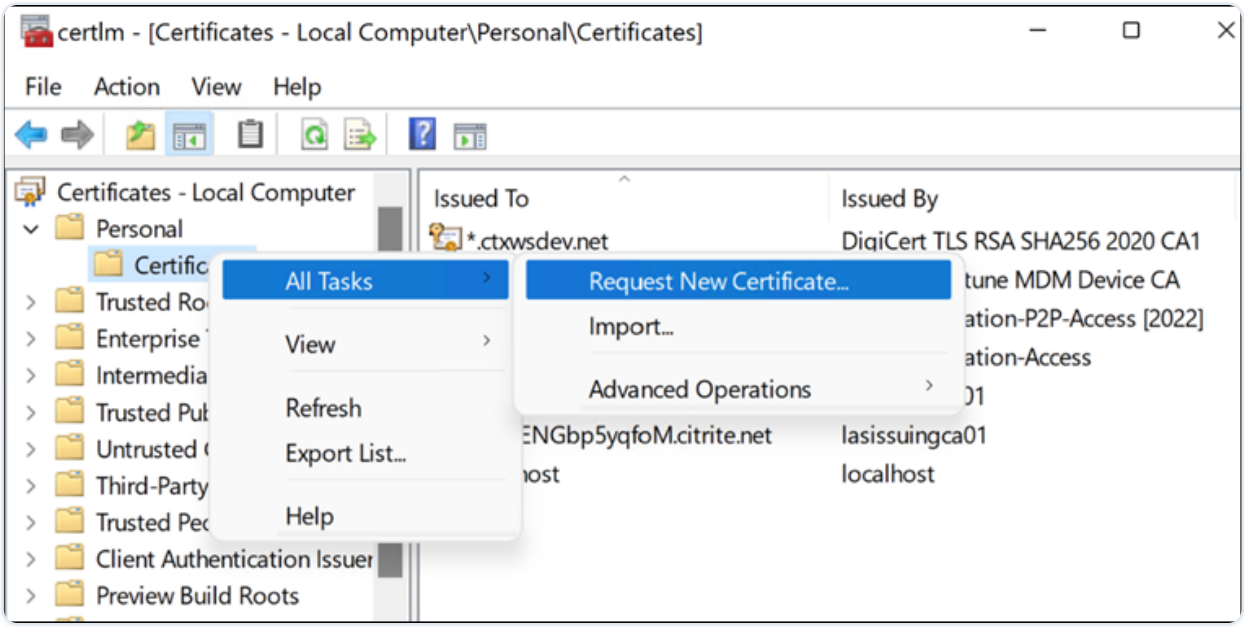
次に、証明書を`443`ポートにバインドします。これは、インストールまたはアップグレードの前、あるいはインストールまたはアップグレードの後に行うことができます。`443`ポートに証明書のバインドが構成されている場合、インストーラーは何も行いません。詳細については、「インストールまたはアップグレードの前」を参照してください。

エンタープライズCAからの証明書を使用する

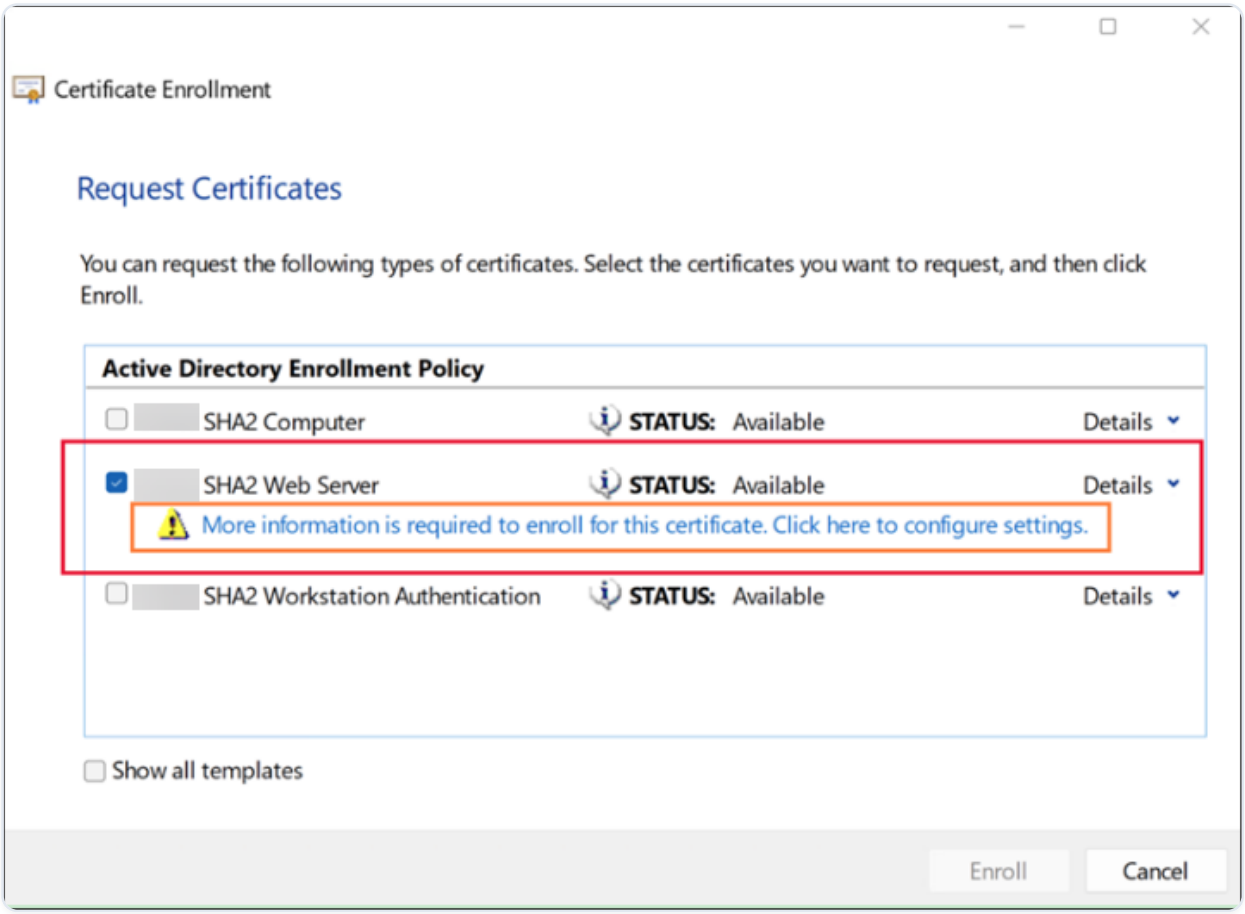
開始する前に、エンタープライズ認証局（CA）サーバーがドメインに展開されていることを確認してください。

証明書を要求するには、次の手順を実行します。

1. サーバーで、**コンピューター証明書の管理コンソール**を開きます。
2. **個人 > 証明書 > すべてのタスク > 新しい証明書の要求**に移動します。

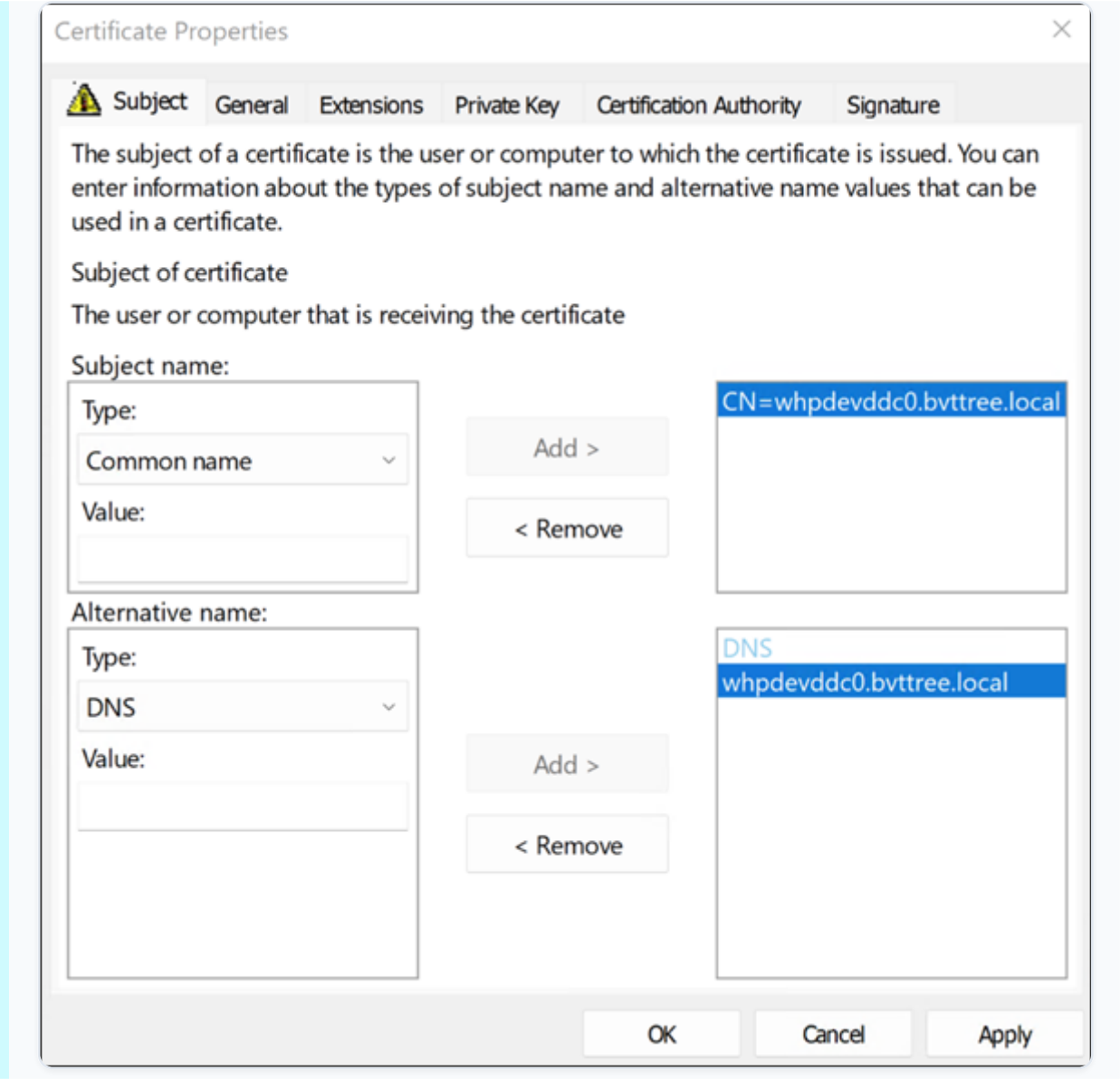


3. **証明書の登録**に移動し、Webサーバーを選択して、警告メッセージをクリックし、必要な情報を入力します。

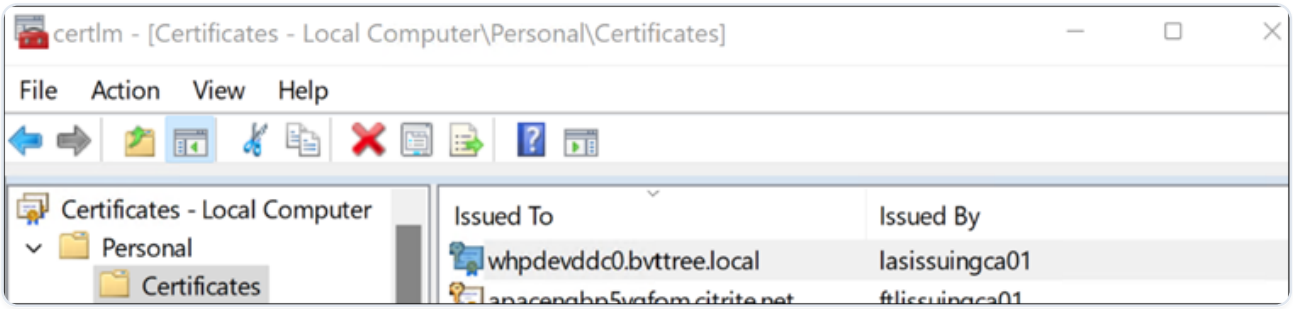


4. サブジェクト名タイプとして**共通名**を選択し、FQDNまたはDNSを入力します。代替名も入力します。

> **注：**
>
> ワイルドカード証明書が必要な場合は、サブジェクト名に`CN=*.bvttree.local`を、代替DNS名に`*.bvttree.local and bvttree.local`を入力できます。



証明書は**個人 > 証明書**の下で利用可能です。

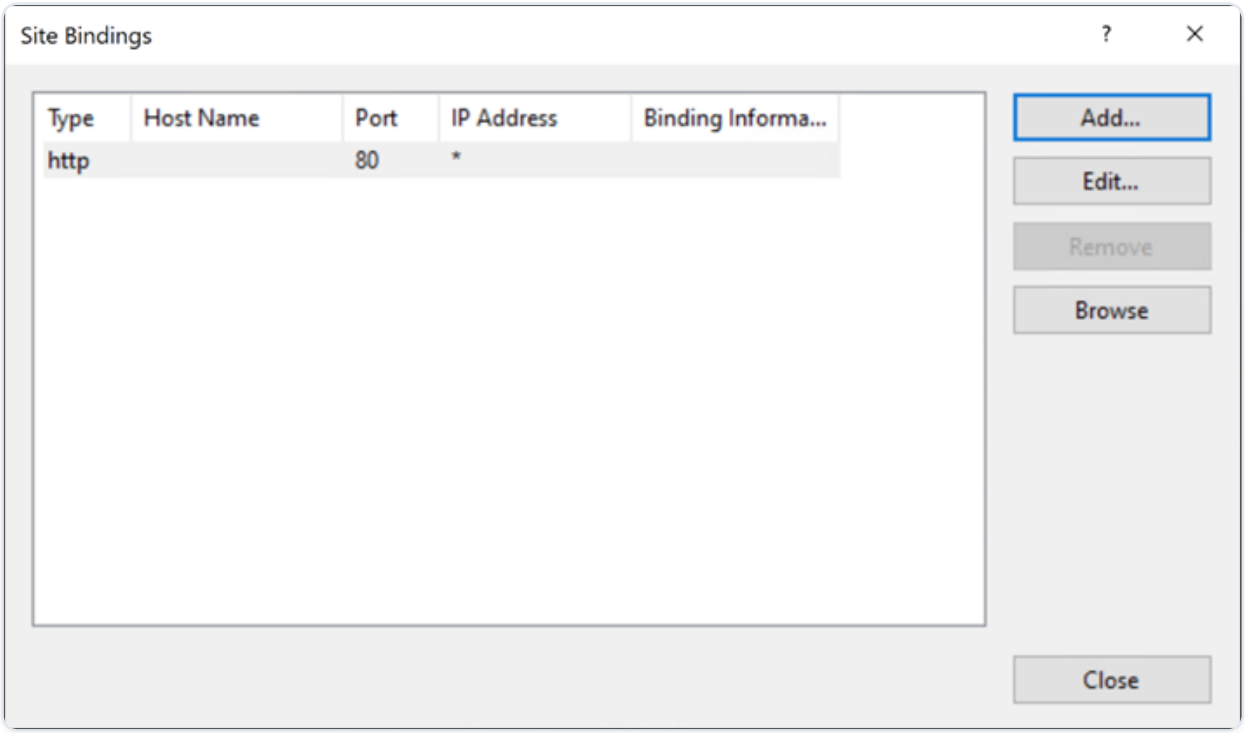


その後、証明書を`443`ポートにバインドします。これは、インストールまたはアップグレードの前、あるいはインストールまたはアップグレードの後に行うことができます。`443`ポートに証明書のバインドが構成されている場合、インストーラーは何も行いません。

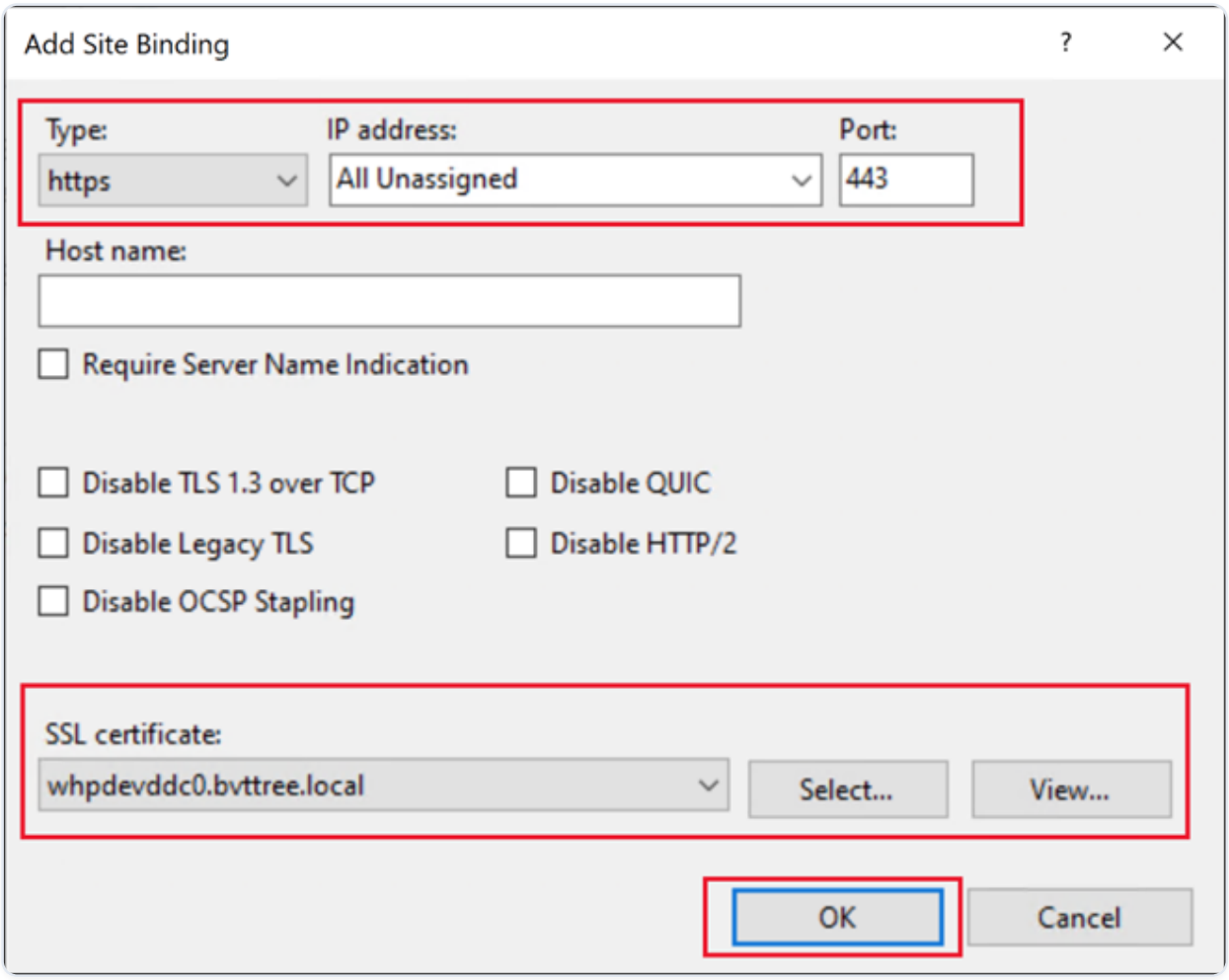
インストールまたはアップグレードの前

証明書を`443`ポートにバインドするには、次の手順を実行します（ただし、`443`に証明書のバインドがまだ構成されておらず、サーバーでIISが有効になっていることが前提です）。

1. 管理者としてWeb Studioサーバーにログオンします。
2. IISマネージャーを開き、**サイト > 既定のWebサイト > バインド**に移動します。
3. **サイトバインド**で、**追加**をクリックします。



4. **サイトバインドの追加**で、種類を`https`に、ポートを443に設定し、CAから要求したSSL証明書を選択して、**OK**をクリックします。



Web Studioをインストールすると、Web StudioとDelivery Controllerは自動的に構成され、証明書を使用して接続を保護します。

または、PowerShellを使用して証明書を変更することもできます。

```
$certSName = 'CN=whpdevddc0.bvttree.local'  # The subject name of the
certificate

$certificate = Get-ChildItem -Path Cert:\LocalMachine\My\ | ? {$_.Subject
-eq $certSName}

netsh http add sslcert ipport=0.0.0.0:443 certhash=$
($certificate.Thumbprint) certstorename=My appid="$($(New-
Guid).ToString("B"))"
```

インストールまたはアップグレード後

Web Studioサーバーに移動し、IISマネージャーを使用して証明書を変更します。 または、PowerShellを使用して証明書を変更することもできます。

```
$certSName = 'CN=whpdevddc0.bvttree.local' # The Enterprise CA certificate
subject.

$certificate = Get-ChildItem -Path Cert:\LocalMachine\My\ | ? {$_.Subject
-eq $certSName}

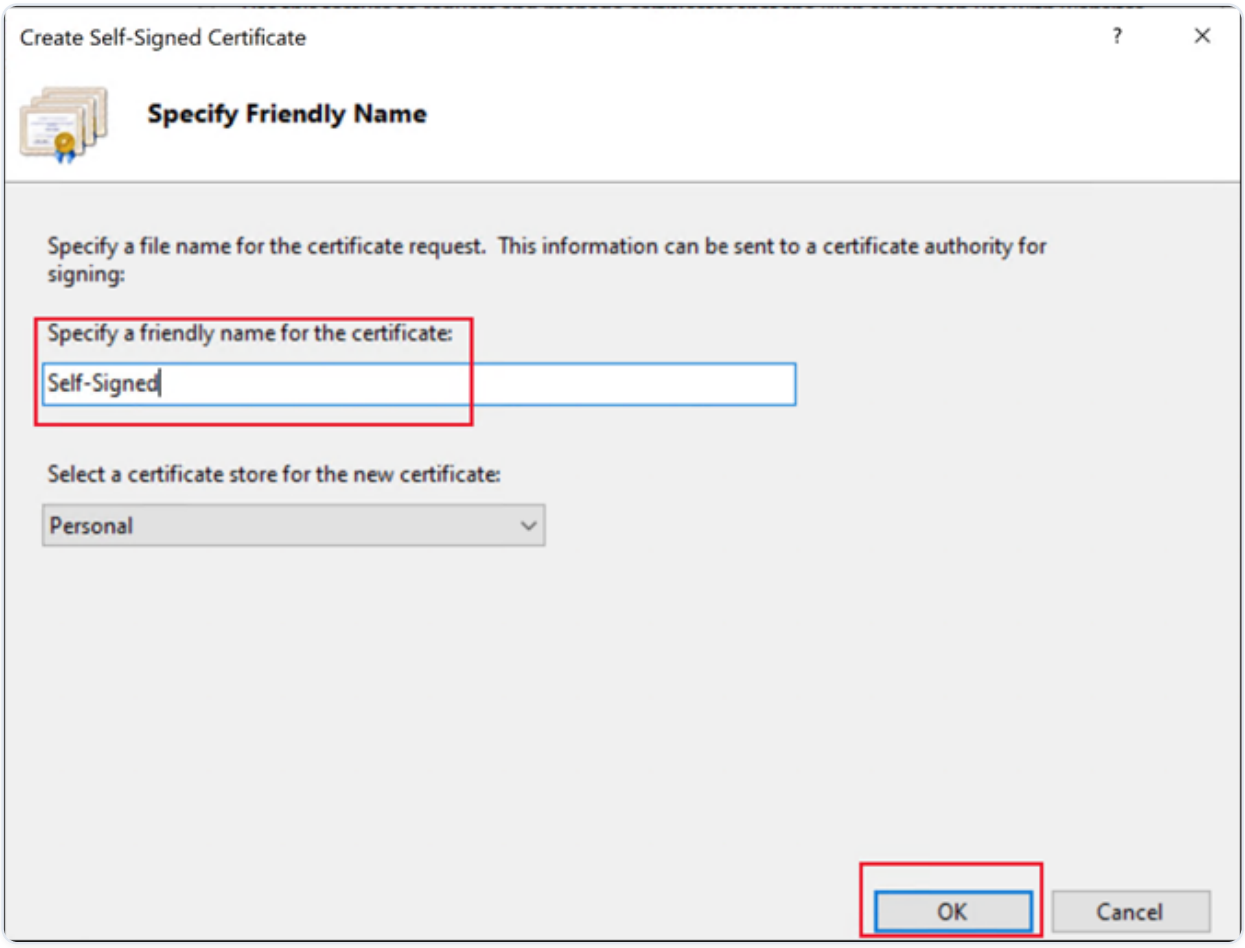
netsh http update sslcert ipport=0.0.0.0:443 certhash=$
($certificate.Thumbprint)
```

新しい自己署名証明書を使用する

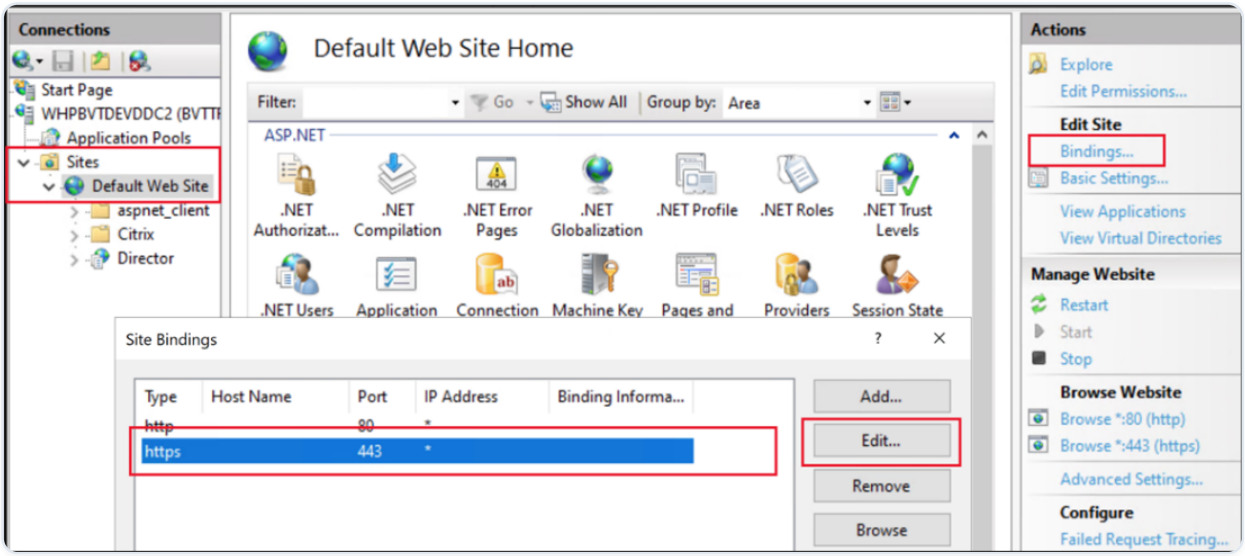
新しい自己署名証明書を生成し、既存の証明書と置き換えることができます。次の手順を実行します。

1. 管理者としてWeb Studioサーバーにログオンします。
2. IISマネージャーを開き、**サーバー証明書**を参照し、**操作**ペインで**自己署名証明書の作成**を選択します。

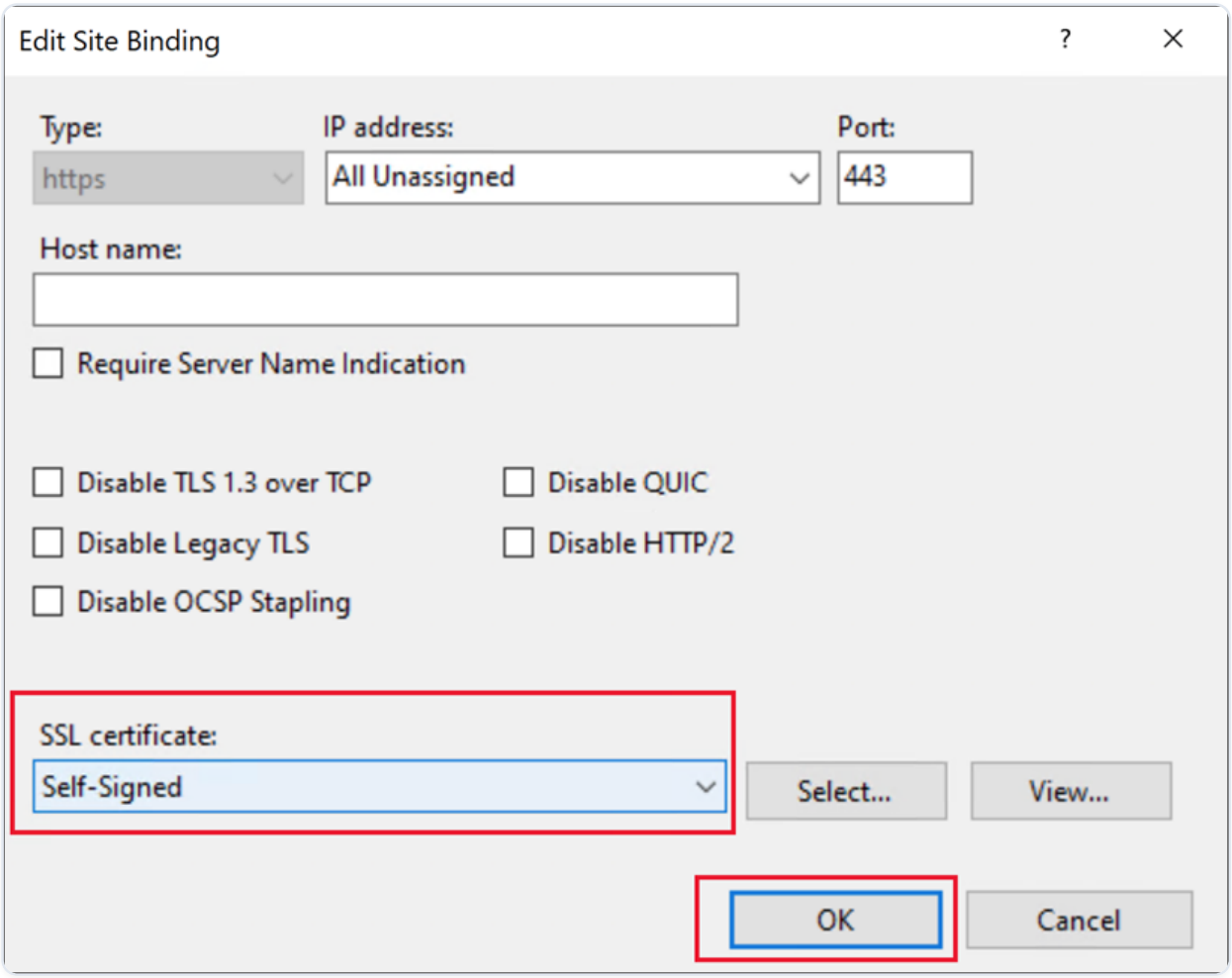
   サーバー証明書(/en-us/citrix-virtual-apps-desktops/2407/media/server-certificates.png)
3. 「**自己署名証明書の作成**」で、証明書の名前を入力し、「**OK**」をクリックします。自己署名証明書が作成されます。



4. **サイト > 既定のWebサイト**を参照し、**操作**ペインで**バインド**を選択し、`https`エントリを選択して、**編集**を選択します。



5. **サイトバインドの編集**で、リストから証明書を選択し、**OK**をクリックします。



これで証明書の変更が完了しました。

または、PowerShellを使用して証明書を変更することもできます。

```
$certSubject = "CN=WHPBVTDEVDDC2.BVTTREE.LOCAL" # The FQDN of the server.

$frindlyName = "Self-Signed-3"

$expireYears = 5



## new self-signed certificate under LocalMachine\My

$certificate = New-SelfSignedCertificate -Subject $certSubject
-CertStoreLocation "Cert:\LocalMachine\My\" -KeyExportPolicy Exportable
-KeySpec Signature -KeyLength 2048 -KeyAlgorithm RSA -HashAlgorithm SHA256
-FriendlyName $frindlyName -NotAfter $
([System.DateTime]::Now.AddYears($expireYears))
```

```
Remove-Item -Path $Env:TEMP\tempCertificate.cer -Force -ErrorAction
SilentlyContinue



## Import this certificate into LocalMachine\Root to let this OS trust
this certificate

Export-Certificate -Type CERT -Force -Cert $certificate -FilePath
$Env:TEMP\tempCertificate.cer -NoClobber

Import-Certificate -FilePath $Env:TEMP\tempCertificate.cer
-CertStoreLocation "Cert:\LocalMachine\Root\"



## Update bind the 0.0.0.0:443 with this certificate

Invoke-Command -ScriptBlock { Param ($param1) netsh http update sslcert
ipport=0.0.0.0:443 certhash=$param1 } -ArgumentList
@($certificate.Thumbprint)
```

Web Studioのスマートカード認証を設定する

この記事では、Web Studioのスマートカード認証を設定および有効にするために必要な手順を説明します。

ステップ1：スマートカードドライバーをインストールする

ステップ2：スマートカードユーザーの証明書を発行する

ステップ3：スマートカードユーザーの証明書を登録する

ステップ4：Web Studio IISサーバーを構成する

ステップ5（オプション）：Web Studioの認証委任を構成する

ステップ6：Web Studioのスマートカード認証を有効にする

> **注：**

> スマートカード認証は、Web Studioサーバーと同じActive Directoryドメインのユーザーに対してのみサポートされます。

ステップ1：スマートカードドライバーをインストールする

以下のマシンにスマートカードドライバーをインストールします。

- 証明書サービスがインストールされているドメインコントローラー。
- Web Studioサーバー
- エンドユーザーがWeb Studioにアクセスするために使用するマシン
- スマートカードユーザーの証明書を登録するために使用するマシン

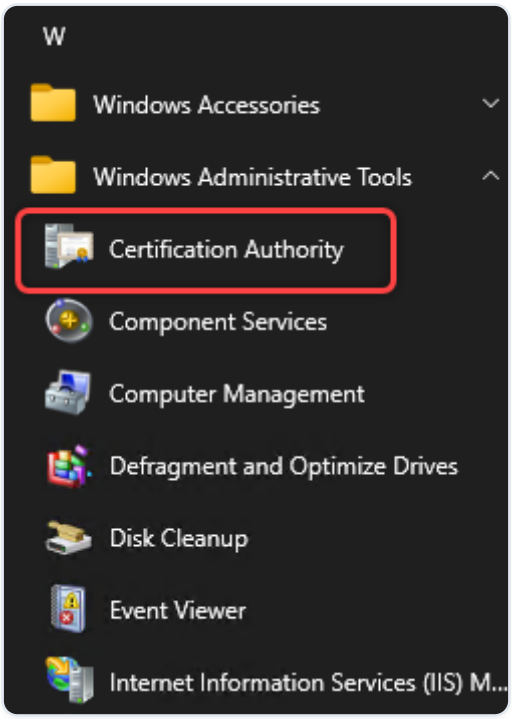
スマートカードドライバーはベンダーによって異なります。たとえば、ITSが提供するスマートカードハードウェアを使用している場合は、SaftNetドライバーを`<https://support.globalsign.com/ssl/ssl-certificates-installation/safenet-drivers>`からダウンロードしてください。

ステップ2：スマートカードユーザーの証明書を発行する

> **注:**
>
> 以下の手順は、プロセスを案内するための例として提供されています。

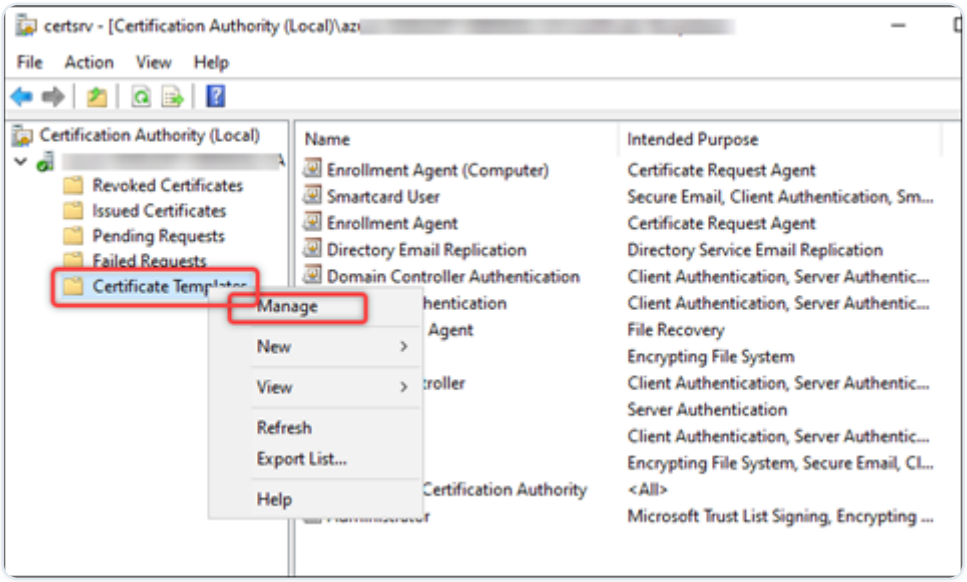
> ドメインコントローラーで、以下の手順に従ってタスクを完了します。

1. ドメインコントローラーにアクセスし、**証明機関**を開きます。



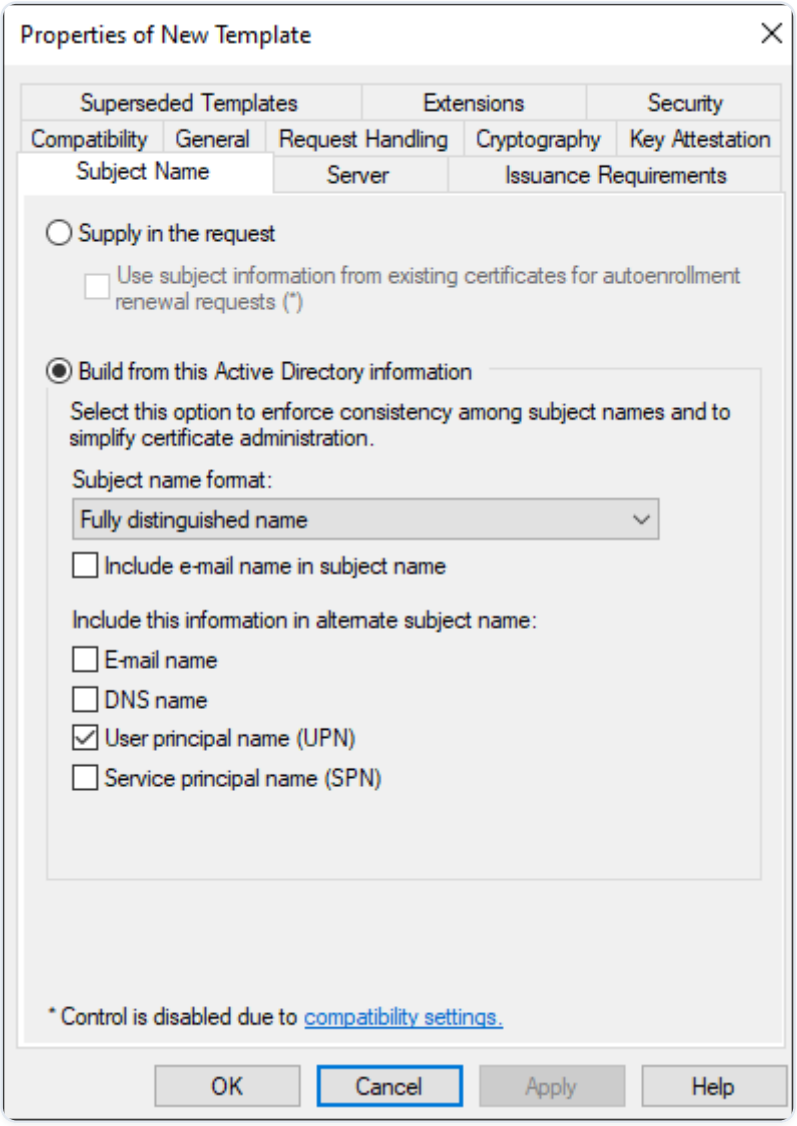
2. **登録エージェント**テンプレートを複製します。詳細な手順は次のとおりです。

   a. **証明書テンプレート**を右クリックし、**管理**を選択します。

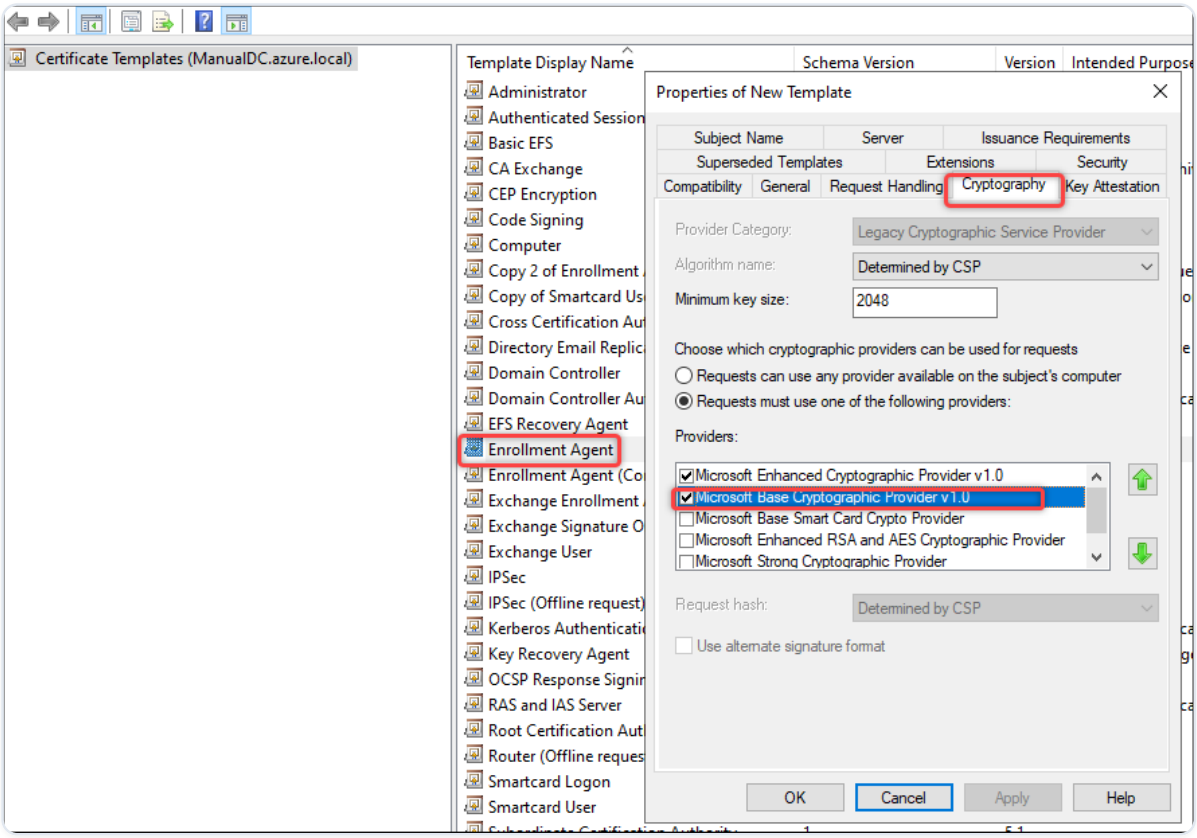


   b. **登録エージェント**を右クリックし、**テンプレートの複製**を選択します。

   c. **サブジェクト名**タブで、**サブジェクト名に電子メールを含める**が選択されていないことを確認します。



d. **暗号化**タブで、**Microsoft Base Smart Card Crypto Provider**を選択し、**OK**をクリックします。**証明書テンプレート**リストに、**登録エージェントのコピー**という名前のテンプレートが表示されます。



3. スマートカードの証明書を発行します。詳細な手順は次のとおりです。

   a. 「**証明書テンプレート**」を右クリックし、「**新規 > 発行するテンプレート**」を選択します。

   b. 「**登録エージェントのコピー**」と「**スマートカードユーザー**」を選択します。

   c. **OK**をクリックします。

ステップ3：スマートカードユーザーの証明書を登録する

> **注:**
>
> 以下の手順は、プロセスをガイドするための例として提供されています。

ドメインに参加している物理Windowsマシンで、各スマートカードの証明書を登録するには、以下の手順に従います。

1. 登録用にドメインに参加している物理Windowsマシンを準備します。

   a. スマートカードドライバーがインストールされていることを確認します。

   b. スマートカードをマシンに挿入します。

c. スマートカードに割り当てるユーザーアカウントを使用してマシンにログオンします。

2. ステップ1で準備したマシンに**証明書**スナップインを追加します。詳細な手順は次のとおりです。

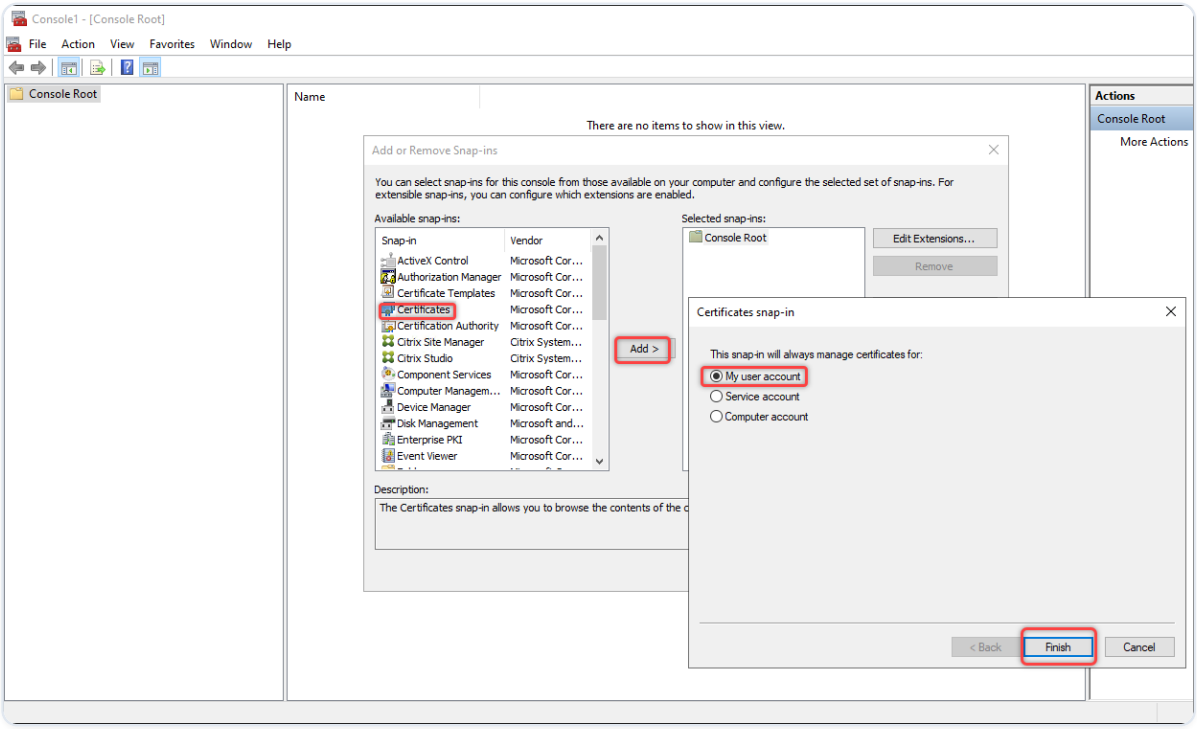
   a. **mmc**を開きます。

   b. 「**ファイル**」をクリックし、次に「**スナップインの追加と削除**」をクリックします。

   c. 表示される「**スナップインの追加と削除**」ウィンドウで、「**証明書**」を選択し、「**追加 >**」をクリックします。

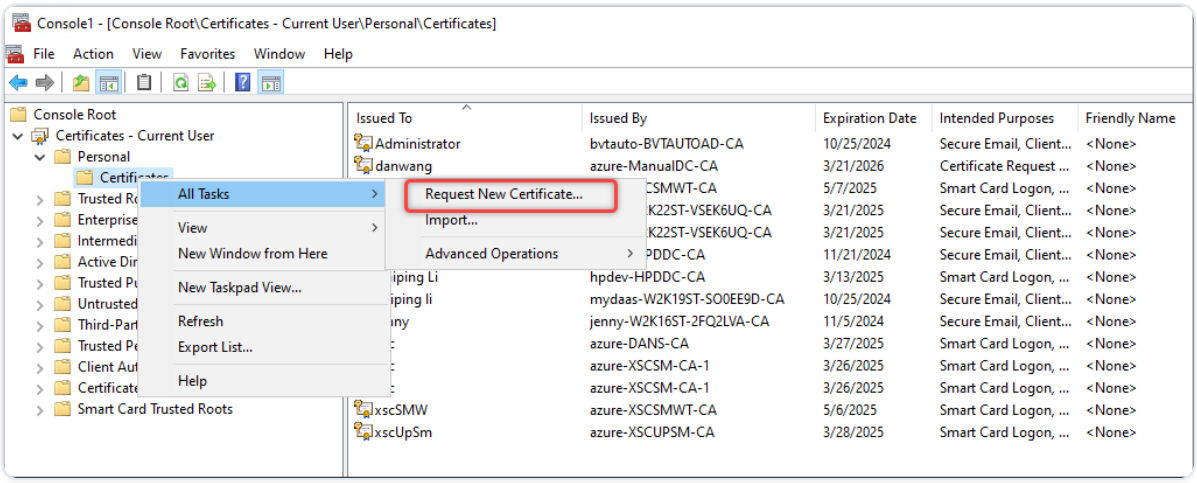
   d. 表示されるダイアログボックスで、「**マイ ユーザー アカウント**」を選択し、「**完了**」をクリックします。

   e. 「**OK**」をクリックします。

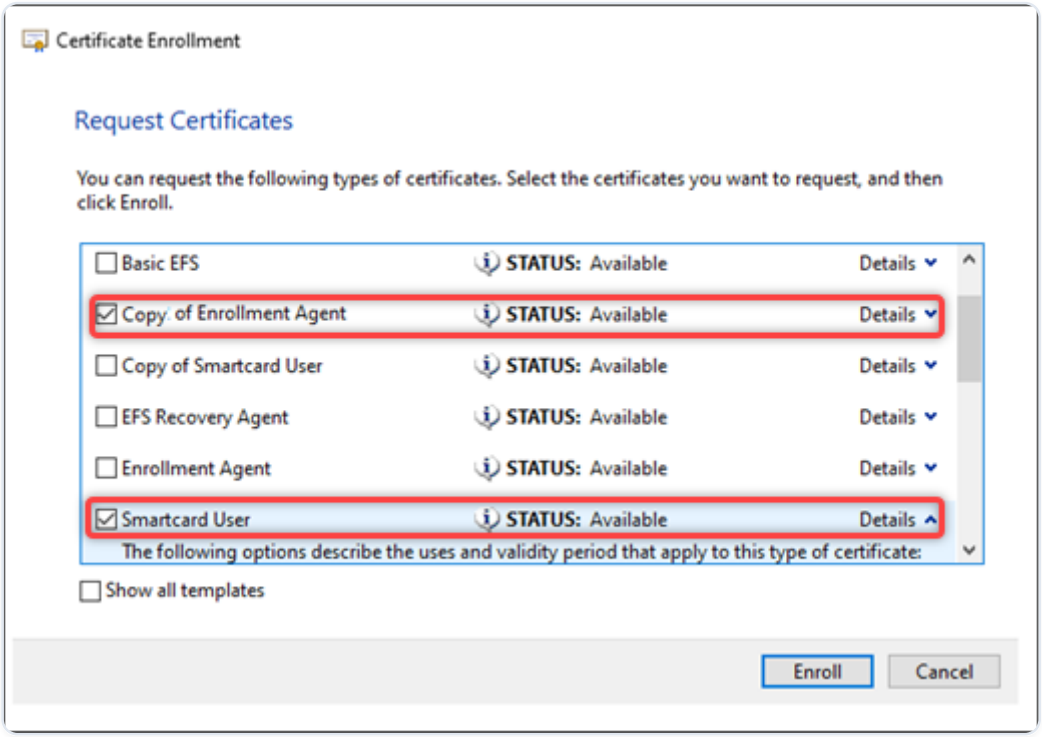


3. 「**証明書**」スナップインの新しい証明書を要求します。詳細な手順は次のとおりです。

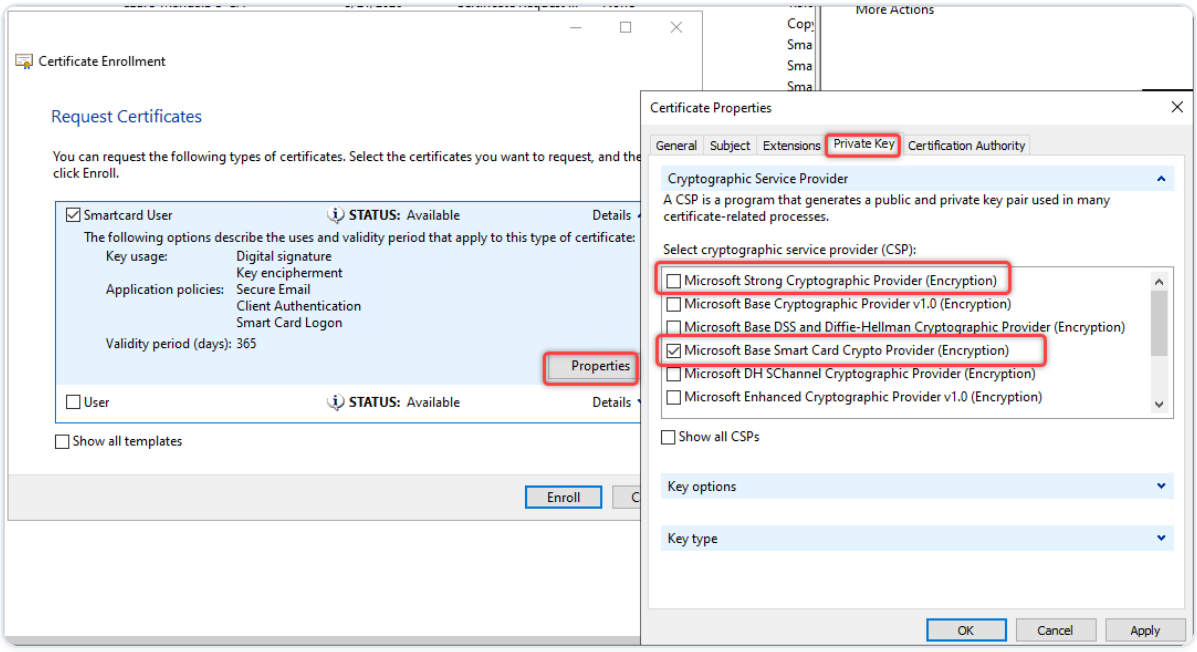
   a. 「**証明書 - 現在のユーザー > 個人**」に移動し、「**証明書**」を右クリックして、「**すべてのタスク > 新しい証明書の要求**」を選択します。



b. 表示される「**証明書の要求**」ダイアログボックスで、「**登録エージェントのコピー**」と「**スマートカード ユーザー**」を選択します。



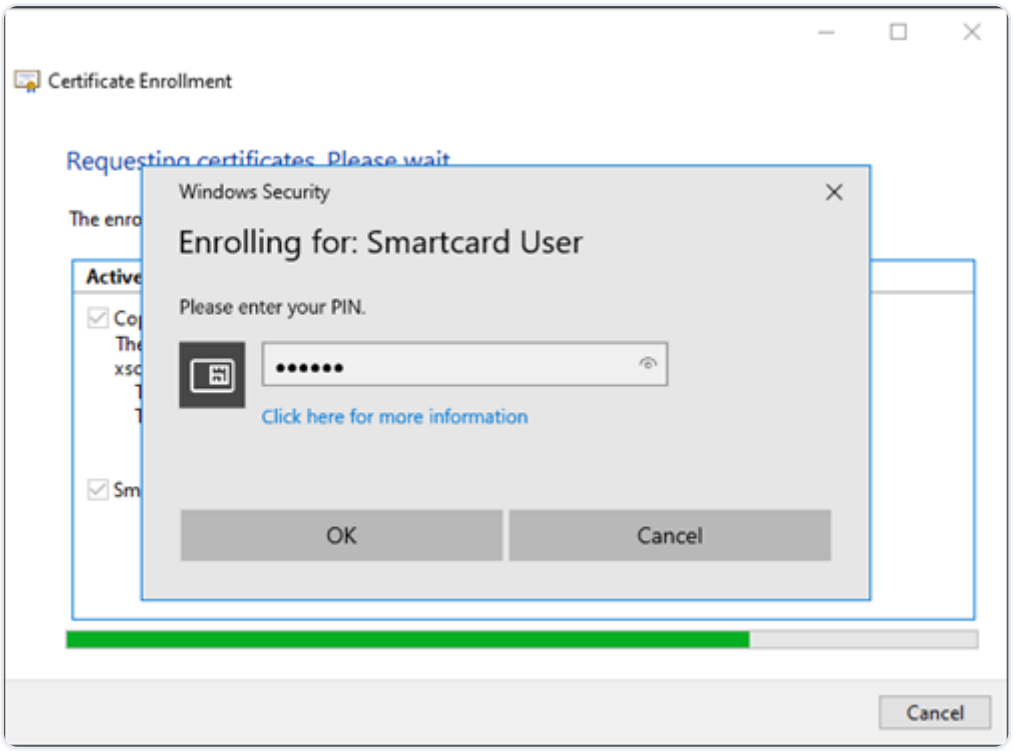
c. 上記のダイアログボックスで、「**スマートカード ユーザー**」の「**詳細**」をクリックし、次に「**プロパティ**」をクリックします。「**証明書のプロパティ**」ダイアログボックスが表示されます。



d. 「**秘密キー**」タブで、「**暗号化サービス プロバイダー**」を展開し、「**Microsoft Strong Cryptographic Provider (暗号化)**」のチェックを外し、「**Microsoft Base Smart Card Crypto Provider (暗号化)**」のみを選択して、「**OK**」をクリックします。

e. 「**登録**」をクリックします。

f. 表示される「**Windows セキュリティ**」ダイアログボックスで、スマートカードのPINコードを入力し、「**OK**」をクリックします。登録が完了したら、「**完了**」をクリックします。



登録が成功すると、次のスクリーンショットに示すように、**証明書 - 現在のユーザー -> 個人 -> 証明書**の下に2つの証明書が表示されます。 「証明書テンプレートの管理」(/en-us/citrix-virtual-apps-desktops/2407/media/add-certificate-result.png)

手順4：Web Studio IISサーバーを構成する

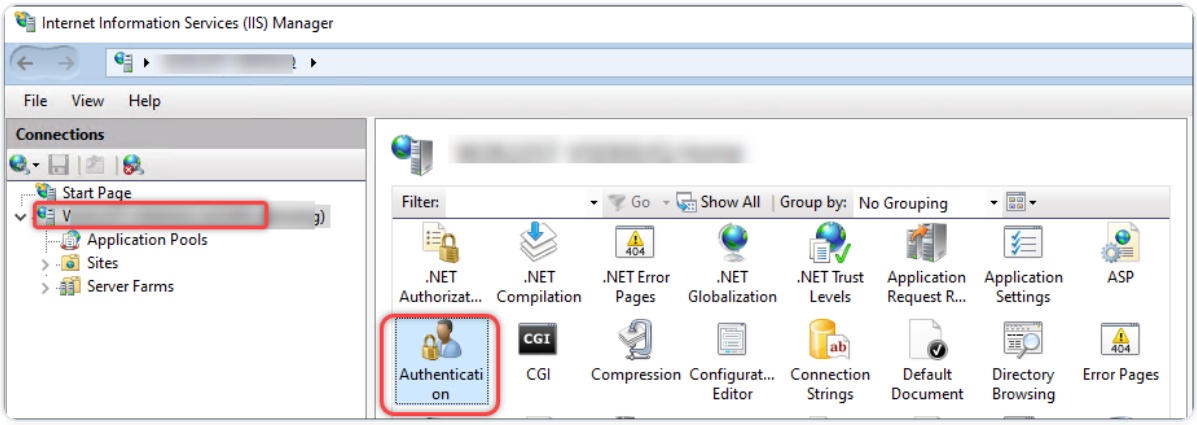
各Web Studioサーバーで、スマートカード認証用にIISを構成するには、次の手順に従います。

1. Web Studioマシンで**クライアント証明書マッピング認証**を有効にします**。

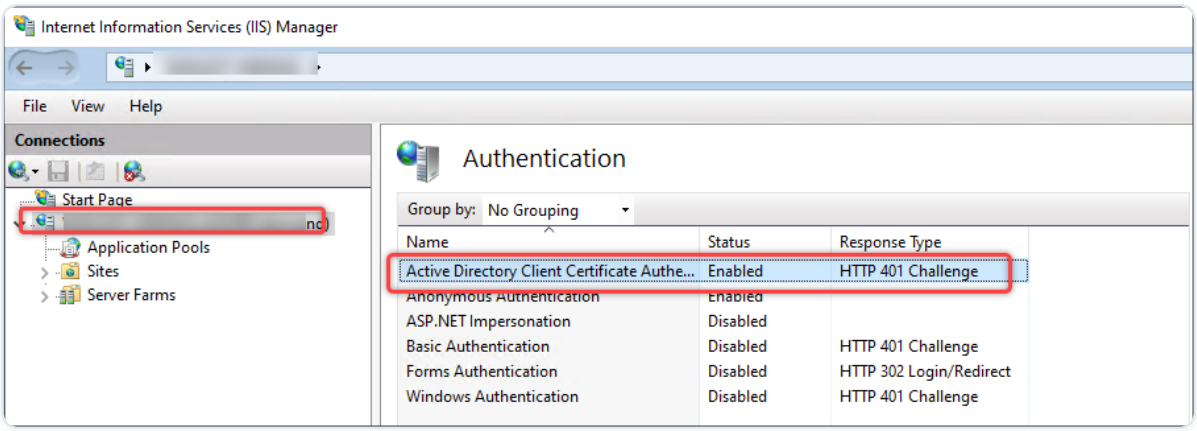
   `<clientCertificateMappingAuthentication>`要素は、IIS 7以降のデフォルトインストールでは利用できません。インストールと有効化の詳細については、このMicrosoftの記事を参照してください。

2. Web Studioマシンで**IISマネージャー**を起動します。
3. マシンで**Active Directoryクライアント証明書認証**を有効にします。詳細な手順は次のとおりです。

   a. 左ペインでマシンを選択し、「**認証**」をダブルクリックします。

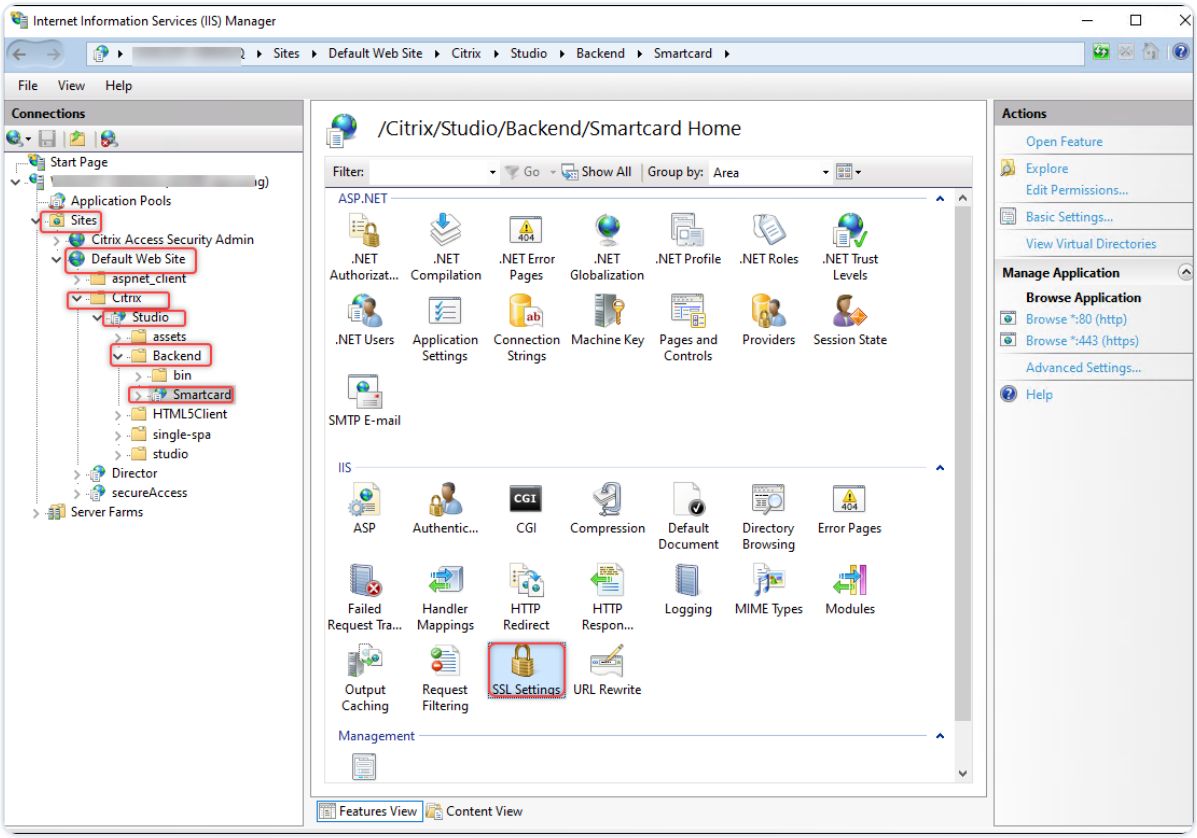


   b. 「**Active Directory クライアント証明書認証**」を有効にします。



4. クライアント証明書認証を使用して、より安全なHTTPSプロトコルのWeb Studioバックエンドモジュールを構成します。

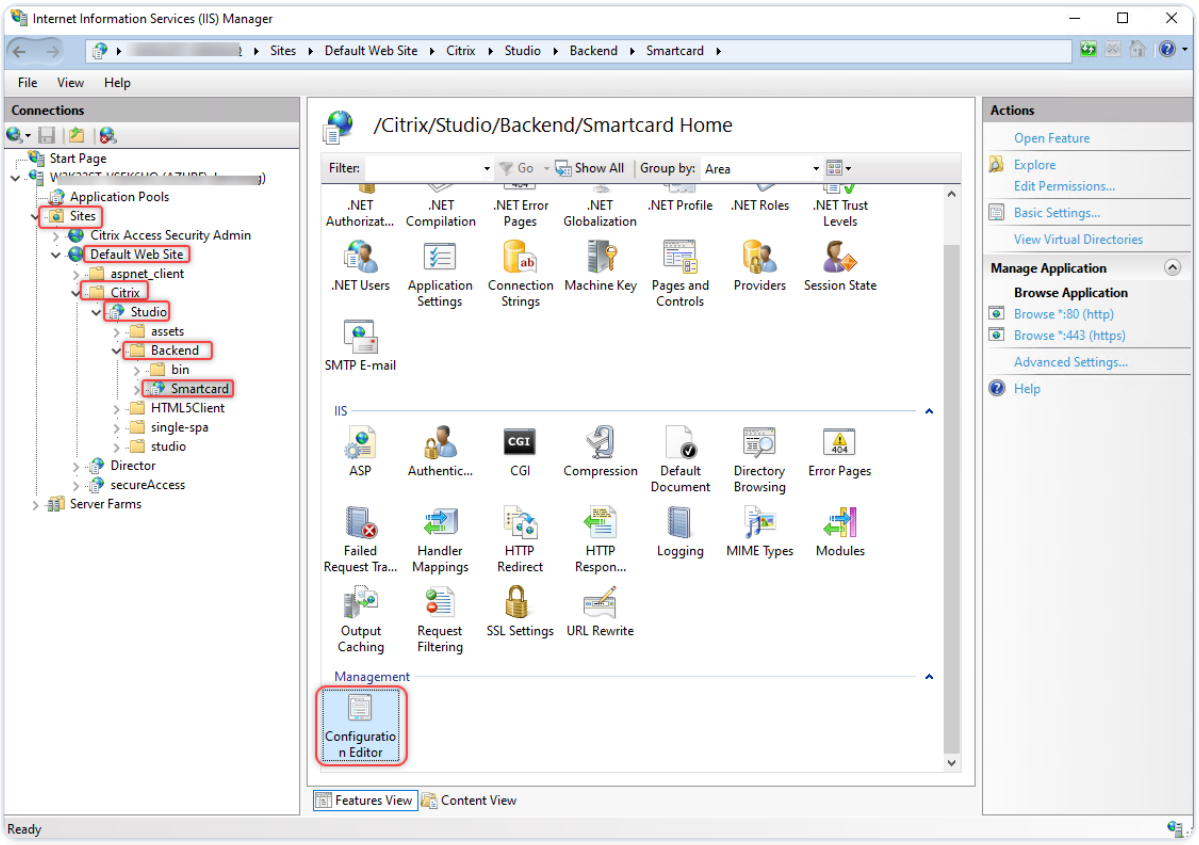
   a. **サイト > 既定のWebサイト > Studio > バックエンド > スマートカード**に移動し、**IIS**セクションで「**SSL設定**」をダブルクリックします。



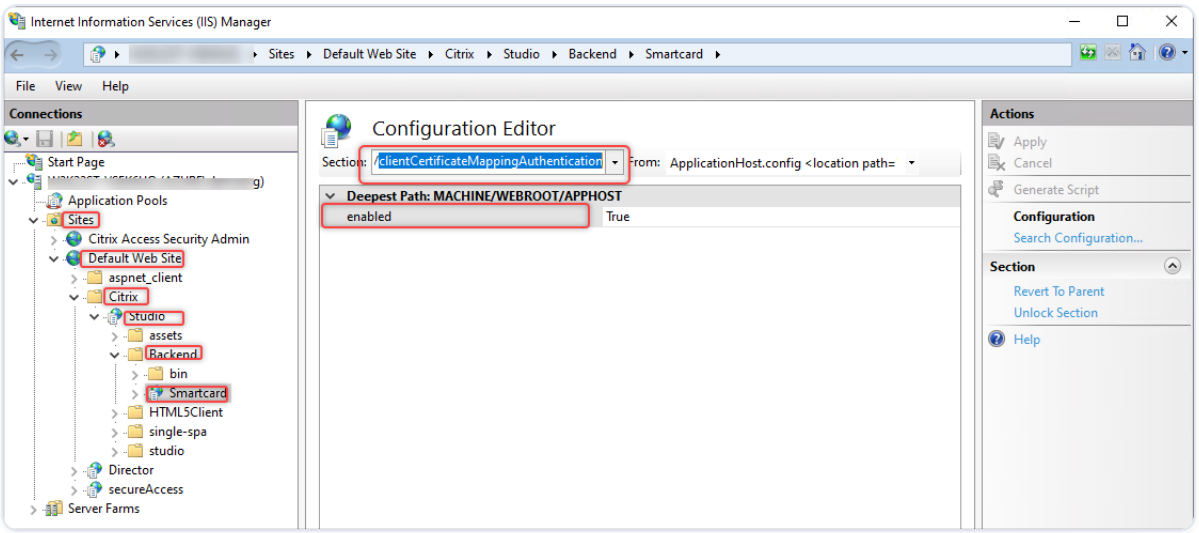
   b. 「**クライアント証明書**」に対して「**必須**」を選択します。

      IISサーバーバックエンド スマートカード SSL必須(/en-us/citrix-virtual-apps-desktops/2407/media/iis-server-backend-smartcard-ssl-required.png)

   c. 「**サイト > 既定のWebサイト > Studio > バックエンド > スマートカード**」に戻り、「**IIS**」セクションの「**構成エディター**」をダブルクリックします。



d. 「**/clientCertificateMappingAuthentication**」が「**有効**」になっていることを確認してください。



5. (Windows 2022のみ) TCP経由のTLS 1.3を無効にします。詳細な手順は次のとおりです。

   a. 「**サイト > 既定のWebサイト**」に移動します。

   b. 「**サイトの編集 > バインド**」をクリックします。

   c. 表示される「**サイトバインド**」ダイアログボックスで、「**https**」レコードを選択し、「**編集**」をクリックします。

Windows 2022 のみ https 編集(/en-us/citrix-virtual-apps-desktops/2407/media/iis-server-default-site-https-edit.png)

d. 表示される「**サイトバインドの編集**」ダイアログボックスで、「**TCP経由のTLS 1.3を無効にする**」を選択し、「**OK**」をクリックします。

Windows 2022のみ https編集 無効(/en-us/citrix-virtual-apps-desktops/2407/media/iis-server-default-site-https-edit-disable.png)

知っておくと良いこと:

Web StudioバックエンドはWeb Studioのモジュールであり、以下の機能を提供します。

- スマートカード認証。
- 統合Windows認証を使用したOrchestrationサービスからのFMAベアラートークンの取得。

手順 5 (オプション) Web Studio の認証委任を構成する

Web StudioとDelivery Controllerが異なるサーバーにインストールされている場合、各Web StudioサーバーからDelivery ControllerへのHOSTおよびHTTPSサービスの委任を構成する必要があります。

各 Web Studio サーバーでタスクを完了するには、次の手順に従います。

1. Delivery Controller™ オーケストレーション HTTPS 証明書をインポートする
2. Web Studio サーバーの委任を構成する
3. （オプション）Web Studio IIS サーバーのサービスアカウントの委任を構成する

Delivery Controller Orchestration HTTPS証明書のインポート

Web Studioサーバーで、**Delivery Controller Orchestration HTTPS**証明書を**信頼されたルート証明機関**にインポートします。詳細な手順は次のとおりです。

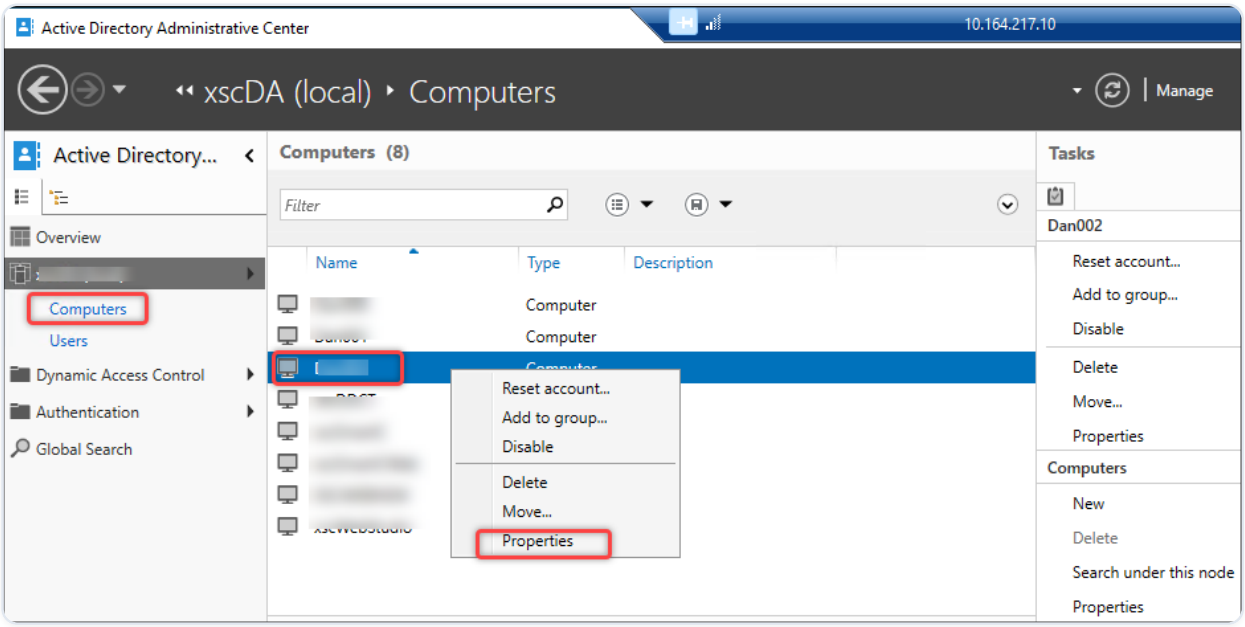
1. **設定 > コンピューター証明書の管理**を開始します。
2. **信頼されたルート証明機関 > 証明書**を右クリックし、**すべてのタスク > インポート**を選択します。

   DDC証明書のインポート(/en-us/citrix-virtual-apps-desktops/2407/media/web-server-ddc-cert-import.png)
3. 画面の指示に従って、**Delivery Controller Orchestration HTTPS**証明書をインポートします。

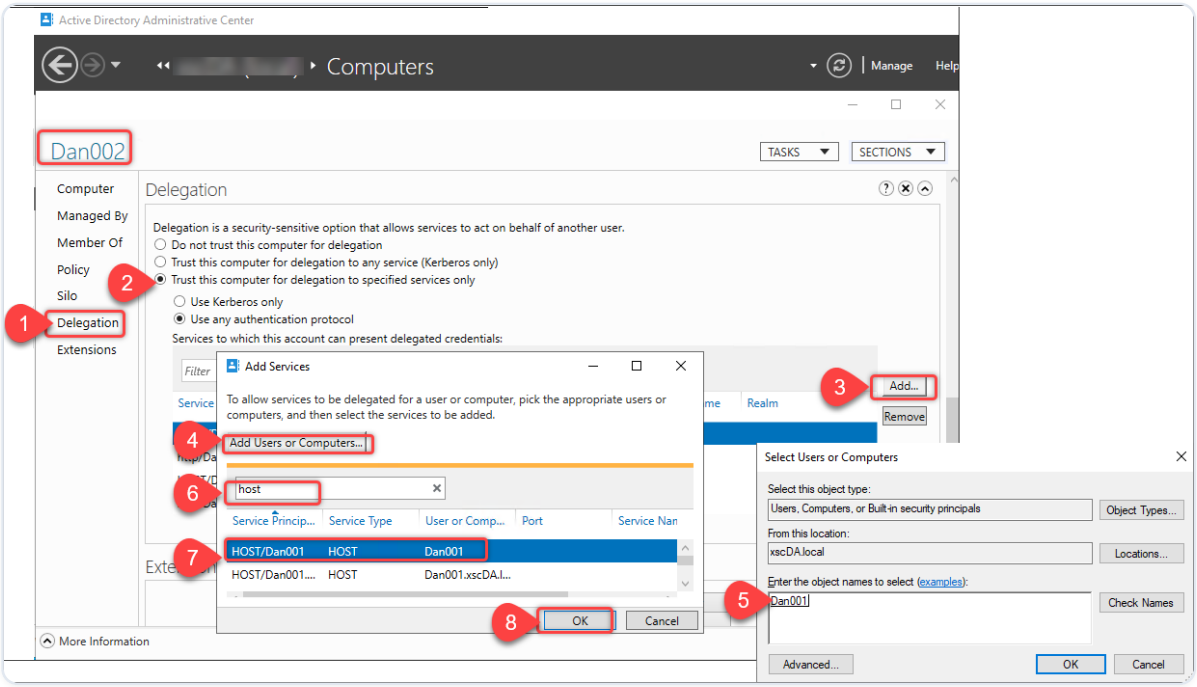
Web Studioサーバーの委任を構成する

ドメインコントローラーで、Web StudioサーバーからDelivery ControllerへのHOSTおよびHTTPサービスの委任を構成します。このタスクを完了するには、次の手順に従います。

1. ドメインコントローラーで、**Active Directory管理センター**を起動します。
2. 委任を構成するWeb Studioサーバーの**コンピューター**アカウントを見つけます（*例：Dan002*）。
3. アカウントを右クリックし、**プロパティ**を選択して、次の手順を完了します。



a. **委任**タブに移動します。



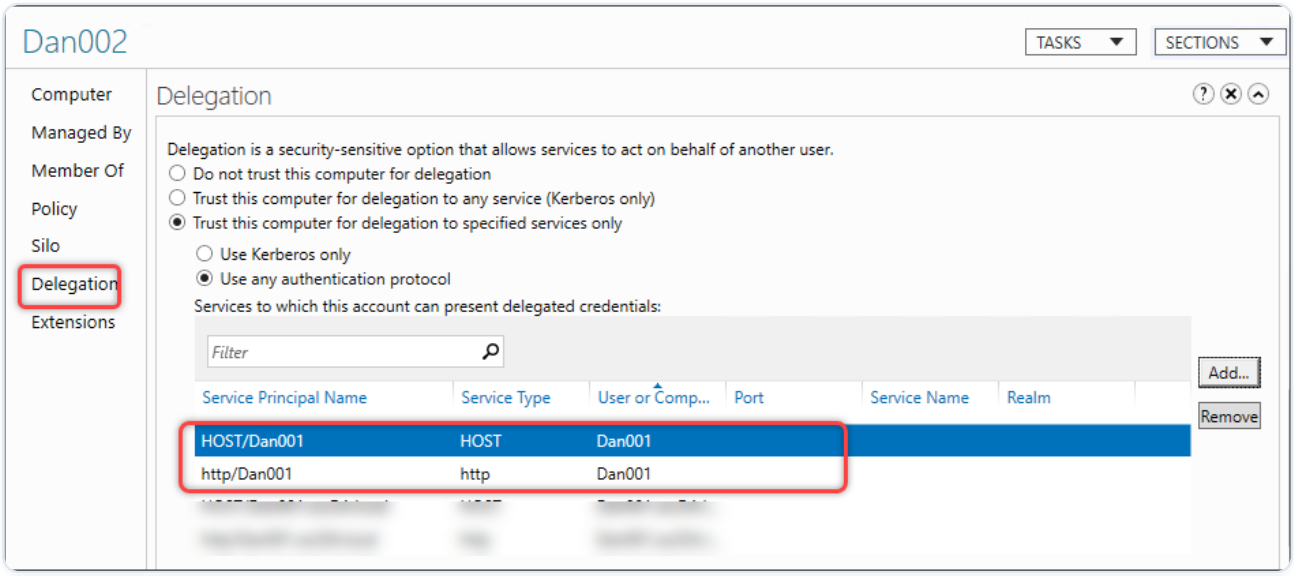
b. **指定されたサービスへの委任でのみ、このユーザーを信頼する > 任意の認証プロトコルを使用する**を選択します。

c. **追加**をクリックして、このコンピューターアカウントを委任できるサービスを指定します。

d. 表示される**サービスの追加**ダイアログボックスで、**ユーザーまたはコンピューターの追加**をクリックして、Delivery Controllerのコンピューター名を見つけます（*例：Dan001*）。

e. **HOST**および**HTTP**サービスを選択し、**OK**をクリックします。

構成結果を次のスクリーンショットに示します。

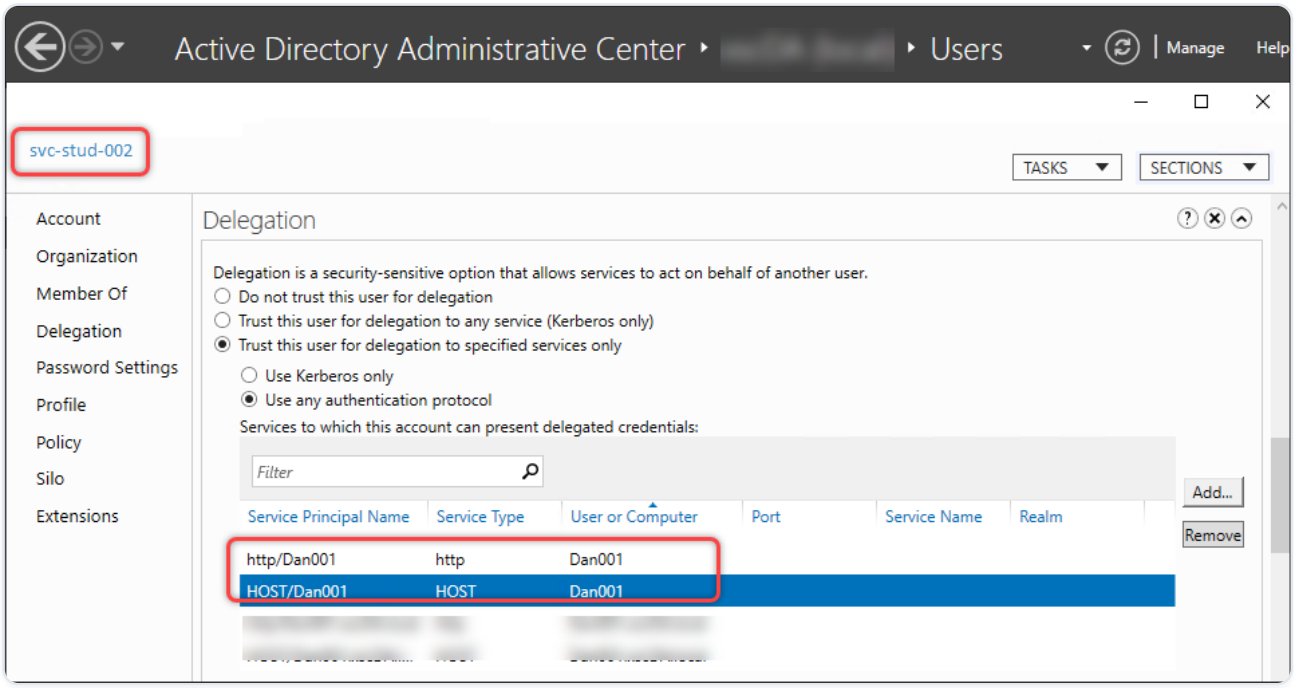


（オプション）Web Studio IIS サーバーのサービスアカウントの委任を構成する

Web Studio IISサーバーにサービスアカウントを構成している場合、このサービスアカウントからDelivery ControllerへのHOSTおよびHTTPサービスの委任も構成する必要があります。この委任が確立されると、Web Studioサーバーは、そのサービスアカウントを使用して、現在のスマートカードユーザーを偽装し、HOSTおよびHTTPサービスのためにDelivery Controllerにアクセスできます。構成を完了するには、次の手順に従います。

1. ドメインコントローラーで、**Active Directory管理センター**を起動します。
2. 委任を構成するWeb Studio IISサーバー（サービスアカウント）の**ユーザー**アカウントを見つけます（*例：svr-stud-002*）。
3. アカウントを右クリックし、**プロパティ**を選択します。
4. Web Studioサーバーの委任を構成するのステップ3で説明されている手順に従って、HOSTサービスとHTTPサービスのために、Web Studio IISサーバーのサービスアカウントを Delivery Controllerに委任します。

構成結果は次のスクリーンショットに示されています。



手順 6：Web Studio のスマートカード認証を有効にする

次の手順に従って、Web Studioのスマートカード認証を有効にします。

1. **Web Studio**にサインインし、左側のペインで**設定**を選択します。
2. 必要に応じて、**スマートカード認証**または**ドメイン資格情報またはスマートカード認証**を選択します。
3. **適用**をクリックします。

   証明書テンプレートの管理(/en-us/citrix-virtual-apps-desktops/2407/media/enable-stud-settings.png)

Ansible を使用した VDA のインストール

概要

この記事では、Ansible を使用して VDA を展開する方法について説明します。詳細については、Ansible ドキュメントを参照してください。

> **注:**
>
> この記事では、Citrix® が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、お客様のニーズに合わせてカスタマイズできます。Citrix は、お客様のニーズに合わせて必要な更新や調整について責任を負いません。

Ansible を使用して VDA を展開するための主要な手順

1. 仮想マシン環境を構成する。
2. Ansible をインストールする
3. Kerberos の構成
   a. Kerberos をインストールする
   b. Kerberos を構成する
4. Ansible を構成する

ステップ 1: 仮想マシン環境を構成する

Windows サーバーで次のコマンドを実行します。

1. PS RemoteSigned を設定します。 `Set-ExecutionPolicy RemoteSigned`
2. WinRM を暗号化なしで使用するように設定します。 `winrm set winrm/config/service '@{AllowUnencrypted="true"}'`

   > **注:**
   >
   > このステップでエラーが発生した場合は、次のコマンドを使用します。 `Enable-PSRemoting -Force`

3. ファイアウォールポート5985を開きます。 `New-NetFirewallRule -DisplayName "Allow WinRm port 5985" -Direction Inbound -Profile Any -Action Allow -LocalPort 5985 -Protocol tcp`

ステップ2：Ansibleのインストール

Ubuntu 20.4以降でAnsibleをインストールするには、次のコマンドを実行します。

- `sudo apt update`
- `sudo apt install software-properties-common`
- `sudo add-apt-repository --yes --update ppa:ansible/ansible`
- `sudo apt install ansible`
- `sudo apt install python3-pip`

ステップ2i：Kerberosのインストール

Kerberosをインストールするには、次のコマンドを実行します。

```
sudo apt install python3-dev libkrb5-dev krb5-user
```

ステップ2ii：Kerberosの構成

Kerberosを構成するには、次のコマンドを実行します。

```
Edit /etc/krb5.conf
```

```
[libdefaults]
        default_realm = [redacted]

# The following krb5.conf variables are only for MIT Kerberos.
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true

# The following encryption type specification will be used by MIT Kerberos
# if uncommented.  In general, the defaults in the MIT Kerberos code are
# correct and overriding these specifications only serves to disable new
# encryption types as they are added, creating interoperability problems.
#
# The only time when you might need to uncomment these lines and change
# the enctypes is if you have local software that will break on ticket
# caches containing ticket encryption types it doesn't know about (such as
# old versions of Sun Java).

#       default_tgs_enctypes = des3-hmac-sha1
#       default_tkt_enctypes = des3-hmac-sha1
#       permitted_enctypes = des3-hmac-sha1

# The following libdefaults parameters are only for Heimdal Kerberos.
        fcc-mit-ticketflags = true

[realms]
        LTSRLAB.NET = {
                kdc = [redacted]
                admin_server = [redacted]
        }
        ATHENA.MIT.EDU = {
                kdc = [redacted]
```

> **注:**
>
> Kerberos レルム名には大文字を使用します。

```
[domain_realm]
        .mit.edu = ATHENA.MIT.EDU
        mit.edu = ATHENA.MIT.EDU
        .media.mit.edu = MEDIA-LAB.MIT.EDU
        media.mit.edu = MEDIA-LAB.MIT.EDU
        .csail.mit.edu = CSAIL.MIT.EDU
        csail.mit.edu = CSAIL.MIT.EDU
        .whoi.edu = ATHENA.MIT.EDU
        whoi.edu = ATHENA.MIT.EDU
        .stanford.edu = stanford.edu
        .slac.stanford.edu = SLAC.STANFORD.EDU
        .toronto.edu = UTORONTO.CA
        .utoronto.ca = UTORONTO.CA
```

ステップ3：Ansibleの構成

Ansibleホストを構成するには、次の手順を実行します。

1. 次のコマンドを実行します。

   `Edit /etc/ansible/hosts`

2. Delivery Controller `Install.yaml` ファイルを構成します

   `/QUIET /NOREBOOT /NORESUME /OPTIMIZE /VERBOSELOG /COMPONENTS VDA /CONTROLLERS 'MyDDC.xd.local' /ENABLE_HDX_PORTS /ENABLE_REAL_TIME_TRANSPORT`

```
- name: Install multi-session VDA using network share path
  hosts: TSVDA

  tasks:

  - name: mount a cvad iso
    community.windows.win_disk_image:
      image_path: \\              \Ansible\Citrix_Virtual_Apps_and_Desktops_7_1912_9000.iso
      state: present
    become: true
    become_method: runas
    become_flags: logon_type=new_credentials logon_flags=netcredentials_only
    vars:
      ansible_become_user:
      ansible_become_password:
    register: disk_image_out

  - name: copy iso file to c drive temp folder
    ansible.windows.win_copy:
      src: "{{disk_image_out.mount_paths[0]}}"
      dest: C:\Temp\
      remote_src: yes

  - name: unmount iso
    community.windows.win_disk_image:
      image_path: \\              \Ansible\Citrix_Virtual_Apps_and_Desktops_7_1912_9000.iso
      state: absent
    become: true
    become_method: runas
    become_flags: logon_type=new_credentials logon_flags=netcredentials_only
    vars:
      ansible_become_user:
      ansible_become_password:
-- INSERT --                                                                    26,83         Top
```

```
- name: unmount iso
  community.windows.win_disk_image:
    image_path: \\                \Ansible\Citrix_Virtual_Apps_and_Desktops_7_1912_9000.iso
    state: absent
  become: true
  become_method: runas
  become_flags: logon_type=new_credentials logon_flags=netcredentials_only
  vars:
    ansible_become_user:
    ansible_become_password:

- name: stop windows upgrade service
  ansible.windows.win_service:
    name: wuauserv
    start_mode: disabled
    state: stopped

- name: Restart server before install
  ansible.windows.win_reboot:

- name: Install vda from exe
  win_package:
    path: C:\Temp\X64\Xendesktop Setup\XendesktopVdaSetup.exe
    arguments: /quiet /verboselog /PORTNUMBER    /logpath 'C:\CitrixInstallationLogs\TSVDA' /components "VDA,PLUGINS"  /CONT
ROLLERS '                    '  /ENABLE_HDX_PORTS /ENABLE_REAL_TIME_TRANSPORT /NOREBOOT /NORESUME
    expected_return_code: [0, 3,3010]
  register: install_vda

- name: debug 1
  debug:
    msg: "{{install_vda}}"

- name: Restart server
```

```
    register: install_vda

- name: debug 1
  debug:
    msg: "{{install_vda}}"

- name: Restart server
  win_reboot:
  when: install_vda.changed

- name: Resume VDA install
  win_package:
    path: C:\Temp\X64\Xendesktop Setup\XendesktopVdaSetup.exe
    expected_return_code: [0,3,3010]
  when: install_vda.changed
  register: vda_resume

- name: debug 2
  debug:
    msg: "{{vda_resume}}"

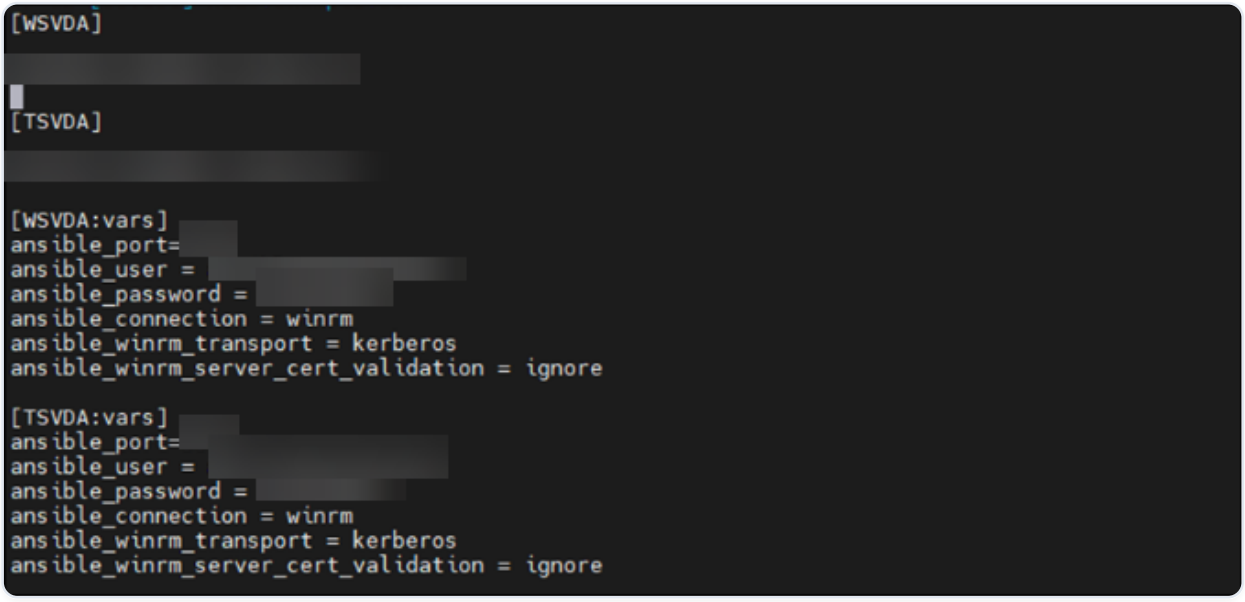
- name: Restart server after VDA install
  win_reboot:
  when: vda_resume.changed

- name: find files
  win_find:
    paths: C:\ProgramData\Citrix\XendesktopSetup\XendesktopVdaSetup.exe
  register: vda_install_find
```

「デリバリーコントローラー」(/en-us/citrix-virtual-apps-desktops/2407/media/delivery-controller-yaml-4.png)

3. 以下のコマンドでyamlファイルを実行します。 `sudo ansible-playbook install.yml -vvv` (詳細モード)
4. 設定ファイルで、他の追加設定とともに複数のホストを構成できます。

`Edit /etc/ansible/hosts`



Call Home の主要データポイント

Call Home は次の主要データポイントを収集します。

(M) = 手動収集時のみ取得 (PowerShell コマンドレット `Start-CitrixCallHomeUpload`)

ファイル名	カテゴリ	データグループ
		マシン
		エックスディーサイト
		サイト情報
		ブローカー DB 情報 (M)
		インストールされている DB バージョン (M)
		ブローカーサービスステータス (M)
		登録済みサービスインスタンス (M)

		ブローカーライセンステスト (M)
		アクティブなHDX™セッション (M)
		ブローカー管理者
		ブローカー管理者権限
		RDS構成 (LicensingSettings、SessionSettings、SpecifiedLicenseServers、およびRegisteredLicenseServersを含む)
		監視サービス (M) (MonitorConfiguration、MonitorDataStore、MonitorDBConnection、MonitorDBSchemaVersion、MonitorService、MonitorServiceAddedCapability、MonitorServiceInstance、MonitorServiceStatus、およびMonitorInstalledDBVersionを含む)
		構成ログ
		接続ログ
		ハイパーバイザー接続 (M)
		ブローカーハイパーバイザー接続
		ハイパーバイザーアラート
		カタログ

		マルチセッションOSエージェント (M)
		シングルセッションOSエージェント (M)
		公開アプリケーション
		デリバリー グループ
		構成済みデリバリーエージェント

		Citrixインストール済みコンポーネント
		Citrix Brokerサービス情報
		ブローカーサービス構成ファイル
		Machine Creation Services™ 構成ファイル
		ホストサービス構成ファイル
		AD IDサービス構成ファイル
		構成サービス構成ファイル
		構成ログサービス構成ファイル
		委任管理サービス構成ファイル
		環境テストサービス構成ファイル
		監視サービス構成ファイル
		Storefront™ サービス構成ファイル

		ワークステーションエージェント構成ファイル
		Citrix VDA情報
		Citrix XD ホットフィックス
		Citrix_VirtualChannel_Graphics_Enum
		Citrix_VirtualChannel_Flash_Enum
		Citrix_VirtualChannel_Printer_Enum

		コンピューター
		BIOS
		メモリ情報
		プロセッサ
		PNP デバイス
		デバイス
		ディスクドライブ
		論理ドライブ
		ページファイル使用量
		ネットワークアダプター
		ネットワークアダプター構成
		ipConfig
		ビデオコントローラー
		IDE コントローラー

		SCSI コントローラー

		HKLM:\Software\Wow6432Node\Citrix
		HKLM:\System\CurrentControlSet\Control\Citrix
		HKLM:\SOFTWARE\Policies\Citrix
		HKLM:\Software\Microsoft\Cryptography
		HKLM:\Software\Wow6432Node\Microsoft\Cryptography
		HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Windows
		HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
		HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
		HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer
		HKLM:\SYSTEM\CurrentControlSet\Control\Print\Environments

		HKLM:\System\CurrentControlSet\Control\セッションマネージャー
		HKLM:\System\CurrentControlSet\Control\ターミナルサーバー
		HKCU:\Control Panel\Desktop
		HKLM:\SOFTWARE\Classes\ShockwaveFlash.ShockwaveFlash\CurVer
		HKLM:\SYSTEM\CurrentControlSet\Control\SystemInformation
		HKLM:\SYSTEM\CurrentControlSet\Control\FileSystem
		HKLM:\SYSTEM\CurrentControlSet\Control\Windows
		HKLM:\SYSTEM\CurrentControlSet\Control\TimeZoneInformation

		ドライバー
		EnvVariables
		OS
		プロセス
		サービス

		サービスパック
		GPResult (ジーピーリザルト)
		マイクロソフト ホットフィックス
		Netstat (ネットスタット)
		PNP ドライバー

		システムイベントログ
		AOT (常時トレース)
		クラッシュダンプ

		アップタイム
		メモリ
		コンピューターシステム
		プロセッサ
		ビデオコントローラ
		ディスクドライブ
		ブラウザ情報
		再起動回数
		メモリ使用量
		ディスク使用量
		ICAセッション解像度
		ICAカラー深度

		メタインストーラーCEIPマシンID

		ストア数
		サーバーグループ内のサーバー数
		ストアあたりのDelivery Controller™数
		HTTPS有効
		Citrix Receiver™向けクラシックエクスペリエンスが有効
		Citrix Receiver向けHTML5 レシーバー設定
		Citrix Receiver向けワークスペースコントロールが有効
		ストア向けリモートアクセスが有効
		ゲートウェイ数
		統合されたNetScaler®認証用の明示的なJSONサービス

プロファイルコンテナのポリシー設定

プロファイルコンテナ

ユーザープロファイルに関連付けられた大きなフォルダーは、ログオンの遅延を引き起こします。Citrix Profile Managementは、プロファイルディスク（VHDXファイル）に含めるフォルダーを指定できるVHDXベースのプロファイルソリューションを提供します。このソリューションは、指定されたフォルダーをネットワークに保存されているプロファイルディスクにマッピングすることで、ログオン時間を短縮します。プロファイルコンテナは、ログオン時にこれらのフォルダーを含

むプロファイルディスクをアタッチするため、フォルダーのコピーをローカルプロファイルに保存する必要がなくなります。これにより、ログオン時間が短縮されます。

プロファイルコンテナのローカルキャッシュを有効にする

このポリシーは、Citrix Profile Managementプロファイルコンテナのローカルキャッシュサポートを有効にします。ポリシーが**有効**に設定されている場合、各ローカルプロファイルは、そのCitrix Profile Managementプロファイルコンテナのローカルキャッシュとして機能します。プロファイルストリーミングが使用されている場合、ローカルにキャッシュされたファイルはオンデマンドで作成されます。それ以外の場合は、ユーザーログオン時に作成されます。ローカルキャッシュ機能を使用するには、ユーザープロファイル全体をCitrix Profile Managementプロファイルコンテナに配置します。

プロファイルコンテナから除外するフォルダー

Citrix Profile Managementプロファイルコンテナから除外するフォルダーのリスト。

プロファイルコンテナに含めるフォルダー

親フォルダーが除外されている場合に、Citrix Profile Managementプロファイルコンテナに保持するフォルダーのリスト。

このリストのフォルダーは、除外されたフォルダーのサブフォルダーである必要があります。そうでない場合、この設定は機能しません。

プロファイルコンテナに含めるファイル

Citrix Profile Managementプロファイルコンテナに含めるファイルのリスト。

このリストのファイルは、除外されたフォルダー内にある必要があります。そうでない場合、この設定は機能しません。

プロファイルコンテナから除外するファイル

Citrix Profile Managementプロファイルコンテナから除外するファイルのリスト。

VHDディスクの圧縮を有効にする

プロファイル管理のVHDディスク圧縮を有効にできます。有効にすると、特定の条件が満たされた場合、ユーザーログオフ時にVHDディスクが自動的に圧縮されます。このポリシーにより、プロファイルコンテナ、OneDriveコンテナ、およびミラーフォルダーコンテナが消費するストレージスペースを節約できます。

必要に応じて、また利用可能なリソースに応じて、詳細設定にある「**VHDディスク圧縮をトリガーする空き領域の比率**」、「**VHDディスク圧縮をトリガーするログオフ回数**」、「**VHDディスク圧縮のデフラグを無効にする**」の各ポリシーを使用して、デフォルトのVHD圧縮設定と動作を調整できます。

プロファイルコンテナのVHD自動拡張を有効にする

プロファイルコンテナのVHD自動拡張を有効にするかどうかを指定できます。有効にすると、すべてのVHD自動拡張設定がプロファイルコンテナに適用されます。

構成の優先順位:

- ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
- ここでも.iniファイルでもこのポリシーが構成されていない場合、無効になります。

VHDコンテナへの排他的アクセスを有効にする

デフォルトでは、VHDコンテナは同時アクセスを許可します。この設定を有効にすると、一度に1つのアクセスのみが許可されます。この機能は、プロファイルコンテナとOneDriveコンテナに適用されます。

> **注:**

> コンテナベースのプロファイルソリューションでプロファイルコンテナに対してこの設定を有効にすると、*プロファイルコンテナの複数セッション書き戻しを有効にする*設定が自動的に無効になります。

> 構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
2. ここでも.iniファイルでもこのポリシーが構成されていない場合、この設定は無効になります。

ログオン時にプロファイルコンテナが利用できない場合にユーザーをログオフする

ユーザーログオン時にプロファイルコンテナが利用できない場合にユーザーを強制的にログオフさせ、(オプションで)ユーザーに表示されるエラーメッセージをカスタマイズできます。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
2. ここでも.iniファイルでもこのポリシーが構成されていない場合、設定は無効になります。

プロファイルコンテナにアクセスするユーザーとグループ

プロファイルコンテナに対してどのADドメインユーザーとグループが `Read & Execute` 権限を持つかを指定できます。デフォルトでは、プロファイルコンテナはその所有者のみがアクセスできます。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの設定が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、プロファイルコンテナはその所有者のみがアクセスできます。